IEEE Open Journal of the Computer Society

Received 25 February 2021; accepted 18 March 2021. Date of publication 23 March 2021;
date of current version 12 April 2021. The review of this paper was arranged by Associate Editor P. Li.

Digital Object Identifier 10.1109/OJCS.2021.3068385

Biometrics and Privacy-Preservation: How Do They Evolve?

QUANG NHAT TRAN, BENJAMIN P. TURNBULL, AND JIANKUN HU (Senior Member, IEEE)

UNSW Canberra, The University of New South Wales, Canberra, ACT 2600, Australia

CORRESPONDING AUTHOR: JIANKUN HU (e-mail: J.Hu@adfa.edu.au)

This work was supported by ARC DP190103660, DP200103207, and LP180100663.

ABSTRACT The emerging field of privacy-preserving biometrics is attracting significant attention, as a paradigm that can address several of the key concerns in cryptographic authentication processes, whilst simultaneously addressing the issues of privacy. This paper contributes to the understanding of the field from following perspectives: (1) It proposes a novel and comprehensive taxonomy of privacy-preserving biometrics for the classification of the knowledge/existing literature in the field. (2) It provides a taxonomy-guided literature survey. (3) Open research problems/future works are discussed. (4) As the techniques used in privacy-preserving biometric authentication systems rely upon, or integrate with, general biometric matching techniques, a taxonomy and summary of the state-of-art biometrics matching techniques has also been developed. Such system-level knowledge organization will help produce excellent self-contained contents of reference materials for researchers in both the biometrics community and cryptography community who would otherwise have difficulty in understanding the relevant materials from the other community.

INDEX TERMS Behavioral biometrics, bio-cryptosystem, biometrics, cancellable biometrics, encryption, face, fingerprint, privacy preserving.

I. INTRODUCTION

Biometrics are the traits of human body characteristics and behavior. From a cryptographic perspective, biometrics possess properties that make them suitable as an authentication factor; they cannot be forgotten like a password or pin, and they can't be lost or stolen like a token. Biometrics can help address the inherent security weakness of cryptography in identifying a genuine user. However, biometrics themselves are limited and will be a permanent loss if compromised. Also, the privacy of biometrics are subject to the protection of legal regulations. Therefore, there is a paradigm shift towards privacy-preserving biometrics authentication technology, which has the potential to address these concerns.

Due to their fuzzy nature, biometrics cannot be protected by simply applying conventional encryption. This leaves them exposed to various threats. As a result, there exists an immediate necessity to devise methods that not only preserve the privacy of biometric data but also ensure the performance of the authentication system. According to the standard set by ISO/IEC FCD 24 745:2011 [1], a biometric protection scheme must be: (i) irreversible, that is computationally infeasible to reconstruct the original biometric data from the encrypted template; and (ii) unlinkable, whereby the encrypted templates generated from the same biometric data are not correlated such that a cross-matching attack is successful.

In comparison with the previously conducted surveys published in this field ([2]–[5]), in addition to the comprehensive review of the major published works, this survey provides a taxonomy for the privacy-preserving mechanisms, which is then used to guide the classification and analysis of existing literature. As many biometric matching techniques in the unprotected domain are integrated into the privacy-preserving biometric authentication systems, a taxonomy and summary of the state-of-art biometric matching techniques in the unprotected domain are also provided. Such system-level knowledge organization will help produce excellent self-contained contents of reference materials for researchers from both the biometrics community and the cryptography community who would otherwise have difficulty in understanding the relevant materials from the other side. Additionally, it provides a structured approach to understanding the domain and its areas of current and emerging research and development.

The structure of this paper is as follows: In section II, a high-level taxonomy overview of privacy-preserving biometric authentication systems is presented. In section III, the categorization of main biometrics is presented. Section IV is dedicated to the privacy-preserving mechanisms' taxonomy. A discussion on the open research problems and future works in the field is provided in section V. Section VI concludes this survey.

II. ABSTRACTION-LEVEL TAXONOMY OF PRIVACY-PRESERVING BIOMETRICS AUTHENTICATION SYSTEMS

Privacy-preserving mechanisms for biometrics are designed to ensure the security of biometrics when used in any authentication system. They are normally categorized into cancellable biometrics template and biometric cryptosystem [2]. In this paper, we present a new perspective on the classification of privacy-preserving techniques in addition to the categorization of the biometrics genres. A privacy-preserving biometric security system consists of biometric component and privacy-preserving mechanisms.

Due to the characteristics of the biometrics, they are categorized into two main types: behavioral biometrics and physiological biometrics. Behavioral biometrics are the types of biometrics that are focused on the actions of the owner. We categorize behavioral biometrics into two sub-categories: extrinsic and intrinsic behavioral biometrics. The reactions that correspond to certain events are extrinsic behavioral biometrics (typing, keystrokes, touchscreen usage patterns, driving styles, and so on) meanwhile those that come from the routine activities of a person are intrinsic behavioral biometrics (gait, voice, and many others). Being the actions of a person, behavioral biometrics are countless, resulting in more studies proposed on the new types being used in an authentication system.

Traditionally, privacy-preserving mechanisms for biometrics have always been categorized as cancellable biometrics and biometric cryptosystem where the former applies a non-invertible transformation onto the biometric data and the latter uses cryptographic techniques to encrypt the biometric data. However, as the field continues expanding, more recent studies that have been proposed require a more complicated and specific categorization. Hence, we propose a novel taxonomy in which each class or sub-class is better specified based on its characteristics:

- Non-invertible Transformation: methods that applies a non-invertible transformation on the biometric data. Biometric matching is performed in the transformed domain. For instance: cancellable biometrics, Hashing, or Homomorphic Encryption.
- Direct Biometrics Key Generation: methods that generate a cryptographic key based on a biometric data.
- Information Hiding Techniques: techniques that, given public information, make it hard to find the corresponding original information.

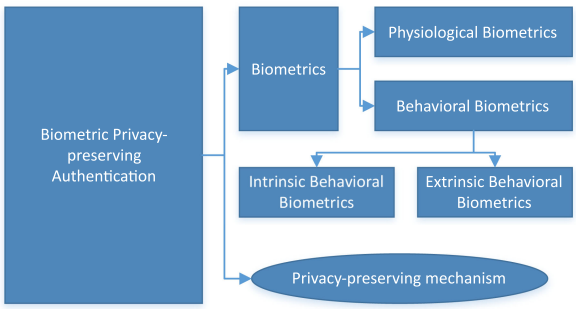

FIGURE 1. Privacy-preserving Biometric-based Authentication System.

- Protocol-based Protection: methods in which protection is achieved by deploying a protocol that usually involves multiple parties.

An abstraction-level taxonomy overview is presented in Figure. 1 where details will be presented in the remaining sections.

III. BIOMETRICS

Biometrics are the traits of human body characteristics and behavior. They are excellent attributes for identity management.

A. BEHAVIORAL BIOMETRICS

Behavioral biometrics focus on recognizing the individual based on the nature of his/her actions. As indicated in Figure 1, behavioral biometrics can be categorized into either extrinsic or intrinsic behavioral biometrics.

1) EXTRINSIC BEHAVIORAL BIOMETRICS

Extrinsic behavioral biometrics are those that occur based on the uniqueness of an individual's behaviour in dealing with specific situations. For example, the identification of touchscreen usage or typing patterns:

Touchscreen has seen a bloom in the industry owing to the wide expansion of smartphone in the digital age. As a result, touchscreen input can be used as an extrinsic behavioral biometric to identify users [6]. In general, touchscreen biometric authentication is user friendly but has a high error rate. Another important extrinsic behavioral is typing patterns. However, as pointed out in [7], the assumption that typing pattern is stable over time does not hold, meaning that it can change over time to to learning. This leads to the fact that the accuracy of a typing-based behavioral biometric authentication is not reliable. In addition, the user's level of familiarity with the language to be typed also affects the identification process. Typing time latency relative order feature and clustering can help improve the system performance [8], [9].

2) INTRINSIC BEHAVIORAL BIOMETRICS

Intrinsic behavioral biometrics come from the natural activities of body. These include, for instance, gait and voice. Intrinsic behavioral biometrics are normally used for distant individual identification and are cooperation agnostic. Wang

and Yan [10] proposed a cross-view gait recognition system with ensemble learning in which multiple gait learners are taken into consideration. Recognition rate when evaluated with CASIA dataset A and B is 95.5% and 96.1%, respectively. Zou *et al.* [11] utilized a CNN and an RNN to learn the gait biometric of each individual from walking data, which is collected using smartphones in the wild with no constraints about speed or path. From the two datasets of 118 individuals collected by smartphones, this algorithm reached 93.5% and 93.7% accuracy rate in identification and authentication, respectively.

