ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

"ΥΔΑΤΟΓΡΑΦΗΣΗ, ΩΣ ΜΕΘΟΔΟΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ"

Επιβλέπων Καθηγητής: Μπελιγιάννης Γρηγόριος

Σπουδάστρια: Φέγγαρη Χαρίκλεια, Α.Μ.:8605

ΜΑΡΤΙΟΣ 2006

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

"ΥΔΑΤΟΓΡΑΦΗΣΗ, ΩΣ ΜΕΘΟΔΟΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ"

Επιβλέπων Καθηγητής: Μπεληγιάννης Γρηγόριος

Σπουδάστρια: Φέγγαρη Χαρίκλεια, Α.Μ.:8605

ΜΑΡΤΙΟΣ 2006

Οι πιο ειλικρινείς ευχαριστίες μου, απευθύνονται στον Κ° Γρηγόριο Μπεληγιάννη, Καθηγητή στο Τ.Ε.Ι. Μεσολογγίου, ο οποίος με τις πολύτιμες συμβουλές του επέτρεψε την ολοκλήρωση αυτής της εργασίας.

Ας βρει εδώ την έκφραση της βαθειάς μου αναγνώρισης, για την εμπιστοσύνη, τον ενθουσιασμό και τη συνεχή συμπαράσταση που μου παρείχε.

ΠΕΡΙΕΧΟΜΕΝΑ

1

ΠΡΟΛΟΓΟΣ

1.1 Εισαγωγή - Σκοπός της διπλωματικής

Η ραγδαία τεχνολογική ανάπτυξη των μέσων επικοινωνίας και η ευρεία χρήση του διαδικτύου που παρατηρήθηκε στον αιώνα που διανύουμε επηρέασε σε καθοριστικό βαθμό κάθε δομή της ανθρώπινης κοινωνίας. Τόσο η οικονομία, η επιστήμη, η τεχνολογία ακόμα και οι διαπροσωπικές σχέσεις των ανθρώπων διαμορφώθηκαν κάτω από διαφορετικές συνθήκες λόγω αυτής της τεχνολογικής ανάπτυξης. Σήμερα, ιδέες και προϊόντα διακινούνται ταχύτατα από την μία άκρη της γης στην άλλη γεγονός που παλαιότερα φαινόταν αδύνατο. Αυτές οι πολλαπλές δυνατότητες που αναπτύχθηκαν έκαναν την πληροφορία να διακινείται πολύ γρήγορα και την ψηφιακή αναπαράσταση των δεδομένων να κυριαρχεί σχεδόν σε όλες τις ανθρώπινες δραστηριότητες. Αυτή η κυριαρχία της ψηφιακής αναπαράστασης έφερε στο προσκήνιο νέες ανάγκες που οδήγησαν και στην ανάπτυξη νέων εννοιών και τεχνικών. Μία έννοια που η ανάγκη της υπερτονίστηκε αρκετά είναι η προστασία των δεδομένων.

Σήμερα τα δεδομένα μπορούν να αναπαραστήσουν τόσο υλικά προϊόντα όσο και οποιαδήποτε μορφή πνευματικής γνώσης, και επιπλέον αυτά μπορεί να μεταφέρονται σε δευτερόλεπτα να αντιγράφονται και να εκπέμπονται ξανά. Η προστασία των δεδομένων προτάσσεται σαν αναγκαία μιας και η κλοπή ή η κακόβουλη χρήση της ψηφιακής πληροφορίας προκαλεί δυσμενείς οικονομικές συνέπειες και πολλά προβλήματα στην ασφάλεια. Για το λόγο αυτό στον περασμένο αιώνα αναπτύχθηκαν σε μεγάλο βαθμό οι μέθοδοι προστασίας δεδομένων όπως η ψηφιακή υπογραφή και η κρυπτογραφία. Η απάντηση που δόθηκε όμως από τις δύο προηγούμενες μεθόδους στην προστασία ηλεκτρονικών δεδομένων ήταν ελλιπής καθώς στα προϊόντα πολυμέσων δεν έδιναν καμία αξιόπιστη απάντηση και ταυτόχρονα οι χρονοβόρες διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης τις έκαναν ελάχιστα εύχρηστες.

Το υδατογράφημα αναπτύχθηκε πάνω στο πεδίο που αδυνατούσαν οι δύο προηγούμενες μορφές προστασίας δεδομένων να εμπλακούν. Σε μία κοινωνία όπου τα συνολικά προϊόντα που παράγονται είναι προϊόντα γνώσης η έννοια της προστασίας των πνευματικών δικαιωμάτων φαντάζει απαραίτητη. Παλαιότερα αν ζητούσε ο Κολόμβος από κάθε κάτοικο της Αμερικής μερίδιο για την ανακάλυψη του θα φάνταζε παράλογο. Σήμερα το σύνολο των εταιριών που ασχολούνται με την παραγωγή ψηφιακών προϊόντων στηρίζουν ένα μεγάλο κομμάτι των εσόδων τους στην εκμετάλλευση των πνευματικών δικαιωμάτων από τα προϊόντα που παράγουν. Η δομή της σημερινής παγκόσμιας οικονομίας στηρίζεται στην παραγωγή και στην εξέλιξη της ψηφιακής τεχνολογίας. Είναι εύλογο λοιπόν μία έννοια όπως τα πνευματικά δικαιώματα πάνω στα ψηφιακά προϊόντα να παίρνει τελείως διαφορετικές διαστάσεις απ' ότι παλιότερα.

Το υδατογράφημα αποτελεί την πρώτη μέθοδο που απαντά επί της ουσίας στο πρόβλημα των πνευματικών δικαιωμάτων. Η έννοια της προστασίας των πνευματικών δικαιωμάτων μπορεί να αναπτύχθηκε για να διαφυλαχθεί η κυριότητα των κατόχων στα προϊόντα αλλά σαν έννοια είναι πολύ παλαιότερη. Το πνευματικό δικαίωμα δηλώνει την κυριαρχία αυτού που παράγει κάτι στο παραγόμενο αντικείμενο. Σε μία κοινωνία που η γνώση διακινείται ελεύθερα και είναι προσβάσιμη από όλους τα πνευματικά δικαιώματα δίνουν τη δυνατότητα της αξίωσης σε αυτόν που παράγει μία ιδέα ή ένα προϊόν και όχι σε αυτόν που μεσολαβεί ή σε αυτόν που το πουλά.

Το να μπορεί μία μέθοδος να αποτρέπει την καταπάτηση των πνευματικών δικαιωμάτων παρ' όλες τις μορφοποιήσεις που μπορούν να εφαρμοσθούν είναι όντως δύσκολο εγχείρημα. Το υδατογράφημα θα πρέπει να περιλαμβάνει την παροχή προστασίας των πνευματικών δικαιωμάτων και να κάνει έκδηλη τις κακόβουλες τροποποιήσεις των δεδομένων.

Το υδατογράφημα προσθέτει επιπλέον πληροφορία σ' ένα προϊόν. Πληροφορία που σχετίζεται με τα πνευματικά δικαιώματα σε ποικίλες μορφές προϊόντων όπως εικόνα, ήχος video. Τα δεδομένα αυτά προστίθενται με τέτοιο τρόπο ώστε να παραμένουν αόρατα για κοινούς παρατηρητές. Η αόρατη σφραγίδα είναι πληροφορία που δεν περιορίζει την πρόσβαση στο αρχικό σήμα αλλά προσπαθεί να παραμένει κρυφή και άθικτη. Οι τεχνολογικές ανακαλύψεις πάνω στο ψηφιακό σήμα έδωσαν πολλαπλές δυνατότητες στην απόκρυψη πληροφορίας και πρόσφεραν στην μέθοδο του υδατογραφήματος πολύτιμη πληροφορία κάνοντας το πολύ αξιόπιστο. Η ένθεση του υδατογραφήματος λοιπόν παίζει καθοριστικό ρόλο στην υδατογράφηση μιας και ο τρόπος καθώς και οι προϋποθέσεις που λαμβάνονται υπόψη στην απόκρυψη δεδομένων επηρεάζουν την αξιοπιστία της υδατογράφησης.

Το υδατογράφημα μπορεί να καθιερώθηκε για την δυνατότητα του να παρέχει προστασία στα πνευματικά δικαιώματα, όμως αποτελεί ία μέθοδο που παρέχει ένα ευρύ φάσμα προστασίας στα προϊόντα μιας και απαντά και στην προστασία της αυθεντικότητας των δεδομένων. Για να μπορέσει η μέθοδος της υδατογράφησης να αποφέρει στο υδατογραφημένο προϊόν εκείνα τα χαρακτηριστικά που να το κάνουν ασφαλές απέναντι στις κακόβουλες επιθέσεις που μπορεί να δεχθεί θα πρέπει τα αποτελέσματα της μεθόδου να διέπονται από κάποιες βασικές προϋποθέσεις:

i. Ανθεκτικότητα του υδατογραφήματος στις βασικές τροποποιήσεις που μπορεί να δεχθεί ώστε το υδατογράφημα να μην μπορεί να αφαιρεθεί,

ii. Μη αντιληπτή ένθεση ώστε ο κοινός χρήστης να μην αντιλαμβάνεται την ύπαρξη της υδατογραφημένης πληροφορίας,

iii. Αξιόπιστη ανίχνευση ώστε κάθε στιγμή να μπορούν με βεβαιότητα να διεκδικηθούν τα πνευματική δικαιώματα από τον νόμιμο κάτοχο,

iv. Πολυπλοκότητα του υδατογραφήματος ώστε να παράγονται πολλαπλά και διακριτά υδατογραφήματα που να μην μπορούν να ευρεθούν με στατιστικές μεθόδους.

v. Τυχαιότητα στην παραγωγή του κλειδιού ώστε η παραγωγή όμοιων υδατογραφημάτων ίδιων με αυτό που ενθέτεται να είναι αδύνατη,

vi. Συσχετισμένο κλειδί υδατογράφησης ώστε ένα υδατογράφημα να προσφέρει αρκετά μεγάλη ασφάλεια (μεγάλο μέγεθος κλειδιού) χωρίς αυτό να επηρεάζει την ποιότητα του υδατογραφημένου προϊόντος. Επιπλέον ο αλγόριθμος υδατογράφησης θα πρέπει να είναι αρκετά εύχρηστος.

vii. Η ένθεση πολλαπλών υδατογραφημάτων δε θα πρέπει να απαγορεύεται μιας και μόνο η ύπαρξη του προϊόντος με το αρχικό υδατογράφημα είναι αυτή που διεκδικεί και τα πνευματικά δικαιώματα.

Στη συγκεκριμένη διπλωματική εργασία έγινε προσπάθεια να προσεγγιστεί η μέθοδος της υδατογράφησης σε τρία επίπεδα:

i. Αναλύοντας την έννοια του υδατογραφήματος και τις βασικές αρχές και προϋποθέσεις της μεθόδου υδατογράφησης.

ii. Μελετώντας την εφαρμογή του υδατογραφήματος και στα τέσσερα πεδία εφαρμογής της (κείμενο, βίντεο, εικόνα, ήχος) μέσα από τις τεχνικές και τις εφαρμογές των μεθόδων υδατογράφησης.

iii. Υλοποίηση σχημάτων υδατογράφησης ήχου και για τις τρεις βασικές τεχνικές της υδατογράφησης ήχου.

Πιστεύουμε ότι μία απλή και γενική αναφορά του υδατογραφήματος αλλά και της εφαρμογής των μεθόδων υδατογράφησης και στα τέσσερα πεδία δε θα μπορούσε να εμβαθύνει στη μέθοδο της προστασίας δεδομένων που προσφέρει το υδατογράφημα χωρίς την υλοποίηση των σχημάτων υδατογράφησης. Επίσης και μία απλή υλοποίηση που δε θα περιλάμβανε την έρευνα του επιστημονικού εύρους που καλύπτει η μέθοδος της υδατογράφησης δε θα μπορούσε να καλύψει συνολικά το γνωστικό πεδίο το οποίο διαπραγματεύεται το υδατογράφημα.

1.2 Συμπεράσματα

Το υδατογράφημα αποτελεί μία εξελισσόμενη επιστημονική μέθοδο προστασίας δεδομένων που καλύπτει έναν ευρύ επιστημονικό και τεχνολογικό πεδίο έρευνας. Αρχικά αναλύθηκε η ιδέα του υδατογραφήματος, οι βασικές έννοιες και αρχές που το διέπουν και τα πεδία με τα οποία ασχολείται. Έπειτα έγινε μία αναλυτική προσέγγιση και επεξήγηση των εφαρμογών και των τεχνικών του υδατογραφήματος, και στα τέσσερα πεδία εφαρμογής (κείμενο, εικόνα, βίντεο, ήχος). Τέλος υλοποιήθηκαν βασικοί αλγόριθμοι υδατογράφησης ήχου. Η υλοποίηση κατέδειξε τις βασικές αρχές και προϋποθέσεις που είναι αναγκαίο να διέπουν το υδατογραφημένο αρχείο ήχου. Ταυτόχρονα έκανε φανερά εκείνα τα σημεία από τους επιστημονικούς στόχους, που θέτει η υδατογράφηση σα μέθοδος προστασίας, και μπορεί να απαντήσει και εκείνα που αδυνατεί. Η μελέτη των αποτελεσμάτων αποτελεί ένα από τα βασικά σημεία που

πρέπει να αναλυθούν, γιατί μόνο μέσα από την παρατήρηση των συμπερασμάτων και την εμβάθυνση στη θεωρία που περικλείει η υδατογράφηση μπορεί η επιστημονική έρευνα πάνω στην προστασία δεδομένων να προχωρήσει και να επιφέρει ουσιαστικά αποτελέσματα.

Συγκεκριμένα μέσα από την εφαρμογή του υδατογραφήματος μπορούμε να βγάλουμε τα εξής βασικά συμπεράσματα για την υδατογράφηση:

a) Το υδατογράφημα για να απαντά στη διαφύλαξη των πνευματικών δικαιωμάτων απαραίτητη προϋπόθεση είναι η διατήρηση της ανθεκτικότητας του ώστε σε καμία περίπτωση να μη μπορεί να αφαιρεθεί.

b) Η ένθεση επιβάλλεται να εκμεταλλευθεί τα ιδιαίτερα χαρακτηριστικά των ψηφιακών σημάτων ώστε η προσθήκη του υδατογραφήματος να παραμένει μη αντιληπτή στο χρήστη. Σ' αυτήν την κατεύθυνση χρήσιμες έως πολύτιμες είναι οι επεξεργασίες των σημάτων που βελτιώνουν την ποιότητα του προϊόντος, τέτοιες είναι:

- Βάθμωση (scaling)
- Φιλτράρισμα
- Κανονικοποίηση
- Επικόλληση (Cropping)
- Δειγματοληψία και Επαναδειγματοληψία
- Συμπίεση - Αποσυμπίεση

Επίσης, το ανθρώπινο οπτικοακουστικό μοντέλο (mpeg) συσχετίζει τις ιδιότητες και τις ειδικές επεξεργασίες των ψηφιακών σημάτων σε σχέση με την ικανότητα της ανθρώπινης όρασης και ακοής να αντιληφθεί κάτι. Η χρήση του mpeg μοντέλου είναι αρκετά σημαντική μιας και πολλές τεχνικές δε θα μπορούσαν να ενθέσουν μη αντιληπτή πληροφορία χωρίς τη βοήθεια του.

c) Ως προς την πολυπλοκότητα των υδατογραφημάτων θα πρέπει να χρησιμοποιούνται ανεπτυγμένες μέθοδοι των εφαρμοσμένων μαθηματικών ώστε να μπορούν να παραχθούν πολλαπλά υδατογραφήματα

d) Ένας σημαντικός παράγοντας του υδατογραφήματος είναι το κλειδί το οποίο πρέπει να διέπεται από δύο βασικά χαρακτηριστικά, την τυχαιότητα στην παραγωγή και να είναι συσχετισμένο με το υδατογράφημα. Για την τυχαία παραγωγή του κλειδιού πρέπει να εφαρμοσθούν έξυπνες και μη στατιστικά ευρέσιμες μέθοδοι. Σε αυτή την κατεύθυνση μπορεί να βοηθήσουν τα εφαρμοσμένα μαθηματικά τα οποία προσφέρουν μία σειρά από μεθόδους που μπορούν να εφαρμοσθούν όπως οι ψευδοτυχαίες γεννήτριες αριθμών. Για την καλή συσχέτιση του κλειδιού με το υδατογράφημα θα πρέπει να χρησιμοποιηθούν και μέθοδοι που χρησιμοποιεί η επιστήμη των σημάτων. Η επεξεργασία των σημάτων συσχετίζει τις ιδιότητες και τις δυνατότητες ενός σήματος με τα εφαρμοσμένα μαθηματικά. Μια τέτοια εφαρμογή είναι η δημιουργία και η χρήση των ψευδοτυχαίων ακολουθιών οι οποίες χρησιμοποιούν τα εφαρμοσμένα μαθηματικά και μορφές επεξεργασίας σήματος (φίλτρο, mpeg μοντέλο) δίνοντας πολύ καλά αποτελέσματα στα υδατογραφημένα προϊόντα όταν χρησιμοποιούνται σαν κλειδί υδατογράφησης.

e) Η ανίχνευση του υδατογραφήματος γίνεται πάντα με μία πιθανότητα λάθους. Η μείωση της πιθανότητας αυτής βασίζεται κατ' αρχάς στην ίδια τη μέθοδο και στον τρόπο που εφαρμόζεται η ένθεση του υδατογραφήματος. Η χρήση των συναρτήσεων πιθανότητας συντελούν ενισχυτικά στην επίτευξη μιας αξιόπιστης ανίχνευσης. Τέλος η ανίχνευση για λόγους ευχρηστίας δεν πρέπει να απαιτεί το αρχικό προϊόν γεγονός που στη συγκεκριμένη υλοποίηση επιτυγχάνεται μόνο από το σχήμα με βάση το μέτρο.

Από τα συμπεράσματα φαίνεται το ευρύ επιστημονικό πεδίο το οποίο απαιτεί η εφαρμογή και έρευνα της μεθόδου υδατογράφησης. Συγκεκριμένα στην υλοποίηση που έγινε για την υδατογράφηση αρχείων ήχου εφαρμόσθηκαν οι τρεις βασικές υδατογράφησης ήχου:

a) Υδατογράφηση με βάση το μέτρο

b) Υδατογράφηση φάσης

c) Υδατογράφηση διεσπαρμένου φάσματος (spreadspectrum)

Η κάθε μία από τις παραπάνω μεθόδους αναλύθηκε ξεχωριστά ως προς το μηχανισμό της μεθόδου υδατογράφησης ήχου, ως προς τον τρόπο που υλοποιήθηκε και τα αποτελέσματα που κατέδειξε. Εδώ θα γίνει μία πιο γενική ανάλυση των συμπερασμάτων ως προς τις διαπιστώσεις που αναδείχθηκαν από την υλοποίηση της υδατογράφησης ήχου συγκρίνοντας και τις τρεις τεχνικές. Έγινε προσπάθεια σε κάθε μία μέθοδο να υπάρξουν οι προϋποθέσεις και τα χαρακτηριστικά που πρέπει να διέπουν ένα υδατογραφημένο ήχο. Η κάθε μέθοδος όμως ανέδειξε και διαφορετικές δυνατότητες γι' αυτό μπορούμε να επισημάνουμε τα εξής:

1) Η μέθοδος του διεσπαρμένου φάσματος (spread spectrum) αποτελεί μία πιο πλήρη μέθοδο υδατογράφησης ήχου καθώς σχεδόν σε όλα τα χαρακτηριστικά που διέπουν τα υδατογραφημένα της αρχεία ήχου επιφέρει καλύτερα αποτελέσματα από τις δύο άλλες τεχνικές. Η διαπίστωση αυτή ήταν αναμενόμενη μιας και η spread spectrum χρησιμοποιεί μία πιο πολύπλοκη τεχνική υδατογράφησης ήχου τόσο για την ένθεση και την ανίχνευση όσο και για την παραγωγή του κλειδιού. Η χρήση των ιδιοτήτων των ηχητικών σημάτων μέσω του οπτικοακουστικού μοντέλου mpeg και επιπλέον των μορφών επεξεργασίας σημάτων (μετασχηματισμός Fourier, φίλτρα, βάθμωση, ενεργειακό φάσμα κτλ) από τη spread spectrum δικαιολογούν τα θετικά της αποτελέσματα.

2) Η μέθοδος της υδατογράφησης φάσης δημιουργεί πολύ ανθεκτικά υδατογραφήματα παρατηρείται όμως μία μικρή παραμόρφωση στο υδατογραφημένο σήμα λόγω της απευθείας τροποποίησης της φάσης του ήχου. Επιπλέον η ανίχνευση του υδατογραφήματος είναι και εδώ αξιόπιστη όμως χρησιμοποιείται το αρχικό προϊόν όπως και στη spread spectrum.

3) Η υδατογράφηση με βάση το μέτρο ενθέτει αρκετή ποσότητα πληροφορίας στο αρχικό αρχείο ήχου και η ποιότητα του υδατογραφημένου αρχείου ήχου είναι πολύ καλή. Παρουσιάζει όμως ένα βασικό μειονέκτημα, την επίδραση του θορύβου καναλιού η οποία μειώνει την ανθεκτικότητα του υδατογραφήματος. Εδώ στον αλγόριθμο εφαρμόσθηκε κατάλληλη μετατόπιση ώστε η επίδραση του θορύβου να μειωθεί, παρ' όλ' αυτά η ανθεκτικότητα του υδατογραφημένου ήχου της spread spectrum είναι σαφώς καλύτερη από εκείνη της phase watermark.

4) Τέλος το κλειδί που προστίθεται από τον ιδιοκτήτη στη spreadspectrum και στη

phase watermark είναι με αναπαράσταση των εννέα δυαδικών ψηφίων, πράγμα που εύκολα μεταβάλλεται στα 128 bits για να είναι η πολυπλοκότητα σχεδόν άπειρη (ο προβλεπόμενος χρόνος είναι για ανεύρεση του κλειδιού με brute force attack είναι 3,237*1032 χρόνια).

Η προστασία δεδομένων με τη μέθοδο της υδατογράφησης αποτελεί μία μέθοδο που οικειοποιήθηκε την εμπειρία και τη γνώση που προϋπήρχε στις προηγούμενες μεθόδους προστασίας δεδομένων (κρυπτογραφία, ψηφιακή υπογραφή) και επιπλέον ασχολήθηκε και με την προστασία των πνευματικών δικαιωμάτων. Στη συνέχεια η προσέγγιση του υδατογραφήματος θα γίνει σ' όλο το επιστημονικό φάσμα που καλύπτει και μέσα από τις μεθόδους που χρησιμοποιεί. Τέλος η υλοποίηση θα καταδείξει με ποιον τρόπο όλα τα προηγούμενα εφαρμόζονται στην πράξη.

2

ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

2.1 Εισαγωγή

Η ταχύτατη ανάπτυξη και εισαγωγή της ψηφιακής τεχνολογίας στη ζωή μας προτάσσει ως πρωταρχική ανάγκη την ανάπτυξη ενός αξιόπιστου και ανθεκτικού μηχανισμού για την προστασία των ψηφιακών δεδομένων είτε αυτά είναι εικόνες, είτε κομμάτια ήχου είτε βίντεο είτε πολυμέσα με τη γενικότερη έννοια. Μεγάλο ενδιαφέρον παρουσιάζεται για τον σχεδιασμό εκείνου του μηχανισμού που θα παρέχει μερική ή απόλυτη προστασία των ψηφιακών δεδομένων από τους πειρατές. Οι επιθέσεις των κακόβουλων χρηστών είναι μέρος της καθημερινότητας στο χώρο της νέας τεχνολογίας και περιλαμβάνουν παράνομη πρόσβαση σε μεταφερόμενα δεδομένα μέσω του διαδικτύου, μετατροπή στο περιεχόμενο των δεδομένων και παραγωγή επαναμετάδοση ή των παράνομων αντιγράφων. Έτσι προκαλούν άγχος σχεδόν σε όλους μιας και οι συνέπειες που μπορούν να αποφέρουν είναι αρκετά μεγάλες και σε οικονομικό κόστος (λόγω απώλειας κερδών που προκαλείται από την μη εξουσιοδοτημένη πρόσβαση) και στην μείωση της αξιοπιστίας των κωδικών ασφαλείας.

Η προστασία δεδομένων αποτελεί πρόκληση για απάντηση και επίλυση. Είναι φυσικό να αναπτυχθούν μέθοδοι που προσπάθησαν να απαντήσουν από διαφορετικές αφετηρίες και που τόσο η ανάπτυξη όσο και η εξέλιξη τους επηρεάζουν την ανάπτυξη της τεχνολογίας και της επιστήμης.

i. Η μετάδοση δεδομένων μέσω των γραμμών επικοινωνίας ενός δικτύου μπορεί να προστατεύεται από μη εξουσιοδοτημένους παραλήπτες χρησιμοποιώντας τεχνικές που

βασίζονται στην κρυπτογραφία. Αυτό επιτυγχάνεται με την χρήση ενός προσωπικού κλειδιού (private key) κατάλληλου για την αποκρυπτογράφηση των λαμβανόμενων δεδομένων μέσω ενός δημοσίου (public) αλγορίθμου ο οποίος είναι υλοποιημένος είτε σε υλικό είτε σε λογισμικό. Στόχος αυτού του είδους των μεθόδων αυτής είναι οι γρήγορες διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης από κάθε εξουσιοδοτημένο χρήστη.

ii. Μια άλλη μέθοδος προστασίας στηρίζεται στη χρήση της ψηφιακής υπογραφής για την πιστοποίηση της αυθεντικότητας του περιεχομένου των προστατευόμενων δεδομένων. Το περιεχόμενο των δεδομένων μπορεί να τροποποιηθεί για πολλαπλούς είτε νόμιμους είτε παράνομους σκοπούς (συμπίεση, αφαίρεση θορύβου, καταστροφική μεταβολή δεδομένων).Η ψηφιακή υπογραφή προστίθεται στα μεταδιδόμενα δεδομένα για να είναι εφικτή η επιβεβαίωση της αυθεντικότητας τους και συνίσταται σε κωδικοποιημένη πληροφορία της ίδιας μορφής με το πληροφοριακό περιεχόμενο των ψηφιακών δεδομένων που θέλουμε να προστατεύσουμε. Η πιστοποίηση της αυθεντικότητας βασίζεται σε δημόσιους (public) αλγορίθμους και προσωπικά κλειδιά (private keys).

iii. Η τρίτη μέθοδος και πιο πρόσφατη που προτάθηκε για την προστασία των δεδομένων είναι το υδατογράφημα. Το υδατογράφημα έρχεται να απαντήσει στο πρόβλημα της προστασίας των πνευματικών δικαιωμάτων στα ψηφιακά δεδομένα. Το γεγονός ότι η αναπαραγωγή ενός ψηφιακού προϊόντος είναι εύκολη και αρκετά προσιτή, σε συνδυασμό με το γεγονός ότι στο διαδίκτυο η επαναμετάδοση ενός αντιγράφου στον υπόλοιπο κόσμο είναι εφικτή, κάνει την απόδειξη της πνευματικής ιδιοκτησίας σχεδόν αδύνατη. Η πιστοποίηση των πνευματικών δικαιωμάτων βάλλεται από αυτούς που παράνομα διεκδικούν τα δικαιώματα εκμετάλλευσης από το δημιουργό του και σε αυτό απαντά το υδατογράφημα προστατεύοντας τα πνευματικά δικαιώματα στα ψηφιακά προϊόντα.. Το υδατογράφημα παρέχει μορφές προστασίας τελείως διαφορετικής μορφής από εκείνες που είθισται να παρέχουν οι προηγούμενες μέθοδοι προστασίας δεδομένων. Με το υδατογράφημα πιστοποιείται η κυριότητα του ιδιοκτήτη του προϊόντος εύκολα με την ένθεση έξυπνου σήματος πάνω στο ψηφιακό προϊόν χωρίς να αλλοιώνεται η ηχητική του ποιότητα ή η ευκρίνεια.

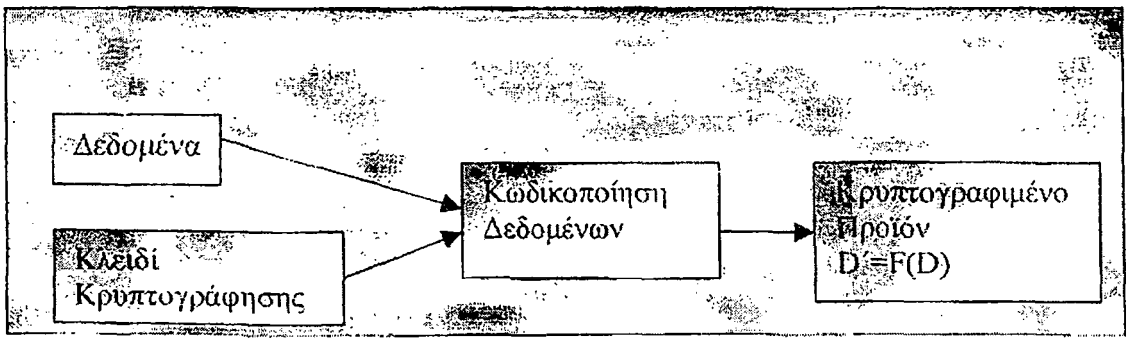
Η ευρύτητα του φάσματος προστασίας της υδατογράφησης οφείλεται στο γεγονός ότι αποτελεί μια τελείως διαφορετική μέθοδο και ως προς τον τρόπο υλοποίησης του μηχανισμού της και ως προς τα θεαματικά αποτελέσματα που επιφέρει. Το υδατογράφημα δεν χρησιμοποιεί την κρυπτογράφηση των δεδομένων, ώστε να κλειδώσει την πληροφορία του προϊόντος αλλά με έξυπνο τρόπο ενσωματώνει πληροφορία προστασίας των πνευματικών δικαιωμάτων στο προϊόν. Έτσι στο υδατογράφημα δεν απαιτείται αποκρυπτογράφηση του προϊόντος από τον νόμιμο κάτοχο για να μπορεί να το χρησιμοποιήσει. Οι δυσάρεστες συνέπειες της χρησιμοποίησης αλγόριθμων κρυπτογράφησης και αποκρυπτογράφησης, όπως χρονικές καθυστερήσεις για την προσέγγιση του τελικού προϊόντος , η πολυπλοκότητα το τεράστιο κόστος των ίδιων των αλγορίθμων, δεν επηρεάζουν την μέθοδο της υδατογράφησης. Το προϊόν βρίσκεται στα χέρια του χρήστη γρήγορα, εύκολα, επιπλέον μπορεί οπότε αυτός το επιλέξει να ανιχνεύσει την αυθεντικότητα του προϊόντος και μάλιστα χωρίς να έχει χρησιμοποιηθεί η δαπανηρή και χρονοβόρα κρυπτογράφηση.

2.2 Κρυπτογραφία (Cryptography)

Η μέθοδος της κρυπτογραφίας [55] όταν πρωτοεμφανίστηκε αποτέλεσε για πολλούς την απάντηση στο πρόβλημα της προστασίας δεδομένων. Η ευρεία χρήση της τα προηγούμενα χρόνια έκανε τους ερευνητές να εμβαθύνουν στη μέθοδο αυτή αλλά αντίστοιχα και στους πειρατές να ανακαλύψουν τα μειονεκτήματα της. Θα ήταν εύστοχο να αναλύσουμε λίγο περισσότερο την μέθοδο αυτή.

Η κρυπτογραφία παρέχει προστασία στην πληροφορία που μεταφέρεται μέσω του τηλεπικοινωνιακού υλικού από τους μη εξουσιοδοτημένους παραλήπτες. Η μέθοδος της κρυπτογράφησης συνίσταται σε δυο επίπεδα:

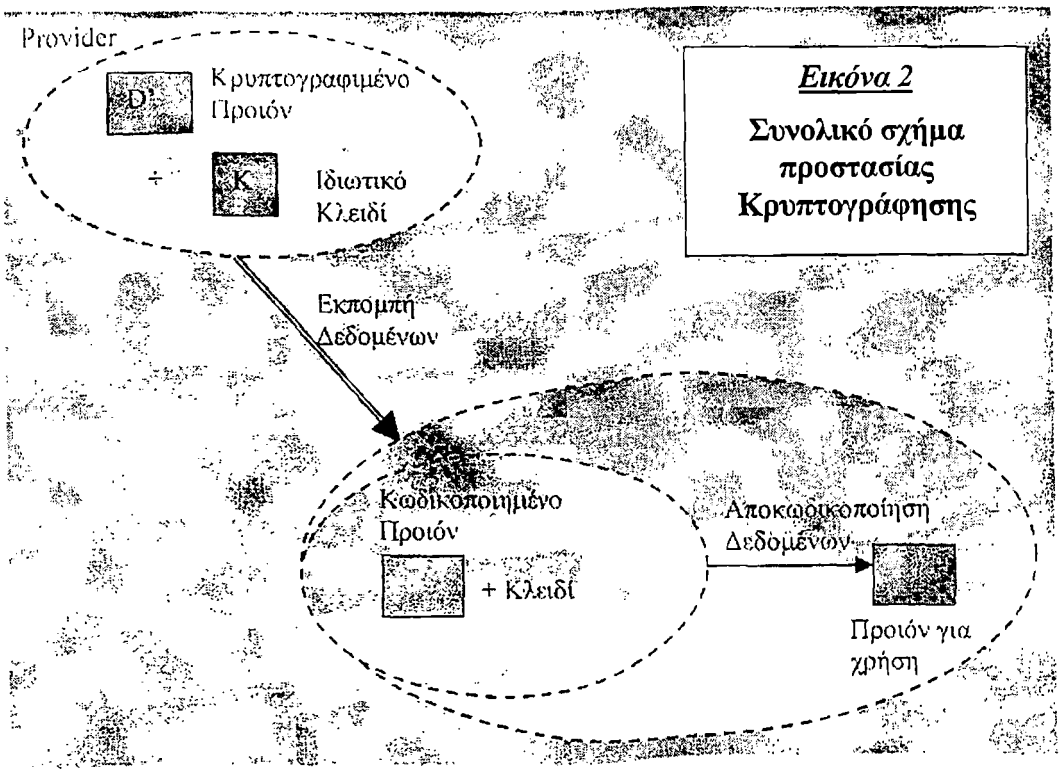
1. Τα πραγματικά δεδομένα στο επίπεδο παροχέα (provider) εκπέμπονται κωδικοποιημένα, χρησιμοποιώντας ο εκπομπός (provider) ένα προσωπικό κλειδί (private key).



Εικόνα 1 **Διαδικασία Κρυπτογράφησης**

2. Οι χρήστες μπορούν να αποκωδικοποιήσουν τα δεδομένα που παρέλαβαν κάτω από δύο προϋποθέσεις:
   - Να έχουν τον κατάλληλο αλγόριθμο υλοποιημένο σε υλικό ή λογισμικό y.

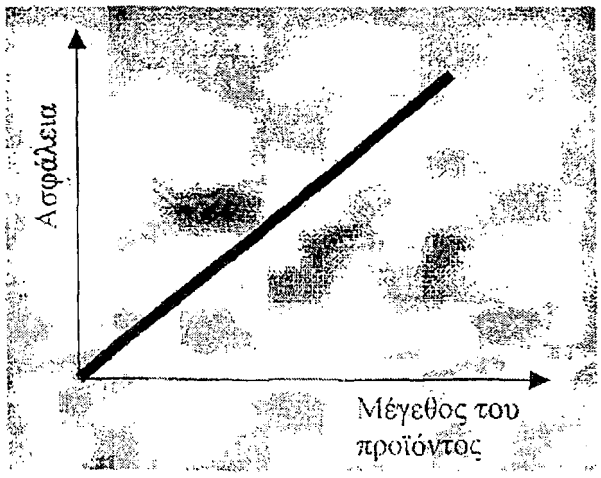
- Να έχουν είτε το ιδιωτικό κλειδί του provider είτε ένα συσχετισμένο δημόσιο κλειδί.



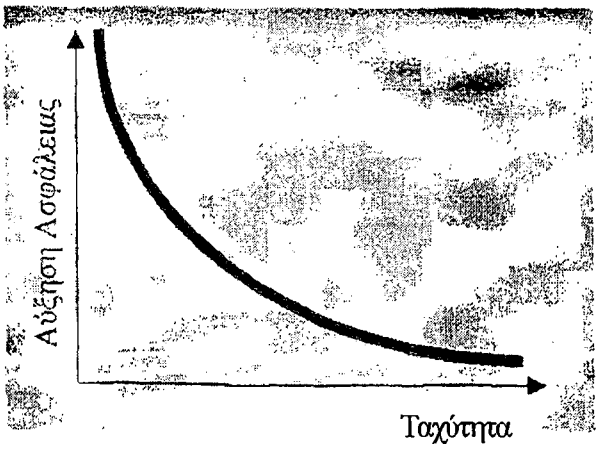
Εικόνα 2

Συνολικό σχήμα προστασίας Κρυπτογράφησης

Η ευρεία χρήση αυτής της μεθόδου είχε σαν αποτέλεσμα τη συσσώρευση αποτελεσμάτων και τη διαπίστωση πλεονεκτημάτων και αδυναμιών. Πολλά μειονεκτήματα μπορούν να παρακαμφθούν, άλλα όμως όχι, ενώ παράλληλα τα συμπεράσματα δεν αποτελούν γνώση μόνον των ερευνητών ή των χρηστών αλλά και των πειρατών. Έτσι, για την επιτυχή χρήση της κρυπτογραφίας η γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Αυτό οδήγησε την υλοποίηση ταχύτατων αλγορίθμων οι οποίοι ήταν στη διάθεση των εξουσιοδοτημένων χρηστών. Επιπλέον η ευρεία χρήση του δικτύου δημιούργησε την εξοικείωση των χρητών με τη νέα τεχνολογία αλλά και διάφορες απαιτήσεις. Η απαίτηση για εύκολη και γρήγορη πρόσβαση όπως και για εύχρηστη λειτουργία έγινε κοινό αίτημα των χρηστών. Η κρυπτογραφία σε ένα ψηφιακό προϊόν αυξάνει αρκετά το μέγεθος των δεδομένων γεγονός που επηρεάζει την ευχρηστία του προϊόντος (μείωση της ταχύτητας παραλαβής) και επιβάλλει τη δαπάνη ικανού χρονικού διαστήματος για τη διεκπεραίωση της αποκρυπτογράφησης στη μεριά του χρήστη. Για να περιοριστούν οι αρνητικές συνέπειες θα πρέπει η κρυπτογραφία να προκαλεί μικρή αύξηση του μεγέθους της πληροφορίας και παράλληλα η διαδικασία της αποκρυπτογράφησης να συντελείται πολύ γρήγορα.



Εικόνα 3 **Διάγραμμα συναρτήσει της ποσότητας**



Εικόνα 4 **Διάγραμμα συναρτήσει της ταχύτητας**

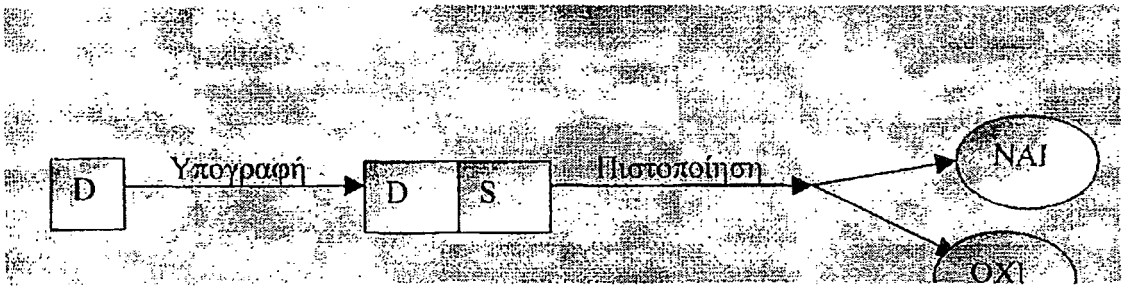
Από μια άλλη οπτική γωνία η μέθοδος αυτή θα πρέπει να είναι επαρκής ώστε να αποτρέπει την αποκρυπτογράφηση από κακόβουλους χρήστες. Εδώ είναι και το δίπολο πού θέτει την κρυπτογραφία στο κέντρο των επιστημονικών αντιπαραθέσεων. Από τη μία πλευρά πρέπει να τίθενται όρια στο μέγεθος των δεδομένων και από την άλλη το χρησιμοποιούμενο κλειδί πρέπει να είναι επαρκές για την προστασία του από την διαδικασία δοκιμής-λάθους ώστε να αποφεύγεται η αποκρυπτογράφηση και συνάμα εύκολα απόκρυπτογραφήσιμο από το νόμιμο κάτοχο.

Τέλος, το μεγαλύτερο πρόβλημα στο χώρο της κρυπτογραφίας είναι πώς αν τελικά τα ψηφιακά δεδομένα αποκρυπτογραφηθούν, δεν υπάρχει κανένα άλλο μέσον ή τρόπος για την απόδειξη ή μη της αυθεντικότητας τους.

2.3 Αυθεντικότητα - Ψηφιακή Υπογραφή (Authentication - Digital Signature)

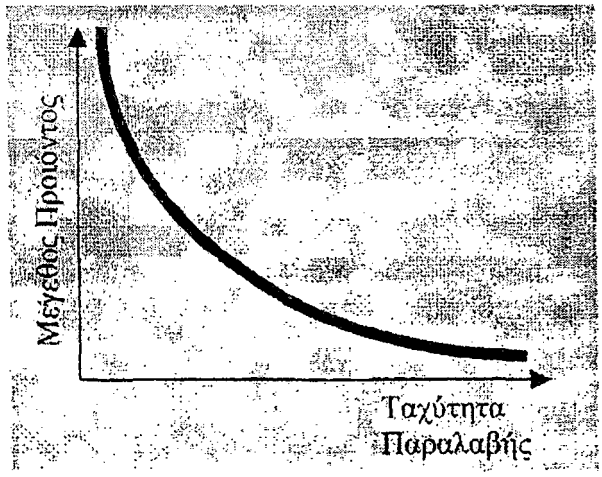
Στην κρυπτογραφία όλη η έρευνα, για την αποφυγή των διαφόρων επιθέσεων, χάνονται όταν το προϊόν αποκρυπτογραφηθεί. Αυτή η συνεχής έρευνα, ο διαρκής αγώνας του ερευνητή να υλοποιήσει έναν αξιόπιστο αλγόριθμο κρυπτογράφησης που να μην είναι προβλέψιμος από τους πειρατές, δεν φαινόταν να έχει τέλος. Υπάρχει στην φύση της ανθρώπινης νόησης να βρίσκει νέους τρόπους και μεθόδους. Από τη μία οι ερευνητές προσπαθούν να δίνουν ολοένα και πιο εφευρετικούς αλγορίθμους κρυπτογράφησης αλλά από την άλλη οι πειρατές κατανοούν τους αλγορίθμους αυτούς ή οικειοποιούνται τις αδυναμίες τους και τους αποκρυπτογραφούν γρήγορα. Εδώ τίθεται πραγματικά ένα ουσιαστικό ερώτημα ότι ίσως η προστασία δεδομένων θα πρέπει να σχετίζεται όχι μόνο με την απαγόρευση στους μη εξουσιοδοτημένους παραλήπτες της κατοχής και αποκρυπτογράφησης του προϊόντος, αλλά και την πιστοποίηση της αυθεντικότητας του.

Η πιστοποίηση της αυθεντικότητας [76] αποτέλεσε την απάντηση σε πολλά μειονεκτήματα της κρυπτογραφίας, δεδομένου ότι ένα ψηφιακό προϊόν υφίσταται αρκετές τροποποιήσεις, με συνέπεια το τροποποιημένο προϊόν να μην έχει καμία σχέση με το αυθεντικό. Έτσι προκύπτει το βασικό μέλημα της εύρεσης μιας μεθόδου που να πιστοποιεί την αυθεντικότητα του προϊόντος. Αυτό είναι και το σκεπτικό, όπου βασίζεται και η υλοποίηση της μεθόδου της ψηφιακής υπογραφής. Η μέθοδος αυτή προσπαθεί να ελέγξει την αυθεντικότητα του περιεχομένου ενός ψηφιακού προϊόντος. Εδώ θα ασχοληθούμε με τα βασικά σημεία της μεθόδου και θα καταδείξουμε τα πλεονεκτήματα και τα μειονεκτήματα της. Η ψηφιακή υπογραφή αποτελείται από ένα κωδικοποιημένο μήνυμα το οποίο πρέπει να αντιστοιχεί σε ένα συγκεκριμένο αυθεντικό προϊόν. Στο επίπεδο του provider, τα δεδομένα στέλνονται μαζί με αυτή την ψηφιακή υπογραφή (digital signature), ενώ στη διαδικασία πιστοποίησης γίνεται μέσω της χρήσης δημοσίων αλγορίθμων και δημοσίων κλειδιών. Η βασική ιδέα βασίζεται στο ότι οποιαδήποτε αλλαγή στο περιεχόμενο των δεδομένων ή στην υπογραφή, θα έχει ως αποτέλεσμα την αποτυχία της πιστοποίησης του προϊόντος. Πράγματι, η λειτουργία-χρησιμοποίηση των ψηφιακών υπογραφών προχώρησε την αντίληψη των ερευνητών για την προστασία των ψηφιακών δεδομένων ένα βήμα μπροστά.



Εικόνα 5 **Διαδικασία ψηφιακής υπογραφής**

Παρόλα αυτά όμως υπάρχουν μειονεκτήματα που παρατηρήθηκαν με την ευρεία εφαρμογή της μεθόδου. Τα προϊόντα που συνήθως διακινούνται μέσω του δικτύου και διεκδικούν την προστασία της αυθεντικότητας τους , πρόκειται για προϊόντα με μεγάλο μέγεθος των οποίων το κόστος παραγωγής τους δεν είναι ευκαταφρόνητο, όπως τα πολυμεσικά προϊόντα (multimedia). Σε αυτή την κατηγορία που είναι και δείχνει αρκετά μεγάλο ενδιαφέρον στο κεφάλαιο της προστασίας των ψηφιακών δεδομένων, η μέθοδος της ψηφιακής υπογραφής δεν δίνει ικανοποιητική απάντηση. Εδώ βρίσκεται και το βασικότερο μειονέκτημα της μεθόδου καθώς οι ασφαλής και έξυπνες υπογραφές για τα πολυμεσικά προϊόντα δεν υπάρχουν. Λαμβάνοντας υπόψη ότι πρόκειται για προϊόντα με μεγάλο μέγεθος και ότι η ψηφιακή υπογραφή είναι ανάλογη με το μέγεθος των δεδομένων, μια λύση μέσω της μεθόδου της αυθεντικότητας δεν είναι αποδοτική.



Εικόνα 6 **Πρόβλημα αποδοτικότητας**

Η απάντηση για την πιστοποίηση των ψηφιακών προϊόντων δεν μπορεί να δοθεί καθολικά από την μέθοδο των ψηφιακών υπογραφών. Η μέθοδος της ψηφιακής υπογραφής αποτέλεσε το κέντρο απασχόλησης πολλών ερευνητών, και αφού η απάντηση της ψηφιακής υπογραφής δεν ήταν επαρκής για την περίπτωση των πολυμεσικών προϊόντων, άνοιξε ένας δίαυλος διαλόγου σχετικά με τους στόχους που θα πρέπει να έχει μια μέθοδος προστασίας των ψηφιακών δεδομένων.

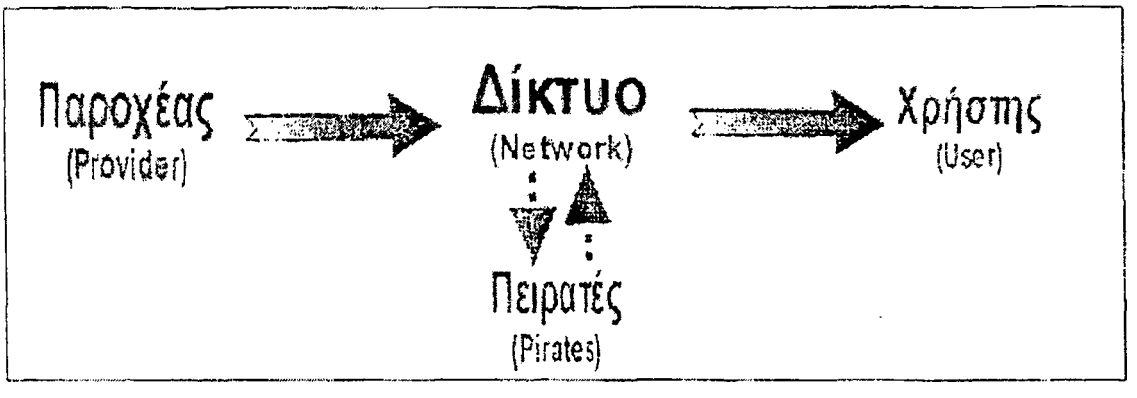
2.4 Η ιδέα της προστασίας των Πνευματικών Δικαιωμάτων

2.4.1 Εισαγωγή

Το δίκτυο (WWW) αποτέλεσε ένα μέσο που άλλαξε ριζικά την αντίληψη του ανθρώπου

για την έννοια της επικοινωνίας και της μεταφοράς δεδομένων. Είναι η μόνη αμφίπλευρη μορφή επικοινωνίας και ίσως ο πιο αποδοτικός τρόπος αναζήτησης και μεταφοράς οποιουδήποτε ψηφιακού προϊόντος. Ένας χρήστης του δικτύου μπορεί να έρθει σε επαφή με οποιοδήποτε σημείο του πλανήτη σε πολύ μικρό χρονικό διάστημα χωρίς να χρειάζεται να δηλώσει την ταυτότητα του.

Ένα τέτοιο τεχνολογικό επίτευγμα που αλλάζει ραγδαία την επικοινωνία και την εμπορικές ανταλλαγές των ανθρώπων ήταν φυσικό να επηρεάσει και την οικονομία, την επιστήμη, τις τέχνες, το εμπόριο, σχεδόν κάθε δραστηριότητα του ανθρώπου. Σήμερα αποτελεί καθημερινή πραγματικότητα η πιο μικρή ως την πιο μεγάλη εταιρία να διαθέτει τα προϊόντα της (τουλάχιστον αυτά που είναι δυνατόν) μέσα από το δίκτυο (WWW), ενώ ταυτόχρονα ένας μέσος χρήστης μπορεί να ψάξει στο δίκτυο με τις μηχανές ψαξίματος για το προϊόν που επιθυμεί σε όλο τον κόσμο και να το παραλάβει με μικρή επιβάρυνση. Εκτός από το άνοιγμα νέων οριζόντων στο εμπόριο και την επιστήμη, δημιουργήθηκαν και αρκετά ερωτήματα - προβλήματα.



Εικόνα 7 **Πρόβλημα προστασίας στο δίκτυο**

Παλαιότερα ένα προϊόν βρισκόταν στο ράφι του μαγαζιού και ο ίδιος ο μαγαζάτορας ήταν υπεύθυνος για την ποιότητα και αξιοπιστία του προϊόντος και ήταν υπόλογος στον πελάτη. Σήμερα οι σχέσεις συναλλαγής είναι πιο περίπλοκες. Σήμερα η αναπαραγωγή ενός ψηφιακού προϊόντος είναι εύκολη και προσιτή ενώ ταυτόχρονα το αντίγραφο που δεν έχει καμία διαφορά από το πρωτότυπο μπορεί να διανεμηθεί μέσω του δικτύου σε χιλιάδες χρήστες. Το γεγονός αυτό διαφοροποιεί τη σχέση παραγωγού - προϊόντος μιας και παλιότερα μόνο ο νόμιμος ιδιοκτήτης είχε το δικαίωμα της παροχής ενός προϊόντος ενώ σήμερα οποιοσδήποτε μπορεί σε λίγο χρόνο και εύκολα να παρέχει το αντίγραφο (όμοιο με το πρότυπο) στον καθένα.

Στο σημείο αυτό πρέπει να μιλήσουμε για την έννοια που πήρε βάρος στον 20° αιώνα τα πνευματικά δικαιώματα. Οι ψηφιακές υπογραφές πιστοποιούσαν μόνο την αυθεντικότητα ενός προϊόντος, που δεν είναι ταυτόσημη με τα πνευματικά δικαιώματα. ένα νόμιμο και αξιόπιστο προϊόν.

2.4.2 Η απάντηση του υδατογραφήματος

Σε μια εποχή που η γνώση εμπορευματοποιείται και τα προϊόντα περιέχουν τεχνογνωσία είναι φυσιολογικό πως η παράνομη αναπαραγωγή και διανομή μειώνει την αξία του προϊόντος. Τα πνευματικά δικαιώματα είναι τα δικαιώματα που έχει ο ιδιοκτήτης για την διανοητική και τεχνολογική του συνεισφορά στην παραγωγή του προϊόντος. Το πρόβλημα που προκύπτει είναι η αποτροπή αυτών που παράνομα διεκδικούν τα πνευματικά δικαιώματα από ένα προϊόν και η πιστοποίηση της αυθεντικότητας του προϊόντος αυτού ώστε οι χρήστες να μπορούν να είναι βέβαιοι ότι χρησιμοποιούν.

Αυτοί είναι λίγοι από τους προβληματισμούς που έστρεψαν τους ερευνητές στην

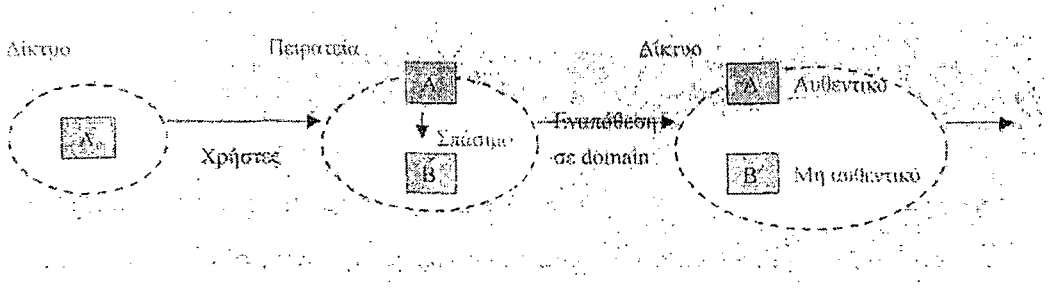
αναζήτηση μιας μεθόδου προστασίας δεδομένων που θα δίνει ικανοποιητική απάντηση και στο πρόβλημα των πνευματικών δικαιωμάτων. Παρόλα αυτά αναλύοντας την νέα ανάγκη που προέκυψε για την προστασία των πνευματικών δικαιωμάτων, θα έπρεπε να απαντάει και στις μέχρι τώρα αιτήσεις που απαντούσαν οι προηγούμενες μέθοδοι. Η μόνη μέθοδος που απαντά στο ζήτημα του copyright είναι η μέθοδος του υδατογραφήματος, χωρίς αυτό να σημαίνει ότι δεν απαντά και στην αυθεντικότητα ενός ψηφιακού προϊόντος. Στην προσπάθεια να αναλύσουμε αυτή την μέθοδο αυτό που πρώτα θα πρέπει να επισημάνουμε είναι ότι η μέθοδος του υδατογραφήματος αναπτύχθηκε στηριζόμενη σε τεχνικές προστασίας των πνευματικών δικαιωμάτων.

