ΠΑΝΕΠΙΣΤΗΜΙΟΝ ΠΕΙΡΑΙΩΣ

ΠΜΣ Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων

Κατεύθυνση Ασφαλείας Ψηφιακών Συστημάτων

Διπλωματική Εργασία

Ψηφιακή Διαχείριση Πνευματικών Δικαιωμάτων (DRM)

ΠΑΡΑΔΕΙΣΑΣ ΜΑΝΩΛΗΣ ΜΤΕ 1064	**ΕΠΙΒΛΕΠΩΝ** ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ ΚΩΝ/ΝΟΣ ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ

ΠΕΙΡΑΙΑΣ 2012

Πίνακας περιεχομένων

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

Περίληψη

Η παρούσα εργασία επιχειρεί να παρουσιάσει τον τομέα της ψηφιακής διαχειρίσεως πνευματικών δικαιωμάτων (Digital Rights Management - DRM), να αναδείξει τα προβλήματα που υπάρχουν στην εφαρμογή της καθώς και την αποτελεσματικότητά της. Επίσης, στο β' σκέλος της εργασίας, παρουσιάζεται μία ρεαλιστική υλοποίηση σχετική με το DRM.

Εισαγωγή

Η προστασία της πνευματικής δημιουργίας είναι μία από τις περιοχές στις οποίες οι τεχνικές και νομικές λύσεις που σχετίζονται με τους όρους χρήσεως της πληροφορίας, είναι πρωτευούσης σημασίας.

Οι εκφράσεις “thin copyright” και “thick copyright” αντιπροσωπεύουν δύο διαφορετικές φιλοσοφίες στον τρόπο που αντιλαμβανόμαστε την προστασία της πνευματικής ιδιοκτησίας. Εν συντομία, η πρώτη αναφέρεται σε μία πιο χαλαρή προσέγγιση στην πνευματική ιδιοκτησία, όπου δίδεται στα έργα όση προστασία χρειάζεται έτσι ώστε να ενθαρρύνεται η δημιουργικότητα αλλά ταυτόχρονα τα έργα να είναι ευρέως διαθέσιμα στο κοινό. Η δεύτερη φιλοσοφία, προστατεύει περισσότερο την πνευματική ιδιοκτησία και έχει ως πρωτεύοντα στόχο την αύξηση των εσόδων. Τα τελευταία χρόνια οδηγούμαστε προς την εφαρμογή αυτής της κατευθύνσεως.

Η είσοδος του διαδικτύου στην ζωή μας τις τελευταίες δύο δεκαετίες, έκανε την διακίνηση πληροφοριών πιο εύκολη. Σε συνδυασμό με την ψηφιοποίηση των έργων που προστατεύονται από την πνευματική ιδιοκτησία, το διαδίκτυο δημιουργεί επαναστατικά δεδομένα για τις δομές της επικοινωνίας μεταξύ των ανθρώπων. Ταυτόχρονα διευκολύνει την παραγωγή νέων προϊόντων με χρήση υλικού που ήδη προστατεύεται από θεσμούς της πνευματικής ιδιοκτησίας. Τα κύρια προβλήματα εντοπίζονται ή σχετίζονται αμέσως με:

1. Την ευκολία και την ακρίβεια της αντιγραφής
2. Την υψηλή ποιότητα των αντιγράφων με αποτέλεσμα την αδυναμία διακρίσεως μεταξύ πρωτοτύπου και αντιγράφου
3. Το χαμηλό κόστος αναπαραγωγής και διανομής των αντιγράφων
4. Την ανωνυμία που χαρακτηρίζει τις διαδικτυακές δραστηριότητες

Όλα τα παραπάνω είχαν ως αποτέλεσμα την δημιουργία τεχνικών μέτρων για την προστασία των ψηφιακών έργων πνευματικής ιδιοκτησίας. Τα τεχνικά αυτά μέτρα αναφέρονται ως Digital Rights Management (DRM) δηλαδή Διαχείριση Ψηφιακών Δικαιωμάτων Πνευματικής Ιδιοκτησίας. Το DRM δεν αποτελεί μία ενιαία τεχνολογία, ούτε μία ενιαία φιλοσοφία. Αναφέρεται σε ένα μεγάλο εύρος προτύπων και τεχνολογιών, εκ των οποίων η πλειοψηφία βρίσκεται ακόμη σε σχεδιασμό. Το DRM δεν είναι ούτε thin copyright αλλά ούτε και thick copyright καθώς στοχεύει στην απόλυτη προστασία των ψηφιακών έργων.

Η αναγκαιότητα υπάρξεως του DRM

Το κίνητρο για την δημιουργία του DRM γίνεται κατανοητό από το παρακάτω παράδειγμα (1). Ας υποθέσουμε ότι έχουμε ένα βιβλίο το οποίο έχουμε δανειστεί από την βιβλιοθήκη του πανεπιστημίου. Τι μας αποτρέπει να δημιουργήσουμε ένα αντίγραφο αυτού του βιβλίου σε ένα φωτοτυπείο; Είναι ο νόμος; Στην πραγματικότητα ο νόμος δεν είναι το πρώτο πράγμα που μας αποτρέπει από το να φτιάξουμε ένα αντίγραφο, αλλά το γεγονός ότι θα ξοδέψουμε αρκετή ώρα και κατά πάσα πιθανότητα περισσότερα χρήματα για το κακέκτυπο του βιβλίου, απ’ ότι για να αγοράσουμε ένα καινούργιο αντίγραφο.

Ας υποθέσουμε για το παραπάνω παράδειγμα, ότι το βιβλίο είναι ψηφιακό. Σε αυτήν την περίπτωση μπορούμε αμέσως να έχουμε ένα αντίγραφο αυτού, της ίδιας ακριβώς

ποιότητος με μηδενικό κόστος. Για την ακρίβεια μπορούμε να δημιουργήσουμε αναρίθμητα αντίγραφα και να τα μοιραστούμε μέσω του διαδικτύου, παρ' όλο που ο νόμος που προστατεύει την πνευματική ιδιοκτησία του ψηφιακού αντιγράφου του βιβλίου είναι ο ίδιος με αυτόν που προστατεύει και το κανονικό βιβλίο!

Η αδυναμία της κρυπτογραφίας

Σε κάθε αναφορά στην προστασία ψηφιακών αρχείων συνήθως υπάρχει η κρυπτογραφία ως η απάντηση στην προστασία. Η προστασία όμως που παρέχει η κρυπτογραφία έχει τους δικούς της περιορισμούς. Η κρυπτογραφία δεν αποτρέπει την αντιγραφή ενός αρχείου. Η αντιγραφή είναι ουσιαστικά μεταφορά άσσων και μηδενικών από ένα σημείο σε ένα άλλο. Το αρχείο, ακόμη και κρυπτογραφημένο, μπορεί να αντιγραφεί και να σταλεί. Βέβαια η χρησιμότητά του χωρίς το κλειδί αποκρυπτογραφήσεως είναι μηδενική. Αν όμως το κλειδί αποκρυπτογραφήσεως είναι γνωστό, το αρχείο δεν έχει καμμία προστασία.

Αυτό που ουσιαστικά ελέγχει η ψηφιακή διαχείριση πνευματικών δικαιωμάτων δεν είναι μόνο η πρόσβαση στο αρχείο αλλά όλες οι λειτουργίες που έχουν σχέση με το αρχείο, όπως η αντιγραφή μερών του αρχείου, η εκτύπωση, η μετατροπή κτλ. Αυτή είναι και η κύρια διαφορά μεταξύ κρυπτογραφίας και DRM.

Παρακάτω παρουσιάζονται αναλυτικά οι τομείς εφαρμογής της ψηφιακής διαχειρίσεως πνευματικών δικαιωμάτων καθώς και οι αποτελεσματικότητα αυτών των μέτρων.

Εφαρμογή του DRM

DRM στις ταινίες

Τις τελευταίες δύο δεκαετίες έχουν γίνει διάφορες προσπάθειες για την προστασία των ψηφιακών κινηματογραφικών ταινιών και σχεδόν όλες, αργά ή γρήγορα απέτυχαν. Παρακάτω παρουσιάζονται οι σημαντικότερες.

Content Scrambling System (CSS)

Το Content Scrambling System (2) (σύστημα κωδικοποιήσεως περιεχομένου) είναι ένα DRM σύστημα που χρησιμοποιεί κρυπτογραφία και εφαρμόστηκε σχεδόν σε όλα τα εμπορικά διατιθέμενα DVD. Δημιουργήθηκε από το DVD Forum. Το CSS χρησιμοποιεί έναν ιδιωτικό αλγόριθμο κρυπτογραφήσεως ροής των 40-bit. Το σύστημα χρησιμοποιήθηκε το 1996 και το 1999 ήταν η πρώτη φορά που παραβιάστηκε από τον Jon Lech Johansen δημιουργό της εφαρμογής DeCSS, ο οποίος κατάφερε να λειτουργήσει ένα CSS-κρυπτογραφημένο DVD σε ένα σύστημα Linux, κάνοντας χρήση της εφαρμογής του.

Ο στόχος του CSS είναι διττός:

1. Το CSS αποτρέπει αντίγραφα δυφίο-προς-δυφίο μιας MPEG ροής δεδομένων, να μπορούν να αναπαραχθούν, καθώς τα αντίγραφα αυτά δεν περιλαμβάνουν τα κλειδιά αποκρυπτογραφήσεως τα οποία βρίσκονται σε μη προσβάσιμη περιοχή της DVD συσκευής.
2. Το CSS δίνει κίνητρο στους κατασκευαστές ώστε να κάνουν τις συσκευές DVD συμβατές με ένα ελεγχόμενο από την βιομηχανία πρότυπο, καθώς εξ αρχής οι CSS δίσκοι δεν μπορούν να αναπαραχθούν σε μη συμβατές συσκευές. Όποιος επιθυμεί να δημιουργήσει συμβατή συσκευή, θα πρέπει να προμηθευτεί άδεια, η οποία να πληροί τις DRM απαιτήσεις του προτύπου (γεωγραφικοί [region] κωδικοί, Macrovision και περιορισμός των λειτουργιών του χρήστη).

Ενώ τα περισσότερα προγράμματα CSS-αποκρυπτογραφήσεως χρησιμοποιούνται για την αναπαραγωγή DVD βίντεο, υπάρχουν αρκετά προγράμματα (DVD Decrypter, AnyDVD, DVD43, Smartripper, DVD Shrink) τα οποία μπορούν να δημιουργήσουν αντίγραφα του DVD στον σκληρό δίσκο και να αφαιρέσουν τους παραπάνω περιορισμούς (CSS κρυπτογράφηση, Macrovision κτλ).

Το CSS έχει πλέον αντικατασταθεί από νεότερα πρότυπα όπως το CPRM (Content Protection for Recordable Media) και το AACS (Advanced Access Content System) που χρησιμοποιούνται για δίσκους υψηλής ευκρινείας (HD) και Blu-ray. Τα πρότυπα αυτά χρησιμοποιούν κλειδιά μήκους 56 και 128 δυφίων, παρέχοντας μεγαλύτερο επίπεδο ασφαλείας από αυτό των 40 δυφίων του CSS.

Protected Media Path

Το λειτουργικό σύστημα Windows Vista της Microsoft περιέχει ένα σύστημα DRM ονόματι Protected Media Path το οποίο περιέχει το Protected Video Path (PVP). Το PVP προσπαθεί να αποτρέψει την αναπαραγωγή προστατευμένου από DRM περιεχομένου όταν παράλληλα εκτελούνται μη επαληθευμένης προελεύσεως προγράμματα, έτσι ώστε να μην υπάρχει πρόσβαση στο προστατευμένο περιεχόμενο. Επιπροσθέτως το PVP μπορεί να

κρυπτογραφήσει την πληροφορία που στέλνεται προς την οθόνη ή την κάρτα γραφικών ώστε να κάνει πιο δύσκολη την μη εξουσιοδοτημένη εγγραφή.

Advanced Access Content System

Το Προηγμένο Σύστημα Πρόσβασης Περιεχομένου (Advanced Access Content System (3) – AACS) είναι ένα πρότυπο για την διανομή περιεχομένου και τον ψηφιακό έλεγχο δικαιωμάτων, με στόχο να απαγορεύσει την πρόσβαση και την αντιγραφή των DVD δίσκων. Οι προδιαγραφές του δημοσιεύτηκαν τον Απρίλιο του 2005 και υιοθετήθηκε ως σχήμα για τον περιορισμό πρόσβασης των δίσκων HD και Blu-ray. Αναπτύχθηκε από την AACS Licensing Administrator, η όποια δημιουργήθηκε με την συμβολή των εταιριών Disney, Intel, Microsoft, Panasonic, Warner Bros, IBM, Toshiba και Sony.

Το AACS χρησιμοποιεί κρυπτογραφία για να ελέγξει και να περιορίσει την χρήση των ψηφιακών μέσων. Κρυπτογραφεί το περιεχόμενο με ένα ή περισσότερα κλειδιά κάνοντας χρήση του αλγορίθμου AES. Η κύρια διαφορά ανάμεσα στο AACS και στο CSS είναι στον τρόπο οργανώσεως των κλειδιών αποκρυπτογραφήσεως. Στο CSS όλες οι DVD συσκευές του ίδιου μοντέλου, έχουν εφοδιαστεί με το ίδιο κλειδί αποκρυπτογραφήσεως. Έτσι κάθε DVD δίσκος περιέχει εκατοντάδες κρυπτογραφημένα κλειδιά, για κάθε μοντέλο DVD συσκευής. Στην περίπτωση γνωστοποιήσεως του κλειδιού θα πρέπει να αντικατασταθούν όλες οι συσκευές του συγκεκριμένου μοντέλου, κάτι που το καθιστά οικονομικά ασύμφορο.

Το AACS εφοδιάζει κάθε DVD συσκευή με ένα διαφορετικό πλήθος κλειδιών αποκρυπτογραφήσεως, τα οποία χρησιμοποιούνται στο σχήμα εκπομπής κρυπτογραφήσεως. Αυτό επιτρέπει την ανάκληση (revoke) μιας συγκεκριμένης συσκευής ή καλλίτερα των κλειδιών που σχετίζονται με την συσκευή. Έτσι αν κάποια κλειδιά γνωστοποιηθούν, αυτά δεν περιλαμβάνονται στα μελλοντικά περιεχόμενα και έτσι αυτές οι συσκευές δεν δύνανται να αναπαράγουν νέες ταινίες.

Marlin

Marlin (DRM) ονομάζεται μία τεχνολογία που δημιουργήθηκε και συντηρείται από μία ομάδα επιχειρήσεων γνωστή και ως Marlin Developer Community (MDC) και εξουσιοδοτείται από τον οργανισμό Marlin Trust Management Organization (MTMO). Ιδρύθηκε το 2005 από τις εταιρίες Intertrust, Panasonic, Philips, Samsung, Sony και από την ίδρυσή του χρησιμοποιείται σε διάφορα μέρη ανά τον κόσμο. Στην Ιαπωνία η υπηρεσία acTVila IPTV χρησιμοποιεί το Marlin για να προστατέψει ροές βίντεο, οι οποίες επιτρέπεται να εγγραφούν σε οικιακή συσκευή DVR. Στην Ευρώπη, το Marlin χρησιμοποιείται από το δίκτυο Philips NetTVs. Επίσης το Marlin DRM απαιτείται σε βιομηχανικές ομάδες όπως το Open IPTV Forum και εθνικές πρωτοβουλίες όπως το YouView στο Ηνωμένο Βασίλειο, το Tivu στην Ιταλία και το HDForum στην Γαλλία.

DRM και μουσική

Σύμπακτοι Δίσκοι Ήχου (Audios CDs)

Δίσκοι που κάνουν χρήση του DRM δεν συμμορφώνονται με το νόμιμο πρότυπο του Compact Disc (CD) και είναι περισσότερο μέσα CD-ROM. Γι αυτό και δεν φέρουν το λογότυπο του CD όπως εκείνοι οι δίσκοι που ακολουθούν το πρότυπο. Οι δίσκοι αυτοί δεν μπορούν να αναπαραχθούν σε όλα τα CD players. Πολλοί καταναλωτές αδυνατούν να αναπαράγουν αυτούς τους δίσκους στους υπολογιστές τους. Προσωπικοί υπολογιστές που χρησιμοποιούν Microsoft Windows ενδέχεται να τερματίσουν την λειτουργία τους στην προσπάθεια να αναπαράγουν αυτούς τους δίσκους (4).

