Εφαρμογή μεθόδων υδατογραφίας και στεγανογραφίας για προστασία περιεχομένου

ΟΡΜΕΝΑΪ ΕΡΚΕΛΑ

ΑΜ: 9382

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΛΙΑΡΟΚΑΠΗΣ ΔΗΜΗΤΡΙΟΣ

ΑΤΕΙ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ

ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τίτλος

ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Εφαρμογή μεθόδων υδατογραφίας και στεγανογραφίας για προστασία περιεχομένου

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

Λιαροκάπης Δημήτριος

ΗΜΕΡΟΜΗΝΙΑ, ΤΟΠΟΣ

2015 - ΑΡΤΑ

Περίληψη

Η ταχεία ανάπτυξη ανταλλαγής ψηφιακών μέσων και μεταφοράς μέσω δικτύων υπολογιστών καθιστά το ζήτημα της προστασία του ψηφιακού περιεχομένου ένα κρίσιμο θέμα για τα πνευματικά δικαιώματα και την πιστοποίηση του ιδιοκτήτη του περιεχομένου. Αυτή η ειδική ανάγκη, έδωσε κίνητρα στους επιστήμονες να μελετήσουν και να αναπτύξουν αποτελεσματικές μεθόδους που είναι σε θέση να προστατέψουν τις ψηφιακές εικόνες, βίντεο, ήχους από κακόβουλες ενέργειες που τείνουν να νοθεύουν ή κάνουν παράνομη χρήση αυτών, χωρίς τη λήψη άδειας από τον ιδιοκτήτη. Μια δημοφιλής και αποτελεσματική μέθοδος που χρησιμοποιείται συνήθως για να εξασφαλίσει την αυθεντικότητα της ψηφιακής εικόνας είναι η γνωστή διαδικασία της υδατογράφησης. Στεγανογραφία είναι η τέχνη ή η πρακτική της απόκρυψης ενός μηνύματος, εικόνας, ή ενός αρχείου μέσα σε ένα άλλο μήνυμα, εικόνα ή αρχείο. Το πλεονέκτημα της στεγανογραφίας έναντι της κρυπτογραφίας είναι ότι το ότι το μυστικό μήνυμα που δεν προσελκύει την προσοχή ως αντικείμενο εξέτασης. Όλες οι τεχνικές απόκρυψης πληροφοριών μπορούν να χρησιμοποιηθούν για την ανταλλαγή steganograms σε τηλεπικοινωνιακά δίκτυα και μπορούν να ταξινομηθούν κάτω από τον γενικό όρο στεγανογραφία δικτύου.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ:Μετασχηματισμός,DCT,Wavelet,moment,Δείκτες εικόνας PSNR,SSIM,Στεγανογραφία,Υδατογραφία,Matlab.

Abstract

The rapid development of digital media exchange and transmission via computer networks makes the issue of protection of digital content a critical issue for the copyright and the certification of the content owner. This particular need has motivated scientists to study and develop effective methods that are able to protect their digital photos, videos, sounds of malicious actions that tend to distort or make unauthorized use thereof, without obtaining permission from the owner. A popular and effective method that is commonly used to ensure the authenticity of the digital image is the known process of watermarking. Steganography is the art or practice of concealing a message, image, or file within another message, image or file. The advantage of steganography over cryptography is that the secret message that does not attract attention as a test article. All information concealment techniques can be used to exchange steganograms telecommunication networks and can be classified under the general term of network steganography.

Κατάλογος περιεχομένων

Περίληψη……..2
Abstract…….3
Κεφάλαιο 1. Μελέτη διάφορων μετασχηματισμών εικόνων 5
1.1 Μετασχηματισμός DCT.....5
1.2 Μετασχηματισμός Wavelet.....6
1.3 Μετασχηματισμός SVD.....10
1.4 Μετασχηματισμός moments.....11
1.5 Δείκτες ποιότητας εικόνας.....12
1.5.1 PSNR.....12
1.5.2 SSIM.....14
1.5.3 Δείκτης ποιότητας εικόνας.....15
Κεφάλαιο 2. Στεγανογραφία.....17
2.1 Ιστορική αναδρομή Στεγανογραφίας.....17
2.2 Ορισμός στεγανογραφίας και μεθοδοι.....21
2.3 Δίκτυα.....24
2.4 Στεγαναλυση.....25
2.5 Στεγανογραφία στην σημερινή εποχή.....27
2.6 Ο ρόλος της στεγανογραφίας στη τρομοκρατία.....28
Κεφάλαιο 3. Υδατογραφία.....30
3.1 Ιστορική αναδρομή Υδατογραφίας 30
3.2 Ορισμός υδατογραφίας και οι κατηγορίες (σε κείμενο-βίντεο-ήχο-εικόνα).....31
3.3 Τεχνική αφαίρεσης υδατογραφίας.....37
3.4 Πιστοποίηση αυθεντικότητας δεδομένων.....39
Κεφάλαιο 4. Εισαγωγή στο MATLAB 42
4.2 Εφαρμογή Στεγανογραφίας…… 44
4.2.1 Κώδικας Στεγανογραφίας…….....48
4.3 Εισαγωγή Υδατογραφίας.....49
4.4 Εξαγωγή Υδατογραφίας.....53
4.5 Προγράμματα χωρίς κώδικα.....59
4.5.1 Απόκρυψη εικόνας.....59
4.5.2 Εμφάνιση κρυμμένης εικόνας.....64
4.5.3 Υδατογραφία.....68
Βιβλιογραφία..... 72

Κεφάλαιο 1. Μελέτη διάφορων μετασχηματισμών εικόνων

1.1 Μετασχηματισμός DCT[1]

Ο μετασχηματισμός διακριτού συνημιτόνου (discrete cosine transform - DCT) εκφράζει μια πεπερασμένη ακολουθία σημείων δεδομένων σε όρους ενός αθροίσματος συναρτήσεων συνημίτονου σε διαφορετικές συχνότητες . Οι μετασχηματισμοί DCT είναι σημαντικοί για πολλές εφαρμογές στον τομέα της επιστήμης και της μηχανικής, από τις απλές τεχνικές συμπίεσης του ήχου (π.χ. MP3) και εικόνας (π.χ. JPEG) (όπου είναι δυνατόν να απορρίπτονται μικρές συνιστώσες υψηλής συχνότητας), ως τις φασματικές μεθόδους για την αριθμητική επίλυση μερικών διαφορικών εξισώσεων . Η χρήση του συνημίτονου και όχι του sine είναι μεγάλης σημασίας σε αυτές τις εφαρμογές καθώς στη συμπίεση, αποδεικνύεται ότι το συνημίτονο είναι πολύ πιο αποδοτικό, ενώ στις διαφορικές εξισώσεις τα συνημίτονα εκφράζουν μια συγκεκριμένη επιλογή των οριακών συνθηκών.

Ειδικότερα, ένας μετασχηματισμός DCT είναι ένας μετασχηματισμό που βασίζεται στον Fourier και είναι παρόμοιος με το διακριτό μετασχηματισμό Fourier (DFT), αλλά χρησιμοποιώντας μόνο πραγματικούς αριθμούς.

Ο DCT χρησιμοποιείται συχνά στην επεξεργασία σήματος και εικόνας, ειδικά για συμπίεση δεδομένων με απώλειες, επειδή έχει μια ισχυρή ιδιότητα "συμπίεσης", οι περισσότερες από τις πληροφορίες του σήματος τείνουν να πρέπει να είναι συγκεντρωμένες σε λίγες συνιστώσες χαμηλής συχνότητας του DCT, πλησιάζοντας τον μετασχηματισμό Karhunen-Loève (ο οποίος είναι βέλτιστος υπό την έννοια decorrelation) για σήματα με βάση ορισμένα όρια των διαδικασιών Markov .

1 Narasimha, M.; Peterson, A. (June 1978). "On the Computation of the Discrete Cosine Transform". IEEE Transactions on Communications 26 (6): 934–936.

1.2 Μετασχηματισμός Wavelet[3][4]

Κατά τα τελευταία έτη, ο μετασχηματισμός wavelet (κυματιδίων) έχει εμφανισθεί έντονα στον τομέα της επεξεργασίας εικόνας / σήματος ως εναλλακτική λύση για το γνωστό Fourier Transform (FT) και τους σχετικούς μετασχηματισμού με αυτόν, δηλαδή, τον διακριτό μετασχηματισμό συνημίτονου (DCT) και τον Διακριτό Μετασχηματισμό ημιτόνου (DST). Στη θεωρία Fourier, ένα σήμα (μια εικόνα θεωρείται ως ένα πεπερασμένο σήμα 2 - D) εκφράζεται ως άθροισμα , θεωρητικά άπειρο, ημιτόνων και συνημιτόνων, κάνοντας τον FT κατάλληλο για την ανάλυση άπειρων και περιοδικών σημάτων. Για αρκετά χρόνια, ο FT κυριάρχησε πλήρως στον τομέα της επεξεργασίας σήματος, όμως, ενώ παρέχει πληροφορίες συχνότητας που περιέχονται στην ανάλυση του σήματος, παρέλειψε να δώσει οποιαδήποτε πληροφορία σχετικά με το χρόνο εμφάνισης του σήματος.

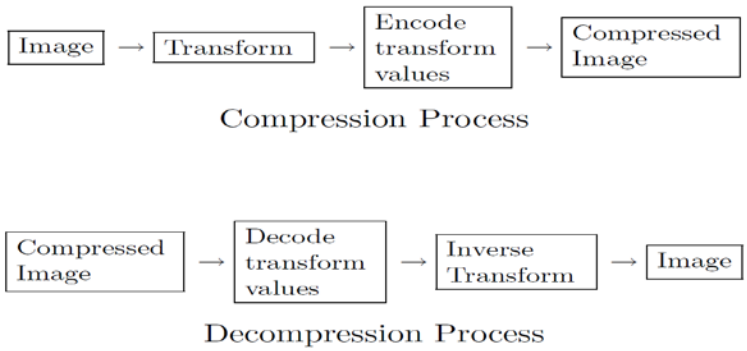
Αυτή η αδυναμία, χωρίς να είναι η μοναδική, ώθησε τους επιστήμονες να διερευνήσουν τη πιθανότητα δημιουργίας ενός μετασχηματισμού που δεν θα έχει τα μειονεκτήματα του FT. Το πρώτο βήμα σε αυτό το μακρύ ταξίδι της έρευνας ήταν να μειωθεί το σήμα σε διάφορα τμήματα και στη συνέχεια να εξετάσουμε το κάθε τμήμα ξεχωριστά. Η ιδέα με μια πρώτη ματιά φαίνεται να είναι πολύ ελπιδοφόρα, δεδομένου ότι επέτρεψε την άντληση πληροφοριών χρόνου και τον εντοπισμός των διαφόρων συνιστωσών συχνοτήτων. Η προσέγγιση αυτή είναι γνωστή ως μετασχηματισμός Short -Time Fourier (STFT). Το θεμελιώδες ερώτημα που τίθεται εδώ είναι πώς θα χωριστεί σε τμήματα το σήμα. Η καλύτερη λύση σε αυτό το δίλημμα ήταν φυσικά να βρεθεί ένα πλήρως επεκτάσιμο διαμορφωμένο παράθυρο στο οποίο καμία περικοπή σήματος δεν θα είναι πλέον αναγκαία. Αυτός ο στόχος επιτεύχθηκε επιτυχώς με την χρήση του μετασχηματισμού wavelet.

Τυπικά, ο μετασχηματισμός wavelet ορίζεται από πολλούς συγγραφείς ως μια μαθηματική τεχνική κατά την οποία αναλύεται ένα συγκεκριμένο σήμα (ή συντίθενται) στο πεδίο του χρόνου με τη χρήση διαφορετικών εκδοχών μίας καθυστερημένης ή μετατοπισμένης συνάρτησης βάσης που ονομάζεται πρωτότυπο wavelet ή η μητέρα wavelet. Ωστόσο, στην πραγματικότητα, ο μετασχηματισμός wavelet βρήκε την ουσία του και προήλθε από διαφορετικούς επιστημονικούς κλάδους και δεν ήταν, όπως ανέφερε ο Mallat, εντελώς νέος για

3 Chui, Charles K. (1992). *An Introduction to Wavelets*. San Diego: Academic Press
4 R. Polikar, (1999). The wavelet tutorial. Διαθέσιμο: http://users.rowan.edu/~polikar/WAVELETS/WTtutorial.html

τους μαθηματικούς που εργάζονται σε θέματα αρμονικής ανάλυσης, ή σε ερευνητές υπολογιστών που μελετούν την επεξεργασία εικόνας πολλαπλών κλιμάκων (Mallat, 1989). Στις αρχές του 20ου αιώνα, ο Haar, ένας Γερμανός μαθηματικός παρουσίασε το πρώτο μετασχηματισμό wavelet (σχεδόν έναν αιώνα μετά την εισαγωγή της FT , από το γαλλικό J. Fourier). Η συνάρτηση βάσης Haar wavelet έχει συμπαγή φορέα και ακέραιους συντελεστές. Αργότερα , η βάση Haar χρησιμοποιείται στη φυσική για να μελετήσει την κίνηση Brown. Από τότε, διαφορετικές εργασίες έχουν πραγματοποιηθεί είτε στην ανάπτυξη της θεωρίας που σχετίζεται με τα wavelet ή προς την εφαρμογή τους σε διάφορους τομείς.

Στον τομέα της επεξεργασίας σήματος, τα μεγάλα επιτεύγματα στις διάφορες μελέτες των Mallat, Meyer και Daubechies επέτρεψαν την εμφάνιση ενός ευρέος φάσματος wavelet-based εφαρμογών. Στην πραγματικότητα, εμπνευσμένος από το έργο που αναπτύχθηκε από τον Mallat σχετικά με τις σχέσεις μεταξύ των φίλτρων Quadrature Mirror (QMF), των αλγόριθμων της πυραμίδας και των ορθοκανονικών βάσεων κυματιδίων (Mallat, 1989), ο Meyer κατασκεύασε τα πρώτα μη - τετριμμένα wavelets (Meyer, 1989). Ωστόσο , το πιο σημαντικό έργο πραγματοποιήθηκε από την Ingrid Daubechies. Με βάση το έργο του Mallat, η Daubechies κατάφερε να κατασκευάσει ένα σύνολο συναρτήσεων wavelet με ορθοκανονική βάση, τα οποία έχουν γίνει ο ακρογωνιαίος λίθος πολλών εφαρμογών (Daubechies, 1988) . Λίγα χρόνια αργότερα, η ίδια συγγραφέας, σε συνεργασία με άλλους (Cody, 1994), παρουσίασε ένα σύνολο συναρτήσεων biorthogonal wavelets, το οποίο χρησιμοποιήθηκε αργότερα σε διάφορες εφαρμογές, ιδίως στην κωδικοποίηση της εικόνας. Πρόσφατα, η JPEG2000, μία συμπίεση βασισμένη στα biorthogonal wavelets έχει υιοθετηθεί ως το νέο πρότυπο συμπίεσης (Ebrahimi et al . , 2002).



Εικόνα 1.1 Συμπίεση με μετασχηματισμό

Εικόνα 1.2 Εικόνα Goldhill με διάφορους τύπους συμπίεσης

Σύμφωνα με τον ίδιο συγγραφέα, για να καλέσει κανείς μια συγκεκριμένη συνάρτηση ως ένα σύστημα wavelet , θα πρέπει να πληροί τις ακόλουθες τρεις ιδιότητες:

- Τα Wavelets είναι δομικά στοιχεία για γενικές λειτουργίες: Χρησιμοποιούνται για να αντιπροσωπεύουν σήματα και γενικότερα συναρτήσεις. Με άλλα λόγια, μια συνάρτηση αντιπροσωπεύεται στο χώρο των wavelets από την μέση της άπειρης ακολουθίας wavelets .
- Τα Wavelets έχουν εντοπισμό χώρου-συχνότητας: Πράγμα που σημαίνει ότι το μεγαλύτερο μέρος της ενέργειας ενός wavelet περιορίζεται σε ένα πεπερασμένο χρονικό διάστημα και ότι ο μετασχηματισμός περιέχει μόνο τις συχνότητες από μια ορισμένη ζώνη συχνοτήτων.
- Τα Wavelets υποστηρίζουν τους γρήγορους και αποτελεσματικούς αλγορίθμους μετασχηματισμού: Η απαίτηση αυτή είναι απαραίτητη κατά την

εφαρμογή του μετασχηματισμού . Συχνά οι μετασχηματισμοί wavelet χρειάζονται O (n) πράξεις, πράγμα που σημαίνει ότι ο αριθμός των πολλαπλασιασμών και των προσθέσεων ακολουθεί γραμμικά το μήκος του σήματος . Αυτή είναι μια άμεση επίπτωση του ότι ο μετασχηματισμός είναι συμπαγής. Ωστόσο, πιο γενικοί γενικότερα WTs απαιτούν O (nlog (n)) εργασίες (π.χ. undecimated wavelet).

Για να βελτιωθεί ο ορισμός των wavelet, τα ακόλουθα τρία χαρακτηριστικά έχουν προστεθεί από τους Sweldens και Daubechies (Sweldens , 1996 & Daubechies , 1992 , 1993), όπως αναφέρεται στο (Burrus et αϊ , 1998) :

- Μοναδικότητα της συνάρτησης παραγωγής : Αναφέρεται στην ικανότητα της δημιουργίας ενός σύστημα κύματος από μια ενιαία συνάρτηση κλιμάκωσης ή μια συνάρτηση wavelet μόνο με κλιμάκωση και μετάφραση.
- Ικανότητα πολλαπλών αναλύσεων: Η έννοια αυτή, η οποία έχει προηγουμένως εισαχθεί από τον Mallat, δηλώνει την ικανότητα του μετασχηματισμού να αντιπροσωπεύει ένα σήμα ή μια συνάρτηση σε διαφορετικό επίπεδο, με διαφορετικά σταθμισμένα αθροίσματα , που προέρχεται από το αρχικό.
- Δυνατότητα δημιουργίας συντελεστών χαμηλότερου επίπεδου από τους συντελεστές υψηλότερου επίπεδου. Αυτό μπορεί να να επιτευχθεί με τη χρήση της δομημένης αλυσίδας φίλτρων που ονομάζονται Filter Banks.

Ο μετασχηματισμός wavelet διαχωρίζεται σε συνεχή (continuous wavelet transforms – CWT) και διακριτό (discrete wavelet transform – DWT).

Ο τύπος που μας δείνει το μετασχηματισμό CWT είναι ο εξής:

$$CWT(\tau, s) = \frac{1}{\sqrt{|s|}} \int_{-\infty}^{+\infty} x(t)\, h^*\left(\frac{t-\tau}{s}\right) dt$$

Ο τύπος υπολογισμού του DWT είναι ο εξής:

$h_{j,k}(t) = \sigma_o^{-j/2}\, h(\sigma_o^{-j}t - kT)$, όπου $\sigma=\sigma_o^j$ και $T=k\sigma_o^j\tau$.

1.3 Μετασχηματισμός SVD[5][6]

Στη γραμμική άλγεβρα, ο μετασχηματισμός Singular Value Decomposition (SVD) είναι η παραγοντοποίηση μίας πραγματικής ή σύνθετης μήτρας, με πολλές χρήσιμες εφαρμογές στην επεξεργασία σήματος και στην στατιστική. Επισήμως, ο SVD μίας μήτρας m × n M πραγματικής ή σύνθετης είναι μια παραγοντοποίηση της μορφής

$$\mathbf{M} = \mathbf{U\Sigma V}^*$$

όπου U είναι μία m × m πραγματική ή πολύπλοκη μήτρα, Σ είναι ένας m × n ορθογώνιος διαγώνιος πίνακας με μη αρνητικούς πραγματικούς αριθμούς στη διαγώνιο, και V * (το συζυγές ανάστροφο του V, ή απλά το ανάστροφο του V, αν V είναι πραγματικός) είναι ένας n × n μοναδιαίος πίνακας. Οι διαγώνιες καταχωρήσεις του Σ είναι γνωστές ως οι ιδιάζουσες τιμές του M. Οι m στήλες του U και οι n στήλες του V ονομάζεται αριστεροί μοναδιαίοι δείκτες και δεξιοί μοναδιαίοι δείκτες του M, αντίστοιχα.

Ο SVD και η eigendecomposition συνδέονται στενά. Δηλαδή:

- Οι αριστεροί μοναδιαίοι δείκτες του M είναι ιδιοδιανύσματα του MM *.
- Οι δεξιοί μοναδιαίοι δείκτες του M είναι ιδιοδιανύσματα του M * M.
- Οι μη μηδενικές ιδιάζουσες τιμές του M (βρίσκονται στις διαγώνιες καταχωρήσεις Σ) είναι οι τετραγωνικές ρίζες των μη μηδενικών ιδιοτιμών των δύο M * M και MM *.

Οι εφαρμογές που χρησιμοποιούν το SVD περιλαμβάνουν τον υπολογισμό του pseudoinverse, ευθεία ελαχίστων τετραγώνων των δεδομένων, προσέγγιση μήτρας, καθώς και τον προσδιορισμό της κατάταξης, εύρους και μηδενικού χώρου της μήτρας.

5 GSL Team (2007). *§14.4 Singular Value Decomposition*. GNU Scientific Library. Reference Manual. Διαθέσιμο: http://www.gnu.org/software/gsl/manual/html_node/Singular-Value-Decomposition.html

6 Wall, Michael E., Andreas Rechtsteiner, Luis M. Rocha (2003). *Singular value decomposition and principal component analysis.* Διαθέσιμο: http://public.lanl.gov/mewall/kluwer2002.html

1.4 Μετασχηματισμός moments[7]

Στην επεξεργασία εικόνας, τεχνητή όραση και σε συναφείς τομείς, ένα στιγμιότυπο εικόνας είναι ορισμένο ειδικά σταθμισμένος μέσος όρος (στιγμιότυπο) των εντάσεων των pixels της εικόνας, ή μια συνάρτηση από τέτοιες στιγμές, συνήθως επιλέγεται να έχουν κάποια θετική ιδιότητα ή ερμηνεία.

Τα στιγμιότυπα εικόνας είναι χρήσιμα για να περιγράψουν αντικείμενα, μετά την τμηματοποίηση. Απλές ιδιότητες της εικόνας που βρίσκονται μέσω στιγμιοτύπων εικόνας περιλαμβάνουν την επιφάνεια (ή τη συνολική ένταση), το κέντρο βάρους, καθώς και πληροφορίες σχετικά με τον προσανατολισμό της .