B. PHYSIOLOGICAL BIOMETRICS

Physiological biometrics are the traits that belong to a human, and include fingerprints, palmprints and finger veins. They are usually unchangeable and are consistent for an individual throughout their life. However, the collection of physiological biometrics is subject to multiple external factors, such as the pressure on the collection device, surface collection cleanliness, and other environmental factors. In this section, we categorize the major physiological biometric authentication into the partitions of fingerprint, face, and iris.

1) FINGERPRINT

The fingerprint has long been applied as a reliable tool for individual identification. This section will review the proposed key advances on the fingerprint matching techniques where most of them are integrated with the various privacy-preserving mechanisms in forming privacy-preserving biometric authentication systems. In order to evaluate the efficiency of fingerprint matching (and other biometrics as well), the False Acceptance Rate (FAR), the False Rejection Rate (FRR), and the Equal Error Rate (EER) indicators are employed. The FAR is the probability that a matching system mistakenly accepts a biometric subject that does not originate from the same biometric instance. On the other hand, the FRR is the probability that a matching system falsely rejects a biometric instance that comes from the same biometric subject as the stored template. As one might have known, when FAR decreases, FRR is likely to increase. Hence, the EER is a balance indicator to evaluate the performance of a biometric matching system. It refers to the rate when the FRR is equal to the FAR. In terms of databases, Fingerprint matching is usually implemented using the FVC databases: FVC2002 DB1-4, FVC2004 DB1-4, and so on. These databases differ in terms of image quality such that fingerprint matching systems can evaluate their capabilities with different level of noise.

Fingerprint matching in the unprotected domain is mostly based on the following methods:

- Ridge-oriented matching [12] relies on the detection and recognition of the ridges on a fingerprint. One of the widely used techniques in this family is the use of ridge count as feature.
- Image-oriented matching [13] considers fingerprint image as a global feature to match.
- Minutia-oriented matching [14] requires the detection of ridge endings or ridge bifurcations, which are called minutiae on a fingerprint and uses them to match.
- Local structure-oriented matching [15] builds composite features that are locally located on a fingerprint and performs matching among them. This method also requires a further step of generating matching score between two fingerprints.

Both ridge-oriented and image-oriented methods have shown to deliver poor performance as the former relies on the accurate detection of ridges while the latter suffers from the distortion of the whole fingerprint image while matching. Yet, with the success of Artificial Intelligence, particularly deep learning, fingerprint presentation attack detection have been found to be successful [13], [16].

A more advanced fingerprint (and even some other biometrics) matching approach that has shown to deliver more reliable performance is Local Structure-based Matching in which features are extracted within a region of the image to limit the influence of distortion caused by external factors. Among all the works that have been proposed, Minutia Cylinder Code (MCC), introduced by Cappelli *et al.* [15] is the current state-of-the-art algorithm. It is a hybrid between local structure-based matching and minutia-based matching methodology, as each of the local structures constructed is based on a minutia. By constructing a 3D data structure to distribute the directional physical distance among the minutiae, this method provides a high performance with low EER and FAR (0.15% and 0.18%, respectively). It is still now considered the state-of-the-art fingerprint matching method.

2) FACE

In parallel with fingerprints, facial recognition has been in development for a significant period of time. Unlike fingerprints, facial recognition does not require complex hardware, and a modern inexpensive camera can produce a face image of suitable quality, even from a distance. Based on the type of input, Facial recognition systems can be categorized into the following methods:

- Image-based matching: image of the face is taken as input. Either features are predefined and extracted from the face region (feature-based facial recognition [17]) or the whole image is used as features (hollistic-based facial recognition). Due to curse of dimensionality, dimension reduction techniques such as PCA, LDA, or ICA are applied in the process of matching. In addition, Artificial Intelligence (AI) [18] has been applied to utilize the power of machine learning for facial recognition.
- Video sequence-based matching: A video sequence is taken as input to perform real-time recognition [19].
- Sensory data-based matching: data collected from sensor is used for matching. Thermal infrared sensors are used to detect the facial features [20]). In addition, 3D modeling is also used for both image [21] and video facial recognition [22] by constructing a three-dimensional model of the face.

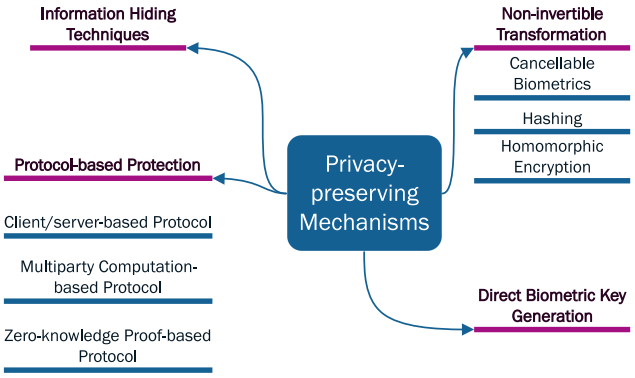

FIGURE 2. Privacy-preserving Mechanisms.

3) IRIS

The iris, considered the biometric with the highest reliability, has been widely used to identify human beings. In order to use the iris as a method of recognition, a sensor is required to scan the iris, from which feature vectors are generated and matched according to a process. Iris recognition methods can be categorized based on the following stages; image acquisition, region segmentation, feature extraction, and matching. Iris recognition systems are categorized into two different types based on their methodology: Phase-based Recognition, Zero-crossing Representation-based Recognition, and Texture analysis-based recognition.

- Phase-based Iris Recognition [23]–[25]: the iris's texture phase information is extracted and used for matching.
- Zero-crossing Representation-based Iris Recognition [26]: the iris's features from images are extracted using the wavelet transform zero crossings.
- Texture analysis-based Iris Recognition [27]–[32]: the iris's detailed texture structure is captured and used as the medium for matching.

IV. PRIVACY-PRESERVING MECHANISMS

This section introduces a new perspective on the categorization of the privacy-preserving mechanisms for biometrics system. An overview of the classes is presented in Figure 2.

In this paper, we categorize privacy-preserving mechanisms into the following categories:

- Non-invertible Transformation.
- Direct Biometrics Key Generation.
- Information Hiding Techniques.
- Protocol-based Protection.

Each of these is discussed separately.

A. NON-INVERTIBLE TRANSFORMATION

Non-invertible Transformation family comprises of one-way transformations applied on the biometrics data such that an adversary cannot retrieve the original biometric data. Comparison of two biometrics is performed in the transformed domain to ensure no information about the original data is leaked.

1) HASHING

Cryptographic hashing generates a hash value from an input data. However, applying it on biometric induces variation, as cryptographic hashing requires the input data to be exactly the same every time. Any slight change to input completely changes the hash produced. In 2004, Jin *et al.* [33] proposed a two-factor authentication method named BioHashing. This work proposed to use an iterative inner product operation to combine the tokenized data with fingerprint data. The resultant data is a separate feature set, which is then binarized using a predefined threshold. This work achieved 0% as its best EER when working with FVC2002 DB1-4 at the time. In 2017, Jin *et al.* [34] proposed an Index of Max (IoM) Hashing as the non-invertible transformation for cancellable fingerprint template with MCC. MCC was used as the fingerprint vector, which is fed into the process of generating template by finding the IoM codes with different approaches (Gaussian Random Projection based IoM and Uniformly Random Permutation based IoM). FVC2002 DB1-3 and FVC2004 DB1-3 were chosen to test this method. Approaching from BioHashing concept, Meetei and Begum [35] combined the iris features with a tokenized pseudo random number. One of the most famous works that have been proposed in protecting the palmprint template is by Connie *et al.* [36] in which a set of pseudo-random keys is used to generate palmhash code, functioning as the protection layer for palmprint template.

