Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης
Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής

Πτυχιακή εργασία

# Μελέτη στεγανογραφικών τεχνικών και επίδειξη χρήσης εργαλείων για συγκάλυψη και αποκάλυψη πληροφοριών

# (Information hiding using steganography techniques and tools)

*Ασουμανάκη Άννα ΑΜ: 2403*

*Υπεύθυνος Καθηγητής : Μανιφάβας Χάρης*

Ηράκλειο – Φεβρουάριος 2015

# ΕΥΧΑΡΙΣΤΙΕΣ

Η ολοκλήρωση αυτής της πτυχιακής υλοποιήθηκε με την υποστήριξη ενός αριθμού ανθρώπων στους οποίους θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες μου. Πρώτα από όλους θα ήθελα να ευχαριστήσω τον κ. Μανιφάβα που μου έδωσε την ευκαιρία να ασχοληθώ με το θέμα που με ενδιαφέρει για την υπομονή και την υποστήριξη που μου έδειξε. Τους γονείς μου και την αδερφή μου που ήταν δίπλα μου όλο αυτό το διάστημα και όλους τους φίλους μου που πραγματικά με βοήθησαν. Ευχαριστώ!

Ασουμανάκη Άννα

# Πίνακας περιεχομένων

**Abstract** ..... 7
**ΚΕΦΑΛΑΙΟ 1** ..... 8
**Κρυπτογραφία (Cryptography)** ..... 8
1.1 Βασικές Έννοιες ..... 8
1.2 Ιστορία της Κρυπτογραφίας ..... 9
1.3 Είδη Κρυπτογραφίας ..... 10
1.4 Κρυπτανάλυση ..... 13
**ΚΕΦΑΛΑΙΟ 2** ..... 17
**Στεγανογραφία (Steganography)** ..... 17
2.1 Βασικές Έννοιες ..... 17
2.2 Ιστορική αναδρομή της Στεγανογραφία ..... 19
2.3 Τεχνικές Στεγανογραφίας ..... 20
2.4 Παράδειγμα Στεγανογραφία ..... 25
2.5 Σύγχρονη Στεγανογραφία ..... 27
2.6 Υδατογράφημα ..... 28
2.7 Πλεονεκτήματα / Μειονεκτήματα (Στεγανογραφία συγκριτικά με την Κρυπτογραφία) ..... 29
2.8 Περιγραφή των διαφόρων μορφών στις οποίες εφαρμόζεται από διάφορες οντότητες ..... 30
*2.8.1 Τύποι Αρχείων – Στεγανογραφικά Προγράμματα* ..... 31
2.9 Υβριδικά συστήματα (συνδυασμός Στεγανογραφία/ κρυπτογραφίας) ..... 32
*2.9.1 Βασική ιδέα μεθόδου:* ..... 32
2.10 Πλεονεκτήματα – Μειονεκτήματα ..... 33
**ΚΕΦΑΛΑΙΟ 3** ..... 35
**Στεγανάλυση(Steganalysis)** ..... 35
3.1 Περίληψη στεγανάλυσης ..... 35
3.2 Βασικές τεχνικές ανίχνευσης στεγανογραφίας ..... 36
3.3 Βασικές τεχνικές επίθεσης ..... 37
3.4 Η στεγανάλυση σε εικόνα ..... 37
*3.4.1 LSB* ..... 37
**ΚΕΦΑΛΑΙΟ 4** ..... 42
**Στεγανογραφικά εργαλεία (Steganography tools)** ..... 42
4.1 Στεγανογραφικά εργαλεία ..... 42
4.2 Εφαρμογές στεγανογραφίας ..... 45
*4.2.1 OpenPuff* ..... 45
*4.2.2 StegoShare* ..... 62

*4.2.3 OpenStego 0.6.1* ..... 70
**ΚΕΦΑΛΑΙΟ 5** ..... 80
**Στεγανάλυση εργαλεία (Steganalysis Tools)** ..... 80
5.1 Διάφορα εργαλεία στεγανάλυσης ..... 80
5.2 Simple-Steganalysis-Suite (SSS) ..... 80
**ΚΕΦΑΛΑΙΟ 6** ..... 101
**Συμπεράσματα** ..... 101

# Πίνακας εικόνων

Εικόνα 1 Παράδειγμα κρυπτογραφίας σε σκυτάλη ..... 9
Εικόνα 2 Παράδειγμα τεχνικής Caesar cipher ..... 10
Εικόνα 3 Απλοποιημένο μοντέλο συμμετρικής κρυπτογράφησης ..... 10
Εικόνα 4 Χάρτης κρυπτοαναλυτικών μεθόδων ..... 15
Εικόνα 5 Μοντέλο στεγανογραφίας ..... 17
Εικόνα 6 Αναπαράσταση στεγανογραφικού συστήματος ..... 22
Εικόνα 7 8 bit palette, 24 bit palette, 8bit grayscale ..... 28
Εικόνα 8 Παράδειγμα υδατογραφήματος ..... 29
Εικόνα 9 Στεγανογραφία - Κρυπτογραφία ..... 29
Εικόνα 10 Οι πιο δημοφιλείς εφαρμογές απόκρυψης πληροφορίας ..... 31
Εικόνα 11 OpenPuff ..... 45
Εικόνα 12 Bits selection level ..... 46
Εικόνα 13 Εμφάνιση παραθύρου για απόκρυψη πληροφορίας ..... 47
Εικόνα 14 Settings for Hide Data ..... 48
Εικόνα 15 Επιλογή τοποθεσίας αποθήκευσης ..... 49
Εικόνα 16 Επιτυχής διαδικασία ..... 50
Εικόνα 17 End-Report OpenPuff ..... 50
Εικόνα 18 Επιλογή αρχείου για unhide ..... 51
Εικόνα 19 Unhide ..... 52
Εικόνα 20 Επιτυχής αποκρυπτογράφηση ..... 52
Εικόνα 21 End-Report OpenPuff ..... 53
Εικόνα 22 Παράθυρο για δημιουργία Watermarking ..... 58
Εικόνα 23 Επιλογή αρχείων carrier ..... 59
Εικόνα 24 Επιτυχής διαδικασία ..... 60
Εικόνα 25 Επιλογή αρχείων για έλεγχο watermarking ..... 61
Εικόνα 26 Final report ..... 62
Εικόνα 27 StegoShare ..... 62
Εικόνα 28 Hide ..... 64
Εικόνα 29 Hide ..... 65
Εικόνα 30 OpenStego ..... 70
Εικόνα 31 Setting for Hide data ..... 71
Εικόνα 32 Extract Data ..... 72
Εικόνα 33 Extract Data Settings ..... 73
Εικόνα 34 Generate signature ..... 74
Εικόνα 35 Embed watermark ..... 75
Εικόνα 36 Verify Watermark ..... 77
Εικόνα 37 Results of the watermark strength check ..... 77
Εικόνα 38 Simple Steganalysis Suite (SSS) ..... 81
Εικόνα 39 before hide the information ..... 82
Εικόνα 40 after hide the information ..... 83
Εικόνα 41 before hide information - pixel value ..... 83
Εικόνα 42 after hide information - pixel value ..... 84
Εικόνα 43 before hide information - chi-square ..... 85
Εικόνα 44 after hide information - chi-square ..... 85

Εικόνα 45  before hide information - Neighbourhood Histogram..... 86
Εικόνα 46 after hide information - Neighbourhood Histogram ..... 86
Εικόνα 47 LSB before hide information ..... 89
Εικόνα 48 LSB After hide informationn..... 90
Εικόνα 49 Pixel Value - before hide information ..... 90
Εικόνα 50 Pixel Value after hide information ..... 91
Εικόνα 51 Chi-square before hide information..... 91
Εικόνα 52 Chi-square after hide information..... 92
Εικόνα 53 Neighbourhood Histogram before hide information..... 92
Εικόνα 54 Neighbourhood Histogram after hide information..... 93
Εικόνα 55 Pixel Difference Histogram before hide information ..... 93
Εικόνα 56 Pixel Difference Histogram after hide information ..... 94
Εικόνα 57 Matrix Average LSB after hide information ..... 95
Εικόνα 58 Chi-square after hide information..... 96
Εικόνα 59 "Neighbours" after hide information ..... 97
Εικόνα 60 Pixel Difference Histogram after hide information ..... 98
Εικόνα 61 Scales settings ..... 99

# Abstract

Nowadays, in the third decade of the birth of the Web, its users list in the billions and the need for communication, learning and entrepreneurship is still evolving rapidly. Thus the Web has the need to evolve according to the needs of humanity. During its first decade the web was static, consisting of mainly text sites with poor information search, this changed with the advent of search engines and the beginning of the era of lifelong activity, with the most dynamic web 2.0.

These days, the web consists of 980 million web pages containing all kind of information in any form. This leads to the creation of the next step in the evolution of the Web, called semantic web or web 3.0. This term was given to us from the inventor of the original World Wide Web, Tim Berners-Lee.

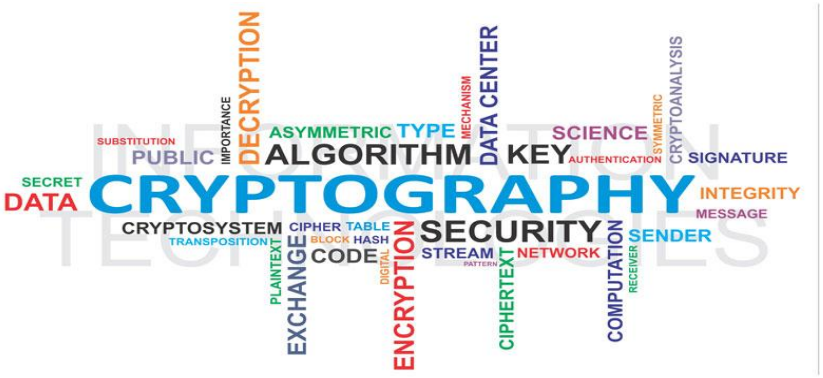
The purpose of this work is to create a time reasoner, a piece of code with the ability to draw inferences using rules written in predicate logic. The time reasoner differs from a simple reasoner, because the rules contain statements relating to time. The reasoner uses metadata from documents from the semantic web. Those documents may be of RDFS, Turtle, and OWL syntax.

*Keywords*: *Cryptography, Steganography, Steganalysis, Security*

# ΚΕΦΑΛΑΙΟ 1

## Κρυπτογραφία (Cryptography)

### 1.1 Βασικές Έννοιες




Κρυπτογραφία είναι η πρακτική και μελέτη των τεχνικών της ασφαλούς επικοινωνίας ακόμα και ανάμεσα σε τρίτους, χωρίς αυτοί να μπορούν να την παρεμβάλουν. Η λέξη κρυπτογραφία είναι σύνθετη από το πρώτο συνθετικό (*κρύπτο-*) που σημαίνει κρυφό και (*-γραφή*) που σημαίνει μελέτη. Σκοπός της κρυπτογραφίας είναι η κρυπτογράφηση μηνυμάτων (εικόνας, ήχου, βίντεο κ.α.), δηλαδή της μετατροπής της πληροφορίας από κατανοητή σε ακατανόητη που για να διαβαστεί θα πρέπει ο παραλήπτης να χρησιμοποιήσει ένα κλειδί. Στην εποχή της πληροφορίας, η επεξεργασία της πληροφορίας γίνεται με τη χρήση μαθηματικών όπως η θεωρία αριθμών, τα διακριτά μαθηματικά, η στατιστική και η συνδυαστική ανάλυση. Επίσης χρησιμοποιούνται και εργαλεία της πληροφορικής επιστήμης όπως, θεωρία πληροφορία και υπολογιστική πολυπλοκότητα.

Στην κρυπτογραφία πρέπει να ισχύουν τέσσερις βασικές λειτουργίες για να θεωρείται επιτυχημένη.

**Εμπιστευτικότητα:** Η πληροφορία που θα μεταδοθεί θα πρέπει να είναι κατανοητή μέσο στα εξουσιοδοτημένα μέλη και όχι σε τρίτους.

**Ακεραιότητα:** Η μεταδιδόμενη πληροφορία θα μπορεί αν αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη, ενώ εάν αλλοιωθεί από τρίτους θα πρέπει η αλλοίωση να είναι ανιχνεύσιμη.

**Μη απάρνηση:** Η αυθεντικότητα της δημιουργίας και της μετάδοσης της πληροφορίας θα πρέπει να είναι εγγυημένη από τον αποστολέα και τον αποδέκτη εξίσου.

**Πιστοποίηση:** Θα πρέπει ο αποστολέας και ο αποδέκτης της πληροφορίας να είναι σε θέση να εξακριβώσουν την ταυτότητα τους, την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση πως οι ταυτότητες τους είναι αυθεντικές.

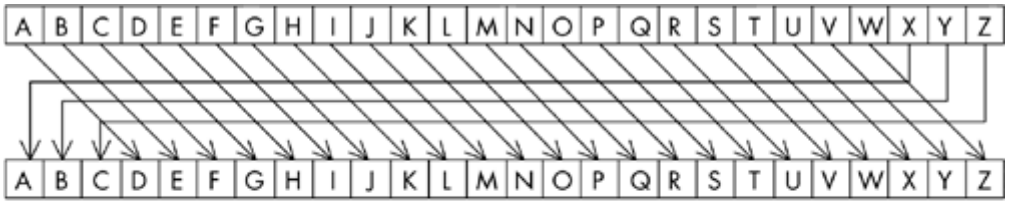
## 1.2 Ιστορία της Κρυπτογραφίας

Αρχαιότητα 1900 π.Χ. – 44 π.Χ.

Κατά την διάρκεια της αρχαιότητας η κρυπτογραφία ήταν αρκετά απλή και βασίζονταν σε αντικαταστάσεις γραμμάτων οι οποίες δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές αλλά στηρίζονταν στην ευρηματική σκέψη των δημιουργών τους.
Η τεχνική της κρυπτογραφίας ανέρχεται έως την αρχαία Αίγυπτο το 1900 π.Χ. με τη μορφή μη συμβατικών ιερογλυφικών. Γύρο στο 1500 π.Χ. συναντάμε παρόμοιες τεχνικές σε πήλινες πλάκες στη Μεσοποταμία και πολύ αργότερα στο Ισραήλ. Στην αρχαία Ελλάδα ήταν γνωστή στους Σπαρτιάτες η πρακτική της σκυτάλης.


*Εικόνα 1 Παράδειγμα κρυπτογραφίας σε σκυτάλη*

Αυτή περιλάμβανε μία σκυτάλη συγκεκριμένου μήκους, στην οποία τυλίγοταν μία λωρίδα από δέρμα ή περγαμηνή. Ο Αποστολέας έγραφε το μήνυμα κατά μήκος της σκυτάλης και έπειτα ξετύλιγε τη λωρίδα, η οποία πλέον ήταν μία σειρά από γράμματα χωρίς κανένα νόημα. Μόνο σε μία σκυτάλη ίδιας διαμέτρου το μήνυμα θα μπορούσε να διαβαστεί. Έως το 2$^{ο}$ αιώνα π.Χ. πολλές άλλες τεχνικές επινοήθηκαν από Έλληνες και Ρωμαίους όπως ο Αριστοτέλης, ο Πυθαγόρας και ο Νέρωνας. Σημαντικό ήταν το κρυπτοσύστημα του Πολύβιου στο οποίο τα γράμματα ενός απλού κειμένου αντικαθίστανται από ζεύγη συμβόλων.
Τέλος αξίζει να αναφερθεί η τεχνική του Ιούλιου Καίσαρα (*Caesar cipher*), στην οποία το κανονικό αλφάβητο μετατίθεται κατά τρία γράμματα προς τα δεξιά, με τα τρία τελευταία να αντικαθίστανται από τα τρία πρώτα.




```
Key:
  3
Plaintext:
  P = HELLO CAESAR CIPHER
Ciphertext:
  C = KHOOR FDHVDU FLSKHU
```

*Εικόνα 2 Παράδειγμα τεχνικής Caesar cipher*

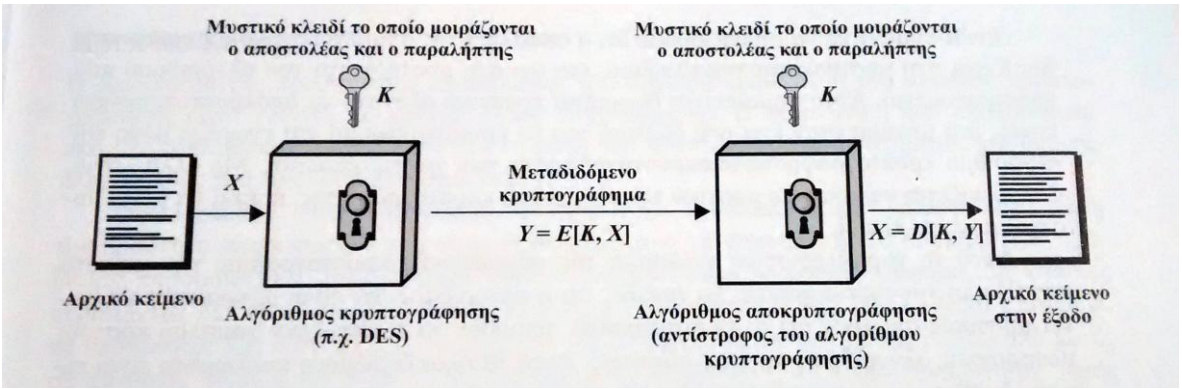
Κατά το Μεσαίωνα η τεχνικές της κρυπτογραφίας αναπτύχθηκαν ιδιαίτερα από τους Άραβες οι οποίοι είναι οι πρώτοι που τεκμηρίωσαν τις αρχές της κρυπτανάλυσης. Στην Ευρώπη και μετά την περίοδο της Αναγέννησης η κρυπτογραφία έγινε ιδιαίτερα σημαντική λόγω της θρησκευτικής επανάστασης και του πολιτικού ανταγωνισμού. Αργότερα γύρω στο 1500 μ.Χ. η κρυπτογραφία έκανε την εμφάνιση της και στην Ιαπωνία, όπου βελτιώθηκε σημαντικά πολύ αργότερα γύρο στο 1860 μ.Χ.

## 1.3 Είδη Κρυπτογραφίας

Κατά κύριο λόγο χρησιμοποιούνται δύο μορφές κρυπτογράφησης, η συμβατική ή συμμετρική κρυπτογράφηση και η κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρη κρυπτογράφηση.

### Συμμετρική κρυπτογραφία

Στην συμμετρική κρυπτογραφία η κρυπτογράφηση αλλά και η αποκρυπτογράφηση πληροφορίας γίνεται με ένα μοναδικό κλειδί, το οποίο είναι γνωστό και ως μυστικό (*secret key*) ή συμμετρικό κλειδί. Το μοναδικό αυτό κλειδί είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη.




*Εικόνα 3 Απλοποιημένο μοντέλο συμμετρικής κρυπτογράφησης*

Το παραπάνω σύστημα συμμετρικής κρυπτογραφίας έχει πέντε συστατικά:

- Είναι αρχικά το απλό κείμενο ή τα αρχικά δεδομένα (*plaintext*) που δίνονται στον αλγόριθμο ως είσοδος.
- Αλγόριθμος κρυπτογράφησης (*encryption algorithm*), ο οποίος διεξάγει διάφορες ενέργειες-αντικαταστήσεις και μετασχηματισμούς στο αρχικό κείμενο.
- Μυστικό κλειδί (*secret key*), το οποίο δίνετε μαζί με το αρχικό κείμενο σαν είσοδο στον αλγόριθμο. Με βάση το κλειδί ο αλγόριθμος διεξάγει τις αντικαταστήσεις και τους μετασχηματισμούς.
- Το μετασχηματισμένο κείμενο που παράγεται ως έξοδος λέγεται κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (*ciphertext*) και εξαρτάται τόσο από το αρχικό κείμενο, όσο και από το μυστικό κλειδί.
- Αλγόριθμος αποκρυπτογράφησης, ο οποίος είναι ο ίδιος αλγόριθμος αλλά σε αντίστροφη εκτέλεση. Δηλαδή, δέχεται σαν είσοδο το μυστικό κλειδί και το μήνυμα το οποίο έχει κρυπτογραφηθεί με το ίδιο κλειδί που κρυπτογραφήθηκε. Το αποτέλεσμα είναι το αρχικό κείμενο.

Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα που θέλει να στείλει, το ίδιο κλειδί χρησιμοποιεί και ο παραλήπτης για να το αποκρυπτογραφήσει.

Φυσικά για να είναι ασφαλής η χρήση της συμμετρικής κρυπτογραφίας θα πρέπει να ισχύουν δύο απαιτήσεις:

1. Θα πρέπει ο αλγόριθμος κρυπτογράφησης να είναι ισχυρός ώστε ένας αντίπαλος που του είναι γνωστός και έχει πρόσβαση σε κρυπτογραφημένα μηνύματα, να μη μπορεί να καταλάβει το μυστικό κλειδί και τελικά ποιο είναι το αρχικό μήνυμα.

2. Η δεύτερη απαίτηση που εξαρτάται από τους χρήστες, είναι η ανταλλαγή του μυστικού κλειδιού. Αν ο αντίπαλος καταφέρεις και κλέψει το μυστικό κλειδί, τότε η επικοινωνία δεν είναι ασφαλής. Να σημειώσουμε ότι η ασφάλεια της συμμετρικής κρυπτογραφίας, δεν βασίζεται στην μυστικότητα του αλγορίθμου αλλά στη μυστικότητα του κλειδιού. Κάποιος ο οποίος δεν έχει το μυστικό κλειδί, θεωρείται αδύνατον να μπορέσει να αποκρυπτογραφήσει ένα κρυπτογράφημα.

Η συμμετρική κρυπτογραφία έχει αρκετά πλεονεκτήματα, μερικά από αυτά είναι: οι υψηλές ταχύτητες κρυπτογράφησης και αποκρυπτογράφησης που πολλές φορές υπερβαίνουν τα 100Mbps.

Επίσης έχει μικρές απαιτήσεις σε μνήμη και υπολογιστική ισχύ. Έχει όμως και αρκετά μειονεκτήματα και το μεγαλύτερο της μειονέκτημα είναι συνεννόηση και ανταλλαγή του κλειδιού.

Μέσα από το Διαδίκτυο δεν είναι ασφαλής η μετάδοση του κλειδιού, γιατί όποιος γνωρίζει για την συναλλαγή και έχει τα κατάλληλα εργαλεία, μπορεί να καταγράψει όλη την επικοινωνία και εφόσον έχει την συνομιλία μπορεί να τροποποιήσει και να πλαστογραφήσει τα μηνύματα που έχουν σταλεί. Φυσικά υπάρχει και η επιλογή άλλου μέσου επικοινωνίας, όπως είναι η τηλεφωνία, αλλά ακόμα και μέσο αυτή της επιλογής δεν υπάρχει εγγύηση ότι δεν παρεμβάλλεται κάποιος τρίτος μεταξύ της γραμμής επικοινωνίας των χρηστών.

Ένα κρυπτογραφικό σύστημα θεωρείται υπολογιστικά ασφαλές, αν το κρυπτογράφημα το οποίο δημιουργεί ικανοποιεί ένα ή περισσότερα από τα παρακάτω κριτήρια:

- Εάν το χρηματικό κόστος για την παραβίαση του κρυπτογραφήματος υπερβαίνει την αξία των κρυπτογραφημένων πληροφοριών.
- Και αν ο χρόνος που απαιτείται για την αποκάλυψη των πληροφοριών υπερβαίνει την ωφέλιμη διάρκεια ζωής των πληροφοριών

Όσο μεγαλύτερη είναι η δυσκολία του υπολογισμού του κλειδιού τόσο πιο επιτυχής είναι η κρυπτογράφηση.

## Ασύμμετρη κρυπτογραφία

Ενώ η συμμετρική κρυπτογραφία βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, η ασύμμετρη κρυπτογραφία ή αλλιώς κρυπτογραφία δημόσιου κλειδιού βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών. Το ένα κλειδί από τα δύο ονομάζεται δημόσιο κλειδί (*public key*), δηλαδή μπορεί να είναι δημόσια γνωστό και διαθέσιμο, το κλειδί αυτό χρησιμοποιείται για την κρυπτογράφηση. Το άλλο κλειδί παραμένει μυστικό.

Τα δύο κλειδιά σχετίζονται μεταξύ τους (με μαθηματική σχέση), δηλαδή τυπικά ένα τέτοιο σύστημα μπορεί να καταρρεύσει, όμως τα δύο αυτά κλειδιά είναι επαρκώς διαφορετικά ώστε αν κάποιος που έχει στη κατοχή του το ένα (το δημόσιο) να μη μπορεί να υπολογίσει το άλλο, συνήθως απαιτεί την παραγοντοποιήσει ενός μεγάλου αριθμού. Ένας πολύ σημαντικός λόγος που χρησιμοποιείται η ασύμμετρη κρυπτογραφία αφορά την πιστοποίηση της αυθεντικότητας.

Η πιστοποίηση της αυθεντικότητας αποτελεί μια σημαντική λειτουργία ασφάλειας δικτύου. Ένα μήνυμα, αρχείο ή έγγραφο θεωρούνται αυθεντικά όταν είναι γνήσια και προέρχονται όντως από την προέλευση που δηλώνουν. Τα λαμβανόμενα μηνύματα γνωρίζουμε ότι είναι αυθεντικά εφόσον έχουν ακολουθήσει την διαδικασία αυθεντικότητας. Είναι πολύ σημαντικό να γνωρίζουμε ότι τα περιεχόμενα του μηνύματος δεν έχουν μεταβληθεί και ότι η προέλευση είναι η αυθεντική.

### Πιστοποίηση αυθεντικότητας με χρήση συμβατικής κρυπτογράφησης

Στην περίπτωση αυτή μπορούμε να σκεφτούμε ότι ο αποστολέας και ο παραλήπτη είναι οι μόνοι που γνωρίζουν την ύπαρξη του κλειδιού (όπως και πρέπει να είναι), τότε μόνο ο αυθεντικός παραλήπτης μπορεί να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα που έλαβε από τον αυθεντικό αποστολέα. Επιπλέον, αν το μήνυμα έχει error- detection code, κώδικα ανίχνευσης σφαλμάτων και αριθμό ακολουθίας, sequence number, ο παραλήπτης βεβαιώνεται ότι το μήνυμα δεν έχει υποστεί τροποποίηση, υπάρχει και η περίπτωση να έχει χρονοσήμανση (timestamp), τότε θα είναι σίγουρο ότι δεν έχει καθυστερήσει περισσότερο από όσο θα ήταν φυσιολογικό για μια μετάδοση μέσω δικτύου.

### Πιστοποίηση αυθεντικότητας μηνυμάτων χωρίς κρυπτογράφηση

Στην περίπτωση αυτή το μήνυμα δεν κρυπτογραφείται, όμως υπάρχουν ετικέτες πιστοποίησης αυθεντικότητας και προσαρμόζονται σε κάθε μήνυμα που στέλνεται. Γίνεται καθημερινά η χρήση συμβατικής κρυπτογραφίας, όπου γίνεται η πιστοποίηση αυθεντικότητας χωρίς την εξασφάλιση απορρήτου. Για παράδειγμα, η ειδοποίηση προς τους χρήστες ότι το δίκτυο δεν είναι διαθέσιμο αυτή τη στιγμή, ή ένα σήμα συναγερμού προς κάποιο κέντρο έλεγχου. Είναι πιο οικονομικό και αξιόπιστο να υπάρχει μόνο ένας προορισμός που είναι υπεύθυνος για την παρακολούθηση της πιστοποίησης αυθεντικότητας.

Η ασύμμετρη κρυπτογραφία χρησιμοποιείται και για την παραγωγή ψηφιακών υπογραφών και αυτό τις δίνει πλήθος από πλεονεκτήματα. Τα ασύμμετρα κρυπτοσυστήματα μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν αποκηρυχθούν από την πηγή τους. Άλλο πλεονέκτημα είναι ότι τα κλειδιά δεν χρειάζεται να μεταδοθούν στο Διαδίκτυο.

## 1.4 Κρυπτανάλυση

Κρυπτανάλυση (*cryptanalysis*) είναι η προσπάθεια ανακάλυψης του κλειδιού κρυπτογράφησης και στη συνέχεια του αρχικού κειμένου. Αποτελεί τον κλάδο της κρυπτογραφίας, ο οποίος ως κύριο αντικείμενο της μελέτης του έχει την ανεύρεση προβλημάτων στους κρυπτογραφικούς αλγορίθμους που χρησιμοποιούνται. Όσο αφορά στις περιπτώσεις των ψηφιακών υπογραφών, ο εχθρός θα προσπαθήσει να πλαστογραφήσει την ψηφιακή υπογραφή κάποιου άλλου ή ακόμα και να αλλοιώσει ήδη ψηφιακά υπογεγραμμένα έγγραφα.

Στον παρακάτω πίνακα συνοψίζονται οι διάφοροι τύποι κρυπταναλυτικών επιθέσεων, η ταξινόμηση γίνεται βάσης της ποσότητας πληροφοριών που μπορεί να είναι γνωστές στον εχθρό.

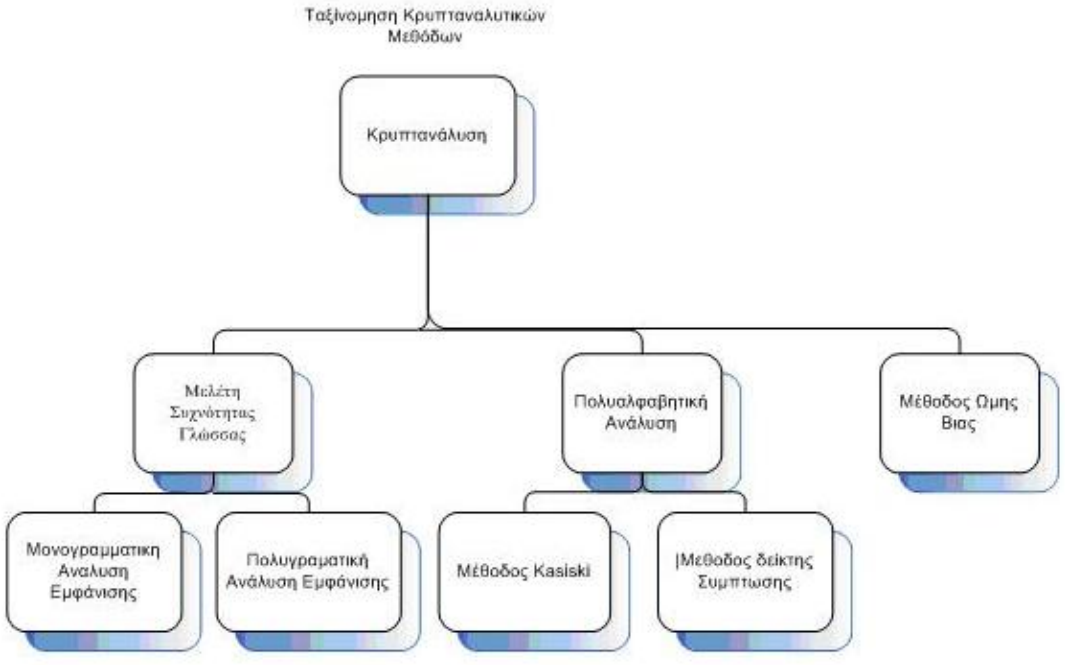
| **Τύπος επίθεσης** | **Στοιχεία γνωστά στον κρυπταναλυτή** |
|---|---|
| Κρυπτογραφήματος | • Αλγόριθμος κρυπτογράφησης<br>• Το κρυπτογράφημα που πρέπει να αποκωδικοποιηθεί |
| Γνωστού αρχικού κειμένου | • Ένα ή περισσότερα ζεύγη αρχικού κειμένου-κρυπτογραφήματος παραγόμενα από το ίδιο μυστικό κλειδί<br>• Αλγόριθμος κρυπτογράφησης<br>• Το κρυπτογράφημα που πρέπει να αποκωδικοποιηθεί |
| Επιλεγμένου αρχικού κειμένου | • Αρχικό κείμενο, επιλεγμένο από τον κρυπταναλυτή, μαζί με το αντίστοιχο κρυπτογραφημένο κείμενο που προκύπτει από το μυστικό κλειδί.<br>• Αλγόριθμος κρυπτογράφησης<br>• Το κρυπτογράφημα που πρέπει να αποκωδικοποιηθεί |
| Επιλεγμένου κρυπτογραφήματος | • Εμφανιζόμενο και επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο κείμενο που προκύπτει από το μυστικό κλειδί.<br>• Αλγόριθμος κρυπτογράφησης<br>• Το κρυπτογράφημα που πρέπει να αποκωδικοποιηθεί |

| | |
|---|---|
| Επιλεγμένο κείμενο | • Αλγόριθμος κρυπτογράφησης<br>• Το κρυπτογράφημα που πρέπει να αποκωδικοποιηθεί<br>• Αρχικό κείμενο, επιλεγμένο από τον κρυπταναλυτή, μαζί με το αντίστοιχο κρυπτογραφημένο κείμενο που προκύπτει από το μυστικό κλειδί.<br>• Εμφανιζόμενο και επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο κείμενο που προκύπτει από το μυστικό κλειδί. |

Πίνακας 1Τύποι επιθέσεων σε κρυπτογραφημένα μηνύματα

Κρυπτανάλυση κλασικών κρυπτοσυστημάτων - Λίγα λόγια

Όσον αφορά τα κλασικά κρυπτοσυστήματα υπάρχουν διάφοροι τύποι κρυπταναλυτικών επιθέσεων. Οι περισσότερες βασίστηκαν πάνω στην γλωσσική δομή του μηνύματος. Στις νεότερες μορφές Κρυπτανάλυσης Κλασικών Κρυπτοσυστημάτων παρατηρείται η είσοδος της στατιστικής στην ανάλυση.




*Εικόνα 4 Χάρτης κρυπτοαναλυτικών μεθόδων*

**Μέθοδος ωμής βίας:** Η επίθεση ωμής βίας (*brute-force attack*) αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Συχνά ο επιτιθέμενος ξεκινά την επίθεση χρησιμοποιώντας τα πιο "πιθανά", κατά την άποψή του κλειδιά, προσπαθώντας με αυτό τον τρόπο να βρει το κλειδί πιο γρήγορα. Πρακτικά, η αναζήτηση σταματά μόλις βρεθεί το κλειδί, χωρίς να χρειαστεί περαιτέρω ενημέρωση της λίστας κλειδιών.

**Ανάλυση συχνότητας γλώσσας:** περιγράφεται η μελέτη της συχνότητας των γραμμάτων (ή ομάδας γραμμάτων) σε ένα κρυπτογραφημένο κείμενο. Όταν το πρωτότυπο κείμενο έχει κρυπτογραφηθεί με κάποια μέθοδο μονοαλφαβητικής αντικατάστασης, με τον μονοαλφαβητική αντικατάσταση εννοούμε ότι κάθε γράμμα του πρωτότυπου αντικαθιστάται μόνο με έναν άλλο χαρακτήρα.
Μελετώντας το κρυπτογραφημένο κείμενο ο κρυπταναλυτής προσπαθεί να βγάλει κάποια συμπεράσματα με βάση την συχνότητα που εμφανίζονται οι ίδιοι χαρακτήρες.
Εκτός από την μονοαλφαβητική αντικατάσταση υπάρχει η κρυπτογραφία πολυαλφαβητικών αντικαταστάσεων, όπου κάθε γράμμα του πρωτότυπου κειμένου μπορεί να αντικατασταθεί με περισσότερους από ένα χαρακτήρες.

**Κρυπτανάλυση Πολυαλφαβητικής Ανάλυση:**

Μέθοδος Kasiski : είναι μία μέθοδος για την διάσπαση πολυαλφαβητικών κρυπτοσυστημάτων. Η βασική ιδέα είναι η ίδια με αυτή της μεθόδου μονοαλφαβητικής αντικατάστασης, η μόνη διαφορά εδώ είναι ότι δεν μιλάμε για μεμονωμένα γράμματα αλλά για λέξεις, δηλαδή ο κρυπταναλυτής ελέγχει το κρυπτογράφημα για επαναλαμβανόμενες λέξεις.
Ο δείκτης σύμπτωσης (index of coincidence) : εκφράζει την πιθανότητα δύο τυχαίοι χαρακτήρες ενός κειμένου να ταυτίζονται.

# ΚΕΦΑΛΑΙΟ 2

## Στεγανογραφία (Steganography)

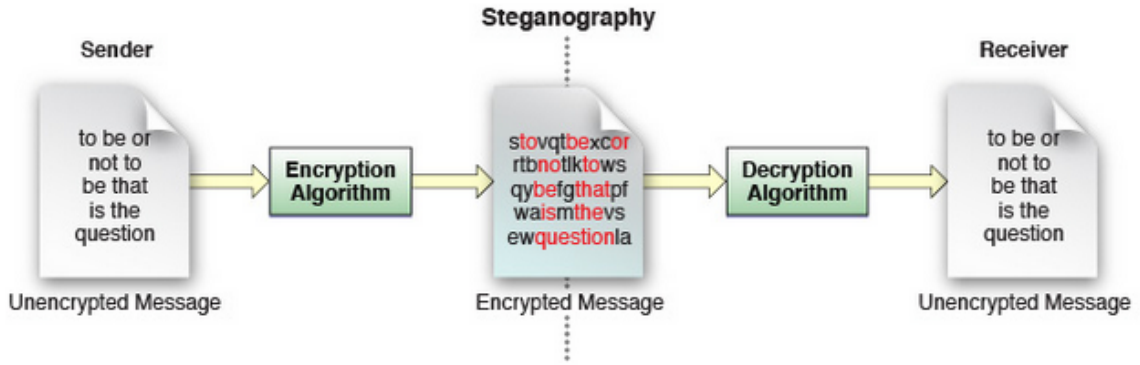
### 2.1 Βασικές Έννοιες

**Ανάλυση λέξης:**

Η λέξη στεγανογραφία προέρχεται από δύο συστατικά της Ελληνικής γλώσσας. Η πρώτη λέξη είναι «στεγανό» και η δεύτερη «γραφή», η λέξη στεγανό σημαίνει "καλυμμένο" ή κρυμμένο και η λέξη γραφή σημαίνει κείμενο, τέχνη, ζωγραφιά.

**Ορισμός:**

Αντίθετα με την κρυπτογράφηση που ο εχθρός μπορεί να ανιχνεύσει και να αιχμαλωτίσει την πληροφορία, η στεγανογραφία είναι η τέχνη του να κρύβεις την επικοινωνία με τέτοιο τρόπο ώστε να μην αντιλαμβάνεται ο εχθρός την ύπαρξη της. Είναι αρχαία τέχνη που έχει διαδοθεί και αναπτυχθεί με την εμφάνιση του διαδίκτυο και γενικά από τα ψηφιακά μέσα.




*Εικόνα 5 Μοντέλο στεγανογραφίας*

Η επικοινωνία γίνετε μέσω "αθώας" πληροφορίας και δεν αφήνει περιθώρια ανίχνευσης της. Αν τοποθετήσουμε την " Αρχή του Kerckhoff " στην στεγανογραφία: "Η ασφάλεια ενός συστήματος πρέπει να βασίζεται στο δεδομένο ότι ο εχθρός έχει πλήρη γνώση των σχεδιαστικών λεπτομερειών και της υλοποίησης ενός στεγανογραφικού συστήματος". Μετέπειτα η μόνη πληροφορία που δεν πρέπει να είναι γνωστή στον εχθρό είναι το μυστικό κλειδί, που ένας τυχαίος αριθμός.

Η στεγανογραφία και το πρόβλημα των "κρυμμένων καναλιών" σχετίζονται άμεσα, όσον αφορά τον σχεδιασμό ενός ασφαλούς περιβάλλοντος επικοινωνίας. Επιπλέον, σχετίζεται και με την τεχνική εκπομπής ευρέως φάσματος, όπου επιτρέπεται η λήψη μηνυμάτων, τα οποία είναι πολύ πιο δυνατά, έως και εκατό φορές, από τον ατμοσφαιρικό θόρυβο.

Οι τηλεφωνικές γραμμές και οι εκπομπές ράδιο, αλλά όπως και τα περισσότερα κανάλια επικοινωνιών, στα σήματα που εκπέμπουν υπάρχει πάντα κάποιος θόρυβος. Στα κοινά επικοινωνιακά συστήματα υπάρχει πλήθος χαρακτηριστικών αλλά μόνο ένα μικρό μέρος που φαίνεται σαν θόρυβος, έχει την δυνατότητα να αντικατασταθεί με το μυστικό σήμα που περιέχει την πληροφορία. Υπάρχει η δυνατότητα να αφαιρέσουμε αυτόν τον θόρυβο και να τοποθετήσουμε στη θέση του το μήνυμα που θέλουμε να μεταφέρουμε με την μορφή θορύβου.

Ο μηχανισμός αυτός είναι η βασική αρχή των στεγανογραφικών συστημάτων. Υπάρχουν πολλά προγράμματα που υλοποιούν στεγανογραφικούς μηχανισμούς. Η βασική σχεδιαστική αρχή είναι: η τοποθέτηση εκπομπής υψηλής εντροπίας στη θέση του θορύβου υψηλής εντροπίας. Η στεγανογραφία είναι δύσκολη υπόθεση για αυτό και είναι δύσκολος ο εντοπισμός της. Υπάρχουν βέβαια οι περιπτώσεις που εντοπίζεται, αλλά μόνο όταν πρόκειται για απλή εφαρμογή της. Για να θεωρηθεί ένα στεγανογραφικό σύστημα καλό, θα πρέπει να παρακολουθεί το κανάλι και να ιδρύει το μοντέλου θορύβου που θα χρησιμοποιήσει με βάση τον θόρυβο του καναλιού και στη συνέχεια να προσαρμόσει τις παραμέτρους των δικών αλγορίθμων. Το πόσο ασφαλές είναι ένα στεγανογραφικό σύστημα, εξαρτάται από τους μηχανισμούς ανάλυσης του θορύβου που κατέχει ο εχθρός.

Η λογική που ακολουθεί η στεγανογραφία, ονομαζόμενη "plausible deniability" που βασίζεται στην άρνηση, δηλαδή ότι κάποιος δεν θα σκεφτεί να ψάξει για κάτι που δεν γνωρίζει την ύπαρξη του. Επίσης, δεν έχει κάποιος την απαιτούμενη υπολογιστική ισχύ, ώστε να μπορέσει να ελέγξει όλα τα δεδομένα που διακινούνται στο διαδίκτυο.

