A XIX-a Conferinţă internaţională – multidisciplinară
„Profesorul Dorin PAVEL – fondatorul hidroenergeticii româneşti”,
CLUJ NAPOCA, 2019

HUMAN BIOMETRICS AND BIOMETRIC RECOGNITION SYSTEMS; AN OVERVIEW

Ahmed AK. TAHIR, Steluța ANGHELUȘ

BIOMETRICA UMANĂ ȘI SISTEMELE DE RECUNOȘTERI BIOMETRICE; O IMAGINE DE ANSAMBLU

Biometric technology is gaining a significant role in presenting the solutions for many issues in various applications that demands person identification such as forensic science, security, finance affairs, border checking and government ministries and offices. It is defined as the technology of analyzing physiological and behavioral traits such as face, fingerprint, iris, retina, voice, and signature etc., for person identification and authorization. Nowadays, lots of research works are carrying out to accomplish biometric recognition systems based on various types of human traits. To provide a comprehensive survey, this paper presents an overview to five biometric traits (iris, fingerprints, face, voice and signature). The overview will cover the way of acquisition, application area, methods of implementation, strength/weakness, and system evaluation.

Keywords: Biometrics, Biometric Recognition System, iris, Fingerprints, Finger Vein, Palm Vein, Face Recognition, Gait Recognition, Human Traits, Voice Recognition, Signature Recognition

Cuvinte cheie: Biometrie, Sistem de recunoaștere biometrică, iris, amprente, vene de deget, vena palmei, recunoaștere a feței, recunoaștere a trecerii, trăsături umane, recunoaștere vocală, recunoaștere semnătură

Tehnologia biometrică câștigă un rol semnificativ în prezentarea soluțiilor pentru numeroase probleme din diferite aplicații care necesită identificarea persoanelor, cum ar fi știința criminalistică, securitatea, afacerile finanțelor, verificarea frontierelor și ministerele și birourile guvernamentale. Este definită ca tehnologia de analiză a trăsăturilor fiziologice și comportamentale,

cum ar fi fața, amprenta, irisul, retina, vocea și semnătura etc., pentru identificarea și autorizarea persoanei. În prezent, multe lucrări de cercetare sunt realizate pentru a obține sisteme de recunoaștere biometrică bazate pe diverse tipuri de trăsături umane. Pentru a furniza un sondaj cuprinzător, acest articol prezintă o imagine de ansamblu asupra a cinci trăsături biometrice (iris, amprente digitale, față, voce și semnătură). Prezentarea generală va acoperi modul de achiziție, zona de aplicare, metodele de implementare, puterea/ slăbiciunea și evaluarea sistemului.

1. Introduction

The term biometric refers to any human physiological or behavioral traits that are measurable and stable over time such as face, retina, fingerprints, finger vein, ear, palm vein, iris, voice, gait, keystroke, signature etc., [1-3].

Nowadays, Human biometric traits represent the main basis of the security systems and became the solution in many civilian and governmental applications such as finance jobs, border checking and government ministries and offices.

Biometric recognition systems have several advantages over the knowledge-based systems which use PIN code, user name and passwords or token-based systems which use key, magnetic or smart card and badge, [4, 5]. They are based upon features and properties that cannot be forgotten, stolen, shared, changed, lost or disclosed. However, biometric recognition systems are costly and require sophisticated and automated methods to identify and authenticate the person as such. In addition, they require measurements of physiological or behavioral characteristics that are present with the persons. Moreover, they require continuous developments to fulfill the society's demands namely in the fields of e-government, e-banking and e-commerce and to prevent fraudulent persons to pass and break the law, [6].

Biometric identification systems are usually designed either for identification or verification or both. In the identification system, which is referred to as one-to-many matching (*Who the person is*?), sample of individual biometric feature(s) is compared to a list of samples in the database in order to be sure that the individual is in the list. In the verification system, which is referred to as one-to-one matching, the checking operation is performed to conform whether a person is really who he\she claim, (*Is the person is really what he claims?*), [7].

The success of biometric recognition system depends on the strength of the biometric trait and the purpose for which it is designed.

