Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κρυπτογράφηση Επεξεργασμένης Εικόνας Σε Ενσωματωμένα Συστήματα

Βαζακοπούλου Καλλιόπη-Μαρίνα
Α.Μ. 2439

Επιβλέπων Καθηγητής:
Κορνάρος Γεώργιος

Δεκέμβριος 2013– Ηράκλειο

Ευχαριστίες

Αρχικά, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή της παρούσας εργασίας καθηγητή κ. Κορνάρο Γεώργιο πρωτίστως για την εμπιστοσύνη αλλά και την υπομονή που έδειξε. Για την ευκαιρία που μου έδωσε να ασχοληθώ με το συγκεκριμένο τομέα της πληροφορικής, την καθοδήγηση αλλά και την πολύτιμη βοήθεια που μου παρείχε καθ' όλη τη διάρκεια συγγραφής της πτυχιακής εργασίας.

Επίσης, να ευχαριστήσω τον βοηθό του επιβλέποντα καθηγητή, κ. Χριστοφοράκη Ιωάννη, για την βοήθειά του αλλά και την υπομονή που έδειξε κατά τη διάρκεια της συνεργασίας μας χωρίς την βοήθεια του οποίου η πορεία της εργασίας θα ήταν πολύ δύσκολη.

Τέλος ευχαριστώ την οικογένεια μου, τους φίλους μου και φυσικά το σκύλο μου το Ράστο για την αμέριστη στήριξη, υπομονή αλλά κυρίως για την ηθική συμπαράσταση που μου προσέφεραν όλο αυτό το χρονικό διάστημα μέχρι την περάτωση των σπουδών μου.

«Υπάρχει πάντα κάτι που φαντάζει απίθανο,
μέχρι τη στιγμή που θα συμβεί»
Νέλσον Μαντέλα

Σύνοψη

Τα πολύπλοκα πολυπύρηνα ενσωματωμένα συστήματα γίνονται όλο και πιο διαδομένα στα σύγχρονα προϊόντα μικροηλεκτρονικής. Η ανάπτυξη αυτών των συστημάτων, δημιουργεί νέες δυνατότητες εξέλιξης σε πολλούς τομείς της επιστήμης και της τεχνολογίας. Η ανάγκη υλοποίησης όλο και περισσότερων εφαρμογών σε τέτοια ανεπτυγμένα συστήματα, τα οποία παρέχουν αποτελεσματικότερη και πιο αξιόπιστη απόδοση αποτελεί αντικείμενο έρευνας της παρούσας εργασίας.

Θέμα της παρούσας πτυχιακής εργασίας είναι, η υλοποίηση αλγορίθμων κρυπτογράφησης σε πολυπύρηνα ενσωματωμένα συστήματα. Επιπλέον εξετάζεται συγκριτικά η απόδοση τεσσάρων αλγορίθμων κρυπτογράφησης, σε ένα σύστημα δύο πυρήνων που υλοποιείται σε μια πρωτότυπη πλατφόρμα της Xilinx. Σε επόμενο στάδιο επιχειρείται η αξιολόγηση της αξιοπιστίας της κρυπτογράφησης/αποκρυπτογράφηση σε μια επεξεργασμένη εικόνα, σε σχέση με τα αποτελέσματα που προέκυψαν από έναν αλγόριθμο επεξεργασίας εικόνας του MATLAB.

Λέξεις κλειδιά: Ενσωματωμένα Συστήματα, ψηφιακή επεξεργασία εικόνας, ανίχνευση ακμών, sobel, αλγόριθμοι παρακολούθησης ακμών, Αλγόριθμοι Επεξεργασίας Εικόνας, Συμμετρική/Ασύμμετρη Κρυπτογραφία, TEA, FPGA.

Πίνακας Περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων/Γραφημάτων

Abstract

This project focuses on the implementation of ciphers into multicores embedded systems. The outcome between four ciphers into a system of two cores, which is based on a prototype platform of Xilinx is also tested. Moreover is attempted to evaluate the reliability of the encryption and decryption of a processed image comparing with the results from the corresponding algorithm of a processed image from MATLAB.

The Complicated ciphers are widespread in the microelectronics. The growth of these systems creates new possibilities for the development of scientific and technological areas. The need to implement more and more of these applications, which are better and more reliable is our main task.

1. Εισαγωγή

Σε αυτήν την εργασία αναπτύξαμε ένα σύστημα που υλοποιεί κρυπτογράφηση επεξεργασμένης εικόνας σε πραγματικό χρόνο. Πρόκειται για την σχεδίαση ενός συστήματος δύο, επεξεργαστών όπου στον ένα υλοποιείται επεξεργασία επιλεγμένης εικόνας (υποστηρίζει διάφορα μεγέθη εικόνας) με την εφαρμογή του αλγόριθμου ανίχνευσης ακμών Sobel. Στον δεύτερο επεξεργαστή υλοποιείται η εφαρμογή κρυπτογράφησης, της ήδη επεξεργασμένης εικόνας, με τους αλγορίθμους TEA, Present, Blowfish και AES. Τα αποτελέσματα της επεξεργασμένης εικόνας επαληθεύονται με τα αντίστοιχα που εξάγει το MATLAB για την ίδια εικόνα. Η εφαρμογή λογισμικού έγινε με χρήση της γλώσσας προγραμματισμού C και βιβλιοθηκών υποστήριξης των αλγορίθμων που απαιτούνται από τους σχεδιαστές τους.

Η αναπτυξιακή πλακέτα που χρησιμοποιήθηκε για την ανάπτυξη της εργασίας είναι η ML405 της Xilinx, που υποστηρίζει Virtex 4 FPGA. Το σύστημα αυτό σχεδιάστηκε και προγραμματίστηκε στο περιβάλλον της Xilinx, ISE Design Suite 12.1 – EDK 12.1.

Η εφαρμογή ξεκινά με την τοποθέτηση της εικόνας που θέλουμε να επεξεργαστούμε στην τοπική μνήμη του επεξεργαστή που είναι επιφορτισμένος με την επεξεργασία της εικόνας. Στη συνέχεια ο αλγόριθμος Sobel ανιχνεύει την εικόνα για ακμές και εξάγει την επεξεργασμένη εικόνα, η οποία παρουσιάζεται σε pixel με τιμές 255 ή 0. Οι δύο επεξεργαστές είναι συνδεδεμένοι με Fast Simplex Link που παρέχει η Xilinx και με το πέρας του αλγορίθμου Sobel, ενημερώνεται ο δεύτερος πυρήνας ώστε να ξεκινήσει η κρυπτογράφηση και αποκρυπτογράφηση της επεξεργασμένης εικόνας. Τα επεξεργασμένα pixel(δεδομένα) έχουμε φροντίσει να αποθηκεύονται στην εξωτερική από το FPGA μνήμη DDR ώστε να έχει πρόσβαση ο δεύτερος επεξεργαστής, ο οποίος τα κρυπτογραφεί και τα αποκρυπτογραφεί.

Για την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων χρησιμοποιήθηκαν τέσσερεις αλγόριθμοι κρυπτογράφησης: TEA, Present, Blowfish και AES. Επιλέχθηκαν αλγόριθμοι διαφορετικής κρυπτογραφικής οικογένειας, και όπως αναδεικνύουν οι μετρήσεις μας είναι εμφανής η διαφορά ταχύτητας και απόδοσης του TEA σε σύγκριση με τους υπόλοιπους.

1.1 Αφορμή για τη διεξαγωγή της εργασίας

Στις μέρες μας τα ενσωματωμένα συστήματα και οι εφαρμογές τους σε πραγματικό χρόνο έχουν καταστεί κεντρικό κομμάτι της ζωής μας. Την ίδια ώρα η πληροφορία και τα δεδομένα που ανταλλάσει η κοινωνία, υπάρχει η ανάγκη να είναι ασφαλή καθόλα τη διάρκεια μιας επικοινωνίας, καθότι πλέον ανταλλάσσονται μάζες πληροφορίας και είναι εύκολο κάποιος να τις μολύνει. Στα υπολογιστικά συστήματα αυτό μπορεί να επιτευχτεί με την κρυπτογράφηση των

μεταδιδόμενων μηνυμάτων. Ευρέως γνωστοί αλγόριθμοι κρυπτογράφησης, όπως οι AES, PRESENT κ.α. χρησιμοποιούνται γι αυτόν τον σκοπό.

Η υλοποίηση τέτοιων αλγορίθμων σε εφαρμογές ενσωματωμένων συστημάτων είναι ένα σύνθετο κομμάτι που δεν είναι διαδεδομένο, ιδιαίτερα σε πλατφόρμες με FPGAs, παρά την αναγκαιότητα σε πολλά συστήματα. Πάνω σε αυτό το συνδυασμό κρυπτογραφημένης πληροφορίας σε εφαρμογές υλοποιημένες σε FPGA, εστιάζει η εργασία μας. Προσπαθήσαμε και πετύχαμε την υλοποίηση της κρυπτογράφησης επεξεργασμένης πληροφορίας σε FPGA πλατφόρμα, ενώ μετρήσαμε τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης δεδομένων για τέσσερις διαφορετικές περιπτώσεις αλγορίθμων κρυπτογράφησης.

Παράλληλα διαπιστώσαμε τη χρήση και φυσικά την υλοποίηση της κρυπτογράφησης σε πραγματικές εφαρμογές, όπως της ανίχνευσης ακμών μιας εικόνας, που πραγματοποιεί ο Sobel αλγόριθμος, στην παρούσα δουλειά. Έτσι είχαμε την δυνατότητα να βγάλουμε συμπεράσματα για ακόμη δύο ερωτήματα που είχαμε: Πρώτον ποιος αλγόριθμος κρυπτογράφησης είναι ταχύτερος στην εκτέλεση του για ένα ενσωματωμένο σύστημα; Δεύτερον πως επηρεάζει η μορφή των δεδομένων τόσο τη διαδικασία της κρυπτογράφησης/αποκρυπτογράφησης όσο και την επεξεργασία εικόνας.

Τέλος είχαμε την δυνατότητα να επαληθεύσουμε τα αποτελέσματα που προέκυψαν από την επεξεργασία του Sobel , με την αντίστοιχη επεξεργασία στο Matlab.

1.2 Επιδιώξεις και στόχοι Εργασίας

Συνοπτικά οι στόχοι της παρούσας εργασίας είναι οι εξής:

- Υλοποίηση και σύγκριση αλγορίθμων κρυπτογράφησης σε αναπτυξιακή πλατφόρμα με FPGA
- Κρυπτογράφηση –αποκρυπτογράφηση πραγματικής εφαρμογής σε FPGA
- Επαλήθευση των αποτελεσμάτων που προκύπτουν από συναρτήσεις επεξεργασίας εικόνας στο MATLAB, σε σχέση με τα αποτελέσματα υλοποίησης των ίδιων συναρτήσεων σε FPGA.
- Αξιολόγηση κρυπτογράφησης-αποκρυπτογράφησης με διαφορετική μορφή δεδομένων.

1.3 Περίληψη Κεφαλαίων

Κεφάλαιο $1^{ο}$: Ορισμένα εισαγωγικά

Κεφάλαιο $2^{ο}$: Παρατίθεται μια εισαγωγή για το τι είναι επεξεργασία ψηφιακής εικόνας στα ενσωματωμένα συστήματα, στα οποία εφαρμόζεται η εργασία μας, όπως επίσης τα είδη.

Κεφάλαιο $3^{ο}$:Παρουσιάζονται οι τεχνικές κρυπτογράφησης σε ψηφιακά επεξεργασμένες εικόνες

Κεφάλαιο 4^{ο}: Γίνεται αναφορά σε εργασίες/έρευνες που έχουν ήδη πραγματοποιηθεί σχετικά με το αντικείμενο που εξετάζουμε.

Κεφάλαιο 5^{ο}: Γίνεται μια γενική περιγραφή της μεθοδολογίας που χρησιμοποιούμε, αλλά και για ποιες άλλες μεθοδολογίες θα μπορούσαν να χρησιμοποιηθούν.

Κεφάλαιο 6^{ο}: Γίνεται περιγραφή της υλοποίησης σε υλικό (Hardware)

Κεφάλαιο 7^{ο} : Γίνεται περιγραφή της υλοποίησης σε (Software)

Κεφάλαιο 8^{ο} :Παρουσιάζουμε τα αποτελέσματα που εξήχθησαν από τα πειράματα που διενεργήσαμε καθώς και τη γενικότερη αξιολόγηση του συστήματος μας.

Κεφάλαιο 9^{ο}: Συμπεράσματα και κατευθύνσεις για μελλοντική ανάπτυξη

*2.*Εισαγωγή στην επεξεργασία εικόνας σε ενσωματωμένα συστήματα.

Η ραγδαία εξέλιξη των υπολογιστών κυρίως μετά το 1975, επέτρεψε την ανάπτυξη ενός νέου κλάδου που περιγράφεται γενικά ως ψηφιακή επεξεργασία εικόνας (ΨΕΕ). Η ψηφιακή επεξεργασία εικόνας αποτελεί πλέον ολόκληρη επιστήμη και έχει ευρύτερες εφαρμογές όπως για παράδειγμα, την αυτοματοποίηση γραφείου, τη ρομποτική και την όραση μηχανής (computer vision). Με τη λέξη ***εικόνα*** δεν νοείται απλά η απεικόνιση μιας σκηνής αλλά ένας τρόπος, με τον οποίο μπορούμε να αποτυπώσουμε πληροφορίες διαφόρων ειδών. Έτσι, έγγραφα, ιατρικά δεδομένα (υπερηχογραφήματα, μαγνητικές τομογραφίες κ.λ.π.), διαστημικά δεδομένα κ.α. μπορούν να ψηφιοποιηθούν και να επεξεργασθούν ως εικόνες.[1] Γενικά μπορούμε να πούμε ότι η ψηφιακή επεξεργασία εικόνας (ΨΕΕ) αναπτύχθηκε για να αντιμετωπίσει τα ακόλουθα κύρια προβλήματα:

- Τη ψηφιοποίηση (digitization), κωδικοποίηση εικόνων με στόχο την εκτύπωση, αποθήκευση και μετάδοση τους.
- Τη βελτιστοποίηση (enhancement) και την αποκατάσταση (restoration) των εικόνων με στόχο την καλύτερη απεικόνιση και κατανόηση τους.
- Την τμηματοποίηση (segmentation) και την περιγραφή εικόνων.
- Την ανάλυση και την κατανόηση των εικόνων.

Με μια διαφορετική κατηγοριοποίηση από την παραπάνω ανάλυση μπορούμε να συμπεράνουμε ότι τα θέματα που αντιμετωπίζει η ψηφιακή επεξεργασία εικόνας (ΨΕΕ) αφορούν αφενός την αξιοποίηση των μέσων και αφετέρου την κατανόηση του περιεχομένου των εικόνων με απώτερο στόχο την προσέγγιση της ανθρώπινης όρασης. Με την έννοια αυτή η ΨΕΕ ταυτίζεται με θέματα ρομποτικής όρασης (robot vision), αναγνώρισης προτύπων (pattern recognition) και τεχνητής νοημοσύνης (artificial intelligence). Οι επιστημονικοί αυτοί κλάδοι δεν είναι οι μόνοι συγγενείς κλάδοι. Γενικά μπορούμε να αναφέρουμε ότι η ΨΕΕ συγγενεύει άμεσα με τους κλάδους:

- Ψηφιακή Επεξεργασία Σημάτων.
- Ρομποτική Όραση και Όραση Μηχανής.
- Τεχνητή Νοημοσύνη.
- Αναγνώριση Προτύπων.
- Νευρωνικά Δίκτυα (Neural Networks).
- Ασαφή Λογική (Fuzzy Logic).
- Κωδικοποίηση.
- Γραφικά Υπολογιστών (Computer Graphics).

Στην ενότητα αυτή θα μελετήσουμε εισαγωγικά θέματα που αφορούν γενικά στην ψηφιακή επεξεργασία εικόνας αλλά και την ΨΕΕ σε ενσωματωμένα συστήματα.

2.1 Επεξεργασία Εικόνας Σε Ενσωματωμένα Συστήματα

Στη σημερινή εποχή η επεξεργασία, μετάδοση και κατανόηση των εικόνων αποτελούν πεδία μιας συνεχώς αναπτυσσόμενης έρευνας. Το μέγεθος μιας εικόνας απαιτεί τεράστια ταχύτητα υλοποίησης των αλγορίθμων για λειτουργία σε πραγματικό χρόνο. Η τεχνολογία ολοκληρωμένων κυκλωμάτων πολύ μεγάλης κλίμακας (VLSI), σε συνδυασμό με την ανάπτυξη αρχιτεκτονικών συνεχούς ροής (pipelining) με μεγάλο βαθμό παραλληλισμού, βοήθησε στη δυνατότητα υλοποίησης πολλών πολύπλοκων αλγόριθμων. Η ταυτόχρονη ελάττωση του κόστους των μνημών, επεξεργαστών, και γενικά της υπολογιστικής ισχύος, έχει κάνει οικονομικά βιώσιμη την ανάπτυξη συστημάτων επικοινωνίας και επεξεργασίας εικόνων ακόμα και για οικιακή χρήση. [2][3].

Η ψηφιακή εικόνα είναι ένα από τα δισδιάστατα ψηφιακά σήματα που παρουσιάζουν σημαντικό ενδιαφέρον στη σημερινή κοινωνία της πληροφορικής και αποτελεί στην εποχή μας μία από τις σημαντικότερες πηγές πληροφορίας. Τη συναντούμε ως εικόνα ακίνητη (φωτογραφία) ή κινούμενη (τηλεόραση), ασπρόμαυρη ή έγχρωμη. Η ψηφιακή εικόνα αποτελεί ό,τι πιο σύγχρονο, τόσο στο χώρο της ενημέρωσης (Internet) και της εκπαίδευσης (multimedia) όσο και στο χώρο του θεάματος και της ψυχαγωγίας (ψηφιακή τηλεόραση, DVD κλπ.).

2.2Επεξεργασία Εικόνας

Η ψηφιακή επεξεργασία εικόνας αποτελεί έναν ευρύ επιστημονικό κλάδο που αναπτύχθηκε με την ραγδαία εξέλιξη των υπολογιστών. Ο όρος εικόνα χρησιμοποιείται ευρύτερα από την απλή απεικόνιση ενός σκηνικού και περιλαμβάνει την αποτύπωση κάθε είδους πληροφοριών. Αποτελεί μια διαρκώς διευρυνόμενη και δυναμική περιοχή με τις εφαρμογές να απευθύνονται τόσο στην καθημερινή ζωή μας, όπως η ιατρική, η εξερεύνηση του διαστήματος, η επιτήρηση, ο έλεγχος ταυτότητας, αυτοματοποιημένη επιθεώρηση της βιομηχανίας αλλά και σε πολλές άλλες περιοχές. Εφαρμογές όπως τις παραπάνω περιλαμβάνουν διαφορετικές διαδικασίες, όπως η βελτίωση της εικόνας και ανίχνευση αντικειμένων [14]. Η υλοποίηση αυτών των εφαρμογών σε έναν υπολογιστή γενικής χρήσεως μπορεί να είναι πιο εύκολη, αλλά δεν είναι χρονικά πολύ αποδοτική λόγω πρόσθετων περιορισμών στη μνήμη και άλλες περιφερειακές συσκευές. Ωστόσο η υλοποίηση ειδικής εφαρμογής του hardware προσφέρει πολύ μεγαλύτερη ταχύτητα από ό, τι μια εφαρμογή λογισμικού.

2.2.1 Δομικά Στοιχεία ψηφιακής εικόνας

Η μετάβαση από τον αναλογικό κόσμο στον ψηφιακό συνεπάγεται τη μετατροπή αναλογικών σημάτων σε ψηφιακά. Έτσι μια πραγματική εικόνα μεταφέρεται στον ψηφιακό κόσμο με τη μορφή διακεκριμένου σήματος η οποία έχει τη μορφή ψηφιακών πινάκων. Μια ψηφιακή εικόνα μπορεί να είναι δυαδική (binary images), μονοχρωματική αποχρώσεων του γκρι (gray-level ή gray-scale images) ή έγχρωμη (color image).

Η εικόνα μπορεί να οριστεί ως μια δισδιάστατη συνάρτηση f(x,y), όπου τα x,y είναι οι συντεταγμένες επιπέδου. Ένταση της εικόνας ονομάζεται το πλάτος της f σε κάθε ζευγάρι συντεταγμένων x,y στο σημείο αυτό. Επίσης η εικόνα μπορεί να θεωρηθεί πως είναι η κατανομή της πληροφορίας στο επίπεδο (x,y). Έτσι η f περιγράφει μια επιφάνεια, η οποία έχει μεγάλη τιμή όπου η εικόνα είναι πιο λευκή ενώ πλησιάζει το μαύρο όπου η f έχει μικρές τιμές. Στην ουσία η f περιγράφει την αμαύρωση της εικόνας σε κάθε θέση (x,y). Ο όρος επίπεδο του γκρι συχνά χρησιμοποιείται στις μονοχρωματικές εικόνες.

Πρακτικά, θα πρέπει να μας γίνει σαφές ότι κάθε εικόνα για να υποστεί ψηφιακή επεξεργασία θα πρέπει κατ' αρχήν να μετατραπεί σε ψηφιακή. Έτσι θα πρέπει να λάβουμε ισαπέχοντα δείγματα της συνάρτησης f (x,y) στις θέσεις x και y. Η πυκνότητα με την οποία θα ληφθούν τα δείγματα καθορίζεται από το **θεώρημα δειγματοληψίας:**

Η απόσταση δύο διαδοχικών δειγμάτων x και y στο επίπεδο θα πρέπει να είναι μικρότερη από την ημιπερίοδο των ταχύτερων εναλλαγών της συνάρτησης f (x,y).

Με άλλα λόγια θα πρέπει να δειγματοληπτούμε αρκετά γρήγορα ώστε να προλαβαίνουμε τις γρήγορες εναλλαγές της αμαύρωσης της εικόνας. Ένας δυαδικός αριθμός των 8 bits (1 byte) επαρκεί για να περιγράψουμε την τιμή της αμαύρωσης ενός δείγματος της εικόνας που καλείται εικονοστοιχείο (picture element- pixel) αφού στη στάθμη 255 αντιστοιχούμε το λευκό ενώ στη στάθμη 0 το μαύρο.

Η ψηφιακή εικόνα αναλύεται με βάση κάποιο ορθογώνιο πλέγμα που λέγεται bitmap. Με βάση αυτό το πλέγμα, η εικόνα μοιράζεται σε μια κάθετη ακολουθία από οριζόντιες σειρές με μικρές υποδιαιρέσεις, που ονομάζονται εικονοστοιχεία ή pixels (picture elements). Κάθε pixel του πλέγματος καθορίζεται από τη θέση του στο πλέγμα (x και y). Συνήθως τα pixels χαρακτηρίζονται ξεκινώντας από την πάνω αριστερή γωνία (0,0) χωρίς αυτό να ισχύει πάντα. Τα λευκά εικονοστοιχεία αντιστοιχούν στο 255 ενώ τα μαύρα στο 0. Κάθε ένα εικονοστοιχείο είναι ένα δείγμα από τη συνάρτηση *f(x,y)* που αντιστοιχεί στην αναλογική εικόνα. Μια ψηφιακή εικόνα παριστάνεται μαθηματικά ως η κβαντισμένη σε πλάτος συνάρτηση :

$$f \rightarrow f_q(n1,n2),$$

όπου οι διακριτές χωρικές μεταβλητές n1 και n2 αντιστοιχούν στις συνεχείς χωρικές μεταβλητές x και y. Στη γενική περίπτωση, μη μέγιστη τιμή του n1 είναι M και του n2 είναι η N. Έτσι μπορούμε να θεωρήσουμε την ψηφιακή εικόνα ως ένα πίνακα διαστάσεων M×N αριθμών που κάθε ένας από αυτούς εκπροσωπεί την τιμή του αντίστοιχου εικονοστοιχείου.[19]

Σε ειδικού τύπου εικόνες, όπως το κείμενο ή το σχέδιο, αρκούν δύο μόνο στάθμες, οι 0 και 1, που αντιστοιχούν στο μαύρο και το λευκό. Στην περίπτωση αυτή ένα μόνο δυαδικό ψηφίο είναι αρκετό για να αναπαραστήσει την πληροφορία.

Σε περίπτωση που η εικόνα είναι **έγχρωμη** τότε σε κάθε θέση (n1,n2) έχει τρεις τιμές, οι οποίες αντιστοιχούν στις τιμές των χρωμάτων κόκκινο, πράσινο και μπλε (Red, Green and Blue –

RGB). Όταν, τέλος, έχουμε διαδοχή εικόνων η συνάρτηση έχει μια επιπλέον μεταβλητή, το χρόνο t. Το σήμα είναι διακριτό και ως προς τον χρόνο (t→n):

$$3f \rightarrow fq \text{ (n1,n2,n3)}$$

2. 3 Οι τύποι των εικόνων και η δομή τους στο MATLAB®

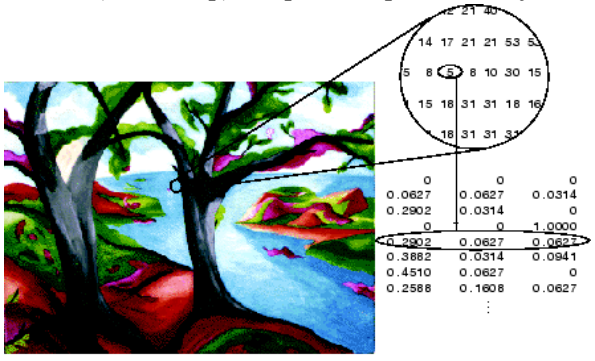
Η βασική δομή της πληροφορίας στο MATLAB® είναι ένα διατεταγμένο σύνολο πραγματικών ή φανταστικών αριθμών. Αυτό το αντικείμενο εξυπηρετεί την αναπαράσταση των εικόνων, οι οποίες είναι διατεταγμένα σύνολα χρωμάτων και εντάσεων του φωτός. Τα στοιχεία των πινάκων αυτών αποτελούνται αποκλειστικά και μόνο από πραγματικές τιμές αφού το MATLAB® δεν υποστηρίζει εικόνες πινάκων φανταστικών τιμών.

Το MATLAB® αποθηκεύει τις περισσότερες εικόνες ως δισδιάστατους πίνακες, στους οποίους κάθε στοιχείο του πίνακα αναφέρεται σε ένα και μοναδικό pixel της εικόνας. Η λέξη pixel προέρχεται από τις λέξεις picture element (στοιχείο εικόνας) και συνήθως αναφέρεται σε μια κουκίδα (dot) της οθόνης του υπολογιστή. Αυτή η συμβατικότητα κάνει την επεξεργασία εικόνων με το MATLAB® όμοια με οποιαδήποτε άλλη εργασία σε πίνακες. [15][16]
Το MATLAB® υποστηρίζει 4 βασικούς τύπους εικόνας:

- ✓ **Ενδεικτικές Εικόνες (indexed images)**
- ✓ **Ασπρόμαυρες Εικόνες (grayscale /intensity images)**
- ✓ **Έγχρωμες Εικόνες (RGB)**
- ✓ **Δυαδικές Εικόνες (Binary)**

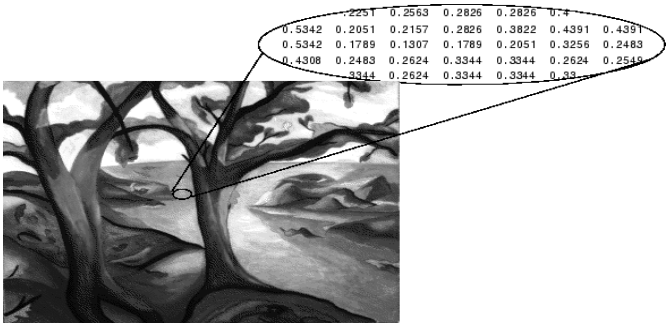
2.3.1 Ενδεικτικές Εικόνες (indexed images)

Μια indexed εικόνα αποτελείται από ένα πίνακα δεδομένων X, και ένα πίνακα χρωμάτων-παλέτα (color map), map. Ο map είναι ένας mx3 πίνακας κλάσης double, ο οποίος περιέχει κινητής υποδιαστολής (floating-point) τιμές εύρους [0,1] και υπάρχει αποθηκευμένος μέσα στο MATLAB®. Κάθε μια από τις γραμμές του map καθορίζει τα κόκκινα, πράσινα και μπλε συστατικά κάθε χρώματος αντίστοιχα. Μια ενδεικτική εικόνα χρησιμοποιεί "direct mapping" των τιμών του pixel σε color map τιμές. Το χρώμα κάθε pixel της εικόνας καθορίζεται χρησιμοποιώντας την ανταποκρινόμενη τιμή του X σαν ένδειξη στον map. Η τιμή 1 δείχνει την πρώτη γραμμή του map , η 2 την δεύτερη κ.ο.κ.[23]



Εικόνα2.3.5 : Indexed Image

2.3.2 Ασπρόμαυρες Εικόνες (grayscale /intensity images)

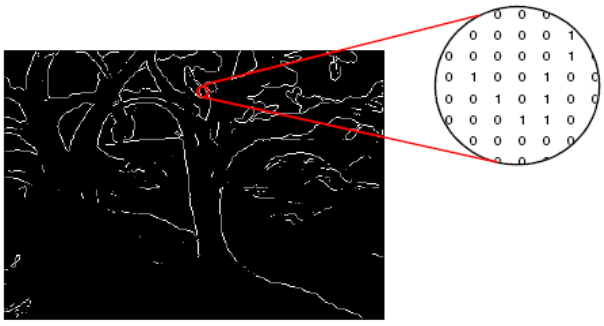


Εικόνα 6.3.2: Binary Image

Μια ασπρόμαυρη εικόνα (εικόνα έντασης) είναι ένας πίνακας δεδομένων I του οποίου οι τιμές αναπαριστούν την ένταση του φωτός. Το MATLAB® αποθηκεύει μια εικόνα έντασης σε ένα απλό πίνακα, του οποίου κάθε στοιχείο αναφέρεται σε ένα και μοναδικό pixel. Ο πίνακας μπορεί να είναι κλάσης double, uint8 ή uint16. Τα στοιχεία του πίνακα αναπαριστούν διάφορες εντάσεις του φωτός (επίπεδα του γκρι) όπου η ένταση 0 αναπαριστά το μαύρο και η ένταση 1, 255 ή 65535 αναπαριστά το λευκό. Ένα ειδικό είδος ασπρόμαυρης εικόνας η οποία όμως περιέχει μόνο μαύρο και άσπρο είναι η δυαδική. Σε μια **δυαδική εικόνα** κάθε pixel προέρχεται από μια από τις δυο διακριτές τιμές (0 ή 1). Βασικά αυτές οι δυο τιμές αναφέρονται σε on ή off. Μια δυαδική εικόνα αποθηκεύεται σε ένα δισδιάστατο πίνακα μηδενικών (off pixels) και μονάδων (on pixels). [23]

2.3.3Δυαδική Εικόνα (Binary Image)

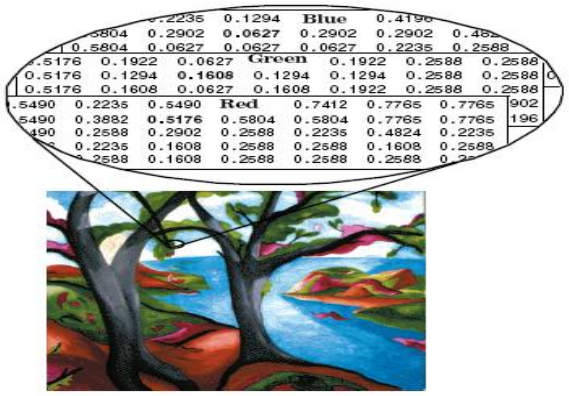
Σε μια binary εικόνα κάθε εικονοστοιχείο παίρνει μια από τις μόνο δυο διακριτές τιμές, 0 και 1. Ουσιωδώς οι δυο αυτές τιμές ανταποκρίνονται στο on και στο off αντίστοιχα. Μια binary εικόνα αποθηκεύεται σαν λογικός πίνακας (logical data class) από μηδενικά και άσσους. Το σχήμα παρακάτω αντιπροσωπεύει μια binary εικόνα. [23]



Εικόνα 2.3.7 : Grayscale/Intensity Image

2.3.4 Έγχρωμη Εικόνα RGB

Μια **RGB εικόνα**, ορισμένες φορές αναφέρεται και σαν "truecolor" (πραγματικού χρώματος) εικόνα, αποθηκεύεται στο MATLAB® σαν ένα πίνακα δεδομένων m x n x 3 ο οποίος καθορίζει τα κόκκινα, πράσινα και μπλε χρωματιστά στοιχεία κάθε ανεξάρτητου pixel. Οι RGB εικόνες δεν χρησιμοποιούν χάρτη χρωμάτων (color map). Το χρώμα του κάθε pixel καθορίζεται από



Εικόνα 2.3.8 : RGB Image

τον συνδυασμό των κόκκινων, πράσινων και μπλε εντάσεων. Ένας RGB MATLAB® πίνακας μπορεί να είναι κλάσης double, uint8 ή uint16. Σε ένα πίνακα κλάσης double κάθε χρώμα είναι μια τιμή στον πίνακα μεταξύ 0 και 1. Ένα pixel του οποίου το χρώμα έχει τιμή (0,0,0) παρουσιάζει το μαύρο ενώ ένα pixel το οποίο έχει τιμή μέσα στον πίνακα (1,1,1) παρουσιάζει το λευκό. Τα στοιχεία των τριών χρωμάτων για κάθε pixel αποθηκεύονται στις τρεις διαστάσεις του πίνακα. [23]

2.4 Αλγόριθμοι Επεξεργασίας Εικόνας

Οι αλγόριθμοι επεξεργασίας εικόνας χωρίζονται σε δύο βασικές κατηγορίες, στο πεδίο του χώρου(spatial) και στο πεδίο της συχνότητας (frequency). Πιο αναλυτικά στο πεδίο της συχνότητας (frequency) γίνεται χρήση τελεστών για μετασχηματισμό της εικόνας ενώ οι διαδικασίες εφαρμόζονται στο πεδίο της συχνότητας (Fourier, Wavelet – κυματίδια), λ.χ. κωδικοποίηση, ανάλυση, απαλοιφή.