Η στεγανογραφία έχει δύο κύριους άξονες κατευθύνσεων: ο πρώτος αποκαλύπτει την κρυφή πληροφορία από τυχόν "ίχνη"  που σχετίζονται με την ταυτότητα της. Παραδείγματος χάρη το πρόγραμμα Stealth εξετάζει τα μηνύματα που έχουν κρυπτογραφηθεί με PGP μηνύματα που φαίνονται άχρηστη πληροφορία. Το πρόγραμμα αυτό παράσχει κάποιου επιπέδου ασφάλεια αλλά δεν μπορεί να ανταπεξέλθει σε κάποιον έμπειρο hacker.

Ο δεύτερος άξονας αφορά την απόκρυψη πληροφορίας μέσα σε άλλη πληροφορία. Δηλαδή όσον αφορά την χρήση μιας εικόνας για μεταφορά δεδομένων, μπορούν να αφαιρεθούν τα λιγότερο σημαντικά bits μιας bitmap της εικόνας και να τοποθετηθούν μέσα τα δεδομένα. Φυσικά θα υπάρξει μια μικρή αλλοίωση με την αλλαγή των bits της εικόνας αλλά είναι τόσο μικρή που χωρίς απευθείας σύγκριση με την αρχική εικόνα, κάποιος δεν θα καταλάβει ότι υπάρχουν αλλαγές, εφόσον δεν είναι αισθητές. Ένας άλλος τύπος αρχείου που επίσης μπορούμε να χρησιμοποιήσουμε στη στεγανογραφία είναι φυσικά και τα ψηφιακά μουσικά αρχεία. Όπως με την εικόνα έτσι και με αυτά τα αρχεία μπορούμε να χρησιμοποιήσουμε τα λιγότερο σημαντικά bits του αρχείου και να τοποθετήσουμε εκεί

την πληροφορία. Ομοίως με τη χρήση εικόνας υπάρχουν αλλαγές αλλά δεν έχουμε αισθητές αλλοιώσεις στο αποτέλεσμα.

Εξαιτίας του ότι οι κυβερνήσεις δεν επιτρέπουν τη χρήση της κρυπτογράφησης από ιδιώτες, για παράδειγμα στη Ρωσία, Γαλλία αλλά και στην Αμερική λόγο πολέμου μεταξύ των κυβερνήσεων, η στεγανογραφία έχει γίνει αναπόσπαστο κομμάτι για να μπορούμε να στέλνουμε κρυπτογραφημένες πληροφορίες.

## 2.2 Ιστορική αναδρομή της Στεγανογραφία

Καθόλα την πορεία της ιστορίας παρατηρούμε ότι ο άνθρωπος ανακάλυπτε νέες μεθόδους για την επικοινωνία με άλλους ανθρώπους κρυφά από τα αδιάκριτα βλήματα. Φυσικά οι πρώτες χρήσεις της στεγανογραφίας δεν ήταν τόσο αποτελεσματικές, εφόσον η τεχνολογία προχωράει με τόσα γοργά βήματα.

Από τις πρώτες στεγανογραφικές τεχνικές είναι αυτή που έλαβε χώρα στην Αρχαία Ελλάδα, από τον Ηρόδοτο, όπου τα κείμενα τους γραφόντουσαν σε πίνακες που είχαν καλυφθεί με κερί. Η ιστορία λέει ότι ο Δημάρατος ήθελε να ενημερώσει τη Σπάρτη ότι ο Ξέρξης έχει σκοπό να διεκδικήσει την Ελλάδα, έτσι λοιπόν ξεκίνησε η αναζήτηση τρόπου μεταφοράς κρυφού μηνύματος. Το επόμενο βήμα ήταν το ξύρισμα του κεφαλιού του μεσολαβητή, γράφοντας το μήνυμα επάνω στο κεφάλι του, ώστε όταν τα μαλλιά μάκραιναν το μήνυμα δεν φαινόταν. Στη συνέχεια ήρθε η ανακάλυψη του αόρατου μελανιού, που έκρυβαν το μήνυμα μέσα σε ένα κατά τα άλλα αθώο μήνυμα. Με την εξέλιξη της τεχνολογίας, ήταν επόμενο ότι θα ανακάλυπταν νέους, εξυπνότερους τρόπους επικοινωνίας οι μεταξύ τους διαπλεκόμενοι. Με την τεχνολογία για βασικό σύμμαχο τους, ανέπτυξαν διάφορες μεθόδους, μεταξύ αυτών και η ονομαζόμενη Null Ciphers. Η χρήση της μεθόδου ήταν η γραφή ενός αθώου ή ακατανόητου μηνύματος και για παράδειγμα το κάθε δεύτερο γράμμα, κάθε λέξης να περιέχει ένα κομμάτι του κρυφού μηνύματος. Παραδείγματος χάρη:

**ΦΣΔΕ0Σ ΔΥ58ΡΕ ΦΝΔΕΣ ΗΑΙΘ ΞΝΕΔ ΥΤΞΗΥ ΛΗΘ ΛΣΠΛ8ΙΟ ΗΗΘ ΛΣΣΣ ΔΤΡ ΓΙΤΡΤ ΚΣΤΡΦ Ι1Φ Η0ΛΙ**

Αυτό το τυχαίο μήνυμα που φαίνεται ότι δεν έχει κανένα νόημα, περιέχει την κρυφή πληροφορία:

**ΣΥΝΑΝΤΗΣΗ ΣΤΙΣ 10**

Με τον καιρό αναπτύχθηκαν νέες τεχνολογίες που θα μπορούσαν να περάσουν περισσότερη πληροφορία και να είναι λιγότερο ευδιάκριτες. Οι Γερμανοί προχώρησαν με την τεχνολογία και

ανέπτυξαν τα Microdots. Τα Microdots (μικροσκοπική τεχνολογία) είναι λιλιπούτιες φωτογραφίες, στο μέγεθος μιας τελείας που περιέχουν δεδομένα.
Η πρώτη εμφάνιση αυτών των αόρατων φωτογραφιών ανακαλύφθηκαν σε έναν δακτυλογραφημένο φάκελο που μετέφερε γερμανός πράκτορας το 1941. Το μήνυμα δεν ήταν κρυμμένο, ούτε κρυπτογραφημένο, ήταν απλά τόσο μικρό ώστε να μη τραβήξει τα βλέμματα. Ο τότε γερμανός διευθυντής του FBI. J.Edgar Hoover χαρακτήρισε την τεχνολογία των Microdots ως "the enemy's masterpiece of espionage", παρόλο το μέγεθος τους, επιτρέπουν τη διαβίβαση μεγάλου όγκου δεδομένων συμπεριλαμβανομένου και διαφόρων σχεδίων και φωτογραφιών.

## 2.3 Τεχνικές Στεγανογραφίας

**Φυσικές Τεχνικές**

Στην αρχαία Ελλάδα οι άνθρωποι έγραφαν μηνύματα σε ξύλο και έπειτα το κάλυπταν με κερί ώστε να το αποκρύψουν. Στη συνέχεια έγραφαν ένα διαφορετικό μη σχετικό μήνυμα πάνω στο κερί, ώστε να μην κινήσει υποψίες.
Μία άλλη τεχνική ήταν η γραφή μηνυμάτων στο σώμα –συνήθως στο κεφάλι- κάποιου σκλάβου. Αρχικά ξύριζαν το κεφάλι του σκλάβου, έπειτα έγραφαν το μήνυμα με μορφή τατουάζ και περίμενα ώσπου να μεγαλώσουν τα μαλλιά του. Έπειτα τον έστελναν στον παραλήπτη με κάποιο δώρο ή ασήμαντο μήνυμα ώστε να μην τον υποψιαστεί κανείς άλλος. Ο Ηρόδοτος περιγράφει ένα τέτοιο εγχείρημα που μάλιστα φάνηκε ιδιαίτερα χρήσιμο επειδή χάρη στον σκλάβο Ηστίετο οι Έλληνες πήραν προειδοποίηση για επικείμενη εισβολή Περσών. Η συγκεκριμένη μέθοδος φυσικά έχει πολλά μειονεκτήματα, όπως το γεγονός πως ο σκλάβος ίσως επιχειρήσει να ξεφύγει και το μήνυμα δεν παραδοθεί ποτέ έως τη χρονική καθυστέρηση έως ότου τα μαλλιά του μακρύνουν για να καλύψουν το μήνυμα επαρκώς.

Άλλο ένα παράδειγμα από τα πρώτα χρόνια της τυπογραφίας είναι ένα μήνυμα να κρυφτεί με τη χρήση διαφορετικών γραμματοσειρών, λόγω των ήδη αυξημένων λαθών που υπήρχαν στα κείμενα ήταν δύσκολο να παρατηρηθεί.
Άλλα παραδείγματα φυσικής στεγανογραφίας περιλαμβάνουν αόρατο μελάνι, χυμό λεμονιού και κώδικα μορς (Morse code) πλεγμένο προσεκτικά σε ρούχα. Φυσικά έχουν εφαρμοστεί και δεκάδες άλλες τεχνικές κυρίως κατά τη διάρκεια του δευτέρου παγκοσμίου πολέμου αλλά και ως το τέλος του ψυχρού πολέμου.

**Ψηφιακές τεχνικές**

Με την εξέλιξη των ηλεκτρονικών υπολογιστών νέες δυνατότητες για στεγανογραφικές τεχνικές αποκαλύφθηκαν. Για παράδειγμα είναι δυνατό να αποκρύβουμε ένα μήνυμα στα bits ενός αρχείου εικόνας που παρουσιάζει έντονο θόρυβο. Μια άλλη τεχνική είναι η επικάλυψη δεδομένων. Αυτό γίνεται αφού κρυπτογραφήσουμε τα δεδομένα μας, τα εισάγουμε σε ένα μεγαλύτερο block δεδομένων που περιέχει ένα χαμηλής σημασίας μήνυμα. Με αυτό τον τρόπο είναι αδύνατο να διαβαστεί το μήνυμα εάν ο παραλήπτης δεν έχει το σωστό κλειδί. Μια άλλη πολύ σημαντική τεχνική που αναπτύχθηκε από τον Ron Rivest είναι το Chaffing and winnowing και δίνει στον αποστολέα τη δυνατότητα να αρνηθεί το encryption του μηνύματος. Αυτό γίνεται επειδή ο αποστολέας στέλνει το μήνυμα μη κρυπτογραφημένο, σαν απλό κείμενο. Προϋπόθεση είναι αποστολέας και παραλήπτης να μοιράζονται ένα μυστικό κλειδί για την πιστοποίηση του μηνύματος.
Κρυφά μηνύματα μπορούν α περιέχονται και μέσα σε εκτελέσιμα αρχεία (.exe), εκμεταλλευόμενα τον πλεονασμό στο σετ εντολών (instruction set) του στόχου-παραλήπτη.
Άλλη μια τεχνική είναι η εμφάνιση φωτογραφιών στη ροή ενός βίντεο πχ μόνο όταν το playback γίνεται σε συγκεκριμένη ταχύτητα.

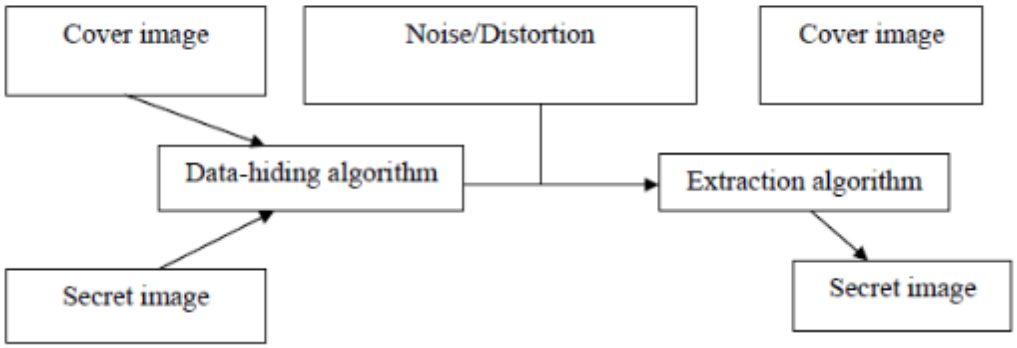
**Ψηφιακό κείμενο**

Μια απλή τεχνική είναι η μετατροπή του χρώματος της γραμματοσειράς στο ίδιο χρώμα με το φόντο ενός αρχείου, ή e-mail ή ακόμα και ενός forum-post.
Επίσης είναι δυνατή η χρήση χαρακτήρων Unicode ίδιων οπτικά με τους αντίστοιχους ASCII αλλά που στην πραγματικότητα περιγράφουν το κρυφό μήνυμα.
Κάτι παρόμοιο μπορεί να εφαρμοστεί με το πρωτόκολλο HTML όπου η χρήση περιττών πρακτικά tags ή κρυφών χαρακτήρων μπορεί να αποκρύψει ένα μήνυμα. Μια πολύ ενδιαφέρουσα περίπτωση είναι η χρήση μη-εκτυπώσιμων Unicode χαρακτήρων όπως οι Zero-Width Joiner(ZWJ) και Zero-Width Non-Joiner (ZWNJ). Οι χαρακτήρες αυτοί ενώνουν και χωρίζουν αραβικούς χαρακτήρες σχηματίζοντας ιδεογράμματα, αλλά σε ένα δυτικό αλφάβητο είναι μη-εκτυπώσιμοι και περιέχουν τιμή 0 ή 1.

**Σύγχρονες τεχνικές στεγανογραφίας σε εικόνα**

Υπάρχουν πολλές μέθοδοι που χρησιμοποιούνται για την απόκρυψη πληροφοριών μέσα σε πολυμεσικούς «ξενιστές» όπως είναι το κείμενο, η εικόνα ή το βίντεο, χωρίς να προκαλούν υποψίες για το περιεχόμενο τους. Οι ξενιστές ονομάζονται αντικείμενα κάλυψης (*cover objects*) σύμφωνα με την ορολογία του τομέα της στεγανογραφίας Οι τεχνικές αυτές μπορούν να χρησιμοποιηθούν σε διαφορετικούς τύπους αρχείων εικόνας.

Στην εικόνα που ακολουθεί, εμφανίζεται ένα βασικό σύστημα απόκρυψης πληροφοριών, στο οποίο φαίνεται ότι η είσοδος είναι μια εικόνα κάλυψης και η μυστική εικόνα, η έξοδος που παράγεται είναι μια στεγο-εικόνα (*stego image*), η οποία φαίνεται να είναι η ίδια εικόνα με την εικόνα κάλυψης στην είσοδο, παρ' όλο που περιέχει ενσωματωμένα τα δεδομένα που εμείς θέλουμε να κρύψουμε. Έπειτα ο παραλήπτης που θα λάβει την εικόνα, για να μπορέσει να ανακτήσει την αρχική εικόνα, θα πρέπει να πραγματοποιήσει την διαδικασία εξαγωγής.




*Εικόνα 6 Αναπαράσταση στεγανογραφικού συστήματος*

Παρακάτω θα δούμε τις τρείς διαφορετικές τεχνικές που υπάρχουν που χρησιμοποιούνται έτσι ώστε να κρύψουμε μια πληροφορία μέσα σε ένα αντικείμενο κάλυψης για παράδειγμα σε μια εικόνα.

- **Αντικατάσταση – τροποποίηση της LSB**

Η αντικατάσταση γίνεται στα byte του αρχείου που δεν είναι πραγματικά αναγκαία ή είναι λιγότερο σημαντικά. Η αλλαγή αυτών των bits της εικόνας, προκαλεί αλλοίωση στην εικόνα, αλλά δεν είναι τόσο εμφανής. Χωρίς απευθείας σύγκριση της τελικής με την αρχική είναι δύσκολο κάποιος να καταλάβει ότι κάτι άλλαξε. Το μέγεθος του αρχείου δεν επηρεάζεται εφόσον δεν προσθέτουμε κάτι έξτρα, αλλά ανάλογα με τον όγκο των δεδομένων που επιθυμούμε να κρύψουμε, το αρχείο θα έχει μικρές ή μεγάλες και αισθητές αλλοιώσεις.

Η μέθοδος LSB λειτουργεί καλύτερα σε αρχεία εικόνας που έχουν υψηλή ανάλυση και κάνουν χρήση πολλών διαφορετικών χρωμάτων, καθώς και με αρχεία ήχου που έχουν πολλούς διαφορετικούς ήχους και υψηλό ρυθμό μετάδοσης bit.

Στην περίπτωση που ο μέσο απόκρυψης είναι μια 24bit εικόνα, θα έχει 8 bit, που αντιπροσωπεύουν κάθε μία από τις τρεις – τιμές χρωμάτων (κόκκινο, πράσινο και μπλε) σε κάθε pixel, δηλαδή είναι δυνατόν να γίνεται απόκρυψη 3 bits μηνύματος.
Εάν εξετάσουμε το μπλε χρώμα, θα καταλήξουμε σε 28 διαφορετικές τιμές. Η διαφορά μεταξύ 11111111 και 11111110 στην ένταση του χρώματος δεν είναι αισθητή. Μια εικόνα 800X600 pixel μπορεί να περιέχει 1.440.000 bits ή 180.000 στενογραφημένα bytes με μυστικά δεδομένα.

Ας υποθέσουμε ότι έχουμε το ακόλουθο πλέγμα. Θεωρούμε ότι έχουμε 3 εικονοστοιχεία (9 bytes μνήμης) μιας εικόνας 24bit με την ακόλουθη κωδικοποίηση:

R G B
1$^{o}$ Pixel (00100111 11101001 11001000)
2$^{o}$ Pixel (00100111 11001000 11101001)
3 $^{o}$ Pixel (11001000 00100111 11101001)

Όταν ο χαρακτήρας 1, η οποία δυαδική τιμή ισούται με 10000001, προστίθεται το ακόλουθο πλέγμα το αποτέλεσμα είναι:

R G B
1$^{o}$ Pixel (00100111 11101000 11001000)
2$^{o}$ Pixel (00100110 11001000 11101000)
3$^{o}$ Pixel (11001000 00100111 11101001)

Σε αυτήν την περίπτωση έπρεπε να γίνει αλλαγή μόνο σε αυτά τα τρία bits, για να προστεθεί ο χαρακτήρας με επιτυχία.

Σε ένα άλλο παράδειγμα, έχουμε το ακόλουθο πλέγμα:

R G B
1$^{o}$ Pixel (00101101 00011100 11011100)
2$^{o}$ Pixel (10100110 11000100 00001100)
3 $^{o}$ Pixel (11010010 10101101 01100011)

Όταν εισαχθεί ο χαρακτήρας 200, όπου η δυαδική αναπαράσταση στο πλέγμα έχουμε το εξής αποτέλεσμα:

R G B

1$^{ο}$ Pixel (00101101 00011110***1*** 11011100)

2$^{ο}$ Pixel (10100110 11000010***1*** 00001100)

3$^{ο}$ Pixel (11010010 10101100 01100011)

Κατά το μέσο όρο, αν τροποποιηθεί το ήμισυ των bits για την απόκρυψη της πληροφορίας είναι αρκετό για να κρύψουμε μικρό όγκο πληροφοριών, φυσικά υπάρχει η δυνατότητα να κρύψουμε περισσότερο όγκο αντικαθιστώντας περισσότερα από ένα bit (2 ή 3) από κάθε χρώμα και οι επιδράσεις να μην μπορούν πάλι να γίνουν αντιληπτές.

Εκτός από την αλλοίωση που θα προκαλέσει στην εικόνα, μικρή αλλά υπάρχει η δυνατότητα να γίνει αντιληπτή με την σύγκριση της αρχικής και τις τελικής, υπάρχει και ένα δεύτερο μειονέκτημα, είναι ότι μας περιορίζει το ποσό δεδομένων που μπορούμε να κρύψουμε στον αριθμό των λιγότερο σημαντικών bits του αρχείου.

- **Μέθοδος LBP (Local Binary Pattern)**

Η μέθοδος ανάλυσης υφής αναπτύχθηκε για την μελέτη των διαβαθμίσεων του γκρι μιας εικόνας. Ο LBP είναι πολύ αποδοτικός και απλοϊκός, χρησιμοποιείται για την κατηγοριοποίηση υφής και με την χρήση της στεγανογραφίας γίνετε η εισαγωγή του μηνύματος. Αναφέρθηκε για πρώτη φορά από τον Harwood και στη συνέχεια έγινε επίσημη ως ταξινομητής υφής από τον Ojala το 1996. Ανταποκρίνεται τέλεια σε μεθόδους αναγνώρισης προτύπων στο ανθρώπινο οπτικό σύστημα.

Στις περισσότερες εικόνες, στις διαβαθμίσεις του χρώματος γκρι περιέχεται κάποιο είδος θορύβου, ο μέθοδος αυτή αντικαθιστά το θόρυβο με την πληροφορία που θέλουμε να κρύψουμε. Ο LBP ταξινομητής ορίζεται ως ένα σύγκρισης υφής που αφήνει αναλλοίωτες τις αποχρώσεις του γκρι και οι οποίες προέρχονται από την εξέταση της υφής σε μία «τοπική» γειτονιά. Η λειτουργία είναι η εξής: χρησιμοποιεί τα pixel ανά ομάδα, αποτελούμενη από 8 γειτονικά pixel και χρησιμοποιώντας την τιμή του κεντρικού pixel ως κατώφλι. Ακολουθεί η διαδικασία για να υπολογίσουμε την τιμή του. Πολλαπλασιάζοντας την τιμή του κατωφλίου (threshold) με τα βάρη που δίνονται για κάθε pixel και προσθέτοντας τα αποτελέσματα.

## 2.4 Παράδειγμα Στεγανογραφία

Ένα παράδειγμα είναι το παρακάτω, η επικοινωνία μεταξύ δύο ατόμων με πάθος στην αστρολογία. Το παρακάτω γράμμα που στέλνετε από την Alice στον φίλο της Bob, με την πρώτη ματιά φαίνεται να είναι ένα αθώο κείμενο, μια απλή συζήτηση ανάμεσα σε δύο λάτρεις της αστρονομίας. Η Alice αναφέρεται στο καινούργιο τηλεσκόπιο που αγόρασε.

My friend Bob,

until yesterday I was using binoculars for stargazing. Today, I decided to try my new telescope. The galaxies in Leo and Ursa Major were unbelievable! Next, I plan to check out some nebulas and then prepare to take a few snapshots of the new comet. Although I am satisfied with the telescope, I think I need to purchase light pollution filters to block the xenon lights from a nearby highway to improve the quality of my pictures.

Cheers,

Alice

Αυτό που δεν θα καταλάβει κάποιος τρίτος είναι ότι το γράμμα που έστειλε η Alice στον Bob, κρύβει ένα κρυφό μήνυμα. Η συζήτηση γίνεται ανάμεσα σε δύο κατασκόπους, όπου ο Bob είναι ο ανώτερος της και περιμένει σημαντικά νέα και φυσικά θέλουν να αποφύγουν τα αδιάκριτα βλέμματα, οπότε αποφασίζουν να χρησιμοποιήσουν στεγανογραφία από την αρχή.
Από την στιγμή που ο Bob λάβει το μήνυμα αντιλαμβάνεται αμέσως ότι η Alice του μεταφέρει τις πληροφορίες κρυμμένες με τη χρήση στεγανογραφίας. Στη συνεχεία, θα ακολουθήσει το πρωτόκολλο που έχουν προσυμφωνήσει. Από το e-mail της Alice καταγράφει όλα τα αρχικά γράμματα κάθε λέξης, το αποτέλεσμα είναι η ακόλουθη σειρά γραμμάτων:

*mfbuyiwubfstidttmnttgilaumwunitptcosnatpttafsotncaiaswttitintplpftbtxlfanhtitqompca*

Έπειτα γράφει την δεκαδική επέκταση του π:

π = 3.141592653689793..

Η αντιστοιχία γίνετε με την ακολουθία γραμμάτων που εξήγαγε προηγουμένως. Δηλαδή, το 3 αντιστοιχεί στο b, το τρίτο γράμμα του χωρίς νόημα κειμένου που έχουμε πιο πάνω. Στη συνέχεια είναι ο αριθμός 1, ο οποίος με τη σειρά του αντιστοιχεί στο γράμμα u, το επόμενο γράμμα με το b, δηλαδή 3+1=4. Το επόμενο γράμμα είναι το u, 4+4=8, άρα το όγδοο γράμμα από την αρχή της

γραμμής. Άλλος τρόπος είναι από το γράμμα που αντιστοιχεί πχ στο 4 (u) μετράμε συν 1 (που είναι ο επόμενος αριθμός), επομένως το επόμενο γράμμα είναι b.

Από τις αντιστοιχήσεις αριθμών – γραμμάτων έχω το εξής αποτέλεσμα:

buubdlupnpsspx

Τελευταίο βήμα για να μπορέσει να διαβάσει το μήνυμα είναι να αντικαταστήσει κάθε γράμμα με το γράμμα εκείνο που προηγείται στο αλφάβητο. Άρα το μήνυμα που έστειλε η Alice στον Bob είναι:

attack tomorrow

Σε αυτό το παράδειγμα που αναφέραμε η Alice αντιστοίχισε το κάθε γράμμα του μηνύματος της με το επόμενο γράμμα της αλφαβήτου. Στη συνέχεια έπρεπε να γράψει ένα κείμενο το όποιο θα είχε νόημα αλλά θα έπρεπε να είναι σίγουρη ότι η τοποθέτηση των λέξεων ακολουθούν τα ψηφία του π.
Εδώ φυσικά να αναφέρουμε ότι Alice και ο Bob θα μπορούσαν να μη χρησιμοποιήσουν την δεκαδική επέκταση του, αλλά να συμφωνήσουν σε μια ακεραία ακολουθία. Για παράδειγμα θα μπορούσαν να χρησιμοποιήσουν έναν ακέραιο που θα προκύπτει από μια γεννήτρια ψευδοτυχαίων αριθμών, τον οποίο θα είχε στείλει ο ένας στον άλλο με ένα κοινό κλειδί. Ο τρόπος με τον οποίο θα τοποθετηθούν τα γράμματα από το μήνυμα, ονομάζεται στεγανογραφικό κλειδί ή stego key. Είναι πολύ δύσκολο για κάποιον που δεν έχει το κλειδί αυτό, να ανακαλύψει ότι στο μήνυμα υπάρχει κρυμμένη πληροφορία.
Η τεχνική αυτή αποδίδει καλύτερα όταν η πληροφορία που θέλουμε να στείλουμε είναι μικρή, αλλιώς είναι πολύ δύσκολο αλλά και μη πρακτικό. Έτσι η χρήση εικόνων ή βίντεο είναι ευκολότερη και πιο πρακτική στο όταν έχουμε ένα μεγάλο μήνυμα, στέλνοντας τα ως αρχεία.

## 2.5 Σύγχρονη Στεγανογραφία


Η στεγανογραφία στους υπολογιστές είναι βασισμένη σε δύο αρχές.

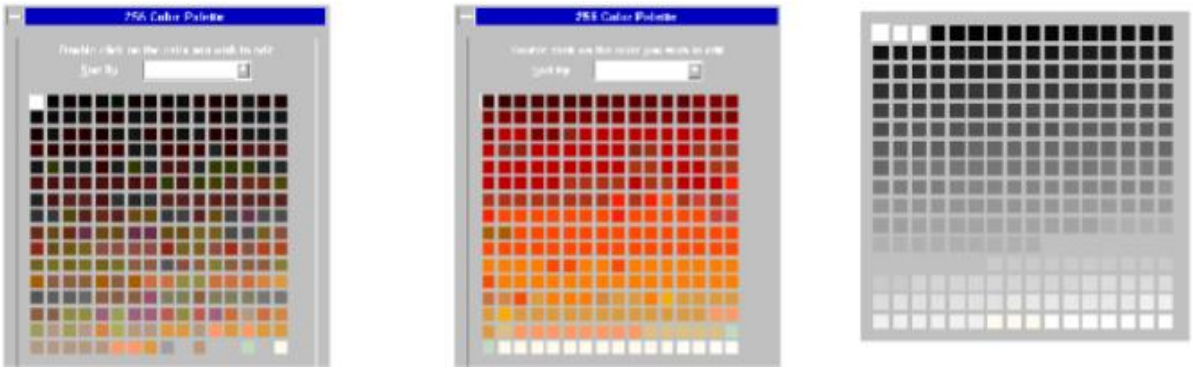
Η πρώτη είναι ότι τα αρχεία που περιέχουν εικόνες ή ήχο έχουν τη δυνατότητα να τροποποιηθούν ως ένα σημείο, χωρίς καμία αλλοίωση της λειτουργικότητάς τους, σε αντίθεση με άλλους τύπους δεδομένων, όπως για παράδειγμα τα προγράμματα, που δεν μπορούν να λειτουργήσουν αν υπάρχει έστω και η παραμικρή αλλαγή.

Η άλλη αρχή βασίζεται ότι ο άνθρωπος δεν είναι τόσο παρατηρητικός ώστε να μπορεί να διακρίνει τις ελάχιστες διαφορές στο χρώμα μιας εικόνας ή στη ποιότητα του ήχου. Φυσικά το να χρησιμοποιήσεις τις περιττές πληροφορίες από ένα αρχείο εικόνας ή ήχου είναι ιδιαίτερα εύκολο, είτε πρόκειται για ήχο 16bit, 8bit, ή ακόμα καλύτερα μιας εικόνας 24bit. Η τροποποίηση που γίνεται στις ψηφιακές εικόνες, αλλάζοντας την τιμή του λιγότερου σημαντικού bit (LSB) του χρώματος του εικονοκυττάρου (pixel) δεν γίνεται αντιληπτή από ανθρώπινο μάτι.

**Ας αναλύσουμε την χρήση της στην εικόνα**

Κατά την μετατροπή της εικόνας από αναλογική μορφή σε ψηφιακή, συνήθως έχουμε την δυνατότητα να επιλέξουμε μεταξύ τριών διαφορετικών ειδών χρωμάτων:

- 24 bit χρωματισμό: το κάθε pixel μπορεί να έχει 224 χρώματα, το κάθε αντιπροσωπεύουν διαφορετικές ποσότητες των τριών βασικών χρωμάτων.
- 8 bit χρώμα: το κάθε pixel μπορεί να έχει 256 χρώματα, όπου η επιλογή τους γίνεται από μία παλέτα ή από ένα πίνακα χρωμάτων.
- 8 bit κλίμακα του γκρίζου: το κάθε pixel μπορεί να έχει 256 αποχρώσεις του γκρίζου.



*Εικόνα 7 8 bit palette, 24 bit palette, 8bit grayscale*

Οι περισσότερες εφαρμογές στεγανογραφίας, δίνουν τις εξής επιλογές:

- **Auto**: δεν απαιτείται κάποιο κλειδί ή κωδικός για την εξαγωγή των δεδομένων, αλλά είναι κρυπτογραφημένα, προφανώς ο παραλήπτης θα πρέπει να γνωρίζει την ύπαρξη τους.
- **Symmetric**: ο αποστολέας χρησιμοποιεί κωδικό για το κρύψιμο των δεδομένων, τον οποίο πρέπει να γνωρίζει και ο παραλήπτης ώστε να μπορέσει να εξάγει τα δεδομένα.
- **Asymmetric unsigned**: το κρύψιμο και η εξαγωγή των δεδομένων γίνεται με την χρήση ενός κλειδιού, που γνωρίζουν ήδη ο αποστολέας και ο παραλήπτης.
- **Asymmetric signed**: Όταν θέλετε να αποκρύψετε τα δεδομένα (σαν αποστολέας) το δημόσιο κλειδί του παραλήπτη και το ιδιωτικό κλειδί σας, δεν απαιτούνται. Όταν θέλετε να εξάγετε τα δεδομένα (σαν παραλήπτης), μόνο το ιδιωτικό κλειδί σας είναι απαραίτητο, αλλά το δημόσιο κλειδί του αποστολέα έχει ζητηθεί. Εάν δεν παρέχεται το δημόσιο κλειδί του αποστολέα, στο τέλος της διαδικασίας εξαγωγής, θα πρέπει να έχετε μια προειδοποίηση πως η ταυτότητα αποστολέα δεν έχει επαληθευθεί. Αν υπάρχει το δημόσιο κλειδί, θα πάρετε ειδοποίηση πως η ταυτότητα του αποστολέα επαληθεύτηκε.

Όσον αφορά τώρα την αποσυμπίεση ενός τέτοιου αρχείου, γίνεται με αντίστοιχο πρόγραμμα, εισάγοντας την κρυπτογραφημένη εικόνα και στη συνέχεια πατώντας το κουμπί extract. Ανάλογα με τύπο που είναι κρυπτογραφημένη η εικόνα, με τους παραπάνω τρόπους που αναφέραμε, θα αποσυμπιεστεί και θα έχουμε στα χέρια μας την αρχική πληροφορία.

## 2.6 Υδατογράφημα

Τα αόρατα υδατογραφήματα, χρησιμοποιούνται για να κρύψουν πληροφορίες σε ένα αρχείο. Αποτελούν δυαδική πληροφορία που ενσωματώνεται σε ένα αρχείο αλλά παραμένει αόρατη, εφόσον δεν αλλοιώνει την εικόνα. Ο εντοπισμός της εφαρμογής του αόρατου ψηφιακού υδατογραφήματος γίνετε αλγοριθμικά. Στην παρακάτω εικόνα φαίνεται το υδατογράφημα που προκύπτει από τη χρήση

ενός συστήματος εντοπισμού υδατογραφημάτων και το αποτέλεσμα που δίνει το σύστημα για ένα κομμάτι της εικόνας που δεν περιέχει υδατογράφημα.


*Εικόνα 8 Παράδειγμα υδατογραφήματος*

Αν ο επίδοξος χρήστης έχει την υποψία ότι το αρχείο (είτε εικόνα, είτε βίντεο, είτε μουσικό αρχείο), με τη χρήση των ψηφιακών υδατογραφημάτων, μπορεί να αποτρέψει μια κλοπή από το μη εξουσιοδοτημένο άτομο και την μη εξουσιοδοτημένη αντιγραφή και χρήση του αρχείου.

Πέρα όμως από την ψυχολογική αποτροπή της παράνομης χρήσης, τα αόρατα ψηφιακά υδατογραφήματα προσδιορίζουν την πηγή, το δημιουργό, τον ιδιοκτήτη, τον εξουσιοδοτημένο χρήστη κ.τ.λ. ενός αρχείου.

Πολλές εταιρείες μάλιστα, αναπτύσσουν λογισμικά τα οποία θέτουν πράκτορες (agents) υδατογραφημάτων σε «περιπολίες» στο διαδίκτυο με στόχο τον εντοπισμό μη εξουσιοδοτημένης χρήσης ψηφιακά υδατογραφημένων τεκμηρίων. Αξίζει εδώ να σημειωθεί πως τα λογισμικά υδατογράφησης αποδίδουν ένα μοναδικό υδατογράφημα σε κάθε ψηφιακό τεκμήριο για κάθε εξουσιοδοτημένο χρήστη.

## 2.7 Πλεονεκτήματα / Μειονεκτήματα (Στεγανογραφία συγκριτικά με την Κρυπτογραφία)

Η στεγανογραφία είναι η τέχνη του να κρύβεις την ίδια την επικοινωνία, ενώ η κρυπτογραφία είναι να κρύβεις το μήνυμα μέσα σε ένα αθώο κείμενο. Στην στεγανογραφία δύσκολα θα καταλάβει κάποιος ότι υπάρχει κρυφό μήνυμα μέσα σε μια εικόνα την οποία έχει κλέψει, εφόσον δεν υπάρχει κάτι για να δει, στην κρυπτογραφία είναι διαφορετικά γιατί φαίνεται το μήνυμα απλά ο τρίτος δεν μπορεί να το διαβάσει, θα γνωρίζει όμως για την επικοινωνία.

| **Στεγανογραφία** | ***Ίσον*** | **Κρυπτογραφία** |
|---|---|---|
| | **με** | |
| **Μυστική επικοινωνία** | | **Μυστική πληροφορία** |

*Εικόνα 9 Στεγανογραφία - Κρυπτογραφία*

Ένα από τα μειονεκτήματα στης Στεγανογραφίας είναι το μέγεθος του αρχικού αρχείου και αυτού του οποίου προκύπτει μετά από χρήση στεγανογραφικής μεθόδου. Κάποιος μπορεί να καταλάβει ότι ένα αρχείο έχει αλλάξει, παρόλο που είναι φαινομενικά το ίδιο, κοιτάζοντας το μέγεθος του συγκριτικά με ένα άλλο ίδιας συμπίεσης. Ο εχθρός θα αντιληφθεί το ύποπτο αρχείο μόνο αν έχει και το αρχικό.
Επίσης δεν είναι πολύ καλή ιδέα να χρησιμοποιήσει κάποιος εικόνα που έχει χρησιμοποιηθεί ξανά, για παράδειγμα η χρήση μίας εικόνας ενός διάσημου προσώπου για κρύψιμο των δεδομένων, μπορεί να αποβεί μοιραία, εφόσον είναι διαθέσιμη στο διαδίκτυο για τον κάθε ένα. Προτιμότερο είναι να γίνει η χρήση μίας δικής του φωτογραφίας, όπως μία εικόνα με τον κήπο του.

Η κρυπτογραφία σαν τεχνική έχει και αυτή το δικά της μειονεκτήματα:
Στην συμμετρική κρυπτογράφηση όπου υπάρχει ένα κλειδί το οποίο πρέπει να είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Το θέμα που τίθεται είναι πως θα γίνει η ανταλλαγή του κλειδιού χωρίς να το υποκλέψει κάποιος τρίτος. Το πλεονέκτημα είναι ότι έχει χαμηλό υπολογιστικό κόστος. Όσον αφορά τα ασύμμετρα κρυπτοσυστήματα όπου υπάρχουν δύο κλειδιά, το δημόσιο και το ιδιωτικό, όπου η ανταλλαγή του ιδιωτικού κλειδιού γίνεται μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Έχει υψηλή ασφάλεια, εφόσον δεν μεταδίδεται το ιδιωτικό κλειδί ούτε υπάρχει κίνδυνος να αποκαλυφθεί. Επιπλέον αποτελεί μέθοδο για ψηφιακές υπογραφές. Σημαίνει ότι κάποιος μπορεί να επιβεβαιώσει την ταυτότητα του μόνο με το ιδιωτικό του κλειδί, το κάθε ιδιωτικό κλειδί, αντιστοιχεί σε κάθε μοναδικό χρήστη. Είναι σύστημα πιστοποίησης ταυτότητας και παρέχει «ψηφιακή» εμπιστοσύνη στον κάτοχο του. Δυστυχώς υπάρχει ένα μεγάλο μειονέκτημα στους ασύμμετρους αλγορίθμους και αυτό είναι η ταχύτητα κρυπτογράφησης.

## 2.8 Περιγραφή των διαφόρων μορφών στις οποίες εφαρμόζεται από διάφορες οντότητες

Η στεγανογραφία χρησιμοποιείται κάθε φορά που κάποιος έχει την επιθυμία να αποτρέψει άτομα χωρίς εξουσιοδότηση να αποκτήσουν πρόσβαση σε πληροφορίες που περιέχονται σε κάποιο μήνυμα.
Υπάρχουν πολλές εφαρμογές για την ψηφιακή στεγανογραφία σε εικόνες, όπως είναι η προστασία της πνευματικής ιδιοκτησίας.
Αν μιλήσουμε για τον τομέα των επιχειρήσεων η στεγανογραφία χρησιμοποιείται για την απόκρυψη μελλοντικών σχεδίων. Η στεγανογραφία χρησιμοποιείται και στον τομέα της βιομηχανικής κατασκοπείας με την αποστολή μηνυμάτων μέσα από κάποια εταιρεία χωρίς να το αντιληφθεί κανείς.
Αν κάποιος χρησιμοποιεί την στεγανογραφία σε προσωπικό επίπεδο, απλώς δεν επιθυμεί τα δεδομένα που θέλει να μεταδοθούν να γνωστοποιηθούν σε τρίτους.

Η στεγανογραφία έχει τρεις δημοφιλείς χρήσεις. Εφαρμόζεται στην ψηφιακή υδατογράφηση, την στεγανογραφία και σε μυστικά κανάλια ανοιχτών συστημάτων που εκτελούν ενσωμάτωση δεδομένων.


*Εικόνα 10 Οι πιο δημοφιλείς εφαρμογές απόκρυψης πληροφορίας*

### *2.8.1 Τύποι Αρχείων – Στεγανογραφικά Προγράμματα*

**JPG:** Μέχρι σήμερα το Jpeg-Jsteg είναι το μόνο στεγανογραφικό πρόγραμμα που κρύβει την πληροφορία σε κωδικοποίηση JPEG.

**GIF:** Τα καλύτερα εργαλεία για στεγανογράφηση σε GIF μορφή είναι τα S-Tools4.Πρόκειται για ένα πρόγραμμα Windows95/NT το οποίο χρησιμοποιεί την τεχνική drag-and-drop.

**BMP:** Στη περίπτωση αυτή η δουλειά μπορεί να γίνει με συνδυασμό των S-Tools4 καιHide4PGP.

**WAV**: Ισχύει ότι και στη περίπτωση των αρχείων BMP.

**VOC**: Μόνο το Hide4PGP μπορεί να επεξεργαστεί αρχεία φωνής.

**GZ**: Ο τύπος αυτός αντιστοιχεί σε αρχεία που προκύπτουν από τον αλγόριθμο συμπίεσης του Linux και άλλων UNIX συστημάτων. Το GZ σημαίνει Gnu Zip ή Gzip.Στα PC τα αρχεία που συμπιέζονται με το GZ διατηρούν τα πρώτα δύο γράμματα της κατάληξής τους και το τρίτο αντικαθίσταται με το γράμμα "z". Για παράδειγμα το αρχείοREADME.TXT θα γινότανε README.TXZ. Τέλος, το πρόγραμμα που χρησιμοποιείται είναι το GZSteg.

**TXT**: Το "Texto" είναι ένα πρόγραμμα που παίρνει σαν είσοδο κρυπτογραφημένα μεPGP (ASCII) αρχεία και παράγει ένα αρχείο αποτελούμενο από ακατανόητες φράσεις. Το "Snow" είναι ένα πρόγραμμα που κρύβει δεδομένα χρησιμοποιώντας tabs και κενά στο τέλος των γραμμών ενός αρχείου κειμένου.