Several studies for comparing the performance of various types of biometric recognition systems have already been carried out. For instance, [1, 3, 5, 7, 8, 9, 10] compared various types of human traits including iris, fingerprints, face, palm vein, voice, gait, ear, signature, DNA, retina, etc. They concluded that the performance of the trait depends on the application area, the cost and how easy it is recorded.

This paper presents an overview over the use of human biometrics for person identification. Five human traits are selected, three physiological traits (iris, fingerprints and face) and two behavioral traits (voice and signature).

2. Biometric Measurements. Characteristics

There are many traits in the human body that can be considered biometric measurements. According to [11, 12] there are seven criteria (pillars) that must be available in the traits in order to be used biometric measurements. These seven pillars are:

1. Universality: Each person should possess the same physiological traits such as fingers, iris, face, etc., and the same behavior traits such as voice, gait, signature, etc.
2. Distinctiveness: The trait must be unique enough to distinguish the person.
3. Permanence: The traits must be stable throughout a person's life.
4. Collectability: Biometric trait should be measured quantitatively and easily.
5. Performance: The trait must provide high recognition accuracy.
6. Acceptability: The way of acquiring of the traits must be accepted by the people. Usually the people prefer to record the train in a non-invasive way.
7. Resistance to Circumvention: The system needs to be hard for any circumvent by fraudulent methods in order to provide efficient security.

The strength of any biometric trait depends to a great extent on the application for which it is used [10, 13]. For instance, some applications may accept some error rate such as highway tolls, whereas others may not such as banking system and criminal investigations. Besides, some application may require quick decision such as border controlling, whereas others may not such as criminal investigation. Table

(1) shows comparisons between five biometric traits (iris, fingerprints, face, voice and signature).

Table 1. Comparisons of biometric traits

Criteria (Pillars) / Biometric Trait	Universality	Permanence	Distinctiveness	Collectivity	Performance	Acceptability	Circumvention
Iris	H	H	H	M	H	M	H
Fingerprints	M	H	H	M	H	M	M
Face	H	L	M	H	L	M	M
Voice	M	M	M	H	M	H	H
Signature	M	L	L	H	L	H	H

3. Biometric System Stages

The components (stages) and implementation of any biometrics system can be represented by the diagram in figure 1.

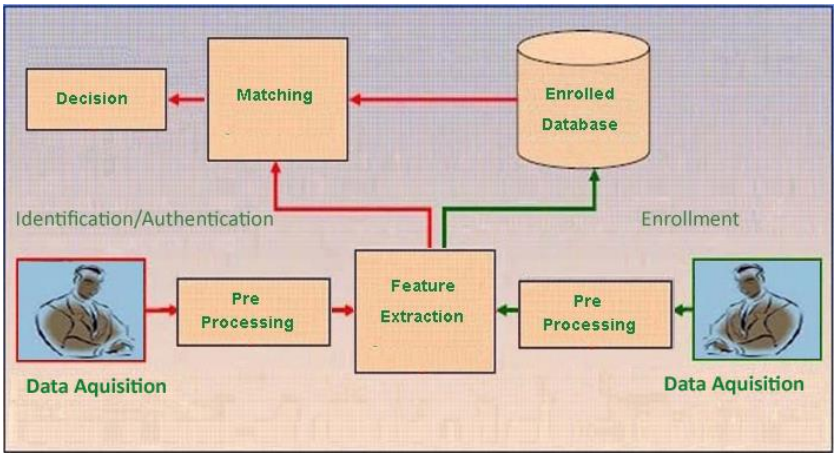

Fig. 1 Components and modes of Biometric Recognition System

The system implementation requires two modes, enrollment and operation. In the enrollment mode, the available traits of users are processed and the features are extracted and saved as a database to be used for comparison in the operation mode. In the operation mode, the

trait of the user is acquired, processed and features are extracted and compared to those in the database according to the purpose of the system whether identification or verification is, [1].

Descriptions of the system stages are given below and the requirements of each stage for the five biometric traits are given in table (2).

1. *Data Acquisition*: Human biometric trait data is usually acquired via a sensor or camera depending on the nature of the trait. For iris and fingerprints, the data is in image form acquired by camera devices, whereas for voice data is a series of values representing the voice signal taken by sensors. The quality of the acquired image or signal is important for accurate identification/verification. In some biometric systems, namely iris and face recognition systems, more than one image is required in order to reach the best matching with the enrolled database [8,14].

