ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΧΕΙΡΙΣΗ ΨΗΦΙΑΚΩΝ ΔΙΑΚΑΙΩΜΑΤΩΝ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΑΤΣΙΚΑΣ ΣΩΚΡΑΤΗΣ
ΦΟΙΤΗΤΡΙΑ: ΛΑΓΟΥΔΑΚΗ ΒΕΡΟΝΙΚΗ

ΑΘΗΝΑ, 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΧΕΙΡΙΣΗ ΨΗΦΙΑΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

ΦΟΙΤΗΤΡΙΑ: ΛΑΓΟΥΔΑΚΗ ΒΕΡΟΝΙΚΗ
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΑΤΣΙΚΑΣ ΣΩΚΡΑΤΗΣ

ΑΘΗΝΑ, 2009

ΠΕΡΙΛΗΨΗ

Η συνεχής πρόοδος και εξέλιξη των ψηφιακών τεχνολογιών και η ραγδαία αύξηση της χρήσης του διαδικτύου έχει οδηγήσει στην διακίνηση μεγάλου όγκου πολυμεσικού περιεχομένου στο διαδίκτυο. Συγχρόνως όμως αναπτύσσεται η πειρατεία, που αποτρέπει τους ιδιοκτήτες του περιεχομένου από την επιλογή του διαδικτύου ως αποδοτικού και φθηνού διαύλου διανομής του ψηφιακού περιεχομένου τους.

Στα πλαίσια της παρούσας εργασίας παρουσιάζεται το νομικό πλαίσιο γύρω από τα δικαιώματα της Πνευματικής ιδιοκτησίας και πως αυτοί ενσωματώνονται στο σύστημα διαχείρισης πνευματικών δικαιωμάτων. Αναλύεται η αναγκαιότητα προστασίας του ψηφιακού περιεχομένου και πως οδηγηθήκαμε σε Σύστημα Ψηφιακής Διαχείρισης Δικαιωμάτων (DRM).

Κατόπιν, παρουσιάζονται ορισμοί DRM συστημάτων. Συγκεκριμένα, προτείνονται τα Συστήματα Ψηφιακής Διαχείρισης Δικαιωμάτων, ως μέσα προστασίας της νομοθετικής κατοχύρωσης των πνευματικών δικαιωμάτων (copyright) και υποστήριξης της διανομής του ψηφιακού περιεχομένου μέσω των δικτύων και του διαδικτύου, για την αποφυγή περιπτώσεων παραβίασης του νόμου της πνευματικής ιδιοκτησίας. Ένα σύστημα DRM πραγματοποιεί τη διαχείριση όλων των δικαιωμάτων σχετικά με τις διαδικασίες περιγραφής,προσδιορισμού,τις εμπορικές συναλλαγές και την προστασία, τον έλεγχο χρήσης και την δίωξη των παραβιάσεων των πνευματικών δικαιωμάτων του ψηφιακού περιεχομένου από την δημιουργία ως την χρήση του.

Στη συνέχεια μελετώνται τα τεχνολογικά μέσα προστασίας των DRM συστημάτων και αναλύονται οι τεχνολογίες κρυπτογράφησης, υδατογράφησης, πληρωμών και τεχνολογίες privacy. Τέλος αναφέρονται ορισμένα από τα εμπορικά συστήματα που είναι διαθέσιμα στην αγορά.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου, τον κύριο Σωκράτη Κάτσικα, για την τιμή που μου έκανε να συνεργαστούμε και για την ευκαιρία που μου έδωσε να ασχοληθώ με αυτό το θέμα.
Θα ήθελα επίσης να ευχαριστήσω την αδερφή μου Μαρίνα και τον καλό μου φίλο Διονύση Κωνσταντόπουλο για την πολύτιμη βοήθεια και την στήριξή τους.
Τέλος, οφείλω ένα μεγάλο ευχαριστώ στους γονείς μου οι οποίοι μου έδωσαν όλα τα απαραίτητα εφόδια για την επιτυχή ολοκλήρωση των σπουδών μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1:
ΕΙΣΑΓΩΓΗ

ΚΕΦΑΛΑΙΟ 1

1. ΕΙΣΑΓΩΓΗ

1.1.ΕΙΣΑΓΩΓΙΚΑ ΣΤΟΙΧΕΙΑ

Το Ίντερνετ στην εποχή μας αποτελεί ένα εκ των βασικότερων μέσων επικοινωνίας και μετάδοσης πληροφοριών σε παγκόσμιο επίπεδο. Μέσω του διαδικτύου οι χρήστες μπορούν και μεταφέρουν τεράστια αρχεία αλλά και διάφορες πληροφορίες ιδιώτες και φορείς συναλλάσσονται σε καθημερινή βάση μέσα από το διαδίκτυο. Το διαδίκτυο αποτελεί σήμερα το βασικό μέσω μετάδοσης ψηφιακών δεδομένων και πληροφοριών με στόχο να ενημερώσει αλλά και διασκεδάσει τους χρήστες.

Το βοηθητικό εργαλείο στην ανάπτυξη του διαδικτύου αποτέλεσε η ψηφιοποίηση των δεδομένων, μια και η τελευταία παρέχει τη δυνατότητα αποθήκευσης τεράστιων αρχείων σε όγκο πληροφόρησης όπως μουσικά αρχεία, επίσημα έγγραφα, οπτικό-ακουστικό υλικό, άρθρα, φωτογραφίες κ.λ.π. Οι χρήστες καταφέρνουν σήμερα μέσω του Ίντερνετ να πετύχουν μέσα σε λίγα δευτερόλεπτα αυτό που στο παρελθόν για το μέσο άνθρωπο ήθελε μέρες ακόμα και μήνες, να μεταβιβάσουν σημαντικά δεδομένα σ' οποιαδήποτε σημείο του πλανήτη.

Το βασικό πρόβλημα σε σχέση με τη μετάδοση ψηφιακών πληροφοριών είναι η καπήλευση των πληροφοριών και των δεδομένων η οποία μπορεί να γίνει κατά την αναπαραγωγή της πληροφόρησης. Θέματα πνευματικών δικαιωμάτων έχουν επηρεάσει το ψηφιακό περιβάλλον. Διάφορα συστήματα όπως το DRM λειτουργούν ως μέσα διαχείρισης ψηφιακών δικαιωμάτων. Στη συγκεκριμένη εργασία θα μελετήσουμε τη λειτουργία των ψηφιακών πληροφοριών και των ψηφιακών δικαιωμάτων και θα δώσουμε ειδική βαρύτητα στους νόμους σε σχέση με τα πνευματικά δικαιώματα.

1.2.ΨΗΦΙΑΚΑ ΑΠΟΘΗΚΕΥΤΙΚΑ ΜΕΣΑ

Ψηφιακά αποθηκευτικά μέσα μπορούμε να χαρακτηρίσουμε μέσα όπως οι σκληροί δίσκοι, τα CD’ς και DVD’ς, τα USB, sticks, οι κάρτες μνήμης τα οποία αποθηκεύουν μεγάλες ποσότητες δεδομένων. Όλα αυτά έρχονται σε αντίθεση με τα παλαιότερα μέσα αποθήκευσης(αναλογικής μορφής), όπως είναι τα βιβλία, οι πίνακες ζωγραφικής και σιγά σιγά αντικαθίστανται.

Με τα σημερινά δεδομένα η ραγδαία αύξηση του όγκου των ψηφιακών πληροφοριών οδήγησε γρηγορότερα και φθηνότερα στην αντιγραφή τους. Έτσι, περισσότερος κόσμος έχει στη διάθεση του, μέσω των υπολογιστών, δυνατότητες που του επιτρέπουν τη δημιουργία ενός ή περισσότερων αντιγράφων.

Αυτό βέβαια σημαίνει πως η φυσική ιδιοκτησία ενός ψηφιακού αντιγράφου δεν έχει τόση σημασία, αφού γίνεται τόσο εύκολα, και μάλιστα ο καθένας που έχει ένα ψηφιακό αντίγραφο έχει κάτι ταυτόσημο με αυτό του ιδιοκτήτη. Έτσι η φυσική κατοχή ενός αντίτυπου δεν εκφράζει κάτι τόσο ουσιαστικό όπως εξέφραζε ενός έντυπου υλικού, και πρέπει να βρούμε άλλους τρόπους για να διαχωρίσουμε σωστά το ποιος μπορεί να το χρησιμοποιεί και με ποιους τρόπους. Άρα είναι επιτακτικότερη η ανάγκη για να προστατευθεί η πνευματική ιδιοκτησία και τίθενται εντονότερα πολλά θέματα σχετικά με την προστασία της πνευματικής ιδιοκτησίας (copyright).
Οι νόμοι της πνευματικής ιδιοκτησίας δεν έχουν προσαρμοστεί πλήρως στα νέα δεδομένα. Είναι διαμορφωμένοι και ισχύουν για τα αποθηκευτικά μέσα αναλογικής μορφής και όχι ψηφιακής. Συμπεραίνουμε λοιπόν, ότι οι νόμοι αυτοί θα πρέπει να υποστούν τροποποιήσεις έτσι ώστε να είναι χρήσιμοι στη νέα πραγματικότητα.

1.3 ΤΑΧΥΤΕΡΗ ΚΑΙ ΤΑΥΤΟΧΡΟΝΗ ΠΡΟΣΒΑΣΗ ΣΕ ΔΕΔΟΜΕΝΑ

Τα δίκτυα υπολογιστών παρέχουν πληροφορίες σε ιδιώτες όπως τη πρόσβαση σε απομακρυσμένες πληροφορίες, καθώς και την επικοινωνία με άτομα που είναι σε απόσταση. Η πρόσβαση στην ενημέρωση και την πληροφόρηση έχει γίνει πιο εύκολη, ενώ παραδοσιακές συνήθειες όπως η αναζήτηση ενός βιβλίου έχουν αντικατασταθεί

από την αναζήτηση μεταξύ χιλιάδων τίτλων στα ‘’ ράφια ‘’ ενός εικονικού βιβλιοπωλείου. Σε αυτού του είδους την πληροφορία έχουν πρόσβαση πολλοί άνθρωποι ταυτόχρονα σε αντίθεση με ένα βιβλίο που το διαβάζει μόνο ένας.
Χαρακτηριστικό παράδειγμα είναι και η επικοινωνία από απόσταση, μέσω του ηλεκτρονικού ταχυδρομείου που επιτρέπει τη ταυτόχρονη μεταφορά εικόνας και ήχου. Ακόμα κάθε χρήστης μπορεί εύκολα να επιλέγει μέσω του υπολογιστή του τη ταινία που επιθυμεί να δεί, το τραγούδι που θέλει να ακουστεί, το παιχνίδι που θέλει να παίξει και εύκολα να το έχει στον υπολογιστή του έναντι ενός πολύ χαμηλού κόστους.

Το κόστος αναπαραγωγής είναι πολύ χαμηλό και για τους ιδιοκτήτες του περιεχομένου και για τους καταναλωτές και κάθε ηλεκτρονικό αντίγραφο είναι τέλειο αντίγραφο του πρωτοτύπου. Ο ιδιοκτήτης ενός μέσων δυνατοτήτων ηλεκτρονικού υπολογιστή έχει σήμερα την ικανότητα να παράγει τέλεια αντίγραφα πρωτότυπων δεδομένων πολλαπλών μέσων (εικόνα, βίντεο και ήχο). Τα δίκτυα υπολογιστών έχουν αλλάξει ραγδαία την οικονομία της διανομής της πληροφορίας. Με ταχύτητες μεταφοράς που αγγίζουν τους δισεκατομμύρια χαρακτήρες το δευτερόλεπτο, τα δίκτυα επιτρέπουν την αποστολή προϊόντων πληροφορίας σε παγκόσμιο επίπεδο, με χαμηλό κόστος και με μεγάλη ταχύτητα. Σαν αποτέλεσμα, είναι πλέον εύκολο για τους κατόχους δικαιωμάτων να διανείμουν την πληροφορία και για άτομα να δημιουργήσουν και να διανείμουν αντίγραφα χωρίς άδεια. Ο παγκόσμιος ιστός έχει αλλάξει την οικονομία των εκδόσεων, επιτρέποντας στον κάθε ένα να είναι ένας εκδότης με παγκόσμιο αγοραστικό κοινό. Η μεγάλη ποικιλία εγγράφων, απόψεων, κειμένων και εργασιών όλων των ειδών που υπάρχουν στον παγκόσμιο ιστό αποδεικνύει ότι εκατομμύρια άνθρωποι στον κόσμο κάνουν χρήση αυτής της δυναμικής του παγκόσμιου ιστού.

1.4.ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΝΟΜΙΚΗ ΠΡΟΣΤΑΣΙΑ.

Η διαχείριση ψηφιακών δικαιωμάτων είναι μια τεχνολογία που προστατεύει το ψηφιακό περιεχόμενο από παράνομη χρήση, όπως αυθαίρετη αντιγραφή και διανομή. Τα βασικά σημεία που προκύπτουν σχετικά με τη συνάφεια της διαχείρισης ψηφιακών δικαιωμάτων με την αγορά γενικά είναι τα εξής. Οι παραγωγοί καταναλωτικών ειδών αντιμετωπίζουν μια σύγκρουση συμφερόντων. Από τη μία οι

τελικοί χρήστες του ψηφιακού περιεχομένου αντιμετωπίζουν τη διαχείριση ψηφιακών δικαιωμάτων ως περιορισμό (εξ ου και η παράφραση: DRM, Digital Restrictions Management= Διαχείριση Ψηφιακών Περιορισμών) και από την άλλη οι πάροχοι ψηφιακού περιεχομένου τη βλέπουν ως μέσω εξασφάλισης των ψηφιακών δεδομένων τους .

Υπάρχουν διάφορες προκλήσεις που προκύπτουν από την εφαρμογή των τεχνολογιών διαχείρισης ψηφιακού περιεχομένου: μερικές από αυτές είναι η έλλειψη νομικής προστασίας, οι κίνδυνοι τεχνικής φύσεως, η εξάρτηση από τους παρόχους συστημάτων διαχείρισης ψηφιακού περιεχομένου και τα κόστη αδειοδότησης .

Η λειτουργικότητα είναι ένας παράγοντας-κλειδί στην ενσωμάτωση των συστημάτων διαχείρισης ψηφιακού περιεχομένου: λόγω της κυκλοφορίας διαφόρων συστημάτων στην αγορά, η διαλειτουργικότητα ίσως συμβάλει στο να γίνει η εφαρμογή τους πιο οικονομική.

Τα πλαίσια διαχείρισης ψηφιακών δικαιωμάτων δίνουν την αίσθηση μιας πολλά υποσχόμενης προσέγγισης της διαλειτουργικότητας. Έχουν αναπτυχθεί από μεγάλες κοινοπραξίες, με στόχο να υπάρξει σύγκλιση μεταξύ των υπαρχόντων συστημάτων διαχείρισης ψηφιακών δικαιωμάτων. Η επιτυχία αυτών των προσπαθειών τυποποίησης, ωστόσο, εξαρτάται από το εύρος της εμπλοκής της βιομηχανίας, από το κατά πόσο πραγματοποιείται εκτεταμένος έλεγχος και από την υποστήριξη σύγχρονων επιχειρηματικών μοντέλων.

Ο όρος 'Ψηφιακά Δικαιώματα' αναφέρεται σε εκείνα τα δικαιώματα που ανήκουν στη σφαίρα του ψηφιοποιημένου κόσμου και ισχύουν για ψηφιακό περιεχόμενο δημοσιευμένο και διανεμημένο σε ηλεκτρονικό σχήμα. Τα Ψηφιακά Δικαιώματα δείχνουν την ελευθερία των ατόμων να εκτελούν ορισμένες πράξεις χρησιμοποιώντας μια ηλεκτρονική συσκευή έναν επεξεργαστή ή γενικά ένα διαδραστικό δίκτυο.

Οι πράξεις που μπορεί ένα άτομο να αναπτύξει μέσα στο ψηφιοποιημένο περιβάλλον είναι παρόμοιες μ' αυτές που μπορεί ν' αναπτύξει μέσα στο κανονικό περιβάλλον το οποίο και βιώνει καθημερινά. Το Ίντερνετ είναι ένα παράλληλο εικονικό περιβάλλον, το οποίο έχει την ανάγκη κανονισμών προστασίας του.

Η δυναμική του διαδικτύου είναι τεράστια, αφού ο χρήστης μπορεί να περάσει μέσω του Ίντερνετ πληροφορίες άμεσα σε κάθε σημείο του πλανήτη και πολλές φορές χωρίς καν να ελεγχθεί.

Η τάση για υποκλοπή των ψηφιακών πληροφοριών αναφέρετε σε μια αντιστοιχία μετάδοσης πληροφοριών στη καθημερινότητα αλλά και την έννοια του copyright, όπως αυτό αναπτύσσεται στην παραδοσιακή νομοθεσία. Πράγματι, στις περισσότερες εθνικές δικαιοδοσίες, το ψηφιακό περιεχόμενο υπόκειται στις ρυθμίσεις της νομοθεσίας για το copyright. Με βάση αυτές τις θέσεις κατανοούμε ότι ενώ το Ίντερνετ είναι ένα λειτουργικό εργαλείο μετάδοσης πληροφοριών ένα εργαλείο ενίσχυσης της έκφρασης, του λόγου και γενικά της αναζήτησης της γνώσης, υπάρχουν αυτοί που δικαιολογημένα είναι υπέρ του copyright, λέγοντας ότι το διαδίκτυο αποτελεί ένα εξαιρετικά επικίνδυνο πεδίο το οποίο πρέπει να περιοριστεί μέσα από τη νομοθεσία προκειμένου να μην έχει ανεξέλεγκτη χρήση και λειτουργία.

Πασίγνωστα προβλήματα μεταξύ των οποίων τα δίκτυα κοινών αρχείων μεταξύ ομότιμων (Peer-to-Peer) , δηλαδή το λογισμικό που χρησιμοποιείται για (βασικά παράνομη) ανταλλαγή μουσικής και άλλων αρχείων, ανέπτυξαν μια σειρά από νομοθετήματα και αυτό είναι μόνο ένα εκ των παραδειγμάτων για την ανεξέλεγκτη χρήση του Ίντερνετ.

Με βάση τα παραπάνω κατανοούμε το λόγο, ανάπτυξης μιας τάσης αυτό- ρύθμισης, έτσι ώστε να διασφαλιστεί και να διατηρηθεί η εφαρμογή και η παρακολούθηση της παραδοσιακής νομοθεσίας για το copyright, με τη χρήση τεχνολογιών όπως τα φίλτρα σε σημεία κοινής πρόσβασης, προκειμένου να διασφαλιστεί, να εντοπιστεί και να ελεγχθεί το ψηφιακό περιεχόμενο.

Η νομοθεσία και η τεχνολογία προχωρούν προκειμένου να σχεδιάσουν το περίγραμμα ενός ρυθμιστικού-προστατευτικού πλαισίου για το ψηφιακό περιεχόμενο. Στην πραγματικότητα, η αντιδραστική νομοθεσία για το copyright και η τεχνολογία για το Digital Rights Management -DRM (Διαχείριση των Ψηφιακών Δικαιωμάτων) επιφέρουν ισχυρό πλήγμα στις ελευθερίες των ανθρώπων, αποστερώντας τους από φυσικά και συνταγματικά κατοχυρωμένα ανθρώπινα δικαιώματα.

Οι μεγάλες εταιρίες των μέσων επικοινωνίας, προκειμένου να διατηρήσουν τα όλο και πιο ξεπερασμένα επιχειρηματικά πρότυπά τους, προσπαθούν να περιορίσουν την πρόσβαση στο περιεχόμενό τους, κλειδώνοντας το με το DRM. Κάποτε, το DRM αποτελούσε μια πρόσθετη πρόνοια στην παραδοσιακή προστασία του copyright, σήμερα όμως έχει μεταμορφωθεί σε έναν περίπλοκο και πολύ-επίπεδο μηχανισμό άμυνας που ελέγχει με κακό τρόπο την αναπαραγωγή και τη διανομή της ηλεκτρονικής πληροφορίας, εμποδίζει την ελεύθερη πρόσβαση των ανθρώπων στο διαδίκτυο.

Επιπλέον, το DRM έχει ενισχυθεί από τους νόμους και υποστηριχθεί από μέτρα κατά της παράκαμψης. Οι μεγάλες εταιρίες των μέσων επικοινωνίας έχουν επιτυχώς ασκήσει πιέσεις στις κυβερνήσεις για να υιοθετήσουν νέες ρυθμίσεις, οι οποίες εκτός του ότι επιτρέπουν και επικυρώνουν τη χρήση του DRM, απαγορεύουν την παράκαμψή του, ανεξάρτητα από το αν η χρήση του υλικού που υπόκειται στο copyright και γίνεται δυνατή από την παράκαμψη αυτή συνιστά παραβίαση του copyright.

Το 1998, για παράδειγμα, τέθηκε σε ισχύ το Digital Millennium Copyright Act (DMCA), για να παρέχει στους κατόχους του copyright πρόσθετη ασφάλεια.
Το DMCA είναι ο νομικός κώδικας που προσφέρει προστασία στον κώδικα λογισμικού που παρέχει το DMR, το οποίο με τη σειρά του στοχεύει στην υποστήριξη του νομικού κώδικα του copyright.

Γίνεται βεβαίως εμφανές ότι το αποτέλεσμα μιας τέτοιας δια-υποστηρικτικής αλληλουχίας μπορεί να προκαλεί σύγχυση και να θέτει σε κίνδυνο τις συνταγματικά κατοχυρωμένες ελευθερίες των ανθρώπων.

Το DMCA έχει προχωρήσει ακόμη πιο μακριά, προγράφοντας συσκευές που προτίθενται να παρακάμψουν τα μέτρα προστασίας του copyright, ακόμη κι αν η παράκαμψη αυτή γίνεται για την άσκηση δικαιωμάτων εύλογης χρήσης ή για την ελευθερία του λόγου. Πιο αυστηρό από την παραδοσιακή νομοθεσία για το copyright, το DMCA ενθαρρύνει τον απόλυτο έλεγχο στα δημιουργικά έργα. Η δίωξη των ψηφιακών δικαιωμάτων έχει γίνει, στις μέρες μας, παγκόσμιο φαινόμενο.

1.5. Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ΨΗΦΙΑΚΟΥ ΕΛΕΓΧΟΥ ΣΕ ΠΑΓΚΟΣΜΙΑ ΚΛΙΜΑΚΑ

Η Ιαπωνία, η Αυστραλία και πολλές ευρωπαϊκές χώρες έχουν υιοθετήσει περιορισμούς του copyright σαν το DMCA. Τουλάχιστον εννιά ακόμη χώρες, συμπεριλαμβανομένων της Χιλής, της Γουατεμάλας και της Σιγκαπούρης, δέχονται πιέσεις για να θέσουν σε ισχύ νόμους όπως το DMCA, μια και αποτελεί προϋπόθεση για την ασφάλεια των συμφωνιών του ελεύθερου εμπορίου που ρυθμίζουν το εμπόριο.

Πριν από το Ίντερνετ, ο νόμος και ειδικότερα το δικαστήριο, ο δικαστής, καθόριζε το θέμα της προστασίας του copyright και τον τρόπο εφαρμογής της νομοθεσίας για το copyright. Ο ανθρώπινος παράγοντας ήταν ο κύριος και μοναδικός διαχειριστής της ρυθμιστικής εξουσίας της νομοθεσίας για το copyright κι αυτό το καθεστώς έδινε μια αίσθηση φυσικότητας στη νομική διαδικασία και συνεπώς μια αίσθηση κοινωνικής ασφάλειας.