## 2.9 Υβριδικά συστήματα (συνδυασμός Στεγανογραφία/ κρυπτογραφίας)

Εάν κάποιος είχε στη κατοχή του ένα αρχείο με κρυμμένη πληροφορία θα μπορούσε εύκολα να καταλάβει ότι κάτι κρύβει το συγκεκριμένο αρχείο και ας μη την βλέπει. Τώρα αν η πληροφορία που κρύβεται στο αρχείο είναι κρυπτογραφημένη τότε σίγουρα θα φτάσει στο σημείο αυτό, αν δεν είναι κρυπτογραφημένο τότε θα μπορεί να εξετάσει όλο το κρυφό μήνυμα. Σε αυτό το σημείο είναι σημαντικό να τονίσουμε ότι για μεγαλύτερη ασφάλεια θα πρέπει την πληροφορία που θέλουμε να κρύψουμε θα την κρυπτογραφήσουμε και στη συνέχεια να την κρύψουμε σε ένα αθώο αρχείο.

### *2.9.1 Βασική ιδέα μεθόδου:*

Η πρώτη σχετική εργασία πραγματοποιήθηκε το 1994 από τους M. Naor και A. Shamir. Ο δεύτερος είναι ένας από τους εφευρέτες του αλγορίθμου RSA.
Η στεγανογραφία σε συνδυασμό με την κρυπτογραφία σαν μία υβριδική μορφή πετυχαίνει ένα πολύ καλό υψηλό επίπεδο ασφαλείας και απορρήτου. Η επεξεργασία της πρώτης φάσης έγινε σε δύο φάσεις: το μήνυμα κρυπτογραφείται με τη βοήθεια κάποιου αλγορίθμου κρυπτογράφησης (DES, RSA, MD5 κλπ) κατόπιν στεγανογραφείται μέσω μιας τυχαίας εικόνας. Το αποτέλεσμα είναι μία αθώα εικόνα, σχεδόν η ίδια με την αρχική εικόνα, που περνάει εντελώς απαρατήρητη. Η αρχική εικόνα με την τελική με γυμνό μάτι είναι πολύ δύσκολο να διακριθούν. Ακόμα και με μεγέθυνση των εικόνων, δεν μπορεί κάποιος να αποφανθεί ποια είναι η αρχική και ποια η τελική. Η διαφορά είναι σε λίγα pixel τα οποία είναι διασκορπισμένα σε ολόκληρη την εικόνα.
Μεγάλο πλεονέκτημα του συνδυασμού αυτού είναι ότι αυξάνει την δυνατότητα προστασίας της μυστικότητας μας, ή την επικοινωνία μας όταν το απαιτούν οι συνθήκες. Όσο μεγαλύτερη ανάλυση και χρωματική ανάλυση έχει η αρχική εικόνα, τόσο πιο δυσδιάκριτες είναι οι διαφορές.

Ο πρώτος αλγόριθμος των Naor και Shamir «χώριζε» την εικόνα σε N περιοχές οι οποίες έπρεπε να συνδυαστούν για να έχουμε το τελικό αποτέλεσμα. Η κάθε περιοχή είναι ένα τμήμα της αρχικής εικόνας, ζωγραφισμένη πάνω σε διαφορετικές διαφάνειες, που τοποθετούνται η μια πάνω στην άλλη για να πάρουμε την αρχική εικόνα. Είναι φυσικό ότι αν ακόμα και με μία λιγότερη (N-1) διαφάνεια δεν ήταν δυνατή η ανάκτηση της κρυπτογραφημένης εικόνας.

Στην συνέχεια της ιστορίας υπήρξαν οι Zenon, Voloshynovskiy και Rytsar, που πρότειναν την εφαρμογή φίλτρου τυχαίας φάσης για την κρυπτογράφηση της εικόνας. Ο αλγόριθμος που πρότειναν οι παραπάνω αποτελείται από τέσσερα βήματα:

- Αρχικά υπολογίζεται ο διακριτός μετασχηματισμός Fourier (DFT) της αρχικής εικόνας
- Στη συνέχεια εφαρμόζεται ένα φίλτρο τυχαίας φάσης στο αποτέλεσμα.

- Υπολογίζεται ο αντίστροφος διακριτός μετασχηματισμός Fourier (Reverse DFT) του αποτελέσματος.
- Και τελικά τα δυαδικά δεδομένα ξαναμετατρέπονται σε εικόνα

Βέβαια υπήρξε ένα πλήθος προτάσεων αντί για την τυχαία μεταβολή φάσης, οι Lee και Chen πρότειναν την αντικατάσταση του λιγότερο σημαντικού bit (LSB) κάθε pixel της αρχικής εικόνα. Οι Chan και Chang πρότειναν με τη σειρά τους την αντικατάσταση των μεσαίων bit κάθε pixel της εικόνας. Οι Chang, Chen και Chung καθώς και οι Hsu και Wu πρότειναν εναλλακτικούς μετασχηματισμούς αντί του DFT, όπως ο διακριτός μετασχηματισμός συνημίτονου (DCT) και ο διακριτός μετασχηματισμός κυματομορφής (DWT). Παρόμοιοι αλγόριθμοι (Low Bit Encoding, Spread Spectrum, Perceptual Masking), έχουν προταθεί και για «ηχητική» κρυπτογραφία όπου το ρόλο της εικόνας διαδραματίζει ένα ηχητικό μήνυμα. Τέλος οι Potdar και Chang πρότειναν την απόκρυψη κειμένου ως εικόνα μέσα σε άλλη εικόνα. Είναι γνωστό ότι η Κρυπτανάλυση κειμένου που έχει κρυπτογραφηθεί ως εικόνα είναι πιο δυσχερής από την Κρυπτανάλυση κειμένου που έχει κρυπτογραφηθεί με παραδοσιακά μέσα. Μια εικόνα έχει μεγαλύτερο μέγεθος από μήνυμα κειμένου το οποίο περιέχει την ίδια ποσότητα πληροφορίας είναι, από τεχνικής άποψης, πιο δύσκολο να υποκλαπεί, λόγο της απαίτησης από πλευράς μνήμης και χρόνου.

## 2.10 Πλεονεκτήματα – Μειονεκτήματα

Υπάρχει πλήθος από πλεονεκτήματα
Παρέχει περισσότερη ασφάλεια από την κοινή κρυπτογραφία και την κοινή στεγανογραφία, εφόσον ο εχθρός δεν μπορεί αποκρυπτογράφηση το μήνυμα, αλλά ούτε υποπτεύεται πως η εικόνα που μεταδίδεται περιέχει κρυπτογραφημένο μήνυμα.
Επιπλέον, εφόσον το κρυπτογραφημένο μήνυμα δεν προκαλεί υποψίες, τότε προστατεύεται και η ταυτότητα του αποστολέα αλλά και του παραλήπτη.

Μειονέκτημα της είναι η αυξανόμενη δυνατότητα για ανεξέλεγκτη χρήση. Πλέον ο κάθε ένας ο όποιος έχει τα κατάλληλα εργαλεία, που είναι μάλιστα δωρεάν και διαθέσιμα στον οποιονδήποτε, μπορεί να κρυπτογραφήσει τα δεδομένα.
Σχετικά με την τεχνική αντικατάστασης του λιγότερου σημαντικού bit (LSB) κάθε pixel δεν γίνεται αντιληπτή από ανθρώπινο μάτι, δυστυχώς όμως υπάρχει κίνδυνος να προκληθεί ανεπανόρθωτη αλλοίωση της κρυπτογραφημένης πληροφορίας στην περίπτωση συμπίεσης – επειδή οι περισσότεροι αλγόριθμοι συμπίεσης αλλοιώνουν το LSB- της τελικής εικόνας. Επειδή υπάρχει αυτή η αλλοίωση

της συμπιεσμένης εικόνας, είναι πιο εύκολο να εντοπιστούν οι διαφορές. Ένα ακόμα μειονέκτημα το οποίο είναι μειονέκτημα και για τον υποκλοπέα, είναι ότι η επεξεργασία της εικόνας έχει μεγαλύτερη πολυπλοκότητα και σε μνήμη και σε χρόνο με την απλή επεξεργασία κειμένου.

# ΚΕΦΑΛΑΙΟ 3

## Στεγανάλυση(Steganalysis)

### 3.1 Περίληψη στεγανάλυσης

Το διαδίκτυο έχει ξεσηκώσει τον σύγχρονο κόσμο με τις εφαρμογές που βασίζονται σε αυτό και με τα υψηλά επίπεδα άνεσης που μας προσφέρει με την χρήση του σε κάθε πτυχή της ανθρώπινης ζωής. Από το Σεπτέμβριο του 2009, περίπου 1,73 δισεκατομμύρια άνθρωποι σε όλο τον κόσμο κάνουν χρήση του διαδικτύου για διάφορους σκοπούς, από την πρόσβαση σε πληροφορίες σχετικά με την εκπαίδευση, για οικονομικές συναλλαγές, την προμήθεια αγαθών και υπηρεσιών. Καθώς ο σύγχρονος κόσμος γίνεται σταδιακά «χωρίς χαρτιά», με τεράστιες ποσότητες πληροφοριών να αποθηκεύονται και να ανταλλάσσονται μέσω του Διαδικτύου, επιβάλλεται να έχουμε ισχυρή ασφάλεια για την προστασία της ιδιωτικής ζωής και της ασφάλειας των προσωπικών δεδομένων.

Οι τεχνικές κρυπτογραφίας έχουν χρησιμοποιηθεί ευρέως για την κρυπτογράφηση των δεδομένων απλού κειμένου, την μεταφορά του και στη συνέχεια ο παραλήπτης να αποκρυπτογραφεί το κρυφό μήνυμα. Ωστόσο, με τα κρυπτογραφήματα τα δεδομένα δεν είναι πάντα σίγουρα ασφαλή. Ένας χάκερ ή ένας εισβολέας που παρακολουθεί ένα κανάλι μπορεί να καταλάβει αν ένα απλό κείμενο, δεν είναι «απλό κείμενο» αλλά ένα κρυπτογραφημένο μήνυμα και δυστυχώς η περιέργεια είναι στη φύση του ανθρώπου, οπότε και εξαπολύει επιθέσεις κρυπτανάλυσης στο κρυπτό-κείμενο, δηλαδή προσπαθεί να αναλύσει το περιεχόμενο του, μέχρι να το αποκρυπτογραφήσει πλήρως ή μερικώς.

Στεγανάλυση είναι η τέχνη της ανίχνευσης κρυμμένου μηνύματος με χρήση στεγανογραφίας στο εσωτερικό ενός αρχείου. Χρησιμοποιείται ως αποτελεσματικός τρόπος για να κριθεί πόσο ασφαλές είναι οι εκάστοτε στεγανογραφικές τεχνικές. Θεωρείται «ιδιωτικό» εργαλείο και είναι λογικό να προσελκύει την ανθρώπινη περιέργεια, γίνονται πολλές προσπάθειες ανάπτυξης μεθόδων για την ανίχνευση μυστικών μηνυμάτων με απώτερο σκοπό την επίθεση.

Ωστόσο το κυνήγι της κρυπτογραφίας/στεγανογραφίας, δεν είναι κάτι καινούργιο, έλαβε έκταση μετά τις τρομοκρατικές επιθέσεις που έγιναν στις 11 Σεπτεμβρίου 2001, όπου η Αλ-Καιντα κατηγορήθηκε πως η μεταξύ τους η επικοινωνία πραγματοποιούνταν με μέθοδο στεγανογραφίας, αποφασίστηκε ότι θα εξελιχτεί η στεγανάλυση, για την αποφυγή επόμενης επίθεσης.

Ακριβώς όπως η κρυπτογράφηση που εφαρμόζει μεθόδους με σκοπό την αποκρυπτογράφηση, με την ίδια νοοτροπία η στεγανογραφία εφαρμόζει τις δικές τις μεθόδους με τον ίδιο σκοπό, την αποκάλυψη του κρυφού μηνύματος.

## 3.2 Βασικές τεχνικές ανίχνευσης στεγανογραφίας

Πλέον υπάρχουν πολλές μέθοδοι για την ανίχνευση της στεγανογραφίας, μερικοί από αυτοί είναι οι παρακάτω:

- Οπτική Μέθοδος: Η πρώτη μέθοδος είναι αυτή της σύγκρισης του ύποπτου αρχείου με το αρχικό αρχείο. Συνήθως υπάρχουν πολλαπλά αντίγραφα φωτογραφιών, αλλά και βίντεο στο διαδίκτυο, με τα οποία μπορεί να γίνει η σύγκριση με τα αρχεία τα οποία έχουν κλαπεί, αν φυσικά έχουν χρησιμοποιήσει κάποιο αρχείο από το διαδίκτυο, γιατί υπάρχει η περίπτωση να έχουν δημιουργήσει νέο. Για παράδειγμα, το ύποπτο αρχείο είναι μία εικόνα JPEG και έχω βρει μία πανομοιότυπη JPEG εικόνα. Η σύγκριση γίνετε στο μέγεθος των αρχείων, το αρχείο με την κρυμμένη πληροφορία θα είναι σαφώς μεγαλύτερο.
- Η άλλη μέθοδος αφορά μουσικά αρχεία, στη περίπτωση που το ύποπτο αρχείο είναι ένα μουσικό κομμάτι, μπορούμε να το ακούσουμε. Αυτή η μέθοδος και η παραπάνω είναι παρόμοιες. Έχουμε δύο αρχεία ήχου, το ύποπτο που θέλουμε να "διαβάσουμε " και έχουμε βρει αρχείο ήχου που χρησιμοποιεί την ίδια συμπίεση (MP3), ακούγοντας το πρώτο το συγκρίνουμε με το δεύτερο, στην περίπτωση που υπάρχουν διαφορές, συμπεραίνουμε ότι στο ένα αρχείο ήχου υπάρχει κρυμμένο μήνυμα.

Η στεγανογραφία αναλύεται σε δύο στάδια, πρώτα ανιχνεύει και στη συνέχεια αποσπά το κρυφό μήνυμα. Κάθε αρχείο εικόνας μπορεί να τροποποιηθεί με στόχο την απόκρυψη πληροφορίας. Η ανίχνευση της εξοικονομεί χρόνο από τη διαδικασία ανάκτησης της, αλλά γίνεται από τη στιγμή που η πληροφορία βρεθεί.

## 3.3 Βασικές τεχνικές επίθεσης

Οι τεχνικές επίθεσης που χρησιμοποιούνται είναι ανάλογα το είδος πληροφορίας που έχει στα χέρια του ο στεγαναλυτής.

- **Στεγό-αποκλειστική** -- η κρυμμένη πληροφορία είναι η μόνη διαθέσιμη για ανάλυση, στη περίπτωση που η αρχική και η κρυπτογραφημένη πληροφορία είναι διαθέσιμές, τότε η επίθεση ονομάζεται: επίθεση "γνωστού μέσου".
- **Επιλεκτική στεγό-επίθεση** – είναι η δεύτερη τεχνική επίθεσης, στην οποία ο στεγαναλυτής έχει την γνώση, τόσο του στεγό-μέσου αλλά και του αλγόριθμου που χρησιμοποιήθηκε. Το στέγο-μέσο δημιουργείται από κάποιο στεγανογραφικό εργαλείο ή αλγόριθμο γνωστού μηνύματος. Ο στόχος της επίθεσης αυτής είναι ο καθορισμός συγκεκριμένων ιδιοτήτων του στέγο-μέσου που προσεγγίζουν στη χρήση κάποιου στεγανογραφικού εργαλείου ή αλγορίθμου.

Χωρίζεται σε δύο κύριες κατηγορίες μεθόδου:

- **Παθητικές** : ανίχνευση παρουσίας κρυφών δεδομένων σε ένα ύποπτο αρχείο.
- **Ενεργές** : εκθέτει μερικές ιδιότητες του μηνύματος ή του αλγορίθμου ενσωμάτωσης. Εξάγει μια έκδοση του μυστικού μηνύματος κατά προσέγγιση, από ένα μήνυμα στέγο.

## 3.4 Η στεγανάλυση σε εικόνα

Οι αλγόριθμοι για στεγανάλυση σε εικόνα είναι κυρίως δύο ειδών: Ειδικοί και Γενικοί αλγόριθμοι.
Η ειδική προσέγγιση αντιπροσωπεύει μια κατηγορία τεχνικών στεγανάλυσης εικόνας που εξαρτάται σε μεγάλο βαθμό από τον στεγανογραφικό αλγόριθμο που χρησιμοποιήθηκε για να κρυφτεί το μήνυμα, έχει υψηλό ποσοστό επιτυχίας στην ανίχνευση της παρουσίας μυστικού μηνύματος.
Η γενική προσέγγιση αντιπροσωπεύει μια κατηγορία τεχνικών στεγανάλυσης εικόνας που είναι ανεξάρτητες από τον αλγόριθμο στεγανογραφίας που χρησιμοποιήθηκε για να κρύψει το μήνυμα.
Τόσο ειδικές όσο και οι γενικές τεχνικές στεγανάλυσης σχεδιάστηκαν κυρίως για την ανίχνευση παρουσίας ενός μυστικού μηνύματος και την αποκωδικοποίηση του, αλλά δεν θεωρείται υποχρεωτική.

### *3.4.1 LSB*

Οι περισσότεροι αλγόριθμοι στεγανογραφίας βασίζονται σε ένα μηχανισμό ενσωμάτωσης που ονομάζεται ενσωμάτωση στο λιγότερο σημαντικό ψηφίο-LSB. Κάθε εικονοστοιχείο(pixel) αναπαριστάτε σαν μία 24bit τιμή και αποτελείται από 3bytes που εκπροσωπούν τα τρία βασικά χρώματα(RGB- κόκκινο, πράσινο, μπλε). Μια RGB τιμή μεγαλύτερη από μία άλλη, συνεπάγεται μεγαλύτερη ένταση. Για παράδειγμα ένα εικονοστοιχείο χ αναπαριστάται ως FF FF FF 16 και

αποτελείται από το σύνολο των τριών αυτών βασικών χρωμάτων στη μέγιστη ένταση τους. Το χρώμα που αντιπροσωπεύεται από αυτό το εικονοστοιχείο είναι το "λευκό". Η ενσωμάτωση στο LSB εκμεταλλεύεται το γεγονός ότι η οποιαδήποτε αλλαγή του λιγότερου σημαντικού στοιχείου καθενός από τα τρία bytes ενός pixel θα παράγει μία μικρή αλλαγή στην ένταση του χρώματος που αντιπροσωπεύεται από το pixel και αυτή η αλλαγή δεν είναι αντιληπτή από το ανθρώπινο μάτι. Για παράδειγμα αλλάζοντας τι τιμές χρωμάτων του εικονοστοιχείου χ προς FE FE FE 16, θα κάνει το χρώμα πιο σκούρο κατά ένα συντελεστή 1/256.
Οι στεγανογραφικοί αλγόριθμοι που βασίζονται σε LSB διαφέρουν στο σχήμα τροποποίησης, μία τροποποίηση των τυχαία επιλεγμένων εικονοστοιχείων ή μείωση των pixel που επιλέγονται σε μια συγκεκριμένη περιοχή της εικόνας.

Οι εικόνες μπορούν να είναι σε διαφορετικές μορφές, οι τρεις πιο συνήθεις μορφές είναι : GIF (Graphics Interchange Format), BMP (Bit Map) and JPEG (Joint Photographic Exchange Group). Κάθε μια από αυτές τις μορφές εικόνας συμπεριφέρεται διαφορετικά όταν ένα μήνυμα έχει ενσωματωθεί σε αυτή. Ως εκ τούτου, υπάρχουν διαφορετικοί αλγόριθμοί στεγανάλυσης εικόνων για κάθε μία από αυτές τις διαφορετικές μορφές εικόνων. Παρακάτω αναλύεται η στεγανάλυση για κάθε μια μορφή εικόνων.

- GIF. Η μορφή GIF υποστηρίζει μέχρι και 8 bits ανά pixel και το χρώμα του εικονοστοιχείου αναφέρεται σαν παλέτα από 0 έως 256 διακριτές τιμές χρώματος (με βάση RGB-24bits). Η ενσωμάτωση σε μια τέτοια μορφή θα αλλάζει την 24bit RGB τιμή ενός pixel και αυτό επιφέρει αλλαγή τιμών στην παλέτα. Η δύναμη του αλγορίθμου αυτού έγκειται στην μείωση της πιθανότητας αλλαγής στο χρώμα στην παλέτα του εικονοστοιχείου και στην όσο πιο μικρή αλλοίωση μπορεί να γίνει. Η στεγανάλυση σε GIF εικόνα διεξάγεται πραγματοποιώντας μια στατιστική ανάλυση της παλέτας της εικόνας και η ανίχνευση γίνεται όταν υπάρχει αισθητή αύξηση στην εντροπία(μέτρηση μεταβολής χρωμάτων στην παλέτα). Η μεταβολή της εντροπίας είναι μέγιστη όταν έχει το μέγιστο μήκος.
- BMP. Οι πρώτες τεχνικές στεγανάλυσης χρησιμοποιήθηκαν κατά κύριο λόγο για τις εικόνες τύπου BMP που χαρακτηρίζονται από ένα χωρίς απώλειες LSB επίπεδο. Η LSB ενσωμάτωση μηνύματος σε αυτές τις εικόνες προκαλεί την αλλαγή τιμών σε δύο αποχρώσεις του γκρι. Είναι πολύ πιθανό να εμφανίσει των μέσο όρο της συχνότητας εμφάνισης των εικονοστοιχείων με τις δύο τιμές κλίμακας του γκρι. Για παράδειγμα εάν μια εικόνα έχει 20 pixels με μια τιμή κλίμακας του γκρι και 40 pixels με την άλλη τιμή απόχρωσης του γκρι, όταν θα γίνει η LSB ενσωμάτωση, ο αριθμός των εικονοστοιχείων με κάθε μία από τις τιμές της γκρίζας κλίμακας, αναμένεται να είναι γύρω στο 30. Η προσέγγιση αυτή προτάθηκε για πρώτη φορά από τον Westfeld και τον Pfitzmann και βασίζεται στην υπόθεση ότι το μήκος

του μηνύματος θα πρέπει να είναι συγκρίσιμο τον αριθμό των pixels στην εικόνα που χρησιμοποιείται για κάλυμμα(για μεγάλα μηνύματα) ή η θέση του κρυμμένου μηνύματος θα πρέπει να είναι γνωστή(για μικρά μηνύματα). Ο Dumitrescu πρότεινε ένα άλλο αλγόριθμο στεγανάλυσης για τις αποχρώσεις του γκρι της εικόνας. Ο αλγόριθμος αυτός υποθέτει ότι μία εικόνα αποτελείται από οριζόντια παρακείμενα εικονοστοιχεία και ταξινομεί το σύνολο όλων αυτών των ζευγών pixel σε (a, b) σε τέσσερα υποσύνολα, ανάλογα με το αν a και b είναι μονό ή ζυγό και αν a <b, a> b ή a = b. Οι τιμές των εικονοστοιχείων τροποποιούνται όταν γίνετε ενσωμάτωση, οδηγώντας και στην τροποποίηση των μελών στις τέσσερις υποομάδες. Η στατιστική ανάλυση σχετικά με τις αλλαγές στη σύνθεση των εικονοστοιχείων στην stego-εικόνα οδηγεί στην ανίχνευση του μήκους του κρυμμένου μηνύματος.

Ο Fridrich πρότεινε μία τεχνική στεγανάλυσης που μελετά έγχρωμες εικόνες bitmap για ενσωμάτωση LSB και παρέχει υψηλά ποσοστά ανίχνευσης για μικρά κρυμμένα μηνύματα. Αυτή η τεχνική κάνει χρήση των χαρακτηριστικών των μοναδικών χρωμάτων, για υψηλή ποιότητα εικόνας bitmap ο αριθμός αυτών είναι το ήμισυ του αριθμού pixel στην εικόνα. Η νέα παλέτα χρωμάτων που λαμβάνεται μετά την ενσωμάτωση LSB χαρακτηρίζεται από υψηλό αριθμό ζευγών χρωμάτων, δηλαδή ζεύγη που έχουν μέγιστη διαφορά με οποιοδήποτε από τα χρώματα. Μπορούμε να πούμε ότι δύο χρώματα (R1, G1, B1) και (R2, G2, B2) είναι κοντά, αν $|R1-R2| \leq 1$ και $|G1-G2| \leq 1$ και $|B1-B2| \leq 1$.

- JPEG. Είναι πολύ δημοφιλής μορφή εικόνας που χρησιμοποιείται στη στενογραφία για κάλυψη. Δύο γνωστοί στεγανογραφικοί αλγόριθμοι για την απόκρυψη του μυστικού μηνύματος σε εικόνες τέτοιου τύπου είναι: ο αλγόριθμος F5 και ο OutGuess αλγόριθμος.
    1. Στόχος του αλγορίθμου F5 ήταν η ενσωμάτωση για εικόνες JPEG που θα παρέχει υψηλής στεγανογραφικής χωρητικότητας χωρίς να θυσιάσει την ασφάλεια. Αντί της αντικατάστασης των LSB των κβαντισμένων συντελεστών DCT με bits του μηνύματος, η απόλυτη τιμή του συντελεστή μειώνετε κατά ένα. Οι συγγραφείς υποστηρίζουν ότι αυτό το είδος της ενσωμάτωσης δεν μπορεί να ανιχνευθεί με την χρήση της στατικής επίθεσης. Ο αλγόριθμος αυτός ενσωματώνει bit μηνύματος σε τυχαία επιλεγμένους συντελεστές DCT και χρησιμοποιεί πλέγμα ενσωμάτωσης που ελαχιστοποιεί τον απαραίτητο αριθμό αλλαγών για την ενσωμάτωση μηνύματος ορισμένου μεγέθους. Η διαδικασία στεγανάλυση σε τέτοιου είδους εικόνες περιλαμβάνει την εικόνα χωρισμένη σε 4 στήλες και στη συνέχεια εφαρμόζοντας ένα πίνακα κβαντισμού για την εκ νέου συμπίεση της εικόνας. Το προκύπτον DCT συντελεστής-ιστόγραμμα θα είναι κατά εκτίμηση κοντά στο πρωτότυπο.

2. Ο αλγόριθμος OutGuess προτάθηκε από τον Neils Provos για την αντιμετώπιση της στατικής επίθεσης Chi-square. Ενσωματώνει το μήνυμα κατά μήκος μίας τυχαίας επιλογής των LSB, ενώ παρακάμπτοντας τα 0 και 1. Αυτό γίνετε δύο φόρες ώστε να κάνει την εικόνα να ταιριάζει με την αρχική εικόνα. Επειδή η επίθεση chi-square βασίζεται στην ανάλυση στατιστικής πρώτης τάξης, δεν μπορεί να ανιχνεύσει τα μηνύματα με έχουν ενσωματωθεί με τον αλγόριθμο OutGuess. Σε επίθεση αυτού του αλγόριθμου για να καταφέρουμε να έχουμε επιτυχία έχουμε το μυαλό μας ότι η ενσωμάτωση μηχανισμού OutGuess γίνετε σε δύο «περάσματα» των LSB. Αυτό σημαίνει ότι ενσωματώνει άλλο μήνυμα στην εικόνα και μερικώς ακυρώνει το προηγούμενο με αποτέλεσμα να έχει διαφορετική επίδραση στην stego- εικόνα από ότι στην αρχική.

   Η ανίχνευση κρυφού μηνύματος αποτελείται από τα εξής βήματα:

   1. Αποσυμπίεση της stego-εικόνας, υπολογίζει τον σχηματισμό των μπλοκ και όσων αυτών υποδηλώνονται Bs(0).
   2. Χρησιμοποιώντας τον αλγόριθμο OutGuess, ενσωματώνουμε το μέγιστο μήκος στην stego –εικόνα (2aP bits), στη συνέχεια γίνετε αποσυμπίεση και υπολογίζει τον σχηματισμό μπλοκ και όσων αυτών υποδηλώνονται Bs(1). Υπολογίζεται η κλίση με την διαφορά S= Bs(1) -Bs(0).
   3. Έπειτα γίνετε η περικοπή της stego-εικόνας σε 4 στήλες. Το αποτέλεσμα που θα πάρουμε είναι η εικόνα που χρησιμοποιήθηκε για την βαθμονόμηση της κλίσης. Γίνεται συμπίεση της εικόνας χρησιμοποιώντας το πλέγμα κβαντοποίησης JPEG όπως στην stego – εικόνα. Μετά αποσυμπιέζει στο χωρικό πεδίο και υπολογίζει τον σχηματισμό των μπλοκ B(0).
   4. Στη συνέχεια χρησιμοποιώντας τον αλγόριθμο OutGuess, ενσωματώνεται το μέγιστο μήκος στην περικομμένη εικόνα και υπολογίζει τα μπλοκ B(1).
   5. Από το προηγούμενο βήμα χρησιμοποιούμαι την εικόνα και με τη χρήση πάλι του OutGuess, γίνετε η ενσωμάτωση του μέγιστου μήκος του μηνύματος στα μπλοκ που υποδηλώνονται B1(1).
   6. Τέλος γίνετε ο υπολογισμός του μηνύματος χρησιμοποιώντας την εξίσωση

      $$p = \frac{S_0 - S}{S_0 - S_1}.$$

      Η κλίση $S_0$=B(1)- B(0) είναι αυτό που περιμένουμε να είναι η αρχική εικόνα (p=0). Η κλίση $S_1$=B1(1)-B(1) είναι αυτό που περιμένουμε να πάρουμε με την ενσωμάτωση του μέγιστου μήκους μηνύματος στην εικόνα(p=1), Η κλίση S= Bs(1) – Bs(0) για την stego- εικόνα ανάμεσα σε στις δύο

προηγούμενες κλίσεις άρα ισχύει $S \in [S1,S0]$, που αντιστοιχεί σε ένα άγνωστο μήκος μηνύματος. Γίνετε χρήση γραμμικής παρεμβολής για να αποκτήσουμε τον τύπο που θα μας δώσει το p, $S = S0 – p(S0 – S1)$.

# ΚΕΦΑΛΑΙΟ 4

## Στεγανογραφικά εργαλεία (Steganography tools)

### 4.1 Στεγανογραφικά εργαλεία

Τα παρακάτω προγράμματα μπορούν να εγκατασταθούν σε διάφορα λειτουργικά συστήματα (Windows, Linux, Macintosh), ενώ τα αρχεία προς απόκρυψη ενσωματώνονται σε εικόνες BMP, JPG, GIF κα. Άλλος γνωστός τρόπος απόκρυψης πληροφορίας, είναι αυτός της χρήσης αρχείων ήχου όπως WAV, PCM, AVI, MIDI, MPEG, MP3, RIFF, και VOC. Στο διαδίκτυο υπάρχουν πολλά στεγανογραφικά εργαλεία τα όποια είναι διαθέσιμα δωρεάν για τον κάθε ένα.

Παρακάτω αναφέρω μερικά από τα πιο γνωστά στεγανογραφικά εργαλεία:

**Jphide-and-Jpseek :** Το Jphide-and-Jpseek επιτρέπει την απόκρυψη ενός αρχείου (π.χ. αρχείο κειμένου με κατάληξη .txt) σε εικόνες τύπου jpeg. Πολύ εύκολο στη χρήση του και αποτελεσματικό, εφόσον το αποτέλεσμα δεν έχει διαφορά με την αρχική εικόνα. Όταν το αρχείο που κρύβουμε καταλαμβάνει μικρό ποσοστό της εικόνας και ο χρήστης δεν έχει την αρχική εικόνα, είναι σχεδόν αδύνατον να καταλάβει κάποιος ότι η εικόνα περιέχει κρυφό μήνυμα. Αν τώρα η αλλαγή στην εικόνα είναι μεγαλύτερη από 15% τότε η αλλαγή είναι ορατή με γυμνό μάτι.

**WbStego :** δίνει την δυνατότητα απόκρυψης κάθε τύπου αρχείου σε εικόνες bitmap, για παράδειγμα HTML και PDF. Οι αλλαγές στο αρχείο που έχει στεγανογραφηθεί δεν διακρίνονται.

**StegoVideo :** δίνει την δυνατότητα να κρύψουμε αρχεία σε ένα αρχείο βίντεο. Επίσης μετά τη συμπίεση ο αλγόριθμος που χρησιμοποιεί επιτρέπει τη μικρότερη δυνατή απώλεια δεδομένων.

**S-Tools :** εκτελεί απόκρυψη αρχείων και φακέλων χρησιμοποιώντας τη στεγανογραφία μέσα σε εικόνες τύπου BMP, GIF καθώς και αρχεία μουσικής τύπου WAV. Οι αλλοιώσεις που προκαλούνται δεν είναι αισθητές.

**Steganos 3 :** Χρησιμοποιεί μια σειρά τεχνικών στεγανογράφησης και κρυπτογράφησης για την απόκρυψη δεδομένων είτε σε αρχεία ήχου είτε σε εικόνες. Παρέχει μια σειρά επιπρόσθετων δυνατοτήτων για την προστασία των σημαντικών εγγράφων.

**OpenPuff :** Είναι μια εύχρηστη εφαρμογή που σας επιτρέπει να κρύψει τα δεδομένα σε κρυπτογραφημένα αρχεία, προκειμένου να τα στείλετε σε άλλους χρήστες. Είναι πρόγραμμα της Microsoft Windows και θεωρείται "ανεξάρτητο πρόγραμμα". (www.softpedia.com/get/Authoring-tools/Authoring-Related/Puff.shtml). Μπορείτε να χρησιμοποιήσετε την εφαρμογή για να κρύψει τα αρχεία κειμένου, εικόνες ή άλλα αρχεία με μέγιστο μέγεθος 256 MB. Ωστόσο, το μέγεθος του μηνύματος επηρεάζει σημαντικά τον αριθμό των αρχείων φορέων που πρέπει να χρησιμοποιηθεί.

Για παράδειγμα, για να στείλετε ένα σύντομο αρχείο κειμένου θα πρέπει να έχετε περίπου τρεις εικόνες ως φορείς. Για μεγαλύτερα αρχεία θα πρέπει να έχετε περισσότερα αρχεία φορείς (δημιουργία αλυσίδας Carrier) ή μεγαλύτερα αρχεία φορείς. Όταν στέλνετε ένα αρχείο, μπορείτε να κρυπτογραφήσετε τις πληροφορίες χρησιμοποιώντας μέχρι και τρεις κωδικούς πρόσβασης και ορίζοντας τη σειρά των αρχείων που θα μεταφέρουν την πληροφορία.

Ο παραλήπτης πρέπει να έχει όλους τους κωδικούς πρόσβασης και να γνωρίζει την ακριβή σειρά των αρχείων. Εάν ένα στοιχείο(είτε κωδικός είτε ένα αρχείο) λείπει τότε οι πληροφορίες δεν μπορούν να ανακτηθούν. Αυτή η εφαρμογή μπορεί επίσης να χρησιμοποιηθεί από μια αφαιρούμενη συσκευή(portable), δεν χρειάζεται την εγκατάσταση της εφαρμογής για να αφήσει ίχνη στο μητρώο του υπολογιστή. Το interface είναι εύκολο στη χρήση και εμφανίζει τα βήματα που απαιτούνται για να κρυπτογραφήσετε τα αρχεία. Παρέχει μεγαλύτερη διακριτική ευχέρεια από ένα συμβατικό πρόγραμμα κρυπτογράφησης αρχείων αποκρύπτοντας τα δεδομένα σε κανονικά αρχεία και όχι χρησιμοποιώντας μια συγκεκριμένη επέκταση. (Εδώ για μεταφορά στην εκτέλεση του προγράμματος)

Υποστηρίζει ένα ευρύ φάσμα μορφών μεταφοράς όπως:

- Εικόνες **Bmp , Jpg , Png , Tga**
- Ήχοι **AIFF , Mp3 , Wav**
- Βίντεο **3gp , Mp4 , Mpeg I , MPEG-II , Vob**
- Flash-Adobe **Flv , Pdf , Swf**

**Υδατογράφηση** είναι η προσθήκη υπογραφής σε ένα αρχείο, είναι ένα συγκεκριμένο αναγνωριστικό σήμα που το προσθέτει ο ιδιοκτήτης του αρχείου, το αναγνωριστικό σήμα αλλιώς λέγεται πνευματικά δικαιώματα. Χρησιμοποιείται από ανθρώπους της τέχνης, ώστε να υπάρχει προστασία των έργων τους. Η πληροφορία μπορεί να είναι μέχρι 32 χαρακτήρες και να αφορούν στοιχεία ιδιοκτησίας του δημιουργού, όπως για παράδειγμα στοιχεία επικοινωνίας. Τα δεδομένα αυτά είναι αόρατα, αλλά δεν απαιτείται κωδικός για την ανάγνωση τους.

**StegoShare :** Το συγκεκριμένο πρόγραμμα υποστηρίζει μόνο εικόνες αλλά υποστηρίζει ένα ευρύ φάσμα τύπων εικόνων (png, jpg, bmp, gif, tiff etc.). Είναι διαθέσιμο δωρεάν στο διαδίκτυο (http://sourceforge.net/projects/stegoshare/). Οι εικόνες είναι καλύτερα να έχουν συγκεκριμένο θέμα (για παράδειγμα τα πουλιά, τα παλιά αυτοκίνητα, εργοστάσια, γέφυρες, πλοία κ.λπ.), μπορείτε επίσης να τραβήξετε τις δικές σας εικόνες με μία ψηφιακή φωτογραφική μηχανή. Επιλέξετε λήψη των εικόνων με τη μέγιστη ανάλυση, μπορείτε να κρύψετε περισσότερες πληροφορίες σε αυτές.

Μπορείτε να αλλάξετε την κλίμακα (ανάλυση αύξηση) φωτογραφίες με το GIMP για όχι περισσότερο από 150-200% (εξαρτάται από την ποιότητα των εικόνων). Η συνολική ανάλυση της εικόνας δείχνει πόσα bytes μπορεί να κρύψει (για παράδειγμα, αν η εικόνα έχει ανάλυση 1280x1024, έχει 1280 * 1024 = 1.310.720 pixels και μπορείτε να ενσωματώσετε σε αυτό περίπου 1,3 Mb κρυμμένη πληροφορία).

Μπορούμε να κρύψουμε αρχείο με μέγεθος μέχρι και 2GB και ο αριθμός των αρχείων carrier που μπορούμε να χρησιμοποιήσουμε είναι μέχρι 65536.

Η επιλογή των εικόνων, γίνετε με την επιλογή του φακέλου του βρίσκονται. Με το πάτημα του Hide, θα δημιουργηθεί αυτόματα ένας φάκελος μέσα στον ίδιο φάκελο με όνομα «out» που θα περιέχει τις νέες εικόνες. Επιτρέπεται να γίνει μετονομασία του φακέλου σε περίπτωση που θέλω να χρησιμοποιήσω τις ίδιες εικόνες για απόκρυψη διαφορετικού αρχείου πληροφορίας.

Μέσος όρος χωρητικότητας είναι 40% - για παράδειγμα αν έχω μέγεθος αρχείων 250MB μπορώ να ενσωματώσω σε αυτό αρχείο μέχρι 100MB.

Χρησιμοποιεί κρυπτογράφηση 128bit, για ακόμα πιο δύσκολη αποκρυπτογράφηση

Έχει πολύ καλή ποιότητα των αποτελεσμάτων εικόνων – δεν είναι αισθητές οι αλλοιώσεις στο ανθρώπινο μάτι.

Το συγκεκριμένο χρησιμοποιείται για την μεταφορά εικόνων μεταξύ ανώνυμων χρηστών(anonymous P2P). Δηλαδή δεν φαίνεται η τοποθεσία τους ή χρησιμοποιούν ψεύτικα ονόματα
(Εδώ για μεταφορά στην εκτέλεση του προγράμματος)

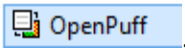
**OpenStego 0.6.1 :** Είναι λογισμικό ανοιχτού κώδικα και είναι διαθέσιμο δωρεάν στο διαδίκτυο(http://sourceforge.net/projects/openstego/?source=typ_redirect).
(Εδώ για μεταφορά στην εκτέλεση του προγράμματος)

Υποστηρίζει δύο κύριες λειτουργίες:

- Data Hiding: Μπορεί να κρύψει οποιουδήποτε τύπου αρχεία σε αρχεία εικόνας αλλά και να εξάγει αυτά. Επιπλέον δίνει τη δυνατότητα να χρησιμοποιήσουμε περισσότερες από μία εικόνα, δηλαδή σε περισσότερα από ένα αρχεία εικόνας να ενσωματωθεί η ίδια πληροφορία.
- Watermarking (Beta): Μπορούμε να υδατογραφήσουμε και να επιβεβαιώσουμε την ψηφιακή υπογραφή που έχουμε φτιάξει. Πρώτα δημιουργούμε το αρχείο με την ψηφιακή υπογραφή (αρχείο με κατάληξη .sig) στη συνέχεια το ενσωματώνουμε στα αρχεία που θέλουμε.

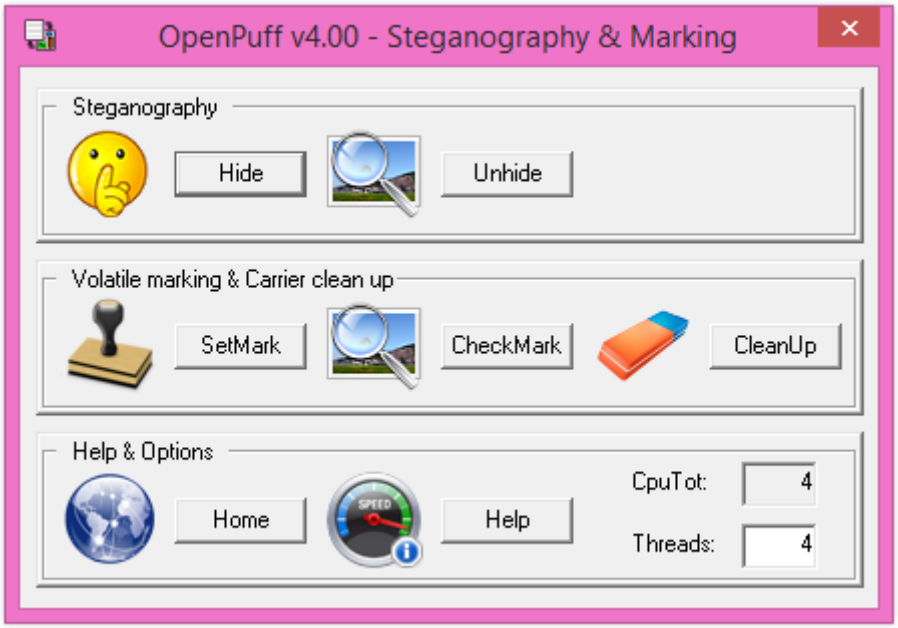
## 4.2 Εφαρμογές στεγανογραφίας

### *4.2.1 OpenPuff*

Κατεβάζουμε το πρόγραμμα από το διαδίκτυο. Κάνουμε extract τα αρχεία του zip για παράδειγμα στην επιφάνεια εργασίας. Για να ξεκινήσει το πρόγραμμα κάνουμε διπλό κλικ στο 

.