2. *Pre-Processing*: This stage involves the removal of noise and any unwanted feature. For example, iris is pre-processed for the removal of reflection point, eyelash and eyelid, [15,16] and the signature is subject to thinning algorithm.

3. *Feature Extraction*: Feature extraction is the most crucial stage in developing the biometric recognition system. It involves the extraction of the most unique feature from the biometric traits.

4. *Storage*: The digital representations of the biometric traits are stored either in a central database or in a card for further identification and verification tasks.

5. *Matching*: In this stage the comparisons are done between the extracted features (templates of the stored traits) and the template of the testing trait. The trait with highest match is taken as the recognized trait..

6. *Decision*: The final decision includes either to identify who is the person or to verify that the person is really what he claims.

Table 2. The requirements of the biometric recognition system for five biometric traits

Stages / Biometric traits	Data Acquisition	Databa-se	Extracted Feature	Methods of Feature Extraction	Methods of Matching
Iris	Infrared Camera	CASIA Version 1-	Iris texture	Hough Transform,	Hamming Distance,

		4, SDUMLA, UBIRIS		Integro-differential Operator,	Convolut-ional Neural networks (CNNs)
Finger-prints	Sensor	CASIA, SDUMLA, Multi-Sensor Finger-print Database	Bifurcations, ridge endings and islands	Gabor Filter	Artificial Neural Networks
Face	Camera	SDUMLA-Face database part 1 and part 2.	Outline, shape and distribution of eyes and nose	Geometric feature based methods, Holistic based meyhods	Template based recogni-tion, Neural networks
Voice	Voice Recorde r + A/D Conver-tor	VoxCeleb, 2000 Hub5, Google Audiset	Voice characteristics	Linear Prediction Coefficients (LPC),), Line Spectral Frequencies (LSF), Discrete Wavelet Transform (DWT)	Template Matching
Signature	Scanner , digitizer	SVC And MCYT	Shape, spatial coordinate and inclination of letters, writing order, pen pressure, pen up/down	dynamic time warping, hidden Markov models and vector quantization	Artificial Neural Networks

4. Evaluations of Biometric Recognition Systems

In general there are several key points upon which the evaluation of biometric system can be done.

These keys include accuracy, application area, strength and weakness, etc. Evaluations of the systems for the five traits are shown in table (3). According to this table, iris recognition system is the best since it provides better accuracy and it is more secure and therefore it can be used for the applications that require high security. Table 3. Evaluations of the biometric recognition systems for five biometric traits.

Table 3

Recogition System	Evaluation
Iris	1. Provides high accuracy. 2. Used in Border Checking, Government Offices and Banking security 3. Difficulty to be replicated 4. Expensive in term of speed and processing methods. 5. Encounter resistance from the user.
Finger-prints	1. Provides medium accuracy 2. Used in Forensic, Border Checking, and Government initiatives such as national ID, voter registration, passport. 3. Very Familiar, acceptable, cheap and easy to use 4. It can be replicated and easy to spoof and wear away with age.
Face	1. Provides medium accuracy 2. Used in Forensic, Border Checking 3. Very Familiar, acceptable, cheap and easy to use 4.The identification can be performed from a distance and can be used in static (image) and dynamic (video) applications. 5. Requires well lighting conditions. 6. The face of a person changes over time and facial expressions and sunglasses may affect the accuracy.
Voice	1. Provides medium accuracy 2. Used in Forensic, Telephone services. 3. Inexpensive and require less hardware. 4. Easy to use as well as no special instructions are needed. 5. The voice quality is very sensitive to noisy environments 6. The emotional and health conditions of the users affect the voice 7.The size of the voice database is large and it can impact the matching speed.
Signature	1. Provides low to medium accuracy 2. Used in Government Offices and Banking security, business validation for transaction contracts and agreements 3. Difficult to mimic the behavioral patterns which are inherent in the process of signing, noninvasive, and user-friendly 4. It has large intra class variability, not stable over time 5. Affected by user health, position and environmental conditions such as writing surface and writing pen

5. Conclusion

In general, Human biometrics (iris, fingerprints, face, voice and signature) provide better speed and accuracy for person identification and verification compared to the knowledge-based systems which use PIN code, user name and passwords and token-based systems which use key, magnetic or smart card and badge. However, amongst the five traits, iris is the most effective trait since it provides highest accuracy, and is difficult to be replicated even it is expensive and encounter resistance from the users.