SDMI

Το Secure Digital Music Initiative (SDMI) είναι ένα forum που δημιουργήθηκε το 1998 από περισσότερες από 200 εταιρίες, με σκοπό να δημιουργήσει τις τεχνολογικές προδιαγραφές ώστε να προστατευτεί η αναπαραγωγή, η αποθήκευση και η διανομή της ψηφιακής μουσικής. Πιο συγκεκριμένα, οι στόχοι του SDMI ήταν η παροχή στους καταναλωτές προσβάσεως στην μουσική online και στα νέα συστήματα διανομής της, να εφαρμόσει DRM περιορισμούς στην δουλειά των καλλιτεχνών και να προωθήσει την δημιουργία νέων κλάδων σχετικών με την μουσική. Το SDMI ήταν μία άμεση απάντηση στην παγκόσμια επιτυχία του προτύπου MP3.

Η στρατηγική της ομάδας του SDMI περιελάμβανε δύο στάδια. Πρώτον είχε ως στόχο να κατασκευάσει ένα ασφαλές ψηφιακό υδατογράφημα. Αυτό θα επέτρεπε στα τραγούδια να φέρουν πληροφορία – ετικέτα με τα στοιχεία τους μέσω του υδατογραφήματος, το οποίο καθιστούσε δύσκολη την αφαίρεση από τα αρχεία χωρίς αυτά να καταστραφούν. Το δεύτερο στάδιο ήταν να διασφαλισθεί ότι οι συμβατοί SDMI αναπαραγωγείς (5), δεν θα αναπαρήγαγαν τραγούδια που έφεραν ετικέτες και δεν είχαν εξουσιοδότηση για την συγκεκριμένη συσκευή. Η λογική ήταν ότι ακόμη και αν τα αρχεία διανέμονταν, αυτά δεν θα μπορούσαν να αναπαραχθούν καθώς οι αναπαραγωγείς δεν θα τα αναπαρήγαγαν.

Το SDMI σταμάτησε την λειτουργία του τον Μάιο του 2001. Η αποτυχία του οφείλεται σε διαφόρους παράγοντες. Οι σημαντικότεροι είναι ότι πρώτον υπήρχε η ανησυχία για το αν η τεχνολογία ήταν όντως αρκετά ασφαλής ώστε να βγει στην γραμμή παραγωγής και δεύτερον η διένεξη ανάμεσα στην μουσική βιομηχανία και τις εταιρίες παραγωγής ηλεκτρικών για το κόστος της υλοποιήσεως της απαραίτητης τεχνολογίας σε επίπεδο υλισμικού.

Η περίπτωση της Sony-BMG

Το 2005, η εταιρία Sony-BMG εισήγαγε μία νέα DRM τεχνολογία η οποία εγκαθιστούσε DRM λογισμικό στον υπολογιστή του χρήστη χωρίς να τον προειδοποιεί. Μεταξύ άλλων, το λογισμικό περιελάμβανε ένα rootkit[1], το οποίο δημιουργούσε μία σοβαρή ευπάθεια ασφαλείας, η οποία μπορούσε να γίνει εκμεταλλεύσιμη. Όταν η φύση του DRM λογισμικού έγινε γνωστή στο κοινό, η Sony-BMG αρχικώς υποβάθμισε την σημασία των ευπαθειών που προκαλούσε το λογισμικό της αλλά εν συνεχεία αναγκάστηκε να αποσύρει εκατομμύρια CDs και να διανείμει λογισμικό το οποίο θα απεγκαθιστούσε το αρχικό λογισμικό. Τα δύο συστήματα που χρησιμοποιήθηκαν από την Sony-BMG ήταν το XCP και το MediaMax, τα οποία θα παρουσιαστούν συνοπτικά παρακάτω.

XCP (6) (Extended Copy Protection)

Την πρώτη φορά που ένα CD προστατευόμενο από το XCP εισέρχεται σε ένα υπολογιστικό σύστημα, αυτόματα (μέσω του autorun.inf) γίνεται η εγκατάσταση του λογισμικού. Κατά την εγκατάσταση, καταγράφονται όλες οι διεργασίες που τρέχουν εκείνη την ώρα στο υπολογιστή και συγκρίνονται με έναν κατάλογο ονομάτων, περίπου διακοσίων προγραμμάτων αντιγραφής και μετατροπής CD. Αν παράλληλα τρέχει κάποιο από αυτά τα προγράμματα τότε η εγκατάσταση σταματάει και ο υπολογιστής εξάγει το CD.

Το XCP χρησιμοποιεί μία ήπια προσέγγιση ως επιπρόσθετη ασφάλεια κατά της αντιγραφής και της μετατροπής των CDs. Εκμεταλλεύεται τον τρόπο που οι συσκευές αναπαραγωγής CDs και οι υπολογιστές διαβάζουν τα multisession CDs, τα CDs που έχουν εγγραφεί σταδιακά, δηλαδή με παραπάνω από μία εγγραφές. Σύμφωνα με το πρότυπο (stamped multisession) οι δίσκοι πρέπει να περιέχουν δύο εγγραφές. Την πρώτη με 1-99 τραγούδια audio και την δεύτερη με ένα αρχείο δεδομένων (data track). Το XCP, ξεφεύγοντας από το πρότυπο και προσθέτοντας ένα δεύτερο αρχείο δεδομένων, έχει ως επίπτωση τα Windows να αντιμετωπίζουν το CD σαν ένα κανονικό multisession CD αρχείων αλλά χωρίς να έχουν πρόσβαση στα τραγούδια. Έτσι η πρόσβαση και ο έλεγχος των τραγουδιών του CD γίνεται μέσω του λογισμικού XCP.

Mediamax (6)

Mediamax ονομάζεται το δεύτερο πακέτο λογισμικού που χρησιμοποιήθηκε από την Sony-BMG. Προορίζονταν για Windrows και Mac OS X. Όταν ένα CD που έχει το Mediamax εισέρχεται σε ένα υπολογιστή με λειτουργικό Windows, αυτόματα (μέσω του autorun.inf) γίνεται η εγκατάσταση του λογισμικού, το οποίο απαγορεύει από άλλα προγράμματα να διαβάσουν το CD. Το πρόγραμμα εγκατάστασης παρουσιάζει την άδεια χρήσης (EULA), την οποία ακόμη και αν ο χρήστης δεν δεχτεί, η εγκατάσταση συνεχίζεται κανονικά! Σε Mac OS X είναι απαραίτητος ο κωδικός διαχειριστή για την εγκατάσταση οποιουδήποτε προγράμματος, οπότε είναι εφικτό ο χρήστης να αποφύγει την εγκατάσταση.

Αφού έχει γίνει η εγκατάσταση, το Mediamax αναζητεί ένα υδατογράφημα μέσω σε κάθε CD ήχου για να αναγνωρίσει αν πρόκειται για προστατευμένο περιεχόμενο. Το

[1] Rootkit ονομάζεται ένας μη ορατός στον χρήστη τύπος κακόβουλου λογισμικού, που έχεις ως σκοπό να αποκρύψει την ύπαρξη συγκεκριμένων διεργασιών έτσι ώστε ο κακόβουλος χρήστης να αποκτήσει επιπλέον δικαιώματα προσβάσεως.

υδατογράφημα παράγεται θέτοντας τα λιγότερα σημαντικά δυφία κάθε τραγουδιού σε 1. Αυτό κάνει το υδατογράφημα αρκετά «εύθραυστο» καθώς κατά τις περισσότερες μετατροπές του αρχείου ήχου, συμπεριλαμβανομένης της μετατροπής σε MP3 και αντίστροφα, το υδατογράφημα χάνεται.

Όταν το Mediamax λειτουργεί κατά την σχεδίασή του, επιτρέπει την μετατροπή των αρχείων ήχου σε αρχεία τύπου WMA (Windows Media Audio). Οι παρακάτω δραστηριότητες επιτρέπονται: Αντιγραφή των τραγουδιών στον σκληρό δίσκο για αναπαραγωγή χωρίς το CD, δημιουργία μέχρι τριών αντιγράφων του CD και αποστολή με email συνδέσμων για τα προστατευόμενα από DRM τραγούδια που λήγει μετά από δέκα ημέρες. Τέλος τα τραγούδια μπορούν να μεταφερθούν σε DRM συμβατούς αναπαραγωγείς.

Κριτική

Το λογισιμικό της Sony-BMG είχε ουσιαστικά επίδραση μόνο σε υπολογιστές με λειτουργικό Windows. Ακόμη και σε αυτούς, ο μέσος χρήστης (π.χ. απενεργοποιώντας την λειτουργία autorun) μπορούσε να παρακάμψει την ασφάλεια του λογισμικού. Οι δύο πρώτες δημοσιεύσεις της Sony-BMG για λογισμικό που θα απεγκαθίστουσε το αρχικό λογισμικό απέτυχαν.

Τον Ιανουάριο του 2007, η EMI σταμάτησε την έκδοση ηχητικών CD με DRM, δηλώνοντας ότι το κόστος του DRM δεν φέρει τα ανάλογα αποτελέσματα (7). Ακολουθώντας την EMI, η Sony-BMG ήταν ο τελευταίος εκδότης που κατήργησε εντελώς την DRM προστασία (8).

Μουσική μέσω διαδικτύου

Όπως έγινε αντιληπτό από τα παραπάνω, η προσπάθεια των εταιριών, για προστασία των ηχητικών CD με DRM εγκατελήφθει, Παρ' όλα αυτά υπάρχουν αρκετά διαδικτυακά καταστήματα που πωλούν τραγούδια τα οποία προστατεύονται από DRM. Παρακάτω αναφέρονται τα σημαντικότερα:

Apple iTunes Store

Πριν το 2009, το Apple iTunes Store χρησιμοποιώντας το DRM σύστημα Fairplay διένειμε μουσική μέσω του διαδικτύου. Η Apple δεν εξουσιοδοτούσε την DRM προστασία σε άλλες εταιρίες και έτσι μόνο οι συσκευές Apple μπορούσαν να αναπαράγουν αυτά τα τραγούδια. Τον Μάιο του 2007 (9), τα τραγούδια της EMI έγιναν διαθέσιμα στο iTunes Plus με υψηλότερη τιμή. Αυτά τα τραγούδια ήταν καλλίτερης ποιότητος (256 kbps) και χωρίς προστασία DRM. Τον Απρίλιο του 2009, όλη η μουσική στο iTunes απαλλάχθηκε από την DRM προστασία.

Fairplay

Το DRM σύστημα Fairplay βασίστηκε πάνω στην τεχνολογία της εταιρίας Veridisc. Είναι δημιουργημένο πάνω στο QuickTime (πρόγραμμα αναπαραγωγής πολυμέσων) και χρησιμοποιείται από το iPhone, iPod, iPad, Apple TV, iTunes και iTunes Store.

Τα προστατευόμενα από το Fairplay αρχεία, είναι κανονικά MP4 αρχεία, με μία κρυπτογραφημένη ηχητική AAC ροή. Η ηχητική ροή είναι κρυπτογραφημένη με τον αλγόριθμο AES σε συνδυασμό με τον αλγόριθμο κατακερματισμού MD5. Το κύριο (master)

κλειδί που απαιτείται για την αποκρυπτογράφηση της ηχητικής ροής είναι επίσης αποθηκευμένο στο MP4 αρχείο.

Κάθε φορά που κάποιος νέος πελάτης χρησιμοποιεί το iTunes για να αγοράσει ένα τραγούδι, τότε ένα νέο τυχαίο κλειδί χρήστη δημιουργείται και χρησιμοποιείται για να κρυπτογραφήσει το κύριο κλειδί. Το τυχαίο κλειδί αποθηκεύεται στους εξυπηρετητές της Apple και στέλνεται επίσης και στους iTunes εξυπηρετητές. Το iTunes αποθηκεύει αυτά τα κρυπτογραφημένα κλειδιά και οποιαδήποτε στιγμή είναι σε θέση να τα ανασύρει, να αποκρυπτογραφήσει το κύριο κλειδί, να αποκρυπτογραφήσει την ηχητική ροή και να αναπαράγει το τραγούδι.

Napster music store

Το διαδικτυακό κατάστημα Napster προσφέρει DRM προστασία βασισμένη σε συνδρομή. Οι χρήστες που είναι συνδρομητές μπορούν να κατεβάζουν απεριόριστο πλήθος τραγουδιών, τα οποία είναι σε μορφή WMA (Windows Media Audio) όσο διαρκεί η συνδρομή τους. Όταν όμως η συνδρομή τους λήξει, όλα τα τραγούδια που έχουν κατέβει από το Napster δεν είναι δυνατόν να αναπαραχθούν μέχρι ο χρήστης να ανανεώσει την συνδρομή του. Το Napster επίσης χρεώνει τους χρήστες που επιθυμούν να μεταφέρουν την μουσική τους σε φορητές συσκευές με επιπλέον 5$/μήνα. Η μουσική που αγοράζεται από το Napster μπορεί να αναπαραχθεί σε συσκευές που φέρουν το λογότυπο Microsoft PlaysForSure. Από τον Ιούνιο του 2009, το Napster προσφέρει MP3 αρχεία χωρίς DRM προστασία, η οποία μπορεί να αναπαραχθεί και σε iPod.

Connect

Η εταιρία Sony δημιούργησε μία διαδικτυακή υπηρεσία που ονομάζεται Connect και χρησιμοποιεί την ιδιωτική DRM τεχνολογία OpenMG. Η μουσική που λαμβάνεται από αυτό το κατάστημα (συνήθως μέσω του λογισμικού SonicStage της Sony) είναι δυνατόν να αναπαραχθεί μόνο σε υπολογιστές με λειτουργικό Microsoft Windows και υλισμικό Sony (συμπεριλαμβανομένων του PSP και των τηλεφώνων Sony-Ericsson).

OpenMG

Το OpenMG είναι ένα σύστημα που δημιουργήθηκε από την Sony και υπακούει στις SDMI απαιτήσεις. Σχεδιάσθηκε για αρχεία ήχου σε ATRAC3 μορφή. Το συμβατό λογισμικό (π.χ. SoniStage) είναι συνήθως ικανό να μετατρέπει αρχεία MP3 και WAV σε OpenMG/ATRAC3 μορφή. Οι επεκτάσεις των κρυπτογραφημένων αρχείων είναι συνήθως .omg και .oma. Το OpenMg συντίθεται από τέσσερα μέρη (10):

1. Τεχνολογία για την αυθεντικοποίηση των συσκευών των καταναλωτών και των εγγραφομένων πολυμέσων.
2. Προστασία του ψηφιακού περιεχομένου (π.χ. από μη εξουσιοδοτημένη εγγραφή)
3. Τεχνολογία για τον διαχωρισμό και την διαχείριση του ψηφιακού περιεχομένου και της άδειας χρήσεως του.
4. DRM τεχνολογία για το ψηφιακό περιεχόμενο.

DRM και ψηφιακά βιβλία (ebooks)

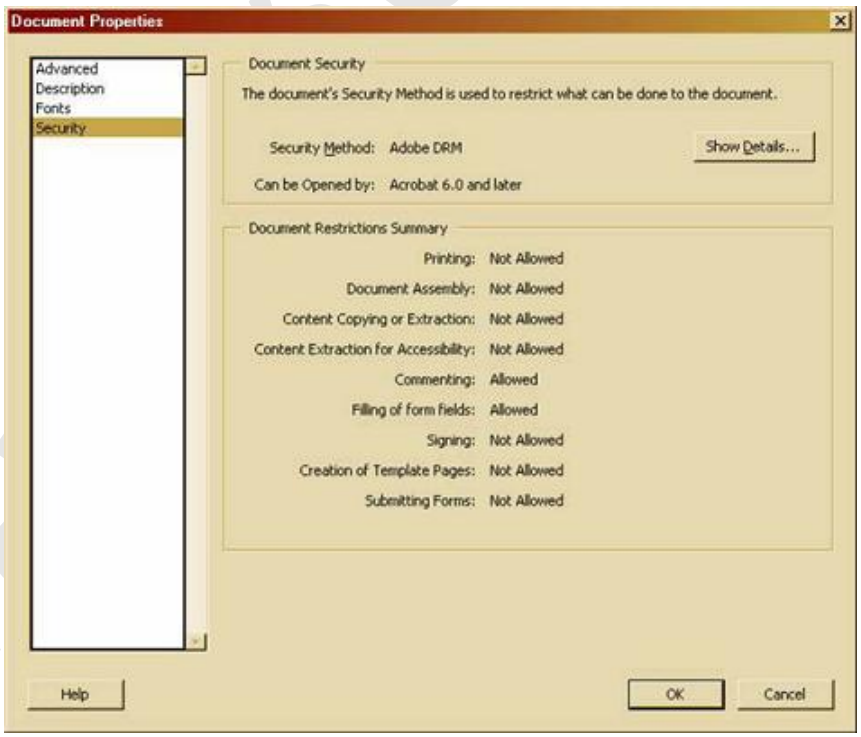
Τα ψηφιακά βιβλία τα οποία διαβάζονται σε έναν υπολογιστή ή έναν αναγνώστη ψηφιακών βιβλίων (e-book reader), χρησιμοποιούν DRM τεχνολογία για τον περιορισμό της αντιγραφής, εκτυπώσεως και την διανομή των βιβλίων. Τα βιβλία συνήθως είναι συμβατά με περιορισμένο αριθμό συσκευών αναγνώσεως. Αρκετοί είναι αυτοί που πιστεύουν ότι η εφαρμογή του DRM στα ψηφιακά βιβλία, κάνει την χρήση τους περίπλοκη (11).

