



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Επισκόπηση Τεχνολογιών Βιομετρικής Αυθεντικοποίησης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ανδρέα Αβραμίδη Σιδηρόπουλου

Επιβλέπων: Κρητικός Κυριάκος

Μέλη εξεταστικής επιτροπής: Καρύδα Μαρία, Κωνσταντίνου Ελισάβετ

Σάμος, Ιούλιος 2025

Η σελίδα αυτή είναι σκόπιμα λευκή.

*Στον πατέρα μου, που έφυγε ξαφνικά
την Παρασκευή 7 Φεβρουαρίου 2025*

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον κ. Κυριάκο Κρητικό, επιβλέπων καθηγητή για την εμπιστοσύνη που έδειξε στο πρόσωπό μου, το ειλικρινές ενδιαφέρον του και την πολύτιμη καθοδήγησή του.

Επίσης, ευχαριστώ το σύνολο του διδακτικού προσωπικού του μεταπτυχιακού προγράμματος για το υψηλό επίπεδο γνώσεων και ανταπόκρισης.

© 2025

του

Ανδρέα Αβραμίδη Σιδηρόπουλου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1	Εισαγωγή	1
1.1	Ασφάλεια Δεδομένων με Χρήση Βιομετρικών Τεχνολογιών	1
1.2	Αντικείμενο της Διπλωματικής	3
1.2.1	Συνεισφορά	4
1.2.2	Σε τι ωφελεί	4
1.3	Δομή Διπλωματικής	5
2	Μεθοδολογία Βιβλιογραφικής Ανασκόπησης	6
2.1	Ερευνητικά Ερωτήματα	6
2.2	Αναζήτηση Άρθρων	6
2.3	Κριτήρια Φιλτραρίσματος Άρθρων	7
2.4	Στατιστική Ανάλυση	7
3	Ανάλυση Βιβλιογραφίας	10
3.1	Εισαγωγή στην Έννοια της Βιομετρικής Αυθεντικοποίησης	10
3.1.1	Πλεονεκτήματα	10
3.1.2	Περιορισμοί	11
3.2	Βασικές Αρχές και Κατηγοριοποίηση Βιομετρικών Συστημάτων	11
3.2.1	Φυσικά και Συμπεριφορικά Βιομετρικά Χαρακτηριστικά	11
3.2.2	Βασικές Λειτουργίες & Αρχιτεκτονική ενός Βιομετρικού Συστήματος	12
3.3	Αναγνώριση Ίριδας και Άλλες Προηγμένες Βιομετρικές Μέθοδοι	14
3.3.1	Η Τεχνολογία της Ίριδας και η Μελέτη του Daugman	14
3.3.2	Ζητήματα Αποθήκευσης και Προστασίας Δεδομένων	14
3.4	Διασύνδεση Βιομετρικής με Κρυπτογραφία	14
3.4.1	Βιομετρικά Κρυπτοσυστήματα και το Fuzzy Vault	14
3.4.2	Robust Hashing	15
3.5	Ανάλυση της Γεωμετρίας του Χεριού και Εναλλακτικές Προσεγγίσεις	16
3.5.1	Η Μελέτη των Kumar και Zhang	16
3.5.2	Ποικιλομορφία Επιλογών για Διάφορα Περιβάλλοντα	16
3.6	Προχωρημένες Τεχνικές και Τάσεις στο Βιομετρικό Πεδίο	16
3.6.1	Πολυτροπικές Βιομετρικές Προσεγγίσεις	17
3.6.2	Ανάλυση Συμπεριφοράς σε Πραγματικό Χρόνο	17
3.6.3	Βιομετρική Αυθεντικοποίηση στο Internet of Things (IoT)	17
3.6.4	Βιομετρική Αυθεντικοποίηση και Blockchain	18

3.6.5	Ενοποίηση με Τεχνητή Νοημοσύνη.....	20
3.7	Προκλήσεις και Προοπτικές στη Βιομετρική Αυθεντικοποίηση.....	20
3.7.1	Ζητήματα Ιδιωτικότητας και Νομοθεσίας.....	20
3.7.2	Ηθικές και Κοινωνικές Διαστάσεις της Βιομετρικής Αυθεντικοποίησης.....	21
3.7.3	Ακρίβεια, Απόδοση και Πραγματικές Συνθήκες.....	22
3.7.4	Προκλήσεις Κλιμάκωσης και Απόδοσης στο Blockchain	22
3.7.5	Τεχνητή Νοημοσύνη και Deepfakes.....	22
3.7.6	Ανοικτά Ερευνητικά Ερωτήματα	23
3.8	Εφαρμογές σε Διάφορους Κλάδους.....	23
3.8.1	Χρηματοπιστωτικός Τομέας και Ηλεκτρονικές Πληρωμές.....	23
3.8.2	Υγειονομική Περίθαλψη και Ταυτοποίηση Ασθενών	24
3.8.3	Κρατικές Υπηρεσίες και Δημόσιοι Φορείς	24
3.8.4	Εγκληματολογία.....	24
3.8.5	Ελεγχόμενη Πρόσβαση σε Εγκαταστάσεις Υψηλής Ασφάλειας.....	24
3.8.6	Εμπορική Χρήση και Καταναλωτικές Εφαρμογές.....	25
3.9	Ευρύτερη Επισκόπηση της Βιβλιογραφίας και Τάσεις.....	26
4	Σύγκριση Βιομετρικών Τεχνολογιών Αυθεντικοποίησης	27
4.1	Εισαγωγή στη Συγκριτική Ανάλυση.....	27
4.2	Επισκόπηση των Κυριότερων Βιομετρικών Τεχνολογιών	28
4.3	Συγκριτική Ανάλυση Βασικών Βιομετρικών Τεχνολογιών	28
4.3.1	Αναγνώριση Δακτυλικών Αποτυπωμάτων (Fingerprint Recognition)	29
4.3.2	Αναγνώριση Προσώπου (Face Recognition).....	31
4.3.3	Αναγνώριση Ιριδας (Iris Recognition)	32
4.3.4	Αναγνώριση Αμφιβληστροειδούς (Retina Recognition)	34
4.3.5	Αναγνώριση Φωνής (Voice Recognition).....	35
4.3.6	Δυναμική Πληκτρολόγηση (Keystroke Dynamics).....	36
4.3.7	Αναγνώριση Βάδισης (Gait Recognition)	38
4.3.8	Αναγνώριση Υπογραφής (Signature Recognition).....	39
4.3.9	Αναγνώριση Παλαμιαίων Αγγείων (Palm Vein Recognition).....	40
4.3.10	Πολυτροπικά Συστήματα (Multimodal Systems)	41
4.4	Πλεονεκτήματα και Μειονεκτήματα των Διαφορετικών Τεχνολογιών.....	43
4.4.1	Αναγνώριση Δακτυλικών Αποτυπωμάτων	43
4.4.2	Αναγνώριση Προσώπου.....	43
4.4.3	Αναγνώριση Ιριδας.....	43
4.4.4	Αναγνώριση Αμφιβληστροειδούς	44
4.4.5	Αναγνώριση Φωνής.....	44

4.4.6	Δυναμική Πληκτρολόγηση	44
4.4.7	Αναγνώριση Βάδισης.....	44
4.4.8	Αναγνώριση Υπογραφής	45
4.4.9	Αναγνώριση Παλαμιαίων Αγγείων	45
4.4.10	Πολυτροπικά Συστήματα	45
4.5	Αποτελέσματα Σύγκρισης και Συμπεράσματα	46
4.5.1	Ενιαίος Συγκριτικός Πίνακας.....	48
4.5.2	Καλύτερες και Χειρότερες Τεχνολογίες ανά Κριτήριο.....	50
5	Επίλογος – Συζήτηση	52
5.1	Επαναπροσδιορισμός της Σημασίας των Βιομετρικών Τεχνολογιών.....	52
5.2	Υπενθύμιση των Κύριων Συμπερασμάτων από τη Σύγκριση των Τεχνολογιών.....	53
5.3	Η Εμπλοκή της Βιομηχανίας και των Κυβερνήσεων.....	55
5.4	Ζητήματα Προστασίας Δεδομένων και Ιδιωτικότητας.....	55
5.5	Τεχνολογικές Τάσεις και Προκλήσεις	56
5.6	Ηθικοί και Νομικοί Προβληματισμοί: Αναγκαία Βήματα Ρύθμισης	57
5.7	Ερευνητικές Προκλήσεις και Κατευθύνσεις.....	58
5.8	Συμπερασματική Επισκόπηση και Προοπτικές	59
5.9	Τελικές Σκέψεις	61
5.10	Επίλογος: Προς μια Ολοκληρωμένη Προσέγγιση	61
	Βιβλιογραφία.....	63

Λίστα Εικόνων

Εικόνα 1: Μέθοδοι βιομετρικής αυθεντικοποίησης.....	2
Εικόνα 2: Διαδικασία βιομετρικής αυθεντικοποίησης.....	3
Εικόνα 3: Αριθμός άρθρων ανά έτος δημοσίευσης.....	8
Εικόνα 4: Ποσοστό άρθρων ανά τύπο/είδος	9
Εικόνα 5: Ποσοστό άρθρων ανά εκδότη.....	9
Εικόνα 6: Διάγραμμα με τα κύρια συστατικά αρχιτεκτονικής ενός βιομετρικού συστήματος ..	13
Εικόνα 7: Βιομετρική αυθεντικοποίηση & Blockchain	18
Εικόνα 8: Παραδείγματα εφαρμογών βιομετρικών τεχνολογιών	25

Λίστα Πινάκων

Πίνακας 1: Πίνακας απαιτήσεων και εφαρμογών βιομετρικών τεχνολογιών.....	47
Πίνακας 2: Ενιαίος συγκριτικός πίνακας βιομετρικών τεχνολογιών	49
Πίνακας 3: Πίνακας τεχνολογιών υψηλής & χαμηλής απόδοσης ανά κριτήριο	51

Ακρωνύμια

AI	Artificial Intelligence
CCTV	Closed Circuit Television
CNNs	Convolutional Neural Networks
EbD	Ethics by Design
EER	Equal Error Rate
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Nonmatch Rate
FRR	False Rejection Rate
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
HCI	Human-Computer Interaction
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standardization
KYC	Know Your Customer
MFCCs	Mel-Frequency Cepstral Coefficients
ML	Machine Learning
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PoA	Proof-of-Authority
PoW	Proof-of-Work
PSD2	Payment Services Directive 2
RNN	Recurrent Neural Networks
SLAs	Service Level Agreements
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Δεδομένων
E.E.	Ευρωπαϊκή Ένωση
TN	Τεχνητή Νοημοσύνη

Περίληψη

Η βιομετρική αυθεντικοποίηση αποτελεί μια από τις πλέον διαδεδομένες και ασφαλείς μεθόδους αυθεντικοποίησης χρηστών, που αξιοποιεί μοναδικά φυσικά και συμπεριφορικά χαρακτηριστικά. Για αυτό τον λόγο, η παρούσα διπλωματική εργασία παρέχει μια εκτενή βιβλιογραφική ανασκόπηση των κυριότερων βιομετρικών τεχνολογιών, αναλύοντας τις βασικές αρχές, τις εφαρμογές και τις προκλήσεις που αντιμετωπίζουν.

Πραγματοποιείται συγκριτική ανάλυση των τεχνικών αναγνώρισης δακτυλικών αποτυπωμάτων, προσώπου, ίριδας, αμφιβληστροειδούς, φωνής, βάδισης, δυναμικής πληκτρολόγησης, υπογραφής, παλαμιαίων αγγείων καθώς και των πολυτροπικών συστημάτων. Επιπλέον, εξετάζονται σύγχρονες σχετικές ως προς την αυθεντικοποίηση προκλήσεις στον τομέα της ασφάλειας, όπως οι επιθέσεις πλαστοπροσωπίας (spoofing), ενώ επισημαίνονται και οι προοπτικές ενσωμάτωσης σημαντικών τεχνολογιών, όπως το blockchain και η τεχνητή νοημοσύνη.

Τέλος, συζητούνται ηθικοί και νομικοί προβληματισμοί σε ζητήματα ιδιωτικότητας και προσωπικών δεδομένων που συνδέονται με τη βιομετρική αυθεντικοποίηση.

Λέξεις Κλειδιά: βιομετρική ασφάλεια, ιδιωτικότητα, βιομετρική αυθεντικοποίηση, αναγνώριση προσώπου, αναγνώριση δακτυλικών αποτυπωμάτων, αναγνώριση ίριδας, πολυτροπικά συστήματα, τεχνητή νοημοσύνη, blockchain

Abstract

Biometric authentication is one of the most widespread and secure methods of user identification, utilising unique physical and behavioural characteristics. To this end, this thesis provides an extensive literature review of the main biometric technologies, analyzing their basic principles, applications and challenges.

A comparative analysis of fingerprint, facial, iris, retinal, voice, gait, dynamic keystroke, signature, palm vessel, and multimodal systems recognition techniques is performed. In addition, current security challenges related to biometric authentication such as spoofing attacks are discussed, and the potential for integrating important technologies, such as blockchain and artificial intelligence is highlighted.

Finally, ethical and legal considerations on privacy and personal data issues connected to biometric authentication are discussed.

Keywords: *biometric security, privacy, biometric authentication, facial recognition, fingerprint recognition, iris recognition, multimodal systems, artificial intelligence, blockchain*

1

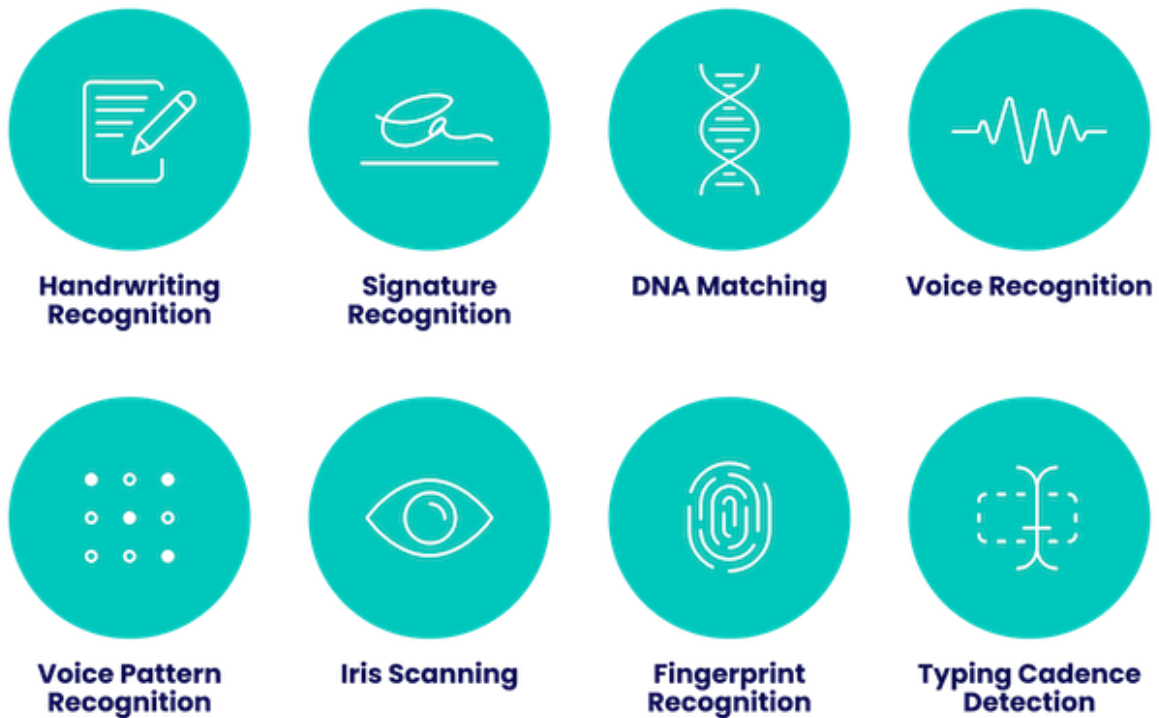
Εισαγωγή

1.1 Ασφάλεια Δεδομένων με Χρήση Βιομετρικών Τεχνολογιών

Η βιομετρική αυθεντικοποίηση (biometric authentication) αποτελεί μία από τις πλέον σύγχρονες και αποτελεσματικές λύσεις για την προστασία της ασφάλειας δεδομένων και της ιδιωτικότητας, καθώς η συνεχής εξέλιξη της τεχνολογίας, η αυξανόμενη εξάρτηση από ψηφιακά συστήματα και η αύξηση του αριθμού και της πολυπλοκότητας των επιθέσεων ασφάλειας ενισχύουν την ανάγκη για αποδοτικές και αξιόπιστες μεθόδους ασφαλείας. Οι παραδοσιακές μέθοδοι αυθεντικοποίησης, όπως τα διαπιστευτήρια πρόσβασης (όνομα & κωδικός χρήστη) (credentials) και οι αριθμοί PIN, αν και ευρέως διαδεδομένες, αποδεικνύονται συχνά ανεπαρκείς μπροστά στις προκλήσεις που θέτουν σύγχρονες κυβερνοαπειλές, όπως οι επιθέσεις brute force, phishing (ηλεκτρονικό ψάρεμα) ή credential harvesting (συγκομιδή διαπιστευτηρίων). Αυτές οι μέθοδοι βασίζονται σε πληροφορίες που μπορούν να ξεχαστούν, να υποκλαπούν ή να παραποιηθούν, αφήνοντας σημαντικά κενά ασφαλείας.

Η βιομετρική αυθεντικοποίηση, από την άλλη πλευρά, προσφέρει μία πιο ασφαλή και αξιόπιστη εναλλακτική, βασισμένη σε μοναδικά φυσικά και συμπεριφορικά χαρακτηριστικά του κάθε ατόμου. Τέτοια χαρακτηριστικά, όπως τα δακτυλικά αποτυπώματα, η ίριδα του ματιού, η φωνή και το μοτίβο πληκτρολόγησης είναι εν γένει δύσκολο να αναπαραχθούν ή να παραποιηθούν, καθιστώντας τις βιομετρικές τεχνολογίες εξαιρετικά ανθεκτικές απέναντι σε παραβιάσεις ασφαλείας. Η χρήση αυτών των τεχνολογιών δεν προσφέρει μόνο βελτιωμένη ασφάλεια, αλλά και αυξημένη ευκολία για τους χρήστες, καθώς καταργεί την ανάγκη απομνημόνευσης περίπλοκων κωδικών πρόσβασης.

Types of Biometrics Used for Authentication & Verification



Εικόνα 1: Μέθοδοι βιομετρικής αυθεντικοποίησης.

Πηγή: [Seon](#)

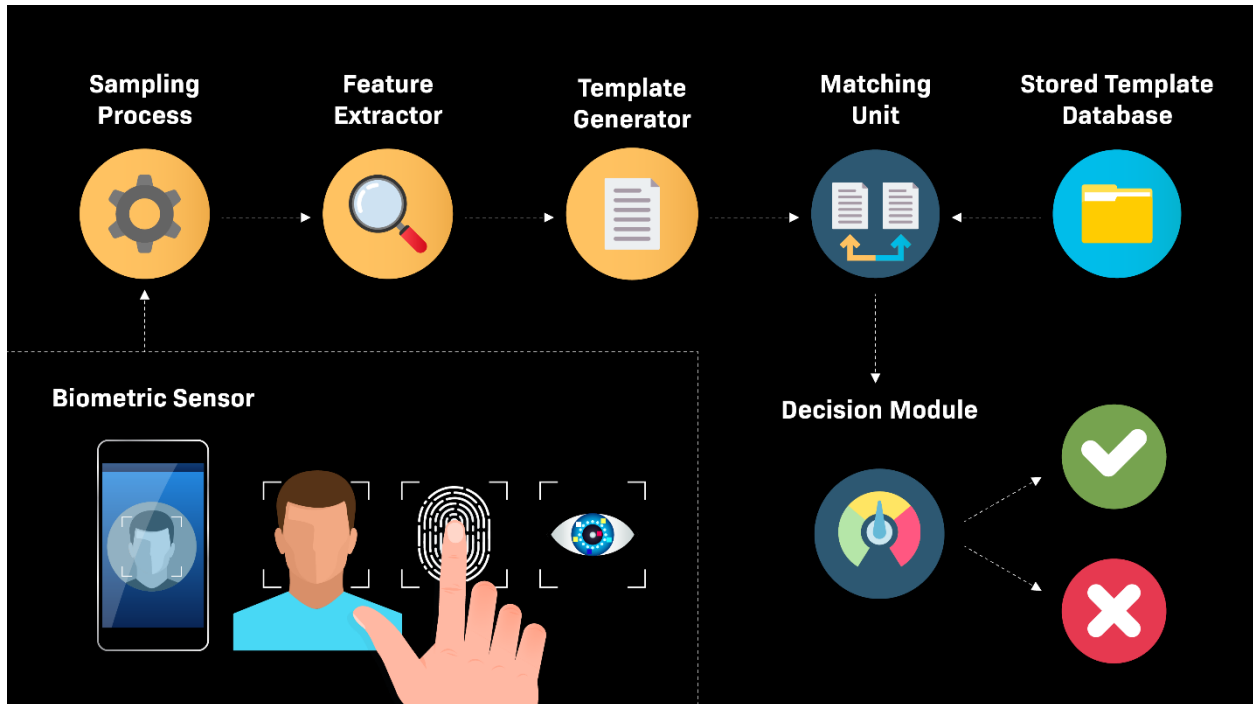
Πέραν της αυξημένης ασφάλειας που παρέχει η βιομετρική αυθεντικοποίηση, η ενσωμάτωσή της σε σύγχρονες τεχνολογίες, όπως τα συστήματα blockchain, αναμένεται να ενισχύσει περαιτέρω την προστασία ευαίσθητων δεδομένων.

Επιπλέον, η ανάπτυξη τεχνολογιών τεχνητής νοημοσύνης (AI – Artificial Intelligence) και μηχανικής μάθησης (ML – Machine Learning) έχει ενισχύσει περαιτέρω την αποτελεσματικότητα των βιομετρικών συστημάτων. Οι σύγχρονοι αλγόριθμοι είναι ικανοί να ανιχνεύουν λεπτές διαφοροποιήσεις στα βιομετρικά χαρακτηριστικά, ενισχύοντας την ακρίβεια της ταυτοποίησης ακόμη και σε απαιτητικά περιβάλλοντα. Αυτό καθιστά τις βιομετρικές τεχνολογίες όχι μόνο αποτελεσματικές, αλλά και προσαρμόσιμες στις ανάγκες διάφορων εφαρμογών, από την εμπορική χρήση έως την εφαρμογή σε συστήματα εθνικής ασφάλειας.

Σχετικά με τις εφαρμογές, η βιομετρική αυθεντικοποίηση, ως μια από τις πλέον πρωτοποριακές τεχνολογίες ασφαλείας, έχει εξελιχθεί σε έναν ακρογωνιαίο λίθο της σύγχρονης ψηφιακής εποχής.

Από την καθημερινή χρήση της για την πρόσβαση σε smartphones και εφαρμογές, έως την εφαρμογή της σε κρίσιμους τομείς, όπως οι τραπεζικές συναλλαγές, η υγειονομική περίθαλψη και οι κυβερνητικές υπηρεσίες, η τεχνολογία αυτή έχει εδραιωθεί ως ένα αναπόσπαστο εργαλείο για τη διασφάλιση της ασφάλειας. Η αναγνώριση προσώπου αποτελεί μία από τις πλέον διαδεδομένες

και ταχύτερα αναπτυσσόμενες βιομετρικές τεχνολογίες. Τα σύγχρονα συστήματα βασίζονται σε αλγόριθμους βαθιάς μάθησης (deep learning), οι οποίοι είναι ικανοί να αναλύουν και να επεξεργάζονται πολύπλοκα χαρακτηριστικά του προσώπου με εξαιρετική ακρίβεια. Αυτή η τεχνολογία έχει βρει εφαρμογή σε κρίσιμους τομείς, όπως η ασφάλεια αεροδρομίων, όπου η επαλήθευση ταυτότητας πρέπει να γίνεται με ακρίβεια και ταχύτητα, καθώς και σε διαδικτυακές συναλλαγές, όπου εξασφαλίζει την ταυτοποίηση χρηστών χωρίς τη χρήση παραδοσιακών κωδικών πρόσβασης.



Εικόνα 2: Διαδικασία βιομετρικής αυθεντικοποίησης.

Πηγή: [BIO-key](#)

Σε ένα κόσμο όπου η ασφάλεια δεδομένων αποτελεί κεντρικό ζήτημα, η βιομετρική αυθεντικοποίηση προσφέρει ένα επίπεδο προστασίας που υπερβαίνει κατά πολύ τις δυνατότητες των παραδοσιακών μεθόδων αυθεντικοποίησης.

1.2 Αντικείμενο της Διπλωματικής

Αντικείμενο της παρούσας διπλωματικής είναι η διερεύνηση των σύγχρονων μεθόδων και τεχνολογιών βιομετρικής αυθεντικοποίησης. Η εργασία επικεντρώνεται στην ανάλυση προηγούμενων ερευνών που έχουν πραγματοποιηθεί στο πεδίο της βιομετρικής αυθεντικοποίησης, εξετάζοντας τη σχετική βιβλιογραφία με στόχο την κατανόηση των τεχνολογιών, των εφαρμογών και την ανάδειξη των σχετικών περιορισμών και των προκλήσεων, όπως η ασφάλεια, η ιδιωτικότητα και η ευχρηστία.

Μέσα από αυτή τη διαδικασία, θα συγκεντρωθούν δεδομένα και πληροφορίες που θα επιτρέψουν την ουσιαστική σύγκριση διαφορετικών προσεγγίσεων, τεχνολογιών και μεθόδων βιομετρικής αυθεντικοποίησης, αναδεικνύοντας τα πλεονεκτήματα και τα μειονεκτήματα της καθεμίας καθώς και τις προϋποθέσεις χρήσης της.

Η εργασία δεν περιορίζεται σε μια απλή τεχνική ανάλυση, αλλά εξετάζει τις επιπτώσεις και τις προεκτάσεις της βιομετρικής αυθεντικοποίησης σε κοινωνικό και νομικό επίπεδο, δίνοντας έμφαση σε ζητήματα διαφάνειας, συγκατάθεσης, ηθικών διλημάτων και τις προκλήσεις που αντιμετωπίζουν οι οργανισμοί κατά την εφαρμογή τέτοιων τεχνολογιών, όπως η συμμόρφωση με ρυθμιστικά πλαίσια, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation – GDPR) της Ευρωπαϊκής Ένωσης (Ε.Ε.) 2016/679 και τα τεχνικά προβλήματα ακρίβειας (False Acceptance Rate – FAR, False Rejection Rate – FRR). Παράλληλα εξετάζονται οι δυνατότητες ενσωμάτωσης νέων τεχνολογιών όπως blockchain, αλλά και της εμπλοκής της τεχνητής νοημοσύνης (AI), ενισχύοντας την λειτουργικότητα και την ασφάλεια των βιομετρικών εφαρμογών και προσφέροντας κατάλληλες διεξόδους τόσο στα ζητήματα ασφάλειας, όσο και σε αυτά που αφορούν την ιδιωτικότητα.

1.2.1 Συνεισφορά

Η συνεισφορά της παρούσας διπλωματικής έγκειται στη συγκεντρωτική και περιεκτική ανάλυση της κατάστασης που επικρατεί σήμερα στον χώρο της βιομετρικής αυθεντικοποίησης, προσφέροντας στον αναγνώστη ένα πλήρες θεωρητικό υπόβαθρο πάνω στις τεχνολογίες, τις μεθόδους και τα συστήματα που χρησιμοποιούνται.

Αν και η εργασία δεν παρέχει πρωτογενή ερευνητικά δεδομένα ή μελέτες περίπτωσης, η δομή και η τεκμηρίωσή της επιτρέπουν την κατανόηση των βασικών τεχνολογικών επιλογών βιομετρικής αυθεντικοποίησης, προσφέροντας μία ολοκληρωμένη και σφαιρική εικόνα.

Ειδικότερα, η εργασία επιχειρεί να καταγράψει με κριτικό και συγκριτικό τρόπο τα πλεονεκτήματα και τα μειονεκτήματα των κυριότερων βιομετρικών τεχνολογιών και να αποτυπώσει σε έναν ενιαίο συγκριτικό πίνακα τα κύρια χαρακτηριστικά κάθε βιομετρικής τεχνολογίας σύμφωνα με βασικούς δείκτες, όπως η ακρίβεια, η ασφάλεια, η ευχρηστία, το κόστος εξοπλισμού, η παρεμβατικότητα, η καταλληλότητα. Επιπλέον, αναδεικνύονται τα βασικά προβλήματα, οι προκλήσεις και οι κίνδυνοι που σχετίζονται με την υιοθέτηση βιομετρικών λύσεων, σε συνδυασμό με τις νομοθετικές και κανονιστικές απαιτήσεις που τις διέπουν.

1.2.2 Σε τι ωφελεί

Η συγκεκριμένη εργασία επιδιώκει μία επικαιροποιημένη και συγκεντρωτική παρουσίαση των τελευταίων τάσεων γύρω από τις βιομετρικές τεχνολογίες. Παρέχει γνώσεις απαραίτητες για την επιλογή των καλύτερων προσεγγίσεων σύμφωνα με τις εκάστοτε απαιτήσεις. Ενισχύει τη συνειδητοποίηση ως προς τους κινδύνους παραβίασης της ιδιωτικότητας και την ανάγκη συμμόρφωσης με ρυθμιστικά πλαίσια ενώ παράλληλα συμβάλλει στην ανάπτυξη υπεύθυνης και ασφαλούς χρήσης των βιομετρικών τεχνολογιών στη σύγχρονη ψηφιακή εποχή.

Είναι ξεκάθαρο από τα προαναφερθέντα πως η εργασία μπορεί να προσφέρει πολύτιμες πληροφορίες για τη λειτουργία και τη χρήση βιομετρικών τεχνολογιών σε φοιτητές, ερευνητές και επαγγελματίες του χώρου της πληροφορικής και της ασφάλειας συστημάτων, διευκολύνοντας τη λήψη αποφάσεων και παρέχοντας κατάλληλη επιστημονική τεκμηρίωση.

Τέλος, αναδεικνύει μείζονα ζητήματα που σχετίζονται με την ηθική, τα κανονιστικά πλαίσια καθώς επισημαίνει ερευνητικά κενά και κατευθύνσεις για μελλοντική έρευνα και ανάπτυξη.