BIBLIOGRAPHY

[1] Kaur, G., and Verma, C.K., *Comparative Analysis of Biometric Modalities*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, issue 4, 2014, Pag. 603-613.

[2] Fronitasari, D., Basari and Gunawan, D., *Palm Vein Feature Extraction Method by Using Optimized DVHLocal Binary Pattern*, International Journal of Computer Science and Information Security (IJCSIS), Vol. 17, No. 5, 2019, Pag. 8-12.

[3] Sabhanayagam, T., Venkatesan, V.P., and Senthamaraikannan, K., *A Comprehensive Survey on Various Biometric Systems*, International Journal of Applied Engineering Research, Vol. 13, No. 5, 2018, pag. 2276-2297.

[4] Achban, A., Sari, J. Y., and Sutardi, *The Implementation of Local Binary Patterns for Biometrics System Based on Dorsal Hand Vein Image*, Indonesian Journal of Information Technology, online ISSN 2599-295, Vol. 2, Issue 2, 2018, pag. 18-26.

[5] Tatepamulwar, C.B., and Pawar, V. P., *Comparison of Biometric Trends Based on Different Criteria*, Asian Journal of Management Sciences Vol. 2, No. 3,Special Issue, 2014, pag. 159-165.

[6] Galbally, J., Marcel, S., and Fierrez, J., *Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition*, IEEE Transactions On Image Processing, Vol. 23, No. 2, 2014, pag. 710-724.

[7] Srivastava, H., *A Comparison Based Study on Biometrics for Human Recognition*, Journal of Computer Engineering, Vol. 15, Issue 1, 2013, pag. 22-29.

[8] Phillips, J., Bowyer, K Transactions.W. and Flynn, P.J. (2007) 'Comments on The CASIA Version 1.0 Iris Data Set', IEEE on Pattern Analysis and Machine Intelligence, vol. 29, no. 10, pp. 1869-1870.

[9] Saini R., Rana N., "Comparison Of Various Biometric Methods", International Journal of Advances in Science and Technology (IJAST) Vol. 2, Issue 1, 2014, pag. 24-30.

[10] Otti C., "Comparison of Biometric Identification Methods", 11th IEEE International Symposium on Applied Computational Intelligence and Informatics May 12-14, 2016 , Timişoara, Romania, Pag. 339-344.

[11] Sareen P., “Biometrics – Introduction, Characteristics, Basic technique, its Types and Various Performance Measures”, International Journal of Emerging Research in Management &Technology, Vol. 3, Issue 4, 2014, Pag. 109-119.
[12] Yadav A. K., and Grewal S. K., “A Comparative Study of Different Biometric Technologies”, IJCSC, Vol. 5, No. 1, 2014, Pag. 37-42.
[13] Mali, K., and Bhattacharya S., “Comparative Study of Different Biometric Features”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, 2013, Pag. 2776-2784.
[14] Yin Y., Liu L., and Sun X., “SDUMLA-HMT: A multimodal Biometric Database’, In Biometric Recognition by (Sun, Z., L., J., Chen, X., Tan, T. (Eds.)), Springer Berlin Heidelberg, 2011, Pag. 260-268.
[15] Tahir, A. AK. and Bindian, A. I., *Localizarea irisului pentru sistemul biometric de identificare a persoanelor*, The XVIII International Conference on Multidisciplinary, "Professor Dorin Paul - Romanian hydropower founder", June-2016 vol. 30/2016, AGIR Edition, ISSN 2067-7138, pp. 215-224. (Conference Proceedings in Romainan and English Languages).
[16] Tahir, A. AK. and Anghelus, S., *A New Method of Eyelid Detection for Iris Recognition System*, The XVIII International Conference on Multidisciplinary, "Professor Dorin Paul - Romanian hydropower founder", June-2018, Cluj, Romania, Vol. 33/2018, ISSN 2067-7138, eISSN 2359-828X, 2018, pp. 171-184.

