J Supercomput (2018) 74:4893–4909
https://doi.org/10.1007/s11227-018-2266-0

ECB4CI: an enhanced cancelable biometric system for securing critical infrastructures

Wencheng Yang[1] · **Song Wang**[2] · **Guanglou Zheng**[1] · **Junaid Chaudhry**[1,3] · **Craig Valli**[1]

Published online: 29 January 2018

Abstract Physical access control is an indispensable component of a critical infrastructure. Traditional password-based methods for access control used in the critical infrastructure security systems have limitations. With the advance of new biometric recognition technologies, security control for critical infrastructures can be improved by the use of biometrics. In this paper, we propose an enhanced cancelable biometric system, which contains two layers, a core layer and an expendable layer, to provide reliable access control for critical infrastructures. The core layer applies random projection-based non-invertible transformation to the fingerprint feature set, so as to provide template protection and revocability. The expendable layer is used to protect the transformation key, which is the main weakness contributing to attacks via record

✉ Guanglou Zheng
g.zheng@ecu.edu.au

Wencheng Yang
w.yang@ecu.edu.au

Song Wang
song.wang@latrobe.edu.au

Junaid Chaudhry
Chaudhry@ieee.org

Craig Valli
c.valli@ecu.edu.au

1 Security Research Institute, School of Science, Edith Cowan University, Joondalup, WA 6027, Australia

2 School of Engineering and Mathematical Sciences, La Trobe University, Melbourne, VIC 3086, Australia

3 College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ, USA

multiplicity. This improvement enhances the overall system security, and undoubtedly, this extra security is an advantage over the existing cancelable biometric systems.

Keywords Access control · Critical infrastructure · Cancelable biometrics · Fuzzy commitment

1 Introduction

The critical assets, like utility substations, data hubs and control centers in communications, utilities and energy industries, must be able to ensure the highest reliability level, because the economic prosperity and social well-being of the nation rely on them to operate the infrastructures and keep the economy healthy. There is no more urgent priority than assuring the continuity, availability and security of the critical infrastructures [1], so to protect critical infrastructure requires advanced physical access systems to reliably manage access control of individuals. Biometric recognition systems, e.g., fingerprint recognition system, which are based on "who you are" to achieve authentication, can defend the critical infrastructure [2] and toughen up critical infrastructure security. Biometric recognition systems have many advantages compared with traditional password- or token-based authentication, which is based on "what you know/have." For example, the use of biometric systems can avoid the trouble of remembering long passwords and token loss [3].

In a typical biometric authentication system, two stages are composed, namely enrollment stage and authentication stage [4]. Specifically, in the enrollment stage, a user presents his/her finger to a sensor where his/her fingerprint image is captured. Then features are extracted from the fingerprint image and stored in the database as a template. In the authentication stage, a user, who wants to be authenticated, presents his/her finger to the sensor. The same algorithm used in the enrollment stage is applied to extracting features, known as a query. The query is then compared with the template stored in the database to output a matching or non-matching report. A typical fingerprint-based authentication system is demonstrated in Fig. 1 as an example.

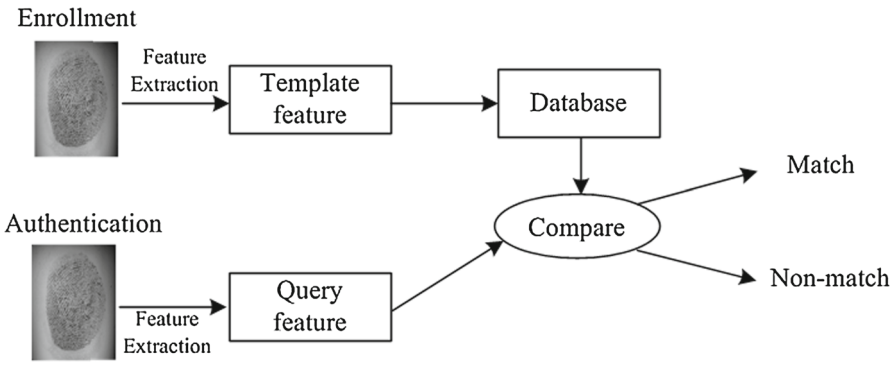

Fig. 1 A typical biometric authentication system including two stages, enrollment and authentication

However, with the widespread deployment of biometric systems, security and privacy issues arise. For example, with the stored biometric templates, e.g., fingerprint minutiae information or face feature data, the whole fingerprint or face image [5] can be reconstructed. Template cross-matching in different applications is another issue which can cause privacy leakage of individuals [6]. These issues make biometric template protection necessary.

1.1 Related work

There are two main categories of biometric template protection: biometric cryptosystems and cancelable biometrics. Specifically, in biometric cryptosystems, a secret key is either bound with or directly generated from biometric features. The biometric features are secured by secure sketches, e.g., fuzzy commitment [7] and fuzzy vault [8]. The concept of fuzzy commitment was first proposed by Juels and Wattenberg in [7] as a type of cryptographic primitive. It combines techniques from the areas of error-correction codes and cryptography. In a fuzzy commitment-based biometric system, according to [7], to encrypt a secret key k, in the enrollment stage, it is inputted into the error-correction code, e.g., BCH, to generate a codeword $C = B_e(k)$, where $B_e(\cdot)$ represents the encoding procedure of the BCH code. The codeword is further bound with the biometric template feature string x to output the helper data $y = C \oplus x$, where $\oplus$ represents the XOR operation. In the authentication stage, in order to retrieve the secret key k, a query feature string x' is extracted and XORed with the helper data y as $C' = x' \oplus y$. Then C' is inputted into the BCH code, as $k' = B_d(C')$, where $B_d(\cdot)$ represents the decoding procedure of the BCH code. If the hamming distance between x' and x is smaller than the error-correction capability of the BCH code, the retrieved secret string k' will be the same as k and the authentication is successful. In [9], Teoh and Kim proposed a method named randomized dynamic quantization transformation to generate random and unique binary strings. Then the generated binary strings are bound with a random bit string using the fuzzy commitment scheme. Fuzzy commitment, as an efficient template protection algorithm, however, has its drawbacks, such as limited security and suffering from cross-matching attack. In [10], the authors provided a comprehensive analysis on the privacy and security of the fuzzy commitment scheme. The analysis shows that a very significant reduction of privacy and security leakage occur because of the dependency of biometric data. In order to prevent the cross-matching attack, Kelkboom et al. [11] applied a random bit-permutation process to securing the fuzzy commitment data.

