Tikrit Journal of Pure Science
ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)
Journal Homepage: http://tjps.tu.edu.iq/index.php/j

Biometric Technologies in Recognition Systems: A Survey

Shihab A. Shawkat[1] , Raya N. Ismail[2]
[1] *Directorate of Education Salahuddin, Tikrit, Iraq*
[2] *Department of Computer , College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq*
DOI: http://dx.doi.org/10.25130/tjps.24.2019.120

ARTICLE INFO.
Article history:
-Received: 21 / 11 / 2018
-Accepted: 17 / 1 / 2019
-Available online: / / 2019
Keywords: Biometrics, Identification, Verification, Recognition, Authentication.
Corresponding Author:
Name: Shihab A. Shawkat
E-mail:
shahab84ahmed@gmail.com
Tel:

ABSTRACT

The ability to recognize people uniquely and to associate personal attributes such as name and nationality with them has been very important to the fabric of human society. Nowadays, modern societies have an explosion in population growth and increased mobility which necessitated building advanced identity management systems for recording and maintaining people's identities. In the last decades, biometrics has played an important role in recognizing people instead of traditional ways such as passwords and keys which can be forgotten or be stolen. Biometric systems employ physiological and/or behavioral characteristics of people to verify their identities. There are different biometric modalities that can be used to recognize people such as fingerprints, face, hand geometry, voice, iris, signature, etc. In this paper, a comprehensive overview have been provided on the major issues of biometric systems including general biometric system architecture, major biometric traits, biometric systems performance, and some relevant works.

1. Introduction

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Therefore, building highly reliable automatic authentication systems, in order to manage identities of people, has become a major research and commercial issue. Identifying people using the conventional technologies, such as password, key, ID card, Personal Identification Number (PIN), etc., are not reliable enough to achieve the security requirements of many of real-life applications. Hence, identifying people based on their personal characteristics, i.e., biometric based authentication, has gained an increasing attention. Biometrics based recognition means recognizing people using their distinct features extracted for their biometric traits such as fingerprint, iris, face, voice, and etc **[1]**.

Generally speaking, biometric traits can be classified into two types: physiological and behavioral. Physiological biometrics is related to the shape of the body such as fingerprint, face, DNA, hand and palm geometry, iris, and retina, while behavioral biometrics is related to the behavior of a person such as gait, voice, signature, and keystroke, as shown in Fig (1). **[2]**.

Fig. 1: The different types of biometrics.

Biometric recognition systems can be classified into two types: identification system and verification systems. In identification systems, the biometric template of the person, who needs to be identified, is compared to all the biometric templates stored in the system during the enrollment phase to find a match, i.e., one-to-many comparison is performed. On the other side, in verification system the biometric template of the person, who needs to be verified, is compared to the biometric template of the claimed

identity that has been acquired during the enrollment phase, i.e., one-to-one comparison is performed **[1] [3]**.

Nowadays, biometric systems are being employed in many real-life applications including commercial, government, and forensic applications. Commercial applications such as computer network logins, Internet access, ATMs, e-commerce, and credit cards. Government applications such as driver's licenses, national ID cards and passport control. Forensic applications such as criminal identification and parenthood determination **[4]**. Although unimodal biometric systems have proofed their efficiency and effectiveness with high degree in these applications, they cannot achieve the high security requirements needed by other applications such as US visit program. Therefore, multi-biometric systems have attracted the attention of the researchers because of the limitations of unibiometric system where the biometric source may become unreliable due to sensor or software malfunction, or poor quality of specific biometric trait of the user **[5]**.