Το πρόγραμμα έχει την εξής μορφή:




*Εικόνα 11 OpenPuff*

Πατώντας το κουμπάκι Hide μας εμφανίζει το επόμενο παράθυρο. Πριν προχωρήσω θα κάνω μια σύντομη περιγραφή για το τι εμφανίζει αυτό.

**Στο βήμα 1:** Όπως παρατηρούμε μας ζητάει να δώσουμε τρεις κωδικούς που να μην συνδέονται με κάποιο τρόπο μεταξύ τους (min 8, max 32) και δείχνει την συνάρτηση που θα χρησιμοποιήσει για το τελικό κλειδί με το οποίο θα γίνει η κρυπτογράφηση. Μπορούμε επίσης να χρησιμοποιήσουμε τους δύο ή μόνο ένα κωδικό, (είναι φυσικά λιγότερο ασφαλές), μη επιλέγοντας τις επιλογές Enable (B),(C).

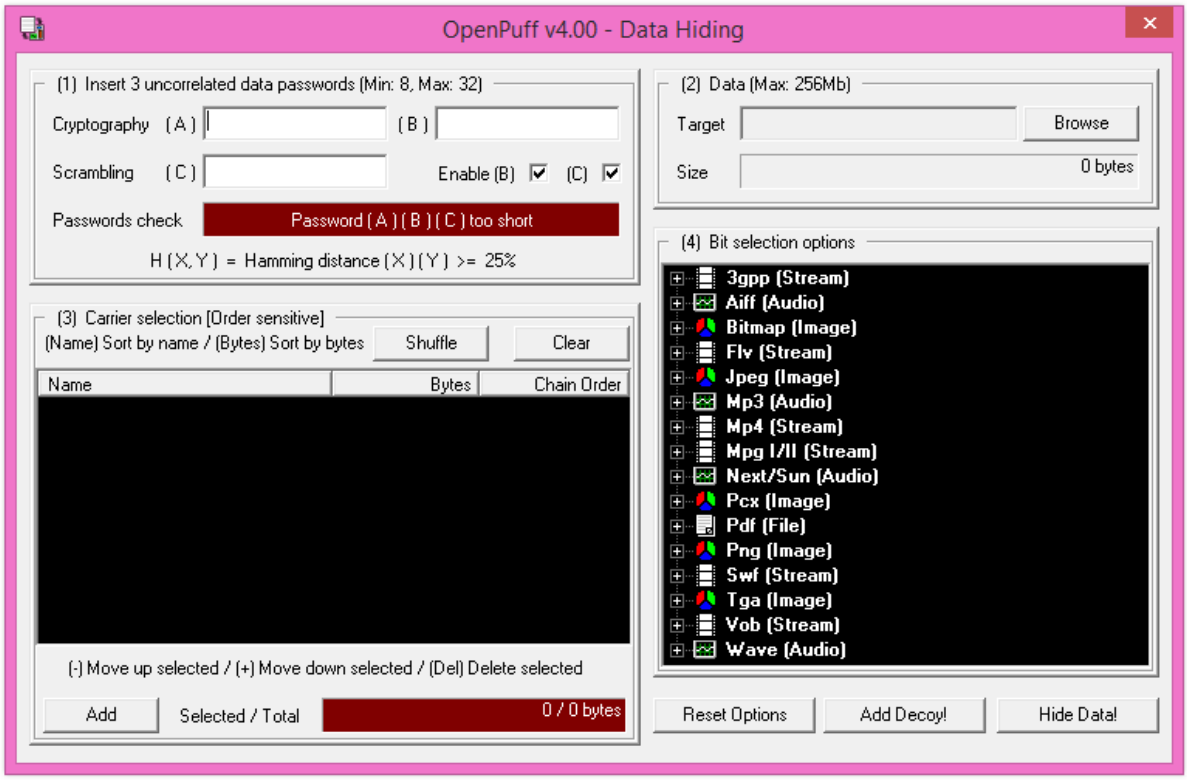
**Στο βήμα 2 :** Πατώντας το Browse γίνετε η επιλογή του αρχείου που θέλουμε να κρύψουμε.

**Στο βήμα 3 :** Στο βήμα αυτό επιλέγουμε το αρχείο ή τα αρχεία (ίδιου ή διαφορετικού τύπου), στα οποία θέλουμε να ενσωματώσουμε το αρχείο από το βήμα 2.

**Στο βήμα 4 :** Επιλέγουμε το τύπο του και την ποιότητα (την ποσότητα της πληροφορίας) που θέλουμε έχει η τελική εικόνα. Για παράδειγμα αν το αρχείο Carrier είναι εικόνα .bmp τότε και το αρχείο που θα δημιουργήσουμε με το κρυμμένο αρχείο θα είναι .bmp. Μπορούμε να επιλέξουμε πόση πληροφορία θέλουμε να ενσωματώσουμε στο αποτέλεσμα με το επιλέξουμε μια επιλογή από τον παρακάτω πίνακα. Αν το αφήσουμε στην προεπιλογή για κάθε τύπο αρχείου είναι 20% - Medium.

| | |
|---|---|
| (*Minimum*) | 1/8 data, 7/8 whitening. |
| (*Very Low*) | 1/7 data, 6/7 whitening. |
| (*Low*) | 1/6 data, 5/6 whitening. |
| (*Medium*) | 1/5 data, 4/5 whitening. |
| (*High*) | 1/4 data, 3/4 whitening. |
| (*Very High*) | 1/3 data, 2/3 whitening. |
| (*Maximum*) | 1/2 data, 1/2 whitening. |

*Εικόνα 12 Bits selection level*




*Εικόνα 13 Εμφάνιση παραθύρου για απόκρυψη πληροφορίας*

Το επόμενο που θα κάνουμε είναι να δώσουμε τις πληροφορίες και τα αρχεία που χρειάζονται, ώστε να πραγματοποιηθεί η απόκρυψη του αρχείου.

**Στο βήμα 1 :** Στο παράδειγμα αυτό ο κωδικός είναι *: (A)* : 456asdf8

Όπως θα παρατηρήσουμε με το που γράψαμε τον κωδικό και μη επιλέγοντας τις επιλογές *Enable (B), (C),* η μπάρα από κάτω έγινε πράσινη και το ποσοστό επιτυχίας του κλειδιού είναι άνω των 25%, αυτό σημαίνει ότι το κλειδί είναι αρκετά δυνατό.

**Στο βήμα 2 :** Πατώντας το Browse επιλέγουμε το αρχείο, το οποίο στο παράδειγμα μας είναι ένα αρχείο κειμένου με κατάληξη .txt.

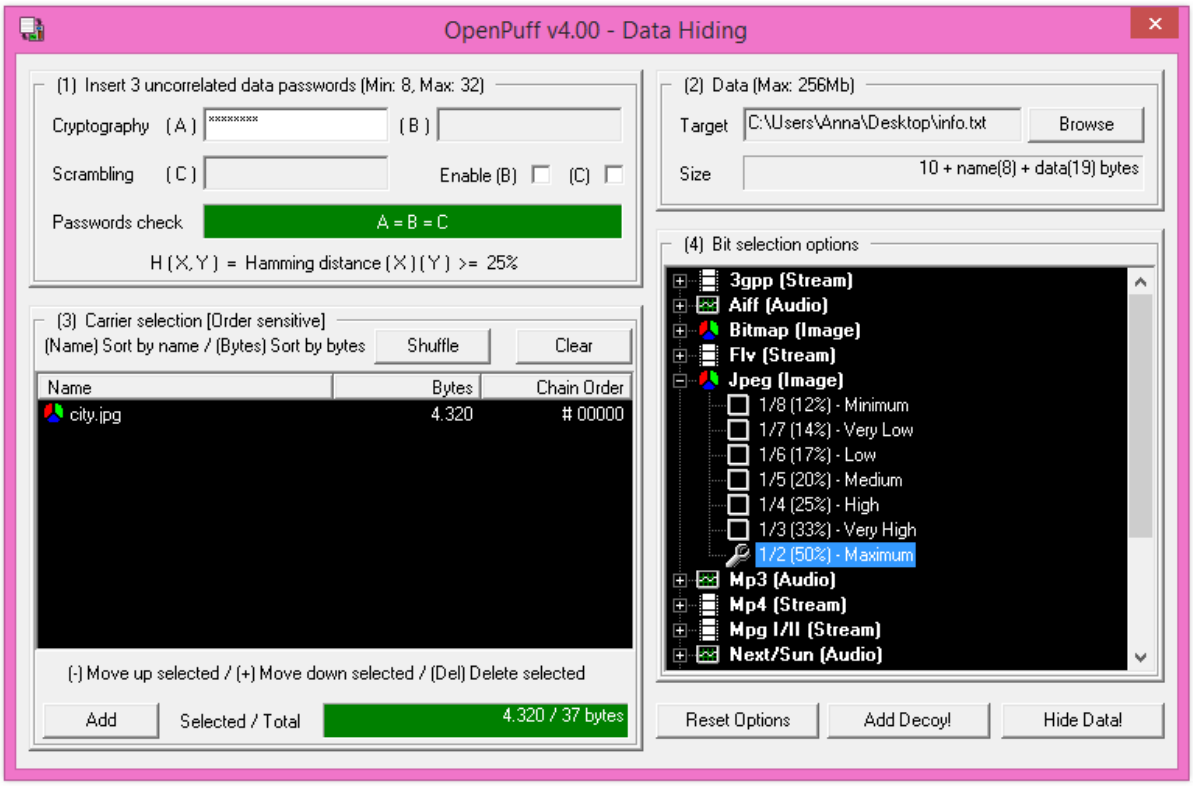
Με το που γίνει η επιλογή του αρχείου, εμφανίζει τα Bytes που θα πρέπει να ενσωματωθούν. Βλέπουμε ότι είναι 10+8+19=37 bytes.

**Στο βήμα 3 :** Εδώ γίνετε η επιλογή του αρχείου, στο οποίο θέλουμε να ενσωματώσουμε το αρχείο από το βήμα 2. Το πρόγραμμα αυτόματα υπολογίζει πόσα bytes χρειάζεται για να μπορέσει να κρύψει

το αρχείο με τις πληροφορίες. Υπάρχει μπάρα *Selected/Total*, αν η μπάρα χρωματιστεί με πράσινο τότε μπορούμε να προχωρήσουμε.

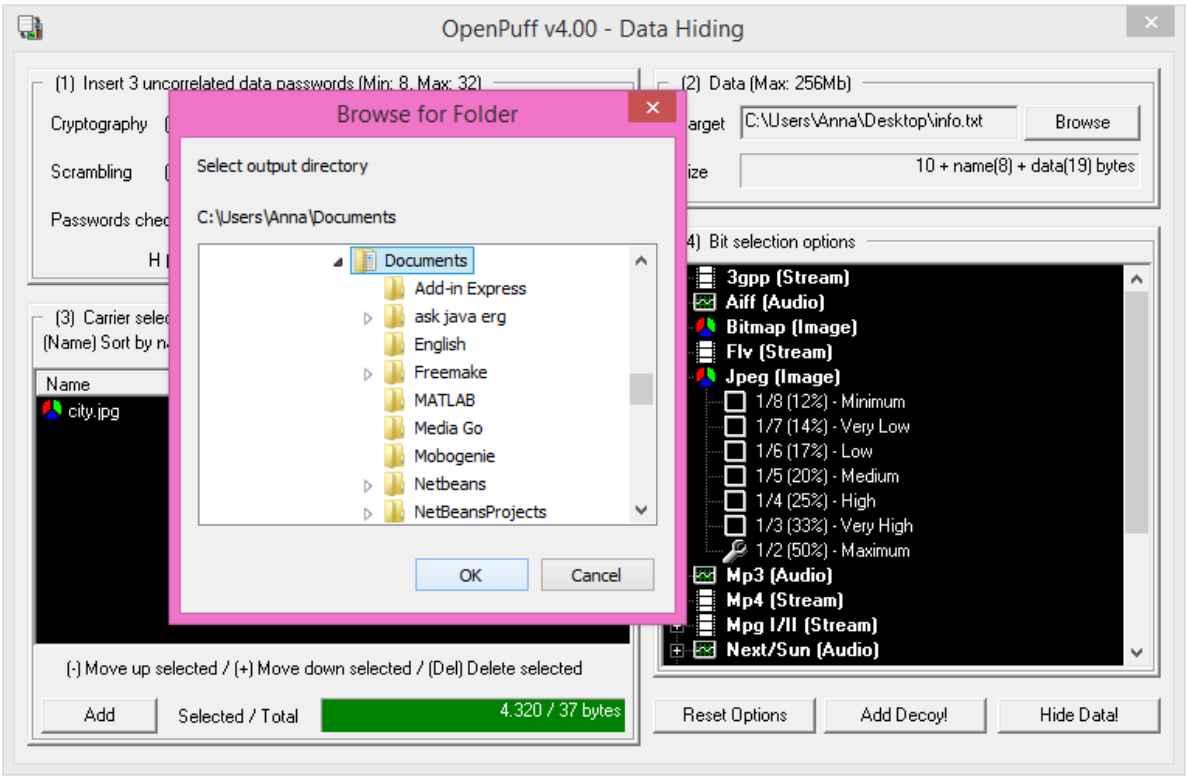
**Στο βήμα 4 :** Στο παράδειγμα αυτό το αρχείο carrier είναι μία εικόνα .jpg, άρα θα επιλέξουμε από το πίνακα *jpeg(image)* και το ποσοστό που θέλουμε, επέλεξα να έχει την καλύτερη ποιότητα (50%).

Άρα όταν τα έχουμε συμπληρώσει όλα το αποτέλεσμα είναι η παρακάτω εικόνα



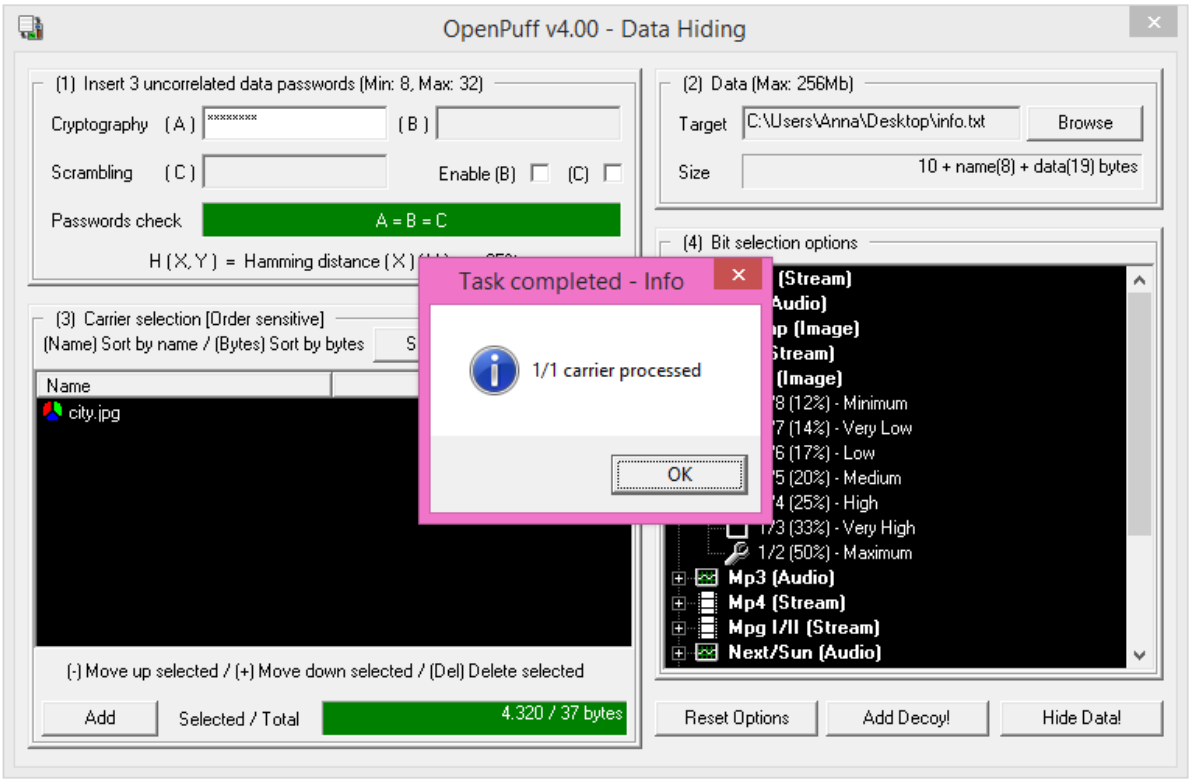

*Εικόνα 14 Settings for Hide Data*

Πατώντας *Hide Data*, επιλέγουμε που θέλουμε να αποθηκευτεί το αποτέλεσμα/νέα εικόνα πχ στα έγγραφα μου.

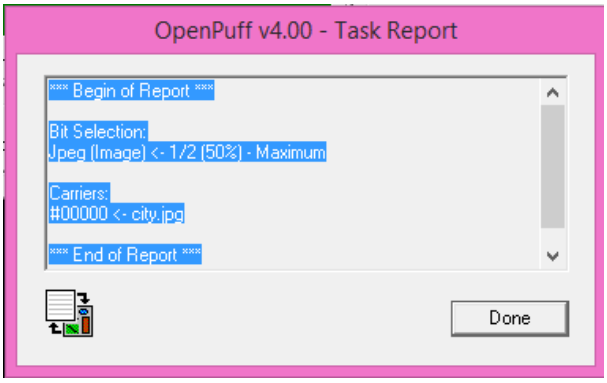



*Εικόνα 15 Επιλογή τοποθεσίας αποθήκευσης*

Στη συνέχεια μας εμφανίζει ότι η διαδικασία έγινε με επιτυχία




*Εικόνα 16 Επιτυχής διαδικασία*




*Εικόνα 17 End-Report OpenPuff*

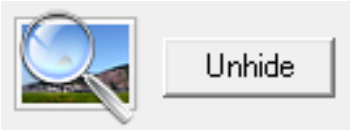
Το Task Report μας δίνει πληροφορίες σχετικά με την διαδικασία που ακολουθήσαμε.

Jpeg(image)← ½(50%) medium

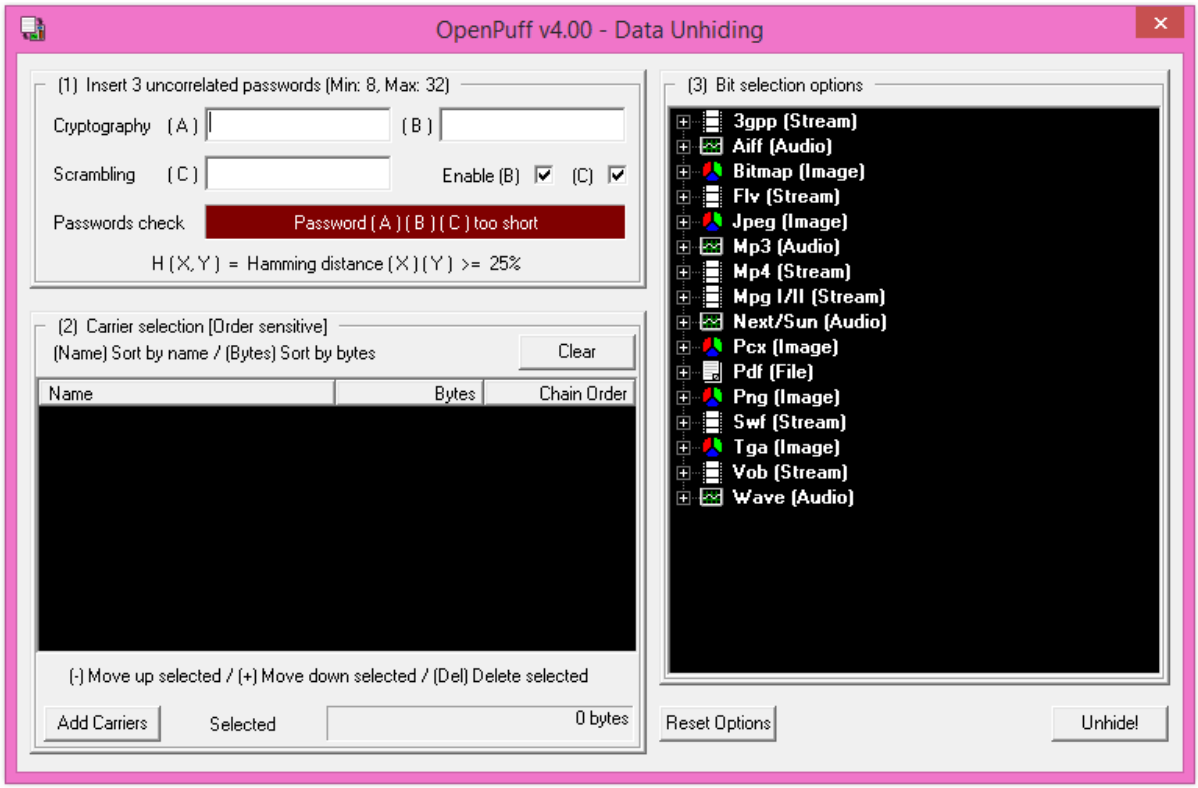
Χρησιμοποιήσαμε εικόνα τύπου Jgep με ποσοστό ποιότητας 50% και ότι χρησιμοποιήσαμε ένα αρχείο με όνομα city.jpg

Τώρα για να εξάγουμε το αρχείο από την εικόνα η διαδικασία είναι η εξής:

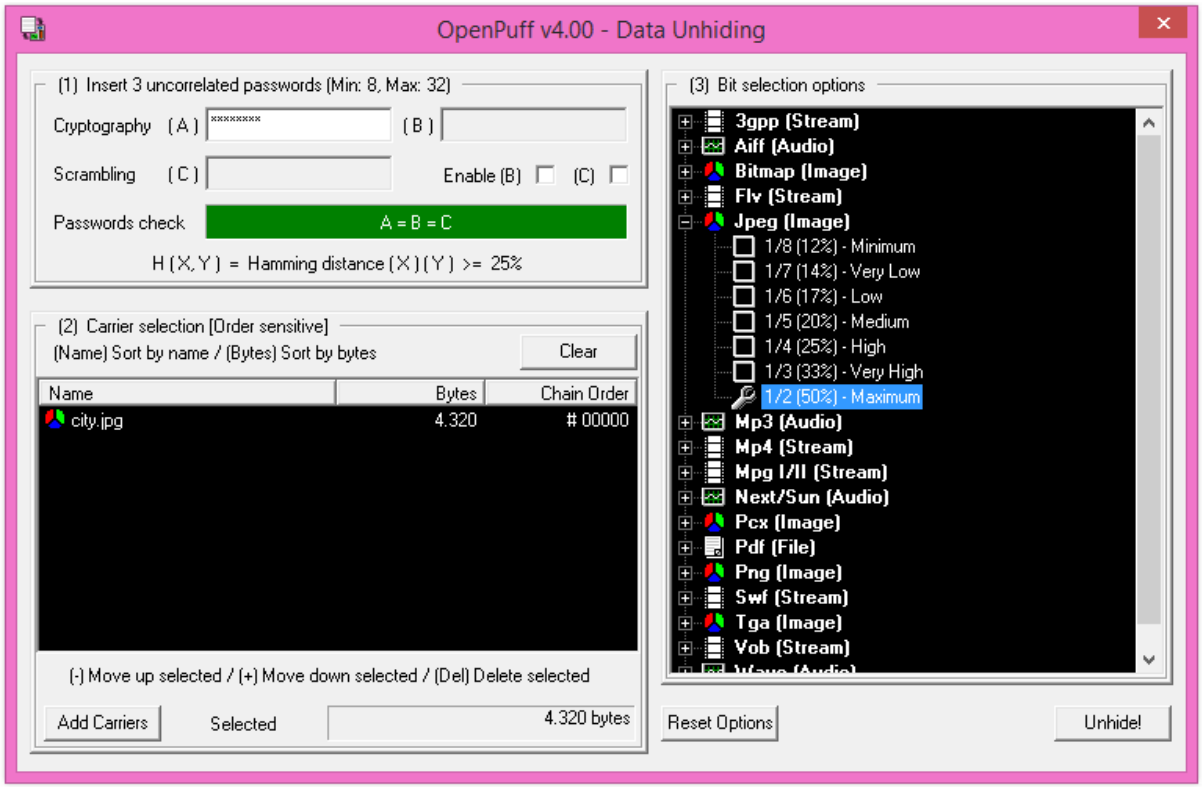
Πατάμε το κουμπάκι *unhide*.



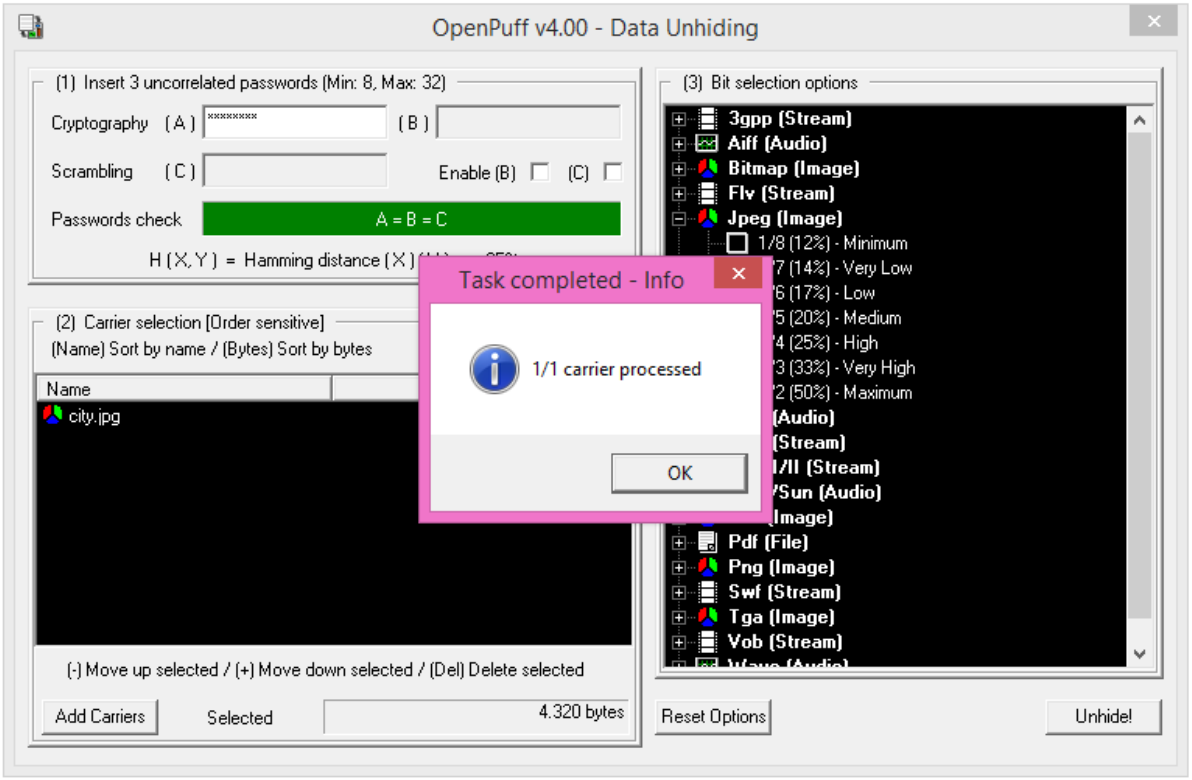

Πατώντας το *unhide* μας εμφανίζει το επόμενο παράθυρο. Πάλι υπάρχουν βήματα που πρέπει να ακολουθήσουμε. Στο πρώτο βήμα μας ζητάει  τον κωδικό (ή τους κωδικούς σε άλλη περίπτωση) που χρησιμοποιήσαμε για την απόκρυψη και το αρχείο εικόνας που περιέχει την πληροφορία.
Στο δεύτερο βήμα επιλέγουμε τα αρχεία που κρύψαμε την πληροφορία, στη περίπτωση αυτή είναι μόνο ένα αρχείο, αλλά αν είχαμε αλυσίδα, δηλαδή περισσότερα από ένα, θα έπρεπε να είναι επιλεγμένα με την ίδια σειρά όταν έγινε η κρυπτογράφηση.



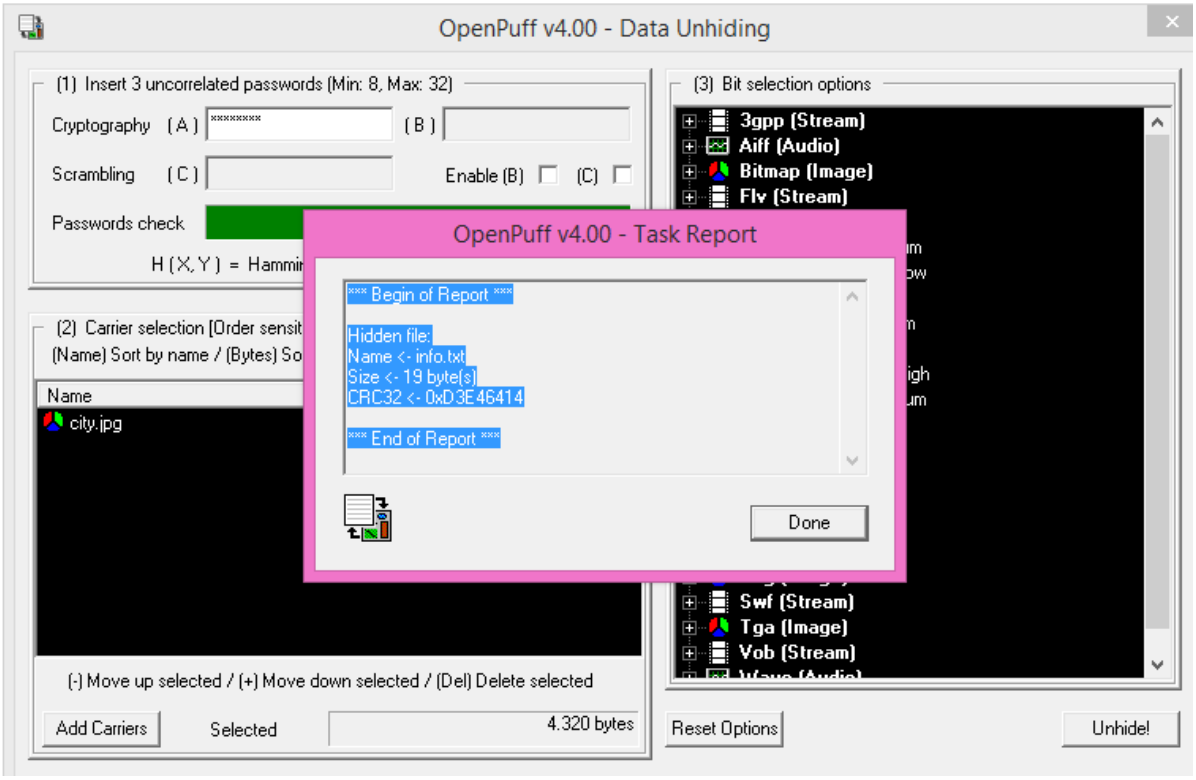

*Εικόνα 18 Επιλογή αρχείου για unhide*




*Εικόνα 19 Unhide*




*Εικόνα 20 Επιτυχής αποκρυπτογράφηση*




*Εικόνα 21 End-Report OpenPuff*

Στο Task Report παίρνουμε πληροφορίες σχετικά με την διαδικασία. Το κρυμμένο αρχείο είναι το info.txt με μέγεθος 19 bytes.

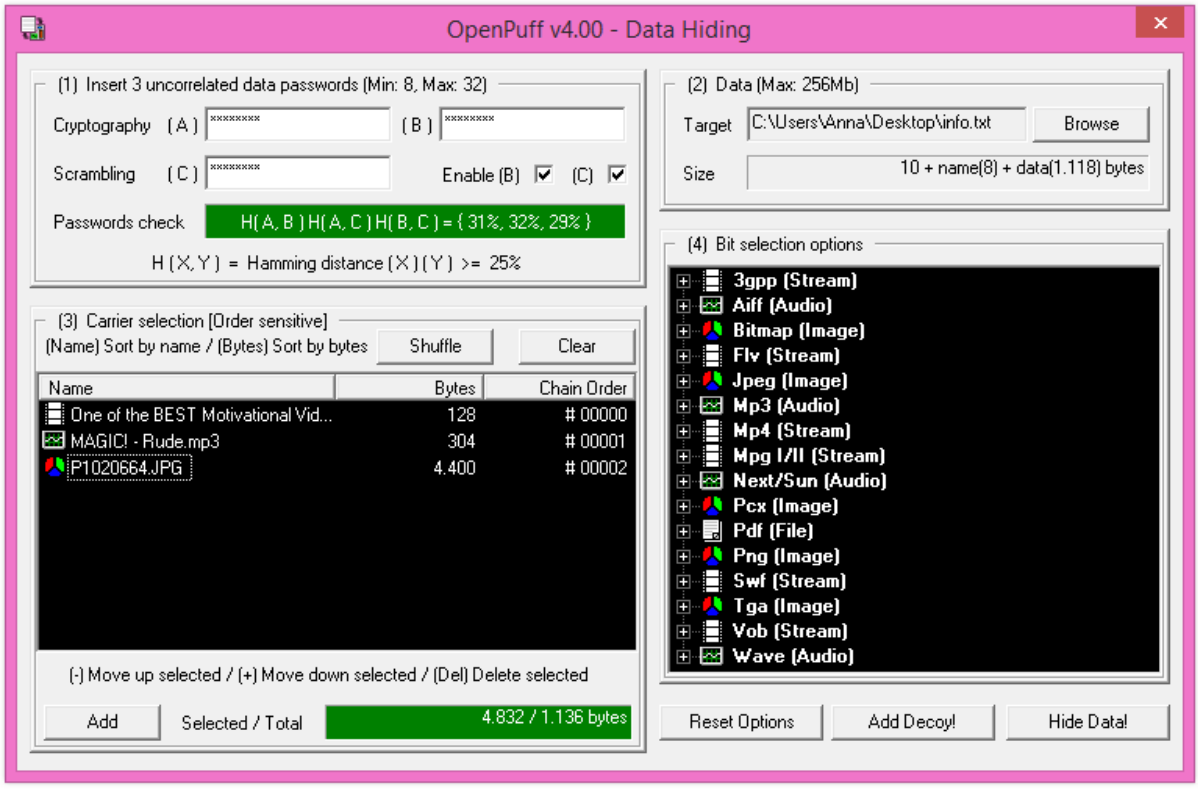
## Παράδειγμα 2

Το προηγούμενο παράδειγμα ήταν η πιο απλή χρήση του προγράμματος, θα δείξω ένα πιο περίπλοκο για να δούμε και την δημιουργία της αλυσίδας Carrier.

Στο βήμα 1 που μας ζητάει τους κωδικούς τώρα θα συμπληρώσω και τις τρεις μπάρες.

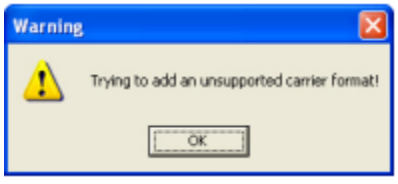
- A: madru879
- B: 98765432
- C: abcdef12

Το αρχείο με την πληροφορία είναι σινολογικά 1.118 Bytes και τα αρχεία που πρέπει να χρησιμοποιήσω ώστε να μπορέσει να «χωρέσει» είναι τα τρία αρχεία που έχω επιλέξει. Βέβαια όπως παρατηρώ θα μπορούσα να έχω χρησιμοποιήσει μόνο την εικόνα, αλλά θέλω να δείξω την δημιουργία αλυσίδας αρχείων. Έχω λοιπόν επιλέξει τρία διαφορετικού τύπου αρχεία (βίντεο, εικόνα και μουσικό κομμάτι).



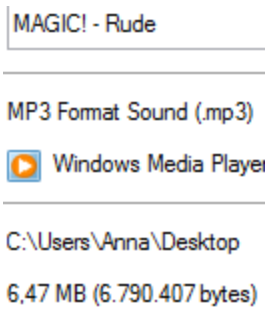

Αν προσπαθήσουμε να επιλέξουμε πολύ μικρά αρχεία, μας προειδοποιεί με το παρακάτω μήνυμα.


Ή αν προσπαθήσουμε να επιλέξουμε αρχείο που δεν υποστηρίζεται από το πρόγραμμα τότε μας εμφανίζει το παρακάτω μήνυμα.

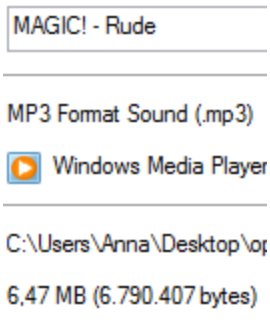



Εφόσον έχουμε τελειώσει με τις ρυθμίσεις και πατήσουμε Hide data, μπορούμε να δούμε και να ελέγξουμε τα αποτελέσματα.

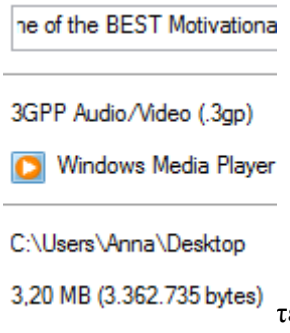
Σύγκριση αποτελεσμάτων:



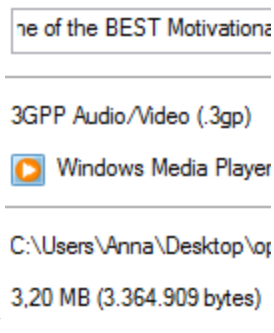

Αρχική1



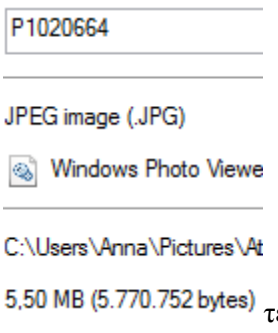

τελικη1



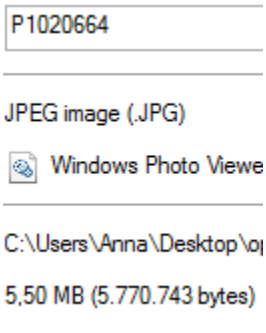

Αρχική2




τελική2

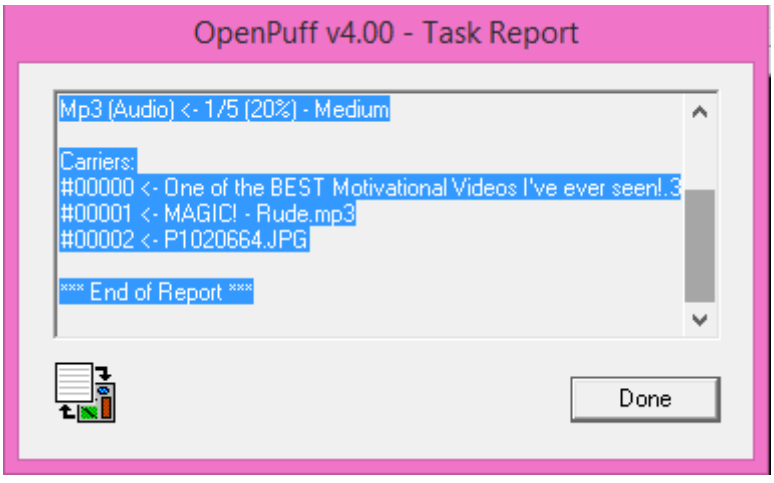



Αρχική3

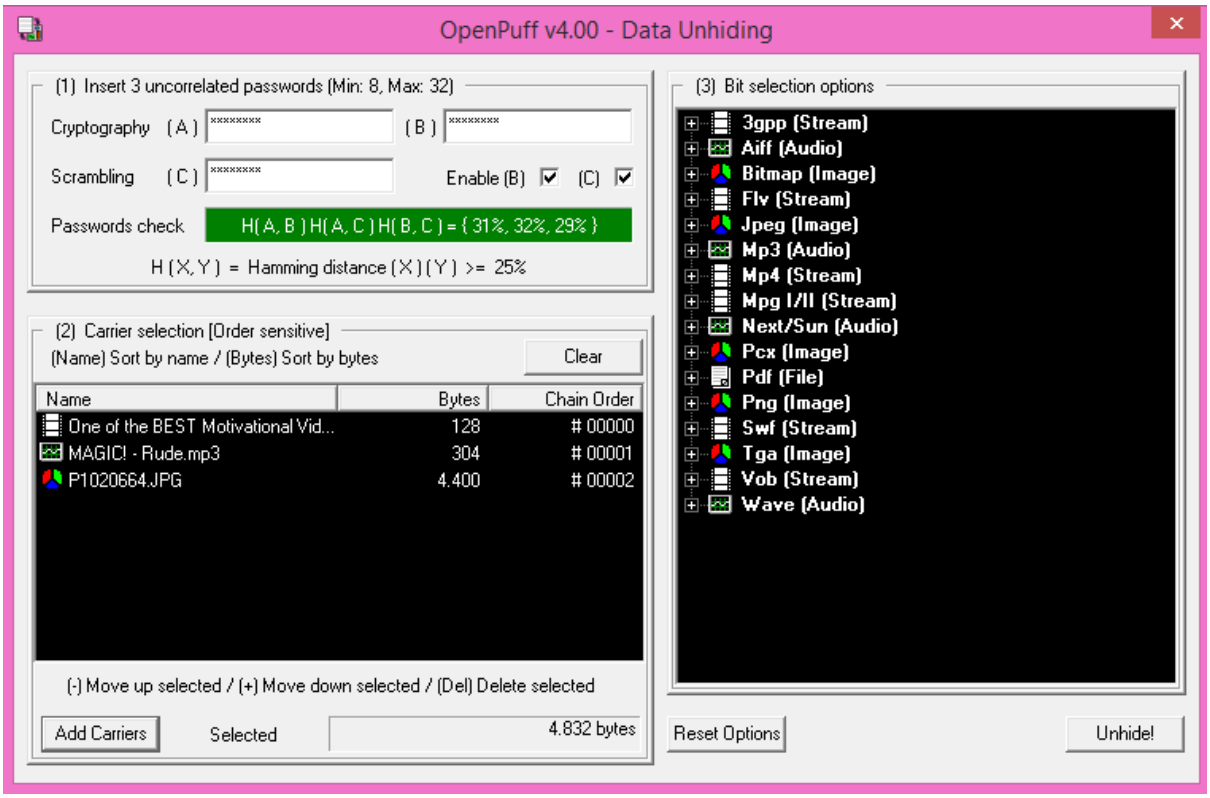



τελική3

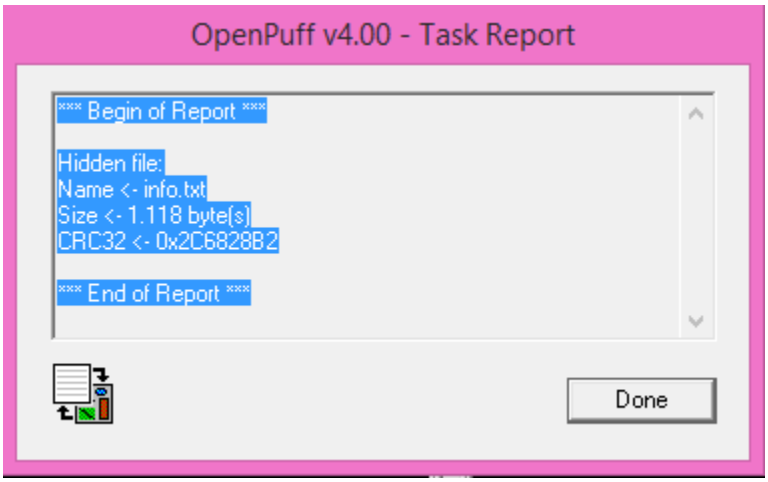
Το αρχείο που επέλεξα να κρύψω δεν ήταν μεγάλο, οπότε η πληροφορία αποθηκεύτηκε μόνο στο αρχείο βίντεο (.3gp), επίσης υπάρχει μία μικρή μείωση μεγέθους στο αρχείο εικόνας επειδή η ποιότητα ήταν στην προεπιλογή (20%).



