

Πανεπιστήμιο Θεσσαλίας

Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών Τηλεπικοινωνιών και δικτύων



Διπλωματική Εργασία

Ταυτοποίηση Χρήστη μέσω Ίριδας
Οφθαλμού σε Πραγματικό Χρόνο

Φοιτητής: Θεοχάρης Σπέντζας
Επιβλέπων: Ιωάννης Κατσαβούνιδης

Βόλος 2011

Πανεπιστήμιο Θεσσαλίας

Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών Τηλεπικοινωνιών και Δικτύων

Διπλωματική Εργασία

Ταυτοποίηση χρήστη μέσω ίριδας οφθαλμού σε πραγματικό χρόνο

Εξεταστική Επιτροπή

Επιβλέπων: Ιωάννης Κατσαβουνίδης

Μέλος: Νικόλαος Μπέλλας

Βόλος 2011

Ευχαριστίες

Η παρούσα διπλωματική εργασία με τίτλο «Ταυτοποίηση χρήστη μέσω ίριδας οφθαλμού σε πραγματικό χρόνο» αποτελεί την ολοκλήρωση των σπουδών μου στο τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών Τηλεπικοινωνιών και Δικτύων του Πανεπιστημίου Θεσσαλίας. Η τελική διαμόρφωση της εργασίας είναι αποτέλεσμα εκτενούς αναζήτησης και έρευνας καθώς και προϊόν υποστήριξης και καθοδήγησης συγκεκριμένων ανθρώπων τους οποίους θα ήθελα σε αυτό το σημείο να ευχαριστήσω θερμά.

Αρχικά θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας, κ. Κατσαβουνίδα Ιωάννη, για την εμπιστοσύνη που μου έδειξε κατά την επιλογή του θέματος, τις πολύτιμες συμβουλές και τις ουσιαστικές παρατηρήσεις για την ολοκλήρωση της εργασίας. Η αρωγή του στην επίβλεψη και διόρθωση της διπλωματικής μου και η υπομονή του ήταν ιδιαίτερα πολύτιμη. Ευχαριστίες, όμως, οφείλω σε όλους του καθηγητές του ΤΜΗΥΤΔ οι γνώσεις, οι συμβουλές και οι παρατηρήσεις των οποίων συνέβαλαν στη λήψη του πτυχίου μου και αποτελούν σημαντικό εφόδιο ζωής.

Δεν μπορώ να παραλείψω να ευχαριστήσω τους φίλους και συμφοιτητές μου για την υποστήριξη τους και τη συνεχή ενθάρρυνση που μου επέδειξαν καθώς και για τα πέντε υπέροχα φοιτητικά χρόνια που μου χάρισαν. Ιδιαίτερα ευχαριστώ τους πολύ καλούς μου φίλους Τζεβελεκίδη Κωνσταντίνο και Μιχαήλογλου Αικατερίνη για την υποστήριξη τους σε κάθε μου βήμα και τις επισημάνσεις τους στην εξέλιξη της διπλωματικής μου εργασίας.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου, για την αμέριστη υποστήριξη και αγάπη που μου επέδειξαν κατά τη διάρκεια των σπουδών μου η οποία αποτέλεσε ισχυρό κίνητρο για την επιτυχή ολοκλήρωσή τους.

Όσο αναφορά το εξώφυλλο της διπλωματικής μου θα ήθελα να ευχαριστήσω τους Κατερίνα Μιχαήλογλου, Ιωάννης Ευθυμιάδης, Δημήτριος Ευθυμιάδης, Κωνσταντίνος Τζεβελεκίδης, Χρήστος Καργίδης, Μαρία Χαραλαμπόγλου και Μαρία Οικονομίδου.

Θεοχάρης Σπέντζας

Βόλος 2011

Περίληψη

Η ταυτοποίηση χρήστη αποτελεί σημαντικό τμήμα στην επιστήμη των υπολογιστών και κυρίως στο τομέα της ασφάλειας των πληροφοριακών συστημάτων. Μια πολύπλοκη μέθοδος αναγνώρισης είναι αυτή που πραγματοποιείται μέσω της ίριδας του οφθαλμού. Σκοπός της παρούσας διπλωματικής είναι η υλοποίηση ενός συστήματος αναγνώρισης ταυτότητας χρήστη μέσω φωτογραφικής μηχανής στην πλατφόρμα IOS. Η εφαρμογή είτε θα λαμβάνει έτοιμες φωτογραφίες είτε θα αποθανατίζει καινούργιες με μοναδικό σκοπό την εξαγωγή και αποθήκευση μιας ξεχωριστής πληροφορίας που θα είναι σε θέση να ξεχωρίζει και να ταυτοποιεί τον χρήστη που διακρίνεται στην φωτογραφία. Υλοποιήθηκε με ελάχιστες βελτιστοποιήσεις και παραλλαγές σε γλώσσα προγραμματισμού C ο αλγόριθμος που επινόησε ο Dr. John Daugman και ενσωματώθηκε σε μία εφαρμογή objective - C που «τρέχει» σε οποιαδήποτε έκδοση κινητού Iphone.

Abstract

The user authentication is an important part in computer science and especially in security of information systems. A complex system of identification is done through the iris of the eye. The objective of my thesis is to implement an identification system id via camera in platform IOS. The application will either take existing pictures or new captures with only purpose saving unique information, in order to be able to distinguish and identify the user, who is visible in the photograph. Implemented with minimal optimizations and variations in C language the algorithm, which was invented by Dr. John Daugman and incorporated in an application in objective - C which "runs" on any mobile version of Iphone.

Περιεχόμενα

ΜΕΡΟΣ Α ΘΕΩΡΗΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ	8
1. ΑΝΑΓΝΩΡΙΣΗ ΧΡΗΣΤΗ	8
<i>Something You Know - SYK</i>	9
<i>Something you Have -SYH</i>	9
<i>Something you Are - SYA</i>	10
2. ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΙΚΕΣ ΑΝΑΓΝΩΡΙΣΗΣ	11
<i>Παράγοντες αξιολόγησης</i>	12
<i>Σημαντικότερες Βιομετρικές Τεχνικές</i>	13
Δακτυλικά αποτυπώματα (fingerprints)	13
Αναγνώριση προσώπου (facial recognition)	14
Γεωμετρία του χεριού (hand geometry),	14
Χροιά της φωνής	14
Ανάλυση γενετικού υλικού (DNA analysis)	15
3. ΑΝΑΓΝΩΡΙΣΗ ΙΡΙΔΑΣ	16
<i>Ανατομία Οφθαλμού</i>	16
<i>Πλεονεκτήματα της αναγνώρισης της ίριδας</i>	17
<i>Μειονεκτήματα</i>	17
<i>Ιστορική Προσέγγιση</i>	17
<i>Εφαρμογή της μεθόδου</i>	17
ΜΕΡΟΣ Β ΥΛΟΠΟΙΗΣΗ	18
ΕΙΣΑΓΩΓΗ	18
4. ΑΠΟΚΤΗΣΗ ΦΩΤΟΓΡΑΦΙΑΣ	19
<i>Προϋποθέσεις</i>	19
5. ΤΜΗΜΑΤΟΠΟΙΗΣΗ	20
<i>Coarse to Fine Strategy</i>	20
6. ΚΑΝΟΝΙΚΟΠΟΙΗΣΗ	22
<i>Από καρτεσιανές σε Πολικές</i>	22
<i>Rubber Sheet Model</i>	22
<i>Σχηματική Αναπαράσταση Μοντέλου</i>	22
<i>Πλεονεκτήματα Rubber Sheet Model</i>	22
<i>Μειονεκτήματα Rubber Sheet Model</i>	23
<i>Παράμετροι και Ακρίβεια Κανονικοποίησης</i>	24
<i>Παράμετροι Κανονικοποίησης</i>	24
<i>Ακρίβεια Κανονικοποίησης</i>	24
7. ΕΞΑΓΩΓΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ	26
<i>Από το Χρόνο στη Συχνότητα</i>	26
<i>Μετασχηματισμός Φουριέ</i>	26
<i>Από το Φουριέ στα Κυματίδια</i>	26
<i>Κυματίδια (Wavelets)</i>	27
<i>Μετασχηματισμός Gabor 2D</i>	27
<i>Παράμετροι του φίλτρου</i>	28
<i>Dc Component</i>	28
<i>Log Gabor φίλτρα</i>	29
<i>Αποδιαμόρφωση</i>	30
8. ΑΠΟΘΗΚΕΥΣΗ ΚΑΙ ΣΥΓΚΡΙΣΗ	32
<i>Αποθήκευση</i>	32

<i>Σύγκριση</i>	32
<i>Ολίσθηση Bits</i>	33
9. ΠΕΡΙΛΗΨΗ ΕΠΙΔΟΣΕΩΝ ΤΑΧΥΤΗΤΑΣ	34
<i>Απόκτηση Εικόνας</i>	34
<i>Τμηματοποίηση</i>	34
<i>Κανονικοποίηση</i>	34
<i>Εξαγωγή Χαρακτηριστικών</i>	34
<i>Σύγκριση Δεδομένων</i>	35
<i>Βελτιστοποίηση Ταχύτητας</i>	35
10. ΓΡΑΦΙΚΟ ΠΕΡΙΒΑΛΛΟΝ ΤΗΣ ΕΦΑΡΜΟΓΗΣ (GUI)	36
11. ΑΠΟΤΕΛΕΣΜΑΤΑ	42
<i>CASIA Iris Image Database</i>	42
<i>Πραγματικές Φωτογραφίες Iphone</i>	42
12. ΜΕΛΛΟΝΤΙΚΕΣ ΒΕΛΤΙΩΣΕΙΣ	43
ΠΗΓΕΣ	44

Μέρος Α Θεωρητική Προσέγγιση

1. Αναγνώριση χρήστη

Η έννοια της αναγνώρισης ορίζει την επιβεβαίωση της γνησιότητας ή εγκυρότητας ενός πράγματος ή αλλιώς τη διαπίστωση της ταυτότητας ενός προσώπου ή πράγματος που κάποιος είχε γνωρίσει παλαιότερα (www.greek-language.gr).

Σε όλα τα υπολογιστικά συστήματα είναι αναγκαία η αναγνώριση των χρηστών. Η ταυτότητα του χρήστη είναι μια βασική παράμετρος για τη λήψη αποφάσεων ελέγχου προσπέλασης. Υπάρχει συχνά ανάγκη για έλεγχο πρόσβασης σε υπολογιστές, κινητά, προστατευόμενα κτήρια και περιοχές, τραπεζικά τερματικά κ.α. Έχουν δημιουργηθεί όλα αυτά τα χρόνια διάφοροι τρόποι αυθεντικοποίησης χρήστη.

Αυθεντικοποίηση ονομάζεται η δυνατότητα να καταλαβαίνει ένας εξυπηρετητής πως ο χρήστης είναι αυτός που δηλώνει ότι είναι, στην περίπτωση που η πρόσβαση σε έναν κατάλογο επιτρέπεται σε χρήστες που κατέχουν την αντίστοιχη συγκεκριμένη άδεια (Σίτας, 2002).

Για την ασφάλεια, λοιπόν, ενός συστήματος απαιτείται η εξακρίβωση των χρηστών η οποία ακολουθεί δύο στάδια, το στάδιο της ταυτοποίησης, δηλαδή της διαδικασίας αναγνώρισης της ταυτότητας του χρήστη και το στάδιο της αυθεντικοποίησης, δηλαδή της διαδικασίας επαλήθευσης της ταυτότητας του.

Άλλωστε όπως είναι γνωστό, η πρώτη γραμμή άμυνας ενός οποιουδήποτε υπολογιστικού συστήματος είναι το σύστημα εξακρίβωσης ταυτότητας χρηστών που χρησιμοποιεί και συνήθως η γραμμή αυτή άμυνας είναι και η πιο ισχυρή. Από το γεγονός αυτό γίνεται εύκολα κατανοητή η μεγάλη σημασία του ρόλου της αναγνώρισης και αυθεντικοποίησης των χρηστών σε κάθε υπολογιστικό σύστημα.

Συγκεκριμένα, η αναγνώριση της ταυτότητας ενός ατόμου – χρήστη μπορεί να επιτευχθεί με πολλές μεθόδους. Κατά καιρούς αλλά και με την εξέλιξη της τεχνολογίας έχουν χρησιμοποιηθεί, άλλοτε περισσότερο άλλοτε λιγότερο, ορισμένες από τις παρακάτω μεθόδους:

- Το όνομα
- Η εμφάνιση, δηλαδή το ύψος, το βάρος, το φύλο, η όψη.
- Κάποιος κωδικός, όπως, π.χ., ένας αριθμός μητρώου.
- Η κατοχή κάποιου αντικειμένου.
- Η βιοδυναμική, δηλαδή πώς εκτελεί κάτι το άτομο.
- Ξένα επιβληθέντα χαρακτηριστικά, όπως, π.χ. ταυτότητες, βραχιόλια, κτλ (Κάτσικας, 2001).

Ωστόσο, ο συντριπτικά πιο διαδεδομένος τρόπος ταυτοποίησης ατόμων από υπολογιστικά συστήματα είναι με τη χρήση κάποιου κωδικού, που συνήθως αναφέρεται ως όνομα χρήστη (username).

Όμοια, η αυθεντικοποίηση ενός ατόμου – χρήστη σε ένα σύστημα ασφαλείας μπορεί να επιτευχθεί με ορισμένες μεθόδους όπως :

- Γνώση μιας πληροφορίας (“Something You Know”).
- Φυσική κατοχή ενός αντικειμένου (“Something You Have”).
- Φυσικά χαρακτηριστικά (“Something You Are”).

Παράλληλα, έχει αναπτυχθεί και η Network-Based Authentication (αυθεντικοποίηση βασισμένη στα δίκτυα), η οποία επιτυγχάνεται μέσω :

- Ταυτοποίησης ενός Η/Υ στο Internet βάσει της IP διεύθυνσης (IP-based authentication) και
- Ταυτοποίησης ενός Η/Υ στο Internet βάσει του ονόματος DNS του Η/Υ (name-based authentication) (Μάγκος, 2007).

