ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (MSc)

ΣΤΑ ΔΙΚΤΥΟΚΕΝΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Κ. ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
"ΔΙΑΧΕΙΡΙΣΗ ΨΗΦΙΑΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ"

ΕΠΙΜΕΛΕΙΑ ΕΡΓΑΣΙΑΣ:
ΚΟΥΡΙΔΟΥ ΑΝΑΣΤΑΣΙΑ ΜΕ0678

Πειραιάς, Νοέμβριος 2008

ΠΕΡΙΛΗΨΗ

Στη σημερινή εποχή η ψηφιακή τεχνολογία έχει κυριεύσει τη ζωή μας και το Internet από μικρό δίκτυο επικοινωνίας έχει εξαπλωθεί σε παγκόσμια κλίμακα και έχει εξελιχθεί σε υπερδίκτυο διανομής πληροφοριών. Μέσω του Διαδικτύου διακινούνται εύκολα και αποτελεσματικά μεγάλοι όγκοι δεδομένων και στοιχείων που αφορούν κάθε είδους πληροφορία. Η πρόσβαση στην πληροφορία γίνεται ευκολότερη χάρη στην ψηφιοποίησή της, στην ανάπτυξη ψηφιακών αποθηκευτικών μέσων και τη δημιουργία δικτύων υπολογιστών με αποκορύφωμα τον παγκόσμιο ιστό. Παρόλα αυτά, οι ραγδαίες αυτές εξελίξεις προκαλούν ποικίλους προβληματισμούς. Η ευκολία αντιγραφής και διανομής ψηφιακού περιεχομένου, χωρίς επιπτώσεις στην ποιότητα, οδήγησε στην ανεξέλεγκτη πειρατεία. Πιο συγκεκριμένα οι εξελίξεις στην τεχνολογία έχουν μεγάλη επίδραση στην ικανότητα διανομής και αναπαραγωγής της πληροφορίας και επίσης θέτουν σε κίνδυνο την εφαρμογή των νόμων της Πνευματικής Ιδιοκτησίας σε ψηφιακά περιβάλλοντα.

Στα πλαίσια της παρούσας Διπλωματικής Εργασίας μελετάται το ζήτημα της διαχείρισης των Πνευματικών Δικαιωμάτων στον ψηφιακό κόσμο, με στόχο την εξάλειψη των κινδύνων και την προστασία της Πνευματικής Ιδιοκτησίας. Συγκεκριμένα, προτείνονται τα Συστήματα Ψηφιακής Διαχείρισης Δικαιωμάτων (DRM) ως μέσα προστασίας του copyright και υποστήριξης της διανομής του ψηφιακού περιεχομένου μέσω των δικτύων και του Διαδικτύου, για την αποφυγή περιπτώσεων παραβίασης του νόμου της Πνευματικής Ιδιοκτησίας. Αρχικά μελετώνται τα χαρακτηριστικά των DRM συστημάτων και αναλύονται πλήρως οι τεχνολογικές τους παράμετροι, όπως για παράδειγμα τεχνολογίες μεταδεδομένων, τεχνολογίες κρυπτογράφησης και υδατογράφησης, μέθοδοι μοναδικής αναγνώρισης, γλώσσες έκφρασης δικαιωμάτων και τεχνολογίες πληρωμών.

Τέλος ακολουθεί μια συνοπτική περιγραφή των κυριότερων προϊόντων, ανά κατηγορία περιεχομένου. Ο στόχος της περιγραφής δεν είναι να αξιολογήσει συγκριτικά τα διαθέσιμα συστήματα, αλλά να αναδείξει μερικά από τα επιμέρους λειτουργικά και τεχνικά χαρακτηριστικά τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1
ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγικά Στοιχεία

Στη σημερινή εποχή η ψηφιακή τεχνολογία έχει κυριεύσει τη ζωή μας και το Internet από μικρό δίκτυο επικοινωνίας έχει εξαπλωθεί σε παγκόσμια κλίμακα και έχει εξελιχθεί σε υπερδίκτυο διανομής πληροφοριών. Μέσω του Διαδικτύου διακινούνται εύκολα και αποτελεσματικά μεγάλοι όγκοι δεδομένων και στοιχείων που αφορούν κάθε είδους πληροφορία, έργα και εισφορές καλλιτεχνών. Ιδιώτες, καλλιτέχνες, επιχειρήσεις, οργανισμοί αλλά και υπουργεία δημιουργούν τη δική τους ιστοσελίδα, ενώ στο διαδίκτυο προωθούνται συνεχώς νέοι τρόποι επενδύσεων.

Η ραγδαία ανάπτυξη του Διαδικτύου και η αυξημένη χρήση ψηφιακής πληροφορίας, οδηγούν σε νέες μορφές επικοινωνίας και εξερεύνησης. Το Διαδίκτυο διαθέτει μια μεγάλη δύναμη, την άμεση διακίνηση της ψηφιακής πληροφορίας. Για το λόγο αυτό ο παγκόσμιος ιστός πήρε μεγάλες διαστάσεις, λειτουργώντας τόσο ως κανάλι διανομής πληροφοριών όσο και ως μέσο διασκέδασης.

Την επανάσταση στο χώρο της τεχνολογίας πληροφόρησης έφεραν οι τεχνολογικές εξελίξεις των τελευταίων ετών. Η πρόσβαση στην πληροφορία γίνεται ευκολότερη χάρη στην ψηφιοποίησή της, στην ανάπτυξη ψηφιακών αποθηκευτικών μέσων και τη δημιουργία δικτύων υπολογιστών με αποκορύφωμα τον παγκόσμιο ιστό. Ως αποτέλεσμα ένας μεγάλος όγκος δεδομένων, όπως μουσικά αρχεία, ταινίες, επιστημονικά άρθρα, φωτογραφίες, διακινούνται εύκολα μέσω Internet και είναι διαθέσιμα σε οποιονδήποτε. Ο Παγκόσμιος Ιστός παρέχει

ελεύθερη πρόσβαση σε πληροφορίες σε εκατομμύρια ανθρώπους που πριν δεν είχαν την δυνατότητα να το κάνουν

Παρόλα αυτά, οι ραγδαίες αυτές εξελίξεις προκαλούν ποικίλους προβληματισμούς. Η ευκολία αντιγραφής και διανομής ψηφιακού περιεχομένου, χωρίς επιπτώσεις στην ποιότητα, οδήγησε στην ανεξέλεγκτη πειρατεία. Πιο συγκεκριμένα οι εξελίξεις στην τεχνολογία έχουν μεγάλη επίδραση στην ικανότητα διανομής και αναπαραγωγής της πληροφορίας και επίσης έχουν καταστήσει αναγκαία την προσαρμογή των νόμων της πνευματικής ιδιοκτησίας, ώστε να μπορούν να εφαρμοστούν και στα ψηφιακά περιβάλλοντα.

Τα DRM συστήματα, αρχικό στόχο είχαν τη «διαχείριση των ψηφιακών δικαιωμάτων». Στην πορεία αποδεικνύεται ότι στο μέλλον ένα πλήρες DRM θα πραγματοποιεί «ψηφιακή διαχείριση των πνευματικών δικαιωμάτων». Δηλαδή δεν θα χειρίζεται μόνο τα δικαιώματα που απορρέουν από την ψηφιακή υπόσταση ενός έργου, αλλά όλα τα πνευματικά δικαιώματα που συνδέονται με αυτό. Συνεπώς, η σωστότερη μετάφραση του DRM συστήματος, είναι «Σύστημα Ψηφιακής Διαχείρισης των Πνευματικών Δικαιωμάτων».

Στις επόμενες παραγράφους θα παρουσιαστούν πιο αναλυτικά οι παράγοντες που θέτουν σε κίνδυνο τα πνευματικά δικαιώματα και προκαλούν προβλήματα στην εφαρμογή των νόμων που διέπουν την Πνευματική Ιδιοκτησία.

1.2 Ψηφιακά Αποθηκευτικά Μέσα – Απελευθέρωση Από το Φυσικό Μέσο

Τα ψηφιακά αποθηκευτικά μέσα, όπως σκληροί δίσκοι, οπτικά μέσα (CDs και DVDs), USB sticks, κάρτες μνήμης, έχουν τη δυνατότητα να αποθηκεύσουν μεγάλες ποσότητες δεδομένων, τα οποία συγχρόνως αποτελούν πνευματική

ιδιοκτησία. Καθώς η ικανότητα αποθήκευσης πληροφορίας σε ψηφιακή μορφή έχει αυξηθεί, τα παραδοσιακά αναλογικά μέσα αποθήκευσης, π.χ. βιβλία, πίνακες ζωγραφικής, έχουν πλέον αντικατασταθεί σε μεγάλο βαθμό. Η αντιγραφή της πληροφορίας πάντα ήταν δυνατή, αλλά η εμφάνιση της ψηφιακής πληροφορίας επιφέρει μια πρωτόγνωρη αύξηση στον όγκο της πληροφορίας που μπορεί εύκολα και με χαμηλό κόστος να αναπαραχθεί. Δεδομένης μάλιστα και την ευρείας διαθεσιμότητας των προσωπικών υπολογιστών, δημιουργείται ένας κόσμος στον οποίο οι άνθρωποι έχουν τη δυνατότητα να αναπαραγάγουν μεγάλο όγκο ψηφιακής πληροφορίας. Εκτός αυτού τα ψηφιακά αντίγραφα που δημιουργούνται αποτελούν πιστά αντίγραφα του πρωτότυπου και συνεπώς διατηρούν την ποιότητα του πρωτότυπου. Συνεπώς έτσι είναι πολύ εύκολη η παραβίαση της πνευματικής ιδιοκτησίας, καθώς η διατήρηση της ποιότητας δεν προσφέρει έναν φυσικό περιορισμό στην αναπαραγωγή.

Όπως προαναφέρθηκε, οι προσωπικοί υπολογιστές παρέχουν εκτεταμένες δυνατότητες δημιουργίας ενός ή και περισσότερων ψηφιακών αντιγράφων. Η δυνατότητα εύκολης αντιγραφής και μεταφοράς της πληροφορίας στην ψηφιακή της μορφή την καθιστά ανεξάρτητη από το μέσο αποθήκευσης, ενώ στην παραδοσιακή της μορφή δεν μπορεί να μεταφερθεί χωρίς το φυσικό μέσο ή χωρίς να αντιγραφεί. Τα ψηφιακά αντίγραφα δεν αποτελούν πρόβλημα όσο οι πληροφορίες που περιέχουν είναι προσωπικά δεδομένα ή δημιουργίες του ιδιοκτήτη, ενώ καταπατούν τα πνευματικά δικαιώματα όταν πρόκειται για δημιουργίες τρίτων. Επίσης πρόβλημα παρουσιάζεται λόγω της απελευθέρωσης του περιεχομένου από το μέσο που το φέρει. Οι νόμοι της πνευματικής ιδιοκτησίας είναι διαμορφωμένοι για να ισχύουν πάνω σε αναλογικό περιεχόμενο ή περιεχόμενο ενσωματωμένο σε φυσικά μέσα (π.χ. βιβλίο) και έχουν ιδιότητες που συνδέονται με τα φυσικά μέσα. Έτσι η ψηφιακή μορφή της πληροφορίας αλλάζει τις ιδιότητες αυτές και απαιτεί τροποποιήσεις έτσι ώστε οι νόμοι να ανταποκρίνονται σε αυτές.

Εκτός από τη δημιουργία πιστών αντιγράφων, είναι πλέον δυνατή η αποθήκευση υψηλής ποιότητας συμπιεσμένων αρχείων μουσικής ή ταινιών σε διάφορα ψηφιακά μέσα (τεχνολογία ripping). Ο συνδυασμός των εξελιγμένων προσωπικών υπολογιστών, των ψηφιακών αποθηκευτικών μέσων, των web εφαρμογών και της ripping τεχνολογίας, παρέχει τη δυνατότητα να μεταφέρουμε περιεχόμενο από το αρχικό φυσικό μέσο σε άλλα μέσα. Με την ανάπτυξη peer-to-peer εφαρμογών, οι χρήστες μπορούν να μοιράζονται τις συλλογές τους on-line, θέτοντας έτσι σε κίνδυνο τα πνευματικά δικαιώματα των δημιουργών.

1.3 Τροποποίηση Περιεχομένου

Η ψηφιακή πληροφορία είναι πολύ εύκολο να τροποποιηθεί, με την προσθήκη επιπλέον δεδομένων ή την διαγραφή ορισμένων άλλων. Πιο συγκεκριμένα ένα ψηφιακό κείμενο μπορεί να αλλάζει δυναμικά, όπως για παράδειγμα ένα άρθρο μπορεί να ανανεώνεται με την προσθήκη σχολίων ή διορθώσεων. Όμως στον αναλογικό κόσμο ένα βιβλίο περιέχει ακριβώς το ίδιο περιεχόμενο με τις ίδιες λέξεις κάθε φορά και ένα μουσικό κομμάτι ενός δίσκου είναι πάντα το ίδιο κάθε φορά που ακούγεται.

Επίσης η ψηφιακή πληροφορία εύκολα συγκρίνεται και αναλύεται. Εκτός αυτού είναι πολύ εύκολο να γίνει αναζήτηση συγκεκριμένων στοιχείων σε ένα ψηφιακό κείμενο μέσω των εργαλείων αναζήτησης που παρέχονται, ενώ αντίστοιχα σε ένα βιβλίο είναι πολύ δύσκολο να ανακαλύψει κανείς αν περιλαμβάνεται μια συγκεκριμένη λέξη.

Τέλος, στον κόσμο της μουσικής, η ευκολία αναζήτησης και αναπαραγωγής της ψηφιακής πληροφορίας έχει οδηγήσει στην τρομακτική αύξηση της δειγματοληψίας (sampling). Αυτό έχει ως αποτέλεσμα την εύκολη επαναχρησιμοποίηση κομματιών προηγούμενων έργων, χωρίς απαραίτητα να τηρούνται οι νόμοι που διέπουν την πνευματική ιδιοκτησία.

Όλα αυτά έχουν ως αποτέλεσμα να είναι πολύ δύσκολο να προστατευθούν τα δικαιώματα που έχουν οριστεί για κάποιο συγκεκριμένο περιεχόμενο, αν αυτό υποστεί κάποιες αλλαγές, έστω και αν αυτές είναι πολύ μικρές.

1.4 Ταυτόχρονη Πρόσβαση και Πρόσβαση Από Απόσταση

Με την ανάπτυξη των δικτύων υπολογιστών παρέχεται πλέον η δυνατότητα ταυτόχρονης πρόσβασης σε περιεχόμενο. Πιο συγκεκριμένα πάρα πολλοί χρήστες μπορούν να προσπελαύνουν το ίδιο περιεχόμενο ταυτόχρονα, χωρίς να επηρεάζεται ο ένας από τον άλλο, ενώ με το αναλογικό περιεχόμενο δεν ίσχυε κάτι τέτοιο. Για παράδειγμα ένα βιβλίο δεν γίνεται να το διαβάζουν ταυτόχρονα περισσότεροι από έναν άνθρωπο ταυτόχρονα. Επίσης οι τεχνολογικές εξελίξεις στον τομέα των υπολογιστών προσφέρουν πλέον την δυνατότητα πρόσβασης σε περιεχόμενο από απόσταση. Ενώ με τα παραδοσιακά μέσα υπήρχαν περιορισμοί πρόσβασης σε πληροφορίες λόγω απόστασης, πλέον είναι δυνατή η προσπέλαση απομακρυσμένου περιεχομένου. Αυτό έχει ως αποτέλεσμα ότι εξαλείφεται ένας ακόμη περιορισμός που εμπόδιζε την παραβίαση της πνευματικής ιδιοκτησίας.

1.5 Ταχύτητα Διανομής

Σήμερα, οι ηλεκτρονικοί υπολογιστές βρίσκονται διασυνδεδεμένοι σε δίκτυα που επιτρέπουν τη ραγδαία και χαμηλού κόστους διακίνηση της πληροφορίας. Με τεράστια ταχύτητα μεγάλοι όγκοι δεδομένων διακινούνται ανάμεσα σε εκατομμύρια χρήστες αλλάζοντας τον χαρακτήρα της διανομής της πληροφορίας και εκμηδενίζοντας ένα ακόμη περιοριστικό χαρακτηριστικό που εμπόδιζε τη παραβίαση της πνευματικής ιδιοκτησίας. Πλέον η αντιγραφή περιεχομένου είναι μια διαδικασία καθόλου χρονοβόρα και χωρίς κανένα κόστος. Αυτό διευκολύνει την περαιτέρω ανάπτυξη της πειρατείας. Είναι πια σύνηθες φαινόμενο η πειρατεία ψηφιακών μουσικών κομματιών. Το μόνο που χρειάζεται είναι η

δημιουργία των αντιγράφων και η διανομή τους. Η αντιγραφή της ψηφιακής πληροφορίας δεν κοστίζει τίποτα στον ιδιοκτήτη του περιεχομένου, ενώ η διανομή από τα δίκτυα είναι γρήγορη και η παράνομη απόκτηση του περιεχομένου από τους χρήστες είναι σαφώς πιο οικονομική, από ότι αν το αγόραζαν.

1.6 Πληθώρα Δημιουργών

Με την ραγδαία ανάπτυξη του Παγκόσμιου Ιστού καθημερινά προστίθενται νέες πληροφορίες στο Διαδίκτυο. Τώρα πια οποιοσδήποτε έχει πρόσβαση στο Διαδίκτυο μπορεί να γίνει δημιουργός περιεχομένου, να κάνει γνωστή τη δουλειά του και να τη συνδέσει με παρόμοιες εργασίες. Σήμερα στον Παγκόσμιο Ιστό υπάρχει μια πληθώρα πληροφοριών και ιδεών, χωρίς όμως να υπάρχει και έλεγχος της αναπαραγωγής και της διανομής της, κάτι που στα παραδοσιακά μέσα γίνονταν από τους εκδότες. Για παράδειγμα ο έλεγχος της αναπαραγωγής μπορεί να χαθεί αν υπάρχει μεγάλη ευκολία δημιουργίας αντιγράφων από αυτούς που απλά επισκοπούν κάποιο έργο. Η απώλεια ελέγχου της αναπαραγωγής μπορεί επίσης να οδηγήσει σε παραβιάσεις του νόμου της πνευματικής ιδιοκτησίας.

1.7 Νόμος Πνευματικής Ιδιοκτησίας

Μία ακόμη συνέπεια του παγκοσμίου ιστού σαν μέσο έκδοσης προκύπτει από την ποικιλία των νόμων και των κανονισμών που ισχύουν ανά χώρα και ήπειρο. Για παράδειγμα οι χρήστες που διακινούν μεταξύ τους παράνομα ψηφιακά μουσικά αντίγραφα, μέσω peer-to-peer εφαρμογών, όπως π.χ. το e-mule, βρίσκονται διάσπαρτοι σε διάφορες χώρες και σημεία του κόσμου. Αυτό έχει ως αποτέλεσμα, να καθίσταται δύσκολος ο καθορισμός του σημείου από το οποίο γίνεται λήψη των δεδομένων. Έτσι δεν μπορεί να προσδιοριστεί και η

δικαιοδοσία των αστυνομικών αρχών και γίνεται ακόμη πιο δύσκολη η εφαρμογή των νόμων περί πνευματικής ιδιοκτησίας.

Επίσης οι νόμοι και οι πρακτικές που ισχύουν για την πνευματική ιδιοκτησία διαφέρουν σε κάθε χώρα, όπως μπορεί να διαφέρει και η στάση απέναντι στην πνευματική ιδιοκτησία, η οποία είναι άμεσα συνυφασμένη με τις αντιλήψεις για το εθνικό συμφέρον. Έτσι ο χρήστης που παρανομεί μπορεί να παρακάμψει τους περιορισμούς που ισχύουν σε μια χώρα μέσω του Διαδικτύου. Για παράδειγμα, τα αρχεία μπορούν εύκολα να μεταφερθούν σε διάφορους τόπους στον κόσμο στους οποίους οι νόμοι είναι λιγότερο αυστηροί και πάλι η πρόσβαση σε αυτά να είναι η ίδια και ανεπηρέαστη.

Η εφαρμογή του νόμου της πνευματικής ιδιοκτησίας παρουσιάζει δυσκολίες που πηγάζουν από την πολυπλοκότητά του. Ο νόμος είναι μια περιγραφή γενικών αρχών (για παράδειγμα το αποκλειστικό δικαίωμα της αναπαραγωγής), και ενός μεγάλου αριθμού ειδικών περιπτώσεων και εξαιρέσεων (όπως το δικαίωμα της εισαγωγής μουσικής υπόκρουσης κ.α.). Η Πνευματική Ιδιοκτησία αφορούσε μέχρι σήμερα κυρίως τις εταιρίες - βιομηχανίες και τους δικηγόρους τους που ήταν υπεύθυνοι για την εφαρμογή των νόμων, για την επίλυση διαφορών σε περιπτώσεις ασάφειας όσον αφορά τα δικαιώματα , για τις διαπραγματεύσεις και τους συμβιβασμούς. Όλοι αυτοί ήταν εξοικειωμένοι με τα θέματα τις Πνευματικής Ιδιοκτησίας και μπορούσαν να αντεπεξέλθουν στις απαιτήσεις που πηγάζουν από την πολυπλοκότητα του νόμου.

Τώρα όμως που τα πνευματικά δικαιώματα και η ιδιοκτησία αφορούν τον απλό πολίτη, η πολυπλοκότητα του νόμου προκαλεί σύγχυση στον απλό χρήστη. Καθημερινά πλέον οι χρήστες του Διαδικτύου έρχονται αντιμέτωποι με τους νόμους που διέπουν την Πνευματική Ιδιοκτησία. Όμως συχνά η κοινή λογική συγκρούεται με το νόμο, δημιουργώντας σύγχυση. Για παράδειγμα ένας χρήστης θεωρεί λογική την χρήση του ίδιου λογισμικού που έχει αγοράσει σε δύο

υπολογιστές, έναν στο σπίτι και έναν στην δουλειά του, όμως στην πραγματικότητα αν δεν έχει αγοράσει δύο άδειες χρήσης, η εγκατάσταση σε δυο υπολογιστές είναι παράνομη.

Οι ασάφειες που προκαλούνται οφείλονται στην παρερμηνεία του όρου «δίκαιη χρήση». Η δίκαιη χρήση επιτρέπει την αναπαραγωγή περιορισμένων ποσοτήτων από υλικό προστατευμένο με το νόμο της πνευματικής ιδιοκτησίας για περιορισμένους σκοπούς, όπως είναι η ανάλυση, η επισκόπηση και ο σχολιασμός του υλικού αυτού. Η δίκαιη χρήση εξαρτάται από τον σκοπό και τον χαρακτήρα της χρήσης (π.χ. εμπορικός, εκπαιδευτικός), την φύση του έργου που προστατεύεται και την επίδραση της χρήσης πάνω στην αγορά του έργου ή πάνω στην εμπορική αξία του έργου.

Ένα από τα πιο φλέγοντα ζητήματα που αφορά στα πνευματικά δικαιώματα είναι το δικαίωμα αναπαραγωγής στον ιδιωτικό βίο, δηλαδή η νομιμότητα της ιδιωτικής, μη εμπορικής αναπαραγωγής. Το ζήτημα δεν αφορά μόνο σε ηλεκτρονικά προϊόντα, αλλά ο κίνδυνος για τους κατόχους των δικαιωμάτων, είναι μεγαλύτερος για την ηλεκτρονική πληροφορία. Γενικά υπάρχει σύγχυση όσον αφορά στο τι είναι νόμιμο και τι όχι. Από την πλευρά τους οι περισσότεροι κάτοχοι πιστεύουν ότι σχεδόν όλες οι αναπαραγωγές χωρίς άδεια είναι παραβάσεις. Οι περισσότεροι όμως απλοί πολίτες πιστεύουν ότι αυτή η αναπαραγωγή είναι νόμιμη. Το τι είναι πραγματικά νομικό βρίσκεται κάπου στη μέση.

Το δικαίωμα της αναπαραγωγής παραδοσιακά αφορούσε τις δημόσιες πράξεις, όπως είναι η δημόσια παρουσίαση ενός προϊόντος. Στη σύγχρονη όμως μορφή της πληροφόρησης η ιδιωτική αναπαραγωγή έχει μεγαλύτερη επίδραση στην αγορά και ο διαχωρισμός μεταξύ της ιδιωτικής και της δημόσιας χρήσης στον ψηφιακό κόσμο δεν είναι ξεκάθαρος. Η κυρίαρχη άποψη στην κοινωνία είναι ότι η ιδιωτική αναπαραγωγή πάντα ή σχεδόν πάντα είναι νόμιμη. Η άποψη

αυτή δύσκολα υποστηρίζεται νομικά ως προς την ορθότητά της. Σκοπός της δίκαιης χρήσης, όπως και άλλων εξαιρέσεων του νόμου περί πνευματικών δικαιωμάτων είναι η εξισορρόπηση των ανταγωνιστικών συμφερόντων μεταξύ των κατόχων των δικαιωμάτων και των απλών χρηστών. Αν και οι ραγδαίες εξελίξεις στην τεχνολογία της διανομής πληροφορίας αλλάζει τις διαδικασίες με τις οποίες προκύπτουν αυτές οι εξαιρέσεις, δε θέτει σε κίνδυνο την πολιτική που υπογραμμίζει τη δίκαιη χρήση. Για το λόγο αυτό η δίκαιη χρήση και οι άλλες εξαιρέσεις του νόμου των πνευματικών δικαιωμάτων πρέπει να συνεχίσουν να διαδραματίζουν σπουδαίο ρόλο στον ψηφιακό κόσμο.

Η δίκαιη χρήση απειλείται όμως από τις τεχνολογικές εξελίξεις και τους νέους τρόπους διανομής, καθώς επίσης και από την ασάφεια που υπάρχει στους νόμους. Για την επίλυση του προβλήματος πρέπει να υπάρξουν σαφείς θεσμοθετημένες αρχές που να μπορεί να τις εφαρμόσει το ευρύ κοινό, π.χ. παρέχοντας νομικά καθορισμένους περιορισμούς στα δικαιώματα αναπαραγωγής. Για τη σωστή προσαρμογή των δικαιωμάτων στο ψηφιακό περιβάλλον, η δίκαιη χρήση και οι εξαιρέσεις του νόμου της πνευματικής ιδιοκτησίας μπορεί να αποδειχτεί ωφέλιμος μηχανισμός.

1.8 Νομική Προστασία Στο Διαδίκτυο

Στο Διαδίκτυο η νομική προστασία του δημιουργού και των κατόχων των δικαιωμάτων επιτυγχάνεται ως εξής:

- Αναγνωρίζονται ή ενισχύονται τα «ψηφιακά δικαιώματα» που έχουν απόλυτο και αποκλειστικό χαρακτήρα, ενώ παράλληλα προβλέπονται περιορισμοί και εξαιρέσεις με στόχο την εξισορρόπηση των συμφερόντων μεταξύ δικαιούχων και χρηστών και του ευρύτερου κοινού γενικά. Η σημασία των ψηφιακών δικαιωμάτων έγκειται ιδίως στο γεγονός ότι σε νομικό επίπεδο επιτρέπουν στο

δικαιούχο να ελέγξει το έργο του σε όλα τα στάδια διανομής του στο Διαδίκτυο, από τον αποστολέα μέχρι τον παραλήπτη συμπεριλαμβανομένων και των ενδιάμεσων σταθμών κατά τη διάρκεια της ψηφιακής διαδικασίας μετάδοσης μέσω Internet.

- Προβλέπονται υποχρεώσεις κατάλληλης έννομης προστασίας κατά των παράνομων δραστηριοτήτων που αλλοιώνουν τις ηλεκτρονικές πληροφορίες διαχείρισης των δικαιωμάτων. Στα «τεχνολογικά μέτρα» που λαμβάνονται για την έννομη προστασία περιλαμβάνονται οι τεχνολογίες ή οι μηχανισμοί που, με το συνήθη τρόπο λειτουργίας τους, αποσκοπούν στο να αποτρέψουν ή να περιορίσουν πράξεις σε σχέση με έργα ή άλλα προστατευόμενα αντικείμενα, που δεν έχουν επιτραπεί από το δικαιούχο πνευματικής ιδιοκτησίας. Τα τεχνολογικά μέτρα θεωρούνται «αποτελεσματικά» όταν η χρήση του προστατευομένου έργου ή άλλου προστατευομένου αντικειμένου ελέγχεται από τους δικαιούχους μέσω της εφαρμογής διαδικασίας ελέγχου της πρόσβασης ή προστασίας.
- Θεσπίζονται κατάλληλες κυρώσεις και μέσα έννομης προστασίας κατά της προσβολής των δικαιωμάτων. Οι κυρώσεις πρέπει να είναι αποτελεσματικές, ανάλογες και αποτρεπτικές. Οι δικαιούχοι των οποίων τα δικαιώματα προσβάλλονται θα πρέπει να έχουν τη δυνατότητα άσκησης αγωγής αποζημίωσης και λήψης ασφαλιστικών μέτρων, καθώς και κατάσχεσης του σχετικού υλικού και των προϊόντων, συσκευών ή συστατικών στοιχείων τα οποία έχουν σκοπό την εξουδετέρωση των τεχνολογικών μέτρων προστασίας.

ΚΕΦΑΛΑΙΟ 2
ΣΥΣΤΗΜΑ ΨΗΦΙΑΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

2.1 Σύστημα Ψηφιακής Διαχείρισης Δικαιωμάτων

2.1.1 Γενικές Έννοιες

Αρχικά είναι σημαντικό να καθοριστούν οι έννοιες **έλεγχος πρόσβασης** (access control), **προστασία από αντιγραφή** (copy protection) και **διαχείριση δικαιωμάτων πνευματικής ιδιοκτησίας**.

- Ένα **σύστημα ελέγχου πρόσβασης** διαχειρίζεται την πρόσβαση ενός χρήστη σε κάποιο περιεχόμενο, συνήθως με χρήση κωδικών (passwords). Σε αυτά τα συστήματα, από τη στιγμή που ο χρήστης αποκτήσει την πρόσβαση στο περιεχόμενο, δεν παρέχεται καμιά περαιτέρω προστασία, επομένως δεν υπάρχει έλεγχος για το πώς θα χρησιμοποιηθεί αυτό το περιεχόμενο. Αυτό το είδος προστασίας χρησιμοποιείται συχνά σε Websites όπου αρκεί ένας απλός μηχανισμός ελέγχου πρόσβασης.
- Ένα **σύστημα προστασίας από αντιγραφή** (copy protection) αποφασίζει αν επιτρέπεται η δημιουργία ενός ή πολλαπλών αντιγράφων, σύμφωνα με το πώς καθορίζεται στις πληροφορίες χρήσης (usage information). Εξασφαλίζει την τήρηση αυτών των κανόνων στον εξοπλισμό του καταναλωτή. Η έννοια της προστασίας αντιγραφής περιέχει και τον έλεγχο διακίνησης του περιεχομένου μέσα αλλά και έξω από το χώρο του χρήστη, όπως η εκ νέου διανομή του στο Internet.
- Ένα **πλήρες σύστημα διαχείρισης δικαιωμάτων πνευματικής ιδιοκτησίας** καλύπτει όλη τη διαδικασία καθορισμού των πληροφοριών που αφορούν στην ηλεκτρονική διαχείριση των δικαιωμάτων, περιέχοντας ακόμη και προσωπικές πληροφορίες, ενώ μπορεί να απαιτεί πρόσβαση σε ευαίσθητα

δεδομένα εμπορικών συναλλαγών. Η χρήση τέτοιων συστημάτων επιτρέπει λεπτομερή έλεγχο στο περιεχόμενο, έτσι ώστε οι δικαιούχοι να μπορούν να καθορίσουν πολύπλοκα μοντέλα χρήσης. Η διαδικασία διαχείρισης των δικαιωμάτων πνευματικής ιδιοκτησίας προϋποθέτει την εκτενή εφαρμογή των DRM τεχνολογιών, οι οποίες μπορούν να ενσωματωθούν από ατομικές συσκευές (PDA) ως και σε εξυπηρετητές Internet μεγάλων εταιριών.

2.1.2 Επιχειρηματικά Μοντέλα Στο Διαδίκτυο

Η ανάπτυξη του Internet δημιούργησε σημαντικές προκλήσεις στα μοντέλα διανομής περιεχομένου. Σύμφωνα με τις στατιστικές, στο τέλος του 2002 υπήρχαν περίπου 9000000 διαφορετικά web sites, ενώ καθημερινά δημιουργούνται 4000 νέα sites. Τα peer-to-peer συστήματα έδωσαν τη δυνατότητα άμεσης πρόσβασης σε διαθέσιμο περιεχόμενο, ακόμη και για τους πιο αμαθείς. Τα πρακτικά και οικονομικά εμπόδια για να γίνει κάποιο περιεχόμενο διαθέσιμο παγκοσμίως έχουν πλέον ξεπεραστεί.

Δυστυχώς για τους κατόχους δικαιωμάτων, οι μηχανισμοί αυτοί όχι μόνο διευκολύνουν τη νόμιμη δημοσίευση και χρήση περιεχομένου, αλλά και τη (συστηματική ή τυχαία) διανομή του πολλαπλές φορές, παρ' όλο που αυτό απαγορεύεται από τη νομοθεσία. Έτσι, καθώς ένας τεράστιος όγκος περιεχομένου γίνεται διαθέσιμος στους χρήστες δωρεάν, ενώ παράλληλα υπάρχουν και οι νόμιμες πηγές που το διανέμουν έναντι κάποιου αντίτιμου, τα επιχειρηματικά μοντέλα που βασίζονται στη διανομή περιεχομένου έναντι αντιτίμου καταρρέουν.

Οι **τεχνολογίες DRM** λοιπόν, με την προϋπόθεση ότι θα είναι αποτελεσματικές, **καλούνται να αποκαταστήσουν αυτά τα επιχειρηματικά μοντέλα, για να διασφαλίσουν τους κατόχους των δικαιωμάτων**. Το παράδοξο είναι ότι οι κάθε είδους εκδότες (ο όρος χρησιμοποιείται για

οποιονδήποτε δημιουργεί περιεχόμενο προς διάθεση στο κοινό) επιθυμούν να παρέχουν πρόσβαση στα έργα τους, παρά να την απαγορεύσουν, κάτι που ισχύει βέβαια και με τη χρήση συστημάτων DRM.

Ο τελευταίος αλλά και βασικός στόχος των 'τεχνικών μέτρων' για τη διανομή πνευματικής ιδιοκτησίας είναι να εξισορροπήσουν τις απαιτήσεις των κατόχων δικαιωμάτων για έλεγχο και προστασία του περιεχομένου τους με τα συμφέροντα των καταναλωτών για πρόσβαση στο περιεχόμενο αυτό. Φυσικά οι καταναλωτές θα προτιμούσαν να έχουν ελεύθερη πρόσβαση αφού είναι δύσκολο να πείσεις κάποιον να πληρώσει για κάτι νοητό (πνευματική ιδιοκτησία), πόσο μάλλον όταν είναι ιδιαίτερα εύκολο να το βρει δωρεάν.

2.1.3 Ορισμός DRM

Από άποψη λειτουργικότητας, ο όρος **Digital Rights Management** σημαίνει πολλά διαφορετικά πράγματα. Για κάποιους είναι απλά μια **τεχνική διαδικασία προστασίας ψηφιακού περιεχομένου**. Για άλλους πρόκειται για μια ο**λοκληρωμένη διαδικασία υποστήριξης ασφαλών συναλλαγών δικαιωμάτων και περιεχομένου** σε δίκτυα όπως το Internet. Γι' αυτό συχνά το DRM χωρίζεται σε δύο λειτουργικούς τομείς.

- **Αναγνώριση και περιγραφή της πνευματικής ιδιοκτησίας και διαχείριση των δικαιωμάτων** που συνδέονται με έργα και τους δημιουργούς τους (διαχείριση ψηφιακών δικαιωμάτων). Οι κάτοχοι δικαιωμάτων πρέπει να προσδώσουν αναγνωριστικά στο περιεχόμενο, να παρέχουν μεταδεδομένα που το περιγράφουν, να καθορίσουν τα δικαιώματα και τους περιορισμούς χρήσης και να διανείμουν το περιεχόμενο.
- **Τεχνική υποστήριξη των περιορισμών χρήσης (ψηφιακή διαχείριση δικαιωμάτων).** Διασφαλίζεται ότι το περιεχόμενο χρησιμοποιείται σύμφωνα με

τους όρους και περιορισμούς χρήσης που έχουν καθοριστεί από τον κάτοχο δικαιωμάτων.

Επομένως το DRM αναφέρεται στην τεχνολογία και στις διαδικασίες που εφαρμόζονται σε ψηφιακό περιεχόμενο για την περιγραφή και αναγνώρισή του καθώς και τον καθορισμό, την εφαρμογή και την υποστήριξη κανόνων χρήσης του με ασφαλή τρόπο.

Ο όρος Digital Rights Management (DRM) προτάθηκε για πρώτη φορά προς το τέλος της δεκαετίας του 1990. Όταν δημιουργείται το περιεχόμενο, ένα σύνολο δικαιωμάτων κληρονομείται στον κάτοχο, που του επιτρέπουν να το δει, να το τροποποιήσει, να το εκτυπώσει, να το εκτελέσει, να το αντιγράψει κ.ά. Τα δικαιώματα αυτά προέρχονται από τρεις πηγές:

- Νομικά: Δικαιώματα τα οποία αποκτήθηκαν είτε αυτόματα από τον νόμο, είτε από κάποια νομική διαδικασία (π.χ. υποβάλλοντας μια πατέντα)
- Συναλλακτικά: Δικαιώματα που αποκτά ή δίνει κάποιος μέσω μιας συναλλαγής, π.χ. αγοράζοντας ένα βιβλίο ή πουλώντας ένα χειρόγραφο σε έναν εκδότη.
- Έμμεσα: Δικαιώματα που ορίζονται από το μέσο που φέρει το περιεχόμενο.

Το πιο σημαντικό σημείο σχετικά με το DRM είναι ότι οι δύο πρώτες πηγές δικαιωμάτων δεν έχουν αλλάξει πολύ με την ανάπτυξη των τεχνολογιών όπως το Internet, τα κινητά τηλέφωνα και τα αρχεία MP3. Οι συναλλαγές παρέμειναν ίδιες παρόλο που πλέον γίνονται μέσω Internet. Αυτό που είναι διαφορετικό είναι η έμμεση φύση των δικαιωμάτων όταν εφαρμόζεται στα παραδοσιακά μέσα. Το Internet έχει κάνει αυτά τα δικαιώματα από έμμεσα άμεσα. Αυτό μπορεί να προκαλέσει τόσο προβλήματα όσο και ευκαιρίες για τους παροχείς περιεχομένου και τους καταναλωτές.

Η έννοια του DRM αναφέρεται στον **ψηφιακό έλεγχο και διαχείριση δικαιωμάτων**. Η ανάγκη για έλεγχο και διαχείριση έχει γίνει μεγαλύτερη τώρα που οι ψηφιακές τεχνολογίες δικτύων έχουν αφαιρέσει τον έμμεσο έλεγχο των κατόχων περιεχομένου που υπάρχει στα μέσα.

2.1.4 Στόχοι Του DRM

Οι κύριοι στόχοι του DRM είναι οι εξής:

- Να παρέχει μια **απαραίτητη υποδομή πληροφορίας** για ψηφιακό περιεχόμενο και των ιδιαίτερων χαρακτηριστικών του. Οι υπηρεσίες που προσφέρονται ποικίλουν από τυπικές e-commerce εφαρμογές (ηλεκτρονικοί κατάλογοι και καλάθι αγορών) μέχρι προηγμένες υπηρεσίες, όπως αναζήτηση π.χ. εικόνων με βάση το κυρίαρχο χρώμα και εντοπισμό μη εξουσιοδοτημένης χρήσης.
- Να **προστατεύσει το copyright** του ψηφιακού περιεχομένου μέσω π.χ. ανθεκτικών τεχνικών υδατογράφησης.
- Να **υποστηρίξει την διαδικασία διαχείρισης ψηφιακών δικαιωμάτων** και τις συναλλαγές που υφίστανται.
- Να παρέχει αποτελεσματικούς **μηχανισμούς ανίχνευσης μη εξουσιοδοτημένης και καταχρηστικής χρήσης του περιεχομένου**.

2.1.5 Το Μέλλον Του DRM

Σήμερα, τα DRM συστήματα βρίσκονται ακόμη σε αρχικό στάδιο ανάπτυξης. Παρ' όλο που οι απαραίτητες τεχνολογίες για την προστασία του ψηφιακού περιεχομένου και των δικαιωμάτων είναι όλο και πιο πολύπλοκες και αποτελεσματικές, η εφαρμογή τους δεν είναι και τόσο εξαπλωμένη. Αυτό οφείλεται εν μέρει στην δυσπιστία των κατόχων δικαιωμάτων, αλλά και στην αντίσταση των καταναλωτών. Ας μην ξεχνάμε ότι οι τελευταίοι έχουν στη

διάθεσή τους μεγάλες ποσότητες περιεχομένου που διακινούνται ελεύθερα στο Internet.

Και ενώ αυτό το πρόβλημα αντιμετωπίζεται από τη μια με δίωξη των 'πειρατών' νομικά και από την άλλη με την ανάπτυξη υπηρεσιών πιο ελκυστικών στους καταναλωτές, στο μέλλον η λύση θα στηρίζεται σε πιο ριζικές προσεγγίσεις, και πιο συγκεκριμένα στην ανάπτυξη του 'trusted computing' ή αλλιώς 'secure engineering'.

Ουσιαστικά το trusted computing πρόκειται για την ανάπτυξη συσκευών που στηρίζονται σε μικροεπεξεργαστές (όπως π.χ. PCs, PDAs, κινητά τηλέφωνα, στερεοφωνικά συστήματα κ.ά.) οι οποίες θα έχουν hardware και software για την προστασία περιεχομένου. Και εδώ το περιεχόμενο μπορεί είτε να αποτελεί πνευματική ιδιοκτησία του δημιουργού είτε απλά ο παροχέας να επιθυμεί η πρόσβαση στο περιεχόμενο να γίνεται σύμφωνα με κάποιες προϋποθέσεις.

Ήδη κάποιες εφαρμογές βρίσκονται σε ανάπτυξη. Υπόσχονται τη δημιουργία ενός έμπιστου δικτυακού περιβάλλοντος, που βασίζεται στην αναγνώριση των χρηστών, των συσκευών και των software modules, και εξασφαλίζει ότι το περιεχόμενο χρησιμοποιείται μόνο σύμφωνα με τους κανόνες που έχουν θέσει οι δημιουργοί. Ένας τέτοιος συνδυασμός ασφάλειας μέσω software και hardware αποτελεί την καλύτερη ελπίδα για ένα απόλυτα έμπιστο και ασφαλές περιβάλλον, ωστόσο προκαλεί και ποικίλους προβληματισμούς, όπως το ζήτημα της privacy του χρήστη. Βέβαια, αυτή η τεχνολογία έχει πολύ δρόμο ακόμη και σύμφωνα με κάποιους ποτέ δεν θα πετύχει. Επομένως θα πρέπει να επικεντρωθούμε στον σχεδιασμό τεχνολογιών αποκλειστικά για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας.

