ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Αναστρέψιμη απόκρυψη δεδομένων σε συμπιεσμένες εικόνες (Reversible data hiding in compressed images)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Γέροντα Αλέξανδρου

Επιβλέπων : Καρύμπαλη Ειρήνη

Μέλη εξεταστικής επιτροπής: Καλλίγερος Εμμανουήλ, Κωνσταντίνου Ελισάβετ

Σάμος, Μάρτιος 2021

Πρόλογος και ευχαριστίες

Η εκπόνηση της παρούσας προπτυχιακής εργασίας πραγματοποιήθηκε κατά το ακαδημαϊκό έτος 2020-2021 στο πλαίσιο ολοκλήρωσης των προπτυχιακών σπουδών, του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων στο Πανεπιστήμιο Αιγαίου.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω την καθηγήτρια Καρύμπαλη Ειρήνη για την επίβλεψη, την πολύτιμη βοήθεια και την καθοδήγηση που μου παρείχε κατά την διάρκεια συγγραφής της παρούσας εργασίας.

Γέροντα Αλέξανδρου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πίνακας Περιεχομένων

Περίληψη

Οι τεχνικές αναστρέψιμης απόκρυψης πληροφορίας εισάγουν στην εικόνα δεδομένα τα οποία είναι αδιόρατα και τα οποία μπορούν να εξαχθούν πλήρως, επιτρέποντας την πλήρη ανακατασκευή των αρχικών εικόνων. Η ιδιότητα της αναστρεψιμότητας των δεδομένων είναι ιδιαίτερα επιθυμητή, όταν υπάρχουν απαιτήσεις διατήρησης της πιστότητας των αρχικών δεδομένων, όπως για παράδειγμα στην επεξεργασία ιατρικών ή στρατιωτικών εικόνων.

Οι περισσότερες τεχνικές έχουν σχεδιαστεί για ασυμπίεστες εικόνες και στη γενική περίπτωση δεν μπορούν να εφαρμοστούν άμεσα σε συμπιεσμένες εικόνες (π.χ. JPEG). Η αναστρέψιμη απόκρυψη δεδομένων σε συμπιεσμένες εικόνες είναι σαφώς πιο δύσκολη, διότι υπάρχει λιγότερος πλεονασμός πληροφορίας (information redundancy) σε σχέση με τις ασυμπίεστες εικόνες και κάθε τροποποίηση επιφέρει επιπλέον αλλοιώσεις στην εικόνα.

Στα πλαίσια της συγκεκριμένης διπλωματικής εργασίας, μελετήθηκαν, υλοποιήθηκαν και αποτιμήθηκαν τεχνικές αναστρέψιμης απόκρυψης δεδομένων σε συμπιεσμένες εικόνες.

Κεφάλαιο 1: Απόκρυψη πληροφορίας

Η μετάδοση πληροφορίας μέσω του διαδικτύου έχει γίνει πολύ συχνή στις μέρες μας, λόγω της εύκολης και γρήγορης πρόσβασης της. Τεχνικές ασφαλούς επικοινωνίας είναι απαραίτητες έτσι ώστε να εξασφαλιστεί η ασφαλής μετάδοση της πληροφορίας. Η κρυπτογραφία και η απόκρυψη πληροφορίας είναι οι δύο κύριες μέθοδοι για ασφαλή επικοινωνία. Στη κρυπτογραφία το αρχικό μήνυμα μετατρέπεται σε ένα νέο ακατανόητο μήνυμα, το οποίο μπορεί να διαβαστεί μόνο αν είναι διαθέσιμο το κατάλληλο κλειδί αποκρυπτογράφησης. Στην απόκρυψη πληροφορίας γίνεται ένθεση ενός μηνύματος σε ένα ψηφιακό αρχείο, με τέτοιο τρόπο που να μην γίνεται αντιληπτή η ύπαρξή του.

Σχήμα 1.1 Η εικόνα Lena πριν και μετά την εισαγωγή 20000 bit μηνύματος

Η υδατογράφηση, η στεγανογραφία και η αναστρέψιμη απόκρυψη πληροφορίας είναι οι κύριες κατηγορίες απόκρυψης πληροφορίας. Στην υδατογράφηση γίνεται προσθήκη πληροφορίας σε ένα αρχείο για την πιστοποίηση της ακεραιότητας και της προέλευσης του ή για την προστασία των πνευματικών δικαιωμάτων του δημιουργού του. Η στεγανογραφία χρησιμοποιείται για κρυφή μετάδοση μηνύματος. Το αρχείο χρησιμοποιείται μόνο για την μετάδοση του μηνύματος και μετά από την εξαγωγή της πληροφορίας από τον παραλήπτη δεν έχει αξία. Αφού έχουμε εισάγει το μήνυμα σε ένα μέσο τότε το έχουμε παραμορφώσει και ο παραλήπτης δεν θα μπορέσει να το επαναφέρει ακόμα και αν έχει εξάγει το μήνυμα. Στην αναστρέψιμη απόκρυψη πληροφορίας εκτός από την πληροφορία που είναι κρυμμένη είναι σημαντικό και το μέσο. Μετά την εξαγωγή της πληροφορίας θα πρέπει να είναι δυνατή η επαναφορά του αρχείου στην μορφή που ήταν πριν την εισαγωγή του κρυφού μηνύματος.

Κατά την ένθεση, γίνεται εισαγωγή του μηνύματος σε ένα ψηφιακό αρχείο, και αυτό μπορεί να ανακτηθεί μόνο από εξουσιοδοτημένους χρήστες. Μετά την ανάκτηση του μηνύματος το αρχείο επανέρχεται στην αρχική του κατάσταση, χωρίς να υπάρξει κάποιου τύπου αλλοίωση.

Σε περίπτωση που το μήνυμα δεν μπορεί να ανακτηθεί ή το αρχείο δεν επαναφέρεται στην αρχική του κατάσταση, θεωρείται ότι έχει υπάρξει κάποιου τύπου επίθεση. Μια επίθεση δεν είναι απαραίτητα κακόβουλη. Επίθεση είναι και η συμπίεση που μπορεί να γίνει σε μία εικόνα. Οι επιθέσεις πρέπει να λαμβάνονται υπόψη στον σχεδιασμό των τεχνικών απόκρυψης πληροφορίας, ώστε αυτές να είναι ανθεκτικές σε επιθέσεις.

Γενικά, οι τεχνικές απόκρυψης πληροφορίας θα πρέπει να έχουν τα ακόλουθα χαρακτηριστικά [1] :

- Το μήνυμα δεν θα πρέπει να είναι αντιληπτό και μόνο εξουσιοδοτημένοι χρήστες θα μπορούν να το ανακτήσουν.
- Οι τεχνικές πρέπει να είναι ανθεκτικές σε επιθέσεις. Ακόμα και αν κάποιος τρίτος καταλάβει ότι σε κάποιο αρχείο υπάρχει κρυμμένο μήνυμα, δεν θα μπορεί να το εξάγει, χωρίς το κατάλληλο κλειδί.
- Πρέπει να υπάρχει η δυνατότητα ένθεσης μεγάλου μήκους μηνύματος. Σε μερικές εφαρμογές είναι σημαντικό το μέσο να συνοδεύεται από μεγάλο όγκο πληροφορίας.
- Οι τεχνικές πρέπει να είναι ανθεκτικές σε μεταβολές του μέσου, όπως αυτές που επιφέρουν π.χ. οι αλγόριθμοι συμπίεσης σε εικόνες ή η επαναδειγματοληψία σε αρχεία ήχου, όπου χάνεται ένα μέρος της πληροφορίας. Το μήνυμα πρέπει να είναι ανακτήσιμο ακόμα και μετά από τέτοιες μεταβολές.
- Ο αλγόριθμος εισαγωγής του μηνύματος να είναι αποδοτικός.

Σε αυτή τη διπλωματική θα γίνει περιγραφή τεχνικών αναστρέψιμης απόκρυψης πληροφορίας (reversible data hiding) σε συμπιεσμένες εικόνες, της διαδικασίας συμπίεσης μιας εικόνας σε αρχείο JPEG και της υλοποίηση δύο τεχνικών RDH σε συμπιεσμένες εικόνες.

Η αναστρέψιμη απόκρυψη πληροφορίας σε εικόνες χρησιμοποιείται όταν πρέπει να είναι δυνατή η ανάκτηση της αρχικής εικόνας. Όταν η απόκρυψη πληροφορίας γίνεται για ιατρική διάγνωση ή για την επιβολή του νόμου είναι σημαντικό να μπορεί να ανακτηθεί το αρχικό μέσο για νομικούς λόγους [2]. Σε εικόνες τηλεπισκόπησης και σε στρατιωτικές εικόνες απαιτείται υψηλή ακρίβεια. Επίσης σε πολλές επιστημονικές έρευνες τα αποτελέσματα πειραμάτων απαιτούν υψηλό κόστος για να επιτευχθούν. Τεχνικές αναστρέψιμης απόκρυψης πληροφορίας οι οποίες χρησιμοποιούν σαν μέσο εικόνες θα αναλυθούν σε επόμενα κεφάλαια.

Μέθοδοι απόκρυψης και κρυπτογράφησης πληροφορίας πριν τους υπολογιστές

Η ασφαλής μετάδοση πληροφορίας έχει ξεκινήσει από τα αρχαία χρόνια δηλαδή πολύ πριν τους ηλεκτρονικούς υπολογιστές. Καθώς ο μόνος τρόπος επικοινωνίας ήταν με φυσικά μέσα

έπρεπε να διασφαλιστεί η ασφάλεια του μηνύματος δηλαδή να μπορεί να διαβαστεί μόνο από τον παραλήπτη και να είναι άχρηστη σε οποιονδήποτε τρίτο. Ο αποστολέας είχε δύο τρόπους να το κάνει αυτό: μπορούσε να κρυπτογραφήσει ή να το αποκρύψει το μήνυμα μέσα σε ένα μέσο με τεχνικές στεγανογραφίας οι οποίες ήταν και οι πρώτες τεχνικές απόκρυψης μηνύματος που αναπτύχθηκαν.

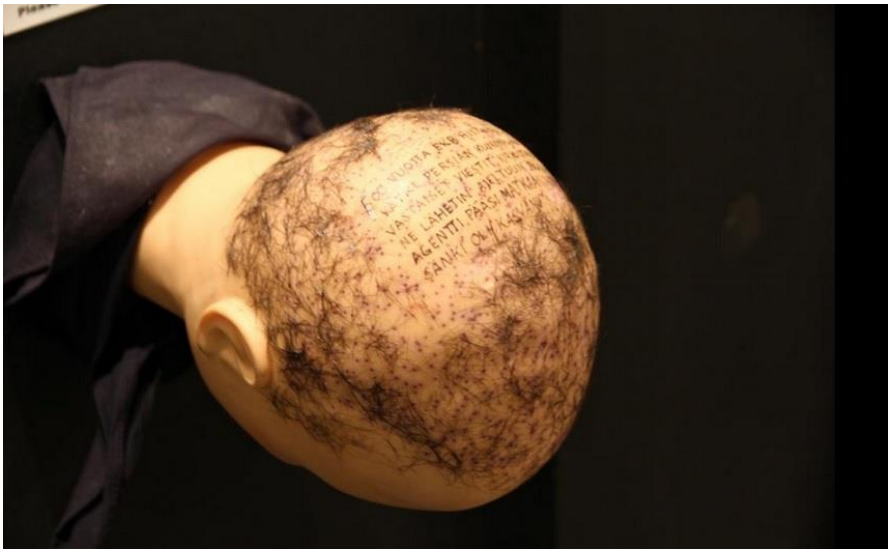
Παραδείγματα κρυπτογραφίας

Ο Ιούλιος Καίσαρας (100 – 44 π.Χ) είχε την δική του τεχνική κρυπτογράφησης γνωστή ως ‘’κώδικας του Καίσαρα‘’ [3] την οποία χρησιμοποιούσε για να επικοινωνήσει με τους φίλους του, καθώς επίσης υλοποίησε και άλλα συστήματα κρυπτογράφησης τα οποία ανέλυσε στο βιβλίο του ‘Valerius Probus’ το οποίο αν και δεν έχει διασωθεί θεωρείται το πρώτο βιβλίο κρυπτογραφίας.

Οι αρχαίοι Σπαρτιάτες για τις στρατιωτικές αποστολές τους, έγραφαν τα κρυπτογραφημένα μηνύματα τους σε μία ταινία τυλιγμένη σε μια σκυτάλη [4], όπου για να διαβάσει κάποιος το μήνυμα έπρεπε να έχει την ίδια ακριβώς σκυτάλη με τον αποστολέα.

Παραδείγματα στεγανογραφίας

Ο τύραννος Ιστιαίος [5] ξύριζε τα κεφάλια των δούλων του και έκανε τατουάζ το μήνυμα στο κεφάλι. Όταν μεγάλωναν τα μαλλιά του δούλου, τον έστελνε να παραδώσει το μήνυμα, όπου ο παραλήπτης έπρεπε να τον ξυρίσει ξανά για να το διαβάσει. Ένας στρατιώτης για να στείλει στη Σπάρτη ένα μήνυμα που έλεγε πως ο Ξέρξης πρόκειται να εισβάλει στην Ελλάδα, αφαίρεσε το κερί από έναν ξύλινο πίνακα και έγραψε πάνω το μήνυμα. Μπόρεσε και έστειλε τον πίνακα στην Σπάρτη χωρίς να γίνει αντιληπτό το μήνυμα από τους Πέρσες καθώς τον κάλυψε ξανά με κερί πριν την αποστολή.



Σχήμα 1.2 Τατουάζ μηνύματος σε κεφάλι σκλάβου

Άλλα παραδείγματα στεγανογραφημένων μηνυμάτων σε φυσικά μέσα ήταν μηνύματα τα οποία είχαν λέξεις ή γράμματα γραμμένα διαφορετικά από το υπόλοιπο κείμενο, μηνύματα με μικρό-τελείες [6] οι οποίες εισάγονταν πάνω στο χαρτί με ειδική 'κάμερα' μικρό-τελειών ή επιστολές με κρυμμένο μήνυμα κάτω από το γραμματόσημο.

Διαφορές της απόκρυψης πληροφορίας από την κρυπτογραφία

Η κρυπτογραφία είναι μία διαδικασία η οποία μετασχηματίζει το περιεχόμενο ενός μηνύματος και παράγει ένα κρυπτό-κείμενο. Δεν γίνεται απόκρυψη του κρυπτό-κειμένου στο μέσο, το κάνει όμως αδύνατο να διαβαστεί. Για την κρυπτογράφηση ενός κειμένου απαιτείται ένας αλγόριθμος και ένα κλειδί κρυπτογράφησης. Για να γίνει επαναφορά του αρχικού κειμένου από το κρυπτό-κείμενο, πρέπει να μας είναι γνωστή η μέθοδος με την οποία έγινε κρυπτογράφηση του μηνύματος, και το κλειδί αποκρυπτογράφησης. Εκτός από ασφαλή επικοινωνία με την κρυπτογραφία μπορούμε επίσης να πιστοποιήσουμε την ταυτότητα του αποστολέα του μηνύματος.

Η απόκρυψη πληροφορίας έχει τον ίδιο σκοπό με την κρυπτογραφία δηλαδή να αποκρύψει την πληροφορία από ανεπιθύμητα άτομα έτσι ώστε μόνο ο παραλήπτης να μπορεί να την εξάγει. Σε αντίθεση όμως με την κρυπτογραφία όπου κάποιος μπορεί να καταλάβει πως το κείμενο που βλέπει είναι κρυπτογραφημένο, η απόκρυψη πληροφορίας μας δίνει την δυνατότητα να κρύψουμε την πληροφορία με τέτοιο τρόπο έτσι ώστε να μην είναι αντιληπτό σε κάποιον τρίτο ότι στο μέσο είναι κρυμμένη πληροφορία. Είναι επίσης και το μεγαλύτερο μειονέκτημα της, καθώς αν κάποιος καταλάβει πως στο μέσο υπάρχει κάποιο κρυμμένο μήνυμα, είναι πιθανό να μπορέσει να το εξάγει. Μπορεί βέβαια να γίνει ένας συνδυασμός των δύο δηλαδή πρώτα να κρυπτογραφήσουμε το μήνυμα και μετά να γίνει απόκρυψη του στο μέσο. Οπότε ακόμα και αν αποκαλυφθεί πως στο μέσο υπάρχει κρυμμένη πληροφορία θα πρέπει να γίνει αποκρυπτογράφηση της για να μπορεί να διαβαστεί.

Στις μέρες μας οι τεχνικές κρυπτογραφίας και απόκρυψης πληροφορίας χρησιμοποιούνται κυρίως στους υπολογιστές. Η κρυπτογραφία μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση χρηστών σε ηλεκτρονικές σελίδες, για την κρυπτογράφηση αρχείων ή για την προστασία λογισμικού από πειρατεία ενώ η απόκρυψη πληροφορίας χρησιμοποιείται για την ασφαλή επικοινωνία μεταξύ οντοτήτων, την ασφαλή αποθήκευση πληροφοριών σε ένα μέσο και για την πιστοποίηση της ιδιοκτησίας ηλεκτρονικών αρχείων.

Ψηφιακά μέσα απόκρυψης πληροφορίας

Οι σύγχρονες τεχνικές απόκρυψης πληροφορίας αφορούν ψηφιακά αρχεία όπως αρχεία κειμένου, ήχου, εικόνας και βίντεο. Οι πιο διάσημες τεχνικές αφορούν την ένθεση μηνύματος σε εικόνες. Παρακάτω γίνεται περιγραφή μερικών τεχνικών που εφαρμόζονται σε αυτά τα αρχεία.

Αρχεία εικόνας

Στα αρχεία εικόνας οι τεχνικές απόκρυψης πληροφορίας αφορούν συμπιεσμένες και ασυμπίεστες εικόνες [7]. Στις ασυμπίεστες εικόνες η πληροφορία εισάγεται μεταβάλλοντας τις τιμές έντασης στα pixel της εικόνας ή αλλάζοντας το λιγότερο σημαντικό bit της διαφοράς τιμών έντασης μεταξύ γειτονικών pixel. Για τις συμπιεσμένες εικόνες η πληροφορία εισάγεται σε κάποιο στάδιο συμπίεσης, συνήθως μετά από μετασχηματισμό DCT. Η διαδικασία συμπίεσης και τεχνικές RDH που αφορούν εικόνες θα εξηγηθούν περισσότερο σε επόμενα κεφάλαια.

Αρχεία ήχου

Στην απόκρυψη πληροφορίας σε αρχεία ήχου, η πληροφορία μπορεί να ενσωματωθεί στο σήμα ήχου [8]. Είναι σημαντικό η ποιότητα του ήχου να μην αλλοιωθεί και το μήνυμα να μην μπορεί να αφαιρεθεί από μεταβολές στο αρχείο ήχου όπως η επαναδειγματοληψία. Μερικές τεχνικές υδατογράφησης σε αρχεία ήχου, εισάγουν πληροφορία προσθέτοντας ηχώ στο διακριτό σήμα. Από το αρχικό σήμα παράγουμε ένα σήμα ηχώς. Στη συνέχεια στο σήμα της ηχώς μεταβάλλονται το πλάτος του σήματος, η καθυστέρηση και ο ρυθμός αποσύνθεσης. Για διαφορά ενός χιλιοστού του δευτερολέπτου μεταξύ του αρχικού σήματος και του σήματος ηχώς δεν πρόκειται να παρατηρηθεί καμία διαφορά στην ποιότητα του ήχου.