Fuzzy commitment methods require the template and query features, e.g., x and x', to be ordered so that their correspondence can be distinct. The features extracted from face or iris can meet this requirement, but the features extracted from fingerprint are represented by a set of unordered minutiae points and thus cannot fulfill this requirement [12]. To solve the issue, Uludag et al. [8] proposed to protect the fingerprint minutiae data with fuzzy vault [13]. The experimental results show that a 128-bit AES key can be feasibly secured by the proposed fuzzy vault. Later, Nagar et al. [14] showed that by using the fuzzy commitment scheme, the security of fuzzy vault can be improved. The authors used the orientation and ridge frequency information in

a minutia's neighborhood to secure/encrypt the polynomial evaluations. To further increase the security of fuzzy vault, Narayanan and Karthikeyan [15] used a double encryption technique, which combines symmetric key and a symmetric key generation. The experimental results demonstrate that better security is achieved. Some other variants of fuzzy vault are also designed and proposed, e.g., [16–19].

Cancelable biometrics is another technique to protect biometric templates. The concept of cancelable biometrics was first proposed by Ratha et al. [20], which is to accomplish authentication by utilizing the transformed version of the biometric data instead of the original biometric data. If the transformed templates are compromised, they can be revoked. Also, the original templates are still secure because the transformation used in the process is non-invertible. Subsequent to [20], a variety of algorithms in cancelable biometrics are presented. In [21], Ratha et al. developed several methods to generate cancelable templates such as Cartesian transformation, polar transformation and functional transformation and presented a brief analysis of their strengths. In [22], Teoh et al. proposed a scheme named BioHash to mix a set of user-specific random vectors with biometric features. In BioHash, a quantized random projection ensemble is used to establish the mathematical foundation of BioHash. Yang et al. [23] proposed a non-invertible transform to perpendicularly project the distances between two minutiae to a circle to create the features. Besides the distances, some other local and global features, such as relative angles between minutiae pairs, orientation and ridge frequency, are also used. Lee and Kim [24] introduced a new way to create cancelable templates without requiring fingerprint image pre-alignment. The core idea is to project the minutiae structures into a predefined 3D array, which is composed of small cells. If a cell contains a minutiae structure, it is set to 1; otherwise, it is set to 0. In this way, a 1D binary string is formed by sequentially concatenating the cells in the 3D array. Ahmad et al. [25] proposed a pair-polar coordinate-based cancelable fingerprint templates, which do not require registration because the pair-polar structure is rotation- and transform-free. Then a many-to-one mapping relationship is established to achieve the one-way transformation. The above methods focus on the generation of stable or registration-free features, while others pay more attention to the design of non-invertible transformations. In [26], Wang and Hu proposed a densely infinite-to-one mapping (DITOM)-based mathematical model to carry out non-invertible transformation. Later, they constructed cancelable fingerprint templates via curtailed circular convolution, which is an effective one-way transform [27]. A partial Hadamard transformation in [28] and a partial discrete Fourier transform-based non-invertible transformation in [29] are proposed by Wang et al. to provide secure protection to the binary biometric representations.

1.2 Motivation and contributions

Regarding the aforementioned cancelable biometric systems, there is a serious security concern, that is, when multiple transformed templates and their corresponding transformation parameters (e.g., the transformation key that generates the transformation matrix) are obtained by the attacker, the biometric template can be compromised by attacks via record multiplicity (ARM) according to the research in [30,31]. In all

the existing cancelable biometric systems, transformation keys are not protected and therefore they are considered publicly available, which makes the original biometric features vulnerable to ARM.

To solve the above issue, in this paper we propose an enhanced cancelable biometric system, which contains two layers, a core layer and an expendable layer. The expendable layer is added to protect the transformation key used in the core layer. In this sense, the expendable layer is considered to be a complement to the core layer and even if the expendable layer is compromised, the biometric templates are still safe. The contribution of this work is highlighted as follows:

1. The transformation key used in cancelable biometrics without protection poses the risk of compromising the original biometric feature set through ARM. To address this, we resort to the fuzzy commitment technique to extract a feature set from the face image to protect the transformation key. If an adversary wants to retrieve the original biometric features, he/she has to break the fuzzy commitment first and then reverse the non-invertible transformation. We call this method cascading encryption. It can defend against the ARM.
2. The proposed system strikes a balance between recognition performance and security. The system with no template protection performs best; recognition performance decreases when the cancelable biometric technique is applied and further declines when the expendable layer is added. However, the system security is clearly strengthened with the addition of the expendable layer.

The rest of the paper is organized as follows. The proposed cascading encryption scheme, which is able to enhance the system security, is introduced in Sect. 2. The experimental results and security analysis are presented in Sect. 3. In Sect. 4, the conclusion is given.

2 The enhanced cancelable biometric system with cascading encryption

The proposed enhanced cancelable biometric system contains two layers, a core layer and an expendable layer. In the core layer, a random projection-based non-invertible transformation is used to protect the fingerprint template. To heighten the security of the core layer, an expendable layer is added, in which a feature set extracted from the face image together with the fuzzy commitment technique is employed to secure the transformation key in the core layer. The details of the two layers are presented below.