2) CANCELLABLE BIOMETRIC TEMPLATES

Ratha *et al.* [37] first proposed the idea of cancellable Biometrics in 2001 as a method to protect biometric data. To be considered as a cancellable template, the following four characteristics are required [37]:

- Non-invertibility: cancellable biometric template cannot be, or is computationally hard to be, reverted to retrieve the original biometric data given the corresponding parameter is exposed to the adversary. Irreversibility is a more accurate term that is used in the ISO/IEC 24 745 standard.
- Revocability: If a cancellable biometric template is compromised, the original biometric data is still safe and able to be used with new sets of parameters to generate new transformed templates. The template generated with the old parameters is no longer valid and is revoked.
- Diversity: Different cancellable biometric templates generated by different set of parameters should have no correlation such that a cross-template attack is not possible.
- Accuracy: Transformation of the biometric data should not degrade the matching process.

Lee *et al.* [38] used each minutia in a fingerprint as a reference point whose invariant features are derived from its neighboring area. The transformation applied on each of the minutiae is determined by two changing functions of distance of orientation, leading to a new position of the minutiae. The proposed method yields EER of 3.4%. A separate work that also employed a minutia-matching methodology,

Ahn *et al.* [39] extracted the features from a triplet of minutiae and applied a shifting transformation on the geometrical properties of the tripplet. Being evaluated with good quality dataset FVC2002 DB2, the proposed work reached EER of 3.61%.

Approaching from the direction of applying two-factor key generated by splitting the projection matrix to produce biometric template, Yang *et al.* [40] projects the biometric features as the transformation in the sense that a dynamic random projection is applied on feature vectors of the local minutia. The projection's content is determined by the feature vectors. In 2011, Ahmad *et al.* [41] designed a cancelabe fingerprint template whose features are constructed based on the relative interaction between two minutiae in a pair polar coordinate system. Yang *et al.* [42] utilized both local and global structures to extract features to which a perpendicular projection is applied as the non-invertible transformation. Yang *et al.* [43] used the Delaunay triangulation method to construct triangles from three minutiae from which local features are extracted. The set of the triangles functions as the set of local structures and is applied with the Polar Transformation defined in [37] on each of its element as the non-invertible transformation. Two fingerprint images are deemed match or non-match based on the number of corresponding triangles. Due to this inflexible tolerance, this method's performance when evaluated with good quality dataset FVC2002 DB1 and FVC2002 DB2 is poor with 5.93% and 4.0%, respectively.

Binary representation has been widely used in designing cancellable fingerprint templates due to its simplicity and lightweight in implementation. Recently, Yang *et al.* [44] proposed a cancellable fingerprint template method using random projection. The remarkable novelty in this work is the decorrelation algorithm, which provides protection against the ARM (Attack via Records Multiplicity).

Over the recent years, Wang *et al.* [45]–[47] have proposed various works on designing non-invertible transformation functions from the perspective of digital signal processing. In 2012 [45], they proposed an infinite to one mapping approach in which the binary strings representation of features are first mapped to the frequency domain by applying the Discrete Fourier Transform (DFT). Afterward, the resultant vectors are multiplied with a parameter matrix whose number of rows equals the number of binary values from the string and number of columns is less that the number of rows. This method achieved EER of 3.5%, 5%, 7.5% for FVC2002 DB1-3, respectively. In 2014, they proposed another alignment-free cancellable template method that uses curtailed circular convolution as the non-invertible transformation [46]. After extracting features and bin-indexing them to produce binary representation, the authors converted them to frequency domain with DFT and remove part of the resultants to get the cancellable templates. This method managed to bring down the EER of the good quality FVC2002 DB1 and FVC2002 DB2 to 2% and 3% but when dealing with lower quality images from FVC2002 DB3, it still reached 6.12%. In 2016 [47], Song and Hu proposed to protect the template of the fingerprint using a non-invertible transformation based on blind system identification concept. Using the same method to extract features, generate binary string, and convert to frequency domain using DFT as the previously mentioned method, the authors then used a finite impulse response (FIR) vector of the moving average model to generate cancellable template. They also showed that under certain circumstances, as long as the length of the FIR vector is within a specified range, the transformation is non-invertible. Both One versus One and FVC protols have been evaluated with FVC2002 DB1-3 and shown competitive performance against the state-of-art methods at the time. Song *et al.* designed partial Hadamard transformations and partial DFT in [48] and [49], respectively. Both works employ a vector as a parameter key to select certain rows of the output matrix accordingly as the cancellable templates of the binary string representation of features. The difference lies in the fact that the former method was used with Hadamard transformation meanwhile the latter method utilized the Discrete Fourier Transformation. Recently, Yang *et al.* [50] proposed a feature-adaptive random projection cancellable biometric template. The projection matrices are determined by a basic matrix that is associated with local features. The four fingerprint databases FVC2002 DB1-3 and FVC2004 DB2 are used to evaluate this approach. Although the authors claimed that the projection matrices are destroyed after use, this method is still not resistant to the ARM.

Taking advantage of MCC's performance, various non-invertible transformations have been proposed to protect the templates. The authors of MCC proposed P-MCC [51] as a template protection scheme in which a KL projection [52] is applied on the MCC vector. However, this projection is not revocable. Hence, in 2014, the authors proposed 2P-MCC [53] with the ability to reissue a compromised template by incorporating a partial permutation-based scheme. In the meantime, Zhang *et al.* [54] proposed two non-invertible transformation to generate cancellable fingerprint templates from MCC: Combo Plate Transformation and Functional Transformation. In 2018, Arjona *et al.* [55] designed Physically Unclonable Functions (PUFs) to apply on P-MCC and named it P-MCC-PUFs.

Similarly to fingerprints, the iris has also been applied with cancellable biometric template to be protected. Recently, Yang *et al.* [56] proposed a cancellable iris system by employing steganography to hide the user's key, decreasing the chance of losing the key to adversary and improving the security of the system. Having been evaluated on CASIA-IrisV3-Interval, MMU-V1, and UBIRIS-V1-Session 1 databases, this method achieved EER of 1.66%, 4.75%, and 3%, respectively. Importantly, by incorporating steganography to hide the user's key in an image, which is not detectable with human eyes, the authors made this method less exposed to the ARM. However, a machine learning technique or a simple method that scans the stego-images's pixels may give knowledge about a secret being hidden. Hence, further analysis may be employed to retrieve the secret.

In addition to fingerprints, iris, and face, the cancellable template design has also been applied to protect other biometrics. These are less common, but there has still been significant enhancements in this area. Palmprints are one of the hidden biometrics that needs to be protected as a person only has 2 palmprints. Due to the large area of the palmprint, more complicated and costly sensor is required, leading to less interest in comparison to other biometrics. However, there are still several cancellable template designs for it. Qiu *et al.* [57] proposed to generate a cancellable palmprint template by utilizing Anisotropic Filter to extract the orientation information and applying chaotic matrix to measure it. Evaluation of the method's performance is conducted on Hong Kong PolyU database and Tongji Contactless Palmprint Dataset, achieving EER of 0%. One of the recently published works on palm vein is by Ahmad *et al.* [58] in which the authors used a wave atom transform (WAT) from which the features are extracted. In order to protect the feature, with a user-specific key, a randomization and quantization are applied to generate the palm vein templates. Under four databases: PolyU, PUT, VERA, and their own database, this method achieved 1.98%, 0%, 3.05%, and 1.49%, respectively.

3) HOMOMORPHIC ENCRYPTION-BASED BIOMETRIC MATCHING

Homomorphic Biometric Encryption though conceptually is similar to cancellable biometric as the former performs matching in encrypted domain while the latter performs in transformed domain, it is a type of bio-cryptosystem as it modifies and applies traditional encryption techniques on biometric data instead of using a non-invertible transformation. Barrero *et al.* [59] utilized homomorphic probabilistic encryption to construct a general framework for multi-biometric template protection with fusions in three levels and achieved EER of 0.12% while the templates storage requires only 200 KB. Recently, Morampudi *et al.* [60] protected the iris used in an authentication system with fully homomorphic encryption. Evaluated with CASIA-V1 database, this method reached an EER of 0.19%.

B. DIRECT BIOMETRIC KEY GENERATION

Direct Biometric Key Generation takes a biometric data as input to generate helper data, from which digital keys are generated. Importantly, biometric key generation schemes do not require either of the biometric template or the private key to be stored in the system, mitigating the risk of them being exposed to adversary when there is an attack targeting the database.

