JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

# COMPREHENSIVE REVIEW OF FINGERPRINT BASED BIOMETRIC SYSTEMS

**Mr.N.Senthilkumar, Dr.R.Ramadevi,Supervisor**

Research Scholar Sathyabama Institute of Science and Technology

Received: 14 Feb 2020 Revised and Accepted: 25 March 2020

**Abstract**: Biometric systems are increasingly substituting for conventional passwords and token based systems in authenticated computer. When designing a biometric system the two most important issues are protection and recognition accuracy. This paper provides a comprehensive analysis based on the latest advances in the field of biometrics(fingerprint-based) which address all of these systems with an direction to enhancing system security and accuracy identification. We will highlight shortcomings of current research work and offer recommendations for future study based on a thorough analysis and discussion. Here we discuss the two most important strike on biometric systems, namely attacks on user interfaces and prototyping databases. In the near future, research emphasis will be on how to establish effective countermeasures to thwart these attacks, thereby providing good defense while retaining high identification accurac y. In addition, accurac y of identification is more likely to be unsatisfactory in non-ideal situations and bus needs careful consideration in the design of biometric systems.

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

## 1. Introduction

Biometrics is a method used to authenticate or classify them using the distinctive patterns of the users' physical or behavioral attributes. Biometric authentication mechanisms (e.g. passwords and PINs) are being gradually replaced with biometric technologies, such as the proliferation of biometric scanners on smartphones and other devices, and an increasing range of services requiring high safety and strong customer care. Passwords have some apparent disadvantages because they can be stolen, lost or forgotten. In contrast, biometrics offer an alternative method to identifying or authenticating biometric character identities in a personal way. Without passwords, it's hard to lose or forget, and hard to copy. A person can recognize other biometric characteristics[2], such as fingerprints, finger-veins, iris, voice , face, etc.

Usually a typical biometric device consists of four components, namely the sensor module, the software extraction module, database setup, and the module in question. The sensor module takes directly onto the biometric image. Extracts from the biometric image of the function module got a set of global or local characteristics. Structured representations of functions shall be stored as template data in template databases. The matching module function is to compare the query and template data in order to reach a matching or non-match verdict[3,4]. As seen in Figure 1, a standard biometric system accomplishes two stages of enrolment and verification.