1.3 Δομή Διπλωματικής

Η παρούσα διπλωματική εργασία αποτελείται συνολικά από πέντε κεφάλαια και τη βιβλιογραφία. Στο πρώτο κεφάλαιο, γίνεται εισαγωγή στη βιομετρική αυθεντικοποίηση, αναλύοντας τη σημασία της στην ασφάλεια δεδομένων, τα πλεονεκτήματα, τους περιορισμούς και τις προκλήσεις που παρουσιάζει καθώς και προσδιορίζεται η συνεισφορά και τα οφέλη της τρέχουσας διπλωματικής εργασίας. Το δεύτερο κεφάλαιο παρουσιάζει την μεθοδολογία της βιβλιογραφικής ανασκόπησης, παρουσιάζοντας τα ερευνητικά ερωτήματα, τα κριτήρια και τα φίλτρα για την επιλογή και συγκέντρωση των πληροφοριών καθώς και τις πηγές αυτών ενώ προχωρά και σε μια πρώτη ποσοτική ανάλυση της επιλεγμένης βιβλιογραφίας. Το τρίτο κεφάλαιο επικεντρώνεται στην ανάλυση της σχετικής βιβλιογραφίας, παρουσιάζοντας τις βασικές αρχές της βιομετρικής αυθεντικοποίησης, τις κατηγορίες των βιομετρικών συστημάτων και τις τεχνολογικές προσεγγίσεις που έχουν προταθεί στη βιβλιογραφία, με έμφαση στη διασύνδεση της βιομετρικής με την κρυπτογραφία, το blockchain και την τεχνητή νοημοσύνη. Στο τέταρτο κεφάλαιο, γίνεται μια συγκριτική ανάλυση των διαφορετικών τεχνολογιών βιομετρικής αυθεντικοποίησης με βάση ορισμένα σημαντικά κριτήρια, παρουσιάζοντας παράλληλα τα κύρια χαρακτηριστικά, τις δυνατότητες και τους περιορισμούς κάθε τεχνολογίας. Τέλος, το τέταρτο κεφάλαιο περιλαμβάνει τα συμπεράσματα της εργασίας, συζητώντας τις προοπτικές της βιομετρικής αυθεντικοποίησης, τις τεχνολογικές τάσεις και τις ερευνητικές προκλήσεις που ανακύπτουν.

2

Μεθοδολογία Βιβλιογραφικής Ανασκόπησης

2.1 Ερευνητικά Ερωτήματα

Η παρούσα διπλωματική εργασία αποτελεί μία βιβλιογραφική ανασκόπηση των τεχνολογιών βιομετρικής αυθεντικοποίησης. Τα κύρια ερευνητικά ερωτήματα που καλείται να απαντήσει καταγράφονται ως εξής, μαζί με τα σημεία της τρέχουσας αναφοράς όπου αυτά απαντώνται:

Ερωτήματα	Ενότητα Αναφοράς
Ποιες είναι οι κυριότερες τεχνολογίες βιομετρικής αυθεντικοποίησης;	4.2
Ποια είναι τα πλεονεκτήματα και οι περιορισμοί κάθε τεχνολογίας;	4.4
Πώς επηρεάζουν παράγοντες όπως, η ασφάλεια, η ιδιωτικότητα και η νομοθεσία, τη χρήση των βιομετρικών συστημάτων;	3.7, 5.3, 5.4, 5.5, 5.6, 5.8
Ποιες τεχνολογικές εξελίξεις αναμένονται στον τομέα της βιομετρικής αυθεντικοποίησης;	3.6, 3.7, 5.4, 5.5, 5.6, 5.7, 5.8

2.2 Αναζήτηση Άρθρων

Για τις ανάγκες της εργασίας αναζητήθηκαν άρθρα στις εξής αξιόπιστες και ευρέως χρησιμοποιούμενες πηγές δεδομένων: Google Scholar, SpringerLink, IEEE Xplore, ACM Digital Library και Research Gate με συγκεκριμένες λέξεις κλειδιά και φράσεις σύμφωνα με τα αντικείμενα που πραγματεύεται η διατριβή, αξιοποιώντας τις λειτουργίες αναζήτησης AND/OR για ακριβέστερα αποτελέσματα.

Ενδεικτικές αναζητήσεις που πραγματοποιήθηκαν:

- “biometric authentication” OR “biometrics”
- “biometric” AND “security” AND “privacy”
- “fingerprint recognition”
- “iris recognition”

- “biometric” AND “blockchain”
- “biometric authentication” AND “security” AND “liveness detection”
- “biometric” AND “challenges”

Επιπλέον, αναζητήθηκαν και στην βάση International Organization for Standardization (ISO) πληροφορίες σχετικά με τα διεθνή πρότυπα.

2.3 Κριτήρια Φιλτραρίσματος Άρθρων

Το φιλτράρισμα των άρθρων πραγματοποιήθηκε σε δύο στάδια.

Στο πρώτο στάδιο τα κριτήρια ένταξης/αποκλεισμού που εφαρμόστηκαν, ήταν η επιλογή άρθρων στην αγγλική γλώσσα, δεδομένου πως η πλειοψηφία των έγκριτων επιστημονικών δημοσιεύσεων γίνεται σε αυτή τη γλώσσα, με ημερομηνία δημοσίευσης μετά το 2000, ώστε να είναι όσο το δυνατόν επίκαιρο το περιεχόμενό τους, ενώ οι αναζητήσεις πραγματοποιήθηκαν σε αξιόπιστες επιστημονικές πηγές δεδομένων (δείτε Ενότητα 2.2) και αποκλείστηκαν άρθρα που προέρχονταν από ενημερωτικές ιστοσελίδες, ειδησεογραφικά μέσα ή blogs (δηλ. «κίτρινη» βιβλιογραφία), καθώς δεν πληρούν τα κριτήρια της επιστημονικής αξιοπιστίας και εγκυρότητας. Από τα εκατό (100) άρθρα που αρχικά συλλέχθηκαν, με την εφαρμογή των παραπάνω κριτηρίων διατηρήθηκαν τα (61) εξήντα ένα.

Στο δεύτερο στάδιο εξετάστηκε το περιεχόμενο των άρθρων και κατόπιν ποιοτικής αξιολόγησης, επιλέχθηκαν άρθρα τα οποία είχαν την μεγαλύτερη συνάφεια με το αντικείμενο της μελέτης, παρέχοντας ουσιαστικές και τεκμηριωμένες πληροφορίες. Επιπλέον, επιλέχθηκαν άρθρα που παρουσίαζαν τα δεδομένα με σαφήνεια και συνοδεύονταν από ερμηνείες, επιχειρηματολογία και χρήση τυποποιημένων μετρικών αξιολόγησης (π.χ. FAR, FRR).

Τελικά, μετά τα δύο στάδια φιλτραρίσματος, επιλέχθηκαν σαράντα έξι (46) άρθρα (75%) τα οποία και συνθέτουν την βάση της παρούσας αναφοράς.

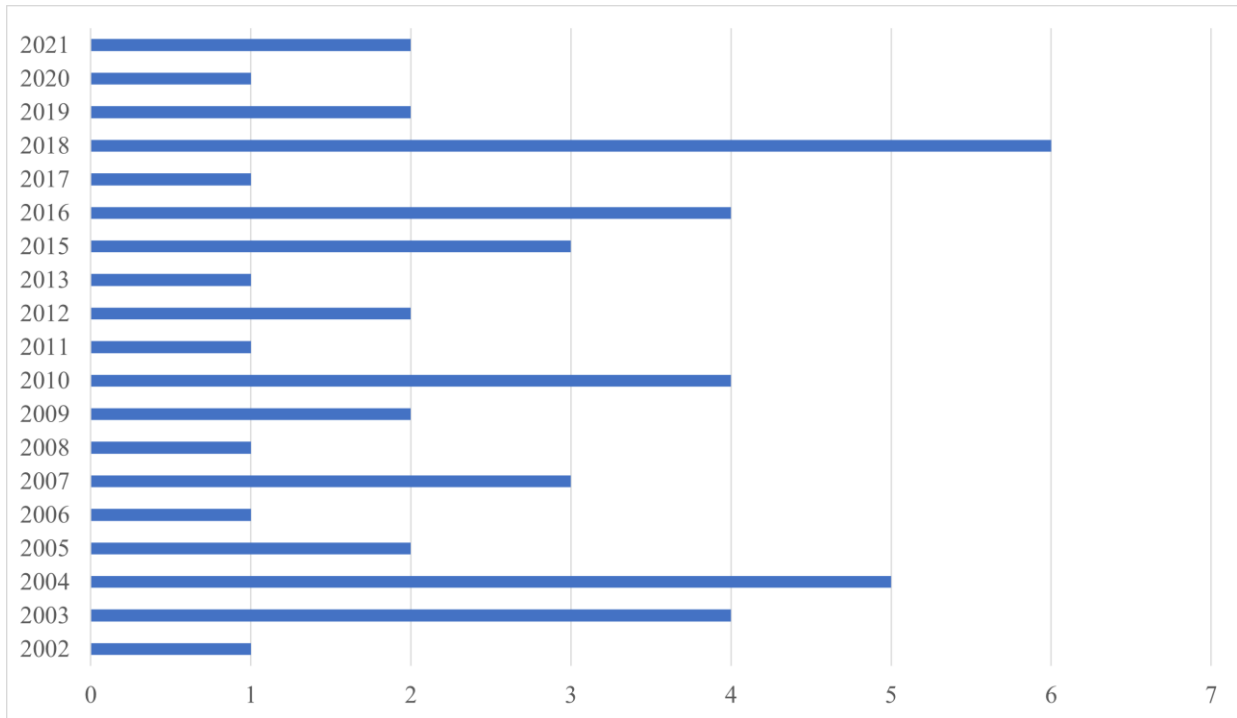
2.4 Στατιστική Ανάλυση

Η στατιστική ανάλυση των άρθρων που επιλέχθηκαν παρουσιάζεται μέσω τριών γραφημάτων. Στο πρώτο γράφημα όπου παρουσιάζεται ο αριθμός των άρθρων ανά έτος δημοσίευσης δεν διακρίνεται κάποιο ιδιαίτερο μοτίβο, ωστόσο διαφαίνεται ότι το ερευνητικό ενδιαφέρον για τις τεχνολογίες βιομετρικής αυθεντικοποίησης παραμένει σταθερό με την πάροδο των ετών. Σε γενικές γραμμές οι πηγές που χρησιμοποιήθηκαν είναι μοιρασμένες σε όλες τις χρονολογίες με το 2018 να συγκεντρώνει τις περισσότερες δημοσιεύσεις, γεγονός πιθανότατα συγκυριακό και όχι εξαιτίας κάποιας τάσης.

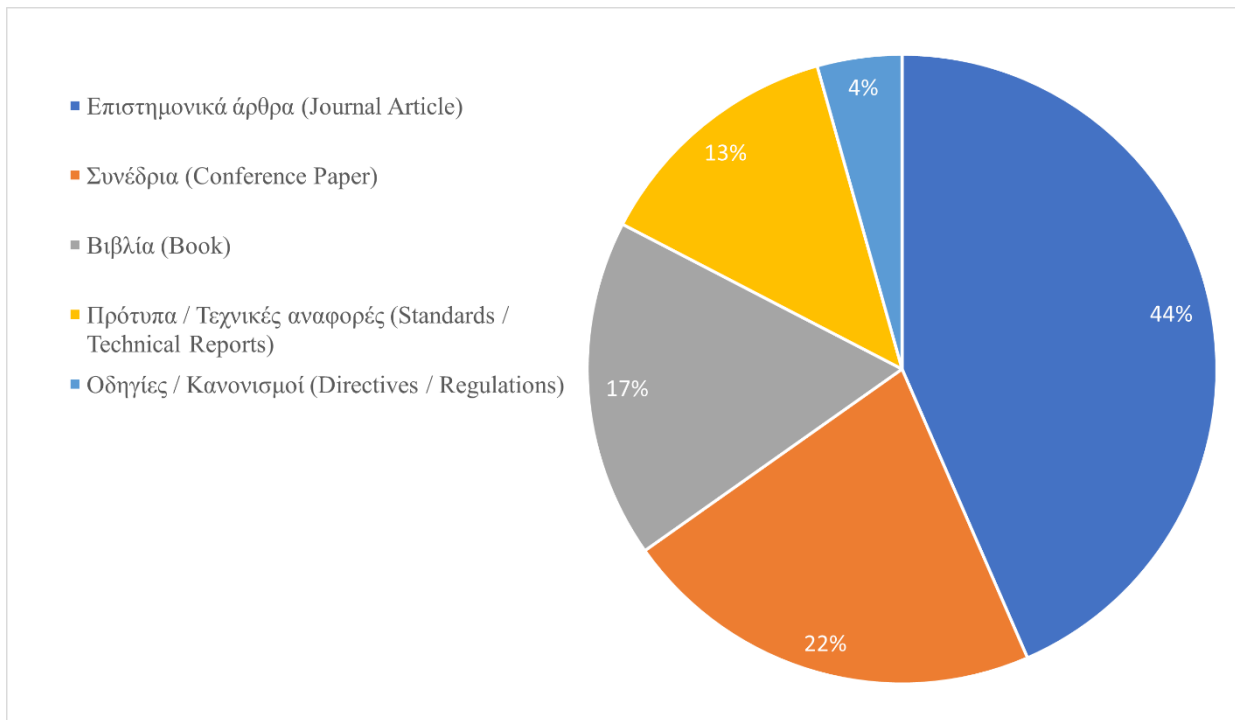
Στο δεύτερο γράφημα εμφανίζεται το ποσοστό των άρθρων ανά τύπο/είδος, όπου φαίνεται, όπως ήταν και αναμενόμενο, πως η συντριπτική πλειοψηφία των πηγών προέρχεται από άρθρα σε συνέδρια, περιοδικά και βιβλία επιβεβαιώνοντας τον ερευνητικό χαρακτήρα της βιβλιογραφίας.

Στο τρίτο γράφημα, απεικονίζεται το ποσοστό των άρθρων ανά εκδοτικό φορέα. Παρατηρείται πως η πλειοψηφία των άρθρων προέρχεται από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών

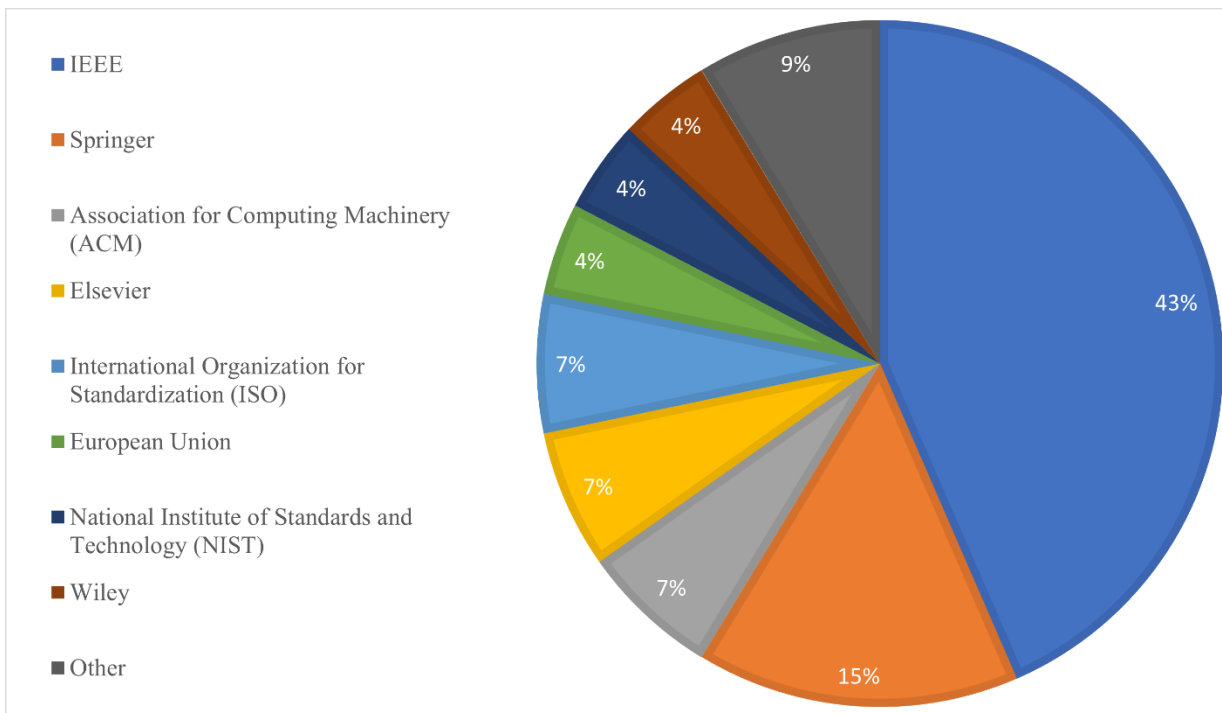
Μηχανικών (Institute of Electrical and Electronics Engineers – IEEE), κάτι το οποίο είναι αναμενόμενο εξαιτίας της τεχνολογικής φύσης του θέματος. Συνολικά, θεωρούμε με βάση τα κριτήρια φιλτραρίσματος και την παρουσιαζόμενη ποσοτική ανάλυση πως εξασφαλίζουν επιστημονική εγκυρότητα καθώς και πλουραρισμό πηγών.



Εικόνα 3: Αριθμός άρθρων ανά έτος δημοσίευσης



Εικόνα 4: Ποσοστό άρθρων ανά τύπο/είδος



Εικόνα 5: Ποσοστό άρθρων ανά εκδότη

3

Ανάλυση Βιβλιογραφίας

Το παρόν κεφάλαιο επικεντρώνεται στην ανάλυση της βιβλιογραφίας που σχετίζεται με τις τεχνολογίες βιομετρικής αυθεντικοποίησης. Παρουσιάζονται οι βασικές έννοιες που σχετίζονται με την βιομετρική αυθεντικοποίηση, οι κατηγορίες των βιομετρικών χαρακτηριστικών και η τυπική αρχιτεκτονική δομή ενός βιομετρικού συστήματος. Ακολουθεί ανάλυση επιμέρους βιομετρικών τεχνολογιών και η σύνδεσή τους με αναδυόμενες τεχνολογίες όπως την τεχνητή νοημοσύνη και το blockchain. Επιπλέον, παρουσιάζονται διαφορετικοί κλάδοι στους οποίους βρίσκουν εφαρμογή οι τεχνολογίες βιομετρικής αυθεντικοποίησης, ηθικά και νομικά ζητήματα, καθώς και οι προοπτικές και τάσεις που διαφαίνονται. Το κεφάλαιο αυτό περιλαμβάνει τόσο τις τεχνολογικές όσο και τις κοινωνικές διαστάσεις της βιομετρικής αυθεντικοποίησης.

3.1 Εισαγωγή στην Έννοια της Βιομετρικής Αυθεντικοποίησης

Σύμφωνα με τους Dharavath, Talukdar, & Laskar (2013) ένα βιομετρικό σύστημα είναι ένα σύστημα αναγνώρισης μοτίβων που πραγματοποιεί την ταυτοποίηση/επαλήθευση ενός ατόμου αντιστοιχίζοντας ένα βιομετρικό χαρακτηριστικό του ατόμου με το διαθέσιμο πρότυπο του ίδιου χαρακτηριστικού στην βάση δεδομένων. Η βιομετρική αυθεντικοποίηση, ως κλάδος που συνδυάζει τεχνικές, τεχνολογίες και μεθόδους για την επαλήθευση της ταυτότητας ενός ατόμου βάσει μοναδικών βιολογικών ή/και συμπεριφορικών χαρακτηριστικών, έχει εξελιχθεί ραγδαία τις τελευταίες δεκαετίες. Ο Jain μαζί με τους συνεργάτες του (Jain, 2004) σημειώνουν ότι αυτή η μορφή αυθεντικοποίησης έχει σχεδιαστεί για να αντιμετωπίσει τις αδυναμίες των παραδοσιακών συστημάτων που βασίζονται σε κωδικούς πρόσβασης (passwords) ή άλλα διαπιστευτήρια, όπως είναι οι κάρτες πρόσβασης (access cards) και τα PIN.

3.1.1 Πλεονεκτήματα

Βασικό πλεονέκτημα των βιομετρικών συστημάτων είναι ότι στηρίζονται σε στοιχεία που είναι εγγενή στον άνθρωπο (π.χ. δακτυλικά αποτυπώματα, ίριδα, γεωμετρία προσώπου, φωνή), άρα δεν μπορούν να “ξεχαστούν” ή να “απωλεσθούν” με την ίδια ευκολία (σε σχέση με τα παραδοσιακά

διαπιστευτήρια). Η αξιοπιστία των βιομετρικών συστημάτων οφείλεται στη μοναδικότητα και σταθερότητα των φυσικών και συμπεριφορικών χαρακτηριστικών του ατόμου, που είναι ιδιαίτερα δύσκολο να παραποιηθούν και αυτό τα καθιστά προτιμητέα επιλογή για συστήματα που απαιτούν υψηλή ασφάλεια.

3.1.2 Περιορισμοί

Ωστόσο, παρά τα προφανή πλεονεκτήματα (αυξημένη ασφάλεια, λιγότερη εξάρτηση από τη μνήμη του χρήστη), εγείρονται σοβαρά ερωτήματα και προκλήσεις, όπως το πώς αποθηκεύονται και πώς προστατεύονται αυτά τα ιδιαίτερα ευαίσθητα δεδομένα, ώστε να τηρείται η ισορροπία ανάμεσα στην ασφάλεια και την προστασία της ιδιωτικότητας.

Ένα από τα πιο κρίσιμα ζητήματα/προκλήσεις είναι η προστασία της ιδιωτικότητας και των δεδομένων. Τα βιομετρικά δεδομένα, σε αντίθεση με τις παραδοσιακές μεθόδους ταυτοποίησης, δεν μπορούν να αλλάξουν ή να επαναδημιουργηθούν σε περίπτωση παραβίασης. Αυτό σημαίνει ότι, εάν τα δεδομένα αυτά διαρρεύσουν, οι συνέπειες μπορεί να είναι σοβαρές και μακροχρόνιες για το επηρεαζόμενο άτομο. Συνεπώς, η ασφάλεια της αποθήκευσης και της διαχείρισης αυτών των δεδομένων αποτελεί ζήτημα υψίστης σημασίας.

Όπως θα διαπιστώσουμε στην συνέχεια του κεφαλαίου (Ενότητα 3.6.4), η υιοθέτηση νέων τεχνολογιών, όπως είναι το blockchain, μπορεί να προσφέρει σημαντικές λύσεις σε αυτό το ζήτημα, επιτρέποντας την εφαρμογή της βιομετρικής αυθεντικοποίησης σε πραγματικά περιβάλλοντα εξασφαλίζοντας την ιδιωτικότητα (των βιομετρικών δεδομένων).

3.2 Βασικές Αρχές και Κατηγοριοποίηση Βιομετρικών Συστημάτων

3.2.1 Φυσικά και Συμπεριφορικά Βιομετρικά Χαρακτηριστικά

Σύμφωνα με τη θεμελιώδη μελέτη του Jain (Jain, 2004), οι βιομετρικές τεχνολογίες διακρίνονται γενικώς σε δύο μεγάλες κατηγορίες ανάλογα με το είδος των βιομετρικών χαρακτηριστικών στα οποία στηρίζονται:

1. *Φυσικά (Physiological) χαρακτηριστικά*: Περιλαμβάνουν στοιχεία, όπως τα δακτυλικά αποτυπώματα, η γεωμετρία του χεριού, η ίριδα, η γεωμετρία προσώπου, η δομή των αυτιών, η ανατομία των φλεβών κ.λπ. Σε γενικές γραμμές τα φυσικά χαρακτηριστικά συνήθως παραμένουν σταθερά κατά τη διάρκεια της ζωής του ατόμου.
2. *Συμπεριφορικά (Behavioral) χαρακτηριστικά*: Εστιάζουν στις συνήθειες ή στον τρόπο εκτέλεσης μιας δραστηριότητας από το άτομο. Τυπικά παραδείγματα περιλαμβάνουν την αναγνώριση φωνής (σε συνδυασμό με τον τρόπο ομιλίας), την ανάλυση χειρόγραφης υπογραφής και τον ρυθμό πληκτρολόγησης (keystroke dynamics). Σε αντίθεση με τα φυσικά χαρακτηριστικά, τα συμπεριφορικά χαρακτηριστικά αλλάζουν με την πάροδο του χρόνου και επηρεάζονται σε μεγαλύτερο βαθμό από την κατάσταση του χρήστη.

Η αποτελεσματικότητα ενός βιομετρικού συστήματος καθορίζεται από διάφορους παράγοντες: την ακρίβειά του, τη δυνατότητα κλιμάκωσής του και την ανθεκτικότητά του απέναντι σε επιθέσεις

(όπως πλαστοπροσωπίας). Κάθε μέθοδος έχει τα δικά της πλεονεκτήματα και μειονεκτήματα· για παράδειγμα, τα δακτυλικά αποτυπώματα είναι ευρέως χρησιμοποιούμενα και τα μέσα συλλογής τους έχουν γίνει οικονομικά προσιτά, όμως η ίριδα προσφέρει, θεωρητικά, ακόμα υψηλότερη ακρίβεια και μοναδικότητα αλλά με μεγαλύτερο κόστος (Daugman, 2004).

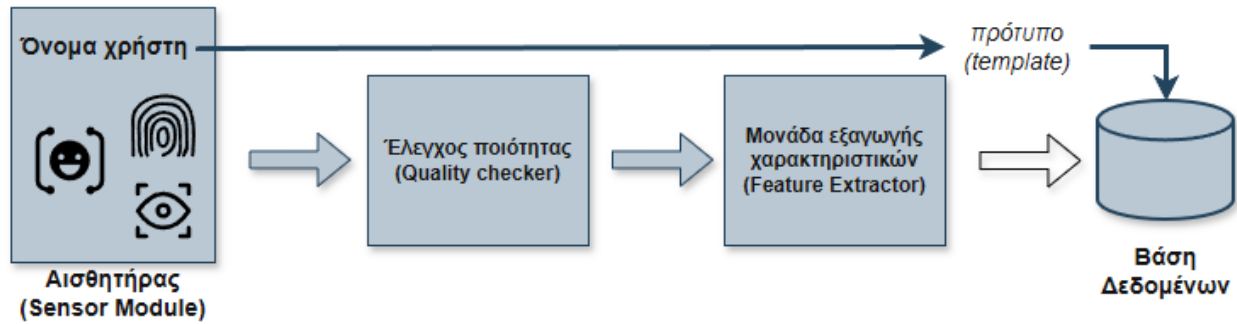
3.2.2 Βασικές Λειτουργίες & Αρχιτεκτονική ενός Βιομετρικού Συστήματος

Η λειτουργία οποιουδήποτε βιομετρικού συστήματος, όπως περιγράφουν οι Jain, Ross και Prabhakar (Jain, 2004), βασίζεται τυπικά στα εξής βήματα:

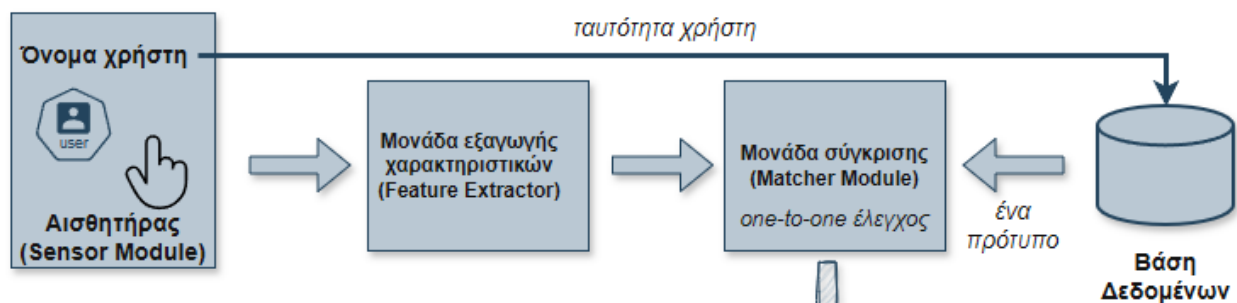
1. *Εγγραφή (Enrollment)*: Κατά τη διαδικασία αυτή, λαμβάνεται το βιομετρικό δείγμα (π.χ. το δακτυλικό αποτύπωμα ή η εικόνα της ίριδας) και δημιουργείται ένα πρότυπο (template) μέσω εξειδικευμένων αλγορίθμων εξαγωγής χαρακτηριστικών. Το πρότυπο ακολουθεί διεθνή πρότυπα ISO/IEC όπου η μορφή του διαφοροποιείται για την κάθε βιομετρική μέθοδο και αποθηκεύεται σε υποκείμενη βάση δεδομένων.
2. *Επαλήθευση (Verification)*: Σύγκριση του δείγματος μόνο με το πρότυπο του χρήστη μέσω ενός one-to-one ελέγχου (εφόσον έχει ήδη εντοπιστεί το πρότυπο του χρήστη μέσω κάποιας άλλης διαδικασίας π.χ. username ή το σύστημα έχει μόνο ένα χρήστη π.χ. κινητό τηλέφωνο). Μέσω της σύγκρισης υπολογίζονται οι αντίστοιχοι δείκτες ομοιότητας. Αν υπερβαίνουν ένα καθορισμένο όριο (threshold), τότε ο χρήστης θεωρείται αυθεντικοποιημένος, διαφορετικά η πρόσβαση απορρίπτεται.
3. *Ταυτοποίηση (Identification)*: Εύρεση της ταυτότητας του χρήστη μέσω μιας one-to-many αντιστοίχισης στην βάση δεδομένων όπου συγκρίνεται το δείγμα με όλα τα πρότυπα χρηστών μέχρι να εντοπιστεί η σωστή αντιστοίχιση, εφόσον υπάρχει.

Τα κύρια συστατικά αρχιτεκτονικής ενός βιομετρικού συστήματος είναι:

1. *Αισθητήρας (Sensor Module)*: Η μονάδα για την συλλογή του βιομετρικού δείγματος.
2. *Μονάδα εξαγωγής χαρακτηριστικών (Feature Extraction Module)*: Εξάγει τα χαρακτηριστικά που θα χρησιμοποιηθούν για την δημιουργία του προτύπου.
3. *Μονάδα σύγκρισης (Matcher Module)*: Η μονάδα που συγκρίνει τα εξαγόμενα χαρακτηριστικά με τα αποθηκευμένα πρότυπα και υπολογίζει τον δείκτη ομοιότητας.
4. *Βάση δεδομένων*: Χρησιμοποιείται για την αποθήκευση των προτύπων και την αναζήτηση κατά την ταυτοποίηση ενός χρήστη.

