IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

Comprehensive Review of Fingerprint Based Biometric Systems

D. Beulah Pretty[1] and D. Evangeline Nesa Priya[2]
Associate Professor, Computer Science and Engineering, Thangavelu Engineering College, Chennai, India[1]
Assistant Professor, Information Technology, T J Institute of Technology, Chennai, India[2]

Abstract: *Biometric systems are increasingly replacing traditional password and token based authentication systems. Security and recognition accuracy are the two most important aspects to consider in designing a biometric system. In this paper, a comprehensive review is presented to shed light on the latest developments in the study of fingerprint-based biometrics covering these two aspects with a view to improving system security and recognition accuracy. Based on a thorough analysis and discussion, limitations of existing research work are outlined and suggestions for future work are provided. The two most critical attacks to biometric systems, namely, attacks to the user interface and template databases are discussed here. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is the research topic in the foreseeable future. Moreover, recognition accuracy under non-ideal conditions is more likely to be unsatisfactory and thus needs particular attention in biometric system design.*

Keywords: biometrics; security; protection; recognition accuracy; fingerprint

I. INTRODUCTION

Biometrics is a technology that uses the unique patterns of physical or behavioral traits of users for authentication or identification. With biometric scanners on smart phones and other devices becoming more prevalent, as well as a growing number of services calling for high security and good customer experience, traditional methods of authentication (e.g., passwords and PINs) are increasingly being replaced by biometric technology [1]. Passwords have some obvious drawbacks as they could be stolen, lost, or forgotten. In contrast, biometrics offer an alternative solution to the task of personal authentication or identification based on biometric traits. To be forgotten or lost is impossible, and unlike passwords, they are hard to forge. There are some biometric traits that can be defined for an individual; for example, fingerprint, finger-vein, iris, voice, face, and so on [2].Generally, a typical biometric system comprises four modules, namely, sensor module, feature extraction module, template database, and matching module. Specifically, the sensor module acquires the biometric image. A set of global or local features are extracted from the acquired biometric image by the feature extraction module. Structured feature representations are stored in the template database as template data. The matching module is responsible for comparing the query and template data to reach a match or non-match verdict. A typical biometric system carries out authentication in two stages the enrollment stage and verification stage as shown in Figure 1.

Take fingerprint recognition as an example. In the stage of enrollment, a user presents their finger to the fingerprint sensor and a fingerprint image is acquired by the sensor module. Certain features of the acquired fingerprint image are extracted, and further adapted or transformed to generate template data for the purpose of comparison in the verification stage. In the verification stage, the fingerprint image of a query is collected by the sensor module. The feature representations of the query fingerprint image go through the same process as in the enrollment stage, so as to obtain query data. The query data are then compared with the template data so that a matching outcome is attained.

DOI: 10.48175/IJARSCT-23206

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

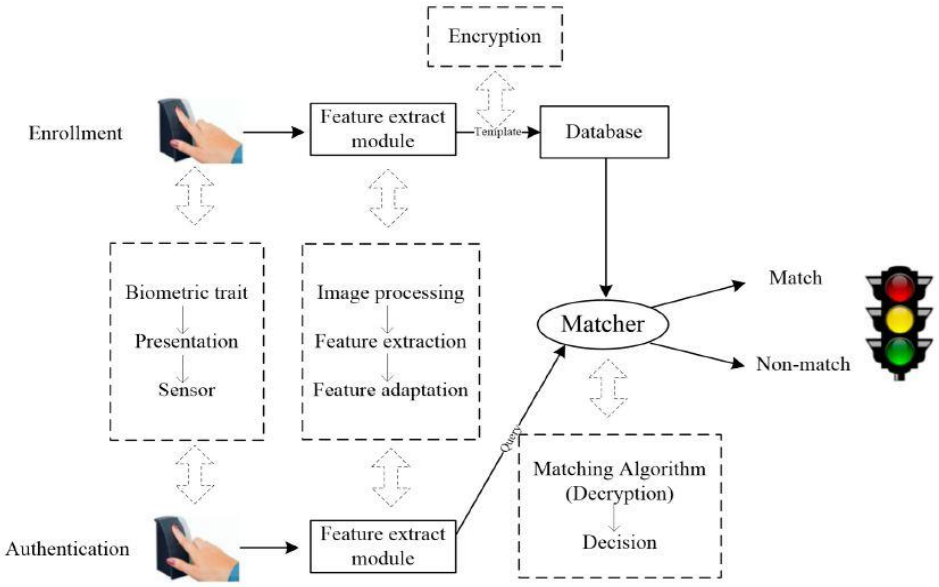

Figure 1. An example of two stages in biometric authentication system.