2.1 Core layer: fingerprint template generation and protection using non-invertible transformation

Because of factors like nonlinear distortion and rotation during fingerprint image acquisition, fingerprint patterns are known for small interclass variability but large intraclass variation [32]. Fingerprint templates generated using global features usually rely on precise registration based on singular points. However, accurate singular point detection is hard. It is observed that a local structure formed by a minutia with its neighboring minutiae tends to be stable in the presence of distortion and translation- and

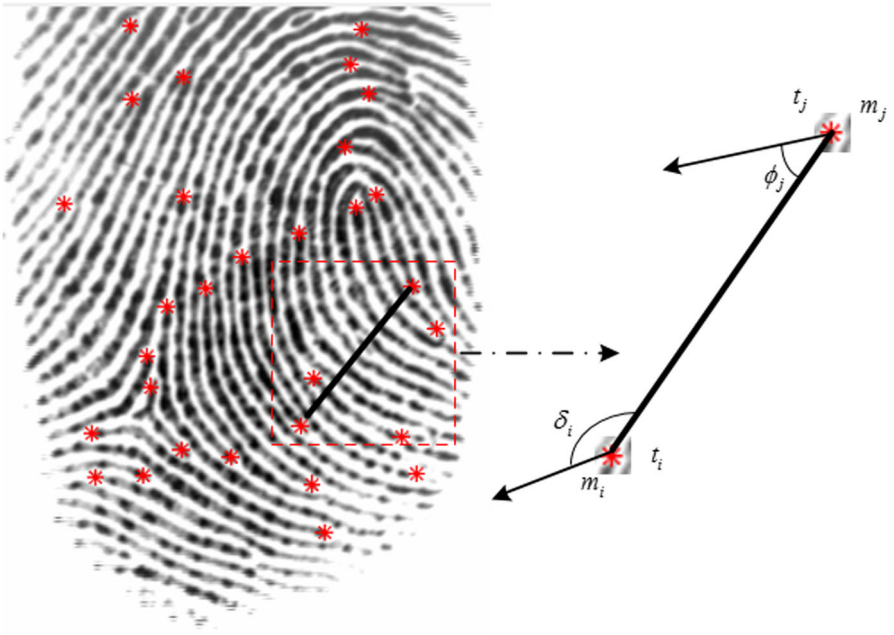

Fig. 2 An example of the minutiae pair

rotation-invariant. Therefore, a minutiae pair-based local structure [26] is employed in this paper.

Given a set of minutiae M which includes N minutiae, each minutia m_i from M can be represented by $m_i = (x, y, \theta, t)_{i\in[1,N]}$, where (x, y) is the coordination of the minutia, θ is the minutia orientation, and t represents the type of the minutia. A local structure, which is formed by two minutiae, $m_i = (x_i, y_i, \theta_i, t_i)$ and $m_j = (x_j, y_j, \theta_j, t_j)$ from minutiae set M, is shown in Fig. 2, and a feature vector V_{ij} can be extracted from it. The feature vector V_{ij} is represented by $V_{ij} = (L_{ij}, \delta_i, \phi_j, t_i, t_j)$, where L_{ij} is the length of the edge between minutiae m_i and m_j; δ_i and ϕ_j are the angles between the orientation of each minutia and the edge, and they are in the range of 0 to 2π. If any two minutiae from minutiae set M form a minutia pair, there is a total of $N \times (N-1)/2$ minutia pairs. Due to the intrauser variation caused by biometric uncertainty between the corresponding minutia pairs from template and query images, the quantization technique similar to that in [24] is applied to mitigating such variation. For example, assume that the edge lengths of L_1 and L_2 are 16 and 18 pixels, respectively; if their absolute values are used to do matching, obviously $L_1 \neq L_2$, however, if all the values between [15–21] are quantized to be 18, then $L_1 = L_2 = 18$. As such, the intrauser variation is alleviated to some extent. In this application, we set the quantization step size to be s_L for L_{ij} and the step size to be s_a for δ_i and ϕ_j. After quantization, the quantized value, e.g., 18, is converted into binary, e.g., 10,010. Assume that l_L, l_δ and l_ϕ are the bit length of the binary outputs of quantized L_{ij}, δ_i and ϕ_j, respectively. Then the length of binary representation for V_{ij} is $l_V = l_L + l_\delta + l_\phi + 2$ and V_{ij}'s corresponding integer value V_{ij}^I is in the range of

$0-2^{l_V}-1$. To add the uncertainty of the feature vector locations, a modulo operation $\mathrm{mod}(V_{ij}^I, p)$ is introduced to the corresponding integer value of each feature vector, where p is a preset parameter. For instance, if the integer value V_{ij}^I is 30,345 and p is set to be 30,000, then $\mathrm{mod}(30,345, 30,000) = 345$. So the 345th bin in the range of $[0, p-1]$ has the value of "1." Those bins without any integer value of a feature vector located are assigned the value of "0." In this way, after going through each feature vector from a total of $N \times (N-1)/2$ minutia pairs, a binary string $\mathbf{b}_f$ of length p can be obtained and 1s in $\mathbf{b}_f$ corresponds to those feature vectors, e.g., V_{ij}.

Regarding the binary string $\mathbf{b}_f$, even if the modulo operation is applied, an adversary is still able to reversely calculate the locations of minutiae, if no further protection is provided. Hence, we decide to apply the random projection-based non-invertible transformation in order to provide further protection to the binary string $\mathbf{b}_f$. The non-invertible transformation can be represented by a system of linear equations as

$$\mathbf{y}_f = \mathbf{M}\mathbf{b}_f \tag{1}$$

where $\mathbf{y}_f$ is the transformed template and $\mathbf{M}$ is the projection matrix of size $q \times p$, generated using the secret key K as a seed. If $K_i \neq K_j$, the generated matrix $\mathbf{M}_i$ is different from $\mathbf{M}_j$. The security provided by Eq. (1) is based on the well-known result in linear algebra that for a system of linear equations, if the coefficient and augmented matrices have the same rank, then solutions exist, but if the rank is smaller than the number of unknowns, then there is an infinite number of solutions [33].

2.2 Expendable layer: enhancing security with cascading encryption

In Sect. 2.1, we indicated that secret key K serves as a seed to generate the projection matrix $\mathbf{M}$, which means if the secret key K is obtained by the adversary, then the projection matrix $\mathbf{M}$ compromised. Assume that such a fingerprint-based cancelable biometric design is used in N_1 different applications, to avoid the cross-matching attack, N_1 different secrets $\{K_i\}_{i=1}^{N_1}$ are used, which lead to N_1 different projection matrixes $\{\mathbf{M}_i\}_{i=1}^{N_1}$. As mentioned in Sect. 1.2, the cancelable biometric system can be compromised by attacks via record multiplicity (ARM) [30,31], if multiple projection matrixes, e.g., $\mathbf{M}$, are obtained by the attacker.

To solve this issue, we propose to protect the secret key K by a feature set extracted from the face image with the fuzzy commitment technique. This feature set acts as an expendable layer, which expands our cancelable biometric system because the adversary who wants to attack the system needs to conquer this layer first. Even if this layer is compromised, the system security maintains the same strength provided by a typical cancelable biometric system.