Στην παρούσα εργασία ασχολούμαστε με αλγόριθμους, κυρίως με τον sobel, οι διαδικασίες των οποίων εφαρμόζονται στο πεδίο του χώρου. Η εικόνα αναπαριστάται σαν πίνακας στοιχείων, λ.χ. αλλαγή φωτεινότητας, κοντράστ, εντοπισμός ακμών, μείωση θορύβου. Καθώς η αναπαράσταση της εικόνας πραγματοποιείται με βάση το pixel στο πεδίο του χώρου μπορούμε να κάνουμε επεξεργασία ιστογράμματος, αλλαγή του χρωματικού μοντέλου, πρόσθεση εικόνων αλλά και λήψη αρνητικού.

Οι αλγόριθμοι επεξεργασίας εικόνων εξυπηρετούν διάφορους σκοπούς σαν τους επόμενους:

- την βελτίωση της ποιότητας των εικόνων, με χρήση κατάλληλων φίλτρων η την αποκατάσταση τους στην αρχική τους μορφή μετά από αλλοίωση τους λόγω επίδρασης θορύβου.
- την κωδικοποίηση τους, έτσι ώστε η πληροφορία τους να μπορεί να περιγραφεί από μία σειρά όσο γίνεται μικρότερου αριθμού bit (συμπίεση δεδομένων) N με σκοπό την γρήγορη μετάδοση τους μέσω διαύλων περιορισμένης χωρητικότητας (bandwidth), ή την αποτελεσματική αποθήκευση τους σε περιορισμένο αποθηκευτικό χώρο με ικανοποιητική ποιότητα εικόνας.
- την μετατροπή φωτογραφιών σε εικόνες δύο μόνο αποχρώσεων (μαύρου-άσπρου), για εκτύπωση ή επίδειξη σε δυαδική μορφή.
- την τροποποίηση των εικόνων (π.χ. pixelate) εφαρμόζοντας έτσι επάνω τους «καλλιτεχνικές» φόρμες και απόψεις.

2.4.1 Αλγόριθμοι Παρακολούθησης Ακμών

Σε πολλές περιπτώσεις είναι επιθυμητό να παρακολουθήσουμε τα περιγράμματα των αντικειμένων για εφαρμογές αναγνώρισης αντικειμένων. Μια προσέγγιση στην παρακολούθηση ακμών είναι να εφαρμόσουμε ανίχνευση ακμών και να παρακολουθήσουμε τα τοπικά στοιχεία ακμής. Οι κατηγορίες στις οποίες χωρίζονται οι αλγόριθμοι παρακολούθησης έυρεσης ακμών είναι οι ακόλουθες.

- **Απλός:** Είναι εξαντλητικός αλγόριθμος εύρεσης. Παράγει σχετικά μικρά τμήματα ακμών επειδή τερματίζει όταν παρουσιάζονται έστω και μικρά κενά.
- **Αναζήτησης γραφήματος:** Μετατρέπει την εικόνα σε προσανατολισμένο γράφημα. Τα στοιχεία ακμής στις θέσεις x_i θεωρούνται κόμβοι του γραφήματος. Έτσι οι αναγνωρισμένες ακμές αντιστοιχούν στις διαδρομές του γραφήματος. Μειονέκτημά του είναι ότι κατά τη διαδικασία της αναζήτησης πρέπει να κρατούνται στοιχεία για όλες τις τρέχουσες καλύτερες διαδρομές, τα αποτελέσματά του όμως είναι καλύτερα από αυτά του απλού.

2.5 Ανίχνευση Ακμών (Edge Detection)

Η ανίχνευση ακμών αποτελεί θεμελιώδες εργαλείο στην επεξεργασία εικόνας και την όραση υπολογιστών, ιδιαίτερα στους τομείς της ανίχνευσης και εξαγωγής χαρακτηριστικών, οι οποίοι αποσκοπούν στον εντοπισμό σημείων σε μια εικόνα στα οποία η φωτεινότητά της αλλάζει απότομα (παρουσιάζει ασυνέχειες). Αλλαγές της φωτεινότητας συνήθως αντιστοιχούν σε διαφοροποίηση ιδιοτήτων της απεικόνισης τρισδιάστατων αντικειμένων όπως αλλαγές της υφής, του βάθους, όρια αντικειμένων, διαφορετικό φωτισμό και αντανάκλαση. Έτσι με την ανίχνευση ακμών μπορούμε να αντλήσουμε πληροφορίες για φυσικές ιδιότητες για τα εικονιζόμενα πραγματικά αντικείμενα.[17]

Ως ακμή σε μία gray-scale εικόνα ορίζεται η σχετική ασυνέχεια μεταξύ δύο διαβαθμίσεων του γκρι. Στην πράξη μια ακμή θεωρείται το σύνορο μεταξύ δύο ομοιογενών περιοχών με διαφορετική φωτεινότητα ή αλλιώς το περίγραμμα αυτών. Είναι απαραίτητο να υιοθετηθούν διάφορες παραδοχές προκειμένου να ξεχωρίσουμε τις ασυνέχειες που έχουν νόημα από εκείνες που δεν έχουν. Για παράδειγμα, οι δύο παρακάτω εικόνες αναπαριστούν μία εικόνα ακτινογραφίας (αριστερά) και μία εικόνα αγγειογραφίας (δεξιά).

Η ανίχνευση των ακμών στην πρώτη εικόνα είναι πολύ πιο εύκολη υπόθεση από ότι στη δεύτερη, καθώς είναι πιο εύκολο να οριστούν οι ασυνέχειες, η μετάβαση δηλαδή από pixels με τιμή 0 (μαύρο) – τα οποία αντιστοιχούν στο φόντο της εικόνας – σε pixels με τιμές μεγαλύτερες του 150 – τα οποία αντιστοιχούν στο σκελετό. Αντίθετα, στη δεύτερη εικόνα θα πρέπει να βρούμε μια φόρμουλα που να ορίζει ποιες μεταβάσεις αποτελούν ασυνέχειες στα gray levels, π.χ. η μετάβαση από pixels με τιμή x1 σε pixels με τιμή x2.

Στην ιδανική περίπτωση, το αποτέλεσμα της εφαρμογής ενός ανιχνευτή ακμών σε μια εικόνα οδηγεί σε ένα σύνολο συνδεδεμένων καμπυλών που δείχνουν τα όρια (περιγράμματα) των διαφόρων αντικειμένων της εικόνας. Ωστόσο, καθώς δεν υπάρχει γενικό μαθηματικό μοντέλο που να καθορίζει τις ακμές σε μια εικόνα, έχουν κατά καιρούς προταθεί διάφορες προσεγγίσεις ανίχνευσης

ακμών που καταλήγουν σε διαφορετικά αποτελέσματα ανίχνευσης. Οι δύο πιο γνωστές τεχνικές ανίχνευσης ακμών είναι οι τεχνικές που προτάθηκαν από τους Sobel και Canny.

2.5.1. Αλγόριθμος Sobel

Ο ***ανιχνευτής ακμών Sobel (Sobel edge detector)***, τον οποίο χρησιμοποιήσαμε στην παρούσα εργασία, είναι μια από τις πιο γνωστές μεθόδους και δίνει έμφαση σε περιοχές υψηλής χωρικής συχνότητας, οι οποίες αντιστοιχούν σε ακμές. Το αποτέλεσμα της όλης εργασίας είναι μια νέα δυαδική εικόνα, ιδίων διαστάσεων με την αρχική, όπου τα εικονοστοιχεία με τη μεγαλύτερη τιμή είναι οι ακμές της αρχικής εικόνας. Μετά την εφαρμογή αυτής της διαδικασίας ακολουθεί κατωφλίωση που συνήθως έγκειται στη διατήρηση ενός ποσοστού των σημείων ακμών που έχουν το υψηλότερο μέτρο κλίσης (gradient). Το μέτρο του διανύσματος κλίσης σε ένα σημείο (x,y) δείχνει πόσο απότομη είναι η ακμή και δίνεται από την σχέση:

Εξίσωση 2.5.1(a): Μέτρο διανύσματος κλίσης :

$$|\nabla f(x,y)| = \sqrt{\left(\frac{\partial f}{\partial x}\right)^2 + \left(\frac{\partial f}{\partial y}\right)^2}$$

Η τεχνική Sobel δίνει έμφαση σε περιοχές υψηλής χωρικής συχνότητας, οι οποίες αντιστοιχούν σε ακμές. Η τεχνική εφαρμόζεται με χρήση ενός τελεστή (τελεστής Sobel) ο οποίος αποτελείται από δύο φίλτρα (μάσκες ακμών), ένα για να ανιχνεύσει τις αλλαγές στην κάθετη κατεύθυνση (Gy) και το άλλο για να ανιχνεύσει τις αλλαγές στην οριζόντια (Gx). Οι δύο μάσκες του τελεστή Sobel είναι οι δύο πυρήνες συνέλιξης 3x3 που παρουσιάζονται παρακάτω. Κατά τη διαδικασία ανίχνευσης ακμών πραγματοποιείται συνέλιξη μεταξύ της εικόνας και των δύο αυτών μασκών. Από τον κατάλληλο συνδυασμό των δύο εικόνων που προκύπτουν αναδεικνύονται οι ακμές των αντικειμένων της εικόνας.

Στην πιο απλή περίπτωση υπολογίζεται ένα μέγεθος κλίσης για κάθε pixel, π.χ. |G|=|Gx|+|Gy|, και στην περίπτωση που αυτό υπερβεί ένα κατώφλι τότε ορίζεται πως το pixel αποτελεί σημείο ακμής και λαμβάνει τιμή 255 (αλλιώς λαμβάνει τιμή 0). Με τη διαδικασία αυτή σαρώνεται όλη η εικόνα και όσα σημεία ανιχνευθούν ότι αποτελούν σημεία ακμών αναδεικνύονται στο προσκήνιο.

Ο τελεστής Sobel υπολογίζει την απόκλιση της έντασης κάθε pixel σε σχέση με τα γειτονικά του και δίνει ως αποτέλεσμα την πιο πιθανή μέγιστη αύξηση από τα σκούρα gray levels στα πιο ανοικτά, καθώς και τη μεταβολή αυτής. Ουσιαστικά δείχνει πώς μεταβάλλεται η τιμή φωτεινότητας στις οριζόντιες και κάθετες κατευθύνσεις, και γι' αυτό τα σημεία μεγάλης μεταβολής είναι πολύ πιθανό να είναι ακμές. Ανήκει στις τεχνικές ανίχνευσης ακμών με χρήση πρώτης παραγώγου. Στο Matlab η ανίχνευση ακμών με την τεχνική Sobel πραγματοποιείται με την εντολή: **I1=edge(I,'Sobel'),** όπου I η αρχική και I1 η τελική εικόνα (εικόνα εξόδου).

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Πίνακας 2.5.2(b): Μάσκες Sobel μεγέθους 3x3

Μια προσέγγιση για τον προσδιορισμό των συνόρων αντικειμένων σε μια εικόνα έγκειται στην εξέταση κάθε εικονοστοιχείου και της άμεσης περιοχής του για να αποφασιστεί αν το εικονοστοιχείο ανήκει πραγματικά στο σύνορο ενός αντικειμένου. Τέτοια εικονοστοιχεία προσδιορίζονται ως εικονοστοιχεία ακμών (edge pixels). Οι παρακάτω αλγόριθμοι προσφέρουν διαφορετικούς τρόπους για την υλοποίηση αυτής της διαδικασίας. [18]

2.5.2 Αλγόριθμος Canny

Ο αλγόριθμος Canny αποτελεί μια από τις καλύτερες τεχνικές ανίχνευσης ακμών. Είναι ένας σύνθετος πολυσταδιακός αλγόριθμος που αναπτύχθηκε το 1986 από τον John F. Canny με στόχο τη βέλτιστη και ευρεία ανίχνευση ακμών. Ο αλγόριθμος εφαρμόζει σταδιακά διάφορες τεχνικές, όπως εξομάλυνση της εικόνας με χρήση Gaussian συνέλιξης, ανίχνευση των περιοχών με υψηλή χωρική πρώτη παράγωγο (συνήθως με χρήση τελεστή Sobel), κατωφλίωση κ.ά., προκειμένου να ανιχνευθεί και αναδειχθεί ένα μεγάλο εύρος ακμών στην εικόνα. Η τεχνική ανίχνευσης ακμών Canny υπερτερεί των τεχνικών ανίχνευσης ακμών με χρήση πρώτης παραγώγου (όπως ο Sobel) στο ότι ανιχνεύει επιπλέον αδύνατες ακμές που ενδεχομένως να περιέχουν σημαντική πληροφορία. Ομοίως με την τεχνική Sobel, η ανίχνευση ακμών με τον αλγόριθμο Canny πραγματοποιείται στο Matlab με την εντολή: **I1=edge(I,'canny').**

Σε εικόνες αποχρώσεων του γκρι συναντούμε περιοχές όπου έχουμε απότομη αλλαγή στις τιμές φωτεινότητας. Αυτό συμβαίνει στα όρια μεταξύ διαφορετικών αντικειμένων της εικόνας. Η διαδικασία εύρεσης αυτών των ορίων ονομάζεται ***ανίχνευση ακμών (edge detection).*** Υπάρχει μεγάλη ποικιλία αλγορίθμων που αφορούν στην επίλυση αυτού του προβλήματος, όμως όλοι βασίζονται στην έννοια της κλίσης της συνάρτησης φωτεινότητας I(k,j) στη θέση (k, j) ενός εικονοστοιχείου της εικόνας.[18]

2.5.3 Αλγόριθμος Roberts

Ο ανιχνευτής ακμών του Roberts είναι ένας τοπικός διαφορικός τελεστής που δέχεται μια εικόνα εισόδου A(m,n) και παράγει την εικόνα εξόδου:

Εξίσωση 2.5.3(a) : Έξοδος Roberts :

$$B(m,n) = \{[\sqrt{A(m,n)} - \sqrt{A(m+1,n+1)}]^2 + [\sqrt{A(m+1,n)} - \sqrt{A(m,n+1)}]^2\}^{\frac{1}{2}}$$

Οι εσωτερικές τετραγωνικές ρίζες κάνουν την διαδικασία παρόμοια με την επεξεργασία που λαμβάνει χώρα στο ανθρώπινο σύστημα όρασης.[18].

-1	0
0	1

0	-1
1	0

Πίνακας 2.5.3(b) : Μάσκες Roberts

2.5.4 Αλγόριθμος Prewitt

Οι τελεστές prewitt προσεγγίζουν την μερική παράγωγο πρώτης τάξης κατά κατεύθυνση γι α την εικόνα. Υπάρχουν 8 διαφορετικές κατευθύνσεις για τις οποίες μπορούμε να υπολογίσου με την μερική παράγωγο, δύο όμως αρκούν για να εντοπίσουμε τις ακμές στην περίπτωση πο υ μας ενδιαφέρει μόνο το μέτρο της ακμής. [18]Στον ανιχνευτή ακμών του Prewitt η διαδικασία είναι ακριβώς η ίδια όπως και με τον ανιχνευτή ακμών του Sobel, αλλά χρησιμοποιούνται οι επόμενοι δύο πυρήνες:

-1	-1	-1
0	0	0
1	1	1

1	0	-1
1	0	-1
1	0	-1

Πίνακας 2.5.4(b) : Μάσκες Prewitt

2.5.5 Αλγόριθμος Kirsch

Ο ανιχνευτής ακμών του Kirsch χρησιμοποιεί 8 συνελικτικούς πυρήνες (βιβλίο «Ανάλυση εικόνας, σελίδα 92). Κάθε εικονοστοιχείο συνελίσσεται και με τις οκτώ μάσκες. Κάθε μάσκα έχει μέγιστη απόκριση σε ακμές κάποιου συγκεκριμένου προσανατολισμού. Επιλέγεται το ολικό μέγιστο και τελικά δημιουργείται μια εικόνα του μεγέθους των ακμών.

Οι μάσκες ακμών (edge templates) είναι μάσκες που μπορούν να χρησιμοποιηθούν για την ανίχνευση ακμών κατά μήκος διαφορετικών διευθύνσεων. Τέτοιες μάσκες μεγέθους 3x3 φαίνονται στον Πίνακα 4.

-1	0	1
-1	0	1
-1	0	1

1	1	1
0	0	0
-1	-1	-1

0	1	1
-1	0	1
-1	-1	0

1	1	0
1	0	-1
0	-1	-1

Πίνακας 2.5.5(b) : Μάσκες Kirsch μεγέθους 3x3

Μια άλλη προσέγγιση στην ανίχνευση ακμών είναι η χρήση του τελεστή Laplace, που ορίζεται συναρτήσει των μερικών παραγώγων δεύτερης τάξεως της f(x,y) ως προς χ και y. Οι παράγωγοι πρώτης τάξεως έχουν τοπικά μέγιστα ή ελάχιστα στις ακμές της εικόνας, εξαιτίας των μεγάλων τοπικών μεταβλητών της φωτεινότητας. Ως εκ τούτου, οι παράγωγοι δεύτερης τάξεως έχουν μηδενισμούς (δηλαδή μεταβάσεις από θετικές σε αρνητικές τιμές και αντιστρόφως) στις περιοχές των ακμών. Έτσι, μια προσέγγιση στην ανίχνευση ακμών είναι να εκτιμήσουμε την έξοδο του τελεστή Laplace και να βρούμε τα σημεία μηδενισμού.

Η διαφόριση είναι μια υψηλοπερατή πράξη. Η διαφόριση δεύτερης τάξης τείνει να αυξήσει το θόρυβο της εικόνας.

-1	-1	-1
-1	8	-1
1	-1	-1

-1	-1	-1
2	2	2
-1	-1	-1

-1	-1	2
-1	2	-1
2	-1	-1

-1	2	-1
-1	2	-1
-1	2	-1

Πίνακας 2.5.5(c) : (α)Μάσκα για ανίχνευση απομονωμένου σημείου.(β) Μάσκες για ανίχνευση Γραμμών

Συνεπώς, ο τελεστής Laplace δημιουργεί αρκετές εσφαλμένες ακμές, ιδιαίτερα σε περιοχές που η μεταβλητότητα της εικόνας είναι μικρή, επειδή μικρές διαταραχές της φωτεινότητας (θόρυβος) τείνουν να προκαλέσουν εσφαλμένους μηδενισμούς. Μια μέθοδος για να μειωθεί η ευαισθησία του στο θόρυβο είναι να λάβουμε υπ' όψη μόνο τους μηδενισμούς στις περιοχές όπου η τοπική μεταβλητότητα είναι μεγάλη, επειδή οι πραγματικές ακμές της εικόνας βρίσκονται σε περιοχές που έχουν μεγάλη τοπική διασπορά. Βάσει αυτής της παρατήρησης, μέτρα της τοπικής διασποράς της φωτεινότητας μπορούν να χρησιμοποιηθούν σαν ανιχνευτές ακμών.

(a) Αρχική Εικόνα

(b) Εικόνα Οριζόντιων Ακμών Roberts

(c) Εικόνα Κατακόρυφων Ακμών Roberts

(d) Εικόνα Ακμών Roberts

(e) Εικόνα Οριζόντιων Ακμών Prewitt

(f) Εικόνα Κατακόρυφων Ακμών Prewitt

(g) Εικόνα Ακμών Prewitt

(h) Εικόνα Οριζόντιων Ακμών Sobel

(i) Εικόνα Κατακόρυφων Ακμών Sobel

(j) Εικόνα Ακμών Sobel

Εικόνα 2.9:Αποτελέσματα Ανιχνευτών Ακμών

2.6 Κατωφλίωση ακμών

Οι περισσότεροι ανιχνευτές ακμών που περιγράφτηκαν παραπάνω παράγουν σαν έξοδο μια εικόνα τόνων γκρι E(k,l). Κάθε στίγμα αυτής της εικόνας έχει ως τιμή την έξοδο του ανιχνευτή ακμών στο αντίστοιχο στίγμα της αυθεντικής εικόνας. Αν η έξοδος του ανιχνευτή ακμών σε κάποιο στίγμα είναι μεγάλη, τότε υπάρχει μια τοπική ακμή. Αλλιώς, η θέση του στίγματος αντιστοιχεί στο φόντο. Συνεπώς, μετά την ανίχνευση ακμών απαιτείται μια κατωφλίωση:

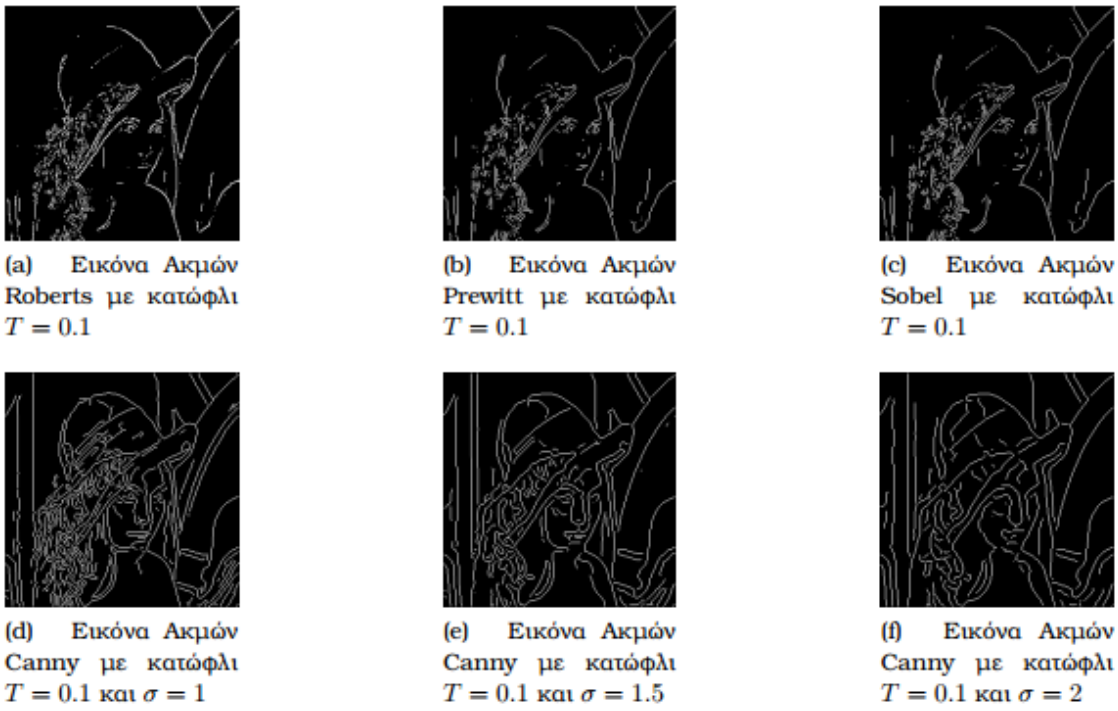
$$E(k,l)=\begin{cases}1 & \text{αν } e(k,l)\geq T\\ 0 & \text{αλλιώς}\end{cases}$$

Εξίσωση 2.6 : Κατωφλίωση Ακμών :

Το κατώφλι T μπορεί να επιλεχθεί με εξέταση του ιστογράμματος της εξόδου του ανιχνευτή ακμών, έτσι ώστε μόνο ένα μικρό ποσοστό των στιγμάτων e(k,l) να είναι πάνω από αυτό. Η κατωφλίωση (Εξίσωση 3) είναι καθολική, επειδή το T επιλέγεται με βάση καθολική πληροφορία και η (Εξίσωση 3) εφαρμόζεται σε ολόκληρη την εικόνα. Σε πολλές εφαρμογές, η έξοδος του ανιχνευτή ακμών μπορεί να χωριστεί σε περιοχές που παρουσιάζουν διαφορετικές στατιστικές ιδιότητες.

Συνεπώς, η καθολική κατωφλίωση μπορεί να προκαλέσει παχιές ακμές σε μια περιοχή και λεπτές ή διακεκομμένες ακμές σε μια άλλη περιοχή. Έτσι, η τοπικά προσαρμοζόμενη κατωφλίωση

είναι επιθυμητή. Η διαδικασία κατωφλίωση περιγράφεται πάλι από την σχέση (Εξίσωση 3), με κατώφλι T (k,l) προσαρμοζόμενο τοπικά. Μπορούν να χρησιμοποιηθούν διάφορες ευριστικές τεχνικές προσαρμογής. [18]



(a) Εικόνα Ακμών Roberts με κατώφλι $T = 0.1$

(b) Εικόνα Ακμών Prewitt με κατώφλι $T = 0.1$

(c) Εικόνα Ακμών Sobel με κατώφλι $T = 0.1$

(d) Εικόνα Ακμών Canny με κατώφλι $T = 0.1$ και $\sigma = 1$

(e) Εικόνα Ακμών Canny με κατώφλι $T = 0.1$ και $\sigma = 1.5$

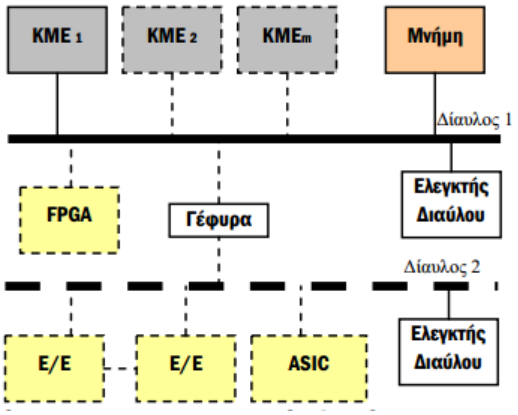
(f) Εικόνα Ακμών Canny με κατώφλι $T = 0.1$ και $\sigma = 2$

Εικόνα 2.6 : Εικόνες Ακμών Roberts, Prewitt, Sobel και Canny

2.7 Εφαρμογές σε Ενσωματωμένα Συστήματα

Ενσωματωμένα Συστήματα είναι αυτά στα οποία κάποιος επεξεργαστής λειτουργεί σαν μέρος μίας ολότητας, επιτελώντας συγκεκριμένο έργο, και στον οποίο εν γένει ο χρήστης δεν έχει πρόσβαση για να αλλάξει το πρόγραμμα ή την λειτουργικότητα του συστήματος. Τα Ενσωματωμένα Συστήματα (embedded systems) είναι υπολογιστικά συστήματα ειδικού σκοπού προσανατολισμένα στο να εξυπηρετήσουν τις ανάγκες των συσκευών της σύγχρονης ζωής όπως κινητά τηλέφωνα, palmtops, ελεγκτές αεροσκαφών και αυτοκινήτων κλπ. Για το λόγο αυτό συνήθως χαρακτηρίζονται από το μικρό τους μέγεθος και τα ιδιαίτερα χαρακτηριστικά τους ως προς την κατανάλωση ισχύος, την απόδοση σε συγκεκριμένες εφαρμογές και το χαμηλό τους κόστος. Ένα «Ενσωματωμένο Σύστημα» (Ε.Σ.) (Embedded System) αποτελεί υπολογιστική μονάδα με αρχιτεκτονική και αρχές λειτουργίας παρόμοιες με αυτές των συμβατικών υπολογιστών, η οποία ωστόσο προσαράζεται στις ανάγκες και απαιτήσεις της εκάστοτε εφαρμογής. Έτσι, και στην περίπτωση των Ε.Σ., βασικό δομικό στοιχείο αποτελεί ένας μικροεπεξεργαστής, ο οποίος βρίσκεται συνδεδεμένος μέσω μιας ιεραρχίας διαύλων με στοιχεία προσωρινής και μόνιμης αποθήκευσης (μνήμες RAM, EPRROM, Flash, non-Volatile). Παράλληλα, στα Ε.Σ. μπορεί να απαντώνται και στοιχεία εξειδικευμένου υλικού τα οποία επικοινωνούν με τα βασικά δομικά στοιχεία και καλούνται να επιτελέσουν

συγκεκριμένες εργασίες ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής σε απόδοση, κατανάλωση ισχύος, λειτουργίες Ε/Ε κ.α. Τα στοιχεία αυτά υλοποιούνται είτε σε μη προγραμματιζόμενο υλικό (VLSI, ASICs) είτε σε προγραμματιζόμενο υλικό (PLDs, FPGAs) και διασυνδέονται μέσω μιας ιεραρχίας (πιθανώς πολλών επιπέδων) διαύλων με τον μικροεπεξεργαστή και τη μνήμη .



Εικόνα 2.7 : Γενικό διάγραμμα αρχιτεκτονικής δομής Ενσωματωμένου Συστήματος

2.7.1 Παραδείγματα Ενσωματωμένων Εφαρμογών

Ας δούμε μερικά παραδείγματα ενσωματωμένων εφαρμογών, κατηγοριοποιημένα. Ο κατάλογος είναι μόνο ενδεικτικός, για να εκτιμηθεί το εύρος της αγοράς αλλά και οι δυνατότητες για περαιτέρω ανάπτυξη τέτοιων συστημάτων. Σε όλες τις παρακάτω κατηγορίες συστημάτων υπάρχει επεξεργαστής, στον οποίο ο χρήστης δεν έχει άμεση πρόσβαση. Για παράδειγμα, μπορεί σε ψηφιακά παιχνίδια τύπου Gameboy να μπορεί ο/η χρήστης να επιλέξει παιχνίδι με εισαγωγή κατάλληλης κασέτας, αλλά δεν έχει την δυνατότητα να προγραμματίσει την κονσόλα. Επίσης, σε διάφορα συστήματα όπως δρομολογητές δικτύων η κατασκευάστρια εταιρία μπορεί να αλλάζει το πρόγραμμα τους, αλλά και πάλι ο χρήστης δεν έχει άμεση πρόσβαση στο λογισμικό. Ενδεικτικές κατηγορίες είναι:

Υπολογιστές και Περιφερειακά

- Ασύρματα περιφερειακά (π.χ. Bluetooth ακουστικά/μικρόφωνα, IR ποντίκια και πληκτρολόγια, κλπ.)
- Ασύρματα δίκτυα (routers και κάρτες για Wi-Fi, 802.11, Bluetooth, κλπ.)
- Κονσόλες παιχνιδιών (π.χ. Sony Playstation, Microsoft Xbox, κλπ.)