Υπάρχουν τέσσερα κύρια πρότυπα για τα ψηφιακά βιβλία. Mobipocket, Topaz, ePub και PDF. Το Kindle της Amazon χρησιμοποιεί το Mobipocket και το Topaz και επίσης υποστηρίζει το πρότυπο PDF. Άλλοι αναγνώστες χρησιμοποιούν κυρίωςτο ePub αλλά με διαφορετικά DRM σχήματα.

Από πλευράς λογισμικού, δύο είναι τα κύρια προγράμματα σε PC και Macintosh, το Adobe Reader και το Microsoft Reader. Καθένα χρησιμοποιεί διαφορετική προσέγγιση ως προς το DRM. Παρακάτω παρουσιάζονται συνοπτικώς:

Adobe Reader

Η πρώτη έκδοση του Adobe Reader που περιελάμβανε κρυπτογραφία ήταν η 5.05. Σε επόμενη έκδοση (6.0) οι τεχνολογίες του PDF reader και του e-book reader συνδυάστηκαν, επιτρέποντας την ανάγνωση προστατευομένων και μη από DRM βιβλίων (1). Αφού ο χρήστης ανοίξει ένα αρχείο με τον Adobe Reader, είναι σε θέση να δει την δήλωση δικαιωμάτων, η οποία αναφέρει ρητά τις επιτρεπόμενες ενέργειες για αυτό το αρχείο. Για παράδειγμα, ένα μη προστατευόμενο αρχείο, επιτρέπει στον χρήστη την εκτύπωση, αντιγραφή και όλες τις άλλες βασικές λειτουργίες. Σε ένα πιο προστατευμένο βιβλίο ο χρήστης δεν δύναται να αντιγράψει ή να τυπώσει το βιβλίο.



Εικόνα 1 : Δήλωση δικαιωμάτων στον Adobe Reader 6.0

Microsoft Reader

Ο Microsoft Reader, διαβάζει αρχεία που έχουν την επέκταση .lit και έχει το δικό του DRM λογισμικό. Υπάρχουν τρεις διαβαθμίσεις σε σχέση με τις επιτρεπόμενες ενέργειες στα βιβλία : sealed, inscribed και owner exclusive. Τα βιβλία που χαρακτηρίζονται ως sealed, έχουν τους λιγοτέρους περιορισμούς και απλά αποτρέπουν την τροποποίηση του εγγράφου. Στο επόμενο στάδιο διαβαθμίσεως ανήκουν τα βιβλία inscribed. Μετά την αγορά και το κατέβασμα του ψηφιακού βιβλίου, ο Microsoft Reader εισάγει στο βιβλίο μία ψηφιακή ετικέτα ταυτότητος (ID Tag). Με αυτόν τον τρόπο, αποθαρρύνεται η διανομή του βιβλίου, καθώς είναι εύκολο να εντοπιστεί ο αρχικός ιδιοκτήτης του (1). Άλλα λογισμικά χρησιμοποιούν παρόμοια συστήματα. Για παράδειγμα το Palm Digital Media, γνωστό πλέον ως Ereader, συνδέει τις πληροφορίες της πιστωτικής κάρτας του αγοραστή με το βιβλίο, ώστε να αποτρέψει την διανομή του (12).

Η πιο αυστηρή μορφή στον Microsoft Reader, από πλευράς ασφάλειας, ονομάζεται owner exclusive και χρησιμοποιεί παραδοσιακές μεθόδους DRM. Για να αγοράσει το βιβλίο ο χρήστης, πρέπει πρώτα να έχει ανοιχτό τον Microsoft Reader, που διαφυλάσσει ότι όταν κατέβει το βιβλίο θα συνδεθεί με τον λογαριασμό Microsoft Passport[2] του υπολογιστή. Έτσι το βιβλίο μπορεί να αναγνωσθεί μόνο στον υπολογιστή που κατέβηκε αποτρέποντας έτσι την αντιγραφή και την διανομή του.

DRM και παιχνίδια υπολογιστή

Ενδιαφέρον έχει η εφαρμογή του DRM στα παιχνίδια υπολογιστή. Παρακάτω περιγράφονται οι κυριότερες τεχνικές που εφαρμόζονται.

Περιορισμένος αριθμός εγκαταστάσεων

Τα παιχνίδια υπολογιστή χρησιμοποιούν κάποιες φορές το DRM για να ελέγξουν τον αριθμό των συστημάτων που θα εγκατασταθεί το παιχνίδι, απαιτώντας αυθεντικοποίηση με έναν εξυπηρετητή μέσω διαδικτύου. Τα περισσότερα παιχνίδια με αυτόν τον περιορισμό επιτρέπουν τρεις ή πέντε εγκαταστάσεις. Αυτό δεν περιορίζει μόνο τους χρήστες που έχουν παραπάνω από τρεις ή πέντε υπολογιστές στο σπίτι τους, αλλά μπορεί να αποδειχθεί και εμπόδιο σε πιθανές αλλαγές του λειτουργικού συστήματος ή σε κάποιο format του δίσκου, καθώς αναλόγως με τον τρόπο που έχει υλοποιηθεί το DRM, κάθε εγκατάσταση μετράται ως νέα ακόμη και αν είναι στο ίδιο υπολογιστικό σύστημα. Αυτό καθιστά το παιχνίδι άχρηστο μετά από μία χρονική περίοδο ακόμη και αν χρησιμοποιείται μόνο από έναν υπολογιστή. Υλοποίηση των παραπάνω είναι το SecuROM της Sony.

Αρκετά παιχνίδια (Call of Duty 4, Assassin's Creed κ.α.) χρησιμοποιούν την τεχνολογία SafeDisc DRM, η οποία δεν έχει αυθεντικοποίηση μέσω διαδικτύου ή πεπερασμένο αριθμό εγκαταστάσεων.

[2] Microsoft Passport ονομάζεται μία διαδικτυακή υπηρεσία της Microsoft που επιτρέπει στον χρήστη να εισέρχεται σε πολλές ιστοσελίδες χρησιμοποιώντας μόνο έναν λογαριασμό και χωρίς να εισάγει κάθε φορά τα διαπιστευτήριά του.

SafeDisc

Το SafeDisc είναι μια προστασία κατά της αντιγραφής για CD/DVD και ταυτόχρονα ένα DRM πρόγραμμα για Windows. Δημιουργήθηκε από την εταιρία Macrovision. Το SafeDisk προσθέτει μία μοναδική ψηφιακή υπογραφή στο οπτικό μέσο κατά την διάρκεια της δημιουργίας του. Κάθε φορά που πρόγραμμα προστατευόμενο από το SafeDisk τρέχει, το SafeDisk εκτελεί πολλαπλούς ελέγχους ασφαλείας και επαληθεύει ότι η ψηφιακή υπογραφή βρίσκεται στο οπτικό μέσο. Η διαδικασία αυθεντικοποιήσεως διαρκεί περίπου 10 – 20 δευτερόλεπτα. Όταν ολοκληρωθεί η αυθεντικοποίηση, τότε το πρόγραμμα ξεκινάει κανονικά. Η ψηφιακή υπογραφή έχει κατασκευασθεί έτσι ώστε η αντιγραφή-μεταφορά της από το γνήσιο μέσο να είναι δύσκολη.

Κάποια προγράμματα είναι σχεδιασμένα ώστε να τρέχουν κατ' ευθείαν από τον σκληρό δίσκο χωρίς να χρειάζεται πρόσβαση σε αρχεία του CD/DVD μετά την αρχική εγκατάσταση. Το SafeDisk επιτρέπει αυτήν την λειτουργία, αρκεί ο χρήστης να έχει το αυθεντικό CD/DVD στην κατοχή του, που είναι απαραίτητο κάθε φορά που το πρόγραμμα ξεκινάει. Αν δεν τοποθετηθεί το CD/DVD στο drive, τότε το SafeDisk αποτρέπει την λειτουργία του προγράμματος.

Επίμονη αυθεντικοποίηση

Αρκετές μεγάλες εταιρίες στον χώρο των ηλεκτρονικών παιχνιδιών βασίστηκαν στην επίμονη αυθεντικοποίηση των χρηστών μέσω διαδικτύου, κυρίως στα μέσα του 2008 και τις αρχές του 2009. Χαρακτηριστικό είναι το παράδειγμα της πλατφόρμας Uplay της εταιρίας Ubisoft. Το σύστημα δουλεύει έχοντας εγκαταστήσει ένα μέρος του παιχνιδιού στον υπολογιστή του χρήστη, ώστε μόνο τα αρχικά μέρη του παιχνιδιού να είναι άμεσα διαθέσιμα και εν συνέχεια κατεβαίνουν τα υπόλοιπα μέρη καθώς το παιχνίδι εξελίσσεται. Χρειάστηκε λίγο παραπάνω από έναν μήνα από την έκδοση του προγράμματος ώστε να παρακαμφθεί η DRM προστασία του (13).

Διαφθορά λογισμικού (software tampering)

Η εταιρία Bohemia Interactive χρησιμοποίησε μία διαφορετικής μορφής τεχνολογία. Όταν υπήρχε υποψία ότι το παιχνίδι δεν ήταν αυθεντικό, εμφανίζονταν σφάλματα (bugs) στον κώδικα του παιχνιδιού όπως όπλα που έχαναν την ακρίβειά τους. Έτσι το παιχνίδι ουσιαστικά γινόταν άχρηστο για τον χρήστη. Ομοίως η εταιρία Croteam στην περίπτωση του πειρατικού αντιγράφου, αντί να εμφανίζει μηνύματα σφάλματος και να σταματήσει το παιχνίδι, δημιουργούσε έναν αόρατο εχθρό που επιτίθονταν στον παίκτη μέχρι αυτός να χάσει (14).

Ψηφιακό υδατογράφημα

Το ψηφιακό υδατογράφημα (15) είναι ένα ψηφιακό σήμα ή πρότυπο που έχει εισαχθεί μέσα σε ένα αρχείο (ήχου, εικόνας κτλ). Καθώς το σήμα ή πρότυπο είναι παρόν σε κάθε αναλλοίωτο αντίγραφο του αρχικού αρχείου, το υδατογράφημα μπορεί να διαδραματίσει τον ρόλο της ψηφιακής υπογραφής για τα αντίγραφα. Ένα δεδομένο υδατογράφημα ενδέχεται να είναι μοναδικό για κάθε αντίγραφο (π.χ. για την αναγνώριση του επιδιωκομένου παραλήπτη) ή κοινό για όλα τα αντίγραφα (π.χ. για την αναγνώριση του δημιουργού). Σε κάθε περίπτωση, η υδατογράφηση του αρχείου περιλαμβάνει την μετατροπή του σε μία διαφορετική μορφή. Αυτό διαφοροποιεί το ψηφιακό υδατογράφημα από το ψηφιακό αποτύπωμα, όπου το αρχικό αρχείο μένει ανέπαφο και ένα νέο δημιουργείται που περιγράφει το περιεχόμενο του πρώτου.

Το ψηφιακό υδατογράφημα έρχεται σε αντιδιαστολή με την κρυπτογραφία δημοσίου κλειδιού, που επίσης μετατρέπει τα αρχικά αρχεία σε μια άλλη μορφή. Είναι κοινή πρακτική η κρυπτογραφία ψηφιακών αρχείων ώστε να γίνουν μη αναγνώσιμα χωρίς το κλειδί αποκρυπτογραφήσεως. Εν αντιθέσει με την κρυπτογραφία, το υδατογράφημα αφήνει το αρχικό αρχείο σχεδόν ανέπαφο και αναγνωρίσιμο. Επιπροσθέτως, το υδατογράφημα, όπως και οι υπογραφές, ενδέχεται να μην επαληθεύεται χωρίς την χρήση συγκεκριμένου λογισμικού. Επίσης, τα κρυπτογραφημένα αρχεία, αφού αποκρυπτογραφηθούν χάνουν ουσιαστικά την προστασία τους ενώ το υδατογράφημα έχει σχεδιαστεί ώστε να είναι παρόν στην θέαση, εκτύπωση και επαναπροώθηση του αρχείου.

Στοιχεία που αποτελούν το υδατογράφημα

Το σύστημα υδατογραφήσεως μπορεί να φανεί σαν ένα τηλεπικοινωνιακό σύστημα που αποτελείται από τρία μέρη: έναν εμφυτευτή, έναν δίαυλο επικοινωνίας και έναν ανιχνευτή. Οι πληροφορίες του υδατογραφήματος, εμφυτεύονται στο ίδιο το σήμα, αντί να τοποθετηθούν στην επικεφαλίδα του αρχείου ή με την χρήση κρυπτογραφίας όπως γίνεται σε άλλες τεχνικές ασφαλείας, με τέτοιο τρόπο ώστε να είναι εξαγώγιμο από τον ανιχνευτή. Πιο συγκεκριμένα, οι πληροφορίες του υδατογραφήματος εμφυτεύονται στο αρχικό σήμα προτού αυτό μεταδοθεί από τον δίαυλο επικοινωνίας, έτσι ώστε να είναι αναγνώσιμο από τον ανιχνευτή στο σημείο λήψεως.

Είδη υδατογραφήματος

Τα υδατογραφήματα και οι τεχνικές υδατογραφήσεως, μπορούν να χωριστούν σε διάφορες κατηγορίες. Οι τεχνικές υδατογραφήσεως μπορούν να χωριστούν σε τέσσερις κατηγορίες αναλόγως με τον τύπο του αρχείου που υδατογραφείται (κειμένου, εικόνας, αρχείου ήχου, αρχείου βίντεο). Διαφορετικά μπορούμε να ταξινομήσουμε τα υδατογραφήματα ακολούθως (16):

- Ορατό υδατογράφημα, το οποίο χρησιμοποιείται κυρίως για να δηλώσει στον υποψήφιο χρήστη ότι το προϊόν προστατεύεται νομικά. Με αυτό τον τρόπο, είναι πιθανό να αποφευχθεί η παραβίαση των πνευματικών δικαιωμάτων και από χρήστες οι οποίοι κατά λάθος θα έκαναν αυτή τη διαδικασία. Ο πιο συνηθισμένος χώρος χρήσης του είναι σε μια ψηφιακή εικόνα.
- Αόρατο υδατογράφημα, το οποίο χρησιμοποιείται για την ανίχνευση κυρίως μιας παράνομης εμπορικής συναλλαγής. Τοποθετούνται σε αρχεία ψηφιακής μορφής

όπως βίντεο ή εικόνες, έχοντας ενσωματωθεί στο συγκεκριμένο υλικό αρχικά. Επίσης θα πρέπει να είναι ανθεκτικά ώστε να αντέχουν στις επιθέσεις που πιθανόν να γίνονται από κάποιους χρήστες.

