Artificial Intelligence Review (2020) 53:3403–3446
https://doi.org/10.1007/s10462-019-09767-8

Cancelable Biometrics: a comprehensive survey

Manisha[1] · **Nitin Kumar**[1]

Published online: 9 October 2019

Abstract
Biometric recognition is a challenging research field but suffers from privacy and security concerns. To address this concern, Cancelable Biometrics is suggested in literature in which a Biometric image of a sample is distorted or transformed in such a manner that it becomes difficult to obtain the original Biometric image from the distorted one. Another important characteristic of Cancelable Biometrics is that it can be reissued if compromised. In this research paper, we present a comprehensive survey of more than 120 techniques suggested by various researchers from time to time for Cancelable Biometrics and a novel taxonomy for the same is developed. Further, various performance measures used in Cancelable Biometrics are reviewed and their mathematical formulations are given. Cancelable Biometrics also suffer from various security attacks as given in literature. A review of these security attacks is carried out. We have also performed a review of databases used in literature for nine different Cancelable Biometrics viz. Face, Iris, Speech, Fingerprint, Signature, Palmprint, ECG, Palmvein and Fingervein. Lastly, we have also given future research directions in this field. This study shall be useful for the researchers and practitioners working in this fascinating research area.

Keywords Taxonomy · Performance · Databases · Survey · Attacks

1 Introduction

Biometric is derived from two Greek words viz. *Bio* means *life* and Metric means *to measure*. There are several traits or characteristics (Jain et al. 2004) such as Finger, Face, Ear, Iris, Gait, Palm, Hand Geometry etc., which are most widely used Biometrics. Biometric technology have been widely used in several applications (Jain et al. 2007) such as access control, border immigration control, corpse identification, surveillance, forensic sectors, human computer interaction, behavior analysis etc. Biometrics are divided into two categories i.e. (i) Physical and (ii) Behavioral. Physical Biometrics are based on measuring the physical characteristics

✉ Nitin Kumar
nitin@nituk.ac.in

Manisha
manisharawat@nituk.ac.in

[1] Department of Computer Science and Engineering, National Institute of Technology, Uttarakhand, Srinagar, India

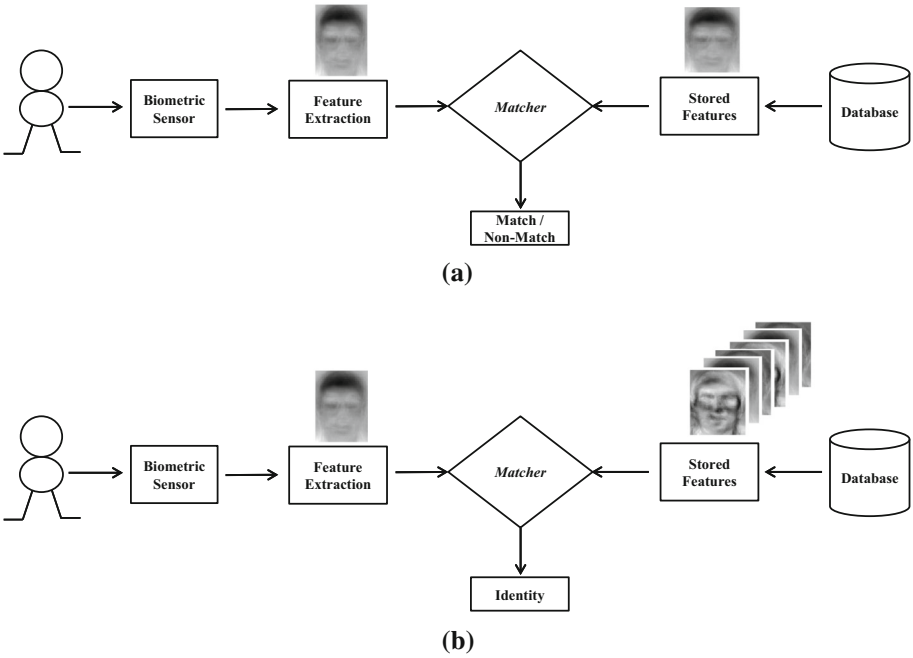

Fig. 1 Biometric recognition process: **a** verification **b** identification

of a person such as Face, Iris, Finger etc. while Behavioral Biometrics are based on measuring behavioral traits of a person such as Gait, Hand Gesture, Speech etc.

Biometric recognition refers to the activity of Identifying and/or Verifying the identity of a person. Biometric recognition usually work in two scenarios: (i) Verification and (ii) Identification. In Verification, the claimed identity by the user is matched with the already stored pattern/features corresponding to the user and a match/non-match is determined by the system. In Identification, user's Biometric is presented to the system and matched with all the stored patterns/features to determine the identity of the user. Sample process of Identification and Verification is shown in Fig. 1. It is apparent from Fig. 1 that Verification is 1:1 matching while Identification is 1:*N* matching.

Although Biometrics is a useful concept but there are some security and privacy concerns which can render breach to the Biometric data of an individual by some intruder or external entity. To address this concern, a concept called Cancelable Biometrics have been introduced by Soutar et al. (1998) in literature and is defined by Patel et al. (2015) as: *Cancelable Biometrics (CB) consist of intentional, repeatable distortions of Biometric signals based on transforms which provide a comparison of Biometric templates in the transformed domain*. Various milestones in the journey of Cancelable Biometrics are depicted in Fig. 2.

Cancelable Biometrics is aimed at enhancing privacy protection and template security in existing Biometric system(s). In this field, the Biometric template of a person is distorted in such a manner that the original data is not available to the intruder but still identity recognition can be performed. The Cancelable Biometric must possesses four important characteristics viz. (i) Diversity (ii) Reusabiltiy or Revocability(iii) Non-invertibility (iv) Performance

– **Diversity**: Same Cancelable Biometric template cannot be used for various applications.

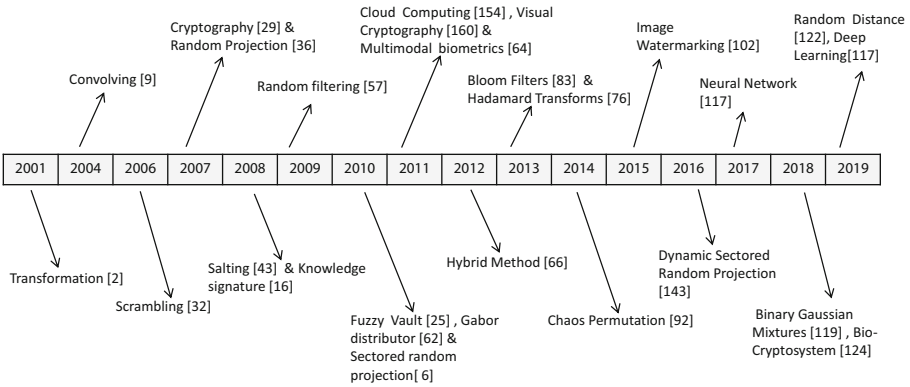

Fig. 2 Selected milestones at various years (written in boxes) for cancelable biometrics

- **Reusability/Revocability**: Template reissued if compromised.
- **Non-invertibility**: Original Biometric cannot be recovered if the generated template got compromised.
- **Performance**: The recognition performance should not deteriorate by the formulation.

Cancelable Biometric recognition process consists of two phases i.e. (i) Enrollment and (ii) Authentication as shown in Fig. 3. During Enrollment, a user presents his/her Biometric to the Biometric scanner. Then, features are selected or extracted from the Biometric image of the user. Afterwards, Cancelable Biometric template is generated using some technique such as Hashing, Filtering, Cryptography etc. These templates are then stored in the database. During Authentication, the Cancelable Biometric template is obtained similar to the Enrollment phase with same feature extraction and Cancelable Biometric template generation methods. Lastly, matching of the probe is done with the already stored templates in the database and Verification/Identification is carried out.

A survey of Cancelable Biometric template generation methods is given by Patel et al. (2015). In their work, Cancelable Biometric methods are broadly divided into ten categories viz. (i) Non-invertible Geometric Transforms (ii) Random Projections (iii) Cancelable Biometric Filters (iv) Bioconvolving (v) Bloom Filters (vi) Knowledge Signatures (vii) Bio-Hashing Methods (viii) Random Permutations (ix) Salting Methods and (x) Hybrid Methods. However, there is no discussion of performance measures and details of databases used for Cancelable Biometrics. Moreover, there has been significant number of techniques proposed by researchers since Patel et al. (2015) paper.

1.1 Contribution

Although Cancelable Biometrics is an emerging and potential research area but lack of comprehensive study on this research area is not available except one or two studies. In this study, we have made the following 5-fold contribution:

(i) We have presented a comprehensive survey of Cancelable Biometric techniques which includes more than 120 research works and is almost double than done by Patel et al. (2015).
(ii) A novel taxonomy of Cancelable Biometric template generation methods is developed.

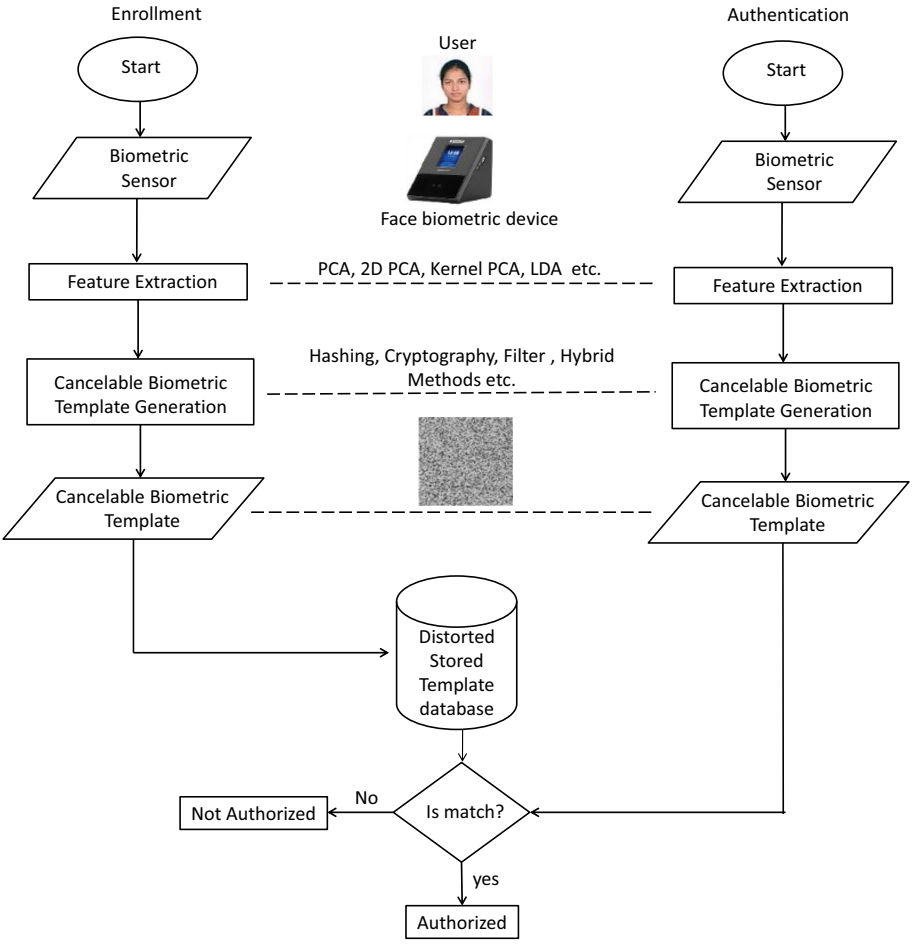

Fig. 3 Flowchart of cancelable biometric recognition process

(iii) A comprehensive review of various performance measures used in Cancelable Biometrics.
(iv) A comprehensive survey of various security attacks in Cancelable Biometric.
(v) A comprehensive review of Biometric databases used in Cancelable Biometric template generation.

The rest of the paper is organized as follows: A comprehensive survey of Cancelable Biometric template generation Methods is given in Sect. 2. Various performance measures are reviewed in Sect. 3 while security attacks are discussed in Sect. 4. Biometric databases are reviewed in Sect. 5 and concluding remarks and future research directions are given in Sect. 6 at the end.

2 Cancelable Biometrics template generation methods

Cancelable Biometric template generation has been a popular research area for the past two decades. Several research works have been suggested in literature for the same using various methods. We have broadly divided these methods into six categories by taking into consideration some factors such as the approach for template generation, single or multiple Biometrics. A novel taxonomy has been proposed and is shown in Fig. 4. Next, we discuss methods under each of these categories.

2.1 Cryptography based methods

Cryptography based methods employ Cryptography algorithms for generation of Cancelable Biometric templates. Based on the type of algorithm used, these techniques are divided into various types such as Visual Cryptography, Image Hashing, Knowledge Signature, Elliptic Curve Cryptography (ECC), Chaos, Steganography, Fuzzy Commitment and Hill Cipher. Next, we describe each of these techniques:

In *Visual Cryptography*, an input image is transformed into another image by exploiting human visual system as shown in Fig. 5. The secret binary image is divided into n non-overlapping patches known as Visual Secret Shares (VSS) and these shares are stored in a decentralized database. To recover original image, all or some shares need to be stack together. This technique is basically works on k-out of-n principle.

In research work (Kaur and Khanna 2016), Visual Cryptography technique has been successfully implemented for generating Cancelable Biometrics templates. Based on efficiency of the templates, the system performance is determined.

Image Hashing is a well known content-based image authentication method. It defines a feature vector called short binary signature that characterizes the image independently without any significant distortion of its contents (Tan et al. 2009). BioHashing is a feature extraction method in which wavelet transform is used to extract the Biometric feature $\mathbf{x} \in \mathbb{R}^N$ from the input Biometric data. Using a user-specific Tokenized Random Number (TRN), n orthogonal pseudo-random vectors, $\mathbf{b_i} \in \mathbb{R}^N$ are generated where dot product of the feature vector and all the random vectors is calculated. Finally, a binary discretization is applied to compute the n bit BioHash (c) template using equation given below:

$$c = Sig\left(\sum_i \mathbf{x}\mathbf{b}_i - \Omega\right) \tag{1}$$

where Sig is defined as a signum function and Ω is an empirically determined threshold which is applied only to a user who holds TRN. Figure 6 shows the process of BioHashing method.

