2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)
Department of Electrical & Electronics Engineering, Galgotias College of Engineering and Technology, Gr. Noida, India

2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-7281-7741-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICACITE51222.2021.9404735

A Study of Biometric Identification and Verification System

Vandana
Chitkara University Institute of Engineering and Technology,
Chitkara University, Punjab
Punjab, India
vandana.bajaj@chitkara.edu.in

Navdeep Kaur
SGGSW University, Fatehgarh Sahib
Punjab, India
Drnavdeep.sggswu@gmail.com

***Abstract*— Conventionally, the identification of users is performed using passwords and PIN numbers. However, due to the rapid changes in technology, these security measure's abuse and theft are also increasing. This led to the birth of the biometric security system, in which the identity verification of individuals is performed based on the feature vectors, which are derived from the physiological and/or behavioral characteristics of humans. The categorization of a biometric system is done as per the number of traits utilization for authentication purposes. There are various available methods for identification such as Face Recognition, Iris Recognition, Voice Recognition, Fingerprint Recognition, etc. As per advancement in technology, information security becomes a major challenge of the IT industry. Thus, authentication plays an important role to deals with security. The key objective of this scheme is to ensure that the rendered services are accessible only by the authorized user and not by an illegal person. Using biometrics, an individual's identity can be confirmed or established. In this paper, a comparative survey of uni and the multi-modal biometric system is presented, and analysis is performed to know the best system. The purpose is to analyze the latest technology based on the progress made and unresolved issues. A general overview of the biometric recognition system is presented, along with the performance, parameters is presented. In addition to the single-modal system, this article also discusses the multi-modal biometric system and its traditional approaches along with the information fusion level. This article highlights the potential, market value, and prospects of biometric technology.**

Keywords*— *Biometric System, Uni-Modal, Multi-modal, authentication, verification, performance metrics

I. INTRODUCTION

With the advancement of Information Technology (IT), the need for security becomes a major issue in the IT sector. Security can be managed in many ways. One way to improve security is to identify or validate a person with a particular technique. Biometric systems are utilized for the identification and verifying of person characteristics using biological and behavioral kinds. A biometric identifier is a unique and measurable feature used to mark and describe an individual [1]. There are two biometrics types: physiological and behavioral characteristics. Faces, fingerprints, veins, and speech are the most reliable and secure approaches to traditional approaches, such as knowledge-based and token-based techniques. This is because the forgotten and stolen probability of biometric traits is less [2]. Types of biometric traits are shown in Fig. 1.

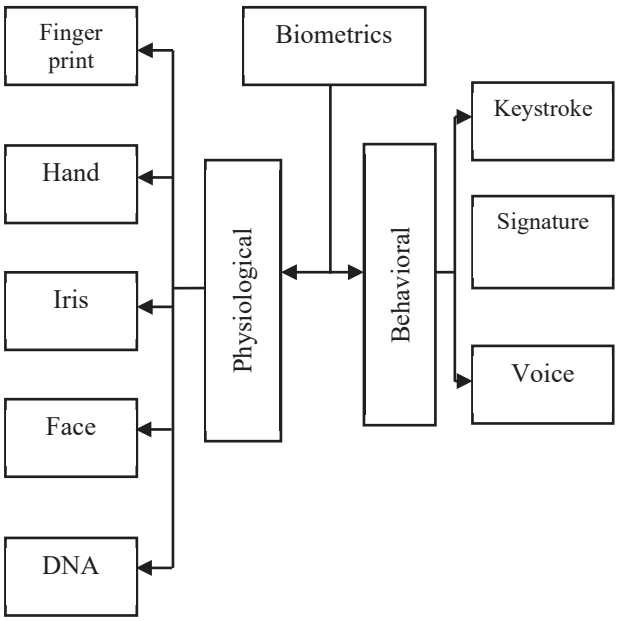

Fig. 1. Biometric traits [3]

