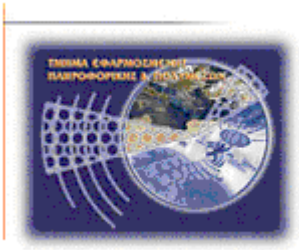
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Παρουσίαση Στεγανογραφικών Τεχνικών

Χριστίνα Καλαϊτζή(ΑΜ:2616)
E-mail: epp2616@teicrete.gr

Ηράκλειο – 11-03-2011

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

***<u>Υπεύθυνη Δήλωση</u>**: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να εκφράσω την ευγνωμοσύνη μου στους γονείς και στην αδερφή μου που με στήριξαν όλα αυτά τα χρόνια και έκαναν μεγάλη υπομονή. Ευχαριστώ πολύ για όλα.
Θα ήθελα να ευχαριστήσω τον κ. Χαράλαμπο Μανιφάβα, επιβλέποντας αυτής της πτυχιακής εργασίας για την καθοδήγηση και τις συμβουλές του. Ήταν μεγάλη τιμή για εμένα να συνεργαστώ μαζί του.

Περίληψη

Στεγανογραφία είναι η τεχνική σύμφωνα με την οποία το μυστικό μήνυμα κρύβεται μέσα σε ένα άλλο είδος πληροφορίας, η διακίνηση της οποίας δεν κινεί καμία υποψία. Στην κρυπτογραφία το μυστικό μήνυμα κωδικοποιείται και παρόλο που η ύπαρξή του είναι γνωστή, η ασφάλεια του αλγόριθμου και του κλειδιού που χρησιμοποιούνται εγγυώνται και την ασφάλεια του μηνύματος. Τα κρυπτογραφημένα μηνύματα όμως αποτελούν στόχο περαιτέρω έρευνας από όποιον έχει ενδιαφέρον να αποκαλύψει το περιεχόμενο της επικοινωνίας. Τα στενογραφημένα μηνύματα δεν αποτελούν στόχο επειδή σκοπός είναι να κρύψουμε την ίδια την ύπαρξη του μηνύματος μέσα σε αθώα πληροφορία.

Η μέθοδος της στεγανογραφίας είναι γνωστή από την αρχαιότητα. Μέχρι σήμερα έχει κάνει την εμφάνισή της σε σημαντικά ιστορικά γεγονότα με πιο πρόσφατα, τους δύο παγκόσμιους πολέμους και την τρομοκρατία. Στο πρόσφατο παρελθόν έχουν αναπτυχθεί τεχνικές οι οποίες κρύβουν μηνύματα μέσα σε αρχεία κειμένου, εικόνων, ήχου ή video χωρίς η αλλοίωση των αρχείων να είναι αντιληπτή από ένα κοινό χρήστη. Επίσης έχουν αναπτυχθεί τεχνικές που συνδυάζουν στεγανογραφία και κρυπτογραφία.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

Κεφάλαιο 1
Εισαγωγή στη Στεγανογραφία

1.1 Γενικά

Σε έναν ιδανικό κόσμο όλοι θα ήμασταν σε θέση να στέλναμε εύκολα το κρυπτογραφημένο κείμενό μας μέσο e-mail ή αρχεία ο ένας στον άλλο χωρίς συνέπειες. Παρόλα αυτά υπάρχουν συχνά περιπτώσεις κατά τις οποίες αυτό δεν είναι δυνατό, είτε επειδή εργαζόμαστε σε μια επιχείρηση που δεν επιτρέπει την ανταλλαγή κρυπτογραφημένων μηνυμάτων μέσο e-mail είτε γιατί η τοπική κυβέρνηση δεν εγκρίνει την χρήση της κρυπτογραφημένης επικοινωνίας (μια πραγματικότητα σε μερικά μέρη του κόσμου). Σε αυτό το σημείο η Στεγανογραφία μπαίνει στη ζωή μας.

Είναι μία αρχαία τεχνική η οποία έχει καταφέρει με τη βοήθεια του διαδικτύου και της τεχνολογίας να αναπτυχθεί και να διαδοθεί ευρέως. Πολλά δημόσια στεγανογραφικά λογισμικά, όπως η S-Εργαλεία, EZStego και Steganos εφαρμόζουν την τεχνική αυτή. Παράλληλα όμως γίνονται εντεταμένες προσπάθειες για προστασία της μυστικότητας μας, άλλα και της οποιαδήποτε επικοινωνίας. Βέβαια παρόλα τα μέτρα που έχουν ληφθεί δεν περιορίζεται η εγκληματική χρήση.

Η Στεγανογραφία τροποποιεί ένα κομμάτι πληροφορίας και το κρύβει μέσα σε άλλη. Τα αρχεία υπολογιστών (εικόνα, ήχος, ακόμη και οι αποθηκευτικοί δίσκοι) περιέχουν αχρησιμοποίητους ή ασήμαντους τομείς δεδομένων. Η τέχνη της Στεγανογραφίας εκμεταλλεύεται αυτές τις περιοχές, αντικαθιστώντας τις με χρήσιμες πληροφορίες. Τα αρχεία αυτά μπορούν να ανταλλαχθούν χωρίς κανείς να ξέρει τι βρίσκεται πραγματικά μέσα τους. Μια φωτογραφία μας μπορεί εύκολα να περιέχει μια προσωπική επιστολή σε έναν φίλο. Η καταγραφή μιας σύντομης πρότασης μπορεί να περιέχει τα σχέδια της επιχείρησής μας για ένα νέο μυστικό προϊόν. Η Στεγανογραφία μπορεί επίσης να χρησιμοποιηθεί για να τοποθετήσει ένα κρυμμένο "εμπορικό σήμα" στις εικόνες, τη μουσική, video και σε λογισμικό, μια τεχνική που θα δούμε παρακάτω με την ονομασία Υδατογράφημα.

Η στεγανογραφία είναι μία τεχνική που χρησιμοποιείται για την απόκρυψη πληροφορίας μέσα σε μία άλλη πληροφορία. Το μήνυμα αποκρύπτεται με διάφορους τρόπους και κανείς δεν υποπτεύεται την ύπαρξή του. Στηρίζεται στο γεγονός ότι οι ανθρώπινες αισθήσεις δεν είναι δυνατό αντιληφθούν μικρές αλλαγές. Από την άλλη η στεγανάλυση αναφέρεται σε μεθόδους που διαχωρίζουν την κρυμμένη πληροφορία από την ορατή πληροφορία.

Σε αντίθεση με τη κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει τη πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Τα περισσότερα συστήματα ασφαλείας, ακόμα και αυτά που χρησιμοποιούμε καθημερινά στο internet, βασίζονται στην κρυπτογράφηση μηνυμάτων. Άλλοτε συμμετρική άλλοτε ασύμμετρη. Σε γενικές γραμμές για να κρυπτογραφήσουμε ένα κείμενο (γενικά οποιοδήποτε αρχείο binary) θα πρέπει να το μετασχηματίσουμε σε

ένα άλλο, χρησιμοποιώντας μια κωδική λέξη και έναν αλγόριθμο κρυπτογράφησης. Το αποτέλεσμα θα είναι να δημιουργήσουμε ένα νέο κείμενο, όπου κανείς δε θα μπορεί να διαβάσει χωρίς να έχει στα χέρια του τον αλγόριθμο αποσυμπίεσης και την κωδική λέξη που χρησιμοποιήσαμε.

Παρακάτω παρουσιάζονται τα πλεονεκτήματα και τα μειονεκτήματα της στεγανογραφίας σε σύγκριση με τη κρυπτογραφία

Πλεονεκτήματα

• Η χρήση της κρυπτογραφίας είναι σε κάποιες περιπτώσεις προβληματική επειδή η παρουσία κρυπτογραφημένης πληροφορίας αποτελεί στόχο.

• Με τη στεγανογραφία η πληροφορία δεν κρυπτογραφείται, απλά κρύβεται

Μειονεκτήματα

• Υψηλή επιβάρυνση για λίγη πληροφορία

• Αν η μέθοδος αποκαλυφθεί τότε δεν παρέχεται καμιά προστασία

1.2 Σκοπός της Πτυχιακής Εργασίας

Η εργασία αυτή έχει σκοπό να ερευνήσει την χρήση της τεχνολογίας αυτής στην σημερινή εποχή σε όλες τις μορφές που παρουσιάζεται και να επικεντρωθεί σε συστήματα εικόνων και video.

1.3 Συνοπτική Περιγραφή Αναφοράς

Στο κεφάλαιο 1 παρουσιάζονται γενικές πληροφορίες για το θέμα της πτυχιακής, την εισαγωγή και την περιγραφή της στεγανογραφίας.

Στο κεφάλαιο 2 παρουσιάζονται διάφορες εμφανίσεις της ιστορικής αναδρομής της στεγανογραφίας και λίγα λόγια για την στεγανογραφία- κρυπτογραφία.

Το κεφάλαιο 3 αναφέρεται στους ορισμούς-ιδιότητες της στεγανογραφίας, τύπους αρχείων, περιγραφή στεγανάλυσης και υδατογραγραφήματος και υλοποίηση στεγανογραφίας σε εικόνες.

Στο κεφάλαιο 4 αναφέρεται η περιγραφή διαδικασίας απόκρυψης κειμένου μέσα σε εικόνα και τέλος μετατροπή μιας εικόνας από αναλογική μορφή σε ψηφιακή και κρύψιμο στοιχείων σε ήχο.

Στο κεφάλαιο 5 περιγράφεται διάφορα θεωρητικά συμπεράσματα επίσης περιγράφεται στην στεγανογραφία και κρυπτογραφία.

Στο κεφάλαιο 6 περιγράφεται αναλυτικά από τα πέντε στεγανογραφικά προγράμματα που αναφέρονται.

1.4 Σχεδιάγραμμα Αναφορά

Κεφάλαιο 2
Ιστορική Αναδρομή της Στεγανογραφίας

Καθ' όλη τη διάρκεια της ιστορίας, ένα πλήθος μεθόδων και παραλλαγών έχουν χρησιμοποιηθεί για να κρύψουν πληροφορίες. Στα πρώτα σημάδια εμφάνισης της Στεγανογραφίας είναι από την εποχή του Ηρόδοτου στην αρχαία Ελλάδα, ο οποίος περιγράφει πως οι έλληνες έκρυβαν ένα μήνυμα σε ειδικές ξύλινες πλάκες που χρησιμοποιούσαν για γραφή και μετά το κάλυπταν με κερί. Σε μια ιστορία του ο Δημάρατος θέλησε να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης σκόπευε να εισβάλει στην Ελλάδα.

Για να αποφύγει τη σύλληψη, έξυσε το μήνυμα στην ξύλινη πλάκα και έπειτα κάλυψε την πλάκα με κερί. Οι πλάκες εμφανίστηκαν να είναι κενές και αχρησιμοποίητες ,έτσι πέρασαν τον έλεγχο από τους φρουρούς χωρίς καμία υποψία.

Μια άλλη έξυπνη μέθοδος ήταν να ξυριστεί το κεφάλι ενός αγγελιοφόρου και να του κάνουν τατουάζ ένα μήνυμα ,μια εικόνα ή και ένα χάρτη (π.χ. πειρατές) στο κεφάλι του. Μετά από λίγο χρόνο αφού μακρύνουν τα μαλλιά του , το μήνυμα θα ήταν μη ορατό έως ότου ξυρίσει πάλι το κεφάλι.

Μια άλλη κοινή μορφή αόρατου μηνύματος είναι μέσο της χρήσης των ‘‘αόρατων μελανιών’’. Σε τέτοια μελάνια χρησιμοποιήθηκαν με πολλή επιτυχία τον δεύτερο παγκόσμιο πόλεμο. Μια αθώα επιστολή μπορεί να περιέχει ένα πολύ διαφορετικό μήνυμα που γράφεται μεταξύ των γραμμών. Νωρίς στον δεύτερο παγκόσμιο πόλεμο η τεχνολογία της Στεγανογραφίας αποτελούταν σχεδόν αποκλειστικά από τα αόρατα μελάνια. Σα κοινά υλικά για τα αόρατα μελάνια είναι γάλα, ξίδι, χυμοί φρούτων και ούρα. Όλοι αυτά σκουραίνουν όταν θερμαίνονται.

Με τη βελτίωση της τεχνολογίας και την ευκολία ως προς την αποκωδικοποίηση των αόρατων μελανιών, περιπλοκότερα μελάνια αναπτύχθηκαν στο να αντιδρούν μόνο σε συγκεκριμένες χημικές ουσίες. Μερικά μηνύματα έπρεπε επεξεργαστούν κατάλληλα όπως οι φωτογραφίες αναπτύσσονται με διάφορες χημικές ουσίες στα εργαστήρια .

Μηνύματα ως Null Ciphers[1] (όχι κρυπτογράφημα) χρησιμοποιήθηκαν επίσης. Στο πραγματικό μήνυμα είναι καμουφλαρισμένο σε ένα αθώο μήνυμα. Λόγω της "φήμης" πολλών ανοικτών κωδικοποιημένων μηνυμάτων, οι ύποπτες επικοινωνίες ανιχνεύθηκαν από διάφορα αντικατασκοπικά φίλτρα . Εν ολίγης αρκετά "αθώα" μηνύματα μπόρεσαν να διαπεράσουν. Ένα παράδειγμα ενός μηνύματος null cipher περιέχει κρυμμένο ένα μήνυμα τέτοιας μορφής:

Π.χ.: Fi**s**hing fr**e**shwater be**n**ds an**d** sa**l**twater
co**a**sts re**w**ards an**y**one fe**e**ling st**r**essed.
Re**s**ourceful ang**g**lers us**u**ally fi**n**d mas**t**erful
le**a**pers fu**n** an**d** ad**m**it sw**o**rdfish ra**n**k
ov**e**rwhelming an**y**day.

[1] http://en.wikipedia.org/wiki/Null_cipher

Διαβάζοντας το τρίτο γράμμα από κάθε λέξη το μήνυμα που προκύπτει είναι :

Send Lawyers, Guns, and Money.

Στο ακόλουθο μήνυμα είναι ένα αληθινό γεγονός που στάλθηκε στον δεύτερο παγκόσμιο πόλεμο :

A**p**parently n**e**utral's p**r**otest i**s** t**h**oroughly d**i**scounted
a**n**d i**g**nored. I**s**man h**a**rd h**i**t. B**l**ockade i**s**sue a**f**fects
p**r**etext f**o**r e**m**bargo o**n** b**y**-products, e**j**ecting s**u**ets a**n**d v**e**getable o**i**ls.

Διαβάζοντας το δεύτερο γράμμα από κάθε λέξη το μήνυμα που προκύπτει είναι :

Pershing sails from NY June 1.

Η ανίχνευση μηνυμάτων βελτιωνόταν, παράλληλα νέες τεχνολογίες αναπτύχθηκαν που θα μπορούσαν να περάσουν περισσότερες πληροφορίες και να είναι λιγότερο ευδιάκριτες. Οι Γερμανοί ανέπτυξαν τα Microdots (μικροσκοπική τεχνολογία) από την οποία ο κάποτε διευθυντής του FBI J.Edgar Hoover χαρακτήρισε ως " the enemy's masterpiece of espionage." Τα Microdots είναι μικροσκοπικές φωτογραφίες που περιέχουν δεδομένα στο μέγεθος μιας τυπωμένης τελείας σε μία δακτυλογραφημένη σελίδα. Τα πρώτα Microdots ανακαλύφθηκαν μεταμφιεσμένα σε έναν δακτυλογραφημένο φάκελο που μεταφέρθηκε από έναν γερμανό πράκτορα το 1941. Το μήνυμα δεν ήταν κρυμμένο, ούτε κρυπτογραφημένο. Απλά ήταν ακριβώς τόσο μικρό ώστε να μην τραβήξει ποτέ τη παραμικρή προσοχή . Παρά το μέγεθος τους, τα Microdots επέτρεψαν τη διαβίβαση μεγάλων σε όγκο πληροφοριών συμπεριλαμβανομένων και διαφορών σχεδίων και φωτογραφιών.

Μετά από πολλές μεθόδους που ανακαλύφθηκαν και που καταδιώχτηκαν, διάφορες κυβερνήσεις έλαβαν ακραία μέτρα που μπορεί να μας φαίνονται πολύ αστεία σήμερα όπως στις ΗΠΑ η απαγόρευση των γρίφων, σταυρολέξων, οδηγίες πλεξίματος, αποκόμματα εφημερίδων, ακόμα και παιδικές ζωγραφιές δεδομένου ότι μπορούν όλα να περιέχουν μυστικά μηνύματα. Οι αρμόδιες αρχές ενέργησαν ακόμη και στην αντικατάσταση των γραμματοσήμων στους φακέλους. Απαγορεύτηκαν επίσης όλες οι διεθνείς παραγγελίες παραδόσεων συγκεκριμένων τύπων λουλουδιών που περιείχαν συγκεκριμένες ημερομηνίες παράδοσης από τις κυβερνήσεις των ΗΠΑ και Βρετανίας. Στην ΕΣΣΔ όλες οι διεθνείς ταχυδρομικές επιστολές απαγορεύτηκαν στην προσπάθεια να εμποδίσουν οποιαδήποτε εχθρική δραστηριότητα.

Με κάθε ανακάλυψη ενός μηνύματος που κρύβεται χρησιμοποιώντας μια υπάρχουσα τεχνολογική εφαρμογή, μια νέα στεγανογραφική τεχνική επινοείται. Υπάρχουν ακόμη και τάσεις για επαναχρησιμοποίηση παλαιών μεθόδων. Στα σχέδια και οι ζωγραφιές έχουν χρησιμοποιηθεί συχνά για να κρύψουν ή να αποκαλύψουν πληροφορίες. Είναι απλό να κωδικοποιηθεί ένα μήνυμα με την ποικιλία γραμμών, χρωμάτων ή άλλων στοιχείων μίας

εικόνας. Οι υπολογιστές φέρνουν μια τέτοια μέθοδο σε νέες διαστάσεις όπως θα δούμε αργότερα.

Ακόμη και το σχεδιάγραμμα ενός εγγράφου μπορεί να παρέχει πληροφορίες για το ίδιο έγγραφο. Ο Brassil και άλλοι, σε μια σειρά δημοσιεύσεων εξετάζουν τον προσδιορισμό εγγράφων και το χαρακτηρίζουν σύμφωνα με τη διαμόρφωση της θέσης των γραμμών και των λέξεων. Παρόμοιες τεχνικές μπορούν επίσης να χρησιμοποιηθούν για να παρέχουν κάποιες άλλες "συγκαλυμμένες" πληροφορίες ακριβώς σαν το 0,1 που είναι πηγές πληροφορίας σε έναν υπολογιστή. Όπως σε ένα από τα παραδείγματά τους, η λέξη-μετατόπιση μπορεί να χρησιμοποιηθεί για να βοηθήσει να προσδιοριστεί ένα έγγραφο. Μια παρόμοια μέθοδος μπορεί να εφαρμοστεί για να εμφανίσει ένα εξ ολοκλήρου διαφορετικό μήνυμα. Η ακόλουθη πρόταση:

Το παρόν αποτελεί μία εργασία όχι για την κρυπτογραφία αλλά για μία συγγενής έννοια. Σην χρησιμοποίησε ο Γερμανικός στρατός κατά τη διάρκεια του Β' παγκοσμίου πολέμου και ονομάζεται στεγανογραφία.

Αν πριν από κάθε λέξη που θέλουμε να περάσουμε αυξήσουμε το κενό διπλάσια από ότι το κανονικό τότε το αποτέλεσμα του αλγορίθμου θα μπορούσε να είναι:

Το παρόν αποτελεί μία εργασία όχι για την κρυπτογραφία αλλά για μία συγγενής έννοια. Την χρησιμοποίησε ο Γερμανικός στρατός κατά τη διάρκεια του Β' παγκοσμίου πολέμου και ονομάζεται στεγανογραφία.

Οι προτάσεις που περιέχουν τις κρυμμένες λέξεις εμφανίζονται αβλαβείς καθώς και όλο το μήνυμα φαίνεται αθώο, αλλά ο συνδυασμός αυτός με τον συγκεκριμένο αλγόριθμο παράγει ένα διαφορετικό μήνυμα:

όχι κρυπτογραφία χρησιμοποίησε στεγανογραφία.

Λίγα λόγια για την στεγανογραφία- κρυπτογραφία…

Η μακροβιότητα της στεγανογραφίας καταδεικνύει ότι σίγουρα παρέχει μια κάποια ασφάλεια, πάσχει ωστόσο από μια θεμελιώδη αδυναμία. Αν αγγελιαφόρος υποστεί σωματική έρευνα και το μήνυμα αποκαλυφθεί, τότε το περιεχόμενο της μυστικής επικοινωνίας φανερώνεται αμέσως. Η υποκλοπή του μηνύματος ακυρώνει αυτομάτως κάθε ασφάλεια. Ένας σχολαστικός φρουρός μπορεί να ψάξει κάθε άτομο που περνάει τα σύνορα και αναπόφευκτα θα υπάρξουν περιπτώσεις όπου το μήνυμα αποκαλύπτεται. Έτσι, λοιπόν, παράλληλα με την ανάπτυξη της στεγανογραφίας εξελίχθηκε η **κρυπτογραφία**[2] από το ελληνικό << κρυπτός>> (<<κρυμμένος>>). Σκοπός της κρυπτογραφίας είναι να αποκρύψει όχι την ύπαρξη ενός μηνύματος, αλλά τη σημασία του, μια διαδικασία γνωστή ως κρυπτογράφηση. Για να καταστεί ένα μήνυμα μη κατανοητό, μετασχηματίζεται σύμφωνα με ένα ειδικό πρωτόκολλο, που έχει συμφωνηθεί από πριν μεταξύ του

[2] http://el.wikipedia.org/wiki/Κρυπτογραφία

αποστολέα και του παραλήπτη. Έτσι ο παραλήπτης μπορεί να αναστρέψει το πρωτόκολλο μετασχηματισμού και να κάνει το μήνυμα κατανοητό. Το πλεονέκτημα της κρυπτογραφίας είναι ότι, ακόμη και αν ο εχθρός υποκλέψει το κρυπτογραφημένο μήνυμα, δεν μπορεί να το διαβάσει. Αν δεν γνωρίζει το πρωτόκολλο μετασχηματισμού, θα του είναι δύσκολο αν όχι αδύνατο, να ανασυνθέσει το αρχικό μήνυμα από το κρυπτογραφημένο κείμενο. Παρότι η στεγανογραφία και η κρυπτογραφία είναι ανεξάρτητες η μία από την άλλη, είναι δυνατό να συνδυαστούν, ώστε να μεγιστοποιηθεί η ασφάλεια ενός μηνύματος. Από τους δυο κλάδους της μυστικής επικοινωνίας, η κρυπτογραφία είναι ο πιο ισχυρός, εξαιτίας της ικανότητας της να εμποδίζει το να πέφτει η πληροφορία σε εχθρικά χέρια.

Κεφάλαιο 3
Στεγανογραφία

3.1 Ορισμός – Ιδιότητες

Όπως καταλαβαίνουμε και από το όνομά της, η στεγανογραφία είναι η τέχνη, που στις μέρες μας έχει εξελιχθεί και σε τεχνική, της επικοινωνίας κατά τρόπο τέτοιο που να κρύβεται η ίδια η ύπαρξη της επικοινωνίας. Σε αντίθεση με τη κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει τη πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Στον παρακάτω πίνακα, που έχει συνταχθεί από τον David Kahn[3] βλέπουμε τις διαφορές της στεγανογραφίας από τη κρυπτογραφία σε σχέση πάντα με τις μεθόδους και τους τύπους που η καθεμία χρησιμοποιεί. Εδώ με τον όρο "ασφάλεια" περιγράφουμε τις μεθόδους προστασίας των πληροφοριών ενώ με τον όρο "ανάκτηση" τις μεθόδους ανάκτησής τους.

[3] http://www.springerlink.com/content/f71x7622t712w2m2/

Ασφάλεια Σήματος	**Ασφάλεια Ανάκτησης**
Ασφάλεια επικοινωνιών	**Ανάκτηση Επικοινωνιών**
• Στεγανογραφία (αόρατα μελάνια, ανοικτοί κώδικες, μηνύματα σε "τρύπια τακούνια") και Ασφάλεια Εκπομπής (συστήματα εκπομπής ευρέως φάσματος)	• Παρεμβολή και Ανίχνευση κατεύθυνσης
• Κρυπτογραφία	• Κρυπτανάλυση
• Ασφάλεια κίνησης (σιγή ασυρμάτου, "χαζά" μηνύματα)	• Ανάλυση κίνησης (ανίχνευση κατεύθυνσης, μελέτη ροής μηνυμάτων και αναγνώριση αποτυπωμάτων ασυρματικών επικοινωνιών)
Ηλεκτρονική Ασφάλεια	**Ηλεκτρονική Ανάκτηση**
• Ασφάλεια Εκπομπής (μετατόπιση συχνοτήτων radar, ευρύ φάσμα)	• Ηλεκτρονική Αναγέννηση (υποκλοπή εκπομπών radar)
• Αντί - Αντίμετρα (παρεμβολές radar)	• Αντίμετρα (παρεμβολές σε radar και λανθασμένη ηχώ τους)

Πίνακας 1: Πίνακας Ασφάλειας David kahn

Η Στεγανογραφία δεν είναι ακριβώς Κρυπτογραφία αλλά είναι οπωσδήποτε ένα μέσο προστασίας της πληροφορίας στον τομέα της ασφάλειας. Αντίθετα με την Κρυπτογραφία όπου σκοπός μας είναι να αλλάξουμε την πληροφορία που θέλουμε να ασφαλίσουμε από οποιουδήποτε είδους επίθεση, έτσι ώστε ο επιτιθέμενος να μην μπορεί να βγάλει νόημα από τα στοιχεία που έχει, ενώ στην Στεγανογραφία σκοπός μας είναι να κρύψουμε την ίδια την ύπαρξη της πληροφορίας.
Θα μπορούσαμε να πούμε ότι η Στεγανογραφία είναι ευρύτερη έννοια της Κρυπτογραφίας (στην περίπτωση που κρυπτογραφούμε αλλά και κρύβουμε).

Η Στεγανογραφία προέρχεται από τις λέξεις

- **Στεγανό** = προστατευμένο - καλυμμένο
- **Γραφή** = γραφή, κείμενο ή σχέδιο, που σημαίνει η γραφή "που καλύπτεται" ή αλλιώς " προστατευμένη" γραφή.

Στεγανογραφία είναι η επιστήμη που σκοπό έχει να κρύψει την πληροφορία έτσι ώστε τα μηνύματα να μπορούν να περάσουν χωρίς να υπάρχει η παραμικρή υποψία ότι υπάρχουν.

Εάν κάποιος ήθελε να εξετάσει ένα αρχείο με κρυμμένες πληροφορίες θα μπορούσε να τις βρει. Στη χειρότερη περίπτωση θα μπορούσε να καταλάβει ότι αυτές υπάρχουν έστω και αν δεν τις έβλεπε. Εάν οι κρυμμένες πληροφορίες είναι κρυπτογραφημένες τότε σίγουρα θα φτάσει μέχρι αυτό το σημείο και θα σταματήσει. Ωστόσο εάν δεν είναι κρυπτογραφημένες τότε θα είναι σε θέση να εξετάσει όλο το "κρυμμένο" μήνυμα. Για το λόγο αυτό δεν θα πρέπει να θεωρούμε τη στεγανογραφία σαν αντικαταστάτη της κρυπτογραφίας αλλά σαν συμπλήρωμά της. Η στεγανογραφία γίνεται όλο και πιο σημαντική στο Κυβερνοχώρο εξαιτίας του ότι κάποιες κυβερνήσεις απαγορεύουν τη χρήση κρυπτογράφησης από ιδιώτες (όπως παλαιότερα στη Γαλλία και στη Ρωσία αλλά και στην Αμερική). Κάνοντας χρήση της στεγανογραφίας μπορούμε να συνεχίσουμε να στέλνουμε κρυμμένα μηνύματα χωρίς να τα βλέπει κανείς.

Η στεγανογραφία βασίζει την ασφάλειά της στο γεγονός ότι κάποιος δεν μπορεί να ψάξει για κάτι που δεν γνωρίζει εάν υπάρχει. Επιπλέον με όλες τις μετακινήσεις δεδομένων στο Internet, κανείς δεν έχει την απαιτούμενη υπολογιστική ισχύ για να περάσει από ανίχνευση όλες τις εικόνες και τα δεδομένα που διακινούνται.

Επίσης, είναι πολύ πιο εύκολο για έναν ιδιώτη να αρνηθεί την αποστολή ενός κρυπτογραφημένου και κρυμμένου στεγανογραφικά, μηνύματος από το να το κάνει για ένα απλά κρυπτογραφημένο. Εάν κάποιος κρύψει πληροφορία σε μια εικόνα μπορεί εύκολα να το αρνηθεί λέγοντας ότι "όπως την πήρα την έστειλα-δεν ήξερα τι είχε μέσα, κάποιος άλλος τα έβαλε" και είναι πολύ δύσκολο για την αρχή που ψάχνει να αποδείξει το αντίθετο.

Οι παρούσες μέθοδοι παροχής πρακτικών στεγανογραφικών υπηρεσιών έχουν δύο κύριους άξονες κατευθύνσεων. Ο πρώτος, ο οποίος δεν είναι και τόσο αποδοτικός, απογυμνώνει τα κρυπτογραφημένα μηνύματα από οποιαδήποτε πληροφορία που αναφέρεται στη ταυτότητά τους . Για παράδειγμα το πρόγραμμα Stealth επεξεργάζεται κατά τέτοιο τρόπο τα κρυπτογραφημένα με PGP[4] μηνύματα που φαίνονται σαν σκουπίδια. Το πρόβλημα με αυτή τη μέθοδο είναι ότι η αναγνώριση ενός PGP μηνύματος είναι πολύ εύκολη υπόθεση ακόμα και αν έχουν αφαιρεθεί οι πληροφορίες αναγνώρισής του. Το Stealth μπορεί να παράσχει ασφάλεια κάποιου επιπέδου αλλά δεν μπορεί να αντιμετωπίσει κάποιον αποφασισμένο hacker.

Ο δεύτερος άξονας της στεγανογραφίας είναι η απόκρυψη δεδομένων μέσα σε άλλα αρχεία. Για παράδειγμα μπορούν να χρησιμοποιηθούν τα λιγότερο σημαντικά bits μιας bitmap εικόνας, μέσα στα οποία μπορεί να κρυφτεί η πληροφορία. Η αλλαγή αυτών των bits της εικόνας προκαλεί ανεπαίσθητες αλλαγές στη μορφή της.
Χωρίς απευθείας σύγκριση με την αρχική εικόνα είναι πραγματικά αδύνατο να πει κανείς ότι κάτι άλλαξε.

Άλλος ένας τύπος αρχείων που μπορεί να χρησιμοποιηθεί για το κρύψιμο πληροφορίας μέσα του είναι τα ψηφιακά μουσικά αρχεία. Με την εισαγωγή του μηνύματος στα λιγότερο σημαντικά bits ενός μουσικού αρχείου κρύβεται η πληροφορία και ομοίως με τα αρχεία εικόνας δεν έχουμε αισθητές αλλοιώσεις στο τελικό, μουσικό, αποτέλεσμα.

[4] http://en.wikipedia.org/wiki/Public-key_cryptography

Ένας τελευταίος και λόγω της φύσης του λιγότερο χρησιμοποιούμενος τρόπος, είναι αυτός της απόκρυψης δεδομένων στα μη χρησιμοποιούμενα sectors των μονάδων αποθήκευσης. Όπως βέβαια αντιλαμβανόμαστε αυτή η μέθοδος δεν μπορεί να χρησιμοποιηθεί σε δικτυακά σχήματα και εδώ απλά γίνεται αναφορά της ύπαρξής της σαν μία επιπλέον δυνατότητα.

Πιθανές χρήσεις της στεγανογρφίας	**Μειονεκτήματα**
Χρησιμοποιείται για να συνδυάσει τις επεξηγηματικές πληροφορίες με μια εικόνα (όπως σημειώσεις του γιατρού που συνοδεύει ένα ακτινών - Χ)	Θα μπορούσε κατά λάθος να υποβαθμίσει ή να καταστήσει μια εικόνα παραπλανητική
Ενσωμάτωση των διορθωτικών στοιχείων ήχου ή εικόνας σε περίπτωση που η διάβρωση εμφανίζεται από μια φτωχή σύνδεση ή μια μετάδοση	Θα μπορούσε να εξουδετερώσει και να είναι αντιπαραγωγική με την αρχική εικόνα
Πρόσωπο με πρόσωπο ιδιωτικές επικοινωνίες	Δεν κρύβουν το γεγονός ότι ένα e-mail εστάλη, ακυρώνοντας το σκοπό της μυστικής επικοινωνίας
Ταχυδρόμηση των μυστικών ανακοινώσεων σχετικά με τον Ιστό για να αποφύγει τη μετάδοση	Κάποιος άλλος με ανίχνευση στεγανογραφίας και ένα εργαλείο ‘σπασίματος’ θα μπορούσε να εκθέσει το μήνυμα.
Προστασία πνευματικής ιδιοκτησίας	Μια μορφή αυτού που ήδη υπάρχει, ονομάζεται ψηφιακή υδατογράφηση, αλλά απαιτεί τη χρήση των χωριστών εργαλείων υλικού επειδή το λογισμικό της στις στεγανογραφίας δεν μπορεί να χρησιμοποιήσει ξεχωριστά εργαλεία υλικού (hardware). Το λογισμικό της στεγανογραφίας, επίσης, δεν μπορεί να προστατεύσει το υδατογράφημα.
Διατήρηση της ανωνυμίας	Είναι πιο εύκολο να ανοίξεις δωρεάν/ ελεύθερα ένα Web - based e-mail ή να χρησιμοποιήσεις ‘επικαλυπτόμενο’ e-mail
Απόκρυψη στοιχείων για το δίκτυο σε περίπτωση παραβίασης	Καλύτερα να κατανοούμε και να χρησιμοποιούμε αποτελεσματικά τυποποιημένη κρυπτογράφηση

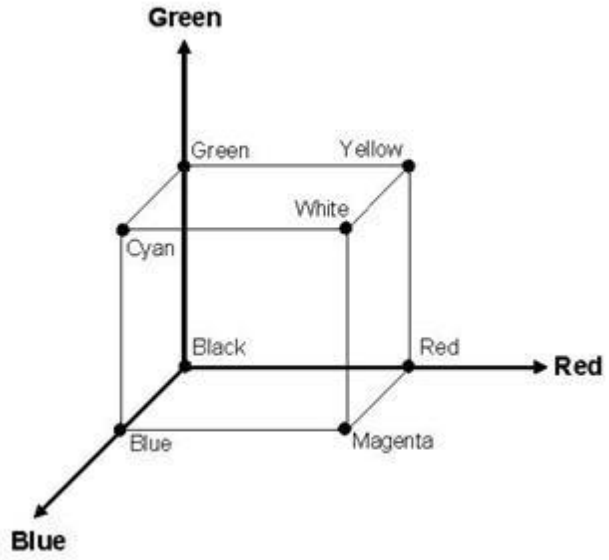
Πίνακας 2 : Πιθανές χρήσεις της στεγανογρφίας & Μειονεκτήματα

3.2 Πως υλοποιείται η στεγανογραφία σε εικόνες.

