Biometric Systems: A Comprehensive Review

Rebin Abdulkareem Hamaamin[1], Omar Mohammed Amin Ali[2], Shahab Wahhab Kareem[3]

1. Computer Science, College of Sciences, Charmo University, Chamchamal, Sulaimani, KRG, Iraq.
2. Department of IT, Chamchamal Technical Institute, Sulaimani Polytechnic University, KRG, Iraq.
3. Department of Technical Information Systems Engineering, Technical Engineering College, Erbil Polytechnic University, KRG, Iraq.

*Corresponding author E-mail: rebin.abdulkarim@chu.edu.iq
https://doi.org/10.29072/basjs.20240110

ARTICLE INFO

Keywords

Biometric, database, authentication, fingerprint, hand, Face, gait, era, iris, speaker,recognition.

ABSTRACT

As the utilization of biometric data grows, it is expected that systems will become more dependable and capable of providing successful outcomes in challenging scenarios and in the face of counterfeiting. Ensuring the security of information is important to the effective functioning of any system. Hence, a stringent approach is necessary to authenticate the identity of each individual prior to granting them access to the stored data. Cancellable biometrics can enhance the security and privacy of users in response to potential threats. This study reviews and discusses many components of the biometric system, including face recognition, fingerprint identification, iris recognition, speaker recognition, gait recognition, ear recognition, and hand scanning. Authentication for the Biometric database is included in each section. For each segment, we will evaluate an article and analyze the discoveries presented in that paper during our review. Authentication is performed by all sections inside a filed biometric database.

Received 24 Feb 2024; Received in revised form 12 Apr 2024; Accepted 22 Apr 2024, Published 30 Apr 2024.

1. Introduction

Biometric technologies such as fingerprint, iris, retinal scan, voice, palm, and facial recognition are utilized to identify and recognize individuals. Various ID systems integrate these technologies alongside biographic data for biometric recognition, which automatically identifies individuals based on biological or behavioral features. Biometric identification involves searching a database to find the biometric reference identifier(s) associated with a single individual. Biometric verification, on the other hand, confirms a biometric claim through comparison. Both processes are integral to biometric recognition and can serve distinct purposes [1]. Every biometric system necessitates a database to store existing data and compare it with new data for discovery or authentication purposes. Each database contains pertinent components tailored to the specific biometric modality. For instance, a fingerprint database requires images, while a voice database necessitates audio recordings. This ensures that all relevant information is appropriately stored and accessible within the designated database [2]. Identity records can often be duplicated, posing challenges for ID systems. To address this issue, biometric identification can be leveraged to conduct a duplicate biometric enrollment check, ensuring the uniqueness of each user within the database. This involves comparing a template generated from a captured biometric to all or a subset of templates stored in the biometric database. Upon detection of a duplicate registration, appropriate measures are taken, such as adding the new template to the database while ensuring individual identification integrity [3]. Certain authentication methods require the user's biometric verification, which involves comparing a template derived from a captured biometric to a single stored template on a one-to-one (1:1) basis. This stored template could be on an ID card, mobile phone, or within a database. Biometrics generally fall into two primary categories: biological and behavioral. Biological biometrics include fingerprints, face, iris, veins, etc., while behavioral biometrics include keystroke dynamics, gait, signature, voice, etc. [4,5]. In our review, we examined various biometric authentication features such as face recognition, fingerprint identification, iris recognition, speaker recognition, gait recognition, ear recognition, and hand scanning. Each of these features plays a crucial role in authenticating individuals by leveraging a biometric database [6].

1. Biometric System

Biometrics are physical or behavioral features of people that can be used to digitally identify them and enable them access to systems, devices, or data. Biometrics is the study of people's unique physical and behavioral features through measurement and statistical analysis. The technology is mostly used for identification and access control, as well as identifying people who are being watched. The underlying idea of biometric authenticationis that each individual can be precisely identified based on their physical or behavioral characteristics [7]. The adoption of e-commerce applications, eaadhaar, and other similar technologies is on the rise these days. As a result, there is a requirement for secure network transactions as well as data kept in databases [8]. Because each portion of biometric contact to preview data, all data is stored in the database, this research will focus on the kind of biometric to illustrate how biometric databases work in biometric authentication [9]. Biometric authentication is employed for identity verification and access control, as well as for tracking individuals within monitored groups. Biometric identifiers, which are unique and measurable characteristics used to label and differentiate individuals, play a pivotal role in this process. The utilization of biometrics enhances the security of the system's authentication. Please refer to Figure (1) for an illustration of the biometric database system [10,11].

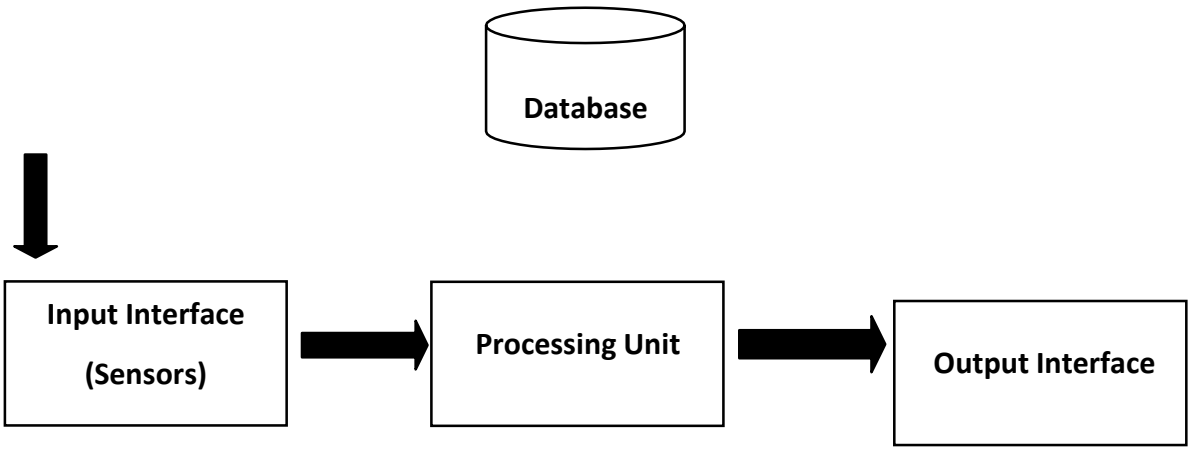

Figure: Biometric Database System.