Face recognition has been extensively researched. There is a considerable amount of work that has been done in face feature extraction [34–38]. In this paper, feature extraction from a face image is the same as that conducted in [38]. Specifically, given a face image I, it is first rotated according to the eye coordinates and cropped into a size of 128×128 pixels. Let $\psi(f_u, \theta_v)$ denote a Gabor filter [39,40] given by its center frequency f_u and orientation θ_v. The face feature extraction procedure is the process of

the filtering operation to the face image I using the Gabor filter $\psi(f_u, \theta_v)$ of size u and orientation v, which is represented as $G_{u,v} = I * \psi(f_u, \theta_v)$, where $G_{u,v}$ is the filtering output. Similar as [38], in which a filter bank comprises Gabor filters of five scales $u = 0, 1, \ldots, 4$ (the maximal frequency $\max(f_u)$ of the filters is 0.25 and the step size between two consecutive filter scales is $\sqrt{2}$) and eight orientations $v = 0, 1, \ldots, 7$ (the maximal value $\max(\theta_v)$ of the orientations is $7\pi/8$, and the step size between two consecutive filter orientations is $\pi/8$), a total of 40 filters are generated. After that the cropped face image I is filtered by 40 Gabor filters $\psi(f_u, \theta_v)$ from the filter bank, resulting in a feature vector $G_{u,v}$ with a dimension of 655,360 ($= 128 \times 128 \times 40$), which is obviously too costly for processing and storage. Therefore, linear discriminant analysis (LDA) as a dimensionality reduction technique is exploited to project the feature vector into a subspace. This process will generate a set of real values, as $\mathbf{r}_c = \mathrm{LDA}(G_{u,v}) = W * (G_{u,v} - \mu)$, where W is the transformation matrix and μ represents the global mean of all training samples calculated by the LDA training process. $\mathbf{r}_c$ is further transformed into a binary feature vector, $\mathbf{b}_c$ of length N_2, by utilizing the BioHashing technique in [41]. The whole process of face feature extraction is illustrated in Fig. 3.

Fuzzy commitment (FC) has been implemented successfully in many biometric systems and is particularly suitable for the binary feature representations. A fuzzy commitment contains two processes as shown in Fig. 4. (1) During the encoding process, BCH(n, k, t) code is used as a part of the encoder of FC, where k is the length of the key that can be secured and it depends on the length of the codeword n and the error-correction capability t. The BCH(n, k, t) code cannot secure the whole secret key K in our application, so only a partial key k^T from K is secured by BCH(n, k, t) code and other part of K is not a secret. The partial key k^T is encoded by the encoder of FC into a codeword $C = B_e(k^T)$ of length N_2, which is the same as the length

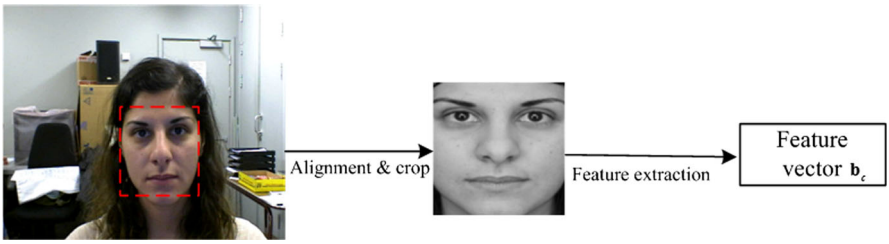

Fig. 3 The process of face feature extraction

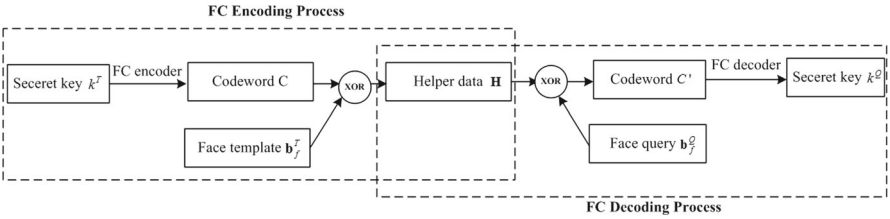

Fig. 4 Encoding and decoding processes of fuzzy commitment

of template binary feature vector $\mathbf{b}_c^T$. The feature vector $\mathbf{b}_c^T$ is then bound with the codeword C, as $\mathbf{H} = \mathbf{b}_c^T \oplus C$, where $\oplus$ represents the XOR operation and $\mathbf{H}$ acts as the helper data. The helper data $\mathbf{H}$ together with the hash value $hash(k^T)$ of k^T are stored in the database. The helper data $\mathbf{H}$ reveal no information about $\mathbf{b}_c$ or C, assuming that the fuzzy commitment is theoretically secure. (2) During the decoding process, the query binary feature vector $\mathbf{b}_c^Q$ and the stored helper data $\mathbf{H}$ are XORed to output a retrieved codeword $C' = \mathbf{b}_c^Q \oplus \mathbf{H}$. If the query feature vector $\mathbf{b}_c^Q$ is close enough to the template feature vector $\mathbf{b}_c^T$, the number of errors in the retrieved codeword C' compared with the codeword C should be smaller than error-correction capability t of the FC decoder, and the retrieved secret key $k^Q = B_d(C')$ will be the same as the original secret key k^T, and vice versa. The hash value $hash(k^Q)$ can be compared with the hash value $hash(k^T)$ to judge whether the secret key has been retrieved correctly or not.

2.3 Two stages of the proposed cancelable biometric system

As mentioned in Sect. 1, a typical biometric authentication system contains two stages, enrollment stage and authentication stage. The whole process of enrollment and authentication stages of the proposed system is shown in Fig. 5.

In the enrollment stage, the template fingerprint feature set $\mathbf{b}_f^T$ is extracted and transformed under the guidance of projection matrix $\mathbf{M}$ generated from secret key K^T, so as to produce the transformed template $\mathbf{y}_f^T$, as $\mathbf{y}_f^T = \mathbf{M}\mathbf{b}_f^T$. The details can be found in Sect. 2.1. The partial secret key k^T from K^T is bound with the face template feature set $\mathbf{b}_c^T$ to output the helper data $\mathbf{H}$, as described in the encoding process in Sect. 2.2. Both the transformed template $\mathbf{y}_f^T$ and helper data $\mathbf{H}$ are stored in the database for verification in the authentication stage.