Είδη Προσωπικής Ευκολίας

- Φορητά Παιχνίδια (π.χ. Gameboy, Nintendo, κλπ.)
- Κινητά τηλέφωνα

- Προσωπικοί Ψηφιακοί Βοηθοί (PDA)
- Φορητά συστήματα παγκοσμίου εντοπισμού (GPS – Global Positioning Systems)

Αυτοκίνητα

- Συστήματα ελέγχου απόδοσης μηχανής
- Συστήματα ελέγχου ρύπων
- Συστήματα ελέγχου άνεσης καμπίνας επιβατών (π.χ. κλιματισμός, ρυθμίσεις καθισμάτων, ρυθμίσεις καθρεφτών, κλπ.)

Οικιακές Συσκευές

- Ψυγεία, κουζίνες, φούρνοι μικροκυμάτων
- Τηλεοράσεις, συσκευές εικόνας (Video Cassette recorder – VCR, Digital Video Disc - DVD)
- Στερεοφωνικά νέας γενιάς και συστήματα αιθουσών προβολής σπιτιού (Home Theater)

Βιομηχανικά Συστήματα

- Βιομηχανικά Ρομπότ
- Αριθμητικά ελεγχόμενα μηχανουργικά μηχανήματα (π.χ. φρέζες με αριθμητικό έλεγχο – Computer Numerical Control – (CNC)

Υγεία, και Υποστηρικτική Τεχνολογία για Άτομα με Ειδικές Ανάγκες (AMEA)

- Φορητοί καρδιογράφοι
- Συστήματα καθαρισμού αίματος
- Συστήματα παρακολούθησης ζωτικών λειτουργιών ασθενών
- Απηνιδοτές
- Αναπηρικά αμαξίδια
- Συσκευές εισόδου ελεγχόμενες από επιστόμιο
- Συστήματα δημιουργίας ήχου (σύνθεση φωνής)

Τηλεπικοινωνίες

- Ψηφιακά τηλεφωνικά κέντρα
- Δικτυακός εξοπλισμός (δρομολογητές - routers, μεταγωγείς - switches, κλπ.)
- Δορυφορικά συστήματα Αγροτική Παραγωγή και Περιβάλλον
- Συστήματα παρακολούθησης και ελέγχου συνθηκών εδάφους
- Συστήματα ελέγχου περιβάλλοντος και αυτόματου ταΐσματος σε κτηνοτροφικές μονάδες
- Συστήματα παρακολούθησης ρύπων
- Συστήματα έγκαιρης προειδοποίησης φυσικών καταστροφών Ασφάλεια
- Συστήματα παρακολούθησης σπιτιών και συναγερμοί
- Συστήματα πυρόσβεσης

Μεταφορές

- Ηλεκτρονικά αεροσκαφών (avionics)

- Συστήματα εντοπισμού θέσης λεωφορείων, τραίνων, κλπ. Και ενημέρωσης επιβατών για επικείμενες αφίξεις
- Φωτεινές ενδείξεις χρόνου αναμονής σε σηματοδότες οδικής κυκλοφορίας και κυκλοφορίας πεζών
- Συστήματα για αυτόματη παρακολούθηση θέσης γραμμάτων/δεμάτων σε ταχυμεταφορικές εταιρίες

Υπηρεσίες

- Συστήματα αυτόματων τραπεζικών συναλλαγών (ATM)
- Συστήματα διατήρησης προτεραιότητας ουρών (π.χ. σε τράπεζες)
- Φωτεινές ενδείξεις (π.χ. κυλιόμενες οθόνες)
- Φορητά συστήματα για παραγγελίες σε εστιατόρια, κλπ. Δημόσια Διοίκηση
- Αυτόματα συστήματα στάθμευσης
- Συστήματα για κλήσεις σε παραβάτες κυκλοφορίας, στάθμευσης, κλπ

3. Κρυπτογράφηση

Ορισμός

Κρυπτογραφία είναι η επιστήμη της προστασίας δεδομένων, η οποία παρέχει τρόπους και μεθόδους για μετατροπή των δεδομένων σε μη αναγνώσιμη μορφή έτσι ώστε να καθίσταται αδύνατη η επεξεργασία και ανάγνωσή τους από μη εξουσιοδοτημένα άτομα. Την πληροφορία θα μπορεί να τη διαβάσει μόνο το άτομο για το οποίο προορίζεται.

Η κρυπτογραφία, λοιπόν, είναι το τεχνολογικό μέσο που παρέχει ασφάλεια στη μετάδοση των δεδομένων σε πληροφοριακά ή επικοινωνιακά συστήματα. Είναι ιδιαίτερα χρήσιμη σε περιπτώσεις αποστολής οικονομικών και προσωπικών δεδομένων και αποτελεί ένα χρήσιμο εργαλείο για την πιστοποίηση της αυθεντικότητας των εμπλεκομένων στη συναλλαγή, αλλά και για τον προσδιορισμό του ενόχου σε περίπτωση που η εμπιστευτικότητα και η ακεραιότητα των δεδομένων έχει παραβιαστεί. Εξαιτίας της ανάπτυξης του ηλεκτρονικού εμπορίου, οι κρυπτογραφικές τεχνικές είναι ιδιαίτερα κρίσιμες για την ανάπτυξη και τη χρήση καλά προστατευμένων πληροφοριακών και επικοινωνιακών δικτύων.

3.1 Μέθοδοι Κρυπτογράφησης

Δύο είναι οι βασικές μέθοδοι κρυπτογράφησης, η συμμετρική και η ασύμμετρη κρυπτογράφηση. Στη συμμετρική κρυπτογράφηση χρησιμοποιούμε το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ενός μηνύματος. Το κοινό αυτό κλειδί θα πρέπει να είναι γνωστό μόνο στα δύο επικοινωνούντα μέρη και κατά συνέπεια η μετάδοσή του από το ένα μέρος στο άλλο θα πρέπει να γίνει με απόλυτη ασφάλεια, κάτι που δεν είναι πάντα εφικτό και καθιστά έτσι τη μέθοδο της συμμετρικής κρυπτογράφησης ως μη απόλυτα αποτελεσματική.

Από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος DES (Data Encryption Standard), που χρησιμοποιείται και από την κυβέρνηση των ΗΠΑ, και το σύστημα Kerberos του γνωστού Πανεπιστημίου MIT. Στην ασύμμετρη κρυπτογράφηση ή κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιούμε διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος. Αυτά είναι το δημόσιο κλειδί (public key) και το ιδιωτικό κλειδί (private key).

3.2 Αλγόριθμοι αντικατάστασης

3.2.1 Αλγόριθμος του Καίσαρα

Ο αλγόριθμος του Καίσαρα αποτελεί μια ειδική κατηγορία των κρυπτογραφικών αλγορίθμων απλής αντικατάστασης (simple substitution cipher). Σε αυτόν τον κρυπτογραφικό αλγόριθμο, το κλειδί αποτελεί μια μετάθεση των γραμμάτων της αλφαβήτου. Η κρυπτογράφηση περιλαμβάνει αντικατάσταση κάθε γράμματος με το αντίστοιχο γράμμα που προκύπτει από τη μετάθεση. Αντίστοιχα, η αποκρυπτογράφηση γίνεται με χρήση της ανάστροφης μετάθεσης. Στον κρυπτογραφικό αλγόριθμο του Καίσαρα (Caesar cipher) το μήνυμα (αρχικό κείμενο) πρέπει να είναι μια ακολουθία από γράμματα. Κάθε γράμμα αντιστοιχίζεται με έναν αριθμό. Το κλειδί k είναι ένας αριθμός από το 1 ως το 25.

Ο κρυπτογραφικός αλγόριθμος του Καίσαρα είναι ουσιαστικά ένας συνηθισμένος τύπος κρυπτογραφικού αλγορίθμου ροής. Είναι πολύ εύκολο να σπάσει (κρυπταναλυθεί). Γενικότερα, παρά τον μεγάλο αριθμό κλειδιών, πράγμα που αποκλείει μια απλά επίθεση εξαντλητικής αναζήτησης (exhaustive search attack) , ένας κρυπτογραφικός αλγόριθμος απλής αντικατάστασης είναι εύκολο να σπάσει.

3.2.2 Αλγόριθμος Vigenere

Ένας άλλος παρόμοιος κρυπτογραφικός αλγόριθμος είναι ο αλγόριθμος Vigenere. Σε αυτόν τα γράμματα αντιστοιχίζονται πάλι με τους αριθμούς από το 0 ως το 25, όπως ακριβώς και με τον κρυπτογραφικό αλγόριθμο του Καίσαρα. Όμως το μυστικό κλειδί, τώρα, δεν είναι ένας αριθμός αλλά μια μικρή ακολουθία γραμμάτων, όπως γα παράδειγμα μια λέξη.

Κατά την κρυπτογράφηση προστίθεται το αριθμητικό ισοδύναμο κάθε γράμματος του αρχικού κειμένου με το αριθμητικό ισοδύναμο ενός γράμματος του κλειδιού. Επειδή συνήθως το μήκος του αρχικού κειμένου είναι μεγαλύτερο από το μήκος του κλειδιού, τα γράμματα του κλειδιού ανακυκλώνονται και επαναλαμβάνεται η χρήση τους όσο χρειάζεται.

Αξίζει να σημειώσουμε ότι ο κρυπτογραφικός αλγόριθμος του Καίσαρα είναι μια ειδική περίπτωση του κρυπτογραφικού αλγορίθμου Vigenere για την περίπτωση που το μήκος της λέξης του κλειδιού είναι ίσο με 1.

Αυτός ο αλγόριθμος ανήκει στην κατηγορία των αποκαλούμενων Κρυπτογραφικών Αλγορίθμων Πολυαλφαβητικής Αντικατάστασης (polyalphabetic substitution ciphers). Ο κρυπτογραφικός αλγόριθμος Vigenere είναι και αυτός μια ειδική μορφή κρυπτογραφικού αλγορίθμου ροής. Ακριβώς όπως με τον κρυπτογραφικό αλγόριθμο του Καίσαρα, χρησιμοποιεί πρόσθεση με υπολογισμό του modulo 26 αντί για πρόσθεση με υπολογισμό του modulo 2 για να συνδυάσει το αρχικό κείμενο με το κλειδί. Είναι απλά η λέξη-κλειδί, η οποία επαναλαμβάνεται όσο χρειάζεται. Φυσιολογικά ο κρυπτογραφικός αλγόριθμος Vigenere σπάζει εύκολα.

3.2.3 Αλγόριθμος σημειωματάριου μιας χρήσης

Ο κρυπτογραφικός αλγόριθμος του σημειωματάριου μιας χρήσης (The one-time pad cipher) ή αλγόριθμος του Vernam είναι μια ειδική παραλλαγή κρυπτογραφικού αλγορίθμου ροής. Το

ψευδοτυχαίο κλειδί αντικαθίσταται από μια τυχαία (μη επαναλαμβανόμενη) ακολουθία δυαδικών ψηφίων (bits) η οποία χρησιμοποιείται μόνο μια φορά (από αυτό προκύπτει και ο χαρακτηρισμός «μιας χρήσης»). Αν χρησιμοποιηθεί σωστά, ο αλγόριθμος αυτός αποδεδειγμένα δεν είναι δυνατόν να σπάσει (unbreakable).

Το μοναδικό πρόβλημα αφόρα τη διαχείριση των κλειδιών. Πριν να καταστεί δυνατή η κρυπτογραφημένη επικοινωνία, τα δυο μέρη (αποστολέας και παραλήπτης) πρέπει να συμφωνήσουν σε τόσο υλικό τυχαίων κλειδιών όσα και τα δεδομένα που θα μεταδοθούν.

3.3 Αλγόριθμοι Μετατόπισης

3.3.1 Μέθοδος της σκυτάλης

Είναι μια μέθοδος κρυπτογραφίας που χρησιμοποιούνταν από τους αρχαίους Έλληνες. Η μέθοδος αυτή αποτελείται από μια σκυτάλη ορισμένης διαμέτρου, η οποία έχει τυλιγμένη γύρω της ελικοειδώς μια λωρίδα δέρματος. Το κείμενο γράφεται σε στήλες, ένα γράμμα σε κάθε έλικα. Όταν ξετυλίγεται η λωρίδα, το κείμενο είναι ακατάλληλο εξαιτίας της ανάμειξης των γραμμάτων. Το "κλειδί" στην μυστικότητα του μηνύματος είναι η διάμετρος του κυλίνδρου .

3.4 Κατηγορίες Κρυπτοσυστημάτων

Τα κρυπτογραφικά συστήματα ταξινομούνται, γενικά, με βάση τρία ανεξάρτητα κριτήρια.

• *Τον τύπο των διαδικασιών που χρησιμοποιούνται για το μετασχηματισμό του αρχικού κειμένου σε ένα κρυπτογράφημα* .

Το σύνολο των αλγορίθμων κρυπτογράφησης στηρίζεται σε δύο γενικές αρχές: στην αντικατάσταση (substitution) σύμφωνα με την οποία κάθε στοιχείο του αρχικού κειμένου, είτε είναι δυαδικό ψηφίο, είτε χαρακτήρας, είτε ομάδα δυαδικών ψηφίων ή χαρακτήρων, αντικαθίσταται από άλλο στοιχείο και στη μετάθεση (permutation) στην οποία τα στοιχεία του αρχικού κειμένου αναδιατάσσονται. Βασική προϋπόθεση αποτελεί η μη απώλεια οποιασδήποτε πληροφορίας, ώστε όλες οι διαδικασίες να είναι αντιστρέψιμες.

• *Τον αριθμό των κλειδιών που χρησιμοποιούνται*.

Εάν ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί, τότε το σύστημα αναφέρεται ως συμμετρικό ή μοναδικού κλειδιού ή μυστικού κλειδιού ή συμβατικής κρυπτογραφίας. Εάν, όμως, ο πομπός και ο δέκτης χρησιμοποιούν διαφορετικά κλειδιά, τότε το σύστημα αναφέρεται ως ασύμμετρο, ή σύστημα ζεύγους κλειδιών, ή κρυπτογραφίας δημοσίου κλειδιού.

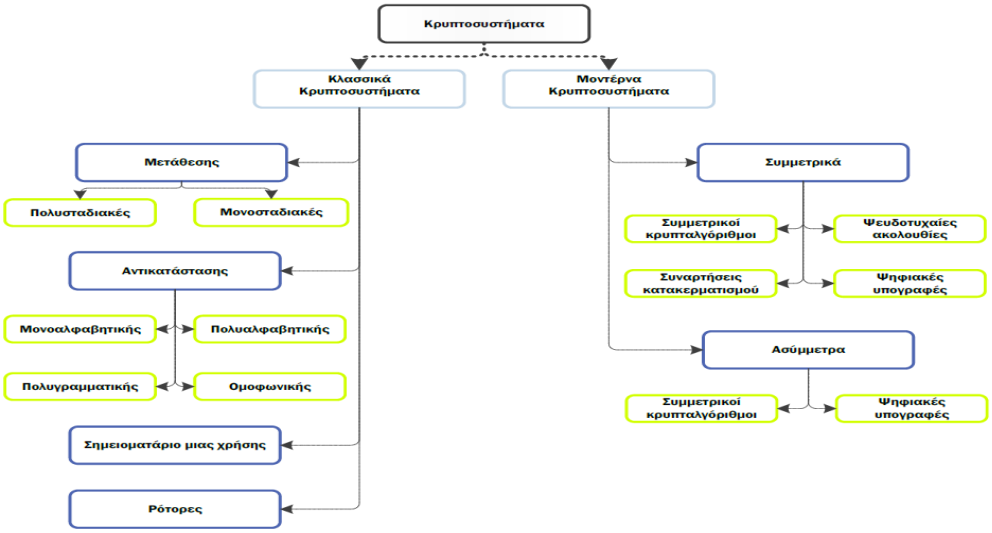
• *Τον τρόπο με τον οποίο επεξεργάζεται το αρχικό κείμενο*.

Ένας κωδικοποιητής τμημάτων (block cipher) επεξεργάζεται την είσοδο ενός τμήματος στοιχείων κάθε φορά, παράγοντας ένα τμήμα εξόδου για κάθε συγκεκριμένο τμήμα εισόδου. Αντίθετα, ένας κωδικοποιητής ροής (stream cipher) επεξεργάζεται κατά συνεχή τρόπο τα στοιχεία εισόδου και κάθε φορά παράγεται ως έξοδος ένα στοιχείο, με τη σειρά που καταφθάνουν τα δεδομένα.

3.5 Σύγχρονα Κρυπτοσυστήματα

Τα σύγχρονα κρυπτοσυστήματα χωρίζονται με βάση τα κλειδιά σε:

- Μυστικού ή Συμμετρικού Κλειδιού (Symmetric Key), χρησιμοποιούν το ίδιο μυστικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.
- Δημοσίου ή Ασύμμετρου Κλειδιού (Asymmetric Key), χρησιμοποιούν διαφορετικό κλειδί για κρυπτογράφηση (δημόσιο κλειδί παραλήπτη) και διαφορετικό για αποκρυπτογράφηση (προσωπικό κλειδί παραλήπτη)

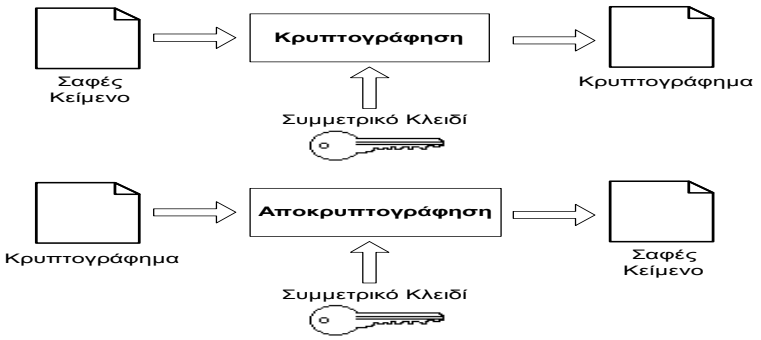


Σχήμα 3.5 : Κρυπτοσύστημα

3.6 Μεθοδολογίες

3.6.1 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, γνωστό ως *μυστικό ή συμμετρικό κλειδί (secret key)*, με το οποίο γίνεται η κρυπτογράφηση και η αποκρυπτογράφηση της πληροφορίας. Ο αποστολέας και ο παραλήπτης είναι οι μοναδικές οντότητες που γνωρίζουν και χρησιμοποιούν το μυστικό κλειδί. Το Σχήμα 3.6.1 περιγράφει την διαδικασία της συμμετρικής κρυπτογραφίας. Τα μηνύματα προς κρυπτογράφηση, γνωστά ως το *σαφές κείμενο (plaintext)*, κρυπτογραφούνται με χρήση του συμμετρικού (ή μυστικού) κλειδιού. Η διαδικασία της κρυπτογράφησης έχει ως έξοδο ένα κείμενο σε ακατανόητη μορφή, γνωστό ως *κρυπτογράφημα (ciphertext)*. Η ασφάλεια της μεταδιδόμενης πληροφορίας επιτυγχάνεται ακριβώς επειδή το κρυπτογράφημα μεταδίδεται σε ακατανόητη μορφή. Η διαδικασία της ανάκτησης της αρχικής πληροφορίας με τη χρήση του ίδιου συμμετρικού κλειδιού ονομάζεται αποκρυπτογράφηση.



Σχήμα 3.6.1 : Διαδικασία συμμετρικής κρυπτογραφίας

Στα πλεονεκτήματα της συμμετρικής κρυπτογραφίας συγκαταλέγονται οι υψηλές ταχύτητες κρυπτογράφησης και αποκρυπτογράφησης που μπορούν να υπερβούν τα 100Mbps καθώς επίσης και οι μικρές απαιτήσεις της σε μνήμη και υπολογιστική ισχύ. Έτσι καθίσταται δυνατή η εφαρμογή της σε περιβάλλοντα όπως αυτά ενός κινητού τηλεφώνου ή μιας έξυπνης κάρτας. Επίσης το μέγεθος του κρυπτογραφήματος είναι αρκετά μικρότερο από αυτό του αρχικού κειμένου.

Η ανάγκη της ανταλλαγής του συμμετρικού κλειδιού μεταξύ αποστολέα και παραλήπτη είναι ένας από τους σημαντικότερους περιορισμούς της συμμετρικής κρυπτογραφίας. Η ασφάλεια της συμμετρικής κρυπτογραφίας βασίζεται αποκλειστικά στο γεγονός ότι ο αποστολέας και ο παραλήπτης μοιράζονται το συμμετρικό κλειδί πριν από την αποστολή του μηνύματος. Έτσι κρίνεται απαραίτητη η επίτευξη μιας ασφαλούς ζεύξης για την μεταφορά του συμμετρικού κλειδιού. Κάτι τέτοιο όμως δεν είναι πάντα εφικτό εξαιτίας πρακτικών αλλά και λειτουργικών δυσκολιών. Η διαδικασία της ασφαλούς ανταλλαγής του συμμετρικού κλειδιού γίνεται ακόμα μεγαλύτερη όταν οι δύο οντότητες, ο παραλήπτης και ο αποστολέας , είναι άγνωστες μεταξύ τους. Σε αυτή την περίπτωση προκύπτει η ανάγκη πιστοποίησης της ταυτότητας κάθε οντότητας έτσι ώστε να αποφευχθεί η διαβίβαση του κλειδιού σε κάποια τρίτη, μη εξουσιοδοτημένη οντότητα. Συνήθως στη συμμετρική κρυπτογραφία η μεταφορά του κλειδιού γίνεται είτε μέσω μιας φυσικής ζεύξης (ανταλλαγή κλειδιού πρόσωπο με πρόσωπο) είτε μέσω μίας έμπιστης τρίτης οντότητας, την οποία οι χρήστες εμπιστεύονται για την ασφαλή μεταφορά του κλειδιού.

Ένας ακόμη σημαντικός περιορισμός αφορά στη δυσκολία κλιμάκωσης της μεθόδου. Καθώς το πλήθος των χρηστών που θέλουν να επικοινωνήσουν μεταξύ τους μεγαλώνει, γίνεται αυτονόητο ότι μεγαλώνει και το πλήθος των κλειδιών που θα χρησιμοποιηθούν για κάθε επιμέρους επικοινωνία. Για την επίτευξη επικοινωνίας μεταξύ n χρηστών απαιτούνται $n^2/2$ μοναδικά συμμετρικά κλειδιά, συμπεριλαμβανομένου και του κλειδιού που έχει κάθε χρήστης για τον εαυτό του. Τα προβλήματα της διαχείρισης των κλειδιών (key management) γίνονται ακόμα μεγαλύτερα γιατί κάθε κλειδί θα πρέπει περιοδικά να αντικαθίσταται από κάποιο καινούριο με σκοπό τη μείωση των δεδομένων που κρυπτογραφούνται με το ίδιο κλειδί.

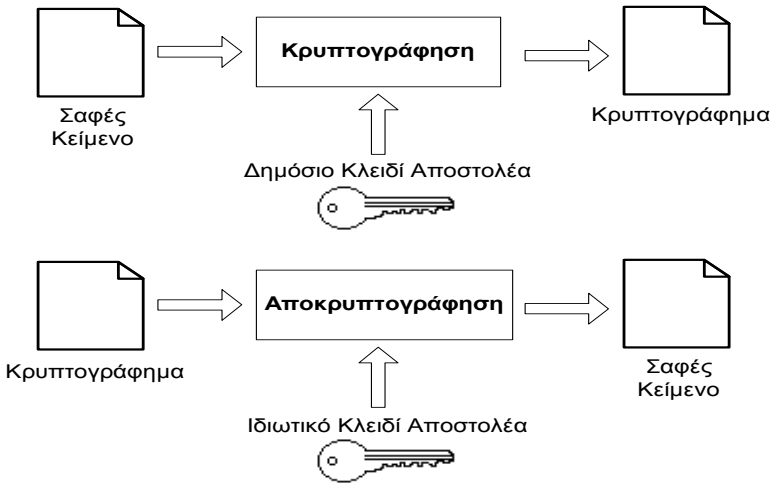
3.6.2 Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου Κλειδιού

Στα μέσα της δεκαετίας του ‘70 οι Whitfield Diffie και Martin Hellman πρότειναν μια νέα τεχνική για τον περιορισμό των προβλημάτων της συμμετρικής κρυπτογραφίας. Η τεχνική αυτή, γνωστή ως *κρυπτογραφία δημοσίου κλειδιού* ή *ασύμμετρη κρυπτογραφία*, βασίζεται στην ύπαρξη ενός *ζεύγους κλειδιών (key pair)*. Σε αυτό το ζεύγος, τα κλειδιά, αν και σχετίζονται μεταξύ τους με κάποια μαθηματική σχέση, είναι επαρκώς διαφορετικά έτσι ώστε η γνώση του ενός να μην επιτρέπει την παραγωγή ή τον υπολογισμό του άλλου. Αυτό σημαίνει ότι το ένα από τα κλειδιά μπορεί να είναι δημόσια γνωστό και διαθέσιμο. Το κλειδί αυτό ονομάζεται *δημόσιο κλειδί (public key)* και

χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Το δεύτερο κλειδί είναι απαραίτητο να μένει ιδιωτικό, γι' αυτό και ονομάζεται *ιδιωτικό κλειδί (private key)* και χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων. Βασικά χαρακτηριστικά του δημόσιου και του ιδιωτικού κλειδιού είναι:

- Κάθε κλειδί είναι ένα δυαδικό αλφαριθμητικό.
- Τα κλειδιά, δημόσια και ιδιωτικά, παράγονται ταυτόχρονα από ειδικό πρόγραμμα λογισμικού.
- Τα κλειδιά δεν είναι ταυτόσημα, αλλά σχετίζονται μοναδικά έτσι ώστε να είναι δυνατή η χρήση τους για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Η διαδικασία μέσω της οποίας παράγεται το ζεύγος των κλειδιών εξασφαλίζει ότι κάθε κλειδί σχετίζεται μοναδικά με το ταίρι του και κανένα κλειδί δεν μπορεί να παραχθεί από το άλλο.
- Τα κλειδιά, δημόσια και ιδιωτικά, που ανήκουν σε ένα ζεύγος είναι συμπληρωματικά, δηλαδή οι πληροφορίες που κρυπτογραφούνται με το ένα κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το άλλο και αντίστροφα. Με άλλα λόγια, ένα μήνυμα που έχει κρυπτογραφηθεί χρησιμοποιώντας ένα δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί.
- Κάθε οντότητα που συμμετέχει σε ένα σύστημα επικοινωνίας δημοσίου κλειδιού έχει το δικό της ζεύγος δημόσιου και ιδιωτικού κλειδιού.
- Το ιδιωτικό κλειδί:
    - Προστατεύεται από τον ιδιοκτήτη του
    - Χρησιμοποιείται για την ψηφιακή υπογραφή μηνυμάτων
- Το δημόσιο κλειδί:
    - Διανέμεται ελεύθερα και είναι προσβάσιμο σε οποιονδήποτε
    - Χρησιμοποιείται για την πιστοποίηση ψηφιακών υπογραφών
    - Χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων
    - Αποθηκεύεται μέσα σε «ψηφιακά πιστοποιητικά» που παρέχουν την ακεραιότητα και την αυθεντικότητα του ιδιοκτήτη του κλειδιού
- Παρόλο που τα δημόσια κλειδιά μπορούν να διανέμονται ελεύθερα, τα ιδιωτικά κλειδιά δε θα πρέπει ποτέ να γίνονται γνωστά σε μη εξουσιοδοτημένες οντότητες.

Το Σχήμα 3.6.2(a) περιγράφει τη διαδικασία κρυπτογράφησης δημοσίου κλειδιού. Ο αποστολέας κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη, το οποίο είναι ελεύθερα διαθέσιμο, το μήνυμα που θέλει να του στείλει. Το κρυπτογραφημένο μήνυμα φτάνει στον παραλήπτη ο οποίος το αποκρυπτογραφεί με το ιδιωτικό κλειδί του.



Σχήμα3.6.2(a) : Διαδικασία Κρυπτογράφησης Δημοσίου Κλειδιού

Η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων καθώς και για την ψηφιακή υπογραφή τους. Η ασφάλεια της κρυπτογραφίας δημοσίου κλειδιού βασίζεται ακριβώς στο γεγονός ότι είναι υπολογιστικά αδύνατη η παραγωγή του ιδιωτικού από το δημόσιο κλειδί. Θεωρητικά, βέβαια, το ιδιωτικό κλειδί μπορεί πάντα να υπολογιστεί αλλά το κόστος σε χρόνο, μνήμη και υπολογιστική ισχύ για κάτι τέτοιο είναι τόσο μεγάλο που καθίσταται πρακτικά αδύνατο.

Το σημαντικότερο πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι ότι δεν απαιτείται ανταλλαγή μυστικού κλειδιού. Το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο, πράγμα που κάνει τη διαχείριση των κλειδιών (key management) πολύ ευκολότερη, ενώ το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, καθιστώντας έτσι δυσκολότερη την παραποίησή του. Επίσης με την κρυπτογραφία δημοσίου κλειδιού καθίσταται δυνατή η υλοποίηση μιας πολύ σημαντικής κρυπτογραφικής λειτουργίας, αυτή της ψηφιακής υπογραφής δεδομένων.

Η κρυπτογραφία δημοσίου κλειδιού έχει μεγάλες απαιτήσεις σε υπολογιστική ισχύ, σχεδόν 100 φορές παραπάνω από αυτή που απαιτείται στην συμμετρική κρυπτογραφία. Επίσης, όπως έχει ήδη αναφερθεί, είναι αρκετά αργή ειδικά όταν πρόκειται για μεγάλα μηνύματα. Γι' αυτό το λόγο συνήθως δεν κρυπτογραφούνται δεδομένα αλλά συμμετρικά κλειδιά, με τη μέθοδο του ψηφιακού φακέλου που περιγράφεται στη συνέχεια.

Πιο αναλυτικά για την ασφαλή αποστολή ενός μηνύματος, ο αποστολέας χρησιμοποιεί για την κρυπτογράφηση του το δημόσιο κλειδί του προβλεπόμενου παραλήπτη. Το μήνυμα είναι δυνατόν να διαβαστεί μόνον από αυτόν (τον παραλήπτη), διότι η αποκρυπτογράφησή του γίνεται με χρήση του μυστικού, ιδιωτικού του κλειδιού. Επομένως, εξασφαλίζεται το απόρρητο του μηνύματος. Εξάλλου, είναι υπολογιστικά ανέφικτο να εξαχθεί το ιδιωτικό κλειδί από το αντίστοιχο δημόσιο κλειδί.

Η ασφάλεια της όλης διαδικασίας βασίζεται στη μυστικότητα των ιδιωτικών κλειδιών. Αν παραβιαστεί η ακεραιότητα του συστήματος, υπάρχει η δυνατότητα να αλλάξουν μόνο τα χρησιμοποιούμενα κλειδιά, αντί να αλλάξει ολόκληρος ο αλγόριθμος κρυπτογράφησης όπως θα συνέβαινε στην περίπτωση της συμμετρικής κρυπτογράφησης. Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στην γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται.

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα σταλεί από τον αποστολέα μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο αφού μπορεί να αποκρυπτογραφηθεί μόνο από το ιδιωτικό του κλειδί. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.

Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι και την πιστοποίηση του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στην συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα (Σχήμα 3.6.2(b)).

Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί και την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει ο οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη την διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

Σχήμα 3.6.2(b) : Επαλήθευση ταυτότητας αποστολέα.