Biometric identification technology has become increasingly common in our daily lives asthe demand for information security and security legislation has grown around the world. Due to its potential to overcome several fundamental constraints of unimodal bio- metric systems, multimodal biometrics technology has garnered interest and popularity inthis respect [12]. In this review paper, we will focus on several types of biometric authentication to examinecertain articles, each of which employed one or more databases. Figure 2 shown the types of biometrics system. Biometric authentication helps a human recognize someone in security, and it is the best approach to recognize someone to verify that person. In this review, focus on this type of biometrics authentication:

- ✓ Face recognition
- ✓ Fingerprint identification
- ✓ Iris Recognition
- ✓ Speaker Recognition
- ✓ Gait Recognition
- ✓ Ear Recognition
- ✓ Hand Scanning

Figure 2: Type of Biometrics System.

For this work, the authors used this topic and reviewed some papers for each one, each of which had a different outcome. After reviewing the papers, the researcher presented the outcome in the form of a table, text, or figure. Finally, show what this topic is about and why this particular aspect of biometrics is significant. Apart from this topic in biometric authentication having some part or field like above, everything that is utilized same as in biometric authentication, when each part has some paper about it, but not reviewed in thispaper, may be reviewed in future work, working in this filed like DNA [13].

2.1.Face recognition

Face recognition is a technique for recognizing or validating an individual's identificationby looking at their face. Face recognition software can identify persons in photographs, videos, or in real time. During police stops, officers may use mobile devices to identify persons. Face recognition software uses computer algorithms to identify specific, distinguishing features on a person's face. These features, such as eye distance or chin shape,are then transformed into a mathematical representation and compared to data from other faces in a face recognition database. A face template is data on a specific face that differs from an image in that it is designed toonly include certain traits that can be used to recognize one face from another. Face recognition technology has been utilized in airports, border crossings, and sporting events such as the Olympics. Face recognition may also be utilized in private locations such as businesses and sports stadiums, although private sector face recognition may be subject to various restrictions [8]. In this review paper, we will look at some papers on face recognition techniques and illustrate how they operate, as well as the methods they use to recognize faces, because eacharticle uses a different approach to identify faces and detect people using biometric systems. Figure 3 show face recognition.

Figure 3: Face Recognition

M. Azimi is Effects of Facial Mood Expressions on Face Biometric Recognition System'sReliability, we gave a one-by-one comparison of all samples from all moods in that paperin order to answer the following questions: 1- Is there a statistically significant difference in matching scores across

samples with various emotional facial expressions? (Which mood is more likely to jeopardize the system's reliability than others?) 2- From the stand-point of the biometric system, what are the best and worst comparison scenarios for each mood? Images with various expressions from the Jaffe Database were utilized to answer the first and second questions. It is vital to notice that in the final answer to the first question, less face-distance indicatesmore matching score, and the best matching score has been attained for the neutral vs. neutral comparison, and answered second question, all feasible comparison scenarios werecompared (normal vs normal, anger vs anger, fear vs fear, happy vs happy, sad vs sad, surprised vs surprised, and fear vs fear) [14]. M. Singh is Multimodal Biometric Database DMCSv1(Data Management and Control System version 1) of 3D Face and Hand Scans, The DMCSv1 multimodal biometric database of 3D face and hand scans is presented in this article. The data was gathered for face, hand, and multimodal recognition research. Struc-tured light technology was used to compile the database. Using the DMCSv1 database, this article used a face and hand biometric method to identify people [15]. O.C. Kurban is A Multi-Biometric Recognition System Based on Deep Features of Faceand Gesture Energy Images, in that paper, the Eircom Kinect Face dataset and the Body Login Gesture Silhouettes dataset were combined with score level to generate a virtual dataset. The VGG (Visual Geometry Group) Face deep learning model was used for the face database. Technique for energy imaging was used to extract and obtain signal characteristics. While the study used CNNs (Convolutional Neural Networks.) and deep learning, a set of machine learning methods known as “deep learning” make use of components of nonlinear transformation models in an attempt to simulate high-level data abstraction. The CNN model is one of the deep learning constructs for computer vision [16].

2.2.Fingerprint identification

One of the most well-known and well-publicized biometrics is fingerprint identification. Fingerprints have been used for identification for over a century due to their unique- ness and constancy through time, but have only recently become automated (i.e. a bio- metric) due to advances in computing power. The high, peaked component of the friction ridge skin shows a sequence of dark lines, while the valley between these ridges appears as white space and represents the low, shallow component of the friction ridge skin [17]. The minutiae, or the location and direction of ridge ends and bifurcations (splits)along a ridge path, are used to identify it [18]. Figure 4 shows a block diagram of a typical Auto-Matic Fingerprint Verification system.