In this paper, a comprehensive review is presented to shed light on the latest development in the study of fingerprint-based biometrics concerning two important aspects-security and recognition accuracy. The main contributions of this paper are highlighted as follows:

1. Security and recognition accuracy, despite being two most important aspects in biometric system design, have not been adequately studied simultaneously. Prior to this review paper, no research work has delivered a comprehensive review considering both of them. In this paper, up-to-date research and insights into security and recognition accuracy are thoroughly analyzed and discussed.
2. Based on a thorough analysis, limitations of existing research are discussed and suggestions for future work to overcome those limitations are provided.
3. The two most critical attacks to biometric systems are discussed in this paper. How to resolve the challenges, so as to defend biometric systems, is the focus of current and future biometric security research.

II. SECURITY ANALYSIS: ATTACKS AND COUNTERMEASURES

Compared with password-based authentication systems, there are two major concerns over biometric systems. First, biometric traits cannot be revoked and reissued in the cases where they are compromised. For example, if a person's fingerprint image is stolen, it is not possible to replace it like replacing a stolen password. Moreover, different applications might use the same biometric trait; if an adversary acquires an individual's biometric trait in one application, they could also use it to gain access to other applications. Second, biometric traits are not secret. An individual could leave their fingerprint on any surface they touch [5]. Ratha et al. identified eight different points of attacks in a biometric system [6]. Attacks can be in various forms (e.g., phishing and farming attacks, front- or back-end attacks), but they can generally be classified into four categories:

(a) Attacks at the interface.
(b) Attacks at the modules.
(c) Attacks to the channels between modules.
(d) Attacks to the template database.

Here threats and security issues related to those attack points in different stages of a generic biometric system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