2.2 Σύγχρονες DRM Τεχνολογίες

2.2.1 Τεχνολογίες Και Συνιστώσες (Components) Του DRM

Συχνά το DRM θεωρείται ως ένα ενιαίο software που μπορεί να εγκατασταθεί στον υπολογιστή και εφεξής να προστατεύει το περιεχόμενο online. Στην πραγματικότητα, το DRM συνδυάζει μια μεγάλη ποικιλία τεχνολογιών και υπηρεσιών, κάποιες από τις οποίες εγκαθίστανται στη συσκευή του χρήστη, άλλες στον server του διανομέα και άλλες υπάρχουν γενικά στο δίκτυο.

Σε γενικές γραμμές, αυτές μπορεί να είναι:

- Τεχνολογίες αναγνώρισης
- Τεχνολογίες μεταδεδομένων
- Τεχνολογίες rights language
- Τεχνολογίες κρυπτογράφησης
- Τεχνολογίες μόνιμης συσχέτισης
- Τεχνολογίες privacy
- Τεχνολογίες πληρωμών

Ουσιαστικά οι τρεις πρώτες τεχνολογίες αφορούν στην **διαχείριση ψηφιακών δικαιωμάτων**, ενώ οι υπόλοιπες τέσσερις στην **ψηφιακή διαχείριση των δικαιωμάτων**.

Τα τελευταία χρόνια υπήρξε εκτεταμένη έρευνα γύρω από τον τρόπο με τον οποίο θα πρέπει να συνδυαστούν όλες οι παραπάνω τεχνολογίες για να παράγουν ένα ασφαλές περιβάλλον για το περιεχόμενο πνευματικής ιδιοκτησίας. Η γενική ιδέα είναι ότι το DRM βασίζεται σε ένα υβριδικό μοντέλο εμπορικών υπηρεσιών, software και πρότυπων συνιστωσών, που συγχρόνως προσφέρει

στον καταναλωτή πρόσβαση στο περιεχόμενο, χωρίς να αντιμετωπίζει προβλήματα τεχνικής φύσεως, όπως π.χ. ασυμβατότητα μεταξύ συστημάτων.

2.2.2 Διαχείριση Ψηφιακών Δικαιωμάτων

Το βασικό στοιχείο ενός ενσωματωμένου συστήματος για τη διαχείριση της πρόσβασης σε πνευματική ιδιοκτησία μέσω κάποιου δικτύου, απαιτεί την ανάπτυξη προτύπων για την αναμφίβολη αναγνώριση και περιγραφή της πνευματικής ιδιοκτησίας, συμπεριλαμβανομένων και των δικαιωμάτων και αδειών που σχετίζονται με αυτή.

2.2.2.1 Τεχνολογίες Αναγνώρισης

2.2.2.1.1 Μοναδικά Αναγνωριστικά

Ένα από τα ζητήματα – κλειδιά που υποστηρίζουν τη μεταφορά από τη φυσική διανομή στην αντίστοιχη ηλεκτρονική είναι η επανάσταση της κοινής τεχνολογικής και οργανωτικής υποδομής για την αναγνώριση, ή την ονομασία, στοιχείων περιεχομένου στο ψηφιακό περιβάλλον. Με τον όρο αναγνώριση εννοούμε την απόδοση μιας 'ετικέτας' σε κάτι έτσι ώστε οποιοσδήποτε να μπορεί να το αναγνωρίζει αναμφίβολα. Η αναμφίβολη αναγνώριση είναι απαραίτητη σε κάθε αυτοματοποιημένη επιχειρηματική διαδικασία και αυτό γίνεται πιο εμφανές όταν αυτές οι διαδικασίες περιλαμβάνουν επικοινωνία που ξεπερνάει τα όρια της επιχείρησης και επομένως τα 'τοπικά' αναγνωριστικά δεν είναι προφανή στους υπόλοιπους εμπλεκόμενους. Ένα σύστημα αναγνώρισης είναι απαραίτητο να λειτουργεί σωστά και με τα ήδη υπάρχοντα συστήματα αναγνώρισης φυσικών ή ιδεατών οντοτήτων πνευματικής ιδιοκτησίας.

Τα μοναδικά αναγνωριστικά είναι απαραίτητα για τη διαχείριση πληροφοριών σε οποιοδήποτε ψηφιακό περιβάλλον. Αναγνωριστικά που έχουν ανατεθεί σε κάποιο περιεχόμενο μπορούν να βρεθούν και ίσως να

ξαναχρησιμοποιηθούν κάπου αλλού χωρίς την άδεια αυτού που τα είχε αναθέσει αρχικά, ο οποίος δεν μπορεί να εγγυηθεί ότι οι υποθέσεις του θα είναι γνωστές σε άλλους. Για να είναι δυνατή μια τέτοια διαλειτουργικότητα απαιτείται ο σχεδιασμός αναγνωριστικών που θα μπορούν να χρησιμοποιηθούν και έξω από τον άμεσο έλεγχο και το περιβάλλον του εκδότη τους. Η αναγκαιότητα της διαλειτουργικότητας προσθέτει και την απαίτηση για μονιμότητα των αναγνωριστικών έτσι ώστε να διατηρείται η διαλειτουργικότητα και στο μέλλον. Επίσης, εφ' όσον έξω από το περιβάλλον που ελέγχει άμεσα ο εκδότης (των αναγνωριστικών) οι υπηρεσίες είναι εξ ορισμού αυθαίρετες, η διαλειτουργικότητα θέτει την ανάγκη επεκτασιμότητας.

Λόγω της απουσίας ενός μονολιθικού πλαισίου αναγνώρισης, η μοναδικότητα αυτών των αναγνωριστικών εξασφαλίζεται στα πλαίσια μιας εξουσιοδοτημένης αρχής για την απόδοση αναγνωριστικών, η οποία αναφέρεται κοινώς ως 'namespace'.

Τα μοναδικά αναγνωριστικά είναι συνήθως, αλλά όχι απαραίτητα, αριθμοί. Ένα εύκολα αναγνωρίσιμο παράδειγμα από τον τομέα της βιομηχανίας περιεχομένου είναι το «ISBN 0 85022 324 4». Τα γράμματα ISBN δείχνουν το namespace, δηλαδή εδώ την Αρχή του International Standard Book Number namespace. Αν το συγκεκριμένο namespace είναι έγκυρο (και το ISBN όντως είναι), ο συνδυασμός του namespace και του αναγνωριστικού θα πρέπει να αντιστοιχούν μοναδικά σε κάτι. Στην συγκεκριμένη περίπτωση είναι ένα προϊόν που θέλει να πουλήσει ένας εκδότης.

2.2.2.1.2 Αναγνωριστικά Δικτύου DOI

Τα περισσότερα αναγνωριστικά που αναφέρονται εδώ προ-υπάρχουν του Internet, γι' αυτό ίσως να απέχουν λίγο από τη σημερινή πραγματικότητα. Το Universal Resource Locator (URL) έχει το βασικό πλεονέκτημα ότι είναι

'actionable' στο δίκτυο, δηλαδή κάνοντας κλικ σε ένα URL συμβαίνει κάτι αναμενόμενο: ο browser μεταφέρεται σε ένα συγκεκριμένο σημείο του World Wide Web.

Μπορεί βέβαια να συμβαίνει μια προβλέψιμη ενέργεια, όμως το αποτέλεσμα δεν είναι πάντα το αναμενόμενο. Η μεταφορά στο σημείο που δείχνει ένα URL δεν ικανοποιεί πάντα τον χρήστη, είτε διότι δεν υπάρχει τίποτα πλέον εκεί, είτε διότι το περιεχόμενό του έχει αλλάξει. Άλλωστε το URL είναι ακριβώς αυτό που λέει και το όνομά του, το αναγνωριστικό μιας τοποθεσίας και όχι του περιεχομένου αυτής. Είναι δηλαδή σαν ένας δείκτης ενός ραφιού βιβλιοθήκης, όπου μπορεί να βρεις το βιβλίο που ψάχνεις ή και όχι.

Η κοινότητα του διαδικτύου, εκπροσωπούμενη από τους οργανισμούς World Wide Web Consortium (W3C) και Internet Engineering Task Force (IETF) ασχολείται με αυτά τα ζητήματα για μια δεκαετία. Το αποτέλεσμα των ερευνών για μόνιμη αναγνώριση στο δίκτυο ήταν το Universal Resource Name (URN), ωστόσο ήταν πολύ δύσκολο να γίνει 'actionable' και επομένως χρήσιμο.

Η βιομηχανία εκδόσεων, με προπορευόμενους τους εκδότες επιστημονικών περιοδικών που εξαπλώνονταν γρήγορα online, αντιλήφθηκε την ανάγκη για μόνιμα actionable αναγνωριστικά περιεχομένου στο δίκτυο και το 1998 ίδρυσε το International DOI Foundation, για την ανάπτυξη του **Digital Object Identifier** (**DOI**), το οποίο είναι ένα actionable **αναγνωριστικό δικτύου** που χρησιμοποιεί την Handle 'resolution' τεχνολογία που αναπτύχθηκε από την Corporation for National Research Initiatives (CNRI). Αυτό θεωρήθηκε ότι ήταν η πρώτη εφαρμογή URN.

Πριν προχωρήσουμε στην παράθεση ορισμένων βασικών χαρακτηριστικών του συστήματος DOI είναι σημαντικό να κάνουμε την ακόλουθη παρατήρηση που αφορά τον θεσμικό ρόλο και το κύρος του οργανισμού που υλοποιεί το

σύστημα μοναδικής αναγνώρισης. Τα συστήματα μοναδικής αναγνώρισης αξιοποιούνται από την οντότητα του Παροχέα Μοναδικών Αναγνωριστικών. Η οντότητα αυτή μπορεί να λειτουργεί μέσω ενός Έμπιστου Τρίτου Οργανισμού ο οποίος να επιτελεί όλες τις απαραίτητες λειτουργίες που απαιτούνται για την μοναδική αναγνώριση του ψηφιακού περιεχομένου σε παγκόσμια δίκτυα. Το σημαντικό στοιχείο είναι η εμπιστοσύνη που θα πρέπει να χαρακτηρίζει τις συναλλαγές μεταξύ των βασικών οντοτήτων. Τόσο ο παροχέας περιεχομένου όσο και ο τελικός καταναλωτής πρέπει να εμπιστεύονται απόλυτα το Τρίτο Οργανισμό που λειτουργεί ως διαμεσολαβητής.

Το σύστημα DOI έχει ένα πλήθος από πρακτικά πλεονεκτήματα:

i. Αναγνωρίζει την οντότητα και όχι την τοποθεσία. Τα αποτελέσματα αυτού είναι τα παρακάτω:

- Αν η τοποθεσία αλλάζει, το DOI παραμένει το ίδιο.
- Η ίδια οντότητα μπορεί να αναγνωρίζεται και να προσπελαύνεται από διαφορετικές τοποθεσίες.
- Στο ψηφιακό περιβάλλον του παγκόσμιου ιστού, αυτό υπερβαίνει το εμπόδιο της ανικανότητας των φυλλομετρητών να χειριστούν τα ονόματα. Τα URLs από μόνα τους δεν είναι ικανά να εκφράσουν τις συσχετίσεις μεταξύ οντοτήτων και τα πολλαπλά στιγμιότυπα που δύναται να έχει ένα στοιχείο περιεχόμενου.

ii. Είναι ένα ανοικτό σύστημα, ελεύθερο στη χρήση. Κάθε ένας που συναντά ένα DOI μπορεί να το επιλέξει ώστε να διασυνδεθεί με τις παρεχόμενες υπηρεσίες.

- Κάθε ένας έχει τη δυνατότητα να δημιουργήσει συστήματα που ενσωματώνουν τη χρήση του DOI στα τοπικά περιβάλλοντα, όπως είναι για παράδειγμα η πρόσβαση σε τοπικά εξουσιοδοτημένα αντίγραφα μιας οντότητας.

iii. Είναι ένα σύστημα στο οποίο γίνεται πλήρης διαχείριση:

- Η ανάθεση του DOI μέσω των υπηρεσιών εγγραφής (registration), που διέπονται από μια καθορισμένη πολιτική, διασφαλίζουν τη μοναδικότητα.
- Η δρομολόγηση γίνεται μέσω ενός συστήματος Διαδικτύου προς όλα τα συσχετιζόμενα δεδομένα ή τις υπηρεσίες που παρέχονται από έναν παροχέα περιεχόμενου ή από μια υπηρεσία ανάθεσης DOI ή προς κάποιες υπηρεσίες που παρέχονται από άλλους χρήστες που χρησιμοποιούν και αυτοί το DOI σα σημείο εισαγωγής.
- Παρέχει σημαντικές πληροφορίες για το αντικείμενο που αναγνωρίζεται (μεταδεδομένα).

Αυτά τα τρία σημεία είναι και ο ορισμός αυτού που συχνά ονομάζεται «αγώγιμο ή ενακτέο (actionable) αναγνωριστικό». Αυτά τα αναγνωριστικά δεν αποτελούν μόνο ένα εργαλείο καθορισμού τοποθεσίας, αλλά εξυπηρετούν και στην έναρξη μιας ενδεχόμενης συναλλαγής.

iv. Το DOI μπορεί να εφαρμοστεί σε οποιαδήποτε μορφή πνευματικής ιδιοκτησίας, σε οποιοδήποτε επίπεδο.

v. Δεν αντικαθιστά τα ήδη υπάρχοντα συστήματα αναγνωριστικών (όπως είναι το ISBN, ISSN, ISRC και άλλα συστήματα μοναδικών αναγνωριστικών) αλλά μπορεί να συνεργαστεί με αυτά όπου αυτό είναι εφαρμόσιμο.

Συνεπώς ένα σύστημα μοναδικών αναγνωριστικών με αυτά τα χαρακτηριστικά μπορεί να διασφαλίσει τη διαλειτουργικότητα.

vi. Μπορεί να εφαρμοσθεί σε κάθε ψηφιακό περιβάλλον. Οι αρχικές υλοποιήσεις είναι Διαδικτυακά προσανατολισμένες. Το σύστημα DOI, εκτός των άλλων, μπορεί να εφαρμοστεί σε ένα Διαδίκτυο με νέα πρωτόκολλα και νέα περιβάλλοντα (τα οποία υπάρχει μεγάλη πιθανότητα να εμφανιστούν στο μέλλον).

vii. Η συσχετιζόμενη πληροφορία (μεταδεδομένα) μπορεί να διαχειριστεί με ελεγχόμενο τρόπο, κατάλληλο να αναπαραστήσει τις οντότητες και τις συσχετίσεις μεταξύ αυτών. Τα μεταδεδόμενα αυτά μπορούν να συνεργαστούν με άλλα μεταδεδομένα από άλλες πηγές και να δημιουργήσουν υπηρεσίες και συναλλαγές.

viii. Το σύστημα DOI είναι επεκτάσιμο και διαλειτουργικό.

2.2.2.1.3 Διαχείριση Αναγνωριστικών

Η πραγματική πρόκληση στα συστήματα προσδιορισμού είναι η διαχείρισή τους. Ο Tim Berners-Lee, πατέρας του World Wide Web, είχε πει χαρακτηριστικά ότι το πρόβλημα της χρήσης του URL ως μόνιμο αναγνωριστικό είναι περισσότερο ένα πρόβλημα κοινωνικό παρά τεχνικό. Ακόμα και τα πιο καλά αναγνωριστικά όπως τα ISBN, έχουν αντιμετωπίσει προκλήσεις κατά την εφαρμογή τους, όταν οι χρήστες θέλουν να αναγνωρίσουν 'out-of-scope' αντικείμενα. (το πιο γνωστό παράδειγμα είναι η εφαρμογή του ISBN σε soft παιχνίδια, που όμως τύχαινε να διανέμονται από αλυσίδα εμπορίου βιβλίων).

Φυσικά είναι απαραίτητο να παρέχονται σαφείς οδηγίες σχετικά με την χρήση των αναγνωριστικών, όμως κανείς δεν μπορεί να εγγυηθεί ότι οι χρήστες πραγματικά εφαρμόζουν τα αναγνωριστικά με τον τρόπο που θα έπρεπε (ή έστω ότι τουλάχιστον τα εφαρμόζουν!). Μια προσέγγιση είναι να εξασφαλίζεται ότι τα αναγνωριστικά ανατίθενται μόνο σε αντικείμενα που μπορούν να περιγραφούν με κάποιες ελάχιστες δομές μεταδεδομένων, που σχετίζονται με το αναγνωριστικό.

Τελικά η διαχείριση των αναγνωριστικών στηρίζεται στη συγκατάθεση των χρηστών οι οποίοι πρέπει να συνειδητοποιήσουν ότι η χρήση αναγνωριστικών είναι προς το συμφέρον τους. Γενικότερα δεν υφίσταται μεγάλο πρόβλημα με τη χρήση αναγνωριστικών όταν το κόστος εφαρμογής είναι σχετικά μικρό. Όταν

όμως το κόστος ένταξης σε ένα σύστημα αναγνώρισης είναι αρκετά υψηλό, όπως π.χ. στο DOI, τότε η πρόκληση είναι μεγάλη. Σε αυτές τις περιπτώσεις, οι οργανισμοί μπορούν να είναι επιφυλακτικοί απέναντι σε συστήματα διαχείρισης, που δεν μπορούν να τα επηρεάσουν άμεσα.

Η εφαρμογή μιας αναμφίβολης υποδομής αναγνώρισης για τη διαχείριση ψηφιακών δικαιωμάτων είναι πολύπλοκη και δύσκολη. Οι βιομηχανίες περιεχομένου δεν έχουν πειστεί ακόμη για την αναγκαιότητα ύπαρξής της. Όμως στον τομέα της μουσικής, όπου η υποδομή για τη διαχείριση των δικαιωμάτων είναι και η πιο ανεπτυγμένη, φαίνεται ξεκάθαρα η σημαντικότητα αυτού του ζητήματος.

Ωστόσο, τα αναγνωριστικά από μόνα τους έχουν μικρή αξία. Απλά επιτρέπουν την ευκολότερη επικοινωνία δυο συστημάτων εξασφαλίζοντας ότι και τα δυο αναφέρονται στο 'ίδιο πράγμα'. Αυτό που δίνει πραγματική αξία σε ένα αναγνωριστικό είναι η ικανότητα να το χρησιμοποιήσεις για να συνδέσεις πληροφορίες για 'το ίδιο πράγμα' σε διαφορετικά συστήματα υπολογιστών.

2.2.2.2 Τεχνολογίες Μεταδεδομένων

2.2.2.2.1 Μεταδεδομένα

Τα μεταδεδομένα υπάρχουν από τότε που ο πρώτος βιβλιοθηκάριος έφτιαξε μια λίστα των αντικειμένων ενός ραφιού με χειρόγραφους πάπυρους. Ουσιαστικά τα μεταδεδομένα είναι δεδομένα για άλλα δεδομένα. Είναι δηλαδή ο όρος της Internet-εποχής για τις πληροφορίες που παραδοσιακά οι βιβλιοθηκάριοι έβαζαν σε καταλόγους, και αναφέρονται κυρίως σε περιγραφικές πληροφορίες για τις web resources.

Ο όρος **μεταδεδομένα** χρησιμοποιείται με πολλούς διαφορετικούς τρόπους. Εμείς θα τον χρησιμοποιούμε με την **έννοια των πληροφοριών που περιγράφουν περιεχόμενο** (το οποίο είναι τα 'δεδομένα'), όπως χρησιμοποιείται και στις βιομηχανίες περιεχομένου.

Η έννοια της περιγραφής είναι βέβαια πολύ γενική. Εμείς θα επικεντρωθούμε κυρίως στα **μεταδεδομένα που σχετίζονται άμεσα με τα αναγνωριστικά**, καθώς αυτά είναι τα μεταδεδομένα που έχουν πιο άμεση εφαρμογή στη διαχείριση ψηφιακών δικαιωμάτων. Τα πρότυπα μεταδεδομένων είναι ακόμη σε πρώιμο στάδιο σε σχέση με αυτό των αναγνωριστικών, αφού η σημαντικότητα της διαλειτουργικότητας των μεταδεδομένων μόλις πρόσφατα άρχισε να γίνεται αντιληπτή.

Τα μεταδεδομένα είναι επιπλέον πληροφορία που σχετίζεται με τα πρωτεύοντα δεδομένα (περιεχόμενο). **Τα μεταδεδομένα είναι, «επιπρόσθετα δεδομένα, τα οποία διασυνδέονται με τα δεδομένα του περιεχομένου, πέραν του ίδιου του αρχείου».** Τα μεταδεδομένα μπορούν να χρησιμοποιηθούν με μια ποικιλία από τρόπους, όπως να παρέχουν πληροφορία για το περιεχόμενο και τη δημιουργία του και να επιτρέπουν την εύκολη διαχείριση του ψηφιακού περιεχομένου μέσω πληροφοριών όπως είναι ο τύπος του, τα δικαιώματα της πνευματικής ιδιοκτησίας ή ο δημιουργός.

Αξίζει να σημειώσουμε ότι μια πολύ μεγάλη ποσότητα μεταδεδομένων έχουν συλλεχθεί σε διαφορετικά σημεία της αλυσίδας παροχής πληροφοριών. Ουσιαστικά, η 'ίδια' πληροφορία έχει καταγραφεί από διαφορετικά άτομα. Η περίσσεια αυτών των συλλογών πληροφοριών και των τρόπων διατήρησής τους, από άποψη κόστους αλλά και ποιότητας, οδήγησε στην ανάπτυξη προτύπων για το διαμοιρασμό δεδομένων.

Μια εγγραφή αποτελείται από ένα σύνολο στοιχείων, απαραίτητων για την περιγραφή ενός αντικειμένου. Για παράδειγμα, ένα σύστημα μεταδεδομένων για βιβλιοθήκες συνήθως περιλαμβάνει ένα σύνολο από εγγραφές μεταδεδομένων με στοιχεία που περιγράφουν το βιβλίο ή κάποιο άλλο αντικείμενο της βιβλιοθήκης: συγγραφέα, τίτλο, ημερομηνία δημιουργίας ή έκδοσης, θέμα, και τον αριθμό που καθορίζει τη θέση του αντικειμένου στο ράφι.

Η σύνδεση μεταξύ των μεταδεδομένων και του αντικειμένου που περιγράφουν μπορεί να πάρει μια από τις παρακάτω μορφές:

1. τα στοιχεία μπορούν να περιέχονται σε μια εγγραφή ξεχωριστά από το αντικείμενο, όπως π.χ. στην περίπτωση του καταλόγου της βιβλιοθήκης ή

2. τα μεταδεδομένα να είναι ενσωματωμένα στο ίδιο το αντικείμενο.

Παραδείγματα ενσωματωμένων μεταδεδομένων που μεταφέρονται μαζί με το αντικείμενο περιλαμβάνουν τα δεδομένα που είναι τυπωμένα πίσω από το εξώφυλλο ενός βιβλίου, ή στην επικεφαλίδα ενός ηλεκτρονικού κειμένου. Πολλά πρότυπα δεν χρησιμοποιούν μία συγκεκριμένη μορφή σύνδεσης από τις δύο, αφήνοντας την επιλογή σε κάθε εφαρμογή.

Παρόλο που η έννοια των μεταδεδομένων προϋπήρχε του Internet και του Web, παγκοσμίως το ενδιαφέρον για πρότυπα μεταδεδομένων αυξήθηκε θεαματικά με την ανάπτυξη των ηλεκτρονικών εκδόσεων και των ψηφιακών βιβλιοθηκών. Οποιοσδήποτε προσπαθεί να βρει πληροφορίες στο διαδίκτυο χρησιμοποιώντας μια από τις πιο διαδεδομένες μηχανές αναζήτησης, καταλήγει να ανακτά εκατοντάδες, αν όχι χιλιάδες, 'hits' χωρίς όμως να έχει τη δυνατότητα να κάνει μια πιο συγκεκριμένη αναζήτηση. Η ευρεία υιοθέτηση περιγραφικών προτύπων και πρακτικών για ηλεκτρονικά αντικείμενα θα βελτιώσει την ανάκτηση σχετικών αντικειμένων, σε οποιοδήποτε χώρο όπου η ανάκτηση πληροφοριών είναι ιδιαίτερα σημαντική.

2.2.2.2.2 Σχέση Αναγνωριστικών Και Μεταδεδομένων

Η σημαντικότητα της σχέσης μεταξύ συστημάτων αναγνώρισης και μεταδεδομένων γίνεται όλο και πιο προφανής σε αυτούς που εμπλέκονται στην καθιέρωση προτύπων αναγνωριστικών. Η επιτροπή ISO που είναι υπεύθυνη για τα πρότυπα του Information and Documentation – Identification and Description, αποφάσισε ότι δεν θα υπάρξει κανένα πρότυπο για αναγνωριστικά που δεν θα περιέχει καθορισμό κάποιων ελάχιστων μεταδεδομένων. Για παράδειγμα, η τρέχουσα αναθεώρηση του ISBN προτύπου περιλαμβάνει ακριβώς ένα τέτοιο σύνολο ελάχιστων μεταδεδομένων, σχεδιασμένο να εγγράφεται με το ISBN.

Ο πρωταρχικός στόχος αυτών των συνόλων ελάχιστων μεταδεδομένων είναι η αποσαφήνιση. Αυτό σημαίνει ότι θα πρέπει να υπάρχουν αρκετά δεδομένα ώστε να είναι δυνατός ο διαχωρισμός μεταξύ δυο επιφανειακά όμοιων αλλά στην πραγματικότητα διαφορετικών αντικειμένων. Δηλαδή, με άλλα λόγια, να μπορούμε να ξεχωρίζουμε δύο οντότητες που έχουν κάποια κοινά γνωρίσματα, αλλά όχι όλα.

Όσον αφορά τον τομέα των εκδόσεων βιβλίων, δίνεται ιδιαίτερη προσοχή έτσι ώστε να εξασφαλίζεται ότι τα πρότυπα των μεταδεδομένων των ISO αναγνωριστικών σχεδιάζονται συμβατά με τα ONIX πρότυπα. Αυτό θα εξασφαλίσει την (μη εμφανή) διαλειτουργικότητα μεταξύ διαφορετικών μεταδεδομένων στον ίδιο τομέα.

2.2.2.2.3 Διαλειτουργικότητα Των Μεταδεδομένων

Ακόμη και αν ένας τομέας, όπως αυτός των εκδόσεων βιβλίων, καθορίσει επιτυχώς εμπορικά πρότυπα που εφαρμόζονται ευρέως σε αυτό τον τομέα, είναι

πολύ πιθανό αυτά τα πρότυπα να μην είναι αποδεκτά πέρα από τα σύνορα αυτού του τομέα.

Σε μια αγορά που εξαπλώνεται παγκοσμίως, και με το αναπόφευκτο της σύγκλισης των media, καθώς όλοι οι τύποι δεδομένων διανέμονται μέσω ενός κοινού καναλιού, η διαλειτουργικότητα πέρα από τα όρια κάθε τομέα κρίνεται απαραίτητη.

Μια βασική προϋπόθεση είναι ότι η ορολογία των μεταδεδομένων πρέπει να είναι καλά διαμορφωμένη, που κυρίως σημαίνει ότι πρέπει να είναι σωστά και αναμφίβολα ορισμένη. Ενώ η λύση για την διαλειτουργικότητα επικεντρωνόταν μέχρι τώρα κυρίως στο συντακτικό, η πραγματική πρόκληση βρίσκεται στη σημασιολογία.

2.2.2.3 Τεχνολογίες Rights Language

2.2.2.3.1 Σημασιολογία Και Rights Expression Languages

Όπως προαναφέρθηκε η ορολογία των μεταδεδομένων πρέπει να είναι καλά διαμορφωμένη, δηλαδή σωστά και αναμφίβολα ορισμένη. Για να ικανοποιηθεί η απαίτηση για καλά ορισμένη σημασιολογία υπάρχει η **ανάγκη δημιουργίας μιας Γλώσσας Έκφρασης Δικαιωμάτων (Rights Expression Language).** Μια Γλώσσα Έκφρασης Δικαιωμάτων (REL) είναι μια γλώσσα **κατανοητή από τις μηχανές** που μπορεί να **καθορίζει δικαιώματα και άδειες χρησιμοποιώντας τους όρους που ορίζονται στο Rights Data Dictionary**. Τεχνικά ένα συντακτικό δικαιωμάτων αποτελεί ένα μέρος της περιγραφής του περιεχομένου και είναι ένα σύνολο όρων που καθορίζουν κανόνες σε σχέση με αυτό το περιεχόμενο. Ουσιαστικά ο ρόλος των σωστά δομημένων λεξικών δεδομένων, δηλαδή λεξικών που ορίζουν τους όρους που

χρησιμοποιούνται στα σύνολα μεταδεδομένων σε συμφωνία με ένα σωστά δομημένο μοντέλο δεδομένων, είναι αυξημένος.

2.2.2.3.2 Ιδιότητες Κανόνων Των Γλωσσών Έκφρασης Δικαιωμάτων

Από τη στιγμή που το περιεχόμενο έχει αναγνωριστεί και περιγραφεί, οι κάτοχοι δικαιωμάτων θα θέλουν να κατασκευάσουν τους κανόνες σύμφωνα με τους οποίους θα μπορούν να έχουν πρόσβαση οι χρήστες στο περιεχόμενο. Αυτοί οι κανόνες θα δώσουν τη δυνατότητα στους κατόχους δικαιωμάτων να δημιουργήσουν επιχειρηματικά μοντέλα, ήδη υπάρχοντα ή νέα. Οι κανόνες όμως αυτού του είδους θα πρέπει να πληρούν κάποιες απαιτήσεις:

- Να είναι fully expressive, δηλαδή θα πρέπει να είναι ικανοί να δίνουν τη δυνατότητα στους κατόχους δικαιωμάτων να εκφράσουν τα δικαιώματά τους και τα συμφέροντά τους ως προς το περιεχόμενο, καθώς και τις σχετικές συμβολαιογραφικές συμφωνίες, με βάση μια ποικιλία επιχειρηματικών μοντέλων και τρόπων χρήσης.
- Να είναι αναμφίβολοι, δηλαδή θα πρέπει να είναι απόλυτα ακριβείς, ώστε να μην μπορούν να ερμηνευθούν με τρόπο διαφορετικό από αυτόν που εννοεί ο κάτοχος δικαιωμάτων.
- Να είναι machine readable, δηλαδή θα πρέπει να 'διαβάζονται' από υπολογιστές και άλλες συσκευές μικροεπεξεργαστών.
- Να είναι secure, δηλαδή να δημιουργούνται με τέτοιο τρόπο, ώστε οποιαδήποτε προσπάθεια παραποίησης να μπορεί να ανιχνευτεί.

Αυτή είναι μόνο μια βασική λίστα απαιτήσεων για μια γλώσσα έκφρασης δικαιωμάτων, η οποία αναδεικνύει και τις ελάχιστες απαιτήσεις. Η χρήση των γλωσσών έκφρασης δικαιωμάτων θα είναι το κλειδί για το μέλλον της ψηφιακής διαχείρισης δικαιωμάτων, αφού παρέχει τα μέσα για την υποστήριξη των υπαρχόντων επιχειρηματικών μοντέλων και για τη δημιουργία νέων.

2.2.2.3.3 Περιγραφή Της Τεχνολογίας Των Γλωσσών Έκφρασης Δικαιωμάτων

Ίσως ο ευκολότερος τρόπος να κατανοήσουμε τι ακριβώς κάνει μια έκφραση δικαιωμάτων, είναι να την εξηγήσουμε ως μια γλώσσα εντολών για υπολογιστή. Σε αυτή την περίπτωση, οι εντολές αναφέρονται στο τι μπορεί να κάνει ένας χρήστης με ένα περιεχόμενο. Ο κάτοχος δικαιωμάτων μετατρέπει την ανθρώπινη άδειά του (π.χ. μπορείς να αντιγράψεις αυτό το περιεχόμενο στον σκληρό δίσκο σου) σε μια λογική γλώσσα, την οποία ένα πρόγραμμα υπολογιστή μπορεί να ερμηνεύσει. Το πρόγραμμα αυτό είναι ουσιαστικά το σύστημα κρυπτογράφησης που προστατεύει το περιεχόμενο, στο οποίο ο χρήστης θέλει να έχει πρόσβαση.

Η τεχνολογία της γλώσσας έκφρασης δικαιωμάτων αναπτύχθηκε για πρώτη φορά στις αρχές του 1990 στο Xerox Parc Research Center. Από τότε η τεχνολογία αυτή έχει γίνει πολύ πολύπλοκη. Ουσιαστικά, είναι βασισμένη στην ιδέα ότι σε έναν χρήστη δίνεται η άδεια να ενεργήσει με συγκεκριμένο τρόπο πάνω σε περιεχόμενο που προστατεύεται από κανόνες πνευματικής ιδιοκτησίας. Για παράδειγμα, ένας κάτοχος δικαιωμάτων θέλει να παραχωρήσει το δικαίωμα στους χρήστες να αντιγράφουν κάποιο περιεχόμενο στο σκληρό τους δίσκο, όμως κάτω από ορισμένες προϋποθέσεις. Ίσως να θέλει να αποτρέψει το περιεχόμενο να περάσει σε τρίτους, δηλαδή να μην αντιγραφεί ξανά, ή να παραποιηθεί με οποιοδήποτε τρόπο. Αυτή είναι μια απλή άδεια την οποία μια έκφραση δικαιωμάτων μπορεί να μετατρέψει σε μια έκφραση δικαιωμάτων που μπορεί να διαβάσει η μηχανή.

Μια γλώσσα έκφρασης δικαιωμάτων είναι γραμμένη και αυτή σε ένα είδος γλώσσας υπολογιστή, συνήθως σε **XML**. Αυτή είναι μια υψηλού επιπέδου γλώσσα υπολογιστή που μπορεί να διαβαστεί και από ανθρώπους. Η XML, πολλές

φορές καλούμενη και ως η γλώσσα του Web, χρησιμοποιείται ευρέως και η σημαντικότητά της ως βάση της γλώσσας έκφρασης δικαιωμάτων είναι ότι είναι γενική, και έτσι βοηθάει στην διαλειτουργικότητα.

2.2.2.3.4 Περιγραφή Της Τεχνολογίας Rights Data Dictionary

Μια γλώσσα έκφρασης δικαιωμάτων απαιτεί πολύ ακριβείς όρους (σημασιολογίες) έτσι ώστε να δημιουργήσει ακριβείς και αναμφίβολες εκφράσεις. Ωστόσο, είναι προφανές ότι η φυσική γλώσσα και η γλώσσα των υπολογιστών είναι δύο τελείως διαφορετικά πράγματα. Η καθημερινή γλώσσα σε καμία περίπτωση δεν είναι ακριβής για έναν υπολογιστή και η κοινωνία βασίζεται στην άποψη ότι η διερμηνεία της γλώσσας είναι απαραίτητη. Για παράδειγμα, όλοι οι νόμοι έχουν σαν βάση το γεγονός ότι δεν μπορούν να είναι τόσο ακριβείς ώστε να αποκλείσουν την παρερμηνεία.

Από την άλλη πλευρά, οι υπολογιστές δεν μπορούν να ανταποκριθούν στην ανακρίβεια. Δεδομένης μιας αμφίβολης έκφρασης, οι υπολογιστές είτε θα αποτύχουν να λειτουργήσουν είτε θα ενεργήσουν με απρόβλεπτο τρόπο. Γι’ αυτό είναι απαραίτητο, να κατασκευάσουμε ένα σύνολο όρων ειδικά σχεδιασμένων για χρήση σε μια γλώσσα έκφρασης δικαιωμάτων. Οι όροι αυτοί αποτελούν τη βάση ενός rights data dictionary.

Ένα καλό παράδειγμα του πώς η φυσική γλώσσα μπορεί να είναι προβληματική όταν εφαρμόζεται σε μια γλώσσα έκφρασης δικαιωμάτων είναι ο όρος ‘copy’. Χρησιμοποιείται ευρέως στη νομοθεσία για copyright, αλλά στα πλαίσια των υπολογιστών η χρήση του είναι άτοπη. Η αντιγραφή θεωρητικά σημαίνει να φτιάξεις ένα ακριβές αντίγραφο ενός αντικειμένου που θα είναι ολόιδιο από όλες τις απόψεις. Ενώ οι άνθρωποι αντιλαμβανόμαστε την έννοια της αντιγραφής, για έναν υπολογιστή αυτό δεν βγάζει νόημα. Πώς γίνεται ένα πράγμα να είναι ακριβώς το ίδιο με ένα άλλο, αφού θα έπρεπε να είναι το ίδιο

αντικείμενο (το ίδιο υλικό, στον ίδιο χώρο και την ίδια στιγμή). Επομένως θεωρητικά δεν θα υπήρχε αντίγραφο. Έτσι, όταν χρησιμοποιείται ο όρος 'copy' σε μια γλώσσα έκφρασης δικαιωμάτων είναι απαραίτητο να εξασφαλίσουμε ότι δεν θα υπάρξει αυτή η ανακρίβεια κατά τη χρήση του.

2.2.2.3.5 Διαλειτουργικότητα Των Γλωσσών Έκφρασης Δικαιωμάτων

Όπως αναφέρθηκε και νωρίτερα, μια έκφραση δικαιωμάτων είναι μια εντολή προς μια συσκευή με μικροεπεξεργαστή ώστε να ενεργήσει με συγκεκριμένο τρόπο. Αυτή η εντολή δίνεται σε ένα πρόγραμμα, το οποίο αποτελεί ένα από τα βασικά μέρη ενός συστήματος ψηφιακής διαχείρισης δικαιωμάτων για την προστασία περιεχομένου. Η εντολή ουσιαστικά λέει στο πρόγραμμα τους όρους και τις προϋποθέσεις κάτω από τις οποίες το περιεχόμενο, το οποίο προς το παρόν είναι μη προσβάσιμο στο χρήστη, μπορεί να χρησιμοποιηθεί. Μια έκφραση δικαιωμάτων, για να είναι χρήσιμη, θα πρέπει να μπορεί να λειτουργήσει σε πλήρη συνεργασία με το πρόγραμμα προστασίας έτσι ώστε οι εντολές που φέρει να γίνουν επακριβώς κατανοητές και να διεκπεραιωθούν.

Αυτή η απαίτηση προϋποθέτει ότι μια γλώσσα έκφρασης δικαιωμάτων μπορεί να λειτουργεί με πολλά διαφορετικά DRM προγράμματα. Χωρίς αυτή τη δυνατότητα, η γλώσσα έκφρασης δικαιωμάτων θα είναι δεμένη αποκλειστικά με ένα μόνο DRM σύστημα και επομένως θα είναι περιορισμένης χρήσης. Η ενσωμάτωση λοιπόν μιας έκφρασης δικαιωμάτων σε πολλά διαφορετικά DRM συστήματα θα είναι το πρώτο βασικό βήμα για να επιτύχουμε την διαλειτουργικότητα για τους χρήστες των DRM. Εξάλλου αν το ίδιο περιεχόμενο, που ελέγχεται από μια έκφραση δικαιωμάτων, μπορεί να χρησιμοποιηθεί σε διάφορα διαφορετικά DRM συστήματα, θα μειώσει και το packaging των κατόχων δικαιωμάτων, που σε αντίθετη περίπτωση θα έπρεπε να παράγουν πολλές διαφορετικές εκφράσεις δικαιωμάτων σε διαφορετικές γλώσσες για πολλά

διαφορετικά συστήματα, αλλά και θα ικανοποιήσει τους χρήστες, αφού μια κοινή έκφραση δικαιωμάτων θα λειτουργεί με την τεχνολογία του δικού τους DRM συστήματος.

ΚΕΦΑΛΑΙΟ 3
ΨΗΦΙΑΚΗ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΑΙΩΜΑΤΩΝ

Ως τώρα έχουμε δείξει ότι για τη διαχείριση των δικαιωμάτων σε ψηφιακό περιεχόμενο απαιτείται μόνιμη αναγνώριση, σαφήνεια στην περιγραφή και ακριβείς κανόνες χρήσης, οι οποίοι μπορούν να παρέχουν αναμφίβολες εντολές σε προγράμματα υπολογιστών για την προστασία περιεχομένου.

Παρακάτω περιγράφονται οι τεχνολογίες για την προστασία του περιεχομένου από μη εξουσιοδοτημένη χρήση, δηλαδή ψηφιακά κλειδιά και κλειδώματα.

3.1 Τεχνολογικά Μέσα Προστασίας - Τεχνολογίες Κρυπτογράφησης

3.1.1 Εισαγωγικά Στοιχεία

Σε προηγούμενες αναφορές της παρούσας εργασίας δόθηκε ιδιαίτερη βαρύτητα στη σημασία και τη νομική θωράκιση που χρήζουν τα τεχνολογικά μέσα στο ευρύτερο πλαίσιο της προστασίας και διαχείρισης των πνευματικών δικαιωμάτων ψηφιακού περιεχομένου. Στο παρόν κεφάλαιο θα πραγματοποιηθεί μια αναλυτική παρουσίαση των τεχνολογιών που χρησιμοποιούνται για το συγκεκριμένο σκοπό καθώς και των σημαντικότερων συστημάτων που αξιοποιούν αντίστοιχες 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.
- **Εξακολουθητική κρυπτογράφηση**: 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.

Στην συνέχεια θα πραγματοποιηθεί μια εκτενέστερη περιγραφή των βασικότερων τεχνολογιών που χρησιμοποιούνται ευρέως σε πολλούς τομείς.

3.1.2 Ασφάλεια Λειτουργικών Συστημάτων

Ο λόγος για τον οποίο θεσμοθετήθηκε η έννοια των πνευματικών δικαιωμάτων είναι η προστασία της καλλιτεχνικής και της πνευματικής δημιουργίας. Όλα τα νομικά μέτρα και οι κανονισμοί που θεσπίζονται αποσκοπούν στη δίκαιη απόδοση του ηθικού δικαιώματος που αποκτά ο δημιουργός επί του έργου του, ο εφευρέτης επί της πρωτοποριακής ιδέας του κ.τ.λ. Η παραπάνω προσπάθεια δυσχεραίνεται από τους ιδιαίτερους κανόνες που διέπουν την ψηφιακή πραγματικότητα.

Το σημαντικότερο ίσως διακριτό πρόγραμμα λογισμικού που χρησιμοποιούν οι υπολογιστές είναι το λειτουργικό σύστημα. Τα λειτουργικά συστήματα είναι υπεύθυνα για την ορθή λειτουργία των υπολογιστών και τη συνεργασία τους με τις περιφερειακές συσκευές. Σημαντικός ακόμα είναι ο ρόλος τους στην επικοινωνία των υπολογιστών μέσω των δικτύων. Κατά αυτή την έννοια, αποτελούν το πρώτο επίπεδο προστασίας του ψηφιακού περιεχομένου από πιθανές ενέργειες κλοπής. Είναι πολύ σημαντικό για ένα ολοκληρωμένο και αποτελεσματικό σύστημα προστασίας ψηφιακού περιεχομένου να υποστηρίζεται από ένα λειτουργικό σύστημα που να του προσφέρει ικανοποιητική ασφάλεια.

Για την θωράκιση των δεδομένων και των υπηρεσιών τους, τα περισσότερα λειτουργικά συστήματα χρησιμοποιούν τους Πυρότοιχους (Firewalls). Πρόκειται για εφαρμογές που περιορίζουν την πρόσβαση των χρηστών στο δίκτυο, αποτρέπουν την εισαγωγή επικίνδυνων προγραμμάτων στο σύστημα και παρέχουν ένα αρκετά στιβαρό τοίχο προστασίας του ψηφιακού περιεχομένου. Επιπλέον, συμπληρωματικοί μηχανισμοί ελέγχου και προστασίας υλοποιούν λειτουργίες και πολιτικές όπως είναι η πιστοποίηση χρηστών, η ελεγχόμενη πρόσβαση στο περιεχόμενο σύμφωνα με τις λίστες ελέγχου πρόσβασης (ACLs-Access Control Lists) κ.α. Η ασφάλεια και η ακεραιότητα του λειτουργικού συστήματος είναι ιδιαίτερα σημαντική κατά το σχεδιασμό ενός αποδοτικού Τεχνολογικού Συστήματος Προστασίας Πνευματικών Δικαιωμάτων.

