ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΙΡΑΙΩΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

**ΔΙΟΙΚΗΣΗ ΤΗΣ ΥΓΕΙΑΣ**

ΤΕΙ
ΠΕΙΡΑΙΑ

ΑΝΤΩΝΟΓΛΟΥ Ι. ΔΗΜΗΤΡΙΟΣ

# ΒΙΟΜΕΤΡΙΚΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

Διπλωματική Εργασία για την απόκτηση
Μεταπτυχιακού Διπλώματος Ειδίκευσης

Πειραιάς, 2012

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΙΡΑΙΩΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ
ΣΠΟΥΔΩΝ

**ΔΙΟΙΚΗΣΗ ΤΗΣ ΥΓΕΙΑΣ**

ΤΕΙ
ΠΕΙΡΑΙΑ

ΑΝΤΩΝΟΓΛΟΥ Ι. ΔΗΜΗΤΡΙΟΣ

# ΒΙΟΜΕΤΡΙΚΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

*Επιβλέπων Καθηγητής :*
Καθηγητής, ΚΑΤΣΑΝΕΒΑΣ ΘΕΟΔΩΡΟΣ

Μελέτη για την απόκτηση
Μεταπτυχιακού Διπλώματος Ειδίκευσης

Πειραιάς, 2012

UNIVERSITY OF
PIRAEUS

MASTER SCIENCE
IN
**HEALTH MANAGEMENT**

T.E.I. OF
PIRAEUS

ANTONOGLOU I. DIMITRIOS

# BIOMETRIC AND APPLICATIONS



Graduate Thesis Submitted for the Degree "Master in Health Management"

Piraeus, 2012

**ΕΥΧΑΡΙΣΤΙΕΣ:**

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Θ. Κατσανέβα για την πολύτιμη καθοδήγηση και συμπαράστασή του κατά την διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας.

## ΠΕΡΙΛΗΨΗ:

Ο όρος βιομετρική αναφέρεται στην αυτοματοποιημένη αναγνώριση ενός ανθρώπου, με βάση χαρακτηριστικά της φυσιολογίας ή της συμπεριφοράς του. Ένα βιομετρικό σύστημα είναι στην ουσία σύστημα αναγνώρισης προτύπων, που εξακριβώνει την ταυτότητα του ατόμου καθορίζοντας την αυθεντικότητα ενός συγκεκριμένου βιολογικού του χαρακτηριστικού. Πρόκειται για μια ανερχόμενη μέθοδο πιστοποίησης, που τα τελευταία χρόνια φαίνεται να κερδίζει έδαφος σε σχέση με τις παραδοσιακές μεθόδους. Σκοπός αυτής της εργασίας είναι να μυήσει τον αναγνώστη στη φιλοσοφία της βιομετρικής, εντοπίζοντας τα πλεονεκτήματα και τις αδυναμίες της. Αυτό επιτυγχάνεται μέσα από την καταγραφή του τρόπου λειτουργίας των βιομετρικών συστημάτων, την αναφορά στις κυρίαρχες βιομετρικές τεχνολογίες της αγοράς και του ευρύτερου χώρου, τη διερεύνηση των διαφόρων βιομετρικών εφαρμογών, τον προβληματισμό γύρω από θέματα ιδιωτικότητας, και τέλος την κάλυψη ζητημάτων ασφαλείας που συνδέονται με τη χρήση βιομετρικής τεχνολογίας.

Η εργασία διαιρείται σε έξι κεφάλαια. Το πρώτο κεφάλαιο εισάγει τον αναγνώστη στην έννοια της βιομετρικής, δίνοντας αρχικά έναν πλήρη ορισμό της. Επίσης, γίνεται διάκριση των βιομετρικών συστημάτων σε συστήματα πιστοποίησης και συστήματα αναγνώρισης, καθώς επίσης και σε συστήματα φυσικής και λογικής πρόσβασης, και αναπτύσσονται οι διαφορές που υπάρχουν μεταξύ τους. Μετά από αυτή την εξοικείωση του αναγνώστη με τους σκοπούς και τις μεθόδους της βιομετρικής, στο δεύτερο κεφάλαιο αναπτύσσονται όλες οι γνωστές βιομετρικές τεχνολογίες, που αξιοποιούν χαρακτηριστικά της φυσιολογίας του ατόμου. Συγκεκριμένα, εξετάζονται σε ξεχωριστές ενότητες το σκανάρισμα των δαχτύλων, του προσώπου, της ίριδας, του χεριού, του αμφιβληστροειδούς χιτώνα, καθώς και το σκανάρισμα AFIS. Τα θέματα που μας απασχολούν είναι τα συστατικά μέρη, ο τρόπος λειτουργίας, οι κυρίαρχες τεχνολογίες, οι εφαρμογές, τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζει κάθε τεχνολογία. Τηρείται μια ενιαία δομή, που διευκολύνει την σύγκριση και κατάταξη των τεχνολογιών, και βοηθάει στο να προβάλλονται τα ιδιαίτερα χαρακτηριστικά τους. Όσα γράφονται στηρίζονται με συγκεκριμένα παραδείγματα, ενώ στο τέλος κάθε ενότητας υπάρχουν σύντομα συμπεράσματα σχετικά με τη χρησιμότητα και τις προοπτικές κάθε τεχνολογίας.

Το τρίτο κεφάλαιο έχει την ίδια δομή με το δεύτερο, με τη διαφορά ότι οι τεχνολογίες που αναπτύσσονται σ' αυτό σχετίζονται με χαρακτηριστικά της συμπεριφοράς του ατόμου. Η διάκριση είναι αναγκαία, λόγω των διαφορών που προκαλούνται σε θέματα απόδοσης και παραβίασης της ιδιωτικότητας. Έτσι, στο ίδιο κεφάλαιο διερευνώνται το σκανάρισμα της φωνής και το σκανάρισμα της υπογραφής καθώς και οι πιθανοί τρόποι ενσωμάτωσης των συναφών τεχνολογιών σε παραδοσιακά σχήματα πιστοποίησης. Και εδώ όσα αναγράφονται, τεκμηριώνονται με παραδείγματα από πραγματικές δοκιμές σε λειτουργικά περιβάλλοντα. Το τέταρτο κεφάλαιο είναι αφιερωμένο στις κατηγορίες των βιομετρικών εφαρμογών. Ανάλογα με το ρόλο του ατόμου, διακρίνουμε τις εφαρμογές πολιτών, τις διοικητικές εφαρμογές υπαλλήλων και τις εμπορικές εφαρμογές ή εφαρμογές πελατών. Με βάση την παραπάνω κατάταξη, προχωρούμε και αναπτύσσουμε περαιτέρω τις κυριότερες βιομετρικές εφαρμογές, που είναι η εγκληματολογική αναγνώριση, η αναγνώριση πολιτών, η επιτήρηση, η πρόσβαση σε υπολογιστές και δίκτυα, η φυσική πρόσβαση, το ηλεκτρονικό εμπόριο και το εμπόριο στο σημείο πώλησης. Για κάθε μία από αυτές τις εφαρμογές εξετάζονται οι τυπικές χρήσεις, οι χρησιμοποιούμενες τεχνολογίες, οι κάθετες αγορές, οι νέες τάσεις, το κόστος ανάπτυξης, καθώς και ζητήματα υλοποίησης. Επίσης, στο τέλος κάθε ενότητας παρατίθενται τα γενικά συμπεράσματα, για κάθε εφαρμογή. Στο πέμπτο κεφάλαιο, εξετάζονται οι περιπτώσεις παραβίασης της ανθρώπινης ιδιωτικότητας, και αναπτύσσονται μέτρα προφύλαξης ενάντια σ' αυτό το ενδεχόμενο. Τέλος, στο έκτο κεφάλαιο παρουσιάζεται η Υπηρεσία της Ελληνικής Αστυνομίας , Διεύθυνση Εγκληματολογικών Εργαστηρίων, που ασχολείται αποκλειστικά με βιομετρικές μεθόδους στο χώρο της ασφάλειας και ειδικότερα το αντικείμενο, οι αρμοδιότητες, η σύσταση και ο τρόπος λειτουργίας και μεθοδολογίας της. Μετά το πέρας του κεφαλαίου ακολουθούν τα γενικά συμπεράσματα και αναφορά στις πηγές της εργασίας.

Σ' όλο το φάσμα της παρούσης εργασίας, αποδεικνύεται ότι η βιομετρική αποτελεί εφραμοσμένη λύση σε πάρα πολλές περιπτώσεις, και ότι δεν κινείται στη σφαίρα του επιστημονικού πειράματος. Η πρόκληση βέβαια είναι να μπορέσει να εξαπλωθεί σε μεγαλύτερη έκταση και να κατακτήσει την αγορά, διατηρώντας τα ίδια επίπεδα αξιοπιστίας και υπευθυνότητας.

**ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ:** Βιομετρία, Μέθοδος πιστοποίησης, Βιομετρικές τεχνολογίες, Βιομετρική εφαρμογή Α.Φ.Ι.Σ., Έλεγχος και ανθρωπομετρικά χαρακτηριστικά.

Graduate Thesis Submitted for the Degree “Master in Health Management” University of Piraeus- TEI of Piraeus, Greece.

Supervisor: Dr Katsanevas Theodoros

The term Biometrics refers to the automated identification of a person based on physiological characteristics or behavior. A biometric system is essentially a pattern recognition system, which verifies the identity of the person determining the authenticity of a particular biological feature. This is an emerging authentication method, which in recent years seems to be gaining ground over traditional methods. The purpose of this paper is to introduce the reader to the concept of biometrics, identifying its strengths and weaknesses. This is achieved by recording the operation of biometric systems, reporting the dominant biometric technologies of the markets and the wider area, exploring the various biometric applications, the concern about privacy issues, and finally cover security issues associated with the use of biometric technology.

The work is divided into six chapters. The first chapter introduces the reader to the concept of biometrics, initially giving a full definition. Also, it distinguishes between biometric systems certification and recognition systems, as well as in natural and logical access, and the developing differences between them. After this the reader is acquainted with the purposes and methods of biometrics in the second chapter all the known biometric technologies are developed that exploit features of the physiology of the individual. Specifically in separate sections addressed the finger scan, the facial, the iris, the hand, the retina, and the AFIS scan. The issues that concern us are the components, the function, the dominant technologies, the applications, the advantages and disadvantages of each technology. A single structure is kept, which facilitates the comparison and ranking of technologies, and helps to highlight the special features. What is written is based on specific examples, while at the end of each section there are short conclusions on the usefulness and potentials of each technology.

The third chapter has the same structure as the second, except that the technologies developed in this are related to the behavioral characteristics of the individual. The distinction is necessary because of the differences caused in performance issues and the violation of privacy. Thus, in the same chapter the scanning of the voice and signature scanning are explored as well as the possible ways to integrate relevant technologies into traditional shapes of certification. And here what ever is written, are documented with examples from actual tests on operating environments. The fourth chapter is devoted to the categories of biometric applications. Depending on the role of the individual, we distinguish the citizens applications, the administrative applications of officials and commercial applications or applications of customers. Based on this classification, we progress and further develop the main biometric applications, which are the forensic identification, the recognition of citizens, surveillance, access to computers and networks, physical access, electronic commerce and trade as a selling point. For each of these applications typical uses, the technologies, vertical markets, new trends, development costs and implementation issues are examined. Also, at the end of each section the overall conclusions for each application are presented. The fifth chapter examines cases of violation of human privacy and develops precautionary measures against this possibility.

Finally, in the sixth chapter, the Office of the Greek Police Department Forensic Laboratory, is presented, which is dedicated to the biometric methods in the field of security and in particular the object, the composition and the operating methods and its methodology. After this chapter, general conclusions and a reference to the sources of labor are followed.

Throughout the range of the present study it is proven that a biometric solution is applied in many cases, and that does not move into the realm of scientific experiment. The challenge of course is for it to be able to spread more extensively and to conquer the market, keeping the same level of reliability and responsibility.

**KEYWORDS:** Biometrics, Authentication method, Biometric technology, Biometric A.F.I.S. implementation, testing and anthropometric characteristics.

**ΠΕΡΙΕΧΟΜΕΝΑ:**

**ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ ΣΤΗ ΒΙΟΜΕΤΡΙΚΗ**



**ΚΕΦΑΛΑΙΟ 2. ΚΥΡΙΑΡΧΕΣ ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΤΗΣ ΦΥΣΙΟΛΟΓΙΑΣ**

**ΚΕΦΑΛΑΙΟ 4. ΟΙ ΚΑΤΗΓΟΡΙΕΣ ΧΡΗΣΗΣ ΤΩΝ ΒΙΟΜΕΤΡΙΚΩΝ ΕΦΑΡΜΟΓΩΝ**



**ΚΕΦΑΛΑΙΟ 5. Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**



**ΚΕΦΑΛΑΙΟ 6. ΔΙΕΥΘΥΝΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΕΡΕΥΝΩΝ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ**

# Κατάλογος Σχημάτων

# 1. ΕΙΣΑΓΩΓΗ ΣΤΗ ΒΙΟΜΕΤΡΙΚΗ

Η πιστοποίηση της αυθεντικότητας είναι μια βασική ανάγκη στην αλληλεπίδραση ανθρώπου και υπολογιστή. Τα παραδοσιακά μέσα για επιβεβαίωση ταυτότητας – κυρίως οι κωδικοί και οι Προσωπικοί Αριθμοί Αναγνώρισης (Personal Identification Numbers (PINs)) – έχουν κυριαρχήσει στο χώρο των υπολογιστών και πιθανότατα θα συνεχίσουν να κυριαρχούν και τα προσεχή χρόνια. Ωστόσο, τον τελευταίο καιρό αναδύονται νέες τεχνολογίες, ικανές να προσφέρουν υψηλότερο βαθμό ασφάλειας. Η βιομετρική ανήκει σε αυτές τις πολλά υποσχόμενες τεχνολογίες πιστοποίησης αυθεντικότητας και μάλιστα συγκεντρώνει τις περισσότερες πιθανότητες για να εξαπλωθεί σύντομα σε ευρεία κλίμακα[1].

## 1.1 Η ΕΝΝΟΙΑ ΤΗΣ ΒΙΟΜΕΤΡΙΚΗΣ

Ο όρος βιομετρική αναφέρεται στην αυτοματοποιημένη χρήση χαρακτηριστικών της φυσιολογίας (physiological characteristics) ή της συμπεριφοράς (behavioral characteristics) του ατόμου, με στόχο τον καθορισμό ή την πιστοποίηση της ταυτότητάς του[2]. Η αυτοματοποιημένη χρήση δηλώνει το γεγονός ότι ο βιομετρικός έλεγχος διεξάγεται από υπολογιστές ή μηχανές. Ο ίδιος ο άνθρωπος καθημερινά ελέγχει χαρακτηριστικά της φυσιολογίας ή της συμπεριφοράς των συνανθρώπων του, για να επιβεβαιώσει ή να προσδιορίσει την ταυτότητά τους. Όμως ο έλεγχός του αυτός δεν είναι αυτοματοποιημένος. Αντίθετα, τα βιομετρικά συστήματα έχουν μια συγκεκριμένη διαδικασία που ακολουθούν. Αυτή η διαδικασία επιτρέπει τη διεξαγωγή χιλιάδων συγκρίσεων το δευτερόλεπτο και συνήθως διαρκεί λίγα δευτερόλεπτα. Συνεπώς και με βάση τα παραπάνω, ένας υπάλληλος της σήμανσης που προσπαθεί - χωρίς τη χρήση υπολογιστή - να βρει σε ποιον ανήκει ένα δακτυλικό αποτύπωμα, δε διεξάγει αυτοματοποιημένη βιομετρική πιστοποίηση ταυτότητας. Αντίθετα, ένα σύστημα που ζητά από το χρήστη να τοποθετήσει το δάχτυλό του στη μονάδα αναγνώρισης και το οποίο αποφασίζει σε πραγματικό χρόνο για το αν υπάρχει ταίριασμα

[1] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, and Arun Ross, “Recent Advances in Fingerprint Verification”.

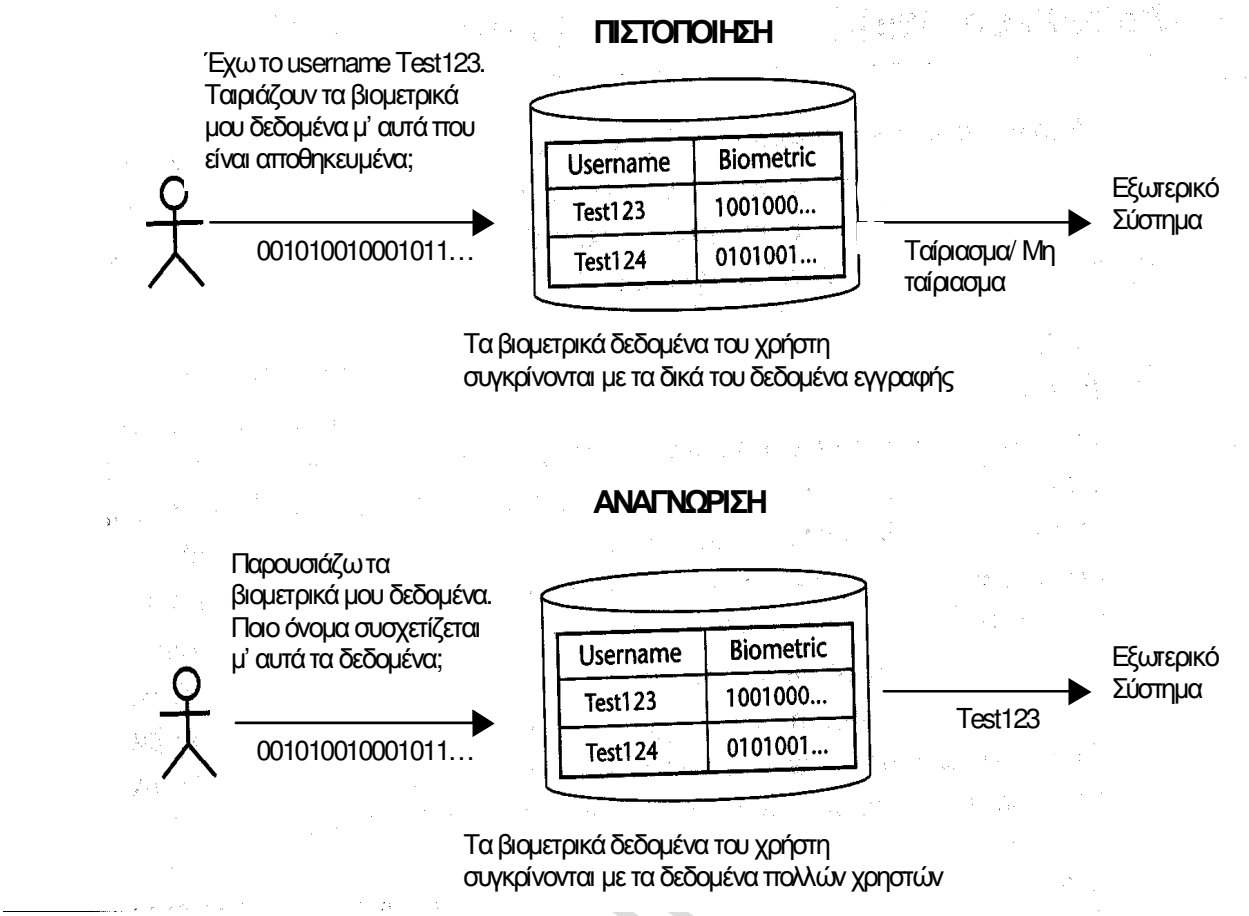
[2] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002.

δακτυλικού αποτυπώματος, πληροί τις προϋποθέσεις διενέργειας αυτοματοποιημένης βιομετρικής αναγνώρισης.

Όπως αναφέρθηκε, η βιομετρική βασίζεται στη μέτρηση διακριτών χαρακτηριστικών της φυσιολογίας ή της συμπεριφοράς του ατόμου. Χαρακτηριστικά της φυσιολογίας του ατόμου είναι για παράδειγμα τα δάχτυλα, το χέρι, το πρόσωπο, ή την ίριδα. Αντίθετα, η φωνή και η υπογραφή θεωρούνται χαρακτηριστικά της συμπεριφοράς. Ο τρόπος διάκρισης στηρίζεται στο ότι τα φυσιολογικά χαρακτηριστικά λαμβάνονται άμεσα, με απευθείας μέτρηση κάποιου σημείου του σώματος, ενώ τα χαρακτηριστικά της συμπεριφοράς είναι το αποτέλεσμα μιας πράξης και γενικά μετρούν με έμμεσο τρόπο τα χαρακτηριστικά του ανθρώπινου σώματος.

Η παραπάνω διάκριση είναι χρήσιμη από την άποψη ότι κάποια ζητήματα απόδοσης και ασφάλειας του βιομετρικού συστήματος διαφέρουν, ανάλογα με το είδος του χαρακτηριστικού που εξετάζεται. Απ' την άλλη η διάκριση είναι σε ένα βαθμό τεχνητή, αφού τα χαρακτηριστικά της συμπεριφοράς βασίζονται σε κάποια χαρακτηριστικά της φυσιολογίας του ατόμου, στα οποία μπορούν και να αναχθούν. Συγκεκριμένα, ο ήχος της φωνής εξαρτάται από τις φωνητικές χορδές, ενώ η υπογραφή από τη δεξιοτεχνία του χεριού και των δαχτύλων. Εξάλλου, και η βιομετρική της φυσιολογίας λαμβάνει πληροφορίες από τη συμπεριφορά του ατόμου, για παράδειγμα από τον τρόπο με τον οποίο το άτομο τοποθετεί το δάχτυλό του στη μονάδα αναγνώρισης ή κοιτάζει την κάμερα.

Ένα από τα κρίσιμα σημεία προς αποσαφήνιση στον ορισμό που δόθηκε για τη βιομετρική, είναι η διαφορά ανάμεσα στον καθορισμό και την πιστοποίηση ταυτότητας. Υπάρχουν βιομετρικά συστήματα που μπορούν να καθορίσουν την ταυτότητα ενός ατόμου με τη βοήθεια μιας βιομετρικής βάσης δεδομένων, χωρίς να χρειαστεί το ίδιο το άτομο να δηλώσει την ταυτότητά του. Αυτή η διαδικασία ονομάζεται αναγνώριση (identification) και τα βιομετρικά συστήματα που τη διεξάγουν συστήματα αναγνώρισης (identification systems). Υπάρχουν όμως και τα βιομετρικά συστήματα πιστοποίησης (verification systems). Σ' αυτά ένα άτομο προσέρχεται ισχυριζόμενο ότι έχει μια συγκεκριμένη ταυτότητα και το βιομετρικό σύστημα καλείται να αποδεχτεί ή να απορρίψει αυτόν τον ισχυρισμό. Τα συστήματα αναγνώρισης και πιστοποίησης διαφέρουν ουσιωδώς μεταξύ τους, τόσο από άποψη ασφάλειας και απόδοσης, όσο κι από άποψη ενσωμάτωσης σε υπάρχοντα συστήματα. Οι διαφορές αυτές αναπαρίστανται στο Σχήμα 1 και αναλύονται εκτενέστερα στην επόμενη ενότητα.




**Σχήμα 1.** Καθορισμός ταυτότητας – Πιστοποίηση ταυτότητας

Τέλος, πρέπει να γίνει ειδική αναφορά στην έννοια της ταυτότητας, που παρουσιάζει κάποιες ιδιαιτερότητες στο χώρο της βιομετρικής. Συχνά η έννοια της ταυτότητας θεωρείται ότι αναφέρεται σε ένα μεμονωμένο άτομο, κάτι όμως που δεν ισχύει πάντα, αφού ένα άτομο μπορεί να παρουσιάζεται κάτω από πολλές, διαφορετικές ταυτότητες. Αν κάποιος για παράδειγμα, έχει εγγραφεί με 10 δάχτυλα σ' ένα βιομετρικό σύστημα, τότε το σύστημα βλέπει δέκα διαφορετικές ταυτότητες και όχι ένα και μοναδικό άτομο. Συνεπώς, η αναγνώριση και η πιστοποίηση της ταυτότητας είναι ισχυρά και αξιόπιστα εργαλεία, μόνο υπό την προϋπόθεση ότι ο αρχικός συσχετισμός ανάμεσα στα βιομετρικά δεδομένα και το άτομο υπήρξε ακριβής. Εάν ένας χρήστης καταχωρηθεί σ' ένα βιομετρικό σύστημα με ψεύτικη ταυτότητα, τότε για κάθε εκ νέου είσοδο του χρήστη θα επικυρώνεται αυτή ακριβώς η ψεύτικη ταυτότητα.

## 1.2 ΣΥΓΧΡΟΝΕΣ ΑΝΤΙΛΗΨΕΙΣ ΓΙΑ ΤΗΝ ΒΙΟΜΕΤΡΙΑ

Εκατομμύρια άνθρωποι σε όλον τον κόσμο χρησιμοποιούν αριθμούς και λέξεις-κλειδιά για να κάνουν τη ζωή τους πιο εύκολη ή έτσι τουλάχιστον νομίζουν. Ως τη στιγμή που η μνήμη τους φθάνει σε οριακό σημείο, αρνιώντας να δώσει πληροφορίες, ακόμη και τις πιο απλές και χρηστικές, όπως είναι προσωπικοί κωδικοί αριθμοί. Τους οποίους μπορεί να χρησιμοποιούν καθημερινά για να έχουν πρόσβαση σε διάφορες συσκευές, από το κινητό τηλέφωνο και τον ηλεκτρονικό υπολογιστή ως τον συναγερμό και τις ΑΤΜ.

Ένας μέσος άνθρωπος μπορεί να συγκρατήσει στη βραχυπρόθεσμη μνήμη του από πέντε ως εννέα (επτά συν δύο) πληροφοριακά στοιχεία. Το επιστημονικό αυτό εύρημα έχει πρακτικό αντίκρισμα στη ζωή μας, καθώς οι αριθμοί που χρειάζεται να αποστηθίσουμε, π.χ. αριθμοί τηλεφώνου, αστυνομικής ταυτότητας κ.ο.κ., δεν ξεπερνούν συνήθως τους επτά. Αυτό που κάνει για την ακρίβεια ο εγκέφαλός μας όταν καλούμαστε να αποστηθίσουμε μια σειρά από αριθμούς είναι ο καλύτερος δυνατός συσχετισμός του κάθε πληροφοριακού στοιχείου και η οργάνωσή τους έτσι ώστε να συγκρατήσουμε τελικά κάποιους συνδυασμούς που μας επιτρέπουν να ανακαλούμε την πληροφορία όταν χρειαστεί[1]. Ο ανθρώπινος εγκέφαλος μπορεί να αποθηκεύσει άπειρες μονάδες πληροφορίας, ενώ έχει τη δυνατότητα να ξεχνάει άλλες τόσες (κάτι που λειτουργεί ως βαλβίδα ασφαλείας της ανθρώπινης μνήμης). Παρ' όλα αυτά στη σημερινή εποχή ο άνθρωπος αντιμετωπίζει όλο και πιο συχνά το εξής πρόβλημα: ο αριθμός των πληροφοριών που καλείται να συσχετίσει ταυτόχρονα είναι υπερβολικά μεγάλος και αυτό του δημιουργεί σύγχυση ή ακόμη και (πρόσκαιρο) μπλακ άουτ όταν πρέπει να ανακαλέσει μια συγκεκριμένη πληροφορία από τη μνήμη.

Πρόκειται για ένα σύνολο (αυτοματοποιημένων) τεχνικών για την αναγνώριση κάποιου ατόμου, οι οποίες βασίζονται σε ένα ιδιαίτερο χαρακτηριστικό της φυσιολογίας ή της συμπεριφοράς του. Οι βιομετρικές μέθοδοι κάνουν πιστοποίηση ή αναγνώριση. Στην πρώτη περίπτωση, που βασίζεται στα φυσικά χαρακτηριστικά του ατόμου, περιλαμβάνονται η αναγνώριση δακτυλικών αποτυπωμάτων, της ίριδας του ματιού, της γεωμετρίας του χεριού, ενώ στη δεύτερη γίνεται (απλή) αναγνώριση μέσω της φωνής του ατόμου και της υπογραφής του.[2]

[1] Εξηγεί ο καθηγητής Μοριακής Νευροβιολογίας στο Πανεπιστήμιο του Τέξας κ. Ε. Σκουλάκης
[2] Εξηγεί ο αναπληρωτής καθηγητής στο Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών του Πανεπιστημίου Πάτρας κ. Δ. Ν. Σερπάνος.

Η χρήση του μυστικού αριθμού pin (Personal Identification Number) και του κωδικού πρόσβασης (password) στις τραπεζικές συναλλαγές, στην κινητή τηλεφωνία, στους ηλεκτρονικούς υπολογιστές αποτελεί την απλούστερη μέθοδο βιομετρίας, που έχει μέχρι στιγμής ευρεία εφαρμογή στην ζωή του σύγχρονου ανθρώπου. Η διάδοση των ηλεκτρονικών συναλλαγών επιβάλλει ωστόσο τη διασφάλιση του χρήστη. Οι παραβιάσεις των κωδικών αυτών με διάφορους τρόπους αποτελούν σχεδόν καθημερινό φαινόμενο και παρ' όλο που καμία μεθοδολογία δεν αποτελεί πανάκεια είναι γεγονός ότι πρέπει πλέον να χρησιμοποιηθούν νέες διαφορετικές μέθοδοι πιστοποίησης της ταυτότητας ενός ατόμου. Το (μείζον) ζήτημα της ασφάλειας που παρέχουν οι βιομετρικές μέθοδοι είναι η μία όψη του θέματος[1].

## 1.3 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η διαδικασία της βιομετρικής πιστοποίησης και αναγνώρισης ακολουθεί ένα συγκεκριμένο διάγραμμα ροής εργασιών. Οι διεργασίες που συντελούνται είναι οι εξής:

- Ο χρήστης αρχικά εγγράφεται στο βιομετρικό σύστημα παρέχοντας ένα δείγμα από τα βιομετρικά δεδομένα του, το οποίο μετατρέπεται σε προσωρινό αρχείο (template).
- Τα προσωρινά αρχεία (templates) αποθηκεύονται στο βιομετρικό σύστημα για να χρησιμοποιηθούν για μελλοντικές συγκρίσεις.
- Κάθε φορά που ο χρήστης πρέπει να υποβληθεί σε πιστοποίηση ή αναγνώριση, προσφέρει τα βιομετρικά του δεδομένα, τα οποία μετατρέπονται σε ένα ένα προσωρινό αρχείο (template).
- Το προσωρινό αρχείο (template) που παράχθηκε συγκρίνεται με ένα ή περισσότερα από τα αποθηκευμένα προσωρινά αρχεία (templates).
- Το αποτέλεσμα της σύγκρισης είναι το ποσοστό εμπιστοσύνης για το συγκεκριμένο δείγμα, το οποίο με τη σειρά του συγκρίνεται με μια τιμή που έχει οριστεί για τη συγκεκριμένη τεχνολογία, το σύστημα, το χρήστη και τη συναλλαγή
- Αν το ποσοστό εμπιστοσύνης υπερβαίνει την τιμή, τότε η σύγκριση θεωρείται επιτυχής και ο χρήστης ενημερώνεται.
- Αν το ποσοστό εμπιστοσύνης είναι μικρότερο από την τιμή, τότε η σύγκριση θεωρείται ανεπιτυχής και ο χρήστης ενημερώνεται[2].

---

[1] Εξηγεί ο καθηγητής Μοριακής Νευροβιολογίας στο Πανεπιστήμιο του Τέξας κ. Ε. Σκουλάκης.

[2] S. C. Dass, A. K. Jain and X. Lu, "Face Detection And Synthesis Using Markov Random Field Models", Proc. International Conference on Pattern Recognition, Quebec City, August 11-15, 2002.

Τα δεδομένα που παρέχει ο χρήστης στο σύστημα είναι μη επεξεργασμένα και δεν μπορούν να χρησιμοποιηθούν αυτούσια για τη διεξαγωγή συγκρίσεων. Πρέπει πρώτα να μετατραπούν σε μια άλλη μορφή, που να μπορεί να αναγνωρίσει και να επεξεργαστεί ο υπολογιστής. Η μορφή αυτή είναι τα προσωρινα αρχεία (templates). Το αρχείο αυτό (template) είναι ένα συστατικό στοιχείο της βιομετρικής τεχνολογίας, ουσιώδες για την κατανόηση του τρόπου λειτουργίας των βιομετρικών συστημάτων. Πρόκειται στην ουσία για ένα μικρό αρχείο, που προκύπτει από τα διακριτά χαρακτηριστικά των βιομετρικών δεδομένων του χρήστη και χρησιμοποιείται για τη διενέργεια συγκρίσεων. Χάρη στην τεχνολογία των αρχείων (templates), τα ίδια τα βιομετρικά δεδομένα δεν αποθηκεύονται στο σύστημα και αγνοούνται σχεδόν απ' όλα τα συστήματα.

Ανάλογα με το πότε παράχθηκαν, τα προσωρινά αρχεία templates διακρίνονται σε εγγραφής και ταιριάσματος. Τα πρώτα παράγονται κατά την αρχική αλληλεπίδραση του χρήστη με το σύστημα και αποθηκεύονται για μελλοντικές συγκρίσεις, ενώ τα δεύτερα παράγονται κατά τη διάρκεια της διαδικασίας αναγνώρισης ή πιστοποίησης, προκύπτουν συνήθως από ένα και μόνο δείγμα και απορρίπτονται μετά τη σύγκριση με τα αποθηκευμένα.

## 1.4 ΣΥΣΤΗΜΑΤΑ ΠΙΣΤΟΠΟΙΗΣΗΣ & ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ

Στη βιομετρική υπάρχουν δύο ειδών συστήματα: τα συστήματα πιστοποίησης και τα συστήματα αναγνώρισης. Τα συστήματα πιστοποίησης απαντούν στο ερώτημα «Είμαι αυτός που ισχυρίζομαι;» ζητώντας από το χρήστη να δηλώσει, αλλά και να αποδείξει την ταυτότητά του. Αυτό γίνεται με την προμήθεια εκ μέρους του των απαραίτητων βιομετρικών δεδομένων και τη σύγκρισή τους με τα βιομετρικά δεδομένα που βρίσκονται αποθηκευμένα στη βάση δεδομένων. Η απάντηση που επιστρέφεται από το σύστημα είναι είτε θετική είτε αρνητική και η προσπάθεια για ταίριασμα γίνεται αποκλειστικά με τα αποθηκευμένα βιομετρικά δεδομένα του φερόμενου ως χρήστη. Γι' αυτό και η πιστοποίηση αναφέρεται και σαν 1:1, δηλαδή ένα-προς-ένα.[1]

[1] N. Duta, A. K. Jain, and Kanti V. Mardia, "Matching of Palmprint", *Pattern Recognition Letters*, vol. 23, Number 4, pp. 477-485, 2002.

Τα συστήματα αναγνώρισης απαντούν στο ερώτημα «Ποιος είμαι;» και δεν απαιτούν από το χρήστη να δηλώσει μια ταυτότητα, προτού διεξαχθεί η βιομετρική μέτρηση. Ο χρήστης απλά προμηθεύει το σύστημα με τα βιομετρικά του δεδομένα, τα οποία συγκρίνονται με τα βιομετρικά δεδομένα ενός πλήθους χρηστών, μέχρι να βρεθεί ταίριασμα. Η απάντηση που επιστρέφει το σύστημα είναι μια ταυτότητα, που μπορεί να είναι ένα όνομα ή ένας αριθμός ID κτλ. Ο έλεγχος αναγνώρισης αναφέρεται και σαν 1:N, δηλαδή ένα-προς-N ή ένα-προς-πολλά, επειδή τα δεδομένα του κάθε ατόμου συγκρίνονται με πολλές εγγραφές κάθε φορά. Στην αναγνώριση υπάρχουν συγκεκριμένες βιομετρικές τεχνολογίες οι οποίες χρησιμοποιούνται, κι αυτές είναι το σκανάρισμα του δακτύλου, το σκανάρισμα της ίριδα και σε ένα βαθμό το σκανάρισμα του προσώπου. Η φωνή, η υπογραφή και το χέρι δεν προσφέρονται τόσο για αναγνώριση, γιατί στηρίζονται σε χαρακτηριστικά της φυσιολογίας και της συμπεριφοράς, τα οποία δεν εγγυώνται τη ρητή διάκριση των ατόμων.

Συστήματα αναγνώρισης με περισσότερους από 100.000 χρήστες θεωρούνται μεγάλης κλίμακας και διαφέρουν σημαντικά σε σχέση με τα συστήματα μικρής κλίμακας, σε ζητήματα ακρίβειας, χρόνου απόκρισης κτλ. Τα συστήματα αναγνώρισης διαιρούνται περαιτέρω σε συστήματα θετικά και συστήματα αρνητικά. Τα θετικά συστήματα αναγνώρισης είναι σχεδιασμένα για να βρίσκουν ταίριασμα ανάμεσα στα βιομετρικά δεδομένα του χρήστη και της βάσης, δηλαδή για κάθε δείγμα πρέπει να υπάρχει και ταίριασμα. Τέτοια συστήματα έχουν για παράδειγμα χρησιμότητα σε μια φυλακή. Αντίθετα, τα αρνητικά συστήματα αναγνώρισης έχουν ως σκοπό να αποκλείσουν την περίπτωση να υπάρχουν ήδη στη βάση δεδομένων τα βιομετρικά δεδομένα ενός ατόμου. Έτσι διασφαλίζεται π.χ. ότι κανείς δεν μπορεί να εγγραφεί δύο φορές σε ένα σύστημα, επωφελούμενος από προνόμια και παροχές που δε δικαιούται.

Κάθε ένα από τα συστήματα πιστοποίησης και αναγνώρισης έχει πλεονεκτήματα και αδυναμίες. Συνήθως η ίδια η εφαρμογή υπαγορεύει τη χρήση του ενός ή του άλλου. Όταν για παράδειγμα πρέπει να διαφυλαχτεί η ασφάλεια ενός υπολογιστή ή ενός δικτύου, συνήθως χρησιμοποιούνται συστήματα πιστοποίησης. Η πρόσβαση σε κτίρια και δωμάτια γίνεται και με συστήματα πιστοποίησης και με συστήματα αναγνώρισης, με τα πρώτα να κυριαρχούν, ενώ τα συστήματα αναγνώρισης κατά κανόνα χρησιμοποιούνται σε προγράμματα δημόσιων παροχών μεγάλης κλίμακας. Αυτό γίνεται για συγκεκριμένους λόγους, που έχουν να κάνουν με τις ιδιαιτερότητες των δύο συστημάτων.

Αναλυτικότερα, τα συστήματα πιστοποίησης είναι συνήθως πιο γρήγορα και ακριβή, γιατί διενεργούν μόνο μία σύγκριση κάθε φορά. Γι' αυτό και η υπολογιστική δύναμη που απαιτούν είναι σαφώς μικρότερη και η πιθανότητα να κάνουν λάθος πολύ μικρή. Ακόμη, ο χρόνος απόκρισής τους συνήθως δεν υπερβαίνει το δευτερόλεπτο. Ωστόσο, τα συστήματα πιστοποίησης μειονεκτούν, ως προς το ότι δεν μπορούν να εξακριβώσουν, αν ένα συγκεκριμένο άτομο βρίσκεται αποθηκευμένο στη βάση δεδομένων περισσότερες από μία φορές. Τα συστήματα αναγνώρισης από την άλλη, έχουν μεγαλύτερες απαιτήσεις σε υπολογιστική ισχύ, αφού τις περισσότερες φορές πρέπει να κάνουν πάρα πολλές συγκρίσεις – ακόμα κι εκατομμύρια – για να υπάρξει αντιστοιχία με τα αποθηκευμένα δεδομένα. Εξαιτίας αυτού του φόρτου των συγκρίσεων όμως, αυξάνεται και η πιθανότητα λάθους. Γι' αυτό τα συστήματα αναγνώρισης χρησιμοποιούνται μόνο στις περιπτώσεις που τα συστήματα πιστοποίησης δεν επαρκούν, όπως – για παράδειγμα – όταν υπάρχει ανάγκη εξάλειψης διπλών εγγραφών. Έτσι, παρότι εκ πρώτης όψεως η χρήση συστημάτων αναγνώρισης σε περιβάλλοντα desktop φαίνεται ελκυστική, στην πραγματικότητα το κόστος σε ακρίβεια και ταχύτητα υπερβαίνει τα οφέλη της εξάλειψης κάποιων επιπλέον ID.

Ωστόσο, υπάρχει και μια μέση λύση που είναι γνωστή ως 1:λίγα, στην οποία η έρευνα για αναγνώριση περιορίζεται σε ένα πολύ μικρό αριθμό χρηστών. Αυτό που συμβαίνει είναι ότι ο χρήστης εφοδιάζει το σύστημα με τα βιομετρικά δεδομένα του, τα οποία στη συνέχεια συγκρίνονται με τα βιομετρικά δεδομένα ενός μικρού αριθμού από εγγεγραμμένους χρήστες. Ο ακριβής αριθμός των χρηστών δεν προσδιορίζεται σαφώς, οι χρήστες μπορεί να είναι 10 ή και 100, έτσι η διαχωριστική γραμμή ανάμεσα στις εφαρμογές 1:λίγα και 1:πολλά είναι λεπτή.

## 1.5 ΣΥΣΤΗΜΑΤΑ ΦΥΣΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΛΟΓΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

Ανάλογα με τον σκοπό τον οποίο εξυπηρετεί η πιστοποίηση ή η αναγνώριση, τα βιομετρικά συστήματα μπορούν να διαιρεθούν σε συστήματα φυσικής πρόσβασης (physical access) και λογικής πρόσβασης (logical access)[1]. Τα συστήματα φυσικής πρόσβασης επιτρέπουν ή αρνούνται την είσοδο ή την έξοδο από μια συγκεκριμένη περιοχή και καταγράφουν την παρουσία ενός ατόμου ή ενός αντικειμένου σε συνδυασμό με τη χρονική στιγμή στην οποία αυτή συνέβη. Συνήθως βέβαια η φυσική πρόσβαση αφορά στην είσοδο σ' ένα κτίριο ή ένα

[1] "Biometrics for Identification and Authentication - Advice on the Selection of Biometric Products", CESG. Issue 1.0, 23 November 2001.

δωμάτιο. Ένα θησαυροφυλάκιο, ο πύργος ελέγχου, το δωμάτιο του server είναι υποψήφιοι χώροι. Άλλες φορές η φυσική πρόσβαση σχετίζεται με την πρόσβαση σε εξοπλισμό ή υλικά, για παράδειγμα με το άνοιγμα μιας θυρίδας ή το ξεκίνημα ενός αυτοκινήτου, αν και πολλές από αυτές τις περιπτώσεις είναι ακόμα υποθετικές. Πάντως, σε συστήματα φυσικής πρόσβασης η βιομετρική αντικαθιστά ή δρα συμπληρωματικά στη χρήση κλειδιών, καρτών πρόσβασης, ατομικών κωδικών αριθμών (PIN) ή την παρουσία φρουρών. Από την άλλη, τα συστήματα λογικής πρόσβασης παρακολουθούν και ανάλογα επιτρέπουν ή αποτρέπουν την πρόσβαση σε πληροφορίες ή δεδομένα. Η πρόσβαση σε έναν Η/Υ (PC) ή στα αποθηκευμένα δεδομένα ενός δικτύου, η επικύρωση μιας συναλλαγής και η διευθέτηση ενός λογαριασμού είναι παραδείγματα περιπτώσεων, όπου η πρόσβαση είναι λογική. Σε όλες τις παραπάνω περιπτώσεις η βιομετρική αντικαθιστά ή δρα σε συνδυασμό με ατομικούς κωδικούς (PINs) και έγγραφα.

Πρέπει να τονιστεί πάντως ότι και σε περιπτώσεις φυσικής και λογικής πρόσβασης ο πυρήνας της βιομετρικής λειτουργικότητας, δηλαδή η απόκτηση και σύγκριση των βιομετρικών δεδομένων, παραμένει ο ίδιος. Έτσι, ο ίδιος αλγόριθμος βιομετρικού ελέγχου μπορεί να χρησιμοποιηθεί και από εφαρμογές desktop και από εφαρμογές που ελέγχουν την είσοδο από μία πόρτα. Το μόνο που αλλάζει είναι το εξωτερικό σύστημα, στο οποίο ενσωματώνεται η βιομετρική λειτουργικότητα κάθε φορά, στο παράδειγμά μας το σύστημα ελέγχου της πόρτας ή το λειτουργικό σύστημα. Και φυσικά αντίστοιχα επηρεάζεται και η λειτουργία που ακολουθεί ένα επιτυχές ταίριασμα, το άνοιγμα δηλαδή της πόρτας ή η πρόσβαση στο λειτουργικό σύστημα.

Η τεράστια σημασία των πληροφοριών που βρίσκονται αποθηκευμένες σε συνεταιρικά δίκτυα και ο αυξανόμενος όγκος των συναλλαγών ηλεκτρονικού εμπορίου , επιχείρηση σε επιχείρηση (business-to-business (B2B)) και επιχείρηση σε πελάτη (business-to-customer (B2C)), ωθεί τη βιομηχανία της βιομετρικής στο να επικεντρώσει το ενδιαφέρον της σε συστήματα και εφαρμογές λογικής πρόσβασης, που μακροπρόθεσμα θεωρούνται πιο επικερδή. Κι αυτό, γιατί ένα άτομο μπορεί μέσα σε μια μέρα να αναγκαστεί να πιστοποιήσει την ταυτότητά του 20 με 30 φορές, ενώ τα περιστατικά στα οποία απαιτείται φυσική πρόσβαση είναι πιο σπάνια. Ακόμη, η αξία των αποθηκευμένων πληροφοριών και το γεγονός της όλο και πιο συχνής ανάγκης για απομακρυσμένη πρόσβαση σε αυτές, ενισχύει την υπάρχουσα τάση για τα συστήματα λογικής πρόσβασης, χωρίς αυτό να σημαίνει ότι η βιομετρική δεν μπορεί να ανταποκριθεί εξίσου καλά και στα δύο είδη εφαρμογών.

Ωστόσο, πρέπει να τονιστεί ότι η διάκριση σε εφαρμογές λογικής και φυσικής πρόσβασης δεν είναι πάντοτε απόλυτη. Υπάρχουν συστήματα αναγνώρισης – ιδίως τα μεγάλης κλίμακας – που είναι δύσκολο να κατηγοριοποιηθούν, για το λόγο ότι δεν υπάρχει σαφής πρόσβαση είτε σε δεδομένα είτε σε κάποια τοποθεσία. Ένα βιομετρικό μηχάνημα αυτόματης ταμειακής ανάληψης (τύπου ATM) για παράδειγμα, παρέχει μεν πρόσβαση σε χρήματα, δηλαδή σε ένα αντικείμενο, αυτό όμως γίνεται εφικτό, αφού πρώτα ο χρήστης έχει λογική πρόσβαση στα δεδομένα που τον αφορούν. Τέλος, ακόμα και αν υπάρξει μια τρίτη κατηγορία, των εφαρμογών εκείνων που είναι δύσκολο να καταταγούν, η διάκριση ανάμεσα σε φυσική και λογική πρόσβαση είναι ένα χρήσιμο εργαλείο για την κατανόηση της βιομετρικής. Και αυτό, γιατί υπάρχουν πολύ σημαντικοί παράγοντες, όπως η ακρίβεια, ο χρόνος απόκρισης, το κόστος, η πολυπλοκότητα ενσωμάτωσης, καθώς και ζητήματα ιδιωτικότητας (privacy), τα οποία διαφοροποιούνται ανάλογα με το είδος της πρόσβασης.

## 1.6 Η ΒΙΟΜΕΤΡΙΚΗ ΣΕ ΣΥΓΚΡΙΣΗ ΜΕ ΤΙΣ ΠΑΡΑΔΟΣΙΑΚΕΣ ΜΕΘΟΔΟΥΣ

Αφού αναπτύξαμε τον τρόπο λειτουργίας της βιομετρικής τεχνολογίας μπορούμε να εκτιμήσουμε περισσότερο τα οφέλη που συνάδουν με τη χρήση της. Η βιομετρική είναι μια τεχνολογία που χρησιμοποιείται σε πάρα πολλές εφαρμογές, από τις πιο μετριοπαθείς ως τις πιο σύνθετες. Προσφέρει σημαντικά πλεονεκτήματα, όπως είναι η αύξηση της ασφάλειας, η διευκόλυνση των πελατών, ο περιορισμός της απάτης, η πρόσβαση σε προσωπικούς και απόρρητους χώρους, η πρόσβαση σε δίκτυα, η ανεύρεση υπόπτων, η αναγνώριση εκφράσεων προσώπων, εφαρμογές ασφάλειας, τάξης και άμυνας και γενικότερα η αναβάθμιση των υπηρεσιών. Συνήθως η βιομετρική έχει έναν ουσιώδη ρόλο να διαδραματίσει στη λειτουργία του συστήματος, αν και υπάρχουν περιπτώσεις στις οποίες χρησιμοποιείται περισσότερο για να αποθαρρύνει επίδοξους παραβάτες. Το βέβαιο είναι ότι προσφέρει αυξημένη βεβαιότητα για την ταυτότητα ενός ατόμου, γεγονός που αποτελεί εγγύηση για την αξιοπιστία, την οικονομική σταθερότητα και την ευημερία του εκάστοτε οργανισμού.

### 1.6.1 Πλεονεκτήματα σε συστήματα πιστοποίησης αυθεντικότητας

Οι πιο διαδεδομένες τεχνολογίες για πιστοποίηση αυθεντικότητας είναι οι κωδικοί (passwords) και οι προσωπικοί αριθμοί αναγνώρισης (PINs). Οι δύο αυτές τεχνολογίες έχουν ένα ευρύ πεδίο εφαρμογών. Ενδεικτικά αναφέρουμε ότι χρησιμοποιούνται για έλεγχο της πρόσβασης σε υπολογιστές, έλεγχο εισόδου σε απαγορευμένες περιοχές κτιρίων, εξουσιοδότηση μηχανών αυτόματης ταμειακής ανάληψης (ATM) κτλ. Σε εφαρμογές με

μεγαλύτερες απαιτήσεις για ασφάλεια βέβαια, είθισται οι κωδικοί να αντικαθίστανται από φορητές κάρτες. Ωστόσο και οι κάρτες, αλλά και τα PINs και οι κωδικοί παρουσιάζουν μια σειρά από προβλήματα, που θέτουν υπό αμφισβήτηση το βαθμό καταλληλότητάς τους για σύγχρονες απαιτητικές εφαρμογές, όπως η on-line πρόσβαση σε λογαριασμούς ή σε απόρρητα ιατρικά δεδομένα κτλ. Η βιομετρική από την άλλη, διακρίνεται για μια σειρά από πλεονεκτήματα στο θέμα της πιστοποίησης αυθεντικότητας, που της επιτρέπουν να επιλύει αυτά τα προβλήματα. Αναλυτικά τα πλεονεκτήματα που παρουσιάζει αναπτύσσονται στις επόμενες παραγράφους.

**Αυξημένη ασφάλεια**

Η βιομετρική[1], σε σύγκριση με παραδοσιακές μεθόδους πιστοποίησης αυθεντικότητας, προσφέρει μεγαλύτερη ασφάλεια, γιατί διασφαλίζει ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στους πόρους εκείνους που απαιτούνται για την πιστοποίηση της ταυτότητάς τους. Αυτή η εγγύηση συνήθως δεν υπάρχει με τους κωδικούς που, όπως αποδεικνύει και η καθημερινή πρακτική, παραβιάζονται και μάλιστα εύκολα. Η ευθύνη βέβαια βαρύνει σε μεγάλο βαθμό τους ίδιους τους χρήστες, οι οποίοι υποπίπτουν σε σωρεία λαθών. Από τα πιο συνηθισμένα είναι να επιλέγουν για κωδικούς λέξεις ή αριθμούς που είναι ευκολομνημόνευτοι (και άρα εύκολα παραβιάσιμοι) ή ακόμα χειρότερα να καταγράφουν τον κωδικό τους σε εμφανές σημείο, από φόβο μην το ξεχάσουν. Το αποτέλεσμα είναι το σύστημα να καθίσταται διάτρητο και ευάλωτο, ακόμα και στις πιο απλές επιθέσεις, όπως είναι το να μαντέψει κάποιος έναν κωδικό. Οι κάρτες δεν επιλύουν εξολοκλήρου το πρόβλημα, αφού και αυτές μπορεί να κλαπούν, να απολεσθούν κτλ.

Τα βιομετρικά δεδομένα αντίθετα, δεν παρουσιάζουν καμία από τις προαναφερθείσες αδυναμίες. Δεν μπορούν να κλαπούν, όπως οι κάρτες, και είναι αδύνατον να τα μαντέψει κανείς, όπως συμβαίνει με τους κωδικούς. Σε αντίθεση με παλαιότερες εποχές, είναι εξαιρετικά απίθανο να ξεγελάσει κανείς τα σύγχρονα μηχανήματα βιομετρικής με τη φωτογραφία ενός προσώπου, τον ηχογραφημένο ήχο μιας φωνής και άλλα παρόμοια τρικ. Ενώ ακόμη και στα συστήματα εκείνα όπου η βιομετρική διαδικασία πιστοποίησης παράγει έναν κωδικό για κάθε χρήστη, δηλαδή και όταν διατηρείται η δομή χρήστης-κωδικός, οι

[1] http://www.biometricgroup.com

προκύπτοντες κωδικοί είναι πολύ μεγάλοι και ιδιαίτερα πολύπλοκοι, κι έτσι δεν συντρέχουν οι κίνδυνοι για τους οποίους κάναμε λόγο.

Όλα τα παραπάνω βέβαια δεν υπονοούν ότι τα βιομετρικά συστήματα είναι άτρωτα και ασφαλή απέναντι σε επιθέσεις. Υπάρχουν σημαντικά ζητήματα ασφαλείας, που πρέπει να αντιμετωπισθούν κατά τη φάση του σχεδιασμού και σε αυτά θα αναφερθούμε εκτενώς σε επόμενη ενότητα. Το γεγονός ωστόσο παραμένει, τα βιομετρικά συστήματα είναι σημαντικά πιο ασφαλή σε σχέση με εκείνα που στηρίζονται σε κάρτες, PINs και κωδικούς κι αυτός είναι και ο λόγος που ολοένα και περισσότερες επιχειρήσεις και φορείς επιλέγουν να τα εντάξουν στο σύστημα ασφαλείας τους.

**Μεγαλύτερη διευκόλυνση**

Όπως ήδη αναφέραμε, οι κωδικοί διατηρούνται απλοί για λόγους εύκολης απομνημόνευσης. Αυτό όμως συνεπάγεται σημαντικούς κινδύνους για την ασφάλεια του συστήματος. Απ' τη στιγμή μάλιστα που ο χρήστης πρέπει να χρησιμοποιεί όχι έναν, αλλά περισσότερους κωδικούς, η πιθανότητα να ξεχάσει κάποιον απ' αυτούς μεγαλώνει, εκτός αν χρησιμοποιεί τον ίδιο κωδικό παντού, πράγμα που μειώνει ακόμα περισσότερο την ασφάλεια του συστήματος. Κάτι αντίστοιχο συμβαίνει με τα έγγραφα και τις κάρτες, τα οποία μπορεί ο χρήστης να απολέσει.

Για προφανείς λόγους τα παραπάνω προβλήματα δεν υφίστανται, όταν χρησιμοποιείται βιομετρική τεχνολογία. Τα βιομετρικά χαρακτηριστικά εκάστου (η ίριδα, τα δακτυλικά αποτυπώματα, το σχήμα προσώπου κτλ.) δεν υπόκεινται σε κίνδυνο απώλειας κι έτσι παρέχουν μεγαλύτερη διευκόλυνση στη διεξαγωγή των συναλλαγών, τόσο για το χρήστη όσο και για το σύστημα.. Σε εφαρμογές υπολογιστών, για παράδειγμα, όταν ο χρήστης επιθυμεί να έχει πρόσβαση σε διάφορους πόρους, μία και μόνο διαδικασία πιστοποίησης αντικαθιστά την ανάγκη για ένα πλήθος κωδικών, απαλλάσσοντας έτσι από το επιπλέον φορτίο τόσο το χρήστη όσο και το διαχειριστή του συστήματος[1].

Επιπλέον, η βιομετρική πιστοποίηση της αυθεντικότητας διευκολύνει σε μεγάλο βαθμό την παραχώρηση προνομίων και δικαιωμάτων υψηλότερου επιπέδου. Συγκεκριμένα, απόρρητα

[1] http://stat.tamu.edu/Biometrics

και ευαίσθητα δεδομένα παραχωρούνται ανενδοίαστα, όταν το δίκτυο προστατεύεται βιομετρικά και όχι με κωδικούς. Έτσι, χάρη στη βιομετρική τεχνολογία, η επικοινωνία ανάμεσα στο χρήστη και την επιχείρηση διεξάγεται απρόσκοπτα και χωρίς την ανθρώπινη παρέμβαση, ακόμα και σε περιπτώσεις που αφορούν προστατευόμενα δεδομένα. Η έλλειψη ενδιάμεσου δε συνιστά αμέλεια των διαχειριστών, ούτε δηλώνει υπεραισιοδοξία για τις υπηρεσίες του συστήματος, αντικατοπτρίζει όμως τις δυνατότητες και το βαθμό εμπιστοσύνης που γεννά στους ενδιαφερόμενους.

**Αυξημένος βαθμός υπευθυνότητας**

Με δεδομένη την αφύπνιση των περισσότερων επιχειρήσεων γύρω από ζητήματα ασφαλείας, υπάρχει σήμερα μεγαλύτερη ανάγκη για αξιόπιστες και ακριβείς μεθόδους ελέγχου και αναφοράς. Αυτή την ανάγκη έρχεται να καλύψει η βιομετρική τεχνολογία, που κλείνει "τρύπες" στο σύστημα, όπως για παράδειγμα το *buddy-punching*, (δηλαδή το χτύπημα της κάρτας ενός εργαζόμενου που απουσιάζει από ένα φίλο συνάδελφο). Τέτοια φαινόμενα αποκλείονται με τη βιομετρική, γεγονός που καλλιεργεί υψηλό αίσθημα σιγουριάς ως προς το πρόσωπο που έχει πρόσβαση στο σύστημα και την ώρα. Έτσι, ακόμα κι όταν οι βιομετρικοί μηχανισμοί ελέγχου σπάνια χρησιμοποιούνται στην πράξη, η ύπαρξή τους και μόνο δρα αποτρεπτικά και καλλιεργεί την υπευθυνότητα σε όλους τους εμπλεκόμενους φορείς.

Τα οφέλη από την ασφάλεια, τη διευκόλυνση και την υπευθυνότητα είναι ορατά σε επιχειρήσεις, συνεταιρισμούς και μεμονωμένους χρήστες και αναφέρονται κυρίως στο θέμα της βιομετρικής επικύρωσης ταυτότητας (biometric verification). Τα οφέλη από τη βιομετρική αναγνώριση (biometric identification) διαφέρουν σημαντικά, ειδικά όταν αυτή εφαρμόζεται σε μεγάλη κλίμακα. [1]

[1] http://www.emory.edu/BUSINESS/et/biometric/Biometrics.htm

### 1.6.2 Πλεονεκτήματα σε συστήματα αναγνώρισης

Σε συστήματα αναγνώρισης, η βιομετρική μπορεί επίσης να χρησιμοποιηθεί για λόγους ασφάλειας, διευκόλυνσης και υπευθυνότητας, ειδικά όταν εφαρμόζεται σε έναν μικρό αριθμό χρηστών. Συνήθως όμως, τα συστήματα αναγνώρισης χρησιμοποιούνται σε μεγάλα περιβάλλοντα, που περιλαμβάνουν από μερικές δεκάδες χιλιάδες ως και μερικές δεκάδες εκατομμύρια χρήστες. Σ' αυτές τις περιπτώσεις η βιομετρική δεν αντικαθιστά προσωπικούς αριθμούς αναγνώρισης (PINs) και κωδικούς, αλλά παρέχει νέους τρόπους για περιορισμό της απάτης. Αυτοί αναπτύσσονται εκτενέστερα στις επόμενες παραγράφους.

**Εξακρίβωση απάτης**

Τα συστήματα αναγνώρισης χρησιμοποιούνται για να καθορίσουν αν οι βιομετρικές πληροφορίες ενός συγκεκριμένου ατόμου απαντώνται περισσότερες από μία φορά σε μια βάση δεδομένων. Έτσι, χάρη σε αυτόν τον άμεσο τρόπο εντοπισμού και αναγνώρισης ατόμων που έχουν ήδη γραφτεί σε ένα πρόγραμμα ή έχουν κάνει χρήση μιας παροχής, περιορίζεται σημαντικά η δυνατότητα εξαπάτησης. Πιο συγκεκριμένα, με τον κατάλληλο βιομετρικό έλεγχο μπορεί για παράδειγμα να ελεγχθεί η περίπτωση κατά την οποία κάποιος να επιχειρεί να ξαναγραφτεί σε ένα πρόγραμμα κοινωνικών παροχών κάτω από ένα διαφορετικό όνομα (προσκομίζοντας ενδεχομένως ψευδή πιστοποιητικά, ψεύτικη ταυτότητα κτλ.).[1]

**Αποτροπή από την απάτη**

Η εξακρίβωση της απάτης σίγουρα είναι ένα κέρδος. Ίσως όμως πιο σημαντικό όφελος είναι η αποτροπή των χρηστών του συστήματος από την απάτη, ως απόρροια της χρήσης βιομετρικών ελέγχων[2]. Παρ' ότι σε κάθε έλεγχο για βιομετρική αναγνώριση, ειδικά όταν η βάση δεδομένων περιέχει εκατομμύρια εγγραφές, υπάρχει ένα ποσοστό λάθους που δεν είναι αμελητέο, αυτό που παρατηρείται είναι ότι οι περισσότεροι δεν επιχειρούν καν να εξαπατήσουν το σύστημα και να διεισδύσουν παράνομα σε αυτό. Και μόνο η ύπαρξη βιομετρικού ελέγχου δηλαδή, φαίνεται να δρα αποθαρρυντικά για πολλούς, οι οποίοι υπό

[1] http://www.privacy.org/pi/

[2]http://www.channelinsider.com/c/a/Security/Are-Enterprises-Ready-for-Biometrics-as-a-Security-Solution

άλλες συνθήκες δε θα είχαν ενδοιασμούς να επιχειρήσουν, για παράδειγμα, διπλή εγγραφή στο σύστημα. Η αποτροπή αυτή αποτελεί σημαντικό κέρδος για την επιχείρηση, η οποία έτσι και χρήματα εξοικονομεί και την ακεραιότητα και γνησιότητα των εγγραφών διασφαλίζει.

Χωρίς διάθεση να υποβαθμιστεί η αξία της βιομετρικής τεχνολογίας, πρέπει να τονιστεί ότι η χρήση της δεν συνίσταται σε όλες τις εφαρμογές και για όλους τους χρήστες. Η πρόκληση είναι να προσδιοριστούν εκείνα τα περιβάλλοντα, στα οποία η εφαρμογή της θα επιφέρει τα μέγιστα οφέλη για τους χρήστες και τους οργανισμούς. Και βέβαια τα οφέλη πρέπει να είναι τέτοια, ώστε να υποσκελίζουν ενδεχόμενους κινδύνους και οικονομικές επιβαρύνσεις. Η εμπειρία πάντως αποδεικνύει ότι η αυξημένη αποτελεσματικότητα και επάρκεια των βιομετρικών συστημάτων συνεχώς διευρύνει το πεδίο εφαρμογής τους.

# 2. ΚΥΡΙΑΡΧΕΣ ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΤΗΣ ΦΥΣΙΟΛΟΓΙΑΣ

Ένα από τα συνηθέστερα ερωτήματα που τίθενται στο χώρο της βιομετρικής αφορά στο ποια είναι η καλύτερη βιομετρική τεχνολογία. Αυτό το ερώτημα είναι πολύ σχετικό και δεν μπορεί να απαντηθεί, αν δε διευκρινιστεί προηγουμένως τι εννοούμε με τον όρο καλύτερο. Υπάρχουν τεχνολογίες με καλύτερα ποσοστά αναγνώρισης των πραγματικών χρηστών, τεχνολογίες που είναι λιγότερο ακριβές ή περισσότερο εύκολες στη χρήση, που εντοπίζουν καλύτερα προσπάθειες για εξαπάτηση ή που απευθύνονται σε ένα ευρύτερο δημογραφικό πληθυσμό κτλ. Η κάθε βιομετρική τεχνολογία δηλαδή, έχει τα πλεονεκτήματα και τις αδυναμίες της και απευθύνεται καλύτερα σε συγκεκριμένες εφαρμογές. Συνεπώς, το ερώτημα για το ποια είναι η καλύτερη βιομετρική τεχνολογία βρίσκεται σε άμεση συνάρτηση με την εκάστοτε εφαρμογή, το δημογραφικό πληθυσμό και τα χρησιμοποιούμενα μέσα υποστήριξης και δεν μπορεί να απαντηθεί σε μια αυθαίρετη βάση. Επομένως, καμία βιομετρική τεχνολογία δεν μπορεί να θεωρηθεί η καλύτερη ή ότι θα κυριαρχήσει σε όλους τους τομείς. Αντίθετα, οι απαιτήσεις της εκάστοτε εφαρμογής καθορίζουν ποια είναι η αρτιότερη βιομετρική λύση, κι επομένως η σύγκριση των τεχνολογιών έχει νόημα μόνο στα πλαίσια συγκεκριμένων εφαρμογών. Αυτό γίνεται περισσότερο σαφές σ' αυτό και στο επόμενο κεφάλαιο, όπου αναπτύσσονται ξεχωριστά οι κυρίαρχες βιομετρικές τεχνολογίες της φυσιολογίας και της συμπεριφοράς, και γίνεται συγκεκριμένη αναφορά στα συστατικά μέρη, τον τρόπο λειτουργίας, τις εφαρμογές, τα πλεονεκτήματα και τα μειονεκτήματά τους.

## 2.1 ΤΟ ΣΚΑΝΑΡΙΣΜΑ ΤΩΝ ΔΑΧΤΥΛΩΝ

Η τεχνολογία σκαναρίσματος δαχτύλων κάνει χρήση των διακριτών χαρακτηριστικών του δακτυλικού αποτυπώματος, με σκοπό την πιστοποίηση ή αναγνώριση των ατόμων. Είναι η πιο συχνά χρησιμοποιούμενη βιομετρική τεχνολογία, που χρησιμοποιείται σε ένα ευρύ πεδίο εφαρμογών λογικής και φυσικής πρόσβασης. Στην αγορά συναντάται σε συσκευές hardware, πακέτα λογισμικού και ολοκληρωμένες λύσεις για επιχειρήσεις. Στο Σχήμα 4 φαίνονται μερικά γνωστά εμπορικά προϊόντα.


**Σχήμα 2.** Συσκευές σκαναρίσματος δαχτύλων διαφόρων χρήσεων

### 2.1.1 Συστατικά μέρη

Τα συστήματα σκαναρίσματος δαχτύλων περιλαμβάνουν υλισμικό (hardware) για απόκτηση εικόνων, τμήματα όπου γίνεται η επεξεργασία των εικόνων. Όλα τα παραπάνω συστατικά μέρη μπορεί να βρίσκονται συγκεντρωμένα σε μια περιφερειακή ή ανεξάρτητη μηχανή ή να είναι διασκορπισμένα σε μια περιφερειακή συσκευή, ένα τοπικό υπολογιστή (PC) και έναν κεντρικό υπολογιστή (server).

Η επιφάνεια στην οποία τοποθετείται το δάχτυλο λέγεται *platen* ή και *scanner*. Ένα *platen* μπορεί να είναι φτιαγμένο από διάφορα υλικά, από γυαλί, πλαστικό, σιλικόνη, πολυμερή κ.α.. Διάφορα καλύμματα το προστατεύουν από φθορές και χτυπήματα, γιατί διαφορετικά μειώνεται σημαντικά η ποιότητα των εικόνων που παρέχει. Ανάλογα με την χρησιμοποιούμενη τεχνολογία, οι περιοχές όπου υπάρχει επαφή δαχτύλου και *platen* μετρούνται με διάφορους τρόπους, είτε με μικροκάμερες ενσωματωμένες σε τσιπ, είτε με υπερηχητική εικονογράφηση ή με βάση τις αλλαγές στα πεδία που παράγει το δάχτυλο. Οι μετρήσεις αυτές μετατρέπονται στη συνέχεια σε ψηφιακό κώδικα, τον οποίο μπορεί να επεξεργαστεί το σύστημα.[1]

Το *platen* είναι μέρος του *module*. Ένα module αποτελεί το βασικό πυρήνα μιας περιφερειακής ή ανεξάρτητης συσκευής σκαναρίσματος δαχτύλων. Συχνά υπάρχει ενσωματωμένο σε πληκτρολόγια, φορητές συσκευές, και συσκευές ελέγχου πόρτας, ενώ μελλοντικά θα αποτελέσει εξάρτημα των κινητών τηλεφώνων, των *smart cards* και των οχημάτων εξόρμησης. Το module έχει σχετικά μικρό μέγεθος και αποτελείται συνήθως από ένα platen προσαρτημένο σε ένα μικρό πίνακα κυκλωμάτων, και από ένα εξάρτημα σύνδεσης, που επιτρέπει την ψηφιακή αποστολή πληροφοριών στην περιφερειακή ή ανεξάρτητη συσκευή[2].

[1] Ruud M. Bolle, Andrew W. Senior, Nalini K. Ratha, and Sharath Pankanti, "Fingerprint Minutiae: A Constructive Definition".

[2] A. K. Jain, S. Prabhakar, and S. Pankanti, "On The Similarity of Identical Twin Fingerprints", Pattern Recognition, Vol. 35, No. 11, pp. 2653-2663, 2002.

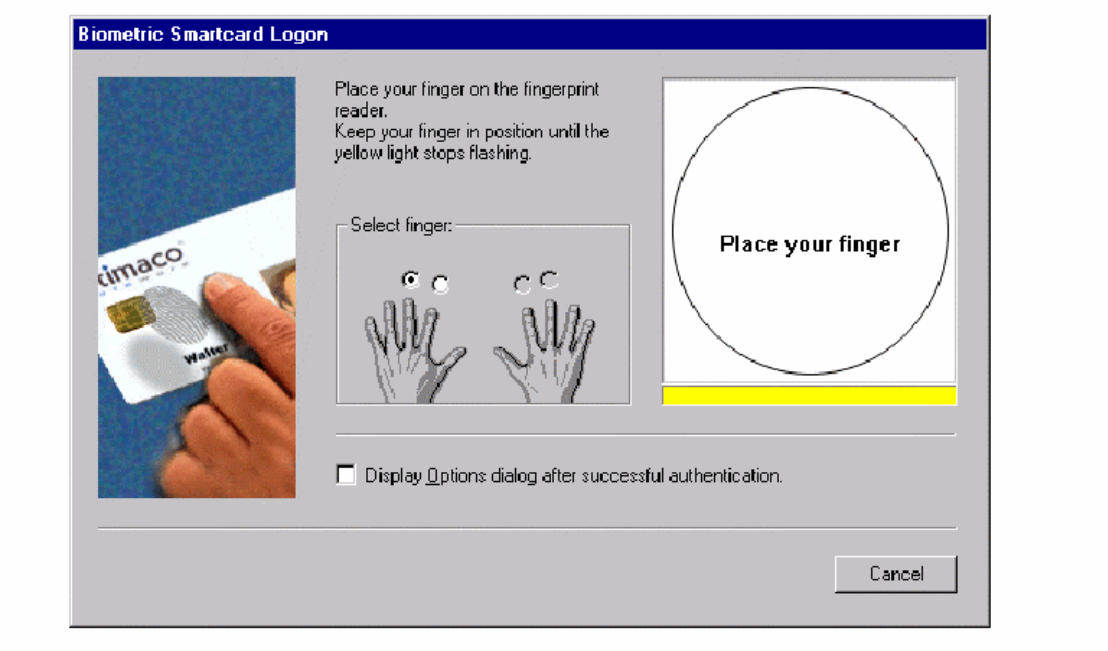
Platten

Module

Peripheral

**Σχήμα 3.** Τα συστατικά μέρη ενός συστήματος σκαναρίσματος δαχτύλων

Τα περισσότερα σύγχρονα modules είναι σε θέση να εκτελούν όλες τις λειτουργίες του συστήματος – απόκτηση εικόνας, επεξεργασία εικόνας, δημιουργία, ταίριασμα, αποθήκευση προσωρινών αρχείων (template) – και να στέλνουν μια θετική ή αρνητική απάντηση για ταίριασμα σε μια εξωτερική εφαρμογή ή το ίδιο το σύστημα. Έτσι, σε αντίθεση με παλαιότερα, που η παραγωγή και το ταίριασμα των προσωρινών αρχείων (templates) γινόταν αποκλειστικά σε ένα τοπικό Η/Υ (PC) ή έναν server, σήμερα αρκετά περιφερειακά μπορούν και πραγματοποιούν όλες τις λειτουργίες εσωτερικά. Αυτό έχει ακόμα μεγαλύτερη αξία στις συσκευές φυσικής πρόσβασης.




**Σχήμα 4.** Ένα βιομετρικό κουτί διαλόγου για σκανάρισμα δαχτύλων

### 2.1.2 Τρόπος λειτουργίας

Η διαδικασία της βιομετρικής πιστοποίησης με σκανάρισμα δαχτύλων περιλαμβάνει πέντε κυρίως στάδια: την απόκτηση της εικόνας, την επεξεργασία της εικόνας, των εντοπισμό των διακριτών χαρακτηριστικών, τη δημιουργία και το ταίριασμα του αρχείου (template). Η βασική διαδικασία είναι σχεδόν η ίδια σε όλα τα εμπορικά προϊόντα με μερικές διαφοροποιήσεις στα επιμέρους σημεία και ιδίως στον τρόπο εξαγωγής των χαρακτηριστικών[1].

**Απόκτηση εικόνας**

Το πρώτο ζήτημα που πρέπει να αντιμετωπιστεί σε ένα σύστημα σκαναρίσματος δαχτύλων είναι η απόκτηση μιας εικόνας του δακτυλικού αποτυπώματος, που να είναι υψηλής ποιότητας. Η ποιότητα της εικόνας μετριέται σε κουκίδες ανά ίντσα (dots per inch (DPI)) και όσο μεγαλύτερο είναι το DPI τόσο μεγαλύτερη είναι η πιστότητα της εικόνας.

[1] "Fingerprint Recognition Devices Coming in 1998", PC World, 19 November 1997.

**Σχήμα 5.** Τυπικές εικόνες σκαναρίσματος δαχτύλων

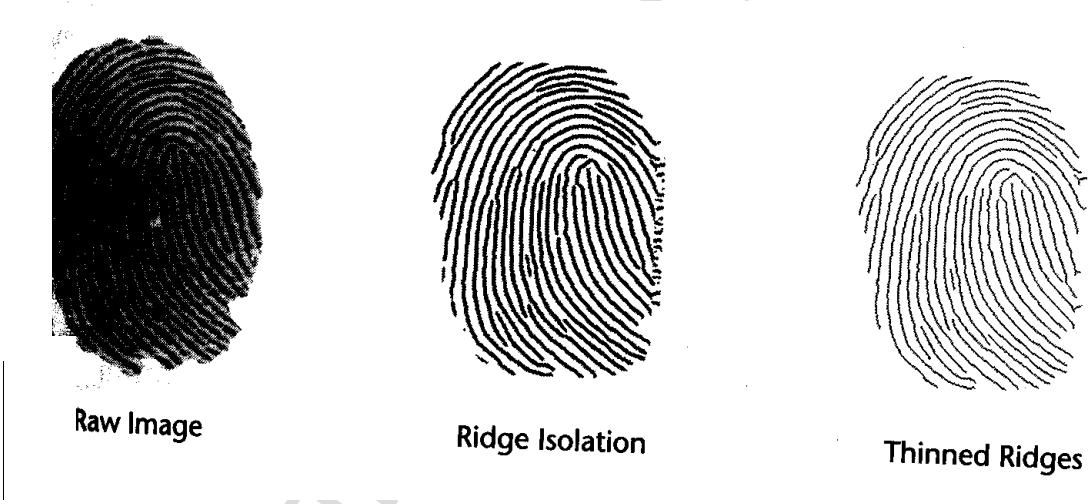
Η απόκτηση μιας σωστής εικόνας αποτελεί μεγάλη πρόκληση στην ανάπτυξη τεχνολογίας σκαναρίσματος δαχτύλων, λόγω των υφιστάμενων δυσκολιών. Υπάρχουν πληθυσμιακές ομάδες που είναι πιο πιθανό να έχουν αχνά αποτυπώματα, είτε λόγω φθοράς είτε λόγω της φυσιολογίας τους. Επιπλέον, περιβαλλοντικοί παράγοντες επηρεάζουν την τελική εικόνα. Αν κάνει πολύ κρύο για παράδειγμα, τα λάδια που υπάρχουν σε ένα δακτυλικό αποτύπωμα και που βοηθούν στην απεικόνισή του μπορεί να έχουν στεγνώσει κι έτσι το αποτύπωμα να μην είναι αρκετά έντονο. Οι χρήστες σ' αυτή την περίπτωση μπορεί να χρειαστεί να πιέσουν στη συσκευή με μεγαλύτερη δύναμη ή να τρίψουν το δάχτυλό τους με την αντίθετη παλάμη για καλύτερο αποτέλεσμα.

Τα προβλήματα δεν σταματούν εδώ. Για να είναι έγκυρη μια διαδικασία εγγραφής ή πιστοποίησης, πρέπει στο platen να είναι τοποθετημένο το κέντρο του δακτυλικού αποτυπώματος. Πολλοί χρήστες όμως, οι οποίοι δεν είναι εξοικειωμένοι με τον τρόπο παροχής δακτυλικών αποτυπωμάτων, τοποθετούν το δάχτυλό τους με τρόπο, ώστε εμφανίζεται μόνο το επάνω μέρος. Αυτό προκαλεί μειωμένο εντοπισμό διακριτών χαρακτηριστικών και άρα μειωμένη πιθανότητα επιτυχημένης λειτουργίας εγγραφής ή πιστοποίησης. Ένα ακόμα ζήτημα σχετικό με την απόκτηση μιας κατάλληλης εικόνας έχει να κάνει με το μέγεθος του platen. Τα τελευταία χρόνια παρατηρείται μια μείωση του μεγέθους του για εμπορικούς λόγους. Όσο όμως η συσκευή γίνεται πιο μικρή,

λιγοστεύουν τα δεδομένα που μπορεί να προσλάβει, ενώ ταλαιπωρούνται οι χρήστες με μεγάλα δάχτυλα.

**Επεξεργασία εικόνας**

Αφού επιτευχθεί ο στόχος της απόκτησης μιας εικόνας υψηλής ποιότητας, πρέπει η εικόνα αυτή να μετασχηματιστεί σε μια εύχρηστη μορφή. Το πρώτο στάδιο είναι η μετατροπή των γκρίζων κουκίδων (pixels) σε άσπρα ή μαύρα, ανάλογα με την περιεκτικότητά τους σε κάθε χρώμα. Το αποτέλεσμα είναι μια σειρά από μαύρες ακρολοφίες, που έρχονται σε αντίθεση με τις άσπρες αυλάκια. Στη συνέχεια, το πάχος των ραβδώσεων προσαρμόζεται από 5 με 8 pixels που είναι κανονικά σε ένα, όπως φαίνεται στο Σχήμα 8, με στόχο τον ακριβή εντοπισμό των χαρακτηριστικών.




**Σχήμα 6.** Τα βήματα που ακολουθούνται στην επεξεργασία εικόνας

**Διακριτά χαρακτηριστικά**

Σε ένα μέσο δακτυλικό αποτύπωμα υπάρχει μια πολύ μεγάλη ποσότητα από διακριτές πληροφορίες, που παραμένουν αρκετά σταθερές κατά τη διάρκεια της ζωής ενός ατόμου και διαφέρουν ακόμα και στην περίπτωση διδύμων. Ο μεγάλος όγκος αυτών των πληροφοριών οφείλεται στην ιδιαίτερη φυσιολογία του δαχτύλου. Ένα δακτυλικό αποτύπωμα χωρίζεται στις ακρολοφίες και τα αυλάκια, που μαζί σχηματίζουν διαφορετικά σχήματα, όπως κόλπους, στροβίλους και τόξα. Τα σχήματα αυτά

περιστρέφονται γύρω από έναν πυρήνα, ενώ υπάρχουν σημεία – συνήθως στην κάτω δεξιά ή αριστερή γωνία του αποτυπώματος – όπου οι ακρολοφίες έχουν τριγωνική μορφή και σχηματίζουν τα λεγόμενα δέλτα[1].

Οι ακρολοφίες και τα αυλάκια χαρακτηρίζονται από ασυνέχειες και ανωμαλίες στην κανονική τους μορφή, γνωστές με τον όρο *minutiae*. Υπάρχουν πολλοί τύποι *minutiae*, με τους πιο συνηθισμένους να είναι τα τελειώματα και τα σημεία διακλαδώσεως των ακρολοφιών. Τα *minutiae* είναι οι σχηματισμοί, στους οποίους βασίζονται οι περισσότερες τεχνολογίες σκαναρίσματος δαχτύλων για τη σύγκριση των αποτυπωμάτων. Ανάλογα με το μέγεθος του *platen* και την ακρίβεια του αλγορίθμου, μια τυπική εικόνα ενός σκαναρισμένου αποτυπώματος μπορεί να παράγει από 15 έως 50 *minutiae*. Είναι προφανές ότι όσο μεγαλώνει το μέγεθος του *platen* υπάρχει δυνατότητα πρόσληψης μεγαλύτερου μέρους του δακτυλικού αποτυπώματος κι έτσι εντοπίζεται μεγαλύτερος αριθμός από *minutiae*.


**Σχήμα 7.** Τα minutiae στο σκανάρισμα δαχτύλων

Αν και οι περισσότερες τεχνολογίες σκαναρίσματος δαχτύλων – σχεδόν το 80% – βασίζονται στη σύγκριση των *minutiae*, υπάρχει και η εναλλακτική πρόταση, που βασίζει την εξαγωγή χαρακτηριστικών σε μια ακολουθία από ακρολοφίες. Η τεχνολογία αυτή μειώνει τις εξαρτήσεις από τα *minutiae*, που έχουν την τάση να φθείρονται, αλλά καθιστά

[1] Ruud M. Bolle, Andrew W. Senior, Nalini K. Ratha, and Sharath Pankanti, "Fingerprint Minutiae: A Constructive Definition".