Prof.Dr. Ahmed AK TAHIR
Head of the Computer Science Dept,
College of Science, University of Duhok,
Kurdistan Region of Iraq
Tel: +964 (0) 750 457 7899
E-mail: ahmdi@uod.ac

Prof. Dr. Ing. Steluta ANGHELUȘ
Technical College, “TRAIAN VUIA”,
Oradea – Romania

BIOMETRICA UMANĂ ȘI SISTEMELE DE RECUNOȘTERI BIOMETRICE; O IMAGINE DE ANSAMBLU

Ahmed AK. TAHIR, Steluța ANGHELUȘ

HUMAN BIOMETRICS AND BIOMETRIC RECOGNITION SYSTEMS; AN OVERVIEW

Tehnologia biometrică câștigă un rol semnificativ în prezentarea soluțiilor pentru numeroase probleme din diferite aplicații care necesită

identificarea persoanelor, cum ar fi știința criminalistică, securitatea, afacerile finanțelor, verificarea frontierelor și ministerele și birourile guvernamentale. Este definită ca tehnologia de analiză a trăsăturilor fiziologice și comportamentale, cum ar fi fața, amprenta, irisul, retina, vocea și semnătura etc., pentru identificarea și autorizarea persoanei. În prezent, multe lucrări de cercetare sunt realizate pentru a obține sisteme de recunoaștere biometrică bazate pe diverse tipuri de trăsături umane. Pentru a furniza un sondaj cuprinzător, acest articol prezintă o imagine de ansamblu asupra a cinci trăsături biometrice (iris, amprente digitale, față, voce și semnătură). Prezentarea generală va acoperi modul de achiziție, zona de aplicare, metodele de implementare, puterea/ slăbiciunea și evaluarea sistemului.

Cuvinte cheie: Biometrie, Sistem de recunoaștere biometrică, iris, amprente, vene de deget, vena palmei, recunoaștere a feței, recunoaștere a trecerii, trăsături umane, recunoaștere vocală, recunoaștere semnătură

1. Introducere

Termenul biometric se referă la orice trăsături fiziologice sau de comportament umane care pot fi măsurabile și stabile în timp, cum ar fi fața, retina, amprentele, vena degetelor, urechea, vena palmei, irisul, vocea, mersul, apăsarea tastei, semnătura etc., [1-3].

În prezent, trăsăturile biometrice umane reprezintă baza principală a sistemelor de securitate și au devenit soluția în multe aplicații civile și guvernamentale, cum ar fi locuri de muncă în finanțe, verificarea frontierelor și ministerele și birourile guvernamentale.

Sistemele de recunoaștere biometrică prezintă mai multe avantaje față de sistemele bazate pe cunoștințe, care folosesc cod PIN, nume de utilizator și parole sau sisteme bazate pe simboluri care folosesc carduri și ecusoane cheie, magnetice sau smart, [4, 5]. Ele se bazează pe caracteristici și proprietăți care nu pot fi uitate, furate, partajate, schimbate, pierdute sau dezvăluite. Cu toate acestea, sistemele de recunoaștere biometrice sunt costisitoare și necesită metode sofisticate și automatizate pentru a identifica și autentifica persoana ca atare. În plus, acestea necesită măsurători ale caracteristicilor fiziologice sau comportamentale care sunt caracteristice/specifice persoanelor. Mai mult, acestea necesită dezvoltări continue pentru a răspunde cerințelor societății, și anume în domeniul e-guvernării, e-banking și comerț electronic și pentru a preveni persoanele frauduloase să treacă și să încalce legea [6].

Sistemele de identificare biometrice sunt de obicei concepute fie pentru identificare, fie pentru verificare, fie pentru ambele. În sistemul de identificare, care este denumit o potrivire unu-la-mulți (cine este

persoana?), Un eșantion de caracteristici biometrice individuale este comparat cu o listă de eșantioane din baza de date pentru a fi sigur că individul este în listă. În sistemul de verificare, care este denumit o potrivire unu la unu, operația de verificare este efectuată pentru a se conforma dacă o persoană este cu adevărat cine se pretinde, (persoana este într-adevăr ceea ce pretinde?), [7] .