Αρχεία βίντεο

Σε αρχεία βίντεο [9] το μπορούμε να κάνουμε ένθεση πληροφορίας σε κάθε καρέ του. Σε μερικά pixel από το κάθε καρέ γίνεται αντικατάσταση του λιγότερο σημαντικού bit τους με ένα

bit πληροφορίας. Επίσης γίνεται να αφαιρεθεί πληροφορία χρώματος χωρίς μεγάλη διαφορά στην ποιότητα και να αντικατασταθεί με πληροφορία μηνύματος.

Ακόμα καθώς τα αρχεία βίντεο είναι ένας συνδυασμός αρχείων εικόνας και ήχου οι τεχνικές που αναφέρθηκαν για αρχεία εικόνας και ήχου μπορούν να χρησιμοποιηθούν και σε αρχεία βίντεο. Το μεγαλύτερο πλεονέκτημα σε αρχεία βίντεο είναι πως καθώς γίνεται γρήγορη εναλλαγή εικόνων και ήχου οπότε κάποιος που το βλέπει δύσκολα θα παρατηρήσει αλλοιώσεις σε αυτό.

Αρχεία κειμένου

Στα αρχεία κειμένου μπορούμε να εισάγουμε ένα μήνυμα χρησιμοποιώντας χαρακτήρες εκτός του πίνακα ascii οι οποίοι να μην φαίνονται διαφορετικοί από τους υπόλοιπους χαρακτήρες ή να γράψουμε το κρυφό μήνυμα σε χρώμα ίδιο με το χρώμα της σελίδας. Επίσης bit μηνύματος μπορούν να εισαχθούν σε ένα κείμενο αλλάζοντας το συνταχτικό του δηλαδή με την εισαγωγή παραπάνω κενών ή τελειών, με παράλειψη κόμματος ανάμεσα σε φράσεις και με την εισαγωγή του χαρακτήρα tab στο τέλος προτάσεων. Για παράδειγμα ένα παραπάνω κενό ανάμεσα σε δύο λέξεις μπορεί να συμβολίζει το bit 0 ενώ δύο παραπάνω κενά το bit 1.

Αν για την σύνταξη του κειμένου χρησιμοποιείται κάποιο συγκεκριμένο πρόγραμμα όπως το Microsoft Word μπορούμε να αξιοποιήσουμε κάποιο χαρακτηριστικό τους όπως την συγγραφή κειμένου από πολλούς συγγραφείς και την παρακολούθηση αλλαγών [10]. Αρχικά σε ένα κείμενο Τ εισάγουμε ένα κρυφό μήνυμα παράγοντας ένα κείμενο Τ’. Στη συνέχεια σβήνουμε το μήνυμα από το κείμενο Τ΄ και παράγουμε το κρυπτό-κείμενο S. Στο Word αυτό θα φαίνεται σαν ένας συγγραφέας να διορθώνει το κείμενο που έγραψε και μπορούμε να εξάγουμε το μήνυμα αναιρώντας τις αλλαγές που έγιναν στο κρυπτό-κείμενο S.

Τέλος σε οποιοδήποτε αρχείο ανεξαρτήτως του τύπου του μπορούμε να εισάγουμε πληροφορία σε τμήματα του που δεν είναι μέρος των περιεχομένων του αρχείου όπως στο τέλος του αρχείου (EOF).

Κεφάλαιο 2: Συμπίεση εικόνας

Οι εικόνες σε ασυμπίεστη μορφή είναι αρχεία τα οποία καταλαμβάνουν αρκετό χώρο σε μία συσκευή και για τη φόρτωση τους σε μια σελίδα στο διαδίκτυο σε χρήστες με αργή σύνδεση, απαιτείται συνήθως αρκετός χρόνος. Παράδειγμα ασυμπίεστης εικόνας είναι ένα αρχείο bmp.

Σχήμα 2.1 Η εικόνα Lena με διαστάσεις 512x512 αποθηκευμένη ως bmp αρχείο. Χώρος στον δίσκο: 257KB

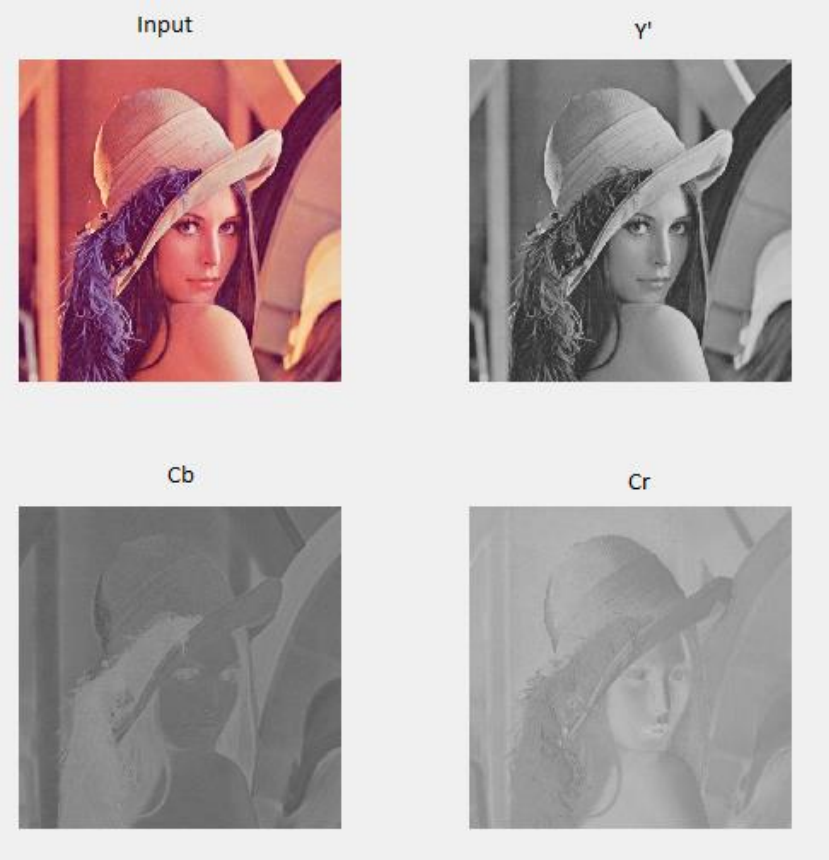
Μία λύση σε αυτό το πρόβλημα είναι να τις συμπιέσουμε και κάθε φορά που ο χρήστης θέλει να δει την εικόνα να γίνεται αποσυμπίεση εκείνη την στιγμή, όπως οι εικόνες PNG. Για παράδειγμα, αν αποθηκεύσουμε την εικόνα της Lena η οποία απεικονίζεται στο Σχήμα 2.1, σε αρχείο PNG, το μέγεθος της στον δίσκο θα ήταν 131 KB, ενώ αν την είχαμε αποθηκεύσει ως bmp θα ήτανε 257KB.

Το PNG είναι ένας τύπος αρχείου που υποστηρίζει συμπίεση χωρίς απώλειες (lossless compression). Ωστόσο, λόγω του τρόπου λειτουργίας του ανθρώπινου συστήματος όρασης (human visual system- HVS), του τρόπου δηλαδή με τον οποίο οι άνθρωποι αντιλαμβάνονται αλλαγές στην πληροφορία μιας εικόνας, μπορεί να επιτευχθεί μεγαλύτερη συμπίεση. Το μάτι μας δεν είναι ιδιαίτερα ευαίσθητο σε αλλαγές που αφορούν το χρώμα ή σε αλλαγές που προκύπτουν από την τροποποίηση των υψηλών συχνοτήτων της εικόνας. Άρα η πληροφορία που δεν γίνεται αντιληπτή μπορεί να αφαιρεθεί. Τότε, μιλάμε για συμπίεση με απώλειες (lossy compression).

Η JPEG συμπίεση προσφέρει μια καλή αναλογία μεγέθους αρχείου και ποιότητας εικόνας. Για να δημιουργήσουμε ένα αρχείο JPEG εφαρμόζουμε μεταβολή χρωματικού μοντέλου, υποδειγματοληψία στις συνιστώσες του χρώματος, μετασχηματισμό DCT, κβαντισμό, κωδικοποίηση DPCM, Huffman - διαδικασίες οι οποίες θα αναλυθούν παρακάτω.

Μεταβολή Χρωματικού Μοντέλου και υποδειγματοληψία

Οι έγχρωμες εικόνες αποτελούνται από τρεις χρωματικές συνιστώσες την κόκκινη, την πράσινη και την μπλε. Στο RGB χρωματικό μοντέλο, το χρώμα κάθε εικονοστοιχείου (pixel) προκύπτει από την ανάμειξη 3 βασικών χρωμάτων. Πριν την συμπίεση της εικόνας, γίνεται μετατροπή της από το RGB χρωματικό μοντέλο στο $Y'C_BC_R$ [11]. Σε αυτό το χρωματικό μοντέλο διαχωρίζεται η πληροφορία του χρώματος από την φωτεινότητα. Η συνιστώσα Y' αντιστοιχεί στην φωτεινότητα, ενώ οι συνιστώσες C_B, C_R περιέχουν την πληροφορία του χρώματος.



Σχήμα 2.2

Μία έγχρωμη εικόνα και οι Y', Cb, Cr χρωματικές συνιστώσες της. Η Y' συνιστώσα είναι στην ουσία μία μετατροπή της αρχικής εικόνας σε grayscale.

Καθώς το ανθρώπινο μάτι είναι πιο ευαίσθητο σε αλλαγές στη φωτεινότητα της εικόνας, στη συνιστώσα Y' δεν γίνεται υποδειγματοληψία. Στις συνιστώσες C_B, C_R, οι οποίες περιέχουν πληροφορία χρώματος γίνεται υποδειγματοληψία, γιατί το μάτι είναι λιγότερο ευαίσθητο σε αλλαγές που αφορούν το χρώμα. Αν για παράδειγμα η εικόνα είχε αρχικά διαστάσεις 500x500 η συνιστώσα Y' θα είχε τις ίδιες διαστάσεις, ενώ οι συνιστώσες C_B, C_R θα είχαν ως διαστάσεις της εικόνας 250x250 για υποδειγματοληψία κατά 2. Αυτό έχει ως αποτέλεσμα μικρή διαφορά στην ποιότητα της εικόνας και μικρότερο μέγεθος αρχείου.

Όταν γίνεται συμπίεση της εικόνας και επιθυμούμε μέγιστη ποιότητα αυτό το στάδιο μπορεί να παραλειφθεί και η συμπίεση γίνεται στο RGB χρωματικό μοντέλο [12] . Αν η εικόνα είναι grayscale δεν γίνεται μετατροπή σε $Y'C_B C_R$ καθώς δεν υπάρχουν χρωματικές συνιστώσες.

Μετασχηματισμός DCT

Ο μετασχηματισμός DCT [13] εφαρμόζεται ξεχωριστά σε κάθε συνιστώσα της εικόνας, αφού πρώτα την έχουμε χωρίσει σε block με ίσο αριθμό γραμμών και στηλών.

Συνήθως τα block αυτά έχουν διαστάσεις 8x8, αλλά μπορεί επίσης να έχουν διαστάσεις 4x4 ή 32x32. Οι διαστάσεις του block που θα επιλεγούν για τον μετασχηματισμό πρέπει να μείνουν ίδιες και στις παρακάτω διαδικασίες. Σε περίπτωση που στο τέλος των γραμμών ή των στηλών της εικόνας περισσεύουν pixel τα οποία δεν ανήκουν σε κάποιο block, γίνεται κατάλληλο zero padding έτσι ώστε όλα τα pixel της εικόνας να ανήκουν σε κάποιο block.

Μετά τον μετασχηματισμό DCT σε κάθε block n x n προκύπτουν ένας DC όρος και n^2–1 AC όροι, δηλαδή για 8x8 block έχουμε έναν DC όρο και 63 AC όρους. Ο DC όρος, που βρίσκεται πάντα στην $1^η$ γραμμή και στην $1^η$ στήλη του block, είναι ανάλογος της μέσης έντασης του block. Οι AC συντελεστές μας δείχνουν την μεταβολή του σήματος (τιμών έντασης) στο block - οι υψηλές τιμές συντελεστών αντιπροσωπεύουν μεγάλη μεταβολή χρώματος ενώ οι συντελεστές με μικρή τιμή, μικρή μεταβολή στο χρώμα.

Πριν τον υπολογισμό του μετασχηματισμού DCT γίνεται μια ολίσθηση κατά -128 επίπεδα έντασης στα pixel της κάθε υπό-εικόνας. Στην αρχική εικόνα υπάρχουν 256 επίπεδα τιμών έντασης. Μετά την ολίσθηση το εύρος τιμών είναι [-128, 127].

	1	2	3	4	5	6	7	8
1	145	55	48	88	137	90	61	33
2	116	101	39	67	90	54	65	45
3	76	114	46	46	97	59	59	47
4	70	135	95	48	82	120	53	46
5	86	121	131	49	76	87	74	50
6	81	75	158	60	72	95	43	46
7	43	51	133	129	70	122	53	61
8	33	51	111	153	86	119	48	58

Σχήμα 2.3 8x8 Pixel Block από την εικόνα Baboon

	1	2	3	4	5	6	7	8
1	-392	81	-75	35	-35	-27	36	-1
2	-22	33	78	96	52	-30	-77	31
3	3	-31	-56	17	84	57	4	-24
4	20	26	7	9	1	26	44	41
5	28	-2	-17	19	-5	-3	4	-8
6	8	-16	-27	12	-3	-4	22	-14
7	-11	5	-6	7	10	-8	6	21
8	0	-10	1	-4	9	7	-18	8

Σχήμα 2.4 8x8 Block Μετά τον μετασχηματισμό DCT στο pixel block

Κβαντισμός

Στη συνέχεια, οι συντελεστές του DCT κβαντιζονται [14], χρησιμοποιώντας κατάλληλους πίνακες κανονικοποίησης, όπως αυτοί που φαίνονται στη συνέχεια για luminance και chrominance:

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

Πίνακας κβαντισμού για luminance

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Πίνακας κβαντισμού για chrominance

Ο πρώτος πίνακας κανονικοποίησης χρησιμοποιείται για τη συνιστώσα που περιέχει την πληροφορία της έντασης ή για grayscale εικόνες, ενώ ο δεύτερος για τις συνιστώσες που περιέχουν την πληροφορία του χρώματος.

Οι τιμές των παραπάνω πινάκων μπορούν να κλιμακωθούν κατάλληλα, ώστε να επιτευχθούν διαφορετικοί βαθμοί συμπίεσης. Μεγάλος βαθμός συμπίεσης συνεπάγεται υποβάθμιση στην ποιότητα της εικόνας και αντίστροφα.

Η κλιμάκωση των τιμών του πίνακα κβαντισμού καθορίζεται από την τιμή μιας παραμέτρου, η οποία λέγεται quality factor (QF) και η οποία κυμαίνεται από το 1 έως το 100. Όσο υψηλότερη τιμή έχει το QF, τόσο καλύτερη ποιότητα θα έχει η κβαντισμένη εικόνα.

Ο πίνακας κβαντισμού π.χ σε συνάρτηση του QF υπολογίζεται ως εξής:

$$QF_{Table}i,j = \left[\frac{50 + S\ x\ Di,j}{100}\right]$$

- Όπου D_{ij} είναι ο αρχικός πίνακας κβαντισμού.
- Το QF είναι το Quality Factor.
- Το S παίρνει τιμή S = 5000 / QF για QF < 50 και S = 200 – 2 x QF για QF >= 50.

Πίνακας κβαντισμού luminance για Quality factor 80:

6	4	4	6	10	16	20	24
5	5	6	8	10	23	24	22
6	5	6	10	16	23	28	22
6	7	9	12	20	35	32	25
7	9	15	22	27	44	41	31
10	14	22	26	32	42	45	37
20	26	31	35	41	48	48	40
29	37	38	39	45	40	41	40

Πίνακας κβαντισμού luminance για Quality factor 100:

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Αφού υπολογιστεί ο πίνακας κβαντισμού, χρησιμοποιείται για την κανονικοποίηση των DCT συντελεστών σε κάθε 8x8 block. Οι τιμές των συντελεστών σε κάθε block διαιρούνται σημείο προς σημείο με τις αντίστοιχες τιμές του πίνακα κανονικοποίησης. Στη συνέχεια, γίνεται στρογγυλοποίηση στον κοντινότερο ακέραιο αριθμό.

Από την παραπάνω διαδικασία παράγεται ένα μεγάλο πλήθος συντελεστών με τιμή ίση με το μηδέν, όπως φαίνεται π.χ στο Σχήμα 2.6

	1	2	3	4	5	6	7	8
1	-392	81	-75	35	-35	-27	36	-1
2	-22	33	78	96	52	-30	-77	31
3	3	-31	-56	17	84	57	4	-24
4	20	26	7	9	1	26	44	41
5	28	-2	-17	19	-5	-3	4	-8
6	8	-16	-27	12	-3	-4	22	-14
7	-11	5	-6	7	10	-8	6	21
8	0	-10	1	-4	9	7	-18	8

Σχήμα 2.5 8x8 DCT Block από την εικόνα Baboon

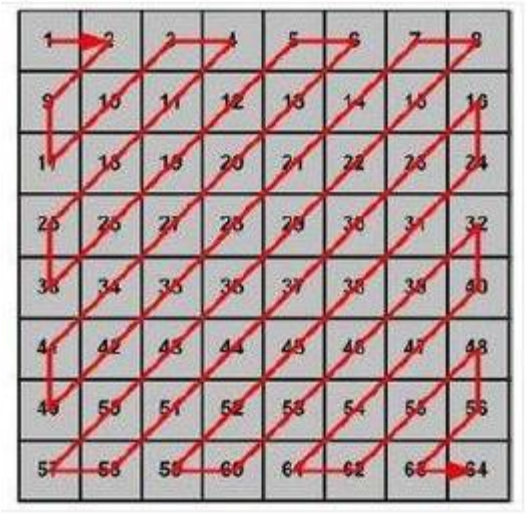
	1	2	3	4	5	6	7	8
1	-65	20	-19	6	-3	-2	2	0
2	-4	7	13	12	5	-1	-3	1
3	1	-6	-9	2	5	2	0	-1
4	3	4	1	1	0	1	1	2
5	4	0	-1	1	0	0	0	0
6	1	-1	-1	0	0	0	0	0
7	-1	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0

Σχήμα 2.6 8x8 Block μετά τον κβαντιισμό στο DCT block με quality factor 80

Μερικά προγράμματα όπως π.χ. το Gimp, δίνουν στον χρήστη την επιλογή να επιλέξει το quality factor που επιθυμεί. Οι κάμερες δίνουν στον χρήστη επιλογές όπως normal, fine, superfine (μέτρια, καλή και μέγιστη ποιότητα), ενώ άλλες κάμερες όπως πχ. της Sony μπορούν και δημιουργούν τον πίνακα κβαντισμού τη στιγμή που γίνεται η λήψη της φωτογραφίας.