πιο κρίσιμη τη σωστή τοποθέτηση του δαχτύλου. Επίσης, τα *templates* που παράγει είναι δύο με τρεις φορές μεγαλύτερα, δηλαδή περίπου 1.000 *bytes*, όταν τα templates που παράγονται με minutiae κυμαίνονται συνήθως μεταξύ 250 και 500 *bytes*.

**Δημιουργία template**

Υπάρχουν εξειδικευμένοι αλγόριθμοι, που καταγράφουν τα minutiae του δακτυλικού αποτυπώματος, βασιζόμενοι σε πληροφορίες, όπως η τοποθεσία και η γωνία του *minutiae*, ο τύπος και η ποιότητά του, η θέση και η απόσταση του σε σχέση με τον πυρήνα κτλ. Κατά την εγγραφή, ο χρήστης συνήθως παρουσιάζει αρκετές φορές κάθε δακτυλικό αποτύπωμα, ούτως ώστε να επιλεχθούν από το σύστημα τα πιο συχνά εμφανιζόμενα *minutiae*. Γενικά, οι εικόνες των αποτυπωμάτων παρουσιάζουν διαστρεβλώσεις και λάθη, τα οποία πρέπει να φιλτραριστούν πριν τη δημιουργία του *template*. Για παράδειγμα, ανωμαλίες λόγω χτυπημάτων ή βρωμιάς μπορεί να εκληφθούν ως *minutiae*. Οι αλγόριθμοι απομονώνουν και αγνοούν τα χαρακτηριστικά εκείνα, που φαίνεται να βρίσκονται σε λάθος μέρος, όπως π.χ. μια ακρολοφία, που διασταυρώνεται κάθετα με μια σειρά από άλλες ακρολοφίες. Έτσι, εξασφαλίζεται σε μεγάλο βαθμό, ότι το παραγόμενο *template* αποτελεί μια αξιόπιστη αναπαράσταση των πραγματικών βιομετρικών δεδομένων.

**Ταίριασμα templates**

Τα *templates* έχουν μέγεθος που κυμαίνεται από 200 έως 1000 *bytes*, είναι δηλαδή πολύ μικρά. Η σύγκριση για το αν δύο templates προέρχονται από το ίδιο άτομο, απαιτεί απαραιτήτως την εφαρμογή του κατάλληλου αλγορίθμου, είναι ανώφελο δηλαδή να επιχειρήσει κανείς να συγκρίνει δύο templates σειριακά ανά *bit.* Ακόμα όμως και με χρήση του αλγορίθμου, το αποτέλεσμα της σύγκρισης δεν είναι ταίριασμα 100%. Αυτό συμβαίνει π.χ. γιατί το σημείο όπου βρίσκεται ένα *minutiae* έχει μετατοπιστεί μερικά *pixels* ή γιατί μερικά *minutiae* διαφέρουν σε σχέση με το *template* της εγγραφής ή ακόμη επειδή ψεύτικα *minutiae* έχουν θεωρηθεί αληθινά. Εξάλλου, η γωνία λήψης του αποτυπώματος είναι έστω και ελάχιστα διαφορετική. Ωστόσο, επειδή αυτά τα προβλήματα είναι γνωστά, οι αλγόριθμοι ταιριάσματος προβλέπουν γι' αυτές τις διαφορές. Έτσι, η σύγκριση που διενεργούν είναι γενικά αποτελεσματική, παρά τις όποιες αλλαγές στα δεδομένα.

Γενικά, για να θεωρηθεί ένα ταίριασμα επιτυχές πρέπει τα δύο templates να έχουν αρκετά κοινά *minutiae*. Το κατώτατο επιτρεπτό ποσοστό των κοινών *minutiae* διαφοροποιείται κάθε φορά, ανάλογα με την επιλεχθείσα τιμή του συστήματος και την πολιτική που εφαρμόζει σε ζητήματα ασφάλειας και διευκόλυνσης των χρηστών.

### 2.1.3 Παραδείγματα Εφαρμογών

Οι διάφορες τεχνολογίες σκαναρίσματος δαχτύλων χρησιμοποιούνται καθημερινά από χιλιάδες ανθρώπους, που διεκδικούν την είσοδό τους σε απαγορευμένες περιοχές, την πρόσβασή τους σε Η/Υ, τη διεκπεραίωση συναλλαγών, στον έλεγχο διαβατηρίων , στον έλεγχο λαθρομετανάστευσης, στις πληρωμές κοινωνικής πρόνοιας, στην πρόσβαση σε χρηματοκιβώτια , καθώς και στην ασφάλεια πιστωτικών καρτών. Σε αντίθεση με άλλες βιομετρικές τεχνολογίες, που απευθύνονται σε συγκεκριμένες εφαρμογές, το σκανάρισμα των δαχτύλων είναι μια τεχνολογία που αφορά σε ένα πολύ μεγάλο εύρος εφαρμογών.

**ΕΞΩΤΕΡΙΚΟ:**

**ΚΑΝΑΔΑΣ:**

**1) Εφαρμογές (H.R.) για έλεγχο εργαζομένων σε Ξενοδοχειακή Μονάδα, ασφάλεια και μετανάστευση.**

Μέχρι πριν λίγα χρόνια η παρακολούθηση των ωρών εργασίας των εργαζομένων γινόταν χειρόγραφα. Ήταν ένα δυσκίνητο σύστημα, βέβαια βελτιώθηκε με την τεχνολογία και την χρήση της πληροφορικής. Ο Διευθυντής μεγάλου ξενοδοχείου του Καναδά αποφάσισε πως ήταν αναγκαία η χρήση βιομετρικών συστημάτων για τον πλήρη έλεγχο της επιχείρησής του. Σαφέστερα τονίζει πως, θέλανε κάτι που θα μπορούσε να παρακολουθεί τις ώρες των ανθρώπων που εργάζονται κυρίως για σκοπούς μισθοδοσίας καθώς επίσης, να παρακολουθείτε και ποιος είναι στο χώρο του ξενοδοχείου σε κάθε δεδομένη στιγμή .
Έτσι, εγκαταστάθηκε το σύστημα της Toshiba ονόματι Experchem που επιτρέπει την είσοδο στους εργαζομένους εφόσον φορούν ένα ηλεκτρονικό ρολόι ακουμπώντας το κοντά σε έναν αναγνώστη και έπειτα την τοποθέτηση ενός δακτύλου σε μια ηλεκτρονική συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων. Το παραπάνω αποτελεί απλώς ένα παράδειγμα από την αυξανόμενη χρήση των βιομετρικών συστημάτων στις εφαρμογές διοίκησης ανθρωπίνων πόρων, για τον πλήρη έλεγχο και είσοδο του προσωπικού- κυρίως

με την βοήθεια δακτυλικών αποτυπωμάτων, αλλά και για ολόκληρο το χέρι, ή την αναγνώριση προσώπου . Ο Διευθυντής του ξενοδοχείου παρατηρεί ιδιαίτερο όφελος λόγω εξάλειψης χρονοβόρων γραφειοκρατικών διαδικασίων, καταγράφοντας αυτόματα πλήρη στοιχεία, μειώνοντας των χρόνο διεργασιών, αντί να εισαχθούν με το χέρι στα φύλλα του χρόνου.

Επίσης, λοιπές τεχνολογίες, όπως οι έξυπνες κάρτες, θα μπορούσαν να επιτύχουν και να ωφελήσουν ιδιαιτέρως. Αλλά οι βιομετρικές μέθοδοι εξαλείφουν τον χρόνο εισαγωγής και επεξεργασίας δεδομένων. Επίσης, όσον αφορά τις βιομετρικές τεχνολογίες που εφαρμόστηκαν στο συγκεκριμένο ξενοδοχείο είναι αδύνατο να παρατηρηθούν παρατυπίες και δόλιες αξιώσεις, δηλαδή κάποιος εργαζόμενος να <<εξυπηρετεί>> κάποιων άλλον περνώντας το βραχιόλι του (όπως γινόταν έως τώρα με τις κάρτες εργασίας>> , αφού αναγκαίο για την είσοδο του εργαζομένου ήταν το αποτύπωμά του. Το Experchem είναι ένα σύστημα βιομετρικής τεχνολογίας που εξασφαλίζει την <<μελλοντική θωράκιση>> της επιχείρησης με απλό τρόπο. "Είναι εύκολο να ξεχάσουμε μια κάρτα. Είναι δύσκολο να ξεχάσουμε το δάχτυλό σας. "[1]

Επίσης, ο Καναδάς έχει αρχίσει την έρευνα στη χρήση της βιομετρικής τεχνολογίας στον τομέα της ασφάλειας και της μετανάστευσης συνόρων μέσω του τεχνικού προγράμματος δημόσιας ασφαλείας και της Κοινότητας βιομετρικής της πρακτικής.

**ΠΟΥΕΡΤΟ ΡΙΚΟ:**

**2) Εφαρμογές (H.R.) για έλεγχο εργαζομένων & πελατών σε Τραπεζικούς φορείς**

Επίσης, η τράπεζα Westernbank στο Πουέρτο Ρίκο χρησιμοποιεί τεχνολογία σκαναρίσματος δαχτύλων και στα 37 τμήματά της. Η τεχνολογία είναι προαιρετική για τους πελάτες και υποχρεωτική για τους υπαλλήλους και, σύμφωνα με στοιχεία της τράπεζας, επιλέγεται από ένα ποσοστό πελατών της τάξεως του 15%. Το συνολικό κόστος για την υποστήριξη του συστήματος ανέρχεται σε $3.000.000[2].

[1] http://www.businessweek.com/technology/content/jun2003/tc2030620_3373_19.htm

[2] http://www.bankersonline.com/articles/bhv012/bhv09n12a2.html

**ΜΕΞΙΚΟ:**

**3) Εφαρμογές (H.R.) πληρωμής εργαζομένων οικονομικού οργανισμού**

Στο Μεξικό, το Groupo Financiero Banorte, που είναι ένας πρωτοποριακός οικονομικός οργανισμός, χρησιμοποιεί ένα συνδυασμό βιομετρικής τεχνολογίας και smart cards για την πληρωμή των εργαζομένων εκείνων, που δε διαθέτουν τραπεζικό λογαριασμό. Η διαδικασία έχει ως εξής: ο εργαζόμενος αρχικά υποβάλλεται σε έλεγχο αποτυπωμάτων και στη συνέχεια χρησιμοποιεί τη smart card, που αντικαθιστά τις επιταγές πληρωμής, για να εξαργυρώσει τα χρήματα. Στις καθημερινές συναλλαγές των υπαλλήλων, η smart card λειτουργεί σαν χρεωστική κάρτα. Η τεχνολογία αυτή, που αρχικά εφαρμόστηκε πιλοτικά σε 4.000 εργαζόμενους, πρόκειται να εξυπηρετήσει σύντομα πάνω από 650.000 άτομα.

**Η.Π.Α.**

**4) Εφαρμογές στην Υγεία για τήρηση ιατρικού αρχείου και απορρήτου και σε Στρατιωτικές Υπηρεσίες**

Στις ΗΠΑ τώρα, το New York State Office of Mental Health από το 1998 έχει στην κατοχή του και χρησιμοποιεί πάνω από 6.000 μονάδες σκαναρίσματος δαχτύλων. Οι μονάδες αυτές χρησιμοποιούνται από το νοσηλευτικό προσωπικό, για λόγους καλύτερης τήρησης του ιατρικού αρχείου και απορρήτου των ασθενών.

Επιπρόσθετα το 2005, σχεδιάστηκαν τα αμερικανικά διαβατήρια βασισμένα σε βιομετρικά στοιχεία. Ορισμένα κυβερνητικά στελέχη, σε πολλές χώρες, έχουν επικρίνει τη χρήση της βιομετρικής τεχνολογίας για την πιθανή ζημιά στις αστικές ελευθερίες, τη ελεύθερη ανάπτυξη της προσωπικότητας, και τον κίνδυνο κλοπής ταυτότητας. Αυτήν την περίοδο, υπάρχει ιδιαίτερη ανησυχία στις Ηνωμένες Πολιτείες (και την Ευρωπαϊκή Ένωση) ότι οι ιδιαίτερες πληροφορίες που περιέχουν τα νέου τύπου διαβατήρια μπορούν «να ξαφριστούν» και να προσδιορίσουν πλήθος προσωπικών χαρακτηριστικών των .

Η κοινή κάρτα πρόσβασης του αμερικανικού υπουργείου Αμύνης, είναι μια κάρτα ταυτότητας που διανέμεται να δοθεί σε όλο το προσωπικό αμερικανικών στρατιωτικών υπηρεσιών. Αυτή η κάρτα περιέχει τα βιομετρικά στοιχεία και τις φωτογραφίες. Επίσης, με λέιζερ χαράζονται ανάγλυφα οι φωτογραφίες και τα ολογράμματα για περαιτέρω

ασφάλεια και μείωση κίνδυνου παραποίησης. Έχουν εκδοθεί ως τώρα πάνω από 10 εκατομμύρια από αυτές τις κάρτες[1].

**ΠΕΝΣΥΛΒΑΝΙΑ**

**5) Εφαρμογές για πίστωση σε Εκπαιδευτικά Ιδρύματα**

Ακόμα, στο Welsh Valley Middle School της Πενσυλβάνια οι μαθητές αντί να πληρώνουν τα γεύματα στην καφετέρια με μετρητά, μπορούν να χρησιμοποιούν χρεωστικά περιφερειακά μηχανήματα με σκανάρισμα δαχτύλων. Στο τέλος κάθε μήνα, ο λογαριασμός αποστέλλεται, είτε στους γονείς των μαθητών είτε σε ένα πρόγραμμα δωρεάν σίτισης. Στην προκειμένη περίπτωση, η εφαρμογή της τεχνολογίας εξυπηρετεί συγκεκριμένη νομοθεσία, που απαγορεύει τη διάκριση και αποκάλυψη των μαθητών που σιτίζονται με κυβερνητικά κονδύλια[2].

**ΓΚΑΜΠΙΑ**

**6) Εφαρμογή για έκδοση δελτίων ταυτοτήτων, αδειών κατοικίας και οδήγησης**

Το βιομετρικό σύστημα προσδιορισμού που χρησιμοποιεί η κυβέρνηση της Γκάμπια επέτρεψε την έκδοση των πρώτων βιομετρικών εγγράφων ταυτότητας τον Ιούλιο του 2009. Τα στοιχεία ενός ατόμου, συμπεριλαμβανομένων των βιομετρικών πληροφοριών τους (thumbprints) συλλαμβάνονται σε μια βάση δεδομένων. Ένας εθνικός αριθμός αναγνώρισης (NIN) αντιστοιχεί σε κάθε πολίτη και είναι μοναδικός. Μεταξύ των βιομετρικών έγγραφων που εκδίδονται στη Γκάμπια περιλαμβάνουν οι κάρτες εθνικών ταυτοτήτων, οι άδειες κατοικίας και οι άδειες οδήγησης.

**ΓΕΡΜΑΝΙΑ**

**7) Εφαρμογές για έκδοση διαβατηρίων και ασφάλεια Ολυμπιακών Αγώνων**

Η αγορά βιομετρικής στη Γερμανία έχει αυξηθεί ιδιαίτερα το έτος 2009. Το μέγεθος αγοράς αυξήθηκε από € 120 εκατομμύρια (2004) σε € 377 εκατομμύρια το (2009). Οι βιομετρικές διαδικασίες του δακτυλικού αποτυπώματος και της αναγνώρισης του

[1] http://www.privacy.org/pi/

[2] http://www.inbiometrics.com/biometriclibrary.htm

προσώπου μπορούν να ωφεληθούν από το κυβερνητικό πρόγραμμα. Το Μάιο του 2005 η γερμανική Άνω Βουλή του Κοινοβουλίου ενέκρινε την εφαρμογή των ePass, ένα διαβατήριο που διανεμήθηκε σε όλους τους γερμανικούς πολίτες που περιέχει βιομετρική τεχνολογία. Τα ePass ήταν στην κυκλοφορία από το Νοέμβριο του 2005, και περιέχει ένα τσιπ που κρατά μια ψηφιακή φωτογραφία και ένα δακτυλικό αποτύπωμα από κάθε χέρι, συνήθως των αντίχειρων. «Ένα τρίτο βιομετρικό προσδιοριστικό μέσω ανιχνεύσεις ίριδων - θα μπορούσε να προστεθεί σε ένα προχωρημένο στάδιο». Η αύξηση στην επικράτηση της βιομετρικής τεχνολογίας στη Γερμανία είναι μια προσπάθεια για να συμμορφωθεί με την τρέχουσα αμερικανική προθεσμία προκειμένου να εισαγάγει τα βιομετρικά διαβατήρια.

Η Γερμανία είναι επίσης μια από τις πρώτες χώρες που εφάρμοσε τη βιομετρική τεχνολογία στους Ολυμπιακούς Αγώνες ώστε να προστατεύσει τους γερμανούς αθλητές. «Οι Ολυμπιακοί Αγώνες είναι πάντα μια διπλωματικά ανήσυχη υπόθεση και τα προηγούμενα γεγονότα έχουν χτυπηθεί από τις τρομοκρατικές επιθέσεις - ειδικότερα στο Μόναχο το 1972 όπου 11 ισραηλινοί αθλητές σκοτώθηκαν».

**ΒΡΑΖΙΛΙΑ**

**8) Εφαρμογές για έκδοση διαβατηρίων**

Ως τα τέλη του 2005, η κυβέρνηση της Βραζιλίας άρχισε την ανάπτυξη του νέου διαβατηρίου της. Το νέο διαβατήριο περιέλαβε διάφορες ιδιότητες ασφαλείας, όπως τη διάτρηση λέιζερ, τα UV κρυμμένα σύμβολα, το στρώμα ασφάλειας πέρα από τα μεταβλητά στοιχεία, την υπογραφή τους, φωτογραφία, και 10 κυλημένα δακτυλικά αποτυπώματα που δίδονταν κατά τη διάρκεια των αιτημάτων διαβατηρίων. Όλο το στοιχείο προγραμματίζεται να αποθηκευτεί στα πρότυπα ηλεκτρονικών διαβατηρίων ICAO. Αυτό επιτρέπει την ηλεκτρονική ανάγνωση και επαλήθευση της ταυτότητας των κατόχων διαβατηρίων δεδομένου ότι τα πρότυπα δακτυλικών αποτυπωμάτων και οι συμβολικές του προσώπου εικόνες θα είναι διαθέσιμα για την αυτόματη αναγνώριση.

**ΙΡΑΚ**

**9) Εφαρμογή για έκδοση ταυτοτήτων και ασφάλεια πολιτών**

Η βιομετρική χρησιμοποιείται εκτενώς στο Ιράκ περιλαμβάνοντας όσο το δυνατόν περισσότερους Ιρακινούς πολίτες. Κατά τη διάρκεια απολογισμού, οι συλλεχθείσες πληροφορίες βιομετρικής καταγράφονται σε μια κεντρική βάση. Ακόμα κι αν ένας Ιρακινός έχει χάσει την κάρτα ταυτότητάς τους, ο προσδιορισμός τους μπορεί να βρεθεί και να ελεγχθεί με τη χρησιμοποίηση των μοναδικών βιομετρικών πληροφοριών . Οι πρόσθετες πληροφορίες μπορούν επίσης να προστεθούν σε κάθε αρχείο απολογισμού.

**ΙΝΔΙΑ**

**10) Εφαρμογές σε έκδοση ταυτοτήτων και ασφάλεια πολιτών**

Η Ινδία αναλαμβάνει μια φιλόδοξη μεγάλη επιχείρηση το 2010 για να παρέχει έναν μοναδικό αριθμό αναγνώρισης σε κάθε ένας από 1.25 δισεκατομμύριο ανθρώπους της. Ο αριθμός αναγνώρισης θα αποθηκευτεί τις κεντρικές βάσεις δεδομένων. αποτελούμενος από βιομετρικές πληροφορίες του ατόμου. Εάν εφαρμόζεται, αυτό θα ήταν η μεγαλύτερη εφαρμογή της βιομετρικής στον κόσμο. Η κυβέρνηση θα χρησιμοποιήσει έπειτα τις πληροφορίες στα δελτία ταυτότητας. Οι ανώτεροι υπάλληλοι στην Ινδία θα περάσουν ένα έτος ταξινομώντας τον πληθυσμό της Ινδίας σύμφωνα με τους δείκτες δημογραφίας.

**ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ**

**11) Εφαρμογή σε σχολεία , ασφάλεια και Εθνικό Σύστημα Υγείας**

Ανιχνευτές δακτυλικών αποτυπωμάτων χρησιμοποιούνται σε μερικά σχολεία για να διευκολύνει την πληρωμή διδάκτρων και σχολικών γευμάτων. Η χρησιμοποίηση τέτοιων βιομετρικών χαρακτηριστικών υπολογίζεται να χρησιμοποιηθεί και σε συστήματα ασφαλείας καθώς και στο Εθνικό Σύστημα Υγείας του Ηνωμένου Βασιλείου για την τήρηση ιατρικού αρχείου και φακέλων ασθενών που περιέχουν άκρως προσωπικά δεδομένα[1].

[1] http://www.biocentricsolutions.com/

**ΙΣΡΑΗΛ**

**12) Εφαρμογή για δημιουργία βάσης δεδομένων**

Η ισραηλινή κυβέρνηση έχει ψηφίσει ένα νομοσχέδιο απαιτώντας τη δημιουργία μιας βιομετρικής βάσης δεδομένων όλων των ισραηλινών κατοίκων. Η βάση δεδομένων θα περιέχει όλα τα δακτυλικά αποτυπώματα και τα περιγράμματα του προσώπου. Οι αντίπαλοι του προτεινόμενου νόμου, συμπεριλαμβανομένων των προεξεχόντων ισραηλινών επιστημόνων και των εμπειρογνωμόνων ασφάλειας, προειδοποίησαν ότι η ύπαρξη μιας τέτοιας βάσης δεδομένων θα μπορούσε να βλάψει την προσωπική ελευθερία και τη Κρατική Ασφάλεια, επειδή οποιεσδήποτε διαρροές θα μπορούσαν να χρησιμοποιηθούν από τους εγκληματίες ή εχθρικά άτομα ενάντια στους ισραηλινούς κατοίκους.

**ΟΛΛΑΝΔΙΑ**

**13) Εφαρμογή για έκδοση ταυτοτήτων**

Αρχικά στις 21 Σεπτεμβρίου 2009, όλα τα νέα ολλανδικά διαβατήρια και οι κάρτες ταυτότητας πρέπει να περιλάβουν τα δακτυλικά αποτυπώματα του κατόχου. Από τις 26 Αυγούστου 2006, τα ολλανδικά διαβατήρια έχουν περιελάβει ένα ηλεκτρονικό τσιπ που περιέχει τις προσωπικές πληροφορίες του κατόχου και της φωτογραφίας διαβατηρίων. Το τσιπ κρατά τα εξής στοιχεία: το όνομα και επώνυμο την υπηκοότητά , την ημερομηνία γέννησης, το φύλο και τον προσωπικό αριθμό ταυτότητας ολλανδικού φόρου και κοινωνικής ασφάλισης[1].

**ΑΥΣΤΡΑΛΙΑ**

**14)Εφαρμογές βιομετρικής τεχνολογίας σε Τραπεζικά Συστήματα**

Το Πρότυπο ISO 19092:2008, που ονομάζεται Χρηματοπιστωτικές υπηρεσίες - Βιομετρικά - Ασφάλεια πλαίσιο, περιγράφει ένα πλαίσιο ασφάλειας για τη χρήση βιομετρικών στοιχείων για την εξακρίβωση της γνησιότητας των καταναλωτών και του προσωπικού στον τομέα των χρηματοπιστωτικών υπηρεσιών από την εικόνα δακτυλικών

[1] http://www.biometricgroup.com/

αποτυπωμάτων. Το πρότυπο καλύπτει τη μεταφορά, αποθήκευση, διάθεση και την ασφάλεια των βιομετρικών στοιχείων των πελατών από τα χρηματοπιστωτικά ιδρύματα.

"Η πραγματικότητα στην Αυστραλία είναι ότι τα επίπεδα απάτης είναι συγκριτικά χαμηλά και έτσι οι τράπεζες προσπαθούν να δικαιολογήσουν το τεράστιο κόστος που θα έχουν τα συστήματα πιστοποίησης της βιομετρικής αυθεντικότητας," τόνισε ο αναλυτής ασφαλείας μεγάλου χρηματοπιστωτικού οίκου James Turner.

«Είναι φθηνότερο για τις τράπεζες να επιστρέψουν τα χρήματα στα άτομα σε περιπτώσεις αποδεδειγμένης απάτης από ό, τι είναι να επεκτείνουν και να επενδύσουν σταδιακά σε συστήματα πιστοποίησης μέσω βιομετρικής αυθεντικότητας," πρόσθεσε ο Turner.

Ο Βιομετρικός έλεγχος γίνεται επίσης δημοφιλής στην επιβολή του νόμου και κρατικούς φορείς. Οι πρόσφατες τοπικές αναπτύξεις της Βιομετρίας περιλαμβάνουν το Υπουργείο Μετανάστευσης και Ιθαγένειας και την Αστυνομία.

Ομάδες Προστασίας Προσωπικών Δεδομένων, ωστόσο, έχουν εγείρει ανησυχίες σχετικά με τη χρήση των βιομετρικών πληροφοριών από τις κυβερνήσεις και τις επιχειρήσεις. Μια πρόσφατη έκθεση επέκρινε την Αυστραλία για τη «συστηματική αποτυχία να διατηρήσει εγγυήσεις» από την καταχρηστική χρήση των βιομετρικών πληροφοριών.

## ΥΠΟΛΟΙΠΗ ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

### 15) Βιομετρικό Διαβατήριο στην Ευρωπαϊκή Ένωση

Ευρωπαϊκά διαβατήρια έχουν προγραμματιστεί να ψηφιακής απεικόνισης και δακτυλικών αποτυπωμάτων σάρωση βιομετρικών στοιχείων τοποθετείται πάνω στο τσιπ RFID. Αυτός ο συνδυασμός των βιομετρικών στοιχείων έχει ως στόχο να δημιουργήσει ένα επίπεδο ασφάλειας και προστασίας από ψευδή έγγραφα ταυτοποίησης. Τεχνικές προδιαγραφές για τα νέα διαβατήρια που έχει καθιερωθεί από την Ευρωπαϊκή Επιτροπή. Οι προδιαγραφές είναι δεσμευτικές για τη συμφωνία του Σένγκεν μέρη, δηλαδή τις χώρες της ΕΕ, εκτός της Ιρλανδίας και του Ηνωμένου Βασιλείου, καθώς και τρία από τα τέσσερα Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών χώρες - Ισλανδία, Νορβηγία και την Ελβετία. Αυτές οι χώρες είναι υποχρεωμένες να εφαρμόσουν τα αναγνώσιμα από μηχάνημα εικόνες προσώπου στα διαβατήρια από την 28.08.2006, και τα δακτυλικά αποτυπώματα από την

29.06.2009. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων έχει δηλώσει ότι το ισχύον νομικό πλαίσιο δεν "αντιμετωπίζει όλα τα πιθανά σχετικό θέμα που προκύπτει από τις εγγενείς ατέλειες των βιομετρικών συστημάτων».

Επί του παρόντος, η βρετανική βιομετρικού διαβατηρίου χρησιμοποιεί μόνο μια ψηφιακή εικόνα και όχι η λήψη δακτυλικών αποτυπωμάτων, ωστόσο αυτό εξετάζεται από την Υπηρεσία Ηνωμένο Βασίλειο Passport. Η γερμανική εκτύπωση διαβατηρίων μετά την 1η Νοεμβρίου 2007, περιλαμβάνει δύο δακτυλικά αποτυπώματα, ένα από κάθε πλευρά, εκτός από μια ψηφιακή φωτογραφία. Τα διαβατήρια της Ρουμανίας θα περιέχει επίσης δύο δακτυλικά αποτυπώματα, ένα από κάθε χέρι. Η Ολλανδία λαμβάνει επίσης τα δακτυλικά αποτυπώματα και είναι το μόνο μέλος της ΕΕ που αποφάσισαν να αποθηκεύσετε αυτά τα δακτυλικά αποτυπώματα κεντρικά. Σύμφωνα με τις απαιτήσεις της ΕΕ, μόνο τα κράτη που έχουν υπογράψει το κεκτημένο του Σένγκεν οφείλουν να προσθέσετε βιομετρικών δακτυλικών αποτυπωμάτων. Σε αυτά τα έθνη της ΕΕ , η τιμή του διαβατηρίου θα είναι:

**Αυστρία** (διαθέσιμο από τις 16 Ιουνίου 2006) Το διαβατήριο ενηλίκου κοστίζει € 69,90. Από το Μάρτιο του 2009 όλα τα νέα διαβατήρια που εκδίδονται περιέχουν δακτυλικά αποτυπώματα.

**Βέλγιο** (θεσπίστηκε τον Οκτώβριο του 2004) € 71 ή € 41 για παιδιά προσθέτοντας τοπικούς φόρους. Τα διαβατήρια αυτά ισχύουν για 5 χρόνια.

**Βουλγαρία** (θεσπίστηκε τον Ιούλιο του 2009) διαθέσιμο από τις 29 Μαρτίου 2010): 40 λέβα (€ 20) για τους ενήλικες. Τα διαβατήρια αυτά ισχύουν για 5 χρόνια.

**Δημοκρατία της Τσεχίας** (διαθέσιμο από την 1η Σεπτεμβρίου 2006) 600 CZK για τους ενήλικες (που ισχύουν για 10 έτη), 100 CZK για τα παιδιά (που ισχύουν 5 έτη). Τα διαβατήρια περιέχουν δακτυλικά αποτυπώματα.

**Κύπρος** (διαθέσιμο από τις 13 Δεκεμβρίου 2010) € 70, για διάστημα 10 ετών.

**Δανία** (διαθέσιμο από την 1η Αυγούστου 2006) DKK 600 για τους ενήλικες (ισχύει για 10 έτη), 115 DKK για τα παιδιά (ισχύει για 5 έτη) και 350 DKK για άνω των 65 ετών (ισχύει για 10 έτη)

**Εσθονία** (διαθέσιμο από τις 22 Μαΐου 2007) ΕΕΚ 450 (€ 28,76) (ισχύει για 5 χρόνια). Όπως, της 29ης Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Φινλανδία** (διαθέσιμο από τις 21 Αυγούστου 2006) € 53 (ισχύει για 5 έτη). Όπως, της 29ης Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Γαλλία** (διαθέσιμα από τον Απρίλιο του 2006) € 86 ή € 89 (ανάλογα με το εάν ο αιτών παρέχει φωτογραφίες), ισχύει για 10 χρόνια. Από τις 16 Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Γερμανία** (διατίθεται από τον Νοέμβριο του 2005) ≤ 23 ετών αιτούντες (ισχύει για 6 έτη) € 37,50 και για > 24 ετών (ισχύει 10 έτη) € 59. Τα διαβατήρια που εκδίδονται από την 1η Νοεμβρίου 2007, σχετικά με περιλαμβάνουν δακτυλικά αποτυπώματα.

**Ελλάδα** (διαθέσιμο από τις 26 Αυγούστου 2006) € 76.40 (ισχύει για 5 χρόνια). Από τον Ιούνιο του 2009, τα διαβατήρια περιέχουν δακτυλικά αποτυπώματα.

**Ουγγαρία** (διαθέσιμο από τις 29 Αυγούστου 2006) 6000 HUF (€ 24), ισχύει για 5 έτη, 10000 HUF (€ 40) ισχύει για 10 χρόνια. Όπως, της 29ης Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Ιρλανδία** (διαθέσιμο από τις 16 Οκτωβρίου 2006) € 80, ισχύει για 10 χρόνια. Δωρεάν για άτομα άνω των 65 ετών. (Που δεν έχουν υπογράψει κεκτημένο του Σένγκεν, δεν υφίσταται υποχρέωση δακτυλικών αποτυπωμάτων βιομετρικών στοιχείων)

**Ιταλία** (διαθέσιμο από τις 26 Οκτωβρίου 2006) € 42.50, ισχύει για 10 χρόνια, καθώς και φορολογική ταινία των € 40,29 ανά έτος (πρώτη είναι υποχρεωτική? η οποία έληξε σφραγίδα φόρος απαιτείται μόνο όταν ταξιδεύουν εκτός της Ευρωπαϊκής Ένωσης). Ως τον Ιανουάριο του 2010 εκδόθηκαν προσφάτως διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Λετονία** (διαθέσιμο από τις 20 Νοεμβρίου 2007) Ένας ενήλικος έχει κόστος για έκδοση διαβατηρίου Ls 5 και ισχύει για 5 χρόνια.

**Λιθουανία** (διαθέσιμο από τις 28 Αυγούστου 2006) LTL 100 (€ 29). Για παιδιά έως 16 ετών, ισχύει μέχρι 5 χρόνια. Για τα άτομα άνω των 16 ετών, για διάστημα 10 ετών.

**Λουξεμβούργο** (διαθέσιμο από τις 28 Αυγούστου 2006) € 30. Ισχύει για 5 χρόνια. Όπως, της 29ης Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Μάλτα** (διατίθεται από τις 8 Οκτωβρίου 2008) € 70 για άνω των 16 ετών πρόσωπα, για διάστημα 10 ετών, € 35 για παιδιά ηλικίας μεταξύ 10-16 ετών (ισχύει για 5 έτη) και € 14 για παιδιά κάτω των 10 ετών (ισχύει για 2 χρόνια).

**Ολλανδία** (διαθέσιμο από τις 28 Αυγούστου 2006) € 11 Περίπου στην κορυφή της τακτικής διαβατηρίου (€ 38,33) κόστος € 49,33. Τα διαβατήρια που εκδίδονται από τις 21 Σεπτεμβρίου 2009 περιλαμβάνουν τα δακτυλικά αποτυπώματα. Ολλανδικά δελτία ταυτότητας είναι παρόμοιων εκδόσεων της σελίδας του κατόχου του διαβατηρίου και περιέχουν τα ίδια βιομετρικά στοιχεία.

**Πολωνία** (διαθέσιμο από τις 28 Αυγούστου 2006) 140 PLN (€ 35) για τους ενήλικες, 70PLN για τους φοιτητές, έγκυρα 10 χρόνια. Τα διαβατήρια που εκδίδονται από τις 29 Ιουνίου 2009 περιλαμβάνουν τα δακτυλικά αποτυπώματα και των δύο δάχτυλα δείκτη.

**Πορτογαλία** (διαθέσιμο από τις 31 Ιουλίου 2006) € 60 για ενήλικες (€ 50 για όσους είναι άνω των 65 ετών), ισχύει για 5 χρόνια. € 40 για παιδιά κάτω των 12, ισχύει για 2 χρόνια. Όλα τα διαβατήρια έχουν 32 σελίδες.

**Ρουμανία** (διαθέσιμο από τις 31 Δεκεμβρίου 2008) 276 RON (€ 67), ισχύει για 5 χρόνια για όσους είναι άνω των 6 ετών, και για 3 χρόνια για εκείνους κάτω των 6. Στις 19 Ιαν 2010, νέο διαβατήριο περιλαμβάνει τόσο εικόνες προσώπου και δακτυλικά αποτυπώματα.

**Σλοβακία** (διατίθεται από τις 15 Ιανουαρίου 2008) Ένα διαβατήριο ενηλίκων (> 13 χρόνια κοστίζει 33,19 € ισχύει για 10 χρόνια, ενώ (5-13 ετών) έκδοση ένα τσιπ χωρίς παιδιού

κοστίζει 13,27 € ισχύει για 5 χρόνια και για τα παιδιά κάτω των 5 ετών 8,29 € , αλλά ισχύει μόνο για 2 χρόνια.

**Σλοβενία** (διαθέσιμο από τις 28 Αυγούστου 2006) € 36 για ενήλικες, ισχύει για 10 χρόνια. € 31 για παιδιά από 3 μέχρι 18 ετών, που ισχύει για 5 χρόνια. € 28 για παιδιά μέχρι 3 ετών, ισχύει για 3 χρόνια. Όλα τα διαβατήρια έχουν 32 σελίδες, 48 σελίδων έκδοση είναι διαθέσιμη σε ένα € 2 επιπλέον χρέωση. Όπως, της 29ης Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Ισπανία** (διαθέσιμο από τις 28 Αυγούστου 2006) στην τιμή των € 13,45 (τιμή στο 7 Νοεμβρίου 2010). Αυτά περιλαμβάνουν τα δακτυλικά αποτυπώματα και των δύο δάχτυλα δείκτη από τον Οκτώβριο του 2009. (Ηλικίας 30 ή λιγότερο ένα ισπανικό διαβατήριο ισχύει για 5 χρόνια, αλλιώς θα παραμείνει σε ισχύ για 10 χρόνια).

**Σουηδία** (διατίθεται από τον Οκτώβριο του 2005) SEK 400 (ισχύει για 5 χρόνια). Όπως, της 29ης Ιουνίου 2009, όλες οι νεοεκδιδόμενες διαβατηρίων περιλαμβάνουν δακτυλικά αποτυπώματα.

**Ηνωμένο Βασίλειο** (που εισήχθη Μάρτιος 2006) £ 77.50 για ενήλικες και £ 49 για παιδιά κάτω των 16 ετών (που δεν έχουν υπογράψει κεκτημένο του Σένγκεν, δεν υφίσταται υποχρέωση δακτυλικών αποτυπωμάτων βιομετρικών στοιχείων)[1] .

**16) Καινοτόμες εφαρμογές από την Advanced Optical Systems (AOS)**

Η αμερικάνικη εταιρία Advanced Optical Systems (AOS), παρουσιάζει το AIRprint, το σκάνερ δακτυλικών αποτυπωμάτων που λειτουργεί από απόσταση δύο μέτρων. Αρχικά, το AIRprint χρησιμοποιεί δύο κάμερες 1.3 megapixel οι οποίες εκπέμπουν γραμμικά πολωμένο φως., η μία κάθετα και η άλλη οριζόντια. Οι δύο ακτίνες αντανακλούν τις κατακόρυφες και καμπυλωτές γραμμές των δακτυλικών αποτυπωμάτων, και έτσι

[1] http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-104850/ , http://rioter.info/english

επιταχύνουν την αναγνώριση του αποτυπώματος. Στη δεδομένη χρονική φάση, το AIRprint μπορεί να σκανάρει ένα δάχτυλο σε 1sec ενώ του παίρνει 4 sec για να το επεξεργαστεί. Υπολογίζεται ότι τον Απρίλη θα μπορεί να σκανάρει και τα πέντε δάχτυλα ενός χεριού ενώ αυτά κινούνται ενώ θα του παίρνει λιγότερο από 1 δευτερόλεπτο να τα επεξεργαστεί και να τα ταυτοποιήσει. Μάλιστα, όπως αναφέρει ο εκπρόσωπος τύπου, περίπου το καλοκαίρι, το σύστημα θα βγει στην αγορά.

Ιδιαίτερο ενδιαφέρον ,ωστόσο, παρουσιάζει η δραστηριότητα του Αμερικάνικου στρατού σ' αυτό το τομέα. Το Υπουργείο Άμυνας των ΗΠΑ επένδυσε 1.5 εκατομμύριο δολάρια για την αναβάθμιση της ακτίνας αναγνώρισης στα 13 μέτρα απόσταση. Όπως μάλιστα δηλώνει ο Jeremy Powell, επικεφαλής στις επιχειρήσεις αναγνώρισης των πεζοναυτών, των ΗΠΑ «είναι ένα βήμα μακριά από το να μπορεί κανείς να αναγνωρίζει την ταυτότητα ενός οποιουδήποτε ατόμου από ασφαλή απόσταση, είτε το γνωρίζει αυτό, είτε όχι!». Η νέα τεχνολογία πρόκειται να εφαρμοστεί στις επιχειρήσεις σε Αφγανιστάν και Ιράκ.

**ΕΛΛΑΔΑ:**

**1) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα μετά από καταγγελία που δέχτηκε σχετικά με τον έλεγχο εισόδου και εξόδου εργαζομένων από τον χώρο της εργασίας του πληροφορεί πως[1]:

· Η συλλογή, καταχώρηση και χρήση βιομετρικών χαρακτηριστικών, όπως είναι τα δακτυλικά αποτυπώματα, αποτελεί αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων που εμπίπτει στο πεδίο εφαρμογής του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001 γιατί τα βιομετρικά χαρακτηριστικά είναι δεδομένα προσωπικού χαρακτήρα σύμφωνα με τον ορισμό που εκτίθεται στο άρθρο 2 του Νόμου και συνεπώς η εν λόγω επεξεργασία πρέπει να διεξάγεται βάση τις αρχές και προϋποθέσεις που προβλέπονται στο Νόμο αυτό.

Η επεξεργασία βιομετρικών δεδομένων στον χώρο εργασίας κρίνεται υπερβολική εκτός από ορισμένες εξαιρετικές περιπτώσεις όπου ο σκοπός της επεξεργασίας επιτρέπει τη χρήση των δεδομένων αυτών.

[1] http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL

Τα βιομετρικά δεδομένα δεν προσδιορίζουν απλώς την ταυτότητα ενός ατόμου, αλλά την επιβεβαιώνουν. Ο εργοδότης για να δικαιολογήσει την αναγκαιότητα χρήσης βιομετρικών δεδομένων, πρέπει να είναι σε θέση να επικαλεστεί εξαιρετικούς λόγους π.χ. ασφάλεια, που επιβάλλουν την υιοθέτηση ανάλογων μέτρων. Πρέπει, επίσης, να είναι σε θέση να αποδείξει ότι η υιοθέτηση οποιωνδήποτε άλλων μέτρων, λιγότερο παρεμβατικών, είναι ανεπαρκής για τους σκοπούς που επιδιώκει. Οι εργοδότες πρέπει πάντα να επιλέγουν το λιγότερο παρεμβατικό τρόπο επεξεργασίας των βιομετρικών δεδομένων των εργοδοτουμένων, ο οποίος να σέβεται την προσωπικότητα και την ιδιωτική τους ζωή.

Μία από τις βασικές προϋποθέσεις για να είναι νόμιμη μια επεξεργασία είναι η αρχή της αναλογικότητας, με βάση την οποία τα δεδομένα που συλλέγονται πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από ότι κάθε φορά είναι απαραίτητο για την εκπλήρωση του σκοπού της επεξεργασίας. Στη περίπτωση αυτή, σκοπός της επεξεργασίας είναι ο έλεγχος της ώρας άφιξης και αναχώρησης των υπαλλήλων από την εργασία τους.

**(α)** Τα δακτυλικά αποτυπώματα συνιστούν προσωπικά δεδομένα των οποίων η επεξεργασία πρέπει να εκτελείται σύμφωνα με τις διατάξεις του Νόμου 138(I)/2001, και ότι ο Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι αρμόδια να ελέγξει τη νομιμότητα της επεξεργασίας των προσωπικών αυτών δεδομένων, εφόσον η συγκεκριμένη επεξεργασία που συνίσταται στη συλλογή, σύγκριση και αρχειοθέτηση των βιομετρικών χαρακτηριστικών αποτελεί αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων.

**(β)** Σε κάθε επεξεργασία προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι τηρούνται οι αρχές και προϋποθέσεις για νόμιμη επεξεργασία, μεταξύ των οποίων είναι και η αρχή της αναλογικότητας με βάση την οποία τα δεδομένα που συλλέγονται πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από ότι κάθε φορά είναι απαραίτητο για την εκπλήρωση του σκοπού της επεξεργασίας (άρθρο 4(γ) του Νόμου).

**(γ)** Είναι γενικά αποδεκτό πως η αναγνώριση του υποκειμένου των δεδομένων με τη μέθοδο της δακτυλοσκόπησης εξυπηρετεί κατά κύριο λόγο την εγκληματολογική πολιτική. Όπως αναφέρεται και σε Απόφαση της Ελληνικής Αρχής Προστασίας Δεδομένων, «η τήρηση αρχείου με δακτυλικά αποτυπώματα για τον έλεγχο της παρουσίας των εργαζομένων, πέρα από την εύλογη αντίδραση των υποκειμένων που προκαλεί, δεν μπορεί να θεωρηθεί ότι βαρύνει περισσότερο από την ανάγκη προστασίας του δικαιώματος του ατόμου στην ιδιωτική του ζωή και δεν συντρέχει λόγος να γίνει εξαίρεση από τη γενική αρχή ότι πληροφορίες τέτοιου είδους συλλέγονται και καταχωρούνται μόνο από αρχές οι οποίες είναι υποχρεωμένες από το νόμο να τηρούν σχετικά αρχεία. Τέτοια εξαίρεση θα μπορούσε να γίνει δεκτή μόνο σε ειδικές περιπτώσεις π.χ. για το σκοπό ελέγχου πρόσβασης σε χώρους απορρήτων αρχείων ή εγκαταστάσεων».

**2) Μη επιτρεπτός έλεγχος εισόδου και εξόδου εργαζομένων με βιομετρικά στοιχεία σε ιδιωτική επιχείρηση**

Φρένο στην ανεξέλεγκτη εφαρμογή των νέων τεχνολογικών μεθόδων επιτήρησης των πολιτών επιχειρεί να βάλει η Αρχή Προστασίας Προσωπικών Δεδομένων.

Με απόφασή της διατάσσει εταιρεία πλαστικών να ξηλώσει το βιομετρικό σύστημα που έχει τοποθετήσει στις εγκαταστάσεις της, προκειμένου να ελέγχει την τήρηση του ωραρίου και την είσοδο και την έξοδο των εργαζομένων στην επιχείρηση, ενώ της επιβάλλει πρόστιμο 1.500 ευρώ για παραβίαση του νόμου για τα προσωπικά δεδομένα.

Η Αρχή ασχολήθηκε με την υπόθεση ύστερα από καταγγελία του Σωματείου Εργατοϋπαλλήλων ότι στην εταιρεία έχει εγκατασταθεί βιομετρικό σύστημα με τη μέθοδο ελέγχου δακτυλικού αποτυπώματος και πως τα στοιχεία που συλλέγονται, καταγράφονται και αποθηκεύονται σε αρχείο.

Το σύστημα τοποθετήθηκε χωρίς να το γνωρίζουν οι εργαζόμενοι αφού η διοίκηση της επιχείρησης αρκέστηκε να τους ενημερώσει παραπλανητικά ότι «για την τήρηση των ωραρίων εργασίας θα τοποθετηθεί υπολογιστής παρουσιών σύμφωνα με τα πλαίσια της Επιθεώρησης Εργασίας».

Στη συνέχεια, όταν το Σωματείο ζήτησε να έχει πρόσβαση στο αρχείο και στα στοιχεία που τηρεί η εταιρεία, οι υπεύθυνοι αρνήθηκαν να ικανοποιήσουν το αίτημα.

Σύμφωνα με την απόφαση (50/2007), η επεξεργασία των δεδομένων των εργαζομένων με τη βιομετρική μέθοδο της ανάλυσης της γεωμετρίας του δακτύλου είναι παράνομη, ενώ επισημαίνεται ότι πρέπει να επιλέγονται ηπιότεροι τρόποι για την άσκηση του εργοδοτικού ελέγχου.

Η Αρχή δεν πείστηκε από τα επιχειρήματα που προέβαλε η εταιρεία, ότι είναι επιβεβλημένη ανάγκη να ελέγχεται η πρόσβαση στους χώρους της γιατί χρησιμοποιούνται εύφλεκτες ύλες και ρεύμα υψηλής τάσης, καθώς και ότι δεν προβλέπεται θέση προσωπάρχη γι' αυτό και είναι καλύτερο για τη λειτουργία της εταιρείας να καταγράφεται ηλεκτρονικά ο χρόνος εργασίας του προσωπικού.

Η μέθοδος της δακτυλοσκόπησης υπερβαίνει το σκοπό της επεξεργασίας και κατά συνέπεια παραβιάζει το νόμο 2472/1997 για τα προσωπικά δεδομένα, αποφάνθηκαν τα μέλη της Αρχής, τα οποία διατάσσουν την εταιρεία να αφαιρέσει το βιομετρικό σύστημα και να καταστρέψει το αρχείο που έχει ήδη δημιουργήσει με τα δεδομένα των εργαζομένων της. Απευθύνουν, επίσης, αυστηρή σύσταση στην εταιρεία να ενημερώνει από εδώ και στο εξής τους εργαζομένους αλλά και την Αρχή για τη λειτουργία οποιουδήποτε αρχείου.

Σύμφωνα με τη νομολογία που έχει χαράξει η Αρχή, «ο έλεγχος της παρουσίας των εργαζομένων με δακτυλικά αποτυπώματα, πέρα από την εύλογη αντίδραση των υποκειμένων που προκαλεί, δεν μπορεί να θεωρηθεί ότι βαρύνει περισσότερο από την ανάγκη προστασίας του δικαιώματος του ατόμου στην ιδιωτική του ζωή».

Μάλιστα, έχει κριθεί ότι «η άρνηση των εργαζομένων να δώσουν τα δακτυλικά τους αποτυπώματα δεν μπορεί να αποτελέσει αιτία για κυρώσεις εκ μέρους των εργοδοτών, εφόσον με τον τρόπο αυτό προσβάλλεται η προσωπικότητά τους και επιπροσθέτως η παραπάνω ενέργεια δεν εμπεριέχεται στο διευθυντικό δικαίωμα του εργοδότη για οργάνωση της επιχείρησής του αλλά, αντιθέτως, ενέχει εκδήλωση βλαπτικής μεταβολής της σύμβασης, την οποία μπορεί αζημίως να αρνηθεί ο εργαζόμενος».

## 3) Επιτρεπτές οι μέθοδοι Βιομετρίας λόγους ασφαλείας στον Κρατικό Αερολιμένα Αθηνών

Ο Διεθνής Αερολιμένας Αθηνών (ΔΑΑ) αποτελεί το μεγαλύτερο κόμβο εισόδου-εξόδου των αλλοδαπών επισκεπτών της χώρας μας[1]. Αναμφισβήτητα, κατά τη διάρκεια των Ολυμπιακών Αγώνων του 2004, οπότε και αναμένονται εκατομμύρια επισκεπτών, ο ΔΑΑ θα επωμισθεί ακόμη μεγαλύτερο φορτίο, γεγονός που καθιστά πρωταρχική την ανάγκη εύρυθμης και ασφαλούς λειτουργίας του. Ένας κρίσιμος επιχειρησιακά χώρος του ΔΑΑ είναι το Κέντρο Επιχειρήσεων (Aviation Services Operation Center, ASOC).

Στόχος του παρόντος έργου είναι η περαιτέρω ενίσχυση και βελτίωση των τεχνικών μέτρων και των διαδικασιών ασφάλειας του ΔΑΑ, η οποία θα επιτευχθεί με τη συστηματική αξιοποίηση επιλεγμένων και σύγχρονων (state-of-the-art) τεχνολογιών ασφάλειας κρίσιμων εγκαταστάσεων και υποδομών. Συγκεκριμένα θα μελετηθεί η εφικτότητα και θα αποτιμηθεί η σκοπιμότητα αξιοποίησης βιομετρικών τεχνολογιών (biometrics) για τον έλεγχο της φυσικής πρόσβασης στο Κέντρο Επιχειρήσεων του Αεροδρομίου, στο πλαίσιο των προβλέψεων της σχετικής νομοθεσίας (Νόμος 2472/1997).

Τα κύρια παραδοτέα του έργου είναι:

• Ανάλυση Επικινδυνότητας του ASOC: Εντοπισμός των απειλών που υφίσταται το ASOC, των πιθανών αδυναμιών του, όπως επίσης και των εκτιμώμενων επιπτώσεων από κάποιο περιστατικό ανασφάλειας.

• Διαχείριση Επικινδυνότητας του ASOC: Πρόταση συγκεκριμένων τεχνικών και οργανωτικών μέτρων που είναι αναγκαία για την αντιμετώπιση των κινδύνων, με επικέντρωση και έμφαση στη σκοπιμότητα χρήσης βιομετρικών τεχνολογιών.

[1] http://www.tovima.gr/

**4) Βιομετρικό Διαβατήριο**

Το βιομετρικό διαβατήριο[1] είναι ένα ηλεκτρονικό έγγραφο, το οποίο χρησιμοποιεί τα βιομετρικά χαρακτηριστικά προκειμένου να πιστοποιήσει την ταυτότητα των κατόχων του. Οι πληροφορίες αποθηκεύονται σε ένα μικροσκοπικό chip, όπως ακριβώς αποθηκεύονται διάφορες πληροφορίες στις έξυπνες κάρτες (smartcards). Το chip χρησιμοποιείτε επίσης, προκειμένου να εξασφαλιστεί η ακεραιότητα του διαβατηρίου καθώς και των βιομετρικών δεδομένων του. Στην Ελλάδα είναι διαθέσιμο από τις 26 Αυγούστου 2006, ισχύει για 5 χρόνια.

Ο συνδυασμός αυτός των βιομετρικών χαρακτηριστικών έχει ως σκοπό να δημιουργήσει ένα επίπεδο ασφάλειας και προστασίας ενάντια στα πλαστά και ψευδή έγγραφα ταυτοποίησης.

Ο I.C.A.O. (International Civil Aviation Organisation) έχει ορίσει την αναγνώριση προσώπου ως το πρωτεύων βιομετρικό χαρακτηριστικό. Η αναγνώριση του δακτυλικού αποτυπώματος, έχει οριστεί ως εφεδρική και μη υποχρεωτική αναγνώριση.

Η αυξανόμενη απειλή της απάτης με χρήση πλαστών ταξιδιωτικών εγγράφων, απαιτεί την ενίσχυση των χαρακτηριστικών γνωρισμάτων ασφάλειας στα διαβατήρια.

Τα βιομετρικά διαβατήρια πέραν του νέου σχεδιασμού διαθέτουν και πρόσθετα χαρακτηριστικά γνωρίσματα ασφαλείας. Χαρακτηριστικά όπως σελίδες με περίπλοκα σχέδια/αναπαραστάσεις, υδατογραφήματα καθώς και το προαναφερόμενο chip.

Η χρήση βιομετρικών δεδομένων βοηθάει στην αντιμετώπιση της απάτης και μπορεί να προσδιορίσει την πλαστότητα ενός εγγράφου. Στην πράξη, η βιομετρική εξακρίβωση μπορεί να χρησιμοποιηθεί σε σημεία ελέγχου (σύνορα) προκειμένου ελεγχθεί και εξακριβωθεί η εικόνα που εμφαίνεται επί του διαβατηρίου με αυτή που κρατείται στο αρχείο της Υπηρεσίας.

Το νέο Ελληνικό διαβατήριο ανταποκρίνεται στα διεθνή πρότυπα όπως καθορίζονται από

[1] http://www.passport.gov.gr/npc-periexomeno/npc-periexomeno/odigies-ekdosis-diavatiriou.html

το I.C.A.O. (International Civil Aviation Organisation). Έχει πολλά νέα χαρακτηριστικά γνωρίσματα ασφάλειας, συμπεριλαμβανομένου ενός chip.

Τα χαρακτηριστικά γνωρίσματα ασφαλείας διασφαλίζουν εάν το διαβατήριο είναι γνήσιο. Επίσης, τα βιομετρικά χαρακτηριστικά του προσώπου βοηθούν ώστε να συνδεθεί ο κάτοχος του διαβατηρίου με το έγγραφο αυτό.

Το αποθηκευμένα δεδομένα που βρίσκονται στο chip, προστατεύονται με τη χρήση προηγμένων ψηφιακών τεχνικών κρυπτογράφησης.

Τα δεδομένα του chip είναι ασφαλή. Αυτή η ασφάλεια επιτυγχάνετε μέσω τριών (3) επιπέδων ασφαλείας:

- Μέσω ψηφιακής υπογραφής η οποία πιστοποιεί αφενός ότι τα κωδικοποιημένα στοιχεία είναι γνήσια και αφετέρου την χώρα που έχει εκδόσει το διαβατήριο.

- Προστασία ενάντια οποιασδήποτε αναρμόδιας ανάγνωσης ("skimming") μέσω του βασικού ελέγχου πρόσβασης (Basic Access Control), ένα ασφαλές πρωτόκολλο πρόσβασης.

- Τα δεδομένα κλειδώνονται κάνοντας χρήση Υποδομής Δημοσίου Κλειδιού (PKI), το οποίο παρέχει προστασία κατά οποιασδήποτε τροποποίησης κωδικοποιημένων δεδομένων. Το PKI είναι η τεχνολογία ψηφιακής κρυπτογράφησης, η οποία επιτρέπει την επικύρωση των δεδομένων ως προς την γνησιότητα τους και εμφανίζει οποιαδήποτε αλλαγή - προσθήκη ή διαγραφή στο chip του διαβατηρίου.

**5) Ταυτότητες Ελλήνων Αστυνομικών**

Παρουσίαση των Νέων Ταυτοτήτων τύπου πιστωτικής κάρτας Αστυνομικού Προσωπικού ( Αστυνομικών- Ειδικών Φρουρών- Συνοριακών Φυλάκων ) από το επίσημο κανάλι της Ελληνικής Αστυνομίας (ΕΛ.ΑΣ.) που εκτυπώνονται στη Διεύθυνση Διαβατηρίων της ΕΛ.ΑΣ. της οποίας το προσωπικό συγκατατίθεται στη βιομετρική επεξεργασία των δακτυλικών του αποτυπωμάτων με ηλεκτρονική σάρωση δακτύλου του

δεξιού χεριού προς επαλήθευση των δεδομένων της κάρτας εισόδου η σάρωση της οποίας προηγείται & η βιομετρική επαλήθευση απαιτείται για το άνοιγμα της θύρας της Δ/νσης.

Οι Νέες Ταυτότητες Αστυνομικού Προσωπικού είναι ηλεκτρονικές μεν την στιγμή, που περιέχουν στην οπίσθια όψη μηχανικώς αναγνώσιμη ζώνη - Machine Readable Zone (MRZ) αλλά όχι βιομετρικές δε αφού δεν περιλαμβάνουν μέσο αποθήκευσης (chip) όπου σχεδιάζουν να ψηφιοποιήσουν τα δακτυλικά αποτυπώματα του συνόλου του πληθυσμού με την αντικατάσταση των Αστυνομικών Δελτίων Ταυτότητας (ΑΔΤ) με τις Κάρτες του Πολίτη.

### 2.1.4 Πλεονεκτήματα

Το σκανάρισμα των δαχτύλων έχει σε σύγκριση με τις ανταγωνιστικές τεχνολογίες ορισμένα πλεονεκτήματα, που οφείλονται στην ίδια τη φύση της τεχνολογίας και στις λειτουργίες της αγοράς.

**Αυξημένη αξιοπιστία και ακρίβεια**

Η μελέτη, ανάλυση και ταξινόμηση των δακτυλικών αποτυπωμάτων έχει ξεκινήσει εδώ και δεκαετίες. Η αξία των αποτυπωμάτων, ως διακριτών προσδιοριστών της ανθρώπινης ύπαρξης είναι εγνωσμένη και δοκιμασμένη στο χρόνο, γι' αυτό παρά την ύπαρξη φυσιολογικών χαρακτηριστικών, που είναι πιο διακριτά απ' το δάχτυλο – η ίριδα και ο αμφιβληστροειδής για παράδειγμα – καμία άλλη βιομετρική τεχνολογία δεν έχει καταφέρει να κλονίσει την πρωτοκαθεδρία του ελέγχουν των αποτυπωμάτων. Χάρη στις σύγχρονες, ισχυρές υλοποιήσεις των συστημάτων σκαναρίσματος δαχτύλων, η διενέργεια χιλιάδων συγκρίσεων με μηδενικά ποσοστά λάθους και με λήψη μόλις ενός με δύο δειγμάτων είναι πλέον εφικτή. Έτσι, εξυπηρετούνται εξίσου οι σκοποί της ασφάλειας των δεδομένων και της διευκόλυνσης των χρηστών.

**Δυνατότητα χρησιμοποίησης σε διαφορετικά περιβάλλοντα**

Χάρη στις μειωμένες απαιτήσεις σε μέγεθος και ενέργεια και την ικανότητα προσαρμογής της στις αλλαγές του περιβάλλοντος, η τεχνολογία σκαναρίσματος δαχτύλων μπορεί και χρησιμοποιείται σε ετερόκλητα περιβάλλοντα, άλλοτε για λογική κι

άλλοτε για φυσική πρόσβαση. Πράγματι, οι συσκευές απόκτησης αποτυπωμάτων είναι πλέον πολύ μικρές – έχουν διαστάσεις περίπου 1,5cm x 1,5cm και πάχος όσο περίπου ένα νόμισμα – ενώ ανταποκρίνονται πολύ καλά σε αλλαγές στο φωτισμό ή τη θερμοκρασία.

Σήμερα, τα προϊόντα σκαναρίσματος δαχτύλων που κυκλοφορούν στην αγορά είναι πάρα πολλά. Μάλιστα ξεπερνούν σε πλήθος τα προϊόντα όλων μαζί των υπολοίπων βιομετρικών τεχνολογιών. Αν και αυτό θα μπορούσε να λειτουργήσει αρνητικά – λόγω του καταιγισμού των ενδιαφερομένων από έναν τεράστιο όγκο βιομετρικών προτάσεων – στην πραγματικότητα, ο υψηλός ανταγωνισμός έχει ως αποτέλεσμα τη διάθεση εύρωστων λύσεων για κάθε περιβάλλον.

**Χρήση εργονομικών συσκευών**

Η τοποθέτηση του δαχτύλου σε μια συσκευή, είναι από πολλές απόψεις μια κίνηση ενστικτώδης, που απαιτεί πολύ λίγη εκπαίδευση. Σε αντίθεση με άλλες βιομετρικές τεχνολογίες, που προϋποθέτουν πολύπλοκες αλληλεπιδράσεις του χρήστη με το σύστημα, οι συσκευές σκαναρίσματος δαχτύλων είναι σχεδιασμένες, έτσι ώστε η τοποθέτηση του δαχτύλου με συγκεκριμένο τρόπο να μπορεί εύκολα να επαναληφθεί. Εξάλλου, πρόσφατες βελτιώσεις έχουν συμβάλει περαιτέρω στην καλύτερη καθοδήγηση του χρήστη για σωστή τοποθέτηση του δαχτύλου.

**Δυνατότητα εγγραφής με πολλά δάχτυλα**

Αν και δε συνηθίζεται, το γεγονός ότι ένα άτομο μπορεί να εγγραφεί και με τα 10 δάχτυλα σ' ένα βιομετρικό σύστημα, προσφέρει ευελιξία, αλλά και πλεονεκτήματα από πλευράς ασφάλειας. Αν για παράδειγμα, η χορήγηση πρόσβασης σε ένα σύστημα προϋποθέτει ταίριασμα δύο διαφορετικών αποτυπωμάτων του χρήστη, τότε η πιθανότητα λάθους είναι αστρονομική. Επιπλέον, οι χρήστες έχουν τη δυνατότητα να συνδέουν συγκεκριμένα δάχτυλα με ειδικές λειτουργίες του συστήματος. Ένας χρήστης δηλαδή, μπορεί να χρησιμοποιεί ένα ορισμένο δάχτυλο σε καταστάσεις κινδύνου (π.χ. όταν η προσπάθεια για φυσική πρόσβαση γίνεται με χρήση απειλής), ένα άλλο δάχτυλο για πρόσβαση σε συγκεκριμένες εφαρμογές κ.ο.κ. Ένα ακόμη όφελος, είναι ότι το σύστημα

μπορεί σε κάθε έλεγχο να ζητάει από το χρήστη τυχαία να επιδείξει ένα από τα δάχτυλα εγγραφής, μειώνοντας έτσι την πιθανότητα κλοπής και χρήσης βιομετρικών δεδομένων.

### 2.1.5 Μειονεκτήματα

Παρά τα σημαντικά πλεονεκτήματα που έχει το σκανάρισμα των δαχτύλων, παρουσιάζει σαν τεχνολογία κάποιες αδυναμίες. Αυτές απαλύνονται σε ένα βαθμό με τον έξυπνο σχεδιασμό των συστημάτων, αλλά δεν παύουν να μειώνουν την αποτελεσματικότητα της συγκεκριμένης τεχνολογίας σε κάποιες εφαρμογές.

**Αδυναμία εγγραφής κάποιων χρηστών**

Υπάρχει ένα ποσοστό χρηστών, το οποίο δεν μπορεί να εγγραφεί στα περισσότερα συστήματα σκαναρίσματος δαχτύλων. Ανάλογα με την χρησιμοποιούμενη υλοποίηση της τεχνολογίας και την εξεταζόμενη πληθυσμιακή ομάδα, το ποσοστό αυτό μπορεί να είναι μικρότερο της μονάδας ή να αγγίζει μεγαλύτερα μονοψήφια νούμερα. Συνήθως τα υψηλά ποσοστά αναφέρονται σε ιδιαίτερες εθνικές και δημογραφικές ομάδες του πληθυσμού, με ιδιαίτερη έμφαση στους ηλικιωμένους, τους εργάτες και τους Ασιάτες.

Οι συνέπειες αυτού του προβλήματος ποικίλλουν ανάλογα με την περίπτωση. Για μια επιχείρηση, η αδυναμία εγγραφής ορισμένων υπαλλήλων συνεπάγεται την ανάγκη ύπαρξης και συντήρησης ενός εναλλακτικού σχήματος πιστοποίησης. Σε εφαρμογές πελατών η αποτυχία εγγραφής προκαλεί αποκλεισμό του πελάτη. Σε μεγάλα συστήματα αναγνώρισης σημαίνει ότι κάποιοι χρήστες έχουν τη δυνατότητα λόγω της έλλειψης βιομετρικού ελέγχου, να εγγραφούν στο σύστημα περισσότερες από μία φορές. Αν πάλι η πολιτική του συστήματος είναι πιο ελαστική στην αποδοχή αμφισβητούμενων αποτυπωμάτων, τότε το σύνηθες αποτέλεσμα είναι η αύξηση των ποσοστών λάθους.

**Μακροπρόθεσμη μείωση απόδοσης**

Αν και το δαχτυλικό αποτύπωμα είναι ένα χαρακτηριστικό της φυσιολογίας του ανθρώπου αρκετά σταθερό στο χρόνο, η καθημερινή φθορά στην οποία υπόκειται επηρεάζει αρνητικά την απόδοση του συστήματος. Έτσι, τα ποσοστά λάθους ορισμένων συστημάτων γνωρίζουν έκρηξη μέσα σε λίγους μήνες, αν και υπάρχουν και συστήματα πολύ αξιόπιστα, με ποσοστά διαχρονικά αμετάβλητα. Γενικά πάντως, τα άτομα που

καταπονούν τα χέρια τους, όπως οι εργάτες, επιβαρύνουν τη συνολική απόδοση των συστημάτων. Η διενέργεια ποιοτικών εγγραφών με περισσότερα από ένα δάχτυλα, και η επανεγγραφή όσων χρηστών αναγνωρίζονται με δυσκολία από το σύστημα, είναι δύο τρόποι περιορισμού και επόπτευσης του προβλήματος.

**Συσχετισμός με εφαρμογές της σήμανσης**

Η διαδικασία σκαναρίσματος δαχτύλων προξενεί σε αρκετούς ανθρώπους τη δυσφορία, λόγω της ομοιότητας που έχει με τη λήψη αποτυπωμάτων για εγκληματολογικούς σκοπούς. Συχνά μάλιστα εκφράζεται ο φόβος, ότι η συλλογή των αποτυπωμάτων εξυπηρετεί σκοπούς της αστυνομίας ή χρησιμεύει στην καταγραφή των δραστηριοτήτων ενός ατόμου. Έτσι, παρά το γεγονός τα σύγχρονα μηχανήματα δεν αποθηκεύουν τις εικόνες των αποτυπωμάτων και δε διαθέτουν τις προϋποθέσεις για να χρησιμοποιηθούν για αλλότριους σκοπούς, περιβάλλονται με δυσπιστία από κάποιους πολίτες. Παρότι δηλαδή δεν ευσταθούν, οι αρνητικοί συνειρμοί που δημιουργούνται στο κοινό καταπραΰνονται δύσκολα, και καταφέρνουν να πλήξουν την ευρύτερη διάδοση και αποδοχή της συγκεκριμένης τεχνολογίας.

**Ανάγκη για εξειδικευμένες συσκευές**

Για να μπορέσει να εδραιωθεί το σκανάρισμα των δαχτύλων, ως μια κυρίαρχη τεχνολογία στην ασφάλεια συστημάτων, πρέπει να επιτευχθεί η διείσδυσή του σε όλους τους χώρους οπού υπάρχει ανάγκη για επικύρωση της αυθεντικότητας, σε περιβάλλοντα desktop, στα σημεία πώλησης, σε φυλασσόμενες εισόδους κτλ. Για να γίνει αυτό όμως, απαιτείται η εγκατάσταση συσκευών, σε μεγάλο βαθμό εξειδικευμένων. Κι αυτό γιατί το σκανάρισμα των δαχτύλων, δεν μπορεί να στηριχθεί σε υπάρχουσες εγκαταστάσεις και μηχανήματα, όπως μπορεί για παράδειγμα το σκανάρισμα της φωνής, που εκμεταλλεύεται την υπάρχουσα υποδομή σε τηλέφωνα και μικρόφωνα. Μάλιστα οι συσκευές που χρησιμοποιούνται στο σκανάρισμα δαχτύλων διαφέρουν από εφαρμογή σε εφαρμογή. Έτσι, η ενσωμάτωση στο πληκτρολόγιο μιας συσκευής σκαναρίσματος, αν και αποτελεί σημαντική πρόοδο για τις εφαρμογές desktop, δεν προσφέρει στο πρόβλημα της θωράκισης των συστημάτων φυσικής πρόσβασης. Υπάρχει συνεπώς μεγάλη εξειδίκευση στις απαιτούμενες συσκευές.

### 2.1.7 Συμπεράσματα

Πρέπει να πούμε ότι, παρά τα προβλήματα που παρουσιάζει η τεχνολογία σκαναρίσματος δαχτύλων, είναι μια λύση που αναμένεται να κυριαρχήσει, γιατί απευθύνεται σε πολλά και διαφορετικά περιβάλλοντα. Δεν αποτελεί βέβαια την ιδανική λύση για κάθε περίσταση, μπορεί όμως να χρησιμοποιηθεί με αποτελεσματικότητα σ' ένα μεγάλο πλήθος εφαρμογών. Επίσης, όσοι θέλουν να κάνουν χρήση της τεχνολογίας έχουν να επιλέξουν μεταξύ δεκάδων προϊόντων της αγοράς, ορισμένα εκ των οποίων είναι συμβατά και με middleware λύσεις. Καθώς μάλιστα η αγορά υιοθετεί ευρέως κάποια standards, οι προτεινόμενες λύσεις αναμένεται να είναι ακόμα πιο αποδοτικές.

## 2.2 ΤΟ ΣΚΑΝΑΡΙΣΜΑ ΤΟΥ ΠΡΟΣΩΠΟΥ

Η τεχνολογία σκαναρίσματος προσώπου διεξάγει πιστοποίηση ή αναγνώριση, βασιζόμενη σε διακριτά χαρακτηριστικά του ανθρώπινου προσώπου. Χρησιμοποιείται κυρίως σε συστήματα αναγνώρισης 1:N, ενίοτε σε συνδυασμό με τεχνολογία καρτών. Η χρήση σκαναρίσματος προσώπου σε εφαρμογές 1:1 για φυσική ή λογική πρόσβαση είναι περιορισμένη. Γενικά, οι πιο πετυχημένης υλοποιήσεις της συγκεκριμένης τεχνολογίας αφορούν σε περιπτώσεις, όπου υπάρχουν ήδη εγκατεστημένες κάμερες και συστήματα καταγραφής[1].

### 2.2.1 Συστατικά μέρη

Ένα σύστημα σκαναρίσματος προσώπου μπορεί να αποτελείται μόνο από το απαιτούμενο λογισμικό για επεξεργασία εικόνων – οπότε οι εικόνες αποκτώνται μέσα από προϋπάρχουσες κάμερες CCTV (closed-circuit television) – ή να αναφέρεται σε ολοκληρωμένες λύσεις, που περιλαμβάνουν κάμερες, σταθμούς εργασίας και back-end επεξεργαστές, για απόκτηση και επεξεργασία εικόνας. Στις περισσότερες περιπτώσεις, τα συστήματα σκαναρίσματος προσώπου είναι σχεδιασμένα να χρησιμοποιούν για την

[1] Shaogang Gong, Stephen J. McKenna and Alexandra Psarrou, "Dynamic Vision: From Images to Face Recognition", October 1999.

απόκτηση των εικόνων, μεθόδους και συσκευές διαφορετικές μεταξύ τους, αξιοποιώντας για παράδειγμα εικόνες από στατικές φωτογραφίες, Web κάμερες, κάμερες παρακολούθησης κτλ. Σπανιότερα, υπάρχει εξειδίκευση των συστημάτων, ως προς τις χρησιμοποιούμενες συσκευές απόκτησης.

Δύο είναι τα βασικά συστατικά μέρη στην τεχνολογία σκαναρίσματος προσώπου: η μηχανή εντοπισμού, που εντοπίζει και καταγράφει πρόσωπα μέσα σε ένα συγκεκριμένο πεδίο δράσης και η μηχανή αναγνώρισης, που συγκρίνει αυτά τα πρόσωπα. Συνήθως, οι δύο μηχανές βρίσκονται στο ίδιο PC ή συσκευή και συνεργάζονται στενά μεταξύ τους. Η εξέλιξη της τεχνολογίας σήμερα, επιτρέπει την επέκταση και ενσωμάτωση της δυνατότητας σκαναρίσματος προσώπου σε αρκετά μικρότερες συσκευές, όπως τα PDAs και τα κινητά τηλέφωνα.

Τα συστήματα σκαναρίσματος προσώπου, σπάνια χρησιμοποιούνται σε εφαρμογές λογικής ή φυσικής πρόσβασης για πιστοποίηση ταυτότητας 1:1, και συνήθως ενσωματώνονται σε συστήματα παρακολούθησης και μεγάλα συστήματα αναγνώρισης. Γι' αυτό και υπάρχει μικρότερη ανάγκη στα συστήματα αυτά, για ενσωμάτωση περίπλοκης λειτουργικότητας μετά από επιτυχημένο ή αποτυχημένο ταίριασμα, σε αντίθεση με ότι συμβαίνει π.χ. στα συστήματα σκαναρίσματος δαχτύλων. Γενικά, το ταίριασμα είναι πολύ πιθανό να πυροδοτήσει την έναρξη κάποιας χειρωνακτικής διαδικασίας, π.χ. την ανάληψη δράσης από τους υπεύθυνους ασφαλείας ενός κτιρίου.

### 2.2.2 Τρόπος λειτουργίας

Ο τρόπος λειτουργίας της τεχνολογίας σκαναρίσματος προσώπου, δε διαφέρει από το παραδοσιακό σχήμα λειτουργίας των βιομετρικών συστημάτων. Περιλαμβάνει την απόκτηση και επεξεργασία εικόνας, την εξαγωγή των διακριτών χαρακτηριστικών, τη δημιουργία των templates και τέλος το ταίριασμα.

**Απόκτηση εικόνας**

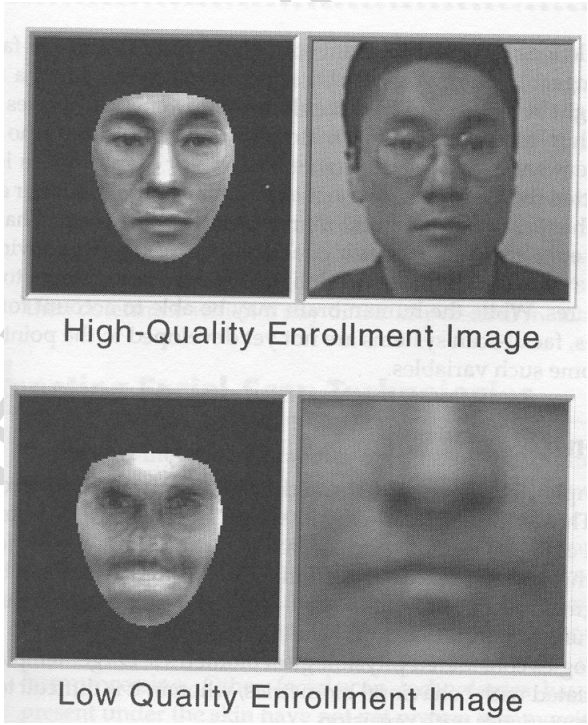
Η τεχνολογία σκαναρίσματος προσώπου χρησιμοποιεί εικόνες από οποιαδήποτε στατική κάμερα ή σύστημα βιντεοσκόπησης υψηλής πιστότητας. Στην ιδανική περίπτωση, ο

χρήστης κοιτάζει απευθείας στην κάμερα και το πρόσωπό του φωτίζεται μέτρια. Αν και κάποιες τεχνολογίες είναι σε θέση να ψάξουν σε ψηφιοποιημένες εικόνες για πρόσωπα μικρά σε μέγεθος, με μόνο 30 pixels ύψος, είναι προτιμότερο και φυσικά ασφαλέστερο οι διαστάσεις του προσώπου και σε μήκος και σε ύψος να ξεπερνούν τα 100 pixels.

Οι λόγοι που δυσχεραίνουν την απόκτηση καλών εικόνων είναι πολλοί. Όταν η απόσταση από την κάμερα είναι μεγάλη, το μέγεθος του προσώπου μικραίνει και άρα επηρεάζεται αρνητικά η συνολική πιστότητα της εικόνας. Η δυνατότητα μεγέθυνσης των προσώπων δεν επιλύει ικανοποιητικά το πρόβλημα. Επιπλέον, οι χρήστες που δεν κοιτάζουν ευθεία στην κάμερα και απέχουν παραπάνω από 15 μοίρες, είτε οριζόντια είτε κάθετα από την ιδανική θέση, δυσχεραίνουν τη λήψη μιας εικόνας επαρκούς για πιστοποίηση. Υπάρχει ακόμα διαφορά στην τιμή threshold που απαιτείται για να μπορέσει ένα σύστημα να εντοπίσει ένα πρόσωπο στο πεδίο λήψης του, και σε εκείνη που απαιτείται για να μπορέσει να το εγγράψει ή να το αναγνωρίσει. Το σύστημα δηλαδή ενδεχομένως να εντοπίσει ένα πρόσωπο, αλλά λόγω π.χ. της γωνίας του προσώπου να αδυνατεί να το εγγράψει στη βάση δεδομένων ή να το αναγνωρίσει. Για να λυθεί το συγκεκριμένο πρόβλημα, οι νεότερες μέθοδοι σκαναρίσματος προσώπου λαμβάνουν εικόνες του χρήστη από διαφορετικές γωνίες, ενώ δηλαδή αυτός κοιτάει επάνω, κάτω, δεξιά, αριστερά. Έτσι, τα παραγόμενα templates είναι πιο περιεκτικά σε πληροφορίες και μειώνονται τα περιθώρια λάθους.

Ένα πιο σοβαρό πρόβλημα είναι ο φωτισμός. Τα βιομετρικά συστήματα αδυνατούν να αποκτήσουν ευκρινείς εικόνες, όταν η έκθεση στο φωτισμό είναι υπερβολική ή πολύ μικρή. Ένα συναφές πρόβλημα είναι η έλλειψη αυτόματης προσαρμογής των περισσότερων συστημάτων, σε άτομα με διαφορετικό τύπο δέρματος. Αυτή η αδυναμία, συνεπάγεται μειωμένη ποιότητα των εικόνων, που προέρχονται από άτομα συγκεκριμένων φυλών κι εθνικοτήτων. Συνήθως, τα περισσότερα προβλήματα αντιμετωπίζουν τα άτομα ισπανικής προέλευσης, οι μαύροι και οι Ασιάτες, για το λόγο ότι οι συσκευές είναι προσαρμοσμένες, ώστε οι βέλτιστες λήψεις να γίνονται στα πιο ανοιχτόχρωμα άτομα. Έτσι, δεν αποκλείεται το παράδοξο για τα ανθρώπινα δεδομένα φαινόμενο, ένα άτομο να στέκεται μπροστά από ένα σύστημα σκαναρίσματος προσώπου και το σύστημα να μην μπορεί να το δει. Τα παραπάνω ζητήματα αντιμετωπίζονται κυρίως με τη χρήση συστημάτων με αυτόματη ικανότητα προσαρμογής στο φωτισμό και το χρώμα του δέρματος.

Ο βαθμός έκτασης των παραπάνω προβλημάτων πάντως διαφέρει, ανάλογα με το αν η τεχνολογία εφαρμόζεται σε συστήματα αναγνώρισης δημοσίου συμφέροντος 1:N, σε συστήματα πιστοποίησης 1:1 ή σε συστήματα παρακολούθησης. Σε γενικές γραμμές, τα μεγάλα συστήματα αναγνώρισης είναι τα λιγότερο πιθανά να παρουσιάσουν πρόβλημα, γιατί η διαδικασία λήψης των εικόνων γίνεται με τρόπο ελεγχόμενο και συνεπή. Συγκεκριμένα, οι χρήστες καλούνται να σταθούν σε μια καθορισμένη απόσταση από την κάμερα, ενώ ο φωτισμός και το φόντο είναι σταθερά. Στα συστήματα πιστοποίησης 1:1 κυριαρχεί η πρωτοβουλία του χρήστη, με συνέπεια παράμετροι, όπως ο φωτισμός και η γωνία λήψης να αλλάζουν κι έτσι να προκαλούνται προβλήματα. Τέλος, στην περίπτωση των συστημάτων παρακολούθησης, τα προβλήματα αυτά είναι ακόμα πιο έντονα, γιατί οι λήψεις συνήθως αφορούν άτομα ανυποψίαστα, με λάθος τοποθέτηση στο φακό, που ενδεχομένως κινούνται. Σε κάθε περίπτωση πάντως, είναι αναγκαίες οι προσπάθειες για περιορισμό των προβλημάτων, γιατί από την απόκτηση σωστών εικόνων του χρήστη εξαρτώνται όλες οι μετέπειτα λειτουργίες. Συνεπώς, η κάθε παράμετρος του συστήματος πρέπει να προσμετράται με πολύ προσοχή.




**Σχήμα 8.** Εικόνες σκαναρίσματος προσώπου υψηλής ποιότητας και χαμηλής ποιότητας

**Επεξεργασία εικόνας**

Μετά την απόκτηση της εικόνας ακολουθεί η επεξεργασία της[1]. Συγκεκριμένα, οι εικόνες αποκόπτονται και παραμένει μόνο το πρόσωπο, ενώ όσες είναι έγχρωμες συνήθως μετατρέπονται σε ασπρόμαυρες. Αυτό διευκολύνει αρχικές συγκρίσεις, που βασίζονται σε γκριζόχρωμα χαρακτηριστικά. Μετά το πρώτο στάδιο, οι προκύπτουσες εικόνες υποβάλλονται σε κανονικοποίηση, για να εξομαλυνθούν οι όποιες διαφοροποιήσεις στον προσανατολισμό και την απόσταση. Για την κανονικοποίηση, αρχικά εντοπίζονται στην εικόνα βασικά χαρακτηριστικά που λειτουργούν σαν ένα πλαίσιο αναφοράς, όπως π.χ. το μέσο του ματιού, και στη συνέχεια η εικόνα του προσώπου περιστρέφεται δεξιόστροφα ή αριστερόστροφα, μέχρι να ισιώσει κατά μήκος ενός οριζόντιου άξονα. Τέλος, αν είναι απαραίτητο, το πρόσωπο μεγεθύνεται, ώστε να καταλάβει έναν ελάχιστο δυνατό χώρο από pixels.