Base BioHashing (Meetei and Begum 2016) is another variant of BioHashing which generates a vector of bits starting from the Biometric feature set and a seed which represents the Hash key. The main problem with BioHashing procedure is its low performance when some imposter tries to access the system by stealing the Hash key. To overcome this problem, Lumini and Nanni (2007) have proposed Extended BioHashing method which is the improved version of Base BioHashing. In this method, Biometric feature vectors are normalized before applying the BioHashing procedure. This is followed by multiple variation values from minimum to maximum and spaces augmentation. Multiple BioHash codes can be generated by simply performing permutaion procedure. In research work (Raja et al. 2018b), another variant of hashing called Kernelized Hashing is introduced which exploits Kernel function. Its

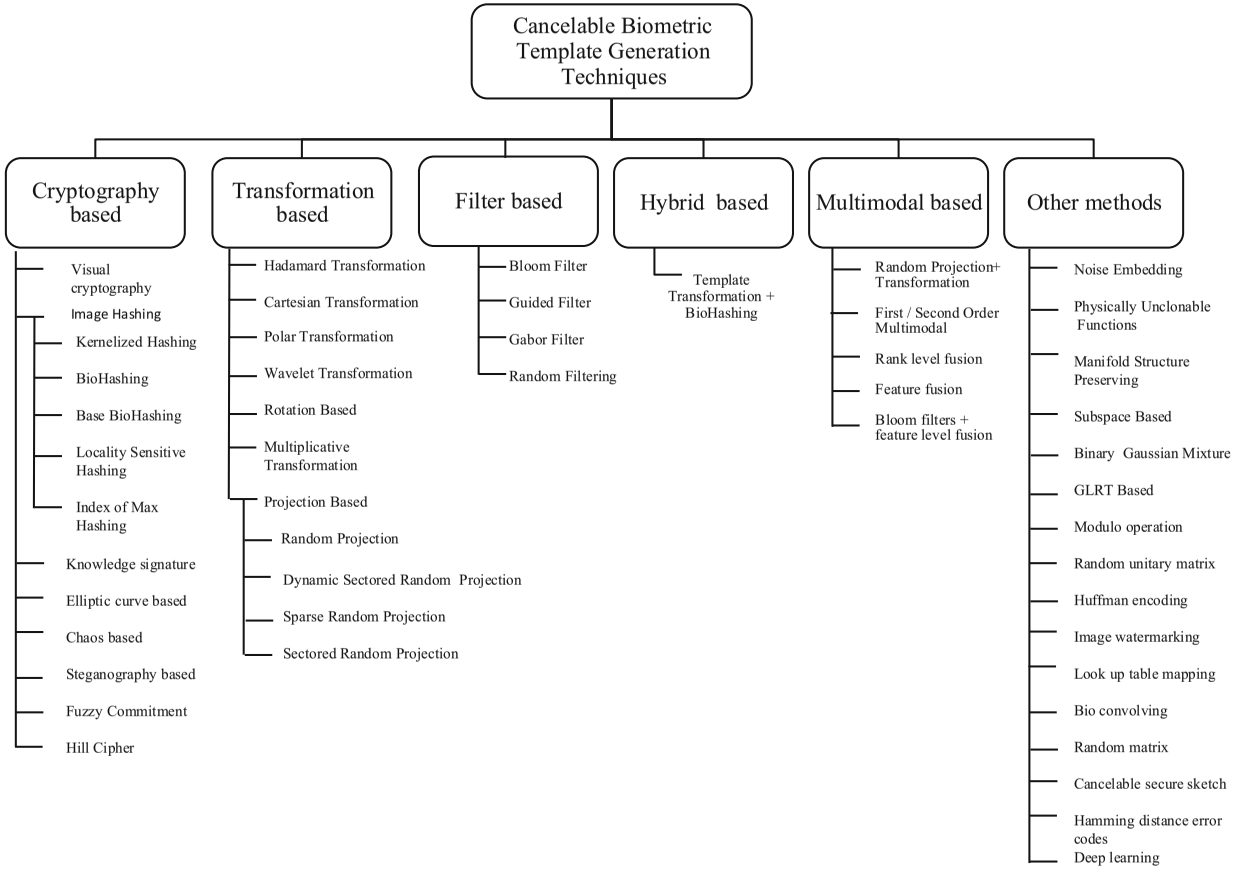

Fig. 4 Proposed taxonomy of cancelable biometric techniques

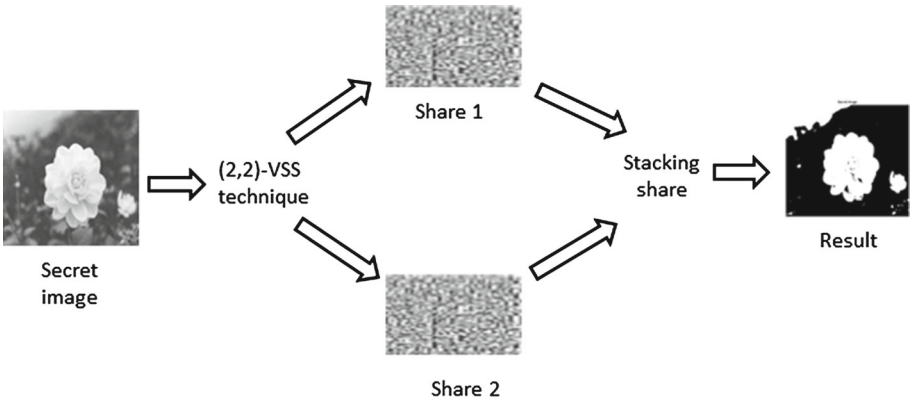

Fig. 5 2-out of-2 visual secret shares in visual cryptography

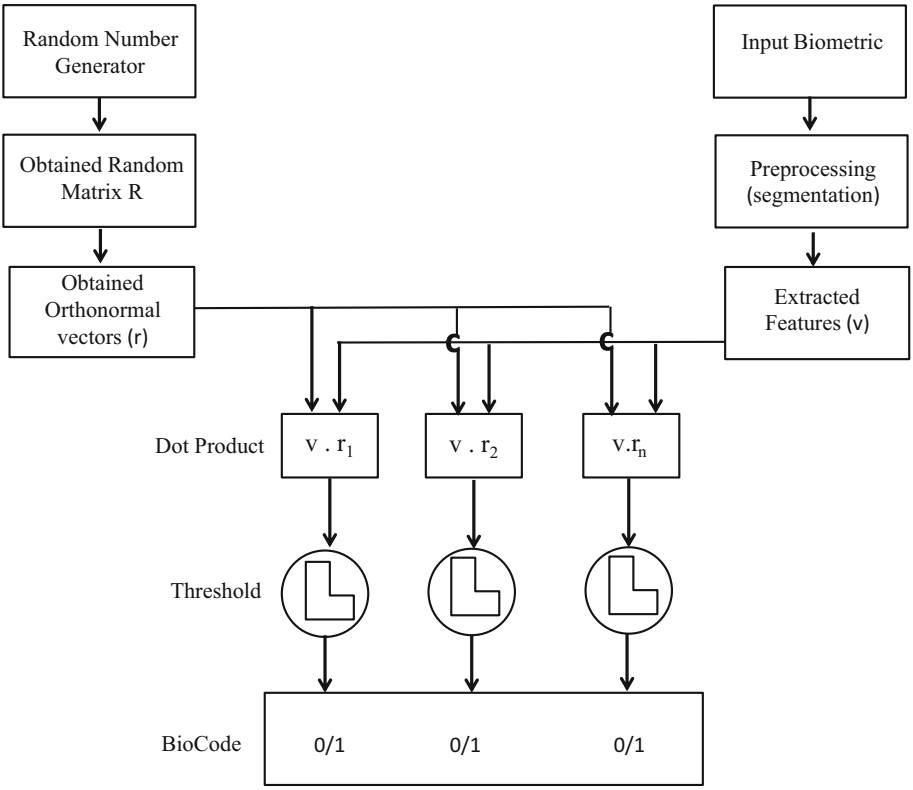

Fig. 6 Schematic representation of BioHashing method

function is defined as given the features **f** of an image in an enrollment database of l subjects, to obtain unique template for each user. Here, we need to derive r hash functions resulting into r bit representation. Hence, the objective here is to learn r hash functions $\{h_x\}_{k=1}^{r}$ for r hash bits corresponding to each user.

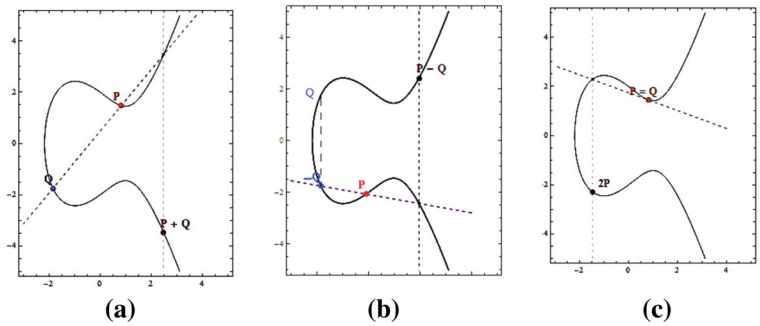

Fig. 7 Addition, subtraction and point doubling in ECC (Singh and Singh 2015)

Locality Sensitive Hashing (LSH) is another technique where a probability distribution on a family H of hash functions (h) such that $P_{h\in H}\,[h(\mathbf{X}) = h(\mathbf{Y})] = S(\mathbf{X}, \mathbf{Y})$ where S is a similarity function defined on the collection of object features $\mathbf{X}$ and $\mathbf{Y}$ (Jin et al. 2018). The main objective in LSH is dimensionality reduction of input features by mapping the similar input data in the same buckets such that count of buckets are smaller than input items. Indexing First Order Hashing (IFOH) is a variant of LSH for Biometric template protection. IFOH works in 4 steps namely (i) Hadamard Product (ii) Windowing (iii) Index Conversion and (iv) Modular Thresholding, to generate an IFOH hashed code from binary Biometric (Kim and Teoh 2018). Index of Max Hashing (IoMH) (Jin et al. 2018) transforms a real valued Biometric feature vector into discrete index (max ranked) hashed code. The main advantage of this technique is that after hashing we get accurate hashed code than other hashing techniques.

Knowledge Signature technique allows one party to convince other parties about its knowledge of certain value, such that no useful information is leaked. It is usually used to confirm the group members in group signatures. In research works (Xu et al. 2008; Camenisch and Stadler 1997), voice print is employed as a knowledge signature which does not represent the original features and represent the identity of the group. The main advantage of this method is that it has only an weak association between the key and the Biometrics feature. Even if the key is disclosed, the Biometrics feature would not be revealed.

Elliptic Curve Cryptography (ECC) technique is used to obtain a stable input from Biometric data which is used to generate the security parameters of the Elliptic Curve, various studies on ECC have concluded that the difficultly to solve an Elliptic Curve Discrete Logarithmic Problem is exponentially hard with respect to the key size used. This property makes ECC a very good choice for encryption/decryption process compared to other cryptographic techniques which are linearly difficult or sub exponentially difficult. Abid et al. (2010) have generated Iris templates using ECC technique. ECC operations are performed on the coordinates points of an Elliptic Curve (Fig. 7). To perform addition of two distinct points, the following equation is used:

$$\begin{aligned} P(x_1, y_1) + Q(x_2, y_2) &= R(x_3, y_3) \\ x_3 &= (\lambda^2 - x_1 - x_2) * mod[P] \\ y_3 &= (\lambda(x_1 - x_3) - y_1) * mod[P] \\ \lambda &= \frac{(y_2 - y_1)}{(x_2 - x_1)} * mod[P] \end{aligned} \tag{2}$$

To perform point subtraction, a mirror coordinate of the subtracted point along x-axis is obtained and point addition is performed on the resulting coordinate and the other coordinate as follows:

$$P(x_1, y_1) - Q(x_2, y_2) = P(x_1, y_1) + Q(x_2, y_2) \tag{3}$$

Point doubling is performed to add two points which are same i.e. they have same coordinate value.

$$\begin{aligned} P(x_1, y_1) + Q(x_1, y_1) &= R(x_3, y_3) \\ x_3 &= (\lambda^2 - 2x_1) * mod[P] \end{aligned} \tag{4}$$

where $\lambda = ((3x_1^2 + a)/(2y_1)) * mod[P]$.

Multiplication is repeated addition of the base coordinate point.

$$kP = P + P + P + P + \cdots\cdots\cdots + ktimes \tag{5}$$

Encryption and Decryption using ECC: Let A and B be the two communicating party. The communicating parties agrees upon the Elliptic curve equation and a Generator.

$$y^2 = \left\{X^3 + ax + b\right\} * mod\,[P] \tag{6}$$

In *Chaos Based* technique, Chaotic sequence is a pseudorandom sequence with complex structure produced by using chaotic map (Nazari et al. 2014) in such a way that the prediction of chaotic sequence becomes a very difficult task. One of the famous chaotic map in polynomial structure is 1-D logistic map (Karabat and Erdogan 2009b). This map generates the pseudo random numbers which represent complicated behaviors with high sensitivity to initial conditions. In *Steganography* technique, a message is hidden inside other multimedia content like image, audio, video is known as Embedding. In research work (Choudhury et al. 2016), the combination of Huffman Encoding and Discrete Cosine Transform (DCT) is used in steganography to conceal a secret image in a cover image. Therefore, retrieving the exact original image from the Stego image is nearly impossible. *Fuzzy Commitment/Vault* technique is a combination of Error Correction Code and Cryptography (Yang et al. 2018a). It can conceal and bind a secret in a way that makes it infeasible for an intruder to learn the secret. Fuzzy Vault could be used to securely store one's secret or Cryptographic key without losing his Biometric information (Xu and Li 2009; You et al. 2017).

In *Hill Cipher Encryption*, plain text **P** is encrypted using a key or transformation function **K** and their matrix multiplication produces ciphertext **C** as given in Eq. (7) below:

$$\mathbf{C} = [\mathbf{K} * \mathbf{P}] * mod(n) \tag{7}$$

where n is 26 in case of text and 256 in case of gray levels.

For decryption of cipher text, we need to compute $\mathbf{K}^{-1}$ as given in Eq. (8) below:

$$\mathbf{P} = [\mathbf{K}^{-1} * \mathbf{C}] * mod(n) \tag{8}$$

Figure 8 shows the encrypted image by Hill Cipher technique. If an intruder tries to decrypt image, he/she will get totally distorted image which does not reveal original user identity. The main advantage of this technique is its simplicity for implementation because it only uses matrix multiplication which in turn provide high speed with high throughput (Kaur and Khanna 2017b).

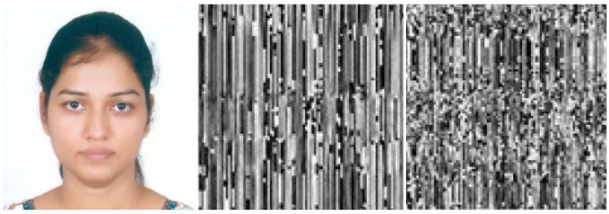

Fig. 8 **a** Input image **b** encrypted image **c** decrypted image

2.2 Transformation based methods

Non Invertible transformation is one of the earliest method for generating Cancelable Biometric templates. In this method, the original Biometric templates are morphed by applying different transformations e.g. Cartesian, Polar etc. In Cartesian transformation, the minutiae positions are measured in rectangular coordinates with reference to the position of the singular point by aligning x-axis with its orientation. The coordinate system is divided into cells of fixed size. The transformation causes changes in the cell positions. In Polar transformation, the minutiae positions are measured in the polar coordinate with reference to the core position. The angles are measured with respect to the core orientation. As a result, the coordinate space is divided into polar regions. The Non Invertible transform consists of changing the polar wedge positions. The minutiae angles also change with differences in the wedge positions before and after transformation. The main problem with Cartesian and Polar transformations is that a small change in minutiae position of the original fingerprint can lead to a large deviation in minutiae position after transformation. Both these transformations are mainly used for fingerprint Biometric. Please refer Patel et al. (2015), Pillai et al. (2010), Popa and Simion (2017), Paul and Gavrilova (2012, 2013a, b, 2014a, b), Paul et al. (2013), Pillai et al. (2011), Quan et al. (2008), Rathgeb and Busch (2013, 2014), Rathgeb et al. (2013, 2014), Ratha et al. (2001, 2006, 2007) for details.

Hadamard transform is a non-sinusoidal, orthogonal transformation whose foundation lies in Walsh functions. Walsh functions are rectangular or square waveforms with values of $+1$ or -1. Hadamard matrix is defined as a matrix whose elements are $+1$ and -1 and its row vectors are pairwise orthogonal. Hadamard Transform is divide into two types (i) Partial Hadamard and (ii) Full Hadamard. Former is Non Invertible while later is Invertible in nature. The research work (Wang and Hu 2013) uses Partial Hadamard Transform which can be formed by selecting some number of rows from Full Hadamard Tranform. The main advantages of Hadamard Transform are (i) low computational cost as only addition and subtraction functions are used and (ii) low storage requirement due to storage of only partial transformation. Hämmerle-Uhl et al. (2013) proposed Iris based Cancelable Biometric template using key dependent Wavelet transformation. This method is free from the problem of data loss and alignment of features. Multiplicative transform is employed by Wang and Hatzinakos (2010) where element by element multiplication of the original Biometric feature vector with some random vector is computed. Index numbers of resulting vector are sorted and stored for retrieving Biometric template.