- Ανθεκτικό υδατογράφημα, το οποίο επίσης χρησιμοποιείται σε παράνομες εμπορικές συναλλαγές ενός αντικειμένου πολλαπλού μέσου, όπως μιας ψηφιακής εικόνας, βίντεο ή ήχο. Η ιδιότητα αυτών των υδατογραφημάτων είναι ότι μπορούν να αντέχουν σε αρκετές μορφές επεξεργασίας εικόνας και ήχου, όπως είναι η συμπίεση, η χρήση κατωπερατού φίλτρου, οι γεωμετρικές μετατροπές της εικόνας και άλλα. Αρχικός σκοπός αυτού του υδατογραφήματος είναι να μην μπορεί να γίνει παράνομη χρήση του αντικειμένου. Ακόμα, όμως, και αν καταφέρει κάποιος χρήστης να αφαιρέσει ή έστω να διεστραβλώσει αρκετά το αντικείμενο, τότε αυτό θα έχει υποστεί τέτοια καταστροφή ώστε να μην μπορεί να γίνει εμπορικά εκμεταλλεύσιμη. Τα ανθεκτικά υδατογραφήματα συνήθως είναι και αόρατα. Επίσης υπάρχει και αντιστρόφως ανάλογη σχέση ανάμεσα στην ανθεκτικότητα και την ποιότητα της ψηφιακής εικόνας.
- Μη ανθεκτικό υδατογράφημα, το οποίο χρησιμοποιείται με έναν άλλο τρόπο. Πιο συγκεκριμένα σε ένα ψηφιακό αντικείμενο ενσωματώνεται αυτό το υδατογράφημα που είναι και αόρατο και μη ανθεκτικό, οπότε αν κάποιος χρήστης προσπαθήσει και εν τέλει καταφέρει να διεστραβλώσει το ψηφιακό αντικείμενο, τότε αυτό δεν θα μπορεί να είναι εμπορικά εκμεταλλεύσιμο.

Τεχνικές υδατογραφήσεως

Υπάρχουν διάφορες τεχνικές για την εφαρμογή της υδατογραφήσεως στο χωρικό πεδίο. Η απλούστερη (συνήθως πολλή απλή για τις περισσότερες εφαρμογές) είναι η εναλλαγή (από 0 σε 1 και αντίστροφα) των λιγότερο σημαντικών δυφίων επιλεγμένων εικονοστοιχείων μίας εικόνας. Αυτό λειτουργεί όταν η εικόνα δεν υφίσταται καμμία τροποποίηση. Μία πιο ανθεκτική υδατογράφηση μπορεί να πραγματοποιηθεί με την υπέρθεση ενός συμβόλου σε μία περιοχή της εικόνας. Το αποτέλεσμα ενδέχεται να είναι ορατό ή μη, αναλόγως με την ένταση του συμβόλου. Η περικοπή εικόνας (συνηθισμένη εργασία στην επεξεργασία) μπορεί να χρησιμοποιηθεί για την απαλοιφή του υδατογραφήματος.

Χωρική υδατογράφηση

Η χωρική υδατογράφηση μπορεί επίσης να εφαρμοστεί χρησιμοποιώντας διαχωρισμό χρωμάτων. Με αυτόν τον τρόπο, το υδατογράφημα εμφανίζεται μόνο σε ένα από το σύνολο των χρωμάτων. Αυτό καθιστά το υδατογράφημα αισθητά δυσδιάκριτο καθώς είναι δύσκολο να γίνει αντιληπτό στο ανθρώπινο μάτι. Παρ' όλα αυτά, γίνεται αμέσως αντιληπτό όταν τα χρώματα διαχωρίζονται για την εκτύπωση. Αυτό καθιστά το αρχείο άχρηστο για εκτύπωση, εκτός αν είναι εφικτή η αφαίρεση του υδατογραφήματος από το σύνολο των χρωμάτων. Αυτή η προσέγγιση χρησιμοποιείται εμπορικά από δημοσιογράφους για να επιθεωρήσουν ψηφιακές εικόνες πριν την αγορά τους.

Υδατογράφηση συχνοτήτων

Η υδατογράφηση μπορεί να εφαρμοστεί στο τοπίο συχνοτήτων εφαρμόζοντας πρώτα ένα μετασχηματισμό όπως ο γρήγορος μετασχηματισμός Fourier (Fast Fourier Transform - FFT). Με έναν παρεμφερή τρόπο με την χωρική υδατογράφηση, οι αξίες των επιλεγμένων συχνοτήτων μπορούν να αλλαχθούν σε σχέση με τις αρχικές. Καθώς οι υψηλές συχνότητες

θα χαθούν κατά την συμπίεση ή την διαβάθμιση, το σήμα υδατογραφήσεως εφαρμόζεται στις χαμηλές συχνότητες, ή καλλίτερα εφαρμόζεται στις συχνότητες που περιέχουν τις πιο σημαντικές πληροφορίες για την αρχική εικόνα. Καθώς τα υδατογραφήματα που εφαρμόζονται με την μέθοδο συχνοτήτων, διασκορπίζονται σε όλο το χωρικό πεδίο κατά τους αντιστρόφους μετασχηματισμούς, αυτή η μέθοδος δεν είναι ευπαθής στην περικοπή εικόνων όπως η χωρική υδατογράφηση. Παρ' όλα αυτά υπάρχει μία αντιστρόφως ανάλογη σχέση ανάμεσα στην αορατότητα και αποκωδικοποίηση καθώς το υδατογράφημα εφαρμόζεται αδιάκριτα σε όλο το χωρικό πεδίο.

Ο παρακάτω πίνακας (15) δείχνει την σύγκριση ανάμεσα στις δύο τεχνικές:

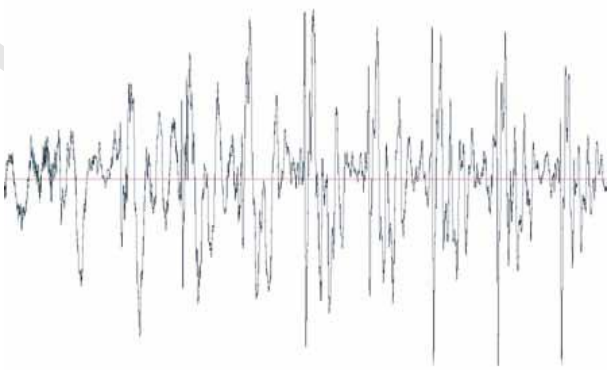
	Χωρική υδατογράφηση	**Υδατογράφηση συχνοτήτων**
Υπολογιστικό κόστος	Χαμηλό	Υψηλό
Ανθεκτικότητα	Χαμηλή	Υψηλότερη
Αντιληπτική Ποιότητα	Υψηλός έλεγχος	Χαμηλός
Χωρητικότητα	Υψηλή (αναλόγως με το μέγεθος του αρχείου)	Χαμηλή
Παράδειγμα εφαρμογής	Κυρίως αυθεντικοποίηση	Πνευματικά δικαιώματα

Πίνακας 1 : Σύγκριση ανάμεσα σε χωρική και υδατογράφηση συχνοτήτων

Δακτυλικό αποτύπωμα

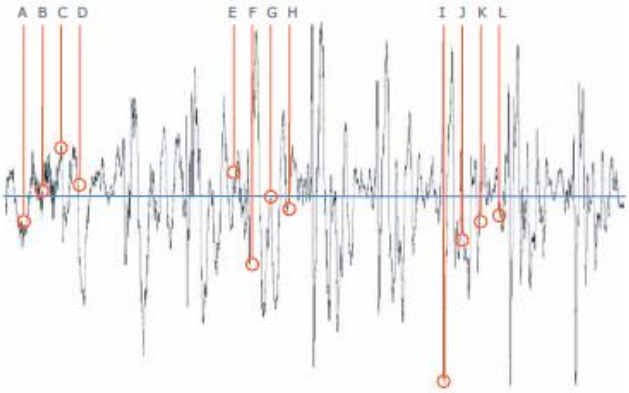
Το δακτυλικό αποτύπωμα (17) (fingerprinting) είναι μία τεχνική ταυτοποιήσεως ψηφιακού περιεχομένου. Ο σκοπός, το περιεχόμενο και η υλοποίηση του δακτυλικού αποτυπώματος είναι αρκετά διαφορετικά από αυτά της υδατογραφήσεως. Η υδατογράφηση στηρίζεται στην ενσωμάτωση πληροφοριών μέσα σε ένα αρχείο (ήχου, εικόνας κτλ), τις οποίες έπειτα χρησιμοποιεί για να αναγνωρίσει το περιεχόμενο του αρχείου. Το αποτύπωμα δεν ενσωματώνει κανενός είδους πληροφορία αλλά αναλύει το αρχείο ώστε να εξάγει τα μοναδικά χαρακτηριστικά του περιεχομένου. Το αναγνωρισμένο πλέον πρότυπο του αρχείου αποθηκεύεται σε μία βάση δεδομένων και μπορεί να χρησιμοποιηθεί για μελλοντική αναγνώριση του αρχείου.

Η παρακάτω εικόνα (17) αναπαριστά την ηχητική κυματομορφή ενός συγκεκριμένου αρχείου μουσικής.



Εικόνα 2 : Κυματομορφή ενός αρχείου μουσικής

Το σύστημα του αποτυπώματος χρειάζεται να δημιουργήσει μία βάση δεδομένων που να μπορεί να χρησιμοποιηθεί για να ταυτοποιήσει ένα συγκεκριμένο μέρος περιεχομένου. Ένας τρόπος για να επιτευχθεί αυτό είναι να αποθηκεύσουμε ολόκληρα αρχεία μουσικής στην βάση και να συγκρίνουμε κάθε αρχείο που συναντάμε με αυτά. Αυτή η λύση θα ήταν λειτουργική αλλά θα χρειάζονταν αρκετός χρόνος για την σύγκριση και το μέγεθος της βάσεως δεδομένων θα ήταν πολύ μεγάλο. Αν προσπαθήσουμε να κάνουμε το ίδιο και για τα αρχεία βίντεο, τότε το μέγεθος της βάσεως θα ήταν ακόμη μεγαλύτερο. Έτσι, αντί για ολόκληρο το αρχείο, αποθηκεύουμε ένα στατιστικό δείγμα του αρχείου. Για παράδειγμα, μπορούμε να λαμβάνουμε τέσσερα δείγματα κάθε δέκατο του δευτερολέπτου, όπως φαίνεται και στην παρακάτω εικόνα (17).



Εικόνα 3 : Δειγματοληψία σε αρχείο ήχου

Ας υποθέσουμε ότι η δειγματοληψία συνεχίζεται κατ' αυτόν τον τρόπο σε όλη την κυματομορφή. Αν το πηγαίο αρχείο είναι ένα τραγούδι διαρκείας δύο λεπτών, το αποτύπωμα θα έχει παραπάνω από 4000 δείγματα και παρ' όλα αυτά θα είναι χίλιες φορές μικρότερο σε μέγεθος από το πηγαίο αρχείο. Αυτό συμβαίνει γιατί αν το πηγαίο αρχείο είχε συχνότητα δειγματοληψίας 48kHz, σημαίνει ότι θα είχε 48000 δείγματα ανά δευτερόλεπτο. Το αποτύπωμα λαμβάνει δείγματα 40 φορές το δευτερόλεπτο, δηλαδή είναι 1000 και πλέον φορές μικρότερο σε μέγεθος. Αυτά τα δείγματα συνιστούν μία μοναδική υπογραφή που αντιστοιχεί στο συγκεκριμένο αρχείο. Οποιοδήποτε άλλο αρχείο ήχου θα είχε άλλα πρότυπα δειγμάτων. Όπως τα πραγματικά δακτυλικά αποτυπώματα δεν λένε στην αστυνομία για το πώς μοιάζουν οι κακοποιοί, έτσι και τα αποτυπώματα δεν μαρτυρούν το περιεχόμενο του αρχείου. Απλώς επιτρέπουν την μοναδική ταυτοποίησή του.

Το αποτύπωμα δημιουργείται από μία σειρά ασυμπιέστων πλαισίων. Το αποτύπωμα μπορεί να ενσωματώσει μεταδεδομένα σχετικά με το αρχείο, μαζί με το πρότυπο του αποτυπώματος. Σε αντίθεση με το υδατογράφημα, όπου η εφαρμογή της υδατογραφήσεως παράγει ένα αρχείο ασυμπιέστων πλαισίων (όπου το παραγόμενο αρχείο είναι μεγάλο σε μέγεθος ακόμη και μετά την συμπίεση), το αποτύπωμα δεν είναι ένα θεάσιμο αρχείο πολυμέσων αλλά ένα πολύ μικρότερο αρχείο που κληρονομεί τα χαρακτηριστικά του περιεχομένου του αρχείου.

Τα αποτυπώματα βίντεο αρχείων είναι ανεξάρτητα από την ανάλυση ή το είδος του αρχείου βίντεο. Μπορούν να χρησιμοποιηθούν για να ταυτοποιήσουν ολόκληρα βίντεο, τμήματα αυτών, ακόμη και πολύ μικρά μέρη του βίντεο. Το αποτύπωμα μπορεί επίσης να

χρησιμοποιηθεί για την αναγνώριση περιεχομένου βίντεο που έχει επεξεργασθεί, όπως για παράδειγμα η χρήση μέρους του βίντεο για την δημιουργία ενός μεγαλυτέρου βίντεο. Ένας από του τρόπους που οι «πειρατές» κλέβουν ταινίες είναι με την παράνομη μαγνητοσκόπηση της ταινίας απ' ευθείας από την οθόνη του κινηματογράφου. Ακόμη και με αυτόν τον τρόπο, το αποτύπωμα είναι σε θέση να αναγνωρίσει το βίντεο.

Δυστυχώς, τα αποτυπώματα αρχείων ήχου, δεν είναι τόσο ανθεκτικά στην παραποίηση όσο τα αποτυπώματα αρχείων βίντεο. Είναι σχετικά εύκολο να τροποποιηθεί ή να αντικατασταθεί πλήρως ένα αρχείο ήχου. Για παράδειγμα, νέα τραγούδια συνήθως συνοδεύουν μικτά αρχεία βίντεο ή πειρατικές ταινίες που κυκλοφορούν σε ξένες χώρες με διαλόγους σε διαφορετική γλώσσα. Έτσι η αναγνώριση περιεχομένου βασισμένη εξ ολοκλήρου σε αρχεία ήχου ενδέχεται να είναι προβληματική.

Μεταδεδομένα

Ο όρος μεταδεδομένα χρησιμοποιείται για να περιγράψει τα δεδομένα των δεδομένων, όλα εκείνα τα δεδομένα δηλαδή που μας βοηθούν να εξάγουμε πληροφορίες για ένα αρχείο. Τέτοια δεδομένα ενδέχεται να είναι ημερομηνία δημιουργίας, το όνομα του δημιουργού, το λογισμικό που δημιούργησε το αρχείο, περιγραφή του περιεχομένου ώστε να διευκολύνεται η αναζήτηση κ.α.

Η κύρια διαφορά μεταξύ μεταδεδομένων και υδατογραφήματος είναι ότι το υδατογράφημα προστίθεται στο αρχείο χωρίς, τις περισσότερες φορές, να είναι φανερό και δεν επηρεάζει το μέγεθός του. Τα μεταδεδομένα υπάρχουν στο ίδιο το αρχείο, αλλά ξεχωριστά από το περιεχόμενό του και τις περισσότερες φορές είναι ορατά χωρίς την χρήση κάποιου ειδικού λογισμικού. Χαρακτηριστικό παράδειγμα είναι τα μεταδεδομένα που χρησιμοποιούνται στα πολυμέσα που αγοράζονται από το iTunes store της Apple για τις εκδόσεις που φέρουν ή μη DRM προστασία. Αυτές οι πληροφορίες περιλαμβάνονται ως μεταδεδομένα του προτύπου MPEG και φέρουν το όνομα του αγοραστή καθώς και το μοναδικό αναγνωριστικό του από την Apple.

Γλώσσες Εκφράσεως Δικαιωμάτων – Rights Expression Languages

Ο έλεγχος στον Adobe Reader και στον Microsoft Reader όπως είδαμε προηγουμένως είναι εμφανώς περιορισμένος. Περιορίζει την πρόσβαση στο αρχείο και δίνει δυνατότητα για κάποιες λειτουργίες όπως η εκτύπωση ή η αντιγραφή μερών του αρχείου. Όμως η ψηφιακή διαχείριση των πνευματικών δικαιωμάτων έχει ανάγκη τεχνικές ελέγχου που να δίνουν την δυνατότητα στον εκδότη του αρχείου για έναν πιο λεπτομερή και σύνθετο τρόπο ελέγχου χρήσεως. Αυτόν τον ρόλο αναλαμβάνουν οι Γλώσσες Εκφράσεως Δικαιωμάτων (Rights Expression Languages – REL).

Μία REL είναι ουσιαστικά μία υψηλού επιπέδου γλώσσα υπολογιστή, η οποία δύναται να εκφράσει ανθρώπινες εντολές για μεταγλώττιση, χωρίς αμφισημία και με έναν ασφαλή τρόπο σε μία υπολογιστική μηχανή. Οι εντολές αφορούν τις επιτρεπόμενες λειτουργίες από τον ιδιοκτήτη ενός αρχείου προς τον χρήστη. Ο πρωτεύων στόχος μίας REL είναι να ενεργοποιήσει ένα από άκρο σε άκρο DRM σύστημα για τον έλεγχο (όσο καιρό αυτός χρειάζεται) και την χρήση προστατευομένων αρχείων που μετακινούνται σε δίκτυα και είναι προσβάσιμα από χρήστες (18).