Στη συνέχεια αναλύονται οι πρώτες τρεις μέθοδοι αυθεντικοποίησης καθώς αυτές είναι που αφορούν αποκλειστικά στην εξακρίβωση των χρηστών.

Something You Know - SYK

Η ταυτοποίηση SYK (*Something You Know - SYK*) προϋποθέτει την απομνημόνευση από το χρήστη μιας μυστικής πληροφορίας, και συνήθως σχετίζεται με έννοιες και τεχνικές όπως:

1. Στατικοί κωδικοί (δηλαδή κωδικοί που δεν αλλάζουν ή που αλλάζουν σπάνια): Passwords, PINs, κλπ.
2. Τεχνικές Πρόκλησης – Απάντησης (challenge-response)
3. Κωδικοί μιας χρήσης (one-time passwords)
4. Χρήση συστημάτων ψηφιακής υπογραφής

Σε αυτό το σημείο καλό είναι να δοθεί ο ορισμός του κωδικού πρόσβασης (ή συνθηματικού), ο οποίος είναι απαραίτητος στη διαδικασία εξακρίβωσης ενός χρήστη. Έτσι, ως κωδικός πρόσβασης ορίζεται η μυστική συμβολοσειρά που χρησιμοποιείται για τον έλεγχο της αυθεντικότητας του χρήστη.

Τα βασικότερα πλεονεκτήματα της μεθόδου αυτής είναι η εύκολη υλοποίηση και εφαρμογή, η παροχή δυνατότητας τροποποίησης, η μικρή πιθανότητα κλοπής ή απώλειας αφού αποτελούν επίκτητα δεδομένα και παροχή ασφάλειας μέσω του συνδυασμού διαφορών συμβόλων, αριθμών και γραμμάτων. Ωστόσο, η μέθοδος διακρίνεται και από ορισμένα σημαντικά μειονεκτήματα με βασικότερο εκείνο της αντιγραφής και της παραβίασης με αυτοπονημένες μεθόδους (Καμπουράκη, 2011).

Something you Have –SYH

Η ταυτοποίηση με τη φυσική κατοχή ενός αντικειμένου (*Something you Have –SYH*) αποτελεί ίσως τον απλούστερο και λιγότερο ασφαλή τύπο ταυτοποίησης, για αυτό συχνά συνδυάζεται με κάποιον από τους άλλους δύο τύπους ταυτοποίησης. Η κατοχή ενός αντικειμένου που μπορεί να κλαπεί, δανειστεί, απωλεσθεί, δε μπορεί να θεωρηθεί το πλέον αξιόπιστο κριτήριο για να πιστοποιήσει κανείς την ταυτότητα ενός υποκειμένου.

Στα πλεονεκτήματα της μεθόδου αυτής μπορεί να αναφερθεί η δυσκολία αντιγραφής καθώς κατασκευάζονται από ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα, ενώ στα σημαντικότερα

μειονεκτήματα ανήκουν το υψηλό κόστος και αυξημένη πιθανότητα απώλειας ή κλοπής (Καμπουράκη, 2011).

Something you Are - SYA

Η ταυτοποίηση με βιομετρικές μεθόδους (*Something you Are - SYA*) αφορά στους ανθρώπους και μόνον, και θα εξεταστεί ξεχωριστά στο επόμενο κεφάλαιο.

Η τελευταία αυτή μέθοδος παρέχει τη μεγαλύτερη ασφάλεια συγκριτικά με τις προαναφερθέντες, ωστόσο βασικό της μειονέκτημα αποτελεί η δυσκολία κατασκευής αξιόπιστων μηχανών αναγνώρισης με χαμηλό κόστος καθώς και ύπαρξη πιθανότητας λάθους (Καμπουράκη, 2011).

Η μέθοδος αυθεντικοποίησης που χρησιμοποιείται περισσότερο είναι η πρώτη, δηλαδή μέσω της γνώσης μια πληροφορίας (SYK), καθώς είναι αυτή που επιτυγχάνεται με το μικρότερο κόστος. Ωστόσο, ο συνδυασμός και των τριών προαναφερθέντων μεθόδων είναι αυτός που οδηγεί στη μέγιστη ασφάλεια του συστήματος και ο λόγος αποφυγής της χρήσης του είναι αφενός το αυξημένο κόστος και αφετέρου η μειωμένη λειτουργικότητα.

Στον παρακάτω πίνακα δίνονται ορισμένα παραδείγματα χρήσης των μεθόδων αυθεντικοποίησης σε συγκεκριμένους προστατευόμενους πόρους.

Πίνακας 1: Σχήματα αυθεντικοποίησης προστατευόμενων πόρων

Προστατευόμενος πόρος	Something You Know	Something You Have	Something You Are	Γεωγραφική θέση
Πλατφόρμα, Host	Όνομα χρήστη/συνθηματικό	Ιδιωτικό κλειδί, έξυπνη κάρτα	Βιομετρικό σύστημα	Αναγνωριστικό υπολογιστή ή διεύθυνση IP
Σύστημα Διαχείρισης Δικτύου	Όνομα χρήστη/συνθηματικό	Ιδιωτικό κλειδί, έξυπνη κάρτα, ψηφιακό πιστοποιητικό	Βιομετρικό σύστημα	Έλεγχος χρονικής στιγμής ή θέσης του Η/Υ από τον οποίο γίνεται η πρόσβαση
Υπηρεσία Δικτύου (FTP, Web, Telnet)	Όνομα χρήστη/συνθηματικό	Ιδιωτικό κλειδί, έξυπνη κάρτα		Διεύθυνση IP
Σύστημα Διαχείρισης Βάσεων Δεδομένων	Όνομα χρήστη/συνθηματικό			Διεύθυνση IP

Πηγή: Παπαδάκης, 2010

2. Βιομετρικές τεχνικές αναγνώρισης

Οι βιομετρικές τεχνικές αναγνώρισης αποτελούν, όπως αναφέρθηκε και παραπάνω, μία από τις πιο αξιόπιστες και ασφαλής μεθόδους αυθεντικοποίησης. Η διαδικασία της εξακρίβωσης σύμφωνα με τις τεχνικές αυτές στηρίζεται σε φυσικά χαρακτηριστικά του ανθρώπινου σώματος τα οποία λειτουργούν ως αποδεικτικά στοιχεία για την αναγνωρισιμότητα του ατόμου.

Τα βιομετρικά χαρακτηριστικά μπορούν να κατηγοριοποιηθούν σε δύο ευρεία σύνολα. Στο πρώτο σύνολο ανήκουν τα βιομετρικά εκείνα γνωρίσματα που υπακούουν στους κανόνες της φυσιολογίας, και τα οποία θεωρούνται μοναδικά για κάθε άτομο, όπως για παράδειγμα:

- τα δακτυλικά αποτυπώματα (fingerprints),
- η αναγνώριση προσώπου (facial recognition),
- η γεωμετρία του χεριού (hand geometry),
- η σάρωση του αμφιβληστροειδούς (retinal scan),
- τα αγγειακά σχέδια (vascular patterns),
- τα αποτύπωμα της παλάμης (palm print),
- η χροιά της φωνής,
- η ανάλυση γενετικού υλικού (DNA analysis) και
- η μέθοδος του Bertillon (Bertillonage),
- η αναγνώριση της ίριδας (iris recognition), που αποτελεί και το αντικείμενο μελέτης της παρούσας διπλωματικής εργασίας (Ροθώνη, 2009).

Στο δεύτερο σύνολο ανήκουν τα βιομετρικά εκείνα χαρακτηριστικά, τα οποία σχετίζονται περισσότερο με ψυχολογικούς παράγοντες, γνωστά επίσης και ως συμπεριφορικά βιομετρικά χαρακτηριστικά. Παραδείγματα συμπεριφορικών βιομετρικών χαρακτηριστικών αποτελούν :

- η υπογραφή (signature recognition),
- ο βηματισμός (gait) και
- η πληκτρολόγηση (keystroke) (Καμπουράκη, 2009).

Τα βιομετρικά συστήματα παρέχουν μεγαλύτερη επιτυχή διάγνωση της ταυτότητας κάποιου σε σχέση με άλλους μηχανισμούς, δεν απαιτούν χρήση κλειδιού, κάρτας ή άλλης συσκευής από το χρήστη και είναι εύκολα στη χρήση τους καθώς δεν απαιτούν την απομνημόνευση κάποιου συνθηματικού πρόσβασης. Επιπλέον, δεν απαιτούν διαδικασίες διαχείρισης σχετικά με την τροποποίηση στοιχείων και συνθηματικών πρόσβασης, ενώ η πιθανότητα ορθής αναγνώρισης βασίζεται σε μοναδικά χαρακτηριστικά. Τα κριτήρια είναι μόνιμα και δεν απαιτούν ανανέωση με εξαίρεση, βέβαια, εκείνα της αναγνώρισης της φωνής, της υπογραφής και της πληκτρολόγησης, τα οποία απαιτούν ανανέωση με το γήρας του χρήστη (Παπαδάκης, 2010).

Παρά τα θετικά στοιχεία της χρήσης βιομετρικών τεχνικών, τα βιομετρικά συστήματα έχουν να επιλύσουν και μια σειρά από σημαντικά μειονεκτήματα, όπως το υψηλό κόστος και αργοί χρόνοι απόκρισης. Επιπρόσθετα, πολλές φορές κάποια φυσικά χαρακτηριστικά του ατόμου όπως εκείνα του προσώπου και της φωνής αλλοιώνονται με το πέρασμα του χρόνου και δεν είναι δυνατή η εξακρίβωση των στοιχείων, με αποτέλεσμα η χρήση της μεθόδου να είναι ανεπιτυχής. Συνήθως, υπάρχει απαίτηση για μεγάλες βάσεις δεδομένων καθώς και υψηλές απαιτήσεις συντήρησης, ενώ σε ορισμένες περιπτώσεις οι διαδικασίες καταχώρισης είναι μακροσκελείς με αποτέλεσμα τη δυσαρέσκεια του χρήστη. Επιπλέον, αναπτύσσονται προβλήματα σχετικά με τις κοινωνικές αντιλήψεις των ατόμων οι οποίες οδηγούν σε αντίσταση των χρηστών, όπως η κοινωνική αντίληψη περί της συσχέτισης των δακτυλικών αποτυπωμάτων με την εγκληματική δραστηριότητα ή της επιβλαβούς χρήσης της χρησιμοποιούμενης ακτινοβολίας για τη λήψη ορισμένων χαρακτηριστικών (Παπαδάκης, 2010).

Για τη διευκόλυνση της επιλογής χρήσης της κατάλληλης βιομετρικής τεχνικής έχουν αναπτυχθεί μια σειρά από κριτηριακούς παράγοντες οι οποίοι επιτρέπουν την αξιολόγηση μέσω μιας μορφής τυποποίησης.

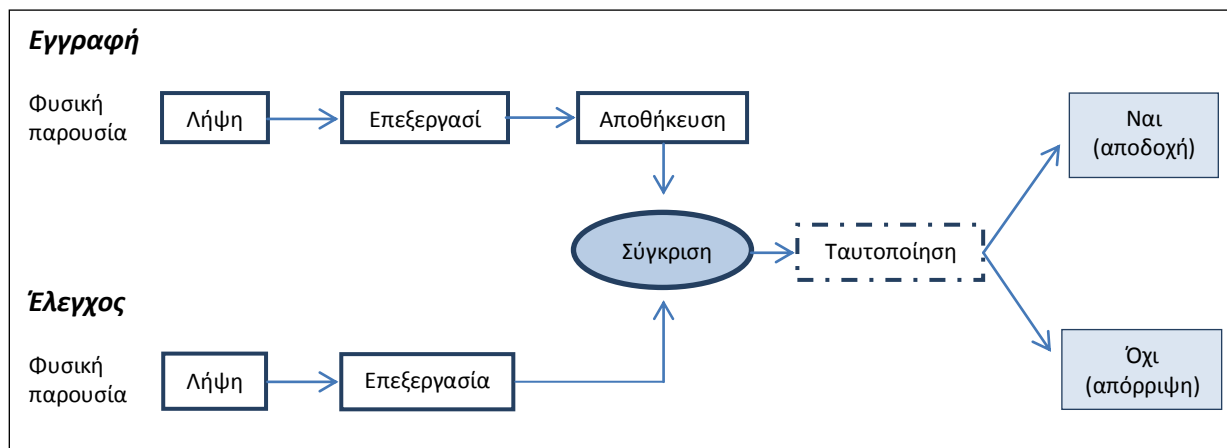
Παράγοντες αξιολόγησης

- Καθολικότητα (Universality). Εξασφαλίζει το βαθμό κατά τον οποίο όλα τα άτομα διαθέτουν το εν λόγω βιομετρικό χαρακτηριστικό.
- Μοναδικότητα (Uniqueness). Σχετίζεται με το βαθμό κατά τον οποίο, το συγκεκριμένο βιομετρικό χαρακτηριστικό είναι ικανό να διαχωρίσει ένα άτομο από τα υπόλοιπα.
- Μονιμότητα (Permanence). Σχετίζεται με το βαθμό κατά τον οποίο το εν λόγω βιομετρικό χαρακτηριστικό παραμένει αναλλοίωτο κατά τη διάρκεια της ζωής του ατόμου.
- Δυνατότητα συλλογής-λήψης του βιομετρικού χαρακτηριστικού (Collectability).
- Επίδοση μεθόδου (Performance). Η επίδοση μετράται ως προς την ακρίβεια των αποτελεσμάτων, ως προς την ταχύτητα με την οποία αυτά εξάγονται και ως προς το βαθμό, κατά τον οποίο τα αποτελέσματα είναι ανεξάρτητα από ορισμένους παράγοντες, οι οποίοι δυσχεραίνουν τη διαδικασία.
- Βαθμός Αποδοχής της μεθόδου από το χρήστη (Acceptability).
- “Παράκαμψη” (Circumvention). Μέσω της παράκαμψης περιγράφεται η ευκολία με την οποία μπορεί στην εν λόγω μέθοδο να χρησιμοποιηθεί κάποιο υποκατάστατο (Ροθώνη, 2009).

