

Τ.Ε.Ι. ΗΠΕΙΡΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ & ΠΛΗΡΟΦΟΡΙΚΗ

ΤΣΑΒΔΑΡΙΔΟΥ ΑΝΑΣΤΑΣΙΑ

ΜΩΡΑΓΙΑΝΝΗΣ ΝΙΚΟΣ

Τ.Ε.Ι ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ
& ΠΛΗΡΟΦΟΡΙΚΗ

ΤΣΑΒΔΑΡΙΔΟΥ ΑΝΑΣΤΑΣΙΑ
ΜΩΡΑΤΙΑΝΝΗΣ ΝΙΚΟΣ

*Η εργασία αυτή είναι αφιερωμένη
στους γονείς μας για όλα όσα μας έχουν προσφέρει.*

Περιεχόμενα

Περίληψη	6
Εισαγωγή	8
Κεφάλαιο 1	
Βιομετρία	10
1.1 Βιομετρική.....	11
1.2 Τεχνολογίες Βιομετρικών.....	12
1.3 Οι Κωδικοί Πρόσβασης Ανήκουν στο Παρελθόν και Αντικαθίστανται από Συστήματα Βιομετρίας.....	14
1.4 Από την Πλαστική Ταυτότητα στις Βιομετρικές Μεθόδους.....	15
1.5 Εφαρμογές.....	16
Κεφάλαιο 2	
Δακτυλικά Αποτυπώματα	19
2.1 Συστήματα Δακτυλικών Αποτυπωμάτων.....	21
2.2 Προσδιορισμός Δακτυλικών Αποτυπωμάτων.....	21
2.2.1 Ταξινόμηση Δακτυλικών Αποτυπωμάτων.....	23
2.2.2 Αύξηση Εικόνας Δακτυλικών Αποτυπωμάτων.....	24
2.3 Υπόδειξη του Δακτύλου.....	25
2.4 Προϊόντα για το PC σας.....	25
2.5 Άλλες Εταιρίες και Προϊόντα.....	27
Κεφάλαιο 3	
Γεωμετρία Χεριών	38
3.1 Προγράμματα Γεωμετρίας Χεριών.....	39
3.2 Γεωμετρία Χεριού Βασισμένη στο Σύστημα Επαλήθευσης.....	40
3.3 Πρότυπα για το Ταίριασμα Μορφής Χεριών.....	41
3.4 Γεωμετρία Χεριών Εναντίον των Δακτυλικών Αποτυπωμάτων.....	42
Κεφάλαιο 4	
Εξέταση Ίριδας και Αμφιβληστροειδούς	43
4.1 Εξέταση Ίριδας.....	44
4.2 Το PC Iris.....	45
4.3 Εξέταση Αμφιβληστροειδούς.....	46
4.4 Έλεγχος Ίριδας στους Αερολιμένες.....	47
Κεφάλαιο 5	
Αναγνώριση Φωνής	49
5.1 Τι Κρύβει μια Απλή Φωνή.....	52
5.2 Οι 4 Ανταγωνιστές του Εξωτερικού.....	56
5.3 Η Ελλάδα σε Καλό Δρόμο.....	62
5.4 Μετά τις Δοκιμές...Η Ελληνική Έκδοση.....	67
5.5 Αναγνώριση Φωνής...Η Οικονομικότερη Λύση.....	68
5.6 Σύστημα Αναγνώρισης Φωνής.....	72
5.6.1 Βασικές Αρχές Αναγνώρισης Φωνής.....	72
5.6.2 Επαλήθευση Ομιλητών.....	73
5.6.3 Επιλογή των Χαρακτηριστικών Γνωρισμάτων.....	76
5.6.4 Ομιλητής που Διαμορφώνει.....	76

Περιεχόμενα (συνέχεια)

5.6.5 Ταίριασμα Σχεδίων.....	77
5.7 Αναγνώριση Φωνής στο Internet.....	78
5.8 Εταιρίες και Προϊόντα.....	78

Κεφάλαιο 6

Γεωμετρία και Θερμογραφία Προσώπου.....	80
6.1 Αναγνώριση Προσώπου. Μια Βιομετρική Τεχνολογία με Πολλαπλές Εφαρμογές.....	81
6.2 Ανίχνευση και Αναγνώριση Προσώπου.....	83
6.3 Θέση Προσώπου.....	85
6.4 Προϊόντα για το PC σας.....	86
6.5 Μέθοδος Αναγνώρισης από τη Siemens.....	87

Κεφάλαιο 7

Άλλες Βιομετρικοί Μέθοδοι.....	88
7.1 Διακρίβωση Υπογραφή.....	89
7.2 Ρυθμός Πληκτρολόγησης.....	91
7.3 Αναγνώριση Φλεβικής Δομής.....	91
7.4 Αναγνώριση Γεωμετρίας Αυτιού.....	92
7.5 Έλεγχος DNA.....	92
7.6 Αναγνώριση Σωματικής Οσμής.....	92
7.7 Αποτυπώματα Παλάμης	92
7.8 Βιομετρικά Συστήματα Αναγνώρισης Φυσικών Χαρακτηριστικών....	93
7.8.1 Αναγνώριση Εικόνας.....	94
7.8.2 Πολύμορφα Βιομετρικά Συστήματα.....	96
7.8.3 Βιομετρική Βασισμένη στην Πρόσβαση Ιστού.....	97
7.9 Μοναδικά Φωτεινά Αποτυπώματα από το Δέρμα.....	99
7.10 Αναγνώριση Βηματισμού.....	99

Κεφάλαιο 8

Εφαρμογές Βιομετρικών Συστημάτων...Παρόν και Μέλλον..

8.1 Ηλεκτρονικό Εμπόριο και Διαδίκτυο.....	104
8.2 Ασφάλεια σε Δίκτυα.....	105
8.3 Τεχνολογία κατά των Καταστροφικών Αεροπειρατών.....	106
8.4 Βιομετρικά Συστήματα Δοκιμάζονται στην Ευρώπη.....	108
8.5 Η "Πρώτη Γραμμή".....	109
8.6 Barcode : Η Τεχνολογία του Γραμμωτού Κώδικα.....	113
8.7 Το Ξενοδοχείο του Μέλλοντος.....	116
8.8 Και οι Έλληνες Φωτογραφίζονται και Δακτυλοσκοπούνται.....	121
8.9 Τεχνολογία Ανίχνευσης Σωμάτων (Rapiscan).....	123
8.10 Οι Βιομετρικές Εφαρμογές Τίθενται ως Στόχος να Αναλάβουν τις Συναλλαγές.....	126
8.11 Διαβατήρια – Θαύματα της Τεχνολογίας.....	128
8.12 Πιο Ασφαλή Προϊόντα από τη Βιομηχανία των Passwords.....	132
8.13 Σύστημα Γλαυκώπης.....	133
8.14 Verichip : Εμφυτευμένες Πληροφορίες στο Ανθρώπινο Σώμα.....	134
8.15 Λογισμικό Επιτρέπει στους Υπολογιστές να Βλέπουν	136

Περιεχόμενα (συνέχεια)

Κεφάλαιο 9

Βιομετρικά Συστήματα...Η Ώρα της Αποτίμησης	137
9.1 Η Ανάλυση Zephyr.....	138
9.2 Δελτίο Ταυτότητας...Το Ανθρώπινο Σώμα.....	141
9.3 Το Εξυπνότερο Σύστημα Ασφάλειας Αμφισβητείται.....	143
9.4 Ψεύτικα Αποτυπώματα Ξεγελούν τις Αρχές.....	144
9.5 Εξαπάτηση Συσκευών Αναγνώρισης Αποτυπωμάτων.....	147
9.6 Τι Γίνεται με το Απόρρητο.....	148
Γλωσσάριο	152
Βιβλιογραφία	155

**ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ
& ΠΛΗΡΟΦΟΡΙΚΗ**

Τσαβδαρίδου Αναστασία
Μωραγιάννης Νίκος

Πτυχιακή εργασία

Επιβλέπων καθηγητής
Στεργίου Ελευθέριος

Σχολή Διοίκησης και Οικονομίας
Τμήμα Τηλεπληροφορικής και Διοίκησης
Τ.Ε.Ι. ΗΠΕΙΡΟΥ

ΠΕΡΙΛΗΨΗ

Στη παρούσα εργασία συζητείται η χρήση βιομετρικών συστημάτων και πληροφορικής. Η βιομετρική είναι η επιστήμη εκείνη που αναλύει στατιστικά τα βιολογικά χαρακτηριστικά του ατόμου. Σήμερα όμως χρησιμοποιούμε αυτόν τον όρο για να αναφερθούμε στις τεχνολογίες εκείνες που αναλύουν τα ανθρώπινα χαρακτηριστικά για λόγους ασφαλείας. Ο ακόλουθος είναι ο κοινά αποδεκτός ορισμός για τη βιομετρία: Βιομετρία είναι η επιστήμη που χρησιμοποιεί ένα μοναδικό και μετρήσιμο χαρακτηριστικό ή συνήθεια ενός ατόμου για τον αυτόματο έλεγχο ή την πιστοποίηση της ταυτότητας του. Οι βιομετρικές τεχνολογίες συνεπώς ασχολούνται με τα φυσικά μέρη του ανθρώπινου σώματος ή τις προσωπικές του συνήθειες. Ο όρος «αυτόματο» σημαίνει ότι η βιομετρική τεχνολογία πρέπει να αναγνωρίζει ή να πιστοποιεί ένα ανθρώπινο χαρακτηριστικό γρήγορα και αυτόματα σε πραγματικό χρόνο. Τα πιο συνηθισμένα φυσιολογικά βιομετρικά χαρακτηριστικά είναι το μάτι (ίρις και αμφιβληστροειδής), το πρόσωπο, το δάκτυλο, το χέρι και η φωνή. Βιομετρικά χαρακτηριστικά συμπεριφοράς είναι ο ρυθμός πληκτρολόγησης και η υπογραφή. Στη βιομηχανία των συστημάτων ασφαλείας τα βιομετρικά συστήματα θεωρείται ότι παρέχουν το ψηλότερο επίπεδο ασφαλείας. Οι μέθοδοι για την πιστοποίηση της ταυτότητας ενός ατόμου χωρίζονται σε τρία επίπεδα:

- **Επίπεδο 1** (χαμηλό επίπεδο ασφαλείας): κάτι το οποίο έχουμε (π.χ. μια ταυτότητα με φωτογραφία).
- **Επίπεδο 2** (μέσο επίπεδο ασφαλείας): κάτι το οποίο γνωρίζουμε (π.χ. ένα συνθηματικό για πρόσβαση στον υπολογιστή ή το PIN του ATM).
- **Επίπεδο 3** (υψηλό επίπεδο ασφαλείας): κάτι το οποίο είμαστε ή κάνουμε (π.χ. αποτυπώματα, φωνή κ.λ.π.).

ΠΕΡΙΛΗΨΗ

Συνοψίζοντας τη συνολική εργασία αρχικά παρουσιάζεται η βιομετρία ως έννοια και οι τεχνολογίες βιομετρικών συστημάτων. Στη συνέχεια αναφέρονται στο δεύτερο κεφάλαιο τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων και τα γενικά χαρακτηριστικά τους. Προχωρώντας στο τρίτο κεφάλαιο αναλύεται η γεωμετρία χεριών. Στο τέταρτο κεφάλαιο γίνεται λόγος για την εξέταση της ίριδας και του αμφιβληστροειδούς καθώς και τις εταιρίες που ασχολούνται με τα συστήματα αυτά. Συνεχίζοντας στο πέμπτο κεφάλαιο γίνεται αναφορά στα συστήματα αναγνώρισης φωνής και στον τρόπο που γίνεται η επαλήθευσή τους. Στο έκτο κεφάλαιο παρουσιάζεται μια βιομετρική τεχνολογία με πολλές εφαρμογές, η γεωμετρία και θερμογραφία προσώπου. Στο έβδομο κεφάλαιο γίνεται συνοπτική αναφορά στις πιο αξιόλογες βιομετρικές μεθόδους που αναπτύσσονται αυτή την περίοδο στα διάφορα εργαστήρια. Προχωρώντας στο όγδοο κεφάλαιο παρουσιάζονται οι εφαρμογές των βιομετρικών συστημάτων σε παρόν και μέλλον. Τέλος στο ένατο κεφάλαιο, έχοντας αναλύσει όλες τις βιομετρικές μεθόδους έρχεται πλέον αναπόφευκτα η ώρα της αποτίμησης.

ΕΙΣΑΓΩΓΗ

Αν πιστεύετε ότι η πρόσβαση στους φυλασσομένους χώρους από τους Αγγέλους του Τσάρλι με χρήση βιομετρικού αναγνώρισης ίριδας ή ότι το βιομετρικό όπλο του Δικαστή Dredd που αναγνώριζε το δαχτυλικό του αποτύπωμα αποτελούν προϊόντα επιστημονικής φαντασίας, τότε έχετε κάνει μεγάλο λάθος. Οι βιομετρικές συσκευές που στηρίζουν τη λειτουργία τους στη μοναδικότητα των ανθρώπων χαρακτηριστικών κυκλοφορούν και μάλιστα και στην ελληνική αγορά.

Η αναγνώριση ενός ατόμου και ο έλεγχος πρόσβασης είναι αναμφισβήτητα δύο τομείς οι οποίοι απαιτούν τη μέγιστη ασφάλεια. Οι κωδικοί PINs, οι έξυπνες κάρτες αλλά και ο συνδυασμός τους, συνέβαλαν, αλλά και προσφέρουν ακόμη τα μέγιστα σε συστήματα ελέγχου πρόσβασης και ηλεκτρονικών συναλλαγών. Ειδικά όταν πρωτοκυκλοφόρησαν στην αγορά θεωρήθηκαν, και όχι άδικα, σχεδόν αδιάβλητα, αφού μέχρι τότε κανένα άλλο σύστημα δεν παρείχε ανάλογη ασφάλεια. Με την πάροδο όμως των χρόνων, η τεχνολογία τους σταδιακά άρχισε να γίνεται προσιτή στον καθένα με αποτέλεσμα να αρχίζουν να εμφανίζονται κρούσματα παραβίασης ή πλαστογράφησης τους.

Παράλληλα, η χρήση πολλών και διαφορετικών καρτών που απαιτούσε η κάθε εφαρμογή αλλά και η αποστήθιση κωδικών PINs, δεν έγιναν αποδεκτές από το ευρύ κοινό, με αποτέλεσμα να δημιουργηθεί η ανάγκη για κάποια νέα συστήματα, τα οποία θα έπρεπε αφενός να είναι εύχρηστα και αφετέρου να είναι πιο ασφαλή. Η ιδέα με τα δαχτυλικά αποτυπώματα ήταν γνωστή από παλιά (ταυτότητες), αφού το δαχτυλικό αποτύπωμα κάθε ανθρώπου είναι αφενός μοναδικό, αφετέρου το μεταφέρει πάντα μαζί του. Εκτός όμως από το δαχτυλικό αποτύπωμα, τα περισσότερα ανθρώπινα χαρακτηριστικά είναι μοναδικά. Ίριδα, αμφιβληστροειδής, DNA, παλάμη, τρόπος πληκτρολόγησης, φωνή, πρόσωπο, υπογραφή και βηματισμός, αποτελούν επίσης, μοναδικά γνωρίσματα του κάθε ανθρώπου.

Από την άλλη πλευρά με δεδομένη την ανάπτυξη της τεχνολογίας, δεν ήταν δύσκολο για τους κατασκευαστές να μετατρέψουν τα χαρακτηριστικά αυτά σε ψηφιακές μορφές, δημιουργώντας έτσι μια νέα τεχνολογία τη βιομετρική τεχνολογία.

Έτσι, δημιουργήθηκαν κατάλληλα συστήματα, τα λεγόμενα βιομετρικά, τα οποία ανάλαβαν την μετατροπή του μοναδικού ανθρώπινου γνωρίσματος σε ψηφιακή μορφή. Με αυτό τον τρόπο, όχι μόνο αυξήθηκε η ασφάλεια, αφού η πλαστογραφία των ανθρώπινων χαρακτηριστικών είναι σαφώς δυσκολότερη, αλλά και απάλλαξε τους χρήστες τους από τη μεταφορά κάρτας ή αποστήθιση κωδικού.

Η πολύχρονη ενασχόληση του ανθρώπου με τα δαχτυλικά αποτυπώματα, δεν άφησε ασυγκίνητους τους κατασκευαστές, οι οποίοι ακολουθώντας την περπατημένη παρουσίασαν τα πρώτα βιομετρικά συστήματα που στηρίζονταν σε αναγνώριση των δαχτυλικών αποτυπωμάτων. Οι πρώτες δυσκολίες που συνάντησαν ήταν απόλυτα λογικές. Ακαθαρσίες ή τραύματα δυσκόλευαν τους βιομετρικούς αναγνώστες και καθιστούσαν τη διαδικασία αναγνώρισης προβληματική. Επίσης, η πολύχρονη εμπειρία όμως με τα δαχτυλικά αποτυπώματα είχε και τα αρνητικά της, αφού οι μέθοδοι πλαστογράφησης τους ήταν ήδη γνωστοί (σκόνη, ζελατίνα). Φυσικά, οι σύγχρονοι βιομετρικοί αναγνώστες δαχτυλοσκόπησης, έχουν ξεπεράσει τα προβλήματα με τραύματα ή ακαθαρσίες, ενώ ο συνδυασμός των συστημάτων αυτών με τις γνωστές τεχνολογίες κωδικού PIN και χρήσης κάρτας, έχουν ενισχύσει σε μέγιστο βαθμό την όλη ασφάλεια τους, με αποτέλεσμα τα συστήματα δαχτυλοσκόπησης να αποτελούν τα πιο διαδεδομένα βιομετρικά της αγοράς.

ΕΙΣΑΓΩΓΗ

Ως βιομετρικό χαρακτηριστικό ο αμφιβληστροειδής είναι ο πλέον πολύπλοκος, με αποτέλεσμα τα αντίστοιχα βιομετρικά να θεωρούνται τα πιο ακριβή. Επειδή όμως ο αμφιβληστροειδής αλλοιώνεται με το πέρασμα του χρόνου, τα πλέον αξιόπιστα βιομετρικά, είναι αυτά που χρησιμοποιούν τεχνολογία αναγνώρισης ίριδας. Η ίριδα, πέραν του ότι δεν αλλοιώνεται με το πέρασμα του χρόνου, είναι πολύ δύσκολο να τραυματιστεί, κάτι που συμβαίνει συχνότερα με το δαχτυλικό αποτύπωμα, ενώ είναι πολύ δύσκολο να αντιγραφεί. Παράλληλα, η αναγνώριση της δεν απαιτεί επαφή με τη συσκευή, ενώ μπορεί να αναγνωριστεί ακόμη και όταν ο χρήστης φοράει γυαλιά. Επίσης, η λειτουργία ανάγνωσης της ίριδας, όπως και κάθε βιομετρικού είναι παντελώς ακίνδυνη. Για όλους αυτούς τους λόγους τα βιομετρικά της ίριδας, χρησιμοποιούνται ως επί τω πλείστο σε εφαρμογές κρίσιμης σημασίας.

Ιδιαίτερη διάδοση έχουν και τα βιομετρικά συστήματα αναγνώρισης προσώπου, τα οποία χρησιμοποιούνται ως επί το πλείστο για αναγνώριση ατόμων που βρίσκονται σε πλήθος, όπως γήπεδα, διαδηλώσεις κτλ. Η αναγνώριση παλάμης είναι ένα ακόμη βιομετρικό που θυμίζει τα βιομετρικά δαχτυλοσκόπησης, ενώ τα βιομετρικά αναγνώρισης φωνής, τρόπου πληκτρολόγησης και φωνής, δεν χαρακτηρίζονται από την υψηλή τους ακρίβεια, με αποτέλεσμα να χρησιμοποιούνται σε εφαρμογές χαμηλού ρίσκου, όπως πρόσβαση σε PC.

Τα βιομετρικά αρχίζουν να εισχωρούν σταδιακά σε κάθε τομέα της καθημερινότητας. Η χρήση των passwords για πρόσβαση σε υπολογιστές, δίκτυα, αλλά και σε φορητές συσκευές, όπως κινητά τηλέφωνα και PDAs, αρχίζει να αντικαθιστάται σταδιακά με βιομετρικά συστήματα. Επίσης, χρησιμοποιούνται σε συστήματα χρονομέτρησης, αλλά η κατεξοχήν εφαρμογή τους δεν είναι άλλη από τα συστήματα ελέγχου πρόσβασης.

Για αυτό ανάμεσα στα πάμπολλα τεχνικά χαρακτηριστικά τους, σημαντικό ρόλο παίζει ο αριθμός των χρηστών που μπορούν να υποστηρίξουν. Ιδιαίτερα σημαντικό χαρακτηριστικό είναι ο χρόνος ταυτοποίησης, ο χρόνος δηλαδή που θα αποφανθεί εάν το υπό έλεγχο άτομο δικαιούται πρόσβαση. Η αξιοπιστία των βιομετρικών περιγράφεται στα τεχνικά τους χαρακτηριστικά ως ποσοστό εσφαλμένων αποδοχών FAR (False Acceptance Rate) και ποσοστό εσφαλμένων απορρίψεων FRR (False Rejection Rate). Συγκεκριμένα, ο λόγος FAR δείχνει το ποσοστό των μη εξουσιοδοτημένων ατόμων που αποδέχτηκε το βιομετρικό και ο λόγος FRR το ποσοστό των εξουσιοδοτημένων προσώπων που δεν αποδέχτηκε.

ΚΕΦΑΛΑΙΟ 1



ΒΙΟΜΕΤΡΙΑ

Βιομετρία

Παρ' όλο που τα περισσότερα λεξικά ορίζουν τη βιομετρική ως τη στατιστική ανάλυση των βιολογικών χαρακτηριστικών του ανθρώπου, τα τελευταία χρόνια ο όρος τείνει να ταυτιστεί με την επιστήμη που αναλύει τα ανθρώπινα χαρακτηριστικά για σκοπούς ασφάλειας. Πράγματι το ανθρώπινο σώμα είναι μία τεράστια πηγή μοναδικών γνωρισμάτων που θα μπορούσαν να χρησιμοποιηθούν για αναγνώριση ταυτότητας. Ένα από αυτά μάλιστα, τα δακτυλικά αποτυπώματα, ήδη χρησιμοποιείται χρόνια τώρα για τέτοιους σκοπούς χωρίς βέβαια τη μεσολάβηση ηλεκτρονικών συσκευών και υπολογιστών. Πλέον, με τη βοήθεια που της προσφέρουν τα σύγχρονα μέσα, η βιομετρική ερευνά για μεγαλύτερη ακρίβεια και ασφάλεια σε άλλα χαρακτηριστικά του ανθρώπινου σώματος όπως η ίριδα του ματιού, το σχήμα του προσώπου ή του χεριού και η φωνή. Και ενώ όλες οι ανωτέρω βιομετρικές μέθοδοι ασχολούνται με τα φυσικά χαρακτηριστικά ενός ατόμου, σιγά σιγά αρχίζουν να αναπτύσσονται ορισμένες οι οποίες έχουν ως βάση συμπεριφορές όπως ο ρυθμός πληκτρολόγησης ή η υπογραφή. Όπου και να βασίζονται πάντως (φυσικό χαρακτηριστικό ή συμπεριφορά), οι βιομετρικές μέθοδοι θεωρείται αυτή τη στιγμή ότι προσφέρουν το υψηλότερο επίπεδο ασφάλειας από όλα τα υπάρχοντα συστήματα όπως είναι τα PINs (Personal Identification Numbers - Προσωπικοί Αριθμοί Αναγνώρισης), οι κάρτες και τα συνθηματικά.

Πολλοί μεγάλοι οργανισμοί, όπως τράπεζες ή κρατικές υπηρεσίες αρχίζουν δειλά δειλά να υιοθετούν τη νέα τεχνολογία με σκοπό την αύξηση της ασφάλειας των συστημάτων τους αλλά και την καλύτερη εξυπηρέτηση των πελατών τους. Η έκπληξη όμως έρχεται από αλλού: Αν κάνετε μια "βόλτα" στις ηλεκτρονικές αγορές του Internet, θα διαπιστώσετε ότι πολλές εταιρίες έχουν κυκλοφορήσει πλήθος από βιομετρικά συστήματα για προσωπικούς υπολογιστές, σε ιδιαίτερα προσιτές τιμές για το μέσο χρήστη (150-200 δολάρια!). Τα συστήματα αυτά υπόσχονται να "θωρακίσουν" τα PCs μας με ποικίλους τρόπους από οποιαδήποτε ανεπιθύμητη εισβολή είτε αυτή έρχεται μέσω τηλεφωνικής γραμμής είτε "εκ των έσω".

Στην εργασία αυτή, θα εξετάσουμε αναλυτικά τις σημαντικότερες βιομετρικές μεθόδους αναλύοντας τα πλεονεκτήματα και τα μειονεκτήματα της καθεμίας, τα πεδία εφαρμογών που μπορεί να έχουν, καθώς και τα σχετικά προϊόντα που κυκλοφορούν στην αγορά. Σίγουρα δεν θα μπορούσε να λείπει ιδιαίτερη αναφορά στη χρήση βιομετρικών μεθόδων σε προσωπικούς υπολογιστές, κάτι που σίγουρα μας ενδιαφέρει όλους.

1.1 ΒΙΟΜΕΤΡΙΚΗ

Η βιομετρική αναφέρεται στον αυτόματο προσδιορισμό ενός προσώπου βασισμένου στα φυσιολογικά ή χαρακτηριστικά της συμπεριφοράς του / της. Αυτή η μέθοδος προσδιορισμού προτιμάται πέρα από τις παραδοσιακές μεθόδους που περιλαμβάνουν τους κωδικούς πρόσβασης και τους αριθμούς PIN για διάφορους λόγους: (I) το πρόσωπο που προσδιορίζεται πρέπει για να είναι φυσικά παρόν στο σημείο προσδιορισμού (II) προσδιορισμός βασισμένος στις βιομετρικές τεχνικές προλαμβάνει την ανάγκη να αναφερθεί ένας κωδικός πρόσβασης. Με την αυξανόμενη χρήση των υπολογιστών ως μηχανήματα της τεχνολογίας πληροφοριών, είναι απαραίτητο να περιοριστεί η πρόσβαση στα ευαίσθητα / προσωπικά στοιχεία.

Με την αντικατάσταση των PINs, οι βιομετρικές τεχνικές μπορούν ενδεχομένως να αποτρέψουν την αναρμόδια πρόσβαση ή την ψευδή χρήση ATMs, των

κυβελοειδών τηλεφώνων, των έξυπνων καρτών, του υπολογιστή γραφείου PCs, των τερματικών σταθμών και των δικτύων υπολογιστών. Τα PINs και οι κωδικοί πρόσβασης μπορούν να ξεχαστούν και οι παραδοσιακές μέθοδοι προσδιορισμού όπως τα διαβατήρια και οι άδειες του οδηγού μπορούν να πλαστογραφηθούν, να κλαπούν ή να χαθούν. Κατά συνέπεια τα βιομετρικά συστήματα προσδιορισμού απολαμβάνουν ένα ανανεωμένο ενδιαφέρον.

Οι διάφοροι τύποι βιομετρικών συστημάτων χρησιμοποιούνται για προσδιορισμό πραγματικού χρόνου. Ο δημοφιλέστερος είναι βασισμένος στην αναγνώριση προσώπου και το ταίριασμα δακτυλικών αποτυπωμάτων. Εντούτοις, υπάρχουν άλλα βιομετρικά συστήματα που χρησιμοποιούν την ίριδα και την αμφιβληστροειδική ανίχνευση, την ομιλία, τη θερμογραφία και τη γεωμετρία χεριών.

Ένα βιομετρικό σύστημα είναι ουσιαστικά ένα σύστημα αναγνώρισης σχεδίων που κάνει έναν προσωπικό προσδιορισμό με τον καθορισμό της αυθεντικότητας ενός συγκεκριμένου φυσιολογικού ή συμπεριφορικού χαρακτηριστικού που κατέχεται από το χρήστη. Ένα σημαντικό ζήτημα στο σχεδιασμό ενός πρακτικού συστήματος είναι να καθοριστεί πώς ένα άτομο προσδιορίζεται. Ανάλογα με το πλαίσιο, ένα βιομετρικό σύστημα μπορεί να είναι είτε ένα σύστημα επαλήθευσης (επικύρωση) είτε ένα σύστημα προσδιορισμού.

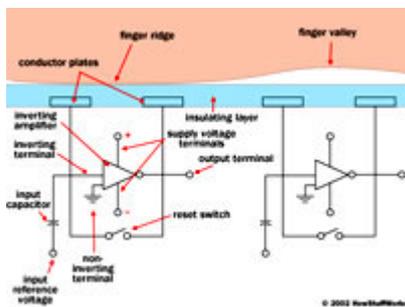
1.2 ΤΕΧΝΟΛΟΓΙΕΣ ΒΙΟΜΕΤΡΙΚΩΝ

Για να καταστεί δυνατή η βιομετρική αναγνώριση κάποιου ατόμου προηγείται - όπως είναι φυσικό- μία διαδικασία λήψης του βιομετρικού δείγματος. Στην πραγματικότητα λαμβάνεται από το άτομο ένας αριθμός δειγμάτων (συνήθως τρία) τα οποία συνδυάζονται βελτιώνοντας και συμπληρώνοντας το ένα το άλλο ώστε το αποτέλεσμα που θα προκύψει να είναι όσο το δυνατόν τελειότερο. Με αυτόν τον τρόπο κατασκευάζεται ένα βιομετρικό πρότυπο με το οποίο θα συγκρίνεται κάθε φορά το δείγμα που θα λαμβάνεται όταν ο χρήστης απαιτεί την είσοδό του στο προστατευμένο σύστημα. Το βήμα αυτό είναι από τα σημαντικότερα αφού η ποιότητα του προτύπου θα κρίνει κατά το μεγαλύτερο ποσοστό την αξιοπιστία του όλου συστήματος. Τη δημιουργία του βιομετρικού προτύπου ακολουθεί το στάδιο της αποθήκευσής του. Εδώ οι επιλογές είναι συνήθως τρεις: (1) αποθήκευση του προτύπου στη βιομετρική συσκευή αναγνώρισης (2) αποθήκευση σε μία κεντρική βάση δεδομένων (3) αποθήκευση σε φορητό μέσο (συνήθως κάποια κάρτα και πάλι) το οποίο μεταφέρει ο ίδιος ο χρήστης. Τέλος, έχουμε τη διαδικασία αίτησης εισόδου του χρήστη στο σύστημα κατά την οποία λαμβάνεται ένα νέο βιομετρικό δείγμα προκειμένου να συγκριθεί με το βιομετρικό πρότυπο. Αν το δείγμα ταιριάζει έστω και με μικρές αποκλίσεις (εξαρτάται πόσο "αυστηρό" έχει ρυθμιστεί να είναι το σύστημα), η είσοδος επιτρέπεται.

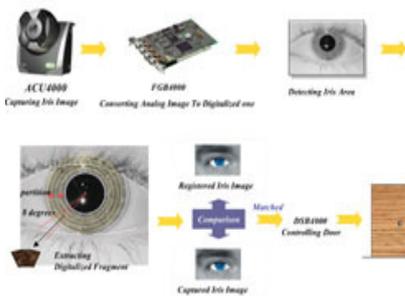
Παρότι τα διάφορα είδη βιομετρικών χρησιμοποιούν διαφορετικές λειτουργίες για να επιτύχουν την αναγνώριση, η αρχή λειτουργίας τους είναι λίγο-πολύ η ίδια. Το πρώτο στάδιο είναι η εγγραφή του χρήστη στο σύστημα. Κατά τη διαδικασία αυτή που συνήθως είναι πιο χρονοβόρα από τις υπόλοιπες, ο χρήστης αποδίδει το βιομετρικό δείγμα του, το οποίο αφού μετατραπεί σε ψηφιακή μορφή, αποθηκεύεται είτε στο ίδιο το βιομετρικό, όταν αυτό είναι αυτόνομο, είτε σε κάποια βάση δεδομένων, δημιουργώντας έτσι ένα βιομετρικό πρότυπο δείγμα (template). Στη χώρα μας υπάρχει νομικό πρόβλημα που περιγράφεται από το νόμο 2472/1997, που σχετίζεται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και στην ουσία δεν επιτρέπει την αποθήκευση των βιομετρικών χαρακτηριστικών σε βάση δεδομένων. Για αυτό το βιομετρικό δείγμα του χρήστη μπορεί να

αποθηκευτεί σε κάποια κάρτα, όπως για παράδειγμα μια κάρτα proximity, η οποία στη συνέχεια πρέπει να αποδοθεί στον κάτοχο του βιομετρικού δείγματος.

Αφού ολοκληρωθεί η διαδικασία της εγγραφής, κάθε φορά που κάποιο εξουσιοδοτημένο άτομο επιχειρήσει να εισέλθει στο σύστημα, πρέπει να αποδώσει το βιομετρικό του δείγμα, το οποίο συγκρίνεται με το πρότυπο και εφόσον ταιριάζουν παρέχεται πρόσβαση. Στην περίπτωση που το δείγμα είναι εγγεγραμμένο σε κάποια κάρτα, το υπό πιστοποίηση άτομο οφείλει να εισαγάγει την κάρτα στη συσκευή. Στην περίπτωση τώρα των βιομετρικών δαχτυλοσκόπησης διακρίνονται ανάλογα με τον τρόπο ανάγνωσης. Τα βιομετρικά οπτικής ανάγνωσης χρησιμοποιούν ένα scanner, το οποίο για να διαβάσει το αποτύπωμα, το σαρώνει με φως. Τα βιομετρικά υπέρηχων δεν απαιτούν την επαφή του δαχτύλου με την επιφάνεια, αφού η συσκευή βομβαρδίζει το δάχτυλο με υπέρηχους και λαμβάνει τα ανακλώμενα από αυτό κύματα. Επειδή το ανθρώπινο δάχτυλο δεν είναι λείο, αλλά αποτελείται από όρη και κοιλάδες, ο χρόνος λήψης του ανακλώμενου υπέρηχου εξαρτάται από το πόσο ψηλά είναι τα όρη ή πόσο χαμηλά είναι οι κοιλάδες.



Τα βιομετρικά θερμικής ανάγνωσης αναγνωρίζουν τις διαφορές θερμοκρασίας που έχει το ανθρώπινο δάχτυλο στα διάφορα σημεία του. Τα βιομετρικά αυτά απαιτούν μετακίνηση του ανθρώπινου δαχτύλου στην επιφάνεια του βιοαισθητήρα. Στα πυκνωτικά βιομετρικά ή ανάγνωσης αφής, που χρησιμοποιούν τεχνολογία CMOS, ο αισθητήρας αποτελείται από μικροσκοπικούς πυκνωτές σε μορφή ολοκληρωμένου (σχήμα 1). Η μία πλάκα του κάθε πυκνωτή είναι σταθερή, ενώ οι υπόλοιπες μετακινούνται ανάλογα με το βάθος και το ύψος των ορέων και των κοιλάδων, αλλάζοντας έτσι τη χωρητικότητά του και άρα το ηλεκτρικό ρεύμα στην έξοδό του. Με αυτό τον τρόπο τα όρη και οι κοιλάδες του ανθρώπινου δαχτύλου μετατρέπονται σε ηλεκτρικό σήμα. Κάθε μικροσκοπικός πυκνωτής αντιστοιχεί σε ένα pixel της εικόνας που σχηματίζεται.



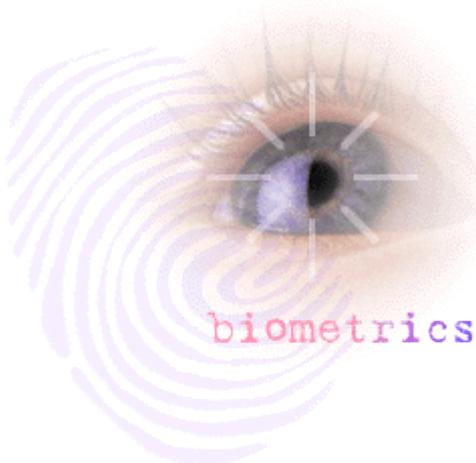
σε ψηφιακή μορφή (σχήμα 2).



Τα βιομετρικά αναγνώρισης ίριδας χρησιμοποιούν ένα κυκλικό πλέγμα, το οποίο επικάθεται στην ίριδα. Μέσω αυτού η κάμερα λαμβάνει ασπρόμαυρες φωτογραφίες και ανάλογα με τις διαβαθμίσεις άσπρου-μαύρου του ματιού, που είναι μοναδικές για κάθε άνθρωπο, επιτυγχάνεται τόσο η εγγραφή, όσο και η πιστοποίηση. Πρέπει να τονίσουμε ότι τα βιομετρικά αναγνώρισης ίριδας ενσωματώνουν στις κάμερες μονάδες Frame Grabber, οι οποίο μετατρέπουν το δείγμα

Το βιομετρικά αναγνώρισης στερεομετρίας παλάμης πραγματοποιούν τρισδιάστατες μετρήσεις, καρπού, παλάμης και δαχτύλων, που περιλαμβάνουν πάχος, επιφάνεια, διαστάσεις και γενικότερα την όλη γεωμετρία της παλάμης (σχήμα 3). Με αυτό τον τρόπο πραγματοποιούνται η εγγραφή και η ταυτοποίηση.

1.3 ΟΙ ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ ΑΝΗΚΟΥΝ ΣΤΟ ΠΑΡΕΛΘΟΝ ΚΑΙ ΑΝΤΙΚΑΘΙΣΤΑΝΤΑΙ ΑΠΟ ΣΥΣΤΗΜΑΤΑ ΒΙΟΜΕΤΡΙΑΣ



Η βιομετρία, η τεχνολογία που προσδιορίζει ηλεκτρονικά τους ανθρώπους από τα φυσικά τους χαρακτηριστικά γνωρίσματα, έχει κάνει μεγάλα άλματα τα τελευταία χρόνια. Είναι έτοιμη η βιομετρική να "πολεμήσει" το παγιωμένο τεχνολογικό κατεστημένο; Ή οι σαρωτές των βολβών του ματιού και των δακτυλικών αποτυπωμάτων, που μπορούν άμεσα να προσδιορίσουν την ταυτότητα ενός προσώπου, θα χρησιμοποιούνται μόνο στις ταινίες του James Bond;

"Σε πέντε χρόνια, οι περισσότεροι άνθρωποι θα χρησιμοποιούν μία βιομετρική συσκευή τουλάχιστον μία φορά την ημέρα. Αυτό ίσως να συμβαίνει στα ATM, στο γραφείο, η κατά την πρόσβασή μας στο διαδίκτυο. Ίσως δημιουργηθεί μία νέα τηλεφωνική συσκευή βιομετρικής αναγνώρισης", υποστηρίζει ο Samir Napanati, συνεργάτης του Διεθνούς Βιομετρικού Οργανισμού, μίας νέας εταιρείας συμβούλων που έχει την έδρα της στη Νέα Υόρκη. Η έρευνα της εταιρείας υπολογίζει ότι η συνολική αγορά για τη βιομετρική ασφάλεια και τα προϊόντα αναγνώρισης ταυτότητας, θα αυξηθεί από 58,4 εκατομμύρια δολάρια το 2002 σε 594 εκατομμύρια δολάρια το 2003. Αλλά η Tere Bracco, αναλυτής της Current Analysis, διατυπώνει μία διαφορετική άποψη, προβλέποντας την αγορά σε 250 ή 300 εκατομμύρια δολάρια. Αν και η βιομετρική τεχνολογία θα παραμείνει μία μικρή αγορά, οι επιχειρήσεις ψάχνουν ακόμα τις νέες εφαρμογές που θα ωθήσουν τις πωλήσεις τους. Πολλές περιοχές ενδιαφέροντος δεν είναι τόσο προκλητικές όσο οι παραδοσιακές βιομετρικές εφαρμογές, όπως η προστασία των πυρηνικών εγκαταστάσεων και οι εφαρμογές διατήρησης στρατιωτικών απορρήτων.

Η βιομετρική εταιρία του Τέξας Biometric Access Corp., επιχείρηση που κατασκευάζει συσκευές αναγνώρισης δακτυλικών αποτυπωμάτων, προάγει τα προϊόντα της στηριζόμενη στην ευκολία χρήσης τους. Ο Hal Jennings, ο πρόεδρος του τμήματος μάρκετινγκ και τεχνικής υποστήριξης, λέει πως "προωθούν τις συσκευές αναγνώρισης δακτυλικών αποτυπωμάτων ως υποκατάστατα των κωδικών πρόσβασης. Χρησιμοποιώντας τη δακτυλοσκόπηση για την ανίχνευση των υπαλλήλων, κατά την είσοδό τους στους υπολογιστές, οι επιχειρήσεις δεν έχουν να ασχολούνται πλέον με τις τακτικές αλλαγές των κωδικών πρόσβασης. "Πολλοί άνθρωποι θεωρούν τη βιομετρική ως σίγουρο μηχανισμό ασφάλειας, αλλά ταυτόχρονα παρέχει και μεγάλη ευκολία κατά τη χρήση της. Είναι γνωστό ότι οι αλλαγές στους κωδικούς πρόσβασης αποτελεί μία αγγαρεία για τους υπαλλήλους ενώ μερικές φορές ξεχνούν να τους αλλάζουν".

Η Bracco, θεωρεί ότι το άμεσο μέλλον της βιομετρικής βρίσκεται στους ανιχνευτές δακτυλικών αποτυπωμάτων για βιομηχανίες σχετικές με την υγειονομική περίθαλψη, τις ασφαλιστικές εταιρείες και τους δικηγόρους, όπου η ασφάλεια είναι υψίστης σημασίας. "Σκέφτομαι ότι μια γρήγορη, απλή ανίχνευση είναι πολύ ευκολότερη και ασφαλέστερη από τους μεγάλους κωδικούς πρόσβασης τους οποίους οι άνθρωποι θα γράψουν και συνήθως θα ξεχάσουν", είπε. Η εξασφάλιση ασφάλειας στο ηλεκτρονικό εμπόριο, είναι επίσης ένας τομέας με αυξανόμενο

ενδιαφέρον για τη βιομετρική βιομηχανία. "Ένα από τα συστήματα που αναπτύσσουμε αυτή τη στιγμή είναι η απευθείας σύνδεση σπιτιού-μεσιτών", λέει ο Nanavati. "Πριν εισέλθετε στην ιστοσελίδα και κάνετε οποιαδήποτε αγορά σας ζητάνε να χρησιμοποιήσετε έναν κωδικό πρόσβασης και ένα όνομα χρηστών. Σύντομα θα είστε σε θέση να αναγνωριστείτε μόνο με ανίχνευση των δαχτύλων σας."

Οποιαδήποτε είναι η εφαρμογή, τα βιομετρικά συστήματα αναγνώρισης ταυτότητας απαιτούν μία υποδομή (κατάλληλες συσκευές). Η Veronique Wittebolle, πρόεδρος της βιομετρικής εταιρείας εφαρμογών Keyware Technologies, ψάχνει τρόπους για να δημιουργήσει εφαρμογές με χρήση υποδομών που ήδη χρησιμοποιούνται ευρέως. Παραδείγματος χάριν, οι ψηφιακές φωτογραφικές μηχανές Wittebolle λαμβάνουν φωτογραφίες που μπορούν να αποσταλούν με το ηλεκτρονικό ταχυδρομείο, ενώ ταυτόχρονα μπορούν να λειτουργήσουν από κοινού με το λογισμικό που επιτρέπει στον υπολογιστή της να αναγνωρίσει το πρόσωπό της. Και οι ευρέως χρησιμοποιούμενες συσκευές αναγνώρισης λόγου, μπορούν να ελέγχουν ακόμα και την ταυτότητα ενός προσώπου μόνο από τη φωνή. "Η υποδομή είναι σημαντική", είπε. "Εάν μπορείτε να τη χρησιμοποιήσετε για άλλα πράγματα εκτός από την αναγνώριση, είστε στην σωστή αφετηρία."

1.4 ΑΠΟ ΤΗΝ ΠΛΑΣΤΙΚΗ ΤΑΥΤΟΤΗΤΑ ΣΤΙΣ ΒΙΟΜΕΤΡΙΚΕΣ ΜΕΘΟΔΟΥΣ

Αν προσπαθούσαμε να κατατάξουμε τα είδη των συστημάτων ασφαλείας με βάση την αποδοτικότητά τους θα καταλήγαμε σίγουρα στο εξής συμπέρασμα: στο χαμηλότερο επίπεδο ασφάλειας είναι τα συστήματα όπου το προς αναγνώριση άτομο είναι κάτοχος κάποιου αναγνωριστικού όπως μία ταυτότητα με φωτογραφία. Τέτοια συστήματα βρίθουν κυριολεκτικά μειονεκτημάτων, αφού το αναγνωριστικό μπορεί να χαθεί, καταστραφεί ή και να παραποιηθεί ή αναπαραχθεί πολύ εύκολα στα χέρια κάποιου ειδικού. Ένα από τα βασικότερα μειονεκτήματα του συστήματος είναι το γεγονός ότι σε καμία περίπτωση ο ελεγκτής δεν μπορεί να είναι σίγουρος ούτε αν το αναγνωριστικό είναι γνήσιο ούτε αν ο κομιστής του είναι αληθινός.

Στο αμέσως επόμενο επίπεδο βρίσκονται τα συστήματα όπου ο χρήστης γνωρίζει κάτι, όπως έναν κωδικό αριθμό ή ένα συνθηματικό. Εδώ τα πράγματα είναι κάπως καλύτερα αλλά το κύριο πρόβλημα παραμένει με κάποια παραλλαγή: Ενώ το μέσο αναγνώρισης (ο κωδικός ή το συνθηματικό) δεν υπάρχει περίπτωση να είναι πλαστό, κανένας δεν μπορεί να διαβεβαιώσει τον ελεγκτή ότι αυτός που το κομίζει είναι το σωστό άτομο.

Στο τρίτο επίπεδο υπάρχουν τα συστήματα που αποτελούν συνδυασμό των δύο προηγούμενων. Εδώ, όπως μπορείτε να καταλάβετε, κατατάσσεται το σύστημα των τραπεζικών καρτών με τα PINs. Αν και υπάρχει σαφής βελτίωση στην αποτελεσματικότητα κανένα τέτοιο σύστημα δεν είναι απολύτως αδιάβλητο. Στο τελευταίο επίπεδο, αυτό της υψηλότερης ασφάλειας, η αναγνώριση γίνεται από κάτι το οποίο ο χρήστης είναι (βιομέτρηση με βάση φυσικό χαρακτηριστικό) ή από κάτι που ο χρήστης κάνει (βιομέτρηση με βάση συμπεριφορά). Τα δακτυλικά αποτυπώματα για παράδειγμα είναι μοναδικά για κάθε άνθρωπο. Γιατί λοιπόν να είστε υποχρεωμένοι να πληκτρολογείτε το PIN σας κάθε φορά που πηγαίνετε στην τράπεζα για να κάνετε ανάληψη από το ATM, ενώ θα μπορούσατε απλώς να τοποθετείτε τον αντίχειρά σας στην ειδική υποδοχή; Στο κάτω κάτω είναι πιθανό την κάρτα σας να τη χάσετε, το PIN σας -κάλλιστα- να το ξεχάσετε αλλά το

δάχτυλό σας σίγουρα θα το έχετε πάντα μαζί σας! Και το πιο σημαντικό: Δεν μπορεί να το έχει κανένας άλλος εκτός από εσάς.

Αποτελούν λοιπόν οι βιομετρικές μέθοδοι τα τέλεια συστήματα ασφάλειας;

Δυστυχώς, κανένα σύστημα δεν είναι τέλειο. Τα φυσικά χαρακτηριστικά των ανθρώπων αλλάζουν, είτε από το χρόνο είτε από αστάθμητους παράγοντες, όπως τα ατυχήματα. Αν το παραπάνω σενάριο με το ATM σας φάνηκε ελκυστικό, φανταστείτε πως σε περίπτωση που ο αντιχειράς σας τραυματιζόταν με κάποιο τρόπο, πιθανώς θα χρειαζόταν να αρχίσετε να ψάχνετε για δανεικά, αφού το μηχάνημα δεν θα μπορούσε να αναγνωρίσει πια το δακτυλικό σας αποτύπωμα. Παρόμοιο πρόβλημα θα είχε και ο εργάτης που θα δοκίμαζε να κάνει ανάληψη με τα χέρια του υπερβολικά λερωμένα από τη δουλειά. Υπάρχουν βέβαια και τα βιομετρικά συστήματα βάσει συμπεριφορών, όπως η διακρίβωση της υπογραφής και ο ρυθμός πληκτρολόγησης. Αυτά όπως μπορείτε να φανταστείτε, μειονεκτούν πολύ περισσότερο έναντι των συστημάτων φυσικών χαρακτηριστικών αφού οι συμπεριφορές αλλάζουν πολύ πιο εύκολα. Για παράδειγμα, καθώς ο άνθρωπος γερνά αλλάζει ο τρόπος υπογραφής του. Ή για να δώσουμε ένα πολύ πιο βραχυπρόθεσμο παράδειγμα, η κούραση μπορεί να μεταβάλλει το ρυθμό πληκτρολόγησης ενός ατόμου κατά τη διάρκεια μίας και μόνο ημέρας.

Εκτός από τα παραπάνω προβλήματα, οι ειδικοί της βιομετρικής έχουν να δώσουν απάντηση σε ένα σωρό άλλα ζητήματα τα οποία κρίνουν τελικά τη βιωσιμότητα κάθε μεθόδου και καθορίζουν τα πεδία εφαρμογών της. Ένα από τα σημαντικότερα θέματα είναι η αποδοχή που βρίσκει ένα βιομετρικό σύστημα από το κοινό. Για να ξαναγυρίσουμε στο παράδειγμα της τράπεζας, ένας σημαντικός λόγος να μη δείτε τελικά ποτέ ένα σύστημα δακτυλικών αποτυπωμάτων σε ATM, είναι γιατί το κοινό έχει συνδέσει παρόμοια συστήματα με ποινικές πρακτικές και διαδικασίες. Κάποιοι πελάτες λοιπόν μπορεί να νοιώσουν πως η τράπεζα τους μεταχειρίζεται σαν εγκληματίες και να "αποσύρουν" -μαζί με τις καταθέσεις τους ασφαλώς- την εμπιστοσύνη τους από αυτήν.

Το θέμα της ακρίβειας είναι και αυτό πολύ βασικό. Πόσο "αυστηρό" πρέπει να είναι ένα βιομετρικό σύστημα; Η προφανής απάντηση "όσο περισσότερο γίνεται" είναι μάλλον λανθασμένη. Ένα πολύ αυστηρό σύστημα είναι αρκετά ευαίσθητο στις μικρές αλλοιώσεις των φυσικών χαρακτηριστικών ή των συμπεριφορών που προαναφέραμε με αποτέλεσμα να ρισκάρει λανθασμένες απορρίψεις. Από την άλλη πλευρά, ένα υπέρμετρα χαλαρό σύστημα θα ενείχε το -σημαντικότερο σίγουρα- κίνδυνο των λανθασμένων αποδοχών. Τέλος, η προσπάθεια που απαιτείται από το χρήστη του συστήματος δεν θα μπορούσε παρά να ήταν και αυτή σημαντικός παράγοντας, ο οποίος μάλιστα συνδέεται άμεσα με την αποδοχή που θα βρει το σύστημα από το κοινό. Ένα σύστημα που θα απαιτούσε ιδιαίτερο κόπο και χρόνο από τους χρήστες του σίγουρα δεν θα ήταν ιδιαίτερα δημοφιλές.

1.5 ΕΦΑΡΜΟΓΕΣ

Όπως ήδη γνωρίζουμε, τα ανά τον κόσμο αστυνομικά σώματα χρησιμοποιούν εδώ και χρόνια τα δακτυλικά αποτυπώματα ως μέσο αναγνώρισης ταυτότητας. Το AFIS (Automated Fingerprint Identification System - Αυτοματοποιημένο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων) αποτελεί πλέον ένα από τα πιο χρήσιμα εργαλεία στα χέρια των ανθρώπων που είναι υπεύθυνοι για την επιβολή και την τήρηση του νόμου. Δεν είναι λοιπόν παράξενο, το γεγονός ότι οι νεότερες βιομετρικές μέθοδοι βρίσκουν το μεγαλύτερο πεδίο εφαρμογής τους εκεί. Φυλακές,

αστυνομικά τμήματα και κεντρικά γραφεία εξοπλίζονται με τα νέα συστήματα συμβάλλοντας έτσι στην εξάλειψη ορισμένων παλαιών πρακτικών απόδρασης κρατουμένων (π.χ. ανταλλαγή θέσεων με κάποιον επισκέπτη) και ταυτόχρονα βοηθώντας τα μέγιστα στο έργο της αστυνόμευσης. Εκτός όμως από αυτές τις προφανείς εφαρμογές, οι βιομετρικές μέθοδοι τείνουν να μπου για τα καλά στην καθημερινή ζωή μας και μάλιστα με πολλούς τρόπους. Η βιομετρική είναι μια γρήγορα εξελισσόμενη τεχνολογία που έχει χρησιμοποιηθεί ευρέως στις ιατροδικαστικές, όπως η εγκληματική ασφάλεια προσδιορισμού και φυλακών. Πρόσφατες πρόοδοι στους βιομετρικούς αισθητήρες και τους αντίστοιχους αλγόριθμους έχουν οδηγήσει στην επέκταση της βιομετρικής επικύρωσης σε έναν μεγάλο αριθμό πολιτικών εφαρμογών. Η βιομετρική μπορεί να χρησιμοποιηθεί για να αποτρέψει την αναρμόδια πρόσβαση σε ATMs, κυψελοειδή τηλέφωνα, έξυπνες κάρτες, τον υπολογιστή γραφείου PCs, τους τερματικούς σταθμούς και τα δίκτυα υπολογιστών. Μπορεί να χρησιμοποιηθεί κατά τη διάρκεια των συναλλαγών που διευθύνονται μέσω του τηλεφώνου και του διαδικτύου (ηλεκτρονικό εμπόριο και ηλεκτρονικές τραπεζικές εργασίες).

ATM: Η βιομετρική μπορεί αν όχι ακόμη να αντικαταστήσει πλήρως, τουλάχιστον να βελτιώσει, το υπάρχον σύστημα ελέγχου πρόσβασης μέσω των καρτών με τα PINs σε αυτόματες ταμειακές μηχανές. Προσθέτοντας στην όλη διαδικασία το βιομετρικό έλεγχο εξαλείφεται ουσιαστικά η περίπτωση ο αιτών την πρόσβαση στο σύστημα να μην είναι ο πραγματικός δικαιούχος.

Ψηφοφορίες: Εκτός του ότι η εφαρμογή βιομετρικών μεθόδων σε ψηφοφορίες προσθέτει στη διαδικασία εξαιρετικά μεγάλη αποτελεσματικότητα και ευελιξία, βοηθά επίσης στην οριστική εξαφάνιση φαινομένων νοθείας του αποτελέσματος (διπλοί ψήφοι κ.λπ.). Αν και η εφαρμογή ενός τέτοιου συστήματος σε εθνικές εκλογές είναι ακόμα μη πραγματοποιήσιμη και πιθανώς να περάσουν πάρα πολλά χρόνια έως ότου καταστεί δυνατή, ψηφοφορίες μικρότερης κλίμακας με χρήση βιομετρήσεων έχουν αρχίσει ήδη να διενεργούνται στην Αμερική.

Internet: Καθώς το ηλεκτρονικό εμπόριο αναπτύσσεται αφήνοντας πίσω τη νηπιακή ηλικία του, το πρόβλημα της ασφάλειας των εμπορικών συναλλαγών μέσω Internet γίνεται όλο και πιο έντονο. Η χρήση της πιστωτικής κάρτας για την αγορά κάποιου προϊόντος πάντα μας δημιουργεί σκεπτικισμό σχετικά με το πόσο ασφαλής είναι μια τέτοια συναλλαγή. Σε ένα σύστημα όμως, όπου ο αριθμός της κάρτας θα συνοδεύονταν από ένα βιομετρικό δείγμα του κατόχου της τα πράγματα θα ήταν πολύ διαφορετικά. Φανταστείτε το εξής σενάριο: Εντοπίσατε επιτέλους το βιβλίο που ψάχνατε για μήνες και πληκτρολογείτε τα στοιχεία σας και τον αριθμό της κάρτας σας στη φόρμα παραγγελίας. Καθώς πατάτε στο κουμπί "Submit" εμφανίζεται ένα μήνυμα που σας προτρέπει να απαγγείτε μία συγκεκριμένη φράση ή λέξη στο μικρόφωνο του υπολογιστικού συστήματός σας. Καλύτερα να φροντίσετε να μην είστε βραχνιασμένοι, λοιπόν!

Ασφάλεια σε δίκτυα: Δεν χρειάζεται να αναλύσουμε εδώ πόσο σημαντικό είναι το θέμα της πρόσβασης σε μεγάλα δίκτυα υπολογιστών. Τα σημερινά συστήματα ασφάλειας με τα συνθηματικά έχουν αποδειχθεί άκρως ανεπαρκή να αποτρέψουν οποιονδήποτε έχει κάποιες γνώσεις και την επιθυμία να παραβιάσει το σύστημα. Αν και δεν πρόκειται να αποτελέσουν πανάκεια, τα βιομετρικά συστήματα σίγουρα θα βελτιώσουν κατά πολύ την υπάρχουσα κατάσταση.

Προσωπικά υπολογιστικά συστήματα: Με τους ταπεινούς προσωπικούς μας υπολογιστές τι γίνεται; Σίγουρα όλοι έχουμε έγγραφα στο δίσκο μας που θεωρούμε αρκετά σημαντικά και προσωπικά ώστε να θέλουμε να μην είναι διαθέσιμα στον καθένα. Ο υπολογιστής του γραφείου μας είναι ακόμα πιο

εκτεθειμένος στις ορέξεις οποιουδήποτε θελήσει να γίνει αδιάκριτος. Όπως όμως αναφέραμε, πολλές εταιρίες βιομετρικών συστημάτων έχουν κάνει ήδη μεγάλα ανοίγματα στην αγορά των προσωπικών υπολογιστών. Τα προϊόντα που έχουν κυκλοφορήσει είναι συνήθως ένας συνδυασμός hardware και software και διακρίνονται από δύο χαρακτηριστικά: (1) έχουν ελάχιστες απαιτήσεις συστήματος, που σημαίνει ότι μπορούν άνετα να τοποθετηθούν και στο μικρότερο μηχάνημα και (2) κοστίζουν ελάχιστα (για παράδειγμα, πολλά από αυτά κοστίζουν όχι περισσότερο από έναν σκληρό δίσκο) που σημαίνει ότι μπορούν να αγοραστούν από τον οποιονδήποτε χρήστη.

Στα κεφάλαια που ακολουθούν θα αναφερθούμε στα πλέον διαδεδομένα βιομετρικά συστήματα ξεχωριστά, αναλύοντας με λεπτομέρειες ζητήματα όπως οι βασικές αρχές λειτουργίας τους, οι διαφορές τους από τις υπόλοιπες βιομετρικές μεθόδους, το πεδίο εφαρμογών στο οποίο απευθύνονται αλλά και η αποδοχή που βρίσκουν από το κοινό. Αναφορές θα βρείτε επίσης στα διάφορα προϊόντα που κυκλοφορούν στην αγορά, καθώς επίσης στις εταιρίες που ειδικεύονται σε αυτόν τον τομέα.

ΚΕΦΑΛΑΙΟ 2

ΔΑΚΤΥΛΙΚΑ
ΑΠΟΤΥΠΩΜΑΤΑ

Χωρίς να προσφέρουν τη μέγιστη ακρίβεια, τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων αποτελούν μία πολύ αξιόπιστη μέθοδο εξακρίβωσης ταυτότητας. Άλλωστε, πώς θα μπορούσε να είναι διαφορετικά όταν τα δακτυλικά αποτυπώματα χρησιμοποιούνται πολλά χρόνια γι' αυτήν τη δουλειά με τεράστια επιτυχία; Ακριβώς αυτό το γεγονός όμως, η χρήση δηλαδή των δακτυλικών αποτυπωμάτων αποκλειστικά για ποινικούς σκοπούς μέχρι σήμερα, ίσως είναι η μεγαλύτερη τροχοπέδη στη διάδοση των βιομετρικών συστημάτων που βασίζονται σε αυτά. Χρόνια τώρα, στη συνείδηση του κόσμου τα δακτυλικά αποτυπώματα ταυτίζονται με την αναγνώριση κακοποιών και, γενικά, με μεθόδους και πρακτικές αστυνόμευσης. Η ταύτιση αυτή, λοιπόν, αναμένεται να επηρεάσει πολλούς ανθρώπους, οι οποίοι πιθανώς να αντιδράσουν αρνητικά σε ένα σύστημα που τους ζητά το δακτυλικό αποτύπωμά τους, πιστεύοντας ότι αντιμετωπίζονται ως εγκληματίες. Πρόκειται ίσως για το σημαντικότερο λόγο που η αποδοχή εκ μέρους του κοινού των βιομετρικών συστημάτων του είδους είναι μεσαία, παρ' όλα τα πλεονεκτήματα που έχουν σε σχέση με τα υπόλοιπα. Για του λόγου το αληθές, ας δούμε αναλυτικότερα μερικά από αυτά.

Ενώ οι υπόλοιπες βιομετρικές μέθοδοι είναι σχετικά μικρής ηλικίας και έχουν ακόμα πολλά προβλήματα να λύσουν, τα δακτυλικά αποτυπώματα κλείνουν σχεδόν έναν αιώνα πρακτικής εφαρμογής. Ο συνδυασμός της νέας τεχνολογίας, λοιπόν, με τη μελέτη που έχει κάνει ο άνθρωπος όλα αυτά τα χρόνια πάνω στο θέμα δεν μπορεί παρά να προσφέρει τα καλύτερα δυνατά αποτελέσματα. Ακριβώς αυτή η σε βάθος τεχνογνωσία αλλά και το γεγονός ότι το είδος των συγκεκριμένων βιομετρήσεων δεν απαιτεί υπερβολικά ακριβό εξοπλισμό έκαναν έναν μεγάλο αριθμό εταιριών να στρέψουν εκεί την προσοχή τους. Αυτή τη στιγμή γύρω στις 70 εταιρίες ασχολούνται με τις βιομετρικές μεθόδους δακτυλικών αποτυπωμάτων, ενώ ο αντίστοιχος αριθμός για τη μέθοδο εξέτασης ίριδας είναι μόλις 2. Έτσι, δεν αποτελεί έκπληξη το γεγονός ότι τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων έχουν στην αγορά τη μεγαλύτερη ποικιλία προϊόντων από ό,τι οποιοδήποτε άλλο σύστημα. Ιδιαίτερο ενδιαφέρον για τους χρήστες ηλεκτρονικών υπολογιστών έχει το γεγονός ότι πάρα πολλά από αυτά τα προϊόντα συνδέονται σε υπολογιστή και μέσω ειδικού software αναλαμβάνουν την προστασία του (για περισσότερες λεπτομέρειες δείτε την ενότητα "Προϊόντα για το PC σας"). Τέλος, δεν πρέπει να παραλείψουμε να αναφέρουμε ότι, σε σχέση με άλλες βιομετρικές μεθόδους, τα δακτυλικά αποτυπώματα απαιτούν ελάχιστη προσπάθεια από το χρήστη, όση δηλαδή χρειάζεται για την τοποθέτηση του αντίχειρά του στην ειδική υποδοχή.

Ασφαλώς, υπάρχουν και μειονεκτήματα. Από τα σοβαρότερα είναι το γεγονός ότι η σωστή "ανάγνωση" των δακτυλικών αποτυπωμάτων δυσκολεύει πολύ κάτω από ειδικές (αλλά όχι και τόσο σπάνιες) συνθήκες, όπως βρώμικα δάχτυλα, τραυματισμοί στα χέρια, πολύ ξηρό ή πολύ λιπαρό δέρμα. Ακόμα, ο τρόπος με τον οποίο ο χρήστης αλληλεπιδρά με το σύστημα μπορεί να προκαλέσει προβλήματα. Για παράδειγμα, υπερβολική πίεση του δαχτύλου μπορεί να έχει ως αποτέλεσμα λανθασμένη λήψη του αποτυπώματος. Οι διάφοροι κατασκευαστές προσπαθούν να ξεπεράσουν τα προβλήματα εξελίσσοντας τις υπάρχουσες μεθόδους ανάγνωσης και δημιουργώντας άλλες εντελώς καινούριες, όπως η μέθοδος των ακουστικών κυμάτων.

2.1 ΣΥΣΤΗΜΑΤΑ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ

Τα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων χωρίζονται, καταρχήν, σε δύο κατηγορίες: Στην πρώτη κατηγορία τοποθετούνται αυτά που κάνουν εξακρίβωση ταυτότητας (ονομάζονται και AFIS - Automatic Fingerprint Identification Systems), ενώ στη δεύτερη εκείνα που κάνουν απλή επιβεβαίωση. Αν και αυτή η διάκριση ισχύει για όλα τα βιομετρικά συστήματα, στα δακτυλικά αποτυπώματα είναι πολύ πιο έντονη λόγω των διαφορών που υπάρχουν στη διαδικασία, τις μεθόδους που χρησιμοποιούνται αλλά και στον απαραίτητο εξοπλισμό. Επίσης, λόγω του γεγονότος ότι μέχρι τώρα τα δακτυλικά αποτυπώματα χρησιμοποιούνταν μόνο για ποινικούς σκοπούς, συνήθως τα σημερινά συστήματα υπόκεινται σε μία περαιτέρω διάκριση, αυτήν της ποινικής ή πολιτικής χρήσης. Όσον αφορά στις μεθόδους ανάγνωσης, σήμερα έχουν ήδη αναπτυχθεί αρκετές, φιλοδοξώντας να λύσουν πολλά από τα προβλήματα που προαναφέρθηκαν. Στη συνέχεια θα δούμε αναλυτικότερα τις σημαντικότερες.

Οπτική ανάγνωση: Η παλαιότερη και πλέον δοκιμασμένη μέθοδος, μοιάζει αρκετά με τη διαδικασία των κοινών scanners. Ο χρήστης αρχικά τοποθετεί το δάχτυλό του σε μία γυάλινη πλάκα. Στη συνέχεια, και αφού η άκρη του δαχτύλου φωτιστεί κατάλληλα, λαμβάνεται η εικόνα του δακτυλικού αποτυπώματος. Οι οπτικοί αναγνώστες δακτυλικών αποτυπωμάτων είναι σήμερα οι πιο συνηθισμένοι. Τα τελευταία χρόνια, εκμεταλλευόμενοι την ανάπτυξη της τεχνολογίας, γίνονται ολοένα μικρότεροι σε μέγεθος αλλά και πιο φθηνοί. Δυστυχώς, είναι και οι πιο επιρρεπείς σε προβλήματα, όταν οι συνθήκες λήψης του αποτυπώματος δεν είναι οι καλύτερες.

Ανάγνωση με υπέρηχους: Η μέθοδος αυτή χρησιμοποιεί ακουστικά κύματα μη αντιληπτά από το ανθρώπινο αυτί. Τα κύματα αυτά "βομβαρδίζουν" το δάκτυλο του χρήστη μετρώντας την πυκνότητα των δακτυλικών του αποτυπωμάτων. Το εμφανές πλεονέκτημα της μεθόδου σε σχέση με τις υπόλοιπες είναι ότι δεν απαιτεί άμεση επαφή του δαχτύλου με τον scanner. Κάτι τέτοιο απλώς σημαίνει ότι δεν επηρεάζεται από πολύ βρώμικα δάχτυλα ή ακόμα και από λεπτά γάντια!

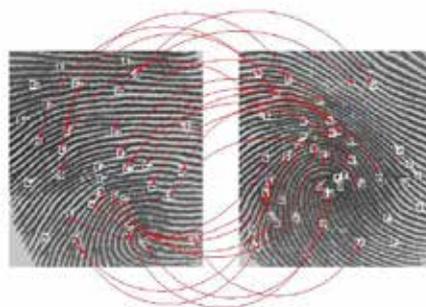
Θερμική ανάγνωση και ανάγνωση αφής: Χρησιμοποιώντας εξελιγμένα chips, αυτές οι μέθοδοι θεωρούνται εξαιρετικά ακριβείς. Ο χρήστης τοποθετεί το δάκτυλό του σε κάποιον αισθητήρα, ο οποίος συλλαμβάνει τη θερμότητα ή την πίεση από το δάχτυλο και τη μετατρέπει σε δεδομένα.

2.2 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ

Μεταξύ όλων των βιομετρικών τεχνικών, το αποτύπωμα, βασισμένο στον προσδιορισμό είναι η παλαιότερη μέθοδος που έχει χρησιμοποιηθεί επιτυχώς σε πολυάριθμες εφαρμογές. Καθένας έχει μοναδικά, αμετάβλητα δακτυλικά αποτυπώματα. Ένα δακτυλικό αποτύπωμα αποτελείται από μια σειρά κορυφογραμμών στην επιφάνεια του δάχτυλου. Η μοναδικότητα ενός δακτυλικού αποτυπώματος μπορεί να καθοριστεί από το σχέδιο των κορυφογραμμών καθώς επίσης και των σημείων μικρολεπτομερειών. Τα σημεία μικρολεπτομερειών είναι τοπικά χαρακτηριστικά κορυφογραμμών που εμφανίζονται είτε σε μια διακλάδωση κορυφογραμμών είτε ένα τελείωμα κορυφογραμμών.



Οι τεχνικές δακτυλικών αποτυπωμάτων μπορούν να τοποθετηθούν σε δύο κατηγορίες: στις μικρολεπτομέρειες και στο συσχετισμό. Οι μικρολεπτομέρειες τεχνικές βρίσκουν αρχικά τα σημεία μικρολεπτομερειών και χαρτογραφούν έπειτα τη σχετική τοποθέτησή τους στο δάχτυλο. Εντούτοις, υπάρχουν μερικές δυσκολίες κατά τη χρησιμοποίηση αυτής της προσέγγισης. Είναι δύσκολο να εξαχθούν τα σημεία μικρολεπτομερειών ακριβώς όταν είναι το δακτυλικό αποτύπωμα χαμηλής ποιότητας. Επίσης αυτή η μέθοδος δεν λαμβάνει υπόψη το σφαιρικό σχέδιο των κορυφογραμμών. Η μέθοδος του συσχετισμού είναι σε θέση να υπερνικήσει μερικές από τις δυσκολίες της μικρολεπτομέρους προσέγγισης. Εντούτοις, έχει μερικές από τις ανεπάρκειές του. Η μέθοδος του συσχετισμού απαιτεί την ακριβή θέση ενός σημείου εγγραφής και επηρεάζεται από τη μετάφραση και την περιστροφή εικόνας.



Το ταίριασμα δακτυλικών αποτυπωμάτων βασισμένο στις μικρολεπτομέρειες έχει προβλήματα στο ταίριασμα των διαφορετικών μεγεθών (μη καταγεγραμμένων) σχεδίων μικρολεπτομερειών. Οι τοπικές δομές κορυφογραμμών δεν μπορούν να χαρακτηριστούν εντελώς από τις μικρολεπτομέρειες. Δοκιμάζουμε μια εναλλακτική αντιπροσώπευση δακτυλικών αποτυπωμάτων που θα συλλάβει περισσότερες τοπικές πληροφορίες και θα παραγάγει έναν σταθερό κώδικα μήκους για το δακτυλικό αποτύπωμα.