**Διακριτά χαρακτηριστικά**

Αφού ολοκληρωθεί η παραμετροποίηση της εικόνας, ξεκινάει η διαδικασία επεξεργασίας των διακριτών χαρακτηριστικών. Αυτό που έχει ενδιαφέρον είναι ότι όλα τα συστήματα προσπαθούν να ταιριάξουν ορατά χαρακτηριστικά του προσώπου, με έναν τρόπο παρόμοιο με αυτόν που χρησιμοποιούν τα άτομα για να αναγνωρίζονται μεταξύ τους. Τα χαρακτηριστικά που επιλέγονται, είναι εκείνα που αλλάζουν λιγότερο με το χρόνο. Συνήθως εξετάζονται οι κόγχες του ματιού, η περιοχή γύρω από τα ζυγωματικά, οι άκρες του στόματος, το σχήμα της μύτης και η σχετική θέση των διαφόρων χαρακτηριστικών μεταξύ τους. Απεναντίας, αποφεύγονται περιοχές του προσώπου που είναι πιθανό να αλλάξουν ή να κρυφτούν, όπως το σημείο του μετώπου απ' όπου ξεκινούν να φυτρώνουν μαλλιά.

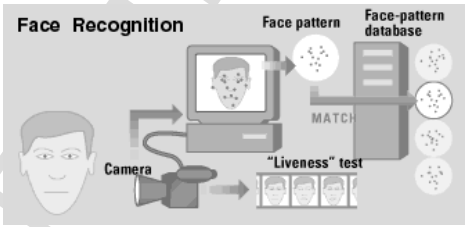
Μια από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει η τεχνολογία σκαναρίσματος προσώπου, είναι ότι το πρόσωπο αποτελεί πεδίο πολύ μεγάλων αλλαγών. Ακόμα και μια δραματική αλλαγή στην έκφραση, μπορεί να αποτελέσει αιτία απόρριψης κάποιου από το σύστημα. Δηλαδή, ένας χρήστης που ενώ γελάει στην εικόνα εγγραφής, κάνει μια

[1] Raffaele Cappelli, Dario Maio, and Davide Maltoni, "Subspace Classification for Face Recognition".

γκριμάτσα την ώρα της πιστοποίησης, έχει αυξημένη πιθανότητα να μην αναγνωριστεί. Αλλά και αλλαγές στον τρόπο χτενίσματος και το μακιγιάζ, η απόκτηση γενειάδας, η προσθήκη ή αφαίρεση γυαλιών, είναι συμπεριφορές που επηρεάζουν την ικανότητα του συστήματος να εντοπίζει διακριτά χαρακτηριστικά. Σε αντίθεση με τον ανθρώπινο νου, που βλέπει πέρα από αυτά τα σημεία, τα όρια των συστημάτων – προς το παρόν τουλάχιστον – είναι πεπερασμένα.

**Ταίριασμα templates**

Για το ταίριασμα των αρχείων templates, το κάθε προϊόν χρησιμοποιεί μια ξεχωριστή μέθοδο. Κοινό σημείο είναι ότι σε κάθε σύγκριση, ανατίθεται ένα ποσοστό εμπιστοσύνης, που όταν ξεπερνά ένα προκαθορισμένο επίπεδο, τότε το ταίριασμα θεωρείται επιτυχές. Σε πολλές περιπτώσεις, το σύστημα αποκτά από την αρχή μια σειρά από εικόνες του χρήστη, τις οποίες συγκρίνει με τα δεδομένα της εγγραφής. Δηλαδή, σε αντίθεση με τα συστήματα των υπολοίπων βιομετρικών τεχνολογιών, που λαμβάνουν ένα δείγμα για πιστοποίηση, και μόνο σε περίπτωση αποτυχίας ζητούν και δεύτερο, τα συστήματα πιστοποίησης 1:1 με σκανάρισμα προσώπου, μπορούν να διενεργούν παράλληλα πολλαπλές συγκρίσεις, και μάλιστα μέσα σε ελάχιστα δευτερόλεπτα. Έτσι, δεν τίθεται τόσο θέμα αποτυχίας μετά από ένα συγκεκριμένο αριθμό αποτυχημένων προσπαθειών, όσο μετά από ένα ορισμένο χρονικό διάστημα[1].




**Σχήμα 9.** Η διαδικασία αναγνώρισης προσώπου

Στα μεγάλα συστήματα αναγνώρισης, μια ιδιαιτερότητα που υπάρχει είναι ότι ο βιομετρικός έλεγχος του προσώπου συνήθως επιστρέφει περισσότερα του ενός ταιριάσματα. Αυτό συμβαίνει, γιατί το σκανάρισμα του προσώπου δεν είναι εξίσου αποτελεσματική βιομετρική τεχνολογία, στην αναγνώριση ατόμων από μια μεγάλη βάση

[1] O. Déniz, M. Castrillón, J. Lorenzo, and M. Hernández, "An Incremental Learning Algorithm for Face Recognition".

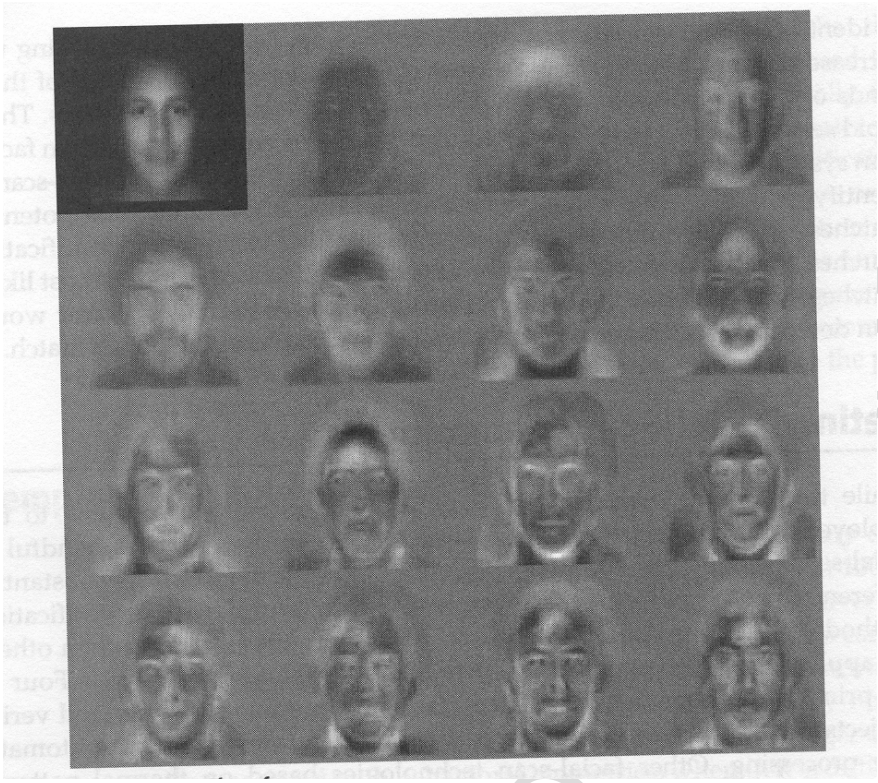
δεδομένων, όσο άλλες. Έτσι, είναι πιθανό το σύστημα να είναι διαμορφωμένο, ώστε από μια βάση δεδομένων με 10.000 εγγεγραμμένα άτομα, να επιστρέφονται τα 10 πιο πιθανά. Από κει και πέρα, χρειάζεται η ανθρώπινη συνδρομή και παρέμβαση, που θα καθορίσει το τελικό αποτέλεσμα.

### 2.2.3 Κυρίαρχες τεχνολογίες

Αυτή τη στιγμή, υπάρχουν πολλές τεχνολογίες σκαναρίσματος προσώπου, που συναγωνίζονται μεταξύ τους. Οι τεχνολογίες αυτές διαφέρουν μεταξύ τους, ως προς τις μεθόδους που χρησιμοποιούν και τις εφαρμογές στις οποίες αποδίδουν καλύτερα. Οι πιο διαδεδομένες είναι η Eigenface, η ανάλυση χαρακτηριστικών, τα νευρωνικά δίκτυα και η αυτόματη επεξεργασία προσώπου, τις οποίες θα αναπτύξουμε παρακάτω. Άλλες μέθοδοι, που βασίζονται σε θερμικές περιοχές που σχηματίζονται κάτω από το δέρμα, δεν έχουν τύχει μέχρι στιγμής ευρύτερης εμπορικής αποδοχής.

**Eigenface**

Η τεχνολογία Eigenface αναπτύχθηκε από το MIT. Χρησιμοποιεί μια βάση δεδομένων από δισδιάστατες, γκριζόχρωμες εικόνες προσώπου, τα λεγόμενα Eigenfaces, από τα οποία παράγονται τα templates, κατά τη διαδικασία πιστοποίησης ή εγγραφής. Το κάθε Eigenface αναπαριστά συγκεκριμένα διακριτά χαρακτηριστικά του προσώπου και κάθε πρόσωπο μπορεί να ανασυντεθεί από τη συνένωση περίπου 100 με 125 Eigenfaces. Η ιδέα των Eigenfaces με κάποιες παραλλαγές, αποτελεί τη βάση ανάπτυξης και άλλων μεθόδων σκαναρίσματος προσώπου.



**Σχήμα 10.** Eigenfaces

Κατά τη διάρκεια της εγγραφής, η εικόνα του προσώπου αναπαρίσταται σαν ένας συνδυασμός από Eigenfaces. Αυτή η αναπαράσταση εκφράζεται στη συνέχεια με αριθμητικούς όρους. Κάθε φορά που υπάρχει ανάγκη πιστοποίησης, το παραγόμενο template συγκρίνεται με το αποθηκευμένο template και εφόσον πληρείται ο ελάχιστος βαθμός συσχέτισης μεταξύ των δύο, το ταίριασμα θεωρείται επιτυχές. Η ίδια αρχή ισχύει και στην περίπτωση αναγνώρισης, με τη διαφορά ότι το πλήθος των συγκρίσεων είναι πολύ μεγαλύτερο. Όπως και οι άλλες τεχνολογίες σκαναρίσματος προσώπου, η τεχνολογία Eigenface αποδίδει καλύτερα, όταν η εικόνα του προσώπου είναι μετωπιαία και γίνεται σε καλές συνθήκες φωτισμού.

**Ανάλυση χαρακτηριστικών**

Η ανάλυση χαρακτηριστικών είναι ίσως η πιο διαδεδομένη τεχνολογία σκαναρίσματος προσώπου. Σχετίζεται με την τεχνολογία Eigenface[1], αλλά επιτρέπει μεγαλύτερες αλλαγές στην εμφάνιση και την έκφραση, π.χ. πρόσωπο χαμογελαστό και πρόσωπο

[1] Sarat C. Dass and A. K. Jain, "Markov Face Models", The Eighth IEEE International Conference on Computer Vision (ICCV), pp. 680-687, Vancouver, Canada, July 9-12, 2001.

στενοχωρημένο. Η μέθοδος αυτή, έχει τη φιλοσοφία ότι αλιεύει χαρακτηριστικά από όλη την επιφάνεια του προσώπου και επιπλέον σημειώνει τη σχετική θέση μεταξύ τους. Βασίζεται στην υπόθεση ότι η παραμικρή κίνηση ενός χαρακτηριστικού, θα συνοδευτεί από παρόμοια κίνηση των εφαπτόμενων χαρακτηριστικών. Για ανάλυση με τη συγκεκριμένη τεχνολογία, θεωρείται ιδανική η μετωπιαία απεικόνιση του προσώπου από απόσταση ενός μέτρου, αλλά επεξεργάσιμες είναι όλες οι εικόνες που απέχουν έως 25 μοίρες από την οριζόντια θέση και 15 από την κατακόρυφη. Να σημειωθεί ότι η Visionics, μια ιδιαίτερα ελπιδοφόρα εταιρεία αναγνώρισης προσώπου, έχει αναπτύξει μια μέθοδο τοπικής ανάλυσης χαρακτηριστικών (Local Feature Analysis, LFA), η οποία συνίσταται στη μείωση των χαρακτηριστικών του προσώπου σε ένα ελάχιστο σύνολο από προσδιοριστικά χαρακτηριστικά, που δεν μπορεί να μειωθεί περαιτέρω.

**Νευρωνικά δίκτυα**

Τα νευρωνικά δίκτυα προσπαθούν με τη χρήση αλγορίθμου να καθορίσουν, αν υπάρχει ταύτιση του φερόμενου ως χρήστη και του πραγματικού χρήστη, ως προς καθολικά χαρακτηριστικά του προσώπου του, που θεωρούνται μοναδικά. Το ιδιαίτερα ενδιαφέρον είναι ότι τα νευρωνικά δίκτυα μαθαίνουν ποια χαρακτηριστικά είναι πιο αποτελεσματικά για σύγκριση, σε σχέση με τους συγκεκριμένους χρήστες που υπάρχουν κάθε φορά στη βάση αναφοράς. Αυτό γίνεται ως εξής: για κάθε χαρακτηριστικό που εξετάζεται, αποφασίζεται αν υπάρχει ταίριασμα. Λάθος απόφαση για ταίριασμα, ωθεί τον αλγόριθμο να μεταβάλλει το βάρος που δίνει σε κάποια χαρακτηριστικά του προσώπου, δηλαδή ο αλγόριθμος προσαρμόζεται στις μεθόδους που αποδεικνύονται πιο αποτελεσματικές. Συνεπώς μακροπρόθεσμα, υπάρχουν μεγαλύτερες πιθανότητες αναγνώρισης κάτω από δύσκολες συνθήκες με τα νευρωνικά δίκτυα.

Σήμερα, υπάρχουν τεχνολογίες σκαναρίσματος προσώπου, που βασίζονται σε πιο εξελιγμένα νευρωνικά μοντέλα, ικανά να ενσωματώσουν χιλιάδες εικόνες προσώπου. Υπάρχει η ελπίδα, ότι αυτά τα εξελιγμένα μοντέλα θα μπορέσουν να επιλύσουν αρκετές αδυναμίες των συστημάτων σκαναρίσματος προσώπου, χάρη στην ικανότητά τους για μάθηση. Προς το παρόν όμως, ο μεγάλος χρόνος εγγραφής που απαιτούν, τα καθιστά λιγότερο κατάλληλα για εφαρμογές παρακολούθησης π.χ., όπου ένα άτομο αντιστοιχίζεται σε με μια λίστα υπόπτων. Άλλωστε, αυτές οι λίστες συνήθως παράγονται

από στατικές εικόνες, οι οποίες δεν είναι τόσο κατάλληλες για εγγραφή σε νευρωνικά δίκτυα.

**Αυτόματη επεξεργασία προσώπου**

Η αυτόματη επεξεργασία προσώπου (Automatic Face Process, AFP) είναι μια σχετικά υποτυπώδης τεχνολογία, που βασίζεται σε αποστάσεις και αναλογίες αποστάσεων, μεταξύ χαρακτηριστικών τα οποία είναι εύκολο να προσδιοριστούν, όπως τα μάτια, η μύτη, οι γωνίες του στόματος κτλ.[1] Αν και συνολικά είναι μια τεχνολογία λιγότερο εύρωστη απ' ότι οι τρεις προηγούμενες, έχει το πλεονέκτημα ότι είναι περισσότερο αποτελεσματική σε συνθήκες κακού φωτισμού, γεγονός που καθιστά τη χρήση της επιθυμητή σε ορισμένες εφαρμογές.

### 2.2.4 Εφαρμογές

Συνήθως, η τεχνολογία σκαναρίσματος προσώπου χρησιμοποιείται, είτε σε περιβάλλοντα, τα οποία διαθέτουν τις απαραίτητες εικόνες προσώπου ή σε περιβάλλοντα, τα οποία έχουν την απαραίτητη υλικοτεχνική υποδομή για να τις αποκτήσουν. Μερικές από τις πιο συνηθισμένες εφαρμογές της συγκεκριμένης τεχνολογίας απαντώνται σε συστήματα αναγνώρισης δημοσίου συμφέροντος, συστήματα παρακολούθησης, συστήματα κρατήσεων, επίβλεψη σε χώρους ασφαλείας, είσοδος σε καταστήματα, ανεύρεση υπόπτων, ηλεκτρονικό εμπόριο, εκπαίδευση καθώς και αναγνώριση εκφράσεων προσώπων για επικοινωνία ανθρώπων μηχανης. Κάποιες ενδιαφέρουσες χρήσεις αναφέρονται επιλεκτικά στις επόμενες παραγράφους.

**ΕΞΩΤΕΡΙΚΟ:**

**ΑΓΓΛΙΑ**

**1) Εφαρμογές σκαναρίσματος προσώπου από την Αστυνομία για ασφάλεια χώρων**

Στο Newham της Αγγλίας, 114 κάμερες CCTV της Αστυνομίας καταγράφουν επί 24ώρου βάσεως οποιαδήποτε δραστηριότητα, στους δρόμους μιας γειτονιάς, που θεωρείται επικίνδυνη. Το χρησιμοποιούμενο σύστημα παρακολούθησης διαθέτει λογισμικό σκαναρίσματος προσώπου της Visionics, με βάση το οποίο συγκρίνει τα πρόσωπα που

[1] Sarat C. Dass and A. K. Jain, "Markov Face Models", The Eighth IEEE International Conference on Computer Vision (ICCV), pp. 680-687, Vancouver, Canada, July 9-12, 2001

αποκτώνται από τις κάμερες, με μια λίστα σεσημασμένων κακοποιών. Έτσι, επιτελείται ο σκοπός της πρόληψης και αποτροπής του εγκλήματος, γεγονός που πιστοποιείται και από τη μείωση στα ποσοστά των επιθέσεων, από 39% σε 21%[1].

**ΜΕΞΙΚΟ**

**2) Εφαρμογή σκαναρίσματος του προσώπου για καταγραφή ψηφοφόρων**

Στις προεδρικές εκλογές του 2000, η μεξικανική κυβέρνηση που απασχολούνται λογισμικό αναγνώρισης προσώπου για την πρόληψη της απάτης ψηφοφόρων. Μερικά άτομα είχαν την εγγραφή του εκλέγειν σύμφωνα με αρκετά διαφορετικά ονόματα, σε μια προσπάθεια να τοποθετήσετε πολλαπλές ψήφους[2]. Με τη σύγκριση νέες εικόνες προσώπου σε εκείνους που έχουν ήδη στη βάση δεδομένων των ψηφοφόρων, οι αρχές ήταν σε θέση να μειώσει διπλές εγγραφές. Ανάλογες τεχνολογίες που χρησιμοποιούνται στις Ηνωμένες Πολιτείες για να αποτρέψει τους ανθρώπους από τη λήψη πλαστά δελτία ταυτότητας και άδειες οδήγησης.

Υπάρχουν επίσης μια σειρά από πιθανές χρήσεις για την αναγνώριση του προσώπου που είναι σε εξέλιξη. Για παράδειγμα, η τεχνολογία θα μπορούσε να χρησιμοποιηθεί ως μέτρο ασφάλειας σε ATM αντί να χρησιμοποιείται μια τραπεζική κάρτα ή ο προσωπικός αριθμός αναγνώρισης, τα ATM τραβάν μια φωτογραφία του προσώπου και συγκρίνουν με τη φωτογραφία του πελάτη στη βάση δεδομένων, για να επιβεβαιώσουν την ταυτότητά . Αυτό το ίδιο θα μπορούσε επίσης να εφαρμοστεί και στους υπολογιστές, με τη χρήση μιας web κάμερα για να συλλάβει μια ψηφιακή εικόνα του εαυτού σας, το πρόσωπό σας θα μπορούσε να αντικαταστήσει τον κωδικό πρόσβασής σας ως μέσο για την log-in.

Επίσης, πέραν των βιομετρικών χρήσεις, σύγχρονες ψηφιακές φωτογραφικές μηχανές ενσωματώνουν συχνά τεχνολογία ανίχνευσης προσώπου, σύστημα που επιτρέπει στην κάμερα να εστιάσει και να μετράται η έκθεση στο πρόσωπο του θέματος, εξασφαλίζοντας έτσι μια εστιασμένη πορτρέτο του προσώπου που φωτογραφίζεται.

[1] http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-1000480/

**Η.Π.Α. (διάφορες πολιτείες)**

**3) Εφαρμογές σκαναρίσματος προσώπου για ασφάλεια σε καζίνο , άδεια οδήγησης, δικαιοσύνη, ασφάλεια και FACEBOOK…**

**ΑΤΛΑΝΤΙΚ ΣΙΤΥ, ΝΙΟΥ ΤΖΕΡΣΙ, ΛΑΣ ΒΕΓΚΑΣ**

Ακόμη, η αμερικάνικη εταιρεία που ασχολείται με βιομετρικές εφαρμογές Biometrica έχει εγκαταστήσει συστήματα σκαναρίσματος προσώπου με λογισμικό σε 70 καζίνο κατά μήκος της γης, μεταξύ των οποίων και το Foxwoods Casino στο Κονέκτικατ, το Trump Marina, το Taj Mahal, το Plaja στο Ατλάντικ Σίτυ και το Νιου Τζέρσεϋ, το Stratosphere Hotel and Casino και το Mirage Resort στο Λας Βέγκας και τη Νεβάδα. Μάλιστα, έχει στην κατοχή της μια βάση δεδομένων με άτομα επικίνδυνα για την ασφάλεια των καζίνο, της οποίας επωφελούνται τα καζίνο με τα οποία συνεργάζεται και οι αντίστοιχες υπηρεσίες επιβολής του νόμου[1].

**ΙΛΙΝΟΙΣ**

Τέλος, η πολιτεία του Ιλινόις έθεσε πρόσφατα σε εφαρμογή ένα σύστημα σκαναρίσματος προσώπου, για τη χορήγηση άδειας οδήγησης στους πολίτες. Το σύστημα αυτό, που απευθύνεται σε 25 εκατομμύρια κατοίκους, διεξάγει έλεγχο 1:N με βάση τους εγγεγραμμένους χρήστες, δηλαδή τους κατόχους άδειας οδήγησης, κι έτσι καθιστά αδύνατη την έκδοση δύο αδειών οδήγησης για το ίδιο άτομο[2].

**ΠΕΝΣΥΛΒΑΝΙΑ**

Αναζητήσεις φωτογραφιών από την σκηνή του εγκλήματος και βίντεο CCTV προβαίνει η Αστυνομία της Πενσυλβάνια, μελετώντας βάση δεδομένων προηγούμενων συλλήψεων. Ένας αριθμός παγωμένων υποθέσεων έχουν επιλυθεί από το σύστημα που άρχισε να λειτουργεί το 2005[3].

[1] http://www.angelfire.com/nt/selcukgun/en/tran_2.htm

[2] A. K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance", IEICE Trans. Fundamentals, Vol. E84-D, No. 7, pp. 788-799, 2001.

[3] http://www.channelinsider.com/c/a/Security/Are-Enterprises-Ready-for-Biometrics-as-a-Security-Solution

**ΚΟΝΕΚΤΙΚΑΤ**

Το *Facebook* έχει παρουσιάσει στο κοινό του εδώ και αρκετό καιρό μια τεχνολογία αναγνώρισης προσώπου για φωτογραφίες. Η ανάπτυξη της αναγνώρισης προσώπου σχεδιάστηκε για να επιταχύνει τη διαδικασία επισήμανσης φωτογραφιών, ωστόσο δημιούργησε ανησυχίες σχετικά με την καταπάτηση της ιδιωτικής ζωής των χρηστών. Η τεχνολογία λειτουργεί ως εξής: σαρώνει τις φωτογραφίες που ανεβάσατε πρόσφατα, συγκρίνει τα πρόσωπα με προηγούμενες φωτογραφίες και στη συνέχεια προσπαθεί να αντιστοιχίσει τα πρόσωπα προτείνοντας ονόματα από τους φίλους σας. Όταν βρεθεί μια αντιστοιχία, το Facebook ειδοποιεί το χρήστη για να επικυρώσει το άτομο που εμφανίζεται στη φωτογραφία.

Ο Γενικός Εισαγγελέας του Κονέκτικατ, George Jepsen, ανέφερε σε επιστολή του προς το Facebook ότι με αυτήν την υπηρεσία καταπατώνται τα δικαιώματα των καταναλωτών για την προστασία της ιδιωτικής τους ζωής. Οι άνθρωποι του Facebook ήρθαν σε επαφή με τον Jespen για να βρεθεί μια λύση. Για αυτόν τον λόγο, από τις αρχές Ιουλίου 2011 «τρέχουν» διαφημίσεις στο Facebook επεξηγώντας στους χρήστες πως να μπλοκάρουν τη χρήση της λειτουργίας αυτής παντελώς.

Μετά την τροποποίηση του συστήματος, ο Jespen ανέφερε σε ανακοίνωσή του, «Το Facebook έχει κάνει σημαντικές αλλαγές που θα παρέχει καλύτερες υπηρεσίες και μεγαλύτερη προστασία της ιδιωτικής ζωής των χρηστών του, όχι μόνο στο Κονέκτικατ, αλλά σε ολόκληρη τη χώρα»[1].

**ΦΛΟΡΙΝΤΑ**

Στο Super Bowl τον Ιανουάριο του 2001, η αστυνομία της Tampa Bay, Florida χρησιμοποιείται Viisage λογισμικό αναγνώρισης προσώπου για την αναζήτηση πιθανών εγκληματιών και τρομοκρατών που συμμετείχαν στην τρομοκρατική επίθεση στις 11/09/2001.

---

[1] http://www.findbiometrics.com/Pages/iris_retinal.html

**ΚΥΒΕΡΝΗΣΗ Η.Π.Α.**

Όταν οι Ταλιμπάν έσκαψαν ένα σύστημα σηράγγων κάτω από την μεγαλύτερη φυλακή του νότιου Αφγανιστάν την περασμένη άνοιξη, άρχισαν και την μεγαλύτερη επιχείρηση εντοπισμού 475 κρατούμενων που είχαν αποδράσει. Αυτό που διευκόλυνε την κατάσταση ήταν το γεγονός ότι ένα μήνα πριν από την απόδραση, Αφγανοί αξιωματούχοι, χρησιμοποιώντας την τεχνολογία των ΗΠΑ, είχαν κάνει σάρωση οφθαλμών, δακτυλικών αποτυπωμάτων και χαρακτηριστικών προσώπου των κρατούμενων των φυλακών Σαρπόζα. Μέσα σε λίγες μέρες από την απόδραση, είχαν καταφέρει να εντοπίσουν και να επαναπροωθήσουν στις φυλακές 35 εξ' αυτών. Οι συλλήψεις τους έγιναν σε συνοριακά περάσματα και σημεία ελέγχου εντός της χώρας. Τα στοιχεία του επιβεβαιώθηκαν από τους φακέλους τους με τα βιομετρικά τεστ από τα οποία είχαν περάσει[1].

Με απόφαση «της τελευταίας στιγμής» η Αμερική έχει βαλθεί να καταγράψει, με το νέο βιομετρικό τρόπο, τα στοιχεία μεγάλου αριθμού ανθρώπων σε Αφγανιστάν και Ιράκ και κυρίως άνδρες σε ηλικία στράτευσης. Η Αμερική, το ΝΑΤΟ με και οι τοπικές αρχές του Αφγανιστάν έχουν ήδη «φακελώσει» 1.5 εκατ. πολίτες της χώρας. Αναλογικά, ο αριθμός ισούται με 1 στους 6 άνδρες μάχιμης ηλικίας από 15 έως 64 ετών. Στο Ιράκ, η καταγραφή πάει ακόμα καλύτερα με 2.2 εκατ. πολιτών να βρίσκονται «στη διάθεση» όποιου χρειαστεί ή αναζητήσει τα στοιχεία τους.

Η καταγραφή δεν αφορά μόνον κρατούμενους φυλακών ή στρατιώτες, αλλά και απλούς πολίτες οι οποίοι είτε αναζητούν εργασία σε κρατικές ή αμερικανικές υπηρεσίες και κυβερνητικά κτίρια είτε επιθυμούν να βγάλουν διαβατήριο ή να χρησιμοποιήσουν τις κρατικές παροχές των υπηρεσιών τους. Η βασική διαφορά από την απλή καταγραφή αποτυπωμάτων έγκειται στο ότι με το νέο βιομετρικό τρόπο μπορούν να καταγραφούν εκατομμύρια αρχεία εντός δευτερολέπτων ακόμα και σε απομακρυσμένες ή δύσβατες περιοχές. Παρόλο που το σύστημα βοηθάει ιδιαίτερα τις αρχές, υπάρχει έντονη διαφωνία από φωνές πολιτικών και νομικών κύκλων που δεν θα ήθελαν να δουν κάτι παρόμοιο να

[1]http://www.nesbary.com/class/621/articles

συμβαίνει στις ΗΠΑ. Βέβαια, με το σκεπτικό ότι τα βιομετρικά τεστ βοηθούν στην καταπολέμηση κάθε είδους απάτης και διαφθοράς, η χρήση τους αυξάνεται ολοένα και περισσότερο παρά τις όποιες αντιρρήσεις. Το υπουργείο Άμυνας των ΗΠΑ στην οκταετία 2007-2015 έχει υπολογισθεί πως θα διαθέσει σχεδόν 2.5 δις ευρώ.

**ΓΕΡΜΑΝΙΑ**

**3) Εφαρμογές σκαναρίσματος προσώπου για ασφάλεια πολιτών και αεροδρομίων**

Η γερμανική ομοσπονδιακή αστυνομία χρησιμοποιούν ένα σύστημα αναγνώρισης προσώπου για πλήρως αυτοματοποιημένους συνοριακούς έλεγχους σε Frankfurt Rhein-Main (διεθνές αεροδρόμιο)[1].

**ΑΥΣΤΡΑΛΙΑ**

**4) Εφαρμογές σκαναρίσματος προσώπου για τελωνεία και ασφάλεια συνόρων**

Η τελωνειακή υπηρεσία της Αυστραλίας έχει ένα αυτοματοποιημένο σύστημα επεξεργασίας των συνόρων που ονομάζεται SmartGate που χρησιμοποιεί την αναγνώριση του προσώπου. Το σύστημα συγκρίνει το πρόσωπο του ατόμου με την εικόνα στο e-διαβατήριο πιστοποιεί μικροτσίπ, ότι ο κάτοχος του διαβατηρίου είναι ο νόμιμος ιδιοκτήτης[2].

**ΒΡΑΖΙΛΙΑ**

**5) Εφαρμογές σκαναρίσματος προσώπου για Αστυνομία**

Οι Βραζιλιάνοι αστυνομικοί θα εφοδιαστούν με γυαλιά, τα οποία θα μπορούν να σκανάρουν πρόσωπα και να αναγνωρίσουν αν πρόκειται για άτομα που έχουν εμπλακεί σε εγκληματικές ενέργειες. Τα γυαλιά, που διαθέτουν προηγμένη τεχνολογία αναγνώρισης προσώπου, έχουν τη δυνατότητα να σκανάρουν έως και 400 πρόσωπα το δευτερόλεπτο σε απόσταση έως και 45 μέτρα. Έχουν τη δυνατότητα να σαρώσουν έως και 46.000 βιομετρικά στοιχεία σε ένα πρόσωπο και να τα συγκρίνουν με αυτά που

[1] http://www.channelinsider.com/c/a/Security/Are-Enterprises-Ready-for-Biometrics-as-a-Security-Solution

[2] Gail R. Light, "Security vs. Liberty: weighing the options", MSU Today, June 20, 2002.

βρίσκονται σε μία βάση δεδομένων με εγκληματίες. Όταν βρίσκουν κάποιον που βρίσκεται στη βάση, ένα κόκκινο φως κάνει την εμφάνισή του και ειδοποιεί τον αστυνομικό ότι έχει εντοπίσει κάποιον ύποπτο. Τα γυαλιά αυτά αναμένεται να είναι χρήσιμα σε μέρη όπου υπάρχει μεγάλη συγκέντρωση πλήθους, ενώ αναμένεται να αξιοποιηθούν και κατά τη διάρκεια του Παγκοσμίου Κυπέλλου Ποδοσφαίρου το 2014, που διοργανώνεται από το Ρίο Ντε Τζανέιρο, για την αποφυγή εγκληματικών πράξεων[1].

**ΡΩΣΙΑ**

**6) Εφαρμογές σκαναρίσματος προσώπου για Τραπεζικές συναλλαγές**

Η ρωσική κρατική τράπεζα Sberbank σχεδιάζει να θέσει σε λειτουργία τα νέα ATM της, που θα είναι τόσο, μα τόσο ασφαλή, ώστε να δίνουν ακόμη και τη δυνατότητα στους χρήστες τους να βγάζουν μια νέα πιστωτική κάρτα, χωρίς καν να έχουν επαφή με κάποιον άνθρωπο υπάλληλο. Όλα θα είναι αυτόματα, και θα διεκπεραιώνονται με το πάτημα μερικών μόνο κουμπιών.

Τα μηχανήματα θα έχουν τη δυνατότητα να αναγνωρίζουν δακτυλικά αποτυπώματα, να σκανάρουν διαβατήρια, και να φωτογραφίζουν το πρόσωπο του πελάτη … τρισδιάστατα[2]!

Θα έχουν επίσης δυνατότητες αναγνώρισης της φωνής, με τεχνολογία εντοπισμού τυχόν ψεμάτων, έτσι ώστε αν κάποιος χρήστης απαντήσει ψευδώς, το μηχάνημα να το αντιλαμβάνεται!

Η τεχνολογία αυτή αναπτύχθηκε από μια εταιρία η οποία συνεργάζεται και με την Ομοσπονδιακή Υπηρεσία Ασφάλειας, που είναι η διάδοχος της πάλαι ποτέ πανίσχυρης σοβιετικής KGB.

Οι προγραμματιστές της εν λόγω εταιρίας εκμεταλλεύτηκαν ηχογραφήσεις των ρωσικών υπηρεσιών ασφάλειας από ανθρώπους που ψεύδονταν, έτσι ώστε να δημιουργήσουν

[1] "Coming Soon: ATMs That Recognize Your Eyes", The Christian Science Monitor, 2 December 1997.

[2] "Coming Soon: ATMs That Recognize Your Eyes", The Christian Science Monitor, 2 December 1997.

τεχνικές ανάλυσης, οι οποίες ανιχνεύουν την ανθρώπινη φωνή, προκειμένου να εντοπίσουν σημάδια νευρικότητας και άγχους, δηλαδή ενδείξεις ψεύδους.

Ως ιδέα, τα μηχανήματα αυτά μπορεί να ακούγονται ενοχλητικά στους Δυτικούς, αλλά η Sberbank επενδύει σε αυτά, και δεν θεωρεί πως οι πελάτες της θα δυσαρεστηθούν ιδιαίτερα. «Απλά προσπαθούμε να βρούμε τρόπους για να ξέρουμε αν ο πελάτης μας λέει την αλήθεια… δεν υπάρχει λόγος ανησυχίας», λένε οι υπεύθυνοι της τράπεζας.

**ΕΛΛΑΔΑ**

**1) Εφαρμογές σκαναρίσματος προσώπου για Τραπεζικές συναλλαγές**

Ένα νέο αμφιλεγόμενο ηλεκτρονικό σύστημα καταγραφής του προσώπου των πελατών της, το οποίο τοποθετούν πολλές Ελληνικές Τράπεζες στις εισόδους των καταστημάτων τους, προκαλεί έντονες αντιδράσεις και απασχολεί την Αρχή Προστασίας Προσωπικών Δεδομένων.

Πολίτες που συναλλάσσονται με Τράπεζες καταγγέλλουν ότι, για να μπουν πλέον σε αρκετά καταστήματά της, περνούν πρώτα από ένα ειδικό κουβούκλιο, το οποίο τους εγκλωβίζει προσωρινά και δεν τους επιτρέπει την είσοδο στην τράπεζα, εάν δεν γυρίσουν το κεφάλι τους σε μια κάμερα που βρίσκεται από πάνω τους! Η κάμερα πρώτα τούς «φωτογραφίζει» και μετά δίνει εντολή να ανοίξει η πόρτα εισόδου στο υποκατάστημα της τράπεζας. Είναι προφανές ότι η πόρτα δεν ανοίγει εάν οι πελάτες φοράνε σκούρα γυαλιά ηλίου, καπέλο ή κρύβουν με κάποιο τρόπο το πρόσωπό τους. Η ενέργεια αυτή γίνεται απλώς για αποτροπή επίδοξων ληστών, οι οποίοι δεν μπορούν να εισέλθουν πλέον στις τράπεζες αυτές εάν φορούν κουκούλα ή κράνος.

Το μείζον πρόβλημα, όμως, της αρχειοθέτησης υλικού χωρίς την άδεια του υποκειμένου επεξεργασίας παραμένει. Γιατί μπορεί τα ηλεκτρονικά συστήματα της τράπεζας να μην είναι σε θέση να «ταυτοποιήσουν» το πρόσωπο που φωτογραφίζουν (αφού δεν γνωρίζουν το όνομά του), ωστόσο καταγράφουν και πιθανότατα αρχειοθετούν τις φωτογραφίες για κάθε ενδεχόμενο.

Επομένως, δύσκολα θα πιστέψει κανείς ότι τα συστήματα της τράπεζας απλώς καταγράφουν στιγμιαία το πρόσωπο του πελάτη, καθαρά για λόγους αποτροπής.

Κατόπιν καταγγελιών πολιτών, η Αρχή πραγματοποίησε ελέγχους σε ορισμένα υποκαταστήματα της ΕΤΕ και διαπίστωσε ότι το νέο σύστημα εισόδου - εξόδου πελατών αποτελείται από: 1) Μια ειδική καμπίνα ασφαλείας, με δύο θύρες, για την είσοδο στο κατάστημα. 2) Μια έγχρωμη κάμερα, που έχει τοποθετηθεί στην καμπίνα ασφαλείας εισόδου. Στο σημείο που έχει τοποθετηθεί η κάμερα υπάρχει μία κόκκινη φωτεινή ένδειξη, ώστε να υποδεικνύεται στους εισερχόμενους η κατεύθυνση προς την οποία πρέπει να κοιτούν. Στην καμπίνα υπάρχει εγκατεστημένο και ένα μεγάφωνο για την παροχή ηχητικών οδηγιών προς τους εισερχόμενους. 3) Έναν τυπικό ηλεκτρονικό υπολογιστή με κατάλληλο υλικό και λογισμικό για τον έλεγχο των θυρών ασφαλείας, την επόπτευση του σήματος εικόνας (βίντεο) από την κάμερα και την επεξεργασία των εικόνων που λαμβάνονται από την κάμερα.

Η διαδικασία για να εισέλθει κάποιος στο κατάστημα της Τράπεζας έχει ως εξής, σύμφωνα με την απόφαση της Αρχής: Το κοινό εισέρχεται στην καμπίνα ασφαλείας μόνο όταν αυτή είναι ελεύθερη (δεν βρίσκεται άλλο πρόσωπο στο εσωτερικό της και οι δύο θύρες είναι κλειστές), γεγονός που υποδεικνύεται από την πράσινη ένδειξη στο λαμπάκι εισόδου. Με την είσοδο στο εσωτερικό της καμπίνας και με τις προϋποθέσεις ότι α) έχει κλείσει η θύρα και β) το πρόσωπο στέκεται στο κέντρο της καμπίνας και κοιτάζει προς την κατεύθυνση της κάμερας, λαμβάνεται ψηφιακή φωτογραφία του. Για το σκοπό αυτό δίδονται και ηχητικές οδηγίες. Το λογισμικό του συστήματος επεξεργάζεται τη φωτογραφία (με τρόπο που θα αναλυθεί πιο κάτω) και αν το αποτέλεσμα αυτής της αυτοματοποιημένης επεξεργασίας είναι ότι η φωτογραφία που έχει ληφθεί είναι συμβατή με τα σχήματα χαρακτηριστικών προσώπου (δηλαδή ο άνθρωπος που βρίσκεται στην καμπίνα δεν φοράει κράνος, μάσκα, μαύρα γυαλιά, μαντίλια που να καλύπτουν το πρόσωπο κτλ), επιτρέπεται η είσοδος στην τράπεζα μέσω της δεύτερης πόρτας, γεγονός που επιβεβαιώνεται από έναν χαρακτηριστικό ήχο και από την πράσινη ένδειξη στο λαμπάκι εισόδου. Η επεξεργασία αυτή διαρκεί πολύ μικρό χρονικό διάστημα, της τάξης του ενός δευτερολέπτου.

Όπως αναφέρεται στην απόφαση της Αρχής, το σύστημα συλλέγει και αποθηκεύει δεδομένα εικόνας αλλά ουσιαστικά επεξεργάζεται βιομετρικά δεδομένα και συγκεκριμένα δεδομένα της γεωμετρίας του προσώπου. Αναλυτικότερα, το σύστημα εξάγει τα χαρακτηριστικά της γεωμετρίας του προσώπου, τα οποία συγκρίνονται με

πρότυπα χαρακτηριστικά, αποθηκευμένα στη βάση δεδομένων του. Τα δεδομένα αυτά, εντάσσονται στην κατηγορία των βιομετρικών, καθώς είναι αποτέλεσμα επεξεργασίας των χαρακτηριστικών του προσώπου. Εντούτοις, δεν πραγματοποιείται καμία περαιτέρω χρήση των βιομετρικών δεδομένων, ούτε είναι δυνατό σε κάποιον χρήστη του συστήματος να εξάγει εκ νέου αυτά τα χαρακτηριστικά για όλες τις αποθηκευμένες φωτογραφίες.

Η ενημέρωση που παρέχεται από την Τράπεζα προς τους εισερχόμενους πελάτες της δεν είναι πλήρης και απόλυτα σαφής. Τα υποκείμενα των δεδομένων, δεν ενημερώνονται για την ακριβή επεξεργασία που πραγματοποιείται (συλλογή και επεξεργασία εικόνων προσώπου, αυτοματοποιημένη επεξεργασία των χαρακτηριστικών του προσώπου), καθώς και για την ύπαρξη και την άσκηση του δικαιώματος πρόσβασης. Με τον τρόπο αυτό δημιουργείται η εσφαλμένη εντύπωση ότι η επεξεργασία που πραγματοποιείται είναι περισσότερο επεμβατική για την ιδιωτικότητά τους (π.χ. δημιουργείται σε πολλούς η εντύπωση ότι πραγματοποιείται βιομετρική ανάλυση της ίριδας του ματιού).

Η τράπεζα υποστηρίζει ότι η εν λόγω επεξεργασία είναι νόμιμη με βάση το άρθρο 5 παρ. 2 στοιχ. ε΄ του Ν. 2472/1997, καθώς από την έναρξη της πιλοτικής εφαρμογής του νέου συστήματος ασφαλείας, τους τελευταίους μήνες του 2008, έχει μειωθεί σημαντικά ο αριθμός των ληστειών στα καταστήματά της και δεν έχει σημειωθεί καμία ληστεία σε κατάστημα που έχει εγκατασταθεί το σύστημα. Σημειώνεται επίσης, ότι στα καταστήματα που σημειώθηκαν ληστείες και υπάρχει εγκατεστημένο απλό σύστημα βιντεοσκόπησης, από τις βιντεοκασέτες που παραδίδονται στις αστυνομικές αρχές δεν είναι δυνατή η αναγνώριση των δραστών, επειδή -κατά κανόνα- αυτοί έχουν καλυμμένα τα πρόσωπά τους.

Η Αρχή καταλήγει ότι «1) Επιφυλάσσεται να αποφανθεί οριστικά για τη νομιμότητα της επεξεργασίας, που διενεργείται με το νέο σύστημα εισόδου - εξόδου πελατών που έχει εγκαταστήσει η Εθνική Τράπεζα της Ελλάδος, μετά την πάροδο ενός έτους από την έκδοση της παρούσας απόφασης. Η τράπεζα έχει την υποχρέωση να προσκομίσει μετά την ετήσια εφαρμογή του νέου συστήματος συγκριτική μελέτη της αποτελεσματικότητάς του σε σχέση με τα προβλεπόμενα στη με αριθμ. 301/2009 απόφαση του Αναπληρωτή Υπουργού Εσωτερικών συστήματα ασφαλείας

2) Επιτρέπει δοκιμαστικά τη λειτουργία του συστήματος μόνο στα 152 καταστήματα της τράπεζας, στα οποία έχει ήδη το εν λόγω σύστημα εγκατασταθεί και υποχρεώνει την τράπεζα να κοινοποιήσει στην Αρχή κατάλογο των ανωτέρω 152 καταστημάτων εντός χρονικού διαστήματος δεκαπέντε ημερών από την κοινοποίηση της παρούσας απόφασης. Τα δεδομένα που συλλέγονται μέσω του συστήματος επιτρέπεται να τηρούνται για χρονικό διάστημα όχι μεγαλύτερο των είκοσι τεσσάρων ωρών από τη λήψη τους, με εξαίρεση την περίπτωση τέλεσης αξιόποινης πράξης

3) Υποχρεώνει την τράπεζα να προβεί σε πληρέστερη ενημέρωση των υποκειμένων των δεδομένων, σύμφωνα με τα διαλαμβανόμενα στο σκεπτικό της παρούσας.

4) Επιβάλλει στην Εθνική Τράπεζα της Ελλάδος ΑΕ πρόστιμο ύψους 30.000 ευρώ για την παράβαση του άρθρου 6 του Ν. 2472/1997».

### 2.2.5 Πλεονεκτήματα

Η τεχνολογία σκαναρίσματος προσώπου έχει πλεονεκτήματα που την κάνουν να ξεχωρίζει από τις υπόλοιπες βιομετρικές τεχνολογίες.

**Δυνατότητα εκμετάλλευσης του υπάρχοντος εξοπλισμού**

Σε αντίθεση με το βιομετρικό έλεγχο άλλων χαρακτηριστικών του ατόμου, το σκανάρισμα του προσώπου δεν απαιτεί την απόκτηση ξεχωριστού hardware ή την εκτενή αναπροσαρμογή του ήδη υπάρχοντος. Στις περισσότερες περιπτώσεις δηλαδή, η απόκτηση των εικόνων μπορεί να γίνει από κοινά συστήματα απεικόνισης, όπως οι κάμερες βιντεοσκόπησης. Σήμερα ειδικά, υπάρχουν πολλά σημεία, ιδίως μέσα στις πόλεις, όπου λειτουργούν κάμερες παρακολούθησης, κάμερες CCTV, καθώς και φωτογραφικά συστήματα. Αλλά και η επεξεργασία της εικόνας αποτελεί έναν αναπτυγμένο κλάδο με ιδιαίτερη άνθιση τα τελευταία χρόνια. Συνεπώς, υπάρχει η απαιτούμενη υλικοτεχνική και γνωσιολογική υποδομή, γεγονός που καθιστά την τεχνολογία σκαναρίσματος προσώπου ιδιαίτερα ελκυστική, τόσο από οικονομικής

άποψης (γιατί δεν υπάρχει ανάγκη εγκατάστασης νέου εξοπλισμού), όσο και από άποψης διευκόλυνσης (γιατί δεν υπάρχει ανάγκη εφαρμογής μιας νέας πολιτικής από τις επιχειρήσεις ή την κυβέρνηση).

**Δυνατότητα λειτουργίας χωρίς φυσική επαφή και συγκατάθεση του χρήστη**

Το σκανάρισμα του προσώπου είναι η μόνη βιομετρική λύση, που μπορεί να παρέχει αναγνώριση από απόσταση, και μάλιστα χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. Γι' αυτό άλλωστε χρησιμοποιείται ευρέως σε περιπτώσεις παρακολούθησης. Πολλά καζίνο έχουν ενσωματώσει συστήματα ελέγχου προσώπου σε ήδη υπάρχοντα κυκλώματα CCTV για τον εντοπισμό όσων κλέβουν στα χαρτιά, ενώ παρόμοια συστήματα έχουν εγκατασταθεί σε δημόσιους χώρους από αστυνομικές και κυβερνητικές υπηρεσίες, με σκοπό την πρόληψη και αποτροπή του εγκλήματος.

Αυτό όμως δεν είναι το μοναδικό όφελος. Είναι γνωστό, ότι κάποιοι χρήστες έχουν αντίρρηση με την κοινή χρήση βιομετρικών συσκευών, οι οποίες προϋποθέτουν φυσική επαφή, όπως είναι για παράδειγμα οι συσκευές σκαναρίσματος δαχτύλων ή χεριών. Συχνά δηλαδή, το άγγιγμα μιας συσκευής προκαλεί δυσφορία, γεννά το φόβο για μικρόβια, αρρώστιες κτλ. Αντίθετα, το σκανάρισμα του προσώπου, επειδή πραγματοποιείται από απόσταση και χωρίς επαφή, δε συνοδεύεται από τις παραπάνω αρνητικές αντιδράσεις.

**Δυνατότητα εγγραφής στατικών εικόνων**

Μια από τις μεγαλύτερες προκλήσεις για τα μεγάλης κλίμακας βιομετρικά συστήματα, είναι η φάση της αρχικής εγγραφής. Εξαιτίας της δυσκολίας συντονισμού προγραμμάτων μεγάλης έκτασης, που περιλαμβάνουν εκατομμύρια χρήστες, μπορεί να χρειαστούν ακόμα και χρόνια, έως ότου εγγραφεί ο συνολικά απαιτούμενος πληθυσμός. Έτσι, κάποια Αυτοματοποιημένα Συστήματα Αναγνώρισης Δακτυλικών Αποτυπωμάτων (Α.Σ.Α.Δ.Α., A.F.I.S.) χρησιμοποιούνται σε προγράμματα πολιτών, με ένα χρονοδιάγραμμα έναρξης της πλήρους λειτουργίας τα 3 με 5 χρόνια. Στα συστήματα προσώπου όμως, αν υπάρχει έστω και μία, υψηλής πιστότητας φωτογραφία ενός ατόμου, τότε αυτή μπορεί να στηρίξει την εγγραφή του στη βάση δεδομένων. Έτσι, πολλά μεγάλα συστήματα αναγνώρισης

χρησιμοποιούν φωτογραφίες προερχόμενες από διάφορα περιβάλλοντα, για να εμπλουτίσουν το αρχείο τους, κάτι που συμβαίνει κατά κράτος στα συστήματα παρακολούθησης. Γενικά, υπάρχουν πάρα πολλές εικόνες διάσπαρτες σε δημόσιες υπηρεσίες – στο Υπουργείο Μεταφορών π.χ. για χορήγηση άδειας οδήγησης – οι οποίες θα μπορούσαν να χρησιμοποιηθούν για εγγραφή σε μία βάση, υπό τον όρο ότι πληρούνται οι νομικές προϋποθέσεις.

### 2.2.6 Μειονεκτήματα

Υπάρχουν πολλοί περιοριστικοί παράγοντες, που μειώνουν την αποτελεσματικότητα του σκαναρίσματος προσώπου σε κάποια περιβάλλοντα.

**Αλλαγές στο περιβάλλον**

Η ακρίβεια της τεχνολογίας σκαναρίσματος προσώπου μειώνεται δραματικά, όταν κατά τη διάρκεια της πιστοποίησης ή της εγγραφής δεν πληρούνται κάποιες προϋποθέσεις. Συγκεκριμένα, ο χρήστης πρέπει να κοιτάζει ευθεία στην κάμερα και η γωνία λήψης να μην είναι ούτε απολύτως οριζόντια, ούτε απολύτως κάθετη. Το πρόσωπο πρέπει να φωτίζεται ομοιόμορφα, κατά προτίμηση από μπροστά. Συνήθως, οι παραπάνω προϋποθέσεις πληρούνται σε συστήματα όπου το περιβάλλον απόκτησης της εικόνας είναι αυστηρά ελεγχόμενο, αλλά αυτό δε συμβαίνει πάντοτε. Έτσι, παράγοντες όπως ο περιβάλλων φωτισμός, η θέση και η ποιότητα της κάμερας, η γωνία λήψης και η σύνθεση του φόντου επηρεάζουν τα ποσοστά λάθους του συστήματος. Γενικά, η μέγιστη απόδοση του συστήματος επιτυγχάνεται, όταν επικρατούν οι ίδιες συνθήκες και στην πιστοποίηση και στην εγγραφή.

**Αλλαγές στα χαρακτηριστικά**

Ακόμα και απλές αλλαγές στην εμφάνιση ενός ατόμου, φαίνεται πως επηρεάζουν την ικανότητα του συστήματος για έγκυρη πιστοποίηση των χρηστών. Αλλαγές στον τρόπο χτενίσματος και το μακιγιάζ, η απόκτηση γενειάδας, η προσθήκη γυαλιών, ακόμα και ουλές ή καπέλα μπορεί να σταθούν αιτίες απόρριψης ενός χρήστη. Για το λόγο αυτό, η συζήτηση για το θέμα των πλαστικών επεμβάσεων ή για το αν τα συστήματα μπορούν να

διακρίνουν δίδυμα αδέρφια μεταξύ τους δεν έχει νόημα, απ' τη στιγμή που τόσο βασικές λειτουργίες μπορούν να επηρεάσουν τη λειτουργία ενός συστήματος.

Με την εξέλιξη της τεχνολογίας, είναι πιθανό πολλά από αυτά τα προβλήματα να ξεπεραστούν. Το πρόσωπο είναι πράγματι ένα διακριτό χαρακτηριστικό και περιέχει αρκετά διακριτά στοιχεία, τη μύτη, το σχήμα των ματιών, τα χείλη κτλ.

**Παραβιάσεις σε θέματα ιδιωτικότητας**

Παρότι η δυνατότητα να λειτουργούν συγκεκαλυμμένα είναι ένα από τα πλεονεκτήματα των συστημάτων αναγνώρισης προσώπου, μπορεί να μετατραπεί σε σοβαρό μειονέκτημα, σε περίπτωση κακής και ασύδοτης χρήσης των συστημάτων. Ο φόβος ότι ανοίγει ο δρόμος για δημιουργία συστημάτων εντοπισμού και για παραβιάσεις σε ζητήματα ιδιωτικότητας, είναι υπαρκτός και όχι αβάσιμος. Στη Φλόριντα των Ηνωμένων Πολιτειών, η χρήση ενός συστήματος σκαναρίσματος προσώπου, με σκοπό τον εντοπισμό εγκληματιών, γνώρισε τις αντιρρήσεις μεγάλης μερίδας του κοινού. Ένα αντίστοιχο σύστημα που χρησιμοποιήθηκε στις εκλογές στην Ουγκάντα για τον εντοπισμό διπλών ψηφοφόρων, επικρίθηκε σκληρά, γιατί είχε ως αποτέλεσμα να μην υποστηρίξουν το υπάρχον σύστημα διακυβέρνησης κάποιοι τρομοκρατημένοι πολίτες. Είναι ευνόητο λοιπόν ότι, αν η τεχνολογία συνδεθεί με θέματα παραβίασης της ιδιωτικότητας, η δυνατότητα εξάπλωσης της θα υποβαθμιστεί σημαντικά.

### 2.2.7 Συμπεράσματα

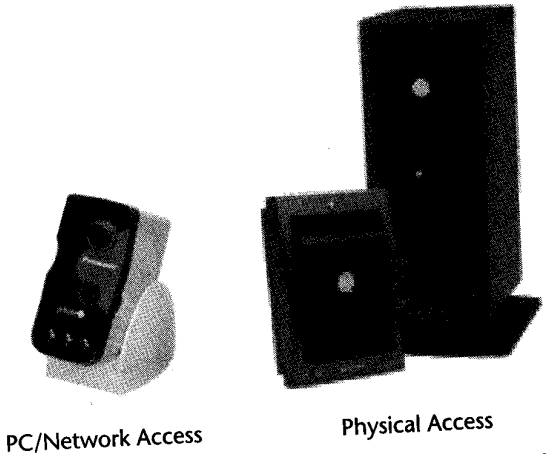
Συμπερασματικά, η τεχνολογία σκαναρίσματος προσώπου πλεονεκτεί, σε σχέση με τις υπόλοιπες βιομετρικές τεχνολογίες, κυρίως σε συστήματα παρακολούθησης, και γενικά όπου υπάρχει δυνατότητα αξιοποίησης προϋπάρχοντος εξοπλισμού και εικόνων.. Στις περιπτώσεις εκείνες, όπου και μόνο η παρουσία ενός βιομετρικού συστήματος είναι επαρκής για την αποτροπή από την απάτη, η τεχνολογία σκαναρίσματος προσώπου είναι ιδιαίτερα χρήσιμη. Αντίθετα, η υλοποίηση ενός συστήματος με υψηλές απαιτήσεις σε αξιοπιστία στο διηνεκές του χρόνου, είναι πολύ πιο δύσκολη, αλλά όχι ανέφικτη.

## 2.3 ΤΟ ΣΚΑΝΑΡΙΣΜΑ ΤΗΣ ΙΡΙΔΑΣ

Η τεχνολογία σκαναρίσματος ίριδας χρησιμοποιεί τα διακριτά χαρακτηριστικά της ανθρώπινης ίριδας, για την πιστοποίηση ή την αναγνώριση των ατόμων. Σε θεωρητικό επίπεδο, είναι μια τεχνολογία που παρουσιάζει ασύγκριτα πλεονεκτήματα, τα οποία αν εκπληρωθούν στην πράξη θα μπορέσει να καθιερωθεί ως η πλέον σημαντική βιομετρική λύση της αγοράς. Σκανάρισμα ίριδας χρησιμοποιείται κατά κύριο λόγο σε εφαρμογές φυσικής πρόσβασης με υψηλές απαιτήσεις ασφαλείας, ενώ η χρήση της τεχνολογίας έχει δοκιμαστεί με επιτυχία σε συστήματα ATM και ταξιδιωτικές εφαρμογές και σύντομα θα τεθεί σε χρήση και σε περιβάλλοντα desktop.

### 2.3.1 Συστατικά μέρη

Ένα σύστημα σκαναρίσματος ίριδας αποτελείται από υλισμικό (front-end hardware) για απόκτηση δεδομένων και από λογισμικό για την τοπική ή κεντρική επεξεργασία τους. Αντίθετα με το πρόσωπο, το σκανάρισμα της ίριδας βασίζεται σε εξειδικευμένες συσκευές, και συγκεκριμένα απαιτεί κάμερες με υπέρυθρο φωτισμό. Αυτές οι κάμερες μπορεί να είναι εξωτερικές ή ενσωματωμένες σε μονάδες φυσικής πρόσβασης (π.χ. κιόσκια), ενώ μπορεί ακόμα να διαθέτουν ενσωματωμένη λειτουργικότητα για κανονική βιντεοσκόπηση.




**Σχήμα 11.** Συσκευές σκαναρίσματος ίριδας

Τα συστατικά μέρη του λογισμικού του συστήματος, δηλαδή η μηχανή επεξεργασίας, η μηχανή ταιριάσματος και η βάση δεδομένων, μπορεί να βρίσκονται συγκεντρωμένα σε ένα τοπικό PC, κατάλληλα προσαρμοσμένο στη μονάδα απόκτησης, ή να είναι διασκορπισμένα ανάμεσα σε ένα τοπικό κι ένα κεντρικό PC. Συνήθως, όταν υπάρχουν πολλές περιφερειακές συσκευές, χρησιμοποιείται ένας κεντρικός server για το ταίριασμα και την αποθήκευση των δεδομένων, ενώ η παραγωγή των templates γίνεται στα τοπικά PCs. Έτσι, κατά μήκος του δικτύου μεταδίδονται templates και όχι οι αυτούσιες εικόνες των δεδομένων.

### 2.3.2 Τρόπος λειτουργίας

Οι μεταβλητές που σχετίζονται με λειτουργίες σκαναρίσματος της ίριδας και παραγωγή templates είναι λιγότερες, σε σχέση με άλλες βιομετρικές τεχνολογίες. Αναλυτικά, τα πέντε τετριμμένα στάδια λειτουργίας του συστήματος περιγράφονται παρακάτω.

**Απόκτηση εικόνας**

Η τεχνολογία σκαναρίσματος ίριδας προϋποθέτει την απόκτηση μιας εικόνας του ματιού υψηλής πιστότητας. Η λήψη γίνεται κάτω από συνθήκες υπέρυθρου φωτισμού, με μήκος κύματος που κυμαίνεται από 700 έως 900 nm, το οποίο είναι ασφαλές, σύμφωνα με την Αμερικανική Ακαδημία Οφθαλμολογίας. Οι ενέργειες που πρέπει να κάνει ο χρήστης διαφέρουν, ανάλογα με τη χρησιμοποιούμενη συσκευή. Υπάρχουν τρεις τύποι συσκευών, αυτές που χρησιμοποιούνται σε κιόσκια, οι συσκευές φυσικής πρόσβασης και οι φτηνές κάμερες για χρήση desktop[1].

Τα συστήματα σε κιόσκια απαιτούν από το χρήστη να σταθεί σε απόσταση λίγο μικρότερη του ενός μέτρου από την κάμερα, η οποία είναι προσαρμοσμένη στο ύψος των ματιών ενός μέσου χρήστη. Όταν κάποιος σταθεί απέναντι απ' την κάμερα, τότε αυτή προσπαθεί να εντοπίσει τα μάτια, από το σχήμα που έχουν. Για να διευκολυνθεί η διαδικασία, ο χρήστης πρέπει να βγάλει τα γυαλιά του, που μπορεί να προκαλέσουν

[1] J. Gonzalez-Rodriguez, J. Fiérrez-Aguilar, J. Ortega-Garcia, and J.J. Lucena-Molina, "Biometric Identification in Forensic Cases According to the Bayesian Approach".

φαινόμενα αντανάκλασης, και να παραμείνει ακίνητος. Απ' τη στιγμή που εντοπιστούν τα μάτια στο πρόσωπο, ο εντοπισμός της ίριδας και η απόκτηση της κατάλληλης εικόνας είναι μια αυτοματοποιημένη διαδικασία, που γίνεται μέσα σε 1 με 2 δευτερόλεπτα.

Οι συσκευές φυσικής πρόσβασης συνήθως απαιτούν μεγαλύτερη προσπάθεια από το χρήστη. Η λήψη της εικόνας γίνεται με μία μικρή κάμερα, που βρίσκεται πίσω από έναν καθρέφτη. Ο χρήστης καλείται να σταθεί σε απόσταση ενός μέτρου περίπου απ' τον καθρέφτη και να κοιτάξει μέσα σ' αυτόν. Μετά πρέπει να μετακινήσει κατάλληλα τα μάτια του, έτσι ώστε η ίριδα να βρεθεί μέσα σε μια συγκεκριμένη περιοχή, διαστάσεων 1,5 x 1,5 ίντσα. Μετά από παραίνεση του συστήματος μάλιστα, ίσως χρειαστεί να πλησιάσει ή να απομακρυνθεί από τον καθρέφτη. Από κει και πέρα, η υψηλής πιστότητας κάμερα αναλαμβάνει τη λήψη μιας σειράς από εικόνες του ματιού. Γενικά, η απόκτηση εικόνας με την παραπάνω διαδικασία είναι πιο απαιτητική, γιατί επαφίεται στην ικανότητα του χρήστη να ακολουθήσει οδηγίες και να αλληλεπιδράσει με το σύστημα. Ακόμα, επειδή μερικοί χρήστες χρησιμοποιούν περισσότερο ένα μάτι μπορεί να δυσκολευτούν να εστιάσουν στον καθρέφτη το άλλο.

Οι κάμερες desktop αποτελούν την πιο πρόσφατη εξέλιξη στις συσκευές σκαναρίσματος ίριδας και χρησιμοποιούνται για λογική πρόσβαση. Για να ληφθεί μια σωστή εικόνα, πρέπει η συσκευή να τοποθετηθεί σε απόσταση περίπου 18 ιντσών και ο χρήστης να ευθυγραμμίσει την ευθεία του βλέμματός του με μια δεσμίδα φωτός ή ένα ολόγραμμα. Οι κάμερες desktop, παρότι εξοικειώνουν το κοινό με τη βιομετρική τεχνολογία σκαναρίσματος ίριδας, έχουν αποδειχθεί σε ορισμένες περιπτώσεις δύσκολες στη χρήση.

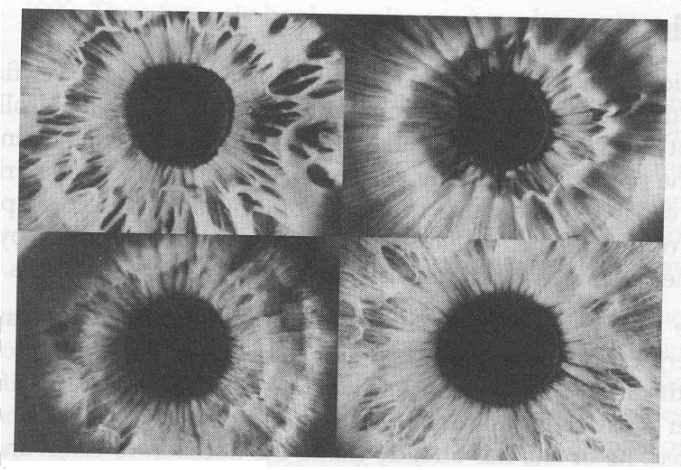
**Επεξεργασία εικόνας**

Ανεξάρτητα από τη συσκευή απόκτησης, η διαδικασία επεξεργασίας της εικόνας παραμένει η ίδια. Συγκεκριμένα, αφού εντοπιστεί το μάτι από την κάμερα, εφαρμόζεται ένας αλγόριθμος, ο οποίος το στενεύει από δεξιά και αριστερά, έως ότου βρεθεί η εξωτερική άκρη της ίριδας. Στη συνέχεια, ο αλγόριθμος εντοπίζει το εσωτερικό άκρο της ίριδας, που είναι το σημείο επαφής με την κόρη. Ο εντοπισμός αυτού του σημείου επαφής της κόρης με την ίριδα, μπορεί να είναι πιο δύσκολος σε χρήστες με πολύ σκούρα μάτια, εξαιτίας του εσωτερικού τρόπου αναπαράστασης των χρωμάτων, σε υπολογιστικά συστήματα με κλίμακα αναπαράστασης χρωμάτων των 8 bit. Απ' τη στιγμή που

προσδιοριστούν με ακρίβεια όλες οι παράμετροι, η εικόνα της ίριδας μετατρέπεται σε ασπρόμαυρη, για να ακολουθήσει στη συνέχεια η εξαγωγή των χαρακτηριστικών.

**Διακριτά χαρακτηριστικά**

Οι σχηματισμοί που συνθέτουν την ίριδα – όση έκπληξη κι αν προκαλεί αυτό – είναι εξαιρετικά επαρκείς για τη διάκριση δύο οποιονδήποτε ατόμων. Το κυρίαρχο χαρακτηριστικό στην ίριδα είναι ο διηθητικός ηθμός, ένας ιστός που δίνει την εντύπωση ότι την διαιρεί με τρόπο ακτινωτό. Άλλα ορατά χαρακτηριστικά είναι οι δακτύλιοι, οι κρύπτες και η στεφάνη. Αυτοί οι σχηματισμοί της ίριδας διαμορφώνονται πριν τη γέννηση του ανθρώπου, και παραμένουν σταθεροί καθ' όλη τη διάρκεια της ζωής του, εκτός και αν συμβεί κάποιο ατύχημα. Από έρευνες, γνωρίζουμε ότι ακόμα και το δεξί και αριστερό μάτι του ίδιου ατόμου έχουν διαφορετικούς σχηματισμούς πάνω τους, ενώ και οι ίριδες των διδύμων δεν έχουν σχεδόν καμία στατιστική ομοιότητα.



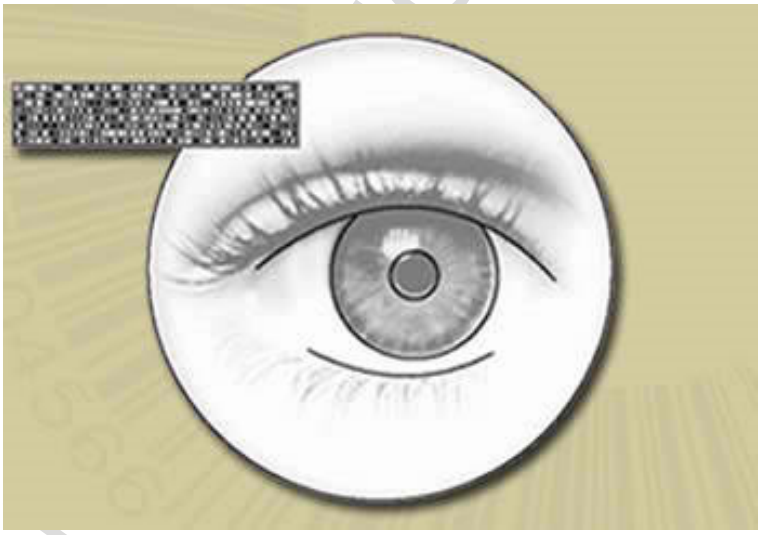
**Σχήμα 12.** Εικόνες της ίριδας

Οι αλγόριθμοι σκαναρίσματος της ίριδας αντιστοιχίζουν τμήματα της ίριδας σε εκατομμύρια ανεξάρτητα διανύσματα. Τα χαρακτηριστικά που προκύπτουν από την ανάλυση της ίριδας, καταγράφονται σε σχέση με το είδος και την τοποθεσία τους. Η απόδοση της τεχνολογίας δεν επηρεάζεται από φαινόμενα, όπως η διαστολή της κόρης, η απόκρυψη τμήματος της ίριδας από το βλέφαρο ή οι αντανακλάσεις της κάμερας. Αυτό

οφείλεται στον κατάλληλο χειρισμό αυτών των φαινομένων από τον αλγόριθμο. Όταν για παράδειγμα η κόρη του ματιού διαστέλλεται, γνωρίζουμε ότι η ίριδα συρρικνώνεται και εκτείνεται με έναν τρόπο κανονικοποιημένο. Με βάση αυτήν την πληροφορία, ο αλγόριθμος κάνει τη σωστή αντιστοίχιση ανάμεσα στη συρρικνωμένη ίριδα της πιστοποίησης και τη μη συρρικνωμένη της εγγραφής. Αλλά και για την απόκρυψη μέρους του ματιού, έχει προβλεφθεί το επάνω και κάτω τμήμα της ίριδας να μη χρησιμοποιούνται για την εξαγωγή των χαρακτηριστικών.

**Δημιουργία template**

Τα διανύσματα που εντοπίζονται από τον αλγόριθμο σκαναρίσματος της ίριδας χρησιμοποιούνται για την παραγωγή templates εγγραφής και ταιριάσματος. Για την παραγωγή του template εγγραφής, ανάλογα με την επιλεχθείσα λύση, μπορεί να χρησιμοποιηθούν από 1 έως 4 λήψεις. Η χρήση πολλών εικόνων μειώνει τον κίνδυνο ασυνέπειας των δεδομένων και παραπλάνησης από αντανακλάσεις.



**Σχήμα 13.** Ένα IrisCode

**Ταίριασμα templates**

Η τεχνολογία σκαναρίσματος ίριδας χρησιμοποιείται κυρίως σε συστήματα αναγνώρισης. Με τα σημερινά τεχνολογικά δεδομένα, εκατομμύρια εγγραφές μπορούν να ερευνηθούν μέσα σε λίγα δευτερόλεπτα. Λόγω της διακριτούς φύσης της ίριδας, το αποτέλεσμα που επιστρέφεται δεν είναι μια λίστα υποψηφίων, αλλά ένα ταίριασμα, που περιβάλλεται από

πολύ υψηλό βαθμό εμπιστοσύνης. Στα συστήματα πιστοποίησης η διαδικασία ταιριάσματος είναι η ίδια, με τη διαφορά ότι η σύγκριση διεξάγεται μόνο με το αποθηκευμένο template.

### 2.3.3 Εφαρμογές

Αν και το σκανάρισμα της ίριδας έχει γνωρίσει πολλές επιτυχείς εφαρμογές σε συστήματα φυσικής πρόσβασης, συστήματα πρόσβασης σε φυλακές, στρατιωτικές εφαρμογές και εφαρμογές τραπεζών (αναλήψεις από ταμειακές μηχανές τύπου ATM όπως στο Moorestown του New Jersey). Παρόλα αυτά έχει συσχετισθεί ελάχιστα με την ασφάλεια των δικτύων και τις εφαρμογές υπολογιστών. Ωστόσο, σύμφωνα με εκτιμήσεις των ειδικών, η ευρεία διάδοση και σε αυτούς τους τομείς είναι κάτι που επίκειται άμεσα[1].

**ΕΞΩΤΕΡΙΚΟ:**

**Η.Π.Α. και λοιπές Πολιτείες (Φλόριντα, Πενσυλβάνια)**

**1) Εφαρμογές για ασφάλεια και αποφυλάκιση φυλακισμένων**

Υπάρχουν πολλές εφαρμογές ανά τον κόσμο, όπου γίνεται βιομετρικός έλεγχος της ίριδας, με στόχο την αναγνώριση. Στις φυλακές της Νέας Υόρκης, της Φλόριντα και της Πενσυλβάνια για παράδειγμα, η τεχνολογία σκαναρίσματος ίριδας χρησιμοποιείται κατά την αποφυλάκιση των κρατουμένων. Ο λόγος είναι η ανάγκη επιβεβαίωσης με τρόπο κατηγορηματικό της ταυτότητας του αποφυλακιζόμενου, ούτως ώστε να μην υπάρχει ο φόβος αποφυλάκισης λάθος ατόμου. Σε κάποια άλλα σωφρονιστικά ιδρύματα, χρησιμοποιείται η ίδια τεχνολογία για την εγγραφή σε μια βάση δεδομένων των επισκεπτών. Κατά την έξοδο των επισκεπτών ελέγχεται ότι δε γίνεται προσπάθεια για απόδραση.



[1] <<Βιομετρικά Συστήματα για έλεγχο πρόσβασης>>, Στέλιος Χ.Α. Θωμόπουλος, Δ/ντης Ινστιτούτου Πληροφορικής και Τεχνολογίας , ΕΚΕΦΕ Δημόκριτος, Μαίος 2003.

**ΑΓΓΛΙΑ, ΙΑΠΩΝΙΑ,ΓΕΡΜΑΝΙΑ**

**2) Εφαρμογές σε δανειοδοτικούς οργανισμούς και τράπεζες**

Η τεχνολογία σκαναρίσματος ίριδας ήταν από τις πρώτες βιομετρικές τεχνολογίες που εφαρμόστηκε πιλοτικά σε περιβάλλοντα ATM. Το 1997, το Nationwide Building Society, ένας δανειοδοτικός οργανισμός στο Swindon της Αγγλίας, έδωσε τη δυνατότητα στους πελάτες του, να έχουν πρόσβαση χωρίς χρήση κάρτας σε μηχανήματα ATM, με ένα απλό σκανάρισμα ίριδας. Η αποδοχή της τεχνολογίας ήταν τεράστια, με ένα ποσοστό 94% των πελατών να προτιμάει το σκανάρισμα της ίριδας από τα παραδοσιακά PINs. Παρόμοια πιλοτικά προγράμματα διεξήχθησαν σ' εφαρμογές πελατών στις τράπεζες Bank United στο Τέξας και Takefuji Bank στην Ιαπωνία. Αλλά και στη Φρανκφούρτη, η Dresdner Bank εφαρμόζει ένα πιλοτικό πρόγραμμα σκαναρίσματος ίριδας από τα τέλη του 1999. Μέχρι στιγμής, η συγκεκριμένη τεχνολογία μπορεί να χρησιμοποιηθεί μόνο απ' τους υπαλλήλους, ενώ περίπου 1.000 χρήστες είχαν εγγραφεί ως τα τέλη του 2000.

**3) Εφαρμογές για ελέγχους σε αεροδρόμια**

Από τον Ιούλιο του 2000, λειτουργεί στο Charlotte/Douglas International Airport της North Carolina ένα σύστημα σκαναρίσματος ίριδας με τεχνολογία από την Iridian (πρώην IriScan)[1]. Οι συσκευές σκαναρίσματος χρησιμοποιούνται για να ελέγχουν την κίνηση των υπαλλήλων σε ευαίσθητες περιοχές, αντικαθιστώντας τα παραδοσιακά μηχανήματα πρόσβασης. Παρόμοιο σύστημα υπάρχει από τις αρχές του 2001 και στο αεροδρόμιο της Φρανκφούρτης. Και τα δύο συστήματα θεωρούνται εξαιρετικά επιτυχημένα και δεν έχει καταγραφεί μέχρι στιγμής περιστατικό λανθασμένης αναγνώρισης. Μια πιο φιλόδοξη εφαρμογή για επιβάτες αυτή τη φορά, ξεκίνησε στο London's Heathrow Airport τον Ιούλιο του 2001. Συγκεκριμένα, δίνεται η δυνατότητα σε επιλεγμένους επιβάτες που ταξιδεύουν συχνά με τη British Airways και τη Virgin Airways, να αποφεύγουν τον κουραστικό έλεγχο μετανάστευσης, επιβεβαιώνοντας την ταυτότητά τους μέσα από ειδικά μηχανήματα σκαναρίσματος ίριδας. Παρόμοιο πρόγραμμα ανακοινώθηκε πως θα λειτουργήσει και στον Καναδά, υπό την αιγίδα του Canadian Airports Council Expedited Passenger Processing System Project. Μ' αυτό το πρόγραμμα, οι πιο συχνοί επιβάτες στα

[1] http://www.findbiometrics.com/Pages/iris_retinal.html

οχτώ μεγαλύτερα αεροδρόμια της χώρας θα έχουν την επιλογή χρήσης μιας ταξιδιωτικής κάρτας με αποθηκευμένο το βιομετρικό τους template. Οι κάρτες θα επιτρέπουν στους κατόχους τους να επιβεβαιώνουν την ταυτότητά τους μέσα από ειδικά κιόσκια.

**ΑΕΡΟΔΡΟΜΙΟ MANCHESTER**

Το αεροδρόμιο του Μάντσεστερ δικαιωματικά κερδίζει τον τίτλο του πρωτοπόρου όσον αφορά τη χρήση συστημάτων ασφαλείας τελευταίας τεχνολογίας καθώς ξεκίνησε την πειραματική χρήση ενός σκάνερ. Αν όλα πάνε καλά σύμφωνα με τους υπεύθυνους υπάρχει πολύ μεγάλη πιθανότητα να καταργήσει εντελώς τα διαβατήρια, αφού θα μπορεί να "σαρώνει" την ίριδα του ματιού κάθε επιβάτη ως μέσο απόδειξης της ταυτότητας του[1].

Όπως και τα δακτυλικά αποτυπώματα, έτσι και η ίριδα είναι μοναδική σε κάθε άνθρωπο, μόνο που στην περίπτωση της ίριδας μιλάμε για ψηφιακό αποτύπωμα. Όπως στις ταινίες επιστημονικής φαντασίας θα μπορούν να μας σκανάρουν όχι μόνο όταν είμαστε μπροστά από τα μηχανήματα σάρωσης αλλά και όταν βρισκόμαστε εν κινήσει.

Το πιλοτικό αυτό πρόγραμμα υποστηρίζεται από τη βρετανική κυβέρνηση και θα δοκιμαστεί σε εθελοντική βάση επί δύο εβδομάδες, για να εκτιμηθεί στη συνέχεια αν θα εγκατασταθεί μόνιμα ή όχι στο αεροδρόμιο. Το επίμαχο σύστημα βιομετρικής τεχνολογίας έχει τη δυνατότητα να αιχμαλωτίζει την εικόνα της ίριδας από γωνίες που καλύπτουν ένα εύρος ως και 120 μοιρών, ακόμη και όταν κάποιος περπατάει (πράγμα αδύνατο στο παρελθόν), φοράει γυαλιά ή ακόμη και μάσκα! Έτσι, θα μπορεί να "διορθώνει" τυχόν κενά ή λάθη του υπάρχοντος συστήματος ασφαλείας ή των τελωνειακών υπηρεσιών.

Για την αρχική καταχώριση στο σύστημα, οι επιβάτες που δέχονται να συμμετάσχουν στο πρόγραμμα υποβάλλονται σε σάρωση της ίριδας κατά το "check in", ώστε να καταχωριστούν τα βιομετρικά τους στοιχεία. Κατόπιν ελέγχονται ξανά όταν εισέρχονται στην ασφαλή περιοχή του αεροδρομίου. Εκεί τους ζητείται να περπατήσουν με φυσιολογικό βήμα σε έναν διάδρομο πέντε μέτρων. Στο τέρμα του διαδρόμου μπορούν

[1] http://www.angelfire.com/nt/selcukgun/en/tran_2.htm

να δουν σε μια οθόνη αν το μηχάνημα τους αναγνώρισε με ακρίβεια ή όχι. Αν και το σύστημα βρίσκεται ακόμη σε αρχικό στάδιο ανάπτυξης, η κατασκευάστρια εταιρεία Human Recognition Systems (Συστήματα Ανθρώπινης Αναγνώρισης) δηλώνει ότι τα πρώτα αποτελέσματα είναι "ιδιαιτέρως θετικά".

Η τεχνολογία αναγνώρισης της ίριδας ενός ατόμου με καταχωρισμένα βιομετρικά στοιχεία ενώ αυτό βρίσκεται εν κινήσει θα μπορούσε να έχει πολλές μελλοντικές εφαρμογές, αλλά η πρώτη μάλλον θα είναι και η σημαντικότερη: η ασφάλεια των αεροδρομίων.

Οι ειδικοί εκτιμούν ότι το νέο σύστημα θα βοηθήσει στη μάχη κατά της τρομοκρατίας, του οργανωμένου εγκλήματος και της παράνομης μετανάστευσης, καθώς οι εγγεγραμμένοι στο σύστημα ταξιδιώτες δεν θα είναι δυνατόν να "ξεγελάσουν" τα σημεία ελέγχου ή να ανταλλάξουν μεταξύ τους τις κάρτες επιβίβασης.

Έτσι οι επιβάτες εσωτερικών και διεθνών πτήσεων θα μπορούν να έχουν πρόσβαση στους ίδιους χώρους του αεροδρομίου, μια και θα μπορούν να αναγνωριστούν με ασφάλεια προτού επιβιβαστούν στο αεροπλάνο. Παράλληλα, η αυτοματοποίηση του συστήματος θα μειώσει σημαντικά τον χρόνο αναμονής για τον έλεγχο των διαβατηρίων.