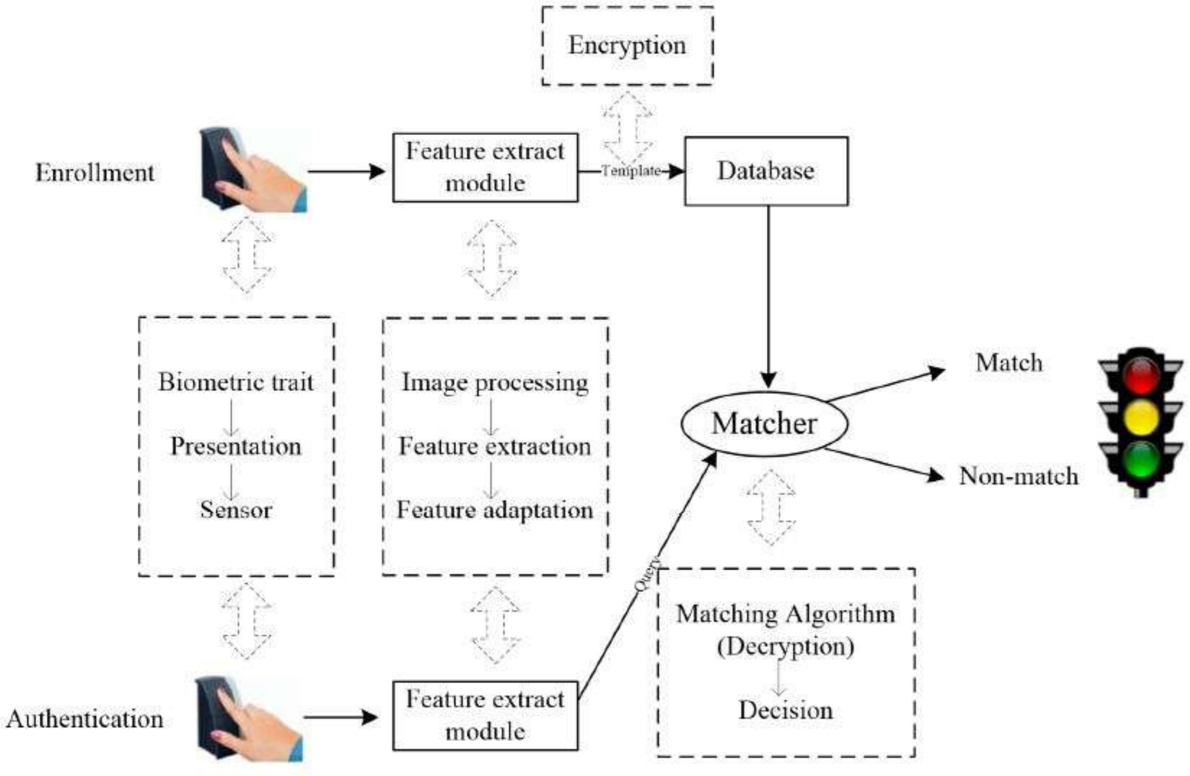

**Figure 1.** Two stages in biometric authentication system example.

Take one for example, fingerprint recognition. A customer must present their fingerprint sensor during the registration stage, and the sensor module will get a fingerprint image. Several characteristics of the obtained fingerprint image are pull out, and it is then modified or converted to produce sample results for comparison during the verification stage. The sensor module gets the fingerprint picture of a question at the verification point. The image function's fingerprint file representations will be passed through the exact identical process which is same as present in the enrollment phase, so that data can be retrieved from file. The inquired data is then matched with the template data in order to get a relative result.

This paper presents a thorough overview on two important aspects of recognition protection and accuracy that will shed some light on the latest advances in Fingerprint-based biometrics research. This paper 's principal contributions are seen as follows:

1. Despite having two major biometric variables, protection and precision recognition at the same time as the device's architecture were not adequately studied. No empirical research had provided a detailed analysis prior to this review article, considering both. This paper analyzes and addresses the accuracy of the research and results of current health and recognition today.

2. Existing limitations of the study and suggestions for future work to overcome those limitations are considered based on a thorough analysis.

3. Two key biometric assaults are dealt with here. Present and future research on biometric protection focuses on how to address security problems with the biometric system.

4. Most of the existing processes, with or without model assistance, were introduced under ideal conditions. In this paper we highlight the importance of taking accuracy of recognition into consideration under the non-ideal conditions. This analysis is supported by good evidence, with thorough comparison.

**Security Analysis: Attacks and Countermeasures**

For biometric loops there are two big challenges, as opposed to password-based authentication schemes. Second, in such cases where they are compromised, biometric attributes can not be removed and reissued. For instance, If the fingerprint image of a person is stolen, for example, that image can not be replaced as a replacement for a stolen password. In addition , various applications using the same biometric characteristics; if an attacker obtain the biometric character of a person, which is used in one of the applications, there is a possibility that, they will still be able to use it for accessing other applications. However, biometric features aren't safe. An person can leave his/her fingerprint on whatever surface it touches[5]. In a biometric framework the Ratha et al. defined eight separate attack points[6]. Attacks can occur in different ways (e.g., farming attacks and phishing, frontal or back-end attack), even so they usually can be grouped into four categories:

A) The Machine Attacks;

B) Module attacks.

C) Assaults on channels between modules.

D) Test Server Attacks.

Here risks and safety issues related to certain points of attack at different stages of a common biometric network.

**Attacks to User Interface and Countermeasures**

Owing to their architecture, spoofing attacks of a fake biometric trait on the user interface (the sensor module). Even though biometric systems are not confidential, unless the system could not differentiate between a hoax and a legitimate biometric characteristic, an attacker may interfere with a fake characteristic (e.g. face mask, artificial fingerprint) used to bypass the biometric system. Several fingerprint sensors are being checked to see if the fake video can be switched away. The test results indicate that most of the sensors tested support fake finger films [7]. Fake fingerprint films are also aimed at a total of 11 separate fingerprint authentication systems showing that, these falsified fingerprint films can be registered in systems and also that falsified fingerprints are likely to be admitted at more than 67%[8].With the ever growing popularity of iPhones, the fingerprint spoofing attack on the Touch ID has gained considerable attention. For example, a unused fingerprint from the iPhone screen had been removed. A framework was produced using a printed circuit board (PCB), using the lifted latent fingerprint, by a Chaos Computer Club (CCC) researcher. Subsequently, by filling the art glue into the mold on the PCB, he created a rubber fingerprint film, which can fool iPhone's Touch ID. Identification of lifelihood is an effective countermeasure for fake biometric attacks. Extensive work has been done in recent years in the research on the detection of liveliness, which is used to assess whether or not the information given comes from a living human being. There are two broad schemes for applying the detection of liveness. One scheme is software-based solutions that make use of knowledge already collected from Biometric sensors, even when hardware based solutions are included in the other system[9]. However, these hardware oriented approaches are typically expensive.

Tan and Schuckers created a wavelet like transformation method to determine suddenness occurence that says the difference between living and nonlive paws. The sudden occurrence can be measured by using statistical characteristics that represent the values of the gray level in a picture along the ridge mask[11]. Experimental findings show that the proposed method allows for the identification of live fingers by optical scanners. Coli et al. used static characteristics together with dynamic characteristics to detect fingerprint resilience to prevent attacks triggered by gelatin or silicon falsified fingerprints from cheating any widely sensors used in fingerprint.