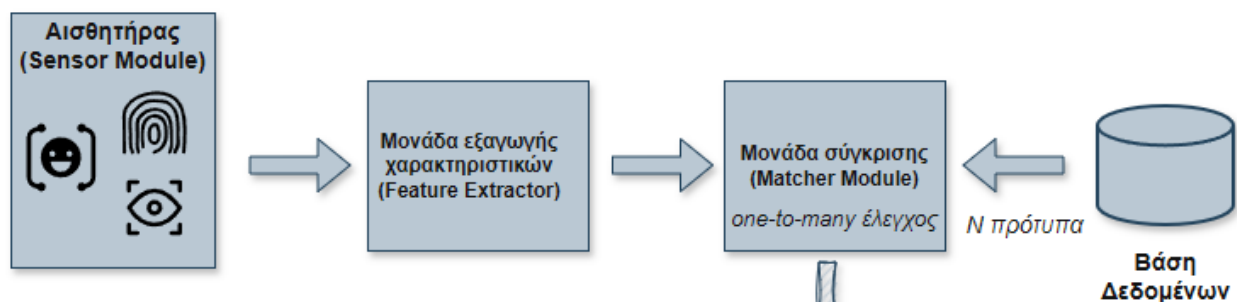


Εγγραφή (Enrollment)



Επαλήθευση (Verification)

Το χαρακτηριστικό αντιστοιχεί/δεν αντιστοιχεί στον χρήστη



Ταυτοποίηση (Identification)

Ταυτοποίηση χρήστη / Ο χρήστης δεν βρέθηκε

Εικόνα 6: Διάγραμμα με τα κύρια συστατικά αρχιτεκτονικής ενός βιομετρικού συστήματος

3.3 Αναγνώριση Ίριδας και Άλλες Προηγμένες Βιομετρικές Μέθοδοι

3.3.1 Η Τεχνολογία της Ίριδας και η Μελέτη του Daugman

Σύμφωνα με τον Daugman (Daugman, 2004), η ίριδα αποτελεί έναν από τους πιο αξιόπιστους βιομετρικούς δείκτες, καθώς η δομή της παραμένει σταθερή και παρουσιάζει υψηλό βαθμό μοναδικότητας ακόμα και μεταξύ μονοζυγωτικών διδύμων. Τα συστήματα αναγνώρισης ίριδας βασίζονται κυρίως στην εξαγωγή χαρακτηριστικών με χρήση φίλτρων Gabor ή σε παρόμοιες τεχνικές, ενώ η διαδικασία σύγκρισης βασίζεται σε υπολογισμό απόστασης τύπου Hamming.

Οι υψηλοί δείκτες ακρίβειας της ίριδας (χαμηλό ποσοστό σφάλματος) καθιστούν αυτή την τεχνολογία κατάλληλη για περιβάλλοντα υψηλής ασφάλειας, όπως αεροδρόμια ή στρατιωτικές εγκαταστάσεις. Παρόλα αυτά, οι υποδομές που απαιτούνται (συγκεκριμένοι σαρωτές, ρύθμιση φωτισμού) ενδεχομένως αυξάνουν το κόστος εγκατάστασης.

3.3.2 Ζητήματα Αποθήκευσης και Προστασίας Δεδομένων

Η αποθήκευση των δεδομένων της ίριδας εγείρει σοβαρές ανησυχίες, καθώς οι πληροφορίες αυτές δεν αλλάζουν καθ' όλη τη διάρκεια της ζωής ενός ανθρώπου. Όπως επισημαίνουν οι Rathgeb και Busch (Rathgeb, 2012), οποιαδήποτε διαρροή ή παραβίαση μιας βάσης δεδομένων που περιέχει βιομετρικά πρότυπα ίριδας είναι εξαιρετικά δύσκολο να αντιμετωπιστεί: σε αντίθεση με έναν κωδικό πρόσβασης, η ίριδα δεν “αλλάζει”. Αν λοιπόν ένας κακόβουλος φορέας καταφέρει να αναδημιουργήσει ή να αντιγράψει το πρότυπο, οι συνέπειες μπορεί να είναι μακροχρόνιες.

Για τον λόγο αυτό, μεγάλο μέρος της ερευνητικής δραστηριότητας εστιάζει στις τεχνικές προστασίας και ανωνυμοποίησης των δεδομένων, κάτι που μας οδηγεί στις μελέτες που συνδέουν τη βιομετρική αυθεντικοποίηση με την κρυπτογραφία (δείτε Ενότητα 3.4).

Η βιβλιογραφία των τελευταίων ετών αναδεικνύει διάφορες πτυχές αυτών των ζητημάτων, επιχειρώντας να δώσει λύσεις για την ανάπτυξη συστημάτων που όχι μόνο θα είναι τεχνικά αποτελεσματικά, αλλά και νομικά και ηθικά αποδεκτά (Jain et al., 2004; Prabhakar et al., 2003).

3.4 Διασύνδεση Βιομετρικής με Κρυπτογραφία

3.4.1 Βιομετρικά Κρυπτοσυστήματα και το Fuzzy Vault

Οι Uludag, Pankanti, Prabhakar και Jain (Uludag, 2004) πραγματοποίησαν μια εκτενή ανάλυση για το πώς μπορεί η κρυπτογραφία να ενσωματωθεί σε βιομετρικές εφαρμογές, ώστε να επιτευχθεί αυξημένη προστασία των δεδομένων κατά την αποθήκευση και την επεξεργασία τους. Η βασική ιδέα των βιομετρικών κρυπτοσυστημάτων είναι ότι το βιομετρικό πρότυπο δεν αποθηκεύεται σε απλή μορφή, αλλά “κλειδώνεται” μέσω κρυπτογραφικών μηχανισμών, με τρόπο που να είναι δυνατή η ανάκτησή του (ή η σύγκρισή του) μόνο αν ο χρήστης προσκομίσει το σωστό βιομετρικό χαρακτηριστικό.

Ένα χαρακτηριστικό παράδειγμα τέτοιας προσέγγισης είναι το “fuzzy vault”, που περιγράφεται από τους Juels και Sudan (Juels, 2006). Σε αυτό το σχήμα:

- Η βιομετρική πληροφορία ενσωματώνεται σε μια κρυπτογραφημένη δομή, μαζί με “παραπλανητικά” (chaff) δεδομένα.
- Χωρίς το σωστό βιομετρικό δείγμα, είναι πρακτικά αδύνατο να διαχωριστούν τα πραγματικά δεδομένα από τα παραπλανητικά.
- Αντιθέτως, με το σωστό δείγμα, το σύστημα μπορεί να ανακτήσει το “κλειδί” και να αποκρυπτογραφήσει τις αποθηκευμένες πληροφορίες.

Αυτή η τεχνική επιλύει εν μέρει το ζήτημα της ασφαλούς αποθήκευσης: ακόμα και αν διαρρεύσει η ακατέργαστη μορφή της “κρυπτογραφημένης θήκης” (vault), ο επιτιθέμενος δεν μπορεί εύκολα να εξαγάγει τη βιομετρική πληροφορία και να τη χρησιμοποιήσει.

3.4.2 Robust Hashing

3.4.2.1 Βασική ιδέα

Παράλληλα, οι Sutcu, Sencar και Memon (Sutcu et al., 2007) εστιάζουν στην ιδέα του robust hashing (ρωμαλέου κατακερματισμού). Στόχος είναι να παραχθεί ένα κρυπτογραφικό hash από βιομετρικά δεδομένα, το οποίο όμως να μην αλλάζει δραστικά σε περίπτωση ελαφρών διαφοροποιήσεων (π.χ. θορύβου στη λήψη του δακτυλικού αποτυπώματος ή διαφορετικής γωνίας στην κάμερα). Αυτή η τεχνική επιτρέπει τη δημιουργία ενός “αποτυπώματος” (fingerprint) των βιομετρικών δεδομένων που δεν αντιγράφεται εύκολα, ενώ παράλληλα παραμένει συμβατό σε μικρές αποκλίσεις και θόρυβο.

Η βασική πρόκληση εδώ είναι να εξισορροπηθεί η ανθεκτικότητα του hashing σε μικρές αλλοιώσεις με την ικανότητά του να διακρίνει διαφορετικούς χρήστες. Μια απλή κρυπτογραφική συνάρτηση hash θα άλλαζε πλήρως ακόμα και με την παραμικρή αλλαγή της εισόδου (property of avalanche effect), κάτι που δεν είναι ιδανικό για βιομετρικά δεδομένα, όπου μικροδιαφορές ανάμεσα σε π.χ. δύο σαρώσεις του ίδιου δακτυλικού αποτυπώματος είναι αναπόφευκτες.

3.4.2.2 Η Αξία του Robust Hashing και η Ανθεκτικότητα σε Πλαστοπροσωπία

Οι επιθέσεις πλαστοπροσωπίας (spoofing attacks) είναι ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν τα βιομετρικά συστήματα. Για παράδειγμα, μπορεί κάποιος να “αντιγράψει” ένα δακτυλικό αποτύπωμα φτιάχνοντας καλούπι σιλικόνης ή να χρησιμοποιήσει υψηλής ανάλυσης φωτογραφίες προσώπου για να εξαπατήσει ένα σύστημα αναγνώρισης προσώπου. Οι Sutcu, Sencar και Memon (Sutcu et al., 2007) προτείνουν τεχνικές βασισμένες σε robust hashing που προσθέτουν επιπλέον στρώματα προστασίας, όπως:

- *Αλγορίθμους εντοπισμού “ζωντανού” δείγματος (liveness detection)*: Π.χ. έλεγχος μικροκινήσεων στην ίριδα, ροή αίματος στα δάκτυλα, ή θερμοκρασία επιφάνειας δέρματος.

- *Χρήση τυχαίων προκλήσεων (challenge-response)*: Το σύστημα ζητά από τον χρήστη να αλληλεπιδράσει με συγκεκριμένο τρόπο (π.χ. να κουνήσει τα μάτια), μειώνοντας έτσι τις πιθανότητες εξαπάτησης με στατικές εικόνες ή βίντεο.

Η διαρκής εξέλιξη των αλγορίθμων πλαστοπροσωπίας και η ανάδυση επιθέσεων με τη χρήση τεχνητής νοημοσύνης (AI) και “deepfakes” καθιστούν τη θωράκιση των βιομετρικών συστημάτων ένα ανεξάντλητο πεδίο έρευνας.

3.5 Ανάλυση της Γεωμετρίας του Χεριού και Εναλλακτικές

Προσεγγίσεις

3.5.1 Η Μελέτη των Kumar και Zhang

Η γεωμετρία του χεριού είναι μια από τις “παλαιότερες” βιομετρικές τεχνικές που βρήκαν εφαρμογή σε εμπορικές λύσεις ελέγχου πρόσβασης, συχνά σε συνδυασμό με αναγνώστες καρτών. Η μελέτη των Kumar και Zhang (Kumar, 2007) αναλύει τους τρόπους με τους οποίους η ακριβής δειγματοληψία και η αξιοποίηση αλγορίθμων διάκρισης με βάση την εντροπία (entropy-based discretization) μπορούν να βελτιώσουν την ακρίβεια των συστημάτων που βασίζονται στη γεωμετρία του χεριού. Ενώ η μέθοδος αυτή δεν φτάνει την ακρίβεια της ίριδας ή των δακτυλικών αποτυπωμάτων, πλεονεκτεί σε περιβάλλοντα όπου, για παράδειγμα, τα δακτυλικά αποτυπώματα μπορεί να μην είναι διαυγή (π.χ. σε βιομηχανίες με πολλή σκόνη ή υγρασία).

3.5.2 Ποικιλομορφία Επιλογών για Διάφορα Περιβάλλοντα

Το εύρος των βιομετρικών επιλογών (γεωμετρία χεριού, αναγνώριση παλάμης, ανάλυση φλεβών κ.λπ.) επιτρέπει την προσαρμογή της εκάστοτε λύσης στις ανάγκες κάθε τομέα ή επιχείρησης. Οι οπτικές σαρώσεις φλεβών, για παράδειγμα, θεωρούνται εξαιρετικά ασφαλείς και δύσκολο να παραβιαστούν, αλλά απαιτούν ιδιαίτερο εξοπλισμό και είναι σχετικά ακριβές. Αντιθέτως, συστήματα βασισμένα στη γεωμετρία του χεριού δεν χρειάζονται πολύπλοκο εξοπλισμό, αλλά είναι λιγότερο ασφαλή σε περιπτώσεις σύνθετων απειλών και ευάλωτα σε επιθέσεις πλαστοπροσωπίας (Jain et al., 2007), π.χ. πλαστικών αντιγράφων χεριού.

Η κεντρική επισήμανση από τη βιβλιογραφία είναι ότι δεν υπάρχει “μία λύση” που να ταιριάζει σε όλα τα περιβάλλοντα· αντίθετα, απαιτείται μια ολιστική προσέγγιση που λαμβάνει υπόψη παράγοντες κόστους, ασφάλειας, ακρίβειας και χρηστικότητας.

3.6 Προχωρημένες Τεχνικές και Τάσεις στο Βιομετρικό Πεδίο

Η ενσωμάτωση αναδυόμενων τεχνολογιών και καινοτομιών με τις τεχνολογίες βιομετρικής αυθεντικοποίησης δημιουργεί θετικές προοπτικές.

3.6.1 Πολυτροπικές Βιομετρικές Προσεγγίσεις

Η πολυτροπική βιομετρική (multimodal biometric) αυθεντικοποίηση αναφέρεται στη χρήση περισσότερων του ενός βιομετρικών χαρακτηριστικών για την αυθεντικοποίηση (π.χ. συνδυασμός δακτυλικού αποτυπώματος, ίριδας και φωνής). Το πλεονέκτημα αυτής της προσέγγισης είναι ότι δυσχεραίνει ακόμη περισσότερο την προσπάθεια πλαστοπροσωπίας (spoofing), ενώ βελτιώνει τους δείκτες FAR και FRR. Βεβαίως, η πολυτροπία απαιτεί επιπλέον εξοπλισμό (π.χ. πολλαπλούς σαρωτές) και πιο σύνθετους αλγορίθμους συνένωσης δεδομένων (data fusion) καθώς απαιτείται ο συνδυασμός διαφορετικών μορφών βιομετρικών χαρακτηριστικών.

3.6.2 Ανάλυση Συμπεριφοράς σε Πραγματικό Χρόνο

Πέρα από τα “στατικά” φυσιολογικά χαρακτηριστικά, ορισμένες μελέτες εξετάζουν τη διαρκή επαλήθευση της ταυτότητας βάσει συμπεριφορικών δεικτών (continuous authentication). Για παράδειγμα:

- Η ταχύτητα και ο ρυθμός πληκτρολόγησης (keystroke dynamics).
- Οι κινήσεις του ποντικιού (mouse dynamics).
- Το μοτίβο βαδίσματος (gait recognition).

Αυτές οι μέθοδοι μπορούν να εντοπίσουν ένα “switch” («αλλαγή διακόπτη») σε ένα σύστημα: αν, π.χ., κάποιος εξουσιοδοτημένος χρήστης αφήσει ανοιχτό τον υπολογιστή του και πάει για διάλειμμα, μπορεί να γίνει ανίχνευση ότι κάποιος άλλος χρησιμοποιεί πλέον το πληκτρολόγιο, οπότε το σύστημα τον αποσυνδέει αυτόματα ή ζητά εκ νέου βιομετρική επαλήθευση.

3.6.3 Βιομετρική Αυθεντικοποίηση στο Internet of Things (IoT)

Ένας από τους πιο υποσχόμενους τομείς εφαρμογής είναι το Internet of Things (IoT) (Διαδίκτυο των Πραγμάτων), όπου η βιομετρική αυθεντικοποίηση μπορεί να χρησιμοποιηθεί για την ασφαλή πρόσβαση σε έξυπνες συσκευές και συστήματα. Στις έξυπνες πόλεις, οι τεχνολογίες αυτές μπορούν να διασφαλίσουν την ασφαλή χρήση των υποδομών, όπως τα μέσα μεταφοράς, τα δημόσια κτίρια και οι υπηρεσίες κοινής ωφέλειας.

Η έρευνα των Yang και Hu (Yang, 2010) επικεντρώνεται στην ασφάλεια του IoT, όπου πλήθος συσκευών διασυνδέονται (έξυπνα ρολόγια, wearables, αισθητήρες σε βιομηχανικά περιβάλλοντα, έξυπνες οικιακές συσκευές κ.ά.). Εφόσον αυτά τα αντικείμενα συχνά συλλέγουν ή διαχειρίζονται κρίσιμα δεδομένα, η διασφάλιση ότι μόνο εξουσιοδοτημένα άτομα τα χειρίζονται είναι κεφαλαιώδους σημασίας. Σε αυτό το πλαίσιο, η βιομετρική αυθεντικοποίηση προσφέρει ένα επιπλέον επίπεδο προστασίας.

Ωστόσο, η ενσωμάτωση των βιομετρικών συστημάτων σε συσκευές IoT δεν είναι απλή υπόθεση. Απαιτείται:

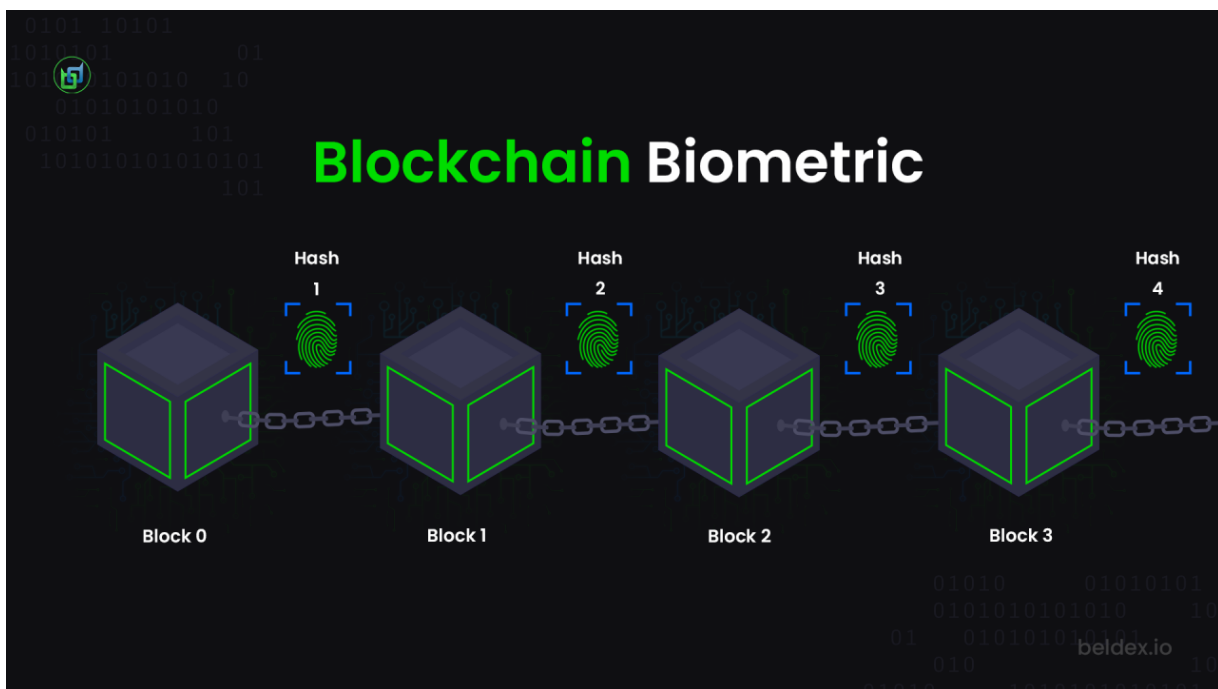
- *Επεξεργαστική ισχύς*: Πολλές IoT συσκευές έχουν χαμηλή υπολογιστική δυνατότητα, κάτι που κάνει την εκτέλεση εξελιγμένων αλγορίθμων επεξεργασίας βιομετρικών δεδομένων δύσκολη.

- *Ασφαλής επικοινωνία:* Τα βιομετρικά δεδομένα πρέπει να μεταφέρονται (ή να αποθηκεύονται) με τρόπο που αποτρέπει τη διαρροή, λ.χ. μέσω κρυπτογραφημένων συνδέσεων.
- *Διαχείριση ενέργειας:* Οι φορητές συσκευές έχουν μπαταρίες περιορισμένης χωρητικότητας· συνεπώς, οι αλγόριθμοι (επεξεργασίας βιομετρικών δεδομένων) θα πρέπει να είναι αρκετά αποδοτικοί, ώστε να μη μειώνουν τη διάρκεια ζωής της μπαταρίας σε υπερβολικό βαθμό.

Παρά τα εμπόδια, η τάση δείχνει ότι ο ρόλος της βιομετρικής αυθεντικοποίησης στις εφαρμογές IoT θα γίνει ολοένα και πιο σημαντικός, δεδομένης της ανάγκης για απρόσκοπτη (και ταυτόχρονα ασφαλή) χρήση των έξυπνων συσκευών σε καθημερινό επίπεδο.

3.6.4 Βιομετρική Αυθεντικοποίηση και Blockchain

Η ενσωμάτωση της βιομετρικής τεχνολογίας με τεχνολογίες blockchain, όπως το Hyperledger Fabric, μπορεί να παρέχει μια αποτελεσματική λύση τόσο στις προκλήσεις ιδιωτικότητας όσο και στα ζητήματα ασφάλειας. Το blockchain, χάρη στη διαφανή και αμετάβλητη φύση του, επιτρέπει την ασφαλή αποθήκευση των βιομετρικών δεδομένων, ενώ ταυτόχρονα διασφαλίζει την ιδιωτικότητα μέσω προηγμένων τεχνικών κρυπτογράφησης. Επιπλέον, η δυνατότητα ανιχνευσιμότητας που παρέχει το blockchain επιτρέπει τη διαφάνεια στις συναλλαγές και τη διαχείριση δεδομένων, καθιστώντας το μια ιδανική πλατφόρμα για την προστασία ευαίσθητων πληροφοριών.



Εικόνα 7: Βιομετρική αυθεντικοποίηση & Blockchain

Πηγή: [Beldex](https://beldex.io)

Οι Khan και Salah (Khan, 2018) αναδεικνύουν τη δυναμική που έχει η ενσωμάτωση των βιομετρικών δεδομένων με την τεχνολογία blockchain. Το blockchain, ως ένα κατακεντρωμένο καθολικό (distributed ledger), μπορεί να επιτρέψει τη διαφάνεια και την αμεταβλητότητα στην αποθήκευση και την κοινή χρήση των βιομετρικών προτύπων:

- *Αμετάβλητη Ιστορικότητα (Immutability)*: Μόλις αποθηκευτούν τα βιομετρικά δεδομένα (ή τα κρυπτογραφικά hash τους) σε ένα blockchain, είναι εξαιρετικά δύσκολο να αλλοιωθούν χωρίς αυτό να γίνει αντιληπτό. Επίσης, η αλλοίωση αυτή έχει μεγάλο κόστος διότι θα πρέπει να αναδημιουργηθεί μεγάλο μέρος του blockchain από το μπλοκ που έχει υποστεί την αλλαγή και έπειτα.
- *Έλεγχος πρόσβασης και Διασφάλιση Ιδιωτικότητας*: Με έξυπνα συμβόλαια (smart contracts), μπορεί να οριστεί ποιος κόμβος έχει πρόσβαση σε ποια δεδομένα και υπό ποιες συνθήκες. Με αυτόν τον τρόπο, ο χρήστης μπορεί να διατηρεί τον έλεγχο των δικών του βιομετρικών πληροφοριών, σε αντίθεση με τις παραδοσιακές, κεντροποιημένες βάσεις δεδομένων.
- *Κρατικά ή Επιχειρησιακά Δίκτυα*: Η τεχνολογία blockchain μπορεί να αξιοποιηθεί σε ιδιωτικά δίκτυα (permissioned blockchains), όπου οι κόμβοι είναι προκαθορισμένοι (π.χ. διάφοροι οργανισμοί-εταίροι), και τα δεδομένα συγχρονίζονται με ασφάλεια και κατακεντρωμένο τρόπο.

Η ωρίμανση της έρευνας σε αυτό το πεδίο υπόσχεται πιο διαφανείς και ανιχνεύσιμες διαδικασίες που ενισχύουν την εμπιστοσύνη των χρηστών, παρόλο που παραμένουν ανοιχτά ορισμένα ζητήματα σχετικά με την κλιμάκωση, την ταχύτητα των συναλλαγών και την ασφάλεια των “έξυπνων συμβολαίων”.

3.6.4.1 Πλεονεκτήματα της Αποκεντρωμένης Αποθήκευσης

Στη μελέτη των Khan και Salah (2018) γίνεται σαφές ότι τα βιομετρικά συστήματα μπορούν να επωφεληθούν από την αποκεντρωμένη φιλοσοφία του blockchain. Αντί να φυλάσσονται τα βιομετρικά πρότυπα σε έναν κεντρικό εξυπηρετητή, διανέμονται σε ένα δίκτυο κόμβων που επικυρώνουν από κοινού τις συναλλαγές. Αυτό:

- Δυσχεραίνει τις επιθέσεις, καθώς ο επιτιθέμενος δεν έχει ένα και μοναδικό σημείο-στόχο (single point of failure) ώστε να επιδράσει στη διαθεσιμότητα του συστήματος.
- Επιτρέπει την ιχνηλασιμότητα (traceability) κάθε πρόσβασης ή τροποποίησης μέσω νέου μπλοκ, χωρίς να αλλάζουν τα ήδη καταγεγραμμένα δεδομένα, διασφαλίζοντας έτσι την ιστορικότητα και την ακεραιότητα.
- Ενισχύει την εμπιστοσύνη, μιας και οι συμμετέχοντες στο δίκτυο μπορούν να επιβεβαιώνουν την ακεραιότητα των δεδομένων όποτε το επιθυμούν.

3.6.4.2 Παράδειγμα Εφαρμογής

Ενδεικτικά, σκεφτείτε ένα σενάριο όπου διαφορετικοί οργανισμοί (μια τράπεζα, μια ασφαλιστική εταιρεία και ένα νοσοκομείο) θέλουν να μοιράζονται βιομετρικά δεδομένα πελατών/ασθενών για

ταχύτερη επαλήθευση ταυτότητας, αλλά χωρίς να έχει κεντρικό έλεγχο ένας εκ των τριών. Ένα consortium blockchain ή ένα permissioned blockchain, με σωστή διαχείριση ρόλων (role-based access), θα μπορούσε να αποθηκεύει τα κρυπτογραφημένα “hash” των βιομετρικών, επιτρέποντας παράλληλα στους κόμβους να επαληθεύουν την ταυτότητα του χρήστη χωρίς να εκθέτουν τις ευαίσθητες πληροφορίες. Έτσι, κάθε φορά που ο χρήστης επιθυμεί να συνδεθεί σε μια υπηρεσία, παρουσιάζει το βιομετρικό δείγμα και η διαλειτουργικότητα μεταξύ των οργανισμών πραγματοποιείται μέσω του blockchain.

3.6.5 Ενοποίηση με Τεχνητή Νοημοσύνη

Παράλληλα με την κλασική προσέγγιση επεξεργασίας σήματος, τα τελευταία χρόνια γίνονται εκτεταμένες προσπάθειες ενσωμάτωσης τεχνικών βαθιάς μάθησης (deep learning) στη βιομετρική αυθεντικοποίηση. Νευρωνικά δίκτυα τύπου Convolutional Neural Networks (CNNs) (Συνελικτικά Νευρωνικά Δίκτυα) μπορούν να μάθουν χαρακτηριστικά των βιομετρικών δεδομένων απευθείας από μεγάλα σύνολα εικόνων, βελτιώνοντας την ακρίβεια και την ανθεκτικότητα σε θόρυβο ή αλλοιώσεις (Plesh et al., 2019). Η ενσωμάτωση τεχνικών τεχνητής νοημοσύνης έχει ήδη αρχίσει να εφαρμόζεται σε σύγχρονα βιομετρικά συστήματα, όπως τα AI-based (βασισμένα σε Τεχνητή Νοημοσύνη) συστήματα, που προσφέρουν βελτιωμένες επιδόσεις και ανθεκτικότητα. Όμως, η τεχνητή νοημοσύνη αναπτύσσεται παράλληλα και στον τομέα των επιθέσεων (adversarial attacks), καθιστώντας αναγκαία την επικαιροποίηση των αμυντικών τεχνικών.

Η ενσωμάτωση της τεχνητής νοημοσύνης και της μηχανικής μάθησης στα βιομετρικά συστήματα έχει ανοίξει νέους ορίζοντες για την ασφάλεια δεδομένων. Οι προσαρμοστικοί αλγόριθμοι είναι πλέον σε θέση να μαθαίνουν και να προσαρμόζονται στη συμπεριφορά του χρήστη, βελτιώνοντας την ακρίβεια και την αποδοτικότητα με την πάροδο του χρόνου. Επιπλέον, η ενσωμάτωση προηγμένων τεχνολογιών επιτρέπει την ανίχνευση πλαστών ή μη εξουσιοδοτημένων προσπαθειών πρόσβασης, ενισχύοντας έτσι την ανθεκτικότητα των συστημάτων απέναντι σε απειλές (Bahmani et al., 2021; Akhtar & Mian, 2018; Sun et al., 2020).

3.7 Προκλήσεις και Προοπτικές στη Βιομετρική Αυθεντικοποίηση

3.7.1 Ζητήματα Ιδιωτικότητας και Νομοθεσίας

Ένα από τα πιο ευαίσθητα σημεία της βιομετρικής αυθεντικοποίησης είναι η διαχείριση και προστασία των δεδομένων. Σε πολλές περιοχές του πλανήτη, η νομοθεσία (όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων – GDPR στην Ευρώπη) επιβάλλει αυστηρούς κανόνες για τη συλλογή, επεξεργασία και αποθήκευση ευαίσθητων πληροφοριών, στις οποίες συγκαταλέγονται και τα βιομετρικά δεδομένα. Αυτές οι απαιτήσεις οδηγούν σε:

- *Πολύπλοκα σχήματα συγκατάθεσης:* Οι χρήστες πρέπει να γνωρίζουν και να αποδέχονται με σαφήνεια πώς θα χρησιμοποιηθούν τα βιομετρικά τους στοιχεία και ποιος τα διαχειρίζεται.

- *Υψηλά κόστη συμμόρφωσης:* Οι οργανισμοί καλούνται να υλοποιήσουν τεχνικά μέτρα προστασίας, όπως ανωνυμοποίηση, κρυπτογράφηση, διαδικασίες ελέγχου πρόσβασης κ.ά. με υψηλό κόστος υλοποίησης.
- *Νομικές ευθύνες:* Τυχόν διαρροή ή κακόβουλη χρήση των βιομετρικών δεδομένων μπορεί να επιφέρει σοβαρές κυρώσεις και πρόστιμα για τις εμπλεκόμενες επιχειρήσεις.

Παράλληλα, εκφράζονται έντονοι ηθικοί προβληματισμοί: μερικοί ερευνητές υποστηρίζουν ότι η εκτεταμένη χρήση βιομετρικών συστημάτων ενδέχεται να διευκολύνει τεχνικές μαζικής επιτήρησης (mass surveillance), ειδικά αν συνδυαστεί με προηγμένες αναλύσεις δεδομένων, όπως η αναγνώριση προσώπου σε δημόσιους χώρους.