Ωστόσο, στην ψηφιακή εποχή όλα υπάρχουν πέρα από τον έλεγχο της γνώσης και είναι βασικά το Ίντερνετ και όχι πλέον τα δικαστήρια που διαχειρίζονται τη δικαιοσύνη.

Ένας μη λειτουργικός κώδικας για το copyright αποτελεί το μέλλον του copyright, όπου οι προγραμματιστές θα κωδικοποιούν τον έλεγχο για την πρόσβαση στο περιεχόμενο, έναν έλεγχο που οι δικαστές δεν θα μπορούν να τσεκάρουν και τα δικαστήρια να επικυρώσουν.
Η τεχνολογία DRM έχει προχωρήσει λίγο παραπέρα από την απλή διασφάλιση της δημόσιας πρόσβασης, τη διατήρηση της εύλογης χρήσης και της προστασίας των κατόχων ψηφιακών δικαιωμάτων από την παράνομη μεταφορά δεδομένων, αποδυναμώνοντας τα ανθρώπινα δικαιώματα ιδίως στον τομέα της ελευθερίας της έκφρασης και της ιδιωτικότητας.

Το σύστημα αδειών του Creative Commons (CC) λειτουργεί προκειμένου να βελτιώσει και να προσαρμόσει το σύστημα του copyright στη σημερινή

ψηφιοποιημένη πραγματικότητα και να δώσει μια ανάσα στην πληθώρα των ψηφιακών δικαιωμάτων, που μπορούν να υπάρξουν.

Το CC αποτελεί έναν από τους πιο φιλόδοξους ανά-προσανατολισμούς του συστήματος του copyright που 'καλλιεργεί ένα commons όπου οι άνθρωποι μπορούν να νιώσουν ελεύθεροι να μοιραστούν τα δικαιώματά τους, να χρησιμοποιήσουν εκ νέου όχι μόνο ιδέες αλλά και λέξεις, εικόνες και μουσική. Επιδιώκει να δημιουργήσει έναν ‘ελεύθερο πολιτισμό’, ενισχυμένο από ένα ήθος μοιράσματος, δημόσιας εκπαίδευσης και δημιουργικής δια-δραστηριότητας'.

Το CC παρέχει εναλλακτικά συστήματα παροχής αδειών και συμβολαίων που επιτρέπουν στους δημιουργούς να οργανώνουν, να διαχειρίζονται και να χρησιμοποιούν εκ νέου τα ψηφιακά δικαιώματά τους, χωρίς να ζητούν την άδεια του κράτους ή της υπάρχουσας νομοθεσίας.

Παρέχοντας τα εργαλεία για την επωφελή χρήση των δυνατοτήτων που προσφέρει το Ίντερνετ, το CC επιχειρεί να αποκαταστήσει την ισορροπία ανάμεσα στην προστασία των ψηφιακών δικαιωμάτων και τις ανάγκες της κοινωνίας για διασφάλιση της προόδου στις τέχνες και τις επιστήμες, χωρίς να λέει στους κατόχους ψηφιακών δικαιωμάτων τι να κάνουν τις ελευθερίες τους.

Οι άδειες CC επιδιώκουν να δημιουργήσουν μια 'ζώνη άνευ ελέγχου' όπου τα ψηφιακά δικαιώματα υπάρχουν χωρίς περιορισμούς, άδειες και νομικές παρεμβάσεις. Η ιδέα τους να διευκολύνουν και να ενθαρρύνουν τη δημιουργικότητα με γενναιόδωρους όρους χορήγησης αδειών, που ευνοούν το μοίρασμα και την εκ νέου χρήση του ψηφιακού περιεχομένου, δείχνει μια θετική στάση απέναντι στην έννοια της ανοικτής πρόσβασης, της κοινότητας και της συνεργασίας, μιας τριάδας που παρέχει ευρύτερη πρόσβαση στη γνώση και την πληροφορία.

Το σύστημα αδειών του CC αποτελεί μια ελπιδοφόρα πρωτοβουλία, μια απόλυτη αλλαγή στην αποδοτικότητα των ατόμων και εγκαινιάζει ένα νέο σχήμα διαχείρισης των ψηφιακών δικαιωμάτων, παρέχοντας ένα εντελώς νέο πρότυπο, πλήρως προσαρμοσμένο στις απαιτήσεις της ψηφιοποιημένης εποχής.

1.6. ΝΟΜΟΣ ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Με την εμπορευματοποίησή της και την ενσωμάτωσή της στην καθημερινή ζωή, η ψηφιακή πληροφορία αναγκαστικά έπρεπε να ακολουθήσει τους νόμους της πνευματικής ιδιοκτησίας. Σήμερα, πράξεις που μπορούν να γίνονται κατ' επανάληψη από το μεσαίο πολίτη, όπως για παράδειγμα η επισκόπηση πληροφοριών και η προώθηση πληροφοριών μέσω του Διαδικτύου, είναι εν αγνοία του παραβιάσεις των νόμων περί πνευματικής ιδιοκτησίας. Άλλες πράξεις όπως η δημιουργία αντιγράφων για προσωπική χρήση ίσως και να απαιτούν κάποια τροποποίηση των νόμων για να δικαιολογηθεί η νομιμότητά τους. Οι χρήστες στην καθημερινή τους ζωή έχουν τη δυνατότητα να έχουν πρόσβαση και να αντιγράφουν μεγάλα ποσά ψηφιακής πληροφορίας, ενώ συγχρόνως έχουν έλλειψη μιας καθαρής εικόνας για το τι είναι αποδεκτό και νόμιμο.

Οι νόμοι περί πνευματικής ιδιοκτησίας έχουν ως στόχο να προστατέψουν τα έργα που χαρακτηρίζονται από δημιουργικότητα, όπως έργα λογοτεχνίας, θεάτρου, μουσικής, τέχνης κ.ά. Ανάμεσα στην πληθώρα των νομικών διατάξεων που αφορούν στα πνευματικά δικαιώματα, υπάρχουν νόμοι που σχετίζονται περισσότερο ή λιγότερο με τα δικαιώματα πνευματικής ιδιοκτησίας, όπως αυτά διαμορφώνονται κατά την ψηφιοποίηση και την προβολή περιεχομένου στο Διαδίκτυο. Επίσης, ένα ακόμη χαρακτηριστικό της νομοθεσίας περί του δικαιώματος αναπαραγωγής είναι ότι παρουσιάζει αρκετές ομοιότητες με την νομοθεσία που αφορά στις εμπορικές συναλλαγές.

Η κυρίαρχη τάση στις περισσότερες χώρες είναι να δίνεται μεγαλύτερη έμφαση στην προστασία των δικαιωμάτων του δημιουργού –ηθικά δικαιώματα. Η συγκεκριμένη προσέγγιση επικρατεί στις νομοθετικές τάσεις όλης της Μεσογειακής Ευρώπης και σε μικρότερο βαθμό στην Αγγλική και στην Αμερικανική νομοθεσία.

Υπάρχει μια αρκετά σημαντική παράδοση στην προσπάθεια εναρμόνισης όλων των χωρών για μία κοινή, διεθνή αντιμετώπιση του προβλήματος. Η ανάγκη για καθολική εναρμόνιση κρίνεται επιτακτική, κυρίως λόγω του αφηρημένου χαρακτήρα των πνευματικών δικαιωμάτων και της αυξημένης δυσκολίας που προκύπτει κατά την εφαρμογή των αναγκαίων περιορισμών. Το Διαδίκτυο και οι επιπρόσθετες

δυνατότητες που πηγάζουν από την ψηφιακή υπόσταση του περιεχομένου επιβεβαιώνουν το γεγονός πως οι εθνικές διατάξεις δεν είναι ικανές να εξασφαλίσουν το απαιτούμενο επίπεδο προστασίας. Ένα χαρακτηριστικό παράδειγμα είναι η περίπλοκη περίπτωση όπου το περιεχόμενο έχει δημιουργηθεί σε μία χώρα, φιλοξενείται από έναν εξυπηρετητή σε μία άλλη χώρα και μπορεί να ανακτηθεί από οποιοδήποτε μέρος της γης.

Ο ρόλος της εθνικής νομοθεσίας είναι να οριοθετήσει το εύρος των ενεργειών που θεωρούνται νόμιμες σε κάθε χώρα. Ωστόσο η ανάλυση των επιμέρους στοιχείων μιας νομοθεσίας δε θα πρέπει να γίνει ανεξάρτητα και αποκομμένα από τη συνολική διεθνή κατάσταση. Η διεθνής κατάσταση συνίσταται από διεθνείς συμφωνίες, οδηγίες και κατευθύνσεις που διαδραματίζουν σημαντικό ρόλο στη διαμόρφωση των επιμέρους νομοθετικών πλαισίων κάθε χώρας. Οι πιο σημαντικές διεθνείς συμβάσεις είναι οι ακόλουθες :

- Η Συνθήκη της Βέρνης(που διαχειρίζεται ο παγκόσμιος οργανισμός πνευματικής ιδιοκτησίας –WIPO)
- Η παγκόσμια συνθήκη περί του δικαιώματος αναπαραγωγής (UCC)
- Η συμφωνία του TRIPR (Trade Related Intellectual Property Rights) υπο την αιγίδα του World Trade Organization.

Το πνεύμα των διεθνών συμβάσεων είναι να προτείνουν ένα σύνολο από ελάχιστες απαιτήσεις που θα πρέπει να υιοθετηθούν από όλα τα συνυπογράφοντα μέλη.

ΚΕΦΑΛΑΙΟ 2:
ΣΥΣΤΗΜΑΤΑ ΨΗΦΙΑΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 2

2.ΣΥΣΤΗΜΑΤΑ ΨΗΦΙΑΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ

2.1. ΓΕΝΙΚΕΣ ΕΝΝΟΙΕΣ

Οι ορισμοί των συστημάτων ελέγχου πρόσβασης, των τεχνικών μέσων προστασίας και των συστημάτων διαχείρισης είναι ακόμη υπό τελικό καθορισμό στη διεθνή κοινότητα. Με βάση το σκοπό και το ρόλο που επιτελούν παρατίθενται οι παρακάτω ορισμοί:

- Ένα σύστημα ελέγχου πρόσβασης διαχειρίζεται την πρόσβαση ενός χρήστη σε κάποιο περιεχόμενο, συνήθως με χρήση κωδικών. Αυτό το σύστημα προστασίας χρησιμοποιείται συχνά σε websites στα οποία όταν ο χρήστης αποκτήσει την πρόσβαση στο περιεχόμενο δεν υπάρχει καμία άλλη προστασία.
- Τεχνικά Μέσα Προστασίας: Είναι μία τεχνολογία που υποστηρίζει τους χρήστες, τους ιδιοκτήτες περιεχομένου και τους οργανισμούς να προστατεύσουν και να διασφαλίσουν το ψηφιακό περιεχόμενο (κείμενο, εικόνα, βίντεο, ήχος, γραφικά) από μη εξουσιοδοτημένη χρήση. Ο ορισμός εμπεριέχει και την ικανότητα ανίχνευσης μίας μη εξουσιοδοτημένης χρήσης.
- Σύστημα Ψηφιακής Διαχείρισης Δικαιωμάτων: Ένα σύστημα που υποστηρίζει τη διαχείριση των δικαιωμάτων του ψηφιακού περιεχομένου για τους προμηθευτές και τους χρήστες και περιλαμβάνει επιχειρηματικά μοντέλα βασισμένα στο χρόνο και στη χρήση.

Κατά τη διεθνή πρακτική δεν υπάρχει διαχωρισμός μεταξύ τεχνικών μέσων προστασίας και συστημάτων διαχείρισης δικαιωμάτων. Συνήθως, γίνεται αναφορά μόνο στον όρο DRMS ο οποίος περιλαμβάνει στον ορισμό του και τα τεχνικά μέσα προστασίας.

Το Δεκέμβριο του 1997 η Ευρωπαϊκή Επιτροπή παρουσίασε μία πρόταση – οδηγία το copyright και τα συγγενικά δικαιώματα στην Κοινωνία της Πληροφορίας που στοχεύει στην επέκταση της προστασίας των πνευματικών δικαιωμάτων σε νέες μορφές τεχνολογίας όπως το Διαδίκτυο, τα CD-Rom, τα DVDs.

Το Ευρωπαϊκό Κοινοβούλιο κατά την πρώτη παρουσίαση στις 10 Φεβρουαρίου 1999 υιοθέτησε έναν αριθμό από τροποποιήσεις στην πρόταση, πολλές από τις οποίες ενσωματώθηκαν στην οδηγία. Με βάση αυτήν την οδηγία, τα κράτη μέλη κλήθηκαν να εναρμονίσουν την εθνική τους νομοθεσία για τη δημιουργία ενός κοινού νομοθετικού πλαισίου στην Ευρωπαϊκή Ένωση.

Τα τεχνικά μέσα προστασίας και διαχείρισης αναγνωρίσθηκαν από τη νομοθεσία και προστατεύονται από ειδικές νομοθετικές ρυθμίσεις. Η υδατοσήμανση, η κρυπτογραφία και άλλες τεχνολογίες είναι πλέον νομικά προστατευμένες και κάθε πράξη εναντίον τους (π.χ. επίθεση στο υδατόσημα μιας ψηφιακής εικόνας) είναι πράξη που μπορεί να διωχθεί νομικά.

Συνεπώς δημιουργήθηκε η απαραίτητη νομική βάση που επιτρέπει τους ιδιοκτήτες περιεχομένου και copyright να απαιτούν οικονομική ανταπόδοση αν τα μέσα προστασίας που χρησιμοποιούν (π.χ. υδατοσήμανση) έχουν δεχθεί επίθεση από τρίτους

2.2. ΟΡΙΣΜΟΣ DRM

Η Διαχείριση Ψηφιακής Πνευματικής Ιδιοκτησίας αναφέρετε στη χρησιμοποίηση κατάλληλων τεχνολογικών μέσων, από εταιρείες ή και απλούς κατόχους πνευματικής ιδιοκτησίας, με σκοπό τον περιορισμό της χρήσης ψηφιακών δεδομένων είτε συσκευών είτε αναπαραγωγής συγκεκριμένων μέσων σε συγκεκριμένες συσκευές.
Η Ψηφιακή Διαχείριση Δικαιωμάτων είναι σχετικά πρόσφατη τεχνολογία. Η χρήση της ξεκίνησε στα μέσα της δεκαετίας του 1990 παρ' όλα αυτά έχει περάσει από πολλά στάδια ανάπτυξης. Αρκετά περισσότερα από ότι φανερώνει η ηλικία της. Από τη μία έχει επαινεθεί ως ο σωτήρας των πνευματικών δικαιωμάτων και από την άλλη έχει κατακριθεί ως εντελώς αναποτελεσματική στην προστασία πνευματικής ιδιοκτησίας. Ένας πρώτος στενός ορισμός του τι είναι DRM έχει ως εξής: «Ψηφιακή Διαχείριση

Δικαιωμάτων είναι ένα είδος λογισμικού εξυπηρετητή αναπτυγμένο με σκοπό να υλοποιεί έναν ασφαλή μηχανισμό διάθεσης ψηφιακού περιεχομένου και ίσως πιο σημαντικά να αποτρέψει την παράνομη διάθεση πληρωμένου ψηφιακού υλικού»

Αν και αυτός ο ορισμός είναι σωστός και αντιπροσωπεύει την επικρατούσα άποψη του τι είναι DRM δεν δίνει την πλήρη εικόνα αφού αγνοεί το περιβάλλον μέσα στο οποίο πρέπει να λειτουργήσει ένα σύστημα DRM. Το περιβάλλον αυτό καθορίζεται από την αλληλουχία των βημάτων που περνά ένα ψηφιακό περιεχόμενο όταν πρόκειται να διατεθεί ως εμπορικό προϊόν. Τα βήματα αυτά είναι:

1. Παραγωγή.
2. Ψηφιοποίηση.
3. Προσάρτηση στοιχείων για την ταυτοποίηση του ψηφιακού αντικειμένου.
4. Προσάρτηση περιγραφών του περιεχομένου.
5. Διανομή.
6. Χρήση από τον καταναλωτή.
7. Επίβλεψη και έλεγχος της χρήσης.
8. Αποκομιδή του χρηματικού αντιτίμου.

Δεν είναι απαραίτητο βέβαια ένα ψηφιακό προϊόν να περάσει από όλα τα παραπάνω στάδια. Για παράδειγμα αν το ψηφιακό περιεχόμενο διατίθεται δωρεάν το βήμα της χρηματικής συναλλαγής δεν είναι απαραίτητο.

Η Διαχείριση Ψηφιακών δικαιωμάτων παίζει ρόλο σε κάθε ένα από τα παραπάνω βήματα. Συνεπώς ένας πιο ολοκληρωμένος ορισμός του τι είναι DRM μπορεί να δοθεί ως εξής:

Η Ψηφιακή διαχείριση δικαιωμάτων καλύπτει την περιγραφή, ταυτοποίηση , συναλλαγή , προστασία , παρακολούθηση, και ανίχνευση όλων των μορφών χρήσης ψηφιακού περιεχομένου τόσο σε άυλη όσο και σε υλική μορφή.

Με λίγα λόγια η Ψηφιακή Διαχείριση δικαιωμάτων καλύπτει οτιδήποτε κάνει κάποιος για να εμπορευθεί ένα ψηφιακό αντικείμενο. Σε αυτή την αλυσίδα βημάτων επεξεργασίας ένα σύστημα DRM επιτελεί πολλές επί μέρους λειτουργίες. Αυτές μπορούν διαχωριστούν σε δύο ευρείες κατηγορίες.

Εικόνα1: Ρόλοι ενός DRM συστήματος

Οι πρώτες είναι αυτές που δίνουν κύριο βάρος στο ρόλο της διαχείριση. Για παράδειγμα η ταυτοποίηση του περιεχομένου, η συλλογή μεταδιδόμενων για αυτό και άλλα. Οι δεύτερες είναι αυτές που δίνουν βάρος στην ανάπτυξη ψηφιακών τεχνικών για τη διαχείριση του περιεχομένου.

2.3. ΠΕΡΙΒΑΛΛΟΝ ΛΕΙΤΟΥΡΓΙΑΣ ΣΥΣΤΗΜΑΤΩΝ DRM

Περιβάλλον λειτουργίας συστημάτων DRM. Τα στοιχεία ενός DRM συστήματος χρησιμοποιούνται στα διάφορα στάδια της αλυσίδας αγοραπωλησίας ενός ψηφιακού περιεχομένου. Ήδη από αυτό το γεγονός και μόνο βλέπουμε ότι κάθε στοιχείο δεν μπορεί να λειτουργήσει ανεξάρτητα από το περιβάλλον του.

Οι τεχνολογίες που χρησιμοποιούνται εξαρτώνται τόσο από το επιχειρηματικό μοντέλο όσο και από την τεχνολογία που είναι διαθέσιμη και επίσης από την ισχύουσα νομοθεσία που διέπει την αγορά. Για παράδειγμα θα ήταν ανώφελο να χρησιμοποιηθούν τεχνολογικά μέσα με πολύ υψηλό κόστος για την προστασία ενός σχετικά ευτελούς αξίας ψηφιακού αντικειμένου.

Όμοια το να χρησιμοποιηθούν τεχνολογικά μέσα που είναι παράνομα σε χώρες των οποίων οι αγορές αντιπροσωπεύουν ένα μεγάλο κομμάτι των πωλήσεων καταδικάζει σε εμπορική αποτυχία μία τέτοια εφαρμογή.

Ένα DRM σύστημα για να είναι επιτυχές πρέπει να στηρίζεται εξ' ίσου στα τρία συστατικά που είναι απαραίτητα για τη λειτουργία του. Την τεχνολογία, την νομοθεσία και το επιχειρηματικό μοντέλο. Αυτά με τη σειρά τους επηρεάζονται από εξωτερικούς παράγοντες των οποίων η επιρροή είναι τέτοια που μπορεί να καταδικάσει σε αποτυχία ένα σύστημα DRM παρ' όλο που η λειτουργία του σε τεχνικό επίπεδο μπορεί να είναι άψογη. Μία συνοπτική παρουσίαση αυτών των παραγόντων δίνουμε παρακάτω.

Οι οικονομικοί παράγοντες βαρύνουν ιδιαίτερα στις αποφάσεις που θα πάρουν οι ιδιοκτήτες και οι διανομείς των ψηφιακών αντικειμένων όσον αφορά την επιλογή της τεχνολογίας που θα χρησιμοποιηθεί για την εμπορική προώθηση των αντικειμένων αυτών. Άλλη μία σημαντική επιρροή της οικονομικής πραγματικότητας είναι ο καθορισμός της καταναλωτικής συνείδησης.

Ποια μοντέλα πώλησης και διακίνησης θα θεωρήσουν θελκτικά οι καταναλωτές και σε τι επιπλέον κόστος θα είναι εκτεθειμένοι. Για παράδειγμα αν για την ανάγνωση ενός ηλεκτρονικού βιβλίου είναι απαραίτητη και η αγορά μίας νέας συσκευής ανάγνωσης αυτό δρα αποτρεπτικά στην απόφαση για την αγορά του ηλεκτρονικού βιβλίου.

Κοινωνιολογικοί παράγοντες παίζουν και αυτοί ρόλο στην υιοθέτηση DRM τεχνολογιών. Οι χρήστες βλέπουν ένα σύστημα DRM ως περιοριστικό στα δικαιώματα που έχουν πάνω στο ψηφιακό αντικείμενο. Για να πεισθούν ότι η χρήση ενός τέτοιου συστήματος είναι αποδεκτή πρέπει το προστατευμένο υλικό να τους δίνει κάποια οφέλη που να αυξάνουν τη χρηστική του αξία. Ένα επίσης σημαντικό εμπόδιο είναι ανησυχίες ότι τα DRM συστήματα αποτρέπουν τους χρήστες από τη δίκαια χρήση του ψηφιακού αντικειμένου.
Παρόλο που τεχνικά είναι εφικτό να αντιμετωπιστούν τέτοιες καταστάσεις προς το παρόν οι DRM τεχνολογίες ασχολούνται κυρίως με το πρόβλημα της προστασίας του ψηφιακού αντικειμένου. Τα παραπάνω ζητήματα πρέπει επίσης να αντιμετωπιστούν και σε ένα διεθνές επίπεδο.

Τα κόστος παραγωγής και διανομής μπορεί να είναι τόσο μεγάλο που δεν δικαιολογεί τη διανομή σε περιορισμένο γεωγραφικά χώρο. Άρα οι παραπάνω παράγοντες οικονομικοί και νομικοί πρέπει να αξιολογούνται για όλες τις περιοχές που πρόκειται να λειτουργήσει το DRM σύστημα. Εξ' άλλου η φύση του διαδικτύου κάνει παγκόσμια διαθέσιμο οποιαδήποτε αντικείμενο το χρησιμοποιήσει ως μέσο διανομής.

2.4. ΛΕΙΤΟΥΡΓΙΚΑ ΣΤΟΙΧΕΙΑ ΕΝΟΣ DRM ΣΥΣΤΗΜΑΤΟΣ

Όπως έχουμε ήδη δει ένα DRM σύστημα πρέπει να εκπληρώσει μία πληθώρα ρόλων. Αντίστοιχα λοιπόν πρέπει να αναπτυχθούν εργαλεία κατάλληλα να υλοποιήσουν τις παρακάτω λειτουργίες.