Η ποιότητα είναι 20% (medium - προεπιλογή), μας εμφανίζει επίσης και την «αλυσίδα αρχείων», είναι η σειρά που επιλέχτηκαν τα αρχεία.

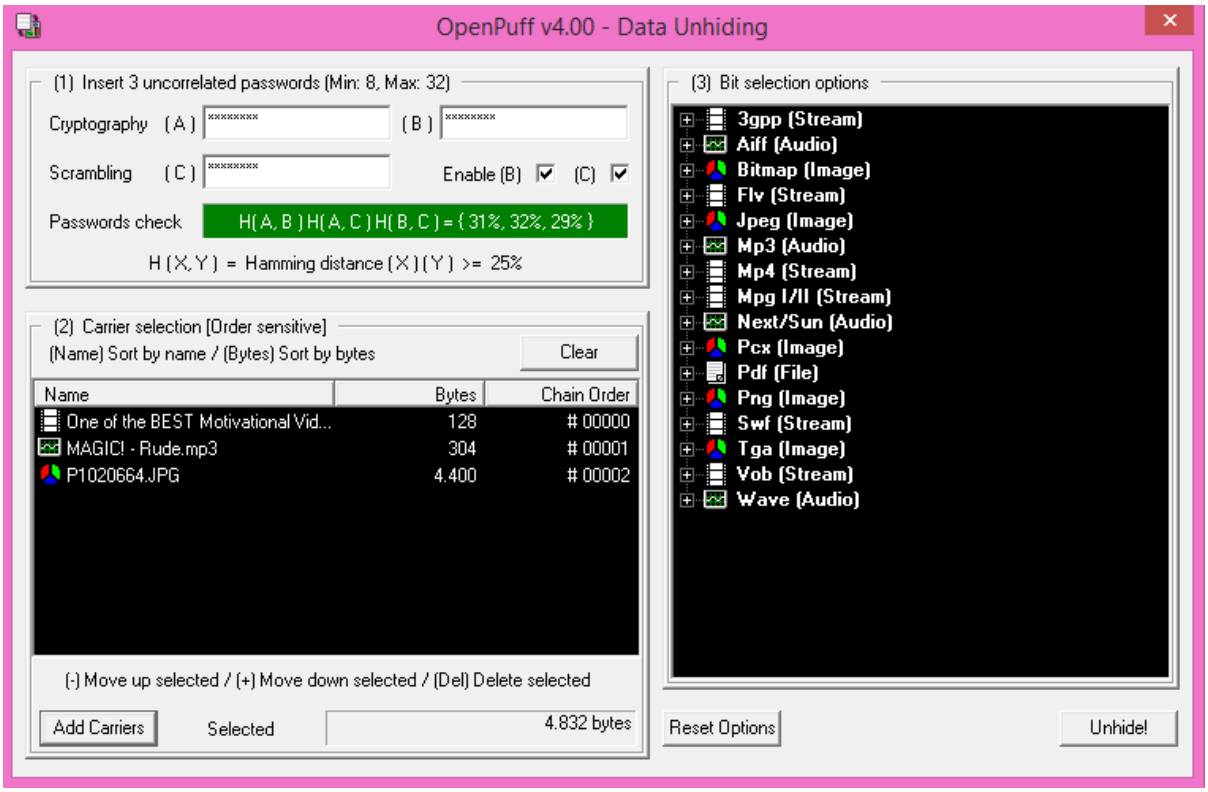



Πατάμε το κουμπί *Unhide!*

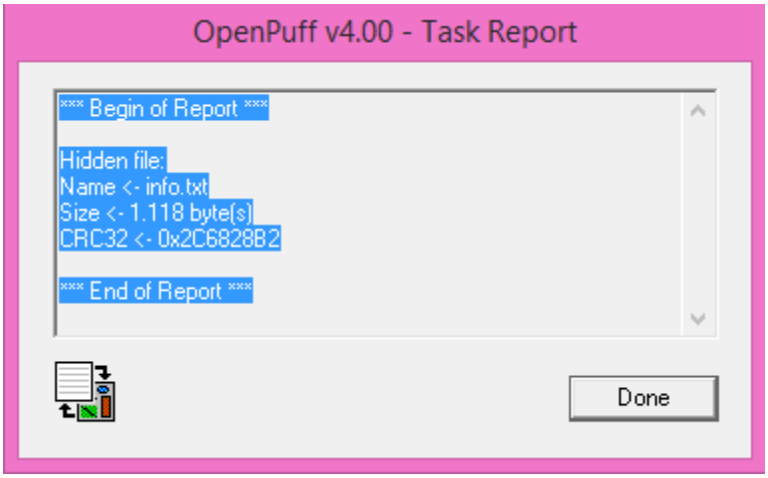



Και μας δίνει το Task Report με το όνομα και το μέγεθος του κρυμμένου αρχείου.

Για την αντιστροφή διαδικασία, εξαγωγή αποτελέσματος. Συμπληρώνουμε τους κωδικούς και επιλέγουμε με την ίδια σειρά τα αρχεία που είχα χρησιμοποιήσει προηγουμένως.




Στη συνέχεια πατάμε *Unhide!* Στην τελική αναφορά που παίρνουμε, εμφανίζεται το όνομα του αρχείου που ενσωμάτωσα info.txt.



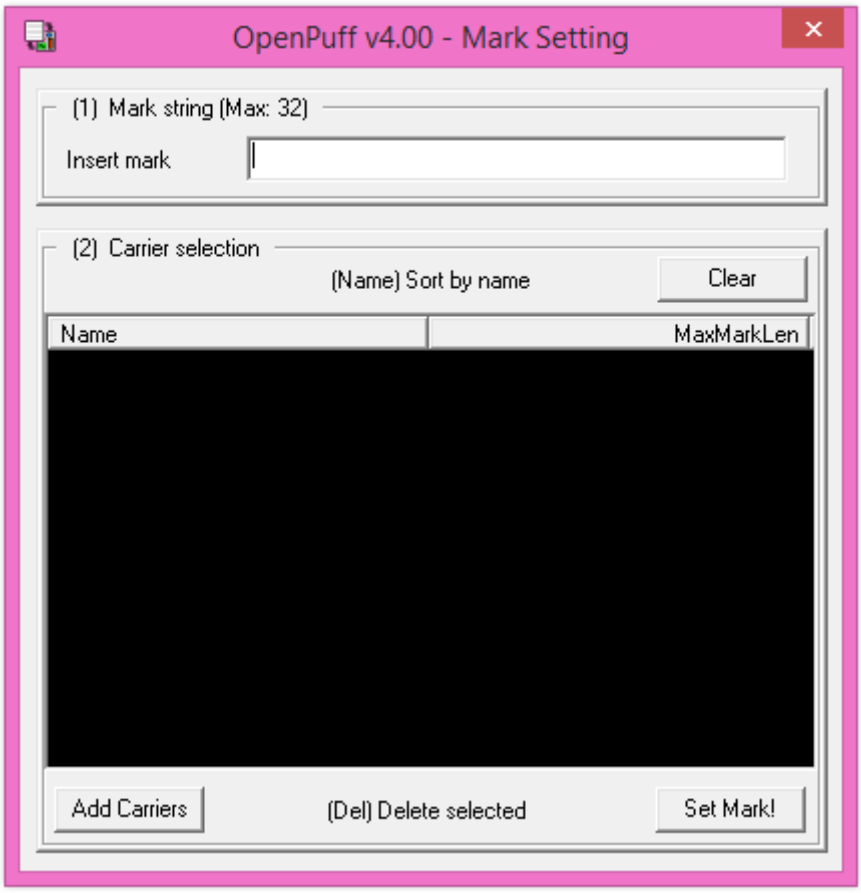

Και πάλι μας δίνει τις πληροφορίες του αρχείου που βρήκε κρυμμένο.

## Marking

Για να προσθέσουμε πνευματικά δικαιώματα και να δημιουργήσουμε **υδατογράφημα** σε ένα ή περισσότερα αρχεία , πατάμε το κουμπί *SetMark*

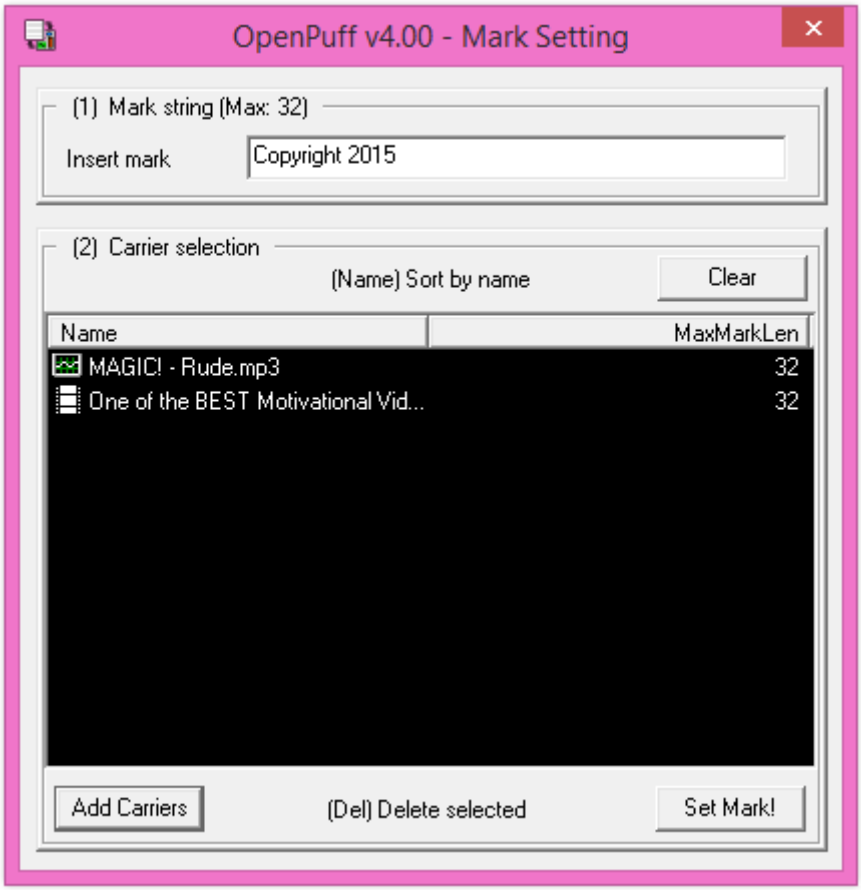

το οποίο μας ανοίγει την παρακάτω καρτέλα.

Όπως παρατηρούμε, η διαδικασία αποτελείται από δύο στάδια. Στο πρώτο στάδιο συμπληρώνουμε το κείμενο με τις πληροφορίες πνευματικών δικαιωμάτων και στο δεύτερο προσθέτουμε τα αρχεία στα οποία θέλουμε να προσθέσουμε τις πληροφορίες αυτές.



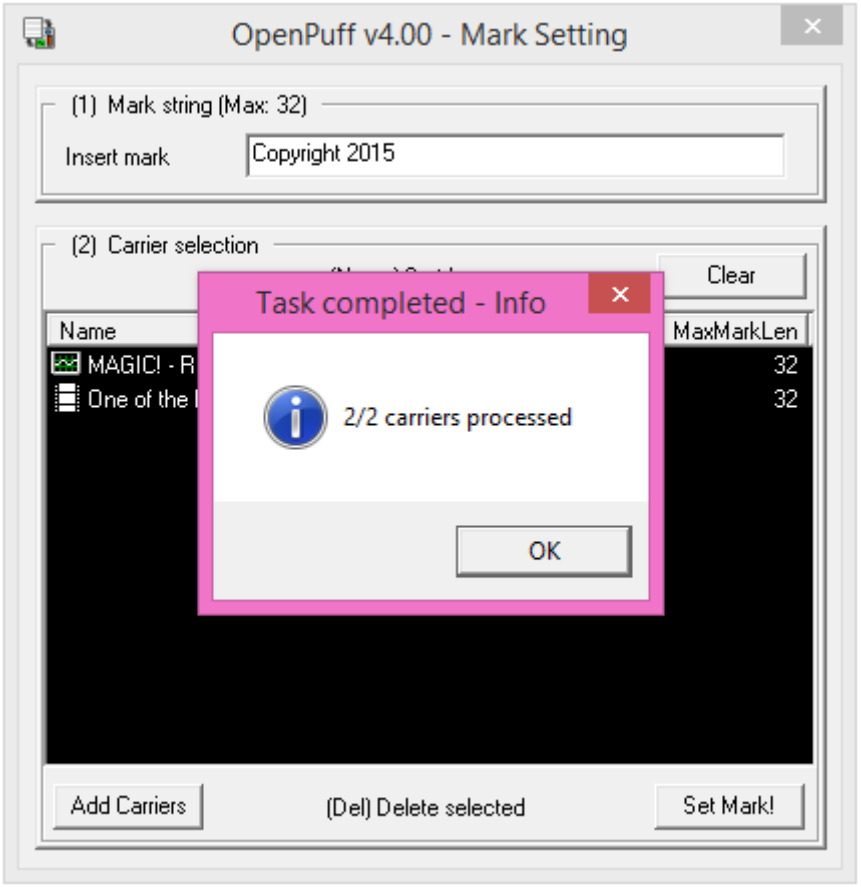

*Εικόνα 22 Παράθυρο για δημιουργία Watermarking*

Στο παράδειγμα αυτό θα χρησιμοποιήσω τη χαρακτηριστική φράση Copyright 2015, αποτελούμενη από 14 χαρακτήρες, την οποία θα ενσωματώσω ταυτόχρονα σε δύο αρχεία(.3gp και .mp3).




*Εικόνα 23 Επιλογή αρχείων carrier*

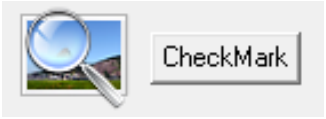
Στη συνέχεια πατάμε *Set Mark!* και θα επιλέξουμε που επιθυμούμε να αποθηκεύσουμε τα νέα αρχεία.

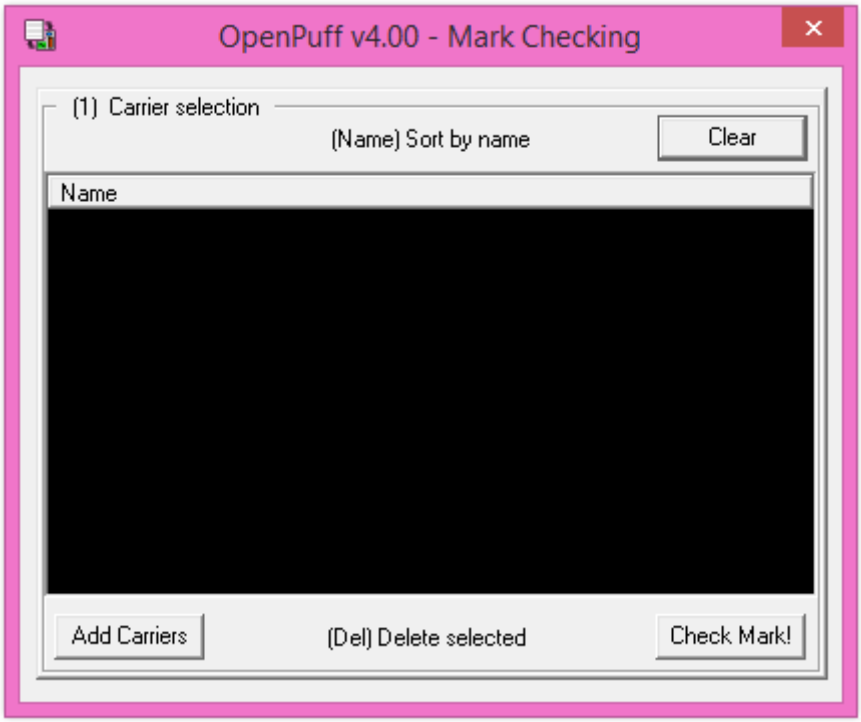



*Εικόνα 24 Επιτυχής διαδικασία*

Μετά το τέλος της διαδικασίας συγκρίνοντας τα δύο αρχεία που χρησιμοποιήσαμε σαν είσοδο, βλέπουμε ότι δεν έχουν καμία διαφορά στο μέγεθος.

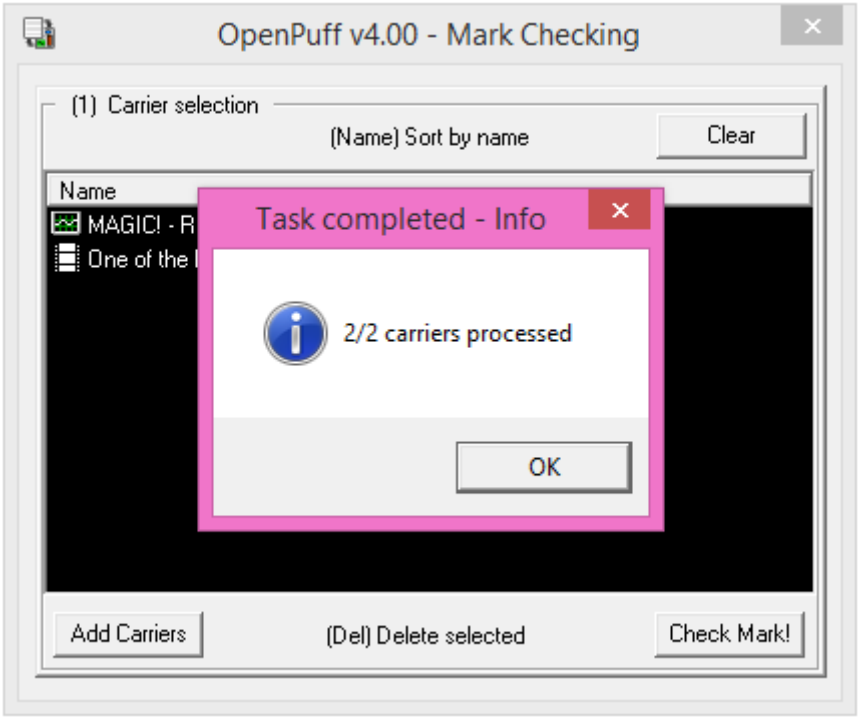
Αν θέλουμε να δούμε τη πληροφορία αυτή, δεν έχουμε παρά να επιλέξουμε



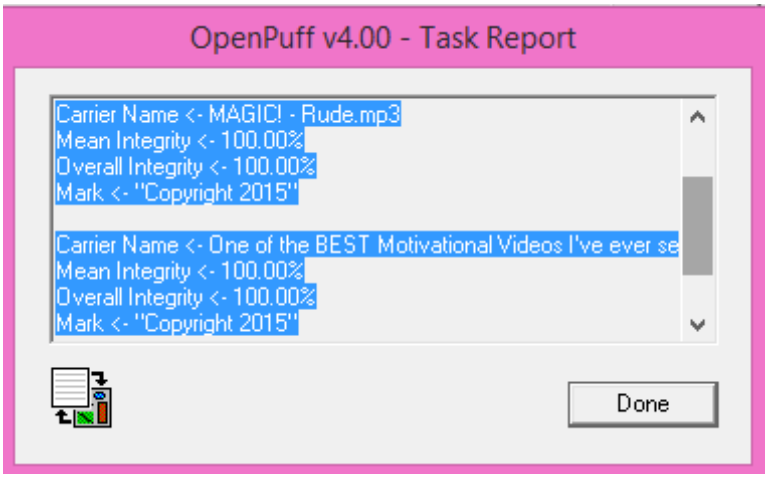



*Εικόνα 25 Επιλογή αρχείων για έλεγχο watermarking*

Προσθέτουμε τα αρχεία που θέλουμε να επιβεβαιώσουμε το watermarking που περιέχουν και στη συνέχεια πατάμε *Check Mark!*



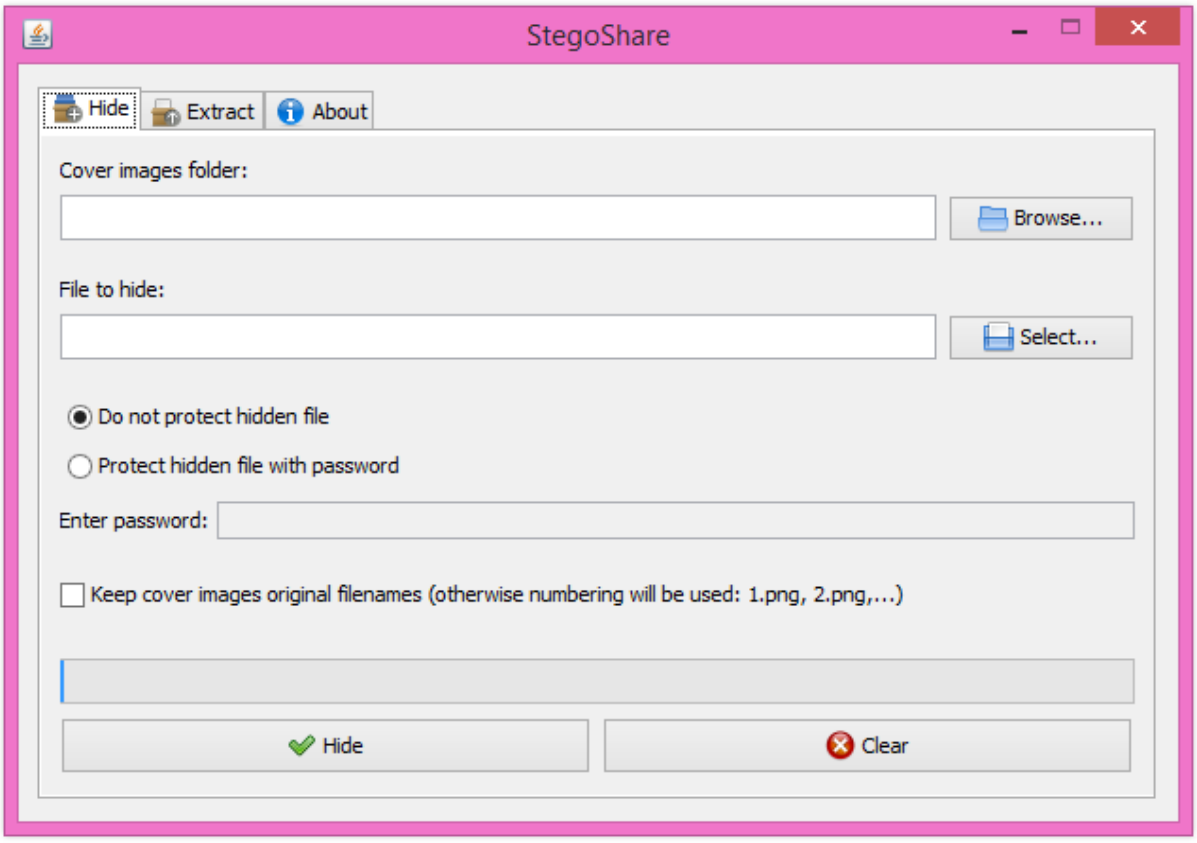
Στη επόμενη εικόνα εμφανίζονται τα στοιχεία των αρχείων και το αναγνωριστικό σήμα.




*Εικόνα 26 Final report*

### *4.2.2 StegoShare*

Η παρακάτω εικόνα δείχνει το περιβάλλον του προγράμματος StegoShare




*Εικόνα 27 StegoShare*

Για να κρύψουμε την πληροφορία μας μένουμε στην πρώτη καρτέλα Hide, πατάμε το κουμπί *Browse...* για να επιλέξουμε τον φάκελο με τις εικόνες που θα χρησιμοποιήσουμε.
Με το κουμπί *Select...*επιλέγουμε το αρχείο που θέλουμε να κρύψουμε.

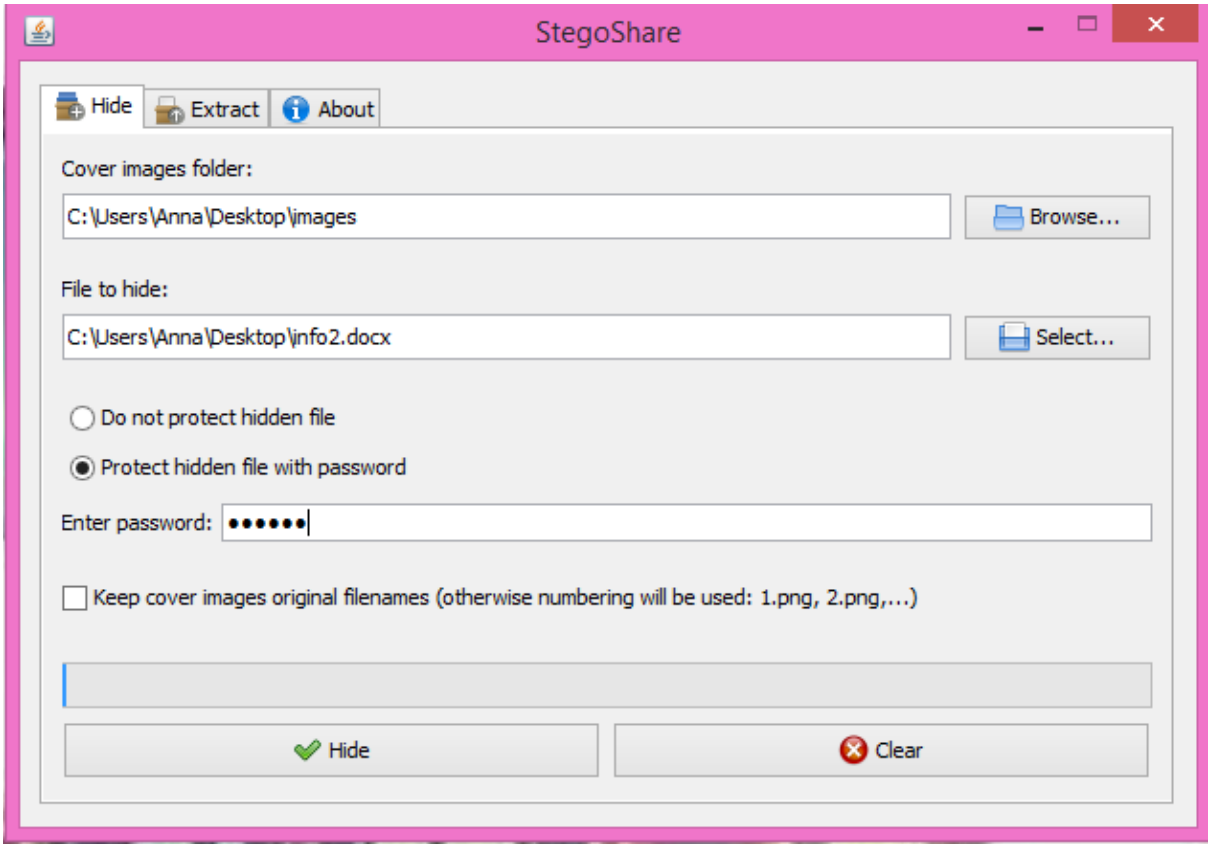
Επιπλέον υπάρχουν δύο επιλογές

- *Do not protect hidden file*
- *Protect hidden file with password*

Με τη πρώτη επιλογή ενσωματώνονται οι πληροφορίες στα αρχεία carrier χωρίς τη χρήση κωδικού. Δηλαδή ο παραλήπτης θα μπορεί να διαβάσει τη πληροφορία απλά εξάγοντας την με ένα πρόγραμμα στεγανάλυσης.

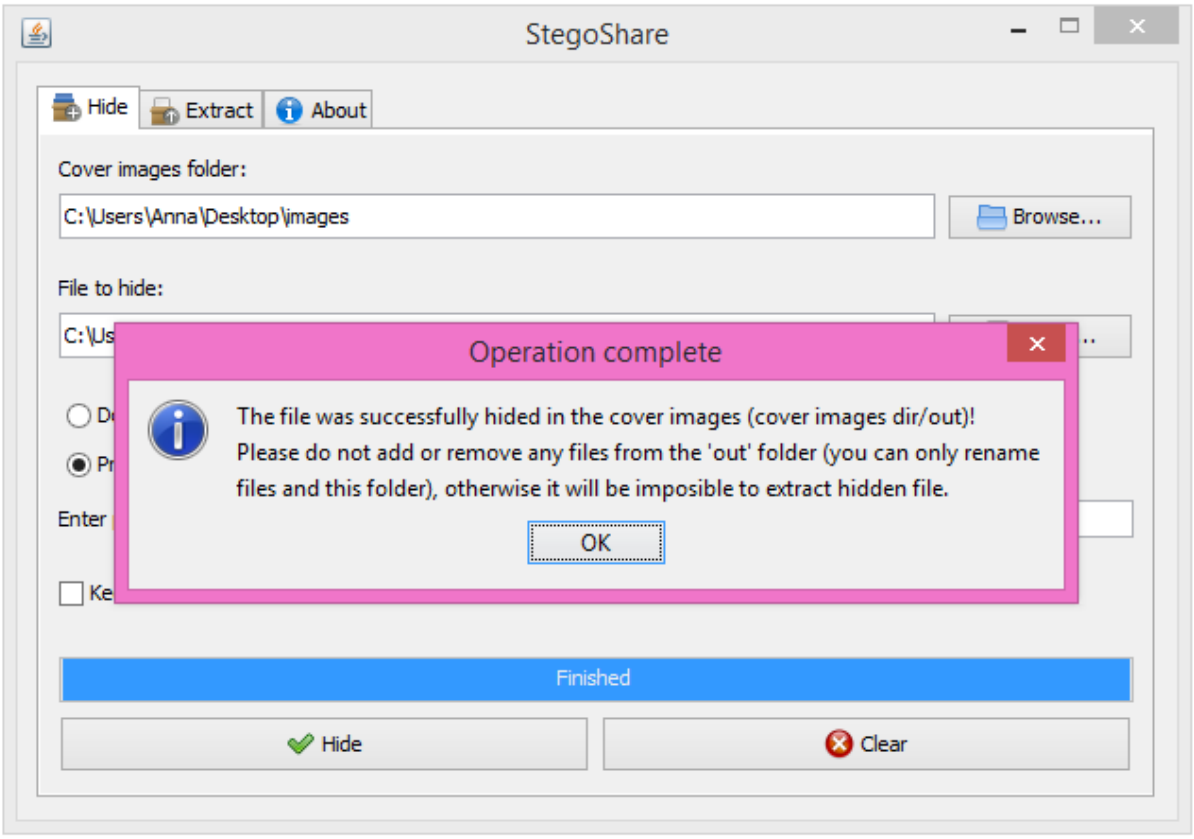
Η άλλη επιλογή είναι όταν θέλουμε οι πληροφορίες να είναι διαθέσιμες μόνο σε άτομα που έχουμε επιλέξει να δώσουμε τον κωδικό. Το κωδικός είναι: **123456**
Τα αποτελέσματα θα αποθηκευτούν σε ένα νέο φάκελο (out) μέσα στο φάκελο που επιλέξαμε λίγο πιο πάνω. Εάν δεν επιλέξουμε το check box: *keep cover original filenames* θα αριθμήσει το αποτέλεσμα πχ 1.png, 2.gif, ...αλλιώς θα αφήσει το αρχικό όνομα της εικόνας.

Το μέγεθος του φακέλου είναι 245KB και του αρχείου .docx είναι 281KB.




*Εικόνα 28 Hide*

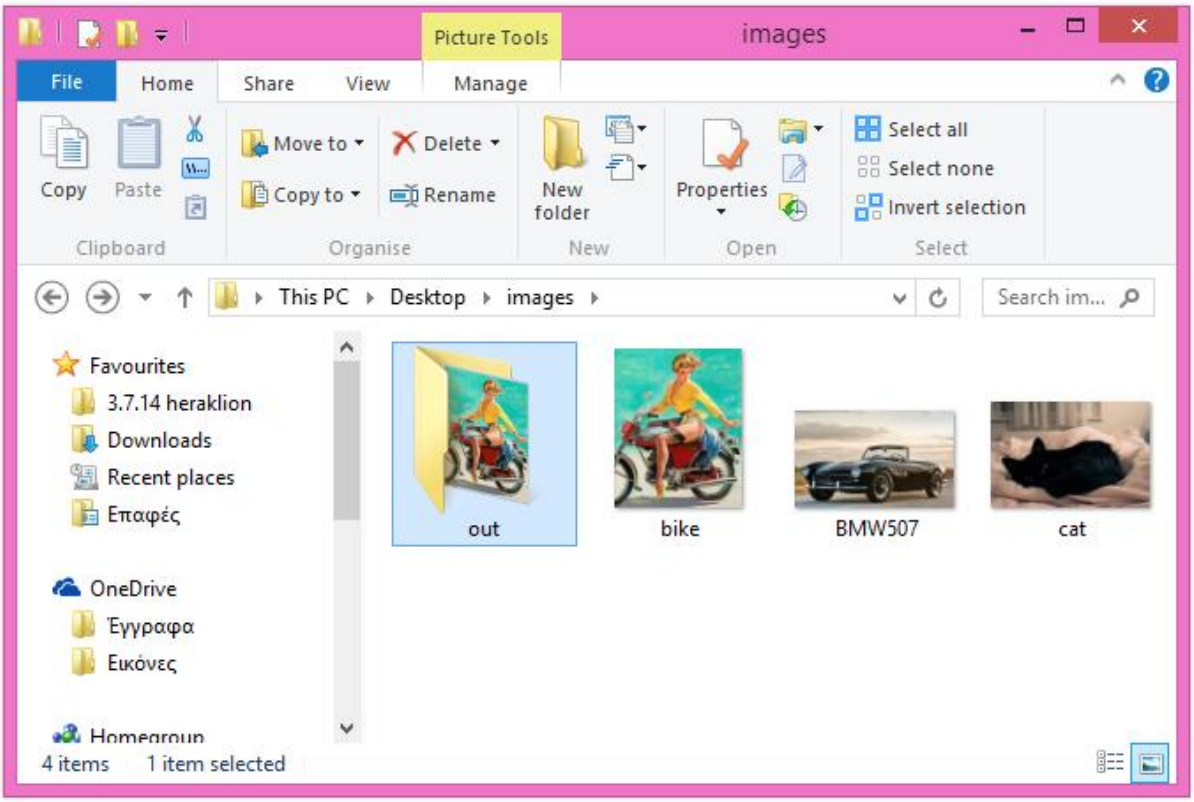
Στην συνέχεια πατάμε το *Hide* ώστε να ξεκινήσει η διαδικασία.



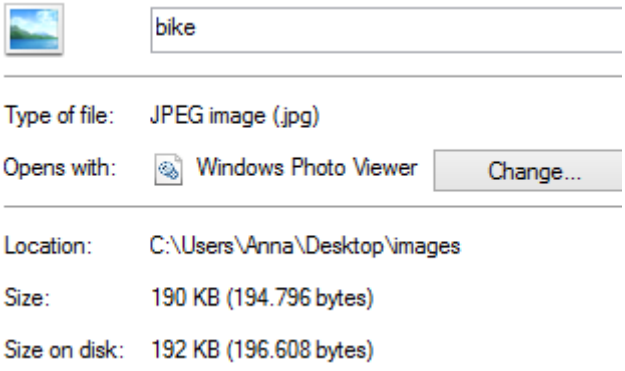

*Εικόνα 29 Hide*

Μας ενημερώνει ότι η διαδικασία επιτεύχθηκε επιτυχώς, ότι έχει δημιουργηθεί ένας φάκελος out όπου έχει αποθηκευτεί το αποτέλεσμα. Επίσης ότι μπορεί να γίνει μετονομασία του φακέλου και των αρχείων αλλά δεν πρέπει να γίνει αλλαγή της θέση τους, αλλιώς δεν θα μπορέσει να γίνει αργότερα η εξαγωγή του κρυμμένου αρχείου

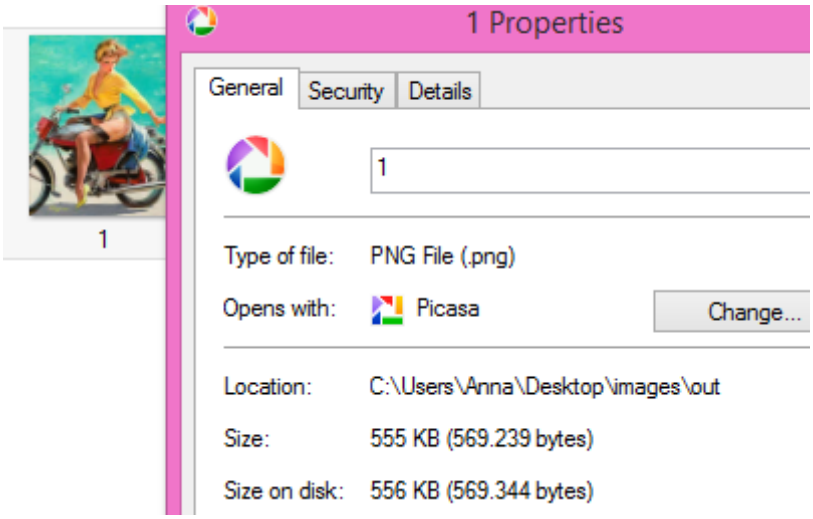
Ανοίγουμε το φάκελο με τα αποτελέσματα.




Στο παράδειγμα αυτό χρησιμοποίησα τρεις εικόνες επειδή το αρχείο που χρησιμοποίησα ήταν αρκετά μικρό έχει χρησιμοποιήσει μόνο μια εικόνα.
Το αρχικό μέγεθος της εικόνας ήταν 190KB.




Το αποτέλεσμα προφανώς θα είναι μεγαλύτερο. Είναι 555KB.

