Edith Cowan University

Research Online

2019

Security and accuracy of fingerprint-based biometrics: A review

Wencheng Yang
Edith Cowan University

Song Wang

Jiankun Hu

Guanglou Zhang
Edith Cowan University

Craig Valli
Edith Cowan University

Security and Accuracy of Fingerprint-Based Biometrics: A Review

Wencheng Yang [1,*] , **Song Wang** [2] , **Jiankun Hu** [3] , **Guanglou Zheng** [1] and **Craig Valli** [1]

1   Security Research Institute, Edith Cowan University, Joondalup, WA 6207, Australia;
    G.Zheng@ecu.edu.au (G.Z.); C.Valli@ecu.edu.au (C.V.)
2   Department of Engineering, La Trobe University, Victoria 3083, Australia; Song.Wang@latrobe.edu.au
3   School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600,
    Australia; J.Hu@adfa.edu.au
*   Correspondence: W.Yang@ecu.edu.au; Tel.: +61-8-6304-5210

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. It is shown in the paper that researchers continue to face challenges in tackling the two most critical attacks to biometric systems, namely, attacks to the user interface and template databases. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is a hot research topic currently, as well as 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. Related challenges and current research trends are also outlined in this paper.

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

1. 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 smartphones 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—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 [3,4]—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.
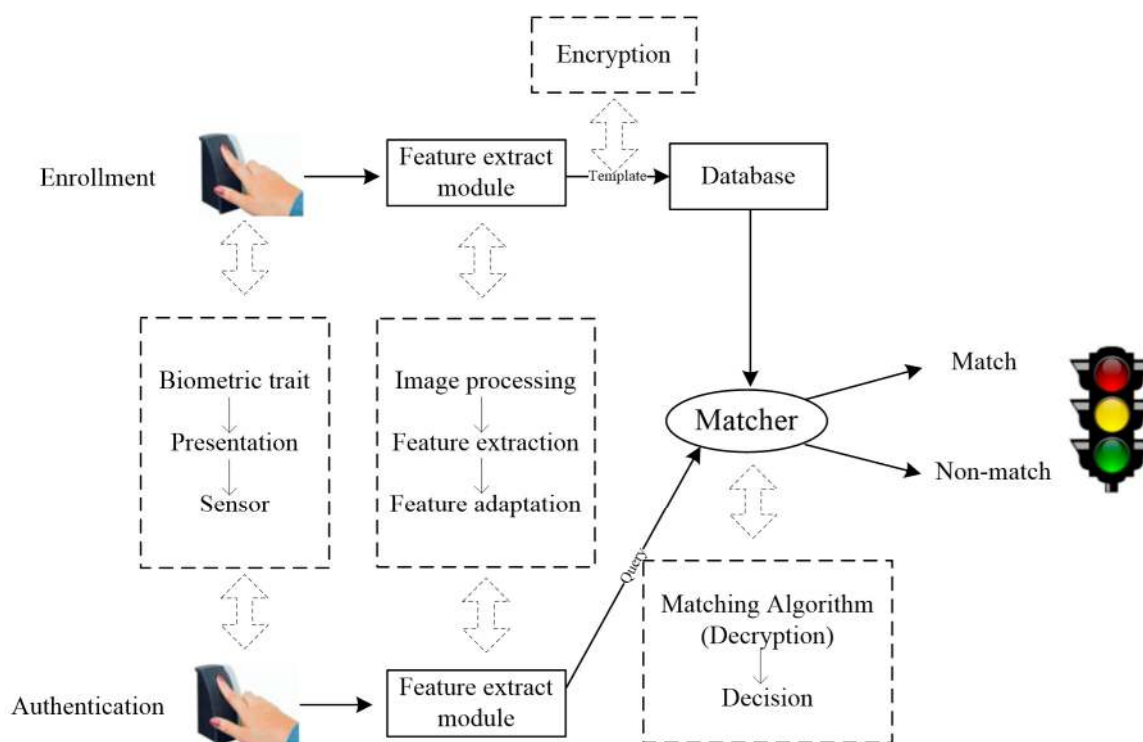

Figure 1. An example of two stages—enrollment and verification—in a biometric authentication system.