Για μία 2D συνεχή συνάρτηση f (x,y) το στιγμιότυπο (μερικές φορές ονομάζεται και ακατέργαστο) της τάξης (p + q) ορίζεται ως

$$M_{pq} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x^p y^q f(x,y)\, dx\, dy$$

για p, q = 0,1,2, ... Η προσαρμογή αυτής σε εικόνα με διαβαθμίσεις (κλίμακα του γκρι) με εντάσεις pixel I (x, y), γίνεται με τα ακατέργαστα στιγμιότυπα που υπολογίζονται ως εξής:

$$M_{ij} = \sum_x \sum_y x^i y^j I(x,y)$$

Σε ορισμένες περιπτώσεις, αυτό μπορεί να υπολογιστεί με την εξέταση της εικόνας ως συνάρτηση πυκνότητας πιθανότητας, δηλαδή, διαιρώντας το παραπάνω με

$$\sum_x \sum_y I(x,y)$$

Ένα θεώρημα μοναδικότητας (Hu, 1962) δηλώνει ότι αν η f (x, y) είναι τμηματικά συνεχής και έχει μη μηδενικές τιμές μόνο σε ένα πεπερασμένο τμήμα του επίπεδου xy, τα στιγμιότυπα όλων των τάξεων υπάρχουν, και η ακολουθία τους (M pq) είναι προσδιορίζεται μονοσήμαντα από την f (x,y). Αντιστρόφως, η (M pq) προσδιορίζει μονοσήμαντα την f (x,y). Στην πράξη, η εικόνα συνοψίζεται με συναρτήσεις στιγμιοτύπων χαμηλότερης τάξης.

7 Coatrieaux et al. (2010). *Reconstruction of tomographic images from limited range projections using discrete Radon transform and Tchebichef moments.* Pattern Recognition 43, pp 1152--1164

1.5 Δείκτες ποιότητας εικόνας

1.5.1 PSNR[8]

Ο μέγιστος λόγος σήματος προς θόρυβο, με τη συντομογραφία PSNR, είναι ένας όρος που δείχνει τη σχέση μεταξύ της μέγιστης δυνατής ισχύος του σήματος και την ισχύ του θορύβου που επηρεάζει την πιστότητα της αναπαράστασης του. Επειδή πολλά σήματα έχουν πολύ μεγάλη δυναμική περιοχή, ο PSNR εκφράζεται συνήθως στην λογαριθμική κλίμακας ντεσιμπέλ.

Ο PSNR πιο συχνά χρησιμοποιείται για τη μέτρηση της ποιότητας της ανοικοδόμησης των codecs ή της συμπίεσης με απώλειες (π.χ., για την συμπίεση εικόνας). Το σήμα σε αυτή την περίπτωση είναι τα αρχικά δεδομένα, και ο θόρυβος είναι το σφάλμα που εισάγεται με τη συμπίεση. Κατά τη σύγκριση των codecs συμπίεσης, ο PSNR είναι μια προσέγγιση για την ανθρώπινη αντίληψη της ποιότητας της ανασυγκρότησης. Παρά το γεγονός ότι ένα υψηλότερο PSNR γενικά δείχνει ότι η ανοικοδόμηση είναι υψηλότερης ποιότητας, σε ορισμένες περιπτώσεις, μπορεί και όχι. Ο δείκτης PSNR ισχύει μόνο όταν χρησιμοποιείται για να συγκρίνει τα αποτελέσματα από τον ίδιο κωδικοποιητή (ή τύπο κωδικοποιητή) και το ίδιο περιεχόμενο.

Ο PSNR είναι πιο εύκολο να ορίζεται μέσω του μέσου τετραγωνικού σφάλματος (MSE). Λαμβάνοντας υπόψη μια μονόχρωμη εικόνα I χωρίς θόρυβο m × n και την θορυβώδη προσέγγιση της K, ο MSE ορίζεται ως εξής:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

8 Huynh-Thu, Q.; Ghanbari, M. (2008). "Scope of validity of PSNR in image/video quality assessment". Electronics Letters 44 (13): 800

Το PSNR ορίζεται τότε ως εξής:

$$
\begin{aligned}
PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\
&= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\
&= 20 \cdot \log_{10} \left(MAX_I \right) - 10 \cdot \log_{10} \left(MSE \right)
\end{aligned}
$$

Εδώ, το MAX_I είναι η μέγιστη δυνατή τιμή εικονοστοιχείου της εικόνας. Όταν τα εικονοστοιχεία αντιπροσωπεύονται χρησιμοποιώντας 8 bits ανά δείγμα, αυτό είναι 255. Γενικότερα, όταν τα δείγματα αντιπροσωπεύονται χρησιμοποιώντας γραμμική PCM με bits B ανά δείγμα, το MAX_I είναι $2^B - 1$. Για έγχρωμες εικόνες με τρεις RGB τιμές ανά pixel, ο ορισμός του PSNR είναι ο ίδιος, εκτός από ότι το MSE είναι το άθροισμα όλων των διαφορών στο τετράγωνο διαιρεμένο με το μέγεθος της εικόνας και με το 3. Εναλλακτικά, για έγχρωμες εικόνες η εικόνα μετατρέπεται σε ένα διαφορετικό χρωματικό χώρο και το PSNR προκύπτει για κάθε κανάλι του εν λόγω χώρου χρώματος, π.χ., YCbCr ή HSL.

Τυπικές τιμές για το PSNR σε lossy συμπίεση εικόνας και βίντεο είναι μεταξύ 30 και 50 dB, εφόσον το βάθος bit είναι 8 Bit, όπου η υψηλότερη τιμή είναι η καλύτερη. Για δεδομένα 16 Bit τυπικές τιμές για το PSNR είναι μεταξύ 60 και 80 dB. Οι αποδεκτές τιμές για την απώλεια ποιότητας της ασύρματης μετάδοσης θεωρείται ότι είναι περίπου 20 dB έως 25 dB.

1.5.2 SSIM[9]

Ο δείκτης δομικής ομοιότητας (SSIM) είναι μια μέθοδος για τη μέτρηση της ομοιότητας μεταξύ δύο εικόνων. Ο δείκτης SSIM είναι μια πλήρης μέτρηση αναφοράς. Με άλλα λόγια, είναι η μέτρηση της ποιότητας της εικόνας που βασίζεται σε μια αρχική ασυμπίεστη ή χωρίς παραμόρφωση εικόνα, ως αναφορά. Ο SSIM έχει σχεδιαστεί για να βελτιώσει τις παραδοσιακές μεθόδους, όπως ο PSNR και το μέσο τετραγωνικό σφάλμα (MSE), τα οποία έχουν αποδειχθεί ότι είναι ασυμβίβαστα με την ανθρώπινη οπτική αντίληψη.

Η διαφορά σε σχέση με άλλες τεχνικές που αναφέρθηκαν προηγουμένως, όπως MSE ή PSNR είναι ότι αυτές οι προσεγγίσεις εκτιμούν αντιληπτά λάθη. Αφετέρου, ο SSIM θεωρεί την υποβάθμιση της εικόνας ως αντιληπτή αλλαγή στις δομικές πληροφορίες. Δομικές πληροφορίες είναι η ιδέα ότι τα εικονοστοιχεία έχουν ισχυρές αλληλεξαρτήσεις ειδικά όταν είναι κοντά στο χώρο. Αυτές οι εξαρτήσεις μεταφέρουν σημαντικές πληροφορίες σχετικά με τη δομή των αντικειμένων στην οπτική σκηνή.

Ο δείκτης SSIM υπολογίζεται σε διάφορα παράθυρα μιας εικόνας. Το μέτρο μεταξύ δύο παραθύρων x και y μεγέθους N × N είναι:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

Αυτή η φόρμουλα, προκειμένου να αξιολογηθεί η ποιότητα της εικόνας εφαρμόζεται μόνο επί της φωτεινότητας. Ο προκύπτων δείκτης SSIM είναι μια δεκαδική τιμή μεταξύ -1 και 1, και η τιμή 1 είναι προσβάσιμη μόνο στην περίπτωση με δύο όμοια σύνολα δεδομένων. Συνήθως υπολογίζεται σε μεγέθη παραθύρων 8 × 8 . Το παράθυρο μπορεί να μετατοπίζεται pixel -by- pixel στην εικόνα, αλλά οι συγγραφείς προτείνουν να χρησιμοποιείται μόνο μια υποομάδα των πιθανών παραθύρων για να μειωθεί η πολυπλοκότητα του υπολογισμού.

9 Salomon, David (2007). Data Compression: The Complete Reference (4 ed.). Springer. p. 281

Η δομική ανομοιότητα (DSSIM) είναι ένας δείκτης που προέρχεται από τον SSIM (αν και η τριγωνική ανισότητα δεν ικανοποιείται απαραίτητα).

$$\mathrm{DSSIM}(x,y) = \frac{1 - \mathrm{SSIM}(x,y)}{2}$$

1.5.3 Δείκτης ποιότητας εικόνας[10]

Ο δείκτης ποιότητας εικόνας μαθηματικά ορίζεται από τη μοντελοποίηση της παραμόρφωσης της εικόνας σε σχέση με την εικόνα αναφοράς ως συνδυασμός τριών παραγόντων: την απώλεια της συσχέτισης, την παραμόρφωση φωτεινότητας, την αντίθεση και την παραμόρφωση.

Εάν οι δύο εικόνες f και g θεωρούνται ως μήτρες με M στήλες και N σειρές που περιέχουν τιμές εικονοστοιχείων f [i, j], g [i, j], αντίστοιχα (0 ≥ i> M, 0 ≥ j> N), ο καθολικός δείκτης ποιότητας εικόνας Q μπορεί να υπολογιστεί ως προϊόν από τρεις συνιστώσες:

$$Q = \frac{\sigma_{fg}}{\sigma_f \sigma_g} \cdot \frac{2\bar{f}\bar{g}}{(\bar{f})^2 + (\bar{g})^2} \cdot \frac{2\sigma_f \sigma_g}{\sigma_f^2 + \sigma_g^2}$$

$$\bar{f} = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f[i,j] \qquad \bar{g} = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} g[i,j]$$

$$\sigma_{fg} = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f[i,j] - \bar{f})(g[i,j] - \bar{g})$$

$$\sigma_f^2 = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f[i,j] - \bar{f})^2 \qquad \sigma_g^2 = \frac{1}{M+N-1} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (g[i,j] - \bar{g})^2$$

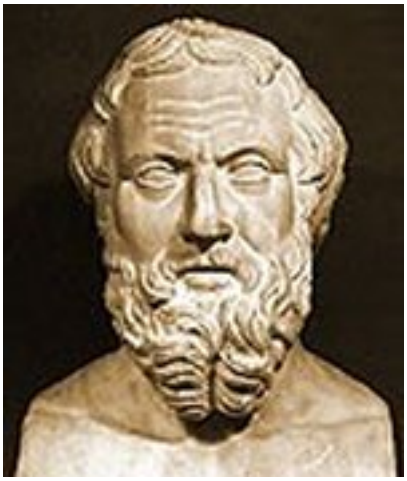
10 http://software.intel.com/sites/products/documentation/hpc/ipp/ippi/ippi_ch11/ch11_image_quality_index.html

Το πρώτο συστατικό είναι ο συντελεστής συσχέτισης, ο οποίος μετρά το βαθμό γραμμικής συσχέτισης μεταξύ των εικόνων f και g. Ποικίλλει στην περιοχή [-1, 1]. Η καλύτερη τιμή 1 λαμβάνεται όταν οι f και g έχουν γραμμική σχέση, πράγμα που σημαίνει ότι η g[i, j] = af [i, j] + b για όλες τις πιθανές τιμές των i και j. Το δεύτερο μέρος, με εύρος τιμών [0, 1], μετρά πόσο κοντά η μέση φωτεινότητα είναι μεταξύ των εικόνων. Καθώς οι σf και σg μπορεί να θεωρηθούν ως εκτιμήσεις της αντίθεσης των f και g, το τρίτο συστατικό μέτρα πόσο όμοιες είναι οι αντιθέσεις των εικόνων. Το εύρος τιμών για αυτό το στοιχείο είναι επίσης το [0, 1]. Το εύρος των τιμών για το δείκτη Q είναι [-1, 1]. Η καλύτερη τιμή 1 επιτυγχάνεται εάν και μόνο εάν οι εικόνες είναι πανομοιότυπες.

Κεφάλαιο 2. Στεγανογραφία

2.1 Ιστορική αναδρομή στεγανογραφίας

Η άνοδος του διαδικτύου μπορεί να θεωρηθεί ως μία από τις σημαντικότερες εξελίξεις των τελευταίων χρόνων. Ο καθένας που έχει έναν υπολογιστή μπορεί να αποκτήσει εύκολη πρόσβαση σε όλες τις πληροφορίες που θέλει να βρει στο διαδίκτυο. Οι τελευταίες ειδήσεις, ψηφιακές βιβλιοθήκες, πληροφορίες σχετικά με τα πανεπιστήμια, επιχειρήσεις, πολιτιστικές εκδηλώσεις και ούτω καθεξής, είναι διαθέσιμες στο ευρύ κοινό. Φυσικά, υπάρχουν επίσης μειονεκτήματα σε αυτή την εξέλιξη. Ψηφιακή αναπαράσταση των πληροφοριών καθιστά δυνατή την παραγωγή παράνομων απεριόριστων τέλειων αντιγράφων. Ειδικά για τα αρχεία ήχου και βίντεο, η βιομηχανία ενδιαφέρεται έντονα για πληροφορίες πνευματικών δικαιωμάτων ή σειριακούς αριθμούς στα δεδομένα προκειμένου να εφαρμόσουν τους νόμους περί πνευματικών δικαιωμάτων. Το ενδιαφέρον για απόκρυψη τεχνικών πληροφοριών έχει αυξηθεί τα τελευταία χρόνια, αλλά θα πρέπει να έχει κανείς κατά νου ότι η στεγανογραφία δεν αποτελεί νέα πρακτική. Στην πραγματικότητα, έχει χρησιμοποιηθεί σε μεγάλο βαθμό καθ'όλη τη διάρκειατης ιστορίας.



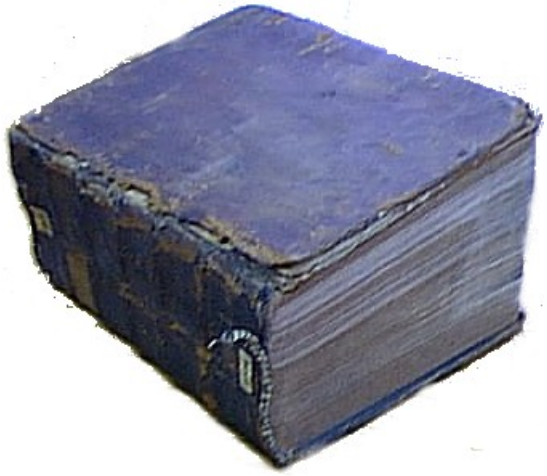
Εικόνα 1: Ηρόδοτος (Πηγή cs.virginia.edu)

Η πρώτη χρήση της στεγανογραφίας αναφέρεται από τον Ηρόδοτο, τον πατέρα της ιστορίας, ο οποίος αναφέρει ότι στην αρχαία ελληνική, κρυφό κείμενο γράφτηκε σε δισκία κεριού. Όταν ο Δημάρετος ήθελε να ενημερώσει τη Σπάρτη ότι ο βασιλιάς της Περσίας, Ξέρξης, σκόπευε να εισβάλει στην Ελλάδα, έγραψε αυτό το μήνυμα σε ένα δισκίο και το καλυψε με κερί. Για να ανακτήσουν το μήνυμα στη Σπάρτη έξυσαν το κερί από το δισκίο. Ο Αινείας ο Στρατηγός αναφέρει σε πολλά έγγραφα του και άλλα στεγανογραφικά συστήματα. Μυστικά γράμματα μπορεί να κρύβονται σε σόλες παπουτσιών στους αγγελιοφόρους ή γυναικεία σκουλαρίκια, μυστικό κείμενο θα μπορούσε να γραφτεί σε τραπέζια από ξύλο που στη συνέχεια ασβεστώνονται. Αινείας πρότεινε επίσης μερικά συστήματα που είναι πολύ παρόμοια με εκείνα, τα είναι σχετικά με την απόκρυψη πληροφοριών σε έγγραφα κειμένου. Μία από αυτές τις προτεινόμενες τεχνικές περιλαμβάνουν απόκρυψη κειμένου με πολύ μικρές οπές κάτω ή πάνω από τα γράμματα ή αλλάζοντας τα ύψη της γραμματοσειράς σε ένα κείμενο (χαρακτηριστικό κωδικοποίησης). Μια άλλη έξυπνη μέθοδος ήταν να ξυρίσει το κεφάλι του αγγελιοφόρου και να ζωγραφίσει τις μυστικές επιστολές στο κεφάλι του αγγελιοφόρου.

Ένα πολύ κοινό στεγανογραφικό καθεστώς στην ιστορία ήταν η χρήση των χημικών ουσιών για να αποκρύψουν πληροφορίες. Αόρατη μελάνη, η οποία δημιουργούταν αρχικά από οργανικές ουσίες (όπως τα ουρία ή γάλα), εξακολουθεί να χρησιμοποιείται από πολλά παιδιά (π.χ. μελάνι με βάση το λεμόνι). Το μυστικό μήνυμα μπορεί να γραφτεί μεταξύ των γραμμών με το αόρατο μελάνι. Εάν το έγγραφο θερμαίνεται ήπια, οι επιστολές με το ειδικό μελάνι θα γίνουν ορατές.

Στην αρχαία Κίνα, οι άνθρωποι χρησιμοποιούσαν χάρτινες μάσκες για να συμφωνήσουν σχετικά με τις τοποθεσίες των μυστικών γραμμάτων. Τόσο ο αποστολέας όσο και ο παραλήπτης είχαν την ίδια μάσκα με έναν αριθμό οπών κομμένες σε τυχαίες θέσεις. Για να αποκρύψει ένα μήνυμα, ο αποστολέας τοποθετεί αυτή τη μάσκα πάνω σε ένα φύλλο χαρτί, γράφει το μυστικό μήνυμα στις οπές και γεμίζει τις άλλες θέσεις συνθέτοντας ένα κείμενο-κάλυμμα. Ο δέκτης μπορεί να διαβάσει το μυστικό μήνυμα τοποθετώντας τη μάσκα του πάνω στο πλήρες μήνυμα. Φυσικά, η τεχνική αυτή προϋποθέτει ότι το κείμενο κάλυμμα

δεν προκαλεί την υποψία ενός τρίτου. Φαίνεται περίεργο ότι ο Cardan, ένας Ιταλός μαθηματικός, βρήκε εκ νέου τη μέθοδο αυτή κατά τον 16ο αιώνα, και ότι μια βρετανική τράπεζα συνέστησε στους πελάτες της το 1992 την ίδια ακριβώς μέθοδο για να κρύψουν τον προσωπικό αριθμό πληροφοριών (για την ταμειακή μηχανή).



Εικόνα 2: Schola Steganographica (Πηγή cs.virginia.edu)

Ο κατάλογος των συστημάτων στεγανογραφίας που χρησιμοποιείται σε όλη την ιστορία είναι μεγάλος. Ο Gaspar Schott εξηγεί στο διάσημο βιβλίο του «Schola Steganographica" πώς μυστικά μηνύματα μπορεί να κρύβονται σε παρτιτούρες. Πιθανές προσεγγίσεις ήταν ότι κάθε κόμβος αντιστοιχεί σε ένα γράμμα ή ότι ο αριθμός των εμφανίσεων κάθε νότας κωδικοποιούσε τη μυστική πληροφορία (που χρησιμοποιείται από τον Johann Sebastian Bach). Ο John Wilkins (1614-1672) πρότεινε με την ιδέα ότι οι μουσικοί θα μπορούσαν να δημιουργήσουν ένα είδος συγκεκαλυμμένου κανάλιου συνομιλίας μεταξύ τους. Επιπλέον, πρότεινε ότι θα ήταν δυνατή η απόκρυψη πληροφοριών σε γεωμετρικά σχέδια με τροποποίηση γεωμετρικών ιδιοτήτων όπως γωνίες ή μήκη γραμμής. Η ιδέα της απόκρυψης μυστικών πληροφοριών σε εικόνες γεννήθηκε μέσω του "Vexierbild», που δημιουργήθηκε από έναν μαθητή του Άλμπρεχτ Ντύρερ (1471-1528), αποτέλεσε το επόμενο βήμα στη μακρόχρονη ιστορία της στεγανογραφίας. Όταν κοιτά κανείς το "Vexierbild" κανονικά, βλέπει ένα παράξενο τοπίο, αλλά κοιτώντας από άλλη πλευρά αποκαλύπτει πορτρέτα διάσημων βασιλιάδων. Τέτοιες αναμορφικές

εικόνες παρέχονται μέσα από καμουφλάζ επικίνδυνων πολιτικών δηλώσεων κατά τη διάρκεια του 16ου και 17ου αιώνα.

Εικόνα 3: Παράδειγμα "Vexierbild" (Πηγή wikipedia.org)

Με τις συνεχείς τεχνικές βελτιώσεις επήλθε περαιτέρω πρόοδος στην απόκρυψη πληροφοριών σε εικόνες. Κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου, οι Γερμανοί ανέπτυξαν τη τεχνολογία microdot. Τα Microdots είναι πολύ μικρές φωτογραφίες, η οποία μπορεί να περιέχει ολόκληρο το περιεχόμενο μιας δακτυλογραφημένης σελίδας. Μια άλλη αρχή της στεγανογραφίας που χρησιμοποιείται ακόμα και σήμερα, είχε ήδη εφευρεθεί από τον 17ο αιώνα. Οι εκδότες των πινάκων λογαρίθμων συνήθιζαν να εισάγουν λάθη εσκεμμένα στα λιγότερο σημαντικά ψηφία.

Τα πολυάριθμα παραδείγματα για την απόκρυψη πληροφοριών στην ιστορία δείχνουν ότι η στεγανογραφία δεν είναι σε καμία περίπτωση ένα νέο πεδίο. Κερδίζει περισσότερη σημασία αυτή τη στιγμή με την τεράστια ποσότητα των πληροφοριών που είναι διαθέσιμες σε όλους σήμερα.

2.2 *Ορισμός στεγανογραφίας και μέθοδοι*

Στεγανογραφία είναι η τέχνη ή η πρακτική της απόκρυψης ενός μηνύματος, εικόνας, ή ενός αρχείου μέσα σε ένα άλλο μήνυμα, εικόνα ή αρχείο. Η πρώτη καταγεγραμμένη χρήση του όρου ήταν το 1499 από τον Johannes Trithemius στο έργο του Steganographia, μια πραγματεία για την κρυπτογραφία και στεγανογραφία, που μεταμφιέζεται ως ένα βιβλίο για μαγεία. Σε γενικές γραμμές, τα κρυμμένα μηνύματα θα εμφανίζονται να είναι (ή να είναι μέρος σε) κάτι άλλο: φωτογραφίες, άρθρα, λίστες αγορών, ή κάποιο άλλο κείμενο. Για παράδειγμα, το κρυφό μήνυμα μπορεί να είναι σε αόρατη μελάνη ανάμεσα στις ορατές γραμμές μίας ιδιωτικής επιστολής. Μερικές εφαρμογές της στεγανογραφία που στερούνται ένα κοινόχρηστο μυστικό είναι μορφές της ασφάλειας μέσω της αδιαφάνειας, ενώ βασικά εξαρτώνται από συστήματα στεγανογραφίας που τηρούν την αρχή Kerckhoffs.