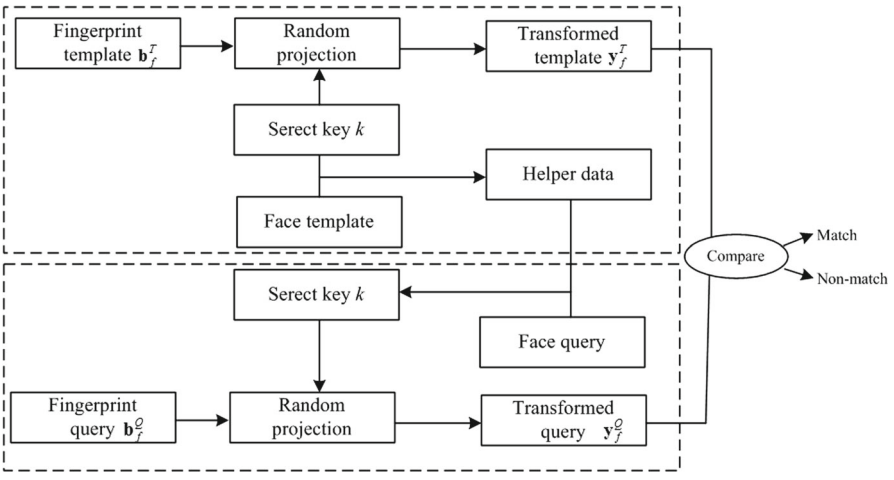

Fig. 5 The flowchart of the proposed cancelable biometric system

In the authentication stage, the first step is to retrieve the secret key used in the enrollment stage. To do this, the query face feature set $\mathbf{b}_c^Q$ together with the helper data $\mathbf{H}$ is inputted into the fuzzy commitment decoder to output a secret key k^Q, as detailed in the decoding process in Sect. 2.2. The hash value $hash(k^Q)$ of k^Q is compared with the hash value $hash(k^T)$ of k^T; if $hash(k^Q) \neq hash(k^T)$, then the matching is considered to be unsuccessful and a non-matching verdict is given directly. If $hash(k^Q) = hash(k^T)$, then the retrieved key k^Q helps to get the secret key K. K is further used as the seed to generate the same projection matrix $\mathbf{M}$ as that used in the enrollment stage; under the guidance of the projection matrix $\mathbf{M}$, the query fingerprint feature set $\mathbf{b}_f^Q$ applies the same transformation as the template feature set, $\mathbf{y}_f^Q = \mathbf{M}\mathbf{b}_f^Q$. Matching is conducted in the transformed domain using the transformed template and query fingerprint feature sets, $\mathbf{y}_f^T$ and $\mathbf{y}_f^Q$, instead of using the original feature sets, $\mathbf{b}_f^T$ and $\mathbf{b}_f^Q$. The similarity score between $\mathbf{y}_f^T$ and $\mathbf{y}_f^Q$ is calculated by the following equation:

$$S(\mathbf{y}_f^T, \mathbf{y}_f^Q) = 1 - \frac{||\mathbf{y}_f^T - \mathbf{y}_f^Q||_2}{||\mathbf{y}_f^T||_2 + ||\mathbf{y}_f^Q||_2} \tag{2}$$

where $||\cdot||_2$ represents the 2-norm. The larger the similarity score, the more similar the template and query feature sets are. The value of $S(\mathbf{y}_f^T, \mathbf{y}_f^Q)$ is in the range of [0, 1]. If the value of $S(\mathbf{y}_f^T, \mathbf{y}_f^Q)$ is larger than a predefined threshold, a match verdict is given, and vice versa.

3 Experimental results and security analysis

3.1 Performance evaluation

The proposed cancelable biometric system is evaluated on publicly available fingerprint Databases DB1 and DB2 of FVC2002 [42], DB2 of FVC2004 [43] and Database DS2 of the Multimodal BioSecure Database [44]. Each database from FVC2002 and FVC2004 contains 800 gray-level fingerprint images, which are collected from 100 fingers with eight images per finger. The software VeriFinger 4.0 of Neurotechnology [45] was utilized for minutiae extraction. In Database DS2, there are 210 users who provided their biometric traits, and each user contributed eight face images. In our experiment, the face images from the first 100 users are employed, so there are 800 faces images. The first four images of each user were used for training.

We evaluate the performance of the proposed system in three different cases. In Case 1, the performance of the system is evaluated with no template protection, i.e., without non-invertible transformation and cascading encryption. In Case 2, the cancelable biometric system without cascading encryption is tested. In Case 1 and Case 2, experiments are only carried out on fingerprint Databases DB1, DB2 of FVC2002 and DB2 of FVC2004 because Case 1 and Case 2 do not involve the cascading encryption provided by the face feature together with fuzzy commitment. In Case 3, we evaluate the performance of the proposed system with full protection to the cancelable template with non-invertible transformation and cascading encryption. In this case, in order to

Table 1 Recognition accuracy (%) of the proposed system under Case 1 and Case 2 in comparison with similar work

Cases	Databases		
	2002DB1	2002DB2	2004DB2
	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)
Tulyakov et al. [47]	3.00	–	–
Ahmad et al. [25]	9.00	6.00	–
Jin et al. [48]	5.19	5.65	11.64
Das et al. [49]	2.27	3.79	–
Wang and Hu [26]	3.5	4.00	–
Wang et al. [29]	0.19	1.00	9.01
Proposed system in Case 1	1.00 (5.00/0)	0.57 (6.00/0)	8.00 (34.00/0)
Proposed system in Case 2	2.00 (13.00/0)	2.34 (11.00/0)	11.57 (47.00/0)

generate two mated image pairs, we combine the first and second images of each finger in the fingerprint databases of FVC2002 and FVC2004 with the fifth and sixth face images from each user of the first 100 users in the Database DS2, respectively.

There are several indices that can be used to measure the system performance [46], such as the (1) false acceptance rate (FAR), which is the ratio of successful imposter attempts to the total imposter attempts, (2) false rejection rate (FRR), which is the ratio of unsuccessful genuine attempts to the total genuine attempts, and (3) equal error rate (EER), which is defined as the error rate when FAR is equal to FRR. In all the three cases, the first image is considered as the template and the second image of the same user is treated as the query to calculate the FRR. At the meantime, the first image of each user is used as template and the first image of all other (different) users is set as the query to calculate the FAR.