Due to some specific properties possessed by biometrics, biometric systems have been adopted in many civilian and military applications [5–8] in the areas of law enforcement, border control, consumer or residential biometrics, and financial services.

(1) Law enforcement: Biometric technology has been embraced with open arms by law enforcement agencies across the world for its efficiency in security-oriented scenarios. In fact, biometrics is not a new tool in law enforcement. Fingerprint biometrics have been adopted by Argentinian criminologists for more than a century. Nowadays, with rapid technological development, biometrics have launched a worldwide revolution in law enforcement. Biometric recognition systems have now been utilized by law enforcement agencies of many countries, including the United States, United Kingdom, Australia, and China. For example, in 2011, the Department of Defense and the FBI started working on the United States' next generation biometric system, named Next Generation Identification (NGI), which is designed to include fingerprint, face, iris, and palm data, and their facial recognition program became fully operational in late 2014 [9].

(2) Border control: In order to prevent identity fraud and strengthen border and national security, many countries employ biometric systems to track and manage the flow of passengers across borders. For instance, since 2008, all non-Americans who travel to the United States are requested to scan their fingerprint by US border security officials [10]. In order to eliminate the need for paper passports, Australia is planning to boost its "Seamless Traveler" program. The proposal

of this program is to have 90 percent of the 35 million annual travelers to enter Australia via a paperless biometric recognition system by 2020 [11].

(3) Consumer biometrics: Consumer devices equipped with biometric systems are standalone products for the consumer market, such as door locks, surveillance systems, automotive, and especially mobile devices (smartphones, tablets, etc.). In the past, passwords were the only secure way of authentication, and fingerprint scanners were most likely used by law enforcement agencies and the military. However, times have changed. In the last decade, biometric technology has developed in leaps and bounds and spread to every corner of our lives as a more secure method of authentication. With the popularity of smart phones, mobile phones utilizing biometrics is a winning combination in the consumer market, allowing biometric technology to become much more widely accepted [12].

(4) Financial services: Finance is the most mature biometrics market outside the domain of law enforcement for the logic that protecting money is the first priority for most people. Financial companies have been early adopters of biometrics. For example, cash machines with fingerprint readers are currently deployed at an increasing pace [13]. Moreover, a new MasterCard, which includes an embedded fingerprint reader, attempts to introduce a biometric authentication layer for card payment [14], so as to enhance customers' comfort level in terms of security and convenience.

Compared with other biometric traits (e.g., face, iris, and voice), fingerprint-based recognition systems are studied most extensively and deployed most widely. For a fingerprint, the pattern of valleys and ridges is determined after birth, and different fingerprint patterns are owned by even identical twins [1]. It has been reported that the recognition accuracy of fingerprint-based recognition systems is very high [15], with the general public showing medium acceptability to fingerprint acquisition [16]. This is why fingerprint biometric systems occupy a large market share and have been adopted in various applications. Although fingerprint recognition shows substantial strength and a prosperous future, it has some unsolved issues, such as insufficient accuracy and security concerns.

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:

i. 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.

ii. Based on a thorough analysis, limitations of existing research are discussed and suggestions for future work to overcome those limitations are provided.

iii. 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.

iv. Most existing methods, either with or without template protection, were set forth in ideal situations. In this paper, we emphasize the importance of considering recognition accuracy under non-ideal conditions. Our analysis is backed by solid evidence and detailed comparison.

The rest of this paper is organized as follows. In Section 2, the security of biometrics is thoroughly analyzed from the perspective of attack points and countermeasures. In Section 3, system recognition accuracy under different conditions is discussed. The conclusion and future work is given in Section 4.