Αναπτύσσουμε αλγορίθμους που είναι πιο γεροί στο θόρυβο της εικόνας δακτυλικών αποτυπωμάτων και παρέχουν μεγάλη ακρίβεια στον πραγματικό χρόνο. Ένα εμπορικό αποτύπωμα-βασισμένο στο σύστημα επικύρωσης απαιτεί ένα πολύ χαμηλό ψεύτικο ποσοστό απόρριψης (FRR) για ένα δεδομένο ψεύτικο ποσοστό αποδοχής (FAR). Αυτό είναι πολύ δύσκολο να επιτευχθεί με οποιαδήποτε τεχνική. Ερευνάμε τις μεθόδους για να συγκεντρώσουμε τα στοιχεία από τις διάφορες τεχνικές για να αυξήσουμε τη γενική ακρίβεια του συστήματος. Σε μια πραγματική εφαρμογή, ο αισθητήρας, το σύστημα αποκτήσεων και η παραλλαγή στην απόδοση του συστήματος κατά τη διάρκεια του χρόνου είναι πολύ κρίσιμοι. Είμαστε επίσης ο τομέας που εξετάζει το σύστημά μας σε έναν περιορισμένο

αριθμό χρηστών για να αξιολογήσουμε την απόδοση των συστημάτων για μια χρονική περίοδο.

2.2.1 ΤΑΞΙΝΟΜΗΣΗ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ

Οι μεγάλοι όγκοι των δακτυλικών αποτυπωμάτων συλλέγονται και αποθηκεύονται καθημερινά σε ένα ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένων των ιατροδικαστικών, του ελέγχου πρόσβασης και της εγγραφής αδειών οδηγών. Μια αυτόματη αναγνώριση ανθρώπων βασισμένη στα δακτυλικά αποτυπώματα απαιτεί ότι το δακτυλικό αποτύπωμα εισαγωγής αντιστοιχείται με έναν μεγάλο αριθμό δακτυλικών αποτυπωμάτων σε μια βάση δεδομένων (η βάση δεδομένων FBI περιέχει περίπου 70 εκατομμύρια δακτυλικά αποτυπώματα!). Για να μειώσει το χρόνο αναζήτησης και την υπολογιστική πολυπλοκότητα, είναι επιθυμητό να ταξινομηθούν αυτά τα δακτυλικά αποτυπώματα κατά τρόπο ακριβή και συνεπή έτσι ώστε το δακτυλικό αποτύπωμα εισαγωγής πρέπει για να αντιστοιχηθεί μόνο με ένα υποσύνολο των δακτυλικών αποτυπωμάτων στη βάση δεδομένων.



Η ταξινόμηση δακτυλικών αποτυπωμάτων είναι μια τεχνική που ορίζει ένα δακτυλικό αποτύπωμα σε έναν από τους διάφορους προ-διευκρινισμένους τύπους που καθιερώθηκαν ήδη στη λογοτεχνία που μπορεί να παρέχει ένα ευρετήριο μηχανισμών. Η ταξινόμηση δακτυλικών αποτυπωμάτων μπορεί να αντιμετωπισθεί ως χονδροειδές ταίριασμα επιπέδων των δακτυλικών αποτυπωμάτων. Ένα δακτυλικό αποτύπωμα εισαγωγής αρχικά αντιστοιχείται με ένα χονδροειδές επίπεδο σε έναν από τους προ-διευκρινισμένους τύπους και έπειτα, σε λεπτότερο επίπεδο συγκρίνεται με το υποσύνολο της βάσης δεδομένων που περιέχει εκείνο τον τύπο δακτυλικών αποτυπωμάτων. Έχουμε αναπτύξει έναν αλγόριθμο για να ταξινομήσουμε τα δακτυλικά αποτυπώματα σε πέντε κατηγορίες, τη σπείρα, το σωστό βρόχο, τον αριστερό βρόχο και την αψίδα. Ο αλγόριθμος χωρίζει τον αριθμό κορυφογραμμών σε τέσσερις κατευθύνσεις (0 βαθμός, 45 βαθμοί, 90 βαθμοί, και 135 βαθμοί) με το φιλτράρισμα του κεντρικού μέρους ενός δακτυλικού αποτυπώματος, με μια τράπεζα των φίλτρων του Gabor. Αυτές οι πληροφορίες κβαντοποιούνται για να παραγάγουν ένα FingerCode που χρησιμοποιείται για την ταξινόμηση. Η ταξινόμησή μας είναι βασισμένη σε ένα δύο-σταδίων ταξινομητή που χρησιμοποιεί έναν κοντινό ταξινομητή στο πρώτο στάδιο και ένα σύνολο νευρικών δικτύων στο δεύτερο στάδιο. Ο ταξινομητής εξετάζεται σε 4.000 εικόνες στη βάση δεδομένων NIST-4. Για ένα πρόβλημα πέμπτης-κατηγορίας, επιτυγχάνεται 90% ακρίβεια ταξινόμησης. Για ένα πρόβλημα

τέταρτης-κατηγορίας είμαστε σε θέση να επιτύχουμε μια ακρίβεια ταξινόμησης 94.8%. Με την ενσωμάτωση μιας επιλογής απόρριψης, η ακρίβεια ταξινόμησης μπορεί να αυξηθεί σε 96% για την ταξινόμηση πέμπτης-κατηγορίας και σε 97,8% για την ταξινόμηση τέταρτης-κατηγορίας όταν απορρίπτεται 30,8% των εικόνων.

2.2.2 ΑΥΞΗΣΗ ΕΙΚΟΝΑΣ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ

Ένα κρίσιμο βήμα στο αυτόματο ταίριασμα δακτυλικών αποτυπωμάτων είναι η αυτόματα απόσπαση μικρολεπτομερειών από τις εικόνες δακτυλικών αποτυπωμάτων εισαγωγής. Εντούτοις, η απόδοση ενός αλγορίθμου εξαγωγής μικρολεπτομερειών στηρίζεται σε μεγάλο ποσοστό στην ποιότητα των εικόνων δακτυλικών αποτυπωμάτων εισαγωγής. Προκειμένου να εξασφαλιστεί ότι η απόδοση ενός αυτόματου συστήματος προσδιορισμού / επαλήθευσης δακτυλικών αποτυπωμάτων θα είναι γερή όσον αφορά την ποιότητα των εικόνων δακτυλικών αποτυπωμάτων, είναι ουσιαστικό να ενσωματωθεί ένας αλγόριθμος αυξήσεων δακτυλικών αποτυπωμάτων στην ενότητα εξαγωγής μικρολεπτομερειών. Έχουμε αναπτύξει έναν γρήγορο αλγόριθμο αυξήσεων δακτυλικών αποτυπωμάτων, ο οποίος μπορεί προσαρμοστικά να βελτιώσει τη σαφήνεια των δομών κορυφογραμμών των εικόνων δακτυλικών αποτυπωμάτων εισαγωγής βασισμένων στον κατ' εκτίμηση τοπικό προσανατολισμό και τη συχνότητα κορυφογραμμών. Έχουμε αξιολογήσει την απόδοση του αλγορίθμου αυξήσεων εικόνας χρησιμοποιώντας το δείκτη καλοσύνης των αποσπασματικών μικρολεπτομερειών και ακρίβειας ενός απευθείας συστήματος σύνδεσης επαλήθευσης δακτυλικών αποτυπωμάτων. Τα πειραματικά αποτελέσματα δείχνουν ότι η ενσωμάτωση των αλγορίθμων αυξήσεων βελτιώνει το δείκτη καλοσύνης και την ακρίβεια επαλήθευσης.



2.3 ΥΠΟΔΕΙΞΗ ΤΟΥ ΔΑΚΤΥΛΟΥ



βιομετρική μέσω των περιπτέρων.

Η ευρύτητα χρησιμοποιημένη και λιγότερη ακριβή βιομετρική τεχνολογία είναι η ανίχνευση δακτυλικών αποτυπωμάτων. Ο Bill Rogers, εκδότης της βιομετρικής αφομοίωσης, λέει ότι οι πιστωτικές ενώσεις έχουν χρησιμοποιήσει επιτυχώς την ανίχνευση αποτυπώματος ATMs από τα περιπτερα πραγματικού χρόνου (ρητό: το δάχτυλο είναι δυνατότερο από το PIN) από το 1997. Ο Rogers βλέπει πολλές εφαρμογές για την ανίχνευση του δακτυλικού αποτυπώματος : "Σύντομα θα βλέπουμε τα νοσοκομεία να διανέμουν τα φάρμακα, σημαντική ανακούφιση, με τη

Ο Rogers λέει ότι το δακτυλικό αποτύπωμά σας θα αποθηκεύεται σε έναν κώδικα ως ταυτότητα στο σημείο της πώλησης. Το Indivos έχει λειτουργήσει με ψηφιακό Persona στην πειραματική ανίχνευση δακτυλικών αποτυπωμάτων για τις ηλεκτρονικές πληρωμές σε ένα Mc Donald's στο Φρέσνο.

Το Welsh Valley Middle School στην Πενσυλβανία εισήγαγε εθελοντικά την ανίχνευση δακτυλικών αποτυπωμάτων για τις ταχείες πληρωμές στη γραμμή μεσημεριανού γεύματος και διπλασίασε τις πωλήσεις των καφετεριών πέρυσι. Η τοπική σχολική περιοχή προγραμματίζει να επεκτείνει το σύστημα στις μηχανές πώλησης. Οι βιβλιοθήκες έχουν εισαγάγει τους ανιχνευτές δακτυλικών αποτυπωμάτων για να ελέγξουν τα βιβλία που δανείζονται οι μαθητές.

2.4 ΠΡΟΪΟΝΤΑ ΓΙΑ ΤΟ PC ΣΑΣ

Αν κάποιος αποφάσιζε να κάνει μία έρευνα αγοράς για ένα σύστημα δακτυλικών αποτυπωμάτων για τον υπολογιστή του, σίγουρα θα τα έχανε μπροστά στην πληθώρα των προϊόντων που υπάρχουν διαθέσιμα αυτή τη στιγμή. Πράγματι, δεν ξέρει κανείς τι να πρωτοδιαλέξει, δεδομένου του ότι οι περισσότερες τιμές κυμαίνονται σε πολύ λογικά επίπεδα για οποιονδήποτε ενδιαφέρεται σοβαρά να αυξήσει την ασφάλεια του προσωπικού του υπολογιστικού συστήματος. Στον περιορισμένο χώρο αυτού του αφιερώματος θα παρουσιάσουμε εντελώς ενδεικτικά ορισμένα πακέτα, με την ελπίδα να κινήσουμε την περιέργεια στους ενδιαφερομένους, ώστε να ρίξουν μια πιο αναλυτική ματιά στις σελίδες του Internet. Τα περισσότερα από αυτά τα προϊόντα προσθέτουν έλεγχο δακτυλικών αποτυπωμάτων στη διαδικασία εκκίνησης των Windows, ενώ μερικά προχωρούν περαιτέρω και προσφέρουν δυνατότητες όπως κρυπτογράφηση αρχείων και έλεγχος εκκίνησης συγκεκριμένων εφαρμογών. Σημειώνουμε επίσης ότι όλα τα πακέτα χρησιμοποιούν οπτικούς αναγνώστες, ενώ σε όλες τις περιπτώσεις οι απαιτήσεις συστήματος είναι ελάχιστες (486 επεξεργαστές ή μικροί Pentium - Windows NT, 95 και 98).

- **U are U:** Το συγκεκριμένο πακέτο ανήκει στην εταιρία Digital Persona (<http://www.digitalpersona.com>) και σίγουρα προσφέρει πολύ περισσότερα από τα 149 δολάρια (134,90 €.) που κοστίζει. Περιέχει οπτικό αναγνώστη συνδεδεμένο σε θύρα USB και ένα πακέτο 4 προγραμμάτων, μέσω των οποίων ο χρήστης μπορεί να αυξήσει στο μέγιστο την ασφάλεια του συστήματός του. Αξίζει να ρίξουμε μια αναλυτικότερη ματιά σε κάθε πρόγραμμα ξεχωριστά.
- **Control Center:** Μέσω αυτού του προγράμματος γίνεται η εισαγωγή των νέων χρηστών καθώς και η διαδικασία λήψης των βιομετρικών προτύπων. One Touch Login: Ο χρήστης έχει τη δυνατότητα να προσθέσει τον έλεγχο δακτυλικών αποτυπωμάτων στη διαδικασία εκκίνησης των Windows, καθώς και να απαγορεύσει τελειώς την είσοδο σε κάθε μη εξουσιοδοτημένο χρήστη (ως γνωστόν, αν κάποιος πατήσει Escape στο πλαίσιο διαλόγου των Windows που ζητάει όνομα χρήστη και συνθηματικό, τα Windows θα ξεκινήσουν σε κατάσταση single user).
- **One Touch Password:** Αν θέλετε να απαγορεύσετε την πρόσβαση στους άλλους σε συγκεκριμένες εφαρμογές του υπολογιστή σας, αυτό το πρόγραμμα είναι για εσάς. Οι εφαρμογές στις οποίες θα εφαρμοστεί το One Touch Password θα εκτελούνται μόνο κατόπιν επιβεβαίωσης δακτυλικού αποτυπώματος.
- **One Touch Screen Saver:** Το ιδιόμορφο αυτό πρόγραμμα προστασίας οθόνης αναλαμβάνει αυτόματα δράση λίγη ώρα αφότου εσείς απομακρυνθείτε από τον υπολογιστή σας, αλλά δεν απενεργοποιείται εκτός κι αν τοποθετήσετε το δάχτυλό σας στον αναγνώστη δακτυλικών αποτυπωμάτων. Στην Deluxe έκδοση του προγράμματος (είναι λίγο ακριβότερη, περίπου 199 δολάρια) συμπεριλαμβάνεται και το πρόγραμμα Private Space. Το συγκεκριμένο πρόγραμμα δημιουργεί έναν εικονικό χώρο στο σκληρό δίσκο σας, στον οποίο μπορείτε να τοποθετήσετε όσα αρχεία ή έγγραφα θέλετε να προστατεύσετε από αδιάκριτα βλέμματα. Τα αρχεία κρυπτογραφούνται αυτόματα, και για να μπορέσει κάποιος να τα ανοίξει πρέπει να περάσει από βιομετρικό έλεγχο.
- **SecureSuite:** Το SecureSuite της I/O Software (<http://www.iosoftware.com>) είναι ένα πακέτο software που μπορεί να συνδυαστεί με μία μεγάλη γκάμα αναγνωστών δακτυλικών αποτυπωμάτων. Το καθένα από τα προγράμματα του πακέτου αναλαμβάνει την προστασία συγκεκριμένων στοιχείων ή διαδικασιών στον υπολογιστή σας, ακριβώς όπως και στο U are U που είδαμε προηγουμένως. Συγκεκριμένα, το πρόγραμμα SecureStart δίνει τη δυνατότητα στο χρήστη να αντιστοιχίσει δακτυλικά αποτυπώματα σε κάθε user name του δικτύου των Windows, ενώ το SecureSession αναλαμβάνει να ελέγξει την πρόσβαση σε μεμονωμένες εφαρμογές. Αρκετά ενδιαφέρον είναι το πρόγραμμα SecureFolder, το οποίο μπορεί να "κλειδώσει" σημαντικά έγγραφα ή φακέλους, και να τα καταστήσει διαθέσιμα στον εξουσιοδοτημένο χρήστη μόνο έπειτα από επιβεβαίωση δακτυλικού αποτυπώματος. Το "κλειδώμα", όπως και στο U are U, επιτυγχάνεται με έναν πολύ ισχυρό αλγόριθμο κρυπτογράφησης. Η τιμή του SecureSuit είναι 129 δολάρια, δηλαδή γύρω στα 117,30 € . Ο αναγνώστης δακτυλικών αποτυπωμάτων που προτείνει η I/O Software για το πακέτο της, ο FIU-500 της Sony, είναι κάπως ακριβός (550 δολάρια), αλλά ο χρήστης μπορεί κάλλιστα να προμηθευτεί το λογισμικό ξεχωριστά και να επιλέξει έναν αναγνώστη της αρεσκείας του.

- **SecureTouch 99:** Το προϊόν αυτό έρχεται από την εταιρία Biometric Access Corporation (<http://www.biometricaccess.com>) και είναι εξαιρετικά φθηνό (119 δολάρια, περίπου 108,50 €.). Το πακέτο περιλαμβάνει αναγνώστη δακτυλικών αποτυπωμάτων καθώς και το λογισμικό SecureTouch PAL, το οποίο μάλιστα είναι freeware, μπορείτε δηλαδή να το κατεβάσετε από τη σελίδα της εταιρίας στο Internet. Οι δυνατότητες του συστήματος εξαντλούνται στον έλεγχο πρόσβασης κατά την εκκίνηση των Windows, κάτι βέβαια διόλου ευκαταφρόνητο.
- **Biomouse:** Άλλο ένα οικονομικό σύστημα, αυτήν τη φορά από την American Biometric Company (<http://www.abio.com>). Το πακέτο περιλαμβάνει αναγνώστη δακτυλικών αποτυπωμάτων και το software Biomouse Suite, ένα σύνολο προγραμμάτων με πολλές δυνατότητες. Η τιμή του προϊόντος είναι 149 δολάρια (γύρω στα 134,90 €.).
- **Keytronic Biometric Secure Finger Scanner Keyboard:** Η εταιρία Keytronic (<http://www.keytronic.com>), συνδυάζοντας αναγνώστη δακτυλικών αποτυπωμάτων και πληκτρολόγιο, προσφέρει στους ενδιαφερομένους μία πρωτότυπη και πολύ εργονομική λύση. Το βιομετρικό πληκτρολόγιο συνοδεύεται από το software Secure Log, το οποίο, όπως μπορούμε να καταλάβουμε από τον τίτλο του, βελτιώνει τον έλεγχο πρόσβασης κατά την εκκίνηση των Windows. Το πακέτο της Keytronic (πληκτρολόγιο και λογισμικό) κοστίζει 169 δολάρια (152,50 €).

2.5 ΑΛΛΕΣ ΕΤΑΙΡΙΕΣ ΚΑΙ ΠΡΟΪΟΝΤΑ

Μία από τις πιο αξιόλογες εταιρίες του χώρου που δεν αναφέρθηκαν ακόμα είναι η Identicator Technology (<http://www.identicator.com>). Εκτός από μία μεγάλη γκάμα αναγνωστών δακτυλικών αποτυπωμάτων, έχει κυκλοφορήσει μία σειρά προϊόντων software, όπως το BioLogon για Windows NT και 95/98, καθώς και ένα SDK (software developer's kit) για την κατασκευή προγραμμάτων με βιομετρικούς ελέγχους. SDK προσφέρει επίσης η εταιρία Veridicom (<http://www.veridicom.com>), το οποίο δίνει όλα τα απαραίτητα εργαλεία στους προγραμματιστές που ενδιαφέρονται να κατασκευάσουν βιομετρικά προγράμματα, χρησιμοποιώντας μάλιστα τις γνωστές γλώσσες προγραμματισμού (Visual Basic, Visual C++ κ.λπ.). Η εταιρία Mytec (<http://www.mytec.com>) ειδικεύεται στη δικτυακή ασφάλεια μέσω της σειράς προϊόντων TouchStone. Τέλος, δεν λείπουν λύσεις παραπλήσιες με το πληκτρολόγιο-αναγνώστη δακτυλικών αποτυπωμάτων της Keytronic που είδαμε προηγουμένως. Η γερμανική εταιρία Cherry (<http://www.cherry.de>) προσφέρει τα δικά της πληκτρολόγια-αναγνώστες, τα οποία συνοδεύονται από το κατάλληλο software.

· Fingerprint scanners

Από τις διάφορες τεχνικές των βιομετρικών κλειδιών, η πιο διαδεδομένη για προσωπική χρήση σε desktop συστήματα, notebooks, PDAs κ.λ.π. είναι αυτή της αναγνώρισης δακτυλικού αποτυπώματος, μέσω των λεγόμενων «fingerprint scanners». Συσκευές, οι οποίες διαθέτουν έναν αισθητήρα, όπου ο χρήστης τοποθετεί το δάκτυλό του για να καταγραφεί το αποτύπωμά του, βάσει του οποίου θα ελέγχεται κάθε ένας που θα προσπαθήσει στο μέλλον να μπει στον υπολογιστή. Το αποτύπωμα αποθηκεύεται σε μία βάση δεδομένων (συνήθως εσωτερικά στη

συσκευή) και το ειδικευμένο software που συνοδεύει αυτές τις συσκευές αναλαμβάνει να συγκρίνει τα χαρακτηριστικά του αποτυπώματος όποιου εκκινεί το σύστημα με τα αποτυπώματα του χρήστη που έχει αποθηκευμένο. Σε περίπτωση μη ταυτοποίησης, ο υπολογιστής κλειδώνει και δεν αφήνει το σύστημα να εκκινήσει.

Δύο είναι οι βασικές τεχνολογίες των fingerprint scanners. Η πρώτη προέρχεται απευθείας από τις ψηφιακές φωτογραφικές μηχανές και έχει αρχίσει να εκλείπει. Η συσκευή διαθέτει αισθητήρα CCD και «φωτογραφίζει» το δάκτυλο του χρήστη. Τα αποτύπωμα αποθηκεύεται με τη μορφή φωτογραφίας. Αυτό σημαίνει ότι η συσκευή μπορεί να παραπλανηθεί από μία υψηλής ανάλυσης φωτογραφία (ακόμη και φωτοτυπία) του δακτύλου του χρήστη, γι' αυτό και δεν προτιμάται πολύ ως λύση από τους κατασκευαστές. Ένας δεύτερος -και ευρέως διαδεδομένος- τύπος αισθητήρα, είναι εκείνος που χρησιμοποιεί πλέγμα κυκλωμάτων ημιαγωγών. Πιο συγκεκριμένα, η επιφάνεια του αισθητήρα αποτελείται από χιλιάδες λεπτεπίλεπτους ακροδέκτες (μικρότεροι από το πλάτος των γραμμών του δέρματος). Οι ακροδέκτες αυτοί μέσω κυκλωμάτων ημιαγωγών φορτίζουν αντίστοιχο αριθμό πυκνωτών. Λόγω του ανάγλυφου της επιφάνειας του χεριού, κάποιοι πυκνωτές φορτίζονται και κάποιοι όχι, καθώς οι γραμμές του δέρματος ακουμπούν μόνο ορισμένους ακροδέκτες μεταδίδοντας το φορτίο του στατικού ηλεκτρισμού, ενώ οι «κοιλιάδες» ανάμεσα στις γραμμές που δεν ακουμπούν τους υπόλοιπους ακροδέκτες αφήνουν τους αντίστοιχους πυκνωτές αφόρτιστους. Η διάταξη των φορτισμένων / μη φορτισμένων πυκνωτών αντιστοιχεί με το αποτύπωμα του χεριού. Με αυτόν τον τρόπο η συσκευή δεν εξαπατάται από φωτογραφίες του δακτύλου του χρήστη, όπως συμβαίνει με τους οπτικούς αισθητήρες.

Σε όλα τα χρόνια ύπαρξης των συσκευών ανίχνευσης δακτυλικού αποτυπώματος το hardware δεν έχει υποστεί σημαντικές αλλαγές, πλην της αύξησης της ανάλυσης. Εκεί που γίνονται μεγάλες βελτιώσεις είναι στο software που χρησιμοποιείται στην ταυτοποίηση. Οι πρώτοι αλγόριθμοι ήταν αρκετά προβληματικοί, οδηγώντας είτε στην ταυτοποίηση «ξένων» αποτυπωμάτων, είτε στην απόρριψη του σωστού. Κατάσταση που έδωσε κακό όνομα στις συσκευές αυτές. Τα τελευταία χρόνια όμως η διαδικασία ταυτοποίησης είναι θεαματικά βελτιωμένη και τα σφάλματα ελαχιστοποιήθηκαν.



Αναγνώριση δακτυλικού αποτυπώματος. Η μέθοδος που έχει επικρατήσει.



Τα μικροσκοπικά fingerprint scanners έχουν εισχωρήσει σε κάθε είδους περιφερειακό.

Στην αγορά υπάρχουν πολλές εναλλακτικές λύσεις -σε διάφορες μορφές- προϊόντων αναγνώρισης βιομετρικών χαρακτηριστικών. Για τους απλούς χρήστες η μέθοδος αναγνώρισης δακτυλικού αποτυπώματος έχει επικρατήσει κατά κράτος σε σχέση με τις υπόλοιπες βιομετρικές μεθόδους. Δυστυχώς, η ελληνική αγορά δεν τα έχει ακόμη «γνωρίσει», παρά την τριετή και πλέον επιτυχημένη πορεία τους στη διεθνή αγορά. Το σίγουρο είναι ότι ούτε ο τύπος (ηλεκτρονικός και μη) έχει φροντίσει να ενημερώσει επαρκώς τους καταναλωτές για αυτές τις απόλυτα ασφαλείς, αρκετά λειτουργικές και -συγκριτικά με το επίπεδο ασφάλειας που προσφέρουν- φθηνές λύσεις.

Ας δούμε τις πιο γνωστές και δοκιμασμένες συσκευές αναγνώρισης βιομετρικών χαρακτηριστικών της αγοράς

Digital Persona U.are.U Personal/Pro



Από τις πλέον φιλικές λύσεις, ο scanner της Digital Persona μπορεί να αποθηκεύσει τα δακτυλικά αποτυπώματα ακόμη και των δέκα δακτύλων του χρήστη, ώστε ακόμη κι αν για κάποιο λόγο (τραυματισμός, βρωμιά) δεν αναγνωρίζεται το ένα δάκτυλο, να μπορείτε να χρησιμοποιήσετε το επόμενο για να «ξεκλειδώσετε» τον υπολογιστή. Συνδέεται σε θύρα USB και μπορεί επιπλέον να αποθηκεύσει passwords εισόδου στα διάφορα sites. Η διαφορά του Personal με το Pro, είναι ότι το τελευταίο απευθύνεται σε επαγγελματίες διαθέτοντας επιπλέον δυνατότητες αυτόματης εισόδου passwords σε τοπικό δίκτυο καθώς και άλλες ευκολίες ειδικά για Web administrators. www.digitalpersona.com

Identix BioTouch USB 200



Η συσκευή αναγνώρισης της Identix, ενσωματώνει μία μικροσκοπική κάμερα CMOS για την «φωτογράφιση» του δακτυλικού αποτυπώματος. Οι εξελιγμένες τεχνικές αναγνώρισης επιτρέπουν την ομαλή λειτουργία ακόμη και αν το δάκτυλο τοποθετείται υπό γωνία, έχει μικροτραυματισμούς ή βρωμιά. Το BioTouch USB 200 συνδέεται σε θύρα USB και συνοδεύεται από το βραβευμένο λογισμικό BioLogon. www.identix.com

Identix BioTouch PC Card



Πανομοιότυπης τεχνολογίας και δυνατοτήτων με το BioTouch USB 200 - η μόνη διαφορά έχει να κάνει με το format της συσκευής. Υπό μορφή PC Card απευθύνεται σε χρήστες notebooks που θα το προτιμήσουν για περισσότερη ευκολία (λόγω φορητότητας). www.identix.com

Targus DEFCON Authenticator



Πέρα από την αναγνώριση του δακτυλικού αποτυπώματος του χρήστη, το DEFCON Authenticator της Targus διαθέτει επιπλέον δύο θύρες USB, αυξάνοντας το συνολικό αριθμό των διαθέσιμων θυρών του PC ή του notebook με το οποίο διασυνδέεται. Σημειωτέον ότι η τεχνολογία οπτικής αναγνώρισης που χρησιμοποιεί η Targus απολαμβάνει την εμπιστοσύνη της IBM. www.targus.com

Panasonic Authenticam



Η Panasonic προτίμησε να επενδύσει στην αναγνώριση της ίριδας. Σε συνεργασία με την Iridian παρουσίασε πριν δύο χρόνια την Authenticam, μία συσκευή που αναγνωρίζει το μάτι του χρήστη. Μέθοδος η οποία, σύμφωνα με την εταιρεία, είναι πιο ασφαλής από το δακτυλικό αποτύπωμα, ενώ επιτυγχάνει τον έλεγχο από απόσταση έως και 50 εκατοστών. Όντας όμως κατά βάση μία κάμερα, η Authenticam προσφέρει επιπλέον «υπηρεσίες», λειτουργώντας τόσο ως web-cam, όσο και ως οπτικός αισθητήρας κίνησης (με χρήση ειδικευμένου λογισμικού). Η Authenticam ζυγίζει μόλις 160 γραμμάρια και συνδέεται μέσω θύρας USB. www.panasonic.com

Sony FIU 710 Fingerprint Reader



Από τις πλέον αποδοτικές προτάσεις της αγοράς, ο εξεταζόμενος scanner της Sony διαθέτει ενσωματωμένο επεξεργαστή και 512K μνήμης για τους υπολογισμούς της εξακρίβωσης της ταυτότητας του χρήστη και την αποθήκευση των δεδομένων των δακτυλικών αποτυπωμάτων αντίστοιχα. Συνδέεται μέσω θύρας USB και είναι η απολύτως λεπτή συσκευή αυτού του είδους, θυμίζοντας πιστωτική κάρτα. www.sony.com

Sony FIU 600 Puppy Fingerprint Reader



Εξελιγμένη μορφή του FIU 710 Fingerprint Reader της ίδιας εταιρείας, διαθέτει scanner μεγαλύτερης ανάλυσης καθώς και συμβατότητα με τα περισσότερα προγράμματα διαχείρισης δακτυλικών αποτυπωμάτων, τρίτων κατασκευαστών. www.sony.com



Sony FIK 900 Fingerprint Identity Token

Η νεότερη πρόταση της Sony στις συσκευές αναγνώρισης δακτυλικού αποτυπώματος έρχεται σε μορφή memory stick. Διαθέτει την τεχνολογία και τις ευκολίες του FIU 710 Fingerprint Reader, 1MB εσωτερικής μνήμης και, βέβαια, αποτελεί την απολύτως μικρότερη συσκευή αναγνώρισης της αγοράς. Δυστυχώς, αν δεν είστε κάτοχος προϊόντων της Sony με θύρα για memory sticks, θα πρέπει να προμηθευτείτε τον κατάλληλο converter. www.sony.com



Toshiba Fingerprint Reader

Από τους παλαιότερους εκπροσώπους της κατηγορίας των συσκευών οπτικής αναγνώρισης δακτυλικών αποτυπωμάτων, αυτή η PC Card με ενσωματωμένο scanner της Toshiba διατίθεται τόσο ως έξτρα, με την αγορά των notebooks της εταιρείας, όσο και ως αυτόνομη συσκευή. Συνοδεύεται από τα προγράμματα BioLogon και BioShield. www.toshiba.com

Πέρα από τους τις αυτόνομες συσκευές αναγνώρισης, τα βιομετρικά «κλειδιά» εισχώρησαν σε υπολογιστές και σε διάφορα περιφερειακά προσφέροντας λύσεις «δύο σε ένα». Αρκετοί κατασκευαστές έχουν προχωρήσει στην ενσωμάτωση βιομετρικών κλειδιών στα προϊόντα τους. Ακολουθούν τα πιο γνωστά προϊόντα της αγοράς που διαθέτουν υποσύστημα αναγνώρισης δακτυλικού αποτυπώματος.



Fujitsu-Siemens Celcius Series

Το βαρύ πυροβολικό των notebooks της Fujitsu-Siemens, η σειρά Celcius που συστήνεται από την εταιρεία ως φορητό Workstation με τις κορυφαίες λύσεις σε κάθε υποσύστημά της (επεξεργαστής Pentium 4 στα 2,5GHz, μνήμη 512MB DDR, οθόνη ανάλυσης 1.600x1.200 pixels και υποσύστημα γραφικών NVIDIA Quatro4 500Go), συνοδεύεται και από στάνταρ scanner δακτυλικού αποτυπώματος. www.fujitsu-siemens.com



HP iPAQ 5450/5550

Ίσως τα πιο «ασφαλή» PDAs της αγοράς, τα iPAQ 5450 και 5550 της HP, ανάμεσα στις υπόλοιπες δυνατότητες που τα κατατάσσουν στην κορυφή της σειράς iPAQ διαθέτουν και ένα μικρό «ματάκι» που αναγνωρίζει μόνο το δάκτυλο του κατόχου τους. www.hp.com



IBM ThinkPad

Οι νεότερες εκδόσεις της σειράς ThinkPad των notebooks της IBM, μπορεί να μη διαθέτουν σύστημα αναγνώρισης δακτυλικού αποτυπώματος ως στάνταρ, ωστόσο, προσφέρεται ως έξτρα το Targos DEFCON authenticator, δηλαδή ο fingerprint scanner σε μορφή PC Card στον οποίο αναφερθήκαμε παραπάνω. Εκείνο που κάνει τη διαφορά είναι ότι τα ThinkPad ενσωματώνουν κύκλωμα που αποθηκεύει κάθε είδος κλειδιού (συμπεριλαμβανομένων των βιομετρικών) προφυλάσσοντάς τα από τα αδιάκριτα μάτια που μπορούν να εισχωρήσουν στη μνήμη και το BIOS του υπολογιστή. www.ibm.com



BioLink U-Match Mouse

Το U-Match Mouse είναι ένα ποντίκι με ενσωματωμένη επιφάνεια αναγνώρισης δακτυλικού αποτυπώματος στην αριστερή πλευρά του. Οι πληροφορίες αποθηκεύονται εσωτερικά υπό μορφή template μήκους 500 bytes για περισσότερη ασφάλεια, ενώ παράλληλα προσφέρονται ευκολίες όπως η αυτόματη εισαγωγή των passwords εισόδου στα διάφορα sites. www.biolinkusa.com



LoqWare LoqFlash

Το USB key της LoqWare προσφέρεται σε τρεις εκδόσεις, των 128MB, των 256MB και των 512MB. Το scanner δακτυλικού αποτυπώματος, ανάλυσης 500dpi προστατεύει τα δεδομένα που είναι αποθηκευμένα στη συσκευή, αλλά δεν προσφέρει περαιτέρω κλείδωμα στο PC, ή το notebook του χρήστη του. www.loqware.com



LogWare LoqDrive 250 SPR

Για ακόμη πιο απαιτητικούς -ως προς τον όγκο των δεδομένων που μεταφέρουν- χρήστες, η LogWare προσφέρει μία ακόμη λύση. Έναν φορητό σκληρό δίσκο που επικοινωνεί μέσω θύρας USB και διαθέτει στη ράχη του ένα οπτικό scanner ανάλυσης 500dpi. Σε περίπτωση που δεν ταυτοποιηθεί το δάκτυλο του χρήστη, το σύστημα κλειδώνει και τα περιεχόμενα μένουν προστατευμένα μακριά από τα αδιάκριτα μάτια. www.logware.com



Keytronic Fingerprint Scanner Board

Ένα διακριτικό πληκτρολόγιο 104 πλήκτρων που ενσωματώνει scanner δακτυλικού αποτυπώματος. Συνοδεύεται από το software BioLogon της Identix, μέσω του οποίου επιτυγχάνεται ο έλεγχος και η ταυτοποίηση σε λιγότερο από ένα δευτερόλεπτο. Προσφέρεται και σε έκδοση με Smartcard reader και συνοδεύεται από διετή εγγύηση. www.keytronic.com



Siemens ID Mouse

Ένα κλασικό wheel-mouse με scanner δακτυλικού αποτυπώματος τύπου ημιαγωγού και ανάλυσης 513dpi στη ράχη του. Για κάθε χρήστη μπορεί να καταγράψει τα αποτυπώματα έως και των δέκα δακτύλων του, ώστε σε περίπτωση τραυματισμού ή άλλου προβλήματος αναγνώρισης να μπορεί να μπει στον υπολογιστή, χωρίς πρόβλημα. www.siemens.com



Sony MicroVault with Fingerprint Access

Το USB key αναγνώρισης δακτυλικού αποτυπώματος που παρουσίασε πολύ πρόσφατα η Sony, αποτελεί ένα από τα πιο ασφαλή μέσα, κλειδώνοντας τόσο τα περιεχόμενά του, όσο και τον υπολογιστή όπου τοποθετείται. Επιπλέον, μπορεί να μεταφέρει τους κωδικούς εισόδου σε sites, υπηρεσίες κ.λπ., ώστε ο χρήστης του να μπορεί να τους χρησιμοποιεί από οποιονδήποτε υπολογιστή. www.sony.com



STAR FINGER-006

Το STAR FINGER-006 είναι ένα εύχρηστο σύστημα ελέγχου πρόσβασης που συνδυάζει αναγνώστη καρτών proximity και σαρωτή δακτυλικού αποτυπώματος, παρέχοντας μεγάλη ασφάλεια, ευκολία στη χρήση και υψηλή αξιοπιστία. Πρόκειται για μία συσκευή φιλική προς τον χρήστη, στην οποία μπορούν να καταχωρηθούν 720 (προαιρετικά ως και 4.500) κάρτες proximity και δακτυλικά αποτυπώματα. Ο ενσωματωμένος αναγνώστης καρτών proximity, ως και από 10 cm απόσταση, καθώς και ο σαρωτής δακτυλικού αποτυπώματος σας δίνουν τη δυνατότητα πολλαπλών ρυθμίσεων ελέγχου πρόσβασης σε κάθε χρήστη και για κάθε ημέρα και ώρα.

Το STAR FINGER-006 έχει έναν επιπλέον αναγνώστη καρτών proximity για έλεγχο εξόδου. Συνδέεται με υπέρυθρες με φορητό υπολογιστή ή palm top, μέσω των οποίων μπορούμε να φορτώσουμε δακτυλικά αποτυπώματα στην μνήμη της συσκευής.

Κύριες Λειτουργίες

- Βιομετρικό και proximity σύστημα ελέγχου πρόσβασης
- 720 χρήστες (προαιρετικά ως 4.500)
- Ενσωματωμένος αναγνώστης καρτών (ως και από 10cm) και σαρωτής δακτυλικού αποτυπώματος
- Διπλή επαλήθευση δακτυλικού αποτυπώματος
- Μικρός χρόνος ανάγνωσης (< 1 δευτ.)
- Αυτόνομη λειτουργία ή σε δίκτυο επικοινωνίας (RS232/RS422) έως και 256 κανάλια
- Σύνδεση με φορητό υπολογιστή μέσω υπέρυθρων
- Ξεχωριστός εξωτερικός αναγνώστης κάρτας εξόδου
- Έξοδοι Wiegand, ABA Track II
- 2 φωτεινές ενδείξεις και βομβητής

STAR FINGER-007

Το STAR FINGER-007 είναι ένα εύχρηστο σύστημα ελέγχου πρόσβασης βασισμένο σε δύο μικροεπεξεργαστές των 8 bit, συνδυάζοντας μικρό κόστος με τη μέγιστη ασφάλεια. Συνδυάζει αναγνώστη καρτών proximity, πληκτρολόγιο κωδικών PIN καθώς και σαρωτή δακτυλικού αποτυπώματος, παρέχοντας μεγάλη ασφάλεια, ευκολία στη χρήση και υψηλή αξιοπιστία. Πρόκειται για μία συσκευή φιλική προς τον χρήστη, στην οποία μπορούν να καταχωρηθούν 720 (προαιρετικά ως και 4.500) κάρτες proximity και δακτυλικά αποτυπώματα. Ο ενσωματωμένος αναγνώστης καρτών proximity, ως και από 10 cm απόσταση, καθώς και ο σαρωτής δακτυλικού αποτυπώματος αλλά και κωδικού PIN στο ενσωματωμένο πληκτρολόγιο, σας δίνει τη δυνατότητα πολλαπλών ρυθμίσεων ελέγχου πρόσβασης σε κάθε χρήστη και για κάθε ημέρα και ώρα.



Το STAR FINGER-007 έχει έναν επιπλέον αναγνώστη καρτών proximity για έλεγχο εξόδου. Επίσης έχει 4 ανεξάρτητες θύρες εισόδου όπου μπορούμε να συνδέσουμε κουμπί εξόδου, επικοινωνία πόρτας, σένσορα PIR και σένσορα θραύσης παραθύρου και να τα προγραμματίσουμε από το ενσωματωμένο πληκτρολόγιο. Μπορούμε να χρησιμοποιούμε την συσκευή μόνη της (standalone) ή συνδεδεμένη στο δίκτυο επικοινωνίας μέσω θύρας RS232/RS422. Έχει ενσωματωμένα δύο ρελέ τύπου FORM-C με αντιμαγνητική προστασία καθώς και 2 εξόδους TTL για διάφορες εφαρμογές, όπως ενεργοποίηση auto-dialer και έλεγχο άλλων συσκευών. Όλες οι ρυθμίσεις, όπως τα στοιχεία δακτυλικών αποτυπωμάτων, η διευθέτηση εισόδου και εξόδου ανά χρήστη και όλα τα καταγεγραμμένα περιστατικά καταγράφονται στον συνδεδεμένο με τη συσκευή Η/Υ όπου μπορούμε να τα διαχειριστούμε μέσω του ειδικού λογισμικού που παρέχεται.

Η κομψή και συμπαγής εμφάνιση του και η πληθώρα λειτουργιών του STAR FINGER-007 σας προσφέρουν ένα σύστημα ελέγχου πρόσβασης υψηλών προδιαγραφών με τα υψηλότερα στάνταρ ασφαλείας.

Κύριες λειτουργίες

- Βιομετρικό και proximity σύστημα ελέγχου πρόσβασης
- Διαχείριση και καταγραφή ώρας εισόδου και εξόδου προσωπικού
- 720 χρήστες (προαιρετικά ως 4.500)
- Ενσωματωμένος αναγνώστης καρτών (ως και από 10cm) και σαρωτής δακτυλικού αποτυπώματος
- Αυτόνομη λειτουργία ή σε δίκτυο επικοινωνίας (RS232/RS422) έως και 32 κανάλια
- Είσοδος με κάρτα RF μόνο, με κάρτα RF και δακτυλικό αποτύπωμα, με κωδικό PIN και δακτυλικό αποτύπωμα ή με συνδυασμό και των τριών
- 4 ανεξάρτητες εισοδοί, 4 έξοδοι και 2 ρελέ τύπου FORM-C
- Λειτουργία αυτόματης διάγνωσης
- Ξεχωριστός εξωτερικός αναγνώστης κάρτας εξόδου
- 10 προγράμματα ώρας και 10 προγράμματα αργιών
- Φωτιζόμενο πληκτρολόγιο



Fingerprint Desktop Scanner

Η ασφαλής γραμμή προϊόντων δακτυλικών αποτυπωμάτων παρέχει τα μέγιστα στην ασφάλεια για τους χρήστες δικτύων. Το σύστημα χρησιμοποιεί αναγνώριση μικρολεπτομερειών δακτυλικών αποτυπωμάτων για να επικυρώσει την πρόσβαση σε έναν κεντρικό υπολογιστή δικτύων, έναν προσωπικό τερματικό σταθμό ή έναν υπολογιστή

σημειωματάρων. Με πολύ μικρό κόστος, τα ασφαλή προϊόντα χρησιμοποιούν το καθένα την ενσωματωμένη συσκευή επικύρωσης για να κάνουν την ανάμνηση των κωδικών πρόσβασης ένα πράγμα του παρελθόντος. Με τον ασφαλή βιομετρικό προσδιορισμό, οι κωδικοί πρόσβασης δεν θα είναι ποτέ οι ίδιοι. Το προϊόν F-SCAN-S001US συνοδεύεται από το λογισμικό BioLogon για μια πλήρη λύση υλικού και λογισμικού. Το λογισμικό που συμπεριλαμβάνετε είναι για Windows 9X και NT 4.0.



KT Multimedia

Το Key Tronic® Multi-Media πληκτρολόγιο μας επιτρέπει να δουλέουμε γρηγορότερα και αποδοτικότερα τοποθετώντας Hot Keys(καυτά κλειδιά) στα άκρα των δακτύλων μας για την ευκολότερη πρόσβαση στο Διαδίκτυο, τα Windows, την αριθμομηχανή, τα παιχνίδια και άλλα. Ένα καυτό κλειδί για το Διαδίκτυο μας αφήνει να ελέγξουμε την πλοήγησή μας στο Ιστό με την αφή μόνο ενός κουμπιού. Το πληκτρολόγιο περιέχει καυτά κλειδιά λογισμικού και 2 χαρακτηριστικές θύρες USB που βρίσκονται κοντά

στο καλώδιο.



KT CORDLESS B

Η ολοκαίνουργια ασύρματη σειρά KT Cordless προσφέρει στο χρήστη ένα εξαιρετικά μοντέρνο ασύρματο πληκτρολόγιο και ποντίκι. Με μια λειτουργούσα απόσταση 2 μέτρων, τα ασύρματα προϊόντα αφαιρούν το φορτίο του γραφείου και ελευθερώνουν χώρο πάνω στον υπολογιστή γραφείου για ένα πολύ καθαρότερο και κατάλληλο εργασιακό περιβάλλον.

Τα 16 Hot-Keys επιτρέπουν τη γρήγορη και εύκολη πρόσβαση σε πολλές εφαρμογές όπως ηλεκτρονικό ταχυδρομείο(email), Διαδίκτυο (internet), CDs και όλα αυτά με το πάτημα ενός κουμπιού μόνο. Το KT Cordless είναι διαθέσιμο σε 2 σύγχρονα χρώματα και σχέδια. Τα Gray+Navy και Black+Silver.



SecureTouch PC

Το SecureTouch PC είναι ένας φθηνός, εύχρηστος αναγνώστης εικόνας δάχτυλων που παρέχει μεγάλη ασφάλεια για τον έλεγχο πρόσβασης σε υπολογιστές ή δίκτυα. Αντίθετα από τους κωδικούς πρόσβασης, που μπορούν να χαθούν, να κλαπούν ή να ξεχαστούν, η επικύρωση εικόνας δάχτυλων βεβαιώνει ότι μόνο τα εξουσιοδοτημένα άτομα αποκτούν πρόσβαση στον υπολογιστή και το δίκτυο.



SecureTouch Advanced

Το SecureTouch Advanced είναι μια καινοτομία που σχεδιάστηκε για να χρησιμοποιηθεί σε περιβάλλοντα με πολύ κόσμο όπως τα λιανικά καταστήματα και οι μεγάλες επιχειρήσεις. Διάφορες λειτουργικές ενότητες είναι διαθέσιμες έτσι ώστε κάθε πελάτης να μπορεί να προσαρμόσει τη λύση που ικανοποιεί ακριβώς τις ανάγκες του . Αυτό το προϊόν επιτρέπει σε πολλές συσκευές να συνδεθούν και να τρέξουν μέσω ενός ενιαίου PC, και είναι κατάλληλο ακόμα και όταν συχνές συναλλαγές εκτελούνται από μια μεγάλη βάση χρηστών.

ΚΕΦΑΛΑΙΟ 3

ΓΕΩΜΕΤΡΙΑ ΧΕΡΙΩΝ



ΓΕΩΜΕΤΡΙΑ ΧΕΡΙΩΝ

Αυτή η προσέγγιση χρησιμοποιεί τη γεωμετρική μορφή του χεριού για την επικύρωση της ταυτότητας ενός χρήστη. Η επικύρωση της ταυτότητας που χρησιμοποιεί τη γεωμετρία χεριών είναι ένα ενδιαφέρον πρόβλημα. Τα μεμονωμένα χαρακτηριστικά γνωρίσματα χεριών δεν είναι αρκετά περιγραφικά για τον προσδιορισμό. Εντούτοις, είναι δυνατό να επινοηθεί μια μέθοδος με το συνδυασμό των διάφορων μεμονωμένων χαρακτηριστικών γνωρισμάτων για να επιτευχθεί η γερή επαλήθευση.

Γεωμετρία χεριών



Όλοι μπορούν τώρα να χρησιμοποιήσουν τη γεωμετρία χεριών, σε ένα περίπτερο, για να επιβεβαιώσουν την ταυτότητά τους. Η γεωμετρία χεριών είναι σχετικά μια βιομετρική χωρίς τις εγκληματικές ενώσεις των δακτυλικών αποτυπωμάτων. Η AutoMon συνεργάστηκε πρόσφατα με τα συστήματα πληροφοριών περιπτέρων που αναπτύσσονται εκθέτοντας τα περίπτερα για τις συμμετέχοντες. Ο Norm Harrison, διευθυντής προγράμματος για το υπουργείο εξωτερικών της Ουάσιγκτον (που δημιούργησε τα περίπτερα που άρχισαν το 1992), λέει ότι οι συμμετέχοντες προτιμούν τα περίπτερα για πληροφορίες. Τα περίπτερα προσδιορίζουν τους συμμετέχοντες μέσω της ανάγνωσης γεωμετρίας χεριών. Ο Harrison εξηγεί, "είναι μέσα και έξω σε πέντε λεπτά. Μπορείτε να χρησιμοποιήσετε το περίπτερο αντί να έρχεστε σε εμένα." Το κράτος της Ουάσιγκτον επεξεργάζεται 13.000 αναφορές περιπτέρων το μήνα.

3.1 ΠΡΟΓΡΑΜΜΑΤΑ ΓΕΩΜΕΤΡΙΑΣ ΧΕΡΙΩΝ

Γεωμετρία χεριού βασισμένη στο σύστημα επαλήθευσης:

Αυτό το πρόγραμμα ερευνά τη χρήση της γεωμετρίας χεριών ως μέτρο της ταυτότητας ενός προσώπου. Το σύστημα αποτελείται από μια συσκευή αποκτήσεων που συλλαμβάνει την κορυφαία όψη και την πλάγια όψη του δεξιού χεριού ενός χρήστη καθώς την τοποθετεί στην επίπεδη επιφάνεια της συσκευής. Ένα στιγμιότυπο του χεριού του χρήστη λαμβάνεται για την επεξεργασία. Ένα σύνολο χαρακτηριστικών γνωρισμάτων έχει προσδιοριστεί που θα μπορούσε να χρησιμοποιηθεί για να αντιπροσωπεύσει το χέρι ενός προσώπου. Αυτά τα χαρακτηριστικά γνωρίσματα περιλαμβάνουν τα μήκη και τα πλάτη των δαχτύλων στις διάφορες θέσεις.

- **Παραμορφωμένο ταίριασμα των μορφών χεριών για την επαλήθευση:**

Αυτό το πρόγραμμα περιλαμβάνει το σχεδιασμό ενός μηχανισμού που θα ευθυγράμμιζε τις μορφές χεριών πριν από την επαλήθευση της ταυτότητας ενός προσώπου. Μια τέτοια προσέγγιση θα ενίσχυε την ακεραιότητα του συνόλου χαρακτηριστικών γνωρισμάτων που παρέχεται κατά τη διάρκεια του σταδίου επαλήθευσης.

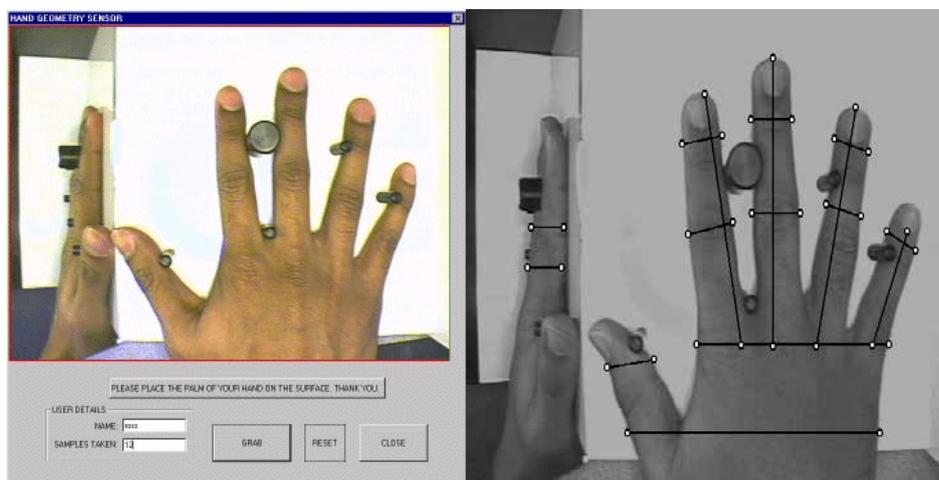
- **Ιστός-πρόσβαση χρησιμοποιεί τη βιομετρική:**

Αυτή η εργασία περιλαμβάνει την εξασφάλιση ενός ιστοχώρου χρησιμοποιώντας τη βιομετρική. Στους χρήστες χορηγείται η πρόσβαση σε ένα σύνολο αρχείων σε έναν ιστοχώρο αφότου έχει ελεγχθεί η ταυτότητά τους χρησιμοποιώντας τη βιομετρική - τη γεωμετρία χεριών ειδικότερα. Πιστεύουμε ότι η βιομετρική βασισμένη στην πρόσβαση-ιστού θα προσθέσει ένα νέο επίπεδο ασφάλειας σε θέματα των υπαρχόντων συστημάτων ασφάλεια-ιστού .

3.2 ΓΕΩΜΕΤΡΙΑ ΧΕΡΙΟΥ ΒΑΣΙΣΜΕΝΗ ΣΤΟ ΣΥΣΤΗΜΑ ΕΠΑΛΗΘΕΥΣΗΣ

Σύλληψη εικόνων χεριών και εξαγωγή των χαρακτηριστικών γνωρισμάτων:

Το σύστημα αποκτήσεων εικόνας αποτελείται από μια πηγή φωτός, μια φωτογραφική μηχανή, έναν ενιαίο καθρέφτη και μια επίπεδη επιφάνεια (με πέντε γόμφους). Ο χρήστης τοποθετεί το χέρι του – παλάμη στην επίπεδη επιφάνεια της συσκευής. Οι πέντε γόμφοι χρησιμεύουν ως τα σημεία ελέγχου για μια κατάλληλη τοποθέτηση του δεξιού χεριού του χρήστη. Η συσκευή έχει επίσης τα εξογκώματα για να αλλάξει την ένταση της πηγής φωτός και το εστιακό μήκος της φωτογραφικής μηχανής. Ο καθρέφτης σχεδιάζει την άποψη του χεριού του χρήστη επάνω στη φωτογραφική μηχανή. Η συσκευή ενώνεται με ένα PC με μια εφαρμογή GUI που παρέχει μια ζωντανή οπτική ανατροφοδότηση της κορυφαιός όψης και της πλάγιας όψης του χεριού. Οι ενισχυτές GUI αιχμαλωτίζουν την εικόνα των χεριών.



Η εξαγωγή χαρακτηριστικών γνωρισμάτων περιλαμβάνει τον υπολογισμό των πλατών και των μηκών των δάχτυλων στις διάφορες θέσεις χρησιμοποιώντας τη συλληφθείσα εικόνα. Αυτές οι μετρικές καθορίζουν το διάνυσμα χαρακτηριστικών γνωρισμάτων του χεριού του χρήστη. Η τρέχουσα ερευνητική εργασία περιλαμβάνει τον προσδιορισμό των νέων χαρακτηριστικών γνωρισμάτων που θα οδηγούσαν στον καλύτερο διαχωρισμό μεταξύ δύο διαφορετικών χεριών και του σχεδιασμού ενός παραμορφωμένου προτύπου για το χέρι.

3.3 ΠΑΡΑΜΟΡΦΩΜΕΝΑ ΠΡΟΤΥΠΑ ΓΙΑ ΤΟ ΤΑΙΡΙΑΣΜΑ ΜΟΡΦΗΣ ΧΕΡΙΩΝ

Προτείνουμε να προσεγγίσουμε το πρακτικό πρόβλημα της επαλήθευσης προσώπων χρησιμοποιώντας τα ισχυρά εργαλεία της παραμορφωμένης ανάλυσης. Αυτό παρακινείται από την περιορισμένη δυνατότητα του συστήματος αποκτήσεων μορφής χεριών για να καταχωρήσει τις διαφορετικές εικόνες χεριών χρησιμοποιώντας τους άκαμπτους γόμφους στην πλάκα στερέωσης ανιχνευτών χεριών. Εάν ο χρήστης δεν έχει εκπαιδευθεί κατάλληλα ή εάν δεν συνεργάζεται κατάλληλα, τότε οι προκύπτουσες εικόνες δεν ευθυγραμμίζονται και η απόδοση επαλήθευσης του συστήματος υποβιβάζεται. Επομένως, είναι απαραίτητο να ευθυγραμμιστούν οι επίκτητες μορφές χεριών πριν εξάγει το διάνυσμα χαρακτηριστικών γνωρισμάτων που χρησιμοποιείται για την επαλήθευση.

Χρησιμοποιούμενη μέθοδος:

Λαμβάνοντας υπόψη ένα ζευγάρι κορυφαίων όψεων εικόνων των χεριών που αποκτιούνται από έναν ανιχνευτή χεριών χρησιμοποιούμε το ακόλουθο παράδειγμα για να ταιριάξουμε τη μορφή των χεριών:

- **Αφαίρεση γόμφων**

Μια μάσκα που περιέχει τις γνωστές θέσεις των πέντε γόμφων χρησιμοποιείται για να αντικαταστήσει τους γόμφους με ένα χρώμα που ταιριάζει με το υπόβαθρο.

- **Εξαγωγή περιγράμματος**

Ένα προσαρμοστικό όριο εφαρμόζεται σε κάθε εικόνα και ένα περίγραμμα μετά από τον αλγόριθμο χρησιμοποιείται για να υπολογίσει τη μορφή του χεριού.

- **Εξαγωγή και ευθυγράμμιση δάχτυλων**

Τα πέντε ζευγάρια των αντίστοιχων δάχτυλων εξαγονται από κάθε περίγραμμα και ευθυγραμμίζονται χωριστά όσον αφορά την άκαμπτη ομάδα μετασχηματισμών. Επιλέξαμε να ευθυγραμμίσουμε τα ζευγάρια των δάχτυλων σε αντιδιαστολή με ολόκληρο το χέρι λόγω των ακόλουθων λόγων: (1) ένα ανθρώπινο χέρι είναι ένα αρθρωμένο αντικείμενο και η κίνηση ενός δάχτυλου δεν μπορεί να περιγραφεί από έναν γραμμικό μετασχηματισμό, αλλά μάλλον από ένα σύνολο τοπικών άκαμπτων μετασχηματισμών και μικρών παραμορφώσεων, (2) υπολογιστικά, είναι γρηγορότερο να ανιχνεύσει και να ευθυγραμμίσει τα μεμονωμένα δάχτυλα από ένα ολόκληρο χέρι.

- **Σωστός υπολογισμός απόστασης ζευγαριού**

Κάθε ευθυγράμμιση στο βήμα 3 παράγει ένα σύνολο αλληλογραφιών σημείου. Το μέσο λάθος ευθυγράμμισης (MAE) μεταξύ των δύο μορφών χεριών ορίζεται ως η μέση απόσταση μεταξύ των αντίστοιχων σημείων.

· Επαλήθευση

Το ζευγάρι των μορφών χεριών λέγεται ότι ανήκει στο ίδιο χέρι εάν το MAE τους είναι μικρότερο από ένα κατώτατο όριο T . Συνήθως, ο κανόνας Neymann - PEARSON που ελαχιστοποιεί το ψεύτικο ποσοστό απόρριψης (FRR) για ένα ψεύτικο ποσοστό αποδοχής (FAR) υιοθετείται για να υπολογίσει το T .

Οι εικόνες παρουσιάζουν την ευθυγράμμιση δύο εικόνων χεριών που λαμβάνονται από τον ίδιο χρήστη:



3.4 ΓΕΩΜΕΤΡΙΑ ΧΕΡΙΩΝ ΕΝΑΝΤΙΟΝ ΤΩΝ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ



Αντίθετα από τα δακτυλικά αποτυπώματα, το ανθρώπινο χέρι δεν είναι μοναδικό. Κάποιος μπορεί να χρησιμοποιήσει το μήκος, το πάχος, και την κυρτότητα δάχτυλων για τους σκοπούς της επαλήθευσης αλλά όχι για τον προσδιορισμό. Για μερικά είδη ελέγχου πρόσβασης όπως τον έλεγχο μετανάστευσης και συνόρων, η εισβολή της βιομετρικής (π.χ., δακτυλικά αποτυπώματα) μπορεί να μην είναι επιθυμητή όπως παραβιάζουν την ιδιωτική ζωή. Σε τέτοιες καταστάσεις είναι επιθυμητό να υπάρξει ένα βιομετρικό σύστημα που είναι ικανοποιητικό για την επαλήθευση. Δεδομένου ότι η γεωμετρία χεριών δεν είναι διακριτική, είναι η ιδανική επιλογή. Επιπλέον, τα στοιχεία γεωμετρίας χεριών είναι ευκολότερο να συλλεχθούν. Με τη συλλογή δακτυλικών αποτυπωμάτων απαιτείται τριβή δέρματος από τα συστήματα απεικόνισης και με τα αμφιβληστροειδή βασισμένα στα συστήματα αναγνώρισης, ο ειδικός φωτισμός είναι απαραίτητος. Επιπλέον, η γεωμετρία χεριών μπορεί να συνδυαστεί εύκολα με άλλη βιομετρική, δηλαδή δακτυλικό αποτύπωμα. Κάποιος μπορεί να προβλέψει ένα σύστημα όπου τα δακτυλικά αποτυπώματα χρησιμοποιούνται για (σπάνια) το προσδιορισμό και η γεωμετρία χεριών χρησιμοποιείται για (τη συχνή) επαλήθευση.

ΚΕΦΑΛΑΙΟ 4

ΕΞΕΤΑΣΗ ΙΡΙΔΑΣ &
ΑΜΦΙΒΛΗΣΤΡΟΕΙΔΟΥΣ

ΜΑΤΙ...ΤΟ ΑΣΦΑΛΕΣΤΕΡΟ PASSWORD

Κάποιοι ισχυρίζονται ότι τα μοναδικά χαρακτηριστικά της ίριδας και του αμφιβληστροειδούς, καθιστούν την τεχνητή αναπαραγωγή τους αδύνατη. Δεν αποτελεί, λοιπόν, έκπληξη το γεγονός ότι τα βιομετρικά συστήματα που βασίζονται στα δύο αυτά μέρη του ματιού είναι τα ακριβέστερα και προσφέρουν τη μεγαλύτερη ασφάλεια.

Εκτός από τη μοναδικότητά τους, η ίριδα και ο αμφιβληστροειδής χιτώνας συγκεντρώνουν και ορισμένες άλλες ιδιότητες που τα καθιστούν θαυμάσια εκλογή για την αναγνώριση της ταυτότητας ενός ατόμου: επηρεάζονται ελάχιστα από το πέρασμα του χρόνου, ενώ δεν είναι ιδιαίτερα δεκτικά σε τραυματισμούς ή άλλους παράγοντες, όπως η κούραση. Πολύ στενά συνδεδεμένα με τον ανθρώπινο εγκέφαλο είναι από τα πρώτα μέρη του ανθρώπινου σώματος που αποσυντίθενται μετά το θάνατο. Έτσι, ακόμα και αυτή η ακραία περίπτωση χρήσης ίριδας ή αμφιβληστροειδούς μετά το θάνατο με σκοπό τη διάπραξη απάτης θα πρέπει να αποκλειστεί. Η εξέταση αμφιβληστροειδούς, μάλιστα, θεωρείται η ασφαλέστερη βιομετρική μέθοδος με πρακτικά μηδενικές πιθανότητες παραβίασης.

Όπως ήδη ίσως υποπτεύεστε, η κορυφαία ασφάλεια είναι λογικό να κοστίζει και ανάλογα. Πράγματι, η εξέταση ίριδας και αμφιβληστροειδούς είναι τα ακριβότερα βιομετρικά συστήματα, με κόστος που κάποιες φορές φτάνει αρκετά εκατομμύρια δραχμές. Έτσι, μπορούμε να συμπεράνουμε ότι το κοινό στο οποίο απευθύνονται είναι κυρίως μεγάλες εταιρίες και οργανισμοί που ενδιαφέρονται να εξασφαλίσουν το καλύτερο που μπορεί να τους προσφέρει η σύγχρονη τεχνολογία στον τομέα της ασφάλειας. Παρ' όλα αυτά, η εταιρία Iriscan (μία από τις δύο εταιρίες που ασχολούνται αποκλειστικά με τη συγκεκριμένη βιομετρική μέθοδο) έχει κυκλοφορήσει το PC Iris, ένα προϊόν με σχετικά χαμηλή τιμή (γύρω στα 454,55 €.), το οποίο απευθύνεται στους χρήστες προσωπικών υπολογιστών.

4.1 ΕΞΕΤΑΣΗ ΙΡΙΔΑΣ

Η διαδικασία εξέτασης της ίριδας είναι σχετικά απλή: Μία κάμερα συλλαμβάνει την εικόνα της ίριδας και τη μετατρέπει σε ένα είδος μοναδικού μαθηματικού κώδικα, τον οποίο συγκρίνει στη συνέχεια με το βιομετρικό πρότυπο. Απαραίτητη προϋπόθεση για τη σωστή λειτουργία του συστήματος είναι το περιβάλλον στο οποίο θα είναι εγκαταστημένο να έχει πολύ καλό φωτισμό, ώστε η "φωτογραφία" της ίριδας να είναι όσο το δυνατόν καλύτερη.

Υπάρχουν δύο είδη μεθόδων αναγνώρισης της ίριδας, η ενεργητική και η παθητική. Κατά την ενεργητική μέθοδο απαιτείται η συμμετοχή του χρήστη, ο οποίος πρέπει να βοηθήσει την κάμερα του συστήματος να εστιάσει στην ίριδα μετακινώντας το κεφάλι του μερικά εκατοστά εμπρός και πίσω. Το γεγονός αυτό σίγουρα υπονομεύει τη λειτουργικότητα και την ευελιξία της μεθόδου, αφού είναι φανερό ότι για να διασφαλιστούν σωστά αποτελέσματα ο χρήστης χρειάζεται καθοδήγηση από κάποιον που θα επιβλέπει την όλη διαδικασία. Αντίθετα, κατά την παθητική εξέταση ίριδας αντί για μία κάμερα υπάρχουν πολλές, οι οποίες εντοπίζουν αυτόματα πρώτα το πρόσωπο, μετά το μάτι, και τέλος την ίριδα του χρήστη, χωρίς να είναι αναγκαία καμία απολύτως συμμετοχή από τον ίδιο. Δεν χρειάζεται να σημειώσουμε ότι το συγκεκριμένο σύστημα έχει τον υψηλότερο δείκτη ευχρηστίας από όλα τα υπόλοιπα (επίσης δεν χρειάζεται να αναφέρουμε ότι

είναι και το ακριβότερο).

Θα περίμενε κάποιος ότι τουλάχιστον η παθητική εξέταση ίριδας θα έβρισκε σχετικά υψηλή αποδοχή από το κοινό. Το γεγονός όμως ότι σε όλες τις παραλλαγές τις μεθόδου ο χρήστης βρίσκεται αντιμέτωπος με κάμερες φαίνεται ότι λειτουργεί ιδιαίτερα αρνητικά στην ψυχολογία του. Άλλωστε, σε κανέναν δεν αρέσει να νοιώθει ότι παρακολουθείται ή, ακόμα περισσότερο, ότι βιντεοσκοπείται ή φωτογραφίζεται. Δεν είναι τυχαίο ότι το μεγαλύτερο μέρος του κοινού θεωρεί αυτές τις μεθόδους από τις περισσότερες "αδιάκριτες".

4.2 TO PC IRIS

Δημιούργημα της πρωτοπόρου εταιρίας στο χώρο της εξέτασης της ίριδας, της IriScan, το προϊόν αυτό ξεφεύγει από τον έλεγχο φυσικής πρόσβασης στον οποίο προσανατολίζονται τα περισσότερα συστήματα του είδους. Αντίθετα, με τη μορφή ενός μικρού και κομψού περιφερειακού και με μία σχετικά προσιτή τιμή, στοχεύει στο να αυξήσει την ασφάλεια των προσωπικών υπολογιστών μας σε διάφορα επίπεδα. Το PC Iris έχει ένα μεγάλο εύρος εφαρμογών, όπως διασφάλιση εμπορικών συναλλαγών μέσω Internet, έλεγχο πρόσβασης σε βάσεις δεδομένων, προστασία εγγράφων και φακέλων, δίκτυα υπολογιστών κ.λπ.

Το πακέτο αποτελείται από μία συσκευή σάρωσης της ίριδας, δύο κάρτες επέκτασης που θα πρέπει να τοποθετηθούν στον υπολογιστή και, φυσικά, το απαραίτητο software. Η χρήση του συστήματος είναι αρκετά απλή: Ο χρήστης τοποθετεί τη συσκευή σάρωσης 7-8 εκατοστά μπροστά από το μάτι του και πατάει το κουμπί εκκίνησης. Η απόκριση του συστήματος είναι πολύ γρήγορη, σε χρόνους συνήθως κάτω των δύο δευτερολέπτων, ενώ το ποσοστό λάθους σχεδόν μηδενικό. Οι απαιτήσεις του PC Iris σε υπολογιστική ισχύ είναι ιδιαίτερα χαμηλές: Pentium 133 και 32MB μνήμη. Όσον αφορά στην τιμή του, αυτή κυμαίνεται στα 500 δολάρια, δηλαδή περίπου 155.000 δρχ. Καθόλου ακριβό γι' αυτά που προσφέρει.

ΆΛΛΑ ΠΡΟΪΟΝΤΑ

Εκτός του PC Iris, η εταιρία IriScan έχει κυκλοφορήσει άλλα δύο προϊόντα, τα οποία είναι προσανατολισμένα στον έλεγχο φυσικής πρόσβασης. Τα System 2100 και 2200 είναι στην ουσία εξειδικευμένα δίκτυα υπολογιστών, με έναν κεντρικό server, στον οποίο υπάρχει η βάση δεδομένων με τα βιομετρικά πρότυπα, και σταθμούς-τερματικά συνδεδεμένα με ειδικές κάμερες σε κάθε σημείο ελέγχου. Το εξελιγμένο System 2200, μάλιστα, προσφέρει ορισμένες εξαιρετικές δυνατότητες, όπως αυτόματη εστίαση στην ίριδα του χρήστη αλλά και φωνητική καθοδήγηση, αν αυτό κριθεί απαραίτητο! Και εδώ οι απαιτήσεις σε υπολογιστική ισχύ είναι σχετικά μικρές: Για τον κεντρικό server χρειάζεται Pentium 233, 5G σκληρός δίσκος και 64MB μνήμη, ενώ για κάθε σημείο ελέγχου Pentium 166, 2,5G σκληρός δίσκος και 16MB μνήμη. Τα συστήματα της IriScan χρησιμοποιούνται από αρκετές εταιρίες για τον έλεγχο πρόσβασης των υπαλλήλων τους, αλλά και σε διάφορες φυλακές για τη σωστή αστυνόμευση των κρατουμένων.

Με τα βιομετρικά συστήματα εξέτασης ίριδας ασχολείται άλλη μία εταιρία, η Sensar, της οποίας τα προϊόντα στοχεύουν σε εντελώς διαφορετικό κοινό από αυτό της IriScan. Αξιοποιώντας τη συνεργασία της με την NCR, το μεγαλύτερο κατασκευαστή ATM αυτή τη στιγμή, έχει ήδη ξεκινήσει αρκετά πιλοτικά προγράμματα χρήσης του συστήματός της σε διάφορα τραπεζικά δίκτυα με αξιοσημείωτη επιτυχία. Παρόμοια επιτυχημένη ήταν και η χρήση του συστήματος στους Χειμερινούς Ολυμπιακούς Αγώνες του Nagano, στην Ιαπωνία, για τον έλεγχο της πρόσβασης στο χώρο φύλαξης των τουφεκίων της σκοποβολής.