Πρακτικά τα παραπάνω σημαίνουν ότι ο κάτοχος των πνευματικών δικαιωμάτων μπορεί να μετατρέψει την ανθρωπίνως αναγνώσιμη άδεια χρήσεως (π.χ. μπορείς να αντιγράψεις το αρχείο στον σκληρό δίσκο και να το αναπαράγεις ως δέκα φορές) σε μία λογική γλώσσα που ένα πρόγραμμα υπολογιστή καταλαβαίνει και μεταγλωττίζει χωρίς αμφισημία. Αυτό μπορεί να γίνει από ένα σύστημα εφαρμογής (DRM) που προστατεύει το περιεχόμενο στο οποίο ο χρήστης επιθυμεί να έχει πρόσβαση, ώστε ο κάτοχος των πνευματικών δικαιωμάτων να είναι σίγουρος ότι η άδεια χρήσεως τηρείται.

Οι REL είναι γραμμένες σε γλώσσα XML (eXtensible Markup Language), η οποία μπορεί να διαβαστεί απ' ευθείας από ανθρώπους καθώς και από υπολογιστές. Η XML συχνά καλείται ως η γλώσσα του Ιστού και είναι ευρέως χρησιμοποιούμενη ως η βάση των γλωσσών εκφράσεως δικαιωμάτων καθώς διακρίνεται για την διαλειτουργικότητά της.

Πρέπει να τονιστεί ότι οι REL δεν είναι ένας τρόπος εκφράσεως των νόμων περί πνευματικής ιδιοκτησίας και ούτε έχουν κάποια νομική ισχύ. Παρακάτω παρουσιάζονται συνοπτικά οι γνωστότερες γλώσσες εκφράσεως δικαιωμάτων.

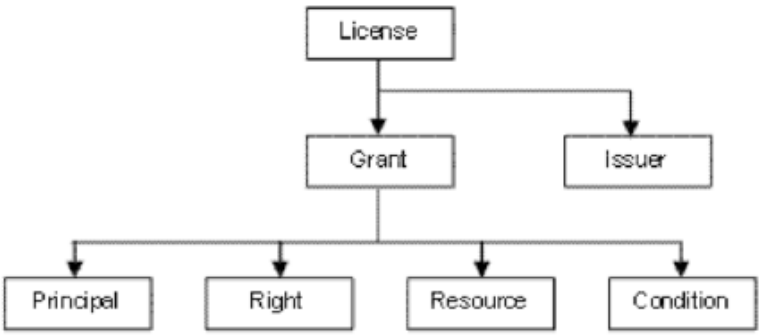
ISO REL (ISO/IEC21000/5:2004)

Η ISO REL είναι βασισμένη στην γλώσσα XrML και είναι δημιούργημα του αμερικάνου επιστήμονα τεχνητής νοημοσύνης Mark Stefik, που την όρισε ως γλώσσα εκφράσεως ψηφιακών δικαιωμάτων, στο Xerox Parc στις αρχές του 1990. Από τότε, η γλώσσα μετακωδικοποιήθηκε σε XML και παρέχει την βάση για το διεθνές πρότυπο ISO/IEC21000/5 που αναπτύχθηκε από το Moving Picture Expert Group (MPEG).

Η ISO REL έχει ένα απλό και επεκτάσιμο μοντέλο για πολλές από τις έννοιες-κλειδιά και τα στοιχεία που την απαρτίζουν. Το μοντέλο δεδομένων περιλαμβάνει τέσσερις βασικές οντότητες. Αυτές οι οντότητες σχηματίζουν το σύνολο. Κατασκευαστικά το σύνολο αποτελείται από τα εξής στοιχεία:

- Την αρχή για την οποία έχει εκδοθεί η παραχώρηση δικαιωμάτων
- Τα δικαιώματα που η παραχώρηση ορίζει
- Οι πόροι πάνω στους οποίους εφαρμόζονται τα δικαιώματα της παραχωρήσεως
- Η κατάσταση η οποία συναντάται πρώτου τα δικαιώματα μπορέσουν να ασκηθούν

Από μόνη της, η παραχώρηση δικαιωμάτων (grant) δεν είναι μία ολοκληρωμένη έκφραση δικαιωμάτων που μπορεί να μεταφερθεί μονοσήμαντα από ένα μέρος σε ένα άλλο. Μία πλήρης έκφραση δικαιωμάτων ονομάζεται άδεια χρήσεως (license). Για είναι λειτουργική μία τυπική άδεια, συνήθως αποτελείται από περισσότερες από μια παραχωρήσεις δικαιωμάτων και ένα εκδότη (issuer), που ταυτοποιεί την πλευρά που εξέδωσε την άδεια. Αυτή η πλευρά κατά πάσα πιθανότητα θα είναι ο ιδιοκτήτης του περιεχομένου. Μια τυπική άδεια φαίνεται στο παρακάτω σχήμα (18) :



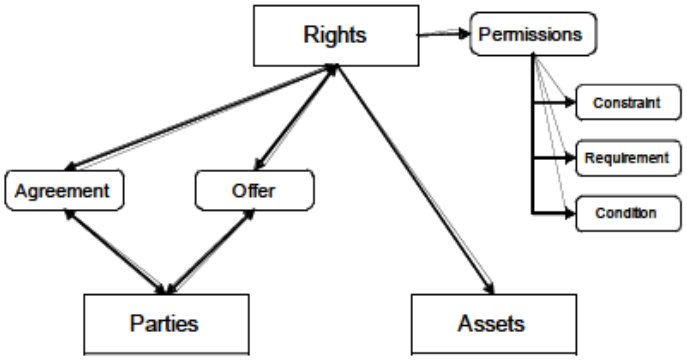
Εικόνα 4 : Ένα τυπικό μοντέλο δεδομένων της ISO REL

Open Digital Rights Language (ODRL)

Η ODRL δημιουργήθηκε από τον Αυστραλό επιστήμονα, Dr Renato Iannella. Δημοσιεύθηκε τον Νοέμβριο του 2001 (έκδοση 1.0). Η ODRL έχει το δικό της υποκείμενο μοντέλο, το οποίο είναι ελαφρώς πιο πολύπλοκο αλλά αρκετοί υποστηρίζουν ότι είναι πιο εύκολο στην κατανόηση από αυτό της ISO REL. Το μοντέλο έχει τρία θεμελιώδη εννοιολογικά στοιχεία:

- Δικαιώματα (Rights)
- Μέρη (Parties)
- Αγαθά (Assets)

Εν αντιθέσει με την ISO REL, δεν διατυπώνει καταστάσεις (conditions) ως ένα από τα βασικά στοιχεία της, αλλά περιλαμβάνει κατάστασεις-περιορισμούς-απαιτήσεις ως ένα υποσύνολο των επιτρεπομένων λειτουργιών (permissions), που με την σειρά τους είναι ένα υποσύνολο των δικαιωμάτων. Η ακόλουθη εικόνα (18) αναπαριστά αυτό το μοντέλο:



Εικόνα 5 : Τυπικό μοντέλο ODRL

Τα αγαθά μπορούν να αντιπροσωπεύουν οποιοδήποτε περιεχόμενο ή οποιοδήποτε υποσύνολο περιεχομένου (π.χ. ένα κεφαλαίο βιβλίου, ένα τραγούδι ή ένα βιβλίο ή ένα ολόκληρο δίσκο ήχου) που μπορεί να αναγνωριστεί μοναδικά. Τα αγαθά μπορούν να είναι είτε ψηφιακά είτε φυσικά.

Τα δικαιώματα περιέχουν επιτρεπόμενες λειτουργίες. Οι προδιαγραφές προτείνουν 21 διαφορετικούς τύπους επιτρεπομένων λειτουργιών (ενώ η ISO REL έχει μόνο 14), όπως εκτύπωση, τροποποίηση, πώληση, μετακίνηση και διαγραφή, ενοποιημένες σε τέσσερις κατηγορίες ώστε να ομαδοποιηθούν παρεμφερείς λειτουργίες (χρήση, επαναχρησιμοποίηση, μεταφορά και διαχείριση αγαθών). Με την σειρά τους αυτές οι επιτρεπόμενες λειτουργίες διέπονται από περιορισμούς, οι οποίοι χωρίζονται σε έξι κατηγορίες (χρήστης, συσκευή, όρια, δικαιώματα, αγαθά και στόχος). Τέλος οι επιτρεπόμενες λειτουργίες περιορίζονται από τις προϋποθέσεις (requirements) των μερών που εκτελούν τις επιτρεπόμενες λειτουργίες και καταστάσεις που είναι εξαιρέσεις, ώστε να ελεγχθούν επιτρεπόμενες λειτουργίες όπως συνθήκες που πρέπει να εκτελεστούν σε συγκεκριμένο χρονικό διάστημα.

Τέλος ως μέρος ορίζεται κάθε οντότητα που παραχωρεί δικαιώματα ή επωφελείται από αυτά. Ως μέρος μπορεί να λογισθεί είτε ανθρώπινος παράγων είτε μία συσκευή.

XrML v1.2

Όπως αναφέρθηκε παραπάνω, η ISO REL χρησιμοποίησε την XrML v.2 ως βάση για την τεχνολογία της. Παρ' όλα αυτά, μία προηγούμενη έκδοση είχε υιοθετηθεί από την Microsoft ως η γλώσσα δικαιωμάτων ενσωματωμένη στο βασισμένο σε εξυπηρετητή σύστημα Rights Management Services (RMS). Το RMS αρχικά στόχευε στην εταιρική αγορά, δίνοντας στην εταιρία ισχυρό έλεγχο πάνω στις επιτρεπόμενες λειτουργίες που συσχετίζονταν με τα εταιρικά έγγραφα (18).

Το RMS εξέδιδε μία άδεια η οποία έπρεπε να αυθεντικοποιηθεί στον εξυπηρετητή ώστε ο χρήστης να έχει πρόσβαση στο έγγραφο. Με αυτόν τον τρόπο, η εταιρία μπορεί να περιορίσει την πρόσβαση του χρήστη, να λήξει τον χρόνο προσβάσεως ή ακόμη και να αποτρέψει την αντιγραφή και την επικόλληση συγκεκριμένων μερών πληροφορίας.

Νομοθεσία

Η ψηφιακή διαχείριση πνευματικών δικαιωμάτων απέκτησε νομικό υπόβαθρο με την υλοποίηση της συνθήκης WIPO[3] Copyright Treaty (WCT), το 1996. Το άρθρο 11 υποχρεώνει τα κράτη μέλη της συνθήκης να ενεργοποιήσουν νόμους ενάντια στην παράκαμψη των μέτρων DRM.

Η συνθήκη WCT έχει υλοποιηθεί στα περισσότερα κράτη μέλη του WIPO. Η αμερικανική υλοποίηση είναι ο νόμος Digital Millennium Copyright Act, ενώ στην Ευρώπη η συνθήκη υλοποιήθηκε το 2001 με την ευρωπαϊκή οδηγία για την πνευματική ιδιοκτησία, που απαιτεί από τις χώρες της Ευρωπαϊκής Ενώσεως να υλοποιήσουν νομική προστασία ενάντια στην παράκαμψη των τεχνολογικών μέτρων DRM. Το 2006, η γαλλική βουλή υιοθέτησε την νομοθεσία ως μέρος του επιμάχου νόμου DADVSI, αλλά προσέθεσε ότι οι DRM τεχνικές θα πρέπει να επιτρέπουν την διαλειτουργικότητα των συστημάτων, μία κίνηση που προκάλεσε αντιπαράθεση στις Ηνωμένες Πολιτείες Αμερικής.

Digital Millennium Copyright Act

Ο νόμος Digital Millennium Copyright Act (19) (DMCA) είναι μία προσθήκη στον αμερικανικό νόμο για την προστασία της πνευματικής ιδιοκτησίας. Εγκρίθηκε στις 14 Μαΐου του 1998 και ποινικοποιεί την παραγωγή και την διάδοση τεχνολογίας που επιτρέπει στους χρήστες να παρακάμψουν τεχνικές μεθόδους που αποτρέπουν την αντιγραφή ψηφιακών έργων. Σύμφωνα με τον νόμο, η παράκαμψη τεχνολογικών μέτρων που ελέγχουν την πρόσβαση σε ένα έργο είναι παράνομη, αν γίνει με σκοπό την παραβίαση των δικαιωμάτων των δικαιούχων του έργου.

Η αντίστροφη μηχανική (reverse engineering) συστημάτων επιτρέπεται ρητά, σύμφωνα με τον νόμο, υπό συγκεκριμένες προϋποθέσεις και συγκεκριμένα για να γίνει εφικτή η διαλειτουργικότητα με άλλα λογισμικά. Τα προγράμματα ανοιχτού κώδικα που αποκωδικοποιούν περιεχόμενο κωδικοποιημένο με CSS και άλλες τεχνικές κρυπτογραφήσεως, αποτελούν ένα ζήτημα στην εφαρμογή του νόμου. Επιτρέπεται η χρήση τους για την εφαρμογή διαλειτουργικότητος ανάμεσα σε λογισμικά ανοιχτού κώδικα και σε λογισμικού κλειστού κώδικα, αλλά χαρακτηρίζεται παράνομη η διανομή τους, όταν προορίζεται για παραβίαση της πνευματικής ιδιοκτησίας.

Ελληνική νομοθεσία

Στην ελληνική νομοθεσία, ο νόμος που προστατεύει στην πνευματική ιδιοκτησία είναι 2121/93 (ΦΕΚ Α' 25/4-3-1993). Στο άρθρο 1, ο 2121/93 ορίζει ότι τα αποκλειστικά και απόλυτα δικαιώματα ενός έργου έχουν οι πνευματικοί δημιουργοί, καθώς και το δικαίωμα της προστασίας του προσωπικού τους δεσμού προς αυτό αλλά και της εκμεταλλεύσεως αυτού. Στο άρθρο 3, ο νόμος αναφέρει ότι το περιουσιακό δικαίωμα δίνει στους δημιουργούς την εξουσία να επιτρέπουν ή να απαγορεύουν την εγγραφή (άμεση ή έμμεση), την προσωρινή ή μόνιμη αναπαραγωγή των έργων τους με οποιοδήποτε μέσο και μορφή, εν όλω ή εν μέρει.

[3] World Intellectual Property Organization

Με τον ορισμό του έργου στο άρθρο 2, ο νόμος περιλαμβάνει και όλα τα πολυμέσα (τραγούδια, βίντεο κτλ.) αφού ως έργο ορίζει «κάθε πρωτότυπο πνευματικό δημιούργημα λόγου, τέχνης ή επιστημής που εκφράζεται με οποιαδήποτε μορφή, ιδίως … τα οπτικοακουστικά έργα …». Ο παραπάνω νόμος, έχει ειδικό άρθρο για τα προγράμματα υπολογιστή (άρθρο 2, παρ. 3), τα οποία θεωρούνται ως έργου λόγου και προστατεύονται από τις διατάξεις περί πνευματικής ιδιοκτησίας.

Στο άρθρο 29 ορίζεται ως διάρκεια της πνευματικής ιδιοκτησίας ενός έργου, η διάρκεια της ζωής του δημιουργού και εβδομήντα (70) έτη μετά τον θάνατο του. Στα ψηφιακά αρχεία και κυρίως στα προγράμματα υπολογιστών, η διάρκεια αυτή αποτρέπει την δημιουργικότητα καθώς ένα πρόγραμμα ηλεκτρονικών υπολογιστών μετά το πέρας μία πενταετίας θεωρείται ξεπερασμένο και συνήθως τίθεται σε αχρηστία.

Τέλος, ο νόμος επιτρέπει την παράκαμψη των τεχνολογικών μέτρων μόνο για τα προγράμματα υπολογιστή υπό προϋποθέσεις, καθώς επιτρέπεται στον νόμιμο χρήστη αντιγράφου η παράκαμψη για να εξασφαλισθεί η διαλειτουργικότητα ενός ανεξάρτητα δημιουργηθέντος προγράμματος με άλλα προγράμματα.