2. 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 [17]. Ratha et al. [18] identified eight different points of attacks in a biometric system, which is shown in Figure 2. 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, e.g., attacks at point 1;
(b)   Attacks at the modules, e.g., attacks at points 3 and 5;
(c)   Attacks to the channels between modules, e.g., attacks at points 2, 4, 7, and 8;
(d)   Attacks to the template database, e.g., attacks at point 6.
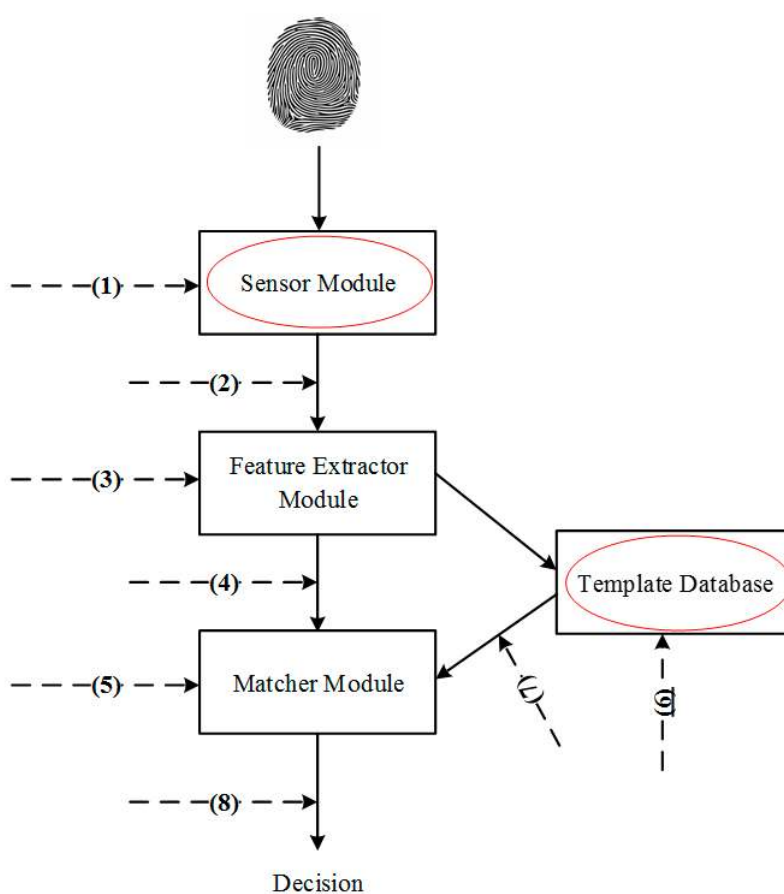
Figure 2. Eight possible attack points to a typical biometric authentication system (adapted from [18]).

Here, threats and security issues related to those attack points in different stages of a generic biometric system are listed in Table 1. In light of the two major concerns mentioned above, in this paper we focus on the investigation of Attacks 1 and 11 (in Table 1) from attack categories a and d (labeled by the red circles in Figure 2), since they represent the most serious and critical threats to users' security and privacy [19].

Table 1. Threats and security issues related to attack points of a generic biometric system (adapted from [20]).

Number	Attacks	Attack Points
1	Spoofing—present fake biometric data to sensor	1
2	Exploit similarity, e.g., using face from identical twins	1
3	Zero-effort attempt—attacker uses own biometric sample to impersonate an authorized user	1
4	Physically destroy the biometric sensor so as to make it out of service	1
5	Replay attack—the attacker intercepts a biometric signal and replay it into the system	2 and 4
6	Cut the communication channel to make the system unavailable	2 and 4
7	Denial of Service attack—alters the information from the channel in order to deny a genuine user from being authenticated	2 and 4
8	Hill-climbing attack—conveniently modify the query image until a desired matching score is obtained.	2 and 4
9	Continuously inject samples in order to deny genuine users to access the system	2 and 4
10	Inject Trojan horse programs	3 and 5
11	Attacker illegally obtains original biometric templates	6
12	Attacker modifies the template such as adding or replacing info	6
13	Read biometric templates from a communication channel and replay	7
14	Alter the information transmitted through a communication channel in order to deny genuine users to access the system	7
15	Cut the communication channel in order to make the system unavailable	7
16	Alter the transported matching or non-matching information in order to deny access of a genuine user or allow an impostor access.	8
17	Cut the communication channel in order to make the system unavailable	8