4.3 ΕΞΕΤΑΣΗ ΑΜΦΙΒΛΗΣΤΡΟΕΙΔΟΥΣ

Όπως προαναφέραμε, η εξέταση αμφιβληστροειδούς θεωρείται αυτή τη στιγμή η ασφαλέστερη βιομετρική μέθοδος. Δυστυχώς, όμως, η μεγάλη συμμετοχή που απαιτεί από την πλευρά του χρήστη την κάνει να θεωρείται η πιο δύσχρηστη. Ο χρήστης τοποθετείται γύρω στους 7 πόντους μπροστά από ένα προσοφθάλμιο και προσπαθεί να εστιάσει μέσα από αυτό για μερικά δευτερόλεπτα σε μία μικρή πράσινη κουκκίδα. Κάποια στιγμή το μάτι αποκτά τη σωστή εστίαση και ένας scanner συλλαμβάνει τη διάταξη των αιμοφόρων αγγείων που βρίσκονται στο κέντρο του αμφιβληστροειδούς και είναι γνωστή ως φοβέα. Από το σημείο αυτό η διαδικασία είναι ίδια με αυτή που ακολουθείται κατά την εξέταση ίριδας. Το σύστημα μετατρέπει την εικόνα σε μία μοναδική μαθηματική αναπαράσταση και τη συγκρίνει με το βιομετρικό πρότυπο.

Έχοντας πολλά κοινά σημεία με την εξέταση της ίριδας, το σύστημα εξέτασης του αμφιβληστροειδούς γνωρίζει και αυτό μέση αποδοχή από το κοινό. Ενδιαφέρον προκαλεί το γεγονός ότι η εν λόγω μέθοδος θεωρείται η πιο "αδιάκριτη" από όλες, εντύπωση που προφανώς δημιουργεί η δοκιμασία στην οποία υποβάλλεται ο χρήστης κατά την αναγνώριση.

ΕΤΑΙΡΙΕΣ ΚΑΙ ΠΡΟΪΟΝΤΑ

Μόνο μία εταιρία ασχολείται με τη βιομετρική αυτή μέθοδο, η EyeDentify. Η εταιρία εξελίσσει και προωθεί το βασικό προϊόν της, το ICAM 2001, το οποίο αριθμεί ήδη αρκετές εγκαταστάσεις σε πολλές μεγάλες εταιρίες και οργανισμούς διάφορων χωρών, κυρίως για περιπτώσεις ελέγχου φυσικής πρόσβασης σε προστατευμένους χώρους. Το ICAM 2001 χρησιμοποιείται επίσης από πολλές αμερικανικές κυβερνητικές υπηρεσίες, μη εξαιρουμένου του FBI.

4.4 ΈΛΕΓΧΟΣ ΙΡΙΔΑΣ ΣΤΟΥΣ ΑΕΡΟΛΙΜΕΝΕΣ



Ο αερολιμένας Heathrow εξετάζει ένα νέο σύστημα ταυτότητας υψηλής τεχνολογίας που εξετάζει το μάτι των επιβατών, παρά το διαβατήριό τους καθώς περνούν από τον έλεγχο μετανάστευσης.

Το Heathrow είναι ο πρώτος βρετανικός αερολιμένας στον οποίο πραγματοποιήθηκε μια μεγάλης κλίμακας δοκιμή ,η αναγνώριση ίριδας. Ο στόχος είναι να επιταχυνθεί η κυκλοφορία των επιβατών μέσω του τερματικού και να ανιχνευθούν οι παράνομοι μετανάστες. Συνολικά 2.000 επιβάτες που πετούν συχνά από τη Βόρεια Αμερική στο Heathrow, με τις πτήσεις της Virgin και British Airways συμμετείχαν στην πέντε μηνών δοκιμή.

ΜΟΝΑΔΙΚΟ

Κάθε επιβάτης θα έχει μια εικόνα μια από την ίριδα του ματιού του που αποθηκεύεται στον υπολογιστή. Αντί της παρουσίασης διαβατηρίου τους στην άφιξη θα πάνε σε ένα περίπτερο όπου σε δευτερόλεπτα μια φωτογραφική μηχανή θα ελέγχει εάν το σχέδιο της ίριδας τους ταιριάζει με τα αρχεία των υπολογιστών. Σε αυτή την περίπτωση η είσοδος θα ανοίγει αυτόματα. Με τη δοκιμή αυτή θα εξεταστεί η τεχνολογία και η αντίδραση των επιβατών. Η αεριωθούμενη διαδικασία αναγνώρισης ιριδών, που αναπτύσσεται στις ΗΠΑ, θεωρείται ότι είναι μια ενιαία μέθοδος προσδιορισμού στον κόσμο με υψηλή ακρίβεια,.

Ο Evan Smith, ανώτερος αντιπρόεδρος της εταιρίας EyeTicket, είπε ότι αυτό ήταν το αποκορύφωμα της εργασίας τεσσάρων ετών. Είπε: "Η ίριδα είναι πιο μοναδική από το δακτυλικό αποτύπωμα και είναι το πιο μοναδικό πράγμα έξω από το ανθρώπινο σώμα. "Είχαμε μια πολύ καλή πρόωρη ανταπόκριση και μια πλημμύρα εφαρμογών. "Αναμένουμε ότι η δοκιμή θα είναι εξαιρετικά δημοφιλής και περιμένουμε ότι η τεχνολογία αυτή θα υιοθετηθεί τελικά στους αερολιμένες σε όλο τον κόσμο."

ΑΣΦΑΛΕΙΑ

Αναμένεται ότι η τεχνολογία θα μπορούσε να έχει μελλοντικά οφέλη ασφάλειας, με τους βρετανικούς αερολιμένες ακόμα και σε ανάλογη περίπτωση με αυτήν τις 11 Σεπτεμβρίου.

Ο Mike Temple διευθυντής της BAA Heathrow είπε: "Με αυτήν την δοκιμή ελπίζουμε να καθορίσουμε ότι η τεχνολογία αναγνώρισης ιριδών μπορεί να αποδειχθεί μια ασφαλής, αποτελεσματική και τα ιδιαίτερα ακριβής σημασίας, διαβεβαιώνοντας ότι οι επιβάτες της άφιξης είναι νόμιμοι εισερχόμενοι στο Ηνωμένο Βασίλειο."

Η δοκιμή κανονίστηκε από τη διεθνή ένωση αεροπορικών μεταφορών (IATA) που απλοποιεί την ομάδα ενδιαφέροντος ταξιδιού επιβατών, η οποία περιλαμβάνει τους αερολιμένες, τις αερογραμμές, τις αρχές μετανάστευσης και τους τεχνολογικούς προμηθευτές παγκοσμίως.

Οι "αυτοματοποιημένοι σταθμοί αναγνώρισης ιρίδων" προγραμματίζονται για τον αερολιμένα JFK της Νέας Υόρκης και τον αερολιμένα Dulles της Ουάσιγκτον.

Ολόκληρη η διαδικασία διαρκεί μόνο μερικά δευτερόλεπτα και δεν υπάρχει καμία επαφή με το σώμα ή με τα λείζερ ή άλλες ενδεχομένως επιβλαβείς πηγές φωτός.

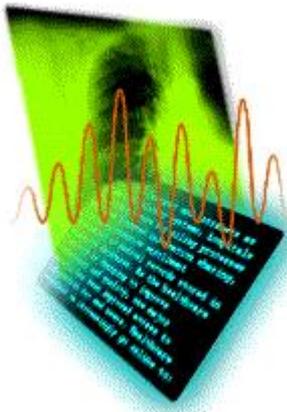
Οι επιβάτες που συμμετέχουν καλούνται να φέρουν τα διαβατήριά τους κατά τη διάρκεια της δοκιμαστικής περιόδου εάν θελήσουν να ελέγξουν οι ανώτεροι υπάλληλοι μετανάστευσης τις λεπτομέρειές τους.

ΚΕΦΑΛΑΙΟ 5

ΑΝΑΓΝΩΡΙΣΗ ΦΩΝΗΣ

Τεχνολογίες Ανθρώπινης Γλώσσας

Ένα όραμα του μέλλοντος



Η τεχνολογία της πληροφορίας αλλάζει τον τρόπο που ζούμε, εργαζόμαστε και αλληλεπιδρούμε με τα πράγματα γύρω μας. Οι βιομηχανίες υπολογιστικών συστημάτων, επικοινωνιών και ηλεκτρονικών συσκευών συγχωνεύονται με το πέρασμα του χρόνου και πολύ σύντομα θα ανακαλύψουμε ότι με οποιοδήποτε πράγμα και αν αλληλεπιδρούμε, από παιχνίδια και τηλέφωνα μέχρι αυτοκίνητα και υπολογιστές θα περικλείει μεγαλύτερη υπολογιστική ισχύ από τον γρηγορότερο σημερινό προσωπικό υπολογιστή. Οι μηχανές του μέλλοντος θα κάνουν πολύ περισσότερα πράγματα για εμάς, υπό τον όρο ότι θα μπορούμε να αλληλεπιδράσουμε με αυτές και να τους πούμε τι θέλουμε.

Μια Ηχηρή Ιδέα

Με την τεχνολογία αναγνώρισης φωνής, όλοι οι άνθρωποι θα μπορούν να μιλούν στις μηχανές με τον ίδιο τρόπο που μιλούν σε άλλους ανθρώπους, με τη συζήτηση. Μηχανές εφοδιασμένες με ειδικά συστήματα θα μπορούν να ανταποκρίνονται στη φωνή, στη φυσική γλώσσα και στις εκφράσεις του προσώπου. Θα μπορούν να συμμετέχουν σε συζητήσεις και θα μπορούν να αναγνωρίσουν, να εξακριβώσουν και να κατατάξουν τους ανθρώπους ανάλογα με τη φωνή και άλλα βιομετρικά χαρακτηριστικά.

Σήμερα, επικοινωνούμε με τις μηχανές με τον άμεσο χειρισμό, χρησιμοποιώντας διακόπτες, τιμόνια, τηλεκοντρόλ ή ποντίκια και οθόνες αφής. Το πληκτρολόγιο «παίζει» έναν πολύ σημαντικό ρόλο στην μεταβίβαση κειμένου και πολύπλοκων εντολών. Όμως, όσο οι δυνατότητες των μηχανών αυξάνονται κανένας από τους παραπάνω τρόπους δεν επαρκεί, για την καλή επικοινωνία χρήστη και μηχανής. Το μελλοντικό όραμα για τις τεχνολογίες ανθρώπινης γλώσσας είναι, να μπορεί να χρησιμοποιηθούν

- από όλους
- με οποιαδήποτε συσκευή
- σε οποιοδήποτε περιβάλλον

Οι τεχνολογίες για την πραγματοποίηση αυτού του οράματος είναι καθοδόν.

Πολλές από τις εξελίξεις που βλέπουμε γύρω μας, στην επιστήμη ή και τους υπολογιστές, είναι φανερό ότι είναι εμπνευσμένες από την επιστημονική φαντασία. Είναι ιδέες, όπως η ρομποτική ή αυτή του ηλεκτρονικού σπιτιού, που τροφοδοτούν το ρητό "life imitates art", "η ζωή μιμείται την τέχνη" (ή και το αντίστροφο, φυσικά). Ίσως να είναι αναμενόμενο από τα πιο ρομαντικά μυαλά στους αντίστοιχους επιστημονικούς ή μηχανολογικούς τομείς να αντλούν την έμπνευσή τους από προϊόντα της φαντασίας που έχουν περάσει στην ευρεία συνείδηση ως εφικτά και υλοποιήσιμα πράγματα. Αυτό που τελικά συμβαίνει είναι να "προσγειώνονται" κατά κάποιον τρόπο οι ιδέες, προσαρμόζοντάς τες στα δεδομένα

της εποχής με προοπτικές για περαιτέρω ανάπτυξη. Ούτως ή άλλως, έτσι επιτυγχάνεται η οποιαδήποτε εξέλιξη σύμφωνα με τον δυτικό τρόπο σκέψης: κάποιος θέτει τη βάση και όλοι οι υπόλοιποι προσπαθούν να χτίσουν πάνω σε αυτή.

Μία από τις γοητευτικότερες ιδέες που έχουν έλθει στο προσκήνιο είναι η αλληλεπίδραση του ανθρώπου με τα μηχανήματα με χρήση φωνητικών εντολών. Ο άνθρωπος διατάζει και ο υπολογιστής υπακούει. Στην επέκταση αυτής της ιδέας υπάρχει φυσικά η τεχνητή νοημοσύνη, κάτι που προς το παρόν φαίνεται μακρινό. Η αναγνώριση φωνής, παρ' όλα αυτά, είναι κάτι που αποτελεί πεδίο έρευνας τα τελευταία χρόνια. Η πρόοδος σε αυτό τον τομέα φαίνεται να πραγματοποιείται με άλματα, κυρίως στο τέλος της προηγούμενης δεκαετίας.

Το ξεκίνημα ήταν, όπως πάντα, ταπεινό και με πενιχρά αποτελέσματα. Κι αυτό εξηγείται αν σκεφτεί κανείς από τη μία με πόσους διαφορετικούς τρόπους μπορεί να προφερθεί μια λέξη (αφήνοντας κατά μέρος το πώς την προφέρουν διαφορετικά άτομα) και, από την άλλη, το πόσο ψυχρή μηχανή είναι ο υπολογιστής. Ήταν εμφανές, ύστερα από λίγες δοκιμές, ότι χρειαζόταν διαφορετική μέθοδος προσέγγισης στο πρόβλημα, με χρήση αλγορίθμων διαφορετικών από τους "συνηθισμένους". Η λύση δόθηκε με τη βοήθεια των νευρωνικών δικτύων.

Τα νευρωνικά δίκτυα έλυσαν το βασικό, αλλά προκάλεσαν επιμέρους προβλήματα. Αυτά κατ' ουσίαν ήταν προβλήματα επεξεργαστικής ισχύος αλλά και μνήμης. Όπως όλοι ξέρουμε, όμως, τα τελευταία χρόνια είδαμε εντυπωσιακή εξέλιξη και στους δύο αυτούς τομείς. Έτσι, έχουμε πλέον τη δυνατότητα όχι μόνο φραστικών εντολών στον υπολογιστή μας αλλά και ελεύθερης υπαγόρευσης. Από ό,τι φαίνεται, μάλιστα, τα σύγχρονα προγράμματα τα καταφέρνουν ιδιαίτερα καλά. Σε αυτό το σημείο υπάρχει μία φιλοσοφικής φύσης ένσταση ορισμένων ερευνητών του συγκεκριμένου τομέα. Το σκεπτικό είναι ότι, για να εξομοιώσουμε την αναγνώριση φωνής με τον υπολογιστή, φαίνεται να πιέζουμε την τεχνολογία στα άκρα (μνήμη και επεξεργαστή), χωρίς να έχουμε το απόλυτο αποτέλεσμα, αλλά μία καλή προσέγγιση. Σε αντίθεση, ο εγκέφαλός μας τα καταφέρνει εξαιρετικά, χωρίς τόσο πολύ κόπο. Το επιχείρημα αυτό προτείνει ότι μάλλον υπάρχει πιο απλός και κομψός τρόπος για να πετύχουμε το ίδιο αποτέλεσμα, ο οποίος τρόπος πιθανόν να επιζητεί συντριπτική αναθεώρηση των ιδεών που έχουμε μέχρι τώρα. Αυτό όμως ίσως ανήκει πιο πολύ στον κόσμο της επιστημονικής φαντασίας κι λιγότερο στην πραγματικότητα!

Περνώντας στο προκείμενο, ύστερα από επαφή με 4 εταιρίες του εξωτερικού, οι οποίες διαθέτουν αντίστοιχα προγράμματα, οι δοκιμές άρχισαν. Και τα τέσσερα, όμως, όσο καλά και να είναι, έχουν ένα σημαντικό μειονέκτημα: δεν υποστηρίζουν ελληνική αναγνώριση φωνής, γεγονός απογοητευτικό για εμάς τους Έλληνες χρήστες, που φαίνεται να έχουμε μείνει λίγο πίσω από το χορό των εξελίξεων. Βέβαια, η έλλειψη της ελληνικής αναγνώρισης από τα προγράμματα που δοκιμάστηκαν, δεν υποβαθμίζει την αξία τους, απλώς θέτει την κριτική που κάνουμε σε άλλη βάση. Κρίνεται δηλαδή αν τα προγράμματα πετυχαίνουν ικανοποιητική αναγνώριση φωνής στη "μητρική" τους γλώσσα. Είναι αναπόφευκτο κάποια στιγμή στο μέλλον να έχουμε και στη γλώσσα μας σωστή αναγνώριση φωνής.

Τέλος, ένα θέμα που πρέπει να θίξουμε, είναι οι απαιτήσεις αυτών των προγραμμάτων. Παρ' όλο που κάθε πρόγραμμα προτείνει μία ελάχιστη σύνθεση για τον υπολογιστή μας, από ό,τι φάνηκε, για να δουλεύουμε σχετικά άνετα με αυτά

τα πακέτα πρέπει να έχουμε επεξεργαστή κλάσης Pentium II και συχνότητα τουλάχιστον 300MHz. Τα πακέτα επίσης προτείνουν ως ελάχιστη RAM τα 64MB, αλλά από την εμπειρία μας φαίνεται ότι χρειαζόμαστε τουλάχιστον 128 MB έτσι ώστε να μπορούμε να δουλέψουμε άνετα και με τον κειμενογράφο της αρεσκείας μας.

5.1 ΤΙ ΚΡΥΒΕΙ ΜΙΑ ΑΠΛΗ ΦΩΝΗ

Η αναγνώριση της ανθρώπινης φωνής από τους υπολογιστές αποτελεί ένα αρκετά περίπλοκο πρόβλημα. Η φύση, τόσο της ανθρώπινης φωνής όσο και των διάφορων εξωγενών παραγόντων που υπεισέρχονται στην όλη διαδικασία, είναι τέτοια, που καθιστά το πρόβλημα μη ντετερμινιστικό. Για αυτόν το λόγο και επεξεργασία σημάτων, μέχρι τη γλωσσολογία.

Στη συνέχεια θα αναφερθούμε στην ιστορία και την εξέλιξη των συστημάτων αναγνώρισης φωνής, στους παράγοντες που υπεισέρχονται κατά την όλη διαδικασία, στις τεχνολογίες που αναπτύχθηκαν, στους διάφορους τύπους των συστημάτων που χρησιμοποιούνται, θα περιγράψουμε τη διαδικασία αναγνώρισης φωνής και τέλος θα παρουσιάσουμε κάποια από τα πιο κοινά προβλήματα που παρουσιάζονται κατά τη διαδικασία αυτή.

ΙΣΤΟΡΙΑ & ΕΞΕΛΙΞΗ

Οι πρώτες προσπάθειες για τη δημιουργία συστημάτων αναγνώρισης φωνής έγιναν στα εργαστήρια της Bell κατά τη δεκαετία του 1960. Οι έρευνες την εποχή εκείνη επικεντρώνονταν κυρίως σε συστήματα τα οποία θα ήταν σε θέση να αναγνωρίζουν μεμονωμένες λέξεις, δηλαδή μη συνεχή λόγο, και τη φωνή ενός μόνο συγκεκριμένου ομιλητή. Το πρώτο προϊόν που κυκλοφόρησε με αυτά τα χαρακτηριστικά ήταν το σύστημα VIP 100, το οποίο αναπτύχθηκε στις αρχές της δεκαετίας του 1970. Οι πρώτες αυτές επιτυχημένες προσπάθειες έδωσαν την κατάλληλη ώθηση, ώστε να αρχίσει παράλληλα η έρευνα για συστήματα αναγνώρισης συνεχούς λόγου, τα οποία δεν θα εξαρτώνται από τον ομιλητή. Η διαθέσιμη υπολογιστική και αποθηκευτική ισχύς της περιόδου εκείνης ήταν ωστόσο περιορισμένη, με αποτέλεσμα οι τεχνολογίες αναγνώρισης φωνής να εξελίσσονται με πολύ αργούς ρυθμούς μέχρι περίπου τα μέσα της δεκαετίας του 1980, όποτε άρχισε να γίνεται ορατή η δυνατότητα δημιουργίας πιο εξελιγμένων συστημάτων, ικανών να χειρίζονται και να αναγνωρίζουν μεγαλύτερο πλήθος λέξεων και συνεχή λόγο. Η δεκαετία του '90 αποτέλεσε σταθμό και περίοδο ωρίμανσης για τα συστήματα αναγνώρισης φωνής, με αποτέλεσμα μέχρι σήμερα να έχουμε μία συνεχή βελτίωση της αξιοπιστίας των συστημάτων και παράλληλα των υπηρεσιών τις οποίες τα συστήματα αυτά μπορούν πλέον να προσφέρουν.

ΤΥΠΟΙ ΣΥΣΤΗΜΑΤΩΝ ΑΝΑΓΝΩΡΙΣΗΣ ΦΩΝΗΣ

Τα συστήματα αναγνώρισης φωνής μπορούν να διαχωριστούν σε διάφορες κατηγορίες, ανάλογα με τα χαρακτηριστικά τους και τους τύπους φωνής που υποστηρίζουν. Μία βασική διάκριση είναι σε συστήματα αναγνώρισης συνεχούς λόγου και διακριτού λόγου:

1. Συστήματα αναγνώρισης διακριτού λόγου

Ονομάζονται τα συστήματα τα οποία προϋποθέτουν ότι ο ομιλητής θα διαχωρίζει τις λέξεις, δηλαδή ότι η ομιλία του θα είναι διακοπτόμενη, θα πραγματοποιεί δηλαδή μικρές παύσεις μεταξύ των λέξεων. Η απαίτηση αυτή προκύπτει από το γεγονός ότι τα εν λόγω συστήματα πρέπει να γνωρίζουν πότε ξεκινάει και πότε σταματάει κάθε λέξη.

2. Συστήματα αναγνώρισης συνεχούς λόγου

Ονομάζονται τα συστήματα τα οποία είναι ικανά να λειτουργήσουν ακόμα και αν η ομιλία είναι συνεχής, όπως δηλαδή συμβαίνει κατά την καθομιλουμένη. Μία δεύτερη βασική διάκριση αφορά στην ευαισθησία την οποία έχουν τα συστήματα όσον αφορά στον ομιλητή. Με βάση αυτό το κριτήριο, τα συστήματα χωρίζονται στις ακόλουθες κατηγορίες:

- Συστήματα αναγνώρισης ενός ομιλητή

Είναι τα συστήματα τα οποία είναι σε θέση να αναγνωρίσουν τη φωνή ενός μόνο ομιλητή και μόνο εφόσον έχουν "προπονηθεί" κατάλληλα. Λέγοντας "προπονηθεί", εννοούμε τη διαδικασία αυτή κατά την οποία τα συστήματα προσαρμόζονται στον τρόπο ομιλίας ενός συγκεκριμένου προσώπου, δηλαδή στην προφορά και στο συχνοτικό περιεχόμενο της φωνής του. Τα συστήματα αυτά είναι και τα απλούστερα δυνατά.

- Προσαρμοζόμενα συστήματα

Τα συστήματα αυτά αποτελούν εξέλιξη των συστημάτων αναγνώρισης ενός ομιλητή. Έχουν τη δυνατότητα να προσαρμόζονται πολύ πιο γρήγορα στη φωνή του εκάστοτε ομιλητή απ' ό,τι τα συστήματα της προηγούμενης κατηγορίας. Η δε λειτουργία τους βασίζεται στη χρήση λεξιλογίων (βάσεων δεδομένων που περιέχουν λέξεις), στα οποία οι λέξεις είναι κωδικοποιημένες με τέτοια μορφή, ώστε να έχουν κάποια χαρακτηριστικά, τα οποία να είναι κοινά για ένα μεγάλο πλήθος ομιλητών.

- Συστήματα ανεξάρτητα ομιλητή

Τα συστήματα αυτά είναι τα πλέον εξελιγμένα και είναι σε θέση να αναγνωρίζουν την ομιλία, ανεξάρτητα από το τι έχει ειπωθεί (ουσιαστικά ανεξάρτητα από το αν γνωρίζουν τη λέξη, δηλαδή αν την έχουν καταχωρισμένη στο λεξιλόγιό τους) και ανεξάρτητα από το ποιος μιλάει. Τα περισσότερα συστήματα από αυτά που χρησιμοποιούνται σήμερα είναι προσαρμοζόμενα συστήματα αναγνώρισης συνεχούς ομιλίας. Δηλαδή είναι ικανά να αναγνωρίζουν συνεχή λόγο, ενώ για να υπάρξει η μέγιστη δυνατή απόδοση, απαιτείται κάποια "προπόνηση" του συστήματος, η οποία συνήθως περιλαμβάνει την ανάγνωση καθορισμένων λέξεων και κειμένων. Τα συστήματα αυτά έχουν το θετικό χαρακτηριστικό ότι μετά την αρχική "προπόνηση", προσαρμόζονται διαρκώς στον ομιλητή μέχρι να προσεγγίσουν το μέγιστο δυνατό της απόδοσής τους. Το βασικό πλεονέκτημα του χαρακτηριστικού αυτού είναι ότι τα συστήματα διατηρούν υψηλή αξιοπιστία, ακόμα και αν η φωνή του ομιλητή αλλοιωθεί προσωρινά, εξαιτίας, για παράδειγμα, ενός κρυολογήματος. Τα συστήματα αυτά συνήθως υποστηρίζουν και την επέκταση του υπάρχοντος λεξιλογίου, είτε κατόπιν επέμβασης του χρήστη είτε μέσω λεξιλογίων τα οποία διατίθενται από τις εταιρίες που τα κατασκεύασαν.

ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΓΝΩΡΙΣΗΣ ΦΩΝΗΣ

Η διαδικασία που ακολουθούν τα διάφορα συστήματα κατά την αναγνώριση φωνής, παρ' όλο που διαφέρει από σύστημα σε σύστημα, ακολουθεί κάποιες βασικές αρχές. Περιληπτικά θα μπορούσαμε να πούμε ότι σε γενικές γραμμές η διαδικασία αποτελείται από τα ακόλουθα βήματα:

- Ψηφιοποίηση του ηχητικού σήματος
- Επεξεργασία σήματος, αναγνώριση φθόγγων, λέξεων και προτάσεων
- Σύγκριση με το υπάρχον λεξιλόγιο
- Επεξεργασία φυσικής γλώσσας

Ψηφιοποίηση του ηχητικού σήματος

Η φωνή, και γενικότερα ο ήχος, είναι ένα συνεχές σήμα (η ένταση της φωνής μπορεί να παίρνει οποιαδήποτε τιμή) συνεχούς χρόνου (δηλαδή ο χρόνος δεν κάνει "απότομα" βήματα, αλλά ακολουθεί συνεχείς μεταβολές). Η συνεχής αυτή φύση του σήματος (θα αναφερόμαστε στη φωνή δηλαδή στο ηχητικό σήμα που αποτελεί και την είσοδο για το σύστημα αναγνώρισης φωνής ως σήμα) καθιστά αδύνατη την επεξεργασία του από οποιονδήποτε υπολογιστή. Για το λόγο αυτόν το σήμα πρέπει να μετατραπεί σε μορφή που ο υπολογιστής να μπορεί εύκολα να αποθηκεύσει και να επεξεργαστεί, δηλαδή σε σήμα διακριτού πλάτους και διακριτού χρόνου, σε σήμα του οποίου η ένταση θα έχει προκαθορισμένες στάθμες και οι στάθμες αυτές θα αντιστοιχούν σε ορισμένες χρονικές στιγμές πολύ μικρής διάρκειας. Η διαδικασία αυτή γίνεται αυτόματα μέσω του ADC, δηλαδή του Analog to Digital Converter της κάρτας ήχου του υπολογιστή, ο οποίος τελικά μετατρέπει το ηλεκτρικό σήμα του μικροφώνου σε bytes.

Τα bytes αυτά αποθηκεύονται στη μνήμη του υπολογιστή. Μετά τη διαδικασία της ψηφιοποίησης λαμβάνει συνήθως χώρα ο περιορισμός των συχνοτήτων του σήματος. Επειδή το ηχητικό σήμα που λαμβάνει το μικρόφωνο περιέχει πολύ περισσότερες συχνότητες από τις ακουστικές, οι οποίες αυξάνουν κατά πολύ το χρόνο επεξεργασίας αλλά και την πιθανότητα σφάλματος, το σήμα διέρχεται από φίλτρο συχνοτήτων, το οποίο επιτρέπει μόνο τη διέλευση των συχνοτήτων από 100Hz έως 3100Hz.

Ακουστική επεξεργασία σήματος

Το στάδιο αυτό περιλαμβάνει την κατάλληλη κωδικοποίηση του σήματος, το διαχωρισμό του σε πολύ μικρά τμήματα, διάρκειας από 10 έως 50 χιλιοστών του δευτερολέπτου και την επεξεργασία τους, η οποία περιλαμβάνει την αναγνώριση των ακουστικών παραμέτρων κάθε τμήματος, δηλαδή κάποιων χαρακτηριστικών κάθε τμήματος, τα οποία αφορούν σε τυχόν επαναλαμβανόμενες μορφές του σήματος, καθώς και κάποια χαρακτηριστικά που αφορούν στις συχνότητες από τις οποίες αποτελείται κάθε τμήμα.

Υπάρχουν δύο βασικές μέθοδοι με τις οποίες αναγνωρίζονται και υπολογίζονται οι ακουστικές παράμετροι, η μέθοδος Linear Predictive Coding (LPC), η οποία είναι αυτή που χρησιμοποιείται κατά κύριο λόγο, και η μέθοδος Filter Bank Analysis.

Έχοντας υπολογίσει τις ακουστικές παραμέτρους, ακολουθεί η σύγκριση με το υπάρχον λεξιλόγιο, δηλαδή το κυρίως μέρος της διαδικασίας, κατά το οποίο οι ακουστικές παράμετροι του σήματος που έχει καταγραφεί θα συγκριθούν με αυτές που είναι καταχωρισμένες στο λεξιλόγιο του προγράμματος ώστε να βρεθούν ομοιότητες που αφορούν σε λέξεις, φθόγγους ή και μικρές προτάσεις. Όσο απλή και αν φαίνεται η διαδικασία αυτή, στην πραγματικότητα είναι η πιο επίπονη, αφού η πιθανότητα να έχουμε ακριβή ομοιότητα σε όλες τις ακουστικές παραμέτρους είναι σχεδόν μηδαμινή. Αυτό που πραγματικά συμβαίνει είναι να επιλεγούν οι πιο πιθανοί φθόγγοι, λέξεις ή προτάσεις και με παράλληλη ορθογραφική, συντακτική και στα πιο εξελιγμένα και πειραματικά συστήματα νοηματική ανάλυση να επιλεγεί από αυτούς ο πιο κατάλληλος.

Η επιλογή του πιο πιθανού φθόγγου ή λέξης γίνεται με διάφορους τρόπους και χρησιμοποιώντας διάφορα μοντέλα. Το πιο γνωστό από αυτά είναι τα νευρωνικά δίκτυα, τα οποία έχουν, συν τοις άλλοις, την ενδιαφέρουσα εγγενή δυνατότητα να αυτοοργανώνονται συνεχώς, δηλαδή να "προπονοούνται" και να μαθαίνουν τα χαρακτηριστικά των ακουστικών παραμέτρων του εκφωνητή μέσω των διορθώσεων που αυτός κάνει.

ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΥΠΕΙΣΕΡΧΟΝΤΑΙ ΣΤΗ ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΓΝΩΡΙΣΗΣ

Η διαδικασία που περιγράψαμε ανωτέρω είναι εν γένει πολύ ευαίσθητη και εξαρτάται από πολλούς απρόβλεπτους παράγοντες, οι οποίοι μπορούν να αλλοιώσουν το ακουστικό περιεχόμενο ενός σήματος, με αποτέλεσμα να ελαττώσουν την αξιοπιστία ακόμα και του καλύτερου συστήματος. Ένας από τους βασικότερους αυτούς παράγοντες είναι ο θόρυβος. Λέγοντας θόρυβο εννοούμε όλα τα τυχαία δυνατά ακουστικά και ηλεκτρικά σήματα, τα οποία επηρεάζουν την είσοδο του συστήματός μας, όπως τυχαίες ομιλίες στο χώρο, υπέρηχοι και υπόηχοι, οι οποίοι δεν υποπίπτουν στην αντίληψή μας, καταγράφονται όμως από το μικρόφωνο (εξ ου και ο περιορισμός με φίλτρα του σήματος στις ακουστικές συχνότητες), ηλεκτρικός θόρυβος από συσκευές που αλλοιώνει την έξοδο του μικροφώνου, ακόμα και ήχοι στους οποίους δεν δίνουμε προσοχή, όπως αυτός από ένα ραδιόφωνο. Όλα αυτά τα σήματα καταγράφονται και επηρεάζουν άμεσα την αξιοπιστία του συστήματος.

Εκτός από το θόρυβο, στη διαδικασία υπεισέρχονται και παράγοντες λιγότερο προφανείς, όπως η προφορά, το ύφος με το οποίο εκφωνούμε τις διάφορες λέξεις και οι διακυμάνσεις στην ένταση της φωνής μας, οι οποίοι μπορούν να αλλάξουν δραματικά το ακουστικό περιεχόμενο των δειγμάτων. Επιπλέον, κατά την αναγνώριση συνεχούς λόγου υπάρχει το πρόβλημα της εύρεσης του τέλους και της αρχής κάθε λέξης. Τέλος, ας μην ξεχνάμε ότι η ίδια ακολουθία φθόγγων μπορεί να αντιστοιχεί σε λέξεις με τελείως διαφορετική γραφή και νόημα (δείτε ως παράδειγμα την πρόταση "I want to write a letter to Mrs. Wright right now"). Ευτυχώς, όσον αφορά στο τελευταίο παράδειγμα, τα περισσότερα συστήματα αναγνώρισης φωνής υλοποιούν ειδικούς αλγόριθμους οι οποίοι αναλύουν στατιστικά την πιθανότητα εύρεσης μίας λέξης μέσα σε μία συγκεκριμένη πρόταση και παράλληλα μαθαίνουν τις ιδιαιτερότητες κάθε ομιλητή, ελαττώνοντας έτσι σημαντικά την πιθανότητα σφάλματος.

Συμπεραίνουμε δηλαδή, τελικά, ότι η αναγνώριση φωνής αποτελεί μία ιδιαίτερα ευαίσθητη και μη ντετερμινιστική διαδικασία.

5.2 ΟΙ 4 ΑΝΤΑΓΩΝΙΣΤΕΣ ΤΟΥ ΕΞΩΤΕΡΙΚΟΥ

1. Dragon NaturallySpeaking Preferred 4

Η σειρά προϊόντων που προσφέρει η Dragon για αναγνώριση φωνής είναι ευρεία και περιλαμβάνει τις εκδόσεις Standard, Preferred και Professional. Η έκδοση Preferred που δοκιμάσαμε είναι μία πάρα πολύ καλή εφαρμογή, ίσως λίγο πιο "βασική" από ό,τι περιμέναμε. Το manual, πάντως, που συνοδεύει το πακέτο είναι το πιο αναλυτικό από τα υπόλοιπα αυτού του συγκριτικού. Επίσης, στο πακέτο περιλαμβάνεται και ένα headset με μικρόφωνο και speaker.

ΕΓΚΑΤΑΣΤΑΣΗ

Η εγκατάσταση είναι μία απλή διαδικασία, όπως απλή είναι και η διαδικασία ρύθμισης του μικροφώνου. Η βασική εκμάθηση του προγράμματος για την προσαρμογή του στα χαρακτηριστικά της φωνής του χρήστη είναι αρκετά απλοποιημένη με τη βοήθεια wizard. Ακόμα, περιλαμβάνεται ένα εύστοχο και λιτό ενημερωτικό βίντεο, για να καθοδηγηθεί ο χρήστης στον τρόπο λειτουργίας του προγράμματος. Έτσι, μέσα σε δεκαπέντε λεπτά, το NaturallySpeaking είναι έτοιμο για χρήση.

ΥΠΑΓΟΡΕΥΟΝΤΑΣ

Το NaturallySpeaking είναι με διαφορά το πιο εντυπωσιακό από τα προγράμματα που δοκιμάσαμε στον τομέα της αναγνώρισης φωνής. Ακόμα και με την ελάχιστη εκμάθηση που επιτρέπει ο κατασκευαστής, το πρόγραμμα αποδίδει με εξαιρετική ακρίβεια αυτά που του υπαγορεύονται. Η καθυστέρηση του προγράμματος κατά τη συντακτική ανάλυση που κάνει για να "καταλάβει" αυτά που "ακούει", είναι μικρή κατά μέσο όρο. Κάτω από το δείκτη του mouse εμφανίζεται ένα μπαλόνι διαλόγου, που αντανakλά τους συνδυασμούς λέξεων που δοκιμάζει το πρόγραμμα εκείνη τη στιγμή και ενημερώνει το χρήστη για την πρόοδο της διαδικασίας αναγνώρισης. Το πρόγραμμα συνοδεύεται από τον δικό του κειμενογράφο για να καταγράφει τις υπαγορεύσεις μας, αλλά δεν έχει ιδιαίτερη προτίμηση σε αυτόν. Μπορεί να χρησιμοποιηθεί και σε άλλες εφαρμογές, όπως το Microsoft Word 97/2000, το Corel Word Perfect 8 και το Star Office 5.1. Ίσως αυτή είναι και η μοναδική αδυναμία του NaturallySpeaking, το γεγονός δηλαδή ότι δεν έχει εξειδικευμένο σετ εντολών για κάποιον κειμενογράφο, έτσι ώστε να είναι δυνατή και η πιο εξελιγμένη μορφοποίηση του κειμένου, πέρα από την υπαγόρευσή του. Υποστηρίζονται, φυσικά, εντολές, όπως bold ή italics, αλλά τίποτα πιο "εξωτικό".

ΕΝΤΟΛΕΣ & WEB

Όπως και τα υπόλοιπα προγράμματα του συγκριτικού, το NaturallySpeaking έχει τη δυνατότητα δυναμικής εκμάθησης. Δηλαδή, όταν το πρόγραμμα δυσκολεύεται να αναγνωρίσει μία λέξη, μπορούμε να δώσουμε την εντολή "correct that" και να δούμε μία λίστα με τις λέξεις που μοιάζουν φωνητικά με αυτήν που υπαγορεύσαμε ή να συλλαβίσουμε (spell) αυτήν που θέλουμε, αν δεν υπάρχει. Επίσης, υπάρχει εκτεταμένη υποστήριξη για επιλογή κειμένου (text selection) και πλοήγηση στο κείμενο.

Το NaturallySpeaking προσφέρει αρκετά καλή ενσωμάτωση με οποιαδήποτε εφαρμογή των Windows, δίνοντας τη δυνατότητα στο χρήστη να οδηγεί με τη φωνή του τα προγράμματα με ελάχιστο κόπο. Οποιοδήποτε μενού ή πλαίσιο διαλόγου μπορεί να ελεγχθεί με τη φωνή. Είναι δυνατόν ακόμα να εκκινήσουμε εφαρμογές που έχουμε ήδη εγκατεστημένες στον υπολογιστή μας και, φυσικά, να εναλλασσόμαστε μεταξύ των παραθύρων που έχουμε ανοικτά εκείνη τη στιγμή, δίνοντας τις κατάλληλες εντολές. Μπορούμε ακόμα να οδηγήσουμε το δείκτη του ποντικιού, με τη χρήση του ειδικού MouseGrid. Ο χρήστης επιλέγει περιοχές της οθόνης σε πλέγματα, που διαδοχικά μικραίνουν μέχρι να εντοπιστεί ακριβώς η περιοχή που επιθυμεί. Η λειτουργία αυτή δεν είναι και η πλέον εύχρηστη, είναι όμως επαρκής σε περιπτώσεις που θέλουμε να τοποθετήσουμε το mouse κάπου στην οθόνη.

Τέλος, ένα ειδικό module που προσφέρει το πακέτο είναι το NaturalWeb. Όπως το όνομά του προτείνει, με αυτό μπορεί κάποιος να σερφάει στο Internet, μέσω ενός σετ εντολών που προστίθεται στο πρόγραμμα ειδικά για αυτόν το σκοπό. Υπάρχουν εντολές, όπως "go back" ή "stop loading" ή ακόμα και "go to favorite yahoo". Για να οδηγηθούμε σε Web site που δεν υπάρχει στα "Αγαπημένα", υπαγορεύουμε "go to address", στη συνέχεια τη σελίδα που θέλουμε και, τέλος, "go there". Για να ακολουθήσουμε links, απλώς τα υπαγορεύουμε και αυτά επιλέγονται.

ΥΠΕΡ

Εξαιρετική αναγνώριση φωνής
Υποστήριξη Web
Εύκολη εγκατάσταση και ρύθμιση
Καλό manual

ΚΑΤΑ

Λίγες εντολές για μορφοποίηση κειμένου
Μικρή εξειδίκευση σε κειμενογράφο

ΑΠΑΙΤΗΣΕΙΣ

Pentium II 200MHz, 64MB RAM

2. IBM ViaVoice Pro Millenium

Η IBM πρωτοπορεί στον τομέα αναγνώρισης φωνής από παλιά. Ήδη από την εποχή του δικού της λειτουργικού συστήματος, του OS2/Warp, προμήθευε ειδικό module που υπάκουε σε φωνητικές εντολές για εκκίνηση εφαρμογών, μετακίνηση παραθύρων και λοιπές συναφείς λειτουργίες. Το ViaVoice είναι η δική της προσφορά στην αγορά και διατίθεται σε τρεις εκδόσεις: τη Standard, τη Web και την Pro. Η έκδοση Pro, την οποία δοκιμάσαμε, ουσιαστικά περιέχει όλα τα πλεονεκτήματα και τη λειτουργικότητα που παρέχουν οι δύο άλλες εκδόσεις.

ΕΓΚΑΤΑΣΤΑΣΗ & TRAINING

Η εγκατάσταση του ViaVoice, συμπεριλαμβάνοντας και ρύθμιση του headset, είναι μία απλή διαδικασία μέχρι τη στιγμή που γίνεται η βασική εκμάθηση. Το πρόγραμμα σε αυτό το σημείο γίνεται κουραστικό καθώς απαιτεί από το χρήστη να εκφωνεί για αρκετή ώρα, ώστε να προσαρμοστεί στη φωνή του (20 με 30 λεπτά). Επιπλέον, αργεί να προλάβει την εκφώνηση του κειμένου και αρκετά συχνά αρνείται να αναγνωρίσει λέξεις. Στο τέλος της διαδικασίας, ανάλογα με τον

επεξεργαστή φυσικά, απαιτούνται 10 με 15 λεπτά για να ανανεώσει το πρόγραμμα τις εσωτερικές δομές του, λαμβάνοντας υπόψη τα χαρακτηριστικά της φωνής του χρήστη. Ο χρήστης, λοιπόν, καταπονείται αρκετά για να προπονήσει το ViaVoice. Ως αντίβαρο, υπάρχει η χρήσιμη επιλογή να ψάξει το ViaVoice κείμενα που υπάρχουν ήδη στο σκληρό δίσκο, για να εντοπίσει λέξεις που δεν υπάρχουν στο λεξικό του και έτσι να το εμπλουτίσει.

Όσον αφορά στην εκμάθηση των βασικών λειτουργιών του προγράμματος, η IBM συμπεριλαμβάνει και ένα CD με οδηγίες βήμα προς βήμα με τη μορφή βίντεο. Το βίντεο ουσιαστικά δίνει αναλυτικές οδηγίες για τη χρήση του προγράμματος και βοηθάει αρκετά, ειδικά τους αρχάριους.

ΥΠΑΓΟΡΕΥΣΗ & ΕΝΤΟΛΕΣ

Στην ελεύθερη υπαγόρευση το ViaVoice έχει μέτρια απόδοση. Το πρόγραμμα αποδεικνύεται αρκετά ανακριβές στην αρχή, αλλά καλύτερεύει λίγο όταν ο χρήστης κάνει κι άλλα (επίπονα) training sessions. Στον τομέα αναγνώρισης εντολών, είναι πιο ακριβές. Η συλλογή από εντολές είναι το βασικό πλεονέκτημα του πακέτου και είναι αρκετά μεγάλη ώστε να δίνει, τελικά, ένα αρκετά ισχυρό πρόγραμμα. Η IBM προσφέρει μάλιστα και τεχνολογία Natural Speech, που σημαίνει ότι οι περισσότερες εντολές, όπως είναι αυτές για τη μορφοποίηση κειμένου, μπορούν να δοθούν με πολλούς και διαφορετικούς τρόπους. Το trademark του προγράμματος είναι ο Woodrow, μία φιγούρα καρτούν (ανάλογη των Office Assistants στο Office 2000), που εμφανίζεται κάθε τόσο όταν χρειάζεται να επέμβει. Ο Woodrow (ή Woody!) προσωποποιεί κατά βάση την text-to-speech μηχανή που έχει το ViaVoice. Μπορεί, λοιπόν, να μας διαβάσει το κείμενο που μόλις υπαγορεύσαμε ή τα e-mails μας κ.ο.κ.

Το ViaVoice είναι εξοπλισμένο με έναν δικό του κειμενογράφο, το SpeakPad, το οποίο χρησιμοποιείται για την υπαγόρευση. Αν και λίγο περιορισμένο, το SpeakPad αποδεικνύεται ευέλικτο και επαρκές. Το γεγονός αυτό δεν σημαίνει, φυσικά, ότι το ViaVoice δεν συνεργάζεται με άλλους κειμενογράφους. Στην πράξη, μάλιστα, συμβαίνει το αντίθετο, καθώς υποστηρίζονται οι περισσότεροι δημοφιλείς επεξεργαστές κειμένου.

Ακόμα το ViaVoice προσφέρει εντολές για την οδήγηση του ποντικιού. Η λειτουργία ονομάζεται Voice Mouse και είναι αρκετά εύκολη στη χρήση. Επίσης απλό και προσεγμένο είναι το surf στο Internet με εντολές φωνής. Το πρόγραμμα μπορεί να ξεκινήσει τον εξ ορισμού browser του συστήματός μας.

Η πλοήγηση σε σελίδες είναι εύκολη αν αυτές υπάρχουν στα Favorites. Τα κουμπιά του Internet Explorer και του Netscape Navigator μπορούν να οδηγηθούν με εντολές. Τα links σε τυχαία σελίδα ακολουθούνται εύκολα, συμπεριλαμβανομένων και των γραφικών links.

Τέλος, το ViaVoice μπορεί να βοηθήσει και στη δημιουργία e-mail μηνυμάτων. Αν και είναι δύσκολο στην αρχή να αναγνωρίσει τα ονόματα στην ατζέντα μας, η διαδικασία είναι σχετικά απλή. Υποστηρίζονται όλοι οι γνωστοί e-mail clients, όπως το Outlook Express, το Netscape Messenger και το Eudora.

ΥΠΕΡ

Καλή παρουσίαση και ενσωμάτωση
Μεγάλη ποικιλία εντολών
Text-to-Speech Engine
Υποστήριξη Web

ΚΑΤΑ

Μέτρια ποιότητα αναγνώρισης φωνής
Δύσκολη εκμάθηση

ΑΠΑΙΤΗΣΕΙΣ

Pentium II 233MHz, 64MB RAM

3. Lernout & Hauspie Voice Xpress 4 Professional

Η εταιρία Lernout & Hauspie ειδικεύεται εδώ και αρκετά χρόνια σε software που αφορά σε αναγνώριση φωνής. Μάλιστα, πρόσφατα απέκτησε και την αγγλική Dragon Systems, μία επίσης σημαντική εταιρία του ίδιου χώρου. Αυτή η συνένωση εταιριών και η συγκέντρωση πόρων πιθανολογείται στο μέλλον να αποδώσουν πολύ καλά αποτελέσματα.

Η τελευταία προσφορά της εταιρίας είναι η σειρά Voice Xpress, μία σειρά που αποτελείται από τις εκδόσεις Standard, Advanced, Professional και Mobile Professional. Η έκδοση που θέσαμε κάτω από το μικροσκόπιο είναι η πιο "ενισχυμένη" της σειράς, η Professional.

ΕΓΚΑΤΑΣΤΑΣΗ & ΛΕΙΤΟΥΡΓΙΑ

Το πρόγραμμα είναι βασικά σχεδιασμένο για να χρησιμοποιηθεί στο περιβάλλον του Microsoft Office, χωρίς όμως αυτό να γίνεται εις βάρος της υπόλοιπης λειτουργικότητας της εφαρμογής. Με την ίδια ευκολία που μπορούμε να εκτελούμε εργασίες στο Office (π.χ. δημιουργία ενός πίνακα στο Word), μπορούμε να ανοίξουμε άλλες εφαρμογές και να εργαστούμε με αυτές. Μετά την εγκατάσταση και το απαραίτητο reboot, φτάνουμε στη διαδικασία των προσωπικών ρυθμίσεων. Αυτές συμπεριλαμβάνουν τη ρύθμιση του μικροφώνου (μαζί με πακέτο περιέχεται και ένα headset), τη μέτρηση θορύβου του περιβάλλοντος και ένα πρώτο training session. Ο wizard αναλαμβάνει να μας καθοδηγήσει γρήγορα κι εύκολα σε αυτά τα βήματα. Είναι αξιοπρόσεκτο το γεγονός ότι η διαδικασία εγκατάστασης και ρύθμισης είναι πολύ εύκολη και γρήγορη, με αποτέλεσμα το software να είναι έτοιμο για χρήση μέσα σε μικρό χρονικό διάστημα.

Γι' αυτό το πακέτο συστήνεται να γίνουν τουλάχιστον έξι training sessions, αλλά ήδη από το πρώτο εντυπωσιάζουν τα αποτελέσματα. Το Voice Xpress έχει υψηλό ποσοστό σωστής αναγνώρισης λέξεων, κυρίως όταν υπαγορεύονται ολόκληρες προτάσεις κι όχι μεμονωμένες λέξεις. Επίσης, γίνεται το αναμενόμενο scan στα εγκατεστημένα προγράμματα που ήδη υπάρχουν, έτσι ώστε να δημιουργηθούν εντολές για τα ήδη εγκατεστημένα προγράμματα (π.χ. εάν έχουμε εγκατεστημένο το MDK 2, δημιουργείται αυτόματα η εντολή "open mdk2").

ΥΠΑΓΟΡΕΥΣΗ & ΕΝΤΟΛΕΣ

Το πακέτο είναι ειδικά σχεδιασμένο ώστε να ενσωματώνεται με το Microsoft Office 2000 και προσφέρει ταχύτητες υπαγόρευσης στο Word περισσότερες από 100 λέξεις το λεπτό! Ο αριθμός φαίνεται εξωφρενικός στην αρχή, αλλά με τη χρήση είναι εμφανές ότι κάτι τέτοιο είναι όντως εφικτό.

Ένα πολύ μεγάλο πλεονέκτημα του Voice Xpress είναι η "Natural Language Technology". Πρόκειται για μία επέκταση του τρόπου που μπορεί να δώσει κάποιος εντολές στα προγράμματα του Office. Ο χρήστης, καθώς υπαγορεύει κείμενο, δεν χρειάζεται να αλλάξει σε "command mode" για να κάνει bold τις προηγούμενες τέσσερις λέξεις, για παράδειγμα. Απλώς κάνει μία μικρή παύση και υπαγορεύει "bold the previous four words". Ακόμα πιο ενδιαφέρον είναι το γεγονός ότι δεν είναι ανάγκη να θυμάται κανείς ακριβώς την εντολή που θέλει, αλλά μπορεί να την εκφράσει ελεύθερα (εντός ορίων φυσικά) με πολλούς τρόπους. Στο προηγούμενο παράδειγμα θα μπορούσε να πει και "bold backwards four words" ή "select the previous four words. Bold it".

Το πρόγραμμα έχει τη δυνατότητα εκμάθησης συγκεκριμένων όρων που δεν υπάρχουν στο λεξικό του, αλλά και αναπροσαρμογής στη φωνή του χρήστη τη στιγμή που το χρησιμοποιεί. Εάν μία λέξη δεν αναγνωρίζεται καλά, τότε μπορεί να προτείνει λέξεις που μοιάζουν ηχητικά για να επιλεγεί ή να συλλαβιστεί (spell) η σωστή.

Η ενσωμάτωση του Voice Xpress με τις υπόλοιπες εφαρμογές χαρακτηρίζεται ως ικανοποιητική. Ο χρήστης, δίνοντας εντολές, έχει τη δυνατότητα να πλοηγηθεί ανάμεσα στα μενού μιας εφαρμογής ή στα πλαίσια διαλόγου, χωρίς κάτι πολύ εξειδικευμένο. Μάλιστα, συνήθως χρησιμοποιούνται shortcuts του πληκτρολογίου, όπως escape, enter και alt-tab.

Τέλος, στο πακέτο συμπεριλαμβάνεται και η εφαρμογή Mobile Xpress, η οποία επιτρέπει την απομαγνητοφώνηση κειμένων που έχουν υπαγορευτεί σε κάποια συσκευή, όπως το κασετόφωνο ή καλύτερα κάποιο digital voice recorder. Το πρόγραμμα αναλαμβάνει τη μετατροπή του μαγνητοφωνημένου λόγου σε κείμενο για το Word με μία απρόσκοπτη διαδικασία.

ΥΠΕΡ

Σχεδόν άμεση χρήση
Natural Language Technology
Καλή ακρίβεια
Ενσωμάτωση στο Office

ΚΑΤΑ

Τυπική χρήση σε άλλες εφαρμογές
Μικρή υποστήριξη για Web

ΑΠΑΙΤΗΣΕΙΣ

Pentium II 300MHz, 64MB RAM

4. Philips FreeSpeech 2000

Η Philips κάνει και αυτή αισθητή την παρουσία της στο χώρο της αναγνώρισης φωνής με ένα αρκετά υποσχόμενο πακέτο. Το FreeSpeech χαρακτηρίζεται από την εξής καινοτομία: προσφέρει αναγνώριση φωνής και σε άλλες γλώσσες εκτός από την αγγλική. Πιο συγκεκριμένα, μπορεί να χειριστεί δεκατρείς συνολικά γλώσσες / ιδιώματα, συμπεριλαμβάνοντας και τα γερμανικά, γαλλικά, ολλανδικά, ισπανικά, ιταλικά. Φυσικά, προς το παρόν, το πρόγραμμα δεν υποστηρίζει την ελληνική γλώσσα. Το πακέτο συμπληρώνει και ένα φτωχό manual, που απλώς σκιαγραφεί τη βασική λειτουργία του προγράμματος. Διατίθεται σε δύο εκδόσεις, μία με μικρόφωνο headset και μία με το ειδικό πολυ-περιφερειακό Philips SpeechMike.

ΕΙΔΙΚΟ HARDWARE

Το πακέτο που είχαμε για review περιλάμβανε το SpeechMike, μία καινοτομία της Philips σε σχέση με τους ανταγωνιστές της. Πρόκειται για ένα trackball, μικρόφωνο και μεγάφωνο σε μία συσκευή. Η ίδια η Philips το προτείνει ως βασικό εργαλείο για καλύτερη αναγνώριση φωνής. Δυστυχώς, όμως, το SpeechMike είναι κακό και στους τρεις τομείς: Το trackball δεν είναι ο καλύτερος αντικαταστάτης του ποντικιού, ειδικά όταν πρέπει να γίνουν διαδικασίες click & drag. Επιπλέον έχει κακή ανάλυση για την κίνησή του και συνδέεται σε σειριακή υποδοχή 9-pin και όχι PS/2, δείχνοντας έτσι την ηλικία του. Το μεγάφωνο είναι μέτριας ποιότητας, όπως και το μικρόφωνο, καθώς δεν είναι κατασκευασμένο για ακύρωση θορύβου από το περιβάλλον (noise cancellation). Εμείς προτιμήσαμε να χρησιμοποιήσουμε ένα headset, κυρίως για να έχουμε καλύτερη απόδοση από το πρόγραμμα.

ΕΓΚΑΤΑΣΤΑΣΗ

Μετά τη διαδικασία εγκατάστασης, που περιλαμβάνει κατά περίπτωση και driver για το SpeechMike, ένας wizard αναλαμβάνει να μας βοηθήσει στη δημιουργία του προσωπικού μας προφίλ φωνής. Η δοκιμή έγινε μόνο για τα αγγλικά, για λόγους σύγκρισης με τα υπόλοιπα πακέτα αυτού του test. Δυστυχώς και εδώ το FreeSpeech αποτυγχάνει. Το training session κρατάει τουλάχιστον για 15 λεπτά χρόνου εκφώνησης. Αυτό σημαίνει ότι συνολικά για το training χρειάζεται περίπου μισή ώρα με 45 λεπτά μαζί με τις διορθώσεις και τις παύσεις στην ανάγνωση. Επίσης, ο οδηγός δεν διευκολύνει καθόλου την κατάσταση, καταντώντας εκνευριστικός στην αναγνώριση ακόμα και λέξεων που προφέρθηκαν σωστά. Σημειωτέον ότι αυτός είναι ο ελάχιστος χρόνος για training, καθώς ο κατασκευαστής προτείνει περισσότερα sessions για μεγαλύτερη ακρίβεια του προγράμματος. Μετά το τέλος αυτής της διαδικασίας, το πρόγραμμα χρειάζεται περίπου δέκα λεπτά για τη δημιουργία των εσωτερικών δομών που θα χρησιμοποιηθούν για την αναγνώριση της φωνής μας.

ΥΠΑΓΟΡΕΥΣΗ

Περνώντας στην κύρια χρήση του FreeSpeech, δηλαδή την υπαγόρευση, τα πράγματα είναι λίγο θολά. Το πρόβλημα μάλλον έγκειται στη γενικότητα του πυρήνα του προγράμματος, στη δυνατότητα δηλαδή χρήσης του για αναγνώριση πολλών και διαφορετικών γλωσσών. Τα άλλα πακέτα έχουν optimized κώδικα για αναγνώριση δομών της αγγλικής, κάτι που τους δίνει το προβάδισμα.

Κατά την ελεύθερη υπαγόρευση το FreeSpeech δεν είχε ακριβώς ικανοποιητικά αποτελέσματα. Η απόκριση του προγράμματος ήταν ελαφρώς αργή και αρκετά ανακριβής, ώστε το προκύπτον κείμενο να θέλει αρκετή διόρθωση με το χέρι. Επίσης, συμπεριλαμβάνεται και μία περίεργη επιλογή για αποθήκευση του κειμένου μαζί με τον ήχο, δηλαδή τη φωνή μας, κατά την υπαγόρευση. Το FreeSpeech εσωτερικά διατηρεί ολόκληρη την υπαγόρευση που κάνουμε σε WAV αρχείο που συνδέεται με το κείμενο που προκύπτει. Έτσι, μπορούμε να κάνουμε κλικ σε μία λέξη και να ακούσουμε ακριβώς πώς την προφέραμε, κάτι που είναι μάλλον ελάχιστα χρήσιμο. Επίσης, να σημειώσουμε ότι το πακέτο δεν δείχνει κάποια ιδιαίτερη προτίμηση σε κάποιον κειμενογράφο, αλλά συνεργάζεται καλά με οποιονδήποτε θελήσουμε.

Η κατάσταση είναι λίγο καλύτερη στον τομέα αναγνώρισης εντολών. Το FreeSpeech αποδίδει γενικά καλύτερα εδώ και προσφέρει μία αρκετά πλούσια συλλογή από εντολές για εκκίνηση εφαρμογών, εναλλαγή ανάμεσα σε ανοικτά παράθυρα και αλληλεπίδραση με πλαίσια διαλόγου, μενού κ.λπ. Επίσης, υπάρχουν εντολές για surf στο Internet και αρκετές για μορφοποίηση κειμένου (bold, italics, bullets...).

ΥΠΕΡ

Πολλές γλώσσες υπαγόρευσης
Υποσχόμενο engine

ΚΑΤΑ

Κακή αναγνώριση φωνής
Περιληπτικό manual
Μέτριο μικρόφωνο (SpeechMike)

ΑΠΑΙΤΗΣΕΙΣ

Pentium II 233MHz, 64MB RAM

5.3 Η ΕΛΛΑΔΑ ΣΕ ΚΑΛΟ ΔΡΟΜΟ

Η προσπάθειά ξεκίνησε πριν από πέντε μήνες. Όταν είχαν αρχίσει να συγκεντρώνονται τα προγράμματα από τις εταιρίες του εξωτερικού, κανείς δεν πίστευε πως στην Ελλάδα γίνονται οποιεσδήποτε προσπάθειες και μάλιστα σοβαρές. Ωστόσο, ύστερα από έρευνά στον ελληνικό χώρο, βρέθηκε πως οι προσπάθειες αυτές βρίσκονται σε εξέλιξη εδώ και αρκετό καιρό, ενώ σύντομα θα απολαμβάνουμε τις πρώτες εφαρμογές.

ΣΤΗΝ IBM, ΣΤΟ ΧΑΛΑΝΔΡΙ...

Η αρχή στην έρευνά έγινε από την IBM Hellas. Το σκεπτικό ήταν απλό: Αν δεν ξέρει κάτι η IBM, η πρωτοπόρος στις προσπάθειες για αναγνώριση ομιλίας από τον υπολογιστή, τότε ποιος θα ξέρει; Έτσι άρχισαν οι επαφές με την κ. Βαρσάμη, marketing communications specialist της IBM Hellas.

Στα γραφεία της IBM ο κ. Λάζαρος Πολυμενάκος, technical leader του project αναγνώρισης ομιλίας στα ελληνικά, αναφέρθηκε στην εξέλιξη των προσπαθειών της IBM και τις δυσκολίες που αντιμετωπίζουν και αποκάλυψε μερικά από τα μελλοντικά σχέδια της εταιρίας στο συγκεκριμένο τομέα. Ο κ. Πολυμενάκος εργάζεται στο T.J. Watson Research Center (IBM, Νέα Υόρκη) και ανέλαβε την επίβλεψη του project στη χώρα μας. Συνεργάτες του στο project αυτό είναι η κ. Βάλια Δεμέστιχα (έχει αναλάβει την κατανόηση φυσικής γλώσσας και την πρόσβαση σε databases) και ο κ. Γιάννης Βαμβακούλας (έχει αναλάβει τα ακουστικά μοντέλα για αναγνώριση), ενώ σημαντική είναι η συμμετοχή του Εθνικού Μετσόβιου Πολυτεχνείου (έδρα κ. Πρωτονοτάριου). Η όλη προσπάθεια ανήκει σε ένα γενικότερο project που ονομάζεται Catch 2004.

Σε σχέση με το χρονοδιάγραμμα της πιθανής εμφάνισης στην ελληνική αγορά πακέτου αναγνώρισης ομιλίας, σύμφωνα με τον κ. Πολυμενάκο, το project αναγνώρισης ελληνικής ομιλίας βρίσκεται σε ερευνητικό στάδιο (η προσπάθεια ξεκίνησε στην αρχή του 2000), αλλά η ολοκλήρωση του τεχνολογικού μέρους τοποθετείται μέσα στο 2001. Από τη στιγμή που η τεχνολογία θα είναι διαθέσιμη στην IBM "εσωτερικά", η εταιρία θα αποφασίσει για την προώθησή της στην αγορά είτε υπό τη μορφή υπηρεσίας είτε ως τελικό προϊόν-πακέτο στον Έλληνα χρήστη. Το συνολικό project αποτελείται από τρία στάδια: την αναγνώριση ανθρώπινης ομιλίας, την κατανόηση φυσικής γλώσσας και το συνδυασμό της τεχνολογίας με συσκευές (κινητά τηλέφωνα, υπολογιστές).

Η ελληνική είναι γλώσσα κλητή, διακρίνεται από πολυμορφία, χρησιμοποιεί σύνθετες λέξεις και πρόσθετα φωνήματα ενώ χαρακτηρίζεται από έλλειψη αυστηρής σύνταξης. Τα προβλήματα αυτά καθιστούν ανέφικτη την αυτούσια χρήση της τεχνολογίας που ενσωματώνεται στο ξενόγλωσσο πακέτο της εταιρίας, ενώ οδήγησαν την ομάδα της IBM στη λήψη περισσότερων στατιστικών δειγμάτων. Η ελληνική γλώσσα όμως, όσον αφορά στην αναγνώριση ομιλίας, έχει και τα θετικά της. Από τη στιγμή που θα αναπτυχθεί το όλο τεχνολογικό μέρος, η επεξεργασία θα είναι αποτελεσματική καθώς η γλώσσα μας κάνει έντονη χρήση φωνηέντων και μεγάλων λέξεων, χαρακτηριστικά τα οποία διευκολύνουν την αναγνώριση. Έτσι, μπορούμε να πούμε πως το σύστημα, αν και είναι ιδιαίτερα δύσκολο στην ανάπτυξη, σε "ανταμείβει" στην επεξεργασία.

Σε ότι αφορά το αβέβαιο μέλλον του πληκτρολογίου, σύμφωνα με τον κ. Πολυμενάκο το πληκτρολόγιο έχει αρκετά χρόνια ζωής ακόμα. Όπως συνέβη μετά την εμφάνιση του mouse, όπου οι δύο συσκευές εισόδου (πληκτρολόγιο και mouse) χρησιμοποιήθηκαν σε συνδυασμό, έτσι θα συμβεί και με τα συστήματα αναγνώρισης φωνής. Ως πιο αποτελεσματικός θα αποδειχτεί ο τρόπος εισαγωγής δεδομένων, ο οποίος θα συνδυάζει σωστά (στο κατάλληλο ποσοστό χρήσης) το πληκτρολόγιο, το mouse και το σύστημα αναγνώρισης ομιλίας. Τα multimodal αυτά συστήματα θα προτρέπουν στη χρήση του κατάλληλου μέσου ανά πάσα στιγμή, έτσι ώστε να διευκολύνουν τη χρήση οποιασδήποτε υπηρεσίας, χωρίς να προκαλούν ερωτηματικά ως προς τη χρήση των ίδιων.

Όλοι, βέβαια, θα αναρωτιούνται για τις εφαρμογές που θα δούμε σύντομα στη χώρα μας είτε από την ίδια την IBM είτε από τρίτους που θα χρησιμοποιήσουν την τεχνολογία της. Βασική εργασία της ομάδας της IBM είναι η ανάπτυξη ενός συστήματος, το οποίο θα μπορεί να εξυπηρετήσει κάθε λογής συσκευές (ακόμα και χωρίς υπολογιστικές δυνατότητες). Πιο αναλυτικά, το σύστημα αυτό δεν χρειάζεται να γνωρίζει αν ο χρήστης βρίσκεται πίσω από έναν υπολογιστή ή ένα κινητό τηλέφωνο, καθώς και τα δύο αυτά θα αντιμετωπίζονται με τον ίδιο τρόπο.

Το μόνο που διαφοροποιεί τις δύο συσκευές είναι ο τρόπος εμφάνισης της πληροφορίας, γεγονός ελάσσονος σημασίας. Όπως, βέβαια, όλοι καταλαβαίνουμε, ο κύριος στόχος είναι η ανάπτυξη ενός συστήματος που θα μπορεί να συνεργάζεται με τηλέφωνα, καθώς σε αυτά εντοπίζεται η κύρια εφαρμογή, όπως και η συντριπτική πλειονότητα των χρηστών της εν λόγω τεχνολογίας. Στο χώρο των υπολογιστών, η πρώτη εφαρμογή που θα αναπτυχθεί από την ίδια την IBM αφορά στη δημιουργία ενός voice portal. Τα voice portals έχουν κάνει ήδη την εμφάνισή τους στο εξωτερικό, αλλά ακόμα δεν έχουν καταφέρει να εδραιωθούν λόγω της μέτριας απόδοσής τους. Πρόκειται για portal sites όπου ο χρήστης δίνει τις εντολές του προφορικά και το site αναλαμβάνει να τις κατανοήσει και να προβεί στην παρουσίαση των κατάλληλων "απαντήσεων". Ο κ. Πολυμενάκος δεν επεκτάθηκε σε σχέδια της IBM περί κάποιου πακέτου που ίσως κυκλοφορήσει στην ελληνική αγορά, αλλά δεν έκρυψε πως η εταιρία θέλει να είναι πανέτοιμη στην Ολυμπιάδα του 2004 στην Αθήνα, έχοντας ήδη αξιοποιήσει η ίδια ή έχοντας προσφέρει την τεχνολογία της σε τρίτους για την ανάπτυξη πλήθους υπηρεσιών. Άραγε, όταν το 2004 θα χρειαστούμε πληροφορίες για τη διεξαγωγή κάποιου αγωνίσματος, θα μιλάμε μόνο σε υπολογιστές; Δεν νομίζουμε πως κάτι τέτοιο θα ήταν ενοχλητικό από τη στιγμή που η απάντηση του "συνομιλητή" μας θα ήταν άμεση και έγκυρη.

Η κ. Δεμέστιχα έκανε μια επίδειξη του συστήματος κατανόησης φυσικής ελληνικής γλώσσας. Στον τομέα αυτό η IBM έχει αναλάβει την τεχνολογία κατανόησης γλώσσας, ενώ το ΕΜΠ την απαιτούμενη βάση δεδομένων. Στη δοκιμή έγιναν ερωτήσεις στο σύστημα, το οποίο με τη σειρά του τις "κατανοούσε", έψαχνε στη βάση δεδομένων του ΕΜΠ και επέστρεφε την απάντηση σε XML, η οποία στη συνέχεια "μεταφραζόταν" σε φυσική γλώσσα. Όλη η διαδικασία δεν διαρκούσε παρά μόνο ελάχιστα δευτερόλεπτα. Η ομάδα της IBM ενημέρωσε ότι πρώτο τομέα εφαρμογής της τεχνολογίας αποτελούν τα πολιτιστικά γεγονότα, ενώ θα ακολουθήσουν τα αθλητικά, τα οποία αποτελούν και τον κύριο στόχο.

ΣΥΝΕΧΕΙΑ ΜΕ... ΔΙΑΛΟΓΟ

Η εταιρία Διάλογος εκπροσωπεί στην Ελλάδα (και στην Τουρκία) την εταιρία Nuance Communications, η οποία εδρεύει στην Αμερική και ειδικεύεται στην ανάπτυξη software για αναγνώριση φωνής. Πιο συγκεκριμένα, η Nuance δεν αναπτύσσει συστήματα voice recognition για συνεχή λόγο σε PC, αλλά κυρίως συστήματα για παροχή υπηρεσιών πάνω από δίκτυα τηλεπικοινωνιών. Έτσι λοιπόν, οι εφαρμογές του πυρήνα που έχει δημιουργήσει η Nuance επικεντρώνονται σε τεχνολογίες, όπως voice portals, πιστοποίηση αυθεντικότητας μέσω φωνής (voice authentication), ηλεκτρονικό εμπόριο κ.λπ. Το σύστημα βασίζεται σε τεχνολογία η οποία αναπτύχθηκε στο ερευνητικό ινστιτούτο του Stanford από τον καθηγητή Βασίλη Διγαλάκη και τους συνεργάτες του.

Στην ελληνική αγορά, η εταιρία Διάλογος χρησιμοποιεί ήδη με επιτυχία τον πυρήνα της Nuance προσαρμοσμένο στα χαρακτηριστικά της ελληνικής γλώσσας. Η προσαρμογή του συστήματος στα ελληνικά στηρίχτηκε σε δείγματα φωνής πολλών χιλιάδων ομιλητών από ολόκληρη την Ελλάδα. Με βάση αυτό, παρέχεται στους συνδρομητές της Cosmote η δυνατότητα ενημέρωσής τους για το Χρηματιστήριο Αξιών Αθηνών, καλώντας τον αριθμό 1656. Η υπηρεσία δεν χρησιμοποιεί τεχνολογία αναγνώρισης διακριτού λόγου (δηλαδή μεμονωμένες λέξεις), αλλά γίνεται και νοηματική ανάλυση του γλωσσικού περιεχομένου. Με αυτό τον τρόπο ο χρήστης μπορεί να ζητήσει τα δεδομένα χρησιμοποιώντας ελεύθερα διατυπωμένο

ερώτημα (query), χωρίς να πρέπει να προφέρει συγκεκριμένες λέξεις για να πάρει το επιθυμητό αποτέλεσμα.