- Ασφαλείς Χώροι Αποθήκευσης. Ο Ρόλος αυτών είναι να μην δίνουν πρόσβαση στο υλικό. Μη εξουσιοδοτημένους χρήστες.Η λειτουργία τους βασίζεται σε κρυπτογραφικούς αλγορίθμους όπως οι AES και DES.
- Περιγραφή δικαιωμάτων χρήσης. Εκφράσεις που καθορίζουν ποιος έχει πρόσβαση στο προστατευμένο αντικείμενο και τι μπορούν να κάνουν με αυτό. Μπορούν να υλοποιηθούν με απλά μέσα όπως σημάνσεις χρήσης (use flags) ή με πιο πολύπλοκα και εκφραστικά μέσα όπως γλώσσες περιγραφής δικαιωμάτων (Rights Expression Languages).
- Συστήματα ταυτοποίησης και περιγραφής ψηφιακών αντικειμένων. Χρησιμοποιούνται για την ταυτοποίηση κατά μοναδικό τρόπο ενός ψηφιακού αντικειμένου καθώς επίσης και την συσχέτιση αυτό του αντικειμένου με μεταδιδόμενα που το περιγράφουν. Παράδειγμα μίας International Standard τέτοιας τεχνολογίας είναι το Book Number (ISBN). Παρόλο που το ISBN δεν επιτρέπει την συσχέτιση μεταδιδόμενων, διεθνείς πωλητές όπως το Amazon.com χρησιμοποιούν αυτό τον κωδικό για να συσχετίσουν μεταδιδόμενα σε δικιά τους μορφή με κάθε βιβλίο.
- Εξακρίβωση της ταυτότητας ατόμων που χρησιμοποιούν ένα DRM σύστημα. Η εξακρίβωση της ταυτότητας των ατόμων που εμπλέκονται σε ένα DRM σύστημα είναι σημαντική από πολλές απόψεις. Πρώτα ο ιδιοκτήτης ενός ψηφιακού αντικειμένου πρέπει να εξασφαλίσει την νομική ισχύ της ιδιοκτησίας που έχει πάνω σε αυτό το αντικείμενο. Πρέπει να βεβαιωθεί

δηλαδή ότι όντως αυτός είναι ιδιοκτήτης του εκάστοτε αντικειμένου με τρόπο αμετάκλητο και αναμφίβολο. Επίσης ο καταναλωτής πρέπει να τακτοποιείται ώστε να μπορεί να περιορίζεται η πρόσβαση σε ένα ψηφιακό αντικείμενο μόνο σε αυτούς τους χρήστες που έχουν εξουσιοδότηση. Προκύπτει βέβαια το ζήτημα της παραβίασης της ιδιωτικότητας του καταναλωτή αφού εταιρίες που θα μετέχουν στην αλυσίδα παροχής DRM ψηφιακού περιεχομένου θα μπορούν να συλλέγουν πολύ λεπτομερείς πληροφορίες για τους καταναλωτές.

- Trusted Third Party. Για να λειτουργήσει η εξακρίβωση της ταυτότητας των μερών που συναλλάσσονται σε ένα ολοκληρωμένο σύστημα DRM πρέπει να υπάρχουν κάποιοι εγγυητές για αυτή την ταυτότητα που να είναι αποδεκτοί από όλους τους συναλλασσόμενους στο DRM σύστημα.
- Ανθεκτικές μορφές ταυτοποίησης των ψηφιακών αντικειμένων. Τεχνολογίες όπως το watermarking και το fingerprinting χρησιμοποιούνται για την εξακρίβωση παραβιάσεων της πνευματικής ιδιοκτησίας. Επίσης βρίσκουν χρήση στη μετάδοση κανόνων χρήσης σε συσκευές αναπαραγωγής, για παράδειγμα το Content Scrambling System των DVD.
- Μηχανισμός αναφοράς γεγονότων. Γεγονότα όπως η αγορά ενός ψηφιακού αντικειμένου ή η αναπαραγωγή του είναι ουσιαστικά για να επιτρέψουν επιχειρηματικά μοντέλα όπως για παράδειγμα πληρωμή επί τη προβολή.
- Συστήματα πληρωμής πρέπει να ενσωματωθούν σε ένα DRM σύστημα. Η χρήση πιστωτικών καρτών ή τραπεζικών λογαριασμών είναι κάποια παραδείγματα.
- Τέλος πρέπει να υπάρχει και η εφαρμογή που θα λειτουργεί ως συνδετικός κρίκος και θα ενοποιεί όλες τις παραπάνω λειτουργίες δίνοντας έτσι μία συνεκτική και συνεπή εικόνα προς τον τελικό χρήστη.

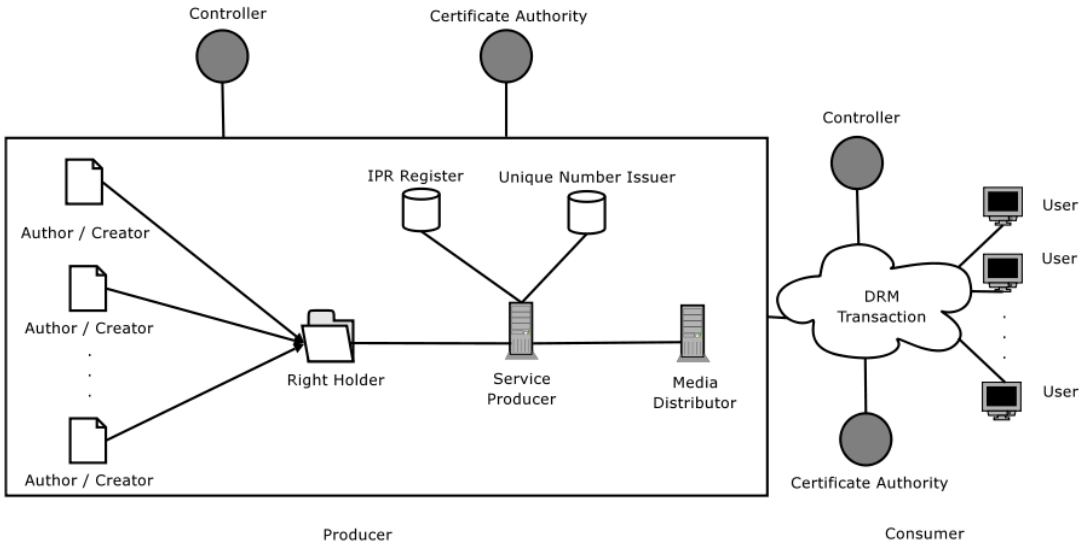
2.5. ΤΑ ΣΥΝΑΛΛΑΣΣΟΜΕΝΑ ΜΕΡΗ ΕΝΟΣ DRM ΣΥΣΤΗΜΑΤΟΣ

Σε ένα DRM σύστημα υπάρχουν πολλοί συναλλασσόμενοι. Στην πιο γενική περίπτωση περιμένουμε να έχουμε τους παρακάτω συναλλασσόμενους.

- Ο δημιουργός του ψηφιακού περιεχομένου. Αυτός μπορεί να είναι ένας άνθρωπος, παρόλα αυτά τίποτα δεν αποκλείει την πιθανότητα δημιουργός του περιεχομένου να είναι μία αυτοματοποιημένη διαδικασία.

- Ο κάτοχος του δικαιώματος αναπαραγωγής. Δεν είναι απαραίτητο ο δημιουργός του περιεχομένου και ο κάτοχος του δικαιώματος αναπαραγωγής να είναι ο ίδιος φορέας.
- Ο πάροχος της υπηρεσίας DRM διανομέας του ψηφιακού περιεχομένου. Είναι αυτός που είναι υπεύθυνος για τη διάθεση του υλικού και την είσπραξη του χρηματικού αντιτίμου. Σε πολλές περιπτώσεις αυτός ο ρόλος εκπληρώνεται από τον πάροχο της υπηρεσίας.
- Ο εξυπηρετητής αδειών χρήσης. Είναι ένας εξυπηρετητής (server) που αντιστοιχεί τα δικαιώματα που έχει κάθε χρήστης σε κάθε ψηφιακό αντικείμενο. Επίσης αναφέρεται και ως μητρώο καταγραφής πνευματικής ιδιοκτησίας.
- Φορέας που υλοποιεί το μηχανισμό ταυτοποίησης του ψηφιακού αντικειμένου.
- Ο ελεγκτής είναι ένα Trusted Third Party ο οποίος επιβεβαιώνει ότι όλες οι συναλλαγές έχουν γίνει νομότυπα.
- Ο φορέας των πιστοποιητικών ταυτότητας. Είναι επίσης ένας TTP ο οποίος διασφαλίζει την πιστοποίηση της ταυτότητας των συμμετεχόντων σε ένα DRM σύστημα.
- Τέλος υπάρχει και ο τελικός χρήστης ο οποίος χρησιμοποιεί την υπηρεσία για την απόκτηση ψηφιακού περιεχομένου.

Σχήμα 2: Εμπλεκόμενοι σε ένα DRM σύστημα

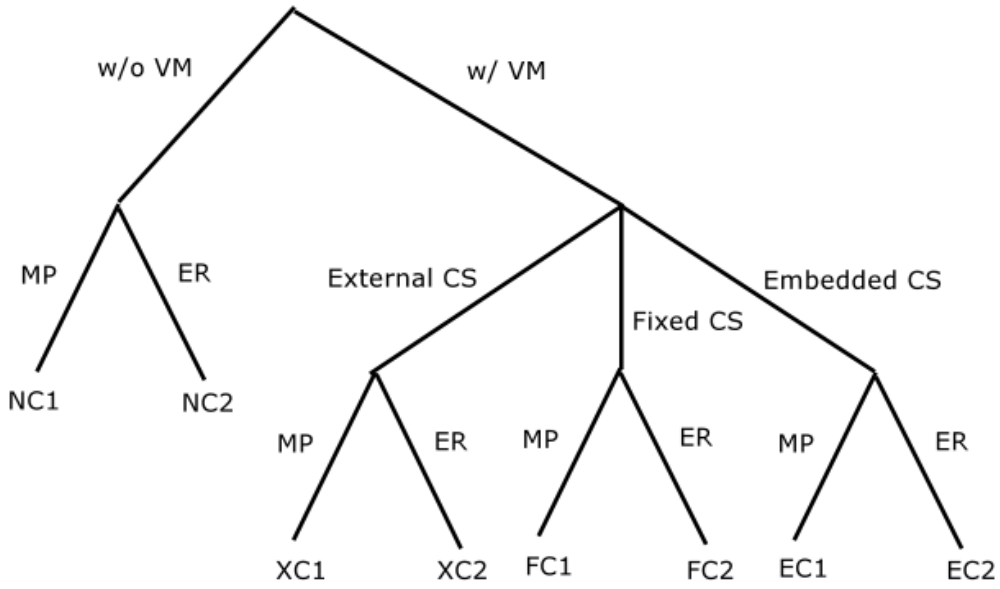


2.6. ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ DRM ΣΥΣΤΗΜΑΤΩΝ

Η ταξινόμηση των DRM συστημάτων γίνεται με βάση τρία κριτήρια.

- Την ύπαρξη ή μη μίας εικονικής μηχανής (virtual machine) σκοπός της οποίας είναι η αναπαραγωγή του ψηφιακού περιεχομένου και η εφαρμογή των κανόνων χρήσης.
- Ο τύπος του συνόλου των κανόνων που ορίζουν τους περιορισμούς στη χρήση του ψηφιακού αντικειμένου
- Το μοντέλο διανομής του ψηφιακού περιεχομένου

Σχήμα 3: Ταξινόμηση DRM συστημάτων



VM: Virtual Machine
MP: Message Push
ER: External Repository
CS: Control Set

NC1: No Control Architecture w/MP
NC2: No Control Architecture w/ER
XC1: External Control Architecture w/MP
XC2: External Control Architecture w/ER
FC1: Fixed Control Architecture w/MP
FC2: Fixed Control Architecture w/ER
EC1: Embedded Control Architecture w/MP
EC2: Embedded Control Architecture w/ER

Η εικονική μηχανή ορίζεται ως λογισμικό το οποίο εκτελείται πάνω σε μία ευάλωτη υπολογιστική πλατφόρμα και χρησιμοποιεί λειτουργίες ελέγχου ώστε να προστατέψει και να διαχειριστεί την πρόσβαση και την χρήση του ψηφιακού περιεχομένου. Μία τέτοια εικονική μηχανή μπορεί να υλοποιηθεί σε διάφορα επίπεδα, από λειτουργία ενσωματωμένη στο λειτουργικό σύστημα ως επιπρόσθετο λογισμικό για κάποιο υπάρχον πρόγραμμα αναπαραγωγής. Είναι προφανές ότι χωρίς την ύπαρξη ενός τέτοιου μηχανισμού δεν είναι δυνατόν να εφαρμοστεί οποιοσδήποτε κανόνας χρήσης του υλικού.

Το σύνολο των κανόνων που περιορίζουν τη χρήση ενός ψηφιακού αντικειμένου συνήθως εκφράζεται με μία γλώσσα έκφρασης δικαιωμάτων. Το πως γίνονται αυτοί διαθέσιμοι στην εικονική μηχανή αναπαραγωγής του ψηφιακού αντικειμένου μας δίνει το επόμενο κριτήριο ταξινόμησης που έχει τρεις κατηγορίες. Πρώτα έχουμε το

σύνολο κανόνων το οποίο είναι αμετάβλητο και είναι ενσωματωμένο στην μηχανή αναπαραγωγής του ψηφιακού αντικειμένου. Το σύνολο αυτών των κανόνων εφαρμόζεται για όλα τα ψηφιακά αντικείμενα που χρησιμοποιούνται σε αυτή την μηχανή αναπαραγωγής και συνήθως είναι αδύνατον ή πολύ δύσκολο να αλλάξουν.

Παράδειγμα τέτοιου συστήματος είναι το Content Scrambling System (CSS) των DVD. Κύριο μειονέκτημα αυτής της μεθόδου είναι η δυσκολία προσαρμογής. Το CSS για παράδειγμα περιείχε σφάλματα υλοποίησης και αποτελέσματα ήταν να παρακαμφτεί μέσα σε λίγους μήνες από την κυκλοφορία του DVD. Επόμενα είναι τα σύνολα κανόνων τα οποία είναι ενσωματωμένα στο ψηφιακό αντικείμενο και τα εξωτερικά του ψηφιακού αντικειμένου σύνολα κανόνων.

Στο πρώτο οι κανόνες είναι μέρος του ψηφιακού αντικειμένου πιθανόν προστατευμένοι κρυπτογραφικά και μπορούν να αλλάζουν για κάθε αντίγραφο που διανέμεται. Τα εξωτερικά σύνολα κανόνων είναι αποθηκευμένα σε δημόσια προσβάσιμους εξυπηρετητές και όταν η μηχανή αναπαραγωγής προσπαθεί να χρησιμοποιήσει ένα προστατευμένο ψηφιακό αντικείμενο πρέπει να συνδεθεί με αυτόν και να ελέγξει τους κανόνες για να κρίνει αν είναι εξουσιοδοτημένη η χρήση του ψηφιακού αντικειμένου.

Η μέθοδος διανομής είναι το τελευταίο κριτήριο ταξινόμησης. Ο διαχωρισμός γίνεται σε δημόσια προσβάσιμα εξωτερικά αποθετήρια και σε μεθόδους διανομής με προώθηση του ψηφιακού περιεχομένου στο χρήστη. Στο πρώτο ο χρήστης δεν είναι αναγκαίο να έχει τοπικά αντίγραφο του ψηφιακού αντικειμένου αλλά μπορεί να έχει πρόσβαση σε αυτό όποτε το απαιτήσει. Στη δεύτερη μέθοδο ο διανομέας πρέπει να προωθήσει το ψηφιακό αντικείμενο στον χρήστη έχοντας έτσι πιο καλό έλεγχο του ποιος το λαμβάνει.

2.7. ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΕΝΟΣ DRM ΣΥΣΤΗΜΑΤΟΣ.

Αν και στην αλυσίδα ενός DRM συστήματος εμπλέκονται πολλοί συναλλασσόμενοι οι οποίοι έχουν διαφορετικά κριτήρια αξιολόγησης του συστήματος όλοι ενδιαφέρονται στα ακόλουθα χαρακτηριστικά του συστήματος.

- Φιλικότητα προς το χρήστη. Είναι απαραίτητη για την προσέλκυση των τελικών χρηστών. Αν μία υπηρεσία είναι δύσχρηστη δεν θα έχει και εμπορική επιτυχία.
- Αξιοπιστία του συστήματος. Ο τελικός χρήστης πρέπει να εμπιστεύεται το σύστημα ότι τα δικαιώματα που έχει θα μπορούν να εφαρμοστούν ανεξάρτητα αντίξοων συνθηκών. Από την άλλη ο ιδιοκτήτης του ψηφιακού αντικειμένου πρέπει να είναι βέβαιος ότι δεν θα διαρρεύσει απροστάτευτο περιεχόμενο από το σύστημα.
- Ασφάλεια. Η ασφάλεια και το αδιάβλητο του DRM συστήματος είναι σημαντική αφού αυτό διαχειρίζεται αντικείμενα οικονομικής αξίας, όπως το ψηφιακό περιεχόμενο και τις χρηματικές συναλλαγές των συμβαλλομένων. Έχει αποδειχτεί ότι κανένα υπάρχον σύστημα δεν είναι 100% ασφαλές. Παρ' ότι αυτό είναι ευρύτερα γνωστό γίνεται αποδεκτό από τους μετέχοντες στο DRM σύστημα αφού η απόλυτη ασφάλεια είναι τεχνικά εφικτή αλλά οικονομικά ασύμφορη και επίσης μειώνει την φιλικότητα προς το χρήστη, πράγμα που επίσης έχει οικονομικό αντίκτυπο.
- Επεκτασιμότητα και ελαστικότητα. Η online διανομή ψηφιακού περιεχομένου είναι σχετικά νέα και βασίζεται ακόμα σε ήδη υπάρχοντα επιχειρηματικά μοντέλα όπως η συνδρομή και η πληρωμή επί τη προβολή (pay per view). Το πιο πιθανό είναι ότι στο μέλλον θα δούμε νέα επιχειρηματικά μοντέλα για τη διανομή ψηφιακού περιεχομένου. Ένα σύστημα DRM πρέπει να είναι ικανό να προσαρμοστεί σε αυτά τα μελλοντικά μοντέλα. Επίσης ένα DRM σύστημα πρέπει να είναι ικανό να ανταπεξέλθει στην αύξηση του όγκου δεδομένων που διαχειρίζεται αφού κάτι τέτοιο είναι αναμενόμενο και επιθυμητό για το μέλλον.
- Εφικτότητα υλοποίησης. Ειδικά οι κατασκευαστές ηλεκτρονικών συσκευών (hardware) έχουν ιδιαίτερο ενδιαφέρον να γνωρίζουν κατά πόσο είναι εφικτή η υλοποίηση ενός DRM συστήματος. Ανάλογα με τις απαιτήσεις της εφαρμογής αυξάνονται και οι απαιτήσεις από τις συσκευές. Πόση μνήμη RAM απαιτείται, πόση επεξεργαστική ισχύ, τι ιδιαίτερα χαρακτηριστικά απαιτούνται (πχ tamper proof memory). Επίσης η απαίτηση για δυνατότητα δικτύωσης και σύνδεσης σε απομακρυσμένα μηχανήματα μπορεί να

περιορίσει σημαντικά τη χρηστικότητα DRM enabled ηλεκτρονικών συσκευών.

- Διαλειτουργικότητα. Για να αποκτήσει ένα σύστημα DRM ευρεία χρήση πρέπει να είναι ικανοποιητικά διαλειτουργικό. Αν για παράδειγμα κάποιος αγοράσει ένα mp3 αρχείο για αναπαραγωγή σε μία φορητή συσκευή θα μπορεί να το αναπαράγει σε μία άλλου τύπου φορητή συσκευή ή στον υπολογιστή στο σπίτι του; Αν ναι τι βήματα θα απαιτούνται ώστε να γίνει αυτό και πόσο εύχρηστα και λειτουργικά θα είναι αυτά. Προσπάθειες τυποποίησης όπως αυτές του MPEG-21 ορίζουν ένα πρότυπο διαλειτουργικότητας χωρίς να περιγράφουν ή να περιορίζουν το συνολικό σύστημα DRM. Μία άλλη όψη της διαλειτουργικότητας είναι η δυνατότητα αναβαθμίσεων χωρίς να βλάπτεται η προς τα πίσω συμβατότητα. Πρέπει δηλαδή μετά από μία αναβάθμιση του λογισμικού της εφαρμογής ότι ψηφιακό περιεχόμενο ήταν διαθέσιμο πριν από αυτή να είναι και μετά την αναβάθμιση.
- Οικονομικό κόστος του DRM συστήματος. Το κόστος αυτό απαρτίζεται από τα εξής επί μέρους κόστη: Κόστος αδειών χρήσης για την τεχνολογία που απαιτείται για τις διαδικασίες που απαιτούνται από τον πάροχο του περιεχομένου, τον πάροχο του συστήματος πληρωμής,του κατασκευαστή των συσκευών που θα χρησιμοποιήσει ο τελικός χρήστης. Το κόστος της υλοποίησης και ενοποίησης της τεχνολογίας που απαιτείται ώστε όλοι οι εμπλεκόμενοι να μπορούν να συμμετάσχουν στο DRM σύστημα. Είναι σημαντικό αυτά τα κόστη να κρατηθούν όσο το δυνατόν χαμηλότερα αφού τελικά αυτά θα επιβαρύνουν τον τελικό χρήστη. Πρέπει λοιπόν το σύστημα DRM να διασφαλίζει χαμηλότερη τελική τιμή από παραδοσιακά μέσα διανομής ή να προσφέρει νέα ελκυστικά χαρακτηριστικά ώστε να προτιμηθεί από τον τελικό χρήστη.

ΚΕΦΑΛΑΙΟ 3:
ΤΕΧΝΟΛΟΓΙΚΑ ΜΕΣΑ ΠΡΟΣΤΑΣΙΑΣ.

ΚΕΦΑΛΑΙΟ 3

3. ΤΕΧΝΟΛΟΓΙΚΑ ΜΕΣΑ ΠΡΟΣΤΑΣΙΑΣ.

3.1. ΕΙΣΑΓΩΓΙΚΑ ΣΤΟΙΧΕΙΑ

Σε προηγούμενες αναφορές της εργασίας δόθηκε ιδιαίτερη βαρύτητα στην νομική πλευρά της προστασίας και διαχείρισης των ψηφιακών δικαιωμάτων. Στο παρόν κεφάλαιο θα αναπτυχθούν οι τεχνολογίες που χρησιμοποιούνται για τον συγκεκριμένο σκοπό καθώς και τα σημαντικότερα συστήματα που αξιοποιούν αυτές τις τεχνολογικές λύσεις.

Τα τεχνολογικά μέσα προστασίας όπως προκύπτουν από τις ενδεδειγμένες πρακτικές και τα προγράμματα συνοψίζονται παρακάτω:

- Ασφάλεια και ακεραιότητα των λειτουργικών συστημάτων των ηλεκτρονικών υπολογιστών: Περιλαμβάνονται και παραδοσιακές μέθοδοι ελέγχου της πρόσβασης σε αρχεία, πιστοποίησης χρηστών, παροχής δικαιωμάτων κ.α.
- Κρυπτογραφία: Επιτρέπει την κρυπτογράφηση του ψηφιακού περιεχομένου, ώστε η αποκρυπτογράφηση του να είναι δυνατή μόνο από τους νόμιμους χρήστες.
- Εξακολουθιτική κρυπτογραφηση: Επιτρέπει στον καταναλωτή να χρησιμοποιεί την πληροφορία όσο το σύστημα τη διατηρεί σε κρυπτογραφημένη μορφή.
- Υδατογραφία ή απόκρυψη δεδομένων (data hiding): Ενσωματώνει πληροφορία (π.χ. σχετικά με τον κάτοχο του δικαιώματος αναπαραγωγής) σε ένα ψηφιακό αρχείο. Ένα ψηφιακό υδατογράφημα βοηθά τους ιδιοκτήτες πνευματικών δικαιωμάτων να ανιχνεύουν τη μη-εξουσιοδοτημένη χρήση, αντιγραφή και διανομή των ψηφιακών δεδομένων.