Κωδικοποίηση DPCM, runlength

Μετά τον κβαντισμό οι συντελεστές του κάθε block αναδιατάσσονται σύμφωνα με τη zigzag διάταξη που περιγράφεται στο Σχήμα 2.7. Έτσι δημιουργείται ένα διάνυσμα στο οποίο οι συντελεστές που αντιστοιχούν στις χαμηλές συχνότητες βρίσκονται στην αρχή του block, ενώ στο τέλος συγκεντρώνονται οι μηδενικοί συντελεστές.



Σχήμα 2.7 Δημιουργία ενός διανύσματος από τους συντελεστές ενός block οι οποίοι αναδιατάσσονται σύμφωνα με την zigzag διάταξη

-65	20	-4	1	7	-19	6	13
-6	3	4	4	-9	12	-3	-2
5	2	1	0	1	-1	-1	-1
1	5	-1	2	0	-3	2	0
1	-1	0	0	0	0	0	0
1	0	1	-1	1	0	0	0
0	0	0	0	0	2	0	0
0	0	0	0	0	1	0	0

Σχήμα 2.8 Διάνυσμα που προκύπτει μετά την αναδιάταξη των συντελεστών σύμφωνα με τη zigzag διάταξη, στο 8x8 block από το προηγούμενο παράδειγμα

Στους DC όρους εφαρμόζεται DPCM κωδικοποίηση. Αλλάζουμε την τιμή κάθε DC όρου με τη διαφορά του σε σχέση με τον αντίστοιχο όρο. Έτσι, οι τιμές που θα κωδικοποιηθούν στη συνέχεια με Huffman είναι μικρότερες, έχοντας ως αποτέλεσμα την παραγωγή μικρότερων κωδικών λέξεων (με λιγότερα bits). Οπότε αφήνουμε την τιμή του DC όρου στο 1ο block ως έχει και αλλάζουμε τις τιμές των DC όρων στα επόμενα blocks ως εξής: $dc_{new} = dc_{current} - dc_{previous}$

1	2	3	4	5	6	7	8	9	10	11	12
-65	-65	-71	-21	-10	3	-28	15	-11	-16	-14	0

1	2	3	4	5	6	7	8	9	10	11	12
-65	0	-6	50	11	13	-31	43	-26	-5	2	14

Σχήμα 2.9 Παράδειγμα DC όρων πριν και μετά την κωδικοποίηση DPCM

Στους AC όρους εφαρμόζεται run length κωδικοποίηση. Για κάθε AC όρο, σημειώνουμε τον αριθμό των μηδενικών που υπάρχουν πριν από αυτόν και ακολουθεί η τιμή του. Υπάρχουν επίσης δύο ξεχωριστές τιμές runlength, η [15 0] που δίνεται όταν υπάρχουν 16 συνεχόμενα μηδενικά και η [0 0] που δίνεται στο τέλος κάθε block.

-65	0	20	0	-4	0	1	0	7	0	-19	0	6	0	13
0	-6	0	3	0	4	0	4	0	-9	0	12	0	-3	0
-2	0	5	0	2	0	1	1	1	0	-1	0	-1	0	-1
0	1	0	5	0	-1	0	2	1	-3	0	2	1	1	0
-1	6	1	1	1	0	-1	0	1	8	2	7	1	0	0

Σχήμα 2.10 Διάνυσμα κβαντισμένων AC όρων σε διάταξη zigzag μετά την run length κωδικοποίηση

Κωδικοποίηση Huffman

Η κωδικοποίηση Huffman είναι το τελευταίο στάδιο της συμπίεσης JPEG το οποίο οδηγεί στην τελική ακολουθία. Διαβάζουμε κάθε block με τη σειρά και κωδικοποιούμε ξεχωριστά τους DC και τους AC συντελεστές. Η κωδικοποίηση είναι της μορφής [<κωδικός>< DC/AC όρος] όπου ο κωδικός αντιστοιχεί στην κατηγορία στην οποία ανήκει ο κάθε όρος.

Range	DC Difference Category	AC Category
0	0	N/A
−1, 1	1	1
−3, −2, 2, 3	2	2
−7, . . . , −4, 4, . . . , 7	3	3
−15, . . . , −8, 8, . . . , 15	4	4
−31, . . . , −16, 16, . . . , 31	5	5
−63, . . . , −32, 32, . . . , 63	6	6
−127, . . . , −64, 64, . . . , 127	7	7
−255, . . . , −128, 128, . . . , 255	8	8
−511, . . . , −256, 256, . . . , 511	9	9
−1023, . . . , −512, 512, . . . , 1023	A	A
−2047, . . . , −1024, 1024, . . . , 2047	B	B
−4095, . . . , −2048, 2048, . . . , 4095	C	C
−8191, . . . , −4096, 4096, . . . , 8191	D	D
−16383, . . . , −8192, 8192, . . . , 16383	E	E
−32767, . . . , −16384, 16384, . . . , 32767	F	N/A

Σχήμα 2.11 Πίνακας με τον οποίο αντιστοιχούμε έναν AC/DC συντελεστή σε μια κατηγόρια

Ξεκινώντας με τον DC συντελεστή για κάθε block, διαβάζουμε το πρώτο στοιχείο του block και το μετατρέπουμε σε δυαδικό αριθμό π.χ -65_{10} -> 0111110_2. Σύμφωνα με το Σχήμα 2.11, ο αριθμός -65 ανήκει στην κατηγορία 7. Ο κωδικός για αυτή την κατηγορία DC όρων είναι 11110, όπως φαίνεται στον ακόλουθο πίνακα [15]:

Category	Base Code	Length	Category	Base Code	Length
0	010	3	6	1110	10
1	011	4	7	11110	12
2	100	5	8	111110	14
3	00	5	9	1111110	16
4	101	7	A	11111110	18
5	110	8	B	111111110	20

Σχήμα 2.12 Jpeg κωδικοποίηση όρων

Άρα για το -65 η τελική ακολουθία bit θα είναι 111100111110.

Η διαδικασία είναι παρόμοια και για τους AC όρους, μόνο που τώρα ο κωδικός καθορίζεται επιπλέον και με βάση τον αριθμό των μηδενικών πριν τον AC όρο. Ένα μέρος του πίνακα με τους κωδικούς για τους AC όρους φαίνεται παρακάτω:

Run/ Category	Base Code	Length	Run/ Category	Base Code	Length
0/0	**1010 (= EOB)**	**4**			
0/1	00	3	1/1	1100	5
0/2	01	4	1/2	111001	8
0/3	100	6	1/3	1111001	10
0/4	1011	8	1/4	111110110	13
0/5	11010	10	1/5	11111110110	16
0/6	111000	12	1/6	1111111110000100	22
0/7	1111000	14	1/7	1111111110000101	23
0/8	1111110110	18	1/8	1111111110000110	24
0/9	1111111110000010	25	1/9	1111111110000111	25
0/A	1111111110000011	26	1/A	1111111110001000	26
2/1	11011	6	3/1	111010	7
2/2	11111000	10	3/2	111110111	11
2/3	1111110111	13	3/3	11111110111	14
2/4	1111111110001001	20	3/4	1111111110010000	20
2/5	1111111110001010	21	3/5	1111111110010001	21
2/6	1111111110001011	22	3/6	1111111110010010	22
2/7	1111111110001100	23	3/7	1111111110010011	23
2/8	1111111110001101	24	3/8	1111111110010100	24
2/9	1111111110001110	25	3/9	1111111110010101	25
2/A	1111111110001111	26	3/A	1111111110010110	26

Σχήμα 2.13 Μέρος του πίνακα κωδικών για AC όρους [15]

Όπου:

- η 1η στήλη αντιστοιχεί στον αριθμό μηδενικών πριν τον όρο και στον κωδικό της κατηγορίας του AC όρου
- στην 2η ο κωδικός
- και στην 3η ο συνολικός αριθμός bit που απαιτούνται για την κωδικοποίηση του όρου (bit κωδικού + bit όρου).

Άρα, για παράδειγμα έστω ότι έχουμε 3 μηδενικούς όρους και έναν AC συντελεστή με τιμή 10 [0 0 0 10]. Μετατρέπουμε τον όρο στο δυαδικό: 10_{10} -> 1010_2. Καθώς πριν από τον όρο υπάρχουν 3 μηδενικά και ο αριθμός 10 ανήκει στην κατηγορία (3/4) επιλέγεται ο κωδικός 1111111110010000 σύμφωνα με το Σχήμα 2.13 και η τελική ακολουθία θα είναι 11111111100100001010.

Για την αποκωδικοποίηση της δυαδικής ακολουθίας που προκύπτει από την JPEG συμπίεση, είναι απαραίτητοι οι παραπάνω πίνακες και ο πίνακας κβαντισμού, οι οποίοι αποθηκεύονται στο JPEG αρχείο.

Επίσης πριν την κωδικοποίηση μπορεί να γίνει βελτιστοποίηση στους πίνακες [16] δηλαδή να δοθούν μικρότεροι κωδικοί Huffman στους AC συντελεστές που εμφανίζονται πιο συχνά, και μεγαλύτεροι σε αυτούς που είναι πιο σπάνιοι.

Οι περισσότερες ψηφιακές κάμερες [16] συνήθως χρησιμοποιούν τους παραπάνω Huffman κωδικούς καθώς η δημιουργία μικρότερων κωδικών Huffman είναι περίπλοκη και ο υπολογισμός τους θα καθυστερούσε. Ωστόσο ένα πρόγραμμα για επεξεργασία εικόνων όπως είναι το photoshop συνήθως δίνουν στον χρήστη την επιλογή να κάνει αποθήκευση της εικόνας με ‘optimized’ πίνακες [17] καθώς ο χρόνος αποθήκευσης με ή χωρίς βελτιστοποίηση για έναν σύγχρονο υπολογιστή είναι σχεδόν ο ίδιος.

Αποτέλεσμα συμπίεσης Jpeg

Η εικόνα Lena μετά την συμπίεση JPEG έχει μέγεθος 36.3 KB, για quality factor 80. Το αρχείο αυτό είναι αρκετά μικρότερο από το αρχείο PNG για την ίδια εικόνα, το οποίο είχε μέγεθος 131 KB. Η διαφορά σε ποιότητα μεταξύ των δύο εικόνων είναι πολύ μικρή.

Αριστερά η εικόνα Lena αποθηκευμένη ως JPEG αρχείο με quality factor 80 και δεξιά η ίδια εικόνα αποθηκευμένη ως PNG.

Κεφάλαιο 3: Τεχνικές Αναστρέψιμης απόκρυψη πληροφορίας σε εικόνες

Οι πρώτες τεχνικές αναστρέψιμης απόκρυψης πληροφορίας υλοποιήθηκαν σε ασυμπίεστες εικόνες. Η ένθεση του μηνύματος γίνεται άμεσα, μεταβάλλοντας τις τιμές των pixel της εικόνας. Για συμπιεσμένες εικόνες όπως JPEG έχουν αναπτυχθεί τεχνικές RDH ωστόσο είναι πολύ λιγότερες από αυτές σε ασυμπίεστες εικόνες καθώς η διαδικασία της συμπίεσης μηδενίζει ορισμένους συντελεστές για να μικρύνει το μέγεθος του αρχείου κάτι που δυσκολεύει την διαδικασία της ένθεσης.

Μετά την ένθεση ενός μηνύματος στην εικόνα, ανεξαρτήτως της τεχνικής που χρησιμοποιήσαμε πρέπει να συγκρίνουμε την ποιότητα της εικόνας μετά την ένθεση με την ποιότητα της αρχικής εικόνας. Αυτό μας βοηθάει να βελτιώσουμε την απόδοση της τεχνικής μας και να την συγκρίνουμε με άλλες τεχνικές. Ένας τρόπος για να συγκρίνουμε τις δύο εικόνες είναι να υπολογίσουμε το PSNR [18] τους. Το PSNR (peak signal to noise ratio) συγκρίνει την αναλογία της ισχύς του σήματος της αρχικής εικόνας και του θορύβου που παράγεται λόγω της ένθεσης. Η μονάδα μέτρησης του είναι το decibel και όσο υψηλότερη είναι η τιμή του, τόσο η νέα εικόνα προσεγγίζει την αρχική όσον αφορά την ποιότητα. Το PSNR το υπολογίζουμε επίσης και μετά από την απωλεστική (lossy) συμπίεση μιας εικόνας όπου ο θόρυβος τώρα παράγεται λόγω της πληροφορίας που χάνεται.

Ένας άλλος τρόπος να συγκρίνουμε την ποιότητα της εικόνα μετά από την ένθεση μηνύματος ή από συμπίεση είναι με τον υπολογισμό της ομοιότητας των δύο εικόνων μέσω του SSIM το οποίο σύμφωνα με τον Alain Hore et al [19] δεν είναι ούτε περισσότερο αλλά ούτε λιγότερο ακριβές από το PSNR. Ωστόσο καθώς στα επιστημονικά άρθρα που μελετήθηκαν για αυτή τη διπλωματική γινόταν χρήση του PSNR για τις συγκρίσεις εικόνων, θα γίνεται αναφορά σε αυτό για την αξιολόγηση της απόδοσης των τεχνικών και για τα πειραματικά αποτελέσματα σε παρακάτω κεφάλαιο.

Τεχνικές Αναστρέψιμης απόκρυψη πληροφορίας σε ασυμπίεστες εικόνες

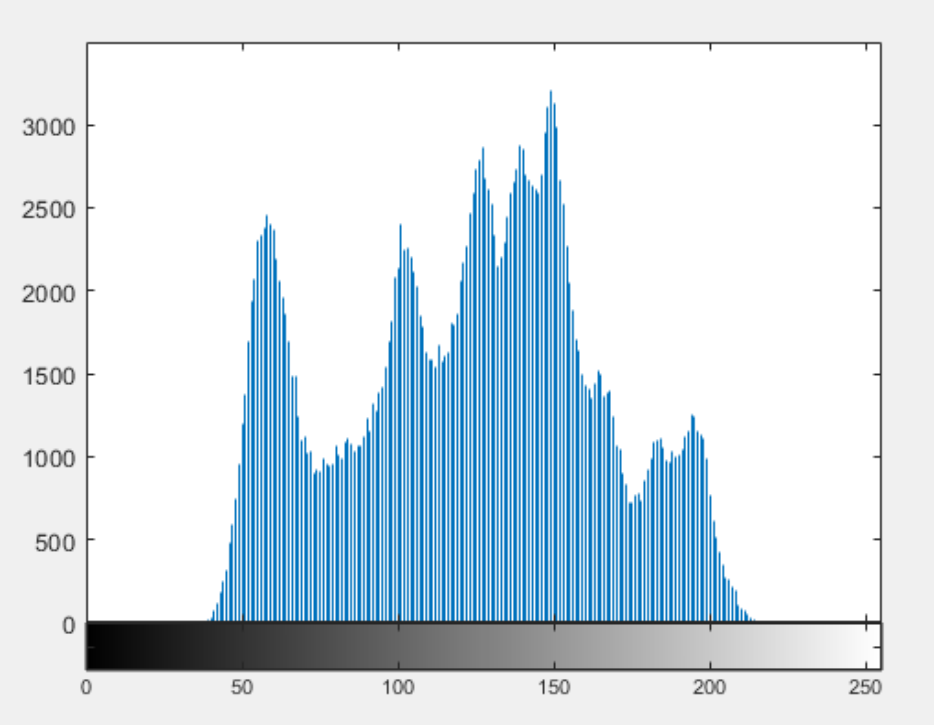
Μετατόπιση ιστογράμματος

Πολλές τεχνικές RDH σε ασυμπίεστες εικόνες βασίζονται στην μετατόπιση ιστογράμματος [20]. Μερικές από αυτές μπορούν να εφαρμοστούν και σε συμπιεσμένες εικόνες όπου αντί για μεταβολή των τιμών έντασης των pixel γίνεται μεταβολή των DCT συντελεστών.

Το ιστόγραμμα μιας εικόνας είναι ένα γράφημα το οποίο μας δείχνει την κατανομή των επιπέδων έντασης στην εικόνα δηλαδή τον αριθμό των pixel που έχουν μία τιμή έντασης. Στον οριζόντιο άξονα βρίσκονται οι τιμές έντασης και στον κατακόρυφο το πλήθος των pixel που έχουν κάθε τιμή έντασης (Σχήμα 3.1). Σε κάθε εικόνα μπορούμε να μετατοπίσουμε το ιστόγραμμα σε ένα σημείο και να εισάγουμε το μήνυμα στο «κενό» που δημιουργήσαμε.

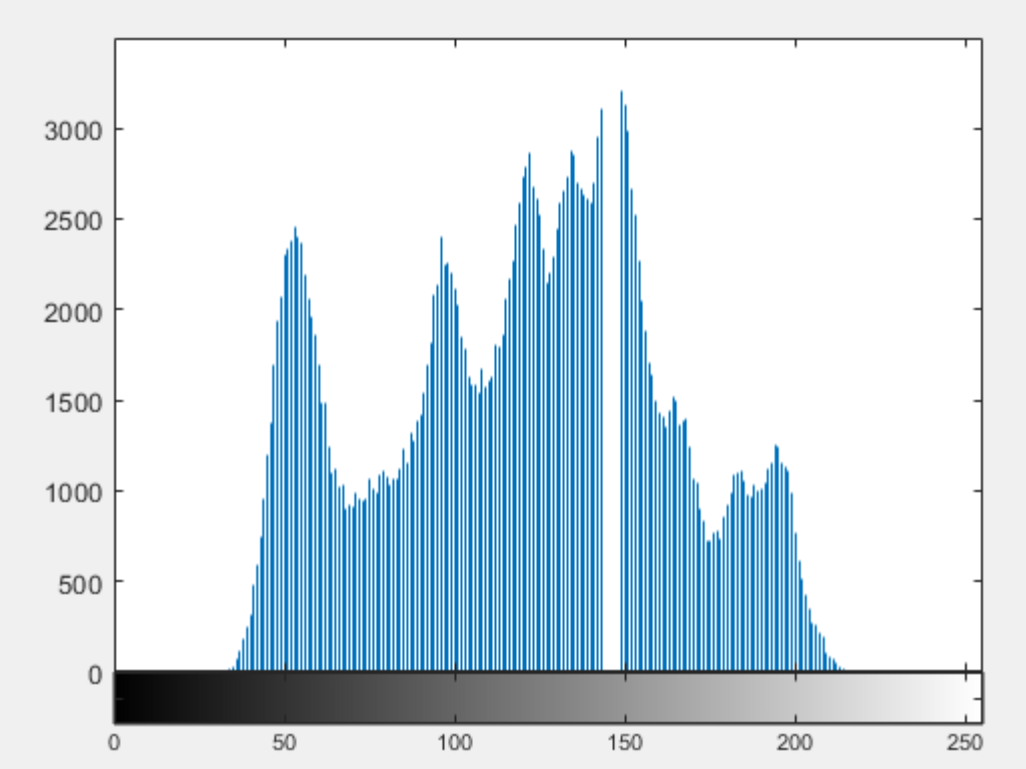
Αρχικά παράγουμε το ιστόγραμμα της αρχικής εικόνας και θέτουμε ένα κατώφλι (T) με βάση το οποίο θα γίνουν μεταβολές στα pixel της εικόνας. Στα pixel της εικόνας με τιμή ίση με το

κατώφλι γίνεται η ένθεση bit μηνύματος. Μπορούμε να θέσουμε το κατώφλι ως την κορυφή του ιστογράμματος, ίσο με την τιμή του pixel με τις περισσότερες εμφανίσεις στην εικόνα αν θέλουμε να γίνει ένθεση μέγιστου μήκους μηνύματος.