Galbally and others have suggested a method that uses fingerprint parameterization to detect liveliness based on quality-related characteristics. Measurement of the way viveness can be seen as a matter of classifying two forms, true or false. The main aspect of this problem is to identify and use a collection of common patterns to produce a classifier outputing a fingerprint image 's probability. Because of several separate fingerprint samples, the proposed technique is capable of conducting classification based on the collected single sample, allowing a process of sampling to be quicker and is having more advantages than current methods. The approach proposed was tested and good accuracy was documented on many publicly available databases (e.g., close to 9 out of 10 fingerprint images were properly classified). Kim developed an image descriptor for handling fingerprint detection over a lifetime [12].

False fingerprints also generate image differences captured for the replica phase by changing the dispersal variance in the gradient field of the frame, to distinguish between live and false fingerprints. The approach proposed describes a new framework, known as a pattern of local consistency, along the existing lines. A judgment can be taken on a true or false fingerprint[13] if the proposed feature is used on the support vector machine ( SVM). In order to solve the problem of motion detection, Jung and Heo have created a CNN architecture. The suggested definition is a solid method of planning and detection. With any receptive area in this system, squared regression errors are used and training from each fingerprint can be carried out directly. The unit result in the squared error layer is influenced by a threshold value. Kundargi and Karandikar proposed that they use the completed transformation of the CLBP and fingerprint wavelet[14]. Because of the difference in local signs and severity of the average gray fingerprint level the CLBP has a high discriminatory potential.Experimental results have shown that the WT domain of CLBP can provide adequate classification efficiency.

Xia and al. Local descriptor provided for viveness detection of the fingerprints, namely local Weber binary. The system proposed comprises two parts, namely local binary differentials module of excitation with differential gradients, and module of local orientation. These two modules' outputs form a vector of the discriminative function that is entered in the SVM classificators. Yuan and others built a fingerprint-based system for the detection of liveliness in neural BP networks[15]. In this step, the Laplacian operator gets image gradient values, and the BP neural network is tested for different parameters to achieve greater accuracy in detection.

This chapter examines many ways to detect liveliness, as the test attacks countermeasure against spoofing. It has been suggested that non-machine-based learning algorithms and machine-based learning algorithms extract unique features to determine whether an input fingerprint is false or true. The three learning algorithms based on computers that show that machine-learning plays an active role in detecting liveness.

### Template Databases and Countermeasures Attacks

Strikes on biometric prototype network are among the biggest and most harming attacks which will make significant effects on biometric information users. Biometric prototype data is typically put in the enrolment stage in a biometric system database, and is it is balanced with query data at the verification step. Because it is not possible to revoke or reset biometric traits, if new, insecure prototype data are stored in a database, serious security issues could arise. For example , an attacker could hack prototype data in the indexed system to gain access (unauthorized) to a biometric system. This enables artificial biometrics to be produced from prototype data if the original (raw) biometric information is retained in the database. The literature offers a selection of raw prototype data protection strategies which typically can be divided into two classes: biometric and biometric cryptosystems[16].

### Cancelable Biometrics

The idea of trying to cancel biometrics would be to use the non-invertible transitional stage enrollment function that is to turn the main design data into several versions. The same non-invertible transformation on the question data will be applied in the verification stage. Transformed domain matching is accomplished using converted template and query data[17]. Ratha et al. were established t hree distinct transformation forms , which was the cartesian,Polar, and Functional Transformations. The features suggested for transformation intentionally distort the initial features, so the actual prototype data can be impracticable or difficult to access computationally.

However, one of the drawback which was present in the proposed solution is found on registration, thereby allowing for efficient singular dot detection. Owing to uncertainty in biometric (examples like image displacement, nonlinear distortion, and acquisition condition) precise registration is usually difficult. Jin et al. also introduced a authentication scheme which is two-factor, called bio-hashing. This would blend the token-based data with the fingerprint features. This is from the iterative interior model used to carve out new set of features[18]. each value is converted to a binary number within the set of functions, based on a predefined threshold. Lee et al. developed fingerprint templates which is cancelable, by extracting an invariant translation and rotation function used every minute regarded as the first freely aligned, this is one of the template design called the cancelable fingerprint[19]. Ahn et al. developed triplets of minutiae, used as a collection of features, and transformed the geometric properties which was then obtained from the triplets[20]. Yang et al. have built versions that can be cancelled with local and global functions [21]. Local characteristics include relative angles and distances among pairs of minutiae while global characteristics include orientation frequencies and ridges. A perpendicular projection in this work transforms the size of a pair of minutiae to accomplish the transformation that isn't the opposite.