Μπορούμε να αποθηκεύσουμε αρχεία για κρυφές πληροφορίες, σχεδόν σε όλα τα πολυμέσα. Υπάρχουν αμέτρητες εφαρμογές για να κρύψετε πληροφορίες σε jpeg, gif, bmp, tiff, png, mp3, wav, aif, aiff, au, qtm, ra, ram, wma, ακόμη και σε μουσικά CD!

Ας πάρουμε το παράδειγμα μιας εικόνας JPEG[5] Για να εξηγήσουμε πως είναι δυνατή η απόκρυψη πληροφοριών σε ένα τέτοιο αρχείο, θα πρέπει να περιγράψουμε από τι αποτελείται.

Γενικά ένα αρχείο εικόνας είναι στην πραγματικότητα αριθμοί! Κάθε εικόνα αποτελείται από ένα συγκεκριμένο αριθμό pixels. Αρκεί λοιπόν να περιγράψουμε το χρώμα που θα έχει κάθε pixel σε αυτήν. Οι υπολογιστές αντιλαμβάνονται τα χρώματα με έναν συνδυασμό τριών βασικών χρωμάτων (RGB[6] = Red, Green, Blue). Αν μια εικόνα είναι αποθηκευμένη με 24bit Color Depth, αυτό αυτομάτως σημαίνει ότι κάθε pixel της περιγράφεται με 24 bits. Κάνοντας την διαίρεση προκύπτει ότι κάθε χρώμα μπορεί να περιγραφεί με 256 διαφορετικές τιμές. Έτσι ένα μαύρο εικονοστοιχείο θα έχει (0,0,0) ενώ ένα άσπρο (255,255,255), όπου σε δεκαδικό είναι ο αριθμός
(11111111, 11111111, 11111111).



Εικόνα 1: Τετράγωνο RGB

Το ανθρώπινο μάτι καταλαβαίνει χρώματα που μπορούν να περιγραφούν με μονάχα 16 bits (και εδώ δε μπορείτε να κάνετε καμία αναβάθμιση!). Συγκεκριμένα 5 για το κόκκινο, 6 για το μπλε και 5 για το πράσινο. Αν λοιπόν μια εικόνα είναι αποθηκευμένη σε 24bit, όπως είδαμε παραπάνω, τότε έχουμε στη διάθεσή μας 8 bits

[5] http://en.wikipedia.org/wiki/JPEG
[6] http://en.wikipedia.org/wiki/RGB_color_model

από κάθε εικονοστοιχείο που μπορούμε να μεταβάλουμε, χωρίς οι αλλαγές να γίνουν αντιληπτές!

Η στενογραφία χρησιμοποιεί το τελευταίο σημαντικό ψηφίο (LSB) για να αποθηκεύει ένα κρυφό μήνυμα, μέσα σε ένα άλλο αρχείο. Αλλάζοντας λοιπόν το λιγότερο σημαντικό ψηφίο για κάθε ένα από τα 3 χρώματα ενός pixel, το αποτέλεσμα δεν θα ήταν ορατό στο ανθρώπινο μάτι, αλλά θα ήταν ικανό για να αποθηκεύσει ένα κρυφό μήνυμα.

Αν λοιπόν κρυπτογραφήσουμε ένα μήνυμα, χρησιμοποιώντας μια αρκετά μεγάλη κωδική λέξη, θα είναι δύσκολο να αποκρυπτογραφηθεί από έναν μη εξουσιοδοτημένο παραλήπτη. Θα καταλάβει όμως ότι το μήνυμα που στείλαμε είναι κρυπτογραφημένο! Αν όμως το αποθηκεύσουμε σε ένα αρχείο υπεράνω πάσης υποψίας (πχ. ένα παιδικό σχέδιο), τότε θα είναι πολύ δύσκολο να καταλάβει ότι αυτό που έλαβε κρύβει πληροφορίες! Δύσκολο αλλά όχι αδύνατο…

3.3 Τύποι Αρχείων - Στεγανογραφικά Προγράμματα

JPG: Μέχρι στιγμής το μόνο στεγανογραφικό πρόγραμμα που κρύβει δεδομένα σε κωδικοποίηση JPEG είναι το Jpeg-Jsteg.

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 και Hide4PGP.

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 αρχείο README.TXT θα γινότανε README.TXZ. Τέλος, το πρόγραμμα που χρησιμοποιείται είναι το GZSteg.

TXT: Το "Texto" είναι ένα πρόγραμμα που παίρνει σαν είσοδο κρυπτογραφημένα με PGP (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.

3.4 Διάφορα στεγανογραφικά εργαλεία (περιγραφή)

MP3Stego
MP3Stego θα αποκρύψει πληροφορίες σε αρχεία MP3 συμπίεσης κατά τη διάρκεια της διαδικασίας. Τα δεδομένα είναι πρώτα συμπιεσμένα, μετά κρυπτογραφούνται και στη συνέχεια, κρυφά εκχωρούνται στον MP3.

JPHide και JPSeek
JPHIDE και JPSEEK είναι προγράμματα που μας επιτρέπουν να κρύψουμε ένα αρχείο σε μια εικόνα JPEG. Υπάρχουν πολλές εκδόσεις και παρόμοια προγράμματα διατίθενται μέσω του διαδικτύου. Ο σχεδιαστικός στόχος δεν ήταν απλώς να κρύψει ένα αρχείο, αλλά να το κάνει με τέτοιο τρόπο ώστε είναι αδύνατον να αποδείξει κάποιος ότι το αρχείο περιέχει ένα κρυφό μήνυμα. Φυσικά είναι πολύ καλύτερο όταν χρησιμοποιείται ένα πλήθος αρχείων, με πολλές λεπτομέρειες.

BlindSide Κρυπτογραφικός Tool
BlindSide είναι ένα παράδειγμα της τέχνης της στεγανογραφίας - το πέρασμα των μυστικών μηνυμάτων - σε μορφή τέτοια που ένας ύποπτος δεν θα αντιληφθεί το μήνυμα που πέρασε. Blindside. Το βοηθητικό πρόγραμμα μπορεί να κρύψει ένα αρχείο (ή αρχεία) σε μια εικόνα bitmap των Windows (αρχείο BMP).

GIFShuffle
Το πρόγραμμα **gifshuffle** χρησιμοποιείται για να κρύψουν μηνύματα σε GIF εικόνες.
Αφήνει την εικόνα εμφανώς αμετάβλητη, λειτουργεί με όλες τις εικόνες GIF, συμπεριλαμβανομένων και εκείνων με διαφάνεια και κινούμενα σχέδια, ενώ παράλληλα παρέχει τη συμπίεση και την κρυπτογράφηση της.

WbStego
WbStego είναι ένα εργαλείο που κρύβει κάθε τύπο αρχείου σε bitmap εικόνες, αρχεία κειμένου, αρχεία HTML ή Adobe PDF αρχεία. Το αρχείο στο οποίο μπορείτε να αποκρύψετε τα στοιχεία δεν έχει οπτικά αλλάξει.

StegoVideo
MSU StegoVideo επιτρέπει να αποκρύψει οποιοδήποτε αρχείο βίντεο σε μια σειρά. Μπορείτε να χρησιμοποιήσετε VirtualDub MSU StegoVideo ως φίλτρο ή ως standalone.exe του προγράμματος, ανεξάρτητα από το VirtualDub.

3.5 Στεγανάλυση

Η στεγανάλυση είναι η τεχνική της ανίχνευσης της κρυμμένης πληροφορίας. Υπάρχουν δύο τύποι επιθέσεων κατά των στεγανογραφικά κρυμμένων μηνυμάτων η ανίχνευση και η απόσπαση τους. Κάθε εικόνα μπορεί να τροποποιηθεί με στόχο τη καταστροφή κάποιας κρυμμένης πληροφορίας που πιθανόν να υπάρχει μέσα της .

Η ανίχνευση της ύπαρξης κρυμμένης πληροφορίας εξοικονομεί χρόνο από τη διαδικασία καταστροφής ή ανάκτησής της αφού αυτή θα γίνεται μόνο όταν η πληροφορία βρεθεί.

Η ορολογία των στεγαναλυτικών τεχνικών είναι παρόμοια με αυτή των τεχνικών κρυπτανάλυσης, υπάρχουν ωστόσο και σημαντικές διαφορές .

Ισχύει η παρακάτω, περιγραφική της λειτουργίας του συστήματος, εξίσωση :

μέσο μεταφοράς + **μήνυμα** + **στεγο-κλειδί** = **στεγο-μέσο** όπου :

- **μέσο μεταφοράς** εικόνα, ήχος, κείμενο ή κάποιος άλλος ψηφιακός κώδικας
- **μήνυμα** η πληροφορία που θέλουμε να κρύψουμε που μαζί με το μέσο μεταφοράς αποτελούν το στεγο-φορέα (stego-carrier)
- **στεγο-κλειδί** επιπλέον πληροφορία ασφάλειας

Όπως ακριβώς η κρυπτανάλυση εφαρμόζει διάφορες τεχνικές με σκοπό την αποκρυπτογράφηση της πληροφορίας, έτσι και η στεγανάλυση εφαρμόζοντας δικές της τεχνικές αποσκοπεί στην ανίχνευση της κρυμμένης πληροφορίας .

Ο στεγαναλυτής χρησιμοποιεί τεχνικές επίθεσης ανάλογα με το τι είδους πληροφορία έχει στα χέρια του. Μία μορφή επίθεσης είναι η "στεγο-αποκλειστική" (stego-only) όπου υπάρχει διαθέσιμη για ανάλυση μόνο η στεγανογραφικά κρυμμένη πληροφορία. Εάν τόσο η αρχική όσο και η κρυπτογραφημένη πληροφορία είναι διαθέσιμες τότε μιλάμε για επίθεση "γνωστού μέσου" (known cover). Η στεγανάλυση μπορεί να χρησιμοποιήσει επίθεση "γνωστού μέσου" όταν το κρυμμένο μήνυμα αποκαλυφθεί κάποια στιγμή αργότερα και ο στεγαναλυτής θέλει να το αναλύσει για την περίπτωση μελλοντικών επιθέσεων. Ωστόσο ακόμα και όταν το μήνυμα είναι διαθέσιμο η διαδικασία μπορεί να είναι εξίσου πολύπλοκη με αυτήν της "στεγο-αποκλειστικής" επίθεσης. Μια άλλη μορφή επίθεσης είναι η "επιλεκτική στεγο-επίθεση". Σε αυτήν τόσο το εργαλείο (αλγόριθμος) που χρησιμοποιήθηκε για τη στεγανογράφηση όσο και το στεγο-μέσο είναι γνωστά. Μια επίθεση επιλεγμένου μέσου είναι αυτή κατά την οποία ο στεγαναλυτής δημιουργεί το στεγο-μέσο από κάποιο στεγανογραφικό εργαλείο ή αλγόριθμο γνωστού μηνύματος. Ο στόχος μιας τέτοιας επίθεσης είναι ο καθορισμός συγκεκριμένων ιδιοτήτων του στεγο-μέσου που συγκλίνουν στη χρήση κάποιου στεγανογραφικού εργαλείου ή αλγορίθμου.

3.5.1 Στεγανάλυση εργαλεία

Stegdetect και **Xsteg**
Stegdetect είναι ένα αυτοματοποιημένο εργαλείο για την ανίχνευση στεγανογραφίας σε εικόνες. Περιέχει επίσης ένα βοηθητικό πρόγραμμα για επίθεση σε JSteg και JPHide, ενώ είναι ικανό να ανιχνεύει πολλές διαφορετικές μεθόδους σε εικόνες JPEG. Αυτό το βοηθητικό πρόγραμμα ονομάζεται Stegbreak. Xsteg είναι το GUI (Graphical User Interface) για τα Stegdetect.

Steganography Analyzer Τεχνούργημα Scanner (StegAlyzerAS)
StegAlyzerAS έχει τη δυνατότητα να σαρώσει ολόκληρο το σύστημα αρχείων, ή μεμονωμένων καταλόγων, για την παρουσία στεγανογραφικών αντικειμένων.

Steganography Analyzer Υπογραφή Scanner (StegAlyzerSS)
StegAlyzerSS μας δίνει τη δυνατότητα να σαρώνουμε κάθε αρχείο σχετικά με τα μέσα ενημέρωσης του υπόπτου για την παρουσία Steganography εφαρμογών στους φακέλους. Εάν μία γνωστή υπογραφή ανιχνεύεται, μπορεί να είναι δυνατή η εξαγωγή πληροφοριών με Steganography εφαρμογές που συνδέονται με την υπογραφή του.

Ψηφιακή Αόρατη Μελάνη
Το έργο αυτό παρέχει μια απλή Java που βασίζεται σε steganography εργαλεία που μπορεί να κρύβονται μέσα σε ένα μήνυμα 24-bit χρώμα εικόνας, έτσι ώστε να γνωρίζει πώς ήταν ενσωματωμένο, ή την εκτέλεση της στατιστικής ανάλυσης, για καταστεί ευκολότερο για να βρούμε το απέκρυψαν μήνυμα.

Συμπίεση αρχείων
Δοκιμάζουμε αυτή τη μέθοδο συμπιέζοντας το πρωτότυπο αρχείο bitmap και το ίδιο αρχείο που χρησιμοποιείται ως αρχείο μεταφορέας με βάση το WinZip .
Με τη σύγκριση των ιδιοτήτων των δύο αυτών αρχείων, παρατηρούμε ότι το αρχικό συμπιεσμένο αρχείο είναι καλύτερο από το αρχείο του μεταφορέα.

3.6 Υδατογράφημα

Αν μιλήσουμε για εμπορικές Στεγανογραφικές εφαρμογές που υπάρχουν στο δίκτυο θα πρέπει σίγουρα να αναφέρουμε το ψηφιακό υδατογράφημα που έχει πάρει μια νέα σημασία στην σύγχρονη ψηφιακή εποχή. Ακόμα και οι εικόνες, το βίντεο, η μουσική, το κείμενο, και το λογισμικό, όλα αντιγράφονται εύκολα και διανέμονται παράνομα, αναγκάζοντας τους συντάκτες να χάνουν μεγάλο μερίδιο πωλήσεων και σε πολλές περιπτώσεις τα πνευματικά τους δικαιώματα. Σο υδατογράφημα είναι μια ειδική τεχνική που εγκαθιστά αόρατα ψηφιακά σημάδια στις εικόνες και στα αρχεία ήχου τα οποία φανερώνουν πληροφορίες πνευματικών δικαιωμάτων. Αυτά τα σημάδια ανιχνεύονται από ειδικά προγράμματα που μπορούν να αντλήσουν πολλές χρήσιμες πληροφορίες από αυτό το ειδικό σήμα (υδατογράφημα).

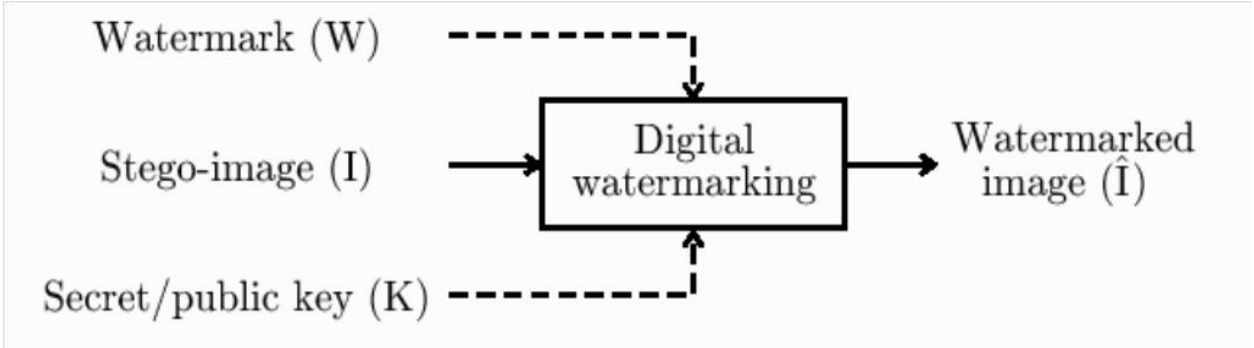
Όταν το αρχείο δημιουργείται, ταυτόχρονα κρατά τα πνευματικά δικαιώματα , το πώς να έρθει σε επαφή με το συντάκτη κλπ.... Όπως ξέρουμε χιλιάδες γνήσια προϊόντα

αναπαράγονται παράνομα και κλέβονται από το δίκτυο κάθε μέρα ώστε να καθίσταται αυτή τη τεχνολογία απαραίτητη και χρήσιμη εάν θέλουμε να προστατέψουμε τα πνευματικά μας δικαιώματα από την πειρατεία.

Υπάρχουν πολλές εταιρίες στο δίκτυο που πωλούν προϊόντα υδατογραφήματος. Μία από τις ηγετικές είναι η Digimarc (http://www.digimarc.com) τις οποίας οι πωλήσεις προγραμμάτων ξεπερνούν το ένα εκατομμύριο. Προσφέρει ελεύθερα το πρόγραμμα PictureMarc το οποίο είναι ένα plug-in στο Photoshop και στο CorelDraw, ή το αυτόνομο ReadMarc. Μόλις εγκατασταθεί, μπορούμε αφού ανοίξουμε ένα αρχείο να διαβάσουμε το κρυμμένο υδατογράφημα που είναι ενσωματωμένο (αν υπάρχει). Για πιο απαιτητικές περιπτώσεις η Digimarc προσφέρει το individual Creator ID (με άδεια ενός έτους) που μας επιτρέπει να ενσωματώνουμε υδατογράφημα στις εικόνες, προτού τις βγάλουμε στον Internet. Έπειτα εταιρικοί χρήστες μπορούν να χρησιμοποιήσουν το MarcSpider το οποίο ψάχνει όλο το δίκτυο για παράνομες εικόνες και αναφέρει οποιαδήποτε παράνομη αναπαραγωγή τους.

Είναι δυνατόν συντάκτες, σχεδιαστές, δημιουργοί να μην πάσχουν πλέον από κλοπές κλπ ; Η ιστορία μας έχει μάθει ότι σε κάθε πρόβλημα υπάρχει μία λύση αλλά και αντιθέτως, σε κάθε λύση υπάρχει ένα πρόβλημα! Όπως πολλά άλλα προγράμματα που σπάζουν τους καθιερωμένους μηχανισμούς ασφάλειας, υπάρχουν προγράμματα που προορίζονται να καταδείξουν την αδυναμία των τρεχόντων αλγόριθμων έτσι ώστε οι επιχειρήσεις να παρακινηθούν και να αναπτύξουν ακόμα πιο γερές υδατογραφικές τεχνολογίες.

Παρά τις προσπάθειες των κατασκευαστών το υδατογράφημα δεν αποδείχθηκε αρκετά γερό. Στο υδατογράφημα μπορεί να επιζήσει πολλών πραγμάτων όπως ρυθμίσεις φωτεινότητας και αντίθεσης, που εφαρμόζουν τα ειδικά φίλτρα ακόμα και εκτύπωση η σάρωση, αλλά δεν μπορεί να επιζήσει από ειδικά προγράμματα όπως το StirMark(http://www.cl.cam.ac.uk/users/fapp2/steganography/image_watermarking/stirmark) και UnZign (http://www.altern.org/watermark) τα οποία είναι δύο παραδείγματα λογισμικού που εμφανίστηκαν στο δίκτυο αμέσως μετά την ανακάλυψη κάθε τεχνολογίας υδατογραφήματος και μπορούν να αφαιρέσουν πληροφορίες πνευματικών δικαιωμάτων από αρχεία. Προφανώς αυτά τα εργαλεία δεν στοχεύουν ενάντια σε κάποιο αλγόριθμο Στεγανογραφίας , αλλά μάλλον σε συγκριτικές μετρήσεις επιδόσεων που μας βοηθούν να ξεχωρίσουμε ώστε να επιλέξουμε το πιο αξιόπιστο για υδατογράφημα λογισμικό. Σα συμπεράσματα στα οποία οδηγούμαστε είναι: μερικά υδατογραφήματα αφαιρούνται εύκολα ή καταστρέφονται με το χειρισμό των διάφορων χαρακτηριστικών του αρχείου, δυστυχώς σήμερα όλα τα υδατογραφήματα μπορούν να καταστραφούν χωρίς σημαντική απώλεια στην ποιότητα της εικόνας.



Πίνακας 3: Γενικό σχήμα ένθεσης ψηφιακών υδατογραφημάτων

Κεφάλαιο 4
Στεγανογραφία με ψηφιακά πολυμέσα

4.1 Στεγανογραφία και υπολογιστές.

Η Στεγανογραφία στους υπολογιστές είναι βασισμένη σε δύο παραδοχές - αρχές. Η πρώτη είναι ότι τα αρχεία που περιέχουν εικόνες ή ήχο μπορούν να αλλάξουν κατά μία ορισμένη επέκταση χωρίς καμία αλλοίωση της λειτουργικότητάς τους αντίθετα από άλλους τύπους δεδομένων (π.χ. τα προγράμματα) που πρέπει να είναι ακριβή προκειμένου να λειτουργήσουν .

Η άλλη αρχή στηρίζεται στην ανικανότητα του ανθρώπου να διακρίνει τις ελάχιστες αλλαγές στο χρώμα μίας εικόνας ή στην ποιότητα του ήχου, το οποίο είναι ιδιαίτερα εύκολο να χρησιμοποιηθεί και να εφαρμοστεί στα δεδομένα που περιέχουν περιττές πληροφορίες, είτε πρόκειται για ήχο 16-bit , 8-bit ή ακόμα καλύτερα μιας εικόνας 24-bit. Η τροποποίηση που γίνεται στις ψηφιακές εικόνες, αλλάζοντας την τιμή του λιγότερου σημαντικού bit (LSB) του χρώματος του εικονοστοιχείου (Pixel) δεν γίνεται αντιληπτή από το ανθρώπινο μάτι.

Σύγχρονες τεχνικές στεγανογραφίας

Απόκρυψη: κρυπτογράφημα μέσα στο κρυπτογράφημα Αυτή η μέθοδος αντιστέκεται σε οποιαδήποτε στατιστική ανάλυση. Αντίθετα, αυτό δεν μπορεί να ειπωθεί για τις μεθόδους που κρύβουν το κρυπτογράφημα μέσα στην εικόνα ή το αρχείο ήχου. Η στατιστική ανάλυση τέτοιας εικόνας ή αρχείου ήχου μπορεί να ανιχνεύσει τα σχέδια που είναι ασυνήθιστα ή μη αναμενόμενα στις ψηφιακές εικόνες ή τους ήχους. Η στεγανογραφική αυτή μέθοδος χρησιμοποιείται π.χ. από TrueCrypt, το οποίο είναι ανοικτό λογισμικό κρυπτογράφησης για τα Windows και τα Linux.

Οι ασυμπίεστες εικόνες ενώ έχουν περισσότερες περιττές πληροφορίες προσφέρουν μεγαλύτερη χωρητικότητα για την απόκρυψη μυστικού μηνύματος σε σύγκριση με συμπιεσμένες εικόνες, χωρίς να προκαλέσουν σοβαρές αλλαγές αντιληπτές από άλλους. Από τη άλλη όταν πρέπει να υποβάλλουμε μία εικόνα σε συμπίεση, τα πράγματα γίνονται πιο περίπλοκα όταν έχουμε να προσαρμόσουμε και την μέθοδο της ενσωμάτωσης.

Δύο από τα πιο δημοφιλή format είναι:
• Graphic interchange format (gif)[7]
• Bitmap (BMP)[8]
Ωστόσο, λόγω της ύπαρξης εξελιγμένων τεχνικών συμπίεσης, η χρήση τους μειώνεται.

[7] http://en.wikipedia.org/wiki/Graphics_Interchange_Format
[8] http://en.wikipedia.org/wiki/Bitmap

GIF (Graphics Interchange Format) είναι μια εικόνα bitmap μορφής που χρησιμοποιείται ευρέως στο World Wide Web, τόσο για ακίνητες εικόνες (παλέτα χρωμάτων raster εικόνες)όσο και για τα κινούμενα σχέδια.
Το GIF περιορίζεται σε 8-bit παλέτα, ή 256 χρώματα. Το γεγονός αυτό καθιστά το GIF μορφή κατάλληλη για την αποθήκευση των γραφικών με σχετικά λίγα χρώματα, όπως απλή διαγράμματα, σχήματα, τα λογότυπα και κινούμενων εικόνων στυλ. Η μορφή GIF υποστηρίζει η εμψύχωση και εξακολουθεί να χρησιμοποιείται ευρέως για την παροχή εικόνας εφέ. Επίσης, χρησιμοποιεί Lossless συμπίεση η οποία είναι πιο αποτελεσματική όταν μεγάλες περιοχές έχουν ένα μόνο χρώμα, και αναποτελεσματική για λεπτομερείς εικόνες.

Η μορφή αρχείου BMP είναι μία μορφή αρχείου εικόνας που χρησιμοποιείται για αποθήκευση bitmap ψηφιακών εικόνων. Σε ασυμπίεστα αρχεία και πολλές μορφές αρχείων Bitmap, τα εικονοστοιχεία αποθηκεύονται με βάθος χρώματος των 1, 4, 8, 16, 24,ή 32 bit ανά Pixel. Εικόνες των 8Bit και λιγότερα μπορεί να είναι είτε αποχρώσεις του γκρι ή δείκτη χρώμα. Ασυμπίεστα αρχεία είναι πολύ μεγαλύτερα από συμπιεσμένες μορφές αρχείων εικόνας για την ίδια εικόνα.
Το αρχείο BMP περιέχει πληροφορίες βίντεο. Μια εικόνα βίντεο αποτελείται από pixels, τα οποία εκπροσωπούνται από τρεις bytes σε ένα αρχείο BMP. Υπάρχει ένα byte για το μπλε χρώμα, άλλο ένα byte αντιπροσωπεύει το πράσινο και το άλλο για το κόκκινο. Η αξία των byte αντιπροσωπεύει την απόχρωση του χρώματος. Δεδομένου ότι ένα χρώμα εκπροσωπείται από 8 bits, υπάρχουν 2 αποχρώσεις του χρώματος, από το 0000 0000 στο 1111 1111.

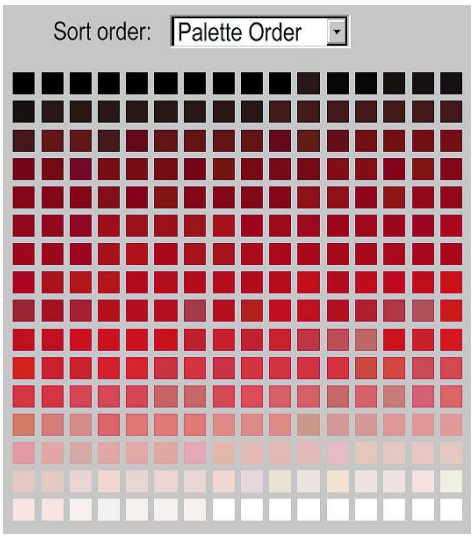
4.2 Εικόνα

Σήμερα, κατά τη μετατροπή μιας εικόνας από αναλογική μορφή σε ψηφιακή ,έχουμε την επιλογή μεταξύ διαφόρων ειδών χρωμάτων :

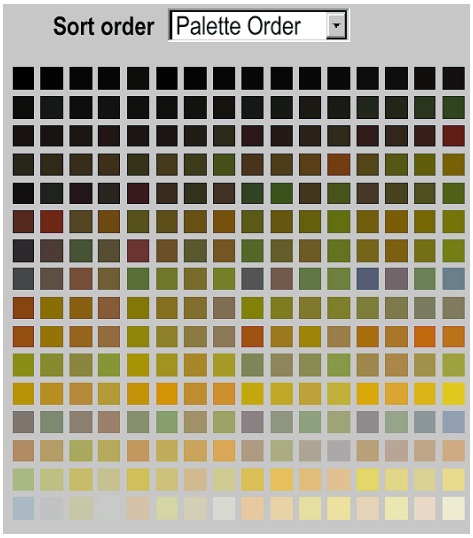
- 24-bit χρωματισμό: κάθε pixel[9] μπορεί να έχει 224 χρώματα, και αυτά αντιπροσωπεύουν διαφορετικές ποσότητες των τριών βασικών χρωμάτων: κόκκινο (R), πράσινο (G), μπλε (B), που δίνονται από 8-bit (256 τιμές) το κάθε ένα.
- 8-bit χρώμα: κάθε pixel μπορεί να έχει 256 (28) χρώματα, που επιλέγονται από μια παλέτα ή αλλιώς από ένα πίνακα χρωμάτων.
- 8-bit κλίμακα του γκρίζου : κάθε pixel μπορεί να έχει 256 (28) σκιές της κλίμακας του γκρίζου.

[9] http://en.wikipedia.org/wiki/Pixel

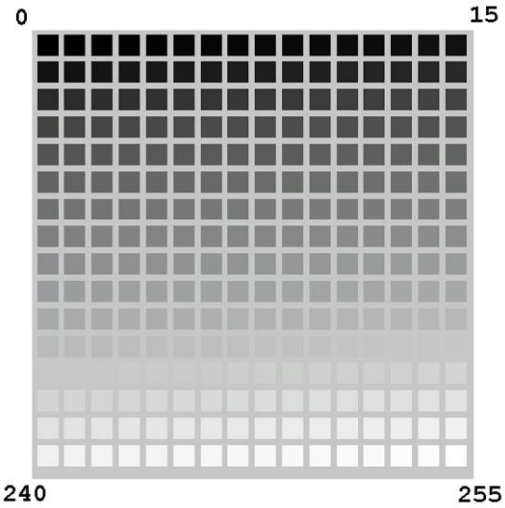
Η μέθοδος εισαγωγής LSB τροποποιεί το LSB κάθε χρώματος σε εικόνες 24-bit ή 8-bit.



Εικόνα 2: 24bit palette



Εικόνα 3: 8bit palette



Εικόνα 4: 8bit grayscale

Παράδειγμα:

Ο χαρακτήρας "A" στον κώδικα ASCII[10] είναι το 65 (δεκαδικό), το οποίο είναι το 1000001 σε δυαδική μορφή.
Χρειάζονται τρία διαδοχικά pixel σε μια εικόνα 24-bit για να αποθηκεύσει ένα "A":
Ας θεωρήσουμε ότι τα pixel πριν από την εισαγωγή είναι:

*Πρώτο pixel**:** 10000000.10100100.10110101,*
*Δεύτερο pixel**:** 10110101.11110011.10110111,*
*Τρίτο pixel**:** 11100111.10110011.00110011*

Οι τιμές κάθε pixel μετά από την εισαγωγή ενός "A" θα είναι:

10000001.10100100.10110100,
10110100.11110010.10110110,
11100110.10110010.00110011

(Οι τιμές σε **bold** είναι αυτές χρειάστηκαν να τροποποιηθούν από τη κωδικοποίηση)
Στο ίδιο παράδειγμα για μια 8-bit εικόνα θα χρειαστούν 8 pixel:

10000000, 10100100, 10110101, 10110101, 11110011,
10110111, 11100111, 10110011

Οι τιμές τους μετά από την εισαγωγή του "A" θα ήταν:

10000001, 10100100, 10110100, 10110100, 11110010,
10110110, 11100110, 10110011

Παρατήρηση :Από τα παραπάνω παραδείγματα συμπεράνουμε ότι η εισαγωγή ενός LSB έχει συνήθως πιθανότητα 50% να αλλάξει για κάθε 8-bit, προσθέτοντας πολύ λίγο θόρυβο στην αρχική εικόνα.

Για εικόνες 24-bit η τροποποίηση μπορεί να επεκταθεί μερικές φορές και στο δεύτερο ή ακόμα και τρίτο LSB χωρίς να είναι ορατή η αλλαγή. Οι 8-bit εικόνες έχουν άντ' αυτού ένα περιορισμένο διάστημα πού μπορούν να επιλεγούν τα χρώματα, έτσι είναι συνήθως δυνατό να αλλαχτεί μόνο το LSB σε αυτά χωρίς η τροποποίηση να είναι ορατά ανιχνεύσιμη.

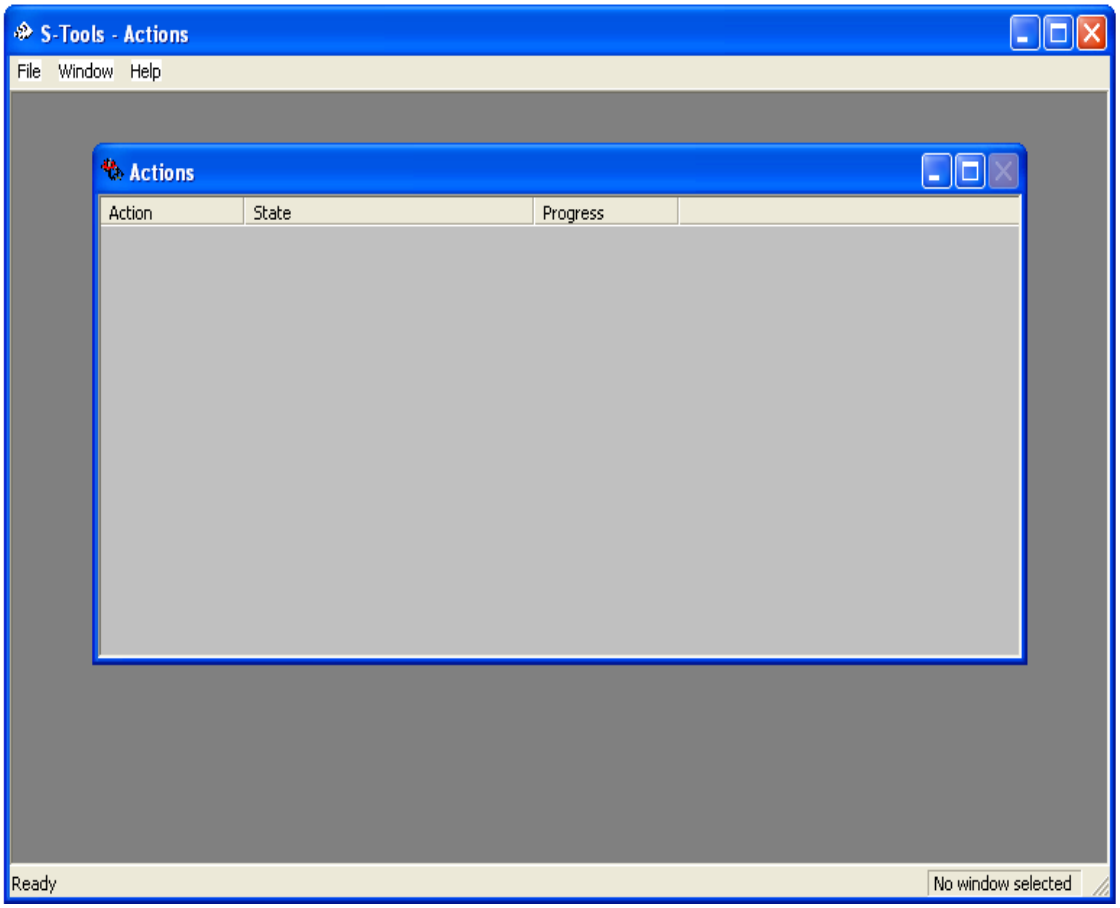
Ας δούμε στην πράξη πως γίνεται από όλα αυτά που έχουμε δει το θεωρητικό επίπεδο…

Θεωρούμε το παρακάτω κείμενο ένα μήνυμα που θέλουμε να κρύψουμε :

Θα πρέπει όλοι μαζί να συμβάλουμε στην ανασυγκρότηση του κράτους. Για το λόγω αυτό θα πρέπει ήσυχα να σταματήσουμε τις εισαγωγές, να ασχοληθούμε με την Ναυτιλία, Αλιεία & Γεωργία για την εγχώρια αγορά, να στραφούμε προς τη Ρωσία και να πουλήσουμε ότι μεταχειρισμένο πήραμε έως σήμερα.