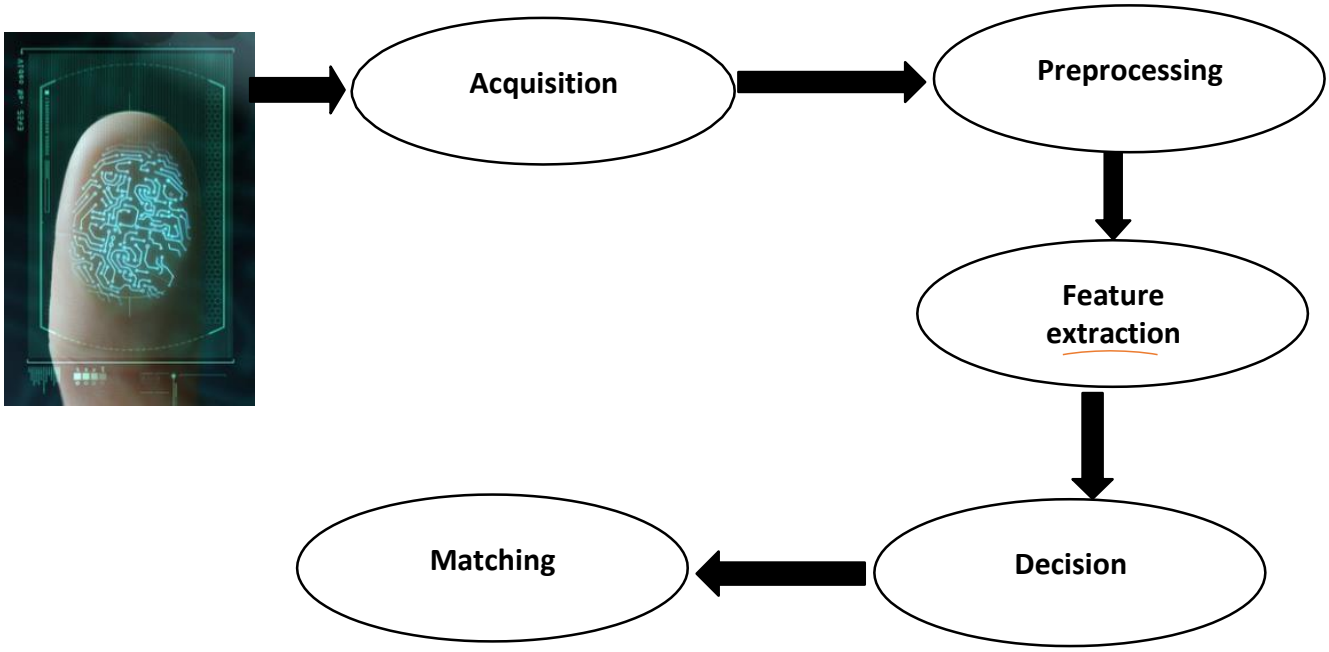

Figure 4: Fingerprint Identification.

Several articles were utilized to review each article, and each article employed some approach or approach to biometric Fingerprint recognition. P. A. and S. D. are Fingerprint Indexing Approaches for Biometric Database, when it is reviewing article work in gives a survey of the current fingerprint indexing methods, as well as examples of several of them. The local ridge line orientation, global feature, minutiae, and other features are used to index fingerprints [19]. That article shows some algorithms used in Fingerprint Indexing, other hand reviewing some articles, shows each article Summary on fingerprint indexing approaches for rolled, plain and latent prints. OF: orientation field, SP: singular points, SIFT: scale invariant feature transform, MCC: minutia cylinder code, RF: ridge frequency, HR: hit rate, PR: penetration rate. Table 1 shows the summary on fingerprint indexing algorithms for rolled, plain, and latent fingerprints.

Table 1: Summary on fingerprint indexing approaches for rolled, plain and latent prints. OF: orientation field, SP: singular points, SIFT: scale invariant feature transform, MCC:

minutia cylinder code, RF: ridge frequency, HR: hit rate, PR: penetration rate [19].

	Authors	Fingerprint Features	Approach	Fingerprint Database	HR @ PR =10%
Rolled	Bhanu and Tan [6]	Minutiae	Triplets	] 2,000 queries and 2,000 templates (NIST SD4)	85.5%
	Wang et al. [17]	OF	Fingerprint Orientation Model based on 2D Fourier Expansion	2,700 queries and 2,700 templates (last 2,700 pairs of NIST SD14)	98%
	Cappelli et al. [9]	Minutiae	MCC	2,700 queries and 24,000 templates (NIST SD14)	95%
	Cappelli [13]	OF + RF		1,000 queries and 1,000,000 templates (generated by SFinGe v4.1)	99.6%
Plain	Bhanu and Tan [6]	Minutiae	Triplets	400 queries and 600 templates (collected by FIU-500-F01 sensor)	100%
	Liang et al.[7]	Minutiae	Triplets	550 queries and 330 templates (FVC2004 DB1)	99%
	Wang et al. [17]	OF	Fingerprint Orientation Model based on 2D Fourier Expansion	Queries and templates not indicated (FVC2002 DB1a)	99.9%
	Shuai et al. [21]	SIFT		500 queries and 300 templates (FVC2000 DB2a)	98%

	Cappelli et al. [9]	Minutiae	MCC	700 queries and 100 templates (FVC2002 DB1a) 99%	99%

2.3 Iris Recognition

Iris Recognition is a biometric way of identifying persons based on distinctive patternsin the ring-shaped portion of the eyeball surrounding the pupil. Because each iris is uniqueto a person, it's an excellent biometric verification tool. A specialized digital camera is used in the Iris Recognition procedure. The camera will take a clean, high-contrast pictureof a person's iris using both visible and near-infrared light. The camera focuses on your eye and locates the center of the pupil, edge of the pupil, edge of the iris, and your eyelids and eyelashes with Iris Recognition. Iris Recognition is one of the most accurate kinds of biometric authentication, and NEC's Iris Recognition technology has been named the most accurate in the industry [20] [21]. For iris, recognition used some techniques like:

- Pupil detection: - The pupil needs to be detected and removed from the acquired eyeimage since only the iris pattern is used for matching purposes.
- Iris detection: - Using an intensity variation technique, the outer iris boundary is discovered.
- Normalization: - The strip is created from the localized iris picture.
- Feature extraction: - The iris' distinctive qualities are determined by extracting the image's features or values.
- Matching: - The iris codes (IC) generated for the database and query photos are compared using the hamming distance method.