2.1 Attacks to User Interface and Countermeasures

Spoofing attacks to the user interface (the sensor module) are mostly because of the presentation of a fake biometric trait. Since biometric traits are not secret, an adversary can intrude into the system with a fake trait (e.g., artificial fingerprint, face mask) to spoof the biometric system if the system is unable to differentiate between a fake and a genuine biometric trait. A number of fingerprint sensors are tested to see if they can reject a fake fingerprint film. The test results show that the fake finger films are accepted by most of the tested sensors [7]. Also, a total of 11 different fingerprint-based authentication systems are attacked with fake fingerprint films, with results showing that fake fingerprint films can be enrolled in the systems and fake fingerprints are accepted with more than 67% probability [8]. With the ever-increasing popularity of iPhones, great attention has been drawn to the fingerprint spoofing attack to Touch ID. For example, a latent fingerprint was lifted from the iPhone screen. From the lifted latent fingerprint, a mold was created by using a printed circuit board (PCB) by a researcher from Chaos Computer Club (CCC). By filling the art glue into the mold on the PCB, he subsequently generated a rubber fingerprint film, by which Touch ID of the iPhone can be fooled. Liveness detection is an effective countermeasure to fake biometric attacks. In recent years, strenuous work has been done in the research of liveness detection, which is used to detect whether the presented feature is from a live human being or not. Two major schemes are available to implement liveness detection. One scheme constitutes software-based solutions, which utilize the information already captured by biometric sensors, while the other scheme includes hardware-based solutions [9]. However, hardware-based solutions are usually more expensive. Tan and Schuckers presented a wavelet transform based method to detect the perspiration phenomenon, so as to tell difference between live and non-live fingers. The perspiration phenomenon can be quantified by using the statistical features, which represent the gray level values along the ridge mask in an image [10]. Experimental results demonstrate that with the proposed method, optical scanners are able to detect live fingers. To prevent spoof attacks from gelatin or silicon fake-fingerprints from deceiving some commonly used fingerprint sensors, Coli et al. utilized static features together with dynamic features for fingerprint vitality detection [11]. Galbally et al. proposed an approach using fingerprint parameterization based on quality related features for liveness detection. The liveness detection process can be considered as a two-class, real or fake, classification problem. The key point of this problem is to find and use a set of unique patterns to generate a classifier that outputs the probability of a fingerprint image. The proposed approach is able to perform classification based on the single acquired sample rather than multiple different samples of the fingerprint, which makes the acquisition process of a sample faster and more expedient than existing methods. The proposed approach was tested on several publicly available databases and good accuracy was reported (e.g., almost 9 out of 10 of the fingerprint images were classified correctly). Kim designed an image descriptor to handle fingerprint liveness detection [12]. It is observed that fake fingerprints tend to generate non-uniformity in the captured image
for the replica fabrication process, so the difference of the dispersion in the image gradient field is exploited to distinguish live and fake fingerprints. In the proposed method, a new feature called local coherence pattern is defined, which is a local pattern of coherence along the dominant direction. After the proposed feature set is fed into the support vector machine (SVM), a decision on a real or fake fingerprint can be made [13]. Jung and Heo introduced a convolutional neural network (CNN) architecture to deal with the liveness detection issue. The proposed architecture is a robust framework for training and detection. Squared regression error for each receptive field is employed in this architecture and the training can be performed directly from each fingerprint. System performance is controlled by a threshold value in the squared error layer. Kundargi and Karandikar proposed using a texture descriptor, called completed local binary pattern (CLBP), together with the wavelet transform (WT) for fingerprint liveness detection [14]. By considering the local sign and magnitude difference with the average gray level of a fingerprint image, the CLBP possesses high discriminatory power. Experimental results verified that the CLBP in the WT domain can offer satisfactory classification performance. Xia et al. developed a local descriptor, namely, Weber local binary, for fingerprint liveness detection. The proposed method is composed of two modules, namely local binary differential excitation module and local binary gradient orientation module. The outputs of these two modules form a discriminative feature vector that is input into the SVM classifiers. Yuan et al. introduced a BP neural network based fingerprint liveness detection method [15]. In this method, image gradient values are obtained by the Laplacian operator and different parameters for the BP neural network are tested to achieve better detection accuracy. In this section, as the countermeasure to spoofing attacks, several liveness detection methods are reviewed. Non-machine learning based

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

algorithms and machine learning based algorithms were proposed to extract unique features to ascertain whether an input fingerprint is fake or real. The three machine learning based algorithms, which shows that machine learning is playing an active role in liveness detection design.

III. ATTACKS TO TEMPLATE DATABASES AND COUNTERMEASURES

Attacks to biometric template databases are some of the most critical and damaging attacks, which can cause serious consequences to users biometric data. In a biometric system, biometric template data are usually placed in a database in the enrollment stage and they are compared with query data in the verification stage. Because biometric traits cannot be revoked or reset, serious security concerns could arise if raw, unprotected template data are stored in a database. For instance, an adversary can hack the template data in the database, thus gaining unauthorized access to a biometric system. Moreover, artificial biometric traits can be created from the template data if original (raw) biometric information is stored in the database. To protect raw template data, a range of techniques have been proposed in literature, which can be generally classified into two categories, namely, cancelable biometrics and biometric cryptosystems [16].