3.1.3 Εισαγωγή Πληροφορίας στην «Κεφαλίδα» του Ψηφιακού Αρχείου

Η πιο απλή προσέγγιση για την προστασία ενός ψηφιακού αντικειμένου είναι η τοποθέτηση πληροφορίας μέσα στο ίδιο το αρχείο αναπαράστασης. Η συντριπτική πλειοψηφία των διαθέσιμων τύπων αναπαράστασης ψηφιακών δεδομένων διαθέτουν τη δυνατότητα να φιλοξενούν πληροφορία πέραν του ψηφιακού περιεχομένου, χωρίς να επηρεάζεται το τελικό αποτέλεσμα της αναπαράστασης. Όλοι οι τύποι ψηφιακών αρχείων (Βίντεο, Εικόνα, Ήχος)

περιλαμβάνουν ένα τμήμα δεδομένων που ονομάζεται συνήθως «Κεφαλίδα» και έχει την ιδιότητα να αγνοείται κατά την διαδικασία της ψηφιακής αναπαραγωγής. Το συγκεκριμένο τμήμα δεδομένων χρησιμοποιείται για να διατηρεί πληροφορίες σχετικά με το ψηφιακό περιεχόμενο του αρχείου. Τέτοιου είδους πληροφορία είναι και τα δεδομένα που ορίζουν τον δημιουργό του έργου, τον κάτοχο των πνευματικών δικαιωμάτων κ.α. Με αυτόν τρόπο η τοποθέτηση πληροφορίας περί της πνευματικής ιδιοκτησίας του ψηφιακού περιεχομένου στην κεφαλίδα του αρχείου αναπαράστασης, μπορεί να αποτελέσει ένα μέσο προστασίας και διαχείρισης των πνευματικών του δικαιωμάτων. Τα παραπάνω ενισχύονται και από συνθήκη του WIPO (World Intellectual Property Organization) σύμφωνα με την οποία, ως παράνομη θεωρείται οποιαδήποτε μη εξουσιοδοτημένη παρέμβαση ή τροποποίηση της πληροφορίας που περιλαμβάνεται στην κεφαλίδα ενός ψηφιακού αρχείου αναπαράστασης πολυμεσικού υλικού. Δυστυχώς, η ευκολία πρόσβασης στο περιεχόμενο της κεφαλίδας ενός αρχείου, που μπορεί να πραγματοποιηθεί ακόμα και με τη χρήση ενός απλού επεξεργαστεί κειμένου, καθώς και η έλλειψη μέριμνας για την διατήρηση των δεδομένων, που απαντάται στη συντριπτική πλειοψηφία των εμπορικά διαθέσιμων εργαλείων αναπαράστασης, συμπίεσης και κωδικοποίησης πολυμεσικού υλικού, καθιστά την παραπάνω τεχνολογική λύση εξαιρετικά επισφαλή, διαβλητή και ακατάλληλη. Για παράδειγμα, μια απλή μετατροπή του format μιας ψηφιακής εικόνας από TIFF σε JPEG με τη χρήση ενός από τα εμπορικά διαθέσιμα εργαλεία αναπαράστασης και επεξεργασίας εικόνας, έχει ως αποτέλεσμα την ολοκληρωτική καταστροφή των δεδομένων της κεφαλίδας του αρχείου. Ακόμα όμως και στην περίπτωση που τα εμπορικά εργαλεία συμμορφωθούν με την συνθήκη του WIPO, η ευκολία με την οποία ένας επίδοξος παραβάτης μπορεί να τροποποιήσει την πληροφορία που φιλοξενείται στην κεφαλίδα ενός αρχείου, δεν επιτρέπει την χρήση της παραπάνω τεχνολογικής λύσης ως αποκλειστικού μέσου προστασίας των πνευματικών δικαιωμάτων ψηφιακού περιεχομένου.

3.1.4 Κρυπτογράφηση

3.1.4.1 Γενικά Στοιχεία

Ως **κρυπτογράφηση** ορίζεται η **σύνταξη ενός κρυπτογραφήματος ενός δηλαδή συνθηματικού και μυστικού κειμένου, μέσω του οποίου μεταδίδεται ένα εμπιστευτικό, απόρρητο ή άκρως απόρρητο μήνυμα.** Αναπτύχθηκε κυρίως για λόγους εθνικής ασφάλειας και αντικατασκοπίας, αλλά εφόσον ζητούμενο πάντα είναι η ασφαλής μετάδοση της πληροφορίας, (η ασφαλής επικοινωνία), ήταν φυσικό (με την εκτεταμένη χρήση του διαδικτύου το οποίο όξυνε την ανάγκη για ασφαλή επικοινωνία και την κατέστησε απαραίτητη ακόμα και για γενική και καθημερινή χρήση), να διαδοθεί και να χρησιμοποιηθεί και από διάφορους οργανισμούς, επιχειρήσεις, ιδιώτες, ή γενικότερα χρήστες του διαδικτύου. Η προστασία του περιεχομένου από μη εξουσιοδοτημένη πρόσβαση απαιτεί κάποιου είδους κρυπτογράφηση. Η **κρυπτογράφηση**, ή αλλιώς η **διαδικασία απόκρυψης πληροφοριών**, έχει αναπτυχθεί εδώ και χιλιάδες χρόνια.

Η πρώτη ιστορική αναφορά στη χρήση της κρυπτογραφίας, χρονολογείται γύρω στο 1900 π.Χ. όταν ένας Αιγύπτιος αντιγραφέας χειρογράφων, χρησιμοποίησε ασυνήθιστα ιερογλυφικά κατά την αντιγραφή μιας επιγραφής. Κάποιοι ειδικοί υποστηρίζουν ότι η κρυπτογραφία προέκυψε αντανακλαστικά λίγο μετά την ανακάλυψη της γραφής και εφαρμόστηκε σε διάφορες περιπτώσεις, από διπλωματικές επιστολές ως και σχέδια μάχης σε περιόδους πολέμου.

Τα πρώτα σημαντικά βήματα της κρυπτογραφίας έγιναν κατά τη διάρκεια των δύο παγκοσμίων πολέμων. Τα πολεμικά κέντρα χρησιμοποιούσαν διάφορες τεχνικές κρυπτογράφησης για την μετάδοση των εντολών τους στα μέτωπα του πολέμου. Εντυπωσιακή ήταν η πρόοδος της επιστήμης της κρυπτογραφίας κατά τη διάρκεια του 2ου παγκοσμίου πολέμου. Διάσημη είναι η κρυπτομηχανή

Enigma που χρησιμοποιήθηκε από τους Γερμανούς για την οργάνωση των γερμανικών υποβρυχίων στον Ατλαντικό. Οι συμμαχικές δυνάμεις είχαν συγκροτήσει μια ομάδα αποτελούμενη από τους καλύτερους επιστήμονες της εποχής με σκοπό την αποκρυπτογράφηση του συγκεκριμένου κώδικα. Χαρακτηριστικό της σπουδαιότητας της επιστήμης της κρυπτογραφίας, είναι το γεγονός πως αρκετοί από του ιστορικούς αναλυτές πιστεύουν πως η έκβαση του πολέμου κρίθηκε από την επιτυχία της επιστημονικής ομάδας να σπάσει τον κώδικα. Η αλαζονεία των Γερμανών που πίστευαν ότι δεν ήταν δυνατή η αποκρυπτογράφηση του κώδικα τους, είχε ως αποτέλεσμα να συνεχίσουν να χρησιμοποιούν την κρυπτομηχανή ακόμα και όταν έλαβαν τις πρώτες ενδείξεις υποκλοπής πληροφοριών από τις συμμαχικές δυνάμεις.

Δεν αποτελεί έκπληξη το γεγονός ότι οι νέες μορφές κρυπτογραφίας παρουσιάστηκαν λίγο μετά την εξάπλωση των ψηφιακών τηλεπικοινωνιών. Σε περιπτώσεις όπου τα δεδομένα πρέπει να μεταδοθούν μέσω μη ασφαλών τηλεπικοινωνιακών καναλιών, η χρήση της κρυπτογραφίας είναι απαραίτητη. Στις παραπάνω περιπτώσεις συγκαταλέγεται κάθε μορφής δίκτυο και ειδικότερα το Διαδίκτυο. Οποιαδήποτε επικοινωνία μεταξύ δύο απομακρυσμένων σημείων θέτει ορισμένα θέματα ασφάλειας:

- **Πιστοποίηση:** Η διαδικασία της εξακρίβωσης της ορθότητας των στοιχείων.
- **Ιδιωτικότητα/Εμπιστευτικότητα:** Η διασφάλιση ότι κανένας δεν είναι σε θέση να διαβάσει την πληροφορία εκτός από τον εξουσιοδοτημένο παραλήπτη.
- **Ακεραιότητα:** Διαβεβαίωση του παραλήπτη ότι το μήνυμα που θα παραλάβει δεν έχει αλλοιωθεί ή παραποιηθεί σε σχέση με το αρχικό.
- **Πιστοποίηση της αυθεντικότητας του αποστολέα:** Μηχανισμός που αποδεικνύει ότι ο φερόμενος ως αποστολέας είναι πραγματικά αυτός που ισχυρίζεται.

Ο ρόλος της κρυπτογράφησης λοιπόν δεν είναι μόνο η προστασία των δεδομένων από κλοπή ή παραποίηση, αλλά και η πιστοποίηση της ταυτότητας του χρήστη.

Στα DRM υπάρχουν κάποιες αναγκαίες προϋποθέσεις κρυπτογράφησης ώστε το σύστημα να είναι ανθεκτικό (**robust),** έχοντας ένα επίπεδο επαρκούς ασφάλειας έτσι ώστε το περιεχόμενο να παραμένει ασφαλές κάτω από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση**.**

- **Επαρκής Ασφάλεια:** τα συστήματα κρυπτογράφησης πρέπει να είναι αρκετά ασφαλή ανάλογα με το περιεχόμενο που προστατεύουν. Παραδείγματος χάριν, μια δημοσίευση εμπορικών βιβλίων είναι πιθανό να χρειάζεται λιγότερη ασφάλεια από ότι ένα κυβερνητικό έγγραφο για πληροφορίες που αφορούν πυρηνικά όπλα. Όμως υπάρχει ένα trade-off ανάμεσα στο επίπεδο της κρυπτογράφησης και στην ευκολία που προσφέρει στον χρήστη, με την έννοια ότι όσο πιο ασφαλής είναι η κρυπτογράφηση τόσο πιο δύσκολη είναι η χρήση της.
- **Ευκολία Χρήστη:** τα συστήματα κρυπτογράφησης δεν πρέπει να είναι επιζήμια για το χρήστη όσον αφορά την χρήση. Παραδείγματος χάριν, δεν θα είναι αποδεκτό ένα σύστημα κρυπτογράφησης που απαιτεί ένας χρήστης να περιμένει μια μεγάλη και αδικαιολόγητη χρονική περίοδο ενώ επηρεάζεται και η διαδικασία ασφάλειας.
- **Ευπάθεια:** ακόμη και τα καλύτερα συστήματα κρυπτογράφησης θα παραβιαστούν τελικά. Εντούτοις, ένα σύστημα κρυπτογράφησης πρέπει να κατασκευαστεί όσο το δυνατόν καλύτερα ώστε μια παραβίαση να μην επηρεάσει τη θεμελιώδη ασφάλεια του συστήματος, αλλά μόνο την συγκεκριμένη συσκευή ή χρήστη.
- **Δυνατότητα Ανανέωσης:** μετά από μια ριζική παραβίαση, πρέπει να είναι δυνατό να αποκατασταθεί η ασφάλεια σε όλο το σύστημα με μια γρήγορη αναβάθμιση λογισμικού.

- **Δυνατότητα ανάκλησης:** σε ένα ασφαλές σύστημα πρέπει να είναι δυνατή η απαγόρευση της πρόσβασης ενός χρήστη σε αυτό. Παραδείγματος χάριν, εάν είναι γνωστό ότι η ταυτότητα ενός χρήστη έχει κλαπεί, πρέπει να μπορεί να αποτραπεί ένα μη εξουσιοδοτημένο άτομο από το να χρησιμοποιήσει την ταυτότητα αυτή για να έχει πρόσβαση στο σύστημα. Αυτό μπορεί να επιτευχθεί με την απόσυρση των δικαιωμάτων πρόσβασης που έχει η κλεμμένη ταυτότητα.

Πολλά από τα προβλήματα που προκύπτουν από την επιβολή των νόμων περί πνευματικής ιδιοκτησίας ψηφιακού περιεχομένου, είναι αντίστοιχα με τα προβλήματα που παρουσιάζονται στις ασφαλείς επικοινωνίες και έχουν λυθεί με την χρήση κρυπτογραφικών μεθόδων. Για παράδειγμα, ένα κοινό πρόβλημα είναι η διασφάλιση της ακεραιότητας του ψηφιακού περιεχομένου μετά την διανομή του, ώστε να είναι δυνατή η ανίχνευση οποιασδήποτε αλλαγής έχει υποστεί. Η κρυπτογραφία έχει λύσει το πρόβλημα της ακεραιότητας των μεταδιδόμενων μηνυμάτων χρησιμοποιώντας ψηφιακές υπογραφές και ιδιωτικά κλειδιά. Ωστόσο, τα παραδοσιακά κρυπτογραφικά συστήματα φέρουν ένα σημαντικό μειονέκτημα που τα καθιστά ακατάλληλα για το πρόβλημα της προστασίας των πνευματικών δικαιωμάτων. Δεν έχουν τη δυνατότητα να συσχετίσουν άρρηκτα την κρυπτογραφημένη πληροφορία με ίδιο το αντικείμενο. Οι τεχνικές κρυπτογράφησης έχουν τη δυνατότητα να κρύψουν την πληροφορία κατά την μετάδοσή της και να παρέχουν βοηθητική πληροφορία για την διασφάλιση της ακεραιότητας του περιεχομένου της, ωστόσο η κρυπτογραφία δεν μπορεί να εμφυτεύσει πληροφορία μέσα στο ίδιο το περιεχόμενο του ψηφιακού αρχείου. Επομένως, η αποκλειστική χρήση τεχνικών κρυπτογραφίας δεν μπορεί να παρέχει εγγυήσεις για την αναδιανομή ή την παραποίηση του περιεχομένου, μετά την παράκαμψη των κρυπτογραφικών μηχανισμών. Τέτοιες εγγυήσεις σε σχέση με το ψηφιακό περιεχόμενο μπορούν να παρέχουν μόνο εξειδικευμένα κρυπτογραφικά συστήματα που έχουν τη δυνατότητα να εμφυτεύσουν επιπρόσθετη πληροφορία μέσα στο ψηφιακό μέσο. Στη συνέχεια ακολουθεί μια συνοπτική αναφορά στις

βασικές κατηγορίες κρυπτογραφικών αλγόριθμων και στα μοντέλα εμπιστοσύνης που χρησιμοποιούνται.

3.1.4.2 Κατηγορίες Κρυπτογραφικών Αλγόριθμων

Η κρυπτογράφηση χωρίζεται βασικά σε δυο κατηγορίες. Την συμμετρική και την ασύμμετρη κρυπτογράφηση. Η **συμμετρική κρυπτογράφηση** είναι αυτή που χ**ρησιμοποιεί το ίδιο μέσο και για την κρυπτογράφηση και για την αποκρυπτογράφηση της πληροφορίας – μηνύματος.** Αντίθετα, η **ασύμμετρη κρυπτογράφηση χρησιμοποιεί διαφορετικά μέσα για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας.**

Η **συμμετρική** κρυπτογράφηση είναι γνωστή και ως κρυπτογράφηση **μοναδικού ή μυστικού κλειδιού**, ενώ η **ασύμμετρη** κρυπτογράφηση χρησιμοποιεί ένα **ζεύγος κλειδιών, το ιδιωτικό (προσωπικό) και το δημόσιο** και αναλόγως του είδους κρυπτογράφησης, ονομάζεται επίσης κρυπτογράφηση δημοσίας κλείδας ή κρυπτογράφηση ιδιωτικής κλείδας. Η τελευταία είναι αλλιώς γνωστή και ως ψηφιακή υπογραφή. Στην συνέχεια θα αναπτυχθούν αναλυτικότερα οι μέθοδοι αυτές με τις οποίες επιτυγχάνεται η κρυπτογράφηση και κατά συνέπεια η ασφαλής διακίνηση της πληροφορίας.

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 Ιδιωτικού 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

- **Συναρτήσεις Κατακερματισμού:** Όπου χρησιμοποιούνται μαθηματικοί μετασχηματισμοί για την αμετάκλητη κρυπτογράφηση της πληροφορίας

3.1.4.3 Συμμετρική Κρυπτογράφηση

Η συμμετρική κρυπτογράφηση βασίζεται στην χρησιμοποίηση **ενός μυστικού, κοινού κλειδιού, γνωστού και στον αποστολέα και στον αποδέκτη της πληροφορίας**. Οι ρόλοι φυσικά μπορούν να εναλλάσσονται. Συνεπώς δυο επιχειρήσεις, οργανισμοί, ιδιώτες που θέλουν μεταξύ τους ασφαλή επικοινωνία, μπορούν να μοιράζονται ένα μυστικό 'κλειδί' έναν 'κωδικό' (στην ουσία έναν αλγόριθμο) με τον οποίο ο ένας κρυπτογραφεί και ο άλλος αποκρυπτογραφεί την μεταξύ τους επικοινωνία.

Η αποκρυπτογράφηση του μηνύματος μπορεί να γίνει μόνο από κάποιον που γνωρίζει το κλειδί, συνεπώς η διακίνηση του κλειδιού, δεν μπορεί να γίνει μέσω του ίδιου διαύλου επικοινωνίας στον οποίον διακινείται και το κρυπτογραφημένο μήνυμα. Αυτό ασφαλώς είναι ευνόητο καθώς αν ο δίαυλος θεωρείτο ασφαλής, δεν θα χρειαζόταν η κρυπτογράφηση των μηνυμάτων και εφόσον ο δίαυλος δεν είναι ασφαλής, πιθανή μετάδοση του κλειδιού μέσω του διαύλου αυτού θα μπορούσε να 'υποκλαπεί' από τρίτους, οι οποίοι εν συνεχεία θα είχαν και την δυνατότητα πρόσβασης στην εμπιστευτική πληροφορία. Συνεπώς πρωταρχικής σημασίας είναι το 'κλειδί' να συμφωνηθεί και να διακινηθεί προς τα 'επιθυμητά' και 'επιτρεπτά' μέρη μέσω διαφορετικών, ασφαλών διαύλων επικοινωνίας.

Εφόσον διασφαλιστεί αυτό, αυτός που θέλει να αποστείλει ένα εμπιστευτικό μήνυμα, κρυπτογραφεί το μήνυμα εφαρμόζοντας τον συγκεκριμένο συμφωνημένο και κοινό αλγόριθμο ('κλειδί'), με αποτέλεσμα η πληροφορία να διακινείται σε μορφή αδύνατον να αναγνωριστεί και να διαβαστεί από οποιονδήποτε. Όταν το μήνυμα φτάσει στον προορισμό του, ο παραλήπτης

εφαρμόζοντας τον ίδιον αλγόριθμο, αποκρυπτογραφεί το μήνυμα και μπορεί πλέον να το διαβάσει.

Αλγόριθμοι Συμμετρικής Κρυπτογράφησης

Ενδεικτικά αναφέρονται εδώ ορισμένοι από τους πιο γνωστούς και ευρύτερα χρησιμοποιημένους αλγόριθμους συμμετρικής κρυπτογράφησης. Αυτοί είναι είτε οι **block ciphers** ή 'τμηματικοί' αλγόριθμοι είτε οι **stream ciphers** ή σειριακοί αλγόριθμοι.

Οι block ciphers είναι αλγόριθμοι που μετατρέπουν ένα block (ένα τμήμα) καθορισμένου μήκους κειμένου (μη κρυπτογραφημένου εννοείται - plaintext), σε block κρυπτογραφημένου κειμένου του ίδιου μήκους (ciphertext). Ο μετασχηματισμός πραγματοποιείται μέσω ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με αντίστροφη διαδικασία (αντίστροφο μετασχηματισμό) στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί (συμμετρική κρυπτογράφηση). Το καθορισμένο μήκος για τους περισσότερους αλγορίθμους (ciphers) είναι 64 bits.

Από τους πιο γνωστούς block ciphers είναι οι:

- **DES (Data Encryption Standard):** πρόκειται για τον ευρύτερα διαδεδομένο block αλγόριθμο (και χρησιμοποιούμενο από το 1976) ο οποίος κρυπτογραφεί ανά τμήματα 64 bit χρησιμοποιώντας κλειδί 56 bit (ή 64 με τα 8 ως bit ισοτιμίας). 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): αναπτύχθηκε το 1990 από τους Lai και Massey, είναι δομημένος όπως ο DES, κρυπτογραφεί επίσης τμήματα των 64 bit αλλά χρησιμοποιεί κλειδί 128 bit και είναι πολύ πιο ισχυρός από τον DES.
- 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.

Οι Stream Ciphers είναι εξαιρετικά ταχείς αλγόριθμοι και σε αντίθεση με τους block ciphers λειτουργούν με μικρότερες μονάδες κειμένου, συνήθως bits. Επιπλέον αντιθέτως με τους block ciphers όπου η κρυπτογράφηση ενός συγκεκριμένου κειμένου με το ίδιο κλειδί, θα είχε πάντα το ίδιο αποτέλεσμα, εδώ ο μετασχηματισμός των μικρών αυτών μονάδων θα ποικίλει αναλόγως του πότε θα αντιμετωπίζονται. Συνεπώς ως προς τις ιδιότητες τους είναι One-time Pad αλγόριθμοι. Για την κρυπτογράφηση παράγουν μια ακολουθία από bits που ονομάζεται key-stream η οποία συνδυάζεται με το κείμενο μέσω μιας X-OR πράξης. Ο ευρύτερα χρησιμοποιούμενος μηχανισμός για την παραγωγή του key-stream είναι ο LFSR (Linear Feedback Shift Register) του οποίου άλλοι συνδυασμοί μπορεί να είναι ο Shift Register Cascade και ο Shrinking ή Self Shrinking Generator.

- RC4: όπως οι RC2 και RC5 δημιουργήθηκε επίσης από τον Ron Rivest για λογαριασμό της RSA. Έχει ομοίως μεταβλητό μήκος κλειδιού, αλλά λειτουργεί σε

επίπεδο byte, θεωρείται εξαιρετικά ασφαλής και ταχύς και είναι ο ευρύτερα χρησιμοποιούμενος.

- A5: Stream Cipher για την προστασία της επικοινωνίας μέσω GSM κινητών τηλεφώνων. Έχει διάφορες εκδόσεις οι οποίες όμως όλες 'έσπασαν' και χρησιμοποιεί τριπλό μηχανισμό LFSR.
- SEAL (Software–optimized Encryption Algorithm): Τα δεδομένα κρυπτογραφούνται ένα bit την φορά και χρησιμοποιεί κλειδί 160 bit.

3.1.4.4 Ασσύμετρη Κρυπτογράφηση

Σε αντίθεση με την συμμετρική κρυπτογράφηση η ασύμμετρη χρησιμοποιεί ένα ζεύγος 'κλειδών', μαθηματικά συσχετισμένων μεταξύ τους. Ένα δημόσιο (public key) και ένα ιδιωτικό (private key). Η χρήση του ζεύγους αυτού κατά την κρυπτογράφηση συνεπάγεται ότι το ένα 'κλειδώνει' ή κρυπτογραφεί το κείμενο και το άλλο το 'ξεκλειδώνει' ή το αποκρυπτογραφεί. Έτσι υπάρχει η κρυπτογράφηση δημόσιου κλειδιού και η κρυπτογράφηση ιδιωτικού κλειδιού ή αλλιώς ψηφιακή υπογραφή.

Η ασύμμετρη κρυπτογράφηση επινοήθηκε για να αντιμετωπίσει το πρόβλημα που αναφέρθηκε στην συμμετρική κρυπτογράφηση ή μάλλον το κυριότερο μειονέκτημα της, αυτό δηλαδή της ασφαλούς διακίνησης του μυστικού κλειδιού. Εφόσον χρησιμοποιεί δυο κλειδιά, το ένα μπορεί να είναι γνωστό και το άλλο πρέπει υποχρεωτικά να είναι απόρρητο. Έτσι επιλύεται το πρόβλημα της μετάδοσης του κλειδιού καθώς δεν ενδιαφέρει αν θα μαθευτεί το δημόσιο, η κρυπτογράφηση όμως είναι πολύ πιο αργή. Στην συνέχεια θα περιγραφεί η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης με την χρήση αυτού του ζεύγους των κλειδών. Η μόνη απαραίτητη προϋπόθεση είναι, ο συσχετισμός του δημόσιου και του ιδιωτικού κλειδιού (στην ουσία του δημόσιου κλειδιού με τον κάτοχο του, ο οποίος είναι ασφαλώς και ο μοναδικός που θα πρέπει να γνωρίζει το ιδιωτικό) να γίνεται από έμπιστη και έγκυρη πηγή. Τέτοια

παραδείγματος χάριν είναι η verisign.com η οποία είναι μια εταιρία που πιστοποιεί ότι το δημόσιο κλειδί που ισχυρίζεται κάποιος ότι του ανήκει (και με το οποίο μπορεί οποιοσδήποτε το γνωρίζει να του αποστείλει εμπιστευτικά μηνύματα), ανήκει πραγματικά σ' αυτόν και όχι σε κάποιον άλλον.

Ασσύμετρη Κρυπτογράφηση Δημόσιου Κλειδιού

Η **Κρυπτογράφηση Δημόσιου Κλειδιού** - ΚΔΚ (Public Key Cryptography - PKC) θεωρείται η τελευταία σημαντική εξέλιξη που έλαβε χώρα στον τομέα της κρυπτογραφίας τα τελευταία 300 με 400 χρόνια. Η ΚΔΚ στη σύγχρονη μορφή της, παρουσιάστηκε αρχικά από τον Καθηγητή Πανεπιστημίου του Stanford Martin Hellman, και τον απόφοιτο Whitfield Diffie το 1976. Η εργασία τους περιέγραφε ένα κρυπτογραφικό σύστημα δύο κλειδιών, όπου δύο άνθρωποι μπορούσαν να επικοινωνήσουν με ασφάλεια πάνω από ένα μη ασφαλές κανάλι επικοινωνίας χωρίς να χρειάζεται να γνωρίζουν το ίδιο μυστικό κλειδί.

Το μαθηματικό τέχνασμα στο οποίο βασίζεται η ΚΔΚ είναι η ύπαρξη των λεγόμενων μονόδρομων συναρτήσεων που ενώ είναι αρκετά απλές κατά τον υπολογισμό τους, δεν συμβαίνει το ίδιο και κατά τον υπολογισμό των αντίστροφων τους που είναι συγκριτικά δύσκολος.

Στη απλή της μορφή η ΚΔΚ χρησιμοποιεί δύο κλειδιά τα οποία συσχετίζονται μαθηματικά χωρίς όμως η γνώση του ενός να επιτρέπει την εύκολη εύρεση του άλλου. Το ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση του κειμένου, ενώ το άλλο κλειδί χρησιμοποιείται για την αποκρυπτογράφηση του. Το σημαντικό στοιχείο είναι πως δεν έχει σημασία πιο κλειδί θα χρησιμοποιηθεί πρώτο, αλλά το ότι και τα δύο κλειδιά είναι απαραίτητα για την συνολική διαδικασία. Καθώς η ΚΔΚ απαιτεί ένα ζεύγος κλειδιών ονομάζεται επίσης και ασύμμετρη κρυπτογραφία.

Στην ΚΔΚ, ένα από τα δύο κλειδιά χαρακτηρίζεται ως δημόσιο κλειδί και μπορεί να διαμοιραστεί σε όσο μεγάλο εύρος αποδεκτών επιθυμεί ο ιδιοκτήτης. Το άλλο κλειδί χαρακτηρίζεται ως ιδιωτικό και δεν πρέπει να διαρρεύσει σε μη εξουσιοδοτημένο χρήστη.

Ασσύμετρη Κρυπτογράφηση Ιδιωτικού Κλειδιού - Ψηφιακή Υπογραφή

Συχνά όταν ακούει κανείς τον όρο υπογραφή, αντιλαμβάνεται μια ιδιόχειρη γραφή με την οποία επιβεβαιώνει την βούληση, την συμφωνία ή την εγγύηση του ο υπογράφων. Η ψηφιακή υπογραφή όμως, δεν έχει σχεδόν καμία σχέση με την ιδιόχειρη υπογραφή, παρά μόνο στο γεγονός ότι και με την ψηφιακή υπογραφή, βεβαιώνεται η ταυτότητα και η βούληση αυτού που υπογράφει. Όπως αναφέρθηκε και παραπάνω η ψηφιακή υπογραφή, αποτελεί μια άλλη μέθοδο κρυπτογράφησης και συγκεκριμένα ασύμμετρης κρυπτογράφησης η οποία επιτυγχάνεται με την χρήση του ιδιωτικού κλειδιού αυτού που κρυπτογραφεί. Εφόσον το κλειδί είναι ιδιωτικό και δεν έχει διαρρεύσει (και είναι ευθύνη του κατόχου του να μην διαρρεύσει) όταν κάποιος λαμβάνει ένα μήνυμα ή μια πληροφορία η οποία έχει κρυπτογραφηθεί με ιδιωτικό κλειδί (όταν δηλαδή δει μια ψηφιακή υπογραφή) είναι σίγουρος ότι το μήνυμα αυτό έχει σταλεί από αυτόν που το υπογράφει. Η επιβεβαίωση γίνεται εφόσον η υπογραφή αποκρυπτογραφηθεί με το δημόσιο κλειδί του αποστολέα. Εκτός αυτού όμως, λόγω της μεθόδου που ακολουθείται, ο αποδέκτης της πληροφορίας, είναι σίγουρος εφόσον επιβεβαιωθεί η ταυτότητα του αποστολέα, ότι η πληροφορία είναι επίσης αναλλοίωτη. Συνεπώς εκτός της προέλευσης πιστοποιείται και η ακεραιότητα του μηνύματος.

Ας περιγραφεί όμως το πώς προκύπτει η αυθεντικότητα. Ο αποστολέας ή δημιουργός του μηνύματος, αφού ολοκληρώσει το μήνυμα που επιθυμεί να στείλει, δημιουργεί με αλγορίθμους κατατεμαχισμού ή κατακερματισμού, μια

σύνοψη του μηνύματος την οποία και κρυπτογραφεί. Η κρυπτογράφηση αυτή γίνεται με το ιδιωτικό κλειδί του αποστολέα το οποίο μόνον αυτός γνωρίζει. Όταν ο παραλήπτης ή αποδέκτης του μηνύματος, λάβει το κείμενο με την ψηφιακή υπογραφή, αποσπά την ψηφιακή υπογραφή και χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα, πιστοποιεί την ταυτότητα του. Παράλληλα έχει αποκρυπτογραφήσει και την σύνοψη του μηνύματος, η οποία δεν μπορεί με κανέναν τρόπο να αλλοιωθεί. Εν συνεχεία ακολουθώντας τον ίδιο αλγόριθμο κατακερματισμού (τον ίδιο που είχε χρησιμοποιήσει και ο αποστολέας) δημιουργεί την σύνοψη του μηνύματος που έλαβε. Σε περίπτωση που το κείμενο είχε αλλοιωθεί, η σύνοψη που θα δημιουργηθεί από τον αποδέκτη, θα διαφέρει από την σύνοψη που είχε δημιουργήσει και κρυπτογραφήσει αρχικά ο αποστολέας. Συνεπώς παραβάλλοντας τις δυο συνόψεις ο αποδέκτης μπορεί να εξακριβωθεί τόσο για την προέλευση όσο και για την ακεραιότητα του μηνύματος. Ο αποστολέας μπορεί αν θέλει να κρυπτογραφήσει το μήνυμα και με την δημόσια κλείδα του αποδέκτη (έτσι επιτυγχάνεται και η εμπιστευτικότητα του μηνύματος).

Αλγόριθμοι Ασύμμετρης Κρυπτογράφησης

- 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.

Συναρτήσεις Κατακερματισμού – Hash Functions

Πρόκειται για έναν μετασχηματισμό στο οποίο εισάγεται ένα μήνυμα οποιουδήποτε μήκους και εξάγει μια ακολουθία χαρακτήρων περιορισμένου μήκους, την hash value. Οι συναρτήσεις κατακερματισμού που ονομάζονται επίσης και κωδικοποίηση μηνύματος καθώς και μονόδρομη κρυπτογράφηση, είναι αλγόριθμοι που κατά κάποιο τρόπο δεν χρησιμοποιούν κλειδί. Αντί αυτού, μία τιμή κατακερματισμού σταθερού μεγέθους υπολογίζεται με βάση το μη κωδικοποιημένο κείμενο, ώστε να είναι αδύνατη η ανάκτηση του περιεχομένου ή του μεγέθους του κειμένου. Η ορθότητα του αλγόριθμου οφείλεται στο γεγονός πως η πιθανότητα για δύο διαφορετικά κείμενα να παράγουν την ίδια τιμή κατακερματισμού είναι σχεδόν μηδενική.

Αλγόριθμοι Κατακερματισμού

- 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.

Ψηφιακοί Φάκελοι - Digital Envelopes

Αναφέρθηκε παραπάνω ότι το κυριότερο μειονέκτημα της συμμετρικής κρυπτογράφησης είναι η ασφαλής μετάδοση του μυστικού κλειδιού ενώ της ασύμμετρης μειονέκτημα είναι ο χρόνος κρυπτογράφησης που είναι κατά πολύ μεγαλύτερος από αυτόν της συμμετρικής. Οι **Ψηφιακοί Φάκελοι αποτελούν έναν συνδυασμό της συμμετρικής και ασύμμετρης κρυπτογράφησης** προκειμένου να επιτευχθεί η **ασφαλής μετάδοση της πληροφορίας** που προσφέρει η ασύμμετρη κρυπτογράφηση και η **ταχύτητα** που προσφέρει η συμμετρική κρυπτογράφηση. Έτσι σε έναν ψηφιακό φάκελο, το κείμενο ή το μήνυμα κρυπτογραφείται συμμετρικά, με ένα μυστικό κλειδί δηλαδή και το κλειδί αυτή κρυπτογραφείται με το δημόσιο κλειδί του αποδέκτη του μηνύματος. Συνεπώς μόνο ο αποδέκτης που γνωρίζει το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μυστικό και εν συνεχεία χρησιμοποιώντας το, μπορεί να αναγνώσει το κείμενο που έχει κρυπτογραφηθεί συμμετρικά. Προκειμένου να επιτευχθεί αυτή η ανταλλαγή μυστικού κλειδιού υπάρχουν συγκεκριμένα

πρωτόκολλα, με ευρύτερα γνωστό και χρησιμοποιούμενο το Diffie Hellman Key Exchange.

Cryptolopes

Μια άλλη εφαρμογή της κρυπτογράφησης είναι οι Cryptolopes. Πρόκειται για φακέλους στους οποίους εμπεριέχεται κρυπτογραφημένο και μη υλικό, κείμενα και τα λοιπά. Το μη κρυπτογραφημένο υλικό μπορεί να είναι όροι χρήσης ή απλό κείμενο. Μπορεί παραδείγματος χάριν η εφαρμογή αυτή να χρησιμοποιηθεί σε Ψηφιακές Βιβλιοθήκες, παρέχοντας στα μη κρυπτογραφημένα μέρη περιλήψεις άρθρων και όρους χρήσης των άρθρων αυτών και το ίδιο το άρθρο να είναι κρυπτογραφημένο, ούτως ώστε να έχει πρόσβαση σ' αυτό οποιοσδήποτε συμφωνήσει πρώτα και τηρήσει τους όρους χρήσης του.

3.1.5 Στεγανογραφία

Ενώ η κρυπτογραφία έχει στόχο την προστασία του περιεχομένου των μηνυμάτων, η στεγανογραφία έχει στόχο την απόκρυψη της ίδιας της ύπαρξης τους. Η λέξη στεγανογραφία προέρχεται από τις ελληνικές λέξεις στέγανο-ς και γραφ-ειν που ετυμολογικά σημαίνουν "συγκαλυμμένη γραφή" και χρησιμοποιείται για να περιγράψει την διαδικασία της απόκρυψης πληροφορίας μέσα σε άλλη πληροφορία.

3.1.5.1 Στεγανογραφία Με Τεχνολογικά Μέσα

Το πιο διάσημο ιστορικό παράδειγμα στεγανογραφίας πηγάζει από την αρχαιότητα. Ο Ηρόδοτος διηγείται ότι γύρω στο 440 π.Χ ο Ιστιαίος ξύρισε το κεφάλι του πιο έμπιστου δούλου του και έγραψε σε αυτό το μήνυμα που ήθελε να στείλει. Όταν τα μαλλιά του δούλου μεγάλωσαν το μήνυμα ήταν πια αόρατο. Στη συνέχεια ο δούλος αναχώρησε για τον προορισμό του με ρητή εντολή να

του ξυρίσουν το κεφάλι με την άφιξη του. Με αυτό τον τρόπο ο Ιστιαίος κατάφερε να υποκινήσει μια εξέγερση κατά των Περσών. Ανάλογες ιστορικές αναφορές δημιουργούν μια μεγάλη λίστα από παραδείγματα χρήσης στεγανογραφικών μεθόδων για την απόκρυψη πληροφορίας μέσα σε άλλη πληροφορία. Μερικά παραδείγματα είναι, η απόκρυψη μηνυμάτων στις πατούσες των αγγελιοφόρων ή στα σκουλαρίκια των γυναικών, κείμενα που γράφονταν σε πλάκες από ξύλο και μετά ασβεστώνονταν κ.α. Άλλες περιπτώσεις περιλαμβάνουν, την απόκρυψη κειμένου με την αλλαγή του μεγέθους των γραμμάτων ή κάνοντας πολύ μικρές τρύπες πάνω ή κάτω από τα γράμματα σε κάποια κείμενα που χρησιμοποιούνται ως επικάλυψη. Η πιο διαδομένη ίσως τεχνική στεγανογραφίας είναι η γραφή μηνυμάτων με αόρατο μελάνι. Πρόκειται για ειδικές ουσίες που γίνονταν ορατές μόνο κάτω από συγκεκριμένες συνθήκες, όπως θερμότητα, υπεριώδη ακτινοβολία κ.α. Χωρίς αυτές τις συνθήκες δεν υπάρχει καμία ένδειξη κειμένου πάνω στο χαρτί. Το αόρατο μελάνι χρησιμοποιήθηκε εκτενώς από τους Γερμανούς κατά τη διάρκεια των δύο παγκοσμίων πολέμων.

3.1.5.2 Στεγανογραφία Με Γλωσσολογικά Μέσα

Μια ευρέως διαδεδομένη τεχνική γλωσσολογικής στεγανογραφίας είναι οι ακροστιχίδες. Το πιο διάσημο παράδειγμα είναι ίσως το έργο του Giovanni Boccaccio "Amorosa visione" το οποίο θεωρείται η μεγαλύτερη γνωστή ακροστιχίδα. Ο Boccaccio έγραψε αρχικά τρία σονέτα μεγέθους 1.500 γραμμάτων. Στη συνέχεια έγραψε μια σειρά από ποιήματα τοποθετώντας στα αρχικά των διαδοχικών τρίστιχων τα γράμματα που σχημάτιζαν τα σονέτα του.

Ο John Wilkins περιέγραψε πως «δύο Μουσικοί μπορούσαν να επικοινωνούν μεταξύ τους χρησιμοποιώντας τα μουσικά τους όργανα με την ίδια ευχέρεια που θα επικοινωνούσαν χρησιμοποιώντας την ανθρώπινη ομιλία».

Πρότεινε ακόμα μία μέθοδο για την απόκρυψη μηνύματος σε ένα γεωμετρικό σχήμα χρησιμοποιώντας τις τελείες, τις γραμμές και τα τρίγωνα.

Μία εύκολη βελτιστοποίηση που μπορεί να γίνει, είναι η απόκρυψη του μηνύματος σε μια τυχαία θέση μέσα στο μέσο. Η γενική ιδέα αποτελεί την καρδιά πολλών στεγανογραφικών συστημάτων. Σύμφωνα με ένα πρωτόκολλο ασφάλειας που χρησιμοποιήθηκε στην αρχαία Κίνα, ο αποστολέας και ο παραλήπτης του μηνύματος είχαν αντίγραφα από ένα χαρτόνι με τρύπες σε τυχαία σημεία. Αρχικά ο αποστολέας τοποθετούσε το χαρτόνι πάνω σε ένα κομμάτι χαρτί και έγραφε τα γράμματα του μηνύματος που ήθελε να στείλει μέσα στις τρύπες. Στη συνέχεια αφού είχε αφαιρέσει το εξωτερικό χαρτόνι έγραφε κάποιο κείμενο που να ταίριαζε με τα γράμματα που είχαν γραφεί ήδη πάνω στο χαρτί. Όταν ο παραλήπτης λάμβανε το γράμμα τοποθετούσε το δικό του αντίτυπο από το χαρτόνι και σχημάτιζε το μήνυμα διαβάζοντας τα γράμματα που φαινόντουσαν από τις τρύπες. Στις αρχές του 16ου αιώνα ο Cardan (1501-1576), Ιταλός μαθηματικός, ξαναανακάλυψε την μέθοδο και την ονόμασε Cardan grille.

3.1.5.3 Στεγανογραφικά Εργαλεία Και Μέθοδοι

Ο σκοπός της συγκεκριμένης παραγράφου είναι να πραγματοποιήσει μια επισκόπηση και συνοπτική περιγραφή των κύριων εργαλείων που διατίθενται ελεύθερα στην αγορά και υλοποιούν μερικές από τις βασικότερες στεγανογραφικές μεθόδους. Ο στόχος των παραπάνω μεθόδων είναι να αποκρύψουν πληροφορία μέσα στα ψηφιακά αρχεία, δείχνοντας πως μπορεί κάποιος να ενσωματώσει κρυφά μηνύματα σε κάποιους από τους πιο διαδεδομένους τύπους αρχείων εικόνας, ήχου και κειμένου. Η συνοπτική αναφορά των στεγανογραφικών μεθόδων που θα ακολουθήσει περιλαμβάνει την περιγραφή μιας μεθόδου για κάθε τύπο αρχείων, ενώ συνοδεύεται παράλληλα από μια αναφορά σε κάποιο εργαλείο που την υλοποιεί.

Στο χώρο της στεγανογραφίας έχει παγιωθεί μια ορισμένη ορολογία ώστε να είναι ξεκάθαρος ο διαχωρισμός ανάμεσα στην πληροφορία που πρόκειται να κρυφθεί, την πληροφορία μέσα στην οποία θα κρυφθεί και την πληροφορία που προκύπτει από τον συνδυασμό των δύο παραπάνω. Οι όροι που θα χρησιμοποιηθούν είναι οι ακόλουθοι:

- **Κάλυμμα (Cover):** χρησιμοποιείται για να περιγράψει το αρχικό, αμετάβλητο, αθώο μήνυμα.
- **Εμφυτευμένη Πληροφορία (Embedded Data):** χρησιμοποιείται για να περιγράψει την πληροφορίας που πρόκειται να τοποθετηθεί με στεγανογραφικό τρόπο στο κάλυμμα.
- **Stego-πληροφορία (Stego data):** χρησιμοποιείται για να περιγράψει την πληροφορία που προκύπτει μετά την εφαρμογή της στεγανογραφικής μεθόδου.