Συνδυάζοντας τις δύο τεχνικές που παρουσιάστηκαν παραπάνω είναι εφικτό να επιτευχθεί και εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα να παραμένει γνωστό μόνο στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης να γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στην συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στην συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

3.6.3 Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου

Ιδιαίτερο ενδιαφέρον για την επίτευξη ασφαλούς επικοινωνίας μεταξύ δύο μερών παρουσιάζει η υβριδική κρυπτογραφία που είναι γνωστή και ως *ψηφιακός φάκελος (digital envelope)* και αξιοποιεί ταυτόχρονα τις τεχνικές συμμετρικής και ασύμμετρης κρυπτογραφίας. Η υβριδική

αυτή κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα. Τα βήματα που ακολουθούνται για τη δημιουργία ενός ψηφιακού φακέλου είναι τα εξής:

1. Δημιουργείται ένα συμμετρικό κλειδί με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας (π.χ. του DES).
2. Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.
3. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.
4. Τα δύο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

Ο παραλήπτης ανοίγει τον ψηφιακό του φάκελο αποκρυπτογραφώντας με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί. Με χρήση του συμμετρικού κλειδιού ο παραλήπτης αποκρυπτογραφεί το αρχικό κείμενο. Μετά την επίτευξη μιας ασφαλούς επικοινωνίας μεταξύ αποστολέα και παραλήπτη το συμμετρικό κλειδί καταστρέφεται.

Η χρήση της υβριδικής κρυπτογραφίας βοήθα στο να ξεπεραστούν κάποιες σημαντικές αδυναμίες της κρυπτογραφίας δημοσίου κλειδιού. Συγκεκριμένα η κρυπτογραφία δημοσίου κλειδιού είναι αρκετά αργή σε σύγκριση με την συμμετρική κρυπτογραφία, ειδικά όταν πρόκειται να κρυπτογραφηθούν μεγάλα μηνύματα. Ακόμα όμως και στην περίπτωση που ο όγκος των προς κρυπτογράφηση δεδομένων είναι μικρός, έχει καθιερωθεί να χρησιμοποιείται η κρυπτογραφία ψηφιακού φακέλου. Με αυτόν τον τρόπο αποφεύγεται οποιαδήποτε σύγχυση ως προς το αν το αποτέλεσμα της αποκρυπτογράφησης είναι δεδομένα ή συμμετρικό κλειδί.

Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούνται ευρέως μέσα ενσωματωμένα συστήματα. Οι εφαρμογές των κρυπτογραφικών αλγορίθμων περιλαμβάνουν την καθιέρωση πιστοποιητικών (π.χ. επικύρωση), εξασφαλίζοντας το περιεχόμενο (π.χ. κρυπτογράφηση/αποκρυπτογράφηση των στοιχείων επικοινωνίας ή των δικαίωμα-ρυθμισμένων αντικειμένων), την προστασία IP, και τον έλεγχο πλαστογράφηση-αντίστασης.

Περιορισμένων πόρων ενσωματωμένα συστήματα μπορούν να επωφεληθούν σε μεγάλο βαθμό από τη χρησιμοποίηση κρυπτογραφικών αλγορίθμων που είναι συντονισμένοι για να καταναλώνουν όσο το δυνατόν ελάχιστους πόρους του συστήματος, ενώ την ίδια στιγμή παρέχει εύλογη απόδοση.

3.7 Αλγόριθμοι Κρυπτογράφησης

Οι κρυπτογραφικοί αλγόριθμοι μπορεί να κατηγοριοποιηθούν ως εξής:

- Δημόσιων (ή ασύμμετρη) κλειδιών αλγόριθμοι
- Ιδιωτικών (ή συμμετρικό) κλειδιών αλγόριθμοι
- Αλγόριθμοι κατακερματισμού.

Οι κρυπτογραφικοί αλγόριθμοι αποτελούν το μέσο για το μετασχηματισμό μηνυμάτων σε κρυπτογραφημένα κείμενα. Μια διαδικασία κρυπτογράφησης συμβολίζεται ως: c= ek (m) , όπου m είναι το αρχικό κείμενο, e είναι ο αλγόριθμος κρυπτογράφησης, k είναι το μυστικό κλειδί και c είναι το κρυπτογραφημένο κείμενο. Αντίστοιχα, η διαδικασία της αποκρυπτογράφησης συμβολίζεται ως : m = dk (c). Συνήθως ο κρυπτογραφικός αλγόριθμος e είναι δημόσια γνωστός και η μυστικότητα του αρχικού κειμένου m εξαρτάται αποκλειστικά από τη μυστικότητα του μυστικού κλειδιού k , αφού το κρυπτογραφημένο κείμενο θεωρείται ότι είναι γνωστό.

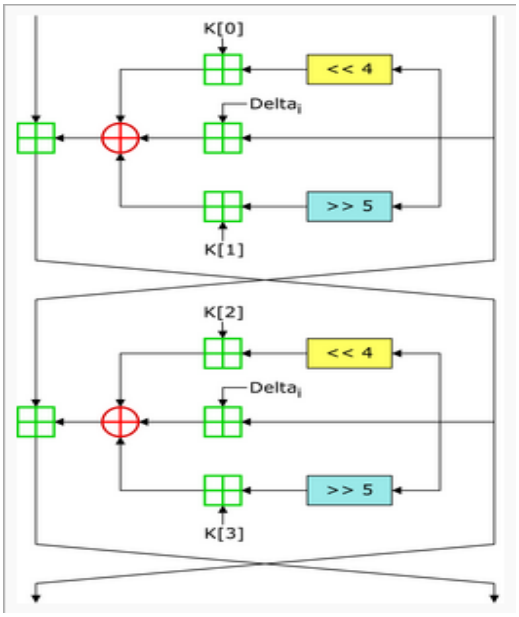
Αντίστοιχα με τα κρυπτογραφικά συστήματα και οι αλγόριθμοι γενικά

ταξινομούνται σε κατηγορίες ανάλογα με τα κλειδιά (συμμετρικούς και ασύμμετρους) και τον τρόπο κρυπτογράφησης των μηνυμάτων (αντικατάστασης και μετατόπισης).

3.8 Αλγόριθμοι Συμμετρικής Κρυπτογράφησης

3.8.1 Αλγόριθμος TEA (Tiny Encryption Algorithm)

Ο TEA (Tiny Encryption Algorithm) είναι ένας ταχύτερους και πιο αποδοτικούς αλγόριθμους κρυπτογράφησης που υπάρχουν. Αναπτύχθηκε από τον David Wheeler και τον Roger Needham στο Εργαστήριο Υπολογιστών του Πανεπιστημίου του Cambridge.. Η δομή Feistel, μέσω της οποίας υλοποιείται ο TEA , αποτελείται από 64 πανομοιότυπους γύρους που αποτελούνται από bit λειτουργιών όπως μετατοπίσεις, προσθήκη / αφαίρεση mod 2^8 και την αποκλειστική ή(XOR) πράξη. Αυτός είναι ένας πολύ έξυπνος τρόπος να παρέχει τις ιδιότητες του αλγόριθμου Shannon οι οποίες είναι το diffusion και το confusion, χωρίς τη ρητή ανάγκη για κουτιά P-και S-boxes, αντίστοιχα. Κρυπτογραφεί 64 bits δεδομένων κάθε φορά με ένα κλειδί των 128-bit. Φαίνεται εξαιρετικά ανθεκτικό στη διαφορική κρυπτανάλυση, και επιτυγχάνει το πλήρες diffusion (όπου μόλις ένα διαφορετικό bit θα προκαλέσει κατά προσέγγιση 32 bit διαφορές στο κρυπτοκείμενο) μετά από μόλις έξι γύρους. Οι επιδόσεις σε ένα σύγχρονο επιτραπέζιο υπολογιστή ή σε ένα σταθμό εργασίας είναι πολύ εντυπωσιακές. Στη παρούσα εργασία για την υλοποίηση της κρυπτογράφησης των δεδομένων μας κάναμε χρήση του αλγόριθμου κρυπτανάλυσης TEA (Tiny Encryption Algorithm) και οι λόγοι για τους οποίους επιλέξαμε τον συγκεκριμένο παρατίθενται στη συνέχεια.



Εικόνα 3.8.1 : Two Feistel rounds (one cycle) of TEA

- Απλότητα : η απλότητα του συγκεκριμένου κώδικα είναι εύκολο να αποδειχθεί αν λάβουμε υπόψη πως οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης εκπροσωπούνται μόνο σε επτά γραμμές κώδικα C. Ο αλγόριθμος απαιτεί πολύ λίγη μνήμη και, σε αντίθεση με άλλα block κρυπταλγορίθμων παρόμοια δύναμη, καθώς δεν απαιτεί πίνακες για τα P-boxes ή S-boxes (αναζήτηση αντιμετάθεσης ή υποκατάστασης). Αντιθέτως, χρησιμοποιεί πολλαπλά περάσματα, επιλέγοντας «ένα μεγάλο αριθμό επαναλήψεων και όχι ένα περίπλοκο πρόγραμμα». [6], οι συντάκτες προτείνουν 32 περάσματα (64 γύροι), αλλά να σημειωθεί ότι μόλις έξι κύκλοι θα παρέχουν εξαιρετικό diffusion , επομένως προτείνουν ότι 16 δεκαέξι περάσματα μπορούν να χρησιμοποιηθούν όπου η απόδοση είναι κρίσιμη. Ο TEA έχει εφαρμοστεί σε πολλές γλώσσες, συμπεριλαμβανομένων των C, C + +, C #, Forth, Java, JavaScript, Macromedia Flash, Perl, PHP, Python, Ruby, SQL Server, Tcl, αλλά και μια πληθώρα από assembly γλώσσες. Έχει αναπτυχθεί

σε πολλούς σύγχρονους server και προσωπικούς υπολογιστές, και σε ενσωματωμένα συστήματα και μικρές συσκευές, όπως οι πλοηγοί Palm, κινητά τηλέφωνα, και το Xbox της Microsoft.

- Απόδοση : Ο TEA απασχολεί ένα δίκτυο Feistel [1] (ένα συμμετρικό block κρυπταλγόριθμου) που χρησιμοποιεί ένα συνδυασμό από bit μετατόπισης, XOR, και λειτουργίες πρόσθεσης ώστε να δημιουργήσει τα απαραίτητα diffusion και confusion των δεδομένων. Κάνει αυτές τις λειτουργίες σε λέξεις των 32 bit και όχι μόνο σε bytes, με αποτέλεσμα την παροχή βελτιστοποίησης που όπως σημειώνουν οι συγγραφείς αποφεύγεται η «σπατάλη την ισχύος ενός υπολογιστή." Ο TEA χρησιμοποιεί ένα κλειδί των 128 bit (4 λέξεις), αναμιγνύοντας σε επιμέρους λεκτικά στοιχεία του σε ένα αποτελεσματικό βασικό πρόγραμμα. Η αρχική εφαρμογή λειτουργεί σε 64 bits (δύο λέξεις) δεδομένων σε έναν χρόνο, αν και παραλλαγές (όπως TEA Block) επιτρέπουν αυθαίρετες μεγέθους μπλοκ.
- Ισχύς : Ο TEA κατάφερε να αντεπεξέλθει χρόνια κρυπτανάλυσης αρκετά καλά. Μερικές μικρές αδυναμίες βρέθηκαν στον αλγόριθμο λίγο μετά τη δημοσίευση του. Αυτές διορθώθηκαν από τους συγγραφείς με τη μορφή των επεκτάσεων TEA, που συχνά αναφέρεται ως XTEA [7]. Οι διορθώσεις δεν μετέβαλαν σημαντικά τον αλγόριθμο με αποτέλεσμα να διατηρήσει την απόδοση και την απλότητα του. Για παράδειγμα, ο αλγόριθμος modifiedXTEA μπορεί ακόμα να εκπροσωπείται σε επτά μόνο γραμμές κώδικα C για καθένα από τα βήματα κρυπτογράφησης και αποκρυπτογράφησης. Την ίδια στιγμή, οι συγγραφείς δημοσίευσαν ένα τροποποιημένο μπλοκ αλγόριθμου (TEA Block), που συχνά αποκαλείται XXTEA (δημοσιεύτηκε το 1998).

Ο TEA ωστόσο υστερεί στην περίπτωση των ισοδύναμων κλειδιών, αυτό οφείλεται στο γεγονός ότι κάθε κλειδί ισοδυναμεί σε τρία άλλα κλειδιά το οποίο τελικά σημαίνει ότι το αποτελεσματικό μέγεθος του κλειδιού είναι μόλις 126 bits. Λόγω αυτής της αδυναμίας έχει αναπτυχθεί μια μέθοδος για hacking στην κονσόλα παιχνιδιού του Microsoft Xbox, όπου ο TEA χρησιμοποιήθηκε ως συνάρτηση κατακερματισμού, [13]. Ο κρυπταλγόριθμος είναι επίσης ευάλωτος σε πιθανό κλειδί επίθεσης που απαιτεί 2^{23} επιλεγμένα απλά κρυπτοκείμενα με ένα πιθανό ζεύγος κλειδιών, με 2^{32} πολυπλοκότητα χρόνου [12].

3.8.2 Αλγόριθμος DES (Data Encryption Standard)

Σύμφωνα με το πρότυπο DES το αρχικό κείμενο είναι μεγέθους 64-bit και το κλειδί έχει μήκος 56-bit. Τα απλά κείμενα μεγαλύτερου μεγέθους επεξεργάζονται σε τμήματα των 64-bit. Το αρχικό κείμενο έχει τρία στάδια επεξεργασίας. Στην αρχή, το κείμενο των 64-bit ακολουθεί έναν αρχικό μετασχηματισμό (initial permutation - IP) στα πλαίσια του οποίου τα bits αναδιατάσσονται για να παραχθεί η μετασχηματισμένη είσοδος. Ακολουθεί ένα στάδιο που αποτελείται από 16 επαναλήψεις της ίδιας λειτουργίας. Η έξοδος της τελευταίας επανάληψης, δηλαδή της δέκατης έκτης, αποτελείται από 64-bit που αποτελούν συνάρτηση του αρχικού κειμένου και του κλειδιού. Το αριστερό μισό τμήμα και το δεξί μισό τμήμα της εξόδου αντιμετατίθενται, ώστε να παραχθεί η αρχική έξοδος. Η τιμή αυτή τροποποιείται με βάση ένα μετασχηματισμό που είναι ο αντίστροφος του αρχικού μετασχηματισμού (inverse initial permutation – IP-1), ώστε να παραχθεί το κρυπτογράφημα των 64-bit.

Το κλειδί των 56 - bit τροποποιείται από μια συνάρτηση μετασχηματισμού. Κατόπιν, για καθεμία από τις 16 επαναλήψεις, παράγεται ένα υποκλειδί Ki από το συνδυασμό μιας αριστερής κυκλικής μετατόπισης και ενός μετασχηματισμού. Η συνάρτηση μετασχηματισμού παραμένει ίδια

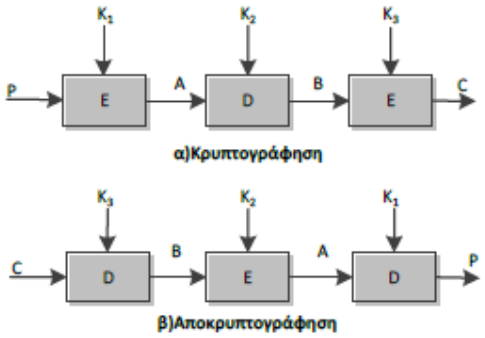
για κάθε επανάληψη, αλλά κάθε φορά παράγεται διαφορετικό υποκλειδί, λόγω της επανειλημμένης μετατόπισης των ψηφίων του κλειδιού. Η διαδικασία της αποκρυπτογράφησης με τον αλγόριθμο DES είναι ουσιαστικά ίδια με τη διαδικασία κρυπτογράφησης, αφού ο κανόνας που ακολουθείται είναι: *Το κρυπτογράφημα χρησιμοποιείται ως είσοδος στον αλγόριθμο DES, αλλά τα κλειδιά Ki τοποθετούνται σε αντίστροφη σειρά*. Ουσιαστικά, το K16 χρησιμοποιείται στην πρώτη επανάληψη, το K15 στη δεύτερη επανάληψη, κ.ο.κ.., έως ότου χρησιμοποιηθεί το K1 στη δέκατη έκτη και τελευταία επανάληψη.

Η ανησυχία που υπήρχε για την ισχύ του αλγορίθμου DES βασιζόταν σε δύο αιτίες: Η πρώτη κατηγορία αιτιών ανησυχίας βασιζόταν στην πιθανότητα να καταστεί εφικτή η κρυπτανάλυση του DES με εκμετάλλευση κάποιων χαρακτηριστικών του αλγορίθμου. Η δεύτερη κατηγορία αιτιών ανησυχίας βασιζόταν στο μήκος του κλειδιού. Ήδη από τα τέλη της δεκαετίας του '70 εμπειρογνώμονες σε θέματα ασφάλειας προειδοποιούσαν ότι η χρονική διάρκεια κατά την οποία ο αλγόριθμος DES με μέγεθος κλειδιού 56 bit θα θεωρείται ασφαλής αλγόριθμος, είναι ολοένα και μικρότερη, λαμβάνοντας υπόψη τις διαφαινόμενες τάσεις αύξησης της ταχύτητας των επεξεργαστών και ταυτόχρονης μείωσης των τιμών του υλικού. Τον Ιούλιο του 1998, το Ίδρυμα Electronic Frontier Foundation - EFF ανακοίνωσε ότι κατάφερε εντός τριών ημερών την κρυπτανάλυση ενός DES κρυπτομηνύματος χρησιμοποιώντας μία μηχανή ειδικού σκοπού αποκαλούμενη DES cracker που κόστισε λιγότερο από 250.000 δολάρια. Το EFF δημοσίευσε λεπτομερή περιγραφή της μηχανής, παρέχοντας τη δυνατότητα και σε όποιον άλλον επιθυμούσε να δημιουργήσει αντίστοιχες ατομικές μηχανές.

3.8.3 Αλγόριθμος Triple DES

Ο TDES ή TDEA ή συνηθέστερα 3DES προτάθηκε αρχικά από τον W. Tuchman και το 1985 προτυποποιήθηκε στο ANSI X9.17, ώστε να χρησιμοποιηθεί σε οικονομικές εφαρμογές. Το 1999, με τη δημοσίευση του ως FIPS PUB 46-3, ο TDES ενσωματώθηκε ως τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES. Ο TDES ακολούθησε τον αλγόριθμο 2DES, ο οποίος δεν αξιοποιήθηκε ευρέως αφού θεωρήθηκε ευάλωτος στις κρυπταναλυτικές επιθέσεις τύπου ενδιάμεσου (man in the middle attack).

Ο TDES χρησιμοποιεί τρία κλειδιά και τρεις εκτελέσεις του αλγορίθμου DES. Ο αλγόριθμος ακολουθεί τη διαδοχή: κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση (EDE – encryption – decryption - encryption). Η αποκρυπτογράφηση ακολουθεί ακριβώς την ίδια διαδικασία με τα κλειδιά σε αντίστροφη. Ο TDES αποτελεί έναν εξαιρετικό αλγόριθμο, ο οποίος επειδή προέρχεται από τον DES παρουσιάζει την ίδια ρωμαλεότητα με αυτόν σε κρυπταναλυτικές επιθέσεις. Επιπλέον, με μήκος κλειδιού 168-bit οι επιθέσεις τύπου εξαντλητικής αναζήτησης είναι πρακτικά ατελέσφορες. Συνεπώς ο TDES αναμένεται ότι θα αξιοποιείται ολοένα και περισσότερο τα επόμενα χρόνια, μέχρι την ολοκληρωτική μετάβαση στις επερχόμενες υλοποιήσεις του AES [5,8,9,15,17,18].



Σχήμα 3.8.3 : TDES

3.8.4 Αλγόριθμος AES (Advanced Encryption Standard)

Τον Ιανουάριο του 1997, το "Εθνικό Ινστιτούτο Προτύπων & Τεχνολογίας" των ΗΠΑ (National Institute of Standards and Technology, NIST) προκήρυξε διεθνή διαγωνισμό για την υιοθέτηση του νέου κρυπτογραφικού προτύπου εμπορικής (μη κυβερνητικής) χρήσεως, του AES. Τελικά ο AES ο αλγόριθμος Rijndael, ο οποίος είχε υποβληθεί από τους Βέλγους κρυπτογράφους J. Daemen και V. Rijmen και έλαβε την οριστική του σχεδιαστική μορφή εγκαθιδρύθηκε στο τέλος του καλοκαιριού του 2001.

Ο αλγόριθμος Rijndael περιλαμβάνει 10, 12 ή 14 κύκλους, ανάλογα με το μήκος του μυστικού κλειδιού. Κάθε κύκλος περιλαμβάνει τέσσερις μετασχηματισμούς, τους: SubByte, ShiftRow, MixColumn, AddRoyndKey. Ο SubByte μετασχηματισμός εφαρμόζεται σε όλα τα bytes του τμήματος. Οι μετασχηματισμοί ShiftRow και MixColumn υποστηρίζουν τη γραμμική ανάμειξη των δεδομένων του τμήματος. Ο μετασχηματισμός AddRoundKey συσχετίζει τα bytes του τμήματος με τα bytes των υποκλείδιων με την πράξη XOR. Επιπλέον, ο μετασχηματισμός AddRoundKey εκτελείται μία ακόμη φορά στη φάση αρχικοποίησης πριν τον πρώτο κύκλο, ενώ στον τελευταίο κύκλο παραλείπεται ο μετασχηματισμός MixColumn [5,8,9,15,17,18].

3.8.5 Αλγόριθμος IDEA (International Data Encryption Algorithm)

Ο αλγόριθμος International Data Encryption Algorithm – IDEA αποτελεί έναν συμμετρικό κωδικοποιητή τμημάτων, που αναπτύχθηκε από τους X. Lai και J. Massey, στο Swiss Federal Institute of Technology, το 1991. Ο IDEA χρησιμοποιεί κλειδί μήκους 128-bit και διαφέρει από τον DES τόσο στη συνάρτηση F, όσο και στη συνάρτηση παραγωγής των υποκλείδιων. Για τη συνάρτηση F, ο IDEA δε χρησιμοποιεί S-boxes, αλλά στηρίζεται σε τρεις διαφορετικές μαθηματικές λειτουργίες: τη δυαδική πράξη XOR, τη δυαδική πρόσθεση ακεραίων των 16-bit και το δυαδικό πολλαπλασιασμό ακεραίων των 16-bit.

Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο σε υλικό όσο και σε λογισμικό. Μερικές όμως αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA ήταν ένας από τους προτεινόμενους 128-bit αντικαταστάτες του DES, έχει υποβληθεί σε αξιοσημείωτη διερεύνηση και εμφανίζεται ανθεκτικός

σε κρυπταναλυτικές επιθέσεις. Ο IDEA χρησιμοποιείται στο προϊόν λογισμικού PGP, ως μία από τις εναλλακτικές επιλογές, καθώς και σε διάφορα εμπορικά προϊόντα [5,8,9,15,17,18].

3.8.6 Αλγόριθμος RC2

Ο κρυπτογραφικός αλγόριθμος RC2 αναπτύχθηκε από τον Ron Rivest της εταιρίας RSA Security το 1987. Είναι ένας κρυπτογραφικός αλγόριθμος τμήματος με μέγεθος block 64 bits που χρησιμοποιεί 18 γύρους σε δίκτυο Feistel. Βασικό χαρακτηριστικό του είναι ότι υποστηρίζει κλειδιά μεταβλητού μεγέθους από 8 έως 128 bits. Αν το μέγεθος του κλειδιού είναι μεγαλύτερο από 56 bits είναι ανεκτικότερος από τον αλγόριθμο DES [5,8,9,15,17,18].

3.8.7 Αλγόριθμος RC4

Ο RC4 είναι ένας αλγόριθμος ροής που σχεδιάστηκε από τον Ron Rivest της εταιρίας RSA Security το 1987 και δημοσιεύτηκε το 1994. Έχει μεταβλητό μήκος κλειδιού από 40 έως 2048 bits και λειτουργεί σε επίπεδο byte. Χρησιμοποιεί 256 γύρους και θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για τη διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL [5,8,9,15,17,18].

3.8.8 Αλγόριθμος RC5

Ο RC5 αναπτύχθηκε το 1994 από τον R. Rivest, έναν από τους σχεδιαστές του αλγορίθμου δημοσίου κλειδιού RSA. Ο RC5 προσδιορίζεται στο RFC 2040 και σχεδιάστηκε για να υποστηρίζει τα ακόλουθα χαρακτηριστικά. Ο RC5 διακρίνεται από καταλληλότητα για υλοποίηση σε υλικό ή λογισμικό και ταχύτητα. Επιπλέον είναι προσαρμόσιμος σε επεξεργαστές διαφορετικών μηκών λέξης ενώ διαθέτει μεταβλητό μήκος γύρων και μεταβλητό μήκος κλειδιού. Τον διακρίνει η απλή του δομή, έχει χαμηλή απαίτηση μνήμης ενώ παράλληλα εξασφαλίζει υψηλή ασφάλεια. Τέλος Ο RC5 ενσωματώνει τις περιστροφές, δηλαδή κυκλικές μετατοπίσεις δυαδικών ψηφίων, των οποίων ο αριθμός είναι στοιχείο εξαρτώμενο από τα δεδομένα. Ο RC5 χρησιμοποιείται σε διάφορα προϊόντα από την RSA Data Security, Inc [5,8,9,15,17,18].

3.8.9 Αλγόριθμος RC6

Ο αλγόριθμος RC6 δημοσιεύτηκε το 1998 και περιλαμβάνει 20 κύκλους μετασχηματισμών. Σε όλους τους κύκλους διεξάγεται μεταβλητή περιστροφή δεδομένων και οι πράξεις που λαμβάνουν χώρα είναι πολλαπλασιασμός, πρόσθεση, XOR και πρόσθεση υποκλείδιων. Έχει μέγεθος τμήματος 128 bits και μέγεθος κλειδιού 128, 192 ή 256 bits [5,8,9,15,17,18].

3.8.10 Αλγόριθμος MARS

Ο αλγόριθμος MARS περιλαμβάνει 32 κύκλους μετασχηματισμών. Από αυτούς, μόνον οι 16 κύκλοι βασίζονται στο μυστικό κλειδί και οι πράξεις που λαμβάνουν χώρα είναι ο πολλαπλασιασμός, η πρόσθεση με κλειδιά των 32-bit και η ολίσθηση ή περιστροφή των δεδομένων. Οι υπόλοιποι 16 κύκλοι αξιοποιούν 8 S-boxes των 32 bit με πράξεις πρόσθεσης και XOR [5,8,9,15,17,18].

3.8.11 Αλγόριθμος Serpent

Ο αλγόριθμος Serpent περιλαμβάνει 32 κύκλους μετασχηματισμών. Στον αλγόριθμο προσδιορίζεται μία αρχική και μία τελική μετάθεση, οι οποίες διευκολύνουν εναλλακτικούς τρόπους λειτουργίας. Σε καθέναν από τους 32 κύκλους περιλαμβάνονται τρία επιμέρους επίπεδα μετασχηματισμών: η πράξη XOR με το υποκλειδί, 32 παράλληλες εφαρμογές ενός από τα 8 S-boxes και ένας γραμμικός μετασχηματισμός [5,8,9,15,17,18].

3.8.12 Αλγόριθμος Twofish

Ο αλγόριθμος Twofish περιλαμβάνει 16 κύκλους, σε καθέναν από τους οποίους εφαρμόζονται 4 S-boxes τα οποία εξαρτώνται από το μυστικό κλειδί. Τα επόμενα στάδια περιλαμβάνουν την αξιοποίηση σταθερών S-boxes, τη διενέργεια μετασχηματισμού pseudo-Hadamard, καθώς και την πρόσθεση του υποκλειδίου [5,8,9,15,17,18].

3.8.13 Αλγόριθμος Blowfish

Ο αλγόριθμος Blowfish αναπτύχθηκε το 1993 από τον επιφανή κρυπτογράφο B. Schneier και καθιερώθηκε ως μία από τις δημοφιλέστερες εναλλακτικές λύσεις του DES. Ο Blowfish σχεδιάστηκε ώστε να είναι εύκολος στην υλοποίηση και να παρουσιάζει μεγάλη ταχύτητα εκτέλεσης. Όπως ο αλγόριθμος DES, ο αλγόριθμος Blowfish χρησιμοποιεί S-boxes, XOR, καθώς και δυαδική πρόσθεση. Αντίθετα από τον DES που χρησιμοποιεί σταθερά S-boxes, ο Blowfish χρησιμοποιεί δυναμικά S-boxes που παράγονται ως συνάρτηση του κλειδιού. Στον Blowfish, τα υποκλείδια και τα S-boxes παράγονται από την επανειλημμένη εφαρμογή του ίδιου του αλγορίθμου Blowfish στο κλειδί. Ο Blowfish δεν είναι κατάλληλος για εφαρμογές στις οποίες το μυστικό κλειδί αλλάζει συχνά.

Ο Blowfish περιλαμβάνεται στους καλύτερους συμβατικούς αλγορίθμους κρυπτογράφησης που έχουν εφαρμοστεί, αφού τα υποκλείδια και τα S-boxes παράγονται από διαδικασία επανειλημμένων εφαρμογών του Blowfish στον εαυτό του. Οι επαναλήψεις αυτές τροποποιούν πλήρως τα δυαδικά ψηφία και καθιστούν την κρυπτανάλυση εξαιρετικά δύσκολη. Οι μέχρι σήμερα δημοσιεύσεις των προσπαθειών για κρυπτανάλυση του Blowfish δεν αναφέρουν πρακτικές αδυναμίες. Ο Blowfish χρησιμοποιείται, επίσης, σε διάφορες εμπορικές εφαρμογές [5,8,9,15,17,18].

3.8.14 Αλγόριθμος CAST-128

Το CAST αποτελεί μία διαδικασία σχεδίασης συμμετρικών αλγορίθμων κρυπτογράφησης, η οποία αναπτύχθηκε το 1997 από τους C. Adams και S. Tavares της εταιρίας Entrust Technologies. Ένας συγκεκριμένος αλγόριθμος που αναπτύχθηκε ως τμήμα του προγράμματος CAST είναι ο CAST-128 που ορίστηκε στο RFC 2144. Στον αλγόριθμο αυτό χρησιμοποιείται μέγεθος κλειδιού που λαμβάνει τιμές μεταξύ 40-bit και 128-bit, με βήματα των 8-bit. Το CAST είναι το αποτέλεσμα μιας μακράς χρονικά διαδικασίας έρευνας και ανάπτυξης και έχει ενσωματώσει σειρά σχολίων από κρυπταναλυτές. Σε πρώτη φάση είχε χρησιμοποιηθεί σε διάφορα προϊόντα, συμπεριλαμβανομένου και του PGP.

Το CAST χρησιμοποιεί σταθερά S-boxes, αλλά μόνον αυτά που είναι σημαντικά μεγαλύτερα των S-boxes που χρησιμοποιούνται στο DES. Τα S-boxes σχεδιάστηκαν προσεκτικά, ώστε να μην παρουσιάζουν γραμμικότητα στη σχέση εισόδου και εξόδου, συνεπώς να είναι ανθεκτικά σε κρυπταναλυτικές επιθέσεις. Η διαδικασία παραγωγής υποκλείδιων που χρησιμοποιείται στον CAST-128 είναι διαφορετική από αυτήν που υιοθετείται σε άλλους συμβατικούς αλγορίθμους κρυπτογράφησης τμημάτων. Οι σχεδιαστές του CAST προσπάθησαν να δημιουργήσουν υποκλείδια με μεγαλύτερο βαθμό ανθεκτικότητας σε γνωστές κρυπταναλυτικές επιθέσεις. Θεωρήθηκε ότι η χρήση μη-γραμμικών S-boxes για παραγωγή κλειδιών από το βασικό κλειδί, παρείχε αυτή την ισχύ. Αξιοσημείωτο χαρακτηριστικό γνώρισμα του CAST-128 αποτελεί η συνάρτηση κύκλου F, η οποία διαφέρει από γύρο σε γύρο, καθιστώντας τον αλγόριθμο κρυπταναλυτικά ανθεκτικότερο [5,8,9,15,17,18].