Η εξακρίβωση των χρηστών μέσω των βιομετρικών τεχνικών επιτυγχάνεται μέσω μιας διαδικασίας που καλείται βιομετρικό σύστημα. Το βιομετρικό σύστημα αποτελείται τις διαδικασίες και συσκευές εισόδου και εξαγωγής χαρακτηριστικών από το αρχικό δείγμα, έναν αποθηκευτικό χώρο (π.χ. μια Βάση Δεδομένων) και τις διαδικασίες αναγνώρισης. Οι διαδικασίες αναγνώρισης είναι δύο, η εγγραφή και ο έλεγχος. Η εγγραφή αφορά στην αποθήκευση ενός χαρακτηριστικού σε μια βάση δεδομένων, ενώ ο έλεγχος στη συσχέτιση με μια αποθηκευμένη εγγραφή. Και για τις δύο αυτές διεργασίες είναι απαραίτητη η παρουσία ενός “αισθητήρα”, ο οποίος αποτελεί τη διεπαφή μεταξύ του πραγματικού συστήματος - αναλογικού σήματος και του βιομετρικού συστήματος. Ο “αισθητήρας” λαμβάνει όλη τη “βιομετρική πληροφορία”, γεγονός που συνήθως πραγματοποιείται

μέσω μιας φωτογραφικής μηχανής ή μιας κάμερας. Στη συνέχεια επιτελείται μια διεργασία, η οποία καλείται προ-επεξεργασία και η οποία σκοπό έχει να ενισχύσει τη ληφθείσα “βιομετρική πληροφορία”. Το στάδιο της προ-επεξεργασίας συνήθως σχετίζεται με την εφαρμογή κάποιων φίλτρων με σκοπό την απομόνωση ή τη μείωση του θορύβου. Το επόμενο βήμα αφορά στην εξαγωγή των χαρακτηριστικών, τα οποία θα πρέπει να είναι ικανά να διαχωρίσουν ένα άτομο από οποιοδήποτε άλλο. Η διαδικασία ολοκληρώνεται με τη δημιουργία ενός προτύπου το οποίο θα χρησιμοποιηθεί για την τελική σύγκριση και ταυτοποίηση. Οι διαδικασίες αναγνώρισης του βιομετρικού συστήματος όπως αναλύθηκαν παραπάνω είναι εμφανείς στο διάγραμμα που ακολουθεί.

Σχήμα 1: Διαδικασίες αναγνώρισης βιομετρικού συστήματος



Κατά τη διαδικασία ταυτοποίησης είναι απαραίτητη η ύπαρξη ενός επιπέδου ανοχής καθώς ένα βιομετρικό χαρακτηριστικό δε μπορεί να είναι 100% ίδιο με το χαρακτηριστικό που είχε ληφθεί κατά την εγγραφή. Το γεγονός αυτό οφείλεται είτε σε περιβαλλοντικούς είτε σε ψυχολογικούς παράγοντες οι οποίοι διαφοροποιούν σε ένα βαθμό το βιομετρικό χαρακτηριστικό που λαμβάνεται και επηρεάζουν τη συνολική διαδικασία ταυτοποίησης. Σύμφωνα με αυτή την παραδοχή, θα ήταν πρακτικά άχρηστο να δημιουργηθεί ένα σύστημα που θα απαιτεί πλήρη (100%) ταύτιση ώστε να επιτραπεί η πρόσβαση, καθώς θα κατέληγε να απορρίπτει τους εξουσιοδοτημένους χρήστες.

Σε αυτό το σημείο κρίνεται απαραίτητη η παρουσίαση των σημαντικότερων βιομετρικών τεχνικών αναγνώρισης οι οποίες αναφέρθηκαν συνοπτικά παραπάνω, ώστε να γίνει κατανοητότερη η χρήση τους. Η τεχνική της αναγνώρισης της ίριδας θα αναπτυχθεί σε επόμενο κεφάλαιο καθώς αποτελεί και το αντικείμενο της παρούσας διπλωματικής εργασίας.

Σημαντικότερες Βιομετρικές Τεχνικές

Δακτυλικά αποτυπώματα (fingerprints)

Τα δακτυλικά αποτυπώματα είναι ίσως η πιο γνωστή και παλαιότερη μέθοδος αναγνώρισης με βιομετρικά χαρακτηριστικά, η οποία όμως δυστυχώς έχει συνδεθεί με την εγκληματικότητα. Τα κύρια πλεονεκτήματα των δακτυλικών αποτυπωμάτων είναι η μοναδικότητά τους, καθώς σε κάθε

άνθρωπο αντιστοιχεί διαφορετικό αποτύπωμα, και η δυσκολία μεταβολής τους, καθώς δεν αλλοιώνονται με το πέρασμα του χρόνου. Ένα δακτυλικό αποτύπωμα αποτελείται από ραβδώσεις, πτυχώσεις και αυλακώσεις οι οποίες σχηματίζονται στα ακροδάχτυλα. Η λήψη του αποτυπώματος γίνεται με δύο τρόπους, με χρήση μελάνης που αποτελεί την παλαιότερη μέθοδο και με σάρωση. Σήμερα, βέβαια, χρησιμοποιείται η σύγχρονη τεχνολογία όπως οπτικοί αναγνώστες, τεχνολογίες σιλικόνης και υπέρηχοι.

Αναγνώριση προσώπου (facial recognition)

Η τεχνική της αναγνώρισης του προσώπου βασίζεται στη λήψη μιας σειράς από φωτογραφίες ενός προσώπου, για κάθε μια από τις οποίες αποθηκεύεται και ένα διάνυσμα. Η σύγκριση και η ταυτοποίηση βασίζεται στα διάφορα αυτά διανύσματα, γεγονός που οδηγεί στο βασικότερο μειονέκτημα της μεθόδου αυτής καθώς το διάνυσμα που αντιστοιχεί σε κάθε φωτογραφία συνδέεται άμεσα με διάφορους παράγοντες που δυσχεραίνουν τη σωστή αναγνώριση, όπως για παράδειγμα η άμεση εξάρτηση από το φωτισμό, από τη γωνία που σχηματίζει το πρόσωπο με την κάμερα, από την απεικόνιση τυχόν συναισθημάτων στο πρόσωπο. Μια βελτίωση της παρούσας μεθόδου είναι η ανάλυση σε τρεις διαστάσεις (3D facial recognition). Με τον τρόπο αυτό, από τις δύο διαστάσεις που μας απασχολούν σε μια εικόνα, καταλήγουμε στις τρεις διαστάσεις. Αυτό επιτυγχάνεται με τη λήψη φωτογραφιών από διάφορες οπτικές γωνίες, έτσι ώστε σε κάθε σημείο του προσώπου με καρτεσιανές συντεταγμένες (x, y) να αντιστοιχεί και μία τρίτη, η οποία θα σχετίζεται με το βάθος.

Γεωμετρία του χεριού (hand geometry),

Τα άτομα στην περίπτωση αυτή καθορίζονται μέσω του σχήματος του χεριού τους. Μετριέται το μήκος της παλάμης κατά πολλές διευθύνσεις, αποθηκεύονται όλα τα αποτελέσματα και στη συνέχεια συγκρίνονται ώστε να ελεγχθεί η ταύτιση. Η μέθοδος αυτή είναι πολύ απλή υπολογιστικά, πράγμα το οποίο αποτελεί πολύ σημαντικό πλεονέκτημα, όμως μειονεκτεί ως προς ένα βασικό παράγοντα καθώς το χέρι δε χαρακτηρίζεται από ένα σύνολο τιμών, μοναδικό για τον κάθε άνθρωπο, σε αντίθεση δηλαδή με τα δακτυλικά αποτυπώματα και την ίριδα, που είναι μοναδικά για τον κάθε άνθρωπο.

Χροιά της φωνής

Τα συστήματα αναγνώρισης της χροιάς της φωνής έχουν ως στόχο την αναγνώριση του υποκειμένου που μιλάει σε αντίθεση με τα συστήματα αναγνώρισης ομιλίας που έχουν ως στόχο την αναγνώριση του περιεχομένου μιας συζήτησης. Η λήψη του φωνητικού δείγματος είναι μια απλή διαδικασία η οποία συνήθως χρησιμοποιεί ένα μικρόφωνο, συνδεδεμένο με έναν Η/Υ. Κατά την εγγραφή το σύστημα ζητάει από το χρήστη να εκφωνήσει μια ή περισσότερες λέξεις/φράσεις. Αργότερα, κατά την αναγνώριση, το σύστημα θα ζητήσει από το χρήστη να εκφωνήσει την ίδια φράση, ώστε να εξάγει το τελικό συμπέρασμα ταύτισης. Σε αντίθεση με άλλα βιολογικά χαρακτηριστικά, η φωνή ενός ανθρώπου δε «χάνεται». Η μέθοδος είναι η πλέον αποδεκτή από τους χρήστες του συστήματος, λόγω της ευκολίας και της διακριτικότητας στον τρόπο λήψης του αποτυπώματος. Επίσης η μέθοδος είναι ιδανική για απομακρυσμένη πρόσβαση όπως για παράδειγμα μέσω τηλεφώνου. Η μέθοδος εμφανίζει καλή αναλογία κόστους/απόδοσης, εφόσον δεν απαιτείται ιδιαίτερος εξοπλισμός, παρά μόνον ειδικό λογισμικό. Ωστόσο, η ακρίβεια της μεθόδου αναγνώρισης μπορεί να επηρεαστεί από εξωγενείς, όπως το θόρυβο, ή άλλους

παράγοντες όπως από τη συναισθηματική φόρτιση, την ηλικία του ομιλούντος ή ακόμα και κάποια ασθένεια.

Ανάλυση γενετικού υλικού (DNA analysis)

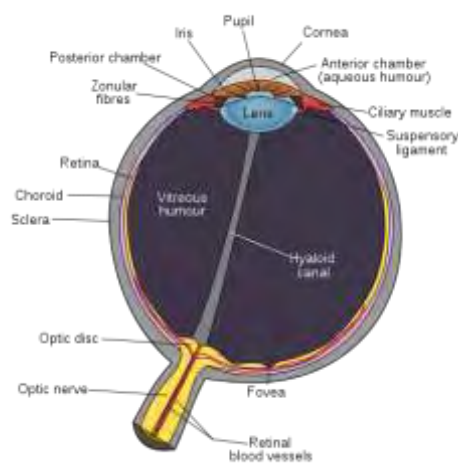
Η ανάλυση του γενετικού υλικού αποτελεί μία από τις πλέον ακριβείς μεθόδους αναγνώρισης, καθώς το γενετικό υλικό του κάθε ανθρώπου είναι μοναδικό. Η αναγνώριση μέσω του DNA απαιτεί την ύπαρξη δειγμάτων αίματος, ιστού κ.λ.π και ως εκ τούτου δεν ευνοείται η ευρεία χρήση της σε συστήματα πρόσβασης.

3. Αναγνώριση ίριδας

Ανατομία Οφθαλμού

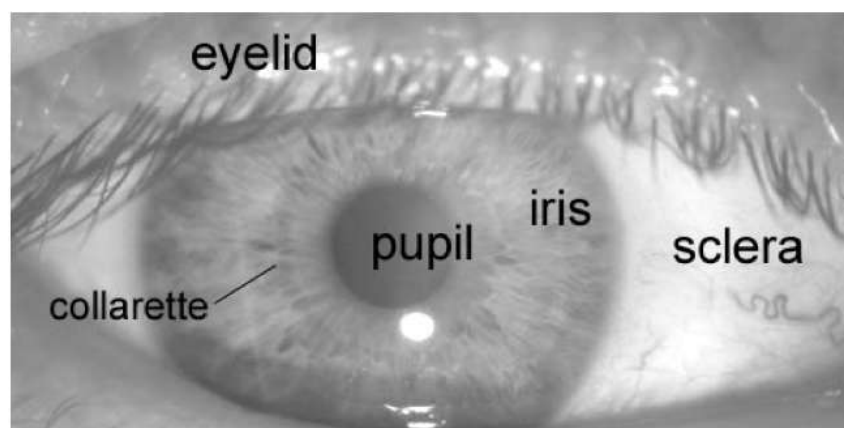
Η αναγνώριση της ίριδας αποτελεί την πλέον ακριβή και αξιόπιστη βιομετρική τεχνική για την ταυτοποίηση ενός ατόμου. «Η ίρις, κοινώς ίριδα, ονομάζεται στην ανατομία του οφθαλμού το δισκοειδές διάτρητο διάφραγμα στην πρόσθια μοίρα του οφθαλμού που βρίσκεται μεταξύ του κερατοειδή χιτώνα και του φακού και στο μέσον της οποίας βρίσκεται το άνοιγμα της κόρης. Ο ρόλος της είναι να ρυθμίζει την ποσότητα του φωτός που μπαίνει στο μάτι και φτάνει στον αμφιβληστροειδή, συστέλλόμενη όταν το φως είναι άφθονο και διαστελλόμενη όταν είναι λίγο, βοηθώντας έτσι την όραση και την αίσθηση βάθους»(www.wikipedia.org).

Εικόνα 3.1: Ανατομία Οφθαλμού



Η ίριδα του ματιού περιέχει ένα πλούσιο και πολύπλοκο μωσαϊκό γραμμών και σχημάτων, τα οποία είναι μοναδικά για κάθε άνθρωπο. Μια μπροστινή όψη του οφθαλμού διακρίνεται στην εικόνα 3.2.

Εικόνα 3.2: Μπροστινή όψη του οφθαλμού



Πλεονεκτήματα της αναγνώρισης της ίριδας

Η επιτυχία της αναγνώρισης της ίριδας βασίζεται σε αρκετούς λόγους. Όλοι σχεδόν οι άνθρωποι έχουν μάτια. Η ίριδα σταθεροποιείται και παραμένει αναλλοίωτη από τα δύο πρώτα χρόνια ζωής του ανθρώπου. Περιέχει πλούσια πληροφορία, κάτι που την καθιστά ικανή για την χρησιμοποίηση της σε ένα σύστημα αναγνώρισης ταυτότητας. Υπάρχει γενετική ανεξαρτησία καθώς δεν υπάρχουν δύο μάτια πανομοιότυπα. Η τοποθεσία της την καθιστά εύκολα προσβάσιμη καθώς μπορεί να φωτογραφηθεί από απόσταση. Η πιθανότητα να προκύψει μετά από την επεξεργασία της ίριδας ίδιο μοτίβο είναι περίπου 1 στις 10^{78} , όταν ο πληθυσμός της γης είναι περίπου 10^{10} . Το γεγονός αυτό αποδεικνύει το βασικότερο πλεονέκτημα της μεθόδου. Έρευνες έχουν δείξει ότι ο έλεγχος πρόσβασης με τη χρήση του αποτυπώματος της ίριδας εμφανίζει ποσοστά ακρίβειας μεγαλύτερα και από τις μεθόδους αναγνώρισης με DNA.