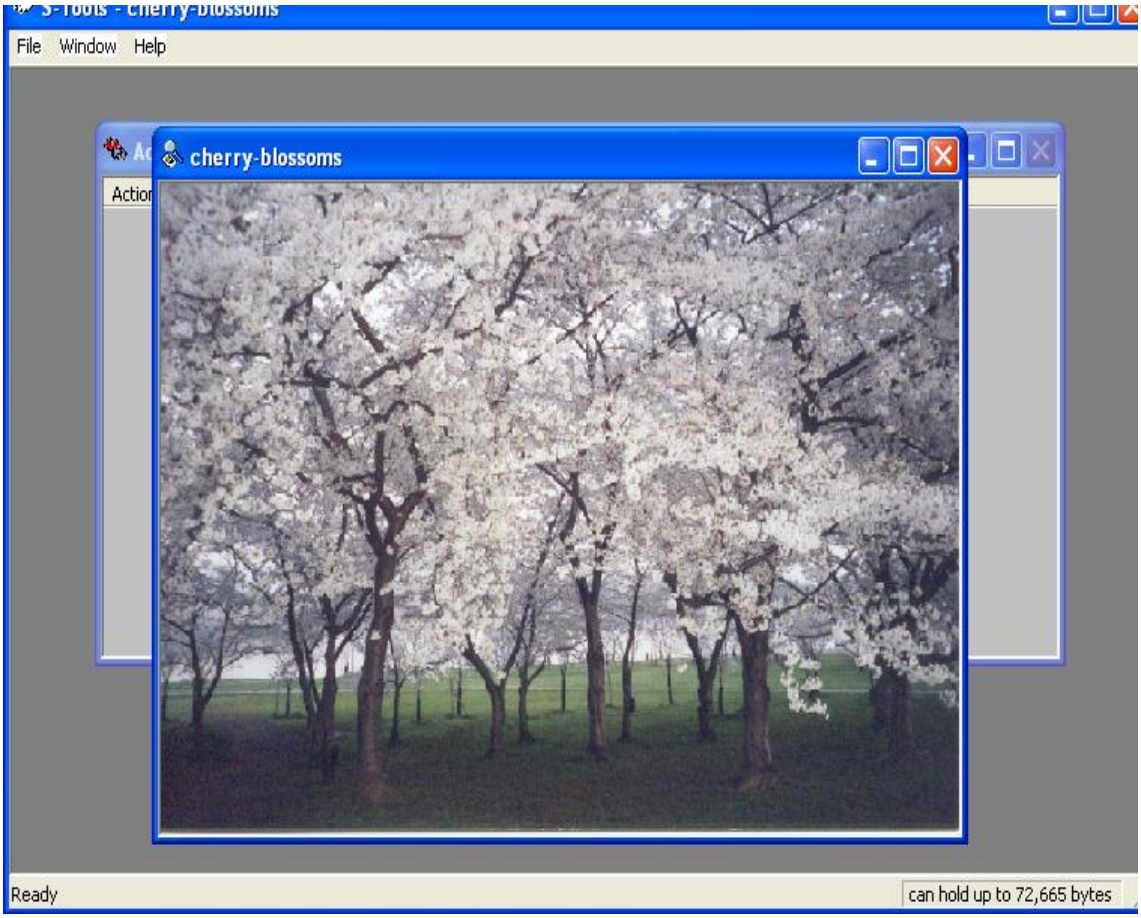
[10] http://el.wikipedia.org/wiki/ASCII

Στο παραπάνω κείμενο θα το κρύψουμε στην εικόνα με τη βοήθεια του προγράμματος S-TOOLS. Το S-Tools είναι ένα λογισμικό κρυπτογράφησης με στεγανογραφικές ικανότητες. Κρύβει αρχεία σε αρχεία τύπου BMP, GIF και WAV αφού πρώτα τα συμπιέσει και τα κρυπτογραφήσει. Τρέχει σε Windows και υποστηρίζει την τεχνική drag and drop . Είναι freeware το οποίο μπορείτε να το κατεβάσετε από το http://www.cryptool.org/index.php/en/download-topmenu-63.html.



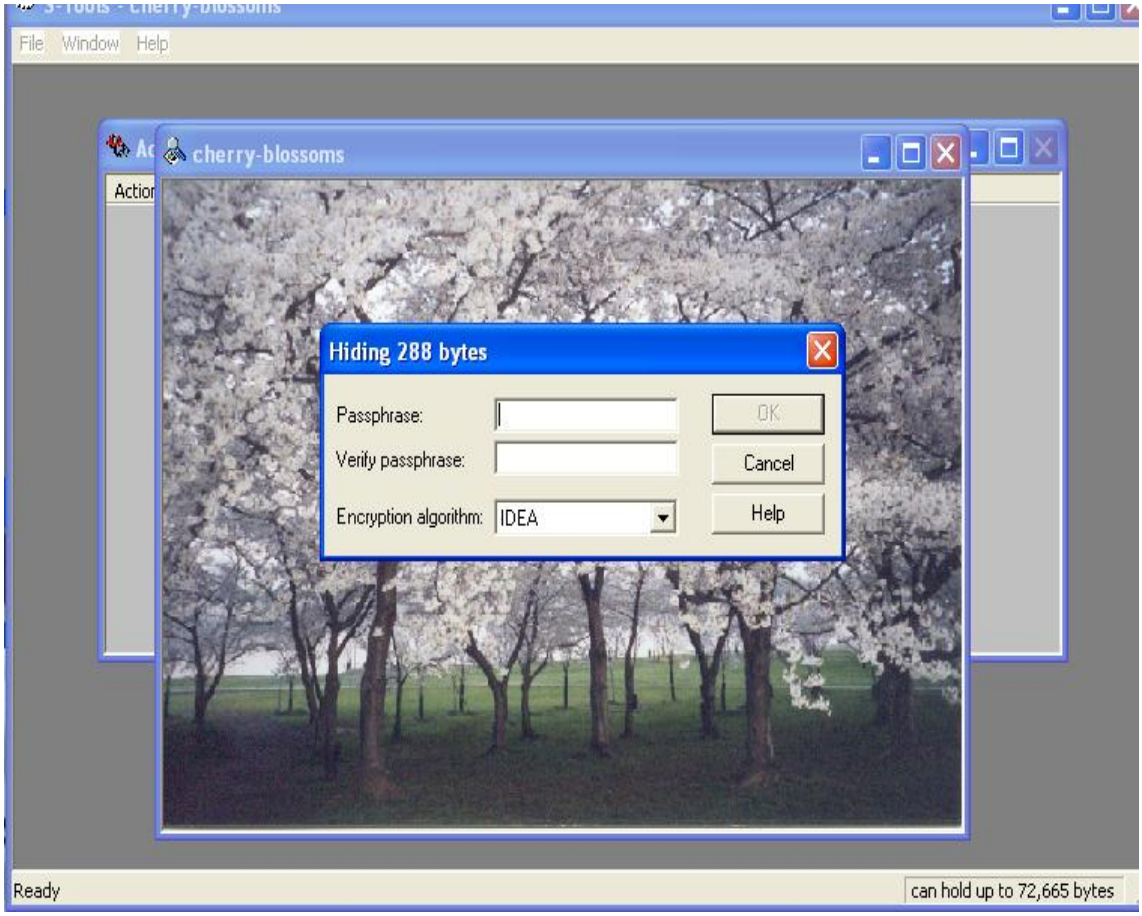
Εικόνα 5: S-Tools (1/7)

Η εικόνα χωρίς το μήνυμα, μόλις έχει φορτωθεί και χωρίς αλλοίωση είναι η παρακάτω. Κάνουμε drag μια οποιοδήποτε εικόνα τύπου (bmp ή GIF)



Εικόνα 6: S-Tools (2/7)

Έπειτα κάνουμε drag το αρχείο κειμένου με μορφή .text να το αποκρύψουμε.

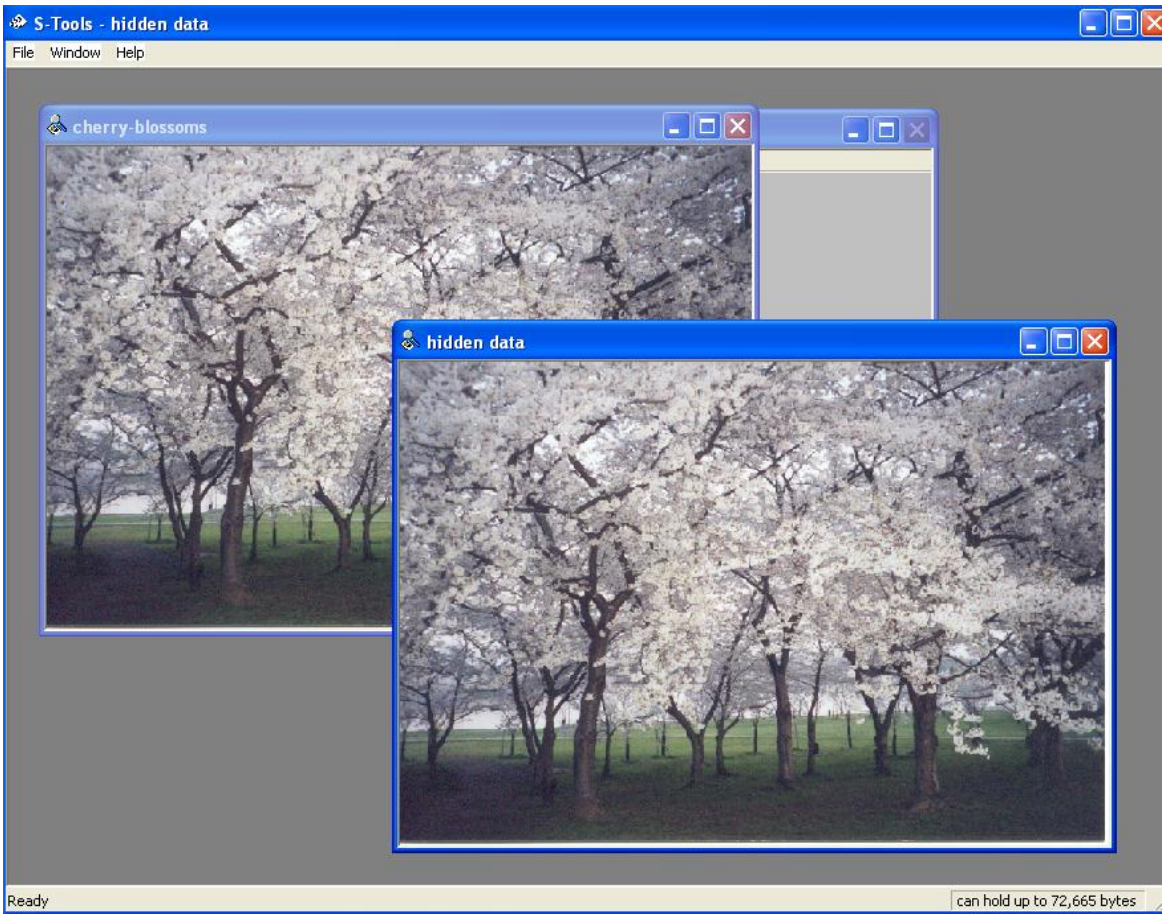


Εικόνα 7: S-Tools (3/7)

Και συμπληρώνουμε το κωδικό και επιλέγουμε τον αλγόριθμο κρυπτογράφησης

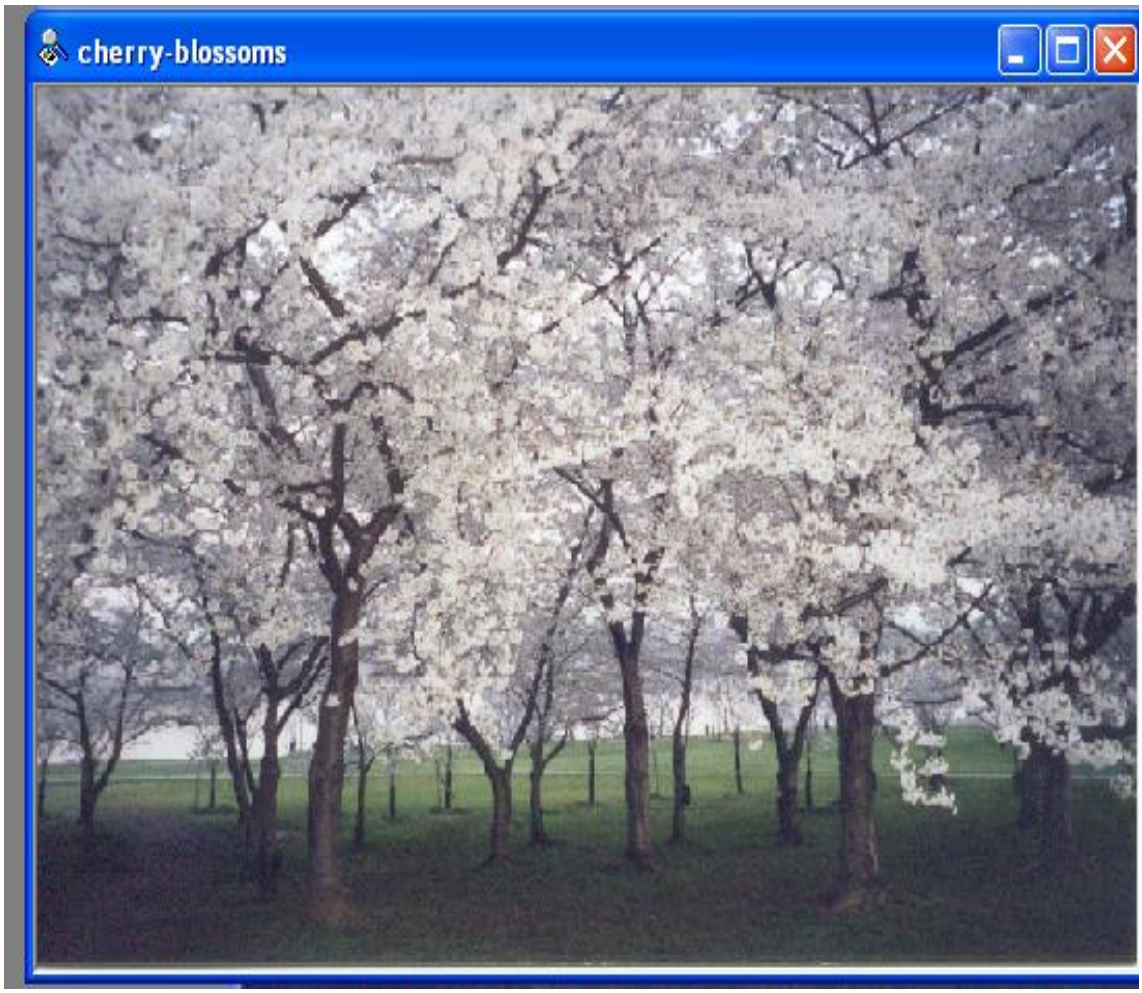
Εικόνα 8: S-Tools (4/7)

Παράγεται μια νέα εικόνα που περιέχει το μυστικό κείμενο.Με δεξί κλικ σώζουμε την εικόνα.

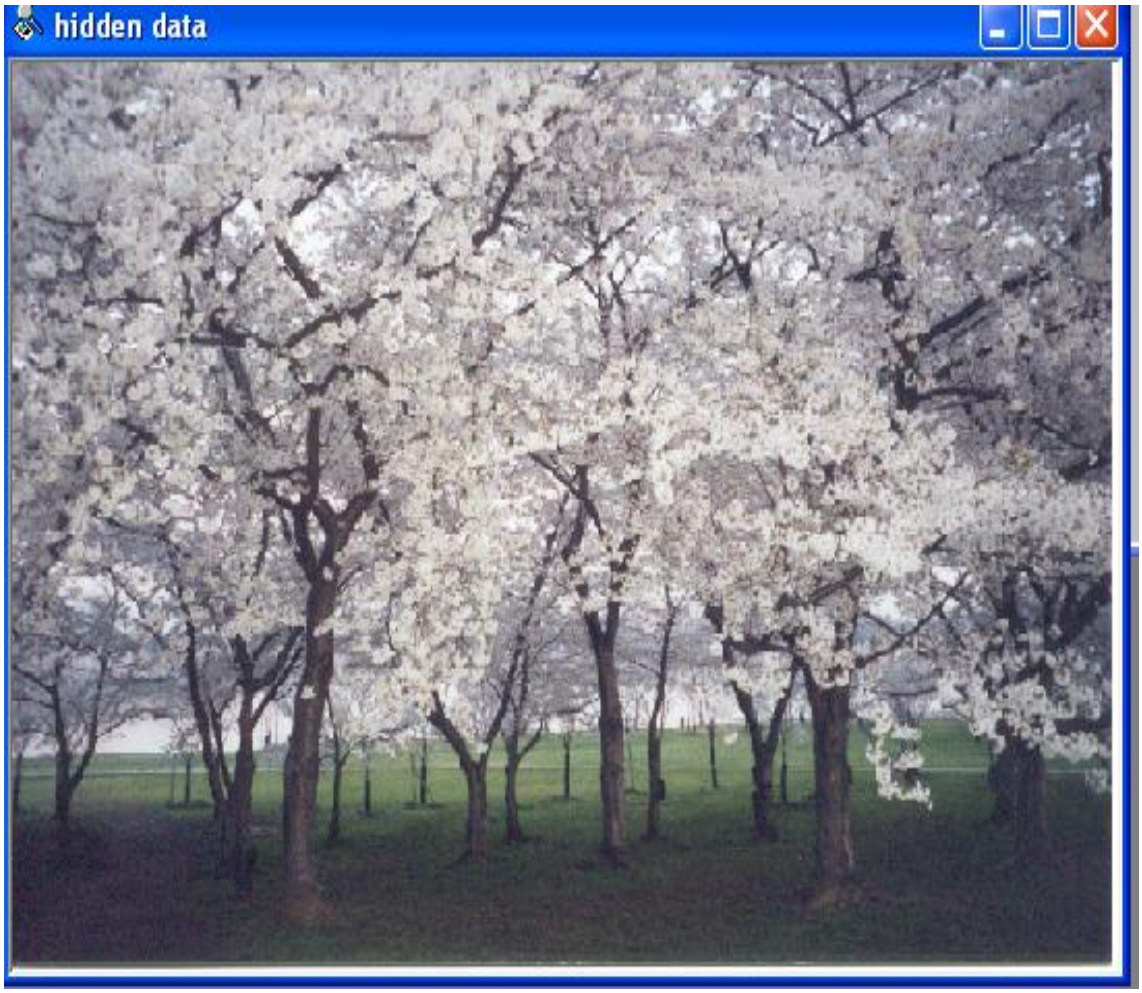


Εικόνα 9: S-Tools (5/7**)**

Παρακάτω δίνουμε τις δύο φωτογραφίες. Στην πρώτη φωτογραφία χωρίς το κείμενο και στην δεύτερη φωτογραφία με το κείμενο.



Εικόνα 10: S-Tools (6/7)



Εικόνα 11: S-Tools (7/7)

Η παραπάνω τεχνική, αν και συνεχώς εξελίσσεται με την πάροδο του χρόνου, έχει ένα σημαντικό μειονέκτημα. Ένας παρατηρητής μπορεί πολύ εύκολα να καταλάβει εαν ένα μήνυμα είναι κρυπτογραφημένο και να αναζητήσει τρόπους για να το διαβάσει… Χρειάζονται λοιπόν τρόποι για να αποκρύψουμε τα κρυπτογραφημένα μηνύματα, έτσι ώστε να μην γίνονται αντιληπτά από τρίτους.

4.3 Ήχος

Στοιχεία που κρύβονται σε ακουστικά σήματα είναι ιδιαίτερα δελεαστικά, επειδή το ανθρώπινο ακουστικό σύστημα δεν λειτουργεί πέρα από ένα δυναμικό εύρος συχνοτήτων. Μπορεί να αντιλαμβάνεται ένα εύρος της δύναμης πάνω από του ενός δισεκατομμύριο προς ένα και ένα εύρος συχνοτήτων μεγαλύτερο από χίλια προς ένα. Η ευαισθησία σε κάθε πρόσθετο τυχαίο θόρυβο είναι επίσης έντονη. Οι διαταραχές σε ένα αρχείο ήχου μπορεί να εντοπίζονται τόσο χαμηλά όπως ένα bit προς δέκα εκατομμύρια (80 DB κάτω από το επίπεδο περιβάλλοντος).

Εντούτοις, υπάρχουν διαθέσιμες μερικές "ευαισθησίες" της ακουστικής αντίληψης . Το ανθρώπινο ακουστικό σύστημα ενώ έχει μεγάλο δυναμικό εύρος συχνοτήτων , έχει επίσης έναν αρκετά μικρό διαφορικό εύρος. Κατά συνέπεια, οι δυνατοί ήχοι τείνουν να καλύψουν πιο ασθενές ήχους . Επιπλέον το ανθρώπινο ακουστικό σύστημα δεν είναι ικανό να αντιληφθεί την απόλυτη φάση αλλά μόνο τη σχετική φάση. Τέλος, υπάρχουν μερικές περιβαλλοντικές διαστρεβλώσεις τέτοιες ώστε να αγνοούνται από τον ακροατή στις περισσότερες περιπτώσεις.

Εκμεταλλευόμαστε πολλά από αυτά τα γνωρίσματα στη παρακάτω μέθοδο καθώς έχουμε λάβει υπόψη προσεκτικά τις ευαισθησίες του ανθρώπινου ακουστικού συστήματος.

Μία ακουστική ακολουθία από αναλογική μορφή για να την επεξεργαστούμε σε ψηφιακή μορφή θα πρέπει πρώτα να ορίσουμε την συχνότητα δειγματοληψίας από την οποία όσο πιο πολλά δείγματα έχουμε τόσο μεγαλύτερο το μέγεθος του αρχείου που θα δημιουργήσουμε αλλά και καλύτερη η ποιότητα του ήχου. Τα βήματα που ακολουθούμε για να κρύψουμε δεδομένα σε ένα ηχητικό αρχείο δεν διαφέρουν και πολύ από αυτά που κάναμε για την εικόνα. Δηλαδή πάλι σκοπός μας είναι να αλλάξουμε το τελευταίο σημαντικό ψηφίο (LSB) του αρχείου ήχου.

Παράδειγμα :
Έχουμε ένα αρχείο ήχου σε wav μορφή με τα ακόλουθα χαρακτηριστικά :
44100 Hz 16-bit stereo του ενός λεπτού.
Διαστάσεις αρχείου = (16-bit x 44100 Hz x 60sec) x 2 (το stereo είναι δικάναλο)
= 84672000 bit

Έχουμε συνεπώς μέγεθος για να κρύψουμε στο αρχείο (χρησιμοποιώντας τα 2 τελευταία LSB) = 84672000 bit / 16 x 2 = 10584000 bit.
Προσοχή : Ποτέ δεν κρύβουμε μία πληροφορία σε ένα wav ή bmp αρχείο και μετά το συμπιέζουμε η ακόμα και να αλλάξουμε τη μορφή του διότι υπάρχει μεγάλος κίνδυνος να χαθούν τα δεδομένα που είχαμε κρύψει.

• Τα ηχητικά δείγματα είναι από την φύση τους ανακριβείς εκτιμήσεις της σωστής αξίας τιμών σε μια δεδομένη χρονική στιγμή. Τα ηχητικά δείγματα σε μορφή WAV αποθηκεύονται είτε σαν 8-bit είτε σαν 16-bit που περνούν τελικά από το μετατροπέα της κάρτας ήχου. Για τα δείγματα 8-bit σημαίνει ότι οι τιμές μπορούν να κυμανθούν μεταξύ 0 και 255 δείγματα , για τα 16-bit κυμαίνονται μεταξύ 0 και 65535. Στο συγκεκριμένο παράδειγμα αυτό που θα κάνουμε είναι να διαμοιράσουμε τα bit-pattern που αντιστοιχούν

στο αρχείο που θέλουμε να κρύψουμε στα λιγότερα σημαντικά bit του ηχητικού δείγματος.

• παραδείγματος χάριν ας υποθέσουμε ότι ένα ηχητικό δείγμα έχει κάπου τα ακόλουθα οκτώ bytes πληροφορίας:
132 134 137 141 121 101 74 38
Σε δυαδικό αυτά θα είναι :
10000100 10000110 10001001 10001101 01111001 01100101 01001010 00100110
(το LSB κάθε αριθμού είναι με κόκκινο)

• Αν θέλουμε να κρύψουμε το δυαδικό 11010101 (213) εσωτερικά σε αυτή την ακολουθία, αντικαθιστούμε απλά το LSB (λιγότερο σημαντικό bit) κάθε byte του δείγματος με το αντίστοιχο κομμάτι byte που προσπαθούμε να κρύψουμε.
Έτσι η παραπάνω ακολουθία θα αλλάξει ως εξής:
133 133 137 142 121 100 74 39
Σε δυαδικό αυτό θα είναι :
10000101 10000101 10001001 10001110 01111001 01100100 01001010 00100111

• Παρατηρούμε ότι η τιμή του ηχητικού δείγματος έχει αλλάξει το πολύ κατά μια μονάδα για το καθένα . Αυτή ή αλλαγή δεν θα είναι αντιληπτή από το ανθρώπινο αυτί και ταυτόχρονα έχουμε κρύψει πάλι 8-bit πληροφορίας μέσα **στο δείγμα.**

4.4 Βίντεο

Το σήμα βίντεο μπορεί να μεταδοθεί σε διάφορα σχήματα. Μπορεί να κωδικοποιηθεί, να διαφοροποιηθεί, να διαβιβαστεί αποκωδικοποιημένο, μπορεί να demodulated και διαμορφωθεί εκ νέου σε επαφή, ή μπορεί να ψηφιοποιηθεί και τέλος να συμπιεστεί και να μεταδοθεί σε πακέτα.

Αρχεία βίντεο είναι γενικά μια συλλογή από εικόνες και ήχους, έτσι οι περισσότερες από τις τεχνικές που παρουσιάζονται για εικόνες και ήχο μπορούν να εφαρμοστούν και σε αρχεία βίντεο. Το μεγάλο πλεονέκτημα του βίντεο είναι ο μεγάλος όγκος των δεδομένων που μπορεί να κρύβει και το γεγονός ότι είναι κινούμενο ρεύμα εικόνων και ήχων. Επομένως, οποιαδήποτε αλλαγή ακόμα και μικρή, θα μπορούσε να περάσει απαρατήρητη από τον άνθρωπο, λόγω της συνεχούς ροής πληροφοριών. Η πραγματική διαδικασία να κρύβουμε ένα αρχείο μέσα σε άλλο είναι σχετικά απλή. Αλλά η προετοιμασία για την διαδικασία (η συρρίκνωση του βίντεο, η διεύρυνση των γραφικών, εύρεση του στεγανογραφικού προγράμματος) είναι αρκετά χρονοβόρα λόγω του μεγέθους των περιορισμών.

Αρχικά θα αναζητήσουμε ένα αρχείο αρκετά μεγάλο για να χρησιμοποιηθεί σαν μεταφορέας αρχείο, ενώ παράλληλα παρέχεται η δυνατότητα προσάρτησης ενός κωδικού πρόσβασης στο κρυφό αρχείο. Οι πληροφορίες προστατεύονται με το κωδικό αυτό, μια και είναι μοναδικός.

Το στέγο-βίντεο επιτρέπει να κρύβεται κάτι σε οποιοδήποτε αρχείο βίντεο. Όταν το πρόγραμμα δημιουργήθηκε ο αλγόριθμος που επιλέχτηκε προέβλεπε μικρή απώλεια δεδομένων μετά το βίντεο. Η διαβίβαση των δεδομένων κάθε φορά υπόκεινται σε κάποιο ποσοστό διαφθοράς λόγω σφαλμάτων, αλλά η μετάδοση βίντεο λόγω της φύσης του πραγματικού χρόνου ασχολείται με αυτά τα λάθη χωρίς την μετάδοση των κατεστραμμένων δεδομένων. Το MPEG-2[11] χρησιμοποιεί δεδομένα που κρύβονται για τη μετάδοση πληροφοριών και διορθώνει λάθη από πολλές τεχνικές απόκρυψης του αποκωδικοποιητή.

Έτσι σε 30 καρέ/δευτερόλεπτο βίντεο μπορούμε να αποθηκεύσουμε 30 φορές τις πληροφορίες μίας ενιαίας εικόνας. Επιπλέον, κάποιοι μπορεί να διαλέξουν πλαίσια για την αποθήκευση με τέτοιο τρόπο ώστε ακόμα και αν κάποιος μπορούσε να εντοπίσει την ύπαρξη τροποποίησης, δεν θα κατάφερνε να εξάγει την πληροφορία.

Κεφάλαιο 5
Γενικά συμπεράσματα

5.1 Στεγανογραφία – Κρυπτογραφία

Η στεγανογραφία συχνά συγχέεται με την κρυπτογραφία, διότι και οι δύο είναι παρόμοιες στον τρόπο που χρησιμοποιούνται για την προστασία των σημαντικών πληροφοριών. Η διαφορά μεταξύ τους είναι ότι η στενογραφία **αποκρύπτει την ύπαρξη του μηνύματος,** ενώ η κρυπτογραφία **μετασχηματίζει το μήνυμα ώστε να το καθιστά ακατανόητο σε οποιονδήποτε τρίτο.**

Εάν ένα άτομο ή άτομα δεν γνωρίζουν ότι υπάρχει κρυφή πληροφορία δεν θα επιχειρήσουν και να αποκρυπτογραφήσουν τις πληροφορίες. Εάν κάποιος ήθελε να εξετάσει ένα αρχείο με κρυμμένες πληροφορίες θα μπορούσε να τις βρει. Στη χειρότερη περίπτωση θα μπορούσε να καταλάβει ότι αυτές υπάρχουν έστω και αν δεν τις έβλεπε. Εάν οι κρυμμένες πληροφορίες είναι κρυπτογραφημένες τότε σίγουρα θα φτάσει μέχρι αυτό το σημείο και θα σταματήσει. Ωστόσο εάν δεν είναι κρυπτογραφημένες τότε θα είναι σε θέση να εξετάσει όλο το "κρυμμένο" μήνυμα. Για το λόγο αυτό δεν θα πρέπει να θεωρούμε τη στεγανογραφία σαν αντικαταστάτη της κρυπτογραφίας αλλά σαν συμπλήρωμά της.

Στο σύστημα της κρυπτογραφίας, οι πληροφορίες κωδικοποιούνται με ένα κλειδί και το πρόσωπο που έχει το κλειδί μπορεί να το αποκρυπτογραφήσει και να διαβάσει τις πληροφορίες, στις οποίες δεν θα έχει κανείς άλλος πρόσβαση.

[11] http://en.wikipedia.org/wiki/MPEG-2

Η στεγανογραφία σε σχέση με την κρυπτογραφία προσθέτει ένα ακόμα επίπεδο ασφαλείας για τα ευαίσθητα αρχεία μας. Αν κάποιος τρίτος αποκτήσει πρόσβαση σε ένα αρχείο προστατευμένο με κωδικό, μπορεί με την χρήση των κατάλληλων εργαλείων (password cracker tools) να ανακαλύψει τον κωδικό προστασίας. (πάντως εάν χρησιμοποιείτε περίπλοκους κωδικούς η διαδικασία του cracking μπορεί να απαιτήσει πολλά χρόνια για να ολοκληρωθεί).

Αυτό που κάνει η στενογραφία ουσιαστικά είναι:

• Ενσωμάτωση μυστικής πληροφορίας σε ένα αρχικό αντικείμενο(cover object)
• Στεγανογραφικό κλειδί (stego key)
• Στεγανογραφημένο αντικείμενο (stego object)
• Στεγανογραφική χωρητικότητα(cover capacity)

Οι λόγοι που οδήγησαν στην ανάπτυξη τέτοιων εφαρμογών είναι:

• Να μπορούν να μεταδίδουν πληροφορίες χωρίς να γίνονται αντιληπτοί από τρίτους.

• Αν γίνουν αντιληπτοί να μην υπάρχει η δυνατότητα να ερμηνευθεί το μήνυμα που μετέδωσαν.

• Αν τελικά υποκλαπεί το μήνυμα, ο παραβάτης να υφίστανται τις συνέπειες του νόμου .

• Αν αλλοιωθούν τα δεδομένα, να υπάρχει η δυνατότητα επαναφοράς στην αρχική τους μορφή.

• Αν διεκδικηθεί η ιδιοκτησία τους, να μπορούν να αποδείξουν την κυριότητα τους.

Η ανθεκτικότητα, η αντοχή και η ευρωστία είναι τρία χαρακτηριστικά που έχουν επιπτώσεις στη στεγανογραφία και τη χρησιμότητα της.

• Η ανθεκτικότητα αναφέρεται στην ικανότητα των ενσωματωμένων στοιχείων να παραμείνουν ανέπαφα, εάν υφίστανται μετασχηματισμός στη στέγο- εικόνα.

• Η ευρωστία είναι ζωτικής σημασίας για προστασία της πνευματικής ιδιοκτησίας, επειδή κάποιοι θα προσπαθήσουν να φιλτράρουν και να καταστρέψουν κάθε πληροφορία ενσωματωμένη σε εικόνες. Το μόνο μειονέκτημα που προσφέρει είναι μία υψηλή επιβάρυνση για μικρή πληροφορία και αν η μέθοδος αποκαλυφθεί δεν παρέχεται καμία προστασία.

• Πέρα από ευρωστία της καταστροφής, η παραποίηση αντοχής αναφέρεται στην δυσκολία για έναν εισβολέα να μεταβάλει ή να σφυρηλατήσει ένα μήνυμα τη στιγμή που θα έχει ενσωματωθεί σε μία στέγο –εικόνα. Όπως ένα πειρατικό αντικαθιστά ένα σήμα πνευματικής ιδιοκτησίας με μία διεκδίκηση της νόμιμης ιδιοκτησίας

Ένα διάσημο πρότυπο για τη στεγανογραφία είναι το πρόβλημα των φυλακισμένων Simmons. Η Alice και ο Bob είναι κλειδωμένοι σε διαφορετικά κελιά αλλά έχουν την άδεια για να επικοινωνούν κάτω από το άγρυπνο μάτι της Eve, που είναι ο φύλακας των φυλακών.

Η Eve ελέγχει την επικοινωνία μεταξύ της Alice και Bob και είναι διατεθειμένη να διακόψει ορισμένες μορφές επικοινωνίας. Στην ιδανική περίπτωση, η Eve θα επιθεωρεί κάθε μήνυμα και θα αποφασίζει αν η επικοινωνία επιτρέπεται ή όχι. Έτσι, κρυπτογραφημένα δεδομένα δεν επιτρέπεται από την Eve να περάσουν γιατί δεν μπορεί να αποκωδικοποιήσει το περιεχόμενο τους.

Η Alice και ο Bob μοιράζονται ένα μυστικό κλειδί *K* το οποίο χρησιμοποιείται για την ενσωμάτωση και για τη λήψη του μηνύματος.