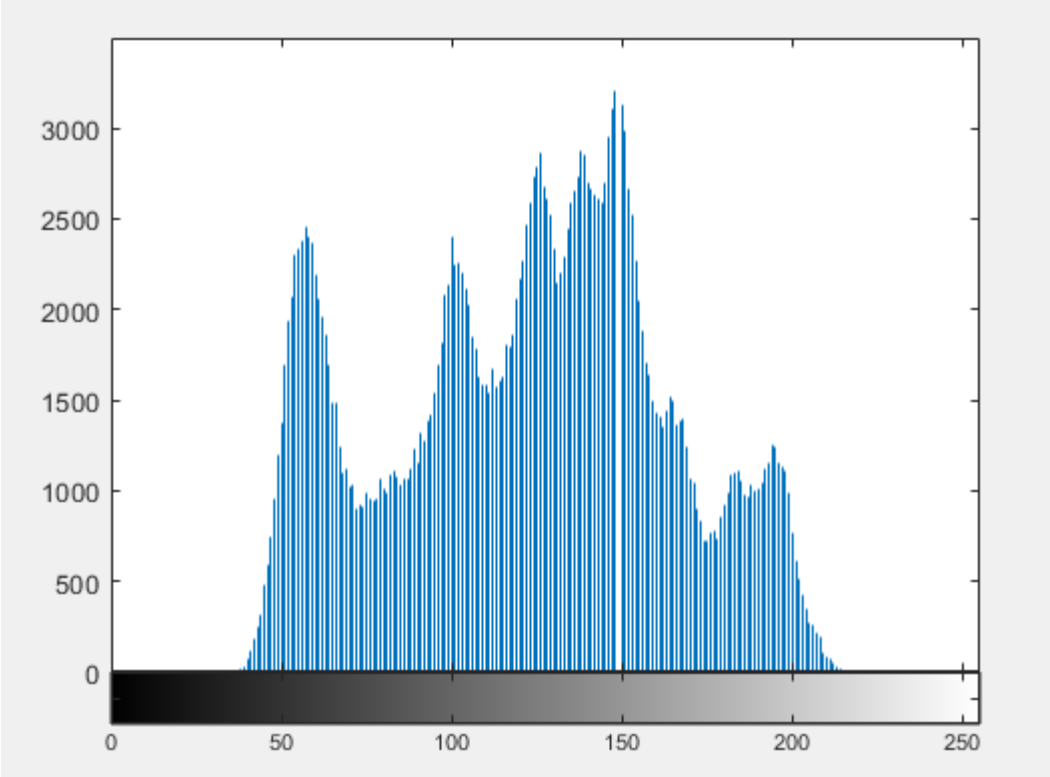
Σχήμα 3.1 Ιστόγραμμα εικόνας Lena (grayscale)

Στη συνέχεια μετατοπίζουμε το ιστόγραμμα (Σχήμα 3.2), δηλαδή μειώνουμε κατά 1 τις τιμές των pixel οι οποίες είναι μικρότερες από T.



Σχήμα 3.2 Μετατόπιση ιστογράμματος στα αριστερά στην εικόνα Lena

Τέλος κάνουμε ένθεση του μηνύματος στις τιμές που είναι ίσες με T. Για να γίνει εισαγωγή bit με τιμή 1 η τιμή των pixel αλλάζει σε T-1 ενώ για εισαγωγή bit με τιμή 0 η τιμή των pixel δεν μεταβάλλεται.



Σχήμα 3.3 Ιστόγραμμα της εικόνας Lena μετά την μετατόπιση ιστογράμματος και την εισαγωγή τυχαίων bit

Το μήνυμα μπορεί να ανακτηθεί εύκολα από την εικόνα εντοπίζοντας τα pixel με τιμές T-1 και T-2. Εξάγουμε το μήνυμα από αυτά τα pixel και αλλάζουμε την τιμή τους σε T. Στη συνέχεια για να επαναφέρουμε την εικόνα στην αρχική της μορφή, κάνουμε μετατόπιση του ιστογράμματος στα δεξιά στα pixel με τιμή μικρότερη από T.

Μεταβολή διαφοράς γειτονικών pixel

Μία άλλη τεχνική RDH αξιοποιεί την διαφορά μεταξύ δύο γειτονικών pixel για την εισαγωγή πληροφορίας στην εικόνα [21]. Αρχικά με τους τύπους L = [(x0 + x1) / 2] και h = x1 – x0 (όπου τα x0 και x1 είναι γειτονικά pixel) γίνεται υπολογισμός του μέσου όρου του ζευγαριού pixel και της διαφοράς τους. Στη συνέχεια γίνεται μεταβολή της διαφοράς τους και προσθήκη ενός bit μηνύματος (m) με τον εξής τύπο: h’ = 2h + m. Για την διατήρηση της ποιότητας της εικόνας ο μέσος όρος του ζευγαριού L δεν μεταβάλλεται. Οι νέες τιμές του ζευγαριού pixel υπολογίζονται με βάση τον αρχικό μέσο όρο (L) και την νέα τιμή διαφοράς των pixel (h’). Με αυτή τη μέθοδο μπορεί να γίνει εισαγωγή αρκετά μεγάλου μήκους μηνύματος (0.5 bit ανά pixel) χωρίς να γίνει αλλοίωση της ποιότητας της εικόνας. Το μήνυμα μπορεί να εξαχθεί από την εικόνα υπολογίζοντας το λιγότερο σημαντικό bit της διαφοράς ενός ζευγαριού pixel στην εικόνα που έχει γίνει η ένθεση.

Ανθεκτική αναστρέψιμη απόκρυψη πληροφορίας σε ασυμπίεστες εικόνες

Το μήνυμα που έχει εισαχθεί σε μια εικόνα μπορεί να μην είναι δυνατό να εξαχθεί μελλοντικά, αν έχουν μεταβληθεί οι τιμές των pixel της εικόνας από συμπίεση ή από κάποια άλλη διαδικασία. Η λύση σε αυτό το πρόβλημα είναι είτε να χρησιμοποιήσουμε μια τεχνική η οποία θα είναι ανθεκτική στη συμπίεση ή μία τεχνική η οποία εισάγει πληροφορία παράλληλα με τη συμπίεση. Ένα παράδειγμα τεχνικής που είναι ανθεκτική στη συμπίεση [22] αξιοποιεί τον μέσο όρο της διαφοράς ζευγαριών pixel σε ένα block της εικόνας. Αρχικά υπολογίζεται η διαφορά α με τον εξής τύπο, όπου τα x και y είναι τα γειτονικά pixel και n ο αριθμός ζευγαριών στο κάθε block (αν το block έχει διαστάσεις 8x8 υπάρχουν n=32 ζευγάρια pixel σε αυτό).

$$a = \frac{1}{n}\sum_{i=1}^{n}(x_i - y_i)$$

Μετά από την συμπίεση JPEG οι τιμές των pixel μπορεί να αλλάξουν τιμή αλλά η τιμή α μένει σταθερή άρα είναι ανθεκτική στη συμπίεση. Στη συνέχεια θέτουμε ένα κατώφλι. Για να εισάγουμε bit μηνύματος με τιμή ένα, μεταβάλουμε την τιμή α ώστε να ξεπερνά το κατώφλι, αλλάζοντας τις τιμές των pixel στο block. Αν το bit μηνύματος έχει τιμή 0 δεν γίνεται καμία αλλαγή στο block. Το μόνο αρνητικό αυτής της τεχνικής είναι πως καθώς σε κάθε block γίνεται εισαγωγή ενός μόνο bit, μπορούν να εισαχθούν με αυτό τον τρόπο μόνο μικρού μήκους μηνύματα.

Αναστρέψιμη απόκρυψη πληροφορίας σε συμπιεσμένες εικόνες

Η διαδικασία της απόκρυψης πληροφορίας σε συμπιεσμένες εικόνες διαφέρει αρκετά από αυτήν στις ασυμπίεστες. Καθώς στα pixel της αρχικής εικόνας εφαρμόζεται κβαντισμός έτσι ώστε να κοπεί μέρος της πληροφορίας και να μικρύνει το τελικό αρχείο, αν εφαρμόσουμε τις τεχνικές που εφαρμόζουμε στις ασυμπίεστες εικόνες το μήνυμα μπορεί να αλλοιωθεί και να μην είναι ανακτήσιμο. Για αυτό η ένθεση θα πρέπει να γίνει σε κάποιο στάδιο της συμπίεσης. Σε αυτές τις τεχνικές είναι σημαντικό η ένθεση να μην επηρεάζει σε μεγάλο βαθμό το μέγεθος του τελικού αρχείου, να διατηρεί την ποιότητα της αρχικής εικόνας και να μπορεί να εισαχθεί αρκετά μεγάλο μήκος μηνύματος.

RDH σε συμπιεσμένες εικόνες με τροποποίηση του πίνακα κβαντισμού

Στην συμπίεση JPEG αφού έχει γίνει επιλογή του κατάλληλου πίνακα κβαντισμού για μια εικόνα, ο πίνακας αυτός μπορεί να τροποποιηθεί έτσι ώστε να μπορεί να γίνει ένθεση του μηνύματος σε DCT συντελεστές [23]. Αρχικά διαιρούμε με το δύο τις ζυγές τιμές του πίνακα

κβαντισμού. Κατά τον κβαντισμό των block εικόνας, στην ίδια θέση όπου έγινε η διαίρεση των τιμών στον πίνακα κβαντισμού, διπλασιάζουμε την τιμή του DCT συντελεστή. Με αυτόν τον τρόπο δεν γίνεται μεταβολή των DCT συντελεστών οπότε δεν αλλοιώνεται η ποιότητα της εικόνα. Αν ο DCT συντελεστής είναι ζυγός μπορούμε να εισάγουμε ένα bit μηνύματος στο λιγότερο σημαντικό bit αυτού του συντελεστή.

Τα μειονεκτήματα αυτής της τεχνικής είναι πως θα χρησιμοποιηθεί ένας ασυνήθιστος πίνακας κβαντισμού τον οποίο πρέπει να αποθηκεύσουμε μαζί με την εικόνα και πως η συμπίεση δε θα είναι τόσο αποδοτική, άρα η συμπιεσμένη εικόνα με το υδατογράφημα θα είναι αρκετά μεγαλύτερη από την εικόνα χωρίς το υδατογράφημα.

RDH σε συμπιεσμένες εικόνες με τροποποίηση των κωδικών Huffman

Μία άλλη τεχνική RDH σε συμπιεσμένες εικόνες αξιοποιεί κωδικούς Huffman [24]. Για την κωδικοποίηση των DCT όρων δεν γίνεται αξιοποίηση όλων των κωδικών Huffman και αρκετοί κωδικοί μένουν αχρησιμοποίητοι. Ένας κωδικός Huffman μπορεί να αλλάξει σε έναν άλλο κωδικό με ίδιο μήκος σε bit. Αρχικά γίνεται εύρεση των κωδικών Huffman που χρησιμοποιούνται για την κωδικοποίηση. Για να γίνει εισαγωγή ενός bit με τιμή ένα γίνεται αντιστοίχιση ενός κωδικού Huffman με έναν άλλο με ίσο αριθμό bit. Για την εισαγωγή ενός bit με τιμή μηδέν δεν γίνεται αλλαγή του κωδικού Hufffman. Απαραίτητη προϋπόθεση είναι οι νέοι κωδικοί να μην χρησιμοποιούνται για την κωδικοποίηση άλλων κβαντισμένων συντελεστών καθώς αυτό θα προκαλέσει προβλήματα στην αποκωδικοποίηση της εικόνας.

Με αυτόν το τρόπο μπορεί το μέγεθος του αρχείου να παραμείνει αμετάβλητο αφού έχουμε εισάγει το μήνυμα. Παρόλο που αυτή η μέθοδος φαίνεται να είναι ιδανική, μπορούν να εισαχθούν μόνο μηνύματα περιορισμένου μήκους άρα μπορεί να χρησιμοποιηθεί μόνο για την ψηφιακή πιστοποίηση [25] (digital image authentication) της εικόνας όπου δεν απαιτείται μεγάλο μήκος μηνύματος. Η ψηφιακή πιστοποίηση χρησιμοποιείται όταν θέλουμε να αποδείξουμε ότι η εικόνα από ένα συμβάν είναι έγκυρη και δεν έχει αλλοιωθεί από κανέναν.

RDH σε συμπιεσμένες εικόνες με τροποποίηση των κβαντισμένων DCT συντελεστών

Σε μία συμπιεσμένη εικόνα αν μερικοί κβαντισμένοι DCT συντελεστές μεταβληθούν ελάχιστα δε θα υπάρξει μεγάλη διαφορά στην τελική εικόνα. Μόνο μικρής και μεσαίας συχνότητας AC συντελεστές επιλέγονται για την εισαγωγή του μηνύματος και ο DC συντελεστής δεν μεταβάλλεται. Τα πλεονεκτήματα αυτού του είδους τεχνικών είναι πως μπορούμε να εισάγουμε μεγάλα σε μέγεθος μηνύματα με υψηλό PSNR σε σχέση με την αρχική εικόνα και με μικρή μεταβολή στο μέγεθος του αρχείου.

Σε αυτή την διπλωματική η υλοποίηση αφορούσε τεχνικές αναστρέψιμης απόκρυψης πληροφορίας με τροποποίηση κβαντισμένων DCT συντελεστών οι οποίες θα αναλυθούν περισσότερο στα παρακάτω κεφάλαια.

Κεφάλαιο 4: Αναστρέψιμη απόκρυψη πληροφορίας με ζεύγη ιστογράμματος

Η πρώτη τεχνική αναστρέψιμης απόκρυψης πληροφορίας σε συμπιεσμένες εικόνες [26] που υλοποιήθηκε αξιοποιεί το ιστόγραμμα των κβαντισμένων AC συντελεστών στα block της εικόνας. Παρακάτω περιγράφονται η διαδικασία ένθεσης του μηνύματος, πως γίνεται η εξαγωγή του και η αποκατάσταση της εικόνας και πως μπορούμε να επιτύχουμε μέγιστο PSNR με αυτή την τεχνική.

Ζεύγη Ιστογράμματος

Η τεχνική δουλεύει με ζεύγη ιστογράμματος AC συντελεστών. Το ιστόγραμμα AC συντελεστών σε ένα block εικόνας μας δείχνει την τιμή των ξεχωριστών AC συντελεστών σε σχέση με το πόσες φορές εμφανίζονται. Εάν μετατοπίσουμε μέρος του ιστογράμματος, δηλαδή αν αυξήσουμε τις τιμές των AC συντελεστών στο block οι οποίες ξεπερνάνε ένα κατώφλι, μπορούμε να εισάγουμε bit μηνύματος στο κενό που δημιουργείται στο ιστόγραμμα.

Το ιστόγραμμα σε ένα block μπορεί να μετατοπιστεί αριστερά ή δεξιά. Όταν αυξάνουμε τις τιμές των AC συντελεστών, μέρος του ιστογράμματος μετατοπίζεται στα δεξιά ενώ όταν μειώνουμε τις τιμές των AC συντελεστών γίνεται μετατόπιση στα αριστερά.

Δύο AC συντελεστές α και β με $\alpha < \beta$ λέμε ότι σχηματίζουν ζευγάρι ιστογράμματος όταν είναι γειτονικοί, δηλαδή αν οι τιμές τους διαφέρουν κατά 1 (π.χ $b = a + 1$) και όταν ένας από τους δύο δεν εμφανίζεται καθόλου στο block, δηλαδή κανένας DCT συντελεστής δεν παίρνει την τιμή του. Συμβολίζεται με $h = [m,n]$ όπου m οι φορές που εμφανίζεται ο α και n οι φορές που εμφανίζεται ο β.

Για να δημιουργήσουμε ένα ζευγάρι ιστογράμματος αρχικά μετατοπίζουμε το ιστόγραμμα θέτοντας ως κατώφλι έναν από τους δύο συντελεστές. Έστω ότι έχουμε ένα block 3x3 και θέλουμε να κάνουμε εισαγωγή bit στις τιμές 1 και 2:

1	1	3
2	3	2
1	1	2

Θέτουμε ως κατώφλι το 1 και μετατοπίζουμε το ιστόγραμμα στα δεξιά για τους συντελεστές με τιμή μεγαλύτερη από 1 δημιουργώντας το ζεύγος $h=[4,0]$ με $a=1$ και $\beta=2$:

1	1	4
3	4	3
1	1	3

Αφού έχουμε δημιουργήσει το ζευγάρι μπορούμε να εισάγουμε bit μηνύματος χρησιμοποιώντας την τιμή του a αν το bit είναι μηδέν και την τιμή του b αν το bit είναι άσσος. Έστω ότι τα bit μηνύματος είναι τα εξής: 1010. Το block μετά την εισαγωγή θα έχει αυτές τις τιμές:

2	1	4
3	4	3
2	1	3

Σε ένα block της εικόνας μπορεί να γίνει εισαγωγή μηνύματος με πολλαπλά ζεύγη ιστογράμματος. Τα ζεύγη αυτά μπορούν να μετατοπίζουν το ιστόγραμμα και αριστερά και δεξιά εναλλάξ για να αξιοποιηθούν και θετικοί και αρνητικοί AC συντελεστές.

Επιλογή μέρους του 8x8 block για την ένθεση του μηνύματος

Για να επιτύχουμε το μέγιστο PSNR σε σχέση με την αρχική εικόνα, πρέπει να επιλέξουμε συγκεκριμένες θέσεις στα block της εικόνας για να εισάγουμε το μήνυμα. Οι συντελεστές στους οποίους θέλουμε να γίνει η ένθεση είναι αυτοί με χαμηλή και μεσαία συχνότητα. Για την επιλογή αυτών των συντελεστών κάνουμε ένθεση μόνο σε μία περιοχή του block. Αυτή η περιοχή εκτός από καλή απόδοση πρέπει να μας επιτρέπει να εισάγουμε και μεγάλο σε μήκος μήνυμα.

Αρχικά κάνουμε προσπέλαση του block σε zigzag διάταξη. Αριθμούμε το κάθε κελί σε σειρά zigzag από 1 έως 64.

1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Πίνακας 1 8x8 Block αριθμημένο σε zigzag διάταξη

Στη συνέχεια επιλέγουμε δύο διαδοχικές τιμές o1, o2 όπου $1 < o1 < o2 < 64$. Η ένθεση του μηνύματος θα γίνει στα κελιά του block με αρίθμηση ανάμεσα σε αυτές τις τιμές. Οι συντελεστές με μικρές η μεσαίες συχνότητες βρίσκονται στο κέντρο ενός block εικόνας οπότε γίνονται πειράματα σε περιοχές με $o1 > 1$ και $o2 < 50$ τα οποία φαίνονται σε παρακάτω κεφάλαιο. Καθώς η περιοχή R: {4, 36} μας δίνει την καλύτερη απόδοση, αυτή επιλέγεται για την ένθεση του μηνύματος.