Multi-biometric system can achieve more accuracy than a unibiometric system for many reasons including: A combination of multiple biometric sources is more unique to an individual than a single biometric sample. Also, the problems associated with a subset of biometric sources, such as noise, imprecision, or drifting caused by aging or by other reasons, can be overcome by using the accurate and problems-free information provided by the other biometric resources. Multi-biometric systems depend on representing each client by multiple sources of biometric information. Multi-biometric systems can be classified into six types based on the kinds of biometric sources. These types are Multi-sensor, Multi-algorithm, Multi-instance, Multi-sample, Multimodal and Hybrid systems **[5][6]**.Like other systems, biometric recognition systems must be validated and their performance must be assessed and evaluated using the suitable criteria. The metrics used to evaluate a biometric system depends on whether the objective of the biometric system is identification or verification. For identification systems, their performance can be assessed using Identification Rate and False Alarm Rate (FAR). For verification systems, their performance can be assessed using a set of metrics such as False Match Rate (FMR), False Non-Match Rate (FNMR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), True Acceptance Rate (TAR), and Weighted Error Rate (WER) **[3]**.

The remaining sections of this research are presented in the following manner: Section two introduces a description of the general architecture of biometric systems. Sections three briefly describes the major biometric technologies and compares among them based on a set of criteria. Section four gives some notes about biometric system performance. Section five presents an overview on some recent related works in the biometrics fields. Finally, the paper is concluded and future work is provided in Section six.

2. General Biometric System Architecture

In general, biometric system operation is done in two phases: enrollment and recognition. In the enrollment phase, there should be a way of capturing the chosen unique characteristic (i.e., the biometric trait). Then, the acquired biometric trait is enhanced by applying preprocessing phase. Then, the discriminating features which can be used in the recognition process are extracted and represented in a way suitable for storage and processing **[7]**.

In the recognition phase, the query input is captured and enhanced and the features are extracted and compared to the previously stored templates. One-to-many comparison process is performed in case of identification while one-to-one comparison process in case of verification **[8]**. Fig (2) shows that block diagram of biometric recognition system architecture.

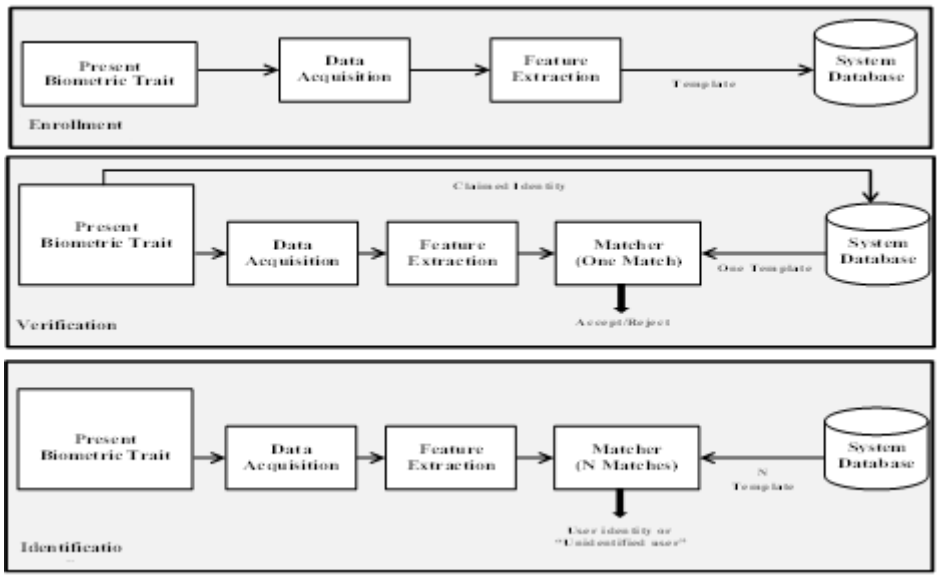

Fig. 2: General block diagram of biometric system architecture.

There are four major steps in each biometric system including data acquisition from sensor, feature extraction, storing the templates in system database and matching **[7,8]**.

1. **Data acquisition from sensor:** in which the biometric data is captured using a sensor.
2. **Feature Extraction:** in which the discriminating features are extracted by adopting specific methods.
3. **Storage step:** in which the biometric templates are stored to be compared later to verify or identify some person.
4. **Matching:** in which the query template is compared to one or many templates to verify or identify some person.