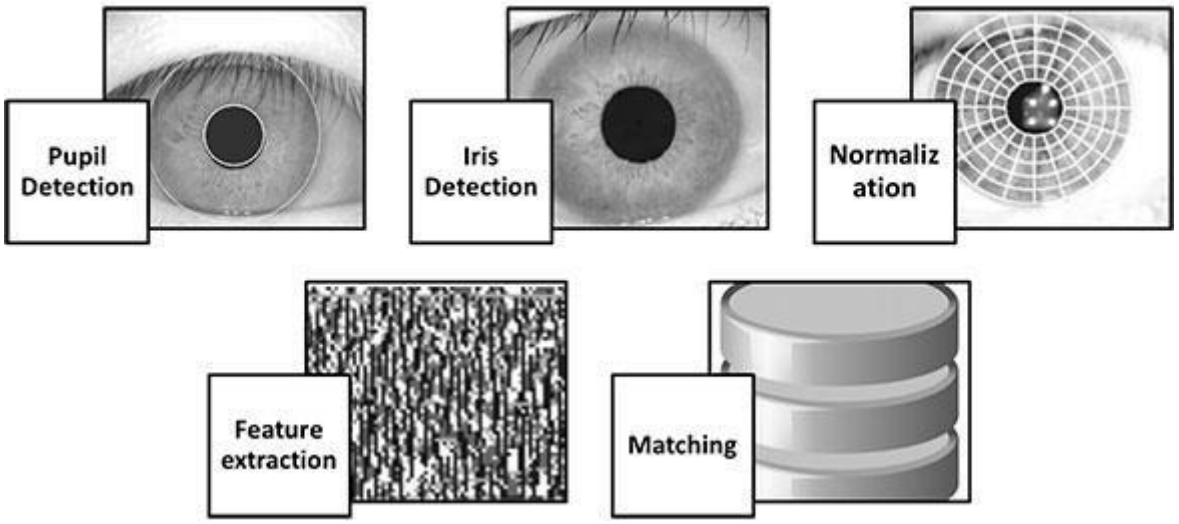

Figure 5: Iris Recognition Technique

For iris recognition in biometrics, use or review several articles to see how other researchers worked on this subject and what approach they used to recognize iris. This review has an article on iris biometric recognition Iris Recognition System: A Novel Approach for Biometric Authentication, the form, intensity, and localization of the pupil and iris were used in the proposed method in the article. The normalization technique converts the segmented region into a rectangular rectangle. The texture-based feature is extracted using the Gray Level Co-occurrence Matrix (GLCM) and Hausdorff Dimension (HD). A supervised SVM machine learning technique was used to classify the retrieved characteristics. The suggested approach is broken down into two stages: enrollment and verification. In the enrollment phase, the individual's iris image is enrolled, and in the recognition phase, the enrolled individual is authenticated by checking his or her iris pattern or characteristic [20]. In these article two Tables; first table compares the result with other methods show in Table 2 and Table 1 the result shows the result for his paper in the field of Sensitivity, Specificity and Accuracy shown in Table 3.

Table 2: Compares of Accuracy of The Proposed System with The Other Methods [20].

N	**Methodology**	**Accuracy (%)**
1	Artificial Neural Network	83.65
2	Support Vector Machine	90.25
3	Proposed System	93.75

Table 3: Results in Terms of Sensitivity, Specificity and Accuracy [20].

Database	**Sensitivity**	**Specificity**	**Accuracy**
CASIA	87.50 %	100 %	93.75 %

2.4 Speaker Recognition

Speaker Recognition is the process of automatically detecting who is speaking by analyzing the speaker- specific information included in voice waves to authenticate the identities of persons using systems. Speaker identification and speaker verification are two types of speaker recognition. The technique of determining from which of the registered speakers a given speech originates is known as speaker identification. The practice of recognizing or rejecting a speaker's asserted identification is known as speaker verification. The majority of applications that use speech to validate a speaker's identification are classified [22]. Speaker recognition is a biometric technique that employs the

speech samples of individualspeakers as input for recognition. The main purpose of this project is to improve the accuracy of a speaker recognition system for a huge speech database [23].

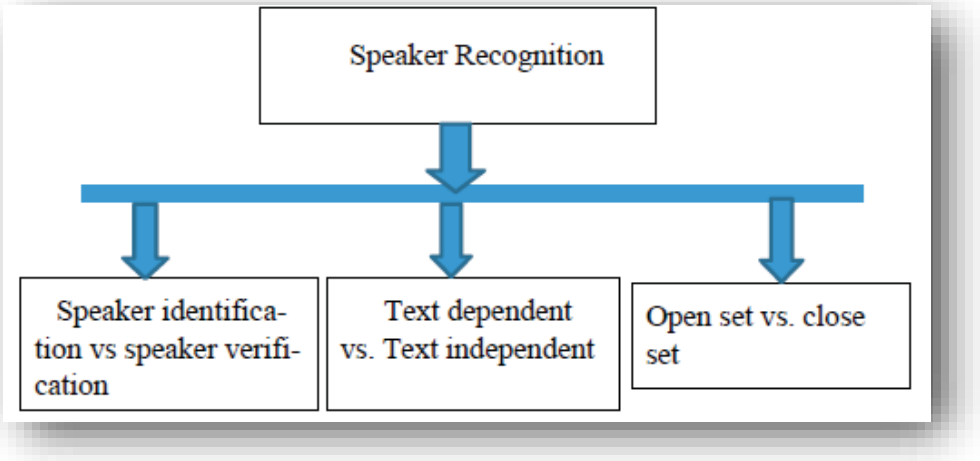

Figure 6: Classification of Speaker Recognition System [24].

This review of speaker identification systems in biometric identification is based on a fewarticles, each of which employed a different method for identifying speakers and finding them in databases. In this review, we used an article that was relevant to our work. A comparison of various combinations of characteristics for a speaker identification system utilizing feedforward artificial neural network (FFANN) and support vector machine (SVM) for 10 and 20 speakers is made in that paper All of the results in the paper can be found in Table (4), which shows compression between artificial neural network (ANN) and SVM when different data and methods are used [24].

Table 4: Different Data and Methods Used in ANN and SVM [24].

Features used	**Accuracy-10 speakers- ANN (320 voices)**	**Accuracy-20 speakers – ANN (640 voices)**	**Accuracy 10 speakers- SVM (320 voices)**	**Accuracy 20 Speakers SVM (640voices)**
MFCC	85.3 %	76.4 %	64.4 5	62.5 %
LPC	80 %	70.5 %	71.6 %	64.4 5 %
ZCR	63.1 5 %	50 %	48.1 5	37.1 %
MFCC +ZCR	86 %	87.3 %	70.6 %	71.7 %

LPC +ZCR	89.1 %	84.2 %	74.2 %	71.9 %
MFCC+LBC	91 %	86.9 %	80.6 %	78.8 %
MFCC+ LPC +ZCR	92.8 %	93.1 %	79.1 %	57.1 %

After showing the above table when using Mel-Frequency Cepstral Coefficients (MFCC), Linear Predictive Coding (LPC), and Zero Crossing Rate (ZCR) characteristics together asan input with an ANN classifier, the accuracy of the system does not suffer when the number of speakers is increased from 10 to 20. But when the number of input speech samples rises, the accuracy of SVM drops. When comparing the results of ANN with SVM, it can be concluded that ANN with MFCC, LPC, and ZCR provides superior accuracy, even though the database size is larger. As a result, we can consider thisresult valuable in the field of speaker recognition research [24].

2.5 Gait Recognition

One of the biometric identification technologies, gait recognition, has received a lot of interest. There have been numerous suggestions that a person's walking style is a distinct behavioral trait that can be used as a biometric. Differing from other biometric identification technologies like facial recognition, gait recognition is widely recognized as the most essential noncontact able, noninvasive biometric identification technique that is difficult to duplicate. Gait recognition is likely to be used in settings such as criminal investigation and access control because of these benefits [25]. S. M. Darkish has developed a multi-model biometric authentication database specifically for human gait recognition. This database differs from existing ones in the literature as it utilizes wearable sensors and a smartphone to capture gait data. Unlike the commonly used databases, which rely on machine vision, floor sensor-based, or wearable sensor approaches, this database offers a unique combination of technology for gait recognition research. [26]. in this study, various results were obtained, including Equal Error Rate (EER) values for five wearable sensors located at different positions. These EER values ranged from 0.17 percent to 2.27 percent across different walking scenarios. However, the EER results for smartphone data varied from 1.23 percent to 4.07 percent. Additionally, the average Genuine Reject Rate (GRR) of sensors positioned on the leg, pocket, and hand decreased as the age group increased. Interestingly, no discernible trend was observed for sensors placed in the upper pocket [27].