Το σχετικό software έχει κάποια ιδιαίτερα χαρακτηριστικά που το καθιστούν πιο περίπλοκο από το συνηθισμένο voice recognition πακέτο σε PC. Καταρχήν, το πρόγραμμα πρέπει να προσαρμόζεται δυναμικά στα φωνητικά χαρακτηριστικά του εκάστοτε χρήστη. Ακόμα, η ποιότητα του φωνητικού δείγματος (sample) είναι χαμηλότερη από το συνηθισμένο δείγμα φωνής από ειδικό μικρόφωνο, καθώς το σήμα μεταφέρεται πάνω από γραμμή που περιορίζει το εύρος συχνοτήτων του. Επιπλέον, συνήθως το σήμα εμπεριέχει και αρκετό θόρυβο, γεγονός το οποίο δυσχεραίνει τη διαδικασία. Λαμβάνοντας υπόψη τους προαναφερόμενους παράγοντες, είναι αξιοθαύμαστα τα αποτελέσματα του συστήματος. Η Nuance παρουσίασε πρόσφατα τον Voyager, ένα σύστημα που συνδυάζει το τηλέφωνο με το Internet. Πρόκειται για έναν φωνητικό browser, ο οποίος συνεργάζεται με voice portals και επιτρέπει στο χρήστη να ζητά πληροφορίες καταλόγων από το τηλέφωνό του.

Τέλος, ο πυρήνας της Nuance, σύμφωνα με πληροφορίες, θα χρησιμοποιηθεί επίσης σε ειδικό σύστημα που θα αναπτυχθεί από το Πολυτεχνείο Κρήτης για λογαριασμό της γνωστής εφημερίδας "Ελευθεροτυπία" και έχει ως στόχο τη δημιουργία software speech-to-text. Σε ειδικές αίθουσες της εφημερίδας γίνονται δοκιμές για την αυτόματη απομαγνητοφώνηση, ένα project που ακούγεται ιδιαίτερα ενδιαφέρον.

(<http://www.nuance.com>, www.speech.gr, www.telecom.tuc.gr)

ΣΤΟ ΠΑΙΧΝΙΔΙ ΚΑΙ Η ΠΑΤΡΑ...

Σε sites ελληνικών πανεπιστημίων, συναντάει κανείς τις προσπάθειες του Πανεπιστημίου Πατρών. Ο καθηγητής κ. Νίκος Φακωτάκης, προϊστάμενος της ομάδας της Ομιλίας και Γλωσσικής Τεχνολογίας (SLT), έχει δώσει σημαντικές πληροφορίες:

Μία από τις πιο σημαντικές σύγχρονες εφαρμογές της γλωσσικής τεχνολογίας αφορά στα "Συστήματα Προφορικού Διαλόγου" (Spoken Dialogue Systems), που για να αποδώσουν απαιτούν τη συγκεντρωμένη ισχύ σχεδόν όλων των ερευνητικών τομέων στο χώρο της γλωσσικής τεχνολογίας (αναγνώριση, κατανόηση και σύνθεση ομιλίας, γλωσσολογική, σημασιολογική και πραγματολογική ανάλυση λόγου, μοντελοποίηση διαλόγου κ.λπ.). Τα συστήματα αυτά επικοινωνούν με τους χρήστες προφορικά και τους προσφέρουν τη δυνατότητα να λαμβάνουν πληροφορίες ή να ολοκληρώνουν συναλλαγές (κυρίως μέσω τηλεφώνου) εύκολα και απλά, χωρίς την ανθρώπινη παρέμβαση. Το Πανεπιστήμιο Πατρών (Εργαστήριο Ενσύρματης Τηλεπικοινωνίας <http://slt.wcl.ee.upatras.gr>) έχει σημαντική παρουσία στο χώρο της γλωσσικής τεχνολογίας διεθνώς. Διεξάγει έρευνα για περισσότερο από 25 χρόνια και έχει να παρουσιάσει σημαντικά θεωρητικά και πρακτικά αποτελέσματα στον ευρύ χώρο της επεξεργασίας ομιλίας και φυσικής γλώσσας. Έχει συμμετάσχει σε μεγάλο αριθμό ερευνητικών / αναπτυξιακών προγραμμάτων (εθνικών και ευρωπαϊκών), χάρη στον οποίο έχει δημιουργήσει σημαντική υποδομή, τόσο σε γλωσσικούς πόρους και εργαλεία όσο και σε τελικά συστήματα. Χαρακτηριστικά προγράμματα που μπορούν να αναφερθούν είναι τα:

- Polyglot (ESPRIT-II): Πολυγλωσσικό σύστημα υπαγόρευσης κειμένων.
- ACCeSS (LE-1802): (1) Αυτόματο διαλογικό σύστημα συμπλήρωσης ασφαλιστικών συμβολαίων. (2) Αυτόματο διαλογικό σύστημα για αναφορά αυτοκινητικών ατυχημάτων.
- IDAS (LE-8315): Αυτόματο διαλογικό σύστημα παροχής πληροφοριών τηλεφωνικού καταλόγου ("131").
- SPEECHDAT-II: Συλλογή δεδομένων ομιλίας μέσω τηλεφώνου σε περισσότερες από 10 ευρωπαϊκές γλώσσες και διαλέκτους (5.000 ομιλητές ανά γλώσσα).
- SPEECHDAT-CAR: Συλλογή δεδομένων ομιλίας σε περιβάλλον αυτοκινήτου σε πολλές ευρωπαϊκές γλώσσες και διαλέκτους (600 ομιλητές ανά γλώσσα).
- ΔΙΑΛΟΓΟΣ (ΕΚΒΑΝ-715): Ανάπτυξη διαλογικού συστήματος επικοινωνίας ανθρώπου - μηχανής.

Στα προαναφερόμενα προγράμματα έχει συμμετάσχει η Knowledge A.E. (<http://www.knowledge.gr>) του ομίλου LOGIC-DIS, η οποία θεωρείται μία από τις πρωτοπόρες εταιρίες σε θέματα γλωσσικής τεχνολογίας στην Ευρώπη. Η εταιρία Knowledge κατάφερε να μετατρέψει όλη την ερευνητική προσπάθεια σε αξιόπιστα συστήματα αναγνώρισης / κατανόησης ομιλίας, τα οποία προωθεί υπό μορφή υπηρεσιών στην αγορά. Χαρακτηριστικά συστήματα ανά περιοχή εφαρμογής αποτελούν τα εξής:

Οικονομικές Υπηρεσίες (Financial Services)

- Τηλε-Τραπεζικά συστήματα (Voice Banking)
- Χρηματιστηριακές Συναλλαγές (Stock Quotes)
- Εξυπηρέτηση Πελατών (Customer Care)
- Επιβεβαίωση Ομιλητή (Speaker Verification)

Τηλεπικοινωνιακές Υπηρεσίες

- (Telecom Services)
- Πληροφορίες Τηλεφωνικού Καταλόγου (Directory Assistance)
- Φωνητικές Πύλες (Voice Portals)
- Προσωπικός Βοηθός Κλήσεων (Personal Call Assistant)
- Εξυπηρέτηση Πελατών (Customer Care)

Υπηρεσίες Διαδικτύου (Internet Services)

- Φωνητικός Έλεγχος Μηνυμάτων (Messaging Command & Control)
- Φωνητικός Χειρισμός Διαδικτύου (Voice Browsing)

Υπηρεσίες Ταξιδιών και Μεταφορών (Travel & Transportation Services)

- Δρομολόγια (Timetable information)
- Ενοικίαση Αυτοκινήτων (Rental Car)
- Κρατήσεις (Reservation)

5.4 ΜΕΤΑ ΤΙΣ ΔΟΚΙΜΕΣ...Η ΕΛΛΗΝΙΚΗ ΕΚΔΟΣΗ

ΤΑ ΞΕΝΑ ΠΡΟΓΡΑΜΜΑΤΑ

Κοιτάζοντας συνολικά και τα τέσσερα προγράμματα, είναι σαφές ότι το καλύτερο στην αναγνώριση φωνής (ελεύθερο κείμενο και εντολές) είναι το Dragon NaturallySpeaking Preferred. Κατά σειρά ακολουθούν τα πακέτο της Lernout & Hauspie, της IBM και της Philips. Ένα κοινό συμπέρασμα είναι ότι όλα τα προγράμματα προτιμούν μία "αμερικανίζουσα" προφορά των λέξεων. Από μια άλλη οπτική γωνία, το πρόγραμμα της Dragon είναι κατά κάποιον τρόπο "φτωχό" σε σύγκριση με τα υπόλοιπα. Σε αυτό τον τομέα το Voice Xpress Professional της Lernout & Hauspie, καθώς και το ViaVoice Millennium της IBM φαίνεται να τα πηγαίνουν καλύτερα, με το πρώτο από τα δύο να έχει πολύ καλύτερα αποτελέσματα από το δεύτερο, προσφέροντας ταυτόχρονα εξαιρετική ενσωμάτωση με το Microsoft Office 2000. Το software της IBM, από την άλλη, προσφέρει καλύτερες εντολές για Web surfing και φιλικότερο περιβάλλον. Η Philips αντιπαρέρχεται όλα αυτά με την παροχή αναγνώρισης φωνής και σε άλλες γλώσσες εκτός από την αγγλική και με το φιλικό στο χρήστη περιβάλλον. Όλα τα πακέτα αποδίδουν πολύ καλύτερα όταν βρίσκονται σε Command Mode, δηλαδή όταν δέχονται μόνο εντολές. Κάτι τέτοιο είναι αναμενόμενο άλλωστε, αφού το software έχει μία περιορισμένη λίστα από λέξεις (σε σχέση με την ελεύθερη υπαγόρευση) και απλώς βρίσκει την πιο κοντινή ηχητικά πρόταση. Το πόσο εύρος καλύπτουν οι εντολές κάθε πακέτου παίζει πιο σημαντικό ρόλο εδώ. Το Voice Xpress και το ViaVoice υπερτερούν για το πλήθος των εντολών τους, καθώς υποστηρίζουν και την τεχνολογία Natural Language, που επιτρέπει την εκφώνηση μιας εντολής με πολλούς διαφορετικούς τρόπους, κάτι που ξεκουράζει το χρήστη. Επίσης, το FreeSpeech της Philips αλλά και το ViaVoice έχουν ταυτόχρονα πολύ καλή υποστήριξη για Web surfing, με το δεύτερο να υπερτερεί. Η επιλογή, τελικά, πρέπει να γίνει λαμβάνοντας κανείς υπόψη την ποιότητα αναγνώρισης φωνής, αλλά και τη λειτουργικότητα που απαιτεί για τον εαυτό του. Προς το παρόν, πάντως, όλα τα παραπάνω προγράμματα έχουν περαιτέρω περιθώρια ανάπτυξης.

ΟΙ ΕΛΛΗΝΙΚΕΣ ΠΡΟΣΠΑΘΕΙΕΣ

Δύο είναι οι βασικές έννοιες που φαίνεται να απασχολούν όσους αναπτύσσουν αυτή τη στιγμή συστήματα αναγνώρισης ομιλίας: τα κινητά τηλέφωνα και οι Ολυμπιακοί Αγώνες του 2004. Αυτό είναι απόλυτα φυσιολογικό, καθώς οι δύο αυτές έννοιες κυριαρχούν και θα κυριαρχούν τα επόμενα χρόνια στη χώρα μας. Οι προσπάθειες εταιριών και πανεπιστημίων έχουν αρχίσει εδώ και αρκετά χρόνια. Ωστόσο, πρόσφατα ξεκίνησαν οι ανακοινώσεις εφαρμογών, οι οποίες θα αυξηθούν στα επόμενα τρία χρόνια.

ΕΝ ΚΑΤΑΚΛΕΙΔΙ

Σύμφωνα με μια πρόσφατη έρευνα, παρατηρήθηκε ότι άτομα που χρησιμοποιούν κατά κόρο προγράμματα αναγνώρισης φωνής, φανέρωσαν συμπτώματα κούρασης των φωνητικών χορδών τους. Το πρόβλημα είναι πιο έντονο σε όσους καπνίζουν και οφείλεται στο ότι οι χρήστες πρέπει να διατηρούν τον τόνο της φωνής τους σχετικά σταθερό και μονότονο, καθώς και στο ότι συνήθως πρέπει να σταματούν ανάμεσα στις λέξεις ή να τις τονίζουν με τρόπο λιγότερο φυσικό.

Η απάντηση της βιομηχανίας σε αυτό είναι η τεχνολογία Συνεχούς Λόγου (Continuous Speech), με την οποία εκφωνούνται ολόκληρες προτάσεις και όχι μεμονωμένες λέξεις. Αν και δεν λύνει ολοκληρωτικά τα θέματα, φαίνεται να είναι ένα πρώτο βήμα προς τη λύση.

Πάντως, το μέλλον για την αναγνώριση φωνής φαίνεται να είναι λαμπρό. Ο υπολογιστής που θα δέχεται εντολές με φωνή δεν φαίνεται να είναι ένας ανεπίτευκτος στόχος. Τα πράγματα έχουν ήδη ωριμάσει για την ενσωμάτωση τέτοιων προγραμμάτων μέσα στα λειτουργικά συστήματα. Και τα τέσσερα προγράμματα κάνουν ειλικρινείς προσπάθειες να αποτελέσουν μια κοινή πλατφόρμα για δουλειές που αφορούν στο λειτουργικό (εκκίνηση προγραμμάτων και χειρισμός τους) αλλά και για δουλειές που απαιτούν τη σύνταξη κειμένου (e-mail ή οποιοδήποτε κείμενο). Ίσως αργότερα στο μέλλον να θεωρούμε ως δεδομένο την αλληλεπίδρασή μας διαμέσου φωνής με οποιαδήποτε μηχανή και όχι, όπως τώρα, ως ένα πειραματικό πρόγραμμα.

5.5 ΑΝΑΓΝΩΡΙΣΗ ΦΩΝΗΣ...Η ΟΙΚΟΝΟΜΙΚΟΤΕΡΗ ΛΥΣΗ



Είναι μερικές φορές που η εξέλιξη της τεχνολογίας μάς αφήνει κυριολεκτικά άφωνους. Ειδικά την εποχή αυτή, που έχει επιταχύνει τους ρυθμούς της και στοχεύει να κατακτήσει χώρους που μέχρι πρόσφατα τους είχε αγγίξει μόνο η επιστημονική φαντασία. Το νέο μεγάλο στοίχημα της τεχνολογίας λέγεται «Αναγνώριση Φωνής» και θα είναι η πρώτη φορά που μια τόσο μεγάλη τεχνολογική επανάσταση... δεν θα μας αφήσει άφωνους. Οι πρώτες εφαρμογές της νέας αυτής τεχνολογίας είναι ήδη εδώ και μερικοί τις χρησιμοποιούν καθημερινά, αφού είναι ενσωματωμένες σε πολλά προϊόντα όπως είναι τα κινητά τηλέφωνα, οι υπολογιστές, οι ειδικοί

εγγραφείς φωνής, ακόμη... και σε μερικά νέα αυτοκίνητα. Όπως γνωρίζουν, όμως, πολλοί από την καθημερινή χρήση της «αναγνώρισης φωνής» οι επιδόσεις της μάλλον δεν είναι και τόσο κορυφαίες, αφού αρκετά κινητά τηλέφωνα άλλο όνομα καλούμε και άλλο παίρνουν. Το τοπίο σίγουρα θα αλλάξει και δεν είναι μακριά ο καιρός όπου πληκτρολόγια, κουμπιά, ρυθμιστικά και άλλα χειριστήρια θα αντικατασταθούν από ένα και μόνο μικρόφωνο. Οι φωνητικές εντολές είναι το μέλλον και σύμφωνα με τους κατασκευαστές η τεχνολογία που θα τις εξυπηρετεί θα κοστίζει αρκετά λιγότερο από ένα τηλεχειριστήριο ή ένα καντράν τηλεφώνου.

Έχοντας το πλεονέκτημα ότι δεν απαιτεί τίποτα περισσότερο από μια κάρτα ήχου και ένα μικρόφωνο, η αναγνώριση φωνής είναι η τέλεια λύση για όσους χρήστες θέλουν να προστατεύσουν τον υπολογιστή τους με μια ελάχιστη οικονομική επιβάρυνση και παράλληλα είναι διατεθειμένοι να κάνουν κάποιες παραχωρήσεις σε θέματα ακριβείας.

Παρ' όλο που η αναγνώριση φωνής είναι μια βιομετρική μέθοδος που υστερεί σε αρκετά σημεία σε σύγκριση με τους κοντινότερους "ανταγωνιστές" της, φαίνεται

πως σιγά-σιγά η προσοχή κατασκευαστών και κοινού στρέφεται επάνω της. Αυτό συμβαίνει για δύο κυρίως λόγους: Ο πρώτος είναι ότι σ' έναν κόσμο που τρέχει όλο και με γρηγορότερους ρυθμούς, η ανάγκη επαλήθευσης της ταυτότητας ατόμων μέσω των τηλεφωνικών γραμμών αυξάνεται συνέχεια. Όπως καταλαβαίνετε, η αναγνώριση φωνής είναι η μόνη βιομετρική μέθοδος που θα μπορούσε να εφαρμοστεί σε μια τέτοια κατάσταση. Ο δεύτερος λόγος είναι ότι το απαιτούμενο hardware (κάρτα ήχου και μικρόφωνο) συμπεριλαμβάνεται πια στον βασικό εξοπλισμό κάθε προσωπικού υπολογιστή, γεγονός που κάνει τη λύση της αναγνώρισης φωνής πολύ ελκυστική σε όποιον χρήστη ενδιαφέρεται να αυξήσει την ασφάλεια του υπολογιστικού του συστήματος. Πολλές εταιρείες λοιπόν, βλέποντας την τεράστια αγορά των προσωπικών υπολογιστών να ανοίγεται μπροστά τους στρέφονται στην αναγνώριση φωνής, βελτιώνοντας την υπάρχουσα τεχνολογία και προσπαθώντας να εξαλείψουν τα εγγενή μειονεκτήματα της μεθόδου.

Το βασικότερο πρόβλημα, πηγή ίσως και όλων των υπολοίπων, είναι το γεγονός ότι το σύστημα δεν μπορεί να λειτουργήσει ικανοποιητικά σε περιβάλλοντα με σχετικά μεγάλο υψηλό εξωτερικού θορύβου. Αν και κανείς δεν σκοπεύει να χρησιμοποιήσει αναγνώριση φωνής σε ATM (ο θόρυβος του δρόμου καθιστά απαγορευτικές τέτοιες σκέψεις), κανείς δεν μπορεί να εξασφαλίσει ότι και σε οποιαδήποτε άλλη χρήση του συστήματος ο χρήστης θα βρίσκεται στο κατάλληλο περιβάλλον. Ένα ανοιχτό παράθυρο σε πολυσύχναστο δρόμο, συνάδελφοι ή πελάτες που συζητούν, μηχανές που λειτουργούν, είναι σίγουρο ότι θα δημιουργούσαν πολλά προβλήματα στο ειδικό λογισμικό που θα προσπαθούσε να εξακριβώσει αν όντως ο χρήστης είναι αυτός που ισχυρίζεται.

Ακόμα κι αν ο θόρυβος είναι ανεκτός όμως, δεν πρέπει να ξεχνάμε ότι οι φωνητικές χορδές είναι από τα πιο ευαίσθητα μέρη του ανθρώπινου σώματος. Αν λοιπόν ο χρήστης είναι κρυωμένος (ή απλώς το προηγούμενο βράδυ έσπευσε να υποστηρίξει την αγαπημένη του ομάδα στον υπέρ πάντων αγώνα) ίσως αντιμετωπίσει δυσκολίες να επιβεβαιώσει την ταυτότητά του σε ένα σύστημα αναγνώρισης φωνής. Και όσο για βαριές περιπτώσεις όπως λαρυγγίτιδα, ας μην το συζητάμε. Η απώλεια φωνής σε ένα βιομετρικό σύστημα αναγνώρισης φωνής, ισοδυναμεί με την απώλεια δαχτύλου σε ένα σύστημα δακτυλικών αποτυπωμάτων. Τέλος, κάτι άλλο που αφήνει έντονα σημάδια στην ανθρώπινη φωνή είναι φυσικά το πέρασμα του χρόνου.

Όλα αυτά έχουν σαν αποτέλεσμα να δυσχεραίνεται η λειτουργία του συστήματος, το οποίο αρχίζει να απαιτεί μεγάλη συμμετοχή από το χρήστη, ζητώντας του κουραστικές επαναλήψεις ή βάζοντάς τον να απαγγείλει υπερβολικά μεγάλες φράσεις. Με αυτόν τον τρόπο αυξάνεται ο όγκος των δεδομένων προς σύγκριση, και διευκολύνεται έτσι η σωστότερη απόφαση. Η αντίδραση των κατασκευαστών βιομετρικών συστημάτων αναγνώρισης φωνής ήταν η ανάπτυξη ειδικής τεχνολογίας αφαίρεσης του εξωτερικού θορύβου από το βιομετρικά δείγματα, στην οποία ήδη έχουν γίνει σημαντικά βήματα. Μάλιστα, αν ρίξετε μια ματιά στις σελίδες των εταιρειών αναγνώρισης φωνής στο Internet, θα δείτε ότι οι περισσότερες διαφημίζουν την ακρίβεια των προϊόντων τους ως παρόμοια με αυτήν των δακτυλικών αποτυπωμάτων. Παρ' όλα αυτά, η αλήθεια είναι ότι σε αυτόν τον τομέα η αναγνώριση φωνής είναι ακόμα αρκετά πίσω σε σύγκριση με τα δακτυλικά αποτυπώματα..

Πρώτες προσπάθειες

Τα τελευταία δέκα χρόνια έχουμε γίνει μάρτυρες πολλών φιλόδοξων προσπαθειών που μας έδωσαν γεύσεις μέλλοντος. Μερικές από τις εταιρείες που έχουν αναπτύξει προϊόντα, αλλά και έχουν πραγματοποιήσει βαθιά έρευνα στο θέμα της αναγνώρισης φωνής, είναι οι Lernout & Hauspie, IBM και Philips. Αυτές πωλούν και έχουν στον κατάλογό τους προϊόντα (λογισμικό) αναγνώρισης φωνής ειδικά για χρήση σε επεξεργαστές κειμένου υπολογιστή. Οι πρώτες εκδόσεις αυτών δεν ήταν και τόσο αποτελεσματικές, οι τελευταίες όμως είναι ικανές να «γράφουν» κείμενα με τη χρήση μικροφώνου, χωρίς να δυσανασχετούν το χρήστη. Επιπροσθέτως, οι εφαρμογές των παραπάνω εταιρειών επιτρέπουν στο χρήστη να «γράφει» με τη φωνή του κάποιο επίσημο έγγραφο χρησιμοποιώντας ειδικούς όρους, χωρίς να αλλάξει καθόλου τον καθημερινό τρόπο ομιλίας του. Το σύστημα από μόνο του απλά για κάθε λέξη προτείνει από το λεξικό κάποιες εναλλακτικές για επιλογή... πάντα με τη φωνή και καθισμένοι αναπαυτικά ακόμη και στην πολυθρόνα μας.

Η προφορική γλώσσα αποτελείται από δεκάδες διαφορετικών αλλά και ταυτόσημων συχνοτήτων, που το σύστημα τις μετατρέπει σε ένα είδος σήματος που έχει ως ταυτότητα τη χροιά της φωνής μας. Οι μόνες συνιστώσες που μεταβάλλονται στη φωνή ενός ανθρώπου σε σχέση με κάποιον άλλο, που όμως μιλούν την ίδια γλώσσα, είναι: η ένταση (το πόσο δυνατά δηλαδή), η ταχύτητα (το πόσο γρήγορα μιλάμε), το γλωσσικό ιδίωμα της κάθε περιοχής (την προφορά, δηλαδή) και το ποσοστό ψευδίσματος ή η εσφαλμένη προφορά. Τα προγράμματα αναγνώρισης φωνής των υπολογιστών αναγνωρίζουν τις λέξεις σε αντιπαραβολή με άλλες που έχουν αποθηκευμένες στη μνήμη, αλλά και με τη χρήση ακουστικών μοντέλων που έχουν αναπτυχθεί με τη βοήθεια της στατιστικής πρόβλεψης και των αγαπημένων φράσεων ή συνδυασμών λέξεων του χρήστη. Για παράδειγμα, μπορούμε να μιλάμε με τον δικό μας τρόπο, όπως «Παπαδόπουλε, θέλω το χαρτί...» και η εφαρμογή να γράφει στον επεξεργαστή κειμένου μας «Αξιότιμε κύριε Παπαδόπουλε, παρακαλείσθε όπως προσκομίσετε το έγγραφο...». Οι παραπάνω εργασίες για να εκτελεστούν καταναλώνουν αρκετή ισχύ από τον υπολογιστή και για το λόγο αυτό προτείνονται μόνο για «δυνατούς» υπολογιστές.

Αυτόματη εκφώνηση

Εκτός από τον απλό χρήστη ενός υπολογιστή, τα προγράμματα αναγνώρισης φωνής αλλά και ειδικές συσκευές ίδιας αποστολής χρησιμοποιούνται εδώ και μερικά χρόνια από διάφορους επαγγελματίες και από ανθρώπους με ειδικές ανάγκες, που δεν μπορούσαν να χρησιμοποιήσουν πληκτρολόγιο. Με τον καιρό, όμως, οι τιμές των προϊόντων αυτών μειώθηκαν και παράλληλα αυξήθηκαν οι επιδόσεις τους. Έτσι φθάσαμε στην εποχή που μπορούμε πια να έχουμε υπολογιστές, χωρίς πληκτρολόγια και hands free κινητά τηλέφωνα. Η αναγνώριση φωνής, βέβαια, δεν θα εφαρμοστεί μόνο για τη συγγραφή κειμένων ή για τηλεφωνικές κλήσεις, αλλά θα χρησιμοποιηθεί σε πλήθος συσκευών και προϊόντων από την τηλεόραση έως το φούρνο μικροκυμάτων και από «έξυπνα» παιχνίδια έως το αυριανό στερεοφωνικό μας. Όπως σήμερα λέμε το «γραφικό περιβάλλον» του υπολογιστή μας, ίσως αύριο να λέμε το φωνητικό!

Σύντομα θα μπορούμε να... λέμε περισσότερα στον υπολογιστή μας, όπως: «Αποθήκευση», «Άνοιγμα αρχείου...» ή «Αποστολή e-mail» και αυτός να ακούει και να εκτελεί τις εντολές μας. Φανταστείτε τον αυριανό σας υπολογιστή ως μια

σελίδα A4 με πάχος μερικών εκατοστών. Μια επίπεδη, δηλαδή, συσκευή «οθόνη-υπολογιστής» σαν και το TabletPC, που παρουσίασε ο Bill Gates στην πρόσφατη έκθεση Comdex στο Λας Βέγκας, χωρίς πληκτρολόγιο και με ασύρματη ικανότητα σύνδεσης στο Διαδίκτυο. Σύμφωνα με έρευνες αγοράς, περισσότερα από τρία δισεκατομμύρια e-mail αποστέλλονται καθημερινά. Χρησιμοποιώντας, όμως, συστήματα «αναγνώρισης φωνής» τόσο για τη συγγραφή όσο και για την ανάγνωση αυτών, φανταστείτε πόσο λιγότερος χρόνος θα χρειάζεται για την παραγωγή τους από τους χρήστες.

Πολλές εταιρείες, όπως η www.internetspeech.com, το γνωρίζουν αυτό και έχουν ήδη αρχίσει να κατασκευάζουν σελίδες όπου να πλοηγούνται με φωνητικές εντολές, αλλά και να εκφωνούνται πληροφορίες στους επισκέπτες. Η παραπάνω εταιρεία, μάλιστα, έχει αναπτύξει ένα σύστημα εκφώνησης του περιεχομένου των ιστοσελίδων χρησιμοποιώντας απλώς μια τηλεφωνική συσκευή και τη φωνή μας (φωνητικές εντολές), χωρίς φυσικά την ανάγκη υπολογιστή. Προς το παρόν το σύστημα αυτό διατίθεται μόνο στη Βόρεια Αμερική. Η τεχνολογία που εφαρμόζεται ονομάζεται NetECHO και αρχικά θα επιτρέπει στους χρήστες του Yahoo e-mail να λαμβάνουν φωνητικά το ηλεκτρονικό τους ταχυδρομείο από το τηλέφωνό τους... ακόμη κι αν δεν βρίσκονται κοντά σε υπολογιστή. Αξίζει να σημειωθεί ότι ακόμη και σήμερα δεν είναι λίγες οι φορές που λαμβάνουμε οδηγίες ή εντολές από κάποια «τηλεφωνήτρια» στη συσκευή μας που δεν υφίσταται ως φυσικό πρόσωπο, αφού είναι συσκευή «εκφώνησης». Το μέλλον της αυτόματης εκφώνησης σίγουρα είναι λαμπρό, μια και θα ενταχθούν σε αυτό δυνατότητες άμεσης μετάφρασης σε άλλη (ή άλλες) γλώσσα και δημιουργίας προσωπικού εκφωνητή στον υπολογιστή μας ή στο διαδίκτυο, όπου αυτός θα έχει την ικανότητα να μας διαβάσει ένα γερμανικό κείμενο σε άπταιστη ελληνική.

Στο αυτοκίνητο

Οι φανατικοί των γκάτζετ θα πρέπει να τρίβουν τα χέρια τους, μια και πολλά από τα επόμενα μοντέλα αυτοκινήτων θα περιέχουν συστήματα αναγνώρισης φωνητικών εντολών. Προς το παρόν τα συστήματα αυτά θα βρει κανείς μόνο σε αυτοκίνητα πολυτελείας, όπως στην Τζάγκουρ S-type, που είναι η πρώτη του είδους που λειτουργεί με φωνητικές εντολές, από το κλιματιστικό έως το ηχητικό της σύστημα. Ανάλογο σύστημα αναγνώρισης φωνής υπάρχει και στο κορυφαίο μοντέλο LS430 της Λέξους, αλλά και σε μερικά μοντέλα της Μερσέντες. Το θέμα της χρήσης του ταμπλό του αυτοκινήτου χωρίς την χρήση των χεριών μας (hands free) κατά τη διάρκεια της οδήγησης σε μερικές χώρες είναι νόμος για λόγους ασφαλείας. Αυτή είναι μια περίπτωση όπου η τεχνολογία αναγνώρισης φωνής κρίνεται απαραίτητη, εφόσον αυτή περιορίζει στο ελάχιστο τη χρήση οποιουδήποτε πλήκτρου στο ταμπλό του αυτοκινήτου, αφήνοντας τα χέρια μας ελεύθερα μόνο για το τιμόνι. Τα επόμενα χρόνια, θα δούμε πολλά τέτοια αυτοκίνητα. Δίχως άλλο, η τεχνολογία της αναγνώρισης φωνής είναι η καλύτερη είδηση για την αυτοκινητική βιομηχανία, μια και θα της ανοίξει το δρόμο για μοντέλα νέας εποχής, χωρίς πλήκτρα και ρυθμιστικά στο ταμπλό παρά μόνο με ένα τιμόνι και ένα μικρόφωνο.

Η αναγνώριση φωνής είναι στο δρόμο για την επανάσταση του τρόπου χρήσης μιας συσκευής, αλλά και του τρόπου επικοινωνίας της με το χρήστη της. Θα τοποθετηθούν μικρόφωνα παντού, από τον υπολογιστή μας έως το ταμπλό του αυτοκινήτου. Οι φωνητικές εντολές έρχονται να λύσουν χέρια.



5.6 ΣΥΣΤΗΜΑ ΑΝΑΓΝΩΡΙΣΗΣ ΦΩΝΗΣ

Ένα σύστημα αναγνώρισης φωνής για την ταυτοποίηση ενός επισκέπτη.

Για να αναγνωρίσουμε ένα άτομο από τη φωνή του, χρησιμοποιούμε τα λεγόμενα "φωνητικά αποτυπώματα". Η ανθρώπινη φωνή δεν είναι ικανή να εκφέρει έναν τόνο κάθε φορά. Αντιθέτως παράγει συνεχόμενους βασικούς τόνους που δημιουργούν τη χροιά που ακούμε. Κάποιοι από τους βασικούς τόνους είναι τυχαίοι και κάποιοι είναι πολλαπλάσιοι των βασικών και ονομάζονται αρμονικές. Από όλα τα χαρακτηριστικά της ανθρώπινης φωνής τα σημαντικότερα είναι η συχνότητα και η ένταση. Η συχνότητα είναι η ταχύτητα με την οποία πάλλεται ο αέρας όταν μιλάμε, ενώ η ένταση είναι η δύναμη με την οποία εξέρχεται ο αέρας από το στόμα. Η μοναδικότητα της φωνής κάθε ανθρώπου οφείλεται τόσο στη φυσιολογία του αναπνευστικού συστήματός του, όσο και στο περιβάλλον μέσα στο οποίο έμαθε να μιλά. Ο συνδυασμός όλων των παραπάνω χαρακτηριστικών δημιουργεί την ανθρώπινη φωνή. Κάθε άνθρωπος όταν μιλά, δημιουργεί ένα μοναδικό διάγραμμα φωνής, που μπορεί να παρουσιαστεί σαν μια γραφική παράσταση που παρουσιάζει τη συχνότητα, την ένταση καθώς και τους τόνους που χρησιμοποιούνται για να διαμορφώσουν τη φωνή. Η διαδικασία από εκεί και πέρα που χρησιμοποιείται στηρίζεται στα μαθησιακά μοντέλα. Το σύστημα που χρησιμοποιούμε για να κάνει την αναγνώριση, "εκπαιδεύεται" και "μαθαίνει" συγκεκριμένες λέξεις από συγκεκριμένο άτομο, φτιάχνοντας μια βάση φωνητικών δεδομένων και συγκρίνοντας, όταν χρειαστεί τη φωνή του. Αναλόγως με τον εξοπλισμό που διαθέτουμε, το ποσοστό επιτυχημένης αναγνώρισης μπορεί να είναι αρκετά υψηλό. Όμως υπάρχουν κάποιοι περιορισμοί και κάποιοι κανόνες που πρέπει να ακολουθούνται. Για παράδειγμα, οι λέξεις και οι φράσεις που θα χρησιμοποιηθούν πρέπει να είναι ακριβώς οι ίδιες. Επίσης ο εξοπλισμός και οι συνθήκες ηχογράφησης πρέπει να είναι ίδιες. Άλλοι παράγοντες που μπορούν να αλλοιώσουν τη διαδικασία αναγνώρισης είναι η κακή υγεία του ατόμου και εξωτερικές παρεμβολές.

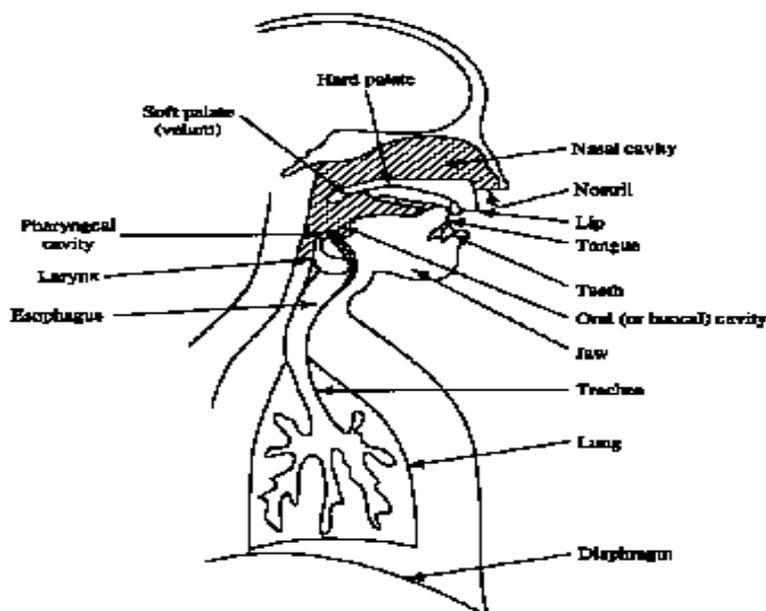
5.6.1 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΝΑΓΝΩΡΙΣΗΣ ΦΩΝΗΣ

Η αναγνώριση φωνής είναι ένα υβριδικό βιομετρικό σύστημα που συνδυάζει φυσικά χαρακτηριστικά με συμπεριφορές, αυξάνοντας με αυτόν τον τρόπο την ποιότητα του βιομετρικού προτύπου. Ξεκινώντας από τα φυσικά χαρακτηριστικά, να πούμε ότι η ανθρώπινη φωνή εξαρτάται από πάρα πολλούς παράγοντες. Το μήκος των φωνητικών χορδών για παράδειγμα, είναι ένας από αυτούς. Το σχήμα του στόματος, των ρινικών κοιλοτήτων, και του λάρυγγα έχει επίσης ιδιαίτερη σημασία. Όλα αυτά αλληλεπιδρούν μεταξύ τους και διαμορφώνουν ένα σύνολο ιδιοτήτων (χροιά, ύψος κ.λπ.) το οποίο χαρακτηρίζει με μοναδικό τρόπο κάθε ανθρώπινη φωνή. Στο σύνολο των φυσικών ιδιοτήτων έρχονται να προστεθούν και μερικές ιδιότητες με βάση συμπεριφορές, όπως ο ρυθμός ομιλίας ή ο τονισμός, οι οποίες διασφαλίζουν ακόμα περισσότερο τη μοναδικότητα του τελικού δείγματος.

5.6.2 Επαλήθευση ομιλητών

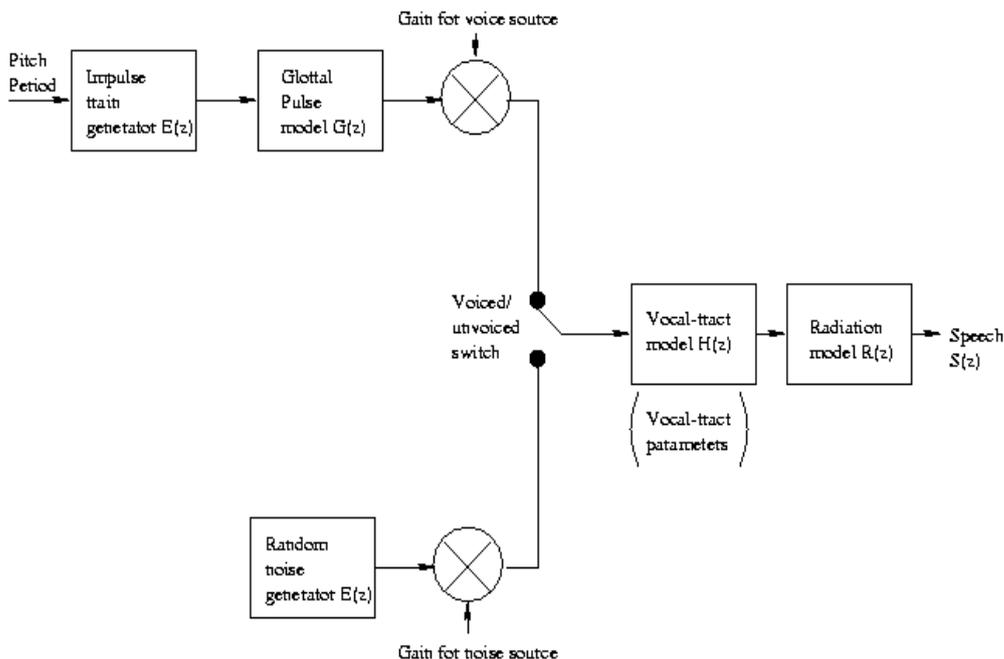
Τα συγκεκριμένα χαρακτηριστικά της ομιλίας του ομιλητή οφείλονται στις διαφορές των φυσιολογικών και συμπεριφορικών πτυχών του συστήματος λεκτικής παραγωγής των ανθρώπων. Η κύρια φυσιολογική πτυχή του ανθρώπινου συστήματος λεκτικής παραγωγής είναι η μορφή φωνητικών κομματιών. Το φωνητικό κομμάτι θεωρείται γενικά ως όργανο λεκτικής παραγωγής επάνω από τις φωνητικές πτυχές, το οποίο αποτελείται από τα εξής: (1) λαρυγγικός φάρυγγας (κάτω από την επιγλωττίδα), (2) προφορικός φάρυγγας (πίσω από τη γλώσσα, μεταξύ της επιγλωττίδας και της μαλακής ύπερων,) (3) στοματική κοιλότητα (μπροστά από τη μαλακή ύπερων και οριακά από τα χείλια, τη γλώσσα και τον ουρανίσκο), (4) ρινικός φάρυγγας (επάνω από τη μαλακή ύπερων, πίσω από τη ρινική κοιλότητα), και (5) ρινική κοιλότητα (επάνω από τον ουρανίσκο και επεκτείνεται από το φάρυγγα στα ρουθούνια). Η σκιασμένη περιοχή στο σχήμα 1 απεικονίζει το φωνητικό κομμάτι.

Σχήμα 1:



Το φωνητικό κομμάτι τροποποιεί το φασματικό περιεχόμενο ενός ακουστικού κύματος καθώς περνά διόμεσων του παράγοντας έτσι την ομιλία. Ως εκ τούτου, είναι κοινό στα συστήματα επαλήθευσης ομιλητών να χρησιμοποιηθούν τα χαρακτηριστικά γνωρίσματα που προέρχονται μόνο από το φωνητικό κομμάτι. Προκειμένου να χαρακτηριστούν τα χαρακτηριστικά γνωρίσματα του φωνητικού κομματιού, ο ανθρώπινος μηχανισμός λεκτικής παραγωγής αντιπροσωπεύεται ως discrete-time σύστημα της μορφής που απεικονίζεται στο σχήμα 2.

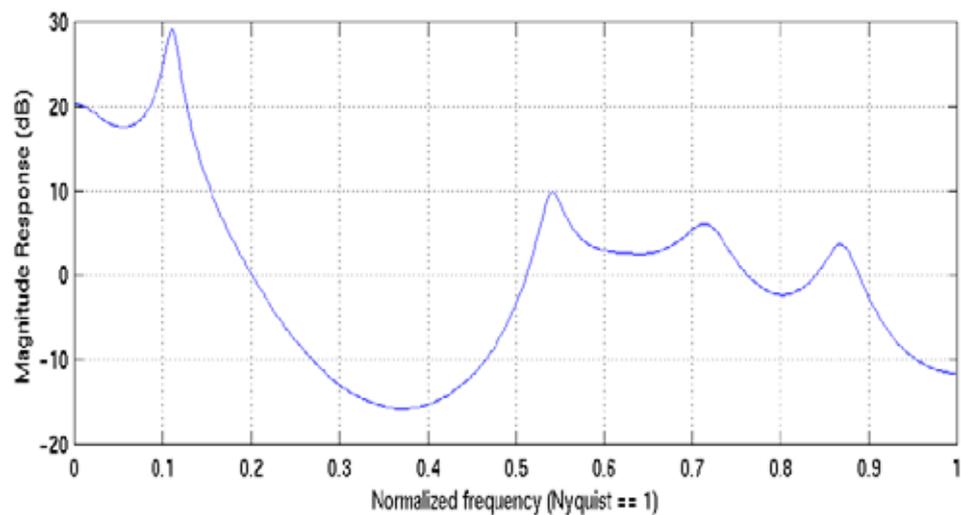
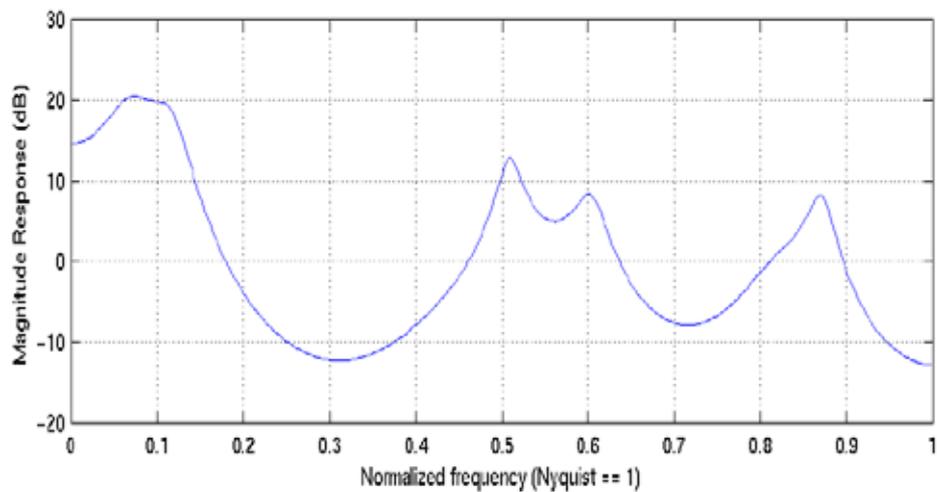
Σχήμα 2:



Το ακουστικό κύμα παράγεται όταν η ροή αέρος από τους πνεύμονες μεταφέρεται από την τραχεία μέσω των φωνητικών πτυχών. Αυτή η πηγή διέγερσης μπορεί να χαρακτηριστεί ως τη φώνηση, το ψιθύρισμα, το προστριβόμενο σύμφωνο, τη συμπίεση, τη δόνηση ή έναν συνδυασμό αυτών. Η διέγερση Phonated εμφανίζεται όταν διαμορφώνεται η ροή αέρος από τις φωνητικές πτυχές. Η ψιθυριστή διέγερση παράγεται από τη ροή αέρος που ορμά κατευθείαν ένα μικρό τριγωνικό άνοιγμα μεταξύ του αρυταινοειδούς χόνδρου στο πίσω τμήμα των σχεδόν κλειστών φωνητικών πτυχών. Η διέγερση Frication παράγεται από τις συστολές στο φωνητικό κομμάτι. Αποτελέσματα διέγερσης συμπίεσης από την απελευθέρωση ενός εντελώς κλειστού και φωνητικού κομματιού. Η διέγερση δόνησης προκαλείται από τον αέρα που ωθείται μέσω μιας περάτωσης εκτός από τις φωνητικές πτυχές, ειδικά στη γλώσσα. Η ομιλία που παράγεται από τη rhotated διέγερση λέγεται εκφρασμένη, όταν παράγεται από τη rhotated διέγερση συν το προστριβόμενο σύμφωνο λέγεται μικτή εκφρασμένη, και όταν παράγεται από άλλους τύπους διεγέρσεων λέγεται άναρθρη. Είναι δυνατό να αντιπροσωπευθεί το φωνητικό κομμάτι σε μια παραμετρική μορφή ως λειτουργία μεταφοράς $H(z)$. Προκειμένου να υπολογιστούν οι παράμετροι του $H(z)$ από το λεκτικό κυματοειδές, είναι απαραίτητο να υποτεθεί κάποια μορφή για το $H(z)$. Ιδανικά, η λειτουργία μεταφοράς πρέπει να περιέχει τους πόλους καθώς επίσης και τα μηδενικά. Επιπλέον, εάν μόνο οι εκφρασμένες περιοχές της ομιλίας χρησιμοποιούνται τότε ένα πρότυπο πόλων για το $H(z)$ είναι ικανοποιητικό. Επιπλέον, η γραμμική ανάλυση πρόβλεψης μπορεί να χρησιμοποιηθεί για να υπολογίσει αποτελεσματικά τις παραμέτρους ενός προτύπου πόλων. Τέλος, μπορεί επίσης να διαπιστωθεί ότι το πρότυπο πόλων είναι το ελάχιστο μέρος της φάσης του αληθινού προτύπου και έχει φάσματα μεγεθών, το οποίο περιέχει τον όγκο των εξαρτώμενων πληροφοριών του ομιλητή.

Η παραπάνω αναφορά υπογραμμίζει επίσης την εξαρτώμενη φύση των προτύπων φωνητικών κομματιών. Δεδομένου ότι το πρότυπο προέρχεται από την παρατηρηθείσα ομιλία, εξαρτάται από την ομιλία. Το σχήμα 3 επεξηγεί τις διαφορές στα πρότυπα για δύο ομιλητές που λένε το ίδιο φωνήεν.

Σχήμα 3:



5.6.3 ΕΠΙΛΟΓΗ ΤΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΓΝΩΡΙΣΜΑΤΩΝ

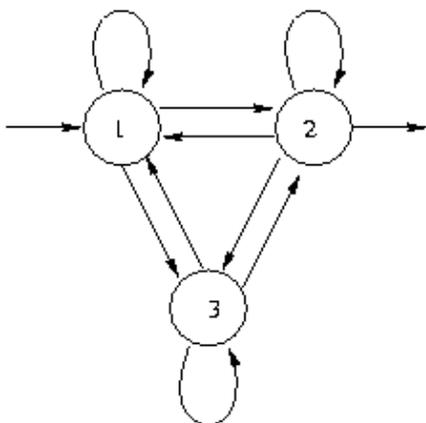
Τα χαρακτηριστικά γνωρίσματα LPC ήταν πολύ δημοφιλή στα συστήματα αναγνώρισης ομιλίας και επαλήθευσης ομιλητών. Εντούτοις, η σύγκριση δύο διανυσμάτων χαρακτηριστικών γνωρισμάτων LPC απαιτεί τη χρήση των υπολογιστικά ακριβών μέτρων ομοιότητας όπως η απόσταση Itakura - Saito και ως εκ τούτου τα χαρακτηριστικά γνωρίσματα LPC είναι ακατάλληλα για τη χρήση σε πραγματικό χρόνο συστήματα. Ο Furui πρότεινε τη χρήση του φάσματος που ορίστηκε ως ο αντίστροφος μετασχηματισμός Φουριέ του λογαρίθμου του φάσματος μεγέθους, στις εφαρμογές αναγνώρισης ομιλίας. Η χρήση του φάσματος επιτρέπει την ομοιότητα μεταξύ δύο φασματικών διανυσμάτων χαρακτηριστικών γνωρισμάτων που υπολογίζονται ως απλή ευκλείδεια απόσταση. Επιπλέον, Ο Atal έχει καταδείξει ότι το φάσμα που προέρχεται από τα χαρακτηριστικά γνωρίσματα LPC οδηγεί στην καλύτερη απόδοση από την όψη FAR και FRR, για ένα σύστημα επαλήθευσης ομιλητών. Συνεπώς, έχουμε αποφασίσει να χρησιμοποιήσουμε το παραγόμενο από το LPC φάσμα για το σύστημα επαλήθευσης των ομιλητών μας.

5.6.4 ΟΜΙΛΗΤΗΣ ΠΟΥ ΔΙΑΜΟΡΦΩΝΕΙ

Χρησιμοποιώντας την φασματική ανάλυση όπως περιγράφεται στο προηγούμενο τμήμα, μια έκφραση μπορεί να αντιπροσωπευθεί ως ακολουθία διανυσμάτων χαρακτηριστικών γνωρισμάτων. Οι εκφράσεις, προφορικές από το ίδιο πρόσωπο αλλά σε διαφορετικούς χρόνους οδηγούν σε παρόμοια ακόμα διαφορετική ακολουθία διανυσμάτων χαρακτηριστικών γνωρισμάτων. Ο σκοπός της διαμόρφωσης φωνής είναι να χτιστεί ένα πρότυπο που συλλαμβάνει αυτές τις παραλλαγές στο αποσπασματικό σύνολο χαρακτηριστικών γνωρισμάτων. Υπάρχουν δύο τύποι προτύπων που έχουν χρησιμοποιηθεί εκτενώς στα συστήματα επαλήθευσης ομιλητών και λεκτικής αναγνώρισης: πιθανολογικά πρότυπα και πρότυπα προτύπων. Το πιθανολογικό πρότυπο μεταχειρίζεται τη διαδικασία λεκτικής παραγωγής ως παραμετρική τυχαία διαδικασία και υποθέτει ότι οι παράμετροι της ελλοχεύουσας πιθανολογικής διαδικασίας μπορούν να υπολογιστούν κατά τρόπο ακριβή, καλά καθορισμένο. Το πρότυπο προτύπων προσπαθεί να διαμορφώσει τη διαδικασία λεκτικής παραγωγής κατά τρόπο μη-παραμετρικό με τη διατήρηση διάφορων ακολουθιών διανυσμάτων, χαρακτηριστικών γνωρισμάτων που προέρχονται από τις πολλαπλάσιες εκφράσεις της ίδιας λέξης από το ίδιο πρόσωπο. Τα μοντέλα προτύπων εξουσίασαν την πρόωρη εργασία στην επαλήθευση ομιλητών και τη λεκτική αναγνώριση επειδή το μοντέλο προτύπων είναι διαισθητικά λογικότερο. Εντούτοις, η πρόσφατη εργασία στα πιθανολογικά πρότυπα έχει καταδείξει ότι αυτά τα πρότυπα είναι πιο εύκαμπτα και ως εκ τούτου επιτρέπουν καλύτερα να διαμορφώσουν τις διαδικασίες λεκτικής παραγωγής. Ένα πολύ δημοφιλές πιθανολογικό πρότυπο για τη διαμόρφωση της διαδικασίας λεκτικής παραγωγής είναι το Hidden Markov Model (HMM). Τα HMMs είναι επεκτάσεις στα συμβατικά Markov πρότυπα, όπου οι παρατηρήσεις είναι μια πιθανολογική λειτουργία του state, δηλ., το πρότυπο είναι μια διπλά ενσωματωμένη πιθανολογική διαδικασία όπου η ελλοχεύουσα πιθανολογική διαδικασία δεν είναι άμεσα αισθητή (είναι κρυμμένη). Το HMM μπορεί μόνο να αντιμετωπισθεί μέσω ενός άλλου συνόλου πιθανολογικών διαδικασιών που παράγουν την ακολουθία παρατηρήσεων. Κατά συνέπεια, το HMM είναι μια πεπερασμένων καταστάσεων μηχανή, όπου μια λειτουργία πυκνότητας πιθανότητας $p(x | s_i)$ συνδέεται με κάθε state s_i . Τα states συνδέονται με ένα δίκτυο μετάβασης, όπου οι πιθανότητες state μετάβασης είναι $a_{ij} = p(s_j |$

s_j). Ένα πλήρως συνδεδεμένο three-state HMM απεικονίζεται στο σχήμα 4.

Σχήμα 4:

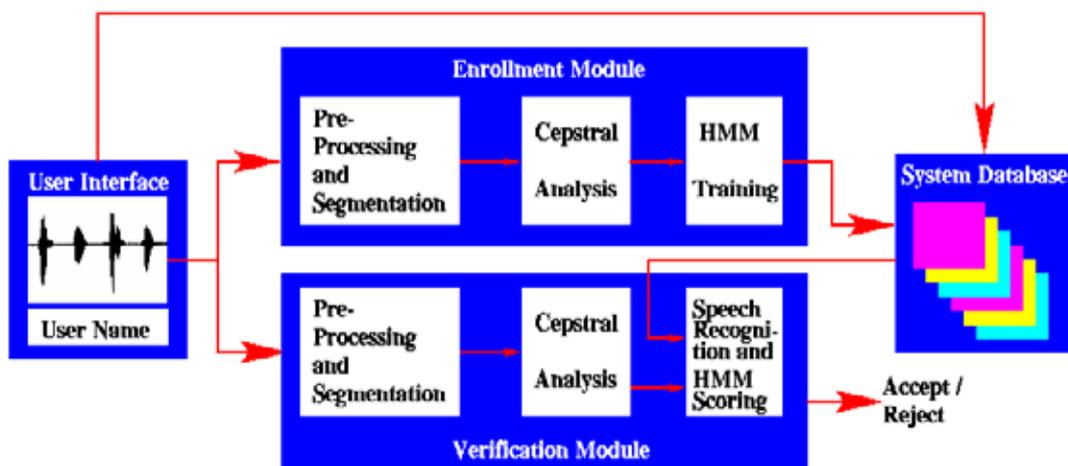


Για τα λεκτικά σήματα, ένας άλλος τύπος του HMM, αποκαλούμενος από τα αριστερά προς τα δεξιά πρότυπα ή πρότυπο Βakis, θεωρείται ότι είναι πιο χρήσιμο. Ένα από τα αριστερά προς τα δεξιά πρότυπα έχει χρονικές αυξήσεις. Οι αυξήσεις state δεικτών που είναι τα states συστημάτων προχωρούν από το αριστερό στο δεξί. Δεδομένου ότι οι ιδιότητες ενός λεκτικού σήματος αλλάζουν κατά τη διάρκεια του χρόνου κατά τρόπο διαδοχικό, αυτό το πρότυπο είναι πολύ καλά ταιριαγμένο για τη διαμόρφωση της διαδικασίας λεκτικής παραγωγής.

5.6.5 ΤΑΙΡΙΑΣΜΑ ΣΧΕΔΙΩΝ

Η διαδικασία ταιριάσματος σχεδίων περιλαμβάνει τη σύγκριση ενός δεδομένου συνόλου διανυσμάτων χαρακτηριστικών γνωρισμάτων εισαγωγής ενάντια στο πρότυπο ομιλητών για την απαιτημένη ταυτότητα και τον υπολογισμό ενός ταιριαστού αποτελέσματος. Για τα Hidden Markov πρότυπα που συζητούνται παραπάνω, το ταιριαστό αποτέλεσμα είναι η πιθανότητα ότι ένα δεδομένο σύνολο διανυσμάτων χαρακτηριστικών γνωρισμάτων παρήχθη από το πρότυπο.

Ένα σύστημα επαλήθευσης ομιλητών:



5.7 ΑΝΑΓΝΩΡΙΣΗ ΦΩΝΗΣ ΣΤΟ INTERNET

Αν θέλετε να διαπιστώσετε την αποτελεσματικότητα της αναγνώρισης φωνής και παράλληλα έχετε μικρόφωνο και σύνδεση στο Internet, υπάρχουν τουλάχιστον δύο τρόποι για να το πετύχετε. Ο πρώτος είναι να κατεβάσετε το πρόγραμμα DemoKey από τις σελίδες των προϊόντων SpeakerKey (η απευθείας διεύθυνση είναι <http://www.speakerkey.com/speakerkey/docs/down.htm>). Το πρόγραμμα αυτό έχει δύο φάσεις. Στην πρώτη, πρέπει να απαγγείλετε δώδεκα ζευγάρια αριθμών που σας προτείνει το πρόγραμμα ώστε να δημιουργήσει ένα φωνητικό προφίλ σας. Στη δεύτερη, τη φάση της αναγνώρισης, το πρόγραμμα προσπαθεί να σας αναγνωρίσει μετά την απαγγελία δύο ζευγαριών αριθμών.

Ο δεύτερος τρόπος είναι να δοκιμάσετε τη διεύθυνση <http://iris1.let.kun.nl/TSpublish/cave>. Στη συγκεκριμένη σελίδα (η οποία αποτελεί στην ουσία ένα on-line demo της μεθόδου) έχουν πρόσβαση μόνο εξουσιοδοτημένοι χρήστες μέσω ενός συστήματος αναγνώρισης φωνής. Αν θέλετε να πειραματιστείτε λοιπόν, δεν έχετε παρά να εγγραφείτε στη λίστα των εξουσιοδοτημένων χρηστών αφήνοντας το φωνητικό σας αποτύπωμα. Την επόμενη φορά που θα επισκεφθείτε την ιστοσελίδα θα πρέπει να απαγγείλετε τη φράση-κλειδί ώστε το σύστημα να σας αναγνωρίσει και να σας επιτρέψει την πρόσβαση.

5.8 ΕΤΑΙΡΕΙΕΣ ΚΑΙ ΠΡΟΪΟΝΤΑ

Χωρίς να φτάνει το πλήθος εταιρειών και προϊόντων των συστημάτων δακτυλικών αποτυπωμάτων, η αναγνώριση φωνής έχει μια αρκετά ευπρεπή εκπροσώπηση στην αγορά. Απ' ότι φαίνεται, οι περισσότερες εταιρείες του χώρου ρίχνουν το βάρος τους στην κατασκευή συστημάτων κατάλληλα για τηλεφωνικά δίκτυα ή για το Internet. Πολλές από αυτές μάλιστα, όπως η ΙΤΤ, εντάσσουν τα προϊόντα τους στα γενικότερα πλαίσια προγραμμάτων υπηρεσιών, τα οποία και χρεώνουν ανάλογα με παραμέτρους όπως η συχνότητα των αναγνωρίσεων σε ορισμένη μονάδα χρόνου, ο αριθμός των σταθμών εργασίας κ.λπ. Έτσι, ο λιγότερο επικερδής τομέας της ασφάλειας των προσωπικών υπολογιστών φαίνεται να μπαίνει σε δεύτερη μοίρα, τουλάχιστον προσωρινά. Παρ' όλα αυτά, και εκεί δε θα μπορούσαν να λείψουν κάποια πολύ αξιόλογα προϊόντα, όπως μπορούμε να δούμε παρακάτω.

• VoicEntry II

Αν έχετε αμφιβολίες σχετικά με το πόσο οικονομικό μπορεί να είναι ένα βιομετρικό σύστημα για τον υπολογιστή σας, το λογισμικό VoicEntry II της T-Netix (<http://www.t-netix.com>) είναι η καλύτερη απόδειξη γι' αυτό. Πρόκειται για ένα ολοκληρωμένο πρόγραμμα προστασίας του συστήματός σας, με λειτουργίες όπως διαχείριση χρηστών, έλεγχο πρόσβασης στα Windows, και κρυπτογράφηση μεμονωμένων αρχείων ή φακέλων. Επιπλέον, στο πρόγραμμα περιέχεται ένας screen-saver ο οποίος απενεργοποιείται μόνο μετά από προφορική εντολή του εξουσιοδοτημένου χρήστη. Το πρόγραμμα δίνει επίσης τη δυνατότητα στο χρήστη να εφαρμόσει βιομετρικό έλεγχο σε οποιοδήποτε άλλο πρόγραμμα προστασίας οθόνης θέλει εκείνος. Η τιμή του πακέτου είναι μόλις 50 δολάρια, δηλαδή γύρω στα 44 €, τη στιγμή που ένα σύστημα δακτυλικών αποτυπωμάτων αντίστοιχων δυνατοτήτων φτάνει τα 132 €.

- **Star Trek: Deep Space Nine Voice Print**

Παρόμοιων δυνατοτήτων και βαθιά επηρεασμένο από την τηλεοπτική σειρά "Start Trek" (όπως άλλωστε μαρτυράει και ο τίτλος του) είναι το πρόγραμμα Star Trek: Deep Space Nine Voice Print της εταιρείας QVoice. Στην τιμή των 80 δολαρίων (73,30 €), το πρόγραμμα είναι λίγο ακριβότερο από το VoiceEntry II, αλλά τουλάχιστον σας αποζημιώνει το γεγονός ότι σας καθοδηγούν οι φωνές των ηρώων της σειράς. Πληροφορίες για το πρόγραμμα μπορείτε να βρείτε στη διεύθυνση (<http://www.cybertown.com/qvoice/startrek.html>).

- **SpeakerKey**

Η ITT Industries (<http://www.ittind.com>) είναι μία από τις πρώτες εταιρείες που ασχολήθηκαν με την αναγνώριση φωνής. Χρησιμοποιώντας την πολύχρονη πείρα της κατασκεύασε τη σειρά προγραμμάτων SpeakerKey, μία από τις πιο ολοκληρωμένες λύσεις για περιπτώσεις όπου η αναγνώριση ταυτότητας μέσω τηλεφωνικού ή άλλου είδους δικτύου είναι απαραίτητη. Το πακέτο περιλαμβάνει τρεις εφαρμογές, κάθε μία από τις οποίες ειδικεύεται και σε έναν τύπο δικτύου: Η εφαρμογή PhoneKey είναι κατάλληλη για περιπτώσεις επιβεβαίωσης ταυτότητας μέσω τηλεφώνου, η εφαρμογή NetKey για τοπικά δίκτυα υπολογιστών, ενώ η εφαρμογή WebKey έχει ως πεδίο δράσης τον Παγκόσμιο Ιστό. Αναλυτικότερες πληροφορίες μπορείτε να πάρετε στη διεύθυνση (<http://www.speakerkey.com>).

ΑΛΛΑ ΠΡΟΪΟΝΤΑ

Επίσης, άξια αναφοράς προϊόντα είναι το VoiceGuardian της Keyware (<http://www.keywareusa.com>), καθώς και τα πακέτα της VeriVoice (<http://www.verivoice.com>), τα οποία μάλιστα καλύπτουν ένα μεγαλύτερο εύρος εφαρμογών, συμπεριλαμβανομένης της υποστήριξης έξυπνων καρτών (smart cards).

MLS ΑΝΑΓΝΩΡΙΣΗ ΦΩΝΗΣ [PRO-083]

Μια πρωτοποριακή και καινοτομική εφαρμογή της MLS που αξιοποιεί τη δύναμη της φωνής σας! Το Πρόγραμμα Φωνητικών Εντολών της MLS δίνει στον υπολογιστή σας τη δυνατότητα να αναγνωρίζει ελληνικά και σε εσάς τη δυνατότητα να χειρίζεστε τις εφαρμογές του MS Office, αλλά και όλες τις εφαρμογές που συνοδεύουν τα Windows, απλά και μόνο με τη φωνή σας. Μεταξύ των εντυπωσιακών δυνατοτήτων τις οποίες σας προσφέρει η πρώτη εφαρμογή Αναγνώρισης Φωνής για τα ελληνικά δεδομένα είναι και οι ακόλουθες: πλοήγηση στο διαδίκτυο, τροποποίηση και διόρθωση κειμένων στο Word, το Σημειωματάριο, το Wordpad και το Outlook Express, επιλογή της αγαπημένης σας μουσικής, επικόλληση κειμένων, δημιουργία φωνητικών πλήκτρων συντόμευσης, χειρισμός της προβολής των παρουσιάσεων του Powerpoint, κ.ά., και όλα αυτά απλά και μόνο ΜΕ ΤΗ ΦΩΝΗ ΣΑΣ.

ΚΕΦΑΛΑΙΟ 6

ΓΕΩΜΕΤΡΙΑ &
ΘΕΡΜΟΓΡΑΦΙΑ
ΠΡΟΣΩΠΟΥ

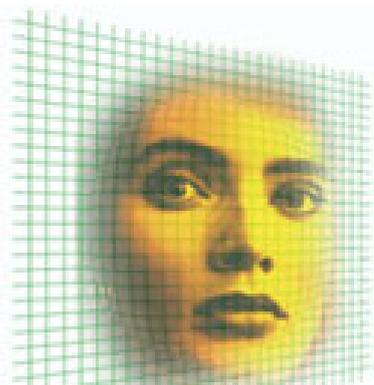
ΓΕΩΜΕΤΡΙΑ ΚΑΙ ΘΕΡΜΟΓΡΑΦΙΑ ΠΡΟΣΩΠΟΥ ΔΥΟ ΠΟΛΛΑ ΥΠΟΣΧΟΜΕΝΕΣ ΝΕΕΣ ΜΕΘΟΔΟΙ

Ανέκαθεν οι άνθρωποι χρησιμοποιούσαν τα χαρακτηριστικά του προσώπου για να θυμούνται και να αναγνωρίζουν ο ένας τον άλλο. Προσπαθώντας να προσομοιώσει τον τρόπο που συμβαίνει αυτό, η μέθοδος της αναγνώρισης προσώπου φιλοδοξεί να αποκτήσει μεγαλύτερη ακρίβεια και ικανότητα προσαρμογής στις αλλαγές.

Η αναγνώριση της ταυτότητας κάποιου ατόμου από την ανάλυση των χαρακτηριστικών του προσώπου του, είναι μια διαδικασία που κάθε άλλο παρά απλή θα μπορούσε να χαρακτηριστεί. Κατ' αρχήν μια κάμερα συλλαμβάνει την εικόνα του προσώπου του χρήστη, και στη συνέχεια το σύστημα προσπαθεί να εντοπίσει διάφορα βασικά σημεία πάνω σ' αυτήν, όπως τις θέσεις των ματιών, του στόματος, της μύτης κ.λπ. Αφού γίνει αυτό, οι αποστάσεις μεταξύ των βασικών σημείων μετριοούνται και τα αποτελέσματα αποθηκεύονται για να αποτελέσουν το βιομετρικό πρότυπο του χρήστη. Πιο εξελιγμένα συστήματα δημιουργούν τρισδιάστατα μοντέλα του προσώπου, προσφέροντας έτσι άλλη μια διάσταση για περισσότερο ακριβείς μετρήσεις.

Παρόμοια τεχνική είναι και η θερμογραφία προσώπου, η οποία χρησιμοποιεί υπέρυθρη κάμερα για να "χαρτογραφήσει" τη ροή του αίματος κάτω από την επιφάνεια του δέρματος. Οι σχηματισμοί θερμότητας των αιμοφόρων αγγείων που βρίσκονται κάτω από το δέρμα του προσώπου, είναι αρκετοί για να επιβεβαιώσουν την ταυτότητα κάποιου, αφού είναι μοναδικοί για κάθε άνθρωπο. Η μέθοδος της θερμογραφίας πλεονεκτεί σε σχέση με αυτήν της γεωμετρίας στο γεγονός ότι μπορεί να λειτουργήσει ικανοποιητικά σε περιβάλλοντα όχι καλά φωτισμένα. Από την άλλη πλευρά, ο εξοπλισμός που απαιτεί είναι πολύ πιο ακριβός.

6.1 ΑΝΑΓΝΩΡΙΣΗ ΠΡΟΣΩΠΟΥ ΜΙΑ ΒΙΟΜΕΤΡΙΚΗ ΤΕΧΝΟΛΟΓΙΑ ΜΕ ΠΟΛΛΑΠΛΕΣ ΕΦΑΡΜΟΓΕΣ



Η τεχνολογία αναγνώρισης προσώπου της εταιρίας Visage όχι μόνο βελτιώνει τις ήδη υπάρχουσες λύσεις εξακρίβωσης ταυτότητας, αλλά και προσφέρει νέες ευκαιρίες για μια ποικιλία νέων εφαρμογών. Το πρόγραμμα χρησιμοποιεί έναν εκλεπτυσμένο αλγόριθμο που βασίζεται στη μέθοδο ανάλυσης PCA (Principle Component Analysis) που έχει αναπτυχθεί στο Media Lab του MIT

Όλη η διαδικασία γίνεται μέσω ενός software που μεταφράζει τα χαρακτηριστικά του προσώπου, όπως αυτά λαμβάνονται από μια εικόνα ή ένα video, σε ένα μοναδικό σετ ψηφιακών δεδομένων, διαμορφώνοντας έτσι αυτό που θα ονομάζαμε ηλεκτρονικό 'αποτύπωμα του προσώπου'. Όπως όλες οι βιοτεχνολογίες, έτσι και αυτή βασίζεται στην ιδιότητα που έχει το ανθρώπινο πρόσωπο να είναι μοναδικό για κάθε άνθρωπο. Το πρόγραμμα χαρτογραφεί την γεωγραφία του ανθρώπινου κρανίου, διαβάζοντας την σχετική θέση και το μέγεθος των διαφόρων χαρακτηριστικών (μέτωπο, μάτια κ.α.) και τις διάφορες γωνίες και καμπυλότητες που αυτό έχει. Το αποτύπωμα που σχηματίζεται χρησιμοποιείται τόσο σε

συστήματα ταυτοποίησης, όσο και σε συστήματα πιστοποίησης, με συγκρίσεις προσώπων που γίνονται σε πραγματικό χρόνο. Κατά την διαδικασία ταυτοποίησης

γίνεται σύγκριση του προσώπου ενός ατόμου με τα πρόσωπα που υπάρχουν σε μια βάση δεδομένων ώστε να καθοριστεί η ταυτότητά του. Η πιστοποίηση χαρακτηρίζεται σαν ένα-προς-ένα ταίριασμα, αφού το πρόσωπο ενός ατόμου συγκρίνεται με ένα μόνο αποθηκευμένο αποτύπωμα με σκοπό να επιβεβαιωθεί η ταυτότητά του.