One of the first biometric key generation schemes was proposed by Davida *et al.* [61] in which they used user-specific error correction to address the uncertainty in testing data. The authors demonstrated this method with iris biometric. Although applicability in iris was shown, whether or not this method is suitable for other biometrics is still doubtful as iris exhibits far less variation in comparison with face or fingerprint features.

Since then, there have been various key-generation designs proposed with different types of biometrics [62]–[66]. In general, direction biometric key generation methods tend to be unreliable due to the biometric data noise. In the next sections, we will introduce works that can effectively retrieve reliable keys from noisy data. We will focus on the concept of Fuzzy Extractor and its applications for being one of the breakthroughs that set a firm foundation for other methods.

Fuzzy Extractor: Fuzzy Extractor [67] is one of the famous biometric key generation schemes. This method differs from FVS (Fuzzy Vault Scheme which will be introduced in the next session) in the sense that instead of using chaff points, high-degree polynomial is used. In their original paper, the authors proposed two primitives: secure sketches and a fuzzy extractor: A secure sketch is a probabilistic function that generates helper data about the noisy input w (w can be considered as, but is not limited to being a biometric input) without significantly revealing it, i.e reducing its entropy. An exact recovery of w can be retrieved given the existence of some w' as input that is computationally close enough to w. Assuming M is the metric space to be used with the scheme and dis calculates the distance between two objects in M, a secure sketch is comprised of two phases: Sketch (SS) and Recover (Rec) such that: (i) SS takes the input w and returns a binary string s; (ii) Rec takes s and w' as input. If $dis(w, w') \leq t$, then w is recovered, i.e: $Rec(w,' s) = w$ where t is the distance threshold or error tolerance. On the other hand, a fuzzy extractor is constructed from a secure sketch and a strong extractor (the reader can refer to the original text in [67] for further information). It can reproduce a nearly uniform random string R from the input w' when $dis(w, w') \leq t$. Additionally, a syndrome key generation scheme that is based on polynomial interpolation that requires low storage space is proposed and called PinSketch.

In the original text, fuzzy extractor is enabled to work with different metric spaces, such as Hamming distance, Set difference, and Edit distance. Hence, it has a wide range of applications to protect biometric template data. There is significant work in this space, especially focusing on fingerprints. Xi *et al.* [68] proposed an alignment-free fingerprint authentication system with fuzzy extractor. In details, rotation and shift free local structures derived from minutia are used to eliminate the alignment process. A near equivalent Dual Layer Structure Check (NeDLSC) is devised to make it applicable to biocrypgraphic constructions. Finally based on NeDLSC, fuzzy extractor is applied. The algorithm is evaluated on FVC2002 DB2, yielding EER of 4.5%. In 2012, Yang *et al.* [69] applied fuzzy extractor to protect the features in a fingerprint authentication system. In their design, Delaunay triangle-based local structures are extracted as registration-free features. The use of fuzzy extractor not only delivers the improvement in matching performance but also makes pre-alignment process unecessary. Upon having been evaluated on FVC2002 DB2, the algorithm achieved 13% of EER.

Various works from unimodal to multimodal biometrics have also employed fuzzy extractor. Chang *et al.* [70] incorporated cancellable multi-biometric with fuzzy extractor and a novel bit-wise encryption.

C. INFORMATION HIDING TECHNIQUE

Information Hiding Technique hides biometric data by fusing it with another piece of data (known as a digital key) to produce public helper data. In authentication phase, the digital key is recovered by applying a retrieval algorithm given the presence of a closely matched biometric query to the template that is used to generate the helper data.

Fuzzy Commitment Scheme: In 1999, Juels and Wattenberg [71] proposed Fuzzy Commitment Scheme (FCS). Given a set C containing error correcting codewords c with length n, witness x being the biometric data with length n, in the enrolment phase, a function F is used to commit codeword c and the biometric data x to create the helper data $F(c, x)$ by estimating and storing the difference vector δ between x and c where $\delta = x - c$. The hash value of the codeword c, denoted as $h(c)$ is stored along with δ. In the authentication phase, given that a biometric data x' is computationally close to x with respect to a pre-defined metric, c can be retrieved by using δ to perform a translation of x' toward x. Decision is made based when comparing the hash value of the result with $h(c)$.

Rathgeb *et al.* [72] used the FCS to protect the fusion at the feature level in which two binary biometric templates are combined. This method was evaluated with the CASIA-v3-Interval iris database [73].

On the other hand, there have been various methods that apply FCS in protecting fingerprint templates: Sandhya and Prasad have proposed quite some works in applying FCS to design a fingerprint-based authentication system: In 2016, the authors used FCS to protect the binary strings generated from the Delaunay neighbor structures [74] and achieved 1.43%, 1.79%, and 5.89% for datasets FVC2002 DB1-3, respectively. In the same year, they proposed a privacy-preserving system for fingerprint with Delaunay triangulation net features based on FCS. In 2017, they [75] combined the concept of cancellable biometrics with FCS to devise their cancellable fingerprint privacy-preserving authentication system using spiral curves, reaching EER of 1.17%, 2.46%, 8.51% when evaluated with datasets FVC2002 DB1-3, respectively. In 2013, Imamverdiyev *et al.* [76] built an FCS-based privacy-preserving biometric authentication system using different combinations of texture descriptors (such as Gabor filter-based FingerCode, local binary pattern, and local direction pattern). In details, the fingerprint texture descriptors, which is the result of the combination, is binarized by a biometric discretization method and protected with FCS. Upon being evaluated with FVC2002 DB2a fingerprint dataset, the results show improvement in the performance of texture-based fingerprints bio-cryptosystem with FCS.

Due to the variations presented in facial recognition, leading to a variant binary string representation, it has rarely been used in an FCS-based bio-cryptosystem. Feng *et al.* [77] combined the transform-based and bio-cryptosystem approach in a three-step hybrid algorithm based on random projection, discriminability-preserving transform, and FCS. Three face databases are used for the evaluation of this method, namely: FERET, CMU-PIE, and FRGC, giving estimated security of 206.3 bits, 203.5 bits, and 347.3 bits, respectively. In 2018, Nazari *et al.* [78] is one of the few who used FCS to protect face features. They integrated face recognition with binarization transformation, chaos feature permutation and FCS. The proposed work was evaluated in three face databases: CMU PIE, FEI, and Extended Yale B. Gilkalaye *et al.* [79] constructed FCS-based bio-cryptosystem with facial recognition by proposing a real-value compatible FCS. Labeled Faces in the Wild (LFW) dataset was used for evaluation.

Recently, Yang *et al.* [80] used FCS to protect the biometric-based healthcare data and stored it along with the cancellable finger vein template on a smart card.

In addition to physiological biometrics, FCS has also been used with behavioral biometric. Specifically, gait-based authentication systems are receiving increasing research interest. Recently, Elrefaei and Al-Mohammadi [81] extracted gait features from gait images with local ternary pattern and calculated the average of a gait cyle using gait energy image before having joined them together and produced feature vector. FCS is used to protected the data. This system achieved good results with 0% of FAR as well as FRR. However, the key length retrieved is only 45-50 bits.

The most obvious disadvantage of FCS is that it requires an ordered representation of the biometric features. As a result, it has limited application due to the difficulties in designing a biometric feature extraction scheme that produces ordered binary string from a noisy input. This problem is addressed by the next introduced work.

Fuzzy Vault Scheme: In 2006, Juels and Sudan proposed one of the most well-known privacy-preserving biometric system concepts called Fuzzy Vault Scheme (FVS) [82] using error correcting code with polynomial encoding. In the enrolment phase, given the biometric feature set A and a polynomial p to encode the key k, $p(A)$ is calculated in addition to the adding of chaff points to hide the genuine points of p. This set of points T is the template. In authentication phase, assuming that A' is the input query biometric feature set, $p(A')$ is calculated. If a large portion of A overlaps with A', sufficient points lying on p are located. Hence, applying error code correction, k is successfully recovered. With this work, the authors enabled privacy-preserving biomeric authentication system to work with un-ordered set, which is one of biometrics' characteristics. In addition, it was proved that without having the same biometric, reconstruction of the polynomial is not possible with the presence of the chaff points.