- Έμπιστα (trusted) συστήματα: Σε μία εκδοχή της μελλοντικής εξέλιξης της επιστήμης της πληροφορικής, η ασφάλεια θα έχει σημαντική θέση στο σχεδιασμό των υπολογιστικών συστημάτων, οδηγώντας στην εκτεταμένη υιοθέτηση συστημάτων προστασίας και ελέγχου της Πνευματικής Ιδιοκτησίας με την αξιοποίηση εξειδικευμένου υλικού και λογισμικού. Τα «έμπιστα» αυτά συστήματα συνθέτουν ένα ανοικτό πεδίο έρευνας.

Κατά πόσο ένα τεχνολογικό μέσο προστασίας είναι αποδοτικό εξαρτάται από την τεχνολογική του πληρότητα, το περιεχόμενο που προστατεύει και την επιχείρηση (ή τομέα) στην οποία είναι εγκατεστημένο.

Τα κυριότερα χαρακτηριστικά του είναι:

- Ευχρηστία: Ένα δύσχρηστο μέσο προστασίας αυτόματα αποθαρρύνει την ευρεία χρήση του.
- Καταλληλότητα ως προς το περιεχόμενο: Το κόστος του σχεδιασμού, της ανάπτυξης και εγκατάστασης του συστήματος πρέπει να είναι σε αρμονία με τον τύπο του περιεχομένου. Για χαμηλού κόστους περιεχόμενο το οποίο ήδη διατίθεται σε λογική τιμή με αναλογικά μέσα (όχι μέσω του Διαδικτύου), δεν υπάρχει λόγος υλοποίησης ενός υψηλού κόστους συστήματος προστασίας το οποίο θα αυξήσει την τιμή της διάθεσης του περιεχόμενου μέσω του Διαδικτύου.
- Καταλληλότητα ως προς την απειλή: Η αποτροπή των έντιμων καταναλωτών (παραβατών χωρίς πρόθεση) από το να διαμοιράζουν μικρού αριθμού αντίγραφα ενός προϊόντος, μπορεί να απαιτεί μόνο ένα λογικά τιμολογημένο ψηφιακό προϊόν, ένα καλό σύστημα διάθεσης και ένα σαφώς καθορισμένο σύνολο οδηγιών. Η αποτροπή της ηλεκτρονικής σύλησης εξαιρετικά πολύτιμου υλικού, το οποίο πρέπει να υπάρχει σε δίκτυο ηλεκτρονικών υπολογιστών, απαιτεί ένα πολύπλοκο μηχανισμό προστασίας και ακόμα και η καλύτερη διαθέσιμη τεχνολογία ίσως να μην αρκεί για την προστασία του.
- Ανάλυση κόστους – οφέλους: Μία πολύπλοκη αλλά απαραίτητη μελέτη που θα πρέπει πάντα να προηγείται των όποιων αποφάσεων.

3.2. ΑΣΦΑΛΕΙΑ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Λειτουργικό σύστημα ή ΛΣ (αγγλ. Operating System ή OS) είναι το λογισμικό του υπολογιστή που είναι υπεύθυνο για την διαχείριση και τον συντονισμό των εργασιών και την κατανομή των διαθέσιμων πόρων. Το λειτουργικό σύστημα παρέχει ένα θεμέλιο, ένα μεσολαβητικό επίπεδο λογικής διασύνδεσης μεταξύ λογισμικού και υλικού, διαμέσου του οποίου οι εφαρμογές αντιλαμβάνονται εμμέσως τον υπολογιστή. Μια από τις κεντρικές αρμοδιότητες του λειτουργικού συστήματος είναι η διαχείριση του υλικού, απαλλάσσοντας έτσι τις εφαρμογές από τον άμεσο και επίπονο χειρισμό του τελευταίου και καθιστώντας ευκολότερο τον προγραμματισμό τους. Σχεδόν όλοι οι υπολογιστές χρησιμοποιούν έναν τύπο λειτουργικού συστήματος. Έτσι ένα αποτελεσματικό σύστημα προστασίας ψηφιακού περιεχομένου πρέπει να έχει ένα λειτουργικό σύστημα που να του προσφέρει ασφάλεια.

Από τα περισσότερα λειτουργικά συστήματα χρησιμοποιούνται οι Πυρότοιχοι οι οποίοι παρέχουν ένα τοίχο προστασίας του ψηφιακού περιεχομένου και αποτρέπουν την εισαγωγή επικίνδυνων προγραμμάτων στο διαδίκτυο. Ακόμα υπάρχουν αρκετοί μηχανισμοί ελέγχου πρόσβασης και πιστοποίησης περιεχομένου. Είναι πολύ σημαντικό λοιπόν ένα αποδοτικό τεχνολογικό σύστημα πνευματικών δικαιωμάτων πρέπει να διασφαλίζει την ασφάλεια και την ακεραιότητα του λειτουργικού του συστήματος.

3.3. ΤΕΧΝΟΛΟΓΙΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

3.3.1. ΚΡΥΠΤΟΓΡΑΦΗΣΗ: ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» ήταν μια ξύλινη ράβδος ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση. Η Κρητική εικονογραφική γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με τη γραμμική γραφή Α χρονικά και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού που ανακαλύφθηκε το 1908 στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων καθιστώντας το Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους απαιτεί μεγάλο αριθμό προσωπικού το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα, ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.Οι Γερμανοί έκαναν εκτενή χρήση ενός συστήματος γνωστού ως "Enigma".

Η τρίτη περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας.

3.3.1.1. ΚΑΤΗΓΟΡΙΕΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ

Η κρυπτογράφηση χωρίζεται σε δύο βασικές κατηγορίες : την συμμετρική και την ασύμμετρη κρυπτογράφηση. Το σύνολο των διαθέσιμων κρυπτογραφικών αλγόριθμων μπορεί να κατηγοριοποιηθεί με αρκετά διαφορετικά κριτήρια. Η κατηγοριοποίηση που ακολουθεί βασίζεται στον αριθμό των κλειδιών που χρησιμοποιούνται για την κωδικοποίηση και την αποκωδικοποίηση. Οι τρεις κατηγορίες κρυπτογραφικών αλγόριθμών που θα παρουσιαστούν είναι:

- Κρυπτογράφηση Μυστικού Κλειδιού: Όπου χρησιμοποιείται ένα μοναδικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση
- Κρυπτογράφηση Δημόσιου Κλειδιού: Όπου χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση
- Μονόδρομες συναρτήσεις σύνοψης: Όπου χρησιμοποιούνται μαθηματικοί μετασχηματισμοί για την αμετάκλητη κρυπτογράφηση της πληροφορίας

3.3.1.2. ΑΛΓΟΡΙΘΜΟΙ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Στους συμμετρικούς αλγόριθμους (ή αλγόριθμους μυστικού κλειδιού) το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες: α) αλγόριθμοι ροής (stream ciphers) οι οποίοι λειτουργούν bit προς bit και β) μπλοκ αλγόριθμοι (block ciphers) οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit).

Από τους πιο γνωστούς Stream Ciphers είναι οι :

- RC4 : δημιουργήθηκε από τον Ron Rivest για λογαριασμό της RSA. Έχει μεταβλητό μήκος κλειδιού αλλά λειτουργεί σε επίπεδο byte,θεωρείται εξαιρετικά ασφαλής και ταχύς και είναι ο ευρύτερα χρησιμοποιούμενος.
- A5 : είναι ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση GSM επικοινωνιών, είναι ένα stream cipher.
- SEAL (Software-optimized Encryption Algorithm) : Τα δεδομένα κρυπτογραφούνται ένα bit τη φορά και χρησιμοποιεί κλειδί 160 bit.

Από τους πιο γνωστούς block ciphers είναι οι :

- DES (Data Encryption Standard): είναι ίσως ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος κρυπτογράφησης, βασίζεται στον αυγερινό αλγόριθμο και κρυπτογραφεί ανα τμήματα 64 bit χρησιμοποιώντας κλειδί 56 bit.

Παραλλαγές του είναι οι αλγόριθμοι:

- Triple-DES, διαφέρει από τον απλό DES ως προς το ότι κρυπτογραφεί το κείμενο τρεις φορές, χρησιμοποιώντας διαφορετικό κλειδί για την κάθε φορά.
- DESX (=X-OR) στο οποίο η είσοδος της κρυπτογράφησης και η έξοδος της αποκρυπτογράφησης περνάει από μια X-OR (exclusive or – x-disjunction) πράξη με ένα επιπλέον κλειδί 64 bit και έτσι αυξάνεται η αντοχή του αλγορίθμου σε επιθέσεις.
- AES (Advanced Encryption Standard): πρόκειται για επέκταση του αλγορίθμου DES. Κρυπτογραφεί block 128 bit και έχει κλείδα 128, 192 ή 256 bit.
- IDEA (International Data Encryption Algorithm : είναι μια συμμετρική κρυπτογράφηση αναπτύχθηκε το 1990 και χρησιμοποιεί 128-bit κλειδιά.
- Blowfish: κατασκευάστηκε από τον Schneier. Κρυπτογραφεί τμήματα 64 bit και έχει μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Επίσης είναι ταχύτερος του DES.
- RC2 με μεταβλητό μήκος κλειδιού και RC5 με μεταβλητό μήκος κλειδιού, μέγεθος block και αριθμό επαναλήψεων. Δημιουργήθηκαν από τον Ron Rivest.

3.3.1.3. ΑΛΓΟΡΙΘΜΟΙ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρη κρυπτογράφηση (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της συμμετρικής κρυπτογράφησης , αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

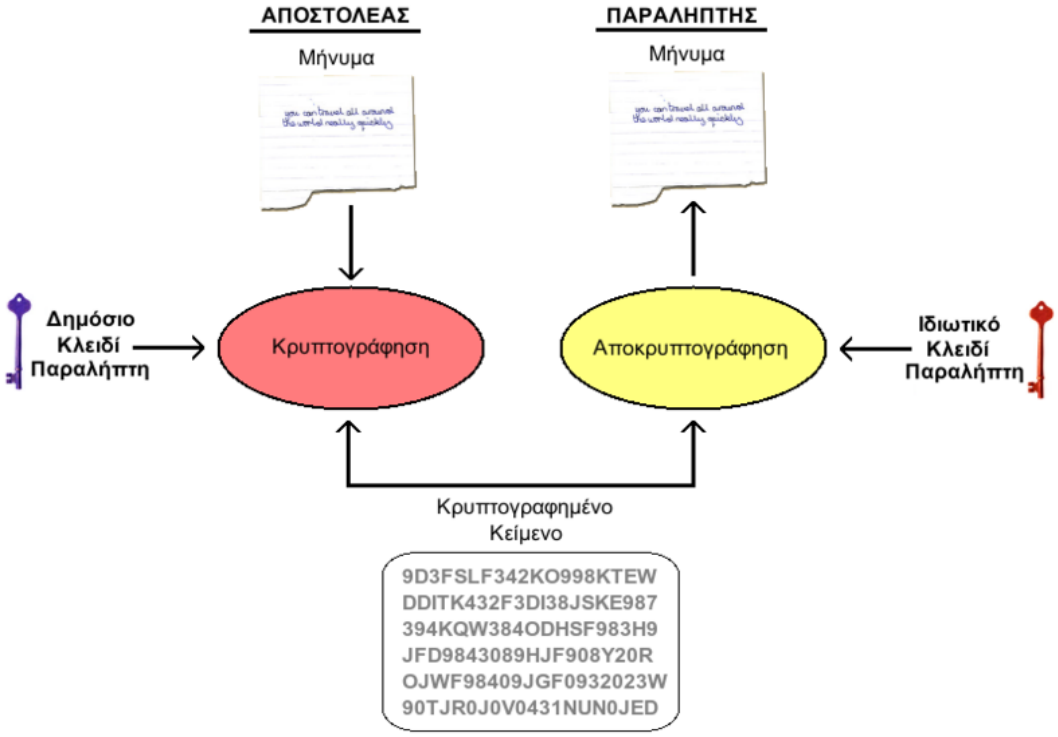
Ένα δημόσιο κλειδί 1024 bits το οποίο αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων.

Χαρακτηριστικά των ασύμμετρων αλγορίθμων είναι τα ακόλουθα:

- Εμπιστευτικότητα

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημενο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στην συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.

Σχήμα 1: Κινήσεις των ασύμμετρων αλγορίθμων



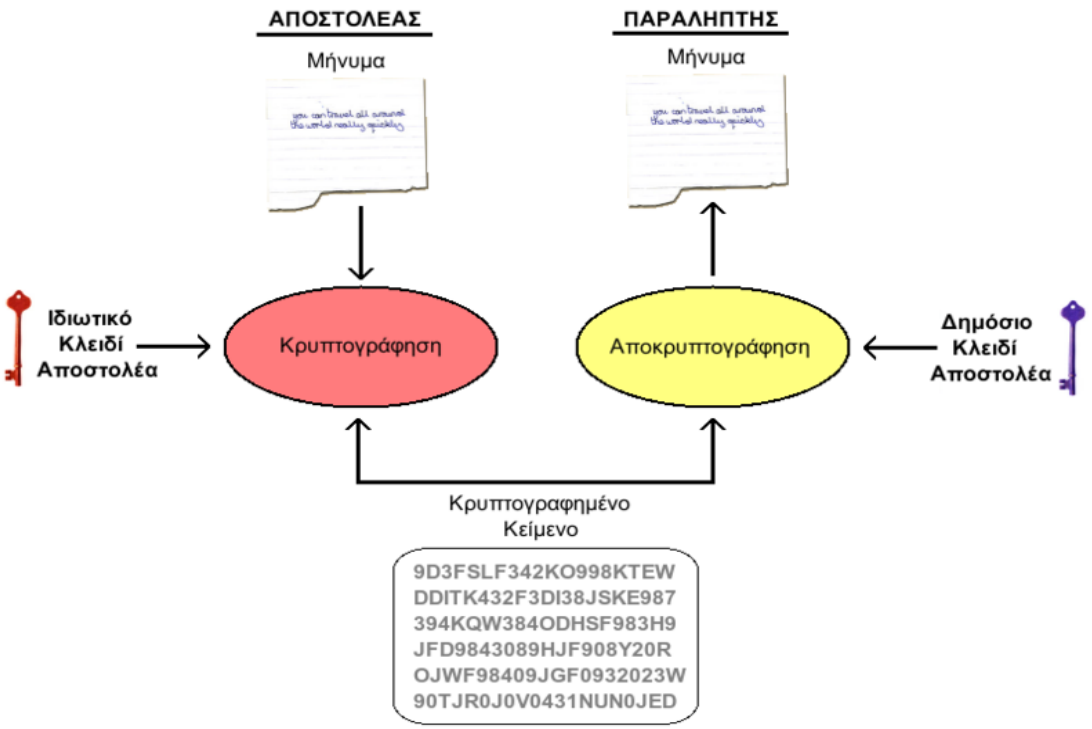
Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα. Αυτό με λίγα λόγια σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

- Πιστοποίηση

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στην συνέχεια στέλνει το μήνυμα στον παραλήπτη

και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.

Σχήμα 2: Κινήσεις των ασύμμετρων αλγορίθμων



Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη την διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

- Εμπιστευτικότητα και Πιστοποίηση

Συνδυάζοντας τις δύο τεχνικές που παρουσιάστηκαν παραπάνω είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και τον

παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στην συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στην συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση). Βέβαια αυτό που γίνεται συνήθως είναι ο αποστολέας να υπογράφει ψηφιακά το μήνυμά του και στην συνέχεια να το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί θα πρέπει να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους αλγόριθμους συμμετρικής κρυπτογράφησης.. Συγκεκριμένα, οι αλγόριθμοι συμμετρικής κρυπτογράφησης χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος.
Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης

στον παραλήπτη για να μπορέσει αυτός με την σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

Παραδείγματα ασύμμετρων αλγορίθμων είναι οι :

- RSA: (Ron Rivest - Adi Shamir – Leonard Adleman) ονομάστηκε έτσι από τα αρχικά των δημιουργών του (οι οποίοι αναφέρονται στις παρενθέσεις) και αναπτύχθηκε το 1977 είναι ο κυριότερος και ευρύτερα χρησιμοποιούμενος αλγόριθμος ασύμμετρης κρυπτογράφησης. Χρησιμεύει και για την κρυπτογράφηση δημόσιου κλειδιού αλλά και για την δημιουργία ψηφιακής υπογραφής. Το σύστημα αυτό χρησιμοποιεί μεγάλου μεγέθους κλειδιά (από 512 έως 1024 bit) τα οποία προκύπτουν ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς p, q και υπολογίζουμε το γινόμενο τους n = pq. Το n καλείται modulus. Διαλέγουμε ένα αριθμό e μικρότερο του n και τέτοιο, ώστε e και (p-1)(q-1) να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό d, ώστε (ed-1) να διαιρείται από το (p-1)(q-1). Τα ζευγάρια (n,e) και (n,d) καλούνται δημόσιο και ιδιωτικό κλειδί, αντίστοιχα.
- ECC (Elliptic curve cryptography): θεωρείται ο ισχυρότερος αλγόριθμος σε δεδομένο μήκος κλείδας με ελάχιστες απαιτήσεις σε μήκος κλειδιού 160 bit όπως καθορίζουν το NIST (National Institute of Standards and Technology) και το ANSI (American National Standards Institute) X9 την στιγμή που για τον RSA και τον DSA ορίζουν ως ελάχιστο μήκος κλείδας τα 1024 bit.
- DSA (Digital Signature Algorithm) και DSS (Digital Signature Standard): Από τον NIST προβάλλεται το πρότυπο DSS το οποίο χρησιμοποιεί τον αλγόριθμο DSA για την παραγωγή ψηφιακών υπογραφών.

Οι συμμετρικοί αλγόριθμοι είναι πολύ πιο γρήγοροι, εφαρμοσμένοι είτε σε υλικό είτε σε λογισμικό. από τους ασύμμετρους αλγόριθμους. Ως εκ τούτου οι συμμετρικοί

αλγόριθμοι χρησιμοποιούνται για την κρυπτογράφηση του κυρίου μέρους των δεδομένων, ενώ οι αλγόριθμοι δημόσιου κλειδιού βρίσκουν κατάλληλη εφαρμογή σε πρωτόκολλα ανταλλαγής κλειδιών και ψηφιακών υπογραφών.

3.3.1.4. ΜΟΝΟΔΡΟΜΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΣΥΝΟΨΗΣ

Οι μονόδρομες συναρτήσεις σύνοψης (one-way hash functions) αποτελούν θεμελιώδη στοιχεία για την ανάπτυξη των περισσότερων πρωτοκόλλων κρυπτογράφησης. Οι συναρτήσεις σύνοψης είναι συναρτήσεις οι οποίες δέχονται σαν είσοδο μια ακολουθία χαρακτήρων μεταβλητού μήκους και παράγουν ένα μήνυμα σταθερού μεγέθους (γενικά μικρότερο) που ονομάζεται τιμή σύνοψης (hash value). Οι μονόδρομες συναρτήσεις σύνοψης είναι συναρτήσεις οι οποίες δουλεύουν μόνο προς την μία κατεύθυνση: είναι εύκολο να υπολογιστεί μια τιμή σύνοψης για κάποιο δεδομένο μήνυμα αλλά είναι αδύνατο να υπολογιστεί το μήνυμα στο οποίο αντιστοιχεί μια συγκεκριμένη τιμή σύνοψης. Μία καλά σχεδιασμένη μονόδρομη συνάρτηση σύνοψης είναι επίσης ελεύθερη από συγκρούσεις (collision-free) δηλαδή είναι δύσκολο να βρεθούν δύο μηνύματα που δίνουν την ίδια τιμή σύνοψης.
Οι μονόδρομες συναρτήσεις σύνοψης χρησιμοποιούνται κυρίως για εφαρμογές επαλήθευσης. Η τιμή σύνοψης αντιστοιχεί πλήρως, και αντιπροσωπεύει το αρχικό μήνυμα. Η αλλαγή έστω και ενός bit στο αρχικό μήνυμα αλλάζει κατά μέσο όρο τα μισά bits της τιμής σύνοψης.

Οι κώδικες πιστοποίησης μηνυμάτων (Message authentication codes, MACs) είναι μονόδρομες συναρτήσεις σύνοψης οι οποίες βασίζονται σε μυστικό κλειδί έτσι ώστε μόνο κάποιος που γνωρίζει το κλειδί αυτό μπορεί να επιβεβαιώσει την τιμή σύνοψης. Είναι πολύ χρήσιμοι για να παρέχουν αυθεντικότητα. Μία μονόδρομη συνάρτηση σύνοψης μπορεί να μετατραπεί σε κώδικα πιστοποίησης αν η τιμή σύνοψης κρυπτογραφηθεί με ένα συμμετρικό αλγόριθμο.

Παραδείγματα μονόδρομων συναρτήσεων σύνοψης είναι οι :

- MD2, MD4, MD5 (Message Digest): Πρόκειται για Hash Function αλγορίθμους που αναπτύχθηκαν από τον Ron Rivest και χρησιμοποιούνται κυρίως για την παραγωγή ψηφιακών υπογραφών. Οι αλγόριθμοι αυτοί δέχονται ένα μήνυμα αυθαίρετου μήκους και εξάγουν ένα Message Digest 128 bits. Εν συνεχεία η σύνοψη αυτή του μηνύματος κρυπτογραφείται με την ιδιωτική κλείδα του αποστολέα. Μοιάζουν και οι τρεις αρκετά με την διαφορά αφ' ενός ότι πρόκειται για διαδοχικές βελτιώσεις και αφ' ετέρου ότι ο MD2 έχει σχεδιαστεί για 8 bit μηχανές ενώ οι MD4 και MD5 για μηχανές 32 bit.
- SHA – SHA-1 (Secure Hash Algorithm): Ο SHA-1 αποτελεί επανέκδοση του SHA και διόρθωνε μια ατέλεια του τελευταίου. Η δομή και η λειτουργία του είναι παρόμοια με την αντίστοιχη του MD4. Ο SHA-1 παίρνει ως είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει message digest 160 bits. Είναι ελαφρά πιο αργός από τον MD5, αλλά το μεγαλύτερο message digest που παράγει τον κάνουν πιο ασφαλή απέναντι σε προσπάθειες αντιστροφής του.
- RIPEMD - : αναπτύχθηκε στην Ευρώπη από τους Hans Dobbertin, Antoon Bosselaers, και Bart Preneel και υπάρχει σε εκδόσεις των 128, 160, 256 και 320 bit εκ των οποίων παίρνει και την αντίστοιχη ονομασία κάθε φορά.

3.3.1.5. ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΟΥ

Η διαχείριση του κλειδιού είναι η διαδικασία παραγωγής, διανομής, επαλήθευσης, χρησιμοποίησης, ενημέρωσης, αποθήκευσης και καταστροφής κλειδιών σε ένα σύστημα κρυπτογράφησης. Η ασφαλής μέθοδος διαχείρισης των κλειδιών είναι πάρα πολύ σημαντική. Στην πράξη οι περισσότερες επιθέσεις σε συστήματα ασφαλείας έχουν ως στόχο τις διαδικασίες διαχείρισης των κλειδιών και όχι τους ίδιους τους αλγόριθμους.