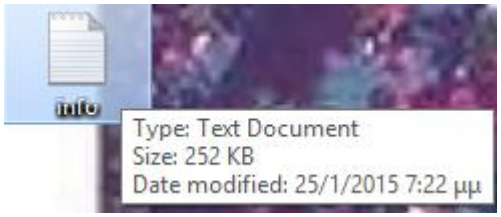


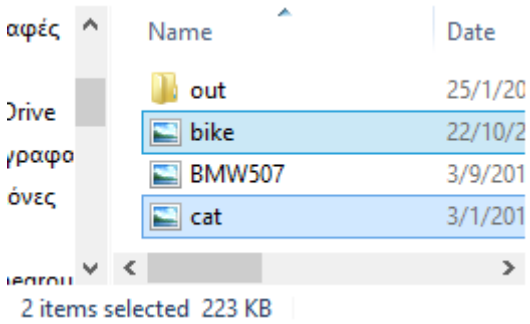

Το σύνολο των αρχείων που χρησιμοποίησα είναι 190+22,3+32,9=245,2KB

Το 40% του μεγέθους είναι 98KB, άρα θα μπορούσα να χρησιμοποιήσω αρχείο μέχρι και 3*98=294KB

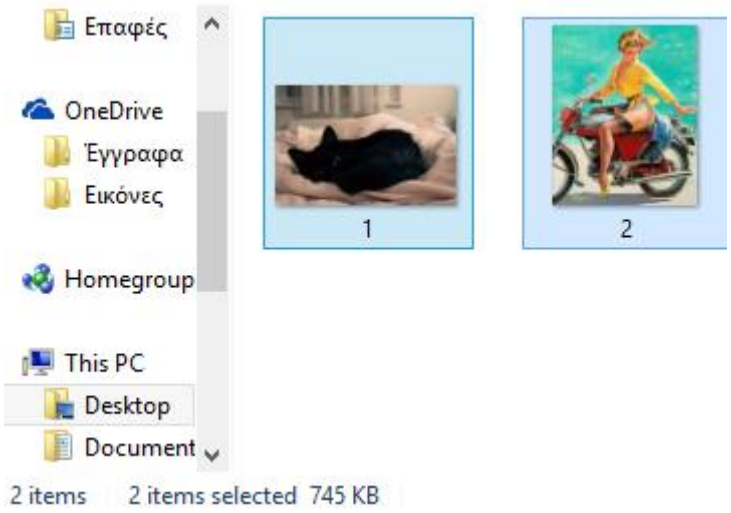
Για παράδειγμα αν το αρχείο info.txt είναι 252KB και επιλέξουμε ξανά τις τρεις εικόνες που χρησιμοποίησα και προηγουμένως

και οι δύο αρχικές εικόνες στο σύνολο τους είναι 223KB

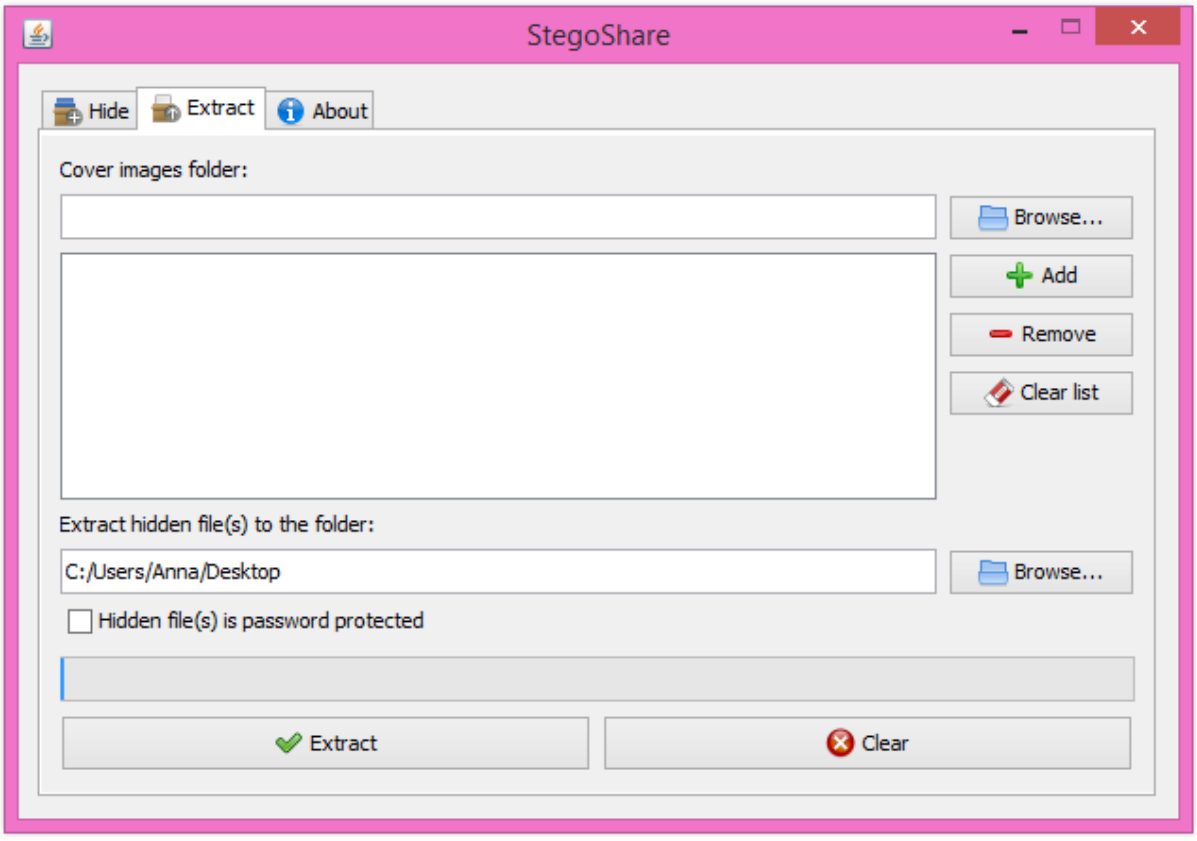



Τότε μετά την ενσωμάτωση του αρχείου οι εικόνες θα έχουν συνολικό μέγεθος 745KB

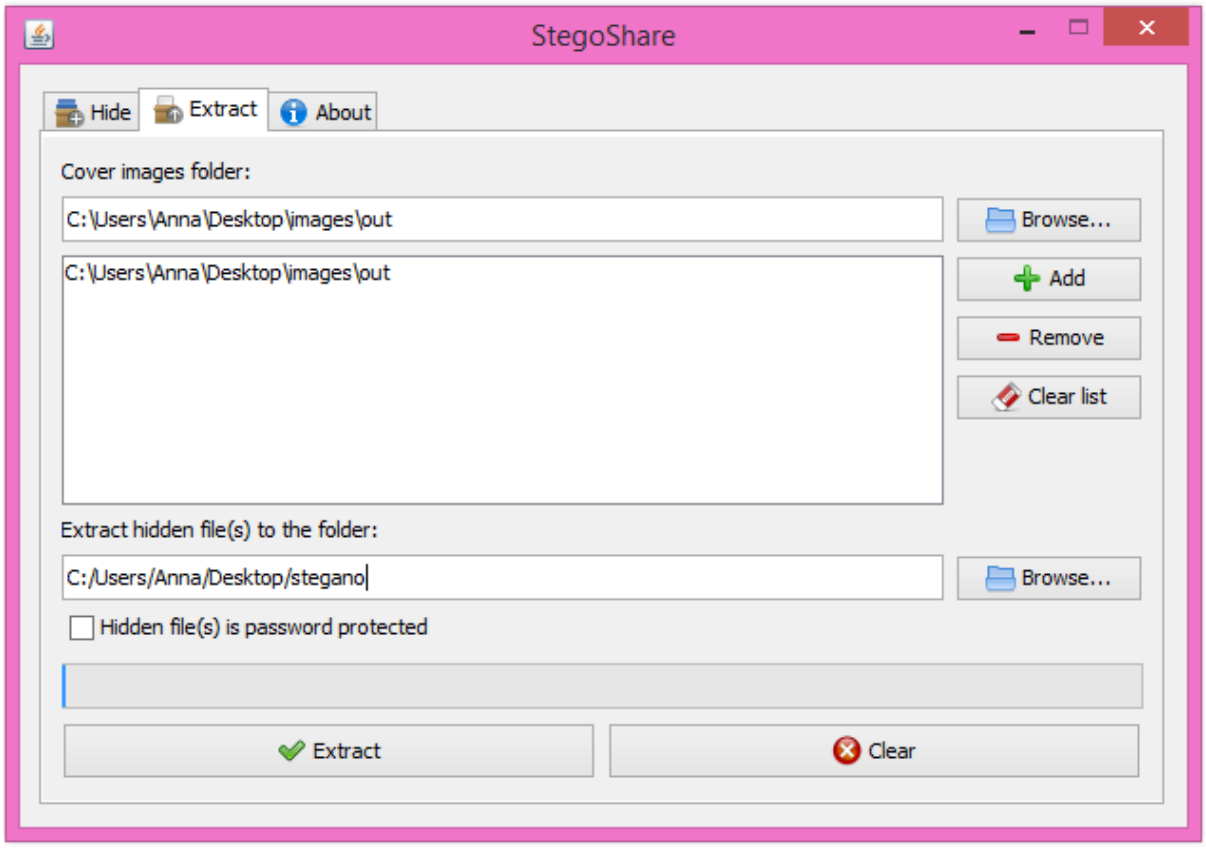



Τώρα αν θέλουμε να κάνουμε την αντίστροφη διαδικασία θα πρέπει να πάμε στην δεύτερη καρτέλα *Extract* . η παρακάτω εικόνα μας δείχνει πως είναι το περιβάλλον.

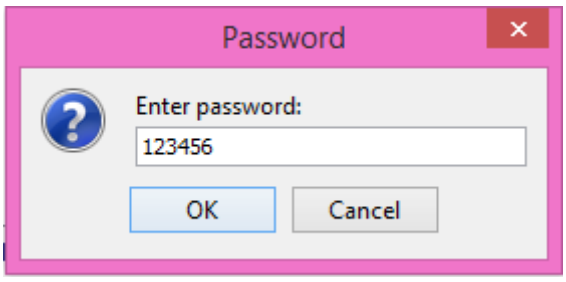



Πατώντας το κουμπί *Browse…* επιλέγουμε το φάκελο (out) που περιέχει τις εικόνες με το κρυμμένο αρχείο, στη συνέχεια θα πρέπει να περαστεί στη λίστα πατώντας το *+Add*. Με το *–Remove* αφαιρώ ένα ένα τους φακέλους που δε χρειάζομαι (αν για παράδειγμα πρόσθεσα στη λίστα δύο φορές τον

ίδιο φάκελο). Με το *Clear list* αφαιρώ όλους του φακέλους που έχω προσθέσει. Επιλέγουμε το σημείο που θέλουμε να αποθηκευτεί και επιλέγουμε *Extract*.

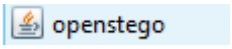



Εφόσον έχουμε «κλικάρει» το *Hidden file(s) is password protected*, το ενημερώνουμε ότι το αρχείο είναι προστατευμένο με κωδικό ασφαλείας. Οπότε θα μας τον ζητήσει.

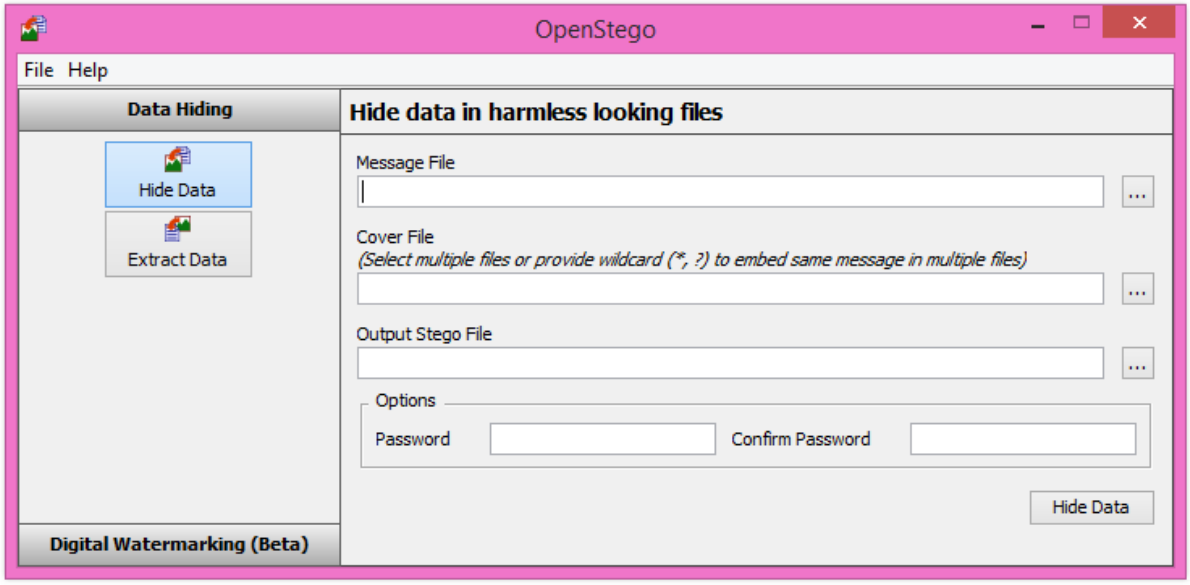



Όταν τελειώσει η όλη διαδικασία, μας εμφανίζει το παρακάτω παράθυρο και μπορούμε να ανοίξουμε το φάκελο να δούμε το αρχείο info.txt.

### *4.2.3 OpenStego 0.6.1*

Όπως και με τα προηγούμενα προγράμματα, κατεβάζουμε τα αρχεία στο υπολογιστή και τα αποθηκεύουμε σε κάποιο σημείο του δίσκου μας. Κάνοντας διπλό κλικ στο 

ανοίγουμε το πρόγραμμα. Η παρακάτω εικόνα είναι το περιβάλλον εργασίας του OpenStego.




*Εικόνα 30 OpenStego*

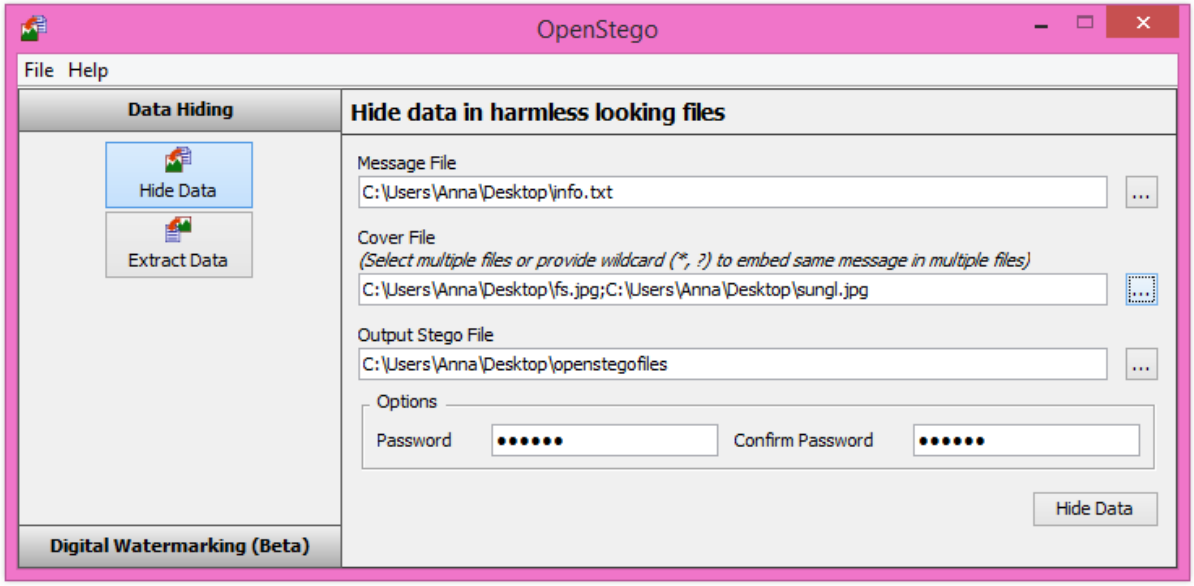
Έχει δύο καρτέλες στην αριστερή πλευρά, *Data Hiding* και *Digital Watermarking (Beta)*. Ας ξεκινήσουμε με τη πρώτη – θα ενσωματώσουμε ένα αρχείο σε μία εικόνα.

Το *Message file* είναι το αρχείο θέλω να κρύψω και το επιλέγω, πατώντας στη δεξιά πλευρά της μπάρας το κουμπί  . Το αρχείο αυτό μπορεί να είναι οποιουδήποτε τύπου αρχείο(αρχεία κειμένου βίντεο, εικόνας κτλ.).

Το *Cover file* είναι το αρχείο ή τα αρχεία εικόνας που θα επιλέξουμε για να κρύψουμε το προηγούμενο αρχείο, επιλέγοντας από το κουμπί  στην δεξιά πλευρά της μπάρας. Το OpenStego μας δίνει τη δυνατότητα να χρησιμοποιήσουμε περισσότερα από ένα αρχεία. Η ίδια πληροφορία θα περιέχεται σε κάθε αρχείο. Έχω επιλέξει δύο αρχεία τα οποία χωρίζονται με «**;**» .

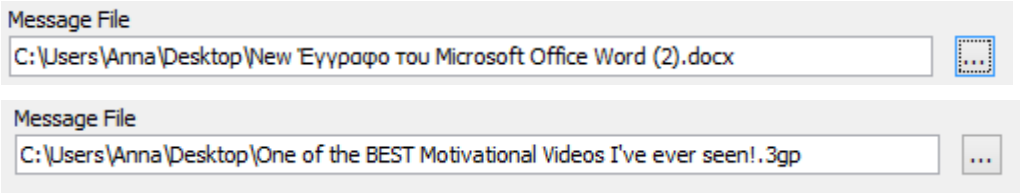
Το *Output Stego* file είναι το σημείο όπου θα αποθηκευτεί η νέα εικόνα/εικόνες. Σαν αποτέλεσμα θα πάρω εικόνα τύπου PNG.

Στο Options μας ζητάει κωδικό (password) και την επιβεβαίωση του κωδικού (confirm password). Στο παράδειγμα αυτό χρησιμοποίησα σαν κωδικό 147852.



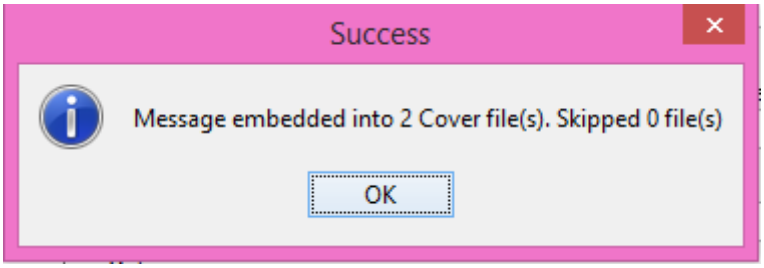

*Εικόνα 31 Setting for Hide data*

Δοκίμασα και αρχεία διαφορετικού τύπου όπως .doc(word) και .3gp(video), είναι ακριβώς η ίδια διαδικασία.

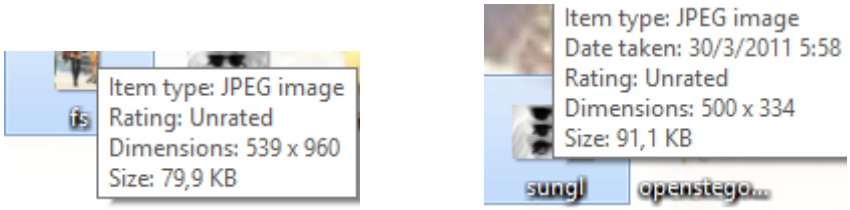



Έπειτα πατάμε *Hide Data*!

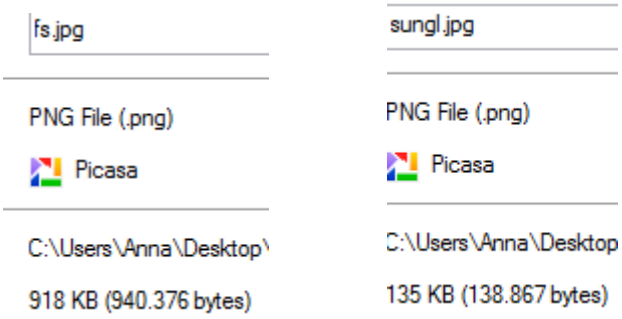
Όταν τελειώσει η διαδικασία, μας ενημερώνει για την κατάσταση με το παρακάτω παράθυρο.




Το μήνυμα ενσωματώθηκε με επιτυχία σε δύο αρχεία.

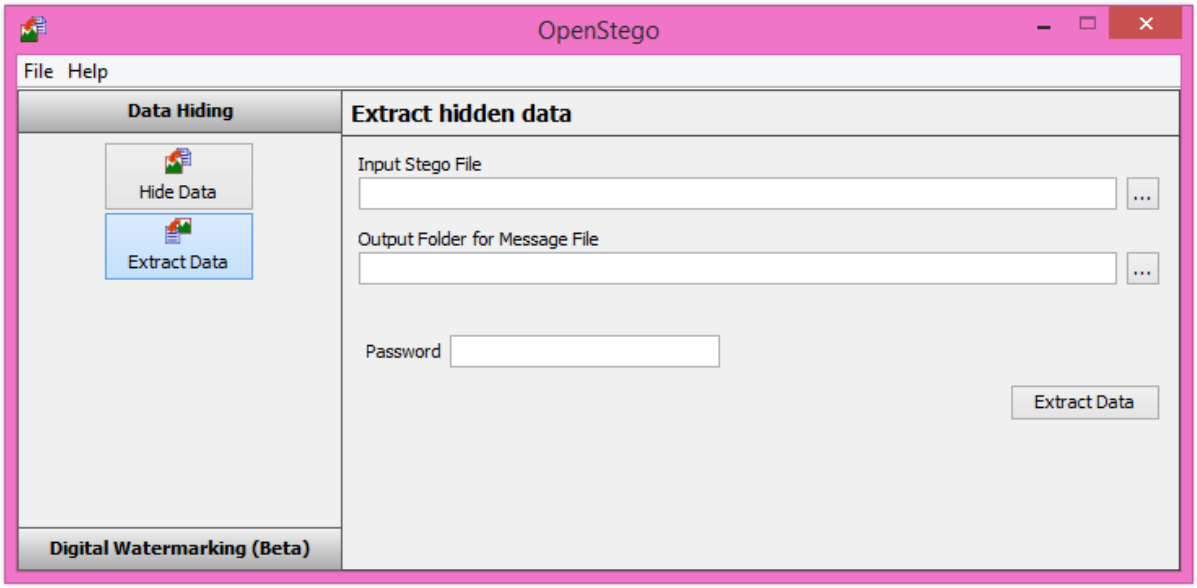



Στις δύο παραπάνω εικόνες εμφανίζονται τα μεγέθη των αρχικών εικόνων.




Κάνοντας σύγκριση των αρχικών εικόνων με των αποτελεσμάτων στο μέγεθος των αρχείων, μπορεί κάποιος να καταλάβει ότι στις τελευταίες κάποιος έχει κρύψει πληροφορία. Επιπλέον, οι αρχικές εικόνες (.jpg) έχουν μετατραπεί σε PNG files.

Για την αντίστροφη διαδικασία επιλέγουμε το *Extract Data*

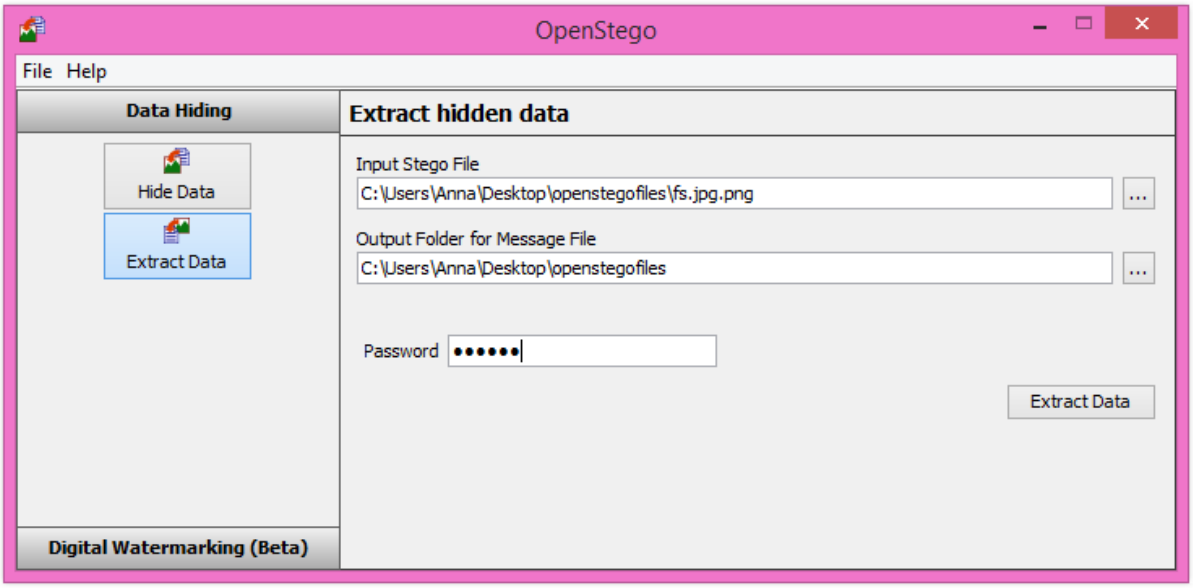



*Εικόνα 32 Extract Data*

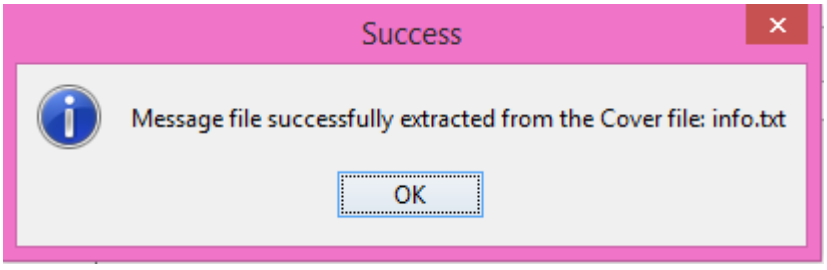
Στο *Input Stego file* επιλέγουμε την εικόνα ή μια από τις εικόνες που έχουμε χρησιμοποιήσει για να κρύψουμε το αρχείο.

Στο *Output folder for message file* επιλέγουμε το σημείο που θέλουμε να αποθηκεύσουμε το εξαγόμενο αρχείο.

Συμπληρώνουμε τον κωδικό (147852) που χρησιμοποιήσαμε για την κρυπτογράφηση και τέλος πατάμε *Extract Data*.




*Εικόνα 33 Extract Data Settings*



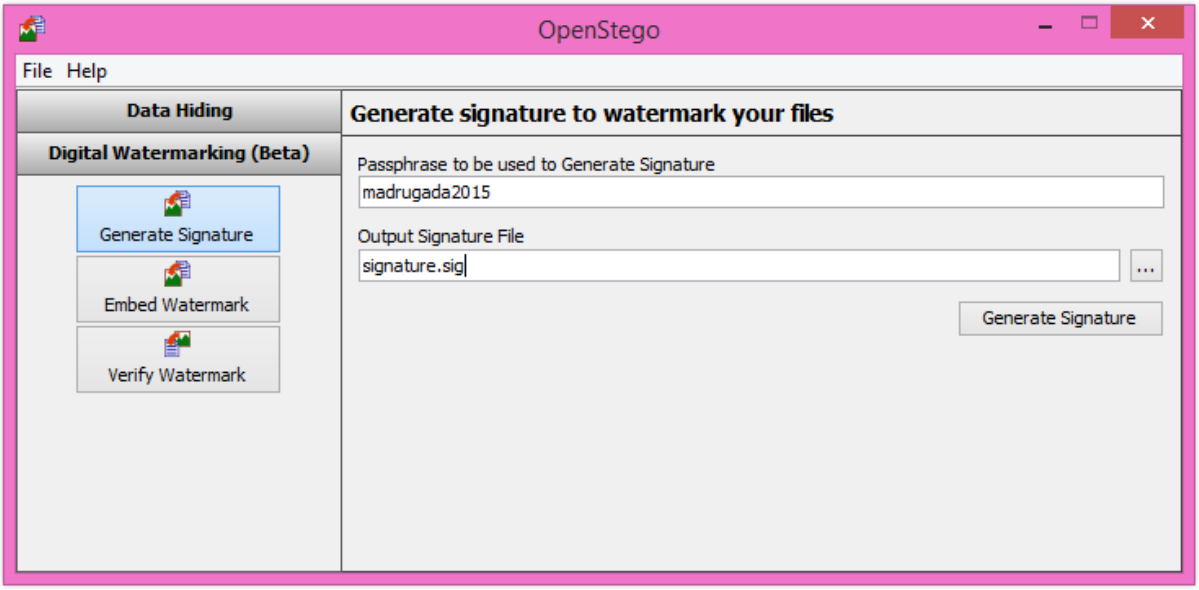

Με το μήνυμα αυτό ξέρουμε ότι επιτεύχθηκε με επιτυχία η εξαγωγή του κρυμμένου αρχείου info.txt.

Η δεύτερη καρτέλα είναι Digital Watermarking – Ψηφιακή Υδατογράφηση.

Η διαδικασία αποτελείται από τρία βήματα

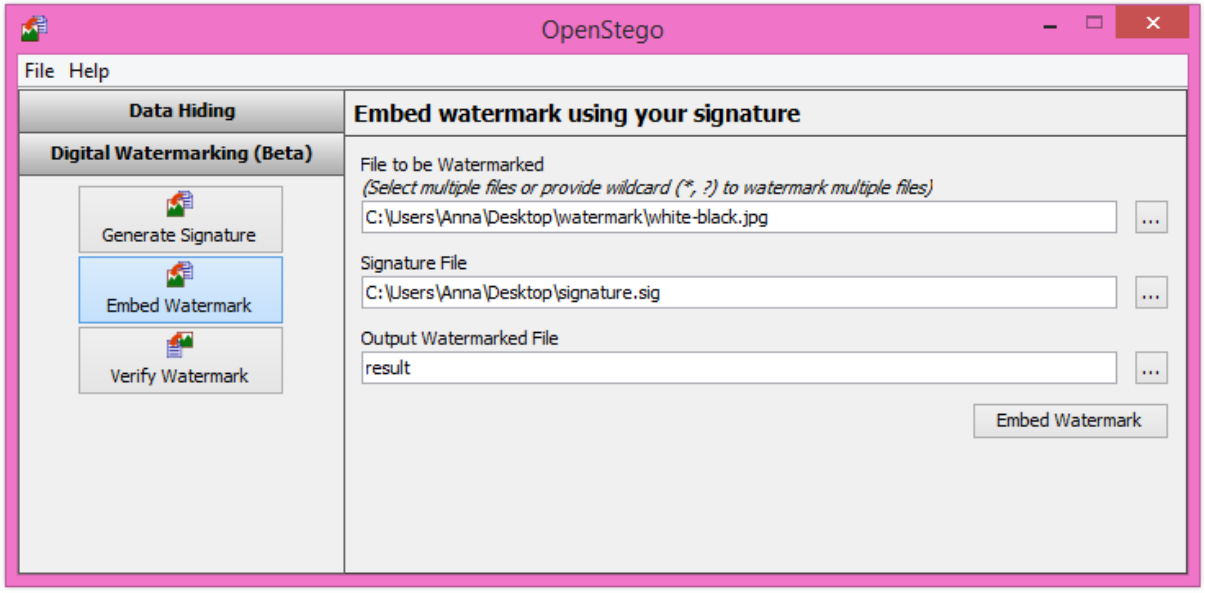
- Generate signature
- Embed watermark
- Verify watermark

Το πρώτο βήμα είναι να δημιουργήσουμε την ψηφιακή υπογραφή από την υπο-καρτέλα *Generate signature*. Στην πρώτη μπάρα - *passphrase to used to generate signature* - γράφουμε το κείμενο που θέλουμε για ψηφιακή υπογραφή. Στην δεύτερη μπάρα - Output signature file - γράφουμε το όνομα που θέλουμε να έχει το αρχείο και του λέμε ότι είναι τύπου .sig.
Έπειτα πατάμε *Generate signature* για να δημιουργήσουμε το αρχείο της ψηφιακής υπογραφής.




*Εικόνα 34 Generate signature*


Εφόσον έχουμε δημιουργήσει το αρχείο αυτό, προχωράμε στην επόμενη υπο-καρτέλα *embed watermark*

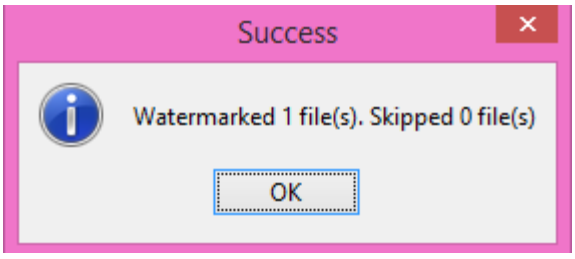



*Εικόνα 35 Embed watermark*

Στη πρώτη μπάρα επιλέγουμε το αρχείο εικόνας που θέλουμε να ενσωματώσουμε την ψηφιακή υπογραφή.

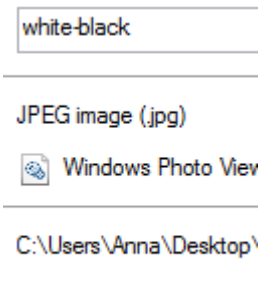
Στην δεύτερη μπάρα επιλέγουμε το αρχείο με κατάληξη .sig.

Και στην Τρίτη μπάρα γράφουμε το όνομα του αρχείου που θα δημιουργηθεί με την ψηφιακή υπογραφή. Εφόσον τα έχουμε δώσει όλες τις πληροφορίες πατάμε *Embed Watermark*.

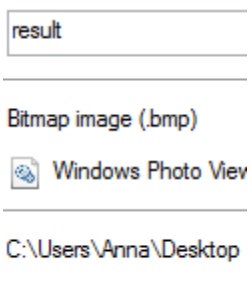



Τώρα θα συγκρίνουμε τα αποτελέσματα.

Αρχική εικόνα:




, αποτέλεσμα:



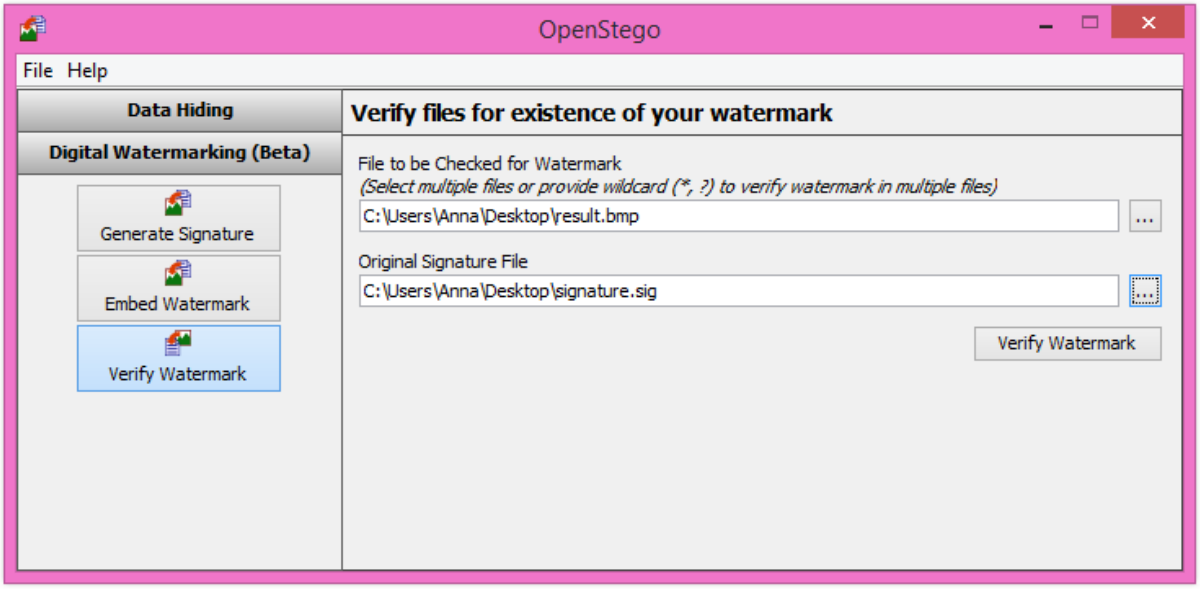
Όπως παρατηρούμε το μέγεθος είναι σχεδόν το διπλάσιο.

Result: 

Original: 

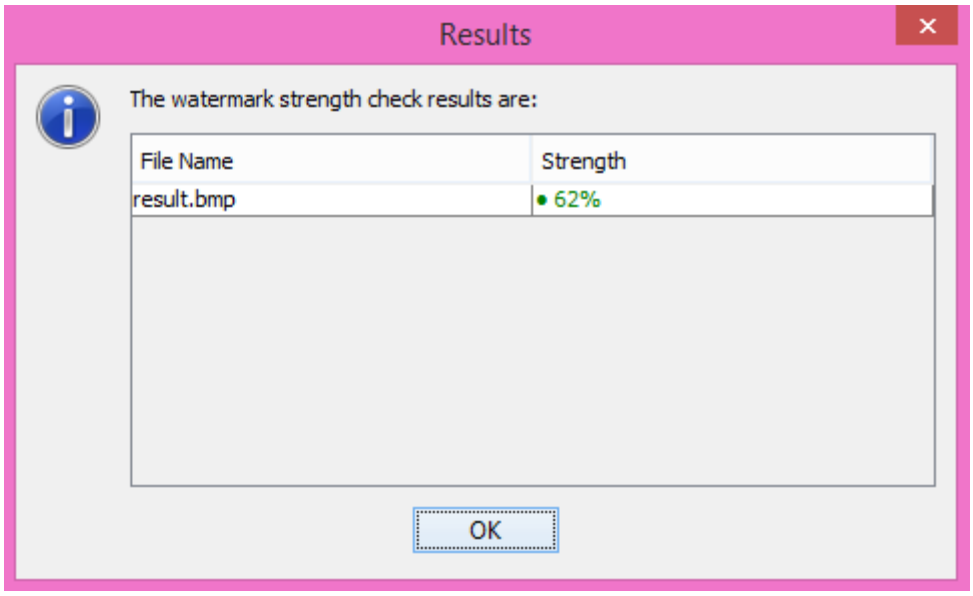
Οι δύο εικόνες μοιάζουν ίδιες, αλλά υπάρχουν αλλοιώσεις στο πρώτη εικόνα.

Για να ελέγξουμε το πόσο δυνατό είναι το υδατογράφημα, μπορούμε να το δούμε από την Τρίτη υποκαρτέλα. Στην πρώτη μπάρα επιλέγω την εικόνα που δημιούργησα πριν με τη ψηφιακή υπογραφή και στην δεύτερη το αρχείο που έφτιαξα με κατάληξη .sig.




*Εικόνα 36 Verify Watermark*

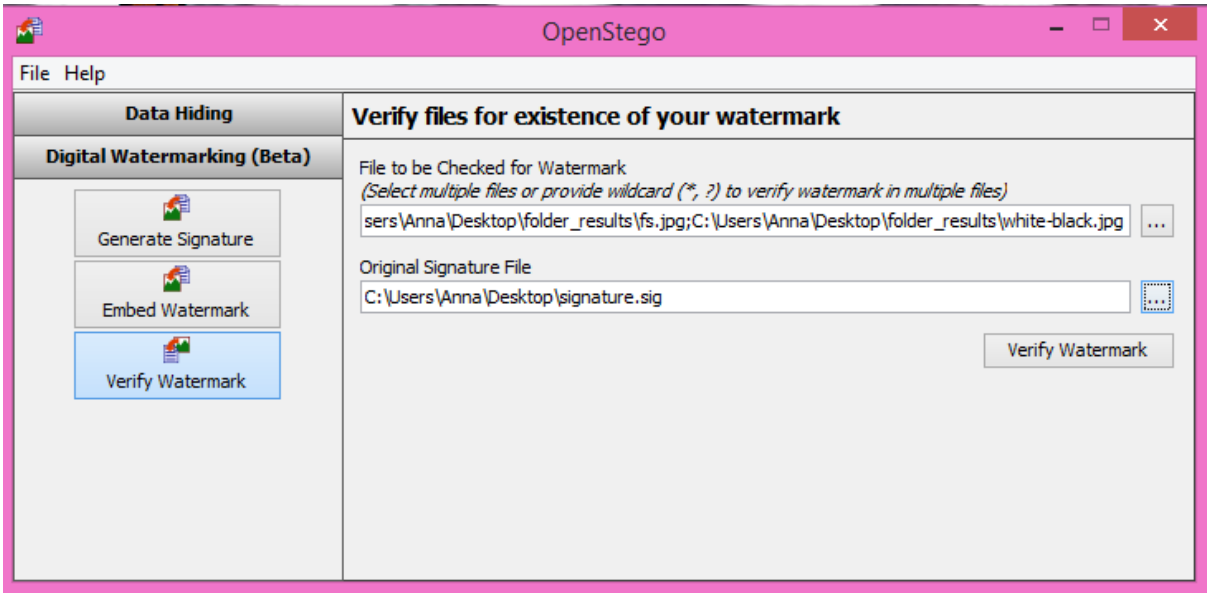
Πατώντας το κουμπί Verify watermark, θα μας εμφανίσει την αναφορά με τα αποτελέσματα.

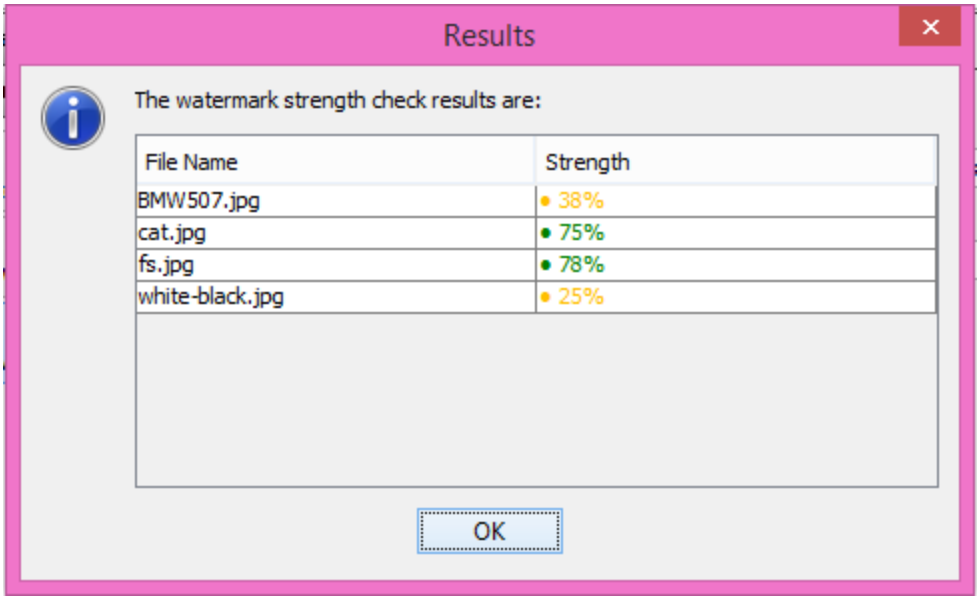



*Εικόνα 37 Results of the watermark strength check*

Στη περίπτωση που είχαμε περισσότερα από ένα αρχεία για ενσωμάτωση της ψηφιακής υπογραφής: Όπως και στο προηγούμενο παράδειγμα επιλέγω τις εικόνες που θέλω, το αρχείο με κατάληξη .sig και συμπληρώνω τον φάκελο που θέλω να αποθηκευτούν τα αποτελέσματα( C:\folder_results).


OpenStego
File Help
Data Hiding
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Embed watermark using your signature
File to be Watermarked
(Select multiple files or provide wildcard (*, ?) to watermark multiple files)
;C:\Users\Anna\Desktop\watermark\fs.jpg;C:\Users\Anna\Desktop\watermark\white-black.jpg
Signature File
C:\Users\Anna\Desktop\signature.sig
Output Watermarked File
C:\folder_results
Embed Watermark


OpenStego
File Help
Data Hiding
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Verify files for existence of your watermark
File to be Checked for Watermark
(Select multiple files or provide wildcard (*, ?) to verify watermark in multiple files)
sers\Anna\Desktop\folder_results\fs.jpg;C:\Users\Anna\Desktop\folder_results\white-black.jpg
Original Signature File
C:\Users\Anna\Desktop\signature.sig
Verify Watermark




Παρατηρώ στην τελευταία εικόνα που βρίσκονται τα αποτελέσματα, ότι δεν έχουν όλες οι εικόνες την ίδια δύναμη της υδατογράφησης, η πρώτη και η τελευταία εικόνα έχουν πολύ χαμηλό ποσοστό. Καλό ποσοστό θεωρείται από 50% και πάνω.

# ΚΕΦΑΛΑΙΟ 5

## Στεγανάλυση εργαλεία (Steganalysis Tools)

### 5.1 Διάφορα εργαλεία στεγανάλυσης

Παρουσίαση κάποιων γνωστών εργαλείων.

**StegExpose**-Είναι ένα εργαλείο στεγανάλυσης που ειδικεύεται στην ανίχνευση στεγανογραφίας σε εικόνες, όπως PNG και BMP(LSB-λιγότερο σημαντικό bit). Εκτός από την ανίχνευση της παρουσίας στεγανογραφίας , το πρόγραμμα διαθέτει επίσης την ποσοτική στεγανάλυση – δηλαδή τον προσδιορισμό του μήκους του κρυμμένου μηνύματος. Χαρακτηριστικά που έχει ( καλά δοκιμασμένα στο παρελθόν) είναι τα εξής:

- Sample Pairs by Dumitrescu (2003)
- RS Analysis by Fridrich (2001)
- Chi Square Attack by Westfeld (2000)
- Primary Sets by Dumitrescu (2002)

**StegSecret**-Είναι εργαλείο στεγανάλυσης ανοικτού πηγαίου κώδικα(GNU/GPL) που καθιστά δυνατή την ανίχνευση κρυμμένων πηλοφοριών σε διάφορα ψηφιακά μέσα. Το πρόγραμμα είναι βασισμένο σε Java και είναι multiplatform εργαλείο στεγανάλυσης που επιτρέπει την ανίχνευση των κρυφών πληροφοριών με την χρήση των πιο γνωστών στεγανογραφικών μεθόδων. Μπορεί να ανιχνεύσει EOF, LSB, DCTs και άλλες τεχνικές. Στόχος του είναι η συλλογή και η εφαρμογή τεχνικών στεγανάλυσης, στα ψηφιακά μέσα όπως εικόνες, ήχος και βίντεο.