3.7.2 Ηθικές και Κοινωνικές Διαστάσεις της Βιομετρικής Αυθεντικοποίησης

3.7.2.1 Μαζική Επιτήρηση και Ανησυχίες Πολιτών

Η πιθανότητα “ορθής” ή “κακής” χρήσης της βιομετρικής είναι ένα από τα δυσκολότερα ηθικά ζητήματα που τίγουν οι σχετικές μελέτες. Εργασίες όπως αυτή των Rathgeb και Busch (Rathgeb, 2012) επισημαίνουν ότι οι πολίτες φοβούνται ενίοτε τη διάβρωση του δικαιώματος στην ιδιωτικότητα· τα βιομετρικά συστήματα μπορούν να καταγράψουν πού και πότε βρέθηκε κάποιος, με απρόβλεπτες συνέπειες. Αν δεν υπάρχουν διαφανείς διαδικασίες και σαφές νομικό πλαίσιο, ελλοχεύει κίνδυνος “biometric profiling” (δημιουργίας βιομετρικών προφίλ), όπου οι άνθρωποι κατηγοριοποιούνται ή ελέγχονται εν αγνοία τους.

3.7.2.2 Ευθύνη και Λογοδοσία

Σε περίπτωση διαρροής ή κατάχρησης βιομετρικών δεδομένων, τίθεται το ερώτημα: ποιος φέρει την ευθύνη; Είναι ο οργανισμός που μάζεψε τα δεδομένα, ο πάροχος της τεχνολογίας ή ο κάτοχος της συσκευής; Τα νομικά καθεστώτα σε κάθε χώρα δεν έχουν ακόμα δώσει ξεκάθαρες απαντήσεις, προκαλώντας αβεβαιότητα τόσο για τους πολίτες όσο και για τις επιχειρήσεις. Ωστόσο είναι δυνατή η σύναψη συμβάσεων (SLAs) μεταξύ των εμπλεκόμενων μερών ώστε να είναι ξεκάθαρες οι υποχρεώσεις, τα δικαιώματα και η κατανομή των ευθυνών αντίστοιχα σε περίπτωση παραβίασης.

3.7.2.3 Προστασία της Βιομετρικής Ταυτότητας

Οι Uludag και συνεργάτες (Uludag, 2004) υπογραμμίζουν τη σημασία της επίγνωσης ότι η βιομετρική ταυτότητα είναι αμετάβλητη. Αν παραβιαστεί ένα δακτυλικό αποτύπωμα, δεν υπάρχει “plan B” – δεν μπορεί κανείς να εκδώσει “νέο δακτυλικό αποτύπωμα”, όπως θα έβγαζε μια καινούργια κάρτα. Αυτό απαιτεί εξαιρετικά αυστηρά πρωτόκολλα ασφαλείας, ιδίως σε μεγάλης κλίμακας εφαρμογές που αφορούν εκατομμύρια χρήστες (π.χ. εθνικές ταυτότητες).

3.7.3 Ακρίβεια, Απόδοση και Πραγματικές Συνθήκες

Παρά τις εξαιρετικές επιδόσεις που αναφέρονται σε ερευνητικές εργασίες, τα βιομετρικά συστήματα πολλές φορές αντιμετωπίζουν προκλήσεις όταν υλοποιούνται σε πραγματικά σενάρια. Παράγοντες, όπως ο φωτισμός, οι αλλαγές στην εμφάνιση (γένια, γυαλιά, τραυματισμοί), η ποιότητα των αισθητήρων, ακόμα και οι περιβαλλοντικές συνθήκες, μπορεί να επηρεάσουν αρνητικά την ακρίβεια.

Για τον λόγο αυτό, η κοινότητα εστιάζει σε συγκεκριμένες μετρικές (metrics) όπως τις FRR (False Rejection Rate) και FAR (False Acceptance Rate), οι οποίες παρέχουν εικόνα για το πόσο συχνά το σύστημα απορρίπτει κάποιον νόμιμο χρήστη (σφάλμα τύπου I) ή δέχεται κάποιον μη νόμιμο (σφάλμα τύπου II). Συχνά, χρησιμοποιείται και ο δείκτης EER (Equal Error Rate), ο οποίος ορίζεται ως το ποσοστό σφάλματος στο οποίο οι τιμές του FRR και του FAR είναι ίσες (Johnson, Tan, & Schuckers, 2010) καθώς αλλάζουμε το κατώφλι ομοιότητας (similarity score threshold). Πρακτικά, είναι μία τιμή που δείχνει πόσο αξιόπιστο είναι το σύστημα (όσο πιο μικρό είναι το EER, τόσο μεγαλύτερη η ακρίβεια). Μια εύθραυστη ισορροπία απαιτείται, ώστε να ρυθμιστεί το σύστημα σε ένα βέλτιστο σημείο όπου επιτυγχάνεται ασφάλεια και χρηστικότητα.

3.7.4 Προκλήσεις Κλιμάκωσης και Απόδοσης στο Blockchain

Το κύριο μειονέκτημα της τεχνολογίας blockchain είναι ότι οι πλατφόρμες συχνά υποφέρουν από ζητήματα απόδοσης (throughput) και ταχύτητας στις συναλλαγές (transaction latency). Για εφαρμογές που απαιτούν άμεση επεξεργασία μεγάλου όγκου βιομετρικών δεδομένων σε πραγματικό χρόνο (λ.χ. σε ένα πολυσύχναστο αεροδρόμιο), η τρέχουσα τεχνολογία blockchain μπορεί να μην ανταποκριθεί επαρκώς. Γι' αυτό, ερευνητικές προσπάθειες στρέφονται προς τη χρήση εναλλακτικών πρωτοκόλλων συναίνεσης (consensus), όπως Proof-of-Authority (PoA) ή συνδυασμοί με sidechains και off-chain αποθήκευση, αντί του κλασικού Proof-of-Work (PoW) το οποίο είναι ενεργοβόρο και αρκετά απαιτητικό σε ισχύ. Τα sidechains είναι παράλληλες αλυσίδες μπλοκ που συνδέονται με το κύριο blockchain επιτρέποντας την εκτέλεση συναλλαγών με μεγαλύτερη ταχύτητα και χωρίς να επιβαρύνουν το βασικό δίκτυο, ενώ η off-chain αποθήκευση μειώνει το μέγεθος των δεδομένων στο blockchain καθώς τα δεδομένα αποθηκεύονται εξωτερικά, διατηρώντας μόνο τα απαραίτητα hashes για επαλήθευση στο blockchain.

3.7.5 Τεχνητή Νοημοσύνη και Deepfakes

Η άνοδος της τεχνητής νοημοσύνης έφερε και πιο προηγμένες μορφές εξαπάτησης: τα λεγόμενα “deepfakes” που μπορούν να παράγουν ψεύτικα βίντεο ή φωνητικά δείγματα. Αυτό εγείρει σοβαρά ερωτήματα για την ασφάλεια συστημάτων αναγνώρισης προσώπου ή φωνής. Γι' αυτό, η ερευνητική κοινότητα εργάζεται πάνω σε αλγόριθμους που μπορούν να ανιχνεύουν συνθετικές εικόνες ή ήχους, εκπαιδεύοντας συνελκτικά νευρωνικά δίκτυα (CNNs) να εντοπίζουν λεπτές ασυμφωνίες που προδίδουν την τεχνητή προέλευσή τους, αξιοποιώντας αντίστοιχες τεχνικές deep learning (Plesh et al., 2019).

3.7.6 Ανοικτά Ερευνητικά Ερωτήματα

Παρά την ήδη πλούσια βιβλιογραφία, υφίστανται ακόμα πολλά ανοιχτά θέματα:

1. *Κλιμάκωση Blockchain για Βιομετρικά Δεδομένα*
 - Πώς επιτυγχάνουμε υψηλό ρυθμό συναλλαγών και επεξεργασίας σε συστήματα που βασίζονται στο blockchain όταν οι βιομετρικές λειτουργίες λαμβάνουν χώρα σε μεγάλους πληθυσμούς ή συνδυάζουν πολλές βιομετρικές μεθόδους αυθεντικοποίησης;
2. *Ανοχή σε Σφάλματα (Error Tolerance)*
 - Πώς μπορούμε να ενσωματώσουμε ακόμα πιο ανεκτικές μεθόδους επαλήθευσης που να μην θυσιάζουν την ακρίβεια;
3. *Χρήση Βιομετρικών σε Κατανεμημένα Περιβάλλοντα (Cloud, Edge)*
 - Ποιος αναλαμβάνει την επεξεργασία; Το cloud (υπολογιστικό νέφος) ή οι ίδιες οι συσκευές (edge computing); Πώς εξισορροπούμε επιδόσεις (βέλτιστη λύση cloud) και ασφάλεια (βέλτιστη λύση edge computing);
4. *Διασύνδεση με την Ανωνυμοποίηση και την Ομοιομορφική Κρυπτογραφία*
 - Σε ποιο βαθμό μπορούν νέες κρυπτογραφικές τεχνικές (όπως η ομοιομορφική κρυπτογραφία) να επιτρέψουν την αυθεντικοποίηση χωρίς αποκάλυψη των βιομετρικών χαρακτηριστικών;
5. *Υπολογιστική και Ενεργειακή Απόδοση*
 - Η κατανάλωση ενέργειας σε φορητές συσκευές, αλλά και το περιβαλλοντικό αποτύπωμα των εκτεταμένων blockchain δικτύων, είναι ζητήματα εξίσου σημαντικά.
6. *Αντιμετώπιση Deepfakes*
 - Ποιες μέθοδοι μπορούν να ενισχύσουν την ανθεκτικότητα απέναντι σε πλαστοπροσωπία μέσω deepfakes; Πως μπορούν τα βιομετρικά συστήματα να διακρίνουν τα αυθεντικά βιομετρικά χαρακτηριστικά έναντι συνθετικών ή deepfake χαρακτηριστικών που δημιουργούνται μέσω εξελιγμένων μοντέλων τεχνητής νοημοσύνης;

3.8 Εφαρμογές σε Διάφορους Κλάδους

3.8.1 Χρηματοπιστωτικός Τομέας και Ηλεκτρονικές Πληρωμές

Η υιοθέτηση της βιομετρικής στα τραπεζικά ιδρύματα και στις πλατφόρμες fintech αναπτύσσεται ραγδαία. Οι χρήστες ήδη χρησιμοποιούν δακτυλικό αποτύπωμα ή αναγνώριση προσώπου για να συνδεθούν σε εφαρμογές mobile banking ή για να εγκρίνουν ηλεκτρονικές πληρωμές. Σε αυτή την περίπτωση, η βιομετρική συχνά λειτουργεί ως “δεύτερος παράγοντας αυθεντικοποίησης” (2FA), προσφέροντας ένα επιπλέον επίπεδο ασφάλειας πέρα από το παραδοσιακά διαπιστευτήρια, όπως PIN ή τον κωδικό. Οι τεχνολογίες αυτές συμμορφώνονται συχνά με ρυθμιστικά πλαίσια, όπως η

PSD2 (Payment Services Directive 2) στην Ε.Ε., η οποία απαιτεί “ισχυρή ταυτοποίηση πελάτη” (European Parliament and Council, 2015).

3.8.2 Υγειονομική Περίθαλψη και Ταυτοποίηση Ασθενών

Σε νοσοκομεία και κλινικές, η ταυτοποίηση των ασθενών μέσω βιομετρικών μεθόδων μειώνει τα περιστατικά λανθασμένης χορήγησης φαρμάκων ή ιατρικών πράξεων. Επιπλέον, μπορεί να ελαχιστοποιήσει τις περιπτώσεις απάτης (π.χ. άτομα που επιχειρούν να λάβουν περίθαλψη με τα στοιχεία κάποιου άλλου). Ωστόσο, ο ευαίσθητος χαρακτήρας των ιατρικών δεδομένων δημιουργεί αυξημένες απαιτήσεις προστασίας και ιδιωτικότητας, σύμφωνα και με τις επισημάνσεις της Rathgeb (Rathgeb, 2012).

3.8.3 Κρατικές Υπηρεσίες και Δημόσιοι Φορείς

Σε αεροδρόμια (π.χ. συστήματα e-Passport και e-Gate) η ταυτοποίηση των επισκεπτών που εισέρχονται και αργότερα εξέρχονται από την χώρα μπορεί να γίνεται πολύ γρήγορα και με υψηλή ακρίβεια με βιομετρικές τεχνολογίες αυθεντικοποίησης όπως την ανάλυση γεωμετρίας χεριού ή την αναγνώριση ίριδας (Boulgouris, Plataniotis, & Micheli-Tzanakou, 2009).

Αντίστοιχα και για τον έλεγχο συνόρων μέσω βιομετρικών τεχνολογιών για την ταυτοποίηση και την αποφυγή παράνομων μεταναστών (π.χ. στις Ηνωμένες Πολιτείες Αμερικής όταν κάποιος εισέρχεται στη χώρα χρησιμοποιούν βιομετρικές τεχνολογίες αναγνώρισης δακτυλικών αποτυπωμάτων, παίρνουν δείγμα και όταν θα εξέλθει από την χώρα επιβεβαιώνουν το βιομετρικό) (Jain et al., 2007).

3.8.4 Εγκληματολογία

Στην εγκληματολογία η βιομετρική αυθεντικοποίηση μπορεί να χρησιμοποιηθεί για ταυτοποίηση πτωμάτων και για την εξιχνίαση εγκλημάτων (Wayman et al., 2005). Επιπλέον, για τον εντοπισμό αγνοούμενων παιδιών ή την απόδειξη ύπαρξης συγγενικών σχέσεων (π.χ. απόδειξη πατρότητας) (Jain et al., 2007).

3.8.5 Ελεγχόμενη Πρόσβαση σε Εγκαταστάσεις Υψηλής Ασφάλειας

Η βιομετρική αυθεντικοποίηση αξιοποιείται ευρέως σε κέντρα δεδομένων, στρατιωτικές βάσεις, ακόμη και σε ορισμένες βιομηχανίες (π.χ. φαρμακευτικά εργαστήρια). Η ενσωμάτωση των βιομετρικών συστημάτων με κρυπτογραφία (Uludag, 2004) μειώνει τη πιθανότητα να “κλαπούν” τα αποθηκευμένα δεδομένα των χρηστών, ενώ τα πολυτροπικά συστήματα πολλαπλής ταυτοποίησης (multi-modal biometric systems) (π.χ. συνδυασμός δακτυλικού αποτυπώματος με αναγνώριση ίριδας) επιτυγχάνουν ακόμη υψηλότερο επίπεδο ασφάλειας.

3.8.6 Εμπορική Χρήση και Καταναλωτικές Εφαρμογές

Τα πιο κοινά παραδείγματα εμπορικής χρήσης είναι στις συσκευές καθημερινής χρήσης, όπως κινητά τηλέφωνα και tablets. Πολλοί καταναλωτές θεωρούν πρακτικό το ξεκλείδωμα συσκευής με ένα απλό άγγιγμα ή μια ματιά. Αυτό δείχνει πώς η βιομετρική αυθεντικοποίηση έχει “περάσει” από το στάδιο των εξειδικευμένων βιομηχανικών εφαρμογών στην ευρεία καταναλωτική αγορά (Jain et al., 2004; Wayman et al., 2005).



Εικόνα 8: Παραδείγματα εφαρμογών βιομετρικών τεχνολογιών

Πηγή: Jain et al. (2004)

(a) αναγνώριση δακτυλικών αποτυπωμάτων για σύνδεση σε υπολογιστή, (b) αναγνώριση δακτυλικών αποτυπωμάτων για πληρωμή με χρήση τερματικού POS, (c) ξεκλείδωμα πόρτας με αναγνώριση δακτυλικών αποτυπωμάτων, (d) αναγνώριση γεωμετρίας χεριού για την είσοδο στη χώρα μέσω αεροδρομίου, (e) συνοριακός έλεγχος με χρήση αναγνώρισης ίριδας, (f) αναγνώριση γεωμετρίας χεριού σε αεροδρόμιο, (g) αναγνώριση προσώπου σε ATM, (h) αναγνώριση δακτυλικού αποτυπώματος για εφαρμογές παρακολούθησης παρουσιών και ωρομέτρησης

3.9 Ευρύτερη Επισκόπηση της Βιβλιογραφίας και Τάσεις

Η παρούσα εκτενής ανασκόπηση αναδεικνύει ότι ο τομέας της βιομετρικής αυθεντικοποίησης έχει εμφανίσει εντυπωσιακή ανάπτυξη:

1. Από πλευράς Αλγορίθμων:
 - Οι νεότερες μέθοδοι βαθιάς μάθησης αυξάνουν την ακρίβεια (Kim, Yeun, & Yoo, 2019).
 - Έχουν προταθεί εξειδικευμένες προσεγγίσεις κρυπτογραφίας (fuzzy vault, robust hashing) που παρέχουν ασφαλείς τρόπους αποθήκευσης βιομετρικών προτύπων.
2. Από πλευράς Εφαρμογών:
 - Το IoT, το blockchain, η TN και η πολυτροπική βιομετρική διευρύνουν τις πιθανές χρήσεις και τις μελλοντικές πρακτικές της βιομετρικής αυθεντικοποίησης.
3. Από πλευράς Ηθικής και Νομοθεσίας:
 - Υπάρχουν σημαντικές προκλήσεις γύρω από την ιδιωτικότητα, τη συμμόρφωση με νομικά πλαίσια (GDPR, κ.λπ.) και την κοινωνική αποδοχή που πρέπει να αντιμετωπισθούν στο άμεσο μέλλον.

Καθώς οι τεχνολογίες ωριμάζουν, η ενσωμάτωση πολλαπλών μορφών βιομετρικής αυθεντικοποίησης σε κρίσιμες εφαρμογές (στρατηγικής σημασίας εγκαταστάσεις, νοσοκομεία, οικονομικές συναλλαγές κ.λπ.) ενδέχεται να γίνει κανόνας. Η πρόκληση συνίσταται στο να διασφαλιστεί ότι αυτές οι λύσεις θα είναι επαρκώς θωρακισμένες και παράλληλα θα σέβονται τα δικαιώματα και την ελευθερία των χρηστών.

4

Σύγκριση Βιομετρικών Τεχνολογιών Αυθεντικοποίησης

4.1 Εισαγωγή στη Συγκριτική Ανάλυση

Η βιομετρική αυθεντικοποίηση αποτελεί ένα ταχέως αναπτυσσόμενο πεδίο τεχνολογικής έρευνας και εφαρμογών, καθώς προσφέρει ασφαλέστερους και πιο αξιόπιστους μηχανισμούς επαλήθευσης και ταυτοποίησης χρηστών σε σύγκριση με τις παραδοσιακές μεθόδους, όπως οι κωδικοί πρόσβασης, τα PIN ή οι έξυπνες κάρτες. Έχοντας ήδη παρουσιάσει μια εισαγωγή στην ιστορική εξέλιξη και τις βασικές έννοιες της βιομετρικής αυθεντικοποίησης, σε αυτό το κεφάλαιο θα εστιάσουμε στην ουσιαστική σύγκριση των διαφόρων τεχνολογιών βιομετρικής αυθεντικοποίησης.

Στόχος είναι να αναδείξουμε:

1. Τα ιδιαίτερα χαρακτηριστικά κάθε τεχνολογίας.
2. Την επιστημονική και τεχνολογική βάση που καθορίζει την ακρίβεια, την ασφάλεια και την ευχρηστία των επιμέρους συστημάτων.
3. Τους παράγοντες που επηρεάζουν την απόδοση σε πραγματικά περιβάλλοντα.
4. Τις εφαρμογές όπου κάθε τεχνολογία επιδεικνύει τα μέγιστα οφέλη.
5. Τα πλεονεκτήματα και τα μειονεκτήματα της κάθε τεχνολογίας, τόσο από τεχνική όσο και από κοινωνική-ηθική σκοπιά.

Τέλος, θα παρουσιάσουμε έναν πίνακα επισκόπησης απαιτήσεων και ενδεικτικών εφαρμογών των τεχνολογιών και έναν ενιαίο συγκριτικό πίνακα, όπου αποτυπώνονται οι βασικοί δείκτες απόδοσης (performance metrics), η ασφάλεια, τα πλεονεκτήματα και τα μειονεκτήματα ανά τεχνολογία και επιπλέον ένας πίνακας όπου παρουσιάζονται οι βιομετρικές τεχνολογίες με την υψηλότερη και την χαμηλότερη απόδοση σε κάθε κριτήριο. Με αυτόν τον τρόπο, ευελπιστούμε να προκύψει μια συνεκτική εικόνα του πεδίου, συμβάλλοντας στη σαφέστερη καθοδήγηση για μελλοντικές έρευνες και υλοποιήσεις και στη διευκόλυνση της λήψης τεκμηριωμένων αποφάσεων από επαγγελματίες του είδους.

4.2 Επισκόπηση των Κυριότερων Βιομετρικών Τεχνολογιών

Προτού προχωρήσουμε στη σε βάθος σύγκριση, κρίνεται αναγκαίο να συνοψίσουμε τα βασικά είδη βιομετρικών τεχνολογιών που μελετώνται και αξιοποιούνται εκτενώς:

1. Αναγνώριση Δακτυλικών Αποτυπωμάτων (Fingerprint Recognition)
2. Αναγνώριση Προσώπου (Face Recognition)
3. Αναγνώριση Ίριδας (Iris Recognition)
4. Αναγνώριση Αμφιβληστροειδούς (Retina Recognition)
5. Αναγνώριση Φωνής (Voice Recognition)
6. Δυναμική Πληκτρολόγησης (Keystroke Dynamics)
7. Αναγνώριση Βάδισης (Gait Recognition)
8. Αναγνώριση Υπογραφής (Signature Recognition)
9. Αναγνώριση Παλαμιαίων Αγγείων (Palm Vein Recognition)
10. Πολυτροπικά Συστήματα (Multimodal Systems)

Κάθε μία από τις παραπάνω κατηγορίες παρουσιάζει διαφορετικές απαιτήσεις σε υποδομές, διαφορετικές τεχνικές προκλήσεις και διαφορετικά επίπεδα αξιοπιστίας. Επιπλέον, η χρηστικότητα τους διαφέρει ανάλογα με το πλαίσιο χρήσης, είτε πρόκειται για φορητές συσκευές, τραπεζικές συναλλαγές ή συστήματα ελέγχου πρόσβασης σε φυσικούς χώρους υψηλής ασφάλειας. Στις επόμενες ενότητες θα γίνει μια αναλυτική επισκόπηση της κάθε κατηγορίας, με έμφαση σε εκείνα τα χαρακτηριστικά που μας επιτρέπουν να συγκρίνουμε τις τεχνολογίες αυτές μεταξύ τους.

4.3 Συγκριτική Ανάλυση Βασικών Βιομετρικών Τεχνολογιών

Η ενότητα αυτή εστιάζει στους τρόπους με τους οποίους μπορούμε να συγκρίνουμε τις βιομετρικές τεχνολογίες, λαμβάνοντας υπόψη πολλαπλές παραμέτρους/κριτήρια:

1. *Τεχνική Υλοποίηση και Προαπαιτούμενα*: Υπάρχουν τεχνικές προκλήσεις στην ανάπτυξη και υλοποίηση; Χρειάζονται ειδικοί αισθητήρες; Πόσο περίπλοκη είναι η προ-επεξεργασία του βιομετρικού σήματος;
2. *Ακρίβεια (Accuracy)*: Ποιο είναι το επίπεδο ακρίβειας; Δηλαδή πόσο χαμηλά είναι τα ποσοστά False Acceptance Rate (FAR) ή False Match Rate (FMR) (το ποσοστό των μη εξουσιοδοτημένων χρηστών που γίνονται αποδεκτοί λανθασμένα από το σύστημα, όπως αυτό προκύπτει από το κλάσμα των λάθους αποδοχών προς τον συνολικό αριθμό προσπαθειών από μη εξουσιοδοτημένους χρήστες) και False Rejection Rate (FRR) ή False Nonmatch Rate (FNMR) (το ποσοστό των εξουσιοδοτημένων χρηστών που απορρίπτονται λανθασμένα από το σύστημα, όπως αυτό προκύπτει από το κλάσμα των λάθους απορρίψεων προς τον συνολικό αριθμό προσπαθειών από εξουσιοδοτημένους χρήστες). Η ακρίβεια μελετάται ως μία εκ των δύο παραμέτρων της απόδοσης (performance). Λαμβάνοντας υπόψη ότι η παράμετρος της ταχύτητας επηρεάζεται πρωτίστως από τον χρόνο λήψης του δείγματος και σε μικρότερο βαθμό από τον χρόνο αναζήτησης, καθώς και τη δυσχέρεια

αποτίμησής της με έναν ενιαίο και αντικειμενικό τρόπο, η παρούσα εργασία εστιάζει στην ανάλυση της ακρίβειας.

3. *Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις*: Πόσο εύκολο ή δύσκολο είναι να παρακαμφθεί η μέθοδος από κακόβουλους χρήστες; Υπάρχουν καταγεγραμμένες περιπτώσεις πλαστοπροσωπίας spoofing;
4. *Ευχρηστία (Usability), Μονιμότητα (Permanence) και Αποδοχή Χρηστών*: Πόσο φιλική είναι η τεχνολογία για τον τελικό χρήστη; Πόσο συχνά απαιτείται επανεγγραφή (re-enrollment); Τι προβλήματα ανέχονται οι χρήστες (π.χ. αναγκαστική σάρωση δακτύλου, λήψη βιομετρικού δείγματος κ.λπ.);
5. *Κόστος και Κλιμάκωση*: Πόσο οικονομικό είναι να υλοποιηθεί σε μαζική κλίμακα; Πόσο εύκολα μπορεί να επεκταθεί η εφαρμογή της μεθόδου σε διαφορετικά περιβάλλοντα και σε μεγάλο αριθμό χρηστών;
6. *Ηθικές και Νομικές Προεκτάσεις*: Τι ζητήματα προστασίας προσωπικών δεδομένων και ιδιωτικότητας προκύπτουν; Πόσο πιθανό είναι να υπάρξουν αντιδράσεις από ομάδες χρηστών ή ρυθμιστικές αρχές;

Στις ενότητες που ακολουθούν, θα εξετάσουμε κάθε τεχνολογία με γνώμονα τα παραπάνω κριτήρια, προχωρώντας σε μια ουσιαστική σύγκριση.

4.3.1 Αναγνώριση Δακτυλικών Αποτυπωμάτων (Fingerprint Recognition)

Η αναγνώριση δακτυλικών αποτυπωμάτων είναι ίσως η πιο διαδεδομένη βιομετρική μέθοδος στη σύγχρονη εποχή. Εφαρμόζεται ευρέως σε φορητές συσκευές (smartphones, tablets), σε συστήματα ελέγχου πρόσβασης, σε αστυνομικά και διαβατηριακά συστήματα, καθώς και σε τραπεζικές συναλλαγές.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Απαιτείται ειδικός αισθητήρας δακτυλικού αποτυπώματος (οπτικός, χωρητικός ή υπερήχων).
- Η προ-επεξεργασία του σήματος περιλαμβάνει τρία βασικά βήματα:
 - ο (α) την αφαίρεση θορύβου (noise reduction) εξαιτίας χαμηλής ποιότητας εισόδου (υγρασία, ξηρότητα δέρματος, φθαρμένα αποτυπώματα)
 - ο (β) την εύρεση χαρακτηριστικών (minutiae) τα οποία θα χρησιμοποιηθούν ως μοναδικά αναγνωριστικά και
 - ο (γ) την κανονικοποίηση (normalization) όπου τα αποτυπώματα ευθυγραμμίζονται και αποκτούν ομοιόμορφη κλίμακα.
- Οι σύγχρονοι αισθητήρες χωρητικού τύπου και υπερήχων ενσωματώνονται σε οθόνες smartphones, καθιστώντας τη διαδικασία πιο απλή για τον χρήστη.

Ακρίβεια (Accuracy)

- Σε καλής ποιότητας αισθητήρες, η ακρίβεια ταυτοποίησης (accuracy) μπορεί να ξεπεράσει το 95-98% (Kim, Yeun, & Yoo, 2019)

- Σύμφωνα με την έρευνα των Jain & Ross (2004), το FAR (False Accept Rate) φτάνει σε πολύ χαμηλά επίπεδα (0,2%), και το FRR (False Reject Rate) εξίσου (0,2%), αναλόγως της ποιότητας αισθητήρα, του αλγορίθμου και της ποιότητας του χαρακτηριστικού. Σε άλλη έρευνα εμφανίζεται FAR 0,001-0,01% και FRR 0,3-0,7% (Bolle, Connell, Pankanti, Ratha, & Senior, 2004).

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Παρά την υψηλή ακρίβεια, έχουν τεκμηριωθεί πολλά περιστατικά πλαστοπροσωπίας, όπως π.χ. η δημιουργία τεχνητών δακτύλων με χρήση σιλικόνης ή 3D εκτυπωμένων καλουπιών (Maltoni, Jain, & Prabhakar, 2003; Bolle et al., 2004).
- Οι χωρητικοί και υπέρηχοι αισθητήρες θεωρούνται πιο ανθεκτικοί στις επιθέσεις ψεύτικων δακτύλων σε σχέση με τους οπτικούς, διότι βασίζονται σε ιδιότητες αγωγιμότητας ή τρισδιάστατης απεικόνισης που είναι δύσκολο να πλαστογραφηθούν.
- Επίσης, έχουν γίνει προσπάθειες χρήσης ζωντανών δειγμάτων (liveness detection) ώστε να ανιχνεύεται εάν το δάκτυλο προέρχεται από ζωντανό άτομο ελέγχοντας ζωτικά σημεία όπως τον σφυγμό και την θερμοκρασία.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η χρήση του δακτυλικού αποτυπώματος θεωρείται αρκετά φιλική και διαδεδομένη, καθώς ο χρήστης απλώς τοποθετεί το δάκτυλό του στον αισθητήρα.
- Σε περιπτώσεις που το δάκτυλο είναι υγρό ή λερωμένο, η ποιότητα του σήματος υποβαθμίζεται, γεγονός που μπορεί να αυξήσει το FRR.
- Η κοινωνική αποδοχή είναι υψηλή, καθώς η διαδικασία λήψης δεν θεωρείται παρεμβατική και πλέον οι περισσότεροι χρήστες είναι εξοικειωμένοι με την τεχνολογία.
- Το δακτυλικό αποτύπωμα μπορεί να διατηρηθεί για μεγάλα χρονικά διαστήματα σε σχέση με τις άλλες τεχνολογίες οπότε θα χαρακτηρίζαμε την μονιμότητά του υψηλή (Prabhakar et al., 2003).

Κόστος και Κλιμάκωση

- Οι αισθητήρες δακτυλικού αποτυπώματος έχουν γίνει εξαιρετικά οικονομικοί και εύκολοι στην ενσωμάτωση.
- Μεγάλη ποικιλία σε διάφορα επίπεδα κόστους, γεγονός που επιτρέπει την επέκταση τόσο σε καταναλωτικές συσκευές όσο και σε βιομηχανικές λύσεις.

Ηθικές και Νομικές Προεκτάσεις

- Η καταγραφή δακτυλικών αποτυπωμάτων από κρατικούς φορείς προϋποθέτει νομοθετικά πλαίσια και ρυθμίσεις προσωπικών δεδομένων (π.χ. GDPR στην Ευρώπη).
- Σε γενικές γραμμές, η ανησυχία σχετικά με την παραβίαση ιδιωτικότητας είναι μετριασμένη, καθώς τα δακτυλικά αποτυπώματα χρησιμοποιούνται ευρέως εδώ και πολλές δεκαετίες.