Το πλεονέκτημα της στεγανογραφίας έναντι της κρυπτογραφίας είναι ότι το ότι το μυστικό μήνυμα που δεν προσελκύει την προσοχή ως αντικείμενο εξέτασης. Έτσι, λαμβάνοντας υπόψη ότι η κρυπτογραφία είναι η πρακτική της προστασίας των περιεχομένων ενός μηνύματος, η στεγανογραφία ασχολείται με την απόκρυψη του γεγονός ότι αποστέλλεται ένα μυστικό μήνυμα, καθώς και την απόκρυψη των περιεχομένων του μηνύματος.

Η στεγανογραφία περιλαμβάνει την απόκρυψη των πληροφοριών μέσα στα αρχεία του υπολογιστή. Στην ψηφιακή στεγανογραφία, οι ηλεκτρονικές επικοινωνίες μπορεί να περιλαμβάνουν steganographic κωδικοποίηση μέσα από ένα στρώμα μεταφοράς, όπως ένα αρχείο εγγράφου, αρχείο εικόνας, πρόγραμμα ή πρωτόκολλο. Τα αρχεία πολυμέσων είναι ιδανικά για steganographic μετάδοση λόγω του μεγάλου μεγέθους τους. Για παράδειγμα, ο αποστολέας μπορεί να ξεκινήσει με ένα αθώο αρχείο εικόνας και να ρυθμίσει το χρώμα του κάθε pixel ή να αντιστοιχεί σε ένα γράμμα της αλφαβήτου, μια αλλαγή τόσο λεπτή που κάποιος όχι που δεν ψάχνει ειδικά για αυτό είναι μάλλον απίθανο να το προσέξει.

Η σύγχρονη στεγανογραφία εισήλθε το 1985 με την έλευση των προσωπικών υπολογιστών που εφαρμόζονται σε κλασικά προβλήματα στεγανογραφίας. Η ανάπτυξη ήταν πολύ αργή, αλλά έκτοτε έχει απογειωθεί, που συνεπάγεται από το μεγάλο αριθμό των διαθέσιμων λογισμικών στεγανογραφίας:

- Απόκρυψη μηνυμάτων στα χαμηλότερα bits σε εικόνες ή αρχεία ήχου που περιέχουν θόρυβο.
- Απόκρυψη δεδομένων εντός κρυπτογραφημένων δεδομένων ή εντός τυχαίων δεδομένων. Τα στοιχεία που πρέπει να αποκρύπτονται πρώτα κρυπτογραφούνται προτού χρησιμοποιηθούν για να αντικαταστήσουν μέρος ενός πολύ μεγαλύτερου μπλοκ κρυπτογραφημένων δεδομένων ή ένα μπλοκ τυχαίων δεδομένων (ένας απαράβατος cipher, όπως το one-time pad δημιουργεί ciphertexts που φαίνονται απολύτως τυχαία, αν κάποιος δεν έχει το ιδιωτικό κλειδί).
- Chaffing και winnowing.
- Μιμικές λειτουργίες μετατρέπουν ένα αρχείο για να έχουν το στατιστικό προφίλ του άλλου. Αυτό μπορεί να ματαιώσει τις στατιστικές μεθόδους που βοηθούν άμεσες επιθέσεις να προσδιορίσουν τη σωστή λύση σε μία επίθεση ciphertext.
- Κρυφά μηνύματα σε παραποιημένα εκτελέσιμα αρχεία, αξιοποιώντας την αβεβαιότητα στο σύνολο στοχοθετημένων εντολών.
- Εικόνες ενσωματωμένες στο υλικό του βίντεο (προαιρετικά αναπαραγωγή με μεγαλύτερη ή μικρότερη ταχύτητα).
- Ενσωμάτωση ανεπαίσθητων καθυστερήσεων σε πακέτα που αποστέλλονται μέσω του δικτύου από το πληκτρολόγιο. Καθυστερήσεις στο πάτημα πλήκτρων σε ορισμένες εφαρμογές (telnet ή λογισμικό απομακρυσμένης επιφάνειας εργασίας), μπορεί να σημαίνει μια καθυστέρηση στα πακέτα, και οι καθυστερήσεις των πακέτων μπορούν να χρησιμοποιηθούν για την κωδικοποίηση των δεδομένων.
- Αλλαγή της σειράς των στοιχείων σε ένα σύνολο.
- Η Content-Aware στεγανογραφία κρύβει πληροφορίες στα σημασιολογία που ένας ανθρώπινος χρήστης αποδίδει σε ένα datagram. Τα συστήματα αυτά προσφέρουν ασφάλεια ενάντια σε μη-ανθρώπινους αντιπάλους.

- Στη Blog-Στεγανογραφία τα μηνύματα είναι αποσπασματικά και τα (κρυπτογραφημένα) κομμάτια προστίθενται ως σχόλια σε web-logs (ή πίνακες pin στις πλατφόρμες κοινωνικής δικτύωσης). Σε αυτή την περίπτωση, η επιλογή των blogs είναι το συμμετρικό κλειδί που χρησιμοποιούν ο αποστολέας και ο παραλήπτης. Ο φορέας του κρυφού μηνύματος είναι όλη η μπλογκόσφαιρα.
- Τροποποιώντας την ηχώ ενός αρχείου ήχου (Echo Στεγανογραφία).
- Ασφαλής Στεγανογραφία ακουστικών σημάτων.
- Στεγανογραφία εικόνων κατάτμησης πολυπλοκότητας bit-plane
- Συμπεριλαμβανομένων των δεδομένων τμήματα ενός αρχείου που έχουν αγνοηθεί , όπως μετά το λογικό πέρας του αρχείου φορέα.
- Μετατροπή του κειμένου στο ίδιο χρώμα με το φόντο σε έγγραφα επεξεργαστή κειμένου, e-mails και μηνύματα φόρουμ.
- Χρήση Unicode χαρακτήρων που μοιάζουν με το πρότυπο σύνολο χαρακτήρων ASCII. Στα περισσότερα συστήματα, δεν υπάρχει καμία οπτική διαφορά από το απλό κείμενο. Σε κάποια συστήματα μπορούν να εμφανιστούν οι γραμματοσειρές με διαφορετικό τρόπο, και η επιπλέον πληροφορία θα ήταν εύκολο να εντοπιστεί.
- Χρησιμοποιώντας κρυφούς χαρακτήρες (ελέγχου), και περιττή χρήση της σήμανσης (π.χ., έντονη γραφή, υπογράμμιση ή πλάγια) για να ενσωματώσει στοιχεία εντός της HTML, το οποίο είναι ορατό από την εξέταση της πηγής του εγγράφου. Σελίδες HTML μπορεί να περιέχουν κώδικα για επιπλέον κενά διαστήματα και καρτέλες στο τέλος των γραμμών, και τα χρώματα, τις γραμματοσειρές και τα μεγέθη, τα οποία δεν είναι ορατά όταν εμφανίζονται.
- Η χρήση μη-εκτυπώσιμων χαρακτήρων Unicode Zero-Widthς Joiner (ZWJ) και Zero-Width Non-Joiner (ZWNJ). Οι χαρακτήρες χρησιμοποιούνται για την ένωση και απομάκρυνση γραμμάτων στα αραβικά, αλλά μπορούν να χρησιμοποιηθούν σε ρωμαϊκά αλφάβητα για την απόκρυψη πληροφοριών, διότι δεν έχουν κανένα νόημα στη ρωμαϊκή αλφάβητο: επειδή έχουν "μηδενικό-πλάτος" δεν εμφανίζονται. Οι ZWJ και ZWNJ μπορούν να αντιπροσωπεύουν τα δυαδικά "1" και "0".

2.3 Δίκτυα

Όλες οι τεχνικές απόκρυψης πληροφοριών μπορούν να χρησιμοποιηθούν για την ανταλλαγή steganograms σε τηλεπικοινωνιακά δίκτυα και μπορούν να ταξινομηθούν κάτω από τον γενικό όρο στεγανογραφία δικτύου. Αυτή η ονοματολογία εισήχθη αρχικά από τον Krzysztof Szczypiorski το 2003. Σε αντίθεση με τις τυπικές στεγανογραφικές μεθόδους που χρησιμοποιούν ψηφιακά μέσα (εικόνες, αρχεία ήχου και βίντεο) ως κάλυμμα για τα κρυφά δεδομένα, η στεγανογραφία δικτύο χρησιμοποιεί τα στοιχεία ελέγχου των πρωτοκόλλων επικοινωνίας και τη βασική τους εγγενή λειτουργικότητα. Ως αποτέλεσμα, τέτοιες μέθοδοι είναι πιο δύσκολο να ανιχνευθούν και να εξαλειφθούν.

Η στεγανογραφία σε ένα τυπικό δίκτυο περιλαμβάνει την τροποποίηση των ιδιοτήτων ενός ενιαίου πρωτοκόλλου δικτύου. Τέτοια τροποποίηση μπορεί να εφαρμοστεί στο PDU (Μονάδα Δεδομένων Πρωτοκόλλου), ή στις χρονικές σχέσεις μεταξύ των ανταλλασσόμενων PDUs, ή και στα δύο (υβριδικές μέθοδοι).

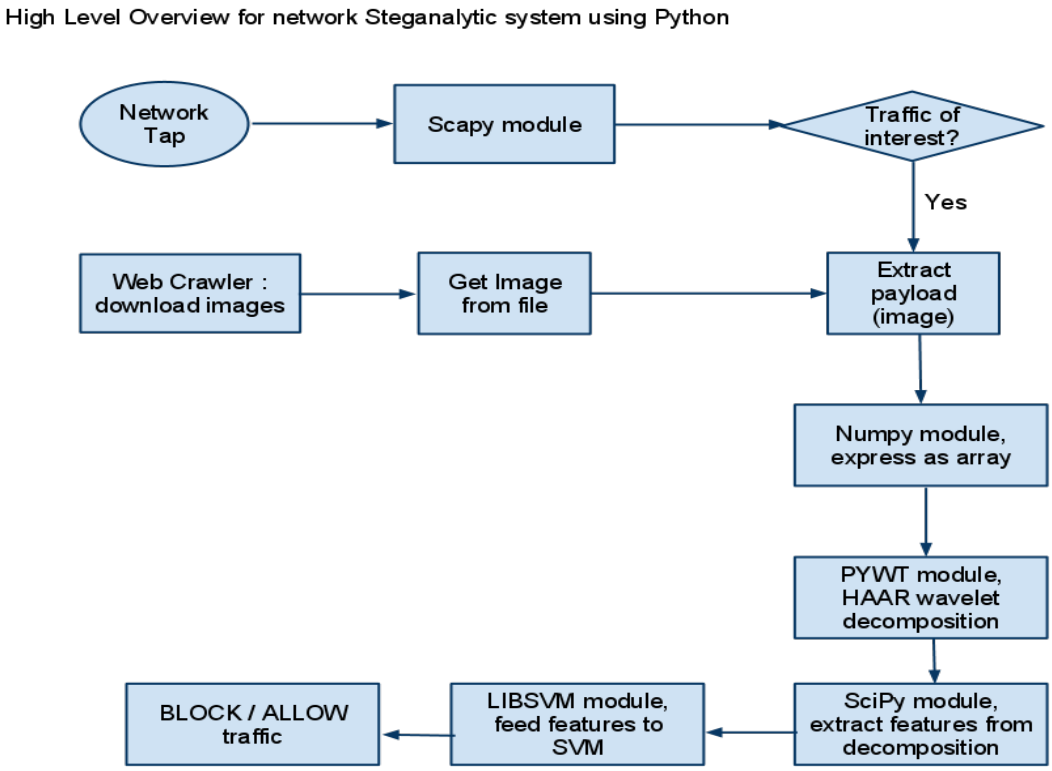
Επιπλέον, είναι εφικτό να αξιοποιήσει τη σχέση ανάμεσα σε δύο ή περισσότερα διαφορετικά πρωτόκολλα δικτύου για να ενεργοποιήσει τη μυστική επικοινωνία. Οι εφαρμογές αυτές εμπίπτουν στην έννοια της στεγανογραφίας μεταξύ πρωτοκόλλων.

Η στεγανογραφία δικτύων καλύπτει ένα ευρύ φάσμα από τεχνικές, οι οποίες περιλαμβάνουν, μεταξύ άλλων:

- Απόκρυψη των μηνυμάτων σε συνομιλίες Voice-over-IP, π.χ. με τη χρήση των καθυστερημένων ή κατεστραμμένων πακέτων που θα έπρεπε κανονικά να αγνοηθεί από τον δέκτη (αυτή η μέθοδος ονομάζεται Στεγανογραφία LACK - Lost Audio Packets), ή, εναλλακτικά, απόκρυψη πληροφοριών σε αχρησιμοποίητα πεδία header.
- WLAN Στεγανογραφία - μετάδοση steganograms σε Ασύρματα Τοπικά Δίκτυα. Ένα πρακτικό παράδειγμα της Στεγανογραφίας WLAN είναι το σύστημα HICCUPS (Hidden Communication System for Corrupted Networks).

2.4 ΣΤΕΓΑΝΑΛΥΣΗ

Στην επιστήμη των υπολογιστών, η ανίχνευση στεγανογραφημένων πακέτων δεδομένων ονομάζεται στεγανάλυση. Η απόκρυψη πληροφοριών εντός ηλεκτρονικών μέσων απαιτεί μεταβολές των ιδιοτήτων των μέσων που μπορούν να εισάγουν κάποια μορφή υποβάθμισης ή ασυνήθιστα χαρακτηριστικά. Αυτά τα χαρακτηριστικά μπορούν να ενεργούν ως υπογραφές που μεταδίδουν την ύπαρξη του ενσωματωμένου μηνύματος, ανατρέποντας έτσι το σκοπό της στεγανογραφίας.



Εικόνα 4: Στεγανάλυση με τη γλώσσα Python (Πηγή: www.snipview.com)

Επιθέσεις και ανάλυση σχετικά με τις κρυφές πληροφορίες μπορεί να λάβουν διάφορες μορφές: την ανίχνευση, την εξόρυξη, και την απενεργοποίηση ή την καταστροφή των κρυμμένων πληροφοριών. Ένας εισβολέας μπορεί, επίσης, να ενσωματώσει αντιπληροφόρηση πάνω από την υπάρχουσα κρυμμένη πληροφορία. Θα εξετασθούν δύο μέθοδοι σταγανάλυσης: η ανίχνευση μηνύματος και η μετάδοση και απενεργοποίηση της ενσωματωμένης πληροφορίας.

Αυτές οι προσεγγίσεις (επιθέσεις) ποικίλλουν ανάλογα με τις μεθόδους που χρησιμοποιούνται για την ενσωμάτωση της πληροφορίας στο μέσο κάλυψης. Στόχος δεν είναι να επιλεγεί η απομάκρυνση ή η απενεργοποίηση των έγκυρων πληροφοριών, όπως τα πνευματικά δικαιώματα, αλλά να εντοπιστεί το σημείο που με το σημείο που είναι ευάλωτο στην εισαγωγή παράνομων πληροφοριών.

Η απλούστερη μέθοδος για την ανίχνευση τροποποιημένων αρχείων, είναι να τα συγκρίνουμε με γνωστά πρωτότυπα. Για παράδειγμα, για να εντοπίσει τις πληροφορίες που διακινούνται μέσω των γραφικών σε μια ιστοσελίδα, ένας αναλυτής μπορεί να διατηρήσει τα γνωστά αντίγραφα αυτών των υλικών και στη συνέχεια να γίνει σύγκρισή τους με τα τρέχοντα περιεχόμενα του site. Οι διαφορές, υποθέτοντας ότι ο φορέας είναι ο ίδιος, θα συνθέτουν το ωφέλιμο φορτίο.

Σε γενικές γραμμές, χρησιμοποιώντας εξαιρετικά υψηλό ποσοστό συμπίεσης καθιστά τη στεγανογραφία δύσκολη, αλλά όχι αδύνατη. Ενώ τα σφάλματα συμπίεσης παρέχουν μια κρυψώνα για τα δεδομένα, η υψηλή συμπίεση μειώνει την ποσότητα των διαθέσιμων δεδομένων για απόκρυψη του ωφέλιμου φορτίου, αυξάνοντας την πυκνότητα κωδικοποίησης και διευκολύνοντας έτσι την ανίχνευση (σε ακραίες περιπτώσεις, ακόμα και από την περιστασιακή παρατήρηση).

2.5 Στεγανογραφία στην σημερινή εποχή

Σε γενικές γραμμές, χρησιμοποιείται ορολογία ανάλογη με (και συνεπείς με) πιο κλασικές τεχνολογίες ραδιοφωνικών και τηλεπικοινωνιακών σημάτων. Ωστόσο, κρίθηκε αναγκαία μια σύντομη περιγραφή κάποιων όρων που εμφανίζονται ειδικά στο λογισμικό και εύκολα συγχέεται. Αυτή είναι πιο σχετική με τα ψηφιακά steganographic συστήματα.

Το *payload* είναι το ωφέλιμο φορτίο δηλαδή τα στοιχεία που πρέπει να κοινοποιούνται κρυφά. Ο φορέας (*carrier)* είναι το σήμα, ρεύμα, ή αρχείο δεδομένων στο οποίο το ωφέλιμο φορτίο είναι κρυμμένο και το οποίο διαφέρει από το "κανάλι (*channel*)" (συνήθως χρησιμοποιείται για να δηλώσει τον τύπο της εισόδου, όπως εικόνα JPEG). Το σήμα, ρεύμα, ή το αρχείο δεδομένων που προκύπτει, έχει το ωφέλιμο φορτίο που κωδικοποιείται σε αυτό και μερικές φορές αναφέρεται ως το πακέτο, το αρχείο stego, ή συγκεκαλυμμένο μήνυμα. Το ποσοστό των bytes, τα δείγματα, ή άλλα στοιχεία σήματος που είναι τροποποιημένα για να κωδικοποιήσουν το ωφέλιμο φορτίο αναφέρονται ως πυκνότητα κωδικοποίησης (*encoding density*) και τυπικά εκφράζεται ως αριθμός μεταξύ 0 και 1.

Σε ένα σύνολο αρχείων, αυτά τα αρχεία που θεωρείται πιθανό να περιέχουν ένα ωφέλιμο φορτίο ονομάζονται ύποπτοι. Αν ο ύποπτος είχε εντοπιστεί μέσω κάποιου τύπου στατιστικής ανάλυσης, θα μπορούσε να αναφέρεται ως υποψήφιος.

Όσο μεγαλύτερο είναι το cover message (ως προς το περιεχόμενο των δεδομένων όσον αφορά τον αριθμό των bits) σε σχέση με το κρυμμένο μήνυμα, τόσο πιο εύκολο είναι να αποκρυφθεί το τελευταίο.

Για το λόγο αυτό, οι ψηφιακές εικόνες (που περιέχουν μεγάλες ποσότητες δεδομένων) χρησιμοποιούνται για να κρύψουν τα μηνύματα στο διαδίκτυο και σε άλλα μέσα επικοινωνίας. Δεν είναι σαφές το πώς συνήθως αυτό γίνεται πραγματικά. Για παράδειγμα: ένα bitmap 24-bit θα έχει 8 bit που αντιπροσωπεύουν κάθε μία από τις τρεις τιμές χρώματος (κόκκινο, πράσινο και μπλε) σε κάθε pixel.

Αν λάβουμε υπόψη μόνο το μπλε, θα υπάρξουν 28 διαφορετικές τιμές του μπλε. Η διαφορά μεταξύ 11111111 και 11111110 στην τιμή για την ένταση του μπλε είναι πιθανό να είναι μη ανιχνεύσιμη από το ανθρώπινο μάτι. Ως εκ τούτου, το λιγότερο σημαντικό bit μπορεί να χρησιμοποιηθεί (περισσότερο ή λιγότερο μη ανιχνεύσιμο) για κάτι άλλο εκτός από πληροφορίες χρώματος. Αν το κάνουμε με το πράσινο και το κόκκινο, μπορούμε να πάρουμε ένα γράμμα του κειμένου ASCII για κάθε τρία εικονοστοιχεία.

Ο στόχος για την κατασκευή της στεγανογραφημένης κωδικοποίησης είναι να εξασφαλιστεί ότι οι αλλαγές στον μεταφορέα (το αρχικό σήμα) λόγω της έγχυσης του ωφέλιμου φορτίου (το σήμα προς συγκεκαλυμμένη ενσωμάτωση) είναι οπτικά (και ιδανικά, στατιστικά) αμελητέες, δηλαδή, οι αλλαγές δεν μπορούν να διακριθούν από το επίπεδο του θορύβου του μεταφορέα. Οποιοδήποτε μέσο μπορεί να είναι ένας φορέας, αλλά είναι καταλληλότερα τα μέσα με ένα μεγάλο ποσό των περιττών ή συμπιεσμένων πληροφοριών.

2.6 Ο ρόλος της στεγανογραφίας στη τρομοκρατία.

Ενώ η στεγανογραφία μπορεί να προσφέρει πολύτιμες λύσεις στη προστασία της ιδιωτικής ζωής στο Internet, προσφέρει επίσης έναν εύκολο τρόπο για τους εγκληματίες να προγραμματίσουν τα εγκλήματά τους και να κρύβουν τις προθέσεις τους. Η στεγανογραφία παίζει μεγάλο ρόλο στον κόσμο των τρομοκρατών. Το Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (UNODC) κυκλοφόρησε μια έκδοση με τίτλο «Η χρήση του Διαδικτύου για τρομοκρατικούς σκοπούς» τον Σεπτέμβριο του 2012, η οποία περιγράφει τη χρήση της στεγανογραφίας από τρομοκράτες για μυστικές επικοινωνίες.

Η στεγανογραφία είναι μια αρχαία μορφή απόκρυψης, που χρονολογείται από την αρχαία Ελλάδα. Στην εποχή του Διαδικτύου, η στεγανογραφία έχει εξελιχθεί σε ψηφιακή μορφή απόκρυψης πληροφοριών. Η δημοσίευση αναφέρει ότι υπάρχει μια πληθώρα εξελιγμένων τεχνολογιών που καθιστούν δύσκολο να εντοπιστεί ο αρχικός αποστολέας, ο παραλήπτης, και το περιεχόμενο των επικοινωνιών μέσω Διαδικτύου.

Εκτός από λογισμικό κρυπτογράφησης και ανωνυμοποίησης, υπάρχει μια ποικιλία από λογισμικό που διατίθεται ώστε να αποκρύψουν τις πληροφορίες που

μεταδίδονται μέσω του Διαδικτύου για παράνομους σκοπούς, όπως το λογισμικό στεγανογραφίας που μπορεί να χρησιμοποιηθεί για να κρύψει τα μηνύματα σε εικόνες.