Ahmad and Hu proposed a pair-polar, coordinate-based, alignment-free structure. In this method the relative position of each minute is used for all other minutiae within a collection of polar co-ordinates. Three local characteristics are extracted from any two minutiae, and transformed to generate the cancelable prototype via a functional transformation. Based on the minute structure, The safety and accuracy of the method were further improved by Wang et al. proposing new transformation functions such as infinite-to-one mapping, shortened circular convolutions and part of Hadamard transformation[22,23]. Zhang, and so on, created the minutia-code

(MCC)-based combination plate and functional transformation[24]; the MCC is a well-known local detailed designer that focuses on the 3D local structures of any minute. The authors of MCC subsequently proposed a safety modeling method called P-MCC, which transforms the KL of the MCC function. However P-MCC does not have a revocability property[25,26]. Then, a partial permutation-dependent scheme[27] proposed the introduction of P-MCC cancelability. A stable fingerprint matching system, called P-MCC-PUFs, was subsequently proposed by Arjona et al., involving two variables, P-MCC and PUF (Physically Unclonable Functions). The scheme proposed achieves optimum efficiency when the vector length of the feature is set at 1024 bits and offers reasonable privacy and data security.

Yang y al. A prototype of randomly predicted, cancelable fingerprints was developed. The developed model can defend attacks by recording multiplicity (ARM), due to functional algorithm (decorrelation) [29]. Meanwhile, Delaunay's suggested that local structure (triangulation-based) in the scheme would decrease the detrimental impact of nonlinear distortion based on the matching output. At the feature stage , two structures, local structure and distant structure were fused by Sandhya and Prasad to create binary-evaluated features, protected by a arbitary projection-based cancelable method of protection[30]. Some researchers have proposed using cancelable multimodal biometrics to further improve safety and recognition efficiency. For instance, Yang et al . introduced cancelable, multimodal biometric system that integrates biometric(i.e. fingerprint) and finger-vein features to gain higher precision and certainity identification with security[31]. The solution presented allows use of an enhanced selective, discrete Fourier transformation to guarantee non-invertibility and authentication. In addition, Dwivedi and Dey introduced a hybrid fusion scheme to merge cancelable fingerprint with iris modalities to eliminate drawbacks in each of the modes[32].Experimental testing of cancelable multimodal biometric systems indicates an improvement in efficiency over their unimodal equivalent.

This section deals with the development of biometrics (cancelable)from the initiation and implementation of these cancelable biometries, that is the early transformation function to the new multiple cancelable biometric designs[33-34]. The definition of biometric cancelation comes in two forms. In order to achieve greater accuracy in identification, one category focuses on extracting and representing secure biometric characteristics, and the other category focuses on developing safe transformation functions that are supposed to be mathematically non-invertible[35]. Future work in biometrics (cancelable) is expected to achieve greater acceptance accuracy and security through the use of multiple cancelable biometrics.

**Biometric Cryptosystems**

Biometric cryptosystem unite biometrics into an encryption key that provides a biometric advantage and advantages for the cryptosystem. A biometric cryptosystem can, unlike an annulable biometric device, provide only information matching and not matching, either plug into biometric characteristics such as Fuzzy Engagement (FC) and Fuzzy Vault (FV) or generate the key straight from biometric features such as Fuzzy Extractor (FE)[36, 37 , 38]. Teoh and Kim used the Fuzzy communication method for fingerprinting[39]. Since biometric features are easy in binary formats, authors use a random dynamic calculation to process features. Nevertheless, in most cases where fingerprints match, the minutia set extracted is a point set, and is unordered. The original Fuzzy Vault concept has been applied to fingerprint minutia data [40] in order to safeguard fingerprint minutia data from the point range. The fingerprint minutia data in this method is feasibly bound by a 128-bit cryptographic key but this method involves alignment of images. Nandakumar et al. later implemented a fuzzy vault scheme based on fingerprints and used the high curvature points to help align the image, thus making the alignment more accurate without escaping any orientation or minute location information that is present in the template data[41,42].