Succesul sistemului de recunoaștere biometrică depinde de puterea trăsăturii biometrice și de scopul pentru care este proiectat. Au fost deja efectuate mai multe studii pentru compararea performanței diferitelor tipuri de sisteme de recunoaștere biometrică. De exemplu, [1, 3, 5, 7, 8, 9, 10] s-au comparat diferite tipuri de trăsături umane incluzând irisul, amprentele, fața, vena palmei, vocea, mersul, urechea, semnătura, ADN-ul, retina etc. că performanța trăsăturii depinde de zona de aplicare, de costul și cât de ușor este înregistrat.

Acest studiu prezintă o imagine de ansamblu asupra utilizării biometriei umane pentru identificarea persoanei. Sunt selectate cinci trăsături umane, trei trăsături fiziologice (iris, amprente și față) și două trăsături comportamentale (voce și semnătura).

2. Măsurători biometrice. Caracteristici

Există multe trăsături în corpul uman care pot fi considerate măsurători biometrice. Conform [11, 12] există șapte criterii (piloni) care trebuie să fie disponibile în trăsături pentru a putea fi utilizate măsurători biometrice. Acești șapte piloni sunt:

1. *Universalitate*: Fiecare persoană trebuie să posede aceleași trăsături fiziologice precum degetele, irisul, fața etc., și aceleași trăsături de comportament precum vocea, mersul, semnătura etc.
2. *Distinctivitate*: trăsătura trebuie să fie suficient de unică pentru a distinge persoana.
3. *Permanența*: trăsăturile trebuie să fie stabile de-a lungul vieții unei persoane.
4. *Colectabilitate*: trăsătura biometrică trebuie măsurată cantitativ și ușor.
5. *Performanță*: trăsătura trebuie să ofere o precizie ridicată a recunoașterii.
6. *Acceptabilitatea*: Modul de dobândire a trăsăturilor trebuie să fie acceptat de către oameni. De obicei, oamenii preferă să înregistreze trendul într-un mod non-invaziv.

7. *Rezistența la circumstanțe*: sistemul trebuie să fie greu pentru orice eludare prin metode frauduloase pentru a oferi securitate eficientă.

Puterea oricărei trăsături biometrice depinde în mare măsură de aplicația pentru care este utilizată [10, 13]. De exemplu, unele aplicații pot accepta unele rate de eroare, cum ar fi taxele de autostradă, în timp ce altele nu pot fi, cum ar fi sistemul bancar și investigațiile penale. În afară de aceasta, unele aplicații pot necesita o decizie rapidă, cum ar fi controlul la frontieră, în timp ce altelesolicită atenție sporită, cum ar fi cercetarea penală. Tabelul (1) prezintă comparații între cinci trăsături biometrice (iris, amprente, față, voce și semnătura).

Tabelul 1. Comparații ale trăsăturilor biometrice

Criterii (Etape) / Trăsături biometrice	Universalitate	Permanența	Distinctivitate	Colectabilitate	Performanță	Acceptabilitatea	Rezistența la circumstanțe
Iris	H	H	H	M	H	M	H
Amprentare	M	H	H	M	H	M	M
Față	H	L	M	H	L	M	M
Voce	M	M	M	H	M	H	H
Semnătura	M	L	L	H	L	H	H

3. Etapele sistemului biometric

Componentele (etapele) și implementarea oricărui sistem de biometrie pot fi reprezentate de diagrama din figura 1.

Implementarea sistemului necesită două moduri, înscrierea și operarea. În modul de înscriere, trăsăturile disponibile ale utilizatorilor sunt procesate, iar funcțiile sunt extrase și salvate ca bază de date pentru a fi folosite pentru comparare în modul de operare. În modul de operare, trăsătura utilizatorului este achiziționată, procesată și caracteristicile sunt extrase și comparate cu cele din baza de date, în funcție de scopul sistemului, indiferent dacă este identificarea sau verificarea, [1]. Descrierile etapelor sistemului sunt prezentate mai jos și cerințele

fiecărei etape pentru cele cinci trăsături biometrice sunt prezentate în tabelul 2.