3.1 Cancelable Biometrics

The concept of cancelable biometrics is that the original template data is transformed into a different version by using a non-invertible transformation function in the enrollment stage. Query data in the verification stage are applied the same non-invertible transformation. Matching is conducted in the transformed domain using the transformed template and query data [17]. Ratha et al. initiated three different transformation functions, known as Cartesian, polar and functional transformations. The proposed transformation functions intentionally distort the original features, so that it is infeasible or computationally difficult to retrieve raw template data. However, one drawback is that the proposed method is registration-based, and hence, accurate detection of singular points is required. Usually, accurate registration is hard because of biometric uncertainty (e.g., image displacement, non-linear distortion, and acquisition condition). Jin et al. proposed a two factor authentication method called bio-hashing. Bio-hashing combines token-based data with fingerprint features by the iterative inner product to create a new feature set [18]. Then each value in the feature set is converted to a binary number based on a predefined threshold. Lee et al. generated cancelable fingerprint templates by extracting a rotation and translation-invariant feature for each minutiae, which is deemed to be the first alignment-free cancelable fingerprint template design [19]. Ahn et al. used triplets of minutiae as a feature set, and transformation is performed on geometrical properties derived from the triplets [20]. Yang et al. created cancelable templates by using both local and global features [21]. Local features include distances and relative angles between minutiae pairs, while global features include orientation and ridge frequency. In this research, the distance of a pair of minutiae is transformed using a perpendicular projection, so as to derive the non-invertible transformation.

Ahmad and Hu proposed an alignment-free structure based on a pair-polar coordinate. In this structure, the relative position of each minutia to all other minutiae among a polar coordinate range is utilized. From any two minutiae, three local features are extracted and transformed by a functional transformation to generate the cancelable template. Based on the minutia structure, Wang et al. further improved system security and accuracy by proposing some new transformation functions, such as infinite-to-one mapping, curtailed circular convolution, and partial Hadamard transform Zhang et al. designed a combo plate and a functional transformation to produce cancelable templates based on the Minutia Cylinder-Code (MCC) [24]. MCC is a well-known local minutia descriptor, which is based on 3D local structures associated with each minutia. The authors of the MCC later proposed a template protection method named P-MCC, which performs a KL transformation on the MCC feature representation. However, P-MCC does not have the property of revocability [25]. Then, 2P-MCC was proposed to add cancelability to P-MCC using a partial permutation based scheme Later, Arjona et al. presented a secure fingerprint matching approach, named P-MCC-PUFs, which contains two factors based on P-MCC and PUFs (Physically Unclonable Functions).The proposed scheme achieves the best performance when the length of the feature vector is set to 1024 bits and provides strong data privacy and security.

Yang et al. designed a cancelable fingerprint template based on random projection. The designed template can defend attacks via record multiplicity (ARM) owing to the feature decorrelation algorithm In the meantime, a Delaunay triangulation-based local structure proposed in the scheme can reduce the negative effect of nonlinear distortion on

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

matching performance. Sandhya and Prasad fused two structures, local structure and distant structure, at the feature level to generate binary-valued features, which are then protected by a random projection based cancelable protection method To further enhance security and recognition performance, some researchers proposed use of multimodal cancelable biometrics. For example, Yang et al. proposed a multimodal cancelable biometric system that fuses fingerprint features and finger-vein features to achieve better recognition accuracy and higher security. In the proposed system, an enhanced partial discrete Fourier transform is utilized to provide non-invertibility and revocability. Also, Dwivedi and Dey proposed a hybrid fusion (score level and decision level fusion) scheme to integrate cancelable fingerprint and iris modalities to reduce limitations in each individual modality .Experimental results of multimodal cancelable biometric systems exhibit performance improvement over their unimodal counterpart. In this section, the evolution of cancelable biometrics, from the introduction of the idea of cancelable biometrics and some early transformation function designs , to the recent multiple cancelable biometrics, is presented. There are two categories in the design of cancelable biometrics. One category centers around the extraction and representation of stable biometric features so as to achieve better recognition accuracy, and the other category focuses on designing secure transformation functions, which are expected to be mathematically non-invertible . It is anticipated that future research work in cancelable biometrics will attempt to achieve both better recognition accuracy and stronger security by using multiple cancelable biometrics