Analyzing both of the above methods ( i.e. registration) involves the rotation and translation of the sample image in relation to the template image. Nevertheless, as Zhang et al.[43] reported, the pre-alignment process will cause undeniable noise (e.g. generation of false data and alteration of the specific point position). Alignment-free approaches which do not need a pre-alignment picture will prevent these deficiencies. Li et al . suggested a fuzzy vault scheme incorporating two local structures; the minutiae descriptor and the local structure minutiae[44, 45]. In the proposed system, the two transformation-invariant local structures are implemented using three fusion methods. As compared to the previously mentioned structures for Fuzzy Engagement and Fuzzy Vault, which are key linking schemes, Fuzzy Extractors are key concept-based development schemes[46]. Arakala et al. Introduced the minutiae-based Fuzzy Extractor in fingerprint authentication. Thanks to a minute fingerprint array, all the information are quantized and are represented by a series of binary strings that are then inserted into an existing safe sketch called PinSketch [47,48].Xi y al. Usage of a dual layer local structure as a fuse extractor [49] was suggested. In this process, rotation- and transformation-free dual layer structures are constructed to protect biometric templates from attack. Some other fuzzy extractor systems with improved performance were later proposed as well [50,51]. Liu and Zhao used l1-minimisation to secure and store the templates for fingerprints in cyphertext form [52]. In the encrypted domain, fingerprint matching is completed, and authentication is only successful when the fingerprint demand is near enough to the fingerprint template. Since the prototype is generated using the Minutia Cylinder-Code (MCC) with the proper design of the secure algorithm, the proposed system achieves high recognition safety and accuracy[53,54].

Since traditional biometric cryptosystems are not equipped with revocability, recent use has been made of the cancelable technique to improve the biometric cryptosystem reliability. Yang et al. Suggested a Fuzzy Vault cancelation process to encrypt fingerprint-based characteristics of the Delaunay triangle group [55]. The cancelable change is accomplished by polar transformation. In this work, the unit of transformation is a triangle rather than a single minute which helps the device to be less prone to biometric uncertainty [56]. Alam et al. have put forward a biometric cryptosystem that combines Fourier's discrete transformation (DFT) with random projection-based cancelable technique to improve safety [57]. From DFT, Polar grid-based fingerprint features and random projection are integrated into the proposed frame and a noninvertible prototype is developed. Optionally, a little toggling is often used to insert noise into the template generated to further improve the protection of the template. Sarkar and Singh introduced the whole new level of cryptographic keys for fingerprint templates that could be cancelled[58]. Specific fingerprint models are disabled and reissued for specific 128-bit long keys[59]. This removes the risk of leakage after the receiver and sender acceptance of the same secret key.

This section provides an extensive discussion and analysis of biometric cryptosystems. For example from the original concepts of Fuzzy Engagement [52], Fuzzy Vault [53] and Fuzzy Extractor [55] and extracted then to many complex algorithms [60, 61,62]. The benefits of encrypted biometric systems is the one when they can directly link or build a cryptographic key that can be used to authenticate and encrypt data. Nevertheless, most encrypted biometric systems neglect the cancelability [63]. Some investigators took this issue to heart and developed revocable biometric cryptosystems to improve device security [64,65]. It should be noted that in increasingly biometric applications, such as face and voice recognition, deep learning techniques have now been used, but there is almost no research on deep learning-based biometric protection [66,67]. This section will also focus on the further research efforts.

### Recognition Accuracy

Biometrics provide major benefits and are used in many applications, but are faced with challenges including insufficient precision in non-ideal environments or in encrypted domains when implementing models.

### 1. Accuracy comparison Ideal vs. Non-Ideal Conditions

Biometric systems often face unreasonable standards for coherence that corresponds to conventional password induced authentication systems. Still, a password-based system, as the password input matches, offers access and vice versa. However, the accuracy of biometric matching can not be 100%. Biometric system accuracy can be calculated using well-known metrics, such as the FAR False Accept Rate, FRR False Reject Rate and Equivalent Error Rate (EER). Precision of recognition usually depends on factors such as image quality performance and corresponding algorithms. The researchers have achieved significant precision and documented this with decades of effort. For example , the online assessment platform FVC-ongoing allows scientists to upload recognition algorithms and compete with other matching algorithms[68,69]. FVC-ongoing offers a benchmark to test these algorithms using a series of sequestrated databases and to calculate outcomes at a rate equal to acceptance and rejection errors[70] by means of Strong, FRR and EER metrics. The latest findings on the FVC-continuing website suggest that the EER = 0.022% has achieved the highest reliability from the fingerprint verification contest, whereas the Beijing Hisign Bio-info Institute also submitted the algorithm called HXKJ[71]. The fingerprint matching algorithm, based on the state of the art MCC (Minutia Cylinder Code), achieved an EER of = 0.48% for FVC2002 DB2, and an EER of = 0.12% for FVC2006 DB2 respectively. Cao et al. To refinish a poor fingerprint picture a latent segmentation and enhancement algorithm[72] has been proposed. A maximum change of decomposition model will reduce the piece-wise background noise and multiple overlapping patches are observed and used for enhancing lateness. resulting in better performance matching. Similarly, with the ultimate goal of increasing matching precision, Araro et al. incorporated input from an example to improve the extracted features from a latent fingerprint image [73].