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 [21]. Also, a total of 11 different fingerprint-based authentication systems are attacked with fake fingerprint films [22], with results showing that fake fingerprint films can be enrolled in the systems and fake fingerprints are accepted with more than 67% probability. 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 [23], 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 [22]. However, hardware-based solutions are usually more expensive.

Tan and Schuckers [24] 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. 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. [25] utilized static features together with dynamic features for fingerprint vitality detection. Before this method was proposed, the static and dynamic features of a fingerprint had been studied separately. Relevant benefits of using both features and performance improvement were achieved and reported in the paper.

Galbally et al. [26] 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 [27] designed an image descriptor to handle fingerprint liveness detection. It is observed [27] 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.

Jung and Heo [28] 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 [29] proposed using a texture descriptor, called completed local binary pattern (CLBP), together with the wavelet transform (WT) for fingerprint liveness detection. 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. [30] 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. [31] introduced a BP neural network based fingerprint liveness detection method. 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 algorithms [24–27,29] and machine learning based algorithms [28,30,31] were proposed to extract unique features to ascertain whether an input fingerprint is fake or real. The three machine learning based algorithms [28,30,31] were all recently published (in 2018), which shows that machine learning is playing an active role in liveness detection design. A comparison of all the above approaches to fingerprint liveness detection is reported in Table 2.

Table 2. The comparison of approaches for fingerprint liveness detection.

Approaches	Year of Publication	Category or Technique	Databases	Sensors	Best Performance (Correct Classification Rate)
Tan and Schuckers [24]	2006	Wavelet transform	Michigan State University (MSU) gummy finger database	Capacitive DC, optical, and electro-optical	80%–100%
Coli et al. [25]	2008	Both static and dynamic features	Private database	Optical	75.35%
Galbally et al. [26]	2012	Fingerprint parameterization based on 1uality related features	ATVS	Optical	90%
Kim [27]	2017	Difference of the dispersion in the image gradient field	LivDet 2009 and ATVS	Optical	95.63% (ATVS) 86.83% (LivDet 2009)
Jung and Heo [28]	2018	Convolutional neural network (CNN)	2015 competition set	Optical	98.60%
Kundargi and Karandikar [29]	2018	Completed local binary pattern (CLBP) and wavelet transform (WT)	LivDet 2011	Optical	91.7%
Xia et al. [30]	2018	Weber local binary and Support Vector Machine (SVM)	LivDet 2011, 2013, 2015	Optical	94.04%
Yuan et al. [31]	2018	BP neural network	LivDet 2013	Optical	93.22%

2.2. 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, according to [19].

2.2.1. 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 [32].

Ratha et al. [33] 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. [34] 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. Then each value in the feature set is converted to a binary number based on a predefined threshold. Lee et al. [35] 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. Ahn et al. [36] used triplets of minutiae as a feature set, and transformation is performed on geometrical properties derived from the triplets. Yang et al. [37] created cancelable

templates by using both local and global features. 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 [38] 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 in [38], Wang et al. [39–42] 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. [43] designed a combo plate and a functional transformation to produce cancelable templates based on the Minutia Cylinder-Code (MCC) [44]. 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 [45], which performs a KL transformation on the MCC feature representation. However, P-MCC does not have the property of revocability. Then, 2P-MCC was proposed to add cancelability to P-MCC using a partial permutation based scheme [46]. Later, Arjona et al. [47] 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. [48] 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 matching performance. Sandhya and Prasad [49] 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. [50] 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 [51] 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 [33], to the recent multiple cancelable biometrics [50], is presented. There are two categories in the design of cancelable biometrics. One category centers around the extraction and representation of stable biometric features [36–38,48] 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 [39–42,46]. 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.