Επιπλέον η ελληνική νομοθεσία προσάρμοσε το εθνικό νομοθετικό πλαίσιο στις ρυθμίσεις της Οδηγίας 2001/29 με το άρθρο 81 Ν.3057/2002 (ΦΕΚ Α΄ 239/10-10-2002). Αξίζει να παρατηρηθεί ότι η Ελλάδα ήταν το πρώτο κράτος μέλος της Ευρωπαϊκής Ένωσης που ολοκλήρωσε τη διαδικασία εναρμόνισης μέσα στην προβλεπόμενη προθεσμία (22-12-2002). Είναι επίσης αξιοσημείωτο ότι τα δικαιώματα και ορισμένοι από τους μηχανισμούς προστασίας που προβλέπονται στην Οδηγία 2001/29 είχαν καθιερωθεί από την ελληνική έννομη τάξη πριν από την εναρμόνιση (20).

Στη συνέχεια η χώρα μας κύρωσε τις δύο Συνθήκες Internet με δύο νόμους που ψηφίστηκαν από το Ελληνικό Κοινοβούλιο το έτος 2003 (Ν. 3183/2003 ΦΕΚ Α΄ 227/26-9-2003 και Ν.3184/2003 και ΦΕΚ Α΄ 228/26.9.2003). Η διαδικασία όμως για την πράξη επικύρωσης δεν μπορεί να γίνει χωριστά από την Ελλάδα, αλλά από όλα τα κράτη μέλη της Κοινότητας με βάση σχετική εξουσιοδότηση που χορηγείται στον Πρόεδρο του Συμβουλίου της Ευρωπαϊκής Ένωσης. Είναι γνωστό ότι σύμφωνα με το άρθρο 2 της Απόφασης του Συμβουλίου της 16^{ης} Μαρτίου 2000 (2000/278/ΕΚ-ΕΕΕΚ L. 89/6-11-2000), ο Πρόεδρος εξουσιοδοτείται να καταθέσει τις πράξεις επικύρωσης στο γενικό διευθυντή του WIPO από την ημερομηνία κατά την οποία τα κράτη μέλη θα θέσουν σε ισχύ τα μέτρα που απαιτούνται προκειμένου να προσαρμοσθεί η υφιστάμενη κοινοτική νομοθεσία στις υποχρεώσεις οι οποίες απορρέουν από τις Συνθήκες Internet.

Ενστάσεις κατά του DRM

Πολλοί οργανισμοί, εξέχοντες άνθρωποι αλλά και άνθρωποι της επιστήμης υπολογιστών αντιτίθενται στο DRM. Δύο αξιοσημείωτες κριτικές είναι αυτή του John Walker, όπως εκφράζεται για παράδειγμα στο άρθρο του “The Digital Imprimatur: How big brother and big media can put the Internet genie back in the bottle” και του Richard Stallman στο άρθρο του “Right to Read”, καθώς και σε άλλες δηλώσεις όπως: Το DRM είναι ένα παράδειγμα

ενός κακοβούλου χαρακτηριστικού - ενός χαρακτηριστικού που σχεδιάστηκε για να βλάψει τον χρήστη του λογισμικού και εξ αυτού δεν πρέπει να λάβει ενθάρρυνση (21).

Υπάρχουν και αρκετοί άλλοι που βλέπου το DRM σε πιο πρωταρχικό επίπεδο. Το TechMediums.com διατυπώνει την άποψη ότι η μουσική που δεν προστατεύεται από DRM είναι ζωτική για την αγορά, καθώς οι ανεξάρτητοι καλλιτέχνες ωφελούνται και μπορούν να έχουν κέρδη από το εμπόριο και την πώληση εισιτηρίων συναυλιών. Ο οργανισμός EFF (Electronic Frontier Foundation) και παρεμφερείς οργανισμοί όπως ο FreeCulture.org έχουν επίσης απόψεις που χαρακτηρίζονται ως ενάντιες στο DRM.

Η τελική έκδοση της άδειας GNU General Public License (έκδοση 3), όπως δημοσιοποιήθηκε από το ίδρυμα Free Software Foundation (FSF), έχει μία διάταξη που «απογυμνώνει» το DRM από την νομική του αξία, έτσι ώστε οι χρήστες να μπορούν να παρακάμψουν το DRM σε λογισμικά GPL χωρίς να παρεμβαίνουν νόμους όπως ο DMCA. Επίσης τον Μάιο του 2006 το FSF ξεκίνησε την εκστρατεία Defective by Design (ελαττωματικό από την σχεδίαση) ενάντια στο DRM. Επίσης η Creative Commons παρέχει επιλογές στην άδειά της, όπου ενθαρρύνουν την διεύρυνση της δημιουργικής δουλειάς χωρίς την χρήστη DRM.

Ο Bill Gates μιλώντας για το DRM το 2006 (CES) είπε ότι «δεν βρίσκεται εκεί που θα έπρεπε και δημιουργεί προβλήματα στους νόμιμους χρήστες όσο προσπαθεί να ξεχωρίσει τους νομίμους από τους παρανόμους χρήστες (22)». Τέλος η Apple σταμάτησε να χρησιμοποιεί την προστασία DRM στο iTunes Store από τον Ιανουάριο του 2009. Παρ' όλα αυτά, χρησιμοποιεί DRM στα βίντεο καθώς θεωρεί ότι η προστασία στα βίντεο αποτελεί διαφορετικό ζήτημα.

Copyleft

Copyleft (23) είναι το όνομα ενός τύπου άδειας χρήσεως σχετικής με τα πνευματικά δικαιώματα. Χρησιμοποιείται το λογοπαίγνιο copyleft (αντί για copyright, όπου right εκτός από δικαίωμα σημαίνει και δεξιά) καθώς αυτός ο τύπος άδειας επιχειρεί να δώσει παραπάνω δικαιώματα στον χρήστη ενός έργου, εν αντιθέσει με τους περιορισμούς που θέτει ο νόμος για τα πνευματικά δικαιώματα.

Ουσιαστικά μία άδεια copyleft παραχωρεί ελευθερίες στην χρήση, τροποποίηση και διανομή ενός έργου, με τον περιορισμό ότι κάθε αντίγραφο ή παράγωγο έργο θα διανέμεται με την ίδια άδεια χρήσεως παραχωρώντας τις ίδιες ελευθερίες. Με άλλα λόγια, copyleft είναι μία γενική μέθοδος για να κάνουμε ένα έργο ελεύθερο και να απαιτήσουμε ότι όλα τα παράγωγά του θα είναι επίσης ελεύθερα. Ο περιορισμός αυτός δεν έρχεται σε αντίθεση με τις ελευθερίες που παρέχονται και που καθιστούν το έργο ελεύθερο περιεχόμενο.

Το Copyleft είναι ένα είδος αδειοδοτήσεως και δύναται να χρησιμοποιηθεί για την διατήρηση των συνθηκών που διέπουν τα πνευματικά δικαιώματα ενός έργου όπως είναι ένα πρόγραμμα υπολογιστή, ένα βιβλίο ή έργα τέχνης. Σε γενικές γραμμές, ο νόμος για τα πνευματικά δικαιώματα (copyright) χρησιμοποιείται από τον δημιουργό του έργου ώστε να αποτρέψει άλλους από την αναπαραγωγή, την ενσωμάτωση ή την διανομή αντιγράφων του έργου του. Στον αντίποδα, με το Copyleft, ο δημιουργός του έργου μπορεί να δώσει σε κάθε

άτομο που λαμβάνει ένα αντίγραφο του έργου του την άδεια να αναπαράγει, να ενσωματώσει ή να διανείμει και απαιτεί ότι το αποτέλεσμα αυτής της διαδικασίας να διέπεται από την ίδια άδεια χρήσεως.

Οι άδειες χρήσεως Copyleft είναι πρωτότυπο παράδειγμα χρήσεως του υπάρχοντος νόμου για τα πνευματικά δικαιώματα ώστε να εξασφαλισθεί ότι τα έργα θα παραμένουν ελεύθερα. Η άδεια GNU General Public License, που γράφτηκε από τον Richard Stallman ήταν η πρώτη άδεια Copyleft που έτυχε ευρείας χρήσεως και συνεχίζει να χρησιμοποιείται μαζικά από τα ελεύθερα έργα. Η Creative Commons, ένας μη κερδοσκοπικός οργανισμός που ιδρύθηκε από τον Lawrence Lessig, παρέχει μία παρόμοια άδεια που ονομάζεται ShareAlike.

Κριτική - Συμπεράσματα

Όπως γίνεται σαφές από τα παραπάνω, η ψηφιακή διαχείριση πνευματικών δικαιωμάτων είναι ένα ζήτημα το οποίο δημιουργεί αντιπαράθεση. Από την μία πλευρά βρίσκονται οι δημιουργοί, οι οποίοι επιθυμούν να προστατέψουν τα έργα τους από την παράνομη αντιγραφή και διάδοση και οι εταιρίες που επιθυμούν να προστατέψουν τα έσοδά τους. Από την άλλη πλευρά βρίσκονται οι καταναλωτές οι οποίοι επιθυμούν να προστατέψουν τα δικαιώματά τους.

Οι τεχνικές DRM που έχουν εφαρμοστεί ως τώρα έχουν αποτύχει στο να προστατέψουν τα έργα και να διαχωρίσουν τους νομίμους από τους παρανόμους χρήστες. Λαμβάνοντας υπ' όψιν και την αντιστρόφως ανάλογη σχέση μεταξύ ασφαλείας και λειτουργικότητος γίνεται κατανοητό ότι όσο μεγαλύτερη είναι η προσπάθεια να προστατευθεί ένα έργο, τόσο λιγότερο εύχρηστο γίνεται. Έτσι φτάνουμε στο σημείο οι νόμιμοι και εξουσιοδοτημένοι χρήστες να είναι αυτοί που ουσιαστικά «ταλαιπωρούνται» από την εφαρμογή του DRM, με χαρακτηριστικό παράδειγμα γνήσιους δίσκους μουσικής που δεν αναπαράγονται σε υπολογιστή ή σε ηχοσύστημα αυτοκινήτου. Επίσης, στην πλειοψηφία από τις τεχνικές DRM που παρουσιάστηκαν παραπάνω, είναι εφικτή η παράκαμψή τους χωρίς ιδιαίτερες γνώσεις.

Από τα παραπάνω γίνεται σαφές, ότι το DRM έχει αποτύχει να πραγματοποιήσει τον σκοπό του γι αυτό και όπως αναφέρθηκε παραπάνω οι περισσότερες εταιρίες προσφέρουν πλέον τα προϊόντα τους ελεύθερα από DRM προστασία.

Μια εφικτή λύση

Καθώς στην εποχή μας όλα γίνονται διαδικτυακά και οι ταχύτητες συνδέσεως στο διαδίκτυο συνεχώς αυξάνονται, η αποθήκευση των ψηφιακών μέσων έχει μειωθεί και η πρόσβαση σε αυτά γίνεται κατ' ευθείαν online.

Μια εφικτή λύση λοιπόν για τα προϊόντα τα οποία απειλούνται πιο πολύ από την πειρατεία (όπως οι δίσκοι μουσικής) θα μπορούσε να είναι η δωρεάν διαδικτυακή τους διάθεση. Όταν όμως ο χρήστης ακούει κάποιο τραγούδι ή διαβάζει κάποιο βιβλίο να υπάρχουν διαφημίσεις, ανάλογες με το ιστορικό περιηγήσεώς του στον ιστό, ώστε οι εταιρίες να έχουν εμμέσως έσοδα.

Κάτι ανάλογο γίνεται από το Youtube και την Vevo. Η εταιρία Vevo είναι το εγχείρημα των εταιριών της μουσικής βιομηχανίας Sony, Universal, Abu Dhabi Media και EMI και ξεκίνησε τον Δεκέμβριο του 2009. Η Vevo προβάλει μουσικά βιντεοκλίπ των εταιριών της κυρίως μέσω του Youtube και σε αυτά τα βίντεο υπάρχουν διαφημίσεις ανάλογες με το ιστορικό περιηγήσεως του χρήστη στον ιστό. Ταυτόχρονα το Youtube κάνοντας χρήση ψηφιακών αποτυπωμάτων αναγνωρίζει τα τραγούδια που ανεβαίνουν στο Youtube από τρίτους χρήστες του και μοιράζει τα έσοδα των διαφημίσεων στις εταιρίες. Τέλος αναλύοντας τις IP διευθύνσεις των επισκεπτών του, εξάγει την χώρα προελεύσεώς τους και αν δεν υπάρχει η κατάλληλη άδεια για την συγκεκριμένη χώρα, κάνει το περιεχόμενο μη διαθέσιμο. Έτσι τα τραγούδια είναι διαθέσιμα «δωρεάν» και οι εταιρίες εμμέσως έχουν έσοδα.

Β’ ΜΕΡΟΣ

Υλοποίηση ψηφιακού υδατογραφήματος σε εικόνα

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, υπάρχουν διάφορες κατηγοριοποιήσεις υδατογραφημάτων. Δύο από αυτές τις κατηγορίες είναι τα ορατά και αόρατα ψηφιακά υδατογραφήματα σε εικόνες. Τα ορατά χρησιμοποιούνται κυρίως για να δηλώσουν στον χρήστη την κυριότητα της εικόνας αλλά και ότι η εικόνα προστατεύεται νομικά. Με αυτόν τρόπο είναι πιθανό να αποφευχθεί η παραβίαση των πνευματικών δικαιωμάτων κυρίως από χρήστες που εν αγνοία τους θα χρησιμοποιούσαν την εικόνα. Τα αόρατα υδατογραφήματα χρησιμοποιούνται κυρίως για την ανίχνευση παρανόμου χρήσεως μίας εικόνας αλλά και για την απόδειξη της κυριότητος μίας εικόνας.

Παρακάτω παρουσιάζεται υλοποίηση ψηφιακών υδατογραφημάτων σε εικόνες και για τις δύο αυτές κατηγορίες. Ο στόχος της υλοποίησης είναι παρουσιαστεί ένα ρεαλιστικό σενάριο και να δοκιμαστεί η ανθεκτικότητα των ψηφιακών υδατογραφημάτων.

Τεχνολογίες που χρησιμοποιήθηκαν στην υλοποίηση

Perl 5.14.2

Για την υλοποίηση χρησιμοποιήθηκε η γλώσσα προγραμματισμού Perl. Αυτό έγινε κυρίως για δύο λόγους:

1. Η Perl δεν χρησιμοποιεί συγκεκριμένα χαρακτηριστικά του λειτουργικού συστήματος και φημίζεται για την φορητότητά της. Σήμερα τα πιο γνωστά λειτουργικά συστήματα την υποστηρίζουν.
2. Είναι σχετικά γρήγορη για τέτοιου είδους διαδικασίες και επειδή είναι γλώσσα που κυρίως χρησιμοποιείται για το διαδίκτυο, τα συγκεκριμένα προγράμματα μπορούν με ελάχιστες αλλαγές να λειτουργήσουν διαδικτυακά ώστε να έχουμε online προσθήκη υδατογραφημάτων σε εικόνες.

GD βιβλιοθήκη

Η GD βιβλιοθήκη γράφτηκε και συντηρείται από τον Lincoln Stein και παρέχει μία αντικειμενοστραφή διεπαφή για την βιβλιοθήκη της C libgd του Thomas Boutell. Παρέχει μία απλή αλλά ταυτόχρονα λογικά δυνατή και γρήγορη διεπαφή για την επεξεργασία bitmap αρχείων. Οι πρόσφατες εκδόσεις της GD μπορούν να δουλέψουν με αρχεία PNG, JPEG, XBM, WBMP (Windows bitmap) καθώς και με ένα δικό της τύπο αρχείων. Προηγούμενες εκδόσεις (πριν την 1.20) συνήθιζαν να λειτουργούν με αρχεία τύπου GIF, γι αυτό και ο εσωτερικός τύπος αρχείων εικόνων GD έχει τόσα κοινά με τα αρχεία GIF (24). Η GD χρησιμοποιείται συνήθως για την δημιουργία πινάκων, γραφικών, μικρογραφιών και σχεδόν για τα πάντα, επί τούτου. Παρ' όλο που δεν δημιουργήθηκε αποκλειστικά για το διαδίκτυο, οι πιο κοινές εφαρμογές της περιλαμβάνουν διαδικτυακή χρήση.

PerlMagick

ImageMagick ονομάζεται μία σουίτα λογισμικού που επιτρέπει την δημιουργία, επεξεργασία και την μετατροπή εικόνων τύπου bitmap. Μπορεί να διαβάσει και να γράψει σε ποικιλία τύπων εικόνας (πάνω από 100) συμπεριλαμβανομένων των DPX, EXR, GIF, JPEG, JPEG-2000, PDF, PhotoCD, PNG, Postscript, SVG και TIFF.