3.1.5.3.1 Απόκρυψη Πληροφορίας Σε Κείμενο

Η στεγανογραφία σε αρχεία κειμένου μπορεί να επιτευχθεί με την χρήση ποικίλων τεχνικών. Οι μέθοδοι που μπορούν να εφαρμοστούν σε αρχεία κειμένου, τόσο σε ηλεκτρονική όσο και σε έντυπη μορφή, περιλαμβάνουν τεχνικές κωδικοποίησης μετατόπισης γραμμών, κωδικοποίησης μετατόπισης λέξεων και κωδικοποίησης χαρακτηριστικών, καθώς και τεχνικές συντακτικού ή σημασιολογικού χαρακτήρα. Οι τρεις πρώτες τεχνικές βασίζονται στην οπτική αλλοίωση της μορφοποίησης ή της όψης του κειμένου, τροποποιώντας το μέγεθος του κενού μεταξύ διαδοχικών γραμμών, του κενού μεταξύ των λέξεων ή ακόμα και κάποια ιδιαίτερα χαρακτηριστικά των γραμμάτων. Ένα απλό παράδειγμα είναι η χρήση ενός ή δύο κενών χαρακτήρων μεταξύ διαδοχικών λέξεων για την κωδικοποίηση δυαδικών τιμών και χρήση των δυαδικών τιμών για την αναπαράσταση πληροφορίας. Οι συντακτικές και οι σημασιολογικές μέθοδοι

στεγανογραφίας σε αρχεία κειμένου αξιοποιούν κάποιες ανεπαίσθητες αλλοιώσεις στην ορθογραφία και τη δομή του κειμένου χωρίς να επηρεάζουν σημαντικά το νόημα ή το ύφος του. Αυτό επιτυγχάνεται με την αναδιατύπωση κάποιων προτάσεων ή χρησιμοποιώντας ζεύγη συνωνύμων λέξεων κάθε ένα από τα οποία συνιστά μια συγκεκριμένη τιμή. Για παράδειγμα η εναλλαγή στη χρήση των λέξεων «ευχαρίστηση» και «ικανοποίηση» σε ένα κείμενο μπορεί να υποδηλώνει δυαδικούς άσσους και μηδενικά. Η αδυναμία που παρουσιάζουν οι παραπάνω στεγανογραφικές τεχνικές είναι η οπτική αλλοίωση που εισάγεται στο κείμενο καθώς και η αλλαγή του νοήματος στις περιπτώσεις της συντακτικής ή σημασιολογικής στεγανογραφίας.

3.1.5.3.2 Απόκρυψη Πληροφορίας Σε Αρχεία Ήχου και Εικόνας

Συνήθως, η χρήση των αρχείων εικόνας με τη μορφή ξενιστών για την εισαγωγή στεγανογραφικών μηνυμάτων βασίζεται στην εκμετάλλευση των περιορισμένων δυνατοτήτων που χαρακτηρίζουν το ανθρώπινο σύστημα όρασης. Η κωδικοποίηση επιπλέον πληροφορίας στο ψηφιακό περιεχόμενο μιας εικόνας έχει ως αποτέλεσμα την αλλοίωση των τιμών ορισμένων αν όχι όλων των pixels. Ωστόσο, η συγκεκριμένη αλλοίωση δεν έχει κανένα αντίκτυπο στο οπτικό αποτέλεσμα της εικόνας, τουλάχιστον για το ανθρώπινο σύστημα όρασης. Μερικές από τις πιο συνήθεις τεχνικές για την κωδικοποίηση μηνυμάτων σε αρχεία εικόνας, μπορούν να κατηγοριοποιηθούν σε δύο κατηγορίες. Σε αυτές που δρουν απευθείας στο περιεχόμενο της εικόνας και σε αυτές που χρησιμοποιούν κάποιους μετασχηματισμούς. Οι τεχνικές που δρουν απευθείας στο περιεχόμενο της εικόνας τροποποιούν την ψηφιακή εικόνα σε επίπεδο bit. Μία από τις πιο γνωστές τεχνικές που ανήκουν σε αυτήν την κατηγορία είναι η μέθοδος του λιγότερου σημαντικού bit. Αντίθετα στη περίπτωση της χρήσης μετασχηματισμών, η τροποποίηση πραγματοποιείται στους συντελεστές που προκύπτουν από την εφαρμογή τους στο περιεχόμενο της εικόνας.

Η απόκρυψη πληροφορίας σε αρχεία ήχου θεωρείται περισσότερο πολύπλοκη καθώς το ανθρώπινο σύστημα ακοής είναι σαφώς πιο ευαίσθητο από το σύστημα όρασης. Εκτός από τη μέθοδο του λιγότερο σημαντικού bit που λειτουργεί με τον ίδιο τρόπο και στα αρχεία ήχου, υπάρχουν αρκετές ακόμα τεχνικές που χρησιμοποιούνται για την απόκρυψη μηνυμάτων μέσα σε μουσικά έργα. Η κωδικοποίηση φάσης λειτουργεί αντικαθιστώντας την φάση ενός τμήματος του ηχητικού σήματος με μία ενδεικτική φάση που αναπαριστά τα δεδομένα. Η συγκεκριμένη τεχνική είναι μία από τις πιο αποτελεσματικές τεχνικές κωδικοποίησης ιδιαίτερα σε ότι αφορά τον «λόγο του σήματος προς το θόρυβο», ελαχιστοποιώντας πραγματικά τα ηχητικά παραπροϊόντα της ενσωμάτωσης της πληροφορίας. Μία άλλη ομάδα βασίζεται στον διασκορπισμό της πληροφορίας σε όλο το εύρος του φάσματος των συχνοτήτων του ηχητικού σήματος. Τέλος, η κωδικοποίηση της πληροφορίας μπορεί να γίνει με την μεταβολή του αρχικού πλάτους του σήματος, την εξασθένηση του ρυθμού και την καθυστέρηση της αντήχησης.

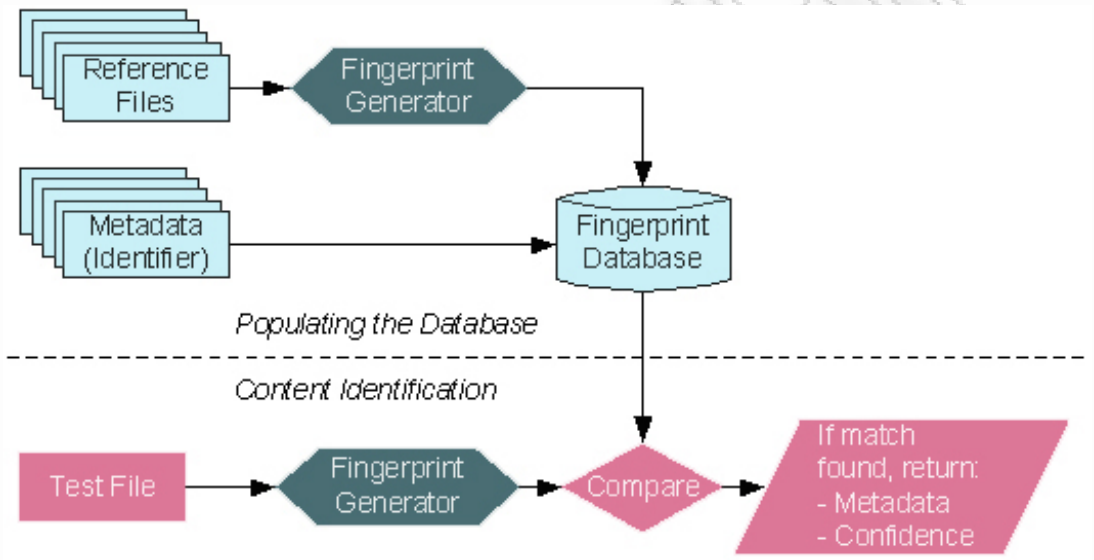
3.2 Τεχνολογικά Μέσα Προστασίας - Τεχνολογίες Μόνιμης Συσχέτισης

Σε αυτό το σημείο δίνεται μια επισκόπηση διάφορων τεχνολογιών που μπορούν να χρησιμοποιηθούν για να καλύψουν τις υψηλού επιπέδου απαιτήσεις για τη μόνιμη συσχέτιση της πληροφορίας με το περιεχόμενο. Οι τεχνολογίες είναι: **fingerprinting, υδατογράφηση, και ψηφιακές υπογραφές.**

3.2.1 Fingerprinting

Οι τεχνολογίες fingerprinting μπορούν να χρησιμοποιηθούν για να αναγνωρισθεί το περιεχόμενο μέσω της διαδικασίας που απεικονίζεται στο παρακάτω διάγραμμα. 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.



Εικόνα 1: Εισαγωγή Fingerprint

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, που απεικονίζεται στο παραπάνω διάγραμμα, 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.

3.2.2 Υδατογράφηση

Η υδατογράφηση χρησιμοποιείται συχνά ως τεχνολογία προστασίας πνευματικών δικαιωμάτων. Το υδατογράφημα είναι "αδιόρατες ενσωματωμένες πληροφορίες". Αυτές οι πληροφορίες (συχνά αρχείο ή αναγνωριστικό IP) μπορούν να εξαχθούν από ειδικό λογισμικό, αν και είναι αδιόρατες στους κανονικούς χρήστες.

Η στεγανογραφία επιδιώκει την απόκρυψη της πληροφορίας χωρίς να λαμβάνει υπόψη το ενδεχόμενο επίθεσης σε αυτήν, προφυλάσσοντάς την μέσα σε κάποιο «στεγανό».

Η κρυπτογραφία εξασφαλίζει ότι η πληροφορία που θα διαβαστεί από μη εξουσιοδοτημένους χρήστες θα είναι άχρηστη και ακατανόητη ή παραπλανητική.

Η ψηφιακή υδατογράφηση διαφοροποιείται από τις δύο παραπάνω μεθόδους, καθώς συνδυάζονται δύο κομμάτια πληροφορίας (η πρωτότυπη και η προστιθέμενη – το υδατογράφημα), με τέτοιο τρόπο ώστε να μπορούν να επεξεργαστούν ανεξάρτητα. Η ψηφιακή υδατογράφηση έχει στόχο την εξασφάλιση της εγκυρότητας ενός αντικειμένου (π.χ. ηλεκτρονικού εγγράφου, ψηφιακού πίνακα), το αναμφισβήτητο της ταυτότητας του ιδιοκτήτη του και ασφαλώς την αποκατάστασή του σε περίπτωση παραποίησης.

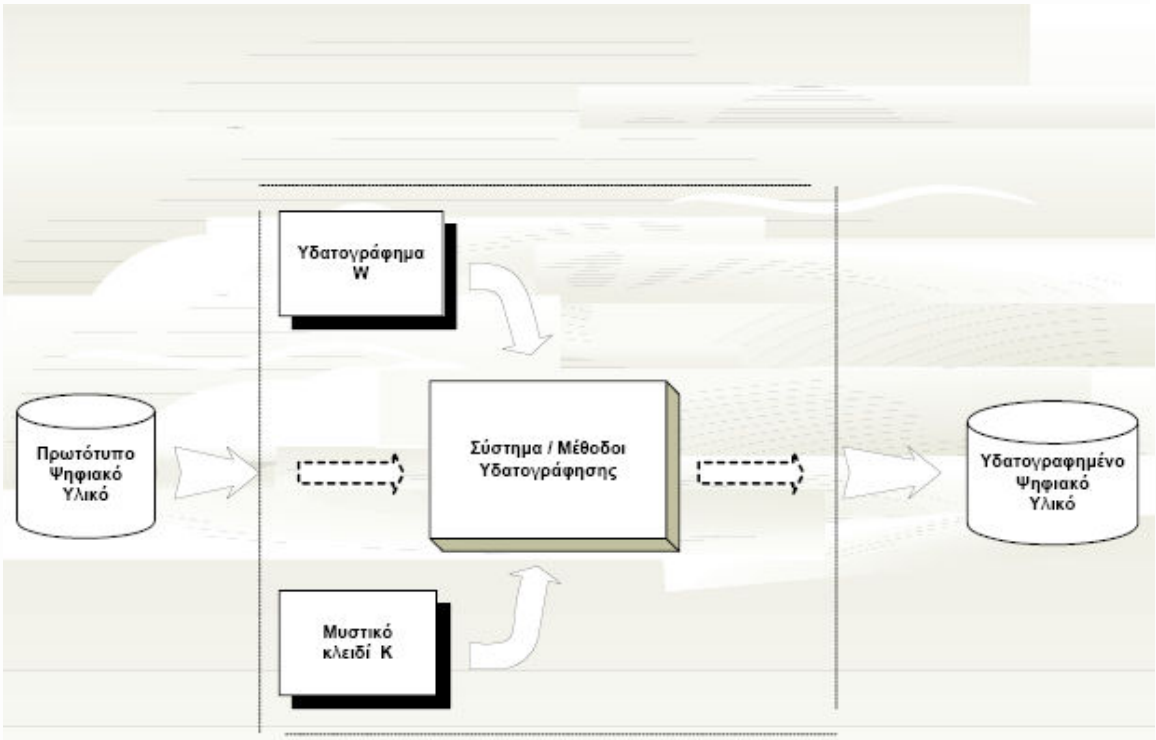
Τα χαρακτηριστικά αυτά καθιστούν την ψηφιακή υδατογράφηση ιδιαίτερα πολύτιμη για την εξασφάλιση της εγκυρότητας στη διακίνηση ψηφιακών δεδομένων πολυμεσικού τύπου μέσω του Παγκόσμιου Ιστού.

Ένα από τα δυσκολότερα προβλήματα που είχε να αντιμετωπίσει η υδατογραφία στα πρώτα της βήματα, ήταν να αποδείξει ότι μπορεί πράγματι να θεωρηθεί διακριτός επιστημονικός τομέας. Ο βαθμός συσχέτισης της

υδατογραφίας με την στεγανογραφία είναι τόσο μεγάλος που πολλοί θεωρούσαν και ακόμα θεωρούν, πως δεν πρόκειται για ξεχωριστή επιστημονική περιοχή αλλά για ένα υποσύνολο του ευρύτερου επιστημονικού πεδίου της στεγανογραφίας. Άλλωστε αντικειμενικός στόχος και των δύο είναι να κρύψουν πληροφορία μέσα σε άλλη πληροφορία. Είναι σημαντικό λοιπόν να αναδειχθούν τα στοιχεία που διαφοροποιούν την υδατογραφία από την στεγανογραφία. Το παράδειγμα του Ηρόδοτου που ξύρισε το κεφάλι του δούλου του Ιστιαίου, είναι ιδανικό.

Στην περίπτωση που το μήνυμα στο κεφάλι του σκλάβου έγραφε "Αυτός ο σκλάβος ανήκει στον Ιστιαίο", τότε το μήνυμα θα αφορούσε το περιεχόμενο που το έφερε (τον σκλάβο), ικανοποιώντας έτσι ένα από τα βασικά κριτήρια της υδατογραφίας. Σε περίπτωση που κάποιος συλλάμβανε τον σκλάβο και ισχυριζόταν ότι του ανήκει, ένα ξύρισμα του κεφαλιού του θα ήταν αρκετό για να αποκαλύψει την αλήθεια. Σε αυτό το παράδειγμα ο σκλάβος είναι σημαντικός για τον αφέντη του Ιστιαίο και το μήνυμα περιέχει χρήσιμη πληροφορία σχετικά με το αντικείμενο που το φέρει.

Τα συστήματα που χρησιμοποιούνται για την εισαγωγή μηνυμάτων σε διάφορα αντικείμενα μπορούν να διαχωριστούν σε συστήματα υδατογράφησης, όπου το μήνυμα σχετίζεται με το αντικείμενο που έχει κρυφτεί και σε συστήματα που το μήνυμα δεν σχετίζεται με το αντικείμενο που το φέρει και δεν μπορούν να θεωρηθούν συστήματα υδατογράφησης. Μπορούν επίσης να διαχωριστούν σε στεγανογραφικά συστήματα όπου η ύπαρξη του μηνύματος είναι κρυφή και σε μη-στεγανογραφικά συστήματα στα οποία δεν είναι απαραίτητη η απόκρυψη της ύπαρξης του μηνύματος.



Εικόνα 2: Διαδικασία Ψηφιακής Υδατογράφησης Δεδομένων

3.2.2.1 Κατηγορίες Ψηφιακής Υδατογράφησης

Υπάρχουν τέσσερις βασικοί τύποι υδατογραφημάτων, οι οποίοι καθορίζουν κάποιες από τις χρήσεις τους:

1. Ορατό υδατογράφημα: Η βασική χρήση των ορατών υδατογραφημάτων είναι για να δηλώσουν ρητά και φανερά ότι η εμπορική χρήση του αντικειμένου είναι νομικά περιορισμένη και προστατεύεται από κανόνες πνευματικής ιδιοκτησίας. Με τον τρόπο αυτό επιτυγχάνεται η αποτροπή της παράνομης αντιγραφής από χρήστες, οι οποίοι δεν έχουν συνείδηση της πράξης τους όταν δημιουργούν ένα αντίγραφο του ψηφιακού αρχείου. Επίσης, μερικές φορές,

ορατά υδατογραφήματα χρησιμοποιούνται, για παράδειγμα, σε ψηφιακές εικόνες και ύστερα από μία εμπορική συναλλαγή αυτά αφαιρούνται και οι ψηφιακές εικόνες, χωρίς το ορατό υδατογράφημα, παραδίδονται στους χρήστες που συμμετέχουν στη συναλλαγή αυτή.

Το ορατό υδατογράφημα αφορά στην ενσωμάτωση μιας ορατής εικόνας (συνήθως το λογότυπο της δικαιούχου εταιρίας), με τέτοιο τρόπο ώστε να φαίνεται ευκρινώς αλλά να μην αλλοιώνει το περιεχόμενο του προστατευόμενου αρχείου. Φυσικά, το υδατογράφημα στοχεύει εξ ορισμού στο να αποτρέψει κάθε προσπάθεια απομάκρυνσης ή αντικατάστασής του από οποιονδήποτε επιχειρήσει να οικειοποιηθεί το προστατευόμενο αρχείο, κατά συνέπεια θα πρέπει να τοποθετείται κατάλληλα, ώστε η απομάκρυνσή του να οδηγεί π.χ. στην καταστροφή του αρχείου.

Εικόνα 3: Το λογότυπο της IBM

Εικόνα 4: Η πρωτότυπη εικόνα μαζί με το λογότυπο

Το υδατογράφημα μπορεί να τοποθετηθεί με διάφορους τρόπους, επαναληπτικά σε όλη την εικόνα, δεξιά ή αριστερά, πάνω ή κάτω ή στο κέντρο της εικόνας, ανάλογα με τη θέση που ικανοποιεί τις απαιτήσεις του δικαιούχου.

2. Αόρατο υδατογράφημα: Τα αόρατα υδατογραφήματα χρησιμοποιούνται κυρίως για την ανίχνευση και τον εντοπισμό μιας παράνομης εμπορικής συναλλαγής. Επίσης χρησιμοποιούνται για την απόδειξη της πνευματικής ιδιοκτησίας ενός ατόμου ή οργανισμού πάνω σε ψηφιακές εικόνες, βίντεο και ήχο. Συνήθως για το σκοπό αυτό χρησιμοποιούνται μηχανές αναζήτησης σχεδιασμένες με βάση αυτά τα υδατογραφήματα. Τα αόρατα υδατογραφήματα έχουν σα βασική προϋπόθεση την ανθεκτικότητά τους στις επιθέσεις των ατόμων που επιθυμούν την παράνομη χρήση του ψηφιακού περιεχομένου. Το αόρατο υδατογράφημα αποτελεί δυαδική πληροφορία που ενσωματώνεται στην αρχική,

αλλά παραμένει αόρατη και δεν την αλλοιώνει εμφανώς. Ο εντοπισμός της εφαρμογής αόρατου υδατογραφήματος σε ένα αρχείο γίνεται αλγοριθμικά, μέσω ειδικού συστήματος ανίχνευσης υδατογραφημάτων.

Εικόνα 5: Εικόνα με αόρατο υδατογράφημα πάνω αριστερά

Εικόνα 6: Το υδατογράφημα που προκύπτει με την χρήση συστήματος στην προηγούμενη εικόνα

Ανάλογα με την εφαρμογή στην οποία χρησιμοποιείται το αόρατο υδατογράφημα, υπάρχουν και οι αντίστοιχες υποπεριπτώσεις:

3. Ανθεκτικό υδατογράφημα: Τα υδατογραφήματα αυτά, συνήθως αόρατα, χρησιμοποιούνται για τον εντοπισμό μιας παράνομης εμπορικής εκμετάλλευσης ενός αντικειμένου (ψηφιακή εικόνα, ψηφιακό βίντεο και ήχος) που προστατεύεται από το νόμο της πνευματικής ιδιοκτησίας. Στόχος της ανθεκτικότητας είναι ο σωστός εντοπισμός του υδατογραφήματος ανεξαρτήτως

της επεξεργασίας που έχει υποστεί η ψηφιακή εικόνα, π.χ. η συμπίεση, η χρήση κατωπερατού φίλτρου, οι γεωμετρικές μετατροπές της εικόνας και άλλες μέθοδοι. Σε περίπτωση μη εντοπισμού του υδατογραφήματος, δηλαδή αν έχει επέλθει η αφαίρεση ή η διαστρέβλωσή του, τότε η ψηφιακή εικόνα θα πρέπει να έχει αλλοιωθεί σε τέτοιο βαθμό που η ποιότητά του να είναι πολύ χαμηλή. Συνεπώς υπάρχει trade-off μεταξύ της ανθεκτικότητας και της ποιότητας της φωτογραφίας. Επίσης υπάρχει trade-off μεταξύ της ανεπαισθητότητας και της ανθεκτικότητας.

4. Μη ανθεκτικό υδατογράφημα: Η χρήση μη ανθεκτικών υδατογραφημάτων είναι καθαρά αποδεικτική της προσπάθειας αλλοίωσης ψηφιακών εικόνων, βίντεο και ήχου. Δηλαδή σε μία ψηφιακή εικόνα για παράδειγμα ενσωματώνεται ένα υδατογράφημα, αόρατο και μη ανθεκτικό. Σε περίπτωση που κάποιος αλλοιώσει το περιεχόμενο της ψηφιακής εικόνας, ταυτόχρονα αλλοιώνει και το αόρατο υδατογράφημα, το οποίο πλέον αποδεικνύει ότι η ψηφιακή εικόνα δεν είναι η πρωτότυπη αλλά ένα παράγωγό της. Η μέθοδος αυτή έχει χρησιμοποιηθεί και σε δικαστήρια για νομικές υποθέσεις.

3.2.2.2 Υδατογράφηση – Εφαρμογές

Η τεχνική της υδατογράφησης ψηφιακών αντικειμένων μπορεί να χρησιμοποιηθεί σε μία μεγάλη ποικιλία εφαρμογών. Σε γενικές γραμμές, όταν παρουσιάζεται η ανάγκη συσχέτισης του ψηφιακού αντικειμένου με κάποια συνοδευτική πληροφορία, η επιλογή των μεθόδων υδατογράφησης για την τοποθέτηση των μεταδεδομένων μέσα στο ψηφιακό αντικείμενο είναι η ιδανικότερη λύση. Υπάρχουν βέβαια και άλλοι τρόποι για τη συσχέτιση πληροφορίας με ένα ψηφιακό αντικείμενο όπως, η τοποθέτηση της πληροφορίας στην κεφαλίδα ενός ψηφιακού αρχείου, η κωδικοποίηση της σε μία ορατή μπάρα στο κάτω μέρος μιας ψηφιακής εικόνας, η ακόμα και η εισαγωγή ενός ηχητικού

μηνύματος σαν επισυναπτόμενο μουσικό αρχείο. Το ερώτημα που τίθεται είναι πότε η υδατογράφηση αποτελεί την κατάλληλη επιλογή. Τι είναι αυτό που προσφέρει η υδατογράφηση και δεν μπορούν να το προσφέρουν οι άλλες τεχνικές.

Η υδατογραφία διαφοροποιείται από τις άλλες τεχνικές σε τρία σημαντικά σημεία. Αρχικά, τα υδατογραφήματα (αόρατα υδατογραφήματα) χαρακτηρίζονται από την επιπλέον ιδιότητα να μην γίνονται αντιληπτά από το ανθρώπινο σύστημα των αισθήσεων. Σε αντίθεση με τους κώδικες μπάρας δεν επηρεάζουν την αισθητική του ψηφιακού αντικειμένου. Επιπλέον, τα υδατογραφήματα είναι αδιαχώριστα από τα αντικείμενα στα οποία ενσωματώνονται. Σε αντίθεση με την πληροφορία που τοποθετείται στις κεφαλίδες των αρχείων, δεν απομακρύνονται με την εφαρμογή απλών μορφών επεξεργασίας, όπως είναι η αλλαγή του τύπου δεδομένων του αρχείου. Τέλος τα υδατογραφήματα υφίστανται την ίδια ακριβώς επεξεργασία που εφαρμόζεται και στο ψηφιακό αντικείμενο. Η τελευταία ιδιότητα επιτρέπει μερικές φορές την διαπίστωση των μετατροπών που έχει υποστεί το ψηφιακό αντικείμενο, από την παρακολούθηση των αλλαγών που έχει υποστεί το υδατογράφημα. Οι τρεις παραπάνω ιδιότητες είναι που καθιστούν την τεχνική της υδατογράφησης κατάλληλη για εφαρμογές συγκεκριμένου τύπου.

Στη συνέχεια ακολουθεί η περιγραφή μερικών εφαρμογών που μπορούν να υλοποιηθούν με τη χρήση υδατογραφικών μεθόδων. Σκοπός της αναφοράς είναι να αναδειχθούν τα ιδιαίτερα χαρακτηριστικά της υδατογραφίας που την καθιστούν κατάλληλη λύση σε κάθε περίπτωση. Σημαντικός είναι ο ρόλος των απαιτήσεων και των προδιαγραφών που παρουσιάζει η εκάστοτε εφαρμογή και των περιορισμών που επιβάλλονται από τη χρήση άλλων τεχνολογιών.

3.2.2.2.1 Έλεγχος Εκπομπής – Broadcast Monitoring

Ο όρος εκπομπή αναφέρεται στα ραδιοκύματα που μεταδίδονται από τους τηλεοπτικούς και ραδιοφωνικούς σταθμούς. Το 1997, ξέσπασε ένα σκάνδαλο στην Ιαπωνία στο χώρο της τηλεοπτικής διαφήμισης. Δύο τουλάχιστον τηλεοπτικοί σταθμοί πραγματοποιούσαν συστηματική κατάχρηση τηλεοπτικού χρόνου. Τα επιτελεία των τηλεοπτικών σταθμών λάμβαναν σημαντικές αποζημιώσεις για διαφημίσεις που δεν μεταδίδονταν ποτέ. Η τακτική υιοθετήθηκε από πολλούς διαφορετικούς τηλεοπτικούς σταθμούς και παρέμεινε απαρατήρητη και αναπόδεικτη για περισσότερο από 20 χρόνια, καθώς δεν υπήρχαν συστήματα ικανά να παρακολουθήσουν τον πραγματικό μέρισμα του τηλεοπτικού χρόνου που αποδιδόταν σε διαφημίσεις.

Η πιο απλή προσέγγιση για την επίτευξη του ελέγχου εκπομπής είναι η τοποθέτηση ανθρώπων για την παρατήρηση και την καταγραφή του μεταδιδόμενου προγράμματος καθ' όλη τη διάρκεια της ημέρας. Ωστόσο, η συγκεκριμένη μέθοδος εμφανίζεται ανακριβής και πολυέξοδη λόγο της ανάμειξης του ανθρώπινου παράγοντα. Η αντικατάσταση του ανθρώπινου δυναμικού με ένα αυτοματοποιημένο σύστημα παρακολούθησης και καταγραφής είναι μια λύση που περιορίζει το κόστος και μειώνει σημαντικά την πιθανότητα λάθους. Οι τεχνικές για την υλοποίηση ενός τέτοιου συστήματος μπορούν να διαχωριστούν σε δύο κατηγορίες. α) Στα συστήματα παθητικής παρακολούθησης, που προσπαθούν να εξομοιώσουν τους ανθρώπινους παρατηρητές και έχουν ως στόχο την άμεση παρακολούθηση της τηλεοπτικής μετάδοσης. β) Στα συστήματα ενεργητικής παρακολούθησης που βασίζονται σε κάποια συνοδευτική πληροφορία που μεταδίδεται παράλληλα με το περιεχόμενο.

Ένα παθητικό σύστημα αποτελείται από έναν υπολογιστή ο οποίος παρακολουθεί τα μεταδιδόμενα τηλεοπτικά σήματα και τα συγκρίνει με ένα σύνολο από προεπιλεγμένα σήματα που αντιστοιχούν στο περιεχόμενο που θέλει

να ελέγξει. Η αναμετάδοση πιστοποιείται όταν η σύγκριση που πραγματοποιείται από τον υπολογιστή αποβεί θετική. Πρόκειται για την πιο άμεση και λιγότερο παρεμβατική αυτοματοποιημένη μέθοδο παρακολούθησης εκπομπής. Δεν προϋποθέτει καμία μορφή συνοδευτικής πληροφορίας κατά τη μετάδοση και επομένως δεν απαιτεί κάποια αλλαγή στα μεταδιδόμενα σήματα των διαφημιστών και των τηλεοπτικών σταθμών.

Ωστόσο, προκύπτει ένας αριθμός από σημαντικά προβλήματα κατά την υλοποίηση και τη λειτουργία των παθητικών συστημάτων ελέγχου εκπομπής. Η σύγκριση ανάμεσα στα μεταδιδόμενα τηλεοπτικά σήματα και τα σήματα που μας ενδιαφέρουν είναι μια χρονοβόρα και απαιτητική διαδικασία, ακόμα και για τους σύγχρονους υπολογιστές με την αυξημένη υπολογιστική ισχύ. Οι εικόνες, το βίντεο και ο ήχος αποτελούνται από αρχεία σημαντικού μεγέθους, με αποτέλεσμα να είναι ακατάλληλα για λειτουργίες σύγκρισης και αναγνώρισης. Είναι απαραίτητη λοιπόν η κωδικοποίηση τους με μονοσήμαντο τρόπο σε μικρότερου μεγέθους αρχεία κατάλληλα για αυτοματοποιημένη σύγκριση. Δυστυχώς όμως, η διαδικασία της κωδικοποίησης εισάγει καινούργια προβλήματα που σχετίζονται κυρίως με την ποιότητα της μετάδοσης των σημάτων. Το μεγάλο μέγεθος του περιεχομένου από τη μία και η αυξημένη πολυπλοκότητα που εισάγεται κατά την κωδικοποίηση από την άλλη, οδηγούν στο συμπέρασμα πως ο σχεδιασμός και η υλοποίηση ενός 100% έμπιστου παθητικού συστήματος παρακολούθησης είναι εξαιρετικά δύσκολη.

Η ακρίβεια που απαιτείται για υπηρεσίες επιβεβαίωσης μπορεί να εξασφαλιστεί μόνο από ένα ενεργητικό σύστημα παρακολούθησης, όπου επιπρόσθετη αναγνωριστική πληροφορία, κατάλληλη για επεξεργασία από υπολογιστή, μεταδίδεται παράλληλα με το περιεχόμενο. Οι τεχνολογικές απαιτήσεις της ενεργητικής παρακολούθησης είναι σαφώς μειωμένες, καθώς η συνοδευτική πληροφορία είναι εύκολα και αξιόπιστα αποκωδικοποιήσιμη χωρίς να χρησιμοποιείται βάση δεδομένων.

Υπάρχουν πάρα πολλοί τρόποι για τη μετάδοση της συνοδευτικής πληροφορίας κατά τη μετάδοση του περιεχομένου. Ο πιο τετριμμένος από όλους είναι να χρησιμοποιηθεί η θεωρία σημάτων και να γίνει εκμετάλλευση εκείνων των περιοχών φάσματος που δεν επηρεάζουν τη μετάδοση του κυρίως περιεχομένου. Ωστόσο, η χρησιμοποίηση του ελεύθερου χώρου στο φάσμα των συχνοτήτων των σημάτων είναι πάντα μια επικίνδυνη επιλογή. Τέλος, εξαιρετικά αμφίβολη κρίνεται και η ανθεκτικότητα της συνοδευτικής πληροφορίας στις κοινές μετατροπές του μεταδιδόμενου σήματος, όπως είναι αυτή από αναλογικό σε ψηφιακό και αντίστροφα. Αντίστοιχες αδυναμίες παρουσιάζουν και άλλες παρόμοιες τεχνικές που κωδικοποιούν την συμπληρωματική πληροφορία στις κεφαλίδες των ψηφιακών αρχείων περιεχομένου. Χαρακτηριστικό είναι το παράδειγμα των ψηφιακών αρχείων φωτογραφίας, που μπορούν να φιλοξενήσουν μεγάλη ποσότητα πληροφορίας στην κεφαλίδα τους (header file) χωρίς να επηρεάζουν καθόλου την ίδια την εικόνα. Οποιαδήποτε μετατροπή ωστόσο του τύπου του αρχείου της φωτογραφίας καταστρέφει ολοκληρωτικά τη συνοδευτική πληροφορία.

Οι παραπάνω αδυναμίες είναι αυτές που καθιστούν την υδατογραφία ως ενδεδειγμένη λύση για την ανάπτυξη ενός ενεργητικού συστήματος παρακολούθησης. Το βασικό πλεονέκτημα έγκειται στο γεγονός ότι η πληροφορία αναγνώρισης ενσωματώνεται μέσα στο ίδιο το περιεχόμενο και δεν τοποθετείται σε κάποιες ειδικές περιοχές του φάσματος συχνότητας, εξασφαλίζοντας παράλληλα άριστη συμβατότητα με την ήδη υπάρχουσα υποδομή σε εξοπλισμό εκπομπής τόσο για ψηφιακή όσο και για αναλογική μετάδοση. Η διαδικασία ενσωμάτωσης της πληροφορίας (embedding process) μέσα στο περιεχόμενο, είναι σαφώς πιο πολύπλοκη από την απλή τοποθέτησή της στην κεφαλίδα ενός ψηφιακού αρχείου και αυτή η πολυπλοκότητα είναι το βασικότερο από τα μειονεκτήματα της υδατογραφίας έναντι των άλλων λύσεων. Ανησυχία υπάρχει επίσης, από την πλευρά των δημιουργών του περιεχομένου και

για την ποιότητα του μεταδιδόμενου σήματος. Πιστεύουν πως η εισαγωγή του υδατογραφήματος στο περιεχόμενο θα υποβαθμίσει την ποιότητα της εικόνας και του ήχου του μεταδιδόμενου σήματος. Ωστόσο, υπάρχει ένας αριθμός από εταιρείες που παρέχουν υπηρεσίες ελέγχου εκπομπής βασιζόμενες στην υδατογραφία καθώς αποτελεί την πιο ενδεδειγμένη λύση για τη συγκεκριμένη εφαρμογή.

3.2.2.2.2 Αναγνώριση Ιδιοκτήτη – Owner Identification

Σύμφωνα με τη νομοθεσία που ισχύει στις Ηνωμένες Πολιτείες της Αμερικής ο δημιουργός μιας καλλιτεχνικής έκφρασης (Μυθιστόρημα, Ζωγραφιά, Τραγούδι κ.α), δεσμεύει αυτόματα το δικαίωμα αναπαραγωγής της, τη στιγμή που η δημιουργία αποτυπώνεται σε κάποιο φυσικό μέσο. Από το 1988, αν ο κάτοχος τους δικαιώματος αναπαραγωγής επιθυμούσε τη διανομή της καλλιτεχνικής του δημιουργίας χωρίς να απολέσει τα πνευματικά του δικαιώματα, θα έπρεπε να συμπεριλάβει μία σημείωση περί των πνευματικών δικαιωμάτων του έργου σε κάθε αντίγραφο. Μετά το 1988, η κατάσταση διαφοροποιήθηκε και η σχετική ειδοποίηση δεν ήταν πια υποχρεωτική. Ωστόσο, αν η παράνομη εκμετάλλευση ενός έργου που βρισκόταν υπό την προστασία του νόμου περί πνευματικών δικαιωμάτων είχε ως αποτέλεσμα μια δικαστική απόφαση αποζημίωσης του κάτοχου των πνευματικών δικαιωμάτων από τον παραβάτη, το μέγεθος της αποζημίωσης θα ήταν αισθητά μειωμένο αν η σχετική ειδοποίηση απουσίαζε.

Σημαντικό ρόλο κατέχει και η ακριβής μορφοποίηση της σημείωσης που θα πρέπει να είναι συμβατή με ένα συγκεκριμένο πρότυπο. Συγκεκριμένα για οπτικά έργα θα πρέπει να έχει την μορφή "Copyright ημερομηνία ιδιοκτήτης", "© ημερομηνία ιδιοκτήτης" ή "Corp. ημερομηνία ιδιοκτήτης". Για ηχητικά έργα η σημείωση περί των πνευματικών δικαιωμάτων παίρνει αντίστοιχη μορφή και θα πρέπει να τοποθετηθεί στην επιφάνεια του φυσικού μέσου, στην ετικέτα, ή στο

πακέτο συσκευασίας, ώστε να παρέχει μία σαφή ειδοποίηση περί του δικαιώματος αναπαραγωγής & της πνευματικής ιδιοκτησίας του έργου.

Οι ειδοποιήσεις περί πνευματικής ιδιοκτησίας που βασίζονται σε γραφήματα, παρουσιάζουν συγκεκριμένες αδυναμίες ως προς την αναγνώριση του ιδιοκτήτη της καλλιτεχνικής δημιουργίας. Η απομάκρυνση τους από το έργο είναι πολύ εύκολη ακόμα και χωρίς κακή πρόθεση. Για παράδειγμα, ένας καθηγητής που φωτοτυπεί κάποιες σημειώσεις στα νόμιμα πλαίσια του εκπαιδευτικού του έργου, μπορεί να παραμελήσει την πρώτη σελίδα που δηλώνει τον κάτοχο των πνευματικών δικαιωμάτων. Ένας καλλιτέχνης που νόμιμα χρησιμοποιεί τη φωτογραφία ενός περιοδικού, μπορεί να αποκόψει το κομμάτι της εικόνας που φέρει το διακριτικό γράφημα χωρίς κάποια σκοπιμότητα. Επομένως, ακόμα και ένας νομοταγής πολίτης που επιθυμεί να χρησιμοποιήσει τη φωτογραφία δεν θα είναι σε θέση να διαπιστώσει αν προστατεύεται από κάποια δέσμευση του δικαιώματος αναπαραγωγής. Ακόμα και στη περίπτωση που θεωρηθεί δεδομένη η προστασία της εικόνας, η εύρεση του δημιουργού ή του κάτοχου των πνευματικών δικαιωμάτων είναι δύσκολη με δεδομένη την απουσία του γραφήματος.

Ένα ακόμα σημαντικό πρόβλημα που προκύπτει από τη χρήση γραφημάτων ως πειστήρια περί της πνευματικής ιδιοκτησίας είναι η άσχημη αίσθηση που δημιουργούν στο σύνολο του έργου. Η τοποθέτηση τους σε κάποια ασήμαντη περιοχή του έργου μπορεί να κάνει το γράφημα λιγότερο αντιαισθητικό, παράλληλα όμως το κάνει περισσότερο ευάλωτο σε ενέργειες απομάκρυνσης του, όπως είναι η αποκοπή του. Η κατάσταση επιδεινώνεται στην περίπτωση όπου το γράφημα βρίσκεται στο φυσικό μέσο (δίσκος, κασέτα, CD κ.α) ή στο πακέτο συσκευασίας. Είναι σχεδόν απίθανο για αυτά τα γραφήματα να ακολουθήσουν το έργο κατά την αντιγραφή του. Σε πολλές περιπτώσεις μάλιστα, το ίδιο το μουσικό ή οπτικό έργο διατίθεται μόνο σε ηλεκτρονική μορφή με

αποτέλεσμα η έννοια του φυσικού μέσου και του πακέτου συσκευασίας να μην έχουν υπόσταση.

Η ιδιότητα που φέρουν τα υδατογραφήματα να είναι ανεπαίσθητα και αδιαχώριστα από το περιεχόμενο, τα καθιστά σαφώς καταλληλότερα από τα γραφήματα για την ενσωμάτωση της ένδειξης περί πνευματική ιδιοκτησίας. Ακόμα και στην περίπτωση που το έργο έχει υποστεί τροποποιήσεις που θα αφαιρούσαν το γράφημα, ένας χρήστης εφοδιασμένος με τον κατάλληλο μηχανισμό ανίχνευσης υδατογραφήματος είναι σε θέση να αναγνωρίσει τον ιδιοκτήτη του έργου.

Η νομική εγκυρότητα ενός συστήματος υδατογράφησης δεν έχει ελεγχθεί ακόμα από κάποιο δικαστήριο. Με δεδομένη την κατάσταση όπου η ένδειξη περί του δικαιώματος αναπαραγωγής φέρει τόσο μεγάλη σπουδαιότητα από νομικής πλευράς, η αντικατάσταση του γραφήματος από ένα ηλεκτρονικό γράφημα σε μορφή υδατογραφήματος, ίσως να φαντάζει την παρούσα στιγμή αρκετά αισιόδοξη. Ωστόσο, η ροπή που παρουσιάζει η νομοθεσία των Ηνωμένων Πολιτειών και της Ευρωπαϊκής Ένωσης προς την αναγνώριση των τεχνολογικών μέσων στης διαδικασία της προστασίας και της διαχείρισης των πνευματικών δικαιωμάτων ψηφιακού περιεχομένου, αποτελεί αισιόδοξο μήνυμα για την οριστική αναγνώριση της υδατογραφίας ως νομικά έγκυρο δικαστικό πειστήριο.

3.2.2.2.3 Πιστοποίηση Ιδιοκτησίας - Proof of Ownership

Παρά το γεγονός πως η υδατογραφία μπορεί να αποτελεί ενδεδειγμένη λύση σε ένα ευρύ σύνολο εφαρμογών, η πιο σπουδαία και απαιτητική εφαρμογή είναι η πιστοποίηση ιδιοκτησίας. Αντικειμενικός σκοπός ανάλογων εφαρμογών είναι η ενσωμάτωση κωδικοποιημένης πληροφορίας μέσα στο περιεχόμενο του έργου, ώστε να αποτρέψει τους επίδοξους παραβάτες από τη διεκδίκηση της ιδιοκτησίας του. Η ανάμειξη στο πρόβλημα των πνευματικών δικαιωμάτων και

ενός τρίτου προσώπου που όχι μόνο χρησιμοποιεί παράνομα το έργο, αλλά διεκδικεί και την πρωτογενή του δημιουργία, περιπλέκει την κατάσταση και αυξάνει σημαντικά τις απαιτήσεις ανθεκτικότητας του υδατογραφήματος. Πέρα από τις κλασικές ακούσιες και τετριμμένες τροποποιήσεις, το υδατογράφημα θα πρέπει να παρουσιάζει ανθεκτικότητα και σε άλλης μορφής επεξεργασία στην οποία ενδέχεται να υποβάλλει το έργο ο επίδοξος παραβάτης για να το απομακρύνει. Η επεξεργασία στην οποία υποβάλλεται το υδατογραφημένο περιεχόμενο παίρνει πολλές μορφές και περιγράφεται συνοπτικά με τον χαρακτηρισμό "επιθέσεις κατά του υδατογραφήματος".