## 2. With vs. Without Template Protection Accuracy

Model security strategies provide security for and protected biometric models

The prototype will leak off as little details as possible from the initial design[74]. Biometrically cryptosystems, reference point information can help improve accuracy of recognition but essential details about the original prototype leaks, which should not therefore it has been common. Random transformation (projection-based) in cancelable biometrics is a standard collective-to-one mapping when dimensions of the original prototype are reduced. A lower-dimensional transformed template is better, because less knowledge about the original template is retained. Nevertheless, with less details preserved from the original design this can contribute to a loss of accuracy [50,75]. Thus there's a balance between accuracy of recognition and defense. It can be shown that, under ideal circumstances, away from real-life environments where the images (e.g. latent fingerprints) collected are of extremely poor quality, the precaution in identifying most biometric devices, with or without prototype protection, is tested[76,77]. Additionally, the reliability of a template-protected system recognition is weaker than that without the template security[78]. The key reason for this is the lack of expertise in the feature adaptation process which translates the original features into a different format matching the corresponding metrics for transformed models , e.g. imitating distance for fuzzy engagement and setting an deviation for fuzzy vault [79,80].Therefore, further research needs to be put into developing stable applications and effective feature-adaptation methods to reduce information loss.

## 2. Conclusions

This article presents a comprehensive evaluation of various essential (as well as competing) initiatives for biometric systems based on fingerprints; that is, security and precision in recognition. As for health, we studied two sorts of threats: user interface attacks, and template database attacks. There is also talks of countermeasures to protect against such assaults. Although improved accuracy of recognition within faulty conditions and new progress in biometric template protection, there are always a range of open issues that call on biometric investigators to resolve. In subsequent work, we explain some obstacles and paths:

1. New advances in deep learning techniques have increased the efficiency of biometric devices through a variety of biometric modalities, for example face-recognition. Deep learning techniques are also considered potential methods to match latent fingerprints [81, 82]. But the use of deep learning algorithms due to the limitations of the algorithms themselves can pose potential threats to biometric systems.

2. For any biometric system on different platforms, like a mobile platform, the safety issues analyzed for a general biometric system ( e.g. spoofing attacks, attacks on biometric templates) are also real. Today, smartphones are becoming increasingly popular, providing a promising platform for biometric usage[83]. Nevertheless, mobile biometrics face more challenges, as smartphones usually have less processing resources and limited storage. Thus, an emerging subject of study is a lightweight, robust architecture of mobile biometric algorithms.

3. Exchange-off between fingerprint model identification security and accuracy continuesto be a safety issue. The highest fingerprint output with protection of the template is the EER = 1.542 percent which is far higher than that EER = 0.022 percent lacking security of the templates. In addition to creating more robust and distinctive features, and better transition functions, the use of multibiometrics is likely the way forward in designing template protection and needs further study.

## 3. 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.

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.

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

17. 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.

18. 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.

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

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

21. 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.

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

23. 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.

24. 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.

25. 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.

26. Galbally, J.; Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. A high performance fingerprint liveness detection method based on quality related features. Future Gener. Comput. Syst. **2012**, 28, 311– 321.

27. Kim, W. Fingerprint liveness detection using local coherence patterns. IEEE Signal Process. Lett. **2017**, 24, 51– 55.

28. Jung, H.; Heo, Y. Fingerprint liveness map construction using convolutional neural network. Electron. Lett. **2018**, 54, 564– 566.

29. Kundargi, J.; Karandikar, R. Fingerprint liveness detection using wavelet-based completed LBP descriptor. In Proceedings of the 2nd International Conference on Computer Vision and Image Processing, Roorkee, India, 9– 12 September 2017; Springer: Berlin, Germany, 2018; pp. 187– 202.

30. Xia, Z.; Yuan, C.; Lv, R.; Sun, X.; Xiong, N.N.; Shi, Y.-Q. A novel weber local binary descriptor for fingerprint liveness detection. IEEE Trans. Syst. Man Cybern. Syst. **2018**.

31. Yuan, C.; Sun, X.; Wu, Q.J. Difference co-occurrence matrix using BP neural network for fingerprint liveness detection. Soft Comput. **2018**, 1– 13.

32. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. **2001**, 40, 614– 634.

33. Ratha, N.K.; Chikkerur, S.; Connell, J.H.; Bolle, R.M. Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **2007**, 29, 561– 572.

34. Jin, A.T.B.; Ling, D.N.C.; Goh, A. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn. **2004**, 37, 2245– 2255.

35. Lee, C.; Choi, J.-Y.; Toh, K.-A.; Lee, S. Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE Trans. Syst. Man Cybern. Part B Cybern. **2007**, 37, 980– 992.

36. Ahn, D.; Kong, S.G.; Chung, Y.-S.; Moon, K.Y. Matching with secure fingerprint templates using non-invertible transform. In Proceedings of the Congress on Image and Signal Processing (CISP’ 08), Sanya, China, 27– 30 May 2008; pp. 29– 33.