Η τεχνολογία αναγνώρισης προσώπου της εταιρίας Visage είναι μοναδική λόγω της ικανότητάς της για γρήγορη επεξεργασία και ακριβές αποτέλεσμα σε πραγματικό χρόνο, σε βάσεις δεδομένων που περιέχουν εκατομμύρια πρόσωπα. Το software μπορεί στιγμιαία να υπολογίσει το αποτύπωμα του προσώπου ενός ατόμου, είτε από ζωντανό video είτε από μια ακίνητη ψηφιακή εικόνα και ύστερα να βρει σε λίγα δευτερόλεπτα, μέσα από μια πολύ μεγάλη βάση δεδομένων, αυτά τα πρόσωπα που μοιάζουν ή αυτό που ταιριάζει ακριβώς. Οι εφαρμογές που μπορεί να έχει το πρόγραμμα είναι πάρα πολλές. Η χρήση του σαν σύστημα πιστοποίησης βρίσκει εφαρμογή σε όλα τα σημεία που πρέπει να γίνει έλεγχος πρόσβασης. Ένα τέτοιο σημείο είναι τα μηχανήματα ATM των τραπεζών. Μεγάλη χρησιμότητα μπορεί να έχει επίσης και η χρήση του στο Internet και στο ηλεκτρονικό εμπόριο. Όμως η μεγάλη γκάμα των εφαρμογών του βρίσκεται στα συστήματα ασφαλείας.

Το μεγάλο πλεονέκτημα της τεχνολογίας αναγνώρισης προσώπου δεν είναι τόσο η ένα προς ένα πιστοποίηση της ταυτότητας κάποιου, που θα του δίνει κάποια δυνατότητα πρόσβασης. Αυτό μπορεί να γίνει με πάρα πολλούς και ίσως και πιο εύκολους τρόπους που βασίζονται είτε σε συνήθειες τρόπους (passwords, PINs, κάρτες, κ.α.), είτε σε άλλες βιομετρικές τεχνολογίες.

Η αναγνώριση προσώπου αποτελεί μια βιομετρική τεχνολογία που έχει ένα σημαντικό πλεονέκτημα σε σχέση με τις άλλες. Το σύστημα μπορεί να καταγράψει το αποτύπωμα του προσώπου, με διακριτικό τρόπο, χωρίς το εν λόγω άτομο να το γνωρίζει και χωρίς να έχει την δυνατότητα να το αρνηθεί. Ο συνδυασμός του προγράμματος με ένα δίκτυο από κάμερες και η χρήση μεγάλων βάσεων δεδομένων, μας δίνουν σε όλη την έκταση τις δυνατότητες του συστήματος αυτού. Μπορεί να γίνεται η καταγραφή ενός πλήθους ανθρώπων με συστήματα video και το πρόγραμμα να εντοπίζει σε πραγματικό χρόνο τα προεπιλεγμένα αυτά άτομα (π.χ. ύποπτοι) που υπάρχουν στη βάση δεδομένων Εκεί λοιπόν που το πρόγραμμα αυτό εμφανίζει τις μεγάλες του ικανότητες, είναι στις περιπτώσεις παρακολούθησης, ταυτοποίησης και επιτήρησης ανάμεσα σε μεγάλο αριθμό ατόμων. Αυτό το κάνει πολύτιμο σε συστήματα ασφαλείας μεγάλων χώρων. Έτσι αποτελεί απαραίτητο εργαλείο, στον εντοπισμό υπόπτων ή ανεπιθύμητων προσώπων σε αεροδρόμια, στρατιωτικές βάσεις, κυβερνητικά κτήρια ή άλλους αντίστοιχους χώρους, όπου υπάρχει ανάγκη να γίνεται εντοπισμός υπόπτων, είτε σε μεγάλη απόσταση, είτε ανάμεσα σε μεγάλο πλήθος. Εκτός αυτών, η τεχνολογία αναγνώρισης προσώπου βρίσκει μεγάλη χρήση στην περίπτωση διαχείρισης καταστάσεων που αφορούν την συγκέντρωση μεγάλου αριθμού ατόμων, όπως θερμόαιμοι οπαδοί ομάδων ή διαδηλωτές. Έχει ήδη χρησιμοποιηθεί σε γήπεδα της Αμερικής, αλλά και στη καταπολέμηση του χουλιγκανισμού στα ποδοσφαιρικά γήπεδα της Αγγλίας. Η εταιρία ήδη παρέχει και νέες λύσεις που συνδυάζουν την τεχνολογία αναγνώρισης προσώπου με άλλες βιομετρικές τεχνολογίες (ίριδα, φωνή, κ.α.) αλλά και με ήδη υπάρχοντα συστήματα ταυτοποίησης που βασίζονται σε κάρτες.

Η τεχνολογία αναγνώρισης προσώπου θα μπορούσε να οδηγήσει στο μέλλον σε ένα κόσμο που δεν θα υπάρχει η ανάγκη για χρήση καρτών, κλειδιών, PIN και

υπογραφών, αφού το πρόσωπό μας θα είναι ένα ιδιωτικό, ασφαλές και βολικό password για όλες τις πιθανές χρήσεις.

ΤΑ ΣΥΝ ΚΑΙ ΤΑ ΠΛΗΝ

Το βασικότερο πρόβλημα της αναγνώρισης προσώπου αποτελεί το γεγονός ότι πολλά από τα χαρακτηριστικά στα οποία βασίζεται η αναγνώριση μπορούν να αλλάξουν πολύ εύκολα με την πάροδο του χρόνου. Για παράδειγμα, το μήκος των μαλλιών. Γυαλιά που μπορεί να φοράει ο χρήστης κατά την αναγνώριση, μούσι ή μουστάκι θα δημιουργούσαν το ίδιο πρόβλημα. Κάποια παραπάνω κιλά ή ακόμα και μια μικρή κλίση του κεφαλιού θα μπορούσαν επίσης να μπερδέψουν το σύστημα. Για να αντεπεξέλθουν στις δυσκολίες αυτές, τα περισσότερα συστήματα αναγνώρισης προσώπου χρησιμοποιούν εξελιγμένες μεθόδους τεχνητής νοημοσύνης και αυτό-εκμάθησης. Με τον τρόπο αυτό προσαρμόζονται στις πιθανές αλλαγές, ώστε να μπορούν να συγκρίνουν με ακρίβεια τα νέα δείγματα με το βιομετρικό πρότυπο του χρήστη που είχε δημιουργηθεί κάποια στιγμή στο παρελθόν.

Στα συν της μεθόδου θα πρέπει να καταλογιστεί το υψηλό επίπεδο ακριβείας που επιτυγχάνεται, καθώς επίσης και η σχετικά καλή αποδοχή που έχει από το κοινό (παρόμοια με αυτήν των απλών φωτογραφιών). Τέλος, σημαντικό πλεονέκτημα είναι ότι η μέθοδος δεν κουράζει το χρήστη, ο οποίος το μόνο που έχει να κάνει είναι να σταθεί ακίνητος για μερικά δευτερόλεπτα.

6.2 Ανίχνευση και αναγνώριση προσώπου

Με αφορμή λόγους που όλοι γνωρίζουμε, οι συζητήσεις περί ασφάλειας είναι πλέον στην ημερήσια διάταξη και μάλιστα με νέα ορμή. Φυσικά στις μέρες μας δεν είναι νοητό να θέτονται ζητήματα ασφαλείας και να απουσιάζει από την κουβέντα η σύγχρονη τεχνολογία. Οι εξελίξεις σε αυτό τον τομέα, τρέχουν με ασύλληπτους ρυθμούς, σε σημείο που ακόμη και αυτοί που παρακολουθούν τις εξελίξεις από πιο κοντά, να μένουν μερικές φορές έκπληκτοι. Συστήματα που μέχρι πριν λίγα χρόνια βλέπαμε μόνο σε ταινίες του τύπου 'Επικίνδυνες Αποστολές', σήμερα να είναι διαθέσιμα στην αγορά και μάλιστα είναι ήδη σε ευρεία εφαρμογή.

Μιλάμε για τα σύγχρονα βιομετρικά συστήματα τα οποία εκμεταλλεύονται την μοναδικότητα κάποιων ανθρώπινων χαρακτηριστικών, ακολουθώντας τα χνάρια της χρήσης των γνωστών σε όλους μας δακτυλικών αποτυπωμάτων, αξιοποιώντας ταυτόχρονα στο έπακρο τις δυνατότητες που προσφέρει η ανάπτυξη της ψηφιακής τεχνολογίας και η τελειοποίηση των προγραμμάτων λογισμικού. Ένα από αυτά τα βιομετρικά που βρίσκονται ήδη σε εφαρμογή και αναμένεται να γνωρίσουν άνθηση στο επόμενο διάστημα, είναι αυτά που στηρίζονται στην αναγνώριση του σχήματος του προσώπου. Ο συνδυασμός τους, με τα ήδη εξαπλωμένα δίκτυα παρακολούθησης με κάμερες, μοιάζει να είναι πολλαπλώς αποδοτικός.

Η εταιρία Visionics διαθέτει σε αυτό τον τομέα το FaceIt ένα software με αξιοσημείωτες επιδόσεις. Το πρόγραμμα είναι σε θέση να ανιχνεύσει και να αναγνωρίσει ένα πρόσωπο, γρήγορα και με ακρίβεια. Το λογισμικό αυτό, από τη στιγμή που ένα αντικείμενο που μοιάζει με κεφάλι γίνει ορατό π.χ. από μια κάμερα, χρησιμοποιεί μια ποικιλία από πρότυπους αλγόριθμους για να καθορίσει αν ένα πρόσωπο είναι όντως παρών σε αυτή την θέση. Αυτοί οι αλγόριθμοι είναι σε θέση

να ανιχνεύσουν την ταυτόχρονη παρουσία πολλών προσώπων και να καθορίσουν την ακριβή τους θέση. Όταν ένα πρόσωπο ανιχνευθεί, εξάγεται από το background, και περνά από μια πρώτη διαδικασία που το αποκαθιστά στο μέγεθος, στη φωτεινότητα και στην έκφραση. Το κανονικοποιημένο πρόσωπο, μετασχηματίζεται ακολούθως σε μια εσωτερική αναπαράσταση που ονομάζεται 'αποτύπωμα προσώπου' (faceprint), κάνοντας χρήση συγκεκριμένων μαθηματικών τεχνικών. Αυτός ο ψηφιακός κώδικας περιέχει κρίσιμες πληροφορίες για τα χαρακτηριστικά του προσώπου και χρησιμοποιείται για να καθορίζει την ταυτότητα κάποιου, ταιριάζοντας το ζωντανό αποτύπωμα, με αυτά που είναι αποθηκευμένα στην βάση δεδομένων.

Αυτό που κάνει το πρόγραμμα πολύ ισχυρό, είναι το γεγονός ότι είναι ιδιαίτερα ανθεκτικό σε πιθανές αλλαγές της φωτεινότητας, του τόνου του δέρματος, της ποσότητας των μαλλιών και του χτενίσματος, στην χρήση γυαλιών κ.ά., αφού κυρίως βασίζει την λειτουργικότητά του στο σχήμα και τα αναλλοίωτα χαρακτηριστικά του προσώπου. Επιπλέον, έχει αποδειχθεί ότι το ψηφιακό αποτύπωμα προσώπου περιέχει επαρκείς πληροφορίες για να διακρίνει με ακρίβεια ένα υποκείμενο ανάμεσα σε εκατομμύρια. Η όλη διαδικασία είναι πλήρως αυτοματοποιημένη, συνεχής και γίνεται σε πραγματικό χρόνο. Το FaceIt ανιχνεύει αυτόματα την ανθρώπινη παρουσία, εντοπίζει και αποτυπώνει πρόσωπα, εξάγει από αυτά εικόνες, τις οποίες και συγκρίνει με αυτές τις οποίες έχει αποθηκευμένες σε βάση δεδομένων, από ανθρώπους που έχει 'δεί' και πριν ή από χρήστες που έχουν προεγγραφεί.

Ειδικότερα είναι σε θέση να πραγματοποιήσει τις παρακάτω λειτουργίες:

- **Λειτουργία Ταυτοποίησης**

Για να καθορίσει την ταυτότητα κάποιου, το FaceIt υπολογίζει γρήγορα τον βαθμό αλληλοεπικάλυψης ανάμεσα στο ζωντανό αποτύπωμα προσώπου και αυτών που είναι ήδη καταχωρημένα στη βάση δεδομένων που υποστηρίζει το πρόγραμμα. Μπορεί έτσι να δώσει, είτε μια λίστα πιθανών υποκειμένων (πρόσωπα με κοινά χαρακτηριστικά), είτε ένα μόνο πρόσωπο (μέγιστος βαθμός ταύτισης) μαζί με ένα επίπεδο βεβαιότητας.

- **Λειτουργία Επαλήθευσης**

Σε αυτή την κατάσταση το πρόγραμμα αποθηκεύει ένα συγκεκριμένο αποτύπωμα προσώπου, στην μνήμη ενός computer ή ακόμη και σε μια smart card. Κάθε φορά που το πρόσωπο αυτό εμφανίζεται ζωντανά, γίνεται η σύγκριση για να εξακριβωθεί αν πρόκειται για το ίδιο άτομο.

- **Λειτουργία Καταγραφής**

Κάνοντας χρήση των ικανοτήτων ανίχνευσης και αναγνώρισης, το FaceIt μπορεί να καταγράψει την παρουσία και την θέση ενός ατόμου σε ένα χώρο.

- **Λειτουργία Παρακολούθησης**

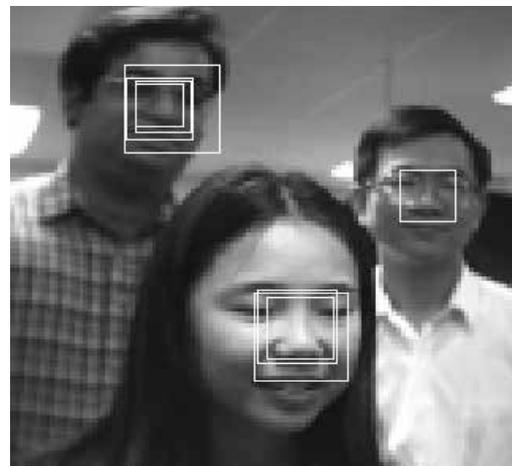
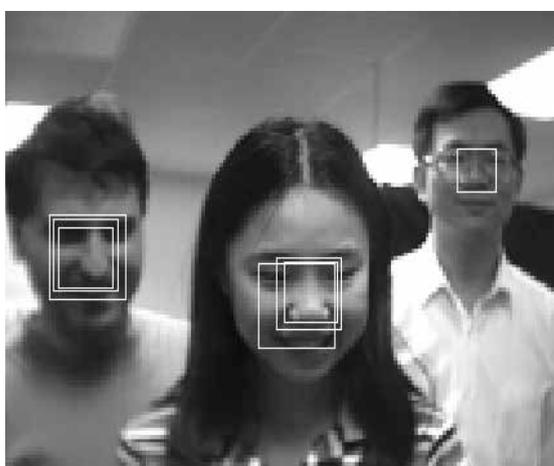
Έχει την ικανότητα να βρίσκει ανθρώπινα πρόσωπα, οπουδήποτε μέσα σε ένα πεδίο και σε οποιαδήποτε απόσταση. Μπορεί στη συνέχεια να μην τα χάνει από τα μάτια του. Η διαδικασία αυτή γίνεται συνεχώς, αυτοματοποιημένα και σε πραγματικό χρόνο.

- **Λειτουργία Αποθήκευσης**

Μπορεί να συμπιέσει τα δεδομένα ενός αποτυπώματος προσώπου στα 84 bytes, επιτρέποντας με αυτό τον τρόπο την αποθήκευση σε smart cards ή σε άλλες περιορισμένων αποθηκευτικών δυνατοτήτων συσκευές.

6.3 ΘΕΣΗ ΠΡΟΣΩΠΟΥ ΑΝΑΚΤΗΣΗ ΠΡΟΣΩΠΟΥ

Το πρόβλημα ανάκτησης προσώπου, γνωστό ως ανίχνευση προσώπου, μπορεί να καθοριστεί ως εξής: λαμβάνοντας υπόψη ένα αυθαίρετο μαύρο και άσπρο, ακόμα η εικόνα, βρίσκει τη θέση και το μέγεθος κάθε ανθρώπινου προσώπου που περιέχει. Υπάρχουν πολλές εφαρμογές στις οποίες η ανθρώπινη ανίχνευση προσώπου διαδραματίζει έναν πολύ σημαντικό ρόλο: αντιπροσωπεύει το πρώτο βήμα σε ένα πλήρως αυτόματο σύστημα αναγνώρισης προσώπου, μπορεί να χρησιμοποιηθεί στη βάση δεδομένων εικόνας, στα συστήματα επιτήρησης και στις ανθρώπου-υπολογιστή διεπαφές. Παρέχει επίσης τη διορατικότητα στο πώς να προσεγγίσει άλλα προβλήματα αναγνώρισης σχεδίων που περιλαμβάνουν τα deformable κατασκευασμένα αντικείμενα. Συγχρόνως, είναι ένα από τα σκληρότερα προβλήματα στην αναγνώριση σχεδίων. Έχουμε σχεδιάσει μια επαγωγική μέθοδο ανίχνευσης εκμάθησης που παράγει μια ανώτατα συγκεκριμένη υπόθεση σύμφωνη με τα στοιχεία κατάρτισης. Τρία διαφορετικά σύνολα χαρακτηριστικών γνωρισμάτων εξετάστηκαν για τον καθορισμό της έννοιας ενός ανθρώπινου προσώπου. Η απόδοση πραγματοποιημένη είναι η ακόλουθη: 85% ποσοστό ανίχνευσης, ένα ποσοστό ψεύτικων συναγερμών 0,04% του αριθμού παραθύρων που αναλύονται και 1 λεπτού ανίχνευσης εικόνας 320 X 240 σε ένα Sun Ultrasparc.



6.4 ΠΡΟΪΟΝΤΑ ΓΙΑ ΤΟ PC ΣΑΣ

· TRUEFACE PC

Η μοναδική απαίτηση που θέτει η αναγνώριση προσώπου από άποψη εξοπλισμού, είναι μια κάμερα. Αν και δεν είναι το πιο φτηνό εξάρτημα για τον υπολογιστή σας, η τιμή της δεν είναι απαγορευτική για κάποιον που θέλει να προστατεύσει το σύστημά του χρησιμοποιώντας αυτή τη νέα μέθοδο. Από τα καλύτερα προϊόντα που θα μπορούσατε να βρείτε γι' αυτόν το σκοπό είναι σίγουρα το TrueFace PC της εταιρείας Miro's (<http://www.miros.com>). Το πρόγραμμα προσφέρει μερικές πολύ καλές δυνατότητες όπως:

- Καταχώρηση μέχρι 5 εξουσιοδοτημένων χρηστών
- Ικανότητα να αντιλαμβάνεται προσπάθειες απάτης, όπως τοποθέτηση φωτογραφιών εξουσιοδοτημένων χρηστών μπροστά στην κάμερα
- Καταγραφή σε βίντεο όσων προσπάθησαν ανεπιτυχώς να αποκτήσουν πρόσβαση στο σύστημα
- Screen-saver που απενεργοποιείται μετά από αναγνώριση προσώπου
- Συνεργασία με οποιαδήποτε κάμερα του εμπορίου

Το πρόγραμμα κοστίζει μόνο 60 δολάρια, δηλαδή γύρω στα 55,70 €. Η σειρά TrueFace περιέχει και άλλα προϊόντα, όλα σχετικά με την αναγνώριση προσώπου: Το TrueFace ID μπορεί να αναγνωρίσει κάποιο άτομο μέσα από μια βάση δεδομένων, το TrueFace Network αυξάνει την ασφάλεια δικτύων προσθέτοντας στους χρήστες πρόσβαση με αναγνώριση προσώπου, ενώ το TrueFace Web έχει κατασκευαστεί για χρήση στο Internet.

Άλλη σημαντική εταιρεία του χώρου είναι η Visionics, δημιουργός της σειράς προϊόντων FaceIt που θυμίζει σε αρκετά σημεία τη σειρά TrueFace. Πληροφορίες για τα προϊόντα FaceIt μπορείτε να πάρετε στη διεύθυνση <http://www.faceit.com>.

Επίσης, η εταιρεία Viisage (<http://www.viisage.com>) διαθέτει μια μεγάλη γκάμα προϊόντων που επιτρέπουν στο χρήστη να δημιουργήσει ένα σύστημα ελέγχου προσαρμοσμένο πραγματικά στις ανάγκες του. Τέλος, η εταιρεία Mr. Payroll (<http://www.mrpayroll.com>) είναι από τις πρώτες που εφάρμοσε τεχνολογία αναγνώρισης προσώπου σε ATM, με πολύ ικανοποιητικά αποτελέσματα

· STAR FACE-007

Κύριες λειτουργίες



- Βιομετρικό σύστημα ελέγχου πρόσβασης
- Συνδυάζει αναγνώριση προσώπου και αναγνώστη proximity
- Συνδυάζει έλεγχο πρόσβασης και ωρομέτρηση προσωπικού
- Μνήμη 3.900 προσώπων (προαιρετικά έως 7.800 πρόσωπα)
- Ενσωματωμένος αναγνώστης RF
- Αυτόνομη λειτουργία ή σύνδεση σε δίκτυο μέσω RS232/RS422 (έως 256 κανάλια)

- Συνδυασμός proximity, αναγνώρισης προσώπου και κωδικού PIN
- 4 ανεξάρτητες εισοδοί, 4 έξοδοι και 2 ρελέ FORM-C
- Αυτόματη διάγνωση
- Ξεχωριστός αναγνώστης εξόδου
- 10 προγράμματα ώρας και 10 προγράμματα αργιών
- Φωτιζόμενο πληκτρολόγιο

Εφαρμογές

- Σύστημα ελέγχου πρόσβασης υψηλής ασφάλειας
- Αυτοματισμοί κτιρίων
- Αυτοματισμοί εργοστασίων - βιομηχανίας
- Ωρομέτρηση προσωπικού

6.5 ΝΕΑ ΜΕΘΟΔΟΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΩΝ ΑΠΟ ΤΗ SIEMENS ΤΑΧΥΤΗΤΑ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑ ΣΕ ΤΡΙΣΔΙΑΣΤΑΤΑ ΜΟΝΤΕΛΑ



Η μέθοδος της Siemens για την αναγνώριση προσώπου.

Η Siemens ανέπτυξε μια νέα μέθοδο αναγνώρισης προσώπων που όπως ισχυρίζεται είναι πολύ ασφαλής, ενώ και ο χρόνος αναγνώρισης ανέρχεται μόλις σε λίγα κλάσματα του δευτερολέπτου. Η μέθοδος αυτή βασίζεται στη λήψη εικόνων video ενός προσώπου και στη σύγκρισή του με τα πρότυπα που υπάρχουν στη βάση δεδομένων του συστήματος. Οι μέθοδοι που χρησιμοποιούν video είναι αρκετά διαδεδομένες, αφού επιτρέπουν γρήγορη δημιουργία του τρισδιάστατου μοντέλου που θα χρησιμοποιηθεί για την επεξεργασία. Αν και θεωρείται αρκετά αξιόπιστη μέθοδος, υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν το αποτέλεσμα της λήψης, όπως είναι ο κακός φωτισμός, ή

η λάθος τοποθέτηση του προσώπου.

Όπως είναι φυσικό, η κακή λήψη ίσως οδηγήσει και σε λανθασμένη αναγνώριση. Κατά τη διάρκεια της διαδικασίας αναγνώρισης, ένα πρότυπο σχήμα αποτελούμενο από παράλληλες χρωματιστές γραμμές, προβάλλεται πάνω στο πρόσωπο, την ώρα που η κάμερα παίρνει μια εικόνα. Ανάλογα με τα ιδιαίτερα χαρακτηριστικά του προσώπου, τη γωνία που έχει η κάμερα και τη θέση του προσώπου, έχουμε και την αντιπαράθεση σε σχέση με τις γραμμές. Με τη βοήθεια όμως των διαφορετικών χρωματιστών γραμμών, μπορεί να υπολογιστεί η απόκλιση και να γίνει ανάλογος υπολογισμός του μοντέλου σύμφωνα με τις τρέχουσες συνθήκες. Χρησιμοποιώντας αυτή τη μέθοδο, οι ερευνητές της Siemens πετυχαίνουν στον υπολογισμό της πλήρους τρισδιάστατης εικόνας του προσώπου σε μια ακρίβεια 0,2 x 0,2 x 0,2mm μέσα σε 40 χιλιοστά του δευτερολέπτου. Αυτή η εικόνα υπολογιστών αναλύεται έπειτα χρησιμοποιώντας τις κλασικές μεθόδους αναγνώρισης προτύπων. Οι δοκιμές που έχουν πραγματοποιηθεί σε πραγματικές συνθήκες έχουν δείξει ότι η νέα μέθοδος μειώνει τα ποσοστά σφάλματος σημαντικά και είναι συγκρίσιμη με τα δισδιάστατα μοντέλα. Επιπλέον, οι μέθοδοι αναγνώρισης που αναλύουν τα τρισδιάστατα πρότυπα είναι δυσκολότερο να εξαπατηθούν. Παραδείγματος χάρη, θα ήταν απολύτως αδύνατο να εξαπατηθεί το σύστημα με την τοποθέτηση μιας φωτογραφίας μπροστά από τη φωτογραφική μηχανή αντί ενός πραγματικού προσώπου.

ΚΕΦΑΛΑΙΟ 7

ΆΛΛΕΣ ΒΙΟΜΕΤΡΙΚΟΙ
ΜΕΘΟΔΟΙ

Η ΒΙΟΜΕΤΡΙΚΗ ΤΟΥ ΜΕΛΛΟΝΤΟΣ

Σε μια τόσο νέα τεχνολογία, όπως αυτή που βασίζονται οι περισσότερες βιομετρικές μέθοδοι, είναι δύσκολο να ξεχωρίσεις το παρόν από το μέλλον. Θα αναφερθούμε συνοπτικά στις πιο αξιολογικές μεθόδους που αναπτύσσονται αυτή τη στιγμή στα διάφορα εργαστήρια, και που αυτή τη στιγμή δεν έχουν ακόμη αξιολογηθεί παρουσία στην αγορά.

Και τώρα τι γίνεται άραγε; Υπάρχουν άλλα μέρη του σώματος που θα μπορούσαν να χρησιμοποιηθούν ως βάση για νέες βιομετρικές μεθόδους; Πάνω απ' όλα, υπάρχει πραγματικά ανάγκη για κάτι τέτοιο; Ειδικά για το δεύτερο ερώτημα, δηλαδή πόσο μας χρειάζονται κάποιες νέες βιομετρικές μέθοδοι που αναπτύσσονται σήμερα, αρκεί να ρίξει κανείς μια ματιά στη συνέχεια του άρθρου (αναγνώριση σωματικής οσμής) για να καταλάβει ότι η απάντηση είναι ένα μεγάλο όχι. Παρόλα αυτά, ας μην είμαστε απόλυτοι. Καθώς όλες οι μέθοδοι βρίσκονται ακόμα στο στάδιο της ανάπτυξης, κανείς δεν μπορεί να πει με σιγουριά αν κάποια από αυτές είναι "σημερινή" ή "μελλοντική", ή ποια είναι αποτελεσματικότερη από την άλλη. Το μόνο κριτήριο για κάτι τέτοιο είναι η παρουσία ανάλογων προϊόντων στην αγορά, κάτι που κρίνει το ενδιαφέρον του κοινού και κατ' επέκταση των εταιρειών για τη συγκεκριμένη μέθοδο. Στη συνέχεια θα δούμε κάποιες μεθόδους που δεν αναφέρθηκαν ακόμα, οι οποίες έχουν αυτό το στοιχείο κοινό: η εκπροσώπησή τους στην αγορά είναι μικρή έως ανύπαρκτη. Η συνεχής ανάπτυξη της τεχνολογίας όμως, σχεδόν μας εγγυάται ότι τουλάχιστον κάποιες από αυτές, θα φτάσουν μια μέρα (αν δεν έχουν φτάσει ήδη) ως τους υπολογιστές μας.

7.1 ΔΙΑΚΡΙΒΩΣΗ ΥΠΟΓΡΑΦΗΣ

Καθώς ο κόσμος είναι συνηθισμένος να χρησιμοποιεί την υπογραφή του ως μέσο εξακρίβωσης της ταυτότητας, η αντίστοιχη βιομετρική μέθοδος αφήνει τις υπόλοιπες χιλιόμετρα πίσω στο θέμα της αποδοχής από το κοινό. Δυστυχώς όμως, καταποντίζεται και η ίδια σε άλλη κατηγορία: την ακρίβεια.

Πολλοί πιστεύουν ότι η βασική λειτουργία ενός συστήματος διακρίβωσης υπογραφής είναι η σύγκριση της "εικόνας" της υπογραφής του χρήστη με κάποιο αποθηκευμένο δείγμα. Τέτοια συστήματα ασφαλώς υπάρχουν, αλλά δεν έχουν καμία απολύτως σχέση με τη Βιομετρική. Το προφανές μειονέκτημα μιας τέτοιας "γραφολογικής" μεθόδου, είναι ότι κάποιος με αρκετό ταλέντο (και υπομονή, ίσως) θα μπορούσε να αναπαράγει την υπογραφή αρκετά πιστά, ώστε να ξεγελάσει τελικά το σύστημα. Αντίθετα, η βιομετρική μέθοδος βασίζεται όχι τόσο στο αποτέλεσμα, αλλά στο πώς αυτό επετεύχθη. Στηριζόμενη κυρίως στη συμπεριφορά του χρήστη κατά τη διαδικασία της υπογραφής, η βιομετρική μέθοδος λαμβάνει υπόψη της παραμέτρους όπως:

- Πόση ώρα χρειάζεται ο χρήστης για να ολοκληρώσει την υπογραφή
- Με ποια γωνία σε σχέση με το χαρτί κρατάει το στυλό
- Ποια είναι η ταχύτητα γραφής και πώς αλλάζει η επιτάχυνση κατά την υπογραφή
- Πόσες φορές σηκώθηκε το στυλό από το χαρτί
- Πόσο πιέζει το στυλό στο χαρτί, σε ποια σημεία αυξάνεται ή μειώνεται αυτή η πίεση.

Ακόμη λοιπόν κι αν κάποιος δοκιμάσει να αντιγράψει υπογραφή με σκοπό την απάτη, καταλαβαίνετε ότι αποκλείεται να μην "συλληφθεί" από ένα τέτοιο σύστημα.

Το άλλο μεγάλο πλεονέκτημα που ήδη αναφέραμε, είναι το γεγονός ότι ο κόσμος θεωρεί πολύ φυσικό να υπογράφει κάπου για να πιστοποιεί με αυτόν τον τρόπο την ταυτότητά του. Είναι κάτι που γινόταν από ανέκαθεν, που γίνεται σήμερα, και που θα συνεχίσει να γίνεται για πάντα. Δεν είναι λοιπόν περίεργο το ότι η βιομετρική αυτή μέθοδος υποσκελίζει όλες τις άλλες στο θέμα της αποδοχής από το κοινό.

Αλλά και στο άλλο βασικό θέμα, το κόστος, η διακρίβωση υπογραφής δεν τα πηγαίνει καθόλου άσχημα. Ο βασικός εξοπλισμός, ένα light-pen δηλαδή, ή ένα ειδικό pad, δεν κοστίζει παρά μόνο μερικές χιλιάδες δραχμές. Βρήκαμε την τέλεια βιομετρική μέθοδο λοιπόν; Μάλλον όχι. Όπως έχουμε ξαναπεί δεν υπάρχει τέλεια βιομετρική μέθοδος. Όλες έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους. Και το μεγάλο μειονέκτημα της διακρίβωσης υπογραφής είναι η ακρίβεια. Θα έχετε ασφαλώς παρατηρήσει ότι η υπογραφή σας αλλάζει. Αλλάζει όταν είστε κουρασμένοι, ή όταν έχετε "καλλιγραφική" διάθεση. Αλλάζει όταν βιαζόσαστε, όταν δεν βιαζόσαστε, ή - το χειρότερο, γιατί δεν μπορείτε να το αποφύγετε - καθώς μεγαλώνετε. Δυστυχώς λοιπόν, η διακρίβωση υπογραφής έχει το χειρότερο "σκορ" στο θέμα της ακρίβειας, και μοιραία κατατάσσεται στην τελευταία θέση.

Η ΔΙΑΔΙΚΑΣΙΑ

Αυτή τη στιγμή υπάρχουν δύο μέθοδοι διακρίβωσης υπογραφής. Στην πρώτη ο χρήστης χρησιμοποιεί ένα ειδικό στυλό, και υπογράφει σε ένα κομμάτι κοινό χαρτί. Το στυλό αυτό έχει ενσωματωμένους αισθητήρες, μέσω των οποίων το σύστημα μπορεί να καταλάβει πόση πίεση χρησιμοποιεί ο χρήστης, πόσες φορές σηκώνεται το στυλό κ.λπ. Στη δεύτερη περίπτωση, χρησιμοποιείται ειδική πινακίδα, στην οποία και γίνεται η υπογραφή. Αυτήν τη φορά οι αισθητήρες είναι στην πινακίδα. Μια τρίτη μέθοδος έκανε την εμφάνισή της τώρα τελευταία, κατά την οποία το σύστημα "ακούει" και ερμηνεύει κατάλληλα τους ήχους που κάνει το στυλό πάνω στο χαρτί.

Αφού ο χρήστης υπογράψει, το σύστημα αναλαμβάνει να μετατρέψει όλες τις παραμέτρους που αναφέραμε παραπάνω σε μια μορφή μαθηματικού κώδικα, αρκετά επαρκή για να χαρακτηρίσει το συγκεκριμένο χρήστη.

ΠΡΟΪΟΝΤΑ

Μετρημένες στα δάχτυλα του ενός χεριού είναι οι εταιρείες που ασχολούνται με τη διακρίβωση υπογραφής, ενώ τα περισσότερα προϊόντα εστιάζουν κυρίως στο θέμα της ηλεκτρονικής υπογραφής εντύπων, παρά στο θέμα της ασφάλειας μέσω της υπογραφής. Παρόλα αυτά, υπάρχουν κάποια που αξίζουν την προσοχή μας.

Η εταιρεία PenOp (<http://www.penop.com>), μια από τις μεγαλύτερες στο χώρο, προωθεί τη σειρά PenOp Signature, τα προϊόντα της οποίας δίνουν τη δυνατότητα ηλεκτρονικής υπογραφής και ελέγχου εγγράφων σε κοινές μορφές, όπως αυτή του Microsoft Word. Η σειρά περιλαμβάνει επίσης SDK (software developer's kit), πρόγραμμα διαχείρισης και αποθήκευσης των βιομετρικών προτύπων, καθώς και δυνατότητα σύνδεσης με γνωστές βάσεις δεδομένων (Access, Oracle κ.λ.π).

Η εταιρεία Cyber-SIGN (<http://www.cybersign.com>) διαθέτει μια σειρά προϊόντων που περιλαμβάνει έλεγχο υπογραφής σε έγγραφα του Microsoft Word, SDK, αλλά και πρόγραμμα προστασίας οθόνης που απενεργοποιείται με έλεγχο υπογραφής. Επίσης, με το προϊόν Cyber-SIGN Server προσφέρει πιο ολοκληρωμένες λύσεις για περιβάλλοντα δικτύου.

Τέλος, η εταιρεία CIC (<http://www.cic.com>) διαθέτει το Sign-It, το οποίο κι αυτό μπορεί να συνεργαστεί με το Word 97. Στην ουσία, το πρόγραμμα επιτρέπει την προσθήκη ηλεκτρονικής υπογραφής στα έγγραφα του Word. Σε περίπτωση που γίνει κάποια αλλαγή στο κείμενο, η υπογραφή αφαιρείται αυτόματα.

7.2 ΡΥΘΜΟΣ ΠΛΗΚΤΡΟΛΟΓΗΣΗΣ

Ο ρυθμός πληκτρολόγησης θεωρείται βιομετρική μέθοδος με βάση συμπεριφορά, και ήδη η ανάπτυξή του βρίσκεται σε καλό σημείο. Η μέθοδος εστιάζει στον τρόπο που πληκτρολογεί κάποιο άτομο, ελέγχοντας παραμέτρους όπως η καθυστέρηση ανάμεσα σε συγκεκριμένα πλήκτρα, ο μέσος όρος ταχύτητας κ.λπ. Το βασικό πρόβλημα της μεθόδου (όπως και όλων των μεθόδων βάσει συμπεριφοράς) είναι ότι η συμπεριφορά του χρήστη αλλάζει σχετικά εύκολα. Για παράδειγμα, καθώς η μέρα περνάει ο ρυθμός πληκτρολόγησης κάποιου πέφτει, αφού η κούραση αρχίζει να ενεργεί. Όσον αφορά τη χρήση της μεθόδου σε μεγάλες μάζες, την καθιστά απαγορευτική το γεγονός ότι πληκτρολόγηση δεν ξέρουν όλοι οι άνθρωποι, και όπως καταλαβαίνετε κάτω από κάποιες ταχύτητες παύει να υφίσταται οποιαδήποτε έννοια μέτρησης.

Η εταιρεία NetNanny (<http://www.netnanny.com>) μας δίνει την ευκαιρία να πάρουμε μια ιδέα για τη βιομετρική του αύριο, με το προϊόν BioPassword, ένα βιομετρικό σύστημα αναγνώρισης ρυθμού πληκτρολόγησης για προσωπικούς υπολογιστές. Στη σελίδα <http://www.biopassword.com> θα βρείτε περισσότερες πληροφορίες.

7.3 ΑΝΑΓΝΩΡΙΣΗ ΦΛΕΒΙΚΗΣ ΔΟΜΗΣ

Η συγκεκριμένη μέθοδος προσπαθεί να "διαβάσει" τη φλεβική δομή που γίνεται αρκετά έντονη στο επάνω μέρος της ανθρώπινης παλάμης. Για να καταστεί αυτό δυνατό, χρησιμοποιείται υπέρυθη ακτινοβολία. Συνήθως, για να τονιστεί ακόμα περισσότερο το "δέντρο" των φλεβών, ο χρήστης υποχρεούται να σφίξει το χέρι του σε γροθιά. Η ανάπτυξη της μεθόδου έχει ξεκινήσει αρκετά χρόνια τώρα, και μάλιστα κάποια προϊόντα υπάρχουν ήδη στην αγορά. Το γεγονός ότι τοποθετείται στα "μελλοντικά" συστήματα οφείλεται κυρίως στο ότι η πρακτική εφαρμογή της είναι ακόμα αρκετά περιορισμένη.

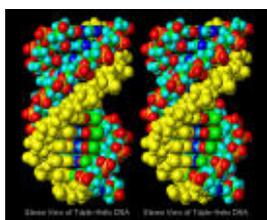
Κάποια βιομετρικά προϊόντα ανάγνωσης της φλεβικής δομής μπορείτε να βρείτε στη σελίδα της Advanced Biometrics (<http://www.adv-bio.net>). Ενδιαφέρουσες πληροφορίες υπάρχουν και στη διεύθυνση <http://innotts.co.uk/~joerice>.

7.4 ΑΝΑΓΝΩΡΙΣΗ ΓΕΩΜΕΤΡΙΑΣ ΑΥΤΙΟΥ



Αυτή η παράξενη βιομετρική μέθοδος, που απ" όλα τα μέρη του σώματος διάλεξε το αυτί ως το μέσο αναγνώρισης, θεωρείται αρκετά ακριβής και εφαρμόζεται ήδη σήμερα από αρκετές αστυνομίες ανά τον κόσμο. Οι βασικές της αρχές είναι παρόμοιες με τα υπόλοιπα συστήματα αναγνώρισης γεωμετρίας, αυτά του προσώπου και του χεριού. Μένει μόνο να δούμε αν κάποια στιγμή θα χρησιμοποιηθεί και για πιο γενικούς σκοπούς.

7.5 ΕΛΕΓΧΟΣ DNA



Αν και ο έλεγχος DNA είναι σήμερα εφικτός μέσα σε διάστημα 10 λεπτών, δεν μπορεί να χαρακτηριστεί βιομετρική μέθοδος αφού η αναγνώριση δεν γίνεται αυτόματα. Αν αυτό γίνει κάποια στιγμή δυνατό, η νέα βιομετρική μέθοδος θα υποσκελίσει όλες τις άλλες στο θέμα της ακριβείας. Παρόλα αυτά, θα πρέπει να βελτιωθεί ο τρόπος λήψης του βιομετρικού δείγματος, αφού όλοι οι σημερινοί τρόποι (λήψη αίματος, σάλιου, ή άλλου σωματικού υγρού) είναι εξαιρετικά προβληματικοί και ανεφάρμοστοι σε ευρύτερη κλίμακα.

7.6 ΑΝΑΓΝΩΡΙΣΗ ΣΩΜΑΤΙΚΗΣ ΟΣΜΗΣ

Αν έχετε ταξιδέψει με τον ηλεκτρικό καλοκαίρι και μεσημβρινές ώρες, σίγουρα θα έχετε διαπιστώσει ότι η σωματική μυρωδιά μπορεί να χαρακτηρίσει κάποιον με πολύ μοναδικό τρόπο... Ακριβώς αυτό το γεγονός προσπαθεί λοιπόν να εκμεταλλευτεί μια νέα βιομετρική μέθοδος, η οποία βρίσκεται ακόμα σε πολύ πρώιμο στάδιο. Το σύστημα βασίζεται στην ανάλυση της χημικής σύστασης της οσμής που εκπέμπει το ανθρώπινο σώμα, ενώ το δείγμα συνήθως λαμβάνεται από το πίσω μέρος της παλάμης.

7.7 ΑΠΟΤΥΠΩΜΑΤΑ ΠΑΛΑΜΗΣ



Το σύστημα αυτό λειτουργεί παρόμοια με τα συστήματα των δακτυλικών αποτυπωμάτων, διαβάζοντας αντί για την άκρη του δαχτύλου τις γραμμώσεις της παλάμης του χρήστη. Μέχρι τώρα έχει χρησιμοποιηθεί μόνο σε ποινικές εφαρμογές, αλλά οι εταιρείες που ασχολούνται με τη μέθοδο ελπίζουν κάποια στιγμή να τη φέρουν και στην πολιτική χρήση. Η μέθοδος θεωρείται αρκετά ακριβής.

7.8 ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΦΥΣΙΚΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ



Στην εποχή μας που η ασφάλεια είναι μια από τις κυριότερες απαιτήσεις, μια μέθοδος που να μπορεί να αναγνωρίσει αξιόπιστα την ταυτότητα ενός ατόμου είναι από τα σημαντικότερα ζητούμενα. Το ρόλο αυτό φιλοδοξούν να αναλάβουν τα συστήματα αναγνώρισης φυσικών χαρακτηριστικών.

Με το πέρασμα του χρόνου και την πρόοδο της τεχνολογίας, καθημερινά ερχόμαστε σε επαφή με επιτεύγματα, που παλιότερα αποτελούσαν πεδίο δράσης και αντικείμενο πόθου της επιστημονικής φαντασίας. Πόσοι άραγε από εμάς δεν θυμόμαστε τον Hal, τον υπολογιστή της Οδύσσειας 2001. Βασική του ικανότητα ήταν ότι μπορούσε να αναγνωρίσει τον ιδιοκτήτη του. Με τις νέες μεθόδους αναγνώρισης φυσικών χαρακτηριστικών, σε λίγο καιρό η εικόνα αυτή θα μας είναι οικεία και καθημερινή. Η αναγνώριση φυσικών χαρακτηριστικών (biometrics) είναι μια σειρά από αυτοματοποιημένες διεργασίες, οι οποίες αναγνωρίζουν ένα άτομο, αναλύοντας κάποια χαρακτηριστικά του. Τα κυριότερα χαρακτηριστικά που μετρώνται και αναγνωρίζονται είναι το πρόσωπο, τα δακτυλικά αποτυπώματα, η μορφολογία του χεριού, ο γραφικός χαρακτήρας, ο αμφιβληστροειδής του ματιού και η φωνή. Η πρώτη κατηγοριοποίηση που μπορούμε να κάνουμε έχει σχέση με το είδος των στοιχείων που χρησιμοποιούμε για την αναγνώριση ενός προσώπου. Παρατηρούμε ότι εκτός από την αναγνώριση φωνής, όλες οι υπόλοιπες μέθοδοι στηρίζονται στην αναγνώριση εικόνας.

Η αναγνώριση φυσικών χαρακτηριστικών στην πράξη

Σε σχέση με παραδοσιακές μεθόδους ταυτοποίησης προσώπων, η αναγνώριση φυσικών χαρακτηριστικών έχει αρκετά πλεονεκτήματα. Είναι αρκετά δυσκολότερο να ξεγελάσει κανείς ένα σύστημα αλλοιώνοντας τα φυσικά χαρακτηριστικά και δίνοντας μια ψεύτικη εικόνα. Από την άλλη όμως, μια και κάθε σύστημα παρουσιάζει κάποια σφάλματα και ποσοστά λάθους, είναι καλύτερα να χρησιμοποιούμε δύο, ή και περισσότερες μεθόδους αναγνώρισης φυσικών χαρακτηριστικών. Ο συνδυασμός των μεθόδων παρέχει ένα πολύ αξιόπιστο αποτέλεσμα και αποτελεί μια αποτελεσματική λύση. Τα πεδία εφαρμογής των biometrics είναι ανεξάντλητα. Κάθε δραστηριότητα που εμπεριέχει ασφάλεια και αναγνώριση προσώπων μπορεί να εμπεριέχει ένα σύστημα biometrics. Αρκετοί ειδικοί υποστηρίζουν ότι η ταυτότητα του μέλλοντος θα είναι μία smartcard, που θα περιέχει δείγματα φωνής, τρισδιάστατες φωτογραφίες και δακτυλικά αποτυπώματα του ατόμου που αναφέρεται. Εφαρμογές που ξεκινούν από τραπεζικές συναλλαγές και φθάνουν έως και την πρόσβαση σε απαγορευμένους χώρους, σταδιακά θα χρησιμοποιήσουν ένα τέτοιο σύστημα και θα αντικαταστήσουν τις παραδοσιακές μεθόδους. Το βασικό σημείο είναι ότι εξαλείφεται ο ανθρώπινος παράγοντας, άρα και το ανθρώπινο ποσοστό λάθους. Από την άλλη όμως, μπορούμε να πούμε ότι η τεχνολογία αναγνώρισης φυσικών

χαρακτηριστικών είναι μόλις στην αρχή της. Τα περιθώρια βελτίωσης των συστημάτων είναι πολύ μεγάλα, ειδικά σε επίπεδο ταχύτητας. Από τη στιγμή που οι αλγόριθμοι ταξινόμησης και ταυτοποίησης και τα υπολογιστικά συστήματα που τους συνοδεύουν γίνουν αρκετά γρήγοροι, τότε και τα στοιχεία θα μπορούν να γίνουν περισσότερα, τα πρόσωπα θα μπορούν να αναλύονται λεπτομερέστερα και τα αποτελέσματα αναγνώρισης θα είναι ακριβέστερα.

7.8.1 ΑΝΑΓΝΩΡΙΣΗ ΕΙΚΟΝΑΣ



Η εικόνα όπως τη βλέπουμε πριν...



...και μετά την επεξεργασία.

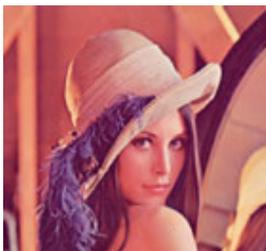
Όλες οι υπόλοιπες μέθοδοι αναγνώρισης φυσικών χαρακτηριστικών στηρίζονται στην αναγνώριση εικόνας. Μέσα στο ανθρώπινο μυαλό το ερέθισμα του σχήματος και του χρώματος αποθηκεύεται και δημιουργείται η εικόνα. Ο άνθρωπος χρησιμοποιεί την αντίληψή του και την προσαρμόζει στην εικόνα που περιμένει να δει.

Για παράδειγμα, θεωρούμε δύο φωτογραφίες όμοιες, χωρίς να απαριθμήσουμε όλες τις ακριβείς λεπτομέρειες του θέματος που απεικονίζει. Κάτι τέτοιο δεν είναι δυνατόν να πραγματοποιηθεί σε ένα υπολογιστικό σύστημα, με αποτέλεσμα η αναγνώριση εικόνας να μην είναι τόσο απλή υπόθεση. Βασική επιδίωξη και κατεύθυνση της έρευνας είναι να μπορέσει να μιμηθεί τον ανθρώπινο εγκέφαλο, οι ερευνητικές ομάδες προσπαθούν να δημιουργήσουν συστήματα που να συμπεριφέρονται και να αντιδρούν στα ερεθίσματα μιας εικόνας όπως ο άνθρωπος.

Κάθε φωτογραφία και γενικότερα κάθε εικόνα αποτελείται από πολλά διαφορετικά στοιχεία που προσδιορίζουν την ταυτότητά της. Αν και κάθε χαρακτηριστικό μιας εικόνας μπορεί να έχει ξεχωριστή μορφή, μπορούμε να κάνουμε κάποιο είδος κατηγοριοποίησης και να δημιουργήσουμε βάση δεδομένων προτύπων, με βάση τα οποία θα γίνεται η σύγκριση. Για παράδειγμα, ένα χρώμα μπορεί να υπάρχει σε αρκετές διαφοροποιήσεις και παραλλαγές. Από τη στιγμή που έχουμε τη δυνατότητα να κατηγοριοποιήσουμε μια εικόνα, μπορούμε να φτιάξουμε ένα

μοντέλο της φωτογραφίας, που να μπορεί να αναγνωστεί και να επεξεργαστεί από ένα υπολογιστικό σύστημα. Η μορφή που εξάγεται από αυτή τη διαδικασία, μπορεί να συγκριθεί μέσω ενός νευρωνικού δικτύου ή ενός έξυπνου συστήματός, με τη βάση δεδομένων με τα πρότυπα και να γίνει η ταυτοποίηση.

Μια και μιλάμε για φυσικά χαρακτηριστικά, δεν θα μπορούσαμε να παραλείψουμε την αναγνώριση προσώπου. Η ιδιαιτερότητα αυτού του χαρακτηριστικού είναι το γεγονός ότι δημιουργεί τρισδιάστατα μοντέλα και άρα η αναγνώρισή του δεν ακολουθεί την προηγούμενη διαδικασία. Αρχικά γίνεται η κωδικοποίηση του μοντέλου με την ανίχνευση των ομογενών περιοχών χρώματος και η καταγραφή τους σε στοιχεία. Κάθε στοιχείο έχει τα δεδομένα που αντιπροσωπεύουν μια περιοχή χρώματος. Αν δύο περιοχές περιέχουν τα ίδια στοιχεία χρώματος και εφάπτονται, τότε επικαλύπτει η μία την άλλη. Αυτή η διαδικασία χρησιμοποιείται μέχρις ότου να καλυφθεί όλη η επιφάνεια του προσώπου. Ουσιαστικά το πρόσωπο χωρίζεται σε κομμάτια και δημιουργείται ένα μοντέλο που αποτελείται από πληροφορίες χρώματος. Άλλο γνώρισμα που εξετάζεται μετά είναι η απόσταση και η θέση που είναι τοποθετημένα τα χαρακτηριστικά του προσώπου. Καταγράφονται οι γωνίες των ματιών, των ρουθουνιών κτλ., προκειμένου να μπορούν να κατηγοριοποιηθούν και να εισαχθούν ή να επεξεργαστούν με τη βάση που περιέχει τα πρότυπα. Ένας άλλος τρόπος που χρησιμοποιείται βασίζεται σε μαθηματικά μοντέλα. Χρησιμοποιούμε μια σύνθετη γραφική παράσταση (γράφος) για να αντιπροσωπεύσουμε ένα χαρακτηριστικό του προσώπου. Από εκεί και πέρα, μπορούμε να δημιουργήσουμε ολόκληρο το πρόσωπο, ενώνοντας όλους τους γράφους και σχηματίζοντας τη συνολική εικόνα. Ο αριθμός, το είδος και η θέση του κάθε γράφου αποτελούν την ταυτότητα κάθε προσώπου. Έχοντας αυτά τα δεδομένα, μπορούμε να συγκρίνουμε το πρόσωπο με τη βάση δεδομένων που έχουμε ήδη καταχωρήσει τη φωτογραφία και μέσω αλγορίθμων σύγκρισης να αναγνωρίσουμε ή όχι, την ταυτότητα του ατόμου. Φυσικά επειδή μιλάμε για τρισδιάστατη απεικόνιση, τα δεδομένα που απαιτούνται είναι αρκετά μεγάλου μεγέθους και γι' αυτό ο χρόνος αναγνώρισης είναι αρκετά μεγάλος.



Ένα πρόσωπο πριν να επεξεργαστεί...



... αναγνωρίζοντας τις χρωματικές περιοχές.

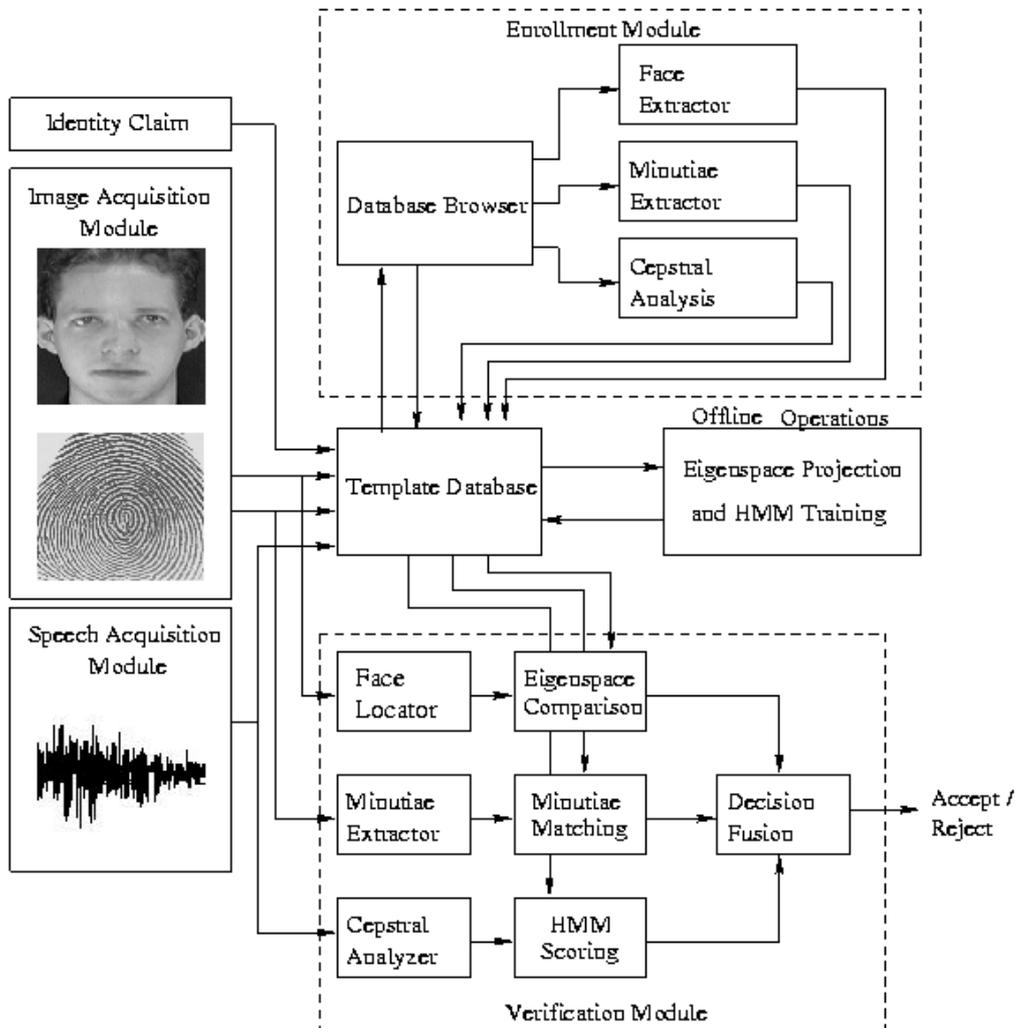
7.8.2 ΠΟΛΥΜΟΡΦΑ ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ

Πρόσωπα και δακτυλικά αποτυπώματα ενσωμάτωσης για τον προσωπικό προσδιορισμό

Ένα αυτόματο προσωπικό σύστημα προσδιορισμού βασισμένο απλώς στα δακτυλικά αποτυπώματα ή τα πρόσωπα δεν είναι συχνά ικανό να καλύψει τις απαιτήσεις απόδοσης συστημάτων. Η αναγνώριση προσώπου είναι γρήγορη αλλά μη αξιόπιστη ενώ η επαλήθευση δακτυλικών αποτυπωμάτων είναι αξιόπιστη αλλά ανεπαρκής στην ανάκτηση βάσεων δεδομένων. Έχουμε αναπτύξει ένα βιομετρικό σύστημα πρωτοτύπων που ενσωματώνει τα πρόσωπα και τα δακτυλικά αποτυπώματα. Το σύστημα υπερνικά τους περιορισμούς των συστημάτων αναγνώρισης προσώπου καθώς επίσης και των συστημάτων επαλήθευσης δακτυλικών αποτυπωμάτων. Το ενσωματωμένο σύστημα πρωτοτύπων λειτουργεί στον τρόπο προσδιορισμού με έναν αποδεκτό χρόνο απόκρισης. Η ταυτότητα που καθιερώνεται από το σύστημα είναι πιο αξιόπιστη από την ταυτότητα που καθιερώνεται από ένα σύστημα αναγνώρισης προσώπου. Επιπλέον, το προτεινόμενο σχήμα τήξης απόφασης επιτρέπει τη βελτίωση απόδοσης με την ενσωμάτωση των πολλαπλάσιων συνθημάτων με τα διαφορετικά μέτρα εμπιστοσύνης. Τα πειραματικά αποτελέσματα καταδεικνύουν ότι το σύστημά μας αποδίδει πολύ καλά. Καλύπτει το χρόνο απόκρισης καθώς επίσης και τις απαιτήσεις ακρίβειας.

Ένα πολύμορφο βιομετρικό σύστημα που χρησιμοποιεί το δακτυλικό αποτύπωμα, το πρόσωπο και την ομιλία:

Ένα βιομετρικό σύστημα που στηρίζεται μόνο σε ένα ενιαίο βιομετρικό προσδιοριστικό, στην παραγωγή ενός προσωπικού προσδιορισμού δεν είναι συχνά ικανό να καλύψει τις επιθυμητές απαιτήσεις απόδοσης. Ο προσδιορισμός βασισμένος στην πολλαπλάσια βιομετρική αντιπροσωπεύει μια αναδυόμενη τάση. Εισάγουμε ένα πολύμορφο βιομετρικό σύστημα, το οποίο ενσωματώνει την αναγνώριση προσώπου, την επαλήθευση δακτυλικών αποτυπωμάτων και την επαλήθευση ομιλητών στην παραγωγή ενός προσωπικού προσδιορισμού. Αυτό το σύστημα εκμεταλλεύεται τις ικανότητες κάθε ατόμου. Μπορεί να χρησιμοποιηθεί για να υπερνικήσει μερικούς από τους περιορισμούς μιας ενιαίας βιομετρικής. Τα προκαταρκτικά πειραματικά αποτελέσματα καταδεικνύουν ότι η ταυτότητα που καθιερώνεται από ένα τέτοιο ενσωματωμένο σύστημα είναι πιο αξιόπιστη από την ταυτότητα που καθιερώνεται από ένα σύστημα αναγνώρισης προσώπου, ένα σύστημα επαλήθευσης δακτυλικών αποτυπωμάτων, και ένα σύστημα επαλήθευσης ομιλητών.

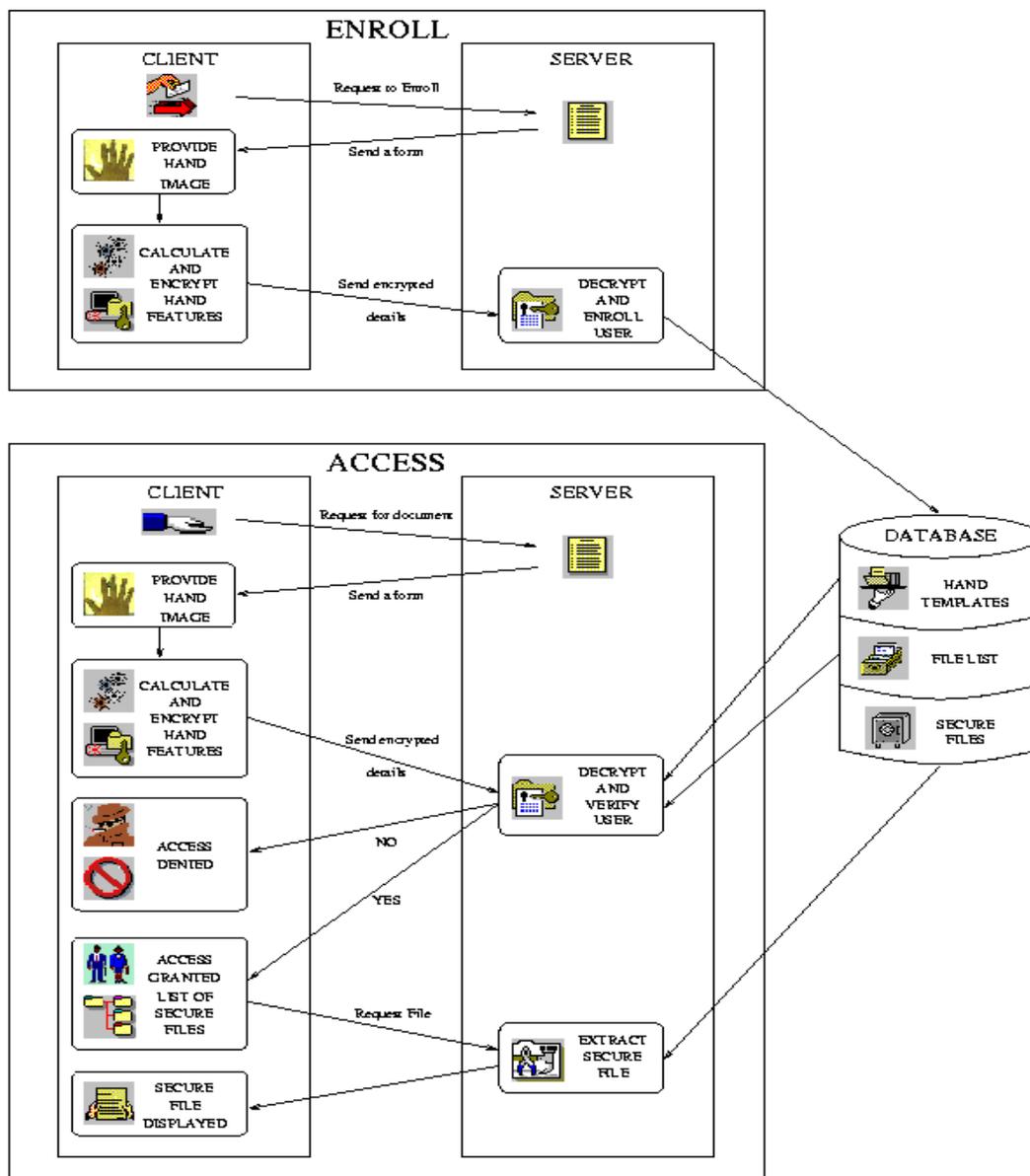


7.8.3 ΒΙΟΜΕΤΡΙΚΗ ΒΑΣΙΣΜΕΝΗ ΣΤΗΝ ΠΡΟΣΒΑΣΗ ΙΣΤΟΥ

Η επικύρωση και η κρυπτογράφηση είναι κρίσιμες για την ασφάλεια δικτύων. Το δημόσιο κλειδί της κρυπτογραφίας παρέχει έναν ασφαλή τρόπο να ανταλλαχθούν οι πληροφορίες αλλά ο σχεδιασμός ενός υψηλού συστήματος επικύρωσης ασφαλείας παραμένει ακόμα ένα ανοικτό πρόβλημα. Οι σύνθετοι κωδικοί πρόσβασης είναι εύκολο να ξεχαστούν ενώ οι απλοί κωδικοί πρόσβασης υποθέτονται εύκολα από τα αναρμόδια πρόσωπα. Αρκετά από τα βιομετρικά χαρακτηριστικά ενός ατόμου είναι μοναδικά και δεν αλλάζουν κατά τη διάρκεια του χρόνου. Αυτές οι ιδιότητες καθιστούν τη βιομετρική κατάλληλη για την επικύρωση. Τα συστήματα επικύρωσης βασισμένα στα δακτυλικά αποτυπώματα, τη φωνή, την ίριδα και τη γεωμετρία χεριών υπάρχουν για τις εφαρμογές όπως ο έλεγχος διαβατηρίων, οι ιατροδικαστικές, οι αυτόματες μηχανές αφηγητών, η άδεια οδηγών και ο έλεγχος συνόρων. Με την αυξανόμενη ανάπτυξη του Διαδικτύου, υπάρχει μια ανάγκη να περιοριστεί η πρόσβαση στα ευαίσθητα στοιχεία όσον αφορά τον Ιστό στους εξουσιοδοτημένους χρήστες. Έχουμε αναπτύξει ένα σύστημα πρωτοτύπων που χρησιμοποιεί τη γεωμετρία χεριών για να επικυρώσει τους χρήστες, για να

περιορίσει την πρόσβαση σε ιστοσελίδες. Η αρχική αξιολόγηση του συστήματος πρωτοτύπων είναι ενθαρρυντική. Οι παρόμοιες τεχνικές μπορούν να χρησιμοποιηθούν για να επικυρώσουν τους ανθρώπους για τις εφαρμογές ηλεκτρονικού εμπορίου.

Το διάγραμμα ροής



7.9 ΜΟΝΑΔΙΚΑ ΦΩΤΕΙΝΑ ΑΠΟΤΥΠΩΜΑΤΑ ΑΠΟ ΤΟ ΔΕΡΜΑ

Τι σας κάνει μοναδικούς; Είναι μήπως οι ραβδώσεις κάτω από τα νύχια σας, οι τριγμοί των οστών σας, το σχήμα του αυτιού ή η οσμή σας; Τα σύνορα της βιομετρίας, όπως βλέπετε, δεν ανήκουν στο χώρο της ποίησης.

Εξαιρεση στον κανόνα αποτελεί η μικρή ασημένια συσκευή με όνομα Αισθητήρας Φωτεινού Αποτυπώματος (ΑΦΑ). Η συσκευή, μία από τις πολλά υποσχόμενες νέες εφαρμογές, λειτουργεί μετρώντας την αντανάκλαση πολύχρωμου φωτός πάνω στο δέρμα σας. Το πάχος του δέρματος, τα αγγεία και άλλα μοναδικά χαρακτηριστικά επηρεάζουν με ένα συγκεκριμένο τρόπο το φως, αφήνοντας ένα ιδιαίτερο αποτύπωμα. Το σύστημα δεν επηρεάζεται από εγκαύματα, εκδορές ή σκόνη. Αν και δοκιμές έχουν γίνει μέχρι στιγμής μόνο σε 500 άτομα, τα φωτεινά αποτυπώματα είναι μοναδικά. «Το σύστημά μας αναγνωρίζει και διαχωρίζει ακόμη και διδύμους», λέει ο Ρομπ Ρόου, συνιδρυτής της κατασκευάστριας εταιρείας στην Αλμπουκέρκι του Νέου Μεξικού.

Εώς τα τέλη του χρόνου, ο αισθητήρας ΑΦΑ θα βρίσκεται σε χρήση. Σε συνδυασμό με ένα ανιχνευτή χειρός, θα ελέγχει την είσοδο στο εργαστήριο επικίνδυνων πειραμάτων του Πανεπιστημίου του Νέου Μεξικού.

Οι αισθητήρες αυτοί ενδιαφέρουν και τους μηχανολόγους της εταιρείας κατασκευής όπλων Smith & Wesson, η οποία επιθυμεί να κατασκευάσει ένα «έξυπνο όπλο». Ένας αισθητήρας ΑΦΑ ενσωματωμένος στη λαβή του όπλου, δεν θα επιτρέπει τη χρήση του από κανέναν άλλον, παρά μόνο από τον ιδιοκτήτη του. Η εταιρεία προσπαθεί τώρα να επιτύχει την κατασκευή αισθητήρα, που θα δίνει τη δυνατότητα χρήσης του όπλου από δύο άτομα.

Ανάλογη αξιοποίηση του αισθητήρα φωτεινού αποτυπώματος θα μπορέσει να προσφέρει μεγάλο βαθμό ασφάλειας στους κατόχους κινητών τηλεφώνων, φορητών υπολογιστών, ακόμη και αυτοκινήτων.

7.10 ΑΝΑΓΝΩΡΙΣΗ ΒΗΜΑΤΙΣΜΟΥ



Στην λίστα με τις τεχνολογίες βιομετρικής αναγνώρισης, όπως των δαχτυλικών αποτυπωμάτων, της ίριδας του ματιού και του σχήματος του προσώπου, πρέπει πλέον να προσθέσουμε και την αναγνώριση βηματισμού. Παρόλο που η συγκεκριμένη τεχνολογία βρίσκεται ακόμα στο στάδιο της ανάπτυξης, θεωρείται αρκετά υποσχόμενη και αναμένεται, όταν τελειοποιηθεί, να αποτελέσει ένα ισχυρό όπλο στην προσπάθεια εντοπισμού εγκληματιών.

Είναι πλέον διαπιστωμένο ότι κάθε ένας από εμάς περπατάει με ένα δικό του μοναδικό τρόπο που ονομάζουμε βηματισμό. Ίσως αυτό από πρώτη μάτια να μας φαίνεται παράξενο, αν όμως λάβουμε υπόψη τα διαφορετικά φυσικά χαρακτηριστικά του κάθε ανθρώπου, καταλήγουμε ότι είναι λογικό οι κινήσεις που εκτελεί κάποιος όταν περπατάει να είναι μοναδικές.

Το γεγονός αυτό αξιοποιείται εδώ και κάποιο διάστημα από ερευνητές, προκειμένου να υλοποιήσουν μια πλατφόρμα που θα διακρίνει αυτές τις διαφορές

και θα δημιουργεί συγκεκριμένα πρότυπα αποσκοπώντας εντέλει, στην σύγκριση και αναγνώριση της ταυτότητας προσώπων. Το έναυσμα για την πραγματοποίηση αυτών των ερευνητικών προγραμμάτων, αλλά και η απαραίτητη χρηματοδότηση για την υλοποίηση τους προήλθε από την DAPRA (Defense Advanced Research Projects Agency) στα πλαίσια του συστήματος ΤΙΑ (Total Information Awareness ή όπως προσφάτως μετονομάστηκε Terrorism Information Awareness). Όσον αφορά την DAPRA ή αλλιώς Υπηρεσία Εξελιγμένων Ερευνητικών Σχεδίων Άμυνας, πρόκειται για μια υπηρεσία ασφαλείας των ΗΠΑ που έχει επιφορτιστεί με το έργο διερεύνησης των ορίων της τεχνολογίας και εκμετάλλευσης των δυνατοτήτων της, με σκοπό την υλοποίηση υπερσύγχρονων συστημάτων ασφαλείας υψηλών δυνατοτήτων. Επιπρόσθετα, το ΤΙΑ αποτελεί ένα σύστημα τεράστιων ηλεκτρονικών αρχείων με χιλιάδες βάσεις δεδομένων και πλήθος από πληροφορίες, που η αμερικανική κυβέρνηση συλλέγει κατά καιρούς και δυστυχώς περιλαμβάνουν και προσωπικά δεδομένα πολιτών. Έτσι, λοιπόν, στις μέρες μας, η προτεραιότητα που δίνεται στις πολιτικές για την αντιμετώπιση της τρομοκρατίας, εκτός από πρόσχημα για την διεξαγωγή πολέμων, οδηγεί και στην υλοποίηση πιλοτικών προγραμμάτων, με σκοπό την αναζήτηση νέων τεχνολογικά προηγμένων συστημάτων ασφαλείας.