Fingerprint is one of the hidden biometrics that urgently need protection. That explains why there are countless studies on securing fingerprints, especially using FVS. Li *et al.* [83] proposed a topological structure-based fingerprint privacy-preserving biometric authentication system with FVS. This

method requires the process of registration in order to identify the core though it does not reveal any information about the minutiae. The performance reported from evaluation with FVC2002 DB2 is 94% of GAR with FAR being 0.03%. In 2009, Xi and Hu [84] proposed a FVS-based Fingerprint based on composite features that requires no pre-alignment and evaluated this method with FVC2002 DB2 dataset, reporting GAR of 98.5% while FAR is 0.01%.

Iris is another hidden biometrics that require complex techniques in order to meaningfully and correctly capture. Lee *et al.* [85] presented a FVS privacy-preserving biometric authentication system with local iris features in which multiple local regions' iris features are extracted from the iris image. Clustering method is applied to generate exact values of the unordered set. The problem of alignment is addressed by using a shift-matching technique. Through experimental results, 128-bit private keys were generated using iris data with no prior registration.

Apart from fingerprints and irises, the face has also been incorporated with FVS. Wu and Yuan [86] proposed to apply FVS on a face online authentication system in which instead of using the original face template, a transformed face template is used with a key with FVS to provide revocability for the face template. However, because the face template is transformed and applied with FVS, it is expected that this method suffers from great degradation. Joshi and Sanghavi [87] integrated a Face FVS in Cloud Computing. Facial features are extracted from user's face image then converted to binary string to be bound with a secret key in FVS.

Beside unimodal privacy-preserving biometric authentication system and single-technique privacy-preserving, FVS has also been used as the protection layer for multimodal privacy-preserving biometric system or as one of the components in a multi-technique privacy-preserving scheme. Leng and Teoh [88] combined 2DPalmHashCode, cancellable biometric, and Fuzzy Vault to protect palmprint templates. Recently, Bobkowska *et al.* [89] combined iris, fingerprint, and face biometrics to construct a multibiometric privacy-preserving biometric authentication system with the purpose of preventing fraud in e-passports with FVS. Another security technique that is also incorporated in this method is the use of steganography in mapping biometric images to one another. The location map functions as the secret key, protected by FVS.

There have also been studies that incorporate multiple methodologies to construct a privacy-preserving biometric authentication system. For instance, Yang *et al.* [90] use biohashing algorithm to generate two transformed templates and apply FCS and Fuzzy Vault to generate two sketches, respectively. The sketches are then fused with two operations: 'AND' operation and 'OR' operation to switch the focus on performance or security.

D. PROTOCOL-BASED PROTECTION

Bio-cryptosystem constructs biometric authentication system using encryption techniques at the protocol level, which plays an important role in ensuring the security of the biometric data. With the rapid development of smart devices, biocryptosystem has become more and more crucial in protecting the user's privacy.

1) CLIENT/SERVER-BASED BIOMETRICS AUTHENTICATION PROTOCOL

Assuming that the server is secure, Xi *et al.* [91] proposed a client/server protocol authentication system based on fingerprint in which the original features from fingerprint are protected by Elliptic Curve Cryptography (ECC) in the transferring from the client to the server. On the server side, biometric keys are generated and protected using FVS. The security of this protocol has been shown by analyses of several types of attack in addition to the details about memory and time usage. Experiments have been evaluated on the NIST Special Database 24 and FVC2002 DB2, yielding competitive results. Odelu *et al.* [92] showed that the multiserver scheme in [93] is exposed to a threat with certain flaws then proposed an improve multi-server authentication protocol with biometric smart card and ECC. Various attack scenarios have been analyzed in addition to the simulation for formal security verification. Recently, dealing with the privacy of autonomous vehicle users, Jiang *et al.* [94] devised a cloud-centric three-factor authentication protocol for authentication and key agreement called CT-AKA in which biometrics, passwords, and smart cards are combined to control access. The authors synthesized three eminent biometric protection techniques FVS, FCS, and Fuzzy Extractor to ensure a leakage-free protocol in addition to two sessions keys being used in the protocol. Formal proof of this method is also provided to show its security strength.

2) SECURE MULTIPARTY COMPUTATION-BASED BIOMETRIC SECURITY PROTOCOL

Secure multiparty computation (SMC) is a powerful cryptography protocol which can protect the input privacy of each participant [95]. It has found some applications in privacy-preserving biometrics security systems [95]–[98]. Bringer *et al.* [95] provided an overview of early SMC's application on privacy-preserving biometrics security. It focused on secure face identification from a database, and secured distance computation of fingerprint and iris representations. Chun *et al.* [96] considered the privacy-preserving biometric authentication problem where the biometric authentication process is outsourced to the cloud and the biometric data are fully encrypted. An outsourceable privacy-preserving biometric authentication (O-PPBA) protocol was proposed. The proposed O-PPBA can take advantages from both homomorphic encryption and the garbled circuit. One drawback is the requirement for another independent cloud service provider. Tian *et al.* [97] stated that existing biometric-based remote user authentication (BRUA) methods in the client-serve setting lack certain privacy considerations., e.g., authorized user's multiple sessions should not be linked while the user's identity remains anonymous to the cloud server. In addressing this

issue, a privacy-preserving biometric-based remote user authentication (PriBioAuth) proposed was proposed. Based on the SMC technique, secure biometrics matching protocol was proposed. One of the advantages is that no user interaction is required for the biometrics matching. Similar to [96], it requires two independent servers. A major issue with these works is that no matching/authentication performance evaluation has been conducted. In the biometrics community and in practice, matching performance is most important. The challenge is the conflicting goal of achieving high biometric authentication accuracy while maintaining high privacy protection.

3) ZERO-KNOWLEDGE PROOF-BASED BIOMETRIC SECURITY PROTOCOL

Zero-knowledge proof is a cryptography protocol where party A can prove to party B that part A has certain knowledge and yet without revealing any other additional information [98]. This nice property is well suited for privacy-preserving biometrics authentication and some interests have been made [99], [100]. In real-life security systems, authentication process involves often many attributes/identifiers, e.g., password, login name, and biometrics etc. of a personal identity. In [99], it proposed a privacy-preserving scheme in addressing the problem of verification of multiple identifiers and proofs of identity. The proposed idea is to generate aggregate signatures on commitments which are then used for privacy-preserving identity proof via the zero-knowledge proof protocol. The security of the proposed scheme has been formally proved under the co-gap Diffie-Hellman assumption for groups with bilinear maps. The authors in [100] proposed a mobile phone-oriented privacy-preserving biometrics authentication scheme. The proposed scheme used machine learning-based classifier to extract a revocable biometric identifier and then produced a cryptographic identify token encoding the biometric identifier. Finally, the cryptographic identity token is embedded into the zero-knowledge proof protocol for the privacy-preserving authentication. The proposed scheme was integrated with a key agreement mechanism to address the man-in-the-middle Mafia attack on the conventional zero-knowledge proof based identify verification protocol. Biometrics matching performance has been provided.

V. OPEN RESEARCH PROBLEMS AND FUTURE AREAS OF WORK

Though some progress has been made in the field of privacy-preserving biometric authentication systems, they still face the fundamental challenge of achieving both high authentication performance and high security strength, while these are two conflicting goals. Privacy-preserving biometric authentication is a rich research topic across several major disciplines such as biometrics, machine learning and cryptography. There are still many interesting open research problems for future work in this area. The following represents both the current open research questions, and also indicates the current research directions in the intersection of biometrics and privacy-preservation.

Behavioral Biometrics. Although behavioral biometrics are just beginning to become popular as another emerging form of biometrics, it has started attracting significant research interest. Behavioural biometric authentication systems possess several promising features which is emerging as an interesting research area within the field: (i) Unlike physiological biometrics, behavioural biometrics do not seem to suffer from spoofing attacks; (ii) Certain types of behavioural biometrics (specifically extrinsic behavioural biometrics) are built upon the combination of the traditional knowledge-based authentication the actions of a person; and (iii) There are countless number of behavioural biometrics, leading to limitless ways for reliable authentication. On the contrary, there are many challenges for behavioral biometrics to overcome, as future works, to take the leading position of physiological biometrics:

- Currently, the number of publicly available behavioral biometrics databases is very limited. Behavioral biometrics authentication systems that have been proposed are mostly evaluated on self-generated databases. As a result, this field lacks a standard benchmark to evaluate each proposed system in an unbiased way. The reason for this might be the countless number of behavioral biometrics discovered, the privacy of such datasets and the sheer size such a dataset would need to be in order to be effective.
- Some behavioral biometrics are potentially imitable (e.g.: car-driving, GUI interaction, even gait in some cases) given enough time and effort, endangering privacy of the user. Strategy needs to be employed to address this issue. One of the widely used strategies is to construct multimodal biometrics authentication systems.
- Compared to physiological biometrics, behavioral biometrics are more impractical to be deployed in casual real-world applications.