Unibiometeric system suffers from problems such as variation in biometric data, low recognition rate, spoofed easily, and many more. To overcome these problems, a multi-model biometric system is designed that used two or more than two biometric traits and results in a higher recognition rate. The input from multiple traits is passed to the sensor measuring unit used in the multimodal biometric system. For example, in the case of a multi-modal system that used face and fingerprint trait, the features of fingerprint such as (ridges, arch, loop, etc.), and face such as (nose, forehead, lips, etc.) are passed and used to know whether the same person captures the face and the fingerprint or not [4]. The sensing strategy is also important in healthcare to transmit the vital parameter of patients at a remote location in a secured manner. By which doctors can adequately monitor the patient by reaching at that location [5]. To arrive doctors at the correct location and on time, the best monitoring and management of vehicles is required. As electronic vehicles are very trending, therefore increased human dependency on them [6]. To increase the high prior knowledge of people regarding advancement in technology, computer animations have as highly effective [7].

The rest of the paper is divided into four sections; section 2 describes the working of the biometric authentication system. Section 3 presents the present state of work for both

Authorized licensed use limited to: Carleton University. Downloaded on June 05,2021 at 06:01:35 UTC from IEEE Xplore. Restrictions apply.

uni and multimodal biometric system. Section 4 represents the conclusion followed by the references.

II. Biometeric Authentication System

Biometric is a pattern identification system that identifies a person's identity by matching features, either biological or behavioral, of biometric traits. Biometric characteristics are a very convenient way to authenticate a person, as they have a high degree of security (challenging to forge) and cannot be stolen, forgotten, or lost [8].

A Biometric system can be defined as an automated identification system in which the human being is identified from his/ her unique features. Authentication can be performed in two ways (i) one-to-many (identification), and one-to-one (verification).

Identification: the authentication of an individual is performed by matching the biometric test sample to the trained structure stored in the database.

Verification: the authentication of an individual is performed by matching the test image to the claimed biometric traits in the database [10].

The simple structure of the biometric authentication system is depicted in Fig. 2. The biometric authentication system worked in two steps (i) enrollment and (ii) authentication. Both steps are shown in Fig. 2(a) and Fig. 2 (b), respectively. Both models used three main steps: image sensing, pre-processing and stored the processed image into a matching database.

In the biometric system, verification and identification are the two essential blocks of identifying human beings [11]. Each block is utilized for different applications and distinct conditions, as discussed above. The identification process is more challenging and costly because the decision is taken after matching the image from the stored images in databases. In contrast, in the verification system, one-to-one matching is performed [12].