Για τη λήψη του δείγματος απαιτείται λήψη φωτογραφίας, η οποία γίνεται συνήθως με τη χρήση υπέρυθρης ακτινοβολίας από κοντινή απόσταση. Η φωτογραφία θα πρέπει να έχει υψηλή ανάλυση, ώστε να μην αλλοιωθούν τα χαρακτηριστικά της ίριδας.

Μειονεκτήματα

Ωστόσο, η μέθοδος έχει να αντιμετωπίσει και ορισμένα μειονεκτήματα, καθώς απαιτείται η λήψη φωτογραφίας από πολύ κοντινή απόσταση και σε υψηλή ανάλυση, γεγονός που συχνά θεωρείται από πολλούς χρήστες του συστήματος ενοχλητικό. Μοναδική περίπτωση αλλοίωσης της ίριδας προκύπτει από διάφορες ασθένειες που μπορούν να προσβάλλουν τον οφθαλμό, κάτι όμως που δεν μπορεί να θεωρηθεί τόσο καταστροφικό για την συνολική επιτυχία της μεθόδου.

Ιστορική Προσέγγιση

Το 1936, ο οφθαλμολόγος Frank Burch, ήταν ο πρώτος που πρότεινε την ιδέα της χρήσης προτύπων ίριδας σαν μέθοδο για αναγνώριση ανθρώπων. Το 1985 δυο οφθαλμολόγοι, ο Drs. Leonard Flom και ο Arap Safir πρότειναν ότι δύο ίριδες δεν μπορούν να είναι πανομοιότυπες και βραβεύθηκαν το 1987 για αυτή τους την διαπίστωση. Ο Dr. Flom προσέγγισε τον Dr. John Daugman για να κατασκευάσει έναν αλγόριθμο για την αναγνώριση της ίριδας. Το 1995 το σύστημα ήταν έτοιμο. Το 1994 ο Dr. Daugman κατοχύρωσε τη μέθοδο και αμέσως ξεκίνησαν να βγαίνουν στην αγορά τα πρώτα εμπορικά προϊόντα.

Εφαρμογή της μεθόδου

Η μέθοδος της αναγνώρισης της ίριδας εφαρμόζεται ως επί των πλείστων σε συστήματα που απαιτούν ύψιστη ασφάλεια όπως τα αυτόματα τραπεζικά μηχανήματα, σε τραπεζικές συναλλαγές μέσω του διαδικτύου, για πρόσβαση σε χώρους υψίστης ασφαλείας, ακόμα και σε περιπτώσεις αναγνώρισης ταξιδιωτών στα αεροδρόμια.

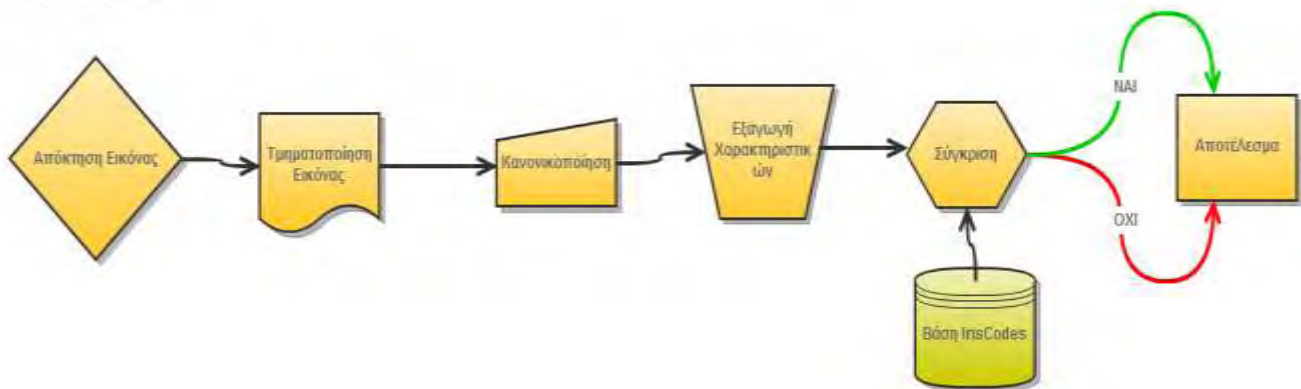
Μέρος Β Υλοποίηση

Εισαγωγή

Στην παρούσα διπλωματική υλοποιήθηκε μια εφαρμογή αναγνώρισης χρήστη μέσω της ίριδας του οφθαλμού για το smartphone Iphone. Ο αλγόριθμος που χρησιμοποιήθηκε ήταν αυτός που εμπνεύστηκε ο Dr. John Daugman το 1994. Υλοποιήθηκε εξ' ολοκλήρου σε γλώσσα προγραμματισμού C και ενσωματώθηκε στο Iphone δημιουργώντας μια εφαρμογή σε γλώσσα Objective-C.

Μια γραφική αναπαράσταση των σταδίων που χρειάζονται για να καταλήξουμε στο ταίριασμα ενός χρήστη φαίνεται στην παρακάτω εικόνα (σχεδίαση με www.glify.com).

Αναγνώριση Ίριδας



Στα παρακάτω κεφάλαια γίνεται μια περιληπτική ανάλυση όλων των βημάτων που απαιτούνται μέχρι το τελικό αποτέλεσμα.

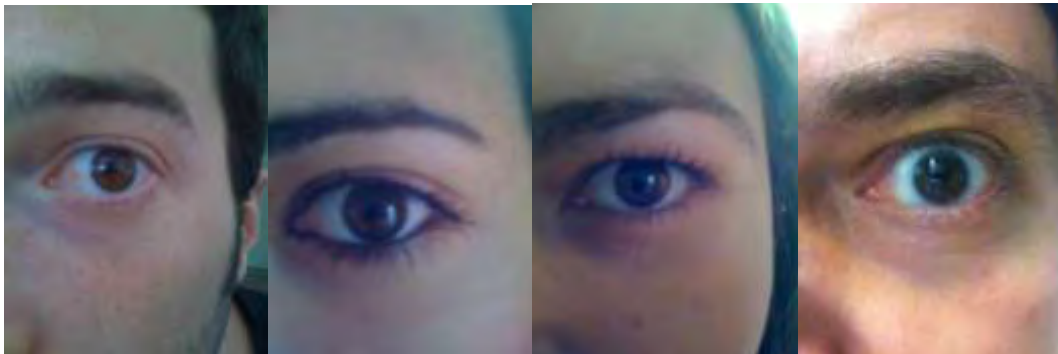
4. Απόκτηση Φωτογραφίας

Το πρώτο βήμα που απαιτείται για να ξεκινήσουμε τη διαδικασία της αναγνώρισης της ίριδας ενός ανθρώπου είναι η απόκτηση μιας φωτογραφίας του οφθαλμού του.

Προϋποθέσεις

Σύμφωνα με τον Dr. John Daugman, για να θεωρηθεί μια φωτογραφία κατάλληλη για επεξεργασία πρέπει να τηρεί δύο βασικές προϋποθέσεις, να έχει ανάλυση τουλάχιστον 640 x 480 και η ίριδα να αποτελείται περίπου από 100 έως 150 εικονοστοιχεία. Και οι δύο κάμερες που είναι εγκατεστημένες στο Iphone πληρούν την πρώτη προϋπόθεση, καθώς η μπροστινή κάμερα είναι VGA camera (0.3 Mpixels) με ανάλυση 640x480 ενώ η οπίσθια κάμερα είναι 5 Mpixels με ανάλυση 2592 x 1936. Η δεύτερη απαίτηση είναι αναγκαία έτσι ώστε να υπάρχει πλούσια πληροφορία κατά την επεξεργασία της ίριδας. Από πόσα εικονοστοιχεία θα αποτελείται η ίριδα στην φωτογραφία καθορίζεται, όπως είναι προφανές, από την εστιακή απόσταση του φακού. Βέβαια, στην δικιά μας περίπτωση αυτό δεν μπορεί να καθοριστεί εύκολα καθώς απεικονίζουμε την ίριδα από φωτογραφική μηχανή κινητού τηλεφώνου. Στην εικόνα 4.1 διακρίνουμε μερικές φωτογραφίες που χρησιμοποιήθηκαν .

Εικόνα 4.1: Δείγματα φωτογραφιών



5. Τμηματοποίηση

Αφού έχει αποκτηθεί η φωτογραφία του χρήστη που επιθυμεί είτε να αναγνωριστεί είτε να εισαχθεί στο σύστημα για μελλοντική αναγνώριση, η πρώτη επεξεργασία που πρέπει να γίνει στη φωτογραφία είναι η τμηματοποίηση και αναγνώριση της θέσης τόσο της ίριδας όσο και της κόρης.

Τόσο η ίριδα όσο και η κόρη έχουν σχήμα κυκλικό. Για να θεωρήσουμε ότι έχει εντοπιστεί η ίριδα μέσα στη φωτογραφία πρέπει να καθοριστούν τόσο οι συντεταγμένες του κέντρου του κύκλου (x,y) όσο και η ακτίνα (r) του κύκλου. Αντίστοιχα πρέπει να υπολογιστούν οι τρεις αυτές τιμές και για την κόρη. Βέβαια η θέση της κόρης δεν είναι τελείως ανεξάρτητη από αυτή της ίριδας. Το κέντρο της κόρης απέχει ελάχιστα συνήθως από εκείνο της ίριδας και με κατεύθυνση προς τη μύτη. Όσον αφορά στην ακτίνα του κύκλου της κόρης γνωρίζουμε από την ανατομία του οφθαλμού ότι θα είναι από 0.1 έως 0.8 σε σχέση με το μέγεθος της ακτίνας της ίριδας.

Η ολοκληρωδιαφορική σχέση που αναλαμβάνει τον εντοπισμό τόσο της ίριδας όσο και της κόρης φαίνεται στην εικόνα 5.1.

Εικόνα 5.1: Daugman Operator

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

Όπου:

$I(x,y)$ είναι η εικόνα εισόδου (Εικόνα 1) που περιέχει τον οφθαλμό.,

$G_\sigma(r)$ είναι μια Gaussian συνάρτηση που χρησιμοποιείται για εξομάλυνση της εικόνας με κλίμακα σ .

Η ολοκληρωδιαφορική σχέση μπορεί να θεωρηθεί ως μια κυκλική ανίχνευση ακμών που ψάχνει την μεγαλύτερη τιμή κατά μήκος της εικόνας, δοκιμάζοντας όλες τις πιθανές τιμές της ακτίνας (r) . Στην συγκεκριμένη υλοποίηση ξεκινάμε επιθυμώντας να εντοπίσουμε την ίριδα. Αφού επιλεγεί ένα πιθανό κέντρο (x_0,y_0) τότε για όλο το εύρος ακτινών που έχουμε επιλέξει, θα υπολογισθεί το παραπάνω ολοκλήρωμα. Αφού υπολογίσουμε την παράγωγο του, θα υπολογίσουμε τη συνέλιξη με το γκαουσιανό φίλτρο, και από όλες τις τιμές θα διαλέξουμε τη μέγιστη. Αυτή η τιμή θα είναι αντιπροσωπευτική για το σημείο (x_0,y_0) ως κέντρο και μια τιμή για ακτίνα r , όπου $r_{\min} < r < r_{\max}$. Αφού γίνουν όλοι οι υπολογισμοί, τότε για κάθε $\{x_0,y_0\}$ θα έχουμε μια ακτίνα και την τιμή που επέστρεψε ο τελεστής. Η μεγαλύτερη τιμή που έχει επιστρέψει ο τελεστής θα επιλεγεί και έτσι θα έχουμε στη διάθεση μας το κέντρο και την ακτίνα της ίριδας. Μιας και τα σημεία της εικόνας είναι πάρα πολλά (τουλάχιστον $307200=380*640$) το να υπολογίζουμε τον τελεστή ανά ένα εικονοστοιχείο είναι υπολογιστικά ακριβό. Για λόγους ταχύτητας χρησιμοποιούμε coarse-to fine αναζήτηση την οποία και θα επεξηγήσουμε στη συνέχεια.