Generic Privacy-preserving Mechanisms: Existing privacy-preserving mechanisms still face one or more of the following attacks, which needs to be addressed in future research.

- Spoofing attacks: Although privacy-preserving biometric authentication systems can provide authentication in the protected domain, they cannot deal with biometrics spoofing attacks [101]. Liveness detection is normally a separate component for spoofing attack detection. However, as some spoofing detection methods will need to utilize the biometrics template information, it will be an interesting research problem on how to incorporate the spoofing attack detection into an integral privacy-preserving biometric authentication system.
- Attack via Record Multiplicity (ARM) [102]: This is a serious attack, in particular for non-invertible transformation based privacy-preserving system, as it can invert the many-to-one mapping via compromising multiple

transformed templates. Li and Hu have shown that some cancellable fingerprint templates are exposed to this kind of threat [103] while other works prove that ARM is applicable to other privacy-preserving techniques ([102], [104], [105]).

- Hill-climbing attack: In this attack, the attacker attractively modifies the input while observing the internal comparison score [106].
- Randomness requirement on the FCS: For FCS, in terms of security, knowledge of the difference vector δ does not reveal either the codeword c or the biometric data x without the presence of biometric data x' that is close to x. However, this is only achievable if the binary biometric data is uniformly random. In reality, due to biometrics' nature, it rarely happens. This is a security issue of FCS. Ignatenko and Willems have proved that FCS does not qualify as a privacy-preserving technique under various scenario. In 2007, Teoh and Kim [107] proposed Randomized Dynamic Quantization to transform the biometric data to achieve a nearly uniformly random biometric data. In addition, FCS keys bound is more exposed to the brute force attack due to low entropy. Hao *et al.* showed 44 bits in [108]. Another vulnerability that FCS is exposed to is the decodability attack that allows the attacker to successfully retrieve the codeword [109]. Kelkboom *et al.* proposed the use of a random bit-permutation process to prevent this attack [110]. Beside the brute force attack presented in [111], assuming that an adversary possesses multiple FVS's that share a mutual key, FVS is also exposed to the threat proposed by Hoon and Miri [112] in which chaff points are systematically identified and removed.
- Other techniques such as FVS and Fuzzy Extractor have also been the target of several attacks. The security of FVS relies on the chaff points created. Based on that, Chang *et al.* [113] proposed a method to find the original minutiae points from the whole set including chaff points. In addition, Fuzzy Extractor becomes insecure when the same input is extracted multiple times and an impostor is able to acquire these samples [114]. Li *et al.* [115] proposed a resuable fuzzy extractor based on the Learning Parity with Noise Assumption.

With the current speed of the AI deployment, more and more biometrics matching schemes are based on form of AI, such as deep learning. There is no doubt that more AI related attacks would be launched against such privacy-preserving biometric authentication systems. More importantly, as smartphones with biometrics authentication have become ubiquitous in real life, privacy-preserving authentication will become a must-have component.

Conventionally, biometrics authentication is a standalone biometrics matching component. However, with the pervasive IoT applications and cloud outsourcing applications, we will see biometrics authentication component being more deeply immersed into the whole cryptography protocol system from key generation, key management and encryption/decryption. This field will increasingly be an area in which future research is necessary and likely to achieve significant gains.

VI. CONCLUSION

Along with the integration of biometric authentication in modern smartphones, privacy-preserving has asserted its crucial role in protecting user biometrics. In order to provide a broader view on the classification of the developing privacy-preserving biometric authentication, in this comprehensive survey, beside reviewing important works, we present a novel taxonomy to categorize unprotected biometric matching and privacy-preserving techniques.

This taxonomy differs from the previously published counterparts in three ways; it includes emerging protocol-level privacy-preserving techniques, it provides higher granularity and perspectives, and is specifically written to assist researchers in biometrics and cryptography better integrate their work and provide a neutral perspective. Specifically, earlier taxonomies only identify Cancellable Biometrics and Bio-cryptosystem as the two main techniques in this space, whereas this paper provides a new perspective of categorization that is appropriate to be applied even with the future development of the field by enlisting them as sub-categories of a higher level category.

In addition to the introduction of a novel taxonomy, open research problems in the intersection of biometric security, authentication and cryptography are also discussed. The vulnerabilities of each outlined process or methodology are mentioned along with proposed resolutions or progress, where applicable. This work then provides a prediction on trends in the field, based on other emerging areas of research and their potential impacts, or where they may be drawing upon works in this space. This work pays particular attention to emerging work in the IoT space, cloud and mobile devices.

There is no doubt that new and emerging biometric recognition systems will become increasingly important in the future; the proliferation of new devices and computing paradigms practically demands it. The need for privacy-preservation in this space is also expanding, and new processes will need to be continued to be developed and refined to allow this. Since behavioral biometric recognition is still at a very early development stage, new categories of this biometric type may emerge. Whether they are privacy-preserving is an interesting question for future research.

REFERENCES

[1] I. O. for Standardization, Iso/iec 24745:2011 information technology - security techniques - biometric information protection. 2011. [Online]. Available: https://www.iso.org/standard/52946.html

[2] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, 2011.

[3] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[4] B. Choudhury, P. Then, B. Issac, V. Raman, and M. K. Haldar, "A survey on biometrics and cancelable biometrics systems," *Int. J. Image Graph.*, vol. 18, no. 01, 2018, Art. no. 1850006.

[5] M. N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, pp. 3403–3446, 2019.

[6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[7] B. Ngugi, B. K. Kahn, and M. Tremaine, "Typing biometrics: Impact of human learning on performance quality," *J. Data Inf. Qual.*, vol. 2, no. 2, pp. 1–21, 2011.

[8] J. Hu, D. Gingrich, and A. Sentosa, "A k-nearest neighbor approach for user authentication through biometric keystroke dynamics," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 1556–1560.

[9] K. Xi, Y. Tang, and J. Hu, "Correlation keystroke verification scheme for user access control in cloud computing environment," *Comput. J.*, vol. 54, no. 10, pp. 1632–1644, 2011.

[10] X. Wang and W. Q. Yan, "Cross-view gait recognition through ensemble learning," *Neural Comput. Appl.*, vol. 32, no. 11, pp. 7275–7287, 2020.

[11] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li, "Deep learning-based gait recognition using smartphones in the wild," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3197–3212, 2020.

[12] J. Feng, Z. Ouyang, and A. Cai, "Fingerprint matching using ridges," *Pattern Recognit.*, vol. 39, no. 11, pp. 2131–2140, 2006.

[13] I. Goel, N. B. Puhan, and B. Mandal, "Deep convolutional neural network for double-identity fingerprint detection," *IEEE Sens. Lett.*, vol. 4, no. 5, pp. 1–4, May 2020.

[14] X. Yin, Y. Zhu, and J. Hu, "Contactless fingerprint recognition based on global minutia topology and loose genetic algorithm," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 28–41, 2019.

[15] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[16] T. Chugh and A. K. Jain, "Fingerprint spoof detector generalization," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 42–55, 2020.

[17] B. Efraty, E. Bilgazyev, S. Shah, and I. A. Kakadiaris, "Profile-based 3d-aided face recognition," *Pattern Recognit.*, vol. 45, no. 1, pp. 43–53, 2012.

[18] M. Agarwal, H. Agrawal, N. Jain, and M. Kumar, "Face recognition using principle component analysis, eigenface and neural network," in *Proc. Int. Conf. Signal Acquisition Process.*, 2010, pp. 310–314.

[19] Y. Li, W. Zheng, Z. Cui, and T. Zhang, "Face recognition based on recurrent regression neural network," *Neurocomputing*, vol. 297, pp. 50–58, 2018.

[20] H. Maeng, H.-C. Choi, U. Park, S.-W. Lee, and A. K. Jain, "Nfrad: Near-infrared face recognition at a distance," in *Proc. Int. Joint Conf. Biometrics*., 2011, pp. 1–7.

[21] M. He, J. Zhang, S. Shan, M. Kan, and X. Chen, "Deformable face net for pose invariant face recognition," *Pattern Recognit.*, vol. 100, 2020, Art. no. 107113.