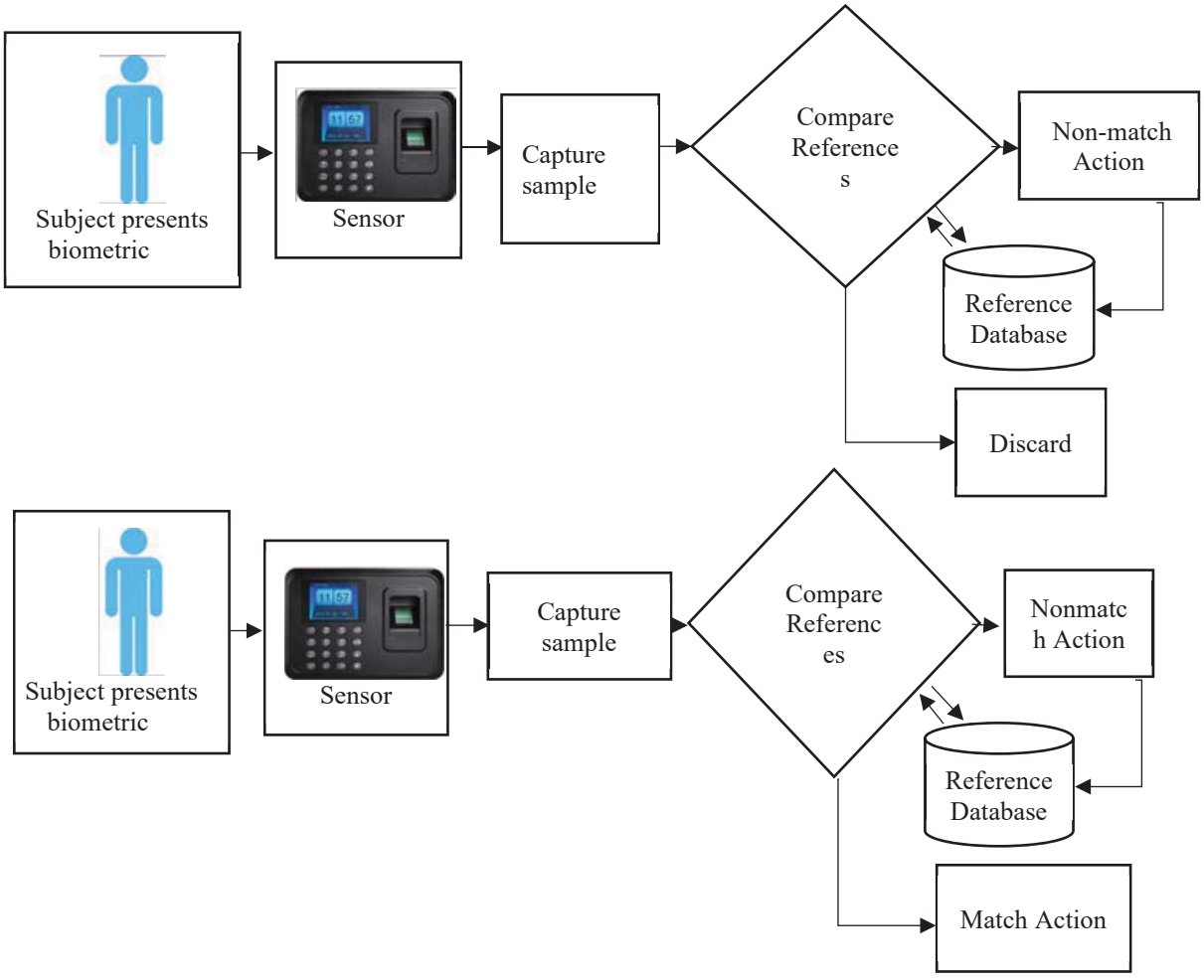

Fig. 2. General Biometric System (a) Enrollment (b) Matching [9]

A. The Enrolment or Registration stage

Biometric identification is the user's presentation of his unique biometric parameter and the process of comparing it with the entire database of available data. To retrieve this kind of personal data, biometric readers are used. The registration of the user can be performed in two ways, either controlled

Authorized licensed use limited to: Carleton University. Downloaded on June 05,2021 at 06:01:35 UTC from IEEE Xplore. Restrictions apply.

way or uncontrolled way. In a controlled way biometric system, the person must be registered by his/ her own willing, whereas, in an uncontrolled biometric system, the presence or the willing of a person is not essential [13]. However, in any form of registration, the presence of an actual person before the biometric sensor is required. Then, the biometric sensor captures his/her biometric sample. The device named the fingerprint sensor is used to capture the image of the fingerprint.

Similarly, the high pixel camera is utilized to recognize and register a person's face and iris. The captured biometric samples are pre-processed and stored into a reference format (template) and compared with the stored biometric sample templates. Only when the captured sample does not match the existing template in the database will it be stored in the database.

B. The Authentication Stage

The authentication process is similar to the registration phase; the difference lies in the matching phase only. The application services for which the system is designed are authenticated if and only if the person's samples are matched to the database samples; otherwise, the access to the particular application is rejected.

C. Performance metrics

The performance of the biometric system is designed based on the following metrics.