2.2.2. 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) [52] and fuzzy vault (FV) [53,54], or directly generating the key from the biometric features, for example, fuzzy extractor (FE) [55].

Teoh and Kim [56] 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. [57] 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. [58] 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. [59]. Alignment-free approaches that require no image pre-alignment can avoid the above shortcomings. Li et al. [60] 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 introduced in [55]. Arakala et al. [61] 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. [62] 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 [63,64] were also proposed with enhanced performance. Liu and Zhao [65] utilized l_1-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) [44] 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. [66] proposed a cancelable fuzzy vault system to encrypt the Delaunay triangle group based fingerprint features. The cancelable transformation is 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. [67] 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 [68] 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 [52], fuzzy vault [53], and fuzzy extractor [55], to various complex algorithms derived afterwards [60–64]. 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 cancelability. Some researchers realized this problem and thus developed biometric cryptosystems

with revocability [67,68], so as to enhance system security. It is worth noting that nowadays deep learning techniques [69] 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.

A comparison of all the above fingerprint template protection approaches, whether it be cancelable biometrics or biometric cryptosystems, are reported in Tables 3 and 4, respectively.

Table 3. The comparison of cancelable biometrics for fingerprint template protection.

Cancelable Biometrics				
Approaches	Year of Publication	Category or Technique	Databases	Best Performance
Ratha et al. [32]	2001	Introduction of the "cancelable biometrics" concept	-	-
Jin et al. [34]	2004	Bio-hashing	FVC2002 DB1-DB4	EER = 0
Ratha et al. [33]	2007	Cartesian, polar, and surface folding transformations	-	-
Lee et al. [35]	2007	The first alignment-free cancelable fingerprint system	FVC2002 DB1	EER = 3.4%
Ahn et al. [36]	2008	Using triplets of minutia points	FVC2002 DB2	EER = 3.61%
Yang et al. [37]	2009	Using local and global features	FVC2002 DB2	EER = 13%
Ahmad and Hu [38]	2010	Using a projection line	FVC2002 DB2	EER ≈ 20%
Wang and Hu [40]	2012	A densely infinite-to-one mapping (DITOM) approach	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER = 3.5% EER = 5% EER = 7.5%
Zhang et al. [43]	2013	A registration-free cancelable fingerprint template based on Minutia Cylinder Code (MCC)	-	-
Wang and Hu [41]	2014	Curtailed circular convolution	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER = 2% EER = 3% EER = 6.12%
Ferrara et al. [46]	2014	A two-factor protection scheme using non-invertible transformation and user-specific key	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2002 DB4 FVC2004 DB1 FVC2006 DB2	EER = 2% EER = 1.1% EER = 4.4% EER = 3.1% EER = 3.0% EER = 0.1%
Wang and Hu [42]	2016	A blind system identification approach	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=4% EER=3% EER=8.5%
Wang et al. [39]	2017	A partial Hadamard transform approach	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2004 DB2	EER = 1% EER = 2% EER = 5.2% EER = 13.3%
Sandhya and Prasad [49]	2017	Using fused structures (both local and distant structures) at the feature level	FVC2004 DB1 FVC2004 DB2 FVC2004 DB3	EER = 11.89% EER = 12.71% EER = 17.60%
Arjona et al. [47]	2018	Physically Unclonable Functions based on minutia cylinder codes	FVC2002 DB2 FVC2002 DB3	EER = 0.39% EER = 0.81%
Yang et al. [48]	2018	Defeat the attacks via record multiplicity (ARM) through the feature decorrelation algorithm	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2004 DB2	EER = 5.75% EER = 4.71% EER = 10.22% EER = 12%
Yang et al. [50]	2018	Cancelable multi-biometric system based on fingerprint and finger-vein	MD-A MD-B	EER = 0.55% EER = 0.69%
Dwivedi and Dey [51]	2018	Fusion at the score level and the decision level	Virtual_A Virtual_B Virtual_C	EER = 0.55% EER = 0.13% EER = 0.5%

Table 4. The comparison of biometric cryptosystems for fingerprint template protection.