Ειδικότερα, το πακέτο “Camouflage” δίνεται ως παράδειγμα λογισμικού που κρύβει πληροφορίες μέσα από τη χρήση της στεγανογραφίας. Το πακέτο “Camouflage” επιτρέπει στο χρήστη να κρύψει τα αρχεία συνδέοντάς τα με το τέλος ενός αρχείου κάλυψης, που ονομάζεται επίσης αρχείο "μεταφορέας". Το αρχείο κάλυμμα διατηρεί τις αρχικές ιδιότητες του αρχείου και τα οπτικά χαρακτηριστικά του? αλλά, το αρχείο χρησιμοποιείται ως φορέας για να αποθηκεύσει ή να μεταδώσει τα κρυφά αρχεία. Αυτό το λογισμικό μπορεί να εφαρμοστεί σε οποιοδήποτε τύπο αρχείου.

Για να υπογραμμίσει την αξία της συνεργασίας τόσο σε εθνικό όσο και σε διεθνές επίπεδο, η δημοσίευση περιλαμβάνει περιγραφή της περίπτωσης που αφορά τις Επαναστατικές Ένοπλες Δυνάμεις της Κολομβίας (FARC).

Ψηφιακά αποδεικτικά στοιχεία που προκύπτουν από τις ισπανικές αρχές κατά τη διάρκεια ερευνών ύποπτων τρομοκρατών αποκάλυψαν την ύπαρξη μίας «διεθνούς επιτροπής» μέσα στη FARC.

Τα στοιχεία αποκαλύπτουν οτι η Επιτροπή λειτουργεί με ένα πρόγραμμα ασφάλειας για τις επικοινωνίες, ιδιαίτερα όσον αφορά τα μηνύματα που μεταδίδονται μέσω του Διαδικτύου. Μία από τις πολλές πτυχές του προγράμματος απαιτεί την χρήση της στεγανογραφίας.

Οι κολομβιανές και ισπανικές αρχές συνεργάστηκαν για να αναλύσουν τα ψηφιακή αποδεικτικά στοιχεία και ήταν σε θέση να αποκρυπτογραφήσουν το περιεχόμενο των μηνυμάτων που αποστέλλονται από τους ηγέτες των FARC στην Κολομβία και την Ισπανία.

Εικόνα 5.1 (Πηγή: http://www.osce.org)

Κεφάλαιο 3. Υδατογραφία

3.1 *Ιστορική αναδρομή υδατογραφίας*

Το υδατογράφημα αρχικά ορίζεται ως μια αναγνωρίσιμη εικόνα ή μοτίβο στο χαρτί που εμφανίζεται ως διάφορες αποχρώσεις όταν φωτίζεται (ή όταν προβάλλεται από το αντανακλώμενο φως, πάνω σε σκούρο φόντο), που προκαλείται από το πάχος ή η παραλλαγές πυκνότητας στο χαρτί. Τα υδατογραφήματα έχουν χρησιμοποιηθεί σε γραμματόσημα, χαρτονομίσματα και άλλα κυβερνητικά έγγραφα για την αποτροπή της παραχάραξης. Υπάρχουν δύο βασικοί τρόποι παραγωγής υδατογραφημάτων σε χαρτί.

Τα υδατογραφήματα ποικίλλουν σε μεγάλο βαθμό στην προβολή τους, ενώ μερικά είναι προφανή σε οπτική επιθεώρηση, άλλα απαιτούν κάποια μελέτη για να ξεχωρίσουν. Διάφορα βοηθήματα έχουν αναπτυχθεί, όπως υγρό υδατογράφημα που βρέχει το χαρτί χωρίς να καταστραφεί. Υδατογραφήματα χρησιμοποιούνται συχνά ως χαρακτηριστικά ασφαλείας των τραπεζογραμματίων, διαβατήρια, γραμματόσημα και άλλα έγγραφα για την αποτροπή της παραχάραξης (χαρτί ασφαλείας).

Το υδατογράφημα είναι πολύ χρήσιμο για την εξέταση του εγγράφου, επειδή μπορεί να χρησιμοποιηθεί για τη χρονολόγηση, τον προσδιορισμό των μεγεθών, τα εμπορικά σήματα και τοποθεσίες, καθώς και τον καθορισμό της ποιότητας ενός φύλλου χαρτιού.

Η κωδικοποίηση αναγνωριστικών κωδικών σε ψηφιοποιημένη μουσική, βίντεο, εικόνα, ή άλλο αρχείο είναι γνωστή ως ψηφιακό υδατογράφημα.

Τα υδατογραφήματα αρχικά ήταν σήματατα αναγνώρισης που παράγονταν κατά τη διάρκεια της διαδικασίας παραγωγής του χαρτιού. Τα πρώτα υδατογραφήματα εμφανίστηκαν στην Ιταλία κατά τη διάρκεια του 13ου αιώνα, αλλά η χρήση τους διαδόθηκε ταχύτατα σε ολόκληρη την Ευρώπη.

Είχαν χρησιμοποιηθεί ως μέσο για την αναγνώριση του χαρτοποιού ή της συντεχνίας που κατασκεύασε το χαρτί. Το υδατογράφημα που παρουσιάζεται στην Εικόνα 4 δημιουργήθηκε από ένα καλώδιο ραμμένο επάνω στο καλούπι του χαρτιού. Υδατογραφήματα συνεχίζουν να χρησιμοποιούνται σήμερα ως σήματα κατασκευαστή και την παρεμπόδιση της πλαστογραφίας.

Εικόνα 6: Υδατογράφημα σε χαρτί 13ου αιώνα (πηγή lib.utexas.edu)

3.2 *Ορισμός υδατογραφίας και οι κατηγορίες (σε κείμενο-βίντεο-ήχο-εικόνα)*

Η ταχεία ανάπτυξη ανταλλαγής ψηφιακών μέσων και μεταφοράς μέσω δικτύων υπολογιστών καθιστά το ζήτημα της προστασία του ψηφιακού περιεχομένου ένα κρίσιμο θέμα για τα πνευματικά δικαιώματα και την πιστοποίηση του ιδιοκτήτη του περιεχομένου.

Αυτή η ειδική ανάγκη, έδωσε κίνητρα στους επιστήμονες να μελετήσουν και να αναπτύξουν αποτελεσματικές μεθόδους που είναι σε θέση να προστατέψουν τις ψηφιακές εικόνες, βίντεο, ήχους από κακόβουλες ενέργειες που τείνουν να νοθεύουν ή κάνουν παράνομη χρήση αυτών, χωρίς τη λήψη άδειας από τον ιδιοκτήτη.

Μια δημοφιλής και αποτελεσματική μέθοδος που χρησιμοποιείται συνήθως για να εξασφαλίσει την αυθεντικότητα της ψηφιακής εικόνας είναι η γνωστή διαδικασία της υδατογράφησης. Η διαδικασία αυτή ασχολείται με την κατάλληλη εισαγωγή πληροφοριών πνευματικών δικαιωμάτων στο περιεχόμενο της εικόνας, προκειμένου να δοθεί μια υπογραφή του ιδιοκτήτη σχετικά με την πνευματική ιδιοκτησία.

Η διαδικασία υδατογράφησης έχει εφαρμοστεί με επιτυχία σε αρκετά ψηφιακά μέσα, όπως φωτογραφίες, βίντεο και ήχο. Ως ασφαλιστική δικλίδα κατά της βλάβης της κρυπτογράφησης ή/και προστασίας από αντιγραφή, η ψηφιακή υδατογράφηση έχει προταθεί ως μια “τελευταία γραμμή άμυνας” από μη εξουσιοδοτημένη διανομή πολύτιμων ψηφιακών μέσων. Ένα σύστημα ψηφιακής υδατογράφησης ενσωματώνει πληροφορίες απευθείας σε ένα έγγραφο. Για παράδειγμα, πληροφορίες σχετικά με τα πνευματικά δικαιώματα, ιδιοκτησία, timestamps κλπ. Η ψηφιακή υδατογράφηση δεν μπορεί από μόνη της να αποτρέψει την αντιγραφή, την τροποποίηση και αναδιανομή των αρχείων.

Ωστόσο, εάν η κρυπτογράφηση και η προστασία από αντιγραφή αποτύχει, η υδατογράφηση επιτρέπει το έγγραφο να αναχθεί στον νόμιμο ιδιοκτήτη του και να αποδειχθεί η μη εξουσιοδοτημένη χρήση του.

Η ψηφιακή υδατογράφηση απαιτεί στοιχεία από πολλούς επιστημονικούς κλάδους, συμπεριλαμβανομένων της επεξεργασίας σήματος, τις τηλεπικοινωνίες, την κρυπτογραφία, η ψυχοφυσική, και το δίκαιο. Επειδή η ψηφιακή υδατογράφηση είναι ένα αρκετά νέο θέμα, εκτός από το ότι τα υδατογραφήματα μπορούν να εισαχθούν με αξιοπιστία και να ανακτηθούν, ζητήματα υψηλότερου επιπέδου, όπως πρωτόκολλα είναι αμφισβητήσιμα.

Σε ό,τι αφορά την υδατογράφηση ψηφιακών εικόνων, υπάρχει ένα ανοιχτό ζήτημα που είναι άρρηκτα συνδεδεμένο με τον εντοπισμό των ιδανικών θέσεων για την εισαγωγή υδατογραφημάτων.

Οι πληροφορίες υδατογραφήματος πρέπει να είναι βέλτιστα ενσωματωμένες, υπό την έννοια ότι η παραμόρφωση που εισάγει το υδατογράφημα θα πρέπει να είναι αμελητέα. Επιπλέον, η συνολική διαδικασία υδατογράφησης εξαρτάται από ένα σύνολο παραμέτρων διαμόρφωσης που πρέπει επίσης να βελτιστοποιηθεί, ώστε να παράγονται υδατογραφημένες εικόνες υψηλής ποιότητας και να εξάγονται υψηλής πιστότητας υδατογραφήματα σε περιβάλλοντα επίθεσης.

Το κείμενο είναι το πιο εκτεταμένα χρησιμοποιούμενο μέσο επικοινωνίας μέσω του Διαδικτύου. Τα κύρια συστατικά των δικτυακών τόπων, βιβλία, εφημερίδες, άρθρα, νομικά έγγραφα είναι το απλό κείμενο. Ως εκ τούτου, το απλό κείμενο απαιτεί μέγιστη προστασία και ασφάλεια από τους παραβάτες πνευματικών δικαιωμάτων. Στο παρελθόν, ένας αριθμός ψηφιακών αλγορίθμων υδατογράφησης έχουν προταθεί για εικόνες, ήχο και βίντεο. Ωστόσο, οι αλγόριθμοι ψηφιακών υδατογραφημάτων για απλό κείμενο είναι ανεπαρκείς και αναποτελεσματικοί.

Η ψηφιακή υδατογράφηση είναι η διαδικασία ένταξης ενός μοναδικού ψηφιακού υδατογραφήματος σε ψηφιακό περιεχόμενο για την προστασία από παράνομη αντιγραφή και παραβίαση πνευματικών δικαιωμάτων. Η διαδικασία της ενσωμάτωσης και της εξόρυξης ενός ψηφιακού υδατογραφήματος και από ένα ψηφιακό αρχείο κειμένου που προσδιορίζει μοναδικά τον αρχικό κάτοχο των πνευματικών δικαιωμάτων αυτού του κειμένου ονομάζεται υδατογράφηση ψηφιακού κειμένου.

Η υδατογράφηση κειμένου συμμορφώνεται με τις ίδιες αρχές με τα αρχεία εικόνας, ήχου ή βίντεο. Το υδατογράφημα θα πρέπει να παραμείνει ανθεκτικό σε τυχαίες επιθέσεις αλλοίωσης, μη ανιχνεύσιμο σε κανέναν, αλλά μόνο τον αρχικό ιδιοκτήτη / συγγραφέα του κειμένου, καθώς και εύκολο και πλήρως αυτόματο να αναπαραχθεί από τον αλγόριθμο εξόρυξης. Η κύρια ανησυχία στην υδατογράφηση κειμένου είναι ότι το απλό κειμένου περιέχει λιγότερο περιττές πληροφορίες σε σύγκριση με τις εικόνες, τον ήχο και το βίντεο που θα μπορούσαν να χρησιμοποιηθούν για την συγκάλυψη της μυστικής επικοινωνίας.

Οι τεχνικές υδατογράφησης κειμένου πρέπει να εμφυτεύσουν μοναδικά και αόρατα υδατογραφήματα σε κείμενο που παραμένουν άθικτα μετά από ποικίλες επιθέσεις αλλοίωσης. Οι ψηφιακές λύσεις υδατογραφίας κειμένου θα πρέπει να διευκολύνουν την αποστολή και λήψη κειμένου μέσω Internet, Intranet, Extranet, και φαξ.

Η υδατογράφηση κειμένου μπορεί να χρησιμοποιηθεί για μεγάλο αριθμό εφαρμογών στον πραγματικό κόσμο. Με την ευρεία χρήση του Διαδικτύου σε όλο τον κόσμο για την ανταλλαγή πληροφοριών, η υδατογράφηση κειμένου έχει αποκτήσει μεγαλύτερη σημασία. Οι αναδυόμενες έννοιες της ψηφιακής βιβλιοθήκης, e-business, e-learning, και e-government, e-books, έχει κάνει την υδατογράφηση κείμενου μια αναγκαιότητα. Νομικά έγγραφα, πιστοποιητικά, ιστοσελίδες, επιχειρηματικά σχέδια, βιβλία, άρθρα, ποίηση, έγγραφα εταιρειών, εμπιστευτικό περιεχόμενο, SMS, e-mail πρέπει να προστατεύονται.

Η υδατογράφηση κειμένου μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς:

- Πιστοποίηση αυθεντικότητας
- Προστασία δικαιωμάτων πνευματικής ιδιοκτησίας
- Πρόληψη δημιουργίας αντιγράφων
- Συγκεκαλυμμένη επικοινωνία,
- Ανίχνευση παραβίασης και δακτυλικών αποτυπωμάτων

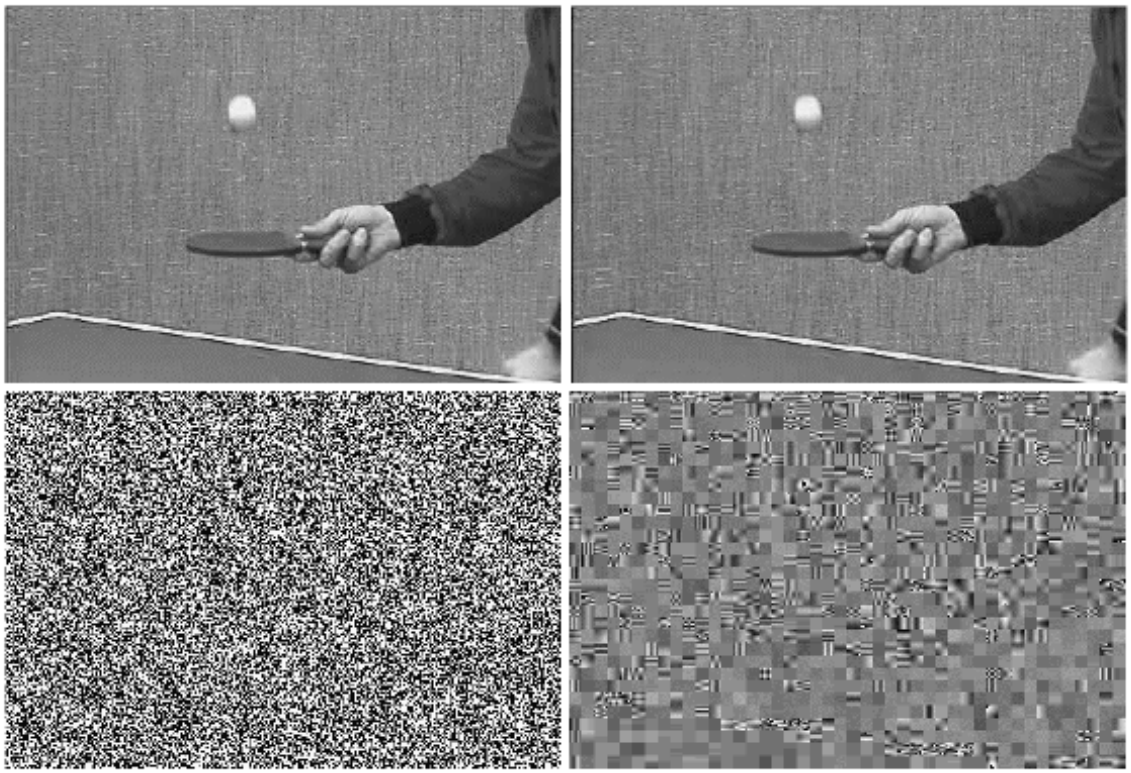
Οι ψηφιακές εικόνες μπορούν να παραχθούν από πολλές πηγές, όπως καθημερινές φωτογραφίες, εικόνες δορυφόρου, ιατρικές σαρώσεις, ή graphics. Τα υδατογραφήματα για φυσικές εικόνες τυπικά τροποποιούν τις εντάσεις των πίξελ ή τους συντελεστές μετασχηματισμού, αν και είναι νοητό ότι ένα υδατογράφημα θα μπορούσε να μεταβάλλει άλλα χαρακτηριστικά όπως τις ακμές.

Μια εικόνα μπορεί να παρατηρηθεί για μια παρατεταμένη χρονική περίοδο, και μπορεί επίσης να υπόκειται σε μεγάλο βαθμό μετατροπών, όπως το φιλτράρισμα, γεωμετρικούς μετασχηματισμούς, συμπίεση, και σύνθεση με άλλες εικόνες, καθώς και εχθρικές επιθέσεις. Έτσι, η ευρωστία και η ασφάλεια είναι συνήθως οι πιο σημαντικές ιδιότητες των υδατογραφημάτων εικόνας. Η ταχύτητα και η πολυπλοκότητα είναι συχνά δευτερογενή χαρακτηριστικά. Επίσης, δεδομένου ότι πολλές εικόνες είναι συμπιεσμένες (π.χ., JPEG ή GIF), οι αλγορίθμοι υδατογράφησης που λειτουργούν με το μετασχηματισμό κυματιδίων μπορεί να είναι χρήσιμοι. Μια πιθανή δυσκολία στην ψηφιακή υδατογράφηση εικόνας είναι το διαθέσιμο πεπερασμένο εύρος ζώνης. Καθώς το μέγεθος της εικόνας μειώνεται, το επιτρεπόμενο μήκος του μηνύματος μειώνεται.

Εικόνα 7: Εισαγωγή υδατογραφήματος σε εικόνα (Πηγή Su et al, 1999)

Ένα υδατογράφημα ήχου είναι ένα μοναδικό ηλεκτρονικό αναγνωριστικό ενσωματωμένο σε ένα ηχητικό σήμα, συνήθως χρησιμοποιείται για να προσδιορίσει την κυριότητα των πνευματικών δικαιωμάτων. Είναι παρόμοιο με ένα υδατογράφημα σε μια εικόνα. Μία από τις πιο ασφαλείς τεχνικές της υδατογράφησης ήχου είναι η υδατογράφηση ήχου ευρέως φάσματος (SSW). Στην SSW, ένα σήμα στενής ζώνης μεταδίδεται σε ένα πολύ μεγαλύτερο εύρος ζώνης, έτσι ώστε η ενέργεια του σήματος που παρουσιάζεται σε κάθε συχνότητα σήματος να είναι μη ανιχνεύσιμη. Έτσι το υδατογράφημα κατανέμεται σε πολλές ζώνες συχνοτήτων έτσι ώστε η ενέργεια σε μία ζώνη είναι μη ανιχνεύσιμη.

Ένα ενδιαφέρον χαρακτηριστικό αυτής της τεχνικής είναι ότι η καταστροφή της υδατογράφησης απαιτεί θόρυβο υψηλής έντασης που πρέπει να προστεθεί σε όλες τις ζώνες συχνοτήτων και έτσι η SSW είναι μια ισχυρή τεχνική υδατογράφησης, διότι, για να την εξαλείψει κανείς, η επίθεση πρέπει να επηρεάζει όλες τις πιθανές ζώνες συχνοτήτων. Αυτό δημιουργεί ορατά ελαττώματα στα δεδομένα.



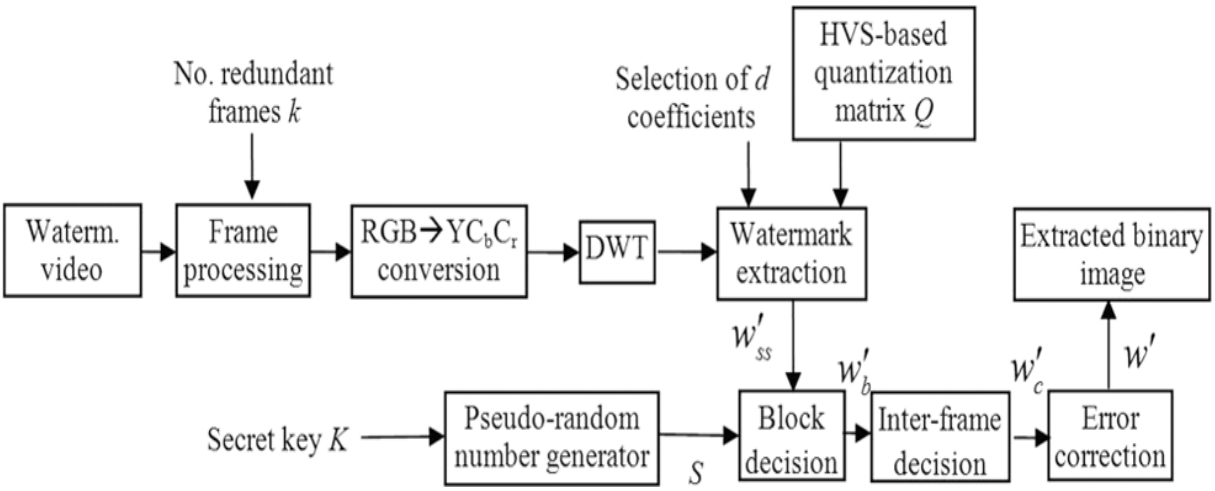
Εικόνα 8: Σύγκριση υδατογράφησης βίντεο σε μη συμπιεσμένη και συμπιεσμένη μορφή (Πηγή Su et al, 1999)

Το ψηφιακό βίντεο είναι μια σειρά από στατικές εικόνες, και πολλές τεχνικές υδατογράφησης μπορούν να επεκταθούν στο βίντεο με απλό τρόπο. Σε αντίθεση με τις μοναδικές εικόνες, μεγάλο εύρος ζώνης των βίντεο σημαίνει ότι μεγάλα μηνύματα μπορούν να ενσωματωθούν στο βίντεο.