4.3.2 Αναγνώριση Προσώπου (Face Recognition)

Η αναγνώριση προσώπου παρουσιάζει αυξημένο ενδιαφέρον τα τελευταία χρόνια, ιδιαίτερα με τη συνδρομή αλγορίθμων μηχανικής μάθησης και νευρωνικών δικτύων, ειδικότερα στο πεδίο της Βαθιάς Μάθησης (Deep Learning). Μεγάλοι τεχνολογικοί κολοσσοί προωθούν λύσεις αναγνώρισης προσώπου για εφαρμογές σε κινητά τηλέφωνα, μέσα κοινωνικής δικτύωσης, συστήματα παρακολούθησης δημόσιων χώρων, κ.λπ.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Πέρα από απλές κάμερες 2D, υπάρχουν και πιο προηγμένοι αισθητήρες που χρησιμοποιούν τεχνολογίες 3D mapping (π.χ. Structured Light, Time-of-Flight) (Jain et al., 2007).
- Η προ-επεξεργασία περιλαμβάνει τον εντοπισμό του προσώπου στην εικόνα (face detection) και την εξαγωγή χαρακτηριστικών (face embeddings), ενώ στη συνέχεια ακολουθεί η σύγκρισή τους με τα αποθηκευμένα πρότυπα στη βάση δεδομένων.
- Τα σύγχρονα συστήματα αξιοποιούν αλγορίθμους deep learning (π.χ. CNN-based architectures, όπως το FaceNet, VGG-Face, κ.λπ.) (Parkhi, Vedaldi, & Zisserman, 2015; Schroff, Kalenichenko, & Philbin, 2015; Plesh et al., 2019).

Ακρίβεια (Accuracy)

- Τα συστήματα αναγνώρισης προσώπου που χρησιμοποιούν 3D αισθητήρες εμφανίζουν υψηλή ακρίβεια, με ποσοστά που προσεγγίζουν το 95% (Banz & Vetter, 2003).
- Σε 2D κάμερες, η ακρίβεια εξαρτάται σε μεγάλο βαθμό από τις συνθήκες φωτισμού, τη γωνία λήψης και την ποιότητα της κάμερας.
- Παρά τη μεγάλη ακρίβεια, ορισμένες συνθήκες περιβάλλοντος (χαμηλός φωτισμός, γωνία λήψης/πόζα, αλλαγές στην εμφάνιση, μάσκες προσώπου) μπορούν να δυσχεράνουν τη σωστή ταυτοποίηση, ωστόσο υπάρχουν τεχνικές βελτίωσης εικόνας (image enhancement) για την αντιμετώπισή τους (Boulgouris et al., 2009; Jain et al., 2007).
- Ένα ενδεικτικό FAR είναι 0,1-1% και FRR 10-20% (Bolle et al., 2004).

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Τα παλαιότερα συστήματα που βασίζονταν σε 2D εικόνες ήταν ευάλωτα σε επιθέσεις «με φωτογραφία» (photo spoofing attack – επίθεση πλαστοπροσωπίας με φωτογραφία), όπου κάποιος τρίτος χρησιμοποιεί μια εκτυπωμένη εικόνα ή μια φωτογραφία σε οθόνη για να ξεγελάσει ένα 2D σύστημα αναγνώρισης προσώπου.
- Οι νεότερες προσεγγίσεις με 3D mapping και αισθητήρες υπέρυθρων (IR) είναι σαφώς πιο ανθεκτικές, καθώς απαιτούν τρισδιάστατη δομή και θερμική πληροφορία του ανθρώπινου προσώπου. Η χρήση των προσεγγίσεων αυτών είτε ανεξάρτητα είτε συνδυαστικά (δηλ. 3D mapping μαζί με οπτικούς αισθητήρες) βελτιώνει την ακρίβεια (Banz & Vetter, 2003).
- Παρά ταύτα, υπάρχουν πειράματα με μάσκες σιλικόνης ή 3D εκτυπώσεις που μπορούν να ξεγελάσουν ακόμα και προηγμένα συστήματα (Akhtar & Mian, 2018), αν και σε πολύ μικρό βαθμό προς το παρόν.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η ευχρηστία είναι πολύ μεγάλη: ο χρήστης απλά κοιτάζει την κάμερα και το σύστημα τον αναγνωρίζει χωρίς περαιτέρω ενέργειες.

- Σε δημόσιους χώρους, η χρήση αναγνώρισης προσώπου εγείρει ηθικά ερωτήματα και αντιδράσεις σχετικά με την προστασία της ιδιωτικότητας και τη διαρκή παρακολούθηση πολιτών (surveillance) ωστόσο η αποδοχή θα λέγαμε πως είναι υψηλή εξαιτίας της μεγάλης ευχρηστίας (Jain et al., 2004; Prabhakar et al., 2003). Θα μπορούσε να είναι πολύ υψηλή αλλά λόγω των προαναφερόμενων αντιδράσεων καθώς και του γεγονότος πως πολλές φορές – παρά τις σχετικές επισημάνσεις στον χώρο – οι χρήστες αγνοούν πως παρακολουθούνται, η αποδοχή τελικά θεωρούμε πως είναι υψηλή.
- Η μονιμότητα είναι μέτρια καθώς το πρόσωπο αλλάζει σημαντικά με την πάροδο των ετών ή εξαιτίας παρεμβάσεων (π.χ. λόγω ατυχημάτων, γένια ή αισθητικών παρεμβάσεων)

Κόστος και Κλιμάκωση

- Στις φορητές συσκευές υψηλής κατηγορίας, η ενσωμάτωση ακριβών αισθητήρων 3D είναι πλέον δεδομένη, αλλά αυξάνει το κόστος της συσκευής.
- Σε επίπεδο συστημάτων παρακολούθησης, η απαιτούμενη υποδομή για real-time επεξεργασία μεγάλων ροών βίντεο είναι υψηλή, με αυξημένες απαιτήσεις σε υπολογιστική ισχύ και δικτυακούς πόρους.

Ηθικές και Νομικές Προεκτάσεις

- Η αναγνώριση προσώπου είναι από τις βιομετρικές τεχνολογίες που έχουν προκαλέσει τις μεγαλύτερες κοινωνικές και πολιτικές συζητήσεις καθώς πέραν των ζητημάτων ιδιωτικότητας συνδέεται και με την πιθανότητα μαζικής παρακολούθησης.
- Επιβάλλονται νομικοί περιορισμοί και ρυθμίσεις (GDPR, διακρατικές συμφωνίες, νομοθεσία για CCTV κ.λπ.) για το πώς και πού επιτρέπεται να γίνεται η συλλογή και χρήση δεδομένων προσώπου (σύμφωνα με τον 2016/679 ΓΚΠΔ της ΕΕ και του νόμου 4624/2019).

4.3.3 Αναγνώριση Ίριδας (Iris Recognition)

Η αναγνώριση ίριδας θεωρείται από πολλούς ερευνητές ως μια από τις πιο αξιόπιστες βιομετρικές μεθόδους, χάρη στη μοναδικότητα και τη σταθερότητα της ίριδας καθ' όλη τη διάρκεια της ενήλικης ζωής ενός ατόμου.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Χρησιμοποιείται ειδικός εξοπλισμός, συνήθως κάμερα κοντινού υπερύθρου (Near-Infrared), ώστε να απαθανατίζεται με σαφήνεια η δομή της ίριδας.
- Η προ-επεξεργασία περιλαμβάνει τα εξής βήματα:
 - (α) τον εντοπισμό της ίριδας (iris localization) με χρήση αλγόριθμων που εντοπίζουν τα όρια και διαχωρίζουν την κόρη και τον χιτώνα
 - (β) την «εξουδετέρωση» του οφθαλμικού υποβάθρου (noise removal) όπου αφαιρούνται οι περιττές πληροφορίες, όπως τα βλέφαρα και πιθανές αντανάκλασεις φωτός
 - (γ) την κανονικοποίηση (normalization) όπου γίνεται μετατροπή σε ομοιόμορφη αναπαράσταση

- ο (δ) την κωδικοποίηση των χαρακτηριστικών (iris code), την δημιουργία δηλαδή του τελικού κώδικα που αναπαριστά μοναδικά την ίριδα του ατόμου.

Ακρίβεια (Accuracy)

- Στα ελεγχόμενα περιβάλλοντα, η ακρίβεια μπορεί να φτάσει σε πολύ υψηλά επίπεδα και θεωρείται το βιομετρικό με την μεγαλύτερη ακρίβεια (Daugman, 2004; Jain et al., 2004).
- Το FAR και το FRR είναι αρκετά χαμηλά (0,94% και 0,99% αντίστοιχα), γεγονός που καθιστά την αναγνώριση ίριδας ιδανική για εφαρμογές υψηλής ασφάλειας (Jain et al., 2007).
- Ωστόσο, η ακρίβεια μπορεί να επηρεαστεί αρνητικά από γυαλιά και φακούς επαφής.

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Η δομή της ίριδας είναι δύσκολο να πλαστογραφηθεί, αν και έχουν υπάρξει ερευνητικές αναφορές σε επιθέσεις πλαστοπροσωπίας που χρησιμοποιούν εκτυπώσεις υψηλής ανάλυσης ή φακούς επαφής (Jain, et al., 2004; Jain et al., 2007).
- Οι τεχνικές ανίχνευσης ζωντάνιας (liveness detection) μπορούν να ενισχύσουν την ανθεκτικότητα σε πλαστοπροσωπία. Ειδικότερα, ο εντοπισμός της κίνησης των ματιών ή οι αντανakλάσεις διαχωρίζουν ένα ζωντανό μάτι από μία φωτογραφία.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η λήψη υψηλής ποιότητας εικόνας της ίριδας απαιτεί ηθελημένη συνεργασία του χρήστη (π.χ. να κοιτάζει σε συγκεκριμένο σημείο με συγκεκριμένη απόσταση). Παρόλα αυτά συνολικά η ευχρηστία είναι μεγάλη διότι υπάρχει οδηγός για την απόσταση και δεν χρειάζεται ο χρήστης να κοιτάζει εστιασμένα για μεγάλο χρονικό διάστημα.
- Κάποιοι χρήστες θεωρούν τη διαδικασία παρεμβατική, καθώς σχετίζεται με την περιοχή των ματιών και ενδεχομένως τη χρήση υπέρυθρων ακτινών, συνεπώς η αποδοχή είναι χαμηλή.
- Η ίριδα αφότου διαμορφωθεί κατά την εφηβική ηλικία και για το υπόλοιπο της ζωής μας δεν μεταβάλλεται εκτός από περιπτώσεις ασθενειών του ματιού (Wayman et al., 2005). Συνεπώς η μονιμότητα είναι υψηλή.

Κόστος και Κλιμάκωση

- Οι κάμερες αναγνώρισης ίριδας είναι ακριβότερες από τους συμβατικούς αισθητήρες δακτυλικών αποτυπωμάτων, ιδίως όταν απαιτείται υψηλή ακρίβεια.
- Σε κλίμακα μαζικής υλοποίησης (π.χ. σε εθνικά συστήματα ταυτοποίησης), το κόστος παραμένει σημαντικά υψηλό, αν και η τιμή εξοπλισμού μειώνεται με την πάροδο του χρόνου και την εξέλιξη της τεχνολογίας.

Ηθικές και Νομικές Προεκτάσεις

- Επειδή τα δεδομένα της ίριδας θεωρούνται αμετάβλητα και εξαιρετικά ευαίσθητα, η διαφύλαξη και σωστή διαχείρισή τους κρίνεται υψίστης σημασίας.
- Σε πολλές χώρες, η ευρεία χρήση αυτής της τεχνολογίας περιορίζεται από νομοθετικά πλαίσια προστασίας της ιδιωτικότητας (π.χ. στην Ευρώπη με τον ΓΚΠΔ).

4.3.4 Αναγνώριση Αμφιβληστροειδούς (*Retina Recognition*)

Η αναγνώριση αμφιβληστροειδούς βασίζεται στα μοναδικά μοτίβα αιμοφόρων αγγείων στο πίσω μέρος του ματιού. Πρόκειται για μια τεχνολογία με υψηλή ακρίβεια αλλά περιορισμένη πρακτική εφαρμογή συγκριτικά με άλλες μεθόδους, για τους λόγους που αναφέρονται στη συνέχεια.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Απαιτείται ειδική συσκευή που εκπέμπει χαμηλής ενέργειας υπέρυθρο φως και αναλύει τον τρόπο που τα αιμοφόρα αγγεία αντανακλούν το φως αυτό.
- Η λήψη εικόνας είναι πιο σύνθετη καθώς χρησιμοποιείται υπέρυθρο φως που διαπερνάει τον αμφιβληστροειδή και απαιτεί από τον χρήστη να τοποθετήσει το μάτι του σε κοντινή επαφή με το όργανο λήψης.

Ακρίβεια (Accuracy)

- Η ακρίβεια μπορεί να είναι αρκετά υψηλή, καθώς το μοτίβο του αμφιβληστροειδούς είναι μοναδικό και σταθερό (Uludag, Pankanti, Prabhakar, & Jain, 2004).

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Η πλαστογράφιση του αμφιβληστροειδούς είναι εξαιρετικά δύσκολη, καθώς πρόκειται για εσωτερικό βιομετρικό χαρακτηριστικό με πολύπλοκα μοτίβα. Οπότε θεωρείται μια από τις πιο ασφαλείς μεθόδους από τεχνική άποψη.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η διαδικασία θεωρείται παρεμβατική και μερικοί χρήστες ενδέχεται να αισθάνονται άβολα με την ιδέα της «σάρωσης» του ματιού ενώ η ευχρηστία είναι χαμηλή εξαιτίας των συνθηκών (πολύ κοντινή απόσταση στον σαρωτή, ακινησία του ματιού σε συνδυασμό με σάρωση με φως του αμφιβληστροειδούς).
- Η ακτινοβολία είναι χαμηλής ενέργειας, αλλά οι φόβοι για πιθανές επιπτώσεις εξακολουθούν να υφίστανται σε μέρος του πληθυσμού.
- Η ανίχνευση του αμφιβληστροειδούς μπορεί να αποκαλύψει ορισμένες ιατρικές καταστάσεις (όπως υπέρταση), κάτι που αποτελεί έναν ακόμη παράγοντα που αποθαρρύνει τους χρήστες, συνεπώς η αποδοχή είναι χαμηλή.
- Με βάση τις τρεις προαναφερόμενες διαπιστώσεις, η αποδοχή της μεθόδου αυτής είναι χαμηλή.
- Η μονιμότητα των χαρακτηριστικών είναι πολύ υψηλή καθώς το βιομετρικό χαρακτηριστικό παραμένει αναλλοίωτο στο πέρασμα των ετών και επηρεάζεται μόνο από σοβαρό τραυματισμό (Bolle et al., 2004).
- Ωστόσο, σε πραγματικές συνθήκες, η χρήση υπερσύγχρονων και ακριβών σαρωτών και η ακριβής τοποθέτηση του ματιού δυσχεραίνουν την ευρεία υιοθέτηση.

Κόστος και Κλιμάκωση

- Η απαιτούμενη συσκευή σάρωσης είναι ακριβή, καθιστώντας δύσκολη την ενσωμάτωση σε καταναλωτικές συσκευές (Bolle et al., 2004).

- Η τεχνολογία αυτή χρησιμοποιείται κυρίως σε εφαρμογές υψηλής ασφάλειας (π.χ. στρατιωτικές εγκαταστάσεις, εργαστήρια πυρηνικής ενέργειας), όπου το κόστος δεν είναι ο κυριότερος περιοριστικός παράγοντας.

Ηθικές και Νομικές Προεκτάσεις

- Όπως και η αναγνώριση ίριδας, η συλλογή αμφιβληστροειδικών δεδομένων απαιτεί ιδιαίτερη προσοχή στη διαχείριση και αποθήκευσή τους δεδομένης της υψηλής μονιμότητας και πολυπλοκότητάς τους (π.χ. στην Ε.Ε. σύμφωνα με τον ΓΚΠΔ).
- Η παρεμβατικότητα της μεθόδου εγείρει ηθικά διλήμματα σχετικά με την υποχρεωτική χρήση της και τον βαθμό συμμετοχής/συναίνεσης του χρήστη.

4.3.5 Αναγνώριση Φωνής (Voice Recognition)

Η αναγνώριση φωνής αποτελεί μια βιομετρική μέθοδο που βασίζεται στα ακουστικά χαρακτηριστικά του ατόμου (συχνότητα, χροιά, έμφαση κ.λπ.). Ιδιαίτερο ενδιαφέρον παρουσιάζει ως μέθοδος απομακρυσμένης αυθεντικοποίησης, αφού μπορεί θεωρητικά να αξιοποιηθεί μέσω τηλεφωνικών δικτύων ή διαδικτυακών υπηρεσιών.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Απαιτείται μικρόφωνο για την καταγραφή φωνής (από απλές συσκευές έως επαγγελματικά μικρόφωνα) και λογισμικό επεξεργασίας σήματος ή/και μηχανικής μάθησης.
- Η προ-επεξεργασία μπορεί να περιλαμβάνει τη φασματική ανάλυση (π.χ. μέσω Mel-Frequency Cepstral Coefficients - MFCCs), το φίλτράρισμα θορύβου και την εξαγωγή σχετικών χαρακτηριστικών (Muda, Begam, & Elamvazuthi, 2010).

Ακρίβεια (Accuracy)

- Η ακρίβεια ποικίλλει σημαντικά, ανάλογα με το περιβάλλον θορύβου, την ποιότητα του μικροφώνου και τη διάλεκτο ή προφορά του ομιλητή.
- Σε ελεγχόμενα περιβάλλοντα, οι αλγόριθμοι προηγμένης ανάλυσης φωνής μπορούν να πετύχουν υψηλά ποσοστά επιτυχίας με FAR 2-5% και FRR 5-10% (Jain et al., 2007). Παρόμοια ποσοστά έχουν προκύψει και σε άλλη έρευνα FAR 2-5% και FRR 10-20% (Bolle et al., 2004).
- Ωστόσο, στις πραγματικές εφαρμογές το περιβάλλον δεν μπορεί να ελεγχθεί. Η ύπαρξη εξωτερικών θορύβων, οι αλλαγές στη φωνή λόγω ασθένειας ή ακόμα και η ψυχολογική κατάσταση του χρήστη αποτελούν παράγοντες απρόβλεπτους και μη ελεγχόμενους από τον ίδιο τον χρήστη ή το σύστημα, με αποτέλεσμα η ακρίβεια να επηρεάζεται σε σημαντικό βαθμό, φθάνοντας σε ένα μέτριο επίπεδο.

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Η τεχνολογία είναι ευάλωτη σε επιθέσεις αναπαραγωγής (playback attack) με προηγούμενες εγγραφές της φωνής του χρήστη ή σύνθεσης φωνής (speech synthesis) (Bolle et al., 2004).
- Υπάρχουν τεχνικές «liveness detection» και ανάλυσης φασματικών υπογραφών για να διαχωριστεί η πραγματική φωνή από ηχογραφήσεις ή συνθετική παραγωγή, αλλά δεν έχουν απόλυτη αποτελεσματικότητα (Zhang, Tan, & Yang, 2017).

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η φωνή μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπου δεν είναι βολικό το άγγιγμα / χρήση συσκευής (hands-free).
- Το να μιλά ο χρήστης σε δημόσιους χώρους για να ταυτοποιηθεί δεν είναι πάντα πρακτικό και θέτει θέματα ηχογράφησης και ιδιωτικότητας, ωστόσο η αποδοχή είναι υψηλή.
- Η μονιμότητα των βιομετρικών δεδομένων είναι σχετικά χαμηλή και μάλιστα επηρεάζεται τόσο από το περιβάλλον όσο και από τον χρήστη.

Κόστος και Κλιμάκωση

- Το κόστος προφανώς εξαρτάται από την ποιότητα του μικροφώνου. Αλλά μπορεί να είναι σχετικά χαμηλό, αφού οι περισσότεροι υπολογιστές και smartphones διαθέτουν μικρόφωνα. Γενικά είναι η τρέχουσα τεχνολογία που χρησιμοποιείται σε τηλεφωνικά κέντρα ή hands-free εφαρμογές.
- Η κλιμάκωση σε μεγάλα συστήματα τηλεφωνικών κέντρων (π.χ. τράπεζες) αποτελεί μια ρεαλιστική επιλογή, εφόσον υπάρχει κατάλληλη υπολογιστική υποδομή για την επεξεργασία των φωνητικών δεδομένων (όπως ισχύει στην περίπτωση του υπολ. νέφους).

Ηθικές και Νομικές Προεκτάσεις

- Η συλλογή φωνητικών δειγμάτων χρήζει προσοχής, ιδίως όταν αυτή γίνεται εν αγνοία του χρήστη ή χωρίς σαφή ενημέρωση.
- Υπάρχουν νομοθεσίες περί ηχογράφησης συνομιλιών και ιδιωτικότητας, που περιορίζουν ή πλαισιώνουν αυστηρά τη χρήση βιομετρικής φωνητικής αυθεντικοποίησης (π.χ. ο GDPR στην Ε.Ε.).

4.3.6 Δυναμική Πληκτρολόγηση (Keystroke Dynamics)

Η δυναμική πληκτρολόγηση εκμεταλλεύεται τη συμπεριφορά του χρήστη κατά την πληκτρολόγηση (π.χ. τον ρυθμό, την πίεση ή τη χρονική απόσταση μεταξύ πατημάτων πλήκτρων). Ανήκει στα λεγόμενα «συμπεριφορικά βιομετρικά» (behavioral biometrics).

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Χρησιμοποιείται λογισμικό σε συσκευές (υπολογιστές, smartphones) για την καταγραφή των χρονικών σφραγίδων (timestamps) και των μοτίβων πληκτρολόγησης. Υπάρχουν διάφορα πρότυπα καταγραφής. Στα πιο συνηθισμένα καταγράφεται ο χρόνος ανάμεσα στο πάτημα δύο πλήκτρων, ο χρόνος ανάμεσα στην απελευθέρωση δύο πλήκτρων, ο χρόνος ανάμεσα στο πάτημα ενός πλήκτρου και την απελευθέρωση ενός άλλου πλήκτρου και ο συνολικός ρυθμός πληκτρολόγησης (Bolle et al., 2004; Jain et al., 2007).
- Δεν απαιτείται επιπλέον εξοπλισμός πέρα από το τυπικό πληκτρολόγιο ή την οθόνη αφής.

Ακρίβεια (Accuracy)

- Τα ποσοστά επιτυχίας μπορεί να κυμαίνονται αρκετά (70-95%), ανάλογα με τον αλγόριθμο και τη σταθερότητα της συμπεριφοράς του χρήστη – τα ποσοστά για FAR και FRR αναφέρονται 27% και 10% αντιστοίχως (Boulgouris et al., 2009), ενώ σε άλλη έρευνα εντοπίζονται τιμές EER 8,5-10% (Mhenni et al., 2016).

- Παράγοντες, όπως η διάθεση του χρήστη, το άγχος ή τυχόν τραυματισμοί στα χέρια μπορεί να επηρεάσουν αρνητικά την ακρίβεια.

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Θεωρητικά, κάποιος εισβολέας θα πρέπει να μιμηθεί όχι μόνο το τι πληκτρολογεί ο χρήστης, αλλά και πώς (ρυθμός, παύσεις κ.λπ.). Αυτό αυξάνει το επίπεδο ασφάλειας σε συνδυασμό με άλλα μέτρα (π.χ. έλεγχος IP, γεωγραφικής θέσης, μοτίβα ποντικιού).
- Ωστόσο, επιθέσεις μέσω keyloggers ή μέσω εκπαίδευσης μηχανών (machine learning) που μαθαίνουν το μοτίβο ενδέχεται να αποτελούν απειλή. Οι keyloggers μπορούν να καταγράψουν ακριβώς τις χρονικές διαφορές μεταξύ των πατημάτων των πλήκτρων και στη συνέχεια κάποιος κακόβουλα να αναπαράγει το μοτίβο. Κατ' επέκταση ο συνδυασμός keylogger και μηχανικής μάθησης μπορεί να αναλύσει και να γενικεύσει το μοτίβο πληκτρολόγησης του χρήστη (Jain et al., 2007).

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η τεχνολογία είναι «αόρατη» στον χρήστη, αφού δεν απαιτεί πρόσθετες ενέργειες πέρα από την κανονική πληκτρολόγηση.
- Μπορεί να εφαρμοστεί ως συμπληρωματική μέθοδος αυθεντικοποίησης σε περιβάλλοντα όπου ο χρήστης ήδη πληκτρολογεί (π.χ. σε εφαρμογές ιστού).
- Η αποδοχή από τους χρήστες είναι μέτρια (Jain et al., 2004), διότι δημιουργείται η αίσθηση πως παρακολουθούνται κάτι το οποίο δεν είναι ευχάριστο.
- Η μονιμότητα του χαρακτηριστικού είναι αρκετά χαμηλή και χρειάζεται αρκετά συχνά ανανέωση του προτύπου. Για να διατηρηθεί η αξιοπιστία αναγνώρισης του τρόπου πληκτρολόγησης ενός ατόμου θα πρέπει να παρακολουθούνται ταυτόχρονα και οι αλλαγές που παρουσιάζει το άτομο στον τρόπο πληκτρολόγησης με την πάροδο του χρόνου (Mhenni et al., 2016)

Κόστος και Κλιμάκωση

- Δεν χρειάζεται επιπλέον εξοπλισμός, οπότε το κόστος είναι σχεδόν μηδενικό.
- Η κλιμάκωση αφορά κατά κύριο λόγο τη διαχείριση μεγάλου όγκου δεδομένων μοτίβων πληκτρολόγησης και τη συνεχή εκπαίδευση των αλγορίθμων μηχανικής μάθησης (ML) για βελτίωση της ακρίβειας.

Ηθικές και Νομικές Προεκτάσεις

- Τα δεδομένα δυναμικής πληκτρολόγησης θεωρούνται βιομετρικά και πρέπει να προστατεύονται.
- Η «αθόρυβη» συλλογή τέτοιων δεδομένων μπορεί να θεωρηθεί αμφιλεγόμενη από άποψη ιδιωτικότητας, εφόσον δεν υπάρχει ρητή συγκατάθεση καθώς προστατεύεται ρητά από τον GDPR ως βιομετρικό δεδομένο.

4.3.7 Αναγνώριση Βάδισης (Gait Recognition)

Η αναγνώριση βάδισης εξετάζει τον τρόπο που κινείται ένα άτομο, κυρίως σε επίπεδο μοτίβου βηματισμού. Πρόκειται για μια μέθοδο που μπορεί να εφαρμοστεί σε συστήματα παρακολούθησης βίντεο από απόσταση, χωρίς να απαιτείται η συνεργασία του χρήστη.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Γίνεται ανάλυση βίντεο όπου καταγράφεται το σχήμα του σώματος και το μοτίβο κίνησης (π.χ. μέσω χρήσης υπολογιστικής όρασης και αλγορίθμων Μηχανικής Μάθησης).
- Εναλλακτικά, φορητές συσκευές με επιταχυνσιόμετρα (smartphones, smartwatches) μπορούν να καταγράφουν τα δεδομένα βάδισης (ανάλογα με τις εκάστοτε ανάγκες).

Ακρίβεια (Accuracy)

- Η ιδανική απόδοση είναι να χρησιμοποιείται μαζί με την αναγνώριση προσώπου με ποσοστό που φτάνει το 91%, ενώ αν χρησιμοποιείται ανεξάρτητα τότε η απόδοση πέφτει στο 68% (Jain et al., 2007).
- Γενικά, η ακρίβεια είναι χαμηλότερη από μεθόδους, όπως η αναγνώριση ίριδας ή δακτυλικού αποτυπώματος, με αποτέλεσμα να μην χρησιμοποιείται σε εφαρμογές υψηλής ασφάλειας.
- Οι αλλαγές στον ρουχισμό, στα υποδήματα ή στο έδαφος μπορούν να επηρεάσουν την ακρίβεια. Επίσης, παράγοντες υγείας (π.χ. τραυματισμός) αλλάζουν το βηματισμό.
- Συνολικά, η απόδοση θα λέγαμε πως είναι χαμηλή (Jain et al., 2004) (ιδιαίτερα όταν η τεχνολογία χρησιμοποιείται ανεξάρτητα από τις άλλες).

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Η αναγνώριση βάδισης δεν είναι τόσο ευάλωτη σε επιθέσεις πλαστοπροσωπίας όσο άλλες μέθοδοι, διότι για να μιμηθεί κάποιος τον τρόπο βάδισης ενός άλλου ατόμου απαιτείται περίπλοκη εκπαίδευση.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Το κύριο πλεονέκτημα είναι ότι δεν απαιτείται καμία ενεργή συνεργασία από τον χρήστη.
- Η παθητική παρακολούθηση του τρόπου βάδισης σε δημόσιους χώρους εγείρει σοβαρά ζητήματα ιδιωτικότητας και ηθικής ωστόσο η αποδοχή είναι υψηλή καθώς είναι μία μη παρεμβατική μέθοδος.
- Η μονιμότητα των βιομετρικών στοιχείων είναι χαμηλή καθώς πρόκειται για έναν συνδυασμό φυσικών και συμπεριφορικών χαρακτηριστικών, τα οποία επηρεάζονται από πολλούς παράγοντες (π.χ. διάθεση, κούραση, ηλικία, τραυματισμοί).

Κόστος και Κλιμάκωση

- Για την εξαγωγή του χαρακτηριστικού είναι απαραίτητη η χρήση βίντεο, κάτι το οποίο συνεπάγεται μεγαλύτερο όγκο δεδομένων και πολύ πιο αυξημένες υπολογιστικές απαιτήσεις τόσο για την εξαγωγή των χαρακτηριστικών όσο και κατά την σύγκριση του προτύπου και φυσικά για την αποθήκευση των προτύπων στην βάση (Boulgouris et al., 2009).

- Σε επίπεδο video surveillance, χρειάζεται υποδομή καμερών και ισχυρών υπολογιστών για επεξεργασία σε πραγματικό χρόνο. Αυτό συνεπάγεται αυξημένο κόστος.
- Σε εφαρμογές με smartphones, το κόστος είναι πολύ μικρό (όσο το κόστος ενός σύγχρονου smartphone), αλλά απαιτείται ανάπτυξη ή ενσωμάτωση συγκεκριμένου λογισμικού (εφαρμογές android) και αλγορίθμων επεξεργασίας σημάτων. Η ανάλυση των δεδομένων μπορεί να γίνει είτε στη συσκευή (client-side) – στο παρασκήνιο για διαρκή αυθεντικοποίηση – είτε εξωτερικά σε υπολογιστή ή στο νέφος (server-side) όπου προκύπτουν ζητήματα καθυστέρησης και ιδιωτικότητας.