		Biometric Cryptosystems		
Approaches	Year of Publication	Category or Technique	Databases	Best Performance
Juels and Watternberg [52]	1999	Introduction of the cryptographic primitive, fuzzy commitment scheme	-	-
Uludag and Jain [53]	2004	Utilization of a fingerprint minutiae line based representation scheme in fuzzy vault	-	-
Dodis et al. [55]	2004	Proposes two primitives: fuzzy extractor and secure sketch	-	-
Uludag et al. [57]	2005	Realization of fuzzy vault with the fingerprint minutiae data	IBM-GTDB	FAR = 0
Arakala et al. [61]	2007	The first fingerprint biometric application—protected Fuzzy Extractor	FVC2000	EER ≈ 10%
Teoh and Kim [56]	2007	Randomized dynamic quantization, transformation to binarized biometric data, and protection by using fuzzy commitment	FVC2002 DB1	FAR = 0, FRR = 0.9%
Nandakumar et al. [58]	2007	An automatic implementation of the fuzzy vault scheme based on fingerprint minutiae. High curvature points are derived from the fingerprint orientation field as helper data to align the template and query minutiae	FVC2002 DB2	FAR = 0, FRR = 10%
Li et al. [60]	2010	An alignment-free fingerprint cryptosystem based on the fuzzy vault scheme, fusing the local features, known minutia descriptor, and minutia local structure	FVC2002 DB1, DB2	FAR = 0.35, FRR = 17.5% FAR = 0, FRR = 10%
Xi et al. [62]	2011	Use the minutia local structure called Dual Layer Structure Check (DLSC) to eliminate the alignment process	FVC2002 DB2	EER = 4.5%
Yang et al. [64]	2012	A registration-free Delaunay triangle-based fuzzy extractor.	FVC2002 DB2	EER = 13%
Karthi and Azhilarasan [63]	2013	Use both the key generating cryptosystem and feature transformation method	FVC2004	FAR = 1%, FRR = 1%
Yang et al. [66]	2013	A minutiae-based fuzzy vault with cancelability by applying a polar transformation to each Delaunay triangle group	FVC2002 DB1, DB2	FAR = 0.38%, FRR = 19% FAR = 2.25%, FRR = 8%
Liu and Zhao [65]	2017	A secured fingerprint MCC matching scheme utilizing l_1-minimization	FVC2002 DB1, DB2 FVC2004 DB1	FAR = 0, FRR = 8.6% FAR = 0, FRR = 16% FAR = 0, FRR = 34.4%
Alam et al. [67]	2018	Bit-toggling strategy to inject noise into the proposed fingerprint template	FVC2002 DB1, DB2, DB3 FVC2004 DB1, DB2, DB3	EER = 1% EER = 2.07% EER = 6.11% EER = 15.44% EER = 9.15% EER = 9.28%
Sarkar and Singh [68]	2018	A symmetric cryptographic key is spawned using cancelable fingerprint template	FVC2002 DB1	-

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.

3.1. 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 [15], 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 [70]. According to the latest results shown on the FVC-ongoing platform [15], 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. The best three matching results of fingerprint (with and without template protection) verification competitions are listed in Table 5, extracted from [15], from which we can see that all of them were contributed by companies. Some algorithms designed by academic researchers also achieve gratifying accuracy. The state-of-the-art MCC (Minutia Cylinder Code) [44] based fingerprint matching algorithm achieved the EER = 0.49% on database FVC2002 DB2, and the EER = 0.12% on database FVC2006 DB2 [45].

Table 5. The best three results of fingerprint verification competitions on the Fingerprint Verification Competition (FVC)-ongoing platform.