**4) Εφαρμογές σε τάξη και ασφάλεια από τις Αμερικάνικες αστυνομικές αρχές**

Δημοσίευμα της Wall Street Journal αναφέρεται σε μια νέα συσκευή αστυνομικού ελέγχου με την οποία σχεδιάζει το αμερικανικό κράτος να εξοπλίσει τις δυνάμεις καταστολής[1].

Μια κινητή συσκευή μπορεί να “σκανάρει” την ίριδα των ματιών ενός υπόπτου και να τη συγκρίνει με τη βάση δεδομένων των αστυνομικών για να αποκαλυφθεί το ποινικό μητρώο του και η ταυτότητά του.

[1] http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-104850/

Η κινητή αυτή συσκευή που ονομάζεται MORIS (Mobile Offender Recognition and Information System) τραβάει μια υψηλής ανάλυσης φωτογραφία περίπου 5 με 6 ίντσες μακριά από τις ίριδες του υπόπτου. Μετά το σύστημα του MORIS αναλύει 235 μοναδικά χαρακτηριστικά και χρησιμοποιεί έναν αλγόριθμο για να "ταιριάξει" αυτό το άτομο με κάποιο στη βάση δεδομένων.

Για την αναγνώριση του προσώπου ο αστυνομικός θα παίρνει φωτογραφία από απόσταση 2 με 5 μέτρων. Βασισμένο σε τεχνολογίες της εταιρίας Animetrics Inc., το σύστημα αναλύει περίπου 130 χαρακτηριστικά σημεία του προσώπου, όπως την απόσταση ανάμεσα στο μάτι και τη μύτη.

Το MORIS κατασκευάζεται από την εταιρία BI2 Technologies, με έδρα την πόλη Plymouth στη Μασαχουσέτη. Η εταιρία ιδρύθηκε το 2006 από τον Mullin, που συντόνιζε δικαστικά προγράμματα για το κράτος, και τον Peter Flynn, πρώην σερίφη. Το πρόσχημα που μπαίνει εδώ είναι η αναγνώριση υπόπτων χωρίς χαρτιά, τραυματιών σε ατυχήματα κ.ά.

Η εταιρία χρησιμοποίησε αλγόριθμους αναγνώρισης ίριδας και τεχνολογίες φωτογραφίας για να κατασκευάσει ένα προϊόν που αναγνωρίζει τους φυλακισμένους, το IRIS (Inmate Identification and Recognition System), το οποίο πούλησαν σε περισσότερα από 320 αστυνομικές υπηρεσίες σε 47 πολιτείες. Οι συσκευές κοστίζουν περίπου 3.000 δολάρια το κομμάτι.

**ΜΕΞΙΚΟ**

**5) Εφαρμογή σκαναρίσματος ίριδας για έκδοση ταυτότητας**

Το Μεξικό θα είναι το πρώτο κράτος που θα συμπεριλάβει την εικόνα της ίριδας του ματιού στις ταυτότητες… ένα σύστημα που η κυβέρνηση η ίδια διαβεβαιώνει πως θα είναι ένα από τα ασφαλέστερα στον κόσμο.

«Οι νομικές, τεχνικές και οικονομικές συνθήκες πλέον πληρούνται για να ξεκινήσει από τις 24 Ιανουαρίου 2011 η έκδοση των δελτίων αυτών» τόνισε στον Τύπο ο Φελίπε Σαμόρα, υπεύθυνος Δικαστικών Υποθέσεων του μεξικανικού υπουργείου Εσωτερικών.

Κατά τον ίδιον, η αξιοπιστία που θα έχουν τα δελτία ταυτότητας που θα περιλαμβάνουν την ίριδα του ματιού και στα οποία θα συνεχίσουν να υπάρχουν και τα δακτυλικά αποτυπώματα, θα φθάνει το 99,9% .

Το μέτρο αυτό θα αρχίσει να εφαρμόζεται προοδευτικά, με πρώτο στάδιο την έκδοση δελτίων σε 28 εκατ. ανηλίκους, και αναμένεται να έχει διάρκεια δύο ετών, ενώ το συνολικό κόστος θα ανέλθει στα 20 εκατ. ευρώ. Η έκδοση της νέας ταυτότητας για τους ενηλίκους προβλέπεται να ξεκινήσει από το 2013.

Το νέο δελτίο αναγνώρισης έχει δρομολογηθεί παρά τις συστάσεις της Εθνικής Επιτροπής για τα Ανθρώπινα Δικαιώματα, η οποία υπογραμμίζει τους κινδύνους που ενδέχεται να υπάρξουν για τις εγγυήσεις ασφάλειας των προσωπικών δεδομένων κατά την καταγραφή τους.

**6) Καινοτόμες εφαρμογές από την Panasonic**

Η Panasonic ανέπτυξε ένα νέο σύστημα ελέγχου πρόσβασης σε χώρους κρίσιμης σημασίας, που βασίζεται στη βιομετρική τεχνολογία αναγνώρισης της ίριδας του ματιού. Το σύστημα αυτό έχει τη δυνατότητα να αναγνωρίζει την ίριδα ενός ανθρώπου, καθώς αυτός περπατάει και κατευθύνεται προς μία είσοδο. Συγκεκριμένα, όταν αυτός πλησιάσει σε απόσταση ενός μέτρου, τότε το σύστημα «σκανάρει» το μάτι του, προκειμένου να πιστοποιήσει την ταυτότητά του.

Αν είναι εξουσιοδοτημένος να έχει πρόσβαση στο συγκεκριμένο χώρο, τότε του επιτρέπει την είσοδο, ανοίγοντας αυτόματα την πόρτα. Πρόκειται για ένα αξιόπιστο και προηγμένης τεχνολογίας σύστημα βιομετρικού ελέγχου πρόσβασης, που αξιοποιεί ένα φυσικό χαρακτηριστικό όπως η ίριδα του ματιού, το οποίο είναι μοναδικό για κάθε άνθρωπο. Το πλεονέκτημά του είναι ότι δεν απαιτεί από αυτόν που υπόκειται στον έλεγχο να εστιάζει το πρόσωπό του μπροστά από κάποιον αναγνώστη, αφού η όλη διαδικασία ελέγχου της ίριδας του ματιού και ταυτοποίησης του ατόμου, γίνεται την ώρα που αυτός περπατάει. Το σύστημα αυτό, που είναι εξοπλισμένο με κάμερες υψηλής ανάλυσης και προηγμένο λογισμικό, μπορεί να χρησιμοποιηθεί σε πρώτη φάση κατά τον έλεγχο επιβατών σε αεροδρόμια ή άλλες περιοχές ασφαλείας.

### 2.3.4 Πλεονεκτήματα

Το σκανάρισμα της ίριδας είναι μια τεχνολογία με πολλά πλεονεκτήματα. Όμως, πολλά από αυτά τα πλεονεκτήματα στηρίζονται κυρίως σε θεωρητικές διαπιστώσεις και δεν έχουν απαραίτητα δοκιμαστεί στην πράξη.

**Αυξημένη ακρίβεια**

Στην ίριδα βρίσκεται συγκεντρωμένος ένας τεράστιος όγκος από διακριτά δεδομένα, ικανά να διαχωρίσουν με σαφή τρόπο δύο οποιουσδήποτε ανθρώπους μεταξύ τους. Είναι χαρακτηριστικό ότι η ίριδα διαφέρει ακόμα και μεταξύ διδύμων ή μεταξύ των ματιών του ίδιου ατόμου – δεξιό κι αριστερό. Εξαιτίας αυτού του πλούτου των διακριτών πληροφοριών, τα templates που παράγονται από το σκανάρισμα της ίριδας είναι τα πλέον ακριβή.

Αυτό φαίνεται κι από τον μέχρι στιγμής έλεγχο της τεχνολογίας σε πραγματικά περιβάλλοντα. Αν και οι δυνατότητες των αντίστοιχων συστημάτων πρέπει να δοκιμαστούν και να εκτιμηθούν πιο εμπεριστατωμένα και συστηματικά σε βάθος χρόνου, τα πρώτα αποτελέσματα είναι ιδιαίτερα ενθαρρυντικά ως προς την ασφάλεια.

**Αντοχή της ίριδας στο χρόνο**

Ίσως το πιο σημαντικό πλεονέκτημα της ίριδας, είναι ότι αποτελεί ένα διακριτό χαρακτηριστικό, που δεν αλλάζει κατά τη διάρκεια ζωής ενός ανθρώπου. Η ανθεκτικότητά της στο χρόνο και τις εξωτερικές συνθήκες, σημαίνει ότι δεν υπάρχει όπως σε άλλα συστήματα, η ανάγκη επανεγγραφής μετά από ορισμένο χρονικό διάστημα. Πολλές επιχειρήσεις δεν στέκονται ιδιαίτερα σ' αυτό το σημείο, μη συνυπολογίζοντας το κόστος σε χρήματα και πόρους από τις επανεγγραφές, και το κόστος σε απόδοση μεταξύ των διαδοχικών επανεγγραφών. Αυτό όμως αποτελεί στρατηγικό λάθος.

**Δυνατότητα χρήσης σε όλες τις εφαρμογές**

Διαχρονικά, η τεχνολογία σκαναρίσματος ίριδας έχει χρησιμοποιηθεί κυρίως σε εφαρμογές φυσικής πρόσβασης και σε εφαρμογές ATM. Χάρη όμως στα άλματα της τεχνολογίας, το μέγεθος μιας συσκευής καταγραφής της ίριδας είναι πλέον το ίδιο με μιας συνηθισμένης κάμερας. Επιπλέον, σε αντίθεση με άλλες τεχνολογίες που, λόγω της φύσης τους, απευθύνονται καλύτερα είτε σε εφαρμογές λογικής είτε φυσικής πρόσβασης, η τεχνολογία της ίριδας μπορεί να χρησιμοποιηθεί εξίσου αποτελεσματικά και στις δύο. Έτσι, ανοίγει ο δρόμος για τη δημιουργία συστημάτων, τα οποία θα ενσωματώνουν ταυτόχρονη λειτουργικότητα και για φυσική και για λογική πρόσβαση, προσφέροντας π.χ. πρόσβαση τόσο σε κτίρια όσο και σε εφαρμογές desktop. Εξάλλου η ίριδα, ως το πιο αξιόπιστο διακριτό χαρακτηριστικό του ανθρώπου, έχει θέση σε μεγάλης κλίμακας εφαρμογές με απαιτήσεις τόσο σε αναγνώριση όσο και σε πιστοποίηση. Προτού γίνει αυτό βέβαια, πρέπει να καταρριφθούν αρκετά εμπόδια, αλλά τελικά η τεχνολογία αυτή αναμένεται να κυριαρχήσει.

### 2.3.5 Μειονεκτήματα

Το σκανάρισμα της ίριδας έχει κάποιες αδυναμίες, που άπτονται κυρίως λειτουργικών ζητημάτων.

**Δυσκολία χρήσης**

Η διαδικασία στην οποία υποβάλλεται ο χρήστης κατά το σκανάρισμα της ίριδας δεν είναι η πιο δύσκολη που συναντάται στο χώρο της βιομετρικής, αλλά ούτε και η πλέον εύκολη. Γενικά, το στήσιμο του χρήστη απέναντι από την κάμερα δεν είναι φυσικό, και για να είναι η θέση του κεφαλιού και των ματιών η ενδεδειγμένη πρέπει να υπάρχει συνέπεια και προσήλωση εκ μέρους του χρήστη, την ώρα της αλληλεπίδρασης με το σύστημα. Επιπλέον, όσοι αντιμετωπίζουν πρόβλημα με τα μάτια τους – πάσχουν για παράδειγμα από μυωπία ή στραβισμό – έχουν μεγαλύτερες δυσκολίες να συμμορφωθούν με τις υποδείξεις του συστήματος και να χρησιμοποιήσουν την τεχνολογία.

Εξάλλου, ο βαθμός δυσκολίας της όλης διαδικασίας κυμαίνεται, ανάλογα με τη συσκευή. Κατά γενική ομολογία, οι συσκευές desktop είναι οι πλέον δύσχρηστες, γιατί ο χρήστης πρέπει μόνος του να λάβει την κατάλληλη θέση, χωρίς να γνωρίζει σε πόση ακριβώς απόσταση από την κάμερα πρέπει να σταθεί. Οι συσκευές φυσικής πρόσβασης είναι ελαφρώς ευκολότερες στη χρήση, γιατί η απόσταση από τη συσκευή λήψης περιορίζεται. Τα συστήματα σε κιόσκια, τα οποία διαθέτουν τις πιο εξελιγμένες κάμερες της αγοράς, είναι τα πιο ευκολόχρηστα, χωρίς αυτό να σημαίνει ότι δεν απαιτούν τη σύμπραξη και την προσοχή των χρηστών.

**Δυσφορία και φόβος**

Υπάρχει ένα ποσοστό χρηστών, οι οποίοι δε νιώθουν καθόλου άνετα με την ιδέα της χρησιμοποίησης μιας βιομετρικής τεχνολογίας, που εξετάζει το μάτι. Όσο παράλογη κι αν είναι η αντίδρασή τους, η σκέψη και μόνο τούς προκαλεί αποστροφή. Άλλοι πάλι ανησυχούν ότι η έκθεση στη συγκεκριμένη τεχνολογία μπορεί να είναι επιβλαβής για το μάτι. Ο φόβος αυτός, υπάρχει και σε όσους δεν είναι ενήμεροι για τον υπέρυθρο φωτισμό στον οποίο βασίζεται το σκανάρισμα της ίριδας. Συνεπώς, σε ένα μελλοντικό σενάριο για υποχρεωτική χρήση της τεχνολογίας σε μεγάλη έκταση, δεν είναι απίθανο να υπάρξουν αντιδράσεις.

**Έλλειψη ανταγωνισμού στην κατασκευή εξειδικευμένων συσκευών**

Η ανάγκη για εξειδικευμένες συσκευές απόκτησης των δεδομένων υπάρχει σε πολλές βιομετρικές τεχνολογίες. Όμως, η ιδιαιτερότητα που υπάρχει με το σκανάρισμα της ίριδας είναι η έλλειψη ανταγωνισμού στην αγορά. Υπάρχουν πολύ λίγες εταιρείες που κατασκευάζουν μηχανές για απόκτηση εικόνων της ίριδας και όλες είναι εξουσιοδοτημένες από την Iridian. Αυτή η έλλειψη ανταγωνιστικών εταιρειών όμως, καθυστερεί την ανάπτυξη της τεχνολογίας. Αυτό δεν έχει να κάνει με τη φύση της τεχνολογίας, αλλά δυστυχώς είναι μια πραγματικότητα που πρέπει να ληφθεί υπόψιν.

### 2.3.6 Συμπεράσματα

Συνοψίζοντας για την τεχνολογία σκαναρίσματος της ίριδας, πρέπει να επαναλάβουμε ότι είναι η πιο ασύμφορα οικονομικά βιομετρική λύση κι αυτό την κάνει ιδιαίτερα ελκυστική. Η πρόκληση που τίθεται για τους ειδικούς πλέον, είναι να μπορέσουν να επαναλάβουν τα αποτελέσματα των εργαστηριακών μετρήσεων και σε πραγματικές συνθήκες.

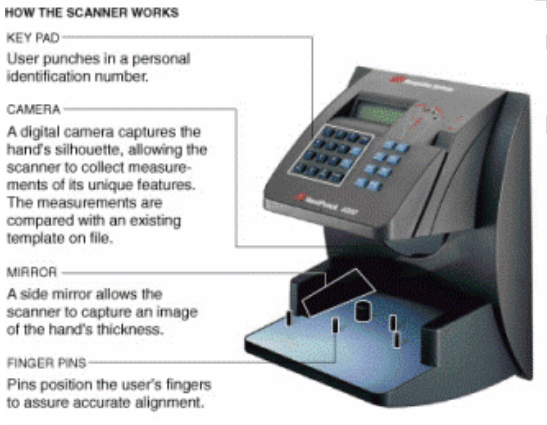
## 2.4 ΤΟ ΣΚΑΝΑΡΙΣΜΑ ΤΟΥ ΧΕΡΙΟΥ

Η τεχνολογία σκαναρίσματος χεριού χρησιμοποιεί τα διακριτά χαρακτηριστικά του χεριού – συγκεκριμένα το ύψος και το πλάτος του πίσω μέρους του χεριού και των δαχτύλων – για να πιστοποιήσει την ταυτότητα των ατόμων. Είναι μια από τις πιο συνηθισμένες βιομετρικές τεχνολογίες και έχει χρησιμοποιηθεί σε χιλιάδες εφαρμογές πιστοποίησης. Πρόκειται για μια λύση περισσότερο επικεντρωμένη στην εκάστοτε εφαρμογή (application-specific) απ' ότι οι περισσότερες βιομετρικές τεχνολογίες και χρησιμοποιείται αποκλειστικά για εφαρμογές φυσικής πρόσβασης και εφαρμογές time and attendance[1].

[1] A. K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance", IEICE Trans. Fundamentals, Vol. E84-D, No. 7, pp. 788-799, 2001.

### 2.4.1 Συστατικά μέρη

Τα συστατικά μέρη ενός συστήματος σκαναρίσματος χεριού – το hardware απόκτησης, το λογισμικό σύγκρισης και ο χώρος αποθήκευσης των δεδομένων – βρίσκονται μέσα στην ίδια, ανεξάρτητη συσκευή. Σε ορισμένες υλοποιήσεις, τα συστήματα σκαναρίσματος χεριού χρησιμοποιούνται σε συνδυασμό με κάρτες, που φέρουν το ID του χρήστη, και με τις οποίες γίνεται η ανάκτηση του κατάλληλου template. Μικροί επεξεργαστές διεκπεραιώνουν τις λειτουργίες παραγωγής και σύγκρισης των templates κι επιστρέφουν το αποτέλεσμα μέσα από οθόνες.




**Σχήμα 14.** Μια συσκευή σκαναρίσματος χεριού

Συνήθως, τα συστήματα σκαναρίσματος χεριού είναι ενσωματωμένα σε υπάρχοντα συστήματα ελέγχου πρόσβασης, συγκεκριμένα σε συστήματα time and attendance και συστήματα ενεργοποίησης του ανοίγματος μιας πόρτας. Όπου απαιτείται, υπάρχει δυνατότητα μία συσκευή να στέλνει δεδομένα σε πολλές άλλες, κι έτσι αποφεύγεται η διαδικασία εγγραφής του χρήστη σε όλες τις συσκευές. Αυτό μπορεί να συμβεί για παράδειγμα, σε ένα χώρο με πολλούς υπαλλήλους και πολλές πόρτες, όπου δεν υπάρχει ανάγκη ο κάθε χρήστης να εγγραφεί σε όλες τις πόρτες στις οποίες έχει πρόσβαση.

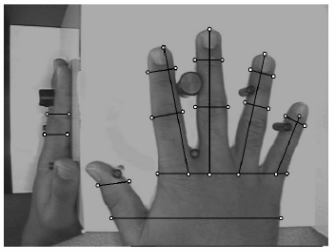
### 2.4.2 Τρόπος λειτουργίας

Επειδή όλες σχεδόν οι συσκευές σκαναρίσματος χεριού που υπάρχουν αυτή τη στιγμή στο εμπόριο, προέρχονται απ' τον ίδιο κατασκευαστή, υπάρχουν πολύ μικρές διαφορές στον τρόπο λειτουργίας τους. Εναλλακτικές προσεγγίσεις, που στηρίζονται στην καταγραφή της δομής δύο δαχτύλων και όχι ολόκληρου του χεριού, λειτουργούν με παρόμοιο τρόπο, αλλά σπάνια χρησιμοποιούνται.

**Απόκτηση και επεξεργασία δεδομένων**

Ένας χρήστης για να εγγραφεί ή να πιστοποιήσει την ταυτότητά του σε ένα σύστημα σκαναρίσματος χεριού πρέπει να τοποθετήσει το δεξί του χέρι σε μια ειδική επιφάνεια καλυμμένη από μέταλλο. Πέντε ειδικά στηρίγματα εξασφαλίζουν ότι το χέρι είναι τοποθετημένο σωστά, με τα δάχτυλα επαρκώς διαχωρισμένα μεταξύ τους και την παλάμη επίπεδη. Πολλές κάμερες αποκτούν τρισδιάστατες εικόνες από την πίσω μεριά και τις πλευρές του χεριού. Ο χρήστης καλείται να τοποθετήσει το χέρι του τρεις φορές στη συσκευή για την εγγραφή, ενώ για την πιστοποίηση μόνο μία[1].

[1] Robert van Kralingen, Corien Prins and Jan Grijpink, "Using your body as a key; legal aspects of biometrics", November 1997.



**Σχήμα 15.** Τα πέντε ειδικά στηρίγματα και τα χαρακτηριστικά που εξάγονται από την εικόνα του χεριού

Οι συσκευές σκαναρίσματος χεριού είναι ολοκληρωμένες μονάδες, με λειτουργίες απόκτησης εικόνας και λειτουργίες επεξεργασίας, που είναι αδιαχώριστες μεταξύ τους. Η διαδικασία απόκτησης είναι εξαιρετικά απλή και σύντομη, η εγγραφή και των τριών εικόνων του χεριού μπορεί να γίνει σε 5 δευτερόλεπτα. Αλλά και η πιστοποίηση γίνεται σχεδόν άμεσα και μπορεί να ολοκληρωθεί σε λιγότερο από 1 δευτερόλεπτο, απ' τη στιγμή που ο χρήστης εισάγει τον προσωπικό κωδικό αναγνώρισης (PIN). Σε περίπτωση που οι χρήστες δεν τοποθετήσουν σωστά τα δάχτυλά τους, τότε LEDs υποδεικνύουν την περιοχή όπου υπάρχει το πρόβλημα.

Υπάρχουν ορισμένοι χρήστες που δεν μπορούν να παρέχουν επαρκή δεδομένα κατά το σκανάρισμα του χεριού για να εγγραφούν. Για παράδειγμα, όσοι υποφέρουν από αρθριτικά μπορεί να μην μπορούν να εκτείνουν τα δάχτυλά τους όπως πρέπει ή να ισιώσουν την παλάμη τους στη συσκευή. Ακόμη, οι χρήστες με πολύ μικρά χέρια μπορεί να μην φτάνουν τα ειδικά στηρίγματα και γενικά να απλώνουν τα δάχτυλά τους ακατάστατα.

**Διακριτά χαρακτηριστικά**

Πολλοί χρήστες θεωρούν λανθασμένα ότι οι ανιχνευτές της παλάμης χρησιμοποιούν για την πιστοποίηση τα αποτυπώματα της παλάμης. Στην πραγματικότητα, μετρούν 90 διαφορετικά χαρακτηριστικά του χεριού και των δαχτύλων, μεταξύ αυτών το συνολικό μήκος, πλάτος και ύψος, την απόσταση ανάμεσα στις κλειδώσεις, τη δομή των οστών κτλ. Αντίθετα, παραβλέπονται οι άκρες των δαχτύλων, που μπορεί να αλλάξουν όψη, όσο τα νύχια μακραίνουν ή κόβονται. Τα χαρακτηριστικά που εξάγονται από το σκανάρισμα του χεριού δεν είναι ιδιαίτερα διακριτά, και αυτό συνεπάγεται ότι δεν μπορούν να

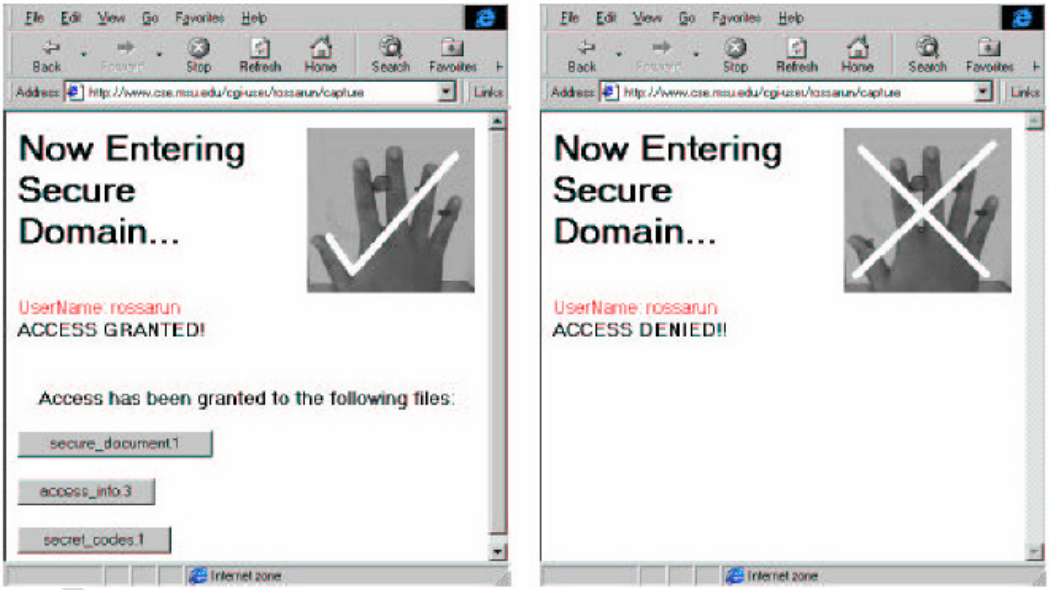
χρησιμοποιηθούν σε συστήματα αναγνώρισης ή σε εφαρμογές με εξαιρετικά υψηλές απαιτήσεις ασφαλείας.

**Δημιουργία template**

Τα διακριτά χαρακτηριστικά του χεριού και των δαχτύλων εξάγονται από τη σειρά των τρισδιάστατων εικόνων και καταγράφονται σε ένα πολύ μικρό template των. Το πολύ μικρό μέγεθος που έχουν, επιτρέπει σε πολλά templates χεριού να αποθηκεύονται σε μικρό χώρο μνήμης, αλλά είναι επίσης ενδεικτικό της έλλειψης διακριτικότητας των δεδομένων του χεριού.

**Ταίριασμα templates**

Παρότι η δομή των οστών και οι κλειδώσεις είναι αρκετά σταθερά χαρακτηριστικά, υπάρχουν περιστάσεις ικανές να τους προκαλέσουν αλλαγές. Το πρήξιμο του χεριού για παράδειγμα μπορεί να κρύψει την υφιστάμενη δομή, ενώ οι διάφοροι τραυματισμοί μπορεί να έχουν παρόμοιες συνέπειες.




**Σχήμα 16.** Μια επιτυχημένη διαδικασία πιστοποίησης, όπου χορηγείται πρόσβαση στα διαθέσιμα αρχεία, και μια αποτυχημένη διαδικασία

### 2.4.3 Εφαρμογές

Το σκανάρισμα του χεριού έχει χρησιμοποιηθεί σε ένα μεγάλο αριθμό από ενδιαφέρουσες εφαρμογές μεγάλης κλίμακας με ιδιαίτερη έμφαση στις εφαρμογές υπαλλήλων. Οι ακόλουθες εφαρμογές, που επικεντρώνονται στην πιστοποίηση της ταυτότητας ταξιδιωτών , στην ασφάλεια πρόσβασης σε κτίρια, σε αεροδρόμια, σε εκπαιδευτικά ιδρύματα καθώς και στην δημιουργία ιατρικών φακέλων ασθενών.

**ΕΞΩΤΕΡΙΚΟ**

**Η.Π.Α. λοιπές πολιτείες και ΙΣΡΑΗΛ**

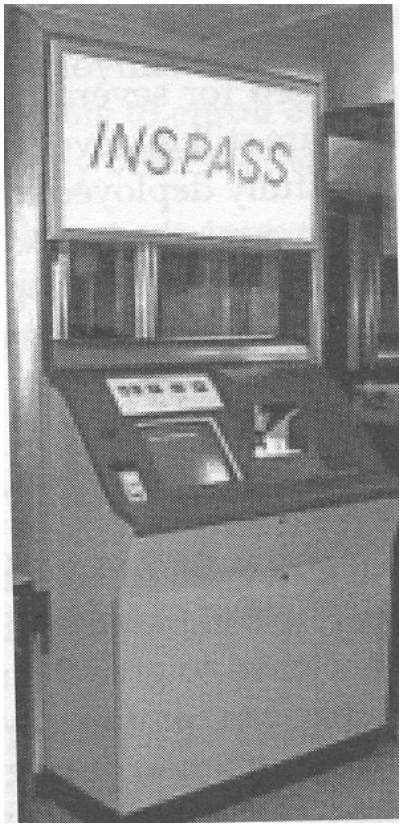
**1)Εφαρμογές σε Υπηρεσίες μετανάστευσης και αεροδρόμια**

Πρόκειται για μέσο πιστοποίησης της αυθεντικότητας ενός ατόμου, το οποίο ελέγχει το σχήμα του χεριού ή των δακτύλων. Ο χρήστης τοποθετεί το χέρι του επάνω σε μια πλάκα έτσι ώστε να ευθυγραμμίζεται με πέντε οδηγούς και το σύστημα φωτογραφίζει το χέρι του εξετάζοντας το τρισδιάστατο σχήμα της παλάμης, το μήκος και το πλάτος των δακτύλων, καθώς και το σχήμα των αρθρώσεων. Η γεωμετρία χεριού έχει εφαρμοστεί ευρέως σε κέντρα δεδομένων τραπεζικών ιδρυμάτων, σε αμερικανικά πανεπιστήμια (αναγνώριση φοιτητών στις φοιτητικές εστίες ή στα εστιατόρια) και εταιρείες (αντικαθιστώντας την κάρτα που διαθέτουν συνήθως οι εργαζόμενοι). Ιδιαίτερα γνωστή έχει γίνει η μέθοδος της γεωμετρίας χεριού τα τελευταία χρόνια λόγω της εφαρμογής της από την Υπηρεσία Μετανάστευσης και Πολιτογράφησης (Immigration Naturalization Service) των ΗΠΑ. Οι συχνοί ταξιδιώτες (οι οποίοι προέρχονται από 23 χώρες με τις οποίες έχει υπογραφεί σχετική σύμβαση με την κυβέρνηση των ΗΠΑ) έχουν αρχειοθετηθεί από την Υπηρεσία έτσι ώστε να επισπεύδεται η διέλευσή τους στο τελωνείο. Συγκεκριμένα, επιδεικνύουν μια ειδική κάρτα που τους έχει χορηγηθεί και κατόπιν υποβάλλονται σε βιομετρικό έλεγχο του χεριού τους[1].

Το σύστημα αυτό που χρησιμοποιεί τεχνολογία σκαναρίσματος χεριού, βρίσκεται σε εφαρμογή από το 1993. Σύμφωνα με στοιχεία του INS, το 1999 ένα ποσοστό 0.64 των

[1]J. Gonzalez-Rodriguez, J. Fiérrez-Aguilar, J. Ortega-Garcia, and J.J. Lucena-Molina, "Biometric Identification in Forensic Cases According to the Bayesian Approach".

διεθνών ταξιδιωτών ήταν εγγεγραμμένοι στο σύστημα, ενώ ένα ποσοστό 0.70 αναμενόταν να έχει εγγραφεί ως το 2001. Προς το παρόν, υπάρχουν 40.000 με 50.000 ενεργοί χρήστες του συστήματος αυτού, που βασίζεται σε κιόσκια και λειτουργεί στη Νέα Υόρκη, το Μαϊάμι, το Λος Άντζελες, το Νιούαρκ, το Σαν Φρανσίσκο και την Ουάσινγκτον. Αντίστοιχα, οι Αμερικανοί και Καναδοί υπήκοοι χαμηλής επικινδυνότητας μπορούν να εγγραφούν στην CANPASS, που όμως χρησιμοποιεί τεχνολογία σκαναρίσματος δαχτύλων, αντί για σκανάρισμα χεριού.




**Σχήμα 17.** Σκανάρισμα χεριού σε κιόσκι

Το 1998, η εταιρεία Ben-Gurion Airport στο Τελ Αβίβ του Ισραήλ, εγκατέστησε ένα παρόμοιο σύστημα τεχνολογίας σκαναρίσματος χεριού, που επιτρέπει στους Ισραηλινούς πολίτες να καταστρατηγούν τις γραμμές, όταν ταξιδεύουν διεθνώς. Λόγω της αυξημένης

ζήτησης εκ μέρους του επιβιβαστικού κοινού, η υλοποίηση πρόσφατα επεκτάθηκε και μπορεί σήμερα να διαχειρίζεται 50.000 επιβάτες μηνιαίως[1].

### 2.4.4 Πλεονεκτήματα

Το σκανάρισμα του χεριού δεν έχει αλλάξει ουσιωδώς από τη στιγμή που εισήχθη στο χώρο του εμπορίου, γεγονός που σημαίνει ότι τα πλεονεκτήματα και οι αδυναμίες του είναι διαπιστωμένες και γερά εδραιωμένες.

**Τεχνολογία ικανή να λειτουργήσει σε απαιτητικά περιβάλλοντα**

Οι συσκευές σκαναρίσματος χεριού κατασκευάζονται από μέταλλο και πλαστικό και αποτελούνται από εξαρτήματα που είναι δύσκολο να υποστούν ζημιές, με άλλα λόγια μπορούν να αντεπεξέλθουν στις ανάγκες ενός απαιτητικού περιβάλλοντος. Γενικά, οι συσκευές σκαναρίσματος χεριού μπορούν να λειτουργήσουν σε εξωτερικούς χώρους, σε χώρους υπό κατασκευή και σε άλλα μέρη, όπου δε θα μπορούσαν να λειτουργήσουν οι περισσότερες βιομετρικές συσκευές. Ακόμη, τα χαρακτηριστικά που μετράνε είναι ανθεκτικά στις καθημερινές και τις περιβαλλοντολογικές αλλαγές, οπότε απ' αυτή την άποψη πλεονεκτούν σε σχέση με συσκευές σκαναρίσματος δαχτύλων και άλλες βιομετρικές τεχνολογίες. Πιο συγκεκριμένα, το σκανάρισμα του χεριού είναι μια τεχνολογία που μπορεί να λειτουργήσει αποτελεσματικά κάτω από ακραίες συνθήκες θερμοκρασίας και υγρασίας και να πιστοποιήσει ορθά χρήστες με βρώμικα χέρια ή και ακόμα όσους φοράνε λεπτά γάντια από λάτεξ. Επειδή μάλιστα οι συσκευές φυσικής πρόσβασης είναι πολύ πιθανό να είναι εκτεθειμένες στα στοιχεία της φύσης, αυτή η ανθεκτικότητα και η ευρωστία των συσκευών σκαναρίσματος χεριού αποτελεί πολύ μεγάλο συγκριτικό πλεονέκτημα.

**Τεχνολογία εδραιωμένη και αξιόπιστη**

Σε αντίθεση με άλλες βιομετρικές τεχνολογίες, των οποίων οι βασικές λειτουργίες βρίσκονται ακόμα σε στάδια ανάπτυξης, ο πυρήνας της τεχνολογίας σκαναρίσματος

[1] <<Βιομετρικά Συστήματα για έλεγχο πρόσβασης>>, Στέλιος Χ.Α. Θωμόπουλος, Δ/ντης Ινστιτούτου Πληροφορικής και Τεχνολογίας , ΕΚΕΦΕ Δημόκριτος, Μαίος 2003.

χεριού έχει παραμείνει αμετάβλητος εδώ και χρόνια. Γενικά, το σκανάρισμα του χεριού είναι μια άρτια χρησιμοποιημένη επιστημονική τεχνολογία, που έχει χρησιμοποιηθεί με επιτυχία σε χιλιάδες εφαρμογές και λειτουργεί με έναν αρκετά προβλέψιμο και σταθερό τρόπο, και σ' αυτό το σημείο πλεονεκτεί σε σχέση με άλλες τεχνολογίες, οι οποίες θεωρητικά είναι πιο αξιόπιστες και βολικές στη χρήση, αλλά η αποτελεσματικότητα τους δεν έχει αποδειχθεί σε βάθος χρόνου μέσα από πραγματικές εφαρμογές.

**Τεχνολογία που δε θεωρείται ενοχλητική**

Οι χρήστες των συσκευών σκαναρίσματος χεριού, σε γενικές γραμμές δεν τις θεωρούν ως ενοχλητικές ή απειλητικές. Αυτό οφείλεται μερικώς στις σχετικά εύκολες διαδικασίες εγγραφής και πιστοποίησης που διαθέτουν. Πράγματι, ο χρήστης δε χρειάζεται να επικεντρώνει όλη την προσοχή του στο σύστημα κατά τη διαδικασία πιστοποίησης, αλλά μπορεί άνετα να μιλάει με άλλους ανθρώπους, να κοιτάζει αλλού κτλ. Ένα ακόμη θετικό σημείο με το σκανάρισμα του χεριού, είναι ότι δεν προκαλεί αρνητικούς συσχετισμούς με δραστηριότητες της σήμανσης, όπως συμβαίνει με τα συστήματα σκαναρίσματος δαχτύλων. Γενικά δηλαδή, επειδή χρησιμοποιείται σε κλειστά συστήματα με ιδιωτικές συσκευές απόκτησης υπάρχει ένας σχετικός εφησυχασμός για ζητήματα ιδιωτικότητας.

**Τεχνολογία που έχει ως βάση σχετικά σταθερά χαρακτηριστικά της φυσιολογίας του ατόμου**

Μετά την ενηλικίωση του ατόμου, οι διαστάσεις του χεριού παραμένουν σχετικά σταθερές κατά τη διάρκεια της ζωής του. Το πέρασμα του χρόνου επηρεάζει μεν την κατάσταση του δέρματος, αλλά συνήθως αφήνει ανέπαφο το σχήμα του χεριού. Ακόμα, μικροί τραυματισμοί, όπως εγκοπές, γρατσουνιές, καψίματα και γδαρσίματα, που στην περίπτωση του σκαναρίσματος δαχτύλων μπορεί να αποβούν καθοριστικοί για την αποτυχία του συστήματος, δεν επηρεάζουν την απόδοση στο σκανάρισμα του χεριού. Άλλες, μη μόνιμες αλλαγές, όπως η απώλεια ή η αύξηση βάρους επίσης δεν επηρεάζουν σε μεγάλο βαθμό την τεχνολογία κι αυτό γιατί οι μετρήσεις καθορίζονται περισσότερο από τη δομή των οστών και όχι τόσο απ' τη σάρκα του ατόμου. Έτσι, με εξαίρεση τα αρθριτικά και το πρήξιμο των χεριών, λόγω εγκυμοσύνης ή τραυματισμού, δεν υπάρχουν

άλλοι παράγοντες που να επιδρούν αρνητικά στην ικανότητα της τεχνολογίας για ορθή πιστοποίηση.

**Τεχνολογία που συνδυάζει τη διευκόλυνση με την αποτροπή από την απάτη**

Τα συστήματα σκαναρίσματος χεριού γενικά μπορούν να εγγράφουν και να πιστοποιούν ένα υψηλό ποσοστό χρηστών, γεγονός που σημαίνει ότι υπάρχει μικρότερη εξάρτηση της τεχνολογίας από έναν εναλλακτικό μηχανισμό πιστοποίησης. Βέβαια, όλες οι βιομετρικές εφαρμογές απαιτούν ένα εναλλακτικό σχήμα πιστοποίησης για τους χρήστες που αδυνατούν να εγγραφούν ή να πιστοποιήσουν την ταυτότητά τους βιομετρικά συνεπή τρόπο. Το σκανάρισμα του χεριού όμως, είναι λιγότερο πιθανό να καταφύγει σε κάποια fallback διαδικασία πιστοποίησης, σε σχέση με τις περισσότερες βιομετρικές τεχνολογίες.

Η ασφάλεια που παρέχεται από τα συστήματα σκαναρίσματος χεριού μεταφράζεται και σε αποτροπή απ' την απάτη. Επειδή μάλιστα οι πραγματικοί χρήστες σπάνια απορρίπτονται απ' το σύστημα, όσοι προσπαθούν να αποκτήσουν πρόσβαση σε ξένους λογαριασμούς πρέπει να φαίνονται σε ένα ειδικό αρχείο και οι προσπάθειές τους για μη εξουσιοδοτημένη είσοδο να καταγράφονται.

### 2.4.5 Μειονεκτήματα

Τα μειονεκτήματα που παρουσιάζει το σκανάρισμα του χεριού περιορίζουν τις περιοχές στις οποίες μπορεί να χρησιμοποιηθεί, καθώς και την ικανότητά του να παρέχει αποτελέσματα με υψηλό επίπεδο εμπιστοσύνης.

**Εκ φύσεως περιορισμένη ακρίβεια**

Η ακρίβεια του σκαναρίσματος χεριού περιορίζεται εκ των πραγμάτων, τόσο από το σχετικά μικρό αριθμό των χαρακτηριστικών του χεριού, όσο και από τη γενική έλλειψη ποικιλίας σ' αυτά τα φυσιολογικά χαρακτηριστικά. Αν και αρκετά διαφορετικά, το μέγεθος και το σχήμα του ανθρώπινου χεριού δεν είναι μοναδικά, όπως τα δακτυλικά αποτυπώματα ή οι σχηματισμοί της ίριδας. Έτσι, παρότι οι διαστάσεις του χεριού δύο ατόμων συνήθως διαφέρουν σημαντικά μεταξύ τους, είναι σχεδόν βέβαιο ότι σε ευρύτερους πληθυσμούς θα υπάρχουν άτομα με πολύ κοντινές διαστάσεις χεριού. Για το

λόγο αυτό, το σκανάρισμα του χεριού είναι κατάλληλο μόνο για πιστοποίηση ένα-προς-ένα, αφού υπάρχουν άλλες βιομετρικές τεχνολογίες με καλύτερες προοπτικές για ασφάλεια. Συνεπώς, όταν η αντοχή στις επιθέσεις είναι το πρώτιστο μέλημα κι έχει βαρύνουσα σημασία, το σκανάρισμα του χεριού δεν είναι η ιδανική λύση.

**Περιορισμένο εύρος δυνατών εφαρμογών**

Για να διευκολυνθεί η τοποθέτηση του χεριού και για να στεγαστούν οι κάμερες που απαιτούνται για την απόκτηση των εικόνων πρέπει οι συσκευές σκαναρίσματος να είναι αρκετά ψηλές και να διαθέτουν ειδικά διαμορφωμένο χώρο για την τοποθέτηση των ποδιών. Αυτό όμως περιορίζει την τεχνολογία σε εφαρμογές φυσικής πρόσβασης και time and attendance, ενώ αποκλείει την πιθανότητα χρήσης της τεχνολογίας σε εφαρμογές για PCs. Έτσι, οι κατασκευαστές και οι διανομείς των συσκευών δεν απευθύνονται στο τμήμα της αγοράς που σχετίζεται με λογικές εφαρμογές, γεγονός που περιορίζει το εύρος των πωλήσεων και των κερδών.

**Υψηλό κόστος**

Το σκανάρισμα του χεριού, επειδή είναι μια λύση κυρίως για εφαρμογές φυσικής πρόσβασης, συναγωνίζεται με τεχνολογίες που βασίζονται σε κάρτες. Όμως, με τυπικό κόστος που φτάνει τα 1500$ ανά μονάδα, οι συσκευές που χρησιμοποιούνται για σκανάρισμα του χεριού είναι ακριβές, σε σχέση με τις συσκευές ανάγνωσης καρτών, ειδικά απ' τη στιγμή που οι περισσότερες εφαρμογές σκαναρίσματος χεριού περιλαμβάνουν και κάρτες ID. Ακόμα και τα συγκρίσιμα συστήματα σκαναρίσματος δαχτύλων, που είναι λιγότερο ώριμα, αλλά ικανά για υψηλότερα επίπεδα ακρίβειας, διατίθενται σε χαμηλότερο κόστος και με διευρυμένη λειτουργικότητα. Συνεπώς, η υψηλή τιμή αποτελεί σημαντικό μειονέκτημα και μπορεί να αποδοθεί στην έλλειψη ανταγωνισμού στην αγορά του σκαναρίσματος χεριού.

### 2.4.6 Συμπεράσματα

Γενικά, το σκανάρισμα του χεριού αποτελεί μια λύση μέσης ασφάλειας που χρησιμοποιείται σε εφαρμογές φυσικής πρόσβασης και time and attendance, παρέχοντας

σημαντικά πλεονεκτήματα σε σχέση με τα παραδοσιακά συστήματα καρτών, όπως την αποθάρρυνση από την απάτη, το γεγονός ότι κανείς δεν μπορεί να χτυπήσει την κάρτα ενός απόντος φίλου συναδέλφου κτλ. Ο πυρήνας της τεχνολογίας δεν έχει αλλάξει τα τελευταία χρόνια, αλλά παράλληλα δεν έχουν διευρυνθεί και οι χώροι εφαρμογής της. Η σχετική σταθερότητα που παρουσιάζει, καθώς και η έλλειψη συσχέτισης με θέματα παραβίασης της ιδιωτικότητας αποδεικνύουν πόσο δύσκολος είναι ο χαρακτηρισμός της βιομετρικής στο σύνολό της, αν δεν υπάρχει αναφορά σε συγκεκριμένη τεχνολογία. Σε σύγκριση με το σκανάρισμα των δαχτύλων και της ίριδας, που είναι δύο πολύ δυναμικές, καθοριστικές και ευαίσθητες τεχνολογίες, το σκανάρισμα του χεριού μοιάζει να ανήκει σε μια τελείως διαφορετική κατηγορία, και όπως είδαμε αυτό έχει τόσο πλεονεκτήματα όσο και μειονεκτήματα.

## 2.5 AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS (AFIS)

Τα βιομετρικά συστήματα που είναι γνωστά με τον όρο Αυτοματοποιημένο Σύστημα Αναγνώρισης Δακτυλικών Αποτυπωμάτων (Α.Σ.Α.Δ.Α. ή A.F.I.S.) διενεργούν μεγάλης κλίμακας έρευνες με τη βοήθεια βάσεων δεδομένων, που έχουν αποθηκευμένες εικόνες και προσωρινά αρχεία templates από δακτυλικά αποτυπώματα. Η τεχνολογία AFIS είναι σε θέση να αναγνωρίσει ένα μεμονωμένο άτομο από μια βάση δεδομένων με εκατομμύρια εγγραφές χρησιμοποιώντας 1, 2, 4 ακόμα και 10 δακτυλικά αποτυπώματα του ατόμου. Αν και είναι πλεονασμός, οι εφαρμογές AFIS συχνά αναφέρονται ως συστήματα AFIS[1].

Τα AFIS είναι ένας τελείως διαφορετικός τύπος βιομετρικής τεχνολογίας, απ' ότι το σκανάρισμα των δαχτύλων, του προσώπου, της ίριδας κ.τ.λ. Πρόκειται για μια τεχνολογία πιο ώριμη και αποδεδειγμένη, που προϋπήρχε των υπολοίπων κι έχει εγγράψει περισσότερους χρήστες απ' ότι οι υπόλοιπες βιομετρικές τεχνολογίες μαζί. Λειτουργεί μέσα σε αυστηρά προσδιορισμένα περιβάλλοντα και, σε αντίθεση με τα περισσότερα βιομετρικά συστήματα, για τα οποία υπάρχει η αξίωση να παρέχουν αποτελέσματα μέσα σε λίγα δευτερόλεπτα, μπορεί να επιστρέψει αποτελέσματα μετά την πάροδο λεπτών, ωρών ακόμα και ημερών. Η τεχνολογία AFIS έχει βρει τη θέση της στην αγορά, κι αυτό είναι ένα ακόμη σημείο στο οποίο διαφέρει από τις περισσότερες

[1] http://en.wikipedia.org/wiki/Automated_fingerprint_identification

βιομετρικές τεχνολογίες, οι οποίες ουσιαστικά τώρα αναδύονται και ανακαλύπτουν τις εφαρμογές που τους ταιριάζουν. Η σχέση που τη συνδέει με τα ζητήματα ιδιωτικότητας είναι ιδιαίτερη, γιατί τα συστήματα AFIS χρειάζεται να αποθηκεύουν εικόνες δακτυλικών αποτυπωμάτων και να αναγνωρίζουν άτομα εξολοκλήρου από τα δακτυλικά τους αποτυπώματα. Αν και είναι απίθανο ότι μη κυβερνητικοί οργανισμοί θα χρησιμοποιήσουν ποτέ την τεχνολογία αυτή, ωστόσο είναι σημαντικό όποιοι ενδιαφέρονται για τη βιομετρική να κατανοήσουν τη φύση και τις ικανότητες των συστημάτων AFIS.

### 2.5.1 Συστατικά μέρη

Τα συστήματα AFIS αποτελούνται από συσκευές front-end ζωντανού σκαναρίσματος, από λογισμικό σε τοπικά PCs τα οποία επεξεργάζονται τα αρχικά δεδομένα, και από κεντρικά PCs που λαμβάνουν, αποθηκεύουν κι επεξεργάζονται περαιτέρω τα δεδομένα των δακτυλικών αποτυπωμάτων. Τα πιο απλά συστήματα AFIS μπορεί να περιέχονται σε μία μόνο εγκατάσταση. Συγκεκριμένα, μια πλειάδα συσκευών ζωντανού σκαναρίσματος προσαρτώνται σε τοπικά PCs, τα οποία δικτυώνονται σε ένα χαμηλού κόστους, μικρής κλίμακας AFIS, που όμως είναι ικανό να διεξάγει σύγκριση με δεκάδες χιλιάδες εγγραφές. Σε μεγαλύτερη κλίμακα, τα συστήματα AFIS αποτελούνται από εκατοντάδες σταθμούς απόκτησης δεδομένων εγκατεστημένους κατά μήκος μιας χώρας ή μιας πολιτείας, από αφοσιωμένα δίκτυα μετάδοσης των βιομετρικών δεδομένων κι από αφοσιωμένα PCs, που κοστίζουν εκατομμύρια δολάρια και μπορούν να εκτελούν δεκάδες εκατομμύρια συγκρίσεις το δευτερόλεπτο. Όσο για τα back-end AFIS αποτελούνται στην ουσία από χώρους για backup αποθήκευση, από συστατικά μέρη για έλεγχο βάσεων δεδομένων, από συστήματα ουρών αναμονής και άλλα λειτουργικά μέρη, που στο σύνολό τους θεωρούνται σαν ένα μαύρο κουτί, με την έννοια ότι εκεί εισέρχονται δαχτυλικά αποτυπώματα κι εξέρχονται αποτελέσματα.

Τα συστήματα AFIS είναι σχεδιασμένα για να ψάχνουν άτομα, τα οποία βρίσκονται εγγεγραμμένα σε μια βάση δεδομένων με εγκληματίες ή πολίτες, και να μεταδίδουν τα αποτελέσματα σε εξωτερικές υπηρεσίες. Χαρακτηριστικό παράδειγμα είναι το FBI' s Integrated AFIS (IAFIS), το οποίο περιέχει εκατομμύρια εγγραφές δακτυλικών αποτυπωμάτων εγκληματιών, είτε σε μελάνι είτε σε εικόνες. Το IAFIS δίνει απαντήσεις

σε αστυνομικά τμήματα κατά τη διενέργεια μιας έρευνας κι ακόμη ενημερώνει απευθείας ή μέσω ενδιαμέσου τους εργοδότες, κατά τον έλεγχο του ιστορικού των εργαζομένων, για το αν ένας υποψήφιος έχει συλληφθεί ή καταδικαστεί κατά το παρελθόν για κάποιο κακούργημα[1].

### 2.5.2 Τρόπος λειτουργίας

Τα AFIS δεν ξεφεύγουν από τη βασική διαδικασία της απόκτησης και επεξεργασίας εικόνων αρχικά, και εν συνεχεία της παραγωγής και σύγκρισης των templates, αντιμετωπίζουν όμως την επιπλέον πρόκληση ότι τα δεδομένα που χρησιμοποιούν πρέπει να είναι αρκετά εύρωστα, για να μπορούν να συγκριθούν με τα αντίστοιχα εκατομμυρίων χρηστών. Γι' αυτό, παρότι τα συστήματα AFIS στηρίζονται σε templates και ιδιωτικές μεθόδους ταξινόμησης, για να μπορούν να διεξάγουν έρευνες μεγάλης κλίμακας, δεν παύουν να αποθηκεύουν τις εικόνες των δαχτυλικών αποτυπωμάτων, ούτως ώστε να είναι δυνατή η χειρωνακτική σύγκριση από ειδικούς της σήμανσης.

**Απόκτηση δεδομένων**

Η εγγραφή είναι μια κρίσιμη διαδικασία στις εφαρμογές AFIS, γιατί απ' αυτήν εξαρτάται σε μεγάλο βαθμό η μετέπειτα ικανότητα ταιριάσματος με μεγάλες βάσεις δεδομένων. Καθώς ο αριθμός των δακτυλικών αποτυπωμάτων σε μια AFIS βάση μεγαλώνει, αυξάνει παράλληλα και η πιθανότητα λανθασμένου ταιριάσματος. Έτσι, για να είναι εφικτή η διενέργεια αξιόπιστων ερευνών με μεγάλες βάσεις δεδομένων, πρέπει οι εικόνες των δακτυλικών αποτυπωμάτων που αποκτώνται κατά τη διάρκεια της εγγραφής και της πιστοποίησης να είναι υψηλής ποιότητας. Αυτές οι εικόνες παραδοσιακά παρέχονται με τη μέθοδο της αποτύπωσης σε μελάνι, δηλαδή τα δακτυλικά αποτυπώματα πρώτα αποτυπώνονται σε χαρτί και στη συνέχεια μετατρέπονται σε ψηφιακή μορφή. Όμως, όλο και συχνότερα τα τελευταία χρόνια υπάρχει η δυνατότητα για απευθείας απόκτηση των αποτυπωμάτων σε ψηφιακή μορφή, μέσα από συσκευές ζωντανού σκαναρίσματος. Αυτές οι συσκευές ποικίλουν σε μέγεθος, έχοντας άλλοτε τις διαστάσεις ενός μεγάλου περιφερειακού desktop κι άλλοτε ενός φωτοτυπικού μηχανήματος, αλλά ποικίλουν και σε κόστος, με την τιμή τους να ξεκινάει από μερικές εκατοντάδες και να φτάνει τις δεκάδες χιλιάδες δολάρια. Είναι ευνόητο βέβαια, ότι η τεχνολογία ζωντανού σκαναρίσματος

[1] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

αποτελεί σημαντική βελτίωση, σε σχέση με τις παραδοσιακές μεθόδους με χρήση μελάνης, για το λόγο ότι η εκτίμηση της ποιότητας του αποτυπώματος γίνεται άμεσα και η εικόνα μπορεί να ξαναποκτηθεί, αν αυτό είναι αναγκαίο. Πράγματι, κατά τον έλεγχο του ποινικού μητρώου των εργαζομένων, ένα μεγάλο ποσοστό αποτυπωμάτων από μελάνι απορρίπτεται απ' τις κρατικές και ομοσπονδιακές υπηρεσίες, λόγω της κακής ποιότητας των εικόνων.


**Σχήμα 18.** Συστήματα ζωντανού σκαναρίσματος

Ανάλογα με την εφαρμογή, τα συστήματα μπορεί να απαιτούν από 1 έως και 10 δαχτυλικά αποτυπώματα. Συγκεκριμένα, εφαρμογές που σχετίζονται με εγκληματολογικές έρευνες και έλεγχο του ιστορικού των υπαλλήλων απαιτούν 10, ενώ εκείνες που αφορούν σε προγράμματα παροχών χρησιμοποιούν κατά κανόνα 2 εικόνες, γιατί ψάχνουν σε μικρότερες βάσεις δεδομένων. Όπως αναφέρθηκε ήδη, για την παραγωγή εύρωστων templates εγγραφής και τη διεξαγωγή αξιόπιστων ερευνών μεγάλης κλίμακας οι εικόνες πρέπει να είναι υψηλής πιστότητας, και γι' αυτό είναι απαραίτητο η διαδικασία της εγγραφής να γίνεται κάτω από επόπτευση. Στην αντίθετη περίπτωση, κανείς δεν εγγυάται ότι οι χρήστες θα είναι συνεργάσιμοι ή ότι θα γνωρίζουν τον τρόπο παροχής ποιοτικών δεδομένων. Ειδικά στις εγκληματολογικές έρευνες, συνηθίζεται να καταγράφεται με κατάλληλη περιστροφική κίνηση του δαχτύλου όλο το αποτύπωμα απ' άκρη σ' άκρη, ούτως ώστε να συγκεντρώνεται ο μέγιστος όγκος πληροφοριών. Αυτή είναι πολύ πιο δύσκολη διαδικασία απ' την απλή τοποθέτηση του δαχτύλου, γι' αυτό η εγγραφή απαιτεί την συνδρομή ενός καλά εκπαιδευμένου λειτουργού και μπορεί να διαρκέσει κάποια λεπτά. Επειδή μάλιστα οποιαδήποτε παραποίηση των αποτυπωμάτων αυξάνει την πιθανότητα ο χρήστης να διαφύγει μιας μελλοντικής έρευνας AFIS, η επίβλεψη χρησιμεύει ακόμη και για να τοποθετούνται τα δάχτυλα με τη σωστή σειρά, αφού αν ένα άτομο τοποθετήσει κρυφά τον αριστερό του μέσο, αντί για τον αριστερό του δείχτη, τότε τα δεδομένα του θα ταξινομηθούν με λάθος τρόπο.

**Επεξεργασία δεδομένων**

Σε πολλά συστήματα AFIS, οι έλεγχοι ποιότητας των δακτυλικών αποτυπωμάτων διενεργούνται προτού αυτά αποσταλούν στο τμήμα εκείνο, όπου γίνεται η κεντρική επεξεργασία. Αυτό αφενός εξασφαλίζει την αποτελεσματικότητα των ερευνών, αφετέρου επιτρέπει την άμεση επανατύπωση, για τους χρήστες που τα δεδομένα τους είναι ανεπαρκή. Τα στάδια της επεξεργασίας εικόνας που περιγράφτηκαν και για το σκανάρισμα των δαχτύλων, δηλαδή η μετατροπή των γκρίζων pixels σε άσπρα ή μαύρα, η προσαρμογή του πάχους των ραβδώσεων κ.τ.λ., λαμβάνουν χώρα και στα περισσότερα συστήματα AFIS.

**Διακριτά χαρακτηριστικά**

Το μέσο δακτυλικό αποτύπωμα έχει έναν αρκετά σημαντικό όγκο από διακριτά δεδομένα, τα οποία είναι μοναδικά για κάθε άτομο και διαφέρουν από δάχτυλο σε δάχτυλο. Η ικανότητα μάλιστα για αξιόπιστη αναγνώριση αυξάνεται εκθετικά, απ' τη στιγμή που για κάθε χρήστη συλλέγονται δεδομένα από περισσότερα του ενός δαχτυλικά του αποτυπώματα. Τα συστήματα AFIS εξάλλου, στηρίζονται σε διακριτά χαρακτηριστικά πέρα από τα minutiae και τους σχηματισμούς εκείνους που χρησιμοποιούν τα συστήματα σκαναρίσματος δαχτύλων. Ακόμη, οι κατασκευαστές των συστημάτων AFIS έχουν αναπτύξει ιδιωτικά σχήματα πιστοποίησης και αλγορίθμους ανάλυσης εικόνας, με σκοπό την ενίσχυση της διακριτικής ικανότητας των δεδομένων του δαχτυλικού αποτυπώματος. Όλες αυτές οι διαδικασίες ταιριάσματος αποτελούν πνευματική ιδιοκτησία των κατασκευαστών AFIS και είναι το επιστέγασμα της μελέτης και δουλειάς δεκαετιών, πάνω στην επεξεργασία εικόνων των δακτυλικών αποτυπωμάτων.

Η χρήση περισσότερων του ενός δαχτυλικών αποτυπωμάτων αποτελεί κλειδί για την επιτυχία των AFIS εφαρμογών, καθώς ένα μόνο αποτύπωμα δεν περιέχει αρκετά δεδομένα, ούτως ώστε να ψάξει με αξιοπιστία το σύστημα σε μια βάση δεδομένων με παραπάνω από 50.000 με 100.000 εγγραφές. Ωστόσο, δύο templates είναι συνήθως επαρκή για συστήματα που περιέχουν αρκετά εκατομμύρια εγγραφές, ενώ συστήματα με δεκάδες εκατομμύρια χρήστες απαιτούν τρία με τέσσερα δακτυλικά αποτυπώματα[1].

**Το AFIS ταίριασμα**

Οι κατασκευαστές των συστημάτων AFIS έχουν επινοήσει διάφορους τρόπους, για να διευκολύνουν την ομολογουμένως δύσκολη διαδικασία της αναζήτησης σε βάσεις δεδομένων AFIS μεγάλης κλίμακας. Πράγματι, αν και τα δακτυλικά αποτυπώματα αποτελούν αρκετά διακριτά χαρακτηριστικά, απ' τη στιγμή που μια βάση δεδομένων υπερβεί ένα συγκεκριμένο μέγεθος, είναι δύσκολο να ελεγχθεί με αξιοπιστία, ειδικά όταν η αναζήτηση γίνεται με βάση δακτυλικά αποτυπώματα χαμηλής ποιότητας. Γι' αυτό κι

[1] http://onin.com/fp/afis/afis.html

ένας από τους κύριους στόχους των κατασκευαστών είναι η μείωση του penetration rate, δηλαδή του ποσοστού της βάσης δεδομένων που ελέγχεται για κάθε νέα εγγραφή.

Ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής, τα συστήματα AFIS μπορεί να είναι διαμορφωμένα να επιστρέφουν, είτε πολλά πιθανά ταιριάσματα ή ένα μόνο πολύ ισχυρό ταίριασμα. Η πρώτη περίπτωση είναι ιδιαίτερα χρήσιμη σε εφαρμογές όπως οι εγκληματολογικές έρευνες, στις οποίες το σύστημα πρώτα επιστρέφει όλες τις εικόνες των αποτυπωμάτων που φαίνεται να ταιριάζουν, και στη συνέχεια ένας ειδικός δαχτυλικών αποτυπωμάτων αναλαμβάνει να συνεχίσει την έρευνα χειρωνακτικά. Σ' αυτές τις περιπτώσεις, ακόμα και δεκάδες αποτυπωμάτων μπορεί να επιστραφούν. Αντίθετα, σε προγράμματα κοινωνικών παροχών όπου η προκληθείσα βλάβη από μια ανεπιτυχή έρευνα είναι ασφαλώς μικρότερη, επιστρέφεται μόνο ένα ταίριασμα και μόνο στην περίπτωση που συνοδεύεται από υψηλό βαθμό σιγουριάς. Έτσι, υπάρχει κέρδος και σε χρόνο και κόστος.

Τα μεγάλης κλίμακας συστήματα AFIS μπορεί να είναι αρκετά ακριβά και πολύπλοκα, και να απαιτούν τεράστια υπολογιστική δύναμη και ικανότητα αποθήκευσης. Για να είναι μάλιστα αποδεκτός ο χρόνος απόκρισης τους, θα πρέπει να είναι ικανά να διεξάγουν εκατομμύρια ταιριάσματα δακτυλικών αποτυπωμάτων το δευτερόλεπτο. Ας θεωρήσουμε ως ενδεικτικό το παράδειγμα ενός AFIS, που τίθεται στην υπηρεσία ενός μακροπρόθεσμου σχεδίου για την παροχή αξιόπιστων εθνικών ID καρτών. Το σύστημα αυτό μπορεί να χρειαστεί να στεγάσει 35 εκατομμύρια άτομα και 4 δακτυλικά αποτυπώματα ανά άτομο. Για να μπορέσει να εγγραφεί όλος αυτός ο πληθυσμός σε 3 με 5 χρόνια, θα πρέπει το σύστημα να επεξεργάζεται δεκάδες χιλιάδες πολίτες καθημερινά. Απ' τη στιγμή μάλιστα που το AFIS φτάσει τα 10 εκατομμύρια πολίτες, θα πρέπει να διεξάγει εκατομμύρια συγκρίσεις για κάθε νέο εγγεγραμμένο, για να ελέγχει ότι δεν έχει ήδη εγγραφεί. Όταν δε το σύστημα αγγίξει τη μέγιστη χωρητικότητά του, τότε ο αριθμός των συγκρίσεων καθημερινώς θα ισούται με δισεκατομμύρια. Συνεπώς, γίνεται αντιληπτό συνεπώς ότι αν υπάρχει επιπλέον η απαίτηση για απόκριση σε σύντομο χρονικό διάστημα, τότε οι συγκρίσεις αυτές θα πρέπει να διεξάγονται πολύ πιο σύντομα.

### 2.5.3 Εφαρμογές

Το AFIS αποτελεί την πιο διαδεδομένη εφαρμογή της βιομετρικής τεχνολογίας, που αναπτύχθηκε στα μέσα προς τέλη της δεκαετίας του ’70, με σκοπό την αυτοματοποίηση των ερευνών πάνω σε δεκάδες εκατομμύρια αποτυπώματα από μελάνι, που βρίσκονταν στα αρχεία του FBI. Χρησιμοποιείται κυρίως στην επιβολή του νόμου, και σε μικρότερο βαθμό στον έλεγχο του ιστορικού υπαλλήλων, σε δημόσια προγράμματα παροχών και σε εθνικά ID προγράμματα. Πιο αναλυτικά, η τεχνολογία AFIS έχει εφαρμογή στη λήψη αποτυπωμάτων, τόσο από συλληφθέντες υπόπτους για την εξακρίβωση της ταυτότητάς τους, όσο και από αποδέκτες παροχών για την αποφυγή διπλών εγγραφών, αλλά και από επαγγελματίες οικονομικών υπηρεσιών που ελέγχεται το ιστορικό τους. Τέλος χρησιμοποιείται και όταν ανακαλύπτονται αποτυπώματα στον τόπο ενός εγκλήματος.

Η χρήση AFIS σε εφαρμογές πολιτών, όπως σε προγράμματα κοινωνικών παροχών και εθνικών ID προγραμμάτων, αποτελεί σίγουρα μια επέκταση για τη συγκεκριμένη τεχνολογία. Κι αυτό γιατί οι έρευνες του ποινικού μητρώου συλληφθέντων υπόπτων ή υποψήφιων εργαζομένων, αποτελούν εφαρμογές στις οποίες τα συστήματα AFIS είναι γερά εδραιωμένα, σε αντίθεση με τις περιπτώσεις εκείνες που δε σχετίζονται με ζητήματα σήμανσης, και οι οποίες συνθέτουν μια αγορά που παραμένει σε μεγάλο βαθμό αναξιοποίητη. Στις επόμενες παραγράφους δίνονται μερικές από τις πιο χαρακτηριστικές AFIS εφαρμογές πολιτών[1].

**ΕΛΛΑΔΑ**

**1) Εφαρμογές AFIS στην Ελληνική Αστυνομία**

**Α.Σ.Α.Δ.Α.**

Το Αυτόματο Σύστημα Αναγνώρισης Δακτυλικών Αποτυπωμάτων (*Α.Σ.Α.Δ.Α.*) τέθηκε σε λειτουργία, στις 16 Ιανουαρίου 1996. Η προμήθεια του όλου συστήματος, έγινε μετά από μία σειρά διαπραγματεύσεων και αφού προσφέρθηκε και πρόσθετος εξοπλισμός και συγκεκριμένα ένας ακόμα σταθμός εισαγωγής στοιχείων. Η προμήθεια ενός

[1] http://www.thefullwiki.org/Automated_fingerprint_identification

συστήματος *Α.Σ.Α.Δ.Α.*, υπήρξε παλαιός στόχος του Υπουργείου Δημοσίας Τάξεως και η εγκατάστασή του στη Διεύθυνση Εγκληματολογικών Υπηρεσιών (Δ.Ε.Ε.) στην Αθήνα και τη Θεσσαλονίκη θα βοηθήσει τα μέγιστα στη δίωξη του εγκλήματος και στην αρτιότερη λειτουργία της Υπηρεσίας αυτής και της Ελληνικής Αστυνομίας γενικότερα. Η προμήθεια αφορά την τελευταία έκδοση *Α.Σ.Α.Δ.Α.* της εταιρείας AFIS 2000 και όχι το αρχικά προσφερθέν και εντάσσεται στα συστήματα ανοικτής αρχιτεκτονικής με λειτουργικό *Unix* δηλαδή μπορεί εύκολα να επεκταθεί και να συνδεθεί με ταυπόλοιπα συστήματα που λειτουργούν στο Υπουργείο Δημοσίας Τάξεως, καθώς και με άλλα *Α.Σ.Α.Δ.Α.* Το σύστημα σαρώνει τα δεκαδακτυλικά αποτυπώματα από μηχανές σάρωσης (*scanner*) και τα συγκρίνει με τα ήδη καταχωρημένα, καθώς και τα αποτυπώματα που έχουν βρεθεί στους τόπους τέλεσης εγκλημάτων. Οι σχετικές βολιδοσκοπήσεις και η έρευνα αγοράς για την προμήθεια αυτού του συστήματος, είχαν αρχίσει από 1988. Οι διαδικασίες προμήθειάς του από την Ελληνική Αστυνομία ξεκίνησαν ουσιαστικά στις 12 Οκτωβρίου 1992, με την ανακοίνωση της σχετικής προκήρυξης[1].

Στις 31 Σεπτεμβρίου 1993, υπέβαλλαν τεχνικές και οικονομικές προσφορές τρεις εταιρείες:

• Η Γαλλική <Morpho>, που συνεργάζεται στην Ελλάδα με την IBM και την Ελληνική Επιστημονική.

• Η Αμερικάνικη <Printrak> που στην Ελλάδα συνεργάζεται με την <Dec> και την <Information Dynamics> και

• η Ιαπωνική <Nec>, που στην Ελλάδα, συνεργάζεται με την <Bull>.

Το Σεπτέμβριο του 1994 τελείωσε η αξιολόγηση των τεχνικών προσφορών των τριών εταιρειών και διενεργήθηκαν δοκιμαστικοί έλεγχοι των συστημάτων στις Ηνωμένες Πολιτείες Αμερικής. Η Επιτροπή Αξιολόγησης, πρότεινε την απόρριψη των τεχνικών προσφορών των εταιρειών <Morpho> και <Nec> και το άνοιγμα της οικονομικής προσφοράς μόνο της εταιρείας <Printrak>. Στις 13 Ιανουαρίου 1995 αποφασίσθηκε το άνοιγμα της οικονομικής προσφοράς της Printrak και η Επιτροπή Αξιολόγησης

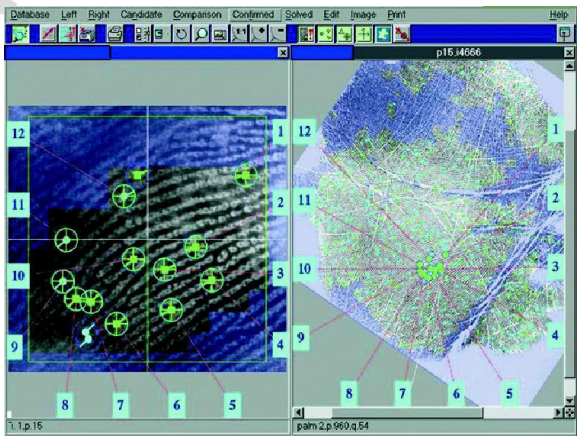
[1]http://www.hellenicpolice.gr/index.php?option=ozo_content&perform=view&id=48&Itemid=0&lan

πρότεινε την προμήθεια του συστήματος, αλλά στην τελευταία έκδοσή του που κυκλοφορούσε στην αγορά, σύμφωνα με γνωστοποίηση της εταιρείας προς το Υπουργείο Δημόσιας Τάξεως, όπως υποχρεούτο από τις τεχνικές προδιαγραφές. Στο σύστημα μέχρι σήμερα έχουν καταχωρηθεί τα αποτυπώματα *315.159* ατόμων. Το σύστημα χρησιμοποιείται διεθνώς από τις Αστυνομικές Υπηρεσίες και είναι πολύτιμο στην εξακρίβωση στοιχείων ταυτότητας και στην διαλεύκανση εγκληματικών πράξεων από τα τμήματα δακτυλικών αποτυπωμάτων που εγκαταλείπονται από τους δράστες στον τόπο του εγκλήματος. Η τιμή αγοράς και εγκατάστασης του συστήματος, με βάση τη σύμβαση που υπεγράφη, ανήλθε στο ποσό των 613.800.000 δραχμών. Η τιμή αγοράς του *Α.Σ.Α.Δ.Α.* με τελική έκπτωση 50 %, επετεύχθη μετά από σκληρές διαπραγματεύσεις με την προμηθεύτρια εταιρεία.

**AFIS**

Το Υπουργείο Προστασίας του πολίτη έχει προκυρήξει σειρά έργων, μέσω της "ΚτΠ" Α.Ε, και αναμένεται η κατάθεση προσφορών για την εγκατάσταση Συστήματος Αναγνώρισης Δακτυλικών Αποτυπωμάτων (AFIS).

Κατά τη διενέργεια του Διεθνούς Ανοικτού Διαγωνισμού με Δημοσίευση της υπ' αρ. 5300/25.05.2011 Διακήρυξης, την 14.07.2011, για το έργο «Ψηφιακές Υπηρεσίες Κοινής Ωφέλειας για την καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας», του Προγράμματος «Ψηφιακή Σύγκλιση», συνολικού προϋπολογισμού ενός εκατομμυρίου τριακοσίων πενήντα χιλιάδων ευρώ (1.350.000 ευρώ), έχουν υποβληθεί προσφορές από οκτώ εταιρείες.



Ηλεκτρονικό δίκτυο αναγνώρισης των πολιτών μέσω δακτυλικών αποτυπωμάτων σχεδιάζει το Υπουργείο Προστασίας του Πολίτη με την προμήθεια του κατάλληλου τεχνολογικού λογισμικού που θα ενώνει όλες τις πύλες εισόδου της χώρας, αλλά και το σύνολο των αστυνομικών διευθύνσεων με ένα κέντρο δεδομένων όπου θα είναι αποθηκευμένα τα δακτυλικά αποτυπώματα όλων των Ελλήνων αλλά και των αλλοδαπών που ζουν στη χώρα μας.

Το πρόγραμμα που έχει τίτλο «Ηλεκτρονική Υπηρεσία Ταυτοποίησης και Αναγνώρισης Πολιτών» θα έχει τη δυνατότητα σύνδεσης με άλλες ψηφιακές υπηρεσίες, όπως το ηλεκτρονικό διαβατήριο (e-passport) και την Κάρτα του Πολίτη, ώστε να επιτυγχάνεται από τις αρχές η ταχύτερη επεξεργασία δεδομένων, ενώ μελλοντικά θα μπορεί να διασυνδεθεί και με φορείς όπως το Εθνικό Σύστημα Υγείας και κοινωνικές υπηρεσίες.

Σύμφωνα με κύκλους του Υπουργείου Προστασίας του Πολίτη, μια εξελιγμένη μορφή της ηλεκτρονικής ταυτοποίησης θα θυμίζει αμερικανική αστυνομική ταινία, όπου ο «ύποπτος» βάζοντας την παλάμη του επάνω στην οθόνη αφής, με την οποία θα είναι εφοδιασμένος ο αστυνομικός, ταυτόχρονα θα εμφανίζονται όλες οι πληροφορίες με τις οποίες θα είναι εφοδιασμένη μία γιγάντια βάση δεδομένων.

Με τη διασύνδεση μάλιστα των αστυνομικών αρχείων, με βάσεις ιατρικών, οικονομικών και φορολογικών δεδομένων, μπορεί εύκολα να αναλογιστεί κανείς πως η εποχή του ηλεκτρονικού «μεγάλου αδελφού» είναι πλέον προ των πυλών και της ελληνικής κοινωνίας.

Παράλληλα, θα μπορεί να χρησιμοποιηθεί από τις αρμόδιες υπηρεσίες Αλλοδαπών για την ταυτοποίηση σε συνεργασία με τις χώρες της Ευρωπαϊκής Ένωσης όλων των προσώπων που εισέρχονται στη χώρα είτε νόμιμα είτε με παράνομους τρόπους.

Σύμφωνα με το σχέδιο υλοποίησης, προβλέπεται η αναβάθμιση του ελέγχου και της υλοποίησης εφαρμογών ηλεκτρονικής διακυβέρνησης στις διαδικασίες των μεταναστευτικών ροών στην Ελλάδα και την ΕΕ (νόμιμους και παράνομους), αλλά και τη χρήση συνδυασμένων (cross-checked) ηλεκτρονικών υπηρεσιών για την ταχύτερη

επεξεργασία, αξιολόγηση των αιτημάτων ασύλου και την έκδοση των αντίστοιχων νομιμοποιητικών εγγράφων.

Πρόσβαση θα έχουν η Διεύθυνση Εγκληματολογικών Ερευνών, η Διεύθυνση Αλλοδαπών, η Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας, οι Διευθύνσεις Ασφαλείας, αλλά και όλες οι αστυνομικές υπηρεσίες της ΕΛΑΣ. Με συσκευές ταυτοποίησης θα είναι εφοδιασμένοι οι αστυνομικοί, που θα μπορούν με αυτό τον τρόπο να πραγματοποιούν ελέγχους προσώπων στις πόλεις αλλά και στις περιοχές αιχμής λαθρομεταναστών, μέσω των αυτοματοποιημένων και ηλεκτρονικών υπηρεσιών που διαθέτει το σύστημα του .

Το πρόγραμμα θα ενισχύσει το ηλεκτρονικό δίκτυο που διαθέτει σήμερα η Ελληνική Αστυνομία, με το οποίο συνδέονται περίπου 1.400 σημεία σε όλη τη χώρα και μέσω αυτού υπάρχει η δυνατότητα πρόσβασης στο σύνολο των εφαρμογών. Η υφιστάμενη υποδομή της ΕΛΑΣ αποτελείται από servers, δικτυακά, PCs, εκτυπωτές, ψηφιοποιητές και αναγνώστες έξυπνων καρτών με την κωδική ονομασία «Police On Line». Το υπάρχον ηλεκτρονικό «οπλοστάσιο», βάσει του σχεδιασμού των νέων τεχνολογιών, πρόκειται να ενισχυθεί με το απαραίτητο λογισμικό και έναν σύγχρονο εξοπλισμό που θα μπορέσει να ψηφιοποιήσει όλα τα δακτυλικά αποτυπώματα από τις αστυνομικές ταυτότητες που υπάρχουν σήμερα.

Παράλληλα, στο σχεδιασμό περιλαμβάνεται και η δημιουργία 105 σταθμών εργασίας συνοριακών ελέγχων, που θα είναι εφοδιασμένοι με αυτόματες συσκευές λήψης «σταθερών δακτυλικών αποτυπωμάτων». Εκεί πάντως που δίνεται ιδιαίτερη προσοχή είναι οι ηλεκτρονικές δικλίδες ασφαλείας του συστήματος, αφού ο πάροχος του λογισμικού θα πρέπει να διασφαλίζει στις αρχές τα απαραίτητα συστήματα προστασίας της τόσο ευαίσθητης βάσης δεδομένων. Στην προκήρυξη μάλιστα του διαγωνισμού γίνεται ειδική μνεία στα θέματα ασφαλείας του δικτύου των δακτυλικών αποτυπωμάτων όπου ο ανάδοχος θα πρέπει να λάβει ειδική μέριμνα για «την προστασία των πληροφοριακών συστημάτων»[1].

[1]http://www.hellenicpolice.gr/index.php?option=ozo_content&perform=view&id=48&Itemid=0&lan

**ΕΞΩΤΕΡΙΚΟ**

**ΔΗΜΟΚΡΑΤΙΑ ΤΩΝ ΦΙΛΙΠΠΙΝΩΝ**

**2) Εφαρμογές AFIS σε κάρτες κοινωνικής ασφάλισης**

Η Δημοκρατία των Φιλιππίνων, σ' ένα πρόγραμμα με εξαετή χρονικό ορίζοντα που ξεκίνησε το 1998, δεσμεύτηκε για τη διανομή καρτών στους πολίτες με τον αριθμό εθνικής κοινωνικής τους ασφάλισης. Το πρόγραμμα αυτό αναμένεται να έχει 35 εκατομμύρια τελικούς. Οι κάρτες προσφέρουν λειτουργικότητα 1:1 αλλά και 1:N, κι έχουν σχεδιαστεί με σκοπό την αποτροπή της απάτης και τη διευκόλυνση της ασφαλούς διανομής δημόσιων αγαθών στους νόμιμους κατόχους. Επίσης περιέχουν barcodes και μαγνητικές ταινίες, καθώς και άλλα χαρακτηριστικά ασφαλείας. Σε μια παρόμοια προσπάθεια, τόσο η Νιγηρία όσο και η Αργεντινή αναμένεται χρησιμοποιήσουν μεγάλης κλίμακας εθνικά συστήματα ID, θέτοντας σ' εφαρμογή τεχνολογία AFIS για την ασφαλή εξακρίβωση της ταυτότητας των κατοίκων[1].

**Η.Π.Α.**

**3) Εφαρμογές AFIS για κοινωνικές αποδοχές**

Επίσης, πάρα πολλές πολιτείες των Ηνωμένων Πολιτειών χρησιμοποιούν τεχνολογία AFIS σε προγράμματα κοινωνικών παροχών, με στόχο την απάλειψη των διπλοεγγεγραμμένων. Το Arizona Fingerprint Imaging Program (AFIP) για παράδειγμα που τέθηκε σε εφαρμογή το 1998, απαιτεί τη λήψη δακτυλικών αποτυπωμάτων από τα άτομα που αιτούν και λαμβάνουν κοινωνικές παροχές με τη μορφή γενικής βοήθειας, οικογενειακού επιδόματος, συσσιτίου κτλ. Με παρόμοιο τρόπο, το Texas' s Lone Star Image System (LSIS) που λειτουργεί από τις αρχές του 1998, χρησιμοποιεί τεχνολογία AFIS, με σκοπό την αποτροπή της απάτης κατά τη λήψη των επιδομάτων οικογενειακής βοηθείας και τη διανομή του συσσιτίου. Τεχνολογία AFIS χρησιμοποιείται κι απ' την κομητεία του Λος Άντζελες στο σύστημα Automated Fingerprint Image Reporting and

[1] A. K. Jain, S. Prabhakar, and A. Ross, "Biometrics-Based Web Access".

Match (AFIRM), του οποίου η χρήση πρόκειται να γενικευτεί σε όλες τις Ηνωμένες Πολιτείες. Αλλά και οι κάτοικοι της Νέας Υόρκης, για να μπορούν να λάβουν όσες παροχές δικαιούνται είναι υποχρεωμένοι να εγγραφούν σ' ένα πρόγραμμα παρόμοιας τεχνολογίας, το New York State' s Public Assistance, που λειτουργεί απ' το 1995 κι εκτιμάται ότι έχει αποσοβήσει από την πολιτεία πολλά εκατομμύρια δολάρια σε απάτη. Τέλος, όσον αφορά στο πρόγραμμα περιορισμού της απάτης σε προγράμματα κοινωνικών παροχών που λειτουργεί στο Κονέκτικατ από το 1996, αυτό σχεδιάστηκε πρωτίστως για λειτουργία 1:N, αλλά μπορεί επίσης να λειτουργήσει και σε μορφή 1:1.