Ένα από αυτά είναι και το project για την αναγνώριση βηματισμού, που ανατέθηκε κυρίως στο Georgia Institute of Technology, ενώ και άλλοι ερευνητές από διάφορα πανεπιστημιακά ιδρύματα ασχολούνται με το συγκεκριμένο θέμα. Απώτερος σκοπός της έρευνας είναι η δημιουργία προηγμένων συστημάτων επιτήρησης, που θα μπορούν να αναγνωρίσουν και να πιστοποιήσουν ανθρώπινους στόχους από τον τρόπο που περπατάνε σε κρίσιμες περιοχές ασφαλείας, όπως αεροδρόμια ή γύρω από κυβερνητικά κτίρια.

Θέλοντας τώρα να αναλύσουμε την τεχνική με την οποία επιτυγχάνεται η αναγνώριση βηματισμού, πρέπει να αναφέρουμε ότι οι μέθοδοι που έχουν αναπτυχθεί βασίζονται σε δύο βασικά μοντέλα. Το ένα χρησιμοποιεί βιντεοκάμερες προκειμένου να συλλαμβάνονται οι εικόνες των ατόμων που περπατάνε, ενώ η άλλη μέθοδος βασίζεται στην τεχνολογία των Radar.

Στην πρώτη περίπτωση κάμερες και υπολογιστές συνεργάζονται προκειμένου να δημιουργήσουν "υπογραφές βηματισμού" που θα είναι μοναδικές για κάθε άνθρωπο. Όταν ένας άνθρωπος περπατάει, τα μέρη του σώματός του - χέρια, γόνατα, πόδια, αγκώνες και άλλα- δημιουργούν ένα συγκεκριμένο επαναλαμβανόμενο πρότυπο κίνησης. Έτσι, λοιπόν, βιντεοκάμερες συλλαμβάνουν την δραστηριότητα της κίνησης και μεταφέρουν τα δεδομένα σε ηλεκτρονικό υπολογιστή για περαιτέρω ανάλυση. Ο υπολογιστής επεξεργάζεται τις κινήσεις και σε συνδυασμό με μαθηματικές συναρτήσεις και αλγόριθμους, δημιουργεί την λεγόμενη "υπογραφή βηματισμού", που είναι ξεχωριστή για τον καθένα και θα αποτελεί εφεξής το στοιχείο αναγνώρισης του (εικόνα 1).

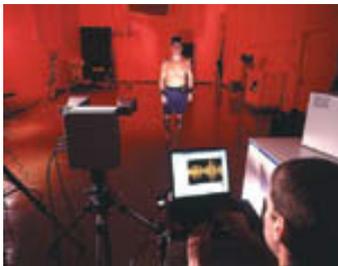


Εικόνα 1. Ειδικό software επεξεργάζεται τις εικόνες βηματισμού και δημιουργεί ένα πρότυπο, ξεχωριστό για κάθε άνθρωπο.

Το συγκεκριμένο μοντέλο επεξεργάζονται ερευνητές από το Ινστιτούτο Τεχνολογίας της Μασαχουσέτης, το πανεπιστήμιο του Southampton, αλλά και από το Carnegie Mellon University επικουρούμενοι από την DAPRA. Οι δοκιμές του προγράμματος πραγματοποιήθηκαν με την συνδρομή εθελοντών που περπάτησαν πάνω σε τεχνητούς διαδρόμους αλλάζοντας κάθε φορά το φόντο. Το ποσοστό ακριβείας στην αντιστοίχιση των προτύπων με το εκάστοτε άτομο που υπόκεινταν

στον έλεγχο, κυμαίνονταν από 90% μέχρι 95%. Σε πρώτη φάση η επίδοση αυτή θεωρείται αρκετά ενθαρρυντική, πρέπει όμως να λάβουμε υπόψη ότι η έρευνα πραγματοποιήθηκε σε ένα καθαρά πειραματικό περιβάλλον με ιδανικές συνθήκες. Στον «πραγματικό κόσμο» όμως υπεισέρχονται παράγοντες, όπως κίνηση μέσα σε πλήθος, διαφορετικές και δύσκολες συνθήκες φωτισμού, καθώς και μεγάλες αποστάσεις. Όλοι αυτοί οι παράγοντες αποτελούν τις μεγάλες προκλήσεις που καλούνται να αντιμετωπίσουν τα συγκεκριμένα συστήματα.

Το δεύτερο βιομετρικό μοντέλο αναγνώρισης βηματισμού υλοποιήθηκε στο Ινστιτούτο Τεχνολογίας της Georgia στην Ατλάντα και προσεγγίζει το ζήτημα κάπως διαφορετικά. Έτσι, αντί να έχουμε βιντεοκάμερες, αξιοποιούνται συσκευές radar όμοιες με αυτές που χρησιμοποιεί η τροχαία για τον έλεγχο της ταχύτητας των οχημάτων (εικόνα 2).

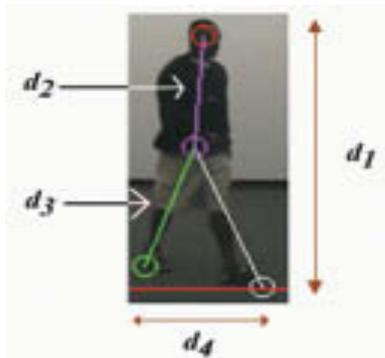


Εικόνα 2. Πειράματα αναγνώρισης βηματισμού στο Ινστιτούτο Τεχνολογίας της Georgia χρησιμοποιούν συσκευές radar, όμοιες με αυτές της τροχαίας.

Η λειτουργία των συσκευών αυτών δεν διαφέρει καθόλου από την αρχή λειτουργίας των radar. Συγκεκριμένα, το σύστημα εκπέμπει κύματα και λαμβάνει τα ανακλώμενα σήματα που προέρχονται από τους εκάστοτε στόχους. Στην προκειμένη περίπτωση πρόκειται για ανθρώπους που κινούνται, με αποτέλεσμα τα ανακλώμενα σήματα που λαμβάνει το radar να διαφέρουν, κάτι άλλωστε που προκύπτει και από το φαινόμενο Doppler. Δηλαδή κάθε αντικείμενο που πλησιάζει πιο κοντά στο radar, παράγει σήματα υψηλότερης συχνότητας σε σχέση με αυτά που απομακρύνονται. Το σύστημα που ανέπτυξαν στο Ινστιτούτο Τεχνολογίας της Georgia είναι αρκετά ευαίσθητο να αναγνωρίζει και να συλλαμβάνει τις μεταβολές στη συχνότητα που οφείλεται στο φαινόμενο Doppler, κατά την διάρκεια των φυσικών κινήσεων βαδίσματος κάθε ανθρώπου. Όταν λοιπόν κάποιος βαδίζει προς την συσκευή ανίχνευσης, ένα συγκεκριμένο μέρος του σώματος του, για παράδειγμα το δεξί του πόδι, θα παράγει υψηλότερη συχνότητα, ενώ κάποιο άλλο σημείο, όπως το δεξί του χέρι θα παρουσιάζει χαμηλότερη συχνότητα. Αναγνωρίζοντας, λοιπόν, το σύστημα αυτές τις διαφορές με μεγάλη ευαισθησία, δημιουργεί μια “υπογραφή βηματισμού” μοναδική για το καθένα που επιτρέπει την διάκριση μεταξύ των ατόμων. Οι υπεύθυνοι του προγράμματος υποστηρίζουν ότι η λειτουργία του συστήματος δεν επηρεάζεται από τα ρούχα ή από ακραίες καιρικές συνθήκες, κάτι που το καθιστούν ιδανικό για συστήματα επιτήρησης εξωτερικών χώρων. Οι εργαστηριακοί έλεγχοι της συγκεκριμένης ομάδας κατέληξαν σε ένα ποσοστό επιτυχίας που κυμαίνονταν από 80% μέχρι 95%, με στόχο όμως το ποσοστό αυτό να παγιωθεί πάνω από 90%. Ένα άλλος τομέας που χρίζει βελτίωση είναι η απόσταση ορθής λειτουργίας του συστήματος, δηλαδή η απόσταση μεταξύ στόχου και ανιχνευτή, όπου τα αποτελέσματα θα ανταποκρίνονται στην πραγματικότητα. Έτσι, ενώ στις αρχές των ερευνών η απόσταση αυτή κυμαίνονταν μεταξύ 5 και 15 μέτρων, τώρα είναι πιθανόν να ξεπεραστούν ακόμα και τα 150 μέτρα.

Στο Ινστιτούτο Τεχνολογίας της Georgia έχουν επίσης αναπτύξει και μια μέθοδο βασισμένη σε εικόνες που συλλαμβάνουν κάμερες και κατόπιν αναλύονται από υπολογιστή. Συγκεκριμένα, αξιοποιείται ειδικό λογισμικό ανάλυσης που

επεξεργάζεται ψηφιακές εικόνες και υπολογίζει στατικές παραμέτρους, όπως η απόσταση μεταξύ συγκεκριμένων σημείων του σώματος, αλλά και παραμέτρους βηματισμού των στόχων καθώς περπατάνε. Η τεχνική αυτή δεν αναλύει το δυναμικό πρότυπο βηματισμού, αλλά χρησιμοποιεί τις κινήσεις κάποιου καθώς περπατάει, προκειμένου να εξαγάγει συμπεράσματα για τις παραμέτρους του σώματος του στόχου. Όπως διακρίνουμε και από το σχήμα 1, το πρώτο σύνολο παραμέτρων σώματος που υπολογίζει αυτή η τεχνική, είναι τέσσερις συγκεκριμένες αποστάσεις.



Σχήμα 1. Οι τέσσερις αποστάσεις $d_1 - d_4$ είναι μοναδικές για κάθε άνθρωπο

Πιο αναλυτικά υπολογίζει το συνολικό ύψος του ατόμου (d_1), την απόσταση ανάμεσα στο κεφάλι και την λεκάνη (d_2), την απόσταση ανάμεσα στη λεκάνη και το κατώτερο σημείο του ποδιού (d_3), καθώς και την απόσταση ανάμεσα στο δεξί και αριστερό πόδι κατά το περπάτημα (d_4). Το δεύτερο σύνολο παραμέτρων, που αποτελεί υποσύνολο του πρώτου και είναι λιγότερο διακριτό, αλλά και λιγότερο ευάλωτο σε λάθος που μπορεί να προκύψει λόγω της απόκλισης των διαφορετικών καταστάσεων απεικόνισης της κίνησης, είναι οι αποστάσεις d_1 και d_3 . Οι αποστάσεις αυτές υπολογίζονται μόνο κατά το μέγιστο σημείο της φάσης του βηματισμού και συνυπολογίζονται προκειμένου να σχηματίσουν ένα τετραδιάστατο διάνυσμα βήματος $w=[d_1,d_2,d_3,d_4]$ και ένα διάνυσμα βήματος δύο διαστάσεων $s=[d_1,d_3]$ για κάθε στόχο. Οι ερευνητές που έχουν αναλάβει την υλοποίηση αυτών των προγραμμάτων, πιστεύουν ότι τα συστήματα αναγνώρισης βηματισμού δεν θα είναι εμπορικά διαθέσιμα τα αμέσως επόμενα χρόνια, μιας και απαιτείται ακόμα κάποιο διάστημα ερευνών προκειμένου να θεωρούνται αρκετά αξιόπιστα. Επίσης, υποστηρίζουν ότι μπορεί να μην αξιοποιηθούν ως αυτόνομα συστήματα, αλλά και να αποτελέσουν μέρος μιας συνολικής πλατφόρμας ασφαλείας, που θα ενσωματώνει και άλλες βιομετρικές τεχνολογίες, όπως για παράδειγμα αναγνώριση σχήματος προσώπου, παρέχοντας έτσι ένα πολυεπίπεδο και πρακτικό σύστημα ασφαλείας.

ΚΕΦΑΛΑΙΟ 8

ΕΦΑΡΜΟΓΕΣ
ΒΙΟΜΕΤΡΙΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ.....
ΠΑΡΟΝ & ΜΕΛΛΟΝ

ΕΦΑΡΜΟΓΕΣ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Όπως ήδη γνωρίζουμε, τα ανά τον κόσμο αστυνομικά σώματα χρησιμοποιούν εδώ και χρόνια τα δακτυλικά αποτυπώματα ως μέσο αναγνώρισης ταυτότητας. Το AFIS (Automated Fingerprint Identification System - Αυτοματοποιημένο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων) αποτελεί πλέον ένα από τα πιο χρήσιμα εργαλεία στα χέρια των ανθρώπων που είναι υπεύθυνοι για την επιβολή και την τήρηση του νόμου. Δεν είναι, λοιπόν, παράξενο το γεγονός ότι οι νεότερες βιομετρικές μέθοδοι βρίσκουν το μεγαλύτερο πεδίο εφαρμογής τους εκεί. Φυλακές, αστυνομικά τμήματα και κεντρικά γραφεία εξοπλίζονται με τα νέα συστήματα, συμβάλλοντας έτσι στην εξάλειψη ορισμένων παλαιών πρακτικών απόδρασης κρατουμένων (π.χ. ανταλλαγή θέσεων με κάποιον επισκέπτη) και ταυτόχρονα βοηθώντας τα μέγιστα στο έργο της αστυνόμευσης. Εκτός όμως από αυτές τις προφανείς εφαρμογές, οι βιομετρικές μέθοδοι τείνουν να μπου για τα καλά στην καθημερινή ζωή μας, και μάλιστα με πολλούς τρόπους.

8.1 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

Καθώς το ηλεκτρονικό εμπόριο αναπτύσσεται αφήνοντας πίσω τη νηπιακή ηλικία του, το πρόβλημα της ασφάλειας των εμπορικών συναλλαγών μέσω Internet γίνεται όλο και πιο έντονο. Η χρήση της πιστωτικής κάρτας για την αγορά κάποιου προϊόντος πάντα μας δημιουργεί σκεπτικισμό σχετικά με το πόσο ασφαλής είναι μια τέτοια συναλλαγή. Σε ένα σύστημα, όμως, όπου ο αριθμός της κάρτας θα συνοδευόταν από ένα βιομετρικό δείγμα του κατόχου της, τα πράγματα θα ήταν πολύ διαφορετικά. Φανταστείτε το εξής σενάριο: Εντοπίσατε επιτέλους το βιβλίο που ψάχνατε για μήνες, και πληκτρολογείτε τα στοιχεία σας και τον αριθμό της κάρτας σας στη φόρμα παραγγελίας. Καθώς πατάτε στο κουμπί "Submit", εμφανίζεται ένα μήνυμα που σας προτρέπει να απαγγείλετε μία συγκεκριμένη φράση ή λέξη στο μικρόφωνο του υπολογιστικού συστήματός σας. Καλύτερα να φροντίσετε να μην είστε βραχνιασμένοι, λοιπόν!

Η βιομετρική τοποθετείται ως λύση για το ηλεκτρονικό εμπόριο και την ασφάλεια Διαδικτύου, με σκοπό να εξασφαλίσει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε ευαίσθητα στοιχεία ή να εκτελούν συναλλαγές. Είτε επικυρώνοντας πελάτες είτε υπάλληλους είτε πολίτες, τα ιδρύματα πρέπει να εξετάσουν τους ακόλουθους παράγοντες:

- Παροχή συμβατότητας πέρα από τη σειρά των ασυμβίβαστων τεχνολογιών δακτυλικών αποτυπωμάτων που αναπτύσσεται στο επίπεδο των υπολογιστών γραφείου.
- Προσαρμογή ατόμων που δεν μπορούν να εγγραφούν ή να επικυρωθούν επιτυχώς, απαιτώντας διαδικασίες επιφύλαξης .
- Ενσωμάτωση των βιομετρικών αποφάσεων αντιστοιχιών στα συστήματα πληρωμής και εκκαθάρισης.
- Καθορισμός των απαιτήσεων ακρίβειας για τα βιομετρικά συστήματα
- Τοποθεσία των βιομετρικών αποθήκευσης και της επεξεργασίας στοιχείων για τη μέγιστη διαθεσιμότητα.
- Ενσωμάτωση των βιομετρικών διαδικασιών απόκτησης στις υπάρχουσες διεπαφές.
- Διοικητικό και λειτουργικό έλεγχο για να διαχειριστεί τους βιομετρικούς απολογισμούς και τις βιομετρικές συναλλαγές.
- Ασφαλή μετάδοση βιομετρικών πληροφοριών.

- Συμβατότητα με τους webserver των Windows και των Unix.
- Διαδικασίες για την επαλήθευση των αρχικών αξιώσεων ταυτότητας.
- Ενσωμάτωση της ανίχνευσης ίριδας , της αναγνώρισης φωνής, και άλλων βιομετρικών τεχνολογιών για πρόσβαση σε λογαριασμούς.

Η IBG έχει σχεδιάσει ιδιαίτερα γερές και εύκαμπτες λύσεις για το ηλεκτρονικό εμπόριο και την επικύρωση Διαδικτύου, που συνδυάζουν την ανεξαρτησία του προμηθευτή με μια πραγματική κατανόηση των απαιτήσεων ασφάλειας και απόδοσης. Η εργασία με IBG περιορίζει τους κινδύνους βαθμιαίας αχρήστευσης της τεχνολογίας, και εξασφαλίζει τη μακροπρόθεσμη βιωσιμότητα του ηλεκτρονικού εμπόριου και του Διαδικτύου.

Η IBG (INTERNATIONAL BIOMETRIC GROUP) είναι η κορυφαία εταιρία της βιομετρικής βιομηχανίας ασφάλειας και των υπηρεσιών τεχνολογίας. Από το 1996, η IBG παρέχει τεχνολογία και υπηρεσίες βιομετρικής ανεξάρτητες από τους προμηθευτές, τη στρατηγική, και τις λύσεις στους χρηματοδοτικούς οργανισμούς, τις κυβερνητικές αντιπροσωπείες, και τις εταιρίες υψηλής τεχνολογίας. Είναι ένας παγκόσμιος χορηγός των διασκέψεων βιομετρικής και των γεγονότων βιομηχανίας, που παρέχει βασικές διευθύνσεις και ειδικές παρουσιάσεις για τη μυστικότητα και την απόδοση των τάσεων της βιομηχανίας των βιομετρικών. Εξετάζει και αξιολογεί τις βιομετρικές τεχνολογίες, τους προμηθευτές, τις εφαρμογές, την απόδοση, και την μυστικότητα. Σχεδιάζει και ενσωματώνει πρότυπα βασισμένα σε βιομετρικές λύσεις για τον πολίτη, τον υπάλληλο, και την επικύρωση πελατών. Παρέχει στρατηγικές για την οικονομικώς αποδοτική ανάπτυξη προϊόντων και τέλος βοηθά τις κυβερνητικές αντιπροσωπείες και άλλες 500 επιχειρήσεις να ενσωματώσουν βιομετρικές τεχνολογίες ασφάλειας για να αυξήσουν την ασφάλεια, να μειώσουν τις δαπάνες, να μειώσουν την απάτη, και να αναπτύξουν νέα προϊόντα και υπηρεσίες.

8.2 ΑΣΦΑΛΕΙΑ ΣΕ ΔΙΚΤΥΑ

Δεδομένου ότι οι όλο και περισσότερο πολύτιμες πληροφορίες γίνονται προσιτές στους υπαλλήλους μέσω LAN και WAN, οι κίνδυνοι που συνδέονται με την αναρμόδια πρόσβαση στα ευαίσθητα στοιχεία γίνονται μεγαλύτεροι. Η προστασία του δικτύου σας με τους κωδικούς πρόσβασης είναι προβληματική, καθώς οι κωδικοί πρόσβασης, χάνονται εύκολα, ή μοιράζονται άπρεπα. Είτε για την ασφάλεια, την ευκολία, είτε για την μείωση του κόστους, η βιομετρική φαίνεται πως είναι μια αποτελεσματική λύση για την ασφάλεια των δικτύων. Σημαντικές προκλήσεις στην ανάπτυξη της βιομετρικής σε αυτό το περιβάλλον περιλαμβάνουν την ακρίβεια και την απόδοση, ενσωματώνοντας τις βιομετρικές αποφάσεις αντιστοιχιών με τα υπάρχοντα συστήματα και εξασφαλίζουν την αποθήκευση και τη διαβίβαση βιομετρικών στοιχείων.

Οι ικανότητες πυρήνων IBG στην ασφάλεια δικτύων περιλαμβάνουν τα εξής:

- Αξιολόγηση και δοκιμή των κύριων βιομετρικών λύσεων για την ασφάλεια δικτύων
- Ένταξη των βιομετρικών λύσεων σε νόμιμες εφαρμογές
- Εύκαμπτο ανεξάρτητο σχέδιο συστημάτων
- Εμμόνη στα αναδυόμενα βιομετρικά πρότυπα
- Ανάπτυξη εφαρμογής
- Πολλαπλάσια ολοκλήρωση συσκευών
- Κρυπτογράφηση των βιομετρικών στοιχείων
- Συγκεκριμένες δυνάμεις και αδυναμίες προμηθευτών

Με πάνω από 150 προμηθευτές που ανταγωνίζονται στη βιομετρική αγορά, η εμπειρία ολοκλήρωσης συστημάτων IBG εξασφαλίζει ότι θα πάρετε το σωστό συνδυασμό βιομετρικών υλικού, λογισμικού, και υλικολογισμικού για τις ανάγκες της επιχείρησή σας. Η IBG έχει την εμπράγματη εμπειρία με την τεχνολογία από κάθε κορυφαίο βιομετρικό προμηθευτή, και έχει εφαρμόσει τις λύσεις τις σε περιβάλλοντα δικτύων για παραπάνω από 500 πελάτες .

8.3 ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑ ΤΩΝ ΚΑΤΑΣΤΡΟΦΙΚΩΝ ΑΕΡΟΠΕΙΡΑΤΩΝ



Μέχρι πρότινος θεωρούσαμε ότι οι αεροπειρατές επεδίωκαν διαπραγματεύσεις. Τώρα πλέον ξέρουμε ότι μπορούν ακόμη και να δώσουν τέλος στη ζωή τους προκειμένου να μετατρέψουν ένα αεροσκάφος σε κατευθυνόμενο πύραυλο που θα σκοτώσει χιλιάδες ανθρώπους.

Τι μπορεί όμως να γίνει ώστε να εμποδίσει τους αυτοκαταστροφικούς αεροπειρατές να ολοκληρώσουν τα σχέδιά τους, εφ' όσον βρίσκονται ήδη στο αεροσκάφος;

Αποκλεισμός της πρόσβασης στο πιλοτήριο.

"Μια πιθανότητα που έχει εξεταστεί στο παρελθόν από αεροπορικές εταιρίες αφορά στο κλειδώμα και την ενίσχυση της πόρτας του πιλοτηρίου" αναφέρει ο David Villurpillai, αντιπρόσωπος της Airbus στην Toulouse. Στις ΗΠΑ, η "Ενωση Πιλότων (Air Line Pilots Association (ALPA)), ανάμεσα σε άλλα μέτρα, υποστηρίζει πλέον την ύπαρξη περισσότερο ανθεκτικών πόρτων στα πιλοτήρια.

Κάτι τέτοιο όμως δεν αναστέλλει τους αεροπειρατές από το να απειλούν τους επιβάτες ή το πλήρωμα του αεροσκάφους μέχρι να ανοιχτεί η πόρτα του πιλοτηρίου, όπως πιστεύεται ότι συνέβη την περασμένη εβδομάδα. "Ετσι μερικοί προτείνουν την ύπαρξη ενός διαχωριστικού τοιχώματος που θα αποκλείει μόνιμα την πρόσβαση από την καμπίνα του αεροσκάφους στο πιλοτήριο.

"Ένας αντίλογος σε αυτήν την ιδέα είναι ότι ένα αποκλεισμένο πιλοτήριο, απαγορεύει στο πλήρωμα να βοηθήσει τον πιλότο σε περίπτωση που αρρωστήσει ή αδυνατεί να εκπληρώσει τα καθήκοντά του. Επίσης, κάτι τέτοιο είναι ασύμφωνο με το ρόλο του πιλότου ως κυβερνήτη ολόκληρου του αεροσκάφους.

"Θα πρέπει να γίνουν αλλαγές όσον αφορά στο ρόλο των πιλότων" λέει η Elizabeth Verdier στο Boeing. "Είναι υπεύθυνοι για τις εξόδους σε περίπτωση κινδύνου, για την ασφάλεια και για την ασφαλή έξοδο κάθε επιβάτη από το αεροσκάφος".

Παρά τις αντιδράσεις αυτές η Ένωση Πιλότων (ALPA) παροτρύνει την έρευνα και την ανάπτυξη καλύτερων και ισχυρότερων πόρτων στα πιλοτήρια. Νέοι κανόνες πρέπει επίσης να υιοθετηθούν ώστε να εξασφαλιστεί ότι η πόρτα του πιλοτηρίου θα παραμένει κλειστή όσο φοβερές κι αν είναι οι απειλές των αεροπειρατών στην καμπίνα του αεροσκάφους.

Βιομετρικά Τεστ

Τι μπορεί να γίνει όμως για να εμποδίσει τους αεροπειρατές να πάρουν τον έλεγχο του αεροσκάφους στην περίπτωση που έχουν ήδη φτάσει στο πιλοτήριο;

Οι ελπίδες εναποτίθενται στις "βιομετρικές τεχνολογίες" που μπορούν να πιστοποιήσουν ότι ο άνθρωπος στο πιλοτήριο είναι ο πραγματικός πιλότος. Υπάρχει ήδη ή βρίσκεται υπό ανάπτυξη, μια ποικιλία ηλεκτρονικών συστημάτων ταυτοποίησης ενός ατόμου, βασιζόμενη σε μετρήσεις βιολογικών χαρακτηριστικών μοναδικών για κάθε άτομο: το πρόσωπο, την ίριδα, τα δακτυλικά αποτυπώματα, τη χροιά της φωνής ή ακόμα και τους χτύπους της καρδιάς.

Οι βιομετρήσεις χρησιμοποιούνται ήδη για την επιβεβαίωση της ταυτότητας ατόμων σε μονάδες πυρηνικής ενέργειας και σε κέντρα ασφαλών τραπεζικών συναλλαγών.

Δεν θα ήταν λογικό να χρησιμοποιηθούν παρόμοιες τεχνικές για την επιβεβαίωση της ταυτότητας του πιλότου; "Ειλικρινά όχι", λέει ο Villurillaί. "Θα απαιτούσε πολύ δουλειά" και συμπληρωματικά αναφέρει ότι θα ήταν καλύτερα να επενδυθούν χρήματα για να σταματήσουν να περνούν στα αεροσκάφη η τρομοκρατία, οι βομβιστικές ενέργειες και τα όπλα. Προσθέτει επίσης ότι οποιαδήποτε νέα συστήματα τοποθετηθούν στα πιλοτήρια, μπορεί να ενοχλούν τους πιλότους που απασχολούνται με πλήθος πραγμάτων κατά τη διάρκεια μιας πτήσης.

Μη ανιχνεύσιμοι ανιχνευτές

Υπάρχουν όμως μερικά νεοεμφανιζόμενα συστήματα που μπορεί να περνούν απαρατήρητα από τον πιλότο. Ένα νέο σύστημα αναγνώρισης των καρδιακών παλμών ελέγχει την ταυτότητα του ατόμου μέσω radar. Ο Gene Greneker και η ομάδα του στο Georgia Tech Research Institute στην Smyrna αναπτύσσουν αυτό το μη-παρεμβαλλόμενο βιομετρικό σύστημα που χρηματοδοτήθηκε από την Defense Advanced Research Projects Agency του Πενταγώνου.

Το σύστημα εκπέμπει ένα ραδιοφωνικό κύμα πολύ χαμηλής ενέργειας που ανακλάται από την καρδιά και χρησιμοποιεί το φαινόμενο Doppler για την ανίχνευση κινήσεων της τάξης μισού χιλιοστού, από τις οποίες δημιουργεί την "υπογραφή του καρδιακού παλμού του ατόμου".

"Έχουμε δημιουργήσει μια επιτραπέζια φορητή συσκευή. Όταν τίθεται σε λειτουργία, βλέπουμε τον παλμό του χτύπου της καρδιάς και μια μακροχρόνια "υπογραφή" της αναπνοής ενός ατόμου που βρίσκεται σε μικρή απόσταση" αναφέρει ο Greneker στο περιοδικό New Scientist. Ένα τέτοιο σύστημα μπορεί να αναφέρει αυτόματα ότι το άτομο είναι εν ζωή - ένας παράγοντας κλειδί που όλα τα βιομετρικά συστήματα επιδιώκουν να λαμβάνουν υπ' όψιν, λέει ο John Woodward,

αναλυτής της γνωστής RAND research organisation, με έδρα κοντά στο Πεντάγωνο στο Arlington της Virginia.

Οποιαδήποτε μορφή νέας τεχνολογίας - ειδικά αυτή που περιλαμβάνει εισαγωγή ραδιοκυμάτων στο πιλοτήριο - θα πρέπει να αποδειχθεί ότι είναι ασφαλής και ρυθμιζόμενη από την Διοίκηση Ομοσπονδιακής Αεροπορίας των ΗΠΑ (US Federal Aviation Administration) και τους συμβαλλόμενους φορείς σε άλλα μέρη. Μέχρι στιγμής η FAA δεν έχει αναφερθεί σε νέα σχέδια ασφάλειας.

Αυτόματος Πιλότος

Τι μπορεί να γίνει για να αποσπαστεί ο έλεγχος του αεροσκάφους από τα άτομα στο πιλοτήριο - που έχουν εξουδετερώσει τους πιλότους και / ή δεν έχουν έλεγχο του αεροσκάφους; Μία λύση είναι να διευρυνθούν οι ικανότητες αυτόματης προσγείωσης του αεροσκάφους.

Υπάρχουν ήδη τεχνικές δυνατότητες ελέγχου και προσγείωσης ενός αεροσκάφους χωρίς τον πιλότο. Ένα τέτοιο σύστημα μπορεί να ενεργοποιηθεί από τον έλεγχο εναέριας κυκλοφορίας, τον πιλότο ή ένα βιομετρικό συναγερμό και να προσγειώσει το αεροπλάνο με ασφάλεια στο κοντινότερο αεροδρόμιο, σε περίπτωση ανάγκης. Τέτοια συστήματα όμως δημιουργούν τόσα προβλήματα, όσα και αυτά που λύνουν, και η χρήση τους είχε αποκλειστεί στο παρελθόν. Τόσο οι πιλότοι όσο και οι επιβάτες έχουν υπάρξει δύσπιστοι όσον αφορά στην παράδοση του ελέγχου του αεροσκάφους σε έναν υπολογιστή κάτω από οποιεσδήποτε συνθήκες.

Επίσης υπάρχει το πρόβλημα της αυτόματης πτήσης σε ελεγχόμενο εναέριο χώρο, όπου όλα τα υπόλοιπα αεροσκάφη υπακούουν σε οδηγίες από τους ελεγκτές εναέριας κυκλοφορίας. Και φυσικά υπάρχει ο κίνδυνος παύσης ή εμπλοκών στη λειτουργία του συστήματος.

8.4 ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΔΟΚΙΜΑΖΟΝΤΑΙ ΣΤΗΝ ΕΥΡΩΠΗ

Το τρομοκρατικό χτύπημα στη Νέα Υόρκη προ διετίας έδωσε το έναυσμα για ενίσχυση των μέτρων ασφαλείας στη διακίνηση επιβατών στα αεροδρόμια. Το ζήτημα αυτό ενδιαφέρει πολύ περισσότερο τη χώρα μας που είναι τουριστικός προορισμός, αλλά και εξ αιτίας των επικείμενων Ολυμπιακών Αγώνων σε κάμποσους μήνες από τώρα.

Οι προσπάθειες εστιάζονται σε βιομετρικές μεθόδους με την βοήθεια ιδιαίτερας εξελιγμένης τεχνολογίας. Τα βασικότερα συστήματα τοποθετούν ως στοιχείο αναγνώρισης την όψη, το πρόσωπο του επιβάτη, άλλα τα δακτυλικά αποτυπώματα και άλλα την ίριδα των ματιών.

Στις ΗΠΑ έχουμε ήδη σημαντική εξέλιξη στην κατεύθυνση αυτή. Αυτό το γεγονός δεν μπορεί να αγνοηθεί από τη χώρα μας, αλλά και ολόκληρη την Ευρώπη, αφού το αργότερο μέχρι τον Οκτώβριο του 2004, εκείνος που επιθυμεί να ταξιδέψει στις ΗΠΑ θα πρέπει να διαθέτει και να επιδεικνύει Ταξιδιωτικό Διαβατήριο με βιομετρικά χαρακτηριστικά. Σε αντίθετη περίπτωση θα επανέλθει η υποχρέωση της Βίζας. Ακόμη, όμως, και στην τελευταία αυτή περίπτωση της Βίζας, οι ταξιδεύοντες στις

ΗΠΑ θα κληθούν να εξοικειωθούν με τις νέες μεθόδους αναγνώρισης που οι αρμόδιες αρχές θεσμοθετούν με ισχύ από την 1η Ιανουαρίου 2004. Έτσι λοιπόν από αυτή τη χρονική στιγμή και εφ' εξής όλοι οι εισερχόμενοι στις ΗΠΑ από αεροδρόμια και λιμάνια θα φωτογραφίζονται και θα δίνουν τα δακτυλικά των αποτυπώματα. Όλα αυτά τα στοιχεία θα προωθούνται σε μία κεντρική τράπεζα δεδομένων και θα συγκρίνονται με αυτά των διαφόρων καταζητούμενων, τρομοκρατών κλπ. Οι πληροφορίες θα είναι στη διάθεση του FBI και άλλων αρμόδιων αρχών ασφαλείας.

Στην Ευρώπη, που ως συνήθως, ακολουθεί την Αμερική, παρατηρείται τελευταία μία κινητικότητα προς την κατεύθυνση αυτή. Ως πρωτοπόροι εμφανίζονται οι Ολλανδοί οι οποίοι ήδη από το τέλος του 2001 εγκατέστησαν στο αεροδρόμιο του Άμστερνταμ ένα σύστημα αναγνώρισης της ίριδος των ματιών. Αξιοπρόσεκτος είναι και ο τρόπος εισαγωγής του συστήματος. Δεν προχώρησαν με μέτρα εξαναγκασμού, αλλά πρόβαλαν το μέτρο σαν ειδικό πλεονέκτημα υπέρ αυτών που ταξιδεύουν συχνά. Στους συγκεκριμένους πολυ-ταξιδευτές παρέχεται η δυνατότητα έναντι ενός σχετικά μικρού τέλους περίπου 100 Ευρώ, να αποκτήσουν το λεγόμενο «Prinium Pass» με βάση το οποίο, ο κάτοχός του, απαλλάσσεται από την υποχρέωση αναμονής σε μεγάλες ουρές ελέγχου των εισερχομένων στη χώρα επιβατών, αλλά έχουν τη δυνατότητα να περάσουν χωρίς καμία χρονοτριβή σε παρακείμενη δίοδο ελέγχου της ίριδος των ματιών. Εδώ αντιπαραβάλλεται η βιομετρικά πιστοποιούμενη ίρις των οφθαλμών με τα αντίστοιχα δεδομένα του ειδικού διαβατηρίου και εφ' όσον αυτά συμφωνούν, ανοίγει αυτομάτως η δίοδος.

Ανάλογες πρωτοβουλίες προγραμματίζει η σκανδιναβική SAS από τον επόμενο Νοέμβριο, ενώ ο Γερμανός Ομοσπονδιακός Υπουργός Εσωτερικών Otto Schily ανακοίνωσε πρόσφατα στο Βερολίνο να εγκαταστήσει η Ομοσπονδιακή κυβέρνηση σε συνεργασία με την Lufthansa για ένα δοκιμαστικό εξάμηνο στο αεροδρόμιο της Φρανκφούρτης, ένα αντίστοιχο σύστημα πιστοποίησης της ταυτότητας των ταξιδιωτών με βάση την ίριδα των ματιών. Δεν είναι λίγοι αυτοί που ασχολούνται με το ζήτημα και ήδη παρατηρούν ότι η αποδοχή των νέων μεθόδων από τους ταξιδιώτες αναδεικνύεται σε μείζονα δυσκολία σε σχέση προς την τεχνολογία, η οποία ομολογουμένως είναι κατ' εξοχήν προηγμένη.

Στη χώρα μας δεν φαίνεται ότι το ζήτημα αυτό έχει λάβει την προσήκουσα δημοσιότητα και πολύ περισσότερο εκτιμάται ότι οι τουριστικές επιχειρήσεις που διακινούν τους ταξιδιώτες, δεν προετοιμάζονται για τις επικείμενες αλλαγές. Είναι χαρακτηριστικό ότι μέχρι το τέλος του έτους 2003 και στα πλαίσια καταπολέμησης της τρομοκρατίας πρόκειται να διαμορφωθεί μία συμφωνία πλαίσιο μεταξύ των Η.Π.Α και της Ε.Ε με βάση την οποία θα ανταλλάσσονται και θα αξιολογούνται στοιχεία διακίνησης επιβατών.

8.5 Η "ΠΡΩΤΗ ΓΡΑΜΜΗ"

Η εξέλιξη των τεχνολογιών της Πληροφορικής στο άνοιγμα του 21ου αιώνα διαμορφώνει αυτό που ονομάζουμε "Κοινωνία της Πληροφορίας". Σε αυτό το περιβάλλον της Υψηλής Τεχνολογίας, η διακίνηση των "πληροφοριών" από και προς οποιοδήποτε σημείο και ανά πάσα στιγμή, επιβάλλει την αξιόπιστη και εύκολη κτήση των πληροφοριών στην "Πρώτη Γραμμή", εκεί δηλαδή όπου η κάθε πληροφορία γεννιέται. Δηλαδή, στο ταμείο, στο κατάστημα, στην αποθήκη, στο εργοστάσιο, στο γραφείο, στο δρόμο και σε χιλιάδες άλλα σημεία της σύγχρονης μας ζωής.

Η ευκολία και η αξιοπιστία της κτήσης των στοιχείων από την "Πρώτη Γραμμή" αποτελεί την υπεραξία και την συμβολή των Τεχνολογιών της Αυτόματης Αναγνώρισης Στοιχείων & Κτήσης Δεδομένων (Automatic Identification & Data Capture Technologies-AIDC). Ο τομέας των τεχνολογιών AIDC ανθεί διεθνώς με αξιόλογους ρυθμούς ανάπτυξης (18-20% ετησίως) που οφείλονται τόσο στην γενικότερη διάδοση της Πληροφορικής, του Διαδικτύου και των Επικοινωνιών (ενσύρματων & ασύρματων) αλλά και στην εδραίωση του e- & m-commerce, του "ηλεκτρονικού e-πιχειρείν" γενικότερα και των κινητών επικοινωνιών της νέας γενιάς (GPRS, 3G, Wi-Fi κ.ά.).

Η εταιρεία Η Datalex A.E. εξειδικεύεται από το 1984 στις Πληροφοριακές Λύσεις της "Πρώτης Γραμμής" (Frontline Solutions), οι οποίες χρησιμοποιούν μια ή περισσότερες από τις Τεχνολογίες της Αυτόματης Αναγνώρισης Στοιχείων και Κτήσης Δεδομένων [Automatic Identification & Data Capture Technologies-AIDC].

Οι τεχνολογίες AIDC περιλαμβάνουν:

- Γραμμωτό Κώδικα [Bar Code]
- Μαγνητική Λωρίδα [Magnetic Stripe]
- Οπτική Αναγνώριση Χαρακτήρων [OCR] και Σημείων [OMR]
- Αναγνώριση Ασύρματης Συχνότητας [Radio Frequency Identification - RFID]
- Αναγνώριση Φωνής & Εικόνας [Voice & Vision Identification]
- Βιομετρικά Συστήματα Αναγνώρισης [Biometrics], όπως δακτυλικό αποτύπωμα, ίριδα, πρόσωπο, παλάμη, κ.λπ.
- Έξυπνες Κάρτες [Smart Cards] και Proximity
- Radio Frequency Data Capture [RF/DC], κ.α.

καθώς και κάθε είδους Συστήματα Κτήσης Στοιχείων με Φορητά Τερματικά, ενσύρματα ή ασύρματα [Batch ή RF].

Το προφίλ και η φιλοσοφία της Datalex είναι πελατοκεντρικά και συνοψίζονται σε δύο slogan: "Κοντά στον Πελάτη!" και "...Από το 1984 τηρούμε πιστά τους κώδικες!". Η πολυετής δραστηριότητα στον συγκεκριμένο τομέα των τεχνολογιών AIDC με ευθύνη και συνέπεια, παρέχοντας ολοκληρωμένες λύσεις σε μια πληθώρα Κλάδων της Αγοράς, μεταφράζεται σε συμπυκνωμένη τεχνογνωσία, με έμπειρο και αφοσιωμένο προσωπικό που δρα σαν ομάδα. Ως εκ τούτου η εταιρεία έχει επιτύχει μια εκτεταμένη αναγνώριση και καταξίωση στην αγορά. Το ανεπτυγμένο αριθμητικά (800 ενεργοί πελάτες κατά την χρήση του 2003) και ποιοτικό πελατολόγιο το οποίο παραμένει κατά ένα μεγάλο ποσοστό σταθερό, προσθέτει αξία στην καλή φήμη (Goodwill) της εταιρείας.

Πρωτεύων στόχος της εταιρείας είναι η απόλυτη δέσμευση και η βέλτιστη παροχή υπηρεσιών προς τους πελάτες μας, εγγυώντας για την καλύτερη ποιοτική υποστήριξη και συμβουλή πριν την πώληση, την άμεση παράδοση ή / και εγκατάσταση κατά την πώληση και την έγκαιρη και άμεση υποστήριξη μετά την πώληση. Με άλλα λόγια, επιδιώκουμε την πλήρη ικανοποίηση των αναγκών του Πελάτη!

Το προφίλ είναι αυτό του «Διανομέα Προστιθέμενης Αξίας ή Value Added Distributor-VAD».

Σκοπός της να παρέχει ποιοτικές και αξιόπιστες λύσεις AIDC από κορυφαίους κατασκευαστές του κλάδου και να εκτελεί τις παραγγελίες των κύριων προϊόντων εντός 24 ωρών!

Οι δραστηριότητες της Datalex, κάνοντας χρήση των τεχνολογιών AIDC καλύπτουν ένα μεγάλο εύρος εφαρμογών σε τομείς, όπως Τράπεζες, Εμπόριο & e-Commerce, Βιομηχανία, Μεταφορές, Ακτοπλοΐα, Υγεία, Ξενοδοχεία, Δημόσιους Οργανισμούς, Αυτοματισμός Γραφείου και πολλές άλλες.

ΔΟΜΗ ΤΗΣ ΕΤΑΙΡΕΙΑΣ

Η δομή της Εταιρείας αποτελείται από:

- Εμπορικό Τμήμα εξειδικευμένο στις Τεχνολογίες AIDC που απευθύνεται προς το Πανελλαδικό δίκτυο συνεργατών μεταπώλησης υιοθετώντας ένα νέο μοντέλο προσέγγισης της αγοράς βασισμένο σε λύσεις προς τρεις κύριους πυλώνες: Retail & Distribution, Transportation & Logistics και Industry. Σκοπός του τμήματος είναι η απόλυτη υποστήριξη των συνεργατών μας. Γι' αυτό το ονομάζουμε (S + I)². Δηλαδή η Datalex ενεργεί σαν "Ο System Integrator τεχνολογιών AIDC για τους System Integrators συνεργάτες μας!".
- Projects & OEM που εστιάζει στην ανάπτυξη και υποστήριξη μεγάλων έργων του Δημοσίου ή Ιδιωτικού τομέα με χρήση τεχνολογιών AIDC.
- Cards & More που προωθεί λύσεις με χρήση έγχρωμων Πλαστικών καρτών.
- R & D, ή αλλιώς Τμήμα Έρευνας & Ανάπτυξης εξειδικευμένου Software για ενσύρματες ή ασύρματες λύσεις Φορητών Τερματικών, άλλες εφαρμογές AIDC, Συνολικές λύσεις, System Integration, κ.ά.
- Τεχνική Υποστήριξη σε hardware & software πριν-κατά-μετά την πώληση.

Εφαρμογές και Δραστηριότητες

- In-Store Εφαρμογές: EPOS (Ηλεκτρονικά Σημεία Πώλησης), Απογραφή, Παραγγελιοδοσία, Συστήματα Self-Scanning, Έλεγχος τιμών κ.ά., χρησιμοποιώντας τις τεχνολογίες AIDC.
- Αποθήκη: Logistics/Συστήματα Διαχείρισης Αποθήκης (WMS), χρησιμοποιώντας Φορητά Τερματικά χειρός ή περονοφόρων είτε ενσύρματα, είτε ασύρματα με τεχνολογίες RF.
- Μεταφορές: Αποθήκες, Κέντρα Διανομής, Εταιρείες Courier, Ταχυδρομεία, Ακτοπλοϊκές Εταιρείες, Ταμείο Εθνικών Οδών (TEO) - Διόδια κ.ά., χρησιμοποιώντας Αναγνώστες Χειρός (Hand Held Readers), Βιομηχανικά Συστήματα Ανάγνωσης (Unattended Scanning Systems), Φορητά Τερματικά, m-Computers, κ.ά.
- Λύσεις Διακίνησης Υλικών: Κέντρα Διανομής & Διαλογής, Εφοδιαστικές Αλυσίδες, Κινητή Τιμολόγηση επί Αυτοκινήτου & m-Computing εφαρμογές, χρησιμοποιώντας Συστήματα Σταθερής & Φορητής Συλλογής Δεδομένων.

- Shop Floor: Αυτοματισμός Εργοστασίων χρησιμοποιώντας Βιομηχανικά Συστήματα Αναγνώρισης, Βιομηχανικά Τερματικά, Φωτοκύτταρα, Ρυθμιστές Θερμοκρασίας, Φράγματα Ασφαλείας μηχανολογικού εξοπλισμού (Safety Barriers), κ.ά.
- Εκτύπωση Γραμμωτού Κώδικα (Bar Code) Σε απλές ή/και "έξυπνες" ετικέτες, κοινές ή θερμικές χάρτινες, nylon ή μεταλλικές, εισιτηρίων Ακτοπλοΐας, θεαμάτων, αθλητικών αγώνων, κλάδου ένδυσης, κουπονιών, κ.ά., σε μεγάλη ποικιλία μεγεθών, χρωμάτων και υλικών.
- Εκτύπωση Πλαστικών Καρτών (μονόχρωμη / έγχρωμη): Ενσωματώνοντας τεχνολογίες όπως Γραμμωτό Κώδικα, Μαγνητική Λωρίδα, Έξυπνη, Εξ' επαφής & Εξ' αποστάσεως, Proximity κ.ά., για την υλοποίηση προγραμμάτων "Loyalty", Membership, εκπαιδευτικές, πιστωτικές, προσωπικού, προσπέλασης, υγείας, ασφάλισης, διαπίστευσης, εφαρμογές προσωποποιημένων πλαστικών καρτών, κ.ά.
- Προσπέλαση, Ωρομέτρηση και Ασφάλεια: Χρησιμοποιώντας Συστήματα Παρουσίας Προσωπικού και Πρόσβασης Εισόδου (Time & Attendance, Access Control).
- Η Datalex λανσάρει την ολοκληρωμένη λύση Διαπίστευσης Ασφαλείας με φορητότητα, e-SCAN (electronic Secure Control Accreditation) η οποία παρέχεται με πολλαπλές παραμετροποιήσεις, επίπεδα ασφαλείας και επιλογή τεχνολογιών Αυτόματης Αναγνώρισης (Bar Code, Magnetic, smart card), επί των καρτών, σε συνδυασμό με Φορητούς Υπολογιστές - Portable Data Computers (batch ή Ασύρματους - RF με ενσωματωμένο ή μη βιομετρικό αναγνώστη), δεμένα αρμονικά με το απαραίτητο εξειδικευμένο λογισμικό. Το σύστημα e-SCAN επιτρέπει την αποτελεσματική, φορητή, ασφαλή εφαρμογή διαπιστεύσεων σε κορυφαίες αθλητικές διοργανώσεις (Ολυμπιακοί Αγώνες), Συνέδρια, Στρατιωτικές εγκαταστάσεις, Αεροδρόμια, Λιμάνια & Μαρίνες, Υπουργεία και δημόσια κτίρια, Γραφεία και Βιομηχανικές εγκαταστάσεις.

Αντιπροσωπείες - Διεθνείς Συνεργασίες

Για την επίτευξη του σκοπού της η, Datalex αντιπροσωπεύει και συνεργάζεται σταθερά με διεθνείς, καταξιωμένες και ποιοτικές εταιρείες (διαπιστευμένες με ISO9000-9001) που κατέχουν ηγετική θέση στον κλάδο των τεχνολογιών Auto Id industry, όπως:

- Datalogic S.p.A. (www.datalogic.com)

Η μεγαλύτερη Ευρωπαϊκή εταιρεία αναγνώστων χειρός - Hand Held Readers (CCD & Laser Bar Code Systems), φορητών τερματικών χειρός- Portable Data Computers (πολλές επιλογές από CCD & Laser Hand Held Terminals, Unattended Scanning Systems (Industrial Scanners, Controllers, Vision Systems κ.λπ.), συστήματα αυτοεξυπηρέτησης ταμείων - Retail Self-Scanning Systems κ.λπ.

- Scantech-ID B.V. (www.sacantech-id.com)
- P.O.S. Scanners & Customer Information Systems
- Datamax Corporation (www.datamaxcorp.com)
- Zebra Technologies (www.zebra.com)
- Carl Valentin G.m.b.H. (www.Valentin-carl.de)

Κορυφαίες εταιρίες με ολοκληρωμένες λύσεις για εκτυπωτές ετικετών, εισιτηρίων, υφασμάτινες κ.λπ. Καλύπτονται τεχνολογίες εκτύπωσης Thermal & Thermal Transfer με εκτυπωτικά κατηγοριών Industrial, Desktop & Mobile Printers συμπεριλαμβανομένων όλων των αναλωσίμων (ετικέτες, μελανοταινίες, ΚΙΤ καθαρισμού κεφαλών κ.λπ.).

- Zebra Plastic Card Printer Solutions (www.zebracards.com)

Κορυφαίος κατασκευαστής εκτυπωτών εγχρώμων Πλαστικών Καρτών & Αναλωσίμων (πρώην Eltron Cards), που αποτελεί τμήμα της Zebra Technologies Corp.

- Sogedex S.A. (www.sogedex.fr)

Αποτελεί τον "One-Stop-Shop" συνεργάτη όσο αφορά τα αξεσουάρ των πλαστικών καρτών (clips, lanyards, pouches, bracelets, consumables and more)

- Datasensor S.p.A. (www.datasensor.com)

Από τους μεγάλους και καινοτόμους προμηθευτές Βιομηχανικών Αυτοματισμών όπως Φωτοκτύπαρα, Ρυθμιστές Θερμοκρασίας, συστήματα Βιομηχανικής Προστασίας με φωτοκουρτίνες, έξυπνους αισθητήρες κ.λπ.

- Escort Memory Systems-EMS RFID (www.ems-rfid.com)

Η EMS, θυγατρική της Datalogic, με έδρα την Silicon Valley της California, ΗΠΑ, διεκδικεί ηγετικό ρόλο στην ανερχόμενη αγορά με τεχνολογίες «Ραδιοσηματικής Αναγνώρισης» - Radio Frequency Identification Systems (RFID).

- Jarltech B.V. (www.Jarltech.com)

Για συμπληρωματικές εφαρμογές των Bar Codes, Magnetic & Smart Card Readers, POS keyboards κλπ.

8.6 BARCODE : Η ΤΕΧΝΟΛΟΓΙΑ ΤΟΥ ΓΡΑΜΜΩΤΟΥ ΚΩΔΙΚΑ ΣΤΗΝ ΥΠΗΡΕΣΙΑ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ



"Ο γραμμωτός κώδικας (barcode) είναι γνωστός σε όλους κυρίως από την παρουσία του στην πλειονότητα των συσκευασμένων προϊόντων, σε βιβλία, περιοδικά, εφημερίδες, κάρτες κ.λπ. Στο κείμενο που ακολουθεί μπορείτε να μάθετε περισσότερες πληροφορίες για τις υπηρεσίες που προσφέρει καθώς και για κάποιες από τις εταιρίες που πρωταγωνιστούν στο εγχώριο επιχειρηματικό πεδίο εφαρμογής του."

Ο γραμμωτός (ή γραμμικός) κώδικας αποτελεί μία από τις πολλές εφαρμογές που ανήκουν στην κατηγορία των τεχνολογιών AIDC (Automatic Identification and Data Capture ή επί το ελληνικότερων, Αυτόματη Αναγνώριση Στοιχείων και Κτήση

Δεδομένων), που επιτρέπουν τη γρήγορη και εύκολη λήψη και αποθήκευση της πληροφορίας τη στιγμή που αυτή δημιουργείται. Στις τεχνολογίες AIDC εντάσσονται επίσης η Μαγνητική Λωρίδα (Magnetic Stripe), η Αναγνώριση Ασύρματης Συχνότητας (Radio Frequency Identification - RFID), η Αναγνώριση Φωνής και Εικόνας (Voice and Vision Identification), τα βιομετρικά συστήματα αναγνώρισης (Biometrics), οι έξυπνες κάρτες (smart cards) και άλλες, λιγότερο γνωστές στο ευρύ κοινό, εφαρμογές.

Στις ΗΠΑ η πρώτη εφαρμογή του

Ο barcode εμφανίστηκε και εφαρμόστηκε πρώτα στις Ηνωμένες Πολιτείες, στα τέλη της δεκαετίας του '60, προκειμένου να καλύψει τις ανάγκες των εκεί σούπερ μάρκετ για γρηγορότερη διακίνηση ("πέρασμα") των αγαθών από τα ταμεία. Ως γνωστόν, στην προ barcode εποχή, οι ταμίες ήταν αναγκασμένοι να πληκτρολογούν στην ταμειακή μηχανή την τιμή του κάθε προϊόντος που επρόκειτο να αγοραστεί από τον πελάτη, με αποτέλεσμα τη δημιουργία ουρών, σφαλμάτων και τη δαπάνη πολύτιμου χρόνου. Το πρώτο σύστημα barcode εκείνης της όχι και τόσο μακρινής εποχής περιοριζόταν στο "χτύπημα" των προϊόντων και δεν επέτρεπε λειτουργίες όπως η αυτόματη ενημέρωση των αποθεμάτων κάθε φορά που ένα προϊόν αγοραζόταν. Στη συνέχεια, η σχετική τεχνολογία αναβαθμίστηκε και ξέφυγε από τα στενά όρια της ταμειακής καταγραφής των εξερχόμενων προϊόντων, καθώς επεκτάθηκε στην καταγραφή και των εισερχόμενων αγαθών, στην απογραφή, στον έλεγχο των αποθεμάτων κ.λπ. Η Ελλάδα εισήλθε στον... κόσμο του barcode στα τέλη της δεκαετίας του '80, γεγονός που συνδυάστηκε με τον πολλαπλασιασμό των πολυκαταστημάτων και σούπερ μάρκετ.

Αυτόματη μεταβίβαση δεδομένων

Η βασική ιδέα που διέπει τη συγκεκριμένη τεχνολογία θα μπορούσε να συνοψιστεί στο εξής: Τοποθετείται μια σειρά πληροφοριών σε ένα προϊόν με τρόπο που ειδικά μηχανήματα μπορούν να τη "διαβάσουν" αυτόματα και να τη μεταβιβάσουν σε κεντρικό υπολογιστικό σύστημα, ώστε το προϊόν να είναι αναγνωρίσιμο. Η μεταφορά των δεδομένων από τα ειδικά μηχανήματα ανάγνωσης (scanners, ανιχνευτές κ.λπ.) σε υπολογιστή μπορεί να γίνει είτε ενσύρματα είτε ασύρματα. Ο δεύτερος τρόπος, που κερδίζει συνεχώς έδαφος και αποτελεί ό,τι πιο εξελιγμένο, υποστηρίζεται από ασύρματα δίκτυα τοπικής εμβέλειας (Wireless Local Area Networks - WLAN) μέσα στα οποία μπορεί να γίνει, χωρίς καλώδια, μετάδοση δεδομένων από ένα φορητό τερματικό σε έναν υπολογιστή λ.χ., και από εκεί οπουδήποτε, ακόμα και στο Internet. Σήμερα οι barcodes είναι παντού, υποκαθιστούν τη χειρόγραφη εισαγωγή ή πληκτρολόγηση της πληροφορίας σε κάποιο σύστημα και ταυτόχρονα "απογειώνουν" τα δεδομένα σε ψηφιακές λεωφόρους υψηλής ταχύτητας και αξιόπιστης διαχείρισης.

Πώς λειτουργεί η τεχνολογία του barcode



Τι είναι όμως και πώς λειτουργεί ο γραμμωτός κώδικας; Κατ' αρχάς, στην πιο συνήθη του μορφή συνίσταται από μια διαδοχή μαύρων και λευκών λωρίδων (bars) τυπωμένων πάνω σε κάποιο προϊόν / συσκευασία. Ανάμεσα στις λωρίδες παρεμβάλλονται κενά διαστήματα ποικίλου μεγέθους. Η σχεδίαση, εκτύπωση και απεικόνιση των λωρίδων ακολουθούν συγκεκριμένους κανόνες και κάθε αλληλουχία λωρίδων αντιστοιχεί αμφιμονοσήμαντα σε κάποιον αριθμό. Αυτό στην πράξη σημαίνει ότι οι αριθμοί μπορούν να συμβολίζονται από διαφορετική κάθε φορά αλληλουχία λωρίδων: άλλοτε μία μαύρη λεπτή λωρίδα μαζί με μία λευκή παχιά λωρίδα μπορούν να αντιστοιχούν στον αριθμό 6, άλλοτε συμβαίνει ο ίδιος συνδυασμός να αντιστοιχεί στον αριθμό 8 κ.ο.κ. Ο πιο κοινός τύπος γραμμωτού κώδικα είναι ο EAN (European Article Numbering), ο οποίος αποτελείται από αριθμοσειρά 13 ψηφίων και απαντάται στα περισσότερα καταναλωτικά είδη.

Ωστόσο, υπάρχουν και άλλοι τύποι barcode με περισσότερα ή και λιγότερα ψηφία από τα 13 του προτύπου EAN, τα οποία βρίσκουν εφαρμογή σε εξειδικευμένους επιχειρηματικούς κλάδους, όπως π.χ. στη σιδηροδρομική βιομηχανία.

Η ανάγνωση του barcode συντελείται ως εξής: ο κωδικός EAN μεταφράζεται μέσα σε κλάσματα δευτερολέπτου από κάποιο scanner σε γλώσσα Η/Υ (δηλ. 0, 1 - δυαδικό σύστημα). Η ανάγνωση του barcode συνίσταται στην αποκωδικοποίηση της ανάκλασης μιας δέσμης ακτινών laser που "πέφτει" πάνω στην ετικέτα barcode. Ο βαθμός ανάκλασης είναι μεταβλητός (άρα ξεχωριστός για κάθε προϊόν) γιατί η δέση laser συναντά διαδοχικά τις λευκές και μαύρες λωρίδες. Τα scanners αποκωδικοποιούν τη μεταβλητή ανάκλαση (σήμα) και τη μετατρέπουν σε αριθμούς ή γράμματα, τα οποία ταυτίζονται ως προς το περιεχόμενο με τους χαρακτήρες που κωδικοποιήθηκαν με μορφή barcode. Έτσι, όταν ένα προϊόν περνά από το ταμείο λαμβάνει χώρα η εξής διαδικασία: αναγνώριση, ανάγνωση, μετάφραση και αποθήκευση, που σημαίνεται από το χαρακτηριστικό "μπιπ" που ακούγεται κάθε φορά που η ταμίας χρησιμοποιεί το scanner. Τη συγκεκριμένη στιγμή ανιχνεύεται το είδος από τη βάση δεδομένων και διατίθενται για εκτύπωση τα επιμέρους προσδιοριστικά στοιχεία του, όπως η περιγραφή του προϊόντος, η τιμή πώλησής του, η ποσότητα κ.λπ., στοιχεία που καταγράφονται στην ταμειακή μηχανή. Συγχρόνως, αφαιρείται το προϊόν από τη βάση δεδομένων της αποθήκης και των αποθεμάτων.

Βασικά πλεονεκτήματα

Γιατί θα πρέπει μια εταιρία να εμπιστευθεί μέρος των δραστηριοτήτων της στην εν λόγω τεχνολογική υποδομή; Ο Μιχάλης Λάμπρου, γενικός διευθυντής της Halos, απαντά προσδιορίζοντας τις ωφέλειες που απορρέουν από τη χρήση τέτοιων εφαρμογών:

- Συνεχής παρακολούθηση των μετακινήσεων των αντικειμένων στις διάφορες φάσεις της εφοδιαστικής αλυσίδας
- Γνώση της θέσης τους ανά πάσα χρονική στιγμή
- Μείωση του χρόνου συλλογής πληροφοριών, γεγονός που συνεπάγεται αύξηση της ταχύτητας διέλευσης των αντικειμένων

- Ακριβής πληροφόρηση, καθώς εκλείπουν τελείως τα λάθη αντιγραφής και πληκτρολόγησης
- Αύξηση του βαθμού λεπτομέρειας της πληροφορίας
- Άμεση μεταβίβαση (real time) της πληροφορίας, εάν αυτό απαιτείται
- Αυτοματοποίηση αναφορών (reporting)

Ο Βύρων Ρηγινός, διευθύνων σύμβουλος της Datalex, προσθέτει: "Σε όλα τα στάδια της πορείας ενός προϊόντος, από την αποθήκευση έως την παραγγελία, την τιμολόγηση και την πώληση, προκύπτουν ουσιαστικά οικονομικά οφέλη μέσα από την καλή οργάνωση και λειτουργία, τόσο για τις συνεργαζόμενες επιχειρήσεις (προμηθευτές, αγοραστές) όσο και για τον τελικό πελάτη, δηλαδή όλους εμάς τους καταναλωτές που βρίσκουμε πάντα αυτό που θέλουμε στο ράφι, στην καλύτερη δυνατή τιμή, και δεν περιμένουμε σε ατελείωτες ουρές στο ταμείο". Κοντολογίς, ο συνδυασμός τεχνολογιών, όπως είναι ο barcode, τα ασύρματα τοπικά δίκτυα και τα φορητά τερματικά, προσφέρει μόνον οφέλη για μια επιχείρηση: μείωση του συνολικού χρόνου συναλλαγής, ποιοτικότερη και ταχύτερη εξυπηρέτηση πελατών, αύξηση του ωφέλιμου χρόνου προώθησης νέων προϊόντων, συνολική αύξηση της παραγωγικότητας ως αποτέλεσμα της καλύτερης αξιοποίησης του χρόνου των εργαζομένων, και πολλά άλλα.

Βαθμός ενσωμάτωσης του barcode από τις ελληνικές επιχειρήσεις

Αν μέχρι τώρα επιδοθήκαμε στην εξέταση του τι κάνει ο barcode για τις επιχειρήσεις, ήρθε η ώρα να εξετάσουμε το τι κάνουν οι επιχειρήσεις μ' αυτόν. Δηλαδή, ποιος ο βαθμός ενσωμάτωσης συστημάτων του είδους στις ελληνικές επιχειρήσεις. Όπως αναφέρει ο Αθανάσιος Δεληγιάννης, γενικός διευθυντής της Barcode Technologies, "το ποσοστό των επιχειρήσεων, ανεξαρτήτως μεγέθους, που έχουν αξιοποιήσει είτε μερικώς είτε πλήρως τις δυνατότητες ενός συστήματος barcode είναι τέτοιο, που μπορούμε να πούμε ότι έχουμε να διανύσουμε αρκετά μεγάλη απόσταση μέχρι να φθάσουμε στο σημείο που βρίσκονται άλλες χώρες είτε εντός της ΕΕ είτε εκτός". Σύμφωνα με τον κ. Δεληγιάννη, η αιτία του φαινομένου βρίσκεται στο "κόστος του απαιτούμενου εξοπλισμού, το οποίο έχει σαφώς πολύ πιο αργό ρυθμό μείωσης σε σχέση με την αντίστοιχη μείωση κόστους που παρατηρείται τα τελευταία χρόνια σε άλλους τομείς, όπως λ.χ. στην πληροφορική (βλ. υπολογιστές)". Ωστόσο, όπως σημειώνει ο Βύρων Ρηγινός, διευθύνων σύμβουλος της Datalex, "οι εφαρμογές γραμμωτού κώδικα αποτελούν επιλέξιμες δαπάνες στο πρόγραμμα "Ανταγωνιστικότητα" του υπουργείου Ανάπτυξης, που χρηματοδοτείται από πόρους του Γ' Κ.Π.Σ", γεγονός που μπορεί να αποβεί θετικό για τη βελτίωση της κατάστασης.

8.7 ΤΟ ΞΕΝΟΔΟΧΕΙΟ ΤΟΥ ΜΕΛΛΟΝΤΟΣ

Το ξενοδοχειακό δωμάτιο του μέλλοντος φαίνεται να είναι εντελώς 'άδειο', εκτός από έναν σταθμό επικοινωνίας ο οποίος θα αποτελείται από μια πολύ μεγάλη οθόνη LCD με σύστημα αναγνώρισης της φωνής, ένα πληκτρολόγιο και ένα εκτυπωτή. Θα είναι έτσι προγραμματισμένο το σύστημα ώστε με ευκολία θα προσαρμόζεται στις ιδιαίτερες απαιτήσεις του πελάτη του ξενοδοχείου με την εισαγωγή μια 'έξυπνης' κάρτας που θα την προμηθεύεται ο πελάτης από την υποδοχή του ξενοδοχείου κατά τη διάρκεια του check-in.

Οι πρώτες ιδέες για το δωμάτιο του μέλλοντος εμφανίστηκαν στην έκθεση EURHOTEC από το 1998, και φυσικά όλο και εξελίσσονται. Όπως έχει δηλώσει ο κ. Oliver Bernet διευθυντής νέων τεχνολογιών στην Swissotel, πριν το όραμα αυτό γίνει πραγματικότητα, τα ξενοδοχεία πρέπει να καταφέρουν να προσφέρουν στο πελάτη τους τα βασικά στοιχεία της ηλεκτρονικής τεχνολογίας και των συστημάτων ηλεκτρονικής ψυχαγωγίας, που ήδη οι πελάτες στις μέρες μας έχουν στα σπίτια τους. Αυτά επιγραμματικά είναι η επίπεδες οθόνες τηλεόρασης, ο περιμετρικός ήχος, και το σύστημα Digital Video Data, DVD. «Ο ταξιδιώτης ίσως μεταφέρει μαζί του τον δικό του εξοπλισμό, με αποτέλεσμα τα ξενοδοχεία να πρέπει να είναι έτοιμα και κατάλληλα εξοπλισμένα ώστε να επιτρέπουν την λειτουργία του. Βέβαια σύντομα αυτά τα συστήματα θα είναι άχρηστα, γιατί τα ξενοδοχεία θα πρέπει να προσφέρουν όλο τον μοντέρνο εξοπλισμό στον ταξιδιώτη και λύσεις πολύ πιο ευέλικτες».

Ο κ. Richard Hyde, διευθυντής ανάπτυξης marketing στα ξενοδοχεία Inter-Continental Hotels & Resorts, δήλωσε ότι σύμφωνα με την έρευνα που έκανε η εταιρία του οι ανάγκες των πελατών για τη νέα τεχνολογία πρέπει να ικανοποιούνται με τέτοιο τρόπο ώστε να είναι πανεύκολο για αυτούς να την εφαρμόσουν. Θα πρέπει οι πελάτες των ξενοδοχείων να μπορούν να συνδεθούν με το γραφείο τους χρησιμοποιώντας τα e-mail, ή να έχουν πολύ εύκολη πρόσβαση στο Internet, να κάνουν χρήση του voice mail, και να έχουν υψηλών προδιαγραφών τηλεοράσεις. Για να γίνει αυτό πραγματικότητα είναι απαραίτητο τα ξενοδοχεία να έχουν την κατάλληλη καλωδίωση, τις σωστές πρίζες, ακόμα και τον σωστό φωτισμό για εργασία μέσα στο δωμάτιο.

«Αυτό που είναι πολύ σημαντικό», τόνισε, «είναι η δυνατότητα από τον πελάτη να χρησιμοποιήσει όλα αυτά και μάλιστα να τα ελέγχει μόνος του. Οι διευθυντές των ξενοδοχείων πρέπει να κρατούν μια λεπτή ισορροπία μεταξύ των τεχνολογικών συστημάτων που απαιτούνται για την παραπάνω προσφορά προς τους πελάτες, και των εσόδων που φέρνει αυτή η επένδυση στο ξενοδοχείο. Αυτό είναι ένα σοβαρό τεχνικό πρόβλημα που έχουν να αντιμετωπίσουν τα ξενοδοχεία».

Το ερώτημα είναι να διατηρήσουν τα ξενοδοχεία την υπάρχουσα μέχρι στιγμής υποδομή τους διακινδυνεύοντας να μην μπορούν να εξυπηρετήσουν στο άμεσο μέλλον τους πελάτες τους ή να επενδύσουν σε μια πιο μοντέρνα υποδομή που όμως στο πιο απώτερο μέλλον θα τους είναι άχρηστη;

Η κοινή πρακτική που πρέπει να ακολουθήσουν τα ξενοδοχεία είναι να προσθέτουν επιπλέον καλωδίωση όταν κάνουν ανακαινίσεις έτσι ώστε όταν θα υπάρχει η αντίστοιχη τεχνολογική υποδομή να είναι έτοιμες οι καλωδιώσεις για την εφαρμογή της.

Ο πλήρης έλεγχος του πελάτη του περιβάλλοντος του δωματίου του ήταν και το κύριο θέμα ανάλυσης που έκανε στα πλαίσια της EURHOTEC και ο κ. Jacques Levy, σύμβουλος ξενοδοχείων της εταιρίας Landis & Staefa.

Ο κ. Levy είπε ότι η εφαρμογή συστημάτων ελέγχου ασφαλείας, φωτισμού, ανανέωσης του αέρα, επικοινωνίας, και ενέργειας μέσα σε κάθε δωμάτιο δηλ. ένα ολοκληρωμένο Σύστημα Διαχείρισης Δωματίου, Room Management System, (RMC) δίνει στους πελάτες μια εικόνα άνεσης, ενώ παράλληλα μειώνει τα κόστη του ξενοδοχείου.