Οι αλγόριθμοι δημόσιου κλειδιού καθιστούν την διαχείριση πολύ πιο εύκολη. Το ιδιωτικό κλειδί δεν χρειάζεται να μεταδοθεί ποτέ. Βέβαια παρουσιάζεται ένα πρόβλημα ο κάθε χρήστης πρέπει να διαθέτει ένα δικό τους ζεύγος κλειδιών. Στα συστήματα που χρησιμοποιούν ασύμμετρη κρυπτογραφία χρειάζονται μέθοδοι

διανομής και επαλήθευσης κλειδιών. Τα πρωτόκολλα CCITT X.509 παρέχουν κανόνες για τις διαδικασίες αυτές.

3.3.1.6. ΠΡΩΤΟΚΟΛΛΑ

Ένα πρωτόκολλο είναι μια σειρά κανόνων που πρέπει να ακολουθηθούν για την εκτέλεση μιας δεδομένης εργασίας. Τα πρωτόκολλα ασφάλειας δεδομένων συχνά περιέχουν την χρήση κάποιων αλγορίθμων κρυπτογράφησης αλλά σε γενικές γραμμές αυτό που προσπαθούν να επιτύχουν δεν είναι μόνο η μυστικότητα αλλά και να παρέχουν όλες τις βασικές υπηρεσίες ασφαλείας που αναφέρθηκαν.

3.3.2. ΣΤΕΓΑΝΟΓΡΑΦΙΑ

3.3.2.1. ΙΣΤΟΡΙΚΑ ΣΤΟΙΧΕΙΑ

Σε όλη τη διαδρομή της ιστορίας ο άνθρωπος συνεχώς ανακάλυπτε νέες μεθόδους που του επέτρεπαν να κρύψει κάποια πολύτιμη πληροφορία. Ένα από τα πρώτα κείμενα που περιγράφουν τη στεγανογραφία έρχεται από τον Ηρόδοτο. Στην αρχαία Ελλάδα τα κείμενα γράφονταν σε πίνακες καλυμμένους με κερί. Σε μια αφήγηση ιστορικού γεγονότος αναφέρεται ότι ο Δημάρατος ήθελε να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης προτίθετο να εισβάλει στην Ελλάδα. Για να αποφύγει την κλοπή του μηνύματος έγραψε το μήνυμά του σε ξύλινη πινακίδα, αφού έξυσε το κερί που αυτή είχε και την οποία μετά κάλυψε πάλι με κερί. Οι πινακίδες φαίνονταν λευκές και αχρησιμοποίητες και με αυτό το τρόπο πέρασαν κάθε έλεγχο.

Ακόμα μία μέθοδος ήταν το ξύρισμα του κεφαλιού του αγγελιοφόρου και το γράψιμο του μηνύματος στο κεφάλι του. Όταν πια τα μαλλιά μεγάλωναν αρκετά το μήνυμα δεν φαινόταν έως ότου το κεφάλι ξαναξυριζόταν.

Μια άλλη κοινή μορφή αόρατης γραφής επιτυγχάνεται με τη χρήση αόρατου μελανιού. Τέτοιου είδους μελάνια χρησιμοποιήθηκαν με επιτυχία μέχρι και στο δεύτερο παγκόσμιο πόλεμο. Ένα αθώο κατά τα φαινόμενα γράμμα μπορεί να περιέχει ένα πολύ διαφορετικό μήνυμα γραμμένο ανάμεσα στις γραμμές που φαίνονται. Την εποχή του δευτέρου παγκοσμίου πολέμου η τεχνολογία της στενογραφίας αποτελείτο

κυρίως από αόρατα μελάνια. Η προέλευση αυτών των μελανιών είναι το γάλα, διάφορα φρούτα, το ξίδι και τα ούρα. Όλα τα παραπάνω συστατικά σκουραίνουν όταν θερμαίνονται και αυτό τους το χαρακτηριστικό εκμεταλλεύτηκε η κρυπτογραφία της εποχής. Με την ανάπτυξη της τεχνολογίας αναπτύχθηκαν νέα, χημικά, υλικά που κάνανε ακριβώς το ίδιο πράγμα αλλά ήθελαν συγκεκριμένη διαδικασία για να εμφανίσουν αυτά που κρύβανε.

Άλλη μέθοδος είναι αυτή των "Null ciphers" μη κρυπτογραφημένων μηνυμάτων. Υπήρχε τότε, όπως και σήμερα, η τεχνική της ανίχνευσης υπόπτων μηνυμάτων μέσω κάποιων ειδικών φίλτρων μιας αυτοματοποιημένης διαδικασίας. Ωστόσο, τα αθώα μηνύματα περνούσαν ανενόχλητα. Το μόνο λοιπόν που είχε να κάνει κάποιος που ήθελε να στείλει κάποια κρυφή πληροφορία ήταν να την κάνει να φαίνεται αθώα. Έτσι έγραφε ένα τυχαίο κείμενο στο οποίο η πληροφορία βρισκόταν σε κάθε δεύτερο, για παράδειγμα, γράμμα των λέξεων του κειμένου.

Καθώς, όμως η τεχνολογία συνέχισε να αναπτύσσεται, βρέθηκαν τρόποι διακίνησης μεγαλύτερου όγκου πληροφορίας με ακόμα πιο αόρατο τρόπο. Οι Γερμανοί ανέπτυξαν τη τεχνολογία των μικροτελειών (microdots). Οι μικροτελείες είναι φωτογραφίες υψηλής ανάλυσης και ασήμαντου μεγέθους □τελείες. Αυτό τ
χρησιμοποιήθηκε από Γερμανούς κατασκόπους κατά τον δεύτερο παγκόσμιο πόλεμο.

3.3.2.2. ΟΡΙΣΜΟΣ

Όπως καταλαβαίνουμε και από το όνομά της, η στεγανογραφία είναι η τέχνη, που στις μέρες μας έχει εξελιχθεί και σε τεχνική, της επικοινωνίας κατά τρόπο τέτοιο που να κρύβεται η ίδια η ύπαρξη της επικοινωνίας. Σε αντίθεση με τη κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει τη πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Στον παρακάτω πίνακα, που έχει συνταχθεί από τον David Kahn βλέπουμε τις διαφορές της στεγανογραφίας από τη κρυπτογραφία σε σχέση πάντα με τις μεθόδους και τους τύπους που η καθεμία χρησιμοποιεί. Εδώ με τον όρο "ασφάλεια"

περιγράφουμε τις μεθόδους προστασίας των πληροφοριών ενώ με τον όρο "ανάκτηση" τις μεθόδους ανάκτησής τους.

Πίνακας 1: Διαφορές της στενογραφίας από την κρυπτογραφία

Ασφάλεια Σήματος	**Ασφάλεια Ανάκτησης**
Ασφάλεια επικοινωνιών	**Ανάκτηση Επικοινωνιών**
• Στεγανογραφία (αόρατα μελάνια, ανοικτοί κώδικες, μηνύματα σε "τρύπια τακούνια") και Ασφάλεια Εκπομπής (συστήματα εκπομπής ευρέως φάσματος)	• Παρεμβολή και Ανίχνευση κατεύθυνσης
• Κρυπτογραφία	• Κρυπτανάλυση
• Ασφάλεια κίνησης (σιγή ασυρμάτου, "χαζά" μηνύματα)	• Ανάλυση κίνησης (ανίχνευση κατεύθυνσης, μελέτη ροής μηνυμάτων και αναγνώριση αποτυπωμάτων ασυρματικών επικοινωνιών)
Ηλεκτρονική Ασφάλεια	**Ηλεκτρονική Ανάκτηση**
• Ασφάλεια Εκπομπής (μετατόπιση συχνοτήτων radar, ευρύ φάσμα)	• Ηλεκτρονική Αναγέννηση (υποκλοπή εκπομπών radar)
• Αντί - Αντίμετρα (παρεμβολές radar)	• Αντίμετρα (παρεμβολές σε radar και λανθασμένη ηχώ τους)

Πήγή: David Kahn, ιδία επεξεργασία

3.3.2.3. ΙΔΙΟΤΗΤΕΣ ΣΤΕΓΑΝΟΓΡΑΦΙΑΣ.

Ένα καλό στεγανογραφικό σύστημα πρέπει να εκπληρώνει τις προδιαγραφές που έθεσε η "Αρχή του Kerckhoff" στην κρυπτογραφία: "Η ασφάλεια ενός συστήματος πρέπει να βασίζεται στο δεδομένο ότι ο "εχθρός" έχει πλήρη γνώση των σχεδιαστικών λεπτομερειών και της υλοποίησης ενός στεγανογραφικού συστήματος". Η μόνη πληροφορία που λείπει από τον "εχθρό" και που πρέπει να κρατηθεί μυστική από αυτόν είναι ένας μικρός και εύκολα ανταλλάξιμος τυχαίος αριθμός, το μυστικό κλειδί, χωρίς το οποίο δεν μπορεί να γνωρίζει εάν στο κανάλι επικοινωνίας διενεργείται κρυφή επικοινωνία. Η στεγανογραφία σχετίζεται άμεσα με το πρόβλημα των "κρυμμένων καναλιών" στο σχεδιασμό ενός ασφαλούς περιβάλλοντος επικοινωνίας, ένας ορισμός που αναφέρεται σε όλα τα μέσα επικοινωνίας που δεν μπορούν εύκολα να περιοριστούν από μηχανισμούς ελέγχου (π. χ. δύο εφαρμογές-διαδικασίες που επικοινωνούν διαμορφώνοντας και μετρώντας το φόρτο της CPU). Η στεγανογραφία σχετίζεται επιπλέον και με τη τεχνική εκπομπής ευρέως φάσματος η οποία επιτρέπει την λήψη μηνυμάτων που είναι εκατό φορές πιο αδύνατα από τον ατμοσφαιρικό θόρυβο, όπως επίσης και με την τεχνική TEMPEST που αναλύει εκπομπές RF των υπολογιστών και του επικοινωνιακού εξοπλισμού με στόχο την πρόσβαση σε στοιχεία που διακινούνται σε αυτά.

Τα περισσότερα κανάλια επικοινωνιών όπως οι τηλεφωνικές γραμμές και οι εκπομπές ράδιο εκπέμπουν σήματα που συνοδεύονται πάντα από κάποιο θόρυβο. Αυτός ο θόρυβος μπορεί να αντικατασταθεί από κάποιο μυστικό σήμα που έχει τη μορφή θορύβου για κάποιον που δεν γνωρίζει το μυστικό κλειδί.

Αυτή είναι και η βασική σχεδιαστική αρχή των στεγανογραφικών συστημάτων η αντικατάσταση του θορύβου υψηλής εντροπίας από μια εκπομπή υψηλής εντροπίας. Υπάρχουν πολλά προγράμματα που υλοποιούν κάποιου είδους στεγανογραφικό μηχανισμό. Ωστόσο, η πραγματικά καλή εφαρμογή της στεγανογραφίας είναι πολύ δύσκολη υπόθεση και για αυτό το λόγο η ανίχνευση της χρήσης της από μηχανισμούς ανάλυσης αποδίδει όταν πρόκειται για απλή εφαρμογή της. Ο θόρυβος των αναλογικών συστημάτων έχει ένα μεγάλο αριθμό ιδιοτήτων που είναι πολύ χαρακτηριστικές για το κανάλι και τον εξοπλισμό του επικοινωνιακού συστήματος. Ένα καλό στεγανογραφικό σύστημα πρέπει να παρακολουθεί το κανάλι, να χτίζει ένα μοντέλο του θορύβου που είναι παρόν και μετά να προσαρμόζει τις παραμέτρους των δικών του αλγορίθμων έτσι ώστε η αντικατάσταση του θορύβου του καναλιού με

τεχνητό θόρυβο, που περιέχει την πληροφορία προς μετάδοση, να είναι επιτυχής. Το κατά πόσο το στεγανογραφικό σύστημα είναι ασφαλές εξαρτάται από τους μηχανισμούς ανάλυσης του θορύβου που έχει στη διάθεσή του ο "εχθρός".

Τα κοινά επικοινωνιακά συστήματα έχουν ένα μεγάλο αριθμό χαρακτηριστικών και μόνο ένα μικρό μέρος από αυτό που φαίνεται σαν θόρυβος μπορεί να αντικατασταθεί από τον στατιστικά πολύ καθαρό θόρυβο που δημιουργεί ένα σύστημα κρυπτογράφησης. Ο θόρυβος στις επικοινωνίες προκαλείται συχνά από τη διαμόρφωση, την κβάντιση και από άλλες διαδικασίες όπως κάθε είδους φίλτρα, συστήματα απαλοιφής της ηχούς, μετατροπείς δεδομένων κ. α. .

Εάν κάποιος ήθελε να εξετάσει ένα αρχείο με κρυμμένες πληροφορίες θα μπορούσε να τις βρει. Στη χειρότερη περίπτωση θα μπορούσε να καταλάβει ότι αυτές υπάρχουν έστω και αν δεν τις έβλεπε. Εάν οι κρυμμένες πληροφορίες είναι κρυπτογραφημένες τότε σίγουρα θα φτάσει μέχρι αυτό το σημείο και θα σταματήσει. Ωστόσο εάν δεν είναι κρυπτογραφημένες τότε θα είναι σε θέση να εξετάσει όλο το "κρυμμένο" μήνυμα. Για το λόγο αυτό δεν θα πρέπει να θεωρούμε τη στεγανογραφία σαν αντικαταστάτη της κρυπτογραφίας αλλά σαν συμπλήρωμά της. Η στεγανογραφία γίνεται όλο και πιο σημαντική στο Κυβερνοχώρο εξαιτίας του ότι οι κυβερνήσεις του κόσμου απαγορεύουν τη χρήση κρυπτογράφησης από ιδιώτες, όπως στη Γαλλία και στη Ρωσία αλλά και στην Αμερική όπου υπάρχει ένας σχετικός πόλεμος της κυβέρνησης και του δημιουργού του PGP. Κάνοντας χρήση της στεγανογραφίας μπορούμε να συνεχίσουμε να στέλνουμε κρυπτογραφημένα μηνύματα χωρίς να τα βλέπει κανείς.

Η στεγανογραφία βασίζει την ασφάλειά της στο γεγονός ότι κάποιος δεν μπορεί να ψάξει για κάτι που δεν γνωρίζει εάν υπάρχει. Επιπλέον με όλες τις μετακινήσεις δεδομένων στο Internet, κανείς δεν έχει την απαιτούμενη υπολογιστική ισχύ για να περάσει από ανίχνευση όλες τις εικόνες και τα δεδομένα που διακινούνται.

Επίσης, είναι πολύ πιο εύκολο για έναν ιδιώτη να αρνηθεί την αποστολή ενός κρυπτογραφημένου και κρυμμένου, στεγανογραφικά, μηνύματος από το να το κάνει για ένα απλά κρυπτογραφημένο. Εάν κάποιος κρύψει πληροφορία σε μια εικόνα μπορεί εύκολα να το αρνηθεί λέγοντας ότι "όπως την πήρα την έστειλα-δεν ήξερα τι

είχε μέσα, κάποιος άλλος τα έβαλε" και είναι πολύ δύσκολο για την αρχή που ψάχνει να αποδείξει το αντίθετο.

Οι παρούσες μέθοδοι παροχής πρακτικών στεγανογραφικών υπηρεσιών έχουν δύο κύριους άξονες κατευθύνσεων. Ο πρώτος, ο οποίος δεν είναι και τόσο αποδοτικός, απογυμνώνει τα κρυπτογραφημένα μηνύματα από οποιαδήποτε πληροφορία που αναφέρεται στη ταυτότητά τους . Για παράδειγμα το πρόγραμμα Stealth επεξεργάζεται κατά τέτοιο τρόπο τα κρυπτογραφημένα με PGP μηνύματα που φαίνονται σαν σκουπίδια. Το πρόβλημα με αυτή τη μέθοδο είναι ότι η αναγνώριση ενός PGP μηνύματος είναι πολύ εύκολη υπόθεση ακόμα και αν έχουν αφαιρεθεί οι πληροφορίες αναγνώρισής του. Το Stealth μπορεί να παράσχει ασφάλεια κάποιου επιπέδου αλλά δεν μπορεί να αντιμετωπίσει κάποιον αποφασισμένο hacker.

Ο δεύτερος άξονας της στεγανογραφίας είναι η απόκρυψη δεδομένων μέσα σε άλλα αρχεία. Για παράδειγμα μπορούν να χρησιμοποιηθούν τα λιγότερο σημαντικά bits μιας bitmap εικόνας, μέσα στα οποία μπορεί να κρυφτεί η πληροφορία. Η αλλαγή αυτών των bits της εικόνας προκαλεί ανεπαίσθητες αλλαγές στη μορφή της. Χωρίς απευθείας σύγκριση με την αρχική εικόνα είναι πραγματικά αδύνατο να πει κανείς ότι κάτι άλλαξε.

Άλλος ένας τύπος αρχείων που μπορεί να χρησιμοποιηθεί για το κρύψιμο πληροφορίας μέσα του είναι τα ψηφιακά μουσικά αρχεία. Με την εισαγωγή του μηνύματος στα λιγότερο σημαντικά bits ενός μουσικού αρχείου κρύβεται η πληροφορία και ομοίως με τα αρχεία εικόνας δεν έχουμε αισθητές αλλοιώσεις στο τελικό, μουσικό, αποτέλεσμα.

Ένας τελευταίος και λόγω της φύσης του λιγότερο χρησιμοποιούμενος τρόπος, είναι αυτός της απόκρυψης δεδομένων στα μη χρησιμοποιούμενα sectors των δισκετών. Όπως βέβαια αντιλαμβανόμαστε αυτή η μέθοδος δεν μπορεί να χρησιμοποιηθεί σε δικτυακά σχήματα και εδώ απλά γίνεται αναφορά της ύπαρξής της σαν μία επιπλέον δυνατότητα

3.4. ΤΕΧΝΟΛΟΓΙΕΣ ΜΟΝΙΜΗΣ ΣΥΣΧΕΤΙΣΗΣ

Οι τεχνολογίες μόνιμης συσχέτισης είναι : fingerprinting, υδατογράφηση ,και ψηφιακές υπογραφές.

3.4.1. FINGERPRINTING

Το fingerprinting, ή οι "τεχνολογίες αναγνώρισης βασισμένες στο περιεχόμενο" λειτουργούν εξάγοντας τα χαρακτηριστικά ενός αρχείου και αποθηκεύοντάς τα σε μια βάση δεδομένων. Όταν το αρχείο είναι άγνωστο, υπολογίζονται τα χαρακτηριστικά του και συγκρίνονται με εκείνα που είναι αποθηκευμένα στη βάση δεδομένων, σε μία προσπάθεια να βρεθεί μια αντιστοιχία. Εάν βρεθεί, το σύστημα θα επιστρέψει τα κατάλληλα μεταδεδομένα από τη βάση δεδομένων των fingerprints.

Προκειμένου να χρησιμοποιηθεί η τεχνολογία του fingerprinting, πρέπει να γίνουν τρία βήματα:

- Πρώτα πρέπει να δημιουργηθεί μια βάση δεδομένων με τα "fingerprints αναφοράς" και κατάλληλα μεταδεδομένα. Αυτό το βήμα, θα πρέπει να γίνει πριν την προσπάθεια να αναγνωριστεί το άγνωστο περιεχόμενο
- Δεύτερον, για να βρεθεί πληροφορία για οποιοδήποτε αρχείο (αποκαλούμενο "αρχείο δοκιμής"), το σύστημα παράγει ένα "fingerprint δοκιμής" από το αρχείο αυτό. Το fingerprint δοκιμής συγκρίνεται έπειτα με όλα τα "fingerprint αναφοράς" που είναι αποθηκευμένα στη βάση δεδομένων των fingerprints
- Τελικά, όταν βρεθεί ένα fingerprint που ταιριάζει, τα μεταδεδομένα που συνδέονται με αυτό θα ληφθούν από τη βάση δεδομένων των fingerprints. Αυτά τα μεταδεδομένα θα είναι η έξοδος της διαδικασίας.

Προγράμματα λογισμικού και υπηρεσίες που χρησιμοποιούν fingerprinting τεχνολογίες είναι διαθέσιμα για διάφορους τύπους μέσων όπως ήχου και εικόνας. Το καλύτερο σύστημα θα αναγνωρίζει σωστά περισσότερα από 95% των αρχείων ακόμη και κάτω από κακές συνθήκες, όπου το αρχείο κακόβουλα ή αναπόφευκτα έχει υποστεί αλλαγές για να υπερνικήσει το fingerprinting σύστημα. Μερικές τεχνολογίες είναι ικανές ακόμα και να κάνουν υψηλά επίπεδα θετικών αντιστοιχιών σε περιπτώσεις όπου το αρχείο δοκιμής έχει δημιουργηθεί με πολύ παρασιτικό θόρυβο.

Τα fingerprints, ενώ είναι ιδιαίτερα αποτελεσματικά με ορισμένους τύπους περιεχομένου, είναι λιγότερο με άλλους, ανάλογα με το "επίπεδο λεπτομέρειας" που παρέχουν. Ως εκ τούτου τα fingerprints είναι κατάλληλα για ήχο, βίντεο και οπτικοακουστικό περιεχόμενο καθώς επίσης και για φωτογραφίες αλλά λιγότερο για γραφικά ή κείμενο.

Η πιο διαδεδομένη χρήση των fingerprinting τεχνολογιών είναι ο έλεγχος ραδιοσταθμών. Επίσης χρησιμοποιούνται όλο και περισσότερο για να ελέγχουν peer-to-peer συστήματα διανομής περιεχομένου για παραβάσεις πνευματικών δικαιωμάτων. Ένα άλλο παράδειγμα χρήσης του fingerprinting είναι το ακόλουθο σενάριο. Ένας χρήστης κάθεται σε ένα εστιατόριο και, ακούγοντας ένα τραγούδι που του αρέσει, ενεργοποιεί τη fingerprinting συσκευή του (π.χ., το κινητό τηλέφωνό του/της) που αναγνωρίζει το τραγούδι και διαβιβάζει κάποιες πληροφορίες σε έναν φορέα παροχής υπηρεσιών. Φθάνοντας σπίτι, ο χρήστης βρίσκει το ίδιο τραγούδι ως ένα audio αρχείο στο e-mail του, που έχει σταλεί από ένα αυτοματοποιημένο σύστημα χρησιμοποιώντας το fingerprint που στάλθηκε από το κινητό τηλέφωνο για να αναγνωριστεί το τραγούδι που άρεσε στον χρήστη.

3.4.2. ΥΔΑΤΟΓΡΑΦΗΣΗ

3.4.2.1. ΟΙ ΠΡΟΓΟΝΟΙ ΤΩΝ ΨΗΦΙΑΚΩΝ ΥΔΑΤΟΓΡΑΦΗΜΑΤΩΝ

Οι τεχνικές για τη δημιουργία υδατογραφημάτων στο χαρτί είναι τόσο παλιές όσο και η ίδια η κατασκευή του και ανάγονται στα τέλη του μεσαίωνα. Η αποτύπωση των υδατογραφημάτων στο χαρτί έχει σαν αποτέλεσμα την εμφάνιση ενός αχνού σχήματος, κειμένου κ.τ.λ. κάθε φορά που το παρατηρούμε στο φως.