1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Πίνακας 2 Η περιοχή {4, 36} που επιλέχθηκε για την ένθεση

Πριν την εισαγωγή bit σε ένα block της εικόνας μπορεί να γίνει αντιγραφή αυτής της περιοχής R σε ένα διάνυσμα. Η μετατόπιση ιστογράμματος και η ένθεση αφορά μόνο τις τιμές αυτού του διανύσματος. Τιμές εκτός του διανύσματος δεν αλλάζουν. Μετά την ένθεση στο διάνυσμα γίνεται αντιγραφή του πίσω στο block της εικόνας, στις ίδιες θέσεις. Το ίδιο γίνεται και με την εξαγωγή του μηνύματος από το block. Οι τιμές του block αντιγράφονται πάλι σε ένα διάνυσμα. Αφού γίνει εξαγωγή του μηνύματος και επαναφορά των αρχικών τιμών, το διάνυσμα μεταφέρεται πίσω στο block.

Επιλογή εύρους τιμών T και S

Πριν ξεκινήσει η εισαγωγή του μηνύματος στα block της εικόνας γίνεται επιλογή των τιμών T και S, όπου |T| > |S|. Η ένθεση του μηνύματος σε ένα block ξεκινάει από τους AC συντελεστές με τιμή μέτρου ίση με T. Στη συνέχεια η ένθεση γίνεται σε συντελεστές με μέτρο μικρότερο από T και σταματάει όταν γίνει ένθεση σε τιμές με μέτρο ίσο με S. Συνεπώς για την εισαγωγή θα πρέπει το πλήθος των AC συντελεστών με μέτρο ανάμεσα σε S και T, να είναι μεγαλύτερο ή ίσο με το μήκος μηνύματος σε bit.

Η επιλογή των τιμών T και S επηρεάζει και το PSNR της εικόνας. Με δύο διαφορετικά εύρη τιμών S και T μπορούμε να εισάγουμε το ίδιο μήκος μηνύματος σε μία εικόνα αλλά το ένα εύρος τιμών να μας δώσει ηψηλότερο PSNR από το άλλο. Αρχικά αποφεύγουμε να κάνουμε εισαγωγή σε συντελεστές με τιμή μηδέν. Πειραματικά αποτελέσματα έχουν δείξει πως η εισαγωγή σε αυτούς τους συντελεστές οδηγεί σε χειρότερο PSNR. Έκτος αυτού η συμπίεση JPEG μηδενίζει AC συντελεστές για την επίτευξη μικρότερου μεγέθους αρχείου, οπότε αν τους επαναφέρουμε για την ένθεση το μέγεθος του αρχείου θα αυξηθεί. Επίσης η διαφορά μεταξύ του μέτρου των S και T πρέπει να είναι μικρή. Κάθε φορά που γίνεται ένθεση bit σε μία τιμή ανάμεσα σε S και T γίνεται μετατόπιση μέρους του ιστογράμματος σε εκείνο το σημείο. Πολλές μετατοπίσεις στο ιστόγραμμα ενός block οδηγούν σε χειρότερο PSNR. Όσο μεγαλύτερη είναι η διαφορά του S και του T, τόσες περισσότερες μετατοπίσεις του ιστογράμματος γίνονται. Ιδανικά το S και το T πρέπει να έχουν ίση σε μέτρο τιμή για να γίνει μόνο μία μετατόπιση σε κάθε block.

Εισαγωγή του μηνύματος

Αφού έχει γίνει η επιλογή της περιοχής R και του εύρους S, T στο οποίο θα εισαχθεί το μήνυμα ξεκινάμε τη διαδικασία εισαγωγής. Μέρος του μηνύματος θα εισαχθεί σειριακά στα block της εικόνας. Αν το μήνυμα είναι αρκετά μεγάλο, μπορεί να χρησιμοποιηθούν και όλα τα block. Ο αλγόριθμος εισαγωγής του μηνύματος αξιοποιεί πολλαπλά ζεύγη ιστογράμματος ανά block.

Η ένθεση ξεκινάει με τους συντελεστές με τιμή P, το οποίο αρχικοποιούμε θέτοντας P = T. Το πρόσημο του P καθορίζει αν η μετατόπιση του ιστογράμματος θα γίνει αριστερά η δεξιά. Μέρος του ιστογράμματος μετατοπίζεται δεξιά για θετικές τιμές P και αριστερά για αρνητικές τιμές. Σε αυτό το παράδειγμα θεωρούμε πως το T έχει θετική τιμή οπότε η μετατόπιση γίνεται πρώτα στα δεξιά. Επίσης, το P μετά από την ένθεση ενός μέρους του μηνύματος στο block αλλάζει τιμή, αν πρόκειται να συνεχιστεί η εισαγωγή στο ίδιο block. Αν το P έχει θετική τιμή, η τιμή του αλλάζει σε -P, ενώ αν η τιμή του είναι αρνητική, την αλλάζουμε σε -P-1.

Για την εισαγωγή γίνεται πρώτα μετατόπιση του ιστογράμματος δεξιά, χρησιμοποιώντας ως κατώφλι το P, και εισάγουμε bit μηνύματος στους συντελεστές με τιμή P κάνοντας πρόσθεση των bit μηνύματος σε αυτούς. Αφού γίνει η ένθεση σε αυτούς τους συντελεστές, αλλάζουμε την τιμή του P, μετατοπίζουμε το ιστόγραμμα αριστερά μειώνοντας τις τιμές των συντελεστών με τιμή μικρότερη από P και εισάγουμε bit μηνύματος στους συντελεστές με τιμή P αφαιρώντας αυτή τη φορά τα bit μηνύματος από αυτούς. Αυτό επαναλαμβάνεται στο block μέχρι το P να γίνει ίσο με S, και ο αλγόριθμος συνεχίζει στα επόμενα block μέχρι να γίνει εισαγωγή όλων των bit μηνύματος σε κάθε block της εικόνας.

Για παράδειγμα, έστω ότι θέλουμε να εισάγουμε το μήνυμα D = [1 0 1 0 1 1] στο παρακάτω block. Η ένθεση θα ξεκινήσει με T=4 και θα σταματήσει για S = -4.

1	-2	-1	3	-4
-4	0	4	-3	6
5	4	2	0	-6
-8	0	7	-5	4
0	0	-4	0	-9

Πρώτα κάνουμε μετατόπιση δεξιά για συντελεστές μεγαλύτερους από 4:

1	-2	-1	3	-4
-4	0	4	-3	7
6	4	2	0	-6
-8	0	8	-5	4
0	0	-4	0	-9

Γίνεται ένθεση των 3^{ων} πρώτων bit [1 0 1] στους συντελεστές με τιμή 4:

1	-2	-1	3	-4
-4	0	5	-3	7
6	4	2	0	-6
-8	0	8	-5	5
0	0	-4	0	-9

Στη συνέχεια μετατοπίζουμε αριστερά τους συντελεστές μικρότερους από -4:

1	-2	-1	3	-4
-4	0	5	-3	7
6	4	2	0	-7
-9	0	8	-6	5
0	0	-4	0	-10

Γίνεται ένθεση των τελευταίων bit [0 1 1] στους συντελεστές με τιμή -4:

1	-2	-1	3	-4
-5	0	5	-3	7
6	4	2	0	-7
-9	0	8	-6	5
0	0	-5	0	-10

Εισαγωγή παραμέτρων στο header της εικόνας

Για την εξαγωγή του μηνύματος, ο παραλήπτης θα πρέπει να γνωρίζει πως έγινε η εισαγωγή του μηνύματος. Το μήκος του μηνύματος, οι τιμές S και T που χρησιμοποιήθηκαν για την μετατόπιση του ιστογράμματος, το εύρος o1, o2 για την επιλογή ενός μέρους του DCT block για να γίνει η ένθεση πρέπει να είναι γνωστές. Μερικές τεχνικές εισάγουν παραμέτρους για την εξαγωγή σαν μέρος του μηνύματος. Σε αυτή την τεχνική μπορεί να γίνει εισαγωγή των παραμέτρων στο header της εικόνας σαν σχόλιο. Έτσι ο παραλήπτης μπορεί εύκολα να εντοπίσει τα block στα οποία έγινε ένθεση του μηνύματος χωρίς επιπρόσθετη πληροφορία από τον

αποστολέα. Καθώς όμως το ίδιο μπορεί να κάνει και ένας μη εξουσιοδοτημένος χρήστης, μπορούμε να στείλουμε ξεχωριστά αυτή την πληροφορία και να αφήσουμε το header κενό.

Εξαγωγή του μηνύματος

Για την εξαγωγή του μηνύματος αρχικά γίνεται εύρεση των παραμέτρων από το header της εικόνας. Στη συνέχεια γίνεται προσπέλαση του κάθε block και γίνεται έλεγχος, αν στο εύρος R υπάρχουν τιμές ίσες με S. Αν ναι, θέτουμε P = S και ακολουθούμε την αντίστροφη διαδικασία από αυτή της ένθεσης. Η τιμή του P μεταβάλλεται παρόμοια με την εισαγωγή, ξεκινάει από S, αλλάζει σε -P-1 αν η τιμή του ήταν είναι θετική ή σε -P αν είχε αρνητική τιμή. Σε αυτό το παράδειγμα η τιμή του S είναι θετική.

Αρχικά εξάγουμε bit μηνύματος από τους συντελεστές με τιμή P ή P+1. Μετά την εξαγωγή από ένα συντελεστή επαναφέρουμε την τιμή του σε P. Αφού εξάγουμε τα bit μετατοπίζουμε αριστερά το ιστόγραμμα για τιμές μεγαλύτερες από P. Στη συνέχεια αλλάζει η τιμή του P και εξάγουμε bit μηνύματος από συντελεστές με τιμή P ή P-1, επαναφέρουμε την τιμή τους σε P και μετατοπίζουμε το ιστόγραμμα στα δεξιά για τιμές μικρότερες από P. Η εξαγωγή από ένα block σταματάει όταν το P πάρει την τιμή T και αυτή η διαδικασία σταματάει όταν έχουν ανακτηθεί όλα τα bit μηνύματος.

Καθώς η εισαγωγή του μηνύματος ξεκινάει από συντελεστές με τιμή T, ενώ η εξαγωγή από συντελεστές με τιμή S, τα bit που εξάγονται από ένα block έχουν λάθος σειρά. Μετά την εξαγωγή από κάθε block θα πρέπει να αλλάξει η σειρά τους από το τελευταίο στο πρώτο. Συνδυάζοντας τα bit που έχουμε εξάγει από το κάθε block της εικόνας, προκύπτει το μήνυμα που είχε εισαχθεί στην εικόνα.

Για παράδειγμα, έστω ότι θέλουμε να εξάγουμε το μήνυμα και να επαναφέρουμε το block όπου έγινε εισαγωγή του μηνύματος D. Ξεκινάμε από S = -4 και σταματάμε την εξαγωγή για T = 4.

1	-2	-1	3	-4
-5	0	5	-3	7
6	4	2	0	-7
-9	0	8	-6	5
0	0	-5	0	-10

Αρχικά, κάνουμε εξαγωγή bit από συντελεστές με τιμές -4, -5. Η προσπέλαση του block γίνεται από το τελευταίο προς το πρώτο κελί. Τα bit που εξάγονται είναι [1 1 0]. Μετά την εξαγωγή επαναφέρουμε την τιμή τους σε -4.

1	-2	-1	3	-4
-4	0	5	-3	7
6	4	2	0	-7
-9	0	8	-6	5
0	0	-4	0	-10

Αφού γίνει η εξαγωγή, μετατοπίζουμε το ιστόγραμμα στα δεξιά για τιμές μικρότερες από -4:

1	-2	-1	3	-4
-4	0	5	-3	7
6	4	2	0	-6
-8	0	8	-5	5
0	0	-4	0	-9

Στη συνέχεια, εξάγουμε τα bit μηνύματος από συντελεστές με τιμή 4, 5 και τα προσθέτουμε στο τέλος του πίνακα [1 1 0 1 0 1] :

1	-2	-1	3	-4
-4	0	4	-3	7
6	4	2	0	-6
-8	0	8	-5	4
0	0	-4	0	-9

Τέλος, μετατοπίζουμε αριστερά για τιμές μεγαλύτερες από 4:

1	-2	-1	3	-4
-4	0	4	-3	6
5	4	2	0	-6
-8	0	7	-5	4
0	0	-4	0	-9

Έχουμε επαναφέρει το block όπως ήταν πριν την ένθεση και έχουμε εξάγει όλα τα bit που είχαν εισαχθεί, αλλά σε λάθος σειρά. Αντιστρέφουμε τον πίνακα -> [1 0 1 0 1 1] και βλέπουμε πως τώρα οι τιμές του είναι ίδιες με αυτές του αρχικού μηνύματος D.

Κεφάλαιο 5: Αναστρέψιμη απόκρυψη πληροφορίας με ολίσθηση ιστογράμματος

Η τεχνική αναστρέψιμης απόκρυψης πληροφορίας του Huang16 [27] δουλεύει επίσης με ολίσθηση ιστογράμματος κάνοντας όμως μετατόπιση μόνο μία φορά. Σε αντίθεση όμως με την τεχνική που παρουσιάστηκε στο προηγούμενο κεφάλαιο, η οποία έκανε ένθεση των bit του μηνύματος σε μικρούς με μέτρο συντελεστές η τεχνική του Huang16 εισάγει το μήνυμα μόνο σε AC συντελεστές με μέτρο ένα έτσι ώστε η απόκρυψη πληροφορίας να γίνει με ελάχιστη παραμόρφωση στην εικόνα. Παρακάτω γίνεται περιγραφή της διαδικασίας ένθεσης του μηνύματος, των κριτηρίων για την επιλογή των block για την εισαγωγή, της ασφάλειας που μας παρέχει αυτή η τεχνική και της διαδικασίας εξαγωγής του μηνύματος και αποκατάστασης της εικόνας.

Επιλογή των Block για την ένθεση του μηνύματος

Έχει παρατηρηθεί ότι εισάγοντας το μήνυμα σε συγκεκριμένα block της εικόνας μπορεί να βελτιωθεί η ποιότητά της. Η επιλογή των block γίνεται πριν αρχίσει η εισαγωγή του μηνύματος.

Αφού υπολογιστεί ο μετασχηματισμός DCT και ο κβαντισμός των συντελεστών του για κάθε block της εικόνας, τα block μπορούν να χωριστούν σε δύο κατηγορίες, τα block που αντιστοιχούν σε ομοιόμορφες περιοχές της εικόνας (flat blocks) και τα block που αντιστοιχούν στις μη ομοιόμορφες περιοχές (textured blocks). Τα flat blocks περιέχουν περισσότερους μηδενικούς συντελεστές.

Η εισαγωγή του μηνύματος είναι καλύτερο να γίνεται σε block με πολλά μηδενικά. Σε αυτά τα block, επικρατούν οι συντελεστές με μέτρο ένα, οι οποίοι χρησιμοποιούνται για την ένθεση. Σε μπλοκ με λίγα μηδενικά υπάρχουν πολλοί AC συντελεστές με τιμές διάφορες του ένα οι οποίοι θα πρέπει να αλλάξουν τιμή κατά την ολίσθηση του ιστογράμματος, κάτι το οποίο θα υποβαθμίσει την ποιότητα της αρχικής εικόνας. Επίσης, δεδομένου ότι σε αυτά τα block δεν έχουμε πολλούς συντελεστές με μέτρο ένα, η ένθεση του μηνύματος πρέπει να γίνει σε περισσότερα block.

Για την επιλογή των block ένθεσης ορίζουμε μια τιμή T ($0 \leq T \leq 63$), η οποία καθορίζει τον ελάχιστο αριθμό μηδενικών που θα έχει ένα block στο οποίο θα γίνει εισαγωγή bit. Ξεκινώντας με T = 63 μετράμε τον αριθμό συντελεστών με μέτρο ένα στα block ένθεσης. Αν το σύνολο αυτών των συντελεστών δεν επαρκεί για την ένθεση, τότε μειώνουμε την τιμή T. Για να επιτύχουμε μέγιστο PSNR σε σχέση με την αρχική εικόνα, θα πρέπει η ένθεση να γίνει με τη χρήση της μέγιστη τιμής που μπορούμε να δώσουμε στο T.

Εισαγωγή του L και του T στα πρώτα block της εικόνας

Για να μπορεί να γίνει εξαγωγή του μηνύματος και επαναφορά της εικόνας θα πρέπει να είναι γνωστό το μήκος του μηνύματος σε bit (L) και ο ελάχιστος αριθμός μηδενικών που μπορεί

να έχει ένα block το οποίο περιέχει bit μηνύματος (T). Καθώς το μέγιστο μήκος του μηνύματος μπορεί να είναι 2^{24} bit και το μέγιστο T είναι 62 (ο DC όρος δεν μεταβάλλεται) δεσμεύουμε 24 bit για το L (l1) και 6 bit για το T (l2) και η εισαγωγή τους μπορεί να γίνει στα πρώτα block ένθεσης όπως περιγράφεται παρακάτω. Αφού γίνει η εισαγωγή των l1 και l2 εισάγουμε το μήνυμα (L) στα block ακολουθούν.

Ασφάλεια της τεχνικής

Η τεχνική του Huang16 εκτός από την διατήρηση της ποιότητας της εικόνας και του μεγέθους του αρχείου, εστιάζει επιπλέον και στην ασφάλεια. Αφού γίνει η επιλογή των block στα οποία θα γίνει η ένθεση, πριν αρχίσει η διαδικασία της εισαγωγής, γίνεται ανακάτεμα των AC συντελεστών. Το ανακάτεμα γίνεται με βάση ένα κλειδί και αφορά μόνο τα block που έχουν επιλεγεί για την ένθεση και μόνο μη μηδενικούς όρους. Στη συνέχεια γίνεται η ένθεση του μηνύματος όπως περιγράφεται παρακάτω. Αφού γίνει η ένθεση οι όροι επιστρέφουν στην αρχική τους θέση. Για να γίνει εξαγωγή του μηνύματος και επαναφορά της εικόνας απαιτείται το ίδιο κλειδί που χρησιμοποιήθηκε σε αυτό το στάδιο. Οι δημιουργοί της τεχνικής επισημαίνουν επίσης πως το ανακάτεμα των όρων θα μπορούσε να εφαρμοστεί και σε άλλες τεχνικές RDH με μεταβολή των DCT συντελεστών.

Σημειώνεται πως οι χρήστες σε μερικές εφαρμογές του RDH κρυπτογράφουν το μήνυμα πριν κάνουν την ένθεση. Με αυτήν την τεχνική προστίθεται ένα ακόμα επίπεδο ασφάλειας ή μπορεί να παραλειφθεί το βήμα της κρυπτογράφησης, αν οι χρήστες θεωρούν ότι το κλειδί με το οποίο έγινε το ανακάτεμα είναι αρκετά ασφαλές.