Coarse to Fine Strategy

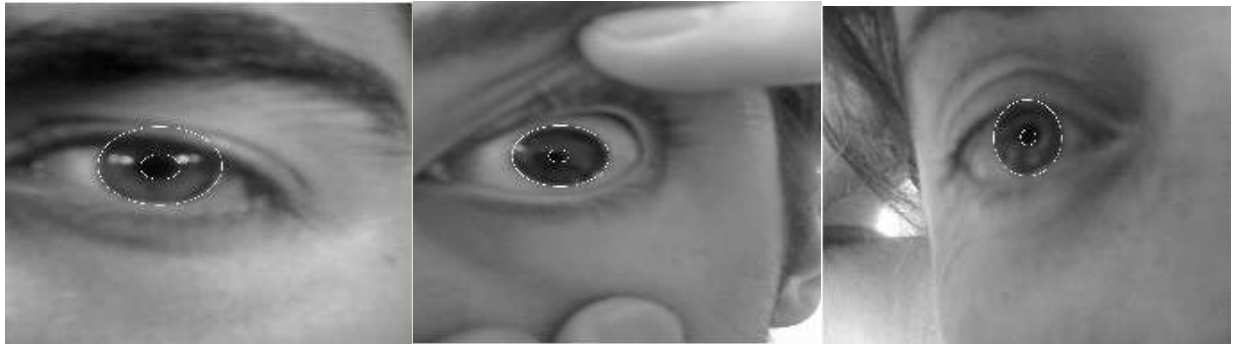
Για να αποφύγουμε πάρα πολλούς υπολογισμούς αναζητούμε τα πιθανά κέντρα ανά δεκαέξι εικονοστοιχεία. Αφού τελειώσουν όλα τα εικονοστοιχεία (μήκος x πλάτος / 16) θα έχουμε εντοπίσει ένα αρκετά κατάλληλο κέντρο. Στη συγκεκριμένη υλοποίηση για λόγους ταχύτητας κατά τη διάρκεια της coarse to fine ανάλυσης πρώτου υπολογίζουμε την σχέση ελέγχουμε την τιμή του εικονοστοιχείου. Έστω δηλαδή ότι ξεκινάμε για το πρώτο εικονοστοιχείο που βρίσκεται στη θέση

(0,0) . Σε περίπτωση που η τιμή της φωτεινότητας του είναι κάτω από τα μισά του μέσου όρου φωτεινότητας της εικόνας αποκλείεται να είναι πιθανό κέντρο ίριδας, οπότε και απορρίπτεται και δεν υπολογίζεται η ολοκληροδιαφορική σχέση για αυτό το $\{x,y\}$. Στη συνέχεια ξανά υπολογίζουμε την ολοκληροδιαφορική σχέση ανά ένα εικονοστοιχείο στα γειτονικά 10×10 εικονοστοιχεία και έχουμε έτσι καταλήξει στις τελικές τιμές τόσο για το κέντρο όσο και για την ακτίνα της ίριδας.

Εντοπισμός Κόρης

Στη συνέχεια χρειάζεται να ξανά υπολογίσουμε την ολοκληροδιαφορική σχέση για την κόρη με τη διαφορά όμως ότι το κέντρο της θα βρίσκεται μέσα σε μια γειτονιά 10×10 εικονοστοιχείων σε σχέση με το κέντρο της ίριδας. Αυτό έχει ως αποτέλεσμα να αποφύγουμε την coarse to search αναζήτηση. Επίσης γνωρίζουμε ακριβώς το εύρος ακτινών που θα αναζητήσουμε. Είναι πάντα 0.1 έως $0.8 *$ ακτίνα ίριδας. Στην εικόνα 5.1 βλέπουμε διάφορα αποτελέσματα τμηματοποίησης .

Εικόνα 5.1: Παραδείγματα Τμηματοποίησης



6. Κανονικοποίηση

Από καρτεσιανές σε Πολικές

Για την υλοποίηση ενός φερέγγυου συστήματος επιβάλλεται το τελικό αποτέλεσμα να είναι ανεξάρτητο από το μέγεθος, τη θέση και τον προσανατολισμό των προτύπων. Για να απαλλαγούμε από αυτά τα προβλήματα οποιαδήποτε φωτογραφία πριν συνεχιστεί η επεξεργασία της σε αυτό εδώ το βήμα κανονικοποιείται έτσι ώστε να απαλλαχθούμε από τυχόν διαφορές μεταξύ των φωτογραφιών. Η βασική ιδέα είναι πως τα εικονοστοιχεία (pixels) τα οποία θα χρησιμοποιηθούν, έτσι ώστε να εξαχθεί ο κώδικας της ίριδας, βρίσκονται τοποθετημένα σε τμήματα δακτυλίου, σε θέσεις δηλαδή που καθιστούν δύσκολη την επεξεργασία τους στα πλαίσια ενός καρτεσιανού συνόλου σημείων. Όπως υπάρχει αρχικά μια εικόνα ορθογώνια, στην οποία περιλαμβάνονται πλην της χρήσιμης – εικονοστοιχεία (pixels) ίριδας- πληροφορίας και άχρηστη πληροφορία, κατά τον τρόπο αυτό θα δημιουργηθεί αντίστοιχα μια νέα ορθογώνια εικόνα, στην οποία, επιπλέον, θα συμπεριλαμβάνεται μονό χρήσιμη πληροφορία. Η διαδικασία αυτή, στην οποία περιλαμβάνεται η χρήσιμη πληροφορία της αρχικής εικόνας, καλείται **ξετύλιγμα της ίριδας**. Ουσιαστικά αποτελεί **μετασχηματισμό των συντεταγμένων των σημείων** που ανήκουν στην ίριδα από καρτεσιανές σε πολικές, καθότι σε σύστημα πολικών συντεταγμένων μπορούν να παρασταθούν τα εικονοστοιχεία (pixels) που ανήκουν στην ίριδα (τμήμα δακτυλίου) χωρίς ασυνέχεια.

Το μοντέλο που προτείνει ο Daugman και ακολουθήθηκε στη συγκεκριμένη υλοποίηση είναι το Rubber Sheet Model.

Rubber Sheet Model

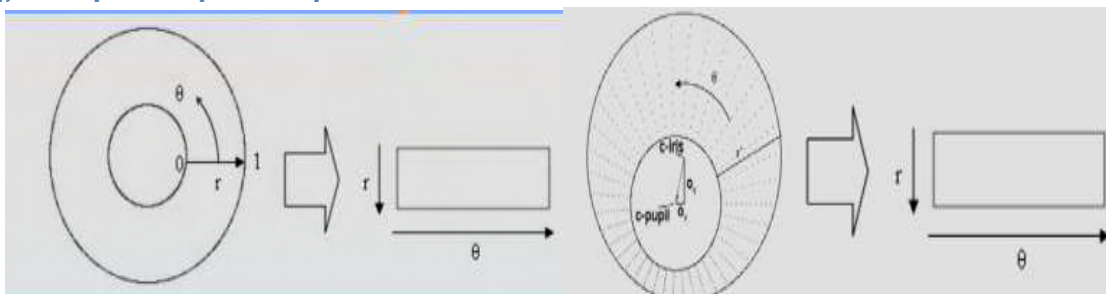
Οι εξισώσεις που περιγράφουν το μοντέλο είναι:

$$x(r,\theta) = (1-r)*x_p(\theta) + r*x_s(\theta)$$

$$y(r,\theta) = (1-r)*y_p(\theta) + r*y_s(\theta)$$

Όπου, x_p, y_p είναι το κέντρο της ίριδας και x_s, y_s το κέντρο της κόρης.

Σχηματική Αναπαράσταση Μοντέλου



Μετά το πέρας του μετασχηματισμού έχουμε «ξετυλίξει» την ίριδα και την κόρη και τις έχουμε αποθηκευμένη σε μια καινούργια εικόνα σταθερού μέγεθος.

Πλεονεκτήματα Rubber Sheet Model

Το μοντέλο αυτό καταφέρνει να εξαλείψει δύο βασικά προβλήματα – διαφορές που έχουν συχνά οι εικόνες. Τα προβλήματα αυτά σχετίζονται με τη διαστολή της ίριδας και την εστιακή απόσταση από την κάμερα (βλ. εικόνα 6.1, 6.2).

Εικόνα 6.1 : Διαστολή Ίριδας



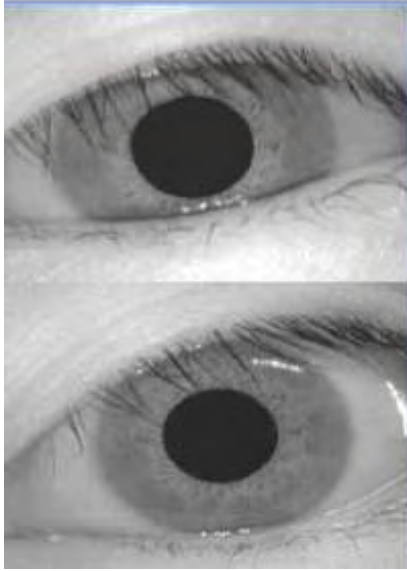
Εικόνα 6.2 : Απόσταση από την κάμερα



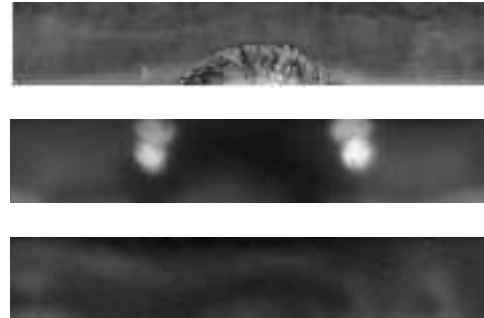
Μειονεκτήματα Rubber Sheet Model

Το μόνο πρόβλημα που αντιμετωπίζει το μοντέλο είναι οι ασυνέπειες που δημιουργούνται λόγω της περιστροφής του ματιού (βλ. εικόνα 6.3)

Εικόνα 6.3: Περιστροφή Ματιού



Εικόνα 6.4: Παραδείγματα κανονικοποίησης



Παράμετροι και Ακρίβεια Κανονικοποίησης

Παράμετροι Κανονικοποίησης

Όλες οι φωτογραφίες που θα περάσουν το στάδιο της κανονικοποίησης θα δώσουν ως αποτέλεσμα μια καινούργια εικόνα με σταθερό μήκος και πλάτος. Η τιμή τόσο του μήκους όσο και του πλάτους καθορίζεται εξ αρχής. Με βάση την σύμβαση που έχουμε το μήκος θεωρείται ότι είναι η γωνία θήτα ενώ το πλάτος είναι η ακτινική απόσταση ρ . Όσο μεγαλώνουν οι τιμές θήτα και ρ τόσο μεγαλύτερη ακρίβεια έχουμε. Όπως είναι εμφανές το θήτα δεν έχει λόγω να είναι μεγαλύτερο από 360 που είναι μία πλήρη περιστροφή, ενώ η ακτίνα ρ δεν μπορεί να ξεπεράσει την τιμή της αφαίρεσης Ακτίνα_Ίριδας μείον Ακτίνα_Κόρης. Σύμφωνα με τον Daugman θέλουμε τα σημεία που κανονικοποιούνται τόσο να ισαπέχουν μεταξύ τους όσο και η απόσταση να είναι 0.2 mm. Θεωρώντας την μέση απόσταση ίριδας - κόρης περίπου 10mm χρειαζόμαστε περίπου 64 σημεία για την ακτίνα. Όσο αναφορά την επιλογή του πλήθους των σημείων κατά την γωνιακή κατεύθυνση κάνουμε τον εξής υπολογισμό:

$2 * \pi * \rho / \text{Σημεία} = 0.2$. Περίπου 256 σημεία.

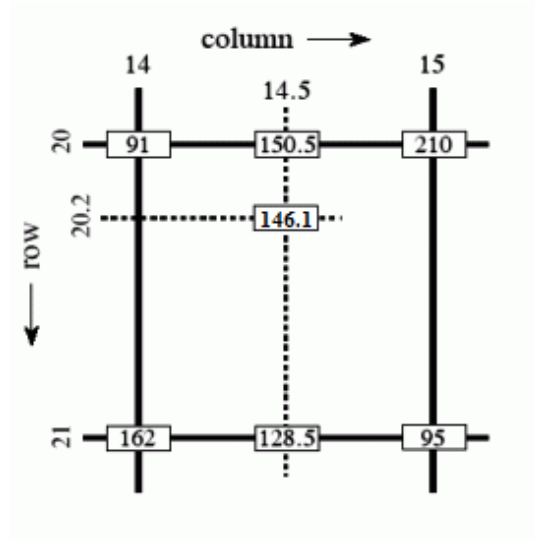
Αυτό έχει ως αποτέλεσμα κάθε κανονικοποιημένη εικόνα να έχει μέγεθος 64x256.

Ακρίβεια Κανονικοποίησης

Κατά την διάρκεια όλης της επεξεργασίας η εικόνα είναι αποθηκευμένη σε ένα δείκτη unsigned char. Στο στάδιο της κανονικοποίησης υπολογίζουμε με βάση τις εξισώσεις 6.1 και 6.2 της συντεταγμένες που θα χρησιμοποιηθούν στην καινούργια κανονικοποιημένη φωτογραφία. Λόγω της στρογγυλοποίησης που υφίσταται η εικόνα σε κάθε υπολογισμό έχει ως αποτέλεσμα να έχουμε

συνεχόμενες ίδιες τιμές. Το πρόβλημα αυτό μας αναγκάζει να μετατρέψουμε την εικόνα σε float και να χρησιμοποιήσουμε παρεμβολή. Ακόμα και η ίδια η στρογγυλοποίηση θεωρείται παρεμβολή και μάλιστα ονομάζεται κοντινότερου γείτονα (Nearest Neighbor), όπου απλά επιλέγεται το εικονοστοιχείο που είναι πιο κοντά στο ζητούμενη θέση χωρίς να λαμβάνονται υπόψη οι γειτονικές τιμές. Στη συγκεκριμένη υλοποίηση χρησιμοποιούμε διγραμμική παρεμβολή (Bilinear Interpolation), όπου χρησιμοποιούνται οι τέσσερις γειτονικές τιμές όπως διακρίνεται και στην εικόνα 6.5.

Εικόνα 6.5: Bilinear Interpolation(Wikipedia.org)



7. Εξαγωγή Χαρακτηριστικών

Σε αυτό το σημείο της επεξεργασίας έχουμε όση πληροφορία χρειαζόμαστε για να εξάγουμε για κάθε ίριδα τα χαρακτηριστικά που χρειαζόμαστε. Ο Dr. John Daugman πρότεινε τη χρήση των Gabor 2D κυματιδίων (wavelets). Πρωτού εξηγήσουμε τα κυματίδια Gabor 2D ας κάνουμε μια μικρή παρένθεση για τα κυματίδια.