3. Major Biometric Technologies

As mentioned previously, biometric traits can be classified into two types: physiological and behavioral. Currently, there are a large number of biometric technologies which have been employed to determine the identities of persons. However, seven biometric technologies are considered the most common biometric technologies including fingerprint recognition, hand geometry recognition, facial recognition, iris and retina recognition, voice recognition, keystroke recognition, and signature recognition. The first four technologies depend on physiological biometric traits while the remaining technologies depend on behavioral biometric traits. Some of these criteria or factors are listed and briefly described in Table **1 [9]**.

Table 1: The properties of biometric traits.

No.	Properties	Description
1	Universality	The characteristic is existing in every person.
2	Distinctiveness	The characteristic can be used to differentiate between people.
3	Permanence	The discriminating features of the characteristic should be fixed and stable over time.
4	Collectability	The characteristic can be quantitatively measured.
5	User-friendliness	The biometric system should be acceptable by the community of users.
6	Accuracy	The system should achieve high accuracy in order to fulfill the security requirements.
7	Circumvention	The system should be robust and cannot be attacked easily.

Consequently, a comparison among the major biometric technologies based on the above factors is presented in Table 2 **[12]**.

Table 2: Comparison among the major biometric traits (H: High, M: Medium, and L: Low)

No.	Biometric Properties	Fingerprint	Hand Geometry	Face	Iris	Retina	Voice	Keystroke	Signature
1	Universality	M	M	H	H	H	M	L	L
2	Distinctiveness	H	M	H	H	H	L	L	L
3	Permanence	H	M	L	H	M	L	L	L
4	Collectability	M	H	H	M	L	M	M	H
5	Performance	H	M	M	H	H	L	L	L
6	Acceptability	M	M	H	L	L	H	M	H
7	Circumvention	M	M	L	L	L	H	M	H

4. Performance of Biometric Systems

Two samples of the same biometric trait taken from the same person, at the same or at different sessions, cannot exactly coincide because of many reasons including improper positioning on the used sensor, bad imaging conditions, changes in the environment, etc. So, the biometric system usually computes the 'match score'***s*** which measure the similarity between the query input and the template stored previously in the database. The higher the matching score is, the greater the possibility that the two samples are taken from the same person. After computing the matching score ***s***, it is compared to the acceptance threshold ***t***. If the ***s*** is greater than or equal to ***t***, the system assumes that the two samples belong to the same person. Otherwise; the two samples are considered from different persons. The distribution of matching scores generated by comparing biometric samples acquired from the same person is called genuine distribution, while the distribution of matching scores generated by comparing biometric samples acquired from different persons is called imposter distribution **[13]**, as shown in Fig (3).

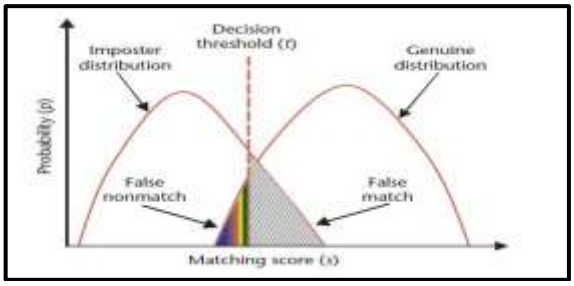

Fig. 3: Biometric system error rates.

5. Related Work

During the last decades huge amounts of research efforts have been done for identifying or verifying the identities of persons. In this section an overview is provided on some recent works in the major seven biometric technologies in addition to some recent works in multi-biometric systems.

In **[14]**, a fingerprint recognition approach based on Discrete Wavelet Transform (DWT) features has been proposed. It has been developed to recognize people using their low quality fingerprints from inked-printed images on paper. Gaber filtering is applied to enhance the fingerprint before the feature extraction step. The Euclidean distance is used to measure the similarity. The FVC2000 database has used for evaluating the proposed system and the results have shown that the proposed approach has 2.80% EER. In **[15]**, the authors addressed some issues, which have not been addressed previously, regarding fingerprint recognition. Their study focused on answering the follwing issues: 1) whether young children's fingerprints contains discriminating features or not. 2) If so, at what age children's fingerprints can be accurately acquired for recognition? 3) whether young children's fingerprints can be used for recognizing them as they age or not. A propriatory database has been collected from 309 children four different times during one year. The involved children had ages ranges from 0 to 5 years. AFIS has been used and the results was 98.9% true accept rate at 0.1% false accept rate for the children of ages higher than 6 months.