37. Yang, H.; Jiang, X.; Kot, A.C. Generating secure cancelable fingerprint templates using local and global features. In Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2009), Beijing, China, 8– 11 August 2009; pp. 645– 649. Symmetry **2019**, 11, 141 17 of 19

38. Ahmad, T.; Hu, J. Generating cancelable biometrie templates using a projection line. In Proceedings of the 11th International Conference on Control Automation Robotics and Vision (ICARCV), Singapore, 7– 10 December 2010; pp. 7– 12.

39. Wang, S.; Deng, G.; Hu, J. A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recogn. **2017**, 61, 447– 458.

40. Wang, S.; Hu, J. Alignment-free cancellable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. Pattern Recogn. **2012**, 45, 4129– 4137.

41. Wang, S.; Hu, J. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recogn. **2014**, 47, 1321– 1329.

42. Wang, S.; Hu, J. A blind system identification approach to cancelable fingerprint templates. Pattern Recogn. **2016**, 54, 14– 22.

43. Zhang, N.; Yang, X.; Zang, Y.; Jia, X.; Tian, J. Generating registration-free cancelable fingerprint templates based on Minutia Cylinder-Code representation. In Proceedings of the IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 29 September– 2 October 2013; pp. 1– 6.

44. Cappelli, R.; Ferrara, M.; Maltoni, D. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. IEEE Trans. Pattern Anal. Mach. Intell. **2010**, 32, 2128– 2141.

45. Ferrara, M.; Maltoni, D.; Cappelli, R. Non-invertible minutia cylinder-code representation. IEEE Trans. Inf. Foren. Sec. **2012**, 7, 1727– 1737.

46. Ferrara, M.; Maltoni, D.; Cappelli, R. A two-factor protection scheme for MCC fingerprint templates. In Proceedings of the 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10– 12 September 2014; pp. 1– 8.

47. Arjona, R.; Prada-Delgado, M.A.; Baturone, I.; Ross, A. Securing minutia cylinder codes for fingerprints through physically unclonable functions: An exploratory study. In Proceedings of the 2018 International Conference on Biometrics (ICB), Gold Coast, Australia, 20– 23 February 2018; pp. 54– 60.

48. Yang, W.; Hu, J.; Wang, S.; Wu, Q. Biometrics based Privacy-Preserving Authentication and Mobile Template Protection. Wirel. Commun. Mobile Comput. **2018**, 2018, 17.

49. Sandhya, M.; Prasad, M.V. Securing fingerprint templates using fused structures. IET Biom. **2017**, 6, 173– 182.

50. Yang,W.;Wang, S.; Hu, J.; Zheng, G.; Valli, C. A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recogn. **2018**, 78, 242– 251.

51. Dwivedi, R.; Dey, S. A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. arXiv, 2018; arXiv:1805.10433.

52. Juels, A.; Wattenberg, M. A fuzzy commitment scheme. In Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 1– 4 November 1999; pp. 28– 36.

53. Uludag, U.; Jain, A.K. Fuzzy fingerprint vault. In Proceedings of theWorkshop Proceedings—Biometrics: Challenges Arising from Theory to Practice, Cambridge, UK, 22– 27 August 2004; pp. 13– 16.

54. Juels, A.; Sudan, M. A fuzzy vault scheme. Des. Codes Cryptogr. **2006**, 38, 237– 257.

55. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Proceedings of the Advances in Cryptology-Eurocrypt 2004, Interlaken, Switzerland, 2– 6 May 2004; pp. 523– 540.

56. Teoh, A.B.J.; Kim, J. Secure biometric template protection in fuzzy commitment scheme. IEICE Electron. Exp. **2007**, 4, 724– 730.

57. Uludag, U.; Pankanti, S.; Jain, A.K. Fuzzy vault for fingerprints. In Proceedings of the 5th International Conference on Audio-and Video-Based Biometric Person Authentication, Hilton Rye Town, NY, USA, 20– 22 July 2005; pp. 310– 319.

58. Nandakumar, K.; Jain, A.K.; Pankanti, S. Fingerprint-based fuzzy vault: Implementation and performance. IEEE Trans. Inf. Forensics Secur. **2007**, 2, 744– 757.

59. Zhang, P.; Hu, J.; Li, C.; Bennamoun, M.; Bhagavatula, V. A pitfall in fingerprint bio-cryptographic key generation. Comput. Secur. **2011**, 30, 311– 319.

60. Li, P.; Yang, X.; Cao, K.; Tao, X.;Wang, R.; Tian, J. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. J. Netw. Comput. Appl. **2010**, 33, 207– 220.

61. Arakala, A.; Jeffers, J.; Horadam, K. Fuzzy extractors for minutiae-based fingerprint authentication. In Proceedings of the 2007 International Conference on Advances in Biometrics, Seoul, Korea, 27– 29 August 2007; pp. 760– 769.