Η ταχύτητα είναι επίσης ένα σημαντικό ζήτημα, λόγω των τεράστιων ποσοτήτων δεδομένων που πρέπει να υποβάλλονται σε επεξεργασία. Εκτός από την παραγωγή βίντεο (που λαμβάνει χώρα πριν τηδιανομή), τα ψηφιακά βίντεο τυπικά αποθηκεύονται και διανέμονται σε συμπιεσμένη μορφή (π.χ., MPEG). Ως εκ τούτου, είναι συχνά επιθυμητό ότι το συμπιεσμένο βίντεο δεν πρέπει να απαιτεί μεγαλύτερο εύρος ζώνης από το μη συμπιεσμένου βίντεο. Αυτός ο περιορισμός bit-rate θα μπορούσε επίσης να είναι ένα ζήτημα για τις μοναδικές εικόνες. Υδατογράφηση βίντεο σε συμπιεσμένο επίπεδο είναι ιδιαίτερα ελκυστική. Η λειτουργία στη συμπιεσμένη ροή δυαδικών ψηφίων εξαλείφει την ανάγκη για ένταση υπολογισμού, χρονοβόρα αποσυμπίεση και ανασυμπίεση, έτσι ώστε το υδατογράφημα μπορεί να ενσωματωθεί κατά το χρόνο της διανομής ή της λήψης.

3.3 *Τεχνική αφαίρεσης υδατογραφίας*

Η διαδικασία εξαγωγής / αφαίρεσης / ανιχνεύσεως είναι ένας αλγόριθμος που εφαρμόζεται στο σήμα με στόχο την εξαγωγή της υδατογραφίας από το μέσο. Αν το σήμα είναι μη τροποποιημένο κατά τη μετάδοση, τότε το υδατογράφημα είναι ακόμα παρόν και μπορεί να εξαχθεί. Σε ισχυρές ψηφιακές εφαρμογές υδατογραφίας, ο αλγόριθμος εξόρυξης θα πρέπει να είναι σε θέση να παράγει το υδατογράφημα σωστά, ακόμη και αν οι τροποποιήσεις ήταν ισχυρές. Σε εύθραυστη ψηφιακή υδατογράφηση, ο αλγόριθμος εξόρυξης θα αποτύχει, εάν υπάρξει οποιαδήποτε αλλαγή στο σήμα.



Εικόνα 9: Εξαγωγή υδατογραφήματος από βίντεο (Πηγή engineering.purdue.edu)

Η ανάπτυξη της τεχνολογίας των πληροφοριών και δικτύων ηλεκτρονικών υπολογιστών διευκολύνει την αντιγραφή, χειραγώγηση, και διανομή των ψηφιακών δεδομένων. Η ψηφιακή υδατογράφηση είναι μια από τις λύσεις που προτείνονται για την αποτελεσματική διασφάλιση των ψηφιακών εικόνων και βίντεο. Οι τεχνικές συνήθως λειτουργούν στο πεδίο του διακριτού μετασχηματισμού κυματιδίων (DWT) και χρησιμοποιούν δυαδικές εικόνες ως υδατογραφήματα που είναι ενσωματωμένες στους συντελεστές κυματιδίων.

Κατά τα τελευταία έτη, ο μετασχηματισμός wavelet (κυματιδίων) έχει εμφανισθεί έντονα στον τομέα της επεξεργασίας εικόνας / σήματος ως εναλλακτική λύση για το γνωστό Fourier Transform (FT) και τους σχετικούς μετασχηματισμού με αυτόν, δηλαδή, τον διακριτό μετασχηματισμό συνημίτονου (DCT) και τον Διακριτό Μετασχηματισμό ημιτόνου (DST). Στη θεωρία Fourier, ένα σήμα (μια εικόνα θεωρείται ως ένα πεπερασμένο σήμα 2 - D) εκφράζεται ως άθροισμα , θεωρητικά άπειρο, ημιτόνων και συνημιτόνων, κάνοντας τον FT κατάλληλο για την ανάλυση άπειρων και περιοδικών σημάτων. Για αρκετά χρόνια, ο FT κυριάρχησε πλήρως στον τομέα της επεξεργασίας σήματος, όμως, ενώ παρέχει πληροφορίες συχνότητας που περιέχονται στην ανάλυση του σήματος, παρέλειψε να δώσει οποιαδήποτε πληροφορία σχετικά με το χρόνο εμφάνισης του σήματος.

Αυτή η αδυναμία, χωρίς να είναι η μοναδική, ώθησε τους επιστήμονες να διερευνήσουν τη πιθανότητα δημιουργίας ενός μετασχηματισμού που δεν θα έχει τα μειονεκτήματα του FT. Το πρώτο βήμα σε αυτό το μακρύ ταξίδι της έρευνας ήταν να μειωθεί το σήμα σε διάφορα τμήματα και στη συνέχεια να εξετάσουμε το κάθε τμήμα ξεχωριστά. Η ιδέα με μια πρώτη ματιά φαίνεται να είναι πολύ ελπιδοφόρα, δεδομένου ότι επέτρεψε την άντληση πληροφοριών χρόνου και τον εντοπισμός των διαφόρων συνιστωσών συχνοτήτων. Η προσέγγιση αυτή είναι γνωστή ως μετασχηματισμός Short -Time Fourier (STFT). Το θεμελιώδες ερώτημα που τίθεται εδώ είναι πώς θα χωριστεί σε τμήματα το σήμα. Η καλύτερη λύση σε αυτό το δίλημμα ήταν φυσικά να βρεθεί ένα πλήρως επεκτάσιμο διαμορφωμένο παράθυρο στο οποίο καμία περικοπή σήματος δεν θα είναι πλέον αναγκαία. Αυτός ο στόχος επιτεύχθηκε επιτυχώς με την χρήση του μετασχηματισμού wavelet.

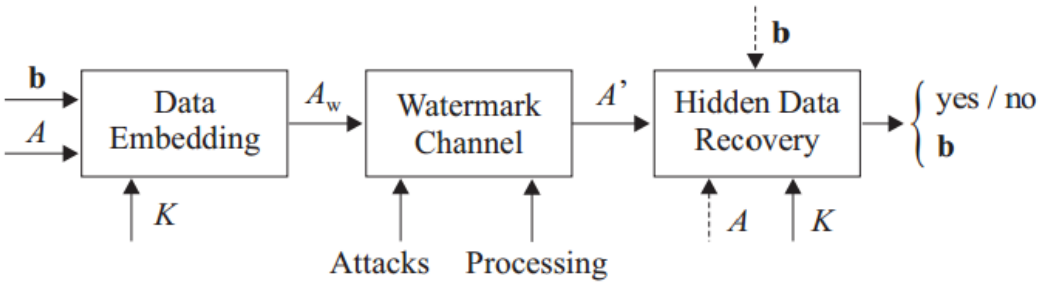
Τυπικά, ο μετασχηματισμός wavelet ορίζεται από πολλούς συγγραφείς ως μια μαθηματική τεχνική κατά την οποία αναλύεται ένα συγκεκριμένο σήμα (ή συντίθενται) στο πεδίο του χρόνου με τη χρήση διαφορετικών εκδοχών μίας καθυστερημένης ή μετατοπισμένης συνάρτησης βάσης που ονομάζεται πρωτότυπο wavelet ή η μήτρα wavelet.

3.4 *Πιστοποίηση αυθεντικότητας δεδομένων*

Η μεγάλη ποικιλία των εργαλείων επεξεργασίας σήματος που διατίθενται σήμερα επιτρέπει σε οποιονδήποτε να τροποποιήσει εύκολα ψηφιακά αντικείμενα πολυμέσων, όπως ήχο, ακόμα και εικόνες ή βίντεο χωρίς να αφήνει κανένα ορατό ίχνος των τροποποιήσεων. Ακόμα κι αν αυτά τα εργαλεία είναι εξαιρετικά χρήσιμα σε διάφορα σενάρια, όπως π.χ. στην αύξηση της αντιληπτής ποιότητα του περιεχομένου πολυμέσων, υπάρχουν περιπτώσεις στις οποίες θα θέλαμε να είμαστε σίγουροι ότι το ψηφιακό περιεχόμενο είναι αυθεντικό, δηλαδή αντιστοιχεί στην αρχική έκδοση. Με άλλο τρόπο, θα θέλαμε να βρούμε έναν τρόπο για να αποφευχθεί η απώλεια της αξιοπιστίας των ψηφιακών δεδομένων. Η πιστοποίηση της αυθεντικότητας είναι η επιστήμη που μελετά την προστασία της ακεραιότητας των ψηφιακών μέσων. Σε γενικές γραμμές, υπάρχουν δύο βασικές μορφές της πιστοποίησης αυθεντικότητας: η παθητική και η ενεργητική. Η παθητική, που ονομάζεται επίσης εγκληματολογική ανάλυση, προσπαθεί να καταλάβει αν ένα ψηφιακό περιεχόμενο έχει αλλοιωθεί με τη χρήση στατιστικής ανάλυσης χωρίς προηγουμένως να έχει προστεθεί ένα σήμα ελέγχου αυθεντικότητας στο ψηφιακό μέσο. Η παθητική πιστοποίηση αυθεντικότητας έχει το επιθυμητό χαρακτηριστικό ότι μπορεί να εφαρμοστεί σε σχεδόν οποιαδήποτε είδος δεδομένων, χωρίς να απαιτείται τροποποίηση κατά τη στιγμή της δημιουργίας. Από την αρνητική πλευρά, η παθητική πιστοποίηση δεν είναι πάντα εφικτή και υπάρχουν αμφιβολίες σχετικά με την αξιοπιστία και την ασφάλεια τή. Αυτό δεν ισχύ με την ενεργό πιστοποίηση, οπότε η ακεραιότητα ενός ψηφιακού περιεχομένου προστατεύεται (και όπως αποδείχθηκε) με την ενσωμάτωση ενός σήματος ελέγχου αυθεντικότητας στο ψηφιακό αρχείο πριν τη διανομή του σε άλλους χρήστες. Ο ενεργός έλεγχος αυθεντικότητας επίσης ονομάζεται υδατογράφηση, δεδομένου ότι χρησιμοποιεί την τεχνολογία υδατογράφησης ώστε να ενσωματώσει το σήμα ελέγχου αυθεντικότητας στο προς προστασία υλικό.

Ο κατάλογος των πρακτικών σεναρίων σχεδόν ενδιαφέρεται υδατογράφηση με βάση ταυτότητας είναι ατελείωτες. Οι πιο προφανείς εφαρμογές είναι αυτές που σχετίζονται με την εγκληματολογία, όπου μια ισχυρή εξασφάλιση της αυθεντικότητας των ψηφιακών εικόνων είναι απαραίτητη λόγω της σημασίας ότι τους ως αποδεικτικά στοιχεία στο δικαστήριο. Ομοίως, η πιστοποίησης αυθεντικότητας μέσω της υδατογράφησης προτάθηκε πρόσφατα ως ένας τρόπος

παροχής της πρωτοτυπίας των ψηφιακών βίντεο που αποκτήθηκαν εντός συστημάτων βιντεοεπιτήρησης.



Εικόνα 10: Πιστοποίηση αυθεντικότητας που βασίεται στην υδατογράφηση (D'Angelo et al. 2008)

Μια άλλη δυνατότητα είναι να γίνει χρήση των ενσωματωμένων υδατογραφημάτων για να διασφαλιστεί η ορθή ανάκτηση του ψηφιακού περιεχομένου που μεταδίδεται μέσω ενός επιρρεπούς σε σφάλματα διαύλου. Το ενσωματωμένο υδατογράφημα μπορεί επίσης να χρησιμοποιηθεί για την ανάκτηση μέρους των πληροφοριών που χάνονται λόγω σφαλμάτων μετάδοσης.

Η πιστοποίηση αυθεντικότητας που βασίζεται στην υδατογράφηση μπορεί επίσης να χρησιμοποιηθεί για να αποδειχθεί η προέλευση και ως εκ τούτου η πρωτοτυπία του ψηφιακού περιεχομένου που αγοράζεται ή διανεμεται μέσω μη αξιόπιστων καναλιών π.χ. στο διαδίκτυο. Σε πολλές περιπτώσεις, στην πραγματικότητα, γνωρίζουμε την προέλευση ενός ψηφιακού περιουσιακού στοιχείου και αποδεικνύοντας την ακεραιότητα του είναι ένας καλός τρόπος για να ληφθούν πληροφορίες σχετικά με την ποιότητα του ίδιου του περιουσιακού στοιχείου, και την καταλληλότητα του κόστους ή την νομιμότητα των εμπορικών συναλλαγών.

Για τον έλεγχο αυθεντικότητας κειμένου, εύθραυστα υδατογραφήματα μπορούν να χρησιμοποιηθούν για να ανιχνεύσουν οποιαδήποτε αλλοίωση σε ένα έγγραφο κειμένου. Αν το υδατογράφημα ανιχνεύεται, το έγγραφο κείμενο είναι γνήσιο, αν όχι, το κείμενο έχει αλλοιωθεί και δεν μπορεί να θεωρηθεί γνήσιο. Είναι πολύ απαραίτητο για την επικύρωση του κειμένου, ειδικά όταν χρησιμοποιείτε για νομικούς λόγους. Σε ευαίσθητες επικοινωνίες π.χ. σε εφαρμογές άμυνας και στην επικοινωνία των επιχειρήσεων, είναι εξαιρετικά σημαντικό για τον έλεγχο αυθεντικότητας, να γίνεται έλεγχος της αξιοπιστία και της πληρότητα των μηνυμάτων κειμένου.

Μια ανασκόπηση των συστημάτων ελέγχου αυθεντικότητας που βασίζονται στην υατογράφηση καταλήγει στην ταξινόμηση των τεχνικών σε τρεις κατηγορίες:

(1) εύθραυστη υδατογράφηση, η οποία ανιχνεύει οποιαδήποτε τροποποίηση του ψηφιακού αρχείου

(2) ημι-εύθραυστη υδατογράφηση, η οποία ανιχνεύει και εντοπίζει κακόβουλες τροποποιήσεις ενώ είναι ανεκτική στις κλασικές τροποποιήσεις του χρήστη όπως συμπίεση,

(3) ισχυρή υδατογράφηση, η οποία ανιχνεύει μόνο σημαντικές αλλαγές στο περιεχόμενο, ενώ επιτρέπει τη διατήρηση του περιεχομένου κατά την επεξεργασία.

Είναι σημαντικό να επισημάνουμε ότι, σύμφωνα με την τρέχουσα κατάσταση της έρευνας, είναι δύσκολο να επιβεβαιωθεί ποια προσέγγιση φαίνεται να είναι πιο κατάλληλη για την εξασφάλιση της αυθεντικότητας προσαρμοσμένη στα αρχεία πολυμέσων. Μια λύση που να ταιριάζει τέλεια με όλους τους περιορισμούς που θέτουν τα πρακτικά σενάρια όλων των ψηφιακών αρχείων δεν υπάρχει, δεδομένου ότι κάθε λύση πρόκειται να εξαρτάται αυστηρά από τη συγκεκριμένη εφαρμογή και το σύστημα για το οποίο προορίζεται.

Σε γενικές γραμμές, οι εύθραυστες μέθοδοι υδατογράφησης είναι πολύ ευαίσθητες στην παραμικρή υποβάθμιση του μέσου, αλλά προσφέρουν μόνο μια αυστηρή υπηρεσία πιστοποίησης, που δεν συνδέεται με τις ανάγκες των χρηστών. Έτσι, η σημερινή τάση είναι όλο και περισσότερο προς τη χρήση των σημι-εύθραυστων ή ισχυρών μεθόδων.

Το κύριο εμπόδιο για την ευρεία αξιοποίηση των μεθόδων αυτών, ωστόσο, είναι ο ορισμός μιας μεθόδου για την εξαγωγή μίας σημασιολογικής περίληψης του αρχείου που θα πιστοποιηθεί. Στην τρέχουσα βιβλιογραφία κάτι τέτοιο συχνά αναφέρεται ως ισχυρός κατακερματισμός, ένα πρόβλημα που έχει λάβει σημαντική προσοχή τα τελευταία χρόνια και που πηγαίνει πέρα από την ιδιαίτερη περίπτωση της πιστοποίησης αυθεντικότητας.

Η προσέγγιση της υδατογράφησης δεν είναι ο μόνος δυνατός τρόπος για να αντιμετωπιστεί το πρόβλημα πιστοποίησης της αυθεντικότητας. Άλλες λύσεις είναι διαθέσιμες συμπεριλαμβανομένων, για παράδειγμα, οι κρυπτογραφικές λύσεις και η παθητική πιστοποίηση αυθεντικότητας που αναφέραμε προηγουμένως μέσω ανάλυσης εγκληματολογίας.

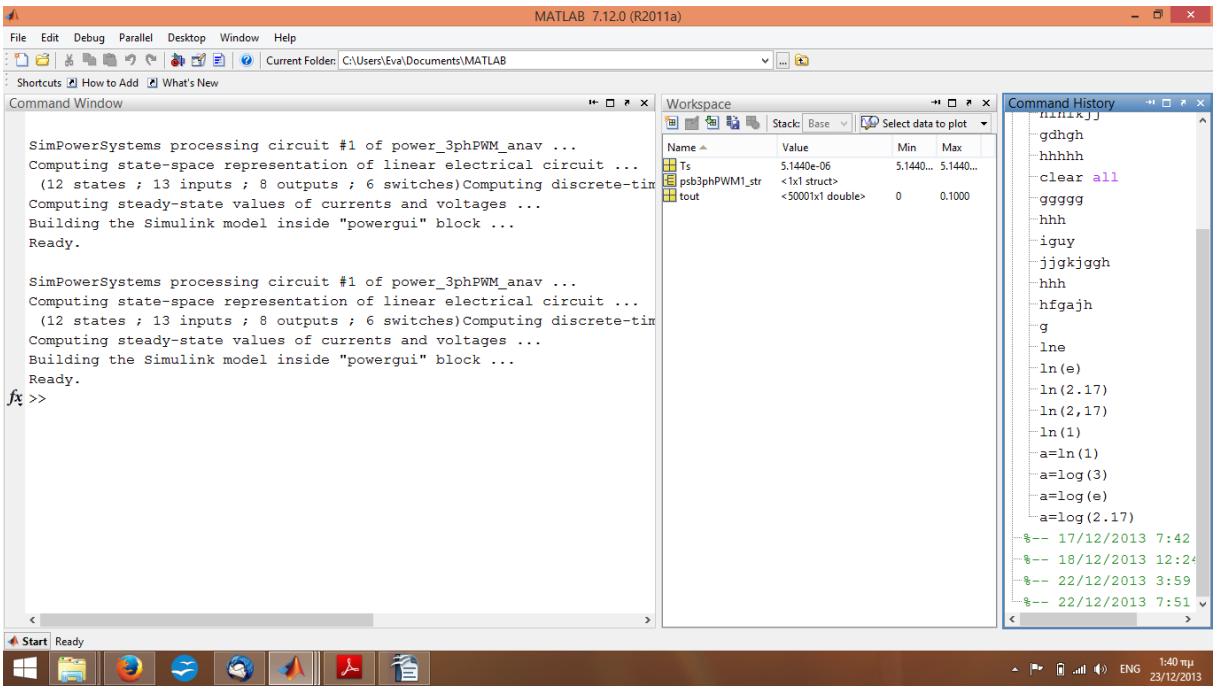
Κεφάλαιο 4. Εφαρμογές

4.1 Εισαγωγή στο Matlab

Το λογισμικό MATLAB χρησιμοποιείται σε πανεπιστημιακά μαθήματα αλλά και ερευνητικές και άλλες εφαρμογές με επιστημονικούς ή και ερευνητικούς υπολογισμούς. Εκτός από την επίλυση αριθμητικών υπολογισμών παρέχει οπτικοποίηση δεδομένων (γραφικές παραστάσεις) και δυνατότητες προγραμματισμού με βάση τη γλώσσα C.

Το Simulink είναι προέκταση του λογισμικού MATLAB. Σκοπός του Simulink είναι η σχεδίαση, η προσομοίωση και η ανάλυση μοντέλων συστημάτων. Η μοντελοποίηση γίνεται μέσα από γραφικό περιβάλλον διεπαφής (GUI). Ένα μοντέλο συστήματος αποτελείται από δομικά στοιχεία που ονομάζονται «blocks». Το Simulink περιλαμβάνει πολλά blocks στις βιβλιοθήκες του, αλλά υπάρχει η δυνατότητα να δημιουργηθούν νέα από τον χρήστη ή να εισαχθούν έτοιμα. Κάθε block έχει δική του εμφάνιση και όνομα και περιγράφεται από τις παραμέτρους με τις οποίες επηρεάζει το υπόλοιπο σύστημα.

Λόγω των πολλών δυνατοτήτων που προσφέρει και του μεγάλου φάσματος εφαρμογών που καλύπτει, το Simulink (και κατ'επέκταση το MATLAB) θεωρείται από τα δημοφιλέστερα εργαλεία του είδους του.



Εικόνα 4.1. Παράθυρο εντολών Matlab

Με τον όρο προσομοίωση εννοούμε την εικονική λειτουργία ενός συστήματος με πραγματικές τιμές των στοιχείων και πραγματικές τιμές τάσεων-εντάσεων. Τα πλεονεκτήματα της προσομοίωσης είναι πολλά. Είναι αναμφισβήτητα ταχύτερος και οικονομικότερος τρόπος από την κατασκευή ενός πραγματικού κυκλώματος. Δίνει την δυνατότητα επανάληψης με ίδιες ή διαφορετικές ελεγχόμενες παραμέτρους. Μας επιτρέπει να πειραματιστούμε αλλάζοντας στοιχεία του κυκλώματος. Όλα αυτά συμβάλλουν στην καλύτερη μελέτη και κατανόηση των λειτουργιών του κυκλώματος.

Παρακάτω παρουσιάζεται ο τρόπος με τον οποίο επιλέχθηκαν οι συναρτήσεις για την υδατογράφηση εικόνας με μετασχηματισμούς 2-D που προσομοιώνονται στο Matlab. Παρουσιάζονται αναλυτικά η διαδικασία υδατογράφησης για κάθε μέθοδο, και τα αποτελέσματα που προκύπτουν από την προσομοίωση της.

4.2 Εφαρμογή στεγανογραφίας

Για την εφαρμογή στεγανογραφίας χρησιμοποιήθηκε ο κώδικας σε Matlab από την σελίδα της Mathworks. Η αρχική εικόνα καθώς και το μήνυμα που θα αποκρυφθεί με τη μέθοδο της στεγανογραφίας φαίνονται αντίστοιχα ακολούθως. Ο κώδικας παρατίθεται στο 4.2.1

1.Cover image

2.Message to be hide

Στη συνέχεια υλοποιούμε την στεγανογραφία με αντικατάσταση μόνο 1 LSB.

Οι δείκτες ποιότητας των εικόνων προκύπτουν ως:

PSNR of message image to extracted image is

13.5040

MSE is

2.9247e+003

Οι στεγανογραφημένη εικόνα δεν παρουσιάζει ιδιαίτερη οπτική παραμόρφωση.

3.Stegnographic image

Η ποιότητα όμως της εικόνας που εξάγεται είναι χαμηλή, καθώς η πληροφορία παραμορφώνεται.