Η πιστοποίηση του πραγματικού ιδιοκτήτη επιτυγχάνεται με τη χρήση ενός μυστικού κλειδιού κατά τη διαδικασία ενσωμάτωσης της κωδικοποιημένης πληροφορίας στο ψηφιακό περιεχόμενο και στη συνέχεια με την επιτυχημένη ανίχνευσή της. Ο κάτοχος του δικαιώματος αναπαραγωγής ενός ψηφιακού αντικειμένου εξασφαλίζει έναν μοναδικό αριθμό, που συνήθως φέρεται με το όνομα μυστικό κλειδί, από μια κεντρική επιτροπή. Ο αριθμός είναι αυστηρά προσωπικός και δεν επιτρέπεται η εκ νέου ανάθεση του ίδιου αριθμού σε άλλο χρήστη. Με τη χρήση του μοναδικού κλειδιού πραγματοποιείται η ενσωμάτωση της κωδικοποιημένης πληροφορίας στο ψηφιακό περιεχόμενο. Η διαμάχη μεταξύ του ιδιοκτήτη και του επίδοξου παραβάτη θα τερματίσει, όταν ο κάτοχος του μυστικού κλειδιού εφαρμόσει, χρησιμοποιώντας το μυστικό του κλειδί, το μηχανισμό ανίχνευσης του υδατογραφήματος και διαπιστώσει την ύπαρξη της κωδικοποιημένης πληροφορίας που είχε τοποθετήσει. Αντίθετα ο έτερος διεκδικητής της κυριότητας του ψηφιακού περιεχομένου δεν είναι σε θέση να επιμείνει στην διεκδίκηση του χωρίς να έχει στην κατοχή του το μυστικό κλειδί που θα του επιτρέψει να ανιχνεύσει το υδατογράφημα.

Η κινητήρια δύναμη για την ανάπτυξη εφαρμογών πιστοποίησης ιδιοκτησίας ήταν αναμφίβολα ο παγκόσμιος ιστός και το Διαδίκτυο. Μεγάλη ποσότητα ψηφιακού υλικού φιλοξενείται σε αναρίθμητους διαδικτυακούς τόπους,

χωρίς να υπάρχει πρόβλεψη για την προστασία του και επομένως χωρίς καμία εγγύηση για την ορθή του χρήση. Το δυσάρεστο αποτέλεσμα είναι, οι κάτοχοι του ψηφιακού περιεχομένου να καταλαμβάνονται από ένα έντονο αίσθημα ανασφάλειας και να αποσύρουν το πλούσιο σε αισθητική και εκπαιδευτική αξία περιεχόμενό τους. Η αυξημένη πολυπλοκότητα που παρουσιάζει η περίπτωση της πιστοποίησης ιδιοκτησίας δεν οφείλεται μόνο στις αυξημένες απαιτήσεις για ανθεκτικότητα έναντι των επιθέσεων, αλλά και σε επιμέρους σχεδιαστικά προβλήματα που θα πρέπει να ληφθούν υπόψη. Για παράδειγμα, θα πρέπει η εφαρμογή να προβλέπει μία απερίφραστη διαδικασία ενσωμάτωσης του υδατογραφήματος ώστε να είναι σε θέση να αποφανθεί για την ιδιοκτησία του ψηφιακού περιεχομένου ακόμα και στην περίπτωση όπου ο επίδοξος διεκδικητής έχει καταφέρει να ενσωματώσει ένα δεύτερο δικό του υδατογράφημα.

3.2.2.2.4 Έλεγχος Αντιγραφής – Copy Control

Μία από τις πιο επιθετικές τακτικές για την προστασία των πνευματικών δικαιωμάτων είναι η πρόληψη και η έγκαιρη απαγόρευση της παραβίασης του δικαιώματος αναπαραγωγής. Ο ουσιαστικός σκοπός μιας εφαρμογής ελέγχου αντιγραφής είναι η παρεμπόδιση της δημιουργίας παράνομων αντιγράφων περιεχομένου με δεσμευμένο το δικαίωμα αναπαραγωγής. Η πρώτη και πιο διαδεδομένη επιλογή κατά της παράνομης αντιγραφής είναι η κρυπτογράφηση. Ένα ψηφιακό αντικείμενο που έχει κρυπτογραφηθεί με τη χρήση ενός μυστικού κλειδιού, καθίσταται αυτόματα άχρηστο για οποιονδήποτε δεν είναι εφοδιασμένος με το συγκεκριμένο κλειδί. Στη συνέχεια το μυστικό κλειδί παραδίδεται στους εξουσιοδοτημένους χρήστες με τρόπο που να κάνει την υποκλοπή του εξαιρετικά δύσκολη. Ένας επίδοξος παραβάτης έχει τρεις τρόπους για να διαβάλει το παραπάνω κρυπτογραφικό σύστημα. Ο πρώτος είναι να αποκρυπτογραφήσει το ψηφιακό περιεχόμενο χωρίς της βοήθεια του μυστικού κλειδιού. Πρόκειται βέβαια για μια επίπονη και χρονοβόρο διαδικασία που εξαρτάται άμεσα από την αποδοτικότητα της μεθόδου κρυπτογράφησης. Μία

λιγότερο επίπονη προσέγγιση είναι να προσπαθήσει με θεμιτούς ή αθέμιτους τρόπους να αποκτήσει το μυστικό κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση του περιεχομένου. Ανάμεσα στους θεμιτούς τρόπους συγκαταλέγεται η εμπειρική μέθοδος των διαδοχικών δοκιμών, όπου με άπληστο τρόπο δοκιμάζονται μια σειρά από κλειδιά μέχρι να εντοπιστεί το σωστό. Υπάρχουν βέβαια και πιο αποδοτικές λύσεις όπου η ακολουθία των δοκιμών διαμορφώνεται χρησιμοποιώντας μεθόδους εύρεσης. Η πιο απλή όμως μέθοδος για την παράκαμψη του κρυπτογραφικού συστήματος, που αποκαλύπτει και την αδυναμία της συγκεκριμένης τεχνολογικής κατεύθυνσης ως λύση στο πρόβλημα του ελέγχου αντιγραφής, είναι η μεταποίηση του ψηφιακού περιεχομένου μετά την νόμιμη απόκτηση του μυστικού κλειδιού και την αποκρυπτογράφηση του. Ο επίδοξος παραβάτης τηρώντας όλες τις προϋποθέσεις και πληρώνοντας το αντίστοιχο αντίτιμο αποκτά το μυστικό κλειδί της κωδικοποίησης και αποκρυπτογραφεί το περιεχόμενο. Στη συνέχεια χρησιμοποιώντας τον κατάλληλο εξοπλισμό πραγματοποιεί την αντιγραφή του αποκωδικοποιημένου αρχείου εικόνας, βίντεο ή ήχου σε ένα καινούργιο αντίγραφο απαλλαγμένο από το κρυπτογραφικό σύστημα. Το νέο αντίγραφο που θα προκύψει στερείται κάθε ασφάλειας και δεν παρέχει πια κανένα έλεγχο αντιγραφής.

Σε αντίθεση με το κρυπτογραφικό σύστημα, τα υδατογραφήματα τοποθετούνται στο ίδιο το ψηφιακό περιεχόμενο και παρευρίσκονται σε κάθε αναπαράσταση του ψηφιακού περιεχομένου με όποιο τρόπο και αν έχει προκύψει. Επομένως, η τεχνολογική επιλογή της υδατογράφησης μπορεί να αποτελέσει την καταλληλότερη επιλογή για την υλοποίηση εφαρμογών ελέγχου αντιγραφής. Ο έλεγχος αντιγραφής είναι πολύ δύσκολο να επιτευχθεί σε ανοικτά συστήματα, σε κλειστά ή ιδιωτικά συστήματα ωστόσο μπορεί να αποτελέσει μια ρεαλιστική επιλογή. Στα κλειστά συστήματα είναι δυνατή η χρήση υδατογραφημάτων για την καταγραφή των περιορισμών του ψηφιακού περιεχομένου σε σχέση με τα δικαιώματα αντιγραφής. Αν κάθε συσκευή, ικανή για την αναπαραγωγή ψηφιακού περιεχομένου, ήταν εξοπλισμένη με έναν

κατάλληλα διαμορφωμένο ανιχνευτή υδατογραφημάτων, θα ήταν δυνατός ο περιορισμός των ενεργειών που θα μπορούσε να πραγματοποιήσει η συσκευή σε συγκεκριμένο ψηφιακό περιεχόμενο ανάλογα με την πληροφορία του υδατογραφήματος. Για παράδειγμα, μία συσκευή αναπαραγωγής αρχείων βίντεο δεν θα επέτρεπε την αναπαραγωγή του αρχείου, αν ανιχνευόταν ένα υδατογράφημα της μορφής "απαγόρευση αντιγραφής". Το πραγματικό, μη τεχνολογικό, πρόβλημα που παρουσιάζεται σε ένα σύστημα ελέγχου αντιγραφής βασισμένο σε τεχνολογίες υδατογράφησης είναι η διασφάλιση της ενσωμάτωσης μηχανισμών ανίχνευσης υδατογραφημάτων στο σύνολο των συσκευών αναπαραγωγής ψηφιακού περιεχομένου. Παρά το γεγονός ότι μια κατασκευαστική εταιρεία που ενσωματώνει στις συσκευές που παράγει ένα τέτοιο μηχανισμό, συμμορφώνεται πλήρως με τις οδηγίες περί προστασίας των πνευματικών δικαιωμάτων, η λειτουργική αξία του προϊόντος μειώνεται δραματικά, ιδιαίτερα στην περίπτωση που στην ευρύτερη αγορά υπάρχουν προϊόντα που στερούνται των ανωτέρω περιορισμών. Όλες οι προσδοκίες προσβλέπουν σε ένα νομικό μοντέλο που θα επιβάλλει τους ανιχνευτές υδατογράφησης σε κάθε νόμιμη συσκευή αναπαραγωγής ψηφιακού περιεχομένου.

3.2.2.2.5 Καταγραφή Δοσοληψιών – Transaction Tracking

Στη συγκεκριμένη εφαρμογή, το υδατογράφημα καταγράφει μία ή περισσότερες δοσοληψίες που πραγματοποιήθηκαν σε κάθε ψηφιακό αντίγραφο του αρχικού έργου, μέσα στο ίδιο το περιεχόμενο του ψηφιακού αντιγράφου. Για παράδειγμα, το υδατογράφημα μπορεί να καταγράψει τον αποδέκτη κάθε νόμιμης πώλησης ή διανομής του έργου. Ο ιδιοκτήτης του έργου χρησιμοποιεί διαφορετικό υδατογράφημα για κάθε αντίγραφο. Σε περίπτωση εσφαλμένης χρήσης του ψηφιακού αντίγραφου (διαρροή στον τύπο ή παράνομη διανομή), ο ιδιοκτήτης είναι σε θέση να εντοπίσει τη πηγή της διαρροής χρησιμοποιώντας τα υδατογραφήματα που έχει τοποθετήσει.

Στη βιβλιογραφία, ο υπεύθυνος για την εσφαλμένη χρήση του έργου αναφέρεται με το όνομα προδότης (traitor), ενώ ο αποδέκτης του έργου αναφέρεται με το όνομα πειρατής (pirate). Καθώς ο συγκεκριμένος διαχωρισμός δεν έχει νόημα σε εφαρμογές όπου δεν υφίσταται το θέμα της πειρατείας, δεν χρησιμοποιείται η παραπάνω ορολογία. Αντιθέτως χρησιμοποιείται ο όρος εχθρός (adversary) για να περιγράψει οποιονδήποτε προσπαθήσει να απομακρύνει, να εξουδετερώσει ή να πλαστογραφήσει ένα υδατογράφημα με σκοπό να παρακάμψει την προβλεπόμενη λειτουργία του.

Ένα παράδειγμα πραγματικής εφαρμογής για την παρακολούθηση των δοσοληψιών, υλοποιήθηκε από την DIVX Corporation. Η DIVX προώθησε στην αγορά μία ειδική συσκευή αναπαραγωγής DVD που ενσωμάτωνε μία τακτική παρακολούθησης επί πληρωμής. Μία μεγάλη ποικιλία από τεχνολογίες ασφάλειας υιοθετήθηκαν με σκοπό να αποτρέψουν την πειρατική χρήση των δίσκων αναπαραγωγής (DVDs), μία από τις οποίες ήταν και ένα υδατογράφημα που σχεδιάστηκε για την καταγραφή των δοσοληψιών. Κάθε συσκευή αναπαραγωγής DIVX τοποθετούσε ένα μοναδικό υδατογράφημα σε κάθε ταινία που έπαιζε. Στην περίπτωση που κάποιος αποφάσιζε να δημιουργήσει ένα αντίγραφο της ταινίας και να το διανέμει στην αγορά, η DIVX corporation μπορούσε να εξετάσει ένα από τα παράνομα αντίγραφα και χρησιμοποιώντας τις τεχνικές της υδατογραφίας, να εντοπίσει τη συγκεκριμένη συσκευή αναπαραγωγής που ήταν υπεύθυνη για την δημιουργία των αντιγράφων. Ωστόσο, τα υδατογραφήματα της DIVX δεν χρησιμοποιήθηκαν ποτέ για τον εντοπισμό παραβιάσεων του δικαιώματος αναπαραγωγής τουλάχιστον πριν το κλείσιμο της εταιρείας.

Η δημιουργία και χρήση ενός μοναδικού ηλεκτρονικού αποτυπώματος είναι εξαιρετικά σημαντική σε διαδικασίες αναγνώρισης και κατηγοριοποίησης. Το γεγονός ότι κάθε ταυτότητα φέρει το δακτυλικό αποτύπωμα του κατόχου της, είναι απόδειξη της σημασίας και της χρησιμότητάς τους. Αντίστοιχες ανάγκες

παρουσιάζονται και στο ψηφιακό κόσμο, όπου κάθε ψηφιακό δημιούργημα έχει την ανάγκη να είναι εξοπλισμένο με ένα αναγνωριστικό που να το χαρακτηρίζει μονοσήμαντα και να το διαφοροποιεί. Το ψηφιακό υδατογράφημα ανταποκρίνεται πλήρως στις παραπάνω απαιτήσεις κυρίως λόγω των ακόλουθων ιδιοτήτων:

i. Δεν γίνεται αντιληπτό από τις ανθρώπινες αισθήσεις.

ii. Είναι ενσωματωμένο στο περιεχόμενο του ψηφιακού έργου και υφίσταται ακριβώς την ίδια επεξεργασία με αυτό.

Η τοποθέτησή του βασίζεται σε ένα μυστικό ιδιωτικό κλειδί και ικανοποιεί την απαίτηση της ύπαρξης μονοσήμαντου αναγνωριστικού για το έργο.

3.2.2.3 Υδατογράφηση – Ιδιότητες

Τα συστήματα υδατογράφησης φέρουν ένα σημαντικό αριθμό από βασικές ιδιότητες που τις περισσότερες φορές εμφανίζονται ως αντικρουόμενες τάσεις όπου ένα καλό σύστημα υδατογράφησης θα πρέπει να σταθμίσει. Η σχετική σπουδαιότητα που παρουσιάζει κάθε ιδιότητα εξαρτάται άμεσα από τις απαιτήσεις της εφαρμογής και το ρόλο που θα διαδραματίσει το υδατογράφημα μέσα σε αυτή. Αρχικά θα πραγματοποιηθεί αναφορά στις ιδιότητες που συνδέονται με την διαδικασία της ενσωμάτωσης του υδατογραφήματος και συγκεκριμένα την αποτελεσματικότητα (effectiveness), την πιστότητα (fidelity) και το φορτίο των δεδομένων (data payload). Στη συνέχεια παρατίθενται οι ιδιότητες που τυπικά συνδέονται με την διαδικασία της ανίχνευσης, τυφλή (blind) & ενημερωμένη (informed) ανίχνευση και ανθεκτικότητα (robustness). Οι επόμενες ιδιότητες, ασφάλεια και χρήση μυστικών κλειδιών αποτελούν αναπόσπαστο στοιχείο κάθε πολιτικής ασφάλειας και συνεπώς της υδατογράφησης. Την λίστα των ιδιοτήτων συμπληρώνει μια ενδεικτική ανάλυση κόστους-οφέλους που θα πρέπει πάντα να προηγείται του σχεδιασμού ενός συστήματος υδατογράφησης.

3.2.2.3.1 Αποτελεσματική Ενσωμάτωση

Ένα ψηφιακό αντικείμενο θεωρείται υδατογραφημένο όταν ο μηχανισμός ανίχνευσης αποκριθεί θετικά κατά τη διαδικασία ανίχνευσης. Σύμφωνα με τον παραπάνω ορισμό, η αποτελεσματικότητα ενός συστήματος υδατογράφησης ορίζεται ως η πιθανότητα η έξοδος του μηχανισμού ενσωμάτωσης υδατογραφημάτων, να είναι πράγματι ένα υδατογραφημένο ψηφιακό αντικείμενο. Πρόκειται ουσιαστικά για τη πιθανότητα ανίχνευσης του υδατογραφήματος αμέσως μετά την τοποθέτηση του, χωρίς να μεσολαβήσει καμία επεξεργασία του ψηφιακού αντικειμένου που θα είχε ως αποτέλεσμα την αλλοίωση του περιεχομένου του. Όπως είναι φανερό ο παραπάνω ορισμός αφήνει ανοικτό το ενδεχόμενο ενός συστήματος υδατογράφησης που θα εμφανίζει αποτελεσματικότητα μικρότερη του 100%.

Παρά το γεγονός πως μία αποτελεσματικότητα της τάξης του 100% είναι πάντα επιθυμητή, υπάρχουν περιπτώσεις που το τίμημα της απόλυτης πιθανότητας είναι αρκετά μεγάλο. Σε συνάρτηση πάντα με την εφαρμογή υδατογράφησης, είναι θεμιτή η ανοχή σε μία ελαφρώς μειωμένη αποτελεσματικότητα με αντίτιμο την αυξημένη αποδοτικότητα άλλων χαρακτηριστικών. Για παράδειγμα, μία αποθήκη φωτογραφικού υλικού χρειάζεται να ενσωματώσει ένα υδατογράφημα, για λόγους πιστοποίησης ιδιοκτησίας, σε χιλιάδες φωτογραφίες ημερησίως. Το σύστημα υδατογράφησης που θα χρησιμοποιηθεί έχει σε προτεραιότητα την προδιαγραφή για υψηλή ποιότητα των υδατογραφημένων φωτογραφιών, με αποτέλεσμα μερικές από τις φωτογραφίες να μην ανταποκρίνονται ικανοποιητικά στη διαδικασία ενσωμάτωσης. Το δίλημμα που προκύπτει για τους ιδιοκτήτες του φωτογραφικού αρχείου είναι αν θα πρέπει να ανεχτούν το γεγονός ότι κάποιες φωτογραφίες θα παραμείνουν χωρίς ουσιαστική προστασία διατηρώντας την ποιότητα τους σε υψηλά επίπεδα, ή θα

πρέπει να εισάγουν περισσότερη αλλοίωση στην ποιότητα των εικόνων ώστε να εξασφαλιστεί η πλήρης αποδοτικότητα του μηχανισμού ανίχνευσης.

Ανάλογα με τη μέθοδο που χρησιμοποιείται, υπάρχουν περιπτώσεις που η αποδοτικότητα του μηχανισμού υδατογράφησης μπορεί να υπολογιστεί αναλυτικά. Έγκυρη ωστόσο είναι και η πιθανότητα που θα προκύψει από μία εμπειρική ανάλυση της αποδοτικότητας, κατά την οποία ο μηχανισμός υδατογράφησης δοκιμάζεται σε ένα σημαντικό αριθμό εικόνων. Το ποσοστό των εικόνων που παρουσιάσουν θετική απόκριση ανίχνευσης προσεγγίζει ικανοποιητικά την πιθανότητα της αποτελεσματικότητας του μηχανισμού, με την προϋπόθεση βέβαια πως οι εικόνες επαρκούν σε πλήθος και είναι κατάλληλα επιλεγμένες ώστε να αντικατοπτρίζουν την πραγματική κατανομή εικόνων του φωτογραφικού αρχείου.

3.2.2.3.2 Πιστότητα – Fidelity

Στη γενική περίπτωση, η πιστότητα ενός συστήματος υδατογράφησης αναφέρεται στην οπτική ομοιότητα μεταξύ του αρχικού και του υδατογραφημένου ψηφιακού αντιγράφου. Ωστόσο, καθώς το υδατογραφημένο αντικείμενο μοιραία θα υποστεί κάποια αλλοίωση κατά την μετάδοση του από τον πομπό στον δέκτη, ένας ελαφρά διαφοροποιημένος ορισμός της πιστότητας θα ήταν καταλληλότερος. Εναλλακτικά, ως πιστότητα ενός συστήματος υδατογράφησης ορίζεται η οπτική ομοιότητα μεταξύ του αρχικού και του υδατογραφημένου έργου όπως αυτό παρουσιάζεται τελικά στον χρήστη.

Για παράδειγμα, όταν ένα ψηφιακό αρχείο βίντεο πρόκειται να μεταδοθεί με την χρήση του NTSC πρότυπου μετάδοσης, ή ένα αρχείο ήχου μέσω AM ραδιόφωνου, η ποιότητα μετάδοσης των συγκεκριμένων τεχνολογιών είναι σχετικά μειωμένη. Το αποτέλεσμα είναι μετά το πέρας της μετάδοσης, οι διαφορές μεταξύ της αρχικής και της υδατογραφημένης εικόνας να είναι πια

αδιάκριτες λόγω της αλλοίωσης που εισάγει το κανάλι μετάδοσης. Αντιθέτως, στα HDTV και DVD πρότυπα βίντεο και ήχου, τα σήματα μετάδοσης βρίσκονται σε πολύ υψηλά επίπεδα ποιότητας και απαιτούν υδατογραφήματα με αυξημένη την ιδιότητα της πιστότητας.

Υπάρχουν βέβαια και περιπτώσεις όπου μία ελαφρά επίδραση των υδατογραφημάτων στην ποιότητα της εικόνας είναι ανεκτή, με κέρδος κάποια αύξηση στην ανθεκτικότητα ή κάποια μείωση στο κόστος.

3.2.2.3.3 Ωφέλιμο Φορτίο Δεδομένων – Data Payload

Το ωφέλιμο φορτίο δεδομένων, αναφέρεται στον αριθμό των bits που ένα σύστημα υδατογράφησης ενσωματώνει στη μονάδα του χρόνου ή σε ένα ψηφιακό αντικείμενο. Για μια ψηφιακή φωτογραφία, το φορτίο των δεδομένων είναι ο αριθμός των bits που κωδικοποιείται μέσα στην εικόνα. Σε ένα αρχείο ήχου αντιθέτως, είναι ο αριθμός των κωδικοποιημένων bits που μεταδίδονται στην μονάδα του χρόνου. Στην περίπτωση του βίντεο, το ωφέλιμο φορτίο δεδομένων μπορεί να αναφέρεται είτε στον αριθμό των bits που μεταδίδονται στην μονάδα του χρόνου είτε σε κάθε καρέ (frame). Ένα υδατογράφημα που ενσωματώνει N-bits αναφέρεται με το όνομα N-bit υδατογράφημα και μπορεί να χρησιμοποιηθεί για να κωδικοποιήσει 2^N διαφορετικά μηνύματα.

Το ωφέλιμο φορτίο που απαιτείται σε κάθε περίπτωση διαφοροποιείται σημαντικά ανάλογα με την εφαρμογή. Οι εφαρμογές ελέγχου αντιγραφής μπορούν να περιορίσουν το ωφέλιμο φορτίο σε 4 με 8 bits πληροφορίας, που θα μεταδίδονται σε τακτά χρονικά διαστήματα των 10 δευτερολέπτων για αρχεία ήχου και 5 λεπτών για αρχεία βίντεο. Σε αντίστοιχα σενάρια, ο ρυθμός μετάδοσης δεδομένων αγγίζει προσεγγιστικά τα 0.5 bits ανά δευτερόλεπτο για τον ήχο και 0.02 bits ανά δευτερόλεπτο για αρχεία βίντεο. Στην αντίθετη

περίπτωση, η καταγραφή της τηλεοπτικής μετάδοσης εμφανίζει απαιτήσεις για τουλάχιστον 24 bits πληροφορίας ώστε να είναι δυνατός ο εντοπισμός όλων των πιθανών διαφημίσεων, με τον επιπλέον περιορισμό ότι η ανίχνευση θα πρέπει να γίνεται στο πρώτο δευτερόλεπτο του διαφημιστικού μηνύματος. Επομένως, ο ρυθμός μετάδοσης δεδομένων στη συγκεκριμένη εφαρμογή της τηλεοπτικής καταγραφής ανέρχεται στα 24 bits ανά δευτερόλεπτο, που είναι τρεις τάξεις μεγέθους μεγαλύτερη από την προηγούμενη εφαρμογή.

Οι περισσότερες εφαρμογές προϋποθέτουν την υποστήριξη δύο λειτουργιών από το μηχανισμό ανίχνευσης. Την ανίχνευση της παρουσίας ή μη του υδατογραφήματος και την αποκωδικοποίηση του ενός από τα 2^N μηνύματα που έχει ενσωματωθεί στο ψηφιακό αντικείμενο. Οι πιθανές απαντήσεις του μηχανισμού ανίχνευσης ανέρχονται σε 2^N+1.

Στη βιβλιογραφία της υδατογράφησης, ένας σημαντικός αριθμός από συστήματα που έχουν προταθεί περιορίζονται στην ενσωμάτωση ενός μονοσήμαντου υδατογραφήματος, οριοθετώντας την απόκριση του μηχανισμού ανίχνευσης σε μια δυαδική ένδειξη παρουσίας ή μη του υδατογραφήματος. Η συγκεκριμένη τακτική αναφέρεται με το όνομα "κωδικοποίηση του ενός bit" καθώς προκύπτουν 2^1 πιθανές απαντήσεις. Καθώς όμως, παρουσιάζεται μια ασυνέπεια με τις ονομαστικές συμβάσεις που χρησιμοποιήθηκαν παραπάνω, για λόγους συνέπειας έχει επικρατήσει ο όρος "κωδικοποίηση μηδενικού bit".

Το ωφέλιμο φορτίο δεδομένων αποτελεί μία από τις σπουδαιότερες σχεδιαστικές επιλογές ενός συστήματος υδατογράφησης. Παρουσιάζει αυξημένη συσχέτιση με άλλες ιδιότητες της υδατογράφησης όπως είναι η επεξεργαστική ισχύς, ο υπολογιστικός χρόνος, η ανθεκτικότητα, η πιστότητα κ.α. Οι επιμέρους προδιαγραφές που θα προκύψουν από την φύση της εφαρμογής, είναι αυτές που θα διαμορφώσουν την κατάλληλη ισορροπία.

3.2.2.3.4 Τυφλή και Ενημερωμένη Ανίχνευση

Αρκετά από τα συστήματα υδατογράφησης που έχουν προταθεί, προϋποθέτουν την παρουσία της αρχικής μη υδατογραφημένης εικόνας κατά τη διαδικασία ανίχνευσης. Για παράδειγμα, σε μια εφαρμογή καταγραφής των δοσοληψιών, είναι συνήθως ο ιδιοκτήτης του αρχικού ψηφιακού έργου που χρησιμοποιεί τον μηχανισμό ανίχνευσης για να εντοπίσει τον υπεύθυνο της διαρροής. Είναι λογικό ο ιδιοκτήτης να έχει στην κατοχή του το αρχικό μη υδατογραφημένο ψηφιακό έργο και να είναι σε θέση να το τροφοδοτήσει στο μηχανισμό ανίχνευσης. Η παρουσία του αρχικού έργου επιδρά ευεργετικά στην αποτελεσματικότητα του μηχανισμού ανίχνευσης, καθώς είναι εφικτή η αφαίρεση του αρχικού ψηφιακού αντικειμένου από το υδατογραφημένο, παράγοντας αυτούσιο το υδατογράφημα. Το πρωτότυπο μπορεί ακόμα να χρησιμοποιηθεί και για το συγχρονισμό του υδατογραφημένου έργου, στην περίπτωση που έχει αποσυγχρονιστεί από την εφαρμογή κάποιας μορφής επεξεργασίας. Ο συγχρονισμός αποτελεί τον πλέον ενδεδειγμένο τρόπο αντιμετώπισης των γεωμετρικών επιθέσεων που συχνά εφαρμόζονται στα ψηφιακά αντικείμενα με σκοπό να καταστήσουν τα υδατογραφήματα μη ανιχνεύσιμα.

Σε άλλες εφαρμογές, είναι επιτακτική η ανάγκη για ανίχνευση του υδατογραφήματος χωρίς να είναι δυνατή η συνδρομή του πρωτότυπου ψηφιακού αντικειμένου. Σε μια εφαρμογή ελέγχου αντιγραφής, ο μηχανισμός ανίχνευσης βρίσκεται σε κάθε μηχανισμό αναπαραγωγής του ψηφιακού αρχείου. Η διανομή του αρχικού ψηφιακού αντικειμένου μαζί με τον μηχανισμό ανίχνευσης είναι αδύνατη καθώς αναιρεί τον αυτοσκοπό του υδατογραφήματος.

Ο μηχανισμός ανίχνευσης που χρειάζεται το πρωτότυπο ψηφιακό αντικείμενο αναφέρεται με το όνομα ενημερωμένος ανιχνευτής. Ο ίδιος όρος χρησιμοποιείται και για τους ανιχνευτές που χρειάζονται ορισμένα μόνο στοιχεία

του πρωτότυπου ψηφιακού περιεχομένου και όχι το σύνολο του. Αντιθέτως, οι ανιχνευτές που δεν χρειάζονται το αρχικό αντικείμενο για να ανιχνεύσουν το υδατογράφημα αναφέρονται με το όνομα τυφλοί ανιχνευτές.

Στη βιβλιογραφία, τα συστήματα που χρησιμοποιούν ενημερωμένους ανιχνευτές αποκαλούνται ιδιωτικά συστήματα υδατογράφησης, ενώ εκείνα με του τυφλούς ανιχνευτές ονομάζονται δημόσια συστήματα υδατογράφησης. Η παραπάνω ορολογία πηγάζει από την γενικότερη χρησιμότητα του συστήματος σε εφαρμογές, όπου μόνο ένα επιλεγμένο σύνολο από ανθρώπους είναι εξουσιοδοτημένο για την ανίχνευση του υδατογραφήματος (ιδιωτικά συστήματα υδατογράφησης) και σε εφαρμογές όπου η ανίχνευση του υδατογραφήματος αποτελεί καθολικό προνόμιο.

3.2.2.3.5 Ανθεκτικότητα – Robustness

Ως ανθεκτικότητα υδατογράφησης ορίζεται η ικανότητα του μηχανισμού ανίχνευσης να ανιχνεύει το υδατογράφημα, ακόμα και στην περίπτωση που το ψηφιακό αντικείμενο έχει υποστεί κάποια επεξεργασία. Μερικά παραδείγματα συνηθισμένων λειτουργιών επεξεργασίας σήματος είναι το φιλτράρισμα (filtering), η συμπίεση με απώλεια πληροφορίας (lossy compression), εκτύπωση & σάρωση και οι γεωμετρικοί μετασχηματισμοί (περιστροφή, αλλαγή της κλίμακας μεγέθους, αποκοπή κ.α). Τα υδατογραφήματα που προορίζονται για αρχεία βίντεο θα πρέπει να παρουσιάζουν ανθεκτικότητα σε αντίστοιχες μορφές επεξεργασίας, στην εγγραφή του ψηφιακού αρχείου σε βιντεοκασέτα, αλλαγές στο ρυθμό των frames και άλλες παρεμβολές. Τα υδατογραφήματα αρχείων ήχου θα πρέπει να είναι ανθεκτικά σε επεξεργασία όπως το φιλτράρισμα, η εγγραφή σε κασέτα ήχου, και διάφορες παραλλαγές στην ταχύτητα αναπαραγωγής.

Η ανθεκτικότητα σε όλες τις πιθανές μορφές επεξεργασίας σήματος δεν αποτελεί επιτακτική ανάγκη για το σύνολο των εφαρμογών υδατογράφησης.

Αντιθέτως, το υδατογράφημα θα πρέπει να σχεδιαστεί με τέτοιο τρόπο ώστε να αντέχει όλες τις μορφές επεξεργασίας που είναι πιθανόν να συμβούν μεταξύ της στιγμής που θα υδατογραφηθεί και εκείνης που θα εξεταστεί. Είναι φανερό πως η ιδιότητα της ανθεκτικότητας του υδατογραφήματος παρουσιάζει αυξημένη εξάρτηση από την εφαρμογή όπου θα χρησιμοποιηθεί το σύστημα προστασίας πνευματικών δικαιωμάτων. Για παράδειγμα, στη εφαρμογή όπου καταγράφεται η τηλεοπτική και ραδιοφωνική εκπομπή, η απαίτηση ανθεκτικότητας του υδατογραφήματος είναι να αντέξει την επεξεργασία που θα υποστεί κατά την αναμετάδοση.

Στην περίπτωση της αναμετάδοσης βίντεο, η διαδικασία συνήθως περιλαμβάνει την συμπίεση του σήματος, την μετατροπή του από ψηφιακή σε αναλογική μορφή, την αναλογική του μετάδοση που ισοδυναμεί με το φιλτράρισμα των χαμηλών συχνοτήτων, την προσθήκη θορύβου κ.α. Σε μια τέτοια εφαρμογή, τα υδατογραφήματα δεν είναι υποχρεωμένα να επιβιώσουν σε επεξεργασία της μορφής, περιστροφή, κλιμάκωση, φιλτράρισμα των υψηλών συχνοτήτων ή άλλου είδους επεξεργασία που είναι πιθανό να συμβεί πριν την διαδικασία εισαγωγής του υδατογραφήματος ή μετά από την ανίχνευση του.

Υπάρχουν και περιπτώσεις που η ανθεκτικότητα του υδατογραφήματος είναι μια ιδιότητα αδιάφορη ή ακόμα και ανεπιθύμητη. Στην πραγματικότητα, ένας σημαντικός κλάδος της έρευνας γύρω από την υδατογραφία εστιάζεται στα εύθραυστα υδατογραφήματα. Ένα εύθραυστο υδατογράφημα είναι ένα υδατογράφημα σχεδιασμένο ώστε να μην παρουσιάζει καμία ανθεκτικότητα. Για παράδειγμα, ένα υδατογράφημα που έχει σχεδιαστεί για λόγους πιστοποίησης της αυθεντικότητας θα πρέπει να είναι εξαιρετικά εύθραυστο. Κάθε επεξεργασία του υδατογραφήματος θα πρέπει να το καθιστά μη ανιχνεύσιμο, ώστε να διαπιστώνεται κατά την πιστοποίηση της αυθεντικότητας αν το ψηφιακό περιεχόμενο έχει υποστεί έστω και την παραμικρή αλλοίωση.

Αντιθέτως, υπάρχουν εφαρμογές που τα υδατογραφήματα θα πρέπει να είναι ανθεκτικά σε κάθε πιθανή τροποποίηση του ψηφιακού περιεχομένου που διατηρεί αναλλοίωτη την ποιότητα του. Πρόκειται για περιπτώσεις όπου η επεξεργασία που ενδέχεται να εφαρμοστεί στον ψηφιακό αντικείμενο είναι απρόβλεπτη.

3.2.2.3.6 Ασφάλεια - Security

Η ασφάλεια ενός υδατογραφήματος έγκειται στην ικανότητα του να αντιστέκεται σε κακόβουλες επιθέσεις. Ως κακόβουλη επίθεση ορίζεται κάθε διαδικασία που έχει αποκλειστικό στόχο την παρεμπόδιση του σκοπού του υδατογραφήματος. Το σύνολο των επιθέσεων που ενδέχεται να υποστεί ένα σύστημα υδατογράφησης μπορεί να διαχωριστεί στις ακόλουθες τρεις κατηγορίες.

- Μη εξουσιοδοτημένη αφαίρεση
- Μη εξουσιοδοτημένη ενσωμάτωση
- Μη εξουσιοδοτημένη ανίχνευση

Η μη εξουσιοδοτημένη αφαίρεση και ενσωμάτωση αναφέρονται με το όνομα ενεργητικές επιθέσεις καθώς τροποποιούν το ίδιο το ψηφιακό αντικείμενο. Η μη εξουσιοδοτημένη ανίχνευση δεν επηρεάζει το ψηφιακό περιεχόμενο και φέρεται με τον χαρακτηρισμό παθητική επίθεση.

Η σημασία των παραπάνω επιθέσεων συνδέεται στενά με την εφαρμογή της υδατογράφησης. Υπάρχουν περιπτώσεις που το υδατογράφημα δεν απειλείται από κακοπροαίρετους εχθρούς και δεν υπάρχει η ανάγκη της ασφάλειας απέναντι σε οποιαδήποτε επίθεση. Για παράδειγμα, μια εφαρμογή που χρησιμοποιεί τα υδατογραφήματα για να παρέχει επιπρόσθετη λειτουργικότητα στους καταναλωτές δεν παρουσιάζει ανάγκη για ασφάλεια. Ωστόσο, υπάρχουν

πολλές εφαρμογές που η ασφάλεια του υδατογραφήματος αποτελεί σημαντική προδιαγραφή και είναι αναγκαίο να γίνει ο διαχωρισμός ανάμεσα στις διαφορετικού τύπου επιθέσεις.

Η μη εξουσιοδοτημένη αφαίρεση αναφέρεται στις επιθέσεις που έχουν ως στόχο να αποτρέψουν την ανίχνευση του υδατογραφήματος. Συνηθίζεται ο διαχωρισμός των μορφών μη εξουσιοδοτημένης ανίχνευσης σε δύο κατηγορίες: επιθέσεις αφαίρεσης και επιθέσεις επικάλυψης. Οι διαφορές των παραπάνω επιθέσεων είναι λεπτές και δεν θα γίνει περαιτέρω αναφορά. Διαισθητικά μπορούμε να πούμε πως η αφαίρεση ενός υδατογραφήματος σημαίνει ότι ένα ψηφιακό αντικείμενο που έχει υποστεί επίθεση δεν περιέχει πια κανένα υδατογράφημα. Δηλαδή, αν ένα υδατογράφημα αφαιρεθεί ολοκληρωτικά δεν είναι δυνατή η ανίχνευση του ούτε με τη χρήση ενός πιο εξελιγμένου και έξυπνου ανιχνευτή. Η απαλοιφή του υδατογραφήματος δεν σημαίνει απαραίτητα την ανακατασκευή του αρχικού ψηφιακού μη υδατογραφημένου αντικειμένου. Αντιθέτως, ο στόχος της επίθεσης είναι να παράγει ένα νέο ψηφιακό αντικείμενο που θα είναι οπτικά όμοιο με το αρχικό και δεν θα είναι σε καμία περίπτωση δυνατή η ανίχνευση κάποιου υδατογραφήματος. Το αρχικό ψηφιακό αντικείμενο ανταποκρίνεται στην παραπάνω απαίτηση ωστόσο είναι μόνο ένα από τα πολλά στιγμιότυπα που την ικανοποιούν.

Επικάλυψη του υδατογραφήματος σημαίνει πως το αντικείμενο που έχει υποστεί επίθεση μπορεί ακόμα να θεωρηθεί πως περιέχει υδατογράφημα, αλλά το υδατογράφημα είναι μη ανιχνεύσιμο από τους διαθέσιμους ανιχνευτές. Πιο έξυπνοι και εξελιγμένοι ανιχνευτές ίσως να είναι σε θέση να ανιχνεύσουν το υδατογράφημα. Για παράδειγμα, αρκετοί ανιχνευτές υδατογράφησης εικόνας δεν είναι σε θέση να ανιχνεύσουν το υδατογράφημα, όταν η εικόνα περιστραφεί έστω και ελάχιστα. Επομένως, κάποιος μπορεί να εφαρμόσει μια περιστροφή της εικόνας αρκετά μικρή ώστε να είναι απαρατήρητη, παράγοντας έτσι μια παραποιημένη εικόνα με αρκετά καλή ποιότητα. Με δεδομένο ότι ο ανιχνευτής

υδατογράφησης είναι ευαίσθητος στις περιστροφές δεν θα καταφέρει να ανιχνεύσει το υδατογράφημα. Ωστόσο, το υδατογράφημα μπορεί ακόμα να ανιχνευθεί από έναν πιο έξυπνο ανιχνευτή που θα καταφέρει να συγχρονίσει την εικόνα. Υπό αυτήν την έννοια μπορεί να θεωρηθεί ότι το υδατογράφημα είναι ακόμα παρών.

Η μη εξουσιοδοτημένη ενσωμάτωση, που συχνά συναντάται με το όνομα "πλαστογραφία", αναφέρεται σε ενέργειες παράνομης τοποθέτησης υδατογραφημάτων σε ψηφιακά αντικείμενα που δεν θα έπρεπε να τα περιέχουν. Για παράδειγμα, σε ένα σύστημα υδατογράφησης που χρησιμοποιείται για το έλεγχο της αυθεντικότητας, η αδυναμία του συστήματος δεν έγκειται στον αν ο επίδοξος παραβάτης μπορεί να καταστήσει το υδατογράφημα μη ανιχνεύσιμο, αλλά στο αν είναι σε θέση να ξεγελάσει τον ανιχνευτή ώστε να αποφανθεί καταφατικά για την ύπαρξη ενός μη έγκυρου υδατογραφήματος. Με αυτό τον τρόπο κατά την διαμάχη για την αυθεντικότητα και την κυριότητα του ψηφιακού αντικειμένου, υπάρχει σημαντική πιθανότητα ο ανιχνευτής να δώσει λάθος απάντηση αφού θα διαπιστώσει την ύπαρξη περισσότερων του ενός υδατογραφημάτων.

Η μη εξουσιοδοτημένη ανίχνευση που ανήκει στις παθητικές επιθέσεις διαχωρίζεται σε τρία επίπεδα ασφάλειας. Το πρώτο πιο διεισδυτικό επίπεδο μη εξουσιοδοτημένης ανίχνευσης είναι εκείνο που ο επίδοξος παραβάτης ανιχνεύει και αποκρυπτογραφεί το ενσωματωμένο μήνυμα. Αποτελεί την πιο απλή και περιεκτική μορφή μη εξουσιοδοτημένης ανάγνωσης. Μία λιγότερο διεισδυτική μορφή επιθέσεων συμβαίνει όταν ο επίδοξος παραβάτης είναι σε θέση να ανιχνεύσει τα υδατογραφήματα και επιπλέον να διαχωρίσει το ένα από το άλλο, αλλά δεν είναι σε θέση να αποκρυπτογραφήσει το περιεχόμενο τους. Η λιγότερο διεισδυτική μορφή επίθεσης συμβαίνει όταν ο παραβάτης είναι σε θέση να διαπιστώσει την ύπαρξη ενός υδατογραφήματος, αλλά δεν είναι σε θέση να

αποκρυπτογραφήσει το περιεχόμενο, ούτε και να διαχωρίσει τα ενσωματωμένα μηνύματα.

Σε γενικές γραμμές, οι παθητικές επιθέσεις εμπίπτουν περισσότερο στον τομέα της στεγανογραφίας παρά της υδατογραφίας, ωστόσο υπάρχουν εφαρμογές υδατογράφησης που παρουσιάζουν αδυναμία στις συγκεκριμένες επιθέσεις. Για παράδειγμα, ας θεωρήσουμε ότι μια εταιρεία που παρέχει υπηρεσίες τηλεοπτικής αναμετάδοσης, ενσωματώνει τα υδατογραφήματα χωρίς καμία επιβάρυνση και χρεώνει για την παραγωγή των αναλυτικών αναφορών ανίχνευσης. Ένας παραβάτης που έχει την δυνατότητα να διαβάζει τα υδατογραφήματα μπορεί να στήσει μία ανταγωνιστική υπηρεσία απαλλαγμένος από το κόστος την ενσωμάτωσης των υδατογραφημάτων.