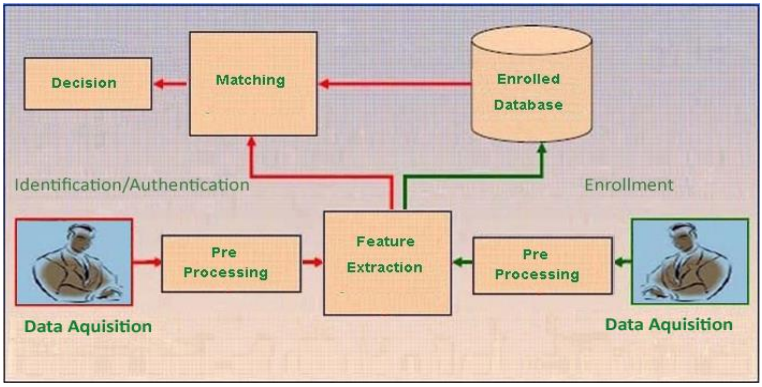

Fig. 1 Componente și moduri ale sistemului de recunoaștere biometrică

1. Achiziționarea datelor: Datele de trăsături biometrice umane sunt de obicei obținute printr-un senzor sau o cameră, în funcție de natura trăsăturii. Pentru iris și amprente digitale, datele sunt sub formă de imagine achiziționate de dispozitivele de cameră, în timp ce pentru date vocale este o serie de valori reprezentând semnalul vocal luat de senzori. Calitatea imaginii sau a semnalului achiziționate este importantă pentru o identificare/verificare exactă. În unele sisteme biometrice, și anume sistemele de recunoaștere a irisului și a feței, sunt necesare mai multe imagini pentru a ajunge la cea mai bună potrivire cu baza de date înscrisă [8, 14].

2. Pre-procesare: Această etapă implică eliminarea zgomotului și a oricărei caracteristici nedorite. De exemplu, irisul este pre-procesat pentru îndepărtarea punctului de reflecție, a genelor și a pleoapei [15, 16], iar semnătura este supusă algoritmului de subțiere.

3. Extragerea caracteristicilor: extragerea caracteristicilor este cea mai crucială etapă în dezvoltarea sistemului de recunoaștere biometrică. Ea implică extragerea celei mai unice trăsături din trăsăturile biometrice.

4. Depozitare: Reprezentările digitale ale trăsăturilor biometrice sunt stocate fie într-o bază de date centrală, fie într-un card pentru activități suplimentare de identificare și verificare.

5. Potrivire: în această etapă, comparațiile se fac între caracteristicile extrase (șabloane ale trăsăturilor stocate) și șablonul trăsăturii de testare. Trăsătura cu cea mai mare potrivire este luată ca trăsătură recunoscută.

6. Decizie: Decizia finală include fie identificarea cine este persoana, fie verificarea dacă persoana respectivă este într-adevăr ceea ce pretinde.

Tabelul 2 prezintă cerințele biometrice sistem de recunoaștere a cinci trăsături biometrice.

Tabelul 2

Etape / Biome-tric / trăsături	Achiziție de date	Baza de date	Metode de caracter extracte	Metode de extracție a caracteristicilor	Metode de extracție
Iris	Cameră infraroșu	CASIA Versiunea 1-4, SDUMLA, UBIRIS	Textura Iris	Hough Transform, Operator integral-diferențial	Distanță de ciocan, Rețele neuronale convolutive (CNN)
Amprente	Sensor	Senzor cu amprente CASIA, SDUMLA	Baza de date cu imprimeu multi-senzor Bifurcații	terminații de creastă și insule Gabor Filtre	Rețele neuronale artificiale
Față	Camera	SDUMLA-Face bază de date partea 1 și partea 2.	Schiță, formă și distribuție a ochilor și nasului	Metode geometrice bazate pe metode holistice bazate pe șabloane	Recunoașterea bazelor de șabloane, rețele neuronale
Voce	Înregistrare vocală Voice Recorder + A/D Convertor	Convertor VoxCeleb, 2000 Hub5, Google Audiset	Caracteristici vocale	Coeficienți de predicție liniară (LPC),), Frecvențe spectrale de linie (LSF), Modele de ondulare discrete (DWT)	Potrivirea șabloanelor
Semnătura	Scanner de semnături	SVC digitalizator și MCYT	Shape, coordonarea spațială și înclinarea literelor, ordinea scrierii, presiunea stiloului, deformarea dinamică în sus/în jos	Deformare dinamică, modele ascunse de Markov și cuantificare vectorială	Rețelele neuronale artificiale

4. Evaluările sistemelor de recunoaștere biometrică

În general, există mai multe puncte cheie asupra cărora se poate face evaluarea sistemului biometric.