Εισαγωγή του μηνύματος

Αφού έχει γίνει επιλογή των block και ανακάτεμα των AC συντελεστών, γίνεται εισαγωγή του μηνύματος. Οι τιμές στους συντελεστές του block αλλάζουν το πολύ κατά ένα και η προσπέλαση των όρων στο block γίνεται σειριακά. Αρχικά γίνεται αύξηση κατά μία τιμή του μέτρου των συντελεστών με τιμή μεγαλύτερη από ένα, έτσι ώστε να ξεχωρίζουν από τους όρους στους οποίους έχει γίνει ένθεση. Στους συντελεστές με μέτρο ίσο με την μονάδα, γίνεται αύξηση του μέτρου τους για εισαγωγή bit με τιμή 1 ενώ για εισαγωγή bit με τιμή 0 το μέτρο τους μένει σταθερό. Η διαδικασία περιγράφεται επίσης με τους εξής τύπους:

$$\text{ACsign} = \begin{cases} AC + sign(AC) * b \text{ για } |\text{AC}| = 1 \\ AC + sign(AC) \text{ για } |\text{AC}| > 1 \end{cases}$$

Όπου:

- AC είναι ένας AC συντελεστής πριν την ένθεση
- Ο AC_{sign} είναι ο AC συντελεστής μετά την ένθεση
- Το b ένα bit μηνύματος.

και η συνάρτηση sign η οποία καθορίζει την αύξηση του μέτρου του AC συντελεστή ανάλογα με το πρόσημό του:

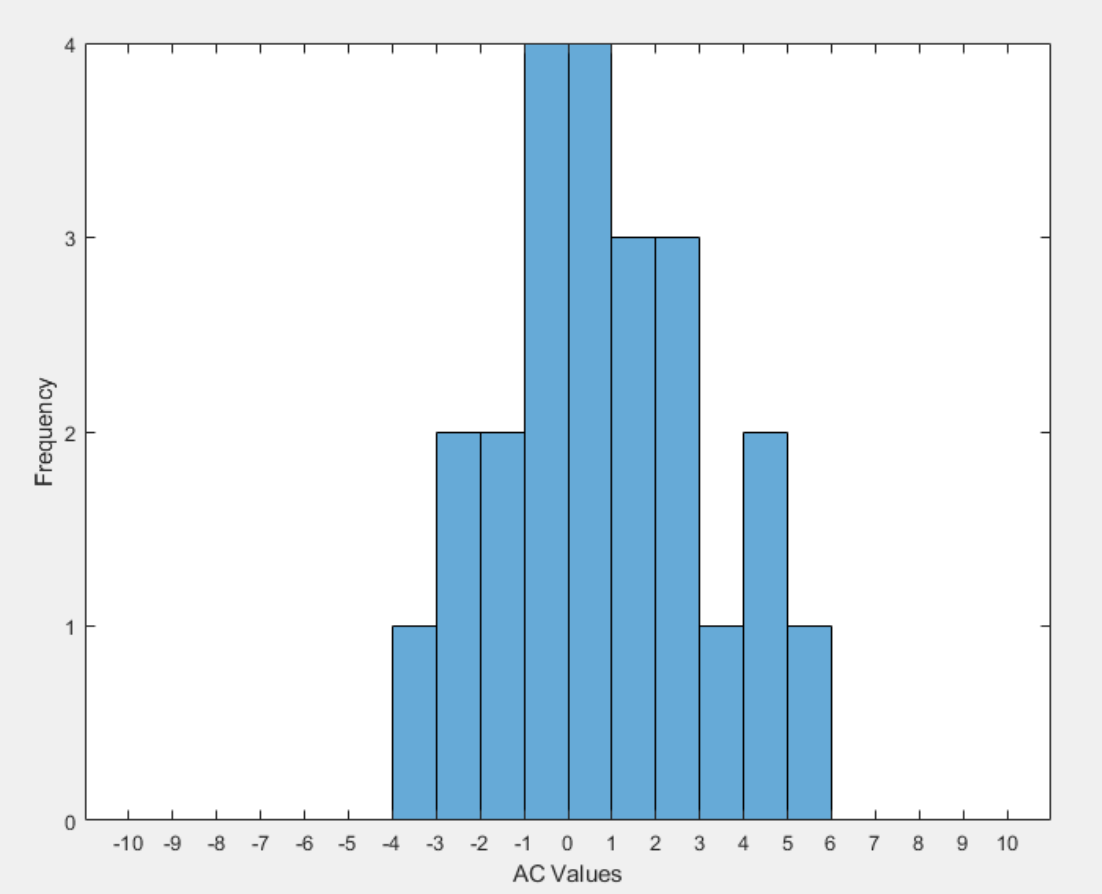
$$\text{sign}(\text{x}) = \begin{cases} 1\ \gamma\iota\alpha\ \text{x} > 0 \\ 0\ \gamma\iota\alpha\ \text{x} = 0 \\ -1\ \gamma\iota\alpha\ \text{x} < 0 \end{cases}$$

Για παράδειγμα έστω ότι έχουμε ένα block 6x4 με κβαντισμένους DCT συντελεστές και το μήνυμα που πρόκειται να εισαχθεί είναι το εξής: C = [1101101].

63	4	-1	0	-4	1
4	-3	0	1	2	-3
-1	-2	0	2	-1	0
-2	1	2	3	-1	5

Πίνακας 3 Για το παράδειγμα της ένθεσης γίνεται χρήση ενός υποθετικού block 6x4 για λόγους ευκολίας. Η διαδικασία είναι η ίδια και για block με διαστάσεις 8x8.

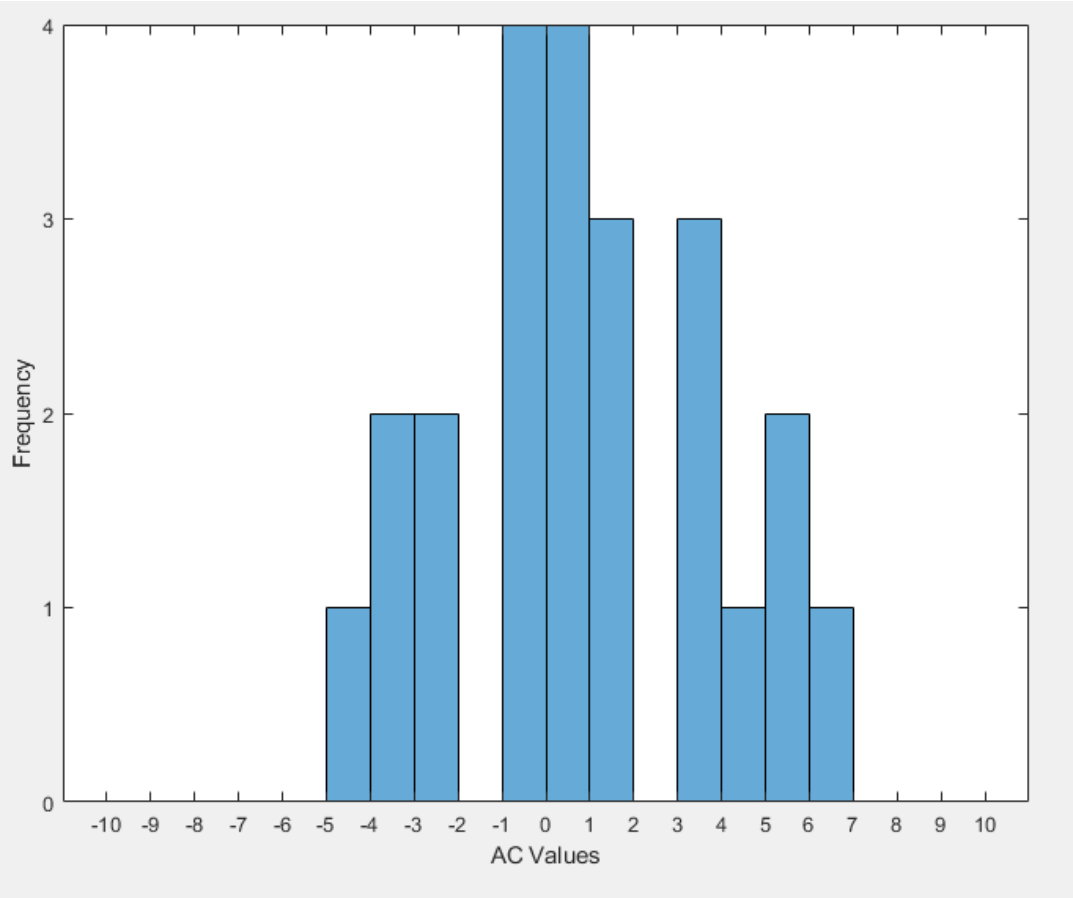
Και το ιστόγραμμα των AC συντελεστών του έχει αυτή τη μορφή:



Πρώτα μεταβάλουμε τους συντελεστές με μέτρο μεγαλύτερο από ένα. Μετά την μετατόπιση οι συντελεστές στο block έχουν τις εξής τιμές:

63	5	-1	0	-5	1
5	-4	0	1	3	-4
-1	-3	0	3	-1	0
-3	1	3	4	-1	6

Και δημιουργείται επίσης ένα κενό στο ιστόγραμμα:

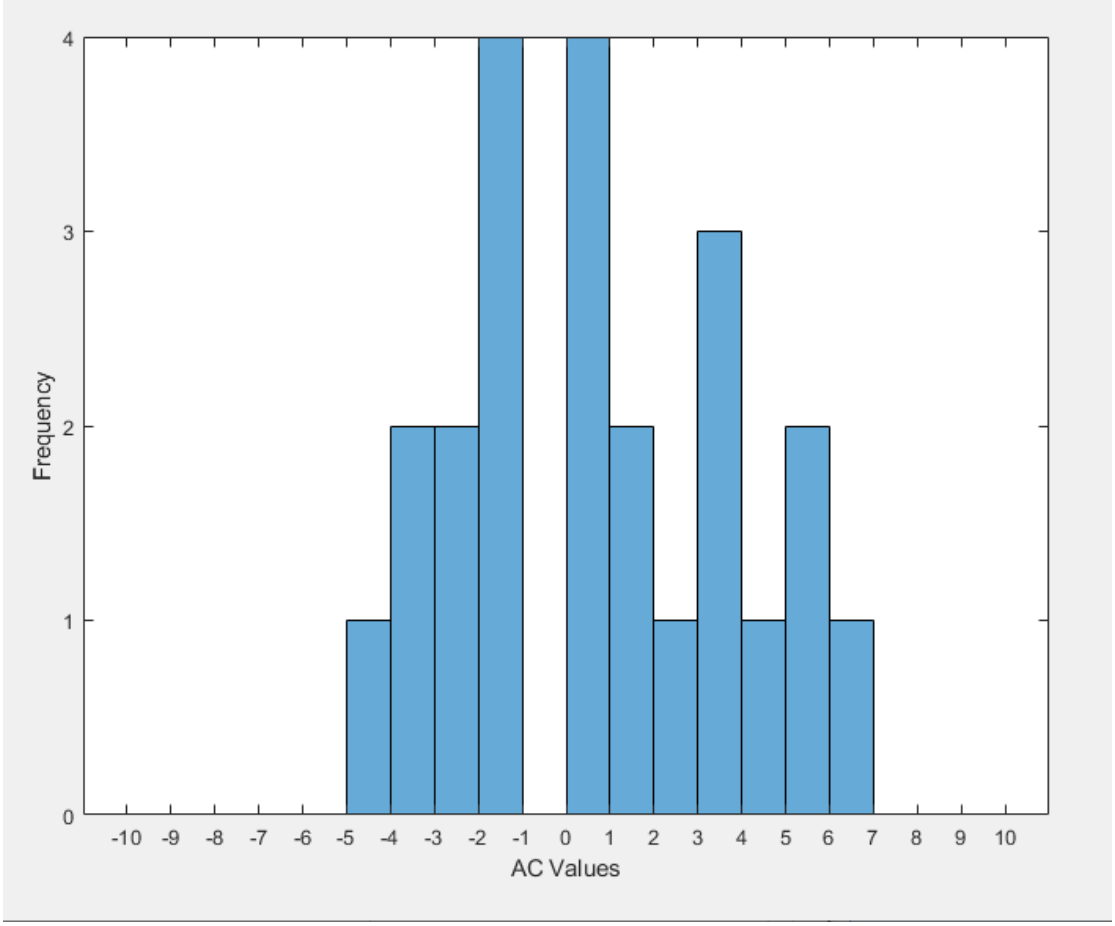


Στη συνέχεια εισάγουμε το μήνυμα C σε συντελεστές με μέτρο ένα:

63	5	-2	0	-5	2
5	-4	0	1	3	-4
-2	-3	0	3	-2	0
-3	1	3	4	-2	6

Παρατηρούμε πως ο DC όρος και τα κελιά με τιμή μηδέν δεν μεταβάλλονται.

Μετά την ένθεση το ιστόγραμμα έχει αυτή τη μορφή:



Εξαγωγή του μηνύματος και επαναφορά της εικόνας

Για να εξάγει κάποιος το μήνυμα θα πρέπει να έχει το κλειδί με το οποίο έχει γίνει το ανακάτεμα των AC όρων. Αφού γίνει εισαγωγή του κλειδιού, γίνεται εύρεση του μήκους του μηνύματος σε bit (L) και του ελάχιστου αριθμού μηδενικών που μπορεί να έχει ένα block το οποίο περιέχει bit μηνύματος (T), από τα πρώτα block της εικόνας. Στη συνέχεια στα block με αριθμό μηδενικών μεγαλύτερων από T και με βάση το κλειδί ανακατέματος, οι μη μηδενικοί AC συντελεστές μετατοπίζονται στη θέση που ήταν όταν έγινε η εισαγωγή του μηνύματος. Η εξαγωγή του μηνύματος γίνεται κάνοντας προσπέλαση των block της εικόνας και ελέγχοντας τον αριθμό μηδενικών σε αυτά.

Όταν βρεθεί ένα block με αριθμό μηδενικών μεγαλύτερο από T, γίνεται πρώτα εξαγωγή των bit μηνύματος από αυτό. Οι συντελεστές που κρατάνε bit μηνύματος με τιμή μηδέν είναι αυτοί που έχουν μέτρο ίσο με ένα, και οι συντελεστές με μέτρο ίσο με δύο κρατάνε bit με τιμή ένα. Όταν συναντάμε αυτούς τους συντελεστές, αποθηκεύουμε το bit που αντιστοιχεί σε αυτούς, και η τιμή του μέτρου τους αλλάζει σε ένα διατηρώντας το πρόσημο τους. Σε αντίθεση με την

προηγούμενη τεχνική τα bit έχουν την ίδια σειρά που είχαν πριν την εισαγωγή. Μετά την εξαγωγή του μηνύματος γίνεται επαναφορά της αρχικής τιμής στους υπόλοιπους AC συντελεστές, οι οποίοι έχουν μέτρο μεγαλύτερο από ένα. Σε αυτούς τους συντελεστές, γίνεται μείωση του μέτρου τους κατά μία τιμή. Τέλος, όταν έχει γίνει εξαγωγή των bit μηνύματος και επαναφορά των συντελεστών από όλα τα block της εικόνας, οι μη μηδενικοί AC συντελεστές γυρνάνε στην αρχική τους θέση. Σε αυτό το σημείο έχει γίνει εξαγωγή του μηνύματος και αποκατάσταση της εικόνας.

Η εξαγωγή του μηνύματος μπορεί περιγράφεται επίσης με τους εξής τύπους:

$$b = \begin{cases} 0\ \gamma\iota\alpha\ |\mathrm{ACsign}| = 1 \\ 1\ \gamma\iota\alpha\ |\mathrm{ACsign}| = 2 \end{cases}$$

$$\mathrm{AC_{rest}} = \begin{cases} \mathrm{sign(ACsign)}\ \gamma\iota\alpha\ 1 \le |\mathrm{ACsign}| \le 2 \\ \mathrm{ACsign} - \mathrm{sign(ACsign)}\ \gamma\iota\alpha\ |\mathrm{ACsign}| \ge 3 \end{cases}$$

Όπου b είναι ένα bit μηνύματος που έχουμε εξάγει από την εικόνα, ο AC_{sign} ένας AC συντελεστής που έχει μεταβληθεί για την ένθεση του μηνύματος AC_{rest} ένας AC συντελεστής μετά την εξαγωγή του μηνύματος.

Για παράδειγμα έστω ότι θέλουμε να εξάγουμε το μήνυμα από το block όπου έγινε η εισαγωγή του μηνύματος C:

63	5	-2	0	-5	2
5	-4	0	1	3	-4
-2	-3	0	3	-2	0
-3	1	3	4	-2	6

Αρχικά εξάγουμε το μήνυμα από συντελεστές με μέτρο ένα και δύο. Αφού εξάγουμε τα bit μηνύματος αλλάζουμε το μέτρο τους σε ένα. Το block μετά την εξαγωγή του μηνύματος C έχει αυτή τη μορφή:

63	5	-1	0	-5	1
5	-4	0	1	3	-4
-1	-3	0	3	-1	0
-3	1	3	4	-1	6

Στη συνέχεια στους συντελεστές με μέτρο μεγαλύτερο του ένα και εκτός του DC όρου, γίνεται μείωση του μέτρου τους κατά μία τιμή:

63	4	-1	0	-4	1
4	-3	0	1	2	-3
-1	-2	0	2	-1	0
-2	1	2	3	-1	5

Σε αυτό το σημείο, έχουμε επαναφέρει τις τιμές των AC συντελεστών και έχουμε εξάγει το μήνυμα C= [1 1 0 1 1 0 1].

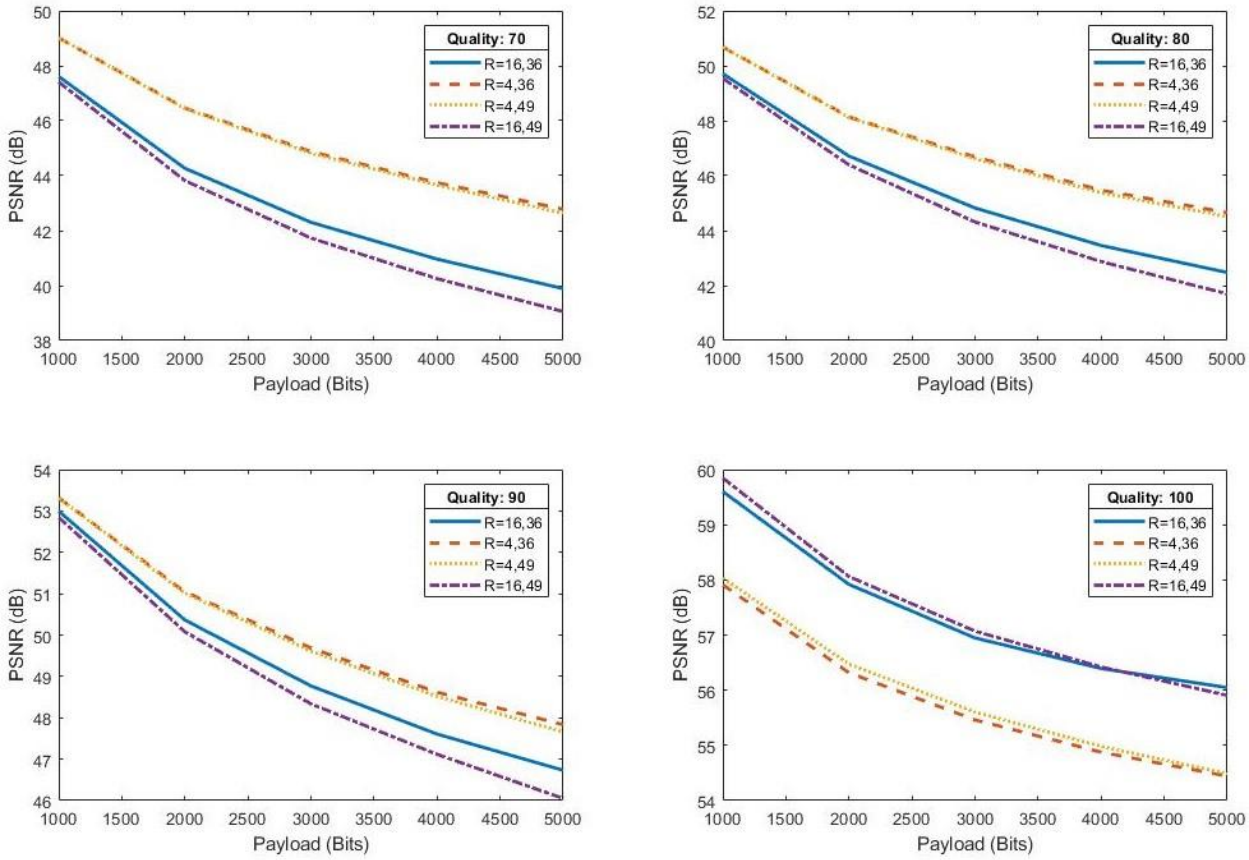
Κεφάλαιο 6: Πειραματικά αποτελέσματα

Παρακάτω γίνονται πειράματα για την επιλογή των παραμέτρων με τις οποίες μπορούμε να επιτύχουμε την καλύτερη απόδοση για την κάθε τεχνική ξεχωριστά και γίνεται σύγκριση της μεταβολής του PSNR και του μεγέθους του αρχείου ανάλογα με το μήκος μηνύματος μεταξύ των δύο τεχνικών, για να συμπεράνουμε ποια τεχνική είναι καλύτερη ή ποια τεχνική μπορεί να χρησιμοποιηθεί ανάλογα με την περίπτωση.