3.2.2.3.7 Κόστος

Η οικονομική αποτίμηση της ενσωμάτωσης μηχανισμών τοποθέτησης και ανίχνευσης υδατογραφημάτων μπορεί να αποβεί εξαιρετικά πολύπλοκή και εξαρτάται άμεσα από το υπάρχον επιχειρηματικό μοντέλο [30]. Από τεχνολογική άποψη, τα δύο κυρίαρχα θέματα είναι η ταχύτητα με την οποία θα πρέπει να διεκπεραιώνεται η τοποθέτηση και η ανίχνευση του υδατογραφήματος, καθώς και ο αριθμός των μηχανισμών τοποθέτησης και ανίχνευσης που θα πρέπει ενσωματωθούν. Ανάλογα θέματα που ανακύπτουν σχετίζονται με το αν οι μηχανισμοί τοποθέτησης και ανίχνευσης θα πρέπει να υλοποιηθούν σαν ειδικού σκοπού συσκευές υλικού ή σαν εφαρμογές λογισμικού.

Στην εφαρμογή της παρακολούθησης αναμετάδοσης, τόσο οι μηχανισμοί τοποθέτησης όσο και οι μηχανισμοί ανίχνευσης θα πρέπει να λειτουργούν σε τουλάχιστον πραγματικό χρόνο. Η συγκεκριμένη απαίτηση προκύπτει από την αναγκαιότητα να μην καθυστερεί το μεταδιδόμενο πρόγραμμα από τον μηχανισμό τοποθέτησης, ενώ ο ανιχνευτής θα πρέπει να ανταποκρίνεται στην

ταχύτητα μετάδοσης του προγράμματος. Από την άλλη μεριά, ένας ανιχνευτής που χρησιμοποιείται για την πιστοποίηση της ιδιοκτησίας είναι χρήσιμος ακόμα και στην περίπτωση που απαιτεί χρόνο ίσο με μερικές μέρες για να αποφανθεί σχετικά με την ύπαρξη του υδατογραφήματος. Ο συγκεκριμένος ανιχνευτής θα χρησιμοποιηθεί μόνο στην περίπτωση που θα προκύψει κάποια διαμάχη σχετικά με την κυριότητα ενός ψηφιακού αντικειμένου, περίπτωση που εμφανίζεται με αρκετά μικρή συχνότητα. Σε αυτή την περίπτωση η απόκριση του ανιχνευτή σχετικά με την παρουσία του υδατογραφήματος είναι αρκετά σημαντική ώστε ο χρήστης να είναι διατεθειμένος να περιμένει.

Μία επιπλέον κρίσιμη παράμετρος που διαδραματίζει σημαντικό ρόλο κατά την οικονομική αποτίμηση ενός συστήματος υδατογράφησης, είναι το γεγονός πως διαφορετικές εφαρμογές απαιτούν διαφορετικό αριθμό μηχανισμών τοποθέτησης και ανίχνευσης. Η παρακολούθηση αναμετάδοσης, στην τετριμμένη της περίπτωση, χρειάζεται ένα μικρό αριθμό από μηχανισμούς τοποθέτησης και μερικές εκατοντάδες ανιχνευτές κατανεμημένους σε διαφορετικά γεωγραφικά σημεία. Η εφαρμογή του ελέγχου αντιγραφής μπορεί να χρειάζεται μόνο ένα μικρό σύνολο από μηχανισμούς τοποθέτησης αλλά χιλιάδες ανιχνευτές που θα συνοδεύουν κάθε συσκευή αναπαραγωγής ψηφιακού περιεχομένου. Αντιστρόφως, στη εφαρμογή ανίχνευσης δοσοληψιών όπως αυτή υλοποιήθηκε από την DIVX και στη οποία κάθε συσκευή αναπαραγωγής τοποθετεί ένα διαφορετικό υδατογράφημα, οι ανάγκες του συστήματος υδατογράφησης προδιαγράφουν την ύπαρξη χιλιάδων μηχανισμών τοποθέτησης και ενός μικρού αριθμού ανιχνευτών. Ο γενικός κανόνας που προκύπτει είναι ότι όσο μεγαλύτερη είναι η ανάγκη σε αριθμό μιας συσκευής τόσο λιγότερο θα πρέπει να κοστίζει.

Το κόστος ενός συστήματος υδατογράφησης για την προστασία του ψηφιακού περιεχομένου και γενικότερα των τεχνολογικών μέσων που επιστρατεύονται για τη προστασία του δικαιώματος αναπαραγωγής και εκμετάλλευσης, δεν θα πρέπει να ξεπερνά την αξία του ίδιου του ψηφιακού

περιεχομένου. Δεν υπάρχει λογική στη χρησιμοποίηση ενός ακριβού συστήματος προστασίας, όταν η αντικειμενική αξία του περιεχομένου και οι δυνατότητες εκμετάλλευσης του δεν μπορούν να ισοσταθμίσουν το δαπανηθέν ποσό.

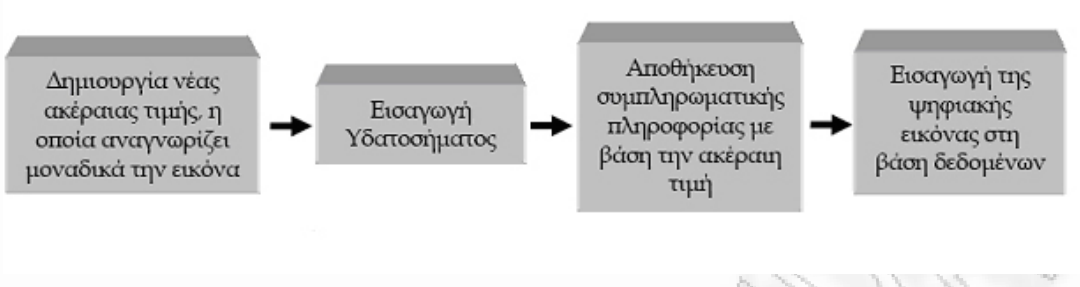
3.2.2.4 Υδατογράφηση – Διαδικασία

Κατά τη διαδικασία υδατογράφησης σε όλα τα αρχεία που πρόκειται να διανεμηθούν εισάγεται ένα υδατογράφημα πριν να μπουν στην αλυσίδα περιεχομένου. Τα βασικά ζητήματα αυτής της διαδικασίας είναι τα εξής:

- Ο σχεδιασμός ενός σήματος υδατογράφησης που θα προστεθεί στο σήμα φιλοξενητή, δηλαδή στο αντικείμενο που θέλουμε να προστατεύσουμε. Τυπικά το σήμα υδατογραφήματος εξαρτάται από ένα κλειδί και την πληροφορία υδατογράφησης, καθώς και από δεδομένα του αντικειμένου.
- Ο σχεδιασμός μίας μεθόδου ενσωμάτωσης που εισάγει το σήμα υδατογράφησης στα δεδομένα φιλοξενητές και έχει σαν αποτέλεσμα ένα σύνολο από υδατογραφημένα δεδομένα.
- Ο σχεδιασμός της μεθόδου εξαγωγής (ανίχνευσης) που ανακτά την υδατογραφημένη πληροφορία από το μίγμα σημάτων χρησιμοποιώντας το κλειδί και πιθανόν και την αρχική πληροφορία.

Μηχανισμός Ενσωμάτωσης

Ένα από τα πιο βασικά χαρακτηριστικά της μεθόδου υδατογράφησης είναι η ικανότητα προ-επεξεργασίας της ψηφιακής εικόνας, η εξαγωγή συμπληρωματικής πληροφορίας και η αποθήκευση της πληροφορίας αυτής σε μια βάση δεδομένων. Η συσχέτιση της ψηφιακής εικόνας με τη συμπληρωματική πληροφορία επιτυγχάνεται με τη χρήση μιας ακέραιας τιμής, του imageid (μοναδικού αναγνωριστικού ανά εικόνα).



Εικόνα 7: Μηχανισμός Ενσωμάτωσης Υδατογραφήματος

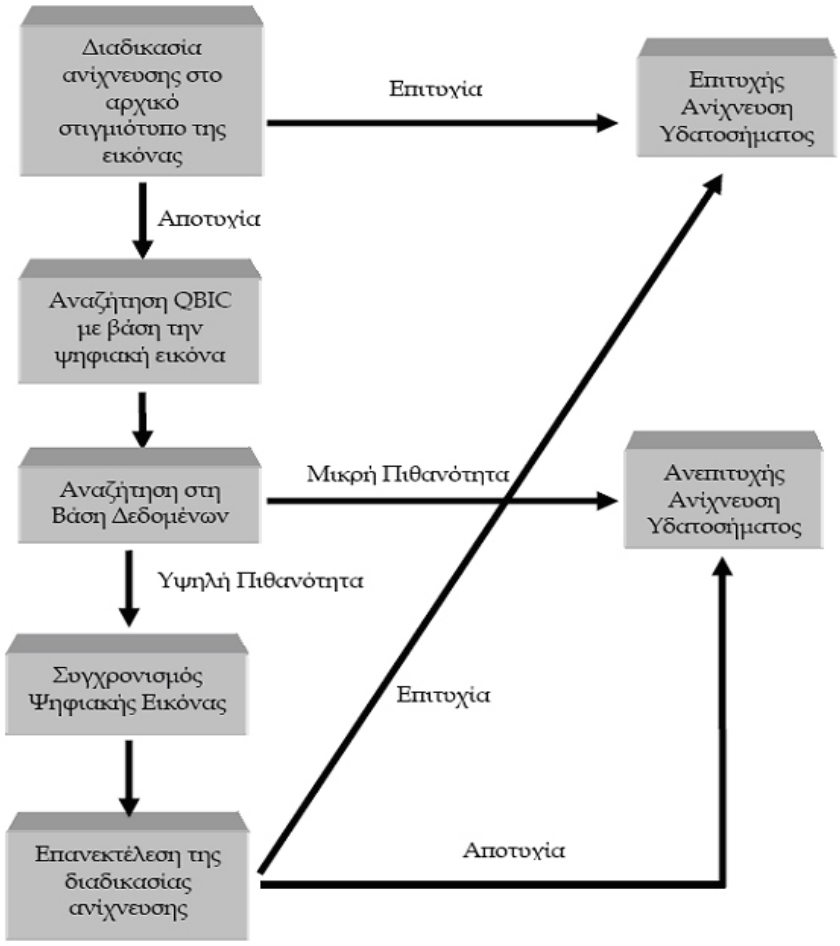
Η συμπληρωματική πληροφορία που εξάγεται υποστηρίζει τη διαδικασία του συγχρονισμού της ψηφιακής εικόνας (image registration) και συνεπώς υποστηρίζει την ανθεκτικότητα έναντι γεωμετρικών επιθέσεων κατά τη διάρκεια της διαδικασίας ανίχνευσης.

Μηχανισμός Ανίχνευσης

Το κύριο μειονέκτημα των περισσότερων μηχανισμών ανίχνευσης υδατογραφημάτων είναι η ανικανότητα αντιμετώπισης των επιθέσεων που εμπλέκουν τον αποσυγχρονισμό του ανιχνευτή. Οι γεωμετρικές επιθέσεις είναι ένα μικρό αλλά σημαντικό υποσύνολο αυτών των επιθέσεων. Το καλύτερο μέτρο αντιμετώπισης του αποσυγχρονισμού είναι η χρήση του συγχρονισμού της εικόνας (image registration). Ο συγχρονισμός της εικόνας είναι η διαδικασία κατά την οποία, ενόσω το υδατογράφημα ενσωματώνεται, γίνεται εξαγωγή ενός στιγμιότυπου της ψηφιακής εικόνας. Με την εύρεση του κατάλληλου στιγμιότυπου και την είσοδο αυτού στο μηχανισμό ανίχνευσης υποστηρίζεται ο συγχρονισμός της ψηφιακής εικόνας στην οποία γίνεται επίθεση και τελικώς η ανίχνευση του υδατογραφήματος. Η εύρεση, παρόλα αυτά, του κατάλληλου στιγμιότυπου χωρίς περαιτέρω διαθέσιμη πληροφορία δεν είναι μια απλή διαδικασία. Στην πιο απλή περίπτωση, η αναγκαία επιπρόσθετη πληροφορία είναι η ίδια η πρωτότυπη εικόνα.

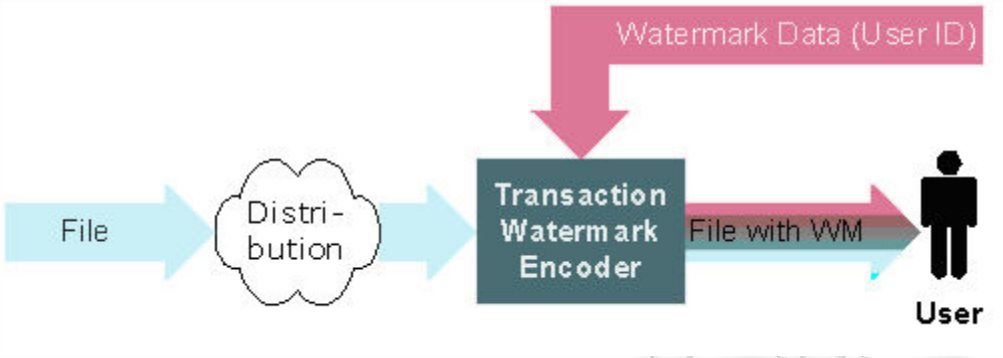
Η διασύνδεση της μεθόδου υδατογράφησης με βάσεις δεδομένων παρέχει τη βάση για την ανάπτυξη ενός ακόμα πιο ισχυρού μηχανισμού ανίχνευσης. Ο ανιχνευτής αρχικά τροφοδοτείται με μια ψηφιακή εικόνα προς ανίχνευση του υδατογραφήματός της. Αν η πρώτη προσπάθεια ανίχνευσης είναι ανεπιτυχής ο ανιχνευτής προσπαθεί να επεξεργασθεί την ψηφιακή εικόνα με σκοπό το συγχρονισμό της, ο οποίος έχει χαθεί από κάποιου τύπου επίθεση. Αν επιτευχθεί ο συγχρονισμός το υδατογράφημα θα ανιχνευθεί. Κατά τη διάρκεια της δεύτερης προσπάθειας η παρουσία της πρωτότυπης εικόνας είναι καθοριστική. Αν και η μέθοδος υδατογράφησης μπορεί να έχει πρόσβαση σε έναν μεγάλο αριθμό ψηφιακών εικόνων που είναι αποθηκευμένες στη βάση δεδομένων είναι αδύνατον να καθορισθεί ποια εικόνα επακριβώς ανταποκρίνεται στο αντίγραφο που βρίσκεται στον ανιχνευτή. Στην επίλυση αυτού του προβλήματος συμβάλλει η ανάπτυξη προηγμένων υπηρεσιών αναζήτησης.

Η διαδικασία της ανίχνευσης ενός υδατογραφήματος φαίνεται στην επόμενη εικόνα:



Εικόνα 8: Μηχανισμός Ανίχνευσης Υδατογραφήματος

Μια δεύτερη μέθοδος που χρησιμοποιεί αυτή την τεχνολογία είναι η ενσωμάτωση ενός "transaction υδατογραφήματος" όπως απεικονίζεται στο παρακάτω διάγραμμα. Τα transaction υδατογραφήματα επιτρέπουν την καθιέρωση μιας σύνδεσης μεταξύ ενός τυχαίου χρήστη στην αλυσίδα περιεχομένου με το περιεχόμενο που "έλαβε". Στα σενάρια όπου απαιτούνται αναγνωριστικά και περιεχομένου και χρηστών, μπορούν να συνδυασθούν και οι δύο τύποι υδατογραφημάτων.



Εικόνα 9: Transaction Υδατογράφημα

Το μέγιστο μέγεθος του "φορτίου" του υδατογραφήματος (είτε πρόκειται για ένα *a priori* είτε για ένα transaction υδατογράφημα) μπορεί να ποικίλει και εξαρτάται από τον τύπο του περιεχομένου, κυρίως λόγω του ποσού των δεδομένων που μπορεί αξιόπιστα και ανθεκτικά να μεταφερθεί μέσα στο υδατογράφημα. Γενικά, όσο μεγαλύτερο είναι το αρχείο, τόσο περισσότερα στοιχεία μπορούν να κρυφτούν μέσα σε αυτό.

3.2.2.5 Υδατογράφηση – Μειονεκτήματα

Αρχικά τα υδατογραφήματα δεν μπορούν να χρησιμοποιηθούν με όλους τους τύπους περιεχομένου. Τα μικρά στοιχεία γραφικών όπως λογότυπα ή κείμενο δεν μπορούν να φέρουν υδατογραφήματα λόγω ενός **γενικού περιορισμού στο ποσό στοιχείων που μπορούν να ενσωματωθούν στο περιεχόμενο**. Το μέγιστο μέγεθος του φορτίου του υδατογραφήματος εξαρτάται από τρεις κύριους παράγοντες:

- τύπος περιεχομένου (audio, video, εικόνες, γραφικά, κείμενα)
- μέγεθος περιεχομένου:

- video: ρυθμός πλαισίων, μέγεθος εικόνων, ποσοστό συμπίεσης, μήκος

- audio: ρυθμός δειγματοληψίας, ποσοστό συμπίεσης, διάρκεια

- εικόνες: μέγεθος εικόνων, ποσοστό συμπίεσης.

• ανθεκτικότητα: Σε ποιες "επιθέσεις" πρέπει να αντεπεξέλθει το υδατογράφημα;

- Κοινή επεξεργασία σήματος: Το υδατογράφημα πρέπει να μπορεί να ανακτηθεί ακόμη και αν έχουν εφαρμοστεί εναντίον των δεδομένων του κοινές λειτουργίες επεξεργασίας σήματος. Αυτές οι λειτουργίες μπορεί να είναι η μετατροπή του σήματος από ψηφιακό σε αναλογικό και από αναλογικό σε ψηφιακό, επανάληψη της δειγματοληψίας, επανασυμπίεση, dithering, κβαντοποίηση και κοινές ενισχύσεις στο χρώμα και το contrast της εικόνας ή στο μπάσο του ήχου και άλλα.

- Κοινές γεωμετρικές παραμορφώσεις (σε δεδομένα βίντεο και εικόνας): Τα υδατογραφήματα σε βίντεο και εικόνα θα πρέπει να είναι ανθεκτικά σε λειτουργίες γεωμετρικής μετατροπής όπως είναι, η περιστροφή, η κλιμάκωση, το cropping.

- Επιθέσεις εξαπάτησης: Το υδατογράφημα πρέπει να είναι ανθεκτικό έναντι των χρηστών που κατέχουν και επεξεργάζονται ένα αντίγραφο των δεδομένων.

Επίσης αν ένα υδατογράφημα πρόκειται να χρησιμοποιηθεί σε δίκη, πρέπει να είναι αδύνατον για τους μη εξουσιοδοτημένους χρήστες να συνδυάσουν τις εικόνες του για να παράγουν ένα διαφορετικό αλλά ισχύον υδατογράφημα με την πρόθεση της παγίδευσης κάποιου άλλου.

Δεύτερον, κάποιος μπορεί να ισχυριστεί ότι ανάλογα με το μέγεθος του φορτίου που ενσωματώνεται σε έναν ορισμένο τύπο περιεχομένου, **η ανθεκτικότητα του υδατογραφήματος μπορεί να ποικίλει**. Δεδομένου ότι αυτοί οι περιορισμοί είναι αρκετά αυστηροί με τους σημερινούς αλγορίθμους υδατογράφησης, έχει ευρέως συμφωνηθεί τα υδατογραφήματα να φέρουν μόνο ένα μικρό ποσό πληροφοριών, χαρακτηριστικά ένα αναγνωριστικό περιεχομένου. Ένας δεύτερος περιορισμός των τεχνολογιών υδατογράφησης είναι ότι η

ενσωμάτωση ενός υδατογραφήματος σημαίνει αλλαγή του αρχικού περιεχομένου. Ενώ σε πολλές περιπτώσεις αυτή η αλλαγή δεν έχει επιπτώσεις στην ποιότητα του υλικού από την πλευρά της ανθρώπινης αντίληψης, μπορεί να καταστήσει δύσκολη την ενσωμάτωση υδατογραφημάτων επανειλημμένα στο ίδιο περιεχόμενο χωρίς να γίνουν αντιληπτά. Ως εκ τούτου, τα υδατογραφήματα δεν μπορούν, παραδείγματος χάριν, να ενσωματωθούν κατά τη διάρκεια της επαναληπτικής διαδικασίας ανάπτυξης μιας διαφήμισης.

Τρίτον, όλα τα συστήματα υδατογραφημάτων που είναι γνωστά σήμερα είναι **ευαίσθητα στην αφαίρεση του υδατογραφήματος**. Δεν είναι συνήθως δυνατή η αφαίρεση του υδατογραφήματος χωρίς να υπάρχουν ουσιαστικές επιπτώσεις στην ποιότητα του περιεχομένου, κάτι που μπορεί να οδηγήσει στην κατάσταση όπου το αρχικό περιεχόμενο να μην μπορεί να ελέγχει.

Ένα τελευταίο μειονέκτημα είναι ότι η **ανίχνευση υδατογραφημάτων δεν μπορεί να λειτουργήσει με legacy περιεχόμενο εάν δεν είχε εισαχθεί εξαρχής υδατογράφημα**.

3.3 Τεχνολογικά Μέσα Προστασίας - Τεχνολογίες Privacy

Μια πτυχή της πρόκλησης της ανάπτυξης μιας αποτελεσματικής υποδομής DRM βρίσκεται στη συντήρηση του privacy, της εμπιστευτικότητας και της προστασίας των προσωπικών στοιχείων. Υπάρχουν πολλές κατανοητές ανησυχίες για το βαθμό στον οποίο οποιαδήποτε υποδομή DRM θα σημαίνει την εξολοκλήρου απαράδεκτη παρείσφρηση στην ιδιωτική και εμπορική ζωή των ανθρώπων, παρόλο που συγχρόνως αποδεικνύεται αποτελεσματική στην προστασία της πνευματικής ιδιοκτησίας.

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. Αυτό γίνεται ιδιαίτερα ευαίσθητο όταν τα ενδιαφερόμενα μέρη είναι μεμονωμένοι καταναλωτές. Ένα μεγάλο μέρος της συζήτησης γύρω από τη διαχείριση του privacy φαίνεται να εστιάζει στην εμπορική αξία των προσωπικών πληροφοριών, σε συνδυασμό με την αφύπνιση για τη "κλοπή ταυτότητας" και την κακή χρήση των πιστωτικών καρτών. Όσο σημαντικά και αν είναι αυτά τα ζητήματα, τείνουν να κάνουν τετριμμένο το θέμα των privacy δικαιωμάτων.

Η κατάλληλη υλοποίηση των "Privacy Enhancing Technologies" ("PETs") στην υποδομή DRM θα αποδειχθεί πιθανώς ουσιαστική στη μακροπρόθεσμη καταναλωτική αποδοχή της. Αυτό θα περιλαμβάνει τη χρήση τεχνολογιών ανωνυμίας, οι οποίες επιτρέπουν την επικύρωση των ταυτοτήτων από "έμπιστους τρίτους" (με άλλα λόγια, από μια οργάνωση που την εμπιστεύεται τόσο ο καταναλωτής όσο και ο διανομέας) χωρίς να αποκαλύπτεται η πραγματική ταυτότητα του καταναλωτή. Ενώ η εμπλοκή τρίτων μπορεί να προσθέσει περιττή πολυπλοκότητα, μια υποδομή DRM που αποτυγχάνει να λάβει υπόψη τις νόμιμες ανησυχίες για το privacy και την εμπιστευτικότητα είναι πιθανό να αποτύχει.

3.4 Τεχνολογικά Μέσα Προστασίας - Τεχνολογίες Πληρωμών

Υπάρχουν διάφοροι τύποι προτύπων πληρωμής διαθέσιμοι με τα συστήματα DRM. Ένας χαρακτηριστικός τρόπος πληρωμής για το περιεχόμενο είναι η εισαγωγή του αριθμού της πιστωτικής κάρτας σε μια ασφαλή ιστοσελίδα που κρυπτογραφείται από το πρωτόκολλο SSL. Η χρησιμοποίηση πιστωτικής κάρτας είναι ο πιο κοινός τρόπος αγοράς περιεχομένου (και αγαθών) on-line. Πρόσφατες εκτιμήσεις από την επιχείρηση πιστωτικών καρτών Visa, έχουν δείξει ότι οι ευρωπαίοι πελάτες ξόδεψαν €2.57 δισεκατομμύρια on-line χρησιμοποιώντας κάρτες Visa κατά τη διάρκεια του 2002, το οποίο είναι κατά

136% υψηλότερο απ' ό,τι την ίδια περίοδο το 2001. Η Visa επίσης υπολογίζει ότι καταγράφηκαν 31,1 εκατομμύρια συναλλαγές on-line κατά τη διάρκεια του 2002, έναντι 14,5 εκατομμυρίων το 2001. Εντούτοις, πολλοί χρήστες είναι ακόμα απρόθυμοι να χρησιμοποιήσουν τις πιστωτικές κάρτες τους άμεσα στον ιστοχώρο ενός on-line καταστήματος λόγω ανησυχίας σχετικά με το privacy και την ασφάλεια, ενώ οι on-line έμποροι έρχονται αντιμέτωποι μερικές φορές με ζητήματα ευθύνης.

Κατά τη διαδικασία χρήσης της πιστωτικής κάρτας, ο χρήστης εισάγει τον αριθμό της πιστωτικής κάρτας σε μια ασφαλή ιστοσελίδα που κρυπτογραφείται από το πρωτόκολλο SSL. Το πρωτόκολλο αυτό κρυπτογραφεί τα δεδομένα κατά τη μεταφορά τους και προαιρετικά πιστοποιεί τους εξυπηρετητές. Επίσης παρέχει εμπιστευτικότητα και ακεραιότητα δεδομένων. Το SSL χρησιμοποιεί τεχνικές ασύμμετρης κρυπτογράφησης στην αρχική "χειραψία", ώστε να επιτευχθούν οι ακόλουθοι στόχοι:

- Ο εξυπηρετητής εμπόρου και ο χρήστης αυθεντικοποιούνται μέσω των ψηφιακών πιστοποιητικών.
- Ο εξυπηρετητής εμπόρου και ο χρήστης συμφωνούν στη χρήση ενός συγκεκριμένου κλειδιού (session key) με το οποίο θα κρυπτογραφηθεί το υπόλοιπο της συναλλαγής. Με τον τρόπο αυτό, όποια πληροφορία ανταλλάσσεται από αυτό το σημείο και μετά είναι κρυπτογραφημένη με κλειδί που γνωρίζουν μόνο οι δύο πλευρές.

Επειδή υπάρχει κίνδυνος να γίνουν γνωστά τα στοιχεία της πιστωτικής κάρτας του χρήστη ή η κάρτα να είναι πλαστή, επεμβαίνει ένα δεύτερο πρωτόκολλο, το SET, το οποίο ορίζει ότι για τη σωστή λειτουργία του συστήματος ηλεκτρονικών πληρωμών δεν είναι απαραίτητη η αποθήκευση των εμπιστευτικών στοιχείων του πελάτη. Έτσι ουσιαστικά εκμηδενίζεται η πιθανότητα να κλαπούν τα στοιχεία της πιστωτικής κάρτας.

Ακόμα κι αν οι περισσότερες on-line πληρωμές γίνονται μέσω πιστωτικών καρτών, αναπτύσσονται αυτήν την περίοδο εναλλακτικοί τρόποι πληρωμής. Ένας εναλλακτικός τρόπος πληρωμής είναι μέσω ψηφιακών μετρητών. Ένα σύστημα ψηφιακών μετρητών αποτελείται συνήθως από τους Πελάτες(χρήστες), τους Πωλητές και την Τράπεζα. Κάθε νόμιμος Πελάτης έχει τη δυνατότητα να παραλάβει ψηφιακό νόμισμα από μια Τράπεζα και ανώνυμα να στείλει το νόμισμα στον Πωλητή. Ακολούθως, ο Πωλητής καταθέτει το ψηφιακό νόμισμα στην Τράπεζα και αυτή μπορεί να εξακριβώσει την εγκυρότητα του νομίσματος. Λόγω της ανωνυμίας του Πελάτη, η Τράπεζα δε μπορεί να συσχετίσει το νόμισμα με τον Πελάτη και όπως και ο Πωλητής, δε μπορεί να ανιχνεύσει και να καταγράψει τις συναλλαγές του Πελάτη.

Εκτός των παραπάνω, διάφορα συστήματα μικροπληρωμών αναπτύσσονται επίσης και θα γίνουν ενδεχομένως μια κοινή μέθοδος αγοράς DRM περιεχομένου, όχι μόνο on-line αλλά και για περιεχόμενο σε άλλες συσκευές. Ο μηχανισμός της μικροπληρωμής βασίζεται στον Παροχέα Υπηρεσιών Πληρωμής, στον Αγοραστή και στον Έμπορο, οι οποίοι διατηρούν μια μακροχρόνια σχέση. Ο Αγοραστής αποστέλλει δέσμη μικροπληρωμών στον Έμπορο, ενώ ένα σύνολο μικροπληρωμών επεξεργάζεται από τον Παροχέα Υπηρεσιών Πληρωμής και αποδίδεται στον Έμπορο. Άλλες επιχειρήσεις έχουν αναπτύξει συστήματα micropayment, τα οποία λειτουργούν μέσω κινητών τηλεφώνων, για χαμηλού κόστους συναλλαγές όπως ένα κομμάτι μουσικής από έναν on-line κατάλογο, ένα eBook ή ένα άρθρο από το επί πληρωμή τμήμα του ιστοχώρου μιας εφημερίδας.

Ένα παράδειγμα εναλλακτικού τρόπου πληρωμών χρησιμοποιεί η μουσική πύλη Popfile.de στη Γερμανία. Η συγκεκριμένη πύλη έχει αναπτύξει ένα σύστημα σε συνεργασία με τη Deutsche Telekom, το οποίο επιτρέπει στους χρήστες να διανείμουν και να κατεβάσουν μουσικά DRM αρχεία και χρεώνει τους χρήστες για το περιεχόμενο μέσω του λογαριασμού τηλεφώνου τους.

Τέλος διάφορες επιχειρήσεις έχουν αναπτύξει συστήματα, τα οποία επιτρέπουν στους χρήστες να εισάγουν την πιστωτική κάρτα τους μια φορά σε έναν κεντρικό server. Μόλις εγγραφεί, ο καταναλωτής έχει πρόσβαση σε ένα ηλεκτρονικό πορτοφόλι, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί για να αγοράσει περιεχόμενο από on-line πύλες, οι οποίες έχουν συμπράξει με την υπηρεσία. Το σύστημα υποστηρίζει ότι εγγυάται την ανωνυμία και το privacy, μειώνοντας ζητήματα ευθύνης στην πλευρά των on-line εμπόρων.

ΚΕΦΑΛΑΙΟ 4
ΕΜΠΟΡΙΚΑ ΔΙΑΘΕΣΙΜΑ ΣΥΣΤΗΜΑΤΑ

4.1 Λογισμικό Κρυπτογράφησης

Στην αγορά κυκλοφορούν αρκετά προγράμματα λογισμικού κρυπτογράφησης. Είναι πολύ σημαντικό να γίνεται σωστή επιλογή του προϊόντος που θα χρησιμοποιηθεί. Υπάρχουν προγράμματα που είτε δεν χρησιμοποιούν αρκετά ασφαλείς αλγόριθμους είτε δημιουργούν σφάλματα (bugs) στην υλοποίηση της κρυπτογράφησης. Επίσης, θα πρέπει η τεχνική κρυπτογράφησης να ελέγχεται από ειδικούς, ενώ οι μέθοδοι πρέπει να είναι γνωστές και το λογισμικό που τις υλοποιεί υψηλής ποιότητας.

4.1.1 Pretty 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. Μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσει όχι μόνο ηλεκτρονικά μηνύματα, αλλά και αρχεία. Επίσης παρέχει και δυνατότητες συμπίεσης.

Το PGP χρησιμοποιεί κρυπτογραφία δημόσιου και ιδιωτικού κλειδιού για να διασφαλίσει εμπιστευτικότητα. Επίσης χρησιμοποιεί ψηφιακές υπογραφές για να αυθεντικοποιήσει την ταυτότητα του αποστολέα, να εξασφαλίσει την ακεραιότητα του μηνύματος και να παρέχει υπηρεσίες μη-αποποίησης. Χρησιμοποιεί συνδυασμό συμμετρικής και ασύμμετρης κρυπτογραφίας για να επιταχύνει τη διαδικασία κρυπτογράφησης. Είναι σχεδιασμένο να κρυπτογραφεί

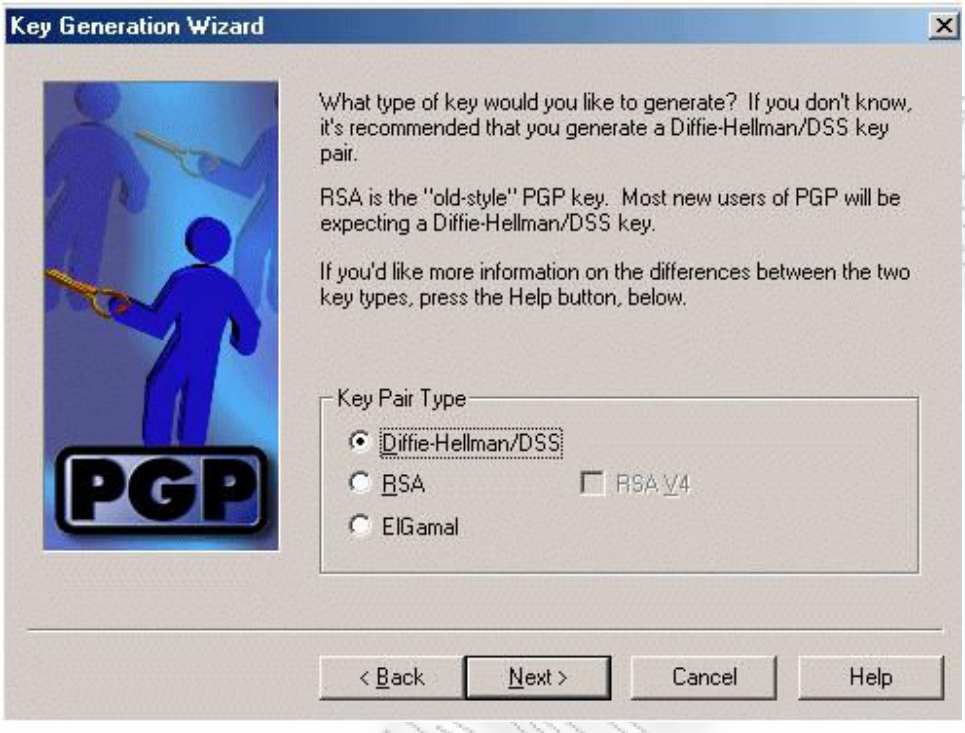
και να αποκρυπτογραφεί μηνύματα με χρήση συμμετρικού κλειδιού, αλλά να χρησιμοποιεί ασύμμετρες μεθόδους για να κρυπτογραφήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για να κρυπτογραφήσει το μήνυμα.

Όταν ένας χρήστης Α θέλει να στείλει ένα e-mail σε ένα χρήστη Β, η διαδικασία έχει ως εξής:

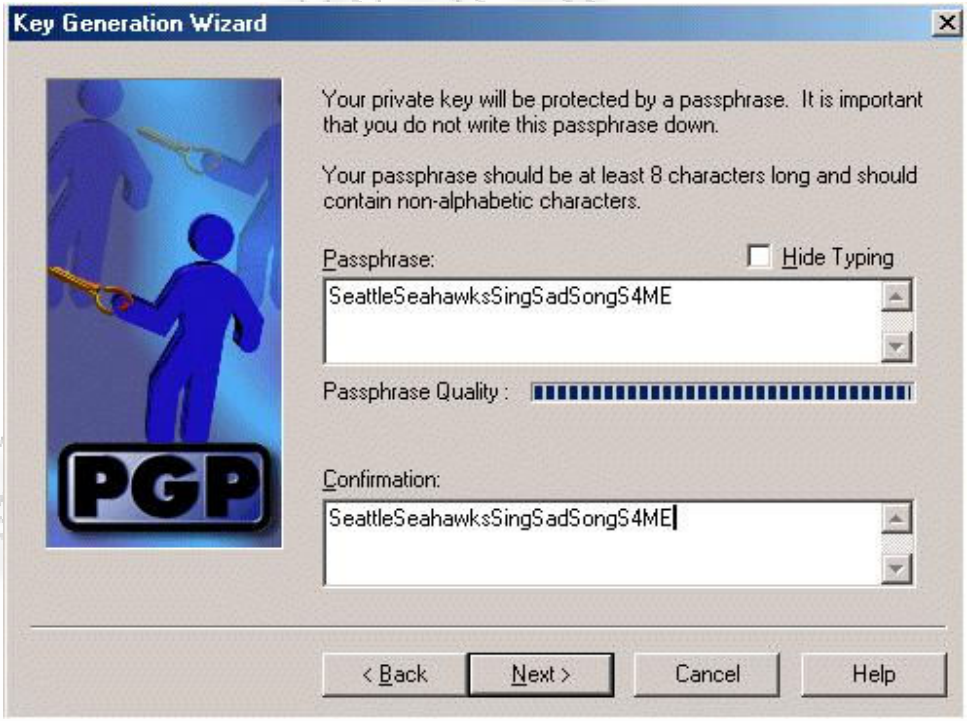
- Ο Α γνωρίζει εκ των προτέρων το δημόσιο κλειδί του Β
- Ο Α κρυπτογραφεί το μήνυμα με τη χρήση κάποιου αλγορίθμου (CAST, tripleDES, IDEA) και ένα (ψευδο)τυχαίο κλειδί που δημιούργησε
- Ο Α κρυπτογραφεί το κλειδί που χρησιμοποίησε για να κρυπτογραφήσει το μήνυμα με τη χρήση π.χ. RSA
- Ο Α μπορεί να υπογράψει ψηφιακά το μήνυμα χρησιμοποιώντας τον αλγόριθμο RSA

Όταν ο Β παραλάβει το μήνυμα:

- Επιβεβαιώνει την ψηφιακή υπογραφή του Α με το δημόσιο κλειδί του Α, το οποίο είτε έχει, είτε μπορεί να το βρει από ένα key ring (τοποθεσίες στο web, όπου κάποιος μπορεί να ανακτήσει τα δημόσια κλειδιά ή πιστοποιητικά των χρηστών PGP)
- Ο Β, χρησιμοποιώντας το ιδιωτικό του κλειδί, αποκρυπτογραφεί το συμμετρικό κλειδί που χρησιμοποίησε ο Α για να κρυπτογραφήσει το μήνυμα
- Με το συμμετρικό κλειδί αυτό, ο Β αποκρυπτογραφεί και διαβάζει το αρχικό μήνυμα



Εικόνα 10: Δημιουργία κλειδιών με το PGP

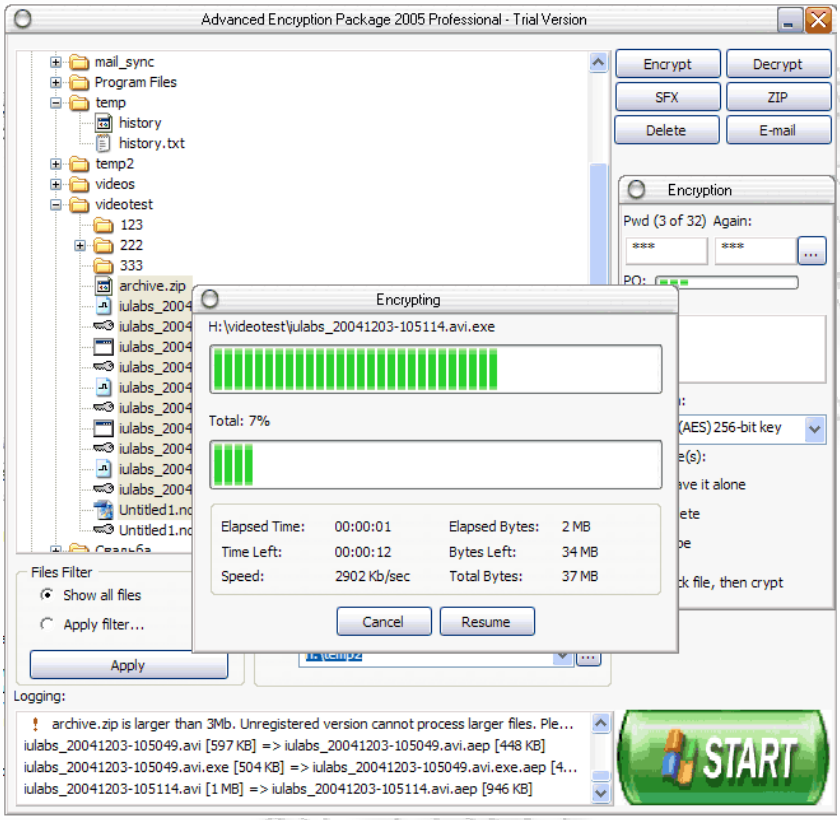


Εικόνα 11: Προστασία κλειδιών με μυστική φράση στο PGP

Εικόνα 12: Επιτυχής δημιουργία κλειδιών και αποστολή στο key ring

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.



Εικόνα 13: Κρυπτογράφηση Αρχείων στο AEP

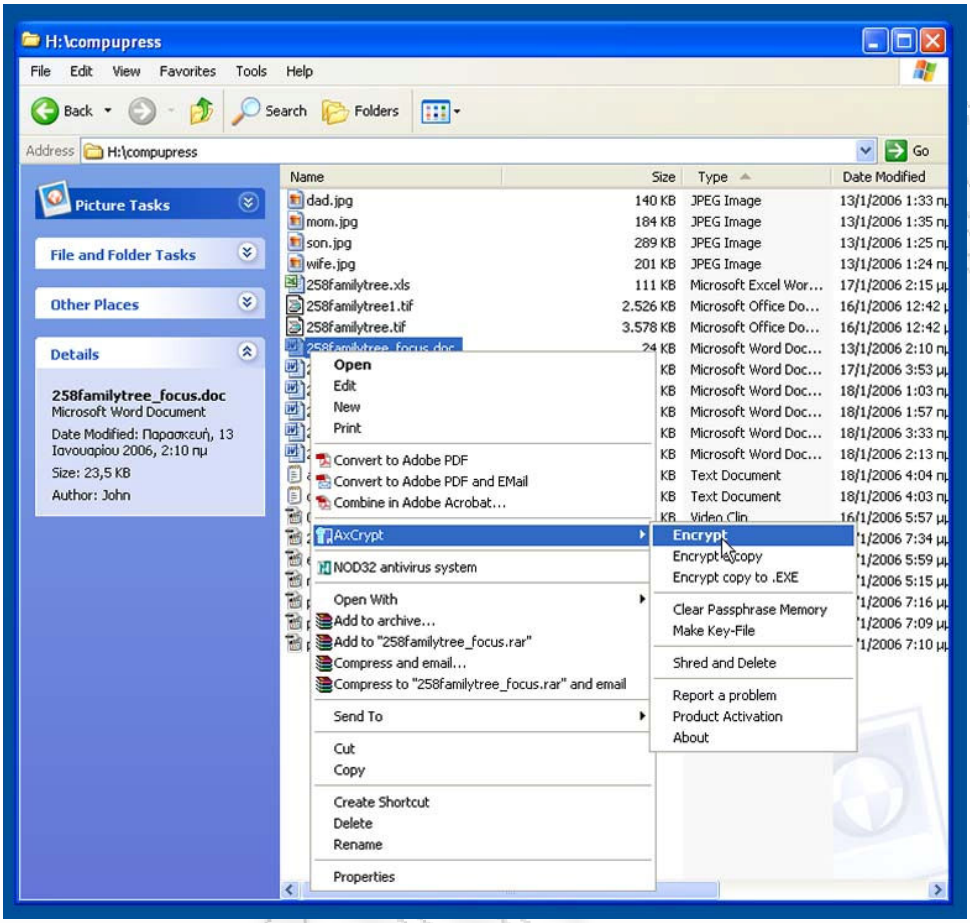
4.1.3 Advanced File Security

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.