## 5) Εφαρμογές AFIS για τις Αστυνομικές Αρχές F.B.I.

Το FBI ανακοίνωσε την πολυαναμενόμενη μετάβαση από το Αυτοματοποιημένο Σύστημα Αναγνώρισης Αποτυπωμάτων (Automated Fingerprint Identification System AFIS), σε ένα αναβαθμισμένο, πιο γρήγορο σύστημα το οποίο και ονομάζει Advanced Fingerprint Information Technology (AFIT). Μέσω του AFIT προετοιμάζεται το έδαφος για ενίσχυση νέων τεχνικών αναγνώρισης δακτυλικών αποτυπωμάτων, όπως αναγνώριση μέσω της παλάμης ή ακόμη πιο εξειδικευμένα μέσω της κόρης του ανθρώπινου ματιού. Το επόμενο βήμα στην πολύχρονη προσπάθεια του FBI είναι το νέο σύστημα αναγνώρισης γνωστό ως Next Generation Identification System (NGI)[1].

Με το νέο σύστημα, αυξάνεται τόσο η ταχύτητα όσο και η ακρίβεια για την εύρεση των πληροφοριών που επιζητούμε", δηλώνει ο John Traxler, διαχειριστής του προγράμματος NGI, το οποίο ταιριάζει τα δακτυλικά αποτυπώματα που υποβάλλονται ηλεκτρονικά και αποθηκεύονται στη βάση δεδομένων του FBI ώστε να βοηθήσουν στην επίλυση τόσο ποινικών όσο και αστικών υποθέσεων.

Το παλιό Αυτοματοποιημένο Σύστημα Αναγνώρισης Αποτυπωμάτων AFI, χρειαζόταν περίπου δύο ώρες για να ανταποκριθεί σε μια αναζήτηση δακτυλικού αποτυπώματος για ποινικές υποθέσεις και 24 ώρες για αστικές υποθέσεις, όπως χαρακτηριστικά δηλώνει ο

[1] http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-100040/

Traxler. “Ο στόχος μας για τις ποινικές υποθέσεις είναι η εύρεση των αποτυπωμάτων να μην ξεπερνά τα 10 λεπτά και για τις αστικές τα 15 λεπτά”.

### 2.5.4 Διαφορές AFIS και σκαναρίσματος δαχτύλων

Τόσο το σκανάρισμα των δαχτύλων όσο και η τεχνολογία AFIS βασίζονται σε διακριτικά χαρακτηριστικά των δακτυλικών αποτυπωμάτων, παρόλα αυτά όμως υπάρχουν αρκετές διαφορές ανάμεσα στις αρχές λειτουργίας τους. Αυτές οι διαφορές ξεκινούν από την αρχική συσκευή απόκτησης, η οποία στα συστήματα AFIS είναι μια συσκευή ζωντανού σκαναρίσματος και όχι ένα περιφερειακό σκαναρίσματος δαχτύλων. Μερικές ακόμα διαφορές των δύο τεχνολογιών είναι οι εξής:

- Τα συστήματα σκαναρίσματος δαχτύλων παρέχουν κατά κανόνα πιστοποίηση αυθεντικότητας 1:1 και παράγουν αποφάσεις για ταίριασμα ή μη ταίριασμα μέσα σε λίγα δευτερόλεπτα. Αντίθετα, τα συστήματα AFIS εκτελούν μεγάλης κλίμακας αναγνώριση, με χρόνους απόκρισης που κυμαίνονται από μερικά λεπτά έως και ώρες.
- Συνήθως τα συστήματα σκαναρίσματος δαχτύλων αποθηκεύουν σε βάσεις δεδομένων, τα templates των δακτυλικών αποτυπωμάτων και όχι τις ίδιες τις εικόνες τους. Απεναντίας, τα συστήματα AFIS αποθηκεύουν εικόνες των αποτυπωμάτων μαζί με τα templates που χρησιμοποιούνται κατά τη διάρκεια των ερευνών.
- Τα συστήματα σκαναρίσματος δαχτύλων αποθηκεύουν τα δεδομένα σε τοπικά PCs smart, συσκευές ή cards. Στα συστήματα AFIS η αποθήκευση γίνεται σε μια κεντρική βάση δεδομένων
- Συνήθως, τα συστήματα σκαναρίσματος δαχτύλων απαιτούν για ταίριασμα 1:1 μόνο ένα template, με επιπρόσθετα templates να λαμβάνονται μόνο σε περίπτωση τραυματισμού ή λανθασμένης απόρριψης του χρήστη. Απ’ την άλλη, τα μεν συστήματα AFIS για επιβολή του νόμου χρησιμοποιούν μέχρι και 10 δακτυλικά αποτυπώματα, τα δε συστήματα AFIS πολιτών από 1 έως 4 αποτυπώματα, για μεγάλης κλίμακας ταιριάσματα 1:N.
- Τα συστήματα σκαναρίσματος δαχτύλων χρησιμοποιούν δεδομένα που προέρχονται από την επίπεδη τοποθέτηση του δαχτύλου στη συσκευή, σε

αντίθεση με τα περισσότερα συστήματα AFIS, που απαιτούν κατάλληλη περιστροφική κίνηση του δαχτύλου, ούτως ώστε να εγγραφεί στη συσκευή ζωντανού σκαναρίσματος όλο το αποτύπωμα απ' άκρη σ' άκρη.

- Τα συστήματα σκαναρίσματος δαχτύλων στηρίζονται σε σχετικά ανέξοδα περιφερειακά, που είναι σχεδιασμένα για μέτρια χρήση. Τα συστήματα AFIS χρησιμοποιούν αρκετά ακριβές συσκευές ζωντανού σκαναρίσματος, που έχουν κατασκευαστεί για βαριά χρήση.
- Τα συστήματα σκαναρίσματος δαχτύλων χρησιμοποιούνται στο δημόσιο και ιδιωτικό τομέα και σ' εφαρμογές για το σπίτι. Αντίθετα, η τεχνολογία AFIS χρησιμοποιείται σχεδόν αποκλειστικά στο δημόσιο τομέα[1].

### 2.5.5 Συμπεράσματα

Συνοψίζοντας, η τεχνολογία AFIS διαφέρει από τις άλλες βιομετρικές τεχνολογίες σε βασικά ζητήματα και γι' αυτό συνήθως δεν ανταγωνίζεται τεχνολογίες, όπως το σκανάρισμα δαχτύλων, προσώπου, ίριδας κτλ. Αντίθετα, χρησιμοποιείται σε συγκεκριμένα είδη εφαρμογών, όπου είναι και η μόνη τεχνολογία που μπορεί να λειτουργήσει αποτελεσματικά. Επειδή μάλιστα υπάρχει εξοικείωση με τα δαχτυλικά αποτυπώματα, ως ένα μέσο αναγνώρισης της ταυτότητας, κι ακόμα η ανάγκη για αναγνώριση των απρόθυμων ατόμων, είναι πολύ πιθανό ότι η τεχνολογία AFIS θα συνεχίσει να αποτελεί ιδιαίτερο κεφάλαιο για τη βιομηχανία της βιομετρικής τα προσεχή χρόνια.

[1] http://www.afis.fr/default.aspx

# 3. ΚΥΡΙΑΡΧΕΣ ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΤΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

Το κεφάλαιο αυτό έχει την ίδια δομή με το προηγούμενο, με τη μόνη διαφορά ότι οι τεχνολογίες που αναπτύσσονται στηρίζονται σε διακριτά χαρακτηριστικά της συμπεριφοράς και όχι της φυσιολογίας του ατόμου. Όπως είδαμε και στο πρώτο γενικό κεφάλαιο, τα χαρακτηριστικά της συμπεριφοράς διαφέρουν σε σχέση με τα χαρακτηριστικά της φυσιολογίας, ως προς το ότι είναι αποτέλεσμα ανθρώπινων ενεργειών. Κατά τα άλλα, μπορούν σχεδόν εξίσου καλά να διαχωρίσουν δύο άτομα μεταξύ τους. Η πιο ελπιδοφόρα βιομετρική τεχνολογία της συμπεριφοράς είναι το σκανάρισμα της φωνής, αν και άλλες τεχνολογίες, όπως το σκανάρισμα της υπογραφής και keystroke αναμένεται να βρουν τη θέση τους στην αγορά. Όλες οι παραπάνω τεχνολογίες εξηγούνται λεπτομερώς στις παρακάτω ενότητες[1].

## 3.1 ΤΟ ΣΚΑΝΑΡΙΣΜΑ ΤΗΣ ΦΩΝΗΣ

Το σκανάρισμα της φωνής επιτρέπει την πιστοποίηση της ταυτότητας ενός ατόμου, χάρη στην ανάλυση διακριτών χαρακτηριστικών της φωνής του. Είναι μια διαδικασία, που εξαρτάται και από παράγοντες της φυσιολογίας και από παράγοντες της συμπεριφοράς του ατόμου. Αυτό οφείλεται στο ότι το σχήμα των φωνητικών χορδών καθορίζει σε μεγάλο βαθμό τον ήχο της φωνής, αλλά η συμπεριφορά του ατόμου είναι εκείνη που τελικά καθορίζει τι θα ειπωθεί και με ποιο τρόπο. Η διαδικασία πιστοποίησης προϋποθέτει την απαγγελία μιας συγκεκριμένης φράσης, που σημαίνει ότι το σύστημα δεν μπορεί να αναγνωρίσει το χρήστη από τυχαία ειπωμένες λέξεις. Το σκανάρισμα της φωνής συχνά συγχέεται με την αναγνώριση λόγου (speech recognition), μια τεχνολογία που μεταφράζει τα λεγόμενα του χρήστη και η οποία δεν έχει καμία σχέση με την αναγνώριση ταυτότητας. Ωστόσο, οι δύο αυτές τεχνολογίες πολύ συχνά χρησιμοποιούνται σε συνδυασμό, για παράδειγμα η αναγνώριση λόγου μεταφράζει τη

[1] J. Markowitz Ph.D., "Voice ID, Applications and Markets for the New Millennium", October 1999.

φράση του χρήστη σε έναν αριθμό λογαριασμού, και το σκανάρισμα της φωνής επιβεβαιώνει ότι τα χαρακτηριστικά της φωνής του χρήστη ταυτίζονται με τα αποθηκευμένα.

### 3.1.1 Συστατικά μέρη

Τα συστήματα σκαναρίσματος φωνής μοιάζουν με τα συστήματα σκαναρίσματος προσώπου, ως προς το ότι μπορούν να στηριχθούν σε μεγάλο βαθμό στο υπάρχον hardware, είτε πρόκειται για μικρόφωνα, είτε για σταθερά ή κινητά τηλέφωνα κτλ. Κατά το σκανάρισμα της φωνής, ο χρήστης απαγγέλλει σε μία από τις παραπάνω συσκευές μια συγκεκριμένη φράση. Η φράση αυτή μετατρέπεται από αναλογική σε ψηφιακή μορφή, και στη συνέχεια μεταδίδεται σε ένα τοπικό ή κεντρικό PC, που φέρει το κατάλληλο λογισμικό για την παραγωγή του template.

Η τεχνολογία σκαναρίσματος φωνής συνήθως ενσωματώνεται στα ήδη υπάρχοντα συστήματα πιστοποίησης αυθεντικότητας, αντικαθιστώντας παλαιότερες μεθόδους αναγνώρισης. Όσο πιο πολύπλοκο είναι το σχήμα πιστοποίησης ενός οργανισμού, τόσο πιο δύσκολη γίνεται η ενσωμάτωση της βιομετρικής τεχνολογίας. Συνήθως, τα συστήματα σκαναρίσματος φωνής λειτουργούν σε συνδυασμό με συστήματα αναγνώρισης λόγου, ούτως ώστε η αναγνώριση του λογαριασμού και η πιστοποίηση του χρήστη να επιτυγχάνονται μέσα από μία μόνο διαδικασία.

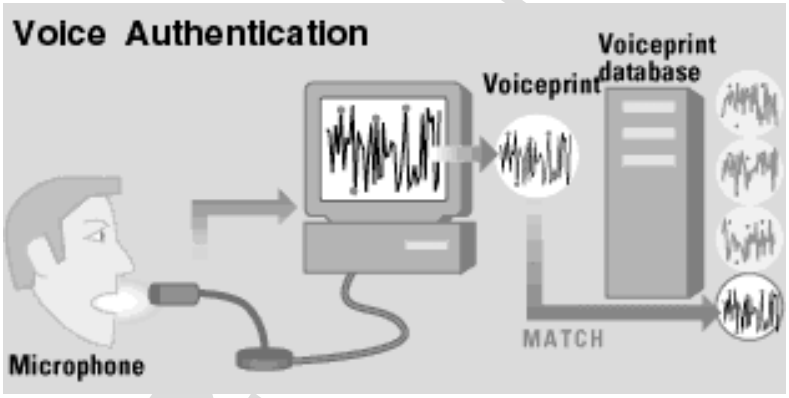
### 3.1.2 Τρόπος λειτουργίας

Η τεχνολογία σκαναρίσματος φωνής αξιοποιεί σε μεγάλο βαθμό υπάρχουσες διαδικασίες, ειδικά σε ότι έχει να κάνει με τηλεφωνικές εφαρμογές. Με εξαίρεση τη διαδικασία εγγραφής, που μπορεί αποδειχθεί κάποιες φορές άβολη για τους χρήστες, το σκανάρισμα της φωνής είναι η βιομετρική τεχνολογία που επηρεάζει και αναστατώνει λιγότερο τη λειτουργία ενός οργανισμού[1].

[1] "Voice software for security", clnet, 13 March 1997.

**Απόκτηση δεδομένων**

Κατά τη διάρκεια της εγγραφής, ο χρήστης καλείται να επιλέξει μια κωδική φράση ή να επαναλάβει μια ακολουθία αριθμών. Η φράση αυτή πρέπει να διαρκεί 1 με 1,5 δευτερόλεπτο. Αν είναι μικρότερη, τότε δεν υπάρχουν αρκετά δεδομένα για αναγνώριση, ενώ αν είναι πολύ μεγαλύτερη, υπάρχει υπερπληθώρα δεδομένων. Και στις δύο περιπτώσεις το αποτέλεσμα είναι αρνητικό από άποψη ακρίβειας. Συνήθως, υπάρχει ανάγκη αρκετών επαναλήψεων της φράσης από το χρήστη, γεγονός που επιμηκύνει τη διαδικασία εγγραφής. Όμως οι επαναλήψεις είναι απαραίτητες, γιατί συχνά μία ή περισσότερες από τις αρχικές εκφορές της φράσης απορρίπτονται, είτε γιατί ο χρήστης μιλάει πολύ δυνατά ή σιγά, είτε γιατί υπερβαίνει το περιθώριο χρόνου κτλ.




**Σχήμα 19.** Η διαδικασία πιστοποίησης φωνής

Η απόκτηση ενός σωστού δείγματος είναι δυσκολότερη με PC, απ' ότι με τηλέφωνο. Αυτό συμβαίνει, γιατί οι περισσότεροι χρήστες δεν είναι εξοικειωμένοι με τα μικροφώνων των PCs, ενώ πολλοί ντρέπονται να απευθύνουν την κωδική φράση στον υπολογιστή, μέσα σε ένα γραφείο με συναδέλφους για παράδειγμα. Γενικά, η σωστή απόκτηση των δεδομένων προϋποθέτει αφενός την τοποθέτηση του χρήστη στη σωστή απόσταση από τη συσκευή λήψης, αφετέρου την απαγγελία της φράσης την κατάλληλη χρονική στιγμή. Για να γίνουν με επιτυχία όμως τα παραπάνω, απαιτείται η εξοικείωση του χρήστη με τη διαδικασία, και λογικό είναι να υπάρχουν και αποτυχημένες προσπάθειες. Η όλη διαδικασία διευκολύνεται, όταν ο χρήστης φέρει στο κεφάλι του σύστημα με ακουστικά και μικρόφωνο. Παρόλα αυτά, εξακολουθεί να υπάρχει ένα άλλο

πρόβλημα, αυτό του περιβάλλοντος θορύβου, από κλιματιστικά, φωτοτυπικά, τηλέφωνα, συζητήσεις κτλ.

Απ' την άλλη, η πιστοποίηση ενός ατόμου με τη βοήθεια τηλεφώνου είναι μια διαδικασία που ενέχει λιγότερα προβλήματα. Οι χρήστες νιώθουν άνετα με το συγκεκριμένο μέσο, ενώ ειδικές μέθοδοι χρησιμοποιούνται για το φιλτράρισμα του θορύβου των τηλεφωνικών γραμμών. Τα πράγματα είναι ελαφρώς χειρότερα με την κινητή τηλεφωνία, λόγω αλλοίωσης του ήχου, διακοπών στην επικοινωνία, δημιουργίας ηχούς και άλλων συναφών προβλημάτων.

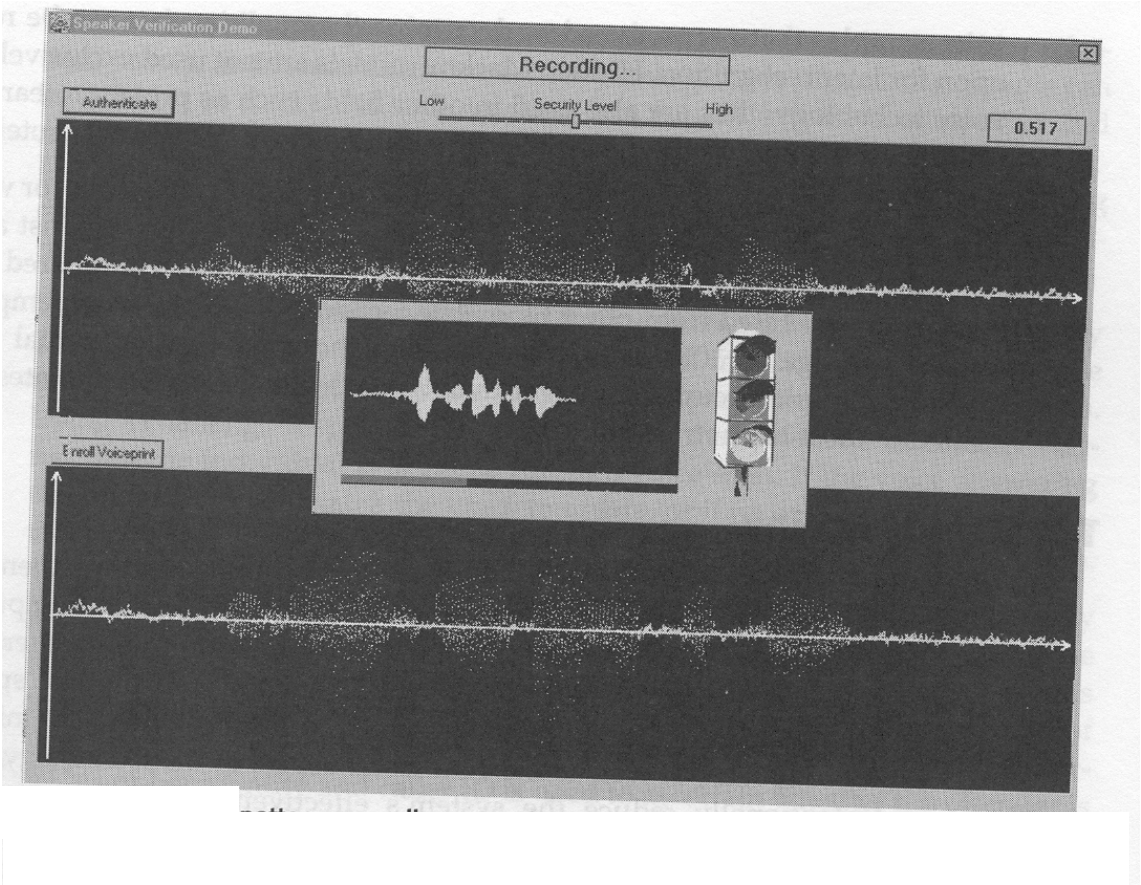
Γενικά, το σκανάρισμα της φωνής μπορεί να βασιστεί στη χρήση μιας οποιασδήποτε ακουστικής συσκευής, η απόδοση όμως του συστήματος ποικίλει, ανάλογα με την ποιότητα του ακουστικού σήματος που εκπέμπει η συσκευή. Για λόγους απόδοσης, συνήθως η ίδια συσκευή χρησιμοποιείται και στην εγγραφή και στην πιστοποίηση.

**Επεξεργασία δεδομένων**

Πριν τη δημιουργία του template, όλα τα συστήματα σκαναρίσματος φωνής επεξεργάζονται τις ηχογραφημένες φράσεις. Η επεξεργασία αυτή ξεκινάει με την εξάλειψη των κενών που υπάρχουν στην αρχή και το τέλος της ηχογράφησης, ούτως ώστε να παραμείνει μόνο η κωδική φράση, και ολοκληρώνεται με το φιλτράρισμα των συχνοτήτων εκείνων, που προκαλούνται από τη χρήση της τηλεφωνικής συσκευής ή του μικροφώνου.

**Διακριτά χαρακτηριστικά**

Η τεχνολογία σκαναρίσματος φωνής διεξάγει μετρήσεις σε ποιοτικά χαρακτηριστικά της φωνής, ορισμένα από τα οποία δε γίνονται αντιληπτά από τον άνθρωπο. Έτσι, πέρα από τον τόνο και τη συχνότητα, οι αλγόριθμοι σκαναρίσματος της φωνής μετρούν μεταβλητές, όπως η ένταση, η έκταση και η ρινική καθαρότητα, υπολογίζουν συντελεστές γραμμικής πρόβλεψης και παράγουν φασματογράμματα, ως συναρτήσεις του χρόνου, της συχνότητας και της ενέργειας.




**Σχήμα 20.** Οι σχηματισμοί της φωνής

Ένα στοιχείο με ιδιαίτερη σημασία, είναι ότι πολλά απ' αυτά τα χαρακτηριστικά που χρησιμοποιούνται για την παραγωγή του template, μπορούν να παραχθούν μόνο από την ανθρώπινη φωνή και όχι από ηχογραφήσεις της, ακόμα κι όταν αυτές είναι υψηλής πιστότητας. Επειδή μάλιστα η ηχογράφηση εισάγει και μη ανθρώπινα στοιχεία, η πιθανότητα κάποιος να παραβιάσει το σύστημα, ηχογραφώντας και αναπαράγοντας τη φωνή κάποιου άλλου (replay attacks – επιθέσεις επανάληψης), αν και δεν μπορεί να αποκλειστεί, τουλάχιστον μειώνεται σημαντικά.

### 3.1.3 Εφαρμογές

Το σκανάρισμα της φωνής δεν έχει χρησιμοποιηθεί τόσο ευρέως, όσο άλλες βιομετρικές τεχνολογίες, παρότι πληροί κάποιες βασικές προϋποθέσεις. Πράγματι, είναι μια τεχνολογία εύρωστη, που στηρίζεται σε υπάρχουσες συσκευές και μπορεί να καλύψει την ανάγκη της αγοράς για τηλεφωνική πιστοποίηση αυθεντικότητας. Χρησιμοποιείται σε τερματικά για επιβεβαίωση φωνής, σε πρόσβαση σε προσωπικούς τηλεφωνητές, δίκτυα ,

τηλεσυσκευές καθώς και για ξεκλείδωμα κινητών τηλεφώνων. Οι ακόλουθες υλοποιήσεις είναι ενδεικτικές για το εύρος των εφαρμογών στις οποίες μπορεί να χρησιμοποιηθεί.

Η τεχνολογία σκαναρίσματος φωνής χρησιμοποιείται σε πολλά προγράμματα επιτήρησης, ατόμων που βρίσκονται έξω από τη φυλακή με αναστολή ή υπό περιοριστικούς όρους. Το όφελος που υπάρχει από τη χρήση της συγκεκριμένης τεχνολογίας, είναι ότι μειώνονται σημαντικά οι απαιτήσεις σε πόρους και ανθρώπινο δυναμικό για τον εντοπισμό των επιτηρούμενων ατόμων, ενώ ο έλεγχος γίνεται πιο συστηματικός. Έτσι, αντιμετωπίζεται για παράδειγμα η περίπτωση, κάποιος να έχει διαφύγει από τη χώρα και αυτό να γίνεται αντιληπτό μετά από καιρό, όταν έρχεται η ώρα για το προγραμματισμένο ραντεβού με τον αξιωματικό επιτήρησης. Μια πιο απαιτητική εφαρμογή της τεχνολογίας, στα πλαίσια του ίδιου προγράμματος αφορά στον έλεγχο ατόμων, που σύμφωνα με απόφαση του δικαστηρίου τιμωρούνται με κατ' οίκον περιορισμό. Σε τακτά διαστήματα, το σύστημα τηλεφωνεί αυτόματα στο σπίτι του ατόμου και το υποβάλει σε μια διαδικασία ερωταποκρίσεων, με βάση την οποία καταλήγει σχετικά με την ταυτότητά του. Σε περίπτωση που δεν επαληθευτεί η ταυτότητα ή που κανείς δε σηκώνει το τηλέφωνο, ενεργοποιείται η κατάλληλη διαδικασία κινδύνου. Κύριοι προμηθευτές της τεχνολογίας γι' αυτά τα σωφρονιστικά προγράμματα είναι οι εταιρείες T-NETIX και Buytel.

**ΕΞΩΤΕΡΙΚΟ**

**ΝΕΑ ΥΟΡΚΗ**

**1) Εφαρμογές σκαναρίσματος φωνής για σωφρονιστικούς λόγους και σε χρηματοοικονομικούς οργανισμούς**

Ένα αρκετά παρόμοιο σύστημα απαγόρευσης της κυκλοφορίας, που στηρίζεται σε σκανάρισμα φωνής, υιοθετήθηκε πρόσφατα από το New York City Department of Corrections. Το NY DOC προμηθεύει τους νεαρούς παραβάτες με ένα pager, στον οποίο τους καλεί σε τακτά χρονικά διαστήματα μετά την ώρα απαγόρευσης. Το κάθε άτομο πρέπει να τηλεφωνήσει μέσα σε περιορισμένο χρονικό διάστημα στην υπηρεσία, που χρησιμοποιεί έλεγχο φωνής, για να ελέγξει την ταυτότητα αυτού που τηλεφωνεί και αναγνώριση κλήσης, για να διαπιστώσει αν βρίσκεται σε επιτρεπτό χώρο.

Εφαρμογές της τεχνολογίας όμως, συναντάμε και στον χρηματοοικονομικό χώρο. Το 1999, ένας βελγικός οικονομικός οργανισμός, ο Bacob, έθεσε σε λειτουργία σύστημα σκαναρίσματος φωνής, για ασφαλείς συναλλαγές μέσω τηλεφώνου. Το σύστημα αναπτύχθηκε από την Keyware με τη βοήθεια της Voxtron, που είναι μια τηλεφωνική εταιρεία. Μια παρόμοια υπηρεσία τηλεφωνικής πρόσβασης λογαριασμού με τεχνολογία SpeakerKey της Buytel, χρησιμοποιείται από την Allied Irish Bank. Στην Αυστραλία, η Timemac Solutions χάρη στην τεχνολογία σκαναρίσματος φωνής και αναγνώρισης λόγου που διαθέτει, επιτρέπει την τηλεφωνική διακίνηση μετοχών τηλεφωνικώς[1].

**ΡΩΣΙΑ**

**2) Εφαρμογές σκαναρίσματος φωνής σε χρηματοοικονομικούς οργανισμούς**

Η μεγαλύτερη τράπεζα της Ρωσίας, η Sberbank ξεκίνησε πρόσφατα την πιλοτική χρησιμοποίηση ATMs, τα οποία όμως θα διαθέτουν όπως λέγεται έναν ανιχνευτή φωνής για λόγους ασφαλείας. Πλέον, άνθρωποι που δεν έιχαν καμία σχέση με την τράπεζα, μπορούν να υποβάλλουν αίτηση για πιστωτική κάρτα, χωρίς να είναι απαραίτητη η ανθρώπινη παρέμβαση.

Επιπροσθέτως είναι σε θέση να σκανάρει το διαβατήριό σας, να καταγράψει δαχτυλικά αποτυπώματα, αλλά και να τραβήξει και 3D φωτογραφία, η οποία θα χρησιμοποιείται για αναγνώριση. Και όπως προαναφέραμε, διαθέτει λογισμικό ανίχνευσης φωνής, με το οποίο είναι δυνατή η εξέταση εάν ο συναλλασσόμενος ψεύδεται ή λέει την αλήθεια, σε μια γενικότερη προσπάθεια αποφυγής, απάτης.

Μάλιστα ο Victor M. Orlovsky από την Sberbank ανέφερε ότι το λογισμικό, επιτυγχάνει τον στόχο του με την ανίχνευση νευρικότητας στον χρήστη ή συναισθηματικών διαταραχών. Τα δεδομένα αυτά, συνδυάζονται μάλιστα με άλλα στοιχεία όπως κάποιου είδους ιστορικό, προκειμένου να καταλήξει(το ATM) σε ένα συμπέρασμα.

Δημοσιεύματα αναφέρουν, ότι η Sberbank επιδιώκει την επέκταση του δικτύου τέτοιου

[1] http://www.emory.edu/BUSINESS/et/biometric/Biometrics.htm

είδους ATMs, εάν και ακόμη δεν έχει βγεί κάποιου είδους χρονοδιάγραμμα. Πρόκειται μάλιστα για τα πρώτα μηχανήματα αυτόματης ανάληψης χρημάτων που φέρουν τέτοιου είδους τεχνολογία. Ωστόσο στην επιφάνεια ήδη έχουν αρχίσει να ξεσπούν αντιδράσεις για τη διαχείριση των συλλεχθέντων προσωπικών δεδομένων αλλά και για την παραβίαση της ιδιωτικότητας γενικότερα

**ΑΥΣΤΡΑΛΙΑ**

**3) Εφαρμογές σκαναρίσματος φωνής σε τραπεζικούς οργανισμούς**

Η National Australia Bank είναι η πρώτη τράπεζα στην Αυστραλία που χρησιμοποιεί βιομετρικά δεδομένα φωνής ως εναλλακτική λύση για PINs για τον έλεγχο ταυτότητας των πελατών και για την τηλεφωνική τραπεζική.

Η βιομετρική μέθοδος σκαναρίσματος φωνής είναι διαθέσιμη σε 3,3 εκατομμύρια ιδιώτες πελάτες του τραπεζικού ομίλου μετά από ένα μήνα μακρά εσωτερική πιλοτική εφαρμογή με 2.000 πελάτες. Η νέα υπηρεσία ασφαλείας ομιλίας θα επιτρέψει στους πελάτες να εγγράφουν το μοτίβο φωνή τους και να χρησιμοποιήσουν αυτό για έλεγχο ταυτότητας.

Ο Εντεταλμένος Γενικός Διευθυντής NAB Personal Banking, Warren Shaw, δήλωσε: Όταν οι πελάτες μας έχουν μια εναλλακτική λύση για να θυμούνται τους κωδικούς πρόσβασης, μέσω της φωνής του. Η νέα λύση ασφάλειας θα σώσει πολύ χρόνο, σύγχυση και απογοήτευση.

### 3.1.4 Πλεονεκτήματα

Τα πλεονεκτήματα του σκαναρίσματος φωνής σχετίζονται με την ιδιαίτερη φύση της συγκεκριμένης τεχνολογίας και τη σχέση που έχει με ορισμένες υπάρχουσες διαδικασίες.

**Δυνατότητα εκμετάλλευσης της υποδομής σε τηλεπικοινωνίες**

Μια από τις μεγαλύτερες δυσκολίες στην υλοποίηση των υπολοίπων βιομετρικών συστημάτων, είναι η ανάγκη ανάπτυξης συσκευών hardware για απόκτηση δεδομένων. Αυτό το πρόβλημα παρακάμπτεται με το σκανάρισμα της φωνής, το οποίο γενικά δεν απαιτεί την εγκατάσταση νέου hardware στο χώρο του χρήστη ή αλλού. Αυτό ισχύει ιδίως για τις τηλεφωνικές εφαρμογές και τις εφαρμογές πρόσβασης σε λογαριασμούς, οι οποίες μπορούν να βασιστούν στην υπάρχουσα υποδομή σε τηλεπικοινωνίες. Έτσι, χάρη στη δυνατότητα εκμετάλλευσης των συσκευών και των γραμμών του τηλεφώνου, στην ουσία τίθενται στη διάθεση του κοινού εκατομμύρια συσκευές πιστοποίησης αυθεντικότητας. Από την άλλη, το ίδιο το σύστημα σκαναρίσματος φωνής λειτουργεί κυρίως σα μια υπορουτίνα, που δρομολογεί τα τηλεφωνήματα, ανάλογα με τη ληφθείσα απόφαση για χορήγηση πρόσβασης.

**Συνδυασμένη χρήση με συστήματα αναγνώρισης λόγου και πιστοποίηση verbal account**

Η τεχνολογία σκαναρίσματος φωνής μπορεί να στηριχθεί στις υπάρχουσες διαδικασίες για πιστοποίηση ταυτότητας και για πρόσβαση λογαριασμών, απαλείφοντας την ανάγκη εισαγωγής πολύπλοκων ή ανεπιθύμητων σεναρίων πιστοποίησης αυθεντικότητας. Τα συστήματα αυτόματης τηλεφωνίας (automated telephone systems) με αναγνώριση λόγου βρίσκονται πλέον παντού, γιατί εξοικονομούν χρήματα για την επιχείρηση, λόγω της μείωσης του αριθμού των υπαλλήλων που απαιτούνται για τη λειτουργία των τηλεφωνικών κέντρων. Το σκανάρισμα της φωνής και η αναγνώριση λόγου μπορούν να λειτουργήσουν ταυτόχρονα με την ίδια έκφραση, κι έτσι οι δύο τεχνολογίες μπορούν να συμπλεύσουν χωρίς πρόβλημα. Το σκανάρισμα της φωνής μπορεί να λειτουργήσει σαν ένας αξιόπιστος μηχανισμός πιστοποίησης της ταυτότητας για τα συστήματα αυτόματης τηλεφωνίας, προσθέτοντας ασφάλεια σε αυτοματοποιημένες συναλλαγές μέσω τηλεφώνου και ιδιαίτερα σε εφαρμογές που αφορούν στην υγεία ή την οικονομία.

Οι παραδοσιακές μέθοδοι πιστοποίησης μέσω τηλεφώνου απαιτούν από το χρήστη την παροχή προσωπικών πληροφοριών. Αυτές οι πληροφορίες όμως, μπορεί να προέρχονται από οποιοδήποτε άτομο είναι σε θέση να τις γνωρίζει. Σ' αυτές τις περιπτώσεις το σκανάρισμα της φωνής μπορεί να λειτουργήσει ως ένας εναλλακτικός τρόπος ενίσχυσης

της ιδιωτικότητας, αντί της διενέργειας εκτενέστερων ερωτήσεων. Αλλά ακόμα και στις περιπτώσεις, όπου το σύστημα είναι σχεδιασμένο απλά για τον περιορισμό του προς διαχείριση φόρτου εργασίας, το σκανάρισμα της φωνής μπορεί να λειτουργήσει αποτελεσματικά. Κι αυτό γιατί οι χρήστες που δεν πιστοποιούνται, δρομολογούνται από το σύστημα στις παραδοσιακές, χειρωνακτικές διαδικασίες πιστοποίησης. Ακόμα κι αν το ποσοστό των χρηστών που εισέρχονται οικειοθελώς στο σύστημα είναι συγκριτικά μικρό, το κέρδος από άποψης διαχείρισης είναι μεγάλο, γιατί όποιος χρήστης πιστοποιείται με επιτυχία από το αυτοματοποιημένο σύστημα πιστοποίησης απαλλάσσει το σύστημα από διαχειριστικό φόρτο.

**Αντοχή στις επιθέσεις**

Όσοι δε γνωρίζουν σε βάθος την τεχνολογία σκαναρίσματος φωνής, δεν τη θεωρούν ως μια ιδιαίτερα ασφαλή τεχνολογία. Στην πραγματικότητα όμως, υπάρχουν συστήματα σκαναρίσματος φωνής, που είναι εξαιρετικά ανθεκτικά σε επιθέσεις, περισσότερο μάλιστα απ' ότι τα συστήματα σκαναρίσματος δαχτύλων. Αυτό δεν οφείλεται τόσο στη δυσκολία του επιτιθέμενου να μαντέψει τη μυστική φράση – παρότι αυτός είναι ένας παράγοντας που ενισχύει σημαντικά την ασφάλεια του συστήματος – όσο στα πλεονεκτήματα που έχει η φύση της τεχνολογίας. Πειράματα που έγιναν και στα οποία οι επιτιθέμενοι γνώριζαν την κωδική φράση, απέδειξαν πράγματι την αντοχή της τεχνολογίας σε προσπάθειες εξαπάτησης. Τα παραπάνω συνηγορούν στο ότι το σκανάρισμα της φωνής έχει θέση σε εφαρμογές με υψηλές απαιτήσεις σε ασφάλεια.

**Απουσία αρνητικών συνειρμών**

Το σκανάρισμα της φωνής είναι μια τεχνολογία που δεν έχει χρησιμοποιηθεί σε περιπτώσεις επιβολής του νόμου, για τον εντοπισμό ατόμων και γενικά σε οποιαδήποτε εφαρμογή τύπου Big Brother. Γι' αυτό δεν προκαλεί αρνητικούς συνειρμούς και συναισθήματα, όπως προκαλεί για παράδειγμα το σκανάρισμα των δαχτύλων ή του προσώπου. Γενικά, δεν υπάρχει ο φόβος ότι η τεχνολογία αυτή μπορεί να αποτελέσει το μέσο για τον εντοπισμό και την παρακολούθηση ατόμων. Κι αυτό ενισχύεται απ' το γεγονός ότι στα συστήματα σκαναρίσματος φωνής η αναγνώριση εξαρτάται άμεσα και από την ειπωθείσα φράση, όχι μόνο απ' τη φωνή. Συνεπώς, η συγκεκριμένη τεχνολογία υπερνικάει ένα πολύ σημαντικό εμπόδιο, το φόβο παραβίασης της ιδιωτικότητας.

### 3.1.5 Μειονεκτήματα

Υπάρχουν κάποιες αδυναμίες της τεχνολογίας σκαναρίσματος φωνής, οι οποίες περιορίζουν τους χώρους στους οποίους μπορεί να χρησιμοποιηθεί με επιτυχία. Αυτές οι αδυναμίες αναπτύσσονται στις παρακάτω παραγράφους.

**Λανθασμένη αντίληψη για μειωμένη ακρίβεια**

Οι περισσότεροι χρήστες θεωρούν ότι το σκανάρισμα της φωνής είναι μια τεχνολογία επιρρεπής σε παραβιάσεις. Κατά συνέπεια, η εμπιστοσύνη με την οποία περιβάλλουν τα συστήματα αυτά είναι πολλές φορές περιορισμένη, κι αυτό έχει αντίκτυπο στο εύρος και την κρισιμότητα των εφαρμογών, στις οποίες χρησιμοποιείται η συγκεκριμένη τεχνολογία. Αυτή η δυσπιστία οφείλεται στο ότι, ενώ οι άνθρωποι χρησιμοποιούν τη φωνή ως ένα μέσο διάκρισης και αναγνώρισης, εντούτοις εύκολα ξεγελιούνται από μιμήσεις ή μαγνητοφωνήσεις. Οι μιμήσεις όμως δεν επηρεάζουν τις μηχανές, επειδή αντιγράφουν χαρακτηριστικά της συμπεριφοράς της ανθρώπινης φωνής και όχι χαρακτηριστικά της φυσιολογίας. Και όπως είδαμε και οι μαγνητοφωνήσεις δεν οδηγούν σε έγκυρη αναγνώριση. Συνεπώς, το πρόβλημα με τα συστήματα σκαναρίσματος φωνής δεν είναι θα λέγαμε οι προσπάθειες εξαπάτησης, όσο η πεποίθηση του κοινού ότι εύκολα παραβιάζονται.

Επίσης, πολλοί χρήστες εκφράζουν το φόβο ότι η φωνή τους δε θα αναγνωριστεί λόγω ασθένειας, έλλειψης ύπνου, διάθεσης κ.τ.λ. Αν και κάτι τέτοιο δεν αποκλείεται, ωστόσο τα σύγχρονα, προηγμένα συστήματα μπορούν να προσαρμοστούν με μεγάλη επιτυχία σ' όλο το εύρος των φυσιολογικών αλλαγών στη φωνή ενός ατόμου. Η άγνοια όμως για το θέμα αυτό, αρκεί για να αναστείλει τη διάδοση των συστημάτων.

**Δυσκολία χρήσης σε PCs**

Πολλά από τα προϊόντα σκαναρίσματος φωνής απευθύνονται σε εφαρμογές λογικής πρόσβασης για PCs, λειτουργώντας ανταγωνιστικά με την τεχνολογία σκαναρίσματος δαχτύλων, αλλά και πολλές άλλες τεχνολογίες. Μέχρι στιγμής όμως και παρά τη

βελτιωμένη τους απόδοση, τα συστήματα σκαναρίσματος φωνής δεν αποτελούν την καλύτερη λύση για εφαρμογές desktop. Αυτό οφείλεται στο ότι οι χρήστες δυσκολεύονται ή ντρέπονται να μιλήσουν στον υπολογιστή τους κι έτσι δεν μπορούν να παρέχουν συνεπή και ακριβή δεδομένα. Αυτή η αδυναμία μπορεί να εξαλειφθεί με το χρόνο, αν οι χρήστες συνηθίσουν να μιλούν στον υπολογιστή για άλλους λόγους, π.χ. σε εφαρμογές speech-to-text, chatting με χρήση φωνής στο Internet, τηλεφωνικές συνομιλίες κ.α. Μέχρι τότε όμως, τη μερίδα του λέοντος σε εφαρμογές desktop αναμένεται να κατέχουν άλλες τεχνολογίες.

### 3.1.6 Συμπεράσματα

Σε γενικές γραμμές, το σκανάρισμα της φωνής είναι μια τεχνολογία εύκολη στη χρήση, που αναμένεται να γιγαντωθεί κατά τα προσεχή χρόνια, χάρη σε μία εφαρμογή: την τηλεφωνική πιστοποίηση ταυτότητας.

## 3.2 ΤΟ ΣΚΑΝΑΡΙΣΜΑ ΤΗΣ ΥΠΟΓΡΑΦΗΣ

Η τεχνολογία σκαναρίσματος υπογραφής χρησιμοποιεί τα διακριτά χαρακτηριστικά της υπογραφής ενός ατόμου, για να πιστοποιήσει την ταυτότητά του. Πρόκειται για μια διαδικασία που εξετάζει συγκεκριμένα χαρακτηριστικά της υπογραφής, όπως η σειρά των σχεδιασμένων γραμμών, η ταχύτητα και η πίεση. Μέχρι στιγμής, η συγκεκριμένη τεχνολογία δεν έχει χρησιμοποιηθεί εκτεταμένα, αλλά υπάρχει η πεποίθηση ότι θα αποκτήσει εξέχοντα ρόλο στην ηλεκτρονική πιστοποίηση αυθεντικότητας εγγράφων[1].

### 3.2.1 Συστατικά μέρη

Τα συστήματα σκαναρίσματος υπογραφής αποτελούνται από συσκευές υλισμικού (hardware) για απόκτηση δεδομένων, οι οποίες είναι κατάλληλα συνδεδεμένες με το τοπικό ή κεντρικό τμήμα, όπου γίνεται η παραγωγή των templates. Οι συσκευές

[1]Masato Kawamoto, Takayuki Hamamoto, and Seiichiro Hangai,
"Improvement of On-line Signature Verification System Robust to Intersession Variability".

απόκτησης είναι πολύ εξειδικευμένες και δεν είναι αυτές που συναντάμε σε απλοϊκές εφαρμογές του εμπορίου. Έτσι, στα βιομετρικά συστήματα, υπάρχουν δύο κύρια είδη hardware για απόκτηση δεδομένων, οι ηλεκτρονικοί πίνακες και οι ηλεκτρονικές πένες. Οι πίνακες αποτελούν το συνηθέστερο μέσο συλλογής δεδομένων και είναι ειδικές ηλεκτρονικές συσκευές, που μπορούν και μετρούν την πίεση και την ταχύτητα της υπογραφής του χρήστη. Σπανιότερα, χρησιμοποιούνται για το σκανάρισμα εξειδικευμένες ηλεκτρονικές πένες, οι οποίες μετρούν τα ίδια χαρακτηριστικά γνωρίσματα με τους πίνακες, ενώ ο χρήστης υπογράφει σε κανονικό χαρτί.

Μετά την εγγραφή, η υπογραφή καθώς και οι μεταβλητές των χαρακτηριστικών της υπογραφής, μεταδίδονται σε ένα τοπικό PC για την παραγωγή του template. Ακολουθεί η διαδικασία σύγκρισης με το αποθηκευμένο template, η οποία μπορεί να γίνει είτε στο τοπικό ή σε ένα κεντρικό PC, ανάλογα με την εφαρμογή. Για εφαρμογές υπαλλήλων, όπως η εντολή αγοράς, η τοπική επεξεργασία είναι συνήθως προτιμητέα. Αντίθετα, σε εφαρμογές πελατών, όπως σε περιπτώσεις ανάληψης χρημάτων, υπάρχει ανάγκη για πιστοποίηση από μια κεντρική μονάδα, αφού ο χρήστης είναι ελεύθερος να προβεί σε ανάληψη από πολλά σημεία.

Τα αποτελέσματα από το σκανάρισμα της υπογραφής μπορούν να ενσωματωθούν σε ήδη υπάρχοντα σχήματα πιστοποίησης ή να είναι η βάση για νέες μορφές πιστοποίησης της αυθεντικότητας. Για παράδειγμα, σε ένα παραδοσιακό σενάριο πιστοποίησης συναλλαγών, το μήνυμα για εξουσιοδότηση της συναλλαγής (authorize transaction message) στέλνεται, αφού αποκτηθεί μια ηλεκτρονική υπογραφή από ένα κεντρικό PC. Αν στην παραπάνω διαδικασία ενσωματωθεί το σκανάρισμα της υπογραφής, τότε προστίθεται μια νέα ρουτίνα που δεν επιτρέπει στο μήνυμα εξουσιοδότησης της συναλλαγής να προωθηθεί, αν τα χαρακτηριστικά της υπογραφής δεν ταιριάζουν με τα αντίστοιχα αρχειοθετημένα. Σε άλλες εφαρμογές, μπορεί το ανεπιτυχές αποτέλεσμα σκαναρίσματος υπογραφής να μην αναστείλει τη συναλλαγή, αλλά απλά να καταγραφεί για ενημέρωση των ενδιαφερομένων ή για μελλοντική επίλυση. Αυτό συμβαίνει συχνά για παράδειγμα, στην πιστοποίηση εγγράφων. Ακόμη, η διαδικασία σκαναρίσματος υπογραφής μπορεί με μια απλή ενσωμάτωση στην διαδικασία login, να αντικαταστήσει προσωπικούς κωδικούς[1].

[1] Friederike D. Griess. "On-line Signature Verification", M.S. Project Report, 2000.

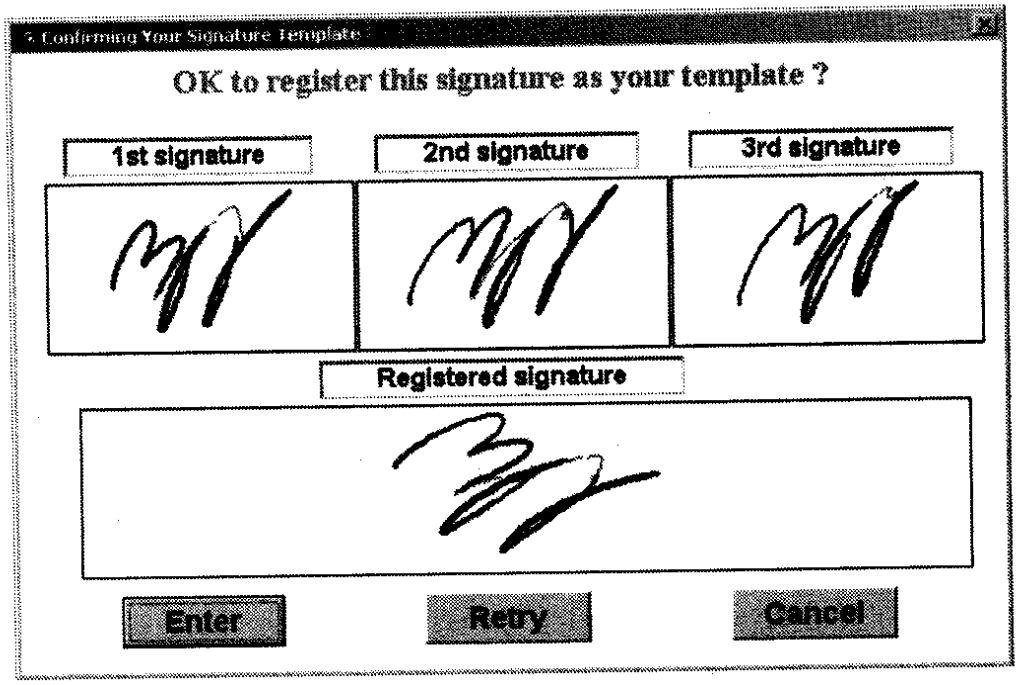
### 3.2.2 Τρόπος λειτουργίας

Σε αντίθεση με τις παραδοσιακές μεθόδους σύγκρισης υπογραφών, το σκανάρισμα της υπογραφής μετράει τη φυσική δραστηριότητα κατά τη διάρκεια της υπογραφής. Παρότι το σύστημα μπορεί παράλληλα να συγκρίνει τις ομοιότητες στην εμφάνιση ανάμεσα σε δύο υπογραφές (αυτό δηλαδή που αποκαλούμε στατική υπογραφή), εντούτοις η έμφαση δε δίνεται σ' αυτή τη σύγκριση. Ο λόγος είναι ότι υπάρχουν πολύ λίγα στοιχεία της φυσιολογίας του ατόμου, που υπεισέρχονται στην υπογραφή, κι έτσι θεωρητικά ένα άτομο θα μπορούσε να μάθει να υπογράφει ακριβώς όπως ένα άλλο άτομο. Ευτυχώς, τα χαρακτηριστικά της συμπεριφοράς, στα οποία βασίζεται η σημερινή τεχνολογία σκαναρίσματος υπογραφής είναι πολύ δύσκολο να τα μιμηθεί κανείς, γεγονός που καθιστά το έργο της παραβίασης των συστημάτων σκαναρίσματος υπογραφής εξαιρετικά δύσκολο.

**Απόκτηση δεδομένων**

Όπως είδαμε, η πλειοψηφία των τεχνολογιών σκαναρίσματος υπογραφής χρησιμοποιούν ηλεκτρονικούς πίνακες για την καταγραφή της δυναμικής της υπογραφής. Η ικανότητα των συστημάτων για σωστό ταίριασμα εξαρτάται σε πολύ μεγάλο βαθμό από τις δυνατότητες και το είδος των πινάκων, που επηρεάζουν και την απόδοση του λογισμικού σύγκρισης. Οι πίνακες high-end μετρούν την πίεση και τις αλλαγές της με εξαιρετική ακρίβεια, ενώ μπορούν να ανιχνεύουν ακόμα και τη θέση της πένας, όταν ο χρήστης την ανασηκώνει ελαφρά για να συνεχίσει την υπογραφή. Άλλοι πίνακες δεν μετρούν καθόλου την πίεση και μπορούν να μετρήσουν μονάχα τη διαφορά, όταν η πένα είναι ανασηκωμένη και όταν γράφει. Σ' αυτή την περίπτωση, η λειτουργικότητα της συσκευής περιορίζει τις μεταβλητές που μπορούν να χρησιμοποιηθούν, κι επομένως την ικανότητα σύγκρισης της τεχνολογίας. Ακόμα, η απόκτηση των δεδομένων μπορεί να γίνει με ειδικά διαμορφωμένα υπολογιστές παλάμης (PDAs). Το γεγονός αυτό μπορεί να βοηθήσει σημαντικά στην εξάπλωση της τεχνολογίας σκαναρίσματος υπογραφής, στο βαθμό που η υπογραφή αναμένεται να γίνει μια συνηθισμένη χρήση των υπολογιστών παλάμης (PDAs).

Η διαδικασία απόκτησης είναι παρόμοια για όλα τα συστήματα. Συνήθως ο χρήστης καλείται να υπογράψει πολλές φορές, για να εξασφαλιστεί ότι ασυνεπή δεδομένα από υπογραφή σε υπογραφή δε θα συμπεριληφθούν στο template εγγραφής. Οι χρήστες με πολύ μεγάλη υπογραφή είναι πιο πιθανό να αντιμετωπίσουν προβλήματα με την εγγραφή και την πιστοποίηση, γιατί η πληθώρα βιομετρικών δεδομένων δυσχεραίνει τον εντοπισμό χαρακτηριστικών που αναπαράγονται ανελλιπώς. Αλλά και οι χρήστες με πολύ μικρή υπογραφή, έχουν το φόβο λάθους αποδοχής, επειδή λιγοστεύουν οι πιθανοί συνδυασμοί δεδομένων.




**Σχήμα 21.** Το interface στο σκανάρισμα της υπογραφής

Για να έχουν υψηλή απόδοση τα συστήματα υπογραφής, πρέπει οι διαδικασίες της εγγραφής και της πιστοποίησης να διαδραματίζονται στο ίδιο περιβάλλον. Με τον όρο περιβάλλον, εννοούμε ότι έχει σημασία αν ο χρήστης είναι όρθιος ή κάθεται, αν στηρίζει τον αγκώνα του κάπου κτλ.

**Επεξεργασία δεδομένων**

Για την επεξεργασία των δεδομένων λαμβάνονται υπόψιν παράγοντες οι οποίοι συνδυάζονται με την εμφάνιση της υπογραφής, όπως η ταχύτητα, η πίεση και η σειρά των γραμμών. Συνήθως, η διάρκεια της υπογραφής κανονικοποιείται, δηλαδή επιμηκύνεται ή συρρικνώνεται σε ένα προκαθορισμένο χρονικό διάστημα, για να διευκολυνθεί η απευθείας σύγκριση. Επίσης, στοιχεία της υπογραφής με μια σχετική ανωμαλία, όπως γραμμές εκτός του έγκυρου πεδίου υπογραφής, σβήνονται. Η ίδια η εικόνα της υπογραφής μπορεί να συμπιεστεί, πριν από τη μετάδοση.

**Διακριτά χαρακτηριστικά**

Η υπογραφή ενός ανθρώπου θεωρείται από μόνη της ένα μοναδικό ανθρώπινο χαρακτηριστικό από πολύ παλιά, αν και είναι γνωστό ότι επιδέξιοι πλαστογράφοι μπορούν να δημιουργήσουν εξαιρετικά πειστικά αντίγραφά της. Ωστόσο, τα χαρακτηριστικά που μετράει το σκανάρισμα της υπογραφής είναι πολύ δύσκολο να αντιγραφούν, γιατί οφείλονται σε ενστικτώδεις μηχανισμούς συμπεριφοράς, που δεν προκύπτουν από τη μελέτη της υπογραφής ή από την παρατήρηση του ατόμου την ώρα που υπογράφει. Η δυναμική της υπογραφής που εξετάζεται με τη διαδικασία του σκαναρίσματος βασίζεται σε μία νέα σύλληψη, που δε θα μπορούσε να υλοποιηθεί, χωρίς τους ειδικούς ηλεκτρονικούς πίνακες.

Όπως όλες οι βιομετρικές τεχνολογίες, τα συστήματα σκαναρίσματος υπογραφής εξάγουν διάφορα χαρακτηριστικά από το σύνολο των υποβληθέντων πληροφοριών, για την παραγωγή του συμπιεσμένου template. Οι συγκεκριμένες λεπτομέρειες αφορούν στο συνολικό χρόνο υπογραφής, την αναλογία του χρόνου που η πένα ήταν ανασηκωμένη και έγραφε, την ταχύτητα και την πίεση που ασκήθηκε, τον αριθμό και την κατεύθυνση των μεμονωμένων γραμμών, το συνολικό μήκος της υπογραφής κ.α. Το βάρος που δίνεται σε καθέναν παράγοντα δε γνωστοποιείται, αλλά παραμένει κρυφό σε κάθε σύστημα[1].

[1] Friederike D. Griess. "On-line Signature Verification", M.S. Project Report, 2000.

**Δημιουργία template**

Επειδή οι εικόνες των υπογραφών, ακόμα και συμπιεσμένες είναι μεγαλύτερες από τα περισσότερα βιομετρικά templates, τα templates υπογραφής δεν περιέχουν εικόνες. Αντίθετα, βασίζονται σε αριθμητικές τιμές, οι οποίες αντιστοιχούν στο σημείο αρχής και τέλους, στα σημεία κατάληξης, στη σχετική πίεση σε κάθε μέρος της υπογραφής κτλ.

**Ταίριασμα templates**

Το σκανάρισμα της υπογραφής είναι μια βιομετρική τεχνολογία που – περισσότερο από κάθε άλλη – συνυπολογίζει πολλούς, ανεξάρτητους μεταξύ τους παράγοντες για να καταλήξει αν υπάρχει ταίριασμα. Για να καταφέρει να ξεγελάσει το σύστημα ένας απατεώνας, πρέπει να μιμηθεί με ακρίβεια όλους αυτούς τους παράγοντες. Για παράδειγμα, αν κάποιος υπογράψει με τη σωστή ακολουθία από γραμμές και την ενδεδειγμένη πίεση, αλλά με πολύ μικρότερη ταχύτητα απορρίπτεται.

### 3.2.3 Εφαρμογές

Λόγω της καινοτομίας της συγκεκριμένης τεχνολογίας, υπάρχουν πολύ λίγες εφαρμογές της, πέρα από τις εφαρμογές πιστοποίησης σε μεμονωμένα PCs και PDAs. Η Charles Schwab & Co. ξεκίνησε ένα πιλοτικό πρόγραμμα, που επιτρέπει την επιλεκτική χρήση του σκαναρίσματος της υπογραφής στους πελάτες με νέους λογαριασμούς. Το σύστημα είναι σχεδιασμένο με σκοπό την καλύτερη θωράκιση των συναλλαγών και τη διευκόλυνση των πελατών. Έτσι, οι χρήστες που περνάνε με επιτυχία τη διαδικασία της βιομετρικής αναγνώρισης απαλλάσσονται από οποιαδήποτε άλλη διαδικασία για πιστοποίηση της ταυτότητάς τους, ενώ η πιθανότητα αποδοχής ενός λάθους χρήστη είναι ελάχιστη. Η υλοποίηση αυτή είναι ενδεικτική των τάσεων στο χώρο του σκαναρίσματος της υπογραφής.

Τα συστήματα που υπάρχουν σήμερα σε καταστήματα και δέχονται υπογραφές πελατών για λόγους τήρησης της συμφωνίας, δε σχετίζονται με τη βιομετρική πιστοποίηση αυθεντικότητας, απλά χρειάζονται για τη συλλογή και αποθήκευση υπογραφών. Η ευρεία αποδοχή αυτών των συστημάτων αποτελεί σημαντική ένδειξη, ότι η προσθήκη σε αυτά

μιας διαδικασίας βιομετρικού ελέγχου, δε θα τύχει πολλών αντιδράσεων, ειδικά απ' τη στιγμή που εγγυάται την ασφάλεια των συναλλαγών. Όμως για να γίνει αυτό πρέπει να υπάρξει η εγκατάσταση των κατάλληλων συσκευών απόκτησης δεδομένων στους διάφορους χώρους[1].

**ΕΛΛΑΔΑ**

**1)Εφαρμογές ηλεκτρονικής υπογραφής για έκδοση κάρτας του πολίτη**

Σύμφωνα με την άποψη που επικρατεί σε κυβερνητικούς κύκλους, η «κάρτα του πολίτη», που θα αντικαταστήσει την παλαιά αστυνομική ταυτότητα, θα είναι βιομετρικού τύπου και θα περιλαμβάνει, εκτός του μικροτσίπ, ψηφιακή φωτογραφία του κατόχου της, τουλάχιστον δύο δακτυλικά του αποτυπώματα, την ηλεκτρονική του υπογραφή για συναλλαγές με διάφορες υπηρεσίες και σωρεία άλλων προσωπικών πληροφοριών (ΑΜΚΑ, ΑΦΜ), τα οποία θα τον ταυτοποιούν.

Το περιεχόμενο της νέας κάρτας προκύπτει, λένε κυβερνητικές πηγές, από τον ευρωπαϊκό κανονισμό 444/2009, που υποχρεώνει όλες τις χώρες της Ε.Ε. να καθιερώσουν εντός δύο ετών βιομετρικά στοιχεία στα διαβατήρια και όλα τα ταξιδιωτικά έγγραφά τους. Ηδη στα ελληνικά διαβατήρια έχουν ενσωματωθεί και η ψηφιακή φωτογραφία και τα δακτυλικά αποτυπώματα για όλους τους πολίτες άνω των 12 ετών.

Με δεδομένο ότι η κάρτα του πολίτη θα αντικαταστήσει την αστυνομική ταυτότητα, η οποία θεωρείται σήμερα ταξιδιωτικό έγγραφο, η κυβέρνηση θεωρεί ότι η υποχρέωση ενσωμάτωσης αυτών των στοιχείων πρέπει να επεκταθεί και στη νέα «κάρτα του πολίτη». Έτσι, δέκα χρόνια μετά την κατάργηση των δακτυλικών αποτυπωμάτων, αυτά επανέρχονται, για λόγους ασφάλειας, μέσω της Ε.Ε.![2]

Οι φόβοι αυτοί αυξάνονται αν αναλογιστεί κανείς ότι στις νέες πλαστικοποιημένες κάρτες θα υπάρχει μικροτσίπ, όπου θα αποθηκεύονται κρίσιμες πληροφορίες, καθώς και μια σειρά από προσωπικά στοιχεία των πολιτών.

[1] http://stat.tamu.edu/Biometrics/

[2] http://www.eett.gr/opencms/opencms/EETT/FAQS/DigitalSignatures/

Μέλη της Αρχής Προστασίας Προσωπικών Δεδομένων, εκτός της γενικής ανησυχίας για την έκταση εφαρμογής της «φοροκάρτας» ότι η έκταση των στοιχείων που ζητείται να καταγράφονται φαίνεται να δημιουργεί πρόβλημα μείζονος διακινδύνευσης στα προσωπικά δεδομένα των πολιτών.

**ΕΞΩΤΕΡΙΚΟ**

**Η.Π.Α.**

**1)Εφαρμογές ηλεκτρονικής υπογραφής για έκδοση διαβατηρίων**

Τα νέα διαβατήρια των πολιτών των ΗΠΑ θα περιλαμβάνουν φωτογραφίες των κατόχων τους με ψηφιακή υπογραφή, έως το τέλος του 2004. Τα νέα διαβατήρια θα περιλαμβάνουν ένα ενσωματωμένο μικροκύκλωμα, που θα αποθηκεύει μια συμπιεσμένη φωτογραφία του προσώπου του κατόχου. Αυτά τα μικροκυκλώματα έχουν σχεδιαστεί ώστε να αποτρέπουν την πλαστογραφία, ενώ κάθε ψηφιακή εικόνα έχει υπογραφεί κρυπτογραφικά ώστε να εγγυάται την αυθεντικότητά της. Αλλά και οι Ευρωπαίοι ταξιδιώτες ίσως χρειαστεί να φέρουν διαβατήρια που περιέχουν βιομετρικές πληροφορίες. Τον Ιούνιο του 2003, η ΕΕ αποφάσισε να διαθέσει 140 εκατ. ευρώ για την ανάπτυξη ενός βιομετρικού συστήματος.

**ΓΕΡΜΑΝΙΑ**

**2)Εφαρμογές ηλεκτρονικής υπογραφής για ασφαλή τηλεφωνία μέσω διαδικτύου**

Γερμανοί ερευνητές από το διάσημο Ινστιτούτο Τεχνολογίας Πληροφορικής Φραουνχόφερ ανέπτυξαν μια ψηφιακή υπογραφή, ειδικά για τη διαδικτυακή τηλεφωνία, που επιτρέπει την αρχειοθέτηση των τηλεφωνικών κλήσεων, με τρόπο νομικά δεσμευτικό. Με άλλα λόγια, είναι δυνατό πια να κλείνει κανείς συμφωνίες από το τηλέφωνο (μέσω Ίντερνετ).[1] Η καινοτομία, που βασίζεται σε λογισμικό κατάλληλο για ασφαλή τηλεφωνία μέσω διαδικτύου (VoIPS) θα επιδειχτεί για πρώτη φορά στη διεθνή έκθεση GSMA Mobile World Congress στη Βαρκελώνη. Οι πληροφορίες φέρουν κατ'

[1]http://www.businessweek.com/technology/content/jun2003/tc20030620_3373_tc119.htm

εξοχήν την Ρωσία και την Κίνα ως τις χώρες εκείνες που αναπτύσσουν εναλλακτικά δίκτυα, ώστε να παρακάμψουν το σύστημα (και τον έλεγχο) της ICANN. *Η διαδικτυακή τηλεφωνία, μέσα σε λίγα χρόνια, έχει εξελιχτεί πια από μια περιθωριακή δραστηριότητα σε καθιερωμένη τεχνολογία*. Οι περισσότερες εταιρίες τηλεπικοινωνιών παρέχουν πια επικοινωνία Voice over Internet Protocol (VoIP).

Η ολοένα στενότερη «όσμωση» του Ίντερνετ με τα τηλέφωνα επιτρέπει σταδιακά την εμφάνιση νέων μορφών επιχειρηματικής δραστηριότητας, αλλά και την ανάγκη για πιο ασφαλείς υπηρεσίες έναντι υποκλοπών κλπ. Στο πλαίσιο αυτό, οι γερμανοί ερευνητές ανέπτυξαν μια εντυπωσιακή νέα δυνατότητα: το κλείσιμο με ασφάλεια ψηφιακών συμφωνιών μέσω τηλεφώνου ανάμεσα σε δύο –ή περισσότερους- συνομιλητές.

Αν, για παράδειγμα, ένας τραπεζίτης συνομιλεί με έναν πελάτη του και καταλήξουν σε μια προφορική συμφωνία, θα είναι πια δυνατό να δώσουν δεσμευτικά νομικό χαρακτήρα στη συμφωνία τους.

Ο τραπεζίτης πατά ένα κουμπί ηχογράφησης στην τηλεφωνική συσκευή και, εφόσον συναινέσει και ο πελάτης, αρχίζει η ψηφιακή καταγραφή της συνομιλίας τους, με βάση τη νέα τεχνολογία της ψηφιακής υπογραφής. Το λογισμικό αυτομάτως «υπογράφει» τα μεταδιδόμενα δεδομένα (data) χρησιμοποιώντας τα κατάλληλα μετα-δεδομένα (metadata). Όλες οι αναγκαίες πληροφορίες αποθηκεύονται στο ενιαίο ψηφιακό αρχείο της τηλεφωνικής κλήσης και καμία αλλαγή δεν μπορεί να γίνει εκ των υστέρων μονομερώς, χωρίς να γίνει αντιληπτή.

Το «ασφαλές VoIP» (VoIPS) είναι κατάλληλο για όλες τις περιστάσεις όπου οι επιχειρήσεις, τράπεζες, ασφαλιστικές εταιρίες, νοσοκομεία, δημόσιες υπηρεσίες και άλλοι οργανισμοί θέλουν να αποθηκεύσουν τις τηλεφωνικές κλήσεις με τους πελάτες τους και γενικότερα με το συναλλασσόμενο κοινό, ώστε να αποκλείσουν αργότερα την πιθανότητα να βρεθούν προ εκπλήξεων και νομικών ασαφειών. Το νέο λογισμικό είναι δυνατό να τοποθετηθεί σε οποιοδήποτε τηλεφωνικό σύστημα IP (που χρησιμοποιεί το πρωτόκολλο του διαδικτύου).

### 3.2.4 Πλεονεκτήματα

Η τεχνολογία σκαναρίσματος υπογραφής έχει πλεονεκτήματα, που την καθιστούν ιδανική για ορισμένες εφαρμογές, στις οποίες η υπογραφή χρησιμοποιείται σαν μέρος μιας ήδη υπάρχουσας διαδικασίας και υπάρχει ανάγκη ο χρήστης να μην μπορεί να αποποιηθεί τη συμμετοχή του.

**Αποτελεσματικότητα έναντι των επιθέσεων**

Το πρώτο και κύριο ζήτημα που αντιμετωπίζει κάθε βιομετρική τεχνολογία είναι ο περιορισμός των προσπαθειών εξαπάτησης. Χάρη στη μεγάλη ποσότητα πληροφοριών που υπάρχουν σε μια υπογραφή, και τη δυσκολία μίμησης εκείνων των χαρακτηριστικών της συμπεριφοράς που καθορίζουν το αποτέλεσμα του σκαναρίσματος υπογραφών, τα αντίστοιχα συστήματα είναι εξαιρετικά ανθεκτικά σε επιθέσεις. Αν κάποιος για παράδειγμα, επιχειρήσει να αντιγράψει από πάνω μια υπογραφή, θα απορριφθεί, γιατί η εμφάνιση δεν είναι καθοριστικός παράγοντας για την αποδοχή. Έτσι, η αποδοχή του χρήστη αποτελεί εγγύηση για την ταυτότητά του, και ως εκ τούτου η τεχνολογία σκαναρίσματος της υπογραφής μπορεί να χρησιμοποιηθεί σε συναλλαγές με μεγάλη σημασία, χωρίς ο χρήστης να μπορεί να αρνηθεί ότι συμμετείχε σε αυτές.

**Αξιοποίηση υπάρχουσων διαδικασιών**

Πιθανολογείται από τις υπάρχουσες ενδείξεις, ότι το σκανάρισμα της υπογραφής θα χρησιμοποιηθεί σε μεγάλη κλίμακα στην πιστοποίηση εγγράφων, συνοδευτικά ως προς τις υπάρχουσες διαδικασίες ελέγχου υπογραφής. Κι αυτό γιατί σήμερα, η υπογραφή χρησιμοποιείται σε πολλές εφαρμογές ως μέσο ελέγχου της ταυτότητας, π.χ. σε τραπεζικές συναλλαγές για ανάληψη χρημάτων. Η προσθήκη της διαδικασίας σκαναρίσματος σ' αυτές τις εφαρμογές αναμένεται να εξαλείψει την απάτη. Χάρη μάλιστα στην ευρεία διάδοση και αξιοπιστία της υπογραφής σε πολλούς χώρους, το πεδίο των μελλοντικών εφαρμογών διευρύνεται.

Ακόμα, το σκανάρισμα της υπογραφής σε συνδυασμό με το PKI, μπορεί να χρησιμοποιηθεί για την πιστοποίηση της αυθεντικότητας, εγγράφων που έχουν μεταδοθεί

ηλεκτρονικά. Τα σημερινά, παραδοσιακά συστήματα μεταδίδουν το κάθε ηλεκτρονικό έγγραφο μαζί με μια ηλεκτρονική υπογραφή, που πιστοποιεί τον αποστολέα και εγγυάται ότι το έγγραφο δεν έχει τροποποιηθεί κατά τη διάρκεια της μετάδοσης. Αυτό το ρόλο της ηλεκτρονικής υπογραφής μπορούν να αντικαταστήσουν επάξια τα βιομετρικά συστήματα, που έχουν το πλεονέκτημα της εξοικείωσης του χρήστη με την ανθρώπινη υπογραφή, ως μέσο πιστοποίησης εγγράφων.

**Απουσία ενστάσεων για παραβίαση της ιδιωτικότητας**

Η χειρόγραφη υπογραφή είναι μια low-tech μέθοδος πιστοποίησης της αυθεντικότητας, που το κοινό έχει αποδεχθεί ως χρήσιμη και μη απειλητική. Το σκανάρισμα της υπογραφής θεωρείται προέκταση της ίδιας διαδικασίας και αντιμετωπίζεται σα μια βελτιωμένη έκδοση με μεγαλύτερη ασφάλεια, που εξακολουθεί να μην παραβιάζει την ιδιωτικότητα του ανθρώπου. Η πεποίθηση αυτή ενισχύεται απ' το ότι η τεχνολογία δεν μπορεί να χρησιμοποιηθεί για αναγνώριση, αλλά μόνο για πιστοποίηση. Αντίθετα, μια στατική υπογραφή μπορεί να χρησιμοποιηθεί για αναγνώριση, αν συγκριθεί με ένα πλήθος από υπογραφές που είναι αποθηκευμένες στη βάση δεδομένων του συστήματος, αλλά με περιορισμένη αποτελεσματικότητα.

**Δυνατότητα αλλαγής της υπογραφής**

Συχνά οι χρήστες εκφράζουν την ανησυχία τους για την αμετάβλητη φύση των βιομετρικών δεδομένων, σε σχέση με τους παραδοσιακούς τρόπους πιστοποίησης. Τα passwords για παράδειγμα, είναι προσωρινά και αυθαίρετα και μπορούν εύκολα να αντικατασταθούν ή να τροποποιηθούν, αντίθετα με τα βιομετρικά δεδομένα που δεν αλλάζουν. Εξαίρεση σ' αυτόν τον κανόνα αποτελεί η υπογραφή, αφού ο χρήστης μπορεί ηθελημένα να τροποποιήσει τον τρόπο υπογραφής του. Το όφελος απ' αυτή τη δυνατότητα είναι ότι πολλοί χρήστες που φοβούνται, παρά τα εχέγγυα αξιοπιστίας του συστήματος, για παραβίαση και υποκλοπή των προσωπικών τους δεδομένων, μπορούν να αλλάξουν τις βιομετρικές τους πληροφορίες.

### 3.2.5 Μειονεκτήματα

Η τεχνολογία σκαναρίσματος υπογραφής παρουσιάζει κάποια μειονεκτήματα, που σχετίζονται με την ίδια τη φύση της τεχνολογίας, αλλά και με τη μέθοδο απόκτησης των δεδομένων. Τα αρνητικά αυτά σημεία περιορίζουν το εύρος των εφαρμογών και το βαθμό εμπιστοσύνης των αντίστοιχων συστημάτων.

**Αυξημένα ποσοστά λάθους**

Όπως με όλες τις βιομετρικές τεχνολογίες, το σκανάρισμα της υπογραφής δε λειτουργεί εξίσου καλά για όλους τους ανθρώπους. Έτσι, χρήστες που, είτε λόγω συνήθειας, είτε λόγω κάποιας πάθησης των μυών δεν μπορούν να υπογράψουν με συνεπή τρόπο, δυσκολεύονται και στην εγγραφή και στην πιστοποίηση. Σχετικά με την εγγραφή, το σύστημα απαιτεί έναν αριθμό από υπογραφές, που να μοιάζουν αρκετά μεταξύ τους, για να μπορεί να εντοπίσει πολλά επαναλαμβανόμενα χαρακτηριστικά. Τα χαρακτηριστικά αυτά πρέπει να διατηρούνται και στην πιστοποίηση, ούτως ώστε να είναι η προσπάθεια για ταίριασμα επιτυχής. Εξυπακούεται ότι ο χρήστης πρέπει να προσέχει και να μην παραλείπει ή προσθέτει ασυναίσθητα τμήματα της υπογραφής, όπως ένα αρχικό γράμμα, ένα μεσαίο όνομα κτλ.

**Έλλειψη εξοικείωσης με την υπογραφή σε πίνακες**

Η διαδικασία υπογραφής σε έναν ηλεκτρονικό πίνακα διαφέρει από το συνηθισμένο τρόπο υπογραφής σε χαρτί. Τόσο η αίσθηση όσο και το οπτικό αποτέλεσμα είναι διαφορετικά, γεγονός που δυσχεραίνει την παροχή μιας σταθερής κάθε φορά υπογραφής. Ειδικά την πρώτη φορά που οι χρήστες έρχονται σε επαφή με τους ηλεκτρονικούς πίνακες, έχουν την τάση να υπογράφουν με τρόπο διαφορετικό και στυλιζαρισμένο, που προκαλεί προβλήματα. Καθώς όμως αναδύονται νέες τεχνολογίες που χρησιμοποιούν χαρτί και μελάνι, το πρόβλημα αυτό αναμένεται να περιοριστεί.

**Περιορισμένες εφαρμογές**

Αν και το σκανάρισμα της υπογραφής απευθύνεται πολύ καλά σε συγκεκριμένες εφαρμογές – κυρίως σ' αυτές που η υπογραφή χρησιμοποιείται ήδη για πιστοποίηση

αυθεντικότητας – υπάρχει αμφιβολία για τη δυνατότητα εξάπλωσης της τεχνολογίας σε ένα μεγάλο εύρος εφαρμογών. Είναι απίθανο δηλαδή αντίστοιχα συστήματα να χρησιμοποιηθούν στο ηλεκτρονικό εμπόριο ή για login σε PC. Ακόμα και σε περιβάλλοντα όμως όπου χρησιμοποιείται ο παραδοσιακός έλεγχος υπογραφής, οι εμπλεκόμενοι μπορεί να μην θεωρήσουν σκόπιμη την επιβάρυνση με επιπλέον φόρτο και κόστος, που συνεπάγεται το σκανάρισμα της υπογραφής, για την εγγραφή, την πιστοποίηση, το χειρισμό εξαιρέσεων κτλ. Έτσι, περιορίζονται οι αγορές στις οποίες αφορά η συγκεκριμένη τεχνολογία.

### 3.2.6 Συμπεράσματα

Συμπερασματικά, το σκανάρισμα της υπογραφής αναμένεται να διαδραματίσει μέτριο ρόλο στη βιομηχανία της βιομετρικής και να ενσωματωθεί σε εφαρμογές, στις οποίες ήδη λαμβάνει χώρα απόκτηση υπογραφών και υπάρχει ανάγκη ο χρήστης να μην μπορεί να αποποιηθεί συγκεκριμένες ενέργειες.

# 4. ΟΙ ΚΑΤΗΓΟΡΙΕΣ ΤΩΝ ΒΙΟΜΕΤΡΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

Όπως ακριβώς οι κυρίαρχες βιομετρικές τεχνολογίες διαφέρουν σε βασικά σημεία μεταξύ τους, έτσι και οι κατηγορίες βιομετρικών εφαρμογών διαφέρουν από πλευράς ασφάλειας, διευκόλυνσης, σχεδιασμού συστήματος κτλ. Η χρήση της βιομετρικής σαν ένα εργαλείο επιτήρησης για παράδειγμα, διαφέρει σημαντικά από τη χρήση της για πρόσβαση σε PCs και δίκτυα. Αυτό οφείλεται στις ιδιαίτερες απαιτήσεις και τη διαφορετική δυναμική της κάθε εφαρμογής.

Για την κατηγοριοποίηση των βιομετρικών εφαρμογών υπάρχει η οριζόντια προσέγγιση, σύμφωνα με την οποία πρέπει πρώτα να γίνει μια εκτίμηση του προβλήματος που καλείται να επιλύσει η βιομετρική, αλλά και των οφελών απ' τη χρήση της. Η προσέγγιση αυτή υπογραμμίζει καλύτερα τις διαφορές μεταξύ των βιομετρικών εφαρμογών και επιτρέπει την καλύτερη κατανόηση και αντιμετώπιση θεμάτων, όπως η ασφάλεια, η ακρίβεια και η ιδιωτικότητα. Από την οριζόντια αυτή κατάταξη προκύπτουν επτά κύριες βιομετρικές εφαρμογές: η εγκληματολογική αναγνώριση, η αναγνώριση πολιτών, εφαρμογές διοίκησης υπαλλήλων , η πρόσβαση σε PCs/ δίκτυα, η φυσική πρόσβαση/time and attendance, το ηλεκτρονικό εμπόριο/τηλεφωνία και το εμπόριο/ATM/σημείο πώλησης. Από αυτές τις εφαρμογές οι δύο πρώτες θεωρούνται ώριμες, ενώ οι υπόλοιπες τώρα αναδύονται. Σε κάθε μία από τις εφτά διαφορετικές βιομετρικές εφαρμογές, αντιστοιχεί μια σειρά από κάθετες αγορές, που έχουν κοινές απαιτήσεις σε βιομετρική αναγνώριση και πιστοποίηση.

Στα επόμενα κεφάλαια, θα αναφερθούμε σε αυτές τις επτά εφαρμογές, αφού πρώτα τις κατατάξουμε σύμφωνα με μια υψηλότερου επιπέδου κατηγοριοποίηση, ανάλογα δηλαδή με την ιδιότητα με την οποία το άτομο υποβάλλεται σε έλεγχο από το βιομετρικό σύστημα. Οι τρεις αυτές ιδιότητες είναι του πολίτη, του υπαλλήλου και του καταναλωτή κι έτσι έχουμε αντίστοιχα τις εφαρμογές πολιτών, τις εφαρμογές υπαλλήλων και τις εφαρμογές πελατών. Αυτό δε σημαίνει ότι όλες ανεξαιρέτως οι βιομετρικές χρήσεις εμπίπτουν στις προαναφερθείσες κατηγορίες εφαρμογών. Μια βιομετρική κλειδαριά για

παράδειγμα, την οποία ένα άτομο εγκαθιστά στην πόρτα του για λόγους ασφαλείας, δεν μπορεί να ενταχθεί σε καμία από τις παραπάνω κατηγορίες. Ωστόσο, οι σημαντικές υλοποιήσεις και χρήσεις της βιομετρικής μπορούν να ταξινομηθούν με βάση το παραπάνω σχήμα.

## 4.1 ΟΙ ΕΦΑΡΜΟΓΕΣ ΠΟΛΙΤΩΝ

Η επιβεβαίωση της ταυτότητας μέσα από εφαρμογές πολιτών συνήθως σχετίζεται με περιπτώσεις επιβολής του νόμου, διανομής αγαθών, χορήγησης αδειών οδήγησης κι εκλογικών βιβλιαρίων. Για να θεωρηθεί μια βιομετρική εφαρμογή ότι απευθύνεται στους πολίτες είναι απαραίτητη η ύπαρξη ενός κυβερνητικού σώματος – συνήθως μιας κρατικής ή ομοσπονδιακής υπηρεσίας – απ' όπου να εκπορεύεται η πιστοποίηση της ταυτότητας. Το σώμα αυτό πρέπει βεβαίως να είναι σε θέση να επιβάλει τη συμμόρφωση με τις αποφάσεις του βιομετρικού συστήματος. Εφαρμογές πολιτών είναι η εγκληματολογική αναγνώριση, η αναγνώριση πολιτών και η επιτήρηση.