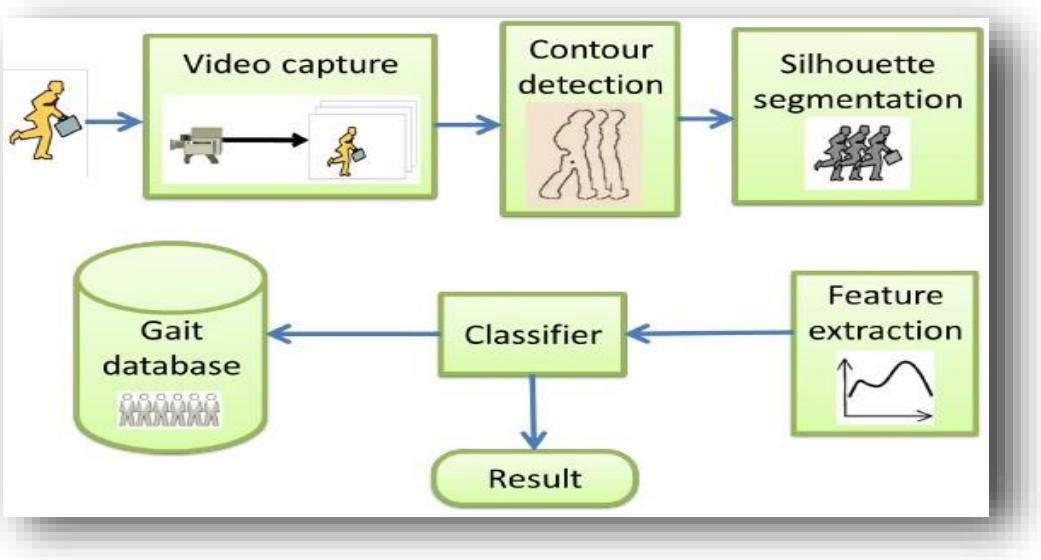

Figure 7: Gait Recognition Technique [27].

2.6 Ear Recognition

With the progress of technology, people are paying greater attention to biometrics recognition. The human ear is a fantastic source of information for passive personrecognition. Because the ear is visible, photographs are easy to capture, and the structure of the ear does not change much over time, it appears to be a good potential solution [28]. Ear biometrics is becoming increasingly popular as one of the most significant biometrics. When combined with other biometrics, ear recognition has distinct advantages that can make identification safer and trustworthy (e.g. face and fingerprint). The human ear is a relatively new class of relatively stable biometrics that has recently attracted the interest of researchers [29]. There are several articles concerning ear biometrics in this section, but just one was used in this review, in that article, in a multimodal biometric recognition system, numerous information derived from distinct biometric modalities is combined to alleviate the variouslimitations experienced in a unimodal biometric system. At the feature level, a new multimodal biometric system based on ECG-ear-iris biometrics is suggested. ECG, ear, and iris biometrics are subjected to preprocessing techniques such as normalization and segmentation. To extract the key characteristics from the ECG signal and convert the ear and iris images to a 1D signal, local texture descriptors such as 1D-LBP (One D-Local Binary Patterns), Shifted-1D-LBP, and 1D-MR-LBP (Multi-Resolution) are employed. To classify an unknown user as real or imposter, KNN and RBF are employed for matching. This article works in some steps to get results, all steps shown in Figure (2). The results of the experiments show that the suggested method outperforms a unimodal biometric system. With an Equal Error Rate (EER) of 0.5 percent, a Correct Recognition Rate (CRR) of 100 percent is attained [30].