Αρχικά τα υδατογραφήματα χρησιμοποιηθήκαν για την αποτύπωση των εμπορικών σημάτων των κατασκευαστών χαρτιού πάνω στα προϊόντα τους με στόχο την εξασφάλιση της αυθεντικότητάς τους. Έχει αποδειχθεί ιστορικά πως η πλαστογράφηση των υδατογραφημάτων είναι εξαιρετικά δύσκολη και η χρήση τους, για την επίτευξη του προαναφερθέντος σκοπού, ιδιαίτερα επιτυχημένη. Έτσι, σύντομα οι κυβερνήσεις των διαφόρων κρατών, άρχισαν να αποτυπώνουν

υδατογραφήματα σε χαρτονομίσματα, γραμματόσημα κ.τ.λ. με στόχο την αποφυγή της πλαστογράφησής τους.

Στην ψηφιακή εποχή μας και με δεδομένη την τεράστια εξάπλωση της χρήσης των ψηφιακών μέσων, τα υδατογραφήματα έγιναν και αυτά ψηφιακά, δηλαδή, μέρος των άυλων αυτών τεκμηρίων για την εξασφάλιση της αυθεντικότητας και των πνευματικών δικαιωμάτων του δημιουργού, ιδιοκτήτη, εξουσιοδοτημένου χρήστη κ.τ.λ.

3.4.2.2. ΨΗΦΙΑΚΑ ΥΔΑΤΟΓΡΑΦΗΜΑΤΑ - ΕΝΝΟΙΕΣ

Στο σημείο αυτό θα ήταν καλό να αποσαφηνιστούν κάποιες έννοιες-τεχνικές που θα μπορούσε κάποιος λανθασμένα να ταυτίσει με την ψηφιακή υδατογράφηση. Οι τεχνικές αυτές είναι εκείνες της στεγανογραφίας και της κρυπτογραφίας.

Η στεγανογραφία είναι μια τεχνική που χρησιμοποιείται για την απόκρυψη δεδομένων-πληροφοριών μέσα σε κάποιο «ψηφιακό στεγανό». Θα μπορούσε κάποιος να πει πως η ψηφιακή υδατογράφηση αποτελεί ένα είδος στεγανογραφίας, όπως θα δούμε στη συνέχεια. Η κρυπτογραφία από την άλλη, αποτελεί τεχνική κατά την οποία τα μεταδιδόμενα δεδομένα-πληροφορίες κωδικοποιούνται με τέτοιο τρόπο, ώστε ακόμα και αν πέσουν στα χέρια μη εξουσιοδοτημένων χρηστών, να είναι ακατανόητα και άχρηστα.

Τα ψηφιακά υδατογραφήματα χρησιμοποιούνται, όπως έχει ήδη τονιστεί και παραπάνω, για την εξασφάλιση της εγκυρότητας ενός αντικειμένου, το αναμφισβήτητο της ταυτότητας του ιδιοκτήτη κ.τ.λ. Αυτό επιτυγχάνεται με την ενσωμάτωση πληροφοριών (υδατογράφημα) στο αρχικό ψηφιακό τεκμήριο και όλη αυτή η διαδικασία ονομάζεται ψηφιακή υδατογράφηση. Η ψηφιακή υδατογράφηση διαφοροποιείται από τις δύο προηγούμενες τεχνικές, καθώς συνδυάζει δυο κομμάτια πληροφορίας, την πρωτότυπη και την προστιθέμενη (υδατογράφημα), με τέτοιο τρόπο ώστε να μπορεί κανείς να τα επεξεργαστεί ανεξάρτητα.

Τα ψηφιακά υδατογραφήματα δε θα πρέπει να συγχέονται με αυτά που στην αγγλική βιβλιογραφία ονομάζονται ως fingerprints. Τα fingerprints αποτελούν

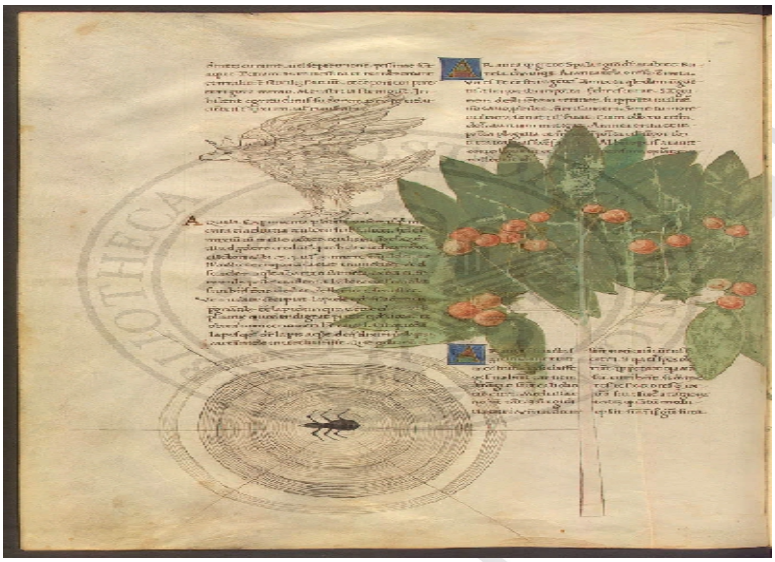
χαρακτηριστικά ενός αντικειμένου τα οποία το διαχωρίζουν από παρόμοια αντικείμενα. Με το fingerprinting, δημιουργείται ένα δεύτερο αρχείο το οποίο «περιγράφει» το περιεχόμενο του αρχικού. Τα fingerprints παρέχουν τη δυνατότητα στον ιδιοκτήτη του ψηφιακού τεκμηρίου που τα περιέχει, να εντοπίσει παράνομες διανομές του από εξουσιοδοτημένους χρήστες.

3.4.2.3. ΟΡΑΤΑ ΚΑΙ ΑΟΡΑΤΑ ΨΗΦΙΑΚΑ ΥΔΑΤΟΓΡΑΦΗΜΑΤΑ

Τα ψηφιακά υδατογραφήματα θα μπορούσαν γενικά να χωριστούν σε δύο μεγάλες κατηγορίες, αυτά που γίνονται αντιληπτά από τον άνθρωπο (ορατά ψηφιακά υδατογραφήματα) και αυτά που δεν γίνονται αντιληπτά (αόρατα ψηφιακά υδατογραφήματα).

Τα ορατά ψηφιακά υδατογραφήματα χρησιμοποιούνται σχεδόν με τον ίδιο τρόπο όπως και οι πρόγονοί τους στο χαρτί, με στόχο την αναγνώριση της πηγής προέλευσης, την εξασφάλιση της ιδιοκτησίας και γιατί όχι, της διαφήμισης. Τα ορατά υδατογραφήματα αφορούν στην ενσωμάτωση μιας ορατής εικόνας στο ψηφιακό τεκμήριο με τέτοιο τρόπο ώστε να φαίνεται ευκρινώς αλλά χωρίς να επηρεάζει την ποιότητα του περιεχομένου της. Ένα τέτοιο υδατογράφημα, φαίνεται στην εικ. 1. (ψηφιοποιημένο χειρόγραφο)

Τα ορατά ψηφιακά υδατογραφήματα χρησιμοποιούνται για άμεση κατάδειξη του ιδιοκτήτη σε αντίθεση με τα αόρατα. Το βασικό τους πλεονέκτημα είναι ότι κατ' ουσίαν, περιορίζουν την εμπορική αξία του ψηφιακού αντικειμένου, χωρίς αυτό να χάνει τη χρησιμότητά του για νόμιμους και εξουσιοδοτημένους σκοπούς. Επομένως, τα ορατά ψηφιακά υδατογραφήματα πάνω σε ψηφιακά τεκμήρια, καθιστούν φανερό το γεγονός πως τα τεκμήρια αυτά ανήκουν σε κάποιον, χωρίς όμως αυτό να μειώνει την ανάγκη και την αξία της χρήσης τους.



Από την άλλη, τα αόρατα ψηφιακά υδατογραφήματα αποτελούν δυαδική πληροφορία που ενσωματώνεται στην αρχική αλλά παραμένει αόρατη για τον άνθρωπο μια και δεν αλλοιώνει εμφανώς την εικόνα. Ο εντοπισμός της εφαρμογής του αόρατου ψηφιακού υδατογραφήματος γίνεται αλγοριθμικά. Τα αόρατα λοιπόν υδατογραφήματα, χρησιμοποιούνται για να κρύψουν πληροφορίες σε ένα ψηφιακό τεκμήριο. Στην επόμενη εικόνα (εικ. 2), παρουσιάζεται μια υδατογραφημένη ψηφιακή φωτογραφία με το αόρατο υδατογράφημα πάνω δεξιά.

Αντίθετα, στην εικ. 3 φαίνεται το υδατογράφημα που προκύπτει από τη χρήση ενός συστήματος εντοπισμού υδατογραφημάτων και το αποτέλεσμα που δίνει το σύστημα για ένα κομμάτι της εικόνας που δεν περιέχει υδατογράφημα.

Τα αόρατα ψηφιακά υδατογραφήματα μπορούν να αποτρέψουν μια κλοπή-μη εξουσιοδοτημένη αντιγραφή, χρήση κ.τ.λ. μόνο όταν ο επίδοξος χρήστης έχει υποψία ότι το ψηφιακό τεκμήριο που πάει να κλέψει είναι υδατογραφημένο. Πέρα όμως από την ψυχολογική αποτροπή της παράνομης χρήσης, τα αόρατα ψηφιακά υδατογραφήματα προσδιορίζουν την πηγή, το δημιουργό, τον ιδιοκτήτη, τον εξουσιοδοτημένο χρήστη κ.τ.λ. ενός ψηφιακού τεκμηρίου. Έτσι, στόχος αποτελεί η μόνιμη και χωρίς δυνατότητα τροποποίησης, ενσωμάτωση πληροφοριών στα ψηφιακά τεκμήρια.

Σε πολλές περιπτώσεις πάντως, και οι δύο τύποι ψηφιακών υδατογραφημάτων (ορατά-αόρατα), αποδεικνύονται εξίσου αποτελεσματικοί. Πολλές εταιρείες μάλιστα, αναπτύσσουν λογισμικά τα οποία θέτουν πράκτορες (agents) υδατογραφημάτων σε «περιπολίες» στο διαδύκτιο με στόχο τον εντοπισμό μη εξουσιοδοτημένης χρήσης ψηφιακά υδατογραφημένων τεκμηρίων. Αξίζει εδώ να σημειωθεί πως τα λογισμικά υδατογράφησης αποδίδουν ένα μοναδικό υδατογράφημα σε κάθε ψηφιακό τεκμήριο για κάθε εξουσιοδοτημένο χρήστη.

Στον παρακάτω πίνακα παρατίθενται βασικά (β) και δευτερεύοντα (δ) οφέλη της χρήσης ψηφιακών υδατογραφημάτων, ορατών και αοράτων.

Πίνακας 2: Βασικά (β) και δευτερεύοντα (δ) οφέλη της χρήσης ψηφιακών υδατογραφημάτων, ορατών και αοράτων

Σκοπός	**Ορατά ψηφιακά υδατογραφήματα**	**Αόρατα ψηφιακά υδατογραφήματα**
1. Καθορισμός ιδιοκτησίας	β	β
2. Αποτροπή κλοπής	β	β
3. Περιγραφή περιεχομένου (meta-level)	-	β
4. Μείωση εμπορικής αξίας χωρίς περιορισμό της χρησιμότητας	β	-
5. Αποθάρρυνση μη εξουσιοδοτημένης δημοσίευσης	β	β
6. Επαλήθευση αυθεντικότητας	δ	β
7. Εντοπισμός πηγής αντικειμένου	β	β
8. «Περιπολίες» δικτύου	δ	β
9. Διαχείριση δικαιωμάτων (rights management)	δ	β

Πηγή: Ιδία επεξεργασία

Ανακεφαλαιώνοντας, θα μπορούσαμε να καταλήξουμε στα εξής δύο γενικά συμπεράσματα: τα ορατά ψηφιακά υδατογραφήματα μειώνουν την εμπορική αξία των ψηφιακών τεκμηρίων καταδεικνύοντας ξεκάθαρα τον ιδιοκτήτη τους ενώ τα αόρατα αυξάνουν τις πιθανότητες «καταδίωξης» και εντοπισμού ενός μη εξουσιοδοτημένου χρήστη.

3.4.2.4. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΠΕΡΙΕΧΟΥΝ ΤΑ ΨΗΦΙΑΚΑ ΥΔΑΤΟΓΡΑΦΗΜΑΤΑ

Για να μπορέσουν τα ψηφιακά υδατογραφήματα να είναι αποτελεσματικά ως προς τους στόχους τους, πρέπει κατά το σχεδιασμό τους να λαμβάνονται υπόψη μια σειρά από παράγοντες. Παρακάτω, αναφέρονται συνοπτικά οι πιο σημαντικοί από αυτούς.

- Επιμονή (persistence):τα ψηφιακά υδατογραφήματα πρέπει να εξακολουθούν να υφίστανται σ' ένα ψηφιακό τεκμήριο, ακόμα κι αν αυτό τροποποιείται (π.χ. αλλαγή χρωμάτων των εικόνων, φιλτράρισμα, συμπίεση κ.τ.λ.)
- Αξιοπιστία (robustness): πρέπει να αντιστέκονται σε ψηφιακές επιθέσεις που έχουν ως στόχο τη διαγραφή, την αλλαγή ή την αντικατάστασή τους παράνομα.
- Μη αποτροπή χρήσης (unobtrusiveness): τόσο τα ορατά όσο και τα αόρατα υδατογραφήματα πρέπει να είναι έτσι ανεπτυγμένα, ώστε να μην αποτρέπουν τους χρήστες από τη χρήση του ψηφιακού τεκμηρίου που τα εμπεριέχει.
- Δυνατότητα αποκωδικοποίησης (decodability): το συγκεκριμένο χαρακτηριστικό προκύπτει από τις επιβολές του νόμου. Σε εφαρμογές αόρατων υδατογραφημάτων, πρέπει αυτά να μπορούν να εντοπιστούν από τις αρμόδιες αρχές ακόμα κι όταν δεν είναι ορατά για τον κοινό χρήστη.
- Χρειάζονται μέθοδοι που να επιτρέπουν την ανάκτηση του ψηφιακού υδατογραφήματος, χωρίς την ανάγκη σύγκρισης με το αρχικό τεκμήριο.
- Το μέγεθος του ψηφιακού υδατογραφήματος δε μπορεί να είναι ανεξέλεγκτο. Όσο μεγαλύτερο είναι το μέγεθος ενός υδατογραφήματος, τόσο πιο δύσκολα ανακτάται. Αν, για παράδειγμα, αποτελεί στόχος η ταύτιση της ιδιοκτησίας και του ιδιοκτήτη ενός ψηφιακού τεκμηρίου, ένα υδατογράφημα των 32bit είναι αρκετό για να ταυτίσει 232 ιδιοκτήτες.

3.4.2.5. ΣΤΑΔΙΑ ΔΙΑΔΙΚΑΣΙΑΣ ΨΗΦΙΑΚΗΣ ΥΔΑΤΟΓΡΑΦΗΣΗΣ

Υπάρχουν τρία στάδια κατά την υδατογράφηση οποιουδήποτε ψηφιακού τεκμηρίου και αυτά είναι τα εξής:

- Παραγωγή ψηφιακού υδατογραφήματος η παραγωγή του ψηφιακού υδατογραφήματος, εξαρτάται από το σκοπό τον οποίο προορίζεται να εξυπηρετήσει. Την πιο συνηθισμένη μέθοδο αποτελεί η χρήση ενός μοντέλου bit (bit pattern) συγκεκριμένου μεγέθους, εάν στόχος αποτελεί η απλή ταύτιση του ιδιοκτήτη ή του εξουσιοδοτημένου χρήστη ενός ψηφιακού τεκμηρίου.
- Ενσωμάτωση του υδατογραφήματος, τεχνικές ενσωμάτωσης θα δούμε στη συνέχεια.
- Ανάκτηση υδατογραφήματος το πιο σημαντικό μέρος κάθε συστήματος υδατογράφησης αποτελεί η ανάκτηση του υδατογραφήματος. Η ανάκτηση αυτή, μπορεί να πραγματοποιηθεί με ή χωρίς την ανάγκη αντιπαραβολής με το αρχικό τεκμήριο.

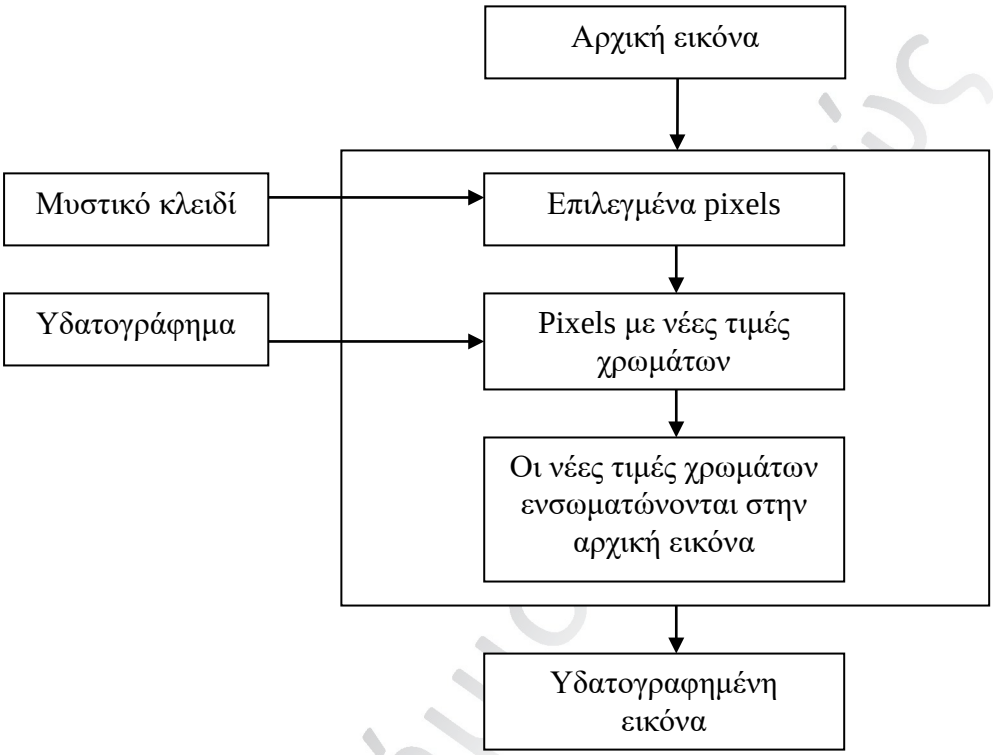
3.4.2.6. ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ ΕΝΣΩΜΑΤΩΣΗΣ ΚΑΙ ΑΝΑΚΤΗΣΗΣ ΨΗΦΙΑΚΩΝ ΥΔΑΤΟΓΡΑΦΗΜΑΤΩΝ.

Τα ψηφιακά υδατογραφήματα αποτελούν, όπως είδαμε και παραπάνω, ψηφιακά δεδομένα που ενσωματώνονται σε ένα ψηφιακό τεκμήριο. Καθώς το υδατογράφημα εντοπίζεται σε κάθε αντίγραφο του υδατογραφημένου τεκμηρίου, τα ψηφιακά δεδομένα μπορούν να χρησιμοποιηθούν ως ψηφιακή υπογραφή (digital signature). Η υπογραφή αυτή μπορεί να χρησιμοποιηθεί ως αποδεικτικό ιδιοκτησίας.

Η υπογραφή πρέπει να είναι παρόμοια και μοναδική σε κάθε αντίγραφο για την ταύτιση του ιδιοκτήτη. Κατ' ουσίαν, η ενσωμάτωση ενός ψηφιακού υδατογραφήματος σε ένα ψηφιακό τεκμήριο μπορεί να περιγραφή ως η μετατροπή

του αρχικού (original) τεκμηρίου σε ένα νέο, το οποίο είναι απόλυτα αναγνωρίσιμο όταν συγκριθεί με το αρχικό. Στο σχήμα 4 παρουσιάζεται σχηματικά η διαδικασία ενσωμάτωσης ενός ψηφιακού υδατογραφήματος σε μία ψηφιακή εικόνα.

Σχήμα 3: Διαδικασία ενσωμάτωσης ενός ψηφιακού υδατογραφήματος σε μία ψηφιακή εικόνα

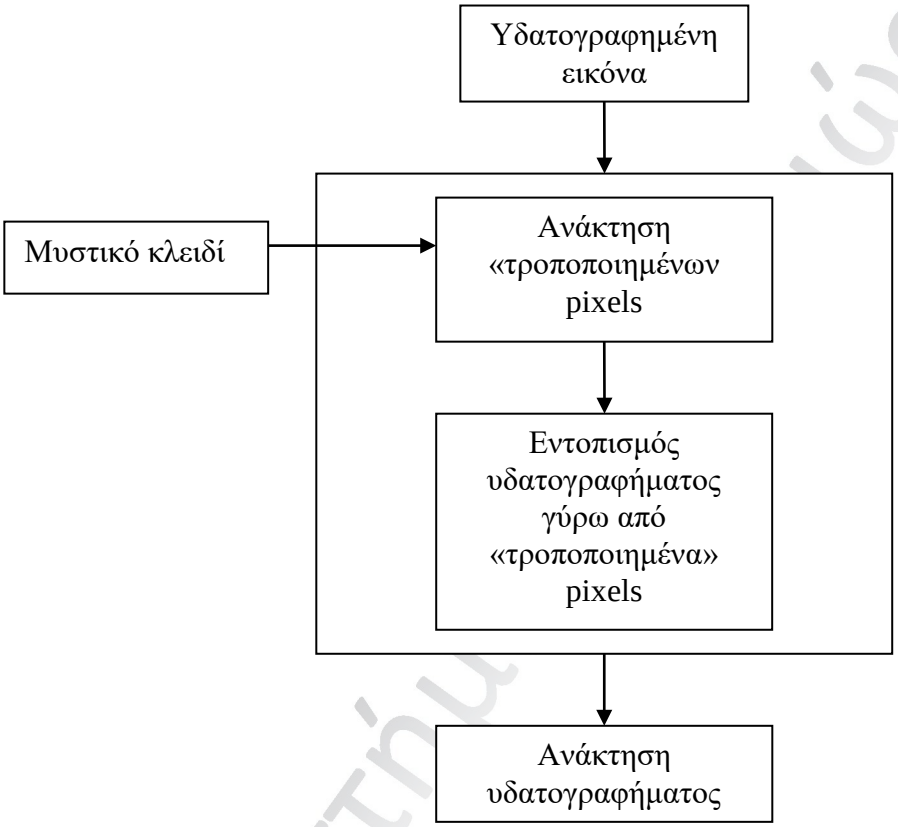


Όπως φαίνεται και στο σχήμα παραπάνω, τυχαία στοιχεία (π.χ. pixels από τα χρώματα της εικόνας) επιλέγονται από το αρχικό τεκμήριο. Τα στοιχεία αυτά επιλέγονται αυθαίρετα με τη βοήθεια ενός μυστικού κλειδιού (secret key)(ακέραιος αριθμός) που παρέχει ένας random generator. Τα στοιχεία αυτά χρησιμοποιούνται για την ενσωμάτωση του υδατογραφήματος. Το μέγεθος του υδατογραφήματος και ο αριθμός των θέσεων (pixels) δεν είναι απαραίτητα ο ίδιος. Η ενσωμάτωση του υδατογραφήματος στα επιλεγμένα pixels δημιουργεί νέα «τροποποιημένα» pixels τα οποία στη συνέχεια ενσωματώνονται στην αρχική εικόνα και έτσι προκύπτει η υδατογραφημένη εικόνα.