In **[16]**, the authors presented a new method called probabilistic self-organizing maps (Prob-SOM) to obtain a model that allows recognizing speakers based on their voice, independently of the text used. the Cepstral coefficients of audio signals are repsented using SOM while the recognition is performed using a probabilistic system. Audio signals have been recorded for 30 speaker during reading a text for 1 minute duration which are further divided 20 secconds for traing and 40 seconds for testing. The proposed system achieved 97.25%. recognition rate.

In **[17]**, the authors employed Subspace Gaussian Mixture Model (SGMM) approach as a probabilistic generative model to estimate speaker vector representations to be used later in the speaker verification task. A speaker verification framework has been proposed based on low-dimensional speaker vectors estimated using SGMMs. The proposed system has been validated using NIST SRE 2010 evaluation set and compared to the well-known i-vector extractor. The proposed system achieved EER of 1.3% in their best case. In **[18]**, the authors proposed using Restricted Boltzmann Machines (RBM) as a non-linear transformation of GMM supervectors for speaker recognition. The experimental results on the core test condition of the NIST SRE 2006 corpus have shown that the proposed RBM supervectors has EER of 7.58%.

In **[19]**, a new distance metric that is effective in dealing with the challenges intrinsic to keystroke dynamics data. CMU dataset has been used to evaluate the proposed keystroke biometrics algorithms which achieved 0.054% EER in the best case. In **[20]**, the authors presented a new approach for the free text analysis of keystrokes that combines monograph and digraph analysis. Also, they used a neural network which employs the relation between the monitored keystrokes for prediciting missing digraphs. The proposed approach has been evluated in both heterogeneous (53 users) and homogeneous environments (17 users). It achieved 0.0152% FAR, 4.82% FRR, and 2.46% EER in heterogenous environments and 0% FAR, 5.01% FRR, and 2.13% EER in homogeneous environment. In **[21]**, the authors proposed user identification and authentication system besed on combining keystroke dynamics features with keystroke acoustic features. They collected a total of 824 samples from 7 subjects for experiments. 46 features including 38 acoustic features are extracted. C-Support Vector Classification (C-SVC) and one-class Support Vector Machine (1-SVM) are applied for user identification and authentication respectively. Their approach achieved 92.8% accuracy for user identification. The False Rejection Rate (FRR) and False Acceptance Rate (FAR) are only 12% and 11% for user authentication.

A summary for the research efferts mentioned above is provided in Table 3.

Table 3: A summary for some research efforts in biometrics research field (Uni.: Unibiometric, Multi.: Multibiometric, V.: Verification, I: Identification)

Ref. No. / year	(Uni/Multi) biometric System	Biometric Trait	System Objective	Used features	Used Classifier	Used Dataset	Perfomance
[win 2011]	Uni.	Fingerprint	V.	Discrete Wavelet Transform	Euclidean distance	FVC2000	2.80% EER
[F jain 2016]	Uni.	Fingerprint	V.	AFIS	AFIS	Propriatory	98.9% TAR at 0.1% FAR
[V Estre 2010]	Uni.	Voice	I.	Cepstral coefficients of the audio signals	Prob-SOM	Propriatory Dataset (30 speaker)	Reconition Accuracy 97.25%
[V molick 2015]	Uni.	Voice	V.	Mel-Frequency Cepstral Coefficients	Subspace Gaussian Mixture Model (SGMM)	NIST SRE 2010	1.3% ERR
[V ghahabi 2015]	Uni.	Voice	V.	GMM reduced by RBMs	Cosine distance	NIST SRE 2006	7.58% ERR
[K zhong 2012]	Uni.	Keystroke	V.	Keystroke Dynamics	KNN with newly proposed distance metric	CMU keystroke dynamics benchmark	0.054% EER
[k ahmed 2014]	Uni.	Keystroke	V.	monographs and digraphs	ANNs	Propriatory Dataset 53 persons in hetro. environmen. --- 17 persons in homo. environmen.	. 0152% FAR 4.82% FRR 2.46% EER --- 0% FAR 5.01% FRR 2.13% EER
[K zhou 2016]	Uni.	Keystroke	I. and V.	keystroke dynamics features and keystroke acoustic features.	C-Support Vector Classification (C-SVC) --- one-class Support Vector Machine (1-SVM)	Propriatory Dataset A total of 824 samples from 7 subjects .	92.8% Identification Accuracy --- 12% FRR 11% FAR