Σε ένα πραγματικό σενάριο, η Eve μπορεί να ανήκει σε μια εταιρεία η οποία προσπαθεί να διατηρήσει κάποιες μυστικές πληροφορίες και η Alice, που ανήκει σε αυτή την εταιρεία, προσπαθεί να μεταδώσει αυτό το μυστικό στο Bob, ο οποίος είναι εκτός.

5.2 Θεωρητικά συμπεράσματα

Η Στεγανογραφία είναι μια αρχαία τέχνη που έχει διαδοθεί και αναπτυχθεί με την εμφάνιση του διαδικτύου και γενικά από τα ψηφιακά μέσα. Δεν είναι πλέον μια μέθοδος που περιορίζεται στη μυστική επικοινωνία μεταξύ δύο κατασκόπων ή κάποια άλλη χρήση της όπως στη διάρκεια του πολέμου. Τα εργαλεία είναι τώρα προσιτά στους χρήστες και σε αρκετές περιπτώσεις δωρεάν μέσω του διαδικτύου, τα οποία πολλές φορές δεν απαιτούν καμία ειδική γνώση για τη χρήση τους.

Αφού το θέμα της πτυχιακής είναι η ασφάλεια, πιστεύω ότι η Στεγανογραφία σε συνδυασμό με την Κρυπτογραφία σαν υβριδική μορφή θα μπορούσε να πετύχει ένα πολύ καλό και υψηλό επίπεδο ασφαλείας και απόρρητου.

Αυτό έχει διάφορα **πλεονεκτήματα** και **μειονεκτήματα**:

Πλεονέκτημα είναι ότι αυξάνει την δυνατότητα προστασίας της μυστικότητάς μας, ή την επικοινωνία μας όταν το απαιτούν οι συνθήκες. Μειονέκτημα είναι η αυξανόμενη δυνατότητα για τους εγκληματίες και τους τρομοκράτες να επικοινωνούν μεταξύ τους χωρίς να ανιχνεύονται από την δικαιοσύνη.

Η απαγόρευση της τεχνολογίας δεν είναι επαρκής για να σταματήσει την εγκληματική χρήση. 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. Στην πραγματικότητα, η Στεγανογραφία είναι μέρος του ίδιου κύκλου με την επιβολή του νόμου και της εγκληματικότητας.
Δεδομένου ότι η ικανότητα της επιβολής του νόμου αυξάνεται, έτσι και η ικανότητα της εγκληματικότητας αυξάνεται. Η μόνη επιλογή είναι η συνεχής πρόοδος και έρευνα για να μην σταματήσει ο κύκλος υπέρ εκείνων που κάνουν κακή χρήση της τεχνολογίας.

Αξίζει να αναφέρουμε και το πρόγραμμα StegoSoftware με το οποίο μπορούμε να κρύψουμε αρχεία οποιουδήποτε είδους σε αρχεία εικόνας gif και bmp καθώς επίσης και σε wav, είναι πραγματικά ένα Στεγανογραφικό και Κρυπτογραφικό προϊόν σε ένα επειδή το αρχείο που κρύβεται κρυπτογραφείται πρώτα χρησιμοποιώντας έναν από τους συμμετρικούς βασικούς αλγορίθμους: DES,[12] τριπλό DES[13], και IDEA[14]. Η χρήση του είναι πολύ απλή, drag and drop το αρχείο στο παράθυρο διαλόγου του προγράμματος, κατόπιν το αρχείο που θέλουμε να κρύψουμε και τέλος επιλέγουμε έναν αλγόριθμο και έναν κωδικό πρόσβασης.

Κεφάλαιο 6
Steganography Tools

- Το πρόγραμμα jphide-and-jpseek εδώ το συγκεκριμένο παράδειγμα είναι για απόκρυψη ενός κειμένου σε εικόνα JPEG .

- Το πρόγραμμα OurSecret, το συγκεκριμένο παράδειγμα αναφέρεται για απόκρυψη σε ένα αρχείο ήχου με κατάληξη .mp3 και σε μια εικόνα με κατάληξη .jpeg και ένα message από το πρόγραμμα μέσα σε ένα αρχείο video με κατάληξη .wmv.

- Το πρόγραμμα Xiao Steganography, θα το χρησιμοποιήσω για να κρύψω σε ένα αρχείο με κατάληξη .pdf μέσα σε ένα αρχείο ήχου με κατάληξη .wav

- Το πρόγραμμα wbStego4, θα το χρησιμοποιήσω επίσης για να κρύψω σε ένα αρχείο με κατάληξη .pdf μέσα σε μια εικόνα .bmp.

- Το πρόγραμμα HIP 2.1 θα το χρησιμοποιήσω για να κρύψω σε ένα αρχείο βίντεο με κατάληξη .avi μέσα σε μια εικόνα .gif.

[12] http://en.wikipedia.org/wiki/Data_Encryption_Standard
[13] http://www.tropsoft.com/strongenc/des3.html
[14] http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

6.1 jphide-and-jpseek

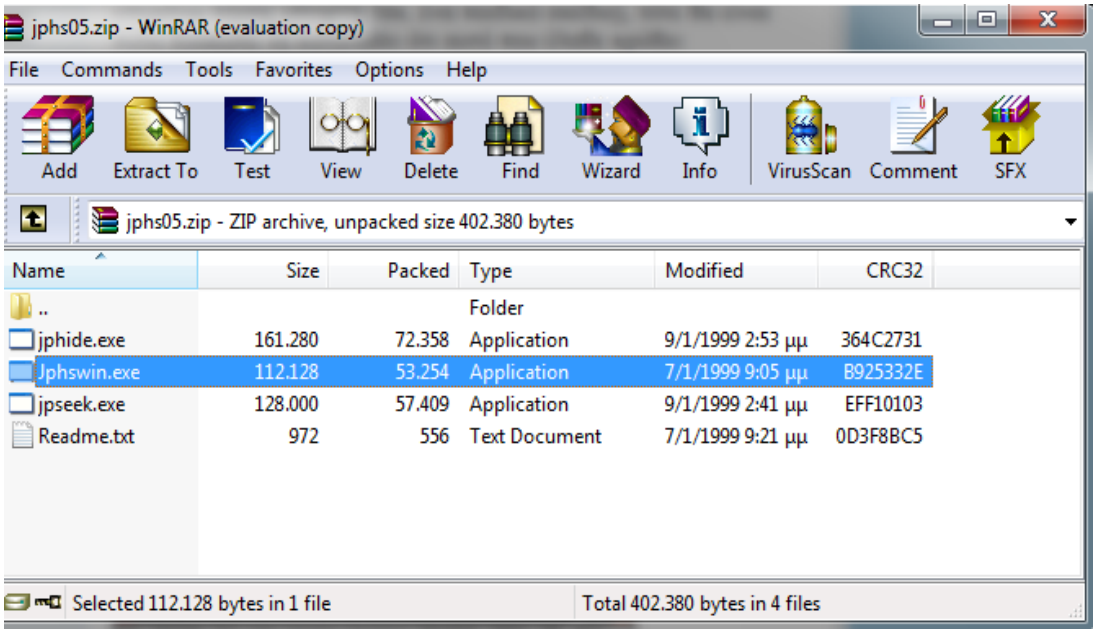
Υπάρχει επίσης και ένα άλλο πρόγραμμα το jphide-and-jpseek που αποτελείται σε εικόνες JPEG. Μπορείτε να κατεβάζετε το πρόγραμμα αυτό http://linux01.gwdg.de/alatham/stego.html (είναι freeware). Όπως αναφέρθηκε στο προηγούμενο παράδειγμα, το πρόγραμμα S-Tool.

Κατεβάστε το πρόγραμμα jphide-and-jpseek και αποσυμπιέστε τα εκτελέσιμα αρχεία σε ένα μέρος στο δίσκο.

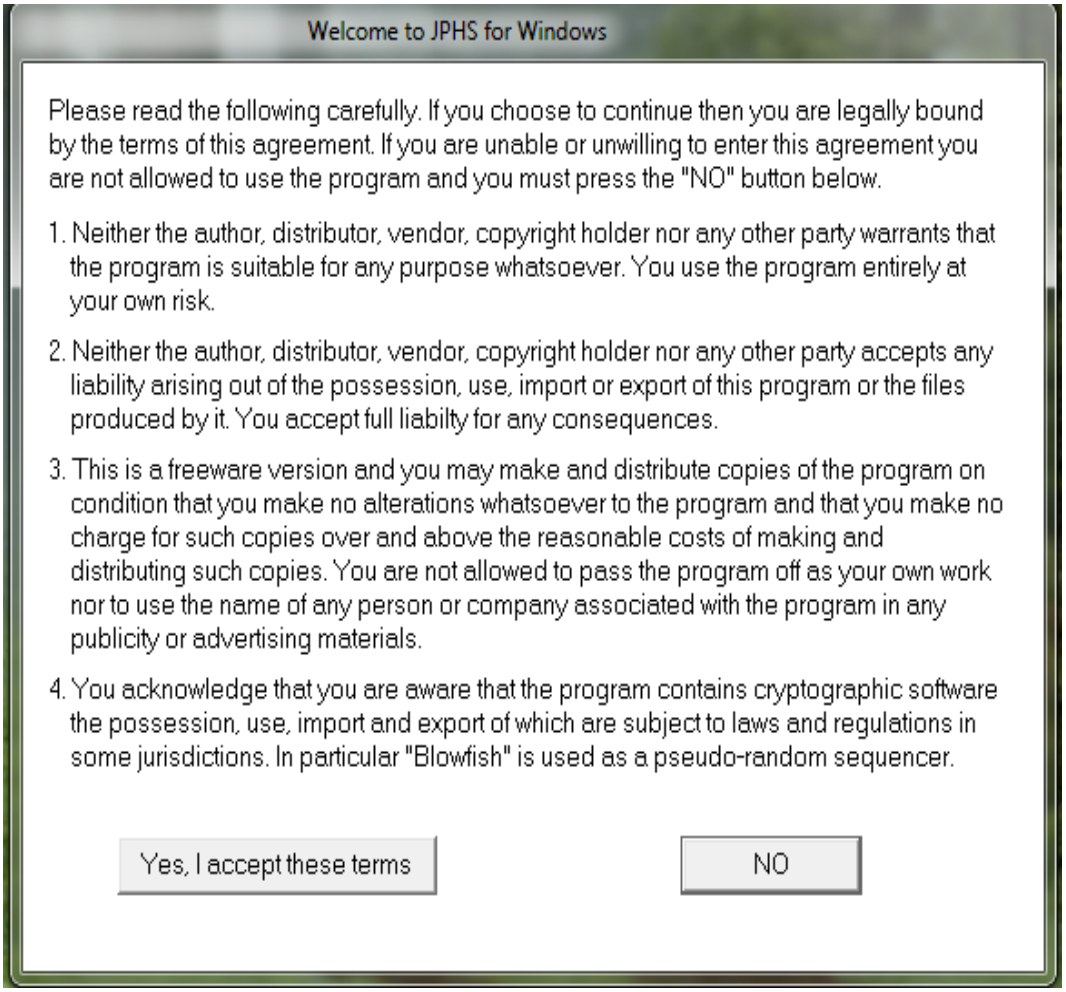
Για απόκρυψη ενός κειμένου σε εικόνα JPEG .

Έπειτα επιλέξετε μια οποιαδήποτε εικόνα με κατάληξη JPEG που θέλετε να χρησιμοποιήσετε.

Εκτελέστε την εφαρμογή jphswin.exe και αποδέχεστε τους όρους χρήσης
(Yes, I accept these terms).

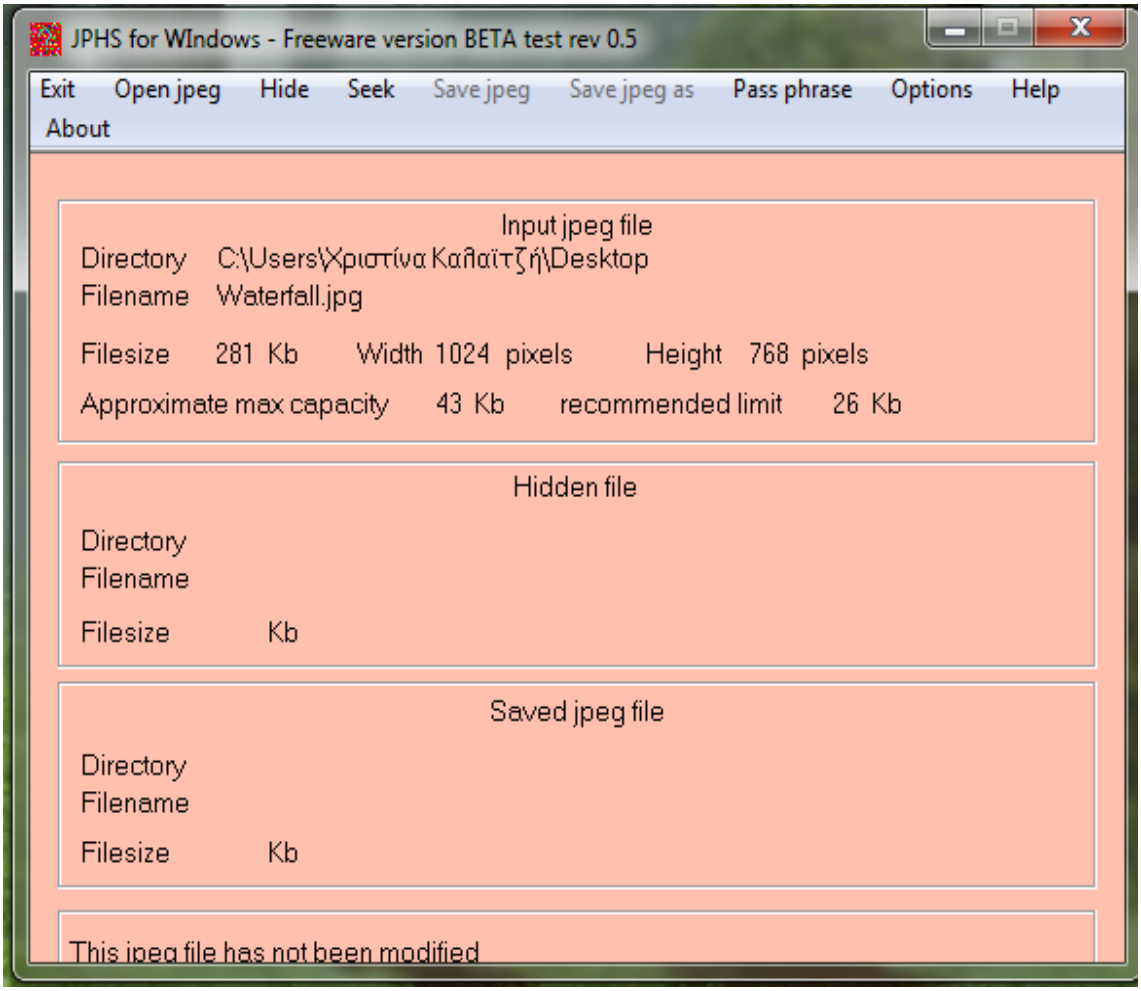


Εικόνα 12: jphide-and-jpseek (1/9)



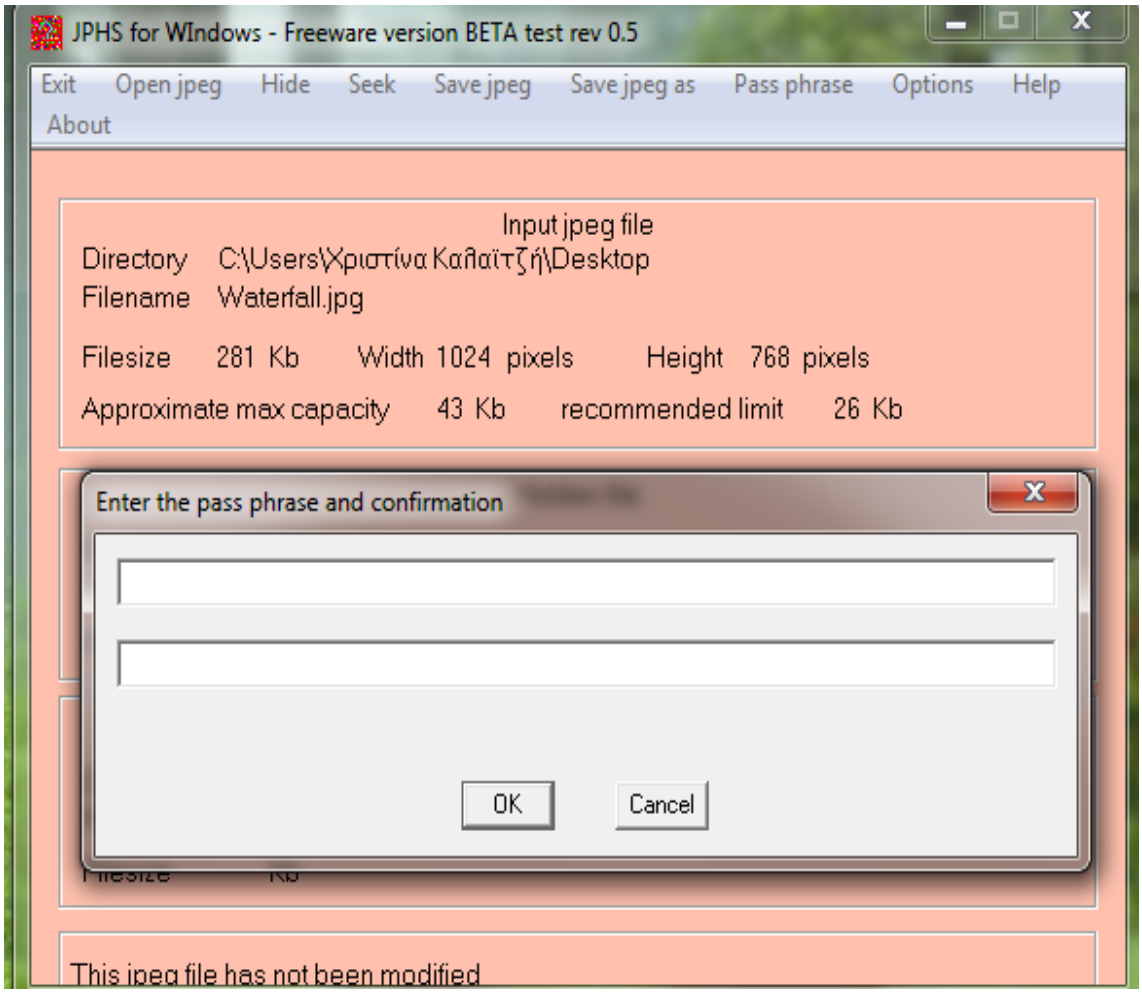
Εικόνα 13: jphide-and-jpseek (2/9)

Επιλέξτε Open JPEG και φορτώστε την εικόνα που θέλετε να επιλέξετε μέσα στο πρόγραμμα.

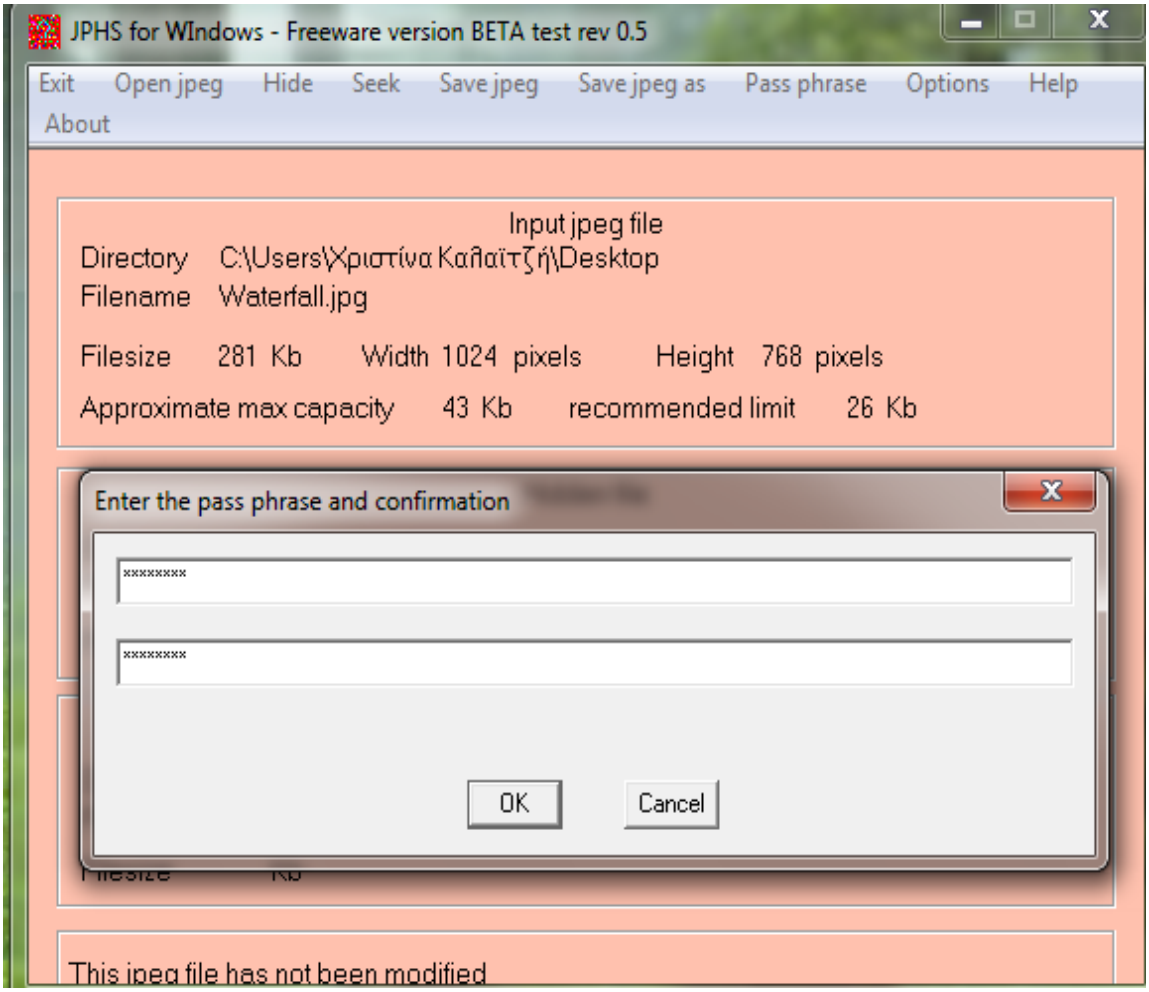


Εικόνα 14: jphide-and-jpseek (3/9)

Έπειτα στην επιλεγμένη εικόνα, κάντε κλικ στο Hide από το μενού της εφαρμογής και εισάγετε τον κωδικό πρόσβασης που επιθυμείτε και στα δυο πεδία του νέου παραθύρου που θα εμφανιστεί. Ύστερα πατήστε οκ.

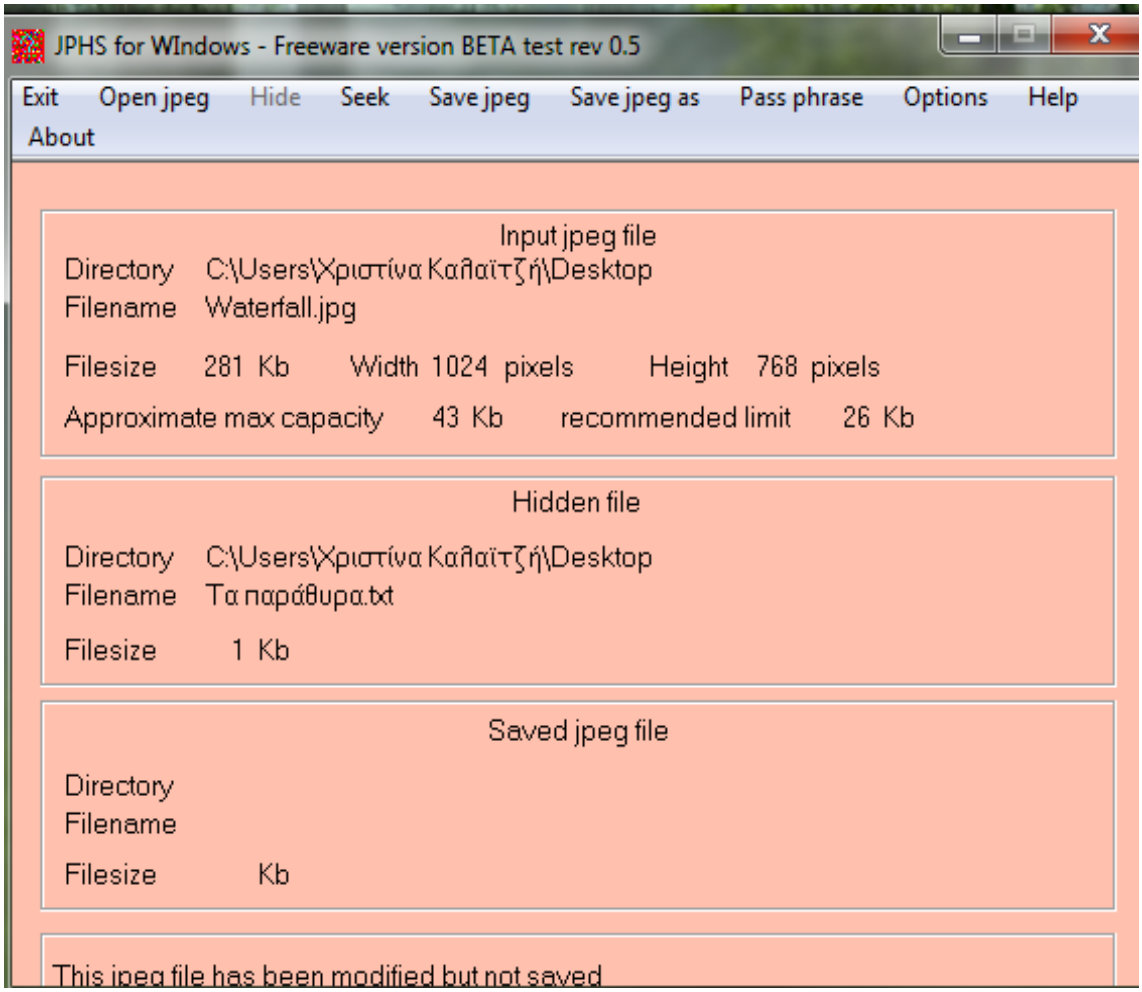


Εικόνα 15: jphide-and-jpseek (4/9)



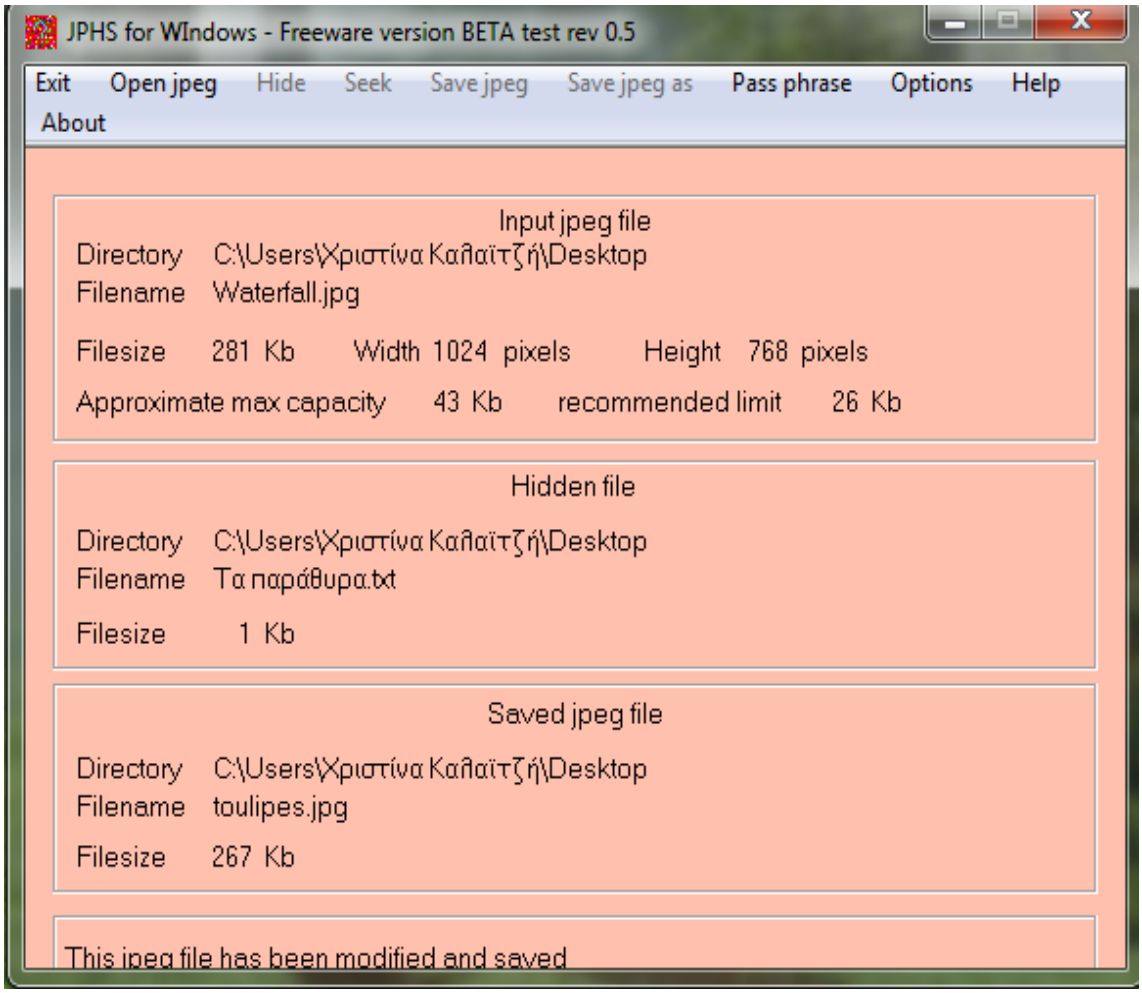
Εικόνα 16: jphide-and-jpseek (5/9)

Στη συνέχεια θα πρέπει να επιλέξετε το αρχείο που θέλετε να αποκρύψετε. Όπως είναι λογικό, το αρχείο δεν μπορεί να είναι μεγαλύτερο από την εικόνα ..



Εικόνα 17: jphide-and-jpseek (6/9)

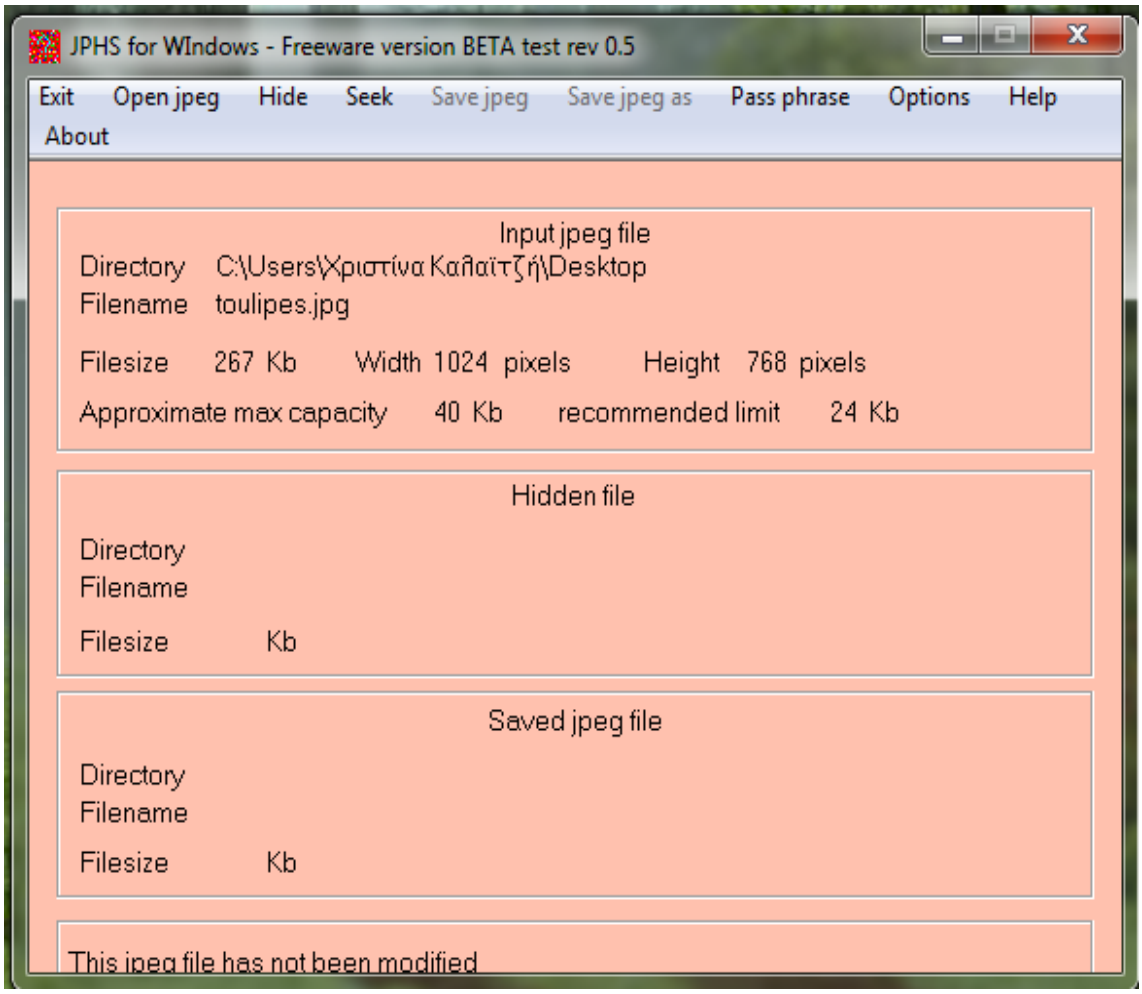
Μετά από αυτό αποθηκεύστε στο Save jpeg για παράδειγμα στην επιφάνεια εργασίας.