Επιλογή παραμέτρων για την 1η τεχνική

Το RDH βρίσκει εφαρμογή σε ιατρικές εικόνες όπου πριν την διαμοίραση τους, προστίθεται σε αυτές ένα Knowledge Digest (πίνακας πληροφοριών). Το Knowledge Digest περιέχει όλες τις λεπτομέρειες για την εικόνα και χρησιμοποιείται για την εύρεση παρόμοιων εικόνων. Σύμφωνα με τον Coatrieux et. al. [28] ένα Knowledge Digest συνήθως έχει μέγεθος 1000 – 2000 bit, με μέγιστο μέγεθος 3500 bit. Για την επιλογή των παραμέτρων o1, o2 για την τεχνική του Xuan07, γίνονται πειράματα για τέσσερεις περιοχές R = {o1, o2} με διαφορετικά quality factor, και επιλέγουμε την περιοχή με την οποία μπορούμε να επιτύχουμε καλύτερο PSNR για την ένθεση μηνύματος μέχρι και 3000 bit. Οι περιοχές αυτές είναι οι R1 = {16, 36}, R2 = {4, 36}, R3 = {4,49}, R4 = {16,49}.

Για QF = 70, 80, 90, 100 ενθέτουμε 1000 - 5000 bit:



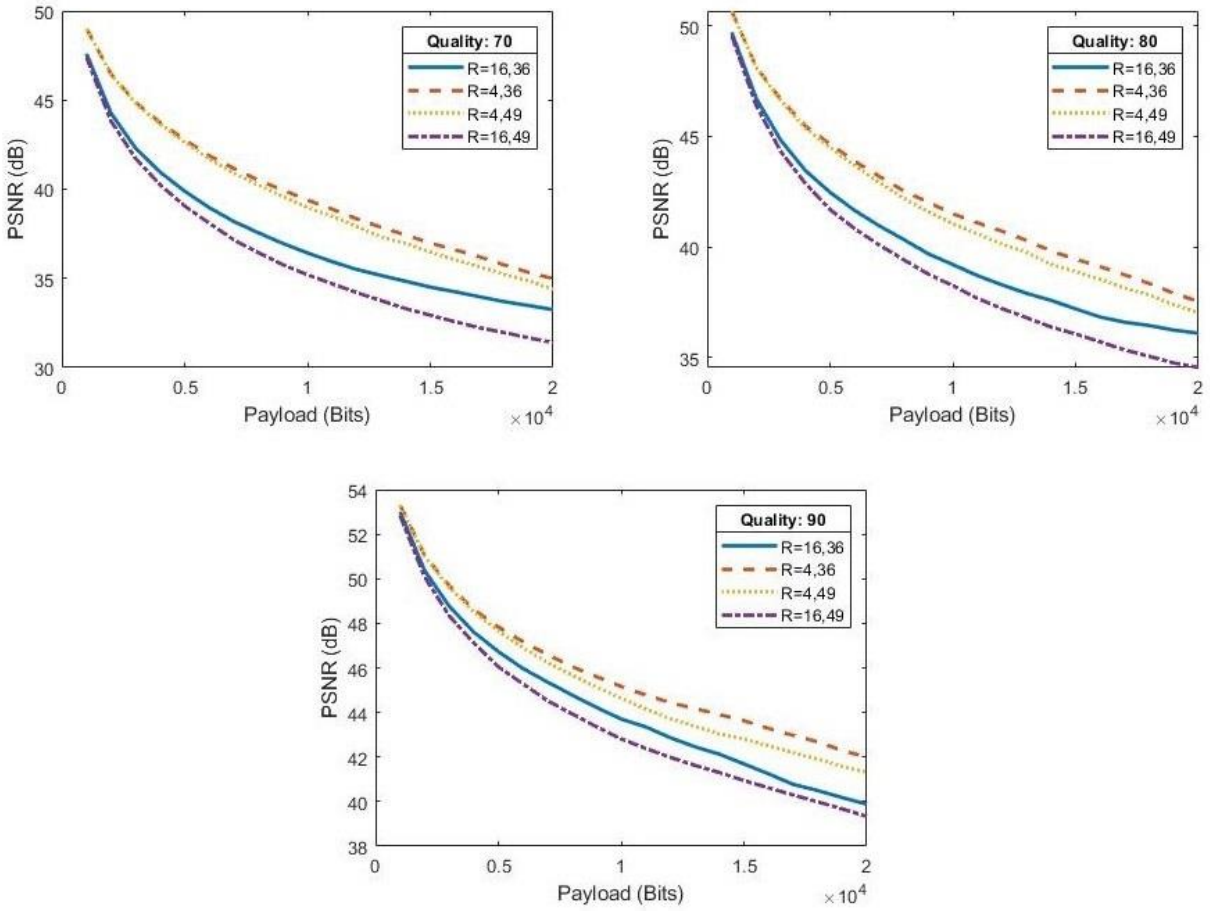
Σχήμα 6.1 Μεταβολή του PSNR μετά την εισαγωγή 1000 - 5000 bit για 4 περιοχές o1, o2 και για Quality Factor 70, 80, 90, 100

Παρατηρούμε πως για quality factor: 70, 80, 90 η περιοχή R = {4,36} μας δίνει το υψηλότερο PSNR σε σχέση με τις υπόλοιπες περιοχές. Οπότε για ποιότητα εικόνας ανάμεσα σε αυτές τις τιμές και για μηνύματα μήκους μέχρι 3000 bit επιλέγεται αυτή η περιοχή.

Τα αποτελέσματα φαίνεται να είναι διαφορετικά για quality factor = 100. Η περιοχή R = {16, 49} μας δίνει το υψηλότερο PSNR ενώ η περιοχή R = {4, 36} που προηγουμένως μας έδινε υψηλότερο PSNR από τις άλλες περιοχές, τώρα μας δίνει το χαμηλότερο. Καθώς ο πίνακας κβαντισμού για αυτό το quality factor αποτελείται από άσσους δεν γίνεται συμπίεση στους DCT συντελεστές και για αυτό τα αποτελέσματα που βλέπουμε στο παραπάνω διάγραμμα καθώς και στα παρακάτω διαγράμματα διαφέρουν από αυτά που επιτυγχάνονται με άλλα quality factor.

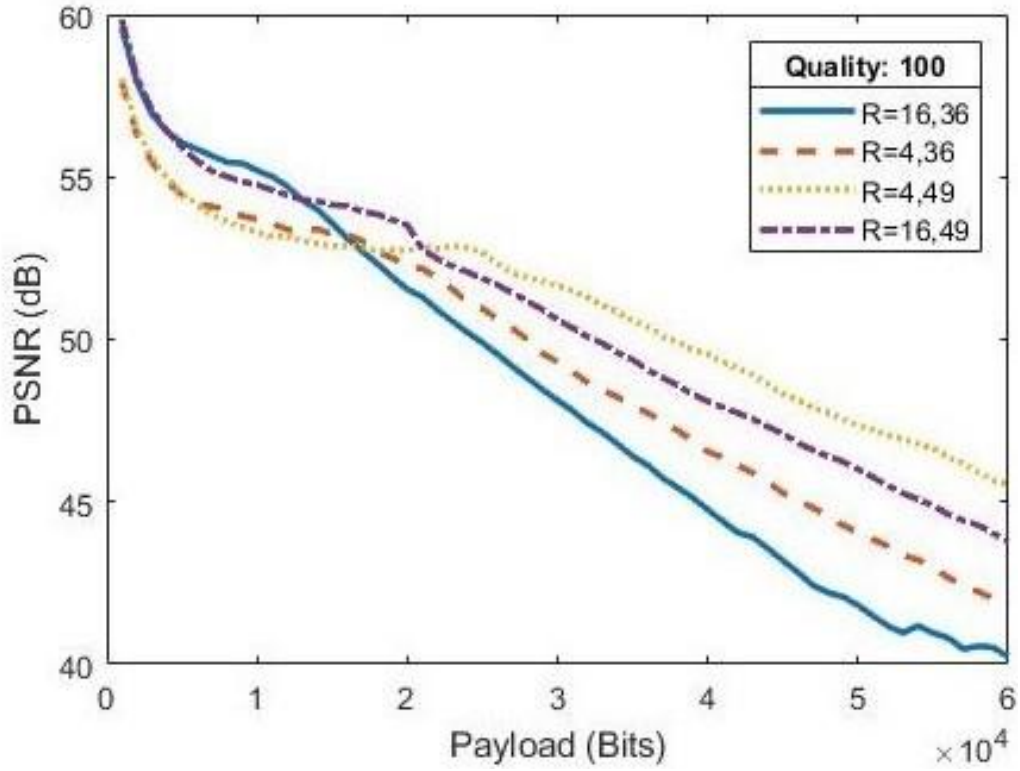
Στη συνέχεια γίνονται πειράματα για εισαγωγή μηνύματος για παραπάνω από 10.000 bit μηνύματος.

Για QF = 70, 80, 90, 100 και 1000 – 60.000 bit:



Σχήμα 6.2 Μεταβολή του PSNR μετά την εισαγωγή 1000 - 20000 bit για 4 περιοχές o1, o2 και για Quality Factor 70, 80, 90, 100

Οπότε, καθώς η περιοχή R = {4, 36} μας δίνει υψηλότερο PSNR για quality factor 70, 80 και 90 θα χρησιμοποιηθεί όταν γίνεται ένθεση έως και 20.000 bit.



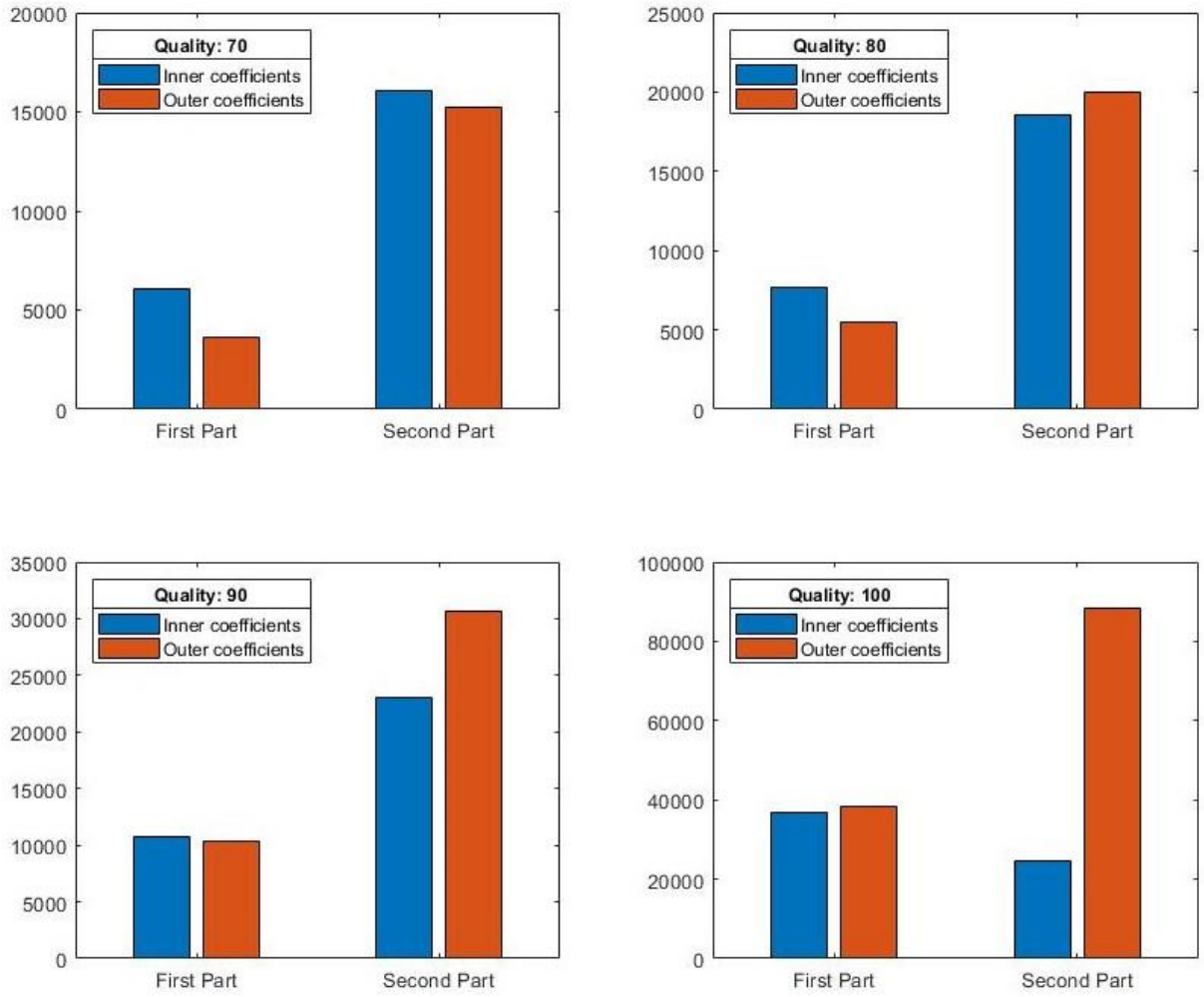
Σχήμα 6.3 Μεταβολή του PSNR μετά την εισαγωγή 1000 - 60000 bit για 4 περιοχές ο1, ο2 και για Quality Factor 100

Οπότε, καθώς η περιοχή R = {4, 49} μας δίνει καλύτερο PSNR για quality factor 100 όταν ενθέτουμε περισσότερα από 10.000 bit μηνύματος στην εικόνα, θα χρησιμοποιηθεί στα επόμενα πειράματα για αυτή την ποιότητα εικόνας και για την σύγκριση με την τεχνική του Huang16.

Επιλογή AC συντελεστών για την τεχνική του Huang16

Στη συνέχεια γίνονται πειράματα για την επιλογή των block για την τεχνική του Huang16. Καθώς η τεχνική αυτή αξιοποιεί AC συντελεστές με μέτρο ένα θα πρέπει να επιλέξουμε block τα οποία έχουν τους περισσότερους συντελεστές με αυτή την τιμή. Αρχικά συμπιέζουμε 1000 εικόνες με διαστάσεις 512 x 512 και quality factor 70, 80, 90, 100. Οι εικόνες με αυτές τις διαστάσεις έχουν 4096 block (8 x 8). Στη συνέχεια χωρίζουμε αυτά τα block σε δύο μέρη (δηλαδή σε κάθε μέρος έχουμε 2048 block) με βάση τον αριθμό μηδενικών τους, όπου στο πρώτο μέρος έχουμε τα block με πολλά μηδενικά και στο δεύτερο τα block με τα λιγότερα μηδενικά. Στη συνέχεια γίνονται διαγράμματα και για τα δύο μέρη ξεχωριστά, για κάθε quality factor,όπου φαίνονται για το κάθε μέρος ο αριθμός των AC συντελεστών με μέτρο ένα και ο αριθμός των συντελεστών με μέτρο μεγαλύτερο του ένα.

Για quality factor 70, 80, 90, 100:

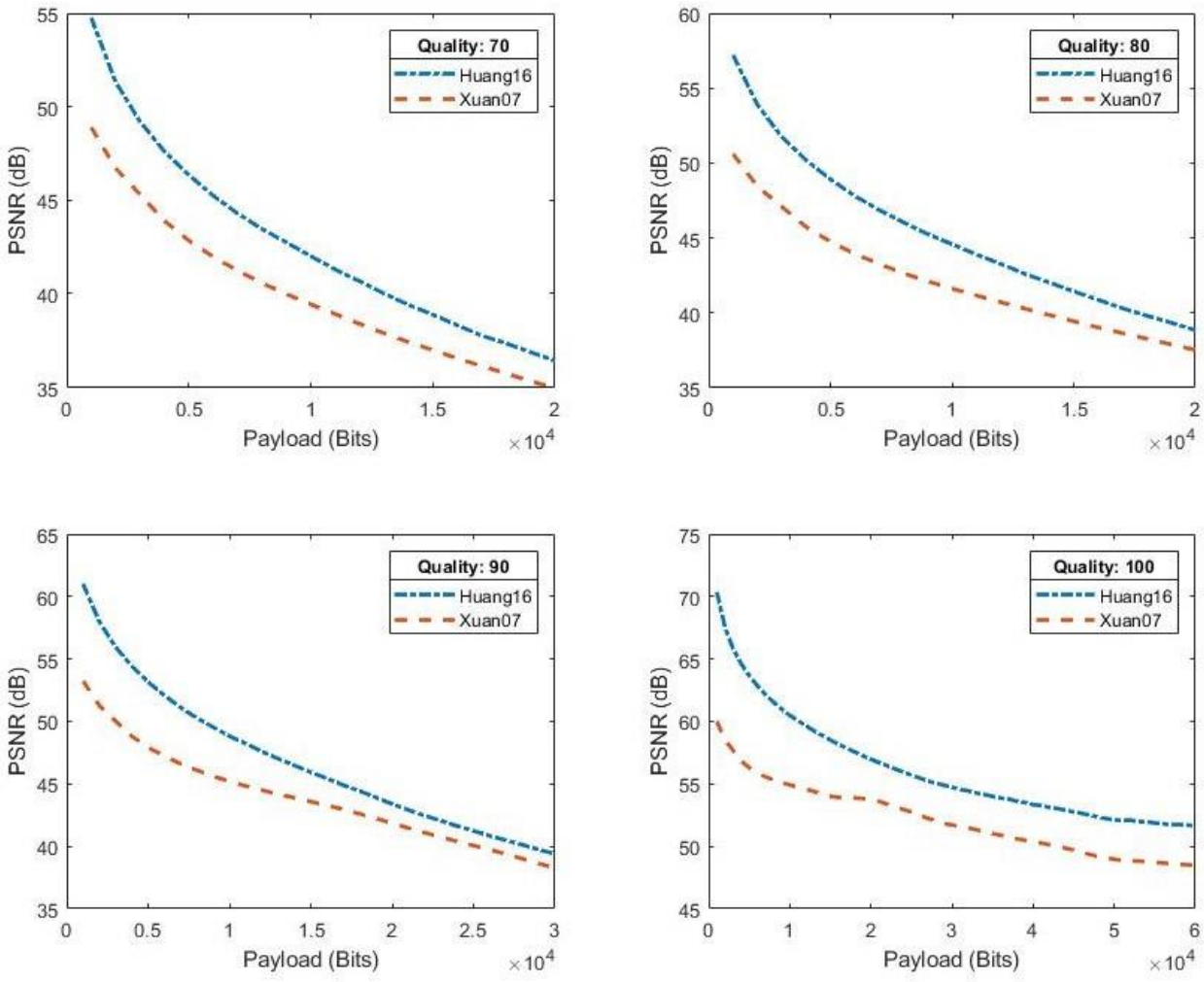


Σχήμα 6.4 Οι Inner Coefficients μας δείχνουν τον αριθμό AC συντελεστών με μέτρο 1 ενώ οι outer coefficients τους συντελεστές με μέτρο μεγαλύτερο από ένα.