4.Extracted image

Στη συνέχεια προχωράμε στην αντικατάσταση 4 LSB. Οι δείκτες ποιότητας εικόνας είναι:

PSNR of message image to extracted image is

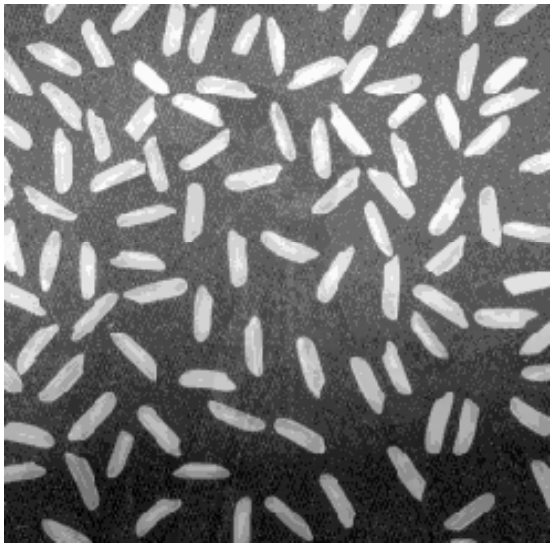
29.0184

MSE is

82.1562

Η στεγανογραφημένη εικόνα παρουσιάζει παραμόρφωση που είναι εμφανής οπτικά. Όμως η εξαγόμενη εικόνα έχει καλύτερη ποιότητα από την προηγούμενη περίπτωση.

3.Stegnographic image



4.Extracted image

4.2.1Κώδικας Στεγανογραφίας

```
%Program of Steganography Using LSB substitution%

cover = input('Enter cover image: ', 's');
message = input('Enter message image name: ', 's');

x = imread(cover);      % cover message
y = imread(message);    % message image
n = input('Enter the no of LSB bits to be subsituted-
');

S=uint8(bitor(bitand(x,bitcmp(2^n-1,8)),bitshift(y,n-8)));
%Stego
E = uint8(bitand(255,bitshift(S,8-n))); %Extracted

origImg = double(y);   %message image
distImg = double(E);   %extracted image

[M N K] = size(origImg);
distImg1=imresize(distImg,[M N]);
error = origImg - distImg1;
MSE = sum(sum(error .* error)) / (M * N);
if(MSE > 0)
    PSNR = 10*log10(M*N./MSE);
else
    PSNR = 99;
end
disp('PSNR of message image to extracted image is')
disp(abs(PSNR))
disp('MSE is')
disp(abs(MSE))

figure(1),imshow(x);title('1.Cover image')
figure(2),imshow(y);title('2.Message to be hide')
figure(3),imshow((abs(S)),[]);title('3.Stegnographic
image')
figure(4),imshow(real(E),[]); title('4.Extracted
image')
```

4.3 Εφαρμογή Υδατογραφία

Βήμα 1:

Η επιλογή της προς υδατογράφηση εικόνας, εκτελεί τις διαδικασίες διαβάσματος της εικόνας και εφαρμογής μετασχηματισμών DWT και SVD στην έγχρωμη εικόνα. Η εικόνα εμφανίζεται στην οθόνη, όπως παρουσιάζεται στην εικόνα 4.2.

Εικόνα 4.2 Εικόνα προς υδατογράφηση.

Ο κώδικας Matlab που υλοποιεί την επιλογή της βασικής εικόνας, και εκτελεί τους μετασχηματισμούς DWT και SVD είναι ο εξής:

```
rgbimage=imread('host.jpg');

figure;
imshow(rgbimage);
title('Original color image');
[h_LL,h_LH,h_HL,h_HH]=dwt2(rgbimage,'haar');
img=h_LL;
red1=img(:,:,1);
green1=img(:,:,2);
blue1=img(:,:,3);
[U_imgr1,S_imgr1,V_imgr1]= svd(red1);
[U_imgg1,S_imgg1,V_imgg1]= svd(green1);
[U_imgb1,S_imgb1,V_imgb1]= svd(blue1);
```

ΕΦΑΡΜΟΓΗ ΜΕΣΧΗΜΑΤΙΣΜΟΥ DWT

ΕΦΑΡΜΟΓΗ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΥ SVD

Βήμα 2

Στο δεύτερο στάδιο επιλέγεται μία εικόνα ως υδατογράφημα. Ομοίως με την προς υδατογράφηση εικόνα, γίνεται εφαρμογή μετασχηματισμών DWT και SVD στην έγχρωμη εικόνα του υδατογραφήματος. Η εικόνα εμφανίζεται στην οθόνη, όπως παρουσιάζεται στην εικόνα 4.3.

Ο κώδικας Matlab που υλοποιεί την επιλογή του υδατογραφήματος, και εκτελεί τους μετασχηματισμούς DWT και SVD είναι ο εξής:

```
rgbimage=imread('watermark.jpg');

figure;
imshow(rgbimage);
title('Watermark image');
[w_LL,w_LH,w_HL,w_HH]=dwt2(rgbimage,'haar');
img_wat=w_LL;
red2=img_wat(:,:,1);
green2=img_wat(:,:,2);
blue2=img_wat(:,:,3);
[U_imgr2,S_imgr2,V_imgr2]= svd(red2);
[U_imgg2,S_imgg2,V_imgg2]= svd(green2);
[U_imgb2,S_imgb2,V_imgb2]= svd(blue2);
```

Watermark image

Εικόνα 4.3 Εικόνα ως υδατογράφημα.

Βήμα 3

Η εισαγωγή του υδατογραφήματος γίνεται εφαρμόζοντας υπέρθεση σε κάθε βασικό χρώμα της βασικής εικόνας RGB με 10% των τιμών των αντίστοιχων συντελεστών της εικόνας υδατογραφήματος. Στη συνέχεια εφαρμόζεται αντίστροφος μετασχηματισμός DWT και η υδατογραφημένη εικόνα αποθηκεύεται και εμφανίζεται στη οθόνη όπως φαίνεται στην εικόνα 4.4

Ο κώδικας Matlab που εκτελεί τις παραπάνω λειτουργίες είναι ο εξής:

```
% watermarking

S_wimgr=S_imgr1+(0.10*S_imgr2);
S_wimgg=S_imgg1+(0.10*S_imgg2);
S_wimgb=S_imgb1+(0.10*S_imgb2);

wimgr = U_imgr1*S_wimgr*V_imgr1';
wimgg = U_imgg1*S_wimgg*V_imgg1';
wimgb = U_imgb1*S_wimgb*V_imgb1';

wimg=cat(3,wimgr,wimgg,wimgb);
newhost_LL=wimg;

%output

rgb2=idwt2(newhost_LL,h_LH,h_HL,h_HH,'haar');
imwrite(uint8(rgb2),'Watermarked.jpg');
figure;imshow(uint8(rgb2));title('Watermarked
   Image');
```

Παρατηρούμε ότι οπτικά δεν είναι εμφανής η εικόνα του υδατογραφήματος.

Εικόνα 4.4 Υδατογραφημένη εικόνα.

4.4 Εξαγωγή υδατογραφήματος

Βήμα 1:

Η επιλογή της αυθεντικής εικόνας (χωρίς το υδατογράφημα), εκτελεί τις διαδικασίες διαβάσματος της εικόνας και εφαρμογής μετασχηματισμών DWT και SVD στην έγχρωμη εικόνα. Η εικόνα εμφανίζεται στην οθόνη, όπως παρουσιάζεται στην εικόνα 4.5.

Εικόνα 4.5 Αυθεντική εικόνα.

Ο κώδικας Matlab που υλοποιεί την επιλογή της αυθεντικής εικόνας, και εκτελεί τους μετασχηματισμούς DWT και SVD είναι ο εξής:

```
rgbimage=imread('host.jpg');
figure;
imshow(rgbimage);
title('Original color image');
[h_LL,h_LH,h_HL,h_HH]=dwt2(rgbimage,'haar');
img=h_LL;
red1=img(:,:,1);
green1=img(:,:,2);
blue1=img(:,:,3);
[U_imgr1,S_imgr1,V_imgr1]= svd(red1);
[U_imgg1,S_imgg1,V_imgg1]= svd(green1);
[U_imgb1,S_imgb1,V_imgb1]= svd(blue1);
```

Βήμα 2:

Η επιλογή της εικόνας υδατογραφήματος, εκτελεί τις διαδικασίες διαβάσματος της εικόνας και εφαρμογής μετασχηματισμών DWT και SVD στην έγχρωμη εικόνα. Η εικόνα εμφανίζεται στην οθόνη, όπως παρουσιάζεται στην εικόνα 4.6.

Ο κώδικας Matlab που υλοποιεί την επιλογή της εικόνας υδατογραφήματος, και εκτελεί τους μετασχηματισμούς DWT και SVD είναι ο εξής:

```
rgbimage=imread('watermark.jpg');
figure;
imshow(rgbimage);
title('Watermark image');
```

```
[w_LL,w_LH,w_HL,w_HH]=dwt2(rgbimage,'haar');
img_wat=w_LL;
red2=img_wat(:,:,1);
green2=img_wat(:,:,2);
blue2=img_wat(:,:,3);
[U_imgr2,S_imgr2,V_imgr2]= svd(red2);
[U_imgg2,S_imgg2,V_imgg2]= svd(green2);
[U_imgb2,S_imgb2,V_imgb2]= svd(blue2);
```

Watermark image

Εικόνα 4.6 Εικόνα υδατογραφήματος.

Βήμα 3:

Η επιλογή της υδατογραφημένης εικόνας, εκτελεί τις διαδικασίες διαβάσματος της εικόνας και εφαρμογής μετασχηματισμών DWT και SVD στην έγχρωμη εικόνα. Η εικόνα εμφανίζεται στην οθόνη, όπως παρουσιάζεται στην εικόνα 4.7.

Εικόνα 4.7 Υδατογραφημένη εικόνα.

Ο κώδικας Matlab που υλοποιεί την επιλογή της υδατογραφημένης εικόνας, και εκτελεί τους μετασχηματισμούς DWT και SVD είναι ο εξής:

```
rgbimage=imread('watermarked.jpg');
figure;
imshow(rgbimage);
title('Watermarked image');
[wm_LL,wm_LH,wm_HL,wm_HH]=dwt2(rgbimage,'haar');
img_w=wm_LL;
red3=img_w(:,:,1);
green3=img_w(:,:,2);
blue3=img_w(:,:,3);
[U_imgr3,S_imgr3,V_imgr3]= svd(red3);
[U_imgg3,S_imgg3,V_imgg3]= svd(green3);
[U_imgb3,S_imgb3,V_imgb3]= svd(blue3);
```

Βήμα 4:

Στο τέταρτο βήμα εκτελούνται οι διαδικασίες εξαγωγής του υδατογραφήματος. Αρχικά αφαιρείται από κάθε πλαίσιο βασικού χρώματος της υδατογραφημένης εικόνας, το αντίστοιχο πλαίσιο της αυθεντικής εικόνας, ώστε να μείνουν μόνο οι τιμές για το υδατογράφημα. Στη συνέχεια οι τιμές αυτές διαιρούνται με το ποσοστό 10% με το οποίο είχε ενταχθεί το υδατογράφημα στην αυθεντική εικόνα, ώστε να ληφθούν οι πραγματικές, αυθεντικές τιμές του υδατογραφήματος. Τέλος εφαρμόζεται ο μετασχηματισμός SVD και τα πλαίσια χρώματος συντίθενται στην εικόνα υδατογραφήματος. Με αυτό τον τρόπο εξάγεται το υδατογράφημα. Η εικόνα εμφανίζεται στην οθόνη, όπως παρουσιάζεται στην εικόνα 4.8.

Ο κώδικας Matlab που υλοποιεί την εξαγωγή του υδατογραφήματος είναι ο εξής:

```
S_ewatr=(S_imgr3-S_imgr1)/0.10;
S_ewatg=(S_imgg3-S_imgg1)/0.10;
S_ewatb=(S_imgb3-S_imgb1)/0.10;
```

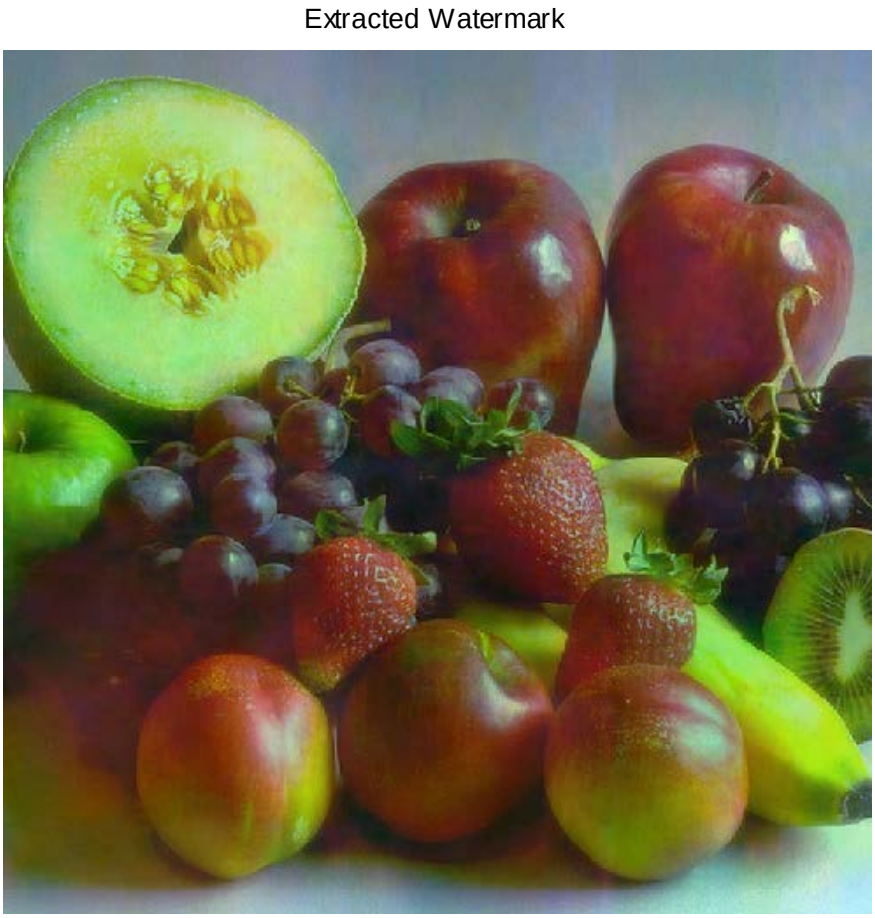
```
ewatr = U_imgr2*S_ewatr*V_imgr2';
ewatg = U_imgg2*S_ewatg*V_imgg2';
ewatb = U_imgb2*S_ewatb*V_imgb2';

ewat=cat(3,ewatr,ewatg,ewatb);

newwatermark_LL=ewat;

%output

rgb2=idwt2(newwatermark_LL,w_LH,w_HL,w_HH,'haar');
figure;imshow(uint8(rgb2));
imwrite(uint8(rgb2),'EWatermark.jpg');title('Extracte
d Watermark');
```



Εικόνα 2.8 Εξαγωγή υδατογραφήματος.

4.5 Προγράμματα χωρίς κώδικα

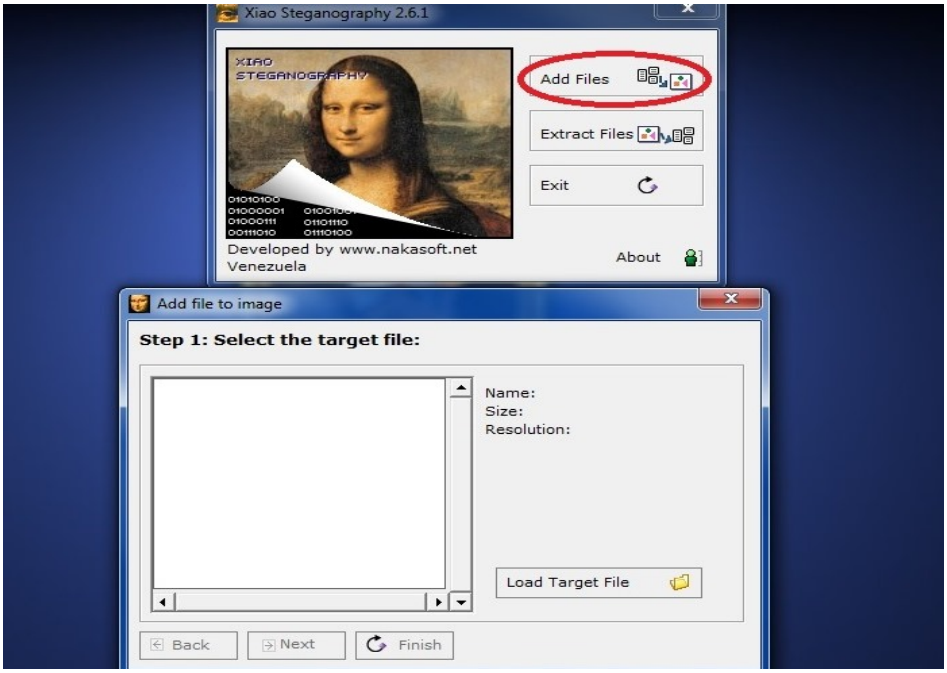
4.5.1Απόκρυψη εικόνας

1. Εφαρμογή στεγανογραφίας με το πρόγραμμα **Xiao Steganography 2.6.1**. Ανοίγουμε το πρόγραμμα.

1

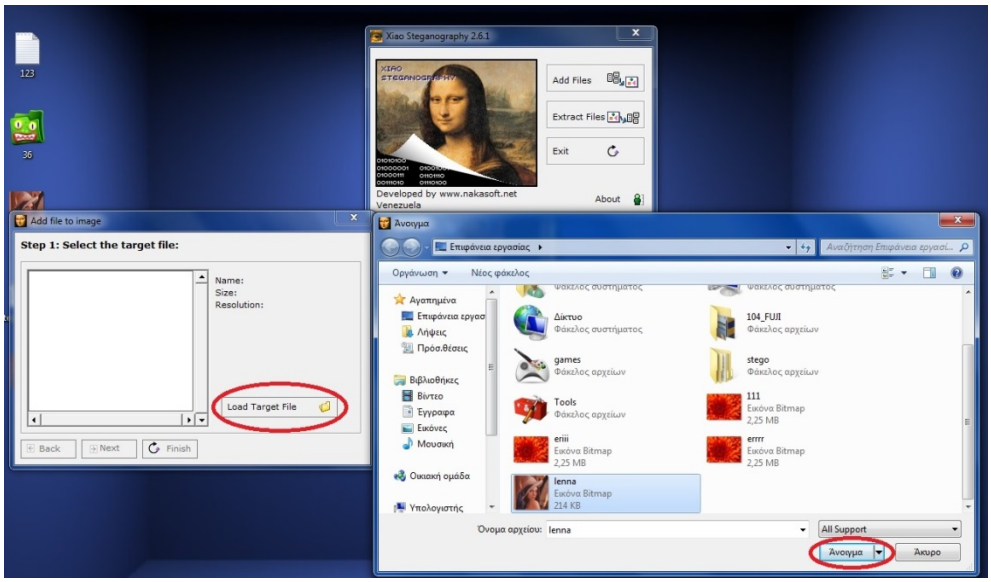
2. Πατάμε πάνω στο **Add Files**.

2



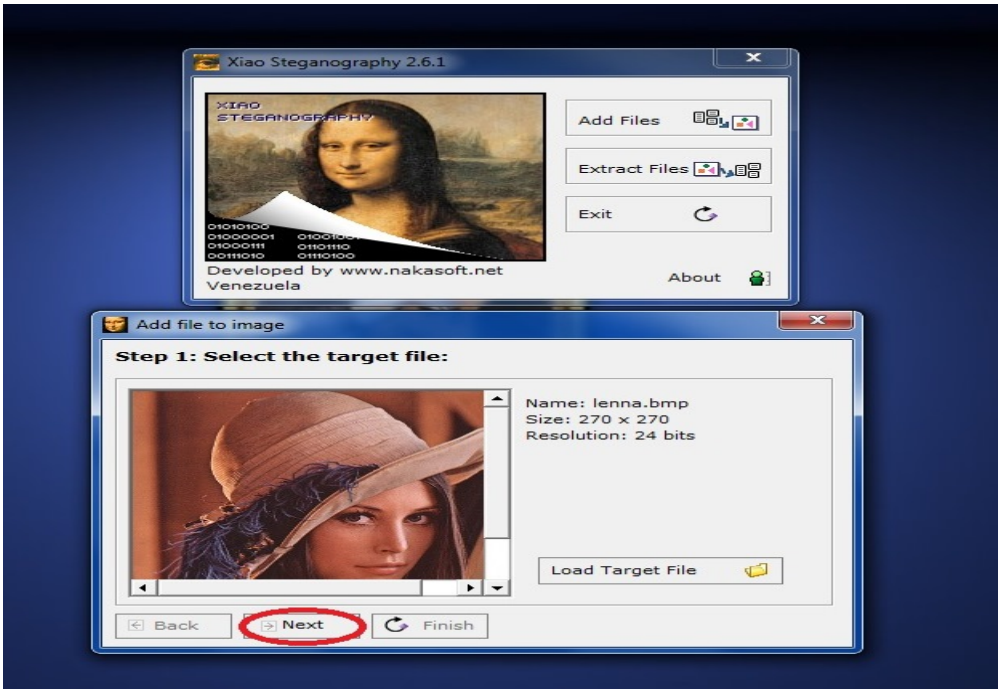
3. Πατάμε το **Local Target File** για να για να διαλέξουμε την εικόνα που θα χρησιμοποιήσουμε

3



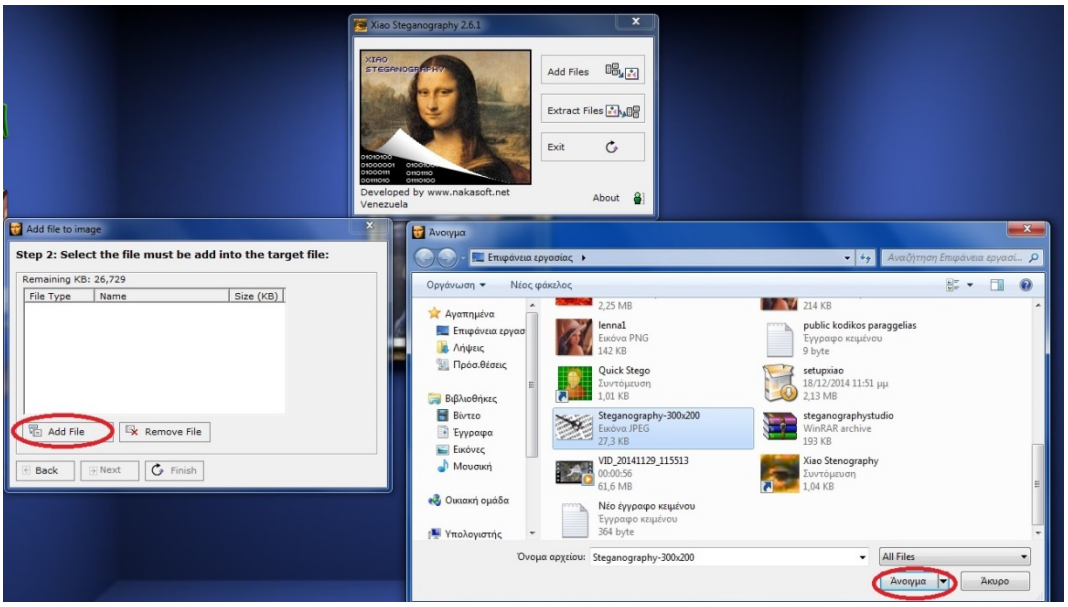
4. Αφού επιλέξουμε την εικόνα πατάμε **Next.**