Εικόνα 18: jphide-and-jpseek (7/9)

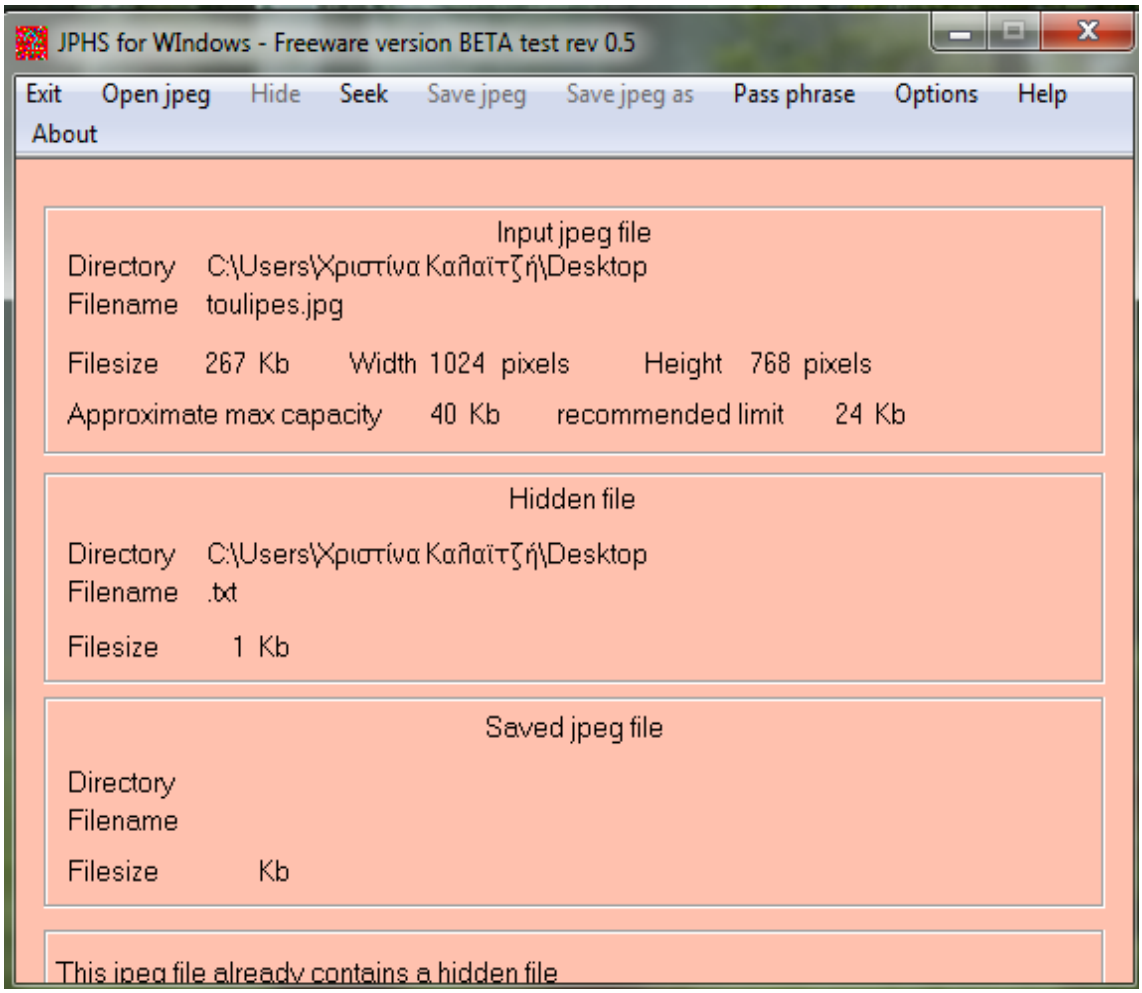
Αν τώρα θέλετε να ανακτήσετε το κρυμμένο κείμενο. Χρησιμοποιήσετε πάλι το πρόγραμμα jphide-and-jpseek με την εφαρμογή jphswin.exe

Επιλέξτε Open JPEG και φορτώστε την κρυπτογραφημένη εικόνα που δημιουργήσατε.



Εικόνα 19: jphide-and-jpseek(8/9)

Επιλέξτε Seek από το μενού της εφαρμογής και εισάγετε τον κωδικό που φτιάξατε και στα δυο πεδία του νέου παραθύρου που θα εμφανιστεί. Έπειτα αποθηκεύστε το αρχείο με κατάληξη .txt. Τέλος ανοίξτε το αρχείο και διαβάστε το μήνυμά του που επιλέξατε.



Εικόνα 20: jphide-and-jpseek (9/9)

6.2 OurSecret

Ακόμα ένα πρόγραμμα στεγανογραφίας είναι το OurSecret το οποίο μπορείτε να το κατεβάσετε από το www.securekit.net (δεν είναι freeware). Αφορά σε αρχεία εικόνες, βίντεο, ήχου κτλ.

Εικόνα 21: OurSecret (1/7)

Το συγκεκριμένο παράδειγμα είναι για απόκρυψη σε ένα αρχείο ήχου με κατάληξη .mp3 και μια εικόνα με κατάληξη .jpeg και ένα message από το πρόγραμμα μέσα σε ένα αρχείο video με κατάληξη .wmv.

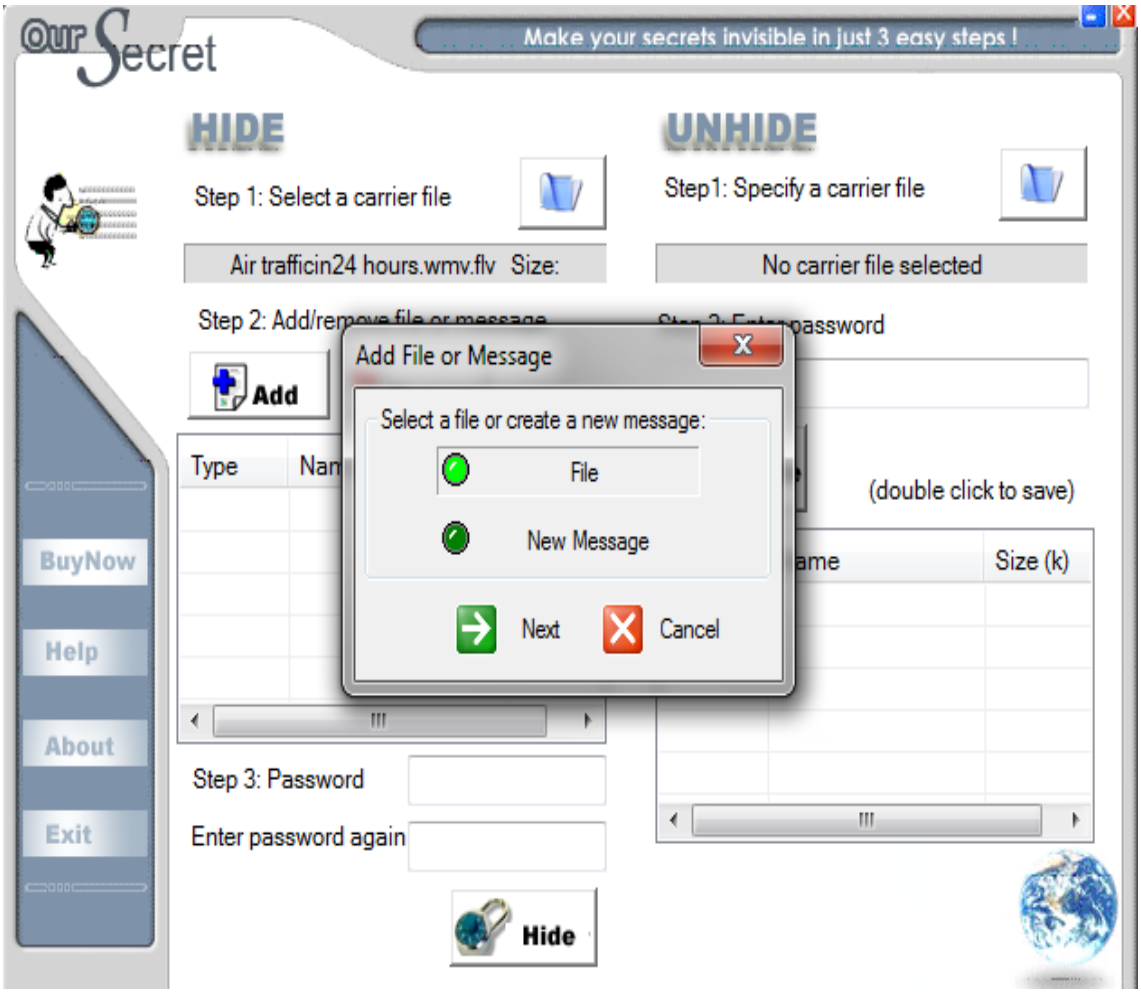
Χρειάζεται μόνο τρία βήματα για να αποκρύψετε τα αρχεία μέσα σε ένα αρχείο.

Πρώτο βήμα: Κάντε κλικ στο εικονίδιο "φάκελο" και επιλέξτε ένα video που επιθυμείτε.

Δεύτερο βήμα: Κάντε κλικ στο εικονίδιο "add" και πατήστε "Next" επιλέξτε ένα αρχείο ήχου που θέλετε να αποκρύψτε στο video.

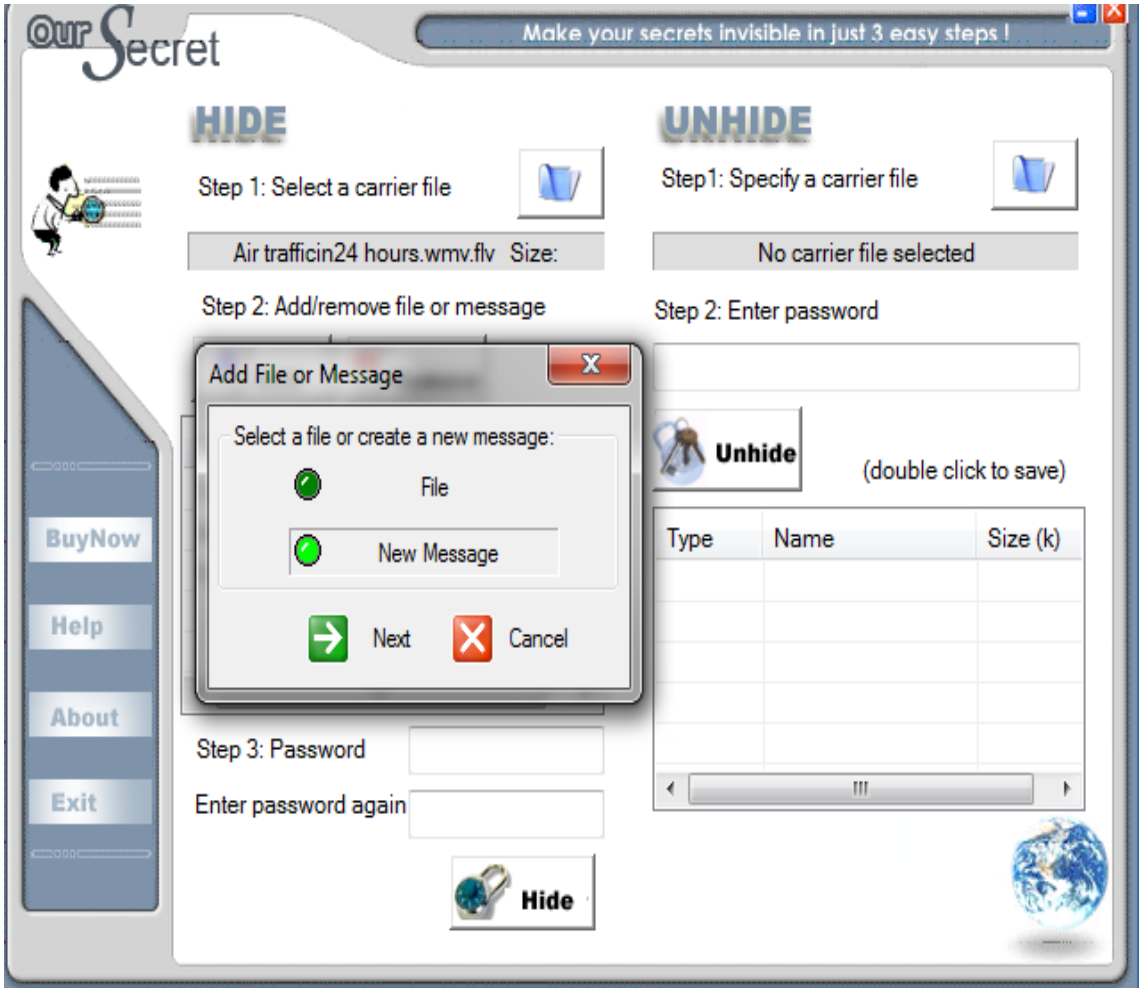
Επίσης μπορείτε να αποκρύψετε ένα ή περισσότερα αρχεία σε οποιοδήποτε αρχείο τύπου. Αν θέλετε να προσθέσετε κι άλλα αρχεία κάντε κλικ ξανά το εικονίδιο "add" την ίδια διαδικασία όπως πριν. Το εικονίδιο "Remove" είναι για διαγραφή αρχείου ή μηνύματος, επιλέγοντάς το.

Σημείωση: Μπορείτε να επιλέξετε οποιοδήποτε αρχείο ως αρχείο του φορέα σας εκτός από txt και το αρχείο htm. Επίσης οι μεταφορείς μπορεί να είναι αρχεία εικόνες, ήχου, ή ακόμα και αρχεία exe.

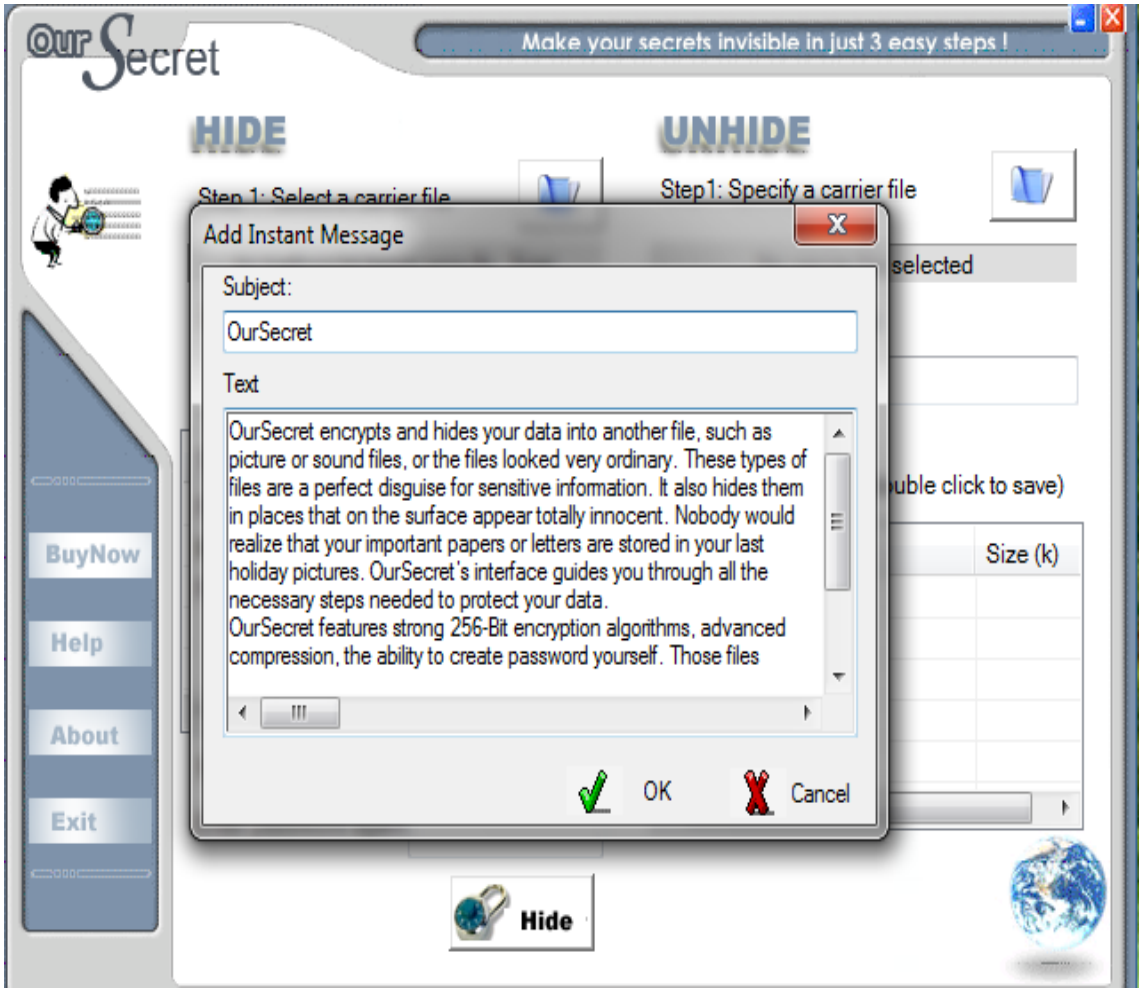


Εικόνα 22: OurSecret (2/7)

Το "New Message" είναι για να γράψετε ένα μήνυμα που επιθυμείτε ή ένα μικρό κείμενο. Έπειτα πατήστε "Next" και όταν τελειώσετε επιλέξτε "OK". Επίσης αν θέλετε να το επεξεργαστείτε ξανά, κάντε απλά διπλό κλικ.

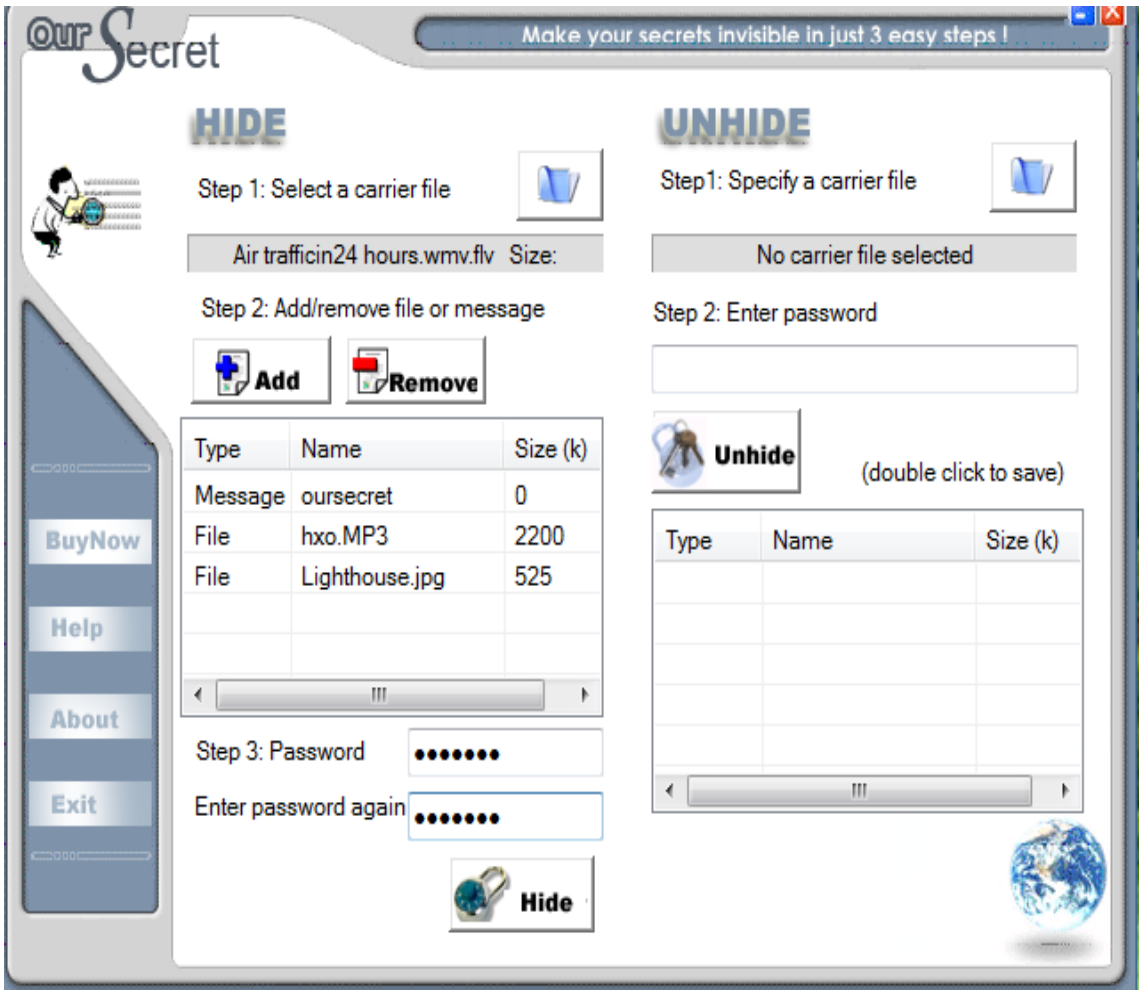


Εικόνα 23: OurSecret (3/7)



Εικόνα 24: OurSecret(4/7)

Τρίτο βήμα: Πληκτρολογήστε τον κωδικό και τον κωδικό επιβεβαίωσης που επιθυμείτε. Έπειτα πατήσετε το εικονίδιο “Hide”. Τέλος αποθηκεύστε π.χ. στην επιφάνεια και μετά κλείστε την εφαρμογή.

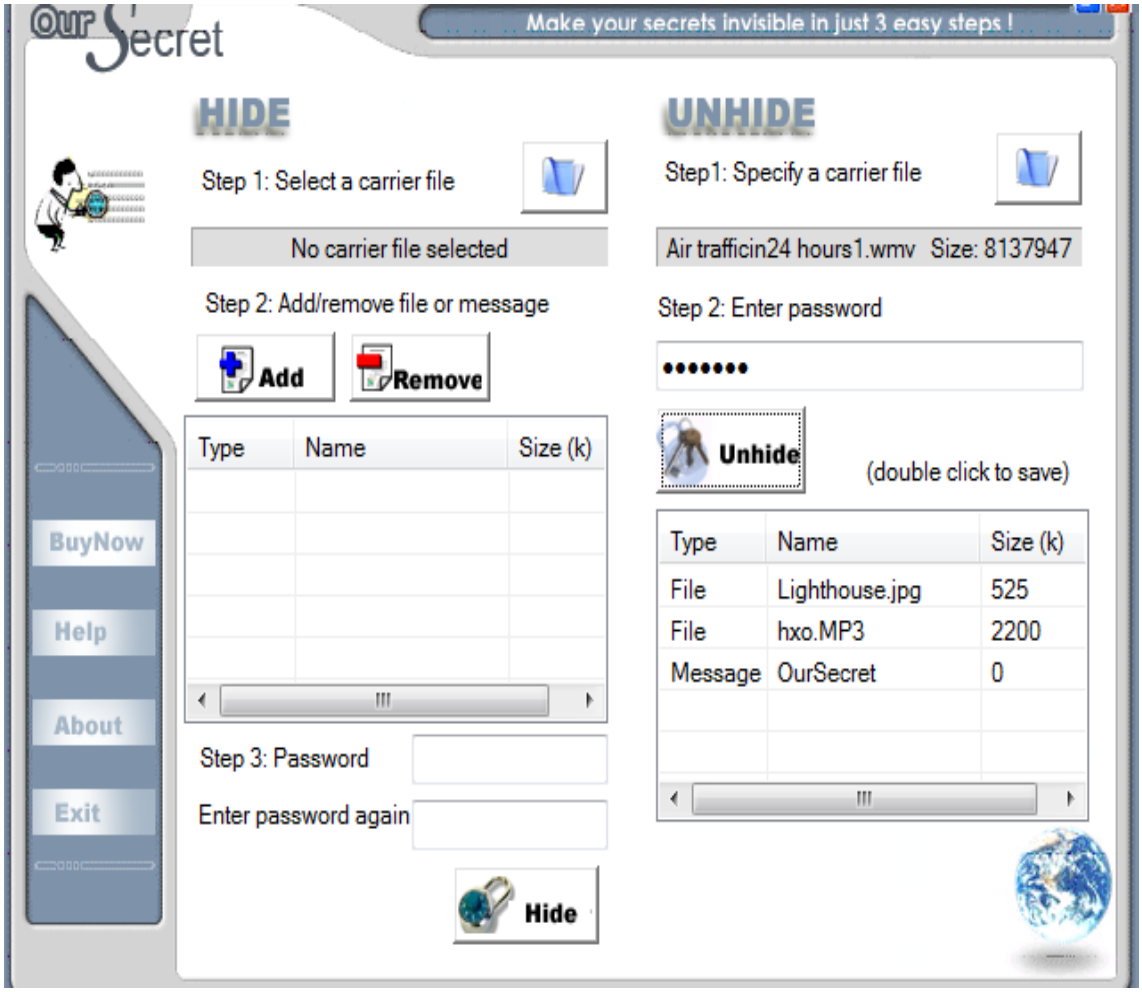


Εικόνα 25: OurSecret(5/7)

Ανοίξτε ξανά την εφαρμογή για να ανακτήσετε τα κρυμμένα αρχεία, πατήστε το εικονίδιο με το "φάκελο", επιλέξτε το κρυπτογραφημένο αρχείο. Έπειτα πληκτρολογήσετε τον κωδικό που δημιουργήσατε.

Εικόνα 26: OurSecret(6/7)

Εμφανίζονται τα κρυμμένα αρχεία. Έπειτα επιλέξτε κάθε αρχείο και αποθηκεύστε π.χ. στην επιφάνεια εργασία.



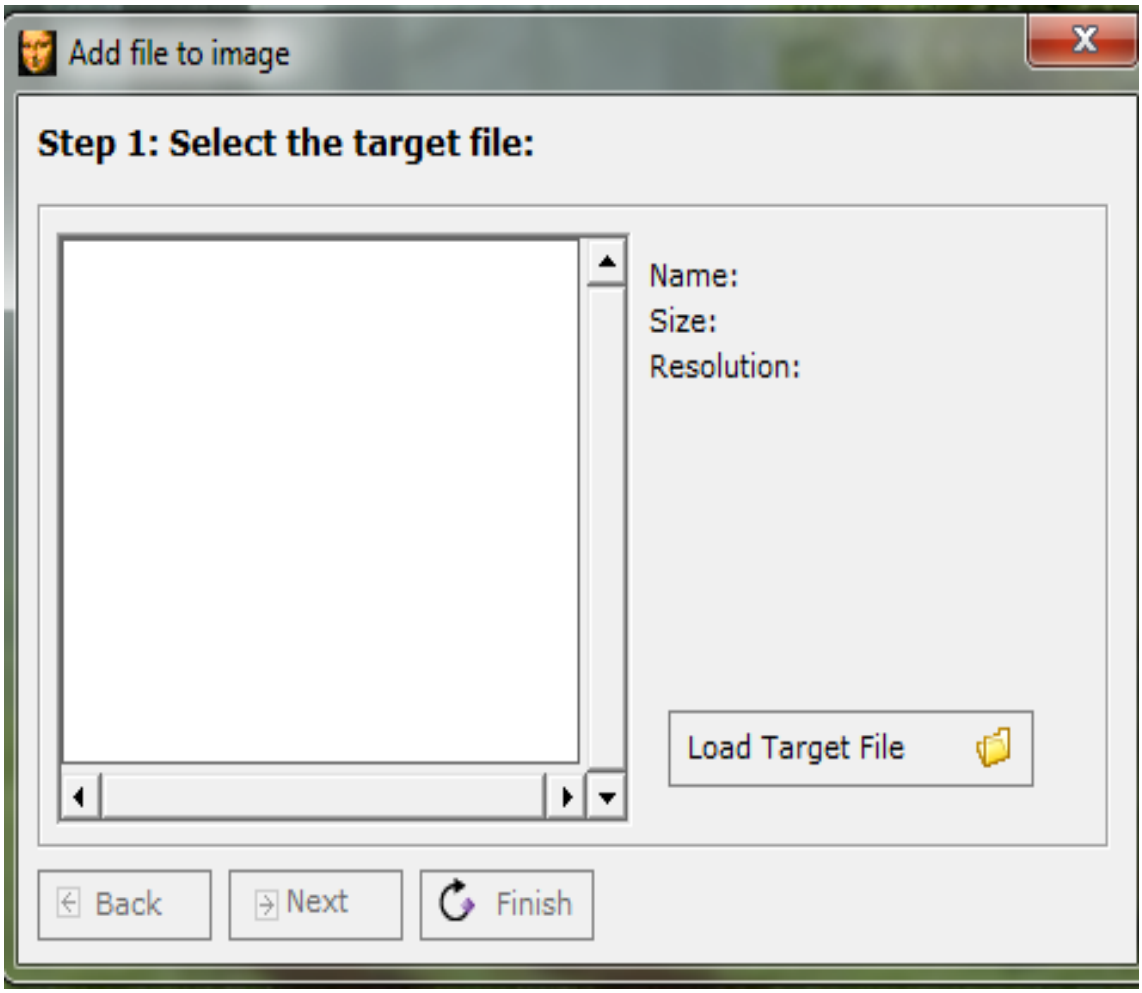
Εικόνα 27: OurSecret(7/7)

6.3 Xiao Stenography

Το Xiao Steganography είναι μια εφαρμογή για να κρύψει τα δεδομένα που αφορά για αρχεία εικόνες με bmp και αρχεία ήχου με wav. Μπορείτε να το κατεβάσετε από το http://download.cnet.com/Xiao-Steganography/3000-2092_4-10541494.html (είναι freeware).

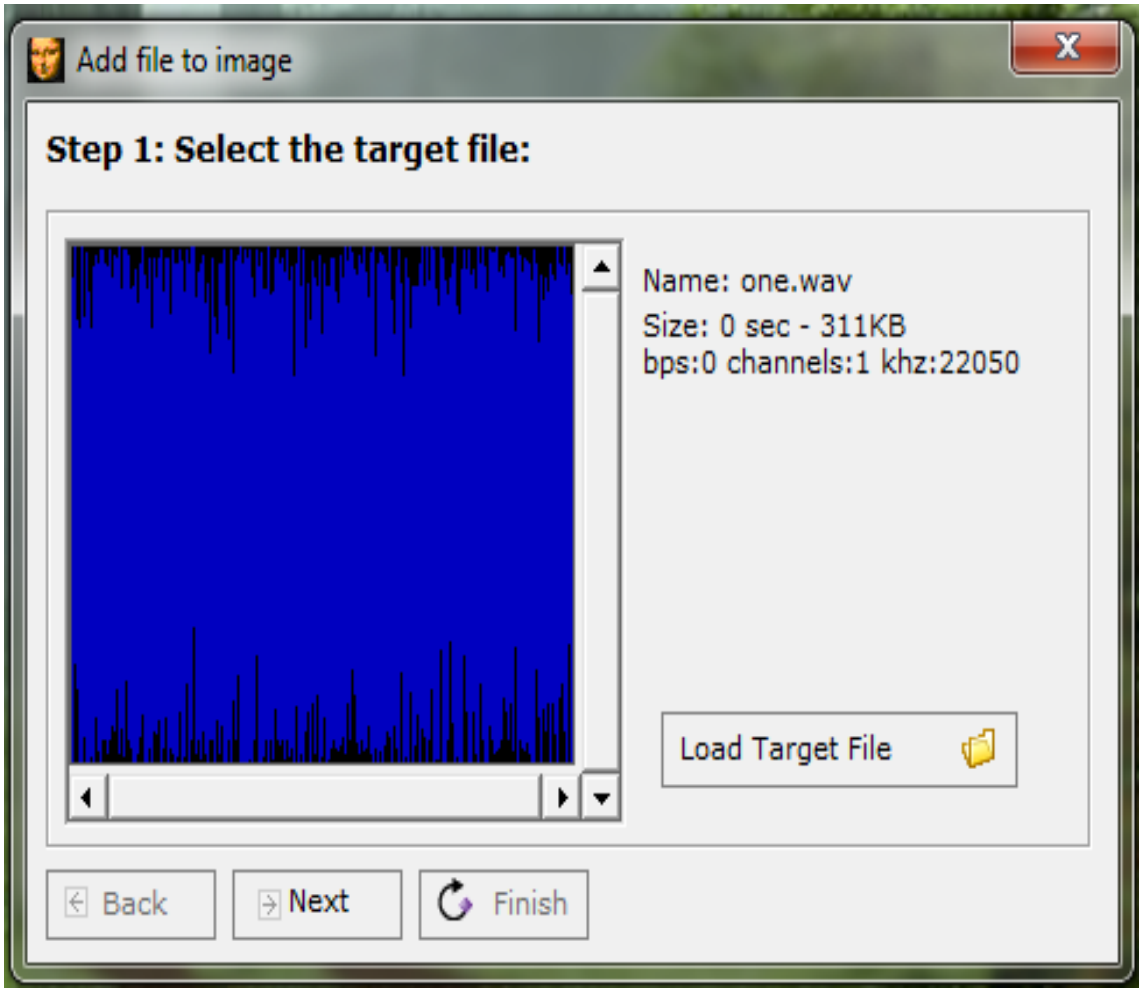
Εικόνα 28: Xiao Steganography(1/12)

Για να αποκρύψετε ένα αρχείο επιλέξετε “Add Files”, όπως φαίνεται την παραπάνω εικόνα, ύστερα πατήστε “Load Target File” για να επιλέξετε το αρχείο που επιθυμείτε για μεταφορέα.



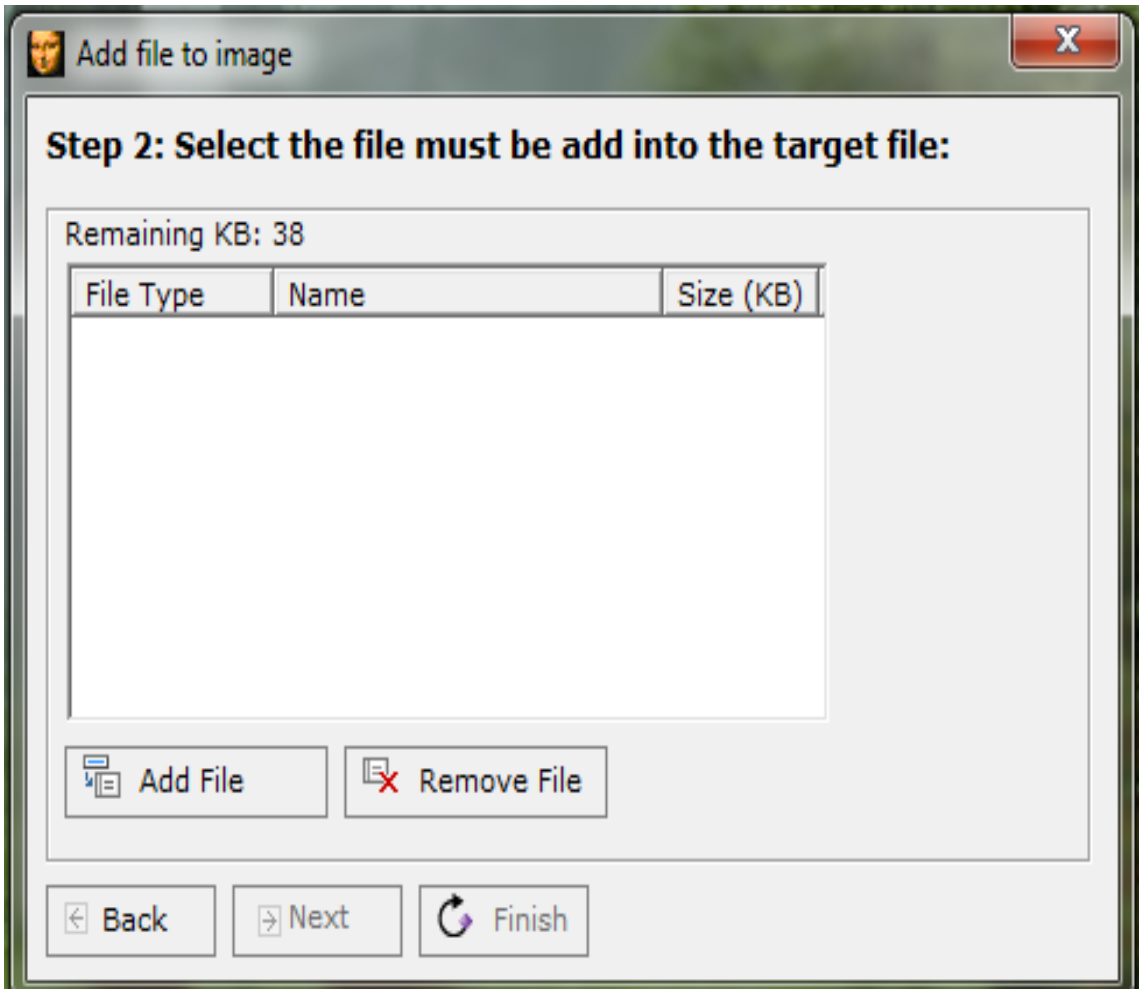
Εικόνα 29: Xiao Steganography (2/12)

Εδώ το συγκεκριμένο παράδειγμα είναι ένα αρχείο ήχου με κατάληξη .wan. Έπειτα πατάμε "Next".