Από το Χρόνο στη Συχνότητα

Η ανάλυση Fourier είναι ένα καλά εδραιωμένο αντικείμενο στην εφαρμοσμένη μαθηματική ανάλυση και μάλιστα ένα από τα παλαιότερα. Ο Joseph Fourier στα τέλη του δεκάτου εβδόμου αιώνα στην προσπάθειά του να ερευνήσει τη διάδοση της θερμότητας εφήυρε την ανάλυση Φουριέ. Η ανάλυση Φουριέ είναι ένα πεδίο των εφαρμοσμένων μαθηματικών το οποίο προέκυψε από την προσπάθεια αναπαράστασης μίας συνάρτησης ως άθροισματος απλούστερων, περιοδικών τριγωνομετρικών συναρτήσεων. Επομένως κεντρική ιδέα στην ανάλυση Φουριέ είναι η προσπάθεια για κατανόηση των ιδιοτήτων μίας συνάρτησης μέσω διάσπασής της σε γνωστά, στοιχειώδη μέρη. Η ανάλυση αυτή οδήγησε στο πασίγνωστο πλέον μετασχηματισμό Φουριέ. (www.wikipedia.org)

Μετασχηματισμός Φουριέ

Ο Μετασχηματισμός Φουριέ αναφέρεται σε μία αυστηρώς ορισμένη μαθηματική διεργασία η οποία αποσυνθέτει μία συνάρτηση σε άθροισμα απείρων περιοδικών ημιτονοειδών και συνημιτονοειδών συναρτήσεων. Το αποτέλεσμα του μετασχηματισμού είναι μία νέα συνάρτηση με διαφορετικό πεδίο ορισμού, η οποία περιγράφει το κατά πόσον συμμετέχει κάθε στοιχειώδες ημίτονο στον σχηματισμό της αρχικής συνάρτησης. Όλες οι συναρτήσεις μπορούν να εκφραστούν σε άθροισμα περιοδικών συναρτήσεων. Όταν η πληροφορία των σημάτων στο πεδίο συχνοτήτων είναι μεγάλης σημασίας σε σχέση με την πληροφορία στο χρόνο. Η χρησιμότητα τους είναι τεράστια και κυρίως στις τηλεπικοινωνίες, αστρονομία, γεωλογία, οπτική.

Ο μετασχηματισμός Fourier για ένα σήμα συνεχούς χρόνου $f(t)$ είναι:

$$\int F(\omega) = e^{-i\omega t} f(t) dt$$

Από το Φουριέ στα Κυματίδια

Το βασικότερο μειονέκτημα του μετασχηματισμού Φουριέ είναι ότι χάνεται η χρονική πληροφορία. Αν το σήμα περιέχει μή στάσιμα χαρακτηριστικά η συγκεκριμένη ανάλυση δεν μπορεί να τα εντοπίσει. Έγινε αρχικά μια προσπάθεια με τον **μετασχηματισμού Φουριέ μικρής διάρκειας** (Short Time Fourier Transform). Η μόνη διαφορά από τον απλό μετασχηματισμό Φουριέ είναι ότι ο συγκεκριμένος μετασχηματισμός όπως γίνεται αντιληπτό και από το όνομα του, το σήμα αναλύεται ένα χρονικό παράθυρο κάθε φορά. Όπως καταλαβαίνει κανείς η επιλογή του παραθύρου παίζει καθοριστικό ρόλο και μπορεί και πάλι να οδηγήσει σε απώλεια της χρονικής πληροφορίας. Βασικότερο πρόβλημα και αυτής της μεθόδου είναι ότι το μέγεθος του παραθύρου παραμένει σταθερό για όλες τις συχνότητες.

Ο μετασχηματισμός Φουριέ μικρής διάρκειας για ένα σήμα συνεχούς χρόνου $f(t)$ είναι:

$$\text{STFT} \{x(t)\} \equiv X(\tau, \omega) = \int_{-\infty}^{\infty} x(t)w(t - \tau)e^{-j\omega t} dt$$

Στα τέλη του εικοστού αιώνα ξεκίνησε για να επίλυση το πρόβλημα της απώλειας της χρονικής πληροφορίας ο μετασχηματισμός κυματιδίων.

Κυματίδια (Wavelets)

Σε συνέχεια του μετασχηματισμού Φουριέ μικρής διάρκειας κάνουμε πάλι χρήση παραθυρικής τεχνικής με περιοχές πλέον μεταβλητού μεγέθους, όπου χρησιμοποιούνται μεγάλα χρονικά παράθυρα εκεί όπου απαιτείται ακρίβεια σε πληροφορίες χαμηλής συχνότητας και μικρότερα χρονικά παράθυρα εκεί όπου απαιτείται ακρίβεια σε πληροφορίες υψηλής συχνότητας. Πλέον η ανάλυση δε χρησιμοποιεί απεικόνιση χρόνου-συχνότητας αλλά απεικόνιση χρόνου-κλίμακας. Τα πρώτα κυματίδια που χρησιμοποιήθηκαν ήταν τα Haar.

Haar wavelet

$$\psi(t) = \begin{cases} 1 & 0 \leq t < 1/2, \\ -1 & 1/2 \leq t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

scaling συνάρτηση $\phi(t)$ περιγράφεται ως εξής

$$\phi(t) = \begin{cases} 1 & 0 \leq t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

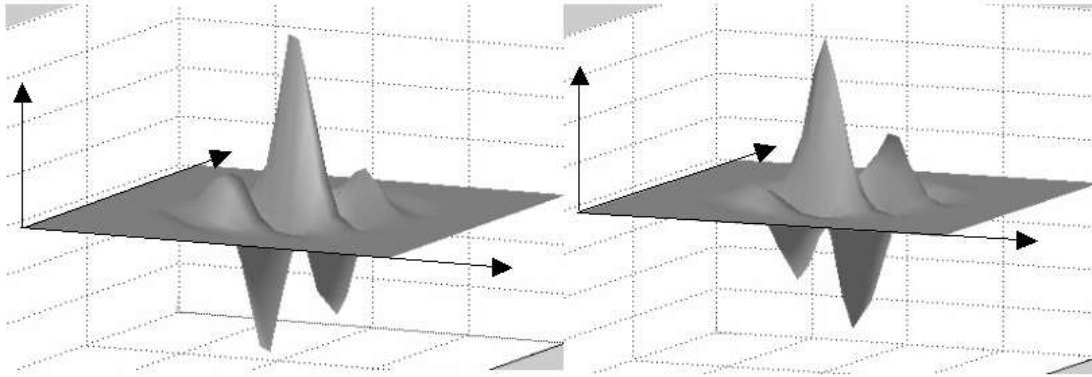
Μετασχηματισμός Gabor 2D

Τα Gabor 2D κυματίδια προτάθηκαν πρώτη φορά από τον Dr. John Daugman το 1980. Το φίλτρο Gabor 2D διαμέσου της εικόνας μπορεί να αναπαρασταθεί ως εξής

$$h_{\{Re,Im\}} = \text{sgn}_{\{Re,Im\}} \int_{\rho} \int_{\phi} I(\rho, \phi) e^{-i\omega(\theta_0 - \phi)} \cdot e^{-(r_0 - \rho)^2 / \alpha^2} e^{-(\theta_0 - \phi)^2 / \beta^2} \rho d\rho d\phi$$

όπου (ρ, ϕ) είναι η θέση μέσα στην εικόνα μιας και η εικόνα μας έχει μεταφερθεί σε πολικές συντεταγμένες, (α, β) είναι το χωρικό εύρος της Gaussian περιβάλλουσας στους άξονες x, y και (ρ_0, θ_0) οι πολικές συντεταγμένες κάθε περιοχής της ίριδας για την οποία υπολογίζεται το $h_{\{Re,Im\}}$.

Εικόνα 7.1: Άρτιο περιττό συμμετρικό Gabor 2D φίλτρο



Παράμετροι του φίλτρου

Παρατηρώντας την μαθηματική έκφραση του φίλτρου διαπιστώνουμε ότι έχει τέσσερις βαθμούς ελευθερίας, τα (α, β) , τα (ρ_0, θ_0) και τη συχνότητα ω μέγα. Σύμφωνα με τον Daugman χρειάζονται 2048 bits για το Iriscode. Μιας και στο στάδιο της αποδιαμόρφωσης φάσης κάθε μιγαδικό αποτέλεσμα του Gabor οδηγεί σε 2 bits τότε πρέπει να υπολογίζουμε 1024 συντελεστές Gabor. Επιλέγοντας κατάλληλες τιμές για το ω μέγα και για το (ρ_0, θ_0) θα προκύψουν 1024 συντελεστές. Από τη θεωρία γνωρίζουμε ότι η συχνότητα πρέπει να εκτείνεται σε 3 οκτάβες μη γραμμικά. Οποτε σίγουρα έχουμε τέσσερις τιμές για τη συχνότητα ω μέγα. Από τα 1024 μας απομένουν $1024/4 = 256$ που θα τους καθορίσουν τα (ρ_0, θ_0) . Άρα το πλήθος των ρ_0, θ_0 δεν θα πρέπει να ξεπερνά τα 256. Έχουμε επιλέξει 4 ρ_0 και 64 θ_0 . Το ρ_0 και το θ_0 μίας και η εικόνα μας έχει ήδη περάσει το στάδιο της κανονικοποίησης (64×256) θα πάρουν κανονικοποιημένες τιμές. Το ρ_0 4 τιμές από 0 έως 64 ενώ το θ_0 64 τιμές από το 0 έως το 256.

Dc Component

Παρατηρούμε ότι για συχνότητα μεγαλύτερη από μία οκτάβα το πραγματικό μέρος του φίλτρου δημιουργεί DC Component. Ως DC component θεωρούμε το μέσο όρο του κυματιδίου. Οπως είναι εμφανές και απο την εικόνα 7.1 ο μέσος όρος δεν είναι μηδέν. Για να απαλλαγούμε απο το DC υλοποιήσαμε τα Log Gabor φίλτρα που εξαλείφουν το DC component.

Log Gabor φίλτρα

Ο τύπος που περιγράφει τα Log Gabor φίλτρα φαίνεται στην εικόνα 7.2.

Εικόνα 7.2

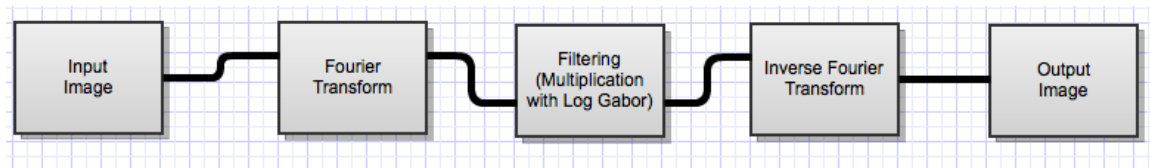
$$G(r) = e^{\frac{-(\log(r/f_0))^2}{2(\log(\sigma/f_0))^2}}$$

Όπου

- f_0 : η κεντρική συχνότητα
- σ : εύρος του φίλτρου

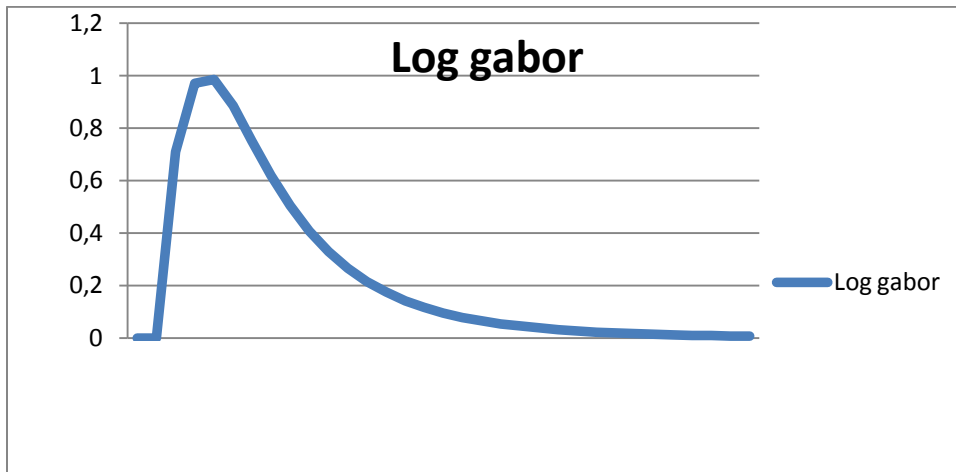
Αρχικά παρατηρούμε ότι το φίλτρο είναι στη πεδίο της συχνότητας. Αρα η εφαρμογή του στην εικόνα μας προϋποθέτει την μετατροπή της εικόνας με μετασχηματισμό Fourier στο πεδίο της συχνότητας.

Εικόνα 7.3 Εφαρμογή του μετασχηματισμού



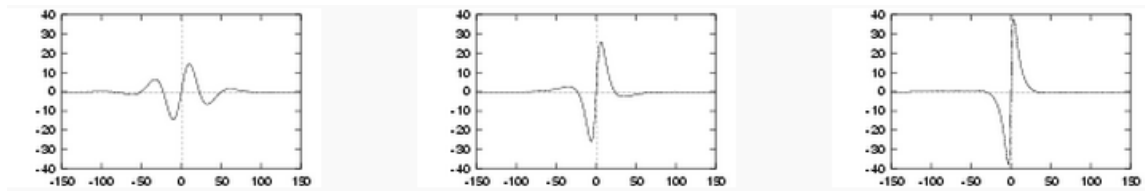
Όπως φαίνεται και στην εικόνα 7.3 αρχικά μετατρέπουμε την εικόνα στο πεδίο της συχνότητας πολλαπλασιάζουμε με τους συντελεστές του Log Gabor και εφαρμόζουμε αντίστροφο μετασχηματισμό Fourier. Η γραφική παράσταση των συντελεστών του Log Gabor φαίνονται στην εικόνα 7.4

Εικόνα 7.4



Ενώ στην εικόνα 7.5 βλέπουμε το φίλτρο με διαφορετικές συχνότητες

Εικόνα 7.5



Παρατηρούμε στην εικόνα 7.5 ότι για οποιαδήποτε συχνότητα δεν έχουμε DC component μιας και ο μέσος όρος είναι μηδέν.

Αποδιαμόρφωση

Αφού υπολογιστούν οι 1024 συντελεστές είτε του Gabor 2D είτε του Log Gabor τόσο οι πραγματικοί όσο και οι φανταστικοί αριθμοί που προκύπτουν, χρησιμοποιούμε την παρακάτω αποδιαμόρφωση φάσης έτσι ώστε να προκύψουν μόνο 2048 bit με μηδέν και ένα.