Αξίζει να σημειωθεί εδώ πως η μετατροπή αυτή διαφέρει από εκείνη που πραγματοποιείται στην κρυπτογραφία, κατά την οποία και εκεί το αρχικό τεκμήριο

μετατρέπεται σε νέο. Το σημείο της διαφοράς έγκειται στο γεγονός πως στην κρυπτογραφία, το νέο τεκμήριο δεν είναι αναγνωρίσιμο όταν συγκριθεί με το αρχικό. Η διαδικασία ανάκτησης των ψηφιακών υδατογραφημάτων ακολουθεί ακριβώς την αντίθετη φορά όπως φαίνεται στο παρακάτω σχήμα (σχήμα 5).

Σχήμα 4: Διαδικασία ανάκτησης των ψηφιακών υδατογραφημάτων



Χρησιμοποιείται το μυστικό κλειδί για την ανάκτηση των «τροποποιημένων» pixels από την υδατογραφημένη εικόνα. Γύρω από αυτά, εντοπίζεται το χρησιμοποιούμενο υδατογράφημα και έτσι, τελικά ανακτάται.

3.4.2.7. ΤΕΧΝΙΚΕΣ ΨΗΦΙΑΚΗΣ ΥΔΑΤΟΓΡΑΦΗΣΗΣ ΣΕ ΕΙΚΟΝΑ ΚΑΙ ΚΕΙΜΕΝΟ

Αν και τα ψηφιακά υδατογραφήματα μπορούν να ενσωματωθούν σε κάθε κατηγορία ψηφιακού τεκμηρίου (αρχεία ήχου, video, εικόνας, κειμένου κάθε μορφής), εδώ θα επικεντρωθούμε σε κάποιες τεχνικές που αφορούν εικόνες και κείμενο.

Η υδατογράφηση ψηφιακών εικόνων, μπορεί να πραγματοποιηθεί σε δυο επίπεδα: σε spatial domain και frequency domain Μια τεχνική υδατογράφησης σε spatial domain, αφορά στην τροποποίηση των υποστοιχείων μιας εικόνας (pixels), όπως αυτή περιγράφηκε στο παράδειγμα της παραγράφου 2.2. Η τεχνική αυτή παρουσιάζει σημαντικά αποτελέσματα όταν η ψηφιακή εικόνα δεν αποτελεί αντικείμενο τροποποιήσεων από των άνθρωπο, αν και φαίνεται πως το υδατογράφημα δεν επηρεάζεται από τη συμπίεση ή το φιλτράρισμα της εικόνας. Η spatial υδατογράφηση, μπορεί να εφαρμοστεί και σε τεχνικές διαχωρισμού των χρωμάτων με τέτοιο τρόπο ώστε το υδατογράφημα να εμφανίζεται μόνο σε ένα χρώμα από ολόκληρο το φάσμα των χρωμάτων. Η τεχνική αυτή καθιστά το ψηφιακό υδατογράφημα αόρατο. Όμως, εμφανίζεται αμέσως όταν τα χρώματα διαχωρίζονται για να εκτυπωθεί η εικόνα. Έτσι, ουσιαστικά, το τεκμήριο καθίσταται άχρηστο μετά την εκτύπωση. Τη μόνη λύση αποτελεί η αφαίρεση του υδατογραφήματος από το φάσμα των χρωμάτων πριν την εκτύπωση.

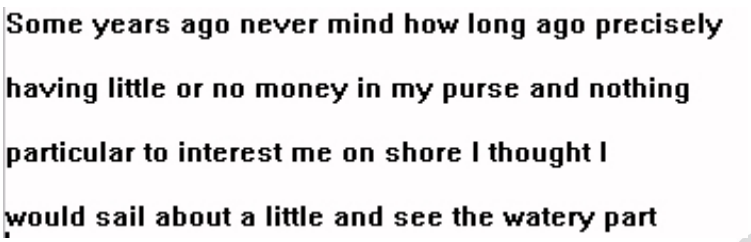
Στο δεύτερο επίπεδο (frequency domain), χρησιμοποιείται τεχνική τροποποίησης της συχνότητας (frequency transformation), κατά την οποία οι τιμές των επιλεγμένων συχνοτήτων τροποποιούνται και έτσι διαφέρουν από εκείνες της αρχικής εικόνας. Με δεδομένο ότι οι υψηλές συχνότητες μπορούν να χαθούν, για παράδειγμα κατά τη συμπίεση, τα υδατογραφήματα εφαρμόζονται σε χαμηλότερες συχνότητες που περιέχουν σημαντικές πληροφορίες της αρχικής εικόνας (feature-based schemes). Η χρήση της τεχνικής αυτής παρέχει τη δυνατότητα εφαρμογής του υδατογραφήματος σ’ ολόκληρο το εύρος της εικόνας και είναι πιο αξιόπιστη ως προς τα αποτελέσματα από την προηγούμενη τεχνική.

Όπως είδαμε και προηγουμένως, ψηφιακά υδατογραφήματα μπορούν να ενσωματωθούν και σε κείμενο. Υπάρχουν τρεις τεχνικές γι’ αυτό: α) κωδικοποίηση γραμμής (text line coding), β) κωδικοποίηση κενού ανάμεσα στις λέξεις (word space coding) και γ) κωδικοποίηση χαρακτήρα (character encoding).

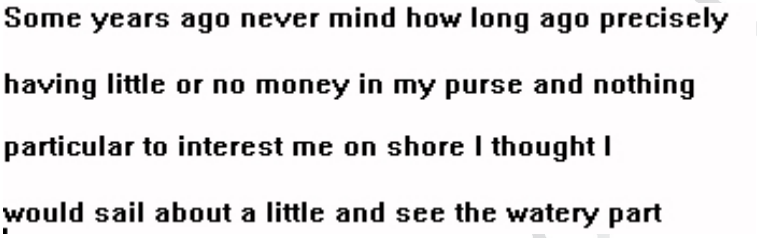
Στην πρώτη περίπτωση (text line coding), οι γραμμές του κειμένου μετακινούνται ανεπαίσθητα προς τα επάνω ή προς τα κάτω για να πραγματοποιηθεί η κωδικοποίηση. Μια τέτοια περίπτωση υδατογράφησης σε κείμενο έχουμε στις εικόνες 6, 7, 8. Το αρχικό κείμενο παρουσιάζεται στην εικόνα 6. Στην εικόνα 7, οι

γραμμές ένα και τρία είναι χαμηλότερα κατά 1 pixel σε σχέση με το αρχικό κείμενο, αποτυπώνοντας έτσι, τον κωδικό 101, όπως φαίνεται τελικά και στην εικόνα 8.

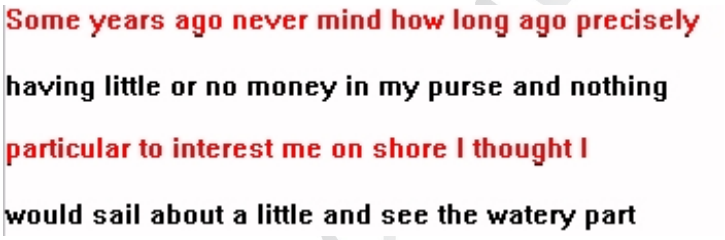
Εικόνα 6



Εικόνα 7



Εικόνα 8



Στη δεύτερη περίπτωση (word space coding), η απόσταση ανάμεσα στις λέξεις αλλάζει Βέβαια, μπορεί κανείς να αποφύγει τους περιορισμούς του ψηφιακού υδατογραφήματος δακτυλογραφώντας ξανά το κείμενο.

Κάτι αντίστοιχο συμβαίνει και στην τρίτη περίπτωση, εκείνη της κωδικοποίησης χαρακτήρων (character encoding).

3.4.2.8. ΠΡΟΒΛΗΜΑΤΑ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΑΠΟ ΤΗ ΔΗΜΙΟΥΡΓΙΑ «ΠΛΑΣΤΩΝ» ΥΔΑΤΟΓΡΑΦΗΜΑΤΩΝ

Το 1997 παρουσιάστηκε ένα σχήμα δημιουργίας «πλαστών» ψηφιακών υδατογραφημάτων. Το σχήμα αυτό μπορεί να χρησιμοποιηθεί με στόχο, κάποιος να ισχυριστεί, ψευδώς, ότι κατέχει την ιδιοκτησία ενός ψηφιακού αντικειμένου, μια και η ανάκτηση της ψηφιακής υπογραφής από ένα υδατογραφημένο τεκμήριο, προϋποθέτει τη σύγκριση με το αρχικό. Το προαναφερθέν σχήμα λειτουργεί δημιουργώντας ένα πλαστό υδατογραφημένο αντίγραφο του αυθεντικού αντιγράφου με αποτελεσματική αναστροφή του δευτέρου. Η αναστροφή αυτή, δημιουργεί ένα πλαστό αντίγραφο της αρχικής εικόνας, το οποίο ικανοποιεί δύο προϋποθέσεις: α) μια σύγκριση των αποκωδικοποιημένων τεκμηρίων (αφαίρεση υδατογραφήματος) τόσο του αυθεντικού αρχικού όσο και του πλαστού αρχικού, φέρουν την υπογραφή του πραγματικού ιδιοκτήτη και β) μια σύγκριση των αποκωδικοποιημένων τεκμηρίων, τόσο του αυθεντικού αρχικού όσο και του πλαστού αρχικού, φέρουν την πλαστή υπογραφή (ανεστραμμένη υδατογράφηση).

Έτσι λοιπόν, η τεχνική της σύγκρισης των υδατογραφημένων τεκμηρίων με τα αρχικά τεκμήρια δε μπορεί να αποδείξει ποιος είναι ο νόμιμος ιδιοκτήτης. Γνωρίζουμε την ύπαρξη πλαστού αντιγράφου αλλά δε γνωρίζουμε ποιο από τα δύο είναι. Αυτό λοιπόν που χρειάζεται, είναι καλύτεροι αλγόριθμοι για τη δημιουργία αρκετά αποτελεσματικών υδατογραφημάτων τα οποία, βεβαίως, θα είναι πιο ανθεκτικά στις επιθέσεις των πλαστογράφων.

3.5. ΤΕΧΝΟΛΟΓΙΕΣ PRIVACY

Ιδιωτικότητα είναι η αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων. Τα DRM μοντέλα στηρίζονται σε μια υποδομή "εμπιστευτικής ταυτότητας", που αφορά εμπιστευτική αναγνώριση του περιεχομένου, των αδειών που είναι σχετικές με το περιεχόμενο, και των συμμετεχόντων στις άδειες που είναι σχετικές με το περιεχόμενο.

Η χρήση τεχνολογιών ανωνυμίας κρίνεται απαραίτητη. Ανώνυμος περιήγηση είναι απλή περιήγηση του World Wide Web με τα περισσότερα από τα στοιχεία ταυτότητάς του καταναλωτή κρυφά. Αυτό γίνεται κυρίως μέσω αυτού που είναι γνωστό ως ανώνυμο browser . Αυτοί είναι οι δικτυακοί τόποι που μπορεί να

χρησιμοποιεί ο καταναλωτής για την είσοδο της διεύθυνση της ιστοσελίδας που θέλει να επισκεφθεί, και η υπηρεσία θα τον μεταφέρει σε αυτή την ιστοσελίδα με πληροφορίες όπως η θέση του υπολογιστή του και η διεύθυνση IP που αποκρύπτονται από την ιστοσελίδα. Για παράδειγμα, όταν ο χρήστης προσπαθήσει να αποκτήσει πρόσβαση σε κάτι σχετικά με ένα ορισμένο τμήμα του Διαδικτύου, ο πληρεξούσιος θα μιλήσει για αυτό το αρχείο ως πρεσβευτής του χρήστη, για την διατήρηση της ιδιωτικής του ζωής . Η πρακτική των ανώνυμων περιηγήσεων μπορεί επίσης να διατηρήσει την ιδιωτική ζωή του χρήστη από πιθανές κατασκοπείες σχετικά με την σύνδεση του.

3.6. ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΩΜΩΝ

Η πρακτική εφαρμογή του ηλεκτρονικού εμπορίου στο σύγχρονο επιχειρηματικό και καταναλωτικό περιβάλλον δημιούργησε την ανάγκη για ανάπτυξη νέων μορφών πληρωμών, περισσότερων κατάλληλων στις νέες διαμορφούμενες συνθήκες συναλλαγής στο κυβερνοχώρο. Έτσι αναπτύχθηκαν τα λεγόμενα Συστήματα Ηλεκτρονικών Πληρωμών για την ηλεκτρονική πλέον διεκπεραίωση των οφειλών των εμπλεκομένων μερών. Οι ηλεκτρονικές πληρωμές αποτελούν αναπόσπαστο τμήμα του ηλεκτρονικού εμπορίου. Τέτοιες πληρωμές είναι οι πιστωτικές κάρτες, η ηλεκτρονική μεταφορά κεφαλαίων, χρεωστικές κάρτες, χρηματοοικονομικό EDI, κάρτες αποθηκευμένης αξίας και έξυπνες κάρτες, ψηφιακό χρήμα και τέλος ηλεκτρονικές επιταγές.

Ο πιο χαρακτηριστική πληρωμή είναι η εισαγωγή του αριθμού της πιστωτικής κάρτας. Πολλοί καταναλωτές είναι ακόμα δύσπιστοι στο κατά πόσο είναι ασφαλές να χρησιμοποιούν την πιστωτική τους κάρτα.

Ο έμπορος μπορεί να είναι κάποιος απατεώνας, ο οποίος θέλει να υποκλέψει πολλούς αριθμούς πιστωτικών καρτών προκειμένου να τις χρησιμοποιήσει για δικά του οφέλη και απλώς δημιούργησε μια ελκυστική σελίδα στο Internet προσφέροντας φθηνά(αλλά ανύπαρκτα) προϊόντα.

Με την ίδια λογική, ο κάτοχος μπορεί να μην είναι ο νόμιμος κάτοχος της κάρτας και απλώς να έχει υποκλέψει τον αριθμό της κάρτας και την ημερομηνία λήξης και να τη

χρησιμοποιεί για την αγορά αγαθών και υπηρεσιών, χρεώνοντας τον λογαριασμό κάποιου άλλους.

Ακόμη και με τη χρήση ειδικής τεχνολογίας SSL (Secure Sockets Layer) δεν είναι απόλυτα εξασφαλισμένη η συναλλαγή μέσω πιστωτικών καρτών στο Internet. Αξίζει να σημειωθεί ότι οι περισσότεροι έμποροι του Internet. Αξίζει να σημειωθεί ότι οι περισσότεροι έμποροι του Internet γράφουν με πολύ μικρά γράμματα ότι η συναλλαγή με πιστωτικές κάρτες δεν είναι απόλυτα εξασφαλισμένη και ότι η χρήση της κάρτας γίνεται με ευθύνη του κατόχου.

Αξίζει ακόμα να τονισθεί ότι με τις σημερινές διαδικασίες, ο κάτοχος μπορεί ακούσια να δεσμευτεί ότι αγόρασε κάποιο προϊόν και να του έλθει η χρέωση στην πιστωτική κάρτα χωρίς να είχε πρόθεση γι'αυτό. Δηλαδή, μέσα απο τις διάφορες σελίδες που βλέπει και απαντά στις ερωτήσεις του εμπόρου, δεν ζητείται με σαφήνεια απο τον κάτοχο αν θέλει να ολοκληρώνει τη συναλλαγή. Οι πιο πολλές επιστροφές που έχουμε σήμερα στις αγορές του Internet αφορούν τέτοιες περιπτώσεις όπου οι κάτοχοι, στην περιπλάνηση τους στις "βιτρίνες" του Internet, άθελα τους αγόρασαν πράγματα που δεν ήθελαν.

Μέχρι το έτος 2000, οι αναλυτές προβλέπουν ότι τα μισά σπίτια στις ΗΠΑ και ένα τρίτο σε Γαλλία, Γερμανία, Ιταλία, Ιαπωνία και Αγγλία θα αγοράζουν on line. Οι ετήσιες πωλήσεις στις ΗΠΑ και την Ευρώπη, που σήμερα είναι περίπου 3,5 δισεκατομμύρια δολάρια, θα φθάσουν το 2000 στα 15-20 δις δολάρια, σύμφωνα με το Forester Research.

Για την εξασφάλιση των on line συναλλαγών δημιουργήθηκε απο τους διεθνείς οργανισμούς Visa και Mastercard η τεχνολογία SET (Secure Electronic Transactions). Το SET σχεδιάστηκε ώστε να εξασφαλίζει τη μέγιστη δυνατή ασφάλεια στις συναλλαγές μέσω καρτών σε οποιοδήποτε on line δίκτυο, περιλαμβανόμενου και του Internet. Με τη χρήση εξαιρετικά προηγμένων ψηφιακών πιστοποιητικών, το SET επιτρέπει την πληρωμή στο Internet κατά τέτοιον τρόπο, που ακόμα και ο έμπορος δεν μαθαίνει τον αριθμό της κάρτας του κατόχου. Επίσης, εξασφαλίζει τόσο στον έμπορο όσο και στον κάτοχο, ότι το άλλο μέρος είναι γνήσιο και η συναλλαγή θα ολοκληρωθεί χωρίς κανένα πρόβλημα. Δηλαδή, τόσο ο έμπορος

θα εισπράξει τα χρήματα του από τον αποδέκτη όσο και ο κάτοχος θα παραλάβει τα αγαθά ή τις υπηρεσίες που πλήρωσε με την κάρτα του.

Η τεχνολογία του SET προστατεύει τις πληρωμές με τέσσερις τρόπους:

- Πρώτον, επιτρέπει στον κάτοχο να πιστοποιήσει ότι ο έμπορος είναι εξουσιοδοτημένος να δέχεται πληρωμές μέσω καρτών, κατά τρόπο ασφαλή με τη χρήση τεχνολογίας SET.
- Δεύτερον, επιτρέπει στον έμπορο, ο οποίος χρησιμοποιεί τεχνολογία SET, να πιστοποιήσει την κάρτα η οποία χρησιμοποιείται για την πληρωμή.
- Τρίτον, η τεχνολογία SET χρησιμοποιεί ένα εξαιρετικά προηγμένο σύστημα κρυπτογράφησης για την προστασία των προσωπικών στοιχείων των συναλλασσομένων.
- Τέταρτον, η τεχνολογία SET εξασφαλίζει ότι οι πληροφορίες που αφορούν την πληρωμή διαβάζονται μόνο απο τον έμπορο και απο την τράπεζα αποδέκτη, οι οποίοι χρησιμοποιούν το σύστημα SET.

Είναι φανερό ότι η τεχνολογία SET εξασφαλίζει με τον καλύτερο δυνατό τρόπο τις συναλλαγές μέσω καρτών σε περιβάλλον on line και θα βοηθήσει σημαντικά στην ανάπτυξη αυτής της δραστηριότητας.

Το σύστημα πληρωμών SET αποτελείται απο τέσσερις εφαρμογές:

- Το πορτοφόλι είναι η εφαρμογή που λειτουργεί στο σύστημα του κατόχου και αποθηκεύει πληροφορίες σχετικά με τον λογαριασμό και επικοινωνεί με τους εμπόρους μέσω του πρωτοκόλλου SET.
- Το POS του εμπόρου είναι η εφαρμογή που συνδέει τον έμπορο με το Πορτοφόλι και το gateway προς τον αποδέκτη.
- Το gateway είναι η εφαρμογή η οποία συνδέει τον έμπορο με το παραδοσιακό σύστημα του αποδέκτη, ο οποίος δίνει την τελική έγκριση για τη συναλλαγή.
- Η πιστοποιούσα αρχή είναι μια εφαρμογή ψηφιακών πιστοποιητικών, η οποία δημιουργεί και διαχειρίζεται τα ψηφιακά πιστοποιητικά ταυτότητας βάσει των προδιαγραφών SET, με τη χρήση κρυπτογραφικών μεθόδων.

ΚΕΦΑΛΑΙΟ 4:
ΕΜΠΟΡΙΚΑ ΔΙΑΘΕΣΙΜΑ ΣΥΣΤΗΜΑΤΑ

ΚΕΦΑΛΑΙΟ 4

4. ΕΜΠΟΡΙΚΑ ΔΙΑΘΕΣΙΜΑ ΣΥΣΤΗΜΑΤΑ

4.1.ΛΟΓΙΣΜΙΚΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ.

4.1.1. RRETTY GOOD PRIVACY(PGP)

Το λογισμικό Pretty Good Privacy (PGP), το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες. Το PGP επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

Διασφάλιση του απορρήτου σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει.

Πιστοποίηση της ταυτότητας σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.
Ευκολία σημαίνει ότι η διασφάλιση του απόρρητου και η πιστοποίησης της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία. Δεν είναι αναγκαία ασφαλή κανάλια για την ανταλλαγή κλειδιών μεταξύ χρηστών κάτι που κάνει το PGP πολύ ευκολότερο στη χρήση από κάθε άλλο αντίστοιχο πακέτο. Αυτό συμβαίνει διότι το PGP είναι βασισμένο σε μια δυναμική νέα τεχνολογία που καλείται κρυπτογράφηση "δημοσίων κλειδιών" (public key).

Το PGP συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με την ταχύτητα της συμβατικής κρυπτογράφησης, περιλήψεις μηνυμάτων για ψηφιακές υπογραφές, συμπίεση δεδομένων πριν την κρυπτογράφηση, καλός εργονομικός

σχεδιασμός και υψηλού επιπέδου διαχείριση κλειδιών. Επιπλέον το PGP εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες.

4.1.2 ADVANCED ENCRYPTION PACKAGE

Το Advanced Encryption Package είναι ένα από τα καλύτερα προγράμματα περιλαμβάνοντας 17 διαφορετικούς αλγόριθμους κρυπτογράφησης. Εύκολο στη χρήση με φιλική προς τον χρήστη διεπιφάνεια, έχει τη δυνατότητα να κρυπτογραφεί αρχεία οποιασδήποτε μορφής, φακέλους, e-mail, ακόμη και σελίδες στον Internet Explorer.

4.1.3 ADVANCED FILE SECURITY

Το Advanced File Security είναι μία ασφαλής και αξιόπιστη μέθοδος για την προστασία δεδομένων από ανεπιθύμητη πρόσβαση. Χρησιμοποιεί τον αλγόριθμο Advanced Encryption Standard για γρήγορη και αξιόπιστη κρυπτογράφηση αρχείων, φακέλων και σκληρών δίσκων. Με την επιλογή του Secure Password Exchange επιτυγχάνεται η ανταλλαγή κρυφών κωδικών μέσω κρυπτογράφησης με τον RSA (2048 bit) αλγόριθμο.

4.1.4 AXCRYPT

Το AxCrypt είναι ένα δωρεάν πρόγραμμα κρυπτογράφησης αρχείων το οποίο είναι αρκετά εύχρηστο και τόσο λιτό που δεν κάνει την παρουσία του εύκολα αισθητή. Λειτουργεί σε όλες τις εκδόσεις των Windows όπως 95, 98, ME, NT, 2000 και XP. Είναι εύχρηστο και ενσωματώνεται στον Windows Explorer. Προσφέρει δυνατή κρυπτογράφηση για τα αρχεία μας χρησιμοποιώντας AES αλγόριθμους με πολύπλοκα κλειδιά μέχρι και των 128-bit. Με τη κρυπτογράφηση, το αρχείο θα αλλάξει μορφή και θα του προστεθεί η κατάληξη ".axx

4.1.5 TRUE CRYPT

Εφαρμογή για τη δημιουργία εικονικών κρυπτογραφημένων δίσκων στον υπολογιστή. Με το πρόγραμμα αυτό μπορεί να κρυπτογραφηθεί ένας ολόκληρος σκληρός δίσκος, μια κίνηση λάμψης USB, ή ακόμα και να δημιουργηθεί ένας εικονικός κρυπτογραφημένος δίσκος σε ένα αρχείο που ενεργεί ως πραγματικός δίσκος.