3.9 Ασύμμετροι Αλγόριθμοι Υλοποίησης Κρυπτογράφησης

Υπάρχουν αρκετοί αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού, καθένας από τους οποίους είναι κατάλληλος για την υλοποίηση μιας ή περισσοτέρων από τις υπηρεσίες που προσφέρει η κρυπτογραφία δημοσίου κλειδιού. Στη συνέχεια περιγράφονται αναλυτικά ορισμένοι από τους πιο γνωστούς αλγορίθμους κρυπτογράφησης δημοσίου κλειδιού.

Στην ενότητα αυτή παρουσιάζουμε μερικούς από τους σημαντικότερους αλγόριθμους δημοσίου κλειδιού κάνοντας αναφορά στη γενική φιλοσοφία τους και στα στάδια που ακολουθούνται κατά τη λειτουργία τους.

3.9.1 Αλγόριθμος RSA

Ένα από τα πρώτα ασύμμετρα κρυπτοσυστήματα που αναπτύχθηκε το 1977 ήταν από τους R. Rivest, A. Shamir και L. Adleman στο MIT και δημοσιεύτηκε για πρώτη φορά το 1978. Από εκείνη τη στιγμή το RSA κυριάρχησε ως η πλέον αποδεκτή και εύκολα υλοποιήσιμη προσέγγιση για ασύμμετρα κρυπτοσυστήματα. Ο RSA είναι αλγόριθμος κρυπτογράφησης στον οποίο το αρχικό και

το κρυπτογραφημένο κείμενο είναι ακέραιοι αριθμοί με τιμές μεταξύ 0 και n-1, για κάποιο n. Ουσιαστικά ο RSA είναι ένας αλγόριθμος για ασύμμετρο κρυπτοσύστημα με δημόσιο και ιδιωτικό κλειδί. Αυτός ο αλγόριθμος είναι κατάλληλος για κρυπτογράφηση/αποκρυπτογράφηση δεδομένων, για την δημιουργία ψηφιακών υπογραφών και την επαλήθευσή τους καθώς και για την ασφαλή μεταφορά κλειδιών. Χρησιμοποιείται ως βάση για τη δημιουργία μιας ασφαλούς γεννήτριας ψευδοτυχαίων αριθμών καθώς και για την ασφάλεια σε ορισμένα ηλεκτρονικά παιχνίδια. Ο RSA βασίζεται στις αρχές της θεωρίας αριθμών

Η ασφάλεια της μεθόδου οφείλεται στην δυσκολία της παραγοντοποίησης μεγάλων αριθμών. Το σημερινό επίπεδο της έρευνας πάνω στην παραγοντοποίηση των αριθμών απαιτεί τα κλειδιά που παράγονται με τον αλγόριθμο RSA να έχουν μήκος τουλάχιστον 1024 bits έτσι ώστε να παρέχεται ικανοποιητική ασφάλεια στις επικοινωνίες μέσα στα επόμενα χρόνια. Ο RSA παρέχει μερικά πλεονεκτήματα τα οποία βοήθησαν στην υλοποίηση πιο ασφαλών και ευκολότερα διαχειρίσιμων συναλλαγών. Τα πλεονεκτήματα αυτά είναι τα ακόλουθα . Αρχικά παρέχει απλοποίηση του προβλήματος της διαχείρισης κλειδιών αλλά και ενισχυμένη ασφάλεια των συναλλαγών

Ο αλγόριθμος RSA είναι κάτι παραπάνω από δεδομένο στην κρυπτογραφία δημοσίου κλειδιού σε σημείο μάλιστα που οι δύο έννοιες να θεωρούνται ταυτόσημες. Η ισχύς του RSA είναι τόσο μεγάλη που η κυβέρνηση των ΗΠΑ έχει περιορίσει σημαντικά την εξαγωγή του αλγορίθμου σε ξένες χώρες. Αν και ο αλγόριθμος RSA είναι ο επικρατέστερος στο χώρο της κρυπτογραφίας δημοσίου κλειδιού έχει κάποιες αδυναμίες. Μερικά από τα πιο σημαντικά προβλήματα που θα μπορούσε να αντιμετωπίσει ο αλγόριθμος αυτός είναι οι αναγραφόμενες. Δυνατότητα παραγοντοποίησης του δημοσίου κλειδιού, Επίθεση επανάληψης (cycle attack) και τέλος επίθεση στο υπόλοιπο RSA[5,8,9,15,17,18]. Παρ' όλες τις οποιεσδήποτε αδυναμίες του, ο RSA συνεχίζει να θεωρείται ως το de facto δεδομένο για την κρυπτογράφηση δημοσίου κλειδιού, ιδιαίτερα όταν πρόκειται για δεδομένα που μεταφέρονται στο Internet.

3.9.2 Αλγόριθμος Digital Signature Algorithm (DSA)

Ο αλγόριθμος DSA (Digital Signature Algorithm) προτάθηκε τον Αύγουστο του 1991 από το NIST (National Institute of Standards and Technology) της Αμερικής. Έχει προτυποποιηθεί ως FIPS 186 (Federal Information Processing Standard). Το πρότυπο αυτό έχει ονομαστεί DSS (Digital Signature Standard και είναι ο πρώτος αλγόριθμος ψηφιακής υπογραφής που αναγνωρίστηκε παγκόσμια. Ο DSA αποτελεί μια παραλλαγή του αλγορίθμου ElGamal για ψηφιακές υπογραφές και σχεδιάστηκε αποκλειστικά για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών και κατά συνέπεια και για τον έλεγχο της ακεραιότητας των δεδομένων. Η ασφάλεια του DSA βασίζεται στη δυσκολία του υπολογισμού διακριτών λογαρίθμων μέσα σε ένα πεπερασμένο σώμα. Έρευνες πάνω στον αλγόριθμο έχουν δείξει την ύπαρξη πρώτων αριθμών οι οποίοι θα μπορούσαν να οδηγήσουν στη δημιουργία κλειδιών ευάλωτων σε επιθέσεις.

Όμως, αυτοί οι αριθμοί είναι ελάχιστοι και μπορούν εύκολα να αποφευχθούν σε μία σωστή διαδικασία δημιουργίας ζεύγους κλειδιών. Από το 1996 προτείνεται το μέγεθος του p να είναι τουλάχιστον 768 bits. Το πρότυπο FIPS 186 δεν επιτρέπει πρώτους αριθμούς p που το μέγεθός τους ξεπερνά τα 1024 bits. Ένα σημαντικό πλεονέκτημα του DSA είναι ότι, η εκθετοποίηση ως διαδικασία μπορεί να προηγείται της δημιουργίας της ψηφιακής υπογραφής, κάτι που δεν είναι εφικτό με τον RSA[5,8,9,15,17,18].

3.9.3 Ανταλλαγή κλειδιών κατά Diffie-Hellman

Ο πρώτος αλγόριθμος δημοσίου κλειδιού προτάθηκε το 1976 από τους Diffie και Hellman. Ο αλγόριθμος αυτός, γνωστός ως DH, είναι αποκλειστικά ένα πρωτόκολλο συμφωνίας κλειδιού. Κάθε μία από τις δύο οντότητες που θέλουν αν επικοινωνήσουν χρησιμοποιεί το δικό της ιδιωτικό κλειδί και το δημόσιο κλειδί της άλλης με σκοπό τη δημιουργία ενός συμμετρικού κλειδιού που καμία άλλη οντότητα δεν μπορεί να υπολογίσει.

Οι πρώτες εκδόσεις του μηχανισμού Diffie-Hellman ήταν ευάλωτες σε επιθέσεις *man-in-the-middle*. Το 1992 αναπτύχθηκε μία ανανεωμένη έκδοση από τους Diffie, Van Oorschot και Wiener που υποστήριζε την πιστοποίηση της ταυτότητας των δύο πλευρών και είχε σαν σκοπό να καταπολεμήσει την επίθεση man-in-the-middle. Τα μηνύματα ανταλλάσσονται υπογεγραμμένα με τα ιδιωτικά κλειδιά του αποστολέα και του παραλήπτη ενώ χρησιμοποιούνται και πιστοποιητικά για την απόκτηση των σωστών δημοσίων κλείδων. Έτσι, ακόμα και αν ένας τρίτος είναι σε θέση να παρακολουθεί την επικοινωνία του αποστολέα και του παραλήπτη, δεν μπορεί να πλαστογραφήσει τα μηνύματα.

3.9.4 Αλγόριθμοι Ελλειπτικών Καμπυλών

Το 1985, οι Neal Koblitz και V. S. Miller πρότειναν ανεξάρτητα ο ένας από τον άλλον την λεγόμενη *κρυπτογραφία ελλειπτικών καμπυλών* (*Elliptic Curve Cryptography*). Η Κρυπτογραφία Ελλειπτικών Καμπυλών βασίζεται στο *πρόβλημα του διακριτού λογαρίθμου.* Συγκεκριμένα δεν υπάρχει γνωστός αλγόριθμος που να επιλύει το πρόβλημα αυτό σε μια κατάλληλα επιλεγμένη ελλειπτική καμπύλη (ECDLP).

Η Κρυπτογραφία Ελλειπτικών Καμπυλών βρίσκει εφαρμογή με τη χρήση των αλγορίθμων DSA και DH ελλειπτικών καμπυλών (ECDSA και ECDH). Οι αλγόριθμοι ECDSA και ECDH υλοποιούνται κάνοντας χρήση ενός συνόλου σημείων, που προκύπτουν ως λύση της εξίσωσης μιας ελλειπτικής καμπύλης πάνω σε ένα πεπερασμένο σώμα (finite field). Η ασφάλειά τους βασίζεται στη δυσκολία του υπολογισμού λογαρίθμων πάνω σε ένα σύνολο σημείων ελλειπτικής καμπύλης. Ο αλγόριθμος ECDSA είναι ένας κατά FIPS (Federal Information Processing Standard) εγκεκριμένος αλγόριθμος για δημιουργία και επαλήθευση ψηφιακών υπογραφών. Ο ECDSA περιγράφεται στο ANSI X9.62. Ας σημειωθεί επίσης ότι είναι δυνατόν να υλοποιηθεί και ο RSA ως αλγόριθμος ελλειπτικής καμπύλης

3.9.5Συναρτήσεις Κατακερματισμού (Hash Functions)

Ο όρος *συνάρτηση κατακερματισμού* (hash function) υποδηλώνει ένα μετασχηματισμό H ο οποίος παίρνει ως είσοδο ένα μήνυμα m ανεξαρτήτου μήκους και δίνει ως έξοδο μία ακολουθία χαρακτήρων h, είναι δηλαδή $h = H(m)$. Η έξοδος h μιας συνάρτησης κατακερματισμού ονομάζεται *τιμή κατακερματισμού (hash value)* ή *σύνοψη μηνύματος (message digest)* και έχει συγκεκριμένο μήκος ανάλογα με το είδος του αλγόριθμου κατακερματισμού που χρησιμοποιείται, συνήθως πολύ μικρότερο από αυτό του αρχικού μηνύματος (σχήμα 2.3). Μπορούμε να φανταστούμε την σύνοψη μηνύματος ως το "ψηφιακό αποτύπωμα" ("digital fingerprint") του εγγράφου.[21]

Σχήμα 3.9.5 : Συνάρτηση κατακερματισμού

Οι σημαντικότερες ιδιότητες των συναρτήσεων κατακερματισμού με μορφή $y = H(x)$ είναι:

- Η είσοδος *x* μπορεί να έχει οποιοδήποτε μήκος
- Η έξοδος *y* έχει περιορισμένο μήκος
- Δεδομένου του x και της συνάρτησης Η είναι εύκολος ο υπολογισμός του $H(x)$
- Η $H(x)$ είναι μονόδρομη (one way function)
- Η $H(x)$ είναι αμφιμονοσήμαντη (συνάρτηση ένα προς ένα)

Μια μονόδρομη συνάρτηση κατακερματισμού είναι μία συνάρτηση κατακερματισμού για την οποία είναι υπολογιστικά ανέφικτο να υπολογιστεί η αντίστροφή της, δηλαδή το αρχικό μήνυμα δεν μπορεί να ανακτηθεί από τη σύνοψή του. Όταν επιπλέον η συνάρτηση είναι αμφιμονοσήμαντη, τότε είναι πολύ δύσκολο να βρεθούν δύο διαφορετικά μηνύματα με την ίδια σύνοψη. Στην περίπτωση που κάτι τέτοιο συμβεί τότε υπάρχει *σύγκρουση* (collision) .

Οι πιο γνωστοί αλγόριθμοι κατακερματισμού είναι οι MD5 με σύνοψη 128 bit, ο SHA-1 με σύνοψη 160 bits και ο RIPEMD-160 με σύνοψη 160 bits. Οι νέες εκδόσεις του αλγορίθμου SHA, SHA-256, SHA-384 και SHA-512 δίνουν σύνοψη μηνύματος 256, 384 και 512 bits αντίστοιχα.

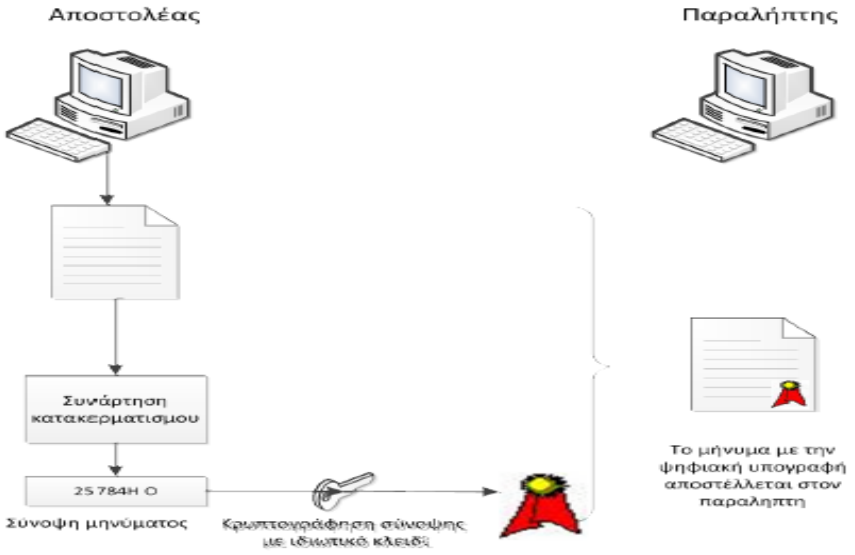
3.9.6 Αλγόριθμος Κατακερματισμού Secure Hash Algorithm-1 (SHA-1)

Ο ασφαλής αλγόριθμος κατακερματισμού *SHA-1* (*Secure Hash Algorithm-1*) **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** αποτελεί μια βελτιωμένη έκδοση του αρχικού αλγορίθμου κατακερματισμού SHA. Αυτός ο αλγόριθμος κατακερματισμού (hash algorithm) σχεδιάστηκε αποκλειστικά για χρήση σε συνδυασμό με τον DSA και συνεπώς δεν μπορεί να χρησιμοποιηθεί με τον RSA ή οποιοδήποτε άλλο αλγόριθμο δημοσίου κλειδιού για ψηφιακή υπογραφή. Οι σχεδιαστικές αρχές του SHA-1 είναι παρεμφερείς με αυτές των συναρτήσεων κατακερματισμού MD2 **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** και κυρίως της συνάρτησης MD5. Ο αλγόριθμος μπορεί να έχει ως είσοδο μηνύματα μήκους μικρότερου από 2^{64} bits. Η έξοδος του αλγορίθμου ονομάζεται σύνοψη μηνύματος (message digest ή hash value ή message fingerprint) και έχει μήκος 160 bit. Είναι πιο αργός από τον MD5 αλλά το μεγαλύτερο message digest που παράγει (ο MD5 παράγει message digest μήκους 128 bits) τον καθιστούν πιο ισχυρό σε προσπάθειες αντιστροφής του.

3.9.7 Ψηφιακή υπογραφή (digital signature)

Η κρυπτογραφία δημοσίου κλειδιού έκανε δυνατή την υλοποίηση μιας εφαρμογής η οποία ήταν δύσκολα επιτεύξιμη με τη χρήση της συμβατικής συμμετρικής κρυπτογραφίας. Πρόκειται για την υπηρεσία της ψηφιακής υπογραφής που είναι για τον ηλεκτρονικό κόσμο ό,τι η χειρόγραφη υπογραφή για τον πραγματικό.

Μια απλή εφαρμογή της κρυπτογραφίας δημοσίου κλειδιού εξασφαλίζει το απόρρητο των δεδομένων όταν αυτά μεταφέρονται μέσα σε ένα δίκτυο επικοινωνιών. Η χρήση της ψηφιακής υπογραφής έρχεται να καλύψει το κενό των υπόλοιπων τριών τομέων ασφάλειας, δηλαδή της πιστοποίησης αυθεντικότητας, του ελέγχου ακεραιότητας και της μη αποκήρυξης.



Σχήμα3.9.7: Διαδικασία Ψηφιακής Υπογραφής

Ανταλλαγή κλειδιών (key exchange)

Η κρυπτογραφία δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί και για την ανταλλαγή κλειδιών μεταξύ δύο οντοτήτων. Αυτό σημαίνει ότι ένα πρωτόκολλο μπορεί να χρησιμοποιεί δημόσια κα ιδιωτικά κλειδιά έτσι ώστε, κατά τη λήξη του πρωτοκόλλου, οι δύο οντότητες να μοιράζονται ένα συμμετρικό κλειδί άγνωστο σε κάθε άλλη οντότητα. Η ανταλλαγή κλειδιών μπορεί να πραγματοποιηθεί με δύο τρόπους:

- Κατά τη *μεταφορά κλειδιού (key transfer)* η μία οντότητα παράγει το συμμετρικό κλειδί και το στέλνει στην δεύτερη οντότητα. Η κρυπτογραφία δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί για να προστατέψει το απόρρητο της συγκεκριμένης μεταφοράς.
- Κατά τη *συμφωνία κλειδιού (key agreement)* και οι δύο οντότητες συμβάλουν στη δημιουργία του συμμετρικού κλειδιού. Η κρυπτογραφία δημοσίου κλειδιού κάνει αυτή τη διαδικασία πολύ απλή σε σύγκριση με τη χρήση της συμμετρικής κρυπτογραφίας.

4. Συναφείς Εργασίες

4.1 Κρυπτογραφία σε ενσωματωμένα συστήματα

Η υλοποίηση της κρυπτογραφίας σε ενσωματωμένα συστήματα είναι ένας τομέας με αρκετές προκλήσεις. Οι απαιτήσεις για υψηλή απόδοση πρέπει να ικανοποιηθούν σε ένα περιβάλλον με περιορισμένους πόρους. Η έρευνα αυτή έχει ακόμη περισσότερες προκλήσεις όταν υπάρχουν επιπλέον περιορισμοί για χαμηλή κατανάλωση ενέργειας. Η υψηλή απόδοση οδηγεί συνήθως σε αυξημένο κόστος, το οποίο δεν είναι πάντοτε επιθυμητό ή εφικτό. Η κρυπτογραφία μπορεί να προστατεύσει ψηφιακά αγαθά με την προϋπόθεση ότι τα μυστικά κλειδιά των αλγορίθμων αποθηκεύονται και προσπελαύνονται με ένα ασφαλή τρόπο. Για το λόγο αυτό προτιμάται η χρήση εξειδικευμένων συσκευών υλικού για την αποθήκευση των μυστικών κλειδιών και την υλοποίηση των κρυπτογραφικών αλγορίθμων, έναντι της χρήσης υπολογιστών γενικού σκοπού. Ωστόσο, κάτι τέτοιο αυξάνει το κόστος υλοποίησης και οδηγεί σε μειωμένη ευελιξία του συστήματος.

Από την άλλη, η ευελιξία απαιτείται, καθώς τα σύγχρονα πρωτόκολλα κρυπτογραφίας δε στηρίζονται σε έναν αποκλειστικά αλγόριθμο, αλλά ορίζονται ώστε να μπορεί να χρησιμοποιηθεί ένα πλήθος κρυπτογραφικών αλγορίθμων, προκειμένου να επιτευχθεί υψηλότερη ασφάλεια και προσαρμοστικότητα στις εξελίξεις του τομέα της κρυπτανάλυσης. Για παράδειγμα, τα ασφαλή δικτυακά πρωτόκολλα SSL και IPSec υποστηρίζουν ένα μεγάλο αριθμό κρυπτογραφικών αλγορίθμων για την επίτευξη της ίδιας λειτουργίας, όπως για παράδειγμα της κρυπτογράφησης δεδομένων. Το πρωτόκολλο που θα χρησιμοποιείται οφείλει να επιτρέπει τη διαπραγμάτευση μεταξύ των συμμετεχόντων για τους αλγόριθμους που θα χρησιμοποιηθούν σε μία συγκεκριμένη συνεδρία επικοινωνίας, ώστε να εγγυηθεί ότι όλοι οι συμμετέχοντες έχουν το επίπεδο ασφάλειας που επιθυμούν και το οποίο ορίζεται από τις πολιτικές ασφάλειάς τους.

Οι μη εξουσιοδοτημένοι επιτιθέμενοι είναι σε θέση να αναλάβουν τον έλεγχο της ροής δεδομένων και την παρακολούθηση ή να ακούσουν την επικοινωνία μεταξύ των δύο μερών. Από αυτό συνεπάγεται ότι η ένταξη της μεθοδικών μέτρων ασφάλειας είναι υποχρεωτική. Υστέρα από έρευνα που πραγματοποιήσαμε διαπιστώσαμε ότι τόσο η κρυπτογραφία όσο και τα ενσωματωμένα σύστημα είναι καίριοι τομείς της πληροφορικής μέσω των οποίων μας παρέχεται ασφάλεια και ευελιξία. Παρακάτω παραθέτουμε μερικές αξιοσημείωτες εφαρμογές που σχετίζονται με την εργασία μας .

4.1.1 Εφαρμογές με τον TEA και λοιπούς lightweight αλγόριθμους

Είναι ευρέως αποδεκτό ότι η ασφάλεια των δεδομένων θα διαδραματίσει κεντρικό ρόλο στο σχεδιασμό των μελλοντικών συστημάτων πληροφορικής. Πολλές από αυτές τις εφαρμογές

πληροφορικής θα υλοποιηθούν όπως τα ενσωματωμένα συστήματα που βασίζονται σε μεγάλο βαθμό στους μηχανισμούς ασφαλείας. Τα παραδείγματα περιλαμβάνουν ασφάλεια σε ασύρματα τηλέφωνα, ασύρματους υπολογιστών, pay-TV, και αντίγραφο προστασίας για audio/video. Να σημειωθεί ότι μεγάλο ποσοστό αυτών των ενσωματωμένων εφαρμογών θα είναι ασύρματο, γεγονός που καθιστά το κανάλι επικοινωνίας είναι ιδιαίτερα ευάλωτο. [20]

4.1.1.1 Εφαρμογή του αλγορίθμου TEA σε Sensors

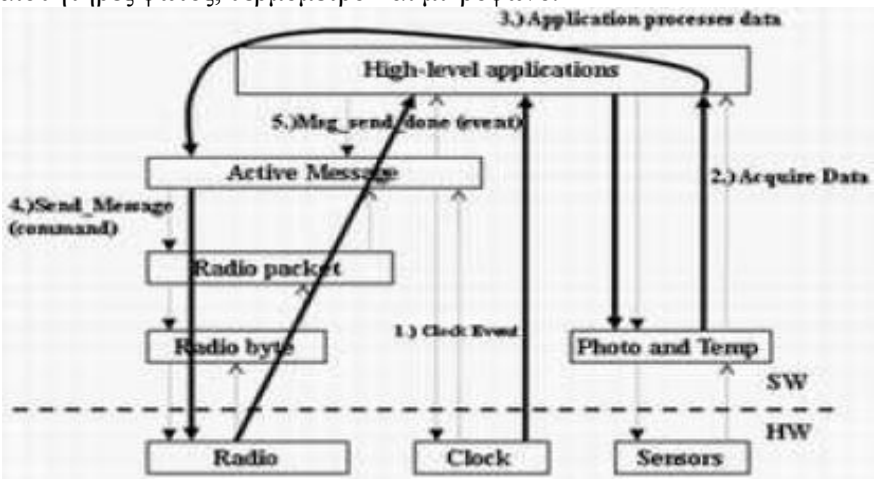
Οι αισθητήρες είναι μικροσκοπικοί υπολογιστές με περιορισμένη υπολογιστική ικανότητα και φυσικούς πόρους. Η εφαρμογή των πρωτοκόλλων ασφάλειας για το δίκτυο αισθητήρων αποτελεί μια μεγάλη πρόκληση. Προκειμένου να παρέχεται υψηλό επίπεδο ασφαλείας για τα δίκτυα αισθητήρων, είναι πολύ σημαντικό να επιλεχθεί ένας μικρός, αποδοτικός και αποτελεσματικός αλγόριθμος κρυπτογράφησης ως εγγύηση. Ο TEA (Tiny Encryption Algorithm) είναι ένας αποτελεσματικός αλγόριθμος που απαιτεί ελάχιστη μνήμη και πόρους. Αυτά τα χαρακτηριστικά καθιστούν τον TEA ως ένα καλό υποψήφιο για το μηχανισμό ασφαλείας για την περίπτωση των αισθητήρων. Στην παρούσα έρευνα που παραθέτουμε περιγράφεται μια εφαρμογή του αλγορίθμου TEA στην πλατφόρμα των δικτύων αισθητήρων (Berkeley Motes) η οποία πραγματοποιήθηκε στο πανεπιστήμιο «Department of Computer Science The University of Alabama» από τους Shuang Liu, Olga V. Gavrylyako και Phillip G. Bradford.

Στο πείραμά λοιπόν που έγινε, τα πακέτα δεδομένων που λαμβάνονται από τη φωτογραφία και τους αισθητήρες θερμοκρασίας, κρυπτογραφούνται στον κόμβο του αισθητήρα χρησιμοποιώντας τον αλγόριθμο TEA. Μετά από αυτό, θα αποστέλλονται στο σταθμό βάσης μέσω ασυρμάτου. Ο σταθμός βάσης θα λάβει τα πακέτα δεδομένων με σκοπό να τα διαβιβάσει στο συνδεδεμένο PC, όπου εκεί τα πακέτα δεδομένων θα αποκρυπτογραφηθούν ώστε να εμφανιστούν με ασφάλεια. Προτείνεται επίσης μια συγκεκριμένη προσέγγιση ώστε να αξιολογείται αποτελεσματικά η απόδοση του TEA όσον αφορά το χρόνο εκτέλεσης στους κόμβους αισθητήρων. Οι πρόσφατες εξελίξεις στην τεχνολογία ασύρματης δικτύωσης και Μίκρο-ηλεκτρο-μηχανικών συστημάτων οδηγούν στην εμφάνιση ενός νέου προϊόντος στην εποχή μετά-PC-δικτυακών αισθητήρων. Δίκτυα αισθητήρων με ad-hoc ρυθμίσεις και προγραμματιζόμενους αισθητήρες θα πρέπει να χρησιμοποιούνται ευρέως σε μια ποικιλία σεναρίων. Ακόμη και οι φουτουριστές, οραματίζονται ότι χιλιάδες εξαιρετικά μικροσκοπικοί αισθητήρες θα πρέπει να ενσωματωθούν στο περιβάλλον χρησιμοποιώντας την περιβαλλοντική ενέργεια, βοηθώντας έτσι τους ανθρώπους να αποκτήσουν περισσότερες φυσικές πληροφορίες [2].

Ωστόσο, δεν αποτελεί έκπληξη το ότι σε πολλές εφαρμογές κατά τη διαβίβαση ευαίσθητων δεδομένων μέσω του δικτύου αισθητήρων απαιτείται η ασφάλεια ώστε να αποφευχθεί η ευάλωτη μετάδοσης. Ένας τρίτος μπορεί να λαμβάνει και να παρέμβει τα ακατέργαστα πακέτα μηνυμάτων σε περίπτωση δεν υπάρχει ασφαλής μηχανισμός για την προστασία της μετάβασης. Σε γενικές γραμμές, όλες οι στρατηγικές ασφάλειας βασίζονται στο να υπογραμμίζουν τα κρυπτογραφικά αρχέτυπα.

Στην περίπτωση του υλικού για το συγκεκριμένο πείραμα χρησιμοποίησαν αισθητήρες με βάση τον ATMEGA128L Μίκρο-ελεγκτή [1]. Είναι ελαφρώς μεγαλύτεροι και πιο ισχυροί από αισθητήρες σε πραγματικές εφαρμογές, αλλά έχουν τα κοινώς σημαντικά χαρακτηριστικά που

αντιπροσωπεύουν πραγματικό δίκτυο αισθητήρων. Ο αισθητήρας έχει τα ακόλουθα στοιχεία: ο επεξεργαστής είναι ο ATMEL 90LS8535 (4 MHz)και είναι μια αρχιτεκτονική Harvard των 4MHz με 8-bit διευθύνσεις. Έχει ως πρόγραμμα 128-Kbyte °ash memory, και 4KB για SRAM. Ενώ λειτουργεί στα 4 MHz και 3,0V, και περιέχει τα εσωτερικά χρονόμετρα / μετρητές. Ο 90LS8535 περιέχει έναν ελεγκτή UART που συνδέεται με σειριακή θύρα ενός σταθμού βάσης του κεντρικού υπολογιστή. Έχει τρεις λειτουργίες του ύπνου: ρελαντί, απενεργοποίησης, και εξοικονόμησης ενέργειας, η οποία μπορεί να μειώσει την κατανάλωση ενέργειας κατά το χρόνο αδράνειας του επεξεργαστή. Διαθέτει επίσης τρία LED's τα οποία μπορεί να εξάγουν αναλογικά σήματα μέσω της I / O θύρας ενώ παράλληλα μπορούν να χρησιμοποιηθούν ως μια προσέγγιση του εντοπισμού σφαλμάτων. Αποτελείται επίσης από ένα radio component το οποίο περιέχει τον πομποδέκτη RF Monolithics των 916.5 MHz και μια κεραία. Η απόσταση μεταφοράς είναι 500 ft . Τέλος υπάρχει ένας συνεπεξεργαστής και μια πλακέτα αισθητήρων η οποία παρέχει αισθητήρες θερμοκρασίας, αισθητήρες φωτός, θερμόμετρο και μικρόφωνο.



Εικόνα 4.1.1.1: Message Processing Sequence in TinyOS.

Η υποδομή του δικτύου αισθητήρων στο συγκεκριμένο πείραμά είναι απλή. Υπάρχει μόνο ένας κόμβος αισθητήρα και ένας σταθμός βάσης σχηματίζοντας ένα απλό δίκτυο αισθητήρων. Ο σταθμός βάσης συνδέεται με έναν κεντρικό υπολογιστή μέσω της σειριακής θύρας. Πρέπει να διασφαλισθεί ότι ο αισθητήρας είναι πάντα στην εμβέλεια του σταθμού βάσης, έτσι ώστε ο ρυθμός απώλειας των πακέτων θα πρέπει να μεωθεί στο μέγιστο βαθμό. Για την απλότητα της εφαρμογής, το αρχικό κλειδί του TEA είναι ένας σταθερός 128-bit αριθμός, ο οποίος δίδεται αρχικά, και ποτέ δεν άλλαξε κατά τη διάρκεια του πειράματος.

Εφάρμοσαν τον αλγόριθμο TEA στον κόμβο αισθητήρα, και κρυπτογράφησαν τα δεδομένα που συνέλλεξαν από τη φωτογραφία και αισθητήρες θερμοκρασίας. Στη συνέχεια, τα κρυπτογραφημένα δεδομένα ενθυλακώνονται σε πακέτα και αποστέλλονται προς το σταθμό βάσης. Μόλις λάβει ένα πακέτο, ο σταθμός βάσης απευθείας προωθεί το πακέτο στο συνδεδεμένο PC, όπου ο αλγόριθμος αποκρυπτογράφησης τρέχει να αποκωδικοποιήσει τα πακέτα και να τα εμφανίσετε στην οθόνη.