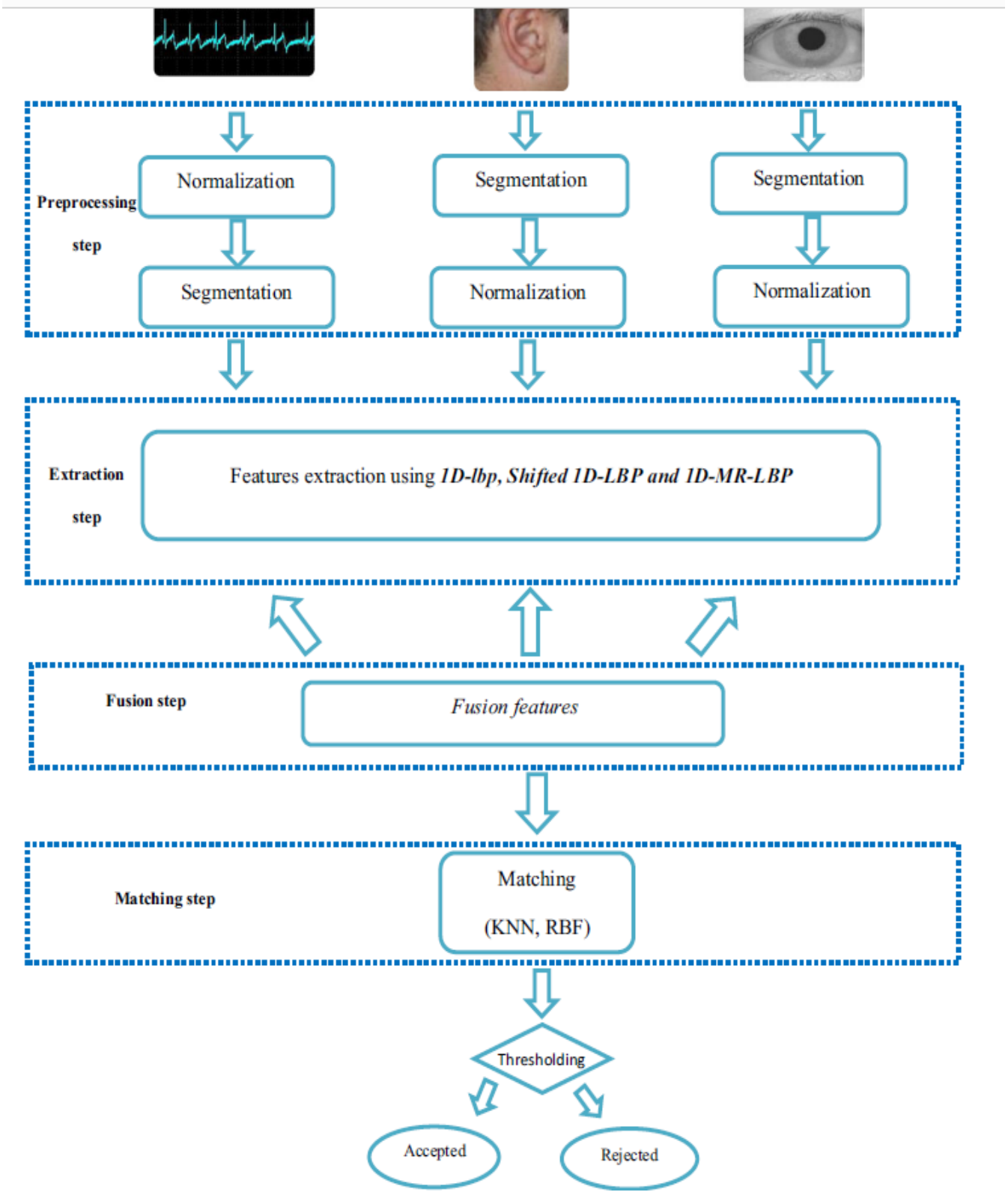

Figure 8: The Proposed Recognition Process [30].

2.7 Hand Scanning

Biometrics researchers discovered that the human hand, particularly the palm, has specific traits that can be used for personal identification. The thickness of the palm area, as well as the width, thickness, and length of the fingers, are among these characteristics. These qualities are used by a large number of commercial systems in a variety of applications. Biometrics based on hand geometry is not a new concept. It is older than palm print, which is part of dactyloscopy, and was originally referenced in the early 1970sof the twentieth century. The first known application was on Wall Street for security checks [31]. Although the human hand has enough anatomical traits to allow for personal identification, it is not deemed unique enough to allow for comprehensive personal identification. Hand geometry changes throughout time, and the shape of the hand can vary as a result of disease, aging, or weight fluctuations. It is based on the fact that everyone's hands are made uniquely [32]. In hand biometrics, the first group is regarded as the traditional approach. Because it is a part of dactiloscopy, the techniques utilized are similar to those used for fingerprints. The size, shape, and flow of papillae are all measured, and minutiae are the most important characteristics to look for during the identification procedure. Figure 3 shows how a biometric system based on hand form works. Hand shape data is collected from registered users during the registration step, and feature sets are derived from the collected data. Per person, data and one or more templates are computed. and then saved in a database [33].

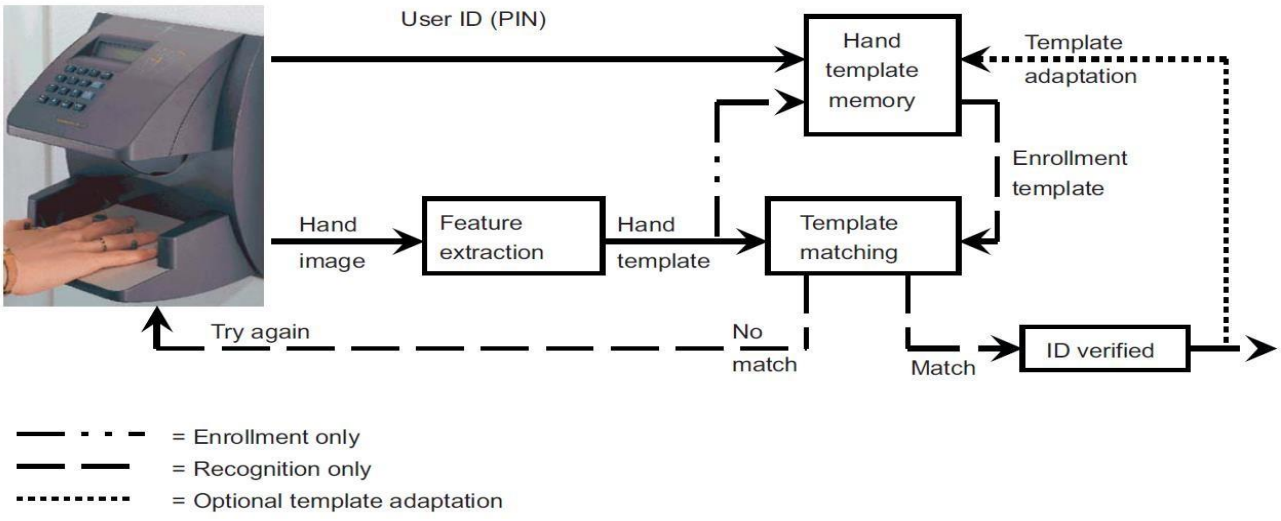

Figure 9: Hand Scanning Method [33].

Conclusions

Biometric identification has arisen as a means of controlling access to both physical and virtual areas in a precise manner. Biometric characteristics, such as digital imprint probes, face probes, voice probes, and so on, are increasingly being employed as alternatives to passwords, PINs, and visual verification techniques. This review paper gives a comprehensive security analysis of the match-in-database biometric technology. It examines the present threat models and suggests a more comprehensive threat model. Thisreview paper examines a portion of the biometric database system. After going through all of the parts, you may find some facts in this section. First, this area gives greater authority to the authentication person and is employed in the security area. Scorned The minimal frequency of inaccuracy in this review allows us to have unique identification for each person. End users do not have to remember their code or anything like that. amount of pinsthe user can benefit from all-factor authentication in this situation. Secure authentication, a focus on a decentralized database, and ensures that the data in the database is correct and complete.