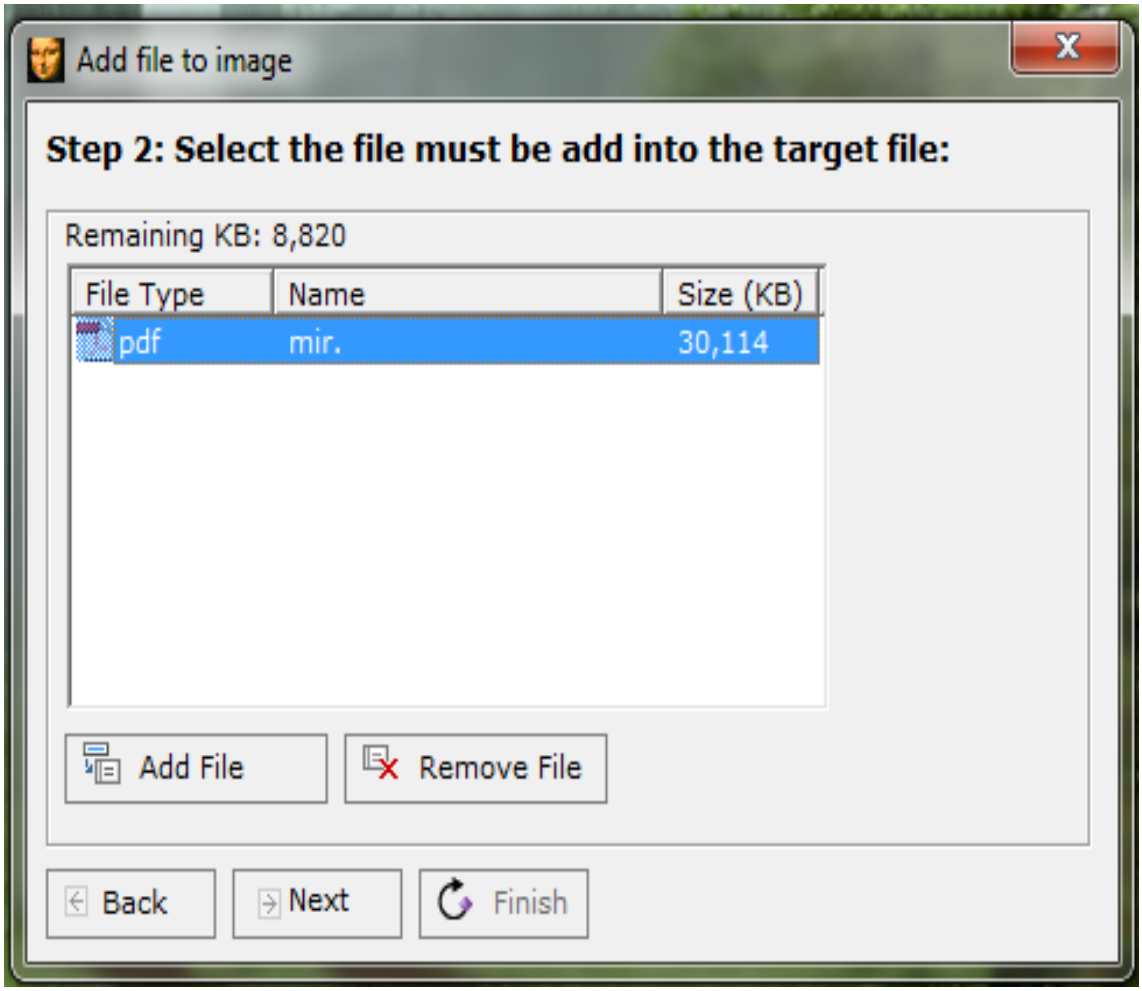
Εικόνα 30: Xiao Steganography(3/12)

Επιλέξετε το “Add File” για να κρύψετε ένα αρχείο που θέλετε, (μπορεί να είναι οποιοδήποτε αρχείο τύπου).

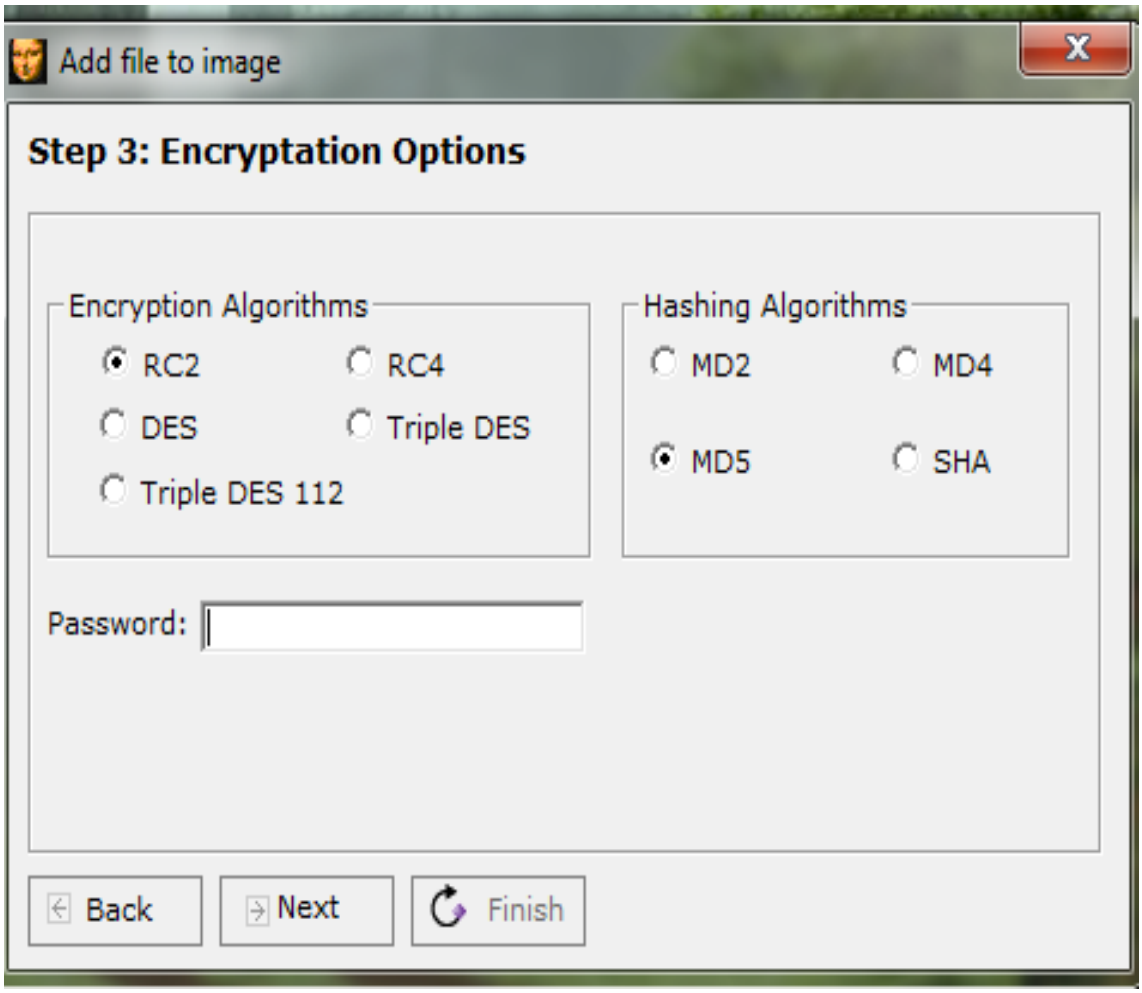


Εικόνα 31: Xiao Steganography(4/12)

Εδώ το συγκεκριμένο παράδειγμα είναι αρχείο με pdf.



Εικόνα 32: Xiao Steganography(5/12)



Εικόνα 33: Xiao Steganography (6/12)

Λίγα λόγια για τους αλγόριθμους…

Αλγόριθμοι κρυπτογράφηση

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα.

Ο DES χρησιμοποιεί κλειδί με μέγεθος 64 bit από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών. Συνδυάζεται με ασύμμετρο κρυπτοσύστημα. Αλλά ο απλός DES είχε αποδοκιμαστεί επειδή είχαν επιδειχθεί πολλές εξαντλητικές επιθέσεις αναζήτησης κλειδιού.

Ο Triple-DES είναι μια επέκταση του συστήματος DES και βασίζεται στο σύστημα DES που χρησιμοποιείται κατά κόρον. Ο Triple-Des (τριπλό DES) κρυπτογραφεί κάθε block κειμένου τρεις φορές, χρησιμοποιώντας τρία διαφορετικά κλειδιά. Ο Triple-DES επιλέχθηκε ως ο απλούστερος τρόπος να μεγαλώσουμε το κλειδί χωρίς να χρειαστεί να πάμε σε κάποιο καινούργιο αλγόριθμο.
Παραδείγματος χάρη: 2 κλειδιά (k_1, k_2) και 3 στάδια σημαίνει τρία κλειδιά και όχι δύο. Ο Triple-DES 112 σημαίνει 112 bits → 2^{112} → 10^{14} χρόνια.

Αλγόριθμοι Κατακερματισμού

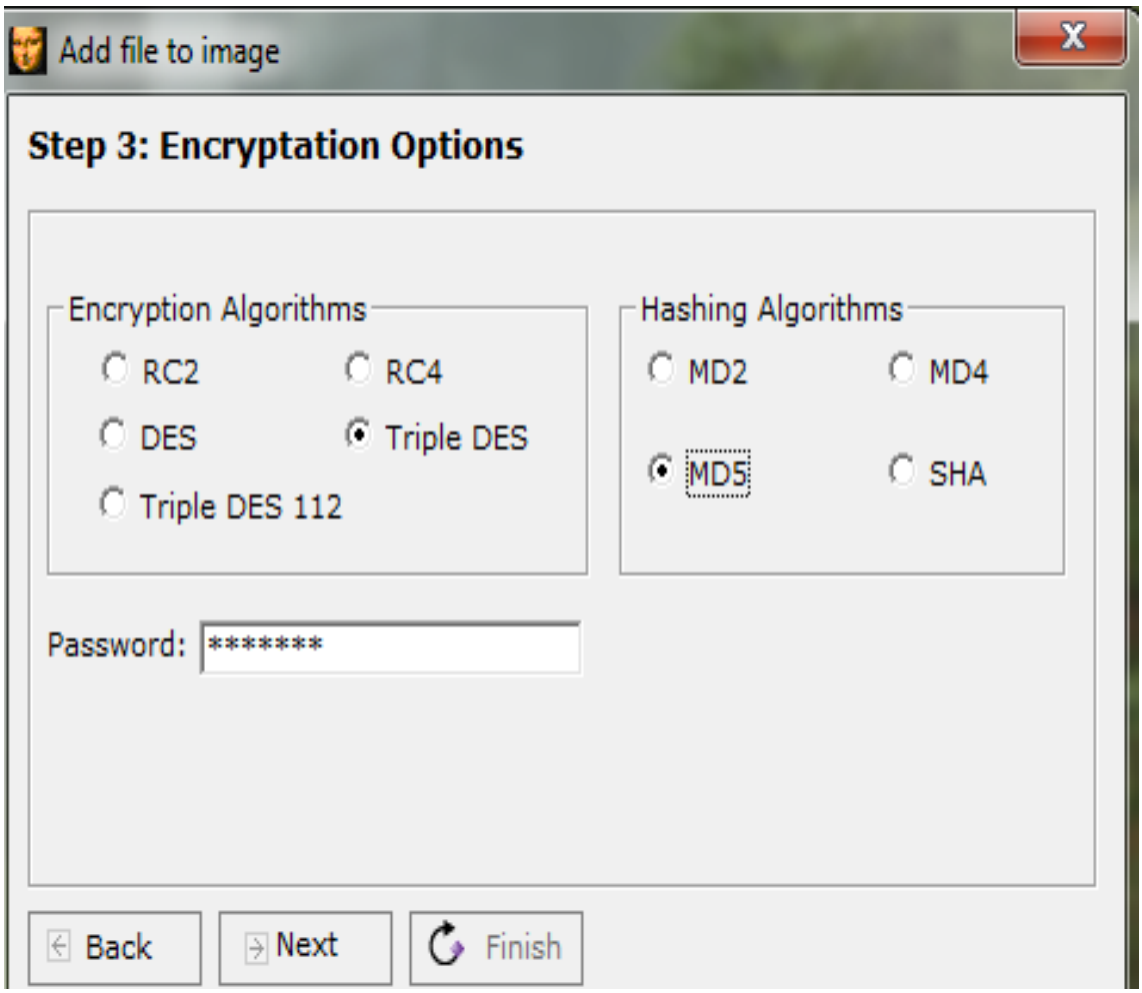
Οι αλγόριθμοι MD2,MD4,MD5 είναι hash functions (συναρτήσεις κατακερματισμού) που έχουν αναπτυχθεί από τον Ron Rivest. Προορίζονται, κυρίως, για την παραγωγή ψηφιακών υπογραφών. Το μήνυμα πρώτα σμικρύνεται με έναν από αυτούς τους αλγόριθμους και έπειτα, το message digest του μηνύματος κρυπτογραφείται με την ιδιωτική κλείδα του αποστολέα. Και οι τρεις παίρνουν στην είσοδο μήνυμα αυθαίρετου μήκους και δίνουν στην έξοδο ένα message digest 128 bits. Παρ' όλο που η κατασκευή τους μοιάζει αρκετά, ο MD2 είχε σχεδιαστεί για μηχανές 8 bit, σε αντίθεση με τους MD4 και MD5 που προορίζονται για μηχανές 32 bits.

Ο MD4 είναι μια δυαδική αναπαράσταση του μηνύματος των 64 bits προστίθεται στο μήνυμα και το αποτέλεσμα επεξεργάζεται με compression function. Τα blocks που διαχειρίζεται ο compression function έχουν μήκος 512 bits και κάθε block επεξεργάζεται πλήρως σε τρεις διακριτούς επαναληπτικούς γύρους. Ο MD4 έχει επανειλημμένα αναλυθεί με διάφορους τρόπους και δεν πρέπει να θεωρείται πλέον ασφαλής.

Ο MD5 Είναι μια κατά πολύ βελτιωμένη έκδοση του MD4, γι' αυτό είναι και λίγο πιο αργός. Η μόνη διάφορα είναι η χρήση τεσσάρων επαναλήψεων κατά την επεξεργασία του κάθε block. Επειδή οι hash functions είναι πιο γρήγοροι από τους αλγόριθμους κρυπτογράφησης και ψηφιακών υπογραφών, συνηθίζεται να παράγεται η υπογραφή των μηνυμάτων με την εφαρμογή κρυπτογραφικών διαδικασιών στο message digest, το οποίο είναι πιο μικρό και εύκολο στην διαχείριση.

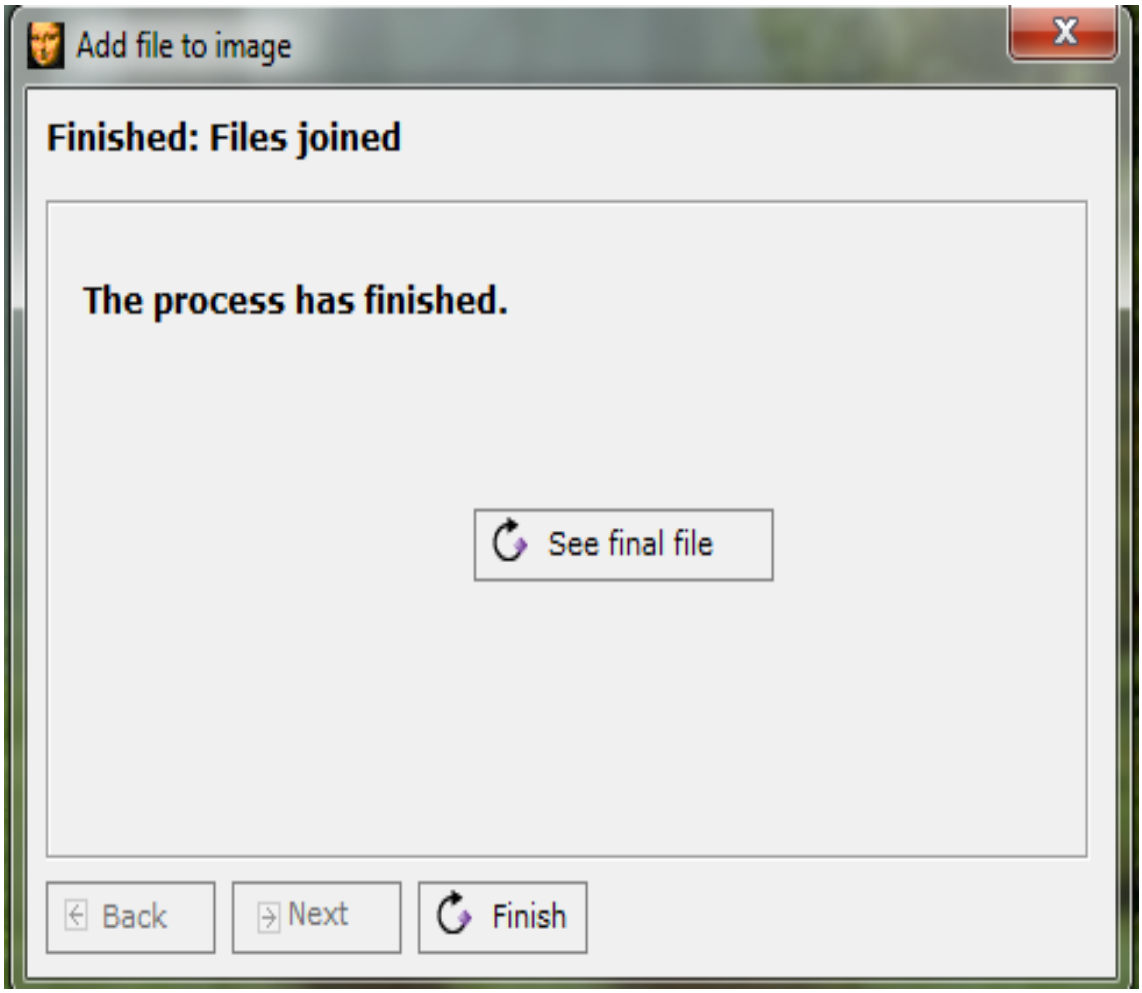
Ο SHA-1, αναπτύχθηκε από το NIST. Ο SHA-1 αποτελεί επανέκδοση του SHA που διόρθωνε μια ατέλεια του τελευταίου. Η δομή και λειτουργία του SHA-1 είναι παρόμοια με την αντίστοιχη του MD4 που αναπτύχθηκε από τον Ron Rivest. Ο SHA-1 παίρνει είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει message digest 160 bits. Είναι ελαφρά πιο αργός από τον MD5.

Επιλέξετε τους παρακάτω αλγόριθμους και πατάμε “Next”.



Εικόνα 34: Xiao Steganography (7/12)

Τέλος, αποθηκεύσετε π.χ. στην επιφάνεια εργασία και δώσετε ένα όνομα. Έπειτα πατάμε Finish και κλείνουμε την εφαρμογή.

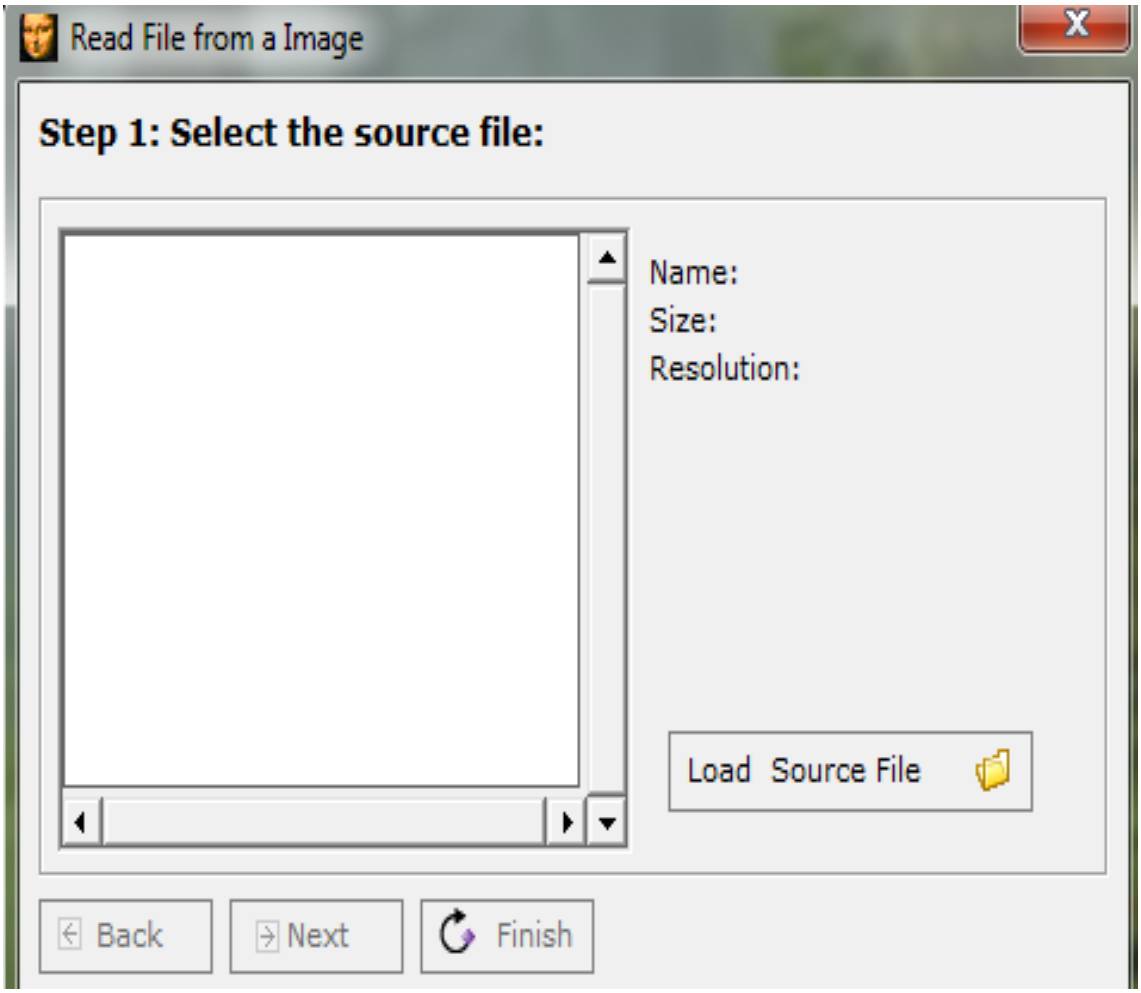


Εικόνα 35: Xiao Steganography (8/12)

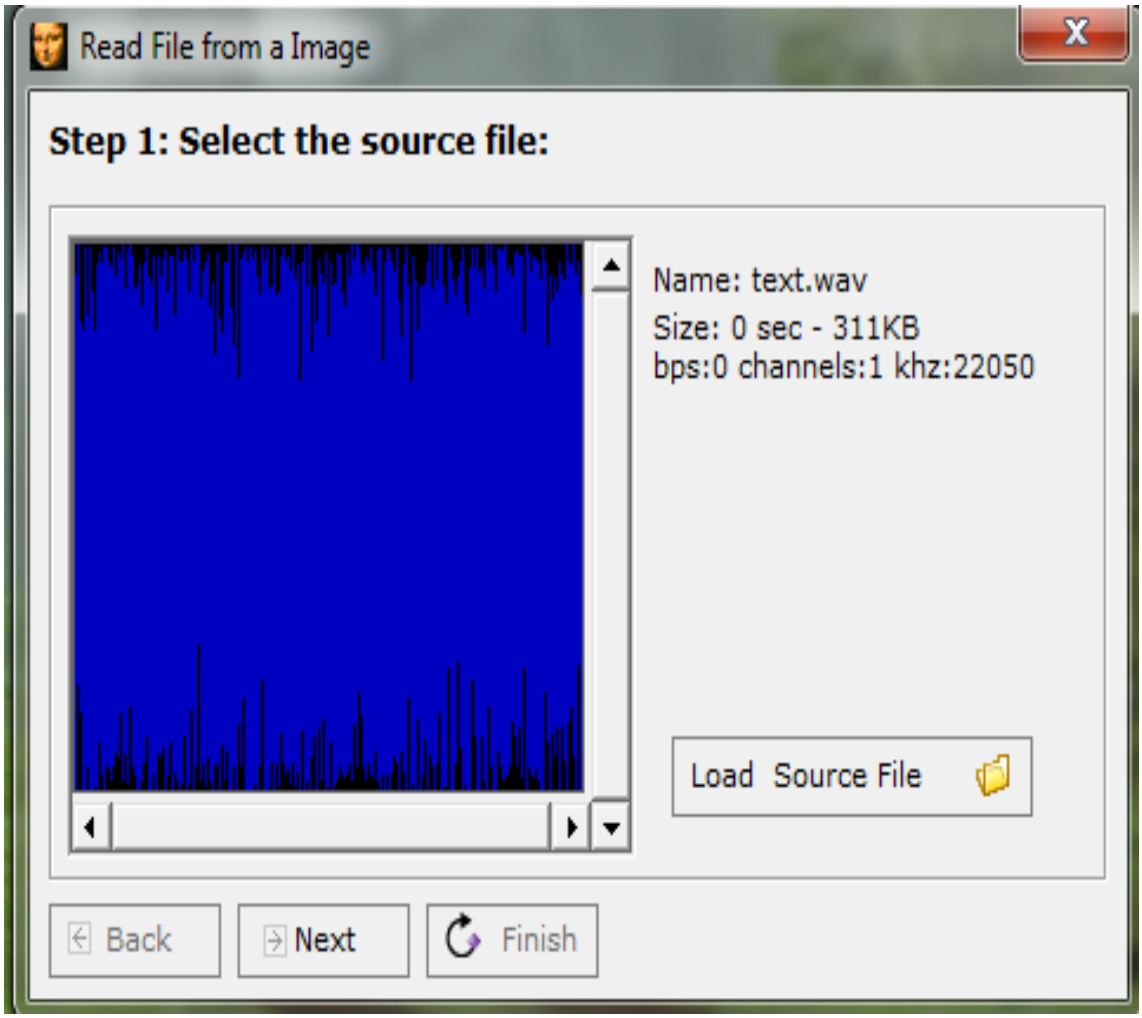
Για να ανακτήσετε το κρυμμένο αρχείο, ανοίγουμε την εφαρμογή και επιλέξετε “Extract Files”.

Εικόνα 36: Xiao Steganography (9/12)

Πατήσετε το “Load Target File” για να επιλέξετε το κρυπτογραφημένο αρχείο και όταν φορτωθεί το αρχείο, πατήσετε το “Next”.

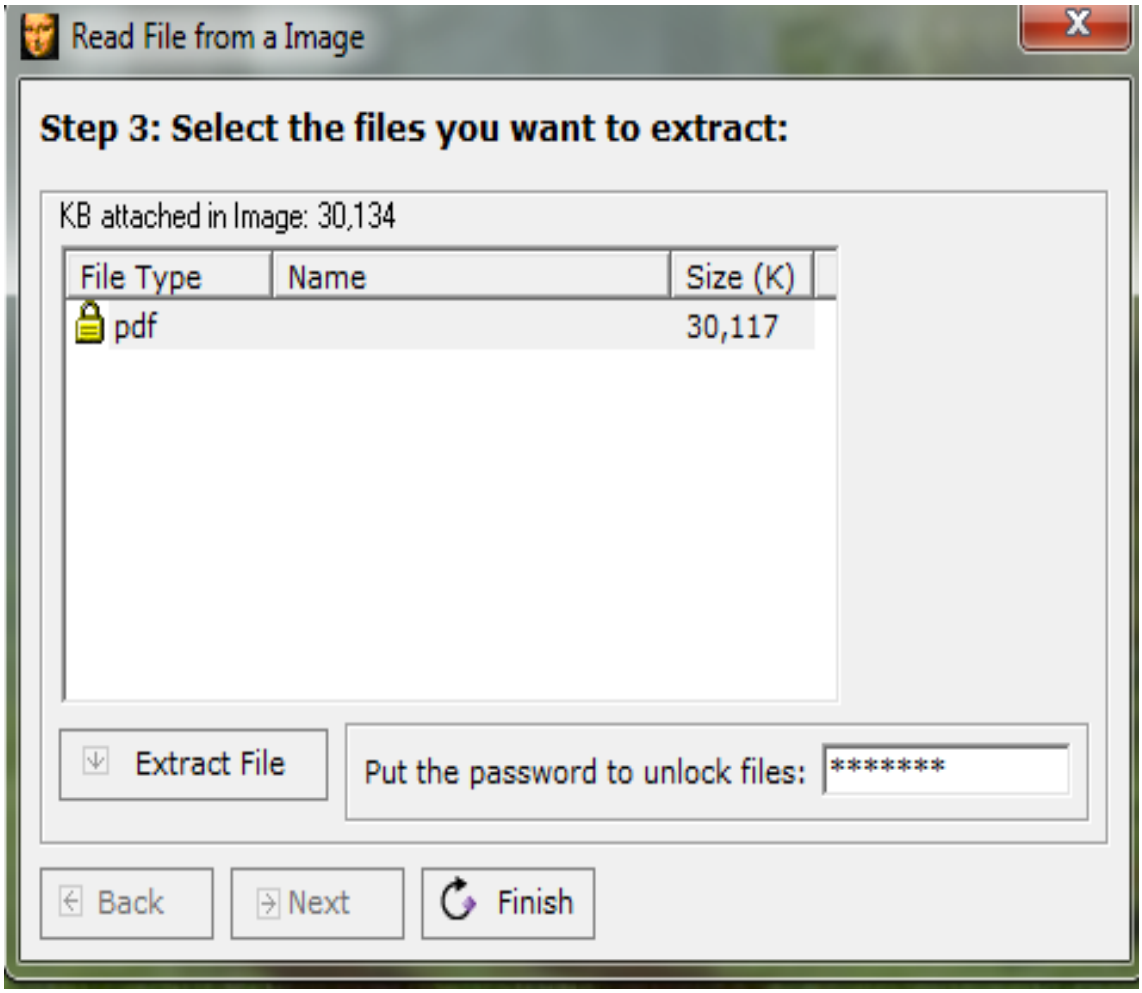


Εικόνα 37: Xiao Steganography (10/12)



Εικόνα 38: Xiao Steganography (11/12)

Πληκτρολογήστε τον κωδικό που δημιουργήσατε και επιλέξτε "Extract File". Έπειτα αποθηκεύστε και δώστε ένα όνομα. Στο τέλος εμφανίζει το κρυμμένο αρχείο.

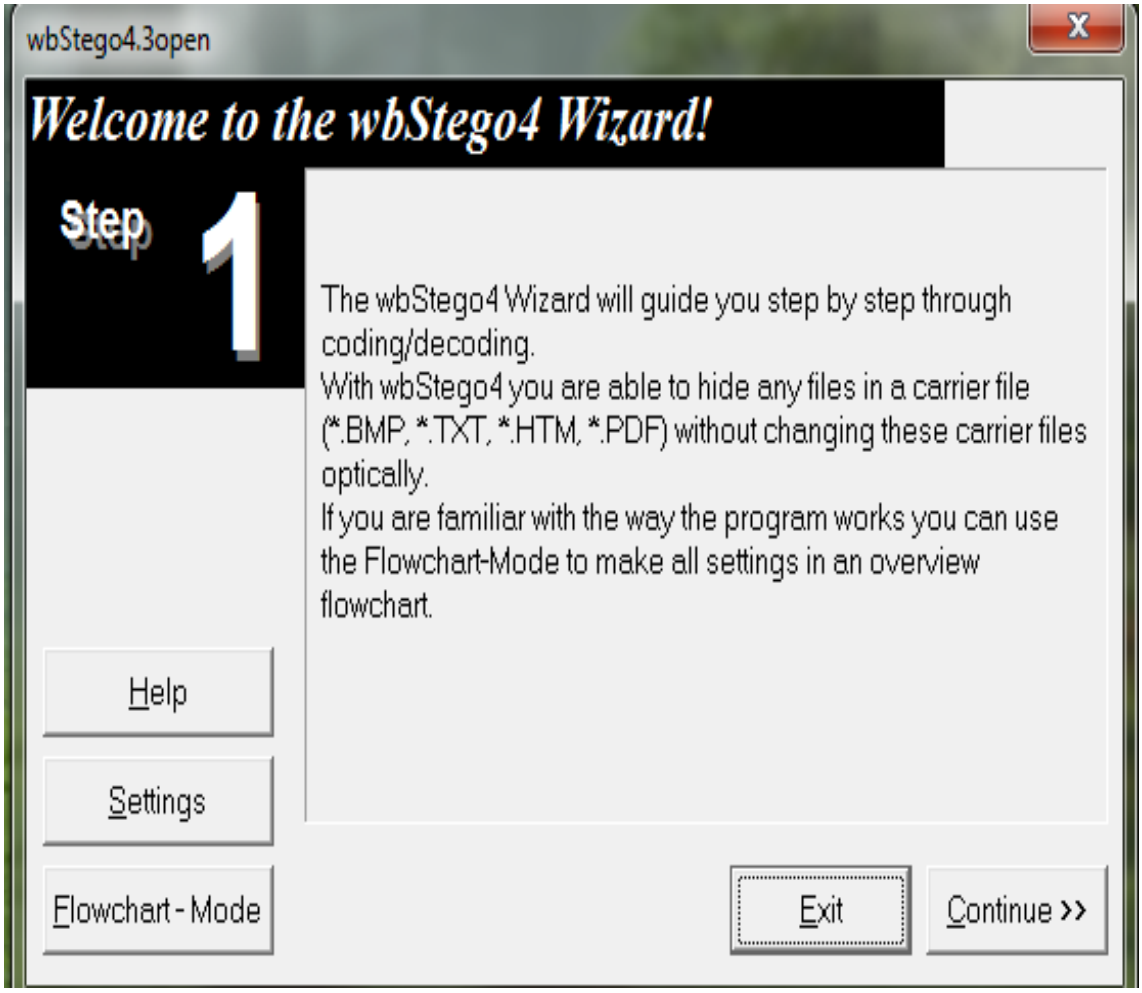


Εικόνα 39: Xiao Steganography (12/12)

6.4 wbStego4

Το WbStego (είναι freeware) είναι ένα εργαλείο που κρύβει κάθε τύπο αρχείου σε bitmap εικόνες, αρχεία κειμένου, αρχεία HTML ή Adobe PDF αρχεία.

Πατάμε το continue.



Εικόνα 40: wbStego4 (1/16)

Επιλέξετε encode για να αποκρύψετε ένα αρχείο και τη συνέχεια πατάμε το continue.