Random Projection (RP) is a Non Invertible method. In this method, the extracted feature vector $\mathbf{x} \in \mathbb{R}^N$ from a Biometric is projected onto a random subspace $\mathbf{A} = [\mathbf{a}_{ij}]$ (where $\mathbf{A} \in \mathbb{R}^{n*N}$ with $n < N$). Here, each entry $\mathbf{a}_{ij}$ of $\mathbf{A}$ is an independent realization of a random variable. This process is described as follows:

$$\mathbf{y} = \mathbf{Ax} \tag{9}$$

where $\mathbf{y}$ is the n dimensional Random Projection vector. Since we are embedding N dimensional feature vectors in a space of a lower dimension n. A detailed description of these methods is given in Pillai et al. (2011), Lingli and Jianghuang (2010), Deshmukh and Balwant (2017), Punithavathi and Geetha (2016). Sector Random Projection (SRP) is another variant of projection which overcomes the problem of Random Projection. Pillai et al. (2010) uses SRM for generating Cancelable template for Iris, in which we firstly divide the whole Iris into different parts called them as Sectors. Secondly, Random Projections are applied on these Sectors separately and finally all these sectors are concatenated to make Cancelable Iris template. Similarly this technique can also be applied to other Biometric traits (Punithavathi and Geetha 2016). Projected these sectored Iris code on a Dynamic Random Projection Matrix, which results in generation of Cancelable Iris templates. This Dynamic Random Projection Matrix is obtained by the Iris features itself without any need of external key. Kim and Toh (2008) used *Sparse Random Projection* for generating Cancelable Face templates. In general, random matrix consists of values between 0 and 1. For speed up the process of template generation and authentication, random matrix consists with the value of -1, 0 and $+1$.

2.3 Filter based methods

Cancelable Biometric Filter is a Convolution based method. *Bloom Filters* is a space efficient probabilistic data structure representing a set to support membership queries. Bloom filter based transformation of any binary feature vector generates irreversible Cancelable Biometric templates. Rathgeb et al. (2015b) used Bloom filter with fuzzy vault for preventing cross matching attack in Cancelable Biometric sysytem. Adaptive Bloom filter is another variant of Bloom filters. Rathgeb et al. (2014) used Adaptive Bloom filter for generting alignment free Cancelable iris Biometric template. This approach enables protection in Biometric templates, generates compressed Biometric data and reduces the computational time while maintaining Biometric recognition performance. In research work (Rathgeb et al. 2015a), Adaptive Bloom filter is used with Multi Biometric traits (Face and Iris) to generate more secure and better performance based Cancelable Biometric template.

Log Gabor filters are widely used in various research works for feature extraction due to better spatial and temporal information. Kaur and Khanna (2017a) used log-Gabor filters with Random Projection to generate Cancelable feature vectors. In this approach, authors have used Salting of extracted log-Gabor magnitude with phase patterns of Biometric signal which results in generatation of Non Invertible binary feature vector. Leng et al. (2010) used Gabour filter bank for feature extraction with Pseudocode Random Number (PRN) for generating Cancelable Palmcode template. A comparative study of seven possible randomization schemes of Gabor filter bank is given for generating Cancelable Palmcode. Kim et al. (2017) used Guided filter with Generalized Likelihood Ratio Test (GLRT) for generating ECG Cancelable Biometric template, which results in very good verification performance. Guided filter (Kim et al. 2017) are used in many computer vision applications such as denoising and artifact removal. Guided filter is usually used for local affine fitting of a guide image or signal in 1D to a noisy image. These filters possess low computational complexity. Takahashi and Hitachi (2009) used Co-relational invariant Random filtering for generating Fingerprint based Cancelable Biometric templates.

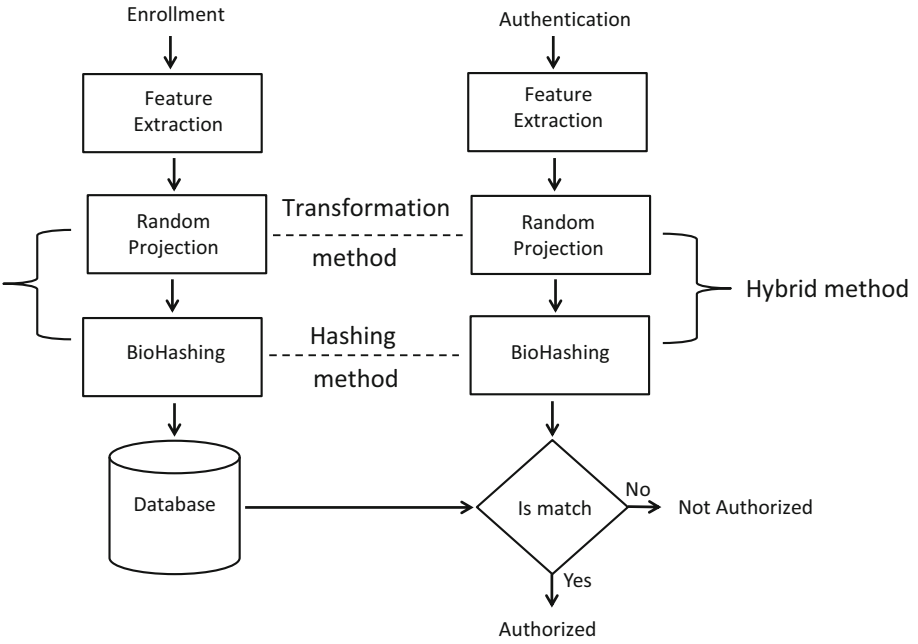

Fig. 9 An example of hybrid method

2.4 Hybrid methods

Hybrid Methods tend to combine two or more methods together to generate Cancelable Biometric template e.g. combination of Cryptography and Transformation Methods as shown in Fig. 9. Cancelability, Discriminability and Security phases are main part of this method (Ghany et al. 2012). Zhu et al. (2012) have employed Random Projection with Fuzzy Vault to generate Voiceprint templates. Wong et al. (2014) proposed a Hybrid method which is a combination of Multi Line Code (MLC) and Secure Sketch (SS) and called it Cancelable Secure Sketch (CaSS). MLC is generated in five phases i.e. (i) Minutiae extraction (ii) Multi Line code (MLC) (iii) Random Projection (iv) Kernel Principal Component Analysis (KPCA) (v) Binarization. The SS is a combination of bit string generated from the MLC (i.e bit string from Binarization step) and a random codeword, chosen from codebook e.g. Reed Solomon (RS) and BCH (Bose-Chaudhuri-Hocquenghem) codes.

2.5 Multimodal based methods

The main problems with Unimodal Biometric system were intraclass variability, variation in data quality and similarity in interclasss samples. In contrast, Multimodal Biometrics combine together multiple Biometric traits with various feature extraction algorithms to generate more secure templates. Multimodality can be achieved by combination of multiple Biometric traits such as taking multiple Biometrics for eg. Iris, Face, fingerprint of same user for identity recognition.

The main advantage of Multimodal Biometric system is that they result good in terms of reliablity, accuracy, spoof attacks, noise sensitivity and more secure than unimodal Biometric

system. Various methods have been suggested in literature for Multimodal Biometrics (Paul and Gavrilova 2012) such as cross fold of random indexes (Paul and Gavrilova 2013b), rank level fusion (Paul and Gavrilova 2014b), situation awareness in real time scenario (Paul et al. 2013), feature fusion (Paul and Gavrilova 2014a), bit extraction method (Chin et al. 2011), random distance method (Kaur and Khanna 2019), Biometric credential system (Suresh and Radhika 2015) etc. Paul and Gavrilova (2013b) have suggested First order, Second order and Multiorder Cancelable Biometric systems. In First order method, the Cancelable template is generated by using any Cancelable Biometric template generation technique once while in Second order method, two Cancelable Biometric template generation techniques are applied sequentially. In Multiorder method, Cancelable Biometric template generation techniques are applied multiple times which may be same technique with different parameters or different techniques altogether. Depending upon the number of times the Cancelable Biometric template generation method is applied, we can achieve high security but at the cost of increased computational complexity.

2.6 Other methods

Bio Convolving is also Non Invertible transform based approach mainly characterized by three transformations (i) Baseline (ii) Mixing and (iii) Shifting. Maiorana et al. (2011) proposed this approach for securing on-line signature templates. This approach can be applied to a various Biometric modalities e.g. Speech, in which spectral or temporal analysis of the voice signal creates discrete sequences. Similarly, In case of Signature and Handwriting recognition, where the extracted sequences based on the Pen's position and amount of pressure and inclination applied.

Random Permutations is another Biometric template protection method in which the gray values of Biometric image are reordered before further processing. Kumar et al. (2018) used Random Permutation Principal Component Analysis (RP-PCA) and Random Permutation Two Dimensional PCA (RP-2DPCA) for generating Face, Iris and Ear Cancelable templates. Two popular methods under this category are widely used for generating Cancelable Iris templates i.e. (i) GRAY-COMBO (ii) BIN-COMBO (Pillai et al. 2010). In GRAY-COMBO, binary feature vector of an Iris image are circularly shifted in horizontal direction using some random offset, then these two randomly selected rows are added or multiplied using addition and multiplication operator as shown in Fig. 10. In BIN-COMBO, horizontal row shifting process is same, after that randomly selected rows are combine with XOR and XNOR operator. The main advantage of this method is that amount of information needed for recognition gets reduced. The main limitation of this method good quality of iris images should be available.

Salting Method is an artificial pattern of pure random noise or synthetic pattern are mixed in original binary Iris image for generating Cancelable Biometric template as shown in Fig. 11. Mainly two approaches are there: (i) GRAY SALT and (ii) BIN SALT. In GRAY SALT, binary pattern Iris image pixel wised added or multiplied with some random image. In BIN

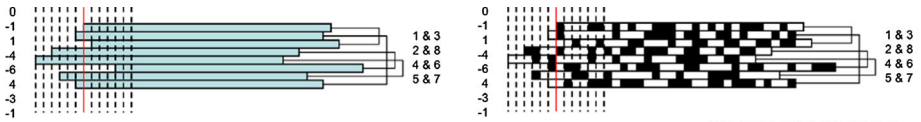

Fig. 10 GRAY-COMBO (left) and BIN-COMBO (right) methods (Pillai et al. 2010)

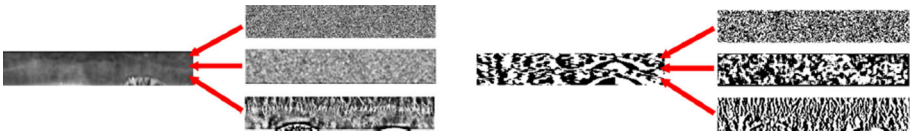

Fig. 11 GRAY-SALT (left) and BIN-SALT (right) methods (Pillai et al. 2010)

SALT, XOR or XNOR operation take place between binary pattern iris image and random image. The main limitation of this method is how to know what amount of artificial pattern we need to add with Iris pattern (Pillai et al. 2010). Addition of strong noise will reduce discerning property of original iris while addition of weaker pattern will reduce the security of the code, as by simply subtraction method we can obtain original iris. One advantage of this method over COMBO method is that no issues with the quality of iris image arises.

Deep learning is the latest concept introduced in the field of Cancelable Biometric template generation method. In research work (Talreja et al. 2017), a secure Multi Biometric system that uses deep neural networks and error-correction coding has been discussed. Two fusion architectures are discussed by the authors (i) Fully Connected Architecture (ii) Bi-linear Architecture. A binary vector template is passed through an appropriate error-correcting decoder to find a closest code word and this code word is hashed to generate the final secure template. Two important blocks of Multi Biometric framework are also introduced (i) Cancelable Template Block (CTB) (ii) Secure Sketch Cancelable Block (SSTB).

look-up table used by Dwivedi and Dey (2015) for generating Cancelable Iris templates. Extracted features with 1-D Log Gabor filter are used for generating rotational invariant codes. A 1-D row vector is generated from these binary codes, which are further divided into word of size M. A decimal vector is generated corresponding to these word, and a look-up table is created for mapping these decimal vector to a particular location. Finally, digits are selected from this look-up tables to generate Cancelable Iris template. The advantage of this method is that many words can go to same location, from which reverse mapping is very difficult. Barbier et al. (2015) proposed an approach, which is a combination of *image watermarking* and BioHashing for providing security and privacy in digital contents/images. Ownership of an image is verified by Watermark, which is computed from BioHashing based Cancelable Biometric technique.

Prasad et al. (2017) presented *Modulo based* Cancelable Iris template generation technique. Firstly, an Iris image is processed by segmentation, normalization and image enhancement respectively. Then, rotational invariant iris codes are generated which are transformed into row vector representation. From these codes consistent bits are identified, which formed consistent bit vector. A Modulo operation is performed on these consistent bit, which uses many to one mapping for template generation. Lee et al. (2018) proposed Iris based Cancelable template generation method based on *Noise Embedding*. In this approach, mainly three phases are used (i) Reduced Random Projection (ii) Hadamard Product and (iii) Decimal Encoding. Noise Embedding based on Reduced Random Projection and Biometric Salting method is used. From many Iris samples, coherent region is identified and Noise or random data/ auxiliary data is added to non coherent region of the iris to make it similar to coherent region. In this method, it is difficult for the intruder to distinguish between coherent and non-coherent region

Wu et al. (2018) proposed ECG Cancelable template recognition technique which is based on *Common Subspace* based *Multiple Signal Classification (MUSIC)* technique. Arjona et al. (2018) proposed two factor Cancelable Fingerprint generation scheme, Protected Minutia

Cylinder Codes(PMCC) are generated from Fingerprint images and *Physically Unclonable Functions* are generated from device's Static Random Access Memory(SRAM). Binary output of both phases are operated with XOR operator, which results in generation of Cancelable Fingerprint template. This approach mainly used in providing security in personal devices e.g. Smart phone, Laptop etc.

Saito et al. (2016) proposed effective *Random Unitary Matrix* for Cancelable Face Biometric template generation. The proposed matrix consists of Random Permutation Matrix and a Unitary Matrix such as Discrete Fourier Transform, which has value between 0 and 1. Raja et al. (2018a) proposed a *Neighborhood Structure Preserving Manifold* based template generation method. The generated template is called as Manifold structure Preserving Biometric Template (MaP BiT). Kanade et al. (2009) generates Cancelable Iris templates with *Error Correcting Codes*, for reduction of variablity in Biometric data. This technique reduces the *Hamming Distance* for the genuine comparisons than imposter comparison. Mtibaa et al. (2018) generates different Cancelable Speech templates by *Gaussian Mixture Models (GMM)*. A binary vector is generated from this model, from this vector by simple shuffling process different keys are generated. With the help of these keys, different Cancelable Speech templates are generated.

In our above research work, we have explained various Cancelable Biometrics templates generation techniques. Each technique has its own advantages and limitations. In Table 1 we have listed a comparison between various techniques and Table 2 lists Acronyms used in this paper.

3 Performance measures

In general, one algorithm is preferred over another algorithm if the performance of that algorithm is better than other algorithms. The performance measures provide us a useful tool to analyze the capability of an algorithm. Various performance measures are used to compare the algorithms or methods depending upon a particular domain or research area. Here, we provide a comprehensive review of the performance measures employed in Cancelable Biometric recognition.