References

[1] D. Jagadiswary, D. Jagadiswary, Biometric authentication using fused multimodal biometric, Pro. Sci., 85(2016)109-116, https://doi.org/10.1016/j.procs.2016.05.187

[2] R. Jain, C Kant, Attacks on biometric systems: an overview, Int. J Adv. Sci. Res., 1(2015)283-288, https://doi.org/10.7439/IJASR.V1I7.1975

[3] P. Tsai, T.P. Tran, L. Cao, a New Multimodal Biometric for Personal Identification, InTech. ,17(2010)342-366, https://doi.org/10.5772/9370

[4] W. Kabir, M.O. Ahmad, M.N.S. Swamy, A novel normalization technique for multimodal biometric systems,(MWSCAS),58th(2015)1-4. https://doi.org/10.1109/MWSCAS.2015.7282214

[5] I.D. Judith, G.J. Mary, M.M. Susanna, Three factor biometric authentication for spiraling of security. (ICETETS), (2016) 1-3, https://doi.org/10.1109/ICETETS.2016.7603017

[6] H.B. Jaafar, N.B. Mukahar, D.A.B. Ramli, December. A methodology of nearest neighbor: Design and comparison of biometric image database, (SCOReD) (2016)1-6, https://doi.org/10.1109/SCORED.2016.7810073

[7] A.D. Algarni, G. El. Banby, S. Ismail, W. El-Shafai, F.E.A. El-Samie, N. F. Soliman, Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications, Entropy, 22(2020)13-61, https://doi.org/10.3390/e22121361

[8] Z. Akhtar, G. Kumar, S. Bakshi, H. Proenca, Experiments with ocular biometric datasets: A practitioner's guideline, IT Professional, 20(2018)50-63,

https://doi.org/10.1109/MITP.2018.032501748

[9] A. Lumini, L. Nanni, Overview of the combination of biometric matchers, Information Fusion, 33(2017)71-85, https://doi.org/10.1016/j.inffus.2016.05.003

[10] E. Bartuzi , K. Roszczewska, M. Trokielewicz, R. Białobrzeski, Mobibits: Multimodal mobile biometric database. (BIOSIG), (2018)1-5, https://doi.org/10.23919/BIOSIG.2018.8553108

[11] N. Alay, H.H. Al-Baity, Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. Sensors, 20(2020)23-55. https://doi.org/1424-8220/20/19/5523

[12] Manisha, N. Kumar, Cancelable biometrics: a comprehensive survey. Artificial Intelligence Review, 53(2020)3403-3446, https://doi.org/10.1007/s10462-019-09767-8

[13] M. Azimi, Effects of Facial Mood Expressions on Face Biometric Recognition System's Reliability.(ARES),1st(2018)1-5, https://doi.org/10.1109/ARESX.2018.8723292

[14] M. M. Singh, R. Singh, A. Ross, A comprehensive overview of biometric fusion. Information Fusion, 52(2019)187-205, https://doi.org/10.1016/j.inffus.2018.12.003.

[15] O.C. Kurban, T. Yildirim, A. Bilgic, A multi-biometric recognition system based on deep features of face and gesture energy image. (INISTA), (2017) 361-364, https://doi.org/10.1109/INISTA.2017.8001186.

[16] M. Joshi, B. Mazumdar, S. Dey, A comprehensive security analysis of match-in-database fingerprint biometric system, Pattern Recognit. Lett, 138(2020)247-266., https://doi.org/10.1016/j.patrec.2020.07.024

[17] N. Singla, M. Kaur, S. Sofat, ,. Latent fingerprint database using reflected ultra violet imaging system. Procedia Comput. Sci, 167(2020)942-951, https://doi.org/10.1016/j.procs.2020.03.393

[18] P.A. Parmar, S.D. Degadwala, Fingerprint indexing approaches for biometric database: a review. Int. J. Comput. Appl. Technol, 130(2015)10-5120, https://doi.org/10.5120/ijca2015907150

[19] R. Shelke, S.B. Bagal, Iris recognition system: a novel approach for biometric authentication. (ICCUBEA) (2017)1-5 https://doi.org/10.1109/ICCUBEA.2017.8463819

[20] V. Rajasekar, J. Premalatha, K. Sathya, Enhanced biometric recognition for secure authentication using iris preprocessing and hyperelliptic curve cryptography. Wireless Commun. Mobile Compu., (2020)1-15, https://doi.org/10.1155/2020/8841021

[21] P. Korshunov, S. Marcel, Impact of score fusion on voice biometrics and presentation attack detection in cross-database evaluations, IEEE J. Sel. Top. Signal Process, 11(2017)695-705, https://doi.org/10.1109/JSTSP.2017.2692389

[22] X. Zhang, Q. Xiong, Y. Dai, X. Xu, Voice biometric identity authentication system based on android smart phone,(ICCC) (2018)1440-1444, https://doi.org/10.1109/CompComm.2018.8780990

[23] N. Chauhan, T. Isshiki, D. Li, Speaker recognition using LPC, MFCC, ZCR features with ANN and SVM classifier for large input database, (ICCCS) (2019)130-133, https://doi.org/10.1109/CCOMS.2019.8821751

[24] R.D. Labati, , A. Genovese, E. Munoz, , V. Piuri, , F. Scotti, G. Sforza, Advanced design of automated border control gates: biometric system techniques and research trends. (ISSE) (2015)412-419, https://doi.org/10.1109/SysEng.2015.7302791

[25] S.M. Darwish, Design of adaptive biometric gait recognition algorithm with free walking directions, IET Biom, 6(2017) 53-60, https://doi.org/10.1049/iet-bmt.2015.0082

[26] S.K. Al Kork, I. Gowthami, X. Savatier, T. Beyrouthy, J.A. Korbane, S. Roshdi, Biometric database for human gait recognition using wearable sensors and a smartphone. (BioSMART) (2017)1-4, https://doi.org/10.1109/BIOSMART.2017.8095329

[27] T.K. Thivakaran, S.V.V.N. Ch. Padira, A.S. Kumar, S.S. Reddy, Fusion Based Multimodel Biometric Authentication System using Ear and Fingerprint, (IJIES),12(2019), https://doi.org/10.22266/IJIES2019.0228.07

[28] Ž. Emeršič, P. Peer, Toolbox for ear biometric recognition evaluation, (EUROCON) (2015)1-6, https://doi.org/10.1109/EUROCON.2015.7313758

[29] M. Regouid, M. Touahria, M.Benouis, N. Costen, Multimodal biometric system for ECG, ear and iris recognition based on local descriptors, Multimedia Tools Appl.,78(2019)22509-22535, https://doi.org/10.1007/s11042-019-7467-x

[30] A. Hassanat, M. Al-Awadi, E. Btoush, A. Al-Btoush, E.A. Alhasanat, G. Altarawneh, New mobile phone and webcam hand images databases for personal authentication and identification, Procedia Manuf., 3(2015)4060-4067, https://doi.org/10.1016/j.promfg.2015.07.977.