1. False Acceptance Rate (FAR)

It is a type-II error utilized in a biometric recognition system to determine the degree of the designed biometric system that how many times the system is accessed by an unauthorized person. FAR can be calculated using equation (1).

$$FAR = \frac{False_{Positive}}{False_{Positive} + True_{Negative}} \quad (1)$$

2. False Rejection Rate (FRR)

FRR is a type -I error. It is used to determine the rate that how many times the system fails to grant access to an authorized person.

$$FRR = \frac{False_{Negative}}{False_{Negative} + True_{Positive}} \quad (2)$$

3. Recognition rate

The recognition rate depends on the size of the used data set for any type of biometric recognition module. Therefore sample size is variable and is not fixed.

$$Recognition\ rate = 1 - (FAR + FRR) * 100 \quad (3)$$

4. Error

It is used to determine the operating characteristics of a biometric system. This should be minimum so that the type-I and type-II errors can be minimized. The total error rate is determined by adding both FAR and FRR values then divided the obtained value by the total number of access [14-15]. The error rate of any biometric system can be represented by Fig. 3.

$$Error = FAR + FRR \quad (4)$$

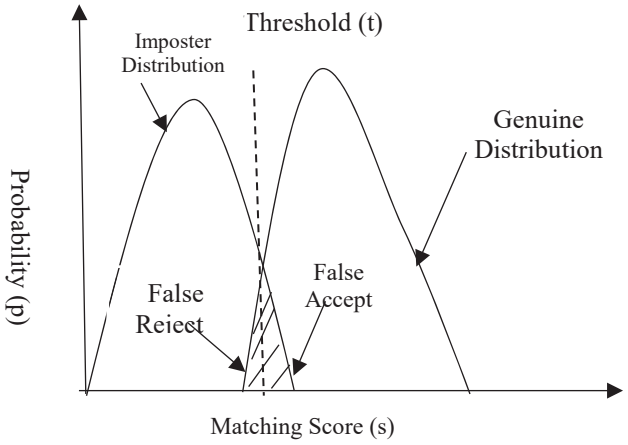

Fig. 3. Error Rate in Biometric System [16]

The performance of a biometric system relies on the value of threshold 't'. If the value of matching score (s) is greater than the threshold value (t), then the case is considered as genuine distribution as represented by the right-side curve in Fig. 3. This is the genuine case when the security user's sample is matched with the samples stored in the database. Otherwise, the system is considered as an imposter distribution as represented by the left side curve. This is when (t<s) and the test samples are not matched to the database samples.

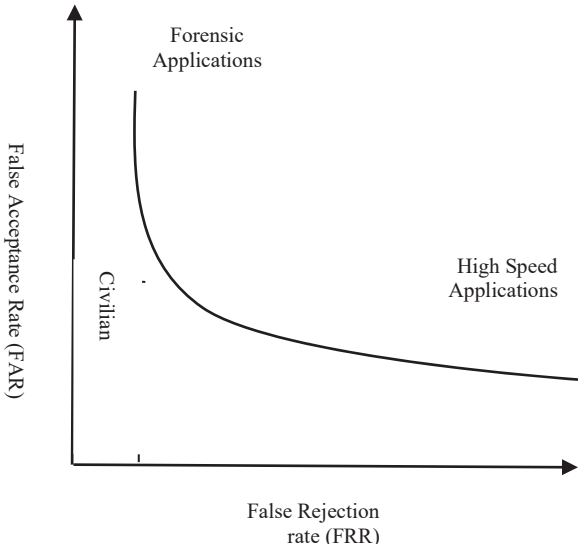

Fig. 4. ROC [16]

For a high-security system, the FRR increases with the increase in the value of 't'. To make biometric system tolerant, t should be decreased, which results in an increase in FAR.

Authorized licensed use limited to: Carleton University. Downloaded on June 05,2021 at 06:01:35 UTC from IEEE Xplore. Restrictions apply.

Therefore, it is necessary to balance the FAR and FRR, so the system can be designed in a balanced way. The tradeoff between FAR and FRR is measured using Receiver Operating Characteristics curves (ROC) as shown in Fig. 4.

III. Present State of Art

In this section, the related work performed by various authors in the field of both unimodal and multi-modal biometric systems is presented. Therefore, this section is divided into two categories, namely unimodal and multimodal biometric systems.