3.1 Performance measures for verification

Two Biometric features belong to same user or not is determined by the similarity score. The matching of two samples of same user is known as authentic or genuine matching. The matching between two samples generated from two different user called imposter matching. Scores are used to express the similarity between a query pattern and genuine pattern. Higher value of score signifies higher similarity between them. A threshold value η is set for recognition process. A Biometric system assigns all attempts a score from closed group of [0, 1]. Score value 1 generally denotes full match and 0 represents no match. The value of threshold is taken very carefully, if it is set to 0, then genuine and intruder users, both are authenticated by the system. If set to 1, some risk should be there that none will be authenticated by the system. So threshold value should chosen very carefully in a closed group of 0 and 1. An intruder score that exceeds the threshold η known as False Accept (False Match), while a genuine score that falls below the threshold η known as False Reject (False Non-match). False positive (FP) signifies imposter scores exceeding threshold, False Negative (FN) denotes genuine user scores below threshold. True Negative (TN) shows truly

Table 1 Advantage and disadvantage of popular cancelable biometric approaches

Technique name	Advantages	Disadvantages	References
Visual Cryptography	Easy to implement, low computational cost , decryption algorithm is not required	High computational complexity for color images	Kaur and Khanna (2016)
BioHashing	Low false acceptance rate (FAR)	Performance is low due to invertible method	Kong et al. (2006), Teoh et al. (2006), Meetei and Begum (2016)
ECC	Required small key size for encryption	Implementation complexity is more	Abid et al. (2010)
Steganography	Good for hiding password/key	Only useful for hiding small message	Choudhury et al. (2016)
Fuzzy Commitment/Vault	Easily handles intra class variablity	Image alignment is required	Yang et al. (2018a)
Hill Cipher	Simple for implementation, high speed, high throughput	Easily broken with Known Plaintext Attack (KPA)	Kaur and Khanna (2017b)
Cartesian/Polar transform	Non invertible technique	A small change in original minutiae produces large deviation in minutiae position	Patel et al. (2015)
Hadamard	Required low computional cost and storage	Compression performance is very poor	Wang and Hu (2013)
Filter based	Alignment free technique	Time complexity is more	Savvides et al. (2004)
Hybrid	More secure due to combination of multiple methods together	High space and time compexity	Ghany et al. (2012)
Multimodal	Low FAR, high reliability, accuracy, security, resistant for spoof attacks	Costly and no standarization till date	Paul and Gavrilova (2012)
CaSS	Hybrid based approach	Time complexity is high due to use of many phases for final output	Wong et al. (2014)
Bio Convolving	Transformed template remains in same domain as origiinal template	Results good in multi Biometric scenerio	Maiorana et al. (2011)
Salting	Easy to implement only random pattern is to be added	Difficult to know quantity of noise, by simply subtraction we can obtain original Biometric	Pillai et al. (2010)
Deep learning	Featue extraction becomes less time consuming	Lots of data and high graphical processing units (GPUs) are required	Talreja et al. (2017)
Look up table	Reverse mapping is difficult due to many to one mapping of bits	With all enteries 0 in a row have risk to privacy invasion	Dwivedi and Dey (2015)

Table 1 continued

Technique name	Advantages	Disadvantages	References
Image water marking	Mostly used for providing restriction on sharing of images	Cannot place large watermark on image	Barbier et al. (2015)
BIN-COMBO	Less information required for recognition	Required good quality of Iris images	Pillai et al. (2010)
Modulo based	Random permutation with many to one bit mapping is used	Performance is low in comparison with other methods	Prasad et al. (2017)
Noise Embedding	Salting based approach	Difficult to know amount of random noise, which is to be added	Lee et al. (2018)

Table 2 Acroynms used in paper

AUC	Area Under Curve	GER	Genuine Error Rate
BCH	Bose–Chaudhuri–Hocquenghem	HTER	Half Total Error Rate
BEP	Break Even Point	IFOH	Indexing First Order Hashing
CER	Crossover Rate	IoMH	Index of Max Hashing
CBS	Cancelable Biometric System	KPCA	Kernel Principal Component Analysis
CaSS	Cancelable Secure Sketch	LSH	Locality Sensitive Hashing
CC	Co-relational Cofficient	MLC	Multi Line COde
DET	Detection Error Rate	PSR	Peak to Sidelobe Ratio
DCT	Discrete Cosine Transform	RS	Reed Solomon
DI	Decidability Index	RP-PCA	Random Permutated Principal Component Analysis
EER	Equal Error Rate	RR	Recognition Rate
EPC	Expected Performance Curve	ROC	Receiver Operating Characteristics
ECC	Eliptic Curve Cryptography	RP-2DPCA	Random Permuted Two Dimensional PCA
FRR	False Rejection Rate	RRP	Reduced Random Projection
FMR	False Match Rate	RP	Random Projection
FNMR	False Non Match Rate	SRAM	Static Random Access Memory
FTC	Failure To Capture	SRP	Sector Random Projection
FTE	Failure To Enroll	SS	Secure Sketch
FP	False Positive	TAR	True Acceptance Rate
FTC	Failure to Capture	TP	True Positive
FPR	False Positive Rate	TN	True Negative
FNR	False Negative Rate	TRN	Tokenized Random Number
FN	False Negative	VSS	Visual Secret Sharing
FTA	Failure to Acquire	WER	Weighted Error Rate
GAR	Genuine Accept Rate		

imposter and True Positive (TP) represents authentic user. Total imposter score and total genuine scores are represented by FP + TN and TP + FN respectively.

- *Failure to Acquire Rate (FTAR) or Failure to Capture Rate (FTCR)* is defined as number of times a Biometric device fails to capture Biometric sample when presented to the sensor. This error generally occurs when the device is not able to locate a Biometric signal e.g. an extremely fade fingerprint cannot be correctly capture by sensor device.
- *False Accept Rate (FAR)/False Positive Rate (FPR)* is defined as the fraction of impostor scores exceeding the threshold η. It can also be defined in terms of FMR and FTA rate as mentioned in below equation. FMR becomes equal to FAR when a single attempt is made by the user to match in a Biometric system against its own stored template.

$$FAR/FPR = \frac{FP}{FP + TN} \tag{10}$$

$$FAR = FPR = FMR * (1 - FTA) \tag{11}$$

- *False Reject Rate (FRR)/ False Negative Rate(FNR)* is defined as the fraction of genuine user score less than threshold η. FRR is an empirical estimate of the probability at which the system incorrectly rejects identity of the genuine user. FNMR becomes equal to FRR

when a single attempt is made by the user to match in a Biometric system against its own stored template.

$$FRR/FNR = \frac{FN}{TP + FN} \tag{12}$$

$$FRR/FNR = FTA + FNMR * (1 - FTA) \tag{13}$$

- *Equal Error Rate (EER)/Crossover Error Rate (CER)/Break Even Point (BEP)* is the rate at which FAR is equal to FRR.
- *True Acceptance Rate (TAR) or Genuine Accept Rate (GAR)* is defined in terms of FRR as follows:

$$TAR = 1 - FRR \tag{14}$$

- *Half Total Error Rate (HTER)* is defined as the average of *FNMR* and *FMR* i.e.

$$HTER = \frac{FNMR + FMR}{2} \tag{15}$$

- *Failure to Enroll rate (FTE)* is defined as, number of users that cannot be successfully enrolled in a Biometric system. Users should facilitate with good training for interacting Biometric system.
- *d-prime value* (d')*/Separablility/Decidabilty Index (DI)* measures the separation between the means of the genuine and impostor probability distributions in standard deviation units and is defined as

$$d' = \frac{\sqrt{2}|\mu_(genuine) - \mu_(imposter)|}{\sqrt{\sigma^2_{genuine} + \sigma^2_{imposter}}} \tag{16}$$

Here μ and σ are the means and standard deviations of the genuine and impostor distributions respectively. A higher d-prime value indicates better performance.

- *F-Ratio* (F_r) is defined as the ratio between means and standard deviations of impostor and genuine user score as follows:

$$F_r = \frac{|\mu_{genuine} - \mu_{imposter}|}{\sigma_{genuine} + \sigma_{imposter}} \tag{17}$$

Here μ and σ are the means and standard deviations of the genuine and impostor distributions respectively.

- *Receiver Operating Characteristic (ROC)* plots FNMR along Y-axis versus FMR in the X-axis, or FRR versus FAR. Alternatively, TAR versus FAR graph is plotted.
- *Detection Error Trade-off (DET) Curve* is similar to an ROC curve except that the axes are often scaled non-linearly to highlight the region of error rates of interest. Commonly used scales include normal deviate scale and logarithmic scale.
- *Expected Performance Curve (EPC)* shows the expected or reachable performance of a model. EPC generally shows the regions where two models are different from each other.
- *Co-relational cofficient (CC)*: In Cancelable Biometric, we can generate different Cancelable templates of same Biometric by changing its tranformation function (key matrix). Templates so generated should not co-relate with each other. Co-relation generally means the amount of mutual information between two templates (Kaur and Khanna 2017b).

$$C_r(T1, T2) = \frac{\sum\sum(T1 - \bar{T1})(T2 - \bar{T2})}{\sqrt{(T1 - \bar{T1})^2 + (T2 - \bar{T2})^2}} \tag{18}$$

Here $\bar{T1}, \bar{T2}$ represents the mean of templates T1, T2 respectively. C_r is calculated from 10 different templates generated for each user and finally co-relation is calculated between every transformed pair. Lower the value of C_r signifies better performance of any Cancelable Biometric

– *Co-relation Index (CI)*: Mean of Co-relational coefficient (C_r) values over a database is defined as Co-relation index (*CI*), which determines the percentage of mutual information content.

$$CI = \frac{1}{N}\sum_{i=1}^{N} C_r \tag{19}$$

Here, N is the total number of samples in database.

– *Efficiency*: The Efficiency of generating accurate matches before and after transformation can be determined as Belguechi et al. (2011a) :

$$efficiency = 1 - \frac{AUC(FAR_T, FRR_T)}{AUC(FRA_0, FRR_0)} \tag{20}$$

where AUC represents Area under ROC, FAR_O and FAR_T represent False Accept Rates in original and transformed domain, and FRR_O and FRR_T represent False Reject Rates in original and transformed domain respectively. Positive value for efficiency denotes increase in performance, while negative value indicates its regression.

– *Diversity*: Multiple transformed templates are generated for same user by only changing key/helper data (Kaur and Khanna 2017b). However, these transformed templates must not correlate to reveal any information about the original template. To determine, if an attacker can obtain any information about the original template, the mutual information content between any two transformed templates X and Y is calculated as

$$I(X, Y) = \sum_{x}\sum_{y} P(x, y) \log \frac{P(x, y)}{P(x)P(y)} \tag{21}$$

where P is the probability estimation function. Here $P(x)$ and $P(y)$ denotes marginal probabilities and $P(x, y)$ denotes joint probability of x and y. Diversity is measured by computing the mean of the highest value of mutual information for various transformed templates as

$$D = \frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M} max(I(f(b_i^0), f(b_i^{j'}))) \tag{22}$$

where $b_i^{j'}$ denotes the jth test data of ith individual in the database, N is the number of samples in database, and M is the number of transformed templates for each individual.

– *Template Capacity (T)*: Number of templates that can reside in the database at one time.

A summary of performance measures for verification employed by various researchers is given in Table 3 (Fig 12). It can be readily observed that FAR/FMR is the most popular performance measure followed by FRR/FNMR, EER and GAR respectively. Besides, some research works have used other performance measures for verification such as Raja et al. (2018a), Raja et al. (2018b), Rathgeb and Busch (2013) and Rathgeb et al. (2015b) used GMR. Sandhya and Prasad (2015) and Sandhya and Prasad (2016) used D' PRIME. Bissessar et al. (2012), Drozdowski et al. (2018) used DET and GER. Punithavathi and Geetha (2016), Kaur and Khanna (2017b) and Kaur and Khanna (2019) used DI. Kim and Toh (2007) used

Table 3 Performance measures used in literature for verification

References	EER	FAR/FMR	FRR/FNMR	GAR
Ratha et al. (2001)	√	√	√	
Savvides et al. (2004)		√	√	
Ratha et al. (2006)		√	√	
Jeong et al. (2006)	√	√	√	
Teoh et al. (2006)	√	√	√	
Boult (2006)	√			
Ratha et al. (2007)		√		√
Teoh and Yuang (2007)	√	√	√	
Lee et al. (2007)	√			
Farooq et al. (2007)	√	√	√	
Teoh and Yuang (2007)	√	√	√	
Kim and Toh (2007)	√	√	√	
Toh et al. (2007)	√	√	√	
Boult et al. (2007)	√	√		
Thomas et al. (2008)		√	√	
Maiorana et al. (2008)	√	√	√	
Zuo et al. (2008)		√		
Chikkerur et al. (2008)		√		√
Aggarwal et al. (2008)		√	√	
Kim and Toh (2008)	√	√	√	
Tan et al. (2009)	√	√	√	
Karabat and Erdogan (2009a)	√			
Xu and Li (2009)		√		√
Bringer et al. (2009)		√		√
Kanade et al. (2009)	√	√	√	
Takahashi and Hitachi (2009)		√	√	
Yang et al. (2009)	√	√		√
Kelkboom et al. (2009)	√	√	√	
Maiorana et al. (2009)	√	√	√	
Xu and Wang (b)		√		√
Maiorana et al. (2010)	√	√	√	
Wang and Hatzinakos (2010)	√	√	√	√
Leng et al. (2010)		√	√	√
Ahmad and Hu (2010)	√	√	√	
Kanade et al. (2010)		√	√	
Kelkboom et al. (2010)	√	√	√	
Abid et al. (2010)		√	√	
Yang et al. (2010)	√	√		√
Rathgeb and Uhl (2011)	√	√	√	
Jenisch and Uhl (2011)	√	√	√	
Belguechi et al. (2011a)	√	√	√	
Pillai et al. (2011)		√		

Table 3 continued

References	EER	FAR/FMR	FRR/FNMR	GAR
Chin et al. (2011)	√	√	√	
Maiorana et al. (2011)	√	√	√	
Zhu et al. (2011)		√	√	
Ouda et al. (2011)		√		√
Belguechi et al. (2011b)	√	√	√	
Nishiuchi and Soya (2011)		√	√	
Zhu et al. (2012)		√	√	
Bissessar et al. (2012)		√	√	
Oh and Toh (2012)	√	√	√	
Paul and Gavrilova (2012)		√	√	√
Leng and Zhang (2012)		√		√
Leng et al. (2012)	√	√		√
Paul and Gavrilova (2013a)		√		√
Zhang et al. (2013)	√	√	√	
Wang and Hu (2013)	√	√	√	√
Rathgeb et al. (2013)	√	√	√	
Dey et al. (2013)	√	√	√	
Rathgeb and Busch (2013)	√	√		
Leng et al. (2013a)	√			
Paul and Gavrilova (2013b)		√	√	√
Wong et al. (2014)	√	√	√	
Chen et al. (2014)		√		√
Hämmerle-Uhl et al. (2013)	√			
Izu et al. (2014)		√	√	
Sui et al. (2014)	√	√	√	
Leng et al. (2014b)	√	√	√	
Bhatega and Sharma (2014)		√	√	
Bringer et al. (2014)		√	√	
Dwivedi and Dey (2015)	√	√	√	
Barbier et al. (2015)	√			
Sandhya and Prasad (2015)	√	√	√	
Rathgeb et al. (2015b)	√			
Suresh and Radhika (2015)		√	√	
Meetei and Begum (2016)	√	√	√	
Sree and Radha (2016)		√	√	√
Choudhury et al. (2016)	√			
Punithavathi and Geetha (2016)	√	√	√	
Rathgeb et al. (2015a)	√	√	√	
You et al. (2017)	√	√		√
Kim et al. (2017)	√	√		
Prasad et al. (2017)	√	√	√	√

Table 3 continued

References	EER	FAR/FMR	FRR/FNMR	GAR
Sandhya and Prasad (2016)	√	√	√	
Kaur and Khanna (2017b)	√	√	√	
Popa and Simion (2017)		√	√	√
Talreja et al. (2017)		√		√
Deshmukh and Balwant (2017)	√	√	√	√
Jin et al. (2018)	√	√	√	
Ali and Tahir (2018)		√	√	
Mtibaa et al. (2018)	√			
Kaur and Khanna (2019)	√	√	√	
Arjona et al. (2018)	√	√	√	
Thomas et al. (2008)	√	√	√	
Raja et al. (2018a)	√	√	√	
Raja et al. (2018b)	√	√	√	
Lee et al. (2018)	√	√	√	
Drozdowski et al. (2018)	√			
Kim and Teoh (2018)	√	√	√	
Total	66	89	70	23

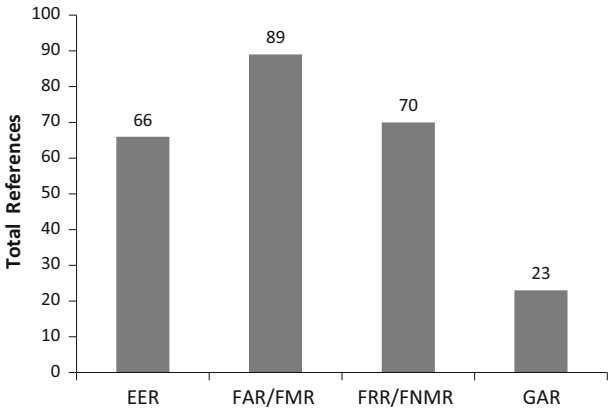

Fig. 12 Bar graph corresponding to Table 3

TER, Belguechi et al. (2011a) used Diversity and Efficiency. Nishiuchi and Soya (2011) and Leng et al. (2013b) used Co-relational Cofficient as their model performance measures. Thomas et al. (2008) used ROC curve (*ROC*).