4.2 Εφαρμογές επεξεργασίας εικόνας/ανίχνευση ακμών σε ενσωματωμένα συστήματα

Τα τελευταία χρόνια έχουμε δει μια άνευ προηγουμένου προσπάθεια από τους ερευνητές στον τομέα της επεξεργασίας εικόνας σε hardware. Προηγούμενη έρευνα μας δείχνει ότι μπορούν να ταξινομηθούν με βάση τον τύπο του υλικού και ο αλγόριθμος επεξεργασίας εικόνας αφαρμοστεί. Το είδος του υλικού θεωρείται για επεξεργασία εικόνας επιτάχυνσης περιλαμβάνουν την εφαρμογή ειδικών ολοκληρωμένων μάρκες (ASIC), Ψηφιακούς επεξεργαστές σήματος (DSP) και Επαναπροσδιοριζόμενης Λογικής Συσκευές (FPGA). Οι αλγόριθμοι επεξεργασίας εικόνας λαμβάνονται υπόψη για την εφαρμογή του υλικού περιλαμβάνουν: συνέλιξη, η εικόνα φιλτράρισμα και άκρη ανίχνευσης (του Sobel, του Prewitt και Canny της ανίχνευσης ακμών). Μερικοί ερευνητές έχουν πραγματοποιήσει υλοποιήσεις υλικού ειδικά για τους πωλητές FPGA όπως Xilinx, Amtel και την Altera.

Η επεξεργασία, μετάδοση και κατανόηση των εικόνων αποτελούν πεδία συνεχώς αναπτυσσόμενης έρευνας. Το μέγεθος μιας εικόνας απαιτεί τεράστια ταχύτητα υλοποίησης των αλγορίθμων για λειτουργία σε πραγματικό χρόνο. Η τεχνολογία ολοκληρωμένων κυκλωμάτων πολύ μεγάλης κλίμακας (VLSI), σε συνδυασμό με την ανάπτυξη αρχιτεκτονικών συνεχούς ροής (pipelining) με μεγάλο βαθμό παραλληλισμού, βοήθησε στη δυνατότητα υλοποίησης πολλών πολύπλοκων αλγόριθμων. Η ταυτόχρονη ελάττωση του κόστους των μνημών, επεξεργαστών, και γενικά της υπολογιστικής ισχύος, έχει κάνει οικονομικά βιώσιμη την ανάπτυξη συστημάτων επικοινωνίας και, επεξεργασίας εικόνων ακόμα και για οικιακή χρήση.

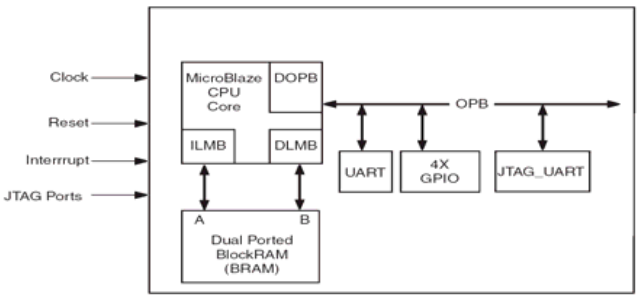
4.2.1 Επεξεργασία Εικόνας σε Ενσωματωμένο Σύστημα FPGA

Μετά από έρευνα που πραγματοποιήσαμε καταλήξαμε σε ορισμένες παρόμοιες εφαρμογές που έχουν υλοποιηθεί στο παρελθόν. Η παρούσα εφαρμογή παρουσιάζει το σχεδιασμό ενός ενσωματωμένου συστήματος επεξεργασίας εικόνας (που ονομάζεται DIPS) στο FPGA. Ο DIPS βασίζεται στο MicroBlaze Xilinx ™ 32-bit (soft-core) πυρήνα επεξεργαστή και εφαρμόζεται στο Spartan-3. Μερικοί αλγόριθμοι εφαρμόζονται στο DIPS, όπως το φίλτρο εικόνας (μέγεθος μάσκας είναι 3x3), η ανίχνευση ακμών, και ο αντίστροφο μετασχηματισμό κυματιδίων. Τα αποτελέσματα από την επεξεργασία θα εμφανιστούν στην εικόνα "Lena".

Στην παρούσα έρευνα, το MicroBlaze™ χρησιμοποιείται ως η καρδιά του συστήματος επεξεργασίας εικόνας (που ονομάζεται DIPS). Βασίζεται ουσιαστικά στο IBM CoreConnect™, είναι ανεπτυγμένη σε IBM on-chip σε bus-συνδέσμους επικοινωνίας τα οποία επιτρέπουν στους chip πυρήνες, από πολλαπλές πηγές, να διασυνδέονται για να δημιουργήσουν ολόκληρο νέο τσιπ. Το DIPS περιλαμβάνει ορισμένα διαθέσιμους περιφερικούς πυρήνες IP, όπως UART, και τον ελεγκτής μνήμης.

Ο DIPS μπορεί να φιλτράρει μια εικόνα, χρησιμοποιώντας 3x3 μάσκες. Δύο είναι τα βασικά φίλτρα, το φίλτρο εξομάλυνσης (low-pass φίλτρο) και η όξυνση φίλτρου (περιλαμβάνουν

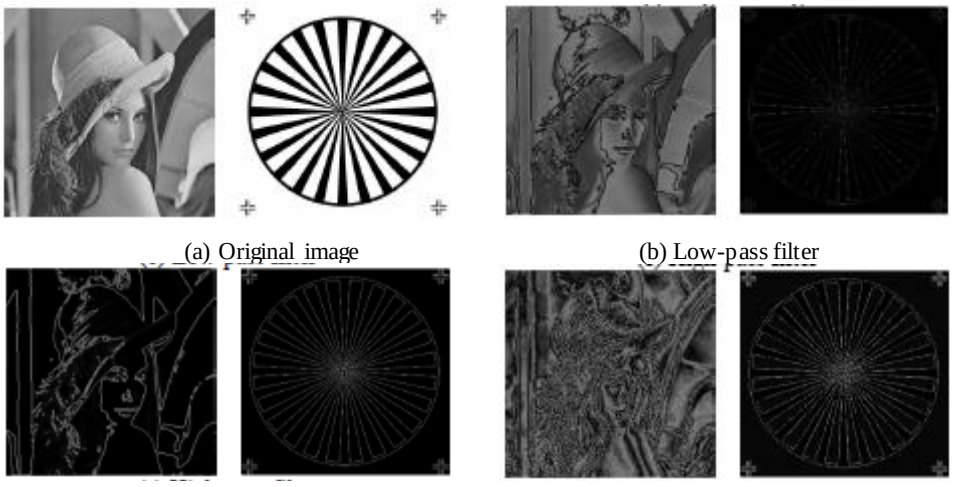
high-pass(διέλευσης υψηλών συχνοτήτων), high-boost, Prewitt και Sobel φίλτρα). Το φίλτρο που θα χρησιμοποιηθεί εξαρτάται από ένα byte ελέγχου από τον υπολογιστή. Η εκάστοτε συνάρτηση εκτελείται σε 3x3 δισδιάστατο πίνακα για κάθε εικόνα, με σύγκριση των μέγιστων διαφόρων μεταξύ των οριζόντιων, κάθετων και διαγώνιων pixels και μια τιμή κατωφλίου. Εάν το μέγιστο των διαφορών είναι μεγαλύτερο από την τιμή κατωφλίου, το εικονοστοιχείο στο κέντρο θα γεμίσει με αυτή την μέγιστη τιμή, αλλιώς το pixel στο κέντρο θα είναι μηδέν.



Σχήμα 4.2.1: The structure of DIPS

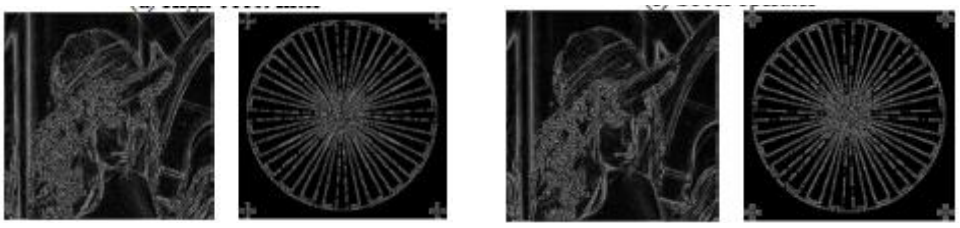
Ο μετασχηματισμούς Wavelets εκτελείται με τη χρήση του Legall 5/3 φίλτρο. Ο DIPS χρησιμοποιεί αυτό το φίλτρο λόγω της σύστασης του JPEG-2000 πρότυπου συμπίεσης εικόνας. Πρόκειται για ένα αναστρέψιμο και χωρίς απώλειες μετασχηματισμό. Για τη βελτίωση υπολογισμού του χρόνου αυτής της συνάρτησης, η μονάδα μετασχηματισμού Wavelets έχει σχεδιαστεί ως ένας IP πυρήνας συμμορφώνεται με το IBM CoreConnect ™ πρότυπο.[22] Η συγκεκριμένη παρουσίαση εισάγει μια μέθοδο για την εφαρμογή ενός συστήματος επεξεργασίας εικόνας σε FPGA. Το MicroBalze™ χρησιμοποιείται για να κάνει εύκολο το σχεδιασμό ενσωματωμένων συστημάτων. Αυτός 32-bit μικροεπεξεργαστής είναι αρκετά ισχυρός ώστε να υποστηρίξει εφαρμογές επεξεργασίας εικόνας, και αρκετά εύκολος ώστε να γίνει κατανοητός γρήγορα. Εκτός από τις παραπάνω λειτουργίες, ο DIPS μπορεί να αναβαθμιστεί για να συμπιέσει μια εικόνα (στο σχεδιασμό φάση). Εάν παρέχονται η είσοδος εικόνας και οι συσκευές εξόδου είναι, ο DIPS μπορεί να χρησιμοποιηθεί ως μια πλατφόρμα για την ανάπτυξη πολλών εφαρμογών στον τομέα της επεξεργασίας εικόνας.

Στην Εικόνα 4.2.1(a) παρατίθενται τα αποτελέσματα της συνάρτησης φίλτρου εικόνας στον DISP.



(a) Original image (b) Low-pass filter

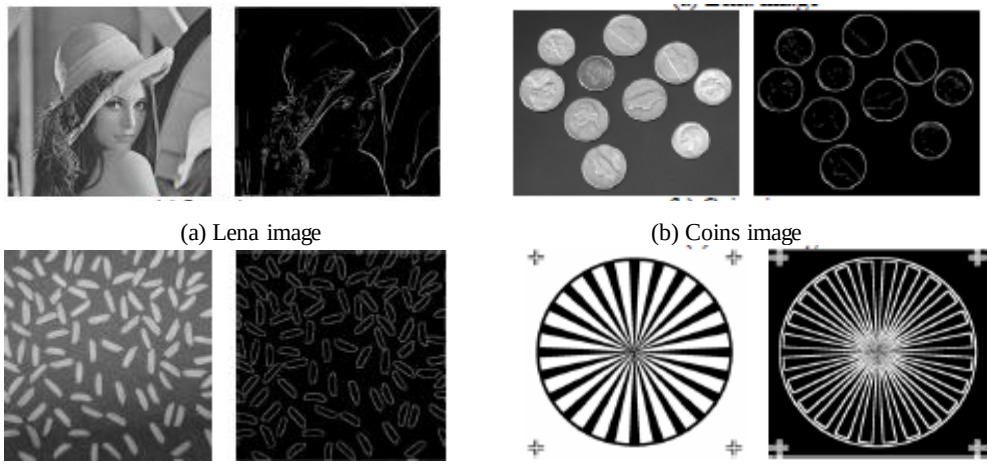
(c) High-pass filter (d) High-boost filter



(e) Sobel operator (f) Prewitt operator

Εικόνα 4.2.1(a): Image filter function

Η Εικόνα 4.2.1(b) παρουσιάζει το αποτέλεσμα της λειτουργίας ανίχνευσης ακμών στον DISP.



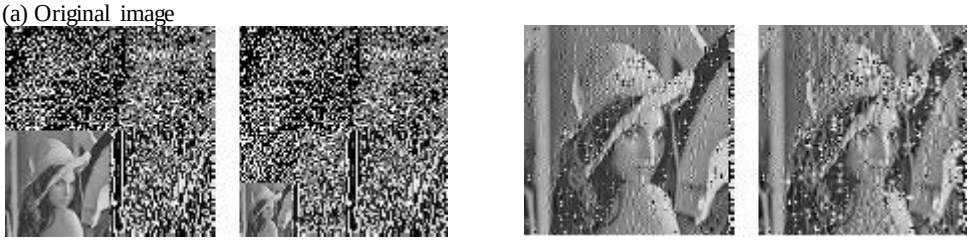
(a) Lena image (b) Coins image

(c) Rice image (d) Pat image

Εικόνα 4.2.1(b): Edge detection function

Η Εικόνα 4.2.1(c) παρουσιάζει τα αποτελέσματα του προς τα εμπρός και αντίστροφου διακριτού μετασχηματισμού wavelets στον DIPS.

(a) Original image



(b) 1-level FDWT (c) 2-level FDWT (d) 1-level IDWT (e) 2-level IDWT

Εικόνα 4.2.1(c): Forward and Inverse Wavelets Transform

Όπως παρουσιάζεται, ο αντίστροφος μετασχηματισμός wavelets έχει σφάλμα λάθους εξαιτίας αποκοπής του άκρου του αριθμού των δυαδικών ψηφίων στη δομή του.

4.3 Κρυπτογράφηση επεξεργασμένων εικόνων σε ενσωματωμένα συστήματα

Πέρα από την μεθοδολογία που τελικώς χρησιμοποιήσαμε υπάρχουν δοκιμασμένες μεθοδολογίες που έχουν ήδη χρησιμοποιηθεί είτε στην περίπτωση υλικού, είτε εκείνη του λογισμικού.

4.3.1 Ψηφιακή Υδατογράφηση (watermarking)

Μια απλή και αποτελεσματική μέθοδος κρυπτογράφησης ψηφιακά επεξεργασμένης εικόνας αποτελεί η ψηφιακή υδατογράφηση. Η μέθοδος υδατογραφήματος είναι μια εξαιρετική τεχνική για να προστατεύσει την πνευματική ιδιοκτησία μιας ψηφιακής εικόνας. Το **ψηφιακό υδατόσημο** (digital watermark) είναι χαρακτηριστική πληροφορία αναγνώρισης ενός ηλεκτρονικού αρχείου/προγράμματος, που τοποθετείται εμβόλιμα στα κυρίως δεδομένα του για την πιστοποίηση της ιδιοκτησίας του. Αποτελεί μια μέθοδο προστασίας για το δημιουργό του αρχείου/προγράμματος. Χρησιμοποιείται από εταιρίες ανάπτυξης λογισμικού, αλλά και από δημιουργούς όπως σκηνοθέτες, συγγραφείς, επαγγελματίες φωτογράφους και μουσικοσυνθέτες.

Pixel	block 1	block 2	block 1 superimposes on block 2
■	(1, 0)	(0, 1)	(1, 1)
■	(0, 1)	(1, 0)	(1, 1)
□	(1, 0)	(1, 0)	(1, 0)
□	(0, 1)	(0, 1)	(0, 1)

Εικόνα 4.3.1.1 A (2, 2)-visual threshold scheme

Η προτεινόμενη μέθοδος υδατογραφήματος είναι κτισμένη πάνω στην έννοια της οπτικής κρυπτογραφίας. Σύμφωνα με την προτεινόμενη μέθοδο, το μοτίβο υδατογραφήματος δεν πρέπει να είναι ενσωματωμένο στην πρωτότυπη εικόνα απευθείας, γεγονός που καθιστά δυσκολότερη τόσο την ανίχνευση όσο και την ανάκτησή της μέσω της υδατογραφημένης εικόνας κάνοντας χρήση παράνομων τρόπων.

Μπορεί να ανακτηθεί από την εικόνα με σήμανση χωρίς να κάνει σύγκριση με την αρχική εικόνα. Ο συμβολαιογράφος, επίσης, μπορεί χωρίς απευθείας σύνδεση να κρίνει το ιδιοκτησιακό καθεστώς της ύποπτης εικόνας με τη μέθοδο αυτή. Το μοτίβο υδατογραφήματος μπορεί να είναι οποιαδήποτε σημαντική μαύρη / άσπρη εικόνα που μπορεί να χρησιμοποιηθεί για να χαρακτηρίζει τον ιδιοκτήτη. Πειραματικά αποτελέσματα δείχνουν ότι το μοτίβο του υδατογραφήματος στη σηματοδοτημένη εικόνα έχει καλή διαφάνεια και ευρωστία. Με την προτεινόμενη μέθοδο, όλα τα εικονοστοιχεία της σηματοδοτημένης εικόνας είναι ίσα με την αρχική εικόνα.

Η οπτική κρυπτογραφία είναι μια νέα έννοια που ορίζεται από τους Naor και Shamir. Πρόκειται για ένα εκτεταμένο είδος του (t, n) συστήματος κατώτατων ορίων που ονομάζεται επίσης και (t, n)-οπτικό σύστημα κατώφλι. Η σκιά του κάθε συμμετέχοντος είναι μια διαφάνεια που δείχνει τυχαία τελείες. Το κοινό μυστικό είναι μια εικόνα που αποτελείται από ασπρόμαυρα pixels. Κάθε t από αυτές τις n σκιές μπορεί να κάνει το κοινό μυστικό να αναγνωρίζεται μέσα από το ανθρώπινο οπτικό σύστημα όταν στοιβάζονται μαζί. Κάθε t-1 (ή και λιγότερο) σκιές όταν στοιβάζονται μαζί μπορούν να δημιουργήσουν καμία γνώση σχετικά με το κοινό μυστικό. Το σύστημα αυτό (2,2) οπτικό κατώφλι είναι εκείνο που χρησιμοποιήθηκε στην παρούσα έρευνα.

The color of the *i*-th pixel in *watermark pattern* is	The left most bit of the R_i-th pixel of Image *M* is	Assign the *i*-th pair, (v_{i1}, v_{i2}), of *verification information V* to be
Black	"1"	(0, 1)
Black	"0"	(1, 0)
White	"1"	(1, 0)
White	"0"	(0, 1)

Εικόνα 4.3.1.2 The rules to assign the value of verification

Η εικόνα που αποθηκεύεται στον υπολογιστή μπορεί να θεωρηθεί μια σύνθεση των pixels. Έστω ότι κάθε ένα pixel αποθηκεύονται σε d bits. Στη συνέχεια, μια 2D γκρι-επίπεδου εικόνα μπορεί εμφανίζεται χρησιμοποιώντας ένα σετ των pixels. Το μοτίβο υδατογραφήματος το οποίο εξετάζεται στο παρόν έγγραφο αποτελείται από μαύρο ή λευκό pixel. Χρησιμοποιεί μόνο ένα bit για να εκφραστεί κάθε pixel. Ο Πίνακας 1 απεικονίζει ένα σύστημα απλό (2,2) του κατώτατου ορίου με βάση την ιδέα των Naor και Shamir. Διευκρινίζεται επίσης ο αλγόριθμος για την κωδικοποίηση κάθε pixel στην επιμερισμένη εικόνα. Ο αλγόριθμος αυτός εφαρμόζεται σε κάθε pixel στην κοινόχρηστη εικόνα προκειμένου να δημιουργηθούν τα αντίστοιχα υποπίξελς σε αντίστοιχες δύο σκιές της. Κάθε εικονοστοιχείο P στην επιμερισμένη εικόνα χωρίζεται σε δύο υποπίξελς σε κάθε μία από αυτές τις δύο σκιές. Εάν το P είναι μαύρο, τότε ο ντίλερ επιλέγει τυχαία μία από τις δύο πρώτες σειρές στον Πίνακα 1. Εάν το P είναι λευκό, τότε ο έμπορος επιλέγει τυχαία ένα από τα τελευταία δύο σειρές στον πίνακα 1. Στη συνέχεια, ο ντίλερ βάζει δύο-δύο τετράγωνα από subpixels στις Στήλες 2 και 3 με τις αντίστοιχες θέσεις στην Shadows 1 και 2, αντίστοιχα.

Το Σχήμα 1 παρουσιάζει το διάγραμμα της μεθόδου αυτής. Ο κάτοχος θα πρέπει να επιλέξει μια h × n μαύρη / λευκή εικόνα για την περίπτωση του σχεδιαγράμματος υδατοσήμου P της / του. Κατά τη διαδικασία ενσωμάτωσης, αυτή / αυτός που παράγει τις πληροφορίες ελέγχου από την αρχική εικόνα με βάση το (2,2)-οπτική κρυπτογραφία θα πρέπει και να καθορίσει το πρότυπο υδατογραφήματος της κοινόχρηστης εικόνας. Ουσιαστικά, οι πληροφορίες επαλήθευσης είναι μια σκιά του οπτικού κρυπτογραφίας.

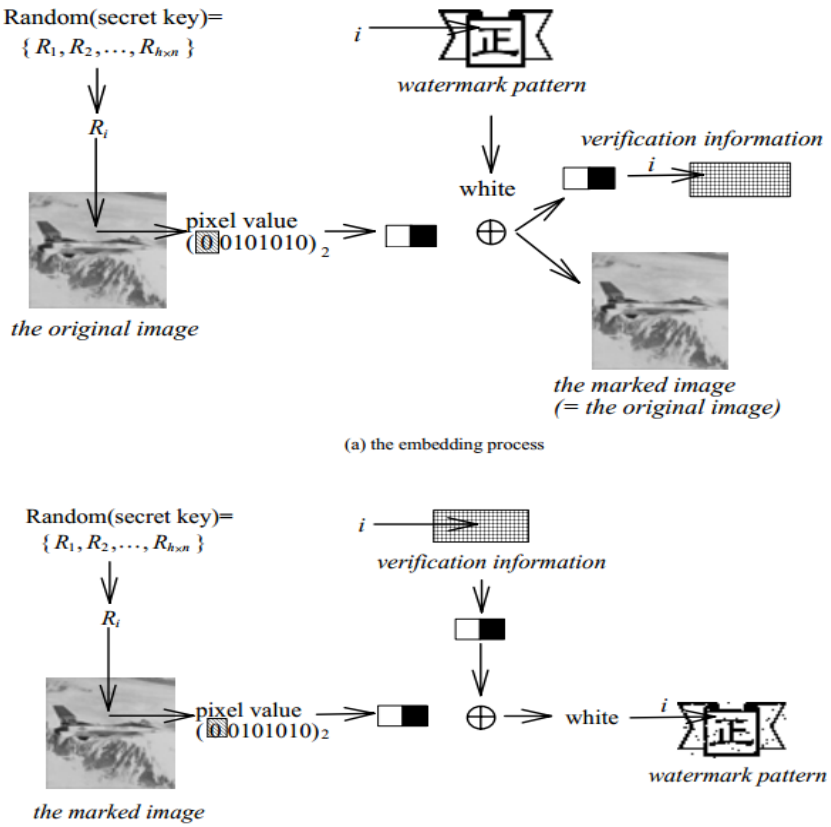
Κατά τη διαδικασία ενσωμάτωσης, ο ιδιοκτήτης θα πρέπει να επιλέξει τυχαία έναν αριθμό ως το μυστικό του κλειδί του / της, S, για να ενσωματώσει το πρότυπο υδατογραφήματος στην εικόνα M. Τα μυστικά κλειδιά για διαφορετικές εικόνες είτε είναι ίσα είτε όχι. Ο κάτοχος πρέπει να κρατήσει κρυφά. Υποθέτουμε ότι ο ιδιοκτήτης θέλει να ενσωματώσει το h × n σχεδιάγραμμα υδατοσήμου στην εικόνα M που είναι ak × l256 γκρι-επιπέδου εικόνα. Ο κάτοχος ενσωματώνει το μοτίβο υδατογραφήματος P στην εικόνα M δημιουργώντας το μυστικό κλειδί, S, καθώς και τις πληροφορίες επαλήθευσης, V, όπως τα παρακάτω βήματα:

Στάδιο 1. Επιλογή ενός τυχαίου αριθμού S ως το μυστικό κλειδί της εικόνας M.

Στάδιο 2. Χρήση του S ως σπόρος για τη δημιουργία h × n διαφορετικούς τυχαίους αριθμούς στο διάστημα [0, k × l]. (Χρησιμοποιούμε Ri για να υποδηλώσει το i-th τυχαίων αριθμών.)

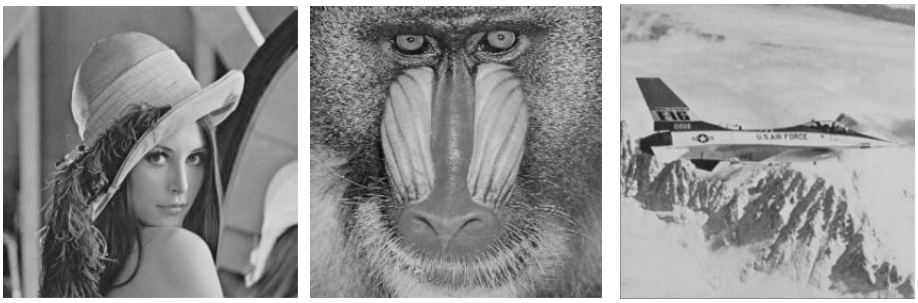
Στάδιο 3. Εκχώρηση το i-οστό ζεύγος (VI1, vi2) των πληροφοριών επαλήθευσης V βάσει του πίνακα 2.

Στάδιο 4. Συναρμολογήστε όλων των (VI1, vi2) ζεύγη για να κατασκευάσουν τις πληροφορίες επαλήθευσης V.



Εικόνα 4.3.1.3 The diagram of the proposed method

Είναι δύσκολο να αξιολογηθεί η επίδραση μιας μεθόδου υδατογραφήματος μόνο θεωρητικά. Αυτή η ενότητα παρουσιάζει ορισμένα πειραματικά αποτελέσματα σχετικά με τις προτεινόμενες μεθόδους. Όλα τα πειράματα πραγματοποιήθηκαν σε έναν προσωπικό υπολογιστή με επεξεργαστή Intel Pentium 100. Τρεις μονόχρωμες εικόνες με 256×256 pixels, “Lena”, “Baboon” και “F-16” (Δίνονται στο Σχήμα 2), χρησιμοποιήθηκαν στα πειράματά. Σε αυτές τις εικόνες, κάθε pixel περιέχει 256 επίπεδα του γκρι. Το Σχήμα 3 δείχνει το μαύρο/λευκό μοτίβο υδατογραφήματος, "Cheng», το οποίο ενσωματώθηκε σε αυτές τις τρεις εικόνες. Σύμφωνα με το Στάδιο 3, η προτεινόμενη μέθοδος δεν αλλάζει οποιαδήποτε τιμή pixel της αρχικής εικόνας για να δημιουργήσει την υδατογραφημένη εικόνα. Με άλλα λόγια, η σήμανση εικόνας είναι η ίδια όπως η αρχική εικόνα. Η διαφάνεια είναι εκείνη που απαιτείται για την προτεινόμενη μέθοδο. Τα πειραματικά αποτελέσματα φαίνονται στον Πίνακα 3.



Εικόνα 4.3.1d :"Lena", "Baboon" και "F-16"

Εικόνα 4.3.1e : The black/white watermark pattern: "Cheng"

PSNR of the *marked image*	The image quality of JPEG compression with Adobe Photoshop (version 4.0)	The recovered *watermark pattern* : "Cheng"
Marked Image = Original Image	0/low (the size of the compressed file is 10582 Bytes)	
	1/low (the size of the compressed file is 12620 Bytes)	
	2/low (the size of the compressed file is 14029 Bytes)	
	3/middle (the size of the compressed file is 15781 Bytes)	
	4/middle (the size of the compressed file is 17590 Bytes)	
	5/middle (the size of the compressed file is 16127 Bytes)	
	6/high (the size of the compressed file is 21012 Bytes)	
	7/high (the size of the compressed file is 25348 Bytes)	
	8/maximal (the size of the compressed file is 31793 Bytes)	
	9/maximal (the size of the compressed file is 40088 Bytes)	
	10/maximal (the size of the compressed file is 48611 Bytes)	

Εικόνα 4.3.1.4 Used method to embed "Cheng" into "Lena" (with 65536 Bytes)

PSNR of the *marked image*	The image quality of JPEG compression with Adobe Photoshop (version 4.0)	The recovered *watermark pattern* : "Cheng"
Marked Image = Original Image	0/low (the size of the compressed file is 18277 Bytes)	
	1/low (the size of the compressed file is 22242 Bytes)	
	2/low (the size of the compressed file is 24562 Bytes)	
	3/middle (the size of the compressed file is 27163 Bytes)	
	4/middle (the size of the compressed file is 30870 Bytes)	
	5/middle (the size of the compressed file is 28524 Bytes)	
	6/high (the size of the compressed file is 33629 Bytes)	
	7/high (the size of the compressed file is 38331 Bytes)	
	8/maximal (the size of the compressed file is 45158 Bytes)	
	9/maximal (the size of the compressed file is 54393 Bytes)	
	10/maximal (the size of the compressed file is 63970 Bytes)	

Εικόνα 4.3.1.5 Used method to embed "Cheng" into "Baboon" (with 65536 Bytes)

Πίνακας 4.3.1(i):Experimental results

PSNR of the *marked image*	The image quality of JPEG compression with Adobe Photoshop (version 4.0)	The recovered *watermark pattern* : "Cheng"
Marked Image = Original Image	0/low (the size of the compressed file is 9867 Bytes)	
	1/low (the size of the compressed file is 11846 Bytes)	
	2/low (the size of the compressed file is 12994 Bytes)	
	3/middle (the size of the compressed file is 14479 Bytes)	
	4/middle (the size of the compressed file is 16579 Bytes)	
	5/middle (the size of the compressed file is 15342 Bytes)	
	6/high (the size of the compressed file is 18295 Bytes)	
	7/high (the size of the compressed file is 21440 Bytes)	
	8/maximal (the size of the compressed file is 26413 Bytes)	
	9/maximal (the size of the compressed file is 33451 Bytes)	
	10/maximal (the size of the compressed file is 41627 Bytes)	

Εικόνα 4.3.1.6 Used method to embed "Cheng" into "F-16" (with 65536 Bytes)

Πίνακας 4.3.1(ii):Experimental results

Η εξάπλωση της ψηφιακής εικόνας δημιουργεί μια πιεστική ανάγκη για συστήματα επιβολής πνευματικών δικαιωμάτων που προστατεύουν την ιδιοκτησία πνευματικών δικαιωμάτων. Το σύστημα υδατογράφηση είναι μια εξαιρετική μέθοδος για την προστασία των πνευματικών δικαιωμάτων ιδιοκτησίας [6]. Στην εργασία αυτή, προτείνεται μια μέθοδος υδατογραφήματος με βάση την οπτική κρυπτογραφία. Παρουσιάζονται συνοπτικά τα χαρακτηριστικά της προτεινόμενης μεθόδου ως εξής:

(1) Το μοτίβο υδατογραφήματος μπορεί να είναι οποιαδήποτε προσημασμένη μαύρη/ λευκή εικόνα που μπορεί να χρησιμοποιηθεί για να το τυπικό δείγμα τον ιδιοκτήτη.

(2) Το μοτίβο υδατογραφήματος δεν πρέπει να ενσωματώνεται στην αρχική εικόνα απευθείας. (Όλα τα εικονοστοιχεία της προσημασμένης εικόνας είναι τα ίδια με εκείνα της αρχικής εικόνας.)

(3) Το μοτίβο υδατογραφήματος μπορεί να επανακτηθεί χωρίς οποιαδήποτε πληροφορία σχετικά με την αρχική εικόνα.

(4) Είναι δύσκολο να ανιχνευθεί το pixel σχετικά με το σχέδιο υδατογραφήματος χωρίς το μυστικό κλειδί που διατηρείται κρυφά από τον ιδιοκτήτη.

(5) Το μοτίβο υδατογραφήματος δεν μπορεί να ανακτηθεί από την προσημασμένη εικόνα, εκτός εάν εκείνος που ανακτά την εικόνα έχει ταυτόχρονα το μυστικό κλειδί και τις πληροφορίες επαλήθευσης.