Ηθικές και Νομικές Προεκτάσεις

- Η διαρκής παρακολούθηση του τρόπου που βαδίζει ένας άνθρωπος εμπίπτει σε ζητήματα προστασίας προσωπικών δεδομένων.
- Μολονότι η μέθοδος μπορεί να ενισχύσει την ασφάλεια σε χώρους υψηλής επικινδυνότητας (π.χ. αεροδρόμια), η νομοθεσία (π.χ. ΓΚΠΔ 2016/679) συνήθως απαιτεί ρητή ενημέρωση του κοινού για την ύπαρξη βιομετρικής καταγραφής.

4.3.8 Αναγνώριση Υπογραφής (Signature Recognition)

Η αναγνώριση υπογραφής, ιδιαίτερα όταν γίνεται ηλεκτρονικά, στοχεύει στο να αναλύσει τόσο το στατικό (σχήμα) όσο και το δυναμικό (ταχύτητα, πίεση) μοτίβο της υπογραφής.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Χρησιμοποιούνται ψηφιακά tablet ή οθόνες αφής που καταγράφουν την κίνηση της πένας/γραφίδας.
- Αλγόριθμοι μηχανικής μάθησης εξετάζουν στοιχεία, όπως το μοτίβο των γραμμών, τη μεταβολή στην πίεση, τη γωνία και την ταχύτητα.
- Τα παραπάνω χαρακτηριστικά κωδικοποιούνται σε ένα πρότυπο (signature template) το οποίο συγκρίνεται με αποθηκευμένα δεδομένα/πρότυπα για επαλήθευση.

Ακρίβεια (Accuracy)

- Η δυναμική υπογραφή εμφανίζει ποσοστό FAR 0,43-0,70% και FRR 2-9% ενώ η στατική υπογραφή εμφανίζει ποσοστό FAR 0,2-0,5% (Bolle et al., 2004).
- Ωστόσο, οι διαφοροποιήσεις στην υπογραφή ενός ατόμου ανάλογα με την ψυχοσωματική του κατάσταση επηρεάζουν την ακρίβεια. Επίσης, έμπειροι παραχαράκτες μπορούν πιθανώς να μιμηθούν υπογραφές.

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Η στατική υπογραφή (σκαναρισμένη σε χαρτί) είναι σχετικά εύκολο να πλαστογραφηθεί.
- Η δυναμική υπογραφή (με την καταγραφή πίεσης, ταχύτητας κ.λπ.) είναι πιο ασφαλής, καθώς ο παραχαράκτης πρέπει να μιμηθεί επακριβώς το δυναμικό προφίλ του χρήστη καθιστώντας αυτό το εγχείρημα πιο δύσκολο.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Πολλοί χρήστες είναι εξοικειωμένοι με την υπογραφή ως μέσο ταυτοποίησης (τράπεζες, συμβόλαια κ.λπ.), συνεπώς η αποδοχή από τους χρήστες είναι υψηλή όπως και η ευχρηστία.

- Η ηλεκτρονική διάσταση ίσως απαιτεί εκπαίδευση σε μεγαλύτερες ηλικίες ή σε χώρες όπου δεν είναι διαδεδομένη η ψηφιακή τεχνολογία.
- Η μονιμότητα είναι σχετικά χαμηλή γιατί η υπογραφή είναι ένα συμπεριφορικό χαρακτηριστικό, το οποίο όχι μόνο αλλάζει με το πέρασμα του χρόνου αλλά επηρεάζεται από την συναισθηματική κατάσταση του χρήστη.

Κόστος και Κλιμάκωση

- Απαιτείται ειδική συσκευή (tablet, γραφίδα) οπότε το κόστος της σε ευρεία κλίμακα μπορεί να είναι αποτρεπτικό ειδικά αν η ασφάλεια είναι πρωταρχική προτεραιότητα και αν αφορά δυναμική υπογραφή.
- Σε επιχειρησιακά περιβάλλοντα (π.χ. delivery, τράπεζες), η χρήση ψηφιακών υπογραφών έχει επεκταθεί σημαντικά, δεδομένου πως η αναγνώριση υπογραφής χρησιμοποιείται για one-to-one έλεγχο.

Ηθικές και Νομικές Προεκτάσεις

- Η υπογραφή είναι ήδη νομικά δεσμευτική σε πολλά πλαίσια, οπότε η ψηφιακή έκδοσή της πρέπει να πληροί τους ίδιους όρους ασφάλειας και νομιμότητας.
- Παρά τη μεγάλη παράδοση χρήσης υπογραφών, η εισαγωγή βιομετρικών/δυναμικών στοιχείων αποτελεί πρόσθετη μεταβλητή που χρειάζεται ρύθμιση καθώς σύμφωνα με τον GDPR πρέπει να δηλώνεται ρητά η επεξεργασία των επιπλέον βιομετρικών δεδομένων πέραν της υπογραφής.

4.3.9 Αναγνώριση Παλαμιαίων Αγγείων (Palm Vein Recognition)

Η αναγνώριση φλεβικού μοτίβου παλάμης (palm vein) εκμεταλλεύεται τη μοναδική διάταξη των φλεβών στην παλάμη του χεριού, η οποία απεικονίζεται με υπέρυθρη ακτινοβολία.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Απαιτείται αισθητήρας υπέρυθρων που μπορεί να «δει» τα αιμοφόρα αγγεία κάτω από το δέρμα.
- Σε αντίθεση με δακτυλικά αποτυπώματα, δεν απαιτείται τόσο πολύ η επαφή του χεριού, αλλά μια σωστή τοποθέτηση πάνω από ή κάτω από τον αισθητήρα.

Ακρίβεια (Accuracy)

- Η ακρίβεια μπορεί να είναι πολύ υψηλή, καθώς τα φλεβικά μοτίβα είναι δύσκολο να αντιγραφούν και είναι διαφορετικά ακόμη και μεταξύ μονοζυγωτικών διδύμων (Jain et al., 2007).
- Εξαρτάται ωστόσο από τη σωστή θέση της παλάμης και από παράγοντες, όπως η κυκλοφορία αίματος, η θερμοκρασία του δέρματος, κ.ά.

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Θεωρείται εξαιρετικά ασφαλής μέθοδος, διότι τα φλεβικά μοτίβα είναι εσωτερικά χαρακτηριστικά, οπότε είναι δύσκολο να υποκλαπούν ή να πλαστογραφηθούν.
- Η «ζωντάνια» του δείγματος αποτελεί εγγενές χαρακτηριστικό, καθώς το αίμα πρέπει να ρέει στο χέρι.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Για πολλούς χρήστες, η σάρωση της παλάμης είναι λιγότερο παρεμβατική από την αναγνώριση ίριδας ή αμφιβληστροειδούς, καθώς δεν αφορά την περιοχή του προσώπου/ματιών.
- Χρειάζεται, όμως, λίγος χρόνος εξοικείωσης για τη σωστή τοποθέτηση της παλάμης πάνω από τον αισθητήρα. Γενικά, η αποδοχή των χρηστών είναι μέτρια όπως και η ευχρηστία.
- Η μονιμότητα του βιομετρικού προτύπου είναι μέτρια και δεν επηρεάζεται τόσο από τις περιβαλλοντικές συνθήκες (π.χ. σκόνη καθώς τα αγγεία βρίσκονται κάτω από το δέρμα) (Jain et al., 2004; Jain et al., 2007).

Κόστος και Κλιμάκωση

- Οι αισθητήρες (υπέρυθρων) palm vein είναι πιο ακριβοί από τους απλούς οπτικούς ή χωρητικούς σαρωτές (scanners), αλλά η τιμή τους παρουσιάζει πτωτική τάση καθώς αναπτύσσεται η τεχνολογία.
- Εν γένει, το κόστος θεωρείται υψηλό αλλά υιοθετείται σε τομείς που έχουν την οικονομική άνεση να το καλύψουν π.χ. τράπεζες. Όμως, το κόστος για entry-level αισθητήρες (για μικρότερες εγκαταστάσεις και βασικό επίπεδο ασφάλειας) θεωρείται μέτριο.
- Η επέκταση σε μαζικά περιβάλλοντα (π.χ. τράπεζες, νοσοκομεία) έχει ήδη ξεκινήσει, με πολλές επιτυχίες ιδίως στην Ιαπωνία και σε τραπεζικά δίκτυα που υιοθετούν την τεχνολογία της Fujitsu ή άλλων παρόχων.

Ηθικές και Νομικές Προεκτάσεις

- Όπως και σε άλλες βιομετρικές μεθόδους, η συλλογή και αποθήκευση των φλεβικών μοτίβων χρήζει αυστηρής εποπτείας και νομικών εγγυήσεων (δείτε GDPR).

4.3.10 Πολυτροπικά Συστήματα (Multimodal Systems)

Τα πολυτροπικά βιομετρικά συστήματα συνδυάζουν περισσότερες από μία βιομετρικές μεθόδους (π.χ. δακτυλικό αποτύπωμα και αναγνώριση προσώπου) για την αύξηση της ακρίβειας και της ασφάλειας. Η λογική είναι ότι η πιθανότητα ένας εισβολέας να παρακάμψει πολλαπλά βιομετρικά χαρακτηριστικά ταυτόχρονα μειώνεται δραστικά.

Τεχνική Υλοποίηση και Προαπαιτούμενα

- Απαιτείται ενοποίηση των αισθητήρων και των αλγορίθμων επεξεργασίας σε ένα ολοκληρωμένο σύστημα λήψης αποφάσεων (fusion).
- Μπορούν να χρησιμοποιηθούν διαφορετικές προσεγγίσεις fusion, όπως early fusion (συνδυασμός των χαρακτηριστικών πριν την ταξινόμηση) ή late fusion (λήψη της απόφασης με συνδυασμό της εκτίμησης του κάθε ταξινομητή). Στην περίπτωση αυτή έχουμε μια μορφή composition/ensemble μοντέλων μηχανικής μάθησης.
- Υπάρχει επίσης η προσέγγιση hybrid fusion, η οποία συνδυάζει χαρακτηριστικά early & late fusion ώστε να αξιοποιεί τα πλεονεκτήματα και των δύο μεθόδων (Atrey, Hossain, El Saddik, & Kankanhalli, 2010).

Ακρίβεια (Accuracy)

- Η ακρίβεια συνήθως βελτιώνεται σημαντικά, καθώς οι αδυναμίες της μίας μεθόδου αντισταθμίζονται από την άλλη.
- Το FAR και το FRR μπορεί να γίνουν εξαιρετικά χαμηλά, ιδίως όταν οι τεχνολογίες είναι ίδιες αλλά εφαρμόζονται με διαφορετικούς τρόπους ή είναι συμπληρωματικές (π.χ. πρόσωπο + φωνή + δακτυλικό αποτύπωμα ή δακτυλικό αποτύπωμα και από τα πέντε δάκτυλα όπου το σύστημα κάθε φορά τυχαία θα ζητάει δύο διαφορετικά δάκτυλα).

Ασφάλεια και Ανθεκτικότητα σε Επιθέσεις

- Η ασφάλεια αυξάνεται, αφού ο επιτιθέμενος πρέπει να πλαστογραφήσει πολλαπλά βιομετρικά στοιχεία, αλλά αν τα βιομετρικά στοιχεία είναι εύκολο να πλαστογραφηθούν, βαθμός αύξησης θα είναι μικρός.
- Ταυτόχρονα, το σύστημα είναι πιο περίπλοκο, αυξάνοντας την πιθανότητα σφαλμάτων στην υλοποίηση ή τη διαχείριση δεδομένων. Συνεπώς μπορεί να προκύψουν ζητήματα διαθεσιμότητας, αξιοπιστίας καθώς και ασφάλειας.

Ευχρηστία, Μονιμότητα και Αποδοχή Χρηστών

- Η ταυτόχρονη χρήση πολλαπλών βιομετρικών στοιχείων ίσως δυσκολέψει την εμπειρία του χρήστη (π.χ. πρέπει και να κοιτάζει την κάμερα και να τοποθετήσει το δάκτυλο στον αισθητήρα), συνεπώς η ευχρηστία μειώνεται.
- Σε ορισμένες περιπτώσεις, μπορεί να χρησιμοποιείται μια μέθοδος ως κύρια (π.χ. δακτυλικό) και άλλη ως εφεδρική (π.χ. φωνή), γεγονός που βελτιώνει την εμπειρία χρήσης. Οπότε, θα λέγαμε πως η αποδοχή των χρηστών είναι μέτρια.
 - Η εφεδρική μέθοδος ενεργοποιείται σε σενάρια όπου η κύρια μέθοδος θα αποτύχει λόγω περιβαλλοντικών παραγόντων. Το σύστημα μπορεί να ανιχνεύσει τις κακές συνθήκες με αισθητήρες φωτισμού ή θορύβου.
- Η μονιμότητα εξαρτάται από τα επιμέρους βιομετρικά χαρακτηριστικά που χρησιμοποιεί το σύστημα.

Κόστος και Κλιμάκωση

- Η χρήση πολλαπλών αισθητήρων ανεβάζει (ενδεχομένως αρκετά) το κόστος, προσθέτει πολυπλοκότητα στο σύστημα και ο όγκος των δεδομένων αυξάνεται, παράγοντες που μπορεί να αποτελέσουν τροχοπέδη στην κλιμάκωση.
- Παρ' όλα αυτά, σε εφαρμογές κρίσιμης σημασίας (π.χ. κυβερνητικές εγκαταστάσεις, στρατιωτικές βάσεις), το αυξημένο κόστος δικαιολογείται.

Ηθικές και Νομικές Προεκτάσεις

- Τα πολυτροπικά συστήματα συλλέγουν περισσότερα βιομετρικά χαρακτηριστικά, γεγονός που εντείνει τις ανησυχίες για παραβίαση ιδιωτικότητας και λανθασμένες ταυτοποιήσεις.
- Επιπρόσθετη παραμετροποίηση του συστήματος ενδέχεται να απαιτείται για τη διασφάλιση ότι η επεξεργασία πολλαπλών βιομετρικών δεδομένων πραγματοποιείται σύμφωνα με τη νομοθεσία και τις προϋποθέσεις της.

4.4 Πλεονεκτήματα και Μειονεκτήματα των Διαφορετικών Τεχνολογιών

Σε αυτή την ενότητα, επιχειρούμε μια πιο ολοκληρωμένη και συγκεντρωτική θεώρηση των πλεονεκτημάτων και μειονεκτημάτων, εστιάζοντας στους βασικούς παράγοντες που επηρεάζουν την επιλογή της κατάλληλης βιομετρικής τεχνολογίας για κάθε εφαρμογή.

4.4.1 Αναγνώριση Δακτυλικών Αποτυπωμάτων

Πλεονεκτήματα

- Ωριμότητα τεχνολογίας και ευρεία εφαρμογή.
- Χαμηλό κόστος ενσωμάτωσης, με πληθώρα αισθητήρων διαθέσιμων.
- Γρήγορη ταυτοποίηση και μεγάλη κοινωνική αποδοχή.

Μειονεκτήματα

- Τρωτότητα σε πλαστοπροσωπία με τεχνητά δάκτυλα, αν δεν υπάρχει liveness detection.
- Υποβάθμιση ακρίβειας σε περιβάλλοντα με υγρασία, σκόνη ή τραυματισμούς στα δάχτυλα.

4.4.2 Αναγνώριση Προσώπου

Πλεονεκτήματα

- Χαμηλή παρεμβατικότητα, ο χρήστης απλώς κοιτάει την κάμερα.
- Μπορεί να εφαρμοστεί σε απομακρυσμένες/μαζικές ταυτοποιήσεις.
- Εντυπωσιακή ακρίβεια με προηγμένα 3D ή IR συστήματα.

Μειονεκτήματα

- Ηθικά και νομικά ζητήματα λόγω παρακολούθησης.
- Ευπάθεια σε 2D πλαστοπροσωπία αν δεν υπάρχει 3D/IR σύστημα.
- Επηρεάζεται από αλλαγές στην εμφάνιση (π.χ. γενειάδα, μάσκες) και στο περιβάλλον (π.χ. χαμηλός φωτισμός).

4.4.3 Αναγνώριση Ίριδας

Πλεονεκτήματα

- Εξαιρετική ακρίβεια, πολύ χαμηλά FAR/FRR και πολύ υψηλή απόδοση.
- Σχετικά δύσκολη πλαστογράφηση.
- Σταθερό βιομετρικό χαρακτηριστικό καθ' όλη τη διάρκεια της ζωής.

Μειονεκτήματα

- Υψηλότερο κόστος εξοπλισμού.
- Απαιτείται στενή απόσταση λήψης και συνεργασία του χρήστη.

4.4.4 Αναγνώριση Αμφιβληστροειδούς

Πλεονεκτήματα

- Από τις πιο ασφαλείς και δύσκολες μεθόδους πλαστογράφησης.
- Πολύ υψηλή ακρίβεια και απόδοση.

Μειονεκτήματα

- Πολύ παρεμβατική και άβολη εμπειρία χρήσης με φόβο για πιθανές επιπτώσεις και αποκαλύψεις ιατρικών καταστάσεων.
- Υψηλό κόστος εξοπλισμού και μεγάλος όγκος.
- Χαμηλή αποδοχή από το ευρύ κοινό.

4.4.5 Αναγνώριση Φωνής

Πλεονεκτήματα

- Δεν απαιτείται φυσική ή οπτική επαφή.
- Ιδιαίτερα χρήσιμη σε τηλεφωνικά κέντρα ή hands-free εφαρμογές.
- Σχετικά χαμηλό κόστος για βασική υλοποίηση.

Μειονεκτήματα

- Επηρεάζεται από θόρυβο περιβάλλοντος, ασθένειες φωνής και τη διάθεση, παράγοντες που στις περισσότερες πρακτικές εφαρμογές δεν μπορούν να εξαλειφθούν.
- Τρωτότητα σε επιθέσεις αναπαραγωγής φωνής ή σύνθεσης φωνής (voice playback or synthesis attacks).
- Αποτελεί πιο ασταθές χαρακτηριστικό σε σχέση με τα άλλα διαθέσιμα βιομετρικά χαρακτηριστικά.

4.4.6 Δυναμική Πληκτρολόγηση

Πλεονεκτήματα

- Δεν απαιτείται επιπλέον εξοπλισμός (μόνο λογισμικό) σε σύγκριση με τις άλλες μεθόδους.
- Εφαρμόζεται αθόρυβα, συμπληρωματικά με άλλα μέτρα.

Μειονεκτήματα

- Μεσαία επίπεδα ακρίβειας, ευαισθησία σε αλλαγές συμπεριφοράς που μπορεί να οφείλονται σε διάφορους παράγοντες – εν γένει, χαμηλή απόδοση.
- Πολύ χαμηλή μονιμότητα με ανάγκη συχνής ανανέωσης των προτύπων.
- Δύσκολο να χρησιμοποιηθεί ως μοναδικός παράγοντας αυθεντικοποίησης.
- Τρωτότητα σε επιθέσεις keylogging σε συνδυασμό με αλγόριθμους μηχανικής μάθησης.

4.4.7 Αναγνώριση Βάδισης

Πλεονεκτήματα

- Χαμηλή παρεμβατικότητα, μπορεί να λειτουργήσει εξ αποστάσεως.
- Χρήσιμη για συστήματα επιτήρησης χωρίς συνεργασία στόχου.
- Δύσκολο να πλαστογραφηθεί.

Μειονεκτήματα

- Χαμηλή ακρίβεια σε σχέση με άλλες μεθόδους.
- Εξαρτάται από ρουχισμό, κούραση, πιθανά προβλήματα υγείας.
- Χαμηλή μονιμότητα των βιομετρικών χαρακτηριστικών αυτού του είδους.
- Υψηλό κόστος όταν εφαρμόζεται video surveillance.
- Σημαντικά ζητήματα προστασίας ιδιωτικότητας.

4.4.8 Αναγνώριση Υπογραφής

Πλεονεκτήματα

- Νομικά και κοινωνικά καθιερωμένη μέθοδος.
- Υψηλή αποδοχή από χρήστες.
- Οι δυναμικές υπογραφές είναι δύσκολο να πλαστογραφηθούν.

Μειονεκτήματα

- Σχετικά μέτρια ακρίβεια, επηρεάζεται από ψυχολογικούς και φυσικούς παράγοντες.
- Χρειάζεται εξοπλισμό (ταμπλέτες, γραφίδες) για δυναμική καταγραφή.
- Μπορεί να απαιτήσει εκπαίδευση.
- Παρουσιάζει σχετικά χαμηλή μονιμότητα.

4.4.9 Αναγνώριση Παλαμιαίων Αγγείων

Πλεονεκτήματα

- Πολύ ασφαλής και δύσκολη στην πλαστογράφιση.
- Απαιτεί ελάχιστη φυσική επαφή (ή και καθόλου σε ορισμένους σαρωτές). – Λιγότερο παρεμβατική.

Μειονεκτήματα

- Απαιτείται ειδικός αισθητήρας IR με σχετικά υψηλό κόστος.
- Χρειάζεται χρόνος εξοικείωσης ως προς τη σωστή τοποθέτηση της παλάμης.

4.4.10 Πολυτροπικά Συστήματα

Πλεονεκτήματα

- Περισσότερη ακρίβεια και ασφάλεια μέσω συνδυασμού μεθόδων.
- Ιδανικά για εφαρμογές υψηλής ασφάλειας (εφόσον χρησιμοποιούνται κατάλληλες συμπληρωματικές τεχνολογίες).

Μειονεκτήματα

- Αυξημένο κόστος και πολυπλοκότητα.
- Ενδεχόμενη επιβάρυνση στην εμπειρία χρήσης.
- Μεγαλύτερος όγκος βιομετρικών δεδομένων προς διαχείριση.

4.5 Αποτελέσματα Σύγκρισης και Συμπεράσματα

Λαμβάνοντας υπόψη τα παραπάνω, καθίσταται σαφές ότι δεν υπάρχει «μία λύση που ταιριάζει σε όλα» στο πεδίο της βιομετρικής αυθεντικοποίησης. Η βέλτιστη επιλογή εξαρτάται από το περιβάλλον της εφαρμογής:

- *Για καθημερινή χρήση σε smartphones:* Η αναγνώριση δακτυλικού αποτυπώματος και η αναγνώριση προσώπου (με 3D ή IR) αποτελούν κυρίαρχες λύσεις, λόγω του υψηλού επιπέδου ευχρηστίας, της ταχύτητας και του χαμηλού κόστους υλοποίησης σε μαζική κλίμακα.
- *Για εφαρμογές υψηλής ασφάλειας:* Η αναγνώριση ίριδας ή αμφιβληστροειδούς, καθώς και τα πολυτροπικά συστήματα που συνδυάζουν πολλαπλές τεχνολογίες, εξασφαλίζουν πολύ χαμηλά ποσοστά λαθών και μεγαλύτερη ανθεκτικότητα σε επιθέσεις, παρά το υψηλότερο κόστος και την πιο σύνθετη εμπειρία χρήσης.
- *Για συστήματα τηλεφωνικής εξυπηρέτησης:* Η αναγνώριση φωνής μπορεί να είναι μια ικανοποιητική λύση, ειδικά όταν συνδυάζεται με συμπληρωματικές ερωτήσεις ασφαλείας ή πολυτροπικές προσεγγίσεις.
- *Για συνεχή ή παθητική ταυτοποίηση:* Τεχνολογίες όπως η δυναμική ηλεκτρολόγηση ή η αναγνώριση βάδισης προσφέρουν μη παρεμβατικούς τρόπους ελέγχου, λειτουργώντας επικουρικά για τη βελτίωση της ασφάλειας.
- *Για συναλλαγές που απαιτούν υπογραφή:* Η ενσωμάτωση δυναμικής αναγνώρισης υπογραφής μπορεί να βελτιώσει την αντίσταση στην απάτη, εντούτοις δεν πρέπει να αποτελεί τη μοναδική μέθοδο ταυτοποίησης.

Η σύγκλιση πολλών μεθόδων (πολυτροπικά συστήματα) συνιστάται σε περιπτώσεις όπου η ασφάλεια και η ακρίβεια είναι κρίσιμες, παρά την αύξηση του κόστους και της πολυπλοκότητας. Επιπλέον, οι νομικές και ηθικές διαστάσεις της συλλογής, αποθήκευσης και επεξεργασίας βιομετρικών δεδομένων έχουν καταστεί πλέον καθοριστικές στη διαμόρφωση της αποδοχής και της ευρείας υιοθέτησης τέτοιων συστημάτων.

Στον παρακάτω πίνακα παρουσιάζονται συνοπτικά οι ενδεικτικές εφαρμογές, καθώς και οι απαιτήσεις εξοπλισμού, περιβάλλοντος και χρήσης για τις τεχνολογίες βιομετρικής αυθεντικοποίησης που εξετάζονται.

Πίνακας 1: Πίνακας απαιτήσεων και εφαρμογών βιομετρικών τεχνολογιών

Τεχνολογία	Καταλληλότητα / Ενδεικτικές Εφαρμογές	Απαιτήσεις Χρήσης	Απαιτήσεις Εξοπλισμού	Απαιτήσεις Περιβάλλοντος / Χρήστη
Δακτυλικά Αποτυπώματα	Smartphones, e-IDs, έλεγχος πρόσβασης	Ταχύτητα >= υψηλή, ευχρηστία >= υψηλή	Αισθητήρας δακτυλικού αποτυπώματος	Περιβάλλον χωρίς σκόνη, στεγνά δάχτυλα
Αναγνώριση Προσώπου	Smartphones, παρακολούθηση, έλεγχος πρόσβασης, social media	Ταχύτητα >= υψηλή, ευχρηστία >= υψηλή	Απλές κάμερες 2D ή προηγμένοι αισθητήρες 3D/IR	Καλός και σταθερός φωτισμός
Αναγνώριση Ίριδας	Εγκαταστάσεις υψηλής ασφάλειας, σύνορα, αεροδρόμια	Ευχρηστία >= μέτρια, ακρίβεια >= υψηλή	Σαρωτής ίριδας	Κοντινή απόσταση, σταθερό βλέμμα
Αναγνώριση Αμφιβληστροειδούς	Στρατιωτικοί χώροι, εγκαταστάσεις πυρηνικής ενέργειας	Ακρίβεια >= υψηλή, ασφάλεια >= υψηλή	Σαρωτής αμφιβληστροειδούς	Ακριβής τοποθέτηση ματιού, κοντινή απόσταση, συνεργασία χρήστη
Αναγνώριση Φωνής	Τηλεφωνικά κέντρα, εξυπηρέτηση πελατών, απλή απομακρυσμένη αυθεντικοποίηση	Αποδοχή >= υψηλή, χωρίς φυσική παρουσία	Μικρόφωνο, ειδικό λογισμικό φωνητικής ανάλυσης	Ήσυχο περιβάλλον, καθαρή φωνή
Δυναμική Πληκτρολόγηση	Συμπληρωματική μέθοδος ασφαλείας σε χρήση υπολογιστή, web apps	Αποδοχή >= μέτρια, διαρκής αυθεντικοποίηση	Πληκτρολόγιο, ειδικό λογισμικό ανάλυσης μοτίβων πληκτρολόγησης	Χωρίς ειδικές απαιτήσεις
Αναγνώριση Βάδισης	Συστήματα επιτήρησης, ειδικά περιβάλλοντα (αεροδρόμια, δημόσιοι χώροι)	Αποδοχή >= υψηλή, χρήση σε ανοιχτούς χώρους	Κάμερες ή φορητές συσκευές με αισθητήρες επιταχυνσιόμετρων	Ανοιχτό οπτικό πεδίο (για χρήση κάμερας)
Αναγνώριση Υπογραφής	Τράπεζες, νομικά έγγραφα, εταιρικές εγκρίσεις	Ευχρηστία >= υψηλή, αποδοχή >= υψηλή, υψηλή ακρίβεια ως συμπληρωματική μέθοδος	Ειδική γραφίδα ή/και ψηφιακά tablet καταγραφής	Σταθερή επιφάνεια υπογραφής
Αναγνώριση Παλαμιαίων Αγγείων	Τράπεζες, νοσοκομεία, επιχειρήσεις με κρίσιμης σημασίας εγκαταστάσεις	Ακρίβεια >= υψηλή, ασφάλεια >= υψηλή	Αισθητήρας υπερύθρων	Συνεργασία χρήστη, σωστή τοποθέτηση, σταθερή θερμοκρασία χώρου
Πολυτροπικά Συστήματα	Στρατιωτικές-κυβερνητικές εγκαταστάσεις, εφαρμογές όπου απαιτείται μηδενική πιθανότητα λάθους	Ακρίβεια >= υψηλή, πολύ υψηλή ασφάλεια	Εξοπλισμός των επιμέρους τεχνολογιών και σύστημα ενοποίησης των επιμέρους τεχνολογιών	Εξαρτάται από τις επιμέρους τεχνολογίες

4.5.1 Ενιαίος Συγκριτικός Πίνακας

Ο παρακάτω πίνακας συνοψίζει τα κύρια χαρακτηριστικά κάθε βιομετρικής τεχνολογίας με βάση ορισμένους βασικούς δείκτες. Επισημαίνεται ότι οι τιμές (π.χ. ακρίβεια, κόστος, κ.λπ.) είναι ενδεικτικές και εξαρτώνται από την ποιότητα του εκάστοτε συστήματος και τις συνθήκες υλοποίησης. Οι τιμές που χρησιμοποιούνται στον πίνακα για να αξιολογήσουν τους δείκτες είναι: «πολύ χαμηλή», «χαμηλή», «μέτρια», «υψηλή» και «πολύ υψηλή». Σε ορισμένες περιπτώσεις παρατίθεται εύρος τιμών, καθώς δεν μπορεί να προσδιοριστεί μία μοναδική τιμή. Αυτό οφείλεται στην εξάρτηση από πολλούς παράγοντες, όπως αναφέρθηκε και προηγουμένως, οι οποίοι οδηγούν σε ποικιλομορφία τιμών. Χαρακτηριστικό παράδειγμα είναι η τεχνολογία πολυτροπικών συστημάτων, η οποία εξαρτάται από τις επιμέρους τεχνολογίες που συνδυάζονται. Η κύρια επιστημονική βάση για την σύνθεση του πίνακα προέρχεται από τις έρευνες των Bolle και Jain (Bolle et al., 2004; Jain et al., 2004), ωστόσο εφαρμόστηκαν αρκετές αλλαγές (σε σχέση με αυτές τις έρευνες) με βάση την επιλεγμένη σύγχρονη βιβλιογραφία που μελετήθηκε.