Οι εφαρμογές πολιτών είναι από τη φύση τους πιο πιθανό να είναι υποχρεωτικές, απ' ότι οι λοιπές βιομετρικές εφαρμογές. Συνήθως κλίνουν προς την κεντρική αποθήκευση δεδομένων, τόσο σε κρατικό όσο και σε ομοσπονδιακό επίπεδο. Ακόμα, είναι εφαρμογές που διενεργούν κυρίως αναγνώριση και όχι πιστοποίηση ταυτότητας, εξυπηρετώντας την ανάγκη αποκάλυψης της ταυτότητας ενός μη συνεργάσιμου ατόμου ή εξακρίβωσης προσπαθειών για ψευδή δήλωση ταυτότητας. Συνήθως πρόκειται για εφαρμογές μεγάλης κλίμακας, που εγγράφουν και ελέγχουν σε ορισμένο χρονικό διάστημα εκατοντάδες χιλιάδες, αν όχι εκατομμύρια άτομα. Τέλος, όπως θα δούμε στο επόμενο και τελευταίο κεφάλαιο, ελλείψει βασικών προϋποθέσεων μπορούν να διολισθήσουν και να παραβιάσουν ζητήματα ιδιωτικότητας.

### 4.1.1 Εγκληματολογική αναγνώριση

Η εγκληματολογική αναγνώριση τάσσει στην υπηρεσία της τις βιομετρικές τεχνολογίες, με σκοπό την αναγνώριση ή την πιστοποίηση της ταυτότητας ενός υπόπτου, ενός κρατούμενου και γενικά ενός ατόμου σε μια εφαρμογή επιβολής του νόμου. Η βιομετρική σ' αυτή την περίπτωση εξυπηρετεί το έργο της αναγνώρισης του

εξεταζόμενου ατόμου, ούτως ώστε να δρομολογηθούν οι απαραίτητες διαδικασίες για την εφαρμογή του νόμου.

**Τυπικές εφαρμογές**

Η εγκληματολογική αναγνώριση υπήρξε η πρώτη εφαρμογή εδώ και δεκαετίες, στην οποία καθιερώθηκε η χρήση βιομετρικής τεχνογνωσίας, αν και με τρόπο μη αυτοματοποιημένο αρχικά. Τα τελευταία 25 χρόνια όμως, οι αυτοματοποιημένες έρευνες δακτυλικών αποτυπωμάτων σε τοπικές, κρατικές και εθνικές βάσεις δεδομένων, όπως και η αυτόματη επεξεργασία φωτογραφιών υπόπτων συνιστούν μεθόδους αποδεκτές και δοκιμασμένες στην εγκληματολογική έρευνα σε παγκόσμιο επίπεδο.

**Νέες τάσεις**

Η ολοένα και μεγαλύτερη ανάπτυξη στην αγορά της εγκληματολογικής αναγνώρισης οφείλεται σε μεγάλο βαθμό στην είσοδο ανέξοδων, λειτουργικών λύσεων που επεκτείνουν τη χρήση της βιομετρικής σε νέες εφαρμογές και περιβάλλοντα. Ένα μεγάλο ζήτημα στην εγκληματολογική αναγνώριση με χρήση βιομετρικής είναι η τιμή, για το λόγο ότι τα συστήματα ζωντανού σκαναρίσματος μπορεί να κοστίζουν δεκάδες χιλιάδες δολάρια. Όμως, με την εξέλιξη της τεχνολογίας και τη συγχώνευση των λύσεων σε ευνοϊκά πακέτα, αυτά τα συστήματα γίνονται όλο και πιο προσιτά στις διάφορες υπηρεσίες σε τοπικό επίπεδο. Τα πακέτα αυτά περιλαμβάνουν εκτός των άλλων ασύρματες εφαρμογές, για μετάδοση δεδομένων από απομακρυσμένες περιοχές σε κεντρικές βάσεις δεδομένων και επιτόπια αναγνώριση σε πραγματικό χρόνο. Ακόμα, υπάρχει η ανάπτυξη τοπικών βάσεων δεδομένων με εικόνες του προσώπου και των δακτυλικών αποτυπωμάτων, που λειτουργεί επίσης προς την ίδια κατεύθυνση, διευκολύνοντας τη γρήγορη αποστολή απαντήσεων από τοπικές, αντί για εθνικές ή κρατικές βάσεις δεδομένων.

Πέρα απ' την άνθιση σε τοπικό επίπεδο όμως, η ανάπτυξη λιγότερο ακριβών συστημάτων αναμένεται να γιγαντώσει τη χρήση τους και στις διεθνείς αγορές. Στις Ηνωμένες Πολιτείες βέβαια, η αγορά φαίνεται κάπως κορεσμένη, δε συμβαίνει το ίδιο όμως με πολλές αγορές εκτός των αμερικανικών συνόρων. Από την άλλη, κάτι που θα

μπορούσε να έχει τεράστιο αντίκτυπο στην αγορά είναι η είσοδος αυτοματοποιημένων λύσεων DNA. Βάσεις δεδομένων βέβαια με το DNA εγκληματιών χρησιμοποιούνται ήδη στις Ηνωμένες Πολιτείες, απλά τώρα γίνονται προσπάθειες για αυτοματοποίηση και εκσυγχρονισμό της διαδικασίας.

Πέρα από την αδιαμφισβήτητη εξέλιξη όμως, στο χώρο της εγκληματολογικής αναγνώρισης υπάρχουν και εμπόδια. Αν και θα ακουστεί παράδοξο, το βασικό εμπόδιο είναι η ίδια η επιτυχία που τα βιομετρικά συστήματα γνωρίζουν μέχρι στιγμής. Πράγματι, πολλές υπηρεσίες έχουν αγοράσει και θέσει σε εφαρμογή με μεγάλη επιτυχία συστήματα εγκληματολογικής αναγνώρισης, έτσι ώστε η μετάβαση σε νεότερα συστήματα να μη θεωρείται εγγυημένη. Αυτό όμως έχει να κάνει κυρίως με τα συστήματα ζωντανού σκαναρίσματος/AFIS και όχι τόσο με τα συστήματα σκαναρίσματος προσώπου, τα οποία παραμένουν σε μεγάλο βαθμό αναξιοποίητα.

**Χρησιμοποιούμενες βιομετρικές τεχνολογίες και κάθετες αγορές**

Στις εγκληματολογικές εφαρμογές, η τεχνολογία AFIS με συσκευές front-end ζωντανού σκαναρίσματος είναι μακράν η πιο συχνά χρησιμοποιούμενη τεχνολογία. Αυτό οφείλεται στο ότι τα δακτυλικά αποτυπώματα αποτελούν εδώ και δεκαετίες ένα καθολικά αποδεκτό μέσο αναγνώρισης, ενώ το ίδιο το FBI διαθέτει εκατομμύρια αρχεία δακτυλικών αποτυπωμάτων. Πέρα από τα AFIS, στις αστυνομικές έρευνες χρησιμοποιείται σε μικρότερο βαθμό και το σκανάρισμα προσώπου, το οποίο αξιοποιεί μεγάλες βάσεις δεδομένων με εικόνες από την προσαγωγή υπόπτων, αλλά παρέχει αποτελέσματα μικρότερης ακρίβειας. Μια ακόμη τεχνολογία, το σκανάρισμα της ίριδας, είναι πιθανό να γνωρίσει με την πάροδο του χρόνου περιορισμένη εφαρμογή στην εγκληματολογική αναγνώριση, καθώς παρέχει τάχιστη αναγνώριση με βάση στατικά βιομετρικά χαρακτηριστικά. Ωστόσο, η έλλειψη βάσεων δεδομένων της ίριδας, προς το παρόν περιορίζει τη χρήση της τεχνολογίας.

Σχετικά με τις κάθετες αγορές, οι εφαρμογές εγκληματολογικής αναγνώρισης αποτελούν τη βασική υποομάδα εφαρμογών, στο χώρο της επιβολής του νόμου. Υπάρχουν βέβαια και άλλες εφαρμογές, όπως η επιτήρηση και η φυσική πρόσβαση, που ενίοτε

χρησιμοποιούνται στα πλαίσια επιβολής του νόμου, όμως οι εγκληματολογικές εφαρμογές είναι οι μόνες που ανήκουν αμιγώς στο χώρο αυτό.

**Κόστος ανάπτυξης**

Το κόστος της εισαγωγής βιομετρικής τεχνολογίας στην εγκληματολογική αναγνώριση καταμερίζεται σε κόστος αγοράς, κόστος ενσωμάτωσης και κόστος σε επισκευή (service) και περιλαμβάνει:

- Εξειδικευμένο υλισμικό (hardware) απόκτησης δεδομένων, όπως συστήματα φωτογράφησης δακτυλικών αποτυπωμάτων.
- Συστήματα μετατροπής καρτών, που μετατρέπουν τις κάρτες με τα δακτυλικά αποτυπώματα των ατόμων σε μελάνι, σε ηλεκτρονικές βάσεις αποτυπωμάτων.
- Συστήματα ταιριάσματος δακτυλικών αποτυπωμάτων, που περιλαμβάνουν λογισμικό και υλισμικό (hardware).
- Λογισμικό για σκανάρισμα προσώπου, το οποίο κατατάσσει και να επεξεργάζεται εικόνες προσώπου.
- Ανάπτυξη, παρακολούθηση και συντήρηση των χρησιμοποιούμενων βιομετρικών συστημάτων.

Συνήθως, για την πώληση εγκληματολογικών συστημάτων αναγνώρισης συνάπτονται πολυετή συμβόλαια. Γενικά, όσο μεγαλώνει το περιβάλλον της εφαρμογής, τόσο πιο πολύπλοκο και εκτενές γίνεται το αντίστοιχο σύστημα, ενώ παράλληλα αυξάνεται και το κόστος. Για να αναφερθεί ένα ακραίο παράδειγμα, το FBI ξόδεψε πάνω από $640 εκατομμύρια σ' ένα πολυετές πρόγραμμα για την ανάπτυξη Integrated AFIS, στα πλαίσια του οποίου τροποποιήθηκαν εκατομμύρια κάρτες δακτυλικών αποτυπωμάτων, ούτως ώστε να μπορούν να ελέγχονται ηλεκτρονικά. Αντίστοιχα η πολιτεία της Οκλαχόμα σύναψε συμφωνία $5 εκατομμυρίων με την Printrak, για να χρησιμοποιεί ένα σύστημα με δυνατότητες αναγνώρισης AFIS και παλάμης[1].

[1] http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-1000850/

**Συμπεράσματα**

Όπως φαίνεται από τα παραπάνω, η εγκληματολογική αναγνώριση είναι μια αρκετά ώριμη βιομετρική εφαρμογή. Αν και υπάρχουν αρκετά εμπόδια στη χρήση της βιομετρικής σε περιοχές, όπως το ηλεκτρονικό εμπόριο ή η πρόσβαση σε PCs και δίκτυα, στις εγκληματολογικές έρευνες φαίνεται πως οι σχετικές διαδικασίες είναι γερά εδραιωμένες. Συνήθως, οι βιομετρικές λύσεις υλοποιούνται με τη μορφή προμήθειας από εξειδικευμένες εταιρείες παροχής, οι οποίες αναλαμβάνουν την εγκατάσταση, εκπαίδευση και διαμόρφωση των συστημάτων και σε πολλές περιπτώσεις ακόμα και για τη λειτουργία τους. Σχετικά με τη χρησιμοποίηση νεότερων βιομετρικών συστημάτων, π.χ. συστημάτων σκαναρίσματος προσώπου, η βασική ανησυχία έχει να κάνει με τη μακροπρόθεσμη βιωσιμότητα τους. Πράγματι, σε αντίθεση με τα συστήματα AFIS, όπου υπάρχουν πρότυπα για το ποιες συσκευές ζωντανού σκαναρίσματος είναι κατάλληλα εξοπλισμένες, μέχρι στιγμής τουλάχιστον δεν έχουν αναπτυχθεί αντίστοιχα πρότυπα λειτουργίας για τις νεότερες λύσεις.

### 4.1.2 Αναγνώριση πολιτών

Η αναγνώριση πολιτών αναφέρεται στη χρήση βιομετρικής, με σκοπό την αναγνώριση ή πιστοποίηση της ταυτότητας ατόμων, κατά την αλληλεπίδρασή τους με κυβερνητικές υπηρεσίες οι οποίες εκδίδουν κάρτες, παρέχουν κοινωνικές υπηρεσίες, επιμελούνται των διαδικασιών ψηφοφορίας, διενεργούν έλεγχο του παρελθόντος υπαλλήλων κτλ. Σ' αυτές τις περιπτώσεις, η βιομετρική χρησιμοποιείται συμπληρωματικά ή στη θέση των παραδοσιακών μεθόδων πιστοποίησης, οι οποίες κατά κανόνα στηρίζονται στην επίδειξη εγγράφων, αποδείξεων, δελτίων και άλλων πιστοποιητικών.

**Τυπικές εφαρμογές**

Με το γενικό όρο αναγνώριση πολιτών καλύπτεται ένα πλήθος επιμέρους εφαρμογών, οι οποίες αφορούν στην αλληλεπίδραση ατόμων με κυβερνητικούς οργανισμούς. Οι κυριότερες από αυτές τις εφαρμογές σχετίζονται με τη συγκρότηση αξιόπιστων εκλογικών καταλόγων, τη διανομή δημόσιων αγαθών στους δικαιούχους, τη διευκόλυνση

υπηρεσιών μετανάστευσης, την έκδοση αδειών οδήγησης και ταυτοτήτων και τον έλεγχο του ποινικού μητρώου υποψηφίων για συγκεκριμένες θέσεις.

**Νέες τάσεις**

Μιλώντας για νέες τάσεις στην αναγνώριση πολιτών, πρέπει να πούμε ότι ορισμένες απόψεις της αναγνώρισης πολιτών αναμένεται να έχουν μεγαλύτερη απήχηση σε Ευρώπη, Καναδά και Ηνωμένες Πολιτείες, ενώ κάποιες άλλες αναμένεται να υιοθετηθούν περισσότερο από την Ασία, τη Νότιο Αμερική και γενικά χώρες που τώρα αναπτύσσονται. Συνολικά, είναι πιθανό τα συστήματα αναγνώρισης πολιτών να γνωρίσουν μεγαλύτερη επιτυχία εκτός των δυτικών χωρών. Πράγματι, πολλές αναπτυγμένες χώρες αντιμετωπίζουν με αρνητική προδιάθεση ή ακόμα και εχθρότητα τα κυβερνητικά βιομετρικά συστήματα, κάτι που δε συμβαίνει με τις υπό ανάπτυξη χώρες, οι οποίες δίνουν πολύ μικρότερη έμφαση σε ζητήματα ιδιωτικότητας, χωρίς βέβαια να μπορεί να αποκλειστεί αλλαγή της στάσης του στο μέλλον.

Μια σημαντική για το μέλλον της αναγνώρισης πολιτών εξέλιξη σχετίζεται με την έκδοση ηλεκτρονικών καρτών που εξυπηρετούν παράλληλα διάφορες λειτουργίες. Οι κάρτες αυτές περιέχουν διάφορες πληροφορίες για την επαγγελματική κατάσταση του ατόμου, για επείγοντα ιατρικά θέματα κτλ. και χρησιμοποιούνται από αναπτυσσόμενες χώρες για την παροχή διαφόρων υπηρεσιών, σε μια προσπάθεια αναβάθμισης της σχέσης του κράτους με τον πολίτη. Εξαιτίας όμως των ευαίσθητων πληροφοριών και του στοιχείου της συναλλαγής, υπάρχει μεγάλη ανάγκη να διασφαλιστούν βιομετρικά αυτές οι κάρτες. Για να επανέλθουμε στις δυτικές χώρες, αυτές μέχρι στιγμής τουλάχιστον, δείχνουν για λόγους ιδιωτικότητας μια σχετική αποστροφή σε προγράμματα αναγνώρισης που βασίζονται σε ηλεκτρονικές κάρτες. Κανείς όμως δεν μπορεί να προβλέψει με ακρίβεια τα εξωτερικά γεγονότα, που ενδεχομένως προκαλέσουν ανατροπή στο σκηνικό, φέροντας τους ενδοιασμούς για θέματα ιδιωτικότητας σε δεύτερη μοίρα.

Γενικά πάντως, η αγορά θα επηρεαστεί από τις τάσεις που θα διαμορφωθούν σε δύο σημαντικές εφαρμογές αναγνώρισης πολιτών. Η πρώτη είναι η πιστοποίηση της ταυτότητας των δικαιούχων σε προγράμματα κοινωνικών παροχών και η δεύτερη η καταγραφή του εκλογικού σώματος. Η τελευταία αυτή εφαρμογή είναι πολύ σημαντική, για το λόγο ότι η πιστοποίηση της ταυτότητας αυτών που ψηφίζουν αποτελεί σημαντικό

και αναπόσπαστο τμήμα της εκλογικής διαδικασίας. Ο μόνος φόβος είναι να χρησιμοποιηθεί η βιομετρική τεχνολογία, όχι για να διευκολύνει ή να βελτιώσει τη διαδικασία εκλογής αντιπροσώπων, αλλά ως μέσο για την επιλεκτική αποθάρρυνση ψηφοφόρων. Γι' αυτό το λόγο, πρέπει η όλη διαδικασία να τύχει της ανάλογης μέριμνας.

Κλειδί όμως στην ανάπτυξη του χώρου αναγνώρισης πολιτών θα αποτελέσει και η διαθεσιμότητα συστημάτων AFIS υψηλής ικανότητας, αφού αυτή η τεχνολογία είναι η μόνη που μπορεί πραγματικά μπορεί να διεξάγει αναγνώριση 1:N και να διαχωρίσει κατηγορηματικά εκατομμύρια ατόμων. Οι βελτιώσεις στα AFIS έχουν πράγματι μειώσει το χρόνο αναζήτησης, με τα αποτελέσματα είναι εξίσου θετικά κι από πλευράς απόδοσης, οπότε θεωρείται βέβαιο ότι τα συστήματα αυτά θα εξαπλωθούν σε περιβάλλοντα απαιτήσεων.

Μοναδικό εμπόδιο μπορεί να σταθεί η πολυπλοκότητα και το κόστος ανάπτυξης αυτών των συστημάτων. Πράγματι, τα μεγάλης κλίμακας εθνικά ID προγράμματα είναι, και χωρίς τη χρήση βιομετρικής, ιδιαίτερα μαζικά, μακροχρόνια και απαιτητικά. Είναι πιθανό λοιπόν να θεωρηθεί, ότι η χρήση βιομετρικής τεχνολογίας δεν εγγυάται την επιστροφή των χρημάτων που δαπανούνται, κι ότι εμπερικλείει ζητήματα που είναι δύσκολο να αντιμετωπιστούν.

**Χρησιμοποιούμενες τεχνολογίες και κάθετες αγορές**

Οι βιομετρικές τεχνολογίες που είναι πιο πιθανό να χρησιμοποιηθούν στην αναγνώριση πολιτών είναι τα AFIS, το σκανάρισμα του προσώπου και το σκανάρισμα των δαχτυλικών αποτυπωμάτων. Οι δύο πρώτες τεχνολογίες είναι σε θέση να παράγουν μεγάλης κλίμακας αναγνώριση 1:N με κλιμακούμενα επίπεδα ακρίβειας, κόστους και ταχύτητας. Το σκανάρισμα των δαχτύλων από την άλλη αναμένεται να χρησιμοποιηθεί σε μικρότερο βαθμό, κυρίως για την πιστοποίηση της ταυτότητας σε διάφορες συναλλαγές.

Σχετικά με τις κάθετες αγορές υπάρχει μερική επικάλυψη στις εφαρμογές κυβερνητικής αναγνώρισης και κυβερνητικής χρήσης, παρότι η κυβέρνηση χρησιμοποιεί βιομετρική τεχνολογία και σε πολλούς άλλους τομείς, πέρα από την αναγνώριση πολιτών.

**Κόστος ανάπτυξης**

Τα μεγαλύτερα ποσά που ξοδεύονται για την αναγνώριση πολιτών αφιερώνονται στο σχεδιασμό και την υλοποίηση συστημάτων μεγάλης κλίμακας. Στις περισσότερες περιπτώσεις, διενεργούνται επιχειρήματα (projects) με πολυετή ορίζοντα, που αναλαμβάνουν την εγγραφή, επεξεργασία και αποθήκευση δεδομένων για εκατομμύρια πολίτες. Γενικά, το κόστος για τους οργανισμούς δεν περιορίζεται στην απόκτηση εξειδικευμένου λογισμικού και υλισμικού, αλλά πολλαπλασιάζεται από τις διάφορες υπηρεσίες υποστήριξης και επισκευής του συστήματος.

**Ζητήματα υλοποίησης**

Ορισμένοι τύποι εφαρμογών αναγνώρισης πολιτών που διεξάγουν αναγνώριση 1:N σε μεγάλη κλίμακα, μπορεί να αποδειχθούν ιδιαίτερα δύσκολοι στην υλοποίησή τους. Αν και η φύση των συστημάτων αναγνώρισης πολιτών διαφέρει ανάλογα με την περίσταση, υπάρχουν ορισμένα κοινά θέματα που πρέπει να αντιμετωπιστούν όπως η εγγραφή, η επεκτασιμότητα, η απόδοση, τα ποσοστά λάθους και η διασφάλιση της ιδιωτικότητας.

Είναι γεγονός ότι τα συστήματα αναγνώρισης πολιτών απευθύνονται σε πολλές χιλιάδες, αν όχι εκατομμύρια άτομα. Η διαδικασία εγγραφής όλων αυτών των ατόμων μπορεί να αποδειχθεί εξαιρετικά πολύπλοκη. Έτσι, για να υπάρχουν εχέγγυα αξιοπιστίας της μετέπειτα λειτουργίας του συστήματος, πρέπει η ταυτότητα κάθε ατόμου να επιβεβαιώνεται με πολύ μεγάλη βεβαιότητα, προτού εγγραφεί. Ακόμα, η ποιότητα της εγγραφής πρέπει να υπακούει σε ορισμένα πρότυπα, ούτως ώστε να διαθέτει μακροπρόθεσμη αξία. Γενικά, υπάρχουν λόγοι που υπαγορεύουν την ύπαρξη εκπαιδευμένου προσωπικού, το οποίο να υποδεικνύει στους χρήστες τον ενδεδειγμένο τρόπο εγγραφής. Έτσι, είναι απαραίτητο τα σωστά δεδομένα να παρέχονται με τη σωστή σειρά, αφού σ' ένα σύστημα που ελέγχει δύο δακτυλικά αποτυπώματα φέρ' ειπείν, μπορεί ο χρήστης να αποφύγει την αναγνώριση με υποβολή των αποτυπωμάτων με ανάποδη σειρά. Ένα ακόμα θέμα είναι το μέγεθος της αρχικής προσπάθειας που πρέπει να καταβληθεί, γιατί μπορεί να είναι τέτοιο, που να υπαγορεύει την ύπαρξη πολλών διασκορπισμένων τερματικών εγγραφής, τα οποία να συνδέονται με ένα κεντρικό σταθμό

επεξεργασίας. Για όλους τους παραπάνω λόγους, ενδέχεται ένας οργανισμός να χρειαστεί να αφιερώσει αρκετούς μήνες μόνο στο σχεδιασμό της διαδικασίας εγγραφής, προτού υπεισέλθει σε πιο τεχνικές απόψεις του συστήματος. Ο σχεδιασμός αυτός, θα πρέπει εκτός των άλλων να μεριμνά για επανάκτηση ή ανανέωση των βιομετρικών δεδομένων, μετά από πολυετή χρονικά διαστήματα.

Για τα συστήματα ταυτότητας (ID) πολιτών που διεξάγουν αναγνώριση 1:N, το ζήτημα της επεκτασιμότητας είναι θεμελιώδες. Κι αυτό, γιατί τα συστήματα αυτά πρέπει εκτός του να αναμένουν, να είναι σε θέση και να ενσωματώσουν πιθανή πληθυσμιακή ανάπτυξη. Υπάρχει βέβαια ένα σημείο, πέρα απ' το οποίο οι βιομετρικές τεχνολογίες αδυνατούν να διεξάγουν με την ίδια αξιοπιστία αναγνώριση πολιτών. Για παράδειγμα, έρευνες που γίνονται με βάση ένα μοναδικό αποτύπωμα παύουν να είναι αρκούντως αποτελεσματικές σε βάσεις δεδομένων που ξεπερνούν τις 100.000 εγγραφές. Ακόμα και όταν υπάρχουν δύο δακτυλικά αποτυπώματα, υπάρχει ένα ανώτατο όριο μερικών εκατομμυρίων πολιτών. Έτσι, ένας οργανισμός που σχεδιάζει ένα βιομετρικό σύστημα για 10 εκατομμύρια χρήστες και με το πέρασμα του χρόνου έρχεται αντιμέτωπος με 12 εκατομμύρια, πρέπει να αναπροσαρμόσει τις δυνατότητες του συστήματος. Καλό είναι για αυτές τις περιπτώσεις να υπάρχει πρόνοια.

Ένα ζήτημα σχετικό με την επεκτασιμότητα, είναι ο χρόνος απόκρισης των συστημάτων, που είναι συνάρτηση του μεγέθους της βάσης δεδομένων, του μέγιστου επιτρεπτού χρόνου εγγραφής και της διαθέσιμης υπολογιστικής δύναμης. Πρόκειται για ένα πολύ σημαντικό θέμα, που άπτεται της σωστής εξυπηρέτησης των πολιτών και της περάτωση κρατικών υποθέσεων. Συνήθως, για να επιταχυνθεί αυτός ο χρόνος επιλέγεται η κατηγοριοποίηση ή το φιλτράρισμα των βιομετρικών δεδομένων με βιομετρικά (π.χ. μορφή δακτυλικού αποτυπώματος) ή μη βιομετρικά κριτήρια (π.χ. φύλο).

Εκτός όμως από το σύντομο χρόνο απόκρισης, οι κατασκευαστές πρέπει να είναι σε θέση να εγγυηθούν αποδεκτά ποσοστά λάθους για το σύστημα. Ένα τελευταίο ζήτημα στις εφαρμογές αναγνώρισης πολιτών είναι η πιθανότητα κακής χρήσης των βιομετρικών δεδομένων. Πρόκειται για μια πιθανότητα που εμπερικλείει πολλούς κινδύνους, εξαιτίας του όγκου και της σημασίας των πληροφοριών που αφορούν σ' ένα σημαντικό τμήμα του πληθυσμού και του κεντρικοποιημένου τρόπου αποθήκευσής τους. Γενικά, είναι αναγκαίο οι κατασκευαστές να αποκλείουν τη μη εξουσιοδοτημένη πρόσβαση στα

δεδομένα, ακόμα και στους εσωτερικούς λειτουργούς του συστήματος. Για να επιτευχθεί αυτό, μπορεί να επιλεγεί ο φυσικός και λογικός διαχωρισμός των δεδομένων, η κρυπτογράφησή τους και άλλα μέσα προστασίας.

**Συμπεράσματα**

Η αναγνώριση πολιτών αποτελεί μια βιομετρική εφαρμογή, η οποία αν και δύσκολη στην υλοποίησή της, είναι συνάμα πολύ επωφελής. Ειδικά σε περιπτώσεις όπου η χώρα πρέπει να γνωρίζει με ασφάλεια ποιοι είναι οι επισκέπτες της, οι αποδέκτες των κοινωνικών πακέτων, το εκλογικό σώμα και άλλα τμήματα του πληθυσμού, η βιομετρική ενδεχομένως να είναι το μόνο σίγουρο κι αποτελεσματικό εργαλείο. Εξάλλου, οι περιορισμοί που υπάρχουν στα συστήματα βιομετρικής αναγνώρισης πολιτών συχνά οφείλονται στον τρόπο λειτουργίας των συστημάτων και όχι στις δυνατότητες της ίδιας της τεχνολογίας.

### 4.1.3 Επιτήρηση

Η επιτήρηση αναφέρεται στη χρήση βιομετρικής τεχνολογίας, με σκοπό την αναγνώριση ή πιστοποίηση της ταυτότητας ενός ή περισσότερων ατόμων που βρίσκονται σε ένα δεδομένο χώρο. Στην επιτήρηση η βιομετρική αντικαθιστά ή συμπληρώνει παραδοσιακές μεθόδους, όπως η χρήση καμερών και η κατ' ιδίαν παρακολούθηση.

**Τυπικές εφαρμογές**

Συστήματα βιομετρικής επιτήρησης χρησιμοποιούνται στην πλειοψηφία των μεγάλων καζίνο της Βόρειας Αμερικής και σε διάφορες αστυνομικές εφαρμογές, οι οποίες για λόγους ασφαλείας ελέγχουν την ταυτότητα των περαστικών σε διάφορα μέρη ή των παρευρισκομένων σε μεγάλα γεγονότα. Βέβαια, η διενέργεια αυτόματου ταιριάσματος μέσα από κάμερες ασφαλείας έχει προκαλέσει κατά καιρούς αντικρουόμενες αντιδράσεις. Όμως μετά τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου, οι αρνητικές αντιδράσεις είναι ηπιότερες και το ενδιαφέρον για την ανάπτυξη βιομετρικών συστημάτων επιτήρησης έχει ενταθεί σημαντικά, ειδικά σε εφαρμογές όπως οι ταξιδιωτικές.

**Νέες τάσεις**

Από την πορεία και την επιτυχία των δύο προαναφερθεισών πολυδιαφημισμένων υλοποιήσεων εξαρτάται σε μεγάλο βαθμό το συνολικό μέλλον των εφαρμογών επιτήρησης. Υπάρχει βέβαια το επιχείρημα, ότι ο συγκεκριμένος τύπος εφαρμογών μπορεί να στηριχθεί στις χιλιάδες κάμερες ασφαλείας που βρίσκονται σε διάφορα σημεία της γης, γεγονός που δίνει πλεονέκτημα σε σχέση με τις εφαρμογές που απαιτούν την εγκατάσταση νέου υλισμικού. Αν και η βιομετρική επιτήρηση μπορεί εν καιρώ να αποδειχτεί ικανή να αξιοποιήσει όλη αυτή την υπάρχουσα υποδομή, προς το παρόν αυτό δε συμβαίνει σε βαθμό ικανοποιητικό[1].

Ήδη πάντως, οι υπεύθυνοι υπηρεσιών για την επιβολή του νόμου έχουν εκφράσει την επιθυμία και το ενδιαφέρον τους για ευρύτερη χρήση της τεχνολογίας και είναι πολύ πιθανό το επιχείρημα της δημόσιας ασφάλειας, να υπερισχύσει σε πολλές περιπτώσεις των φόβων για παραβίαση της ιδιωτικότητας. Αλλά και πολλές ιδιωτικές εταιρείες φαίνονται πρόθυμες να ενσωματώσουν δυνατότητα για αυτοματοποιημένη επιτήρηση στα προϊόντα και τις υπηρεσίες που προσφέρουν.

Ωστόσο, δύο παράγοντες μπορούν να σταθούν εμπόδιο στην ανάδειξη της επιτήρησης. Ο πρώτος είναι η ελλιπής απόδοση. Πράγματι, η μόνη τεχνολογία που μπορεί να χρησιμοποιηθεί μέχρι στιγμής σε συνθήκες επιτήρησης είναι το σκανάρισμα του προσώπου, που όμως διέπεται από ορισμένα μειονεκτήματα από πλευράς ακρίβειας, λόγω των δυσμενών συνθηκών φωτισμού, της απόστασης, της γωνίας λήψης και άλλων παραγόντων που επηρεάζουν την απόκτηση δεδομένων. Ο δεύτερος εξίσου σημαντικός παράγοντας είναι η απειλή κατά της ιδιωτικότητας. Η απειλή αυτή σχετίζεται εν μέρει με το θέμα της απόδοσης, αφού η λανθασμένη αναγνώριση πολιτών εγείρει αρκετά ερωτήματα σχετικά με ζητήματα ιδιωτικότητας. Έτσι, ακόμα κι όταν τα συστήματα επιτήρησης χρησιμοποιούνται για λόγους κυρίως αποθάρρυνσης των επίδοξων παρανόμων, θα πρέπει να είναι σε θέση να επιδείξουν κάποιο μέτρο της αποτελεσματικότητάς τους, για να μπορεί να συντελεστεί ο σκοπός της αποθάρρυνσης.

[1] <<Βιομετρικά Συστήματα για έλεγχο πρόσβασης>>, Στέλιος Χ.Α. Θωμόπουλος, Δ/ντης Ινστιτούτου Πληροφορικής και Τεχνολογίας , ΕΚΕΦΕ Δημόκριτος, Μαίος 2003.

**Χρησιμοποιούμενες βιομετρικές τεχνολογίες και κάθετες αγορές**

Προς το παρόν, το σκανάρισμα του προσώπου είναι η μοναδική τεχνολογία η οποία μπορεί να εφαρμοστεί σε εφαρμογές επιτήρησης. Βέβαια, είναι πιθανό το σκανάρισμα της φωνής να χρησιμοποιηθεί στο μέλλον πιο εκτενώς για πιστοποίηση ταυτότητας 1:1 κατά την παρακολούθηση συνομιλιών, όμως αυτό δε συνιστά επιτήρηση με την παραδοσιακή έννοια 1:N. Σήμερα, ο χώρος των τυχερών παιχνιδιών και της επιβολής του νόμου αποτελούν τις δύο κάθετες αγορές που έχουν αγκαλιάσει την τεχνολογία.

**Κόστος ανάπτυξης**

Το κόστος για τα συστήματα επιτήρησης ποικίλει σε μεγάλο βαθμό, ανάλογα με το αν η τεχνολογία σκαναρίσματος προσώπου στηρίζεται σε υπάρχουσες συσκευές ή απαιτεί την εγκατάσταση νέων. Από κει και πέρα, το μεγαλύτερο κόστος αφορά στη χορήγηση αδειών για τη χρήση του κατάλληλου λογισμικού. Πράγματι, ανάλογα με την εφαρμογή, η άδεια μπορεί να δίδεται για έρευνα σε μια συγκεκριμένη βάση δεδομένων ή για ένα ορισμένο χρονικό διάστημα. Άδειες για εκτεταμένη χρήση όπως είναι λογικό, απαιτούν καταβολή επιπλέον χρημάτων. Γενικά πάντως, οι τιμές που ορίζουν οι εταιρείες σκαναρίσματος προσώπου στις λύσεις λογισμικού που διαθέτουν δεν διέπονται από μια κοινή λογική, κι αυτό αποδίδεται στο γεγονός πως πρόκειται για μια αρκετά νέα τεχνολογία. Συνοψίζοντας περί κόστους, είναι πιθανή η εμφάνιση πρόσθετων οικονομικών επιβαρύνσεων, λόγω της ανάγκης για υποστήριξη, παρακολούθηση και διασφάλιση των αποτελεσμάτων και για ειδοποίηση των ειδικών.

**Ζητήματα υλοποίησης**

Επειδή η βιομετρική τεχνολογία είναι λιγότερο αποδεδειγμένη στο χώρο της επιτήρησης απ' ότι οπουδήποτε αλλού, η συζήτηση γύρω από τα θέματα ανάπτυξης στις εφαρμογές επιτήρησης είναι ιδιαίτερα σημαντική. Σχετικά με το υλισμικό απόκτησης, συχνά αναφέρεται για την τεχνολογία σκαναρίσματος προσώπου, ότι μπορεί να στηριχθεί σε εικόνες προερχόμενες από ήδη υπάρχοντα εξοπλισμό, π.χ. από κάμερες CCTV. Δυστυχώς, αυτό δεν είναι πάντοτε εφικτό, κυρίως εξαιτίας παραγόντων όπως η απόσταση, η γωνία λήψης, ο φωτισμός κτλ. Σε αρκετές περιπτώσεις δηλαδή, για να

υπάρχει η απαραίτητη ακρίβεια και πιστότητα στις λήψεις, απαιτείται η αγορά καμερών υψηλής ποιότητας για αποκλειστική χρήση και ακόμα η τοποθέτησή τους σε ειδικά σημεία σε κατάλληλη απόσταση και γωνία.

Απ' την άλλη, είναι γνωστό ότι η αποτελεσματικότητα των λύσεων σκαναρίσματος προσώπου εξαρτάται σε μεγάλο βαθμό από την ποιότητα της εγγραφής. Πράγματι, για την εγγραφή στα περισσότερα συστήματα απαιτείται η απόκτηση πολλών εικόνων του προσώπου και μάλιστα από ελαφρώς διαφορετικές γωνίες, ούτως ώστε να υπάρχει η δυνατότητα ενσωμάτωσης και χειρισμού ενός μικρού εύρους κινήσεων. Δυστυχώς όμως, στις περισσότερες περιπτώσεις επιτήρησης η εγγραφή πρέπει να γίνει μέσα από μία, χαμηλής ποιότητας φωτογραφία, γεγονός που δυσχεραίνει τις προσπάθειες για ταίριασμα, ελλείψει επαρκών δεδομένων για διάκριση. Είναι ωστόσο μια πραγματικότητα, η οποία δεν μπορεί να αγνοηθεί από αυτούς που εφαρμόζουν την τεχνολογία. Εξάλλου, κάτι ακόμα που πρέπει να συνυπολογιστεί είναι το μέγεθος της βάσης δεδομένων, σε σχέση με την οποία γίνεται η σύγκριση, καθώς και το ποσοστό υπόπτων της βάσης, που πιθανολογείται ότι βρίσκεται μέσα στο χώρο που επιτηρείται. Αν για παράδειγμα, ένα σύστημα σκανάρει 1 εκατομμύρια πρόσωπα ετησίως, με την προσδοκία να αναγνωρίσει μέσα σ' αυτά 10 τρομοκράτες (που κατά πάσα πιθανότητα δε θα εμφανιστούν επειδή ο χώρος εποπτεύεται) τότε ο λόγος ύπαρξης του συγκεκριμένου συστήματος αργά ή γρήγορα θα αμφισβητηθεί. Αν όμως η προσπάθεια γίνεται για την αναγνώριση 100 γνωστών τρομοκρατών από μια ομάδα 100.000 παρακολουθούμενων ατόμων, τότε το αντίστοιχο σύστημα αυτομάτως καθίσταται περισσότερο βιώσιμο.

Ένα άλλο θέμα είναι ότι τα συστήματα επιτήρησης, όπως και όλα τα βιομετρικά συστήματα άλλωστε, δεν παρέχουν ταίριασμα 100%, αλλά μόνο κάποιο επίπεδο εμπιστοσύνης. Επομένως, προκειμένου να καθοριστεί με βεβαιότητα εάν υπάρχει ταίριασμα, χρειάζεται η ανθρώπινη παρέμβαση. Αυτό σημαίνει ότι, εφόσον δοθεί απάντηση για ταίριασμα από το βιομετρικό σύστημα, πρέπει να επινοηθεί ένας τρόπος για να αναχαιτιστεί το άτομο, ενώ απ' την άλλη παραμένει το ενδεχόμενο κάποιο άτομο να μην έχει αναγνωριστεί σωστά, ακόμα και μετά την ανθρώπινη παρέμβαση.

Σχετικά τέλος με το αποτρεπτικό έργο των συστημάτων, θεωρείται απίθανο ένα σύστημα σκαναρίσματος προσώπου που δεν είναι ορατό, να συμβάλλει στην αποθάρρυνση από την τέλεση εγκλημάτων, απ' τη στιγμή που η λειτουργία του παραμένει άγνωστη για το

μεγαλύτερο ποσοστό ανθρώπων. Αντίθετα, οι κάμερες σε κοινή θέα, πέρα απ' το ότι είναι πιο αποτελεσματικές στην αναγνώριση ατόμων, είναι περισσότερο πιθανό να προκαλέσουν περίεργη συμπεριφορά, όπως ηθελημένες προσπάθειες για μεταμφίεση και αλλοίωση χαρακτηριστικών μπροστά από τις κάμερες επιτήρησης. Πάντως, στις περισσότερες περιπτώσεις επιτήρησης το στοιχείο της αποτροπής μπορεί να επιτευχθεί μέσα από την έξυπνη χρήση της τεχνολογίας.

**Συμπεράσματα**

Η επιτήρηση είναι μια πολύ ενδιαφέρουσα βιομετρική εφαρμογή, που συνδυάζει μια διαδικασία εγγραφής η οποία πραγματοποιείται κάτω από δύσκολους όρους, με μια επίσης δύσκολη διαδικασία απόκτησης δεδομένων. Δεν είναι απορίας άξιον λοιπόν, που η επιτήρηση δεν αποτελεί μια αποδεδειγμένα αξιόπιστη εφαρμογή της βιομετρικής τεχνολογίας. Αν ωστόσο σημειωθεί πρόοδος στην ικανότητα των συστημάτων για εγγραφή, απόκτηση και αναγνώριση προσώπων μέσα από εικόνες και συσκευές χαμηλότερης ποιότητας, τότε αναμφίβολα η βιωσιμότητα της συγκεκριμένης λύσης θα ενισχυθεί.

## 4.2 ΟΙ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ

Οι εφαρμογές στη διοίκηση ανθρώπινου δυναμικού αναφέρονται στην πιστοποίηση της αυθεντικότητας ενός ατόμου, το οποίο φέρει την ιδιότητα του εργαζομένου, στο περιβάλλον εργασίας του. Η πιστοποίηση γίνεται με βάση ένα δείγμα βιομετρικών δεδομένων του ατόμου, κι έχει σαν αποτέλεσμα τη χορήγηση πρόσβασης σε δεδομένα της εργασίας ή την αλληλεπίδραση με τον εργοδότη και την ευρύτερη διοίκηση. Το διαφοροποιό στοιχείο στις εφαρμογές διοίκησης υπαλλήλων είναι η ύπαρξη μιας επιχείρησης, δημόσιας ή ιδιωτικής, η οποία υποχρεώνει τα άτομα σε βιομετρική πιστοποίηση της αυθεντικότητας και επιβάλλει συμμόρφωση με τις αποφάσεις του συστήματος. Συνήθως οι εφαρμογές υπαλλήλων πραγματοποιούνται σε κλειστά συστήματα και απευθύνονται στο προσωπικό ενός τμήματος, ενός τομέα ή και ολόκληρης της επιχείρησης. Σ' αυτή την κατηγορία υπάγονται οι εφαρμογές πρόσβασης σε PCs και δίκτυα, καθώς και οι εφαρμογές φυσικής πρόσβασης, επιτήρησης και time and attendance.

Οι εφαρμογές διοίκησης ανθρώπινου δυναμικού κατά κύριο λόγο χρησιμοποιούνται για πιστοποίηση και όχι αναγνώριση της ταυτότητας ενός ατόμου. Άλλοτε είναι υποχρεωτικές και άλλοτε όχι, το γεγονός όμως είναι ότι ένα άτομο με την ιδιότητα του εργαζομένου, είναι περισσότερο εύκολο να πειθαναγκαστεί στη χρήση βιομετρικής, γεγονός που εγείρει ανησυχίες για ζητήματα ιδιωτικότητας. Απ' την άλλη, υπάρχει το επιχείρημα των κινδύνων που προκαλεί η μη εξουσιοδοτημένη πρόσβαση σε πόρους ή η αδυναμία καταλογισμού ευθυνών σε περιπτώσεις κακής χρήσης των δεδομένων, κι έτσι το όλο θέμα αποκτά πολύ μεγάλο ενδιαφέρον.

### 4.2.1 Διοίκηση Ανθρώπινου Δυναμικού

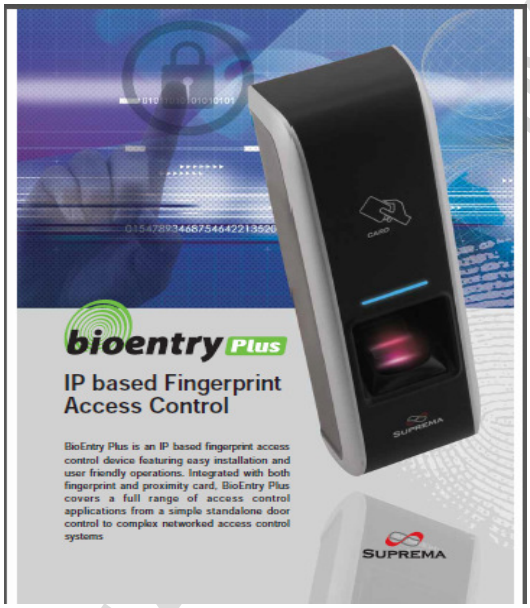
Οι βιομετρικές εφαρμογές διαδραματίζουν σημαντικό ρόλο στη διοίκηση ανθρωπινου δυναμικού . Σαφέστερα, δίνουν έγκυρες και αδιαπραγμάτευτες πληροφορίες στη διοίκηση για τους υπαλλήλους της, ενδυναμώνοντας αυτήν με τον πλήρη έλεγχο του οργανισμού. Είναι ιδιαίτερα σημαντικό για τους προϊστάμενους ενός οργανισμού να γνωρίζει όλες τις απαραίτητες πληροφορίες για το προσωπικό, δηλ. το πότε εισήλθαν στην επιχείρηση, το πότε εξήλθαν, που εισήλθαν, πόσο χρόνο διήρκησε η παραμονή τους σε έναν χώρο ή και γενικότερα στο περιβάλλον της επιχείρησης.

Αυτές οι βιομετρικές εφαρμογές απαντώνται με τις λεγόμενες βιομετρικές κλειδαριές που μέσω του δακτυλικού αποτυπώματος ή τις ίριδας του εργαζομένου, επιτρέπεται η είσοδος και η έξοδος του, καταγράφοντας βέβαια και τις αντίστοιχες πληροφορίες. Οι κλειδαριές αυτές χρησιμοποιούνται σε πολλές επιχειρήσεις και οργανισμούς (Αερολιμένας Αθηνών, Αττικό Μετρό κ.τ.λ.) στην Ελλάδα καθώς επεκτείνονται συνεχώς για την ασφάλεια των εργαζομένων, της επιχείρησης – οργανισμού και γενικότερα των πολιτών. Στο εξωτερικό οι εφαρμογές αυτές έχουν ήδη επεκταθεί από την δεκαετία του 1990 και είναι απτές σε ποικίλες επιχειρήσεις και οργανισμούς (Τράπεζες, αστυνομία, στρατό, αερολιμένες κ.τ.λ.).

Στην Ελλάδα σήμερα, υπάρχουν αρκετοί εισαγωγείς (biokey, Stamatiou key center, Fokas security devices) βιομετρικών κλειδαριών , όπως παρατηρούμε και από τους

παρακάτω καταλόγους το κόστος ανέρχεται από 500€ έως 1000€ αναλόγως την ποιότητα και την χρήση των συσκευών.

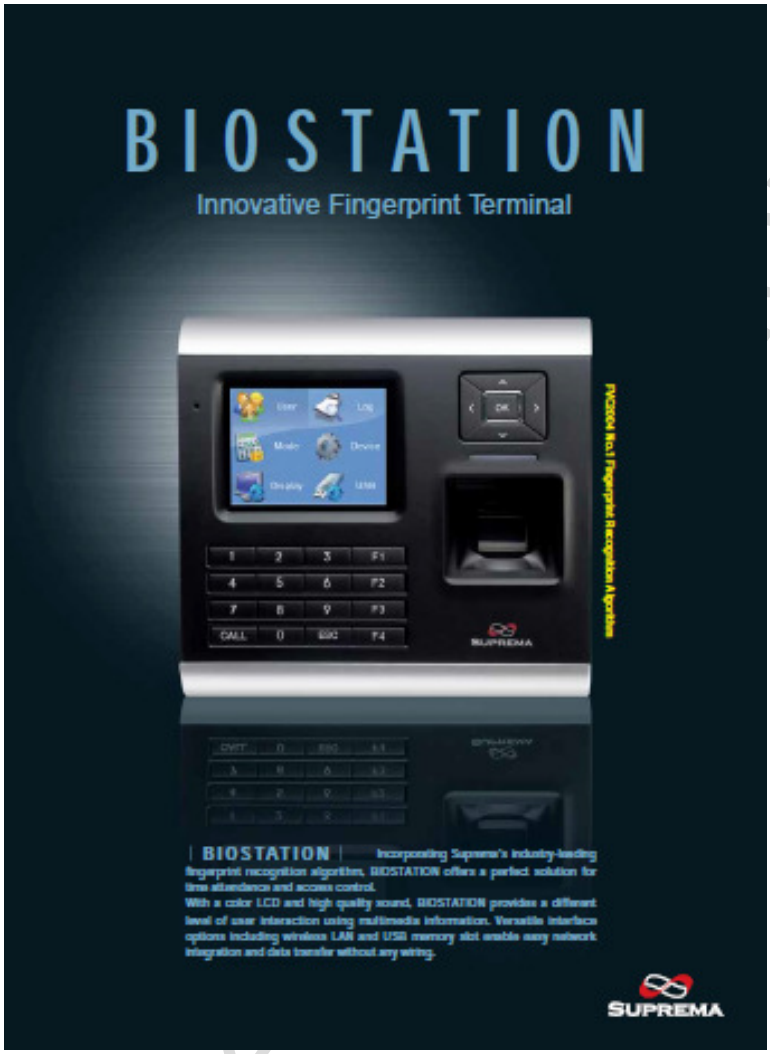
Ακόμη, υπάρχουν εξελιγμένα συστήματα στον χώρο της βιομετρικής τεχνολογίας όπως θα παραθέσουμε παρακάτω, τα οποία έχουν την μορφή βραχιολιού και επικοινωνούν ασύρματα (wireless bluetooth) με έναν κεντρικό server μετρώντας κίνηση, καρδιακούς παλμούς, αναπνοή και κυκλοφορία του αίματος του εργαζομένου , δίνοντας στη διοίκηση και ιδιαίτερα στη διοίκηση ανθρωπίνων πόρων, μοναδικές πληροφορίες για τους εργαζομένους της, δηλ. όχι το μόνο που κινήθηκαν αλλά και το πόσο κινήθηκαν, εάν αγχώθηκαν, εάν εργάζονται, ακόμη και εάν κοιμούνται …… Η τεχνολογία αυτή είναι ιδιαίτερα δαπανηρή και δεν έχει εφαρμοστεί σε καμία επιχείρηση στην Ελλάδα. Αντίθετα εφαρμόζεται στις Η.Π.Α. και την Γερμανία σε μεγάλες αυτοκινητοβιομηχανίες (Chrysler-Damler) με μεγάλο αριθμό εργαζομένων. Η τεχνολογία με τα βραχιόλια κοστίζει για χώρο 1000 τ.μ. περίπου 15.000€ ενώ ο πομπός – βραχιόλι για κάθε εργαζόμενο κοστίζει 200€. Η τεχνολογία αυτή εισάγεται στην Ελλάδα από εταιρεία που ασχολείται στον χώρο.[1]

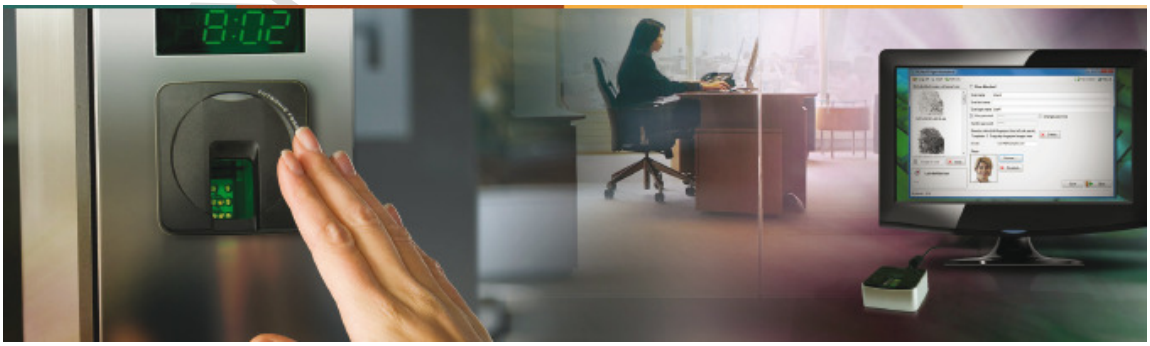


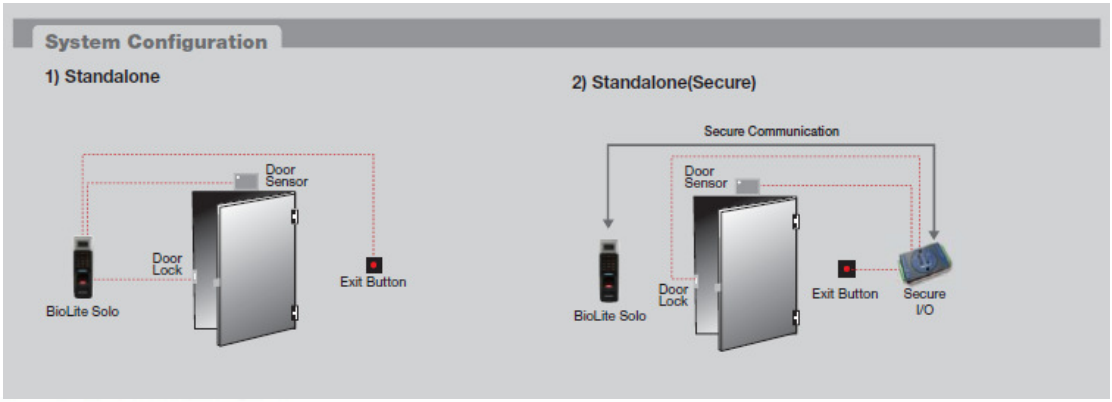


[1] http://www.fokasp.gr/search.php?search=1&company=10&jsenabled=1

**Σχήμα 22:** Βιομετρικές συσκευές






## Τιμοκατάλογος

## Βιομετρικά Συστήματα Access Control με δυνατότητα Καταγραφής

| Κωδικός | Μοντέλο | Περιγραφή | Τιμή | |
|---|---|---|---|---|
| 5111.SU.BIOS.001 | **BioStation OC** | Βιομετρικό σύστημα ελέγχου πρόσβασης<br>Ικανότητα εγγραφής 50.000 δακτυλικά αποτυπώματα<br>1 έξοδος ρελέ<br>Δυνατότητα επιλογής αναγνώστη<br>Καταγραφή για 500.000 συμβάντα<br>Ήχος 16 bit<br>Οθόνη 2,5" LCD 65.000 χρωμάτων<br>USB/RS232/485, wifi/10/100 LAN<br>Χρονοπαρουσία, γεφύρωση με ERP,λογιστικά πακέτα μισθοδοσίας<br>διαχείριση ανθρώπινων πόρων | **1,070€** |  |
| 5111.SU.BIOS.010 | | Biostation Mirfare | **1,220€** | |
| 5111.SU.BIOS.014 | | Biostation HID | **1,250€** | |
| 5111.SU.BIOS.015 | | Biostation Wireless | **1,250€** | |
| 5111.SU.BIOS.016 | | Biostation Wireless RF | **1,360€** | |
| 5111.SU.BIOS.012 | | Mirfare<br><br>Βιομετρικό σύστημα ελέγχου πρόσβασης<br>Ικανότητα εγγραφής 5.000 δακτυλικά αποτυπώματα<br>1 έξοδος ρελέ<br>Οπτικός αναγνώστης 500 dpi<br>Καταγραφή για 50.000 συμβάντα<br>Ταχύτητα ανάγνωσης <1 sec<br>RS485,10/100 LAN<br>Καταστάσεις λειτουργίας: Αποτύπωμα, RF κάρτα, RF+αποτύπωμα<br>Χρονοπαρουσία, γεφύρωση με ERP,λογιστικά πακέτα μισθοδοσίας<br>διαχείριση ανθρώπινων πόρων<br>Θερμοκρασία λειτουργίας -20oC εως +50o C | **660€** |  |
| 5111.SU.BIOS.008 | **BioLite Solo OC** | Αυτόνομο βιομετρικό σύστημα ελέγχου πρόσβασης<br>Δείκτης Προστασίας IP65 - Ιδανικό για εξωτερικούς χώρους<br>Ικανότητα εγγραφής 400 δακτυλικά αποτυπώματα (200 χρήστες)<br>1 έξοδος ρελέ<br>Οπτικός αναγνώστης 500 dpi<br>Καταγραφή για 5.000 συμβάντα<br>Ταχύτητα ανάγνωσης <1 sec<br>RS 485<br>Καταστάσεις λειτουργίας: Αποτύπωμα, PIN, Αποτύπωμα + PIN<br>Πληκτρολόγιο 12 πλήκτρων<br>Οθόνη Τύπου LED | **580€** |  |
| 5111.SU.BIOS.011 | | Mirfare<br><br>Δικτυακό βιομετρικό σύστημα ελέγχου πρόσβασης<br>Δείκτης Προστασίας IP65 - Ιδανικό για εξωτερικούς χώρους<br>Ικανότητα εγγραφής 10.000 δακτυλικά αποτυπώματα (5.000 χρήστες)<br>1 έξοδος ρελέ<br>Οπτικός αναγνώστης 500 dpi<br>Καταγραφή για 50.000 συμβάντα<br>Ταχύτητα ανάγνωσης <1 sec<br>RS 485,TCP,IP<br>Πληκτρολόγιο 12 πλήκτρων<br>Οθόνη Τύπου LED | **825€** |  |

### 4.2.2 Πρόσβαση σε PCs/δίκτυα

Η πρόσβαση σε PCs και δίκτυα αναφέρεται στη χρήση βιομετρικής, με σκοπό την αναγνώριση ή πιστοποίηση της ταυτότητας ατόμων, τα οποία αποκτούν πρόσβαση σε PCs, PDAs, δίκτυα, εφαρμογές και άλλους πόρους σχετικούς με υπολογιστές. Στις προαναφερθείσες εφαρμογές, η βιομετρική λειτουργεί είτε συμπληρωματικά ή στη θέση παραδοσιακών μηχανισμών πιστοποίησης, όπως είναι οι κωδικοί και τα tokens. Αυτή τη στιγμή, οι λύσεις λογισμικού και οι λύσεις hardware που υπάρχουν στο εμπόριο για πρόσβαση σε PCs και δίκτυα, είναι περισσότερες απ' ότι για κάθε άλλη εφαρμογή. Γενικά, η βιομετρική αποτελεί σήμερα μια προφανή λύση για τη διασφάλιση της πρόσβασης σε υπολογιστές, γεγονός που οφείλεται σε πολλούς παράγοντες, όπως η διάδοση της χρήσης φορητών συσκευών στο σπίτι και το γραφείο, η πληθώρα των πόρων σε συνεταιρικά δίκτυα και το διαδίκτυο, η ανάγκη για πιστοποίηση σε επίπεδο χρήστη κτλ.

**Τυπικές εφαρμογές**

Από τις εφτά οριζόντιες αγορές, η πρόσβαση σε PCs και δίκτυα είναι εκείνη που εννοιολογικά, πλησιάζει περισσότερο τη λογική πρόσβαση με την παραδοσιακή έννοια. Είναι γεγονός ότι η χρήση της βιομετρικής για login σε PCs, laptops και άλλες συσκευές, αποτελεί μια φυσική εξέλιξη για τη συγκεκριμένη τεχνολογία. Το ίδιο ισχύει για τη χρήση της σε post-login εφαρμογές, όπως η πρόσβαση σε ευαίσθητα αρχεία, εφαρμογές, δίκτυα και βάσεις δεδομένων.

Γενικά, η βιομετρική τεχνολογία μπορεί να λειτουργήσει πολύ καλά σε επίπεδο λειτουργικού συστήματος και να αξιοποιήσει μηχανισμούς ασφαλείας και τη σχέση εμπιστοσύνης. Έτσι, δεν είναι τυχαία η χρήση της στα συστήματα ασφαλείας των windows και novell. Σ' αυτά τα περιβάλλοντα, η βιομετρική χρησιμοποιείται κυρίως σ' εφαρμογές client/server, διευκολύνοντας τους διαχειριστές του συστήματος στον έλεγχο και στην απομάκρυνση μη εξουσιοδοτημένων χρηστών και στην καλύτερη διαχείριση των επιπέδων ασφαλείας. Υπάρχουν βέβαια και λύσεις, που εφαρμόζονται μόνο στο

λογισμικό του πελάτη (client). Αυτές ελέγχουν μόνο την πρόσβαση στο ίδιο το PC και είναι περισσότερο διαδεδομένες σε κινητά περιβάλλοντα.

Μέχρι στιγμής, ο ιδιωτικός χαρακτήρας της βιομετρικής και κάποιες αστάθειες στην απόδοσή της, έχουν κάνει πολλές εταιρείες διστακτικές στη χρήση της. Κάποιες επιχειρήσεις δηλαδή, επιλέγουν να περιμένουν έως ότου ωριμάσει η τεχνολογία, για να έχει σίγουρο αντίκρισμα η επένδυσή τους. Τόσο η Microsoft όσο και η Intel έχουν ανακοινώσει την πρόθεσή τους να ενσωματώσουν βιομετρικό λογισμικό στα συστήματα πιστοποίησης που διαθέτουν. Η υλοποίηση αυτών των προθέσεων θα αποτελέσει βαρόμετρο για την αποδοχή της τεχνολογίας και θα ανοίξει το δρόμο για καθιέρωσή της και σε εφαρμογές e-mail, κτλ. Το 2000 και το 2001 ανακοινώθηκαν μια σειρά από μεγάλης κλίμακας εφαρμογές για βιομετρική πρόσβαση σε PCs και δίκτυα. Όλες αυτές οι εφαρμογές κάνουν χρήση σκαναρίσματος δαχτύλων κι εμείς απλά αναφέρουμε τις πιο ενδιαφέρουσες. Τον Ιανουάριο του 2001, η πόλη Glendale της Καλιφόρνια ξεκίνησε μια εφαρμογή για 2100 υπαλλήλους του δήμου, ενώ το Μάρτιο του 2001, το New York State Office of Mental Health ανακοίνωσε ότι το πρόγραμμα που έθεσε σε εφαρμογή το 1998, έφτασε αισίως τους 6000 υπαλλήλους. Στις αρχές του 2000, το Credit Union Central ανακοίνωσε σχέδια με διετή χρονικό ορίζοντα, για επέκταση των βιομετρικών εγγραφών από 500 σε 2000. Τέλος, μια βρετανική εταιρεία παραγωγής αποφάσισε τη χρήση περιφερειακής συσκευής σκαναρίσματος δαχτύλων για την ασφάλιση ενός δικτύου 4000 θέσεων.

Τέλος, σχετικά με τους οικιακούς ή τους μεμονωμένους χρήστες, στην αγορά διατίθενται πολλές λύσεις. Δυστυχώς όμως, οι λύσεις αυτές δεν είναι γνωστές στο ευρύ κοινό και είναι και σχετικά ακριβές. Πράγματι, μια περιφερειακή συσκευή που κοστίζει 100€ μπορεί να αποτελεί μια φυσιολογική επένδυση για μια επιχείρηση, αλλά θεωρείται ακριβή για τους περισσότερους οικιακούς χρήστες.

**Νέες τάσεις**

Από τα υπάρχοντα στοιχεία, προκύπτει ότι η βιομετρική θα αποκτήσει ακόμα πιο σημαντικό ρόλο στις εφαρμογές πρόσβασης σε υπολογιστές, λόγω του μεγάλου όγκου των πληροφοριών που διατίθενται σε διαμοιραζόμενα δίκτυα, και της ευαίσθητης φύσης αυτών των πληροφοριών. Η εξάπλωση στη χρήση βιομετρικής αναμένεται να αγγίξει, πέρα απ' τις εφαρμογές για desktop και φορητά PCs, το χώρο των ασύρματων δικτύων και των εικονικών ιδιωτικών δικτύων (virtual private networks (VPNs)).

Γενικά, οι όποιες εξελίξεις αναμένεται να έχουν ως κινητήριο δύναμη την απαίτηση των εταιρειών, που αποθηκεύουν και διαχειρίζονται ευαίσθητα δεδομένα, για μεγαλύτερο έλεγχο και δυνατότητα καταμερισμού ευθυνών. Κι αυτό γιατί, πέρα απ' την πιστοποίηση, η βιομετρική καταγράφει ένα ίχνος, το οποίο αποδεικνύει ότι ένα συγκεκριμένο άτομο παρέστη σ' ένα χώρο μια δεδομένη χρονική στιγμή. Αυτό σημαίνει ότι κανείς δεν μπορεί να αποποιηθεί τις πράξεις του και έτσι μειώνεται ο καταμερισμός συλλογικών ευθυνών.

Την ίδια στιγμή όμως, τίθενται και εμπόδια στην ανάπτυξη της βιομετρικής αγοράς. Ζητήματα ιδιωτικότητας και νομικά θέματα φέρ' ειπείν, αποτρέπουν κάποιες εταιρείες από τη βιομετρική, ειδικά όταν η χρήση της πρέπει να είναι υποχρεωτική. Δεν είναι σπάνιο εξάλλου, υπάλληλοι να αντιδρούν στη θέα βιομετρικών συστημάτων ή να ισχυρίζονται αδυναμία εγγραφής. Έτσι, απ' τη στιγμή που δεν έχει διαμορφωθεί ακόμα το κατάλληλο νομοθετικό πλαίσιο – όχι απαραίτητα για να περιορίσει τη χρήση βιομετρικής, αλλά για να προσδιορίσει τους όρους λειτουργίας της – είναι λογικό οι εταιρείες να είναι διστακτικές.

**Κόστος ανάπτυξης**

Το κόστος υλοποίησης μιας βιομετρικής λύσης για PCs και δίκτυα, ειδικά στα πλαίσια μιας επιχείρησης, κυμαίνεται ανάλογα με τον αριθμό των χρηστών, την πολυπλοκότητα του περιβάλλοντος και το είδος της βιομετρικής τεχνολογίας που χρησιμοποιείται. Οι περισσότερες υλοποιήσεις συστημάτων για επιχειρήσεις προϋποθέτουν την αγορά και εγκατάσταση περιφερειακών συσκευών, το αντίτιμο των οποίων καταβάλλεται εκ των προτέρων ή με δόσεις βάσει συμβολαίου. Το ευτύχημα είναι ότι, πλέον το κόστος του υλισμικού έχει μειωθεί πολύ – αυτή τη στιγμή υπάρχουν υψηλής ποιότητας συσκευές

σκαναρίσματος δαχτύλων των 100€ – ενώ αναμένεται περαιτέρω μείωση των τιμών με την ενσωμάτωση της βιομετρικής σε πληκτρολόγια και άλλες περιφερειακές συσκευές.

Πέρα από το κόστος του υλισμικού ανά συσκευή, μπορεί να υπάρξει ανάγκη για ξεχωριστό διακανονισμό στην αγορά λογισμικού. Συνήθως, η χορήγηση της άδειας χρήσης του λογισμικού γίνεται ανά χρήστη ή ανά θέση. Τα πακέτα λογισμικού της αγοράς που απευθύνονται σε επιχειρήσεις επιτρέπουν κεντρική αποθήκευση, πιστοποίηση και διαχείριση των βιομετρικών δεδομένων, ενώ η τιμή τους κυμαίνεται από 500€ ως 1500€.

Για να γίνουν πιο κατανοητά τα παραπάνω μεγέθη, μια επιχείρηση που υλοποιεί μια εφαρμογή σκαναρίσματος δαχτύλων 1000 θέσεων για login στα Windows, αντιμετωπίζει ένα συνολικό κόστος που κυμαίνεται από 100.000€ ως 250.000€, ανάλογα με τον τύπο της συσκευής σκαναρίσματος και το αν χρησιμοποιεί λογισμικό μιας συγκεκριμένης τεχνολογίας ή μια πιο ευέλικτη λύση. Στο παραπάνω ποσό δεν περιλαμβάνεται το κόστος έρευνας, δοκιμής και εκτίμησης της καλύτερης λύσης, ούτε το κόστος υλοποίησης και διαχείρισης του συστήματος ή το κόστος εκπαίδευσης και εγγραφής των χρηστών. Παρότι αυτά τα κόστη δεν είναι ιδιαιτέρως μεγάλα, ειδικά αν αναλογιστεί κανείς το ύψος της επένδυσης που προστατεύεται, εξηγούν γιατί θεωρούνται τόσο ελκυστικές κάποιες άλλες τεχνολογίες, που στηρίζονται σε υπάρχουσα υποδομή.

Τέλος, μια αγορά που μόλις τώρα αναδύεται στο χώρο προτείνει τη διενέργεια βιομετρικής πιστοποίησης μέσω διαδικτύου ή από εξωτερικές εταιρείες παροχής υπηρεσιών, με την απλή καταβολή από τις επιχειρήσεις μιας μηνιαίας συνδρομής. Προς το παρόν η συγκεκριμένη τάση δεν έχει εδραιωθεί για να μπορούμε να αναφερθούμε με ακρίβεια σε κόστος, αλλά οι τιμές που ακούγονται είναι περί τα 8€ με 15€ ανά χρήστη το μήνα.

**Συμπεράσματα**

Η πρόσβαση σε PCs και δίκτυα ενδεχομένως ν' αποτελέσει μια απ' τις πρώτες περιοχές, αν όχι την πρώτη, όπου η αλληλεπίδραση ανθρώπου και βιομετρικής θα υφίσταται σε καθημερινή βάση. Αν και η αντίστοιχη αγορά μόλις τώρα αναδύεται, οι λύσεις που διατίθενται στο εμπόριο είναι πολύ πιο ώριμες απ' αυτές που υπάρχουν για πολλές άλλες

βιομετρικές εφαρμογές. Αυτό σημαίνει ότι η χρήση βιομετρικής δεν εμπερικλείει τόσο μεγάλο ρίσκο. Ειδικά απ΄ τη στιγμή που κολοσσοί όπως η Microsoft και η Intel εντάξουν τη βιομετρική λογική στις διαδικασίες πιστοποίησής τους, οι προσφερόμενες λύσεις θα γίνουν λιγότερο ακριβές και θα απλοποιηθούν σε σημαντικό βαθμό.

### 4.2.3 Φυσική πρόσβαση/Time and attendance

Οι εφαρμογές φυσικής πρόσβασης και time and attendance αναφέρονται στη χρήση βιομετρικής, με σκοπό την αναγνώριση ή την πιστοποίηση της ταυτότητας ατόμων που, εισέρχονται ή εξέρχονται από μια ορισμένη περιοχή (συνήθως ένα κτίριο ή ένα δωμάτιο) σε μια δεδομένη χρονική στιγμή. Πρόκειται για εφαρμογές όπου η βιομετρική χρησιμοποιείται συμπληρωματικά ή στη θέση κλειδιών, σημάτων, καρτών κτλ.

**Τυπικές εφαρμογές**

Οι πρώτες εμπορικές χρήσεις της βιομετρικής τεχνολογίας πραγματοποιήθηκαν σ' εφαρμογές φυσικής πρόσβασης, με την εγκατάσταση συσκευών ελέγχου σε προστατευόμενες περιοχές, όπως στρατιωτικές εγκαταστάσεις, τράπεζες και ρευματοφόρες εγκαταστάσεις. Πίσω από αυτή την πρώιμη χρήση κρύβεται ένα ισχυρό κίνητρο. Πράγματι, κλειδιά και σήματα μοιράζονται εύκολα μεταξύ ατόμων, χωρίς μάλιστα να είναι πάντοτε εφικτός ο εντοπισμός του πραγματικού ιδιοκτήτη, ενώ αντίθετα η χρήση βιομετρικών χαρακτηριστικών προϋποθέτει τη ρητή συγκατάθεση του εγγεγραμμένου χρήστη, κι ακόμη παράγει ένα ίχνος που οδηγεί απευθείας σ' αυτόν. Τέλος, στις περισσότερες λύσεις φυσικής πρόσβασης σπάνια δίνεται συνολική πρόσβαση σε μια εγκατάσταση και συνήθως υπάρχει επιλεκτική πρόσβαση σε ορισμένα δωμάτια[1].

Και στις εφαρμογές φυσικής πρόσβασης (time and attendance) υπάρχει η ίδια ανάγκη για εγγυημένη πιστοποίηση αυθεντικότητας, με τη μόνη διαφορά ότι το ενδιαφέρον δεν στρέφεται γύρω από τον έλεγχο της πρόσβασης σε ευαίσθητες περιοχές, αλλά την εξακρίβωση και αποθάρρυνση από την απάτη. Συχνά αλλά όχι πάντα, οι λύσεις time and attendance είναι δεμένες με συστήματα φυσικής πρόσβασης. Πράγματι, επιτυχημένες υλοποιήσεις βιομετρικών συστημάτων σε περιβάλλοντα φυσικής πρόσβασης έχουν

[1] Version 1.0, 12 January 2000, Biometrics Working Group (UK).

γλιτώσει πολλές επιχειρήσεις από το λεγόμενο buddy-punching, δηλαδή το χτύπημα της κάρτας κάποιου που απουσιάζει, από ένα φίλο συνάδελφο.

**Νέες τάσεις**

Η ανάπτυξη της αγοράς φυσικής πρόσβασης και time and attendance θα επέλθει μέσα απ' την παραγωγή γρηγορότερων, φτηνότερων και ακριβέστερων συσκευών. Οι λόγοι που μέχρι στιγμής τουλάχιστον η βιομετρική δε γνωρίζει πιο ευρεία αποδοχή σε περιβάλλοντα φυσικής πρόσβασης, είναι το υψηλό κόστος και η δυσκολία χρήσης των αντίστοιχων συστημάτων. Η αγορά time and attendance φαίνεται να έχει προβάδισμα, εξαιτίας της αποτελεσματικότητας της βιομετρικής στον εντοπισμό και την αποτροπή της απάτης σε εφαρμογές μεγάλης κλίμακας. Εάν μάλιστα οι κατασκευαστές καταφέρουν να ενσωματώσουν αυτή τη λειτουργικότητα και σε άλλες εφαρμογές ανθρώπινου δυναμικού, τότε το μέλλον της τεχνολογίας διαγράφεται ευοίωνο.

Ωστόσο, τα έσοδα μπορεί και πάλι να μην είναι τα αναμενόμενα, εξαιτίας της χρήσης μόνο μίας συσκευής από πολλούς χρήστες. Σε αντίθεση δηλαδή με άλλες οριζόντιες αγορές, για παράδειγμα την αγορά πρόσβασης σε PCs, όπου σε κάθε PC πρέπει να υπάρχει μια εξειδικευμένη συσκευή, στις εφαρμογές φυσικής πρόσβασης ή time and attendance αρκούν λίγες συσκευές για να εξυπηρετήσουν πολλούς χρήστες. Εξάλλου, δεν υπάρχει και η δυνατότητα επέκτασης του ρόλου αυτών των συσκευών, με την προσθήκη νέας λειτουργικότητας. Ένα τελευταίο εμπόδιο, είναι ότι στον ίδιο χώρο κινούνται πολλές αξιόλογες, ανταγωνιστικές τεχνολογίες και άρα υπάρχει μια πληθώρα λύσεων απ' τις οποίες μπορούν να επιλέξουν οι εταιρείες. Πολλοί μάλιστα από αυτούς που εγκαθιστούν συστήματα ασφαλείας, αποτρέπουν πιθανούς αγοραστές απ' την επιλογή βιομετρικών συστημάτων, ωθώντας τους προς απλούστερες λύσεις, όπως είναι οι proximity cards.

**Χρησιμοποιούμενες τεχνολογίες και κάθετες αγορές**

Το σκανάρισμα του χεριού και των δαχτύλων αποτελούν τις δύο πιο συχνά χρησιμοποιούμενες βιομετρικές λύσεις στις εφαρμογές φυσικής πρόσβασης και time and attendance. Συγκεκριμένα, το σκανάρισμα του χεριού χρησιμοποιείται ήδη απ' τη δεκαετία του '80 σε αρκετές εγκαταστάσεις, ενώ το σκανάρισμα των δαχτύλων φαίνεται

πως έχει εξασφαλίσει τη θέση του στην αγορά, χάρη στη μεγαλύτερη ακρίβεια και ευελιξία που διαθέτει.

Αναφορικά με τις κάθετες αγορές, η βιομετρική χρησιμοποιείται σήμερα σε περιβάλλοντα φυσικής πρόσβασης, αρκετά ετερόκλητα μεταξύ τους και με διαφορετικές απαιτήσεις ασφαλείας, μεταξύ των οποίων σε σχολεία, κέντρα υγείας, καζίνο κτλ. Δεν υπάρχει ένα συγκεκριμένο περιβάλλον φυσικής πρόσβασης, στο οποίο οι υπάρχουσες βιομετρικές λύσεις να απευθύνονται καλύτερα, αν και η βιομηχανία των μεταφορών συγκεκριμένα, έχει θέσει σ' εφαρμογή πολλές από αυτές τις λύσεις, με σκοπό τη χορήγηση πρόσβασης στους εργαζομένους.

**Κόστος ανάπτυξης**

Το κόστος για την υλοποίηση μιας λύσης φυσικής πρόσβασης είναι κατά κύριο λόγο κόστος υλισμικού και ενσωμάτωσης, και λιγότερο κόστος λογισμικού. Οι τιμές για τις περισσότερες λύσεις φυσικής πρόσβασης/time and attendance κυμαίνονται στην καλύτερη περίπτωση από 600€ για συσκευές σκαναρίσματος δαχτύλων μέχρι 1500€ με 2000€ για συσκευές σκαναρίσματος χεριού και αρκετές χιλιάδες ευρώ για συσκευές σκαναρίσματος ίριδας. Όλες αυτές οι συσκευές συνήθως πωλούνται σε μικρό αριθμό κομματιών από αποκλειστικούς αντιπροσώπους και εγκαθίστανται από επαγγελματίες, οι οποίοι εξασφαλίζουν τη σωστή επικοινωνία με τα ήδη υπάρχοντα συστήματα ασφαλείας. Το κόστος της εγκατάστασης εξαρτάται από τον αριθμό των τεμαχίων, την πολυπλοκότητα του υπάρχοντος συστήματος ασφαλείας και τις τροποποιήσεις που πρέπει να γίνουν σε πόρτες και τοίχους. Για τις υλοποιήσεις εκείνες, όπου πολλά σημεία εισόδου ελέγχονται από ένα μοναδικό σύστημα διαχείρισης, διατίθεται το κατάλληλο λογισμικό που επιτρέπει τη συλλογή και διανομή πληροφοριών από και προς τις συσκευές και απαλλάσσει από την ανάγκη εγγραφής σε κάθε μία τοποθεσία ξεχωριστά.

Απ' την άλλη, οι λύσεις time and attendance προσανατολίζονται περισσότερο προς το λογισμικό, με τις συσκευές απόκτησης βιομετρικών δεδομένων να είναι ενσωματωμένες σε ένα κεντρικό σύστημα επιθεώρησης, το οποίο συνδέεται με το σύστημα πληρωμής. Γι' αυτές τις λύσεις, το κόστος εξαρτάται από το λογισμικό, το hardware, και οποιεσδήποτε περαιτέρω τροποποιήσεις απαιτούνται, για την ενσωμάτωση των φυσικών και λογικών μερών του βιομετρικού συστήματος στο παλαιό σύστημα.

**Ζητήματα υλοποίησης**

Υπάρχουν πολλά θέματα που αφορούν στον τρόπο υλοποίησης βιομετρικών συστημάτων για εφαρμογές φυσικής πρόσβασης και time and attendance. Το πρώτο απ' αυτά, αφορά στην προσαρμογή των ατόμων στο βιομετρικό σύστημα. Ανάλογα με το παλαιό σύστημα πιστοποίησης, οι χρήστες μπορεί να θεωρήσουν το καινούριο ως ελαφρώς ή πολύ πιο δύσχρηστο. Για παράδειγμα, είναι πολύ πιθανό όσοι έχουν συνηθίσει στη χρήση proximity cards, να δυσκολευτούν στην προσαρμογή στη βιομετρική πιστοποίηση και να θεωρήσουν τη νέα διαδικασία πολύ απαιτητική συγκριτικά, από άποψη κόπου και συγκέντρωσης. Αυτό μπορεί να απολήξει στο να κρατάνε οι χρήστες ανοιχτές τις πόρτες ασφαλείας, εκλαμβάνοντας το ίδιο το σύστημα σαν μια ενόχληση. Το πρόβλημα αυτό είναι πολύ λιγότερο έντονο στις εφαρμογές time and attendance που είναι ανεξάρτητες από λύσεις φυσικής πρόσβασης, για το λόγο ότι οι χρήστες δεν έχουν άλλη επιλογή από τη βιομετρική πιστοποίηση[1].

Ένα ακόμα θέμα υλοποίησης, αφορά στο χρόνο που διαρκεί η εξακρίβωση ταυτότητας και στην πιθανή δημιουργία ουρών αναμονής. Το ζήτημα τίθεται περισσότερο έντονο, σε περιπτώσεις όπου πολλοί χρήστες περνούν την ίδια χρονική στιγμή από ένα σημείο επιβεβλημένης βιομετρικής πιστοποίησης, όπως για παράδειγμα συμβαίνει κατά την έναρξη μιας βάρδιας. Στο χρόνο πιστοποίησης εξάλλου, προσμετρώνται όχι μόνο ο χρόνος παροχής βιομετρικών δεδομένων και απόκρισης του συστήματος, αλλά και ο χρόνος εισαγωγής του PIN ή μιας κάρτας ή κάποιου άλλου δεδομένου που να δηλώνει την ταυτότητα του ατόμου.

Τέλος, όπως συμβαίνει σε όλες τις εφαρμογές, υπάρχει ένα ποσοστό χρηστών το οποίο δεν μπορεί να πιστοποιηθεί από το σύστημα, είτε λόγω αδυναμίας εγγραφής είτε λόγω λάθους απόρριψης. Αυτό που έχει ενδιαφέρον όμως στις περιπτώσεις φυσικής πρόσβασης, είναι ότι η υλοποίηση fallback διαδικασιών είναι πιο δύσκολη, απ' ότι π.χ. σε desktop εφαρμογές. Κι αν για τους χρήστες που αδυνατούν να εγγραφούν, μια πιθανή λύση είναι η χρήση κωδικών PIN – υπό την προϋπόθεση βέβαια ότι οι συσκευές είναι σε

[1] "Best Practices in Testing and Reporting Performance of Biometric Devices",

θέση να χρησιμοποιούν PINs – ο χειρισμός των χρηστών που απορρίπτονται λανθασμένα από το σύστημα είναι πιο σύνθετος. Πρέπει να σημειωθεί εξάλλου ότι, όταν υπάρχει έκθεση σε στοιχεία της φύσης, γεγονός συνηθισμένο σ' εφαρμογές φυσικής πρόσβασης, είναι δυνατόν ν' αυξηθούν τα ποσοστά λάθους. Συνήθως εξάλλου, δεν υπάρχει η δυνατότητα αναζήτησης βοήθειας σε κάποιο κοντινό γραφείο, ενώ είναι λίγες οι συσκευές ανάγνωσης, που μπορούν και επεξεργάζονται ταυτόχρονα και βιομετρικές πληροφορίες και σήματα. Μια λύση είναι να δίνεται στους χρήστες ένας κωδικός μιας χρήσης για τέτοιες περιπτώσεις, τον οποίο να χρησιμοποιούν για να επανεγγραφούν στο σύστημα με διαφορετική τιμή threshold κι επίπεδο εμπιστοσύνης.