Το υδατογράφημα μεταβάλει αυστηρά τα ψηφιακά δεδομένα ούτως ώστε να προσάπτεται σε αυτά αόρατη πληροφορία σχετικά με την ιδιοκτησία. Το υδατογράφημα μπορεί να περιέχει πληροφορία που να πιστοποιούν και την αυθεντικότητα όπως το όνομα του δημιουργού, την εταιρία παραγωγής η και επιπλέον πληροφορίες όπως ημερομηνία και ώρα παραγωγής. Υπάρχουν αλγόριθμοι που μπορούν τροποποιώντας ένα ψηφιακό προϊόν να εναποθέσουν μέσα σε αυτό ένα υδατογράφήμα και να πιστοποιήσουν την κυριότητα του. Μπορεί με την χρήση δημοσίων ή ιδιωτικών κλειδιών να γίνει εντοπισμός του υδατογραφήματος και επιπλέον να μπορεί να ελεγχθεί η εγκυρότητα του προϊόντος άρα και να αναγνωριστεί η αυθεντικότητα του. Άρα το υδατογράφημα γεννιέται και ανιχνεύεται σε ένα ψηφιακό προϊόν.

Η οριοθέτηση των πνευματικών δικαιωμάτων σε ένα περιβάλλον όπου ο παγκόσμιος ιστός είναι ένα δύσκολο εγχείρημα. Το υδατογράφημα προσπαθεί να απόδοση μια τεχνολογικά ευφυή προστασία στα ψηφιακά προϊόντα, γεγονός που απαιτεί και πολλαπλές προϋποθέσεις. Αν σκεφτεί κανείς πως η τεχνολογική εξέλιξη στον τομέα της ψηφιακής τεχνολογίας είναι ραγδαία, η ανάπτυξη ενός αξιόπιστου και ανθεκτικού σχήματος για την προστασία των δεδομένων των πολυμεσικών προϊόντων τίθεται υπό αμφισβήτηση. Το υδατογράφημα πρέπει να μπορεί να απαντάει στη σημερινή πραγματικότητα όπου η μετάδοση, μετατροπή και αποθήκευση προϊόντων σε ψηφιακή μορφή είναι συνήθεις ενέργειες ενός απλού χρήστη.

Η ηλεκτρονική βιβλιογραφία, οι ψηφιακές βιβλιοθήκες, οι βάσεις δεδομένων και ο παγκόσμιος ιστός είναι εφαρμογές της τεχνολογίας με βάση τα ψηφιακά προϊόντα οι οποίες βάλλονται συνεχώς από τις επιθέσεις πειρατών. Η πειρατεία περιλαμβάνει παράνομη πρόσβαση στα μεταδιδόμενα δεδομένα μέσω των δικτύων μεταφοράς, πολλαπλές και ποικίλες τροποποιήσεις της πληροφορίας και επαναμετάδοση. Επιθέσεις τις οποίες ένα σχήμα προστασίας δεδομένων όπως το υδατογράφήμα πρέπει να λαμβάνει σοβαρά υπόψη του.

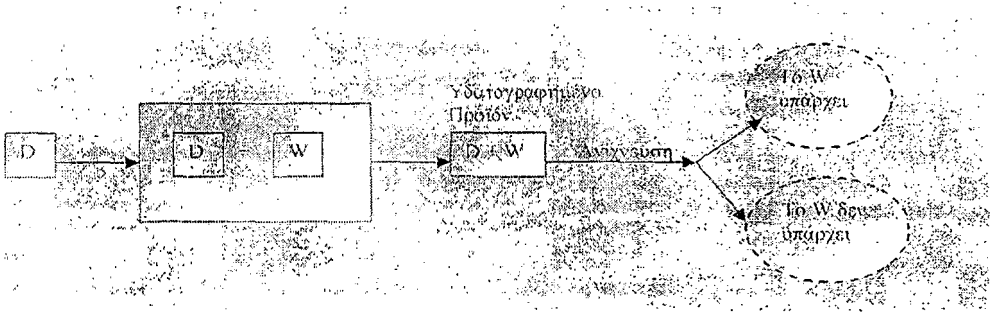
Είναι προφανές λοιπόν ότι τα ψηφιακά δεδομένα διακινούνται και μορφοποιούνται μέσω διαδικτυακών εφαρμογών και υπηρεσιών. Ένα προϊόν διατίθεται στο κοινό μέσω ηλεκτρονικών σελίδων που περιέχουν προνόμια ομότιμης εταιρίας ή είναι ιδιόκτητες. Η πρόσβαση σε αυτές τις σελίδες γίνεται από οποιοδήποτε χρήστη υπολογιστή. Για να εγγυηθεί το υδατογράφημα προστασία των πνευματικών δικαιωμάτων, θα πρέπει να εμποδίσει τους πειρατές από τη διάθεση παράνομων προϊόντων στους χρήστες μέσω της αναπαραγωγής του αυθεντικού προϊόντος .Οι πειρατές μπορεί να καταφέρουν με διάφορες τροποποιήσεις να διαθέσουν στους χρήστες του δικτύου το παράνομο υλικό. Αυτές οι δραστηριότητες δεν είναι καθόλου παράξενες ή σπάνιες και γι αυτό το λόγο ο ιδιοκτήτης και ο χρήστης έχουν απαιτήσεις.



Εικόνα 8 **Πρόβλημα Προστασίας του Δικτύου**

Ο ιδιοκτήτης, είτε είναι εταιρία που επένδυσε σε ένα προϊόν και απαιτεί να της πιστοποιηθεί η τεχνογνωσία πάνω στο προϊόν είτε είναι ο απλός δημιουργός που απαιτεί τα δικαιώματα του στην πνευματική του εργασία, επιθυμούν προστασία των προϊόντων τους στο χώρο που τα διαθέτουν. Απαιτείται λοιπόν μια μέθοδος προστασίας που να είναι συνεργάσιμη με μια μέθοδο ψαξίματος του παγκόσμιου ιστού ώστε να πιστοποιείται η εγκυρότητα των προϊόντων σε όλο το πεδίο πρόσβασης.

Οι χρήστες με τη σειρά τους απαιτούν να λαμβάνουν τα αυθεντικά προϊόντα που προσφέρουν συγκεκριμένες δυνατότητες, εφόσον οι ίδιοι έχουν ακολουθήσει νόμιμες διαδικασίες απόκτησης τους. Το υδατογράφημα έρχεται να απαντήσει στις παραπάνω απαιτήσεις καθώς μπορεί να εναποθέτει στα ψηφιακά προϊόντα διάφανη πληροφορία, η οποία υπάρχει μέσα στα δεδομένα που μεταφέρονται μέσω του δικτύου. Το υδατογράφημα δημιουργείται από τον ιδιοκτήτη ή με την εξουσιοδότηση του ίδιου από άλλους και μπορεί οποιαδήποτε στιγμή η ύπαρξη του ή η έλλειψη του αλλά πολύ περισσότερο και η απόπειρα μετατροπής του να ανιχνευθεί. Για να μπορέσει να γίνει κατανοητό αυτό, θα πρέπει να δώσουμε την εικόνα του βασικού μηχανισμού του υδατογραφήματος.



Εικόνα 9 **Μηχανισμός Υδατογράφησης**

2.4.3 Ορισμός του υδατογραφήματος

Καταρχήν μπορούμε να θεωρήσουμε το υδατογράφημα ως ένα ψηφιακό σήμα W, το οποίο υπερτίθεται στο ψηφιακό προϊόν μέσω μιας διαδικασίας ενσωμάτωσης. Μιας και η ενασχόληση μας περιλαμβάνει ψηφιακά προϊόντα, είναι βολικό για μας να περιγράψουμε το υδατογράφημα W σαν ένα σήμα δυαδικών ή τριαδικών συνιστωσών.

$$w = \{w(k); w(k) \in \{-1,0,1\}, £ \in w^d\}$$

όπου W^, η χωροδιάσταση όπου ανήκει το σύνολο των πιθανών σημάτων του υδατογραφήματος, και το d καταδεικνύει τον βαθμό ή με άλλα λόγια την διάσταση του χώρου.

Στην μονοδιάστατη αναπαράσταση το υδατογράφημα επεξεργάζεται ένα σήμα ήχου. Στην δισδιάστατη, ένα σήμα εικόνας και στην τρισδιάστατη ένα σήμα βίντεο. Το k είναι το διάνυσμα που προσδιορίζει τον μονοδιάστατο ή πολυδιάστατο χώρο W^. Το k αντιστοιχεί σε έναν μεγάλης ακρίβειας αριθμό ή ένα σετ αριθμών που χρησιμοποιούνται στην παραγωγή του W.

Έτσι λοιπόν οριοθετούμε την έννοια του υδατογραφήματος στον ψηφιακό κόσμο με την βοήθεια των διανυσμάτων και των σημάτων. Για να μπορέσουμε να προσεγγίσουμε βαθύτερα το υδατογράφημα θα πρέπει αρχικά να δούμε λεπτομερέστατα τη διαδικασία παραγωγής του σήματος W.

2.4.4 Διάγραμμα προστασίας του υδατογραφήματος

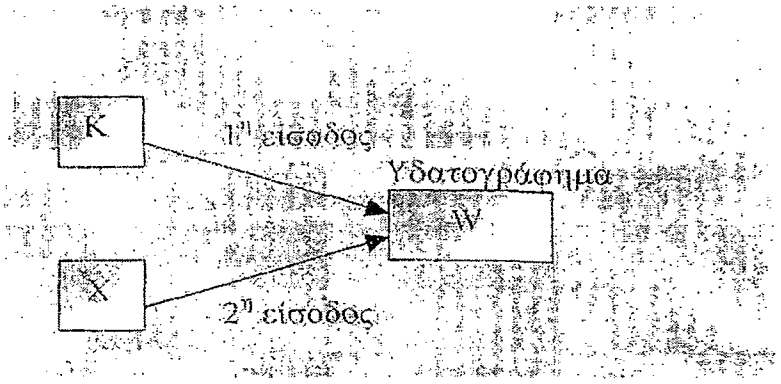
2.4.4.1 Παραγωγή του υδατογραφήματος (Watermark Generation)

Στην παραγωγή του υδατογραφήματος W [47] πρέπει να προσεχθούν σχεδόν όλα τα χαρακτηριστικά του ψηφιακού προϊόντος που θέλουμε να υδατογραφήσουμε έτσι ώστε η προσθήκη του υδατογραφήματος στο ψηφιακό προϊόν να μην αλλοιώνει την ποιότητα του εξασφαλίζοντας όσο είναι δυνατό τη μέγιστη αξιοπιστία του σε εξωγενείς κακόβουλες επιθέσεις.

Σημαντική ιδιότητα του υδατογραφήματος είναι η προσθήκη πληροφορίας να γίνει σε περιοχές δεδομένων, που η ανεύρεση της να είναι δύσκολη. Αυτό απαιτεί πολύ καλή γνώση των χαρακτηριστικών των σημάτων όπως επίσης και επίγνωση των χειρισμών που χρησιμοποιούν οι κακόβουλοι χρήστες. Αν τα δεδομένα προστεθούν εκεί που δεν υπάρχει πληροφορία τότε το υδατογράφημα θα αφαιρεθεί ακόμα και με τη χρήση συμπίεσης με απώλεια δεδομένων (lossy compression).

Η πληροφορία που ενσωματώνεται στο αρχικό σήμα πρέπει να είναι μοναδική. Γι' αυτό είναι σημαντικό να χρησιμοποιείται κλειδί υδατογράφησης k. Το αρχικό προϊόν μέσω του κλειδιού υδατογράφησης και ενός αλγορίθμου παράγουν το υδατογράφημα. Το υδατογράφημα πρέπει να είναι μοναδικό ώστε να μη μπορεί να προβλεφθεί με στατιστικές μεθόδους ή με μεθόδους σύγκρισης. Η παραγωγή του υδατογραφήματος πρέπει να δώσει σημασία στην ποιότητα του προϊόντος όπως επίσης και στο κλειδί k.

Η επιλογή του κλειδιού παίζει σημαντικό ρόλο ώστε να διασφαλίζεται ότι το υδατογράφημα είναι διαφορετικό ακόμη κι αν χρησιμοποιηθεί το ίδιο προϊόν. Επιλέγοντας το κλειδί με τυχαίο τρόπο αποτρέπεται κάθε δυνατότητα ανεύρεσης του υδατογραφήματος με στατιστικές μεθόδους. Ένα υδατογράφημα που παράγεται χρησιμοποιώντας τυχαίο κλειδί και παίρνοντας υπόψιν τα τεχνικά χαρακτηριστικά του ψηφιακού προϊόντος είναι βέλτιστο και μπορεί να αποδώσει ένα ευρύ φάσμα προστασίας στο προϊόν έχοντας καλύψει την προϋπόθεση της μοναδικότητας και της αξιοπιστίας και τέλος είναι έτοιμο να ενσωματωθεί στο ψηφιακό προϊόν.

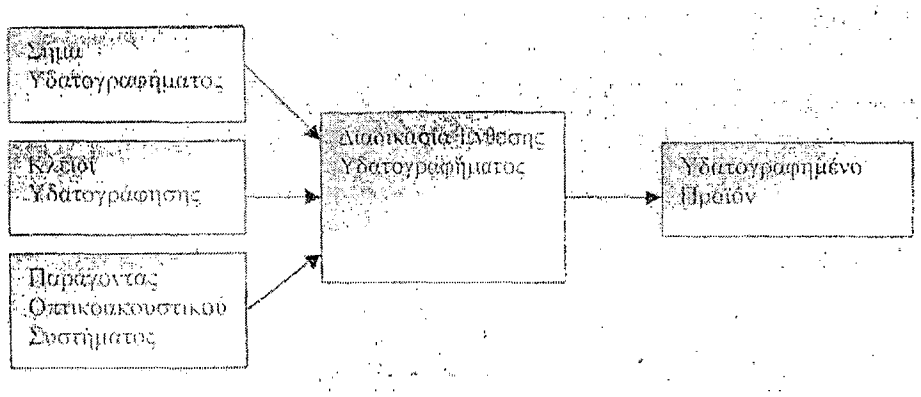


Εικόνα 10 **Κλειδί Υδατογράφησης**

2.4.4.2 Διαδικασία ένθεσης (Embedding)

Το υδατογράφημα που παράχθηκε με την παραπάνω διαδικασία προστίθεται στο ψηφιακό προϊόν. Το υδατογραφημένο προϊόν προκύπτει από την ένθεση του παραγόμενου υδατογραφήματος κι ενός συγκεκριμένου προϊόντος Χ. Η διαδικασία ένθεσης πρέπει να βασίζεται στα χαρακτηριστικά των ψηφιακών σημάτων ώστε το αποτέλεσμα της υδατογράφησης να περιέχει πληροφορία που δε διακρίνεται.

Η σπουδαιότητα της μη ορατότητας του υδατογραφήματος είναι καθοριστικής σημασίας στη διαδικασία της ένθεσης του υδατογραφήματος. Κατά την ένθεση λαμβάνονται υπόψιν οι ακουστικές ή οι οπτικές δυνατότητες του ανθρώπου. Η αποκρυπτογράφηση των ψηφιακών σημάτων δίνει τη δυνατότητα κρατώντας τις κατάλληλες ισορροπίες και συνυπολογίζοντας τα συμπεράσματα που προκύπτουν από τη μελέτη των ψηφιακών προϊόντων να μπορεί να προστίθεται πληροφορία που να μη γίνεται αντιληπτή.



Εικόνα 11 **Διαδικασία Ένθεσης Υδατογραφήματος**

Η διαδικασία προσθήκης πληροφορίας πρέπει να υλοποιείται με τέτοιο τρόπο ώστε να μη γίνεται αντιληπτή η ύπαρξη επιπλέον πληροφορίας και ταυτόχρονα να τοποθετεί την πληροφορία έτσι ώστε να μην μπορεί να αφαιρεθεί.

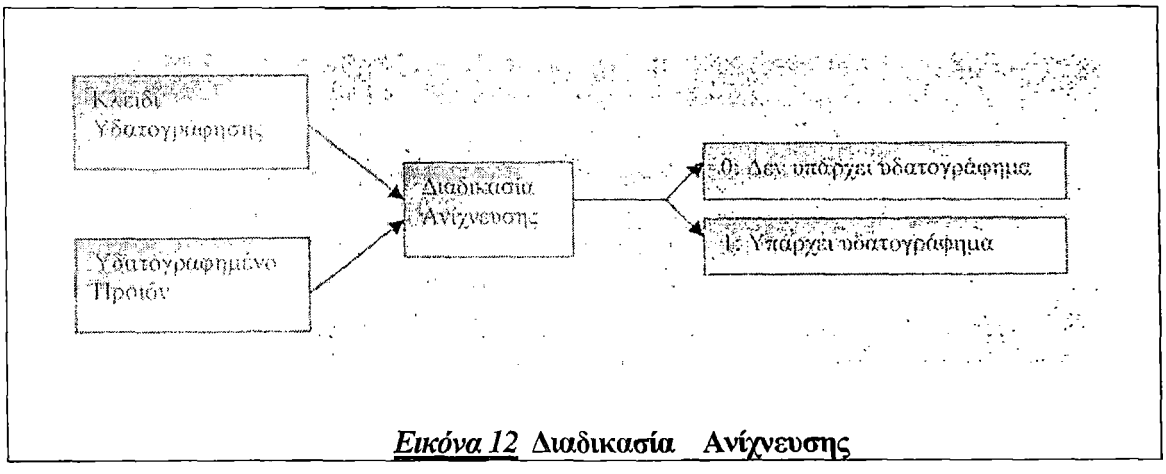
Γι' αυτό το λόγο θα πρέπει τα επιπλέον δεδομένα να προστίθενται σ' εκείνες τις περιοχές του ψηφιακού προϊόντος που να μην μπορούν να αφαιρεθούν ή η αφαίρεση τους να έχει σαν αποτέλεσμα και την απώλεια πολύτιμης πληροφορίας

2.4.4.3 Ανίχνευση υδατογραφήματος (Watermark Detection)

Η ανίχνευση του υδατογραφήματος δίνει τη δυνατότητα έχοντας ένα συγκεκριμένο προϊόν να μπορεί να αναγνωρισθεί αν το προϊόν έχει το ορθό υδατογράφημα ή όχι. Η κατάδειξη ή όχι της ύπαρξης υδατογραφήματος είναι απαραίτητη διότι η διαφύλαξη των πνευματικών δικαιωμάτων είναι εφικτή μόνο αν μπορεί να γίνει διαχωρισμός του νόμιμου προϊόντος από αυτό που αποκτήθηκε παράνομα. Συνεπώς η ανίχνευση του υδατογραφήματος απαιτείται ώστε η απόδειξη της κυριότητας του νόμιμου ιδιοκτήτη να πιστοποιείται και ταυτόχρονα να μπορεί να αποτραπεί οποιαδήποτε διεκδίκηση πνευματικών δικαιωμάτων πάνω στο συγκεκριμένο προϊόν από κάποιο άλλο.

Για να μπορέσει να γίνει ανίχνευση του υδατογραφήματος σε αρκετές περιπτώσεις δεν είναι απαραίτητο το αρχικό προϊόν αλλά μόνο το κλειδί υδατογράφησης και το προϊόν. Χρησιμοποιώντας το κλειδί το οποίο ανήκει μόνο στο νόμιμο κάτοχο μπορεί να γίνει έλεγχος ύπαρξης του υδατογραφήματος μόνο απ' αυτόν που θέλει να επιβεβαιώσει την πνευματική του ιδιοκτησία ή για να αποδείξει τη μη γνησιότητα του προϊόντος. Το γεγονός ότι δεν απαιτείται το αρχικό προϊόν σε πολλές τεχνικές συμβάλει αρκετά στην ταχύτατη ανίχνευση ενώ ταυτόχρονα η ανίχνευση γίνεται μόνο βάση του κλειδιού που βρίσκεται στα χέρια του ιδιοκτήτη. Κάθε απόπειρα για παράνομη διεκδίκηση πνευματικών δικαιωμάτων αποτρέπεται και κάθε παράνομο προϊόν μπορεί με εγκυρότητα να αποδειχθεί.

Η διαδικασία του ελέγχου της ύπαρξης ή όχι του υδατογραφήματος έχοντας ένα συγκεκριμένο προϊόν και το κλειδί πρέπει να μπορεί να αποφανθεί ότι το συγκεκριμένο προϊόν έχει ή όχι το υδατογράφημα και η βεβαιότητα απόκρισης πρέπει να είναι αρκετά μεγάλη ώστε η διαδικασία να είναι έγκυρη. Υπάρχει περίπτωση να παρατηρηθούν κάποιες αποκλίσεις στην απόκριση του ελέγχου ύπαρξης του υδατογραφήματος πράγμα που αποφέρει δυσάρεστες συνέπειες μιας και η ανίχνευση πρέπει να γίνεται με επαρκή βεβαιότητα. Με τη βοήθεια των μαθηματικών μπορεί να χρησιμοποιηθούν πιθανοτικές συναρτήσεις που να προβλέπουν την πιθανότητα λάθους της αποδοχής ή απόρριψης ενός προϊόντος. Έτσι μπορεί να υπάρξει μία εκτίμηση για την αξιοπιστία μίας διαδικασίας.



Εικόνα 12 **Διαδικασία Ανίχνευσης**

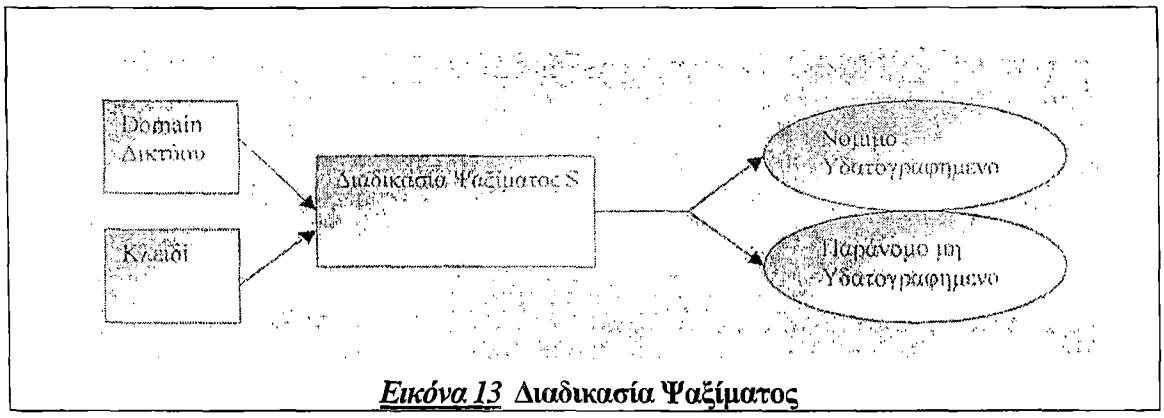
2.4.4.4 Ψάξιμο στο Διαδίκτυο (Web Searching)

Οι πειρατές μεταδίδουν συχνά τα μη αυθεντικά προϊόντα τοποθετώντας τα σε γνωστές πειρατικές ή μη, σελίδες του διαδικτύου. Εφόσον τα προϊόντα που διατείθονται στο δίκτυο βρίσκονται στις σελίδες του, επιτάσσεται διαδικασία ψαξίματος των συγκεκριμένων πεδίων (domain) για την εύρεση των παράνομων προϊόντων. Γι αυτό η μέθοδος του υδατογραφήματος πρέπει να συνδυάζεται με μια διαδικασία web-crawling. Η διαδικασία

αυτή αναζήτησης των δικτυακών τόπων παρέχει την ανίχνευση του υδατογραφήματος στα προϊόντα που εντοπίζεται σε αυτές τις δικτυακές σελίδες.

X=S (**Domain Name**)
XGX

Είναι προφανές πως ο εντοπισμός της ύπαρξης ή όχι του υδατογραφήματος πιστοποιεί την ύπαρξη νόμιμων ή παράνομων προϊόντων στο δικτυακό χώρο, όπου διακινούνται - υπάρχουν πολυάριθμα προϊόντα. Ο έλεγχος της εγκυρότητας ενός προϊόντος γίνεται με την αναγνώριση του υδατογραφήματος μέσα σε αυτό και αποτελεί ένα από τα βασικότερα χαρακτηριστικά του υδατογραφήματος.



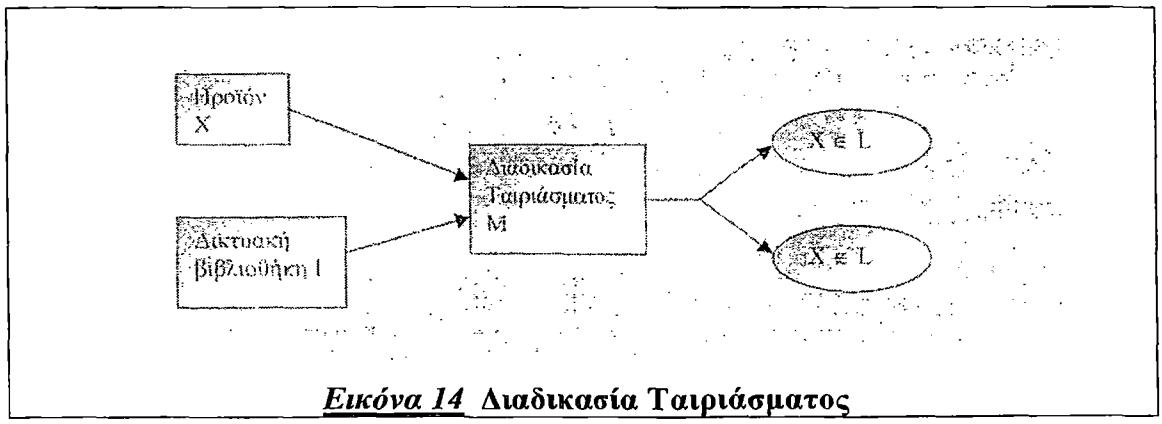
Εικόνα 13 **Διαδικασία Ψαξίματος**

2.4.4.5 Αναζήτηση / Αντιστοιχία προϊόντος σε βιβλιοθήκη (Product Search/Matching in Library)

Είναι φυσικό οι πραγματικοί δημιουργοί να αποθηκεύουν τα προϊόντα τους σε προσωπικές ηλεκτρονικές βιβλιοθήκες χωρίς μεγάλο κόστος. Αυτές οι βιβλιοθήκες από όπου μπορούν να διατεθούν τα προϊόντα τις συμβολίζουμε με Z. Θα ήταν χρήσιμο να μπορούμε να ελέγχουμε οποιοδήποτε προϊόν με τα αυθεντικά της L έτσι ώστε να προφυλαχτούν τα πνευματικά δικαιώματα του ιδιοκτήτη του αυθεντικού προϊόντος.

Δεδομένου προϊόντος X ο provider πρέπει να μπορεί να χρησιμοποιεί μια «διαδικασία ταιριάσματος» για να ελεγχθεί αν το τυχαίο προϊόν X περιλαμβάνεται Λ στην βιβλιοθήκη Z. Ας ορίσουμε αυτή τη διαδικασία M που έχει είσοδο το τυχαίο προϊόν X και την L και αποκρίνεται δηλ. επιστρέφει τιμή 1 όταν το X περιλαμβάνεται στη L και 0 διαφορετικά.

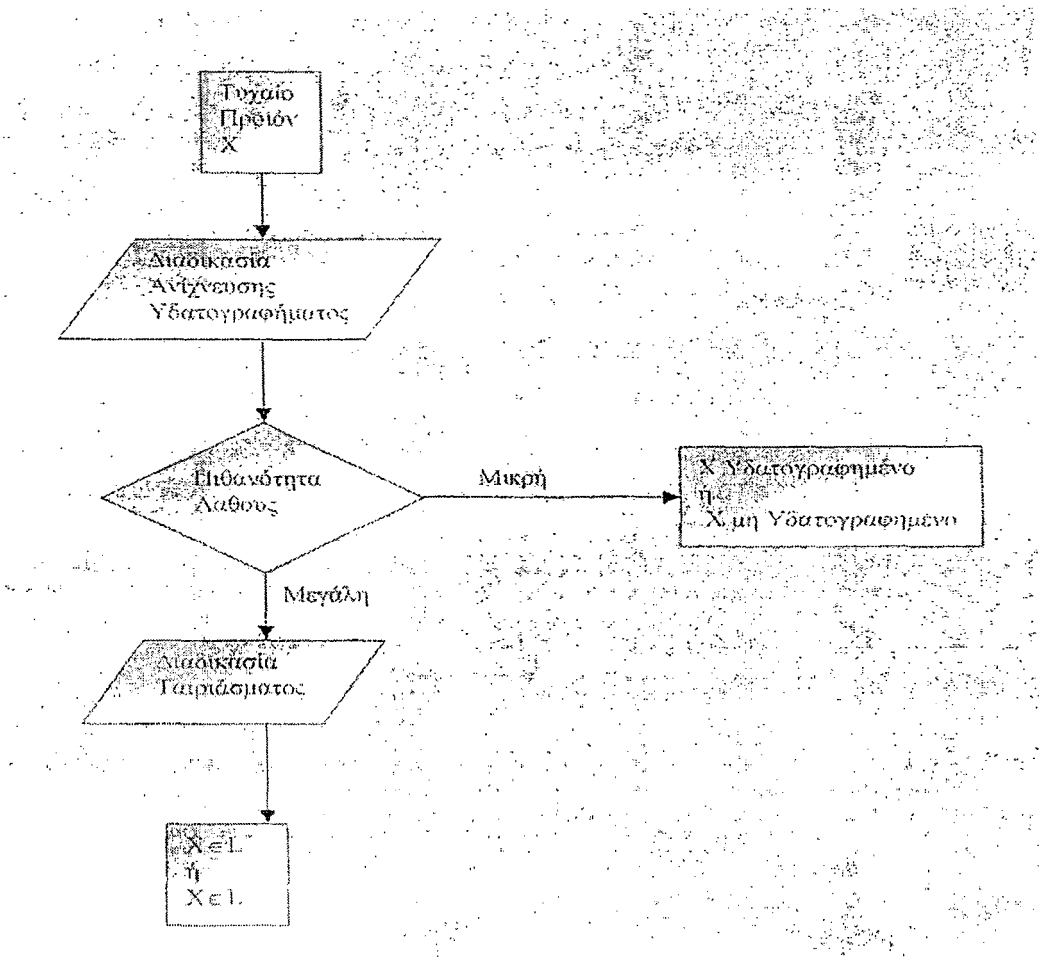
$$\iota(X, L) = \begin{cases} 1, \text{αν } \chi \in L \\ 0, \text{άλλο υ} \end{cases}$$



Εικόνα 14 **Διαδικασία Ταιριάσματος**

Η διαδικασία ταιριάσματος και στην μαθηματική θεωρία και στην πράξη της δεν είναι

απλή, μιας και βασίζεται σε αλγορίθμους με μεγάλη πολυπλοκότητα. Η μεγάλη πολυπλοκότητα της διαδικασίας κάνει μη πρακτική και εύχρηστη την εφαρμογή της σε μεγάλο πλήθος προϊόντων, π.χ. σε κάποιο internet domain που μας ενδιαφέρει. Για αυτό το λόγο αρχικά χρησιμοποιούμε την διαδικασία, ανίχνευσης και στην περίπτωση που δεν έχουμε πιστοποίηση με μεγάλη βεβαιότητα τότε χρησιμοποιούμε τη διαδικασία ταιριάσματος $\hat{WI}$ για καλύτερο και πιο αξιόπιστο αποτέλεσμα.



Εικόνα 15 **Διαδικασία Ελέγχου**

2.4.5 Βασικές Λειτουργίες του Υδατογραφήματος

Αρχικά το υδατογράφημα καθιερώθηκε ως απάντηση στην προστασία των πνευματικών δικαιωμάτων μιας και πριν την ανάπτυξη της μεθόδου της υδατογράφησης καμία από τις προηγούμενες μεθόδους δεν είχε εμπλακεί με το θέμα της πνευματικής ιδιοκτησίας. Το διάγραμμα προστασίας του υδατογραφήματος χρησιμοποιώντας ένα μεγάλο εύρος από τεχνικές δίνει απάντηση τόσο στην προστασία δεδομένων όσο και στη διαφύλαξη της αυθεντικότητας και των πνευματικών δικαιωμάτων.

2.4.5.1 Προστασία των πνευματικών δικαιωμάτων (Copyright Protection)

Το υδατογράφημα καθιερώθηκε με την ονομασία της copyright ταμπέλας πνευματικών δικαιωμάτων, από αυτό και μόνο καταδεικνύεται η σπουδαιότητα του για την προστασία των πνευματικών δικαιωμάτων. Το υδατογράφημα περικλείει συγκεκριμένη πληροφορία

για το νόμιμο ιδιοκτήτη ή ένα τυχαίο μοναδικό σήμα του συγκεκριμένου ιδιοκτήτη. Αυτό από μόνο του δεν καταδεικνύει σε όλο του το εύρος την ουσία της προφύλαξης των πνευματικών δικαιωμάτων, γι αυτό απαραίτητο είναι να δώσουμε τα βασικά σημεία του σχήματος προστασίας των πνευματικών δικαιωμάτων του υδατογραφήματος.

Κάθε ιδιοκτήτης πνευματικών δικαιωμάτων κατέχει ένα μοναδικό αριθμό μεγάλης ακρίβειας (ή ένα σετ αριθμών), που συνθέτει το ιδιωτικό κλειδί υδατογράφησης (private key) [47].Κατέχοντας το ιδιωτικό κλειδί και ένα ελεύθερο, δημόσιο ή ιδιωτικό αλγόριθμο, ο ιδιοκτήτης των πνευματικών δικαιωμάτων μεταβάλει το ψηφιακό προϊόν υδατογραφώντας το. Φυσικά οι αλγόριθμοι τροποποιούν με έξυπνο και πολύπλοκο τρόπο που καμία σχέση δεν έχει με μορφοποίηση των επικεφαλίδων και άλλη παραπλήσια πληροφορία.

	Παραγωγή ή Τροποποίηση Υδατογραφήματος	Ανίνευση Υδατογραφήματος
Απαιτήσεις	Ιδιωτικός ή δημόσιος αλγόριθμος παραγωγής W	Αλγόριθμος Ανίχνευσης
	Κλειδί Υδατογράφησης	Κλειδί Υδατογραφήματος

Εικόνα 16 **Σχήμα προστασίας υδατογραφήματος για τα πνευματικά δικαιώματα**

Ο ιδιοκτήτης πνευματικών δικαιωμάτων χρησιμοποιεί αλγόριθμο ανίχνευσης, ο οποίος μπορεί να ελέγξει ή να αποκρυπτογραφήσει τους συγκεκριμένους μετασχηματισμούς. Την δυνατότητα εκτέλεσης του αλγορίθμου την έχει ο νόμιμος ιδιοκτήτης ώστε να χρησιμοποιεί τα αποτελέσματα του για την αναγνώριση της νόμιμης ή μη κατοχής του προϊόντος. Το παραπάνω σχήμα επιτυγχάνει εφόσον κανένας πειρατής δεν θα μπορέσει να εναποθέσει όμοιο υδατογράφημα με του νόμιμου ιδιοκτήτη σε οποιοδήποτε προϊόν. Για το λόγο αυτό προτιμάται το private key να είναι τυχαίος αριθμός μεγάλης ακρίβειας.

Το υδατογράφημα μπορεί να δώσει απάντηση στην προστασία τόσο των πνευματικών δικαιωμάτων όσο και στην πιστοποίηση της αυθεντικότητας των δεδομένων, παρόλο που δεν έχουν ταυτόσημους στόχους. Υπάρχει διαφορά μεταξύ της έννοιας των πνευματικών δικαιωμάτων και της αυθεντικότητας των δεδομένων άρα και διαφορετικές επιλογές που πρέπει να κάνουμε αν θέλουμε να δώσουμε βάση στην προστασία του ενός ή του άλλου.

2.4.5.2 Αυθεντικοποίηση (Authentication)

Μιλώντας για αυθεντικότητα [76] εννοούμε έναν πολύπλοκο μηχανισμό που διασφαλίζει την γνησιότητα των δεδομένων. Για να πιστοποιήσει την αυθεντικότητα των περιεχομένων ενός προϊόντος το υδατογράφημα περιέχει πολύτιμες πληροφορίες, όπως το όνομα του δημιουργού την ημερομηνία παραγωγής, τον κάτοχο των πνευματικών δικαιωμάτων κ.α.

Για να πετύχει το υδατογράφημα στη διασφάλιση της ακεραιότητα των δεδομένων και στην ακεραιότητα των περιεχομένων του προϊόντος πρέπει να υλοποιεί κάποιες συγκεκριμένες προϋποθέσεις. Παρακάτω δίνουμε το βασικό σχήμα ενεργειών και

καταστάσεων που γίνονται για το σκοπό αυτό:

1. Ο αυθεντικός δημιουργός κατέχει ένα μοναδικό ιδιωτικό κλειδί Kpr (private key).
2. Το ιδιωτικό κλειδί και το προϊόν αποτελούν την είσοδο του αλγορίθμου. Ο αλγόριθμος μορφοποιεί τα δεδομένα συνδυάζοντας το κλειδί και την πληροφορία έτσι ώστε να ενσωματωθεί σε αυτό η πληροφορία αυθεντικότητας, η οποία είναι μοναδική. Ο αλγόριθμος είναι αυτός που καταδεικνύει και το δημόσιο κλειδί Kpub (public key).
3. Ο παραλήπτης θα πρέπει να μπορεί να ελέγξει την αυθεντικότητα, για το λόγο αυτό χρησιμοποιεί το δημόσιο κλειδί Kpub και ένα διαδεδομένο αλγόριθμο που παρέχει μια δυαδική απάντηση καταδεικνύοντας την αυθεντικότητα του προϊόντος. Έτσι διασφαλίζεται η ακεραιότητα των δεδομένων μιας και αυτό που είναι απαραίτητο στον κάθε χρήστη είναι το δημόσιο κλειδί (Kpub). Εδώ πρέπει να επισημάνουμε πως σε καμία περίπτωση δεν θα πρέπει να επιτρέπεται η αφαίρεση του υδατογραφήματος.

Η διαδικασία της πιστοποίησης των δεδομένων , βασίζεται στην ύπαρξη του υδατογραφήματος, και για αυτό είναι επιτακτικό το υδατογράφημα να είναι ανθεκτικό σε οποιαδήποτε χειρισμό αφαίρεσης. Η διαδικασία ένθεσης υδατογραφήματος έχει μεγάλη σημασία μιας και ο αλγόριθμος θα πρέπει να ενθέτει κατάλληλα το υδατογράφημα στο ψηφιακό προϊόν ώστε οποιαδήποτε προσπάθεια αφαίρεσης του από κακόβουλους χρήστες να έχει ως αποτέλεσμα την καταστροφή πληροφορίας και δεδομένων του προϊόντος. Άμεσο αποτέλεσμα αυτού είναι ένας πειρατής να έχει περιθώριο μόνο να αναπαράγει (αντιγράφει) το προϊόν μαζί με το υδατογράφημα το οποίο οδηγεί την πιστοποίηση της αυθεντικότητας του σε αποτυχία. Οι δραστηριότητες των πειρατών πάνω στα υδατογραφημένα προϊόντα είναι περιορισμένες και όσες επιτρέπονται πιστοποιούν αποδείξεις αυθεντικότητας που καμία σχέση δεν έχουν με τις πραγματικές.

Παρόλο λοιπόν που το υδατογράφημα απαντά ουσιαστικά και αδιαμφισβήτητα στο πρόβλημα της αυθεντικότητας (όπως αντίστοιχα έκαναν και οι μέθοδοι της υπογραφής) έγινε ευρέως γνωστό γιατί βοηθά στην οριοθέτηση των πνευματικών δικαιωμάτων.

	Διαδικασία παραγωγής του W ή μορφοποίησης	Διαδικασία πιστοποίησης υδατογραφήματος
Απαιτήσεις	Ιδιωτικός αλγόριθμος παραγωγής του W	Δημόσιος αλγόριθμος ανίχνευσης Υδατογραφήματος
	Ιδιωτικό κλειδί Kpr	Δημόσιο κλειδί Kpub

Εικόνα 17 **Διάγραμμα προστασίας για την αυθεντικότητα**

2.4.5.3 Διαφορές λειτουργιών Αυθεντικοποίηση και διασφάλισης πνευματικών δικαιωμάτων [90]

Στην αυθεντικοποίηση μας ενδιαφέρει κανείς να μην μπορεί να επέμβει στο προϊόν και το προϊόν να παραμένει αυθεντικό παρόλες τις προσπάθειες του πειρατή. Από την άλλη

μεριά στην προστασία των πνευματικών δικαιωμάτων μας ενδιαφέρει το υδατογράφημα να παραμένει στο προϊόν κάτω από οποιεσδήποτε συνθήκες ώστε να υπάρχει πάντα η σφραγίδα του δημιουργού.

Αυτή η διαφορετικότητα των δύο εννοιών σηματοδοτούν και αλληλοσυγκρουόμενες προϋποθέσεις που πρέπει να ικανοποιηθούν. Έτσι παραδείγματος χάριν όταν μας ενδιαφέρει, μέσω της προστασίας του υδατογραφήματος, να προστατεύσουμε καταρχάς τα πνευματικά δικαιώματα, θα πρέπει το υδατογράφημα να παραμένει στο προϊόν κάτω από οποιαδήποτε συνθήκη, ώστε ο αρχικός δημιουργός να είναι εμφανής πάντα. Από την άλλη όταν μας ενδιαφέρει για το υδατογραφημένο προϊόν να πιστοποιείται πάντα η αυθεντικότητα των δεδομένων του πρώτα και κύρια, θα πρέπει οποιαδήποτε παρέμβαση, οποιουδήποτε στο προϊόν, να καταδεικνύεται.

Πράγμα που σημαίνει ότι το υδατογράφημα θα πρέπει να είναι ευαίσθητο σε οποιαδήποτε επίθεση του πειρατή, ώστε να καταδεικνύεται η απόπειρα παρέμβασης. Άρα λοιπόν, η προστασία των πνευματικών δικαιωμάτων επιζητά ένα ανθεκτικό υδατογράφημα ,ενώ η προστασία της αυθεντικότητας ένα ευπαθές σε οποιαδήποτε μη επιτρεπτή παρέμβαση υδατογράφημα.

Είναι φανερό λοιπόν πως το υδατογράφημα απαντά και στις δύο μορφές προστασίας με διαφορετικό τρόπο. Αυτό είναι και η επιτυχία του υδατογραφήματος όπου προσέχοντας τα χαρακτηριστικά του και δίνοντας βάρος σε συγκεκριμένα σημεία, μπορεί να χρησιμοποιηθεί είτε για την προστασία της αυθεντικότητας των δεδομένων, είτε για την προστασία των πνευματικών δικαιωμάτων.

3

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΥΔΑΤΟΓΡΑΦΗΣΗΣ

3.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο είδαμε τις πολλαπλές απαντήσεις που μπορεί να δώσει το υδατογράφημα στην προστασία των δεδομένων. Πρέπει όμως να αναφερθούμε πιο συγκεκριμένα στις βασικές έννοιες του υδατογραφήματος. Οι απαντήσεις που δίνει το υδατογράφημα πρέπει να καλύπτουν τις απαιτήσεις της σημερινής εποχής.

Τα στάδια του μηχανισμού προστασίας του υδατογραφήματος είναι μεν αρκετά αλλά από μόνα τους δεν καλύπτουν το εύρος της προστασίας που πρέπει να παρέχεται. Μεγάλη σημασία έχουν τα χαρακτηριστικά και οι προϋποθέσεις που πρέπει να λαμβάνονται υπόψη από την διαδικασία υδατογράφησης. Τα χαρακτηριστικά αυτά σχετίζονται άμεσα με τις πραγματικές απειλές που δέχονται τα ψηφιακά δεδομένα στη σημερινή εποχή. Είναι αναγκαίο λοιπόν να κωδικοποιηθούν οι απαιτήσεις που προκύπτουν για να είναι εφικτό να αποδοθεί μία ικανοποιητική προσέγγιση τους.

Καταρχάς τα αντικείμενα με τα οποία ασχολείται η προστασία δεδομένων μέσω του υδατογραφήματος είναι τα ψηφιακά προϊόντα. Η ανάπτυξη της ψηφιακής τεχνολογίας δημιούργησε ένα ευρύ φάσμα εφαρμογών που μπορούν να υποστούν τα ψηφιακά προϊόντα. Επίσης η τεχνολογική ανάπτυξη των δικτύων και των Η/Υ έκανε όλους τους ανθρώπους να είναι δυνητικοί χρήστες του παγκόσμιου ιστού, μέσα από τον οποίο λαμβάνουν χώρα άπειρες συναλλαγές ψηφιακών προϊόντων σε πολύ μικρό χρονικό διάστημα. Μέσα σε αυτή την χαοτική καθημερινότητα έπρεπε να οριοθετηθούν οι ενέργειες και οι δυνατότητες του καθενός. Ήταν εύλογη η

ανάπτυξη του ηλεκτρονικού εμπορίου, μέσα όμως από συναλλαγές που ελάχιστη σχέση είχαν με την παλαιού τύπου αγοροπωλησία προϊόντων.

Η οριοθέτηση του ρόλου και των δυνατοτήτων του καθενός είναι απαραίτητη μιας και προσπαθούμε να δώσουμε χαρακτηριστικά προστασίας στα προϊόντα. Γνωρίζονται, τις ενέργειες που ενδέχεται να εφαρμοστούν, πρέπει να οριοθετήσουμε αυτές που δεν επιτρέπονται και αυτές που είναι θεμιτές ώστε το σχήμα προστασίας του υδατογραφήματος, εκτιμώντας κάποια χαρακτηριστικά, να αποτρέπει ή όχι τις ενέργειες αυτές.

3.2 Οριοθέτηση βασικών εννοιών του διαδικτύου σχετιζόμενων με τη διαδικασία υδατογράφησης

Η υδατογράφηση χρησιμοποιείται από πολλά προϊόντα τα οποία βρίσκονται στο διαδίκτυο (internet). Είναι εύλογο λοιπόν πολλά από τα βασικά χαρακτηριστικά του παγκοσμίου ιστού (www) να εμπλέκονται άμεσα με τη μορφή και τη δομή της διαδικασίας υδατογράφησης.

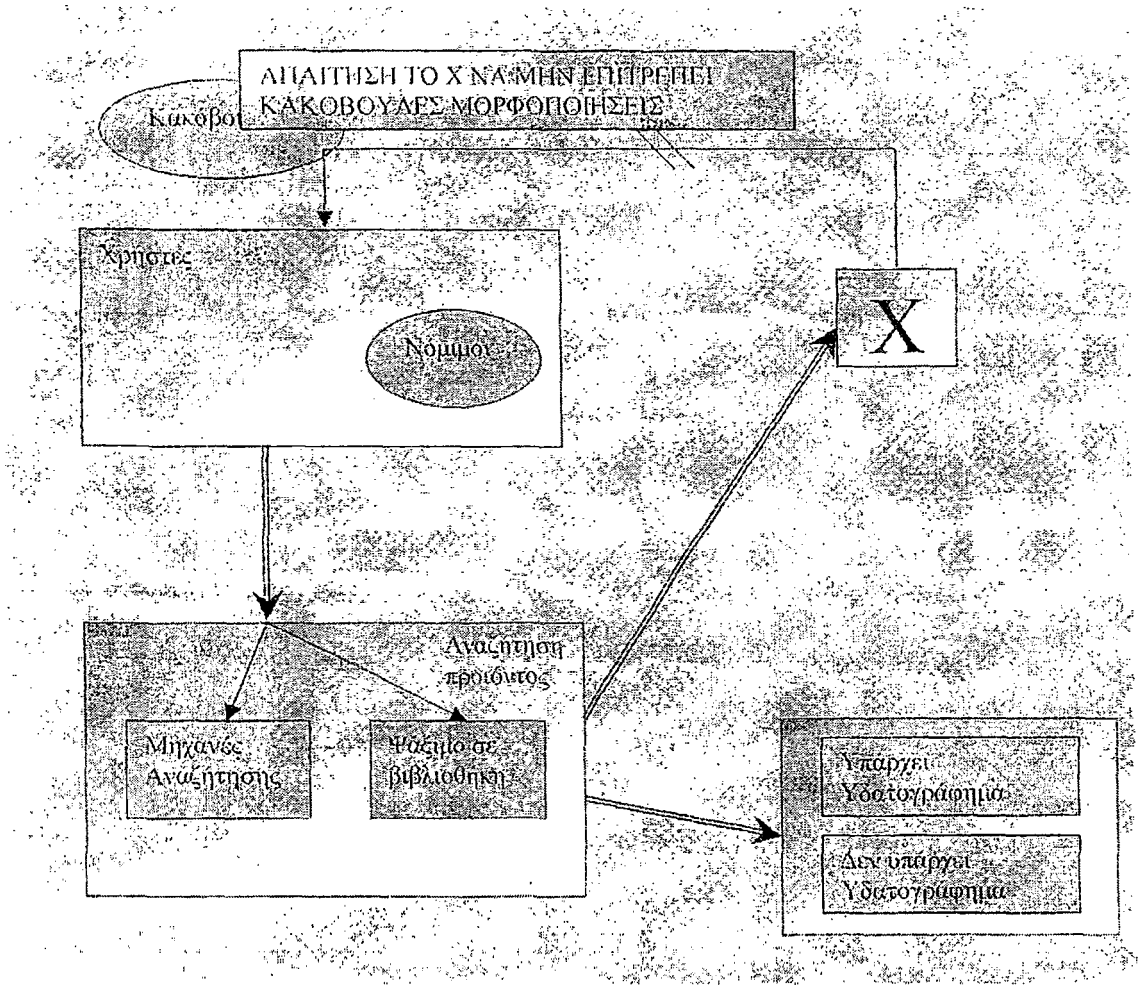
Για να μπορέσουν τα υδατογραφημένα προϊόντα να αντεπεξέρχονται στις δυνατότητες που προσφέρει το διαδίκτυο θα πρέπει να οριοθετηθούν εκείνες οι συνθήκες που σχετίζονται άμεσα με τις διαδικασίες υδατογράφησης.

- **Πειρατές**: Η έννοια του πειρατή έγινε γνωστή σε όλους μόλις ο παγκόσμιος ιστός αποτέλεσε μαζικό μέσο επικοινωνίας και μεταφοράς δεδομένων. Σαν πειρατές ορίζονται αυτοί που έχουν παράνομη πρόσβαση σε περιοχές του δικτύου ή παράνομη χρήση οποιουδήποτε ψηφιακού προϊόντος. Οι πειρατές δρουν μέσα στο δίκτυο, όπου υπάρχει πληθώρα πληροφοριών και ψηφιακών προϊόντων, και προσπαθούν να τα οικειοποιηθούν. Ο κάθε χρήστης δύναται να είναι πειρατής μιας και το δίκτυο δίνει τη δυνατότητα ανομίας σε μεγαλύτερο βαθμό από ότι οι προσωπικές συνδιαλλαγές και στον κάθε χρήστη επιτρέπεται ένα σύνολο ενεργειών. Οι πειρατές μπορούν να εφαρμόσουν οποιαδήποτε μετατροπή σε ένα ψηφιακό προϊόν που βρίσκεται σε μια ιστοσελίδα ή σε μια ηλεκτρονική βιβλιοθήκη. Η μετατροπή αυτή μπορεί είτε να αλλοιώσει το προϊόν είτε να το «σπάσει» και να το μετατρέψει σε αυθεντικό αντίγραφο. Το γεγονός αυτό παίρνει τεράστιες διαστάσεις μιας και η επαναμετάδοση του «μη αυθεντικού» προϊόντος είναι εφικτή, ανέξοδη και μη ελέγξιμη. Έτσι ακόμη και σήμερα το διαδίκτυο κατακλύζεται από «μη αυθεντικά» προϊόντα που μπορεί κάποιος να τα χρησιμοποιήσει είτε εις γνώσιν του είτε όχι.
- **Ιδιοκτήτες πνευματικών δικαιωμάτων**: Η έννοια της πνευματικής ιδιοκτησίας υιοθετήθηκε αρχικά από προϊόντα πνευματικής διεργασίας και πιστοποιούσε το δημιουργό και την ιδιοκτησία στην πρωτοτυπία μιας ιδέας. Πρωτοεμφανίστηκαν πνευματικά δικαιώματα στα βιβλία και στην μουσική. Σήμερα η τεχνολογική ανάπτυξη βασίζεται και αναπτύσσεται στα ψηφιακά προϊόντα που αποτελούν προϊόντα γνώσης. Τα μεγαλύτερα τεχνολογικά επιτεύγματα του $20^{ου}$ αιώνα σχετίζονται άμεσα με την ψηφιακή τεχνολογία μιας και το σύνολο των προϊόντων αιχμής είναι ψηφιακά. Είναι επόμενο λοιπόν οι ιδιοκτήτες ή οι δημιουργοί των προϊόντων να θέλουν να προασπίζουν την κυριότητα τους πάνω σε αυτά. Ο ιδιοκτήτης του ψηφιακού προϊόντος θέλει να

μην μπορεί οποιοσδήποτε με παράνομες ενέργειες να βλάψει το προϊόν και να μπορεί ο ίδιος οποιαδήποτε στιγμή να πιστοποιήσει την κυριότητα του πάνω στο προϊόν. Με αυτό τον τρόπο προφυλάσσονται τα πνευματικά δικαιώματα του προϊόντος από οποιονδήποτε θέλει παράνομα να τα διεκδικήσει και επιπλέον η γνησιότητα του αυθεντικού προϊόντος ανήκει αποκλειστικά σε όσους αυτός εξουσιοδοτεί.

- **Χρήστες**: Οι χρήστες θέλουν να μπορεί να πιστοποιηθεί η αυθεντικότητα του προϊόντος που έχουν στα χέρια τους. Ένα γνήσιο προϊόν πιστοποιεί και κάποιες συγκεκριμένες δυνατότητες και χαρακτηριστικά. Ο νόμιμος χρήστης θέλει να γνωρίζει τη γνησιότητα του προϊόντος που χρησιμοποιεί ώστε να είναι σίγουρος για τη αξιοπιστία του. Η γνησιότητα πρέπει να μπορεί να πιστοποιείται από τον ίδιο, εφόσον έχουν χρησιμοποιηθεί νόμιμες διαδικασίες για την απόκτηση του αυθεντικού προϊόντος. Πολλές φορές παρέχονται συγκεκριμένες δυνατότητες στους νόμιμους κατόχους του προϊόντος οι οποίες είναι σημαντικές. Αλλά και χωρίς αυτές, ο νόμιμος κάτοχος θέλει το προϊόν του να είναι ακέραιο και να μπορεί να πιστοποιηθεί η γνησιότητα του ώστε να γνωρίζει ότι δεν έχει εξαπατηθεί.
- **Αναζήτηση στον Παγκόσμιο Ιστό**: Σε ένα περιβάλλον όπως είναι ο παγκόσμιος ιστός όπου υπάρχουν εκατομμύρια ψηφιακά προϊόντα, πολλοί καταφεύγουν στις μηχανές ψαξίματος ώστε να μπορέσουν να εντοπίσουν το προϊόν για το οποίο ενδιαφέρονται. Σχεδόν κάθε χρήστης του διαδικτύου χρησιμοποιεί μηχανές αναζήτησης που ερευνούν τους δικτυακούς τόπους για την ύπαρξη του προϊόντος που επιθυμεί να αποκτήσει. Επομένως θα πρέπει μια πλήρης διαδικασία προστασίας δεδομένων να μπορεί να συνδυαστεί και με τις μηχανές αναζήτησης. Αν ένα προϊόν υπάρχει σε ένα συγκεκριμένο domain, θα πρέπει η διαδικασία του υδατογραφήματος - μηχανής αναζήτησης να πιστοποιεί ότι σε αυτό το domain όντως βρίσκεται το αυθεντικό προϊόν. Εφόσον τα ψηφιακά προϊόντα διατίθονται μέσω ιστοσελίδων θα πρέπει να πιστοποιείται αν υπάρχει ένα αυθεντικό προϊόν σε ένα domain.
- **Αναζήτηση σε βιβλιοθήκη**: Νόμιμοι κάτοχοι ψηφιακών προϊόντων, εκθέτουν τα προϊόντα τους σε ψηφιακές βιβλιοθήκες. Αυτές τις βιβλιοθήκες μπορεί να τις προσπελάσει ο καθένας και να αναζητήσει το αντικείμενο που τον ενδιαφέρει. Οι χρήστες που ερευνούν αυτές τις βιβλιοθήκες ενδιαφέρονται για τα νόμιμα προϊόντα. Είναι μείζονος σημασίας, αυτές οι βιβλιοθήκες να περιλαμβάνουν μόνο νόμιμα προϊόντα και να μην επιτρέπουν την ύπαρξη παράνομων αντιγράφων. Επιπλέον οποιοδήποτε άλλο αντίγραφο θα πρέπει να συγκρίνεται με το νόμιμο προϊόντα της βιβλιοθήκης ώστε να αποδεικνύεται η γνησιότητα του. Πολλές μεγάλες εταιρίες έχουν τεράστιες ηλεκτρονικές βιβλιοθήκες που είναι εύκολα προσβάσιμες και ο καθένας μπορεί να ελέγξει οποιοδήποτε προϊόν με το αντίστοιχο γνήσιο της βιβλιοθήκης. Αυτό θα περιορίσει σε μεγάλο βαθμό τη διακίνηση παράνομων αντιγράφων μέσω του παγκόσμιου ιστού. Το γεγονός τη οριοθέτησης των νόμιμων ή παράνομων ενεργειών τόσο των χρηστών όσο και των νόμιμων κατόχων, είναι αρκετά σημαντικό για την κατανόηση των προϋποθέσεων που

απαιτούνται ώστε να μπορεί το υδατογράφημα να παρέχει προστασία των πνευματικών δικαιωμάτων.