The performance of the proposed system in Case 1 and Case 2, compared with similar work, is reported in Table 1. From Table 1, we can see that the proposed system in Case 1 performs better than Case 2. This is because in Case 1, the system uses the original feature set, of which the feature length 2^{l_V} is larger than that q of the transformed feature in Case 2. It means that the feature set used in Case 1 contains more information than the feature set in Case 2, which leads to better performance. Note that in Case 1, the EER on Database 2002DB1 is 1.00%, which is worse than that 0.57% on Database 2002DB2, but the results turn around, when FAR $= 0$, FRR is 5.00% on Database 2002DB1 which is better than FRR $= 6.00\%$ on Database 2002DB2. EER is the error rate when FAR is equal to FRR, so even if EER on 2002DB1 is worse than that on 2002DB2, it does not necessarily mean that FRR must be worse than that on 2002DB2 under the same FAR, e.g., FAR $= 0$. Also the receiver operating characteristics (ROC) curve of the proposed system under Case 1 and Case 2 is shown in Fig. 6.

When we compare the proposed system in Case 2 with other similar cancelable biometric systems, the proposed system performs better than most existing methods, except that in [29]. The method in [29] uses a bunch of local structures, and each

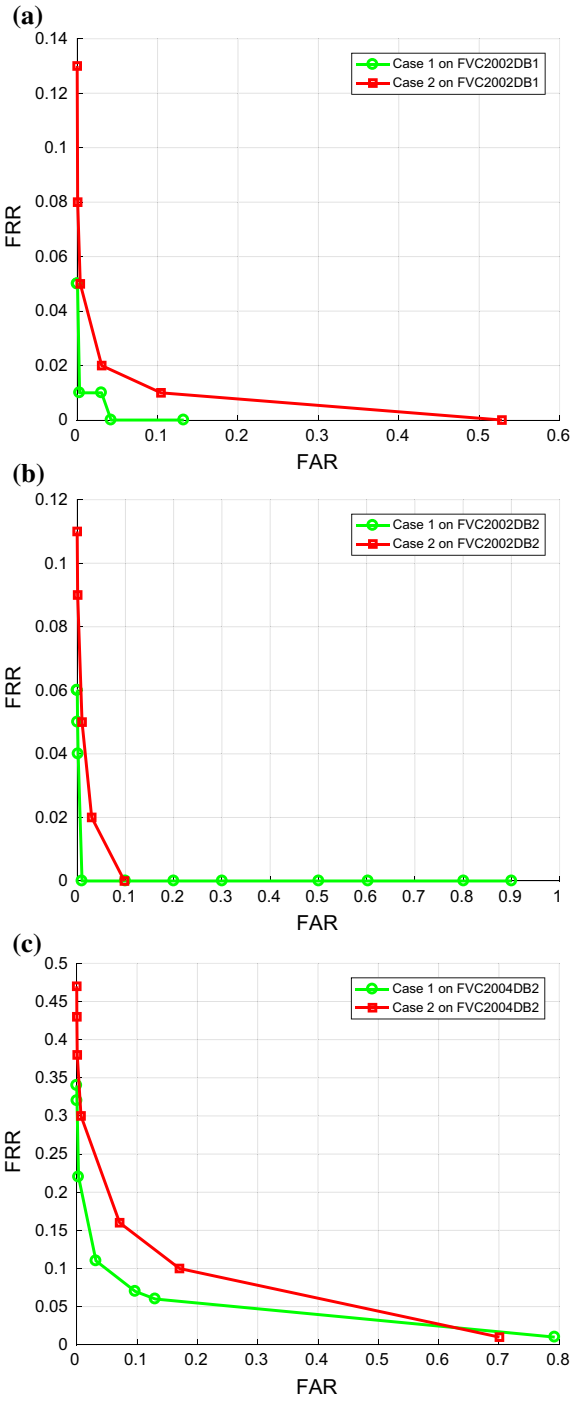

Fig. 6 **a** The ROC curve of the proposed system under Case 1 and Case 2 on Database FVC2002DB1. **b** The ROC curve of the proposed system under Case 1 and Case 2 on Database FVC2002DB2. **c** The ROC curve of the proposed system under Case 1 and Case 2 on Database FVC2004DB2

Table 2 Recognition accuracy (%) of the proposed system in Case 3 with different key lengths

Key length k (bits)	Databases		
	2002DB1+DS2	2002DB2+DS2	2004DB2+DS2
	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)
15	13.00/0	13.00/0	13.00/0
29	16.00/0	16.00/0	16.00/0
36	35.00/0	35.00/0	35.00/0
64	59.00/0	59.00/0	59.00/0

local structure contributes a feature vector. Assume that if the template contains N feature vectors and the query contains M feature vectors, in the matching process a total of $N \times M$ comparisons must be made. Compared with the method in [29], the template or query in the proposed system contains only one feature vector, so only one matching attempt is needed, which is more efficient for practical implementation. Moreover, the proposed system contains an extra expendable layer, which can provide higher security than the method in [29].

The performance of proposed system in Case 3 is listed in Table 2. It can be observed that when the key length k increases, the system performance decreases. For example, when key length k is 15 bits, the performance is FAR $= 0$ and FRR $= 13\%$, while when key length k is 64 bits, the performance decreases to be FAR $= 0$ and FRR $= 59\%$. It shows the compromise between the performance and security level. Also it can be seen that the performance on all the three combined databases is the same. The reason is that in the authentication stage, the key used to generate the transformation matrix has to be retrieved from the fuzzy commitment secure sketch. If the retrieved key is different from that used in the enrollment stage, matching would fail. Therefore, the matching performance of the proposed system tremendously relies on the performance of the expendable layer.