(6) Ο εκάστοτε συμβολαιογράφος μπορεί να επιδικάσει την κυριότητα της εικόνας εκτός σύνδεσης.

4.3.2 Ασφαλής μετάδοση εικόνας σε πολλαπλές FPGA

Έως τώρα οι μηχανικούς σχεδιασμού ενσωματωμένων έχουν υλοποιήσει με επιτυχία τα σχέδιά τους μέσω της εφαρμογή ειδικών ολοκληρωμένων κυκλωμάτων (ASIC) και / ή ψηφιακών επεξεργαστών σήματος (DSP), ωστόσο, με την πρόοδο της τεχνολογίας VLSI μια πολύ ισχυρή συσκευή υλικού, δηλαδή η Field Programmable Gate Array (FPGA), συνδυάζει τα βασικά πλεονεκτήματα της ASICS και DSPs η οποία αναπτύχθηκε έχει τη δυνατότητα επαναπρογραμματισμού καθιστώντας την μια πολύ ελκυστική συσκευή για την ταχεία προτυποποίηση.

Η επικοινωνία της εικόνας και των τηλεοπτικών στοιχείων σε πολλαπλές FPGA's δεν είναι πλέον μακριά από τη διατύπωση της ασφαλούς μετάδοσης μεταξύ τους, και κατόπιν η συνάφεια της κρυπτογραφίας είναι όντως αναπόφευκτη.[7] Το Hardware που σχεδιάζει για την εικόνα και την επεξεργασία βίντεο χρησιμοποιείται για ταχύτερη απόδοση και όχι το λογισμικό, με σκοπό να ανταποκριθεί στις απαιτήσεις των τελικών χρηστών, διατηρώντας τη σχετικότητα της αγοράς και την ίδια στιγμή την ασφάλεια που αποτελεί μια άλλη ανησυχία. Έτσι η ανάγκη να γνωστοποιούν τα στοιχεία αυτά μέσα με ασφάλεια, μεταξύ πολλαπλών πλατφορμών μετά την επεξεργασία για την ενίσχυση της ανθρώπινης αντίληψης και ικανοποίησης της.

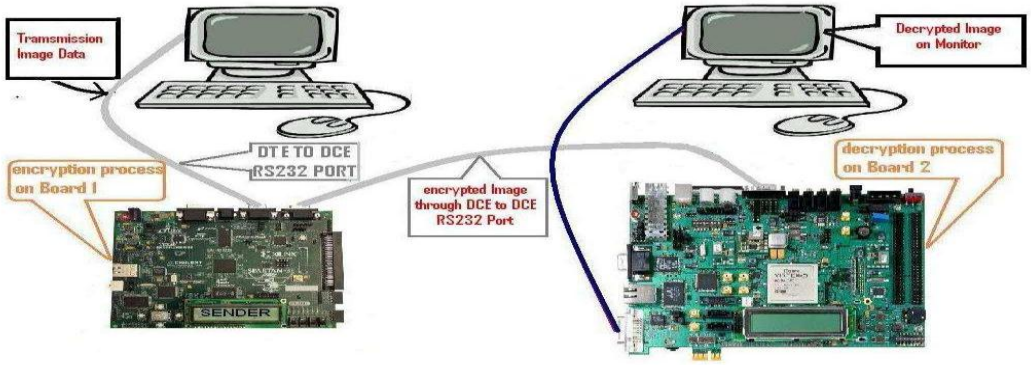
Οι εφαρμογές εικόνας που χρησιμοποιούνται στο διαδίκτυο, τα συστήματα πολυμέσων, την ιατρική, και την τηλεϊατρική, με σκοπό την επικοινωνία, ενώ η ανακοίνωση αυτή δεν είναι εξασφαλισμένη καθόλου θα μπορούσε να πέσει στο θήραμα οποιουδήποτε εισβολέα που θα μπορούσε να επιτεθεί στις μεταδιδόμενες εικόνες εκ τούτου ευαίσθητες εικόνες μπορούν να αποκαλυφθούν σε μη εξουσιοδοτημένο πρόσωπο.

Έτσι, στην συγκεκριμένη εργασία που παραθέτουμε περιγράφεται ένα μοντέλο αρχιτεκτονικής υλικού που θα μπορούσε να είναι η ραχοκοκαλιά της κύριο μοντέλο του υλικού του εξασφάλισε μετάδοση εικόνας. Το μοντέλο περιλαμβάνει δύο πλατφόρμες FPGA δηλαδή η Xilinx Spartan 3E και Virtex 5 που οδηγούν σε μια ετερογενή επικοινωνία μεταξύ τους, και RS-232 καλώδιο για το μέσο μετάδοσης. Ως ένα πρώτο βήμα, από τον κεντρικό υπολογιστή μια τιμή pixel της ψηφιακής εικόνας διαβάζεται και αποστέλλεται στη σειριακή θύρα του υπολογιστή στην πλατφόρμα του Mathworks MATLAB. Έπειτα η φόρμα μέσω της σειριακής θύρας του υπολογιστή μεταδίδει τα δεδομένα εικόνας στη DCE θύρα της πρώτης FPGA πλατφόρμα η οποία στην πραγματικότητα αποδίδει όπως μια μηχανή κρυπτογράφησης εκτελώντας κρυπταλγόριθμο ροής, ο αλγόριθμος κρυπτογράφησης ονομάζεται RC4 [9].

Τα κρυπτογραφημένα δεδομένα εικόνας αποστέλλονται στη συνέχεια στη δεύτερη πλατφόρμα FPGA η οποία στην πραγματικότητα λειτουργεί ως κινητήρας αποκρυπτογράφησης από το μέσο εκτέλεση μέρους αποκρυπτογράφησης του RC4. Τα κρυπτογραφημένα δεδομένα εικόνας και η αρχική εικόνα προβάλλονται σε μια οθόνη TFT που ενεργεί ως μια μονάδα οθόνης. Για την επίτευξη αυτού του σκοπού έπρεπε να προσαρμόσουν έναν ελεγκτή interface TFT από την πλακέτα στην μονάδα εμφάνισης το οποίο είναι ένα άλλο πλεονέκτημα της εργασίας αυτής. Για λόγους επαλήθευσης έχουν δημιουργήσει το interface TFT στην πρώτη πλακέτα για την παρατήρηση του κρυπτογραφημένου εικόνα όπως φαίνεται στο σχήμα 6.

Εικόνα 4.3.2(a) : Output images for secured image transmission.

Υπάρχουν μερικές εργασίες διαθέσιμες οι οποίες έδωσαν κατά κάποιο τρόπο το έναυσμα για να πραγματοποιηθεί η συγκεκριμένη έρευνα/εφαρμογή. Πιο συγκεκριμένα με την εξασφαλισμένη μετάδοση εικόνας, αλλά το βασικό μοντέλο που περιγράφεται εδώ είναι απλό, αποτελεσματικό και εύκολο να υλοποιηθεί. Παρακάτω δίνεται το περίγραμμα του πειράματος που διεξήχθη.



Εικόνα 4.3.2(a) :Secured image transmission on multiple FPGA platform

Ουσιαστικά αυτό το έγγραφο, συζήτησε εν συντομία το έργο που έχει πραγματοποιηθεί στην περιοχή επεξεργασίας εικόνας ιδίως με έμφαση την εφαρμογή του στη συσκευή υλικού, καθώς και τη διαβίβαση των δεδομένων εικόνας μέσα από ένα ασφαλή τρόπο.

5. Μεθοδολογία για την επεξεργασία της εικόνας

Στο παρόν κεφάλαιο παραθέτουμε μια γενική περιγραφή της μεθοδολογίας που ακολουθήσαμε, σε σχέση με άλλες πιθανές μεθόδους για την κρυπτογράφηση της επεξεργασίας εικόνας.

5.1 Μεθοδολογία Εύρεσης Ακμών με Ανιχνευτή Sobel

Σε πρώτο στάδιο στην παρούσα εργασία, ασχοληθήκαμε με την επεξεργασία εικόνας. Πιο συγκεκριμένα κάνοντας χρήση του προγράμματος MATLAB® εισαγάγαμε εικόνες με σκοπό την εύρεση ακμών μέσω του ανιχνευτή Sobel. Αρχικά χρησιμοποιήσαμε την εικόνα *'cameraman.bmp'* στην οποία εφαρμόσαμε την εντολή «*imcrop*» ώστε να πάρουμε ένα τμήμα αυτής με τελικό στόχο να περάσουμε το φίλτρο εύρεσης ακμών του Sobel. Το αποτέλεσμα που πήραμε από την επεξεργασμένη εικόνα παρουσιάζεται παρακάτω.

Εικόνα5.1a : Αρχική Εικόνα

Εικόνα5.1b: Cropped Εικόνα

Στη συνέχεια θελήσαμε να συγκρίνουμε τα αρχικά αποτελέσματα της εικόνας η οποία έχει υποστεί μάσκα Sobel, που πήραμε από το MATLAB® με εκείνα από το dual core σύστημα σε FPGA. Η διαδικασία που ακολουθήσαμε αναλύεται στη συνέχεια. Αφού περάσαμε την αρχική εικόνα (*'cameraman.bmp')* σε ένα συγκεκριμένο dual core σύστημα στη συνέχεια εφαρμόσαμε τον αλγόριθμο Sobel. Τα αποτελέσματα που πήραμε στο HyperTerminal ήταν τελικά η επεξεργασμένη εικόνα. Σε επόμενο στάδιο πήραμε τα pixel που λάβαμε από το minicom, τα περάσαμε στο Matlab και ενεργοποιήσαμε την εντολή «*imshow*» ώστε να δούμε την εικόνα στην οποία αντιστοιχούν τα pixel που πήραμε από το dual core σύστημα.

Εικόνα5.1c : Cropped Εικόνα Matlab

Εικόνα5.1d : Cropped Εικόνα Xilinx

Από τις εικόνες που παρατίθενται διαπιστώνουμε ότι τα αποτελέσματα στα οποία καταλήγουμε και στις δύο περιπτώσεις είναι όμοια.

5.2 Μεθοδολογία κρυπτογράφησης της εικόνας Sobel και TEA

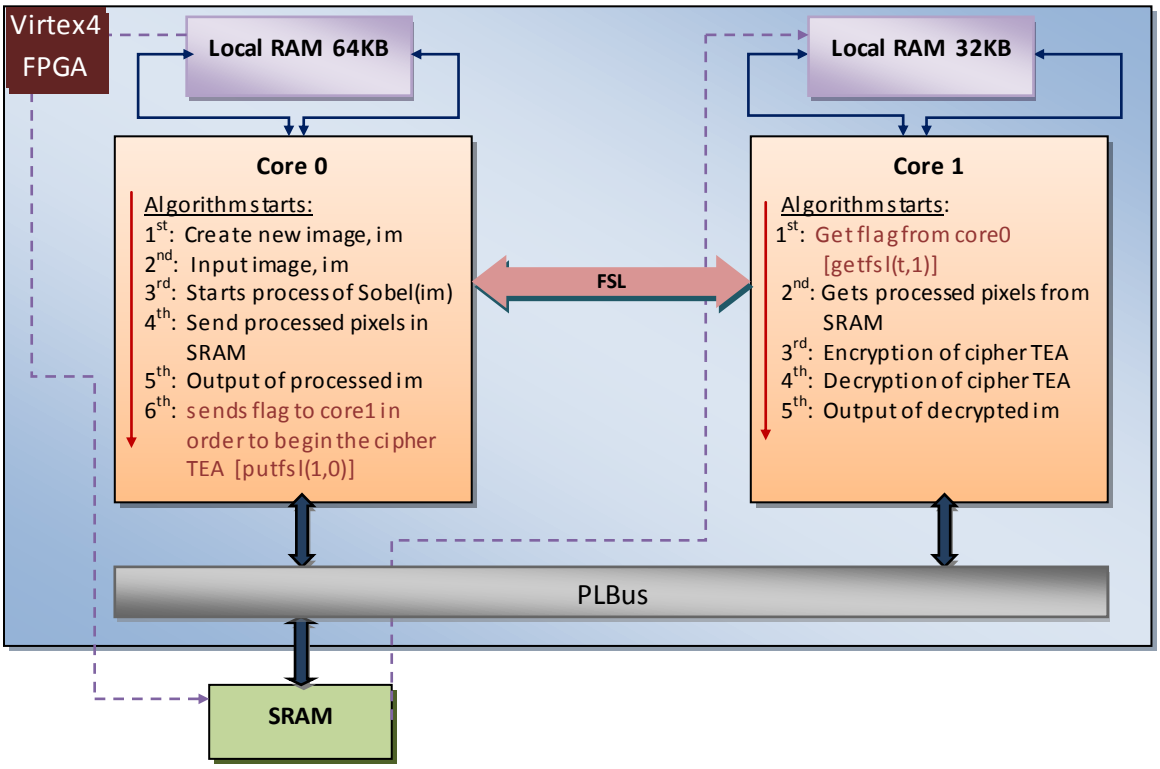
Σε επόμενο στάδιο επιχειρήσαμε να κρυπτογραφήσουμε την επεξεργασμένη εικόνα. Ουσιαστικά χρησιμοποιήσαμε ένα σύστημα dual core, όπως αναφέρουμε παραπάνω, όπου ένας είναι ο πυρήνας πάνω στον οποίο εκτελείται ο αλγόριθμος Sobel ενώ ο δεύτερος είναι εκείνος που αφού λάβει τα επεξεργασμένα pixel στη συνέχεια αναλαμβάνει να τα κρυπτογραφήσει μέσω του κρυπταλγόριθμου TEA. Με τη βοήθεια και πάλι του HyperTerminal διαπιστώνουμε ότι τα pixel εκείνα που δίνουμε στην είσοδο του αλγορίθμου TEA τα οποία θέλουμε να κρυπτογραφήσουμε, είναι όμοια με εκείνα που παίρνουμε κατά τη έξοδο, δηλαδή κατά τη διαδικασία της αποκρυπτογράφησης.

5.2.1 Αλγόριθμοι επεξεργασίας εικόνας και λοιποί lightweight αλγόριθμοι

Στο σημείο αυτό να αναφέρουμε ότι από πειράματα που πήραμε πριν καταλήξουμε στην τελική επιλογή τόσο για τον αλγόριθμο επεξεργασίας εικόνας , τον Sobel όσο και για τον αλγόριθμο κρυπτογράφησης, τον TEA υπάρχουν οι παρακάτω δυνατοί συνδυασμοί αλγορίθμων που θα μπορούσαν να μας οδηγήσουν στο ίδιο αποτέλεσμα.

Ένας συνδυασμός αλγορίθμων θα μπορούσε να είναι και πάλι η επιλογή του ανιχνευτή Sobel αλλά όσο αφορά την κρυπτογράφηση θα μπορούσε να χρησιμοποιηθεί ο αλγόριθμος Present. Επίσης ένας άλλος συνδυασμός που θα μπορούσαμε να έχουμε επιλέξει θα μπορούσε να ήταν ο ανιχνευτής ακμών Canny σε συνδυασμό με τον κρυπταλγόριθμο TEA. Ακόμα ένας άλλος συνδυασμός αλγορίθμων θα μπορούσε να είναι ο αλγόριθμος επεξεργασίας εικόνων Canny με τον αλγόριθμος κρυπτανάλυσης Present.

Τέλος ο λόγος για τον οποίο καταλήξαμε να χρησιμοποιήσουμε τον συνδυασμό των αλγορίθμων Sobel και TEA για την κρυπτογράφηση της επεξεργασμένης εικόνας ήταν διότι τόσο ο Sobel όσο και ο TEA διακρίνονται για την απλότητα τους κάτι που τους καθιστά εύκολους στην κατανόηση αλλά και γρήγορους από άποψη υλοποίησης . Βέβαια η απλότητα που τους χαρακτηρίζει σε καμία περίπτωση δεν επηρεάζει είτε την αποδοτικότητα είτε την ισχύ τους. Αντιθέτως να τονίσουμε ότι πρώτον ο Sobel είναι ένας από τους πιο γνωστούς αλγόριθμους που χρησιμοποιείται για εύρεση ακμών και δεύτερον ο TEA είναι αλγόριθμος κρυπτανάλυσης που η χρήση του ενδείκνυται κυρίως για ενσωματωμένα συστήματα.



Εικόνα5.2.1 : Οι λειτουργίες των επεξεργαστών και η αρχιτεκτονική του υποσυστήματος.

6. Περιγραφή Υλοποίησης σε Υλικό (Hardware)

6.1Αρχιτεκτονική Συστήματος

Από άποψη υλικού για την υλοποίηση της παρούσας εργασίας, δομήσαμε την αρχιτεκτονική μας στηριζόμενοι στην βασική αρχιτεκτονική που έχει διαμορφώσει η Xilinx στα συστήματα της. Βασιζόμαστε δηλαδή τους επεξεργαστές microblaze 7.30 a, οι οποίοι συνδέονται με το PLB Bus, ώστε να έχουν πρόσβαση με τα περιφερειακά και τις εξωτερικές μνήμες. Η ευχρηστία των FPGA's και η προχωρημένη αναπτυξιακή πλακέτα της Xilinx(ml 405) μας επιτρέπουν την προσθήκη αρκετών επεξεργαστών καθώς και τον παράλληλο προγραμματισμό τους.

6.2Επεξεργαστές και Επικοινωνία

Αρχικά τοποθετήσαμε στο σύστημα μας δύο microblaze . Τον microblaze0(core 0) στον οποίο εφαρμόζεται ο ανιχνευτής ακμών Sobel σε ψηφιακή εικόνα και τον microblaze1(core 1) στην περίπτωση του οποίου η επεξεργασμένη εικόνα θα υποστεί τον κρυπταλγόριθμο TEA. Να σημειώσουμε ότι και οι δύο επεξεργαστές είναι προγραμματισμένοι στην ίδια συχνότητα των *100MHz*. Αν και εξυπηρετούνται από τις μνήμες που αναφέραμε παραπάνω προκύπτει και η ανάγκη άμεσης επικοινωνίας μεταξύ τους για την ορθή λειτουργία του συστήματος. Το FSL bus , το οποίο παρέχεται από τη Xilinx, είναι εκείνο που δίνει τη δυνατότητα μέσω της χρήση κατάλληλων εντελών να στέλνουν μεταξύ τους μηνύματα οι επεξεργαστές. Κάθε επεξεργαστής προγραμματίζεται κατάλληλα αναλόγως τις απατήσεις που έγκειται από την χρησιμότητα του.

6.3Μνήμες

Ο κάθε microblaze επεξεργαστής συνδέεται με την τοπική του μνήμη BRAM. Στην περίπτωση του microblaze_0 η χωρητικότητα της τοπικής μνήμης εντοπίζεται στα 64k ενώ για τον microblaze _1 η χωρητικότητα περιορίζεται στα 32k. Τέλος χρησιμοποιείται η SRAM με χωρητικότητα 1M, στην οποία στέλνονται από τον microblaze_0 τα επεξεργασμένα pixels, τα οποία με τη σειρά του θα πάρει ο microblaze _1 για να ξεκινήσει η κρυπτογράφηση .

6.4Buses

Το PLB Bus χρησιμοποιείται από τη Xilinx για την επίτευξη της επικοινωνίας μεταξύ επεξεργαστών και περιφερειακών, στο οποίο συνδέονται, επεξεργαστές, εξωτερικές ή κοινόχρηστες – εσωτερικές μνήμες και τα περιφερειακά.

6.5Περιφερειακά

Από τα περιφερειακά που συνδέονται στο PLB Bus εμείς χρησιμοποιούμε τον timer /counter της Xilinx για μετρήσεις του χρόνου εκτέλεσης του αλγορίθμου Sobel, του χρόνου μεταφοράς των επεξεργασμένων pixels από την BRAM του microblaze_0 στην SRAM και τέλος του χρόνου εκτέλεσης του αλγορίθμου TEA τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση. Η επικοινωνία των επεξεργαστών και των περιφερειακών συγχρονίζεται από τοποθετημένους arbiters(διαιτητές) που είναι υπεύθυνοι για το ποιος θα «μιλήσει» πρώτος σύμφωνα με το που θέλει να «μιλήσει»

7. Περιγραφή Υλοποίησης σε λογισμικό (Software)

7.1 Περιγραφή λογισμικού του Αλγορίθμου Sobel

Η ψηφιακή εικόνα που χρησιμοποιήσαμε είναι ένας δισδιάστατος πίνακας μεγέθους 30x29 την οποία περάσαμε στη δομή τύπου «image», παρατηρούμε το σχετικό κομμάτι του κώδικα στην εικόνα χ.χ.

```
struct image {
                    struct header *info;          //Pointer to header
                    unsigned char **data;         //Pixel values
};
typedef struct image * IMAGE;
….

IMAGE im;
          im = (IMAGE)newimage (ROWS, COLUMNS);
          im->info->oi  = 30;
          im->info->oj  = 29;
```

Ο δείκτης *dstpoint* δείχνει στον πίνακα που είναι αποθηκευμένη η επεξεργασμένη εικόνα ο οποίος θα χρησιμοποιηθεί για να περάσουμε την εικόνα στην SRAM.Με την εντολή : **(dstPoint + count_sobel)= x->data[i][j] ;* περνάμε στην SRAM τα επεξεργασμένα pixels

```
for (i=0; i<x->info->nr;  i++) {
    for (j=0; j<x->info->nc;  j++){
          x->data[i][j]  = z->data[i][j];

*(dstPoint + count_sobel)= x->data[i][j]  ;
count_sobel++;
          }
    }
```

Με την παρακάτω εντολή βλέπουμε στην οθόνη , σε μορφή πίνακα τα pixels αφού έχουν υποστεί το φίλτρο Sobel.

```
xil_printf  ("%d %d %d\r\n", image->info->nc,  image->info->nr,  255);
```

Στο παρακάτω κομμάτι κώδικα, το οποίο εντοπίζουμε στη main, πραγματοποιούνται οι ακόλουθες λειτουργίες. Αρχικά περνάμε την εικόνα την οποία θέλουμε να επεξεργαστούμε στην δομή τύπου im και αφού γεμίσει ο πίνακας στη συνέχεια είναι σειρά της συνάρτησης Sobel. Αφού ολοκληρωθεί ο Sobel παίρνουμε σαν έξοδο την επεξεργασμένη εικόνα και ενημερώνουμε μέσω του fls , στέλνοντας flag στον core1 πως ολοκληρώθηκε ο Sobel και ότι μπορεί να ξεκινήσει τη λειτουργία του.

```
for (i=0; i<ROWS; i++)
        for (j=0; j<COLUMNS; j++)
            im->data[i][j] = croped[i][j];
  sobel(im);

   Output_PBM (im, "sobel.pgm");
putfsl(1,0);
```

7.2 Περιγραφή λογισμικού του Αλγορίθμου TEA

Ο microblaze_1 ξεκινάει τη λειτουργία του μόλις λάβει το μήνυμα από τον microblaze_0 ότι ο αλγόριθμος Sobel έχει ολοκληρωθεί. Η επικοινωνία αυτή επιτυγχάνεται μέσω του fsl. Αρχικά η σύνταξη της εντολής ήταν getfsl(t,0) αλλά για να αρχίσει να τρέχει ο TEA έπρεπε να του δώσουμε την τιμή 1. Η διαδικασία παρουσιάζεται παρακάτω.

```
getfsl(t,1);
```

Περνάμε στον μονοδιάστατο πίνακα in[] τα 870 επεξεργασμένα pixels της εικόνας με σκοπό στη συνέχεια να εφαρμόσουμε τη μάσκα του TEA

```
for(t=0 ; t<870 ;t++){
        in[t] = *(dstPoint + t) ;
            // xil_printf("%d, ElementsForCrypto%d\r\n",t,in[t]);
}
```

Είσοδος του αλγορίθμου κρυπτογράφησης είναι ο πίνακας in_trans[2]. Δίνουμε στον πίνακα τα επεξεργασμένα pixels που έχουμε αποθηκευμένα στην SRAM, ανα 2, καθώς ο αλγόριθμος υποστηρίζει κρυπτογράφηση έως 2 στοιχεία. **Περνάμε ανα 2 pixel την επεξεργασμένη εικόνα στον πίνακα-είσοδο του αλγορίθμου κρυπτογράφησης**

```
1  …
   for(j=0;j<435;j++){
2          in_trans[0]=in[j];
           in_trans[1]=in[++j];
3          …
```

Με την παρακάτω εντολή καλούμε τη συνάρτηση κρυπτογράφησης του αλγορίθμου TEA .

```
1  xtea_encipher ( in_trans, out, key);
```

Με τις παρακάτω εντολές περνάμε τα αποτελέσματα της μάσκας του αλγορίθμου TEA, (παίρνουμε δηλαδή το αποτέλεσμα της κρυπτογράφησης) ο οποίος δουλεύει για δύο pixels κάθε φορά , στα v0 και v1.

```
1  en_result[0]=v0;
2  en_result[1]=v1;
```

Αφού ολοκληρωθεί η κρυπτογράφηση περνάμε τα κρυπτογραφημένα pixels στον πίνακα in_trans[] ,με τελικό στόχο η συνάρτηση της αποκρυπτογράφησης να τα πάρει ως είσοδο.

```
1  in_trans[0]= en_result[0];
2  in_trans[1]= en_result[1];
```

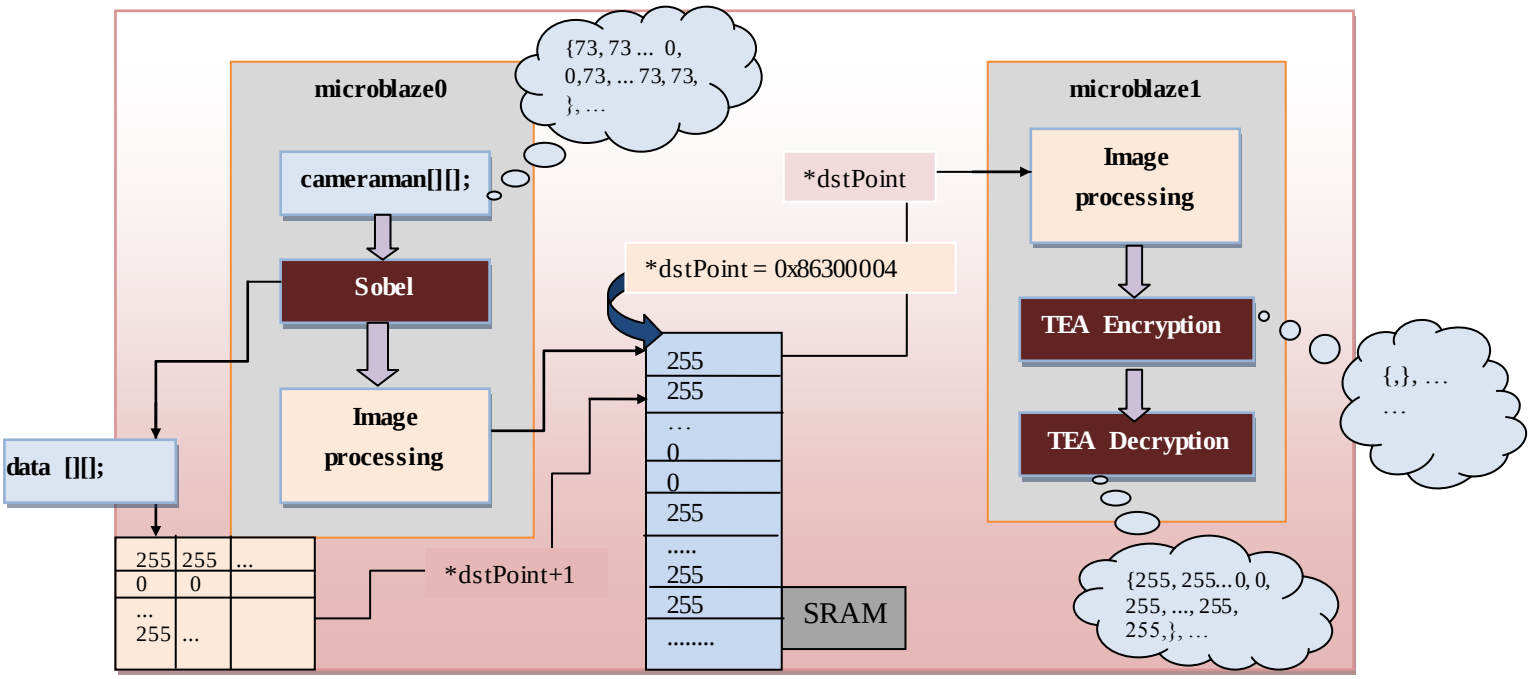
Με την παρακάτω εντολή καλούμε τη συνάρτηση αποκρυπτογράφησης του αλγορίθμου TEA.

```
1  xtea_decipher ( in_trans, out, key);
```

Τέλος πήραμε μετρήσεις για το πόσο χρόνο διήρκησαν ο αλγόριθμος του Sobel, η μεταφορά των επεξεργασμένων pixels από τη BRAM στην SRAM και τέλος πόσος χρόνος δαπανήθηκε έως ότου ολοκληρωθούν τόσο ο αλγόριθμος κρυπτογράφησης του TEA όσο και ο αλγόριθμος αποκρυπτογράφησης του TEA. Για την περάτωση των προαναφερθέντων μετρήσεων χρησιμοποιήσαμε τις συναρτήσεις που ενεργοποιούν τον hardware timer της Xilinx. Παρακάτω αναλύουμε τη ιεραρχική διαδικασία που ακολουθήσαμε ώστε να πάρουμε τα επιθυμητά αποτελέσματα.

Πιο αναλυτικά για την έναρξη του μετρητή χρησιμοποιήσαμε την εντολή:*XTmrCtr_Start(&XPS_Timer,0);* ενώ για τη λήξη καταγραφής του μετρητή εφαρμόσαμε την εντολή: *XTmrCtr_Stop(&XPS_Timer,0)*. Σε επόμενο στάδιο ενεργοποιήσαμε την εντολή:*Value_encipher= XTmrCtr_GetValue(&XPS_Timer,0);* ώστε να πάρουμε την τιμή του μετρητή μέσω της μεταβλητής *Value_encipher*. Τέλος μηδενίσαμε, κάναμε δηλαδή επαναφορά στον μετρητή ώστε να πάρουμε πιθανές επόμενες μετρήσεις. Στο σχήμα που παραθέτουμε φαίνεται η σειρά με την οποία εφαρμόστηκαν οι συναρτήσεις του Timer στην περίπτωση της κρυπτογράφησης των επεξεργασμένων pixels.

```
1  XTmrCtr_Start(&XPS_Timer,0) ;
2   xtea_encipher ( in_trans,  out,  key);
3    XTmrCtr_Stop(&XPS_Timer,0) ;
4       Value_encipher = XTmrCtr_GetValue(&XPS_Timer,0) ;
   ....
...
5    XTmrCtr_Reset(&XPS_Timer,0) ;
```



Σχημα 7.1: Διαδικασίες επεξεργασίας και κρυπτογράφησης της εικόνας. Μεταφορά δεδομένων από και προς την κοινόχρηστη SRAM

8. Μετρήσεις-Αποτελέσματα

Στο τρέχον κεφάλαιο παραθέτουμε τις μετρήσεις και τα σχετικά αποτελέσματα απόδοσης και αξιολόγησης των αλγορίθμων κρυπτογράφησης και επεξεργασίας εικόνας που χρησιμοποιήσαμε για την υλοποίηση της εργασίας. Αρχικά συγκρίναμε τον χρόνο κρυπτογράφησης και αποκρυπτογράφησης των τεσσάρων αλγόριθμων, έπειτα εξάγαμε το συνολικό χρόνο εκτέλεσης του κάθε αλγορίθμου σε σχέση με τις διαδικασίες της εφαρμογής μας. Ο χρόνος εκτέλεσης μετριέται με βάση τη συχνότητα των 100Mhz του ρολογιού του Microblaze επεξεργαστή μας. **Δηλαδή η περίοδος T=1/F ενός κύκλου ρολογιού μετριέται στα 10ns.**

8.1 Σύγκριση αλγορίθμων (TEA, Present, Blowfish, AES)

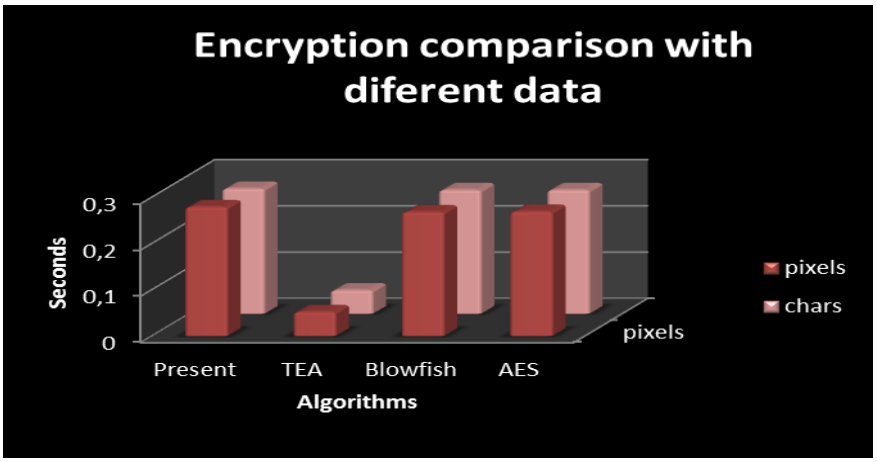
Επιλέξαμε τέσσερεις αλγορίθμους για να συγκρίνουμε και να πραγματοποιήσουμε την κρυπτογράφηση της εικόνας, τον TEA, τον Present, τον Blowfish και τον AES. Τα χαρακτηριστικά των οποίων εξηγήσαμε στο κεφάλαιο 3.