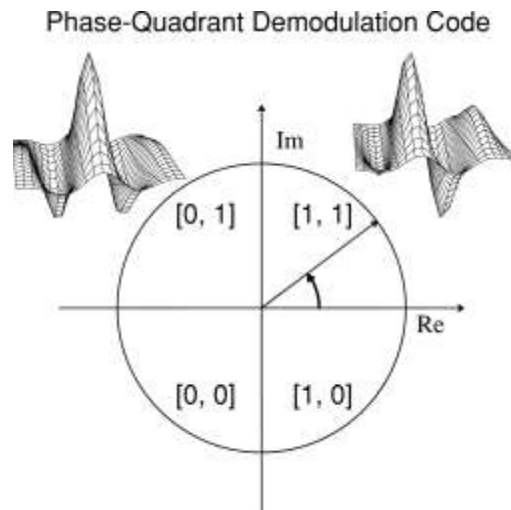
$$h_{Re} = 1 \text{ εαν } Re \geq 0$$

$$h_{Re} = 0 \text{ εαν } Re < 0$$

$$h_{Im} = 1 \text{ εαν } Im \geq 0$$

$$h_{Im} = 0 \text{ εαν } Im < 0$$

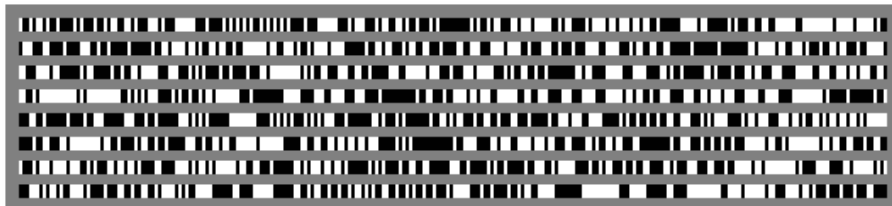
Εικόνα 7.6 Αποδιαμόρφωση Φάσης



Ο λόγος που κρατάμε μόνο την φάση και όχι το πλάτος είναι γιατί μας ενδιαφέρουν μόνο οι εναλλαγές χρώματος μέσα στην εικόνα. Ο λόγος που έχουμε δυο bits είναι γιατί μας ενδιαφέρει τόσο κατα τη κατεύθυνση της ακτίνας όσο και της γωνίας. Τα bits που προκύπτουν ονομάζονται ευρέως IrisCode και μαζί με κάποια στοιχεία για το χρήστη (πχ όνομα, επίθετο) αποθηκεύονται για μελλοντική χρήση σε βάση δεδομένων. Σε αυτά τα bits θα ανατρέχει το σύστημα κάθε φορά έτσι ώστε να συγκρίνει και να καταλήξει σε ταυτοποίηση ή αποτυχία ταυτοποίησης.

Το τελικό αποτέλεσμα που έχουμε φαίνεται στην εικόνα 7.7

Εικόνα 7.7 IrisCode



8. Αποθήκευση και Σύγκριση

Αρχικά εντοπίσαμε την ίριδα και την κόρη του ματιού, στη συνέχεια κανονικοποιήσαμε τα αποτελέσματα και τέλος εξάγαμε 2048 bits μέσω των Gabor 2d κυματιδίων. Η επεξεργασία της εικόνας του χρήστη έχει λάβει τέλος. Βασικό χαρακτηριστικό της μεθόδου που αναλύουμε είναι ότι το αποτέλεσμα κάθε φωτογραφίας που έχουμε στη διάθεση μας για να επεξεργαστούμε, ανεξαρτήτου μεγέθους, καταλήγει στο IrisCode, δηλαδή σε 2048 bits. Προτού εξηγήσουμε τη σύγκριση που απαιτείται για να εντοπίσουμε τυχόν ταιρίασμα, ας αναλύσουμε με πιο τρόπο αποθηκεύσαμε σε επίπεδο εφαρμογής Iphone τα δεδομένα μας.

Αποθήκευση

Κάθε χρήστης που χρησιμοποιεί την εφαρμογή προτού εισάγει τη φωτογραφία του, δηλώνει τόσο το όνομα του όσο και το επίθετο του. Το όνομα και το επίθετο μαζί με το αποτέλεσμα από τα φίλτρα, τα 2048 bits, αποθηκεύονται σε μία βάση δεδομένων Sql. Η βάση παραμένει και μετά το κλείσιμο της εφαρμογής και ξαναχρησιμοποιείται σε περίπτωση που χρησιμοποιηθεί η εφαρμογή όχι για εισαγωγή νέου χρήστη αλλά για ταυτοποίηση υπάρχοντος χρήστη.

Σύγκριση

Το τελευταίο στάδιο της επεξεργασίας μας είναι η σύγκριση των IrisCodes. Σε πάρα πολλές εφαρμογές η διαδικασία της σύγκρισης των δεδομένων θεωρείται τόσο πολύπλοκη όσο και χρονοβόρα. Αντιθέτως το στάδιο της σύγκρισης εδώ είναι ταχύτατο και με αμελητέα πολυπλοκότητα. Το μόνο που χρειάζεται για να θεωρήσουμε ότι βρήκαμε ταιρίασμα είναι να υπολογίσουμε την απόσταση Hamming με τον εξής τρόπο:

$$HD = (\text{IrisCode}(A) \text{ XOR } \text{IrisCode}(B)) / 2048$$

Αναλόγως τι αποτέλεσμα θα προκύψει από τον παραπάνω υπολογισμό θα είναι το μόνο στοιχείο με το οποίο θα αποφασίσουμε εάν έχουμε αναγνώριση. Ιδανικά σε περίπτωση ταιριάσματος το HD πρέπει να είναι σχεδόν μηδέν. Ως κατώφλι για το ταιρίασμα θεωρούμε το 30%, δηλαδή το 0.3 .

Πίνακας 8.1: Πιθανότητα για ψευδή αποτελέσματα ταιριάσματος αναλόγως με το κατώφλι του HD

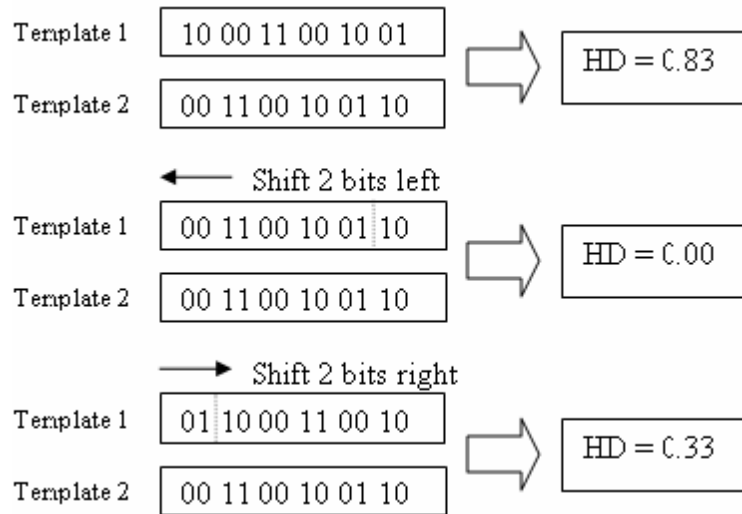
HD Criterion	Odds of False Match
0.26	1 in 1013
0.27	1 in 1012
0.28	1 in 1011
0.29	1 in 13 billion
0.30	1 in 1.5 billion
0.31	1 in 185 million
0.32	1 in 26 million
0.33	1 in 4 million
0.34	1 in 690,000
0.35	1 in 133,000

Ολίσθηση Bits

Η διαδικασία της κανονικοποίησης όπως περιγράψαμε και στο κεφάλαιο 6 γίνεται για να αποφύγουμε ασυνέπειες μεγέθους λόγω της απόστασης της κάμερας αλλά και τυχόν διαστολής της κόρης. Το μοντέλο όμως δεν μπορεί να επιλύσει ασυνέπειες περιστροφής. Για να επιλύσουμε αυτό το πρόβλημα το οποίο είναι σε θέση να «καταστρέψει» το αποτέλεσμα της ταυτοποίησης κατά την διάρκεια του ταιριάσματος ολισθαίνουμε bits από ένα από τα δύο πρότυπα προς σύγκριση.

Ολισθαίνουμε προς τη μία κατεύθυνση μιας και η ολίσθηση είναι περιστροφική, μέχρι να ταυτιστούν τα δύο πρότυπα και να βρούμε την ελάχιστη απόσταση Hamming. Ολισθαίνουμε θ θέσεις τόσο δεξιά όσο και αριστερά. Ο αριθμός των bits που θα μετακινούμαστε σε κάθε ολίσθηση εξαρτάται από το πλήθος των φίλτρων που χρησιμοποιούμε.

Εικόνα 8.1 : Παράδειγμα bit shifting



9. Περίληψη Επιδόσεων Ταχύτητας

Απόκτηση Εικόνας

Σε αυτό το κεφάλαιο θα αναλύσουμε τις επιδόσεις ταχύτητας της εφαρμογής σε κάθε στάδιο του αλγορίθμου αναγνώρισης της ίριδας. Για την απόκτηση της εικόνας είτε χρησιμοποιήσουμε έτοιμη φωτογραφία από την βιβλιοθήκη του κινητού είτε τραβήξουμε μια καινούργια φωτογραφία ο χρόνος μέχρι να αποκτήσουμε στα «χέρια» μας προγραμματιστικά την φωτογραφία είναι σταθερός και περίπου 70msec.

Τμηματοποίηση

Στη συνέχεια πρέπει να εντοπίσουμε την ίριδα και την κόρη που είναι και το πιο χρονοβόρο τμήμα του αλγορίθμου. Ο χρόνος που χρειάζεται η τμηματοποίηση εξαρτάται από το μέγεθος της εικόνας. Στο πίνακα 9.1 βλέπουμε τους χρόνους αναλόγως το μέγεθος της εικόνας.

Τμηματοποίηση	Μέγεθος Εικόνας	Χρόνος
<u>Κάμερα</u>		
Μπροστινή Iphone 4	480x640	4seconds
Iphone 3g/3gs	1600x1200	7seconds
Πίσω Iphone 4	2592 x 1936	15seconds

Ο λόγος που βλέπουμε τόσο μεγάλη διαφορά στους χρόνους έχει να κάνει με το πόσα πιθανά κέντρα δοκιμάζουμε στην αρχή. Για μία εικόνα 1600x1200 δοκιμάζονται περίπου εξήντα χιλιάδες εικονοστοιχεία για πιθανά κέντρα. Για αυτά, μόνο εκείνα που έχουν φωτεινότητα χαμηλότερη από το μίσο του μέσου όρου φωτεινότητας της εικόνας θα υπολογιστεί η τελεστής του Daugman. Για κάθε εικονοστοιχείο που υπολογίζεται για αυτό ο τελεστής του Daugman απαιτούνται 600 αθροίσματα 250 αφαιρέσεις και πολλαπλασιασμοί και τέλος μια αναζήτηση μεγίστου σε πίνακα 250 θέσεων. Για να εξαλείψουμε το χρονικό πρόβλημα που αντικρίζουμε με τις φωτογραφίες των 5 M pixels απλά σμικραίνουμε τις εικόνες σε 1600 x 1200 ανάλυση.

Κανονικοποίηση

Το ξετύλιγμα της ίριδας χρειάζεται περίπου 1msec ανεξαρτήτου μεγέθους φωτογραφίας.

Εξαγωγή Χαρακτηριστικών

Η εξαγωγή χαρακτηριστικών μέσω του Gabor δεν εξαρτάται από το μέγεθος της εικόνας μιας και η κανονικοποιημένη εικόνα έχει σταθερό μέγεθος(320 x 360). Χρειάζεται περίπου 3 δευτερόλεπτα για να ολοκληρωθεί ο υπολογισμός του Gabor.

Σύγκριση Δεδομένων

Μιας και το μόνο που χρειάζεται για να συγκρίνουμε τα δεδομένα είναι μια πράξη XOR μεταξύ 2048 bits ο χρόνος είναι περίπου στα 50 μ s (microseconds). Το πόσο θα καθυστερήσει η αναζήτηση έχει να κάνει με πόσα IrisCodes περιέχει μέσα η βάση δεδομένων μας.

Βελτιστοποίηση Ταχύτητας

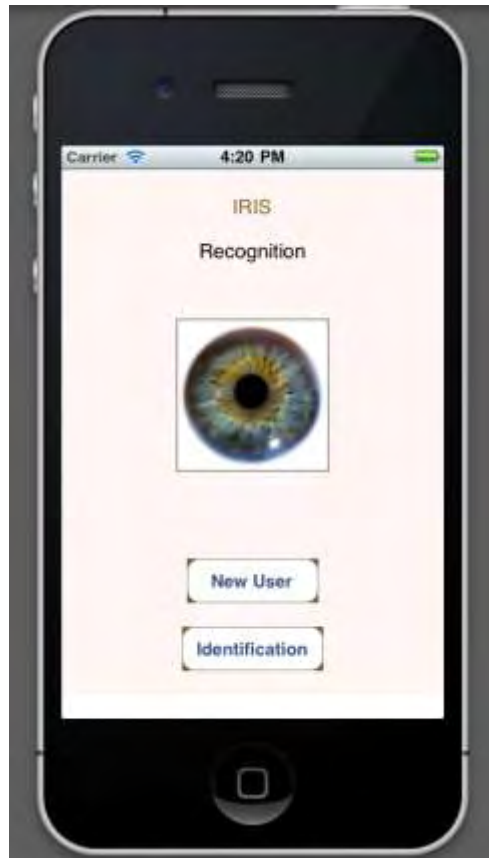
Μιας και όλα τα καινούργια μοντέλα του Iphone έχουν Cortex A8 Neon SIMD (Single Instruction Multiple Data) ειδικά στο στάδιο της τμηματοποίησης μπορεί και πρέπει να υλοποιηθεί παράλληλα. Υπολογίζεται περίπου ένα Speed Up 4 με 8 x.

10. Γραφικό Περιβάλλον της Εφαρμογής (GUI)

Το γραφικό περιβάλλον δημιουργήθηκε εξολοκλήρου σε objective-c και ο έλεγχος έγινε με το Iphone Simulator που εμπεριέχεται στο Xcode. Στις παρακάτω εικόνες βλέπουμε ένα «τρέξιμο» της εφαρμογής.