**Συμπεράσματα**

Η φυσική πρόσβαση αποτελεί μια δυνατή βιομετρική εφαρμογή, η οποία απευθύνεται σε συγκεκριμένα περιβάλλοντα και βελτιώνει σημαντικά τις ήδη υπάρχουσες λύσεις. Τόσο ο αριθμός όσο και το πεδίο δράσης των εφαρμογών φυσικής πρόσβασης προβλέπεται ότι θα διευρυνθεί, ενώ ακόμα πιο ραγδαία αναμένεται η εξέλιξη των λύσεων time and attendance, οι οποίες προσκρούουν σε λιγότερες υφιστάμενες διαδικασίες.

Όσο κινούμαστε από τις εφαρμογές υπαλλήλων στις εφαρμογές πελατών, ο πυρήνας της χρησιμοποιούμενης τεχνολογίας παραμένει ουσιαστικά ο ίδιος. Ωστόσο, στο επόμενο κεφάλαιο θα δούμε ότι στις εφαρμογές πελατών οι συνθήκες και οι όροι διεξαγωγής της πιστοποίησης αλλάζουν δραματικά.

## 4.3 ΟΙ ΕΦΑΡΜΟΓΕΣ ΠΕΛΑΤΩΝ

Οι εφαρμογές πελατών αναφέρονται στη χρήση βιομετρικής, με σκοπό την πιστοποίηση της αυθεντικότητας ενός ατόμου, που πραγματοποιεί μια συναλλαγή με την ιδιότητα του πελάτη. Πρόκειται για εφαρμογές με δύο συναλλασσόμενα μέρη, τον προμηθευτή των αγαθών ή υπηρεσιών και τον καταναλωτή. Το καθοριστικό στοιχείο σ' αυτές τις εφαρμογές, είναι ότι ο προμηθευτής πιστοποιεί τους καταναλωτές κι επιβάλλει συμμόρφωση με τις αποφάσεις του βιομετρικού συστήματος. Συνήθως, οι εφαρμογές πελατών πραγματοποιούνται σε ανοιχτά συστήματα, που μπορούν και ενσωματώνουν ένα ποσοστό της υπάρχουσας βάσης πελατών.

Οι εφαρμογές πελατών είναι συνήθως πιστοποίησης και όχι αναγνώρισης. Τις λίγες φορές που γίνεται αναγνώριση δεν είναι για λόγους ασφάλειας, αλλά διευκόλυνσης των χρηστών, οι οποίοι δεν είναι υποχρεωμένοι να θυμούνται το username. Ακόμα, οι εφαρμογές πελατών είναι σχεδόν πάντα προαιρετικές. Δεν υπάρχει καμία υπόνοια εξαναγκασμού σε αυτές – σε αντίθεση με τις εφαρμογές υπαλλήλων – ενώ συνήθως η εγγραφή στο σύστημα ανταμείβεται. Αντίστοιχα, οι ανησυχίες για θέματα ιδιωτικότητας ή για επιπλοκές από τη χρήση βιομετρικής είναι περιορισμένες. Προς το παρόν βέβαια, οι εφαρμογές πελατών έχουν αναπτυχθεί λιγότερο από τις υπόλοιπες, αν κι ενδεχομένως να αποδειχθούν οι πιο κερδοφόρες.

### 4.3.1 Ηλεκτρονικό εμπόριο/Τηλεφωνία

Στις εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας η βιομετρική χρησιμοποιείται, με σκοπό την αναγνώριση ή πιστοποίηση της ταυτότητας ατόμων, τα οποία διεξάγουν απομακρυσμένες συναλλαγές για απόκτηση αγαθών και υπηρεσιών. Πρόκειται για περιπτώσεις, όπου η βιομετρική τεχνολογία λειτουργεί συμπληρωματικά ή στη θέση παραδοσιακών μηχανισμών πιστοποίησης, όπως οι κωδικοί (PINs) ή η αλληλεπίδραση με ερωταποκρίσεις (challenge-and-response interaction).

Αν και υπάρχουν διαφορές, ιδίως στις τεχνολογίες απόκτησης που χρησιμοποιεί η κάθε εφαρμογή, το ηλεκτρονικό εμπόριο και η τηλεφωνία αποτελούν μια λογική ομάδα, για διάφορους λόγους. Πρώτα απ' όλα και οι δύο εφαρμογές χαρακτηρίζονται από υψηλό έλλειμμα εμπιστοσύνης, ενώ εμπλέκουν κάποια απομακρυσμένα, ενδιαφερόμενα μέρη. Υπάρχει ανάγκη να διαπιστωθεί η ταυτότητα αυτών των μερών, κι αυτό δύσκολα μπορεί να γίνει χωρίς τη χρήση βιομετρικής. Εξάλλου, και στις δύο εφαρμογές η διαδικασία εγγραφής είναι μάλλον αβέβαιη, γεγονός που προκαλεί χαμηλό βαθμό σιγουριάς για κάποιους εγγεγραμμένους χρήστες. Ακόμα, επειδή και οι δύο εφαρμογές προορίζονται για χρήση σε επίπεδο συναλλαγών, ενδέχεται να αναπτύξουν παρόμοια μοντέλα κοστολόγησης και εσόδων. Το πλεονέκτημα που έχει η τηλεφωνία, ότι δηλαδή μπορεί να στηριχθεί σε υπάρχουσα υποδομή – τα τηλέφωνα – αναμένεται να περιοριστεί από την εξάπλωση των συσκευών σκαναρίσματος δαχτύλων. Μια τελευταία ομοιότητα έχει να κάνει με το ότι και οι δύο εφαρμογές ευνοούν την καθιέρωση ενός τρίτου μέρους (third

party), που να μπορεί να επεξεργάζεται τις συναλλαγές και να δρομολογεί ανάλογα τις απαντήσεις σε απομακρυσμένες περιοχές.

**Τυπικές εφαρμογές**

Μέχρι στιγμής, δεν έχει υπάρξει κάποια τυπική εφαρμογή ηλεκτρονικού εμπορίου, αφού ελάχιστα εμπορικά Web sites χρησιμοποιούν βιομετρική πιστοποίηση για να ελέγξουν την ταυτότητα των πελατών ή των αγοραστών τους. Κάποιες υλοποιήσεις υπάρχουν στο χώρο της τηλεφωνίας, όπου επιλεγμένοι οικονομικοί οργανισμοί διασφαλίζουν την πρόσβαση σε λογαριασμούς, με τηλεφωνική βιομετρική πιστοποίησης. Μέσα στα επόμενα ένα με δύο χρόνια, αναμένεται να υπάρξει και η τυπική εφαρμογή συναλλαγής με χρήση βιομετρικής, όπου το άτομο θα σκανάρει το δάχτυλό του ή θα επαναλαμβάνει μια κωδική φράση, για την πραγμάτωση μιας συναλλαγής. Αυτές οι εφαρμογές, θα εμφανιστούν πρώτα σε περιβάλλοντα επιχείρηση σε επιχείρηση (Business to Business), και συγκεκριμένα σε συναλλαγές υψηλής αξίας για τη δημιουργία ενός ίχνους παρακολούθησης. Με την πάροδο του χρόνου, η χρήση βιομετρικής θα εξαπλωθεί, για να καλύψει ένα ευρύτερο φάσμα συναλλαγών.

**Νέες τάσεις**

Αν και το αρχικό αίσθημα εφορίας για το ηλεκτρονικό εμπόριο έχει κοπάσει, εξακολουθούν να υπάρχουν λόγοι για επέκταση της χρήσης βιομετρικής στις εφαρμογές αυτής της κατηγορίας. Πράγματι, το ηλεκτρονικό εμπόριο και η τηλεφωνία αποτελούν ίσως τις μόνες εφαρμογές, στις οποίες και οι δύο πλευρές – δηλαδή ο έμπορος και ο αγοραστής – έχουν ισχυρό κίνητρο για να διεξάγουν ισχυρή πιστοποίηση αυθεντικότητας. Αντίθετα δηλαδή με την ασφάλεια δικτύων, όπου οι οργανισμοί έχουν μεγαλύτερο κίνητρο για την υλοποίηση βιομετρικής, απ' ότι οι υπάλληλοι για τη χρήση της, στις συναλλαγές ηλεκτρονικού εμπορίου και τηλεφωνίας οι δύο πλευρές επωφελούνται εξίσου. Ο μεν πωλητής ή κάτοχος των πληροφοριών, επειδή μειώνεται ο κίνδυνος να εξαπατηθεί, ενώ ο αγοραστής, επειδή νιώθει σιγουριά ότι είναι ο μόνος που μπορεί να εξουσιοδοτήσει συναλλαγές μέσω του λογαριασμού του.

Για την εξάπλωση των εφαρμογών ηλεκτρονικού εμπορίου και τηλεφωνίας, απαραίτητη προϋπόθεση είναι η ευρεία διαθεσιμότητα των συσκευών απόκτησης. Στη μεν

τηλεφωνία, οι συσκευές αυτές είναι ήδη πανταχού παρούσες και η μόνη διαφορά είναι ότι θα γίνουν ακόμα πιο δεσπόζουσες στην καθημερινότητά μας. Στο ηλεκτρονικό εμπόριο, οι συσκευές σκαναρίσματος δαχτύλων, πρώτα θα χρησιμοποιηθούν για πρόσβαση σε PCs και δίκτυα και στη συνέχεια αναμένεται να γνωρίσουν απήχηση ως λύσεις ηλεκτρονικού εμπορίου. Βέβαια, αυτό προϋποθέτει ότι οι μεγάλες εταιρείες, όπως η Microsoft και η Intel, θα συνεχίσουν προς την κατεύθυνση της ενσωμάτωσης βιομετρικής λειτουργικότητας στο λογισμικό τους.

Μέχρι σήμερα, τα μόνα έσοδα για τη βιομηχανία της βιομετρικής προέρχονταν από την πώληση συσκευών υλισμικού, τη χορήγηση αδειών λογισμικού και τις μετέπειτα υπηρεσίες επισκευής. Οι βιομετρικές λύσεις δηλαδή, ήταν συσκευές προς πώληση, οι οποίες απέφεραν κέρδη μια κι έξω για τις εταιρείες που τις πωλούσαν, ή είχαν τη μορφή υποδομής, που προσφερόταν με αντίτιμο την καταβολή μηνιαίας συνδρομής. Μια επαναστατική εξέλιξη όμως, υπόσχεται να διαφοροποιήσει αυτό το σχήμα. Πρόκειται για την καθιέρωση ενός μοντέλου εσόδων ανά συναλλαγή, το οποίο στηρίζεται στη χρησιμοποίηση μιας συσκευής πολλές φορές τη μέρα σε διαφορετικές εφαρμογές. Έτσι, αντί για την πώληση των συσκευών ανά θέση έναντι 150€ το κομμάτι, π.χ. θα μπορεί η ίδια συσκευή να αποτελεί συνεχή πηγή εσόδων για την εταιρεία που τη διαθέτει. Για να γίνει βέβαια αυτό, πρέπει να ολοκληρωθεί η κατάλληλη υποδομή, που θα υποστηρίζει το μοντέλο.

Μια τελευταία πρόβλεψη, σχετίζεται με την επικείμενη είσοδο αξιόπιστων τρίτων στο χώρο του ηλεκτρονικού εμπορίου και της τηλεφωνίας. Αυτή τη στιγμή, δεν υπάρχουν εταιρείες παροχής βιομετρικής, που να είναι αρκετά μεγάλες και εδραιωμένες στο χώρο, ώστε να θεωρούνται αξιόπιστες για ένα τέτοιο ρόλο. Παρόλα αυτά, πιστεύεται ότι εταιρείες με φήμη στην αξιόπιστη επεξεργασία συναλλαγών, την αποθήκευση δεδομένων και τη διαμεσολάβηση σε συναλλαγές, θα εισέλθουν και στο χώρο της βιομετρικής, εφόσον υπάρξουν κάποια εχέγγυα αξιοπιστίας, που προς το παρόν δεν τηρούνται. Αν πάντως αποτύχει η προσπάθεια για είσοδο τρίτων, τότε η βιομετρική αγορά θα επηρεαστεί αρνητικά.

**Χρησιμοποιούμενες τεχνολογίες και κάθετες αγορές**

Στις εφαρμογές ηλεκτρονικού εμπορίου, το σκανάρισμα των δαχτύλων θα επικρατήσει ως τεχνολογία, εφόσον βέβαια καθιερωθεί για desktop χρήση, όπως αναμένεται. Ενδεχομένως να χρησιμοποιηθούν και άλλες τεχνολογίες, π.χ. το σκανάρισμα της ίριδας ή του προσώπου, αλλά σίγουρα το σκανάρισμα των δαχτύλων έχει το προβάδισμα. Στο χώρο της τηλεφωνίας τώρα, το σκανάρισμα της φωνής συγκεντρώνει όλες τις πιθανότητες να κυριαρχήσει, με τις συσκευές κινητής τηλεφωνίας που διαθέτουν σκανάρισμα δαχτύλων όμως να διεκδικούν κάποιο βαθμό αποδοχής.

Οι δύο προφανείς κάθετες αγορές, στις οποίες μπορούν να εφαρμοστεί το ηλεκτρονικό εμπόριο αλλά και η τηλεφωνία, είναι οι οικονομικές υπηρεσίες και το σύστημα υγείας. Κι αυτό γιατί η πρόσβαση σε λογαριασμούς, οι οικονομικές συναλλαγές και η εξουσιοδότηση ιατρικών υπηρεσιών αποτελούν δραστηριότητες, για τις οποίες η απομακρυσμένη πιστοποίηση αποτελεί αναγκαιότητα.

**Κόστος ανάπτυξης**

Η βιομετρική δεν έχει χρησιμοποιηθεί μέχρι στιγμής σε κάποια εφαρμογή ηλεκτρονικού εμπορίου μεγάλης κλίμακας και η χρήση της στην τηλεφωνία είναι περιορισμένη. Έτσι, το κόστος ανάπτυξης δεν μπορεί να προσδιοριστεί με ακρίβεια. Είναι πιθανό ότι οι έμποροι θα πληρώνουν ένα σταθερό ή βάση ποσοστών αντίτιμο, για τις βιομετρικές υπηρεσίες των οποίων θα επωφελούνται. Ένα μέρος αυτού του ποσού θα αποδίδεται στους παρασκευαστές της βιομετρικής τεχνολογίας, για τη χορήγηση της κατάλληλης άδειας. Το μεγαλύτερο όμως ποσό θα δίνεται σε εξειδικευμένους χειριστές της τεχνολογίας, σε άτομα δηλαδή επιφορτισμένα με το έργο της ανάπτυξης εσωτερικών λύσεων λογισμικού και της παροχής επιπλέον λειτουργικότητας. Ένα πολύ αληθοφανές σενάριο αναφέρεται στην είσοδο στο χώρο ειδικών προμηθευτών βιομετρικής πιστοποίησης, δηλαδή εταιρειών με αποκλειστικό αντικείμενο την επιβεβαίωση της ταυτότητας των χρηστών. Είναι κάτι ανάλογο με τα οικονομικά ιδρύματα που χρησιμοποιούνται από τους εμπόρους στις συναλλαγές με πιστωτικές κάρτες και τα οποία επιβεβαιώνουν την οικονομική πίστη του πελάτη. Αντίστοιχα, οι προμηθευτές βιομετρικής πιστοποίησης θα απαλλάσσουν τους εμπόρους από το βάρος της

πιστοποίησης, επιτρέποντάς τους τη διενέργεια βιομετρικών συναλλαγών, στις οποίες αλλιώς δε θα είχαν πρόσβαση.

Στο χώρο της τηλεφωνίας, οι έμποροι και οι επιχειρήσεις μπορούν, είτε να υλοποιήσουν εσωτερικές λύσεις, που κοστίζουν μερικές δεκάδες χιλιάδες δολλάρια, ή να επιλέξουν εξωτερικές λύσεις, με δρομολόγηση όσων τηλεφωνούν σε τρίτους για πιστοποίηση. Πάντως, οι εφαρμογές τηλεφωνίας έχουν το πλεονέκτημα, ότι δε στηρίζονται σε πολλές, μη συμβατές συσκευές, όπως συμβαίνει στο χώρο του ηλεκτρονικού εμπορίου. Κι ακόμα, η χρήση βιομετρικής θα επιτρέψει στο χώρο αυτό συναλλαγές υψηλότερης αξίας και κινδύνου, απ' αυτές που εκτελούνται σήμερα.

**Ζητήματα υλοποίησης**

Κατά την υλοποίηση βιομετρικών συστημάτων για απομακρυσμένες συναλλαγές τίθενται ορισμένα ζητήματα. Το πρώτο απ' αυτά είναι η εγγραφή. Στις εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας, υπάρχει η ιδιαιτερότητα ότι οι χρήστες εγγράφονται απομακρυσμένα. Αυτό συνεπάγεται αυξημένο κίνδυνο για ψευδείς εγγραφές αφενός, και αφετέρου κακή ποιότητα των εγγραφών των νόμιμων χρηστών. Για την αποφυγή ψευδών εγγραφών, πρέπει να προηγείται μια μη βιομετρική διαδικασία πιστοποίηση της αυθεντικότητας, η οποία να στηρίζεται σε πληροφορίες πιο απόρρητες από το όνομα, την ημερομηνία γέννησης και τον αριθμό κοινωνικής ασφάλισης του χρήστη. Διαφορετικά, το σύστημα υπονομεύεται και τίθενται σε κίνδυνο λογαριασμοί ανυποψίαστων πολιτών. Απ' την άλλη, οι κακής ποιότητας εγγραφές υπονομεύουν το σύστημα με ένα εντελώς διαφορετικό τρόπο. Πράγματι, σε περιβάλλοντα που επιβλέπονται, γίνονται έλεγχοι που εξασφαλίζουν ότι οι εγγραφές τηρούν ένα ελάχιστο επίπεδο ποιότητας, κι αυτό μειώνει την πιθανότητα λανθασμένης απόρριψης. Αυτή η δυνατότητα επίβλεψης δεν υπάρχει στις απομακρυσμένες συναλλαγές, κι έτσι οι χαμηλής ποιότητας εγγραφές προκαλούν, όχι μόνο αυξημένο ποσοστό λανθασμένων απορρίψεων, αλλά και αυξημένο δείκτη λανθασμένων πιστοποιήσεων.

Ένα άλλο θέμα που τίθεται, είναι ο διαμοιρασμός από διάφορα ιδρύματα των δεδομένων εγγραφής των χρηστών, που συνήθως πραγματοποιείται με τη μεσολάβηση τρίτων. Πράγματι, η απαίτηση να εγγράφεται ο χρήστης ξεχωριστά, για κάθε μία από τις διάφορες εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας, δε φαίνεται λογική και

είναι πολύ πιο πρακτικό, η αρχική εγγραφή του χρήστη σ' ένα βιομετρικό σύστημα, να χρησιμοποιείται ως βάση μελλοντικών πιστοποιήσεων για ένα σύνολο συστημάτων. Απαραίτητη προϋπόθεση βέβαια, είναι η συγκατάθεση του εμπόρου, και κυρίως του ίδιου του χρήστη, ο οποίος μπορεί να αντιλαμβάνεται τα συνολικά πλεονεκτήματα, αλλά παράλληλα να φοβάται για πιθανή κακή χρήση των δεδομένων του. Οι φόβοι αυτοί πάντως αναμένεται να κοπάσουν, με την καθιέρωση αξιόπιστων third parties, που θα φέρουν την ευθύνη για το σωστό χειρισμό και τη διανομή των δεδομένων της εγγραφής.

Ένα ακόμα θέμα, αφορά στον καταμερισμό ευθυνών, σε περίπτωση λανθασμένης χορήγησης πρόσβασης. Πράγματι, οι πιθανότητες λένε ότι ακόμα και τα εύρωστα βιομετρικά συστήματα θα υποπέσουν κάποια στιγμή σε λάθος πιστοποίηση, επιτρέποντας έτσι τη διεκπεραίωση μιας συναλλαγής από έναν ψεύτικο χρήστη. Σ' αυτές τις περιπτώσεις, πρέπει να ξεκαθαριστεί αν η ευθύνη οικονομικής αποζημίωσης του πραγματικού χρήστη βαραίνει τον έμπορο ή τον προμηθευτή της βιομετρικής πιστοποίησης. Πάντως, αν η επιλεχθείσα λύση είναι εξωτερική, που σημαίνει ότι η πιστοποίηση δε βρίσκεται κάτω από τον άμεσο έλεγχο της επιχείρησης, το πιο πιθανό είναι να θεωρηθεί υπόλογος ο προμηθευτής.

Ένα ακόμα ζήτημα στις εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας, αφορά στην απόρριψη ενός μικρού ποσοστού έγκυρων χρηστών. Για να μην ταλαιπωρούνται περαιτέρω οι χρήστες, είναι αναγκαία η ύπαρξη fallback διαδικασιών για μη βιομετρική πιστοποίηση. Στις εφαρμογές τηλεφωνίας για παράδειγμα, μπορεί οι μη επιβεβαιωμένοι χρήστες να δρομολογούνται σ' έναν operator, ο οποίος και να πιστοποιεί την ταυτότητά τους με κατάλληλη υποβολή ερωτήσεων. Η αντιμετώπιση του προβλήματος γίνεται πιο σύνθετη στις εφαρμογές ηλεκτρονικού εμπορίου. Στις εφαρμογές με σκανάρισμα δαχτύλων, μια λύση είναι η χρησιμοποίηση ενός εναλλακτικού δακτυλικού αποτυπώματος. Άλλη λύση είναι η χρήση passwords, που όμως φέρει στην επιφάνεια όλα τα μειονεκτήματα της χρήσης κωδικών. Εξάλλου, υπάρχει και η δυνατότητα χρήσης ενός μηχανισμού ερωταποκρίσεων και στη συνέχεια επανεγγραφής του χρήστη στο σύστημα, για την αποφυγή μελλοντικών προβλημάτων. Το μειονέκτημα αυτής της διαδικασίας είναι ότι ο χρήστης έχει συνηθίσει σε γρήγορους μηχανισμούς πιστοποίησης για on-line συναλλαγές. Γενικά πάντως, μετά από μια σειρά αποτυχημένων προσπαθειών για πιστοποίηση είναι συνήθης τακτική το κλείδωμα του λογαριασμού, ούτως ώστε να εξαλειφθεί η πιθανότητα παραβίασής του.

Σημαντικό θέμα αποτελεί επίσης η συμβατότητα των συσκευών. Συνήθως οι εγγραφές που πραγματοποιούνται σε μία συσκευή, δεν μπορούν να χρησιμεύσουν για πιστοποίηση σε μια άλλη. Αυτό το πρόβλημα καλούνται να λύσουν οι επιχειρήσεις που χρησιμοποιούν βιομετρικά συστήματα, και οι οποίες ενδιαφέρονται για τη χρήση συμβατών συσκευών, που όμως να διακρίνονται και από ένα ελάχιστο βαθμό ακρίβειας και απόδοσης. Αντίστοιχη συμβατότητα βέβαια, πρέπει να χαρακτηρίζει και τις υποδομές των επιχειρήσεων.

Εξάλλου, παρά την εξάπλωση που αναμένεται να γνωρίσει η βιομετρική στις εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας, οι παραδοσιακές διαδικασίες και ρουτίνες πιστοποίησης της αυθεντικότητας θα διατηρηθούν. Η βιομετρική τεχνολογία, τουλάχιστον στην αρχή, θα στηριχθεί στα υπάρχοντα back end συστήματα και δε θα τα αντικαταστήσει. Είναι πολύ ρεαλιστικό το παράδειγμα ενός συστήματος, στο οποίο το 80% των πελατών χρησιμοποιεί passwords και το 20% βιομετρική τεχνολογία. Σ' αυτό το σύστημα, είναι πιθανό οι βιομετρικές συναλλαγές να σημειώνονται με ειδική ένδειξη, ώστε να υποβάλλονται σε διαφορετικές διαδικασίες επεξεργασίας και χρέωσης. Εντούτοις, το επιστρεφόμενο αποτέλεσμα δεν πρέπει να ξεχωρίζει από το αποτέλεσμα που επιστρέφεται με χρήση password. Συνεπώς, η βιομετρική τεχνολογία πρέπει να είναι σε θέση να τροφοδοτεί το παραδοσιακό σχήμα πιστοποίησης με τις απαντήσεις της.

Επίσης, οι επιχειρήσεις πρέπει να εξισορροπήσουν την ανάγκη για αποτροπή επιθέσεων με την απαίτηση για επιβεβαίωση των έγκυρων χρηστών. Αυτό σημαίνει, ότι πρέπει να θέσουν τις προτεραιότητές τους και να προσαρμόσουν ανάλογα τα επίπεδα ασφάλειας του συστήματος. Το επιθυμητό επίπεδο ασφαλείας, συνήθως βρίσκεται μετά από δοκιμές στην πράξη, αφού τα μέτρα ακρίβειας που επικαλούνται οι προμηθευτές βασίζονται κατά κανόνα σε εργαστηριακές δοκιμές, που δεν αντικατοπτρίζουν πλήρως τις πραγματικές συνθήκες. Πάντως, ένα καλά σχεδιασμένο σύστημα, με ασφαλείς διαδικασίες μπορεί να περιορίσει τις λανθασμένες απορρίψεις, χωρίς να αποτελεί εύκολο στόχο για τους επιτιθέμενους.

Καθώς η αγορά του ηλεκτρονικού εμπορίου και της τηλεφωνίας διευρύνεται, οι επιχειρήσεις έχουν να επιλέξουν μεταξύ της ανάπτυξης κατάλληλης εσωτερικής υποδομής και της δρομολόγησης της διαδικασίας πιστοποίησης σε κάποια εξωτερική

εταιρεία. Και οι δύο προσεγγίσεις χαρακτηρίζονται από πλεονεκτήματα και μειονεκτήματα. Για παράδειγμα, η ύπαρξη εσωτερικής υποδομής μειώνει την εξάρτηση από third parties και διασφαλίζει το χειρισμό των δεδομένων με τρόπο συνεπή με την πολιτική της επιχείρησης. Επιπλέον, ζητήματα απόδοσης αντιμετωπίζονται πιο καλά και άμεσα, αφού τα PCs που διεξάγουν την πιστοποίηση βρίσκονται υπό τον έλεγχο της επιχείρησης. Από την άλλη, η εσωτερική υποδομή προϋποθέτει διαρκή ετοιμότητα της επιχείρησης για αποθήκευση και επεξεργασία δεδομένων, κι ακόμη την ενημέρωσή της για θέματα ακρίβειας κι απόδοσης των συσκευών. Επίσης, σημαίνει ότι όποια προβλήματα εγείρονται αντιμετωπίζονται από την ίδια και το ανθρώπινο δυναμικό της.

Αντίθετα, η ανάπτυξη υποδομής για εξωτερική πιστοποίηση επιτρέπει στις επιχειρήσεις να επικεντρωθούν στο αντικείμενό τους, επωφελούμενες της δυνατότητας για βιομετρική πιστοποίηση, με την καταβολή ελάχιστης δυνατής προσπάθειας. Γενικά, οι διαδικασίες εγγραφής, απόκτησης και διαχείρισης των δεδομένων περνούν πέρα από τον έλεγχό των επιχειρήσεων, οι οποίες δε χρειάζεται να είναι ενήμερες για τις τρέχουσες βιομετρικές εξελίξεις. Ακόμη και το κόστος είναι συγκριτικά πιο προβλέψιμο, αφού συνήθως οι έμποροι καλούνται να καταβάλουν περιοδικά ένα σταθερό ποσό. Από την άλλη όμως, η εξωτερική πιστοποίηση προϋποθέτει εμπιστοσύνη στις ικανότητες ενός τρίτου να διαχειρίζεται και να διασφαλίζει την ακεραιότητα ευαίσθητων προσωπικών δεδομένων. Η εξάρτηση αυτή επεκτείνεται και σε θέματα ταχύτητας επεξεργασίας των συναλλαγών, χρήσης ή όχι αποδοτικών συσκευών κτλ. Γι' αυτό δεν είναι απορίας άξιον, που πολλοί οργανισμοί διστάζουν να εναποθέσουν τη διαχείριση αυτών των κρίσιμων ζητημάτων σε ένα τρίτο φορέα.

**Συμπεράσματα**

Στις εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας, η βιομετρική χρησιμοποιείται με σκοπό την επίλυση προβλημάτων, τα οποία είναι σύμφυτα με την απομακρυσμένη πιστοποίηση μεταξύ δύο μερών, που δε γνωρίζονται και δεν εμπιστεύονται το ένα το άλλο. Καθώς η ανάγκη για διεκπεραίωση συναλλαγών υψηλής αξίας και ανταλλαγής δεδομένων αποκτά ολοένα και περισσότερο κρίσιμο κι επιτακτικό χαρακτήρα, η χρήση της βιομετρικής αναμένεται να εξαπλωθεί στο άμεσο μέλλον και να αποτελέσει σημαντική κι επικερδή πρόταση.

### 4.3.2 Εμπόριο/ATM/Σημείο πώλησης

Οι εφαρμογές εμπορίου, ATM και σημείου πώλησης (point of sale - POS) αναφέρονται στη χρήση βιομετρικής, με σκοπό την αναγνώριση ή την πιστοποίηση της ταυτότητας ενός ατόμου, που προσέρχεται σ' ένα σημείο και συναλλάσσεται από κοντά για την απόκτηση αγαθών ή υπηρεσιών. Στις περιπτώσεις αυτές, η βιομετρική λειτουργεί συμπληρωματικά ή στη θέση παραδοσιακών σχημάτων πιστοποίησης, όπως είναι η επίδειξη της ταυτότητας, η χρήση υπογραφής, PINs κτλ.[1]

Οι εφαρμογές αυτής της κατηγορίας μπορεί να διαφέρουν σημαντικά μεταξύ τους, ενώ είναι συνήθως εφαρμογές πιστοποίησης ή αναγνώρισης ένα-προς-λίγα, που σημαίνει ότι η έρευνα εντοπισμού γίνεται με βάση μια μικρή ομάδα εγγεγραμμένων χρηστών. Οι εφαρμογές εμπορίου, ATM και σημείου πώλησης μοιάζουν με τις εφαρμογές ηλεκτρονικού εμπορίου και τηλεφωνίας, ως προς το ότι είναι και οι δύο κατά κανόνα εθελοντικές, αφού δεν είναι προς όφελος των εταιρειών να εξαναγκάζουν τους πελάτες σε βιομετρική πιστοποίηση. Διαφέρουν όμως, ως προς το ότι οι εφαρμογές εμπορίου πραγματοποιούνται πολύ πιο συχνά υπό συνθήκες επίβλεψης, σε σύγκριση με τις εφαρμογές ηλεκτρονικού εμπορίου.

**Τυπικές εφαρμογές**

Μέχρι στιγμής, η βιομετρική χρησιμοποιείται σε πολύ λίγες εφαρμογές εμπορίου, ATM και σημείου πώλησης. Ακόμα όμως και αυτές οι λίγες, όχι ιδιαίτερα φιλόδοξες εφαρμογές αποδεικνύουν τη βιωσιμότητα των βιομετρικών λύσεων σ΄ αυτά τα περιβάλλοντα. Η πιο συνηθισμένη εφαρμογή της βιομετρικής, είναι σε κιόσκια ATM. Πράγματι, τα μηχανήματα ATM συνθέτουν το ιδανικό περιβάλλον για να εφαρμοστεί η βιομετρική τεχνολογία, αφού το σύνηθες σχήμα πιστοποίησης που χρησιμοποιούν, τα PINs, είναι επιρρεπή σε παραβίαση, εύκολο να τα μαντέψει ή να τα ξεχάσει κανείς. Πάντως, ακόμα κι όταν εφαρμόζεται σε ειδικά αναπροσαρμοσμένα ATMs στη θέση

[1] http://www.bankersonline.com/articles/bhv09n12/bhv09n12a2.html

PINs, η βιομετρική συνήθως δεν καταργεί την ανάγκη ύπαρξης καρτών ή κάποιου άλλου προσδιοριστή.[1]

Στις εφαρμογές εμπορίου/σημείου πώλησης η βιομετρική συνήθως χρησιμοποιείται με τη μορφή σκαναρίσματος δαχτύλων, για την πληρωμή των συναλλαγών μέσω ενός προκαθορισμένου λογαριασμού. Αυτό που συμβαίνει δηλαδή, είναι ότι υπάρχει σύνδεση των δεδομένων του χρήστη με ένα χρεωστικό ή πιστωτικό λογαριασμό, ο οποίος χρεώνεται μετά από επιτυχημένη πιστοποίηση. Αυτό το σχήμα, εφαρμόζεται στην Αμερική, σε πολλά παντοπωλεία και καφετέριες, παράλληλα με τον παραδοσιακό τρόπο πληρωμής. Τα βιομετρικά συστήματα που χρησιμοποιούνται, συνήθως δεν είναι ενσωματωμένα στα υπάρχοντα συστήματα πελατών και δρουν ως ανεξάρτητα συστήματα, με ξεχωριστές βάσεις δεδομένων. Οι βιομετρικές συναλλαγές καταχωρούνται ξεχωριστά, αλλά συνδέονται και με το υπάρχον σύστημα καταχωρίσεων.

**Νέες τάσεις**

Η χρήση της βιομετρικής σε εφαρμογές εμπορίου/ATM/σημείου πώλησης οφείλεται κατά κύριο λόγο στην ανάγκη των επιχειρήσεων για περιορισμό της απάτης, και λιγότερο στην επιθυμία τους να ηγηθούν των εξελίξεων. Πράγματι, η απάτη με χρήση επιταγών και πιστωτικών καρτών ταλαιπωρεί το χώρο του εμπορίου και ιδιαίτερα τους πωλητές που θεωρούνται υπόλογοι για τη ζημία της επιχείρησης. Αν ωστόσο, για τη χρήση επιταγών απαιτείται προηγούμενη εγγραφή του πελάτη στο βιομετρικό σύστημα και συσχέτισή του με έναν ενεργό λογαριασμό, αυτό αποτελεί ριζικό μέτρο καταπολέμησης της απάτης. Το μέτρο αυτό, μπορεί να θεωρηθεί ότι διευκολύνει και τους πελάτες, οι οποίοι δε χρειάζεται να επιδεικνύουν την ταυτότητα τους ή κάποιο άλλο έγγραφο για πιστοποίησή.

Ο παράγοντας που αναμένεται να αποτελέσει κλειδί για την ευρεία διάδοση της βιομετρικής είναι η ικανότητα εγγραφής ενός μεγάλου αριθμού χρηστών μέσα από ένα μέτριο πλήθος συσκευών. Επιπλέον, η δυνατότητα συνέργιας της βιομετρικής με τις smart cards ενδέχεται να εκτινάξει στα ύψη τις εφαρμογές εμπορίου, αφού οι smart cards

[1] http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-004850/

είναι κατάλληλες για αποθήκευση των βιομετρικών δεδομένων και πιστοποιούν την ταυτότητα των κατόχων τους, που είναι και το μεγάλο πρόβλημα στις εφαρμογές εμπορίου. Έτσι, ειδικά σε χώρες εκτός των Ηνωμένων Πολιτειών, η ανάπτυξη υποδομής για συνδυασμένη χρήση βιομετρικής και smart cards είναι πολύ πιθανή.

Από την άλλη, ένας παράγοντας που ενδεχομένως εμποδίσει την εξάπλωση της βιομετρικής στο χώρο του εμπορίου, είναι η δυσκολία και πολυπλοκότητα υλοποίησης των αντίστοιχων συστημάτων. Σε αντίθεση με τις απομακρυσμένες συναλλαγές, όπου οι συσκευές απόκτησης βρίσκονται ήδη στη θέση τους ή θα βρίσκονται σε μεγάλο βαθμό μέσα στα επόμενα δύο χρόνια, οι βιομετρικές συναλλαγές που γίνονται κατά πρόσωπο προϋποθέτουν την υλοποίηση και ενσωμάτωση εξειδικευμένων συσκευών στα υπάρχοντα συστήματα. Η ενσωμάτωση όμως βιομετρικής σε ATMs έχει αποδειχθεί πολυέξοδη, ενώ ακόμα και η πτώση των τιμών των ATM μηχανημάτων αυξάνει το κόστος ενσωμάτωσης βιομετρικής λειτουργικότητας σε αυτά. Αλλά και στις περιπτώσεις του σημείου πώλησης, η ενσωμάτωση βιομετρικής μπορεί να αποδειχθεί εξίσου πολύπλοκη, ειδικά αν αναλογιστεί κανείς το εύρος των τερματικών, υπολογιστικών συστημάτων και συστημάτων καταχωρίσεων, με τα οποία υπάρχει ανάγκη για αλληλεπίδραση.

Άλλα προβλήματα, σχετίζονται με την ανάγκη εκπαίδευσης των χρηστών, αλλά και των καθημερινών λειτουργών του συστήματος. Ειδικά μάλιστα για τους χρήστες, που δεν έχουν κάποιο κίνητρο να χρησιμοποιήσουν το σύστημα (όσοι για παράδειγμα είναι εγγεγραμμένοι σ' ένα υποχρεωτικό σύστημα), η διαδικασία εκπαίδευσης μπορεί να αποβεί ιδιαιτέρως δύσκολη. Ένας ακόμα λόγος που μπορεί να ανακόψει την πορεία της βιομετρικής είναι ο φόβος για πιθανά λάθη του συστήματος. Ως γνωστόν, η βιομετρική υποπίπτει ενίοτε σε λάθη απόρριψης έγκυρων χρηστών. Στο χώρο του εμπορίου όμως, αυτά τα λάθη έχουν σημαντικό αντίκτυπο, αφού αμφισβητείται η ταυτότητα έγκυρων πελατών. Γι' αυτό, η ακολουθούμενη πολιτική πρέπει να εξισορροπεί την ανάγκη για αποτροπή της απάτης με τις συνέπειες από τη λανθασμένη απόρριψη πελατών.

**Χρησιμοποιούμενες τεχνολογίες και κάθετες αγορές**

Το σκανάρισμα του προσώπου, των δαχτύλων και της ίριδας έχει χρησιμοποιηθεί με επιτυχία σε κιόσκια ATM σε Βόρεια Αμερική, Ευρώπη και Ασία, χωρίς ωστόσο να υπάρχει μια τυπική ATM συναλλαγή[1]. Όταν χρησιμοποιείται σκανάρισμα δαχτύλων, οι χρήστες συνήθως καλούνται να παρουσιάσουν μια κάρτα ή έναν προσδιοριστή, για να μπορέσει να ακολουθήσει ταίριασμα 1:1. Το σκανάρισμα της ίριδας χρησιμοποιείται σε ATMs κυρίως σε εφαρμογές αναγνώρισης, όπου το άτομο αναγνωρίζεται από το σύστημα, χωρίς προηγούμενη εισαγωγή δεδομένων ή παρουσίαση token. Αντίστοιχα, το σκανάρισμα του προσώπου εξυπηρετεί περιπτώσεις πιστοποίησης ή και περιπτώσεις αναγνώρισης από μια υποβαθμισμένη βάση δεδομένων.

Από τις τρεις τεχνολογίες, το σκανάρισμα του προσώπου είναι η πιο διαδεδομένη λύση, με σχεδόν ένα εκατομμύριο εγγεγραμμένους χρήστες. Ωστόσο, σε περίπτωση που το σκανάρισμα του προσώπου αποτύχει στην πιστοποίηση, κάτι που δεν είναι ασυνήθιστο, τότε οι χρήστες αποστέλλονται σε ένα άτομο ειδικά επιφορτισμένο με το έργο της πιστοποίησης. Γενικά, το σκανάρισμα των δαχτύλων αναμένεται να επικρατήσει ως τεχνολογία, στις εφαρμογές εμπορίου και σημείου πώλησης, αφού παρέχει την ιδανικό συνδυασμό ακρίβειας και ευκολίας χρήσης. Το σκανάρισμα του προσώπου υπολείπεται σε ασφάλεια και δεν μπορεί να χρησιμοποιηθεί για σύγκριση με βάσεις δεδομένων που δεν είναι υποβαθμισμένες, ενώ το σκανάρισμα της ίριδας είναι μια λύση αρκετά ακριβή, στην οποία πιθανόν να μην αντεπεξέλθουν αυτά τα περιβάλλοντα.

**Κόστος ανάπτυξης**

Στα περιβάλλοντα εμπορίου, ATM και σημείου πώλησης οι τιμές δεν έχουν ακόμα οριοθετηθεί με ακρίβεια. Στην καλύτερη, από οικονομικής πλευράς περίπτωση, υπάρχουν συσκευές σκαναρίσματος δαχτύλων των $500 αρκετά εύρωστες για να αντεπεξέλθουν σε βαριά χρήση στα ταμεία των εμπορικών καταστημάτων. Το κόστος βέβαια, μπορεί να

[1] Η τυπική χρήση περιλαμβάνει πιστοποίηση με σκανάρισμα προσώπου και εισαγωγή του αριθμού κοινωνικής ασφάλισης, εν είδει μοναδικού προσδιοριστή.

φτάσει και σε δεκάδες χιλιάδες δολάρια, όπως στην περίπτωση ATM συστημάτων με σκανάρισμα ίριδας. Πάντως, οι πιο ακριβές λύσεις είναι εκείνες που απαιτούν ενσωμάτωση βιομετρικής λειτουργικότητας στα υπάρχοντα συστήματα. Το κόστος σ' αυτές τις περιπτώσεις είναι κυμαινόμενο, ανάλογα με το εύρος της εφαρμογής και την πολυπλοκότητα του παλαιού συστήματος. Οι λιγότερο ακριβές λύσεις, είναι εκείνες των ανεξάρτητων βιομετρικών συστημάτων, που απαιτούν πέρασμα της βιομετρικής συναλλαγής στο υπάρχον σύστημα καταχωρίσεων από τους ταμίες. Αυτά τα συστήματα συνήθως μισθώνονται επ' αόριστο από τα καταστήματα, με αντίτιμο μια μηνιαία συνδρομή κι ένα ποσοστό επί της αξίας των συναλλαγών. Το τελικό ποσό δικαιολογείται, αν αναλογιστεί κανείς την ετήσια ζημία των επιχειρήσεων λόγω απάτης. Εξάλλου, στη μηνιαία συνδρομή συνήθως περιλαμβάνονται και τα κόστη υλοποίησης, ενσωμάτωσης και εκπαίδευσης, σε μια προσπάθεια να περιοριστούν οι αρχικές δαπάνες της επιχείρησης.

Πάντως, ένας από τους λόγους που αυτός ο τομέας θεωρείται τόσο ελκυστικός για τις εταιρείες βιομετρικής, είναι επειδή μπορεί να εφαρμοστεί το μοντέλο εσόδων ανά συναλλαγή. Οι ίδιοι οι κατασκευαστές βιομετρικού hardware και αλγορίθμων δε θα αποκομίσουν πολλά, αφού ένας περιορισμένος αριθμός συσκευών μπορεί να καλύψει τις ανάγκες ενός εμπορικού καταστήματος. Όμως, οι εταιρείες παροχής βιομετρικών λύσεων, που θα προσφέρουν πλήρη βιομετρικά συστήματα πληρωμής, θα είναι και οι τελικοί αποδέκτες των μεγαλύτερων εσόδων.

**Ζητήματα υλοποίησης**

Υπάρχουν ορισμένα βασικά ζητήματα που πρέπει να αντιμετωπιστούν, κατά την υλοποίηση βιομετρικών συστημάτων για εμπορικές εφαρμογές. Πρώτα απ' όλα, οι χρήστες ως γνωστόν, είναι συνηθισμένοι σε συγκεκριμένες διαδικασίες πιστοποίησης στο χώρο του εμπορίου. Είναι σημαντικό επομένως, να εξασφαλίσουν οι κατασκευαστές, ότι τα νέα συστήματα θα είναι εργονομικά και εύκολα στη χρήση, ακόμα και για τους μη εξοικειωμένους χρήστες. Εξάλλου, η ακρίβεια των βιομετρικών συστημάτων εξαρτάται άμεσα από την ικανότητα των χρηστών να αλληλεπιδρούν μ' αυτά με τρόπο συνεπή.

Ένα άλλο ζήτημα που πρέπει να διευκρινιστεί, είναι ο βαθμός ενσωμάτωσης των βιομετρικών συστημάτων στα ήδη υπάρχοντα. Στα ATMs για παράδειγμα, η πολύ στενή

ενσωμάτωση αποτελεί αναγκαιότητα και προϋπόθεση για την πυροδότηση της διαδικασίας χορήγησης χρημάτων. Στα περιβάλλοντα εμπορίου και σημείου πώλησης όμως, υπάρχει μεγαλύτερη ευχέρεια επιλογών. Μία λύση είναι η υλοποίηση ανεξάρτητων βιομετρικών συστημάτων, που είναι μεν πιο φτηνά, αλλά έχουν περιορισμένη λειτουργικότητα και απαιτούν τη χειρωνακτική εισαγωγή ορισμένων πληροφοριών. Η άλλη λύση, υπαγορεύει τη σύνδεση των βιομετρικών συστημάτων με τα συστήματα καταχώρισης των συναλλαγών, ούτως ώστε κάθε πετυχημένη βιομετρική πιστοποίηση να συνεπάγεται απευθείας ολοκλήρωση της συναλλαγής. Η λύση αυτή σίγουρα είναι προτιμότερη για εφαρμογές μεγάλης κλίμακας, γιατί επιτρέπει την καλύτερη παρακολούθηση και τον εντοπισμό των συναλλαγών.

Αυτό που πρέπει να γίνει αντιληπτό πάντως στην περίπτωση των εφαρμογών εμπορίου, είναι ότι οι επιχειρήσεις κυρίως επωφελούνται και όχι ο πελάτης. Κι αυτό γιατί οι πελάτες, μπορεί να αισθάνονται ικανοποιημένοι από τη μη χρήση PINs και εγγράφων πιστοποίησης, αλλά και πάλι είναι υποχρεωμένοι να χρησιμοποιούν κάρτες ή κάποιον άλλο προσδιοριστή. Επομένως, είναι σημαντικό οι επιχειρήσεις να εξηγήσουν στους πελάτες τους, τους λόγους χρήσης αυτών των συστημάτων, και να τους δώσουν επιπλέον κίνητρα για να εγγραφούν. Πέρα από αυτό, είναι αναγκαίο να εξαλειφθεί με βάσιμα επιχειρήματα και επίκληση του τρόπου λειτουργίας του συστήματος, κάθε φόβος για παραβίαση της ιδιωτικότητας.

**Συμπεράσματα**

Η βιομετρική αποτελεί μια λύση, με περιορισμένες ως τώρα εφαρμογές στο χώρο του εμπορίου. Το κατά πόσο θα καταφέρει να εξαπλωθεί και να πρωταγωνιστήσει στο χώρο, εξαρτάται απ' το αν η ανάγκη για ασφάλεια, διευκόλυνση και αποτροπή της απάτης υπερισχύσει του υψηλού κόστους και της πολυπλοκότητας της τεχνολογίας.

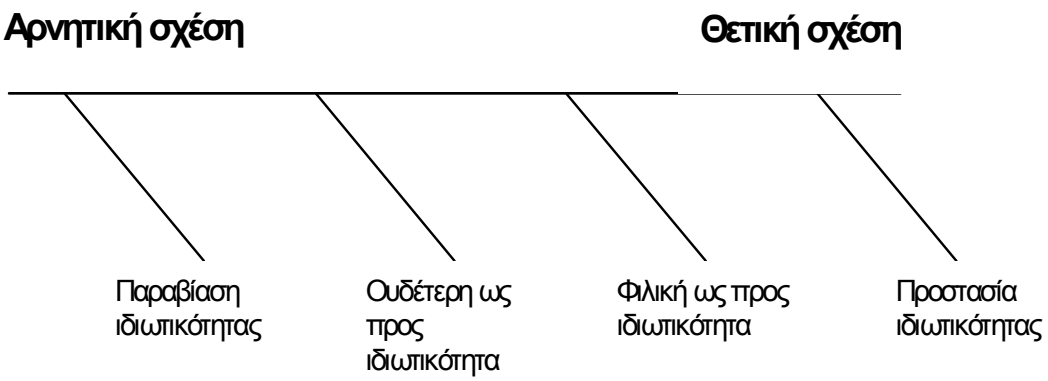
## 5.1 ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Η έννοια της ιδιωτικότητας είναι δύσκολο να οριστεί, γιατί οι απαιτήσεις σε ιδιωτικότητα μεταβάλλονται, ανάλογα με τις τεχνολογικές εξελίξεις, το βαθμό εμπιστοσύνης απέναντι στα κρατικά και δημόσια ιδρύματα και τη συναίνεση του κοινού για παραχωρήσεις σε θέματα ιδιωτικότητας, με στόχο την επίτευξη μεγαλύτερης ασφάλειας. Γενικά πάντως,

μπορεί κάποιος να είναι ταυτόχρονα υπέρμαχος και της βιομετρικής και των ζητημάτων ιδιωτικότητας, αρκεί η βιομετρική να υλοποιείται με τρόπο συνεπή ως προς κάποιες βασικές αρχές[1].

### 5.1.1 Σχέσεις βιομετρικής και ιδιωτικότητας

Η βιομετρική μπορεί να παραβιάζει την ιδιωτικότητα, να είναι ουδέτερη σε θέματα ιδιωτικότητας, να είναι φιλική σε θέματα ιδιωτικότητας, ή τέλος να προστατεύει την ιδιωτικότητα, όπως φαίνεται και στο Σχήμα 32.




Στο χειρότερο δυνατό σενάριο, η χρήση της βιομετρικής παραβιάζει την ιδιωτικότητα. Η βιομετρική είναι μια τεχνολογία, που μπορεί να εφαρμοστεί, χωρίς τη γνώση ή την έγκριση του ατόμου. Μπορεί ακόμα να στηριχτεί στη διαρροή πληροφοριών από άλλες πηγές. Επομένως, αν δεν υπόκειται σε περιορισμούς, ενδεχομένως χρησιμοποιηθεί για λόγους παραβίασης της ιδιωτικότητας, όπως για τον εντοπισμό ατόμων, την κατάργηση της ανωνυμίας κτλ. Στην κατηγορία αυτή, υπάγονται ακόμα και συστήματα που είναι εν δυνάμει ικανά για παραβιάσεις της ιδιωτικότητας, χωρίς να έχουν χρησιμοποιηθεί γι' αυτό το σκοπό, αφού και μόνο το ενδεχόμενο κακής χρήσης τους τα καθιστά ζημιογόνα. Η βιομετρική είναι ουδέτερη σε θέματα ιδιωτικότητας, όταν δε λαμβάνει μέτρα προφύλαξης ή σχεδιαστικά μέτρα για τη διασφάλιση των παραμέτρων ιδιωτικότητας, αλλά παρόλα αυτά δεν μπορεί να χρησιμοποιηθεί με τρόπο που να παραβιάζει την ιδιωτικότητα. Πολλές βιομετρικές τεχνολογίες, που δεν μπορούν να προστατεύσουν τις πληροφορίες των ατόμων, αλλά δεν έχουν τη δυνατότητα να δράσουν υπονομευτικά προς την έννοια της ιδιωτικότητας, ανήκουν σ' αυτή την κατηγορία.

[1] http://www.tovima.gr/relatedarticles/articlelist/

Οι εφαρμογές που είναι φιλικές σε θέματα ιδιωτικότητας ενσωματώνουν ειδικά σχεδιαστικά στοιχεία και διαδικασίες ελέγχου, ούτως ώστε να μην υπάρχει περιθώριο χρήσης των βιομετρικών δεδομένων με τρόπο που να παραβιάζει την ιδιωτικότητα. Συστήματα που προνοούν για κρυπτογράφηση των δεδομένων, που απαιτούν πολλούς διαχειριστές για πρόσβαση στη βάση δεδομένων ή που αποθηκεύουν τα βιομετρικά δεδομένα ξεχωριστά από τα προσωπικά δεδομένα λειτουργούν προς αυτή την κατεύθυνση. Αν και στα συστήματα που είναι φιλικά σε ζητήματα ιδιωτικότητας η προστασία δεν είναι απόλυτη, ωστόσο λαμβάνονται κάποιες ενέργειες, που καθιστούν απίθανη την κακόβουλη χρήση των βιομετρικών δεδομένων. Εφαρμογές που προστατεύουν την ιδιωτικότητα, θεωρούνται εκείνες στις οποίες το κίνητρο διεξαγωγής βιομετρικής πιστοποίησης είναι η προστασία προσωπικών πληροφοριών του ατόμου, που διαφορετικά θα αποτελούσαν αντικείμενο παραβίασης. Η παροχή στο χρήστη του δικαιώματος πρόσβασης σε τραπεζικούς λογαριασμούς, ιατρικά δεδομένα ή άλλα προσωπικά αρχεία, μέσα από μια εναλλακτική διαδικασία βιομετρικής πιστοποίησης, αντί για την παραδοσιακή πιστοποίηση με κάρτες και κωδικούς, είναι μια τυπική εφαρμογή αυτής της κατηγορίας. Αντίστοιχα, η υποχρεωτική υποβολή σε βιομετρικό έλεγχο για πρόσβαση σε ευαίσθητα αρχεία είναι μια διαδικασία που προστατεύει την ιδιωτικότητα, αφού αποθαρρύνει τους υπαλλήλους από την πρόσβαση σε προστατευόμενα δεδομένα, αφήνοντας ίχνη ικανά να προδώσουν τον παραβάτη.

Γενικά, η διαχωριστική γραμμή, ανάμεσα στα διάφορα είδη ιδιωτικότητας, δεν είναι πάντα ευκρινής και είναι εύκολο να παραβιαστεί. Πολλές φορές είναι η ίδια η εφαρμογή και όχι η τεχνολογία, που καθορίζει το βαθμό προστασίας της ιδιωτικότητας.

### 5.1.2 Τα σημαντικότερα ζητήματα ιδιωτικότητας

Τα θέματα ιδιωτικότητας χωρίζονται σε δύο κατηγορίες, στην παραβίαση των πληροφοριών και στους προσωπικούς φόβους των ατόμων. Η πρώτη κατηγορία σχετίζεται με τη μη εξουσιοδοτημένη συλλογή, αποθήκευση και χρήση βιομετρικών πληροφοριών, ενώ η δεύτερη αναφέρεται στη δυσφορία που προκαλεί σε πολλά άτομα η χρήση βιομετρικών τεχνολογιών. Αν και κάθε εφαρμογή πρέπει να αντιμετωπίζει και τα δύο ζητήματα, μεγαλύτερη έμφαση δίνεται στην παραβίαση πληροφοριών.

**Παραβίαση πληροφοριών**

Χάρη στην πρόοδο της τεχνολογίας, οι ιδιωτικοί και δημόσιοι οργανισμοί έχουν πλέον τη δυνατότητα της συγκέντρωσης, αποθήκευσης και σύγκρισης διαφόρων πληροφοριών για κάθε άτομο. Χρησιμοποιώντας προσδιοριστές, όπως το όνομα, η διεύθυνση και ο αριθμός κοινωνικής ασφάλισης, οι διάφοροι οργανισμοί μπορούν να ψάξουν και σε άλλες βάσεις δεδομένων για πληροφορίες σχετικές με κάθε άτομο. Αυτές οι πληροφορίες μπορεί να σχετίζονται με το εργασιακό, οικονομικό ή ιατρικό ιστορικό του ατόμου, τις αγοραστικές του συνήθειες και τα προσωπικά του ενδιαφέροντα. Ορισμένες φορές αυτός ο διαμοιρασμός και η δυνατότητα συνάθροισης πληροφοριών είναι επωφελής, όπως στην περίπτωση επείγουσων ιατρικών πληροφοριών, τις οποίες μοιράζονται πολλά νοσοκομεία. Όμως εύκολα μπορεί να γίνει κατάχρηση και η ύπαρξη βάσεων δεδομένων, που είναι σε θέση να εξερευνηθούν, να καταλήξει στη δημιουργία συγκεντρωτικών προφίλ των χρηστών. Αυτά τα προφίλ μπορεί να έχουν ως συνέπεια οι εργοδότες να κάνουν προσλήψεις, ανάλογα με ιδιωτικές ιατρικές πληροφορίες, ή οι ασφαλιστές να προσαρμόζουν τα ασφάλιστρα για όσα άτομα έχουν παρουσιάσει διάφορες παθήσεις κτλ.

Εξαιτίας λοιπόν των κινδύνων που δημιουργούνται από τη μη εξουσιοδοτημένη διαρροή προσωπικών δεδομένων, είναι πολύ σημαντικό να προστατεύεται το δικαίωμα του ατόμου να ασκεί έλεγχο και να δίνει τη συγκατάθεσή του για τη συλλογή, αποθήκευση, χρήση ή αποκάλυψη των δεδομένων που τον αφορούν. Αυτό είναι στην ουσία το δικαίωμα στη μη παραβίαση των πληροφοριών. Γενικά, το πρόβλημα δεν προκαλείται από τα βιομετρικά δεδομένα καθεαυτά, αλλά από τη σύνδεσή τους με προσωπικές πληροφορίες του ατόμου. Η πιθανή διαρροή, παραβίαση ή κακή χρήση αυτών των προσωπικών πληροφοριών συνιστά παραβίαση της ιδιωτικότητας. Η λύση δεν είναι η διενέργεια ελέγχου, προς αποφυγήν των μη εξουσιοδοτημένων διαρροών, αφού αν είναι έστω και θεωρητικά δυνατό να διαρρεύσουν προσωπικά δεδομένα, υπάρχει κίνδυνος από άποψη ιδιωτικότητας. Ιδανικά δηλαδή, σε ένα σύστημα που είναι φιλικό για την ιδιωτικότητα, πρέπει να μην υπάρχει τρόπος διαρροής και συσχέτισης με προσωπικά δεδομένα, ακόμα κι αν η διαρροή αυτή είναι νομικά κατοχυρωμένη. Προς το παρόν, φαίνεται πως υπάρχει ευαισθησία του νομοθέτη σε θέματα ιδιωτικότητας, αλλά λόγω των παγκόσμιων εξελίξεων είναι πολύ πιθανό αυτή η στάση να αλλάξει και να ζητηθεί χρήση βιομετρικών δεδομένων για σκοπό, πέρα από τον προκαθορισμένο. Αν αυτό όμως είναι ανέφικτο από κατασκευής του συστήματος, τότε δεν τίθεται ανάλογο θέμα. Συνεπώς, ο

σχεδιασμός των ευφυών βιομετρικών συστημάτων περιορίζει τη μετατροπή των δεδομένων σε εργαλεία παραβίασης της ιδιωτικότητας.

Γενικά πάντως, η βιομετρική θεωρείται ως μια τεχνολογία εξαιρετικά επίφοβη για ζητήματα παραβίασης πληροφοριών, γιατί βασίζεται σε ανθρώπινα δεδομένα, που συνιστούν ένα προσδιοριστή αμετάβλητο. Η αναλλοίωτη φύση του προσδιοριστή, προκαλεί την ανησυχία, ότι αυτός μπορεί να αποτελέσει το μέσο για τον εντοπισμό πληροφοριών σε διάφορες βάσεις δεδομένων, που αφορούν σε όλους τους τομείς της ζωής του ατόμου, από την εργασία ως την ιδιωτική ζωή. Οι μεγαλύτερες απειλές για την παραβίαση των πληροφοριών είναι η μη εξουσιοδοτημένη χρήση των βιομετρικών δεδομένων, η μη εξουσιοδοτημένη συλλογή τους, η περιττή συλλογή δεδομένων και η μη εξουσιοδοτημένη αποκάλυψη. Όλα αυτά τα ζητήματα αναπτύσσονται στις επόμενες παραγράφους.

Σε θέματα ιδιωτικότητας, οι μη εξουσιοδοτημένες χρήσεις των βιομετρικών δεδομένων αντιπροσωπεύουν τη μεγαλύτερη απειλή. Η ύπαρξη για παράδειγμα, μιας βάσης με δεδομένα σκαναρίσματος δαχτύλων ή προσώπου, αποτελεί πολύ μεγάλο πειρασμό για τις υπηρεσίες καταστολής του εγκλήματος ή τους ιδιωτικούς οργανισμούς, να ψάξουν εκεί μέσα για προσωπικά δεδομένα. Το πρόβλημα δηλαδή δημιουργείται, λόγω πιθανής χρήσης των βιομετρικών δεδομένων, για σκοπούς πέρα απ' τους καθορισμένους και ιδίως για εφαρμογές της σήμανσης και για εφαρμογές μοναδικού προσδιοριστή. Αναλυτικά, οι αντιδράσεις για τις δύο αυτές εφαρμογές αναπτύσσονται παρακάτω.

Όσον αφορά στη σήμανση, η διεξαγωγή εγκληματολογικών ερευνών με τη βοήθεια βάσεων δεδομένων που δεν είναι της σήμανσης (π.χ. η βάση δεδομένων με τις άδειες οδήγησης) είναι εξαιρετικά προβληματική από άποψης ιδιωτικότητας και διευρύνει επικίνδυνα το κυβερνητικό πεδίο ερευνών. Με δεδομένο φέρ' ειπείν ότι τα δακτυλικά αποτυπώματα αποτελούν το κύριο μέσο αναγνώρισης σε εφαρμογές της αστυνομίας, είναι εύλογο γιατί υπάρχουν αντιδράσεις σε κρατικά προγράμματα, στα οποία οι χρήστες, για να τύχουν κάποιων δημόσιων παροχών, υποβάλλονται σε σκανάρισμα δαχτύλων. Ο κύριος φόβος είναι ότι οι παρεχόμενες πληροφορίες ενδεχομένως τεθούν στην υπηρεσία αστυνομικών υπηρεσιών, είτε μέσα από ψηφιακές εικόνες των αποτυπωμάτων, είτε με λήψη αποτυπωμάτων εκ των υστέρων από την επιφάνεια σκαναρίσματος. Συνεπώς, ο φόβος είναι ότι κάθε βάση βιομετρικών δεδομένων αποτελεί μια εν δυνάμει βάση

δεδομένων με εγκληματίες, ικανή να αυξήσει την ικανότητα των εμπλεκόμενων φορέων στη διερεύνηση του εγκλήματος.

Ο δεύτερος μεγάλος φόβος είναι ότι τα βιομετρικά δεδομένα θα αποτελέσουν ένα είδος μοναδικού προσδιοριστή του ατόμου, με ότι αυτό συνεπάγεται. Ένας μοναδικός προσδιοριστής είναι ένας σταθερός αριθμός ή μια τιμή, που σχετίζεται με ένα μόνο συγκεκριμένο άτομο και χρησιμοποιείται για τον εντοπισμό πληροφοριών σε μια βάση δεδομένων. Ο αριθμός κοινωνικής ασφάλισης είναι ένα τέτοιο παράδειγμα. Η χρήση μοναδικών προσδιοριστών ενέχει κινδύνους, ειδικά σήμερα που σχεδόν κάθε ανθρώπινη δραστηριότητα – οι αγορές, οι ιατρικές πληροφορίες, οι οικονομικές συναλλαγές – καταγράφεται σε κάποιου είδους βάση δεδομένων. Ο κίνδυνος είναι ότι οι μοναδικοί προσδιοριστές μπορούν να χρησιμοποιηθούν για την παρακολούθηση, τη διαρροή και τον εντοπισμό των καθημερινών ανθρώπινων δραστηριοτήτων σε διάφορες βάσεις δεδομένων, που μπορεί να είναι ανόμοιες και ετερόκλητες μεταξύ τους.

Παρότι λίγες βιομετρικές τεχνολογίες μπορούν να συγκεντρώσουν τις απαραίτητες βιομετρικές πληροφορίες χωρίς τη γνώση του υποκειμένου, το ενδεχόμενο αυτό δεν παύει να προκαλεί ανησυχία. Οι τεχνολογίες σκαναρίσματος προσώπου, φωνής, υπογραφής και keystroke μπορούν να εξυπηρετήσουν αυτό το σκοπό, γιατί στηρίζονται σε συνηθισμένες συσκευές, όπως κάμερες και τηλέφωνα, για την απόκτηση των βιομετρικών πληροφοριών. Μέχρι στιγμής, μόνο το σκανάρισμα προσώπου έχει χρησιμοποιηθεί για συγκέντρωση βιομετρικών πληροφοριών, άνευ εξουσιοδότησης του χρήστη. Σε ορισμένες περιπτώσεις, π.χ. σε εφαρμογές επιτήρησης, η εξουσιοδότηση ενδεχομένως υπονοείται, ενώ άλλες φορές η ένδειξη με πινακίδες ότι στη συγκεκριμένη περιοχή λειτουργεί βιομετρικό σύστημα είναι επαρκής εξουσιοδότηση για τη μετέπειτα συλλογή πληροφοριών.

Ένα ακόμα θέμα είναι η περιττή συλλογή δεδομένων. Η βιομετρική είναι μια λύση που απευθύνεται σε συγκεκριμένα προβλήματα πιστοποίησης ταυτότητας, που έχουν να κάνουν είτε με τον έλεγχο της φυσικής πρόσβασης σε συγκεκριμένες τοποθεσίες, είτε με τον έλεγχο της λογικής πρόσβασης σε συγκεκριμένα δεδομένα, ή τέλος με τη διασφάλιση ότι κανείς δεν μπορεί να γραφεί παραπάνω από μία φορές σε ένα σύστημα. Όταν η βιομετρική εφαρμόζεται σε περιβάλλοντα, όπου τα οφέλη από τη χρήση της είναι μόνο ονομαστικά ή δεν είναι καλά ορισμένα, τότε υπονομεύεται η έννοια της μη παραβίασης

πληροφοριών. Η μη απαραίτητη συλλογή δεδομένων αντιβαίνει σε μια βασική αρχή της ιδιωτικότητας, ότι δηλαδή οι προσωπικές πληροφορίες συγκεντρώνονται μόνο για συγκεκριμένους λόγους και κάτω από συγκεκριμένες συνθήκες. Εξάλλου, η συλλογή μη αναγκαίων δεδομένων, λειτουργεί προς όφελος και της μη εξουσιοδοτημένης χρήσης τους.

Τέλος, η μη εξουσιοδοτημένη αποκάλυψη, συνήθως αναφέρεται στην ενέργεια ενός οργανισμού να μοιραστεί με άλλους φορείς βιομετρικές πληροφορίες, χωρίς τη ρητή συγκατάθεση του χρήστη. Η πράξη αυτή αντιβαίνει σε μια άλλη βασική αρχή της ιδιωτικότητας, ότι δηλαδή ο χρήστης έχει το δικαίωμα να ασκεί έλεγχο στα προσωπικά του δεδομένα. Στις αρνητικές συνέπειες της μη εξουσιοδοτημένης αποκάλυψης, συγκαταλέγεται ότι ο χρήστης δε γνωρίζει τους σκοπούς, για τους οποίους θα χρησιμοποιηθούν τα βιομετρικά του δεδομένα, τις πληροφορίες με τις οποίες θα συσχετιστούν και τα μέτρα που θα ληφθούν για τη φύλαξή τους.

Όλες οι προαναφερθέντες παραβιάσεις μπορούν να θεωρηθούν ως διαφορετικές εκφάνσεις του λεγόμενου function creep. Function creep καλείται η εκτεταμένη χρήση μιας τεχνολογίας, ενός συστήματος ή μιας υλοποίησης, για σκοπούς πέρα από τους αρχικά προβλεπόμενους. Ένα χαρακτηριστικό παράδειγμα είναι η συγκέντρωση από πολλά ιδρύματα των αριθμών κοινωνικής ασφάλισης, και η χρήση τους για λόγους πιστοποίησης, πέρα από τους αρχικούς. Συνέπεια αυτής της εκτεταμένης χρήσης, είναι ότι δίνεται η δυνατότητα σε υπηρεσίες συλλογής πληροφοριών να χρησιμοποιούν αυτόν τον προσδιοριστή, για να εντοπίζουν και να συνδέουν πληροφορίες, κατά μήκος των βάσεων δεδομένων. Παρότι αυτή η ζεύξη των δεδομένων είναι σε αρκετές περιπτώσεις χρήσιμη και επωφελής, ελλοχεύει κινδύνους, που είναι κάθε άλλο παρά αμελητέοι. Στην πιο ακραία περίπτωση, μπορεί να καταστήσει εφικτή την παρακολούθηση της ανθρώπινης κίνησης και συμπεριφοράς, με απώτερο στόχο την καταπίεση των ατόμων. Αυτό το σενάριο και άλλα παρόμοια δεν είναι απίθανα, αλλά ευτυχώς υπάρχουν μέτρα προστασίας ενάντια σ' αυτούς τους κινδύνους, τα οποία θα εξετάσουμε στη συνέχεια.

**Προσωπικοί φόβοι**

Πέρα από τα θέματα της παραβίασης πληροφοριών, η βιομετρική δέχεται κριτική και για θέματα που άπτονται προσωπικών φόβων των ατόμων. Υπάρχει ένα ποσοστό του

πληθυσμού, το οποίο αντιλαμβάνεται τη βιομετρική, ως μια διαδικασία προσβλητική και ενοχλητική, η οποία παραβιάζει την ιδιωτικότητά του. Αν κι αυτή η αποστροφή μπορεί να οφείλεται στον υποβόσκοντα φόβο για ζητήματα παραβίασης πληροφοριών, συνήθως σχετίζεται με θρησκευτικές, προσωπικές ή κοινωνικές πεποιθήσεις. Μερικά άτομα για παράδειγμα, μπορεί να θεωρήσουν την εγκατάσταση ενός βιομετρικού συστήματος στο χώρο εργασίας, ως ένδειξη έλλειψης εμπιστοσύνης και να αισθανθούν θιγμένα στην προοπτική χρήσης του συστήματος[1].

Είναι συχνό φαινόμενο βέβαια οι νέες, πρωτοποριακές τεχνολογίες να συναντούν έντονες αντιδράσεις πριν την καθιέρωση. Τα ATMs για παράδειγμα, αντιμετωπίζονταν με καχυποψία για χρόνια. Στην Αμερική και τον Καναδά οι smart cards θεωρείται ότι παραβιάζουν την ιδιωτικότητα του πολίτη, την ίδια στιγμή που δισεκατομμύρια έχουν τεθεί σε κυκλοφορία στην Ευρώπη, την Ασία, την Αφρική και τη Νότια Αμερική. Δεν πρέπει να προκαλεί συνεπώς εντύπωση ότι, αν κι εκατομμύρια χρήστες έχουν εγγραφεί σε βιομετρικά συστήματα διαφορετικής πολυπλοκότητας και σκοπού σε όλο τον κόσμο, η βιομετρική τεχνολογία εξακολουθεί να θεωρείται από πολλούς φουτουριστική ή απειλητική.

Γενικά, είναι πιο δύσκολο να καμφθούν οι αντιρρήσεις για ζητήματα παραβίασης πληροφοριών, παρά οι ιδιαίτεροι προσωπικοί φόβοι. Ο λόγος είναι ότι οι κίνδυνοι παραβίασης πληροφοριών μπορούν να περιοριστούν, με τη λήψη συγκεκριμένων γενικών μέτρων προστασίας των βιομετρικών πληροφοριών, ενώ απ' την άλλη οι αντιδράσεις που οφείλονται σε προσωπικούς φόβους είναι αυτό ακριβώς που δηλώνει η λέξη, δηλαδή προσωπικές. Έτσι, ο τρόπος χειρισμού αυτών των αντιδράσεων εξαρτάται απ' το αν η τεχνολογία απευθύνεται σε πελάτες, υπαλλήλους ή πελάτες, απ' το αν είναι προαιρετική ή υποχρεωτική κτλ. Για παράδειγμα, τα υποχρεωτικά συστήματα συνοδεύονται συνήθως από τις περισσότερες φωνές διαμαρτυρίας και αντιμετωπίζονται με μεγαλύτερη αποδοκιμασία. Γενικά πάντως, η καλύτερη αντιμετώπιση σ' αυτές τις περιπτώσεις είναι να γίνει σαφές, για ποιους λόγους χρησιμοποιούνται συστήματα βιομετρικής, σε ποιες παρόμοιες καταστάσεις έχουν χρησιμοποιηθεί στο παρελθόν και ποιος είναι ο τρόπος λειτουργίας τους.

[1] http://rioter.info/2009/10/06B1-giorgio-agamben/

Με την πάροδο του χρόνου, ο εγκλιματισμός των ανθρώπων στη βιομετρική τεχνολογία αναμένεται να περιορίσει τις ενστάσεις που πηγάζουν από προσωπικούς φόβους. Είναι γεγονός ότι άτομα που έχουν εμπειρία απ' τη χρήση βιομετρικών συστημάτων, τα υποστηρίζουν πολύ πιο ένθερμα. Η έλλειψη εξοικείωσης με την τεχνολογία προκαλεί τάση απαξίωσής της, αλλά – ευτυχώς για τη βιομηχανία της βιομετρικής – οι μετρήσεις δείχνουν ότι, αφού κάποιος έλθει σε επαφή μαζί της, συνήθως δεν έχει πρόβλημα να τη χρησιμοποιεί σε μόνιμη βάση.

### 5.1.3 Αρετές της βιομετρικής τεχνολογίας σε θέματα προστασίας της ιδιωτικότητας

Αν και αρκετοί προβληματισμοί για θέματα ιδιωτικότητας είναι γερά θεμελιωμένοι, κάποιοι άλλοι βασίζονται σε παρανοήσεις του τρόπου λειτουργίας της τεχνολογίας. Γενικά, υπάρχουν κάποιες αρχές στον τρόπο λειτουργίας, τόσο της βιομετρικής τεχνολογίας όσο και της βιομηχανίας της βιομετρικής, που περιορίζουν το ενδεχόμενο χρήσης της με τρόπο που να παραβιάζει την ιδιωτικότητα. Αυτά τα στοιχεία που είναι φιλικά για την ιδιωτικότητα και είναι σύμφυτα με τη βιομετρική, εξηγούνται παρακάτω.

Τα περισσότερα βιομετρικά συστήματα, με σημαντικότερη εξαίρεση τα συστήματα της σήμανσης, δεν αποθηκεύουν ακατέργαστα βιομετρικά δεδομένα, όπως εικόνες προσώπου ή δακτυλικών αποτυπωμάτων. Αντ' αυτού χρησιμοποιούν τα βιομετρικά templates, γεγονός που προφυλάσσει από πολλούς κινδύνους ιδιωτικότητας. Η αποθήκευση ακατέργαστων εικόνων διευκολύνει σε μεγάλο βαθμό τον εντοπισμό δεδομένων κατά μήκος των βάσεων, για το λόγο ότι η εύρεση μπορεί να γίνει με μια απλή διαδικασία δυαδικής αναζήτησης. Αντίθετα, τα templates είναι διαφορετικά σε κάθε λήψη δεδομένων και δεν μπορούν να χρησιμοποιηθούν για την ανακατασκευή των αρχικών εικόνων. Το σημαντικότερο είναι ότι απαιτείται ειδικός αλγόριθμος, ο οποίος είναι διαφορετικός και κρυφός σε κάθε σύστημα, για να καθοριστεί αν οι πληροφορίες μιας βάσης δεδομένων μπορούν να αντιστοιχηθούν με πληροφορίες μιας άλλης. Αυτό σημαίνει ότι ο εντοπισμός είναι πολύ πιο δύσκολος.

Ακόμα, το εύρος των βιομετρικών τεχνολογιών, οι οποίες χρησιμοποιούνται σε διαφορετικές εφαρμογές, περιορίζει την πιθανότητα καθιέρωσης ενός καθολικού βιομετρικού προσδιοριστή. Είναι λειτουργικά αδύνατον όμως να υπάρξει σύνδεση, με

κοινό παρονομαστή τη βιομετρική, στα δεδομένα ενός ατόμου, που χρησιμοποιεί διαφορετικές βιομετρικές τεχνολογίες για διαφορετικές εφαρμογές. Κάποιος για παράδειγμα, που υποβάλλεται σε σκανάρισμα δαχτύλου για πρόσβαση σε δίκτυο, σκανάρισμα χεριού για είσοδο σε ασφαλισμένες περιοχές και σκανάρισμα φωνής για τηλεφωνική πρόσβαση λογαριασμών, δε διατρέχει κίνδυνο συσχέτισης των δεδομένων του από κάποια βιομετρική μέτρηση.

Ένας επίσης παράγοντας, που ελαττώνει την πιθανότητα χρήσης των βιομετρικών δεδομένων με τρόπο που να παραβιάζει την ιδιωτικότητα, είναι η δυνατότητα εγγραφής με διαφορετικά βιομετρικά δείγματα σε κάποιες περιπτώσεις, ειδικά σε βιομετρικά συστήματα που εξετάζουν τη συμπεριφορά, όπως τα συστήματα σκαναρίσματος φωνής και υπογραφής. Για να γίνει πιο κατανοητό, κάποιος μπορεί να χρησιμοποιεί την πλήρη του υπογραφή σε ένα βιομετρικό σύστημα και μια πιο σύντομη σε ένα άλλο. Γενικά, ο αριθμός των δυνατών εγγραφών του ίδιου χρήστη σε ένα βιομετρικό σύστημα συμπεριφοράς είναι απεριόριστος.

Τέλος, στο χώρο της βιομετρικής υπάρχουν πάρα πολλές εταιρείες και κάθε μία διαθέτει ξεχωριστή τεχνολογία, που δεν είναι διαθέσιμη στο κοινό, γεγονός που δυσχεραίνει τον εντοπισμό δεδομένων κατά μήκος των βάσεων. Οι διάφορες εταιρείες δρουν ανταγωνιστικά μεταξύ τους κι έτσι παράγονται πολλοί τύποι templates, που μπορούν να συγκριθούν μόνο με templates της ίδιας τεχνολογίας. Επειδή μάλιστα υπάρχει εξειδίκευση και στα συστήματα ίδιας τεχνολογίας, ανάλογα με το είδος της εφαρμογής – δηλαδή άλλα συστήματα είναι κατάλληλα για φυσική πρόσβαση, άλλα για πρόσβαση σε PC, άλλα για αναγνώριση με smart card – παράγονται πολύ διαφορετικά templates, για τη σύγκριση των οποίων απαιτούνται διαφορετικοί αλγόριθμοι.

# 6. ΔΙΕΥΘΥΝΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΕΡΕΥΝΩΝ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

## 6.1 Η ΕΠΙΣΤΗΜΟΝΙΚΗ ΕΡΕΥΝΑ ΣΤΗΝ ΑΣΤΥΝΟΜΙΑ

Η δίωξη του εγκλήματος και η τιμωρία των ενόχων είναι ζητήματα που απασχόλησαν τις ανθρώπινες κοινωνίες από της δημιουργίας των. Ο τρόπος όμως διώξεως των εγκληματιών ήταν ανάλογος με τις εκάστοτε κρατούσες κοινωνικές αντιλήψεις, την εξέλιξη και την πνευματική και πολιτιστική ανάπτυξη των λαών. Οι Υπηρεσίες διώξεως του εγκλήματος ακολούθησαν την εξελικτική πορεία των ανθρωπίνων κοινωνιών, διαρκώς εξελισσόμενες και οργανούμενες. Γίνεται μία διαρκής πάλη μεταξύ διωκτικών οργάνων και εγκληματιών, οι μεν εφαρμόζοντας νέες μεθόδους διώξεως, οι δε ανακαλύπτοντας νέα ευφυή και σατανικά σχέδια δράσεως και διαφυγής[1].

Σε κοινωνίες πρωτόγονες και απολίτιστες, πρωτόγονα και βάρβαρα ήταν και τα εφαρμοζόμενα μέσα διώξεων κατά των κακοποιών, η δε επιβαλλόμενη σ' αυτούς ποινή συνήθως ήταν δυσανάλογος προς το διαπραχθέν αδίκημα. Αντίθετα, στις πολιτισμένες κοινωνίες – ως η σημερινή – στις οποίες προέχει ο σεβασμός και η κατοχύρωση των ατομικών και κοινωνικών δικαιωμάτων του πολίτη, οι Υπηρεσίες Δίωξης του εγκλήματος, οπλισμένες με σύγχρονα επιστημονικά μέσα, εφαρμόζουν μεθόδους ασφαλείς και ανταποκρινόμενες στην όλη κοινωνική εξέλιξη και κατάσταση. Η επιτυχής εφαρμογή δε του σκοπού αυτού προδίδει και τον βαθμό πολιτισμού του Κράτους.

Κατά την εκτέλεση της αποστολής της η Αστυνομία οφείλει να ενεργεί προληπτικά και κατασταλτικά. Οφείλει δηλαδή να προλαμβάνει τη διάπραξη εγκλημάτων, και όταν τούτο δεν είναι εφικτό – λόγω του ότι δεν είναι πανταχού παρούσα – να ενεργεί για την εξιχνίαση διαπραχθέντων αδικημάτων, να ανακαλύπτει τον ένοχο και να τον αποστέλλει αρμοδίως.

[1] Διευθυνση Εγκληματολογικών Ερευνών: Α/Α ΜΗΝΟΠΕΤΡΑΣ Χαράλαμπος

Νέες επιστήμες, όπως η Ψυχολογία, Βιολογία, Εγκληματολογία κλπ βοήθησαν πολύ στη γνώση του εγκληματία, καθόρισαν τις ροπές και τις τάσεις του και προσδιόρισαν τον τρόπο ενεργείας του.

Η Επιστημονική Έρευνα στην Αστυνομία διενεργείται από τη Διεύθυνση Εγκληματολογικών Ερευνών (Δ.Ε.Ε.) η οποία, σύμφωνα με το άρθρο 7 του Π.Δ. 198/92, είναι αυτοτελής Κεντρική Υπηρεσία του Υ.Δ.Τ. και εφαρμόζοντας επιστημονικοτεχνικές και άλλες πρόσφορες μεθόδους, διεθνώς παραδεκτές, υποβοηθεί το έργο των Κρατικών Υπηρεσιών στην πρόληψη, δίωξη και καταστολή του εγκλήματος.

Ειδικότερα, για το σκοπό αυτό :

1. Εξακριβώνει την ταυτότητα κάθε ατόμου, με βάση τη δακτυλοσκοπική ή άλλη επιστημονική και τεχνική μέθοδο.

2. Διαθέτει, μετά από αίτημα των αρμοδίων Αρχών, ειδικευμένο προσωπικό για την πλήρη διερεύνηση και απεικόνιση (φωτογράφηση, κινηματογράφηση κλπ) του τόπου τελέσεως εγκλημάτων ή άλλων συμβάντων αστυνομικού ενδιαφέροντος, προς ανεύρεση και περισυλλογή ιχνών και πειστηρίων.