3.2 Security analysis

Two protection layers in the proposed cancelable system are used to secure the biometric template. In the core layer, the fingerprint template is protected by the random projection-based non-invertible transformation. The non-invertible transformation brings about a system of linear equations. To conquer this linear equation system is computationally infeasible for the following reason. The random projection-based transformation represented in Eq. (1) effectively constitutes an underdetermined system of linear equations. Because the projection matrix $\mathbf{M}$ is a $q \times p$ column rank-deficient matrix with q being smaller than p, the rank of matrix $\mathbf{M}$ is $rank(\mathbf{M}) = q$, which is less than the number of unknowns, namely elements of the fingerprint feature $\mathbf{b}_f$. It is a well-known result in linear algebra [33] that when the coefficient and augmented matrixes of Eq. (1) have the same rank, there is an infinite number of solutions for Eq. (1). Clearly $\mathbf{b}_f$ is just one among a large number of solutions,

which makes the search for $\mathbf{b}_f$ tremendously difficult. However, the adversary can only launch the ARM attack by obtaining multiple transformation matrices (which equals to the secret key K) and transformed feature sets (e.g., $\mathbf{y}_f$) from the same original feature set (e.g., $\mathbf{b}_f$). In this case, the expendable layer can provide certain security to protect the secret key. Considering the security provided by the expendable layer, in the fuzzy commitment scheme, the BCH(n, k, t) code is used for error correction. In our application, $n = N_2 = 127$, and k is the length of the partial secret key k. k is a variable and set to be the range of 15–64 bits, which impacts on the system performance, as shown in Table 2. Under the brute force attack, the expendable layer can provide extra security of 15–64 bits to the system if the adversary tries to steal the secret key k. However, with an increase of k, the performance decreases, which shows the compromise between recognition accuracy and system security. When considering the security provided by fuzzy commitment to the face feature vector $\mathbf{b}_c^T$ under the case that the adversary would like to conquer the face modality, by the sphere-packing bound [50], the security provided by a fuzzy commitment is equal to the entropy of $\mathbf{b}_c^T$ by given helper data $\mathbf{H}$, which can be expressed as $H_\infty(\mathbf{b}_c^T|\mathbf{H}) = \log_2\left(2^n / \binom{n}{t}\right)$. The security $H_\infty(\mathbf{b}_c^T|\mathbf{H})$ is variable under different values n and t of BCH(n, k, t). For example, when BCH(127, 15, 27) is used, the security $H_\infty(\mathbf{b}_c^T|\mathbf{H}) = 35$ bits, while when BCH(127, 64, 10) is used, the security $H_\infty(\mathbf{b}_c^T|\mathbf{H}) = 79$ bits.

4 Conclusion

A critical infrastructure may fail to work without a reliable access control system. Such a failure can have dire consequences on the entire infrastructure network because many interdependencies exist between different critical infrastructures. To secure critical infrastructures, in this paper we have proposed an enhanced cancelable biometric system to provide security-tightened access control. Given that a cancelable biometric system is likely to suffer from attacks via record multiplicity (ARM), we design cascading encryption to enhance the security of the fingerprint-based cancelable biometric system (i.e., core layer) by binding the transformation key for non-invertible transformation with the face feature set using fuzzy commitment (i.e., expendable layer). Experimental results show that with just the core layer, our cancelable biometric system performs better than most existing methods and with the addition of the expendable layer, the overall system security is improved at the expense of recognition performance. For future work, we will explore more distinguishing features, e.g., features from iris or finger vein, so as to toughen up the system security while maintaining good recognition performance. Also cancelable biometrics can be applied in other applications [51–53], e.g., body area networks and medical devices, to provide security.

Acknowledgements This paper is supported by Early Career Grant Scheme of ECU of Australia through Project G1003411 and Defence Science and Technology Group (DST) of Australia through Project CERA 221.

References

1. Rinaldi SM, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst 21(6):11–25
2. Brown G, Carlyle M, Salmerón J, Wood K (2006) Defending critical infrastructure. Interfaces 36(6):530–544
3. Yang W, Hu J, Yang J, Wang S, Shu L (2013) Biometrics for securing mobile payments: benefits, challenges and solutions. In: 2013 6th International Congress on Image and Signal Processing (CISP), 16–18 Dec 2013, pp 1699–1704. https://doi.org/10.1109/cisp.2013.6743950
4. Prabhakar S, Pankanti S, Jain AK (2003) Biometric recognition: security and privacy concerns. IEEE Secur Priv 1(2):33–42. https://doi.org/10.1109/MSECP.2003.1193209
5. Cao K, Jain AK (2015) Learning fingerprint reconstruction: from minutiae to image. IEEE Trans Inf Forensics Secur 10(1):104–117
6. Scheirer WJ, Boult TE (2007) Cracking fuzzy vaults and biometric encryption. In: Biometrics Symposium, 2007. IEEE, pp 1–6
7. Juels A, Wattenberg MA (1999) fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference on Computer and Communications Security. ACM, pp 28–36
8. Uludag U, Pankanti S, Jain AK (2005) Fuzzy vault for fingerprints. In: Audio-and Video-Based Biometric Person Authentication. Springer, pp 310–319
9. Teoh ABJ, Kim J (2007) Secure biometric template protection in fuzzy commitment scheme. IEICE Electron Express 4(23):724–730
10. Zhou X, Kuijper A, Veldhuis R, Busch C (2011) Quantifying privacy and security of biometric fuzzy commitment. In: 2011 International Joint Conference on Biometrics (IJCB). IEEE, pp 1–8
11. Kelkboom EJC, Breebaart J, Kevenaar TAM, Buhan I, Veldhuis RNJ (2011) Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. IEEE Trans Inf Forensics Secur 6(1):107–121
12. Yang W, Hu J, Wang SA (2013) Delaunay triangle group based fuzzy vault with cancellability. In: 2013 6th International Congress on Image and Signal Processing (CISP), 16–18 Dec 2013, pp 1676–1681. https://doi.org/10.1109/cisp.2013.6743946
13. Juels A, Sudan M (2006) A fuzzy vault scheme. Des Codes Cryptogr 38(2):237–257
14. Nagar A, Nandakumar K, Jain AK (2008) Securing fingerprint template: fuzzy vault with minutiae descriptors. In: 19th International Conference on Pattern Recognition. IEEE, pp 1–4
15. Narayanan R, Karthikeyan S (2012) Double encryption based secure fuzzy vault construction using fingerprint biometric features. In: 2012 International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME). IEEE, pp 178–182
16. Tams B, Merkle J, Rathgeb C, Wagner J, Korte U, Busch C (2015) Improved fuzzy vault scheme for alignment-free fingerprint features. In: 2015 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, pp 1–12
17. Tams B, Mihăilescu P, Munk A (2015) Security considerations in minutiae-based fuzzy vaults. IEEE Trans Inf Forensics Secur 10(5):985–998
18. Li C, Hu J (2016) A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures. IEEE Trans Inf Forensics Secur 11(3):543–555
19. Neu M, Korte U, Ullmann M (2016) Improvement of fuzzy vault for multiple fingerprints with angles. In: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, pp 1–8
20. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
21. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572
22. Teoh ABJ, Kuan YW, Lee S (2008) Cancellable biometrics and annotations on biohash. Pattern Recogn 41(6):2034–2044
23. Yang H, Jiang X, Kot AC (2009) Generating secure cancelable fingerprint templates using local and global features. In: 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009. IEEE, pp 645–649
24. Lee C, Kim J (2010) Cancelable fingerprint templates using minutiae-based bit-strings. J Netw Comput Appl 33(3):236–246
25. Ahmad T, Hu J, Wang S (2011) Pair-polar coordinate-based cancelable fingerprint templates. Pattern Recogn 44(10):2555–2564