3.2 Biometric Cryptosystems

A biometric cryptosystem combines biometrics with a cryptographic key and merges the advantages of both biometrics and cryptosystems. Different to a cancelable biometric system, which can only provide a match or non-match report, a biometric cryptosystem can output a key by either binding it with the biometric features, such as fuzzy commitment (FC) and fuzzy vault (FV), or directly generating the key from the biometric features, for example, fuzzy extractor (FE) Teoh and Kim utilized the fuzzy commitment scheme to protect fingerprint features . Since it is convenient to have biometric features in the binary format, the authors processed the features with a randomized dynamic quantization transformation. However, in most cases of fingerprint minutiae matching, the extracted minutia set is a point set and is unordered. To protect the fingerprint minutia data in the point set, Uludag et al. applied the original concept of fuzzy vault to the fingerprint minutia data. In this method, a 128-bit cryptographic key is feasibly bound with the fingerprint minutia data, but this method requires image alignment. Later, Nandakumar et al. introduced a fingerprint minutiae based fuzzy vault scheme and utilized the high curvature points to assist image alignment, thus making alignment more accurate without leaking any orientation information or minutia position within the template data. All the above-mentioned approaches require pre-alignment (i.e., registration) to rotate and translate the query image with respect to the template image. However, the pre-alignment process may cause non-negligible noise (e.g., generating fake minutiae and altering the singular point position), as investigated by Zhang et al. . Alignment-free approaches that require no image pre-alignment can avoid the above shortcomings. Li et al. proposed a fuzzy vault scheme, which combines two local structures, the minutiae descriptor and minutia local structure. By using three fusion approaches, the two transformation-invariant local structures are integrated in the proposed scheme. Unlike the schemes of fuzzy commitment and fuzzy vault discussed earlier, which are key binding schemes, fuzzy extractors are key generation schemes based on the concept Arakala et al. implemented the fuzzy extractor in minutiae-based fingerprint authentication. Given a fingerprint minutia set, all the minutiae are quantized and represented by a set of binary strings, which are subsequently input into an existing secure sketch, named PinSketch Xi et al. proposed a fuzzy extractor using a dual-layer local structure. In this system, rotation- and transformation-free dual-layer structures are developed to guard biometric templates against attacks. Later, some other fuzzy extractor systems were also proposed with enhanced performance. Liu and Zhao utilized l1-minimization to secure the fingerprint templates and store them in cyphertext form. Fingerprint matching is carried out in the encrypted domain and authentication is successful only when the query fingerprint is close enough to the template fingerprint. As the template is generated from the Minutia Cylinder-Code (MCC) with the proper design of the secure algorithm, the proposed system achieves high security and recognition accuracy. Given the fact that conventional biometric cryptosystems are not equipped with revocability, recently, the cancelable technique is employed to enhance the security of biometric cryptosystem. Yang et al. proposed a cancelable fuzzy vault system to encrypt the Delaunay triangle group based fingerprint features. The cancelable transformation is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

derived from the polar transformation. The transformation unit in this work is a triangle instead of a single minutia, which enables the system to be less sensitive to biometric uncertainty. Alam et al. put forward a biometric cryptosystem, which incorporates the discrete Fourier transform (DFT) and random projection based cancelable technique to heighten security .In the proposed system, polar grid based fingerprint features are transformed by using the DFT and random projection, creating a non-invertible template. Also, a bit-toggling strategy is utilized to inject noise into the generated template, so as to further strengthen template security. Sarkar and Singh proposed generation of cryptographic keys from cancelable fingerprint templates . Different keys with a length of 128 bits can be generated by cancelling and reissuing different fingerprint templates. This reduces the potential risk that the same secret key that existed with the receiver and sender could be leaked after negotiation.

In this section, detailed analysis and discussion about biometric cryptosystems are given, from the initial concepts, e.g., fuzzy commitment, fuzzy vault, and fuzzy extractor, to various complex algorithms derived afterwards. One of the advantages of biometric cryptosystems is that they can bind or directly generate a cryptographic key, which can be used for both authentication and data encryption. However, most biometric cryptosystems are not equipped with cancel ability. Some researchers realized this problem and thus developed biometric cryptosystems with revocability, so as to enhance system security. It is worth noting that nowadays deep learning techniques have been involved in more and more biometric applications, e.g., face and voice recognition, but there is almost no research regarding the security of deep learning based biometrics. Therefore, more research effort should be devoted to this direction.