Αρχικά ανοίγουμε την εφαρμογή όπου η κεντρική της εμφάνιση φαίνεται στην εικόνα 10.1.

Εικόνα 10.1



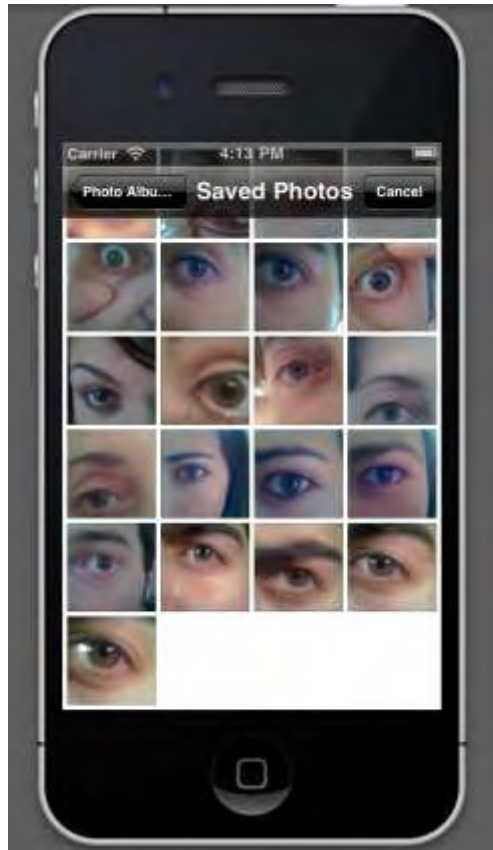
Μιας και τρέχουμε την εφαρμογή για πρώτη φορά πρέπει να εισάγουμε κάποιο χρήστη, έτσι ώστε να δημιουργηθεί η βάση δεδομένων μας για να μπορεί να πραγματοποιηθεί η αναζήτηση-ταυτοποίηση. Πατώντας «New User» αλλάζουμε απεικόνιση όπως βλέπουμε στην εικόνα 10.2.

Εικόνα 10.2



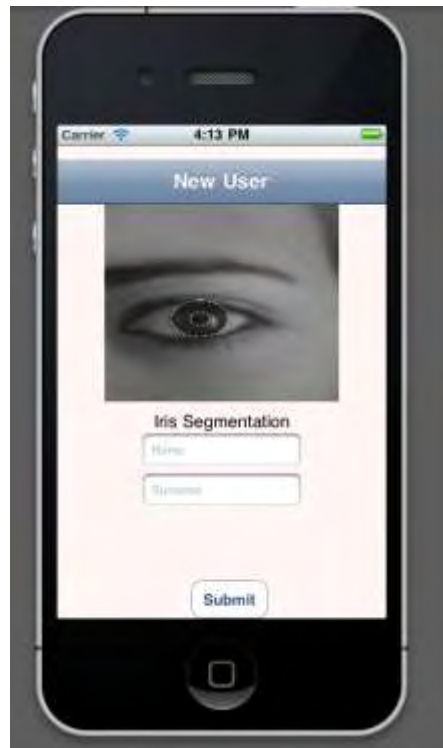
Σε αυτή την απεικόνιση αν τρέχαμε την εφαρμογή απευθείας στη συσκευή και όχι σε προσομοιωτή τότε εκτός από το «Εισαγωγή από τη βιβλιοθήκη» θα αντικρίζαμε και ένα ακόμα κουμπί «Απευθείας από κάμερα», το οποίο θα μας έδινε τη δυνατότητα να τραβήξουμε απευθείας φωτογραφία από την κάμερα του κινητού μας. Μιας και ο προσομοιωτής δεν έχει κάμερα το κουμπί παραμένει κρυφό και ανενεργό. Αφού επιλέξουμε «Insert from Library» τότε ανοίγουν όπως θα δούμε στην εικόνα 10.3 όλες οι φωτογραφίες που είναι αποθηκευμένες στο κινητό μας.

Εικόνα 10.3



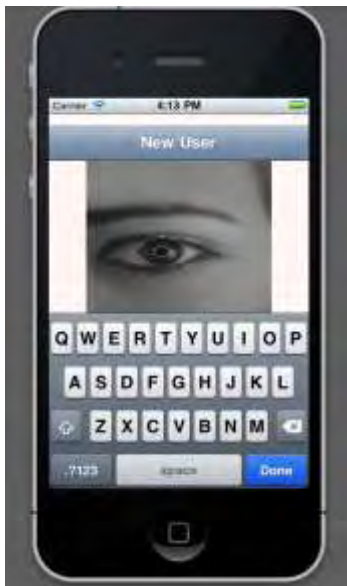
Στη συνέχεια επιλέγουμε όποια φωτογραφία θέλουμε και μετά από ορισμένα δευτερόλεπτα (ανάλογα και ποια έκδοση Iphone χρησιμοποιούμε) αντικρίζουμε την εικόνα 10.4.

Εικόνα 10.4



Διακρίνουμε τη φωτογραφία που επιλέξαμε και τον εντοπισμό τόσο της ίριδας όσο και της κόρης. Αφού ο εντοπισμός ήταν επιτυχής και η φωτογραφία μας είναι ξεκάθαρη, εισάγουμε το όνομα και το επίθετο του ανθρώπου που αντικρίζουμε στην εικόνα(εικόνα 10.5) και πατάμε “Submit” όπου η εφαρμογή μας ενημερώνει για επιτυχημένη ή αποτυχημένη εισαγωγή στη βάση δεδομένων (εικόνα 10.6).

Εικόνα 10.5

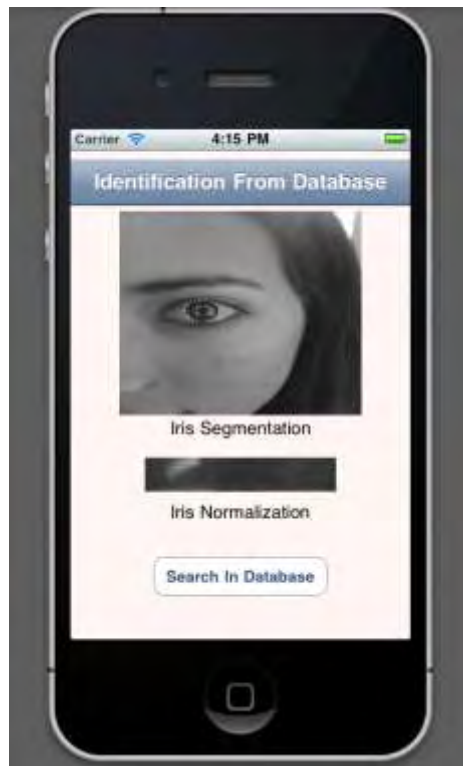


Εικόνα 10.6



Ολοκληρώσαμε το πρώτο βασικό κομμάτι της εφαρμογής. Τώρα το μόνο που απέμεινε είναι να εισάγουμε μια διαφορετική φωτογραφία του ίδιου ανθρώπου και να προσπαθήσουμε να το αναγνωρίσουμε. Επιστρέφουμε και πάλι στην αρχική μας εμφάνιση και επιλέγουμε «Identification». Επιλέγουμε «Insert from Library» καθώς πάλι δεν έχουμε κάμερα. Επιλέγουμε μια φωτογραφία με τον ίδιο τρόπο και μας εμφανίζεται το ακόλουθο (βλ. εικόνα 10.7):

Εικόνα 10.7



Πιέζοντας το κουμπί «Search in Database» η εφαρμογή ψάχνει όλες τις εγγραφές της βάσης σύμφωνα με αυτή την ίριδα και σε περίπτωση επιτυχίας επιστρέφει το ονοματεπώνυμο του ανθρώπου που βρίσκεται στη φωτογραφία(Εικόνα 10.8). Σε αντίθετη περίπτωση, μας ενημερώνει για την αποτυχία της ταυτοποίησης (Εικόνα 10.9).



Εικόνα 10.8 και 10.9 : Αποτελέσματα ταυτοποίησης.

11.Αποτελέσματα

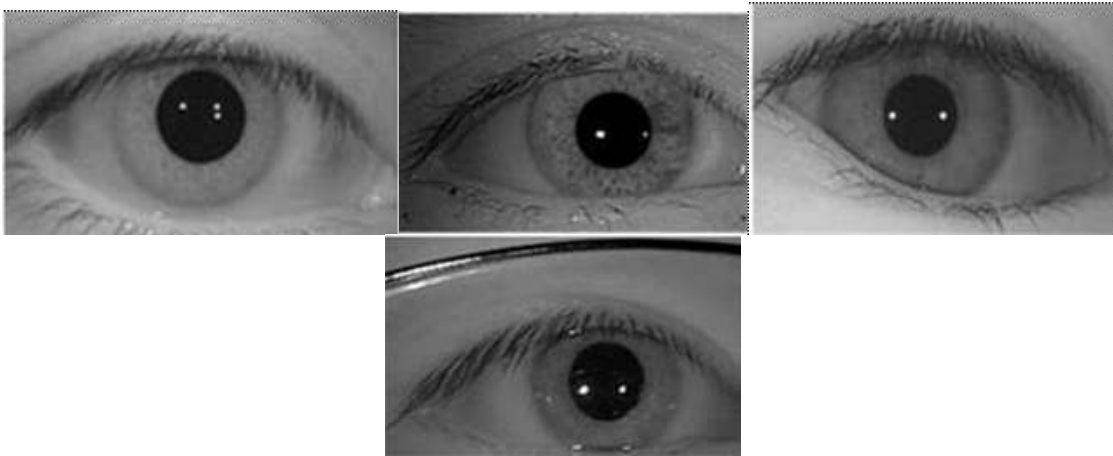
Σε όλη τη διάρκεια των δοκιμών για να εξαλείψουμε τυχόν τυχαία αποτελέσματα εισάγουμε στην βάση οχτώ διαφορετικούς ανθρώπους. Για κάθε ένα από τους οχτώ έχουμε στη διάθεση μας άλλες τρεις φωτογραφίες όπου τις χρησιμοποιούμε για να ανιχνεύσουμε το κάθε ένα χρήστη από τους οχτώ. Χρησιμοποιούμε δηλαδή συνολικά τριάντα δύο φωτογραφίες.

CASIA Iris Image Database

Αρχικά έγιναν μετρήσεις με φωτογραφίες τραβηγμένες από ειδική υπέρυθρη κάμερα με πολύ χαμηλά επίπεδα θορύβου. Οι φωτογραφίες αποκτήθηκαν από την ιστοσελίδα του Biometrics Ideal Test **CASIA Iris Image Database Version 4.0**. Παραδείγματα αυτών των φωτογραφιών φαίνονται στην εικόνα 11.1. Με κατώφλι στο 0.20 είχαμε

- ✓ 100% αναγνώριση - επιτυχία
- ✓ 0 false positive errors.
- ✓ 0% μη αναγνώριση

Εικόνα 11.1: Παραδείγματα εικόνων από **CASIA Iris Image Database**



Πραγματικές Φωτογραφίες Iphone

Εγιναν μετρήσεις και με πραγματικές φωτογραφίες από τη κάμερα του Iphone. Τα αποτελέσματα είναι

- ✓ 60% αναγνώριση
- ✓ 10% false positive error
- ✓ 20% μη αναγνώριση

Σαφώς το βασικό πρόβλημα είναι το false positive error το οποίο βασίζεται κυρίως στο θόρυβο που υπάρχει στις φωτογραφίες του κινητού τόσο από εξωτερικούς παράγοντες περιβάλλοντος όσο και αντανάκλαση λόγω του φακού.

12. Μελλοντικές Βελτιώσεις

Υπάρχουν αρκετά σημεία στην υλοποίηση που μπορούν να βελτιωθούν. Απο άποψη χρόνου «τρεξίματος» το βήμα της τμηματοποίησης χρειάζεται βελτιστοποίηση καθώς είναι ιδιαίτερα χρονοβόρο. Φωτογραφίες ίριδας που παρεμποδίζονται απο τα βλέφαρα θα ήταν επιθυμητό να απορρίπτονται αυτόματα απο το πρόγραμμα χωρίς την παρέμβαση του χρήστη. Χρήση άχρηστων στοιχείων της ίριδας για βελτίωση της απόστασης Hamming. Υλοποίηση της εφαρμογής και σε άλλες πλατφόρμες κινητής τηλεφωνίας πχ Android, Windows Mobile.

Πηγές

<http://www.cl.cam.ac.uk/~jgd1000/> (main site of Dr. John Daugman)

Σίτας Α., 2002, Ψηφιοποίηση υλικού και δημιουργία ψηφιακών βάσεων δεδομένων, διαθέσιμο στο <http://eprints.rclis.org/bitstream/10760/7019/1/Sitas-Psifiopoiisi.pdf>

Καμπουράκη Ν., 2011, Τυποποίηση και Αυθεντικοποίηση, Σημειώσεις μαθήματος, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου, διαθέσιμο στο http://www.icsd.aegean.gr/website_files/proptyxiako/185755266.pdf

Μάγκος Ε., 2007, Ασφάλεια υπολογιστών και προστασία δεδομένων, Σημειώσεις μαθήματος, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Κάτσικας Σ., 2001, Ασφάλεια Υπολογιστών, εκδόσεις ΕΣΠΙ,ΕΑΠ, Πάτρα

http://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=%CE%B1%CE%BD%CE%B1%CE%B3%CE%BD%CF%8E%CF%81%CE%B9%CF%83%CE%B7&dq= πρόσβαση στις 28/06/2011

Frankin Cheung, "Iris Recognition", BSc thesis, University of Queensland, Australia, 1999

[http://el.wikipedia.org/wiki/%CE%8A%CF%81%CE%B9%CF%82_\(%CE%BF%CF%86%CE%B8%CE%B1%CE%BB%CE%BC%CE%BF%CF%8D\)](http://el.wikipedia.org/wiki/%CE%8A%CF%81%CE%B9%CF%82_(%CE%BF%CF%86%CE%B8%CE%B1%CE%BB%CE%BC%CE%BF%CF%8D))

<http://www.biometrics.gov/Documents/irisrec.pdf>