[22] W. N. I. Al-Obaydy and S. A. Suandi, "Automatic pose normalization for open-set single-sample face recognition in video surveillance," *Multimedia Tools Appl.*, vol. 79, no. 3, pp. 2897–2915, 2020.

[23] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 15, no. 11, pp. 1148–1161, Nov. 1993.

[24] J. Daugman, "How iris recognition works," in *the Essential Guide to Image Processing*. Elsevier, 2009, pp. 715–739.

[25] C.-W. Tan and A. Kumar, "Accurate iris recognition at a distance using stabilized iris encoding and zernike moments phase features," *IEEE Trans. Image Process.*, vol. 23, no. 9, pp. 3962–3974, Sep. 2014.

[26] W. W. Boles and B. Boashash, "A human identification technique using images of the iris and wavelet transform," *IEEE Trans. Signal Process.*, vol. 46, no. 4, pp. 1185–1188, Apr. 1998.

[27] R. P. Wildes *et al.*, "A machine-vision system for iris recognition," *Mach. Vis. Appl.*, vol. 9, no. 1, pp. 1–8, 1996.

[28] R. P. Wildes, "Iris recognition: An emerging biometric technology," *Proc. IEEE*, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.

[29] S. Lim, K. Lee, O. Byeon, and T. Kim, "Efficient iris recognition through improvement of feature vector and classifier," *ETRI J.*, vol. 23, no. 2, pp. 61–70, 2001.

[30] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification based on iris patterns," in *Proc. 15th Int. Conf. Pattern Recognit.*, vol. 2., 2000, pp. 801–804.

[31] L. Ma *et al.*, "Iris recognition based on multichannel gabor filtering," in *Proc. 5th Asian Conf. Comput. Vis.*, vol. 1, 2002, pp. 279–283.

[32] L. Ma, Y. Wang, and T. Tan, "Iris recognition using circular symmetric filters," in *Proc. Object Recognit. Supported User Interact. Serv. Robots*, 2002, pp. 414–417.

[33] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.

[34] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[35] T. C. Meetei and S. A. Begum, "A variant of cancelable iris biometric based on biohashing," in *Proc. Int. Conf. Signal Inf. Process.*, 2016, pp. 1–5.

[36] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: A novel approach for cancelable biometrics," *Inf. Process. Lett.*, vol. 93, no. 1, pp. 1–5, 2005.

[37] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[38] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Trans. Syst., Man, Cybern., Part B.*, vol. 37, no. 4, pp. 980–992, Aug. 2007.

[39] D. Ahn, S. G. Kong, Y.-S. Chung, and K. Y. Moon, "Matching with secure fingerprint templates using non-invertible transform," in *Proc. Congr. Image Signal Process.*, 2008, pp. 29–33.

[40] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *Proc. 4th IEEE Int. Conf. Biometrics: Theory, Appl. Syst.*, 2010, pp. 1–7.

[41] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognit.*, vol. 44, no. 10-11, pp. 2555–2564, 2011.

[42] H. Yang, X. Jiang, and A. C. Kot, "Generating secure cancelable fingerprint templates using local and global features," in *Proc.2nd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, 2009, pp. 645–649.

[43] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with delaunay triangle-based local structures," in *Proc. Int. Symp. Cyberspace Saf. Secur.*, 2013, pp. 81–91.

[44] W. Yang, J. Hu, S. Wang, and Q. Wu, "Biometrics based privacy-preserving authentication and mobile template protection," *Wireless. Commun. Mobile Comput.*, vol. 2018, 2018.

[45] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach," *Pattern Recognit.*, vol. 45, no. 12, pp. 4129–4137, 2012.

[46] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, 2014.

[47] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognit.*, vol. 54, pp. 14–22, 2016.

[48] S. Wang, G. Deng, and J. Hu, "A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognit.*, vol. 61, pp. 447–458, 2017.

[49] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, 2017.

[50] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," *J. Inf. Secur. Appl.*, vol. 58, 2021, Art. no. 102704.

[51] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible minutia cylinder-code representation," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 6, pp. 1727–1737, Dec. 2012.

[52] K. Fukunaga, "Statistical pattern recognition," in *Handbook of Pattern Recognition and Computer Vision*, Singapore: World Scientific, 1993, pp. 33–60.

[53] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *Proc. Int. Conf. Biometrics Special Int. Group*., 2014, pp. 1–8.

[54] N. Zhang, X. Yang, Y. Zang, X. Jia, and J. Tian, "Generating registration-free cancelable fingerprint templates based on minutia cylinder-code representation," in *Proc. IEEE 6th Int. Conf. Biometrics: Theory, Appl. Syst.*, 2013, pp. 1–6.

[55] R. Arjona, M. A. Prada-Delgado, I. Baturone, and A. Ross, "Securing minutia cylinder codes for fingerprints through physically unclonable functions: An exploratory study," in *Proc. Int. Conf. Biometrics*., 2018, pp. 54–60.

[56] W. Yang *et al.*, "A cancelable iris-and steganography-based user authentication system for the Internet of Things," *Sensors*, vol. 19, no. 13, pp. 2985–3000, 2019.

[57] J. Qiu, H. Li, and C. Zhao, "Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication," *Comput. Secur.*, vol. 82, pp. 1–14, 2019.

[58] F. Ahmad, L.-M. Cheng, and A. Khan, "Lightweight and privacy-preserving template generation for palm-vein-based human recognition," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 184–194, 2019.

[59] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, 2017.

[60] M. K. Morampudi, M. V. Prasad, and U. Raju, "Privacy-preserving iris authentication using fully homomorphic encryption," *Multimedia Tools Appl.*, vol. 79, pp. 19215–19237, 2020.

[61] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Secur. Privacy*., 1998, pp. 148–157.

[62] C. Rathgeb and A. Uhl, "Context-based biometric key generation for iris," *IET Comput. Vis.*, vol. 5, no. 6, pp. 389–397, 2011.

[63] A. Beng, J. Teoh, and K.-A. Toh, "Secure biometric-key generation with biometric helper," in *Proc. 3rd IEEE Conf. Ind. Electron. Appl*., 2008, pp. 2145–2150.

[64] C. Rathgeb and A. Uhl, "An iris-based interval-mapping scheme for biometric key generation," in *Proc. 6th Int. Symp. Image Signal Process. Anal.*, 2009, pp. 511–516.

[65] N. D. Roy and A. Biswas,"Fast and robust retinal biometric key generation using deep neural nets," *Multimedia Tools Appl.*, vol. 79, no. 9, pp. 6823–6843, 2020.

[66] Y. S. Pagar and G. Chowdhary, "Strengthening elliptic curve cryptography-key generation via biometric fusion approach," in *Computing in Engineering and Technology*, Springer, 2020, pp. 87–101.

[67] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2004, pp. 523–540.

[68] K. Xi, J. Hu, and F. Han, "An alignment free fingerprint fuzzy extractor using near-equivalent dual layer structure check (NeDLSC) algorithm," in *Proc. 6th IEEE Conf. Ind. Electron. Appl.*, 2011, pp. 1040–1045.

[69] W. Yang, J. Hu, and S. Wang, "A delaunay triangle-based fuzzy extractor for fingerprint authentication," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, 2012, pp. 66–70.

[70] D. Chang, S. Garg, M. Hasan, and S. Mishra, "Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3152–3167, 2020.

[71] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, 1999, pp. 28–36.

[72] C. Rathge, A. Uhl, and P. Wild, "Reliability-balanced feature level fusion for fuzzy commitment scheme," in *Proc. Int. Joint Conf. Biometrics*., 2011, pp. 1–7.

[73] L. Zhang, Z. Sun, T. Tan, and S. Hu, "Robust biometric key extraction based on iris cryptosystem," in *Proc. Int. Conf. Biometrics*., 2009, pp. 1060–1069.

[74] M. Sandhya and M. V. Prasad, "A bio-cryptosystem for fingerprints using Delaunay neighbor structures (dns) and fuzzy commitment scheme," in *Proc. Adv. Signal Process. Intell. Recognit. Syst.*, 2016, pp. 159–171.

[75] M. Sandhya and M. V. Prasad, "Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 31, no. 4, 2017, Art. no. 1756004.

[76] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Syst. Appl.*, vol. 40, no. 5, pp. 1888–1901, 2013.