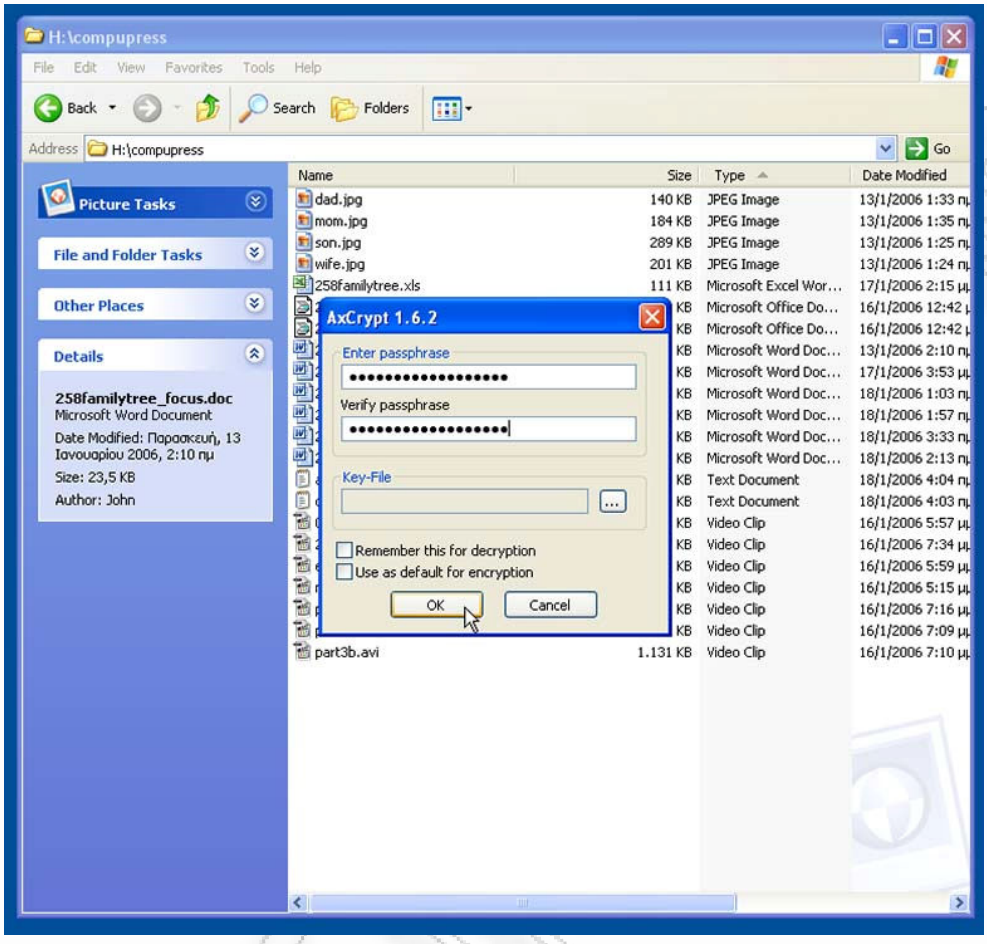
Εικόνα 24: Κρυπτογράφηση με Advanced File Security

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



Εικόνα 35: Επιλογή αρχείου για κρυπτογράφηση με AxCrypt



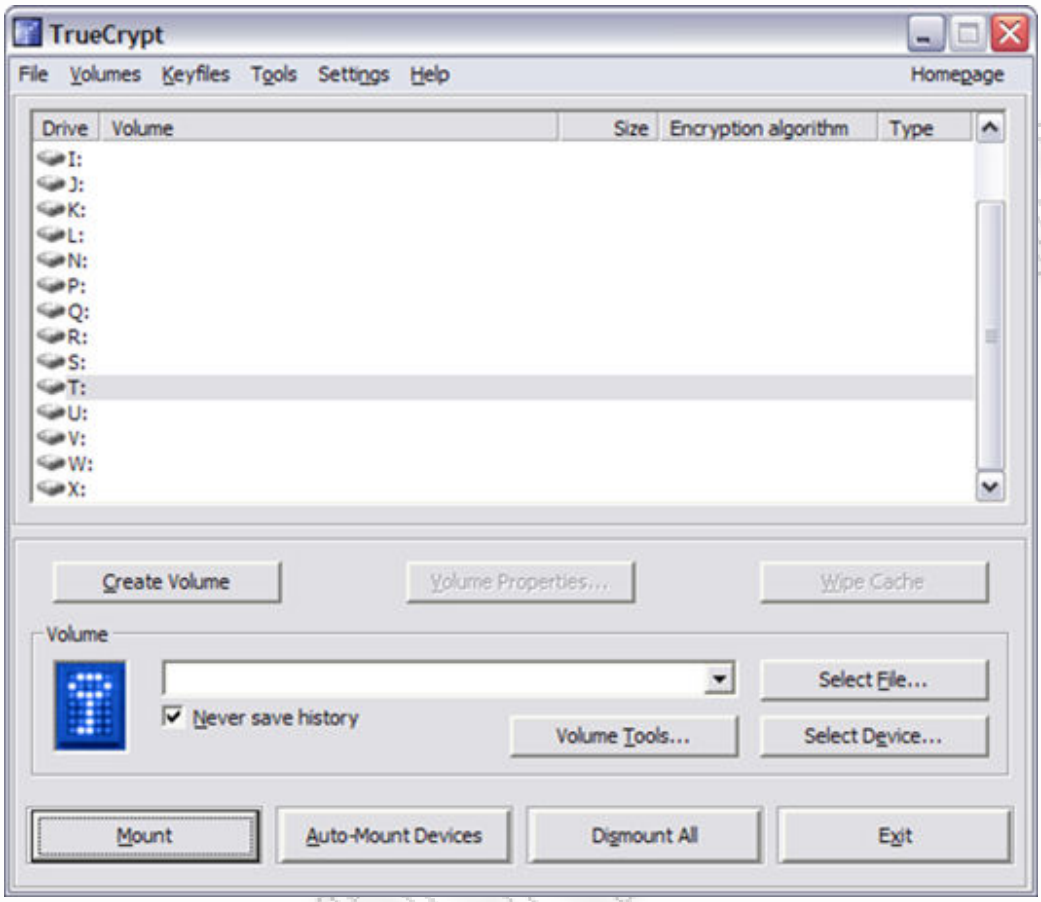
Εικόνα 46: Εισαγωγή μυστικής φράσης – κλειδί στο AxCrypt

4.1.5 TrueCrypt

Εφαρμογή για τη δημιουργία εικονικών κρυπτογραφημένων δίσκων στον υπολογιστή. Οτιδήποτε αποθηκεύεται στον εικονικό δίσκο κρυπτογραφείται αυτόματα. Με το πρόγραμμα TrueCrypt υπάρχει δυνατότητα δημιουργίας ενός κρυπτογραφημένου αρχείου σε οποιοδήποτε αποθηκευτικό μέσο (σκληρός δίσκος, cdrom, δισκέτα, usb memory stick κ.α.) που εμφανίζεται στο σύστημα σαν ένας επιπλέον δίσκος. Όσο ο δίσκος αυτός είναι συνδεδεμένος, τα αρχεία που βρίσκονται εκεί διαβάζονται, αντιγράφονται, αποθηκεύνται, όπως θα γινόταν σε οποιοδήποτε δίσκο. Το σύστημα από μόνο του αναλαμβάνει να τα

κρυπτογραφεί και αποκωδικοποιεί κατά περίπτωση. Τη στιγμή που θα αποσυνδεθεί αυτός ο εικονικός δίσκος, τα δεδομένα δεν μπορούν πια να διαβαστούν. Και κάθε φορά που κλείνει ο υπολογιστής, ο δίσκος αυτός αποσυνδέεται. Για να συνδεθεί πάλι ο δίσκος αυτός, απαιτείται η εισαγωγή του κωδικού.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.

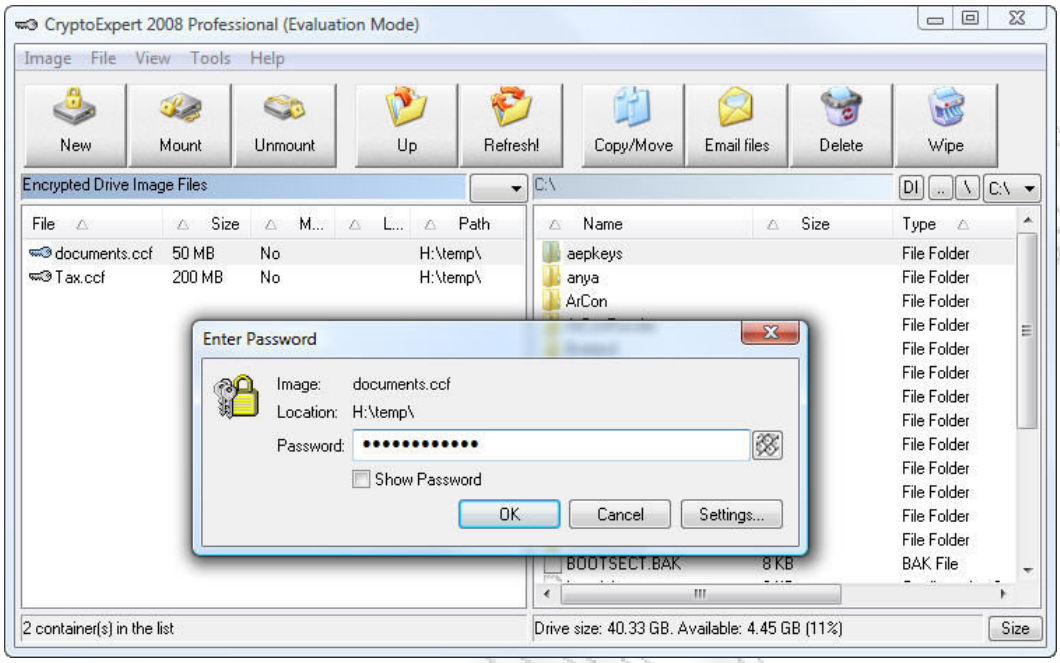
Ακόμα και τα περιεχόμενα ενός email μπορούν να κρυπτογραφηθούν με αυτόν τον τρόπο. Δημιουργείται ένα μικρό κρυπτογραφημένο αρχείο (πχ. μεγέθους 300kb) με το TrueCrypt, στο οποίο εισάγουμε για παράδειγμα ένα αρχείο(πχ. μεγέθους 200kb). Μπορούμε μετά να εισάγουμε το κρυπτογραφημένο αρχείο-δίσκο των 300kb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



Εικόνα 57: Κρυπτογράφηση Δίσκων με το TrueCrypt

4.1.6 CryptoExpert

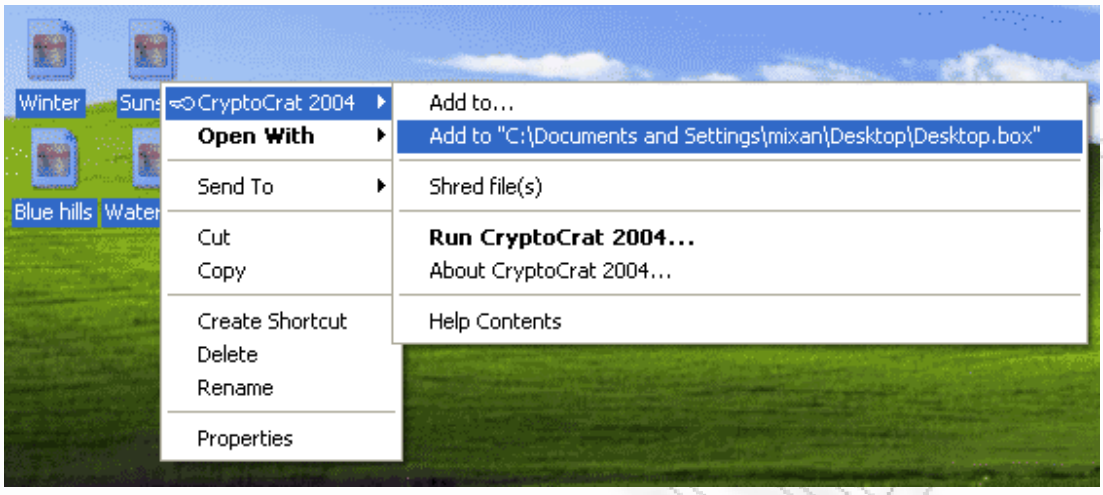
Εφαρμογή κρυπτογράφησης που δίνει τη δυνατότητα δημιουργίας μιας σειράς από εικονικούς κρυπτογραφημένους δίσκους για την ασφαλή αποθήκευση των αρχείων. Η κρυπτογράφηση γίνεται σε περιβάλλον 128bit.



Εικόνα 68: Κρυπτογράφηση Δίσκων με το CryptoExpert

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.



Εικόνα 19: Επιλογή αρχείων προς κρυπτογράφηση με το CryptoCrat

4.1.8 Άλλα Προγράμματα Κρυπτογράφησης

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 Λογισμικό Υδατογράφησης

Παρά το γεγονός πως η τεχνολογία της υδατογράφησης και τα συστήματα που έχουν αναπτυχθεί γύρω από αυτή είναι ακόμα σε πρώιμη φάση, υπάρχει ένας σημαντικός αριθμός από εταιρείες λογισμικού που έχουν προχωρήσει στο σχεδιασμό και την ανάπτυξη εφαρμογών υδατογράφησης. Ωστόσο, ακόμα και στην περίπτωση που οι προδιαγραφές των συστημάτων είναι κοινές, τα προϊόντα που προτείνονται από δύο διαφορετικές εταιρείες παρουσιάζουν σημαντικές διαφορές. Στη συνέχεια θα πραγματοποιηθεί μία συνοπτική αναφορά στα κυριότερα, εμπορικά διαθέσιμα προϊόντα.

Ακολουθεί μια συνοπτική περιγραφή των κυριότερων προϊόντων, ανά κατηγορία περιεχομένου. Ο στόχος της περιγραφής δεν είναι να αξιολογήσει συγκριτικά τα διαθέσιμα συστήματα, αλλά να αναδείξει μερικά από τα επιμέρους λειτουργικά και τεχνικά χαρακτηριστικά τους.

4.2.1 Ψηφιακή Υδατογράφηση Αρχείων Εικόνας

Η υδατογράφηση ψηφιακών εικόνων είναι χωρίς αμφιβολία ο πιο ώριμος από τους επιμέρους τομείς της υδατογραφίας, καθώς η προστασία των εικόνων ήταν η κινητήρια δύναμη που οδήγησε στην ανάπτυξη και την εξάπλωση των ψηφιακών υδατογραφημάτων. Η ψηφιακή εικόνα έχει γίνει αντικείμενο εκτεταμένης έρευνας και μελέτης, με αποτέλεσμα η πλειοψηφία των αλγόριθμων υδατογράφησης που απαντώνται στην βιβλιογραφία να αναφέρονται στην προστασία φωτογραφιών. Στην πραγματικότητα, ακόμα και οι αλγόριθμοι που προτείνονται για την ψηφιακή υδατογράφηση ψηφιακών αρχείων ήχου ή βίντεο, είναι τις περισσότερες φορές παραλλαγές των αλγόριθμων εικόνας. Η ωριμότητα της υδατογράφησης στο συγκεκριμένο τομέα αντικατοπτρίζεται, όπως μαρτυράει και ο παραπάνω πίνακας, στον μεγάλο αριθμό των σχετικών προϊόντων που είναι

διαθέσιμα στην αγορά. Συγκεκριμένα, μερικές από τις εταιρείες που παρουσιάζουν αξιοσημείωτη δραστηριότητα στο χώρο της υδατογράφησης εικόνας είναι οι ακόλουθες:

4.2.1.1 Alpha Tec Ltd

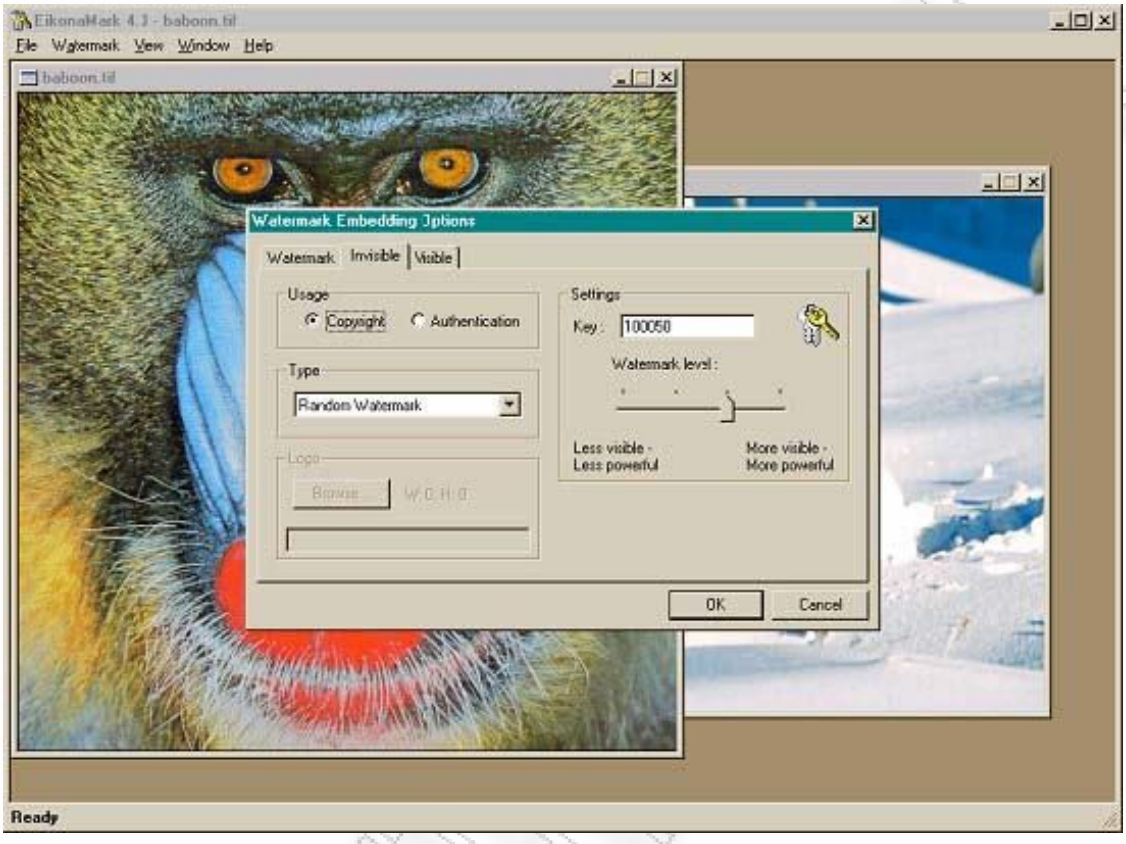
Η Alpha Tec. είναι μια εταιρεία που εδρεύει στην Ελλάδα και έχει ως αντικείμενο την Έρευνα & Ανάπτυξη εξειδικευμένων εφαρμογών για ψηφιακές εικόνες / βίντεο και πολυμέσα. Ιδρύθηκε το 1989 και έχει να επιδείξει αξιοσημείωτη δραστηριότητα, καθώς και μία σημαντική αλυσίδα προϊόντων στον τομέα της. Στο χώρο της ψηφιακής υδατογράφησης εικόνων η Alpa Tec. προτείνει το EikonaMark.

EikonaMark:

Αποτελεί ένα εξειδικευμένο προϊόν λογισμικού για την ενσωμάτωση και την ανίχνευση "ορατών" & "αόρατων" υδατογραφημάτων στο ψηφιακό περιεχόμενο των εικόνων. Οι ψηφιακές υπογραφές που κωδικοποιούνται σε ηλεκτρονικά αρχεία, μπορούν να χρησιμοποιηθούν για την προστασία του copyright και την πιστοποίηση της ιδιοκτησίας των εικόνων που τις φέρουν. Ο κάτοχος των δικαιωμάτων μιας εικόνας μπορεί να χρησιμοποιήσει το EikonaMark για να αποκρύψει στο περιεχόμενο της ένα μοναδικό αριθμό, ενδεικτικό της ιδιοκτησίας του επί του ψηφιακού έργου. Στη συνέχεια μπορεί να αποδείξει την ιδιοκτησία του σε μια ενδεχόμενη διαμάχη, ανιχνεύοντας τον παραπάνω ενδεικτικό αριθμό με τη μορφή υδατογραφήματος. Η δυνατότητα τοποθέτησης ορατών υδατογραφημάτων είναι επίσης χρήσιμη για την προστασία των πνευματικών δικαιωμάτων ψηφιακού περιεχομένου, ιδιαίτερα στην περίπτωση δημοσιοποίησής του στο Διαδίκτυο. Η υδατογράφηση των εικόνων που προβάλλονται στο Διαδίκτυο με ορατά υδατογραφήματα, μπορεί να αποτρέψει τους επισκέπτες από τη χρησιμοποίησή τους με αθέμιτο τρόπο. Μερικά από τα πιο σημαντικά τεχνικά & λειτουργικά χαρακτηριστικά του Eikonamark είναι συνοπτικά τα εξής:

- Τα υδατογραφήματα μπορούν να είναι ορατά ή αόρατα. Τα αόρατα υδατογραφήματα επιτυγχάνουν μεγάλο βαθμό διαφάνειας και σε καμία περίπτωση δεν γίνονται αντιληπτά από το ανθρώπινο σύστημα όρασης.
- Η ανίχνευση ή η απομάκρυνση των υδατογραφημάτων από ένα μη εξουσιοδοτημένο χρήστη είναι εξαιρετικά δύσκολη
- Υποστηρίζει την "τυφλή - μη ενημερωμένη ανίχνευση" καθώς η αρχική μη υδατογραφημένη εικόνα δεν χρησιμοποιείται κατά τη διαδικασία της ανίχνευσης.
- Υπάρχει η δυνατότητα επιλογής ανάμεσα σε zero-bit & multi-bit υδατογραφήματα. Είναι εφικτή δηλαδή η άρρηκτη διασύνδεση ψηφιακών εικόνων και μοναδικών αναγνωριστικών με τη χρήση αόρατων υδατογραφημάτων.
- Επιτυγχάνει ανθεκτικότητα σε μια μεγάλη ποικιλία από επιθέσεις. Τα υδατογραφήματα που χρησιμοποιούνται από το Eikonamark παραμένουν ανιχνεύσιμα ακόμα και μετά την εφαρμογή εξειδικευμένων επιθέσεων όπως είναι, η JPEG συμπίεση, οι επιθέσεις επεξεργασίας σήματος, οι γεωμετρικές επιθέσεις κ.α.
- Οι υπηρεσίες υδατογράφησης που προσφέρει το EikonaMark είναι διαθέσιμες στον χρήστη αφενός μέσω μιας εύχρηστης παραθυρικής διεπαφής που υποστηρίζει επιπλέον την μαζική υδατογράφηση εικόνων και αφετέρου μέσω μιας πλατφόρμας ανάπτυξης λογισμικού (SDK) για την εύκολη και αποτελεσματική ενσωμάτωση της υδατογράφησης σε ένα ήδη υπάρχον πληροφοριακό σύστημα επεξεργασίας εικόνων.
- Υποστηρίζει όλους τους βασικούς τύπου δεδομένων ψηφιακών αρχείων εικόνας όπως, TIFF, JPEG, GIF, BMP, TARGA κ.α

Η λειτουργικότητα του EikonaMark στην προσπάθεια προστασίας των πνευματικών δικαιωμάτων ψηφιακών αρχείων εικόνας και τον εντοπισμό παράνομων χρήσεων στο Διαδίκτυο, συμπληρώνεται από έναν αυτοματοποιημένο πράκτορα (agent). Η λειτουργία του είναι να εντοπίζει και να αναφέρει τις περιπτώσεις όπου λαμβάνει χώρα παράνομη χρήση εικόνας.



Εικόνα 20 : Δημιουργία Υδατογραφήματος στο EikonaMark

Alphacrawler:

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. Αποκλειστικός σκοπός του Alphacrawle*r* είναι η σάρωση των εικόνων ενός διαδικτυακού τόπου, με αφετηρία ένα URL. Ο μηχανισμός εξετάζει, για παρουσία υδατογραφημάτων, όλα τα αρχεία εικόνας που φιλοξενούνται σε μια διαδικτυακή σελίδα. Ο έλεγχος συνεχίζεται σε δεύτερο επίπεδο σε όλες τις διαδικτυακές σελίδες που αναφέρονται από την τρέχουσα. Το βάθος αναζήτησης καθορίζεται από τον χρήστη. Το αποτέλεσμα της αυτοματοποιημένης αναζήτησης είναι μια αναφορά που περιέχει τις ηλεκτρονικές διευθύνσεις των σελίδων που ελέγχθηκαν

και μια συμπληρωματική αναφορά που περιέχει μόνο τις ηλεκτρονικές διευθύνσεις των σελίδων που περιείχαν υδατογραφημένες εικόνες.

4.2.1.2 Digimarc

Οι λύσεις που προτείνονται από τη Digimarc σε ότι αφορά την προστασία ψηφιακού περιεχομένου, στηρίζονται σχεδόν αποκλειστικά στην τεχνολογία της υδατογράφησης. Η Digimarc είναι μία από τις πλέον δραστήριες εταιρείες στο χώρο της ψηφιακής υδατογράφησης και τα προϊόντα που προτείνει αποσκοπούν στην προστασία, την διαχείριση και τον εντοπισμό των ψηφιακών και έντυπων φωτογραφιών. Τα προϊόντα και οι εφαρμογές λογισμικού της Digimarc έχουν διεισδύσει σε σημαντικό βαθμό στη βιομηχανία της αξιοποίησης ψηφιακού περιεχομένου και αποτελούν μια αξιόπιστη λύση για κάθε πολιτιστικό οργανισμό που επιθυμεί να αποκτήσει ψηφιακό προφίλ χωρίς να χάσει το έλεγχο της πνευματικής του ιδιοκτησίας. Η παρουσία της Digimarc στην αγορά της προστασίας των πνευματικών δικαιωμάτων εκφράζεται με τα ακόλουθα προϊόντα:

ImageBridge:

Πρόκειται για το πιο διάσημο από τα προϊόντα της Digimarc. Ο ρόλος του είναι να τοποθετεί και να ανιχνεύει ανθεκτικά υδατογραφήματα στο ψηφιακό περιεχόμενο των εικόνων που θέλει να προστατέψει. Η λειτουργία των υδατογραφημάτων έγκειται στην πιστοποίηση της ιδιοκτησίας και την άμεση διασύνδεση μιας εικόνας με τα μεταδεδομένα που αφορούν τον κάτοχο των δικαιωμάτων και τους περιορισμούς χρήσεις. Ανάμεσα στις λειτουργικές & τεχνικές προδιαγραφές του ImageBridge συγκαταλέγονται και οι ακόλουθες:

- **Προσαρμοστικότητα:** Το ImageBridge μπορεί να ενσωματωθεί με αρκετούς τρόπους στο λειτουργικό μοντέλο παραγωγής και αξιοποίησης ψηφιακού υλικού. Μπορεί να χρησιμοποιηθεί με τη μορφή ενός plug-in που είναι

συμβατό με τις σημαντικότερες εφαρμογές διαχείρισης και επεξεργασίας εικόνας, όπως τα προϊόντα της Adobe, Corel κ.α.

• **Μεταφερσιμότητα:** Οι υπηρεσίες του ImageBridge διατίθενται μέσω μιας πλατφόρμας ανάπτυξης λογισμικού (SDK – Software Development Kit), παρέχοντας στον οργανισμό τη δυνατότητα να ενσωματώσει αποτελεσματικά την υπηρεσία της υδατογράφησης στο πληροφοριακό σύστημα που χρησιμοποιεί.

• **Αδιορατότητα:** Ως προς την αδιορατότητα και την ανθεκτικότητα των υδατογραφημάτων που χρησιμοποιούνται από το ImageBridge, το εργαλείο υποστηρίζει αρκετά διαφορετικά επίπεδα στάθμισης. Ωστόσο, σε γενικές γραμμές τα υδατογραφήματα που χρησιμοποιούνται πληρούν σε ικανοποιητικό βαθμό την προδιαγραφή της αδιορατότητας.

• **Τυφλή – Μη ενημερωμένη ανίχνευση:** Η ανίχνευση του υδατογραφήματος πραγματοποιείται χωρίς να είναι απαραίτητη η παρουσία της αρχικής μη υδατογραφημένης εικόνας ικανοποιώντας την απαίτηση για τυφλή ανίχνευση των υδατογραφημάτων.

• **Διαλειτουργικότητα:** Υποστηρίζονται όλοι οι βασικοί τύποι αρχείων εικόνας.

• **Multi-bit Υδατογραφήματα:** Παρέχεται η δυνατότητα ενσωμάτωσης multibit υδατογραφημάτων που μπορούν να αξιοποιηθούν ανάλογα με τις ανάγκες του οργανισμού. Το πεδίο τιμών κυμαίνεται από 1 έως 16777215 όταν αντιστοιχεί στο "ImageID" ή στο "TransactionID". Η τρίτη επιλογή είναι το Copyright Year και συμπληρώνεται με την κατάλληλη χρονολογία.

• **Ανθεκτικότητα:** Η ανθεκτικότητα των υδατογραφημάτων της Digimarc είναι ικανοποιητική, καθώς παραμένουν ανιχνεύσιμα ακόμα και μετά την εφαρμογή ενός αρκετά μεγάλου συνόλου επιθέσεων, όπως συμπίεση, επεξεργασία σήματος, γεωμετρικοί μετασχηματισμοί κ.α.

Η λειτουργικότητα που προσφέρει το συγκεκριμένο προϊόν συμπληρώνεται από μία εξειδικευμένη εφαρμογή, υπεύθυνη για την ανίχνευση των υδατογραφημάτων. Ο ImageBridge Reader όπως ονομάζεται, αξιοποιεί τον μηχανισμό ανίχνευσης του ImageBridge και παρέχει μία αυτοματοποιημένη εφαρμογή για τη σάρωση των ψηφιακών εικόνων και την ανίχνευση των υδατογραφημάτων που ενδεχομένως να περιέχουν. Η λειτουργικότητα της εφαρμογής υποστηρίζεται από ένα ειδικό plug-in που μπορεί να ενσωματωθεί σε μια σειρά από προϊόντα όπως, το Adobe Photoshop, JASC Paintshop Pro, ULead Photo Impact ή ακόμα και τον Internet & Windows Explorer της Microsoft. Στην περίπτωση του Internet Explorer το plug-in της Digimarc εξετάζει τις εικόνες που φιλοξενούνται από τη διαδικτυακή σελίδα που επισκέπτεται ο χρήστης και τον ειδοποιεί σε περίπτωση που ανιχνευθεί κάποιο γνωστό υδατογράφημα. Αντίστοιχη είναι η λειτουργία του plug-in και στο Windows Browser, όπου πραγματοποιείται η εξέταση όλων των εικόνων που περιέχονται σε έναν φάκελο.

Η τελευταία από τις υπηρεσίες που παρέχεται από το ImageBridge και βασίζεται την τεχνολογία της υδατογράφησης είναι η διασύνδεση της ψηφιακής εικόνας με τα μεταδεδομένα της. Η επιτυχημένη ανίχνευση ενός υδατογραφήματος της Digimarc, καταδεικνύεται από μία χαρακτηριστική ένδειξη που εμφανίζεται στην κάτω δεξιά γωνία της εικόνας. Το σημάδι εκτός από ενδεικτικό της ύπαρξης του υδατογραφήματος λειτουργεί ταυτόχρονα και σαν link, που οδηγεί τον χρήστη σε ένα σύνολο από πληροφορίες, σχετικές με το περιεχόμενο του υδατογραφήματος που ενυπάρχει στη συγκεκριμένη φωτογραφία. Οι πληροφορίες αφορούν συνήθως τον κάτοχο των δικαιωμάτων, ενώ συμπληρωματικές διαδικτυακές αναφορές ενδέχεται να οδηγούν σε επιπρόσθετα δεδομένα για την εικόνα.

Επιπλέον, το ImageBridge συνοδεύεται με μία ακόμα αυτοματοποιημένη εφαρμογή που αξιοποιεί το μηχανισμό ανίχνευσης υδατογραφημάτων. Η λειτουργία της εφαρμογής είναι να σαρώνει το Διαδίκτυο με σκοπό την ανίχνευση παράνομων χρήσεων ψηφιακών εικόνων. Συγκεκριμένα, το **MarcSpider** παρέχει αυτοματοποιημένες υπηρεσίες ανίχνευσης των εικόνων που προστατεύονται με copyright, χρησιμοποιώντας ως σημείο εκκίνησης ένα συγκεκριμένο URL. Ως εναλλακτική λειτουργία υπάρχει η δυνατότητα σάρωσης του Διαδικτύου με άπληστο τρόπο, με στόχο την ανεύρεση των υδατογραφημάτων της Digimarc. Την εξαντλητική έρευνα του διαδικτύου ακολουθεί μία αναλυτική αναφορά των αποτελεσμάτων της αναζήτησης. Ο κάτοχος των δικαιωμάτων μπορεί να χρησιμοποιήσει τα αποτελέσματα της αναφοράς, για να διαπιστώσει σε ποιες ιστοσελίδες πραγματοποιείται παράνομη χρήση των ψηφιακών του εικόνων.

4.2.1.3 MarkAny

Η MarkAny είναι μία εταιρεία με έδρα την Κορέα και αντικείμενο την προστασία και διαχείριση των δικαιωμάτων πνευματικής ιδιοκτησίας ψηφιακού υλικού. Παρουσιάζει έντονη δραστηριότητα στο χώρο των DRM συστημάτων και αξιοποιεί όλα τα διαθέσιμα μέσα για την αποτελεσματική προστασία και διαχείριση των δικαιωμάτων πνευματικής ιδιοκτησίας. Σε αυτό το πλαίσιο, η εταιρεία προτείνει ορισμένες λύσεις για την ψηφιακή υδατογράφηση εικόνων, με στόχο τη χρήση τους κατά την εφαρμογή των πολιτικών προστασίας και διαχείρισης δικαιωμάτων. Συγκεκριμένα το προϊόν που διατίθεται εμπορικά από την MarkAny είναι το MAIM 2.0:

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. Τα λειτουργικά χαρακτηριστικά της εφαρμογής είναι τα ακόλουθα:

• Αυξημένη ανθεκτικότητα έναντι της συμπίεσης και των λοιπών επιθέσεων επεξεργασίας εικόνας

• Υδατογραφήματα πολλαπλών bit ώστε να υποστηρίζεται η κωδικοποίηση μεγάλου εύρους ακέραιων αριθμών στο περιεχόμενο των εικόνων

• Λειτουργίες μαζικής υδατογράφησης εικόνων και αυτοματοποιημένης ανίχνευσης των υδατογραφημάτων

• Η τεχνολογία της υδατογράφησης είναι διαθέσιμη στον τελικό χρήση είτε μέσω μιας φιλικής διεπαφής, είτε μέσω της πλατφόρμας ανάπτυξης λογισμικού (SDK).

• Υποστηρίζει BMP, JPEG, PNG, GIF & TIFF ψηφιακά αρχεία εικόνας

4.2.1.4 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. Τα προϊόντα της MediaSec υποστηρίζουν εφαρμογές, όπως η προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας, η πιστοποίηση της αυθεντικότητας πολυμεσικού υλικού, η διασφάλιση της αυθεντικότητας ηλεκτρονικών και έντυπων εγγράφων και η παρεμπόδιση της πλαστογραφίας, της παραποίησης και της αντιγραφής.

Σε πλήρη συμφωνία με τις βασικές αρχές της ψηφιακής υδατογράφησης, η MediaSec χρησιμοποιεί την εν λόγω τεχνολογία για την απόκρυψη πληροφορίας στο ψηφιακό περιεχόμενο των αντικειμένων. Τα δεδομένα είναι αόρατα για το ανθρώπινο σύστημα όρασης και ανιχνεύονται μόνο από το ειδικό λογισμικό της

εταιρείας. Η διαδικασία της κωδικοποίησης και της αποκωδικοποίησης του υδατογραφήματος στηρίζεται σε ένα μυστικό κλειδί που προσθέτει ένα επιπλέον επίπεδο ασφάλειας στην πολιτική προστασίας του οργανισμού. Από τα προϊόντα που διατίθενται εμπορικά, αυτό που αφορά ψηφιακές εικόνες είναι το MediaSign Digital.

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. Μία σειρά από κατάλληλα δεδομένα που ενσωματώνονται στο ψηφιακό περιεχόμενο μιας εικόνας ή των διαδοχικών καρέ ενός αρχείου βίντεο, είναι ικανά να καταδείξουν το νόμιμο ιδιοκτήτη τους. Οι λειτουργικές προδιαγραφές του MediaSec Digital είναι οι ακόλουθες:

Ασφάλεια:

• Ενσωματώνει στο ψηφιακό αντικείμενο μία ηλεκτρονική υπογραφή με τη μορφή timestamp.

• Σημαντικές πληροφορίες όπως είναι το απεικονιζόμενο αντικείμενο, η ημερομηνία και η ώρα ψηφιοποίησης, ενσωματώνονται στο ψηφιακό περιεχόμενο των εικόνων με τη μορφή υδατογραφημάτων

• Τα ψηφιακά υδατογραφήματα είναι αόρατα για το ανθρώπινο σύστημα όρασης.

Εύκολη και συμφέρουσα ενσωμάτωση:

• Η επιβεβαίωση της ύπαρξης των ψηφιακών υδατογραφημάτων είναι πλήρως αυτοματοποιημένη

• Υποστηρίζονται οι βασικοί τύποι ψηφιακών αρχείων

• Δεν είναι αναγκαία η αναδιάρθρωση του λειτουργικού μοντέλου που χρησιμοποιεί ο οργανισμός, καθώς το MediaSec μπορεί να ενσωματωθεί εύκολα σε μία ήδη υπάρχουσα εφαρμογή επεξεργασίας εικόνων

Δεν απαιτείται κανένα επιπλέον κόστος σε εξοπλισμό

4.2.1.5 Sealtronic

Η Sealtronic όπως και η MarkAny είναι μια εταιρεία που εδρεύει στην Κορέα και δραστηριοποιείται στο χώρο της αξιοποίησης ψηφιακού υλικού. Όλες οι προσπάθειες της εταιρείας είναι προσανατολισμένες στην ασφάλεια και την προστασία της αξίας που φέρει η πληροφορία σε περιβάλλοντα ψηφιακής πραγματικότητας. Προτεραιότητα των τεχνολογικών λύσεων που προτείνονται είναι η εξασφάλιση της ασφαλούς διανομής του ψηφιακού περιεχομένου, η προστασία των πνευματικών του δικαιωμάτων και η μεγιστοποίηση της παραγωγικότητας της βιομηχανίας που το εκμεταλλεύεται.

Η οικογένεια των προϊόντων που προτείνει η εταιρεία για την αντιμετώπιση του προβλήματος της προστασίας του δικαιώματος αναπαραγωγής, φέρει το όνομα MagicTag και χρησιμοποιεί την τεχνολογία της υδατογράφησης για την απόκρυψη πληροφορίας σε περιοχές του ψηφιακού περιεχομένου που δεν γίνονται αντιληπτές από το ανθρώπινο σύστημα αισθήσεων. Ο στόχος της οικογένειας των προϊόντων MagicTag είναι να παρέχουν στους κατόχους του περιεχομένου ένα τεχνολογικό μέσο, που θα υποστηρίζει υπηρεσίες ασφάλειας, όπως η πιστοποίηση της ιδιοκτησίας του copyright, η απόδειξη μη εξουσιοδοτημένης χρήσης, η παροχή συγκεκριμένων δικαιωμάτων σε έναν εγκεκριμένο χρήστη και η μετάδοση εμπιστευτικής πληροφορίας. Το προϊόν της οικογένειας MagicTag που προτείνεται για την προστασία των πνευματικών δικαιωμάτων ψηφιακών εικόνων είναι το MT Image.

MT Image: Το MT Image ενσωματώνει ανθεκτικά αόρατα υδατογραφήματα στα pixels μιας ψηφιακής εικόνας. Ανάμεσα στις λειτουργικές προδιαγραφές του MT Image περιλαμβάνονται τα ακόλουθα:

• Αυξημένη ανθεκτικότητα σε επιθέσεις, όπως συμπίεση, αλλαγή της κλίμακας μεγέθους, περιστροφή, αποκοπή κ.α.

• Διάθεση των λειτουργιών που προσφέρει η προτεινόμενη μέθοδος υδατογραφίας, με τη μορφή μιας ολοκληρωμένης πλατφόρμας ανάπτυξης λογισμικού (SDK).

• Η αρχική μη υδατογραφημένη εικόνα δεν είναι απαραίτητη κατά τη διαδικασία της ανίχνευσης. (Τυφλή - Μη ενημερωμένη ανίχνευση).

• Δυνατότητα ενσωμάτωσης multi-bit υδατογραφημάτων στο ψηφιακό περιεχόμενο των εικόνων για την κωδικοποίηση ακέραιων αριθμών.

4.2.1.6 Signum Technologies

Η εταιρεία Signum Technologies δραστηριοποιείται στην αγορά την προστασίας των πνευματικών δικαιωμάτων με μία σημαντική αλυσίδα από προϊόντα. Η τεχνολογία της υδατογραφίας είναι η πλατφόρμα στην οποία στηρίζονται τα προϊόντα της Signum για την προστασία του copyright. Ο στόχος της Signum είναι να υποστηρίξει την πολιτική ασφαλείας των οργανισμών, που έχουν στην κατοχή τους και εκμεταλλεύονται εμπορικά, μεγάλης αξίας ψηφιακό περιεχόμενο. Σε αυτές τις περιπτώσεις, η άρρηκτη διασύνδεση των υδατογραφημάτων με τα ψηφιακά αντικείμενα, καθιστά δυνατή την εποπτεία των εικόνων που δημοσιοποιούνται στο Διαδίκτυο, αντιστοιχίζοντάς τες με τις πληροφορίες που αφορούν τα πνευματικά τους δικαιώματα. Ανάμεσα στους καταναλωτές των προϊόντων της Signum συγκαταλέγονται τα μουσεία, τα φωτογραφικά αρχεία, οι φωτογράφοι, οι εκδότες κ.α. 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. Με αντίστοιχο τρόπο υλοποιείται και η διαδικασία της ανίχνευσης, όπου η εφαρμογή δέχεται ως είσοδο έναν φάκελο με εικόνες και καταγράφει σε ένα αρχείο κειμένου τα αποτελέσματα της διαδικασίας. Πρόκειται για το προϊόν της εταιρείας που ενσωματώνει τη λειτουργικότητα της υδατογράφησης μέσα σε μια εύχρηστη παραθυρική εφαρμογή.