Πίνακας 2: Ενιαίος συγκριτικός πίνακας βιομετρικών τεχνολογιών

Τεχνολογία	Ακρίβεια	Ασφάλεια (Spoofing)	Ευχρηστία	Μονιμότητα	Αποδοχή	Κόστος Εξοπλισμού
Δακτυλικά Αποτυπώματα	Υψηλή	Μέτρια έως Υψηλή	Πολύ Υψηλή	Υψηλή	Υψηλή	Χαμηλό έως Μέτριο
Αναγνώριση Προσώπου	Μέτρια έως Υψηλή	Χαμηλή (2D) Υψηλή (3D)	Πολύ Υψηλή	Μέτρια	Υψηλή	Μέτριο έως Υψηλό (ιδίως για 3D)
Αναγνώριση Ίριδας	Υψηλή	Υψηλή	Μέτρια	Υψηλή έως Πολύ Υψηλή	Μέτρια έως Υψηλή	Μέτριο
Αναγνώριση Αμφιβληστροειδούς	Πολύ Υψηλή	Πολύ Υψηλή	Χαμηλή	Πολύ Υψηλή	Χαμηλή	Υψηλό
Αναγνώριση Φωνής	Μέτρια	Χαμηλή έως Μέτρια	Υψηλή	Χαμηλή	Υψηλή	Πολύ Χαμηλό έως Χαμηλό
Δυναμική Πληκτρολόγηση	Μέτρια	Μέτρια	Πολύ Υψηλή	Πολύ Χαμηλή	Μέτρια	Πολύ Χαμηλό
Αναγνώριση Βάδισης	Χαμηλή	Υψηλή	Πολύ Υψηλή	Χαμηλή	Υψηλή	Μέτριο έως Υψηλό
Αναγνώριση Υπογραφής	Μέτρια έως Υψηλή	Χαμηλή (στατική) Υψηλή (δυναμική)	Υψηλή	Χαμηλή	Υψηλή	Χαμηλό (στατική) Μέτριο (δυναμική)
Αναγνώριση Παλαμιαίων Αγγείων	Πολύ Υψηλή	Πολύ Υψηλή	Μέτρια	Μέτρια	Μέτρια	Μέτριο έως Υψηλό (ειδικός IR αισθητήρας)
Πολυτροπικά Συστήματα	Υψηλή έως Πολύ Υψηλή	Πολύ Υψηλή	Μέτρια έως Πολύ Υψηλή (εξαρτάται από την εφαρμογή)	Χαμηλή-Υψηλή	Χαμηλή έως Υψηλή (ανάλογα με τις μεθόδους)	Χαμηλό έως Πολύ Υψηλό

4.5.2 Καλύτερες και Χειρότερες Τεχνολογίες ανά Κριτήριο

Ο παρακάτω πίνακας εμφανίζει τις τεχνολογίες που εμφανίζουν την υψηλότερη και χαμηλότερη απόδοση σε κάθε κριτήριο. Όπου θεωρήθηκε πως η διαφορά μεταξύ τεχνολογιών είναι μικρή αναγράφονται περισσότερες από μία τεχνολογίες. Η υψηλότερη και χαμηλότερη απόδοση βασίστηκε στις τιμές αξιολόγησης που αναφέρονται στον Πίνακα 2 για τις τεχνολογίες που συγκρίνονται. Όταν ένα κριτήριο έχει θετική κατεύθυνση τιμών (π.χ. ακρίβεια), τότε υψηλότερη απόδοση σημαίνει μεγαλύτερη τιμή και χαμηλότερη απόδοση μικρότερη τιμή. Αντίστοιχα όταν ένα κριτήριο έχει αρνητική κατεύθυνση τιμών (π.χ. κόστος εξοπλισμού), τότε υψηλότερη απόδοση σημαίνει μικρότερη τιμή και χαμηλότερη απόδοση μεγαλύτερη τιμή.

Είναι σημαντικό να επισημανθεί πως δεν υπάρχει «καλύτερη βιομετρική τεχνολογία», αλλά κάθε φορά ανάλογα με τις απαιτήσεις και το πλαίσιο εφαρμογής επιλέγεται η βέλτιστη λύση. Ωστόσο, παρατηρώντας τον παρακάτω πίνακα (ο οποίος επιδεικνύει τις καλύτερες & χειρότερες τεχνολογίες ανά κριτήριο) και κυρίως λαμβάνοντας υπόψη όλα τα προαναφερθέντα θα μπορούσε να ειπωθεί πως τρεις τεχνολογίες ξεχωρίζουν παρουσιάζοντας ισορροπημένη απόδοση στα κύρια κριτήρια. Οι τεχνολογίες αυτές είναι: η αναγνώριση δακτυλικών αποτυπωμάτων, η αναγνώριση ίριδας και η αναγνώριση προσώπου. Παρότι οι τεχνολογίες αυτές δεν εμφανίζονται συχνά ως κορυφαίες σε απόδοση στα κριτήρια, παρουσιάζουν συνολικά ισορροπημένες επιδόσεις με σταθερά καλή απόδοση σε όλα τα βασικά χαρακτηριστικά αξιολόγησης, προσφέροντας λύσεις σε πλήθος σεναρίων. Αντίθετα, η αναγνώριση αμφιβληστροειδούς εμφανίζει σοβαρά λειτουργικά μειονεκτήματα και παρά το γεγονός ότι ενσωματώνει το ασφαλέστερο βιομετρικό χαρακτηριστικό είναι η λιγότερο πρακτική λύση και ίσως η «χειρότερη τεχνολογία». Τέλος, ιδιαίτερη αναφορά αξίζει στα πολυτροπικά συστήματα, τα οποία διαθέτουν τις μεγαλύτερες προοπτικές εξέλιξης και αποτελεσματικότητας, υπό την προϋπόθεση ότι θα αντιμετωπιστούν επιτυχώς ζητήματα απόδοσης, πολυπλοκότητας και κόστους.

Πίνακας 3: Πίνακας τεχνολογιών υψηλής & χαμηλής απόδοσης ανά κριτήριο

Βασικοί Δείκτες	Τεχνολογίες υψηλής απόδοσης	Τεχνολογίες χαμηλής απόδοσης
Ακρίβεια	↑ Αναγνώριση αμφιβληστροειδούς ↑ Αναγνώριση παλαμιαίων αγγείων	↓ Αναγνώριση βάδισης
Ασφάλεια	↑ Πολυτροπικά συστήματα ↑ Αναγνώριση αμφιβληστροειδούς ↑ Αναγνώριση παλαμιαίων αγγείων	↓ Αναγνώριση φωνής
Ευχρηστία	↑ Αναγνώριση προσώπου ↑ Δακτυλικά αποτυπώματα ↑ Δυναμική πληκτρολόγηση ↑ Αναγνώριση βάδισης	↓ Αναγνώριση αμφιβληστροειδούς
Μονιμότητα	↑ Αναγνώριση αμφιβληστροειδούς ↑ Αναγνώριση ίριδας	↓ Δυναμική πληκτρολόγηση
Αποδοχή	↑ Αναγνώριση φωνής ↑ Αναγνώριση υπογραφής ↑ Αναγνώριση βάδισης ↑ Αναγνώριση προσώπου ↑ Δακτυλικά αποτυπώματα	↓ Αναγνώριση αμφιβληστροειδούς
Κόστος εξοπλισμού	↑ Δυναμική πληκτρολόγηση ↑ Αναγνώριση φωνής	↓ Αναγνώριση αμφιβληστροειδούς

5

Επίλογος – Συζήτηση

Η παρούσα συγκριτική επισκόπηση αναδεικνύει με ενάργεια τη σύνθετη και πολυδιάστατη φύση του πεδίου των βιομετρικών τεχνολογιών αυθεντικοποίησης. Συγκεντρώνοντας τα πορίσματα από την εμβριθή εξέταση διαφορετικών προσεγγίσεων, είναι εφικτό να συνάγουμε μια σειρά από συμπεράσματα που αναδεικνύουν όχι μόνο τα ισχυρά σημεία και τις αδυναμίες κάθε τεχνολογίας, αλλά και τις προοπτικές μελλοντικής εξέλιξης. Στον βαθμό που η ανθρωπότητα προσανατολίζεται όλο και περισσότερο προς την ψηφιοποίηση των διαδικασιών, την αυτοματοποίηση και τη διάχυτη χρήση τεχνητής νοημοσύνης, ο ρόλος της βιομετρικής αυθεντικοποίησης καθίσταται καίριος για την κατοχύρωση ενός ισορροπημένου επιπέδου ασφάλειας και χρηστικότητας.

Σε αυτό το τελευταίο τμήμα της εργασίας, το οποίο λειτουργεί ως συνολική συζήτηση και επίλογος, επιχειρείται να παρουσιαστούν τα πλέον κρίσιμα ζητήματα του πεδίου, καθώς και να προσδιοριστούν οι μελλοντικές κατευθύνσεις που θα διαμορφώσουν την περαιτέρω ανάπτυξη των βιομετρικών μεθόδων. Η στόχευση έγκειται όχι μόνο στο να ανακεφαλαιώσουμε όσα διερευνήθηκαν και συγκρίθηκαν προηγουμένως, αλλά και στο να αναδείξουμε τις ουσιώδεις προκλήσεις και τους περιορισμούς που δημιουργούν ευκαιρίες για καινοτομία, επιστημονική πρόοδο και διερεύνηση από την ακαδημαϊκή κοινότητα, τη βιομηχανία και τα ρυθμιστικά όργανα.

5.1 Επαναπροσδιορισμός της Σημασίας των Βιομετρικών Τεχνολογιών

Η αναζήτηση ασφαλών, πρακτικών και ταυτόχρονα φιλικών προς τον χρήστη τρόπων αυθεντικοποίησης επηρεάζει άμεσα τόσο την καθημερινότητα των πολιτών όσο και την υποδομή των οργανισμών (δημόσιων ή ιδιωτικών). Οι παραδοσιακοί μηχανισμοί ταυτοποίησης, όπως οι κωδικοί πρόσβασης (passwords) και οι κάρτες πρόσβασης, έχουν αναδείξει αδυναμίες ως προς την ανθεκτικότητά τους σε επιθέσεις και την ευκολία με την οποία παραβιάζονται ή κλέβονται. Σε αυτό το πλαίσιο, οι βιομετρικές τεχνολογίες ήρθαν να συμπληρώσουν—και, σε πολλές περιπτώσεις, να αντικαταστήσουν—τους παραδοσιακούς τρόπους επαλήθευσης της ταυτότητας, προωθώντας την ιδέα ότι «είσαι ό,τι είσαι» (something you are) σε αντίθεση με το «κάτι που κατέχεις» (κάρτα, token) ή «κάτι που γνωρίζεις» (κωδικός).

Ωστόσο, η ευρεία χρήση βιομετρικών συστημάτων δεν είναι απλώς τεχνικό ζήτημα· εμπερικλείει επίσης κοινωνικές, νομικές και ηθικές διαστάσεις, οι οποίες οφείλουν να τεθούν στο επίκεντρο κάθε σοβαρής αναπτυξιακής πολιτικής ή τεχνολογικής σχεδίασης. Η αναζήτηση του βέλτιστου σημείου ισορροπίας ανάμεσα στη λειτουργικότητα και την προστασία των δικαιωμάτων των πολιτών – ειδικά στην εποχή των ψηφιακών δεδομένων και της μεγάλης κλίμακας επεξεργασίας πληροφοριών – αποτελεί διαρκή πρόκληση.

5.2 Υπενθύμιση των Κύριων Συμπερασμάτων από τη Σύγκριση των Τεχνολογιών

Η ανάλυση που προηγήθηκε κατέδειξε ότι οι διάφορες βιομετρικές μέθοδοι (λ.χ. δακτυλικά αποτυπώματα, αναγνώριση προσώπου, ίριδας, φωνής, δυναμική πληκτρολόγησης κ.λπ.) παρουσιάζουν διαφορετικά επίπεδα ακρίβειας, ασφάλειας, κόστους, κλιμάκωσης, παρεμβατικότητας, αποδοχής από τους χρήστες, νομικής πολυπλοκότητας, και καταλληλότητας. Σε γενικές γραμμές, δεν μπορεί να θεωρηθεί ότι υπάρχει μία καθολική λύση που να καλύπτει όλες τις χρήσεις, ακριβώς διότι οι ανάγκες των εφαρμογών διαφέρουν σημαντικά ως προς τις απαιτήσεις ασφάλειας, τον αριθμό των χρηστών, τις τεχνικές υποδομές, την κλίμακα εφαρμογής και τις συνθήκες χρήσης. Ακολουθεί μία σύνοψη, με τα πιο χαρακτηριστικά πλεονεκτήματα και περιορισμούς της κάθε τεχνολογίας.

1. Αναγνώριση Δακτυλικών Αποτυπωμάτων:

- Διαθέτει υψηλή ωριμότητα και ευρεία υιοθέτηση, με κόστος που κυμαίνεται πλέον σε ιδιαίτερα προσιτά επίπεδα και με υψηλή ακρίβεια.
- Εντούτοις, υφίσταται κίνδυνος πλαστοπροσωπίας, ιδιαίτερα αν δεν εφαρμοστούν προχωρημένες τεχνικές liveness detection.

2. Αναγνώριση Προσώπου:

- Προσφέρει υψηλή χρηστικότητα και ταχύτητα χρήσης, ιδιαίτερα αν αξιοποιούνται 3D αισθητήρες ή υπέρυθρες κάμερες, αλλά επιφέρει σοβαρές ηθικές και νομικές προκλήσεις σχετικά με την ιδιωτικότητα (π.χ. μαζική επιτήρηση).
- Η αποτελεσματικότητα εξαρτάται από τον φωτισμό, την ποιότητα της κάμερας και την ύπαρξη 3D αισθητήρων (που μειώνουν τις επιθέσεις πλαστογράφησης με φωτογραφίες ή βίντεο) και την εφαρμογή τεχνικών βελτίωσης εικόνας (που μετριάζουν την χαμηλή ποιότητα απεικόνισης).

3. Αναγνώριση Ίριδας και Αμφιβληστροειδούς:

- Θεωρούνται από τις πλέον ακριβείς και ασφαλείς μεθόδους λόγω της μοναδικότητας των προτύπων του ματιού, αλλά παρουσιάζουν περιορισμένη εμπορική χρήση διότι απαιτούν υψηλής ακρίβειας και κόστους εξοπλισμό και συχνά θεωρούνται περισσότερο «παρεμβατικές».
- Η ανάγκη στενής συνεργασίας του χρήστη και η ψυχολογική αντίσταση που εκφράζεται από ορισμένους για «σάρωση ματιών» αποτελεί επιπλέον φραγμό στην ενσωμάτωσή τους σε ευρεία κλίμακα.

4. Αναγνώριση Φωνής:

- Είναι κατάλληλη προς χρήση για απομακρυσμένες εφαρμογές (π.χ. τηλεφωνικά κέντρα) ή σε περιπτώσεις όπου η αλληλεπίδραση είναι φωνητική (assistants), όμως επηρεάζεται σημαντικά από θορύβους περιβάλλοντος και αλλοιώσεις στη φωνή (π.χ. λόγω ασθένειας).
- Λόγω του ότι δεν υπάρχει ανθεκτικότητα σε επιθέσεις αναπαραγωγής (playback), σε μεγάλο βαθμό θεωρείται μέθοδος που απαιτεί συμπληρωματική ασφάλεια, οπότε δεν μπορεί να χρησιμοποιηθεί ως ανεξάρτητος μηχανισμός αυθεντικοποίησης σε κρίσιμες εφαρμογές.

5. Δυναμική Πληκτρολόγηση, Αναγνώριση Βάδισης:

- Προσφέρουν μια «διαρκή» ή «αθόρυβη» επιτήρηση της ταυτότητας, δίχως να απαιτείται συνειδητή συμμετοχή του χρήστη.
- Παρουσιάζουν ωστόσο χαμηλότερη ακρίβεια συγκριτικά με τα φυσιολογικά χαρακτηριστικά (όπως δακτυλικά αποτυπώματα ή ίριδα), ενώ υποκύπτουν σε διακυμάνσεις λόγω ψυχοσωματικών παραμέτρων.

6. Αναγνώριση Υπογραφής:

- Νομικά και κοινωνικά καθιερωμένη μέθοδος με υψηλή αποδοχή από τους χρήστες.
- Παρουσιάζει μέτρια ακρίβεια, και επηρεάζεται από φυσικούς ή ψυχολογικούς παράγοντες.

7. Αναγνώριση Παλαμιαίων Αγγείων:

- Είναι εξαιρετικά δύσκολη η πλαστογράφηση.
- Απαιτεί ειδικό εξοπλισμό με σημαντικό κόστος καθώς και εξοικείωση για σωστή τοποθέτηση της παλάμης.

8. Πολυτροπικά Συστήματα:

- Συνιστούν μια ιδιαίτερα αξιόλογη στρατηγική αύξησης της ακρίβειας και της ασφάλειας, καθώς ενώνουν διαφορετικά βιομετρικά χαρακτηριστικά, καθιστώντας την πλαστογράφηση πολύ πιο δύσκολη.
- Εντούτοις, συνεπάγονται υψηλότερο κόστος και πολύπλοκες απαιτήσεις συντήρησης σε σχέση με τις μεμονωμένες μεθόδους, ενώ επιφέρουν και επιπρόσθετες ανησυχίες για την προστασία ιδιωτικότητας, αφού συλλέγονται και επεξεργάζονται πολλαπλά στοιχεία για τον ίδιο χρήστη.

Η διεξοδική σύγκριση αυτών των μεθόδων καθιστά σαφή τη διαπίστωση ότι κάθε τεχνολογία έχει τον δικό της ρόλο, τις δικές της «αγορές στόχου» και το δικό της βέλτιστο πεδίο εφαρμογής. Δεν θα είχε νόημα μια τράπεζα να βασίσει εξ ολοκλήρου τις συναλλαγές της μόνο στην αναγνώριση βάδισης ή στον έλεγχο φωνής, όπως επίσης δεν είναι ιδανικό να χρησιμοποιείται αναγνώριση αμφιβληστροειδούς για μια απλή είσοδο σε λογαριασμό email.

5.3 Η Εμπλοκή της Βιομηχανίας και των Κυβερνήσεων

Όπως κάθε τεχνολογικό πεδίο που επηρεάζει καθολικά τη λειτουργία της οικονομίας, η εξέλιξη των βιομετρικών δεν εξαρτάται μόνο από τα πανεπιστήμια ή τα ερευνητικά κέντρα, αλλά εμπλέκονται σε αυτό ενεργά οι εταιρείες τεχνολογίας, οι πάροχοι υπηρεσιών (finance, healthcare, security, telecom, κ.ά.) και οι κυβερνήσεις που χρηματοδοτούν έργα και νομοθετούν τους όρους χρήσης. Στο πλαίσιο αυτό, διαφαίνεται μια κοινή τάση:

- Οι μεγάλες πολυεθνικές (Big Tech) επενδύουν πολλούς πόρους σε έρευνα και ανάπτυξη (R&D) γύρω από την αναγνώριση προσώπου, την ανάλυση φωνής, τους αλγορίθμους ΑΙ για βελτίωση της εμπειρίας χρήστη, κ.λπ. Παράλληλα, όμως, έρχονται συχνά αντιμέτωπες με επικρίσεις για «επεκτατισμό» (surveillance capitalism - καπιταλισμός παρακολούθησης), δεδομένου ότι μπορεί να συγκεντρώνουν τεράστιες βάσεις δεδομένων από δισεκατομμύρια χρήστες παγκοσμίως.
- Οι κυβερνήσεις, από την πλευρά τους, προωθούν την ενσωμάτωση βιομετρικών συστημάτων σε εθνικά μητρώα πολιτών (e-ID cards, e-passports), ενώ παράλληλα προσπαθούν να βρουν μια ισορροπία ανάμεσα στη διασφάλιση της ασφάλειας των συνόρων και την προστασία των ελευθεριών των πολιτών.
- Ο τραπεζικός και ασφαλιστικός τομέας πρωτοστατεί στην υιοθέτηση βιομετρικών λύσεων, ειδικά για την επαλήθευση πελατών σε ηλεκτρονικές συναλλαγές, προσπαθώντας να μειώσει την απάτη και να βελτιώσει την εμπειρία των πελατών. Στην ίδια κατεύθυνση, εταιρείες fintech και startups καινοτομούν, προτείνοντας πολυτροπικά μοντέλα ελέγχου ταυτότητας ή καθιστώντας δυνατή την εξ αποστάσεως δημιουργία λογαριασμών (e-KYC) με βιομετρικό έλεγχο.
- Ο τομέας της υγείας (νοσοκομεία, κλινικές, φαρμακευτικές) εκδηλώνει επίσης ενδιαφέρον, είτε για την ασφαλή αυθεντικοποίηση ασθενών (ώστε να αποφευχθούν ιατρικά λάθη και διπλές εγγραφές) είτε για την παροχή εξ αποστάσεως ιατρικών υπηρεσιών (τηλεϊατρική), όπου η επαλήθευση της ταυτότητας του ασθενούς αποτελεί κρίσιμο παράγοντα.

Συνεπώς, καθίσταται σαφές ότι η βιομετρική αυθεντικοποίηση έχει διεισδύσει βαθιά σε πολλαπλούς κλάδους της οικονομίας και της κοινωνίας. Η ορθή αξιοποίηση και η βιώσιμη ανάπτυξή της προϋποθέτουν τη συνεργασία μεταξύ διαφορετικών ενδιαφερομένων μερών, καθώς και μια αλληλοτροφοδοτούμενη σχέση μεταξύ αγοράς, έρευνας και κράτους.

5.4 Ζητήματα Προστασίας Δεδομένων και Ιδιωτικότητας

Ένα από τα κρίσιμότερα θέματα που αναδεικνύεται από την έρευνα και απασχολεί τον ακαδημαϊκό και τον επαγγελματικό χώρο αφορά την προστασία των βιομετρικών δεδομένων. Δεδομένου ότι τα συγκεκριμένα δεδομένα (π.χ. δακτυλικό αποτύπωμα, μοτίβο ίριδας, φωνή, πρόσωπο) αφορούν μοναδικές βιολογικές ιδιότητες ενός ατόμου, η κλοπή ή η μη εξουσιοδοτημένη πρόσβαση σε αυτά τα δεδομένα μπορεί να έχει μακροπρόθεσμες επιπτώσεις που υπερβαίνουν κατά πολύ μια απλή διαρροή κωδικού πρόσβασης. Εάν ο κωδικός πρόσβασης διαρρεύσει, μπορεί να αλλάξει. Ωστόσο, τα φυσιολογικά χαρακτηριστικά του ατόμου, όπως τα δακτυλικά αποτυπώματα ή η ίριδα, δεν

μπορούν να τροποποιηθούν. Αυτό σημαίνει ότι μια παραβίαση σε βιομετρικά δεδομένα μπορεί να είναι δυνητικά μη αναστρέψιμη.

Οι νομικές και θεσμικές προεκτάσεις είναι εξίσου σύνθετες. Η Ευρωπαϊκή Ένωση, για παράδειγμα, μέσω του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), θέτει αυστηρούς όρους για τη συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων, στα οποία συμπεριλαμβάνονται τα βιομετρικά. Κάθε φορέας που εφαρμόζει βιομετρικά συστήματα καλείται να υιοθετήσει ειδικά μέτρα ασφαλείας, όπως η κρυπτογράφηση, η αποφυγή καταγραφής των ωμών βιομετρικών δεδομένων (raw data), και η χρήση των λεγόμενων «βιομετρικών προτύπων», τα οποία είναι μη αναστρέψιμες (non-reversible) παραστατικές αναπαραστάσεις του πραγματικού βιομετρικού χαρακτηριστικού, αντί για τις ίδιες τις εικόνες ή τους πλήρεις ήχους, χρησιμοποιώντας αλγόριθμους εξαγωγής χαρακτηριστικών ώστε να παραχθούν τα βιομετρικά πρότυπα.

Επιπλέον, η αρχή της ελαχιστοποίησης δεδομένων επιτάσσει τη συλλογή όσο το δυνατόν λιγότερων και αυστηρά αναγκαίων βιομετρικών στοιχείων, προκειμένου να διασφαλίζεται η αναλογικότητα της όλης διαδικασίας κάτι που ωστόσο μπορεί να εγείρει προκλήσεις στα πολυτροπικά βιομετρικά συστήματα. Σε αυτό το σημείο, η σύγκριση διαφόρων μεθόδων μπορεί να λάβει υπόψη τον βαθμό κινδύνου που ενέχει η συλλογή συγκεκριμένου είδους βιομετρικών: παραδείγματος χάρη, μια φορητή συσκευή που αποθηκεύει το δακτυλικό αποτύπωμα τοπικά (και δεν το στέλνει σε απομακρυσμένο διακομιστή) θέτει μικρότερο κίνδυνο διαρροής (πολλών βιομετρικών δεδομένων) σε σύγκριση με μια κεντρική βάση δεδομένων που συνδυάζει εκατομμύρια αποτυπώματα ή αναπαραστάσεις προσώπων.

Η ηθική διάσταση της ευρείας χρήσης βιομετρικών συστημάτων, ειδικότερα σε δημόσιους χώρους ή σε εφαρμογές επιτήρησης, εμπλέκει προβληματισμούς σχετικά με τη λεγόμενη «κοινωνία επιτήρησης» (surveillance society) και την πιθανή διεύρυνση μιας «υπόνοιας αστυνόμευσης». Οι υποστηρικτές τέτοιων τεχνολογιών προτάσσουν επιχειρήματα για αυξημένη ασφάλεια, ταχεία αναγνώριση ατόμων υπόπτων ή καταζητούμενων, αποφυγή τρομοκρατικών ενεργειών κ.λπ., ενώ οι επικριτές εστιάζουν στη διακινδύνευση της ανωνυμίας, της ελεύθερης μετακίνησης και της δημοκρατίας. Αυτό το πεδίο είναι εξαιρετικά νευραλγικό, καλώντας τους επιστήμονες και τους πολιτικούς ιθύνοντες να αναπτύξουν ρυθμιστικά πλαίσια που θα εξασφαλίζουν τη νομιμότητα, τη διαφάνεια και την αναγκαιότητα της οποιασδήποτε χρήσης βιομετρικών μεθόδων.

5.5 Τεχνολογικές Τάσεις και Προκλήσεις

Η αλματώδης ανάπτυξη του υπολογιστικού νέφους (cloud computing), σε συνδυασμό με την ευρεία διάδοση των αλγορίθμων βαθιάς μάθησης (deep learning), ανοίγει δρόμους για σημαντικές βελτιώσεις στην ακρίβεια και την ταχύτητα των βιομετρικών συστημάτων. Η δυνατότητα επεξεργασίας τεράστιων όγκων δεδομένων, σε συνδυασμό με εξελιγμένες τεχνικές νευρωνικών δικτύων (π.χ. CNN, RNN, Transformer-based μοντέλα) βελτιώνει την ικανότητα εντοπισμού λεπτομερειών και χαρακτηριστικών, ακόμη και σε δύσκολες συνθήκες (π.χ. κακός φωτισμός, θόρυβος, κομμάτια του προσώπου κρυμμένα από μάσκες ή γυαλιά, αλλοίωση φωνής λόγω κρούς κ.ά.).

Ωστόσο, η ίδια η τεχνητή νοημοσύνη και ειδικότερα οι τεχνικές, όπως τα Generative Adversarial Networks (GANs), δημιουργούν νέες απειλές πλαστοπροσωπίας. Για παράδειγμα,

deepfake βίντεο που αναπαριστούν το πρόσωπο ενός ατόμου να λέει ή να κάνει πράγματα που στην πραγματικότητα δεν έχει πει ή κάνει, μπορούν να χρησιμοποιηθούν ως πρώτης τάξεως επιθέσεις για συστήματα αναγνώρισης προσώπου. Ομοίως, η συνθετική φωνή (speech synthesis) επιτρέπει την εντυπωσιακά ρεαλιστική αναπαραγωγή της φωνής ενός ατόμου, γεγονός που επηρεάζει αρνητικά την ασφάλεια των συστημάτων αναγνώρισης φωνής. Επομένως, η συνεχής «κούρσα εξοπλισμών» μεταξύ των αμυντικών τεχνολογιών (π.χ. liveness detection, εντοπισμός deepfake) και των επιτιθέμενων αναμένεται να κλιμακωθεί στο άμεσο μέλλον.

Ένα άλλο κομβικό σημείο είναι η ενσωμάτωση βιομετρικών μεθόδων σε φορητές και «φορετές» (wearable) συσκευές. Η αύξηση των δυνατοτήτων επεξεργασίας σε smartphones, smartwatches και IoT συσκευές επιτρέπει τη δημιουργία πολυτροπικών συστημάτων αναγνώρισης (π.χ. συνδυασμός καρδιακού ρυθμού, βηματισμού, προσώπου και φωνής) σε ατομικό επίπεδο, διατηρώντας τα δεδομένα στην ίδια τη συσκευή, χωρίς απαραίτητα να αποστέλλονται σε κεντρικούς διακομιστές. Αυτή η προσέγγιση επιτρέπει τον λεγόμενο «edge computing» (υπολογισμό στην ακμή του δικτύου) ή την λεγόμενη «on-device AI» (TN στην συσκευή), μειώνοντας τους κινδύνους διαρροής σε κεντρικές υποδομές, αλλά ταυτόχρονα εγείρει θέματα σχετιζόμενα με την ασφάλεια της ίδιας της συσκευής και την ενεργειακή της κατανάλωση.

5.6 Ηθικοί και Νομικοί Προβληματισμοί: Αναγκαία Βήματα Ρύθμισης

Η συζήτηση για τα βιομετρικά συστήματα δεν μπορεί να είναι μονοδιάστατη, περιοριζόμενη αποκλειστικά σε τεχνολογικές αναλύσεις. Οι πτυχές που άπτονται των ατομικών δικαιωμάτων, της εμπιστοσύνης του κοινού και της πιθανότητας κατάχρησης δεδομένων παραμένουν στο επίκεντρο. Κάθε φορά που προωθείται η χρήση κάποιας νέας εφαρμογής βιομετρικής ταυτοποίησης, είναι απαραίτητο να συνεκτιμώνται τα εξής:

Η Αρχή της Νομιμότητας: Η συλλογή και επεξεργασία βιομετρικών δεδομένων πρέπει να έχει σαφή νομική βάση. Στην Ε.Ε., αυτή η βάση έχει σχέση τόσο με τον GDPR, όσο και με εθνικές νομοθεσίες. Στο ίδιο πλαίσιο, απαιτείται η θέσπιση σαφών όρων για την ενημέρωση των χρηστών, τη συγκατάθεση τους, τη διαχείριση και τον χρόνο αποθήκευσης των δεδομένων.

Η Αρχή της Αναλογικότητας: Η χρήση βιομετρικών συστημάτων οφείλει να ανταποκρίνεται σε πραγματικές ανάγκες και να είναι αναλογική του σκοπού. Εάν π.χ. απαιτείται υψηλή ασφάλεια για ένα στρατιωτικό κέντρο, τότε η εφαρμογή πολύ αυστηρών μεθόδων (όπως αμφιβληστροειδούς ή ίριδας) μπορεί να δικαιολογηθεί. Εάν, όμως, πρόκειται για μια απλή εγγραφή σε ιστοσελίδα, η χρήση υπερεξελιγμένων βιομετρικών συστημάτων ενδέχεται να κριθεί υπερβολική, ασύμφορη και δυσανάλογη.

Διαφάνεια και Λογοδοσία: Οι χρήστες ή οι πολίτες πρέπει να έχουν το δικαίωμα πρόσβασης σε πληροφορίες σχετικά με το ποιες βιομετρικές μέθοδοι χρησιμοποιούνται, σε ποιον ανήκει η υποδομή, πού φυλάσσονται τα δεδομένα και υπό ποιες συνθήκες διαγράφονται ή ανωνυμοποιούνται.