Το πλεονέκτημα του TrueCrypt είναι ότι μπορεί να δημιουργηθεί ένας εικονικός δίσκος στον υπολογιστή που θα κοιτάξει και θα αισθανθεί ακριβώς όπως ένας κανονικός δίσκος. Ένα αρχείο αποθηκεύεται στον υπολογιστή, αλλά κρυπτογραφείται εντελώς και εξασφαλίζει, έτσι ώστε όταν κλείνει ο υπολογιστής , τα στοιχεία ΔΕΝ ΜΠΟΡΟΥΝ να ανακτηθούν εκτός αν είναι γνωστός ο σωστός κωδικός πρόσβασης. Φυσικά, αυτό σημαίνει ότι εάν ξεχαστεί ο κωδικός πρόσβασής , τα στοιχεία θα χαθούν για πάντα. .Το κρυπτογραφημένο αρχείο λειτουργεί ως δίσκος και μπορεί να μεταφερθεί (ανάλογα με το μέγεθός του) σε ένα usb flash disk. Με αυτόν τον τρόπο, τα δεδομένα δεν μπορούν να διαβαστούν αν δεν χρησιμοποιηθεί το πρόγραμμα TrueCrypt και ο κατάλληλος κωδικός.

Ακόμα και τα περιεχόμενα ενός email μπορούν να κρυπτογραφηθούν με αυτόν τον τρόπο. Δημιουργείται ένα μικρό κρυπτογραφημένο αρχείο (πχ. μεγέθους 300kb) με το TrueCrypt, στο οποίο εισάγουμε για παράδειγμα ένα αρχείο(πχ. μεγέθους 200kb). Μπορούμε μετά να εισάγουμε το κρυπτογραφημένο αρχείο-δίσκο των 300kb ως επισυναπτόμενο αρχείο σε email που θα αποσταλεί. Κανένας ενδιάμεσος σταθμός δεν θα μπορεί να το διαβάσει αν δε διαθέτει τον κατάλληλο κωδικό

4.1.6 CRYPTOEXPERT

Εφαρμογή κρυπτογράφησης που δίνει τη δυνατότητα δημιουργίας μιας σειράς από εικονικούς κρυπτογραφημένους δίσκους για την ασφαλή αποθήκευση των αρχείων. Η κρυπτογράφηση γίνεται σε περιβάλλον 128bit.

4.1.7 CRYPTOCRAT

Το CryptoCrat κρυπτογραφεί αρχεία και φακέλους χρησιμοποιώντας όλους τους γνωστούς αλγόριθμους (Advanced Encryption Standard (Rijndael), GOST, Twofish,

Serpent, MARS, Diamond2) χρησιμοποιώντας απλές παραθυρικές οθόνες και η επιλογή αρχείων προς κρυπτογράφηση πραγματοποιείται απλά με δεξί κλικ πάνω στα αρχεία.

4.1.8 ΆΛΛΑ ΠΡΟΓΡΑΜΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Ομοίως με τα προαναφερθέντα υπάρχουν πολλά άλλα προγράμματα κρυπτογράφησης τα οποία εξυπηρετούν με τον ίδιο τρόπο τον χρήστη. Μερικά από αυτά είναι:

- DriveCrypt
- Cryptainer LE
- CryptoMite
- KPKFile
- Efsinfo
- BitCrypt Free
- CrossCrypt
- Advanced File Security
- Private Disk
- Zero Footprint Crypt
- Universal Shield

4.2.ΛΟΓΙΣΜΙΚΟ ΥΔΑΤΟΓΡΑΦΗΣΗΣ

4.2.1.ΨΗΦΙΑΚΗ ΥΔΑΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ ΕΙΚΟΝΑΣ

Ένας από τους τομείς της υδατογραφίας είναι και η υδατογράφηση ψηφιακών εικόνων. Η προστασία των εικόνων έχει γίνει αρκετές φορές αντικείμενο μελέτης και οι περισσότεροι αλγόριθμοι που χρησιμοποιούνται στην ψηφιακή υδατογράφηση είναι παραλλαγές των αλγόριθμων εικόνας. Υπάρχουν πολλές εταιρίες που δραστηριοποιούνται στον χώρο της υδατογράφησης εικόνας μερικές από τις οποίες είναι οι ακόλουθες :

- Alpha Tec Ltd : στο χώρο της ψηφιακής υδατογράφησης εικόνων προτείνει το EikonaMark και το Alphacrawler. Το EikonaMark αποτελεί ένα εξειδικευμένο προϊόν λογισμικού για την ενσωμάτωση και την ανίχνευση "ορατών" & "αόρατων" υδατογραφημάτων στο ψηφιακό περιεχόμενο των εικόνων. Ο Alphacrawler είναι μία αυτοματοποιημένη μηχανή σάρωσης του Διαδικτύου και αξιοποιείται, κατά κύριο λόγο, στις υπηρεσίες προστασίας του δικαιώματος αναπαραγωγής και πιστοποίησης των ψηφιακών εικόνων.
- Digimarc : Η παρουσία της Digimarc στην αγορά της προστασίας των πνευματικών δικαιωμάτων εκφράζεται με το πιο διάσημο προιόν της το ImageBridge.Ο ρόλος του είναι να τοποθετεί και να ανιχνεύει ανθεκτικά υδατογραφήματα στο ψηφιακό περιεχόμενο των εικόνων που θέλει να προστατέψει.
- MarkAny : Είναι μία εταιρεία με έδρα την Κορέα και αντικείμενο την προστασία και διαχείριση των δικαιωμάτων πνευματικής ιδιοκτησίας ψηφιακού υλικού. Το προϊόν που διατίθεται εμπορικά από την MarkAny είναι το MAIM 2.0. Η λειτουργικότητα που προσφέρει το MAIM 2.0 είναι η προστασία του δικαιώματος αναπαραγωγής για λογαριασμό των δημιουργών εικόνων, κωδικοποιώντας ενδεικτική πληροφορία στο εσωτερικό τους. Συγκεκριμένα, το MAIM 2.0 επιτρέπει στους διανομείς ψηφιακών εικόνων να δημοσιοποιούν το περιεχόμενο τους χωρίς να ανησυχούν για ενδεχόμενα κρούσματα παράνομης αντιγραφής και διανομής του.
- MediaSec : Η MediaSec Technologies δραστηριοποιείται στο χώρο της σχεδίασης, της ανάπτυξης και της εμπορικής εκμετάλλευσης προϊόντων και λύσεων που στηρίζονται σε τεχνικές απόκρυψης πληροφορίας και ως επί το πλείστον στην ψηφιακή υδατογραφία Από τα προϊόντα που διατίθενται εμπορικά, αυτό που αφορά ψηφιακές εικόνες είναι το MediaSign Digital. : Πρόκειται για ένα προϊόν που παρέχει ασφάλεια και συνιστά μια συμφέρουσα λύση για την προστασία ψηφιακών αρχείων εικόνας και βίντεο, έναντι μη εξουσιοδοτημένων χρήσεων και τροποποιήσεων.
- Sealtronic: Η Sealtronic όπως και η MarkAny είναι μια εταιρεία που εδρεύει στην Κορέα και δραστηριοποιείται στο χώρο της αξιοποίησης ψηφιακού υλικού. Το προϊόν της οικογένειας MagicTag που προτείνεται για την προστασία των πνευματικών δικαιωμάτων ψηφιακών εικόνων είναι το MT

Image. Το MT Image ενσωματώνει ανθεκτικά αόρατα υδατογραφήματα στα pixels μιας ψηφιακής εικόνας.

- Signum Technologies: Η εταιρεία Signum Technologies δραστηριοποιείται στην αγορά την προστασίας των πνευματικών δικαιωμάτων με μία σημαντική αλυσίδα από προϊόντα. . Η αλυσίδα των προϊόντων υδατογράφησης της Signum φέρει το πρόθεμα SureSign και περιλαμβάνει τα ακόλουθα: SureSign Enterprise: Αποτελεί μία αρκετά ισχυρή εφαρμογή που παρέχει τη δυνατότητα αυτοματοποιημένης υδατογράφησης εικόνων, SureSign Image SDK, είναι η πλατφόρμα ανάπτυξης λογισμικού που παρέχεται από τη Suresign και δίνει την ευκαιρία στον αναλυτή προγραμματιστή να ενσωματώσει τις υπηρεσίες υδατογράφησης στο σύστημα διαχείρισης εικόνων που χρησιμοποιεί, χωρίς να είναι αναγκαία η χρήση της παραθυρικής εφαρμογής.

4.2.2.ΨΗΦΙΑΚΗ ΥΔΑΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ ΗΧΟΥ

Τον τελευταίο καιρό τα ψηφιακά αρχεία ήχου έχουν γίνει αντικείμενο εκμετάλλευσης και παράνομης αντιγραφής από τους χρήστες του διαδικτύου. Η λύση της υδατογράφησης είναι ικανή να εντοπίσει μία παράνομη χρήση και να στηρίξει μία κατηγορία εναντίον του παραβάτη. Οι εταιρίες που δραστηριοποιούνται στην ψηφιακή υδατογράφηση αρχείων ήχου, πολλές από τις οποίες δραστηριοποιούνται και στην ψηφιακή εικόνα, είναι :

- Alpa Tec Ltd : Για την προστασία των ψηφιακών αρχείων ήχου προτείνει το AudioMark. Αποτελεί το προϊόν που σχεδιάστηκε από την Alpha Tec. για την ενσωμάτωση υδατογραφημάτων σε ψηφιακά αρχεία ήχου και τη μετέπειτα ανίχνευσή τους.
- Blue Spike : Η Blue Spike είναι μια εταιρεία που απευθύνεται σε εκείνους που δημιουργούν, παράγουν, δημοσιοποιούν και διανέμουν ψηφιακά μουσικά έργα. . Το προϊόν φέρει το όνομα Giovanni .Πρόκειται για ένα αρκετά ισχυρό εργαλείο, ιδιαίτερα χρήσιμο στις εταιρείες που πραγματοποιούν πωλήσεις μέσω του Διαδικτύου.
- MarkAny: Σε αντιστοιχία με το MAIM 2.0 η MarkAny για τη ψηφιακή υδατογράφηση αρχείων ήχου προτείνει το προϊόν MAO 2.0. Πρόκειται για

ένα εργαλείο που κωδικοποιεί πληροφορία πνευματικής ιδιοκτησίας μέσα στο περιεχόμενο των αρχείων ήχου.

- Sealtronic: Ακόμα μία εταιρεία που πέρα από τις ψηφιακές εικόνες προτείνει λύσεις και για τα ψηφιακά αρχεία ήχου είναι η Sealtronic. Το προϊόν υδατογράφησης μουσικών έργων που λανσάρει ανήκει επίσης στην οικογένεια MagicTag και φέρει το όνομα MT Audio.
- Verance: είναι μια εταιρεία που δραστηριοποιείται στο χώρο της αξιοποίησης ψηφιακού περιεχομένου και προσφέρει καινοτόμες λύσεις, βασισμένες στην τεχνολογία της υδατογράφησης, με στόχο την προστασία, τη διαχείριση και την εποπτεία ηχητικού και οπτικοακουστικού υλικού. Τα προϊόντα λογισμικού που διατίθενται συνοδευτικά με τις άδειες τοποθέτησης και ανίχνευσης υδατογραφημάτων είναι τα ακόλουθα: Verance Audio Watermark Embedder: Το εργαλείο που προσφέρει η Verance είναι αρκετά αξιόπιστο και προτείνεται από το SDMI (Secure Digital Music Initiative) ως η πιο αποτελεσματική τεχνολογία υδατογράφησης για την προστασία μουσικών έργων. Ενσωματώνει ένα μοναδικό αναγνωριστικό κώδικα στην κυματομορφή του ηχητικού σήματος. Verance Audio Watermark Detector: Πρόκειται για το αντίστοιχο εργαλείο της εταιρείας που χρησιμοποιείται για την ανίχνευση των υδατογραφημάτων σε ψηφιακά αρχεία ήχου.

4.2.3 ΨΗΦΙΑΚΗ ΥΔΑΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ ΒΙΝΤΕΟ

Τα ψηφιακά αρχεία βίντεο θα μπορούσε κανείς να ισχυριστεί ότι ένα υπερσύνολο των παραπάνω, καθώς μπορούν να ιδωθούν ως συνδυασμός εικόνων και ηχητικών θεμάτων. Οι αλγόριθμοι υδατογράφησης που χρησιμοποιούνται για τη προστασία αρχείων εικόνας και ήχου θα μπορούσαν παράλληλα, να χρησιμοποιηθούν και για την προστασία αρχείων βίντεο. Πράγματι, ένας τετριμμένος αλγόριθμος θα μπορούσε να χρησιμοποιήσει τις μεθόδους υδατογράφησης εικόνας για να τοποθετήσει υδατογραφήματα στα διαδοχικά καρέ που συνθέτουν το αρχείο βίντεο, ή αντίστοιχα να απομονώσει τον ήχο και να τον χρησιμοποιήσει ως είσοδο σε ένα εργαλείο υδατογράφησης ψηφιακών αρχείων ήχου. Τα παραπάνω επαληθεύονται και από την αγορά, καθώς οι λύσεις που προτείνονται για τη ψηφιακή υδατογράφηση αρχείων

βίντεο προέρχονται από εταιρείες που διαθέτουν αντίστοιχα προϊόντα για εικόνες και μουσικά έργα.

4.2.4 ΆΛΛΑ ΠΡΟΓΡΑΜΜΑΤΑ ΥΔΑΤΟΓΡΑΦΗΣΗΣ

Ομοίως με τα προαναφερθέντα υπάρχουν πολλά άλλα προγράμματα υδατογράφησης τα οποία εξυπηρετούν με τον ίδιο τρόπο τον χρήστη. Μερικά από αυτά είναι:

- iWatermark
- Easy Watermark Creator
- Watermark Factory
- Visual Watermark
- WatermarkIt

4.3. ΛΟΓΙΣΜΙΚΟ ΣΤΕΓΑΝΟΓΡΑΦΙΑΣ

Στα ψηφιακά δεδομένα, η στεγανογραφία βρίσκει εφαρμογή στην απόκρυψη οποιουδήποτε αρχείου σε κάποιο άλλο αρχείο της ίδιας η άλλης μορφής (format). Τα προγράμματα που υλοποιούν αυτην την εφαρμογή είναι :

- Snow: Το συγκεκριμένο εργαλείο υλοποιεί την τεχνική κωδικοποίησης πληροφορίας με την χρήση των κενών χαρακτήρων.
- Hide in Picture: Εφαρμογή η οποία δίνει τη δυνατότητα να «κρυφτούν» αρχεία μέσα σε εικόνες τύπου .bmp ή .gif.
- wbStego: Εφαρμογή η οποία δίνει τη δυνατότητα να κρυπτογραφηθούν και να στεγανοποιηθούν δεδομένα μέσα σε άλλα αρχεία, όπως εικόνες τύπου bitmap(bmp), αρχεία κειμένου (txt), ιστοσελίδες (html) και αρχεία κειμένου (pdf).
- Hermetic Stego : είναι ακόμη μία απλή εφαρμογή για απόκρυψη αρχείων μέσα σε εικόνες.

4.3.1. ΆΛΛΑ ΠΡΟΓΡΑΜΜΑΤΑ ΣΤΕΓΑΝΟΓΡΑΦΙΑΣ

Ομοίως με τα προαναφερθέντα υπάρχουν πολλά άλλα προγράμματα στεγανογραφίας τα οποία εξυπηρετούν με τον ίδιο τρόπο τον χρήστη. Μερικά από αυτά είναι:

- Camouflage
- dc-Steganograph
- Empty Pic
- EzStego
- Hide and Seek
- Hide Unhide
- In Plain View
- jpeg-jsteg
- Stegotif
- Stext
- TextHide
- Textego
- StegParty

ΚΕΦΑΛΑΙΟ 5:
ΣΥΜΠΕΡΑΣΜΑΤΑ

ΚΕΦΑΛΑΙΟ 5

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στη σημερινή εποχή η ψηφιακή τεχνολογία έχει κυριεύσει τη ζωή μας και το internet από μικρό δίκτυ επικοινωνίας έχει εξαπλωθεί σε παγκόσμια κλίμακα και έχει εξελιχθεί σε υπερδίκτυο διανομής πληροφοριών.

Χάρη στην ψηφοποίηση των πληροφοριών, στην ανάπτυξη των αποθηκευτικών μέσων και την δημιουργία δικτύων υπολογιστών η πρόσβαση σε κάθε είδους πληροφορία γίνεται ευκολότερη με μικρότερο κόστος. Αυτό δημιουργεί ποικίλους προβληματισμούς καθώς η ευκολία αντιγραφής και διανομής ψηφιακού περιεχομένου, χωρίς επιπτώσεις στην ποιότητα, οδηγεί στην ανεξέλεγκτη πειρατεία. Γι' αυτό κρίνεται αναγκαία η δημιουργία Συστημάτων για την Διαχείριση των Ψηφιακών Δικαιωμάτων.

Μεγάλες εταιρείες διαθέτουν στην αγορά λογισμικά τα οποία προσπαθούν με τεχνολογικά μέσα προστασίας να διασφαλίσουν τα πνευματικά δικαιώματα των δημιουργών και να περιορίσουν την πειρατεία. Οι κυβερνήσεις και διάφοροι οργανισμοί από την πλευρά τους προσπαθούν να αντιμετωπίσουν το πρόβλημα δίνοντας βάση στη νομική πλευρά του θέματος. Ο χρήστης συνδέει την προστασία των πνευματικών δικαιωμάτων με την απαγόρευση της ελεύθερης διακίνησης πληροφοριών στο διαδίκτυο και θεωρεί τον όρο αρνητικό. Υπάρχουν όμως περιπτώσεις, όπως σε θέματα της πολιτισμικής μας κληρονομιάς, όπου η προστασία των πνευματικών δικαιωμάτων είναι επιτακτική.

Για το ζήτημα της προστασίας και της διαχείρισης των πνευματικών δικαιωμάτων , απαιτείται προτυποποίηση των τεχνολογιών που χρησιμοποιούνται και η δημιουργία νέων συστημάτων, εφαρμογών και υπηρεσιών. Στο μέλλον η ανάγκη για ασφάλεια θα παίζει σημαντικό ρόλο στον σχεδιασμό και την υλοποίηση υπολογιστικών συστημάτων. Ως πιθανότερη εξέλιξη θεωρείται η ανάπτυξη και η υιοθέτηση

συστημάτων, που θα βασίζονται στο υλικό και θα ενσωματώνουν διαδικασίες ελέγχου της Πνευματικής Ιδιοκτησίας καθ' όλη τη λειτουργία τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Οδηγός – Εγχειρίδιο για την προστασία και διαχείριση των πνευματικών δικαιωμάτων ψηφιακού πολιτιστικού περιεχομένου. Α. Σκόδρας, Σ. Νικολόπουλος, Ε. Καρατζάς, Δ. Τσώλης, Δ. Μεϊδάνης, Πάτρα 2004
- Τα Δικαιώματα Πνευματικής Ιδιοκτησίας στην Ψηφιακή Εποχή:Ζητήματα Προστασίας και Διαχείρισης. Ένα Πρότυπο Σύστημα Ψηφιακής Διαχείρισης των Πνευματικών Δικαιωμάτων
- (http://www.infosoc.gr/meletes/)
- Arms William, The online edition of Digital Libraries: Chapter 7 Access management and security, MIT Press:2000 (updated with additional material by the author)
- http://www.cs.cornell.edu/wya/DigLib/new/Chapter7.html
- Gladney H.M and Bennett J.L, *What do we mean by Authentic?* D-Lib Magazine, July/August 2003, Volume 9 Number 7/8 ISSN 1082-9873.
- http://www.dlib.org/dlib/july03/gladney/07gladney.html
- Encryption Technology Windows on Computing, No. 22, University of Washington Computing & Communications Winter 1999
- http://www.washington.edu/computing/windows/issue22/encryption.html
- Brown Lawrie Cryptography and Computer Security - Cryptography Lecture 12 Modern Stream Ciphers November 2001
- http://www.cs.adfa.edu.au/courses/ACSC2010/coursework/lectures/ss-less12.html
- http://www.dlib.org/dlib/december97/ibm/12lotspiech.html
- Steganography and Digital Watermarking Tool Table
- http://www.jjtc.com/Steganography/toolmatrix.htm
- Μάγκος Εμμανουήλ *Ασφάλεια στο World Wide Web* Πειραιάς 1997
- http://thalis.cs.unipi.gr/~emagos/THE%20WHOLE%20THING%201.pdf
- Μάγκος Κ. και Νιξαρλίδης Α. *Ασφάλεια στο διαδίκτυο (Κεφάλαιο 3ο)* Ιούλιος 1999
- http://www.lab.epmhs.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio3.htm
- Καλουπτσίδης και άλλοι. Ανάλυση και Σχεδιασμός Συμμετρικών Κρυπτογραφικών Αλγορίθμων Αθήνα, ΕΚΠΑ 31/10/2001
- http://www.army.gr/html/GR_Army/drasi/synedrio_programma.html
- Χαλάτσης Κ. Κρυπτογραφία – Σύγχρονες Τάσεις. (διαθέσιμο από την διεύθυνση του συνεδρίου, δεύτερη ημέρα 4η θεματική ενότητα)
- http://www.army.gr/html/GR_Army/drasi/synedrio_programma.html

- Encyclopedia4u.com Cryptography και σχετικές με αλγορίθμους συνδέσεις
- http://www.encyclopedia4u.com/c/cryptography-1.html
- Trust and Technologies for Copyright Protection and Management, Dimitrios K. Tsolis, Theodore S. Papatheodorou, 1st International Conference on Trust Management 28 - 30 May 2003, Heraklion, Crete, Greece
- Μελέτη/Αξιολόγηση ανθεκτικής μεθόδου Υδατογράφησης ψηφιακών εικόνων και ενσωμάτωση της μεθόδου στη ανάπτυξη συστήματος προστασίας και διαχείρισης των Πνευματικών Δικαιωμάτων ψηφιακού περιεχομένου, βασισμένου σε τεχνολογίες XML, Μεταπτυχιακή Εργασία – Νικολόπουλος Ν. Σπυρίδων, Μεταπτυχιακό Δίπλωμα Ειδίκευσης – Επιστήμη & Τεχνολογία Υπολογιστών, Πανεπιστήμιο Πατρών 2004.
- Digital Watermarking, Ingerman J. Cox, Matthew L. Miller. Jefrey A. Bloom, Morgan Kaufman Publishers
- Digital Rights Manegement (DRM) Architectures, Renato Iannella, D-Lib Magezine Article, Volume 7 Number 6, June 2001.
- Digital Object Identifier, http://www.doi.org/
- Digital Rights Management Workshop, http://www.w3.org/2000/12/drm-ws/
- Open Digital Rights Language (ODRL), Renato Iannella, 2002-08-08
- Rights Management: Managing the Layers of Rights and Roles in the Knowledge Based Economy, Peter Higgs, 2000, IPR Systems Report
- http://www.iprsystems.com/assets/0.2_Rights_Management.pdf
- Electronic Book Exchange, http://www.ebxwg.org/
- Τεχνικές ανάπτυξης λογισμικού για την προστασία, διαχείριση και αξιοποίηση της πνευματικής ιδιοκτησίας σε πληροφοριακά συστήματα διαδικτύου και ηλεκτρονικού εμπορίου", Δημήτριος Κ. Τσώλης, Πανεπιστήμιο Πατρών, Φεβρουάριος 2004
- Copyright Clearance Center – CCC, http://www.copyright.com/
- http://www.watermarkingworld.org/optimark/index.html