Εικόνα 18 **Παροχή προστασίας στο Δίκτυο**

Η κάλυψη αυτών των απαιτήσεων δημιουργεί ένα σύνολο μένουν σε ένα αφαιρετικό επίπεδο αλλά καθιστούν υποχρεωτική την ύπαρξη κάποιων χαρακτηριστικών στα υδατογραφημένα προϊόντα. Υπάρχουν λοιπόν κάποια χαρακτηριστικά γνωρίσματα που προϋποτίθενται ώστε η υδατογραφήσει να επιτυγχάνει την υπεράσπιση των πνευματικών δικαιωμάτων.

3.3 Χαρακτηριστικά Υδατογράφησης

Η διαδικασία της υδατογράφησης στηρίζεται στην ένθεση δεδομένων μέσα σε ένα ψηφιακό προϊόν ώστε να είναι εφικτή η πιστοποίηση της αυθεντικότητας ή η διασφάλιση των πνευματικών δικαιωμάτων του ιδιοκτήτη. Είναι εύλογο μιας και η διαδικασία εμπλέκει ψηφιοποιημένο σήμα σε ψηφιακά δεδομένα να είναι αρκετά πολύπλοκη .Καθώς πολυάριθμοι παράγοντες επηρεάζουν τόσο τη διαδικασία ένθεσης όσο και το τελικό αποτέλεσμα όσον αφορά την ποιότητα εικόνας ή ήχου του υδατογραφημένου προϊόντος.

Όταν έχουμε να χειριστούμε ψηφιακά δεδομένα πολλαπλές συνθήκες επεμβαίνουν σε αυτούς. Ας σκεφτούμε πως στην συγκεκριμένη περίπτωση η ποιότητα των δεδομένων που πρέπει να ενσωματωθούν, παίζει σημαντικό ρόλο τόσο στην διαδικασία ένθεσης,

όσο και στην ποιότητα του αποτελέσματος. Οι συνθήκες που επηρεάζουν την ποιότητα ενός σήματος είναι πράγματι πάρα πολλοί, γι' αυτό τον λόγο και κάθε διαδικασία επεξεργασίας σήματος θα πρέπει να λαμβάνει υπόψη της εκείνες τις συνθήκες που επηρεάζουν αυτή. Για να μπορέσουν οι συνθήκες που συμβάλλουν σημαντικά στην υδατογράφηση να ληφθούν υπόψη χρησιμοποιούνται οι βασικές έννοιες της μεθόδου υδατογράφησης.

Η μέθοδος του υδατογραφήματος απαιτεί κάποια βασικά χαρακτηριστικά στο υδατογραφημένο προϊόν, αυτά τα χαρακτηριστικά αποτελούν την βάση ώστε να ορισθούν οι βασικές έννοιες του μηχανισμού της υδατογράφησης. Οι βασικές αυτές έννοιες του υδατογραφήματος είναι μείζονος σημασίας μιας και αυτές δίνουν στο υδατογραφημένο προϊόν χαρακτηριστικά που πιστοποιούν την προστασία του από τους πειρατές.. Η αξιοπιστία που σχετίζεται με τη μέθοδο του υδατογραφήματος ώστε ένα υδατογραφημένο προϊόν να διέπεται από εκείνα τα χαρακτηριστικά που το κάνουν απόλυτα ασφαλές («άσπαστο») και ανθεκτικό, σχετίζεται άμεσα με τις βασικές έννοιες που πρέπει να υπακούει το υδατογραφημένο προϊόν. Σ' αυτό το σημείο θα ασχοληθούμε αναλυτικά με τις ***βασικές έννοιες της υδατογράφησης***:

Α. Πνευματική ιδιοκτησία (Copyright Protection) [16]

Μη αντιληπτή ένθεση (Perceptual Invisibility)

Ένα από τα κύρια χαρακτηριστικά της υδατογράφησης είναι ότι η ένθεση του υδατογραφήματος να μην γίνεται αντιληπτή από το χρήστη με την πτώση της ποιότητας του υδατογραφημένου προϊόντος. Το υδατογράφημα πρέπει να συμπεριφέρεται σαν μια αόρατη αυτή σφραγίδα ώστε κανένας παρατηρητής να μην μπορεί να αντιληφθεί την ύπαρξη της.

Γι' αυτό και η επεξεργασία του αρχικού σήματος πρέπει να είναι πολύ προσεκτική ώστε κατά τη διαδικασία ένθεσης του υδατογραφήματος να μην υπάρξει αλλοίωση του. Η ψηφιακή τεχνολογία μας δίνει τη δυνατότητα να κρύψουμε δεδομένα μέσα σε άλλα δεδομένα με τρόπο που να μην γίνονται αντιληπτά. Σ' αυτό το στάδιο πρέπει να λαμβάνουμε υπόψη μας και τις οπτικές -ακουστικές δυνατότητες της ανθρώπινης όρασης και ακοής. Ένας κοινός παραλήπτης δεν πρέπει να αντιλαμβάνεται ότι κάτι κρύβεται στο προϊόν του. Βέβαια το υδατογραφημένο προϊόν θα είναι σίγουρα διαφορετικό από το αρχικό αυθεντικό προϊόν, αλλά με τρόπο μη αντιληπτό στις αισθήσεις του χρήστη του. Μπορεί να υπάρχουν κάποιες διαφορές που φαίνονται πολύ δύσκολα συγκρίνοντας το αρχικό με το υδατογραφημένο προϊόν, αυτό όμως δεν μας ενδιαφέρει μιας και το αρχικό προϊόν το κατέχει μόνο ο ιδιοκτήτης.

Οποιαδήποτε λοιπόν διαμόρφωση του αρχικού προϊόντος κατά τη διαδικασία του υδατογραφήματος θα πρέπει να μην αλλοιώνει την ποιότητα του προϊόντος ώστε μια τέτοια αλλοίωση γίνεται αντιληπτή από τον τελικό χρήστη μέσα στο ψηφιακό προϊόν. Θα πρέπει επίσης να υπάρχει προσεκτικός έλεγχος για το αν το υδατογράφημα είναι καλά «κρυμμένα».

Στατιστικώς διαφανής ένθεση (Statistical Invisibility)

Το υδατογράφημα πρέπει να είναι μοναδικό και διακριτό για κάθε προϊόν που χρησιμοποιείται. Επίσης το υδατογράφημα πρέπει να αποτελεί μια αόρατη σφραγίδα για τον παρατηρητή. Αυτές οι ιδιότητες του υδατογραφήματος θα πρέπει να ισχύουν όχι μόνο όταν ο χρήστης έχει στη διάθεση του ένα, αλλά και περισσότερα προϊόντα ακόμα και από τον ίδιο ιδιοκτήτη. Με άλλα λόγια το υδατογράφημα δεν θα πρέπει σε καμία περίπτωση να ανακαλύπτεται με στατιστικές μεθόδους.

από τον ιδιοκτήτη να είναι εφικτή. Επιπλέον το κλειδί, εκτός από το ρόλο ενός μεμονωμένου αριθμού που κατοχυρώνει την κυριότητα του ιδιοκτήτη και του επιτρέπει τις παραπάνω διαδικασίες, παίζει πολύ σημαντικό ρόλο στη διαδικασία της ένθεσης.

Επιπλέον, το κλειδί δεν παίζει μόνο σημαντικό ρόλο στην προστασία της κυριότητας του ιδιοκτήτη αλλά και στην παραγωγή του υδατογραφήματος με βάση το προϊόν. Το κλειδί παίζει σημαντικό ρόλο στην ποιότητα του παραγόμενου υδατογραφημένου προϊόντος διότι για την παραγωγή του υδατογραφήματος απαιτείται μόνο το κλειδί και ο αλγόριθμος παραγωγής. Ο συσχετισμός του κλειδιού με τον αλγόριθμο, δημιουργούν το υδατογράφημα, και ο τρόπος με τον οποίο συνδυάζονται πρέπει να είναι τέτοιος ώστε να μην αλλοιώνεται η ποιότητα του προϊόντος. Για ένα υδατογραφημένο προϊόν όπου η απόκρυψη του υδατογραφήματος δεν θα είναι αντιληπτή από το χρήστη, απαιτείται καλός συνδυασμός μεταξύ του κλειδιού και του αλγορίθμου παραγωγής. Γι αυτό και είναι αναγκαίο η επιλογή του κλειδιού να επηρεάζει τη δόμηση του αλγορίθμου και το αντίστροφο.

Ο ρόλος του κλειδιού είναι μεγάλης και πολλαπλής σημασίας και πρέπει να διέπεται τόσο από το χαρακτηριστικό της μοναδικότητας, όσο και από την τυχαιότητα της παραγωγής του κλειδιού υδατογράφησης.

Τυχαιότητα στην παραγωγή του κλειδιού υδατογράφησης (Randomness in Production)

Το γεγονός ότι το κλειδί πρέπει να παράγεται με τυχαίο τρόπο είναι καθοριστικής σημασίας. Η μέθοδος του υδατογραφήματος όσο πρωτοπόρα κι αν είναι, είναι και αυτή μια μέθοδος προστασίας δεδομένων. Η εμπειρία και τα συμπεράσματα που υπάρχουν από τις προηγούμενες μεθόδους, ισχύουν και σε αυτή, ειδικά οι επιτυχίες και επαληθευμένες διαπιστώσεις. Η τυχαιότητα είναι ένα χαρακτηριστικό αναντικατάστατο, που πρέπει να διέπει το κλειδί ώστε να μην μπορεί να ανακαλυφθεί, χωρίς το οποίο δε μπορούμε να μιλήσουμε σοβαρά για ασφάλεια.

Η τυχαία παραγωγή ενός αριθμού ή συμβολοσειράς ή ακολουθίας διαδίκων ψηφίων, είναι η μόνη μορφή παραγωγής κλειδιού που κάνει αδύνατο να ευρεθεί με οποιαδήποτε μορφής μαθηματικούς συνδυασμούς. Η εξελίξει των μαθηματικών και οι εφαρμογές τους σε ότι αφορά τις γεννήτριες τυχαίων αριθμών όπως οι ψευδοτυχαίες ακολουθίες (PN-ακολουθίες), παίζουν σημαντικό ρόλο στην εξέλιξη των μεθόδων προστασίας δεδομένων διότι τους δίνουν πολλαπλές δυνατότητες. Παρόλο που παρουσιάζουν μεγάλη πολυπλοκότητα, είναι αναγκαία η χρήση τους για την επίτευξη μεγαλύτερης ασφάλειας.

Στην παρούσα διπλωματική γίνεται χρήση της τυχαιότητας του κλειδιού υδατογράφησης στους αλγορίθμους που έχουν υλοποιηθεί και παρουσιάζονται στο παρακάτω κεφάλαιο. Για την τυχαία παραγωγή ενός κλειδιού υδατογράφησης χρησιμοποιήθηκαν δύο τρόποι:

- Μέσω του αλγορίθμου που κωδικοποιεί τυχαία bit, διαλέγοντας με τυχαίο τρόπο πια από τα bit θα θέσει 1 ή 0.
- Μέσω γεννήτριας συνάρτησης παραγωγής τυχαίων τιμών.

Και οι δύο τρόποι χρησιμοποιούνται ανάλογα με τις ανάγκες που υπάρχουν για την φύση του κλειδιού σε κάθε αλγόριθμο. Η τυχαιότητα στην παραγωγή του υδατογραφήματος επιλέχθηκε σαν ένα χαρακτηριστικό διότι αποτρέπει την παραγωγή όμοιου υδατογραφήματος των μεθόδων που υλοποιήσαμε. Το υδατογράφημα που παράγεται από τη συνάρτηση παραγωγής G σε συνδυασμό με το τυχαίο κλειδί είναι

μοναδικό, συνεπώς και το υδατογραφημένο προϊόν είναι μοναδικό για κάθε κλειδί.

Αξιόπιστη ανίχνευση (Trustworthy Detection)

Ένα από τα κύρια χαρακτηριστικά της υδατογράφησης είναι και η δυνατότητα της ανίχνευσης ή όχι του υδατογραφήματος στο υδατογραφημένο προϊόν. Ένα συγκεκριμένο προϊόν θα πρέπει να μπορεί να ελεγχθεί αν σε αυτό υπάρχει το ορθό υδατογράφημα ή όχι, ώστε να μπορούν να αποδοθούν τα πνευματικά δικαιώματα. Η πιστοποίηση των πνευματικών δικαιωμάτων δεν ολοκληρώνεται με την επιτυχή προσθήκη υδατογραφήματος σε ένα προϊόν, αλλά απαιτείται το υδατογράφημα να συνιστά και μια επαρκής και αξιόπιστη απάντηση σε ότι αφορά την διαδικασία ανίχνευσης του υδατογραφήματος. Η ανίχνευση επιτυγχάνεται χωρίς να είναι αναγκαίο το αρχικό προϊόν αλλά μόνη της η συνάρτηση ανίχνευσης η οποία παίρνει σαν είσοδο το κλειδί και το υδατογραφημένο προϊόν και δίνει σαν αποτέλεσμα μια καταφατική ή αρνητική απάντηση όσον αφορά την ύπαρξη του υδατογραφήματος. Ακριβώς λόγω της κρισιμότητας της διαδικασίας ανίχνευσης, υπάρχουν συναρτήσεις πιθανότητες λάθους που δίνουν για μια συγκεκριμένη συνάρτηση ανίχνευσης G την συνάρτηση πιθανότητας που υπάρχει η απόκριση της G να είναι λάθος ή όχι.

Αυτές οι συναρτήσεις πιθανότητας λάθους θα πρέπει να υπολογίζονται και τα αποτελέσματα τους να λαμβάνονται υπόψη. Υπάρχει η δυνατότητα κατά τη διαδικασία ανίχνευσης του υδατογραφήματος, με τη βοήθεια των συναρτήσεων πιθανότητας λάθους και των συναρτήσεων των λάθος συναγερμών (false alarm) να έχουμε μια εκτίμηση της αξιοπιστίας της διαδικασίας ανίχνευσης. Η εκτίμηση αυτή πρέπει να λαμβάνεται σοβαρά υπόψη και στην περίπτωση που αν οι συναρτήσεις πιθανότητας λάθους και λάθους συναγερμού είναι μεγάλη, να απορρίπτεται. Το υδατογράφημα αποτελεί μια έγκυρη απόδειξη πνευματικής ιδιοκτησίας, όταν η ανίχνευση του υδατογραφήματος σε ένα ψηφιακό προϊόν ακολουθείται από μηδαμινή πιθανότητα λάθους. Πάντα πρέπει να γίνεται ένας έλεγχος και να διατηρείται μια ισορροπία μεταξύ της τιμής της συνάρτησης πιθανότητας λάθους και της πιθανότητας λάθους συναγερμού ώστε και το προϊόν να είναι αξιόπιστο και η συνάρτηση ανίχνευσης να είναι εύχρηστη.

Διαχωρισμός των χαρακτηριστικών ανάλογα με τον βασικό στόχο της μεθόδου υδατογράφησης

Τα παραπάνω χαρακτηριστικά συμβάλουν στην προστασία των δεδομένων με καθολικό τρόπο. Το υδατογράφημα δίνοντας απόλυτη απάντηση στην προστασία των πνευματικών δικαιωμάτων εμπεριέχει στα χαρακτηριστικά του και κάποια που σχετίζονται μόνο με τα πνευματικά δικαιώματα. Το υδατογράφημα παρ' όλου που έγινε ευρέως γνωστό για την σχέση του με την προστασία της πνευματικής ιδιοκτησίας, δίνει απάντηση και στην αυθεντικότητα. Εδώ βρίσκεται ένα κρίσιμο σημείο. Οι ερευνητές που σχεδιάζουν μία μορφή προστασίας για ένα προϊόν πρέπει να συγκεκριμενοποιήσουν τις απαιτήσεις που πρέπει να καλύψουν σε μεγαλύτερο ή σε μικρότερο βαθμό. Η οριοθέτηση των απαιτήσεων που πρέπει να καλυφθούν είναι πρωταρχικής σημασίας, ώστε στην ανάπτυξη της μεθόδου να δοθεί βάρος στα ανάλογα σημεία.

Τα παρακάτω δύο χαρακτηριστικά είναι απαραίτητα εφόσον έχει επιλεγεί ο βασικός στόχος της μεθόδου της υδατογράφησης να είναι η προστασία των πνευματικών δικαιωμάτων. Τα παρακάτω χαρακτηριστικά υιοθετήθηκαν από το σχήμα υλοποίησης που δημιουργήσαμε και υπακούουν σ' αυτό τόσο οι αλγόριθμοι όσο και τα αποτελέσματα της υδατογράφησης.

Ανθεκτικότητα (Robustness)

Εφόσον το υδατογράφημα χρησιμοποιείται για την πιστοποίηση των πνευματικών δικαιωμάτων του υδατογραφημένου προϊόντος, θα πρέπει να μην είναι ευάλωτο σε διάφορες επιθέσεις που μπορεί να δεχθεί από κακόβουλους χρήστες και να παραμένει στο προϊόν που έχει εντεθεί. Στο σημείο αυτό υπάρχει ένας έντονος προβληματισμός σχετικά με το μεγάλο και ποικίλο αριθμό των επιθέσεων που μπορεί να δεχθεί ένα υδατογραφημένο ψηφιακό προϊόν τόσο από πειρατές όσο και από νόμιμους χρήστες.

Ένας χρήστης που έχει ακολουθήσει τη νόμιμη διαδικασία απόκτησης ενός προϊόντος, απαιτεί από αυτό να είναι εύχρηστο, δηλαδή να του δίνεται η δυνατότητα να το επεξεργαστεί όταν αυτό είναι απαραίτητο (π.χ συμπίεση, αποσυμπίεση, φιλτράρισμα για αφαίρεση θορύβου, αλλαγή συντεταγμένων κ.α). Από την άλλη οι πειρατές χρησιμοποιούν αρκετές μεθόδους επεξεργασίας προκειμένου να σπάσουν την προστασία του προϊόντος πολλές από τις οποίες είναι ίδιες με αυτές των απλών χρηστών. Μιας και η μέθοδος της υδατογράφησης διαφυλάσσει τα πνευματικά δικαιώματα, η αόρατη σφραγίδα του ιδιοκτήτη είναι αναγκαίο να υπάρχει για να πιστοποιεί την κυριότητα του προϊόντος.

Η πληθώρα των επιθέσεων που μπορεί να υποστεί ένα ψηφιακό προϊόν, σε καμία περίπτωση δεν πρέπει να έχει ως αποτέλεσμα την αφαίρεση της κρυμμένης πληροφορίας. Το υδατογράφημα εφόσον εξυπηρετεί την προστασία των πνευματικών δικαιωμάτων πρέπει να είναι ανθεκτικό σε διάφορες μορφές επεξεργασίας δεδομένων, που δεν αλλοιώνουν την ποιότητα του υδατογραφημένου προϊόντος. Αν η επεξεργασία αλλοιώσει την ποιότητα της του ψηφιακού προϊόντος τότε σίγουρα και το υδατογράφημα ενδέχεται να αλλοιωθεί .Αυτό όμως δεν θα έχει ουσιαστική επίπτωση γιατί το προϊόν θα έχει καταστραφεί ουσιαστικά.

Η ανθεκτικότητα του υδατογραφήματος είναι ένα ουσιώδες χαρακτηριστικό για την προστασία πνευματικών δικαιωμάτων και δίνει την δυνατότητα η ιδιοκτησία των πνευματικών δικαιωμάτων ενός προϊόντος να πιστοποιείται από διάφορες επιθέσεις που μπορεί να δεχθεί. Οι πειρατές λοιπόν θα έχουν να επιλέξουν ανάμεσα σε δύο περιπτώσεις. Είτε μπορούν να έχουν ένα προϊόν υδατογραφημένο όπου η πιστοποίηση των πνευματικών δικαιωμάτων του να είναι εύκολη είτε μπορούν να έχουν ένα προϊόν απαλλαγμένο από το υδατογράφημα αλλά άχρηστο.

Υπάρχουν πολλές τεχνικές επεξεργασίες ψηφιακών δεδομένων για την επεξεργασία του ψηφιακού προϊόντος ώστε να είναι εύχρηστο οι οποίες δεν αλλοιώνουν τα δεδομένα, το υδατογράφημα πρέπει να μένει ανεπηρέαστο από αυτές. *Τέτοιες τεχνικές είναι*:

1. Φιλτράρισμα [78] για εξαγωγή θορύβου, με σκοπό τη βελτίωση της ποιότητας του προϊόντος. Είναι πιθανόν κάποιος να χρησιμοποιήσει φίλτρο για την αφαίρεση του υδατογραφήματος καθώς αυτό μπορεί να έχει εντεθεί σαν θόρυβος με την γενικότερη έννοια. Για την αντιμετώπιση αυτής της περίπτωσης το υδατογράφημα πρέπει να προστεθεί με τέτοιο τρόπο ώστε ένα απλό φιλτράρισμα σε συγκεκριμένη περιοχή να μην μπορεί να το αφαιρέσει. Η προσθήκη του υδατογραφήματος W θα πρέπει να γίνεται σε συχνοτική περιοχή που υπάρχει πολύτιμη πληροφορία του αρχικού προϊόντος, έτσι ώστε οποιασδήποτε μορφής φιλτράρισμα σε αυτό το συχνοτικό εύρος να προκαλέσει απώλεια πολύτιμης πληροφορίας, άρα και αχρήστευση του προϊόντος. Η επεξεργασία του σήματος δημιουργεί επιπλέον κινδύνους που πρέπει να προσεχθούν ώστε να διατηρηθεί το υδατογράφημα σε κάθε περίπτωση.

2. Συμπίεση με απώλεια δεδομένων[58] (lossy compression) που εφαρμόζεται σχεδόν σε όλα τα πολυμεσικά προϊόντα κατά κύριο λόγο για εξοικονόμηση χωρητικότητας, αλλά σε κάποιες περιπτώσεις απαιτείται και από κάποιες εφαρμογές πολυμέσων. Η συμπίεση πρέπει να γίνεται με τέτοιο τρόπο ώστε η απώλεια πληροφορίας να μη προκαλεί σημαντική αλλοίωση της ποιότητας του προϊόντος. Η συμπίεση μπορεί να προκαλέσει την αφαίρεση του υδατογραφήματος αν η διαδικασία ένθεσης δεν είναι η βέλτιστη. Μια βέλτιστη διαδικασία ένθεσης υδατογραφήματος εναποθέτει την κρυμμένη πληροφορία εκεί που υπάρχει σημαντική ποσότητα πληροφορίας η οποία αν αφαιρεθεί αλλοιώνεται το προϊόν.

3. Γεωμετρικές παραμορφώσεις που συσχετίζονται στην ελεύθερη βούληση του χρήστη για επεξεργασία του ψηφιακού προϊόντος. Τα ψηφιακά προϊόντα και ειδικότερα η εικόνα και το βίντεο μέσω διαφόρων μορφών επεξεργασίας[56] μπορούν να βελτιώσουν την ποιότητα τους και να δώσουν τη δυνατότητα να δημιουργηθούν πολυμεσικά προϊόντα που το αποτέλεσμα τους είναι εικαστικά επιτυχημένο και τόσο θεαματικό που παλαιότερα φαινόταν σχεδόν αδύνατο. Είναι φυσικό και επόμενο, δεδομένου ότι αναπτύχθηκε ολόκληρη τεχνολογία πάνω στα εικαστικά και θεαματικά αποτελέσματα της ψηφιοποίησης της εικόνας και του ήχου, αυτές οι διεργασίες μορφοποιήσεις να επιτρέπονται σε ένα υδατογραφημένο βίντεο ή εικόνα. Τέτοιες μορφές επεξεργασίας είναι:

   I. Βάθμωση, τροποποίηση δηλαδή του μεγέθους του προϊόντος τηρούμενων των αναλογιών του,

   II. Περιστροφή, δηλαδή αλλαγή της μορφής του προϊόντος περιστρέφοντας το γύρω από κάποιο άξονα,

   III. Αντανάκλαση εικόνας ή καρέ,

   IV. Cropping,

   V. Εισαγωγή ή εξαγωγή σειράς, στήλης ή καρέ.

4. Μετατροπή ενός ψηφιακού προϊόντος από τη μία μορφή αναπαράστασης (format)oTr|V άλλη. Η πληθώρα ψηφιακών προϊόντων οδήγησε και στη δημιουργία ενός μεγάλου αριθμού διαφορετικών αναπαραστάσεων τους. Η αλλαγή της μορφής αναπαράστασης ενός ψηφιακού προϊόντος συμβάλει στην ύπαρξη πολλών ψηφιακών προϊόντων με διαφορετικά χαρακτηριστικά και τα κάνει πιο εύχρηστα μιας και το πλήθος των εφαρμογών στις οποίες χρησιμοποιούνται είναι μεγαλύτερο. Ένα υδατογραφημένο προϊόν που επιτρέπει την αλλαγή της μορφής αναπαράστασης είναι πολύ χρήσιμο αλλά παρόλα αυτά απαιτεί επιπλέον πολυπλοκότητα. Η χρησιμότητα ενός προϊόντος καταδεικνύει πολλές φορές και την σπουδαιότητα του υδατογραφήματος. Ακόμη και αν η παραγωγή γίνεται με ποιο δύσκολο τρόπο θα πρέπει να μπορεί να συνδυασθεί με διεργασίες εκτύπωσης ή επανασάρωσης. Μπορεί μεγάλο ποσοστό της επεξεργασίας σήματος να σχετίζεται με ψηφιακά σήματα όμως και το αναλογικό σήμα έχει την χρησιμότητα του. Τα διαφορετικά χαρακτηριστικά και οι δυνατότητες του ψηφιακού και του αναλογικού σήματος κάνουν το ένα να υπερέχει ή να υστερεί από το άλλο σε διαφορετικούς τομείς ανάλογα με τις ανάγκες. Έτσι η χρήση και των δύο είναι εύλογη, διότι σε πολλές εφαρμογές ανάλογα με την περίπτωση άλλοτε χρησιμοποιούμε σαν είσοδο αναλογικό κι άλλοτε ψηφιακό σήμα. Η μετατροπή του σήματος από ψηφιακό σε αναλογικό είναι και σύνηθες και απαραίτητο ώστε να οικειοποιηθούμε τα θετικά χαρακτηριστικά του καθενός. Είναι φυσικό λοιπόν το υδατογραφημένο σήμα να επιτρέπει αυτήν την μετατροπή αν σκεφτεί κανείς πως οι τηλεφωνικές γραμμές

στην Ελλάδα την καθιστούν απαραίτητη.

5. Τέλος ένα ψηφιακό προϊόν όπως οι σταθερές εικόνες [56]είναι ένα προϊόν που επιτρέπει πληθώρα από επεξεργασίες που είναι πολύ συνηθισμένες όπως διόρθωση χρώματος, αύξηση της αντίθεσης των χρωμάτων, κανονικοποίηση ιστογράμματος (histogram equalization etc.) Το υδατογράφημα πρέπει να είναι ανθεκτικό σε αυτές τις μορφές επεξεργασίας Είναι σημαντικό λοιπόν η προσθήκη του υδατογραφήματος αν σχετίζεται με τα «ορατά» χαρακτηριστικά μιας εικόνας να λαμβάνει υπόψη αυτούς τους μετασχηματισμούς και να παραμένει το υδατογράφημα αόρατο.

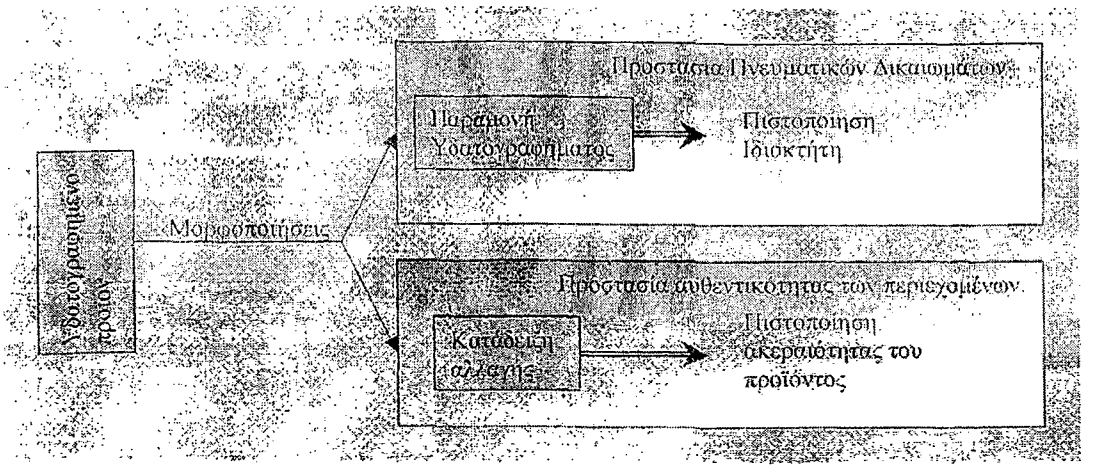
Ένθεση πολλαπλών υδατογραφημάτων (Multiple watermark embedding) [171]

Είναι εύλογο πώς όσοι θα ήθελαν να παρέχουν μια επιπλέον προστασία σ' ένα προϊόν ή θα τους ενδιέφερε η πιστοποίηση των πνευματικών τους δικαιωμάτων να βλέπουν με αρκετό ενδιαφέρον το υδατογράφημα. Η μέθοδος του υδατογραφήματος είναι μία μέθοδος προστασίας αρκετά πρόσφατη οπότε αρκετοί είναι εκείνοι που θα ήθελαν να την παρατηρήσουν και πολλοί περισσότεροι αυτοί που θα ήθελαν να την εφαρμόσουν. Πάνω λοιπόν στο υδατογράφημα υπάρχουν ερευνητές που επεξεργάζονται την υδατογράφηση σαν μέθοδο προστασίας όπως και άλλοι που ήδη την εφαρμόζουν. Είναι εύλογο λοιπόν ένα οποιοδήποτε ψηφιακό προϊόν να μπορεί να υδατογραφηθεί ακόμη και αν είναι ήδη υδατογραφημένο. Η απαγόρευση της υδατογράφησης ενός ήδη υδατογραφημένου προϊόντος δε θα είχε κανένα νόημα μιας και ο καθένας νόμιμος παραλήπτης θα μπορούσε να επικυρώσει την κατοχή ενός προϊόντος μ' ένα υδατογράφημα.

Η διαδικασία της υδατογράφηση θα πρέπει να επιτρέπει την πολλαπλή υδατογράφηση ενός προϊόντος χωρίς να υπάρχει πρόβλημα του υδατογραφήματος. Μίας και ο νόμιμος κάτοχος των πνευματικών του δικαιωμάτων είναι ο μόνος που κατέχει το προϊόν που περιέχει ένα μόνο υδατογράφημα.

Η παράνομη διεκδίκηση πνευματικών δικαιωμάτων αποτρέπεται διότι οποιοσδήποτε θα ήθελε να του αποδοθούν πνευματικά δικαιώματα θα πρέπει να ενθέτει το προϊόν με ένα υδατογράφημα. Τα πνευματικά δικαιώματα δεν αποτελούν μία αφηρημένη έννοια αλλά σχετίζονται με την τεχνογνωσία και την επιστημονική γνώση που περικλείει το προϊόν. Πολλές φορές ιδιαίτερα οι εταιρίες που ασχολούνται με τεχνολογία αιχμής μπορούν να πουλήσουν και τα πνευματικά δικαιώματα σ' άλλο ιδιοκτήτη ή να τα αποδώσουν σ' άλλη εταιρία. Γ'ια μια τέτοια διευθέτηση το πολλαπλό υδατογράφημα είναι αρκετά χρήσιμο. Η μεταφορά των πνευματικών δικαιωμάτων από τον ένα ιδιοκτήτη στο άλλο μπορεί να γίνει με την εναπόθεση νέου υδατογραφήματος που να καταδεικνύει το νέο κύριο της πνευματικής ιδιοκτησίας.

Η εναπόθεση πολλαπλού υδατογραφήματος σ' ένα προϊόν είναι ελεύθερη, όμως δε θα πρέπει σε καμία περίπτωση να αλλοιώνει το ήδη υπάρχον υδατογράφημα. Καθώς στην πνευματική ιδιοκτησία καθοριστικό ρόλο παίζει να μπορεί πάντα να αποδειχθεί η κυριότητα του κατόχου, δηλαδή στη συγκεκριμένη περίπτωση η παραμονή του υδατογραφήματος στο προϊόν να μην βλάπτεται από την επιπλέον προσθήκη ενός ξένου υδατογραφήματος γι' αυτό και επιτρέπεται.



Εικόνα 19 **Διαχωρισμός Προστασίας Πνευματικών Δικαιωμάτων - Προστασίας αυθεντικότητας των περιεχομένων**

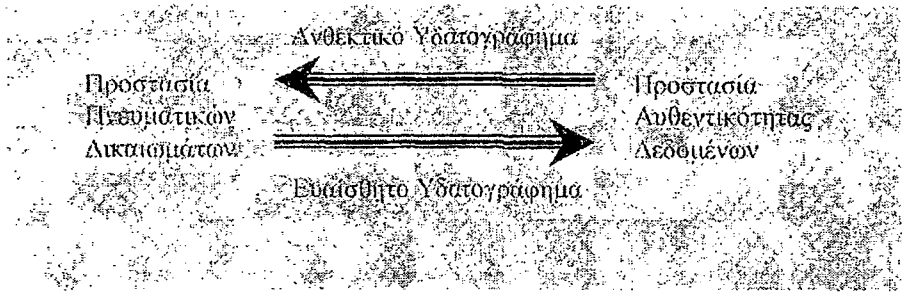
Β. Αυθεντικοποίηση (Authentication) [76]

Τα παραπάνω χαρακτηριστικά δηλαδή η μη αντιληπτή ένθεση, πολυπλοκότητα, συσχετισμένο κλειδί, τυχαιότητα στην παραγωγή του κλειδιού, αξιόπιστη ανίχνευση και στατιστικώς διαφανής ένθεση υιοθετούνται μιας και συμβάλουν στα γενικά χαρακτηριστικά της προστασίας δεδομένων. Παρ' όλ' αυτά αντί για αυθεντικά απαιτούνται εύθραυστα υδατογραφήματα.

Η πιστοποίηση της αυθεντικότητας των δεδομένων σχετίζεται αντιστρόφως ανάλογα με εκείνη της προστασίας των πνευματικών δικαιωμάτων. Από τη μία στην πιστοποίηση της αυθεντικότητας των περιεχομένων των δεδομένων κύριος και βασικός στόχος είναι οποιαδήποτε μορφής επέμβαση για αλλοίωση ή αφαίρεση του υδατογραφήματος να είναι εμφανής και από την άλλη σε ότι αφορά την προστασία της πνευματικής ιδιοκτησίας κύριο μέλημα μας είναι η παραμονή της αόρατης σφραγίδας παρ' όλες τις επεμβάσεις. Οι αντιθετικοί αυτοί στόχοι καταδεικνύουν τον προβληματισμό που απαιτείται για την επιλογή αυτής που θα υπερισχύσει. Τα ειδικά χαρακτηριστικά του προϊόντος και άλλες συνθήκες πρέπει να συνυπολογισθούν ώστε να αποδοθεί στο προϊόν καταλληλότερη μορφή προστασίας. Φυσικά τα δύο παραπάνω χαρακτηριστικά (ανθεκτικότητα-ένθεση πολλαπλών υδατογραφημάτων) που αφορούν ολοκληρωτικά την προστασία δεδομένων δεν είναι μόνο αδιάφορα για την προστασία της αυθεντικότητας αλλά και συμβάλουν αρνητικά σ' αυτή. Η τόσο διαφορετική συνεισφορά των χαρακτηριστικών στις δύο κατηγορίες προστασίας δεδομένων (πνευματικών δικαιωμάτων-αυθεντικότητας) είναι εύλογη μιας και εξυπηρετούν αντίθετους στόχους.

Το μέγεθος της διαφορετικότητας των δυο αυτών κατηγοριών καταδεικνύεται αν σκεφτούμε πως το υδατογράφημα που επιθυμεί να προφυλάσσει πρώτιστος τα πνευματικά δικαιώματα πρέπει να είναι ανθεκτικό σε κάθε μορφής παρέμβασης, ενώ το υδατογράφημα προστασίας της αυθεντικότητας των περιεχομένων πρέπει να είναι «ευερέθιστο» σε οποιαδήποτε επέμβαση του γίνεται και να την προδίδει.

Τα χαρακτηριστικά του υδατογραφημένου προϊόντος σχετίζονται άμεσα με τις απαιτήσεις που πρέπει να καλύπτονται, έτσι κάποια χαρακτηριστικά αποκρύπτονται ή υιοθετούνται σύμφωνα με την δομή προστασίας που επιλέγεται. Δίνοντας βάρος στην προστασία της αυθεντικότητας των δεδομένων είναι φυσιολογικό να μη συμπεριληφθούν τα δύο παραπάνω χαρακτηριστικά του προϊόντος και να υιοθετηθεί η επιλογή της ευαισθησίας του υδατογραφήματος.



Εικόνα 20 **Σχέση**
Πνευματικών Δικαιωμάτων - Αυθεντικότητας Δεδομένων

Ευαισθησία του Υδατογραφήματος (Watermark Sensitivity)

Στην περίπτωση της πιστοποίησης της αυθεντικότητας των περιεχομένων ενός προϊόντος απαιτούνται εύθραυστα υδατογραφήματα, τα οποία δε θα αντέχουν μια ποικιλία από επιθέσεις. Αντίθετα πρέπει να προδίδουν την παρέμβαση που λαμβάνει χώρα στο υδατογραφημένο προϊόν αλλοιώνοντας τόσο το προϊόν όσο και το υδατογράφημα.

Η τροποποίηση ενός υδατογραφημένου προϊόντος θα πρέπει να είναι έκδηλη ακόμη κι αν αυτό επιφέρει την απώλεια της δυνατότητας ανίχνευσης του υδατογραφήματος στο συγκεκριμένο τροποποιημένο προϊόν. Παρόλα αυτά δεν μπορεί ένα ψηφιακό προϊόν να μην επιτρέπει καμία επεξεργασία για να κάνει έκδηλη κάθε τροποποίηση γιατί οδηγεί το προϊόν σε αχρηστία. Έτσι η ανθεντικότητα του υδατογραφήματος πρέπει να υπάρχει και να είναι επιθυμητή για κάποιες περιπτώσεις που οι μετασχηματισμοί του προϊόντος δεν καταστρέφουν την αυθεντικότητα π.χ.

i. Συμπίεση υψηλής ποιότητας[94] όπου δε χάνεται αρκετή πληροφορία ώστε να καταδεικνύεται το υδατογράφημα.

ii. Επικάλυψη (Cropping)[49] σε μη ενδιαφέρουσες περιοχές. Cropping δηλ. Σε περιοχή δεδομένων όπου η πληροφορία που υπάρχει εκεί δεν επηρεάζει το υδατογράφημα.

iii. Άλλους μη σημαντικούς μετασχηματισμούς που είναι απαραίτητοι και κάνουν το προϊόν συμβατό με το πολυμεσικό περιβάλλον.

4

ΥΔΑΤΟΓΡΑΦΗΜΑ ΣΕ ΚΕΙΜΕΝΟ

4.1 Εισαγωγή

Για να μπορέσουμε να δώσουμε μια εικόνα των μεθόδων και γενικότερα της χρήσης του υδατογραφήματος στο κείμενο (text) θα πρέπει να περιγράψουμε μια βασική διάκριση στα είδη του κειμένου. Η διάκριση αυτή είναι αναγκαία μιας και σε αυτή στηρίζεται η διαφοροποίηση των μεθόδων υδατογράφησης. Έτσι διακρίνουμε το κείμενο σε δύο κατηγορίες στο [72] hard-copy text και στο soft-copy text [35].

Το hard-copy text μπορούμε να το θεωρήσουμε σαν μια υψηλά δομημένη (highly structured) εικόνα και έτσι το κείμενο δύναται να υποστεί μια πληθώρα τεχνικών υδατογράφησης ίδιων με αυτές που εφαρμόζονται στην εικόνα.

Απεναντίας το soft-copy text αποτελεί ένα δύσκολο πεδίο για υδατογράφηση καθώς είναι αρκετά δύσκολη η ένθεση της πληροφορίας μέσα σε αυτό. Το εμπόδιο αυτό είναι αναμενόμενο μιας και σε ένα αρχείο κειμένου υπάρχει σχετική έλλειψη από πλεονάζουσα πληροφορία σε σχέση με ένα αρχείο εικόνας ή ήχου. Παραδείγματος χάριν παρόλο που είναι εύκολο σε μία εικόνα να κάνουμε τροποποιήσεις όπου δεν γίνονται αντιληπτές, η προσθήκη ενός επιπλέον γράμματος ή μιας τελείας δύναται

να γίνει αντιληπτή από οποιονδήποτε διαβάζει το κείμενο.

Η ένθεση πληροφορίας μέσα σε ένα κείμενο είναι πρωταρχικής σημασίας να περιλαμβάνει τροποποιήσεις του κειμένου που να μην γίνονται ορατές από τον αναγνώστη. Εξ' άλλου από τις βασικές ιδέες του υδατογραφήματος είναι η διαφάνεια στην ένθεση και αυτή θα πρέπει να τη διαφυλάξουμε κατά την υδατογράφηση κειμένου.

4.2 Τεχνικές υδατογράφησης σε κείμενο

Πάνω σε αυτές τις βασικές ιδέες έχουν αναπτυχθεί πολλές μέθοδοι για την υδατογράφηση σε κείμενο. Η υδατογράφηση hard-copy text σχετίζεται άμεσα με την υδατογράφηση εικόνας όπου εκεί υπάρχει μία ποικιλία τεχνικών. Για το soft-copy text παρόλο που αποτελεί ένα δύσκολο αντικείμενο, έχουν αναπτυχθεί και εδώ κάποιες αξιόπιστες τεχνικές. Υπάρχουν τρεις βασικές μέθοδοι κωδικοποίησης δεδομένων μέσα στο κείμενο.

1. Οι μέθοδοι των ανοιχτών διαστημάτων [1] που η κωδικοποίηση τους βασίζεται στον χειρισμό των λευκών διαστημάτων (της μη χρησιμοποιημένης περιοχής στην εκτυπωμένη σελίδα).
2. Συντακτικοί μέθοδοι. [1] Σε αυτήν την περίπτωση χρησιμοποιείται η στίξη ενός κειμένου.
3. Σημασιολογικοί μέθοδοι[1] που η κωδικοποίηση βασίζεται στο χειρισμό των ίδιων των λέξεων.

Επειδή και στις τρεις κατηγορίες έχουν βασιστεί αρκετές τεχνικές για αυτό θα ήταν σκόπιμο να τις εξετάσουμε χωριστά.

4.2.1 Μέθοδος ανοιχτών διαστημάτων[85] [35]

Η μέθοδος αυτή χρησιμοποιεί το γεγονός ότι ο αριθμός των ανοιχτών διαστημάτων δεν έχει μεγάλη σπουδαιότητα για το κείμενο. Αρχικά η αλλαγή του αριθμού των διαστημάτων σε μία γραμμή δεν επιφέρει σχεδόν καμία αλλαγή στο νόημα της φράσης ή της πρότασης.

Επιπλέον οποιοσδήποτε αναγνώστης είναι σπάνιο να παρατηρήσει τους χειρισμούς που έχουν γίνει στα κενά διαστήματα. Έτσι πάνω σε αυτή την ιδέα αναπτύχθηκαν τρεις τεχνικές υδατογράφησης μιας και οι τροποποιήσεις κειμένου είναι δυνατές χωρίς να γίνονται αντιληπτές.

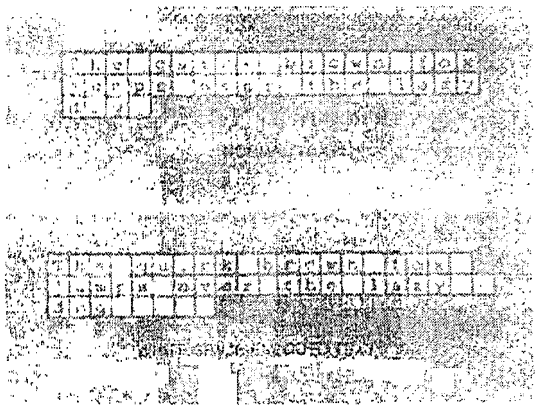
1. Η πρώτη τεχνική ενθέτει ένα δυαδικό μήνυμα μέσα στο κείμενο τοποθετώντας ένα ή δύο κενά διαστήματα μετά από κάθε τερματικό χαρακτήρα. Ας φέρουμε ένα παράδειγμα για να γίνει πιο αντιληπτή η τεχνική υδατογράφησης κειμένου. Το απλό κενό κωδικοποιεί ένα «0» ενώ τα δύο κενά κωδικοποιούν ένα «1». Έτσι το κλειδί που είναι ένας δυαδικός αριθμός που επιλέγεται για λόγους ασφάλειας από μια ψευδοτυχαία γεννήτρια αριθμών εντίθεται μεσώ της παραπάνω διαδικασίας υδατογράφησης με χρήση των κενών διαστημάτων σε όλο το κείμενο. Επιτυγχάνεται λοιπόν η υδατογράφηση ενός soft-copy text μοναδική για κάθε κείμενο και διαφανή προς τον αναγνώστη.

   Η τεχνική αυτή έχει αρκετά μειονεκτήματα. Εναι αρκετά μη αποδοτική μιας και απαιτείται μια μεγάλη ποσότητα κειμένου για την κωδικοποίηση λίγων δυαδικών ψηφίων, (π.χ. ένα bit σε κάθε πρόταση εξισώνεται με μία τιμή δεδομένων τουλάχιστον ένα bit ανά 160 bytes υποθέτοντας ότι οι προτάσεις

είναι κατά μέσο όρο δύο γραμμές κειμένου ογδόντα χαρακτήρων. Επιπλέον η υδατογράφηση σχετίζεται άμεσα με τη δομή του κειμένου. Έτσι κείμενα με ιδιαίτερη δομή περιορίζουν τη δυνατότητα υδατγράφησης όπως π.χ. κείμενα σύγχρονης ποίησης. Επιπλέον πολλοί επεξεργαστές κειμένου μορφοποιούν από μόνοι τους τον αριθμό των κενών μετά τους τερματικούς χαρακτήρες. Τέλος η αντιφατική-υπερβολική χρήση των λευκών διαστημάτων είναι πια αόρατη.

Αρκετά από τα παραπάνω μειονεκτήματα κάνουν την ικανότητα της παραπάνω υδατογράφησης, ελλειπή.

2. Μια δεύτερη μέθοδος εκμετάλλευσης των λευκών διαστημάτων [1] για ένθεση υδατογραφήματος είναι η εισαγωγή κενών διαστημάτων στο τέλος κάθε γραμμής. Τα δεδομένα εντίθενται επιτρέποντας ένα προκαθορισμένο κενό στο τέλος κάθε γραμμής. Δύο κενά διαστήματα κωδικοποιούν ένα bit για κάθε γραμμή, τέσσερα κενά κωδικοποιούν δύο bit, οκτώ κωδικοποιούν τρία κ.ο.κ. Έτσι σε σχέση με την προηγούμενη μέθοδο μπορούμε να κωδικοποιήσουμε πολύ μεγαλύτερη ποσότητα πληροφορίας. Επίσης η μέθοδος αυτή εφαρμόζεται σε οποιοδήποτε είδους κειμένου ενώ ταυτόχρονα η υδατογράφηση δε γίνεται αντιληπτή από τον οποιοδήποτε αναγνώστη. Βέβαια και αυτή η μέθοδος παρουσιάζει προβλήματα καθώς σήμερα υπάρχουν πληθώρα προγραμμάτων που επιτελούν αυτόματα μορφοποίηση κειμένου και αφαιρούν τα επιπλέον, ή όσα θεωρούνται άσκοπα κενά, όπως παραδείγματος χάρη το πρόγραμμα send mail. Αυτή η μέθοδος είναι σαφώς καλύτερη μιας και επιλύει το πρόβλημα του ποσού της πληροφορίας που κωδικοποιείται παρ' ολ' αυτά έχει και αυτή κάποια μειονεκτήματα που προαναφέρθηκαν.



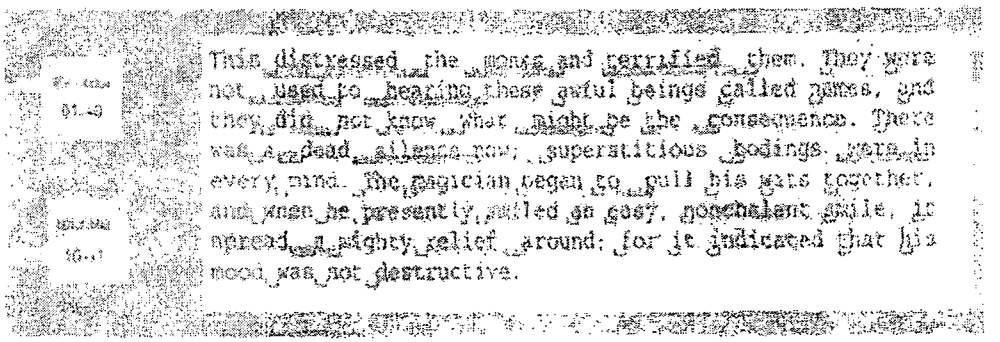
Εικόνα 23 **Παράδειγμα ένθεσης κρυφών δεδομένων χρησιμοποιώντας τα κενά**

3. Η Τρίτη τεχνική η οποία κάνει χρήση των λευκών διαστημάτων στην ένθεση υδατογραφήματος και περιλαμβάνει δεξιό έλεγχο κειμένου[1]. Τα επιπλέον δεδομένα εντίθενται ελέγχοντας που είναι τοποθετημένα τα επιπλέον κενά καθώς η θέση των κενών αποτελεί το βασικό χαρακτηριστικό της τεχνικής αυτής. Ένα κενό μεταξύ 2 λέξεων ερμηνεύεται σαν ένα «0», 2 κενά ως ένα «1». Με τον τρόπο αυτό έχουμε σαν απόρροια να εντίθενται αρκετά bits σε κάθε γραμμή.

Εξαιτίας των περιορισμών κατά το έλεγχο κειμένου υπήρξε μια περαιτέρω

βελτίωση της μεθόδου. Καταρχάς δεν μπορεί να χρησιμοποιούνται όλα τα κενά μέσα σε λέξεις ως κρυμμένα δεδομένα γι' αυτό είναι αναγκαίο να γίνει ένας διαχορισμός των κενών σε αυτά που θεωρούνται κρυμμένα bits δεδομένων και σε αυτά που θεωρούνται μέρος του αρχικού κειμένου.

Έτσι χρησιμοποιούμε μια Manchester τύπου κωδικοποίηση. Η Manchester τεχνική κωδικοποιεί ομάδες από bits σε ζεύγη των 2 bits ερμηνεύοντας το 01 σε 1 και το 10 σε 0. Το string από bits «00» και «11» είναι το «κενό». Για παράδειγμα το κωδικοποιημένο μήνυμα 1000101101 μειώνεται σε 001 αφού το 110011 είναι το «κενό».


This distressed the people and terrified them. They were not used to hearing these awful beings called names, and they did not know what might be the consequence. There was a dead silence now; superstitious bodings were in every mind. The magician began to pull his pots together, and when he presently pulled an easy, nonchalant smile, it spread a mighty relief around; for it indicated that his mood was not destructive.

Αυτή η μέθοδος αναιρεί πολλά από τα μειονεκτήματα των άλλων δύο παραπάνω.Όμως και εδώ τα γενικά μειονεκτήματα των τεχνικών των λευκών διαστημάτων διατηρούνται. Σ' αυτό το σημείο καλό είναι να αναφέρουμε συμπεράσματα γενικά για τις μεθόδους που χρησιμοποιούν στη κωδικοποίηση τα κενά διαστήματα.

Οι μέθοδοι που χρησιμοποιούν στην κωδικοποίηση του κειμένου τα κενά διαστήματα έχουν χρησιμότητα όσο το κείμενο παραμένει σε μορφή χαρακτήρων ASCII. Όταν η μορφή του κειμένου αλλάξει (από την ASCII μορφή του) τότε παρουσιάζονται τα μειονεκτήματα που προαναφέραμε. Έτσι έχουμε τις δυσμενείς συνέπειες απώλειας δεδομένων κατά την εκτύπωση του κειμένου. Βέβαια το εκτυπωμένο αρχείο μπορεί να μην είναι ένα κείμενο με τη μορφή ASCII χαρακτήρων όμως παρουσιάζει πολλές περαιτέρω δυνατότητες μιας και σαν hard-copy text υπόκειται σε πληθώρα επεξεργασιών.

Οι επεξεργασίες και η μορφοποίηση ενός εκτυπωμένου κειμένου δεν μένει στην αλλαγή της θέσης των κενών ή στην μετατόπιση των σημείων στίξης αλλά χρησιμοποιεί πολλές τεχνικές από την υδατογράφηση εικόνας π.χ. Patchwork.

Συμπεραίνουμε πως έχει νόημα η ενασχόληση και η παρατήρηση των μεθόδων αυτών εφόσον μας ενδιαφέρει η υδατογράφηση κειμένου σε μορφή ASCII ειδάλλως πρέπει να ασχοληθούμε με τις μεθόδους υδατογράφησης του hard-copy text. Βέβαια υπάρχουν και άλλες αξιόπιστες τεχνικές για την υδατογράφηση soft-copy text.

4.2.2 Συντακτικές μέθοδοι [54], [1]

Το γεγονός του ότι το κενό μέσα σε κείμενα θεωρείται ιδιαίτερος χαρακτήρας για τις μεθόδους απόκρυψης δεδομένων, έχει τα πλεονεκτήματα του και τα μειονεκτήματα του. Ως βασικό πλεονέκτημα κατατάσσουμε το ότι ένας αναγνώστης δεν μπορεί να αντιληφθεί εύκολα την πρόσθεση ή αφαίρεση κενού σε ένα κείμενο. Από την άλλη όμως, όπως ειπώθηκε και παραπάνω, ένας επεξεργαστής κειμένου μπορεί εύκολα να αποκόψει τα περιττά κενά στο κείμενο,

πράγμα που θα κατέστρεφε τα κρυφά δεδομένα.