«Πριν ευχηθούμε στο πελάτη μας καληνύχτα, πρέπει να έχουν επιβεβαιώσει ότι του προσφέρουμε μια καλή νύχτα», είπε χαρακτηριστικά ο κ. Levy. «Τα ξενοδοχεία είναι πολύπλοκες εγκαταστάσεις και κατά συνέπεια καταναλώνουν

πολύ ενέργεια. Παρόλα αυτά πολλά ξενοδοχεία τεσσάρων και πέντε ακόμα αστέρων δεν έχουν σύστημα RMC ή ακόμα και Σύστημα Διαχείρισης Κτιρίου Building Management System (BMS), και στον τομέα διοικούνται τελείως τυχαία. Στο μέλλον τα ξενοδοχεία θα διαθέτουν ολοκληρωμένα συστήματα RMC και BMS, και μάλιστα θα είναι φτιαγμένα που στην πραγματικότητα θα είναι ένα μόνο κεντρικό σύστημα, με αποτέλεσμα να έχουν σημαντικές μειώσεις στο κόστος λειτουργίας τους», πρόβλεψε ο κ. Levy.

Το ξενοδοχείο του μέλλοντος συνδυάζει την μοντέρνα τεχνολογία με τις ανάγκες των ταξιδιωτών

- Εικονική πραγματικότητα
- Βιομετρικά συστήματα αναγνώρισης
- Και όχι μόνο αυτά...

Στις μέρες μας στο πανεπιστήμιο του Houston στο Conrad N. Hilton College of Hotel and Restaurant Management μελετώνται τρία διαφορετικά σενάρια για τις ανάγκες των ταξιδιωτών. Αυτά τα σενάρια εστιάζουν την προσοχή τους στα ακόλουθα:

- στα προβλήματα του ύπνου
- στην μείωση του άγχους
- και σε νέες αντιλήψεις ώστε το δωμάτιο του μέλλοντος να είναι πιο άνετο, ασφαλέστερο, πιο παραγωγικό για αυτούς που ταξιδεύουν για επαγγελματικούς λόγους

Σύμφωνα με τον πρόεδρο του πανεπιστημίου κ. Alan Stutts, που είναι υπεύθυνος για την υλοποίηση των θεωριών στο ξενοδοχείο που υπάρχει μέσα στο πανεπιστήμιο, «με τις συνεχείς τεχνολογικές αναβαθμίσεις και την αύξηση της χρήσης από την πλευρά των πελατών της τεχνολογίας οι ξενοδόχοι πρέπει να είναι σε θέση να προσφέρουν διαμονή προσαρμοσμένη στις συγκεκριμένες ανάγκες του κάθε πελάτη σε ατομικό επίπεδο, (custom-design accommodations), ανάλογα με την ηλικία του, την υγεία του, την φύση της εργασίας του, το άγχος του, ακόμα και τις προτιμήσεις του σε amenities».

Το Conrad Hilton College έχει σχεδιάσει τρία διαφορετικά δωμάτια τα οποία προσφέρουν:

- Σύστημα αφύπνισης που ξυπνά τους πελάτες με προοδευτική αύξηση του φωτός και όχι με ηχητικό θόρυβο που είναι πολύ ενοχλητικός.
- Δωμάτια που διαμορφώνουν διαφορετικές συνθήκες φωτισμού, θορύβου, και θερμοκρασίας έτσι ώστε να δημιουργούν διαφορετικό περιβάλλον ανάλογα με τις απαιτήσεις του κάθε πελάτη.
- Συστήματα κλειδώματος που βασίζονται σε κωδικούς σκανάροντας το δάκτυλο, ή την παλάμη ή τον αμφιβληστροειδή του ματιού του πελάτη.
- Παράθυρα που αντικαθίστανται με εικόνες που διαλέγει ο πελάτης από ηλεκτρονική σύστημα ώστε να βλέπει τοπία που θα του προκαλούν χαλάρωση.

- Η διάταξη των δωματίων θα πρέπει να είναι τέτοια ώστε να εξυπηρετεί τους γηραιότερους πελάτες, αφού όπως αναφέρεται ιδιαίτερα στις ΗΠΑ το 2010, το 50% του πληθυσμού θα είναι πάνω από 65 χρονών. Αυτές οι αλλαγές προϋποθέτουν διαφορετικό φωτισμό, ευκολότερη χρήση των επίπλων και του ανοίγματος των εσωτερικών θυρών, και ντουζ αντί για μπανιέρες.
- Με το άγγιγμα ενός κουμπιού ενεργοποίηση τέτοιων ακουσμάτων που θα χαλαρώνουν
- Εσωτερική διασκέδαση που θα βασίζεται στην εικονική πραγματικότητα
- Ηλεκτρονικά ελεγχόμενα στρώματα ώστε να ξεκουράζουν τα σώματα των πελατών
- Μέσα στα δωμάτια συστήματα για σωματική εξάσκηση των πελατών
- Διατροφή που θα είναι βασισμένη στην ενδυνάμωση της υγείας των πελατών και σε συγκεκριμένες δίαιτες.

ΚΑΤΙ ΓΙΑ ΟΛΟΥΣ

Ο στόχος για το δωμάτιο του μέλλοντος είναι η εξυπηρέτηση όλων των τύπων καλεσμένων ακόμα και εκείνων που έχουν συγκεκριμένες ανάγκες και αναπηρίες.

Έρευνες έχουν δείξει ότι το στρες των πελατών αυξάνεται γιατί είναι χωρισμένοι από τις οικογένειές τους. Ως αποτέλεσμα, η τεχνολογία προσπαθεί να βρει τρόπους να συνδέσει τους πελάτες με τις οικογένειές τους με σχετικά χαμηλό κόστος.

Επιπλέον, κάποιος από τους πελάτες μπορεί να θέλει αντί για καραμέλα στο μαξιλάρι του μια βιταμίνη, ή αντί για μπουρνούζι αθλητικά ρούχα, ή κάτι άλλο. Ο βασικός σκοπός όμως των ξενοδοχείων παραμένει ο ίδιος με το παρελθόν: να δώσουν στους πελάτες τους ένα άνετο μέρος να μείνουν και να κοιμηθούν.

Τα επόμενα χρόνια, κάθε ξενοδοχείο από την χαμηλότερη κατηγορία μέχρι και τα πολυτελείας που δεν θα δίνει τη δυνατότητα στους πελάτες του για μεγάλες ταχύτητες σύνδεσης στο Internet θα πρέπει να γνωρίζει ότι θα έχει ένα μεγάλο ανταγωνιστικό μειονέκτημα.

Τι επιφυλάσσει το μέλλον;

Βέβαια αυτή η εξυπηρέτηση είναι μόνο η αρχή! Τι άλλα προϊόντα και υπηρεσίες θα πρέπει να προσφέρουν τα ξενοδοχεία στο μέλλον; Τι μπορούν να περιμένουν οι πελάτες να βρουν στα δωμάτια τους το άμεσο μέλλον;

Φωτισμός και θερμοκρασία δωματίου που θα ενεργοποιείται με την θερμοκρασία του σώματος του πελάτη

Μόλις μπει ο πελάτης στο δωμάτιο ή περπατήσει στο διάδρομο του ξενοδοχείου το σύστημα θα ενεργοποιείται, ενώ με την αναχώρηση του θα σταματά τη λειτουργία του.

Με αυτή την τεχνολογία, τα ξενοδοχεία θα έχουν καλύτερα αποτελέσματα στην μείωση της ενέργειας και στην μείωση του κόστους λειτουργίας τους. Οι πελάτες ως γνωστόν δεν θέλουν να περπατούν σε σκοτεινούς διαδρόμους, αλλά όταν φεύγουν από τα δωμάτια τους δεν ασχολούνται με το να σβήσουν τα φώτα, την θέρμανση και τον εξαερισμό.

Φορητά συστήματα αναγνώρισης του πελάτη

Αυτά τα συστήματα, που σύντομα θα κυκλοφορήσουν, δίνουν στους υπαλλήλους του ξενοδοχείου τη δυνατότητα να αναγνωρίσουν αν ο πελάτης είναι στο δωμάτιο του και έτσι να μην τον ενοχλήσουν. Με αυτό τον τρόπο, και βελτιώνονται οι σχέσεις πελάτη – ξενοδοχείου, αλλά και το προσωπικό γλιτώνει χρόνο αφού δεν πάει στο δωμάτιο το χρονικό διάστημα που είναι μέσα ο πελάτης.

Ασύρματα δίκτυα

Στα μεγάλα ξενοδοχεία τουλάχιστον είναι άκρως απαραίτητα συστήματα ασύρματα που θα παρακολουθούν όλες τις ενέργειες των υπαλλήλων είτε μεταξύ τους είτε σε σχέση με τους πελάτες. Παραδείγματος χάριν, όταν η καμαριέρα φτιάξει το δωμάτιο ενός πελάτη, πατά ένα κουμπί στο ασύρματο φορητό της μηχανήμα, και αμέσως ενημερώνεται και το τμήμα των ορόφων, αλλά και η ρεσεψιόν, ότι το συγκεκριμένο δωμάτιο είναι έτοιμο. Έτσι λοιπόν, και καλύτερος θα είναι ο συντονισμός μεταξύ των τμημάτων και εξοικονόμηση χρόνου και κόστους θα υπάρχει. Η καλύτερη επικοινωνία έχει ως αποτέλεσμα την αύξηση της παραγωγικότητας και της εξυπηρέτησης των πελατών.

Σύστημα Voice over Internet provider (VOIP)

Το σύστημα VOIP είναι μια τεχνολογία επικοινωνίας και αναμένεται να υιοθετηθεί από τον ξενοδοχειακό κλάδο τα επόμενα χρόνια. Οι πελάτες θα κερδίζουν από το χαμηλό κόστος και την υψηλή ποιότητα των τηλεφώνων μέσω του Internet. Όμως, επειδή τα τηλεφωνήματα αποτελούν πηγή εσόδων για το ξενοδοχείο, πολλά ξενοδοχεία αντιστέκονται σε αυτή την τεχνολογία.

Υψηλής ποιότητας video conferencing

Μέχρι το 2004 ή το 2005 αναμένεται τα συστήματα υψηλής ποιότητας video conferencing να είναι πια κάτι κοινό μέσα στα ξενοδοχεία, με δεδομένο μάλιστα ότι το κόστος αυτής της επικοινωνίας όλο και μειώνεται. Τα ξενοδοχεία έτσι θα κερδίζουν έσοδα και θα προσελκύουν περισσότερους ταξιδιώτες που ταξιδεύουν για επαγγελματικούς λόγους, όπως και συνέδρια, ενώ οι πελάτες θα απολαμβάνουν υπηρεσίες χαμηλού κόστους, υψηλή επικοινωνία, και συνέδρια με συμμετοχές από όλα τα μέρη του κόσμου.

Ασύρματα Property Management System (PMS)

Αυτό το ασύρματο φορητό σύστημα που είναι λίγο μεγαλύτερο από ένα PalmPilot, επιτρέπει στο προσωπικό του ξενοδοχείου να κάνει check in σε ένα πελάτη, να βρει ένα δωμάτιο στα πολύ μεγάλα ξενοδοχεία, να εκδώσει ένα κλειδί, να πληρωθεί με πιστωτική κάρτα, να πάρει την υπογραφή του πελάτη, και να καταγράψει τις προτιμήσεις και τα σχόλια ενός πελάτη. Όλες αυτές οι πληροφορίες στέλνονται αυτόματα στο κεντρικό ηλεκτρονικό σύστημα του ξενοδοχείου. Τα συστήματα αυτά είναι ήδη διαθέσιμα στην αγορά και στα επόμενα χρόνια θα εξοπλίζουν πολλά ξενοδοχεία. Με αυτό το σύστημα, τα ξενοδοχεία εξυπηρετούν καλύτερα τον πελάτη τους και διατηρούν λεπτομερή πηγή πληροφοριών. Οι συχνόι πελάτες μπορούν να κάνουν check in πολύ πιο γρήγορα, και το προσωπικό του

ξενοδοχείου να έχει μπροστά του αμέσως τις πληροφορίες που χρειάζεται, ώστε στους καλύτερους πελάτες να δίνουν προσφορές και εκπτώσεις.

Τα παραπάνω συστήματα είναι χρήσιμα για όλα τα ξενοδοχεία, είτε οι πελάτες τους ταξιδεύουν για επαγγελματικούς λόγους είτε για διακοπές. Στις μέρες μας, οι επαγγελματίες δουλεύουν και στο σπίτι τους ή παίρνουν τις οικογένειες τους όταν πάνε για μικρά ιδίως συνέδρια, ενώ οι τουρίστες που κάνουν διακοπές θέλουν να έχουν πρόσβαση στο e-mail τους, και στο Internet. Έτσι τα δωμάτια των ξενοδοχείων δεν πρέπει να σχεδιάζονται αποκλειστικά για εκείνους που ταξιδεύουν για επαγγελματικούς λόγους ή για εκείνους που ταξιδεύουν για διακοπές. Πρέπει να σχεδιάζονται για τον άνθρωπο του σήμερα που χρησιμοποιεί την τεχνολογία στις διακοπές του και συνδυάζει τις διακοπές του με την εργασία του. Τα πιο επιτυχημένα ξενοδοχεία δεν έχουν ως αγορά στόχο την μία ή την άλλη ομάδα, είναι ικανά να εξυπηρετήσουν και τις δύο.

Βέβαια, αυτό δεν σημαίνει ότι κάθε πελάτης έχει μαζί του το κινητό του ή τον φορητό του υπολογιστή, και είναι πρόθυμος να χρησιμοποιήσει την υψηλή τεχνολογία. Πολλοί άνθρωποι ακόμα προτιμούν τις ανθρώπινες επαφές κατά την διάρκεια της διαμονής τους σε ένα ξενοδοχείο. Έτσι δεν πρέπει να νομίζουμε ότι η παραδοσιακή ρεσεψιόν, οι γκρουμ, το ταμείο, θα ανήκουν στο παρελθόν, αντίθετα θα είναι εκεί έτοιμοι να χρησιμοποιήσουν μόλις χρειαστεί τα πιο σύγχρονα τεχνολογικά συστήματα.

8.8 ΚΑΙ ΟΙ ΕΛΛΗΝΕΣ ΦΩΤΟΓΡΑΦΙΖΟΝΤΑΙ ΚΑΙ ΔΑΚΤΥΛΟΣΚΟΠΟΥΝΤΑΙ

Από τη Δευτέρα (5.1.2004) ο κόσμος μπήκε για τα καλά στη "βιομετρική εποχή". Το πρόταγμα των πλούσιων κρατών για όλο και περισσότερη "ασφάλεια" απέναντι στον (καλοσυντηρούμενο) μπαμπούλα των ασύμμετρων τρομοκρατικών απειλών, οδηγεί σε όλο και πιο εξελιγμένα συστήματα ολοκληρωτικής παρακολούθησης και ανεξέλεγκτης αστυνόμευσης των πάντων. Τελευταία αμερικάνικη κρεασιόν, το US-VISIT. Το συμπληρωματικό βιομετρικό φακέλωμα, δηλαδή, των περίπου 25 εκατομμυρίων ξένων πολιτών που πρόκειται να πατήσουν το πόδι τους στο έδαφος της υπερδύναμης κατά το 2004. Μολονότι όλοι αυτοί οι ταξιδιώτες ήδη υφίστανται τις εξευτελιστικές και δαπανηρές διαδικασίες από τις αμερικανικές προξενικές αρχές στον τόπο καταγωγής τους, για την έκδοση της πολυπόθητης βίζας, οφείλουν πλέον να επανελέγχονται (δακτυλοσκόπηση, φωτογράφιση και συνέντευξη) σαν εγκληματίες στις εισόδους της "χώρας της ελευθερίας", ώστε να διασταυρώνονται και να εμπλουτίζονται οι φάκελοί τους.

Το σύστημα US-VISIT συνεργάζεται με το γνωστό CAPPs (Πληροφορικό Σύστημα Προληπτικού Ελέγχου), που τσεκάρει τους υφιστάμενους φακέλους δεκάδων εκατομμυρίων πολιτών απ' όλες τις χώρες με τα προσωπικά δεδομένα των ταξιδιωτών με τα οποία το τροφοδοτούν οι αεροπορικές εταιρείες συστηματικά από το περασμένο καλοκαίρι, χαρακτηρίζοντάς τους ως περισσότερο ή λιγότερο επίφοβους για την "εθνική ασφάλεια" των Η.Π.Α. Όλα αυτά τα προγράμματα του παγκόσμιου φακελώματος εντάσσονται στο τερατώδες ΤΙΑ, το Σύστημα Ολικής Παρακολούθησης του Πενταγώνου που διευθύνει ο περιβόητος στρατηγός Τζον Ποϊντέξτερ (σκάνδαλο Ιράν-Κόντρας), το οποίο σταδιακά πρόκειται να συγκεντρώσει αναλυτικές πληροφορίες συνδυάζοντας όλες τις διαθέσιμες πηγές: από τις κινήσεις των πιστωτικών καρτών και των τραπεζικών λογαριασμών, τις τηλεφωνικές κλήσεις και τις επισκέψεις στο Ιντερνετ, έως το ποινικό μητρώο και τους φακέλους φρονημάτων των πολιτών σε όλο τον κόσμο (και βεβαίως στις Η.Π.Α) που κατασκευάζουν αδιάκοπα οι συνεργαζόμενες κρατικές και διακρατικές

αρχές ασφαλείας (όπως η Eurorol, Shengen κ.λπ. στις οποίες μεταβιβάζει τα προσωπικά μας δεδομένα και η Ελληνική Αστυνομία).

Σύμφωνα με την κυβέρνηση των Η.Π.Α, από το νέο σύστημα εξευτελισμού των επισκεπτών κατά την είσοδό τους (με δακτυλοσκοπήσεις, φωτογραφίες κ.λπ.), εξαιρούνται οι πολίτες 27 κρατών που ήδη έχουν ευθυγραμμιστεί με τις "αντιτρομοκρατικές" απαιτήσεις του Στέιτ Ντιπάρτμεντ, εφαρμόζοντας σε αγαστή συνεργασία με τις αμερικανικές αρχές ασφαλείας το πρόγραμμα Visa Waiver Program (VWP). Με λίγα λόγια οι υπήκοοι των χωρών της Ε.Ε. (εκτός Ελλάδος) κατέχουν ειδικά διαβατήρια με ψηφιακές πληροφορίες που διαβάζονται αυτόματα από τα ηλεκτρονικά συστήματα ελέγχου και καταγραφής των Η.Π.Α, εφόσον αυτά τα διαβατήρια περιέχουν (πιστοποιημένα από τον "Μεγάλο Αδελφό") τα "βιομετρικά" τους δεδομένα. Επομένως, όσοι θύμωσαν και σκέφτηκαν ότι θα έπρεπε να διαμαρτυρηθούμε για διακριτική και δυσμενή μεταχείριση των Ελλήνων ταξιδιωτών από τις Η.Π.Α, και ίσως να προβούμε, με βάση την αρχή της αμοιβαιότητας, σε μέτρα ανάλογα μ' αυτά που επέβαλλε η Βραζιλία στους αμερικανούς τουρίστες -τους οποίους δακτυλοσκοπεί και φωτογραφίζει.

Μέσα στο 2004 ολόκληρη η Ευρωπαϊκή Ένωση, όπως ήδη από τον περασμένο Οκτώβριο έχει αποφασίσει, συνεπώς και το ελληνικό κράτος, θα προσχωρήσει στο ενιαίο "βιομετρικό" μοντέλο φακελώματος όλων των ευρωπαίων πολιτών και των αλλοδαπών που την επισκέπτονται, ακολουθώντας ακριβώς ό,τι ζητά και επιβάλλει σταδιακά σε όλα τα "προηγμένα" κράτη η υπερδύναμη.

Εύλογα θα αναρωτηθείτε για το πού τελικά οδεύει ο "νομικός πολιτισμός" των ανεπτυγμένων δυτικών δημοκρατιών, στον πυρήνα του οποίου υποτίθεται ότι βρίσκεται ο ευλαβικός σεβασμός του απαραβίαστου της προσωπικής ζωής, των ατομικών δικαιωμάτων και των ελευθεριών, όπου κανένας πολίτης δεν παρακολουθείται, δεν φακελώνεται, δεν υφίσταται διακρίσεις κ.ο.κ.

Τα βιομετρικά της ελληνικής αγοράς

Στη συνέχεια του αφιερώματος μας, κάνουμε αναφορά στα βιομετρικά που κυκλοφορούν στην ελληνική αγορά. Όπως μπορείτε να διαπιστώσετε και μόνοι σας τα περισσότερα από αυτά και συγκεκριμένα τα 11, χρησιμοποιούν τεχνολογία αναγνώρισης δαχτυλικού αποτυπώματος. Από αυτά αναμφισβήτητα ξεχωρίζει το AccessGuard, το οποίο εκτός από τον αναγνώστη proximity, μπορεί να υποστηρίξει μέχρι και 20.000 εγγραφές. Το CR-BIOP-A της Position Technology διαθέτει επίσης αναγνώστη proximity και υποστηρίζει 4.000 χρήστες, ενώ το V-Station της Bioscrypt υποστηρίζει 3.000 χρήστες. Με αναγνώστη proximity έρχονται και το V-prox της Bioscrypt, το Star Finger-006 της ID Teck και το CR-BIOP-A της Position Technology. Ειδική μνεία πρέπει να γίνει και στο SmartTouch της Integrated Technologies, το οποίο είναι το μόνο που επιτρέπει την αποθήκευση του βιομετρικού δείγματος σε κάρτα proximity.

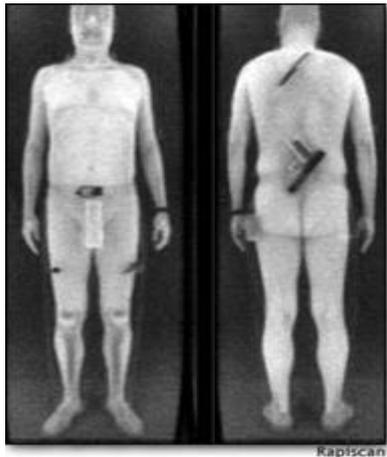
Βιομετρικά αναγνώρισης παλάμης στην ελληνική αγορά κυκλοφορούν μόλις δύο, τα οποία προέρχονται από την ίδια εταιρία, την RSI. Το Handkey II μπορεί με κατάλληλη επέκταση να χρησιμοποιηθεί για τον έλεγχο πρόσβασης 35.512 ατόμων, ενώ το HandPunch 2000 χρησιμοποιείται για ωρομέτρηση προσωπικού.

Στον τομέα της αναγνώρισης ίριδας παρουσιάζουμε 4 βιομετρικά. Από αυτά το το BM-ET500 της Panasonic είναι το μόνο που δεν απαιτεί από το "στήσιμο" του υπό πιστοποίηση ατόμου. Το IrisAccess TM 3000 και το TrueEye της Senex

διακρίνονται για τον μικρό χρόνο ταυτοποίησης, ο οποίος είναι λιγότερο από 1sec, ενώ αρκετά γρήγορο είναι και το BM-ET300 της Panasonic, αφού για να αποφανθεί χρειάζεται μόλις 1,5sec.

8.9 ΤΕΧΝΟΛΟΓΙΑ ΑΝΙΧΝΕΥΣΗΣ ΣΩΜΑΤΩΝ (RAPISCAN)

Οι αερολιμένες επιδιώκουν την ασφάλεια υψηλής τεχνολογίας



Μια επίδειξη της τεχνολογίας ανίχνευσης σωμάτων (Rapiscan) παρουσιάζει μπροστινή άποψη ενός επιβάτη με εκρηκτικά, κλειδιά και νομίσματα. Η οπίσθια άποψη αποκαλύπτει ένα Glock 17 περιστροφο, ένα κεραμικό μαχαίρι 4-ίντσών και ένα πορτοφόλι.

Μπορούν να δουν μέσω των ενδυμάτων σας και να πουν ακριβώς ποιοι είστε ακριβώς με το βλέμμα στα μάτια σας. Μερικοί μπορούν ακόμη και να σας μυρίσουν. Νέες συσκευές ασφάλειας υψηλής τεχνολογίας έχουν μπει στην αγορά, και θα μπορούσαν σύντομα σε έναν αερολιμένα να βρίσκονται κοντά σε σας. Αλλά οι διάφορες νέες τεχνολογίες είναι σίγουρο ότι θα τρέξουν σε μια αναταραχή, δεδομένου ότι το κοινό αποφασίζει ακριβώς κατά πόσο είναι πρόθυμο να πληρώσει — κυριολεκτικά και μεταφορικά — για να αισθανθεί ασφαλές πάλι.

Σε μία προσπάθεια να σταματήσουν τους πιθανούς τρομοκράτες στις διαδρομές τους, η ΑΜΕΡΙΚΑΝΙΚΗ κυβέρνηση και ένας αριθμός αερολιμένων σε ολόκληρη τη χώρα εξετάζουν τα νέα μηχανήματα και τα συστήματα βιομετρικής ,που μπορούν να προσδιορίσουν τους επιβάτες από τα μοναδικά φυσικά γνωρίσματα όπως ένα δακτυλικό αποτύπωμα ή την ίριδα.

\$50 εκατομμύρια ετησίως διατίθενται για την ανάπτυξη της προηγμένης τεχνολογίας. Η αντιπροσωπεία ασφάλειας μεταφορών(TSA) είναι υπεύθυνη για τα σημεία ελέγχου αερολιμένων όλου του έθνους.

"Το συνέδριο ανοίγει το καρνέ επιταγών του," λέει ο Tom Jensen, Πρόεδρος της εθνικής ασφαλούς συμμαχίας ουρανών, μια μη κερδοσκοπική ομάδα που εξετάζει τις νέα συσκευές και τα πρωτότυπα εναέριας ασφάλειας.

Για να αποφύγει τις κακές επιλογές από τους νομοθέτες που είναι πρόθυμοι να καθησυχάσουν τον τρέχοντα φόβο του κοινού, το TSA έχει ζητήσει από τους ασφαλείς ουρανούς βοήθεια. Τώρα, στο διεθνή αερολιμένα του Ορλάντο στη Φλώριδα, οι επιβάτες μπορούν να προσφερθούν εθελοντικά να περάσουν από τις διαδικασίες ασφάλειας με σκοπό να εξετάσουν μια σειρά νέων συσκευών.

Εικονική αναζήτηση λουριδών

Ένα από τα πιο αμφισβητούμενα στοιχεία της τεχνολογίας Rapiscan είναι ότι εξασφαλίζει τον ανιχνευτή 1000 σωμάτων, μια χαμηλής ενέργειας ακτίνα X που υπερβαίνει τους σημερινούς ανιχνευτές μετάλλων με την ακτινοβολία μέσω των ενδυμάτων ενός επιβάτη για να αποκαλύψει την ύπαρξη ξένων αντικειμένων δίπλα στο δέρμα τους. Μπορεί να ανιχνεύσει το μέταλλο, καθώς επίσης και οτιδήποτε ανόργανο όπως για παράδειγμα ένα πολυμερές πυροβόλο όπλο ή ακόμα και πλαστικές εκρηκτικές ύλες.

Αλλά εξασφαλίζει επίσης και άλλες μορφές, συμπεριλαμβανομένης της γενικής περιλήψης του σώματος και των γεννητικών οργάνων. « Αυτό, φυσικά, είναι μια εικονική αναζήτηση λουριδών » λέει ο Barry Steinhardt.

Οι κατασκευαστές της μηχανής, καθώς επίσης και εκείνοι που έχουν εξετάσει τον ανιχνευτή 1000 ισχυρίζονται ότι η τεχνική αναζήτηση- λουρίδας έχει ανθίσει. Σύμφωνα με τον Jensen, οι εικόνες της ακτίνας X των πιο ιδιωτικών μερών των ανθρώπων, είναι μαυρισμένες στην καλύτερη περίπτωση. Επιπλέον, οι άνθρωποι που χειρίζονται τα μηχανήματα (άνδρες για τους άνδρες και γυναίκες για τις γυναίκες), κάθονται πίσω από έναν τοίχο και δεν βλέπουν τον επιβάτη εκτός κι αν ανιχνεύουν κάτι ύποπτο.

Τέλος, μόνο ορισμένοι επιβάτες -που επιλέγονται είτε τυχαία, είτε επειδή κάτι για τη συμπεριφορά ή την εμφάνισή τους ανησυχεί τους υπεύθυνους -θα καλούνταν να έχουν την ανίχνευση αρχικά.

Χέρια «μακριά»

Ο Bryan Allman, ο διευθυντής προγράμματος για τον ανιχνευτή σωμάτων Rapiscan, λέει ότι μερικοί ταξιδιώτες μπορούν να προτιμήσουν τη μηχανή πέρα από τις τρέχουσες μεθόδους επιθεώρησης. "Πετώ όπως όλοι," λέει. "Και δεν το απολαμβάνω όταν τυγχάνω σωματικής ερευνάς στους αερολιμένες. "Ο ανιχνευτής σωμάτων είναι πολύ λιγότερο ενοχλητικός κατά την άποψή μου, επειδή κανένας δεν σας αγγίζει."

Οι μηχανές εκπέμπουν την ακτινοβολία, αλλά τα επίπεδα είναι τόσο χαμηλά που δεν τίθεται θέμα ιατρικής ανησυχίας.

Η ομοσπονδιακή υπηρεσία μετανάστευσης και εγκλιματισμού χρησιμοποιεί ήδη τους ανιχνευτές σωμάτων, αλλά η διαδεδομένη χρήση τους θα μπορούσε ακόμα να είναι μερικά έτη μακριά.

Ακόμη και οι λιγότερο αμφισβητούμενες συσκευές που εξετάζονται από την κυβέρνηση θα έδιναν στους υπεύθυνους μεγάλη βοήθεια. Ένας ανιχνευτής μπουκαλιών στο πείραμα του Ορλάντο, παραδείγματος χάριν, μπορεί να καθορίσει ποιο είδος ουσίας είναι σε ένα σφραγισμένο εμπορευματοκιβώτιο.

Και μια ακτίνα X διπλής-εικόνας εξετάζει τις τσάντες από δύο κατευθύνσεις ταυτόχρονα. "Σε μια διάσταση, ένα μαχαίρι μοιάζει ακριβώς με μια γραμμή," λέει Jensen, "αλλά μια άλλη οπτική γωνία θα παρουσίαζε την επίπεδη πλευρά της λεπίδας, γεγονός που καθιστά τις εργασίες των υπευθύνων πολύ γρηγορότερες και ευκολότερες."

Η βιομετρία είναι το "κλειδί"

Τα μέλη αεροπορίας συμφωνούν, εντούτοις, ότι η ανάπτυξη όλων αυτών των συσκευών υψηλής τεχνολογίας θα ήταν πάρα πολύ ακριβή και χρονοβόρα, εκτός κι αν συνδυάζονταν με τις βιομετρικές κάρτες ταυτότητας που θα προσδιόριζαν τους προ-καλυμμένους επιβάτες.

"Πρέπει να πάρετε τους χαμηλού-κινδύνου ανθρώπους και να τους περάσετε μέσω του συστήματος γρήγορα, έτσι ώστε να μπορείτε να επικεντρωθείτε στους ανθρώπους υψηλού-κινδύνου," λέει ο Robert Atkinson, ένας κύριος υπερασπιστής του προοδευτικού πολιτικού ιδρύματος που είναι γνωστό ως κάρτα "εμπιστευμένων ταξιδιωτών".

Προτεινόμενο ως εθελοντικό σύστημα, στα αεροδρόμια θα χορηγούνταν μια κάρτα μόνο μετά από έναν αρχικό έλεγχο υπόβαθρου, χρησιμοποιώντας τους υπολογιστές που συνδέονται με τις βάσεις δεδομένων του FBI και INS.

Κατόπιν, στις πύλες εισόδου αερογραμμών, θα ζητούνταν στους επιβάτες να βάλουν ένα δάχτυλο σε έναν ανιχνευτή ή να εξεταστούν στο προσοφθάλμιο για να αποδειχθεί ότι πράγματι είναι το πρόσωπο που ισχυρίζονται ότι είναι.

Με τον τρόπο αυτό οι αποκαλούμενοι "εμπιστευμένοι ταξιδιώτες" θα περνούσαν από τους τυποποιημένους ελέγχους ασφάλειας, αλλά δεν θα υποβάλλονταν σε χρονοβόρα εξέταση.

Προσδιορίζοντας τους "κακούς δράστες"



Στο Ισραήλ, που κρατιέται ψηλά ως πρότυπο για την ασφάλεια αερολιμένων, ένα βιομετρικό πρόγραμμα για τους επιβάτες υπάρχει ήδη. Κατά τη διάρκεια των προηγούμενων τριών ετών, 85.000 Ισραηλίτες έχουν υπογράψει για το σύστημα εισόδων EDS, το οποίο επιτρέπει τους επιβάτες να κινούνται γρηγορότερα μέσω της ασφάλειας στα ειδικά ηλεκτρονικά περιπτερα όπου παρεμβάλλουν απλά τις κάρτες τους και βάζουν τα χέρια τους σε έναν ειδικό αναγνώστη.

"Η βιομετρική έχει μειώσει το χρόνο αεροπλάνου-συγκράτησης στο Ben Gurion από περίπου δύο ώρες ανά επιβάτη σε 15 λεπτά," λέει ο Bret Kidd, αντιπρόεδρος στα συστήματα ηλεκτρονικών στοιχείων, το οποίο διαχειρίζεται τη σαφή είσοδο. "Η σωματική ασφάλεια πρέπει πάντα φυσικά να υπάρχει, αλλά πρέπει επίσης να προσδιορίσετε τους κακούς δράστες, και οι βοήθειες της βιομετρικής βοηθούν να επισπεύσετε τη διαδικασία."

Ο Kidd θεωρεί ότι συστήματα όπως το EDS Express Entry, η πρόσφατη έκδοση της οποίας παρουσιάστηκε στην πρόσφατη διάσκεψη τεχνολογίας COMDEX στο Σικάγο, θα χρησιμοποιηθεί τελικά στις Ηνωμένες Πολιτείες.

"Η σκέψη μέχρι τώρα ήταν ότι εάν πρόκειται να αυξήσουμε την ασφάλεια, θα πρέπει να μειώσουμε την ευκολία και την αποδοτικότητα," λέει ο Kidd. "Αυτό που λέμε τώρα είναι ότι με τη βιομετρική, αυτό είναι εφικτό."

Αποφυγή ενός άλλου 11/9

Το ACLU έχει αντιτάξει με συνέπεια την ιδέα των βιομετρικών καρτών — ακόμα κι αν είναι εθελοντικές — λόγω των ανησυχιών και φόβων ότι μπορεί να χορηγηθούν άδικα βασισμένες στη φυλετική σκιαγράφιση.

Αλλά ο Atkinson, που έγραψε το πολιτικό έγγραφο του Κογκρέσου "Πώς η τεχνολογία μπορεί να βοηθήσει στο να γίνουν οι αερολιμένες ασφαλείς ξανά" επιμένει ότι ενσωματώνοντας τη βιομετρική σε όλα τα επίπεδα ασφάλειας αερολιμένων, μπορεί να είναι ο μόνος τρόπος να αποτραπούν περισσότερες επιθέσεις όπως αυτές στις 11 Σεπτεμβρίου.

"Τέσσερις από τους πέντε αεροπειρατές στην πτήση Dulles είχαν πλαστά διπλώματα οδήγησης," λέει ο Atkinson. "Έτσι, όταν μιλάμε για τους ανθρώπους που οδηγούν τα αεροπλάνα στα κτήρια, η δικαιοσύνη και η μυστικότητα δεν πρέπει να είναι τα τελευταία κριτήρια."

8.10 ΟΙ ΒΙΟΜΕΤΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ ΤΙΘΕΝΤΑΙ ΩΣ ΣΤΟΧΟΣ ΝΑ ΑΝΑΛΑΒΟΥΝ ΤΙΣ ΣΥΝΑΛΛΑΓΕΣ



Η βιομετρική είναι η τεχνολογία που θεωρείται κατάλληλη για την ασφάλεια. Το επόμενο βήμα είναι η βιομετρική για την ενεργοποιημένη θέση πώλησης και τις οικονομικές συναλλαγές για να καταπολεμήσει την απάτη και να ενισχύσει την ταχύτητα και την ευκολία.

Ασφάλεια εναντίον της μυστικότητας

Η βιομετρική χωρίζεται σε δύο τύπους: συμπεριφορικός (η παραδοσιακή υπογραφή και η φωνή) και φυσιολογικός (πρόσωπο, δακτυλικό αποτύπωμα, χέρι, και αναγνώριση ίριδων). Η διαδεδομένη υιοθέτηση της πιο αξιόπιστης φυσιολογικής αναγνώρισης έχει επιβραδυνθεί από το κόστος και την απροθυμία να γίνει αποδεκτό τι βλέπουν πολλοί ως εισβολή της ιδιωτικής ζωής. Στο περυσινό Κύπελλο Snoper η αστυνομία της Τάμπα ανίχνευσε κρυφά 100.000 οπαδούς στην

αναζήτηση γνωστών εγκληματιών. Αλλά η πρόσφατη επείγουσα ανάγκη για να σφίξει την αμερικανική ασφάλεια φαίνεται να γυρίζει την παλίρροια.

Ο Δρ Joseph Atick, Πρόεδρος και CEO του Visionics – πρωτοπόρος στην τεχνολογία της αναγνώρισης προσώπου - πρόσφατα θεωρήθηκε ένας από τους κορυφαίους επιχειρηματίες της επιχειρησιακής εβδομάδας για το 2001, μια ένδειξη της μεγάλης ακτινοβολίας της βιομετρικής. Ο Δρ Atick βλέπει τη βιομετρική να χρησιμοποιείται για την επαλήθευση ταυτότητας, οικονομικές συναλλαγές, και ακόμη και ως εναλλακτικό σύστημα πληρωμής για λιανικό: Η "επαλήθευση ταυτότητας για τις συναλλαγές ηλεκτρονικού εμπορίου θα ήταν ιδανική να ταιριάξει τον άνθρωπο με τη δράση." Το μεγαλύτερο μέρος της επιχείρησης Visionics είναι η αναγνώριση δακτυλικών αποτυπωμάτων και η τεχνολογία FaceIt της αποτελεί προς το παρόν το 10% του εισοδήματός της. Ο Δρ Atick βλέπει τη βιομετρική να εξελίσσεται βαθμιαία: "Θα μπορούσατε να υποχρεωθείτε για να καθιερώσετε την ταυτότητά σας για να ολοκληρώσετε μια συναλλαγή. Οι έξυπνες κάρτες με τις πληροφορίες δακτυλικών αποτυπωμάτων θα λειτουργούσαν ως ένα μη-δικτυωμένο πρότυπο αυτοεξυπηρητήσεων, και αργότερα, δικτυωμένα περίπτερα θα χρησιμοποιούσαν τους αισθητήρες δακτυλικών αποτυπωμάτων αντί της κάρτας."

Τα αεριωθούμενα καταστήματα της ενωμένης λιανικής πώλησης στη Νότια Αφρική ολοκλήρωσαν τη βιομετρική αξία ενός προσώπου (Biocom's Face Value), η οποία χρησιμοποιεί την τεχνολογία FaceIt για να καταχωρήσει τα πρόσωπα των πελατών με τα στοιχεία των πιστωτικών καρτών τους σε εθελοντική βάση. Μια μικρή φωτογραφική μηχανή δίπλα στον κατάλογο μετρητών ανιχνεύει έπειτα κάθε πρόσωπο. Ο Jan De Lange, ανώτερος υπάλληλος διαδικασιών για το λιανοπωλητή μόδας λέει, "είναι μια τεράστια επιτυχία, με την αποδοχή πελατών κατά 99,7%. Οι πελάτες πλησιάζουν και ξέρετε τα ονόματά τους." Ο De Lange λέει ότι το επόμενο βήμα είναι να δημιουργηθεί ένα πρόγραμμα πίστης για να ανταμείψει τους εγγεγραμμένους και για να περιορίσει τις κάρτες: "Η πρόθεση είναι ότι το μόνο που χρειάζεστε είναι το πρόσωπό σας για να ολοκληρώσετε μια συναλλαγή." Ο De Lange εξηγεί, "εξετάζουμε το αποτύπωμα και την ίριδα, αλλά είναι όλοι ενεργοί-ο πελάτης πρέπει να κάνει κάτι. Η αναγνώριση του προσώπου είναι παθητική."

Η παθητικότητα της αναγνώρισης του προσώπου είναι ο λόγος που προκαλεί τις ανησυχίες για την ιδιωτική ζωή, αν και είναι ένα χρήσιμο εργαλείο για να καταπολεμήσει την απάτη. Σύμφωνα με τον Πρόεδρο Viisage και τον CEO Tom Colatosti, "ευρέως έχει αναφερθεί ότι υπήρξαν 750.000 άνθρωποι πέρυσι οι οποίοι ήταν θύματα κλοπής ταυτοτήτων."

Το Infonox χρησιμοποιεί το προϊόν Viisage για να εγγράψει τους χρήστες πιστωτικών καρτών για τις αυτοματοποιημένες μηχανές ταμιών (ACMs) στις χαρτοπαικτικές λέσχες Harrah και Mohegan. Τα ACMs φωτογραφίζουν τους νέους εγγεγραμμένους και τυπώνουν μια απόδειξη. Ένας ταμίας ελέγχει τη φωτογραφία σε σχέση με μια ταυτότητα εικόνων και κτυπάει την πιστωτική κάρτα. Έκτοτε, το ACM χρησιμοποιεί την αναγνώριση του προσώπου αντί του PIN. Για λιανικό, ο Πρόεδρος του Infonox και του CTO ο Δρ Safwan Shah εξηγεί, "οι άνθρωποι είναι οι πιο άνετοι με τη διανομή πληροφοριών στο σημείο της πώλησης. Γιατί να μη γίνεται η χρήση του αφού μπορεί να αναπτύξει την τεχνολογία και την ασφάλεια;"

8.11 ΔΙΑΒΑΤΗΡΙΑ-ΘΑΥΜΑΤΑ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ Διαβατήριο με μικροτσιπ και ολόγραμμα

Κρυφές φωτογραφίες, αόρατη μελάνη και βιομετρικά στοιχεία του κατόχου καθιστούν ασφαλή τα νέα ελληνικά ταξιδιωτικά έγγραφα.

Ψηφιακή εκτύπωση φωτογραφίας και στοιχείων, χρήση ειδικής, εξαιρετικά λεπτής μεμβράνης, που καταστρέφεται πολύ εύκολα σε προσπάθεια αποκόλλησής της, ψηφιακά ολογράμματα τυπωμένα πάνω σε αυτήν, δεύτερη φωτογραφία σε μικρότερο μέγεθος, αόρατη διά γυμνού οφθαλμού, χρήση υπεριώδους και υπέρυθρης μελάνης, που είναι πολύ δύσκολο να αναπαραχθούν. Αυτά είναι μερικά από τα χαρακτηριστικά που διαθέτει το νέο διαβατήριο της χώρας μας, τα οποία το καθιστούν εξαιρετικά ασφαλές, ίσως το ασφαλέστερο διεθνώς αυτή τη στιγμή. Το νέο διαβατήριο, που έχει ήδη σχεδιασθεί ως προς τις προδιαγραφές ασφαλείας, θα αρχίσει να παράγεται από την 1η Ιουλίου, οπότε και περνάει στην Ελληνική Αστυνομία η ευθύνη έκδοσης διαβατηρίων.

Για το νέο διαβατήριο μιλάει σήμερα αποκλειστικά στην «Κ» ο άνθρωπος που ουσιαστικά το δημιούργησε, ο δρ Ηλίας Σαμαράς, γενικός διευθυντής του έργου - για λογαριασμό της ΕΛ.ΑΣ. και του υπουργείου Δημόσιας Τάξης-, δημιουργίας της νέας Κεντρικής Υπηρεσίας Έκδοσης Διαβατηρίων και παροχής του μηχανογραφικού συστήματος για τα νέα διαβατήρια. Ο κ. Σαμαράς, απόφοιτος του Πολυτεχνείου του MIT, του Columbia University, με σπουδές και στο Harvard Business School, είχε αναλάβει στο πρόσφατο παρελθόν την εφαρμογή της ίδιας τεχνολογίας έκδοσης πιστοποιητικών (TOPPAN) για λογαριασμό των Η.Π.Α, του Καναδά και άλλων χωρών, δημιουργώντας τα δικά τους διαβατήρια.

Αγόρασε πλαστό

Όπως επισημαίνει, όταν ανέλαβε το έργο δημιουργίας του νέου διαβατηρίου και γνωρίζοντας πολύ καλά την πίεση και τη διεθνή κατακραυγή που έχει δεχθεί η χώρα μας για τα διαβατήρια που διαθέτει, έβαλε προσωπικό στοιχείο να δημιουργήσει ένα διαβατήριο περισσότερο ασφαλές από οποιοδήποτε άλλο κυκλοφορεί. Μάλιστα, ένα από τα πρώτα πράγματα που έκανε ήταν να προσεγγίσει κύκλωμα παραχαράκτων και έναντι 4.398,83 € να προμηθευτεί ένα πλαστό διαβατήριο για να διαπιστώσει πόσο εύκολη ήταν η παραχάραξη του ισχύοντος σήμερα διαβατηρίου. Προσθέτει επιπλέον ότι με την τεχνολογία TOPPA έχουν παραχθεί διεθνώς περισσότερα από 70 εκατομμύρια διαβατήρια με μηδενικό ιστορικό παραχάραξης ή πλαστογράφησης μέχρι σήμερα.

Πώς θα είναι, λοιπόν, το νέο ελληνικό διαβατήριο; Κατ' αρχάς τα νέα διαβατήρια θα είναι ψηφιακά, δηλαδή θα αποτυπώνονται σε αυτά με ψηφιακή τεχνολογία η φωτογραφία και τα στοιχεία του κατόχου. Αυτή είναι η πρώτη διαφορά με αυτά που κυκλοφορούν σήμερα. Επιπλέον, η φωτογραφία και τα στοιχεία της ταυτότητας δεν θα αποτυπώνονται στο εσωτερικό του οπισθόφυλλου, όπως γίνεται τώρα, αλλά στη δεύτερη εσωτερική σελίδα του διαβατηρίου. Αυτή η εκτύπωση θεωρείται πιο ασφαλής από εκείνη του διαβατηρίου των Η.Π.Α, για παράδειγμα, όπου η εκτύπωση γίνεται στο εσωτερικό του εξωφύλλου, διότι, όπως επισημαίνει ο κ. Σαμαράς, το εξώφυλλο έχει πάχος τέτοιο, που θα μπορούσε να επιτρέψει προσπάθεια παραχάραξης με χρήση λείζερ. Αντίθετα, το εσωτερικό φύλλο είναι τόσο λεπτό, ώστε η παραμικρή ανάλογη απόπειρα το καταστρέφει αμέσως.

Η «κρυφή» φωτογραφία

Σε ένα άλλο σημείο της ίδιας σελίδας θα υπάρχει η λεγόμενη «κρυφή» φωτογραφία. Πρόκειται ουσιαστικά για την ίδια φωτογραφία, που είναι ορατή, η οποία όμως τυπώνεται για δεύτερη φορά σε μικρότερο μέγεθος με τη χρήση υπεριώδους μελάνης, και είναι αόρατη διά γυμνού οφθαλμού, «διαβάζεται» όμως με τη χρήση ειδικής δέσμης φωτός, που χρησιμοποιείται κατά τον έλεγχο στα σημεία εισόδου και εξόδου από μια χώρα.

Η σελίδα αυτή θα είναι καλυμμένη με πλαστική μεμβράνη, όπως ισχύει και τώρα. Η διαφορά είναι ότι η μεμβράνη των νέων διαβατηρίων είναι εξαιρετικά λεπτή, το πάχος της είναι μόλις δέκα χιλιοστά του χιλιοστού και, ως εκ τούτου, καταστρέφεται πολύ εύκολα εάν κάποιος επιχειρήσει να την «πειράξει». Επάνω στη μεμβράνη τυπώνονται ψηφιακά ολογράμματα. Διά γυμνού οφθαλμού τα ολογράμματα μπορεί να μοιάζουν με απλές γραμμές. Στην ουσία είναι λέξεις και φράσεις γραμμένες με πολύ μικρά στοιχεία και, όπως αναφέρει ο κ. Σαμαράς, για επιπλέον ασφάλεια μπορεί να γίνει αναγραμματισμός ή ακόμη και εσκεμμένα ορθογραφικά λάθη, τα οποία θα γνωρίζουν οι αρχές αλλά όχι και οι επίδοξοι παραχαράκτες. Επιπλέον, στη μεμβράνη θα τυπωθούν και διάφορα θέματα από τον ελληνικό πολιτισμό διαχρονικά, όπως για παράδειγμα ο Παρθενώνας. Ανάλογα θέματα θα τυπωθούν και ως φόντο σε όλες τις εσωτερικές σελίδες του διαβατηρίου, το οποίο θα αλλάξει και χρώμα και από μπορντό θα γίνει, πιθανότατα, μπλε.

Βιομετρικά στοιχεία

Εφ' όσον οριστικοποιηθεί η λήψη σχετικής απόφασης από την Ευρωπαϊκή Ένωση, έπειτα από τη σχετική απόφαση του ICAO, του διεθνούς οργανισμού, που δραστηριοποιείται υπό την αιγίδα του Ο.Η.Ε και ασχολείται με την ασφάλεια των αερομεταφορών, για ενσωμάτωση βιομετρικών στοιχείων στα διαβατήρια, σε δεύτερη φάση έχει προβλεφθεί και αυτή η δυνατότητα. Στο οπισθόφυλλο του διαβατηρίου θα βρίσκεται ενσωματωμένο ένα μικροτσίπ, σε μέγεθος περίπου ενός τετραγωνικού εκατοστού. Σε αυτό θα αποθηκεύεται φωτογραφία του κατόχου, δακτυλικό αποτύπωμα σε ψηφιακή μορφή ή αποτύπωμα της ίριδας του ματιού. Αυτά τα τρία και με αυτή τη σειρά, είναι τα πλέον έγκυρα βιομετρικά στοιχεία, σύμφωνα με την ICAO. Το μικροτσίπ θα περιβάλλεται από ένα μεταλλικό πλέγμα, που λειτουργεί σαν κεραία με εμβέλεια περίπου ενός μέτρου. Μέσω αυτής θα δίδεται η δυνατότητα στα μηχανήματα ελέγχου των αεροδρομίων να «διαβάζουν» ένα διαβατήριο από απόσταση, ακόμη κι αν ο κάτοχός του το έχει στην τσέπη ή στην τσάντα του.

Η «αντοχή» των νέων διαβατηρίων απέναντι σε προσπάθειες παραχάραξης ελέγχθηκε εξονυχιστικά στα εργαστήρια της Διεύθυνσης Εγκληματολογικών Ερευνών της ΕΛ.ΑΣ. και πέρασε τη δοκιμασία. Μέρος των δικλίδων ασφαλείας που διαθέτουν, όπως η «κρυφή» φωτογραφία, χρησιμοποιήθηκε και στις κάρτες διαπίστευσης των Ολυμπιακών Αγώνων της Αθήνας.

Η νέα διαδικασία έκδοσης

Η Κεντρική Υπηρεσία Έκδοσης Διαβατηρίων (ΚΥΕΔ) θα στεγαστεί σε κτίριο της Ελληνικής Αστυνομίας την οδό Χίου 8, στην Καισαριανή. Αναμένται να είναι έτοιμη η εγκατάσταση στα τέλη Μαΐου και να ακολουθήσει ένα δίμηνο δοκιμών και εκπαίδευσης του προσωπικού. Η Υπηρεσία θα λειτουργεί 24 ώρες το 24ωρο και σε αυτή θα απασχολούνται εκατό αστυνομικοί υπάλληλοι και θα πρόκειται για μια απροσπέλαστη εγκατάσταση με ιδιαίτερα αυστηρά μέτρα ασφαλείας και ελέγχου πρόσβασης, καθώς για την είσοδο θα απαιτείται η κατοχή μαγνητικής κάρτας, αλλά και η σάρωση δακτυλικών αποτυπωμάτων. Το εσωτερικό της εγκατάστασης, ώστε να είναι λειτουργική, σχεδιάσθηκε από την αρχιτέκτονα κ. Αλεξάνδρα Παπαγεωργίου, εγγονή του Δημήτρη Πικιώνη, η οποία έχει σχεδιάσει και το αντίστοιχο κέντρο έκδοσης διαβατηρίων των Η.Π.Α.

Έξι χιλιάδες την ημέρα

Η ΚΥΕΔ έχει δυνατότητα παραγωγής 6.000 διαβατηρίων την ημέρα. Ο χρόνος έκδοσης του διαβατηρίου από τη στιγμή που ο πολίτης θα καταθέσει τη σχετική αίτηση είναι πέντε ημέρες. Σε επείγουσες περιπτώσεις όμως, θα υπάρχει η δυνατότητα έκδοσης εντός 24 ωρών. Ας δούμε όμως πώς θα είναι η διαδικασία έκδοσης του νέου διαβατηρίου. Ο ενδιαφερόμενος θα καταθέτει σχετική αίτηση, συνοδευόμενη από φωτογραφία του και φωτοτυπία της Αστυνομικής Ταυτότητας στο Αστυνομικό Τμήμα της περιοχής του, οπουδήποτε στη χώρα, όπου θα γίνεται και άμεσα έλεγχος ταυτοπροσωπίας. Η αίτηση και τα υπόλοιπα πιστοποιητικά θα φθάνουν στο Τμήμα Υποδοχής της ΚΥΕΔ μέσα σε μπλε φάκελο και θα σαρώνονται σε έγχρωμο σκάνερ.

Τα δεδομένα θα προωθούνται στο Τμήμα Εισαγωγής Δεδομένων, όπου τα στοιχεία των σκαναρισμένων εγγράφων θα μεταφέρονται σε προκάτ φόρμες. Οι φόρμες αυτές θα ελέγχονται από το Τμήμα Έγκρισης, το οποίο θα είναι συνδεδεμένο με βάση δεδομένων της Αστυνομίας και θα δίνει την έγκριση ότι ο αιτών χορήγηση διαβατηρίου δεν είναι παράνομος και μπορεί να το λάβει. Στη συνέχεια το διαβατήριό θα εκτυπώνεται. Ακολουθεί ο έλεγχος ποιότητας, ο οποίος, εφόσον το διαβατήριό είναι εντάξει, θα συνοδεύεται από απόδειξη πιστοποίησης. Το διαβατήριό μαζί με την απόδειξη θα αποστέλλονται, μέσα σε πράσινο φάκελο, στο Αστυνομικό Τμήμα όπου έγινε η αίτηση, προκειμένου το πιστοποιητικό να επιδοθεί στον κάτοχό του.

Ενημέρωση

Όποιος καταθέτει αίτηση έκδοσης διαβατηρίου θα μπορεί να ενημερώνεται για την πορεία της διαδικασίας, είτε μέσω Ιντερνετ με εισαγωγή προσωπικού κωδικού είτε μέσω τηλεφώνου είτε με αποστολή SMS στο κινητό του, εάν το ζητήσει.

Ελληνικά βιομετρικά διαβατήρια



Τα βιομετρικά διαβατήρια θα διαθέτουν μικροσίπ με τη φωτογραφία, το αποτύπωμα και άλλα στοιχεία του κατόχου.

Από το Μάιο του 2005 θα αρχίσουν να εκδίδονται τα νέα ελληνικά διαβατήρια, για τα οποία υπάρχουν ήδη αρκετές αντιδράσεις. Τα καινούρια έγγραφα θα είναι ακριβώς όπως τα αμερικανικά και μάλιστα η κατασκευή τους ανατέθηκε σε αμερικανική εταιρεία, η οποία φτιάχνει τα διαβατήρια στις Η.Π.Α.

Όπως αναφέρει η εφημερίδα Έθνος, τις οριστικές αποφάσεις για την έκδοσή τους έλαβε πριν από λίγες ημέρες το υπουργείο Δημόσιας Τάξης έπειτα από αρκετή καθυστέρηση, καθώς έπρεπε να είχε αρχίσει η έκδοσή τους από τον περασμένο Ιούλιο, σύμφωνα με το αρχικό πρόγραμμα.

Τα νέα διαβατήρια θα περιλαμβάνουν αυστηρά προσωπικά δεδομένα, γι' αυτό υπάρχει κίνδυνος να μετατραπούν σε ένα μέσον υπερσύγχρονου ηλεκτρονικού φακελώματος για τους πολίτες όλου του κόσμου στο όνομα κάποιας τρομοκρατικής απειλής.

Πρόκειται για βιομετρικά διαβατήρια, τα οποία θα διαθέτουν μικροσίπ που εκτός από την ψηφιακή εικόνα του κατόχου τους θα περιλαμβάνουν δακτυλικά αποτυπώματα, χρώμα της ίριδας του ματιού και άλλα προσωπικά δεδομένα.

Το αρχηγείο της ΕΛ.ΑΣ. υπέγραψε απόφαση με την οποία κατακυρώθηκε η σύμβαση με αμερικανική εταιρεία που θα φτιάχνει τα διαβατήρια στη χώρα μας. Το κόστος ανέρχεται στο 1,5 εκατ. ευρώ. Πρόκειται για την ίδια εταιρεία που φτιάχνει και τα διαβατήρια των Αμερικανών.

Στους χώρους έκδοσης των νέων διαβατηρίων ελάχιστοι θα έχουν πρόσβαση. Μάλιστα, στον χώρο των προσωπικών δεδομένων δύο άτομα θα έχουν κλειδιά. Και για να ανοίξουν οι πόρτες θα πρέπει να είναι παρόντες και οι δύο και να χρησιμοποιηθούν και τα δύο κλειδιά.

8.12 ΠΙΟ ΑΣΦΑΛΗ ΠΡΟΪΟΝΤΑ ΑΠΟ ΤΗ ΒΙΟΜΗΧΑΝΙΑ ΤΩΝ PASSWORDS

Συνήθως είναι λέξεις ή αριθμοί με συναισθηματική αξία, που να μπορείς να θυμάσαι. Χρησιμοποιούνται πια σχεδόν σε κάθε πλοήγηση στο Διαδίκτυο. Όμως, πόση σιγουριά παρέχουν οι κωδικοί πρόσβασης, τα γνωστά σε όλους password;

Όσο αυξάνονται οι ιστοσελίδες που απαιτούν κωδικό πρόσβασης τόσο μειώνεται η ασφάλεια που αυτός παρέχει. Οι ειδικοί υποστηρίζουν ότι το password αποτελεί, πλέον, μια «εφεύρεση» του παρελθόντος και η αξία του διαρκώς μειώνεται. Τα συστήματα πρόσθετης ασφάλειας βρίσκονται ήδη στην ευρωπαϊκή αγορά.

Από τους πρωτοπόρους στην εφαρμογή τέτοιων συστημάτων είναι οι σκανδιναβικές χώρες, όπου οι τράπεζες και πολλές άλλες επιχειρήσεις χρησιμοποιούν διπλό σύστημα κωδικού. Οι σουηδικές τράπεζες, για παράδειγμα, στέλνουν στους πελάτες τους ειδικές κάρτες με κωδικούς.

Κάθε φορά που ο πελάτης θέλει να πραγματοποιήσει κάποια ηλεκτρονική συναλλαγή, πληκτρολογεί το password που έχει ο ίδιος ορίσει και στη συνέχεια τους κωδικούς που περιέχει η κάρτα της τράπεζας. Οι κάρτες ανανεώνονται σε τακτά χρονικά διαστήματα, καθώς οι κωδικοί που περιέχει καθεμιά από αυτές είναι μιας χρήσης.

Η MasterCard International δοκιμάζει ανάλογα συστήματα στη Βρετανία, στη Γερμανία και στη Βραζιλία: κάρτες με «έξυπνα» τσιπ, τις οποίες ο χρήστης περνάει από ειδικό μηχάνημα, για να αποκτήσει ένα password μιας χρήσης.

Στη Σιγκαπούρη, οι πελάτες των τραπεζών που θέλουν να ανοίξουν νέους λογαριασμούς για μεταφορά κεφαλαίου, αποκτούν δεύτερο password μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου ή με SMS στο κινητό τους τηλέφωνο.

Με ανάλογο τρόπο λειτουργούν τα βιομετρικά συστήματα, με τη διαφορά ότι το ένα ή και τα δύο passwords αντικαθίστανται από δακτυλικό αποτύπωμα ή εικόνα της ίριδας του ματιού. Μόνο που, σε αυτή την περίπτωση, οι ηλεκτρονικοί υπολογιστές πρέπει να είναι εξοπλισμένοι με ειδικό σκάνερ που «διαβάζει» την ίριδα ή το δακτυλικό αποτύπωμα.

Η βελγική εταιρεία Vasco Data Security International λανσάρει μια συσκευή σε μέγεθος μπρελόκ. Ο χρήστης πληκτρολογεί το password που έχει επιλέξει για κάθε μια από τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί και η συσκευή «παράγει» ένα δεύτερο password, μοναδικό για κάθε περίπτωση.

Περίπλοκος κωδικός

Έως ότου η χρήση τέτοιων ασφαλείας γίνει... τρόπος ζωής για όλες τις ηλεκτρονικές υπηρεσίες, υπάρχουν κάποια προγράμματα, όπως το Norton Password Manager της Symantec ή το Keychain της Apple, τα οποία αποθηκεύουν όλους τους κωδικούς πρόσβασης του χρήστη σε κρυπτογραφημένη μορφή. Αν, βέβαια, χάσεις ή ξεχάσεις τον κεντρικό κωδικό πρόσβασης στο πρόγραμμα, χάνεις αυτομάτως όλους τους κωδικούς!

Οι ειδικοί συμβουλεύουν τους χρήστες τους - κυρίως για υπηρεσίες που σχετίζονται με οικονομικές συναλλαγές - να επιλέγουν όσο το δυνατό πιο περίπλοκα passwords.

Συνιστούν συνδυασμούς γραμμάτων και αριθμών, ώστε η... ζωή των επιτηδίων να γίνει πιο δύσκολη, στην περίπτωση που επιχειρήσουν να εισβάλουν στα προσωπικά στοιχεία κάποιου.

«Επικίνδυνο» θεωρείται και αυτό που συνηθίζουν πολλοί χρήστες του Ίντερνετ, να χρησιμοποιούν δηλαδή ένα password για όλες τις υπηρεσίες. Και αυτό γιατί, από τη στιγμή που θα βρουν τη λέξη - κλειδί οι παράνομοι του Διαδικτύου, αποκτούν πρόσβαση σε όλα τα στοιχεία του χρήστη.

Από την άλλη, είναι ανθρωπίνως αδύνατο να θυμάται κανείς δεκάδες κωδικούς πρόσβασης και μάλιστα περίπλοκους.

8.13 ΓΛΑΥΚΩΠΙΣ: Σύστημα Ταυτοποίησης και Αναγνώρισης βασισμένο σε Βιομετρικά Χαρακτηριστικά για Εξουσιοδότηση Προσπέλασης και Έλεγχο Φυσικής Πρόσβασης



Αντικείμενο του έργου είναι η υλοποίηση ολοκληρωμένου συστήματος για διενέργεια ελέγχων με σκοπό την αναγνώριση και ταυτοποίηση ανθρώπων που επιθυμούν πρόσβαση σε φυσικούς χώρους, προσπέλαση σε πληροφοριακούς πόρους, ή εικονική πρόσβαση για χειρισμό συσκευής ή συστήματος. Οι διαδικασίες ελέγχου που προτείνονται βασίζονται στην επεξεργασία και ανάλυση των βιομετρικών χαρακτηριστικών.

Το κύριο πλεονέκτημα που παρέχει ο έλεγχος πρόσβασης που βασίζεται σε βιομετρικά χαρακτηριστικά είναι η απόλυτη ταυτοποίηση του έχοντος το δικαίωμα πρόσβασης με το άτομο που την επιθυμεί. Αυτό επιτυγχάνεται σε αντιδιαστολή με άλλους ελέγχους που βασίζονται σε PINs, κάρτες, κωδικούς πρόσβασης, κ.λπ. των οποίων τη γνώση ή κατοχή δύναται να την έχει διαφορετικό άτομο και με αυτό τον τρόπο να υφίσταται ουσιαστική παραπλάνηση του συστήματος.

Οι τεχνολογίες στις οποίες θα βασιστεί η ανάπτυξη του έργου αναφέρονται στον έλεγχο πρόσβασης που βασίζεται στα δακτυλικά αποτυπώματα, στη γεωμετρία παλάμης, στην ίριδα και στην αναγνώριση προσώπου. Η μελέτη των τεχνολογιών θα έχει ως βασικό σκοπό τη γενικότερη αξιολόγησή τους όπως και των σχετικών τεχνικών και μεθοδολογιών που εφαρμόζονται αλλά και ως στόχο την υλοποίηση πρωτότυπων ή η βελτιστοποίηση υπάρχοντων αλγορίθμων όπου αυτό απαιτείται. Επίσης, θα αξιολογηθούν υπάρχοντα υποσυστήματα που βασίζονται στις τεχνολογίες αναφοράς με σκοπό την πιθανή ενσωμάτωση δυνατοτήτων ή συστατικών τμημάτων τους στο τελικό προϊόν του έργου.

Στα κύρια στάδια του έργου θα υλοποιηθούν και θα ολοκληρωθούν ως πλήρες σύστημα, τα υποσυστήματα υλικού (συσκευές καταγραφής, σταθμοί πρόσβασης, διακομιστές) και του λογισμικού ανάλυσης χαρακτηριστικών και θα προκύπτει η δυνατότητα παροχής του συνόλου των επιθυμητών λειτουργιών. Ιδιαίτερη έμφαση θα δοθεί στην ανοικτή αρχιτεκτονική και στη δυνατότητα παραμετροποίησης των συστημάτων αυτών.

Η ανάπτυξη του ειδικού λογισμικού διαχείρισης και λειτουργίας των συστημάτων με δυνατότητες καθορισμού ειδικών κριτηρίων πρόσβασης αποτελεί το βασικό αντικείμενο του έργου και συνιστά και την ουσιαστική καινοτομία της πρότασης καθώς ολοκληρωμένα συστήματα τέτοιων προδιαγραφών δεν είναι διαθέσιμα. Επιπρόσθετα, το σύστημα θα παρέχει δυνατότητες συνδυασμένου ελέγχου πρόσβασης βασισμένου και σε λοιπά κριτήρια που δε σχετίζονται με βιομετρικά χαρακτηριστικά όπως, π.χ., γνώση κωδικού πρόσβασης, κατοχή έξυπνης κάρτας, κ.λπ. Ο συνδυασμένος έλεγχος θα επεκτείνεται και στον σειριακό ή παράλληλο έλεγχο διαφορετικών βιομετρικών χαρακτηριστικών.

Γενικά, το έργο θα καλύψει τα συστατικά μέρη ενός συστήματος ελέγχου που αφορούν στο λογισμικό επεξεργασίας δεδομένων και απόδοσης ειδικών κριτηρίων ταξινόμησης, στη βάση δεδομένων και το λογισμικό προσπέλασης σε αυτήν και στο ειδικό λογισμικό διαχείρισης του συστήματος, παραμετροποίησης σύμφωνα με τα απαιτούμενα κριτήρια και συνολικού ελέγχου των λοιπών εμπλεκόμενων μονάδων.

Τα επιδιωκόμενα αποτελέσματα του έργου είναι:

- Η ανάλυση και μελέτη του εξοπλισμού καταγραφής βιομετρικών χαρακτηριστικών
- Η μελέτη μεθοδολογιών, ο σχεδιασμός πρωτότυπων και η βελτιστοποίηση υπάρχοντων αλγορίθμων ανάλυσης και κωδικοποίησης βιομετρικών χαρακτηριστικών
- Η ανάπτυξη συστατικών λογισμικού που θα βασίζονται στους αλγόριθμους αυτούς
- Η κατά περίπτωση ενσωμάτωση τμημάτων από υπάρχοντα υποσυστήματα
- Η μελέτη του ευρύτερου πεδίου ώστε να διασφαλίζεται η συμβατότητα με άλλα συστήματα και μεθόδους ελέγχου πρόσβασης
- Ο σχεδιασμός ολοκληρωμένου συστήματος το οποίο θα ενσωματώνει τις συσκευές και το λογισμικό, θα ορίζει τις παραμέτρους και θα συνιστά πλήρη λύση διαθέσιμη για εμπορική αξιοποίηση - Ο στόχος αυτός είναι ο βασικός και από τον βαθμό επίτευξής του θα αξιολογηθεί η συνολική επιτυχία του Έργου.
- Η σύνταξη πλάνου αξιοποίησης και εμπορικής εκμετάλλευσης.

Η υλοποίηση του συστήματος, θεωρείται ότι θα προσφέρει ένα καινοτομικό προϊόν του οποίου η εμπορική προώθηση αναμένεται ότι θα αποδώσει σε σύντομο χρονικό διάστημα δεδομένων της αναγκών που υπάρχουν στο πεδίο αναφοράς και της μη ύπαρξης εναλλακτικών ολοκληρωμένων συστημάτων τέτοιου τύπου.

8.14 VERICHIP :ΕΜΦΥΤΕΥΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΣΤΟ ΑΝΘΡΩΠΙΝΟ ΣΩΜΑ



Ίσως κάποια στιγμή να έχουμε συναντήσει το τεχνολογικό επίτευγμα που θα περιγράψουμε σε σενάριο επιστημονικής φαντασίας, όμως σήμερα η εμφύτευση μικροεπεξεργαστή στο ανθρώπινο σώμα με σκοπό την εξακρίβωση ιδιαίτερων ατομικών χαρακτηριστικών είναι μια πραγματικότητα.

Η εταιρία Applied Digital Solutions, μια εταιρία που επικεντρώνεται στην ανάπτυξη προηγμένων τεχνολογικά

μικροσκοπικών συστημάτων παρακολούθησης και ειδοποίησης, ανακοίνωσε πρόσφατα ότι είναι έτοιμη να διαθέσει προς χρήση την επαναστατική τεχνολογία VeriChip. Η δημιουργία του VeriChip προσδίδει μια νέα διάσταση στην τεχνολογία των μικροεπεξεργαστών και έρχεται να προσθέσει σε αυτή μια νέα εφαρμογή πέρα από τις ήδη υπάρχουσες. Έτσι, λοιπόν, είναι πλέον εφικτή η εμφύτευση ενός μικροεπεξεργαστή στο ανθρώπινο σώμα, που θα εμπεριέχει αποθηκευμένα δεδομένα εξακρίβωσης της ταυτότητας του ατόμου ή διάφορες άλλες ιατρικές πληροφορίες, όπως για παράδειγμα το ιατρικό ιστορικό ενός προσώπου και λεπτομέρειες για τεχνικά όργανα που πιθανόν του έχουν εμφυτευτεί.

Το VeriChip είναι ένας πολύ περιορισμένων διαστάσεων (12mm x 2,1mm) μηχανισμός ραδιοσυχνότητας, που ο καθένας περιέχει το δικό του κωδικό αναγνώρισης. Το άλλο απαραίτητο στοιχείο για την ολοκλήρωση της συγκεκριμένης μεθόδου εξακρίβωσης, είναι ένας φορητός ηλεκτρονικός ανιχνευτής, που «διαβάζει» τις αποθηκευμένες πληροφορίες από το chip. Χρησιμοποιώντας λοιπόν αυτόν τον ανιχνευτή, μεταβιβάζουμε ενέργεια διάμεσου του ανθρώπινου σώματος και ενεργοποιείται ο αδρανής μέχρι τότε μικροεπεξεργαστής, εκπέμποντας ένα RF σήμα. Έτσι, μεταδίδεται ο αριθμός εξακρίβωσης και άλλες πληροφορίες που είναι αποθηκευμένες στο chip. Τα αποτελέσματα μπορούν να προβληθούν στον ανιχνευτή, υπάρχει όμως και η δυνατότητα αποστολής τους μέσω τηλεφωνικών γραμμών και Internet σε μια βάση δεδομένων που επεξεργάζεται αποκλειστικά εξουσιοδοτημένο προσωπικό. Η διαδικασία εμφύτευσης του VeriChip είναι αρκετά απλή και απαιτεί μόνο τοπική αναισθησία και μία μικροσκοπική τομή.