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.

Τα plug-ins της Suresign χρησιμοποιούν ως ξενιστές τα πλέον διαδεδομένα λογισμικά επεξεργασίας εικόνας της Adobe και της Corel, καθώς και τον Windows Explorer της Microsoft, όπου εμφανίζονται με τη μορφή ενός επιπλέον tab στη επιλογή "Ιδιότητες" των αρχείων εικόνας.

Τα λειτουργικά χαρακτηριστικά των προϊόντων της Signum είναι τα ακόλουθα:

• Η διαβάθμιση της προσδοκώμενης ανθεκτικότητας έχει 5 κλίμακες και μπορούμε να θεωρήσουμε πως η αλλοίωση που υφίσταται η εικόνα ακόμα και στην επιλογή για μέγιστη ανθεκτικότητα δεν γίνεται αντιληπτή από το ανθρώπινο σύστημα αισθήσεων

• Ο μηχανισμός ανίχνευσης είναι "τυφλός", καθώς ολοκληρώνει τη διαδικασία χωρίς να χρησιμοποιεί την αρχική εικόνα, ενώ υποστηρίζονται

ψηφιακά αρχεία εικόνας τύπου JPEG, TIFF, BMP, PCX, PNG, Targa και PICT - RGB, CMYK ή greyscale

• Η μορφή των υδατογραφημάτων που χρησιμοποιούνται από τα παραπάνω προϊόντα είναι της μορφής "AANNNNN", όπου A είναι κάποιος αλφαριθμητικός χαρακτήρας και N είναι ένα αριθμητικό ψηφίο. Οι αλφαριθμητικοί χαρακτήρες χρησιμοποιούνται για τη λειτουργία του μηχανισμού ενσωμάτωσης, ενώ οι αριθμητικοί χαρακτήρες είναι κατάλληλοι για να διασυνδέσουν μοναδικά ένα ψηφιακό αντικείμενο με έναν ακέραιο αριθμό

• Ικανοποιητική κρίνεται η ανθεκτικότητα των υδατογραφημάτων έναντι των επιθέσεων απομάκρυνσής τους

4.2.2 Ψηφιακή Υδατογράφηση Αρχείων Ήχου

Τα ψηφιακά αρχεία ήχου έγιναν αντικείμενο εκτεταμένης καταχρηστικής εκμετάλλευσης και παράνομης αντιγραφής από τους χρήστες του Διαδικτύου, ιδιαίτερα μετά την έλευση των ομότιμων (peer to peer) εφαρμογών. Η λειτουργία που προσφέρουν οι συγκεκριμένες εφαρμογές είναι ένα εύχρηστο διαδικτυακό περιβάλλον για τη διαφήμιση και την ελεύθερη ανταλλαγή ψηφιακών αρχείων. Σε πολύ μικρό χρονικό διάστημα μετατράπηκαν στον παράδεισο της παράνομης αντιγραφής, καθώς οι χρήστες τους αντάλλασσαν ψηφιακό περιεχόμενο χωρίς να αποδίδουν καμία αποζημίωση στους δημιουργούς των έργων. Η τεχνολογική λύση της υδατογράφησης δεν μπορεί να αποτρέψει τους χρήστες από την παράνομη ανταλλαγή των αρχείων τους, ωστόσο είναι ικανή να εντοπίσει μια παράνομη χρήση και να στηρίξει μια ενδεχόμενη κατηγορία εναντίον του παραβάτη. Η πλειοψηφία των μεθόδων υδατογράφησης που ενσωματώνουν αόρατα υδατογραφήματα στο περιεχόμενο των ψηφιακών αρχείων, στηρίζεται στη θεωρία σημάτων και συγκεκριμένα στην εφαρμογή ορισμένων βασικών διακριτών μετασχηματισμών. Αντίστοιχες μαθηματικές λύσεις είναι και αυτές που θεμελιώνουν τις μεθόδους υδατογράφησης που χρησιμοποιούνται για την προστασία των ψηφιακών εικόνων. Δεν είναι τυχαίο

λοιπόν πως το σύνολο των εταιριών που δραστηριοποιούνται στο χώρο της ψηφιακής εικόνας, προτείνει λύσεις και για την ψηφιακή υδατογράφηση αρχείων ήχου. Οι διαφορές ανάμεσα στις αντίστοιχες μεθόδους υδατογράφησης προέρχονται από το διαφορετικό φάσμα συχνοτήτων, την ποσότητα της πληροφορίας που μπορεί λειτουργεί ως ξενιστής του υδατογραφήματος κ.α.

4.2.2.1 Alpha Tec Ltd

Για την προστασία των ψηφιακών αρχείων ήχου η Alpa Tec Ltd προτείνει το AudioMark.

AudioMark:

Αποτελεί το προϊόν που σχεδιάστηκε από την Alpha Tec. για την ενσωμάτωση υδατογραφημάτων σε ψηφιακά αρχεία ήχου και τη μετέπειτα ανίχνευσή τους. Τα υδατογραφήματα που χρησιμοποιούνται από το AudioMark δεν γίνονται αντιληπτά από το ανθρώπινο σύστημα ακοής και μπορούν να αποτελέσουν ισχυρό νομικό επιχείρημα για τον ιδιοκτήτη ενός μουσικού έργου σε περίπτωση αντιδικίας. Συνεπώς, η πρωταρχική χρήση του AudioMark είναι να προστατέψει το δικαίωμα αναπαραγωγής ψηφιακών αρχείων ήχου, εφοδιάζοντας το νόμιμο ιδιοκτήτη με ένα τεχνολογικό και νομικά έγκυρο μέσο προστασίας. Ο νόμιμος κάτοχος των δικαιωμάτων χρησιμοποιεί ένα μυστικό κλειδί για να δημιουργήσει ένα μοναδικό ηχητικό σήμα. Το συγκεκριμένο σήμα τοποθετείται μέσα στο ψηφιακό περιεχόμενο του μουσικού έργου με τρόπο ώστε να μην γίνεται αντιληπτό από το ανθρώπινο σύστημα ακοής. Κατά την αντιδικία ανάμεσα στον νόμιμο κάτοχο και τον έτερο διεκδικητή, μόνο εκείνος που έχει στην κατοχή του το μυστικό κλειδί είναι σε θέση να ανιχνεύσει το υδατογράφημα που είναι τοποθετημένο στην εικόνα και να αποδείξει ότι αποτελεί ιδιοκτησία του. Ανάμεσα στα λειτουργικά & τεχνικά χαρακτηριστικά του AudioMark συγκαταλέγονται και τα ακόλουθα:

• Τα ψηφιακά υδατογραφήματα που χρησιμοποιεί δεν επηρεάζουν καθόλου το τελικό ηχητικό αποτέλεσμα του μουσικού έργου.
• Η ανίχνευση ή η απομάκρυνση ενός υδατογραφήματος από το αρχείο που έχει τοποθετηθεί είναι εξαιρετικά δύσκολη από ένα μη εξουσιοδοτημένο άτομο.
• Υποστηρίζει ψηφιακά αρχεία ήχου τύπου Wav & Raw.
• Η διαδικασία της ανίχνευσης δεν προϋποθέτει την παρουσία του αρχικού μη υδατογραφημένου ψηφιακού αρχείου.
• Παρουσιάζει αυξημένη ανθεκτικότητα έναντι ενός εκτεταμένου συνόλου επιθέσεων όπως είναι, η MPEG συμπίεση ήχου με χαμηλό παράγοντα ποιότητας (μεγάλο λόγο συμπίεσης), καθώς και οι επιθέσεις επεξεργασίας σήματος (Φιλτράρισμα, επανα-δειγματοληψία κ.α).
• Η διαδικασία της ενσωμάτωσης και ανίχνευσης υδατογραφημάτων διεξάγεται σε πραγματικό χρόνο.
• Η λειτουργικότητά του παρέχεται μέσω μιας εύχρηστης διαπεφής για την υδατογράφηση αρχείων ήχου. Η συγκεκριμένη εφαρμογή υποστηρίζει και την αυτοματοποιημένη μαζική επεξεργασία ενός συνόλου ψηφιακών αρχείων.

Διατίθεται μέσω πλατφόρμας ανάπτυξης λογισμικού (SDK) κατάλληλη για την ενσωμάτωση των υπηρεσιών υδατογράφησης στο ευρύτερο πληροφοριακό σύστημα διαχείρισης του ψηφιακού αποθέματος ενός οργανισμού.

4.2.2.2 Blue Spike

Η Blue Spike είναι μια εταιρεία που απευθύνεται σε εκείνους που δημιουργούν, παράγουν, δημοσιοποιούν και διανέμουν ψηφιακά μουσικά έργα. Οι τεχνολογικές λύσεις που προτείνονται από τη Blue Spike προστατεύουν το ηλεκτρονικό περιεχόμενο, στηριζόμενες στα ψηφιακά υδατογραφήματα και τις κρυπτογραφικές τεχνικές που ενσωματώνουν.

Το προϊόν που προσανατολίζεται στην προστασία ψηφιακών αρχείων ήχου είναι η πρώτη από τις τεχνολογικές λύσεις που προτείνει η Blue Spike και

βασίζεται στην υδατογραφία. Πρόκειται για ένα αρκετά ισχυρό εργαλείο, ιδιαίτερα χρήσιμο στις εταιρείες που πραγματοποιούν πωλήσεις μέσω του Διαδικτύου. Το προϊόν φέρει το όνομα **Giovanni** και έχει τα ακόλουθα χαρακτηριστικά.

• Χρησιμοποιεί multi-bit υδατογραφήματα που παρέχουν στο μηχανισμό ανίχνευσης τη δυνατότητα να κωδικοποιήσει από 8 μέχρι 256 bit.
• Η θέση που τοποθετείται το υδατογράφημα είναι προϊόν κρυπτογραφικής διαδικασίας και είναι γνωστή μόνο στον κάτοχο του μυστικού κλειδιού. Με αυτόν τον τρόπο ενισχύεται η ασφάλεια του συστήματος.
• Ο χρόνος απόκρισης του μηχανισμού ανίχνευσης κυμαίνεται από 15 έως 60 δευτερόλεπτα.
• Το ηχητικό υδατογράφημα δεν επηρεάζει καθόλου το ακουστικό αποτέλεσμα του μουσικού έργου.
• Παρουσιάζει αξιοσημείωτη ανθεκτικότητα σε επιθέσεις συμπίεσης (MPEG), επεξεργασίας σήματος, καθώς και στη μετατροπή του αρχείου από ψηφιακή σε αναλογική μορφή.

4.2.2.3 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. Οι υπηρεσίες που προσφέρει ομοιάζουν σημαντικά με αυτές του MAIM 2.Ο και έχουν σκοπό την απαγόρευση της παράνομης αντιγραφής και διακίνησης μουσικών έργων. Οι λειτουργικές προδιαγραφές του **MAO 2.0** είναι οι ακόλουθες:

- Τα υδατογραφήματα που χρησιμοποιούνται δεν γίνονται αντιληπτά από το ανθρώπινο σύστημα ακοής
- Επιτυγχάνει ανθεκτικότητα έναντι των επιθέσεων συμπίεσης και επεξεργασίας σήματος
- Υποστηρίζει τη μαζική και σε πραγματικό χρόνο επεξεργασία ψηφιακών αρχείων
- Είναι διαθέσιμο σε μορφή εύχρηστης παραθυρικής διεπαφής, αλλά οι λειτουργίες υδατογράφησης υποστηρίζονται και μέσω της πλατφόρμας ανάπτυξης λογισμικού που προσφέρει (SDK).
- Υποστηρίζει αρχεία τύπου WAV, WMA, ACC, Q-Design, ETRAC.

4.2.2.4 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. Οι εφαρμογές που χρησιμοποιούν το MT Audio σχετίζονται όπως και τα υπόλοιπα προϊόντα της οικογένειας, με την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας και τη διασφάλιση του δικαιώματος αναπαραγωγής. Κύριο χαρακτηριστικό του είναι η εκμετάλλευση των ιδιοτήτων του ανθρώπινου συστήματος ακοής, με στόχο την επίτευξη της μικρότερης δυνατής αλλοίωσης του ηχητικού σήματος και την ταυτόχρονη αύξηση της ανθεκτικότητας έναντι των επιθέσεων αφαίρεσής του. Ακολουθούν μερικά από τα σημαντικότερα λειτουργικά χαρακτηριστικά του **MT Audio**.

- Το ανθρώπινο σύστημα ακοής δεν μπορεί να αντιληφθεί τη διαφορά ανάμεσα στο αρχικό και υδατογραφημένο μουσικό έργο.
- Έχει τη δυνατότητα να κωδικοποιήσει αρκετά μεγάλη ποσότητα πληροφορίας με τη μορφή υδατογραφήματος.

• Είναι ανθεκτικό σε ένα σημαντικό σύνολο από επιθέσεις, όπως ορίζονται από το SDMI & STEP.

Όπως όλα τα προϊόντα της οικογένειας MagicTag είναι διαθέσιμα μέσω μίας πλατφόρμας ανάπτυξης λογισμικού

4.2.2.5 Verance

Η 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. Η τεχνολογία την ψηφιακής υδατογράφησης μουσικών έργων προσφέρει μια αποτελεσματική λύση στο πρόβλημα της προστασίας του δικαιώματος αναπαραγωγής και τη διαχείριση των δικαιωμάτων. Η αλυσίδα των προϊόντων υδατογράφησης που προτείνει η Verance διακρίνεται σε δύο κατηγορίες:

Λογισμικό & Άδειες ενσωμάτωσης υδατογραφημάτων:

Τα προϊόντα της συγκεκριμένης κατηγορίας απευθύνονται στους οργανισμούς που θέλουν να εγκαταστήσουν ένα εξειδικευμένο μηχανισμό ελέγχου του ψηφιακού ηχητικού τους αρχείου. Η Verance συνάπτει ειδικές άδειες με τις οποίες επιτρέπει την υδατογράφηση του ψηφιακού αποθέματος ενός οργανισμού. Παράλληλα με την άδεια η εταιρεία προσφέρει και κάποια βοηθητικά πακέτα λογισμικού που επιτελούν την διαδικασία της ενσωμάτωσης υδατογραφημάτων.

Λογισμικό & Άδειες ανίχνευσης υδατογραφημάτων:

Αντίστοιχα η εταιρεία παρέχει και άδειες για την ανίχνευση των υδατογραφημάτων που έχουν τοποθετηθεί με τα δικά της εργαλεία. Ολοκληρώνεται έτσι η διαδικασία του ελέγχου και το σύστημα παρέχει πλήρη εποπτεία του περιεχομένου που δημοσιοποιείται στο Διαδίκτυο. Την άδεια

συνοδεύουν και σε αυτή την περίπτωση βοηθητικά πακέτα λογισμικού για τη διαδικασία της ανίχνευσης.

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. Ο συγκεκριμένος κώδικας συνοδεύει πάντα το μουσικό έργο, ανεξάρτητα από τις αλλοιώσεις που ενδέχεται να υποστεί κατά τη μετάδοση ή επανεγγραφή του. Η λειτουργικότητα που προσφέρει ο Audio Watermark Embedder αποσκοπεί στη αποτελεσματική διαχείριση, εποπτεία και έλεγχο του ψηφιακού ηχητικού υλικού. Ανάμεσα στα λειτουργικά χαρακτηριστικά του εργαλείου υδατογράφησης συγκαταλέγονται τα ακόλουθα:

- **Διαφάνεια:** Τα υδατογραφήματα που χρησιμοποιεί δεν έχουν καμία απολύτως επίπτωση στο ηχητικό αποτέλεσμα του μουσικού έργου.
- **Ανθεκτικότητα:** Η ανθεκτικότητα των υδατογραφημάτων ανταποκρίνεται θετικά σε ενέργειες που αλλοιώνουν το ψηφιακό περιεχόμενο όπως, η μετάδοση και η αναμετάδοση του σήματος, η συμπίεσή του, η εγγραφή του σε αναλογικά μέσα κ.α.

- **Ασφάλεια:** Αντιμετωπίζει με επιτυχία ενέργειες πλαστογράφησης, μη εξουσιοδοτημένης παραποίησης, αποκωδικοποίησης και διαγραφής του κωδικοποιημένου σήματος

Άλλα επιπλέον χαρακτηριστικά του Audio Watermark Embedder είναι:

• Διατίθεται σαν ανεξάρτητη φιλική προς τον χρήστη παραθυρική εφαρμογή, αλλά και σαν πλατφόρμα ανάπτυξης λογισμικού (SDK), που δίνει στον χρήστη τη δυνατότητα να ενσωματώσει τις λειτουργίες της υδατογράφησης στο περιβάλλον εργασίας του.
• Έχει τη δυνατότητα της μαζικής επεξεργασίας και υδατογράφησης ψηφιακών αρχείων ήχου
• Οι τύποι των αρχείων ήχου που υποστηρίζει είναι, Microsoft WAV, Raw PCM, DVD-Audio & DDP.

Verance Audio Watermark Detector:

Πρόκειται για το αντίστοιχο εργαλείο της εταιρείας που χρησιμοποιείται για την ανίχνευση των υδατογραφημάτων σε ψηφιακά αρχεία ήχου. Παρουσιάζει συμβατότητα με το SDMI και τα λειτουργικά του χαρακτηριστικά είναι αντίστοιχα με αυτά του Embedder.

4.2.3 Ψηφιακή Υδατογράφηση Αρχείων Βίντεο

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. Ωστόσο, ένας αποτελεσματικός αλγόριθμος θα πρέπει να

εκμεταλλεύεται όλες τις επιμέρους ιδιότητες που χαρακτηρίζουν ένα αρχείο βίντεο.

4.2.3.1 Alpha Tec Ltd

Όπως συμβαίνει με όλες τις εταιρείες που διαθέτουν προϊόντα υδατογράφησης για ψηφιακά αρχεία ήχου και εικόνας και η Alpha Tec. Ltd εκμεταλλεύεται την τεχνογνωσία της στα δύο προηγούμενα πεδία, ώστε να συνθέσει έναν αλγόριθμο κατάλληλο για την υδατογράφηση αρχείων βίντεο. Η λύση που προτείνεται από την εταιρεία για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας αρχείων βίντεο είναι το VideoMark.

VideoMark:

Το VideoMark είναι ένα προϊόν λογισμικού που ενσωματώνει και ανιχνεύει αόρατα υδατογραφήματα σε ψηφιακά αρχεία βίντεο με στόχο την προστασία του δικαιώματος αναπαραγωγής τους. Τα υδατογραφήματα που χρησιμοποιούνται αντιστοιχούν σε συγκεκριμένους αναγνωριστικούς αριθμούς (ID-numbers) που αποκαλούνται κλειδιά υδατογράφησης. Κάθε νόμιμος δικαιούχος χρησιμοποιεί το κλειδί του για την ενσωμάτωση ενός αόρατου υδατογραφήματος στο ψηφιακό περιεχόμενο ενός αρχείου βίντεο. Το υδατογράφημα μπορεί να ανιχνευθεί στη συνέχεια χρησιμοποιώντας το VideoMark και το σωστό κλειδί υδατογράφησης. Τα βασικά λειτουργικά και τεχνικά χαρακτηριστικά του VideoMark είναι τα ακόλουθα:

• Τα υδατογραφήματα που χρησιμοποιούνται δεν γίνονται αντιληπτά από το ανθρώπινο σύστημα όρασης και ακοής κατά την αναπαραγωγή του υδατογραφημένου αρχείου βίντεο. Παρέχονται 5 διαφορετικά επίπεδα στάθμισης, μεταξύ της δύναμης ενσωμάτωσης του υδατογραφήματος και της αλλοίωσης του αισθητικού αποτελέσματος του αρχείου

• Η ανίχνευση των υδατογραφημάτων πραγματοποιείται για κάθε καρέ (frame) του βίντεο ανεξάρτητα. Το αποτέλεσμα της εξαντλητικής διαδικασίας είναι τα υδατογραφήματα να ανιχνεύονται με μεγάλη βεβαιότητα και πολύ μικρό αριθμό σφαλμάτων.

• Η ανίχνευση ή η αφαίρεση των υδατογραφημάτων είναι αδύνατη, αν δεν είναι γνωστό το μυστικό κλειδί υδατογράφησης.
• Τα υδατογραφήματα είναι ανθεκτικά στην MPEG2 κωδικοποίηση με λόγο συμπίεσης 1:50.
• Η διαδικασία της υδατογράφησης ή της ανίχνευσης μπορεί να εφαρμοστεί επιλεκτικά σε ένα τμήμα της ψηφιακού αρχείου ή στο σύνολό του.
• Η παρουσία του αρχικού μη υδατογραφημένου αρχείου δεν είναι απαραίτητη κατά τη διαδικασία ανίχνευσης

Οι υπηρεσίες υδατογράφησης που προσφέρει το VideoMark είναι διαθέσιμες στον τελικό χρήστη μέσω μιας εύχρηστης παραθυρικής διεπαφής και μιας πλατφόρμας ανάπτυξης λογισμικού.

4.2.3.2 MarkAny

Η Κορεάτικη εταιρεία προτείνει λύσεις και για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας ψηφιακών αρχείων βίντεο. Η τεχνολογική βάση είναι βέβαια η υδατογραφία και το προϊόν που προτείνεται είναι το Esignia – Video 1.5

MarkAny Video Watermarking – Esignia – Video 1.5:

Το συγκεκριμένο εργαλείο υδατογράφησης αρχείων βίντεο εξασφαλίζει την προστασία των πνευματικών δικαιωμάτων, τοποθετώντας υδατογραφήματα στο ψηφιακό περιεχόμενο. Τα χαρακτηριστικά του Esignia – Video 1.5 είναι τα εξής:

- Χρησιμοποιεί αόρατα υδατογραφήματα
- Η ενσωμάτωση και η ανίχνευση επιτυγχάνεται σε πραγματικό χρόνο
- Κατά την επιλογή του υδατογραφήματος ο χρήστης μπορεί να επιλέξει ανάμεσα σε ένα λογότυπο και σε ένα κλειδί, που χρησιμοποιείται για την κρυπτογράφηση της πληροφορίας

- Τα υδατογραφήματα που χρησιμοποιούνται είναι ανθεκτικά σε επιθέσεις αποκοπής και αλλαγής της κλίμακας του μεγέθους
- Το σύνολο της πληροφορίας που έχει τη δυνατότητα να κωδικοποιηθεί στο εσωτερικό περιεχόμενο ενός αρχείου βίντεο είναι 64 bits.
- Δεν είναι απαραίτητη η παρουσία του αρχικού μη υδατογραφημένου ψηφιακού αρχείου για τη διαδικασία της ανίχνευσης

Είναι συμβατό με τα διεθνή πρότυπα, ενώ οι τύποι αρχείων που υποστηρίζονται είναι MPEG-2, m2v, avi, asf, WMV, κ.α.

4.2.3.3 MediaSec

Η λύση που προτείνει η MediaSec για την προστασία των πνευματικών δικαιωμάτων αρχείων βίντεο, δε διαφοροποιείται από την αντίστοιχη λύση που προτείνει για τις ψηφιακές εικόνες. Η λειτουργίες της υδατογράφησης ενσωματώνονται στο ίδιο προϊόν λογισμικού "MediaSign Digital" και τα χαρακτηριστικά του είναι αντίστοιχα με αυτά που αναφέρθηκαν παραπάνω.

4.2.3.4 Sealtronic

Η οικογένεια προϊόντων MagicTag της Sealtronic περιέχει και το αντίστοιχο προϊόν για την προστασία των πνευματικών δικαιωμάτων αρχείων βίντεο.

MT Video:

Το MT Video ενσωματώνει ανθεκτικά, αόρατα υδατογραφήματα στα εικονοστοιχεία των εικόνων που συνθέτουν το βίντεο. Μερικά από τα χαρακτηριστικά του είναι:

- Η διαδικασία της ανίχνευσης μπορεί να γίνει σε πραγματικό χρόνο
- Η ποιοτική υποβάθμιση που εισάγεται από την υδατογράφηση δεν γίνεται αντιληπτή από το ανθρώπινο σύστημα αισθήσεων
- Παρουσιάζει ικανοποιητική ανθεκτικότητα έναντι αρκετών τεχνητών επιθέσεων

4.2.4 Άλλα Προγράμματα Υδατογράφησης

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 Λογισμικό Στεγανογραφίας

Στα ψηφιακά δεδομένα, η στεγανογραφία βρίσκει εφαρμογή στην απόκρυψη οποιουδήποτε αρχείου σε κάποιο άλλο αρχείο της ίδιας η άλλης μορφής (format).

Η στεγανογραφία γίνεται σε τρία βήματα, με την βοήθεια ειδικού λογισμικού.

1. Αρχικά επιλέγεται το αρχείο προς απόκρυψη.
2. Στην συνέχεια επιλέγεται το αρχείο στο οποίο θα αποκρυφτεί το προηγούμενο.

3. Τέλος εισάγεται κάποιος κωδικό προστασίας.

Ο παραλήπτης για να ανακτήσει το κρυμμένο αρχείο θα πρέπει να εγκαταστήσει το ίδιο λογισμικό στεγανογραφίας που χρησιμοποιήθηκε καθώς και να γνωρίζει τον κωδικό προστασίας. Έτσι όσοι δε γνωρίζουν τα δύο αυτά στοιχεία το μόνο που θα μπορούν να δουν είναι το αρχείο στο οποίο βρίσκεται κρυμμένη η πληροφορία, χωρίς όμως να μπορούν να δουν την ίδια.

Τα προγράμματα που παρουσιάζονται παρακάτω ακολουθούν αυτά τα τρία βήματα για την απόκρυψη πληροφοριών.

4.3.1 Snow

Ένα απλό εργαλείο που υλοποιεί στεγανογραφικές τεχνικές είναι το Snow. Το συγκεκριμένο εργαλείο υλοποιεί την τεχνική κωδικοποίησης πληροφορίας με την χρήση των κενών χαρακτήρων. Η στεγανογραφία κενών χαρακτήρων συνίσταται στην εκμετάλλευση των διαστημάτων μεταξύ διαδοχικών λέξεων ή στην περίπτωση του συγκεκριμένου εργαλείου των διαστημάτων στο τέλος των γραμμών. Το Snow είναι ένα πρόγραμμα λογισμικού που διατίθεται ελεύθερα στην αγορά και κωδικοποιεί πληροφορία μέσα σε ένα κείμενο με την προσαρμογή των κενών διαστημάτων που ακολουθούν το τέλος κάθε γραμμής.

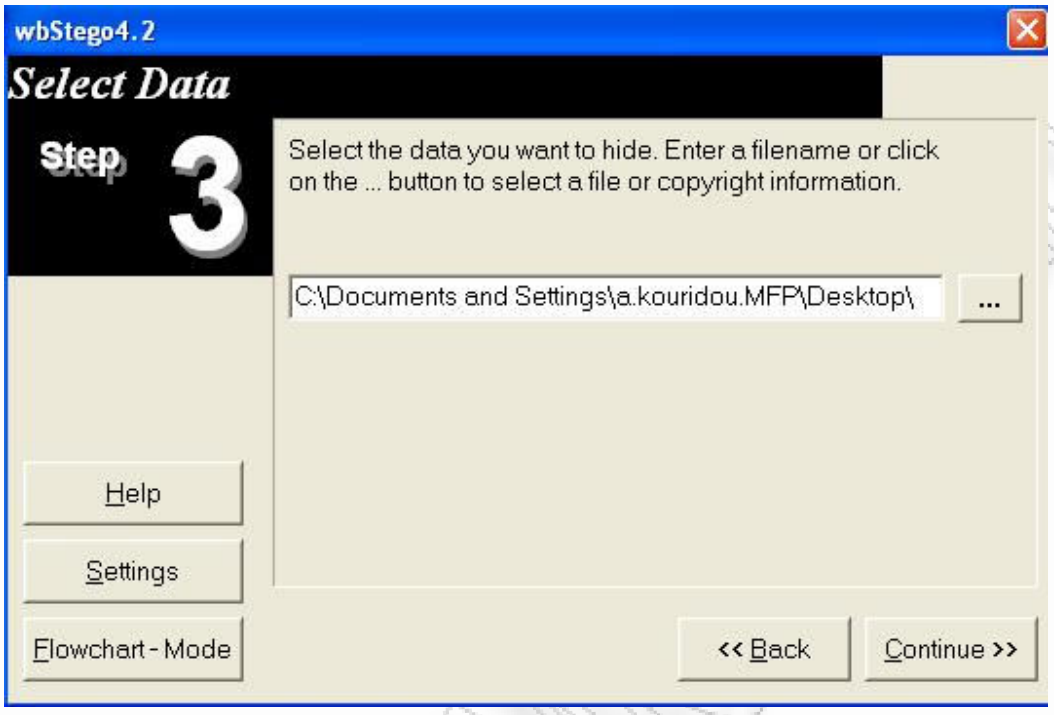
4.3.2 Hide in Picture

Εφαρμογή η οποία δίνει τη δυνατότητα να «κρυφτούν» αρχεία μέσα σε εικόνες τύπου .bmp ή .gif.

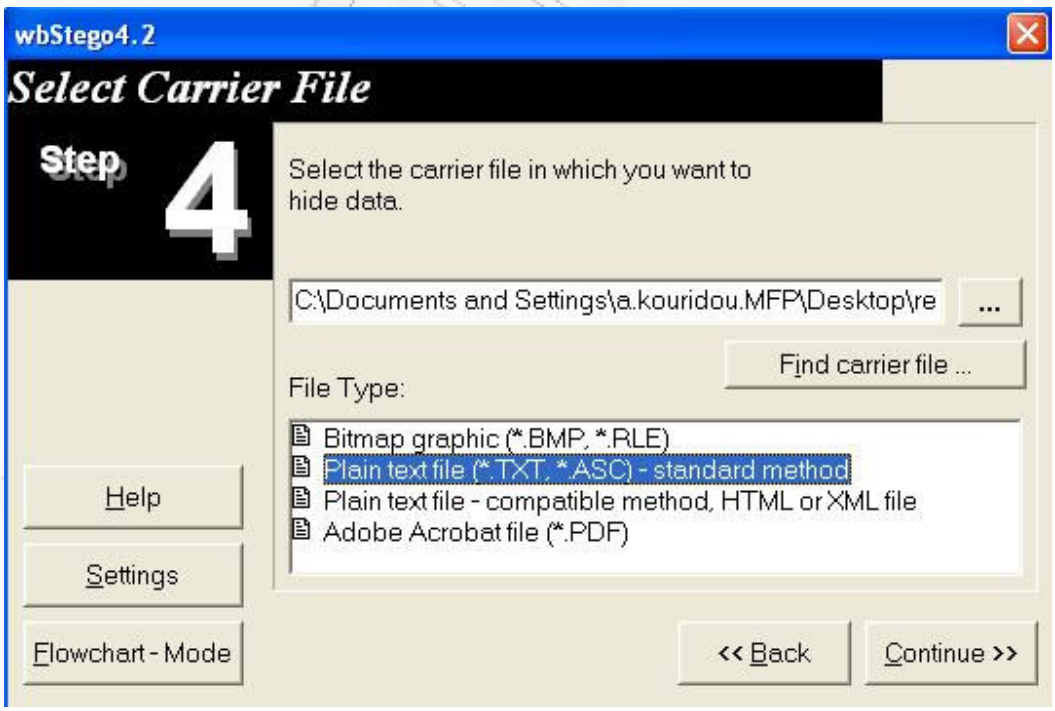
Εικόνα 21: Απόκρυψη αρχείου σε εικόνα με το Hide in Picture

4.3.3 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).



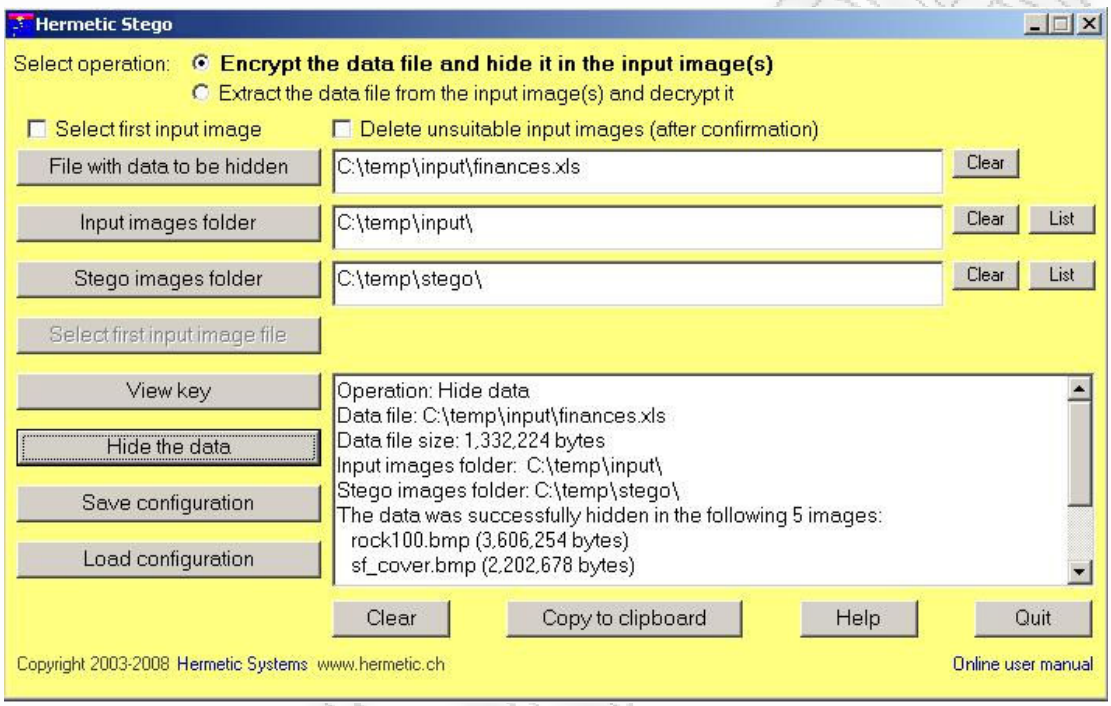
Εικόνα 22: Επιλογή αρχείου προς απόκρυψη με το wbStego



Εικόνα 23: Επιλογή αρχείου στο οποίο θα γίνει η απόκρυψη του προηγούμενου

4.3.4 Hermetic Stego

Το Hermetic Stego είναι ακόμη μία απλή εφαρμογή για απόκρυψη αρχείων μέσα σε εικόνες.



Εικόνα 24: Απόκρυψη αρχείων με το Hermetic Stego

4.3.5 Άλλα Προγράμματα Στεγανογραφίας

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

Στις μέρες μας η «προστασία των πνευματικών δικαιωμάτων» είναι ένας όρος ιδιαίτερα παρεξηγημένος. Η ραγδαία εξάπλωση του Διαδικτύου δεν επέτρεψε την καθιέρωση των εμπορικών δομών που διέπουν τις καθημερινές μας συναλλαγές πριν την εξάπλωση του ηλεκτρονικού εμπορίου. Για το λόγο αυτό, οι μεγάλες βιομηχανίες της μουσικής και του κινηματογράφου εφαρμόζουν στο όνομα των πνευματικών δικαιωμάτων κινήσεις απαγόρευσης και καταστολής για να εξασφαλίσουν τα οικονομικά τους συμφέροντας. Έχοντας, λοιπόν, ο απλός χρήστης συνδέσει την προστασία των πνευματικών δικαιωμάτων με την απαγόρευση και την αποτροπή της ελεύθερης διακίνησης στο Διαδίκτυο, θεωρεί τον όρο αρνητικό και καταφέρεται εναντίον του. Πρέπει, όμως, να επιτραπεί αυτή η γενίκευση; Υπάρχουν τομείς όπου η προστασία των πνευματικών δικαιωμάτων κρίνεται απαραίτητη. Η ψηφιοποίηση είναι ο μόνος δρόμος για τη διάσωση και τη μακροπρόθεσμη διατήρηση της πολιτιστικής μας κληρονομιάς αλλά και για την εκπαιδευτική της αξιοποίηση.

Στην παρούσα εργασία, πραγματοποιήθηκε εκτενής μελέτη του ζητήματος της προστασίας και διαχείρισης των πνευματικών δικαιωμάτων. Η διαχείριση ψηφιακών δικαιωμάτων (DRM, Digital Rights Management) είναι μια τεχνολογία που προστατεύει το ψηφιακό περιεχόμενο από παράνομη χρήση, όπως αυθαίρετη αντιγραφή και διανομή.

Στη συνέχεια πραγματοποιήθηκε εκτενής αναφορά στα βασικά τεχνολογικά μέσα προστασίας ψηφιακών αντικειμένων, όπως η Κρυπτογραφία, η Στεγανογραφία και η Υδατογραφία. Εκτός από τα τεχνολογικά μέσα, η προστασία των ψηφιακών πόρων γίνεται και με την κατάλληλη τεκμηρίωση τους με επιπρόσθετη πληροφορία.

Τέλος, παρουσιάστηκε μια συνοπτική περιγραφή των κυριότερων εμπορικά διαθέσιμων προϊόντων, ανά κατηγορία περιεχομένου. Ο στόχος της περιγραφής

δεν ήταν να αξιολογηθούνι συγκριτικά τα διαθέσιμα συστήματα, αλλά να αναδειχθούν μερικά από τα επιμέρους λειτουργικά και τεχνικά χαρακτηριστικά τους.

ΚΕΦΑΛΑΙΟ 6
ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] 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

[2] Τα Δικαιώματα Πνευματικής Ιδιοκτησίας στην Ψηφιακή Εποχή:Ζητήματα Προστασίας και Διαχείρισης. Ένα Πρότυπο Σύστημα Ψηφιακής Διαχείρισης των Πνευματικών Δικαιωμάτων

[3] (http://www.infosoc.gr/meletes/)

[4] Arms William, The online edition of Digital Libraries: Chapter 7 Access management and security, MIT Press:2000 (updated with additional material by the author)

[5] http://www.cs.cornell.edu/wya/DigLib/new/Chapter7.html

[6] 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.

[7] http://www.dlib.org/dlib/july03/gladney/07gladney.html

[8] Encryption Technology Windows on Computing, No. 22, University of Washington Computing & Communications Winter 1999

[9] http://www.washington.edu/computing/windows/issue22/encryption.html

[10] Brown Lawrie Cryptography and Computer Security - Cryptography Lecture 12 Modern Stream Ciphers November 2001

[11] http://www.cs.adfa.edu.au/courses/ACSC2010/coursework/lectures/ss-less12.html

[12] Mintzer Fred et al. Safeguarding Digital Library Contents and Users: Digital Watermarking D-Lib Magazine, December 1997 ISSN 1082-9873.

[13] http://www.dlib.org/dlib/december97/ibm/12lotspiech.html

[14] Steganography and Digital Watermarking Tool Table

[15] http://www.jjtc.com/Steganography/toolmatrix.htm

[16] Μάγκος Εμμανουήλ *Ασφάλεια στο World Wide Web* Πειραιάς 1997

[17] http://thalis.cs.unipi.gr/~emagos/THE%20WHOLE%20THING%201.pdf

[18] Μάγκος Κ. και Νιξαρλίδης Α. *Ασφάλεια στο διαδίκτυο (Κεφάλαιο 3ο)* Ιούλιος 1999

[19] http://www.lab.epmhs.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio3.htm

[20] Καλουπτσίδης και άλλοι. Ανάλυση και Σχεδιασμός Συμμετρικών Κρυπτογραφικών Αλγορίθμων Αθήνα, ΕΚΠΑ 31/10/2001

[21] http://www.army.gr/html/GR_Army/drasi/synedrio_programma.html

[22] Χαλάτσης Κ. Κρυπτογραφία – Σύγχρονες Τάσεις. (διαθέσιμο από την διεύθυνση του συνεδρίου, δεύτερη ημέρα 4η θεματική ενότητα)

[23] http://www.army.gr/html/GR_Army/drasi/synedrio_programma.html

[24] Encyclopedia4u.com Cryptography και σχετικές με αλγορίθμους συνδέσεις

[25] http://www.encyclopedia4u.com/c/cryptography-1.html

[26] 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

[27] 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.

[28] Digital Watermarking, Ingerman J. Cox, Matthew L. Miller. Jefrey A. Bloom, Morgan Kaufman Publishers

[29] INFORMATION HIDING – techniques for steganography and digital watermarking", Stefan Katzenbeisser, Fabien A. P. Petitcolas, Artech House Publishers

[30] An Overview of Cryptography Gary C. Kessler, May 1998, 30 October 2004

[31] Herodotus, The Histories, London, England: J.M. Dent & Sons, Ltd, 1992

[32] Kahn, D., The Codebreakers-The story of secret Writing, New York, New York, USA: Scribner, 1996.

[33] Wilkins, E. H., A History of Italian Literature, London: Geoffrey Cumberlege, Oxford University Press. 1954.

[34] Wilkins, J., Mercury: or the Secret and Swift Messenger: Shewing, How a Man May With Privacy and Speed Communicate His Thoughts to a Friend at Any Distance, London: printed for Rich Baldwin, near Oxford-Arms in the Warnick-lane, 2nd ed., 1694.

[35] Current Steganography Tools & Methods, Erin Michaud, GSEC Practical, Version 1.4b, April 2003.

[36] 2003, Sellars, Duncan. "An Introduction to Steganography", March, 2003

[37] Bender, W., et al. "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, Nos. 3&4, 1996: 313-336

[38] http://www.darkside.com.au/snow

[39] http://steghide.sourceforge.net/

[40] Digital Rights Manegement (DRM) Architectures, Renato Iannella, D-Lib Magezine Article, Volume 7 Number 6, June 2001.

[41] Digital Object Identifier, http://www.doi.org/

[42] Digital Rights Management Workshop, http://www.w3.org/2000/12/drm-ws/

[43] Open Digital Rights Language (ODRL), Renato Iannella, 2002-08-08

[44] Rights Management: Managing the Layers of Rights and Roles in the Knowledge Based Economy, Peter Higgs, 2000, IPR Systems Report

[45] http://www.iprsystems.com/assets/0.2_Rights_Management.pdf

[46] Electronic Book Exchange, http://www.ebxwg.org/

[47] 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

[48] Copyright Clearance Center – CCC, http://www.copyright.com/

[49] http://www.watermarkingworld.org/optimark/index.html

[50] http://watermarking.unige.ch/Checkmark/index.html

[51] http://www.cl.cam.ac.uk/~mgk25/stirmark.html

[52] http://www.petitcolas.net/fabien/watermarking/2mosaic/index.htmlSafeguarding

[53] Digital Library Contents and Users - Digital Images of Treasured Antiquities των Henry M. Gladney, Fred Mintzer, και Fabio Schiattarella, D-Lib Magazine Ιούλιος/Αύγουστος 1997

[54] http://www.digimarc.com/imaging/ibplus_over.htm

[55] http://www.signumtech.com/template3.asp?pageID=4&prodID=2

[56] http://www.signumtech.com/template3.asp?pageID=4&prodID=7

[57] http://www.bluespike.com/giovanni.html

[58] http://www.mediasec.com/html/en/products_services/syscop.htm

[59] http://www.sims.berkeley.edu/courses/is290-1/f96/watermark.html

[60] http://www.imprimatur.net/protect.htm

[61] http://www.ad-mkt-review.com/public_html/air/ai028.html

[62] http://www.burks.de/stegano/snow.html

[63] http://www.free.gr/get/list.php?cat_id=51