Αυτό δηλαδή που πρέπει να λάβουμε υπόψιν και να δώσουμε λύση, είναι η ανθεκτικότητα των κρυφών δεδομένων απέναντι σε μορφοποιήσεις κειμένου. Απάντηση σε αυτό δίνουν οι συντακτικοί και σημασιολογικοί μέθοδοι. Καταρχήν θα πρέπει να σημειώσουμε το ότι βασιζόμενοι στο γεγονός ότι αυτές οι μέθοδοι δεν παρεμβάλλονται στη μέθοδο ανοιχτών διαστημάτων, μπορούμε κάλλιστα και τα δύο είδη μεθόδων να χρησιμοποιηθούν παράλληλα.

Όσον αφορά τις συντακτικές μεθόδους μπορούμε να κάνουμε τις εξής παρατηρήσεις. Πολλές φορές η χρήση των σημείων στίξης όπως το κόμμα μπορεί να είναι διφορούμενοι π.χ η φράση «δυο, τρία , και τέσσερα» είναι ίδια συντακτικά με τη φράση «δυο, τρία και τέσσερα». Επίσης σε πολλές γλώσσες μπορούν να υπάρξουν εναλλακτικοί τρόποι χρήσης των χρόνων της γραμματικής. Όπως και η προσεχτική χρήση συντομεύσεων και συνηρημένων είναι φαινόμενα που εμφανίζονται στο γραπτό λόγο.

Κωδικοποιώντας τα παραπάνω μπορούμε να επιτύχουμε απόκρυψη δεδομένων η οποία όμως, λαμβάνοντας υπόψη τη μικρή συχνότητα εμφάνισης τέτοιων φαινομένων, φτάνει σε ρυθμούς των μερικών bit ανά Kbyte κειμένου.

Τέλος θα πρέπει να προσέξουμε το γεγονός ότι μερικές φορές η αλλαγή ενός τόνου ή ενός κόμματος μπορεί να κάνει το κείμενο δυσνόητο ή να αλλάξει εντελώς την ένια του.

4.2.3 Σημασιολογικές Μέθοδοι [1]

Η τελευταία μέθοδος απόκρυψης δεδομένων είναι η αλλαγή των ίδιων των λέξεων του κειμένου με συνώνυμες λέξεις. Η σημασιολογική μέθοδος είναι παρόμοια με την συντακτική μόνο που εδώ κωδικοποιούμε συνώνυμα χωρίζοντας τα σε πρωτεύοντα και δευτερεύοντα, κωδικοποιώντας τα αντίστοιχα σε μηδενικά και άσους. Το αν ένα συνώνυμο είναι πρωτεύον ή δευτερεύον δεν έχει σχέση με το ρυθμό τον οποίο θα χρησιμοποιείται.

Ορισμένες λέξεις μπορούν να έχουν περισσότερα Από ένα συνώνυμα. Στην περίπτωση αυτή χρησιμοποιούμε περισσότερα bit δεδομένων για κάθε αντικατάσταση λέξης βελτιώνοντας έτσι το ρυθμό κρυφών δεδομένων.

Τέλος θα πρέπει να προσέξουμε τα προβλήματα που μπορεί να εμφανιστούν με την αντικατάσταση συνώνυμων λέξεων οι οποίες αλλοιώνουν το νόημα της πρότασης όπως π.χ. η αντικατάσταση της λέξης πρώτος με τη λέξη αρχικός στην φράση «είσαι και ο πρώτος».

4.3 Συμπεράσματα

Έχουμε παρουσιάσει διάφορες πιθανές τεχνικές για την ένθεση κρυφής πληροφορίας σε κείμενο. Κάνοντας το διαχωρισμό του κειμένου σε hard-copy και soft-copy επισημαίνουμε την χρησιμότητα κυρίως των soft-copy μεθόδων μιας και στην περίπτωση του hard-copy μεταβαίνουμε στο πεδίο της εικόνας όπου χρησιμοποιούνται διαφορετικές τεχνικές και διαδικασίες.

Το βασικό συμπέρασμα που βγαίνει από τις τρεις μεθόδους είναι ότι παρόλη την πιθανή επιτυχία στην ένθεση κρυφής πληροφορίας που μπορεί να έχουν, δημιουργούν πολλά προβλήματα, τα οποία πρέπει να ξεπεραστούν για να θεωρούνται βέλτιστες. Πρώτο είναι ότι για τις δύο τελευταίες μεθόδους χρειάζεται να είναι πολύ προσεχτική η χρήση τους γιατί πολύ εύκολα μπορεί να χαθεί η μη

ορατότητα της κρυφής πληροφορίας Από μια λάθος αντικατάσταση ή χειρισμό. Δεύτερο και κυριότερο είναι ότι και οι τρεις μέθοδοι επιτυγχάνουν αρκετά χαμηλό ρυθμό ένθεσης κρυφών δεδομένων μέσα στο κείμενο.

5

ΥΔΑΤΟΓΡΑΦΗΣΗ ΣΕ ΚΙΝΟΥΜΕΝΗ ΕΙΚΟΝΑ (VIDEO)

5.1 Εισαγωγή

Η υδατογράφηση σε video [40], [64] αποτελεί μία μέθοδο προστασίας που προστατεύει τα πνευματικά δικαιώματα στα αρχεία video. Επιπλέον ανιχνεύει τα παραγόμενα παράνομα αντίγραφα επιβλέποντας τη χρήση των πολυμεσικών προϊόντων και ελέγχοντας την ακολουθία δεδομένων που μεταφέρονται μεσώ του δικτύου και των εξυπηρετητών (servers).

Μία επιτυχής σχεδίαση ενός αλγορίθμου που ενθέτει υδατογράφημα σ' ένα σήμα video θα πρέπει να μπορεί να ενσωματώνει οποιασδήποτε μορφής πληροφορίας όπως δυαδικές κωδικοποιημένες λέξεις κα.

Τα υδατογραφήματα όπως ταμπέλες ή κώδικες πρέπει να ενσωματώνονται στο video με τέτοιο τρόπο ώστε να παραμένει «αόρατο» από τον κοινό παρατηρητή και ταυτόχρονα είναι πολύ δύσκολη έως αδύνατη η αφαίρεση του ακόμη και αν χρησιμοποιηθούν ποικίλες πολυμεσικές επεξεργασίες στο προϊόν.

Η επιτυχία της τεχνικής υδατογράφησης ενός πολυμεσικού προϊόντος στηρίζεται στην παραμονή της ταμπέλας που πιστοποιεί τα πνευματικά δικαιώματα. Γι' αυτό το λόγο η ταμπέλα που ενθέτεται θα πρέπει να παρέχει προστασία και ανθεκτικότητα απέναντι σε μία ποικιλία μορφοποιήσεων επεξεργασιών που μπορεί να αποφέρουν την πλαστογραφία της ταμπέλας πνευματικών δικαιωμάτων, την

παραβίαση ή την αχρηστία του κλειδιού υδατογράφησης.

5.2 Κακόβουλες Επιθέσεις (Attacks)

Επιθέσεις που στοχεύουν στην αφαίρεση ή την τροποποίηση του υδατογραφημένου video ώστε να παραβιαστεί η προστασία πνευματικών δικαιωμάτων είναι οι παρακάτω [73]:

1. Εντοπισμός της περιοχής που έχει ενσωματωθεί το υδατογράφημα με διαδικασίες σύγκρισης υδατογραφημένων video με το αρχικό.
2. Ανεύρεση της τροποποίησης των υδατογραφημένων δεδομένων τα οποία έχουν προστεθεί στο video. Το γεγονός αυτό μπορεί να είναι αποτέλεσμα μέσω οπτικής και στατιστικής ανάλυσης του video.

   Με τη χρήση της IBM [38] μορφοποίησης όπου επιτυγχάνει την αφαίρεση του υδατογραφήματος ώστε να δημιουργηθεί ένα εικονικό αντίτυπο του αρχικού αυθεντικού προϊόντος. Η ύπαρξη αυτού του προϊόντος διεκδικεί την ιδιοκτησία των πνευματικών δικαιωμάτων. Το γεγονός αυτό επιτυγχάνεται με την ανάπτυξη όχι ενός νέου ή ίδιου αλγόριθμου υδατογράφησης αλλά με την ανάπτυξη ενός αλγόριθμου που μπορεί να αφαιρέσει το αρχικό υδατογράφημα.
3. Με τη βοήθεια επεξεργασίας πολυμεσικών προϊόντων μπορεί να αλλοιωθεί ή να αφαιρεθεί η πληροφορία που ενσωματώνονται. Σ' αυτή την προϊόντα αυτά εφαρμόζεται αρκετά συχνά η MPEG [41], [30] συμπίεση που αποτελεί μία συμπίεση των δεδομένων προκαλώντας απώλεια δεδομένων και κλιμάκωση των δειγμάτων.

   Η MPEG συμπίεση στο video αποτελεί καθοριστικό παράγοντα για την υδατογράφηση σε ψηφιακό video μιας και η οποιαδήποτε μορφοποίηση των καρέ του προϊόντος μπορεί να παραμορφώσει τόσο το υδατογράφημα όσο και το ίδιο το προϊόν. Από άλλη οπτική γωνία η MPEG συμπίεση κάνει το προϊόν αρκετά πιο εύχρηστο και αποτελεί μία ευρέα διαδεδομένη τεχνική. Μία μέθοδος προστασίας θα πρέπει να απαντά στην απαίτηση για προστασία του προϊόντος από τους κακόβουλους χρήστες χωρίς όμως να περιορίζει αρκετά την ευελιξία χρήσης του.

   Το υδατογράφημα απαντώντας στην υδατογράφηση του MPEG video καταφέρνει να προσφέρει επί της ουσίας ασφάλεια στα προϊόντα βίντεο χωρίς να μειώσει τις δυνατότητες του προϊόντος.

5.3 Απαιτήσεις για MPEG Video Υδατογράφηση

Οι MPEG αλγόριθμοι συμπίεσης σημάτων χρησιμοποιούν το διακριτό μετασχηματισμό συνημίτονων (DCT) για την κωδικοποίηση των μπλοκ της εικόνας AS [94] πρόβλεψης και της κίνησης. Το αποτέλεσμα της MPEG συμπίεσης είναι μία ακολουθία από συχνοτικά περιεχόμενα για τα I καρέ (εικόνα) για το P καρέ (πρόβλεψη) και για το M καρέ (κίνησης).

Η παραπάνω επεξεργασία θα πρέπει να συνδυάζεται με τα χαρακτηριστικά που είναι αναγκαίο το υδατογραφημένο βίντεο να έχει. Για το λόγο αυτό θα πρέπει να προσεχθούν κάποιοι παράγοντες που σχετίζονται με την MPEG συμπίεση ώστε να μην αλλοιώσει το υδατογράφημα.

1. Η πολυμεσική πληροφορία που ενσωματώνεται στο βίντεο θα πρέπει να είναι ανθεκτική σε μεγάλους βαθμούς συμπίεσης του διακριτού μετασχηματισμού συνημίτονου (DCT) στην επανόρθωση της κίνησης και στην πρόβλεψη.
2. Το υδατογράφημα θα πρέπει να χαρακτηρίζεται από ανθεκτικότητα και στην κλιμάκωση του σήματος που αποτελεί μία συνηθισμένη πολυμεσική επεξεργασία.
3. Η ένθεση υδατογραφημένης πληροφορίας θα πρέπει να γίνεται σε κάθε ένα από τα καρέ και των τριών κατηγοριών ώστε η αποκοπή κάποιου αριθμού από καρέ να μην αποφέρει την αφαίρεση της υδατογραφημένης πληροφορίας.
4. Αναγκαία είναι η ορθή αποκωδικοποίηση των συχνοτήτων των καρέ ώστε να μην υπάρξει ορατή διαφορά στον κοινό παρατηρητή. Η διαδικασία της διατήρησης της διαφάνειας του υδατογραφήματος του βίντεο απαιτεί προσεκτική υδατογράφηση και ανίχνευση μιας και μία μορφοποίηση ή αλλαγή σ' ένα καρέ (π.χ. I) επηρεάζει και την κωδικοποίηση στα άλλα (P και B καρέ).
5. Απαιτείται ο αλγόριθμος να χαρακτηρίζεται από ταχύτατη απόδοση για βιντεοσκοπημένο ή πραγματικού χρόνου βίντεο. Όμως η σημαντικότητα αυτού του παράγοντα δεν είναι μέγιστη μιας και τα περιβάλλοντα που χρησιμοποιούνται για την παρακολούθηση ή επεξεργασία του βίντεο δεν απαιτούν σειριακό πραγματικό χρόνο.

5.4 Τεχνικές Υδατογράφησης Video

Ήδη έγινε αναφορά στην υδατογράφηση του MPEG βίντεο που αποτελεί μία από τις βασικές μεθόδους υδατογράφησης. Εκτός απο αυτή υπάρχουν και δύο άλλες βασικές τεχνικές, που χρησιμοποιούνται για την υδατογράφηση του video που είναι επίσης σημαντικές η μέθοδος Zhao Koch [17]και η μέθοδος Fridrich[32].

5.4.1 Ο αλγόριθμος του Zhao Koch

Η τεχνική αυτή ενθέτει πληροφορία που πιστοποιεί τα πνευματικά δικαιώματα στο πεδίο της συχνότητας.

Διαδικασία ένθεσης

1. Αρχικά η πληροφορία που σχετίζεται με την φωτεινότητα Y υφίσταται διακριτό μετασχηματισμό συνημίτονου (DCT) με βάση τη συχνότητα και έπειτα κβαντίζεται. Τα κβαντισμένα δείγματα ουσιαστικά είναι μετατροπή του συνεχούς σήματος σε διακριτό.
2. Έπειτα επιλέγονται με τυχαίο τρόπο 3 συντελεστές από τα προηγούμενα κβαντισμένα διακριτά δείγματα του διακριτού μετασχηματισμού Fourier. Οι τρεις συντελεστές του Fourier χρησιμοποιούνται για την αποθήκευση ενός διάδικου ψηφίου στην πληροφορία του υδατογραφήματος που πιστοποιεί την αυθεντικότητα.
3. Το κλειδί σ' αυτή τη διαδικασία αποτελεί η αντιστοίχηση περιοχών του αρχικού σήματος με 1 ή 0 ανάλογα με την τυχαία επιλογή. Αντιστοιχίζοντας το 1 και το 0 σε πρότυπα και σε συνδυασμό με τους

συντελεστές παράγεται η υδατογραφημένη πληροφορία.

Διαδικασία Ανίχνευσης

Για τη διαδικασία ανίχνευσης υδατογραφήματος χρησιμοποιείται σαν είσοδος το κλειδί και οι συντελεστές που παράχθηκαν όπως περιγράφτηκε παραπάνω και σαν έξοδο παίρνουμε τα 1 και 0 που εισήχθηκαν στο σήμα του video κατά την ένθεση. Στη διαδικασία της ανίχνευσης είναι φανερό πως δεν απαιτείται η ύπαρξη του αρχικού σήματος γεγονός που διευκολύνει την πιστοποίηση του υδατογραφημένου βίντεο και επισπεύδει την ανίχνευση.

Η διαδικασία Zhao Koch είναι αρκετά ανθεκτική και στη συνηθισμένη MPEG συμπίεση που υφίστανται τα αρχεία βίντεο. Όμως η τεχνική αυτή δεν είναι ανθεκτική σε επεξεργασίες όπως κλιμάκωση ή μετατόπιση των συνημίτονων καθώς οι διαστάσεις χρησιμοποιούνται για την παραγωγή του υδατογραφήματος. Η μέθοδος του Zhao Koch χρησιμοποιείται ευρέως μιας και επιτρέπει στο υδατογραφημένο προϊόν την MPEG συμπίεση και την κωδικοποίηση των P και των B καρέ. Για την βελτίωση της σχέσης μεταξύ της καλής ποιότητας του video και της ανθεκτικότητας στις επιλεγόμενες μορφές επεξεργασίας χρησιμοποιείται η διαδικασία διόρθωσης των λαθών.

5.4.2 Ο Fridrich Αλγόριθμος

Διαδικασία Ένθεσης

Η μέθοδος στηρίζεται στη πρόσθεση ενός προτύπου του οποίου η ενέργεια συγκεντρώνεται ως επί το πλείστον στις χαμηλές συχνότητες.

Το πρότυπο παράγεται χρησιμοποιώντας μία ψευδοτυχαία γεννήτρια αριθμών και ένα αυτόματο με δυνατότητα ανάγνωσης κανόνων. Η μέθοδος χρησιμοποιεί κατά κύριο λόγο την ένθεση του προτύπου το οποίο σχετίζεται άμεσα με τη συχνότητα του υδατογραφήματος.

Η συχνότητα διάδικου ψηφίου του υδατογραφήματος χρησιμοποιείται για την αρχικοποίηση της ψευδοτυχαίας γεννήτριας ώστε να δημιουργήσει ένα τυχαίο μαύρο ή άσπρο αρχικοποιημένο πρότυπο στο ίδιο μέγεθος με την εικόνα. Έπειτα εφαρμόζεται φίλτρο ώστε η ενέργεια του σήματος να παραμείνει σε χαμηλά επίπεδα και έπειτα το πρότυπα προστίθενται στην εικόνα.

Η μέθοδος αυτή παρουσιάζει μία μικρή αντιληπτή παραμόρφωση μιας και το πρότυπο που προστίθεται επιδρά στα χαρακτηριστικά του video. Η παραμόρφωση αυτή μπορεί να ελατωθεί χρησιμοποιώντας κατάλληλο φίλτρο.

Επιπλέον το υδατογραφημένο βίντεο είναι ανθεκτικό σε πολλούς μετασχηματισμούς όπως JPEG συμπίεση επαναδειγματοληψία, υπο-δειγματοληψία, πρόσθεση θορύβου. Τέλος το υδατογράφημα είναι αρκετά ανθεκτικό στις μορφοποιήσεις που χρησιμοποιούν επικάλυψη και στην εισαγωγή πολλαπλού υδατογραφήματος.

Ένα από τα βασικά μειονεκτήματα αυτής της τεχνικής είναι ότι η διαδικασία της ανίχνευσης απαιτεί την ύπαρξη του αρχικού σήματος. Ειδικά στη διαδικασία υδατογράφησης βίντεο αυτό είναι αρκετά δύσκολο γι' αυτό και χρησιμοποιούνται κάποιες στατιστικές μέθοδοι ώστε να αποφευχθεί. Επίσης ένα άλλο μειονέκτημα είναι ότι στην υδατογράφηση του βίντεο επιθυμητή είναι η πληροφορία που ενθέτεται να περιέχει αναγκαία στοιχεία του κατόχου των πνευματικών δικαιωμάτων γεγονός που επίσης δεν είναι εφικτό μ' αυτήν την τεχνική.

Η πρόσθεση της πιστοποίησης των στοιχείων του ιδιοκτήτη μπορεί να γίνε με

κώδικες λέξεις,πράγμα που εξασθενεί κάπως το τελευταίο μειονέκτημα. Η μέθοδος του Fridrich δεν προκαλεί αλοίωση της ποιότητας και αυτή διατηρείται ακόμη και αν εφαρμοσθούν πολλαπλή μετασχηματισμοί στο υδατογραφημένο βίντεο γι'αυτούς τους λόγους αποτελεί μία αξιόπιστη μέθοδος υδατογραφήσεις.

5.4.3 MPEG Υδατογράφηση

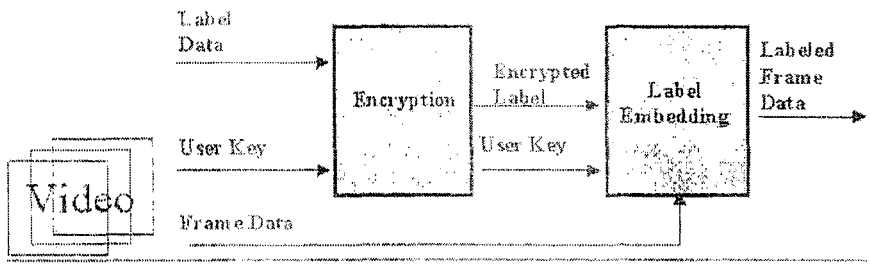
Η τεχνική υδατογράφησης προσαρμόζεται στη δυνατότητα να εντεθεί πληροφορία υδατογραφήματος στο video που να μην είναι αντιληπτή. Χρησιμοποιεί γι' αυτό το λόγοτα χαρακτηριστικά του ανθρώπινου οπτικού συστήματος.

Οι παράμετροι που οικειοποιείται από το οπτικό σύστημα είναι η ομοιομορφία και τα χαρακτηριστικά των ακμών σ' ένα μπλοκ. Τα στοιχεία που σχετίζονται με τις ικανότητες του ανθρώπου σχετικά με τις ακμές μιας φωτογραφίας βασίζονται κυρίως στην ανάλυση του διακριτού μετασχηματισμού Fourier. Οι παράγοντες του D.F.T. κυμαίνονται ανάλογα με το αν μία ακμή μπορεί να διαχωριστεί σε σχέση με τα διανυσματικά χαρακτηριστικά της οριζόντιας ή κάθετης γραμμής.

Η ομοιομορφία και τα χαρακτηριστικά των ακμών αποτελούν 2 προϋποθέσεις που λαμβάνονται υπόψιν από τους αλγόριθμους υδατογράφησης ώστε να μη γίνεται αντιληπτό αποτέλεσμα. Η γενική κωδικοποίηση MPEG [22] του video ακολουθεί τα παρακάτω στάδια.

Διαδικασία ένθεσης

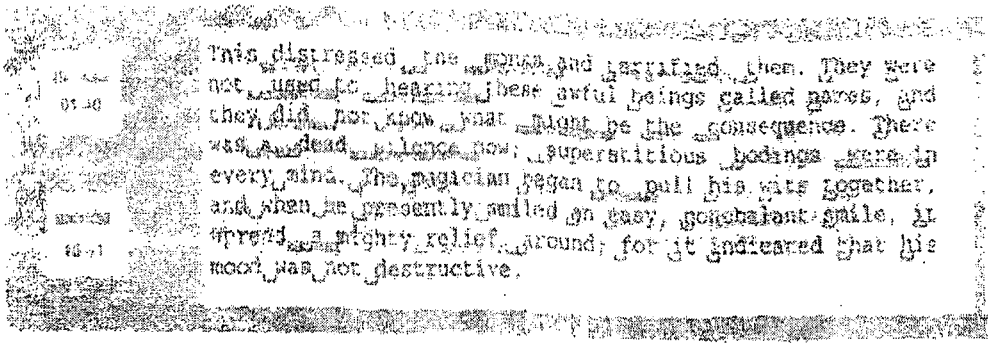
1. Αρχικά το MPEG βίντεο αποκωδικοποιούνται και παράγονται τα απλά καρέ.
2. Η πληροφορία που ενσωματώνεται στο βίντεο κωδικοποιείται από ένα ιδιωτικά κλειδί.
3. Το υδατογράφημα ενσωματώνεται στο βίντεο με τη χρήση του κλειδιού.



Εικόνα 26 **Διαδικασία ένθεσης MPEG**

Διαδικασία ανίγνευσης

1. Το MPEG βίντεο υφίσταται αποκωδικοποίηση για να παραχθούν τα απλά καρέ.
2. Με τη βοήθεια του ιδιωτικού κλειδιού και των υδατογραφημένων δεδομένων παράγεται το υδατογράφημα. Η ανίχνευση του υδατογραφήματος γίνεται με τη βοήθεια του κλειδιού και του κωδικοποιημένου υδατογραφήματος απ' όπου παράγεται η πληροφορία που εντέθηκε στο υδατογράφημα και η πιστοποίηση είναι εφικτή.



Εικόνα 27 **Διαδικασία ανίχνευσης MPEG**

1_{ov}	16	11	10	16	24	40	51	61
	12	12	14	19	26	58	60	55
	14	13	16	24	40	57	69	56
	14	17	22	29	51	87	80	62
	18	22	37	56	68	109	103	77
	24	35	55	64	81	104	113	92
	49	64	78	87	103	121	120	101
	72	92	95	98	112	100	103	99

High

Εικόνα 28 **Πίνακας Κβαντισμένων Συντελεστών**

Το κλειδί χρησιμοποιείται και στα δύο στάδια και διαφυλάσσει την μοναδικότητα του υδατογραφήματος. Το κλειδί δημιουργείται από μία γεννήτρια παραγωγής τυχαίων αριθμών. Η MPEG υδατογράφηση χρησιμοποιεί δύο μεθόδους υλοποίησης μια υλοποίηση στο πεδίο των συχνοτήτων και μια στο πεδίο του χρόνου.

5.4.3.1 MPEG Υδατογράφηση στο συχνοτικό πεδίο[22].

Η διαδικασία ένθεσης ακολουθεί τα εξής 3 στάδια:

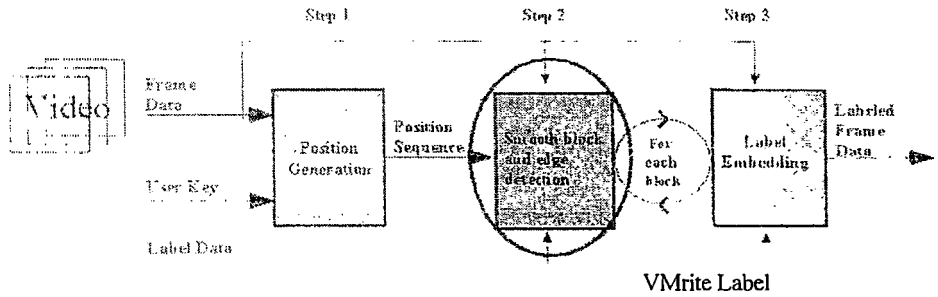
1. Η γεννήτρια τυχαίας παραγωγής αριθμών παράγει μία συχνότητα. Στην τιμή της παραπάνω συχνότητας εφαρμόζεται διακριτός μετασχηματισμός Fourier.
2. Με τη βοήθεια των ειδικών παραμέτρων που καθορίζουν τα χαρακτηριστικά του οπτικού συστήματος του ανθρώπου γίνεται ανίχνευσης της λειότητας ή των ακμών της εικόνας. Οι παράμετροι αυτοί συνδυάζονται με τα αποτελέσματα του διακριτού μετασχηματισμού ώστε να συνδυασθούν. Έχει παρατηρηθεί πως όσο δεν υπάρχει η παρουσία των 0 στους κβαντισμένου συντελεστές Fourier για μία συγκεκριμένη περιοχή του σήματος τόσο αυξάνει και η ομαλότητα της εικόνας.

Ο έλεγχος αυτός που πραγματοποιείται με τη βοήθεια των συντελεστών καταδεικνύει σε ποιες περιοχές του σήματος υπάρχει ομαλότητα καταγράφοντας τους μη μηδενικούς κβαντισμένους συντελεστές σ' έναν πίνακα Qm.

Ομοίως γίνεται και ο έλεγχος των χαρακτηριστικών των ακμών μόνο που αυτοί περιλαμβάνουν περισσότερους συντελεστές. Οι μικρότεροι κβαντισμένοι συντελεστές DFT που αντιστοιχίζονται στις ακμές είναι οι απόλυτες τιμές 1,2,8, 9, 10, 16, 17. Υψηλές τιμές αυτών των παραμέτρων δείχνουν και την ύπαρξη ακμών στο συγκεκριμένο μπλοκ.

Τελικά ο καθορισμός του επιπέδου που καθορίζει την ανοχή του σήματος ενάντια στις παραμορφώσεις λόγω της ένθεσης του υδατογραφήματος υπολογίζεται ως εξής:

Επίπεδο = κλίμακα λειότητας + λειότητα + κλίμακα ακμών + ακμές + μετατόπιση.



Εικόνα 29 **Ένθεση με MPEO Υδατογράφηση στο συχνοτικό πεδίο**

Η παράμετρος της μετατόπισης απαιτείται ώστε να υπάρξει μία δυναμική βάση για το υδατογράφημα. Τα χαρακτηριστικά του μπλοκ ζυγίζονται από τις παραμέτρους κλίμακα λειότητας και κλίμακα ακμών που υπολογίζονται ως εξής:

Κλίμακα λειότητας = -10, κλίμακα ακμών = 0,27 και μετατόπιση = 50.

Το επίπεδο έχει κυμαίνεται από έως 50.

Αν το επίπεδο > 50 επίπεδο = 50

Αν το επίπεδο < 0 επίπεδο = 0

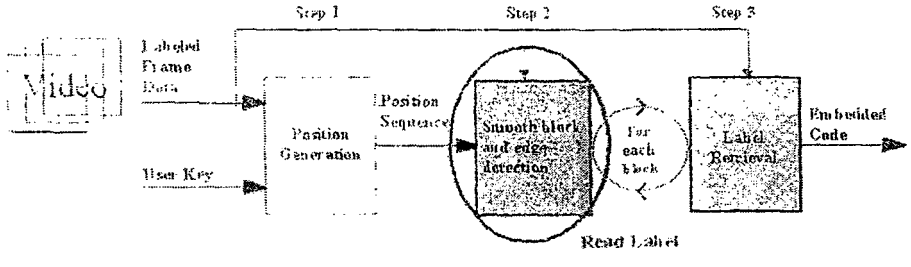
Πριν την εισαγωγή του υδατογραφήματος ένα διάδικο ψηφίο προστίθεται για τη διόρθωση λαθών.

3. Όπως και στον αλγόριθμο Zhoa-Koch η δυαδική τιμή του υδατογραφήματος και επιλέγοντας 3 συντελεστές του μετασχηματισμού DFT xl, χ2, χ3 και όπως φαίνεται στον πίνακα αν θέλω να αλλάξω μία τιμή αλλάζω και τους συντελεστές χ1, χ2, χ3.

5.4.3.2 Η ανίχνευση Υδατογραφήματος

Τα πρώτα δύο στάδια στη διαδικασία της ανίχνευσης υδατογραφήματος είναι ίδια με εκείνης της ένθεσης. Στο τρίτο στάδιο οι περιοχές που ενθέτονται τα δεδομένα εντοπίζονται με τη βοήθεια του κλειδιού. Η λειτουργία του πίνακα που φαίνεται

παραπάνω σε συνδυασμό με τους τρεις παράγοντες επιτυγχάνει την αποκωδικοποίηση του υδατογραφημένου προϊόντος.



Εικόνα 30 Ανίχνευση MPEG Υδατογράφηση στο συχνοτικό πεδίο

5.4.3.3 Συμπεράσματα

Η τεχνική της MPEG υδατογράφησης video στο συχνοτικό πεδίο[95] επιτρέπει τόσο τη γρήγορη κωδικοποίηση και την αποκωδικοποίηση του προϊόντος. Επιπλέον ένα από τα βασικότερα πλεονεκτήματα της μεθόδου είναι ότι το MPEG υδατογράφημα είναι συμβατό με αρκετές μορφές επεξεργασίας όπως εκτύπωση ή επανασάρωση. Ταυτόχρονα ελάχιστη παραμόρφωση εισέρχεται στο video. Όμως η τεχνική αυτή ενισχύει σε μικρό βαθμό την αλλοίωση λόγο των γεωμετρικών αλλαγών που εισάγει όπως αλλαγή μεγέθους της εικόνας, η περιστροφή και η μετατόπιση της εικόνας. Γενικώς η τεχνική αυτή είναι αποτελεσματική όσο οι άλλες μέθοδοι υδατογράφησης, ενώ ταυτόχρονα παρέχει ενισχυμένη ανθεκτικότητα σ' ένα μεγάλο αριθμό μετασχηματισμών που μπορούν να υποστούν τα υδατογραφημένα video.

5.4.4. MPEG Υδατογράφημα στο χωρικό επίπεδο [22]

Η τεχνική αυτή τροποποιεί αρκετά τη μέθοδο του Fridrich ώστε να αποφευχθούν τα μειονεκτήματα της. Η ανίχνευση του υδατογραφήματος δεν απαιτεί το αρχικό βίντεο ενώ ταυτόχρονα η ένθεση του υδατογραφήματος πραγματοποιείται σε κάθε καρέ, ώστε η αλλοίωση ή η αφαίρεση του υδατογραφήματος να αποτρέπεται.

Διαδικασία ένθεσης

Αρχικά χρησιμοποιείται ο Zhao-Koch αλγόριθμος για να προσδιορισθούν τα μπλοκ που θα υποστούν τροποποίηση λόγω της υδατογράφησης. Στη συνέχεια δημιουργείται ένα 8x8 τυχαίο πρότυπο με ένα ψευδοτυχαίο κλειδί. Για την αποφυγή των υψηλών συχνοτήτων σ' αυτό το πρότυπο χρησιμοποιείται ένα αυτόματο με κανόνες απόφασης. Οι κανόνες που χρησιμοποιεί το πρότυπο ελέγχουν τον αριθμό των άσσων που έχουν οι γειτονικές θέσεις και αν αυτός είναι μεγαλύτερος του 5 θέτουν το διάδικο ψηφίο ίσο με 1, ενώ αν είναι μικρότερος του 3 το θέτει ίσο με 0. Εφαρμόζοντας τους κανόνες απόφασης αυτού του πεπερασμένου αυτόματου τις περισότερες φορές επιτυγχάνεται η δημιουργία ενός προτύπου M με χαμηλές συχνότητες. Τέλος η συσχέτιση μεταξύ του προτύπου M και της φωτεινότητας του block εφαρμόζεται ανάλογα με το διάδικο ψηφίο που εντίθεται κάθε φορά.

Διαδικασία ανίχνευσης

Στη διαδικασία ανίχνευσης η παραγωγή του προτύπου M με τη βοήθεια του αυτόματου απαιτείται επίσης. Ταυτόχρονα χρησιμοποιούνται και οι ίδιοι κανόνες

απόφασης. Για να μπορέσει να γίνει ο έλεγχος της συσχέτισης μεταξύ του 8x8 προτύπου και της φωτεινότητας υπολογίζεται ο μέσος όρος φωτεινότητας avl για τη θέση που αντιστοιχεί στο 1 και ο μέσος όρος φωτεινότητας avO για τη θέση που αντιστοιχεί στο 0 στο πρότυπο Μ.

Η ανίχνευση γίνεται με τη χρήση των παρακάτω τύπων. Αν avl>0 τότε το διάδικο ψηφίο θέτεται ίσο με 1 αλλιώς ίσο με 0. Μ' αυτό τον τρόπο παράγεται η κωδικοποιημένη λέξη με την BHC κωδικοποίηση ώστε να δημιουργηθεί η κωδικοποιημένη πληροφορία υδατογράφησης. Αν αυτή συμπίπτει με την πραγματική τότε το υδατογράφημα υπάρχει στο υδατογραφημένο video ειδάλλως απορρίπτεται.

Το υδατογράφημένο προϊόν μιας και ενθέτει υδατογραφημένη πληροφορία σε κάθε καρέ προσφέρει αξιόπιστη ασφάλεια μιας και το υδατογράφημα είναι πραγματικά δύσκολο να αφαιρεθεί ακόμα κι αν απομακρυνθούν κάποια καρέ από το video. Ταυτόχρονα η μη απαίτηση του αρχικού σήματος κάνει τη διαδικασία ανίχνευσης πιο εύκολη δίνει παράλληλα τη δυνατότητα να εισαχθεί στο υδατογράφημα κωδική πληροφορία του ιδιοκτήτη.

5. 5 Αποτελέσματα

Η υδατογράφηση σε video ασχολείται με ένα αρκετά περίπλοκο πεδίο των ψηφιακών σημάτων. Παρόλ' αυτά χρησιμοποιώντας τους παράγοντες του οπτικοακουστικού ανθρώπινου συστήματος και τα ειδικά χαρακτηριστικά του video επιτυγχάνει ικανοποιητικά αποτελέσματα.

Ο Zhoa-Koch [17] αλγόριθμος με τη βοήθεια της διόρθωσης λαθών ανταποκρίνεται στην MPEG συμπίεση. Η ποιότητα των καρέ που τροποποιούνται απο την επίθεση αυτή, μπορεί να βελτιωθεί. Επίσης η προσέγγιση του Fridrich [32]αλγορίθμου είναι δυνατόν να ενθέσει περισσότερη πληροφορία και επιτυγχάνει την ανίχνευση του υδατογραφήματος χωρίς το αρχικό σήμα.

Ανάλογα με τις ανάγκες και τις απαιτήσεις του προς υδατογράφησης προϊόντος επιλέγεται και η κατάλληλη μέθοδος υδατογράφησης, ώστε να ενισχυθούν οι παράγοντες που αξιολογούνται σαν ουσιώδεις.

6

ΥΔΑΤΟΓΡΑΦΗΣΗ ΣΕ ΕΙΚΟΝΑ

6.1 Ειδικές συνθήκες συην υδατογράφηση εικόνας

Η υδατογράφηση σε εικόνα παρουσιάζει αρκετό ενδιαφέρον κυρίως λόγο των ιδιοτήτων του συστήματος όρασης του ανθρώπου. Οι εικόνες προσφέρουν ένα αρκετά μικρό αρχικό σήμα στο οποίο μπορούμε να ενθέσουμε δεδομένα. Μια εικόνα 200x200 εικονοστοιχίων, κωδικοποιημένη σε 8 bit, παρέχει περίπου 40KB δεδομένων τα οποία μπορούμε να επεξεργαστούμε. Επίσης οι εικόνες επιδέχονται μια σειρά από μορφές επεξεργασίας που ποικίλουν από απλές γραμμικές επεξεργασίες, ως πολύπλοκες μη γραμμικές όπως cropping, θόλωμα, φιλτράρισμα, και συμπίεση με απώλεια δεδομένων [94]. Το υδατογράφημα θα πρέπει να είναι ανθεκτικό σε όλες αυτές τις επεξεργασίες.

Παρά τις παραπάνω προκλήσεις, οι εικόνες είναι πιθανοί δέκτες για υδατογραφήματά. Υπάρχουν πολλά χαρακτηριστικά στο οπτικό σύστημα μας που επιδέχονται εκμετάλλευσης. Για το σκοπό αυτό, ένα από αυτά είναι η διαφορετική ευαισθησία στην αντίθεση της εικόνας ως συνάρτηση της χωρικής συχνότητας και του φαινόμενου συγκάλυψης των ακρών (και στην φωτεινότητα και στη χρωματικότητα). Το οπτικό σύστημα του ανθρώπου έχει μικρή ευαισθησία στις αλλαγές της φωτεινότητας (λιγότερο από ένα μέρος στα 30 τυχαία δείγματα. Στις ομοιόμορφες εικόνες αυτή η ευαισθησία αλλάζει και φτάνει στο ένα μέρος στα 240. Οι τυπικές οθόνες και οι εκτυπωτές επίσης έχουν μικρό δυναμικό πεδίο. Σε μια εικόνα των 8 bit υπάρχει χώρος να κρύψουμε δεδομένα σε μέρη ψευδοτυχαίων αλλαγών στη φωτεινότητα. Ένα ακόμα χαρακτηριστικό προς εκμετάλλευση του οπτικού συστήματος είναι η χαμηλή

ευαισθησία στις χαμηλές χωρικές συχνότητες, όπως π.χ. η ομοιόμορφη αλλαγή της φωτεινότητας μιας εικόνας. Τέλος ένα επιπλέον χαρακτηριστικό είναι ότι στις ψηφιακές εικόνες μια τεχνική απόκρυψης δεδομένων μπορεί να έχει πρόσβαση σε οποιοδήποτε εικονοστοιχείο ή μια σειρά από εικοστοιχεία.

6.2 Τεχνικές

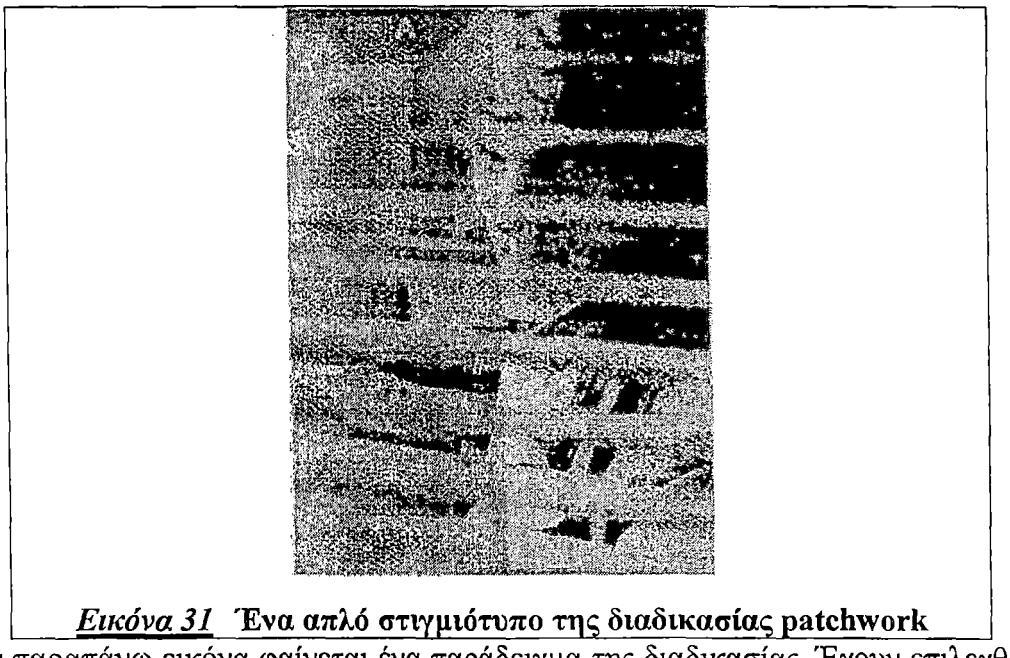
Σύμφωνα με αυτές τις παρατηρήσεις αναπτύχθηκαν διάφορες μέθοδοι υδατογράφησης σε εικόνες. Κάποιες από αυτές εφαρμόζονται για υδατογράφηση ενώ κάποιες άλλες για ένθεση μεγάλου μεγέθους υδατογραφημάτων, όπως μια εικόνα-υδατογράφημα. Κάποιες είναι ανθεκτικές σε γραμμικές μορφοποιήσεις της εικόνας ενώ κάποιες άλλες είναι περισσότερο ανθεκτικές σε μη γραμμικές μορφοποιήσεις όπως το φιλτράρισμα.

6.2.1 Μικρού ρυθμού απόκρυψη δεδομένων [21]

Στην υδατογράφηση χαμηλού ρυθμού ένθεσης δεδομένων, περιμένουμε υδατογραφήματα με αυξημένη ανθεκτικότητα αλλά λίγο εύρος. Η έμφαση δίνεται στην αντίσταση του υδατογραφήματος σε απόπειρες αφαίρεσης του από τρίτους. Παρακάτω θα αναλύσουμε τεχνικές, στατιστικές και διαισθητικές όπως την μέθοδο συρραφής (Patchwork) και την μέθοδο κωδικοποίησης της υφής (texture block coding) της εικόνας.

6.2.1.1 Συρραφή (Patchwork) [17], [1]

Η τεχνική στατιστικής προσέγγισης την οποία ονομάζουμε συρραφή, βασίζεται σε μια ψευδοτυχαία στατιστική διαδικασία. Η τεχνική αυτή ενθέτει αόρατα συγκεκριμένη στατιστική πληροφορία την οποία θα ονομάζουμε μπάλωμα (patch) στην αρχική εικόνα . Το μπάλωμα έχει Gaussian κατανομή.



Εικόνα 31 **Ένα απλό στιγμιότυπο της διαδικασίας patchwork**

Στην παραπάνω εικόνα φαίνεται ένα παράδειγμα της διαδικασίας. Έχουν επιλεχθεί να εντεθούν δύο μπαλώματα. Το Α μπάλωμα, του οποίου τα περιεχόμενα έχουν φωτιστεί και το Β του οποίου τα περιεχόμενα έχουν σκοτιστεί (για τους σκοπούς του παραδείγματος αυτό έχει γίνει σε υπερβολικό βαθμό).

Η μοναδική στατιστική πληροφορία που παράγεται σαν αποτέλεσμα της διαδικασίας αυτής είναι αυτό που σηματοδοτεί την ύπαρξη ή όχι του υδατογραφήματος. Η συρραφή είναι ανεξάρτητη από τα περιεχόμενα της αρχικής εικόνας και γι αυτό είναι

και ανθεκτικό σε πολλούς μη γραμμικούς μετασχηματισμούς της εικόνας όπως είναι το φιλτράρισμα.

Για την παρακάτω ανάλυση πρέπει πρώτα να κάνουμε τις εξής μη περιορίστηκες παραδοχές. Δουλεύουμε σε σύστημα 256 βαθμίδων ξεκινώντας από το 0, όλα τα επίπεδα φωτεινότητας είναι ισοπίθανα και όλα τα δείγματα είναι ανεξάρτητα μεταξύ τους.

Διαδικασία Ενθεσης

Ο αλγόριθμος της συρραφής είναι ο ακόλουθος. Παίρνουμε δύο τυχαία σημεία στην εικόνα Α και Β. Έστω α η φωτεινότητα του σημείου Α και β η φωτεινότητα του σημείου Β αντίστοιχα. Έστω επίσης

$$S=a-b$$

Η μέση τιμή του S μετά την συνεχή επανάληψη της διαδικασίας αυτής αναμένεται να είναι 0. Βέβαια αυτό δεν δείχνει την ακριβή τιμή του S για μια συγκεκριμένη επανάληψη. Αυτό συμβαίνει λόγο της μεγάλης διασποράς σ του S. Η διασπορά μπορεί να υπολογισθεί όπως παρακάτω [Drake] κάνοντας πρώτα την διαπίστωση ότι τα α και β είναι ανεξάρτητα μεταξύ τους.

$$a_s^2 = Ja^2 + o_b^2$$

όπου το Q_a για S ομοιόμορφης κατανομής είναι

$$\sigma^2 \ll 5418$$

$$2 \quad 2$$

Τώρα, $(J_a$ — $(J$ η λόγο του ότι τα α και β είναι δείγματα από το ίδιο σετ.

Άρα :

$$\sigma^2 = 2\chi\sigma^2 = 2\chi^{(255\ o)2}. 10836$$

από το οποίο βγάζουμε μια σταθερή διασπορά σ§=104. Αυτό σημαίνει ότι με πιθανότητα περισσότερη του 0.5, το S θα έχει τιμή μεγαλύτερη του 43 ή μικρότερη του -43. Θεωρώντας μια Gaussian συγκέντρωση, μια μοναδική διασπορά δεν προσφέρει κανένα συμπέρασμα. Αυτό βέβαια μπορεί να λυθεί επαναλαμβάνοντας τη διαδικασία πολλές φορές.

Έστω ότι κάνουμε ν επαναλήψεις και ότι at και βι οι τιμές των α και β στην ιοστή επανάληψη, S;. Τότε το Sn ορίζεται ως εξής:

Η αναμενόμενη τιμή του Sn είναι: Τώρα η διασπορά είναι:

$$S_n = \overset{n}{\underset{M}{YS.}} = \overset{n}{\underset{i=1}{Ya-b_i}}$$

Η αναμενόμενη τιμή του Sn είναι:
Τώρα η διασπορά είναι:

$$a_{Sn} = nx_a^2{}_s$$

και η σταθερή απόκλιση είναι:

$$Q- \quad = 4nxa \ \ll v \ll x104$$

Τώρα μπορούμε να υπολογίσουμε το SJOOOO Υια μια εικόνα, και αν απέχει κατά περισσότερο από μερικές σταθερές απόκλισης τότε ήμαστε αρκετά σίγουροι ότι υπάρχει κωδικοποίηση γιατί όπως θα δείξουμε και παρακάτω, για μεγάλα n το Sn' έχει Gaussian κατανομή.

Διαδικασία Ανίχνευσης

Η μέθοδος συρραφής μετατρέπει τεχνητά το S για μια εικόνα, έτσι ώστε το Sn' να είναι αρκετές σταθερές απόκλισης μακριά. Για να αποκωδικοποιήσουμε μια εικόνα κάνουμε τα εξής :

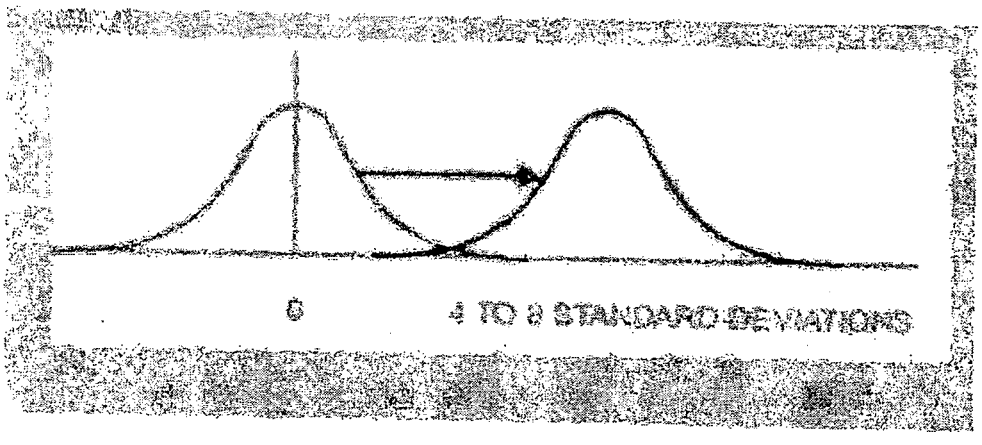
Χρησιμοποιούμε ένα κλειδί από γνωστή γεννήτρια ψευδοτυχαίων αριθμών για να διαλέξουμε τα α, και β,. Αυτό είναι σημαντικό γιατί πρέπει ο αποκωδικοποίητης να επισκεφτεί τα ίδια σημεία κατά την αποκωδικοποίηση

Ανεβάζουμε την φωτεινότητα του σημείου α κατά ένα αριθμό δ ο οποίος είναι συνήθως 1-5 θέσεις. Κατεβάζουμε τη φωτεινότητα του σημείου β κατά τον ίδιο αριθμό δ. Επαναλαμβάνουμε τη διαδικασία για η=10000 συνήθως Τώρα το αποκωδικοποιημένο Sn' θα είναι

£=2δ.+2>.-*.>

Για κάθε βήμα προσθέτουμε την τιμή 26. Έτσι μετά από ν επαναλήψεις περιμένουμε το Sn' να είναι ίσο με :

$$S'n = — * 0.028\delta\, Jn$$



Εικόνα 32 **Όσο το δ ή το η αυξάνεται, η κατανομή του S'n μετακινείται προς τα δεξιά**

Ενισχυτικές Τεχνικές

Όσο το δ ή το n αυξάνεται, η κατανομή του Sn' μετακινείται προς τα δεξιά. Αν το μετακινήσουμε αρκετά τότε ένα σημείο που βρίσκεται στη μια κατανομή, είναι απίθανο να βρίσκεται και στο κέντρο της άλλης.

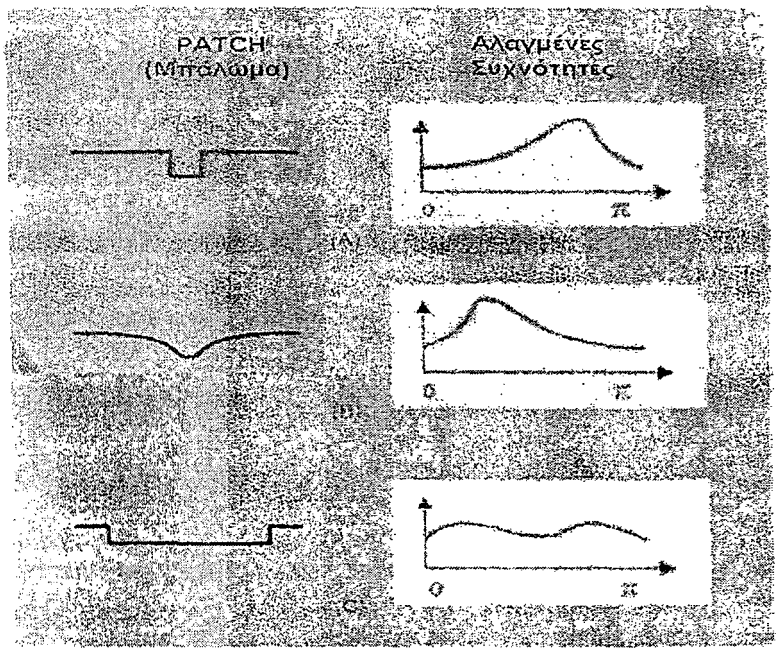
Αν και οι ήδη υπάρχοντες μέθοδοι είναι ικανοποιητικές, έχουμε φτιάξει και μία σειρά από βελτιώσεις.

4. Χρήση μπαλωμάτων από ομάδες εικονοστοιχείων αντί του ενός. Αυτό έχει σαν αποτέλεσμα να μετατοπίζει το θόρυβο της μεθόδου σε χαμηλότερο συχνοτικό φάσμα έτσι ώστε να είναι δυσκολότερο να αφαιρεθεί από συμπίεση με αφαίρεση δεδομένων ή από απλά πεπερασμένα φίλτρα.

5. Κάνοντας την τεχνική συρραφής πιο ανθεκτική με το να χρησιμοποιούμε συναφή κωδικοποίηση ή κάποιο ευρηματικό χαρακτιριστικό βασισμένο στην αναγνώριση χαρακτηριστικών. Η αποκωδικοποίηση της συρραφής είναι ευαίσθητη σε συσχετιστικές μορφοποιήσεις όπως περιστροφή και κλιμάκωση.
6. Χρησιμοποιώντας το χαρακτηριστικό ότι η τεχνική της συρραφής είναι ιδιαίτερα ανθεκτική στο cropping[49]. Μην έχοντας τα σημεία έξω από την εικόνα, η τεχνική της συρραφής μειώνεται ως προς την ακρίβεια της λογαριθμικά σε σχέση με τη μείωση της εικόνας. Η τεχνική της συραφής συρραφή είναι επίσης ανθεκτική και στο gamma correction γιατί οι σχετικές αποστάσεις της φωτεινότητας παραμένουν ίδιες.

Αποτελέσματα Διαπιστώσεις

Μορφή μπαλώματος

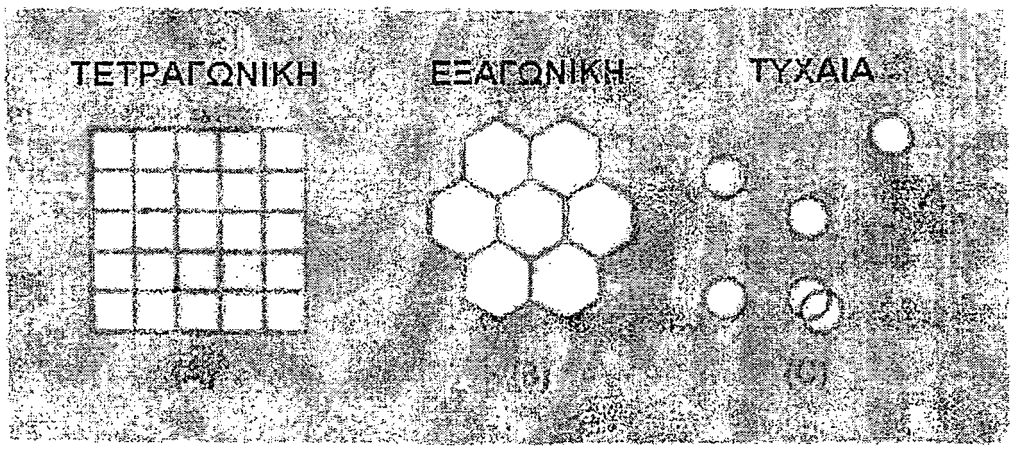


Εικόνα 33 **Το περίγρομα του κομματιού καθορίζει ποιες συχνότητες πρέπει να αλαχθούν κατά τη διαδικασία Patchwork**

Η παραπάνω εικόνα δείχνει τρεις πιθανές μονοδιάστατες μορφές μπαλώματος, και δίπλα φαίνεται μια εκτίμηση του φάσματος το πως θα φαίνεται μια γραμμή με αυτά τα μπαλώματα. Στην εικόνα 33Α το μπάλωμα που χρησιμοποιούμε είναι μικρό, με μυτερές γωνίες. Αυτό προκαλεί την πλειονότητα της ενέργειας του μπαλώματος να μαζεύεται στις υψηλές συχνότητες κάνοντας δυσκολότερο το να εντοπιστεί αλλά και ευκολότερο να αφαιρεθεί από συμπίεση με αφαίρεση δεδομένων. Από την άλλη μεριά, στην εικόνα 33Β η ενέργεια συγκεντρώνεται στις χαμηλές συχνότητες. Στην εικόνα 33C ένα ευρύ με μυτερές γωνίες μπάλωμα, κάνει την ενέργεια να μοιρασθεί ομοιόμορφα στο φάσμα συχνοτήτων της εικόνας.