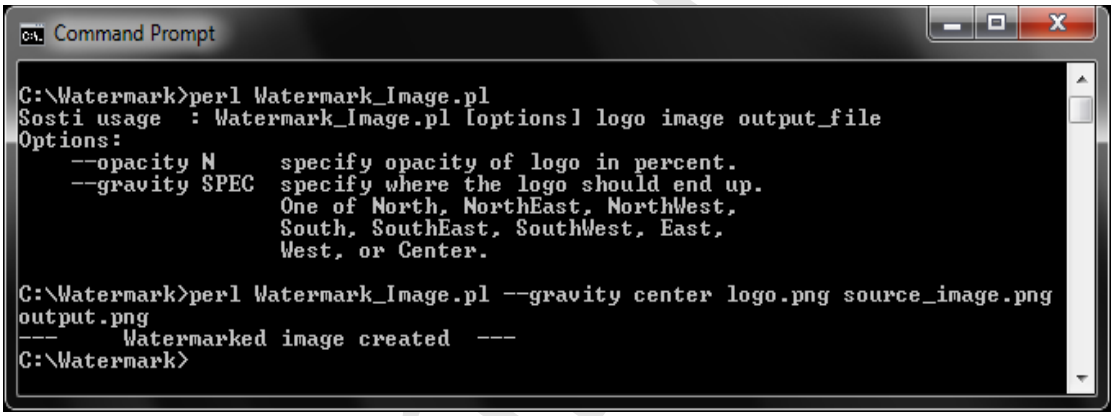
PerlMagick ονομάζεται η αντικειμενοστραφής Perl διεπαφή που κάνει εφικτή την χρήση του λογισμικού ImageMagick. Παρέχει όλες τις λειτουργίες του ImageMagick σε ένα Perl script και την κάνει κατάλληλη για διαδικτυακά CGI script.

Ορατό υδατογράφημα

Στην υλοποίηση του ορατού υδατογραφήματος, ο χρήστης έχει να επιλέξει ανάμεσα σε ψηφιακό υδατογράφημα εικόνας ή κειμένου.

Στην πρώτη περίπτωση ο χρήστης επιλέγει μία μικρή φωτογραφία με το σήμα κατατεθέν (logo) που θέλει να ενσωματώσει στην κύρια φωτογραφία και αφού επιλέξει το ποσοστό ορατότητας του logo και την θέση που αυτό θα τοποθετηθεί, δημιουργείται η τελική εικόνα. Σε αυτήν την υλοποίηση χρησιμοποιείται η βιβλιοθήκη GD έναντι της PerlMagick λόγω της ταχύτητας επεξεργασίας.

Στην παρακάτω εικόνα φαίνεται η λειτουργία του προγράμματος από την γραμμή εντολών καθώς και οι οδηγίες που δίνονται για να βοηθήσουν τον χρήστη.



Εικόνα 6 : Δημιουργία ορατού υδατογραφήματος εικόνας

Παρακάτω φαίνεται η τελική εικόνα που δημιουργήθηκε η οποία περιέχει το υδατογράφημα με ποσοστό διαφάνειας 30% και τοποθετημένο στο κέντρο.

Εικόνα 7 : Φωτογραφία με υδατογράφημα εικόνας

Στην δεύτερη περίπτωση, ο χρήστης αφού επιλέξει την εικόνα που θέλει να υδατογραφήσει καθώς, το όνομα του τελικού αρχείου, την θέση του υδατογραφήματος αλλά και το κείμενο που θα τοποθετηθεί, δημιουργείται η τελική εικόνα. Σε αυτήν την υλοποίηση χρησιμοποιείται η βιβλιοθήκη ImageMagick. Η ταχύτητα επεξεργασίας είναι μικρότερη από αυτήν της βιβλιοθήκης GD. Στις παρακάτω εικόνες φαίνεται η λειτουργία του προγράμματος και η παραχθείσα εικόνα. Η προεπιλεγμένη τοποθεσία του υδατογραφήματος είναι το κέντρο της εικόνας.

Εικόνα 8 : Δημιουργία ορατού υδατογραφήματος κειμένου

Εικόνα 9 : Φωτογραφία με υδατογράφημα κειμένου

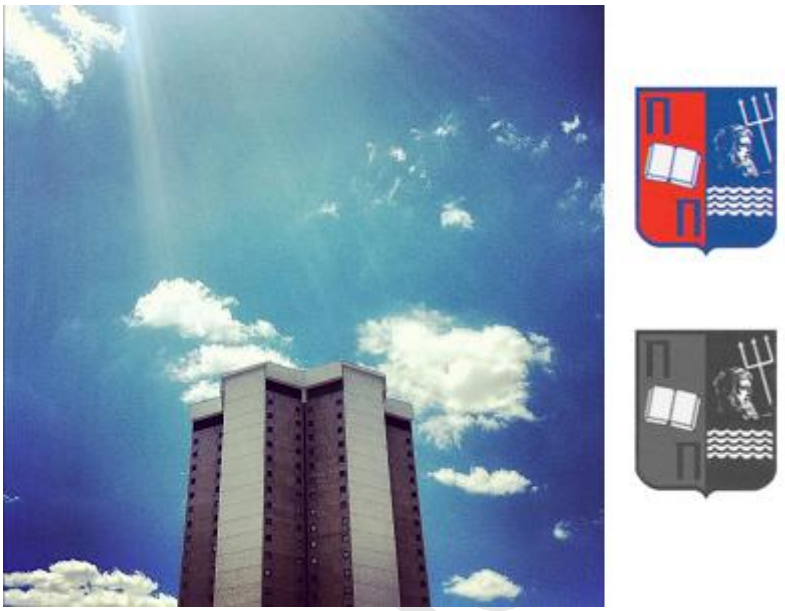
Αόρατο υδατογράφημα

Όταν η αλλαγή της εμφανίσεως μίας εικόνας δεν αποτελεί επιλογή, τότε ένα αόρατο υδατογράφημα μπορεί να προστεθεί κάνοντας χρήση της τεχνικής της στεγανογραφίας. Η στεγανογραφία είναι η τεχνική (κάποιοι την ονομάζουν τέχνη) της αποκρύψεως πληροφορίας μέσα σε δεδομένα με τέτοιον τρόπο ώστε κάποιος τρίτος (πέρα από τον αποστολέα και τον αποδέκτη) να μην δύναται ή να είναι σχεδόν απίθανο να εντοπίσει αυτήν την πληροφορία. Η PerlMagick παρέχει την συνάρτηση Stegano() που επιτρέπει αυτήν υλοποίηση.

Στην υλοποίηση του αόρατου υδατογραφήματος ο χρήστης επιλέγει την εικόνα (logo) που θέλει να κρύψει μέσα στην κύρια εικόνα καθώς και το offset του logo. Η κύρια εικόνα πρέπει να έχει μέγεθος μεγαλύτερο από 256 εικονοστοιχεία σε μήκος και πλάτος, ώστε να υπάρχουν αρκετά δυφία για να κρυφτεί το logo. Η τελική εικόνα που παράγεται πρέπει να είναι ασυμπίεστη, δηλαδή αποκλείεται το ευρέως χρησιμοποιούμενο πρότυπο jpeg, καθώς το πρότυπο αυτό για να πετύχει μείωση του μεγέθους χρησιμοποιεί απώλεια πληροφορίας.

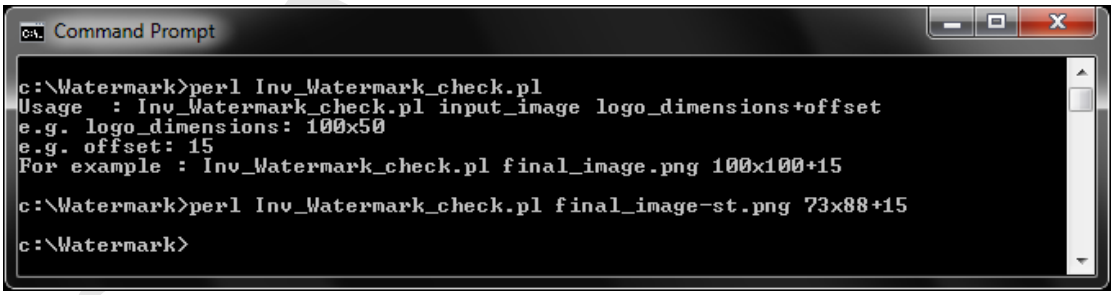
Εικόνα 10 : Προσθήκη αοράτου υδατογραφήματος σε εικόνα

Η παρακάτω εικόνα παρ' όλο που φαίνεται ανέπαφη, περιέχει ένα αόρατο υδατογράφημα. Να σημειωθεί ότι η συγκεκριμένη μέθοδος δεν αποθηκεύει το logo αυτούσιο αλλά ένα ασπρόμαυρο αντίγραφό του, το οποίο είναι αρκετό για την απόδειξη της κυριότητος μιας εικόνας. Η μόνη διαφορά που έχει η παραχθείσα εικόνα είναι στο μέγεθός της, το οποίο έχει αυξηθεί, καθώς τα λιγότερα σημαντικά δυφία χρησιμοποιούνται για να κρύψουν το logo.



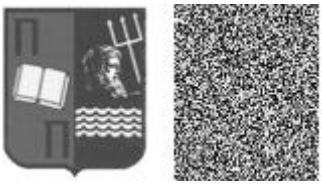
Εικόνα 11 : Εικόνα που περιέχει αόρατο υδατογράφημα

Το δεύτερο σκέλος περιλαμβάνει την ανάκτηση του logo μέσα από την εικόνα. Αυτό που χρειάζεται να ξέρει κάποιος για ανακτήσει το logo είναι τις διαστάσεις του και το offset του, τα οποία λειτουργούν ως κλειδί αποκρυπτογραφήσεως. Στην συγκεκριμένη περίπτωση οι διαστάσεις είναι 73x88 και το offset που δώσαμε είναι 15.



Εικόνα 12 : Εξαγωγή αοράτου υδατογραφήματος από εικόνα

Ως αποτέλεσμα εξάγεται το logo. Αν το κλειδί αποκρυπτογραφήσεως (δηλαδή διαστάσεις και offset) δοθούν λανθασμένα, τότε η εικόνα που θα εξαχθεί φαίνεται δεξιά.



Εικόνα 13 : Επιτυχή και ανεπιτυχής εξαγωγή του αοράτου υδατογραφήματος

Συμπεράσματα - Ανθεκτικότητα αοράτου υδατογραφήματος

Δυστυχώς, η συγκεκριμένη στεγανογραφική τεχνική δεν είναι ιδιαίτερα ανθεκτική. Θα αντέξει σε μερική επεξεργασία (π.χ. blurring) αλλά στην περικοπή και ειδικά στην μετατροπή σε απωλεστικούς τύπους αρχείων (π.χ. jpeg ή gif) ενδέχεται το υδατογράφημα να γίνει μη ανακτήσιμο. Αυτό το πρόβλημα δεν είναι πρόβλημα της υλοποίησης μέσω της διεπαφής ImageMagick αλλά περισσότερο πρόβλημα της ίδιας της στεγανογραφίας.

Εν κατακλείδι, για να έχουμε ανθεκτική προστασία των ψηφιακών εικόνων από την κλοπή, είναι καλύτερο να χρησιμοποιήσουμε άλλες τεχνικές όπως εμφανείς δηλώσεις πνευματικών δικαιωμάτων και νομικές γνωστοποιήσεις. Η στεγανογραφία μπορεί να «νικηθεί» με εύκολο σχετικά τρόπο (24).

Ψηφιακό δακτυλικό αποτύπωμα σε εικόνες

Όπως έγινε κατανοητό το αόρατο υδατογράφημα σε εικόνες έχει πολύ μικρή ανθεκτικότητα. Μία καλλίτερη τεχνική ταυτοποιήσεως ψηφιακού περιεχομένου είναι το ψηφιακό αποτύπωμα, το οποίο παρουσιάστηκε σε προηγούμενο κεφάλαιο. Υπενθυμίζεται ότι η κύρια διαφορά ανάμεσα σε υδατογράφημα και αποτύπωμα, είναι ότι στην πρώτη περίπτωση εισάγουμε πληροφορία στο ίδιο το αρχείο ενώ στην δεύτερη δημιουργούμε ένα πολύ μικρό αρχείο που «περιγράφει» το περιεχόμενό του.

Η παρακάτω υλοποίηση προσπαθεί να δημιουργήσει ένα αλγόριθμο παρόμοιο με αυτόν της ιστοσελίδος tineye.com. Περιληπτικά αυτό που κάνει η ιστοσελίδα είναι δεδομένης μίας φωτογραφίας να εντοπίζει σε ποιες άλλες ιστοσελίδες υπάρχει η ίδια φωτογραφία και όχι κάποια παρόμοια. Ο αλγόριθμος εντοπίζει αντίγραφα της φωτογραφίας ακόμη και αν αυτά έχουν άλλο μέγεθος, διαφορετικό λόγο πλάτους-ύψους ακόμη και αν οι φωτογραφίες έχουν υποστεί επεξεργασία. Επίσημα η ιστοσελίδα το μόνο που αναφέρει σχετικά με τον τρόπο λειτουργίας του αλγορίθμου είναι ότι χρησιμοποιεί ψηφιακά δακτυλικά αποτυπώματα. Παρακάτω γίνεται μία ανάλυση για το πώς δουλεύει η παρούσα υλοποίηση.

Αντιληπτικές συναρτήσεις κατακερματισμού (Perceptual hash functions)

Στην τομέα της κρυπτογραφίας, όταν επιθυμούμε να αποδείξουμε ότι δύο αρχεία είναι ίδια συνήθως χρησιμοποιούμε κρυπτογραφικές συναρτήσεις κατακερματισμού (π.χ. SHA1, MD5 κτλ). Στην συγκεκριμένη περίπτωση αυτό δεν είναι αρκετό καθώς αν πειράξουμε ένα δυφίο στην εικόνα (π.χ. αλλάζοντας τις διαστάσεις της) η συνάρτηση κατακερματισμού θα παράξει διαφορετικό αποτέλεσμα. Γι αυτόν τον λόγο γίνεται χρήση αντιληπτικών (perceptual) συναρτήσεων κατακερματισμού.

Οι αντιληπτικές συναρτήσεις κατακερματισμού είναι τροποποιημένες συναρτήσεις κατακερματισμού προορισμένες για περιεχόμενο πολυμέσων. Παρομοίως με τις κρυπτογραφικές, παράγουν διαφορετική έξοδο για κάθε διαφορετική είσοδο. Η κύρια διαφοράς τους είναι ότι ο ορισμός της διαφορετικής εισόδου είναι διαφορετικός. Με άλλα λόγια το αποτέλεσμα της εξόδου μίας αντιληπτικής συναρτήσεως αλλάζει όχι όταν αλλάξει ένα δυφίο της εισόδου, αλλά όταν η είσοδος αλλάξει αντιληπτικά-εμφανισιακά. Για παράδειγμα μία εικόνα και η συμπιεσμένη JPEG εκδοχή της θα πρέπει να έχουν την ίδια αντιληπτική συνάρτηση καθώς εμφανισιακά είναι ίδιες παρ' όλο που από πλευράς δυφίων είναι εντελώς διαφορετικές (25).

Μια καλή συνάρτηση κατακερματισμού οφείλει να:

1. Είναι ανθεκτική: Η επεξεργασία που δεν αλλάζει την εμφάνιση της εικόνας δεν θα πρέπει να αλλάζει και το αποτέλεσμα της συναρτήσεως.
2. Είναι μοναδική: Διαφορετικές οπτικά είσοδοι θα πρέπει να έχουν διαφορετικές εξόδους.
3. Είναι ασφαλής: Θα πρέπει να είναι πολύ δύσκολο να βρεθούν διαφορετικές είσοδοι που παράγουν ίδιες εξόδους.

Πώς δουλεύει η παρούσα υλοποίηση

Στις φωτογραφίες, η υψηλή ανάλυση μας δίνει λεπτομέρεια ενώ η χαμηλή ανάλυση μας δίνει την δομή της εικόνας. Με αυτήν την λογική δημιουργήθηκε η παρακάτω υλοποίηση, η οποία παρουσιάζεται παρακάτω.