62. Xi, K.; Hu, J.; Han, F. An alignment free fingerprint fuzzy extractor using near-equivalent Dual Layer Structure Check (NeDLSC) algorithm. In Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), Beijing, China, 21– 23 June 2011; pp. 1040– 1045.

63. Karthi, G.; Azhilarasan, M. Hybrid multimodal template protection technique using fuzzy extractor and random projection. IJRCCT **2013**, 2, 381– 386.

64. Yang, W.; Hu, J.; Wang, S. A Delaunay Triangle-Based Fuzzy Extractor for Fingerprint Authentication. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 25– 27 June 2012; pp. 66– 70.

65. Liu, E.; Zhao, Q. Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with I1 minimization. Neurocomputing **2017**, 259, 3– 13.

66. Yang,W.; Hu, J.;Wang, S. A Delaunay triangle group based fuzzy vault with cancellability. In Proceedings of the 2013 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, 16– 18 December 2013; pp. 1676– 1681.

67. Alam, B.; Jin, Z.; Yap, W.-S.; Goi, B.-M. An alignment-free cancelable fingerprint template for bio-cryptosystems. J. Netw. Comput. Appl. **2018**, 115, 20– 32.

68. Sarkar, A.; Singh, B.K. Cryptographic key generation from cancelable fingerprint templates. In Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 15– 17 March 2018; pp. 1– 6.

69. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. Nature **2015**, 521, 436.

70. Cappelli, R.; Maio, D.; Maltoni, D.;Wayman, J.L.; Jain, A.K. Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern Anal. Mach. Intel. **2006**, 28, 3– 18.

71. Yoon, S.; Cao, K.; Liu, E.; Jain, A.K. LFIQ: Latent fingerprint image quality. In Proceedings of the 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 29 September– 2 October 2013; pp. 1– 8.

72. Cao, K.; Liu, E.; Jain, A.K. Segmentation and enhancement of latent fingerprints: A course to fine ridgestructure dictionary. IEEE Trans. Pattern Anal. Mach. Intell. **2014**, 36, 1847– 1859.

73. Arora, S.S.; Liu, E.; Cao, K.; Jain, A.K. Latent fingerprint matching: Performance gain via feedback from exemplar prints. IEEE Trans. Pattern Anal. Mach. Intell. **2014**, 36, 2452– 2465.

74. Nandakumar, K.; Jain, A.K. Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Process. Mag. **2015**, 32, 88– 100.

75. Yang, W.; Wang, S.; Zheng, G.; Chaudhry, J.; Valli, C. ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures. J. Supercomput. **2018**, 74, 4893– 4909.

76. Liu, E.; Zhao, H.; Liang, J.; Pang, L.; Xie, M.; Chen, H.; Li, Y.; Li, P.; Tian, J. A key binding system based on n-nearest minutiae structure of fingerprint. Pattern Recogn. Lett. **2011**, 32, 666– 675.

77. Yang, W.; Hu, J.; Wang, S.; Stojmenovic, M. An Alignment-free fingerprint bio-cryptosystem based on modified voronoi neighbor structures. Pattern Recogn. **2014**, 47, 1309– 1320.

78. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz,W.R.; Pedrini, H.; Falcao, A.X.; Rocha, A. Deep representations for iris, face, and fingerprint spoofing detection. IEEE Trans. Inf. Foren. Sec. **2015**, 10, 864– 879.

79. Goodfellow, I.; Bengio, Y.; Courville, A. Deep Learning; MIT press: Cambridge, MA, USA, 2016; Volume 1, 800p.

80. Pandya, B.; Cosma, G.; Alani, A.A.; Taherkhani, A.; Bharadi, V.; McGinnity, T.M. Fingerprint classification using a deep convolutional neural network. In Proceedings of the 2018 4th International Conference on Information Management (ICIM), Oxford, UK, 25– 27 May 2018; pp. 86– 91.

81. Yang, W.; Hu, J.; Yang, J.; Wang, S.; Lu, L. Biometrics for securing mobile payments: Benefits, challenges and solutions. In Proceedings of the 2013 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, 16– 18 December 2013; pp. 1699– 1704.

82. Spolaor, R.; Li, Q.; Monaro, M.; Conti, M.; Gamberini, L.; Sartori, G. Biometric authentication methods on smartphones: A survey. PsychNology J. **2016**, 14, 87– 98.

83. Wojciechowska, A.; Chora´s, M.; Kozik, R. The overview of trends and challenges in mobile biometrics. J. Appl. Mathem. Comput. Mech. **2017**, 16, 173– 185.

84. Rattani, A.; Reddy, N.; Derakhshani, R. Convolutional neural networks for gender prediction from smartphone-based ocular images. IET Biom. **2018**, 7, 423– 430.