3.2 Performance measures for identification

A summary of performance measures for Identification employed by various researchers is given in Table 4. These papers includes various measures such as Recognition rate/Identification rate, Rank, Classification accuracy. In comparison with papers who used

Table 4 Performance measures for identification

References	Performance measures
Xu et al. (2008)	Accuracy
Pillai et al. (2010)	Recognition Rate
Patel et al. (2010)	Recognition Rate
Lingli and Jianghuang (2010)	Recognition Rate
Prasanalakshmi and Kannammal (2010)	Accuracy
Pillai et al. (2011)	Recognition Rate
Takahashi and Naganuma (2012)	Accuracy
Paul and Gavrilova (2013a)	Classification Accuracy
Paul et al. (2013)	Classification Accuracy
Paul and Gavrilova (2014b)	Rank k
Nazari et al. (2014)	Recognition Accuracy
Tams and Rathgeb (2014)	Accuracy, Identification Rate, Rank
Chen et al. (2014)	Recognition Rate, Rank.
Bommagani et al. (2014)	Identification Rate, Rank
Saito et al. (2016)	Recognition Rate, Accuracy
Choudhury et al. (2016)	Accuracy
Issac et al. (2017)	Accuracy
Jiménez and Raj (2017)	Accuracy
Punithavathi et al. (2017)	Accuracy
Chen et al. (2017)	Recognition Rate, Training & Testing time
Kumar et al. (2018)	Classification Accuracy
Wu et al. (2018)	Identification Rate, Training & Testing time
Drozdowski et al. (2018)	Identification Rate

Verification's performance measures, identification's measure count is low. Researcher generally used Identification/Recognition Rate, Accuracy, Classification Accuracy, Training Time, Testing Time as performance measures for Identification.

- *Identification Rate or Recognition Rate*: The identification rate is an estimate of the probability that a subject is identified correctly at least at rank-k.
- *Accuracy*: It is ratio between True cases (both True Positive and True Negative) to all possible cases.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{23}$$

- *Classification Accuracy*: The classification accuracy A_i of an individual program i depends on the number of samples correctly classified (true positives plus true negatives) and is evaluated by the formula:

$$A_i = \frac{t}{n} * 100 \tag{24}$$

where t is the number of sample cases correctly classified, and n is the total number of sample cases.

Table 5 References who didn't use any performance measure for cancelable biometrics

References
Lalithamani and Soman (2009b)
Lalithamani and Soman (2009a)
Sarier (2010)
Takahashi and Hirata (2011b)
Chandra and Kanagalakshmi (2011)
Egner et al. (2012)
Andalib and Abdulla-Al-Shami (2013)
Othman and Ross (2013)
Ueshige and Sakurai (2014)
Batool et al. (2015)
Khodabacchus et al. (2016)
Rachapalli and Kalluri (2017)
Sarkar and Singh (2017)

– *Training Time*: The process of training an model involves providing learning algorithm or model with training data to learn from.
– *Testing Time*: The process of testing an model involves testing a learning algorithm or model with testing data.

3.3 Other performance measures

During our research, we studied that some researcher use specific performance measure for their research work e.g. Savvides et al. (2004) used Peak to sidelobe ratio(PSR), which is the ratio between peak mean to the standard deviation. where mean and standard deviation are calculated in an angular region centered at the peak. Quan et al. (2008) used equations of mixture of Gaussian kernels and electric potential field to generate Cancelable Fingerprint template. The performance is totally based on, how quickly intruder can find the values of variables used in these equations. Leng and Zhang (2012) generates Cancelable Palmprint templates. In this, for enhancing the performance of Palmhash code, Gaussian valued PRN is used instead of Palmhash code with three valued PRN. We also observed that some researcher didn't use any performance measure for their research work. Majority of these work include Cloud based technique for storage of Cancelable Biometric template and stable Key generation technique from noisy Biometric data. Table 5 listed research works, who didn't use any performance measures.

4 Attacks on Cancelable Biometrics

Various attacks are possible on Cancelable Biometric system i.e. sensor level, application level and database level. Paul et al. (2013) have discussed various attack point situations. In one situation, when system becomes aware that some intruder attempt to access the system, then it can change the intermediate transformation function and generate some wrong templates. In second situaion, system will block that account and later on when the genuine user tries to access the account, he will get some alert message about his credential, and finally a new

template will be issued to the genuine user. we have studied various types of attacks existed in literature viz. Brute force, Attack via Multiplicity, Lost token, Dictionary based, Spoofing, Intrusion, Cryptanalysis, Hill climbing, Inverse and Pre-image attack etc.

In *Brute force attack*, an intruder tries various combination of password/key to log into the system. An intruder has no infomation about the genuine user. If an intruder tried to stole m bits BioHash key, then he/she has to check all 2^m combination to guess the actual key/password. so its computational complexity is high. In Mtibaa et al. (2018), system has the threshold value 0.012 and binary vector of 1024 bits in length. If an adversary tries to guess the correct binary vector by Brute force attack, its guessing complexity will take $2^{1024} * (1 - 0.012)$ number of attempts. As in Cancelable Biometric, we can generate multiple templates from the same user Biometric by only changing some key parameter or transformation functions. In *Attack via Record Multiplicity attack*, an intruder tried to find Co-relation among multiple encoded templates created from the same Biometric for accessing the original template and the secrets.

In *Lost token attack or smart attack or Stolen key attack*, an intruder knows some information such as token/password of user. He/She will try to apply this token on his/her own Biometric for getting estimated original template. suppose if m features are there so intruder must attempt $m!$ permutation of these features with 2^m computational complexity (Nazari et al. 2014). In *Dictionary based attack*, intruder tries only those samples that are deemed most likely to succeed. In *Spoofing attacks* intruder will use artificial fingers, recorded videos, contact lenses at sensor device. In *Doppelganger threat*, compromised databases which consists of millions users will permit an intruder to access close matches they can directly imitate. In *Intrusion attack*, when an intruder gets succeed in accessing templates stored in database then by reverse engineering process he/she will try to generate physical clone of stolen template.

In *Privacy violation attack*, an intruder uses compromised templates of genuine user to log into other applications/systems. *Cryptanalysis* is the study of the Cipher text. In *Cryptanalysis attack*, attacker tries to find Plain text from the Cipher text without the knowledge by which algorithms and functions these encryption are performed. In *Stolen Biometric feature attack*, stolen features of the genuine users are tried with the various key combination to log into the systems/ applications. In *Hill climbing attack*, no prior information about the user is known. Iteratively synthetic templates of the user's Biometric submitted at the matcher untill the successful recognition. In each attempt, the data is modified on the basis of previous attempt result. Prasad et al. (2017) explain Hill climbing attack for iris codes. In *Inverse attack*, number of transformed features mapped onto original arrays for every reference position (Sandhya and Prasad 2016).

Pre-image attack on a Biometric system tries to find closely similar Biometric samples to spoof. This attack can be easily computed through a Brute force attack, whose computational complexity is of order $O(2^n)$ for an n bit hash. *Cipher text only Attack (COA)*, is a well known attack in the Symmetric key cryptosystem where intruder tried to restore the Plain text from Cipher text. While in *Known Plaintext Attack (KPA)*, an adversary has accessed to both Plain text and Cipher text. These can be used to reveal further secret information such as Crypto keys. In *Chosen Ciphertext Attack (CCA)*, an adversary can gather information of secret key or transformation key by decrypting the chosen Cipher texts. In *Equation attack*, different equations have some parametric variables for generating templates. If these variables values are guessed by the attacker then he/she will easily cracked the transformed templates (Table 6).

Table 6 Various attacks on cancelable biometric system

Attack	Description	Type of attack	Requirement	References
Brute force	Without having much information about the authorized user, intruder tried all password/key combination to log into the system	Key based	For n bit, 2^n combinations are computed	Lee et al. (2007), Nazari et al. (2014), Mtibaa et al. (2018)
Attack via Record Multiplicity	Calculate existence of co-relation between the various templates generated from the same Biometric/user	Database level	Calculated in Eq. 18 in Sect. 3.1	Kaur and Khanna (2019), Kaur and Khanna (2017b)
Lost token or Stolen key	Intruder has information such as password/key then he/she will try this password/key to his/her Biometric features to gain estimation of original template	forgery level	For m features, $m!$ feature permutation with 2^m computational complexity	Nazari et al. (2014)
Dictionary based	Intruder only tries those samples that are most likely to succeed, disgarding the rest	Database level	n selected samples	Wu et al. (2018)
Spoofing	Forgery like artifical Fingerprint or clone features of Fingers, Iris, Palmprint, Palmvein presented at sensor site	Sensor level	Liveness detection can somehow solve this issue	Popa and Simion (2017)
Doppelganger	Compromised databases which consists of millions of users will permit an intruder to access close matches they can directly imitate	Database level	Database access	Boult et al. (2007)
Intrusion	After accessing database, generating original physical clone of stolen template by reverse engineering process	Invertible transformation level	Database access	Rachapalli and Kalluri (2017)
Privacy violation attack	Use of genuine user's stolen template in other applications by cross matching	Application level	Database access	Rachapalli and Kalluri (2017)
Cryptanalysis	Getting plain text from cipher text without knowing which transformation or cryptography function is used for encryption	Crypto-graphy	Cipher text known	Rachapalli and Kalluri (2017)

Table 6 continued

Attack	Description	Type of attack	Requirement	References
Stolen Biometric feature	Stolen features of genuine users are tried with the various key combination to access system or applications	Sensor level	Features accessed	Mtibaa et al. (2018)
Hill climbing	Synthetic templates submitted to the matcher untill successful recognition	Matcher level	Feature updation	Sandhya and Prasad (2016)
Inverse	Number of transformed features reverse mapped onto the arrays for changes in corresponding position	Invertible transformation level	Mapping function	Sandhya and Prasad (2016)
Pre-image	A Biometric system tries to find similar Biometric samples to spoof it. The most common way to find a Pre-image is by Brute force attack	Key based	For an n bit hash computational complexity of order $O(2^n)$ BioHashing suffers from this	Wu et al. (2018)
Cipher text Only (COA)	An intruder attempts to get plain text from the cipher text	Crypto-graphy	Cipher text	Kim and Teoh (2018)
Known Plaintext (KPA)	Both plain text and cipher text known to the intruder to get the secret key information	Crypto-graphy	both plaintext and cipher text	Kim and Teoh (2018)
Chosen Ciphertext (CCA)	From ciphertext information about secret key is reterived	Crypto-graphy	Cipher text	Kim and Teoh (2018)
Equation	Equations with some parametric variables are used for generating templates. By giving various solutions to these variables intruder can get access to original template	transform-ation level	Guessed parametric variables values	Quan et al. (2008)

5 Databases used in Cancelable Biometrics

When an algorithm is compared with other algorithms, we require a standard set of images. Several researchers have put efforts in developing various set of images called Databases. The performance of Cancelable Biometric algorithms are tested on a large variety of databases. Here, we provide a comprehensive review of databases used by various researchers in Cancelable Biometric recognition as listed in Table 7 (Figs. 13, 14, 15, 16).

5.1 Face databases

5.1.1 CMU PIE

The PIE (pose, illumination, expression) database formed at Carnegie Mellon University(CMU) in the year 2000 with 13 different pose, 43 different illumination conditions and 4 different expressions. It consists with 41,368 images of 68 persons under various conditions. The main drawback of this database is that limited number of persons taken for images under a single recording session with few expressions.

5.1.2 CMU multi PIE

The CMU Multi PIE database overcome the problem arises with CMU PIE. This database contains 750,000 images of 337 persons. Database consists of high resolution color images in two formats viz. JPG(joint photographic group for high resolution images) or PNG (portable network group for multi view images). Images have been taken under 15 view points and 19 illumination conditions with different facial expression, which require 305 GB space for storage.

5.1.3 AR

This Database formed by **A**leix Martinez and **R**obert Benavente. Images in this database includes facial expression, illumination, and occlusion. Database consists with more than 4000 images of 126 peoples among which, 70 male and 56 female are included. Each image has the size of 768×576 pixels.

5.1.4 FERET

Facial Recognition Technology database was collected in 15 sessions and 1564 sets. This database contains color 14126 images of 1199 peoples. Two facial, two illumination and between 9 and 20 pose variation are taken during formation of this database. To maintain consistency, whole database formed under same environment and physical setup condition.

5.1.5 BERC

The BERC database was formed by Bio-metrics Engineering Research Center. Database consist with 5238 images of 390 subjects in the age group of 3 to 83 years. Images are of very high resolution 3648×2736 pixels compare with all other database. Images are taken under same light, facial expression, illumination and occlusion with/without glasses.