4



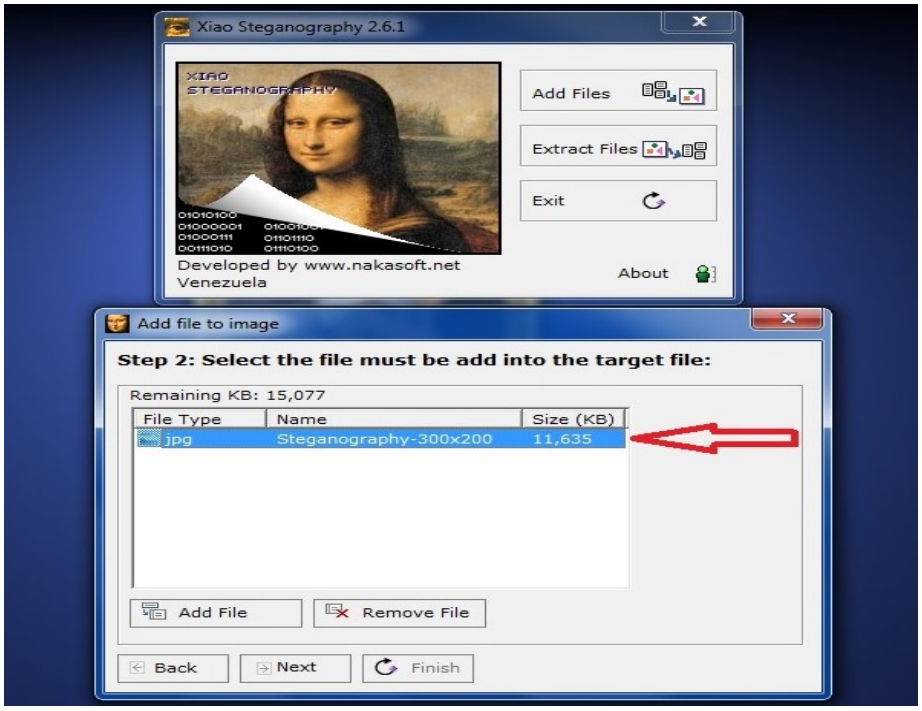
5. Ύστερα πρέπει να επιλέξουμε το έγγραφο ή την εικόνα που θέλουμε να κρύψουμε. Πατάμε **Add File→Επιλογή εγγράφου→Άνοιγμα**

5



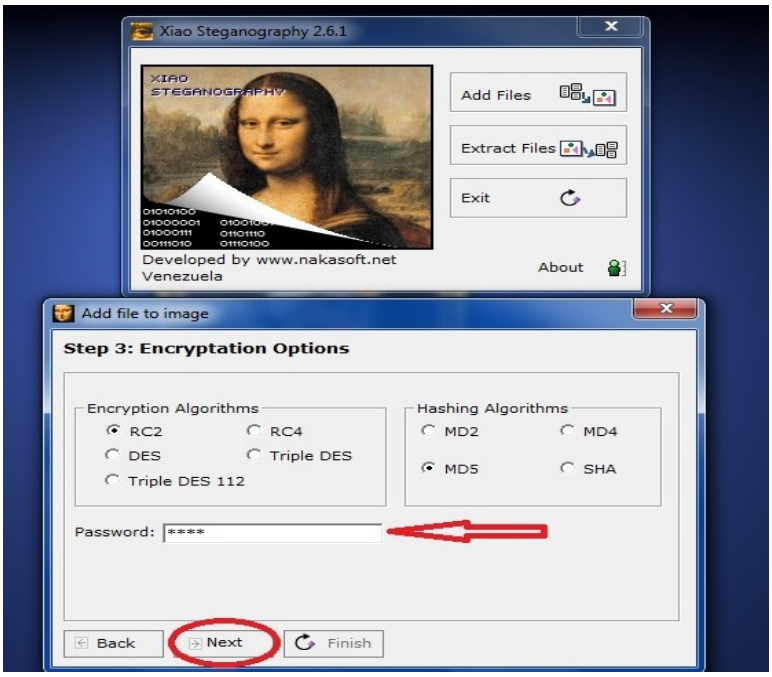
6. Εφόσον η εικόνα είναι στο επιτρεπόμενο όριο τότε συνεχίζουμε με το **Next.**

6



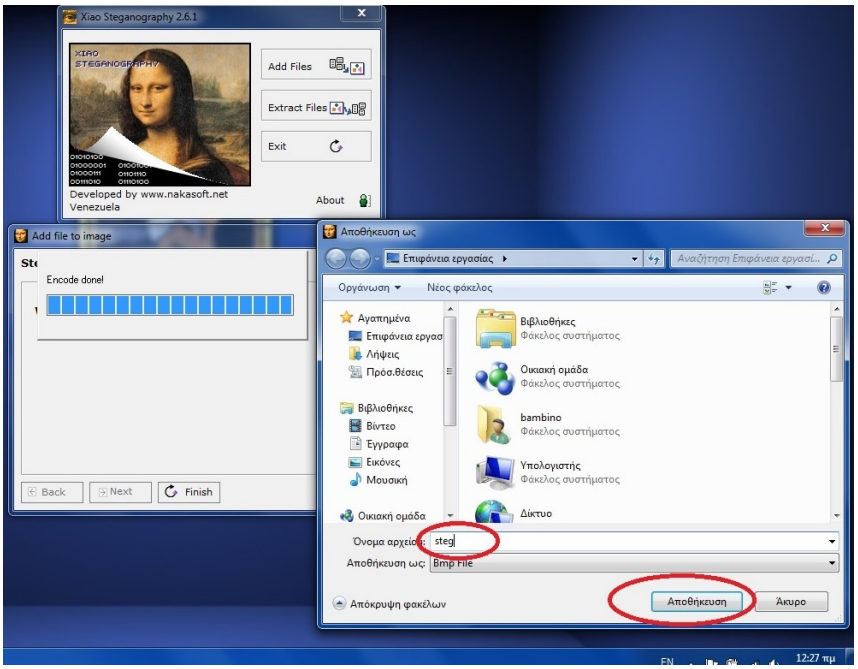
7. Βάζουμε κωδικό → Next

7



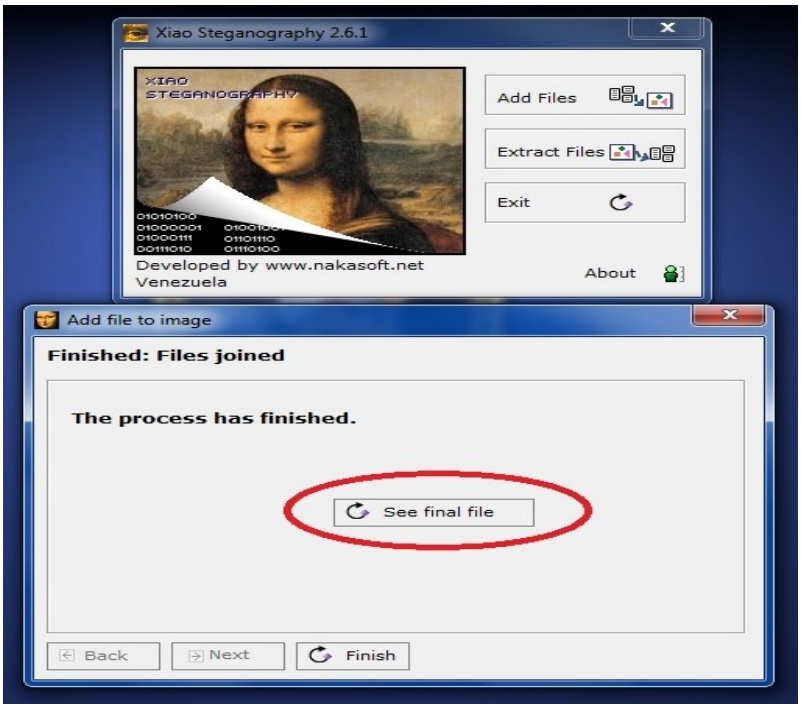
8. Αποθηκεύουμε την εικόνα με το όνομα που επιθυμούμε.→**Αποθήκευση**

8



9. Ανοίγουμε την τελική εικόνα.→ **See final file**

9



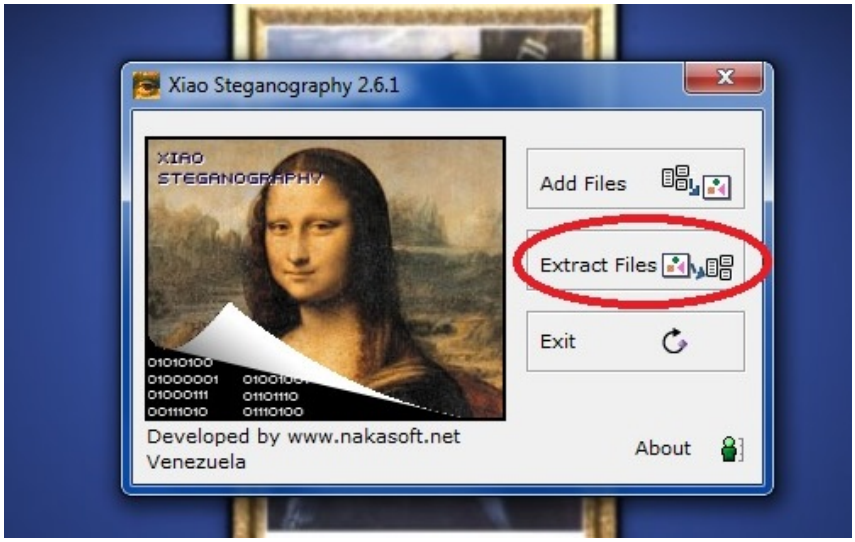
10. Εδώ βλέπουμε την εικόνα χωρίς καμμία εμφανή αλλαγή.

10

4.5.2 Εμφάνιση κρυμμένης εικόνας

1. Για να εμφανίσουμε την κρυμμένη εικόνα ανοίγουμε το πρόγραμα **Xiao.**
   Πατάμε **Extract Files.**

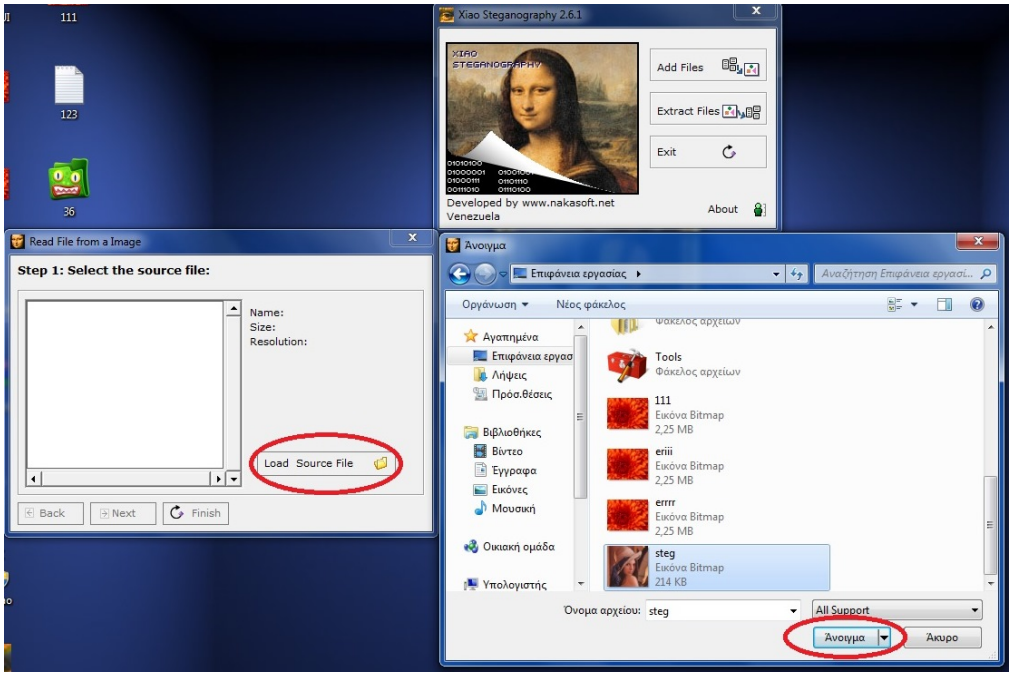
1



2. → **Load Source File** για να διαλέξουμε την εικόνα μεσα στην οποία είναι κρυμμένη η άλλη εικόνα

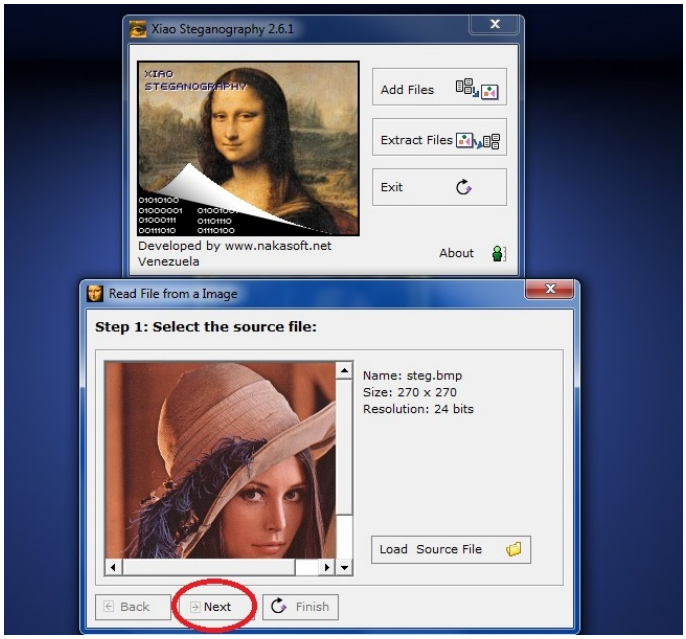
   → **Άνοιγμα**

2



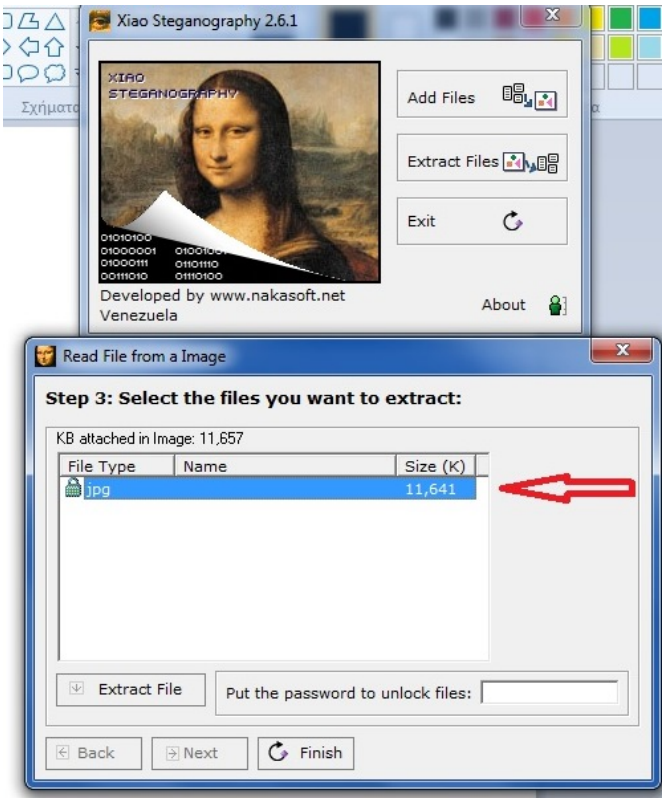
3. Αφού έχουμε διαλέξει την εικόνα προχωράμε με →**Next**

3



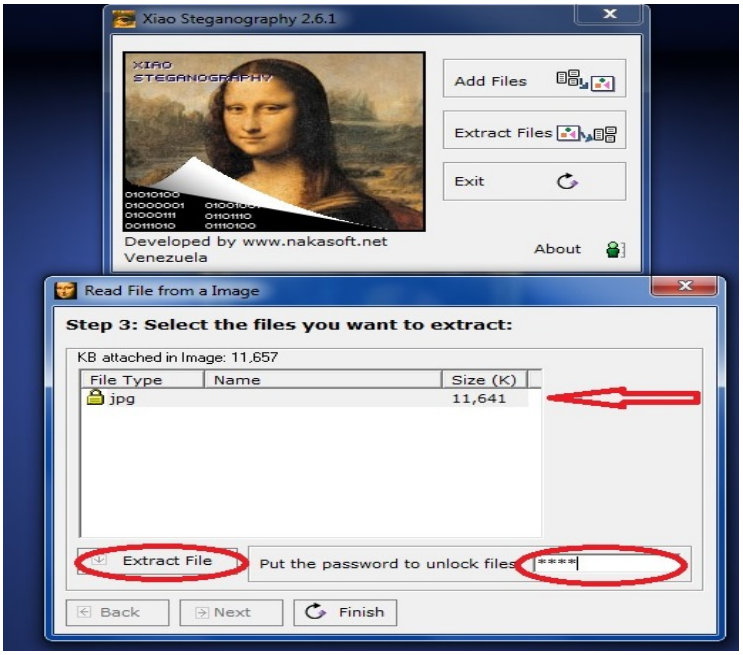
4. Εδώ εμφανίζετε το μέγεθος της εικόνας

4



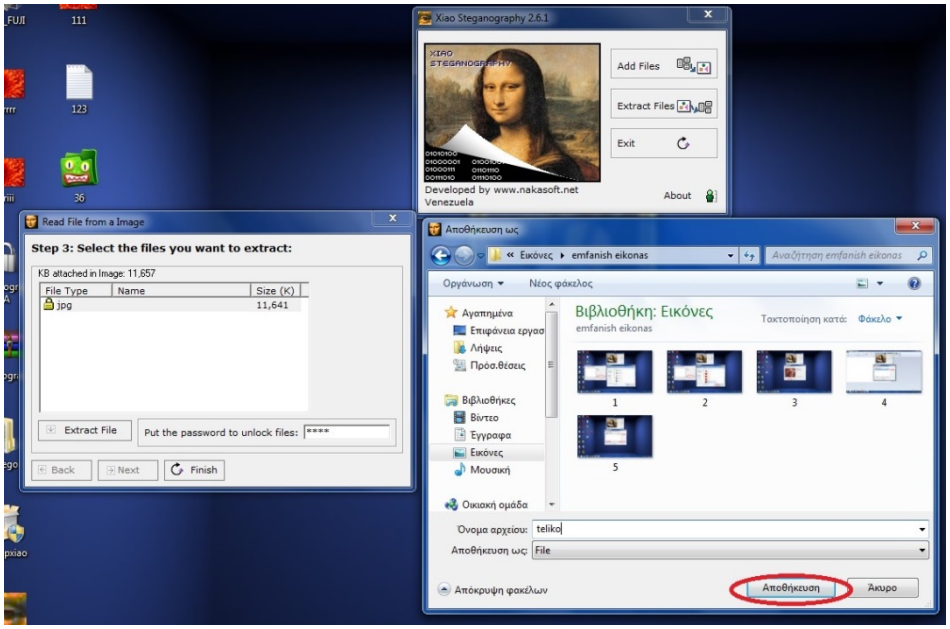
5. Βάζουμε το κωδικό
→ **Extract File**

5



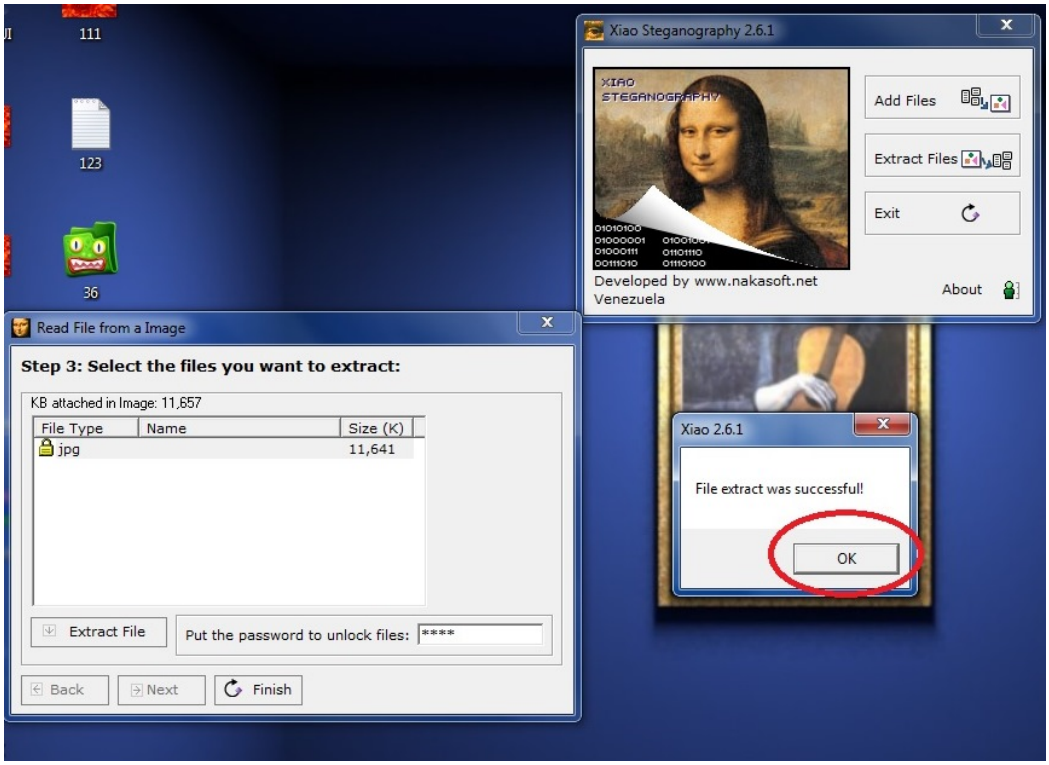
6. Γράφουμε το όνομα που θέλουμε να αποθηκεύσουμε την κρυμμένη εικόνα.
→ **Αποθήκευση**