Κυρώσεις και Επιβολή: Η καθιέρωση κυρώσεων για τυχόν παραβιάσεις των όρων χρήσης, η έγκαιρη ενημέρωση των αρμόδιων αρχών (π.χ. αρχή προστασίας δεδομένων προσωπικού χαρακτήρα) σε περίπτωση διαρροής ή επίθεσης, και η ύπαρξη μηχανισμών ελέγχου (audits) είναι

θεμέλιοι λίθοι για την οικοδόμηση εμπιστοσύνης μεταξύ χρηστών και οργανισμών/φορέων που διαχειρίζονται τα βιομετρικά δεδομένα τους.

Η Διεθνής Διάσταση: Δεδομένου ότι οι τεχνολογίες αυτές αναπτύσσονται και εμπορευματοποιούνται από πολυεθνικές εταιρείες ή ερευνητικούς φορείς με διεθνή απήχηση, χρειάζεται διακρατική συνεργασία και εναρμόνιση των ρυθμιστικών πλαισίων. Το διαδίκτυο και οι παγκόσμιες αλυσίδες τροφοδοσίας καθιστούν δύσκολο τον εθνικό έλεγχο. Συνεπώς, δομές όπως η Ευρωπαϊκή Επιτροπή, ο ΟΟΣΑ ή άλλα διεθνή φόρα μπορούν να παίξουν καθοριστικό ρόλο στο να τεθούν βασικοί κανόνες.

5.7 Ερευνητικές Προκλήσεις και Κατευθύνσεις

Με βάση την παραπάνω ανάλυση σχετικών ζητημάτων και προβληματισμών που άπτονται της χρήσης βιομετρικών συστημάτων, αναδύονται ποικίλες ερευνητικές προκλήσεις που θα πρέπει να αντιμετωπιστούν. Οι κυριότερες εστιάζουν στους εξής άξονες:

Βελτίωση Ακρίβειας σε Πραγματικές Συνθήκες: Πολλά συστήματα (π.χ. αναγνώριση προσώπου και αναγνώριση φωνής) επιδεικνύουν εξαιρετικές επιδόσεις σε εργαστηριακό περιβάλλον ή σε ελεγχόμενα σύνολα δεδομένων (datasets) ωστόσο, η υλοποίηση στον πραγματικό κόσμο (με μεταβαλλόμενο φωτισμό, πολυκοσμία, κίνηση, θόρυβο κ.ά.) συχνά συνοδεύεται από δραστική μείωση της ακρίβειας. Χρειάζεται περαιτέρω έρευνα στον τομέα αλγορίθμων συνολικά, τόσο στους αλγόριθμους που χρησιμοποιούνται κατά την διαδικασία απόκτησης και εξαγωγής του βιομετρικού χαρακτηριστικού όσο και στην διαδικασία σύγκρισης, όπου η ανάγκη ύπαρξης στιβαρών αλγορίθμων που να μην “καταρρέουν” υπό υποδεέστερες συνθήκες είναι ξεκάθαρη. Καθώς και απαιτείται η ανάπτυξη ή χρήση αλγορίθμων που ενισχύουν την ποιότητα των δεδομένων, πριν εξαχθούν από αυτά τα βιομετρικά χαρακτηριστικά.

Εντοπισμός και Αναγνώριση Επιθέσεων Πλαστοπροσωπίας σε Βάθος: Με την εξέλιξη των deepfakes, των 3D εκτυπώσεων και της συνθετικής φωνής, ακόμη και πολύ ασφαλείς μέθοδοι (όπως αναγνώριση προσώπου 3D ή ίριδας) μπορεί να γίνουν εκτεθειμένες. Έτσι, οι τεχνικές ανίχνευσης ζωντάνιας (liveness detection) και πιστοποίησης της αυθεντικότητας του δείγματος αποκτούν στρατηγική σημασία, ακόμη περισσότερο για τις πιο ευαίσθητες μεθόδους (όπως αναγνώριση δακτυλικών αποτυπωμάτων). Ο τομέας της αντίπαλης μηχανικής μάθησης (adversarial machine learning) συμπληρωματικά ως προς τις προαναφερόμενες τεχνικές μπορεί να δώσει λύσεις που θα θωρακίζουν τα συστήματα βιομετρικής αναγνώρισης έναντι τέτοιων σχετικών επιθέσεων.

Πολυτροπικά Συστήματα και Έξυπνη Ενοποίηση (Fusion & Hybrid Fusion): Η βέλτιστη αρχιτεκτονική συνδυασμού διαφόρων βιομετρικών πτυχών παραμένει ανοικτό ερευνητικό πεδίο. Ερωτήματα όπως η σειρά συλλογής δεδομένων, ο βαθμός βαρύτητας κάθε βιομετρικού δείκτη, η διαχείριση των σφαλμάτων (π.χ. FAR, FRR) και η χρονική καθυστέρηση χρήσης απασχολούν έντονα τους σχεδιαστές. Παράλληλα, τα πολυτροπικά μοντέλα μπορεί να συνεπάγονται υπέρογκους υπολογιστικούς πόρους, δημιουργώντας ανάγκες για αποτελεσματικούς αλγόριθμους συμπίεσης δεδομένων ή/και αξιοποίησης επιταχυντών υλικού (hardware accelerators) (π.χ. GPUs, TPUs), πάντοτε στα πλαίσια του υπολογιστικού νέφους ή των επεκτάσεών του (π.χ. edge ή fog computing).

Εμπειρία Χρηστών (User Experience) και Κοινωνική Αποδοχή: Παρόλο που η βιομετρική τεχνολογία εστιάζει κατά κύριο λόγο στην ασφάλεια (π.χ. αναγνώριση ίριδας όπου μαζί με την ευχρηστία που βελτιώθηκε με το πέρασμα του χρόνου, βελτιώθηκε και η αποδοχή της), η παράμετρος της ευχρηστίας και της αποδοχής από το κοινό έχει αποδειχθεί καθοριστική για την επιτυχημένη διάδοσή της. Η σχεδίαση διεπαφών που παρέχουν αίσθημα ασφάλειας και ιδιωτικότητας, η ελαχιστοποίηση της παρεμβατικότητας (π.χ. να μη νιώθει ο χρήστης ότι “κατασκοπεύεται”) και η σαφής επικοινωνία σχετικά με τους σκοπούς και τις μεθόδους χρήσης των βιομετρικών αποτελούν καίριες συνιστώσες της έρευνας που αγγίζει τον χώρο της αλληλεπίδρασης ανθρώπου-υπολογιστή (HCI) και της κοινωνιολογίας της τεχνολογίας.

Υπεύθυνη Τεχνητή Νοημοσύνη και Ηθικός Σχεδιασμός (Responsible AI & Ethics by Design): Η ενσωμάτωση ηθικών αρχών από το αρχικό στάδιο σχεδιασμού (EbD) των τεχνολογιών βιομετρικής αυθεντικοποίησης μπορεί να αποτελέσει ένα επιπλέον εργαλείο για την δημιουργία ευρέως κοινωνικά αποδεκτών λύσεων. Επιπλέον, με την αναμενόμενη υιοθέτηση της TN, το Responsible AI μπορεί να ενισχύσει την διαφάνεια που χρειάζονται οι χρήστες για να αισθανθούν ασφάλεια και να ξεπεράσουν τους δισταγμούς τους σχετικά με την χρήση τέτοιου είδους τεχνολογιών.

Διαλειτουργικότητα και Προτυποποίηση (Interoperability & Standardization): Η έλλειψη κοινών διεθνών προτύπων αναμφίβολα αποτελεί μία ερευνητική πρόκληση. Η ανάπτυξη ανοιχτών, ασφαλών και επεκτάσιμων προτύπων που θα βοηθούν την διαλειτουργικότητα και θα διασφαλίζουν την ιδιωτικότητα είναι ένα κρίσιμο βήμα προς την ευρεία εφαρμογή των τεχνολογιών βιομετρικής αυθεντικοποίησης.

Αυτό-Κυρίαρχη Ταυτότητα (Self-Sovereign Identity) και Blockchain Εφαρμογές: Μια ακόμα αναδυόμενη τάση είναι η αποκεντρωμένη ταυτότητα, όπου τα διαπιστευτήρια (credentials) βρίσκονται υπό τον έλεγχο του ίδιου του χρήστη, χωρίς κεντρικά σημεία αποθήκευσης που θα μπορούσαν να γίνουν στόχοι επιθέσεων. Εδώ, τεχνολογίες όπως το blockchain ή παρόμοιες κατακεντρωμένες βάσεις δεδομένων (distributed ledgers) μπορούν να ενισχύσουν την ασφάλεια, την ακεραιότητα και την εμπιστοσύνη στο σύστημα. Η βιομετρική ταυτοποίηση θα μπορούσε να ενσωματωθεί ως ένα κρίσιμο βήμα επικύρωσης της ταυτότητας του χρήστη σε αυτό το πλαίσιο, εξαλείφοντας την ανάγκη να εμπιστευόμαστε έναν κεντρικό πάροχο.

5.8 Συμπερασματική Επισκόπηση και Προοπτικές

Η εκτενής βιβλιογραφία, όπως παρουσιάστηκε και μέσα από τις ερευνητικές εργασίες των Daugman (2004), Rathgeb & Busch (2012), Juels & Sudan (2006), Kumar & Zhang (2007), Sutcu et al. (2007) και πολλών άλλων, αποδεικνύει την πολυπλοκότητα αλλά και τη ραγδαία πρόοδο του πεδίου της βιομετρικής αυθεντικοποίησης. Τα συστήματα αυτά:

- Προσφέρουν βελτιωμένη ασφάλεια σε σύγκριση με τους παραδοσιακούς κωδικούς, εκμεταλλευόμενα τις εγγενείς ιδιαιτερότητες του ανθρώπινου σώματος.
- Απαιτούν ωστόσο ισχυρές δικλίδες ασφαλείας για την προστασία των δεδομένων, καθώς η φύση τους είναι αμετάβλητη και εξαιρετικά ευαίσθητη σε περίπτωση παραβίασης.

- Εμπλουτίζονται με κρυπτογραφία (fuzzy vault, robust hashing) και βρίσκουν εφαρμογή σε νέες περιοχές, όπως το IoT και το blockchain, επεκτείνοντας δραστικά τις δυνατότητες και τις προοπτικές τους.

Ταυτόχρονα, διαφαίνεται ότι οι ερευνητικές τάσεις θα συνεχίσουν να εστιάζουν στη βελτίωση της ακρίβειας και της ανθεκτικότητας (ανίχνευση spoofing, αντιμετώπιση deepfakes), καθώς και στη διασφάλιση της ιδιωτικότητας (συμβατότητα με αυστηρά νομικά πλαίσια και ηθικές προδιαγραφές). Οι λύσεις που αναδύονται πρέπει να ισορροπούν ανάμεσα σε τεχνολογικούς, νομικούς και κοινωνικούς παράγοντες, ώστε να μπορούν να υιοθετηθούν ευρέως και να προσφέρουν πράγματι αυξημένη ασφάλεια στην ψηφιακή εποχή.

Συνοψίζοντας, ο κλάδος της βιομετρικής αυθεντικοποίησης δεν μοιάζει με μια στατική πραγματικότητα, αλλά εξελίσσεται με ταχείς ρυθμούς, αντανακλώντας τις επιταγές της ψηφιακής εποχής και τις μεταβαλλόμενες ανάγκες ασφάλειας. Στην παρούσα εργασία, η συγκριτική προσέγγιση επέτρεψε την ανάδειξη των κρίσιμων χαρακτηριστικών κάθε μεθόδου, οδηγώντας σε συμπεράσματα σχετικά με τις επιδόσεις, τις προκλήσεις και τις εφαρμογές. Ωστόσο, το ίδιο το μέλλον αυτών των τεχνολογιών διαμορφώνεται από πολλούς εξωτερικούς παράγοντες:

Τεχνολογική Πρόοδος: Η εξέλιξη των αισθητήρων και των αλγορίθμων ΑΙ μπορεί να εκτοξεύσει την ακρίβεια ή να επιλύσει ζητήματα που σήμερα φαντάζουν δυσεπίλυτα (π.χ. spoofing). Ταυτόχρονα, όμως, η ίδια πρόοδος δημιουργεί και νέες μορφές απειλών.

Οικονομική Βιωσιμότητα: Καθώς πέφτει το κόστος των αισθητήρων και βελτιώνεται η απόδοση, γίνεται πιο ελκυστική η μαζική ενσωμάτωση βιομετρικών συστημάτων σε εμπορικές εφαρμογές. Από την άλλη, ο ανταγωνισμός μπορεί να ενισχύσει καινοτομίες που διεκδικούν μεγαλύτερη ασφάλεια ή καλύτερη εμπειρία χρήστη, αλλά ταυτόχρονα ελλοχεύει ο κίνδυνος αυτές οι καινοτομίες να παραμείνουν ιδιόκτητες, οδηγώντας σε εξάρτηση από συγκεκριμένους παρόχους (vendor lock-in), κάτι που ενδέχεται να είναι και επικίνδυνο.

Ρυθμιστικό Πλαίσιο και Κοινωνική Αποδοχή: Καμία τεχνολογία δεν μπορεί να αναπτυχθεί εκθετικά χωρίς τη συναίνεση της κοινωνίας και το κατάλληλο νομικό θεμέλιο. Είναι πιθανό να δούμε αυστηρότερες ρυθμίσεις ή ακόμη και απαγορεύσεις για συγκεκριμένες χρήσεις βιομετρικών (π.χ. αναγνώριση προσώπου σε δημόσιους χώρους). Αυτές οι νομοθετικές εξελίξεις θα καθορίσουν τον ρυθμό και την κατεύθυνση ανάπτυξης του κλάδου.

Η Συνύπαρξη με Άλλες Τεχνολογίες: Η σύγκλιση βιομετρικών συστημάτων με blockchain, Internet of Things, Big Data analytics (ανάλυση μεγάλων δεδομένων) και cloud/fog/edge computing είναι ήδη ορατή. Το πώς θα εξελιχθούν αυτές οι αλληλεπιδράσεις θα σημαδέψει τις επόμενες δεκαετίες ως προς το ζήτημα της (βιομετρικής) αυθεντικοποίησης και της διαχείρισης ταυτότητας.

Διαφοροποίηση Αναγκών κατά Κλάδο: Δεν είναι το ίδιο να σχεδιάζεις ένα βιομετρικό σύστημα για τραπεζικές συναλλαγές υψηλής αξίας, όπως για την είσοδο σε ένα εκπαιδευτικό περιβάλλον ή για τη χρήση από μια υπηρεσία delivery. Η εξατομίκευση των λύσεων προς τις ανάγκες κάθε κλάδου σημαίνει ότι ενδέχεται να αναδυθούν περισσότερα συστήματα «κάθετης» εξειδίκευσης παρά ένα ή δύο κυρίαρχα «οριζόντια» συστήματα που εφαρμόζονται παντού. Αν και η καθετοποίηση προσφέρει προσαρμογή και ίσως καλύτερες αποδόσεις μπορεί να οδηγήσει σε κατακερματισμό της αγοράς και αυξημένο κόστος συντήρησης. Το ιδανικό σενάριο θα ήταν μια

ισορροπία, μεταξύ επαρκούς εξειδίκευσης του κάθε κλάδου και ταυτόχρονα χρήσης κοινών προτύπων για διαλειτουργικότητα και επεκτασιμότητα.

Ανοιχτά Πρότυπα και Διαλειτουργικότητα: Οι ιδιόκτητες (proprietary) λύσεις και τα κλειστά οικοσυστήματα (vendor lock-in) μπορεί να περιορίσουν την ανάπτυξη και την καινοτομία. Η ύπαρξη και η προώθηση διεθνών προτύπων, όπως το ISO/IEC 19794 μπορεί να ενισχύσει την ευελιξία και να διασφαλίσει την διαλειτουργικότητα συστημάτων.

5.9 Τελικές Σκέψεις

Ολοκληρώνοντας αυτή τη συζήτηση, καθίσταται σαφές ότι η βιομετρική αυθεντικοποίηση ξεπερνά κατά πολύ το πεδίο της απλής τεχνολογικής καινοτομίας. Αποτελεί τομή που φέρνει μαζί τα πεδία της πληροφορικής, της μηχανικής μάθησης, της βιοϊατρικής, της νομικής επιστήμης, της κοινωνιολογίας και της ηθικής. Το ερώτημα που προκύπτει δεν περιορίζεται στο «πώς θα φτιάξουμε το ασφαλέστερο σύστημα;», αλλά επεκτείνεται στο «ποιοι κίνδυνοι αναλαμβάνονται για την ιδιωτικότητα;», «πόσο διαφανές είναι το σύστημα σε περίπτωση εσφαλμένων ταυτοποιήσεων;», «είναι εφικτό να υπάρξει συναίνεση πολιτών σε μαζική κλίμακα;» και «ποιος φορέας θα έχει την τελική εξουσία και έλεγχο πάνω στα βιομετρικά δεδομένα;».

Οι απαντήσεις σε αυτά τα ερωτήματα δεν είναι μονοσήμαντες και διαφοροποιούνται ανάλογα με το πολιτισμικό, οικονομικό και νομοθετικό πλαίσιο. Σε μέρη του κόσμου όπου η έμφαση στην ατομική ελευθερία και στην προστασία προσωπικών δεδομένων είναι ισχυρότερη, είναι πιθανό να συναντάμε αντιδράσεις σε πρακτικές μαζικής αναγνώρισης προσώπου. Αντίθετα, άλλες γεωγραφικές περιοχές μπορεί να προσπερνούν αυτές τις ανησυχίες ή να θέτουν διαφορετικές προτεραιότητες (π.χ. ασφάλεια και αποτροπή εγκλήματος) και να προωθούν τη βιομετρική τεχνολογία χωρίς σημαντικούς περιορισμούς.

Σε κάθε περίπτωση, η συζήτηση γύρω από τα βιομετρικά δεδομένα, την ασφάλεια και την ιδιωτικότητα μοιάζει με ένα παγκόσμιο εργαστήριο για το πώς ο σύγχρονος πολιτισμός αντιλαμβάνεται την ταυτότητα και την ελευθερία των μελών του. Μια ανοιχτή, διαρκής συνεργασία μεταξύ των ειδικών της πληροφορικής, των νομικών, των φιλοσόφων της τεχνολογίας, αλλά και των φορέων της κοινωνίας πολιτών (ΜΚΟ, ομάδες πολιτών, δημοσιογράφοι) κρίνεται απολύτως απαραίτητη για να διασφαλιστεί ότι οι εξελίξεις θα υπηρετούν το ευρύτερο κοινό συμφέρον, αντί να το εκμεταλλεύονται.

5.10 Επίλογος: Προς μια Ολοκληρωμένη Προσέγγιση

Συγκεντρώνοντας όλα τα προηγούμενα σημεία σε μια καταληκτική παρατήρηση, μπορούμε να πούμε ότι η βιομετρική αυθεντικοποίηση βρίσκεται σε μια φάση «εξωστρεφούς ωρίμανσης». Η τεχνολογία ωριμάζει, οι αγορές την αποδέχονται, τα κόστη μειώνονται, η ακαδημαϊκή έρευνα συνεχίζει να παράγει καινοτομία, και τα ρυθμιστικά πλαίσια δοκιμάζουν να αντιμετωπίσουν τις κοινωνικοπολιτικές προκλήσεις που προκύπτουν. Ταυτόχρονα, καμία από τις επιμέρους μεθόδους (αυθεντικοποίησης) δεν φαίνεται να είναι ικανή από μόνη της να κυριαρχήσει σε όλα τα επίπεδα χρήσης, καθώς οι απαιτήσεις διαφέρουν άρδην από πλαίσιο σε πλαίσιο και από κλάδο σε κλάδο.

Η πιο πιθανή έκβαση, λοιπόν, για το εγγύς μέλλον είναι η άνθηση ευέλικτων και πολυτροπικών λύσεων που θα επιτρέπουν στο εκάστοτε σύστημα να επιλέγει την καλύτερη μέθοδο ανάλογα με το είδος της εφαρμογής ή να «συνθέτει» πολλαπλές μεθόδους όταν απαιτείται υψηλότερο επίπεδο ακρίβειας για την ταυτότητα ενός χρήστη. Παράλληλα, η ευαισθητοποίηση των πολιτών αλλά και των οργανισμών για τις επιπτώσεις σε επίπεδο ιδιωτικότητας θα ωθεί προς την υιοθέτηση πιο «φειδωλών» ή αποκεντρωμένων μοντέλων συλλογής βιομετρικών, όπου δεν θα αποθηκεύονται σε κεντρικούς διακομιστές ή δεν θα χρησιμοποιούνται για συνεχή και αδιάκριτη παρακολούθηση.

Η ερευνητική κοινότητα αναμένεται να ενισχύσει τη συμβολή της μέσα από την ανάπτυξη νέων τεχνικών, την αποκάλυψη τρωτών σημείων και την βελτίωση της αξιοπιστίας και της απόδοσης σε πραγματικά περιβάλλοντα μέσω του σχεδιασμού αποτελεσματικότερων αλγορίθμων. Η συνεργασία μεταξύ δημοσίου τομέα, ιδιωτικών εταιρειών και πανεπιστημιακών/ερευνητικών κέντρων μπορεί να αποτελέσει τον καταλύτη για υπεύθυνη και βιώσιμη πρόοδο. Σε αυτό το σημείο έγκειται η μεγάλη προοπτική της επόμενης δεκαετίας: το πώς θα χτιστεί εμπιστοσύνη γύρω από τις βιομετρικές τεχνολογίες, ώστε να μεγιστοποιηθεί το συλλογικό όφελος και να ελαχιστοποιηθούν οι κίνδυνοι.

Κλείνοντας, οφείλουμε να τονίσουμε ότι η βιομετρική αυθεντικοποίηση δεν αποτελεί μόνο τεχνολογική καινοτομία, αλλά και κομβικό στοιχείο ενός ευρύτερου ψηφιακού οικοσυστήματος που περιλαμβάνει την κυβερνοασφάλεια, τα μεγάλα δεδομένα (big data), την τεχνητή νοημοσύνη και τις αναδυόμενες τεχνολογίες. Η επόμενη φάση της τεχνολογικής εξέλιξης αναπόφευκτα θα βασιστεί σε ακόμη στενότερη σχέση μεταξύ του φυσικού και του ψηφιακού «εαυτού» των ανθρώπων. Ως εκ τούτου, η επιτυχημένη ανάπτυξη βιομετρικών συστημάτων καλείται να καθοδηγείται από ένα «ήθος καινοτομίας» που θα λαμβάνει σοβαρά υπόψη το δημόσιο συμφέρον, τα ανθρώπινα δικαιώματα και την προάσπιση της ανθρώπινης αξιοπρέπειας.

Η συζήτηση, επομένως, για τα βιομετρικά συστήματα θα παραμείνει ζωντανή και επίκαιρη. Μέσα στα επόμενα χρόνια, νέα επιτεύγματα θα οδηγήσουν σε πιο σύνθετες μορφές (πολυτροπικής) αναγνώρισης, όπως η συνδυαστική ανάλυση πολλαπλών φυσιολογικών και συμπεριφορικών δεδομένων σε πραγματικό χρόνο (continuous authentication). Η βαθιά ενσωμάτωση αισθητήρων σε έξυπνα περιβάλλοντα—οχήματα, κατοικίες, δημόσιες υποδομές—θα δώσει τη δυνατότητα για αυτόματη ανίχνευση κινδύνων, διάγνωση παθήσεων ή πρόγνωση ατυχημάτων, εμπλέκοντας όμως ακόμα περισσότερα προσωπικά δεδομένα. Έτσι, η ανάγκη για νέες, εξελιγμένες μορφές κρυπτογραφίας, αποκέντρωσης και ελέγχου των δεδομένων δεν θα είναι απλώς επιθυμία, αλλά επιτακτική απαίτηση.

Σε τελική ανάλυση, οι εξελίξεις στον χώρο της βιομετρικής αναγνώρισης όχι μόνο αντικατοπτρίζουν τη δυναμική της τεχνολογικής προόδου, αλλά και διαμορφώνουν την αντίληψή μας για την ανθρώπινη ταυτότητα, την κοινωνική οργάνωση και την ηθική της ψηφιακής εποχής. Εναπόκειται σε όλους τους εμπλεκόμενους—από τον τελικό χρήστη και τον σχεδιαστή λογισμικού μέχρι τον νομοθέτη και τον ερευνητή—να διασφαλίσουν ότι η μετάβαση σε ένα πιο βιομετρικό μέλλον θα πραγματοποιηθεί με όρους ασφάλειας, αξιοπιστίας, σεβασμού και ανοιχτού διαλόγου. Μόνο έτσι θα εκπληρωθεί η υπόσχεση των βιομετρικών τεχνολογιών ως θεμέλιου λίθου για μια καλύτερη και πιο εξατομικευμένη εμπειρία στον ψηφιακό κόσμο, χωρίς να διακυβεύονται θεμελιώδεις αρχές της ανθρώπινης ελευθερίας.

Βιβλιογραφία

- Akhtar, N., & Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: A survey. *Ieee Access*, 6, 14410-14430.
- Atrey, P. K., Hossain, M. A., El Saddik, A., & Kankanhalli, M. S. (2010). Multimodal fusion for multimedia analysis: a survey. *Multimedia systems*, 16, 345-379.
- Bahmani, K., Plesh, R., Johnson, P., Schuckers, S., & Swyka, T. (2021, September). High fidelity fingerprint generation: Quality, uniqueness, and privacy. In *2021 IEEE International Conference on Image Processing (ICIP)* (pp. 3018-3022). IEEE.
- Blanz, V., & Vetter, T. (2003). Face recognition based on fitting a 3D morphable model. *IEEE Transactions on pattern analysis and machine intelligence*, 25(9), 1063-1074.
- Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). *Guide to Biometrics*. Springer.
- Boulgouris, N. V., Plataniotis, K. N., & Micheli-Tzanakou, E. (Eds.). (2009). *Biometrics: Theory, Methods, and Applications*. Wiley-IEEE Press.
- Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008). Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding*, 110(2), 281-307.
- Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21-30.
- Dhanasekar, N. S., Raghavendra, R., Raja, K. B., & Busch, C. (2018). Multimodal biometric systems: A comparative analysis. In *2018 International Conference on Biometrics (ICB)* (pp. 1-8). IEEE.
- Dharavath, K., Talukdar, F. A., & Laskar, R. H. (2013, December). Study on biometric authentication systems, challenges and future trends: A review. In *2013 IEEE international conference on computational intelligence and computing research* (pp. 1-7). IEEE.
- European Parliament and Council. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2)*. Consolidated version 17/01/2025. Official Journal of the European Union.
- European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*.
- Hesham Rakha, & Selmán, A. A. (2018). Liveness detection for biometric authentication systems. *Computers & Security*, 78, 355-366.
- International Biometric Group (IBG). (2012). *Biometric Market and Industry Report*.
- International Organization for Standardization. (2021). *ISO/IEC 19794-7:2021 – Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data*. International Organization for Standardization.
- International Organization for Standardization. (2011). *ISO/IEC 24745:2011 – Information technology – Security techniques – Biometric information protection*. International Organization for Standardization.

- International Organization for Standardization. (2016). *ISO/IEC 30107-1:2016 – Information technology – Biometric presentation attack detection – Part 1: Framework*. International Organization for Standardization.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), 4-20.
- Jain, A. K., & Ross, A. (2004). *Multibiometric systems*. *Communications of the ACM*, 47(1), 34.
- Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). *Handbook of Biometrics*. Springer.
- Jain, A. K., Feng, J., & Ross, A. (2009). Fingerprints at a distance: Challenges and opportunities. *IEEE Systems Journal*, 3(4), 486–494.
- Johnson, P. A., Tan, B., & Schuckers, S. (2010, December). Multimodal fusion vulnerability to non-zero effort (spoof) imposters. In *2010 IEEE International Workshop on Information Forensics and Security* (pp. 1-5). IEEE.
- Johnson, P., & Schuckers, S. (2016). Fingerprint Spoofing and Liveness Detection. *Forensic Science: A Multidisciplinary Approach*, 373-382.
- Joshi, P., Rathore, M. M., Park, J. H., & Bhan, V. (2018). A biometrics based novel key generation and distribution scheme for smart grid communication. *IEEE Access*, 6, 30276–30284.
- Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2), 237-257.
- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82, 395-411.
- Kim, S. K., Yeun, C. Y., & Yoo, P. D. (2019). An enhanced machine learning-based biometric authentication system using RR-interval framed electrocardiograms. *IEEE Access*, 7, 168669-168674.
- Ko, K. (2007). *User's guide to NIST biometric image software (NBIS) (NIST Interagency/Internal Report No. 7392)*. National Institute of Standards and Technology.
- Kumar, A., & Zhang, D. (2007). Hand-geometry recognition using entropy-based discretization. *IEEE Transactions on information forensics and security*, 2(2), 181-187.
- Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). FVC2000: Fingerprint verification competition. *IEEE transactions on pattern analysis and machine intelligence*, 24(3), 402-412.
- Maltoni, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. Springer.
- Mhenni, A., Rosenberger, C., Cherrier, E., & Amara, N. (2016). Keystroke template update with adapted thresholds. 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), 483-488.
- Muda, L., Begam, M., & Elamvazuthi, I. (2010). Voice recognition algorithms using mel frequency cepstral coefficient (MFCC) and dynamic time warping (DTW) techniques.
- Parkhi, O., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In *BMVC 2015-Proceedings of the British Machine Vision Conference 2015*. British Machine Vision Association.
- Plesh, R., Bahmani, K., Jang, G., Yambay, D., Brownlee, K., Swyka, T., ... & Schuckers, S. (2019, June). Fingerprint presentation attack detection utilizing time-series, color fingerprint captures. In *2019 International Conference on Biometrics (ICB)* (pp. 1-8). IEEE.
- Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2), 33–42.

- Quinn, G. W., Quinn, G. W., Grother, P., & Matey, J. (2018). *IREX IX part one: Performance of Iris recognition algorithms*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
- Rathgeb, C. & Busch, C. (2012). Multi-biometric template protection: Issues and challenges. *Springer*.
- Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 815-823).
- Sun, Y., Liu, J., Wang, J., Cao, Y., & Kato, N. (2020). When machine learning meets privacy in 6G: A survey. *IEEE Communications Surveys & Tutorials*, 22(4), 2694-2724.
- Sutcu, Y., Sencar, H. T., & Memon, N. (2005, August). A secure biometric authentication scheme based on robust hashing. In *Proceedings of the 7th Workshop on Multimedia and Security* (pp. 111-116).
- Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6), 948-960.
- Yang, J. &. (2010). Internet of Things security: Biometric-authentication based system for data access. *IEEE Transactions on Consumer Electronics*, 2710-2718.
- Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2005). *Biometric systems: Technology, design and performance evaluation*. Springer Science & Business Media.
- Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics: Identity Assurance in the Information Age*. McGraw-Hill Osborne Media.
- Zhang, L., Tan, S., & Yang, J. (2017, October). Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 57-71).