A. Unimodal Biometric System

The technique depends on the fact that a single physical trait is capable enough to recognize a person's identity. A system that inherits this fact for authentication, identification, and validation of a person's identity using singular biometric properties is known as a unimodal biometric system, and the technique is referred as unimodal biometrics. Several researchers have worked on the uni-modal biometric system; the performance of those is discussed in the following section.

Tanwar et al. (2019) have presented a survey on fingerprint authentication systems. The paper has reviewed a number of papers in which the researchers have considered multiple factors like data type, image enhancement, feature extraction, and post-processing approaches. The authors have concluded that using the Gabor filter and minutiae extraction technique, the system provides better accuracy [17]. Espinosa-Duro (2002) has presented a unimodal recognition system using fingerprint images. Two patterns of fingerprint images have been used that have been sensed using inkless sensor and traditional method (ink print) over blank paper, then the images have been scanned. For image processing, techniques like image enhancement, noise reduction, image binarization, thinning, and minutiae feature extraction have been used. The performance of the designed model has been analyzed based on two datasets [18]. In 2003 the researcher Espinosa-Duro replaced the first technique by collecting the fingerprint samples using optical sensors while reaming the second method (ink print) as the same [19]. El-Sisi et al. (2011) have developed a biometric system using fingerprint trait, which is enhanced using Gabor filter. The system has been designed in MATLAB software in which the algorithm like minutiae as feature extraction has been used. The system has been designed for limited areas with satisfactory security levels [20]. Chingovska et al. (2012) have detected face spoofing threat using the Local Binary Pattern (LBP) method. Here, three types of attacks, namely, printed photographs, videos displayed on electronic gadgets, and photos of different sizes, have been identified. To test the designed model, a replay attack database has been considered that contains all the attack mentioned above types [21]. Patel et al. (2019) proposed a novel algorithm that helps identify minutiae and enhances the acceptance rate and accuracy level during fingerprint recognition. Due to change in environmental condition, several reasons, such as finger displacement during the scanning process, behaviour of the user, and working of the scanner, that causes the reduction pf acceptance rate during fingerprint recognition. The author demonstrated that the proposed work was categorized into two different phases, i.e., pre-processing and post-processing. In the pre-processing phase, removing noise, making the clear fingerprint image for feature extraction, and enhancing the post-processing phase for eliminating false extracted minutiae. After the simulation on FVC2000 and Finger DOS database result shows, the proposed algorithm has 98.7% accuracy [22].

A very few works have been seen in the uni-modal biometric system. The reason for this is that today's gadgets need to be more secure, and hence double security has been provided by using multi-modal biometric systems. The work-done by researchers is provided in the following section.

B. Multi-modal biometric system

Similar methods are used in complex, strict, and complex security systems. In such cases, several types of biometric characteristics of a person (user) are used, which are combined in one system.

Hezil and Abdelhani (2017) have used ear and palmprint biometric traits at the feature level. These two traits are containing useful information that is helpful to discriminate person. The features of these traits have been extracted using local binary pattern weber local descriptor and binarized approach. The experiments have been performed on the database taken from IIT Delhi, and the designed model obtained a higher recognition rate [23]. Eskandari et al. (2013) have taken the decision based on score level fusion of two biometric traits (face and iris). Instead of using features, the researchers have used scores for matching purposes. Local and Gabor filters have been used for extracting features. The designed model has been tested on different databases, namely, ORL, BANCA (face), CASIA, and UBIRIS (Iris). The results have been analyzed using ROC characteristics [24]. Jagadeesan et al. (2010) have introduced a cryptography key generation approach using fingerprint and iris traits. The features of both fingerprint and iris have been extracted using minutia and canny edge detection, respectively. The fusion has been performed based on feature level and for security purposes a key of 256 bit has been created [25]. Basha et al. (2011) have designed a novel access control system using iris and fingerprint. The fusion score has been generated on the basis of rank level.