Εικόνα 41: wbStego4 (2/16)

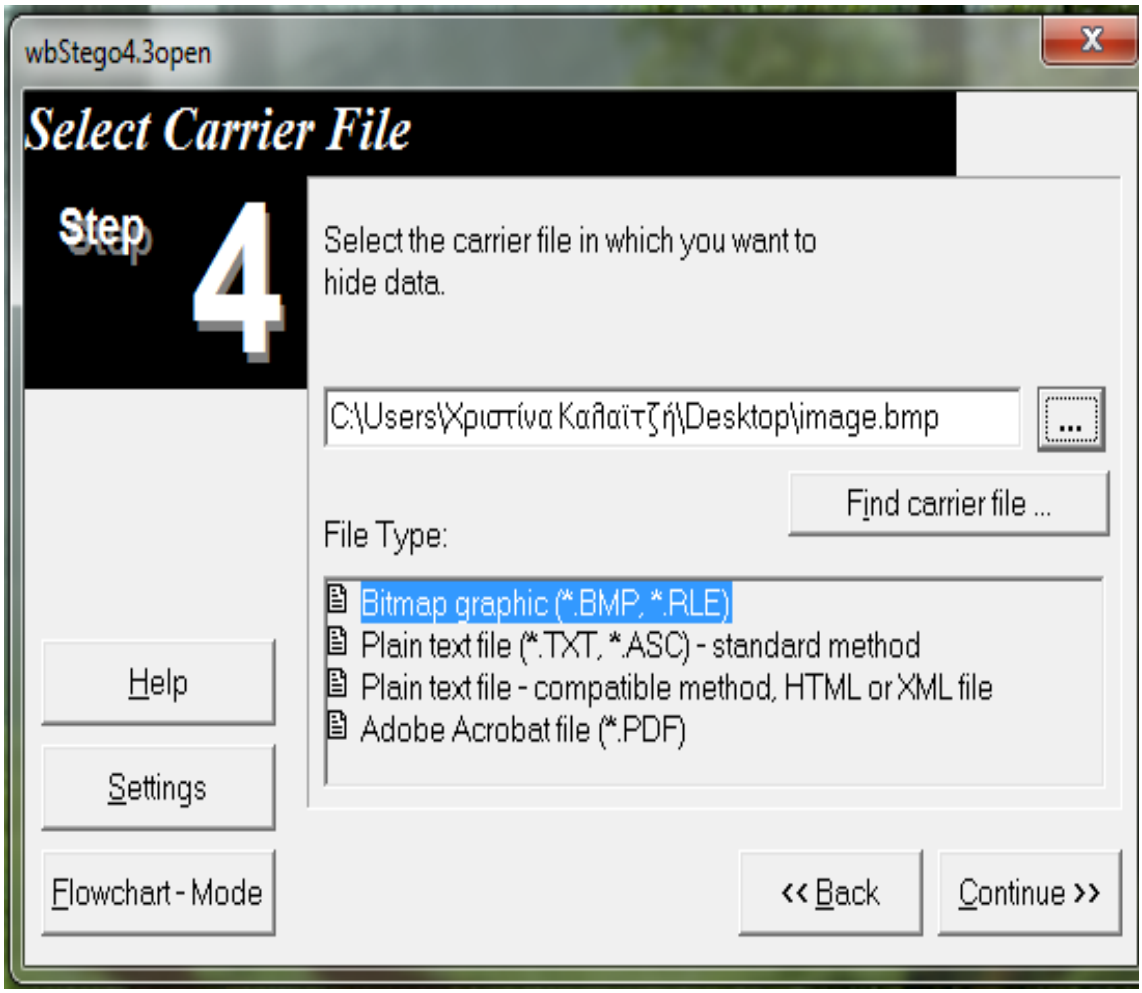
Πατήσετε το κουτάκι (…) εκεί που είναι επιλεγμένο έπειτα το continue.

Εικόνα 42: wbStego4 (3/16)

Εδώ το συγκεκριμένο παράδειγμα είναι ένα αρχείο με κατάληξη .pdf.

Εικόνα 43: wbStego4 (4/16)

Επιλέξετε μια εικόνα για μεταφορέα με κατάληξη .bmp και να είναι επιλεγμένο το Bitmap graphic(*.BMP, *.RLE). Αν ήταν για παράδειγμα ένα αρχείο με ιστοσελίδα (με κατάληξη .html) θα πρέπει να επιλέξετε το Plain text file-compatible method, HTML or XML file.

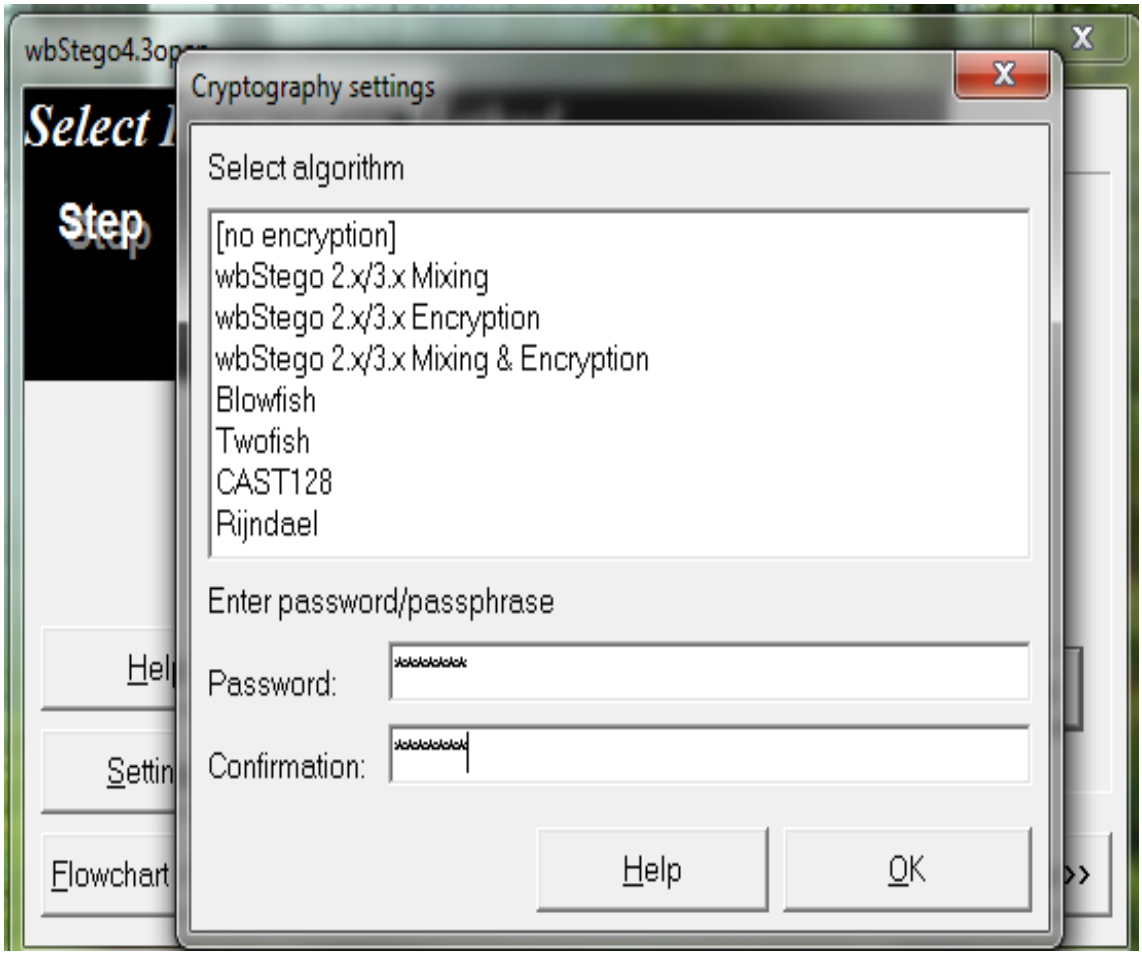


Εικόνα 44: wbStego4 (5/16)

Στη συνέχεια πατάμε το cryptography settings

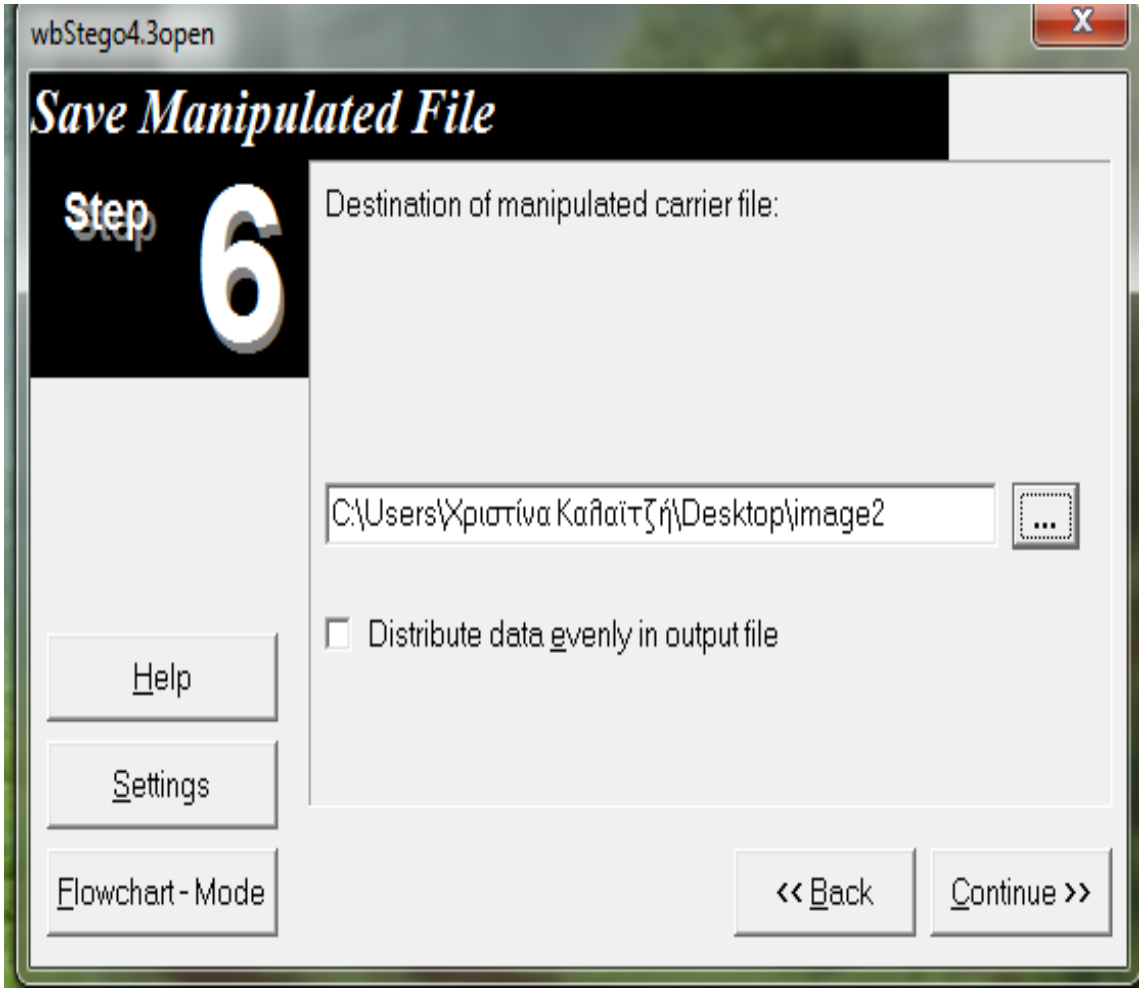
Εικόνα 45: wbStego4 (6/16)

Έπειτα πληκτρολογούμε το κωδικό και το κωδικό επιβεβαίωση και πατήσετε OK και μετά το continue.



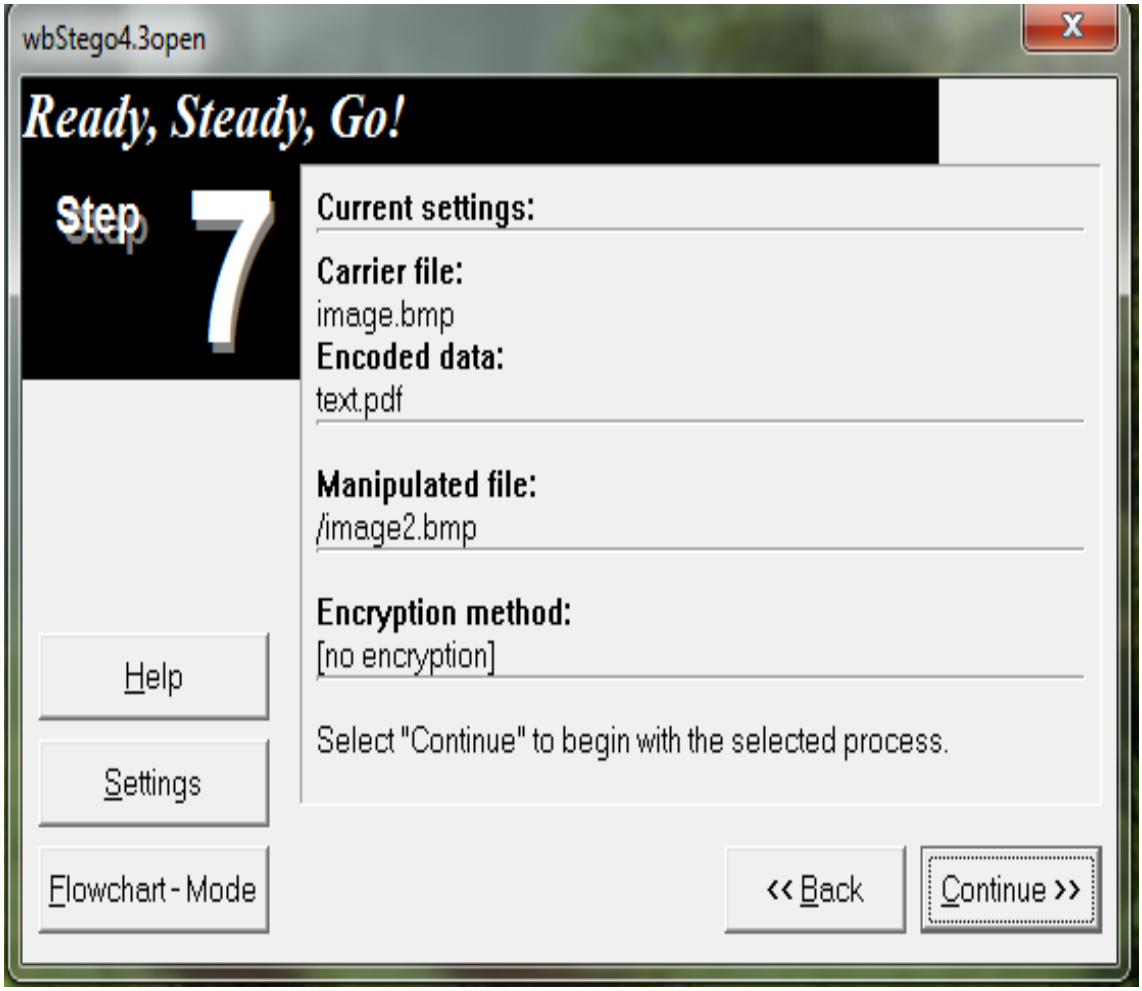
Εικόνα 46: wbStego4 (7/16)

Πατήσετε το κουτάκι (…) για να αποθηκεύσετε τη κρυπτογραφημένη εικόνα (π.χ. στην επιφάνεια εργασία) και να δώσετε ένα όνομα.



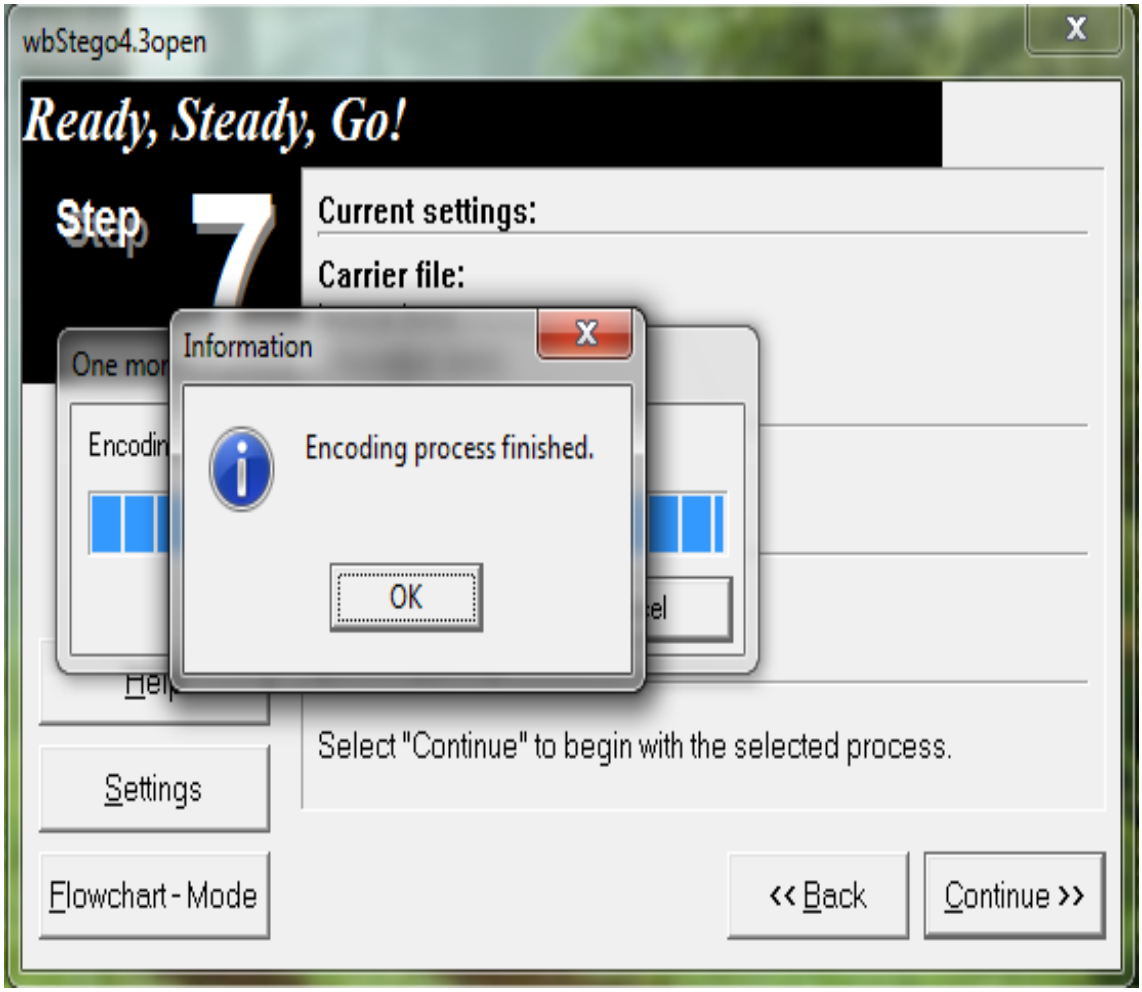
Εικόνα 47: wbStego4 (8/16)

Δείχνει τα στοιχεία που είχατε κάνει τα παραπάνω βήματα.



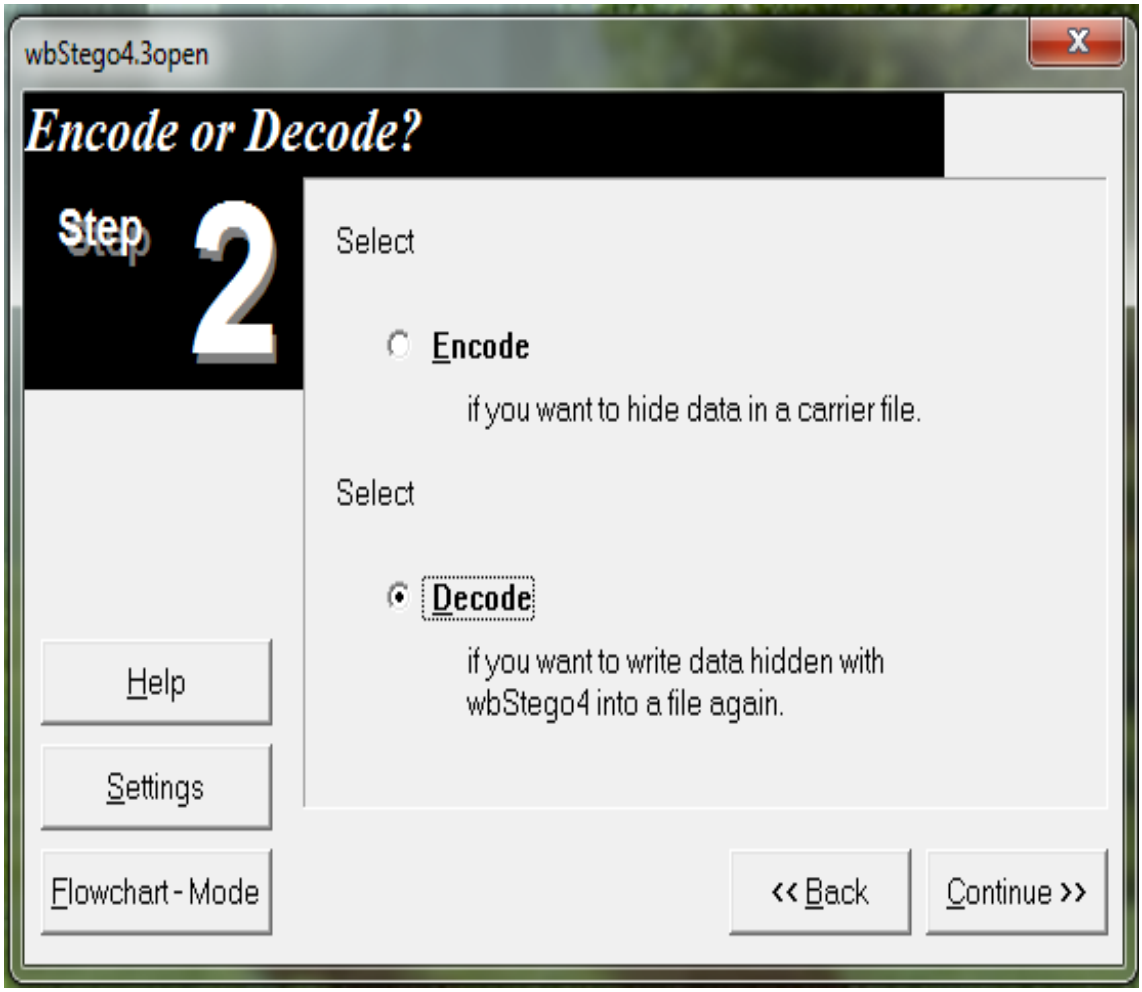
Εικόνα 48: wbStego4 (9/16)

Πατήσετε OK και η εικόνα κρυπτογραφήθηκε.



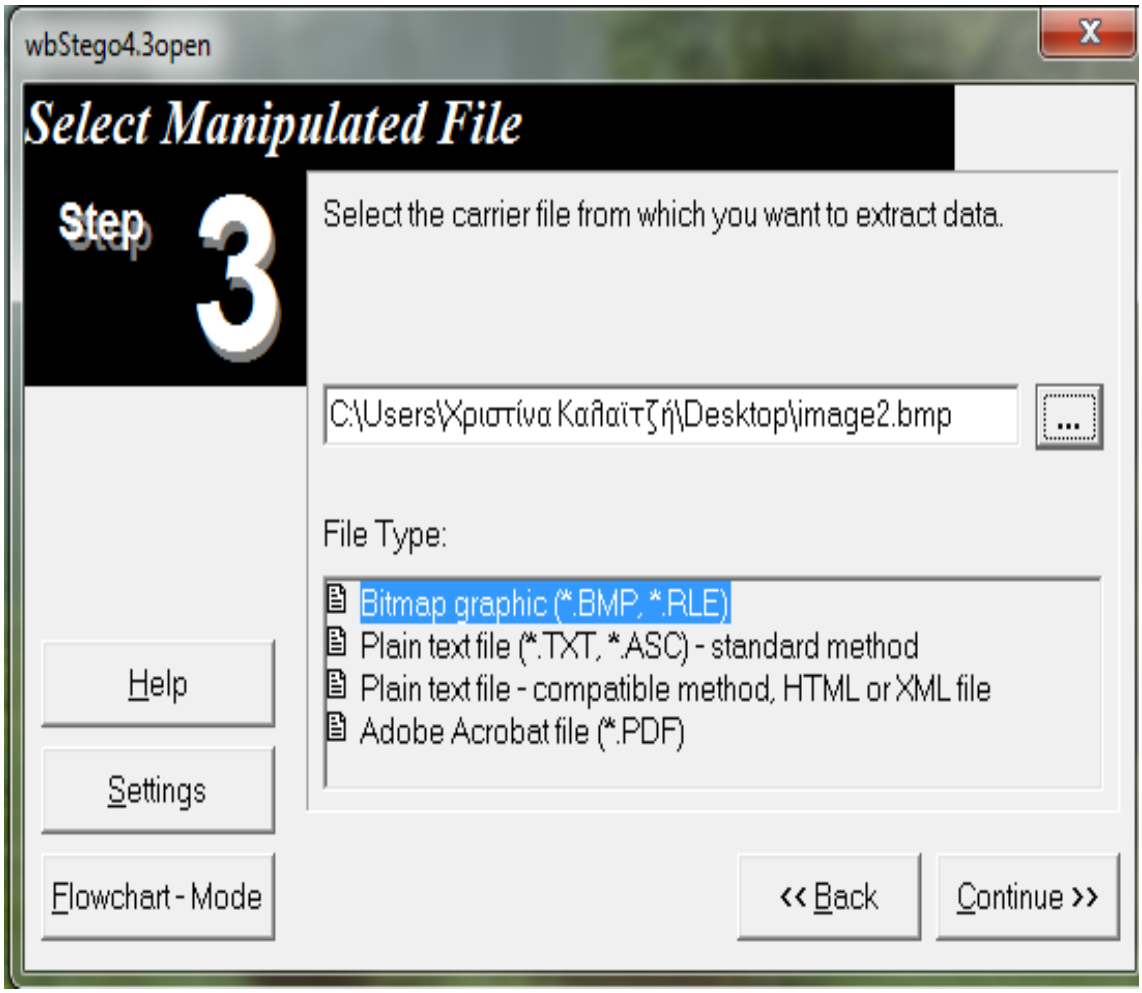
Εικόνα 49: wbStego4 (10/16)

Για να ανακτήσετε το κρυμμένο αρχείο, ανοίγουμε την εφαρμογή, πατάμε το πρώτο παράθυρο Continue και εδώ είναι το δεύτερο παράθυρο επιλέξετε το Decode.



Εικόνα 50: wbStego4 (11/16)

Πατήσετε το κουτάκι (…) για να πάρετε τη κρυπτογραφημένη εικόνα και να είναι επιλεγμένο Bitmap graphic(*.BMP, *.RLE).

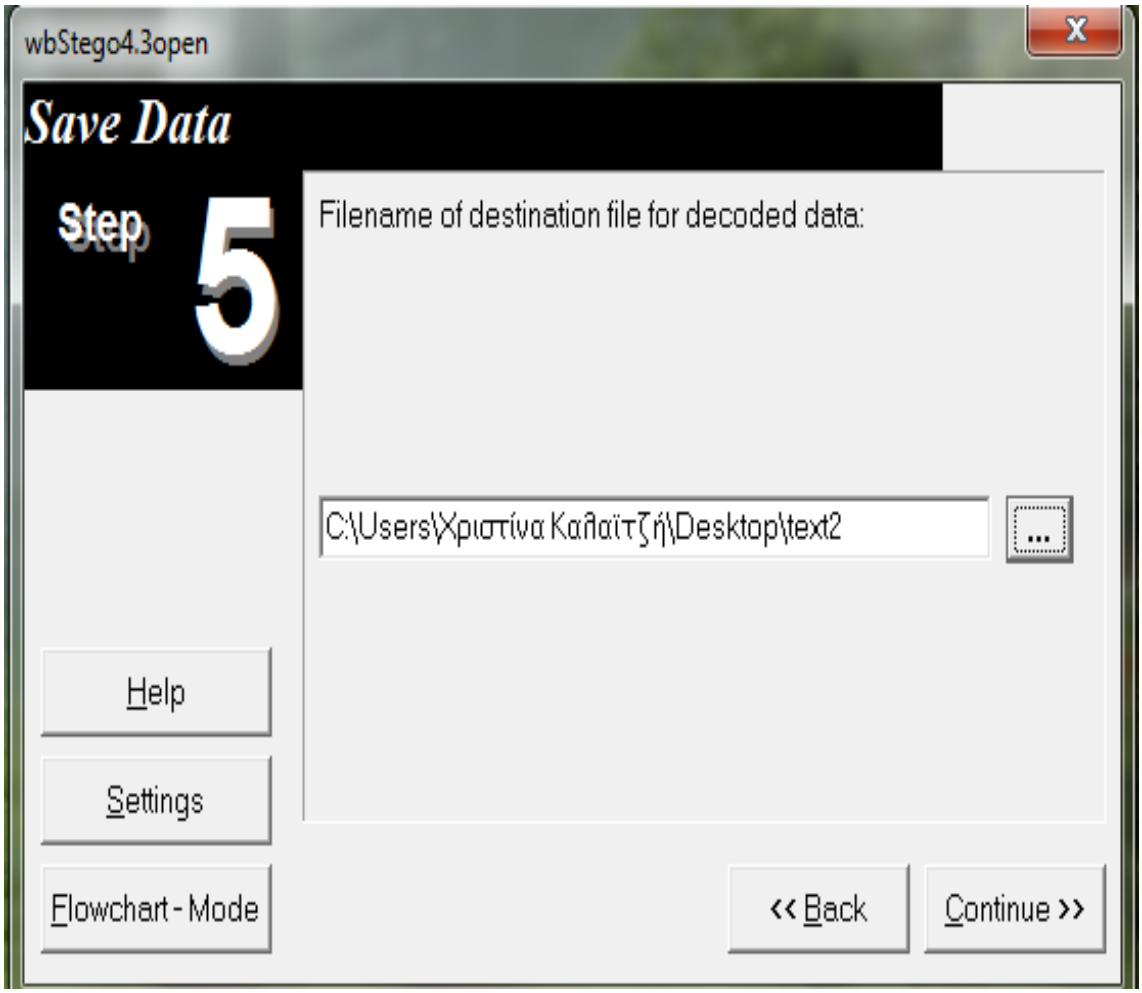


Εικόνα 51: wbStego4 (12/16)

Πληκτρολογήσετε το κωδικό που είχατε δημιουργήσει.

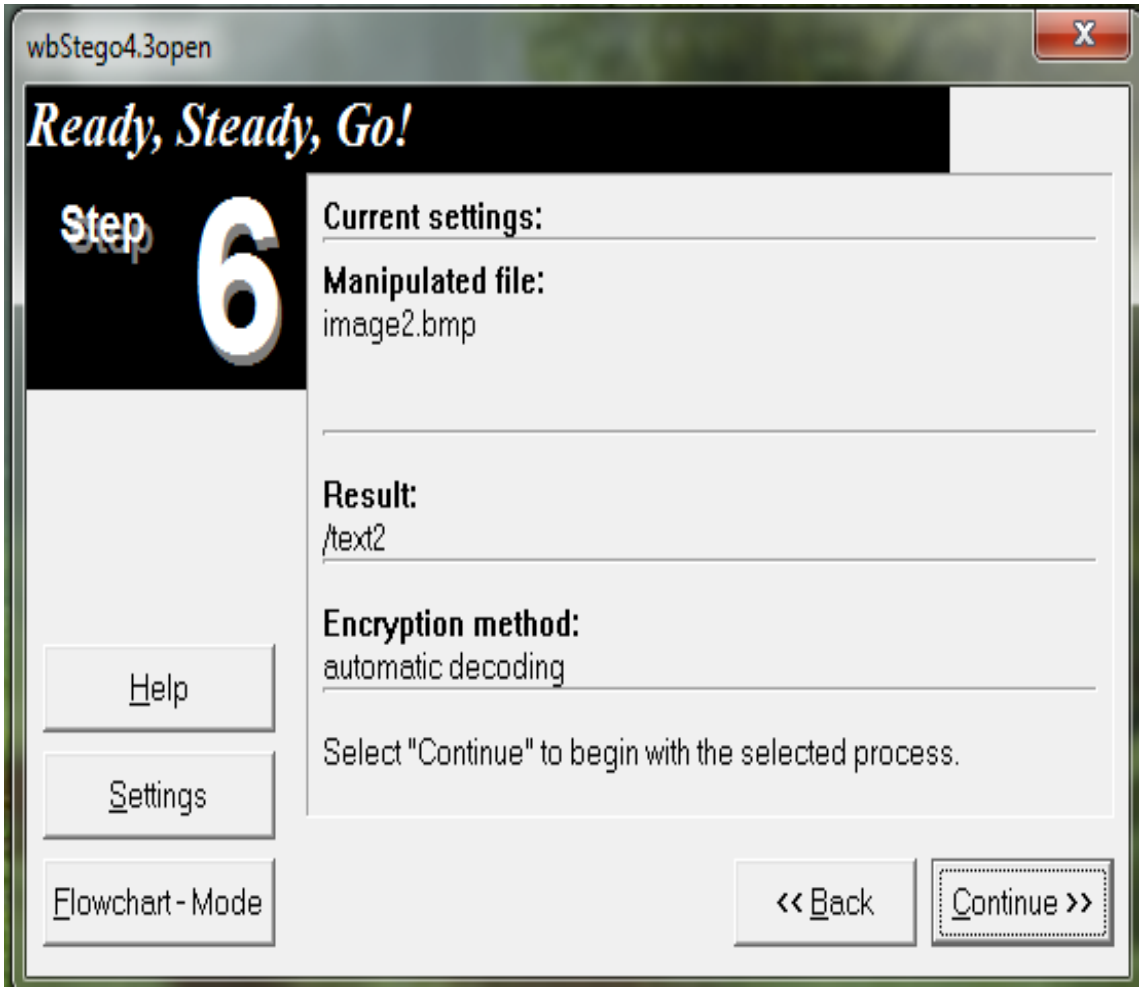
Εικόνα 52: wbStego4 (13/16)

Πατήσετε το κουτάκι (…) για να αποθηκεύσετε το κρυμμένο αρχείο (π.χ. στην επιφάνεια εργασία) και να δώσετε ένα όνομα.