Η επιλογή του μπαλώματος εξαρτάται από τις αναμενόμενες μεταβολές της εικόνας. Αν είναι πιθανή μια JPEG κωδικοποίηση, τότε επιλέγουμε ένα μπάλωμα που έχει την ενέργεια του στις χαμηλές συχνότητες. Αν είναι πιθανή μια αύξηση της αντίθεσης τότε επιλέγουμε ένα μπάλωμα υψηλών συχνοτήτων. Σε περίπτωση που δεν ξέρουμε τις πιθανές μορφοποιήσεις της εικόνας, τότε επιλέγουμε μπάλωμα με διασπαρμένη την

ενέργεια του.



Εικόνα 34 **Η τοποθέτηση του κομματιού επιρεάζει την εμφάνιση του**

Η συσχέτιση και ο συνδυασμός των μπαλωμάτων σχετίζεται με την ορατότητα των μπαλωμάτων. Η πιο απλή μορφή φαίνεται στην εικόνα μιας απλής γραφικά τετραγωνικής μορφής που μπορεί να αποτελεί μία εύκολη λύση όμως αν ο αριθμός των μπαλωμάτων n αυξάνει δεν αποτελεί σοφή λύση. Μιας και η αύξηση του n προκαλεί πιο έντονες ακμές στις οποίες το ανθρώπινο οπτικό σύστημα έχει ευαισθησία σ' αυτές. Μία δεύτερη επιλογή σπάει τη συμμετρία χρησιμοποιώντας εξάγωνο για την υλοποίηση του σχήματος των μπαλωμάτων. Μ' αυτό τον τρόπο εξασθενείτε αρκετά το πρόβλημα της προηγούμενης περίπτωσης. Η επιλογή που προτιμάται όμως είναι η τυχαία τοποθέτηση των μπαλωμάτων. Η σωστή επιλογή του σχήματος του μπαλώματος βοηθάει αρκετά τη μέθοδο συρραφής να επιφέρει ικανοποιητικά ποιοτικά αποτελέσματα.

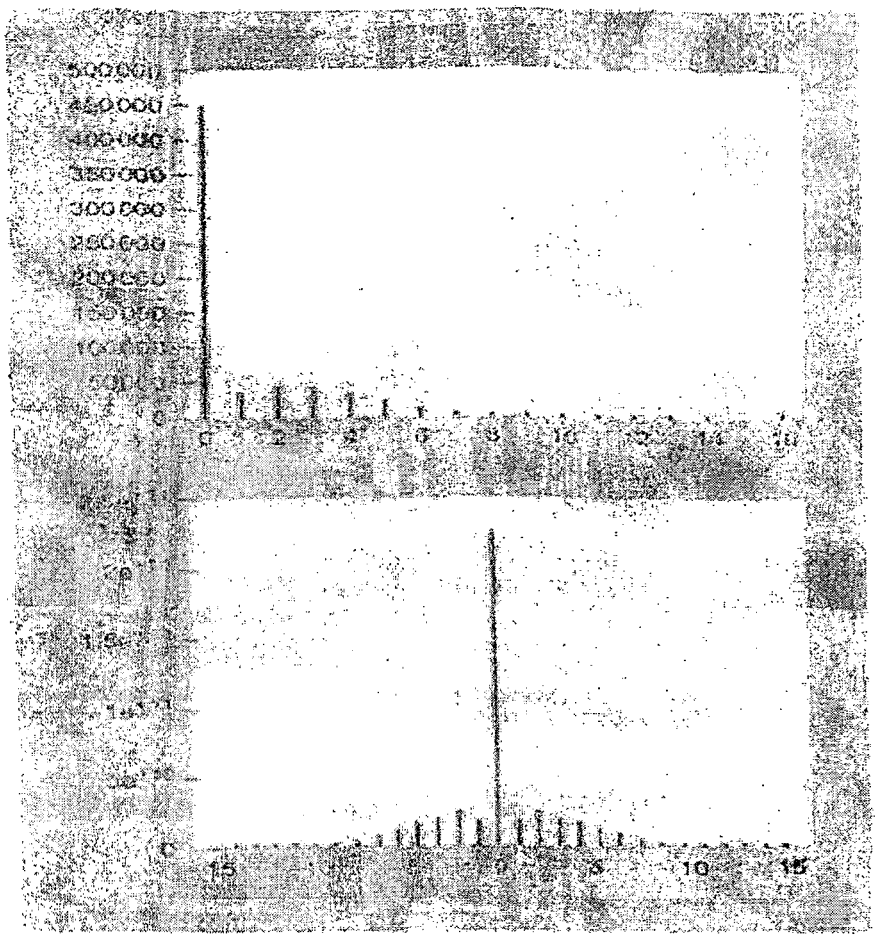
Ομοιομορφία

Μία απλοϊκή παραδοχή ενός ομοιόμορφου ιστογράμματος φωτεινότητας έχει γίνει παραπάνω. Στη τεχνική της συρραφής όμως, η μόνη παραδοχή που κάνουμε είναι ότι η αναμενόμενη τιμή του Si είναι μηδέν.

Μπορεί να δειχθεί ότι η παραδοχή αυτή ισχύει πάντα: Έστω ar είναι η χρονική αντεστραμμένη σειρά των a:

Θεωρούμαι Ar=A* (A* μιγαδικός συζυγής)

Εφαρμογή του F(a*ar)=A A* (F=Fourier) A A* πραγματικός F"*(A A*) ρητός από τον ορισμό Οι Ρητές σειρές είναι συμμετρικές στο μηδέν

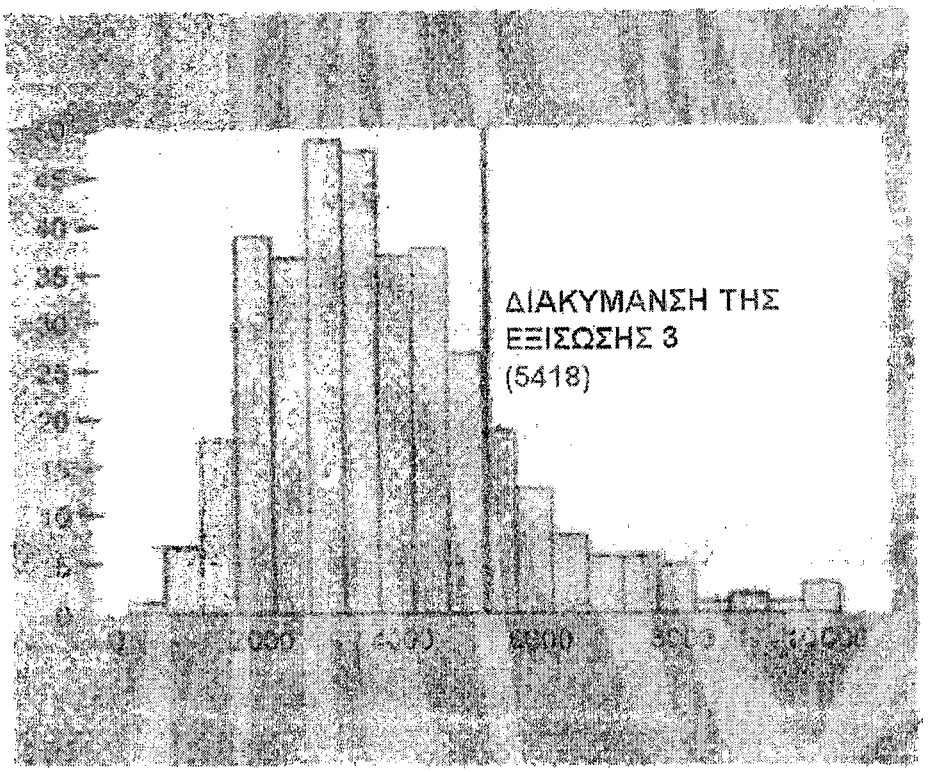


Εικόνα 35 **Ιστόγραμμα του σχήματος 2 και η αυτοσυσχέτησή του**

Στην παραπάνω εικόνα επάνω φαίνεται το ιστόγραμμα μιας εικόνας που είναι τυχαίας κατανομής. Κάτω φαίνεται το αποτέλεσμα παίρνοντας το μιγαδικό συζυγή το οποίο είναι συμμετρικό γύρω από το μηδέν.

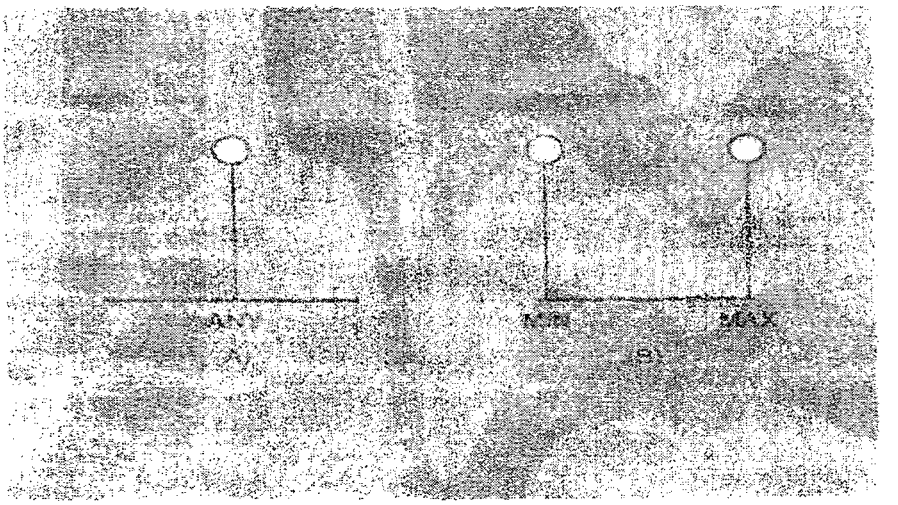
Διασπορά

Ψάχνοντας μεγάλο αριθμό από εικόνες, είναι θεμιτό να υπάρχει μία εκτίμηση της διασποράς έτσι ώστε μόνο οι ύποπτες εικόνες να εξετάζονται διεξοδικά.



Εικόνα 36 **Ιστόγραμμα της διακύμανσης της φωτεινότητας απο 365 φωτογραφίες**

Εξετάζοντας πειραματικά ένα αριθμό από φωτογραφίες βρίσκουμε μία μέση τιμή διασποράς 3877.4. Η κατανομή φαίνεται στην εικόνα 36. Έτσι η εκτίμηση που βγαίνει από την παραδοχή της ομοιομορφίας και είναι 5418 είναι μία λογική τιμή που μπορούμε να χρησιμοποιήσουμε για μία μέση εικόνα.



Εικόνα 37 **Ιστογράμματα φωτογραφιών με ελάχιστη (Α) και μέγιστη (Β) διακύμανση**

Όπως φαίνεται στην εικόνα 37, η ελάχιστη τιμή είναι μηδέν. Η μέγιστη τιμή είναι αυτή μιας δίχρωμης εικόνας, η μισή μαύρη και η μίση άσπρη και είναι 16256. Άρα η

εκτίμηση της αναμενόμενης διασποράς που θα κάνουμε, βρίσκεται σε αυτά τα όρια. Για μία όμως εικόνα, η εκτίμηση της διασποράς είναι λεπτό θέμα γιατί η τεχνική της συρραφής αυξάνει ελάχιστα αυτή την τιμή. Αυτό εξαρτάται από πολλούς παράγοντες όπως το μέγεθος και το βάθος του μπαλώματος, τον αριθμό των μπαλωμάτων και το αρχικό ιστόγραμμα της εικόνας. Πάντως η τιμή μιας μέσης εικόνας που αναφέραμε πιο πάνω είναι μία καλή επιλογή.

Συμπεράσματα

Υπάρχουν ορισμένοι περιορισμοί στη μέθοδο συρραφής. Ο πρώτος είναι ότι η συρραφή μπορεί να κρύψει αποδοτικά πολύ μικρό αριθμό δεδομένων, πράγμα που την κάνει μη αποδοτική για υδατογράφημα. Ο δεύτερος είναι ότι πρέπει να καταχωρείς τη θέση των εικονοστοιχείων στην εικόνα. Επίσης είναι ακόμα δύσκολο να αποκωδικοποιηθεί εικόνα που υπέστη σοβαρούς συσχετιστικούς μετασχηματισμούς. Βέβαια χωρίς το απαραίτητο κλειδί για την ψευδοτυχαία γεννήτρια είναι αδύνατο να αφαιρεθεί το μπάλωμα χωρίς να αλλοιωθεί η εικόνα πέραν κάθε αναγνώρισης.

Η μέθοδος συρραφής υπόκειται σε επιθέσει κρυπτογραφίας αν χρησιμοποιηθεί για να κωδικοποιήσει μεγάλο αριθμό εικόνων με το ίδιο κλειδί. Αν οι εικόνες συνενωθούν και βγει ο μέσος όρος τους, τα μπαλώματα φαίνονται σα φωτεινές ή σκοτεινές περιοχές. Έτσι είναι εύκολο να σπάσει η μέθοδος. Αυτό μπορεί να αποφευχθεί είτε χρησιμοποιώντας δύο κλειδιά είτε χρησιμοποιώντας διάφορες ψευδοτυχαίες μορφές για τα μπαλώματα. Ακόμα και η χρησιμοποίηση δύο κλειδιών αυξάνοντας το χρόνο κωδικοποίησης αυξάνει κατά πολύ την ανθεκτικότητα του υδατογραφήματος σε τέτοιες επιθέσεις.

6.2.1.2 Κωδικοποίηση Μπλοκ Υφών (Texture Block Coding) [5], [1]

Μία δεύτερη μέθοδος χαμηλού ρυθμού είναι η κωδικοποίηση υφής. Αυτή η μέθοδος κρύβει δεδομένα μέσα σε συνεχή πρότυπα υφής της εικόνας. Παίρνει δηλαδή ένα πρότυπο (pattern) υφής από ένα μέρος της εικόνας και το αντιγράφει σε άλλο μέρος που έχει παρόμοιο πρότυπο. Έτσι σαν αποτέλεσμα έχουμε δύο περιοχές με πανομοιότυπη υφή. Οι περιοχές αυτές μπορούν να ανιχνευθούν ως εξής:

1. Αυτοσυσχετίζουμε την εικόνα με τον εαυτό της. Έτσι θα παραχθούν αιχμές στις περιοχές που είναι πανομοιότυπες.
2. Μετατοπίζουμε την εικόνα σύμφωνα με τις αιχμές του βήματος 1 και αφαιρούμε την εικόνα από το μετατοπισμένο αντίγραφο γεμίζοντας τις άκρες με μηδενικά όπου χρειάζεται
3. Τετραγωνίζουμε το αποτέλεσμα και θέτουμε ένα κατώφλι για να πάρουμε μόνο τις τιμές κοντά στο μηδέν.

Λόγω του ότι οι δύο περιοχές είναι πανομοιότυπες μορφοποιούνται με τον ίδιο τρόπο αν η εικόνα μορφοποιηθεί ομοιόμορφα. Αν η περιοχή επιλεγεί αρκετά μεγάλη, το εσωτερικό μέρος αλλάζει ίδια σε ένα μεγάλο αριθμό από μη γεωμετρικές μορφοποιήσεις.

Η κωδικοποίηση υφής έχει και τα μειονεκτήματα της. Μέχρι στιγμής χρειάζεται ο ανθρώπινος παράγοντας για να επιλέξει τις περιοχές και να εκτιμήσει το τελικό αποτέλεσμα. Θα μπορούσε να χρησιμοποιηθεί αυτοματοποιημένος τρόπος για να εκτιμηθούν οι περιοχές αλλά η αποδοτικότητα του θα είναι χαμηλή αν η εικόνα δεν έχει μεγάλες ομοιόμορφες περιοχές.

Εικόνα 38 **Παράδειγμα κωδικοποίησης κομματιού υφής (texture block coding)**

Παραπέρα μελέτες γίνονται για τη δυνατότητα αποκοπής και αντιγραφής περιοχής της εικόνας μόνο από ένα συγκεκριμένο φάσμα συχνοτήτων. Αυτό θα είχε σαν αποτέλεσμα πολύ περισσότερη ανθεκτικότητα και θα έκανε λιγότερο εμφανή την αλλαγή.

6.2.2 Κωδικοποίηση υψηλού ρυθμού [5], [6], [1]

Μέθοδοι κωδικοποίησης υψηλού ρυθμού μπορούν να σχεδιαστούν ώστε να έχουν την ελάχιστη εμφανή διάφορα στο αρχικό σήμα. Δεν έχουν και αυτές ανοσία σε μορφοποιήσεις της εικόνας. Όμως επιτρέπουν την ένθεση μεγάλου σχετικά όγκου κρυφής πληροφορίας.

Συνήθεις τεχνικές κωδικοποίησης υψηλού ρυθμού είναι η αντικατάσταση του λιγότερου σημαντικού δυαδικού ψηφίου με την κρυφή πληροφορία. Άλλες τεχνικές είναι, η εισαγωγή υψηλής συχνότητας, χαμηλού μέτρου, θορύβου, όπως και η χρησιμοποίηση απευθείας ακολουθίας κωδικοποίησης ευρέως φάσματος.

Όλες οι μέθοδοι υψηλού ρυθμού μπορούν να γίνουν ανθεκτικότερες με τη χρησιμοποίηση διόρθωσης λαθών [67] θυσιάζοντας το ρυθμό ένθεσης. Τέτοιες μέθοδοι είναι καλές όταν πιστεύεται ότι θα υπάρχει αρκετός έλεγχος στην εικόνα. Γενικά καμία μέθοδος δεν είναι ανθεκτική σε όλα τα είδη μορφοποιήσεων. Ο συνδυασμός όμως των μεθόδων μπορεί να δρα συμπληρωματικά όσον αφορά την ανθεκτικότητα. Τέτοιοι συνδυασμοί μεθόδων είναι απαραίτητοι για την αποκωδικοποίηση μετά από μη γεωμετρικές μορφοποιήσεις όπως συσχετιστικές μορφοποιήσεις και για τη διατήρηση του συγχρονισμού στην κωδικοποίηση ευρέως φάσματος.

Κάποιες μέθοδοι, όπως η συρραφή, είναι ιδιαίτερα ευαίσθητες σε συσχετιστικές τροποποιήσεις. Γι' αυτό χρειάζεται να αναπτυχθούν τεχνικές που θα βοηθούν στην επανάκτηση των κρυφών δεδομένων μετά από τέτοιες μορφοποιήσεις. Μία τέτοια

μέθοδος είναι η συσχετισμένη κωδικοποίηση. Εκτίμηση της γεωμετρικής μορφοποίησης που υπέστη η εικόνα, μπορεί να γίνει συγκρίνοντας την αρχική με τη μορφοποιημένη εικόνα ως προς το σχήμα, το μέγεθος και τον προσανατολισμό της. Μιας και οι γεωμετρικές τροποποιήσεις είναι γραμμικές, μπορεί να γίνει αντίστροφος μετασχηματισμός [40]. Έτσι η εικόνα είναι έτοιμη για αποκωδικοποίηση.

7

ΥΔΑΤΟΓΡΑΦΗΣΗ ΣΕ ΗΧΟ

7.1.1 Εισαγωγή

Στην υδατογράφηση των αρχείων ήχου υπάρχουν κάποιες επιπλέον ιδιαίτερες συνθήκες, οι οποίες έχουν άμεση επίδραση στην ανάπτυξη των τεχνικών χαρακτηριστικών. Η μελέτη και η εκμετάλλευση αυτών των στοιχείων συμβάλλουν στην ανάπτυξη πιο αξιόπιστων μεθόδων μιας και χρησιμοποιούν τις ιδιαιτερότητες κάθε προϊόντος ώστε να αποδίδουν προϊόντα που απαντούν στις ανάγκες και απαιτήσεις που υπάρχουν.

7.1.2 Ειδικά Χαρακτηριστικά

1) Ανθρώπινο Ακουστικό Σύστημα (Human Auditory System HAS). Τα ψηφιακά αρχεία ήχου περικλείουν αρκετή ποσότητα πληροφορίας όπου ένα μεγάλο ποσοστό περικλείει κρίσιμη πληροφορία και ένα άλλο πλεονάζουσα πληροφορία. Αυτή η ιδιαιτερότητα στη μορφή των δεδομένων που περικλείονται σ' ένα ηχητικό σήμα δίνει τη δυνατότητα στα υδατογραφήματα που εντίθενται σε αρχεία ήχου να είναι ανθεκτικά στους μετασχηματισμούς.

Αν σκεφτεί κανείς πως η αλλαγή ενός ψηφιακού δεδομένου σε μία περιοχή του ηχητικού σήματος δεν μπορεί να προκαλέσει την αλλοίωση του, ο ήχος αποτελεί ένα πεδίο εφαρμογής που ανταποκρίνεται στη μέθοδο υδατογράφησης με τρόπο που αποφέρει ένα πλήθος από δυνατότητες. Η ανθεκτικότητα του υδατογραφημένου σήματος σε ένα πλήθος από επεξεργασίες σχετίζεται άμεσα και με το μέγεθος του υδατογραφήματος που ενθέτεται στο υδατογραφημένο προϊόν. Σ' αυτό το σημείο βρίσκεται ένα αξιοσημείωτο χαρακτηριστικό των αρχείων ήχου, μιας και η αλλαγή ενός μεγάλου αριθμού από τα δεδομένα του μπορεί να έχει σαν αποτέλεσμα τη μη αντιληπτή διαφορά από τα αρχικό προϊόν.

Τα παραπάνω χαρακτηριστικά αποτελούν μία πρόκληση για τους ερευνητές που εφαρμόζουν υδατογράφηση σε ήχου μιας και η φύση του προϊόντος διευρύνει τον ορίζοντα των δυνατών ενεργειών και το αποτέλεσμα ανταποκρίνεται στους στόχους για βέλτιστη υδατογράφηση. Η ευρύτητα που προσφέρει ο ήχος στην επεξεργασία του προωθεί από τη μία την ανάπτυξη πιο ευφυών και τεχνολογικά άρτιων τεχνικών αλλά από την άλλη, αυτή η ευκολία κεντρίζει το ενδιαφέρον και των κακόβουλων χρηστών. Οι πειρατές οικειοποιούνται πολλές από τις δυνατότητες των ηχητικών προϊόντων για πιο εξειδικευμένη και επίμονη επεξεργασία. Οι μορφοποιήσεις και οι αλλαγές που επιδέχεται ένα προϊόν δεν αποτελεί καθολικά θετικό παράγοντα για μια μέθοδο προστασίας δεδομένων, αλλά πρέπει να διατηρείται ένα όριο όπου από τη μία να διατηρεί την ευχρηστία και την εφαρμογή τεχνικών ενώ από την άλλη να αποτρέπει τις κακόβουλες μορφοποιήσεις. Το κρίσιμο αυτό σημείο απαντιέται σε κάθε τεχνική με διαφορετικό τρόπο.

Ο ήχος προσφέρει εκείνες τις προϋποθέσεις ώστε να ανταποκρίνεται ακόμη και στις πιο εξειδικευμένες και ιδιαίτερες υλοποιήσεις υδατογράφησης, γεγονός που αποτελεί έναν παράγοντα που αν αξιοποιηθεί σωστά δίνει ευφυή υδατογραφήματα. Άν υπάρξει η κατάλληλη δρομολόγηση πρόβλεψης εκείνων των ενεργειών (attacks) που δεν είναι επιθυμητές να αποτρέπονται τότε τα υδατογραφήματα του ήχου μπορεί να είναι ανθεκτικά προς αυτές.

Εξάλλου τα χαρακτηριστικά σχετίζονται άμεσα με τις τεχνικές υδατογράφησης και μπορούν να αποδώσουν σ' αυτές πολύτιμα χαρακτηριστικά αλλά εξίσου σχηματικός είναι και ο ρόλος της ανάπτυξης και μεθοδολογίας τως ίδιων τως τεχνικών. Ο ήχος συνδέεται άμεσα με τις αισθήσεις του ανθρώπου, μία διαπίστωση που συνέβαλε στην ανάπτυξη της υδατογράφησης ήχου. Αφού η βασική έννοια του υδατογραφήματος είναι να προστίθεται πληροφορία πιστοποίησης πνευματικών δικαιωμάτων, που να μην είναι αντιληπτή, η γνώση των ακουστικών ικανοτήτων του ανθρώπου σχετίζεται άμεσα με μέγεθος του υδατογραφήματος.

Επόμενος η μελέτη και η καταγραφή των ακουστικών δυνατοτήτων του ανθρώπου αποτελεί πολύτιμη πληροφορία ώστε να επιτευχθεί η μη αντιληπτή ένθεση υδατογραφήματος. Το ακουστικό σύστημα του ανθρώπου οριοθετεί το εύρος των ήχων που μπορεί να ακούσει ο άνθρωπος. Η επίγνωση ατού του συστήματος επισημαίνει με ποιο τρόπο και σε ποια περιοχή μπορεί η ύπαρξη επιπλέον πληροφορίας να μη γίνεται αντιληπτή από τον άνθρωπο.

Το ακουστικό σύστημα του ανθρώπου [42] ασχολείται με ένα ευρύ δυναμικό πεδίο, δηλαδή ορίζει τα όρια ανάμεσα από τα οποία ένας κοινός άνθρωπος αντιλαμβάνεται έναν ήχο ενώ ταυτόχρονα καθορίζεται η ευαισθησία του στον θόρυβο. Έτσι οι διαταράξεις σ' ένα αρχείο ήχου μπορεί να γίνουν αντιληπτές όσο ένα κομμάτι σε 10 εκατομμύρια (80 db κάτω από το ambient επίπεδο). Παρόλαυτά υπάρχουν μερικά «κενά σημεία» διαθέσιμα . Σε περιοχή του ηχητικού σήματος που χαρακτηρίζεται από ένα μεγάλο δυναμικό εύρος το ακουστικό σύστημα του ανθρώπου (HAS) μπορεί να αντιληφθεί τη διαφορά αρκετά δύσκολα. Η δυναμική ενέργεια ενός ηχητικού σήματος εκφράζει τη μεγάλη ηχητική ένταση του ήχου (υψηλό τόνο). Έτσι σε μία περιοχή μεγάλης έντασης ένας υψηλός ήχος επικαλύπτει έναν πιο χαμηλό. Η επικάλυψη αυτή σχετίζεται άμεσα με τις εφαρμογές φίλτρων καθώς η μάσκα ενός σήματος επηρεάζει είτε το μέτρο είτε τη συχνότητα.

Το ενδεχόμενο της εφαρμογής φίλτρου στο υδατογραφημένο αρχείου ήχου μιας και αποτελεί μία συνηθισμένη επεξεργασία πρέπει να ληφθεί υπόψιν. Οι επιπτώσεις του φιλτραρίσματος πάνω σ' ένα ηχητικό σήμα σχετίζεται άμεσα με τα χαρακτηριστικά του φίλτρου. Στην περίπτωση που υλοποιηθεί φιλτράρισμα με βάση τις συχνότητες για να υπάρξει επικάλυψη του υψηλού τόνου από το χαμηλό θα πρέπει αυτά να βρίσκονται

στην ίδια ή κοντινή συχνοτική περιοχή ώστε η επίδραση του φίλτρου να έχει παρόμοια επίδραση και στους αντίστοιχους ήχους, Να μπορεί δηλαδή ο δυνατότερος να κάνει τον πιο αδύναμο να μην παρατηρείται.

Το φιλτράρισμα που εφαρμόζεται σ' ένα ψηφιακό σήμα ήχου έχει πολλαπλά χαρακτηριστικά τα οποία επιδρούν στα βασικά στοιχεία του σήματος. Η επεξεργασία των σημάτων μπορεί να εφαρμοστεί εκμεταλλευόμενη τα ιδιαίτερα χαρακτηριστικά του σήματος και τα κατάλληλα εργαλεία έτσι ώστε να μορφοποιήσει το σήμα αποδίδοντας του ένα σύνολο ιδιοτήτων που επιλέγονται κάθε φορά ανάλογα με τις απαιτήσεις.

Το φιλτράρισμα επηρεάζει καταρχάς το εύρος του συχνοτικού περιεχομένου αποσκοπώντας να υπολογίσει ένα κατώφλι (threshold) πάνω η κάτω από το οποίο δε θα επιτρέπεται η εκπομπή σήματος. Μία τέτοια επεξεργασία καταρχάς θα πρέπει να λαμβάνει υπόψιν της το εύρος φάσματος, την πυκνότητα του το επίπεδο ηχητικής πίεσης και το θόρυβο που περικλείει ο ήχος. Όλα τα παραπάνω χαρακτηριστικά αν συνδυαστούν κατάλληλα με το κατώφλι του φίλτρου μπορούν να επιτύχουν την κάλυψη της επιπλέον ηχητικής πληροφορίας από κάποια άλλη. Για να μπορέσει ένα σήμα να εντεθεί έναντι κάποιου άλλου πρέπει τα ποιοτικά στοιχεία τους να μπορούν να συνδυαστούν έτσι ώστε να αποφέρουν το επιθυμητό αποτέλεσμα. Έτσι για να μπορέσει ένα σήμα να χρησιμοποιηθεί σα μάσκα σ' ένα άλλο θα πρέπει ένα ευρείας ζώνης ηχητικό σήμα το οποίο να μπορεί συγκαλύψει ένα μικρού εύρους ζώνης συχνοτήτων ήχο, όπως ένας τόνος. Γι' αυτό το λόγο ο θόρυβος που συνήθως έχει ένα ευρύ φάσμα συχνοτήτων μπορεί να επικαλύψει έναν ήχο σαν τον τόνο ενώ το αντίθετο δεν γίνεται καθώς μπορεί ο τόνος να έχει μεγαλύτερη συχνότητα αλλά το εύρος του το κάνει αδύναμο να εντεθεί σ' ένα ευρύ φάσμα

Το φιλτράρισμα συνήθως εφαρμόζεται στις υψηλές συχνότητες είτε αφού χρησιμοποιηθεί μάσκα δυνατού σήματος είτε μετά ώστε οι αδύναμοι ήχοι να παραμένουν μη αντιληπτοί. Επιπλέον ο άνθρωπος αντιλαμβάνεται ως επί το πλείστον τον ήχο βασιζόμενος στη διαφορά της φάσης και όχι στη διαφορά του μέτρου. Μπορεί λοιπόν ακόμη και ένα σήμα με συγκεκριμένες συχνότητες να αναπαρασταθεί σε διαφορετικές τιμές συχνοτήτων κρατώντας την απόλυτη διαφορά φάσης ίδια και ο κοινός παρατηρητής να μη αντιληφθεί τη μηδαμινή διαφορά. Διατηρώντας την ίδια «απόλυτη» διαφορά φάσης μπορεί ο ήχος να επιτρέπει την ενσωμάτωση επιπλέον πληροφορίας ή τη μορφοποίηση της πληροφορίας έτσι ώστε ο ήχος να ακούγεται ίδιος.

Οι τεχνικές που επεξεργάζονται ήχο βάσει το μέτρο του φάσματος [1], [51] του ηχητικού σήματος προσφέρουν την ικανότητα τροποποίησης του ήχου μιας και η φύση και ο βαθμός του μέτρου ενός ηχητικού σήματος δεν επηρεάζει σημαντικά την ακουστική του σήματος. Αντίθετα αν αυτές βασίζονται στην επεξεργασία με βάση τη φάση [1], [4] τότε η ένθεση φασματικής πληροφορίας επιβάλει την πιο λεπτομερή μορφοποίηση καθώς η παραμικρή αλλαγή της φάσης κάνει έκδηλη τη διαφορά. Ομως μπορεί αν προσεχθεί η απόλυτη φάση να διατηρηθεί στα ίδια επίπεδα να επιτευχθεί μία επιτυχής απόκρυψη ήχου. Τέλος ένας σημαντικός παράγων που ενισχύει τη δυνατότητα της απόκρυψης ηχητικού σήματος είναι η ύπαρξη θορύβου. Ο άνθρωπος γίνεται δέκτης μιας μεγάλης ποσότητας θορύβου μιας και στις ακουστικές του δραστηριότητες εκτός από αυτό που θέλει να αντιληφθεί αμέτρητοι άλλοι παράγοντες παράγουν ήχους αδιάφορους γι' αυτόν. Η εκπαίδευση του ανθρώπου στις καθημερινές συνθήκες, είχε ως αποτέλεσμα την ανθεκτικότητα σε διάφορες κατηγορίες θορύβου. Ένα φάσμα που χαρακτηρίζει τους θορύβους που ο κοινός άνθρωπος έχει συνηθίσει να μην παρατηρεί αποτελεί ένα καλό πεδίο διαπραγμάτευσης για το υδατογράφημα.

Το ακουστικό σύστημα του ανθρώπου αποτελεί ένα εδάφιο που χρήζει ιδιαίτερης μελέτης από τις τεχνικές υδατογράφησης ήχου μιας και συμβάλλει στο να μην γίνεται

αντιληπτή η πληροφορία του υδατογραφήματος που ενσωματώνεται από το ανθρώπινο αυτί ενώ ταυτόχρονα παρέχει πολύτιμα χαρακτηριστικά στο υδατογραφημένο προϊόν ενισχύοντας την ασφάλεια του.

2) Η μορφή και η δομή των ηχητικών σημάτων: Ένας δεύτερος παράγων που πρέπει να αναλυθεί είναι η μορφή και η δομή των ηχητικών σημάτων τα οποία τίθενται προς επεξεργασία για να εντεθεί υδατογράφημα σ' αυτά. Αυτό έχει ως συνέπεια, η ανάπτυξη μεθόδων υδατογράφησης σε ήχο να επηρεάζεται απο τα πιθανά περιβάλλοντα από τα οποία θα περάσει το σήμα κατά την διαδικασία της κωδικοποίησης και της αποκωδικοποίησης. Στα ψηφιακά προϊόντα και ιδιαίτερα στον ήχο αυτά θεωρούνται απαραίτητα για την ευχρηστία του προϊόντος όπως τη διάδοση μέσω δικτύου ή την αποκωδικοποίηση του μέσω διαφόρων πραγμάτων κτλ. Συγκεκριμένα για τον ήχο υπάρχουν 2 βασικοί μετασχηματισμοί που πρέπει να ληφθούν υπόψιν.

- Αρχικά το μέσο αποθήκευσης [42] δηλαδή η μορφή και η δόμηση των δεδομένων του ήχου κατά την αποθήκευση του προϊόντος. Όπως είναι ευρέως γνωστό ο ήχος που μεταδίδεται και χρησιμοποιείται αναπαρίσταται σε ψηφιακή μορφή.
- Επιπλέον σημαντικό ρόλο παίζει και διαδρομή εκπομπής που θα ακολουθήσει το σήμα για την παλαβή του από το χρήστη, του δικτύου μιας και στον παγκόσμιο ιστό τα ψηφιακά δεδομένα που μεταφέρονται επεξεργάζονται ποικιλοτρόπως.

7.2 Παράμετροι Επίδρασης στην Υδατογράφηση σε Ήχο

7.2.1 Δυαδική Αναπαράσταση

Υπάρχουν διαφορετικές μορφές αναπαράστασης [1], [51]ενός ψηφιακού αρχείου ήχου και αυτό γιατί υπάρχουν παράγοντες που επηρεάζουν τη μορφή αποθήκευσης του ψηφιακού ήχου. Δύο τέτοιοι παράμετροι που επιδρούν στη μορφή αναπαράστασης είναι η μέθοδος κβαντίσμου των δειγμάτων και ο ρυθμός δειγματοληψίας.

Ρυθμός Δειγματοληψίας

Ο ρυθμός δειγματοληψίας ενός ηχητικού σήματος επιδρά άμεσα στις τεχνικές υδατογράφησης μιας και σχετίζεται άμεσα με την επιλογή εκείνου του εύρους συχνοτήτων που περεχεί την χρήσιμη πληροφορία του αρχικού ηχητικού σήματος.. Διαφορετικοί ρυθμοί συχνοτήτων ορίζουν και διαφορετικά διαστήματα του εύρους ζώνης συχνοτήτων που περικλείει σημαντική πληροφορία. Οι πιο συχνοί ρυθμοί δειγματοληψίας που επιλέγονται για την αναπαράσταση του ήχου είναι 8 KHz, 16 KHz και 44.1 KHz. Η δειγματοληψία ενός σήματος για να μην υπάρχει επικάλυψη θα πρέπει να είναι τουλάχιστον μεγαλύτερη κατά 2 φορές από τη μέγιστη συχνότητα του ηχητικού σήματος σύμφωνα με τον κανόνα του Nyquist.

Μ' αυτό τον τρόπο θέτεται ένα όριο από το ρυθμό δειγματοληψίας για το συχνοτικό περιεχόμενο που περικλείει χρήσιμα δεδομένα. Έτσι αύξηση του ρυθμού δειγματοληψίας αυξάνει το διάστημα που περιέχει χρήσιμα δεδομένα. Όμως οι περισσότερες μέθοδοι υδατογράφησης σε ήχο έχουν καταφέρει να ελέγξουν την αύξηση αυτή, περιορίζοντας τη σε γραμμική αναλογία μεταξύ του ρυθμού και των διαστημάτων δεδομένων.

Μέθοδος κβαντίσμου

Εξίσου σημαντικός παράγοντας είναι η μέθοδος κβαντίσμου των δειγμάτων. Η πιο διαδεδομένη μέθοδος αναπαράστασης των δειγμάτων με υψηλή ποιότητα ψηφιακού ήχου είναι ο κβαντισμός 16 δυαδικών ψηφίων (Windows Audio Visual - WAV). Παράλληλα υπάρχουν κι άλλες μορφές κβαντίσμου των δεδομένων όπως ο Audio Intergage Format (AIFF), όπως επίσης και κβαντισμοί που χρησιμοποιούν χαμηλή ποιότητα ήχου μεσώ λογαριθμικής σμίκρυνσης σε 8 δυαδικά ψηφία ή μ-δυαδικά ψηφία (bit). Αν και τα WAV αρχεία ως επί το πλείστον χρησιμοποιούνται λόγω της καλής ποιότητας ήχου που προσφέρουν και οι μέθοδοι κβαντίσου χαμηλής ποιότητας επιλέγοντας μιας και αποτρέπουν την παραμόρφωση του ηχητικού σήματος.

Τέλος επειδή και τα αρχεία ήχου περικλείουν μεγάλη ποσότητα δεδομένων απαιτείται συμπίεση του προϊόντος ώστε να είναι εύχρηστο. Τα αρχεία ήχου συνήθως συμπιέζονται με απώλεια πληροφορίας (lossy compression) με ειδικούς αλγόριθμους όπως ο ISO - MPEG AUDIO[23]. Η χρήση συμπιεστικών αλγορίθμων συμπίεσης επηρεάζουν σε μεγάλο βαθμό τα χαρακτηριστικά του σήματος καθώς η απώλεια δεδομένων που προκαλούν επιτρέπει την ύπαρξη μόνο της πληροφορίας που γίνεται αντιληπτή. Η απώλεια των δεδομένων που προκαλεί ο αλγόριθμος MPEG σήμα μπορεί να είναι τελείως διαφορετικό παρόλαυτά ο ήχος του είναι ίδιος όπως με την έννοια των ελαχίστων τετραγώνων.

7.2.2 Περιβάλλον Μετάδοσης

Τα αρχεία ήχου μεταφέρονται τόσο μέσω του παγκόσμιου ιστού όσο και μέσω του τηλεπικοινωνιακού δικτύου. Υπάρχουν πολλές διαφορετικές μορφές μετάδοσης[1] που μπορεί να εφαρμοσθούν για τη μετάδοση ήχου του από τον πομπό στο δείκτη. Η πρώτη μέθοδος είναι η εκπομπή ψηφιακού σήματος και η μέχρι το τέλος παραμονή σε ψηφιακό περιβάλλον.

Εδώ το σήμα δεν υφίσταται μορφοποιήσεις που αλλάζουν την ψηφιακή μορφή του, αλλά παραμένει σε αυτή από τη στιγμή που εκπέμπεται κατά τη διάρκεια της διαδρομής που ακολουθεί και κατά την άφιξη του στο δέκτη. Αυτή η μέθοδος μετάδοσης συμβάλει στο λιγότερο βαθμό στην μορφοποίηση του υδατογραφημένου αρχείου ήχου μιας και η δειγματοληψία του παραμένει αναλλοίωτη από τη στιγμή που κωδικοποιείται έως την αποκωδικοποίηση του.

Όμως επιλέγεται μόνο στην περίπτωση που μεταφέρονται αρχεία ήχου μικρού όγκου μιας και σε αντίθετη περίπτωση δεν αποτελεί σοφή επιλογή γιατί μεγάλη ποσότητα δεδομένων, μέσω του δικτύου δημιουργεί φόρτο σε αυτό και επιβραδύνει την ταχύτητα παραλαβής.

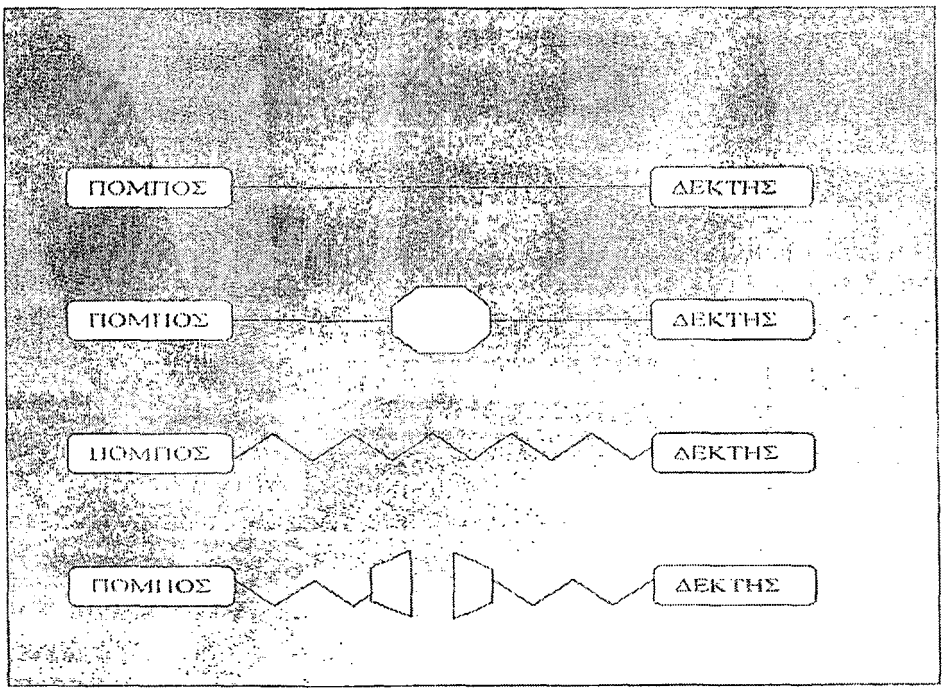
Μία δεύτερη μέθοδος είναι η εκπομπή του σήματος σε ψηφιακή μορφή, η μετέπειτα επαναδειγματοληψία αλλάζοντας το ρυθμό δειγματοληψίας (είτε από υψηλότερο σε χαμηλότερο είτε αντίστροφα) και τελικά φτάνει στο δέκτη σε ψηφιακή μορφή. Ο ήχος κατά την άφιξη του στο δέκτη παραμένει ψηφιακός αλλά με διαφορετικό ρυθμό. Η αλλοίωση του ηχητικού σήματος εδώ δεν είναι μεγάλη μιας και αυτή η μέθοδος διατηρεί την απόλυτη φάση και μέτρο του ήχου αναλοίωτη. Η τρίτη περίπτωση μετάδοσης ήχου περιλαμβάνει εκπομπή του ήχου σε αναλογική μορφή, μετάδωση μέσω αναλογικού δικτύου και επαναδειγματοληψία. Ο ήχος φτάνει στο δέκτη σε αναλογική μορφή αλλά με διαφορετική δομή μιας και οι μορφοποιήσεις της φάσης του μέτρου και του ρυθμού δειγματοληψίας δεν αποτρέπονται. Η αλλοίωση του σήματος είναι εμφανής ενώ η αλλαγή της φάσης αποτρέπεται σ' ένα μεγάλο βαθμό.

Στην τελευταία περίπτωση το σήμα διαδίδεται με την αναπαραγωγή του στον αέρα και την επαναδειγματοληψία από ένα μικρόφωνο. Το σήμα είναι πιθανόν να υποστεί

άγνωστες μορφοποιήσεις μη δυαδικές γεγονός που επιφέρει αρκετές αλλοιώσεις στο σήμα. Οι αλλαγές αυτές μπορεί να είναι στη φάση, στο μέτρο και στις αρμονικές. Η μετατόπιση του συχνοτικού περιοχομένου του σήματος καταδεικνύει μη αξιοπιστία της μεθόδου εκπομπής.

Συμπερασματικά η αναπαράσταση του σήματος και ο τρόπος μετάδοσης του πρέπει να ληφθούν υπόψιν και να μελετηθούν με σοβαρότητα κατά την εφαρμογή μιας μεθόδου που ενσωματώνει επιπλέον πληροφορία στον ήχο όπως το υδατογράφημα, εφόσον ο ρυθμός των δεδομένων εξαρτάται σε μεγάλο βαθμό από το ρυθμό δειγματοληψίας και την κωδικοποίηση που υφίσταται ο ήχος.

Κάθε τεχνική αποδίδει σε κάθε παράγοντα την κατάλληλη τιμή ώστε η επιλογή αυτή να αποφέρει ένα υδατογραφημένο ήχο μη αντιληπτό και ανθεκτικό στις διάφορες μορφές επεξεργασίας. Έτσι οι περισσότερες τεχνικές χρησιμοποιούν την τιμή των 16bps ως ρυθμό δειγματοληψίας αλλά γενικώς κυμαίνεται η τιμή από 2bps έως 128bps.



Εικόνα 39 **Περιβάλλοντα Διάδοσης Ήχου**

7.3 Σχήματα Υδατογράφησης Ήχου

Οι τεχνικές που προτείνονται στον ήχο μπορούν να κατηγοριοποιηθούν σε τρεις βασικές κατηγορίες:

1) Στις μεθόδους με βάση τη μορφή των δεδομένων του αρχείου ήχου. Δηλαδή αν το αρχείο ήχου είναι σε συμπιεσμένη μορφή ή σε μη συμπιεσμένη μορφή.

2) Στις μεθόδους με βάση το πεδίο αναπαράστασης στο πεδίο των συχνοτήτων.

3) Στις μεθόδους με βάση το πεδίο αναπαράστασης στο πεδίο του χρόνου ο τρόπος αναπαράστασης του αρχείου ήχου χαρακτηρίζει τη δομή και τη μορφή των ψηφιακών δεδομένων. Είναι εύλογο λοιπόν να επιρεάζει καθοριστικά τη μέθοδο

υδατογράφησης στον τρόπο με τον οποίο ενθέτει την ψηφιακή πληροφορία του υδατογραφήματος στο αρχείο ήχου. Η σπουδαιότητα λοιπόν των τριών κατηγοριών αναπαράστασης αρχείων ήχου καθορίζει και τρεις διαφορετικές κατηγορίες υδατογράφησης, οι οποίες χρίζουν η κάθε μία ξεχωριστής ανάλυσης.

7.3.1 Σχήμα Υδατογράφησης σε συμπιεσμένο αρχείο ήχου (MPEG) [43], [23], [28]

Η συμπιεσμένη μορφή (mpeg) ενός αρχείου ήχου αποτελεί μία κοινή αναπαράσταση ήχου που χρησιμοποιείται ευρέως τόσο από το σύνολο των χρηστών του διαδυκτίου όσο και γενικότερα αυτών που χρησιμοποιούν ψηφιακά αρχεία ήχου. Είναι σημαντικό λοιπόν μία μέθοδος όπως η υδατογράφηση να μπορεί να εφαρμοσθεί κατευθείαν σε ηχογραφημένο αρχείο ήχου με συμπιεσμένη μορφή mpeg. Υπάρχουν τρεις βασικές λόγοι που κάνουν την υδατογράφηση σε mpeg ηχητικά δεδομένα αρκετά σημαντική:

1) Σήμερα όπου η τεχνολογία για εφαρμογές πάνω σε αρχεία ήχου έχει αναπτυχθεί αρκετά γιατί κοινές επεξεργασίες και εφαρμογές ψηφιακών αρχείων ήχου με μορφή κωδικοποίησης mpeg είναι διαθέσιμες σε όλους. Επίσης οι εφαρμογές αυτές μαζί με την ευρεία χρήση του διαδυκτίου που αποτελεί μέσο διακίνησης ψηφιακών προϊόντων καθιέρωσαν ττρχρήση αρχείων ήχου σε συμπιεσμένη μορφή. Καθώς η mpeg μορφή του ήχου έδωσε τη δυνατότητα στα ηχητικά δεδομένα να απαιτούν λιγότερους πόρους όπως χώρους σκληρού δίσκου ή εύρος ζώνης δικτύου (bandwith) έκανε τα αρχεία ήχου πιο προσιτά. Σήμερα λοιπόν η αντιγραφή, η διακίνηση, η αναπαραγωγή και η διανομή ενός αρχείου ήχου είναι πολύ πιο εύκολη και πολύ πιο γρήγορη χάρις την mpeg μορφή των αρχείων ήχου γι' αυτό και μία μέθοδος που εφαρμόζεται κατευθείαν σε mpeg κωδικοποιημένα δεδομένα ήχου προτάσσεται σαν αναγκαία.

2) Αν δεν υπήρχε η δυνατότητα της υδατογράφησης σε mpeg κωδικοποιημένα ηχητικά δεδομένα τότε θα απαιτούνταν στα mpeg αρχεία ήχου επιπλέον διαδικασία αποσυμπίεσης και επανασυμπίεσης κατά τη διαδικασία υδατογράφησης. Η διαδικασία υδατογράφησης θα απαιτούσε την αποσυμπίεση των κωδικοποιημένων mpeg δεδομένων, την υδατογράφηση τους και την επανασυμπίεσή τους κάνοντας τη χρονοβόρα και μη αποδοτική.

3) Εξαιτίας της παραμόρφωσης του ήχου ή οποία είναι πιο ευαίσθητα στο ανθρώπινο αυτί απ' ότι η παραμόρφωση μιας εικόνας στο ανθρώπινο μάτι οι συνήθης κωδικοποιήσεις mpeg για βίντεο δε θα ήταν αποδοτικές για mpeg κωδικοποίηση ήχου. Η ανάπτυξη λοιπόν μεθόδων υδατογράφησης σε κωδικοποιημένο ήχο mpeg είναι αναπόφευκτη, ώστε να μπορεί να έχει ποιοτικά αποτελέσματα που να μην είναι αντιληπτά από τις ακουστικές ικανότητες του ανθρώπου.

Η mpeg συμπίεση ήχου είναι μία συμπίεση με απώλεια δεδομένων η οποία χρησιμοποιεί το ανθρώπινο ακουστικό σύστημα. Μπορεί να παρέχει έναν παράγοντα συμπίεσης ίσο με 6 προς 1 ή μεγαλύτερο καθώς αφαιρεί τα αντιληπτά άσχετα κομάτια του αρχείου ήχου και κάνοντας την παραμόρφωση του ηχητικού σήματος μη αντιληπτή στο ανθρώπινο αυτί. Η mpeg κωδικοποίηση ήχου ακολουθεί τα παρακάτω βήματα:

1) Τα δείγματα του ηχητικού αρχείου εισόδου τροφοδοτούνται στον κωδικοποιητή.

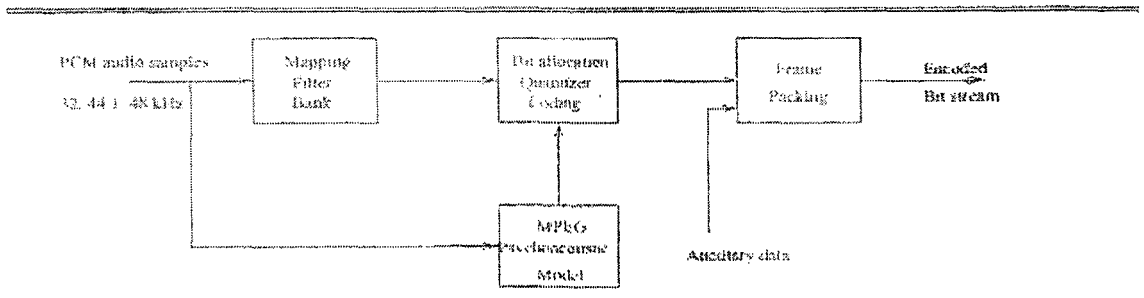
2) Τα ηχητικά δείγματα διέρχονται μέσα από ένα σχεδιασμένο ζωνοπερατό φίλτρο το οποίο δημιουργεί μία αναπαράσταση της εισόδου όπου τα δείγματα ομαδοποιούνται σε σχέση με τις υποπεριοχές του συχνοτικού εύρους που επιφέρει η εφαρμογή φίλτρου. Στην πραγματικότητα διαιρείται η πληροφορία του ήχου σε

υποδιαστήματα του εύρους συχνοτήτων.

3) Την ίδια ώρα τα δείγματα ήχου της εισόδου διέρχονται από το mpeg οπτικοακουστικό μοντέλο το οποίο δημιουργεί ένα σύνολο από δεδομένα ώστε να ελεγχθεί ο κβαντισμός και η κωδικοποίηση σε κάθε υποσύνολο του εύρους συχνοτήτων. Το ποσοστό της ενέργειας του σήματος χρησιμοποιείται από τη διαδικασία κβαντισμού και κωδικοποίησης ώστε να προσδιοριστούν οι περιοχές που περιέχουν πληροφορία θορύβου για να μην είναι αντιληπτός στο ανθρώπινο αυτί ο ηχητικός θόρυβος κβαντισμού.

4) Τέλος τα δείγματα των υποσυνόλων κβαντίζονται μέσω ενός σχηματισμού σε μορφή μπλοκ που ομαδοποιεί τα πλαίσια του ήχου (frame packing block formats) σε κωδικοποιημένη ροή δεδομένων εξόδου.