Κατ' αρχήν μειώνουμε το μέγεθος της εικόνας. Είναι ο πιο γρήγορος τρόπος ώστε να αφαιρέσουμε την λεπτομέρεια από την εικόνα ώστε να κρατήσουμε την δομή της. Για την ακρίβεια δημιουργούμε μία μικρογραφία της εικόνας η οποία είναι 8x8 εικονοστοιχεία. Δεν δίνουμε βάση στον λόγο πλάτους/ύψους καθώς με αυτόν τον τρόπο μπορούμε να συγκρίνουμε και εικόνες που έχουν διαφορετικές διαστάσεις. Η μικρογραφία που έχει παραχθεί ουσιαστικά αναπαραστεί το πρότυπο-δομή που ακολουθεί η εικόνα.

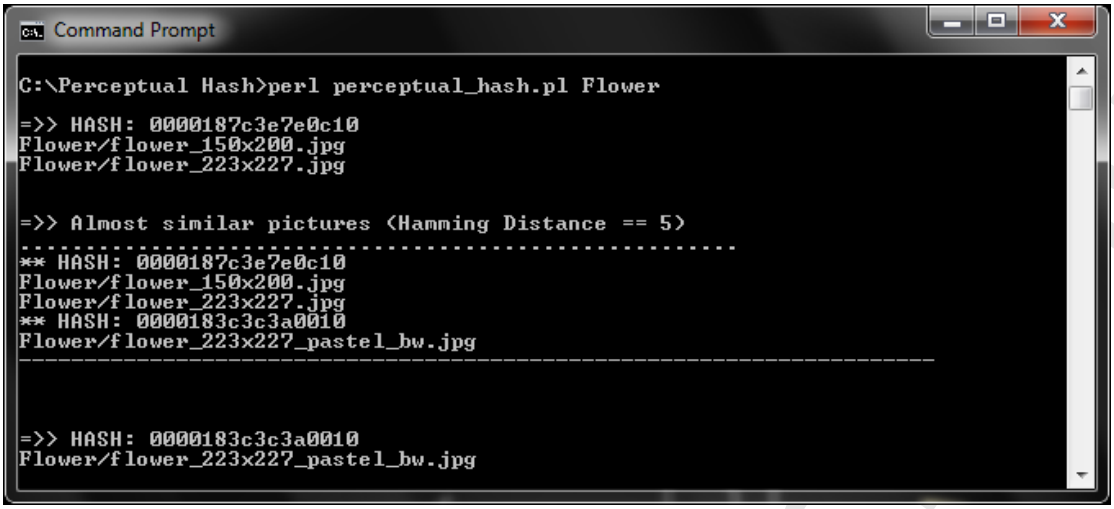
Κάθε εικονοστοιχείο από τα συνολικά 64 (8x8), αναπαριστάται ανάλογα με το ποσοστό του κοκκίνου (R), του πρασίνου (G) και του κυανού (B) που έχει, για παράδειγμα (R,G,B) = (0.783031967650874, 0.710154879072251, 0.61556420233463). Το χρώμα του κάθε εικονοστοιχείου βγαίνει υπολογίζοντας το 1/3 του αθροίσματος των τριών χρωμάτων που το συντελούν [(R,G,B)/3], που στην συγκεκριμένη περίπτωση είναι 0.702917016353.

Εν συνεχεία υπολογίζουμε τον μέσο όρο των συνολικά 64 χρωμάτων της εικόνας. Ελέγχουμε κάθε εικονοστοιχείο και αν το χρώμα του είναι κάτω από το μέσο χρώμα τότε θέτουμε ένα δυφίο 1 διαφορετικά 0 και έτσι σχηματίζουμε για κάθε εικόνα έναν αριθμό 64 διφύων που την χαρακτηρίζει (δακτυλικό αποτύπωμα).

Για να συγκρίνουμε δύο εικόνες, αρκεί να συγκρίνουμε τα δύο αποτυπώματά τους και να υπολογίσουμε σε πόσες θέσεις διαφέρουν (απόσταση Hamming). Αν η διαφορά είναι μηδέν τότε οι συγκριθείσες εικόνες είναι οι ίδιες. Αν η διαφορά μέχρι 5 τότε έχουμε παρόμοιες εικόνες και αν η διαφορά είναι μεγαλύτερη τότε κατά πάσα πιθανότητα έχουμε διαφορετικές εικόνες.

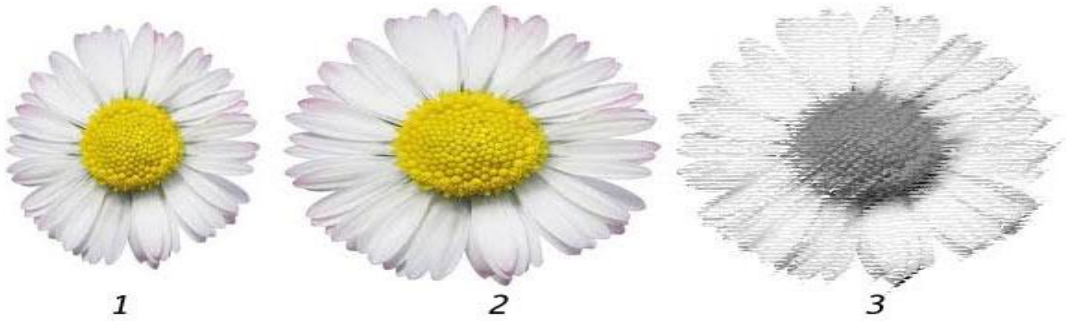
Παρ' όλη την απλότητα του αλγορίθμου, παρατηρούμε ότι ο αλγόριθμος πληροί τις παραπάνω προδιαγραφές μίας καλής αντιληπτικής συναρτήσεως κατακερματισμού. Είναι δηλαδή ανθεκτικός, είναι ασφαλής και παράγει διαφορετικά αποτελέσματα για κάθε διαφορετική οπτικά είσοδο.

Παρακάτω φαίνεται η λειτουργία του προγράμματος:



Εικόνα 14 : Λειτουργία προγράμματος δημιουργία αποτυπώματος σε εικόνα

Στον φάκελο "Flower" υπάρχουν τρεις εικόνες που αναπαριστούν ένα λουλούδι. Η πρωτότυπη έχει διαστάσεις 223x227. Η δεύτερη είναι η ίδια εικόνα με διαστάσεις 150x200 και η τρίτη έχει υποστεί επεξεργασία και έχει γίνει ασπρόμαυρη. Παρ' όλα αυτά το πρόγραμμα δίνει απόσταση Hamming ίση με 5 συγκρίνοντας την πρωτότυπη εικόνα με τις άλλες δύο, οπότε είναι ασφαλές να θεωρήσουμε ότι μιλάμε για την ίδια εικόνα.



Εικόνα 15 : Περιεχόμενου φακέλου Flower

Στον φάκελο "Mona Lisa" υπάρχουν 3 επεξεργασμένες φωτογραφίες του κλασικού έργου καθώς και η πρωτότυπη. Παρ' όλο που υπάρχουν αρκετά εφέ και επεξεργασία και διαφορετικά μεγέθη, επειδή το πρότυπο-μοτίβο της εικόνας παραμένει το ίδιο, το πρόγραμμα αναγνωρίζει ως παρόμοιες τις παρακάτω εικόνες. Έτσι το πρόγραμμα δίνει απόσταση hamming 4 μεταξύ της εικόνας 1 και της 2, ομοίως 4 μεταξύ της εικόνας 1 και 4 και 3 μεταξύ της εικόνας 1 και 3.

Εικόνα 16 : Επεξεργασμένες εκδοχές του κλασικού πίνακα που το πρόγραμμα αναγνωρίζει ως παρόμοιες

Συμπεράσματα – Ανθεκτικότητα ψηφιακού δακτυλικού αποτυπώματος

Όπως έγινε κατανοητό το ψηφιακό δακτυλικό αποτύπωμα είναι μία πολλή ανθεκτική τεχνική η οποία δεν επηρεάζεται σε μεγάλο βαθμό από την επεξεργασία και μπορεί να χρησιμοποιηθεί σε πραγματικές συνθήκες, καθώς στις μέρες η χρήση εικόνων στο διαδίκτυο χωρίς άδεια από τον δημιουργό τους είναι πολύ συχνό φαινόμενο.

Η συγκεκριμένη υλοποίηση σε συνδυασμό με ένα πρόγραμμα (web spider) που θα ανιχνεύει τις ιστοσελίδες και θα αποθηκεύει τα αποτυπώματα των εικόνων σε μία βάση δεδομένων μπορεί να αποδείξει την κυριότητα μίας εικόνας καθώς και αν αυτή χρησιμοποιείται χωρίς άδεια. Η σύγκριση των αποτυπωμάτων μπορεί να γίνει πολύ γρήγορα, καθώς αυτά θα βρίσκονται αποθηκευμένα στην βάση δεδομένων.

Παράρτημα

Κώδικας δημιουργίας ψηφιακού δακτυλικού αποτυπώματος

perceptual_hash.pl

```
1.  #!/usr/bin/perl
2.
3.  use strict;
4.  use warnings;
5.
6.  use File::Spec;
7.  use lib File::Spec->curdir();
8.
9.  use File::Find qw(find);
10. use Image::Hash qw(get_image_hash);
11.
12. my @dirs = grep -d, @ARGV;
13.
14. @dirs || die "Usage: perl $0 <dir1> <dir2> ...\n";
15.
16. my %check;
17. find {
18. wanted => sub {
19. my $hash = get_image_hash($_);
20. if (defined $hash) {
21. push @{$check{$hash}}, $_;
22. }
23. },
24. no_chdir => 1,
25. } => @dirs;
26.
27. sub cmp_diff {
28. my ($s1, $s2) = @_;
29. scalar grep { $_ > 0 } unpack('C*', '' . $s1 ^ '' . $s2);
30. }
31.
32. my %seen;
33. foreach my $key (keys %check) {
34.
35. print "\n=>> HASH: $key\n", join("\n", @{$check{$key}}), "\n\n";
36.
37. foreach my $comp_key (keys %check) {
38.
39. if ($key ne $comp_key) {
40.
41. next if $seen{$key}{$comp_key};
42. next if $seen{$comp_key}{$key};
43.
44. $seen{$key}{$comp_key} = 1;
45. $seen{$comp_key}{$key} = 1;
46.
47. my $diff = cmp_diff($key, $comp_key);
48.
49. if ($diff <= 5) {
```

```
50. print "\n=>> Almost similar pictures (Hamming Distance == $diff)\n", '.' x 55, "\n";
51. print "** HASH: $key\n";
52. foreach my $img (@{$check{$key}}) {
        print "$img\n";
53. }
54. print "** HASH: $comp_key\n";
55. foreach my $img (@{$check{$comp_key}}) {
        print "$img\n";
56. }
57. print '-' x 70, "\n\n\n";
58. }
59. }
60. }
61. }
```

Image::Hash

```
1.  package Image::Hash;
2.
3.  use strict;
4.  use warnings;
5.
6.  use Image::Magick;
7.  use List::Util qw(sum);
8.
9.  our $VERSION = '0.1';
10.
11. require Exporter;
12. our @ISA = qw(Exporter);
13. our @EXPORT = qw(get_image_hash);
14.
15. sub get_image_hash {
16. my ($image) = @_;
17.
18. return if not $image =~ /\.(?:jpe?g|png)$/i;
19. return if not -f $image;
20.
21. my $p = new Image::Magick;
22. my $error = $p->Read(filename => $image);
23. $error && do { warn $error; return };
24.
25. my ($width, $height) = (8, 8);
26.
27. $error = $p->Resize(width => $width, height => $height);
28. $error && do { warn $error; return };
29.
30. my @colors;
31. my $avg = 0;
32. for (my $y = 0 ; $y < $height ; $y++) {
        for (my $x = 0 ; $x < $width ; $x++) {
                push @colors, [$p->GetPixel(x => $x, y => $y)];
                $avg += sum(@{$colors[-1]}) / 3;
        }
```

```
33. }
34. $avg /= $width * $height;
35.
36. my $i    = 0;
37. my $hash = q{};
38. foreach my $color (@colors) {
        vec($hash, $i++, 1) = sum(@{$color}) / 3 < $avg ? 1 : 0;    # set the bits
39. }
40.
41. return scalar unpack("H*", $hash);
42. }
```

Βιβλιογραφία

1. **Coyle, Karen.** *The Technology of Rights: Digital Rights Management.* 2003.

2. The Content Scrambling System (CSS) - A Technical Description. *tinyted.net.* [Ηλεκτρονικό] [Παραπομπή: 17 05 2012.] http://www.tinyted.net/eddie/css.html.

3. **Administrator, AACS Licensing.** *Advanced Access Content System (AACS) - Pre-recorded Video Book.* 2006.

4. **Lewis, Rita.** What is DRM and why should I care? *Firefox.org.* [Ηλεκτρονικό] [Παραπομπή: 18 05 2012.] http://firefox.org/news/articles/1045/1/What-is-DRM-and-why-should-I-care/Page1.html.

5. **INITIATIVE, SECURE DIGITAL MUSIC.** *SDMI Portable Device Specification.* Los Angeles : s.n., 1999.

6. **Halderman, Felten.** *Lessons from the Sony CD DRM Episode.* s.l. : Princeton University.

7. DRM on audio CD's abolished. *lxer.* [Ηλεκτρονικό] [Παραπομπή: 21 5 2012.] http://lxer.com/module/newswire/view/78008/index.html.

8. Sony BMG Plans to Drop DRM. *businessweek.com.* [Ηλεκτρονικό] [Παραπομπή: 21 05 2012.] http://www.businessweek.com/technology/content/jan2008/tc2008013_398775.htm.

9. Apple Unveils Higher Quality DRM-Free Music on the iTunes. *Apple.com.* [Ηλεκτρονικό] [Παραπομπή: 22 05 2012.] http://www.apple.com/pr/library/2007/04/02Apple-Unveils-Higher-Quality-DRM-Free-Music-on-the-iTunes-Store.html.

10. OpenMG - Technical Overview and Benefits. *openmginfo.* [Ηλεκτρονικό] [Παραπομπή: 22 05 2012.] http://www.openmginfo.com/overview/tech.html.

11. eBooks and Digital Rights Management (DRM), for ePublishers. *tinhat.com.* [Ηλεκτρονικό] [Παραπομπή: 22 05 2012.] http://www.tinhat.com/ebooks_epublishing/epublishers_drm.html.

12. **Noring, Jon.** The Perils of DRM Overkill For Large Publishers. *teleread.org.* [Ηλεκτρονικό] [Παραπομπή: 23 05 2012.] http://web.archive.org/web/20080403175200/http://www.teleread.org/publishersdrm.htm.

13. **Yam, Marcus.** Ubisoft's DRM for Assassin's Creed II is Cracked. *tomshardware.com.* [Ηλεκτρονικό] [Παραπομπή: 23 05 2012.] http://www.tomshardware.com/news/assassins-creed-crack-hack-drm-ac2,10260.html.

14. Serious Sam's DRM Is A Giant Pink Scorpion. *rockpapershotgun.com.* [Ηλεκτρονικό] [Παραπομπή: 23 05 2012.] http://www.rockpapershotgun.com/2011/12/07/serious-sams-drm-is-a-giant-pink-scorpion/.

15. **El-Gayyar, Mahmoud.** *Watermarking Techniques - Spatial Domain - Digital Rights Seminar.* 2006.

16. **Αικατερίνη, Χατζηδιάκου.** *Ανάπτυξη υπηρεσιών Διαδικτύου για την προστασία και διαχείριση των πνευματικών δικαιωμάτων ψηφιακού περιεχομένου με τη χρήση τεχνολογιών υδατοσήμανσης.* Πάτρα : s.n., 2009.

17. **Milano, Dominic.** *Content Control: Digital Watermarking and Fingerprinting.*

18. **Barlas, Chris.** *Digital Rights Expression Languages.* 2006.

19. **Summary, U.S. Copyright Office.** *THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998.* 1998.

20. **Καλλινίκου, Διονυσία.** *Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.* 2005.

21. **O'Riordan, Ciaran.** *Transcript of Opening session of first international GPLv3 conference.* 2006.

22. **Michael Arrington.** Bill Gates On The Future Of DRM. *http://techcrunch.com.* [Ηλεκτρονικό] [Παραπομπή: 28 05 2012.] http://techcrunch.com/2006/12/14/bill-gates-on-the-future-of-drm/.

23. What is Copyleft? *GNU.* [Ηλεκτρονικό] [Παραπομπή: 31 05 2012.] http://www.gnu.org/copyleft/copyleft.en.html.

24. **VERBRUGGEN, MARTIEN.** *Graphics Programming with Perl.* 2002.

25. Perceptual Hashing. *poly.edu.* [Ηλεκτρονικό] 05 08 2012. http://isis.poly.edu/projects/percephash.