Table 7 Databases used in cancelable biometric

Biometric	Database	No. of identities	Total No. of images	Resolution	Image format	References
Face	CMU Multi PIE	337	750,000	640 × 486	.jpg & .png	Savvides et al. (2004)
	AR	126	4,000	768 × 576	.jpg	Kong et al. (2006), Kim and Toh (2007)
	FERET	1199	14,126	181 × 241	RGB	Teoh et al. (2006), Teoh and Yuang (2007), Paul and Gavrilova (2013a), Paul et al. (2013), Paul and Gavrilova (2014a), Paul and Gavrilova (2014b)
	BERC	390	5238	3648 × 2736	.jpeg	Kim and Toh (2007)
Face	ORL(AT&T)	40	400	92 × 112	.pgm	Teoh and Yuang (2007), Nazari et al. (2014)
	FRGC	465	4007	1200 × 1600	.jpeg	Chikkerur et al. (2008) , Kelkboom et al. (2009)
	M2VTS	37	185	286 × 350	.pgm	Karabat and Erdogan (2009a), Punithavathi et al. (2017)
	XM2VTSDB	295	2360	576 × 720	.jpg	Bommagani et al. (2014)
	VALID	106	530	720 × 576	.jpeg	Chen et al. (2014)
	Yale	15	165	320 × 243	.pgm	Lingli and Jianghuang (2010)
Iris	IIT Delhi	224	1120	320 × 240	.bmp	Punithavathi et al. (2017)
	CASIA Ver1	108	756	320 × 280	.bmp	Tan et al. (2009), Rathgeb and Uhl (2011), Sui et al. (2014), Punithavathi et al. (2017)
	CASIA Ver2	60	1200	640 × 480	.bmp	Kanade et al. (2009)
	CASIA Ver3	700	22034	640 × 480	.jpeg	Rathgeb and Uhl (2011), Rathgeb et al. (2013), Sui et al. (2014)
	NIST-ICE	244	2953	480 × 640	.jpeg	Kanade et al. (2009)
	CBS	244	2953	640 × 240	.bmp	Kanade et al. (2009), Yang et al. (2009)

Table 7 continued

Biometric	Database	No. of identities	Total No. of images	Resolution	Image format	References
Speech	TIMIT	630	6300	16 bit 16 kHz	.wav	Mtibaa et al. (2018)
	VidTIMIT	43	430	16 bit 32 kHz	.wav	Hämmerle-Uhl et al. (2013), Paul et al. (2013), Paul and Gavrilova (2014a), Paul and Gavrilova (2014b)
Fingerprint	FVC 2002	110	800	500 dpi	.tif	Quan et al. (2008), Lee et al. (2007), Xu and Li (2009), Wang and Hu (2013)
	IBM-99	188	376	512 dpi	NA	Ratha et al. (2007), Thomas et al. (2008)
Signature	MCYT	330	16500	300 × 300	.jpeg	Maiorana et al. (2008)
Palmprint	PolyU	100	600	384 × 284	.bmp	Leng et al. (2013b), Leng et al. (2014b), Chen et al. (2014)
ECG	PTB	290	549	2000 A/D units/mV	.dat	Kim et al. (2017)
Palmvein	MU	136	2720	480 × 680	NA	Leng et al. (2013a)
Fingervein	FV-HMTD	106	636	320 × 240	NA	Yang et al. (2018b)

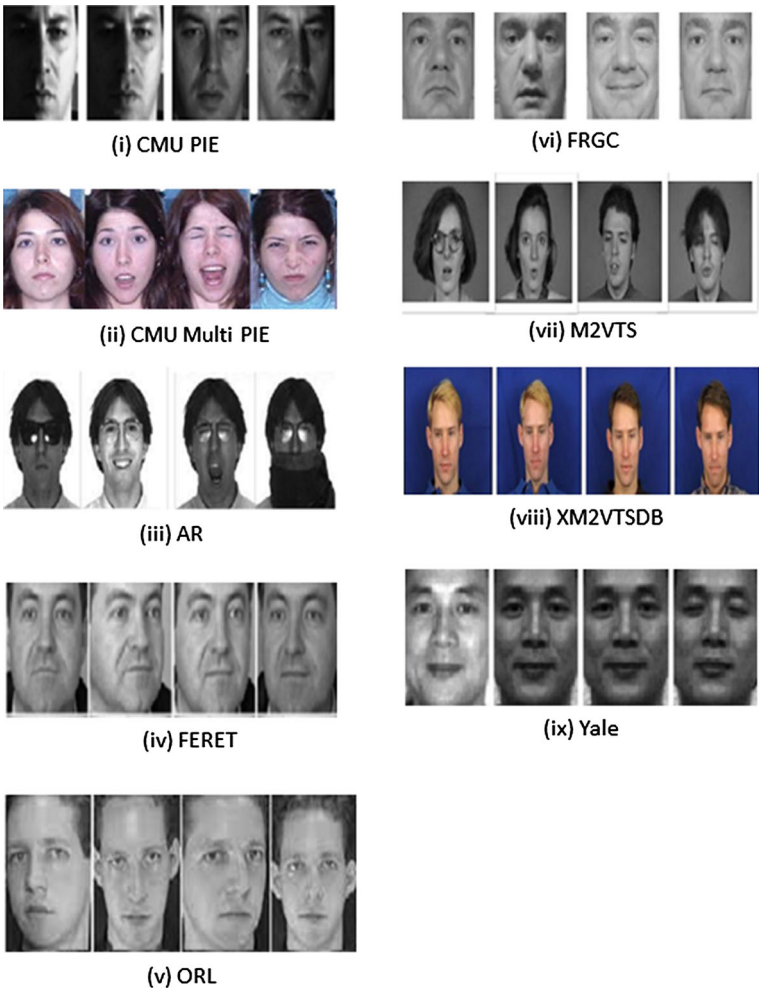

Fig. 13 Face databases sample images

5.1.6 ORL

This database formed at Olivetti Research Laboratory formerly named as American Telephone & Telegraph Company. This database contains 400 images of 40 subjects with resolution of 92 × 112. Some people imaged at different times and with variation in facial expression eg. by changing the lighting, with open and closed eyes, with/ without smiling, presence/absence of glasses.

5.1.7 FRGC

Face Recognition Grand Challenge database consists 4007 images of 465 subjects either with 1704 × 2272 pixels or 1200 × 1600 pixels resolution. In this database images are of high

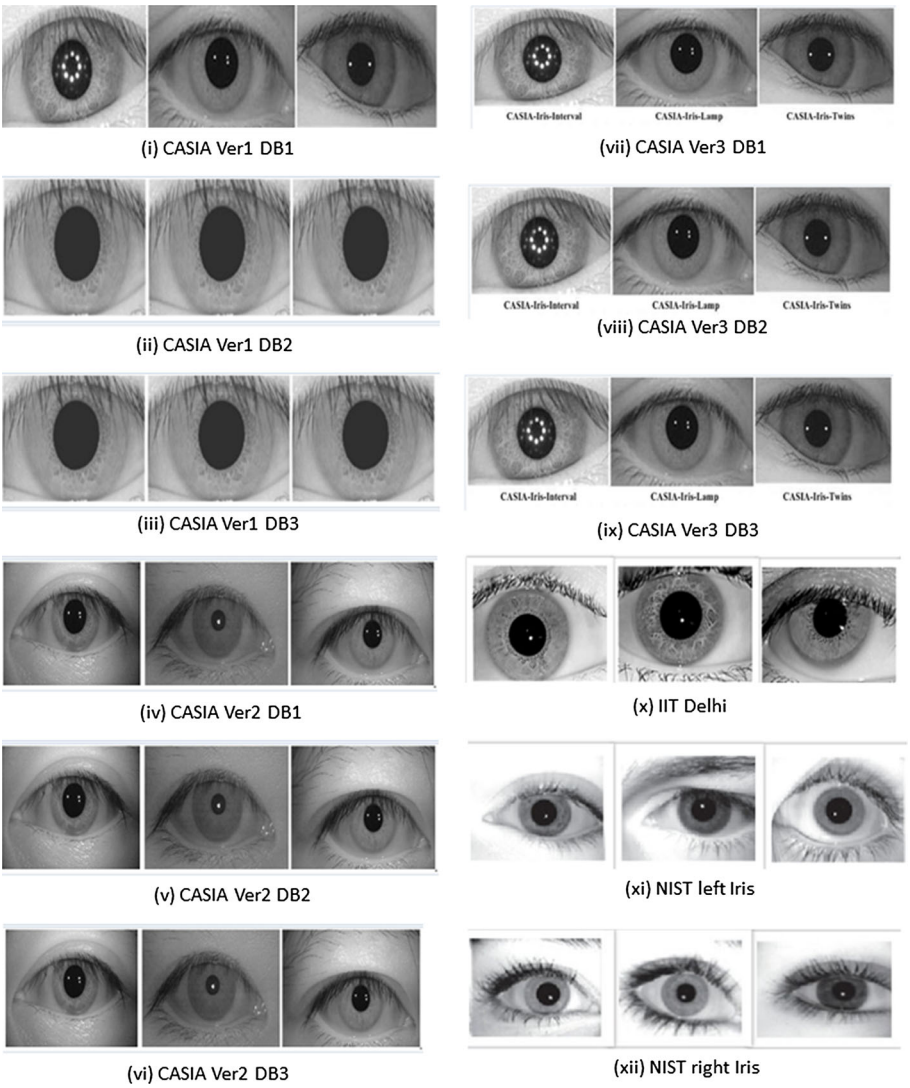

Fig. 14 CASIA, IIT Delhi, NIST Iris databases sample images

MCYT Signature

Section ID	Sentence ID	Sentence text
Session 1	sa1	She had your dark suit in greasy wash water all year
	sa2	Don't ask me to carry an oily rag like that
	si1398	Do they make class-biased decisions?
	si2028	He took his mask from his forehead and threw it, unexpectedly, across the deck
	si768	Make lid for sugar bowl the same as jar lids, omitting design disk
	sx138	The clumsy customer spilled some expensive perfume
Session 2	sx228	The viewpoint overlooked the ocean
	sx318	Please dig my potatoes up before frost
Session 3	sx408	I'd ride the subway, but I haven't enough change
	sx48	Grandmother outgrew her upbringing in petticoats

Sentences used in VidTIMIT

Fig. 15 MCYT Signatures, VidTIMIT speech sentences sample images

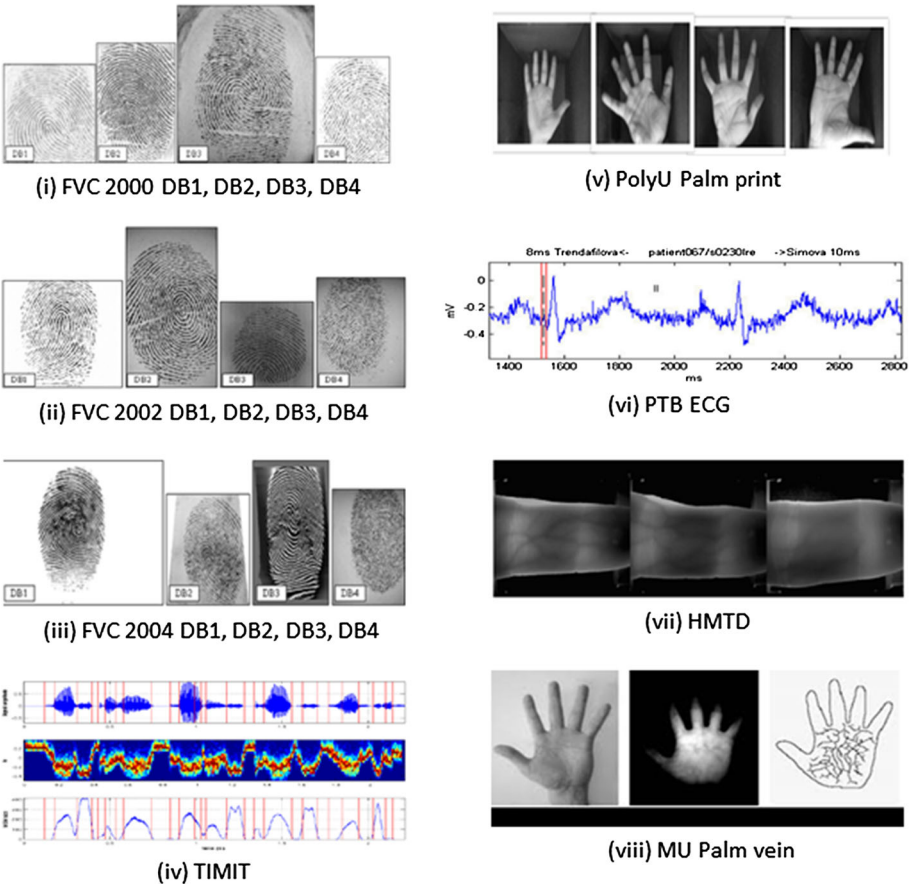

Fig. 16 FVC 2000, 2002, 2004 Fingerprint, TIMIT Speech, PolyU Palm print, PTB ECG, HMTD, MU Palm vein databases sample images

resolution, with 3D face recognition and new preprocessing techniques. each image can have size between 1.2 MB to 3.1 MB.

5.1.8 M2VTS

Multi Modal Verification for Teleservices and Security database consists of 185 images of 37 peoples (5 images/person). During imaged on each shot people have been asked to count from '0' to '9' in their native language and head rotation from 0 to -90 and 0 to $+90$ degrees.

5.1.9 XM2VTSDB

Extended M2VTS Multimodal Database contains 2360 images of 295 subjects with 576×720 pixels resolution. Peoples are imaged while rotating head and speaking head shot. This database contains video sequences, 3D model and 32 KHz 16-bit sound files.

5.1.10 VALID

VALID is also a multi modal database, which consists of 530 images of 106 subjects(5 images per subject) with 720 × 576 pixels resolution. Some Images are taken in real office scenario with no noise, rest are in different illumination and with acoustic noise.

5.1.11 Yale

Yale database contains total of 165 grayscale images of 15 individuals with 320 × 243 pixels resolution. In this database 11 images per person is taken under different facial expression for eg. happy, sad, sleepy. surprised and with/without glasses.

5.2 Iris databases

5.2.1 IIT Delhi

Indian Institute of Technology Iris Database collected at Biometrics Research Laboratory in year 2007. This database contains total of 1120 images of 224 subjects including 176 males and 48 females. Database images are of resolution 320 × 240 pixels taken from students and staff between age group 14-55 years of IIT Delhi in indoor environment.

5.2.2 CASIA Ver1, Ver2, Ver3

This database named after Centre for Biometrics and Security Research (CBSR) Institute of Automation, at Chinese Academy of Sciences (CASIA), China. This database have three versions. CASIA-IrisV1 consist of 756 images from 108 eyes with a resolution of 320 × 280. CASIA-IrisV2 contains 1200 images of 60 unique subjects with a resolution of 640 × 480. CASIA-IrisV3 consists with 22,035 iris images of more than 700 subjects same resolution of 640 × 480.

5.2.3 NIST ICE

National Institute of Standards and Technology (NIST) for the Iris Challenge Evaluation (ICE) formed by 2,953 images with 480 × 640 pixels resolution of 244 different eyes.

5.2.4 CBS

Casia-BioSecure database is divided into two parts: BioSecureV1 and CasiaV2. This database consists with total of 2953 images of 244 different iris with resolution of 640 × 240 pixels. These images are captured in different session, illumination and with/without spectacles.

5.3 Speech databases

5.3.1 TIMIT

Texas Instruments (TI) Massachusetts Institute of Technology(MIT) database consist of 6300 sentences spoken by 630 speakers (10 samples from each speaker) including 430 males and

192 females. Database consists of 2 dialects of American English, read by 630 speakers, 450 phonetically compact sentences and 1890 phonetically diverse sentences. It also includes orthographic, phonetic and word transcriptions as well as a 16-bit, 16kHz speech waveform file for each utterance.

5.3.2 VidTIMIT

This database contains 43 peoples video and corresponding audio recordings with a total of 430(10 recording/person). This database recorded in 3 sessions, in addition with sentences, people have been asked to rotate their head in sequence(left, right, back to the center, up, then down and finally return to center) in each session. Each person video data is stored in sequence of 512×384 pixels jpeg image. The corresponding audio is stored with 16 bit and 32 kHz wav file.

5.4 Finger databases

5.4.1 FVC

Fingerprint verification competition is an international competition focused on fingerprint verification software assessment. FVC has 3 version FVC2000, FVC2002 and FVC2004 with 4 databases namely DB1, DB2, DB3, DB4 databases. FVC 2002 contains total of 800 images of 110 peoples with 500 dpi each.

5.4.2 IBM-99

International Business Machine optical database contains total of 376 images (188×2) of 188 user's fingerprint pairs, each image with 512 dpi.

5.5 Signature database

5.5.1 MCYT

Ministerio de Ciencia y Tecnologia, Spanish Ministry of Science and Technology MCYT bimodal database consists total of 16500 images of 330 subjects with each image has size of 300×300. They used CMOS-based capacitive capture device and an optical capture device with a resolution of 500 dpi.

5.6 Palmprint database

5.6.1 PolyU

HongKong Polytechnic University (PolyU) Palmprint Version 2 Database consists of 600 grayscale images of 100 users (6 palm images/user), the original image size is 384×284 pixels at 75 dpi. From oriented palmprint, image size of 128×128 is cropped.

5.7 ECG database

5.7.1 PTB

Physikalisch-Technische-Bundesanstalt is a public database contains records of the Frank-lead vectorcardiogram and the standard 12-lead ECGs, sampled at 1000 Hz. Aprox 549 images were collected from 290 subjects.

5.8 Palmvein database

5.8.1 MU

In Multimedia University Palmvein Database images are collected from people residing in various countries such as such as China, Malaysia, India, Africa, and so on. Total of 2720 images were taken of 136 peoples with visible and infrared web cams in contact less environment. About 20 samples were taken from each user (10 images per hand).

5.9 Fingervein database

5.9.1 FV-HMTD

Homologous Multimodal Traits finger-vein database consists of total 636 images of 106 users with 6 images per user (index finger, middle finger and ring finger of both hands). Each image size is of 320×240 pixels.