[77] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 103–117, Mar. 2010.

[78] S. Nazari, M.-S. Moin, and H. R. Kanan, "Securing templates in a face recognition system using error-correcting output code and chaos theory," *Comput. Elect. Eng.*, vol. 72, pp. 644–659, 2018.

[79] B. P. Gilkalaye, A. Rattani, and R. Derakhshani, "Euclidean-distance based fuzzy commitment scheme for biometric template security," in *Proc. 7th Int. Workshop Biometrics Forensics*, 2019, pp. 1–6.

[80] W. Yang *et al.*, "Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem," *IEEE Access*, vol. 6, pp. 36939–36947, 2018.

[81] L. A. Elrefaei and A. M. Al-Mohammadi, "Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme," *J. King Saud University-Comput. Inf. Sci.*, 2019.

[82] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptogr.*, vol. 38, no. 2, pp. 237–257, 2006.

[83] J. Li, X. Yang, J. Tian, P. Shi, and P. Li, "Topological structure-based alignment for fingerprint fuzzy vault," in *Proc. 19th Int. Conf. Pattern Recognit.*, 2008, pp. 1–4.

[84] K. Xi and J. Hu, "Biometric mobile template protection: A composite feature based fingerprint fuzzy vault," in *Proc. IEEE Int. Conf. Commun.*, 2009, pp. 1–5.

[85] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, and J. Kim, "A new method for generating an invariant iris private key based on the fuzzy vault system," *IEEE Trans. Syst., Man, Cybern.*, *Part B*, vol. 38, no. 5, pp. 1302–1313, Oct. 2008.

[86] L. Wu and S. Yuan, "A face based fuzzy vault scheme for secure online authentication," in *Proc. 2nd Int. Symp. Data, Privacy, E-Commerce*, 2010, pp. 45–49.

[87] V. Joshi and P. Sanghavi, "Three tier data storage security in cloud using face fuzzy vault," in *Proc. Int. Conf. Comput., Commun. Appl.*, 2012, pp. 1–6.

[88] L. Leng and A. B. J. Teoh, "Alignment-free row-co-occurrence cancelable palmprint fuzzy vault," *Pattern Recognit.*, vol. 48, no. 7, pp. 2290–2303, 2015.

[89] K. Bobkowska, K. Nagaty, and M. Przyborski, "Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault," *IET Image Process.*, vol. 13, no. 13, pp. 2516–2528, 2019.

[90] W. Yang, J. Hu, and S. Wang, "A finger-vein based cancellable bio-cryptosystem," in *Proc. Int. Conf. Netw. Syst. Secur.*, 2013, pp. 784–790.

[91] K. Xi, T. Ahmad, F. Han, and J. Hu, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 487–499, 2011.

[92] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[93] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.

[94] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9390–9401, Sep. 2020.

[95] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 42–52, Mar. 2013.

[96] H. Chun, Y. Elmehdwi, F. Li, P. Bhattacharya, and W. Jiang, "Outsourceable two-party privacy-preserving biometric authentication," in *Proc. 9th ACM Symp. Inf., Comput. Commun. Secur.*, 2014, pp. 401–412.

[97] Y. Tian, Y. Li, X. Liu, R. H. Deng, and B. Sengupta, "Pribioauth: Privacy-preserving biometric-based remote user authentication," in *Proc. IEEE Conf. Dependable Secure Comput.*, 2018, pp. 1–8.

[98] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Conf. Theory Appl. Cryptographic Techn.*, 1986, pp. 186–194.

[99] A. Bhargav-Spantzel, A. C. Squicciarini, R. Xue, and E. Bertino, "Multifactor identity verification using aggregated proof of knowledge," *IEEE Trans. Syst., Man, Cybern., Part C. (Applications and Reviews)*, vol. 40, no. 4, pp. 372–383, Jul. 2010.

[100] H. Gunasinghe and E. Bertino, "Privbiomtauth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 1042–1057, Apr. 2018.
[101] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Int. Conf. Audio Video-Based Biometric Person Authentication*, 2001, pp. 223–228.
[102] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proc. Biometrics Symp. IEEE*, 2007, pp. 1–6.
[103] C. Li and J. Hu, "Attacks via record multiplicity on cancelable biometrics templates," *Concurrency Comput.: Pract. Experience*, vol. 26, no. 8, pp. 1593–1605, 2014.
[104] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proc. 30th IEEE Symp. Secur. Privacy*, 2009, pp. 188–203.
[105] I. Buhan-Dulman, J. Merchan, and E. Kelkboom, "Efficient strategies for playing the indistinguishability game for fuzzy sketches," in *Proc. IEEE Workshop Inf. Forensics Secur. (WIFS)*, 2010.
[106] A. Adler, "Vulnerabilities in biometric encryption systems," in *Proc. Int. Conf. Audio-and Video-Based Biometric Person Authentication*, 2005, pp. 1100–1109.
[107] A. B. J. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electron. Exp.*, vol. 4, no. 23, pp. 724–730, 2007.
[108] F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," Comput. Lab., Univ. Cambridge, Tech. Rep. UCAM-CL-TR-640, Jul. 2005. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-640.pdf
[109] F. Carter and A. Stoianov, "Implications of biometric encryption on wide spread use of biometrics," in *EBF Biometric Encryption Seminar* (Jun. 2008), vol. 29, 2008.
[110] E. J. Kelkboom, J. Breebaart, T. A. Kevenaar, I. Buhan, and R. N. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 1, pp. 107–121, Mar. 2011.
[111] P. Mihailescu, A. Munk, and B. Tams, "The fuzzy vault for fingerprints is vulnerable to brute force attack," *BIOSIG*, 2009, pp. 43–54.
[112] H. T. Poon and A. Miri, "A collusion attack on the fuzzy vault scheme," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 27–34, 2009.
[113] E.-C. Chang, R. Shen, and F. W. Teo, "Finding the original point set hidden among chaff," in *Proc. ACM Symp. Inf., Comput. Commun. Secur.*, 2006, pp. 182–188.
[114] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, 2004, pp. 82–91.
[115] Y. Li, S. Liu, D. Gu, and K. Chen, "Reusable fuzzy extractor based on the LPN assumption," *Comput. J.*, vol. 63, no. 12, pp. 1826–1834, 2020.

QUANG NHAT TRAN received the B.S. degree majoring in computer science from New Mexico Highlands University, Las Vegas, NM, USA, in 2012 and Masters by Research degree from the University of New South Wales, Canberra, NSW, Australia, where he is currently working toward the Ph.D. degree with the University of New South Wales. In 2013, he became a Lecturer with the Department of Computer Science and Technology, Posts and Telecommunication, Institute of Technology, Hanoi, Vietnam. His research interests include computer security, biometric template protection, biometric cryptography, blockchain technology, and applications.

BENJAMIN TURNBULL received the Bachelor degree in software engineering (Hons) in 2003 and Ph.D. degree in digital forensics in 2007, both from the University of South Australia. He is also CISSP certified, He is currently a Senior Lecturer with the Australian Centre for Cyber Security, University of New South Wales, Canberra, NSW, Australia. He was previously with the Australian Defence Force. His research interests include cyber-resilience, cyber-kinetic impact analysis, and novel methods for network analysis.

JIANKUN HU (Senior Member, IEEE) received the B.E. degree from Hunan University, Changsha, China, in 1983, the Ph.D. degree in control engineering from the Harbin Institute of Technology, Harbin, China, in 1993, and the Masters by Research degree in computer science and software engineering from Monash University, Melbourne, VIC, Australia, in 2000. He is currently a Full Professor with the School of Engineering and Information Technology, University of New South Wales, Canberra, NSW, Australia. From 1995 to 1996, he was with the Ruhr University, Bochum, Germany, on the prestigious German Alexander von Humboldt Fellowship and from 1998 to 1999, a Research Fellow with Melbourne University, Melbourne, VIC, Australia. He has authored or coauthored many papers in high quality conferences and journals including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE in his area of research which include cyber security, including Image Processing, Forensics, and machine learning. He was on the Editorial Board of up to seven international journals including the top Journals IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and was the Security Symposium Chair of IEEE flagship conferences of IEEE ICC and IEEE Globecom. He was the recipient of the nine Australian Research Council (ARC) grants and was with the prestigious Panel of Mathematics, Information and Computing Sciences, ARC Excellence in Research for Australia Evaluation Committee.