Το παρακάτω πρόγραμμα θα γίνει περιγραφή και η υλοποίηση του.

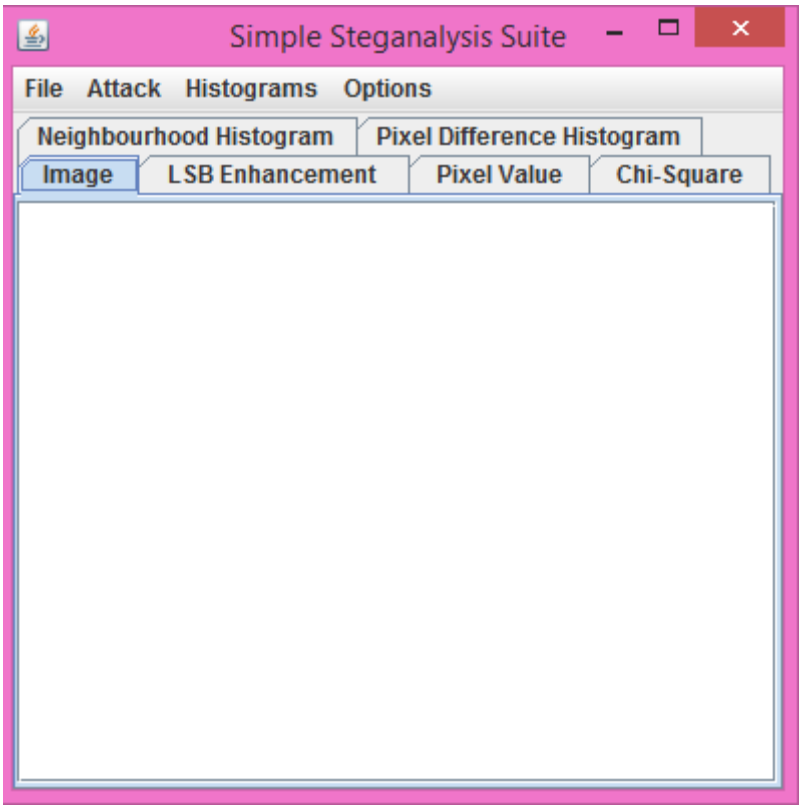
### 5.2 Simple-Steganalysis-Suite (SSS)

Το πρόγραμμα αυτό είναι ένα απλό Java πρόγραμμα για την στεγανάλυση εικόνων που μπορεί να διαβάσει μία εικόνα τη φορά. Προσφέρει δύο ειδών επιθέσεων και διάφορα ιστογράμματα όπως:

- Ενίσχυση LSB
- Chi-Square
- Ιστόγραμμα με γειτονικά pixels
- Ιστόγραμμα Pixel Difference

Η ανικανότητα του ανθρώπου να μη μπορεί να παρατηρεί την παραμικρή λεπτομέρεια, είναι το όπλο που χρησιμοποιείται χρόνια τώρα για τη μεταφορά κρυφών μηνυμάτων σε εικόνες.

Το πρόγραμμα έχει την εξής μορφή:



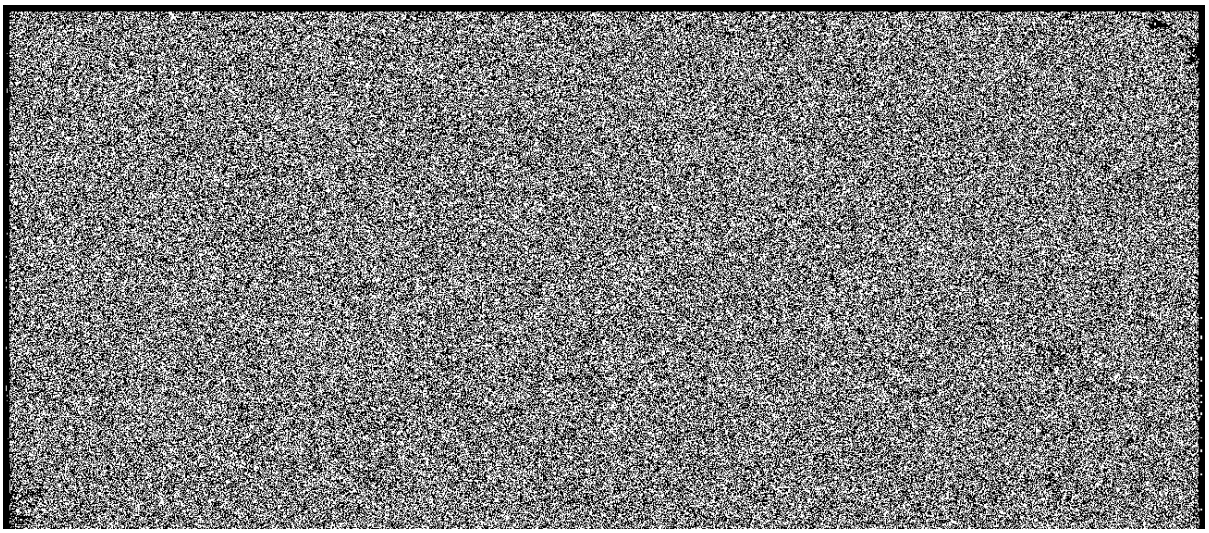

*Εικόνα 38 Simple Steganalysis Suite (SSS)*

## Παράδειγμα 1- ασπρόμαυρη εικόνα

Θα ξεκινήσω να αναλύω τις λειτουργίες με ένα παράδειγμα. Για το παρακάτω παράδειγμα χρησιμοποίησα μία εικόνα **χωρίς κρυφό μήνυμα**, αποθήκευσα τις πληροφορίες που δίνει το πρόγραμμα και συνέχεια **ενσωμάτωσα ένα μήνυμα και ξανά πήρα αποτελέσματα**. Χρησιμοποίησα ασπρόμαυρή εικόνα για να είναι εμφανή τα αποτελέσματα.

Η παρακάτω εικόνα είναι η αρχική εικόνα που χρησιμοποίησα(πριν το κρύψιμο του αρχείου)

LSB Enhancement Είναι η ρύθμιση του το λιγότερου σημαντικού bit του εικονοστοιχείου με αξία έως 255, αν είναι 1, αν είναι 0 το αφήνει όπως είναι. Το αποτέλεσμα θα είναι ότι η εικόνα θα έχει κάποια φανταχτερά χρώματα στα σημεία όπου το LSB ήταν 1.

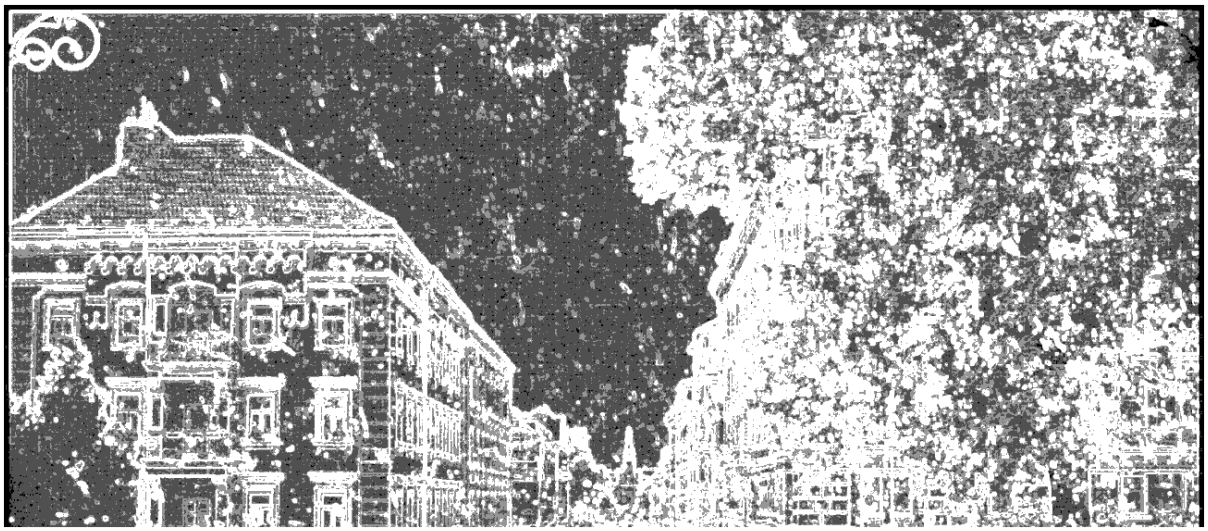


*Εικόνα 39 before hide the information -LSB*

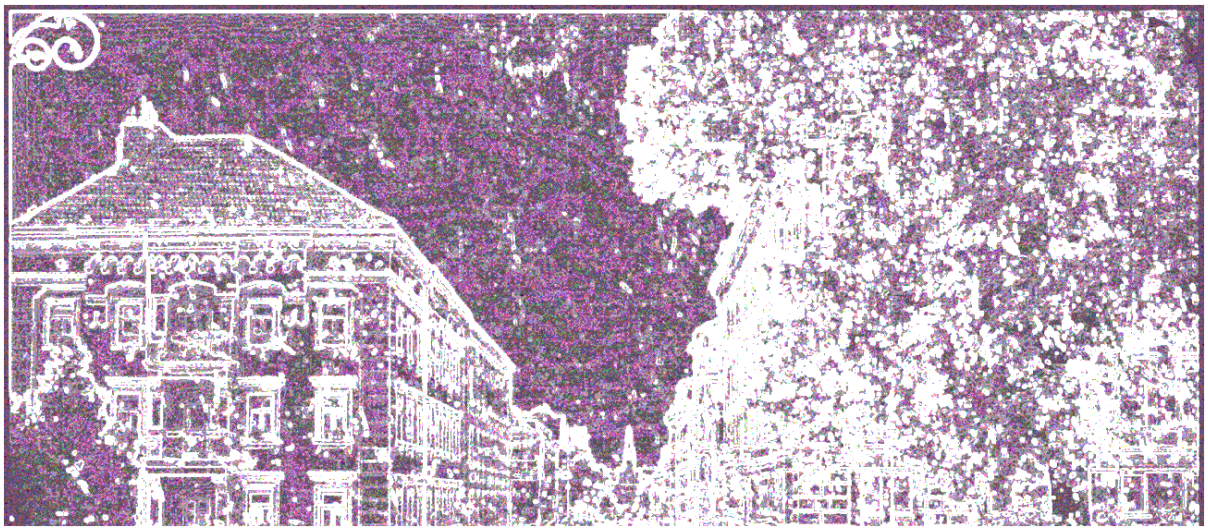
*Εικόνα 40 after hide the information - LSB*

Παρατηρούμε ότι στο αποτέλεσμα με το κρυφό μήνυμα υπάρχουν χρωματιστά pixels. Χωρίς να συγκρίνουμε με την από πάνω εικόνα καταλαβαίνουμε ότι στην εικόνα μας υπάρχει κρυφό μήνυμα

Και με την επίθεση **pixel value** καταλαβαίνουμε την παρουσία του κρυφού μηνύματος, ο χρωματισμός και εδώ είναι εμφανής.



*Εικόνα 41 before hide information - pixel value*



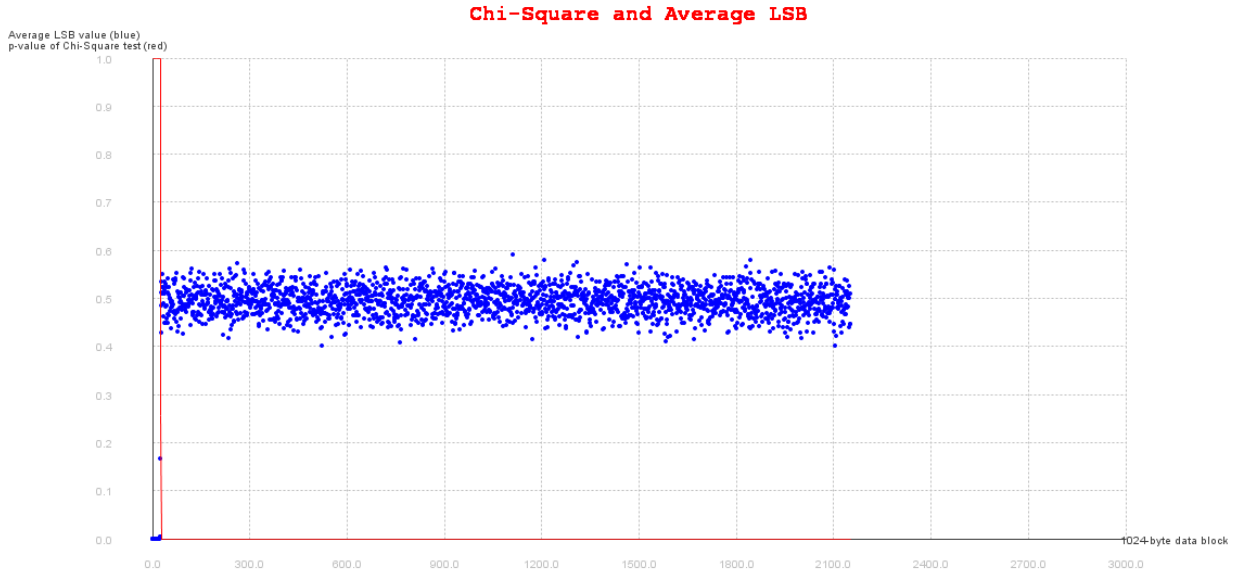
*Εικόνα 42 after hide information - pixel value*

Η φόρμουλα υπολογισμού του chi-square ( $\chi^2$) είναι:

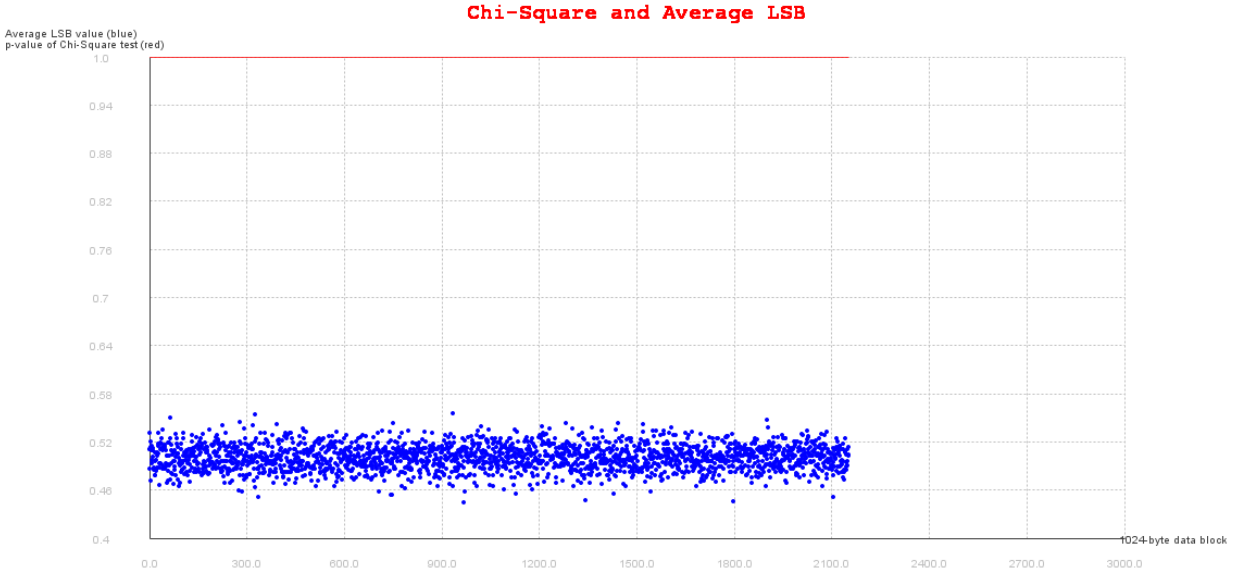
$$\chi^2 = \chi(o-e)^2/e$$

Δηλαδή, chi-square είναι το άθροισμα των τετραγώνων διαφοράς μεταξύ των παρατηρούμενων (ο) και τα αναμενόμενων στοιχείων (ε), διαιρούμενο με τα αναμενόμενα δεδομένα σε όλες τις πιθανές κατηγορίες.

Η επίθεση chi-square είναι μια στατική δοκιμή για να διαπιστωθεί ένα δεδομένο σύνολο των παρατηρούμενων δεδομένων και της αναμενόμενο σύνολο δεδομένων είναι παρόμοιο ή όχι. Αυτή είναι η βασική ιδέα, μπορούμε να διαβάσουμε για αυτό σε κάθε βιβλίο στατιστικής. Η ιδέα αυτής είναι να συγκρίνουμε το ζεύγος τιμών παρατηρώντας τις συχνότητες, με τις αναμενόμενες συχνότητες και να γίνει ο υπολογισμός της τιμής χ που θα εκπροσωπήσει την πιθανότητα ότι η εικόνα έχει κάποια κρυφά δεδομένα. Τι εννοούμε με τον όρο ζεύγος τιμών. Σύμφωνα με τους Westfeld & Pfitzmann όταν ορισμένα στοιχεία όπως ένα κρυπτογραφημένο κείμενο είναι ενσωματωμένο σε μια εικόνα, οι αρχικές τιμές των LSB αλλάζουν με τέτοιο τρόπο ώστε τα ζευγάρια γίνονται σχεδόν ίσα, ενώ διαφέρουν τόσο πολύ όταν δεν υπάρχει η ενσωμάτωση. Μπορούμε να βρούμε να ζεύγη τιμών με τις ακόλουθες αλληλουχίες δυαδικών ψηφίων. Για παράδειγμα αν έχουμε εικόνα 8bit, θα έχουμε ως αποτέλεσμα 128 ζεύγη τιμών όπως 0-1, 2-3 …, 254-255.

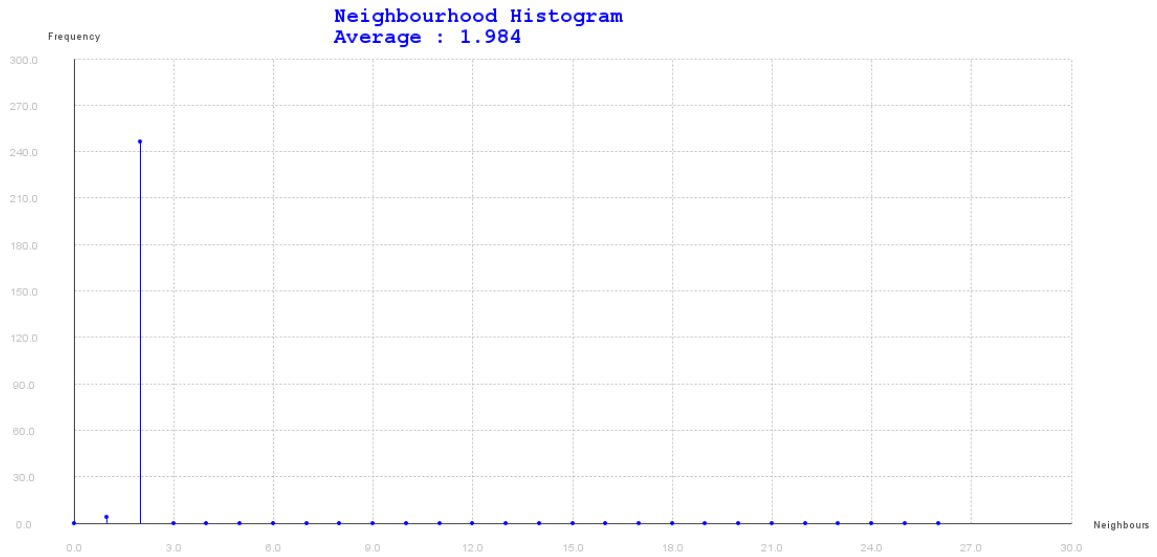



*Εικόνα 43 before hide information - chi-square*

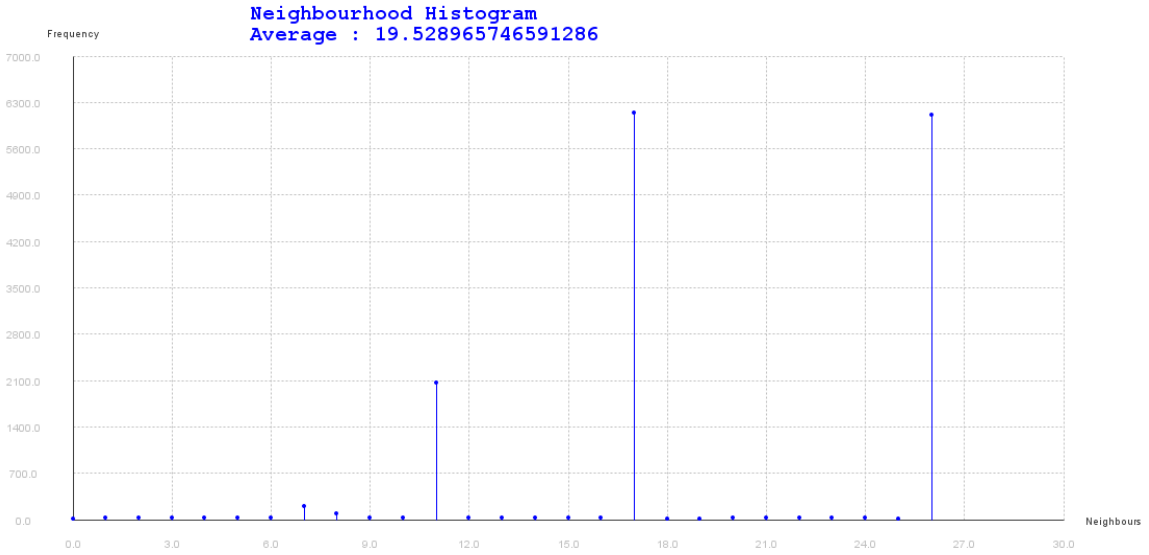



*Εικόνα 44 after hide information - chi-square*

Neighbourhood Histogram. Το ιστόγραμμα γειτονίας μας δείχνει τις τιμές των εικονοστοιχείων που είναι κοντά σε τιμές μεταξύ τους.

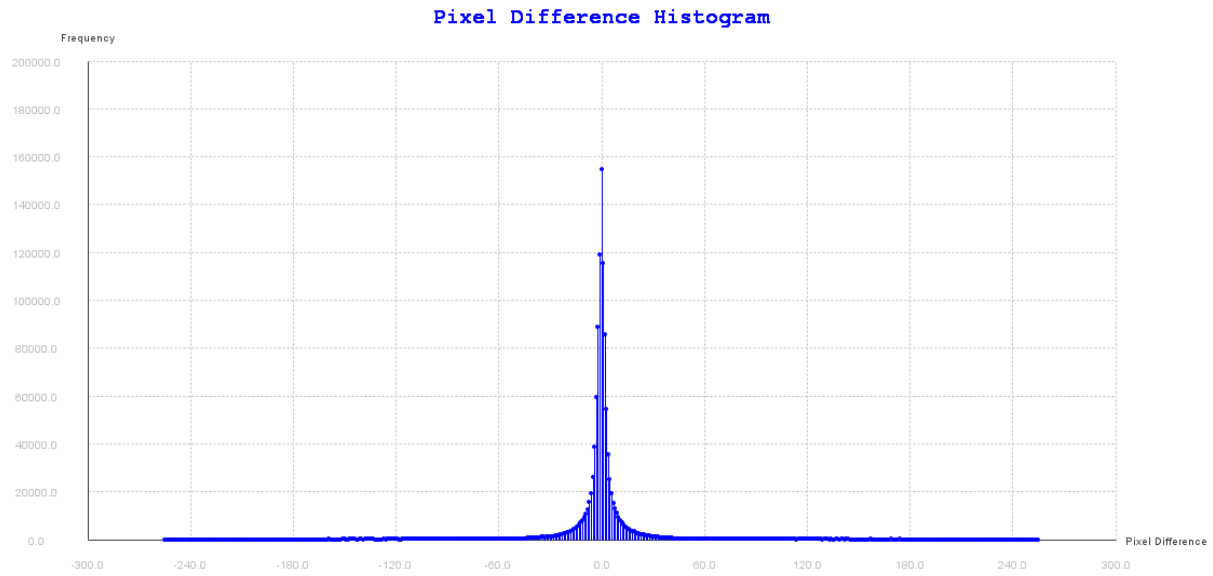



*Εικόνα 45 before hide information - Neighbourhood Histogram*

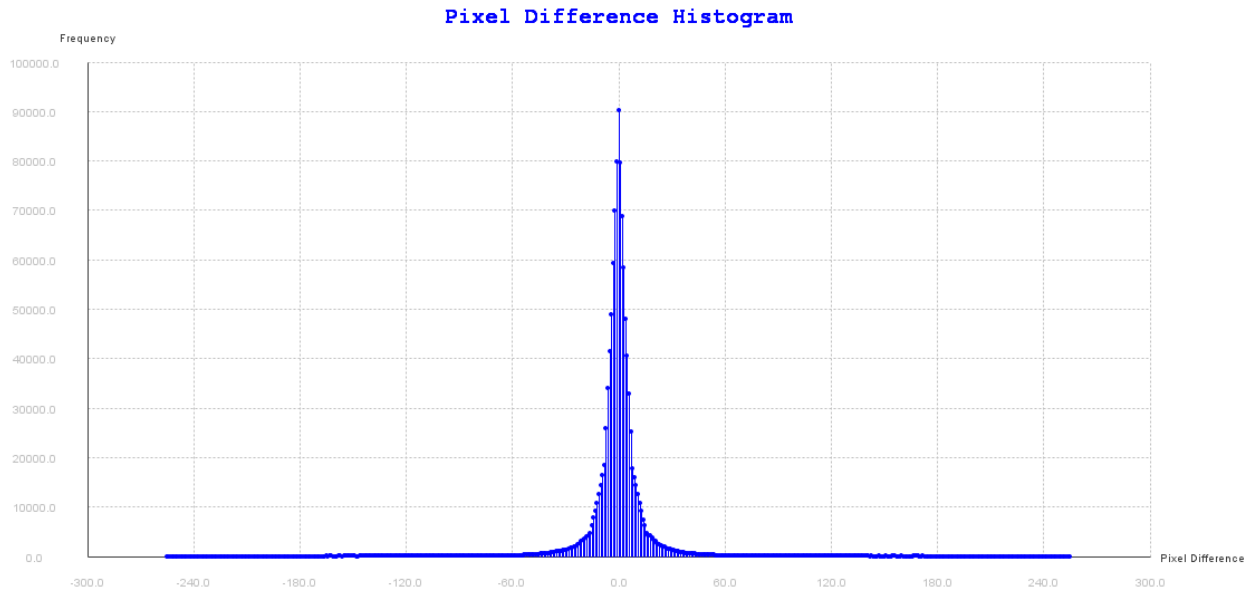



*Εικόνα 46 after hide information - Neighbourhood Histogram*

**Pixel Difference Histogram**: χαρακτηρίζεται η ένταση της τιμής της εικόνας στη θέση (i, j) ως I (í, j) και η διαφορά της εικόνας ορίζεται ως D(i,j)=I(i,j)-I(i,j+1). Το ιστόγραμμα αυτό ορίζεται ως το ιστόγραμμα της διαφοράς της εικόνας D. Γενικά πιστεύεται ότι η διαφορά της εικόνας ακολουθεί μια γενικευμένη κατανομή Gauss.




*Εικόνα 47 before hide information - Pixel difference histogram*



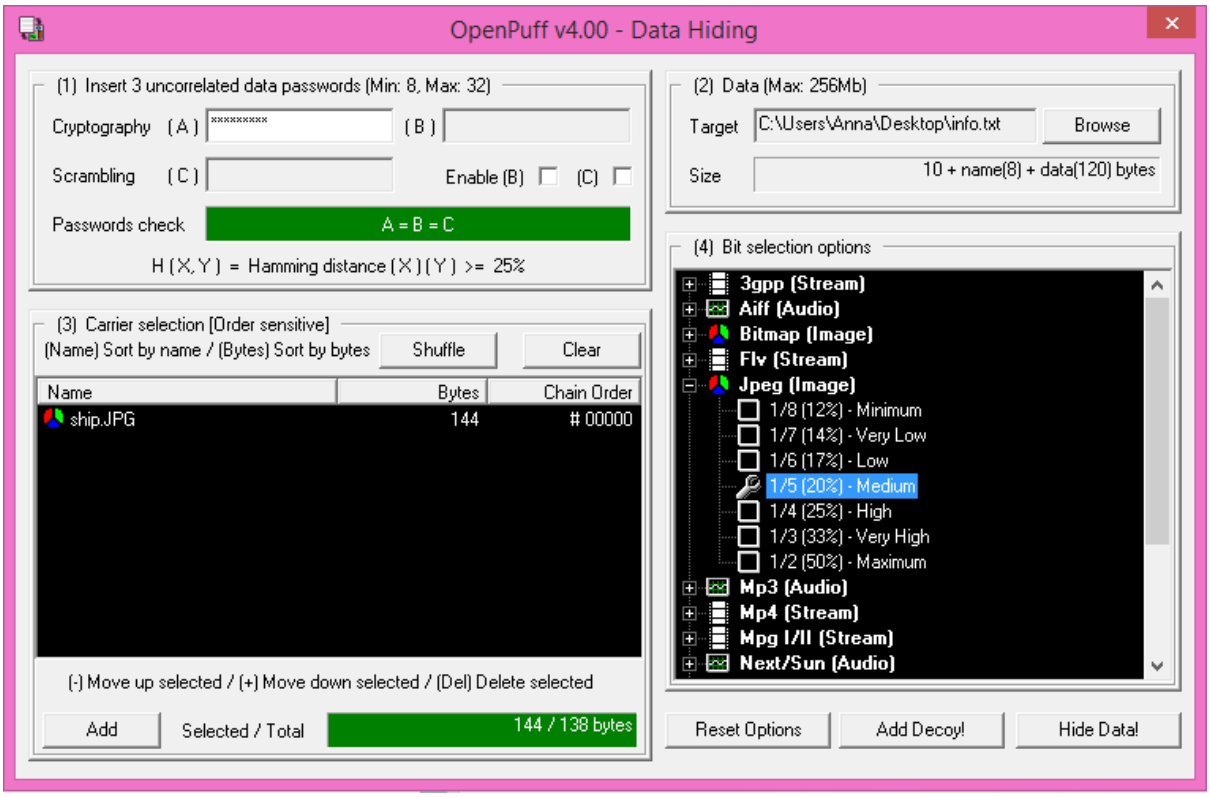

*Εικόνα 48 after hide information - Pixel difference histogram*

## Παράδειγμα 2- έγχρωμη εικόνα

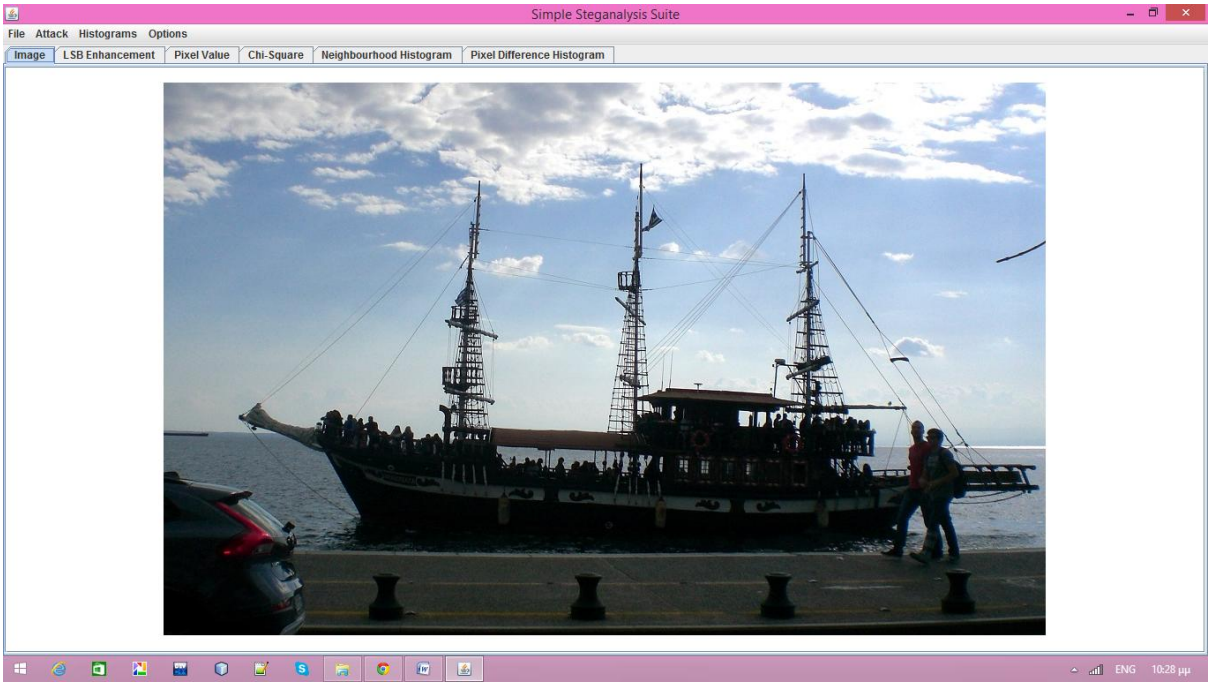
Και στο παράδειγμα 2 έχω πάρει τα στατιστικά και τα γραφήματα από την εικόνα χωρίς κρυμμένη πληροφορία και με κρυμμένη πληροφορία. Παρακάτω θα γίνουν συγκρίσεις μεταξύ των γραφημάτων και των στατιστικών.

Χαρακτηριστικά εικόνας: Όνομα ship.jpg με μέγεθος 204KB. Το αρχείο που ενσωμάτωσα είναι αρχείο .txt με μέγεθος 120 bytes

Για την ενσωμάτωση του αρχείου χρησιμοποίησα το OpenPuff.



Η επιλογή της εικόνας γίνετε File→ Open Image

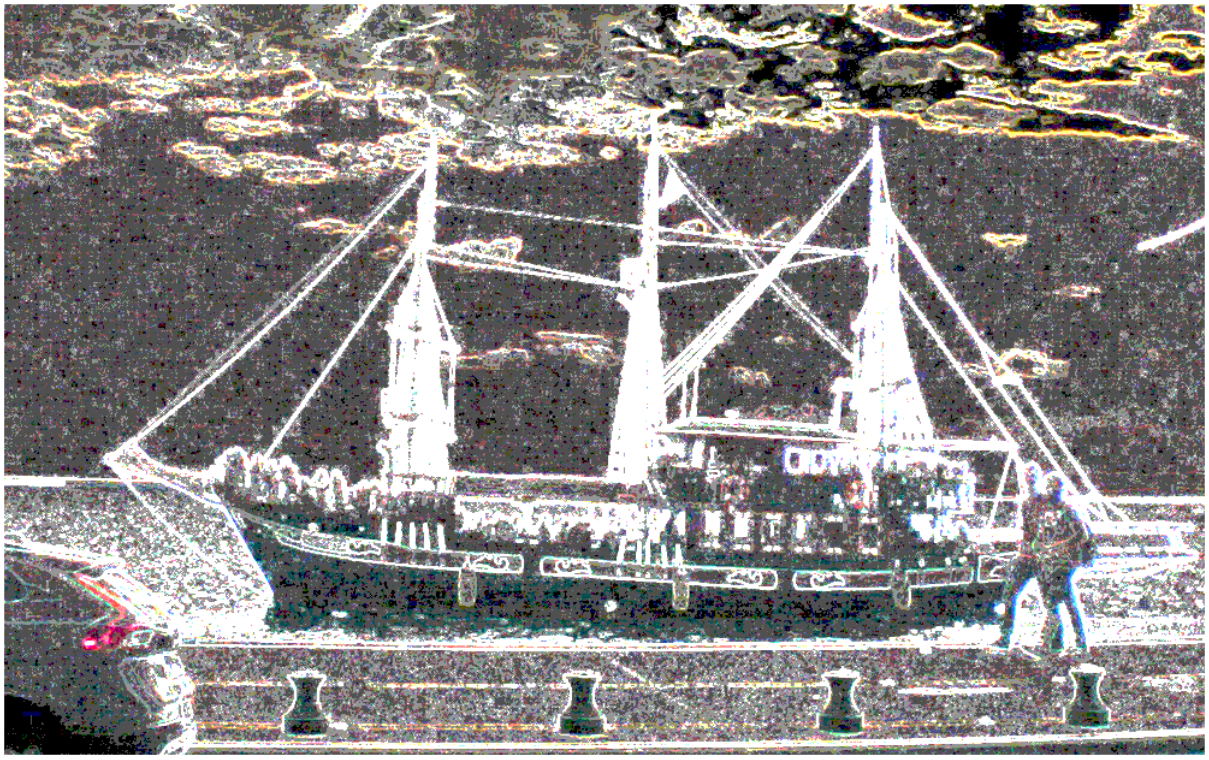



Η πρώτη σύγκριση θα γίνει με τα πρώτα αποτελέσματα της LSB Enhancement επίθεσης

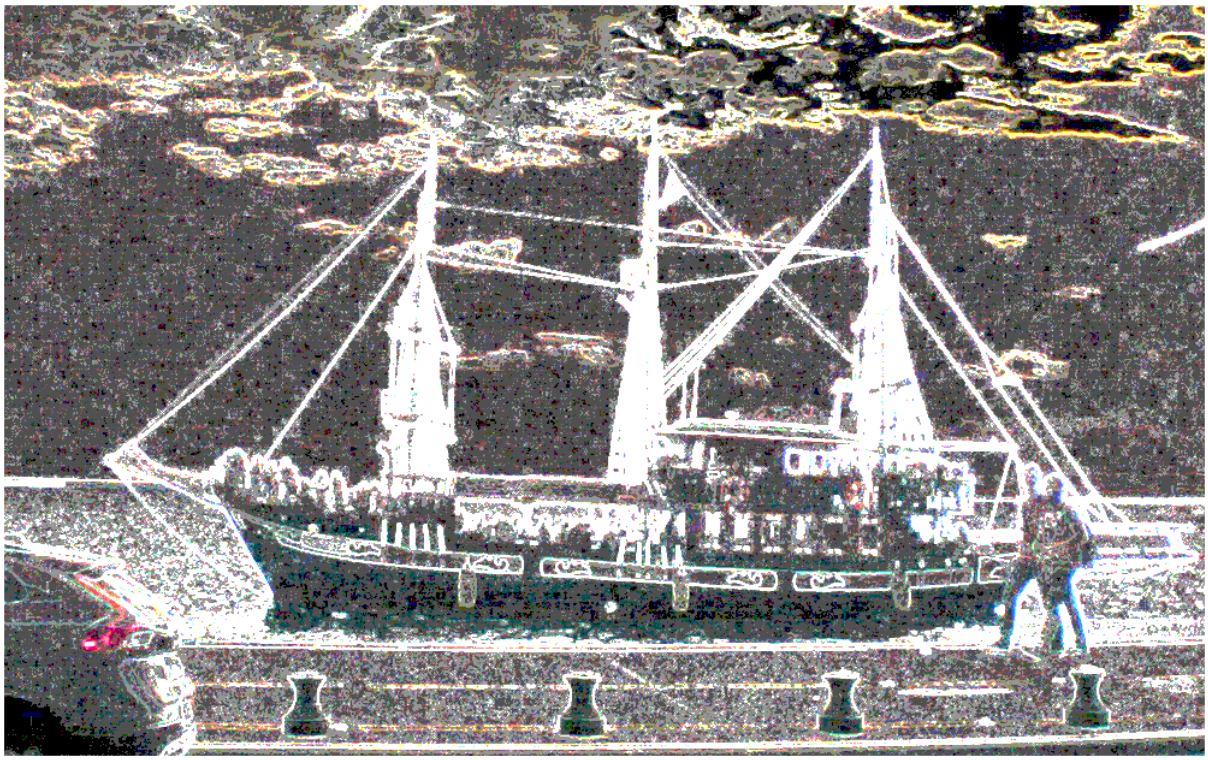
*Εικόνα 49 LSB before hide information*

*Εικόνα 50 LSB After hide informationn*

Αν δούμε με γρήγορη ματιά τις εικόνες, δεν θα παρατηρήσουμε ότι υπάρχουν μικρές διαφορές μεταξύ των δύο εικόνων. Κάποια pixel έχουν διαφορετικές τιμές πριν και μετά την ενσωμάτωση του αρχείου.