3.3 Recognition Accuracy

Although biometric technology renders considerable benefits and is being used in many applications, it faces challenges, such as insufficient accuracy under non-ideal conditions or in the encrypted domain when template protection is implemented.

A. Accuracy under Ideal vs. Non-Ideal Conditions

Biometric systems sometimes confront unrealistic expectations of achieving the matching accuracy of traditional password-based authentication systems. A password-based system always offers a crisp result—it grants access if the input password is a match, and vice versa. However, biometric matching cannot be 100% accurate. The accuracy of a biometric system can be evaluated by using well-known performance indicators, e.g., False Accept Rate (FAR), False Reject Rate (FRR), and Equal Error Rate (EER). Recognition accuracy generally depends on factors such as input image quality and matching algorithms. With decades of efforts from researchers, remarkable matching accuracy has been achieved and reported. For instance, there is an online evaluation platform, named FVC-ongoing, where researchers can upload their recognition algorithms and compete with other algorithms on matching accuracy. FVC-ongoing sets up a benchmark to evaluate those algorithms using a set of sequestered databases and the results are evaluated by indicators—FAR, FRR, and EER—which is the rate at which both acceptance and rejection errors are equal . According to the latest results shown on the FVC-ongoing platform, the best matching accuracy out of the fingerprint verification competition reached the EER = 0.022%, achieved by the algorithm, named HXKJ, contributed by Beijing Hisign Bio-info Institute. Some algorithms designed by academic researchers also achieve gratifying accuracy. The state-of-the-art MCC (Minutia Cylinder Code) based fingerprint matching algorithm achieved the EER = 0.49% on database FVC2002 DB2, and the EER = 0.12% on database FVC2006 DB2.

Cao et al. proposed a latent segmentation and enhancement algorithm to refine a poor fingerprint image . By using a total variation decomposition model, the piecewise-smooth background noise can be removed and several overlapping patches are defined and used for latent enhancement, leading to better matching performance. Also, Araro et al. incorporated feedback information from an example to refine the extracted features from a latent fingerprint image with the eventual goal of increasing the matching accuracy.

B. Accuracy Without vs. With Template Protection

Template protection techniques provide safeguards to biometric templates and the protected template should leak as little information of the original template as possible. In biometric cryptosystems, information of reference points can help to enhance the recognition accuracy but will leak important information about the original template, and thus it

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

should not be made public. In cancelable biometrics, random projection based transformation is a typical many-to-one mapping, in which the dimension of the original template is reduced. Because less information of the original template is kept, a lower-dimensional transformed template is more secure. However, with less information of the original template preserved, it might result in accuracy degradation. Therefore, there is a balance between recognition accuracy and security. It can be seen that recognition accuracy of most existing biometric systems, either with or without template protection, are tested in ideal conditions, which are far from real-life scenarios, where the obtained images (e.g., latent fingerprint) are of extremely low quality. Also, the recognition accuracy of the systems with template protection is lower than that without template protection . The main reason is the information loss in the process of feature adaptation, which converts original features into another format to satisfy the matching metrics for transformed templates, e.g., hamming distance for fuzzy commitment and set difference for fuzzy vault. Therefore, more study needs to be put into the design of stable features and suitable feature adaptation methods, so as to minimize information loss.

IV. CONCLUSION

This paper gives a comprehensive review of two significant (and competing) measures for fingerprint-based biometric systems; that is, security and recognition accuracy. In regards to security, we have analyzed two categories of attacks: attacks to user interface and attacks to template databases. Countermeasures to defend against these attacks are also discussed. Despite the improvement in recognition accuracy under non-ideal conditions and recent advances in biometric template protection, a number of open issues still exist, which call upon biometric researchers to resolve them. We highlight some research challenges and future directions in the following:

1. New developments in deep learning techniques have enhanced the performance of biometric systems across a wide range of biometric modalities, such as face recognition modality. We envisage that deep learning techniques will also be potential tools for latent fingerprint matching. However, the use of deep learning algorithms may bring potential threats to biometric systems because of the vulnerabilities of those deep learning algorithms themselves.