6 Conclusion and future work

Cancelable Biometrics is an emerging research area. Researchers from different backgrounds such as Cryptography, Machine Learning, Computer Vision, Statistics etc. have come together for solving this interesting problem. However, there is no comprehensive study which enumerates the state of the art methods in Cancelable Biometrics. In this paper, we have presented a comprehensive review of more than 120 methods proposed by various researchers in the past few decades. Further, a novel taxonomy has been developed for classification of these methods into six categories viz. (i) Cryptography based methods (ii) Transformation based methods (iii) Filter based methods (iv) Hybrid methods (v) Multimodal methods (vi) Other methods along with advantages and disadvantages of various techniques under each category. We have also discussed various performance measures used in cancelable biometrics for verification and identification. Furthermore, various security attacks in Cancelable Biometrics and datasets used for variety of biometrics have been described.

Now, we would like to draw the attention of the readers towards future directions in cancelable biometrics. As most of the Cancelable Biometrics result into decreased performance, novel feature extraction methods which can provide enhanced security of cancelable biometric template should be invented for better verification and identification. Further, the computational complexity and storage requirements of these methods must be less, otherwise the real time application of the method may not be feasible. We have also observed that False Accept Rate/False Match Rate, False Reject rate/False Non Match Rate and Equal

Error Rate are the most popular performance measures used in literature. Hence, researchers can focus on proposing new performance measures for verification as well as identification. The security attacks in cancelable biometrics tend to weaken the system. The researchers can look for novel techniques which can either prevent or detect these attacks. Lastly, if the attack is successful, then techniques can be developed for ensuring that the biometric data is not revealed in any manner to the intruders. We have also noticed that datasets of some biometrics such as Signature, Palmprint, ECG, Palmvein are less used. For other Biometrics such as Speech and Fingerprint, only limited number of samples are available in the databases. This puts constraints on the performance testing of methods. hence, the researchers can further explore this direction in future. Recently, deep learning is also employed in Cancelable Biometrics and requires large number of training samples. However, except CMU Multi PIE, there is no large database used in literature. Even, Deep learning itself can be explored for better performance in Cancelable Biometrics. Furthermore, instead of storing the Cancelable Biometric templates in a single database, Cloud storage is also being used for storing Cancelable templates in a distributed manner which is another research direction in this field. Lastly, there may be cases when only single image per person is available. In that case, the development of cancelable template may not be easy. This can be another research direction in Cancelable Biometrics.

Acknowledgements One of the authors Dr. Nitin Kumar is thankful to Uttarakhand State Council of Science and Technology, Dehradun, India for providing financial assistance towards the implementation of Project Sanction No. UCS&T/R&D-05/18-19/15202.

References

Abid M, Kanade S, Petrovska-Delacrétaz D, Dorizzi B, Afifi H (2010) Iris based authentication mechanism for e-passports. In: 2nd International workshop on security and communication networks (IWSCN). IEEE, pp 1–5

Aggarwal G, Ratha NK, Connell JH, Bolle RM (2008) Physics-based revocable face recognition. In: IEEE international conference on acoustics, speech and signal processing. IEEE, pp 5232–5235

Ahmad T, Hu J (2010) Generating Cancelable Biometric templates using a projection line. In: 11th International conference on control automation robotics and vision. IEEE, pp 7–12

Ali MA, Tahir NM (2018) Cancelable Biometrics technique for iris recognition. In: IEEE symposium on computer applications & industrial electronics (ISCAIE). IEEE, pp 434–437

Andalib AS, Abdulla-Al-Shami M (2013) A novel key generation scheme for Biometric cryptosystems using fingerprint minutiae. In: 2nd International conference on informatics, electronics and vision (ICIEV). IEEE, pp 1–6

Arjona R, Prada-Delgad MA, Baturone I, Ross A (2018) Securing minutia cylinder codes for fingerprints through physically unclonable functions: an exploratory study. In: International conference on Biometrics (ICB). IEEE, pp 54–60

Barbier M, Le JM, Rosenberge C (2015) Image watermarking with biometric data for copyright protection. In: 10th International conference on availability, reliability and security (ARES). IEEE, pp 618–625

Batool R, Naveed G, Khan A (2015) Biometric authentication in cloud computing. Int J Comput Appl 129(11):6–9

Belguechi R, Cherrier E, Rosenberger C (2011a) Evaluation of Cancelable Biometric systems: application to finger-knuckle-prints. In: International conference on hand-based biometrics (ICHB). IEEE, pp 1–6

Belguechi R, Le-Goff T, Cherrier E, Rosenberger C (2011b) Study of the robustness of a Cancelable Biometric system. In: Conference on network and information systems security. IEEE, pp 1–7

Belhadj F, Akrouf S (2015) Secure fingerprint-based authentication and non-repudiation services for mobile learning systems. In: International conference on interactive mobile communication technologies and learning (IMCL). IEEE, pp 200–204

Bhatega A, Sharma K (2014) Secure cancelable fingerprint key generation. In: Power India international conference (PIICON) (no. 6). IEEE, pp 1–4

Bissessar D, Gorodnichy DO, Stoianov A, Thieme M (2012) Assessment of privacy enhancing technologies for biometrics. In: Symposium on computational intelligence for security and defence applications. IEEE, pp 1–9

Bolle RM, Connell JH, Ratha NK (2002) Biometric perils and patches. Pattern Recognit 35(12):2727–2738

Bommagani AS, Valenti MC, Ross A (2014) A framework for secure cloud-empowered mobile Biometrics. In: Military communications conference (MILCOM). IEEE, pp 255–261

Boult T (2006) Robust distance measures for face-recognition supporting revocable biometric tokens. In: International conference on automatic face and gesture recognition (FGR06), vol 7. IEEE, pp 560–566

Boult TE, Scheirer WJ, Woodworth R (2007) Revocable fingerprint biotokens: accuracy and security analysis. In: Conference on computer vision and pattern recognition. IEEE, pp 1–8

Bringer J, Chabanne H, Kindarji B (2009) Anonymous identification with cancelable biometrics. In: Proceedings of international symposium on image and signal processing and analysis, vol 6. IEEE, pp 494–499

Bringer J, Chabanne H, Morel C (2014) Shuffling is not sufficient: security analysis of cancelable iris codes based on a secret permutation. In: International joint conference on biometrics (IJCB). IEEE, pp 1–8

Camenisch J, Stadler M (1997) Efficient group signature schemes for large groups. In: Annual international cryptology conference. Springer, Berlin, pp 410–424

Chandra E, Kanagalakshmi K (2011) Cancelable Biometric template generation and protection schemes: a review. In: International conference on electronics computer technology, vol 3(no. 5). IEEE, pp 15–20

Chen X, Zheng L, Liu Z, Zhang J (2014) Privacy-preserving Biometrics using matrix random low-rank approximation approach. In: International symposium on biometrics and security technologies (ISBAST). IEEE, pp 6–12

Chen PT, Wu SC, Hsieh JH (2017) A Cancelable Biometric scheme based on multi-lead ECGs. In: Annual international conference of the engineering in medicine and biology society (EMBC) vol 39. IEEE, pp 3497–3500

Chikkerur S, Ratha NK, Connell JH, Bolle RM (2008) Generating registration-free cancelable fingerprint templates. In: IEEE international conference on biometrics: theory, applications and systems, vol 2. IEEE, pp 1–6

Chin YJ, Ong TS, Teoh AB, Goh MK (2011) Multimodal biometrics based bit extraction method for template security. In: Conference on industrial electronics and applications, vol 6. IEEE, pp 1971–1976

Choudhury B, Then P, Raman V, Issac B, Haldar MK (2016) Cancelable iris Biometrics based on data hiding schemes. In: IEEE student conference on research and development (SCOReD). IEEE, pp 1–6

Connie T, Teoh A, Goh M, Ngo D (2005) Palmhashing: a novel approach for Cancelable Biometrics. Inf Process Lett 93(1):1–5

Deshmukh M, Balwant MK (2017) Generating Cancelable Palmprint templates using local binary pattern and random projection. In: International conference on signal-image technology & internet-based systems (SITIS), vol 13. IEEE, pp 203–209

Dey N, Nandi B, Dey M, Biswas D, Das A, Chaudhuri SS (2013) BioHash code generation from electrocardiogram features. In: Advance computing conference (IACC), vol 3. IEEE, pp 732–735

Drozdowski P, Garg S, Rathgeb C, Gomez-Barrcro M, Chang D, Busch C (2018) Privacy-preserving indexing of Iris-codes with cancelable bloom filter-based search structures. In: European signal processing conference (EUSIPCO), vol 26. IEEE, pp 2360–2364

Dwivedi R, Dey S (2015) Cancelable iris template generation using look-up table mapping. In: International conference on signal processing and integrated networks (SPIN), vol 2. IEEE, pp 785–790

Egner A, Soceanu A, Moldoveanu F (2012) Managing secure authentication for standard mobile medical networks. In: Symposium on computers and communications (ISCC). IEEE, pp 390–393

Farooq F, Bolle RM, Jea TY, Ratha N (2007) Anonymous and revocable fingerprint recognition. In: Conference on computer vision and pattern recognition. IEEE, pp 1–7

Ghany KK, Hefny HA, Hassanien AE, Ghali NI (2012) A hybrid approach for biometric template security. In: Proceedings of the 2012 international conference on advances in social networks analysis and mining (ASONAM 2012). IEEE Computer Society, pp 941–942

Hämmerle-Uhl J, Pschernig E, Uhl A (2013) Cancelable iris-templates using key-dependent wavelet transforms. In: International conference on biometrics (ICB). IEEE, pp 1–8

Hirata S, Takahashi K (2009) Cancelable biometrics with perfect secrecy for correlation-based matching. In: International conference on biometrics. Springer, Berlin, pp 868–878

Issac CM, Kanaga EG (2017) Probing on classification algorithms and features of brain signals suitable for Cancelable Biometric authentication. In: IEEE international conference on computational intelligence and computing research (ICCIC). IEEE, pp 1–4

Izu T, Sakemi Y, Takenaka M, Torii N (2014) A spoofing attack against a Cancelable Biometric authentication scheme. In: International conference on advanced information networking and applications (AINA), vol 28. IEEE, pp 234–239

Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol 14(1):1–47

Jain AK, Flynn P, Ross AA (2007) Handbook of biometrics. Springer, Berlin

Jenisch S, Uhl A (2011) Security analysis of a cancelable iris recognition system based on block remapping. In: IEEE international conference on image processing, vol 18. IEEE, pp 3213–3216

Jeong M, Lee C, Kim J, Choi JY, Toh KA, Kim J (2006) Changeable biometrics for appearance based face recognition. In: biometrics symposium: special session on research at the biometric consortium conference. IEEE, pp 1–5

Jiménez A, Raj B (2017) A two factor transformation for speaker verification through l comparison. In: IEEE workshop on information forensics and security (WIFS). IEEE, pp 1–6

Jin Z, Hwang JY, Lai YL, Kim S, Teoh ABJ (2018) Ranking-based locality sensitive hashing-enabled Cancelable Biometrics: index-of-max hashing. IEEE Trans Inf Forensics Secur 13(2):393–407

Kanade S, Petrovska-Delacrétaz D, Dorizzi B (2009) Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data. In: IEEE conference on computer vision and pattern recognition. IEEE, pp 120–127

Kanade S, Petrovska-Delacrétaz D, Dorizzi B (2010) Generating and sharing biometrics based session keys for secure cryptographic applications. In: Fourth IEEE international conference on biometrics: theory, applications and systems (BTAS). IEEE, pp 1–7

Karabat C, Erdogan H (2009a) A Cancelable Biometric hashing for secure biometric verification system. In: Fifth international conference on intelligent information hiding and multimedia signal processing. IEEE, pp 1082–1085

Karabat C, Erdogan H (2009b) Trustworthy biometric hashing method. IEEE Signal Process Commun Appl Conf 17:65–68

Kaur H, Khanna P (2015) Gaussian random projection based non-invertible Cancelable Biometric templates. Procedia Comput Sci 54:661–670

Kaur H, Khanna P (2016) Biometric template protection using Cancelable Biometrics and visual cryptography techniques. Multimed Tools Appl 75(23):16333–16361

Kaur H, Khanna P (2017a) Cancelable features using log-Gabor filters for biometric authentication. Multimed Tools Appl 76(4):4673–4694

Kaur H, Khanna P (2017b) Non-invertible biometric encryption to generate Cancelable Biometric templates. In: Proceedings of the World Congress on Engineering and Computer Science, vol 1, pp 1–4

Kaur H, Khanna P (2019) Random distance method for generating unimodal and multimodal Cancelable Biometric features. IEEE Trans Inf Forensics Secur 14(3):709–719

Kelkboom EJ, Zhou X, Breebaart J, Veldhuis RN, Busch C (2009) Multi-algorithm fusion with template protection. In: International conference on biometrics: theory, applications, and systems, vol 3. IEEE, pp 1–8

Kelkboom EJ, Molina GG, Breebaart J, Veldhuis RN, Kevenaar TA, Jonker W (2010) Binary biometrics: an analytic framework to estimate the performance curves under Gaussian assumption. IEEE Trans Syst Man Cybern A Syst Hum 40(3):555–571

Khodabacchus MY, Soyjaudah KMS, Ramsawok G (2016) Fingerprint code authentication protocol on cloud. In: International conference on emerging technologies and innovative business practices for the transformation of societies (EmergiTech). IEEE, pp 162–166

Khodabacchus MY, Soyjaudah KMS, Ramsawock G (2017) Secured SAML cloud authentication using fingerprint. In: International conference on next generation computing applications (NextComp), vol 1. IEEE, pp 151–156

Kim J, Teoh AB (2018) One-factor Cancellable Biometrics based on indexing-first-order hashing for fingerprint authentication. In: International conference on pattern recognition (ICPR), vol 24. IEEE, pp 3108–3113

Kim Y, Toh KA (2007) A method to enhance face biometric security. In: International conference on biometrics: theory, applications, and systems, vol 1. IEEE, pp 1–6

Kim Y, Toh KA (2008) Sparse random projection for efficient cancelable face feature extraction. In: Conference on industrial electronics and applications, vol 3. IEEE, pp 2139–2144

Kim H, Nguyen MP, Chun SY (2017) Cancelable ECG Biometrics using GLRT and performance improvement using guided filter with irreversible guide signal. In: Annual international conference of engineering in medicine and biology society (EMBC), vol 39. IEEE, pp 454–457

Kong A, Cheung KH, Zhang D, Kamel M, You J (2006) An analysis of BioHashing and its variants. Pattern Recognit 39(7):1359–1368

Kumar N, Singh S, Kumar A (2018) Random permutation principal component analysis for Cancelable Biometric recognition. Appl Intell 48(9):2824–2836