6. Conclusion

Biometric technologies are playing an important and noticeable role in our modern society by being involved in many real-life applications such security systems, access control system, e-commerce, etc. This paper only briefly touched the main issues of biometric systems and technologies. The performance of biometric systems greatly vary upon the operating and external conditions as no universal biometric technology exists. The best performance is obtained where the technology is designed for strict controlled conditions and where data acquisition is accomplished under human supervision. Also, an overview on some reseach efforts in the field is provided. A biometric system can be easily attacked and spoofed, a critical open issue yet to be solved. Intensive work is still undergoing to improve their performance while protecting them against various attacks. The multimodal biometric systems can be improved by enhancing matching algorithms. Therefore, a robust, efficient, and accurate matching algortihm based on swarm intelligence techniques, is entended to be desigend as a future work.

References

[1] Chen, Ching-Han, and Chia Te Chu. (2006). "*Fusion of face and iris features for multimodal biometrics."* In International Conference on Biometrics, Springer, Berlin Heidelberg, pp 571-580.

[2] Vats, Sandhya, and Harkeerat Kaur. (2016). *"A Comparative Study of Different Biometric Features."* International Journal of Advanced Research in Computer Science 7(6), pp 169-171 .

[3] Marcel, Sébastien. (2013). *"BEAT–biometrics evaluation and testing."* Biometric technology today 2013, 1(2), pp 3-22.

[4] Dunstone, Ted, and Neil Yager. (2008). "*Biometric system and data analysis: Design, evaluation, and data mining*", Springer Science & Business Media, pp 45-69.

[5] Jain, Anil, Arun A. Ross, and Karthik Nandakumar. (2011). *"Introduction to biometrics"*, Springer Science & Business Media, pp 40-55.

[6] Aly, Ola M., Houda M. Onsi, Gouda I. Salama, and Tarek A. Mahmoud. (2012). *"Multimodal biometric system using iris, palmprint and finger knuckle."* International journal of computer applications 57(16), pp (112-125).

[7] Miura, Naoto, Akio Nagasaka, and Takafumi Miyatake. (2007). *"Extraction of finger-vein patterns using maximum curvature points in image profiles."* IEICE TRANSACTIONS on Information and Systems 90(8), pp 1185-1194 .

[8] Freeman, William T., and Michal Roth. (1995). *"Orientation histograms for hand gesture*