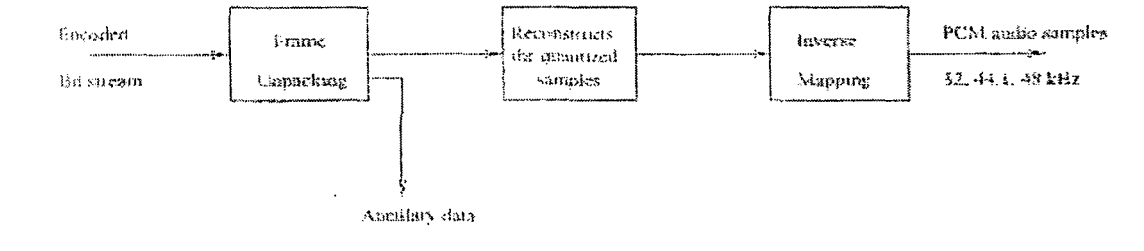
Το παρακάτω σχήμα δείχνει τη βασική δομή ενός mpeg κωδικοποιητή ήχου.



Εικόνα 40 **Η Βασική Δομή ενός mpeg Κωδικοποιητή**

Η διαδικασία αποκωδικοποίησης ήχου mpeg είναι μία απλή αντιστροφή της διαδικασίας αποκωδικοποίησης ήχου mpeg. Η διαδικασία αποκωδικοποίησης λαμβάνει την κωδικοποιημένη ροή δεδομένων σε δυαδική αναπαράσταση και μέσα από το διάγραμμα των μπλοκ που ομαδοποιούν τα πλαίσια του ήχου επαναδομεί τα συχνοτικά δείγματα. Τα συχνοτικά αυτά δείγματα αντιστοιχούν στα υποσύνολα του εύρους συχνοτήτων. Έπειτα γίνεται μία αντιστροφή της εφαρμογής ζωνοπερατού φίλτρου όπου οι ομαδοποιημένες περιοχές του εύρους ζώνης συχνοτήτων του ήχου χρησιμοποιούνται ώστε να παραχθεί το ηχητικό σήμα σε μορφή χρονικών ηχητικών δειγμάτων.

Η παρακάτω εικόνα δείχνει τη διαδικασία αποκωδικοποίησης.



Εικόνα 41 **Διαδικασία Αποκωδικοποίησης**

Υπάρχουν διαφορετικά τεχνικά χαρακτηριστικά της mpeg ηχητικής συμπίεσης ανάλογα με τις διαφορετικές τεχνικές και εφαρμογές που εφαρμόζονται. Στην mpeg κωδικοποιημένη μορφή ήχου μπορούμε να διακρίνουμε τρεις βασικές κατηγορίες που ορίζουν και διαφορετικές μορφές συμπιεσμένης mpeg αναπαράστασης ήχου:

Α) Ανάλογα με το ρυθμό δειγματοληψίας του ηχητικού σήματος εισόδου.

Β) Ανάλογα με τα κανάλια που χρησιμοποιεί το ηχητικό σήμα για αναπαράσταση.

C) Ανάλογα με τα τρία στρώματα (layers) της κωδικοποίησης mpeg του ήχου.

Α) Η mpeg αναπαράσταση σα συμπιεσμένη μορφή ήχου υποστηρίζει τρεις διαφορετικές μορφές εισόδου του ηχητικού σήματος ανάλογα με το ρυθμό δειγματοληψίας του ήχου εισόδου στα 32 στα 44.1 και στα 48 Khz.

Β) Επίσης υπάρχουν τέσσερα διαφορετικά μοντέλα καναλιών όπου η mpeg συμπιεσμένη μορφή ήχου μπορεί να αναπαρασταθεί.

1. Του ενός καναλιού δηλαδή του μονοφωνική ήχου.
2. Των δύο καναλιών όπου δύο ανεξάρητα ηχητικά σήματα κωδικοποιούνται σε μία δυαδική ροή δεδομένων.
3. Της στερεοφωνικής αναπαράστασης ήχου όπου το αριστερό και το δεξί σήμα ενός στερεοφωνικού ζευγαριού κωδικοποιείται σε μία ροή δεδομένων δυαδικής αναπαράστασης.
4. Την αναμειγμένη στερεοφωνική αναπαράσταση όπου σε αντίθεση με τη απλή στερεοφωνική αναπαράσταση εδώ λαμβάνεται υπόψη η στερεοφωνική διαφορά και η πλεονάζουσα πληροφορία μεταξύ των καναλιών.

C) Ανάλογα με τις τεχνικές εφαρμογές που χρησιμοποιούν τη mpeg συμπιεσμένη μορφή ήχου μπορούμε να διακρίνουμε τρία διαφορετικά στρώματα της mpeg κωδικοποίησης με αυξημένη πολυπλοκότητα κωδικοποίησης.

Το στρώμα ένα (layer I)[43] περιλαμβάνει το βασικό σχεδιασμό των ηχητικών σημάτων σε 32 υποδιαστήματα του εύρους ζώνης συχνοτήτων, τα προκαθορισμένα τμήματα πληροφορίας που μορφοποιούν τα δεδομένα σε μπλοκ, το οπτικοακουστικό μοντέλο που προσδιορίζει τις περιοχές πληροφορίας και τέλος τον κβαντισμό των δειγμάτων. Στο στρώμα αυτό είναι αρκετά βολική η χρήση ρυθμού δεδομένων πάνω από 128 kbps για κάθε κανάλι.

Το στρώμα δύο (layer II) [43] παρέχει μία επιπρόσθετη κωδικοποίηση για τον προσδιορισμό των περιοχών πληροφορίας, για τους παράγοντες βάθμωσης (scale factors) και για τα δείγματα ήχου. Ο ρυθμός των δεδομένων κυμαίνεται γύρω από τα 128 Kbps για κάθε κανάλι.

Το στρώμα τρία (layer III) [28] εισάγει μία συχνοτική ανάλυση βασιζόμενη σε ένα υβριδικό μοντέλο φίλτρου. Χρησιμοποιεί ένα μη ομοιόμορφο κβαντισμό και μία κωδικοποίηση βάση της εντροπίας που στηρίζεται στη Hoffman [43] κωδικοποίηση. Τα αποτελέσματα της τεχνικής αυτού του στρώματος χαρακτηρίζονται από βέλτιστη ποιότητα ήχου, ειδικά όταν ο ρυθμός δειγματοληψίας γίνεται γύρω στα 64 Kbps για κάθε κανάλι.

Ο αλγόριθμος mpeg συμπίεσης ήχου μπορεί να εφαρμόσει συμπίεση στο αρχείο ήχου με παράγοντα που κυμαίνεται από 2.7 έως 24. Οι παράγοντες συμπίεσης εξαρτώνται από το διαφορετικό προκαθορισμένο ρυθμό δειγματοληψίας από 32 έως 224 Kbps. Η mpeg κωδικοποίηση του ήχου σχετίζεται με τη ροή των ηχητικών πλαισίων. Το πλαίσιο (frame) είναι η μικρότερη δυνατή μονάδα η οποία μπορεί να αποκωδικοποιηθεί μεμονωμένα. Κάθε πλαίσιο περιέχει δεδομένα ηχητικής πληροφορίας, μία επικεφαλίδα μεγέθους τεσσάρων byte (4-byte) έναν πιθανό κώδικα

διόρθωσης λαθών (CRC) και βοηθητική πληροφορία. Η επικεφαλίδα των πλαισίων καθορίζει τη βασική δομή της πληροφορίας σχετικά με τη ροή των δυαδικών δεδομένων σαν μία λέξη χρονισμού όπου καταδεικνύει το αρχικό σημείο ενός καινούργιου πλαισίου.

Τα ωφέλιμα φορτία της δομής των στρωμάτων I και II της mpeg κωδικοποίησης είναι συναφή ενώ η αντίληψη του στρώματος III της mpeg κωδικοποίησης είναι διαφορετική, γι' αυτό και είναι σημαντικό να αναλυθεί η δομή του στρώματος II κωδικοποίησης που αντιπροσωπεύει σε βασικά σημεία και την κωδικοποίηση του στρώματος I. Στο στρώμα II της mpeg συμπιεσμένης μορφής ήχου κάθε πλαίσιο περιλαμβάνει 1152 δείγματα. Κάθε υποσύνολο του εύρους ζώνης συχνοτήτων περιλαμβάνει τρία σύνολα δειγμάτων με 12 δείγματα το κάθε σύνολο. Η κωδικοποίηση μπορεί να χρησιμοποιήσει διαφορετικά παράγοντα βάθμωσης για κάθε ένα από τα σύνολα των 12 δειγμάτων. Το ωφέλιμο φορτίο της πληροφορίας ενός mpeg ηχητικού πλαισίου αποτελείται από τρία μέρη:

a) Την πληροφορία επιλογής του παράγοντα βάθμωσης.

b) Το πεδίο των παραγόντων βάθμωσης.

c) Το πεδίο των δειγμάτων.

Η παρακάτω εικόνα δείχνει τη δομή ενός mpeg κωδικοποιημένου ήχου στο στρώμα Π.

Mea<fer	CRC	Bit AJIacalion	Scate Factors	Encoded Samples	Ancillar y Data

Εικόνα 42 **Βασική Δομή MPEG layer 2 Αρχείου Ήχου**

Τα ηχητικά δεδομένα όπως και άλλοι τύποι πολυμεσικών δεδομένων συχνά αποθηκεύονται και μεταφέρονται - εκπέμπονται σε συμπιεσμένη μορφή όπως ο mpeg συμπιεσμένος ήχος. Ο μηχανισμός υδατογράφησης θα πρέπει να ενασχολείται με τη συμπιεσμένη μορφή δεδομένων. Παρόλο που η υδατογράφηση με τα σχήματα υδατογράφησης όπως του Boney [18], [19] έχει πολύ θετικά αποτελέσματα σε μη συμπιεσμένα δεδομένα είναι αναγκαίο το υδατογράφημα να μπορεί να εφαρμοσθεί και σε δεδομένα που είναι συμπιεσμένα με mpeg κωδικοποίηση.

Παραγωγή υδατογραφήματος

Καταρχάς το υδατογράφημα θα πρέπει να απαντά στην προστασία των πνευματικών δικαιωμάτων του ιδιοκτήτη και να μην επιτρέπει τη δημιουργία και τη χρήση πλαστών υδατογραφημάτων που επιδιώκουν την διεκδίκηση των δικαιωμάτων του ιδιοκτήτη. Υπάρχουν πολλές διαφορετικές προσεγγίσεις για την προστασία των πνευματικών δικαιωμάτων του ιδιοκτήτη από την παραπάνω επίθεση ώστε η υδατογράφηση να αποτελεί μη αντιστρεπτή διαδικασία. Το υδατογράφημα που κατασκευάζεται για mpeg κωδικοποιημένο ήχο μπορεί να απαντά με μη αντιστρεπτό τρόπο στην ιδιοκτησία των πνευματικών δικαιωμάτων ακολουθώντας τα παρακάτω βήματα:

1) Αρχικά γίνεται η επιλογή του κλειδιού και για κάθε mpeg κωδικοποιημένο ηχητικό πλαίσιο α_j, όπου j = 1,...,N (όπου N ο αριθμός των ηχητικών πλαισίων). Έπειτα εφαρμόζουμε μία συνάρτηση κρυπτογράφησης (DES) η οποία μαζί με το κλειδί υδατογράφησης δίνει μία ψευδοτυχαία δυαδική συχνότητα.

$$RBS = DES_{KEY} \quad (\text{Για κάθε ηχητικό πλαίσιο } \alpha_j)$$

2) Αν θεωρήσουμε τη συνάρτηση κρυπτογράφησης RBS_i ως την ψευδοτυχαία δυαδική συχνότητα για κάθε i-οστό byte και w_i το i-οστό δυαδικό ψηφίο (bit) της

ακολουθίας υδατογραφημένων δυαδικών ψηφίων τότε το υδατογράφημα μπορεί να δημιουργηθεί με τον εξής τρόπο:

$$w_i = \begin{cases} -1 & \alpha\nu \ \mathrm{RBS}_i \ \text{ζυγός αριθμός} \\ 1 & \delta\iota\alpha\phi o\rho\varepsilon\tau\iota\kappa\ \acute{\alpha} \end{cases}$$

Η δυαδική συχνότητα υδατογράφησης εφαρμόζεται επανελλειμένα στα ηχητικά δεδομένα που βρίσκονται στο ίδιο ηχητικό πλαίσιο αν το μέγεθος της δυαδικής συχνότητας υδατογράφησης στο στοιχείο i είναι μικρότερη από τον αριθμό των δειγμάτων στο συγκεκριμένο πλαίσιο.

Διαδικασία ένθεσης

Υπάρχουν δύο σημαντικά βασικά μέρη στο πεδίο αναπαράστασης των δεδομένων με την κωδικοποιημένη μορφή mpeg ήχου, το ένα είναι οι παράγοντες βάθμωσης και το άλλο τα κωδικοποιημένα δείγματα. Και τα δύο αυτά μέρη μιας και επηρεάζουν την κωδικοποιημένη μορφή του ηχητικού αρχείου είναι εύλογο να χρησιμοποιούνται στην διαδικασία ένθεσης του υδατογραφήματος, γι' αυτό και μελετώντας τη διαδικασία ένθεσης πρέπει να αναλυθούν οι παρακάτω δύο διαδικασίες:

1) Υδατογράφηση με βάση τους παράγοντες βάθμωσης (scale factors).

Ο παράγοντας βάθμωσης στην κωδικοποίηση της mpeg συμπίεσης ήχου είναι ο πολλαπλασιαστής που κάνει τα δείγματα να μπορούν καθολικά να χρησιμοποιήσουν το εύρος κβαντισμού. Στην αποκωδικοποίηση πολλαπλασιάζεται ο παράγοντας βάθμωσης με την αποκωδικοποιημένη κβαντισμένη έξοδο ώστε να παραχθούν τα κβαντισμένα δείγματα που αντιστοιχούν στα υποσύνολα του συχνοτικού εύρους. Η διαδικασία υδατογράφησης προσθέτει στο δυαδικό ψηφίο (bit) του υδατογραφήματος yy. στο δείκτη που αντιπροσωπεύει τον παράγοντα βάθμωσης με δύο προϋποθέσεις:

1) Αν ο παράγοντας είναι ίσος με μηδέν και το w_i = -1, τότε δεν κάνουμε τίποτα.

2) Αν ο παράγοντας είναι ίσος με 62 και το w_i = -1 τότε δεν κάνουμε τίποτα.

Αν υποθέσουμε ότι ο παράγοντας βάθμωσης του δείκτη $\mathrm{ScaleFactor}_i(\mathrm{index})$ για το i - οστό παράγοντα βάθμωσης του οποίου το επίπεδο δηλώνεται από το δείκτη και ότι ο i-οστός παράγοντας βάθμωσης του υδατογραφήματος $\mathrm{ScaleFactor}_i(w_i)$ είναι ίσος με 1, τότε η διαδικασία υδατογράφησης μπορεί να περιγραφεί ως:

$$ScaleFactor_i(w_i) = \begin{cases} ScaleFactor_i(index) & \alpha\nu \quad \mathrm{index} + w_i = -1 \ \acute{\eta} \ 63 \\ ScaleFactor_i(index + w_i) & \delta\iota\alpha\phi o\rho\varepsilon\tau\iota\kappa\acute{\alpha} \end{cases}$$

Το παραπάνω σχήμα υδατογράφησης είναι αρκετά αξιόπιστο. Παρ' ολ' αυτά έχει μειονεκτήματα. Το πρώτο μειονέκτημα είναι ότι μερικές ακολουθίες των ηχητικών δεδομένων χαρακτηρίζονται από λίγους παράγοντες βάθμωσης για ένα πλαίσιο και έτσι η υδατογράφηση που βασίζεται στα πλαίσια του αρχείου ήχου δεν μπορεί να υδατογραφήσει αρκετή πληροφορία από το αρχικό σήμα ήχου. Μία λύση για το μειονέκτημα αυτό είναι η ομαδοποίηση των πλαισίων έτσι ώστε ο μηχανισμός υδατογράφησης να γίνεται σε ένα σύνολο από πλαίσια και όχι σε κάθε πλαίσιο ξεχωριστά. Δεύτερον όταν ο παράγοντας βάθμωσης αυξάνεται κατά ένα επίπεδο ή μειώνεται κατά ένα δεν παρατηρείται ηχητική παραμόρφωση, όμως όταν αυτός αυξάνεται ή μειώνεται για δύο επίπεδα ή περισσότερα προκαλείται ηχητική παραμόρφωση στο υδατογραφημένο αρχείο ήχου που μπορεί να γίνει αντιληπτή από

το ανθρώπινο αυτί. Γι' αυτό και το πολλαπλό υδατογράφημα παρουσιάζει ένα πρόβλημα συμβατότητας με τον παραπάνω μηχανισμό υδατογράφησης.

2) Υδατογράφηση με βάση τα κωδικοποιημένα δείγματα

Η άλλη επιλογή είναι η ένθεση του υδατογραφήματος στα δεδομένα της πληροφορίας του αρχείου ήχου. Η βασική ιδέα του σχήματος αυτού βασίζεται στην πρόσθεση υδατογραφήματος (-1/1 συχνότητα δυαδικών ψηφίων) στα κωδικοποιημένα δείγματα συχνότητας. Η τροποποίηση των κωδικοποιημένων δειγμάτων επιβάλλεται να γίνει με αρκετή προσοχή γιατί μπορεί να επιφέρει αρκετή παραμόρφωση στο ηχητικό αρχείο. Σκεπτόμενοι ότι η τροποποίηση κάθε κωδικοποιημένου δείγματος μπορεί να επιφέρει ηχητική παραμόρφωση που μπορεί να ανιχνευθεί από το ανθρώπινο αυτί δεν επιλέγεται σε καμία περίπτωση η αλλαγή του συνόλου των κωδικοποιημένων δειγμάτων. Για την επίλυση αυτού του προβλήματος αυξάνουμε την παράμετρο του διαστήματος (spacing parameter, sp) των δειγμάτων δηλαδή προσεγγιστικά σε κάθε sp δείγματα επιλέγουμε τυχαία ένα ή δύο δείγματα για την εφαρμογή υδατογράφησης. Η χρήση της παραμέτρου διαστήματος δίνει τη δυνατότητα στη μέθοδο υδατογράφησης να προσαρμόζεται σε δεδομένα ήχου που είναι κωδικοποιημένα με mpeg κωδικοποίηση.

Η μέθοδος της υδατογράφησης χρησιμοποιεί μία διαδικασία ελαφρώς μορφοποιημένη έτσι ώστε να ενσωματώνει και τον παράγοντα του διαστήματος sp, όπως φαίνεται παρακάτω:

$$w_i = \begin{cases} -1 & \alpha\nu \quad \mathrm{RBS}_i = 0 \\ 1 & \alpha\nu \quad \mathrm{RBS}_i = 1 \\ 0 & \textit{διαφορετικ ά} \end{cases}$$

Η διαδικασία υδατογράφησης είναι παρόμοια με την προηγούμενη εκτός απ' το ότι πρέπει να γίνεται βέβαιο ότι τα δείγματα που υδατογραφούνται δεν έχουν τη μορφή του «111...1» επειδή η κωδικοποίηση ενός τέτοιου δείγματος δεν επιτρέπεται από τις βασικές αρχές της mpeg κωδικοποίησης. Αν αναπαραστήσουμε το i-οστό δείγμα με Sample σε ένα ηχητικό πλαίσιο, το i-οστό υδατογραφημένο δείγμα με $\mathrm{SampleW}_i$ και τον αριθμό των δυαδικών ψηφίων που εντοπίζονται σε κάθε i-οστό δείγμα με w_i, τότε η συνάρτηση υδατογράφησης μπορεί να αναπαρασταθεί από τον παρακάτω τύπο:

$$SampleW_i = \begin{cases} Sample_i & \text{αν κ κά bit τit } (\mathrm{Sample}_i + \mathrm{w}_i) = 1 \\ Sample_i + w_i & \text{διαφορετικά} \end{cases}$$

Και τα δύο σχήματα υδατογράφησης για κωδικοποιημένα δεδομένα ήχου ήχου με mpeg συμπίεση τόσο της υδατογράφησης που βασίζεται στους παράγοντες βάθμωσης όσο και της υδατογράφησης που βασίζεται στα κωδικοποιημένα δείγματα έχουν άμεση σχέση με τη μέθοδο υδατογράφησης του διασκορπισμένου φάσματος [4] (spread spectrum). Οι δύο αυτές μέθοδοι υδατογράφησης σχεδιάστηκαν ώστε να μπορεί η υδατογράφηση να απαντά και στη συμπιεσμένη μορφή ηχητικών αρχείων. Μ' αυτό τον τρόπο επιτυγχάνεται η υδατογράφηση στο πεδίο των συμπιεσμένων δεδομένων δίνοντας αξιόπιστα αποτελέσματα και ταυτόχρονα αποφεύγοντας χρονοβόρες διαδικασίες κωδικοποίησης και αποκωδικοποίησης.

7.3.2 Σχήμα Υδατογράφησης για το πεδίο του χρόνου [19], [18], [4]

Ο αλγόριθμος υδατογράφησης που προτείνεται ενσωματώνει το υδατογράφημα στο

πεδίο του χρόνου ενός ηχητικού σήματος αλάζοντας το μέτρο κάθε ηχητικού δείγματος. Σ' αυτή τη μέθοδο υδατογράφησης δεν απαιτείται το αρχικό σήμα για την ανίχνευση του υδατογραφήματος.

Η διαδικασία ένθεσης υδατογραφήματος επεξεργάζεται το ηχητικό σήμα το οποίο αναπαρίσταται από 16 bit ή 8 bit συχνοτικά δείγματα αλλάζοντας το λιγότερο σημαντικό δυαδικό ψηφίο (low bit coding) για κάθε δείγμα. Μ' αυτό τον τρόπο αλλάζει ελάχιστα το μέτρο του κάθε δείγματος έτσι ώστε να μη παρατηρηθεί στο κωδικοποιημένο ήχο καμία αντιληπτή διαφορά.

Αν υποθέσουμε πως ο αριθμός των δειγμάτων είναι N. Το N θα πρέπει να είναι τουλάχιστον ίσο με 88200, ώστε να υπάρχει μία στοιχειώδης ποιότητα στον ήχο. Το δείγμα του υδατογραφημένου σήματος ψ(i) δίνεται από τον τύπο:

$$\psi(i) = x(i)+f(x(i),w(i))$$

όπου x(i) κάθε Νιοστό δείγμα του αρχικού σήματος που ενσωματώνεται σ' αυτό πληροφορία w(i) τυχαίο δείγμα του σήματος του υδατογραφήματος και f(x(i), w(i)) η συνάρτηση που υπολογίζει τις βασικές ιδιότητες του ηχητικού φάσματος ώστε να αποτρέψει το υδατογράφημα να γίνει αντιληπτό από το ανθρώπινο αυτί.

Επίσης το σήμα της ποσότητας θορύβου υπολογίζεται από τον τύπο:

$$SNR = 10\log_{10}\frac{\sum_{n} x^2(n)}{\sum_{n}[x(n)-y(n)]^2}$$

Η διαδικασία ανίχνευσης του αλγορίθμου αυτού βασίζεται στο παρακάτω γινόμενο

$$S = \sum_{i=1}^{n}\psi(i)w(i) = \sum_{i=1}^{n}[x(i)w(i) + f(x(i), w(i))\cdot w(i)]$$

Αν η τυχαία γεννήτρια ω παράγει στατιστικά ίσους αριθμούς στις διακριτές τιμές εξόδου και η μέση τιμή του σήματος πιχ είναι ίση με 0 τότε ο πρώτος όρος της παραπάνω παράστασης είναι 0. Ειδάλλως αν κάποιες από τις τυχαίες τιμές της εξόδου εμφανίζονται πιο συχνά τότε παράγεται ένα Aw το οποίο πρέπει να ληφθεί υπόψιν και η παραπάνω παράσταση τροποποιείται ως εξής:

$$S = \sum_{i=1}^{n=\Delta\omega} x(i)w(i) + \sum_{i=1}^{\Delta\omega} x(i)w(i) + \sum_{i=1}^{N} f(x(i)w(i)u(i))$$

Ο πρώτος παράγοντας είναι ίσος με 0 όπως εξηγήθηκε παραπάνω. Αν δεν υπάρχει υδατογράφημα στο σήμα τότε η παράσταση ισούται:

$$S = \frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i)$$

Αλλά το x(i) δε θα ήταν καλό να χρησιμοποιηθεί στη διαδικασία ανίχνευσης μιας και αποτελεί το αρχικό σήμα. Έτσι αντικαθίσταται με το ψ(i) στους δύο τελευταίους παράγοντες παράστασης χωρίς μεγάλο σφάλμα.

Τελικά η ανίχνευση της σταθεράς r κανονικοποιείται στο 0 ή στο 1 αφαιρώντας την τιμή Δw/N|S| από το S και διαιρώντας το αποτέλεσμα με τον παράγοντα $\sum_{i=0}^{w} f(\psi(i), w(i))w(i)$. Η σταθερά ανίχνευσης r που χρησιμοποιείται στην ανίχνευση υδατογραφήματος δίνεται από τον τύπο:

$$r = \frac{S - \frac{\Delta w}{N}|S|}{\sum_{i=1}^{N} f(\psi(i), w(i))w(i)}$$

Η προτεινόμενη μέθοδος υδατογράφησης επιτρέπει την ένθεση πληροφορίας για έναν μεγάλο αριθμό υδατογραφημάτων δεν αποτρέπει την εισαγωγή θορύβου στο υδατογραφημένο σήμα, που προκαλεί ηχητική παραμόρφωση. Η παραμόρφωση αυτή σχετίζεται με το πλάτος του υδατογραφημένου σήματος. Η αύξηση του πλάτους με τη σειρά της επιφέρει και αύξηση της παραμόρφωσης. Το πρόβλημα αυτό επιλύεται καθώς με διαδκασίες δοκιμής αυξάνουμε το πλάτος και όταν παραχθεί το πρώτο υδατογράφημα που σ' αυτό εισέρχεται παραμόρφωση τότε σαν αξιόπιστο υδατογράφημα επιλέγεται το προηγούμενο. Με την παραπάνω διαδικασία το πρόβλημα περιορίζεται και επιτυγχάνεται ένα υδατογράφημα χωρίς παραμόρφωση και ταυτόχρονα δίνει έναν αρκετό αριθμό υδατογραφημάτων.

Η παραπάνω μέθοδος εμφανίζει πιθανότητα λάθους συναγερμού ακόμη και όταν χρησιμοποιείται υδατογραφημένος ήχος αλλά με λάθος κλειδί. Τέλος το υδατογράφημα αυτής της τεχνικής είναι ανθεκτικό και στις επεξεργασίες όπως φιλτράρισμα, επαναδειγματοληψία και MPEG συμπίεση.

7.3.3. Σχήμα υδατογράφησης στο πεδίο της συχνότητας

7.3.3.1 Σχήμα υδατογράφησης στο πεδίο της συχνότητας (Το αρχικό σήμα δεν απαιτείται) [28]

Ο αλγόριθμος υδατογράφησης που θα παρουσιαστεί εδώ αποτελεί ένα συμμετρικό αλγόριθμο 1bit που βασίζεται σε στατιστικές μεθόδους. Χρησιμοποιεί την επεξεργασία του σήματος με την αναπαράσταση του σε μετασχηματισμό Fourier και δεν απαιτεί το αρχικό σήμα ήχου για την αυθεντικοποίηση του υδατογραφημένου ήχου.

Διαδικασία

Η διαδικασία του βασίζεται σε δομή μπλοκ μιας και ενσωματώνει τον ίδιο ήχο υδατογράφησης ανά ίσα χρονικά διαστήματα των 1-2 δευτερολέπτων. Για να μπορέσει να γίνει καλύτερη μελέτη του αλγορίθμου υδατογράφησης θα θεωρήσουμε ότι ο αριθμός των δειγμάτων είναι 2N μιας και χρησιμοποιείται στην επεξεργασία Fourier για να πετυχαίνεται καλύτερη αναπαράσταση των συχνοτήτων.

Η διαδικασία περιλαμβάνει 4 στάδια:

1) Το κλειδί υδατογράφησης καθώς επίσης και το σήμα υδατογράφησης θα πρέπει να δημιουργούνται με τη συμβολή μιας τυχαίας γεννήτριας αριθμών. Η γεννήτρια αριθμών χρησιμοποιείται για τη δημιουργία δύο ψευδοτυχαίων υποσυνόλων A και B που σχετίζονται μεταξύ τους και περιέχουν ίδιο αριθμό στοιχείων M (M<=N) από το αρχικό σήμα. Τα δύο διανύσματα α, β ορίζονται σαν τα διανύσματα που αντιστοιχούν στα στοιχεία των δύο υποσυνόλων (A και B) αντίστοιχα.

2) Ορίζονται δύο υποθέσεις, η υπόθεση ελέγχου (H_0) για την περίπτωση που το υδατογράφημα δεν είναι ενσωματωμένο στο ηχητικό προϊόν και η εναλλακτική υπόθεση (H_1) για την περίπτωση όπου το υδατογράφημα υπάρχει στον ήχο. Επιπλέον χρησιμοποιούνται 2 φόρμουλες που βασίζονται στον έλεγχο με βάση τα στατιστικά στοιχεία και μία συνάρτηση F(z) όπου z η στατιστική φόρμουλα. Υπάρχουν λοιπόν δύο τύποι λαθών

$$I: \int_{T}^{+\infty} \phi(z)dz = P_I$$

$$II: \int_{-\infty}^{T} \phi_m(z)dz = P_{II}$$

Προφανώς η P_I αντιστοιχεί στην υπόθεση H_1 και σηματοδοτεί την πιθανότητα λάθους ανίχνευσης υδατογραφήματος ενώ δεν υπάρχει. Η P_{II} αντιστοιχεί στη υπόθεση H_0 και σηματοδοτεί την πιθανότητα λάθους απόρριψης ενώ το υδατογράφημα υπάρχει στον ήχο.

3) Η πιθανότητα λάθους $1\text{-}P_I$ με τη βοήθεια των τύπων του μετασχηματισμού Fourier και την ύπαρξη ενός διανύσματος παραμέτρων $\vec{k}$ μεγέθους 2N υπολογίζεται από τον παρακάτω τύπο.

$$\int \phi_m\left(f\left(e_A\left(\vec{a},\vec{b},\vec{k}\right), e_B\left(\vec{a},\vec{b},\vec{k}\right)\right)\right)dz = P_{II}$$

4) Έπειτα γίνεται η τυχαία επιλογή κάποιων στοιχείων $a_i \in A$ και $b_i \in B$ τα οποία τροποποιούνται από τη συνάρτηση της ένθεσης του υδατογραφήματος e_A , e_B αντίστοιχα:

$$a_i = e_A\left(\vec{a},\vec{b},\vec{k}\right),\ b_i = e_B\left(\vec{a},\vec{b},\vec{k}\right),\ i = 1,...,M$$

Η επεξεργασία των a_i και b_i γίνεται με τέτοιο τρόπο ώστε η πιθανότητες λάθους να παραμένουν σε ένα περιοριστικό επίπεδο ενώ ταυτόχρονα η επεξεργασία αυτή να μη γίνεται ηχητικά αντιληπτή.

Διαδικασία Ανίγνευσης

Η διαδικασία ανίχνευσης γίνεται με τη βοήθεια των παρακάτω διαπιστώσεων:

- Το κάθε ιδιωτικό κλειδί και το υδατογράφημα καθορίζουν την επιλογή εκείνων των στοιχείων που θα τροποποιηθούν ορίζοντας τα υποσύνολα A και B.
- Η πιθανότητα να απορριφθεί ένα προϊόν με βάση τη ύπαρξη υδατογραφήματος σ' αυτό, όταν όντως δεν έχει ενσωματωθεί σ' αυτό υδατογράφημα είναι $1 - P_i$. Η πιθανότητα αυτή μπορεί να υπολογισθεί.
- Αν ένα δείγμα θα επιλεγεί για να μορφοποιηθεί ελέγχεται από το σ του δείγματος E(Z) και αν το E(Z) <= T το υδατογράφημα δεν ενθέτεται σ' αυτό. Η τεχνική αυτή της υδατογράφησης στηρίζεται στο ότι το υδατογραφημένο προϊόν πρέπει να είναι αξιόπιστο τόσο ως προς την ποιότητα ός και ως προς την ασφάλεια και την ανθεκτικότητα.

Η αξιοπιστία του υδατογραφήματος ελέγχεται μέσω των συναρτήσεων πιθανότητας. Έχει προστεθεί λοιπόν ακόμη και η πιθανότητα όταν κάποιος προβλέψει - ανιχνεύσει κρυφή πληροφορία (παράγοντες) με διάφορες επεξεργασίες του ήχου ή με στατιστικές μεθόδους η ασφάλεια να παραμένει σε ψηλά επίπεδα. Ο αλγόριθμος είναι ανθεκτικός ακόμη και στις επεξεργασίες ήχου όπως το MPEG-1 layer 2 στη συμπίεση, σε χαμηλό-ύψο περατά φίλτρα της επαναδειγματοληψίας και τον επανακβαντισμό του υδατογραφημένου ήχου.

7.3.3.2 Σχήμα υδατογράφησης στο πεδίο συχνότητας που απαιτεί το αρχικό προϊόν [19], [4]

Αρχικά πρέπει να υπολογισθεί το κατώφλι της μάσκας που θα εφαρμόσουμε. Ο υπολογισμός γίνεται χρησιμοποιώντας το MPEG. Ο υπολογισμός του κατωφλίου του

φίλτρου γίνεται σε διαδοχικά κομμάτια του ήχου και έπειτα κάθε τμήμα ζυγίζεται από ένα Hamming παράθυρο. Μ' αυτό τον τρόπο το υδατογράφημα ενθέτεται στο ηχητικό σήμα με τρόπο που δε γίνεται αντιληπτό ενώ ταυτόχρονα μπορεί να ανιχνευθεί εύκολα λόγω των ειδικών χαρακτηριστικών των PN ακολουθιών.

Το σχήμα υδατογράφησης είναι ανθεκτικό στο θόρυβο που εισέρχεται σ' ένα ψηφιακό σήμα, την συμπίεση με απώλεια δεδομένων, την επαναδειγματοληψία και την χρονική πολυπλεξία. Τα αποτελέσματα της τεχνικής βασίζονται στην εκμετάλλευση του MPEG1 ακουστικού συστήματος των PN ακολουθιών και στο συχνοτικό παράθυρο MPEG

Το ανθρώπινο αυτί λειτουργεί σαν ένας αναλυτής συχνοτήτων μιας και αντιλαμβάνεται τους ήχους με βάση τις συχνότητες που κυμαίνονται από 10Hz εως 15Khz. Το ανθρώπινο ακουστικό σύστημα μπορεί να μοντελοποιηθεί από ένα σετ από 26 ζωνοπερατά φίλτρα των οποίων το εύρος ζώνης αυξάνει με την αύξηση της συχνότητας. Οι 26 ζώνες είναι γνωστές και ως κρίσιμες ζώνες (0-15500).

Οι κρίσιμες ζώνες προσδιορίζονται γύρω από την κεντρική συχνότητα. Ο ρόλος της κεντρικής συχνότητας συμβάλει ενισχυτικά στο θόρυβο αυξάνοντας το εύρος του έως ότου υπάρξει αντιληπτή διαφορά ήχου στον τόνο το κέντρο της συχνότητας.

Γι' αυτό το λόγο ένας ασθενής τόνος που εξαπλώνεται στις κρίσιμες ζώνες που επικαλύπτεται από έναν ισχυρότερο τόνο ο ασθενής τόνος δε θα γίνει αντιληπτός.

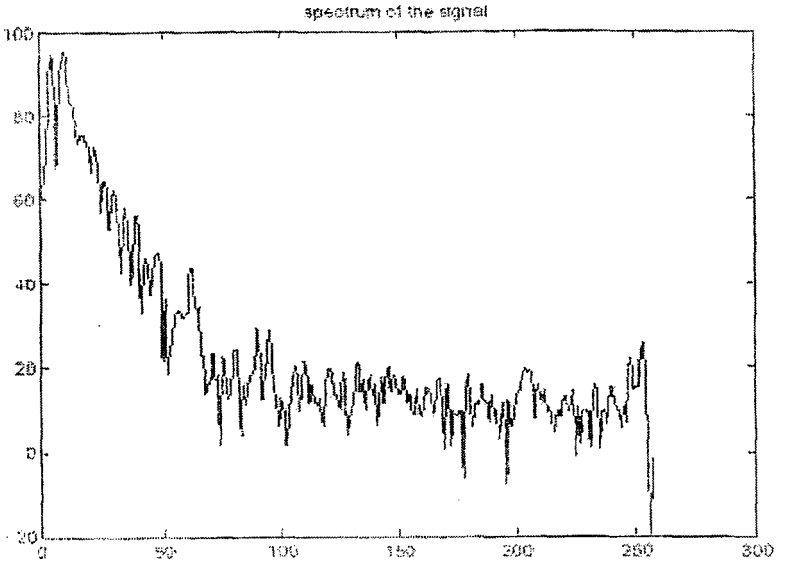
Οι συχνότητες των μοντέλων που εφαρμόζουν μάσκα έχουν ήδη προσδιορισθεί για τη διαφανή κωδικοποίηση των ηχητικών σημάτων, ώστε να μην υπάρξει κωδικοποίηση άσχετης πληροφορίας. Ενα τέτοιο μοντέλο είναι το MPEG1. Τα βήματα για την εφαρμογή μάσκας του MPEG1 μοντέλου είναι τα παρακάτω(32ΚΗζ ρυθμός δείγματος).

1) Σε κάθε 16 ms δείγματος του ηχητικού σήματος λαμβάνονται 512 δείγματα s(n) και ζυγίζονται από ένα Hannigton παράθυρο

$$h(n): h(n) = \frac{\sqrt{8/3}}{2}\left(1 - \cos\left(2\pi \frac{n}{N}\right)\right)$$

Το ενεργειακό φάσμα του σήματος s(n) υπολογίζεται από τον τύπο:

$$S(k) = 10\log_{10}\left[\frac{1}{N}\sum_{n=0}^{N-1} S(n)h(n)e^{\left(-j2\pi\frac{nk}{N}\right)}\right]$$



Εικόνα 43 **Το Φασματικό Εύρος του Σήματος**

2) Αναγνώριση των τονικών σημάτων. Η αναγνώριση των τονικών (πληροφορία) και τον μη τονικών (θόρυβος) του σήματος είναι απαραίτητη γιατί τα μοντέλα μάσκας είναι διαφορετικά. Το τονικό περιεχόμενο του ήχου είναι τοπικό μέγιστο στο εύρος του δηλ.:

$$S(k) > S(k+1), k!S(k) \geq S(k-1)$$

$$S(k) - S(++j) \geq 7dB$$

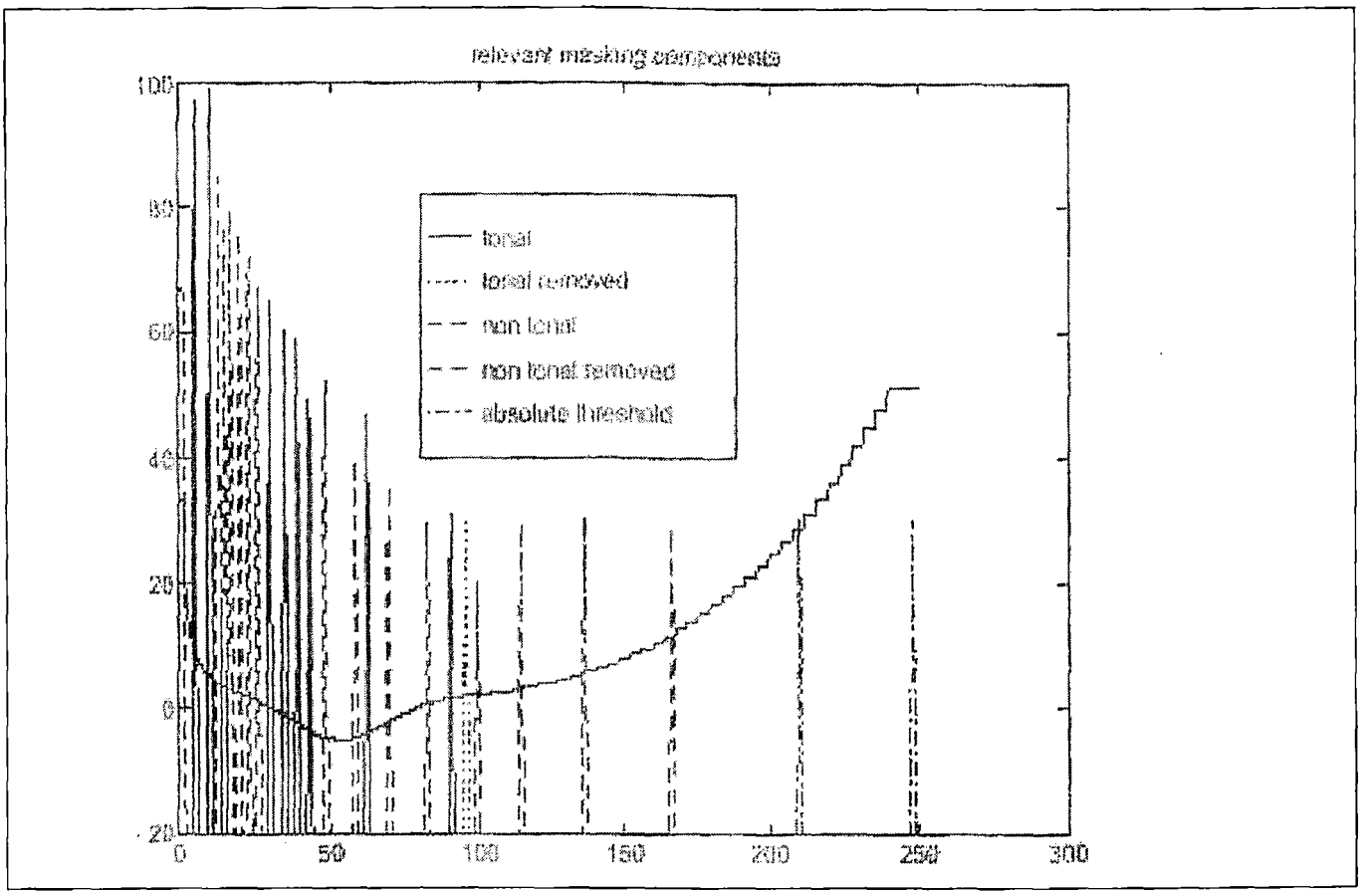
$$\psi \in [-2,2], \text{ εάν } 2<k<63$$

$$\psi \in [-3,-2,2,3], \text{ εάν } 63 < k < 127$$

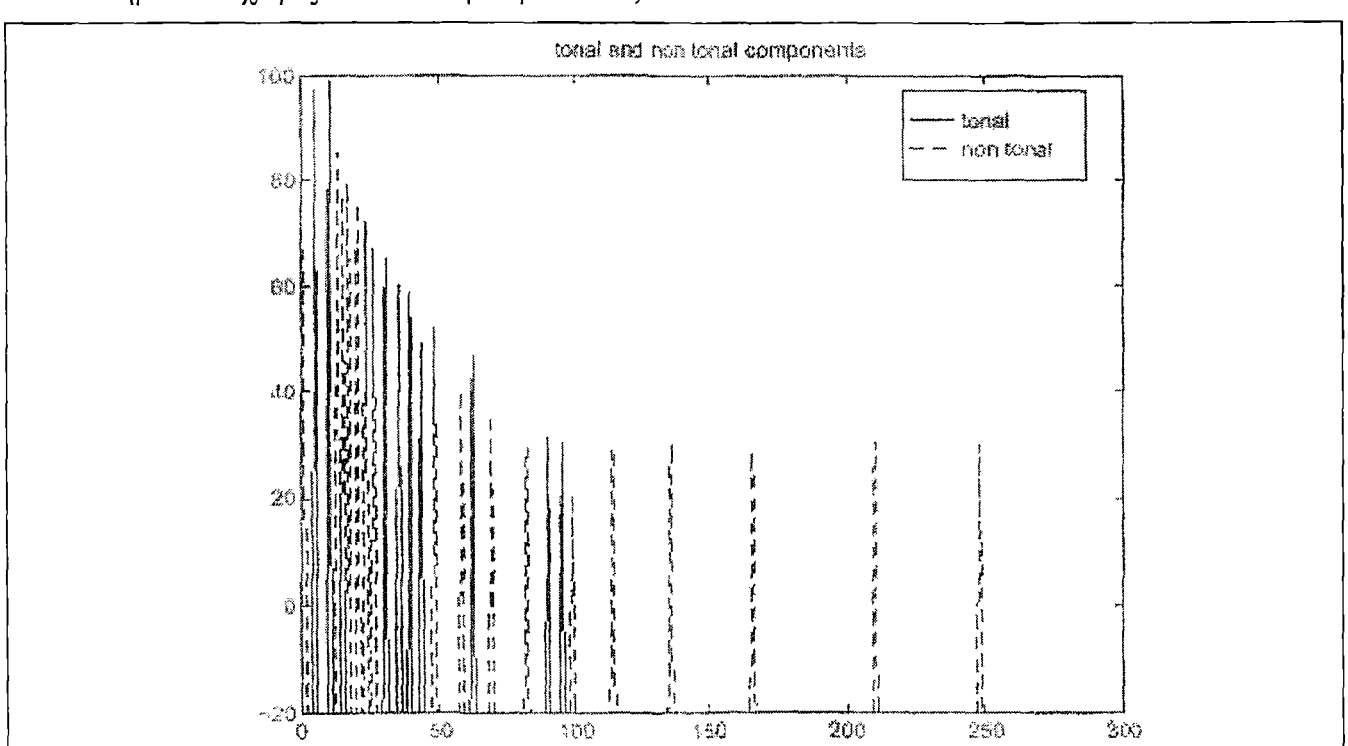
$$\psi \in [-6...-2, 2,...6], \text{ εάν } 127<k<250$$

Προσθέτουμε σε κάθε ένταση σημείου την ένταση των προηγούμενων και των επόμενων σημείων. Τα υπόλοιπα τονικά σημεία στο ίδιο εύρος δε μας ενδιαφέρουν.

Τα μη τονικά σημεία υλοποιούνται από το άθροισμα των εντάσεων των σημείων του σήματος που παραμένουν σε κάθε μία από τις 26 κρίσιμες ζώνες μεταξύ 0 και 15500Hz. Αυτά τα «ηχητικά φίλτρα» μπορεί να υπολογισθούν από ορθοκανονικά φίλτρα αυξάνοντας τη συχνότητα.



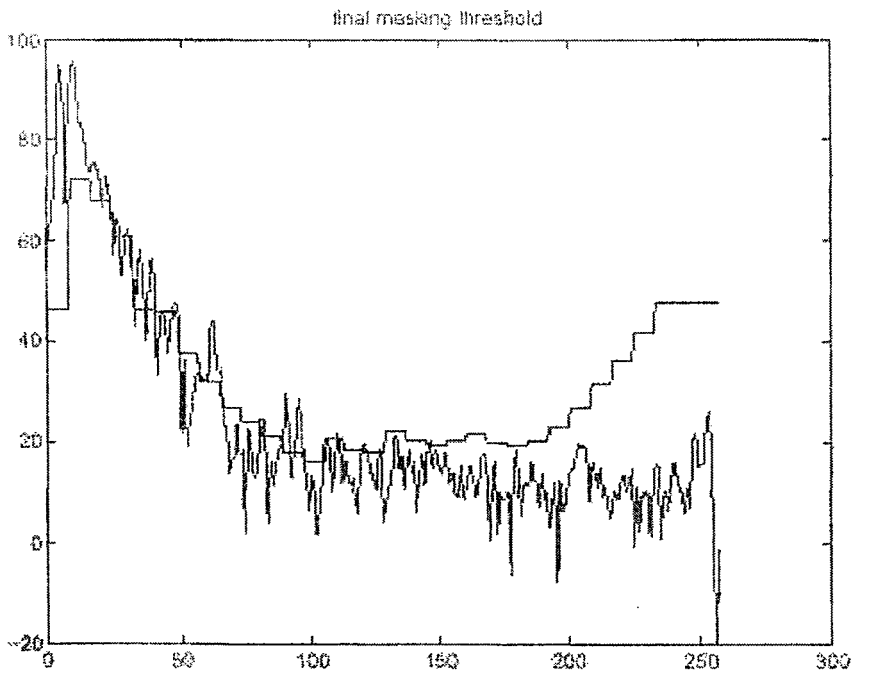
Αυτά τα τονικά σημεία (περιεχόμενα) από το απόλυτο ακουστικό φάσμα και τα τονικά σημεία διαχωρίζονται σε λιγότερα από 0,5 Barks.



Εικόνα 44 **Η Τονική και μη Τονική Πληροφορία του Ήχου**

3) Σ' αυτό το βήμα υπολογίζουμε για τα συχνοτικά χαρακτηριστικά του

ανθρώπινου ακουστικού συστήματος (HAS) . Για να γίνει αυτό χρειαζόμαστε να διακριτοποιήσουμε τον άξονα της συχνότητας σύμφωνα με την ακουστική ευαισθησία η οποία είναι καλύτερη για μικρές συχνότητες.



Εικόνα 45 **Τελική τιμή του Κατοφλίου με βάση το Αρχικό Σήμα**

Οι καμπύλες απόκρυψης (masking curves) είναι τώρα σχεδόν γραφικές (μεδιαφορετικές χαμηλότερες και υψηλότερες διακύμανσης που εξαρτώνται από την απόσταση του στοιχείου που αποκρύπτει ή αποκρύπτεται (masking and masked component) και εξαρτάται από περιεχόμενα διαφορετικά για τα τονικά και μη τονικά χαρακτηριστικά.

Χρησιμοποιούμε το F_i για να συμβολίζουμε το σετ συχνοτήτων που παρουσιάζονται στο σήμα δοκιμής. Το καθολικό εύρος ζώνης για κάθε συχνότητα f2 χρησιμοποιεί στον υπολογισμό το απόλυτο ηχητικό εύρος ζώνης S_0 και τις καμπύλες P_2 τονικών στοιχείων και N_n μη τονικών στοιχείων.

Το εύρος ζώνης της μάσκας είναι τώρα το ελάχιστο του τοπικού εύρους ζώνης και του απόλυτου κατωφλίου για καθεμία από τις 32 ίσου πλάτους υποζώνες του φάσματος.

Χρησιμοποιούμε το f_1 για να συμβολίσουμε το σετ των συχνοτήτων στο σήμα δοκιμής και f_2 για να συμβολίζουμε το κατώφλι των συχνοτήτων ώστε να υπολογιστεί το απόλυτο ακουστικό κατώφλι s_a.

Και πεδίο για την καμπύλη μάσκας των N_t τονικών περιεχομένων και N_n μη τονικών. Για να μην είναι αντιληπτό το υδατογράφημα, το απόλυτο κατώφλι για κάθε συχνότητα f_2 πρέπει να πέσει κάτω από το κατώφλι μάσκας:

$$S_m(f_2) = 10 \cdot \log_{10}\left[10^{S_a(f_2)/10} + \sum_{j=1}^{N_L} 10^{P_2(f_2, f_1, p_1)/10} + \sum_{j=1}^{N_H} 10^{P_2(f_2, f_1, p_1)/10}\right]$$

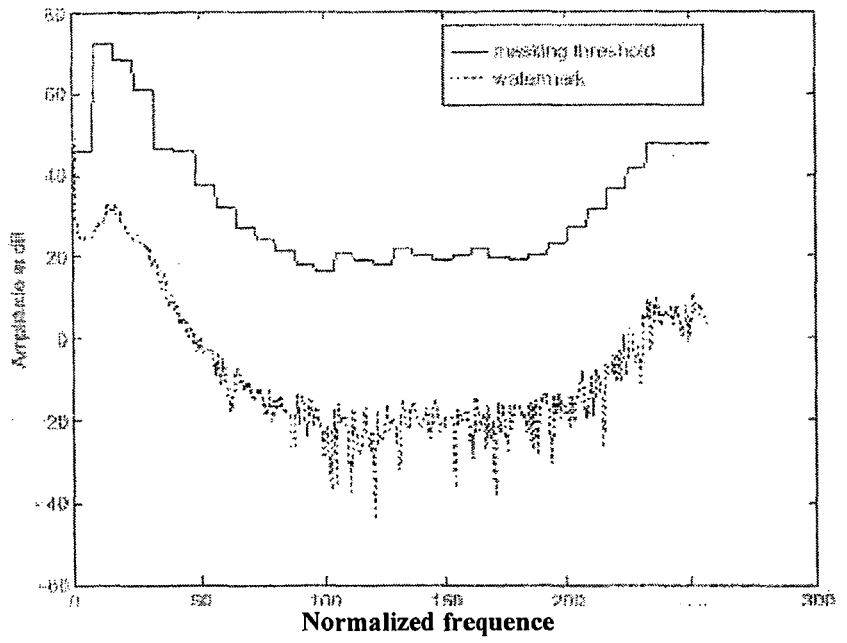
Ψευδοτυχαίες ακολουθίες (Pn sequences)

Οι PN [4], [18] ακολουθίες χρησιμοποιούνται από τον αλγόριθμο υδατογράφησης γιατί είναι ένας εύκολος τρόπος για να παραχθούν διακριτοί αριθμοί και να γίνει αξιόπιστη αναγνώριση του υδατογραφήματος. Σαν τυχαίες δυαδικές ακολουθίες οι PN ακολουθίες έχουν «0» και «1» ισοπίθανα.

Τα χαρακτηριστικά που προσδιορίζουν τις PN ακολουθίες είναι η μεγάλη ανθεκτικότητα τους στον ήχο και οι ιδιότητα αυτοσυσχέτησης .Η χρήση των PN ακολουθιών είναι ευρεία και εφαρμόζεται σε πολλές τεχνικές όπως η τεχνική διεσπαρμένου φάσματος που χρησιμοποιείται στις τηλεπικοινωνίες. Η ευρεία χρήση τους ακόμη και από εφαρμογές που δεν εμπλέκονται με σχήματα προστασίας χρησιμοποιεί τις ικανότητες που περικλείουν οι PN ακολουθίες ώστε να μπορεί να γίνει επιτυχής αναγνώριση μεταδιδόμενων ηχητικών δεδομένων παρόλο την παρουσία θορύβου ευρέως φάσματος.

Τα ηχητικά σήματα που χαρακτηρίζονται από διασκορπισμένο φάσμα είναι ανθεκτικά στην παρεμβολή γεγονός που τα κάνει πολύτιμα για μεταφορά μέσω του παγκόσμιου ιστού καθώς σε τέτοια περιβάλοντα τα δεδομένα υφίστανται πολύ θόρυβο που εισέρχεται σ' αυτά από το κανάλι μετάδοσης.

Οι PN ακολουθίες είναι ένας περιοδικός θόρυβος με δυαδική αναπαράσταση η οποία χρειάζεται για την παραγωγή της μόνο modulo2 αθροιστές. Η τυχαία παραγωγή 1 ή 0 με συγκεκριμένο ρυθμό αποτελεί την PN ακολουθία.