Aceste chei includ precizia, aria de aplicare, rezistența și slăbiciunea etc. Evaluările sistemelor pentru cele cinci trăsături sunt prezentate în tabelul 3.

Conform acestui tabel, sistemul de recunoaștere a irisului este cel mai bun, deoarece oferă o precizie mai bună și este mai sigur și, prin urmare, poate fi utilizat pentru aplicațiile care necesită o securitate ridicată.

Tabelul 3 prezintă evaluările sistemelor de recunoaștere biometrică pentru cinci trăsături biometrice.

Tabelul 3

Recunoaștere Sistem	Evaluare
Iris	1. Oferă precizie ridicată. 2. Folosit în verificarea frontierelor, birourile guvernamentale și securitatea bancară 3. Dificultate de replicat 4. Costisitoare în termeni de viteză și metode de procesare. 5. Rezistența la întâlnire a utilizatorului.
Deget amprentă	1. Oferă precizie medie 2. Folosit în inițiativele criminalistice, verificarea frontierelor și guvernamentale, precum ID național, înregistrarea alegătorilor, pașaport. 3. Foarte familiar, acceptabil, ieftin și ușor de utilizat 4. Poate fi replicat și ușor de stricat și de purtat odată cu vârsta.
Față	1. Oferă precizie medie 2. Utilizat în criminalistică, verificare la frontieră 3. Foarte familiar, acceptabil, ieftin și ușor de utilizat 4.Identificarea poate fi realizată de la distanță și poate fi utilizată în aplicații statice (imagine) și dinamice (video). 5. Necesită condiții de iluminare bine. 6. Fața unei persoane se schimbă în timp, iar expresiile faciale și ochelarii de soare pot afecta precizia.

Voce	1. Oferă precizie medie 2. Folosit în serviciile de telefonie criminalistică. 3. ieftin și necesită mai puțin hardware. 4. Ușor de utilizat, precum și nu sunt necesare instrucțiuni speciale. 5. Calitatea vocii este foarte sensibilă la mediile zgomotoase 6. Condițiile emoționale și de sănătate ale utilizatorilor afectează vocea 7. Dimensiunea bazei de date vocale este mare și poate afecta viteza de potrivire.
Semnătură	1. Oferă precizie scăzută până la medie 2. Folosit în birourile guvernamentale și securitatea bancară, validarea afacerilor pentru contracte și acorduri de tranzacții 3. dificil de imitat modelele de comportament care sunt inerente în procesul de semnare, noninvaziv și ușor de utilizat 4. Are variabilitate mare în cadrul clasei, nu este stabilă în timp 5. Afectat de sănătatea utilizatorului, poziția și condițiile de mediu, cum ar fi suprafața de scris și stiloul de scris

5. Concluzie

În general, biometria umană (iris, amprente, față, voce și semnătură) asigură o viteză și o precizie mai bune pentru identificarea și verificarea persoanei, comparativ cu sistemele bazate pe cunoștințe care utilizează cod PIN, nume de utilizator și parole și sisteme bazate pe simboluri care utilizează cheia, placă magnetică sau inteligentă și ecuson. Cu toate acestea, printre cele cinci trăsături, irisul este cea mai eficientă trăsătură, deoarece oferă o precizie cea mai ridicată și este dificil de replicat chiar dacă este scump și rezistența utilizatorilor.

Prof.Dr. Ahmed AK TAHIR
Șef departament informatică,
Colegiul de Științe, Universitatea din Duhok,
Regiunea Kurdistan din Irak,
Tel: +964 (0) 750 457 7899,
E-mail: ahmdi@uod.ac

Prof. Dr. Ing. Steluta ANGHELUȘ
Colegiul Tehnic, „TRAIAN VUIA”, Oradea – România
E-mail: stelanghelus@gmail.com