[31] A. Selwal, S.K. Gupta, Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry, Perspect. Sci., 8(2016)705-708, https://doi.org/10.1016/j.pisc.2016.06.065

[32] W. Sankowski, P.S. Nowak, P. Krotewicz, Multimodal biometric database dmcsv1 of 3d face and hand scans, (MIXDES) (2015)93-97, https://doi.org/10.1109/MIXDES.2015.7208488

[33] S.A. Abdulrahman, B. Alhayani, A comprehensive survey on the biometric systems based on physiological and behavioural characteristics, Mater. Today Proc., 80(2023) 2642-2646, https: doi.org/10.1016/j.matpr.2021.07.005.

[34] S. Dargan, M. Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Syst. Appl., 143(2020)113-114. https://doi.org/10.1016/j.eswa.2019.113114.

[35] M.Y. Shams, Hybrid neural networks in generic biometric system: A survey, (JAIM), 1(2022) 1-20. https://doi.org/10.54216/JAIM.010102.

[36] A. Sarkar, B.K. Singh, A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools Appl., 79(2020), 27721-27776. https://doi.org/10.1007/s11042-020-09197-7

[37] B. Alhayani, S.T. Abbas, D.Z. Khutar, H.J. Nd. Mohammed, Best ways computation intelligent of face cyber-attacks. Mater. Today Proc, (2021)26-31, https://doi.org/10.1016/j.matpr.2021.02.557

[38] J.S. Ahmed, H.J. Mohammed, I.Z. Chaloob, Application of a fuzzy multi-objective defuzzification method to solve a transportation problem, Mater. Today Proc., (2021)2214-7853. https://doi.org/10.1016/j.matpr.2020.12.1062.

[39] H.A. Daham, H.J. Mohammed, An evolutionary algorithm approach for vehicle routing problems with backhauls, Mater. Today Proc.,(2021) 2214-7853, https://doi.org/10.1016/j.matpr.2020.12.1028

[40] R. Yamashita, D. Oshimi May,The motivations for and barriers to academic conference attendance: Insights from an international sport management conference, J. Conv. Event Tour., 24(2023), 294-312, https://doi.org/10.1080/15470148.2023.2205184

[41] V. Veeraiah, K.R. Kumar, P.L. Kumari, S. Ahamad, , R. Bansal, A. Gupta, Application of biometric system to enhance the security in virtual world. (ICACITE), (2022)719-723, https://doi.org/10.1109/ICACITE53722.2022.9823850

[42] R.A. Hamaamin, S.H. Wady, A.W.K. Sangawi, COVID-19 Classification based on Neutrosophic Set Transfer Learning Approach. UHD, 6(2022) 11-18, https://doi.org/10.21928/uhdjst.v6n2y2022.pp11-18

[43] T. De Freitas Pereira, S. Marcel, Fairness in biometrics: a figure of merit to assess biometric verification systems. IEEE Trans. Biom. Behav. Identity Sci., 4(2021)19-29. https://doi.org/10.1109/TBIOM.2021.3102862

[44] O.M.A. O. Ali, S.W. Kareem, A.S. Mohammed Evaluation of electrocardiogram signals classification using CNN, SVM, and LSTM algorithm: A review. (IEC) (2022)185-191. https://doi.org/10.1109/IEC54822.2022.9807511

[45] K. Shaheed, P. Szczuko, M. Kumar, I. Qureshi, Q. Abbas, I. Ullah, Deep learning techniques for biometric security: A systematic review of presentation attack detection systems. Eng. Appl. Artif. Intell., 129(2024)107569, https://doi.org/10.1016/j.engappai.2023.107569

[46] M. Carvalho, S. Brás, Addressing intra-subject variability in electrocardiogram-based biometric systems through a hybrid architecture. Biomed. Signal Process. Control, 87(2024)105465. https://doi.org/10.1016/j.bspc.2023.105465

[47] Kokal, Sara, M. Vanamala, R. Dave. "Deep Learning and Machine Learning, Better Together Than Apart: A Review on Biometrics Mobile Authentication, (JCP), 3(2023)227-258. https://doi.org/10.3390/jcp3020013

[48] M. Rahman, A. Murmu, P. Kumar, N.R. Moparthi, S. Namasudra, A novel compression-based 2D-chaotic sine map for enhancing privacy and security of biometric identification systems, J. Inf. Secur. Appl., 80(2024)103677. https://doi.org/10.1016/j.jisa.2023.103677

[49] L. D. Silva, Maria, C. Gouveia, D. F. Albuquerque, H. P. D. Silva., Radar-Based Invisible Biometric Authentication, Info., 15(2024)1-44. https://doi.org/10.3390/info15010044.

الأنظمة البيومترية: مراجعة شاملة

ريبين عبدالكريم حمەأمين[1]
عمر محمدامين على[2]
شهاب وهاب كريم[3]
1. قسم علوم الحاسوب، كلية العلوم، جامعة جرمو، جمجمال، السليمانية، إقليم كوردستان، العراق.
2. قسم تكنولوجيا المعلومات، معهد جمجمال التقني، جامعة السليمانية التقنية، جمجمال، السليمانية، اقليم كوردستان، العراق.
3. قسم هندسة نظم المعلومات التقنية، كلية الهندسة التقنية، جامعة أربيل التقنية، إقليم كوردستان، العراق.

المستخلص

ومع زيادة استخدام البيانات البيومترية، من المتوقع أن تصبح الأنظمة أكثر موثوقية وقدرة على تقديم نتائج ناجحة في المواقف الصعبة وضد التزييف. أمن المعلومات أمر بالغ الأهمية لنجاح أي نظام. ونتيجة لذلك، يلزم اتباع أسلوب صارم للتحقق من هوية كل شخص قبل منحه حق الوصول إلى البيانات المخزنة. وبالتالي يمكن استخدام القياسات الحيوية القابلة للإلغاء لتحسين أمان وخصوصية المستخدمين في مواجهة التهديدات. للسبب المذكور أعلاه، يتم مراجعة نظام قاعدة البيانات البيومترية. يعد التعرف على الوجه، والتعرف على بصمات الأصابع، والتعرف على قزحية العين، والتعرف على السماعات، والتعرف على المشية، والتعرف على الأذن، ومسح اليد، كلها أجزاء من نظام القياسات الحيوية التي تمت مراجعتها ومناقشتها في هذه الورقة. يتضمن كل جزء المصادقة على قاعدة البيانات البيومترية. لكل جزء، سنراجع مقالًا ونناقش نتائج تلك الورقة في مراجعتنا. للتوثيق، تعمل جميع الأقسام في قاعدة بيانات بيومترية مخزنة.