2. The security issues (e.g., spoofing attacks, attacks to biometric templates) analyzed for a general biometric system are also valid to any biometric system on different platforms, for example, a mobile platform. Nowadays, smart phones are becoming more and more popular, thus forming a promising platform for the use of biometrics However, mobile biometrics face more challenges, since smart phones usually have less computing capability and limited energy. Therefore, light-weight secure algorithm design for mobile biometrics is an emerging research topic.

1.Trade-off between security and recognition accuracy in fingerprint template protection remains a challenge. The best matching performance of fingerprint competition with template protection is the EER = 1.542%, which is much worse than that (EER = 0.022%) without template protection .Besides exploring more robust and distinctive features and designing better transformation functions, the use of multi-biometrics in template protection design is likely to be the way forward and deserves further research.

REFERENCES

[1]. Jain, A.K.; Flynn, P.; Ross, A.A. Handbook of Biometrics; Springer: New York, NY, USA, 2007.

[2]. Riaz, N.; Riaz, N.; Riaz, A.; Riaz, A.; Khan, S.A.; Khan, S.A. Biometric template security: An overview. Sensor Rev. **2017**, 38, 120–127.

[3]. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. IEEE Secur. Priv. **2003**, 1, 33–42.

[4]. Awad, A.I.; Hassanien, A.E. Impact of Some Biometric Modalities on Forensic Science. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications; Springer: Berlin, Germany, 2014; pp. 47–62.

[5]. Zheng, G.; Shankaran, R.; Orgun, M.A.; Qiao, L.; Saleem, K. Ideas and challenges for securing wireless implantable medical devices: A review. IEEE Sens. J. **2016**, 17, 562–576.

[6]. Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A.; Zhou, J.; Qiao, L.; Saleem, K. Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. IEEE J. Biomed. Health Inf. **2017**, 21, 655–663.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

[7]. Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A. Encryption for implantable medical devices using modified one-time pads. IEEE Access **2015**, 3, 825–836.

[8]. Awad, A.I.; Hassanien, A.E.; Zawbaa, H.M. A Cattle Identification Approach Using Live Captured Muzzle Print Images. In Advances in Security of Information and Communication Networks; Springer: Berlin, Germany, 2013; pp. 143–152.

[9]. Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **2004**, 14, 4–20.

[10]. Tipton, S.J.; White, D.J., II; Sershon, C.; Choi, Y.B. iOS security and privacy: Authentication methods, permissions, and potential pitfalls with touch id. Int. J. Comput. Inf. Technol. **2014**, 3, 482–489.

[11]. Ratha, N.K.; Connell, J.H.; Bolle, R.M. An analysis of minutiae matching strength. In Proceedings of the 3rd International Conference on Audio-and Video-Based Biometric Person Authentication, Halmstad, Sweden, 6–8 June 2001; pp. 223–228.

[12]. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 2008, 1–17.

[13]. El-Abed, M.; Lacharme, P.; Rosenberger, C. Privacy and Security Assessment of Biometric Systems; Cambridge Scholar Publishing: Cambridge, UK, 2015.

[14]. Kang, H.; Lee, B.; Kim, H.; Shin, D.; Kim, J. A study on performance evaluation of the liveness detection for various fingerprint sensor modules. In Proceedings of the International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, Oxford, UK, 3–5 September 2003; pp. 1245–1253.

[15]. Schuckers, S.A. Spoofing and anti-spoofing measures. Inf. Secur. Tech. Rep. **2002**, 7, 56–62.

[16]. Yang, W.; Hu, J.; Fernandes, C.; Sivaraman, V.; Wu, Q. Vulnerability analysis of iPhone 6. In Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 457–463.

[17]. Tan, B.; Schuckers, S. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), New York, NY, USA, 17–22 June 2006; p. 26.

[18]. Coli, P.; Marcialis, G.L.; Roli, F. Fingerprint silicon replicas: Static and dynamic features for vitality detection using an optical capture device. Int. J. Image Graphics **2008**, 8, 495–512.