3. Εξετάζει ίχνη και πειστήρια και με την αξιοποίηση αυτών συμβάλλει στη διαλεύκανση των ερευνούμενων υποθέσεων.

4. Παρακολουθεί την κίνηση της εγκληματικότητας στη Χώρα με τη συγκέντρωση και την κατάλληλη ταξινόμηση των περιεχομένων σ' αυτή στοιχείων από όλες τις ασχολούμενες με τη δίωξη του εγκλήματος Αρχές, σε σχέση με τα εγκληματούντα άτομα και τα τελούμενα από αυτά εγκλήματα.

5. Εκδίδει Δελτία Εγκληματολογικών Αναζητήσεων (Δ.Ε.Α.) και αποστέλλει αυτά στις αρμόδιες Αρχές για την αναζήτηση και σύλληψη καταδιωκομένων προσώπων, ανεύρεση εξαφανισθέντων ατόμων και απωλεσθέντων ή κλαπέντων αντικειμένων.

6. Παρέχει προς τις αρμόδιες Αρχές, αυτεπάγγελτα ή μετά από αίτημα αυτών, στοιχεία που μπορούν να συμβάλουν στην πρόληψη, τη δίωξη και την καταστολή της εγκληματικότητας, καθώς και κάθε πληροφορία της αρμοδιότητάς της.

7. Τηρεί αρχεία δακτυλικών αποτυπωμάτων, ατομικών φακέλων εγκληματούντων ατόμων (ημεδαπών και αλλοδαπών), φωτογραφιών, μεθόδων δράσεως, σωματικών χαρακτηριστικών (MODUS OPERANDI) και άλλα συναφή μετά αντιστοίχων ευρετηρίων καθώς και ειδικές συλλογές κάθε είδους αποτυπωμάτων, εντυπωμάτων, ιχνών, ουσιών και λοιπών αντικειμένων.

8. Μεριμνά για την εκπαίδευση-μετεκπαίδευση του προσωπικού της και για την επαγγελματική επιμόρφωση στην εγκληματολογική επιστήμη και τέχνη των υπηρετούντων στην Ελληνική Αστυνομία ή σε άλλες Κρατικές Υπηρεσίες, που είναι επιφορτισμένες με οποιονδήποτε τρόπο με τη δίωξη του εγκλήματος.

9. Εφαρμόζει κάθε νέο επίτευγμα της Επιστήμης ή Τεχνολογίας, διεθνώς παραδεκτό και αναγνωρισμένο.

10. Φροντίζει για τον έγκαιρο εφοδιασμό των Υπηρεσιών της με τον απαραίτητο σύγχρονο επιστημονικοτεχνικό εξοπλισμό και λοιπά υλικά και μέσα για την εύρυθμη λειτουργία τους.

11. Εφαρμόζει σύγχρονες μεθόδους μηχανοργανώσεως των εργασιών της και ηλεκτρονικής επεξεργασίας των εγκληματολογικών στοιχείων σημάνσεως και λοιπών αντικειμένων αυτής.

12. Μεριμνά για την προώθηση της έρευνας, τη βελτίωση των εργασιών και την αποδοτικότητά της, δυνάμενη να αναπτύσσει ερευνητικά προγράμματα σε θέματα εγκληματολογικού ενδιαφέροντος, αυτοτελώς ή σε συνεργασία με άλλες ημεδαπές ή αλλοδαπές Αρχές, Υπηρεσίες και λοιπούς Φορείς.

13. Εισηγείται αρμοδίως τη λήψη νομοθετικών ή άλλων μέτρων, αποσκοπούντων στην πρόληψη, προσφορότερη δίωξη και καταστολή της εγκληματικότητας καθώς και σε άλλα θέματα αρμοδιότητάς της.

14. Αποστέλλει, ύστερα από έγκριση, σε προηγμένα εργαστήρια της Αλλοδαπής, πειστήρια εγκλημάτων, όταν απαιτούνται ειδικές εξετάσεις που δεν μπορούν να πραγματοποιηθούν σ' αυτήν.

15. Εκπροσωπείται με εξειδικευμένο προσωπικό της σε συνέδρια, συνδιασκέψεις, ομάδες εργασίας, για θέματα εγκληματολογικού ενδιαφέροντος, στην Ημεδαπή ή Αλλοδαπή.

16. Τηρεί την απαραίτητη επαφή και συνεργασία με συναφείς Υπηρεσίες και Οργανισμούς της Αλλοδαπής, είτε απευθείας είτε δια της Διευθύνσεως Διεθνούς Αστυνομικής Συνεργασίας (Δ.Δ.Α.Σ.).

Η τοπική αρμοδιότητα της Δ.Ε.Ε. εκτείνεται σ' ολόκληρη την Επικράτεια.

***Συγκρότηση – Διάρθρωση***

Η Δ.Ε.Ε. συγκροτείται από την Κεντρική και τις Περιφερειακές αυτής Υπηρεσίες.

Η Κεντρική Υπηρεσία της Δ.Ε.Ε. εδρεύει στην Αθήνα και διαρθρώνεται εσωτερικά στα ακόλουθα Τμήματα (Σχετ.: Υπ' αριθμ.7001/2/599-γ 30-09-92 απόφαση Υ.Δ.Τ.)[1] :

α. Εσωτερικών Λειτουργιών

β. Δακτυλοσκοπίας

γ. Εξερευνήσεων

δ. Χημείου

ε. Εργαστηρίων

στ. Καταδιωκτικών-Στατιστικής

ζ. Μεθοδικοτήτων-Φωτογραφικού

η. Αρχείων

Οι Περιφερειακές Υπηρεσίες της Δ.Ε.Ε. είναι :

[1] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=48&Itemid=39&lang=

- Η Υποδιεύθυνση Εγκληματολογικών Ερευνών Βορείου Ελλάδος (Υ.Ε.Ε.Β.Ε.), που εδρεύει στη Θεσσαλονίκη και διαρθρώνεται σε Τμήματα ανάλογα και αντίστοιχα με αυτά της Κεντρικής Υπηρεσίας.

- Τα Γραφεία Εγκλ/κών Ερευνών (Γ.Ε.Ε.) που έχουν έδρα στις πόλεις που υπάρχει έδρα Πρωτοδικείου και εδαφική αρμοδιότητα αυτήν του Πρωτοδικείου υπαγωγής τους.

## 6.2 Η ΕΠΙΣΤΗΜΟΝΙΚΗ ΕΡΕΥΝΑ ΣΤΗΝ ΕΞΑΚΡΙΒΩΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ

Η ασφαλής και ταχεία εξακρίβωση της ταυτότητας ενός ατόμου, αποτελεί δραστικό μέσο της Αστυνομίας για την πρόληψη και καταστολή της εγκληματικότητας.

Με την έννοια **«εξακρίβωση της ταυτότητας»** εννοούμε τη φυσική ταυτότητα (που εξαρτάται από βιολογικούς παράγοντες) και τη νομική (που εξαρτάται από νομικές ιδιότητες ή καταστάσεις, όπως Θρησκεία, ιθαγένεια κτλ)[1].

Η εξακρίβωση της ταυτότητας ενός ατόμου υπήρξε ανέκαθεν δυσχερές ζήτημα για την Αστυνομία, καθ' όσον οι διάφοροι εγκληματίες καταβάλλουν πολλές προσπάθειες γα να αποφύγουν την εξακρίβωση της ταυτότητάς των, είτε με τη μεταβολή της νομικής τους ταυτότητας (π.χ. ψεύτικο όνομα, πλαστογραφημένα πιστοποιητικά κ.α.) είτε με τη μεταβολή της φυσικής τους ταυτότητας (π.χ. μεταμφίεση προσώπου, πλαστική εγχείρηση κ.α.).

Παλαιότερα στη χώρα μας το πρόβλημα της εξακρίβωσης της ταυτότητας δεν ήταν έντονο, καθότι και οι μεγαλύτερες πόλεις είχαν μικρό αριθμό κατοίκων και τα μέσα συγκοινωνίας ελάχιστα. Αυτοί οι άνθρωποι λοιπόν αλληλογνωρίζονταν και είχαν αυστηρό κοινωνικό έλεγχο, η Αστυνομία δε μπορούσε με σχετική ευκολία να διαπιστώσει την απουσία, τη μετακίνηση, την ασχολία και εν γένει το χαρακτήρα αυτών. Σήμερα όμως υπάρχουν πόλεις εκατομμυρίων κατοίκων και τη χώρα μας επισκέπτονται εκατομμύρια ανθρώπων διαφόρου εθνικότητας και χαρακτήρα. Σήμερα επίσης, η μετακίνηση των εγκληματιών εντός ή εκτός της χώρας, με την εξέλιξη και πρόοδο των

[1] Διευθυνση Εγκληματολογικών Ερευνών: Α/Α ΖΩΓΡΑΦΟΣ Νικόλαος

συγκοινωνιακών μέσων, είναι εύκολη και σύντομη. Με την εφαρμοζόμενη όμως αλάθητη μέθοδο της δακτυλοσκοπίας, εξουδετερώνονται οι σκόπιμες αυτές μεταβολές, καθώς επίσης διευκρινίζονται συνωνυμίες που υπάρχουν, διότι συχνές είναι οι ταλαιπωρίες νομοταγών πολιτών από τυχαίες ή σκόπιμες συνωνυμίες με καταδιωκόμενα άτομα.

Ο εγκληματίας τα πάντα μπορεί να αμφισβητήσει, τα δακτυλικά του όμως αποτυπώματα ποτέ. Αυτά είναι αψευδείς μάρτυρες και αμερόληπτοι. Δεν ομιλούν, και όμως, για τον γνωρίζοντα αποκαλύπτουν περισσότερα κι από τον ομιλητικότερο μάρτυρα, Είναι πάντα αμετάβλητοι στη διάθεσή μας, έτοιμοι να επαναλάβουν επακριβώς όσα εξαρχής φανέρωσαν.

**Τέλος, σήμερα πολλοί κακοποιοί ανήκουν στις υψηλές βαθμίδες της κοινωνίας μας, έχουν καλούς τρόπους, μιλούν ξένες γλώσσες, είναι επιστήμονες γενικά, γι' αυτό δε το λόγο είναι και περισσότερο επικίνδυνοι και ραδιούργοι των κοινών κακοποιών.**

## 6.3 ΜΕΘΟΔΟΙ – ΣΥΣΤΗΜΑΤΑ ΕΞΑΚΡΙΒΩΣΗΣ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ

Για την εξακρίβωση της ταυτότητας των εγκληματιών χρησιμοποιήθηκαν μέχρι σήμερα διάφοροι μέθοδοι-συστήματα, ανάλογα με τις κρατούσες αντιλήψεις γύρω από τα ανθρώπινα δικαιώματα. Όλα βέβαια απέβλεπαν στη βεβαίωση της ταυτότητας του εγκληματία και την εξακρίβωση του ποινικού παρελθόντος.

Τα κυριότερα από τα συστήματα αυτά είναι :

- Η μέθοδος του στιγματισμού και ακρωτηριασμού.
- Η περιγραφική μέθοδος.
- Η ανθρωπομετρική μέθοδος.
- Η φωτογραφική μέθοδος.
- Η δακτυλοσκοπική μέθοδος.

***Μέθοδος Στιγματισμού και Ακρωτηριασμού***

Η μέθοδος αυτή εφαρμοζόταν από την αρχαιότητα μέχρι τον 18$^{ο}$ αιώνα, για την αναγνώριση των εγκληματιών. Ο στιγματισμός γινόταν ανεξίτηλα με πυρακτωμένο σίδερο (στιγέα) σε εμφανή κυρίως μέρη του σώματός των ή τιμωρούσαν αυτούς με σωματικές ποινές, δηλαδή αποκοπή αυτιών, μύτης, δακτύλων κλπ., με αποτέλεσμα αναλόγως του αποκοπέντος τμήματος να φαίνεται το έγκλημα που είχε διαπράξει. Στο βυζαντινό δίκαιο, η μοιχεία τιμωρούνταν με κοπή της μύτης, στη Γερμανία η κλοπή με κοπή των αυτιών, στη Γαλλία έστιζαν με πυρακτωμένο σίδερο γράμματα στο σώμα του εγκληματία, π.χ. το γράμμα V (VOLEUR=κλέπτης) κλπ.

Η μέθοδος αυτή καταργήθηκε μετά το Μεσαίωνα, και αποτελεί μελανό σημείο στην προσπάθεια του ανθρώπου να βρει και να εφαρμόσει μεθόδους εξακρίβωσης της ταυτότητας. Σήμερα βέβαια έχουμε περιπτώσεις αυτοστιγματισμού ατόμων (τατουάζ) που σχηματίζουν σε διάφορα μέρη του σώματός των παραστάσεις που γίνονται με βελόνα και υγροποιημένα χρώματα. Αυτοί οι στιγματισμοί βοηθούν πολλές φορές στην Αστυνομία στην εξακρίβωση ταυτότητος ζώντων αλλά και αγνώστων πτωμάτων.

***Περιγραφική Μέθοδος (PORTRAIT PARLE)***

Αυτή είναι η δια λέξεων «φωτογραφία» της εξωτερικής εμφάνισης ενός ατόμου από ένα άλλο άτομο. Η μέθοδος αυτή είναι αρχαιότητα, χρησιμοποιηθείσα από τους Έλληνες της Αλεξάνδρειας το 145π.Χ. Κατά τη μέθοδο αυτή περιγράφεται το ανθρώπινο σώμα και τα ιδιαίτερα χαρακτηριστικά του : ανάστημα, πρόσωπο, χρώμα οφθαλμών, μύτη, στόμα, αυτιά, διάταξη δοντιών, φωνή, βάδισμα, ουλές, φακίδες, στίξεις κτλ.

Την περιγραφική μέθοδο διαμόρφωσε ο Γάλλος BERTILLON στο τέλος του 19$^{ου}$ αιώνα, που την ονόμασε και Portrait Parle, ήτοι «εικόνα με λέξεις». Η μέθοδος αυτή παρουσίαζε μειονεκτήματα, διότι η περιγραφή των χαρακτηριστικών ενός ατόμου διέφερε, και ήταν ανάλογη με την αντίληψη και εκτίμηση του εκάστοτε Αστυνομικού ή άλλου ατόμου που περιέγραφε τον εγκληματία. Επίσης, η μεταβολή των χαρακτηριστικών του ανθρωπίνου σώματος, οι σκόπιμες παραλλαγές και αλλοιώσεις των χαρακτηριστικών, οδηγούσαν πολλές φορές στην κατάρτιση – για το ίδιο άτομο – δύο ανόμοιων περιγραφικών δελτίων.

Πάντως η περιγραφική μέθοδος εφαρμόζεται σήμερα για την ανακάλυψη αγνώστων εγκλημάτων με περιγραφή των υπόπτων ή δραστών από αυτόπτες μάρτυρες. Για την περιγραφή των παραπάνω αναφερομένων χαρακτηριστικών, χρησιμοποιείται σήμερα το Δελτίο Διαπραχθέντος Εγκλήματος.

Σε σοβαρές περιπτώσεις εγκλημάτων, για την εξακρίβωση της ταυτότητας αγνώστων στοιχείων ατόμων, χρησιμοποιείται από την Αστυνομία η «σύνθεση» της εικόνας του αναζητουμένου.

Για να γίνει η σύνθεση της εικόνας όμως πρέπει να προηγηθεί η περιγραφή του καταζητούμενου από τους αυτόπτες μάρτυρες. Η σύνθεση αυτή γίνεται με την προσαρμογή εικόνων ή σχεδίων μικρών τμημάτων του προσώπου που υπάρχουν σε ειδικό κουτί "INDENTITY-KIT".

Στη συνέχεια με τη διασταύρωση των γνωμών, μεταβάλλεται η εικόνα, μέχρι που να επιτευχθεί η κατά το δυνατόν ακριβέστερη σύνθεση της εικόνας του καταζητούμενου αγνώστου ατόμου.

***Ανθρωπομετρική Μέθοδος***

Η ανθρωπομετρική μέθοδος ήταν γνωστή από αρκετό χρόνο. Εφαρμόστηκε στη Ρωσία – μετά την κατάργηση του στιγματισμού – το 1863.

Στην Ευρώπη εφαρμόστηκε κατ' αρχάς στο Βέλγιο το 1860, αλλά ο κύριος δημιουργός αυτής υπήρξε ο Γάλλος εγκληματολόγος BERTILLON με έναρξη εφαρμογής το 1885, με την κατάρτιση ειδικού αρχείου στην Ασφάλεια του Παρισιού.

Το σύστημα αυτό γενικά συνίσταται στην καταμέτρηση του ύψους του ατόμου, όρθιου και καθήμενου, του μήκους και πλάτους της κεφαλής, μήκους πήχεως αριστερού χεριού κλπ..

Για τις μετρήσεις αυτές ο BERTILLON χρησιμοποίησε όργανα ακριβείας όπως το κρανιόμετρο, το δίμετρο κλπ. Το σύστημα αυτό όμως παρουσίασε αρκετά μειονεκτήματα :

α. Δεν έχει εφαρμογή στους ανηλίκους, για το λόγο ότι τα οστά τους μεταβάλλουν μήκη με την πάροδο του χρόνου.

β. Η λόγω γήρατος ή παθήσεων ή εγχειρήσεων κλπ διαφοροποίηση του μήκους των οστών διαφόρων ατόμων.

γ. Η δυσχέρεια στην αρχειοθέτηση και αναζήτηση των ανθρωπομετρικών στοιχείων στο Αρχείο.

Στην Ελλάδα το ανθρωπομετρικό σύστημα εφαρμόστηκε κατά το 1912 από τον Καθηγητή της Ιατροδικαστικής Ιω. Γεωργιάδη, σε συνδυασμό με το σύστημα BERTILLON. Σήμερα αναγράφεται μόνο το ανάστημα στο δακτυλοσκοπικό δελτίο, προς διευκόλυνση των Αστυνομικών Αρχών σε περίπτωση αναζητήσεώς του.

***Φωτογραφική Μέθοδος***

Αυτή εφαρμόστηκε κατ' αρχάς στο Βέλγιο το 1843 και στη Γαλλία το 1874 από τον BERTILLON.

Κατά τη μέθοδο αυτή λαμβάνονται φωτογραφίες του κατηγορουμένου σε τρεις στάσεις : κατά τομή (προφίλ), κατά μέτωπο και κατά τα ¾ του προσώπου από την αριστερή παρειά. Όμως παρά τη διευκόλυνση της Αστυνομίας από τη μέθοδο αυτή, δεν μπορεί να θεωρηθεί αλάθητος μέθοδος, διότι παρουσιάζει μειονεκτήματα, όπως :

- Δεν υπάρχει τρόπος ταξιθέτησης των φωτογραφιών στο Αρχείο, ώστε να είναι εύκολη και γρήγορη η αναζήτηση και ανεύρεση της φωτογραφίας σε ελάχιστο χρόνο.
- Υπάρχει κίνδυνος πλάνης του συγκρίνοντος δύο φωτογραφίες του ιδίου ατόμου, που έχουν ληφθεί κάτω από διαφορετικό φωτισμό ή άλλες συνθήκες ή και αντίστροφα, δύο φωτογραφίες διαφορετικών ατόμων να θεωρηθούν του ιδίου ατόμου.

- Με την πάροδο του χρόνου αλλάζουν τα χαρακτηριστικά του ατόμου και υπάρχει αδυναμία σύγκρισης δύο φωτογραφιών του ιδίου ατόμου, όταν οι φωτογραφίες έχουν ληφθεί μεταξύ τους σε μακρά χρονικά διαστήματα.

Μετά την εφαρμογή της Δακτυλοσκοπίας, η φωτογραφική μέθοδος εγκαταλείφθηκε κατά βάση, σαν αυτοτελές μέσο εξακρίβωσης της ταυτότητας. Παραμένει όμως χρήσιμη για την ανακάλυψη αγνώστων ενόχων εγκλημάτων, αναγνωριζομένων από το θύμα και τους μάρτυρες, με την επίδειξη σ' αυτούς φωτογραφιών, για την ανεύρεση δραπετών, για την εξακρίβωση της ταυτότητας εξαφανιζομένου, με τη δημοσίευση της φωτογραφίας του στο Δ.Ε.Α. ή στον ημερήσιο τύπο ή στην τηλεόραση και σε πολλές άλλες περιπτώσεις.

Στη Δ.Ε.Ε. και στο γραφείο Μεθοδικοτήτων (MODUS OPERANDI), υπάρχει πλήρες αρχείο φωτογραφιών των καθ' έξη και κατ' επάγγελμα εγκληματιών οι οποίοι εγκληματούν κατά ορισμένη μέθοδο, οι φωτογραφίες αυτές είναι ταξινομημένες κατά κατηγορία εγκλήματος, κατ' ανάστημα και ηλικία και αναλόγως των ελαττωματικοτήτων και των ιδιαιτέρων χαρακτηριστικών των εγκληματιών (π.χ. ουλές, κατεστραμμένοι αριστεροί ή δεξιοί οφθαλμοί κλπ). Η ανανέωση των φωτογραφιών πρέπει να γίνεται σε ορισμένα χρονικά διαστήματα.

***Δακτυλοσκοπική Μέθοδος***

Η μόνη μέχρι σήμερα μέθοδος που, όπως αποδείχθηκε από τη μακροχρόνια εφαρμογή της, είναι τέλεια και αλάνθαστη, είναι η δακτυλοσκοπική μέθοδος εξακρίβωσης της ταυτότητας.

Η μέθοδος αυτή συνίσταται στην εξακρίβωση της ταυτότητας κάθε ατόμου ζωντανού ή νεκρού, με βάση τα δακτυλικά αποτυπώματά του, ή δακτυλικό αποτύπωμα ή μέρος του δακτυλικού αποτυπώματος και μόνο.

Η αξία της δακτυλοσκοπικής μεθόδου σαν ακαταμάχητο όπλο στην πάλη κατά του εγκλήματος βασίζεται σε ορισμένες θεμελιώδεις ιδιότητες οι οποίες είναι εμπειρικά και επιστημονικά βεβαιωμένες. Οι ιδιότητες αυτές είναι :

**α. <u>Το Αμετάβλητο</u>**

Από το 4$^{ο}$ μήνα της κυήσεως, καθ' όλο το βίο του ανθρώπου, και μετά θάνατο ακόμη, μέχρι της τελείας αποσυνθέσεως του δέρματος των δακτύλων, οι θηλοειδείς γραμμές παραμένουν αμετάβλητες. Η φυσιολογική ανάπτυξη του ανθρωπίνου σώματος συνεπιφέρει βέβαια και αυτή των θηλοειδών γραμμών, οι οποίες όμως δεν μεταβάλλονται κατά σχήμα ή ιδιαίτερα χαρακτηριστικά σημεία. Η διατήρηση αμεταβλήτων των θηλοειδών γραμμών εξαρτάται και από τις συνθήκες που ευρίσκεται το πτώμα : π.χ. ανευρεθέν πτώμα μετά την τήξη του χιονιού σε όρος, παρουσίαζε εκμεταλλεύσιμα αποτυπώματα μετά εξάμηνο από το θάνατο.

**β. <u>Το Αναλλοίωτο</u>**

Οι θηλοειδείς γραμμές των δακτύλων, στην περίπτωση που καταστραφεί η κερατίνη στιβάδα (επιδερμίδα) παραμένουν αναλλοίωτες και αμετάβλητες, λόγω του ότι η κατωτέρω στιβάδα της επιδερμίδας, η καλούμενη «βλαστική» είναι κοιτίδα αναπαραγωγής κυττάρων, κι έτσι σχηματίζονται σύντομα νέες στιβάδες, ακριβώς όμοιες με τις κατεστραμμένες και αναπαράγονται πανομοιότυπα θηλόγραμμα. Όταν όμως η βλάβη είναι σοβαρή και καταστραφεί η βλαστική στιβάδα, τότε εξαλείφονται οι θηλοειδείς γραμμές και σχηματίζεται μόνιμο τραύμα (ουλή) στη ράγα του δακτύλου.

Η εκούσια καταστροφή των θηλοειδών γραμμών με μικροεπεμβάσεις ή τριβή τους σε σκληρές επιφάνειες, επιφέρει μόνο πρόσκαιρη καταστροφή και αλλοίωση αυτών.

Από τις δερματικές παθήσεις, κυρίως η λέπρα προκαλεί καταστροφή των θηλογράμμων. Υπάρχουν βέβαια και κατηγορίες ανθρώπων που, ένεκα του επαγγέλματός τους, π.χ. εργάτες που χρησιμοποιούν καυστικές ουσίες, οικοδόμοι κλπ, προκαλούνται από τη μακροχρόνια επίδραση αυτών φθορές των θηλογράμμων και ως εκ τούτου καθίσταται δύσκολη η διαπίστωσή τους δακτυλοσκοπικώς.

**γ. <u>Το Ανόμοιο</u>**

Τα ιδιαίτερα χαρακτηριστικά των δακτυλικών αποτυπωμάτων είναι ανόμοια στα διάφορα άτομα. Ουδέποτε υπάρχει ταύτιση αποτυπωμάτων δύο ατόμων. Ακόμη, κανένα δακτυλικό αποτύπωμα δεν ταυτίζεται με άλλο, έστω και του ιδίου ατόμου αλλά διαφορετικού δακτύλου.

Τα δακτυλικά αποτυπώματα δεν **κληρονομούνται**, γιατί διαφορετικά δεν θα υπήρχε ανομοιότητα. Η ανομοιότητα αυτή διατηρήθηκε μέχρι σήμερα και σε άτομα που προέρχονται από το ίδιο ωάριο-σπερματοζωάριο (μονοωγενείς δίδυμοι). Κληρονομούνται όμως τα σχήματα των τύπων ή και σπάνια σχήματα θηλοειδών γραμμών. Άλλο όμως η ομοιότητα των τύπων και άλλο η ταύτιση των χαρακτηριστικών σημείων των δακτυλικών αποτυπωμάτων.

Πολλοί, αγνοώντας τους κανόνες της Δακτυλοσκοπίας, προτείνουν, στις δίκες περί πατρότητας, να εξετασθούν και οι τύποι των δακτυλικών αποτυπωμάτων, πράγμα βέβαια άσκοπό. Η φυλή του ατόμου δεν μπορεί να προσδιοριστεί από τα δακτυλικά αποτυπώματα.

## 6.4 Αυτόματο Σύστημα Αναγνώρισης Δακτυλικών Αποτυπωμάτων (Α.Σ.Α.Δ.Α./A.F.I.S.)

Η Διεύθυνση Εγκληματολογικών Ερευνών ήθελε από καιρό να περάσει από το χειρωνακτικό σύστημα στο αυτόματο. Με Δημόσιο διαγωνισμό που προκήρυξε, προέβη στην αγορά ενός τέτοιου συστήματος της Αμερικάνικης Εταιρείας PRINTRAK. Το Α.Σ.Α.Δ.Α. τοποθετήθηκε στο 14$^{ο}$ όροφο του Αστυνομικού Μεγάρου Αθηνών, όπου στεγάζεται η Δ.Ε.Ε. Το σύστημα αποτελείται από 6 σταθμούς εργασίας, συνδεδεμένους σε τοπικό δίκτυο και από ένα απομεμακρυσμένο σταθμό, ο οποίος είναι εγκατεστημένος στην Υ.Ε.Ε.Β.Ε. στη Θεσσαλονίκη.

Η διαμόρφωση του συστήματος έχει ως εξής :

1. Δύο πολυλειτουργικοί σταθμοί (IWS), ένας στην έδρα της Δ.Ε.Ε. και ένας στην έδρα τη Υ.Ε.Ε.Β.Ε. Ο πολυλειτουργικός σταθμός εργασίας έχει τη δυνατότητα εισαγωγής – αναζήτησης-επαλήθευσης δεκαδακτυλικών και λανθανόντων.

2. Δύο σταθμοί εισαγωγής-αναζήτησης λανθανόντων και επαλήθευσης δεκαδακτυλικών και λανθανόντων.

3. Τρεις σταθμοί επαλήθευσης αναζητήσεων δεκαδακτυλικών και λανθανόντων.

Με το Α.Σ.Α.Δ.Α. μπορούμε να κάνουμε τις παρακάτω συζητήσεις :

- Δεκαδακτυλικό προς Δεκαδακτυλικό
- Δεκαδακτυλικό προς Λανθάνον
- Λανθάνον προς Δεκαδακτυλικό
- Λανθάνον προς Λανθάνον

Το Σύστημα άρχισε να λειτουργεί στις αρχές Μαρτίου 1996.

Επί του παρόντος η Υπηρεσία σχηματίζει τη Βάση των Δεκαδακτυλικών δελτίων στο Α.Σ.Α.Δ.Α., δηλαδή μετατρέπει τα δακτυλοσκοπικά δελτία σε ηλεκτρονική μορφή. Παράλληλα η Υπηρεσία αναζητεί αποτυπώματα που βρίσκονται στους τόπους των εγκληματικών πράξεων (λανθάνοντα) προς τα δακτυλοσκοπικά δελτία και ήδη έχει κάνει αρκετές διαπιστώσεις ταυτότητας αγνώστων δραστών, διαφόρων εγκληματικών πράξεων, μεταξύ των οποίων και ανθρωποκτονίες.

Η σημασία του συστήματος είναι τεράστια. Ενδεικτικά αναφέρεται ότι για να αναζητηθεί ένα μεμονωμένο δακτυλικό αποτύπωμα προς μία βάση αναζήτησης 100.000 ΔΔ. απαιτούνται χιλιάδες ανθρωποώρες, ενώ το Α.Σ.Α.Δ.Α., το αναζητεί με μεγάλη ασφάλεια και ακρίβεια μέσα σε ένα περίπου λεπτό.

## 6.5 ΤΜΗΜΑ ΜΕΘΟΔΙΚΟΤΗΤΩΝ – ΦΩΤΟΓΡΑΦΙΚΟ

### ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΦΩΤΟΓΡΑΦΙΑ

**ΓΕΝΙΚΑ**

Την ιχνογράφηση και την σχεδίαση, ως μέσο απεικόνισης της σκηνής του εγκλήματος των αρχών του περασμένου αιώνα, ακολούθησε η συστηματική εισαγωγή της φωτογραφίας το 1882 από τον Γάλλο εγκληματολόγο ALFONSO BERTILLON (1853-1914).

Ταυτόχρονα καθιερώθηκε η χρήση της φωτογραφίας στην διαπίστωση της ταυτότητας και την εγκληματολογική σήμανση – μέθοδος που υιοθετήθηκε στις αρχές του 1900 και στην Ελλάδα.

Σήμερα η «φωτογράφηση» και η «δακτυλοσκοπική σήμανση» αποτελούν τις κυρίαρχες μεθόδους της διαπίστωσης της ταυτότητας, η δε φωτογραφική τεκμηρίωση της σκηνής του εγκλήματος ή συμβάντος αστυνομικού ενδιαφέροντος, κανόνας καθημερινής Εγκληματολογικής πρακτικής.

Στη διάθεση της σύγχρονης Εγκληματολογικής Φωτογραφίας, δεν τίθενται μόνο οι κλασσικές φωτογραφικές μηχανές (φορητές ή STUDIO, κλασσικών φωτογραφικών υλικών ή άμεσης εμφάνισης), αλλά πληθώρα καινοτομιών της σύγχρονης τεχνολογίας. Αυτές έχουν σχέση με την τυποποιημένη φωτογράφηση προσώπων, με αυτόματα εργαστήρια εμφάνισης-εκτύπωσης ασπρόμαυρης και έγχρωμης φωτογραφίας, φωτιστικά laser και οπτικές ίνες, φωτογράφηση και βιντεοσκόπηση από ελικόπτερα, ψηφιακή καταγραφή των εικόνων σε οπτικούς δίσκους, επεξεργασία εικόνας με ηλεκτρονικούς υπολογιστές, σύνδεση με δορυφόρους και μεταφορά της μέσω των παγκοσμίων δικτύων ηλεκτρονικής επικοινωνίας (όπως το INTERNET) κλπ..

Οι δυνατότητες της σύγχρονης Εγκληματολογικής Φωτογραφίας είναι πάρα πολλές και διαφαίνονται με την εξάπλωση και εμπέδωση της τεχνολογικής εξέλιξης, ακόμα περισσότερες.

Ενδεικτικά αναφέρονται οι παρακάτω εφαρμογές, οι οποίες από το 1995 αποτελούν καθημερινή πρακτική του Φωτογραφικού Γραφείου της Δ.Ε.Ε. :

α. Η αρχειοθέτηση των φωτογραφικών των καταζητούμενων προσώπων, σε οπτικούς δίσκους και η επίδειξή τους μέσω ηλεκτρονικών υπολογιστών.

β. Η αποστολή φωτογραφιών μέσω των modem-fax των Ηλεκτρονικών Υπολογιστών, από τις κεντρικές στις περιφερειακές Υπηρεσίες.

γ. Η ηλεκτρονική επεξεργασία και η βελτίωση/εκτύπωση εικόνας, από βίντεο κλειστών κυκλωμάτων (Τράπεζες – Αθλητικούς χώρους κλπ).

δ. Η φωτογράφηση δακτυλικών αποτυπωμάτων με ακτίνες laser.

ε. Η δημιουργία σκίτσων δραστών μέσω ειδικών προγραμμάτων ηλεκτρονικών υπολογιστών.

## Η ΧΡΗΣΙΜΟΤΗΤΑ ΤΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΦΩΤΟΓΡΑΦΙΑΣ

Η φωτογραφία σαν μέσο απεικόνισης της σκηνής του εγκλήματος, έχει ιδιαίτερη αξία για τις Δικαστικές και Αστυνομικές Αρχές, διότι μ' αυτή[1] :

α. Εικονίζεται λεπτομερώς η σκηνή του εγκλήματος.

β. Καθίσταται ευχερής η μελέτη όλων των λεπτομερειών της ερευνώμενης υπόθεσης από Αστυνομικούς και παράγοντες της δίκης.

γ. Συγκρατούνται λεπτομέρειες των ιχνών και πειστηρίων, που διαφορετικά θα ήταν αδύνατο να διατηρηθούν για μεγάλο χρονικό διάστημα.

[1] Διευθυνση Εγκληματολογικών Ερευνών: Α/Α ΤΡΥΦΕΡΗ Θεοδώρου

δ. Επιβοηθείται η μνήμη των Ανακριτικών υπαλλήλων και ενισχύεται η πεποίθησή τους για τον τρόπο που έλαβαν χώρα τα διάφορα γεγονότα.

ε. Εξασφαλίζεται αδιάψευστη μαρτυρία και ισχυρή αντικειμενική απόδειξη των γεγονότων, π.χ. επαληθεύεται ή διαψεύδεται μία μαρτυρική κατάθεση.

στ. Ομιλείται η γλώσσα της αλήθειας και ενημερώνεται αμέσως οποιοσδήποτε αρμόδιος, για το γεγονός σε ελάχιστο χρόνο.

ζ. Εξασφαλίζεται συνεχής αναπαράσταση της σκηνής του εγκλήματος για υποβοήθηση των ειδικών επιστημόνων και εμπειρογνωμόνων στην εργαστηριακή έρευνα των διαφόρων ιχνών και πειστηρίων.

## ΑΣΠΡΟΜΑΥΡΗ ΚΑΙ ΕΓΧΡΩΜΗ ΦΩΤΟΓΡΑΦΙΑ

Η επιτυχής και μακρόχρονη χρήση της Ασπρόμαυρης Φωτογραφίας στην εξυπηρέτηση των Εγκληματολογικών τεκμηριώσεων και η έλλειψη εμπειρίας στην έγχρωμη φωτογράφηση, δημιούργησε και το μύθο περί της ακαταλληλότητας χρήσης των έγχρωμων υλικών για τον ίδιο σκοπό.

Στην πραγματικότητα η έγχρωμη φωτογραφία δεν υστερεί σε τίποτα απέναντι στην ασπρόμαυρη, ούτε προς τη μακροζωία, ούτε ως προς την ποιότητα. Αντίθετα υπερτερεί σημαντικά γιατί απεικονίζει με τον καλύτερο τρόπο την ανθρώπινη επιδερμίδα, τους μώλωπες και τα τραύματα, ξεχωρίζει τα φυσικά από τα επίκτητα σημάδια του δέρματος και δίνει πληρέστερη την εικόνα του προς αναγνώριση ατόμου. Ας μην ξεχνάμε ότι οι άνθρωποι βλέπουν «έγχρωμα» και αδυνατούν να ξεχωρίσουν π.χ. μια κηλίδα αίματος από μια κηλίδα λαδιού, στην ασπρόμαυρη φωτογραφία.

Η καθιέρωση λοιπόν της έγχρωμης φωτογραφίας, τόσο στην αποτύπωση της σκηνής του εγκλήματος, όσο και στην φωτογράφηση των προσαγομένων προσώπων, κρίνεται στην εποχή μας επιβεβλημένη. Τούτο δεν σημαίνει ότι δεν υπάρχουν ειδικοί τομείς (π.χ. φωτογράφηση αποτυπωμάτων) όπου το ασπρόμαυρο παραμένει – και πρέπει να παραμείνει – το κυρίαρχο σε χρήση υλικό.

Εκτός από τα προαναφερθέντα «κλασικά» υλικά, η τεχνολογία παρέχει σήμερα τη δυνατότητα της «άυλης» (μαγνητικής, ηλεκτρονικής, ψηφιακής κλπ) φωτογράφησης / αποθήκευσης. Οι Εγκληματολογικές Υπηρεσίες θα πρέπει να παρακολουθούν και να υιοθετούν τις διευκολύνουσες το έργο τους τεχνολογικές καινοτομίες, έχοντας πάντα υπόψη τους ότι είναι πιο πρόσφορες σε σκόπιμες παρεμβάσεις/αλλοιώσεις, ενώ και νομικά υπάρχει ασάφεια ως προς την αποδεικτικής τους ισχύ.

**ΤΡΟΠΟΙ ΔΡΑΣΗΣ ΕΓΚΛΗΜΑΤΙΩΝ – (MODUS OPERANDI)**

Η αδυναμία εξευρέσεως πάντοτε δακτυλικών αποτυπωμάτων προσδιοριστικών της ταυτότητάς του δράστη στο χώρο του εγκλήματος, οδήγησε της Διωκτικές Αρχές στην αναζήτηση άλλων δηλωτικών της ταυτότητάς του στοιχείων.

Μεταξύ αυτών – αρχικά στην Αγγλία και αργότερα στις περισσότερες χώρες του κόσμου – χρησιμοποιήθηκε και η μέθοδος επισημάνσεως του δράστη, ανάλογα με τον τρόπο δράσης αυτού (Modus Operandi).

Παρατηρήθηκε δηλαδή ότι οι περισσότεροι «καθ' έξη και κατ' επάγγελμα εγκληματίες», χρησιμοποιούν στη διάπραξη των εγκλημάτων τους κατά κανόνα μια τυποποιημένη μέθοδο, που τους εξασφαλίζει την μέγιστη επιτυχία. Η μέθοδος αυτή στηρίζονταν κυρίως στην εμπειρία και τις ειδικές γνώσεις, που απέκτησαν από το επάγγελμα που κάποτε στη ζωή τους ασκούσαν.

Έτσι λόγω των γνώσεων αυτών, ευκολότερα παντός άλλου ο κλειδαράς θα διέπραττε διαρρήξεις οικιών-καταστημάτων, ο λιθογράφος παραχαράξεις νομισμάτων και ο τεχνίτης αυτοκινήτων κλοπές αυτών.

Με βάση λοιπόν συγκεκριμένους «τρόπους δράσης», τηρούνται στο Γραφείο MODUS OPERANDI της Δ.Ε.Ε. συλλογές υπόπτων δραστών προς επίδειξη στους παθόντες. Οι συλλογές αυτές αυτονόητα περιέχουν μόνο σεσημασμένα και μάλιστα με βεβαιότητα συχνής δράσεως πρόσωπα (καθ' εξή και κατ' επάγγελμα εγκληματίες).

Η ανωτέρω μέθοδος αποδείχτηκε ιδιαίτερα αποτελεσματική, αφού μόνο από την Κεντρική Υπηρεσία της Δ.Ε.Ε. την τελευταία 5ετία (1990-1995) αναγνωρίστηκαν 638 άγνωστοι δράστες.

## 6.6 ΤΜΗΜΑ ΕΡΓΑΣΤΗΡΙΩΝ / ΕΡΓΑΣΤΗΡΙΟ ΓΡΑΦΟΛΟΓΙΑΣ

Το Εργαστήριο Γραφολογίας, εφαρμόζοντας κάθε πρόσφορη επιστημονική μέθοδο και τεχνική, ενεργεί εξετάσεις χειρογράφων, δακτυλογραφημένων και άλλων εγγράφων, προς εξιχνίαση εγκλημάτων, στη διάπραξη των οποίων χρησιμοποιήθηκαν κατά τρόπο άμεσο ή έμμεσο τα έγγραφα αυτά. Ως τέτοια έγγραφα ενδεικτικά μπορεί να αναφερθούν, οι ανώνυμες απειλητικές εξυβριστικές-εκβιαστικές επιστολές, προκηρύξεις παρανόμων Οργανώσεων, επιστολές αυτόχειρα, επιταγές, συναλλαγματικές, διαθήκες κλπ., επί των οποίων αμφισβητούνται το κείμενο ή οι υπογραφές.

Επίσης, διερευνάται η νόθευση εγγράφων – δια της εξέτασης του ενιαίου της γραφής αυτών ή της χρήσεως της ίδιας ή διαφορετικής απόχρωσης μελάνης – ή ανάγνωση απαληφθείσης γραφής κλπ.

## ΓΡΑΦΟΛΟΓΙΑ

Γραφολογία είναι η επιστήμη που εξετάζει τους γραφικούς σχηματισμούς ενός ανθρώπου ή μηχανικού μέσου, είτε προς διακρίβωση της πατρότητας ενός εγγράφου, είτε (αν προέρχονται από άνθρωπο) προς διάγνωση του χαρακτήρα ενός ανθρώπου, είτε προς διάγνωση μιας ασθένειας αυτού, εξ ων και η διάκριση σε Δικαστική Γραφολογία, Χαρακτηρολογία ή Ψυχοδιαγνωστική Γραφολογία και Παθολογική Γραφολογία, αντίστοιχα.

Η Γραφολογία, ως επιστήμη, έχει ίδιο αντικείμενο και ίδια μεθοδολογία, βασίζεται δε - κυρίως – στην έρευνα και στο πείραμα.

Πλέον ανεπτυγμένος, διαδεδομένος και πολύ συχνά τιθέμενος στις υπηρεσίες του Συστήματος Απονομής της Δικαιοσύνης είναι ο κλάδος της Δικαστικής Γραφολογίας, που επιδιώκει επιστημονικά να διακριβώσει την ταυτότητα του φορέα μιας γραφής (ή / και μιας υπογραφής) και εν πάση περιπτώσει να εξιχνιάσει τις πλαστοποιήσεις – ως

νοθεύσεις αυθεντικών εγγράφων ή ως εξ υπαρχής καταρτίσεις πλαστών – της γραφής, νοούμενης, είτε ως δηλώσεως βουλήσεως έχουσας έννομες συνέπειες, συστάσεως, αλλοιώσεως, καταργήσεως δικαιωμάτων και υποχρεώσεων, είτε ως αποδείξεως ή μαρτυρίας γεγονότος του εξωτερικού κόσμου.

Η Δικαστική γραφολογία, ασχολούμενη με την πραγματογνωμοσύνη της γραφής αποτελεί κλάδο της Νομικής Επιστήμης, είναι δε ενταγμένη στην Εγκληματολογία και ειδικότερα στην Επιστημονική Αστυνομία και Ανακριτική, καθόσον αποσκοπεί – με τη βοήθεια επιστημονικών μεθόδων – στην ανεύρεση των δραστών τελεσθέντων εγκλημάτων, στα οποία προ, κατά ή μετά την τέλεσή τους χρησιμοποιήθηκε γραφή κλπ.

***Συνοπτική ιστορική επισκόπηση της γραφολογίας***

Τα πρώτα ίχνη της γραφολογίας εμφανίστηκαν κατά τον $14^{ο}$ αιώνα, αλλά η επιστήμη της γραφολογίας ανεπτύχθη κατά τον $17^{ο}$ αιώνα. Ως κύριος θεμελιωτής της θεωρείται ο συγγραφέας H.Michon, ο οποίος προσπάθησε – κατά τρόπο εμπειρικό – να την συστηματοποιήσει.

Τη μεθοδική μελέτη της νέας αυτής επιστήμης ανέλαβαν οι Γερμανοί με κυριότερους ερευνητές τους A. ERLENMEYER, L. KLAGES, MAYER, OSMBORN κλπ και στη συνέχεια άλλοι, των οποίων τα συγγράμματα μελετώνται μέχρι σήμερα.

**ΓΡΑΦΗ**

Γραφή καλείται η δια χαράξεως ή βαφής επί της επιφανείας χάρτου ή άλλης ύλης παράσταση γραμμάτων ή συμβόλων ή άλλων γραμμικών σχημάτων, τα οποία έχουν καθορισμένη φωνητική ή εννοιολογική αξία και ο – δια συνθέσεως αυτών – σχηματισμός λέξεων, φράσεων και διανοημάτων προς μετάδοση σε μακράν ευρισκόμενους ή προς υπόμνηση γεγονότος ή προς διαιώνιση στους μεταγενέστερους ή προς έκφραση βουλήσεων ή προς απλή έκφραση εσωτερικών βιωμάτων.

## ΔΙΑΚΡΙΣΕΙΣ ΤΗΣ ΓΡΑΦΗΣ

***Αναλόγως του μέσου ή του οργάνου με το οποίο παράγεται :***

- Σε χειρόγραφη (παραγόμενη με το χέρι).
- Σε μηχανική (παραγόμενη δια μηχανικών μέσων).
- Σε δακτυλογραφημένη (ή παραγόμενη με γραφομηχανή).
- Σε τυπογραφική – (παραγόμενη με κάθε τυπογραφικό μέσο).
- Σε πολυγραφική (παραγόμενη με πολύγραφο).
- Σε παραγόμενη δια printer Η/Υ.

***Αναλόγως του σχήματος :***

- Σε ατομική η οποία χαράσσεται ελεύθερα, χωρίς κάποια προσπάθεια.
- Σε καλλιγραφική.
- Σε γοτθική (με ευθείες γραμμές).
- Σε κυριλλική γραφή (γωνιώδης).
- Σε τυπογραφική (με σχήματα προσομοιάζονται με τα γράμματα του τύπου).

***Αναλόγως του μεγέθους των γραμμάτων :***

- Σε υπερμεγέθη.
- Σε μεγάλη.
- Σε συνήθη.
- Σε μικρή.
- Σε μικροσκοπική.

***Αναλόγως της κατεύθυνσης των γραμμάτων :***

- Σε κλίνουσα προς τα δεξιά.
- Σε κλίνουσα προς τα αριστερά.
- Σε όρθια.

***Είδη Γραμμάτων :***

- Γενική διάκριση = Κεφαλαία – Μικρά.
- Γραφοτεχνική άποψη.
- Βραχέα (ο, ω, α κλπ).
- Μεσαία με μήκη προς τα πάνω (δ, λ, β).
- Μεσαία με μήκη προς τα κάτω (μ, γ, ρ).
- Μακρά (ζ, ξ, ψ).

## ΠΑΡΑΓΟΝΤΕΣ ΤΗΣ ΓΡΑΦΗΣ

Κυριότεροι παράγοντες της γραφής :

- Ο χάρτης – Ιδιόμορφες γραφικές επιφάνειες.
- Η μελάνη.
- Τα μολυβδοκόνδυλα.
- Οι γραφίδες.

## ΚΥΡΙΟΤΕΡΑ ΓΡΑΦΟΛΟΓΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Τα κυριότερα γραφολογικά χαρακτηριστικά είναι :

- Ιδιορρυθμίες χάραξης τω γραμμάτων, αριθμών, υπογραφικών σχηματισμών.
- Κατανομή της γραφής ή των γραμμικών σχηματισμών.
- Έκταση και μέγεθος της γραφής / γραμμικών σχηματισμών.
- Θέση της γραφής (κλίνουσα, κάθετη κλπ).
- Ταχύτητα της γραφής – Ρυθμικότητα.

- Η πορεία της γραφίδας.
- Σύνδεση της γραφής.
- Κατεύθυνση των στίχων.
- Πλάτος των γραμμών.
- Ένταση της χάραξης (γραφική πίεση).
- Μεσογραμματικές – μεσολεκτικές αποστάσεις.
- Το γραφικό σύστημα.
- Η ορθογραφία – Το συντακτικό.
- Η χαρακτική ευχέρεια.
- Η απλούστευση ή στολισμός της γραφής.
- Εν γένει τρόπος διευθέτησης γραφής / υπογραφών στο διαθέσιμο γραφικό πεδίο κλπ.

## ΘΕΜΕΛΙΩΔΕΙΣ ΝΟΜΟΙ ΤΗΣ ΓΡΑΦΟΛΟΓΙΑΣ

### *α. Αυτοματισμός της γραφής*

Αυτοματισμός είναι η άνευ βουλητικής ενεργείας και γενικώς ενσυνειδήτου επενέργειας αυθόρμητος και κατ' επανάληψη εκδήλωση κινήσεων και ενεργειών.

Η γραφή ενός ατόμου, όταν αυτή φθάσει σε απόλυτο βαθμό εκμάθησης και εξοικείωσης και απαλλαγής από τα εκάστοτε πρότυπα, χαράσσεται τελείως ασυνείδητα, χωρίς ενσυνείδητο έλεγχο των ενεργειών των χειρών, των μυών και του εγκεφάλου.

### *β. Η ατομικότητα της γραφής*

Η Γραφολογία στηρίζεται στην ατομικότητα του γραφικού χαρακτήρα, η οποία διατηρείται – μετά τη σταθεροποίησή του – καθ' όλη τη διάρκεια της ζωής του, εξελίσσεται και μεταβάλλεται δε παράλληλα με την εξέλιξη της προσωπικότητάς του.

Όπως δύο πρόσωπα ως προς τον χαρακτήρα και την ιδιοσυγκρασία τους, δεν μπορεί να είναι απολύτως όμοια, έτσι και οι γραφές δύο ατόμων, δεν μπορεί να είναι απολύτως όμοιες, δηλ. υπάρχουν τόσοι γραφικοί χαρακτήρες όσο και ψυχικοί.

Κάθε άνθρωπος είναι κάτοχος ενός μόνο γραφικού χαρακτήρα που αποτελεί την σφραγίδα της προσωπικότητάς του.

Η ατομικότητα μάλιστα μιας ελεύθερης γραφής δεν τροποποιείται με όποιο μέλος/μέρος του σώματος και αν χρησιμοποιηθεί από τον γραφέα (στόμα, πόδι κλπ), αρκεί βέβαια το μέλος αυτό του σώματος να έχει αποκτήσει την σχετική λειτουργικότητα.

***γ. Ηθελημένη ή σκόπιμη αλλοίωση του γραφικού χαρακτήρα***

Στην πράξη συναντάται το φαινόμενο της σκόπιμης αλλοιώσεως της γραφής, σε περίπτωση που κάποιος θέλει να καταστήσει αδύνατη τη διάγνωση της προέλευσης της γραφής (ανώνυμες-εκβιαστικές επιστολές, πλαστογραφίες κλπ).

Βέβαια, σε τέτοιες περιπτώσεις, συνήθως η γραφή παρουσιάζει μια εικόνα «μάχης» μεταξύ των ανθισταμένων φυσικών συνηθειών του χεριού στην απόδοση των χαρακτήρων αφενός και αφετέρου της «υποχρέωσης» του να αποδώσει τη σκοπούμενη επιτηδευματική γραφή.

Ερωτάται : είναι δυνατό να μεταβάλει κανείς τον γραφικό του χαρακτήρα τόσο, ώστε να μη μπορεί να διαπιστωθεί η αλλοίωση.

Η απάντηση της Γραφολογίας στο ερώτημα αυτό είναι ότι η «ηθελημένη» μεταβολή του γραφικού χαρακτήρα είναι έργο δυσχερές και επικίνδυνο και η διάγνωση από τον ειδικό γραφολόγο κατά κανόνα είναι δυνατή.

***δ. Απομίμηση ξένης Γραφής***

Αυτή διαφέρει από την ηθελημένη αλλοίωση, στο ότι επιλέγεται ο τρόπος της αλλοίωσης. Ο απομιμούμενος μεταβάλλει την γραφή του, με βάση τη γραφή ενός άλλου ατόμου, την οποία έχει ως πρότυπο.

Ερωτάται : Είναι δυνατή η απομίμηση ξένης γραφής; Και σε καταφατική περίπτωση, είναι δυνατό να παραπλανηθεί είτε ο τρίτος είτε το ίδιο το θύμα της απομίμησης.

Η πείρα από την πράξη αποδεικνύει πως έχουν γίνει πολλές προσπάθειες για απομίμηση ξένης γραφής και έχουν παραπλανηθεί πολλοί, ακόμη και εκείνοι των οποίων η γραφή και υπογραφή έγινε αντικείμενο απομίμησης.

Αλλά μια απομίμηση ξένου γραφικού χαρακτήρα δεν μπορεί να διαφύγει τη διάγνωση από τον ειδικό γραφολόγο. Είναι πραγματικά ευτύχημα για τη συναλλακτική και γενικά την κοινωνική ζωή ότι η Γραφολογία σήμερα βρίσκεται σε τέτοιο σημείο εξέλιξης, ώστε παρέχει τη μέθοδο και τα κριτήρια, με τα οποία μπορεί αν διαγνωσθεί ή τουλάχιστο να πιθανολογηθεί σοβαρά, εάν έχουμε περίπτωση απομίμησης ξένου γραφικού χαρακτήρα.

Η προσπάθεια απομίμησης ξένου γραφικού χαρακτήρα, έχει πολλά κοινά με την ελεύθερη καλούμενη απομίμηση υπογραφής. Εάν λάβουμε υπόψη ότι η απομίμηση υπογραφής προϋποθέτει την ύπαρξη ιδιαιτέρων ικανοτήτων στο πρόσωπο που την επιχειρεί, γίνεται φανερό ότι η προσπάθεια απομίμησης ξένης γραφής είναι πολύ δυσκολότερο εγχείρημα, καθ' όσον εκείνος που επιχειρεί μια απομίμηση γραφής, αφήνει τα ίχνη του εγχειρήματός του, δηλ. αφήνει στοιχεία του δικού του γραφικού χαρακτήρα.

***ε. Αθέλητες – προσωρινές γραφικές αλλοιώσεις***

Σε αντίθεση με την σκόπιμη αλλοίωση της γραφής, γίνεται λόγος και για αθέλητη, όταν μια γραφή αλλοιώνεται προσωρινά από επιδράσεις που δεν προέρχονται από την ενσυνείδητη εξωτερίκευση της βουλήσεως. Οι αιτίες μπορεί να είναι ψυχοσωματικές ή

γραφοτεχνικές. Στις πρώτες ανήκουν οι οργανικές διαταραχές, οι ψυχικές διεγέρσεις, οι διαταραχές από την χρήση οινοπνεύματος, το ψύχος κλπ.

Στις γραφοτεχνικές αιτίες ανήκουν οι μη φυσιολογικές συνθήκες χάραξης όπως : γράψιμο σε λανθασμένη στάση του σώματος (π.χ όρθιος), λανθασμένη θέση χεριού που γράφει, γράψιμο σε ανώμαλη επιφάνεια στήριξης, κινούμενη επιφάνεια, χρήση ελαττωματικής γραφίδας κλπ., οι παραπάνω αλλοιώσεις, δεν μπορούν να μεταβάλλουν τον γραφικό χαρακτήρα και να παραπλανήσουν τους ειδικούς.

***στ. Παθολογικές μεταβολές της γραφής***

Προκειμένου να διακρίνουμε τις παθολογικές μεταβολές της γραφής από τις αθέλητες ή ηθελημένες αλλοιώσεις της γραφής, πρέπει να γίνει λόγος περί της Παθολογίας της γραφής. Οι παθολογικές μεταβολές της γραφής διακρίνονται σε μηχανικές και ψυχικές, καθόσον γράφουμε με το χέρι και τον εγκέφαλο.

*Οι μηχανικές μεταβολές διακρίνονται από :*

- Άτακτο γραφή.
- Τρέμουσα γραφή.

*Οι ψυχικές μεταβολές διακρίνονται από :*

- Αγραφία.
- Παραγραμματισμό.
- Γραφικό σπασμό.
- Γραφή παραλυτικών.

Η άτακτος γραφή συναντάται φυσιολογικώς στα παιδιά, όταν αρχίζουν να γράφουν παθολογικώς δε εξαιτίας :

- Ασθενειών.
- Τραυματισμός μελών.
- Υπερκόπωσης.
- Αλκοολισμού.

Η τρέμουσα γραφή εμφανίζεται συνεπεία :

- Γήρατος.
- Ψύχους.
- Χρήσης ναρκωτικών ουσιών.

Η αγραφία διακρίνεται σε :

- Άτακτο.
- Αναμνησιακή.
- Οπτική.
- Ακουστική.

Παραγραμματισμός είναι η αδυναμία να συνδέσει κάποιος τις παραστάσεις του εγκεφάλου με τα σημεία γραφής. Ο ασθενής, δεν πέφτει μόνο σε λάθη ως προς τις συλλαβές και τις λέξεις, αλλά και τις αντικαθιστά με άλλες παραπλήσιες.

Η γραφή των παραλυτικών συναντάται σε ασθενείς που πα΄σχουν από οργανική πάθηση της φαιάς ουσίας του εγκεφάλου και χαρακτηρίζονται από σφάλματα εννοιών.

## ΠΑΡΑΜΟΡΦΩΣΗ ΤΗΣ ΓΡΑΦΗΣ

Παραμόρφωση της γραφής είναι η θεληματική εκούσια αλλοίωση της γραφής, η οποία γίνεται με σκοπό να αποκρύψει την προέλευσή της ή να ενοχοποιήσει τρίτο άτομο.

***Τρόποι παραμόρφωσης της γραφής***

- Δια της χρησιμοποίησης γραμμάτων τύπου.
- Δια της χρησιμοποίησης διαφόρου τύπου γραφής.
- Δια της χρησιμοποίησης καλλιγραφικού τύπου γραφής.
- Δια της χρησιμοποίησης ιδίας επινοήσεως γραφής.
- Δια της χρησιμοποίησης ξένης δι απομίμησης γραφής.
- Δια της χρησιμοποίησης μηχανικώς παραχθεισών λέξεων και γραμμάτων.

Στις περισσότερες παραπάνω περιπτώσεις, η παραμόρφωση επιτυγχάνεται είτε με την προσπάθεια του χαράκτη να καταπνίξει τα ατομικά του γραφολογικά γνωρίσματα, είτε με την προσπάθεια να εισαγάγει στην γραφή ξένα γραφολογικά γνωρίσματα-ιδιορρυθμίες.

**ΠΛΑΣΤΟΓΡΑΦΗΣΗ ΞΕΝΗΣ ΥΠΟΓΡΑΦΗΣ**

Η πλαστογράφηση ή απομίμηση υπογραφής, αποτελεί την πλέον συνήθη περίπτωση.

*Τρόποι απομίμησης :*

- Δια της ελευθέρας απομίμησης.
- Με την βοήθεια αποτυπωτικού χάρτου (carbon).
- Με την βοήθεια υάλινης πλάκας.
- Δια φωτογραφήσεως.

*Σκαρίφημα ιδίας εμπνεύσεως (φανταστικής υπογραφής)*

- Φανταστική απόδοση με μόνο σκοπό εισαγωγής ξένων υπογραφικών στοιχείων.
- Φανταστική χάραξη με διάθεση απόδοσης κάποιων χαρακτηριστικών, που κατ' εικασία προσιδιάζουν στον φερόμενο ως υπογραφέα κλπ.

- Βραδύτητα ενεργείας.
- Διστακτικότητα ή αβεβαιότητα κινήσεων.
- Συχνή αλλαγή στάσεως γραφίδας.
- Αποσβέσεις.
- Διορθώσεις ή διπλοχαράξεις.

## ΑΝΤΙΠΑΡΑΒΟΛΗ ΚΑΙ ΕΚΤΙΜΗΣΗ ΓΡΑΦΟΛΟΓΙΚΩΝ ΓΝΩΡΙΣΜΑΤΩΝ

Πριν την αντιπαραβολή και εκτίμηση των γραφολογικών γνωρισμάτων, προέχει το ζήτημα της αναζήτησης, ανεύρεσης και επισήμανσης αυτών.

Αυτό εξαρτάται κυρίως :

- Από την πείρα του ειδικού.
- Από την ποσότητα και ποιότητα του γραφολογικού υλικού.
- Από την συχνότητα εμφανίσεως των γραφολογικών γνωρισμάτων.
- Από την διαπίστωση ότι τα ίδια γνωρίσματα υπάρχουν στα συγκρινόμενα κείμενα.

Αφού γίνουν οι παραπάνω εργασίες, ο ειδικός πρέπει να ερευνήσει εάν τα γνωρίσματα είναι φυσιολογικά ή είναι προϊόν παραμόρφωσης, απομίμησης κλπ.

Η εκτίμηση των γραφολογικών γνωρισμάτων είναι ζήτημα πείρας και παρατηρητικότητας, κατάταξης αυτών σε πρωτεύοντα (ιδιορρυθμίες) ή δευτερεύοντα (κοινότυπα) και συχνότητα εμφανίσεως.

# ΣΥΜΠΕΡΑΣΜΑΤΑ

Η πιστοποίηση της αυθεντικότητας αποτελεί ένα καίριο ζήτημα στην ασφάλεια των συστημάτων. Τα παραδοσιακά μέσα για επιβεβαίωση ταυτότητας, όπως οι κωδικοί και τα PINs, έχουν κυριαρχήσει στο χώρο των υπολογιστών και η κυριαρχία τους αναμένεται να συνεχιστεί και τα επόμενα χρόνια. Ωστόσο, οι αυξανόμενες απαιτήσεις για ασφάλεια και διευκόλυνση των χρηστών οδηγούν στην ανάδυση νέων, ελπιδοφόρων τεχνολογιών. Η βιομετρική αποτελεί μια νέα τάση στο χώρο της πιστοποίησης αυθεντικότητας, που συγκεντρώνει αρκετές πιθανότητες για να κυριαρχήσει στο μέλλον.

Υπάρχουν κάποιοι αντικειμενικοί παράγοντες που ευνοούν την εξάπλωση και καθιέρωση της βιομετρικής. Πράγματι, η χρήση βιομετρικής τεχνολογίας υποκινείται σήμερα από την αλματώδη αύξηση της υπολογιστικής ισχύος, και επιβάλλεται από την υψηλή διασύνδεση των υπολογιστών παγκοσμίως. Ήδη απ' το 1999, το κόστος και το μέγεθος των βιομετρικών συστημάτων μειώνεται, ενώ αυξάνεται η ακρίβεια και η ευκολία χρήσης τους. Έτσι, σήμερα η βιομετρική χρησιμοποιείται σε αρκετές εφαρμογές, από τις πιο μετριοπαθείς ως τις πιο σύνθετες, προσφέροντας σημαντικά πλεονεκτήματα, όπως η αύξηση της ασφάλειας, η διευκόλυνση των πελατών, ο περιορισμός της απάτης και η γενικότερη αναβάθμιση των υπηρεσιών. Σε κάθε περίπτωση, προσφέρει αυξημένη βεβαιότητα για την ταυτότητα ενός ατόμου, γεγονός που αποτελεί εγγύηση για την αξιοπιστία, την οικονομική σταθερότητα και την ευημερία των οργανισμών.

Αυτό δε σημαίνει ότι τα βιομετρικά συστήματα είναι άτρωτα απέναντι σε επιθέσεις. Υπάρχουν σημαντικά ζητήματα ασφαλείας, που πρέπει να αντιμετωπισθούν κατά τη φάση του σχεδιασμού και της υλοποίησής τους, αφού τα θεωρητικά πλεονεκτήματα που διαθέτουν, μπορεί στην πράξη να εξανεμιστούν, αν δεν τεθεί το κατάλληλο πλαίσιο λειτουργίας. Αυτό που πρέπει να γίνει αντιληπτό, είναι ότι για να μπορέσει η βιομετρική να λειτουργήσει με τρόπο αδιάβλητο, πρέπει απαραιτήτως να πληρούνται κάποιες προϋποθέσεις. Συγκεκριμένα, είναι αναγκαίο να αναπτυχθεί και να υιοθετηθεί σε μεγάλη κλίμακα ένα εξειδικευμένο βιομετρικό πρωτόκολλο ασφαλείας, με τα χαρακτηριστικά που προτείνονται στο πέμπτο κεφάλαιο της παρούσης εργασίας. Στην αντίθετη περίπτωση, ενδεχομένως η βιομετρική τεχνολογία να αποτελέσει το Δούρειο Ίππο για την

εξαπόλυση επιθέσεων, με τραγικές συνέπειες για την αξιοπιστία της. Επίσης, ενδείκνυται η χρήση εξειδικευμένων συσκευών hardware, που να μην μπορούν να αλλοιωθούν από εξωτερικές παρεμβάσεις, και να χαρακτηρίζονται από ικανοποιητική απόδοση. Κι αυτό γιατί, παρότι οι συσκευές δεν επηρεάζουν το χρησιμοποιούμενο αλγόριθμο σύγκρισης, ευθύνονται για τα δεδομένα που προσκομίζουν στο σύστημα, και άρα συνιστούν ένα σημαντικό παράγοντα ασφαλείας.

Όλα αυτά τα μέτρα και οι προφυλάξεις αποσκοπούν, αφενός στο να θωρακίσουν την ασφάλεια των συστημάτων, και αφετέρου στο να πείσουν το κοινό, που θα είναι και ο τελικός αποδέκτης και κριτής της βιομετρικής τεχνολογίας, για την ευρωστία και την αξιοπιστία της. Σύμφωνα με τις υπάρχουσες ενδείξεις, η βιομετρική θα γνωρίσει άνθιση μέσα στις επόμενες δεκαετίες και θα έχει τις πρώτες γενικευμένες της εφαρμογές. Το διάστημα αυτό όμως, θα κρίνει στην ουσία το μέλλον της τεχνολογίας, καθορίζοντας αν η άνθιση αυτή θα είναι πρόσκαιρη ή συνεχής. Αν δηλαδή η βιομετρική καταφέρει μέσα από τις πρώτες μαζικές εφαρμογές της, να πείσει για τη σοβαρότητα και τα εχέγγυα αξιοπιστίας που διαθέτει, υποσκελίζοντας τις αντιδράσεις για θέματα ιδιωτικότητας, τότε πράγματι θα καθιερωθεί. Άλλωστε, οι συνθήκες σήμερα το ευνοούν, με το κλίμα φόβου που έχει καλλιεργηθεί στους πολίτες ανά την υφήλιο, για μελλοντικές επιθέσεις πανταχόθεν. Αν όμως, οι εφαρμογές της βιομετρικής τεχνολογίας κριθούν ανεπαρκείς σε θέματα ασφαλείας, ή θεωρηθεί ότι παραβιάζουν ζωτικά ανθρώπινα δικαιώματα, τότε οι αντιδράσεις ενάντια στη χρήση της θα οξυνθούν, με συνέπεια να ευνοηθούν άλλες τεχνολογίες πιστοποίησης της αυθεντικότητας. Γι' αυτό άλλωστε, είναι ιδιαίτερα σημαντικό η βιομετρική να χεησιμοποιηθεί με σύνεση και προσοχή, ώστε να καταφέρει να ικανοποιήσει το διττό της ρόλο, δηλαδή την ασφάλιση των διαφόρων συστημάτων και την ικανοποίηση των χρηστών.

Πρέπει επίσης να σημειωθεί, ότι η βιομετρική τεχνολογία από μόνη της δεν αποτελεί πανάκεια για την αντιμετώπιση όλων των προβλημάτων ασφαλείας. Ακόμα δηλαδή και αν επιλυθούν επιτυχώς όλα τα σχεδιαστικά ζητήματα, εξακολουθούν να υφίστανται κάποιες ακραίες, εξεζητημένες επιθέσεις, όπως αυτές που συζητήθηκαν στο τελευταίο κεφάλαιο. Έτσι, για λόγους μεγαλύτερης ασφάλειας, είναι σκόπιμο ο βιομετρικός έλεγχος να συνοδεύονται από την παράλληλη χρήση ενός κωδικού ή μιας κάρτας ή και των δύο. Μ' αυτόν τον τρόπο, ο χρήστης συνδυάζει κάτι που γνωρίζει (έναν κωδικό) με κάτι που έχει (μια κάρτα) και κάτι που είναι (ένα βιολογικό χαρακτηριστικό), και αυτό επιφέρει

καίριο πλήγμα στις προσπάθειες ορισμένων για εξαπάτηση. Σ' αυτή την περίπτωση, η βιομετρική λειτουργεί συμπληρωματικά προς τα παραδοσιακά σχήματα πιστοποίησης και δεν τα αντικαθιστά, και έτσι και η μετάβαση σε αυτή γίνεται ομαλότερα.

Σχετικά τέλος με το ποια είναι η καλύτερη βιομετρική τεχνολογία, πρέπει να τονίσουμε ότι η κάθε μία έχει τα πλεονεκτήματα και τις αδυναμίες της, και απευθύνεται καλύτερα σε συγκεκριμένες εφαρμογές. Συνεπώς, το ερώτημα αυτό βρίσκεται σε άμεση συνάρτηση με την εκάστοτε εφαρμογή, το δημογραφικό πληθυσμό και τα διαθέσιμα μέσα υποστήριξης, και δεν μπορεί να απαντηθεί σε μια αυθαίρετη βάση. Γενικά, καμία βιομετρική τεχνολογία δεν μπορεί να θεωρηθεί ως η καλύτερη ή ότι θα κυριαρχήσει σε όλους τους τομείς, αντίθετα, οι απαιτήσεις της εκάστοτε εφαρμογής καθορίζουν την αρτιότερη βιομετρική λύση κάθε φορά, κι επομένως η σύγκριση των τεχνολογιών έχει νόημα μόνο στα πλαίσια συγκεκριμένων εφαρμογών. Αυτό που έχει εξέχουσα σημασία συνεπώς, είναι να διερευνώνται ξεχωριστά και με μεγάλη προσοχή οι απαιτήσεις και οι ιδιαιτερότητες της εκάστοτε εφαρμογής.

Σήμερα, αντικρίζουμε την αυγή μιας κοινωνίας η οποία προορίζει για όλους τους πολίτες της αυτά που ως τώρα προόριζε για τους παραβάτες. Σύμφωνα με ένα σχέδιο που έχει ήδη αρχίσει να υλοποιείται, η φυσική σχέση του Κράτους με αυτούς που ο Rousseau αποκαλούσε μέλη της επικράτειας, θα είναι βιομετρική, που πάει να πεί, γενική καχυποψία.

Υπο την πίεση της αύξουσας αποθράσσυνσης των μεταβιομηχανικών κοινωνιών, η έννοια του πολίτη προοδευτικά οδεύει από αυτή της απόλυτης πολιτικής συμμετοχής στην ολοένα και πιο έντονη συμπεριφορά σαν σε δυνάμει εγκλήματίες. Έτσι το πολιτικό σώμα μετατρέπεται σε εγκληματικό σώμα.

Οι κίνδυνοι μιας τέτοιας κατάστασης είναι φανεροί σε όλους, εκτός από όσους δεν θέλουν να δουν. Δεν μπορούμε να ξέρουμε καλά-καλά αν οι φωτογραφίες που επέτρεπαν στους ναζιστές αστυνομικούς να εντοπίσουν και να χαρτογραφήσουν τους εβραίους στις κατεχόμενες χώρες, επισπεύδοντας έτσι τη μετανάστευσή τους, ήταν αρχικά επαγγελματικές κάρτες ή δελτία ταυτότητας. Τί θα συμβεί όταν μια εξουσιαστική δύναμη κάνει χρήση των βιομετρικών δεδομένων ενός ολόκληρου πληθυσμού;

Γίνεται όλο και πιο ανησυχητικό που οι ευρωπαϊκές χώρες, αφού επέβαλαν τη βιομετρική επιτήρηση στους μετανάστες, τώρα ετοιμάζονται να την επεκτείνουν σε όλους τους κατοίκους τους. Οι αιτιολογίες της ασφάλειας που δικαιολογούν μια τέτοια πρακτική δεν είναι καθόλου πειστικές, μιας και ακόμα κι αν μπορούν να αποτρέψουν κάποιον "σεσημασμένο" να εγκληματίσει ξανά, δεν μπορούν να σταματήσουν το πρώτο έγκλημα ή μια πράξη "τρομοκρατίας". Από την άλλη, είναι απόλυτα αποτελεσματικές για τον μαζικό έλεγχο των ατόμων. Την ημέρα που η βιομετρική επιτήρηση θα γενικευθεί και η επιτήρηση από κάμερες θα εγκατασταθεί σε όλους τους δρόμους, κάθε κριτική και κάθε αξιοπρέπεια θα είναι αδύνατες.

Σαν κατακλείδα, μπορούμε να πούμε ότι η βιομετρική τεχνολογία θα απασχολήσει έντονα την κοινή γνώμη κατά τα προσεχή χρόνια, προκαλώντας ετερόκλητες αντιδράσεις και συναισθήματα. Άλλοτε θετικά, για τα ομολογουμένως εντυπωσιακά αποτελέσματά της, και άλλοτε αρνητικά, λόγω των φόβων για κακή χρήση της και διαρροή ευαίσθητων πληροφοριών του ατόμου. Αυτό που έχει σημασία να θυμηθούμε πάντως, είναι ότι καμία τεχνολογία δεν είναι από μόνη της καλή ή κακή, και ότι η χρήση της από τον άνθρωπο καθορίζει εν τέλει το είδος των επιπτώσεων που θα έχει.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


1. Anil Jain, Ruud Bolle and Sharath Pankanti, “BIOMETRICS: Personal Identification in Networked Society”, January 1999.

2. Jerome Swartz, “The Growing "MAGIC" of Automatic Identification”, *Robotics and Automation Magazine,* March 1999 Volume 6 Number 1.

3. Anil K. Jain, Sharath Pankanti, Salil Prabhakar, and Arun Ross, “Recent Advances in Fingerprint Verification”.

4. S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", *IEEE Transactions on PAMI*, Vol. 24, No. 8, pp. 1010-1025, 2002.

5. Kenneth Nilsson and Josef Bigun, “Complex Filters Applied to Fingerprint Images Detecting Prominent Symmetry Points Used for Alignment”.

6. A. K. Jain, S. Prabhakar and A. Ross, "Fingerprint Matching: Data Acquisition and Performance Evaluation", MSU Technical Report TR99-14, 1999.

7. Ruud M. Bolle, Andrew W. Senior, Nalini K. Ratha, and Sharath Pankanti, “Fingerprint Minutiae: A Constructive Definition”.

8. “Fingerprint Recognition Devices Coming in 1998”, *PC World*, 19 November 1997.

9. A. K. Jain, S. Prabhakar, and S. Pankanti, “On The Similarity of Identical Twin Fingerprints”, *Pattern Recognition*, Vol. 35, No. 11, pp. 2653-2663, 2002.

10. O. Déniz, M. Castrillón, J. Lorenzo, and M. Hernández, “An Incremental Learning Algorithm for Face Recognition”.

11. S. C. Dass, A. K. Jain and X. Lu, "Face Detection And Synthesis Using Markov Random Field Models", *Proc. International Conference on Pattern Recognition*, Quebec City, August 11-15, 2002.

12. Sarat C. Dass and A. K. Jain, "Markov Face Models", *The Eighth IEEE International Conference on Computer Vision (ICCV)*, pp. 680-687, Vancouver, Canada, July 9-12, 2001.

13. M. Castrillón Santana, J. Lorenzo Navarro, J. Cabrera Gámez, F.M. Hernández Tejera, and J. Méndez Rodríguez, "Detection of Frontal Faces in Video Streams".

14. Hichem Sahbi and Nozha Boujemaa, "Coarse to Fine Face Detection Based on Skin Color Adaption".

15. Hichem Sahbi and Nozha Boujemaa, "Robust Face Recognition Using Dynamic Space Warping".

16. Raffaele Cappelli, Dario Maio, and Davide Maltoni, "Subspace Classification for Face Recognition".

17. Shaogang Gong, Stephen J. McKenna and Alexandra Psarrou, "Dynamic Vision: From Images to Face Recognition", October 1999.

18. Arun Ross, "A Prototype Hand Geometry-based Verification System", M.S. Project Report, 1999.

19. N. Duta, A. K. Jain, and Kanti V. Mardia, "Matching of Palmprint", *Pattern Recognition Letters*, vol. 23, Number 4, pp. 477-485, 2002.

20. Martin Huddart, "Hand geometry biometric systems offer proven results for airport security", November 5, 2001.

21. N. Ratha, S. Chen, K. Karu and A.K. Jain, "A Real-time Matching System for Large Fingerprint Databases", *IEEE Trans. PAMI*, Vol. 18, No 8, pp. 799-813, 1996.

22. J. Markowitz Ph.D., "Voice ID, Applications and Markets for the New Millennium", October 1999.

23. "Voice software for security", *c|net,* 13 March 1997.

24. Masato Kawamoto, Takayuki Hamamoto, and Seiichiro Hangai, "Improvement of On-line Signature Verification System Robust to Intersession Variability".

25. A. K. Jain, Friederike D. Griess, and Scott D. Connell, "On-line Signature Verification", *Pattern Recognition*, vol. 35, no. 12, pp. 2963--2972, Dec 2002.

26. "Tool Monitors Keystroke Rhythms for ID", *TechWeb News,* October 7, 1998.

27. Friederike D. Griess. "On-line Signature Verification", M.S. Project Report, 2000.

28. "Keyboards to Read Your Fingerprints", *PC World*, 17 November 1997.

29. "Biometrics for Identification and Authentication - Advice on the Selection of Biometric Products", CESG. Issue 1.0, 23 November 2001.

30. "Protect Your PC With Face Recognition", *PC World*, 13 August 1997.

31. A. K. Jain, S. Prabhakar, and A. Ross, "Biometrics-Based Web Access".

32. "Visionics Corp. changes the face of the PC security", *Government Computer News*, 24 November 1997.

33. J. Gonzalez-Rodriguez, J. Fiérrez-Aguilar, J. Ortega-Garcia, and J.J. Lucena-Molina, “Biometric Identification in Forensic Cases According to the Bayesian Approach”.

34. Albert Pang, “Fingerprints to Replace Passwords for Net Access - Demand for Biometric Technology Grows”, February 16, 1998.

35. “Fingerprint security on the PC”, *c|net*, 7 January 1998.

36. “Coming Soon: ATMs That Recognize Your Eyes”, *The Christian Science Monitor*, 2 December 1997.

37. A. K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance", *IEICE Trans. Fundamentals*, Vol. E84-D, No. 7, pp. 788-799, 2001.

38. Simon Liu and Mark Silverman, “A Practical Guide to Biometric SecurityTechnology”, *IEEE Computer Society*, IT Pro - Security, Jan-Feb.

39. Gail R. Light, “Security vs. Liberty: weighing the options”, *MSU Today,* June 20, 2002.

40. Robert van Kralingen, Corien Prins and Jan Grijpink, “Using your body as a key; legal aspects of biometrics”, November 1997.

41. APIs reach out and touch human-ID systems *TechWeb News,* February 09, 1998.

*42.* “Biometrics”, *COMPUTER, Vol. 33, No. 2, February 2000.*

43. “Best Practices in Testing and Reporting Performance of Biometric Devices”,

44. Version 1.0, 12 January 2000, Biometrics Working Group (UK).

45. Gael Hackez, Francois Koeune and Jean-Jacques Qyisquater, “Biometrics, access control, smart cards: A not so simple combination”

46. <<Βιομετρικά Συστήματα για έλεγχο πρόσβασης>>, Στέλιος Χ.Α. Θωμόπουλος, Δ/ντης Ινστιτούτου Πληροφορικής και Τεχνολογίας , ΕΚΕΦΕ Δημόκριτος, Μαίος 2003.

47. Διπλωματική εργασία στο Μεταπτυχιακό Πρόγραμμα στη Διοίκηση Επιχειρήσεων για Στελέχη, <<Έξυπνες κάρτες υγείας: το κλειδί για το εθνικό σύστημα υγείας του μέλλοντος>>, Κουτσούκου Κατερίνα, Πειραιάς, Απρίλης 2005.

48. Διπλωματική εργασία του Τμήματος Εφαρμοσμένης Πληροφορικής , Πανεπιστήμιο Πληροφορικής, << Ασφάλεια και Εφαρμογές κρυπτογραφικών εργαλείων στον χώρο της υγείας>>, Παταρίδης Θεόδωρος, Θεσσαλινίκη Ιούνιος 2010.

49. Ευχαριστώ τους κάτωθι Αξιωματικούς της Ελληνικής Αστυνομίας για τις χρήσιμες πληροφορίες σχετικά με την Διευθυνση Εγκληματολογικών Ερευνών: Α/Α ΜΗΝΟΠΕΤΡΑ Χαράλαμπο, Α/Α ΖΩΓΡΑΦΟ Νικόλαο, Α/Α ΤΡΥΦΕΡΗ Θεόδωρο και Α/Α ΤΑΓΛΑΡΙΔΗ Ιωάννη.

# LINKS


1. http://www.biometrics.org
2. http://www.biocentricsolutions.com/
3. http://www.biometricgroup.com/
4. http://www.inbiometrics.com/biometriclibrary.htm
5. http://bio-tech-inc.com/bio.htm
6. http://stat.tamu.edu/Biometrics/
7. http://www.findbiometrics.com/Pages/iris_retinal.html
8. http://www.iris-scan.com/
9. http://www.eyeticket.com/
10. http://www.iridiantech.com/
11. http://www.nesbary.com/class/621/articles
12. http://www.emory.edu/BUSINESS/et/biometric/Biometrics.htm
13. http://www.angelfire.com/nt/selcukgun/en/tran_2.htm
14. http://www.privacy.org/pi/
15. http://www.bankersonline.com/articles/bhv09n12/bhv09n12a2.html

16. http://www.nigeriannewsservice.com/media

17. http://www.greektechforum.com/forums/forumdisplay.php

18. http://www.channelinsider.com/c/a/Security/Are-Enterprises-Ready-for-Biometrics-as-a-Security-Solution

19. http://www.biometricidentitycards.info/articles/biometric_identity_cards.html

20. http://www.businessweek.com/technology/content/jun2003/tc20030620_3373_tc119.htm

21. http://www.silicon.com/management/cio-insights/2003/06/25/biometrics-key-to-future-of-police-crime-fighting-10004850/

22. http://rioter.info/english

23. http://www.tovima.gr/

**ΣΗΜΕΙΩΣΕΙΣ:**