	Published on	Benchmark	Participant	Type	Algorithm	EER
Without template protection	27/07/2017	FV-STD-1.0	Beijing Hisign Bio-info Institute	Company	HXKJ	0.022%
	09/02/2016	FV-STD-1.0	Neurotechnology Company	Company	MM_FV	0.042%
	29/08/2011	FV-STD-1.0	Tiger IT Bangladesh	Company	TigerAFIS	0.108%
With template protection	28/12/2013	STFV-STD-1.0	Securics, Inc	Company	Biotope	1.541%
	25/03/2013	STFV-STD-1.0	Biometric System Laboratory	Academic Research Group	P-MCC64	2.207%
	25/02/2013	STFV-STD-1.0	Institute of Automation, Chinese Academy of Sciences	Academic Research Group	SCT	4.082%

However, all the above matching results are based on databases (e.g., FV-STD-1.0) containing images with better quality than images acquired under non-ideal conditions, such as fingerprint images from crime scenes. In Figure 3, we show a comparison of sample fingerprint images from FV-STD-1.0 used in the FVC-ongoing Competition and sample images obtained from non-ideal conditions.

The images acquired from the surfaces of objects at crime scenes are usually referred to as latent fingerprints, as shown in Figure 3. Although state-of-the-art algorithms have achieved impressively high matching accuracy using rolled and plain images acquired in an attended mode, as shown in Table 5, matching accuracy with latent fingerprints is still far from satisfactory due to factors like poor ridge structure, complex background noise, and non-linear distortion on the latent images [71]. Significant progress has been made in improving the matching accuracy of latent fingerprints. Cao et al. [72] 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. [73] incorporated feedback information from an exemplar to refine the extracted features from a latent fingerprint image with the eventual goal of increasing the matching accuracy.

Fingerprint samples of FV-STD-1.0

Latent fingerprint samples

Figure 3. Comparison of sample fingerprint images used in FVC-ongoing Competition and those acquired under non-ideal conditions (adapted from [72]).

3.2. 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 [74]. 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 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 [50,75]. Therefore, there is a balance between recognition accuracy and security.

The best three fingerprint matching results with and without template protection in the FVC-ongoing Competition, listed in Table 5, show that matching accuracy with template protection is much worse than that without template protection. Also, recognition accuracy of some existing systems in literature with low/no level of security versus others with high level of security is reported in Table 6 for comparison. From Table 6, we can see that with the same or similar FAR, when the security level is high, the FRR becomes worse. For example, for database FVC2002DB1, results in [45] show that when FAR is 0, FRR is 3.18% with the original feature, whereas FRR increases to 51.29% when the highest security level is set to protect the original feature. Some recently published methods do not give recognition results on low/no level of security. Therefore, their recognition performance in the "Low/No security" column is indicated by "-".

Table 6. Recognition accuracy (FRR/FAR) of some systems in literature with low/no and high security.

Approaches	Low/No Security	High Security	Databases
Li et al. [60]	(17.5/0.35)	(35.8/0)	FVC2002 DB1
Liu et al. [76]	(14.33/0)	(20.40/0)	FVC2002 DB1
Ferrara et al. [45]	(3.18/0)	(51.29/0)	FVC2002 DB1
Yang et al. [77]	-	(3.38/3.38)	FVC2002 DB1
Sandhya and Prasad [49]	-	2.19/2.19	FVC2002 DB1
Wang et al. [39]	-	(1.0/1.0)	FVC2002 DB1
Liu and Zhao [65]	-	(8.6/0)	FVC2002 DB1
Arjona et al. [47]	-	(15.14/0)	FVC2002 DB3
Yang et al. [48]	(4/4)	(4.57/4.57)	FVC2002 DB3
Alam et al. [67]	-	(5.95/5.95)	FVC2002 DB1

In this section, recognition accuracy, as the other important measure in biometric system design, is discussed and analyzed. From our thorough analysis, 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.