Εικόνα 46 **Εφαρμογή του Κατωφλίου στην PN Ακολουθία και Κανονικοποίηση**

Η ύπαρξη των modulo2 αθροιστών για την παραγωγή της αποτρέπει τη μηδενική κατάσταση δηλ την παραγωγή στην έξοδο μόνο μηδενικών κατά τη δημιουργία της PN ακολουθίας. Η μέγιστη περίοδος μιας PN ακολουθίας είναι

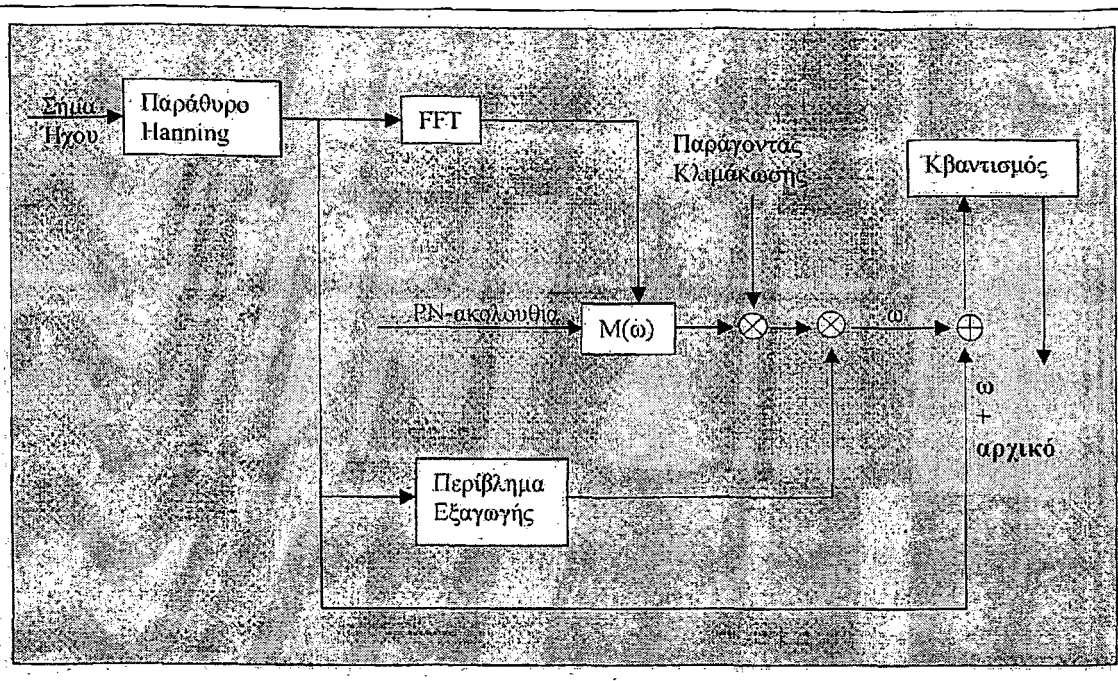
$$N=2^m-1$$

Οι PN ακολουθίες εφαρμόζονται και στο υδατογράφημα γιατί αποτελούν έναν εύκολο τρόπο παραγωγής ενός τυχαίου και διακριτού διάδικου σήματος που μπορεί να πιστοποιήσει την κυριότητα του ιδιοκτήτη.

Οι PN ακολουθίες αποτελούνται από τυχαίο ισοπίθανο αριθμό 0 και 1 ενώ ταυτόχρονα τα ιδιαίτερα χαρακτηριστικά της PN ακολουθίας διευκολύνουν τόσο την διαδικασία παραγωγής αλλά και την ανίχνευση του υδατογραφήματος.

Η συνάρτηση αυτοσυσχέτισης έχει περίοδο N και είναι περιοδική πράγμα που δημιουργεί ένα αυτοσυντονιζόμενο σήμα με συχνότητα m. Δίνεται η δυνατότητα λοιπόν τα δεδομένα που ενθέτονται να μπορούν να συγχρονισθούν και κατά τη διαδικασία της ανίχνευσης. Το γεγονός αυτό έχει βαρύνουσα σημασία και διευκολύνει αρκετά τη διαδικασία ανίχνευσης ιδιαίτερα όταν το ηχητικό υδατογραφημένο σήμα επαναδηγματοληπτείται ή υφίσταται άλλες μορφές επεξεργασίας.

Διαδικασία ένθεσης

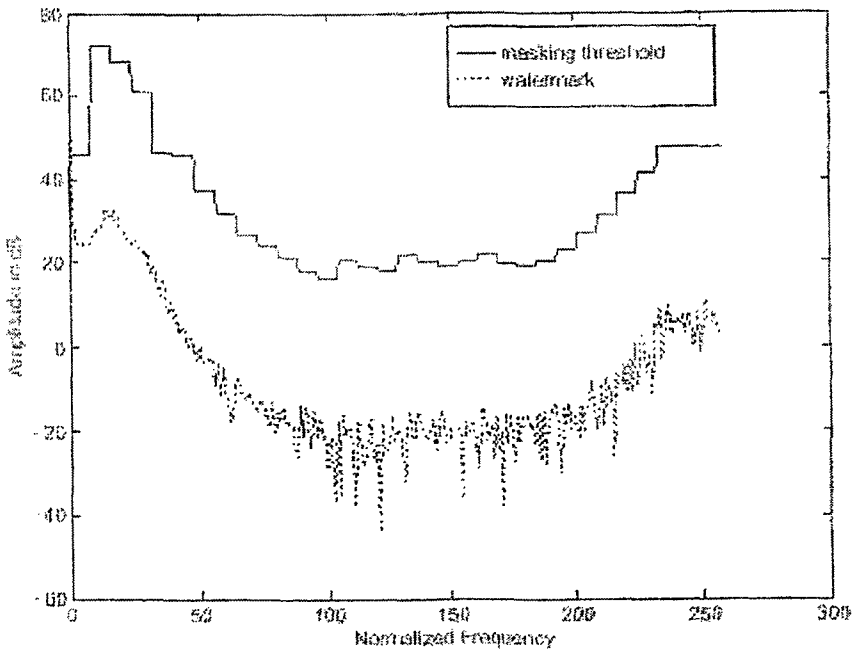


Εικόνα 47 **Παραγωγέας Υδατογραφήματος : Πρώτο στάδιο για ήχο**

Κάθε σήμα υδατογράφησης πρέπει να χαρακτηρίζεται με ένα μοναδικό κλειδί. Στην τεχνική αυτή η μοναδικότητα εξασφαλίζεται από την PN ακολουθία η οποία φιλτράρεται σύμφωνα με το MPEG2 [41], [43] ακουστικό ανθρώπινο σύστημα.

Για την παραγωγή του υδατογραφήματος ακολουθούμε τα εξής στάδια:

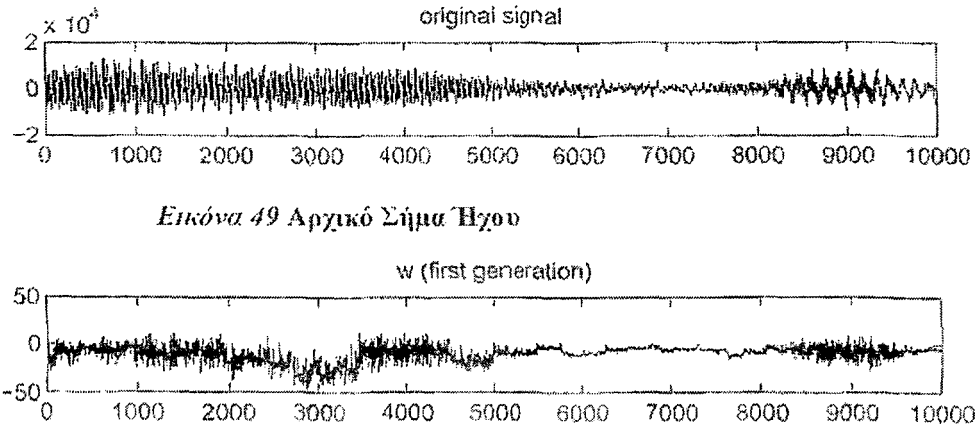
1) Αρχικά υπολογίζεται το κατώφλι της μάσκας που θα εφαρμοσθεί στην PN ακολουθία. Το κατώφλι υπολογίζεται με την τεχνική MPEG1 [4]. Ετσι υπολογίζεται το όριο φράγματος για κάθε κομμάτι του ήχου συνήθως το κάθε κομμάτι του ήχου περιέχει 512 δείγματα. Κάθε τμήμα ζυγίζεται από το Harming παράθυρο και τα διαδοχικά μπλοκ (blocks) επικαλύπτονται κατά 50 τις εκατό. Το κατώφλι της μάσκας υπολογίζεται με το δέκατο σε σειρά των πόλων του φίλτρου M(w) χρησιμοποιώντας το ελάχιστο τετραγωνικό κριτήριο (μέθοδος ελαχίστων τετραγώνων). Μ' αυτό τον τρόπο η συχνότητα seq(w) της PN ακολουθίας τροποποιείται από το κατώφλι της μάσκας M(w) ώστε το επίπεδο του φάσματος να παραμένει κάτω από το κατώφλι της μάσκας.



Εικόνα 48 **Το Φασματικό Εύρος της PN σε σχέση με την εφαρμογή μάσκας**

Το σήμα που προκύπτει από το φίλτρο αποτελεί το κλειδί της τεχνικής της υδατογράφησης, είναι μοναδικό και ταυτόχρονα εμποδίζει την παρεμβολή των χρονικών χαρακτηριστικών, όπως προ-ήχος. Το υδατογράφημα προστίθεται στο σήμα

λΥπρώτου σταδίου=(πραγματικό σήμα + w) όπου w δηλώνει την PN ακολουθία κάτω από το επίπεδο της μάσκας.



Εικόνα 49 **Αρχικό Σήμα Ήχου**

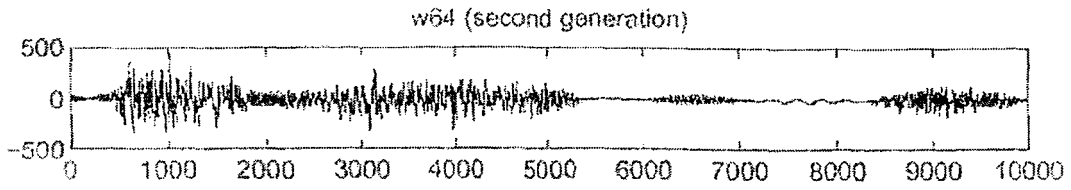
Εικόνα 50 **Υδατογάφημα πρώτου σταδίου**

2) Για να μπορεί το υδατογράφημα να παραμένει μη αντιληπτό από το ανθρώπινο αυτί πρέπει να δημιουργήσουμε το w64 [4]. Η δημιουργία του ω64 σημαίνει ότι το σήμα κωδικοποιείται και αποκωδικοποιείται στα 64Kps/second

W64 = (\νπρώτ0 στάδιο) 64-(Αρχικό σχήμα) 64

Η παραγωγή του w64 είναι απαραίτητη γιατί το υδατογράφημα πρέπει να εισέλθει εκεί που υπάρχει σημαντική πληροφορία του ήχου που είναι αντιλιπτή απο το χρήστη. Αν δεν υλοποιηθεί η σωστή ενσωμάτωση του υδατογραφήματος θα υπάρξει σφάλμα στη

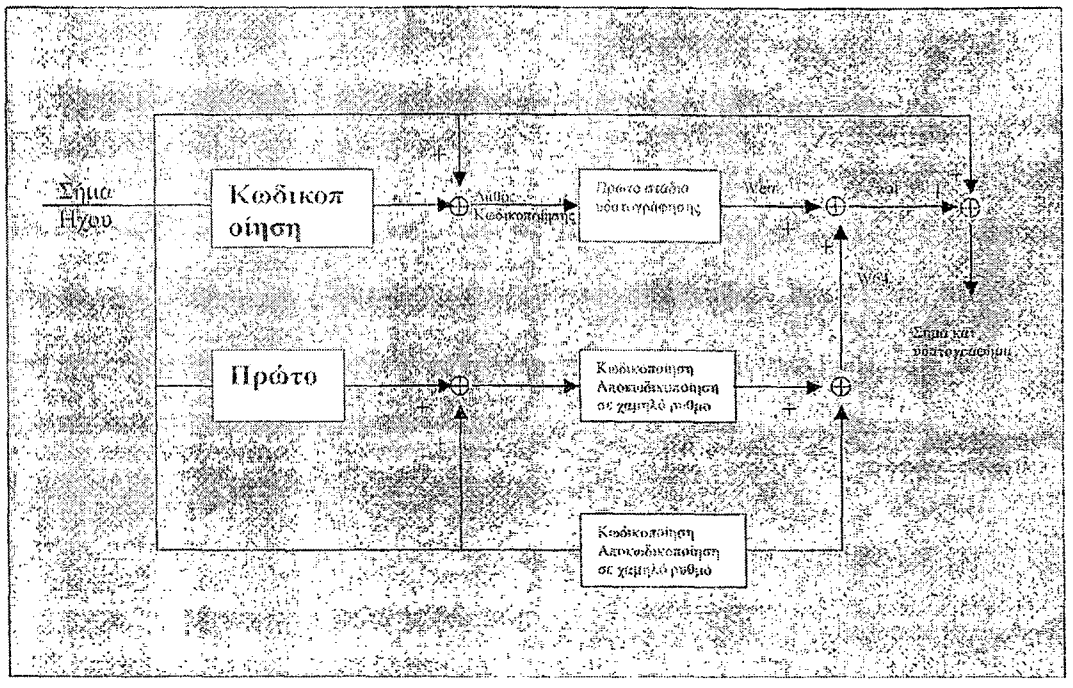
διαδικασία υδατογράφησης.



Εικόνα 51 **Κωδικοποιημένη Μορφή Υδατογραφήματος**

3) Παραγωγή Werr = (Αρχικό σχήμα)-(Αρχίκό σχήμα)64.

4) Και το τελικό υδατογράφημα είναι wat=W64+werr



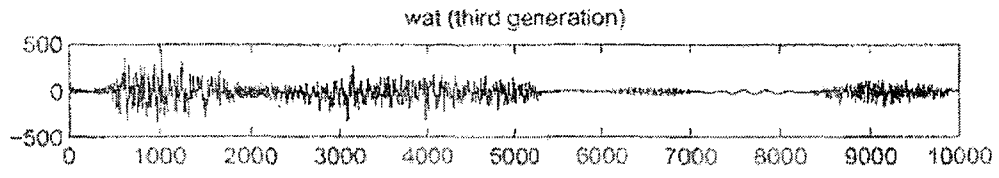
Εικόνα 52 **Πλήρης Παραγωγέας Υδατογραφήματος για ήχο**

Ανίχνευση Υδατογραφήματος

Κατά τη διαδικασία ανίχνευσης του υδατογραφήματος απαιτείται το αρχικό σήμα και φυσικά το κλειδί της διαδικασίας δηλαδή η PN ακολουθία. Η μέθοδος της ανίχνευσης ελέγχει αν η διαφορά που υπάρχει στον υπο έλεγχο ήχο και στο αρχικό σήμα οφείλεται απλά στην ύπαρξη θορύβου ή στην αλλαγή του υδατογραφήματος. Οι υποθέσεις που γίνονται είναι δύο.

$$\mathbf{H0: x(t)=r(t)-s(t)=n(t)}$$
$$\mathbf{Hi: x(t)=r(t)-s(t)=w(t)+n(t)}$$

Μία λύση για την πιστοποίηση της ύπαρξης πειραματικού προϊόντος είναι ησυσχέτιση του σήματος χ(ί) με το ω με χρήση κατωφλίου.



Εικόνα 53 **Υδατογράφημα του Τελικού Σταδίου Παραγωγής**

Η επιλογή διαφορετικών PN ακολουθιών αποτελεί ένα μηχανισμό που αποτρέπει σε μεγάλο βαθμό την πειρατεία και αν η PN ακολουθία είναι αρκετά μεγάλη μπορεί να ενισχύει την ασφάλεια του κλειδιού, όμως δημιουργεί αυξημένη πολυπλοκότητα και κάνει αρκετά πιο δύσκολη τόσο την διαδικασία ένθεσης όσο και την ανίχνευση.

7.4 Γενικές Τεχνικές για την Υδατογράφηση ήχου

7.4.1 Υδατογράφηση του μικρότερου διαδίκου ψηφίου (Low Bit Coding) [1]

Η μέθοδος της υδατογράφησης του μικρότερου διάδικου ψηφίου (low bit coding) αποτελεί μία από πιο απλές μεθόδους υδατογράφησης αρχείων ήχου. Στη μέθοδο αυτή η ένθεση του υδατογραφήματος γίνεται με την αντικατάσταση του λιγότερο σημαντικού διαδίκου ψηφίου.

Η αλλαγή αυτή έχει ως αποτέλεσμα την ενσωμάτωση μεγάλης ποσότητας πληροφορίας καθώς σε κάθε byte πληροφορίας εντίθεται από ένα διάδικο ψηφίο του υδατογραφήματος. Έτσι επιτυγχάνεται η χρήση μεγάλης χωρητικότητας στο ίδιο κανάλι μιας και τα δεδομένα που αναπαρίστανται σ' αυτό αυξάνουν. Με τον τρόπο λοιπόν αυτό μπορεί να επιτευχθεί η μετάδοση περισσότερης πληροφορίας ανά μονάδα εύρους ζώνης. Με τη μέθοδο αυτή μπορεί να μεταφερθεί 1Kbps ανά 1KHz.

Η μετάδοση περισσότερης πληροφορίας ανά ηχητικό κανάλι αντιπαρατίθεται με την εισαγωγή αξιοσημείωτου θορύβου που επιφέρει η τεχνική αυτή. Η επίδραση του θορύβου σ' ένα ηχητικό αρχείο μπορεί να έχει αρκετά δυσάρεστες συνέπειες. Στην τεχνική που υδατογραφούμε το λιγότερο σημαντικό ψηφίο, ο θόρυβος που εισέρχεται λόγω της υδατογράφησης δεν είναι σημαντικός καθώς το λιγότερο σημαντικό ψηφίο αντιστοιχεί σε συχνότητα χαμηλής ενέργειας και πολές φορές καλύπτεται απο θορύβους που υπάρχουν στο περιβάλον. Ετσι π.χ ένας ήχος από το θόρυβο ενός πλήθους που ζητωκραυγάζει επικαλύπτει τον ήχο του λιγότερου σημαντικού ψηφίου αντίθετα ένας καθαρός τονικό ήχος όπως ενός κουαρτέτο εγχόρδων δε θα επέφερε το ίδιο αποτέλεσμα.

Η υδατογράφηση επιφέρει αρκετό θόρυβο σε συχνοτικές περιοχές με μεγάλη ενέργεια. Για να επιλυθεί το πρόβλημα αυτό εξασθενούμε το υπο υδατογράφηση σήμα. Ο περιορισμός της ενέργειας του σήματος μετά την ένθεση του υδατογραφήματος είναι εφικτός με διάφορες τεχνικές επεξεργασίας ήχου όπως φίλτρα.

Ένα από τα βασικά μειονεκτήματα της μεθόδου αυτής είναι η μικρή ανθεκτικότητα της στους μετασχηματισμούς. Ο ήχος κατά τη μετάδοση του μπορεί να υποστεί αρκετούς μετασχηματισμούς, οι οποίοι μπορούν να αλλοιώσουν τον υδατογραφημένο ήχο ή ακόμη και το προϊόν. Στο δίκτυο κατά τη μεταφορά του ήχου πολλές φορές

εισέρχεται σ' αυτόν θόρυβος από το κανάλι, ο οποίος επικαλύπτει το υδατογράφημα. Επίσης μορφές επεξεργασίας όπως η επαναδειγματοληψία τροποποιούν το υδατοργαφημένο προϊόν σε τέτοιο βαθμό ώστε το υδατογράφημα να αλλοιωθεί. Ακόμη και στις συνηθισμένες επεξεργασίες ήχου το υδατογράφημα όταν εντίθεται στο λιγότερο σημαντικό ψηφίο, δεν παραμένει ή αλλοιώνεται.

Για να μπορέσει να γίνει το υδατογράφημα πιο ανθεκτικό, επιλέγεται η αύξηση του ρυθμού δεδομένων που υδατογραφούνται ώστε ακόμη και απώλεια ή η αλλοίωση κάποιων να μη επιφέρει την αφαίρεση του υδατογραφήματος. Η αύξηση του ρυθμού δεδομένων που υδατογραφούνται ελαττώνει την ποιότητα του υδατογραφημένου ήχου και εισέρχεται στο προϊόν επιπλέον θόρυβος γι' αυτό θα πρέπει να κρατιέται σ' ένα επίπεδο.

Λόγω των παραπάνω σοβαρών δυσμενών παραγόντων η μέθοδος αυτή χρησιμοποιείται μόνο σε μέσα μετάδοσης που διατηρούν τον ήχο σε ψηφιακή μορφή κατά την μετάδοση από τον εκπομπό έως τον δέκτη.

7.4.2 Υδατογράφηση φάσης

Η υδατογράφηση φάσης [1], [18] στηρίζεται στην αντικατάσταση της φάσης των ηχητικών δεδομένων με μια νέα τροποποιημένη φάση. Η τροποποίηση της φάσης των δειγμάτων ήχου γίνεται με τέτοιο τρόπο ώστε η διαφορά φάσης μεταξύ διαδοχικών δειγμάτων, να παραμένει ίδια, ενω στην φάση του κάθε δείγματος ξεχωριστά, προστίθεται μια φάση αναφοράς. Ο στόχος αυτός επιτυγχάνεται από πιο περίπλοκη υλοποίηση αφού η παραποίηση της φάσης επιδρά στην ακουστική του ήχου σε πολύ πιο μεγάλο βαθμό από ότι η αλλαγή στο μέτρο του ηχητικού σήματος.

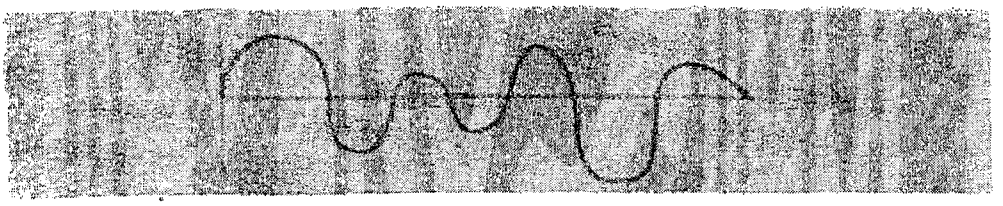
Αρχικά θα πρέπει η αναπαράσταση του ήχου να γίνει με βάση τη φάση του ηχητικού σήματος. Η υδατογράφηση φάσης αντικαθιστά τη φάση ενός αρχικού κομματιού του ήχου με μια άλλη που αναπαριστά τα δεδομένα. Ενώ η φάση στα γειτονικά τμήματα ήχου τροποποιείται με τέτοιο τρόπο ώστε η σχετική φάση μεταξύ των κομματιών να παραμένει ίδια.

Η μέθοδος αυτή μπορεί να απαιτεί μεγαλύτερη πολυπλοκότητα από την υδατογράφηση του μικρότερου σημαντικού ψηφίου, αλλά υπερέχει ξεκάθαρα. Η υδατογράφηση φάσης αποτελεί μία ευρέως διαδομένη μέθοδο και είναι πολύ αποτελεσματική γιατί το υδατογραφημένο σήμα χαρακτηρίζεται από μεγάλο λόγο σήματος προς θόρυβο.

Επειδή στη φάση δεν εισέρχεται θόρυβος, η επεξεργασία της είναι ανθεκτική. Παρολαυτά αν δεν προσεχθεί να διατηρηθεί η διαφορά μεταξύ των σημάτων του ήχου τότε η διαφορά μεταξύ αρχικού και υδατογραφημένου σήματος μπορεί να γίνει αντιληπτή. Αποφεύγεται λοιπόν η μεγάλη αύξηση της σχετικής φάσης μεταξύ των τμημάτων, καθώς θα επιφέρει αλλοίωση του παραγόμενου ήχου.

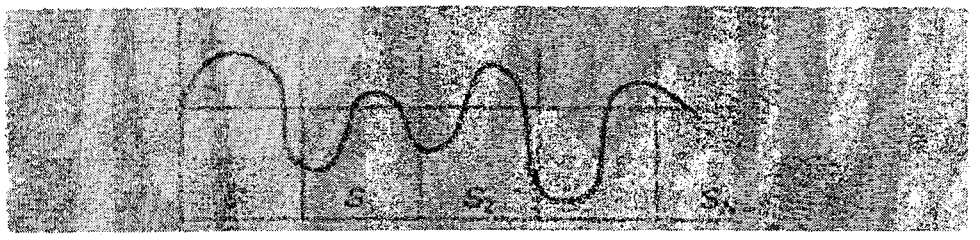
Η ανθεκτικότητα του υδατογραφημένου σήματος είναι ικανοποιητική σε συνηθισμένες μορφές επεξεργασίας. Βέβαια αυτό δεν επιτυγχάνεται σε κάθε μορφή επεξεργασίας αλλά για υδατογράφηση που τροποποιεί ελάχιστα τη φάση ο θόρυβος που εισάγει το υδατογράφημα παραμένει μη αντιλυπτός από τον κοινό χρήστη.

Διαδικασία ένθεσης



Εικόνα 54 Α) ΑΡΧΙΚΟ ΣΗΜΑ ΗΧΟΥ

1) Αρχικά ο ψηφιακός ήχος θα πρέπει να αναπαρασταθεί με βάση τη φάση. Έτσι σπάμε το σήμα σε N διαφορετικά κομμάτια. Ο αριθμός N δεν πρέπει να είναι αρκετά μεγάλος γιατί η μεγάλη αύξηση του N συμβάλει και στην αύξηση της πολυπλοκότητας της διαδικασίας. Αντίθετα θα πρέπει να είναι αρκετός ώστε οι παρακάτω επεξεργασίες να είναι εφικτές και αξιόπιστες.

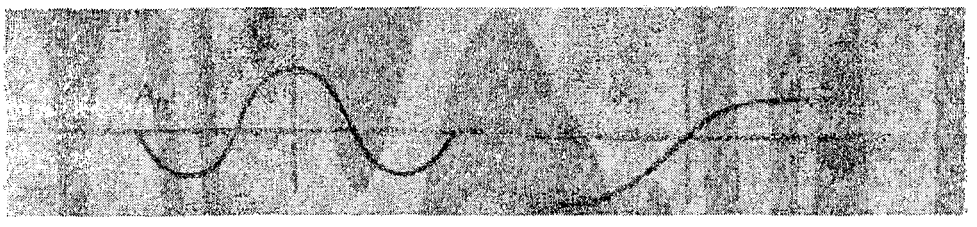


Εικόνα 55 **Β) ΣΠΑΜΕ ΣΕ Ν ΤΜΗΜΑΤΑ S**

2) Έπειτα εφαρμόζεται διακριτός μετασχηματισμός Fourier K σημείων (DFT) κάθε τμήμα Sn[i] με K=1/N. Επιπρόσθετα δημιουργούνται δύο διανύσματα ένα της φάσης Φκ(ωκ) και ένα του μέτρου Αν(ωκ) όπου 0<=κ<=κ-1.

$$FFT(S\{i\}) = A(t)\text{-}e^{-\Phi\,\omega},$$

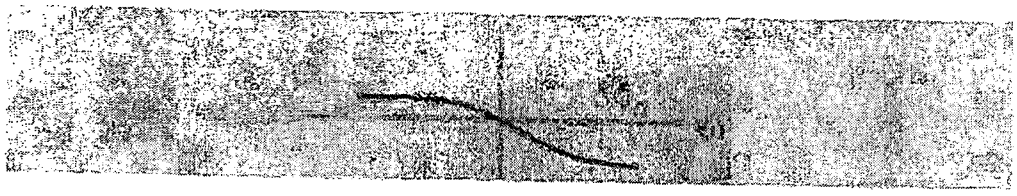
Όπου A(t) το μέτρο και Φ(ΐ) η φάση με Φ(ΐ) Φκ(ωκ) <=: φάση.



Εικόνα 56 **C) ΜΕΤΑΣΧΗΜΑΤΙΖΟΥΜΕ ΚΑΘΕ ΤΜΗΜΑ ΣΕ ΜΕΤΡΟ ΚΑΙ ΦΑΣΗ**

3) Αποθηκεύεται η διαφορά φάσης ανάμεσα σε κάθε γειτονικό τμήμα δηλ για n:0<=n<=N-1

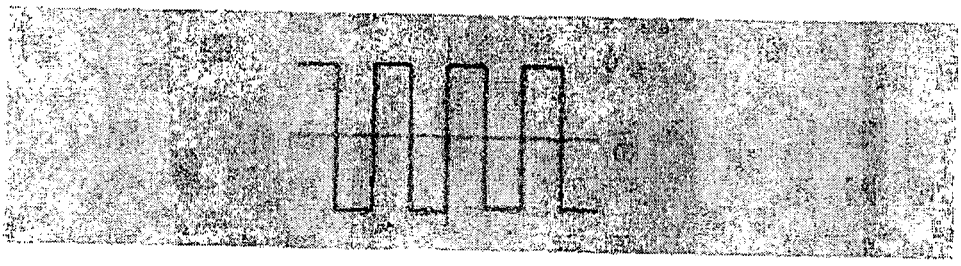
$$\Delta\Phi(\eta+1)(\omega\kappa) = \Phi\nu+1 - \Phi\eta(\omega\kappa)$$



Εικόνα 57 **Ό) ΒΡΙΣΚΟΥΜΕ ΤΗ ΔΙΑΦΟΡΑ ΦΑΣΗΣ ΔΙΠΛΑΝΩΝ ΤΜΗΜΑΤΩΝ Φη+1-Φη**

4) Ένα διάδικο σετ από δεδομένα αναπαρίσταται χρησιμοποιώντας η/2 ή -η/2 για την τιμή 0 ή 1 αντίστοιχα. Φο = $<D_{data}$.

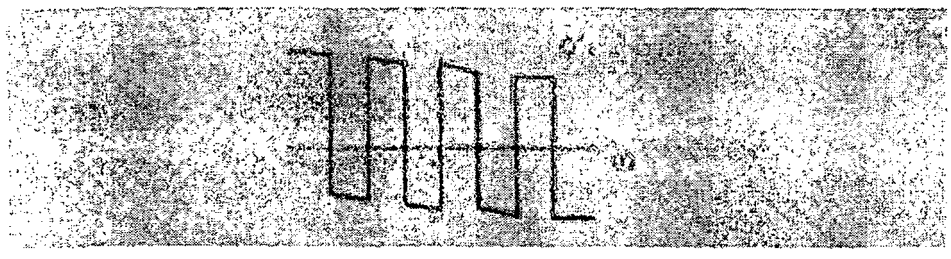
4)



Εικόνα 58 **Ε) ΓΙΑ ΤΟ ΤΜΗΜΑ SO ΔΗΜΙΟΥΡΓΟΥΜΕ ΜΙΑ ΤΕΧΝΗΤΗ ΑΠΟΛΥΤΗ ΦΑΣΗ Φ'Ο**

5) Τα διανύσματα της φάσης ορίζονται ξανά με τη χρήση του παρακάτω μετασχηματισμού. Ο υπολογισμός της φάσης είναι:

$$\begin{bmatrix} \phi_1(\omega_k) \\ \phi_2(\omega_k) \\ \dots \\ \phi_p(\omega_k) \\ \dots \\ \phi_N(\omega_k) \end{bmatrix} = \begin{bmatrix} \phi_0(\omega_k) \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \phi_{N-1}(\omega_k) \end{bmatrix} + \begin{bmatrix} \Delta\phi_1 \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \Delta\phi_N \end{bmatrix}$$

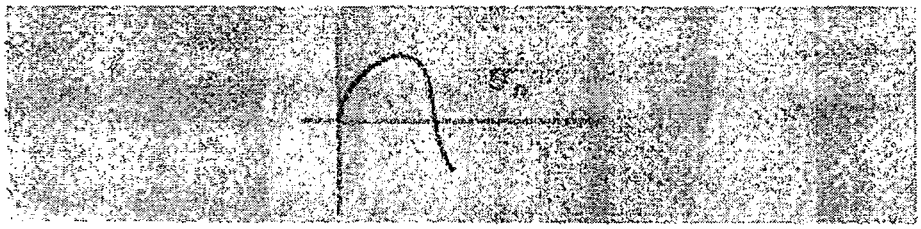


Εικόνα 59 **Έ) ΓΙΑ ΤΑ ΥΠΟΛΟΙΠΑ ΤΜΗΜΑΤΑ ΔΗΜΙΟΥΡΓΟΥΜΕ**

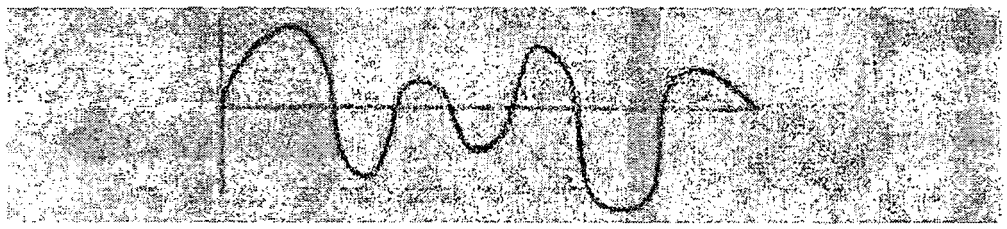
ΚΑΙΝΟΥΡΓΙΑ ΠΛΑΙΣΙΑ ΦΑΣΗΣ ($\Phi_0+\Delta\Phi_1$)

6) Χρησιμοποιώντας την τροποποιημένη φάση και το αρχικό διάνυσμα του μέτρου υπολογίζουμε τις νέες τιμές του διακριτού μετασχηματισμού Fourier με βάση την νέα φάση

$$FFT'(S_i) = A(t)e^{-\phi(t)} \text{ από } \varphi(t) = \varphi_{i-n} + \Delta\varphi_t$$



Εικόνα 60 **G) ΣΥΝΔΙΑΖΟΥΜΕ ΤΗΝ ΚΑΙΝΟΥΡΓΙΑ ΦΑΣΗ ΜΕ ΤΟ ΑΡΧΙΚΟ ΠΛΑΤΟΣ ΓΙΑ ΤΗΝ ΠΑΡΑΓΩΓΗ ΚΑΙΝΟΥΡΓΙΟΥ ΤΜΗΜΑΤΟΣ S'_n**



Εικόνα 61 **Η) ΣΥΝΔΕΟΥΜΕ ΤΑ ΚΑΙΝΟΥΡΓΙΑ ΤΜΗΜΑΤΑ ΓΙΑΤΗΝ ΠΑΡΑΓΩΓΗ ΤΗΣ ΕΞΟΔΟΥ**

7) Τέλος εφαρμόζοντας τον αντίστροφο μετασχηματισμό Fourier παίρνουμε το τελικό υδατογραφημένο ήχο.

$$IDFT(k_i) = S_i$$

Εφόσον η $\Phi_0(\omega_k)$ αλλάζει οι απόλυτες φάσεις που αντιστοιχούν στο κάθε τμήμα του ήχου μεταβάλλονται αντίστοιχα, όμως η σχετική διαφορά φάσης μεταξύ των γειτονικών κομματιών παραμένει ίδια. Μ' αυτό τον τρόπο πετυχαίνουμε να διατηρούμε αναλλοίωτη την διαφορά φάσης στην οποία το ανθρώπινο ακουστικό σύστημα είναι πιο ευαίσθητο.

Ανίχνευση

Κατά τη διαδικασία ανίχνευσης ο συγχρονισμός της συχνότητας γίνεται πριν την αποκωδικοποίηση. Για να μπορέσει να γίνει ανίχνευση του υδατογραφημένου ήχου θα πρέπει να είναι γνωστό:

- Το φασματικό εύρος των τμημάτων δηλ. το μήκος των N κομματιών του ήχου
- Τα σημεία που είχαν υποβληθεί διακριτό μετασχηματισμό Fourier και τα διαστήματα των δεδομένων.

Στη μέθοδο προστίθενται δυαδικά δεδομένα που κατά τη διαδικασία ένθεσης όπου μπορεί να είναι 0 ή 1. Εφόσον αυτή η τιμή τροποποιείται, ανάλογα τροποποιούνται και οι φάσεις που αντιστοιχούν σε κάθε κομμάτι του σήματος, γι' αυτό και η τιμή του διάδικου αριθμού πρέπει να είναι κι αυτή γνωστή.

Αποτελέσματα

Η υδατογράφηση φάσης δεν επιτρέπει την εισαγωγή θορύβου και την παραμόρφωση του σήματος του υδατογραφήματος. Ομως μπορεί να υπάρξει παραμόρφωση μέσω της διασποράς της φάσης αν δεν διατηρηθούν οι διαφορές φάσης μεταξύ των τμημάτων του ήχου. Για να ελαττωθεί ο παράγοντας αυτός η διασπορά της φάσης χρησιμοποιεί το ρυθμό δεδομένων της υδατογραφημένης φάσης. Επιπλέον η διασπορά της φάσης σχετίζεται άμεσα με την πρόσθεση των δυαδικών δεδομένων στη φάση ($\Phi_0(\omega_k)$). Το πλάτος της φάσης που προστίθεται πρέπει να είναι αρκετά κοντά στην πραγματική τιμή ώστε να μειωθεί η παραμόρφωση. Αντίθετα η διαφορά της φάσης του σήματος που προστίθεται πρέπει να είναι μέγιστη ώστε να περιορίζεται η επίδραση θορύβου πάνω στο σήμα.

Μία άλλη πηγή που συμβάλλει στην αλλοίωση του υδατογραφημένου ήχου είναι ο ρυθμός με τον οποίο μεταβάλλεται η τροποποιημένη φάση. Η αλλαγή της φάσης όπως φαίνεται και από τον τύπο πραγματοποιείται με κάποιον ρυθμό και έπειτα το αποτέλεσμα αποθηκεύεται ώστε να υπολογισθεί ο παράγοντας του διακριτού μετασχηματισμού Fourier. Αν σε κάθε βήμα υπάρχει παραμόρφωση τότε και στις τιμές που δίνει ο Fourier αντιστοιχούνται συχνότητες των οποίων η φάση διαφέρει απο από τις γειτονικές. Μ' άλλα λόγια η σχετική διαφορά φάσης των γειτονικών κομματιών δε διατηρείται σταθερή ή τουλάχιστον ελάχιστα διαφοροποιημένη αλλά παρουσιάζει μεγάλες αποκλίσεις από την αρχική σχετική διαφορά φάσης. Μιας και η παραμόρφωση οφείλεται στη μεγάλη συχνότητα αλλαγής της φάσης τότε οι αλλαγές της φάσης πρέπει να γίνονται πιο αραιά και οι μεταβάσεις μεταξύ των τροποποιημένων φάσεων να είναι πιο ομαλές. Έτσι διατηρείται η παραμόρφωση σ' ένα επίπεδο που στο ακουστικό σύστημα του ανθρώπου δε γίνεται αντιληπτό.

*Εικόνα 62*Οξεία vs. Ομαλής Μετάβασης

Στο σχήμα φαίνονται οι αλλαγές της φάσης στη μία περίπτωση Α που οι μεταβάσεις είναι απότομες δηλαδή υπάρχει μεγάλος ρυθμός αλλαγής (αιχμηρές άκρες). Τότε θα υπάρχει παραμόρφωση που είναι διακριτή ενώ αντίθετα στην περίπτωση Β που οι μεταβάσεις είναι πιο ομαλές η παραμόρφωση δε θα είναι αντιληπτή.

7.4.3 Μέθοδος Διεσπαρμένου Φάσματος (Spread Spectrum) [13], [74], [75]

Σε ένα κανονικό κανάλι επικοινωνίας είναι συχνά επιθυμητό η πληροφορία του σήματος που μεταδίδεται να είναι συγκεντρωμένη σε ένα μικρό εύρος συχνοτήτων έτσι ώστε το εύρος ζώνης που είναι διαθέσιμο να μπορεί να φιλοξενήσει και άλλα κανάλια επικοινωνίας και επιπλέον η ισχύς του σήματος να είναι μεγάλη. Παρόλαυτά ένα σήμα μικρού εύρους ζώνης επηρεάζεται αρκετά από τις παρεμβολές άλλων σημάτων ενώ ταυτόχρονα δεν είναι ανθεκτικό στις διάφορες επεξεργασίες ψηφιακών σημάτων.

Η μέθοδος του διασκορπισμένου φάσματος σχεδιάστηκε έτσι ώστε να ενθέτει μία ροή από δεδομένα διασπείροντας την πληροφορία σε όσο το δυνατόν μεγαλύτερο μέρος του φάσματος συχννοτίτων. Διασπείροντας πληροφορία σχεδόν σ' όλο το εύρος του φάσματος συχνοτήτων του ήχου η προφύλαξη της πληροφορίας του σήματος ενισχύεται και δεν επηρεάζεται ακόμη και από την παρεμβολή άλλων συχνοτήτων.

Η μέθοδος Spread Spectrum [4], [74], [75] χρησιμοποιείται με πολλούς τρόπους στα τηλεποικοινωνικακά μέσα εμείς θα επικεντρώσουμε σε μια μορφή, που ονομάζεται (Direct Sequence Spread Spectrum encoding DSSS).

Η DSSS μέθοδος διευρύνει το εύρος του σήματος πολλαπλασιάζοντας το σήμα μ' ένα άλλο σήμα που λέγεται chip. Το chip αποτελεί έναν ψευδοτυχαίο θόρυβο με ευρύ φάσμα που μορφοποιείται σ' έναν συγκεκριμένο ρυθμό. Εφόσον ο ήχος είναι δειγματοληπτιμένος σε διακριτό χρόνο χρησιμοποιούμε το ρυθμό του chip ίδιο με τον ρυθμό δειγματοληψίας. Η τιμή αυτή του ρυθμού του chip δίνει τη δυνατότητα του καλύτερου συντονισμού της DSSS διαδικασίας. Γιατί μ' αυτό τον τρόπο επιτρέπεται ο πιο εύκολος καθορισμός της αρχής και του τέλους του κβαντίσου του chip ώστε να διασφαλίζονται οι απαιτήσεις για «κλείδωμα» της φάσης.

Εφόσον ο ρυθμός του chip είναι ίδιος με αυτή των δεδομένων όσο αυξάνεται ο ρυθμός του chip τόσο μεγαλώνει και ο ρυθμός των συσχετιζόμενων δεδομένων. Επιτυγχάνετε λοιπόν το κλείδωμα της φάσης που αν δεν επιλεγόταν να γίνει με την εξίσωση των ρυθμών θα απαιτούνταν πολύπλοκοι αλγόριθμοι.

Για να μπορέσει να γίνει κατανοητός ο τρόπος με τον οποίο η DSS σκορπά την πληροφορία σ' όσο το δυνατόν μεγαλύτερο εύρος του σήματος θα αναλυθεί η διαδικασία της Direct Sequence Spread Spectrum.

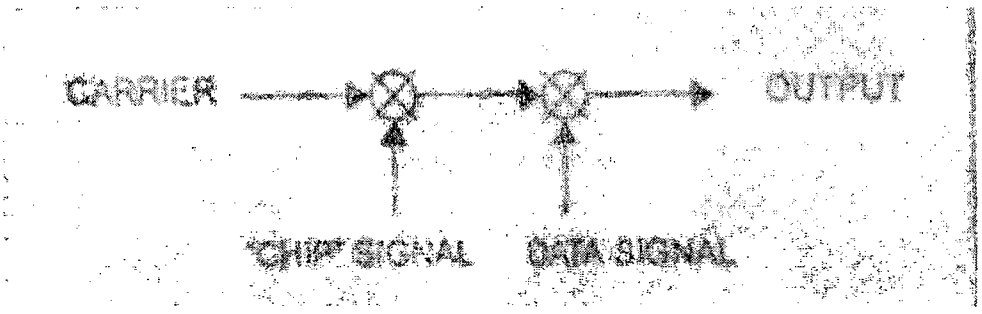
Διαδικασία

Στην DSSS το κλειδί υδατογράφησης είναι ένας ψευδοτυχαίος θόρυβος με επίπεδη συχνότητα πάνω από το εύρος συχνοτήτων του σήματος π.χ λευκός Gauss θόρυβος. Κατά τη διαδικασία της ένθεσης του υδατογραφήματος το κλειδί χρησιμοποιείται για την κωδικοποίηση αλλά και την αποκωδικοποίηση της πληροφορίας.

Η κωδικοποίηση μέσω του κλειδιού [1] λαμβάνει χώρα, έτσι ώστε ο ψευδοτυχαίος αυτός θόρυβος σε συνδυασμό με το αρχικό σήμα να επιτυγχάνει τον υπολογισμό της συχνότητας που θα εφαρμοστεί στην συχνότητα του διασκορπισμένου διανύσματος.

1) Αρχικά παράγουμε το κλειδί δηλαδή ένα φέρον σήμα πολλαπλασιάζεται μ' ένα τετραγωνικό παλμό.
2) Το παραπάνω σήμα συνελίσεται και με chip.

Το σήμα που έχει προκύψει από τις πιο πάνω διαδικασίες περιορίζεται (με κάποιο φίλτρο) και προστίθεται στο αρχικό σήμα.



Εικόνα 63 Διαδικασία παραγωγής W στην Spread Spectrum

Στην DSSS υλοποιείται δι-φασική μετατροπή και ταυτόχρονη μετατόπιση του σήματος. Στην αποκωδικοποίηση απαιτείται η γνώση της φάσης φο και φο+η που αναπαριστούν αντίστοιχα το «0» και το «1» αντίστοιχα.

Ανίχνευση

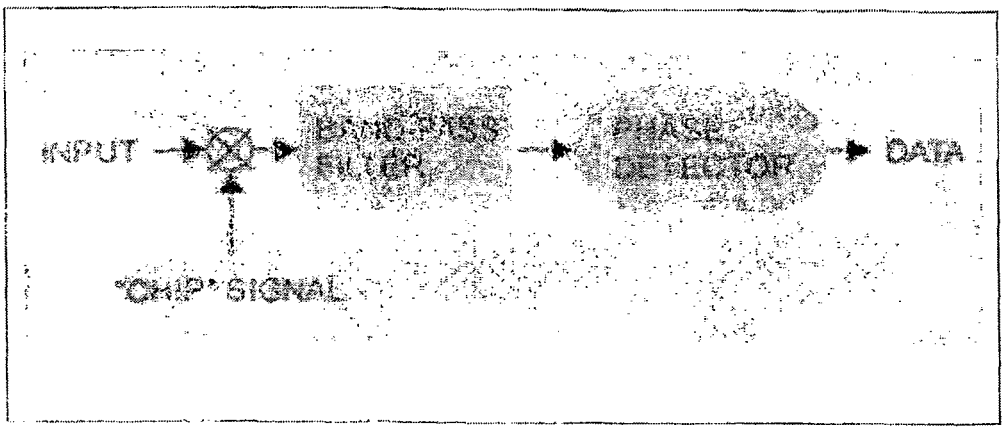
Στην ανίχνευση απαιτούνται οι εξής παράγοντες

1) Το ψευδοτυχαίο κλειδί πρέπει να είναι «μέγιστο» ώστε να μπορεί να λάβει χώρα ένας μεγάλος αριθμός συνδυασμών για να μην υπάρξει επανάληψη στη φάση της αποκωδικοποίησης. Επίσης το κλειδί θα πρέπει να έχει επίπεδο φάσμα συχνοτήτων ώστε να είναι εφικτή η αναπαράσταση του διάδικου αριθμού.

2) Η εναλαγή μηδενικών και άσσων είναι γνωστή στον παραλήπτη ώστε να επιτευχθεί ο συγχρονισμός και επιπλέον για να είναι γνωστή η περιοχή του φάσματος όπου εκπέμπηκαν κωδικοποιημένα δεδομένα με DSS. Γι αυτό το λόγο στην DSSS αποκωδικοποίηση ο παραλήπτης θα πρέπει να γνωρίζει το ρυθμό του chip και του φέροντος σήματος όπως επίσης και την συχνότητα του φέροντος σήματος.

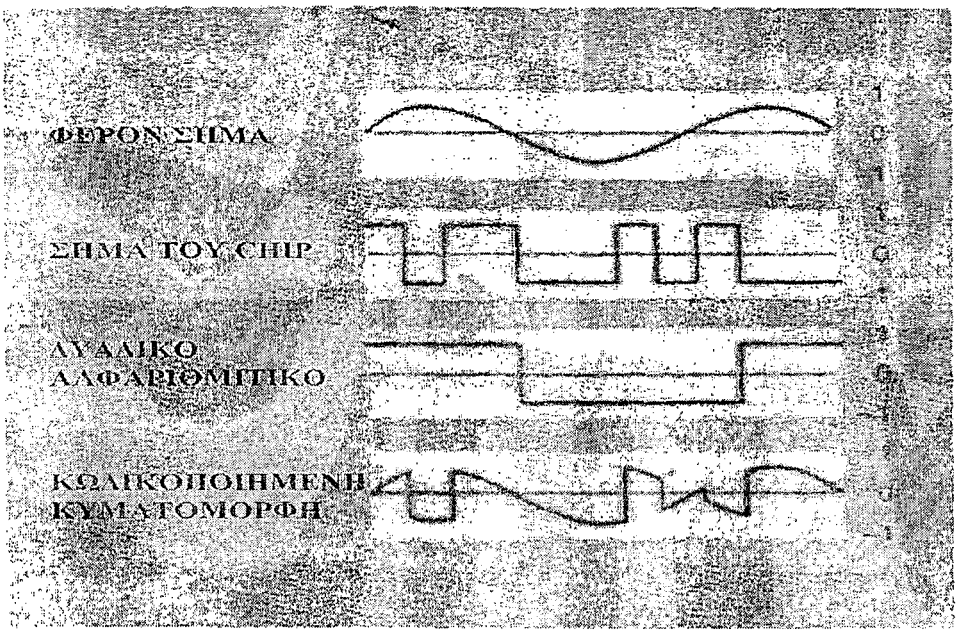
Έτσι γνωρίζοντας το ρυθμό του chip συνελίσουμε τον υδατογραφημένο ήχο ώστε να επιτευχθεί συγχρονισμός. Έπειτα εφαρμόζουμε ένα ζωνοπερατό φίλτρο στη συχνότητα που βρίσκονται τα διασπαρμένα δεδομένα.

Γνωρίζοντας το Φ_0 αποκωδικοποιείται η φάση όπου κάθε Φ_0 αντιστοιχείται στο 0 και κάθε Φ_{0+n} στο 1 και προκύπτει ένας διάδικο string που συγκρίνεται και επιτυγχάνεται η διαδικασία της πιστοποίησης.



Εικόνα 64 Διαδικασία αποκωδικοποίησης W στην Spread Spectrum

Αποτελέσματα

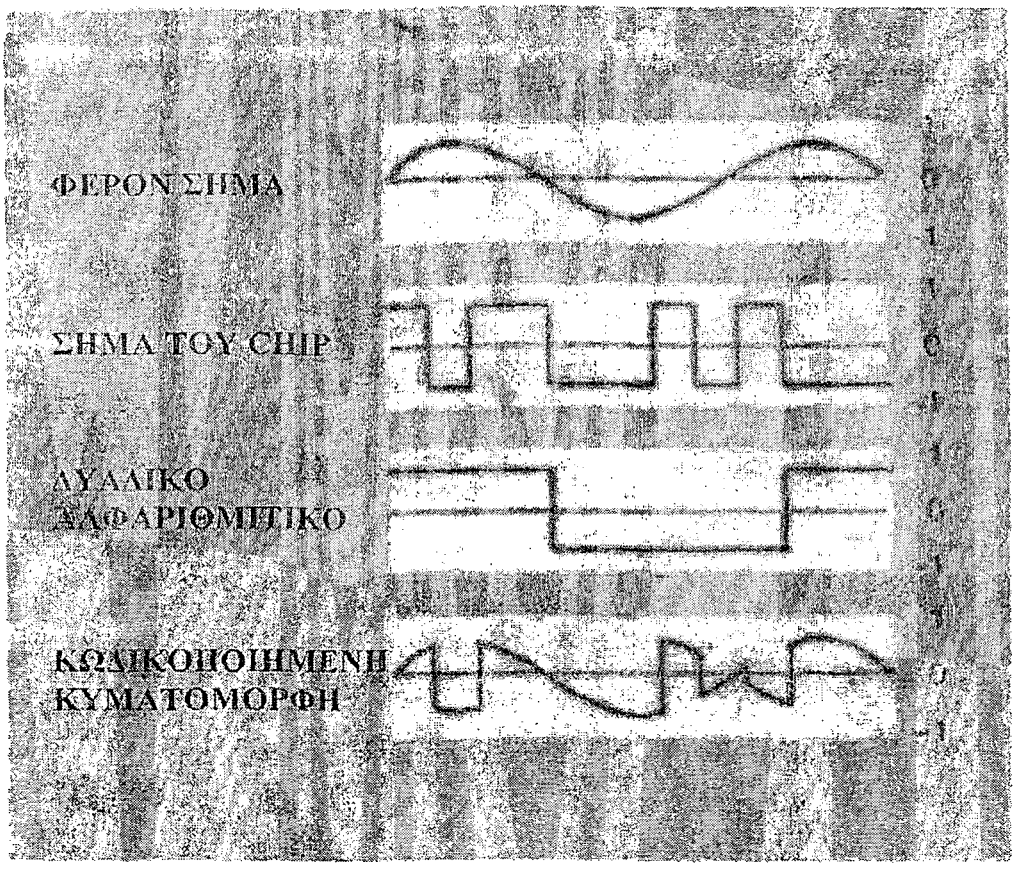


Εικόνα 65 **Αναμεμιγμένα σήματα κατά την κωδικοποίηση Spread Spectrum**

Σε αντίθεση με την υδατογράφηση φάσης, η μέθοδος διασπαρμένου φάσματος χρησιμοποιεί τις ιδιότητες του ήχου που σχετίζονται με το συχνοτικό εύρος και εισάγει επιπρόσθετα τυχαίο θόρυβο στον ήχο. Η ένθεση θορύβου στο ηχητικό σήμα θα πρέπει να διατηρείται σ' ένα χαμηλό επίπεδο - ώστε να μην εισέρχεται αρκετός θόρυβος και επιπλέον να παραμένει μη αντιληπτός.

Ο τετραγωνικός παλμός που πολλαπλασιάζεται με το φέρον σήμα και δημιουργεί το κλειδί υδατογράφησης πρέπει το εύρος συχνοτήτων του να συνδυάζεται με την ενέργεια του σήματος. Για να επιτευχθεί αυτό πρέπει να υπολογισθεί το δυναμικό εύρος του ήχου και αν ο τετραγωνικός παλμός έχει μεγαλύτερο ενεργειακό φάσμα θα πρέπει να εξασθενηθεί ώστε τουλάχιστον να χαρακτηρίζεται από το μισό δυναμικό ενεργειακό φάσμα.

Αποτελέσματα



Εικόνα 65 **Αναμεμιγμένα σήματα κατά την κωδικοποίηση Spread Spectrum**

Σε αντίθεση με την υδατογράφηση φάσης, η μέθοδος διασπαρμένου φάσματος χρησιμοποιεί τις ιδιότητες του ήχου που σχετίζονται με το συχνοτικό εύρος και εισάγει επιπρόσθετα τυχαίο θόρυβο στον ήχο. Η ένθεση θορύβου στο ηχητικό σήμα θα πρέπει να διατηρείται σ' ένα χαμηλό επίπεδο - ώστε να μην εισέρχεται αρκετός θόρυβος και επιπλέον να παραμένει μη αντιληπτός.

Ο τετραγωνικός παλμός που πολλαπλασιάζεται με το φέρον σήμα και δημιουργεί το κλειδί υδατογράφησης πρέπει το εύρος συχνοτήτων του να συνδυάζεται με την ενέργεια του σήματος. Για να επιτευχθεί αυτό πρέπει να υπολογισθεί το δυναμικό εύρος του ήχου και αν ο τετραγωνικός παλμός έχει μεγαλύτερο ενεργειακό φάσμα θα πρέπει να εξασθενηθεί ώστε τουλάχιστον να χαρακτηρίζεται από το μισό δυναμικό ενεργειακό φάσμα.

Μ' αυτό τον τρόπο ο υδατογραφημένος ήχος ενθέτεται με προσοχή ώστε να μη γίνεται αντιληπτή η ύπαρξη του μιας και ο υδατογραφημένος ήχος έχει ομοιόμορφο ενεργειακό φάσμα.