8.1.1Διαδικασία κρυπτογράφησης

Αρχικά ξεκινήσαμε με τη διαδικασία της κρυπτογράφησης για την εικόνα 256x256 και μετρήσαμε για κάθε αλγόριθμο τον χρόνο εκτέλεσης του. (Πίνακας 1). Στη συνέχεια πραγματοποιήσαμε την ίδια διαδικασία αλλά αυτή τη φορά έχοντας δεδομένα εισόδου 255x255 χαρακτήρες. Είναι χαρακτηριστικό όπως βλέπουμε και στο σχετικό γράφημα (Γράφημα 1) πως η διαδικασία της κρυπτογράφησης έχει κατά πολύ, μικρότερο χρόνο στον αλγόριθμο TEA.

Κρυπτογράφηση		
	seconds	
	pixels	chars
Present	0,279	0,271
TEA	5,21E-02	5,12E-02
Blowfish	0,268	0,268
AES	0,269	0,268

Πίνακας 1: Χρόνος κρυπτογράφησης ανά αλγόριθμο



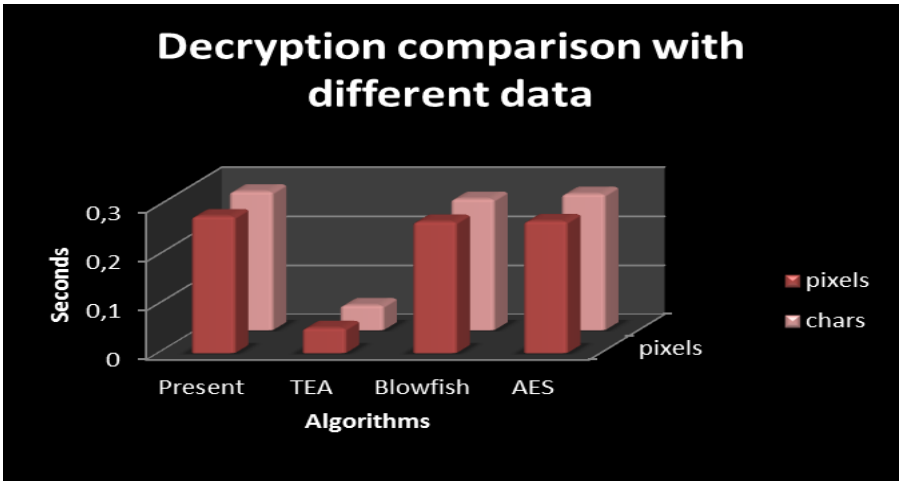
Γράφημα 1: Σύγκριση αλγορίθμων κρυπτογράφησης με a. Pixels και b. Chars

8.1.2 Διαδικασία αποκρυπτογράφησης

Στη συνέχεια κάναμε ακριβώς την ίδια διαδικασία, αλλά αυτή τη φορά για την διαδικασία αποκρυπτογράφησης των τεσσάρων αλγορίθμων. Το βασικό συμπέρασμα που προκύπτει ξανά είναι η μεγάλη διαφορά στον χρόνο εκτέλεσης των υπόλοιπων αλγορίθμων σε σύγκριση με τον TEA. **Συνολικά δεν προκύπτει κάποια ιδιαίτερη διαφοροποίηση σχετικά με την είσοδο διαφορετικών δεδομένων στους αλγορίθμους κρυπτογράφησης και αποκρυπτογράφησης**. (Πίνακας 2, Γράφημα 2)

Αποκρυπτογράφηση		
	seconds	
	pixels	chars
Present	0,279	0,283
TEA	5,12E-02	5,11E-02
Blowfish	0,268	0,268
AES	0,269	0,278

Πίνακας 2: Χρόνος αποκρυπτογράφησης ανά αλγόριθμο



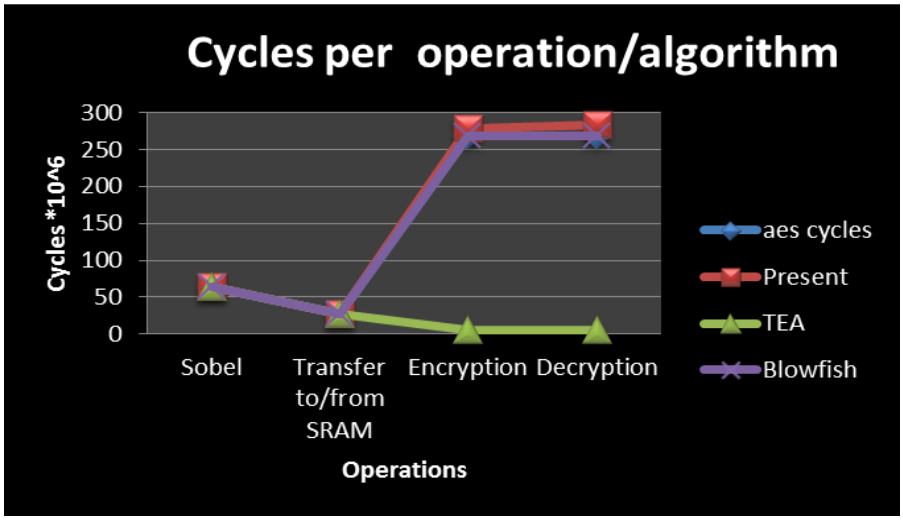
Γράφημα 2: Σύγκριση αλγορίθμων αποκρυπτογράφησης με a. Pixels και b. Chars

8.2 Χρονική επιβάρυνση ανα διαδικασία

Αφού ολοκληρώθηκαν οι παραπάνω μετρήσεις, υπολογίσαμε πιο συγκεκριμένα, τους κύκλους που απαιτούνται για κάθε μία από τις τέσσερεις βασικές διαδικασίες για την ολοκλήρωση συνολικά της εργασίας. Οι διαδικασίες αυτές είναι:

1. **Η ανίχνευση ακμών(Sobel)**
2. **Μεταφορά δεδομένων από και προς την SRAM**
3. **Κρυπτογράφηση**
4. **Αποκρυπτογράφηση**

Παρατηρώντας το Γράφημα 3**,** είναι ξεκάθαρη και πάλι η υπεροχή των διαδικασιών του TEA (κρυπτογράφηση-αποκρυπτογράφηση) έναντι των υπολοίπων αλγόριθμων. Διαπιστώνουμε επιπλέον την απαίτηση σε κύκλους ανά διαδικασία για κάθε αλγόριθμο.



Γράφημα 3: Κύκλοι ανα διαδικασία συνολικής εκτέλεσης

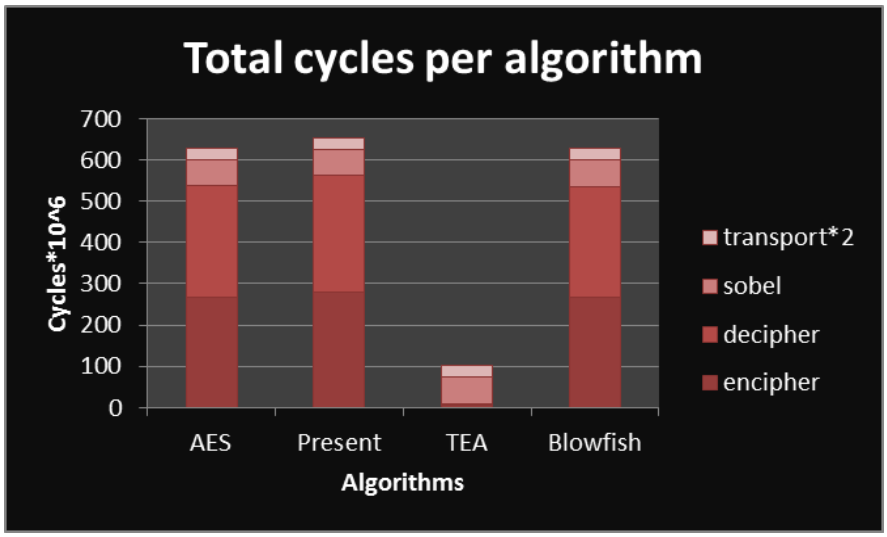
8.2.1 Συνολικό αριθμός κύκλων ανά αλγόριθμο

Τέλος με βάση την παραπάνω μέτρηση προκύπτει ο συνολικός αριθμών κύκλων ανά αλγόριθμο, από την πρόσθεση των κύκλων ανά διαδικασία που μετρήσαμε. Παρατηρούμε λοιπόν, στον Πίνακα 3, πως **ο αλγόριθμος TEA χρειάζεται μόλις 101,9*10^6 κύκλους, είναι δηλαδή σχεδόν 6 φορές πιο ταχύς από τους άλλους τρεις.** Αυτό είναι απόρροια της πολύ μικρής ανάγκης σε κύκλους της κρυπτογράφησης και αποκρυπτογράφησης του αλγορίθμους σε σύγκριση με τους υπολοίπους.

Total Cycles / Algorithm				
	AES	Present	TEA	Blowfish
encipher	268	279	5	268
decipher	269	283	5	268
sobel	63,9	63,9	63,9	63,9
transport*2	2,80E+01	28	28	28
Total(*10^6)	**628,9**	**653,9**	**101,9**	**627,9**

Πίνακας3: Συνολικοί απαιτούμενοι κύκλοι ανά αλγόριθμο

Τέλος στο Γράφημα 4 καταγράφεται ο χρόνος εκτέλεσης του κάθε αλγορίθμου που προκύπτει από την άθροιση των διαδικασιών. Τους λιγότερους κύκλους απαιτεί ο TEA και τους περισσότερους ο Present.



Γράφημα 4: Συνολικοί κύκλοι ανα διαδικασία και αλγόριθμο

9. Συμπεράσματα – Μελλοντικές Επεκτάσεις

Από την μεθοδολογία που αναπτύξαμε προκύπτουν κάποια βασικά συμπεράσματα, τόσο για τη συγκεκριμένη μεθοδολογία όσο και γενικότερα για την επιστημονική προσπάθεια γύρω από το ζήτημα της αξιοπιστίας των ενσωματωμένων συστημάτων.

Όσο αφορά τη δική μας εργασία, προκύπτουν **τέσσερα κύρια συμπεράσματα:**

1. Ο αλγόριθμος TEA εξάγει τα ίδια αποτελέσματα σε μικρότερη χρονική διάρκεια από τους Present, AES και Blowfish.

2. Τα δεδομένα που εισάγονται ως είσοδο στους αλγορίθμους κρυπτογράφησης δεν επηρεάζουν σημαντικά την συνολική λειτουργία.

3. Η επεξεργασία εικόνας που πραγματοποιείται έχει τα ίδια αποτελέσματα με εκείνα των συναρτήσεων του Matlab

4. Υλοποιείται η κρυπτογράφηση πραγματικής εφαρμογής σύντομα, με την επιλογή του κατάλληλου αλγορίθμου κρυπτογράφησης.

9.1Μελλοντικές επεκτάσεις

Πλήθος επεκτάσεων μπορούν να ελεγχτούν με βάση την μεθοδολογία που αναπτύξαμε παραπάνω:

- Σύγκριση με άλλα υποσυστήματα και μεθοδολογίας για την εξαγωγή πληρέστερων συμπερασμάτων
- Σύγκριση των αλγορίθμων με μεγαλύτερο φάσμα δεδομένων
- Δημιουργία HW Block που θα αναλάβει τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων μνήμης, υλοποιώντας των TEA.

Βιβλιογραφία

[1] Προηγμένες εφαρμογές των μαθηματικών στην ψηφιακή επεξεργασία σήματος με χρήση της Matlab, ΑΤΕΙ Κρήτης Παράρτημα Χανίων τμ. Ηλεκτρονικής, 2010

[2] Peter Mc Curry, Fearghal Morgan, Liam Kilmartin. Xilinx FPGA implementation of a pixel processor for object detection applications. In the Proc. Irish Signals and Systems Conference, Volume 3, Page(s):346 – 349, Oct. 2001.

[3] ImageProcessingAlgorithm.pdf

[4] Νικόλαος Παπαμάρκος, «Τι είναι μια ψηφιακή εικόνα», Κεφάλαιο 1, Ψηφιακή Επεξεργασία & Ανάλυση Εικόνας, ISBN 960-387-352-7, Β.Γκιούρδας Εκδοτική, σελ.2-4.

[5] Maria Petrou, Panagiota Bosdogianni, "What is an Image?". Image Processing The Fundamentals, Willy Publications 1999, σελ. 1.

[6] Ren-Junn Hwang *Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C*. «A Digital Image Copyright Protection Scheme Based on Visual Cryptography»

[7] Sangeet Saha1, Chandrajit pal2, Rourab paul3, Satyabrata Maity 4, Suman Sau5 «A brief experience on journey through hardware developments for image processing and it's applications on Cryptography» Dept of Computer Science & Engineering 1, A. K. Choudhury School of Information Technology2,3,4,5 University Of Calcutta, Kolkata, India 92, A.P.C Road,Kolkata-700009

[9] http://en.wikipedia.org/wiki/RC4

[10] Hameed A. Younis, Dr. Turki Y. Abdalla, Dr. Abdulkareem Y. Abdalla , " A Modified Technique For Image Encryption ",online access

[11] Sapna Sasidharan and Deepu Sleeba Philip , "A FAST PARTIAL IMAGE ENCRYPTION SCHEME WITH nWAVELET TRANSFORM AND RC4" , International Journal of Advances in Engineering & Technology, Sept 2011. ©IJAET ISSN: 2231-1963

[12] Matthew D. Russell. Tinyness: An Overview of TEA and Related Ciphers. Draft v0.3, February 2004

[13] J. Kelsey et al. Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X New DES, RC2, and TEA. In First International Conference on Information and Communication Security, pages 233–246, 1997.

[14] John C. Ross. Image Processing Hand book, CRC Press. 1994.

[15] ΑΘΑΝΑΣΙΑ ΚΟΛΟΒΟΥ (Ε.Τ.Ε.Π.), «Εισαγωγή στην Επεξεργασία Εικόνας ΠΑΡΑΔΕΙΓΜΑΤΑ ΜΕ ΧΡΗΣΗ MATLAB», ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ,2012

[16]ΠΑΝΑΓΙΩΤΟΥ ΙΩΑΝΝΑ, " *Προχωρημένες Εφαρμογές Επεξεργασίας Εικόνας στο MATLAB*", ΑΤΕΙ ΛΑΡΙΣΑΣ ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ, 2012

[17] Νικόλαος Χ. Αναστασιάδης, « Υλοποίηση Αλγόριθμου Ανίχνευσης Ακμών σε προγραμματιζόμενη ψηφίδα Xilinx», ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ, *Αθήνα, Ιούλιος 2009*

[18] Κολλήγα Χρυσούλα & Κακαγιάννη Μαρία «Αλγόριθμοι Επεξεργασίας Εικόνας Ανάπτυξη Λογισμικού Αναγνώρισης Προσώπου» , Καστοριά Απρίλιος 2009

[19] Νικόλαος Α. Νάννος, «ΑΝΑΠΤΥΞΗ ΕΞΕΛΙΓΜΕΝΩΝ ΑΛΓΟΡΙΘΜΩΝ ΓΙΑ ΤΗΝ ΨΗΦΙΑΚΗ ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΙ ΑΝΑΛΥΣΗ ΚΥΤΤΑΡΟΠΑΘΟΛΟΓΙΚΩΝ ΕΙΚΟΝΩΝ ΜΕ ΧΡΗΣΗ ΠΛΑΤΟΦΟΡΜΑΣ MATLAB» , Αθήνα, Οκτώβριος 2011

[20] Miller Alexander Prof. Dr.-Ing. Gunar Schorcht Professorship for Networks, IT-Security, Cryptology, University of Applied Sciences Erfurt University of Applied Sciences Erfurt Applied Computer Science Applied Computer Science « Embedded Systems Security: Performance Investigation of Various Cryptographic Techniques in Embedded Systems »

[21] Χρυσούλα Π. Σκλιά, Επέκταση περιηγητή για διαχείριση πιστοποιητικών σε τεχνολογία έξυπνων καρτών, Εθνικό Μετσόβιο Πολυτεχνείο Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών Τομέας Συστημάτων μετάδοσης πληροφορίας και τεχνολογίας υλικών,Αθήνα, Οκτώβριος 2006

[22] Vo Ky Chau and Truong Quang Vinh « EMBEDDED IMAGE PROCESSING SYSTEM ON FPGA» Deparment of Electrical and Electronic Engineering, University of Technology, Viet Nam

[23]http://www.mathworks.com/help/matlab/creating_plots/image-types.html

Παράρτημα

Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής

Κρυπτογράφηση Επεξεργασμένης Εικόνας Σε Ενσωματωμένα Συστήματα

Βαζακοπούλου Καλλιόπη – Μαρίνα
ΑΜ: 2439

Επόπτης: Κορνάρος Γεώργιος,
Καθηγητής Εφαρμογών

1

Περίγραμμα

- *Εισαγωγή*
  - *Περιγραφή Εργασίας*
  - *Αφορμή & Στόχοι*
- Εφαρμογές της Προτεινόμενης Μεθοδολογίας
- *Συναφείς Εργασίες*
- *Ανάλυση Μεθοδολογίας & Συστήματος σε FPGA*
  - *Επεξεργασία Εικόνας*
    - MATLAB® vs. FPGA
  - *Κρυπτογράφηση-Αποκρυπτογράφηση*
- *Μετρήσεις-Αποτελέσματα/Συμπεράσματα*
- *Μελλοντικές Επεκτάσεις*

2

Εισαγωγή

Περιγραφή Εργασίας

- Σχεδίαση ενός συστήματος δύο επεξεργαστών microblaze
  - 1ος : επεξεργασία επιλεγμένης εικόνας με την εφαρμογή του αλγόριθμου ανίχνευσης ακμών Sobel.
  - 2ος : κρυπτογράφηση με τους αλγορίθμους TEA, Present, Blowfish και AES.
- Επαλήθευση των αποτελεσμάτων της επεξεργασμένης εικόνας με τα αντίστοιχα που εξάγει το MATLAB® για την ίδια εικόνα.
- Μετρήσεις Απόδοσης και Βελτιστοποίησης διαφορετικών κρυπταλγορίθμων.
- Υλοποίηση στο ml405 της Xilinx με FPGA Virtex4.

3

Εισαγωγή

Αφορμή & Στόχοι

- Υλοποίηση κρυπτογράφησης μιας πραγματικής εφαρμογής σε FPGA πλατφόρμα.
- Υλοποίηση και σύγκριση αλγορίθμων κρυπτογράφησης σε αναπτυξιακή πλατφόρμα με FPGA
- Επαλήθευση αποτελεσμάτων FPGA με MATLAB®.
- Αξιολόγηση κρυπτογράφησης-αποκρυπτογράφησης με διαφορετική μορφή δεδομένων

4

Εφαρμογές της Προτεινόμενης Μεθοδολογίας

- Είδη Προσωπικής Ευκολίας
  - Κινητά τηλέφωνα
  - Προσωπικοί Ψηφιακοί Βοηθοί (PDA)
- Τηλεπικοινωνίες
  - Ψηφιακά τηλεφωνικά κέντρα
  - Δικτυακός εξοπλισμός (δρομολογητές - routers, μεταγωγείς - switches, κλπ.)
- Υπολογιστές και Περιφερειακά
  - Ασύρματα δίκτυα (routers και κάρτες για Wi-Fi, κλπ.)
- Υπηρεσίες
  - Συστήματα αυτόματων τραπεζικών συναλλαγών (ATM), συναλλαγές με πιστωτικές κάρτες

5

Συναφείς Εργασίες

- Εφαρμογή του αλγορίθμου TEA σε Sensors
  - Peter Mc Curry, Fearghal Morgan, Liam Kilmartin. Xilinx FPGA implementation of a pixel processor for object detection applications.
- Επεξεργασία Εικόνας σε Ενσωματωμένο Σύστημα FPGA
  - Vo Ky Chau and Truong Quang Vinh «EMBEDDED IMAGE PROCESSING SYSTEM ON FPGA» Department of Electrical and Electronic Engineering, University of Technology, Viet Nam
- Ψηφιακή Υδατογράφηση (watermarking)
  - *Ren-Junn Hwang Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.* «A Digital Image Copyright Protection Scheme Based on Visual Cryptography»
- Ασφαλής μετάδοση εικόνας σε πολλαπλές FPGA
  - Sangeet Saha1, Chandrajit pal2, Rourab paul3, Satyabrata Maity 4, Suman Sau5 «A brief experience on journey through hardware developments for image processing and it's applications on Cryptography»

6

Ανάλυση Μεθοδολογίας & Συστήματος σε FPGA

Επεξεργασία Εικόνας(Sobel) Σύγκριση MATLAB® *με* FPGA

- Εφαρμογή του ανιχνευτή Sobel στην εικόνα *'cameraman.bmp' στο* MATLAB® με σκοπό την εύρεση ακμών μέσω.

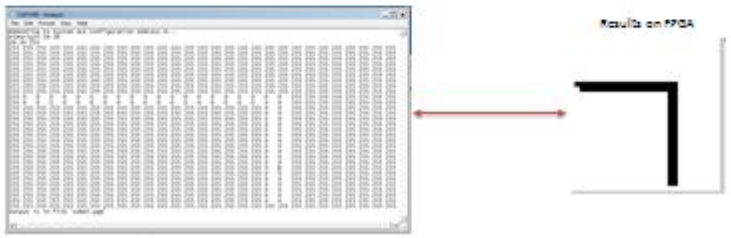
- Σύγκριση αρχικών αποτελεσμάτων εικόνας (έχει υποστεί μάσκα Sobel), από το MATLAB® με του dual core συστήματος σε FPGA.

7

MATLAB® vs. FPGA

- **MATLAB® processing**

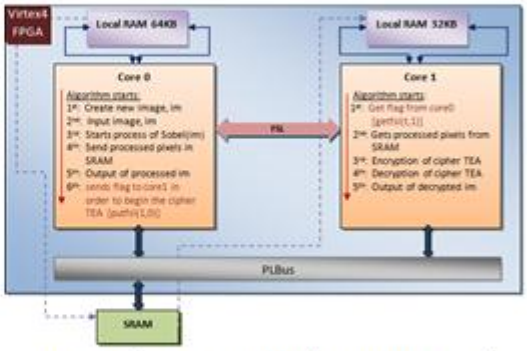
- **FPGA processing**



8

Ανάλυση Μεθοδολογίας & Συστήματος σε FPGA

- FSL: Επικοινωνία επεξεργαστών
- Core 0 : Sobel, flag = "true"
- Core 1 : flag= "true", TEA
- SRAM : Αποθήκευση επεξεργασμένων Pixels
- PLBus : Επικοινωνία επεξεργαστών με τα περιφερειακά.



Οι λειτουργίες των επεξεργαστών και η αρχιτεκτονική του υποσυστήματος

9

Ανάλυση Μεθοδολογίας & Συστήματος σε FPGA

Επεξεργασία Εικόνας- Sobel

- Δημιουργία-Εισαγωγή Εικόνας

```
IMAGE im;
    im = (IMAGE)newimage (ROWS, COLUMNS);
    im->info->oi = 256;
    im->info->oj = 256;
```

- Μεταφορά επεξεργασμένων pixels στην SRAM

```
for (i=0; i<x->info->nr; i++) {
    for (j=0; j<x->info->nc; j++){
        x->data[i][j] = z->data[i][j];
          *(dstPoint + count_sobel)= x->data[i][j] ;
          count_sobel++;
  }
}
```

- Έξοδος επεξεργασμένης εικόνας

```
for (i=0; i<ROWS; i++)
    for (j=0; j<COLUMNS; j++)
        im->data[i][j] = cameraman[i][j];
sobel (im);
Output_PBM (im, "sobel.pgm");
putfsl(1,0);
```

1ος : microblaze

Sobel

Core 0

Algorithm starts:

1st: Create new image, im
2nd: Input image, im
3rd: Starts process of Sobel(im)
4th: Send processed pixels in SRAM
5th: Output of processed im
6th: Sends flag to core1 in order to begin the cipher TEA (putfsl(1,0))

10

Ανάλυση Μεθοδολογίας & Συστήματος σε FPGA

Κρυπτογράφηση Επεξεργασμένης Εικόνας- TEA

- Εκκίνηση του TEA

```
getfsl(t,1);
```

- Εξαγωγή των επεξεργασμένων pixels από την SRAM

```
for(t=0 ; t<65536 ;t++){
    in[t] = *(dstPoint + t) ;
}
```

- Εισαγωγή ανα 2 pixel της επεξεργασμένης εικόνας –είσοδος του αλγορίθμου κρυπτογράφησης

```
...
for(j=0;j<32768;j++){
    in_trans[0]=in[j];
    in_trans[1]=in[++j];
...
```

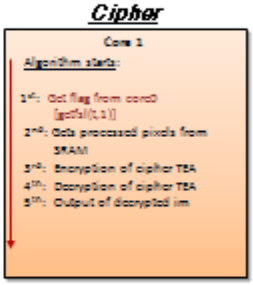
- Συναρτήσεις Κρυπτογράφησης/ Αποκρυπτογράφησης

```
xtea_encipher ( in_trans,  out,  key);

xtea_decipher ( in_trans,  out,  key);
```

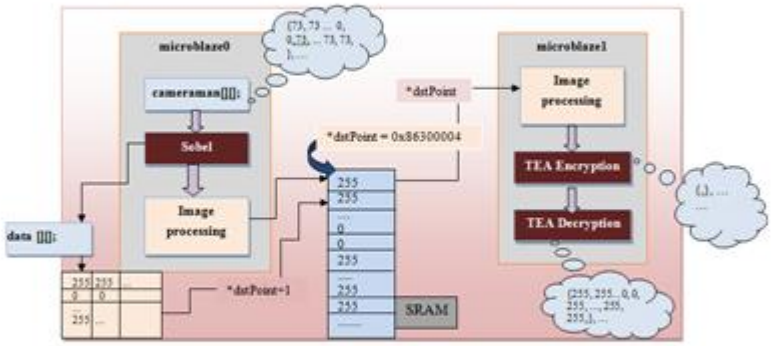
2ος : microblaze

Cipher



11

Ανάλυση Μεθοδολογίας & Συστήματος σε FPGA



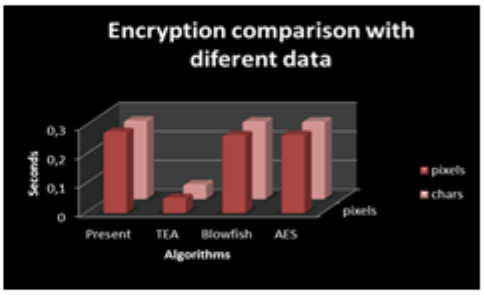
Εκτελούμενες Διεργασίες ανά επεξεργαστή και μεταφορά επεξεργασμένης εικόνας από και προς την κοινόχρηστη SRAM μνήμη

12

Μετρήσεις-Αποτελέσματα

- Σύγκριση αλγορίθμων κρυπτογράφησης

Κρυπτογράφηση		
	seconds	
	pixels	chars
Present	0,279	0,271
TEA	5,11E-02	5,12E-02
Blowfish	0,266	0,266
AES	0,269	0,266



F=100Mhz
T=10ns

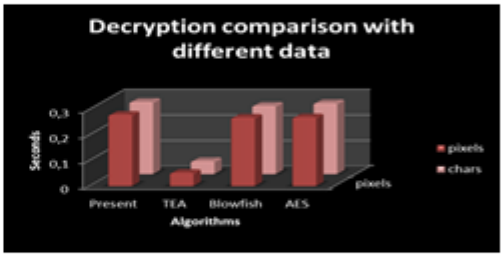
- Εμφανής η διαφορά του TEA με τους υπόλοιπους!

13

Μετρήσεις-Αποτελέσματα

- Σύγκριση αλγορίθμων αποκρυπτογράφησης

Αποκρυπτογράφηση		
	seconds	
	pixels	chars
Present	0,279	0,265
TEA	5,12E-02	5,11E-02
Blowfish	0,266	0,266
AES	0,269	0,276



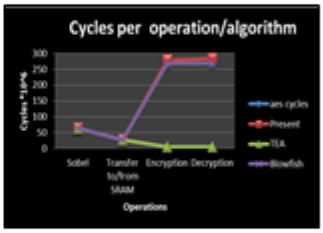
- Είτε με δεδομένα εισόδου pixels, είτε με chars, παρόμοια αποτελέσματα!

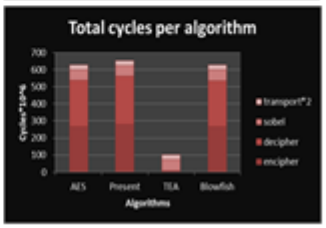
14

Μετρήσεις-Αποτελέσματα

- Απαιτούμενοι κύκλοι για κάθε διαδικασία

Total Cycles / Algorithm				
	AES	Present	TEA	Blowfish
encipher	265	279	5	265
decipher	269	283	5	265
sobel	65,9	65,9	65,9	65,9
transport*2	2,80E+01	28	28	28
Total(*10^6)	628,9	653,9	101,9	627,9





- **Ο TEA είναι σχεδόν 6 φορές πιο ταχύς από τους Present, AES και Blowfish!**

15

Συμπεράσματα

- Ο αλγόριθμος TEA εξάγει τα ίδια αποτελέσματα σε μικρότερη χρονική διάρκεια από τους Present, AES και Blowfish.
- Τα δεδομένα που εισάγονται ως είσοδο στους αλγορίθμους κρυπτογράφησης δεν επηρεάζουν σημαντικά την συνολική λειτουργία.
- Η επεξεργασία εικόνας που πραγματοποιείται έχει τα ίδια αποτελέσματα με εκείνα των συναρτήσεων του MATLAB®
- Υλοποιείται η κρυπτογράφηση πραγματικής εφαρμογής σύντομα, με την επιλογή του κατάλληλου αλγορίθμου κρυπτογράφησης.

16

Μελλοντικές επεκτάσεις

- Σύγκριση με άλλα υποσυστήματα και μεθοδολογίες για την εξαγωγή πληρέστερων συμπερασμάτων
- Σύγκριση των αλγορίθμων με μεγαλύτερο φάσμα δεδομένων
- Δημιουργία HW Block που θα αναλάβει τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων μνήμης, υλοποιώντας των TEA

17

Ευχαριστώ πολύ! ☺

18