4. Conclusions

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. A total of 42 research articles in the area of biometric security (8 in liveness detection, 18 in cancelable biometrics, and 16 in biometric cryptography) are reviewed and discussed. In regards to recognition accuracy, in our opinion, although remarkable recognition accuracy has been attained, matching performance can still be unsatisfactory under some non-ideal conditions (e.g., latent fingerprint matching) or when the system security level is high. Since the requirements of system security impact recognition accuracy, it calls for the biometric system designers to carefully consider how to strike a good balance between recognition accuracy and security.

In view of the above issues, some latest research outcomes are analyzed and summarized in this paper. 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:

i. 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 [78–80] 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.

ii. 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, smartphones are becoming more and more popular, thus

forming a promising platform for the use of biometrics [81]. However, mobile biometrics face more challenges, since smartphones usually have less computing capability and limited energy. Therefore, light-weight secure algorithm design for mobile biometrics is an emerging research topic [82–84].

iii.   Trade-off between security and recognition accuracy in fingerprint template protection remains a challenge. As shown in Table 5, 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. [CrossRef]
3.   Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv.* **2003**, *1*, 33–42. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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.   The FBI Now Has the Largest Biometric Database in the World. Will It Lead to More Surveillance? Available online: http://www.ibtimes.com/fbi-now-has-largest-biometric-database-world-will-it-lead-more-surveillance-2345062 (accessed on 27 November 2018).
10. U.S. Security Officials Will Begin Scanning All 10 Fingerprints of Most Non-Americans Traveling to the United States. Available online: https://travel.state.gov/content/visas/en/news/u-s--security-officials-will-begin-scanning-all-10-fingerprints-.html (accessed on 27 November 2018).
11. Australia Wants to Streamline Its Border Control Using Biometrics. Available online: http://www.smithsonianmag.com/innovation/australia-wants-to-streamline-its-border-control-using-biometrics-180962052/ (accessed on 27 November 2018).
12. How Biometrics on Smartphones is Changing our Lives. Available online: http://www.m2sys.com/blog/biometric-resources/biometrics-on-smartphones/ (accessed on 27 November 2018).
13. Biometrics for Finance Applications. Available online: https://www.tractica.com/research/biometrics-for-finance-applications/ (accessed on 27 November 2018).
14. MasterCard Trials Biometric Bankcard with Embedded Fingerprint Reader. Available online: https://techcrunch.com/2017/04/20/mastercard-trials-biometric-bankcard-with-embedded-fingerprint-reader/ (accessed on 27 November 2018).

15. Maio, D.; Maltoni, D.; Capelli, R.; Franco, A.; Ferrara, M.; Turroni, F. FVC-onGoing: On-Line Evaluation of Fingerprint Recognition Algorithms. 2013. Available online: https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx (accessed on 25 January 2019).

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

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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

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

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**. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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.

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. [CrossRef]
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. [CrossRef]
41. Wang, S.; Hu, J. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recogn.* **2014**, *47*, 1321–1329. [CrossRef]
42. Wang, S.; Hu, J. A blind system identification approach to cancelable fingerprint templates. *Pattern Recogn.* **2016**, *54*, 14–22. [CrossRef]
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. [CrossRef]
45. Ferrara, M.; Maltoni, D.; Cappelli, R. Non-invertible minutia cylinder-code representation. *IEEE Trans. Inf. Foren. Sec.* **2012**, *7*, 1727–1737. [CrossRef]
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. [CrossRef]
49. Sandhya, M.; Prasad, M.V. Securing fingerprint templates using fused structures. *IET Biom.* **2017**, *6*, 173–182. [CrossRef]
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. [CrossRef]
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 the Workshop 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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]

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 I_1 minimization. *Neurocomputing* **2017**, *259*, 3–13. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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 coarse to fine ridgestructure dictionary. *IEEE Trans. Pattern Anal. Mach. Intell.* **2014**, *36*, 1847–1859. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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. [CrossRef]

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.; Choraś, M.; Kozik, R. The overview of trends and challenges in mobile biometrics. *J. Appl. Mathem. Comput. Mech.* **2017**, *16*, 173–185. [CrossRef]

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