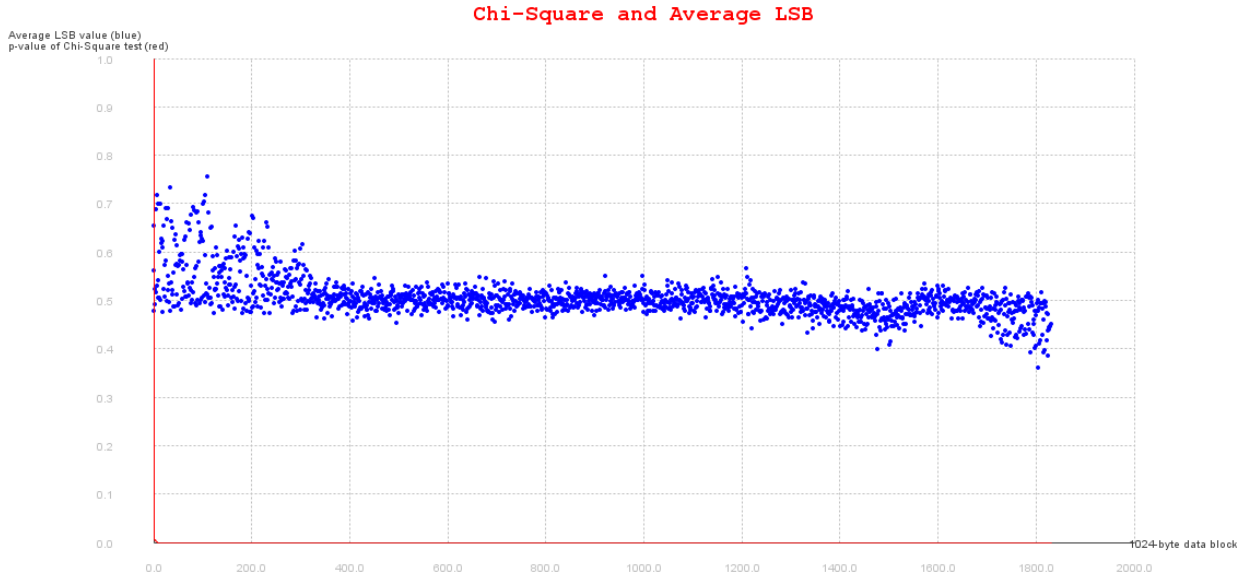


*Εικόνα 51 Pixel Value - before hide information*

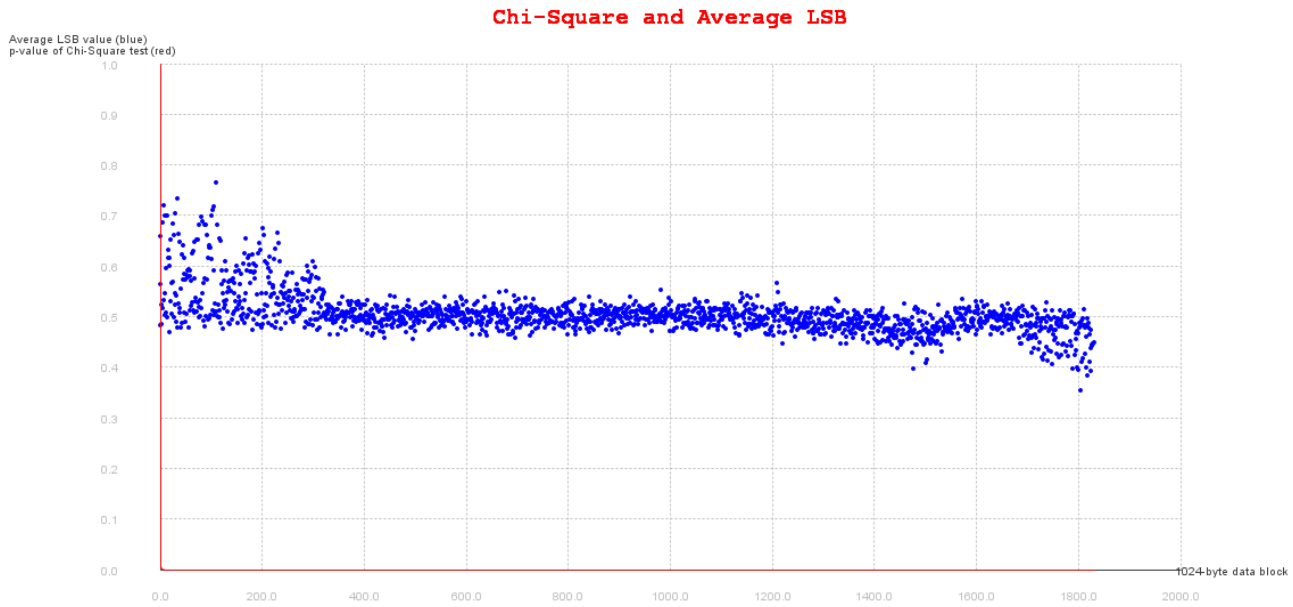


*Εικόνα 52 Pixel Value after hide information*

Ορισμός του Chi-Square: είναι μέτρηση των προσδοκιών σε σύγκριση με τα αληθινά αποτελέσματα. Τα στοιχεία που χρησιμοποιούνται είναι τυχαίες τιμές, με μεγάλη εμβέλεια.




*Εικόνα 53 Chi-square before hide information*

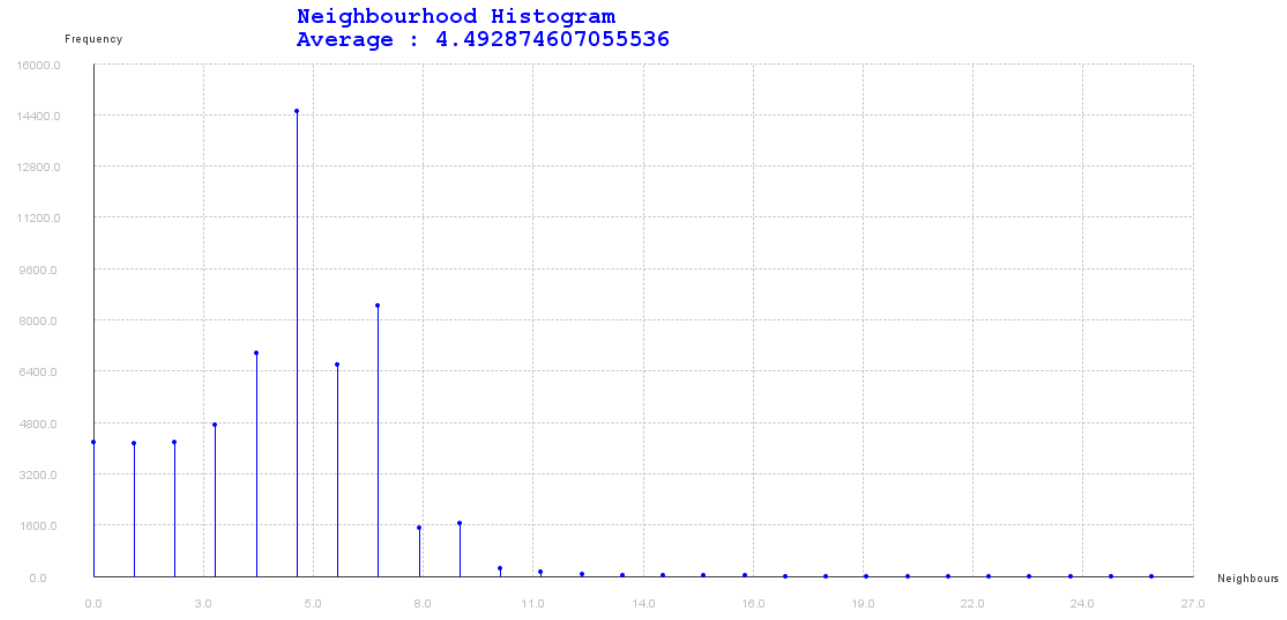



*Εικόνα 54 Chi-square after hide information*

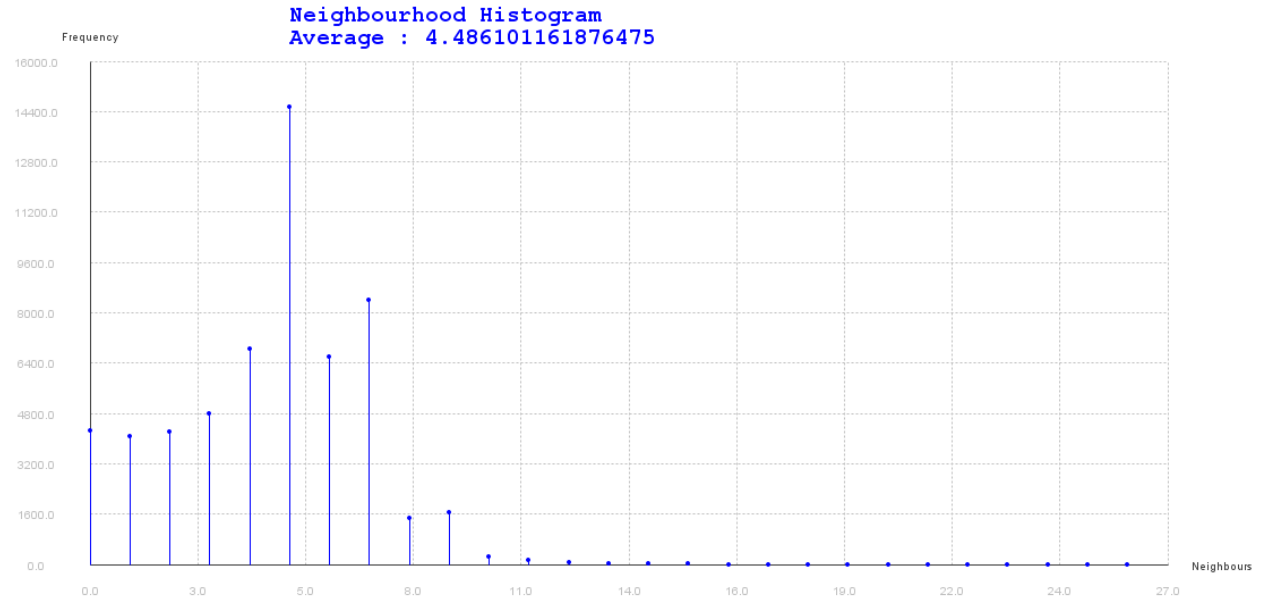
Με μπλε χρώμα Average LSB

Η κόκκινη γραμμή Chi Square

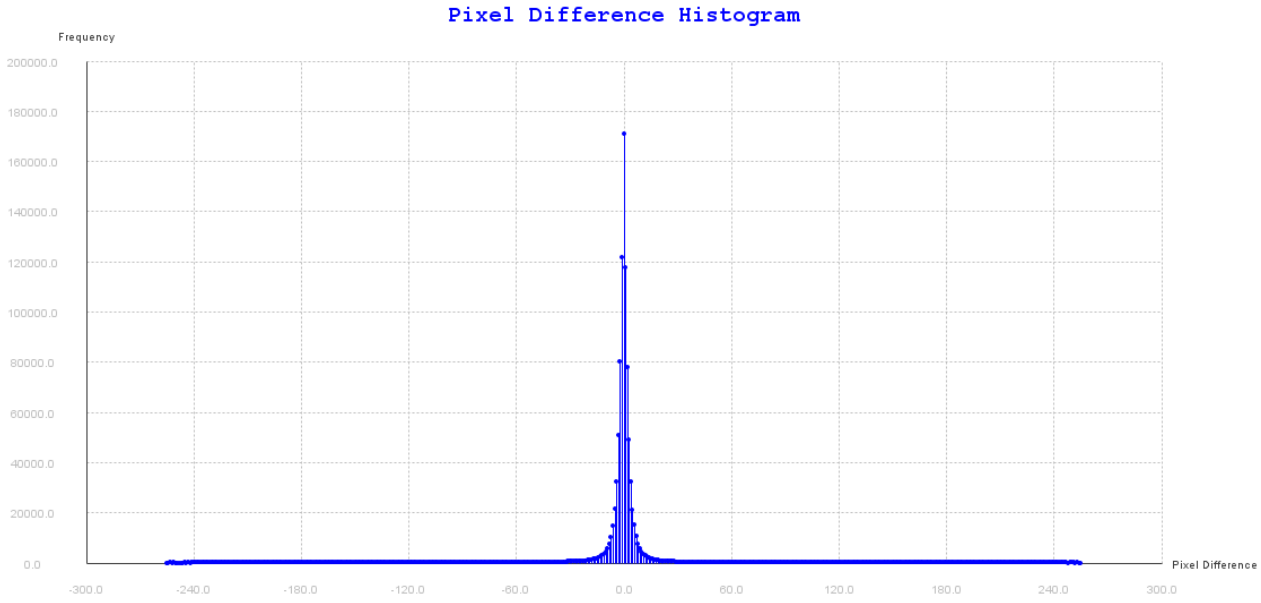
Στα γραφήματα αυτά παρατηρούμε μικρές διαφορές μεταξύ τους, είναι η διαφορά των τιμών των ελάχιστων σημαντικών ψηφίων.



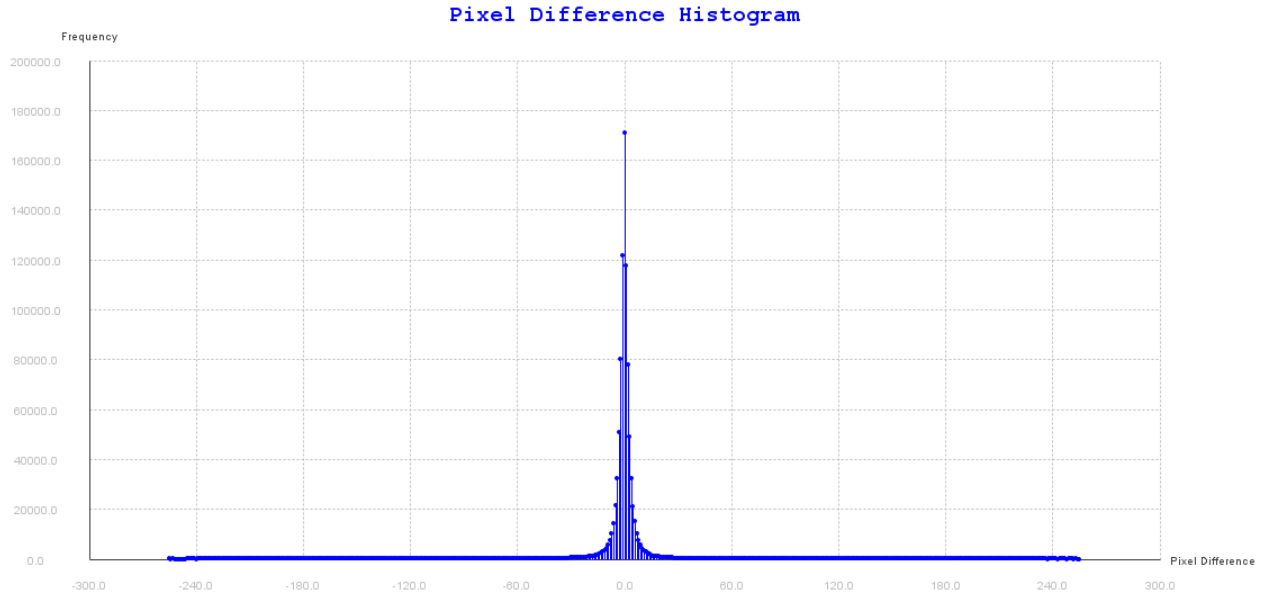

*Εικόνα 55 Neighbourhood Histogram before hide information*




*Εικόνα 56 Neighbourhood Histogram after hide information*




*Εικόνα 57 Pixel Difference Histogram before hide information*

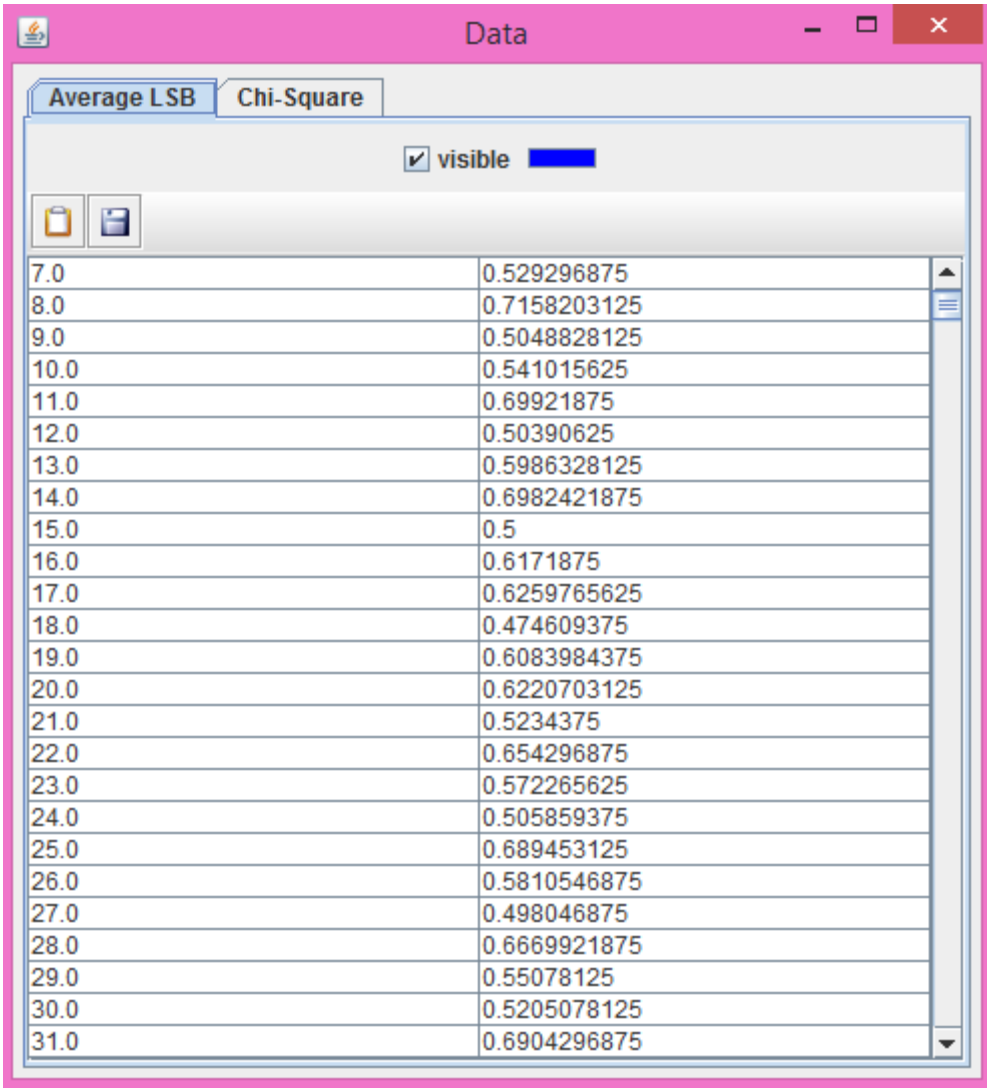



*Εικόνα 58 Pixel Difference Histogram after hide information*

Παρατηρούμε και εδώ ότι υπάρχουν πολύ μικρές διαφορές μεταξύ των γραφικών.

Επειδή όμως οι διαφορές είναι πολλοί μικρές, το πρόγραμμα μας δίνει τη δυνατότητα να έχουμε τα αποτελέσματα σε πίνακα, ώστε να μπορεί να γίνει ευκολότερα η σύγκριση. Στις παρακάτω εικόνες θα δείξω τα αποτελέσματα της εικόνας που περιέχει το κρυφό μήνυμα.

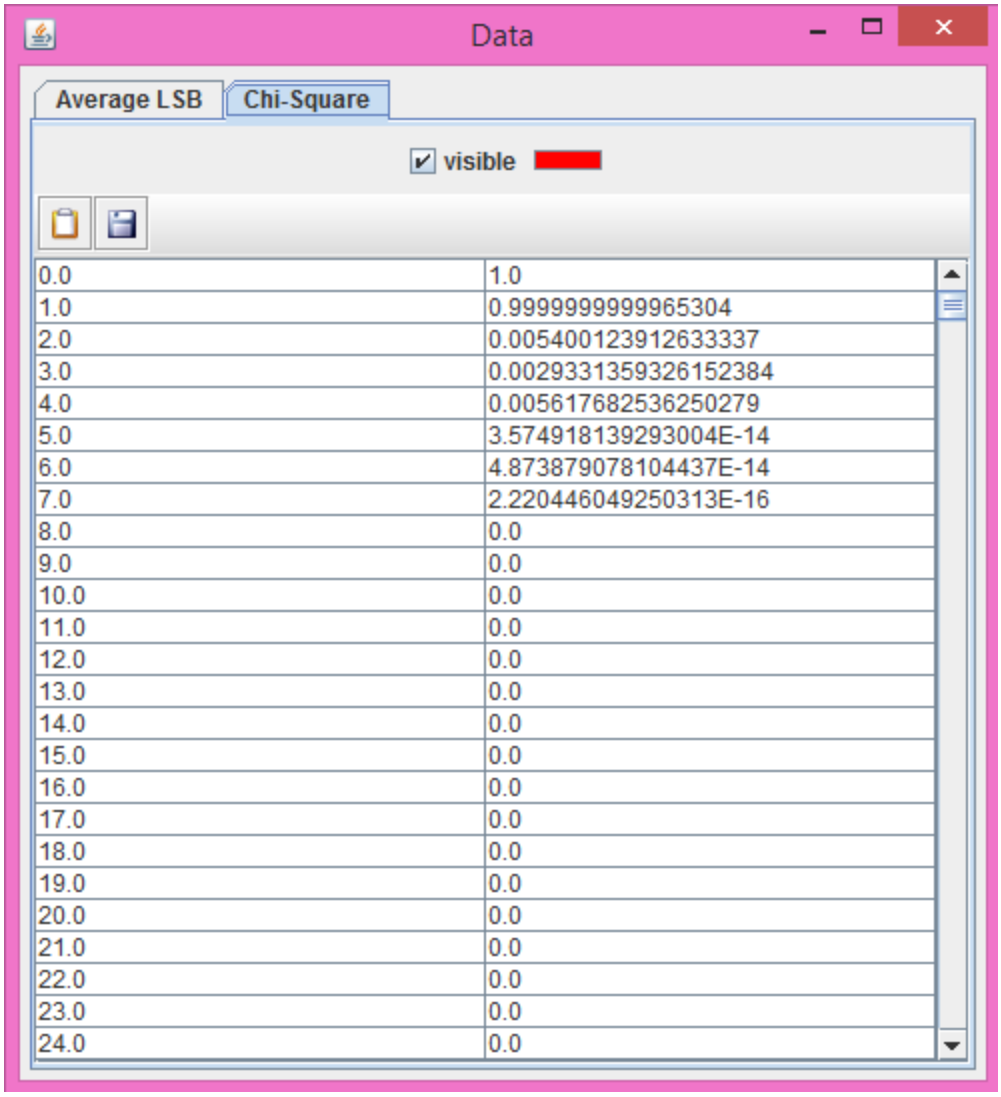
Στην αριστερή στήλη είναι τυχαίες τιμές στην δεξιά είναι οι τιμές μέσου όρου των LSB που πήρε σε αντιστοιχία με αυτές.




| | |
|---|---|
| 7.0 | 0.529296875 |
| 8.0 | 0.7158203125 |
| 9.0 | 0.5048828125 |
| 10.0 | 0.541015625 |
| 11.0 | 0.69921875 |
| 12.0 | 0.50390625 |
| 13.0 | 0.5986328125 |
| 14.0 | 0.6982421875 |
| 15.0 | 0.5 |
| 16.0 | 0.6171875 |
| 17.0 | 0.6259765625 |
| 18.0 | 0.474609375 |
| 19.0 | 0.6083984375 |
| 20.0 | 0.6220703125 |
| 21.0 | 0.5234375 |
| 22.0 | 0.654296875 |
| 23.0 | 0.572265625 |
| 24.0 | 0.505859375 |
| 25.0 | 0.689453125 |
| 26.0 | 0.5810546875 |
| 27.0 | 0.498046875 |
| 28.0 | 0.6669921875 |
| 29.0 | 0.55078125 |
| 30.0 | 0.5205078125 |
| 31.0 | 0.6904296875 |

*Εικόνα 59 Matrix Average LSB after hide information*

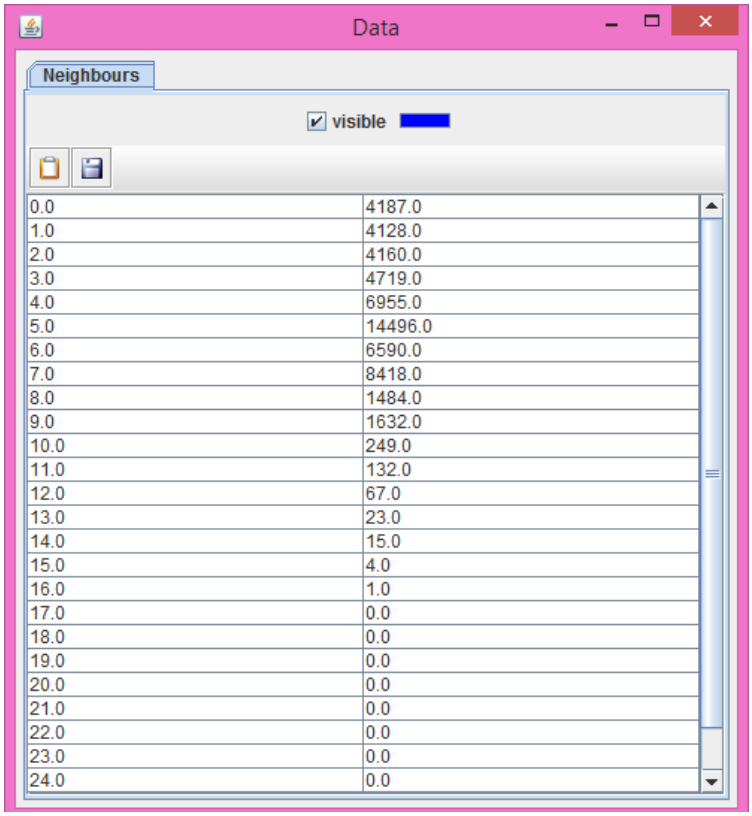
Στην καρτέλα του Chi-square στην αριστερή στήλη είναι τυχαίες τιμές και στην δεξιά οι τιμές που αντιστοιχούν σε αυτές.




| | |
|---|---|
| 0.0 | 1.0 |
| 1.0 | 0.9999999999965304 |
| 2.0 | 0.005400123912633337 |
| 3.0 | 0.0029331359326152384 |
| 4.0 | 0.005617682536250279 |
| 5.0 | 3.574918139293004E-14 |
| 6.0 | 4.873879078104437E-14 |
| 7.0 | 2.220446049250313E-16 |
| 8.0 | 0.0 |
| 9.0 | 0.0 |
| 10.0 | 0.0 |
| 11.0 | 0.0 |
| 12.0 | 0.0 |
| 13.0 | 0.0 |
| 14.0 | 0.0 |
| 15.0 | 0.0 |
| 16.0 | 0.0 |
| 17.0 | 0.0 |
| 18.0 | 0.0 |
| 19.0 | 0.0 |
| 20.0 | 0.0 |
| 21.0 | 0.0 |
| 22.0 | 0.0 |
| 23.0 | 0.0 |
| 24.0 | 0.0 |

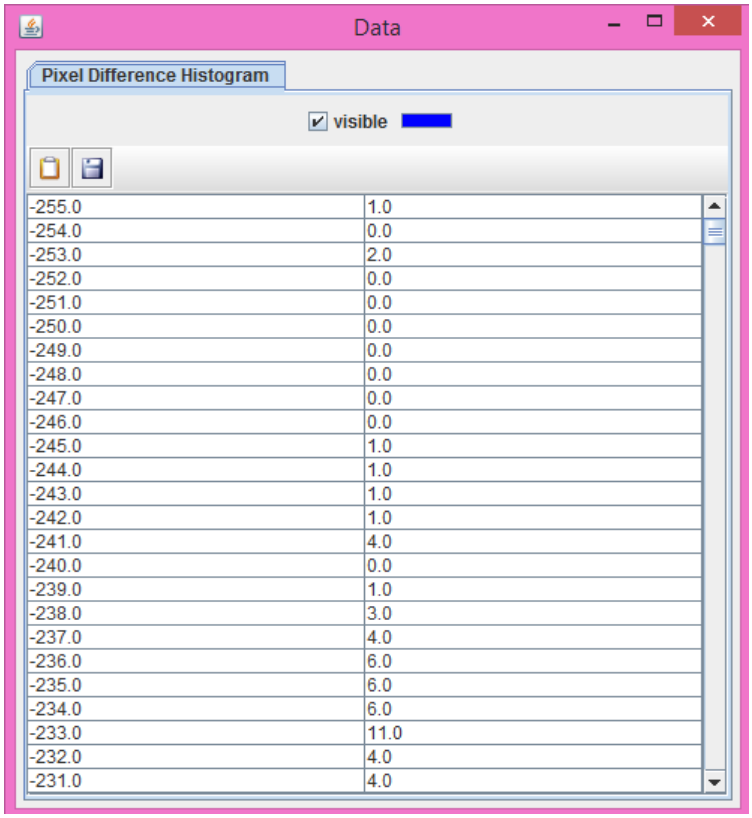
*Εικόνα 60 Chi-square after hide information*

Άλλα δείγματα που μπορούμε να πάρουμε είναι από την καρτέλα neighbourhood histogram. Είναι κατά πόσο ίδιες τιμές έχουν τα γειτονικά εικονοστοιχεία.




| | |
|---|---|
| 0.0 | 4187.0 |
| 1.0 | 4128.0 |
| 2.0 | 4160.0 |
| 3.0 | 4719.0 |
| 4.0 | 6955.0 |
| 5.0 | 14496.0 |
| 6.0 | 6590.0 |
| 7.0 | 8418.0 |
| 8.0 | 1484.0 |
| 9.0 | 1632.0 |
| 10.0 | 249.0 |
| 11.0 | 132.0 |
| 12.0 | 67.0 |
| 13.0 | 23.0 |
| 14.0 | 15.0 |
| 15.0 | 4.0 |
| 16.0 | 1.0 |
| 17.0 | 0.0 |
| 18.0 | 0.0 |
| 19.0 | 0.0 |
| 20.0 | 0.0 |
| 21.0 | 0.0 |
| 22.0 | 0.0 |
| 23.0 | 0.0 |
| 24.0 | 0.0 |

*Εικόνα 61 "Neighbours" after hide information*




| | |
|---|---|
| -255.0 | 1.0 |
| -254.0 | 0.0 |
| -253.0 | 2.0 |
| -252.0 | 0.0 |
| -251.0 | 0.0 |
| -250.0 | 0.0 |
| -249.0 | 0.0 |
| -248.0 | 0.0 |
| -247.0 | 0.0 |
| -246.0 | 0.0 |
| -245.0 | 1.0 |
| -244.0 | 1.0 |
| -243.0 | 1.0 |
| -242.0 | 1.0 |
| -241.0 | 4.0 |
| -240.0 | 0.0 |
| -239.0 | 1.0 |
| -238.0 | 3.0 |
| -237.0 | 4.0 |
| -236.0 | 6.0 |
| -235.0 | 6.0 |
| -234.0 | 6.0 |
| -233.0 | 11.0 |
| -232.0 | 4.0 |
| -231.0 | 4.0 |

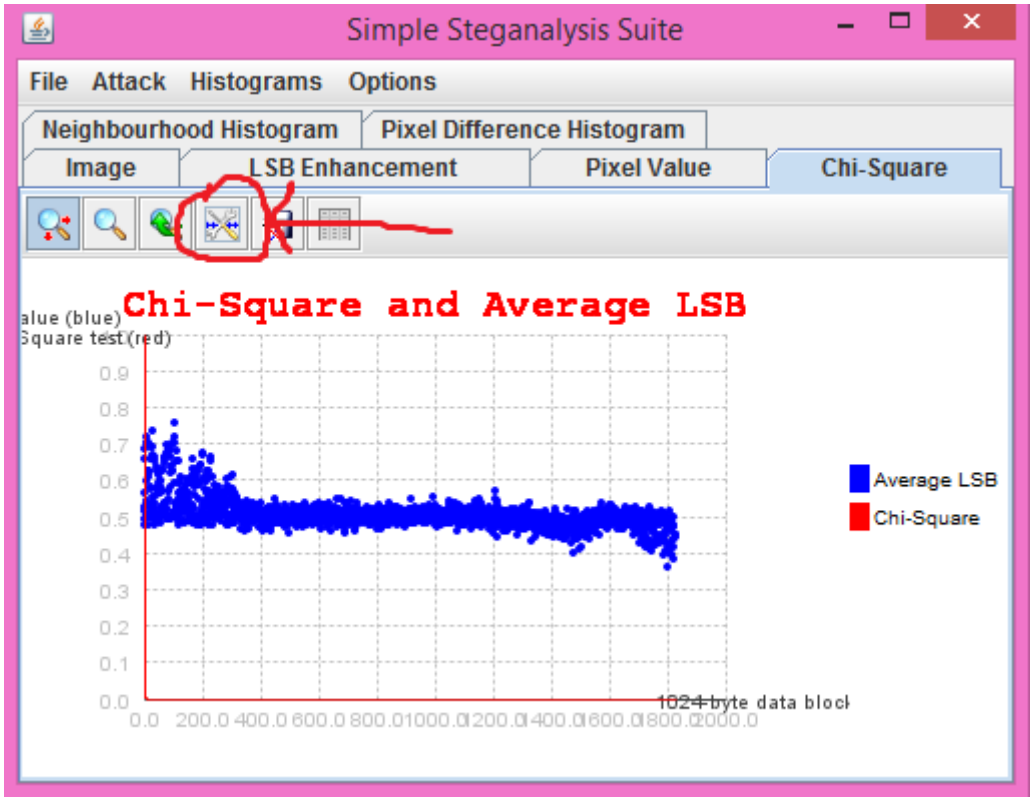
*Εικόνα 62 Pixel Difference Histogram after hide information*

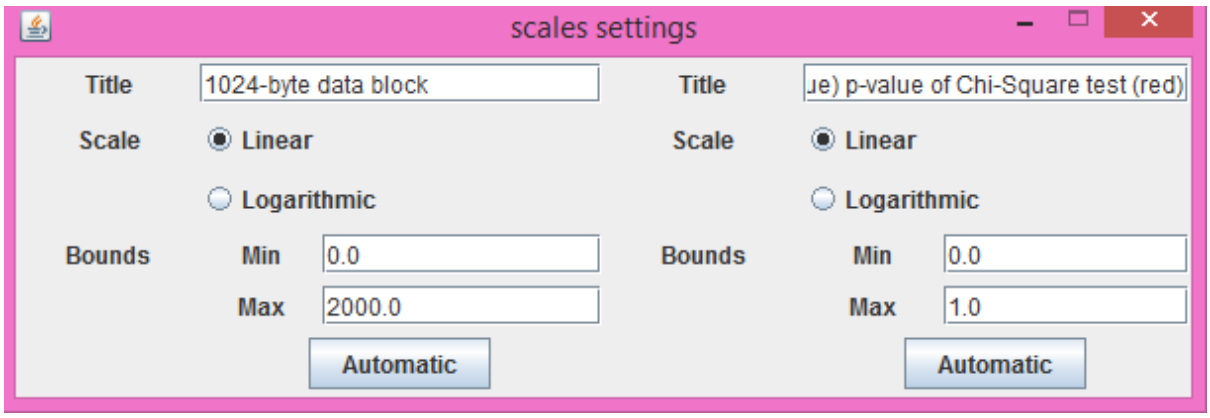
Οι τιμές είναι πολλές οπότε απλά επέλεξα να δείξω μόνο τις πρώτες τιμές που εμφανίζονται από το πρόγραμμα. Τον ίδιο πίνακα με διαφορετικές τιμές φυσικά, θα πάρουμε και από την εικόνα χωρίς το ενσωματωμένο αρχείο και συγκρίνοντας τα παρατηρούμε ότι υπάρχουν διαφορές στις τιμές.

Υπάρχουν διάφορες ρυθμίσεις όπως: scales settings, ρυθμίζεις την κλίμακα με την οποία θέλεις να εμφανίζονται τα δεδομένα(mix-max). Τους τίτλους των στηλών, οριζόντιος-κάθετος.

Τις ίδιες ρυθμίσεις έχουν οι καρτέλες *Chi-square, Neighbourhood Histogram* και *Pixel Difference Histogram*. Αν ρυθμίσεις σε μια καρτέλα τις τιμές, δεν σημαίνει ότι όλες οι καρτέλες έχουν πάρει τις ρυθμίσεις αυτές. Πρέπει σε κάθε μια ξεχωριστά να προσθέσεις τις αλλαγές.

Το άνοιγμα των ρυθμίσεων αυτών γίνεται με το πάτημα του τέταρτου κουμπιού (όπως φαίνεται στην παρακάτω εικόνα) σε κάθε μια από τις καρτέλες που προανέφερα.

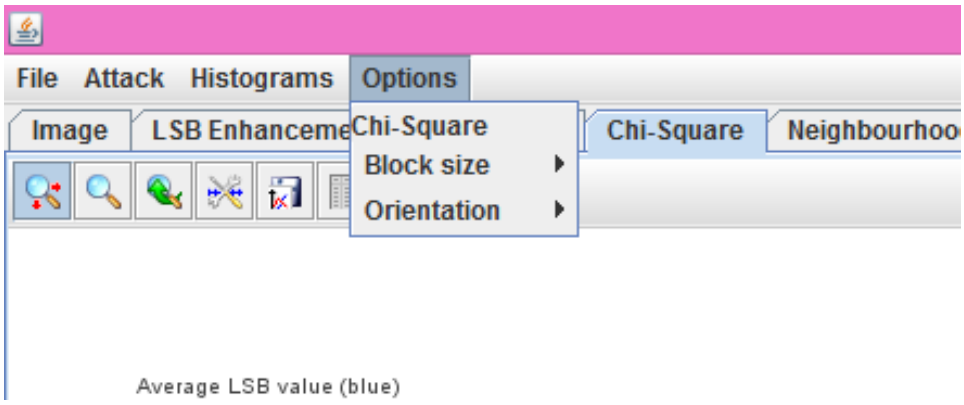



*Εικόνα 63 Scales settings*

Άλλες ρυθμίσεις για τη γραφική παράσταση chi-square είναι από το μενού *Options*, *Block size* και *Orientation*.

- Block size είναι το μήκος από bits με τα οποία δουλεύουν οι κρυπταλγόριθμοι.
- Orientation είναι ο προσανατολισμός των δεδομένων.


File
Attack
Histograms
Options
Image
LSB Enhanceme
Chi-Square
Block size
Orientation
Chi-Square
Neighbourhoo
Average LSB value (blue)

# ΚΕΦΑΛΑΙΟ 6

## Συμπεράσματα

Από τα αρχαία χρόνια γνωρίζουμε ότι η στεγανογραφία χρησιμοποιείται για την επικοινωνία μεταξύ κατασκόπων ή κατά τη διάρκεια πολέμου (βλ. Ηρόδοτος στην αρχαία Ελλάδα). Στη σύγχρονη εποχή η στεγανογραφία πλέον χρησιμοποιείται και από χρήστες που δεν έχουν καμία γνώση του αντικειμένου, λόγω ότι τα στεγανογραφικά εργαλεία είναι διαθέσιμα και στις περισσότερες φορές δωρεάν, επιπλέον το περιβάλλον εργασίας του κάθε προγράμματος σε αρκετές περιπτώσεις είναι εύχρηστο, αλλά στην περίπτωση που είναι περίπλοκο, για κάθε πρόγραμμα υπάρχει αντίστοιχο manual που και αυτό διατίθεται δωρεάν στο διαδίκτυο.

Η Στεγανογραφία σε συνδυασμό με την Κρυπτογραφία σαν μία υβριδική μορφή θα μπορούσε να πετύχει ένα πολύ καλό υψηλό επίπεδο ασφαλείας και απόρρητου, αλλά είναι ακόμα σε πρώιμο στάδιο. Απώτερος σκοπός των συστημάτων είναι να μην είναι κατανοητό όχι μόνο το μήνυμα (κρυπτογραφία) αλλά και την ίδια την ύπαρξη του μηνύματος(στεγανογραφία).

Αυτό έχει διάφορα πλεονεκτήματα και μειονεκτήματα. Πλεονέκτημα είναι ότι αυξάνει την δυνατότητα προστασίας της μυστικότητάς μας, ή την επικοινωνία όταν το απαιτούν οι συνθήκες. Μειονέκτημα είναι η αυξανόμενη δυνατότητα για ανεξέλεγκτη χρήση των τρομοκρατών.

Η Στεγανάλυση ενώ κατευθύνεται στο να γίνει αποτελεσματική, αντιμετωπίζει πολλά εμπόδια για να γίνει μια αξιόπιστη μέθοδος ανίχνευσης στεγανογραφικής δραστηριότητας. Η Στεγανογραφία και η Στεγανάλυση είναι ακόμα σε στάδια έρευνας και ανάπτυξης. Δεδομένου ότι οι τεχνικές για το κρύψιμο πληροφορίας βελτιώνονται, το ίδιο ισχύει και για την ανίχνευση.

Η μόνη επιλογή είναι η συνεχής πρόοδος. Η συνεχής πρόοδος και η έρευνα είναι ο μόνος τρόπος στο να μην σταματήσει ο κύκλος υπέρ εκείνων που κάνουν κακή χρήση της τεχνολογίας ή εναντίον εκείνων που την χρησιμοποιούν εις βάρος μας.

## *Βιβλιογραφία*


1. Γεώργιος Τσακάμης, Μεταπτυχιακή Διατριβή, Πανεπιστήμιο Πειραιώς - Τμήμα Πληροφορικής, 2011
2. Αποστολίδου Κυρική, Διπλωματική Εργασία, ΤΕΙ Δυτικής Μακεδονίας – ΠΜΣ Επιχειρηματικής Πληροφορικής
3. Σεβαστάκη Ιωάννα, Πτυχιακή Εργασία, Σχολή Τεχνολογικών Εφαρμογών – Τμήμα Εφαρμοσμένης Πληροφορικής, 2010
4. Μπαλκούρας Σωτήριος, Ειδική Επιστημονική Εργασία, Πανεπιστήμιο Πατρών, 2013

*Αναφορές*


1. Τι είναι η Στεγανογραφία που και πως την χρησιμοποιούμε, Γιώργος Επιτήδειος, 11/2013
2. openstego.info
3. stegoshare.sourceforge.net/
4. Steganalysis of JPEG Images: Breaking the F5 Algorithm, Jessica Fridrich, Mirosla Goljan, Dorin Hogea, 2010
5. Steganalysis Algorithms for detecting the hidden information image, audio and video cover media, Natarajan Meghanathan and Lopamudra Nayak, 2010
6. Ψηφιακό υδατόσημο, βικιπαίδεια.
7. Ritter's Crypto Glossary and Dictionary of Technical Cryptography, Terry Ritter, 8/2007
8. A Message in a Picture, Faure Bastien, 2012
9. OPENPUFFV4.00 STEGANOGRAPHY& WATERMARKING, manual en 7/2012
10. Attacking the OutGuess, Jessica Fridrich, Miroslav Goljan, Dorin Hogea
11. Pixel-Value Differencing Steganography: Attacks andImprovements, El-Sayed M. El-Alfy, Azzat A. Al-Sadi,
12. Image Steganography and Steganalysis: Concepts and Practice, Rajarathnam Chandramouli, Mehdi Kharrazi, Nasir Memon, 2004
13. http://bastienfaure.fr/forensic-challenge
14. Steganalysis: Chi-Square Attack & LSB Enhancement, http://cuneytcaliskan.blogspot.gr, 12/2011
15. Image steganography and steganalysis: consepts and practice, Rajarathnam Chandramouli, Mehdi Kharrazi, Nasir Memon,