6



7. → **OK**

7



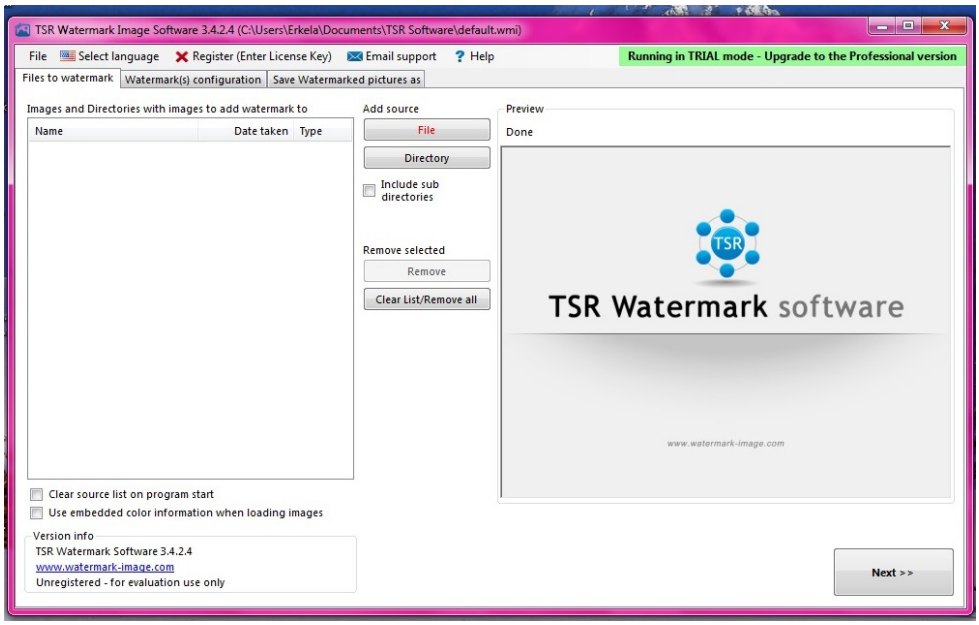
8. Κρυμμένη εικόνα

8

4.5.3 Υδατογραφία σε εικόνα

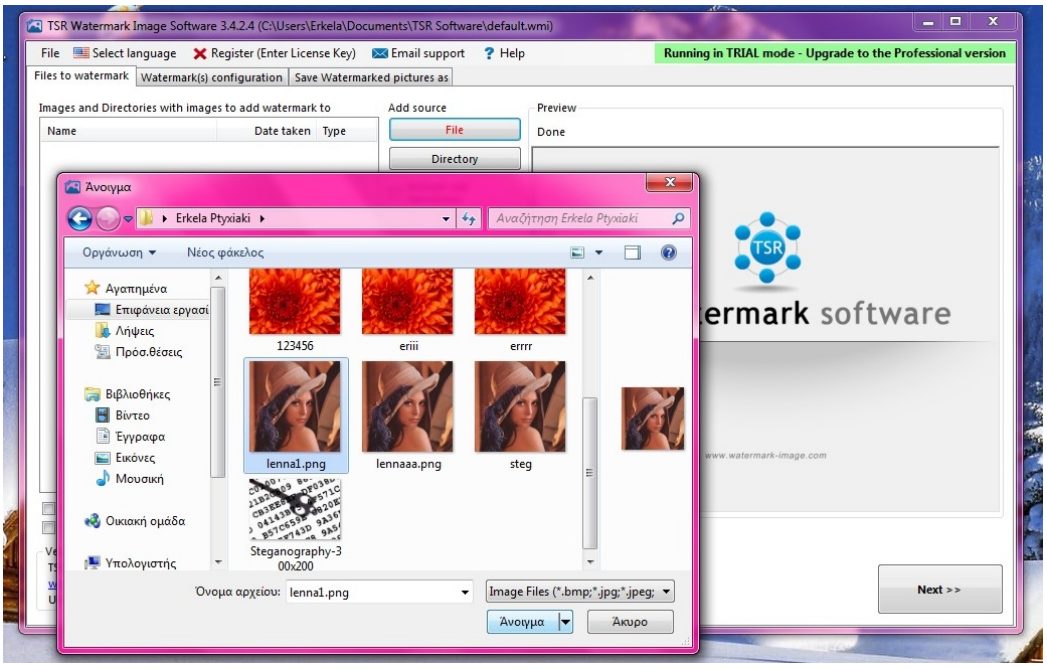
1. Άνοιγμα προγράμματος (TSR Watermark Image Software)
   →**File**

1



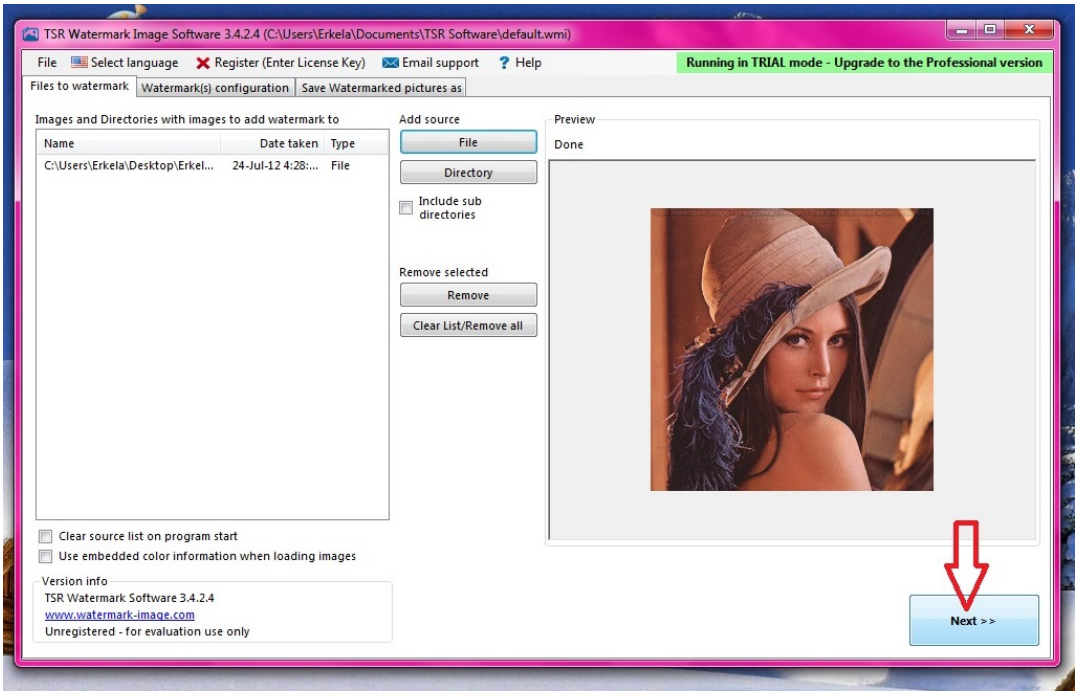
2. Επιλογή της εικόνας που επιθυμούμε
   →**Άνοιγμα**

2



3. →**Next**

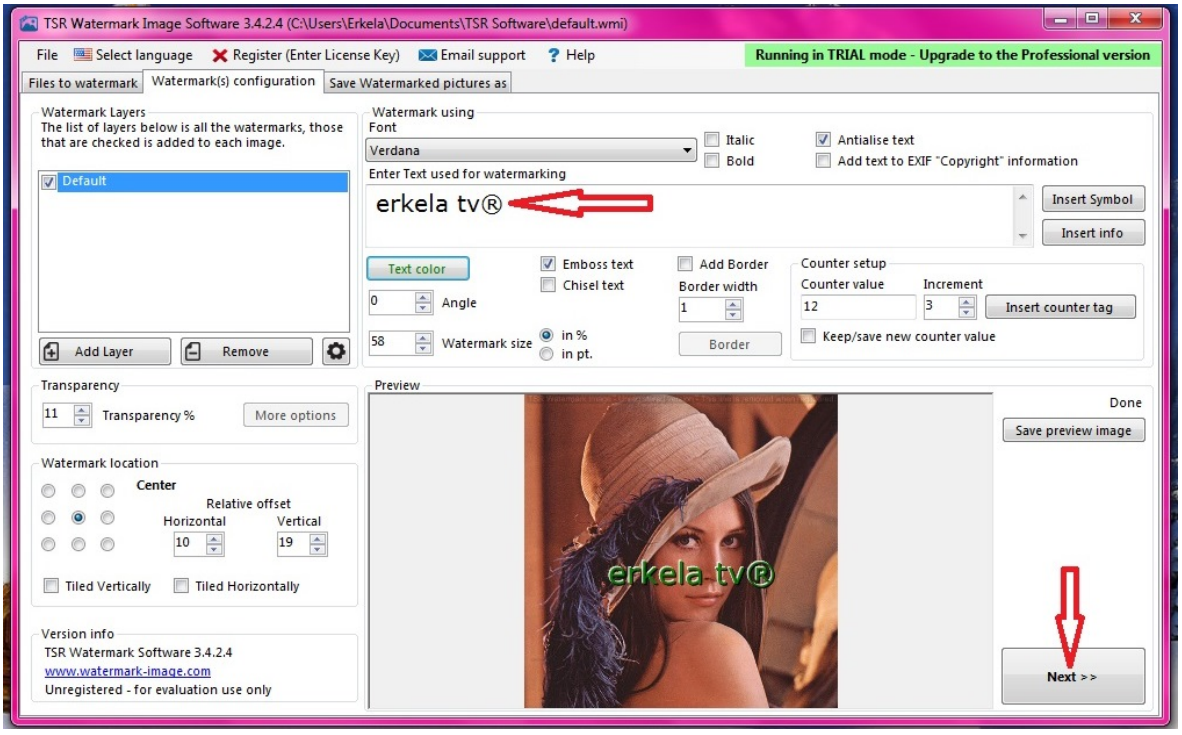
3



4. Επιλογή και ρυθμίσεις υδατογραφίας

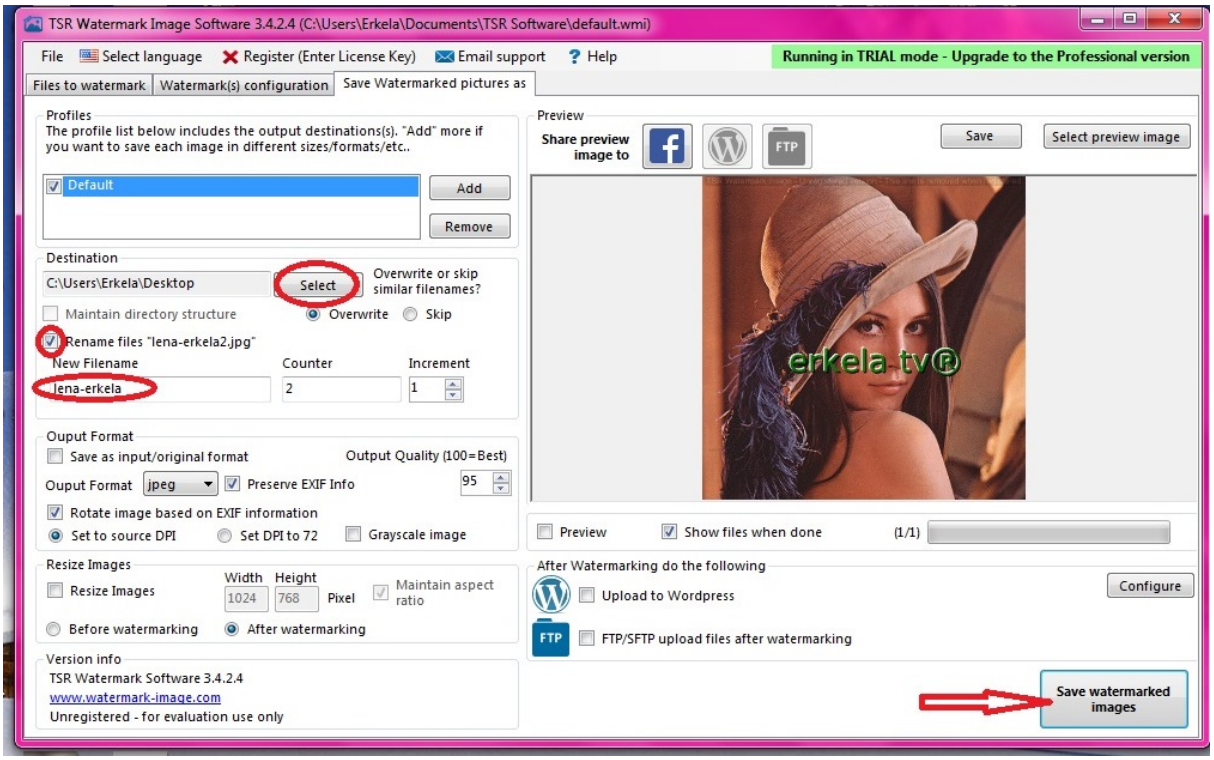
→ **Next**

4



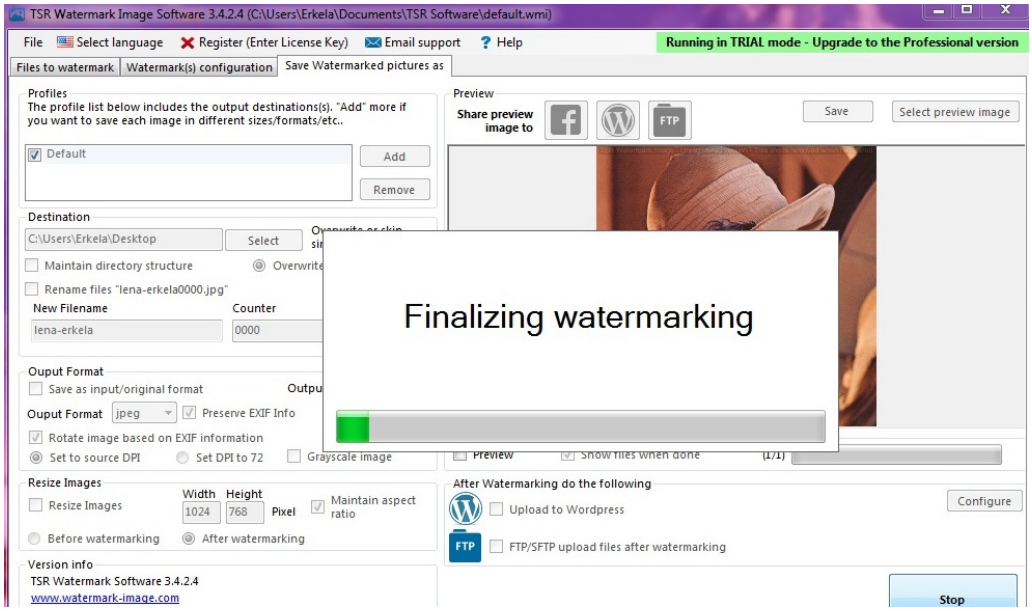
5. Επιλογή θέσεις αρχείου-Επιλογή ονόματος νέας εικόνας
→ **Save watermarked images**

5



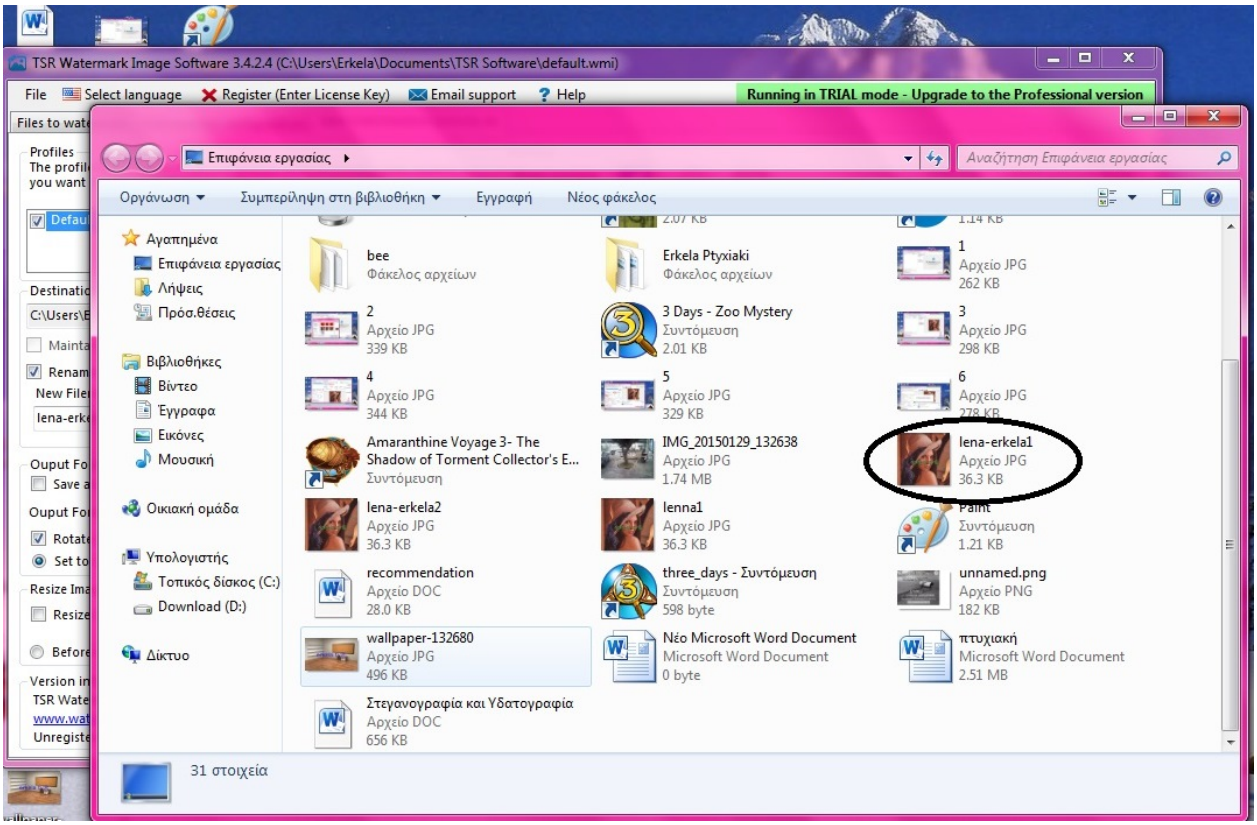
6. Αποθήκευση

6



7. Εμφάνιση εικόνας

7



8. Τελική εικόνα

8

Βιβλιογραφία

- Narasimha, M.; Peterson, A. (June 1978). "On the Computation of the Discrete Cosine Transform". IEEE Transactions on Communications 26 (6): 934–936.
- Chui, Charles K. (1992). *An Introduction to Wavelets*. San Diego: Academic Press
- R. Polikar, (1999). The wavelet tutorial. Διαθέσιμο: http://users.rowan.edu/~polikar/WAVELETS/WTtutorial.html
- GSL Team (2007). *§14.4 Singular Value Decomposition*. GNU Scientific Library. Reference Manual. Διαθέσιμο: http://www.gnu.org/software/gsl/manual/html_node/Singular-Value-Decomposition.html
- Wall, Michael E., Andreas Rechtsteiner, Luis M. Rocha (2003). *Singular value decomposition and principal component analysis*. Διαθέσιμο: http://public.lanl.gov/mewall/kluwer2002.html
- Coatrieaux et al. (2010). *Reconstruction of tomographic images from limited range projections using discrete Radon transform and Tchebichef moments*. Pattern Recognition 43, pp 1152—1164
- Παπακώστας, Τσουγένης και Κουλουριώτης (2014). *Moment-based local image watermarking via genetic optimization*, Applied Mathematics and Computation, 227, p 222-236.
- Huynh-Thu, Q.; Ghanbari, M. (2008). "Scope of validity of PSNR in image/video quality assessment". Electronics Letters 44 (13): 800
- Salomon, David (2007). Data Compression: The Complete Reference (4 ed.). Springer. p. 281
- Fridrich, Jessica; M. Goljan and D. Soukal (2004). "Searching for the Stego Key". Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 5306: 70–82. Retrieved 23 January 2014.

- Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet. Archived from the original on 2007-07-16.
- Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "Information Hiding: A survey" (pdf). Proceedings of the IEEE (special issue) 87 (7): 1062–78. doi:10.1109/5.771065.
- Trimenius "Polygraphiae (cf. p. 71f)". Digitale Sammlungen.
- Akbas E. Ali (2010). "A New Text Steganography Method By Using Non-Printing Unicode Characters". Eng. & Tech. Journal 28 (1).
- Social Steganogrphy: how teens smuggle meaning past the authority figures in their lives, Boing Boing, May 22, 2013.
- Krzysztof Szczypiorski (4 November 2003). "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System - HICCUPS". Institute of Telecommunications Seminar.
- Patrick Philippe Meier (5 June 2009). "Steganography 2.0: Digital Resistance against Repressive Regimes". irevolution.wordpress.com.
- Craig Rowland (May 1997). "Covert Channels in the TCP/IP Suite". First Monday Journal.
- Steven J. Murdoch and Stephen Lewis (2005). "Embedding Covert Channels into TCP/IP". Information Hiding Workshop.
- Kamran Ahsan and Deepa Kundur (December 2002). "Practical Data Hiding in TCP/IP". ACM Wksp. Multimedia Security.
- Kundur D. and Ahsan K. (April 2003). "Practical Internet Steganography: Data Hiding in IP". Texas Wksp. Security of Information Systems.
- Wojciech Mazurczyk and Krzysztof Szczypiorski (November 2008). "Steganography of VoIP Streams". Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico.
- Bartosz Jankowski, Wojciech Mazurczyk, and Krzysztof Szczypiorski (11 May 2010). "Information Hiding Using Improper Frame Padding".

- Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski (February 2010). "Vice Over IP: The VoIP Steganography Threat". IEEE Spectrum.
- Krzysztof Szczypiorski (October 2003). "HICCUPS: Hidden Communication System for Corrupted Networks". In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, pp. 31-40.
- Jonathan K. Su, Frank Hartung, Bernd Girod (1999) “Digital Watermarking of Text, Image, and Video Documents” Elsevier.
- Angela D’Angelo, Giacomo Cancelli, Mauro Barni (2008) “Watermark-based Authentication” Department of Information Engineering, University of Siena.
- Stephanie R. Betancourt (2004) “ Steganography: A New Age of Terrorism” Global Information Assurance Certification Paper, GSEC Practical Version 1.2f
- Johnson, Jajodia (1998) “Steganalysis: The Investigation of Hidden Information”, Proceedings of IEEE Information Technology Conference, Syracuse, New York, USA.
- http://www.mathworks.com/matlabcentral/fileexchange/41326-steganography-using-lsb-substitution
- http://www.mathworks.com/matlabcentral/fileexchange/45052-color-image-dwt-svd-watermarking
- http://prr.hec.gov.pk/Chapters/718S-3.pdf
- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.8680&rep=rep1&type=pdf
- http://stegano.net/tutorial/steg-history.html
- http://www.snipview.com/q/Steganalysis
- http://www.lib.utexas.edu/engin/trademark/timeline/ren/watermarks.html
- https://www.cl.cam.ac.uk/teaching/0910/R08/work/slides-ma485-watermarking.pdf
- https://www.backbonesecurity.com/TerroristUseofSteganography.aspx
- http://www.zdnet.com/article/terrorists-and-steganography/