TABLE I. Comparative Analysis of Existing Biometric System

References	Biometric Traits	Technique Used	Recognition Rate
Turk et al. (1991) [28]	Face	PCA	70
Wang et al. (2006) [29]	Face	LDA	78.50
Eskandari et al. (2013) [24]	Face and Iris	Local and Global feature extractor	98.25
Gottumukkal and Vijayan (2004) [30]	Face	PCA	73.50
Ahonen et al. (2006) [28]	Face	LBP	79.75
Patel et al. (2019) [22]	Fingerprint	Gabor Filter	98.7

To make system more secure, rank has been generated based on Borda count, highest rank, and logistic regression technique. The system response is very fast (0.45s) to recognize an individual. Also, the FAR and FRR determined are approximately equal, and a minimum error of 0.25 5 has been obtained [26]. Radha and Kavitha (2012) have introduced a fusion-based biometric system using fingerprint and iris traits. The fusion decision has been taken based on the

Authorized licensed use limited to: Carleton University. Downloaded on June 05,2021 at 06:01:35 UTC from IEEE Xplore. Restrictions apply.

feature level. To obtained the desired features from both traits Gabor filter has been used. For match score generation, hamming distance technique is used. From experiments, the designed model performed well with FAR, FRR of 0 % and 4.3 %, respectively, with a minimum execution time of 0.14 s [27]. For the most popular biometric identification methods today, the average recognition rate is listed in table 1.

As suggested in the literature review [22], [26] and [27] used minutiae feature extraction to remove the false extracted minutiae and get exact core point detection in fingerprint recognition. For feature extraction purposes of face and iris recognition, in prior work used PCA [28, 30], LDA [29], and LBP [28] in [24] the authors also used Local and Global feature extractor.

IV. Conclusion

Biometrics is a technology that recognizes humans based on their physiological and behavioural features. In this technological world, various types of condensed biometric scanners are now available, and computers are capable of processing massive amounts of data, and the designing of biometric authentication systems are now available at reasonable prices. In addition, the current world is still facing threats from terrorism, and the implementation of strict security and surveillance measures has become a global concern. Since biometric systems are superior to conventional security systems, these systems have become a good choice for access control, personnel identification, and authorization. In this paper, essential information about biometric technology has been provided to help new researchers decide a topic in this field according to their interests. The information from the general structure of the biometric system to the emerging biometric technologies has been provided. Separate state of the art performed by researchers to design an access control biometric system (uni-modal and multi-modal) have been presented. At last, one must have concluded that a multi-modal biometric system provides better accuracy compared to a uni-modal system.

References

[1] R. K. Rowe, U. Uludag, M. Demirkus, S. Parthasaradhi, and A.K. Jain, "A multispectral whole-hand biometric authentication system," In 2007 Biometrics Symposium pp. 1-6, September 2007, IEEE.

[2] A. Eng, and L. A. Wahsheh, "Look into my eyes: A survey of biometric security," In 2013 10th International Conference on Information Technology: New Generations, pp. 422-427, April 2013, IEEE.

[3] I. M. Alsaadi, "Physiological biometric authentication systems, advantages, disadvantages and future development: A review," International Journal of Scientific & Technology Research, vol. 4, pp. 285-289, 2015.

[4] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," International Journal of u-and e-Service, Science and Technology, vol. 2, pp.13-28, 2009.

[5] N. Kumar, S. Panda, P. Pradhan and R. Kaushal, "IoT Based Hybrid System for Patient Monitoring and Medication," EAI Endorsed Transactions on Pervasive Health and Technology, vol. 5, 2019.

[6] R. K. Kaushal, S. N. Panda and N. Kumar, "Proposing Effective Framework for Animation Based Learning Environment for Engineering Students," Journal of Engineering Education Transformations, vol. 33, pp.48-61, 2020.

[7] R. K. Kaushal, S. N. Panda and N. Kumar, "An IoT Based Approach to Monitor and Replace Batteries for Battery Operated Vehicle," In IOP Conference Series: Materials Science and Engineering, IOP Publishing, vol. 993, p.012119, 2020.