Όπως προαναφέρθηκε, κύρια εφαρμογή του VeriChip αποτελεί η αναγνώριση ιατρικών ατομικών στοιχείων. Είναι γεγονός ότι πάρα πολλά τεχνικά ιατρικά όργανα εμφυτεύονται χειρουργικά κάθε χρόνο σε ασθενείς. Τέτοια όργανα όπως είναι τα τεχνικά αρθρώματα, βηματοδότες ή άλλα ορθοπεδικά βοηθήματα, πολλές φορές είναι απαραίτητα για την επιβίωση των ανθρώπων, ενώ μπορούν να συμβάλουν σημαντικά στη βελτίωση της ποιότητας ζωής τους. Κατά καιρούς όμως απαιτούν διάφορες ρυθμίσεις, επιδιορθώσεις ή και αντικατάσταση. Σε τέτοιες καταστάσεις το μικροσκοπικό VeriChip μπορεί να παίξει σημαντικό ρόλο, αφού υπάρχει δυνατότητα τοποθέτησής του μέσα στο δέρμα, ακριβώς πάνω από τα εμφυτευμένα ιατρικά όργανα, ώστε να παρέχει υποστήριξη στους ασθενείς παρέχοντας κρίσιμες ιατρικές πληροφορίες για τις εμφυτευμένες διατάξεις στους κατασκευαστές τους με μια ασφαλή και γρήγορη μέθοδο.

Το VeriChip αποτελεί μια αξιόπιστη πηγή δεδομένων που αφορούν τον ασθενή, οι οποίες περιλαμβάνουν το όνομα και την ιατρική του κατάσταση, καθώς και πληροφορίες για τυχόν αναγκαίες ρυθμίσεις του εμφυτευμένου οργάνου. Δεν αποκλείεται όμως στο μέλλον η χρήση αυτή να επεκταθεί, αποθηκεύοντας πλήρη ιατρικά στοιχεία στο chip, ώστε αυτά να μπορούν να ανακτηθούν εσπευσμένα σε μια ενδεχόμενη επείγουσα κατάσταση. Εκτός από τα ευεργετικά αποτελέσματα που μπορεί να έχει η εμφύτευση του VeriChip στο σώμα κάποιου ασθενή, μπορεί να χρησιμοποιηθεί και ως σύστημα εξακρίβωσης ταυτότητας. Άλλωστε, η εξακρίβωση της ταυτότητας ενός ατόμου για εφαρμογές που απαιτείται ελεγχόμενη πρόσβαση με ασφάλεια και ταχύτητα, είναι ένα ζήτημα που απασχολεί πολλούς το τελευταίο διάστημα. Έτσι, έχουν αναπτυχθεί διάφορες μέθοδοι, με πιο εξελιγμένη τη χρήση βιομετρικών συστημάτων αναγνώρισης των μοναδικών φυσικών ανθρώπινων χαρακτηριστικών όπως τα δαχτυλικά αποτυπώματα, η ίριδα του ματιού και το σχήμα του προσώπου.

Το VeriChip, βασιζόμενο στη σύγχρονη τεχνολογία των μικροεπεξεργαστών, μπορεί να αποτελέσει ένα εναλλακτικό μέσο εξακρίβωσης της ταυτότητας ενός ατόμου, όπου η περίπτωση απώλειας, κλοπής ή παραποίησης δεδομένων εξαλείφεται. Τη συγκεκριμένη χρήση του VeriChip μπορούμε να εκμεταλλευτούμε σε ήδη υπάρχουσες περιοχές, όπου υπάρχει η ανάγκη εξακρίβωσης της ταυτότητας ή και σε εφαρμογές έρευνας και διάσωσης, μιας και πρόθεση των κατασκευαστών είναι να παράγουν στο μέλλον μια προηγμένη έκδοση του VeriChip, όπου θα μπορεί να εκμεταλλευτεί ένα παγκόσμιο σύστημα προσδιορισμού θέσης, όπως το GPS. Καθώς το όλο εγχείρημα άρχισε να γίνεται γνωστό, ιδιαίτερα στις ΗΠΑ, άρχισαν ήδη να διατυπώνονται ορισμένες ενστάσεις για τη χρήση του κυρίως σε θρησκευτικό επίπεδο, συσχετίζοντας το VeriChip με προφητείες της Αποκάλυψης του Ιωάννη, που αναφέρονται στη σήμανση όλων των ανθρώπων με συγκεκριμένο αριθμό, που υποχρεωτικά θα φέρουν όλοι, ώστε να εκτελούν τις συναλλαγές τους. Οι υπεύθυνοι αντικρούοντας αυτό τον ισχυρισμό υποστήριξαν ότι το VeriChip δεν θα χρησιμοποιείται για οικονομικές συναλλαγές, παρά μόνο για ιατρικές καταγραφές και επείγουσες ανάγκες, όπως, για παράδειγμα, περιπτώσεις απαγωγών και προπάντων, η απόφαση της τοποθέτησης ή όχι του VeriChip σε κάποιον θα ανήκει αποκλειστικά σε αυτόν.

8.15 ΛΟΓΙΣΜΙΚΟ ΕΠΙΤΡΕΠΕΙ ΣΤΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ ΝΑ ΒΛΕΠΟΥΝ



Οι ερευνητές της εταιρείας υπολογιστών Intel υποστηρίζουν ότι ο λογισμικός κώδικας που ανέπτυξαν θα δώσει μια νέα διάσταση στην αλληλεπίδραση ανθρώπου και υπολογιστή.

Μέχρι τώρα, οι εφαρμογές όρασης για υπολογιστές περιοριζόντουσαν σε δύο διαστάσεις. Όμως ο νέος «στερεοσκοπικός» κώδικας της Intel επιτρέπει στους υπολογιστές να αναγνωρίζουν το 'βάθος' όπως τις 'επίπεδες' εικόνες, έτσι ώστε να μπορούν να διακρίνουν μεμονωμένα αντικείμενα και επιφάνειες σε ένα χώρο.

Ο νέος στερεοσκοπικός κώδικας είναι μία ανοιχτή εφαρμογή πάνω στην οποία μπορούν να οικοδομηθούν εμπορικές εφαρμογές. Ο κώδικας υποστηρίζει τις εφαρμογές όρασης όπως η αναγνώριση χειρονομιών, ο εντοπισμός αντικειμένων και η αναγνώριση προσώπων.

Οι ερευνητές λένε ότι στο μέλλον αυτές οι τεχνολογίες μπορεί να οδηγήσουν σε περισσότερο επιτηδευμένες μεθόδους διασύνδεσης υπολογιστών, καλύτερα συστήματα ασφάλειας και βιομετρικά εργαλεία αλλά και να βελτιώσουν τις μεθόδους ρομποτικής και εξερεύνησης του διαστήματος.

ΚΕΦΑΛΑΙΟ 9



BioMetric
Systems

ΒΙΟΜΕΤΡΙΚΑ
ΣΥΣΤΗΜΑΤΑ...Η ΩΡΑ
ΤΗΣ ΑΠΟΤΙΜΗΣΗΣ

Έχοντας αναλύσει στις προηγούμενες σελίδες όλες τις βιομετρικές μεθόδους, έρχεται πλέον αναπόφευκτα η ώρα της αποτίμησης. Θα προσπαθήσουμε να απαντήσουμε σε δύο μεγάλα ερωτήματα που μάλλον απασχολούν όσους μας ακολούθησαν ως εδώ: Πώς μπορεί η Βιομετρική να επηρεάσει τη ζωή μας από εδώ και πέρα, και, τελικά, ποιο είναι το καλύτερο βιομετρικό σύστημα;

Ας ξεκινήσουμε λοιπόν από το δεύτερο ερώτημα. Η αποδοτικότητα των διαφόρων βιομετρικών συστημάτων εκτιμάται με βάση τέσσερα κριτήρια: την προσπάθεια που απαιτούν από το χρήστη, το πόσο "διακριτικά" είναι απέναντί του, το κόστος τους, και το επίπεδο ακριβείας που έχουν. Τα δύο πρώτα από αυτά τα κριτήρια (προσπάθεια από το χρήστη και διακριτικότητα), ονομάζονται κριτήρια χρήστη και είναι αυτά που διαμορφώνουν τον πολύ σημαντικό παράγοντα "αποδοχή από το κοινό". Τα δύο άλλα (κόστος και ακρίβεια) είναι τα τεχνολογικά κριτήρια.

9.1 Η ΑΝΑΛΥΣΗ ZEPHYR

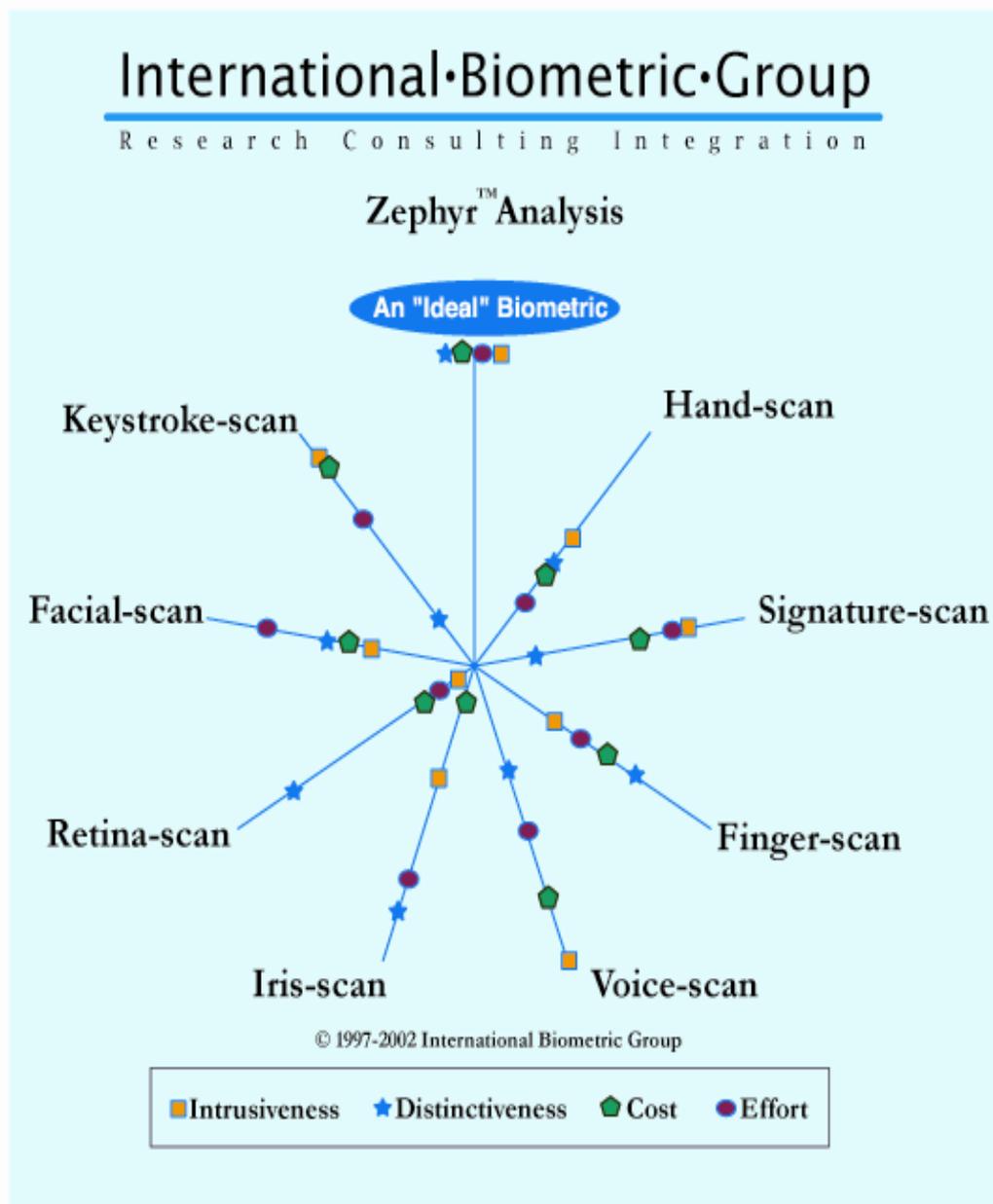
Η ανάλυση Zephyr του International Biometric Group (<http://www.biometricgroup.com>) είναι μια πολύ χρήσιμη μέθοδος σύγκρισης των κυριότερων βιομετρικών συστημάτων σε σχέση με αυτά τα τέσσερα κριτήρια, της οποίας τα αποτελέσματα συγκεντρώθηκαν σε δύο διαγράμματα (γνωστά και ως διαγράμματα Zephyr). Το πρώτο διάγραμμα, το οποίο μπορείτε να δείτε και στο σχήμα που συνοδεύει το άρθρο, έχει τις απόλυτες επιδόσεις των τεσσάρων κριτηρίων αντιστοιχισμένες στις κορυφές ενός ρόμβου. Με άλλα λόγια, ένα ιδανικό βιομετρικό σύστημα θα σχημάτιζε ένα τέλειο ρόμβο, ενώ ένα βιομετρικό σύστημα με μηδενικές επιδόσεις θα συρρικνωνόταν σε ένα σημείο στο κέντρο του ρόμβου. Χρησιμοποιώντας το υπόμνημα μπορείτε να δείτε ποια τετράπλευρα αντιπροσωπεύουν συγκεκριμένα βιομετρικά συστήματα. Το δεύτερο διάγραμμα, περιέχει τις ίδιες ακριβώς πληροφορίες με τη διαφορά ότι στις κορυφές του σχήματος αυτή τη φορά βρίσκονται τα βιομετρικά συστήματα και όχι τα κριτήρια. Αποφασίσαμε να φιλοξενήσουμε το πρώτο από τα δύο διαγράμματα, γιατί μάλλον είναι πιο παραστατικό για τον αναγνώστη που θέλει να συγκρίνει τα συστήματα μεταξύ τους (αν θέλετε να ρίξετε μια ματιά και στο δεύτερο διάγραμμα επισκεφθείτε τη διεύθυνση www.biometricgroup.com/a_biometric_0/zephyr.htm).

Επίσης, μην παραξενευτείτε που στο διάγραμμα θα βρείτε και το σύστημα των PIN. Παρόλο που δεν είναι βιομετρικό σύστημα, συμπεριλήφθηκε ως μέτρο σύγκρισης, και ως ο κύριος σημερινός ανταγωνιστής των βιομετρικών συστημάτων.

Η γραφική αυτή αναπαράσταση της σύγκρισης των διαφόρων συστημάτων, επιβεβαιώνει με τον καλύτερο τρόπο το ρητό "μια εικόνα αξίζει όσο χίλιες λέξεις". Προσέξτε ότι τα συστήματα με πολύ υψηλή ακρίβεια (όπως η παθητική εξέταση ίριδας, ή η εξέταση αμφιβληστροειδούς) έχουν τις χειρότερες επιδόσεις στο κόστος. Αρκετά λογικό, αφού χρησιμοποιούν την τελειότερη τεχνολογία. Όπως είναι αναμενόμενο, ισχύει και το αντίστροφο: Τα φτηνά συστήματα (όπως αναγνώριση φωνής) πάσχουν από άποψη ακριβείας.

Επίσης, άξιο προσοχής είναι το τετράπλευρο της διακρίβωσης υπογραφής. Πάρα πολύ καλό στις τρεις κορυφές, αλλά στο κριτήριο της ακριβείας είναι τελευταίο (ο μικρός μαύρος ρόμβος που βλέπετε μετά ανήκει στο σύστημα των PIN, το οποίο δεν συγκαταλέγεται στα βιομετρικά συστήματα).

Τέλος, στο τετράπλευρο του αμφιβληστροειδούς, η κορυφή της διακριτικότητας κοντεύει να ταυτιστεί με το κέντρο του ρόμβου, προφανώς επειδή η διαδικασία στην οποία υποβάλλεται ο χρήστης τον κάνει να νοιώθει υπερβολικά άβολα.



ΤΟ ΚΑΛΥΤΕΡΟ ΒΙΟΜΕΤΡΙΚΟ ΣΥΣΤΗΜΑ

Αν η μελέτη του διαγράμματος μάλλον σας μπέρδεψε παρά σας βοήθησε στην αναζήτηση του καλύτερου βιομετρικού συστήματος, αυτό συνέβη επειδή στην πραγματικότητα η απάντηση στο ερώτημα αυτό δεν είναι μόνο μία, αλλά εξαρτάται στενά από την εφαρμογή για την οποία πρόκειται να χρησιμοποιηθεί το συγκεκριμένο σύστημα. Για παράδειγμα, σκεφτείτε μία πυρηνική εγκατάσταση. Το μόνο κριτήριο που μπορεί να ισχύσει εδώ από τα τέσσερα που αναφέραμε προηγουμένως είναι σίγουρα η ασφάλεια. Κόστος, προσπάθεια από το χρήστη ή διακριτικότητα δεν έχουν καμία απολύτως σημασία. Ποιος χρήστης του συστήματος θα μπορούσε να παραπονεθεί ότι το σύστημα τον κουράζει ή τον προσβάλλει; Από την άλλη πλευρά, στην περίπτωση ενός συστήματος ελέγχου ταυτότητας σε αεροδρόμιο, αυτομάτως τα κριτήρια αλλάζουν. Αν το σύστημα αφιέρωνε 10 λεπτά για κάθε επιβάτη, το πιο πιθανό είναι οι περισσότεροι από αυτούς να χάνανε την πτήση τους. Εκεί, η προσπάθεια που πρέπει να καταβάλλει ο χρήστης, η ευχρηστία δηλαδή του συστήματος, είναι από τα σημαντικότερα κριτήρια.

Αν θέλετε να βρείτε το καλύτερο βιομετρικό σύστημα λοιπόν, πρώτα καθορίστε την εφαρμογή που θέλετε να το εφαρμόσετε, εξακριβώστε τις προτεραιότητές της, και μετά χρησιμοποιήστε τα διαγράμματα Zephyr για να το εντοπίσετε.

ΤΙ ΜΕΛΛΕΙ ΓΕΝΕΣΘΑΙ

Αν και πάντα, το να μιλάς για το μέλλον (ιδιαίτερα το κοντινό) περιέχει τον κίνδυνο να διαψευστείς, οι κρίσεις που θα αποτολμήσουμε στις επόμενες παραγράφους έχουν αρκετά ισχυρές βάσεις. Παρακάμπτοντας την αυτονόητη αύξηση της χρήσης βιομετρικών μεθόδων για ποινικούς σκοπούς, ξεκινάμε αμέσως με τα υπόλοιπα.

Κατ' αρχήν, θα πρέπει να θεωρήσουμε σχεδόν σίγουρο ότι σε λίγα χρόνια από σήμερα, κάθε πιστωτική ή άλλου είδους τραπεζική κάρτα θα συνοδεύεται από βιομετρικό δείγμα. Ιδιαίτερα ευάλωτο στην απάτη το σημερινό σύστημα των PIN, κάποια στιγμή στο κοντινό μέλλον θα ενισχυθεί με κάποιο βιομετρικό σύστημα, όπως εξέταση ίριδας ή δακτυλικού αποτυπώματος.

Η ασφάλεια στο Internet είναι άλλο ένα θέμα, στο οποίο η συμμετοχή των βιομετρικών συστημάτων αναμένεται να είναι μεγάλη. Καθώς ο βασικός εξοπλισμός για μεθόδους όπως η αναγνώριση φωνής ή γεωμετρίας προσώπου υπάρχει ήδη στα περισσότερα υπολογιστικά συστήματα, μένει μόνο να αναπτυχθεί και η κατάλληλη υποδομή. Είναι λογικό να υποθέσουμε ότι κάτι τέτοιο θα ξεκινήσει από τα μεγαλύτερα ηλεκτρονικά καταστήματα και θα προχωρήσει και στα μικρότερα.

Οι βιομετρικές μεθόδους θα συμβάλλουν επίσης τα μέγιστα στην καταπολέμηση της τηλεφωνικής απάτης. Όλο και περισσότερο το τηλέφωνο χρησιμοποιείτε ως μέσο επιβεβαίωσης ταυτότητας για διαφόρων ειδών συναλλαγές. Η ανάπτυξη της μεθόδου αναγνώρισης φωνής μπορεί να εξαφανίσει κάθε είδους φαινόμενα με σκοπό την απάτη.

Όσον αφορά στην εφαρμογή βιομετρικών μεθόδων σε προσωπικούς υπολογιστές, όπως διαπιστώσατε και μόνοι σας είναι σήμερα μια πραγματικότητα. Το πλήθος των προϊόντων που συναντήσαμε στις σελίδες αυτού του αφιερώματος άλλωστε,

άμεσα εφαρμόσιμων σε οποιοδήποτε σύστημα και με ελάχιστο κόστος, αποτελεί την καλύτερη απόδειξη γι' αυτό.

Τα βιομετρικά συστήματα περιμένουν να χρησιμοποιηθούν σε ένα σωρό από τις καθημερινές δραστηριότητές μας, σε ένα μέλλον όχι και τόσο μακρινό. Ήδη έχουν κυκλοφορήσει προϊόντα όπως βιομετρικές κλειδαριές κατοικιών ή αυτοκινήτων, που μας "φωνάζουν" ότι τα συμβατικά κλειδιά έχουν αποκτήσει ένα σημαντικό αντίπαλο. Πολλές εταιρείες θα προτιμήσουν κάποιο βιομετρικό σύστημα ελέγχου πρόσβασης των υπαλλήλων τους από το παραδοσιακό και παρωχημένο σύστημα του "χτυπήματος" των καρτών. Τέλος, ο έλεγχος σε μέρη όπως αεροδρόμια και σύνορα θα βελτιωθεί σημαντικά.

Αν κάποια από τα παραπάνω φαίνονται κάπως υπερβολικά, δεν πρέπει να ξεχνάμε κάτι πολύ σημαντικό: Ότι η απαραίτητη τεχνολογία είναι υπαρκτή, χειροπιαστή, διαθέσιμη στον οποιοδήποτε ενδιαφέρεται να δοκιμάσει τα αποτελέσματά της. Αυτό σημαίνει ότι η Βιομετρική έχει όλες τις προϋποθέσεις να εισχωρήσει σε κάθε πτυχή της καθημερινής μας ζωής, να μας βοηθήσει να την οργανώσουμε καλύτερα, αλλά και να προστατεύσουμε τους εαυτούς μας και την περιουσία μας με περισσότερη αποτελεσματικότητα. Αν και η ολοκληρωτική εξάλειψη της απάτης (με οποιαδήποτε μορφή), δεν παύει να είναι μια ουτοπία στο σημερινό κόσμο, η Βιομετρική μας δίνει τα εργαλεία για να την περιορίσουμε στο ελάχιστο, και αυτό είναι σίγουρα η μεγαλύτερη προσφορά της.

9.2 ΔΕΛΤΙΟ ΤΑΥΤΟΤΗΤΑΣ...ΤΟ ΑΝΘΡΩΠΙΝΟ ΣΩΜΑ

Η βιομετρία καταγράφει το πρόσωπο, την παλάμη, την ίριδα του ματιού σας και τα χρησιμοποιεί ως μοναδικά στοιχεία αναγνώρισης «Σας παρακαλώ, πλησιάστε λίγο», λέει μία μηχανική γυναικεία φωνή, παράδοξα θερμή, την ίδια ώρα που μια κάμερα εστιάζει στο μάτι του επισκέπτη στη χρηματιστηριακή εταιρεία Thales Fund Management της Νέας Υόρκης, στον 45ο όροφο ενός εβένινου πύργου στο Μανχάταν. «Λυπάμαι. Δεν σας αναγνωρίζουμε. Δεν είστε αναγνωρίσιμος», λέει αυτή η χωρίς σώμα φωνή. «Μας αρέσει η αίσθηση της επιστημονικής φαντασίας, κάτι σαν το Star Trek, ενώ και ο επισκέπτης εντυπωσιάζεται», εξηγεί η Λόρελ Γκαλγκάνο, υπεύθυνη του προηγμένου συστήματος ασφαλείας.

Τα βιομετρικά συστήματα εντυπωσιάζουν μεγάλη μερίδα του επιχειρηματικού κόσμου. Τα σκάνερ της ίριδας είναι από τα πιο δημοφιλή, όπως αναφέρει σε άρθρο του το περιοδικό US News and World Report. Τα συστήματα αυτά που καταγράφουν την ίριδα, το δακτυλικό αποτύπωμα ή το σχήμα του προσώπου και του χεριού, μετατρέπουν τα βιολογικά χαρακτηριστικά σε ταυτότητα αναγνώρισης. Ακόμα και πριν από τις επιθέσεις της 11ης Σεπτεμβρίου, η βιομηχανία που παράγει βιομετρικά συστήματα αναπτυσσόταν ραγδαία, καθώς οι σαρωτές και το αντίστοιχο λογισμικό γίνονταν φθηνότερα και πιο αποτελεσματικά.

Οι κατασκευάστριες εταιρείες του χώρου εκτιμούν ότι οι πωλήσεις έφθασαν τα 170 εκατομμύρια δολάρια ετησίως για το 2001, παρουσιάζοντας αύξηση της τάξης του 70% σε σχέση με το προηγούμενο έτος. Οι πιο πρόσφατες εκτιμήσεις ανεβάζουν τις πωλήσεις στο ύψος του ενός δισεκατομμυρίου δολαρίων μέχρι το 2004, αποτέλεσμα των νέων συνθηκών ασφαλείας στα αεροδρόμια και σε άλλους χώρους υψηλής επιτήρησης.

Χιλιάδες ανάλογα συστήματα δοκιμάζονται ή χρησιμοποιούνται ήδη από επιχειρήσεις. Πολλοί εργαζόμενοι δεν κτυπούν πια κάρτα στην είσοδο ή στην έξοδο· απλώς τοποθετούν την παλάμη τους σε ειδική οθόνη. Η παρουσία χιλιάδων μαθητών στα γεύματα των σχολικών συγκροτημάτων επιβεβαιώνεται με τον ίδιο τρόπο. Σε μερικά αμερικανικά αεροδρόμια σκάνερ προσώπου ελέγχουν τους επιβάτες, ενώ η υπηρεσία λαχείων της Νέας Υόρκης χρησιμοποιεί ανιχνευτές ίριδας για την είσοδο υπαλλήλων της σε ειδικό χώρο, όπου φυλάσσεται το λογισμικό της επιχείρησης.

Βιομετρικά "Λουκέτα"

Παρανοήσατε; Ασφαλίστε τα δεδομένα σας με... βιομετρικούς τρόπους

Οι κωδικοί διαρρέουν ή σπάνε, τα κλειδιά και οι κάρτες χάνονται ή αντιγράφονται. Όταν η ασφάλεια των δεδομένων μας είναι κρίσιμης σημασίας, οι συμβατικές μέθοδοι αποδεικνύονται... ανασφαλείς. Πώς θα διαφυλάξουμε τα πολύτιμα αρχεία μας από τα ξένα χέρια;

Όπως πολλά πράγματα, έτσι και η λεγόμενη «βιομετρική ασφάλεια» είναι γνωστή και διαδεδομένη στο εξωτερικό, αλλά στη χώρα μας είτε ο κόσμος δεν τη γνωρίζει, είτε τη βλέπει με πολύ στραβό μάτι. Κι όμως, πρόκειται για μία αρκετά απλή και φθηνή μέθοδο που εξασφαλίζει με τον καλύτερο τρόπο το απόρρητο των προσωπικών σας ηλεκτρονικών αρχείων.

Βιομετρική ασφάλεια

Το τρίπτυχο της ασφάλειας έχει να κάνει με τρεις ερωτήσεις: «τι ξέρεις;», «τι έχεις;», «τι είσαι;», κατά σειρά επιπέδου ασφάλειας. Προφανώς, η πρώτη αντιστοιχεί στα passwords και η δεύτερη στα φυσικά κλειδιά, τις κάρτες κ.λπ. Πώς απαντιέται όμως το τρίτο ερώτημα; Μα... με τα χαρακτηριστικά του ίδιου μας του εαυτού. Το μεγαλύτερο επίπεδο ασφάλειας καλύπτεται με την αναγνώριση των αυστηρά προσωπικών μας χαρακτηριστικών, όπως των δακτυλικών μας αποτυπωμάτων, της ίριδας του ματιού μας, της φωνής μας, του σχήματος της παλάμης ή του προσώπου μας. Ο έλεγχος και η ταυτοποίηση αυτών των χαρακτηριστικών ορίζουν και το ανώτερο επίπεδο ασφάλειας. Τα δε συστήματα που αναλαμβάνουν αυτές τις διαδικασίες ονομάζονται βιομετρικά. Μπορεί να τα έχετε δει σε έργα επιστημονικής φαντασίας όπου πόρτες ανοίγουν αφού ο ήρωας τοποθετήσει το χέρι του πάνω σε μία επιφάνεια αναγνώρισης, ή όταν μία ακτίνα «σκανάρει» την ίριδα του ματιού του. Ωστόσο, τέτοιες συσκευές όχι μόνο δεν ανήκουν στη σφαίρα του φανταστικού, αλλά έχουν εδώ και μερικά χρόνια μετατραπεί σε φθηνές και εύχρηστες ηλεκτρονικές κλειδαριές στα χέρια του απλού χρήστη. Η αγορά μάλιστα προσφέρει πολλές εναλλακτικές λύσεις.

Τα συν και τα πλην

Δεν υπάρχει αμφιβολία. Οι βιομετρικές συσκευές είναι οι πλέον ασφαλείς. Εάν το απόρρητο των αρχείων σας είναι απόλυτα κρίσιμης σημασίας, τέτοιες συσκευές αποτελούν μονόδρομο και μία απαραίτητη επένδυση χωρίς μάλιστα ιδιαίτερο κόστος.

Μια ματιά στα χαρακτηριστικά που κάνουν αυτού του είδους τα «κλειδιά» τόσο αποτελεσματικά, μας δείχνει ότι:

1. Τα φυσικά χαρακτηριστικά (δακτυλικά αποτυπώματα, χαρακτηριστικά ίριδας) είναι σχεδόν αδύνατο να υποκλαπούν.
2. Δε χρειάζεται ο χρήστης να θυμάται αριθμούς και κωδικούς.
3. Δεν μπορεί κάποιος να «μαντέψει» τα φυσικά χαρακτηριστικά, όπως μπορεί να κάνει για παράδειγμα με ένα password.
4. Τα χέρια και τα μάτια είναι «εξαρτήματα» που κουβαλάμε πάντα μαζί μας. Μία κάρτα ή ένα κλειδί, εύκολα μπορεί να παραπέσει ή να ξεχαστεί κάπου.

Πρόκειται λοιπόν για το ανυπέρβλητο σύστημα ασφαλείας; Η αλήθεια είναι ότι υπάρχουν προβλήματα στη χρήση τέτοιων «κλειδιών»:

1. Ειδικά στα «κλειδιά» δακτυλικών αποτυπωμάτων, υπάρχει η δυνατότητα να φτιαχτεί ομοίωμα του δακτύλου του χρήστη. Οι πιο φθηνές μάλιστα λύσεις δεν μπορούν να διακρίνουν καν αν πρόκειται για πραγματικό δάκτυλο, ή για φωτοτυπία!
2. Πιθανοί τραυματισμοί, μπορούν να αλλοιώσουν τα χαρακτηριστικά μας. Ακόμη και μία γρατσουνιά στο δάκτυλο μπορεί να προκαλέσει ενοχλητικούς μπελάδες.
3. Συχνά, πρέπει να γίνει δύο και τρεις φορές ο έλεγχος για την ταυτοποίηση του χρήστη (scanners με προβλήματα... όρασης).
4. Αν με κάποιο τρόπο γίνει δυνατή η αντιγραφή της μοναδικής ταυτότητας, όπως π.χ. των δακτυλικών αποτυπωμάτων, τότε δεν υπάρχουν απλές λύσεις του στυλ «μου έκλεψαν τον κωδικό μου, αλλά μπορώ να τον αλλάξω».

Και βέβαια δεν χρειάζεται να αναφέρουμε με λεπτομέρειες τις πιο... ανατριχιαστικές μεθόδους κλοπής ενός βιομετρικού «κλειδιού». Όλοι μπορούμε να τις φανταστούμε.

Με δεδομένο λοιπόν ότι υπάρχουν αρκετές λύσεις στην αγορά κόστους έως 200 ευρώ, ο συνδυασμός βιομετρικού μέσου και κλασικού κωδικού, μετατρέπει τον υπολογιστή σας σε απόρθητο φρούριο με τρόπο εύκολο και ιδιαίτερα φθηνό. Άλλωστε μία πιθανή κλοπή πολύτιμων δεδομένων πολλές φορές είναι πρακτικά αδύνατο να κοστολογηθεί.

9.3 ΤΟ ΕΞΥΠΝΟΤΕΡΟ ΣΥΣΤΗΜΑ ΑΣΦΑΛΕΙΑΣ ΑΜΦΙΣΒΗΤΕΙΤΑΙ

Όπως κάθε εποχή καλλιεργεί τους τεχνολογικούς της θρύλους, έτσι και η δική μας λατρεύει τη βιομετρική. Η τεχνολογία που θα αναγνωρίζει την κατατομή του προσώπου, την ίριδα του ματιού ή τη χροιά της φωνής θεωρείται το εξυπνότερο διαβατήριο, ένα εντελώς προσωπικό «δελτίο ταυτότητας» που δεν μπορεί να χαθεί, να κλαπεί ή να πλαστογραφηθεί. Ακόμη και οι όποιες αντιρρήσεις συνήθως δεν αφορούν την αποτελεσματικότητα της τεχνολογίας αυτής, που θεωρείται

δεδομένη, αλλά εστιάζονται στην απειλή παραβίασης της ιδιωτικής ζωής και στην πιθανότητα να χρησιμοποιηθεί η βιομετρική ως εργαλείο κοινωνικού ελέγχου.

Ο βρετανικός Economist εκφράζει μια εντελώς διαφορετική άποψη. «Biometrics, Too flaky to trust», δηλαδή «Βιομετρική, υπερβολικά ανυπόστατη για να την εμπιστευθούμε», γράφει η επικεφαλίδα. Σύμφωνα με το περιοδικό, η τεχνολογία που με τόση θέρμη προωθούν οι κυβερνήσεις στις δύο όχθες του Ατλαντικού είναι υπερβολικά διάτρητη για να χρησιμοποιηθεί σε μεγάλη κλίμακα και δεν αποτελεί επουδενί τη λύση στα προβλήματα ασφαλείας. «Η βιομετρική τεχνολογία υπάρχει εδώ και καιρό, όμως δεν έχει χρησιμοποιηθεί ευρέως και υπάρχει λόγος γι' αυτό», γράφει το περιοδικό. «Ενώ σε ορισμένες περιπτώσεις μπορεί να ενισχύσει την ασφάλεια, συχνότερα τα μειονεκτήματά της είναι πολύ σημαντικότερα από τα πλεονεκτήματα. Ακόμη και τα πιο εξελιγμένα συστήματα εσφαλμένα απορρίπτουν ένα μικρό ποσοστό ατόμων χωρίς να πρέπει και εσφαλμένα επιτρέπουν την πρόσβαση σε κάποιους, τους οποίους θα έπρεπε να σταματήσουν».

Κοινώς, η τεχνολογία δεν είναι αλάνθαστη. Καθώς μάλιστα το κόστος της παραμένει υψηλό, γεννάται το ερώτημα μήπως τελικά βλάπτει, αντί να ενισχύει, την ασφάλεια, αποσπώντας πόρους από πιο χρήσιμα μέτρα. Το General Accounting Office, η υπηρεσία ελέγχου δαπανών του Αμερικανικού Κογκρέσου, που εκλήθη να γνωμοδοτήσει επί του θέματος εξέφρασε σημαντικές επιφυλάξεις και ζήτησε περισσότερη μελέτη. «Η βιομετρική... πολύ πρόσφατα έφθασε να πραγματοποιεί με αποδεκτό τρόπο υπηρεσίες βασικής ταυτοποίησης», έγραψε το GAO το Σεπτέμβριο, μετά από ένα χρόνο μελέτης των υπαρχόντων συστημάτων.

Ο Economist, που παραθέτει και τις αντιρρήσεις του GAO, καταλήγει στο αιρετικό συμπέρασμα ότι η τεχνολογία είναι ιδιαίτερος δημοφιλής μεταξύ των πολιτικών «γιατί δίνει την εντύπωση ότι τα μέτρα ασφαλείας βελτιώνονται δραματικά».

Όλη αυτή η συζήτηση δεν είναι ούτε θεωρητική ούτε μακρινή. Μπορεί τον περασμένο μήνα το «Ελευθέριος Βενιζέλος» να υποχρεώθηκε από την Αρχή Προστασίας Προσωπικών Δεδομένων να σταματήσει το πιλοτικό πρόγραμμα για την βιομετρικών δεδομένων των επιβατών, όμως η Ευρωπαϊκή Ένωση ετοιμάζεται σύντομα να προσθέσει τέτοια στοιχεία στα διαβατήρια. Όποιος δεν σχεδιάζει να επισκεφθεί τις ΗΠΑ, από τις 5 Ιανουαρίου 2004 είναι πολύ πιθανό να περάσει, κατά την είσοδο στη χώρα, από σαρωτή για την ψηφιακή αποτύπωση του προσώπου και του χεριού.

Για όλ' αυτά, μας προετοιμάζει εδώ και χρόνια το Χόλιγουντ, με ταινίες όπως το Mission Impossible, την επιτομή του βιομετρικού μέλλοντος. Στην ταινία αυτή πάντως ο Τομ Κρουζ βρίσκει μια χαρά τον τρόπο να ξεγελάσει τα βιομετρικά συστήματα ασφαλείας...

9.4 ΨΕΥΤΙΚΑ ΑΠΟΤΥΠΩΜΑΤΑ ΞΕΓΕΛΟΥΝ ΤΙΣ ΑΡΧΕΣ

Ψεύτικα δακτυλικά αποτυπώματα, φτιαγμένα από απλά υλικά μπορούν να εξαπατήσουν εύκολα τα βιομετρικά συστήματα ασφαλείας που χρησιμοποιούνται για να αναγνωρίζεται η ταυτότητα των ατόμων.

Τα ψεύτικα δακτυλικά αποτυπώματα δημιουργήθηκαν με τη χρήση ζελατίνας από Ιάπωνες ερευνητές που κατάφεραν να παραπλανήσουν τα βιομετρικά συστήματα ασφαλείας ότι «διάβαζαν» τα πραγματικά στοιχεία.

Οι επιστήμονες διαπίστωσαν ότι μπορούσαν να φτιάξουν πειστικά ψεύτικα αντίγραφα χρησιμοποιώντας ακόμη και δακτυλικά αποτυπώματα που είχαν αποτυπωθεί στο γυαλί.

Οι ειδικοί των βιομετρικών συστημάτων ασφαλείας βέβαια διατυπώνουν αμφιβολίες σχετικά με οποιοδήποτε ισχυρισμό πλέον ότι το δακτυλικό αποτύπωμα στα βιομετρικά συστήματα μπορεί να προσφέρει την ασφάλεια που υποσχόταν. Η εργασία της «αποκαθήςλωσης» των δακτυλικών αποτυπωμάτων έγινε από τον καθηγητή Tsutomu Matsumoto και τους συναδέλφους του στο Πανεπιστήμιο της Γιοκοχάμα.

Στην πρώτη ομάδα των πειραμάτων οι ερευνητές χρησιμοποίησαν ψεύτικα δάκτυλα που δημιουργήθηκαν όταν ζελατίνα χύθηκε πάνω σ' ένα εύπλαστο πλαστικό. Τα δακτυλικά αποτυπώματα που δημιουργήθηκαν με αυτή τη μέθοδο ξεγέλασαν τις συσκευές αναγνώρισης των δακτυλικών αποτυπωμάτων στο 80% των περιπτώσεων.

Η κατασκευή των ψεύτικων δαχτύλων έγινε μέσα σε λίγα λεπτά με τη χρήση ευτελών υλικών και κόστισε ελάχιστα. Οι ερευνητές ανέπτυξαν επίσης έναν ακόμη τρόπο να δημιουργήσουν ψεύτικα δακτυλικά αποτυπώματα χρησιμοποιώντας τα αποτυπώματα που μένουν πάνω στο γυαλί.

Αρχικά το αφανές αποτύπωμα σκληραίνει χρησιμοποιώντας μια ειδική κόλλα που κολλάει στις ζάρες της επιφάνειας που απομένουν όταν ένα δάκτυλο αγγίξει μια σκληρή επιφάνεια. Αυτό το βελτιωμένο αποτύπωμα κατόπιν φωτογραφίζεται με μια ψηφιακή κάμερα και στη συνέχεια βελτιώνεται με τη χρήση του Adobe Photoshop για να είναι πιο εμφανής η διάκριση ανάμεσα στις προεξοχές και τις εγχοπές. Και σ' αυτή την περίπτωση τα ψεύτικα αποτυπώματα ξεγέλασαν στο 80% των περιπτώσεων τα βιομετρικά συστήματα αναγνώρισης των δακτυλικών αποτυπωμάτων.

Ο ειδικός σε συστήματα ασφαλείας Bruce Schneier, μετά την παρουσίαση της μελέτης του Tsutomu Matsumoto, δήλωσε πως το γεγονός ότι τα συστήματα ξεγελάστηκαν με συστατικά που μπορεί ο καθένας να βρει και να χρησιμοποιήσει θα έπρεπε να είναι αρκετό για να σταματήσει η χρήση των βιομετρικών συστημάτων ασφαλείας που βασίζονται στα δακτυλικά αποτυπώματα. Το πείραμα του καθηγητή δείχνει, υποστηρίζει, ότι ένας επαγγελματίας μπορεί να κάνει πολύ περισσότερα και να ξεγελάσει αυτά τα συστήματα.

Ο καθηγητής Matsumoto και οι συνάδελφοί του παρουσίασαν για πρώτη φορά την εργασία τους στη Σύνοδο για την Ηλεκτρονική Εικόνα τον Ιανουάριο του 2002.

ΟΥΤΕ ΟΙ ΑΝΙΧΝΕΥΤΕΣ ΕΙΝΑΙ ΑΛΑΝΘΑΣΤΟΙ

Οι ειδικοί της βιομετρίας καθώς και ορισμένοι πωλητές τέτοιων συστημάτων ανησυχούν ότι οι εταιρείες του χώρου υπόσχονται υπερβολικές δυνατότητες στους πελάτες τους. Θεωρητικά, μόλις το δακτυλικό σας αποτύπωμα ή το πρόσωπό σας γίνει η ταυτότητά σας, δεν χρειάζεται πλέον να ανησυχείτε μήπως τα δεδομένα αυτά χαθούν. Τα συστήματα βιομετρίας, όμως, μπορούν να ξεγελαστούν, αφού και τα συστήματα ανίχνευσης προσώπου ή δακτυλικών αποτυπωμάτων δεν είναι αλάνθαστα.

«Εκείνοι που υποστηρίζουν ότι τα συστήματα βιομετρίας εξασφαλίζουν αλάνθαστη μέθοδο αναγνώρισης κάνουν λάθος», εκτιμά ο διευθυντής βιομετρικών ερευνών του Πανεπιστημίου του Σαν Χοσέ στην Καλιφόρνια, Τζιμ Γουέιμαν. Επιπλέον, η ανίχνευση προσώπου μπορεί να γίνεται χωρίς την άδεια του ατόμου που ελέγχεται, γεγονός που παραβιάζει το προσωπικό απόρρητο. Σαν αποτέλεσμα πληθαίνουν όσοι ζητούν την ψήφιση νομοσχεδίων, που θα εξασφαλίζουν τις ατομικές ελευθερίες και το σεβασμό της ιδιωτικής ζωής.

Εμπορικές επιτυχίες

Ορισμένα συστήματα βιομετρίας υπήρξαν πάντως μεγάλες εμπορικές επιτυχίες, βελτιώνοντας πραγματικά τόσο την ασφάλεια όσο και την άνεση. Σε ένα παντοπωλείο της αλυσίδας Γκριστίδης στη Νέα Υόρκη, οι κάρτες ωραρίου του προσωπικού αντικαταστάθηκαν από σκάνερ παλάμης. «Δεν μπορείς να κοροϊδέψεις το αφεντικό, αλλά ούτε κι αυτός μπορεί να σε κατηγορήσει ότι χτυπάς τις κάρτες συναδέλφων σου», λέει υπάλληλος του καταστήματος. Η πολιτεία της Νέας Υόρκης χρησιμοποιεί το σύστημα αυτό για την υποβολή αιτήσεων χορήγησης επιδομάτων κοινωνικής βοήθειας, αποθηκεύοντας τα στοιχεία του δικαιούχου σε δευτερόλεπτα και αποτρέποντας τις απάτες. Σε μία προσπάθεια να αντιμετωπισθούν οι επικριτές των συστημάτων αυτών, η νομοθεσία απαγορεύει την παροχή πληροφοριών που προήλθαν από συστήματα σκάνερ στο FBI, χωρίς προηγούμενη δικαστική εντολή.

Επίσης, το επιβατικό κοινό εκφράζεται θετικά για το σύστημα INSPASS. Το πρόγραμμα αυτό επιτρέπει σε 65.000 επιβάτες που ταξιδεύουν καθημερινά προς και από τις χώρες του εξωτερικού, να περνούν ταχύτατα από τον έλεγχο της υπηρεσίας μετανάστευσης των Η.Π.Α, ακουμπώντας την παλάμη τους σε σκάνερ, το οποίο συνδέεται με μια βάση δεδομένων όπου έχουν περαστεί οι ανεπιθύμητοι. Εάν το σύστημα δεν καταφέρει να αναγνωρίσει τον επιβάτη, αυτός έχει τη δυνατότητα να περάσει μπροστά και να εξυπηρετηθεί από υπάλληλο της υπηρεσίας.

Δεν τα «διαβάζουν» όλα

Η τεχνολογία, όμως, δεν στερείται προβλημάτων. Οι ψηφιακές μηχανές αναγνώρισης δακτυλικών αποτυπωμάτων δεν μπορούν να «διαβάσουν» τα αποτυπώματα διαφόρων επαγγελματιών, όπως των κομμωτών, οι οποίοι χρησιμοποιούν δραστικά χημικά ή και των ηλικιωμένων, που τα χέρια τους έχουν φθαρεί από το χρόνο. Πρόσφατες έρευνες έδειξαν ότι τα μηχανήματα αυτά δεν μπορούν να διαβάσουν δακτυλικά αποτυπώματα στο 12% των περιπτώσεων, ενώ τα ποσοστά αστοχίας σε ανιχνευτές προσώπου είναι τραγικά. Σε δοκιμές που έγιναν, τα σκάνερ προσώπου δεν μπόρεσαν καν να αναγνωρίσουν δεδομένα, τα οποία είχαν εισαχθεί στο σύστημα, σε ποσοστό άνω του 33%. Οι κατασκευάστριες εταιρείες, όμως, υποστηρίζουν ότι βελτιώνουν συνεχώς το λογισμικό τους.

Πάντως, η τεχνολογία των σκάνερ προσώπου χρησιμοποιείται σήμερα σε ένα διαρκώς αυξανόμενο αριθμό αεροδρομίων των ΗΠΑ, όπως στη Βοστώνη, στο Φρέσκο, στο Κλιργουότερ, στο Παλμ Μπιτς και στο Ντάλας - Φορτ Γουέρθ, συνήθως και για την είσοδο σε χώρους ασφαλείας, τις περισσότερες φορές εν αγνοία των επιβατών. Τα συστήματα αυτά έχουν τη δυνατότητα να συγκρίνουν τα πρόσωπα των διερχομένων με βάσεις δεδομένων του FBI, όπου είναι καταχωρισμένα πρόσωπα τρομοκρατών και καταζητούμενων εγκληματιών.

Παρ' όλα αυτά, η ευκολία με την οποία τα συστήματα αυτά μπορούν να παραπλανηθούν, όπως όταν το συγκεκριμένο πρόσωπο φορά γυαλιά ηλίου ή όταν ο φωτισμός διαφοροποιηθεί, τα μετατρέπει μάλλον σε συστήματα ανάσχεσης. Δηλαδή, σε συστήματα που αποτρέπουν τους υπόπτους, περισσότερο με την παρουσία τους και λιγότερο με την πραγματική τους αξία. «Το να σκανάρεις γενικά το πλήθος είναι προβληματικό. Στην πραγματικότητα αυτό που χρειάζεται ένα αεροδρόμιο είναι ένα σημείο ελέγχου όπου θα περνά ένας - ένας επιβάτης», λέει ο Τομ Κολατόστι, διευθυντής της Βίσατζ Τεχνολοτζι.

Απόκρυψη και κάλυψη

Πολλά τέτοια συστήματα μπορούν να ξεγελασθούν. Νέα μελέτη του Πανεπιστημίου της Γιοκοχάμα στην Ιαπωνία δείχνει ότι χρησιμοποιώντας ψεύτικα δάχτυλα από ζελατίνη, μπορούμε εύκολα να ξεγελάσουμε τα συστήματα ελέγχου παλάμης. Κατασκευάστριες εταιρείες, όμως, υποστηρίζουν ότι προστατεύονται από το ενδεχόμενο αυτό με σκάνερ που μελετούν τη διαστολή της κόρης του ματιού, τη ροή αίματος στα άκρα των δακτύλων και άλλες αποδείξεις του γεγονότος ότι το δείγμα που εξετάζουν είναι «ζωντανό» και όχι ομοίωμα.

Ωστόσο, πολλοί ειδικοί διαφωνούν με την εκτίμηση εταιρειών, που θεωρούν αδύνατη την υπεξαίρεση και αντιγραφή δακτυλικού αποτυπώματος ή του αμφιβληστροειδούς του ματιού. Ένας χάκερ ηλεκτρονικών υπολογιστών, ο οποίος θα διεισδύσει σε ένα ελλιπώς ασφαλισμένο σύστημα θα μπορεί να εξασφαλίσει τα βιομετρικά δεδομένα άλλων και να τα χρησιμοποιήσει, ώστε να εισβάλει σε ασφαλή δίκτυα. Η μέθοδος αυτή, ονομαζόμενη «replay», μπορεί να οδηγήσει την κλοπή ταυτότητας σε νέα επίπεδα, ανάλογα των σύγχρονων τεχνολογικών δυνατοτήτων. «Το δακτυλικό σας αποτύπωμα είναι μοναδικό για πάντα. Εάν πάψει να είναι ασφαλές, δεν μπορείτε να αποκτήσετε καινούργιο», λέει ο Τζακ Φεν, αναλυτής του ομίλου Gartner.

9.5 ΕΞΑΠΑΤΗΣΗ ΣΥΣΚΕΥΩΝ ΑΝΑΓΝΩΡΙΣΗΣ ΑΠΟΤΥΠΩΜΑΤΩΝ



Με μερικές απλές δοκιμές με υλικά που βρίσκονται σε κάθε νοικοκυριό, ο Ιάπωνας ειδικός σε θέματα κρυπτογραφίας κ. Tsutomu Matsumoto, έδειξε ότι είναι ιδιαίτερα εύκολο να εξαπατήσει κανείς τις συσκευές αναγνώρισης αποτυπωμάτων με εξοπλισμό το κόστος του οποίου δεν ξεπερνά τα 10 ευρώ.

Οι συσκευές αναγνώρισης δακτυλικών αποτυπωμάτων ανήκουν στα επωνομαζόμενα βιομετρικά συστήματα ασφαλείας τα οποία αποτελούν τη νεώτερη και πλέον

εξελιγμένη τεχνολογία αναγνώρισης ατόμων με σκοπό τον έλεγχο πρόσβασης σε χώρους ή πληροφορίες. Οι κατασκευάστριες εταιρείες αυτών των συσκευών εδώ και χρόνια διαφημίζουν τα προϊόντα τους ως ιδιαιτέρως ασφαλή και ότι είναι σχεδόν αδύνατον να τις εξαπατήσει με ένα πλαστό αποτύπωμα.

Ο καθηγητής μαθηματικών κ. Matsumoto όμως μαζί με μαθητές του από το πανεπιστήμιο της Γιοκοχάμα απέδειξαν ακριβώς το αντίθετο χρησιμοποιώντας ένα αντίγραφο δακτυλικού αποτυπώματος από ζελατίνη. Ακόμη πιο ενδιαφέρον όμως είναι ότι η ομάδα κατάφερε να εξαπατήσει τις εν λόγω συσκευές δημιουργώντας αντίγραφα από δακτυλικά αποτυπώματα που πήρε από ένα κοινό ποτήρι, γεγονός το οποίο έκανε τους ειδικούς να εκφράζουν σοβαρές αμφιβολίες για το αν αυτού του είδους οι βιομετρικές συσκευές θα μπορούσαν να γίνουν ποτέ εντελώς ασφαλείς. "Ένα ψεύτικο δάκτυλο από ζελατίνη μπορεί να χρησιμοποιηθεί ακόμη και σε χώρους που επιβλέπονται από φρουρούς, ενώ κατόπιν ο χρήστης μπορεί να ακόμη και να "καταπιεί τα αποδεικτικά στοιχεία", δήλωσε χαρακτηριστικά ένας ειδικός σε θέματα ασφαλείας.

Για το πρώτο πείραμα, ο κ. Matsumoto δημιούργησε ένα καλούπι πιέζοντας ένα "ζωντανό" δάκτυλο πάνω σε εύπλαστο πλαστικό όπως αυτό που πωλείται στα καταστήματα ειδών hobby για μοντελισμό. Κατόπιν έλιωσε μαγειρική ζελατίνη την οποία και έχυσε μέσα στο καλούπι. Από τις δοκιμές που έκανε, το τελικό προϊόν, το δάκτυλο από ζελατίνη, ήταν αρκετό για να εξαπατήσει τους ανιχνευτές δακτυλικών αποτυπωμάτων σε ποσοστό 80%!

Αν για το πρώτο πείραμα ήταν αναγκαία η "συγκατάθεση" του κατόχου του δακτύλου, στο δεύτερο πείραμα ο κ. Matsumoto και η ομάδα του προσπάθησαν να αντιγράψουν ένα οποιοδήποτε δακτυλικό αποτύπωμα από ένα καθημερινό αντικείμενο όπως π.χ. ένα ποτήρι.

Το αφανές δακτυλικό αποτύπωμα καταρχάς ενισχύθηκε με την χρήση μιας ειδικής κόλλας η οποία κολλάει πάνω στα νεκρά κύτταρα (cyanoacrylate adhesive) και κατόπιν φωτογραφίστηκε με μια ψηφιακή μηχανή. Με τη χρήση ενός προγράμματος επεξεργασίας εικόνας βελτιώθηκε το κοντράστ και η τελική εικόνα εκτυπώθηκε σε μια διαφάνεια. Η διαφάνεια αυτή με τη σειρά της, αποτυπώθηκε σε μια φωτοευαίσθητη πλακέτα (PCB), η οποία είχε αγοραστεί από ένα μαγαζί με ηλεκτρονικά υλικά για χομπίστες, ώστε να δημιουργηθεί ένα τρισδιάστατο εκμαγείο. Τέλος, χρησιμοποιήθηκε και πάλι ζελατίνη για τη δημιουργία του τελικού, αντιγραμμένου, δακτυλικού αποτυπώματος. Και πάλι, οι συσκευές ανίχνευσης δακτυλικών αποτυπωμάτων "την πάτησαν" σε ποσοστό 80%!

Ο καθηγητής δοκίμασε τα προπλάσματά του σε έντεκα διαφορετικά μοντέλα ανιχνευτών που διατίθενται στο εμπόριο και κατάφερε να τα "εξαπατήσει" όλα.

Ακόμη και τα συστήματα που χρησιμοποιούν τεχνικές εντοπισμού "ζωντανών δακτύλων" (live fingers) εξαπατήθηκαν μετά από λίγες δοκιμές με την εφύγρανση του προπλάσματος.

9.6 ΤΙ ΓΙΝΕΤΑΙ ΜΕ ΤΟ ΑΠΟΡΡΗΤΟ

Οι ανησυχίες για την καταπάτηση δικαιωμάτων του πολίτη, όπως του απορρήτου της ιδιωτικής ζωής, μπορεί να καθυστερήσουν την αποδοχή τέτοιων συστημάτων από το κοινωνικό σύνολο. Σε ορισμένες περιπτώσεις, όμως, η βιομετρία μπορεί να ενισχύσει την προστασία του απορρήτου. Ένα σύστημα ελέγχου αποτυπωμάτων, το οποίο θα ελέγχει την πρόσβαση σε ιατρικά δεδομένα, για παράδειγμα, θα μπορεί να καταρτίσει έναν κατάλογο με εκείνους που ανέτρεξαν στις πληροφορίες αυτές.

Ο έλεγχος προσώπων, όμως, που μπορεί να πραγματοποιηθεί και εν αγνοία των υποκείμενων σε αυτόν, έχει προκαλέσει φόβους σε οργανώσεις για την προάσπιση των ατομικών ελευθεριών.

Το σύστημα ελέγχου προσώπων της εταιρείας Visionics αναπτύχθηκε στο πλαίσιο εκστρατείας κατά του εγκλήματος στην Τάμπα της Φλόριντα. Ο επικεφαλής της αστυνομίας της κομητείας, Μπιλ Τοντ, ανέφερε ότι το σύστημα αποκαθλώθηκε μόλις δύο μήνες μετά την εγκατάστασή του, εξαιτίας τεχνικού προβλήματος. Μετά την αναβάθμιση του λογισμικού, όμως, το σύστημα επανήλθε στους δρόμους της πόλης. Το σύστημα, που περιλαμβάνει 36 κάμερες, ελέγχεται από έναν αστυνομικό στο κέντρο επιχειρήσεων. Ο χειριστής του μπορεί να κινήσει τις κάμερες με τέτοιο τρόπο, ώστε να εστιάσει στα πρόσωπα των πεζών και των αυτοκινητιστών και να τα συγκρίνει με βάση δεδομένων.

Ενώ ο Τοντ δηλώνει ότι η βάση δεδομένων περιέχει μόνο φωτογραφίες καταζητούμενων εγκληματιών, παιδιών που αγνοούνται και καταδικών για σεξουαλικά εγκλήματα, η τοπική αστυνομία έχει ζητήσει να συμπεριληφθούν ακόμη και άλλοι ύποπτοι, όπως μέλη συμμοριών. Η Αμερικανική Οργάνωση για την Προάσπιση των Ατομικών Δικαιωμάτων, ACLU, εκτιμά ότι η τεχνολογία αυτή είναι υπεύθυνη για σημαντικά σφάλματα, ενώ και ο Τοντ παραδέχεται ότι το σύστημα δεν έχει οδηγήσει σε καμία σύλληψη. «Το νέο σύστημα δεν υποκαθιστά τις διωκτικές αρχές, αλλά διευκολύνει κάπως το έργο τους», λέει ο Φράνσις Ζελάσι, εκπρόσωπος της εταιρείας Visionics.

Σε ορισμένες περιπτώσεις το πρόβλημα της προστασίας της ιδιωτικής ζωής είναι περισσότερο νοητό, παρά πραγματικό. Τα σχολεία της περιφέρειας του Μέριον, κοντά στη Φιλαδέλφεια των ΗΠΑ, εγκατέστησαν σύστημα ελέγχου δακτυλικών αποτυπωμάτων, για την καταμέτρηση των χορηγούμενων γευμάτων σε μαθητές. Το σύστημα επιτρέπει στις ουρές των μικρών μαθητών να κινούνται ταχύτερα, ενώ διασφαλίζεται και το απόρρητο της ταυτότητας των μαθητών εκείνων που λαμβάνουν δωρεάν γεύματα εξαιτίας των χαμηλών αποδοχών των γονέων τους. Αν και το σύστημα δεν εξετάζει το πλήρες αποτύπωμα, αλλά μόνο το ψηφιακό σχηματικό τους διάγραμμα, ορισμένοι γονείς παραπονέθηκαν ότι θυμίζει επικίνδυνα τις παραδοσιακές αστυνομικές μεθόδους καταγραφής αποτυπωμάτων. Έπειτα από συναπτά αρνητικά δημοσιεύματα του Τύπου, το πρόγραμμα αποσύρθηκε πέρυσι. Πάντως σαράντα άλλες σχολικές περιφέρειες συνεχίζουν να χρησιμοποιούν το σύστημα.

Βιο-ιδιωτική ζωή

Οι υποθέσεις αυτές ώθησαν εκπροσώπους κατασκευαστριών εταιρειών να ζητήσουν τη νομοθετική κάλυψη της πρωτοποριακής βιομηχανίας. Ο Σαμίρ Ναναβατί, συνétaιρος στην IBG, υποστηρίζει ότι η εταιρεία του σέβεται τους κανόνες της «βιο-ιδιωτικής ζωής», τους οποίους ορίζει ως εξής: Πείτε στους ανθρώπους τι είδους στοιχεία συλλέγετε, ελαχιστοποιήστε τον όγκο των συλλεγόμενων πληροφοριών, χρησιμοποιήστε τα στοιχεία μόνο για τους λόγους που έχετε δηλώσει και δώστε στους χρήστες την ευκαιρία να διορθώσουν τα στοιχεία τους.

Ο Ναναβατί ανησυχεί επίσης για ενδεχόμενη ανήθικη χρήση της τεχνολογίας αυτής. Πρόσφατα συμβάντα στη Νέα Υόρκη αποκάλυψαν τα μειονεκτήματα των

βιομετρικών συστημάτων. Αγανακτισμένοι εργαζόμενοι στο νοσοκομείο New York - Presbyterian, όπου οι ουρές μπροστά από τα μηχανήματα ανάγνωσης παλάμης προκαλούσαν μεγάλες καθυστερήσεις, έσπασαν τα μηχανήματα ύστερα από δύο εβδομάδες υπομονής.

Ο ιδανικός συνδυασμός, σύμφωνα με τον Ναναβατί, έγκειται στον σχεδιασμό ενός συστήματος, το οποίο θα λαμβάνει υπόψη τις ανάγκες ασφαλείας, αλλά και την εξυπηρέτηση των εργαζομένων. Αυτό μπορεί ορισμένες φορές να σημαίνει ακόμη και την... απουσία τέτοιου συστήματος.

ΕΠΙΛΟΓΟΣ

Ο βιομετρικός έλεγχος είναι μια αυτοματοποιημένη μέθοδος με την οποία η ταυτότητα ενός ατόμου εξακριβώνεται εξετάζοντας ένα μοναδικό και σταθερό φυσιολογικό γνώρισμα ή χαρακτηριστικό συμπεριφοράς ενός ατόμου. Ορισμένα χαρακτηριστικά είναι πρακτικά αμετάβλητα και μπορεί να επηρεάζονται τόσο από ελεγχόμενους όσο και από λιγότερο ελεγχόμενους, ψυχολογικούς παράγοντες. Σε κάθε περίπτωση, πάντως, η χρήση βιομετρικών χαρακτηριστικών παρέχει ένα αισθητά ψηλότερο επίπεδο πιστοποίησης από ότι τα συνθηματικά ή οι έξυπνες κάρτες.

Επειδή ακριβώς τα βιομετρικά χαρακτηριστικά είναι μοναδικά για κάθε άτομο μπορούν να χρησιμοποιηθούν για να αποφευχθεί η κλοπή ή η απάτη. Αντίθετα από έναν προσωπικό αριθμό αναγνώρισης (PIN) ή ένα συνθηματικό, ένα βιομετρικό χαρακτηριστικό δεν μπορεί να ξεχαστεί, χαθεί ή κλαπεί.

Σήμερα υπάρχουν περισσότεροι από 10.000 χώροι υπολογιστών, θησαυροφυλάκια, εργαστήρια, νοσοκομειακές μονάδες, τράπεζες αίματος, στρατιωτικές εγκαταστάσεις ή αυτόματες ταμειολογιστικές μηχανές που ελέγχονται από συσκευές που σαρώνουν τα φυσικά χαρακτηριστικά ενός ατόμου.

Συμπερασματικά, φαίνεται ότι οι βιομετρικές τεχνικές μπορούν να έχουν μια πλειάδα εφαρμογών. Μένει μόνο να αποδειχτεί κατά πόσο θα υλοποιηθούν πραγματικά –αν όχι όλες- οι περισσότερες βιομετρικές τεχνολογίες, σε σημείο που να είναι λειτουργικές και να προσφέρουν τον απαιτούμενο έλεγχο χωρίς να είναι εύκολη η εξαπάτηση των συστημάτων. Επίσης, σημαντικό είναι να βρεθεί η χρυσή τομή μεταξύ της αναγκαιότητας για τον ανωτέρω έλεγχο χωρίς όμως να παραβιάζονται τα βασικά ανθρώπινα δικαιώματα.



ΓΛΩΣΣΑΡΙΟ

ADC	: Analog to Digital Converter / Μετατροπέας αναλογικού σε ψηφιακό.
AFIS	: Automated Fingerprint Identification System / Αυτοματοποιημένο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων.
ATM	: Αυτόματη ταμειακή μηχανή.
BIOS	: Basic Input Output System. Το βασικό σύστημα εισόδου – εξόδου της μητρικής.
Bit	: Binary Digit. Δυαδικό ψηφίο (1 ή 0).
Byte	: 8 bits / ένας χαρακτήρας.
CD	: Compact Disk. Αποθηκευτικό μέσο.
CMOS	: Complementary Metal Oxide Semiconductor / Συμπληρωματικός μεταλλικός ημιαγωγός οξειδίου. Τεχνολογία με την οποία φτιάχνονται τα περισσότερα ολοκληρωμένα κυκλώματα.
Database	: Βάση δεδομένων.
Desktop συστήματα	: Συστήματα επιφάνειας εργασίας.
Discrete-time σύστημα	: Σύστημα διακριτού χρόνου.
DNA	: Δεοξυ-ριβο-νουκλεϊκό οξύ. Χημική ένωση που βρίσκεται στα κύτταρα των οργανισμών.
E-mail	: Electronic Mail. Ταχυδρομείο μέσω Internet.
FAR	: False Acceptance Rate / Ψεύτικο ποσοστό αποδοχής.
Finger Code	: Κώδικας δακτύλων.
Fingerprint Reader	: Αναγνώστες δακτυλικών αποτυπωμάτων.
Fingerprint scanners	: Σαρωτές δακτυλικών αποτυπωμάτων.
Frame Grabber	: Πλαίσιο Grabber.
Freeware	: Δωρεάν λογισμικό.
FRR	: False Rejection Rate / Ψεύτικο ποσοστό απόρριψης.
Hardware	: Υλικό.

Internet	: Διαδίκτυο. Τεράστιος αριθμός διασυνδεδεμένων υπολογιστών και δικτύων που επικοινωνούν με το πρωτόκολλο TCP / IP.
Kb	: Kilobyte. 1024 bytes.
LAN	: Local Area Network. Τοπικό δίκτυο.
Manual	: Χειροκίνητα.
Mb	: Megabyte. 1024 Kilobytes.
Module	: Στοιχείο.
Mouse	: Το "ποντίκι" του υπολογιστή.
Notebook	: Σημειωματάριο.
Password	: Σύνθημα. Συνήθως χρησιμοποιείται μαζί με το Login ώστε να αποκτήσουμε πρόσβαση σε προφυλαγμένο δικτυακό χώρο.
PC	: Personal Computer. Προσωπικός Υπολογιστής.
PCA	: Principle Component Analysis / Ανάλυση τμημάτων αρχής.
PDA	: Personal Digital Assistant / Προσωπικός ψηφιακός βοηθός. Υπολογιστής παλάμης.
PIN	: Personal Identification Number / Προσωπικοί Αριθμοί Αναγνώρισης.
Pixel	: Ορθογώνιο πλέγμα στοιχείων εικόνας.
Project	: Πρόγραμμα.
Proximity Cards	: Κάρτες Προσέγγισης. Ελέγχουν την πρόσβαση σε διαβαθμισμένους χώρους.
RAM	: Random Access Memory. Η μνήμη του Υπολογιστή.
Reboot	: Επανεκκίνηση. Χρησιμοποιείται είτε για να "ξεκολλήσει" το σύστημα, είτε για να ολοκληρωθεί η εγκατάσταση ενός καινούριου προγράμματος.
Review	: Αναθεώρηση.
Scanner	: Ανιχνευτής, σαρωτής.
Server	: Διακομιστής. Ισχυρός υπολογιστής που προσφέρει χώρο εγκατάστασης δικτυακών τόπων ή πακέτο λογισμικού με το οποίο επικοινωνούν άλλα λογισμικά – πελάτες (clients).
Site	: Ιστοσελίδα. Νεολογισμός που αναφέρεται στις σελίδες που είναι αναρτημένες στο διαδίκτυο.
Software	: Λογισμικό.
Speaker	: Ομιλητής.
Submit	: Υπόδειξη, υποβολή.
Template	: Πρότυπο.

ΓΛΩΣΣΑΡΙΟ

User name	: Όνομα χρήστη.
WAN	: Wide Area Network. Δίκτυο ευρείας περιοχής.
WAV αρχείο	: Αρχείο ψηφιακής μουσικής ασυμπίεστο και κατά μέσο όρο ένα (1) λεπτό μουσικής αντιστοιχεί σε 10 MB στο σκληρό δίσκο.
Web administrators	: Διαχειριστής ιστοσελίδων.
Web servers	: Λογισμικό που τρέχει σε ένα κόμβο Internet και επιτρέπει σε άλλους υπολογιστές να αποκτούν αντίγραφα των web σελίδων που είναι αποθηκευμένες σε αυτόν.
Wizard	: Βοηθός.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Δημήτρης Καρτσακλής :Computer για όλους, "Βιομετρικά συστήματα αναγνώρισης", 1/9/1999, Τεύχος 182.
- Εφημερίδα "ΤΑ ΝΕΑ" 7/1/2004 και 15/6/2004.
- Εφημερίδα "ΕΛΕΥΘΕΡΟΤΥΠΙΑ" 10/1/2004.
- Εφημερίδα "ΚΑΘΗΜΕΡΙΝΗ".
- www.biometricgroup.com.
- www.google.com.
- News in.gr, 9/11/2004.
- <http://biometrics.cse.msu.edu/info.html>
- <http://www.cgomag.gr/Articlescgo.asp?MainTitle=%C2%C9%CF%CC%C5%D4%D1%C9%CA%C1+%D3%D5%D3%D4%C7%CC%C1%D4%C1+%C1%CD%C1%C3%CD%D9%D1%C9%D3%C7%D3&ArTeuxous=182&CategoryID=2&selected=afieroma>
- Κώστας Νάκος, Νίκος Βλασσόπουλος, Γιώργος Ροπόδης : Computer για όλους , "Αναγνώριση φωνής", Τεύχος 194 1/10/2000.
- Πέτρος Παπαθανασίου :Techlife, 25/11/2003.
- Τεχνική, Ιούλιος-Αύγουστος 2003, Τεύχος 439.
- Νίκος Κυρλόγλου (ειδικός επιστήμονας πληροφορικής ΕΒΕΑ) : Ανάπτυξη "Βιομετρικά συστήματα πιστοποίησης", Τεύχη Μαΐου, Ιουνίου, Ιουλίου 2002 .
- Paul Marks, Catherine Zandonella και Justin Mullins. Defeating the suicide hijackers, From New Scientist Online News 19:00 19 September 01.