Lalithamani N, Soman KP (2009a) An efficient approach for non-invertible cryptographic key generation from cancelable fingerprint biometrics. In: International conference on advances in recent technologies in communication and computing. IEEE, pp 47–52
Lalithamani N, Soman KP (2009b) Towards generating irrevocable key for cryptography from cancelable fingerprints. In: International conference on computer science and information technology, vol 2. IEEE, pp 563–568
Lee C, Choi JY, Toh KA, Lee S, Kim J (2007) Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE Trans Syst Man Cybern B Cybern 37(4):980–992
Lee DH, Lee SH, Cho NI (2018) Cancelable Biometrics using noise embedding. In: International conference on pattern recognition (ICPR), vol 24. IEEE, pp 3390–3395
Leng L, Zhang J (2012) Palmhash code for Palmprint verification and protection. In: IEEE Canadian conference on electrical & computer engineering (CCECE), vol 25. IEEE, pp 1–4
Leng L, Zhang JS, Khan MK, Bi X, Ji M (2010) Cancelable palmcode generated from randomized gabor filters for palmprint protection. In: International conference of image and vision computing New Zealand, vol 25. IEEE, pp 1–6
Leng L, Zhang S, Bi X, Khan M K (2012) Two-dimensional cancelable Biometric scheme. In: International conference on wavelet analysis and pattern recognition (ICWAPR). IEEE, pp 164–169
Leng L, Li M, Teoh ABJ (2013a) Conjugate 2dpalmhash code for secure palm-print-vein verification. In: International congress on image and signal processing (CISP), vol 6(no 3). IEEE, pp 1705–1710
Leng L, Teoh ABJ, Li M, Khan MK (2013b) Orientation range for transposition according to the correlation analysis of 2DPalmHash Code. In: International symposium on biometrics and security technologies (ISBAST). IEEE, pp 230–234
Leng L, Teoh AB, Li M, Khan MK (2014a) Analysis of correlation of 2DPalmHash code and orienta tion range suitable for transposition. Neurocomputing 131:377–387
Leng L, Li M, Teoh ABJ (2014b) Matching reduction of 2DPalmHash code. In: International symposium on biometrics and security technologies (ISBAST). IEEE, pp 124–128
Lingli Z, Jianghuang L (2010) Security algorithm of face recognition based on binary pattern and random projection. In: Cognitive informatics (ICCI), vol 9. IEEE, pp 733–738
Lumini A, Nanni L (2007) An improved biohashing for human authentication. Pattern Recognit 40(3):1057–1065
Maiorana E, Campisi P, Ortega-Garcia J, Neri A (2008) Cancelable Biometrics for HMM-based signature recognition. In: International conference on biometrics: theory, applications and systems, vol 2. IEEE, pp 1–6
Maiorana E, Campisi P, Neri A (2009) Template protection for dynamic time warping based biometric signature authentication. In: International conference on digital signal processing, vol 16. IEEE, pp 1–6
Maiorana E, Campisi P, Fierrez J, Ortega J, Neri A (2010) Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Trans Syst Man Cybern 40(3):525–538
Maiorana E, Campisi P, Neri A (2011) Bioconvolving: cancelable templates for a multi-biometrics signature recognition system. In: IEEE international systems conference. IEEE, pp 495–500
Meetei TC, Begum SA (2016) A variant of cancelable iris biometric based on BioHashing. In: International conference on signal and information processing (IConSIP). IEEE, pp 1–5
Mtibaa A, Petrovska-Delacretaz D, Hamida AB (2018) Cancelable speaker verification system based on binary Gaussian mixtures. In: International conference on advanced technologies for signal and image processing (ATSIP), vol 4. IEEE, pp 1–6
Nazari S, Moin MS, Kanan HR (2014) Cancelable face using chaos permutation. In: International symposium on telecommunications (IST), vol 7. IEEE, pp 925–928
Nishiuchi N, Soya H (2011) Cancelable Biometric identification by combining biological data with artifacts. In: International conference on biometrics and Kansei engineering (ICBAKE), pp 61–64
Oh K, Toh KA (2012) Extracting sclera features for cancelable identity verification. In: International conference on Biometrics (ICB), vol 5. IEEE, pp 245–250
Othman A, Ross A (2013) On mixing fingerprints. IEEE Trans Inf Forensics Secur 8(1):260–267
Ouda O, Tusmura N, Nakaguchi T (2011) Securing bioencoded iris codes against correlation attacks. In: IEEE international conference on communications (ICC). IEEE, pp 1–5
Patel VM, Chellappa R, Tistarelli M (2010) Sparse representations and random projections for robust and cancelable biometrics. In: International conference on control automation robotics and vision, vol 11. IEEE, pp 1–6
Patel VM, Ratha NK, Chellappa R (2015) Cancelable Biometrics: a review. IEEE Signal Process Mag 32(5):54–65
Paul PP, Gavrilova M (2012) Multimodal cancelable Biometrics. In: International conference on cognitive informatics & cognitive computing (ICCI* CC), vol 11. IEEE, pp 43–49

Paul PP, Gavrilova M (2013a) Cancelable fusion using social network analysis. In: Proceedings of the IEEE/ACM international conference on advances in social networks analysis and mining. ACM, pp 1469–1471
Paul PP, Gavrilova M (2013b) Novel multimodal template generation algorithm. In: IEEE international conference on cognitive informatics & cognitive computing (ICCI* CC), vol 12. IEEE, pp 76–82
Paul PP, Gavrilova M (2014a) Multimodal Biometrics using cancelable feature fusion. In: International conference on cyberworlds (CW). IEEE, pp 279–284
Paul PP, Gavrilova M (2014b) Rank level fusion of multimodal Cancelable Biometrics. In: IEEE international conference on cognitive informatics & cognitive computing (ICCI* CC), vol 13. IEEE, pp 80–87
Paul PP, Gavrilova M, Klimenko S (2013) Situation awareness through multimodal Biometric template security in real-time environments. In: International conference on cyberworlds (CW). IEEE, pp 82–88
Pillai JK, Patel VM, Chellappa R, Ratha NK (2010) Sectored random projections for cancelable iris biometrics. In: IEEE international conference on acoustics, speech and signal processing, pp 1838–1841
Pillai JK, Patel VM, Chellappa R, Ratha NK (2011) Secure and robust iris recognition using random projections and sparse representations. IEEE Trans Pattern Anal Mach Intell 33(9):1877–1893
Popa D, Simion E (2017) Enhancing security by combining Biometrics and cryptography. In: International conference on electronics, computers and artificial intelligence (ECAI), vol 9. IEEE, pp 1–7
Prasad MV, Jyothi A, Lasya K (2017) Cancelable iris template generation using modulo operation. In: International conference on signal-image technology & internet-based systems (SITIS), vol 13. IEEE, pp 210–217
Prasanalakshmi B, Kannammal A (2010) Secure cryptosystem from palm vein Biometrics in smart card. In: Computer and automation engineering (ICCAE), vol 2(no 1). IEEE, pp 653–657
Pravinchandra MM, Diwanji HM, Shah JS, Kotak H(2012) Performace analysis of encryption and decryption using genetic based cancelable non-invertible fingerprint based key in MANET. In: International conference on communication systems and network technologies (CSNT). IEEE, pp 357–361
Punithavathi P, Geetha S (2016) Dynamic sectored random projection for cancelable iris template. In: International conference on advances in computing, communications and informatics (ICACCI). IEEE, pp 711–715
Punithavathi P, Geetha S, Shanmugam S (2017) Cloud-based framework for cancelable biometric system. In: IEEE international conference on cloud computing in emerging markets (CCEM). IEEE, pp 35–38
Quan F, Fei S, Anni C, Feifei Z (2008) Cracking cancelable fingerprint template of Ratha. In: International symposium on computer science and computational technology, vol 2. IEEE, pp 572–575
Rachapalli DR, Kalluri HK (2017) A survey on Biometric template protection using cancelable Biometric scheme. In: International conference on electrical, computer and communication technologies (ICECCT), vol 2. IEEE, pp 1–4
Raja KB, Raghavendra R, Busch C (2018a) Manifold-structure preserving biometric templates—a preliminary study on fully cancelable smartphone biometric templates. In: IEEE international conference on multimedia & expo workshops (ICMEW). IEEE, pp 1–7
Raja KB, Raghavendra R, Busch C (2018b) Towards protected and cancelable multi-spectral face templates using feature fusion and kernalized hashing. In: International conference on information fusion (FUSION), vol 21. IEEE, pp 2098–2106
Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
Ratha N, Connell J, Bolle RM, Chikkerur S (2006) Cancelable Biometrics: a case study in fingerprints. In: International conference on pattern recognition (ICPR'06), vol 18(no. 4). IEEE, pp 370–373
Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572
Rathgeb C, Busch C (2013) Comparison score fusion towards an optimal alignment for enhancing cancelable iris biometrics. In: Fourth international conference on emerging security technologies (EST). IEEE, pp 51–54
Rathgeb C, Busch C (2014) Cancelable multi-Biometrics: mixing iris-codes based on adaptive bloom filters. Comput Secur 42:1–12
Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 2011(1):1–3
Rathgeb C, Breitinger F, Busch C (2013) Alignment-free cancelable iris Biometric templates based on adaptive bloom filters. In: International conference on Biometrics (ICB). IEEE, pp 1–8
Rathgeb C, Breitinger F, Busch C, Baier H (2014) On application of bloom filters to iris biometrics. IET Biom 3(4):207–218

Rathgeb C, Gomez-Barrero M, Busch C, Galbally J, Fierrez J (2015a) Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: International workshop on biometrics and forensics (IWBF 2015), vol 3. IEEE, pp 1–6

Rathgeb C, Wagner J, Tams B, Busch C (2015b) Preventing the cross-matching attack in bloom filter-based Cancelable Biometrics. In: International workshop on biometrics and forensics (IWBF). IEEE, pp 1–6

Ross A, Othman A (2010) Visual cryptography for biometric privacy. IEEE Trans Inf Forensics Secur 6(1):70–81

Ross A, Shah J, Jain AK (2007) From template to image: reconstructing fingerprints from minutiae points. IEEE Trans Pattern Anal Mach Intell 29(4):544–560

Saito Y, Nakamura I, Shiota S, Kiya H (2016) An efficient random unitary matrix for biometric template protection. In: joint international conference on soft computing and intelligent systems (SCIS) and international symposium on advanced intelligent systems (ISIS), vol 8 & 17. IEEE, pp 366–370

Sandhya M, Prasad MV (2015) k-Nearest Neighborhood structure (k-NNS) based alignment-free method for fingerprint template protection. In: International conference on Biometrics (ICB). IEEE, pp 386–393

Sandhya M, Prasad MV (2016) Securing fingerprint templates using fused structures. IET Biom 6(3):173–182

Sarier ND (2010) Practical multi-factor biometric remote authentication. In: International conference on biometrics: theory, applications and systems (BTAS), vol 4. IEEE, pp 1–6

Sarkar A, Singh BK (2017) Cancelable Biometric based key generation for symmetric cryptography. In: International conference on inventive communication and computational technologies (ICICCT). IEEE, pp 404–409

Savvides M, Kumar BV, Khosla PK (2004) Cancelable biometric filters for face recognition. Proc Int Conf Pattern Recognit 17(3):922–925

Singh LD, Singh KM (2015) Image encryption using elliptic curve cryptography. Procedia Comput Sci 54:472–481

Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV (1998) Biometric encryption using image processing. Opt Secur Counterfeit Deterrence Techn 3314:178–189

Sree SS, Radha N (2016) Cancellable multimodal biometric user authentication system with fuzzy vault. In: International conference on computer communication and informatics (ICCCI). IEEE, pp 1–6

Sui Y, Zou X, Du EY, Li F (2014) Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method. IEEE Trans Comput 63(4):902–916

Suresh P, Radhika KR (2015) Biometric credential system: multimodal cancelable anonymous identity management. In: International advance computing conference (IACC). IEEE, pp 353–356

Takahashi K, Hirata S (2011a) Cancelable Biometrics with provable security and its application to fingerprint verification. IEICE Trans Fundam Electron Commun Comput Sci 94(1):233–244

Takahashi K, Hirata S (2011b) Parameter management schemes for cancelable biometrics. In: IEEE workshop on computational intelligence in biometrics and identity management (CIBIM). IEEE, pp 145–151

Takahashi K, Hitachi SH (2009) Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering. In: International conference on biometrics: theory, applications, and systems, vol 3. IEEE, pp 1–6

Takahashi K, Naganuma K (2012) Unconditionally provably secure Cancellable Biometrics based on a quotient polynomial ring. IET Biom 1(1):63–71

Talreja V, Valenti MC, Nasrabadi NM (2017) MultiBiometric secure system based on deep learning. In: IEEE global conference on signal and information processing (GlobalSIP). IEEE, pp 298–302

Tams B, Rathgeb C (2014) Towards efficient privacy-preserving two-stage identification for fingerprint-based Biometric cryptosystems. In: IEEE international joint conference on Biometrics (IJCB). IEEE, pp 1–8

Tan F, Ong TS, Tee C, Teoh AB (2009) Image hashing enabled technique for biometric template protection. In: TENCON IEEE region conference, vol 10. IEEE, pp 1–5

Teoh AB, Yuang CT (2007) Cancelable Biometrics realization with multispace random projections. IEEE Trans Syst Man Cybern B Cybern 37(5):1096–1106

Teoh AB, Goh A, Ngo DC (2006) Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans Pattern Anal Mach Intell 28(12):1892–1901

Teoh AB, Kuan YW, Lee S (2008) Cancellable biometrics and annotations on biohash. Pattern Recognit 41(6):2034–2044

Thomas AO, Ratha NK, Connell JH, Bolle RM (2008) Comparative analysis of registration based and registration free methods for cancelable fingerprint biometrics. In: International conference on pattern recognition, vol 19. IEEE, pp 1–4

Toh KA, Lee C, Choi JY, Kim J (2007) Performance based revocable biometrics. In: IEEE conference on industrial electronics and applications, vol 2. IEEE, pp 647–652

Ueshige Y, Sakurai K (2014) Towards receipt-freeness in remote biometric authentication. In: Fifth international conference on emerging security technologies. IEEE, pp 8–12

Wang Y, Hatzinakos D (2010) Cancelable face recognition using random multiplicative transform. In: International conference on pattern recognition, vol 20. IEEE, pp 1261–1264
Wang S, Hu J (2013) A Hadamard transform-based method for the design of cancellable fingerprint templates. In: International Congress on image and signal processing (CISP), vol 3(no 6). IEEE, pp 1682–1687
Wong WJ, Wong MD, Teoh A BJ (2014) A security-and privacy-driven hybrid Biometric template protection technique. In: International conference on electronics, information and communications (ICEIC). IEEE, pp 1–5
Wu SC, Chen PT, Swindlehurst AL, Hung PL (2018) Cancelable biometric recognition with ECGs: subspace-based approaches. IEEE Trans Inf Forensics Secur 14(5):1323–1336
Xu W, Cheng M (2008) Cancelable voiceprint template based on chaff-points-mixture method. In: International conference on computational intelligence and security, vol 2. IEEE, pp 263–266
Xu D, Li B (2009) A pseudo-random sequence fingerprint key algorithm based on fuzzy vault. In: International conference on mechatronics and automation. IEEE, pp 2421–2425
Xu D, Wang X (2010) A scheme for cancelable fingerprint fuzzy vault based on chaotic sequence. In: IEEE international conference on mechatronics and automation. IEEE, pp 329–332
Xu W, He Q, Li Y, Li T (2008) Cancelable voiceprint templates based on knowledge signatures. In: International symposium on electronic commerce and security. IEEE, pp 412–415
Yang H, Jiang X, Kot AC (2009) Generating secure cancelable fingerprint templates using local and global features. In: International conference on computer science and information technology, vol 2. IEEE, pp 645–649
Yang K, Du Y, Zhou Z, Belcher C (2010) Gabor descriptor based cancelable iris recognition method. In: IEEE international conference on image processing. IEEE, pp 4085–4088
Yang W, Wang S, Hu J, Zheng G, Chaudhry J, Adi E, Valli C (2018a) Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. IEEE Access 6:36939–36947
Yang W, Wang S, Hu J, Zheng G, Valli C (2018b) A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recognit 78:242–251
You L, Yang L, Yu W, Wu Z (2017) A cancelable fuzzy vault algorithm based on transformed fingerprint features. Chin J Electron 26(2):236–43
Zhang N, Yang X, Zang Y, Jia X, Tian J (2013) Generating registration-free cancelable fingerprint templates based on minutia cylinder-code representation. In: International conference on biometrics: theory, applications and systems (BTAS), vol 6. IEEE, pp 1–6
Zhu HH, He QH, Tang H, Cao WH (2011) Voiceprint-biometric template design and authentication based on cloud computing security. In: International conference on cloud and service computing. IEEE, pp 302–308
Zhu HH, He QH, Li YX (2012) A two-step hybrid approach for voiceprint-biometric template protection. In: International conference on machine learning and cybernetics, vol 2. IEEE, pp 560–565
Zuo J, Ratha NK, Connell JH (2008) Cancelable iris biometric. In: International conference on pattern recognition, vol 19. IEEE, pp 1–4