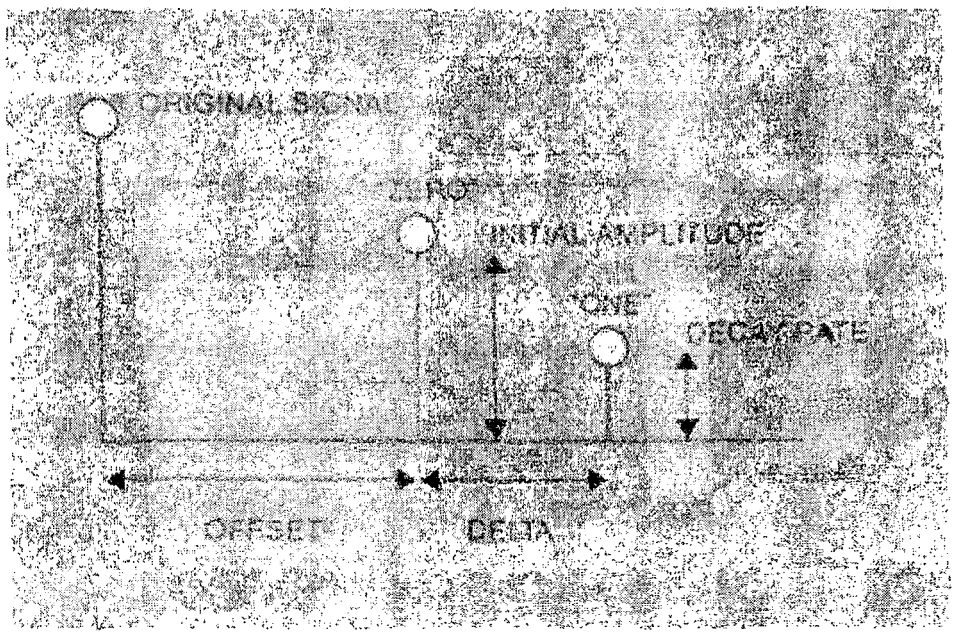
Επιπλέον συνήθεις συχνοτικές επεξεργασίες σημάτων π.χ. φιλτράρισμα ή επαναδειγματοληψία δεν αλλοιώνουν το υδατογραφη μα καθώς η περιοχή που διαμοιράζεται ο θόρυβος είναι ευρεία και περιέχει σημαντική πληροφορία του σήματος.

Τέλος ένα μικρό τμήμα κωδικοποιημένου παλμικού σήματος συνδέεται και προστίθεται για αρχικό σήμα ώστε ο μεταφερόμενος θόρυβος να ελαττώνεται με την ισοστάθμιση και ομαλοποίηση του σήματος πάνω στα επίπεδα συχνότητας του τμήματος αυτού κατά τη φάση της ανίχνευσης.

Η DSSS επιτυγχάνει να αποτρέψει την αλλοίωση του υδατογραφημένου σήματος όταν υπάρχει επίθεση (attack) σε ένα μέρος του πεδίου συχνοτήτων κάνοντας το υδατογραφημένο ήχο αξιόπιστο και ασφαλή.

7.4.4 Echo data hiding [l], [3]

Η μέθοδος Echo data hiding ενσωματώνει πληροφορία στο αρχικό ηχητικό σήμα εισάγοντας ηχώ (echo)[l]. Τα δεδομένα προστίθενται τροποποιώντας τρεις παραμέτρους της ηχούς: Το αρχικοποιημένο διανύσματα, το ρυθμό εξασθένησης και την απόκλιση.



Εικόνα 66 **Τροποποιήσιμοι παράμετροι από την Echo Data Hiding**

Η αύξηση της απόκλισης μεταξύ του σήματος και της ηχούς ελαττώνεται τα δύο σήματα αναμιγνύονται. Υπάρχει ένα συγκεκριμένο σημείο στην απόσταση μεταξύ εισαγώμενης ηχούς και ήχου όπου το ανθρώπινο αυτί δεν αντιλαμβάνεται διαφορά.

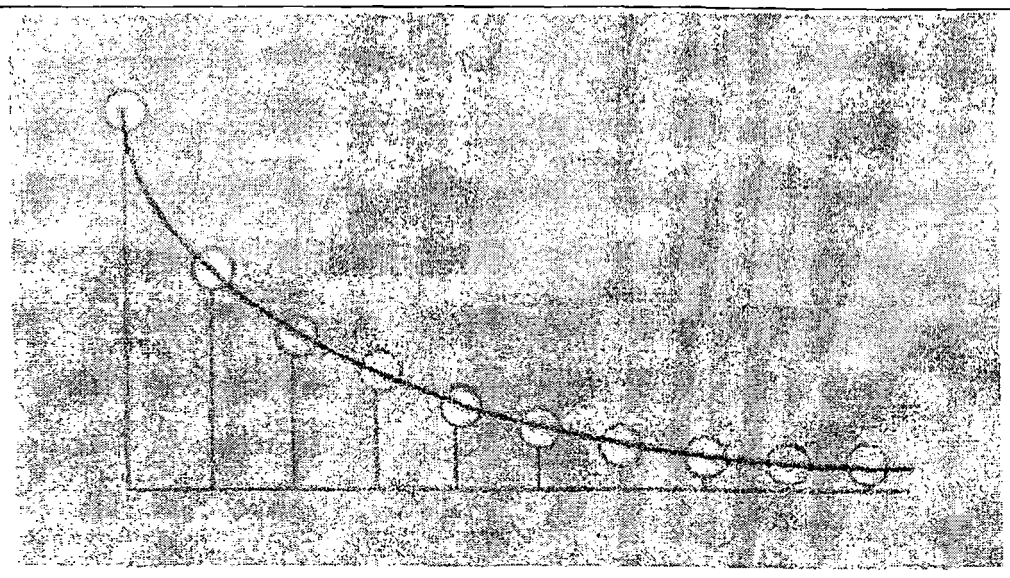
Η ηχός γίνεται αντιληπτή από τον άνθρωπο ως την πρόσθεση στον ήχο αντιηχούς. Αυτό το σημείο όπου δε γίνεται αντιληπτή η ήχος είναι δύσκολο να καθοριστεί με ακρίβεια γιατί εξαρτάται από την ποιότητα ηχογράφησης, το είδος του ήχου και τον ακροατή. Γενικά έχει ευρεθεί ότι όταν η απόκλιση είναι κοντά στο 1/1000 του δευτερολέπτου το φαινόμενο δε γίνεται αντιληπτό.

Στην ένθεση της ηχούς ο κωδικοποίητης χρησιμοποιεί δύο χρόνους καθυστέρησης. Ο ένας αναπαριστά τη μονάδα «1» (απόκλιση) και ο άλλος την αναπαράσταση του «0» (απόκλιση+δέλτα). Και οι δύο χρονικές καθυστερήσεις είναι κάτω από το κατώφλι, που αντιλαμβάνεται ο άνθρωπος την ηχό. Από μία άλλη οπτική γωνία αυξάνοντας το χρόνο καθυστέρησης μπορεί επίσης να επιτύχουμε τη μη αντίληψη της ηχούς από το ανθρώπινο αυτί μετατοπίζοντας το αρχικοποιημένο διάνυσμα και το ρυθμό καθυστέρησης κάτω από το επίπεδο ακοής του ανθρώπου

Διαδικασία ένθεσης

Η διαδικασία ένθεσης αποτελείται απο δύο μέρη, καθένα απο τα οποία μπορεί να αναπαρασταθεί με 2 πιθανές κλίσεις συστήματος (πυρήνας), μία για το δυαδικό 1 και

μία για το διάδικο 0. Στη χρονική αναπαράσταση του ήχου οι κλήσεις συστήματος είναι εκθετικές συναρτήσεις διακριτού χρόνου που διαφέρουν στην καθυστέρηση μεταξύ των παλμών.

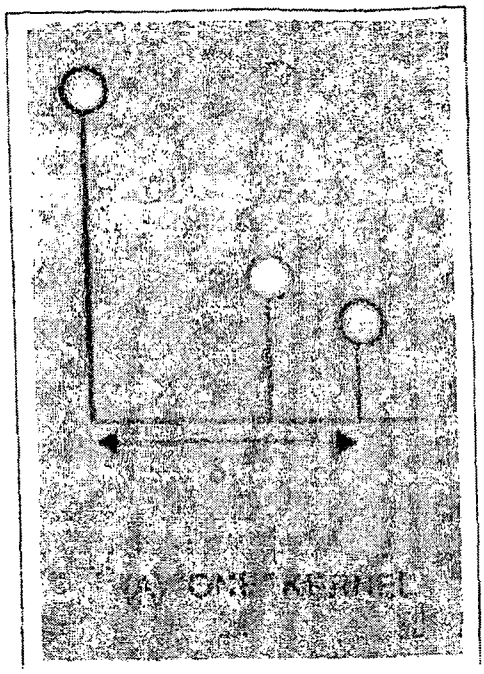


Εικόνα 67 **Εκθετική συνάρτηση διακριτού χρόνου**

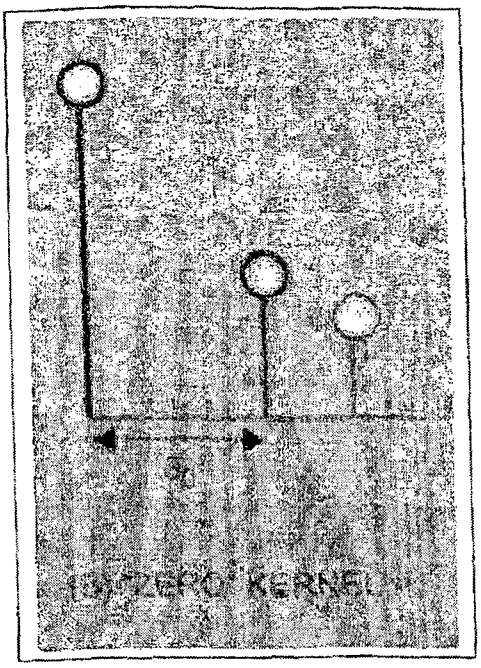
161

Αν υποθέσουμε ότι χρησιμοποιούμε έναν τόνο για τον ήχο και έναν για την ηχώ η αναπαράσταση των συναρτήσεων του συστήματος (κλήσεις συστήματος) φαίνεται παρακάτω όπως και ο πυρήνας για τη μία συνάρτηση που αντιστοιχεί στο «0».

Η καθυστέρηση (δ) είναι η καθυστέρηση μεταξύ του πραγματικού σήματος και της ηχούς που εξαρτάται από το είδος του πυρήνα που επιλέγουμε. Η καθυστέρηση για τον πυρήνα που κωδικοποιεί το 1 είναι δ_1 και για το 0 αντίστοιχα δ_0.

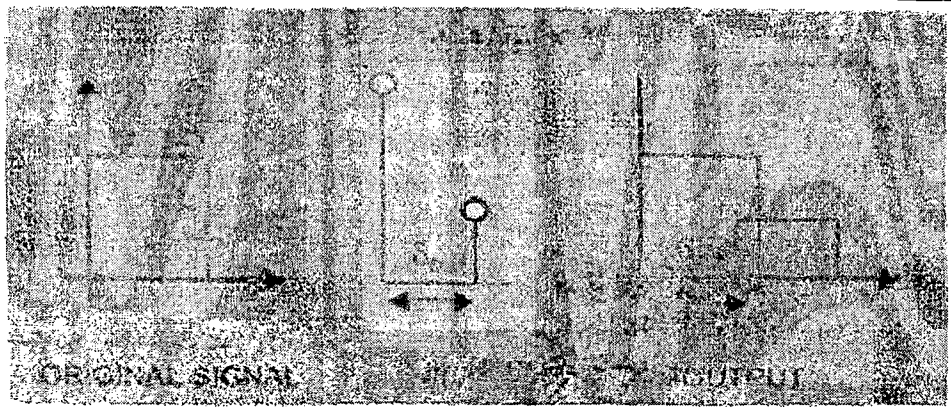


Εικόνα 68 Καθηστέρηση Ηχούς-Πυρηνα (1)



Εικόνα 69 Καθηστέρηση Ηχούς-Πυρηνα (0)

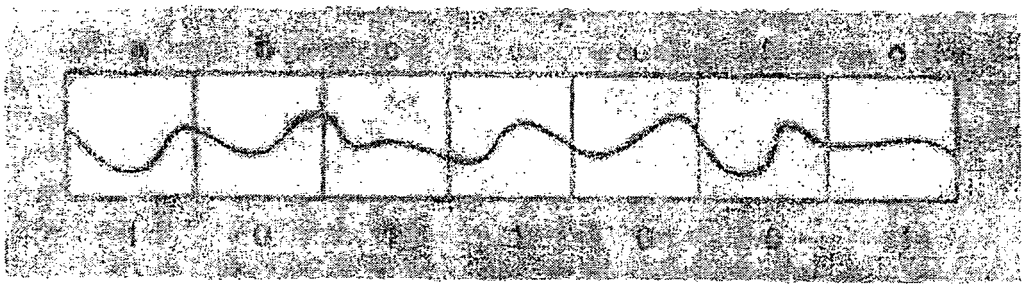
Για να επιτευχθεί η κωδικοποίηση περισσότερα από ένα bit το σήμα διαιρείται σε μικρότερα μέρη.



Εικόνα 70 **Κωδικοποιημένο Σήμα του zero kernel με echo data hiding**

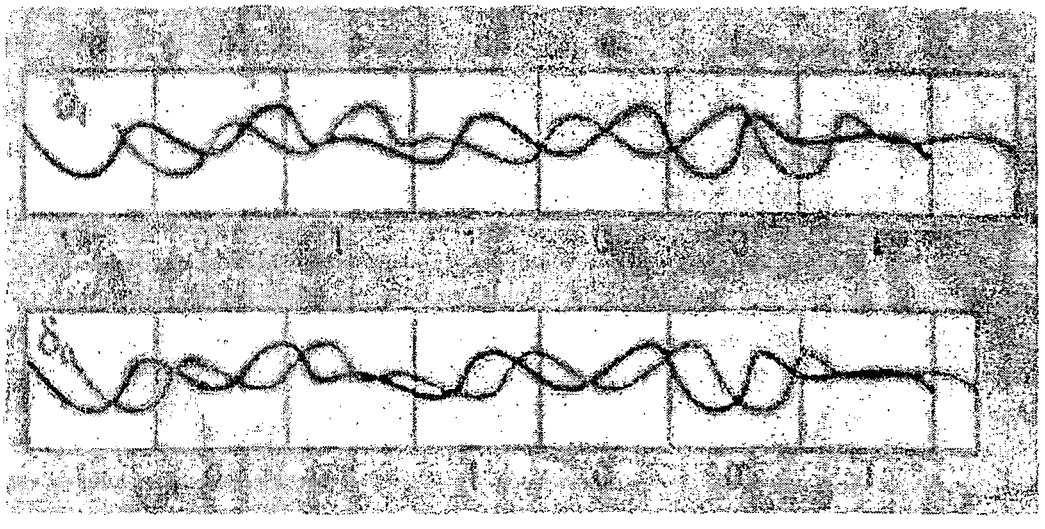
Κάθε διακεκριμένο μέρος μπορεί να κωδικοποιηθεί με το επιθυμητό bit θεωρώντας το κάθε τμήμα του ήχου σαν ξεχωριστό σήμα. Η διαδικασία έχει ώς εξής:

Αρχικά το ηχητικό σήμα που αναπαρίσταται με βάση το χρόνο διαιρείται σε N διαφορετικά κομμάτια (στο σχήμα N=7) και σε καθένα από αυτά ανάλογα με την πληροφορία αντιστοιχίζεται το «1» ή το «0».



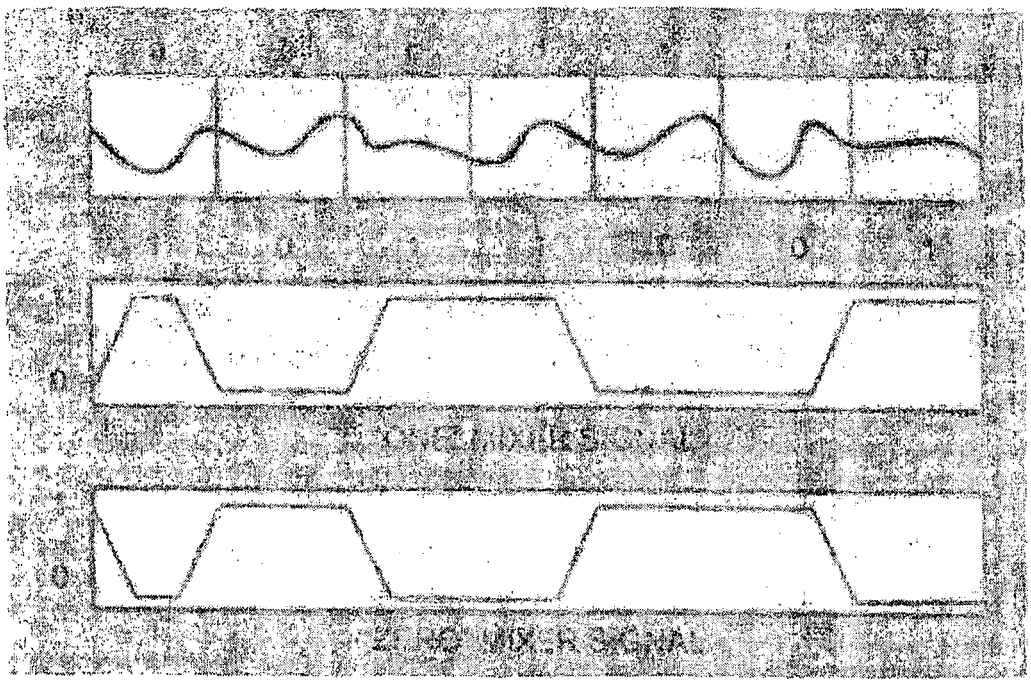
Εικόνα 71 **Διαιρεμένο σήμα για N=7 τμήματα για κωδικοποίηση πληροφορίας**

Το κάθε κομμάτια του ήχου το επεξεργαζόμαστε σαν ένα διακριτό ξεχωριστό σήμα. Στα τμήματα του ήχου που έχουν αντιστοιχηθεί με «1» συνελίσουμε τον ήχο που περικλείουν με το σήμα του «πυρήνα» ενώ αντίστοιχα αυτά που έχουν αντιστοιχηθεί με «0» τα συνελίσουμε με το σήμα του πυρήνα που αντιστοιχεί στο «0». Μ' άλλα λόγια τα τμήματα που συνελίσονταΐ κλιμακώνονται μεσώ του ηχητικού σήματος ανάλογα με το ποιο δυαδικό ψηφίο αντιστοιχίζεται στα τμήματα



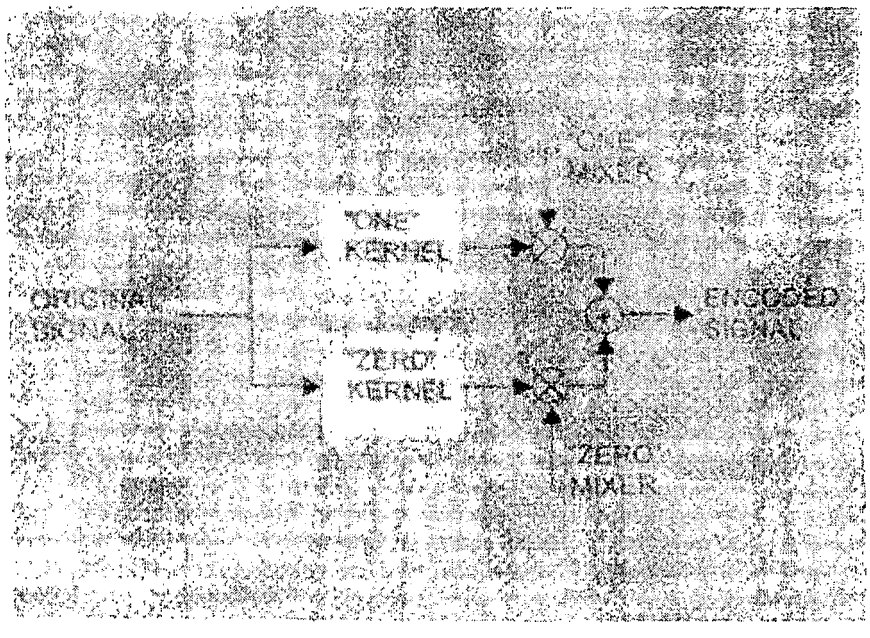
Εικόνα 73 **Συνελημένα Σήματα**

Το αποτέλεσμα της συνέλιξης δημιουργεί δύο μεικτά σήματα. Αυτό που προκύπτει από την συνέλιξη με το σήμα του πυρήνα «0» και αυτό που προκύπτει από το σήμα του πυρήνα «1». Τα δύο αυτά σήματα προστίθενται και δίνουν ένα αναμεμιγμένο[10] σήμα.



Εικόνα 75 **Αναμεμιγμένα σήματα**

Το αναμεμιγμένο σήμα είναι είτε «1» είτε «0» ανάλογα με το διάδικο ψηφίο που επιλέγεται να ενσωματωθεί στο κομμάτι του σήματος. Επιπλέον αποδίδει μία ομαλή μετάδοση μεταξύ των κομματιών ήχου που κωδικοποιείται με διαφορετικά δυαδικά ψηφία αλλά που αποτρέπεται η αλλαγή της καμπύλωσης του ηχητικού σήματος στο τελικό αναμιγμένο σήμα.



Εικόνα 76 **Διαδικασία Κωδικοποίησης**

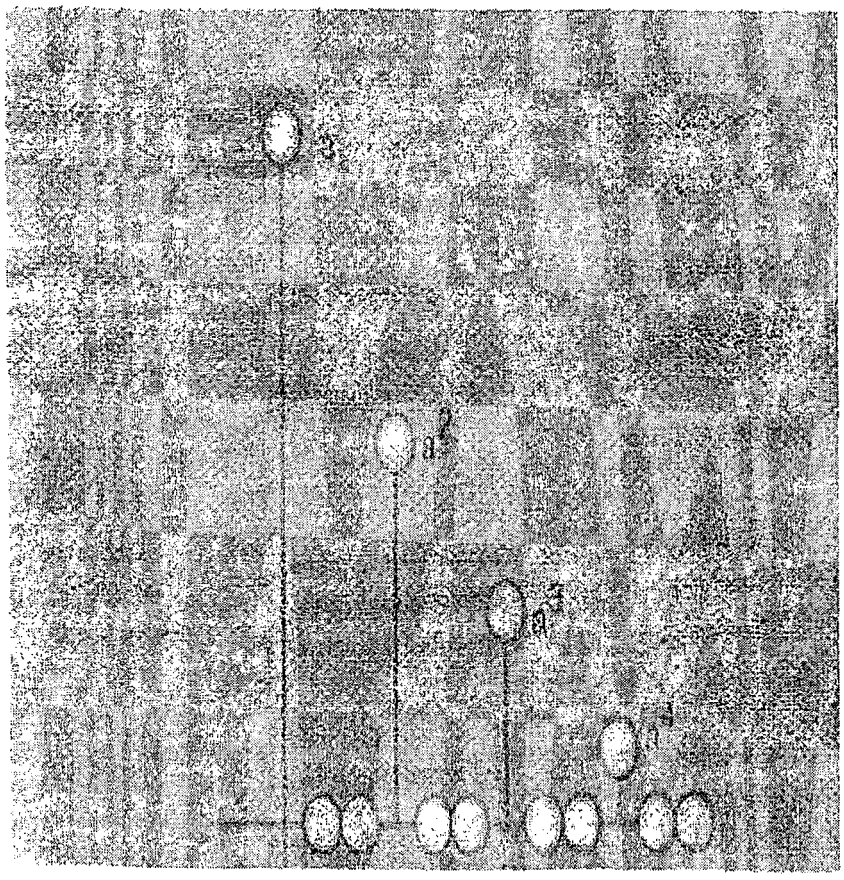
Ανίχνευση

Το υδατογράφημα ενσωματώνεται στο ηχητικό σήμα ενισχύοντας την ηχώ του με έναν από τους δύο πυρήνες καθυστέρησης. Η διαδικασία ανίχνευσης επιτυγχάνεται χρησιμοποιώντας την απόσταση των ήχων μεταξύ τους. Για να μπορέσει να επιτευχθεί

ανίχνευση, ελέγχεται το πλάτος (και στις δύο περιοχές) του αυτοσυσχετιζόμενου σήματος cepstrum

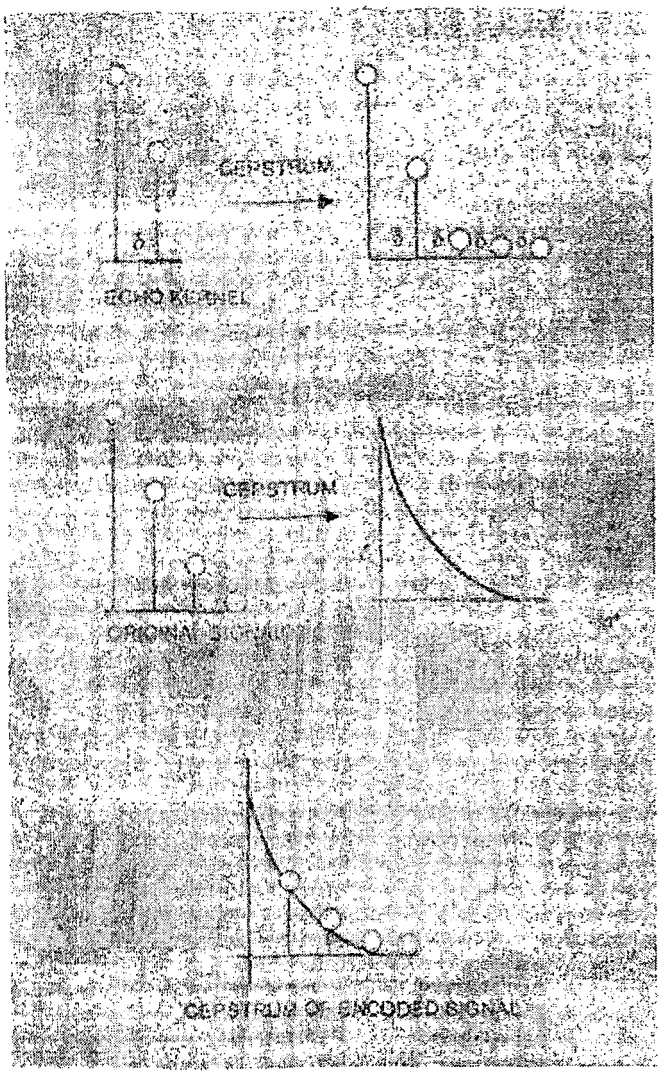
$$F-1(Incomplex(f(x)2))$$

Η ηχός αποτελείται από ένα αριθμό «τόνων» διακριτών μεταξύ τους, ενώ οπουδήποτε αλλού θέτεται «0».



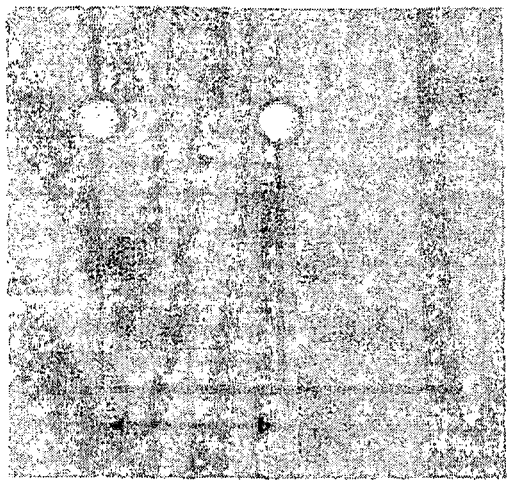
Εικόνα 77 **Ηχητικό Σήμα**

2) Έπειτα θα πρέπει να υπολογισθεί το διάνυσμα του cepstrum της διαδικασίας ενίσχυσης της ηχούς.

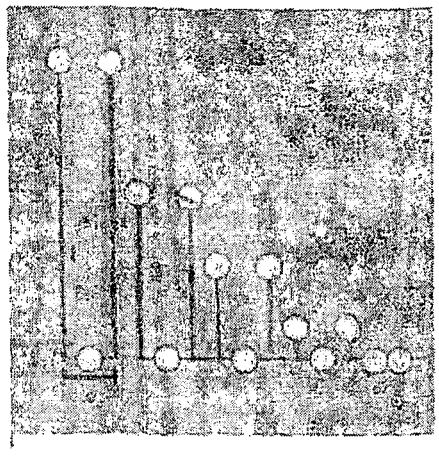


Εικόνα 78 **Παραγωγή Cepstrum για την κωδικοποίηση ηχούς**

Το αποτέλεσμα της υλοποίησης του cepstrum [l] είναι ότι επιτυγχάνεται καλύτερος διαχωρισμός μεταξύ της ηχούς και πραγματικού σήματος ήχου. Δυστυχώς η διαδικασία αυτή διπλασιάζει την ηχό κάθε (δ) δευτερόλεπτα.



Εικόνα 80 Πυρήνας με καθυστέρηση δ



Εικόνα 79 Το αποτέλεσμα της κωδικοποίησης με ηχώ

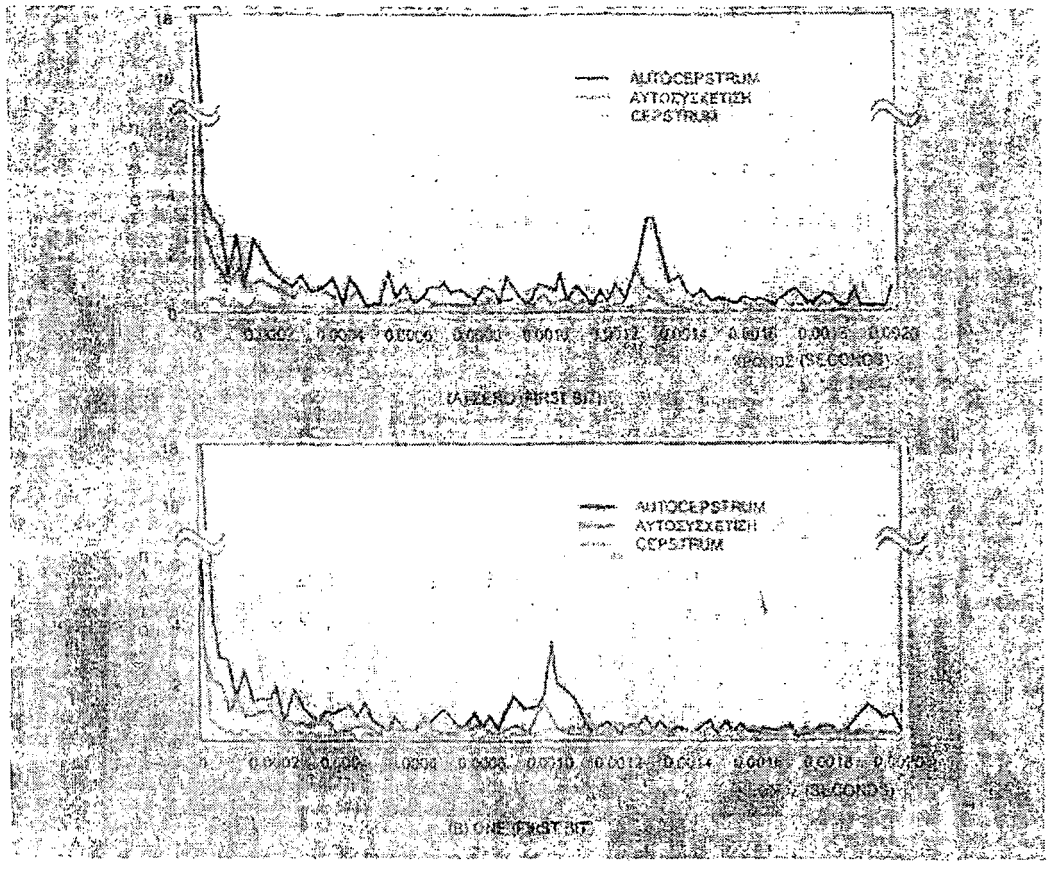
Επιπλέον το μέτρο των τόνων του σήματος αναπαρίσταται από τις ηχούς, σχετίζεται σε πολύ μικρό βαθμό με το αρχικό σήμα

Η επίλυση αυτού του προβλήματος επιτυγχάνεται με την αυτοσυσχέτηση του διανύσματος cepstrum. Μόνο ο πρώτος παλμός είναι αρκετά ενισχυμένος μιας και επανενισχύεται από τους επόμενους τόνους. Γι' αυτό το λόγο τοποθετούμε μία ακίδα στη θέση του πρώτου τόνου, στον πρώτο παλμό η ακόμα τοποθετείται στα (δ_1) ή (δ_0) δευτερόλεπτα μετά το αρχικό σήμα.

Ο κανόνας για την επιλογή του 1 ή του 0 βασίζεται στον χρόνο καθυστέρησης (δ) πριν την ακίδα (spike) στην αυτοσυσχέτιση. Κατά την ανίχνευση εντοπίζεται το «1» αν το μέτρο της αυτοσυσχετιζόμενης συνάρτησης είναι μεγαλύτερο στα (δ_1) δευτερόλεπτα από το μέτρο εκείνων στα (δ_0) δευτερόλεπτα. Το μηδέν επιλέγεται στην αντίθετη περίπτωση.

Αποτελέσματα

Χρησιμοποιώντας την echo data hiding μέθοδο είναι εφικτή η εισαγωγή και ανίχνευση πληροφορίας σε μία ροή ψηφιακών δεδομένων με τη μικρότερη μεταβολή του αρχικού ηχητικού σήματος. Ο υδατογραφημένος ήχος δεν είναι αντιληπτός από το ανθρώπινο αυτί, ιδιαίτερα όταν χρησιμοποιούνται 16bps.



Εικόνα 81 **Αποτέλεσμα autocepstrum και αυτοσυσχέτισης στα Α : «1» και Β : «0»**

Έτσι η παραμόρφωση του αρχικού σήματος είναι πραγματικά μικρή και η υδατογράφηση δίνει βέλτιστα σε αποτελέσματα. Το μοναδικό μειονέκτημα είναι ότι δίνει έναν πιο ελαφρός εμπλουτισμένο ήχο λόγω της ένθεσης της ηχούς.

7.5 Συμπληρωματικές τεχνικές

Εκτός από τις παραπάνω βασικές τεχνικές υδατογράφησης ήχου που έχουν χρησιμοποιηθεί ευρέως υπάρχουν και κάποιες συμπληρωματικές τεχνικές υδατογράφησης ήχου που επίσης εφαρμόζονται. Αυτές είναι:

7.5.1 Προσαρμοσμένη Εξασθένηση Διανύσματος (Adaptic data attenuation)

Η βέλτιστη εξασθένηση του διανύσματος σχετίζεται άμεσα με την αλλαγή του επίπεδου θορύβου του ήχου που υδατογραφείται. Αυτή η τεχνική προσαρμόζει την εξασθένηση ώστε στα μικρά κομμάτια οι αλλαγές του ήχου ή του επίπεδου θορύβου να διατηρούν την κωδικοποιημένη πληροφορία θορύβου αρκετά χαμηλά στα αδύνατα ηχητικά κομμάτια ενώ στα ηχηρά κομμάτια προκαλεί την αύξηση του κωδικοποιημένου θορύβου.

7.5.2 Ανθεκτικότητα και κωδικοποίηση με διόρθωση λαθών

Η διαδικασία κωδικοποίησης χρησιμοποιείται στα δεδομένα που πρόκειται να ενσωματωθούν έτσι ώστε να αντισταθμίσει τα λάθη που προκαλούνται λόγω του θορύβου του καναλιού ή των μορφοποιήσεων του αρχικού ηχητικού σήματος. Η

εφαρμογή αυτής της τεχνικής επηρεάζει την αντιθετική σχέση του υδατογραφημένου ήχου που υπάρχει ανάμεσα στην ανθεκτικότητα και την ύπαρξη μεγάλου ρυθμού δεδομένων.

7.5.3 Ανάλυση των περιεχομένων του ήχου

Αυτή η τεχνική χρησιμοποιείται έτσι για να επιφέρει μία καλή ισορροπία μεταξύ της μέγιστης ποιότητας του ήχου που ενσωματώνεται στον αρχικό ήχο και της ενίσχυσης τα δεδομένα παραμένουν μη αντιληπτά. Βελτιώνει την ανίχνευση του λευκού Gaussian θορύβου όταν αυτός ενθέτεται σ' ένα ηχητικό σήμα το οποίο βρίσκεται πάνω από το επίπεδο του πραγματικού θορύβου του σήματος. Για να μπορέσει να το επιτύχει χρησιμοποιεί μία κβαντισμένη αναπαράσταση του επίπεδου του θορύβου η οποία βοηθά στον υπολογισμό του μέτρου της αλλαγής στα γειτονικά δείγματα του αρχικού σήματος.

Η κβαντισμένη αναπαράσταση του επίπεδου του θορύβου είναι:

$$\sigma^{2}_{\text{τοπικό}} = \frac{1}{|S_{\max}|} \times \frac{1}{N} \times \sum_{n=1}^{N-1} [s(n+1) - s(n)]^2$$

Αυτή η μέθοδος αναπαράστασης χρησιμοποιείται για την κατηγοριοποίηση των ηχητικών σημάτων ανάλογα με το επίπεδο θορύβου που περικλείουν.

Βιβλιογραφία

[I] W. Bender, D.Gruhl, N.Morimoto, and A.Lu. Techniques for data hiding. IBM Systems Journal, 35(3&4):313-335, 1996.

[2] Daniel Cruchl, Walter Bender. Echo Hiding

[3] W. Bender, "Data Hiding," News in the Future, MIT Media Laboratory, unpublished lecture notes (1994).

[4] P. Bassia and I. Pitas, Robust audio watermarking in the time domain, Signal processing IX, theories and applications: proceedings of Eusipco-98, Ninth European Signal Processing Conference, Rhodes, Greece, 8-11 September 1998 (Patras, Greece) (S. Theodoridis et al., eds.), Typorama Editions, 1998, pp. 25-28

[5] A.G.Bors and I.Pitas. Image watermarking using dct domain constrains. In Proceedings of ICIP'96, volume III, pages 231-234, Lausanne, Switzerland, September 1996

[6] G.Voyagtzis and I.Pitas. Chaotic mixing of digital images and applications to watermarking. In Proceedings of ECMAST'96, pages 687-694, Louvainn-la-Neuve, Belgium, 29-30 May 1996.

[7] I.Pitas. A method for signature casting on digital images. In Proceedings of ICIP'96, volume III, pages 215-218, Lausanne, Switzerland, September 1996

[8] N.Nikolaidis and I.Pitas. Robust image watermarking in the spatial domain. Signal processing, sp-issue on Copyright Protaction and Access control, to appear in 1998

[9]I. Pitas and T. Kaskalis, Applying signatures on digital images," in Nonlinear Signal Processing Workshop, Thessaloniki, Greece, pp. 460(463,1995.

[10] G.Voyatzis and I.Pitas. Digital image watermarking using mixing systems. Computer & Graphics, 22(3), 1998.

[II] E. Koch and J. Zhao, Towards robust and hidden image copyright labeling," in Nonlinear Signal Processing Workshop, Thessaloniki, Greece, pp. 452{455, 1995.

[12] J. A. Bloom, I. J. Cox, T. Kalker, J.-P. Linnartz, M. L. Miller, and B. Traw, Copy protection for DVD video. Proceedings of the IEEE, 87(7): 1267-1276, 1999.

[13] I.J.Cox, J.Kilian, F.T.Leighton and T.Shamoon. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12):1673-1687, 12 1997

[14] I. J. Cox and M. Miller. A Review of Watermarking and the Importance of Perceptual Modeling. In Proceedings of the IS&T/SPIE Conference on Human Vision & Electronic Imaging II,volume 3016, pages 92{99, San Jose, CA, February 1997.

[15] I. J. Cox and J.-P. Linnartz. Some general methods for tam-pering with watermarks. IEEE Trans, on Selected Areas of Communications, 16(4):587-593, 1998.

[16] J. Zhao E. Koch, J. Rmdfrey. Copyright Protection for Multimedia Data. In Proceedings of the International Conference on Digital Media and Electronic Publishing, pages 203(213, London,UK, 1996.

[17]E.Koch and J.Zhao. Towards robust and hidden image copyright labeling. In

Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Proceeding, pages 452-455, N.Marmaras, Greece, 20-22 June 1995.
[18] A. H. Tew_k, M. D. Swanson, B. Zhu, K. Hamdy,and L. Boney, Transparent Robust Watermarking for Images and Audio." To be submitted IEEE Trans, on Signal Proc, 1996.
[19] L. Boney, A.H.TewJc,· and K. N. Hamdy. Digital Watermarks for Audio Signals. In Proceedings of 1996 IEEE International Conference on Multimedia Computing and Systems, pages 473-480,Hiroshima, Japan, June 1996.
[20] Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik. Audio watermarking and data embedding - Current state of the art, challenges and future directions
[21] B. Zhu, A. Tew_k, and O. Gerek, Low Bit Rate Near-Transparent Image Coding," in Proc. of the SPIE Int. Conf. on Wavelet Apps. for Dual Use, vol. 2491, (Orlando, FL), pp. 173(184, 1995.
[22] L. Qiao and K. Nahrstedt. Watermarking Method for MPEG Encoded Video: Towards Resolving Rightful Ownership. Technical Report UIUCDCS-R-97-2032, University of Illinois at Urbana- Champaign, Urbana, IL, 1997.
[23] Lintian Qiao and Klara Nahrstedt: Non-Invertible Watermarking Methods For MPEG Encoded Audio, June, 1998.S.Craver, N. Memon, B-L. Yeo, and M. Yeung.
[24] Klara Nahrstedt and Smith: An application Driven-aproach of to networking multimedia systems
[25] Andersen, D. B. (1997b). Windows Sockets 2 Service Provider Interface. Technical report, Intel Corp. Version 2.2.1.
[26] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Attacks on copyright marking systems. Second International Workshop on Information Hiding, 14-17 April, 1998, Portland, Oregon,USA (Berlin, Germany / Heidelberg, Germany / London, UK /etc.) (David Aucsmith, ed.), Lecture Notes in Computer Science,vol. 1525, Springer-Verlag, 1998, pp. 219-239.
[27] F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn. Informa-tion hiding - a survey. Proceedings of the IEEE, 87(7): 1062-1077, 1999.
[28] D. K. Koukopoulos and Y.C. Stamatiou A Compressed-Domain Watermarking Algorithm for Mpeg Audio Layer 3
[29] Dittmann, J., Steinmetz, A., Nack, F., Steinmetz, R.: Interactive Watermarking Environments, to appear in IEEE Multimedia 1998, Austin Texas
[30] Dittmann Robust MPEG Video Watermarking Technologies
[31]Dittmann, L, Steinmetz, A.: Konzeption von Sicherheitsmechanismen fur das Projekt DiVidEd, GMD- Studie '97
[32] Fridrich, J. Methods for data hidung, Center for Intelligent Systems & Department of Systems Science and Industrial Engineering, SUNY Binghamton, Methods for Data Hiding", working paper (1997)
[33] Solomon, D. and Russinovich, M. (2000). Inside Windows 2000. Microsoft Press, Bellevue, WA, USA, 3rd edition.
[34] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman. Electronic Marking and Identication Techniques to Discourage Document Copying. In Proceedings of IEEE INFOCOM'94,volume 3, pages 1278(1287, Toronto, June 1994.
[35] G. Caronni. Assuring Ownership Rights for Digital Images. In Proceedings of Reliable IT Systems, VIS'95. Vieweg Publishing , Company, 1995.

[36] D.Kundur and D.Hatzinakos. A robust digital image watermarking method using wavelet-based fusion. In Proceedings of ICIP'97, volume I, pages 544-547, Atlanda, USA, October 1997.
[37] S. Craver, N. Memon, B. Yeo, and M. Yeung. Can Invisible Watermarks Resolve Rightful Ownerships? Technical Report RC 20509, IBM Research Division, July 1996.
[38] J. O Ruanaidh, W.J. Dowling, and F.M. Boland. Phase watermarking of digital images. In Proceedings of ICIP'96, volume III,pages 239-242, Lausanne, Switcherland, September 1996.
[39] Klara Nahrstedt and Smith: An application Driven-aproach of to networking multimedia systems
[40] R. L. Lagendijk G. C. Langelaar, J. C. A. van der Lubbe. Robust Labeling Methods for Copy Protection of Images. In Proceedings of the SPIE Conference onStorage and Retrieval for Image and Video Databases V, volume 3022, pages 298{309, San Jose, CA, February 1997.
[41] F. H. Hartung and B. Girod. Watermarking of MPEG-2 Encoded Video without Decoding and Reencoding. In Proceedings of the SPIE Conference on Multimedia Computing and Networking 1997, volume 3020, pages 264(274, San Jose, CA, February 1997.
[42] International Standards Organization. Information technology { Coding of Moving Pictures and Associated Audio for Digital Storage Media at up to about 1.5 mbit/s { Part 3: Audio. International Standard ISO/IEC IS 11172-3, 1993.
[43] D. Pan. A Tutorial on Mpeg/audio Compression. IEEE Multimedia, pages 60 {74, Summer 1995.
[44] J.J. Quisquarter, J.F.Delaigle, J.M.Boucqueau and B.Macq. Digital images protection techniques in a broadcast framework : An overview. In Proceedings of ECMAST'96, pages 711-727, Louvain-la- Neuve, Belgium, 28-30 May 1996
[45] J. R. Smith and B. O. Comiskey. Modulation and Information Hiding in Images. In Workshop on Information Hiding, Isaac Newton Institute, University ofCambridge, UK, May 1996.Springer-Verlag Lecture Notes in Computer Science Volume 1174.
[46] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding Secret Information into a Dithered Multi-level Image. In Proceedings of 1990 IEEE Military Communications Conference, pages 216{220, 1990.
[47] L. F. Turner. Digital Data Security System. Patent IPN WO 89/08915, 1989.
[48] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A Digital Watermark. In Proceedings of the International Conference on Image Processing, volume 2, pages 86{90, IEEE, 1994.
[49] J. O Ruanaidh and T.Pun. Rotation, scale and translation invariant digital image watermarking. In Proceedings of ICIP'97, volume I, pages 536-539, Atlanta, USA, October 1997.
[50] Christoph Busch, Wolfgang Funk, and Stephen Wolthusen, Digital watermarking: From concepts to real-time video applications, IEEE Computer Graphics and Applications 19 (1999), no. 1, 25-35.
[51] C. Neubauer and J. Herre, Digital watermarking and its influ-ence on audio quality, Proceedings of the 105th Convention of the Audio Engineering Society, San Francisco, USA 26-29 September, 1998 (Anonymous, ed.), 1998.

[52] Busch, C, Funk, W., and Wolthusen, S. (1999). Digital watermarking: From concepts to real-time video applications. IEEE Computer Graphics and Applications, 19(1):25—35.
[53] L. Piron, M. Arnold, M. Kutter, W. Funk, M. Boucqueau, and F. Craven, Octalis benchmarking: comparison of four water-marking techniques, Security and Watermarking of Multime-dia Contents (San Jose, California) (Ping Wah Wong and Ed-ward J. Delp, eds.), vol. 3657, January 1999, pp. 240-250.
[54] D.L. Hecht. Embedded data clyph technology for hardcopy digital documents. In proceedings of SPIE, volume 2171, 1995.
[55] B.M. Macq and J.J.Quisquarter. Cryptology or Digital TV broadcasting. Proceeding of the IEEE, 83:944-957, June 1995
[56] O. Bruyndonckx, J.-J. Quisquater, andB. Macq, Spatial method for copyright labeling of digital images," in Nonlinear Signal Processing Workshop, Thessaloniki, Greece, pp. 456(459, 1995.
[57] J. R. Smith and B. O. Comiskey, Modulation and Information Hiding in Images." to appear 1996 Workshop on Information Hiding, University of Cambridge, UK.
[58] N. Jayant, J. Johnston, andR. Safranek, Signal Compression Based on Models of Human Perception," Proc. of the IEEE, vol. 81, pp. 1385{1422,oct 1993.
[59] S.Flaykin, Communication Systems, 3rd Edition.New York, NY: John Wiley and Sons, 1994.
[60] G. E. Legge and J. M. Foley, Contrast Masking in Human Vision," J. Opt. Soc. Am., vol. 70, no. 12, pp. 1458(1471, 1980.
[61] Chiou-Ting Hsu, Ja-Ling Wu. DCT-Based Watermarking for Video. IEEE Transactions on Consumer Electronincs, Vol 44, No 1,February 1988 pp 206-216
[62] M. Kutter, F. Jordan, and F.Bossen. Digital watermarking of color images using amplitude modulation. Journal of Electronic Imaging, 7(2):326-332, 1998.
[63] A.Papoulis. Probability & Statistics. Prentice Hall, 1991.
[64] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp. Perceptual watermarks for digital images and video. Proc. of the IEEE,87(7): 1108-1126, 1999.
[65] Scott Moskowitz: So this is Convergence Technical, Economic, Legal, Crypto-graphic,and Philosophical Considerations for Secure Implementations of Digital Water-marking,Blue Spike inc., 1998.
[66] Fabien A.P. Petitcolas: MP3Stego, Com-puter Laboratory, Cambridge, August 1998.
[67] P. Sweene, Error Control Coding (An Introduction), Prentice-Hall International Ltd., Englewood Cliffs, NJ (1991).
[68] E. Adelson, Digital Signal Encoding and Decoding Apparatus,U.S. Patent No. 4,939,515 (1990).
[69] R. Machado, "Stego," http://www.nitv.net/~mech/Romana/stego.html (1994).
[70] D.R.Stinson. Cryptografy, Theory and Practice. CRC Press New York, 1995
[71] A. Lippman, Receiver-Compatible Enhanced EDTV System, U.S. Patent No. 5,010,405 (1991).
[72] D. L. Hecht, "Embedded Data Glyph Technology for Hardcopy Digital Documents," SPIE 2171(1995).
[73] K. Matsui and K. Tanaka, "Video-Steganography: How to Secretly Embed a Signature in a Picture,"IMA Intellectual Property Project Proceedings (1994).
[74] R. C. Dixon, Spread Spectrum Systems, John Wiley & Sons, Inc., New York

(1976).
[75] S.K.Marvin, Spread Spectrum Handbook, McGraw-Hill, Inc.,New York (1985).
[76] Digimarc Corporation, Identification/Authentication Coding Method and Apparatus, U.S. Patent (1995).
[77] A. V. Drake, Fundamentals of Applied Probability, McGraw-Hill, Inc., New York (1967).
[78] L. R. Rabiner and R. W. Schaffer, Digital Processing of Speech Signal, Prentice-Hall, Inc., Englewood Cliffs, NJ (1975).
[79] A. V. Oppenheim and R. W. Shaffer, Discrete-Time Signal Processing, Prentice-Hall, Inc., Englewood Cliffs, NJ (1989).
[80] http://www.informatik.tu-muenchen.de/ stowasse/security.html. [81] http://www.sag.org/pressreleases/prla990826 spotchecks.html, 1999.
[82] C. R. Abbey and H. H. Pursel. Data channel monitor. United States Patent, (3,415,947), 1968.
[83] D. E. H. amd C. M. Solar. Automatic monitor for programs broadcast. United States Patent, (4,025,851), 1977.
[84] A. E. Bell. The dynamic digital disk. IEEESpectrum,36(10):28-35, 1999.
[85] J.Brassil, S.Low, N.Maxemchuck and L.O.Gorman. Electronick marking of identification techniques to discourage document copying. In proceedings of Infocom'94, pages 1278-1287, June 1994
[86] R. S. Broughton and W. C. Laumeister. Interactive video method and apparatus. United States Patent, (4,807,031),1989.
[87] X.G.Xia, C.G.Boncelet and G.R.Arce. A multiresolution watermark for digital images. In Proceedings of ICIP'97, volume I, pages 548-551, Atlanda, USA, October 1997.
[88] M. G. Crosby. Communication including submerged identi-fication signal. United States Patent, (3,845,391), 1974.
[89] G. L. Friedman. The trustworthy camera: restoring credi-bility to the photographic image. IEEE Trans. On Consumer Electronics, 39(4):905-910, 1993.
[90] G. L. Friedman. Digital camera with apparatus for authen-tication of images produced from an image file. U.S. Patent,(5,499,294), 1996.
[91] F. Hartung and M. Kutter. Multimedia watermarking tech-niques. Proceedings of the IEEE, 87(7):1079-1107, 1999.
[92] E. F. Hembrooke. Identification of sound and like signals.United States Patent, (3,004,104), 1961.
[93] D. Kilburn. Dirty linen, dark secrets. Adweek, 1997.
[94] C.-Y. Lin and S.-F. Chang. A robust image authentication algorithm surviving jpeg compression. In SPIE Storage and Retireval of Image/Video Databases, 1998.
[95] C.-Y. Lin and S.-F. Chang. Issues and solutions for authen-tieating mpeg video. In Proc. IS&T/SPIE Syposium on Elec-tronic Imaging: Science and Technology (EΓ99) - SPIE Se-curity and Watermarking of Multimedia Contents, 1999.
[96] T. Ohsawa and M. Karita. Automatic telecasting or ra-dio broadcasting monitoring system. United States Patent,(3,760,275), 1973.
[97] Busch, C., Graf, F., Wolthusen, S., and Zeidler, A. (2000). A system for in-

tellectual property protection. In Proceedings of the World Multiconference on Systemics, Cybernetics, and Informatics (SCI 2000) /Int'l Conf. on In-formation Systems Analysis and Synthesis (ISAS 2000), Orlando, FL, pages 225-230.
[98] G. J. Simmons. The prisoners' problem and the subliminal channel. In Proc. CRYPTO'83, pages 51-67. Plenum Press,1984.
[99] D. R. Stinson. Cryptography: Theory and Practice. CRC Press, 1995.
[100] W. M. Tomberlin, L. G. MacKenzie, and P. K. Bennett. System for transmitting and receiving coded entertainment programs. United States Patent, (2,630,525), 1953.
[101] Jones, M.B. (1993). Interposition agents: Transparently interposing user code at the system interface. In Liskov, B., editor, Proceedings of the 14th Symposium on Oper ating Systems Principles, pages 80-93, New York, NY, USA. ACM Press.
[102] Dierks, T. and Allen, C. (1999). RFC 2246: The TLS Protocol Version 1.0.Frier, A, Karlton, P., and Kocher, P. (1996). The Secure Socket Layer (SSL) 3.0 Protocol. Technical report, Netscape Communications Corp.
[103] McKusick, M. K., Bostic, K., Karels, M. I, and Quarterman, J. S. (1996). The Design and Implementation of the 4.4 BSD UNIX Operating System. Addison-Wesley Publishing Company.
[104]National Institute for Standards and Technology (U. S.) (1995). Secure Hash Standard (SHA). Federal information processing standards publication 180-1, NIST, Gaithersburg, MD, USA.
[105]National Institute of Standards and Technology (U. S.) (1994). Data Encryption Standard (DES). Federal information processing standards publication 46-2, NIST, Gaithersburg, MD, USA. Supersedes FIPS PUB 46-1-1988 January 22.
[106] Reynolds, F. and Heller, J. (1991). Kernel support for network protocol servers. In USENIX, editor, Proceedings of the USENIXMach Symposium: November 20-22, 1991, Monterey, California, USA, pages 149-162, Berkeley, CA, USA. USENIX.
[107] Snider, L. B. and Seikaly, D. S. (2000). Report on Investigation: Improper Handling of Classified Information by John M. Deutch. Central Intelligence Agency Inspector General Report 1998-0028-IG. Unclassified, FOUO.
[108]Solomon, D. (1998). Inside Windows NT. Microsoft Press, Bellevue, WA, USA,2nd edition.