[8] A. k. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on circuits and systems for video technology, vol.14, pp.4-20, 2004.

[9] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," In 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-7, 2013, IEEE.

[10] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A novel biometric approach for human identification and verification using eye blinking signal," IEEE Signal Processing Letters, vol. 22, pp. 876-880, 2014.

[11] A. K. Jain, P. Flynn, and A. A. (Eds.) Ross, "Handbook of biometrics," Springer Science & Business Media, 2007.

[12] A. K. Jain, "Biometric recognition," Nature, vol. 449, pp. 38-40, 2017.

[13] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE security & privacy, vol. 1, pp. 33-42, 2013.

[14] M. Tistarelli, and M. S. Nixon, "Advances in Biometrics: Third International Conferences, ICB 2009, Alghero, Italy, June 2-5, 2009, Proceedings, vol. 5558, 2019, Springer.

[15] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance," In Proceedings AutoID, vol. 99, pp. 59-64, 1999, Citeseer.

[16] M. Elhoseny, A. Elkhateb, A. Sahlol, and A. E. Hassanien, "Multimodal biometric personal identification and verification," In Advances in Soft Computing and Machine Learning in Image Processing, pp. 249-276, 2018, Springer, Cham.

[17] S. Tanwar, M. S. Obaidat, S. Tyagi, and N. Kumar, "Online signature-based biometric recognition," In Biometric-based physical and cybersecurity systems, pp. 255-285, 2019, Springer, Cham.

[18] V. Espinosa-Duro, "Minutiae detection algorithm for fingerprint recognition," IEEE Aerospace and Electronic Systems Magazine, vol. 17, pp. 7-10, 2002.

[19] V. Espinosa-Duro, "Fingerprints thinning algorithm," IEEE Aerospace and Electronic Systems Magazine, vol.18, pp. 28-30, 2003.

[20] A. El-Sisi, "Design and implementation biometric access control system using fingerprint for restricted area based on gabor filter," Int. Arab J. Inf. Technol., vol. 8, pp. 355-363, 2011.

[21] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," In 2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG), pp. 1-7, 2012, IEEE.

[22] M. B. Patel, S. M. Parikh, and A. R. Patel, "An improved approach in fingerprint recognition algorithm," In Smart Computational Strategies: Theoretical and Practical Aspects, pp. 135-151, 2019. Springer, Singapore.

[23] N. Hezil, and A. Boukrouche, "Multimodal biometric recognition using human ear and palmprint. IET Biometrics, vol. 6, pp. 351-359, 2017.

[24] M. Eskandari, O. Toygar, and H. Demirel, "A new approach for face-iris multimodal biometric recognition using score fusion," International Journal of Pattern Recognition and Artificial Intelligence, vol. 27, pp.1356004, 2013.

[25] A. Jagadeesan, T. Thillaikkarasi, and K. Duraiswamy, " Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature," International Journal of Computer Applications, vol. 2, pp.16-26, 2010.

[26] A. J. Basha, V. Palanisamy, and T. Purusothaman, "Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features," In Second Journal of Computer Science, 2011.

[27] N. Radha, and A. Kavitha, "Rank level fusion using fingerprint and iris biometrics," Indian Journal of Computer Science and Engineering, vol. 2, pp. 917-923, 2012.

[28] M. Turk, and A. Pentland, "Eigenfaces for recognition," Journal of cognitive neuroscience, vol. 3, pp. 71-86, 1991.

[29] X. Wang, and X. Tang, "Random sampling for subspace face recognition," International Journal of Computer Vision, vol. 70, pp. 91-104, 2006.

[30] R. Gottumukkal, and V. K. Asari, "An improved face recognition technique based on modular PCA approach," Pattern Recognition Letters, vol. 25, pp. 429-436, 2004.

Authorized licensed use limited to: Carleton University. Downloaded on June 05,2021 at 06:01:35 UTC from IEEE Xplore. Restrictions apply.