Οι συντελεστές με μέτρο ένα, στο πρώτο μέρος με τα περισσότερα μηδενικά, είναι περισσότεροι από τους υπόλοιπους συντελεστές. Στο δεύτερο μέρος με τα λιγότερα μηδενικά, οι συντελεστές με μέτρο μεγαλύτερο από ένα είναι περισσότεροι από αυτούς με μέτρο ένα. Σε αυτούς τους συντελεστές δεν γίνεται εισαγωγή bit μηνύματος αλλά η μετατόπιση που γίνεται σε αυτούς μπορεί να αλλοιώσει την ποιότητα της εικόνας. Οπότε η ένθεση πρέπει να δίνει προτεραιότητα στα block στο πρώτο μέρος. Τα block στο δεύτερο μέρος αξιοποιούνται μόνο όταν γίνεται ένθεση μεγάλου μήκους μηνύματος και αφού έχει γίνει ένθεση στο πρώτο μέρος.

Μεταβολή του PSNR σε σχέση με το μήκος μηνύματος

Παρακάτω γίνεται σύγκριση της ποιότητας των δύο τεχνικών μετά την ένθεση για διάφορα quality factor και διαφορετικό μήκος μηνύματος για 200 εικόνες. Σε κάθε εικόνα γίνεται εισαγωγή από 1000 μέχρι 20.000, 30.000 ή 60.000 bit ανάλογα με το quality factor. Για την τεχνική του Xuan07 χρησιμοποιείται για την ένθεση η περιοχή R που επιλέχθηκε στα πειράματα παραπάνω και για την τεχνική του Huang16 η εισαγωγή γίνεται στα block με τα περισσότερα μηδενικά.



Σχήμα 6.5 Σύγκριση των δύο τεχνικών κάνοντας ένθεση μηνύματος από 1000 μέχρι 60000 bit σε 100 εικόνες και για quality factor 70,80,80, 100

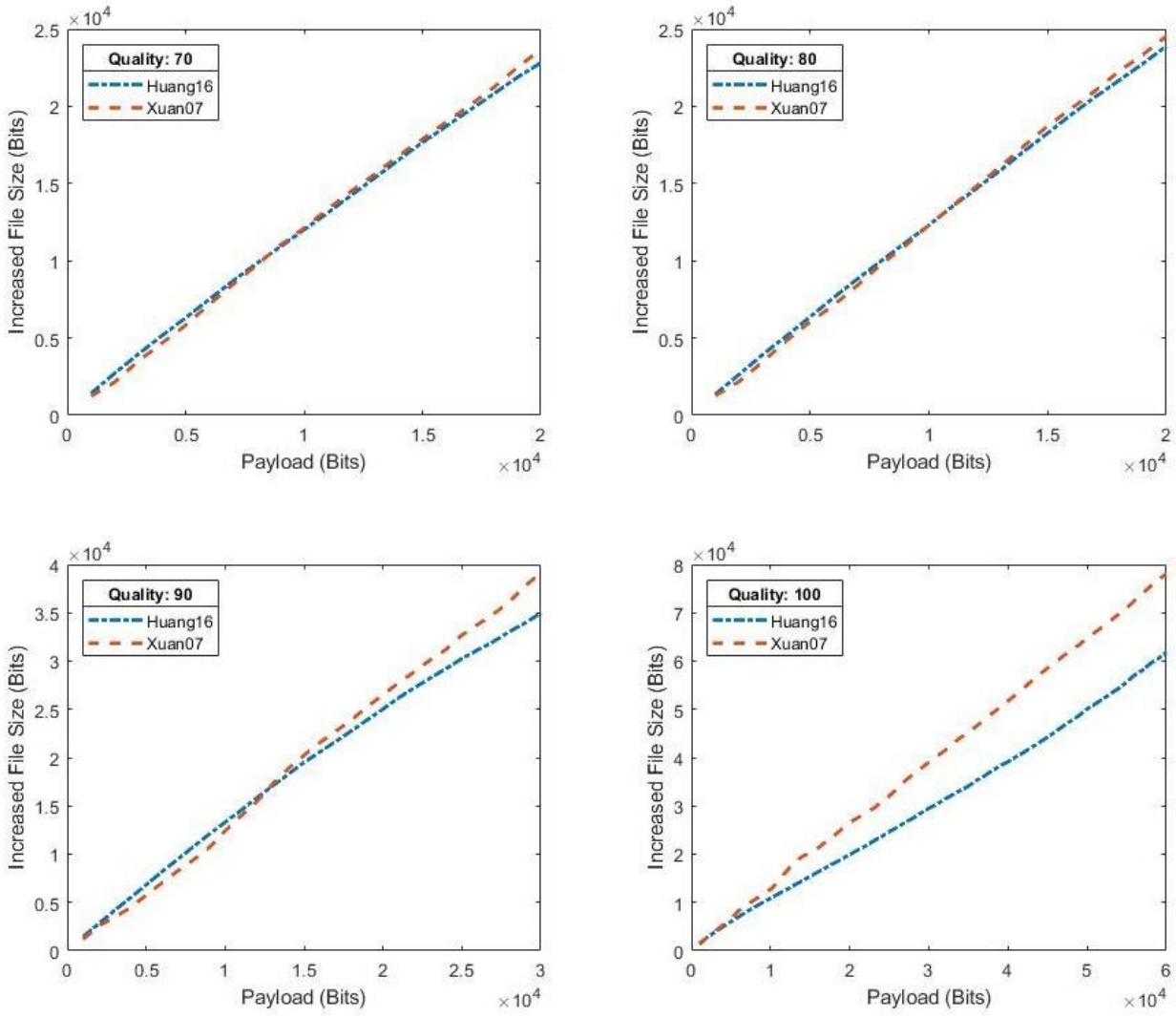
Στα διαγράμματα παραπάνω φαίνεται πως η τεχνική του Huang16 είναι πιο αποδοτική από αυτή του Xuan07 όσον αφορά την ποιότητα της εικόνας. Ωστόσο για αρκετές εικόνες οι οποίες επιλέχθηκαν για τα πειράματα, η εισαγωγή δεν ήταν δυνατή με την τεχνική του Huang16. Ο λόγος ήταν πως αυτές οι εικόνες δεν είχαν αρκετούς συντελεστές με τιμές με μέτρο ένα τους οποίους αξιοποιεί η συγκεκριμένη τεχνική, οπότε δεν μπορούσε να γίνει ένθεση πάνω από 10.000 bit σε αυτές. Η τεχνική του Xuan07 δεν έχει αυτό το πρόβλημα, καθώς η ένθεση μπορεί

να γίνει σε οποιονδήποτε AC συντελεστή. Τα αποτελέσματα για αυτές τις εικόνες δεν συμπεριλήφθηκαν στην παραγωγή των καμπυλών στο Σχήμα 6.5. Και για τις δύο τεχνικές χρησιμοποιήθηκαν οι ίδιες εικόνες.

Αύξηση του μεγέθους αρχείου

Στη συνέχεια, γίνεται σύγκριση της αύξησης του μεγέθους αρχείου για τις δύο τεχνικές, για 200 εικόνες. Σε κάθε εικόνα, γίνεται εισαγωγή από 1000 μέχρι 20.000, 30.000 ή 60.000 bit, ανάλογα με το quality factor. Οι εικόνες που δεν χρησιμοποιήθηκαν πριν για την τεχνική του Huang16, δεν χρησιμοποιήθηκαν ούτε εδώ.

Για quality factor 70, 80, 90, 100:



Σχήμα 6.6 Αύξηση του μεγέθους αρχείου 100 εικόνων για εισαγωγή μηνύματος από 1000 μέχρι 60000 bit και quality factor 70, 80, 90, 100

Από τα παραπάνω αποτελέσματα παρατηρούμε πως στις περισσότερες περιπτώσεις στην τεχνική του Huang16 το μέγεθος του αρχείου παραμένει μικρότερο από αυτό του Xuan07. Η τεχνική του Xuan βέβαια μπορεί να μας δώσει καλύτερη απόδοση σε μερικές περιπτώσεις. Ωστόσο η τεχνική αυτή μπορεί να αξιοποιήσει και μη μηδενικούς συντελεστές κάτι που αυξάνει αρκετά το μέγεθος του αρχείου. Καθώς η τεχνική του Huang16 έχει την καλύτερη απόδοση από τις δύο προτείνεται η χρήση της στις περισσότερες περιπτώσεις, ενώ η χρήση της τεχνικής του Xuan07 προτείνεται σε περιπτώσεις όπου η τεχνική του Huang16 δεν μπορεί να εφαρμοστεί.

Κεφάλαιο 7: Συμπεράσματα

Στην παρούσα διπλωματική εργασία υλοποιήθηκαν δύο τεχνικές για την αναστρέψιμη εισαγωγή πληροφορίας σε εικόνες JPEG. Οι τεχνικές αυτές εφαρμόστηκαν σε grayscale JPEG εικόνες και συγκεκριμένα σε κβαντισμένους DCT συντελεστές. Με την χρήση αυτών των τεχνικών, ο χρήστης μπορεί να κάνει ένθεση ενός μηνύματος μήκους από 1.000 μέχρι και 60.000 bit ανάλογα με το quality factor της εικόνας. Για την εισαγωγή ενός μηνύματος απαιτείται η διεύθυνση της εικόνας στον δίσκο, το ίδιο το μήνυμα σε bit και ένα κλειδί που επιλέγεται από τον χρήστη (μόνο για την τεχνική του Huang16). Προαιρετικά μπορούν να γίνουν αλλαγές στις παραμέτρους ένθεσης, οι οποίες επιτρέπουν καλύτερη απόδοση ή την ένθεση μεγαλύτερου μήκους μηνύματος.

Στα πλαίσια αυτής της διπλωματικής έγιναν πειράματα για την εύρεση των καλύτερων παραμέτρων για την ένθεση και για την σύγκριση των δύο τεχνικών. Αυτά αφορούσαν συγκρίσεις της μεταβολής του PSNR και του μεγέθους του αρχείου ανάλογα με το μήκος του μηνύματος που προστίθεται στην εικόνα. Επίσης υπήρξαν συγκρίσεις μεταξύ των τιμών και των θέσεων των συντελεστών στα block της εικόνας, οι οποίοι μεταβάλλονται κατά την ένθεση. Από αυτά καταλήξαμε πως η περιοχή σε zigzag διάταξη που μας δίνει καλύτερη απόδοση στην τεχνική του Xuan07 είναι η R = {4, 36}. Για την τεχνική του Huang16 κάνουμε ένθεση μόνο σε συντελεστές με μέτρο ένα και με προτεραιότητα στα block με πολλούς AC συντελεστές με τιμή μηδέν. Από την σύγκριση των δύο τεχνικών διαπιστώθηκε πως η τεχνική του Huang16 έχει καλύτερη απόδοση από αυτή του Xuan07, τόσο στην ποιότητα της εικόνας, όσο και στο μέγεθος του αρχείου. Το μόνο μειονέκτημα της τεχνικής είναι πως αν μία εικόνα δεν περιέχει αρκετούς DCT συντελεστές με τιμή με μέτρο ένα η ένθεση είναι αδύνατη, ενώ με την τεχνική του Xuan07 η ένθεση είναι δυνατή ανεξαρτήτως της τιμής των συντελεστών.

Προτεινόμενες επεκτάσεις των τεχνικών που υλοποιήθηκαν

Οι τεχνικές που παρουσιάστηκαν και υλοποιήθηκαν σε αυτή τη διπλωματική εργασία θα μπορούσαν να έχουν τις ακόλουθες επεκτάσεις ή βελτιώσεις:

- **Κρυπτογράφηση του μηνύματος πριν την ένθεση:** Όπως αναφέρθηκε στα προηγούμενα κεφάλαια, πολλοί χρήστες επιθυμούν το μήνυμα που εισάγουν σε μία εικόνα να είναι κρυπτογραφημένο. Άρα θα μπορούσε να χρησιμοποιηθεί κάποιος αλγόριθμος κρυπτογράφησης πριν την διαδικασία της ένθεσης και η αντίστοιχη αποκρυπτογράφηση μετά την εξαγωγή του μηνύματος από την εικόνα.
- **Αξιοποίηση της πληροφορίας χρώματος για την εισαγωγή πληροφορίας:** Οι τεχνικές που υλοποιήθηκαν σε αυτή τη διπλωματική εφαρμόζονται μόνο σε grayscale εικόνες. Για την εφαρμογή τους σε έγχρωμες εικόνες θα πρέπει να γίνει πρώτα μετατροπή των

εικόνων στο χρωματικό μοντέλο $Y'C_BC_R$ για να διαχωριστεί η πληροφορία του χρώματος και μετά να γίνει εισαγωγή του υδατογραφήματος στην συνιστώσα Y.

- **Μείωση του χρόνου εκτέλεσης των τεχνικών:** Για τη βελτίωση της απόδοσης των αλγορίθμων όσον αφορά το χρόνο εκτέλεσης, η ένθεση και η εξαγωγή του μηνύματος μπορούν να επιταχυνθούν, αν εκμεταλλευτούμε την παράλληλη επεξεργασία δεδομένων που προσφέρει η GPU (Graphics Processing Unit, Μονάδα Επεξεργασίας Γραφικών). Δεδομένου κιόλας ότι οι διαδικασίες συμπίεσης / αποσυμπίεσης εφαρμόζονται σε block της εικόνας, είναι προφανές ότι είναι εφικτός ο παράλληλος προγραμματισμός τους.
- **Βελτιστοποίηση των τεχνικών με στόχο την υλοποίηση τους σε υλικό με χαμηλό κόστος:** Σε αρκετές ασύρματες εφαρμογές, τα κρίσιμα προς μετάδοση δεδομένα είναι εικόνες και για την αυθεντικοποίηση τους μπορεί να χρησιμοποιηθεί RDH. Προκειμένου να αντιμετωπιστούν προβλήματα περιορισμών στους πόρους ή/και στην κατανάλωση ισχύος (π.χ σε κόμβους ασύρματων δικτύων), είναι απαραίτητη η μετάβαση στο υλικό, με χαμηλό κόστος.

Κεφάλαιο 8: Βιβλιογραφία

[1] V. T. a. R. A. Ahmad Shaik, «Data Security Through Data Hiding in Images: A Review».

[2] Y. Q. Shi, Reversible Data Hiding.

[3] Wikipedia, Caesar cipher.

[4] Wikipedia, «Scytale».

[5] defencegr, Η στεγανογραφία του Ιστιαίου του Μιλήσιου.

[6] C. B. V. R. Catherine Taylor Clelland, Hiding messages in DNA microdots.

[7] Shi, Y.-Q., Li, X., Zhang, X., Wu, H.-T., & Ma, B. (2016). Reversible data hiding: Advances in the past two decades. IEEE Access, 4, 3210–3237. doi:10.1109/access.2016.2573308.

[8] D. B. a. T.-h. K. Poulami Dutta, Data Hiding in Audio Signal: A Review.

[9] Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. M. (2014). Video steganography: a comprehensive review. Multimedia Tools and Applications, 74(17), 7063–7094. doi:10.1007/s11042-014-1952-z.

[10] Liu, T.-Y., & Tsai, W.-H. (2007). A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique. IEEE Transactions on Information Forensics and Security, 2(1), 24–30. doi:10.1109/tifs.2006.890310 .

[11] E. Dumic, M. Mustra, S. Grgic και G. Gvozden, Image Quality of 4:2:2 and 4:2:0 Chroma Subsampling Formats, Researchgate, 2009.

[12] Wikipedia, JPEG Color_space_transformation.

[13] K. Cabeen και P. Gent, Image Compression and the Discrete Cosine Transform, College of the Redwoods.

[14] F. T. Wedaj, S. Kim και F. Huang, Improved reversible data hiding in JPEG images based on new coefficient selection strategy, EURASIP Journal on Image and Video Processing volume 2017:63, DOI, 10.1186/s13640-017-0206-1, 2017.

[15] R. C. Gonzalez και R. E. Woods, Digital Image Processing 3rd edition, Pearson Preutice Hall, 2008.

[16] Impulse Adventure Optimized JPEG.

[17] Impulse Adventure JPEG Huffman Coding.

[18] R. B. I. S. B. S. Nik Shahidah Afifi Bt Md Taujuddin, «A Comparative Analysis of PSNR value for Images using Wavelet Based Thresholding Methods».

[19] D. Z. Alain Horé, «Image quality metrics: PSNR vs. SSIM».

[20] S. M. Fallahpour M.H, «High capacity lossless data hiding based on histogram modification».

[21] J. Tian, Reversible Data Embedding Using a Difference Expansion.

[22] Y. Q. S. N. A. W. S. Q. S. a. X. L. Z. Ni, Robust lossless image data hiding, in Proc. IEEE Int. Conf. Multimedia Expo, Jun. 2004,.

[23] J. F. M. G. R. Du, «Lossless Data Embedding For All Image Formats».

[24] B. G. M. R. J. B. M. P. M. Y. J. NaikRaikar, «Data Embedding in JPEG Bitstream».

[25] primeauforensics, DIGITAL IMAGE AUTHENTICATION.

[26] Y. Q. S. Z. N. P. C. X. C. a. X. T. G. Xuan, «Reversible data hiding for JPEG images based on histogram Pairs».

[27] X. Q. H. J. K. J. H. Fangjun Huang, «Reversible Data Hiding in JPEG Images».

[28] M. I. C. L. G. J.-M. C. C. R. F. I. Gouenou Coatrieux, «Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images».

[29] W. Z. K. C. S.-J. L. N. Y. Dongdong Hou, «Reversible Data Hiding in Color Image With Grayscale Invariance».