recognition." In International workshop on automatic face and gesture recognition,12, pp 296-301 .
[9] Jain, Anil, Lin Hong, and Sharath Pankanti. (2000). *"Biometric identification."* Communications of the ACM 43(2) , pp 90-98.
[10] Jain, Anil K., Arun A. Ross, and Karthik Nandakumar. (2011) . *"Introduction." In Introduction to Biometrics"* ,Springer, Boston, MA, pp 1-49.
[11] Bhatt, Shanthi, and T. Santhanam. (2013). "*Keystroke dynamics for biometric authentication—A survey."* In Pattern Recognition, Informatics and Mobile Engineering (PRIME), International Conference on, IEEE, pp 17-23.
[12] Delac, Kresimir, and Mislav Grgic. (2004). "*A survey of biometric recognition methods."* In Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, IEEE, pp 184-193 .
[13] Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. (2003). *"Biometric recognition: Security and privacy concerns."* IEEE security & privacy 99(2) , pp 33-42.
[14] Win, Zin Mar, and Myint Myint Sein. (2011). *"Texture feature based fingerprint recognition for low quality images."* In Micro-NanoMechatronics and Human Science (MHS), International Symposium on, IEEE, pp 333-338,.
[15] Jain, Anil K., Sunpreet S. Arora, Kai Cao, Lacey Best-Rowden, and Anjoo Bhatnagar. (2017). *"Fingerprint Recognition of Young Children."* IEEE Transactions on Information Forensics and Security 12(7), pp 1501-1514.
[16] Estrebou, Cesar, Laura Lanzarini, and Waldo Hasperué. ,(2010). *"Voice recognition based on probabilistic SOM."* In Proceedings of the Conference: Conferencia Latinoamericana en Informática, At Asunción, Paraguay.
[17] Motlicek, Petr, Subhadeep Dey, Srikanth Madikeri, and Lukas Burget. (2015). *"Employment of subspace gaussian mixture models in speaker recognition."* In Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on, IEEE, pp 4445-4449 .
[18] Ghahabi, Omid, and Javier Hernando. (2015). *"Restricted Boltzmann machine supervectors for speaker recognition."* In Acoustics, Speech and Signal Processing (ICASSP),International Conference on, IEEE, pp 4804-4808 .
[19] Zhong, Yu, Yunbin Deng, and Anil K. Jain. (2012) *"Keystroke dynamics for user authentication."* In Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE Computer Society Conference on, IEEE, pp 117-123.
[20] Ahmed, Ahmed A., and Issa Traore. (2014). *"Biometric recognition based on free-text keystroke dynamics."* IEEE transactions on cybernetics 44(4) pp 458-472.
[21] Zhou, Qianqian, Yanni Yang, Feng Hong, Yuan Feng, and Zhongwen Guo. (2016). *"User Identification and Authentication Using Keystroke Dynamics with Acoustic Signal."* In Mobile Ad-Hoc and Sensor Networks (MSN), 12th International Conference on, IEEE, pp 445-449 .
[22] Ahmed.T and Al-Senaidy.A.M. (2013). "Software tools in bioinformatics and issues faced implementation." Global Engineers & Technologists review.
[23] Jean-Michel Claverie. (2000). "From bioinformatics to computational biology." Cold spring Horbor Laboratory Press.
[24] Khalid Raza. (2012). "Application of data mining in bioinformatics." Indian journal of computer science and engineering Vol 1 No 2, 114-118.

دراسة التقنيات القياسات الحيوية في أنظمة التعرف

شهاب احمد شوكت[1] ، ريا نزار اسماعيل[2]

[1]مديرية تربية صلاح الدين ، تكريت ، العراق

[2]قسم الحاسوب ، كلية علوم الحاسوب والرياضيات ، جامعة تكريت ، تكريت ، العراق

الملخص

إن عملية التعرف على الأشخاص وربط الصفات الشخصية مثل الاسم والجنسية بكل شخص هو امر هام للغاية للحفاظ على نسيج المجتمع. ولكن حدوث الانفجار السكاني وكثرة تنقل البشر هذه الأيام في مجتمعاتنا الحديثة استلزم بناء انظمة متطورة لأداء هويات الاشخاص. في العقود الأخير، لعبت القياسات الحيوية دورا حيويا في التعرف على الأشخاص بدلا من الطرق التقليدية مثل كلمات السر او المفاتيح والتي تكون عرضة للنسيان او السرقة. تستخدم نظم القياسات الحيوية الخصائص الفسيولوجية و/أو السلوكية للأشخاص لتحديد هوياتهم. هنالك انواع مختلفة من الخصائص البيولوجية او السلوكية التى يمكن استخدامها فى عملية التعرف مثل بصمات الأصابع، الوجه، هندسة اليد، القزحية، التوقيع.. الخ. في هذا البحث، نقدم لمحة شاملة عن القضايا الرئيسية للنظم البيومترية بما في ذلك المعمارية العامة لنظم التعرف التي تعتمد على القياسات الحيوية، انواع القياسات الحيوية الرئيسية ، وأداء تلك النظم ، وبعض الأعمال ذات الصلة.