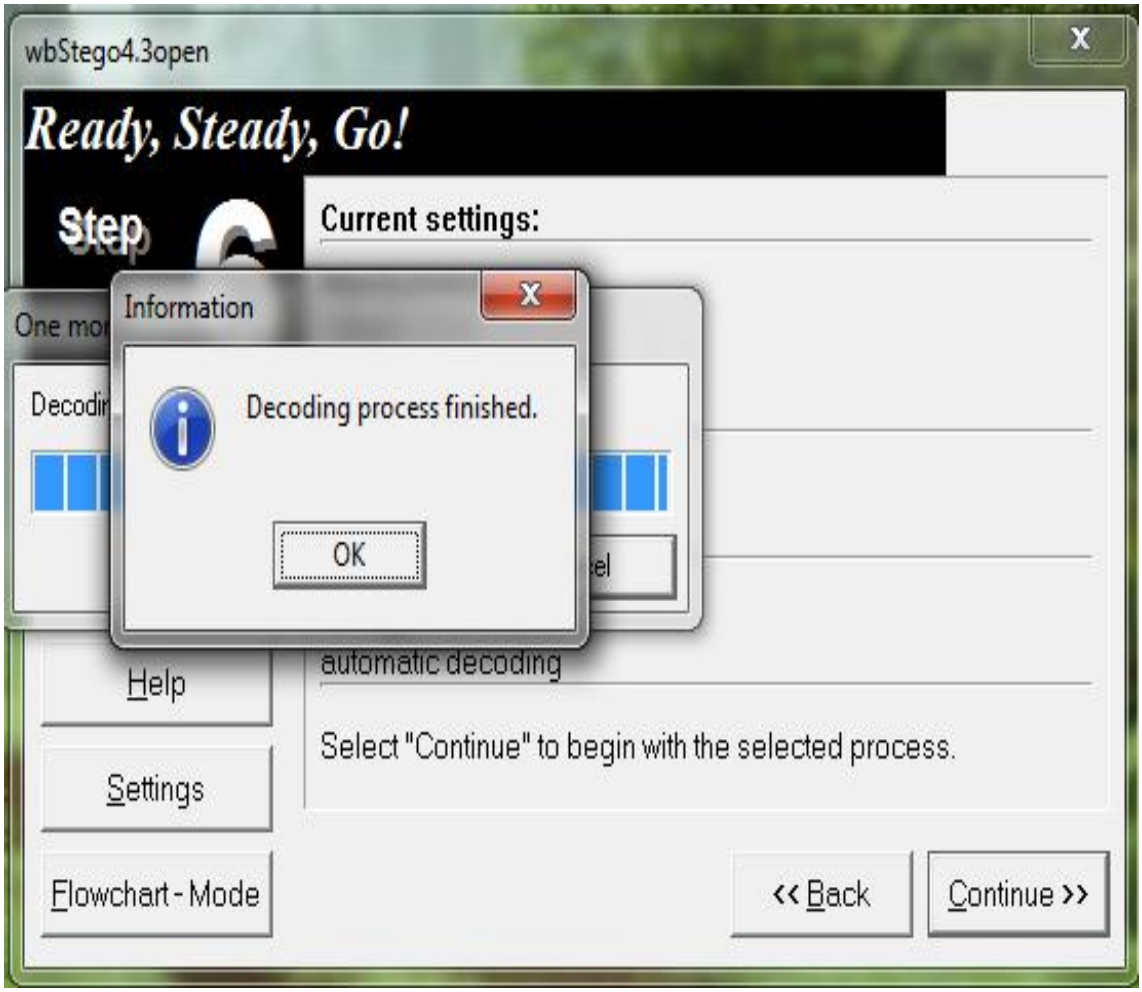
Εικόνα 53: wbStego4 (14/16)

Έπειτα πατάμε το continue.



Εικόνα 54: wbStego4 (15/16)

Πατάμε OK και το κρυμμένο κείμενο αποθηκεύτηκε.

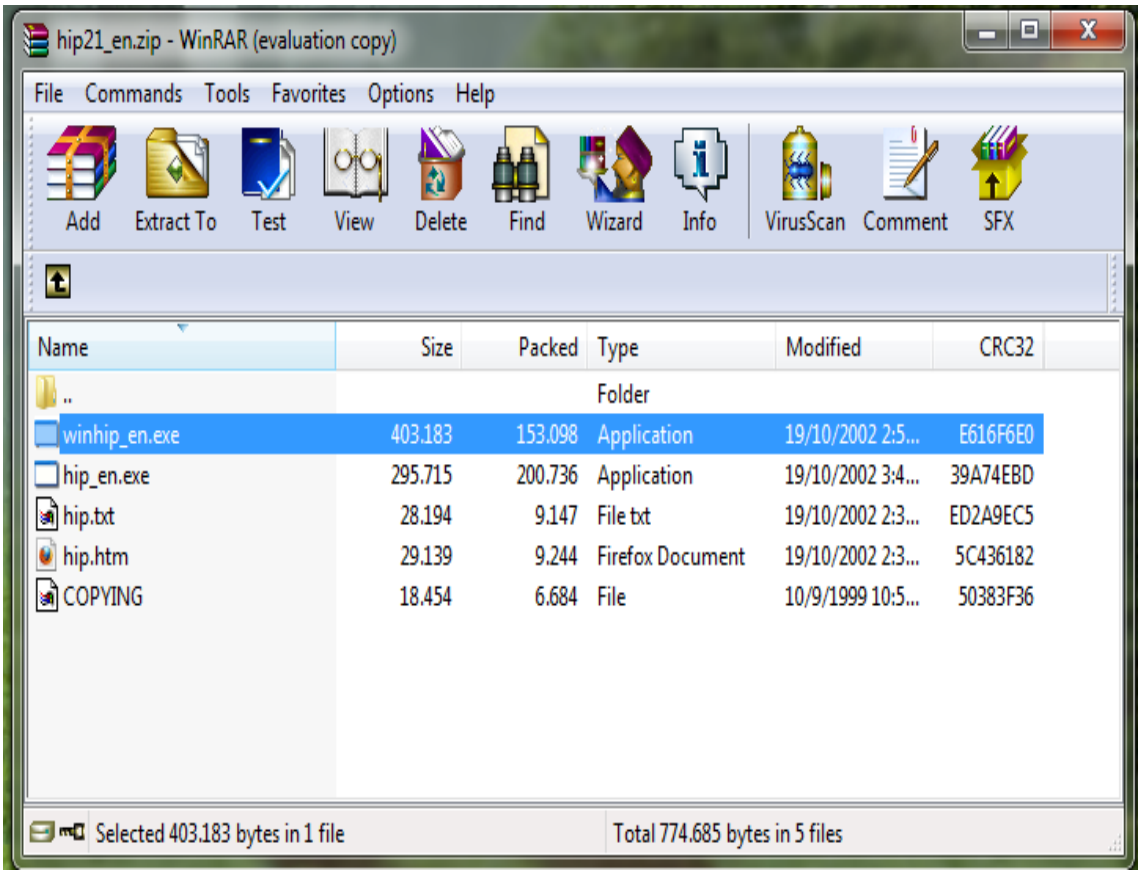


Εικόνα 55: wbStego4 (16/16)

7.5 HIP 2.1

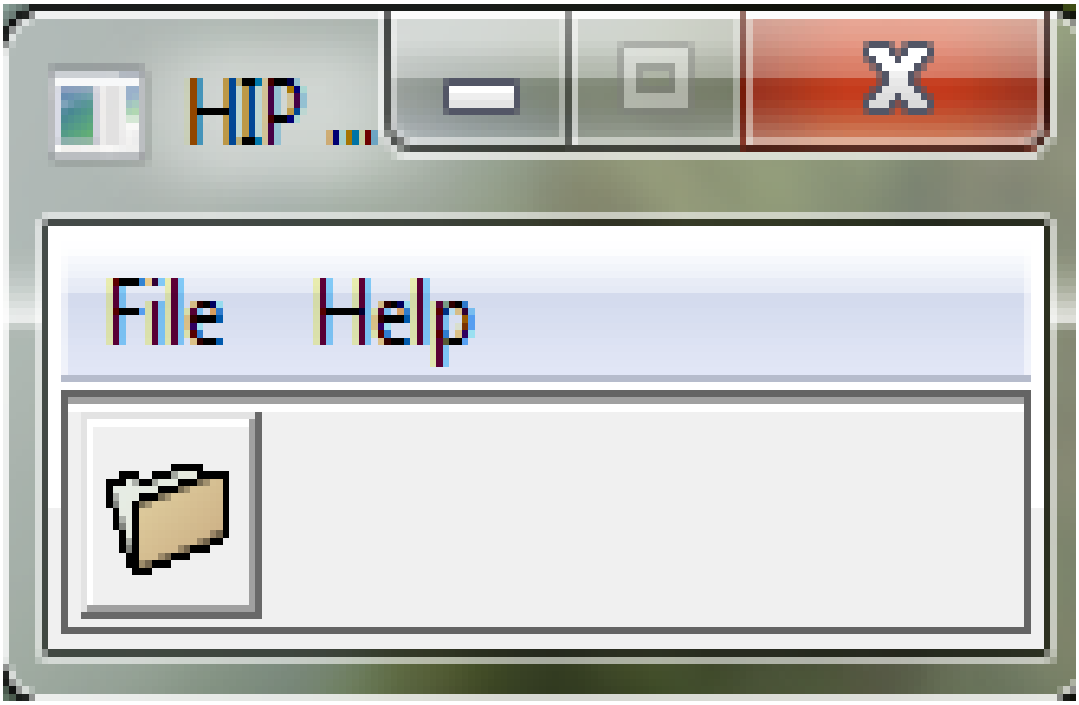
Ακόμα ένα πρόγραμμα στεγανογραφίας είναι το HIP 2.1 το οποίο μπορείτε να το κατεβάσετε από το http://sourceforge.net/projects/hide-in-picture/files/hide-in-picture/2.1/hip21_en.zip/download (Είναι freeware) και αποθήκευσε το σε ένα μέρος στο δίσκο. Αυτό το πρόγραμμα μπορεί να διαβαστεί και να γράψει μόνο με εικόνες με κατάληξη .gif.

Για να ανοίξουμε το πρόγραμμα, αποσυμπιέζουμε το αρχείο και πηγαίνουμε στο winhip_en.exe.

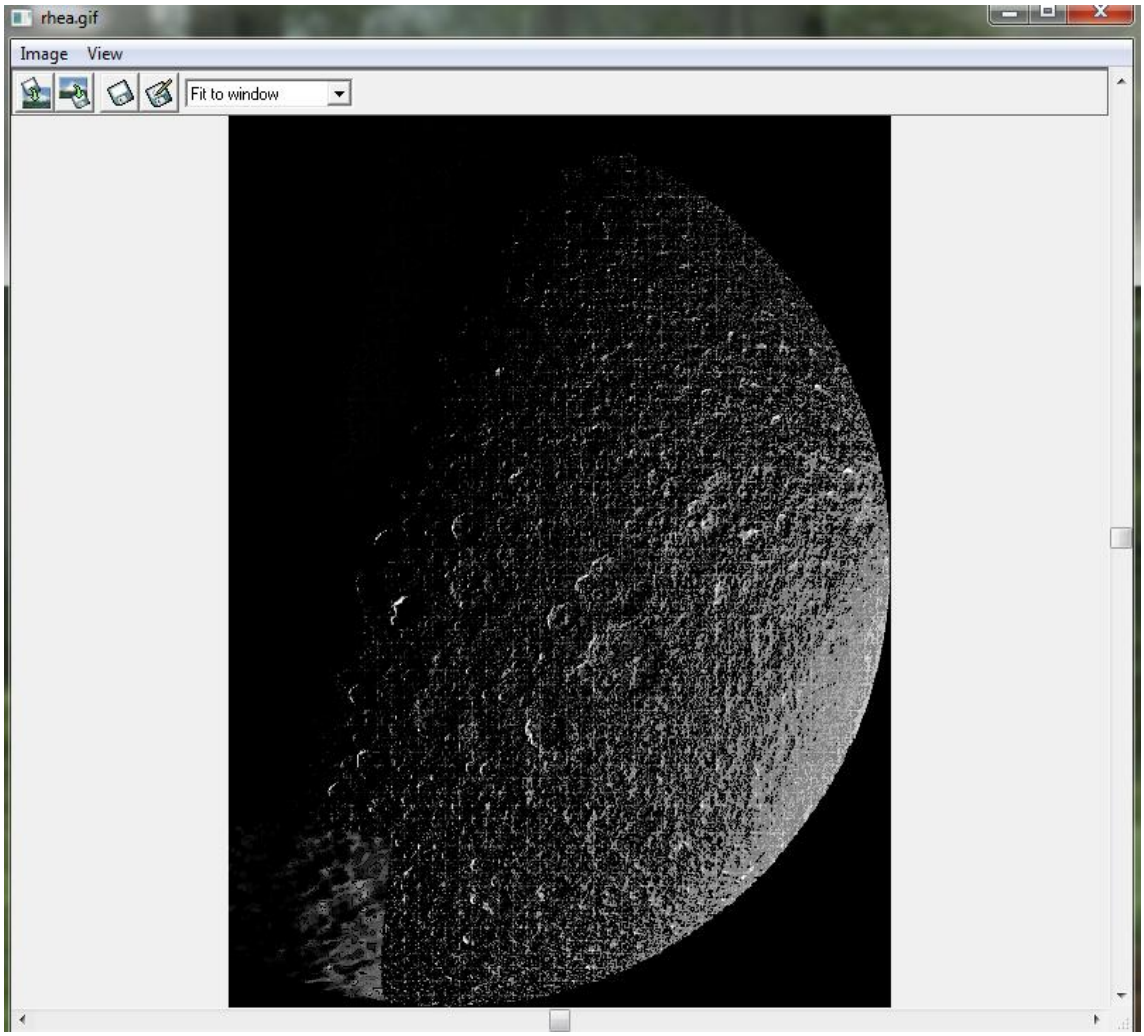


Εικόνα 56: Το πρόγραμμα

Επιλέξετε μια εικόνα με κατάληξη .gif για μεταφορέα, πηγαίνοντας από το μενού File ή από το εικονίδιο.

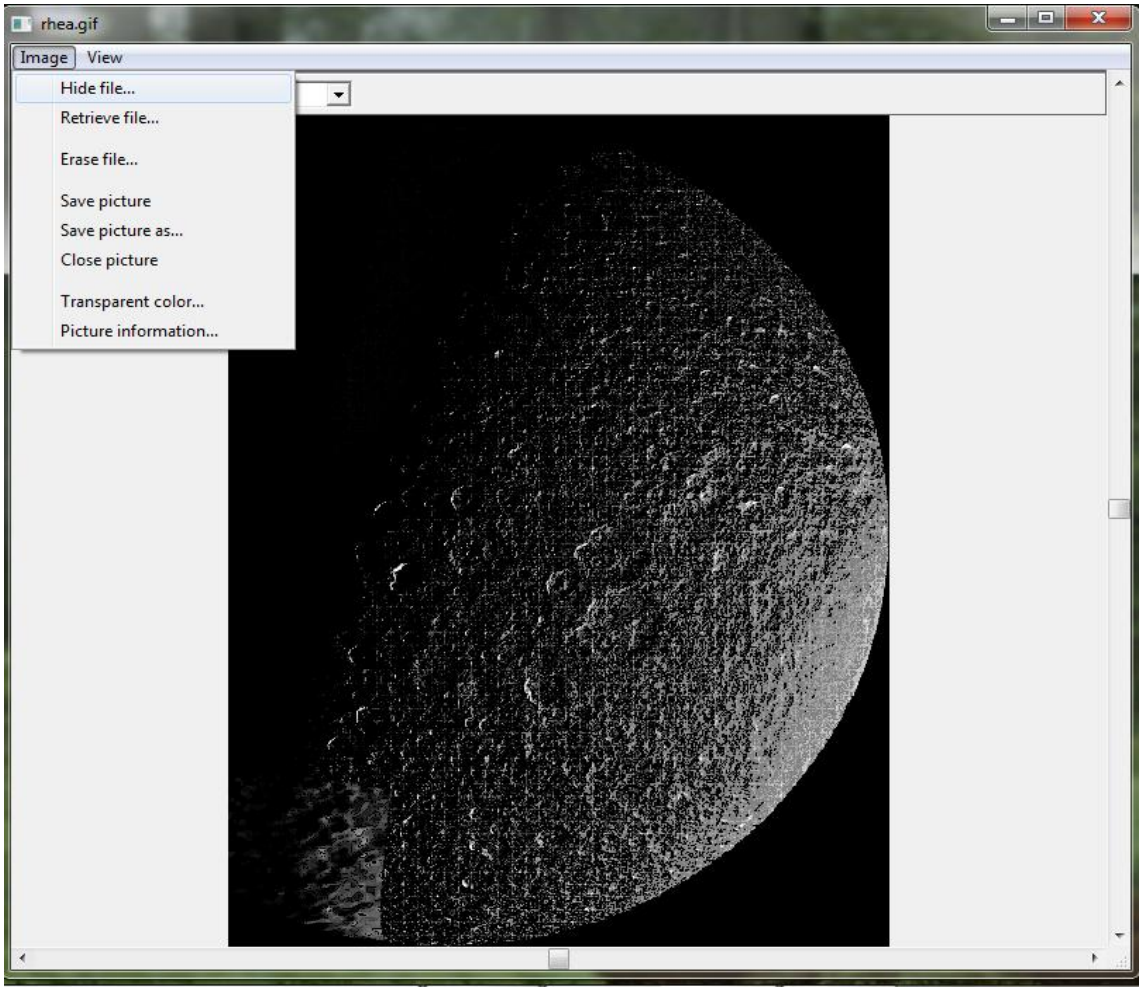


Εικόνα 57: HIP 2.1



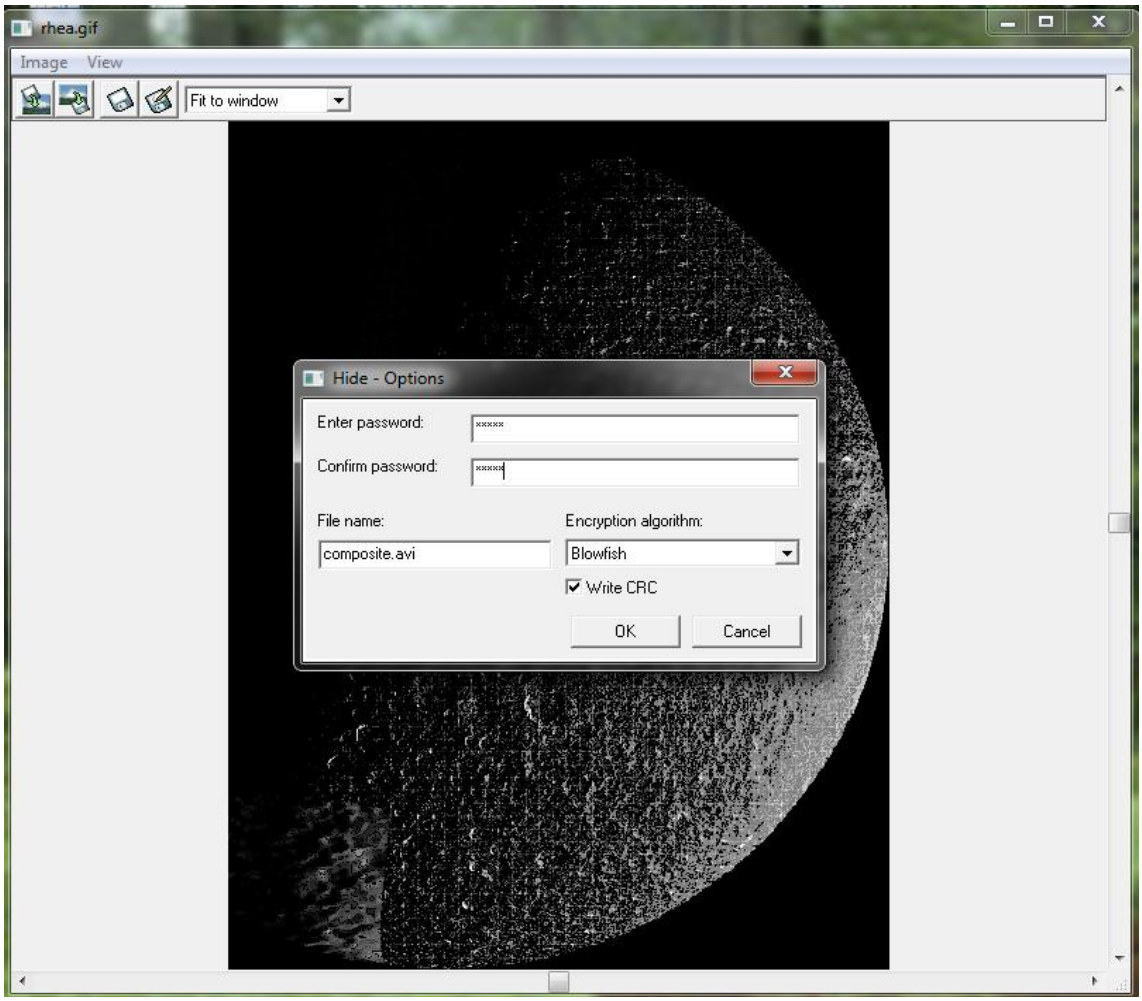
Εικόνα 58: Μια εικόνα με .gif

Για να αποκρύψετε ένα αρχείο που επιθυμείτε, επιλέξετε από το μενού image → Hide file.



Εικόνα 59: Hide file

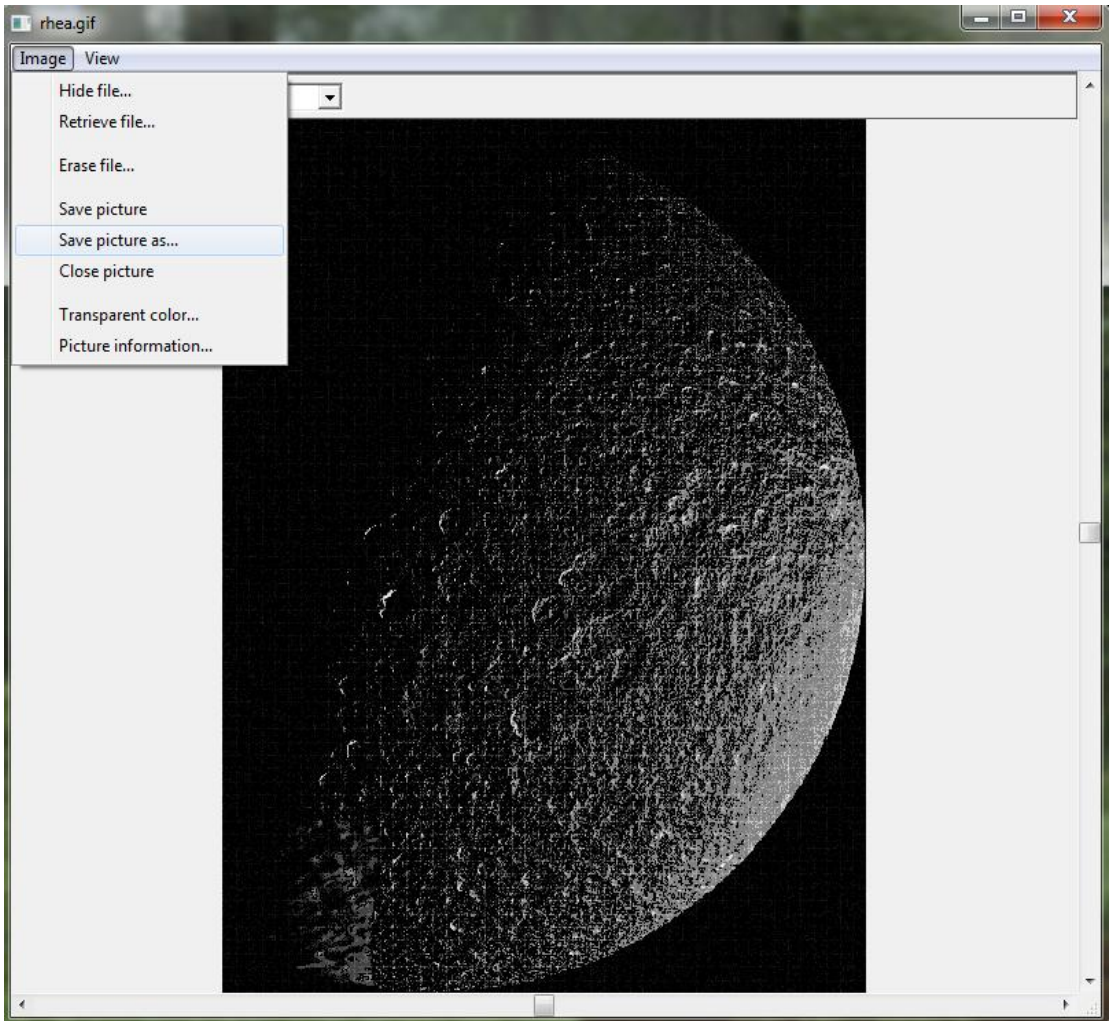
Εδώ το συγκεκριμένο παράδειγμα το αρχείο απόκρυψη είναι ένα βίντεο με κατάληξη .avi. Πληκτρολογήσετε το κωδικό, έπειτα πατήσετε οκ.



Εικόνα 60: password

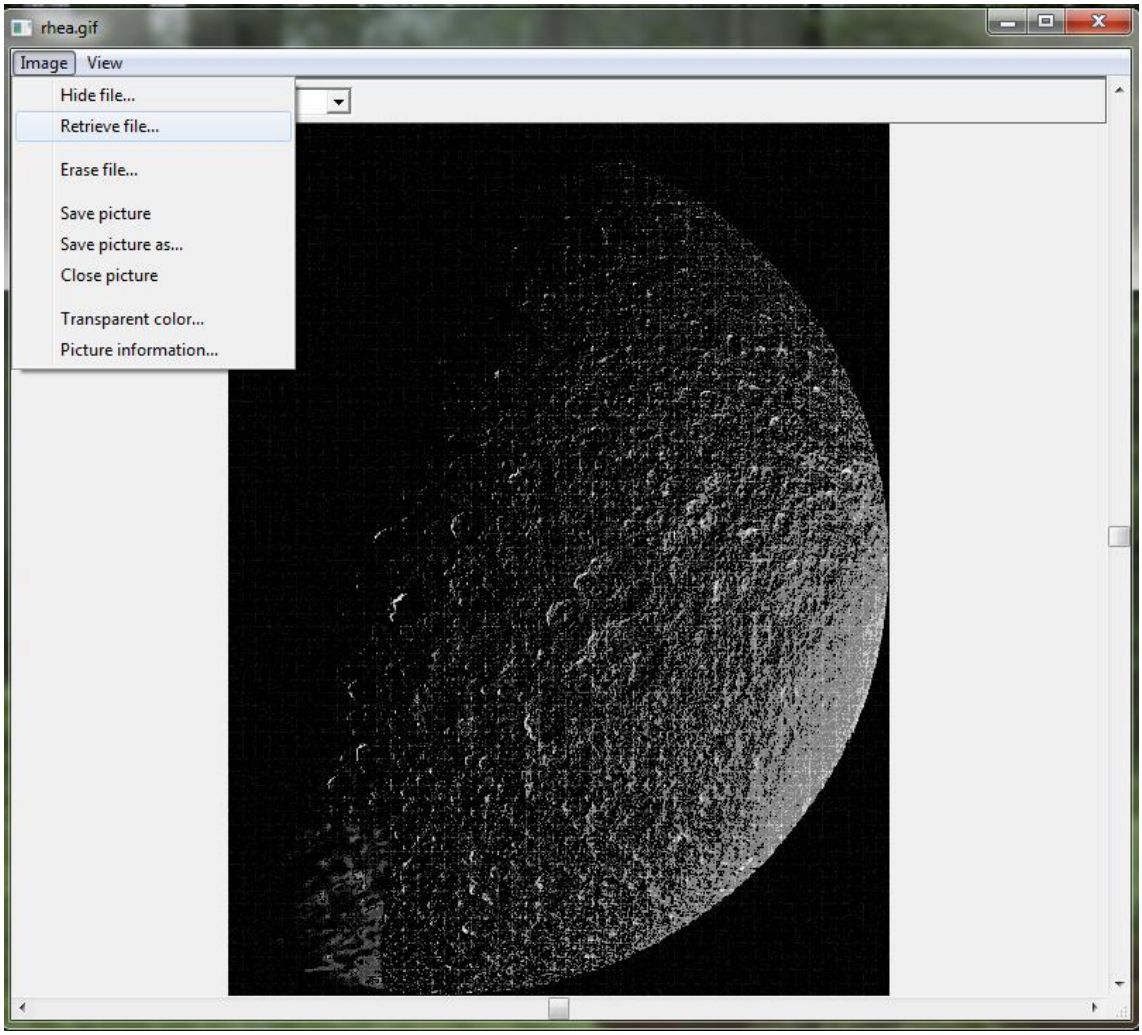
Σημείωση: το αρχείο απόκρυψη δεν μπορεί να είναι μεγαλύτερο από το αρχείο μεταφορέα, πρέπει να είναι μικρότερο.

Πρέπει να αποθηκεύσετε (π.χ. στην επιφάνεια εργασία) την κρυπτογραφημένη εικόνα επιλέξετε από το μενού image→ Save picture as… Και η εικόνα κρυπτογραφήθηκε.



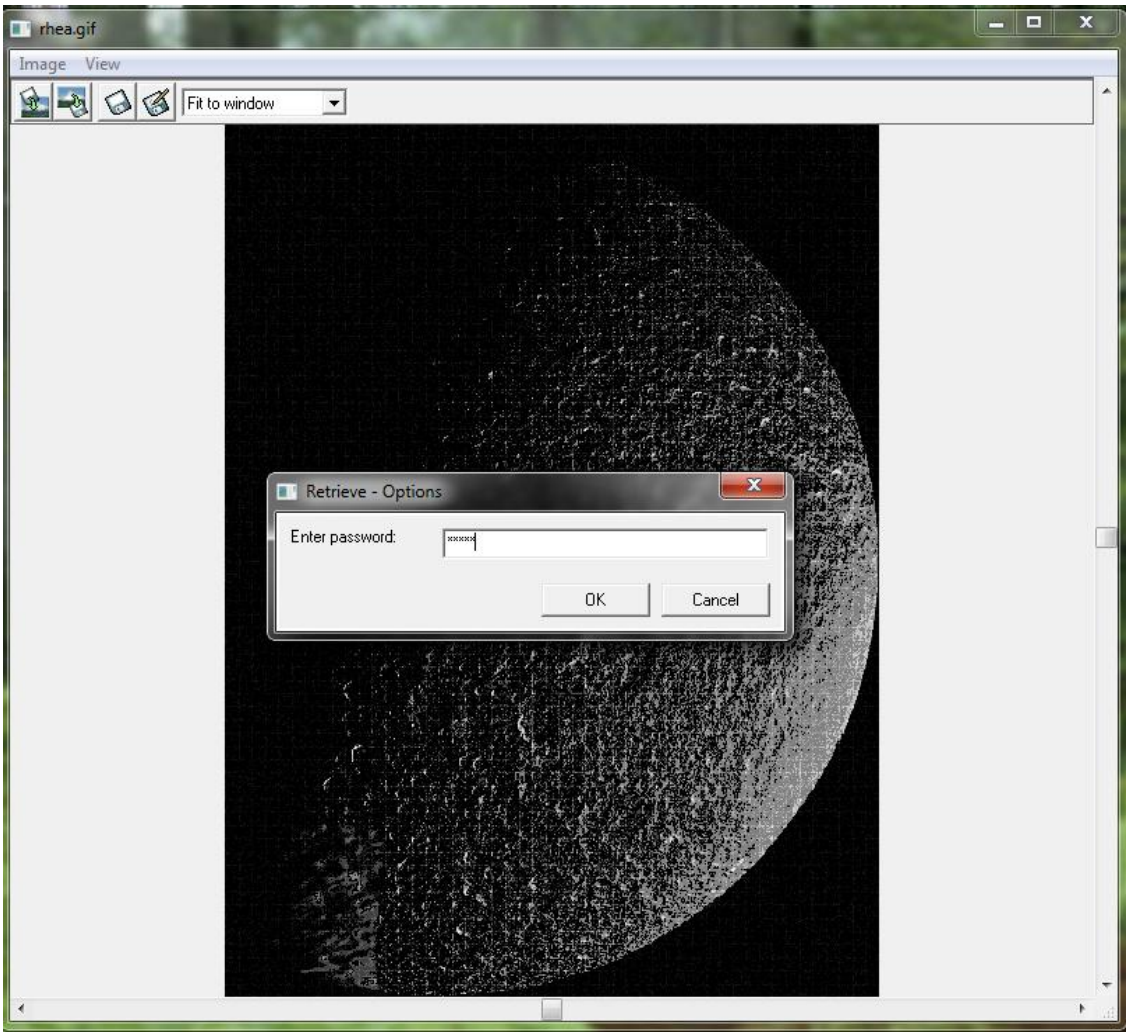
Εικόνα 61: Save picture

Για να ανακτήσετε το κρυμμένο αρχείο, επιλέξετε την κρυπτογραφημένη εικόνα που αποθηκεύσατε. Επιλέξετε από το μενού image→ Retrieve file…



Εικόνα 62: Retrieve file

Πληκτρολογήσετε τον κωδικό που δημιουργήσατε. Έπειτα αποθηκεύστε το (π.χ. στην επιφάνεια εργασία). Τέλος εμφανίζει το κρυμμένο αρχείο.



Εικόνα 63: password

Βιβλιογραφία

URL'S

Περί Στεγανογραφίας και Στεγανάλυσης:
http://somethingdigital.blogspot.com/2007/10/blog-post_24.html

DPGR Virtual Community:
http://www.dpgr.gr/forum/index.php?action=printpage;topic=8503.0

Στεγανογραφία - η τέχνη της παραπλάνησης:
http://techingreek.blogspot.com/2007/08/blog-post.html

Βασικές Έννοιες, Στεγανογραφία:
http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/steganografia.htm

Τι είναι η στεγανογραφία:
http://www.eeei.gr/interbiz/articles/steganog.htm

HOWTO Στεγανογραφία με το outguess:
http://ilug.gr/index.php?option=com_smf&Itemid=27&topic=533.0

Στεγανογραφία:
http://www.pcw.gr/forum/viewtopic.php?f=22&t=2104&start=0&st=0&sk=t&sd=a

Στεγανογραφία:
http://www.vezeris.gr/LinkClick.aspx?fileticket=Ew5JsMo9lwQ%3D&tabid=357&mid=936&language=en-US

ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΣΤΗΝ ΑΡΧΑΙΟΤΗΤΑ:
http://www.army.gr/files/File/epitheorisi/200401_%CE%95%CE%A0%CE%99%CE%9A%CE%9F%CE%99%CE%9D%CE%A9%CE%9D%CE%99%CE%95%CE%A3%20%CE%9A%CE%91%CE%99%20%CE%A4%CE%97%CE%9B%CE%95%CE%A0%CE%99%CE%9A%CE%9F%CE%99%CE%9D%CE%A9%CE%9D%CE%99%CE%95%CE%A3%20%CE%A3%CE%A4%CE%97%CE%9D%20%CE%91%CE%A1%CE%A7%CE%91%CE%99%CE%9F%CE%A4%CE%97%CE%A4%CE%91.pdf

Steganography:
http://www.worldlingo.com/ma/enwiki/el/Steganography

Στεγανογραφία, ψηφιακό υδατογράφημα και copyright στη φωτογραφία:
http://www.photomind.gr/forum/showthread.php?t=1256

S-Tools:
http://www.kgk.gr/2006/01/09/steganography/

http://linux01.gwdg.de/alatham/stego.html

Our Secret 2.0:
www.securekit.net

Xiao Steganography:
http://download.cnet.com/Xiao-Steganography/3000-2092_4-10541494.html

HIP 2.1:
http://sourceforge.net/projects/hide-in-picture/files/hide-in-picture/2.1/hip21_en.zip/download

StegoArchive.Com:
http://members.cox.net/ebmmd/stego/stego.html

QuickStudy: Steganography: Hidden Data:
http://www.computerworld.com/s/article/71726/Steganography_Hidden_Data

Steganography Tools:
http://www.cotse.com/tools/stega.htm

Information Hiding: Steganography & Digital Watermarking:
http://www.jjtc.com/Steganography/

Steganography - JPHS (JPHide and JPSeek):
http://xmonsterhunter.blogspot.com/2009/10/steganography-jphs-jphide-and-jpseek.html