26. Wang S, Hu J (2012) Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. Pattern Recogn 45:4129–4137
27. Wang S, Hu J (2014) Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recogn 47(3):1321–1329
28. Wang S, Deng G, Hu J (2017) A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recogn 61:447–458
29. Wang S, Yang W, Hu J (2017) Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. Pattern Recogn 66:295–301
30. Quan F, Fei S, Anni C, Feifei Z (2008) Cracking cancelable fingerprint template of Ratha. In: International Symposium on Computer Science and Computational Technology, 2008. ISCSCT'08. IEEE, pp 572–575
31. Li C, Hu J (2013) Attacks via record multiplicity on cancelable biometrics templates. Pract Exp Concurr Comput 26:1593–1605
32. Yang W, Hu J, Wang S (2014) The effect of spurious and missing minutiae on Delaunay triangulation based on its application to fingerprint authentication. In: 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2014), China, Xiamen, p 4
33. Kreyszig E (2010) Advanced engineering mathematics. Wiley, New York
34. Blanz V, Vetter T (2003) Face recognition based on fitting a 3D morphable model. IEEE Trans Pattern Anal Mach Intell 25(9):1063–1074
35. Ding C, Tao D (2017) Trunk-branch ensemble convolutional neural networks for video-based face recognition. IEEE Trans Pattern Anal Mach Intell. https://doi.org/10.1109/TPAMI.2017.2700390
36. Nazari S, Moin M-S, Kanan HR (2017) A discriminant binarization transform using genetic algorithm and error-corecting output code for face template protection. Int J Mach Learn Cybern. https://doi.org/10.1007/s13042-017-0723-3
37. Yang M, Wang X, Liu W, Shen L (2017) Joint regularized nearest points for image set based face recognition. Image Vis Comput 58:47–60
38. Pavešić ŠVN (2010) The complete gabor-fisher classifier for robust face recognition. EURASIP J Adv Signal Process 2010:26. https://doi.org/10.1155/2010/847680
39. Riaz F, Silva FB, Ribeiro MD, Coimbra MT (2012) Invariant gabor texture descriptors for classification of gastroenterology images. IEEE Trans Biomed Eng 59(10):2893–2904
40. Ali H, Sharif M, Yasmin M, Rehmani MH (2017) Computer-based classification of chromoendoscopy images using homogeneous texture descriptors. Comput Biol Med 88:84–92
41. Jin ATB, Ling DNC, Goh A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn 37(11):2245–2255
42. Fingerprint Verification Competition (2002). http://bias.csr.unibo.it/fvc2002
43. Fingerprint Verification Competition (2004). http://bias.csr.unibo.it/fvc2004
44. Ortega-Garcia J, Fierrez J, Alonso-Fernandez F, Galbally J, Freire MR, Gonzalez-Rodriguez J, Garcia-Mateo C, Alba-Castro JL, Gonzalez-Agulla E, Otero-Muras E, Garcia-Salicetti S, Allano L, Ly-Van B, Dorizzi B, Kittler J, Bourlai T, Poh N, Deravi F, Ng MNR, Fairhurst M, Hennebert J, Humm A, Tistarelli M, Brodo L, Richiardi J, Drygajlo A, Ganster H, Sukno FM, Pavani SK, Frangi A, Akarun L, Savran A (2010) The multiscenario multienvironment biosecure multimodal database (BMDB). IEEE Trans Pattern Anal Mach Intell 32(6):1097–1111. https://doi.org/10.1109/TPAMI.2009.76
45. Veri Finger SDK, Neuro Technology (2010). http://www.neurotechnology.com/verifinger.html
46. Yang W, Hu J, Stojmenovic M (2012) NDTC: a novel topology-based fingerprint matching algorithm using N-layer Delaunay triangulation net check. In: 2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA). IEEE, pp 866–870
47. Tulyakov S, Farooq F, Mansukhani P, Govindaraju V (2007) Symmetric hash functions for secure fingerprint biometric systems. Pattern Recogn Lett 28(16):2427–2436
48. Jin Z, Jin Teoh AB, Ong TS, Tee C (2011) Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. Expert Syst Appl 39:6157–6167
49. Das P, Karthik K, Chandra Garai B (2012) A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. Pattern Recogn 45(9):3373–3388. https://doi.org/10.1016/j.patcog.2012.02.022
50. MacWilliams F, Sloane N (2006) The theory of error-correcting codes. North-Holland, Amsterdam
51. Chaudhry J, Qidwai UA, Rittenhouse RG, Lee M (2012) Vulnerabilities and verification of cryptographic protocols and their future in wireless body area networks. In: 2012 International Conference on Emerging Technologies (ICET). IEEE, pp 1–5

52. Rittenhouse RG, Chaudry JA, Lee M (2013) Security in graphical authentication. Int J Secur Appl 7(3):347–356
53. Chaudhry J, Farmand S, Islam SM, Islam MR, Hannay P, Valli C (2017) Discovering trends for the development of novel authentication applications for dementia patients. In: International Conference on Applications and Techniques in Cyber Security and Intelligence. Springer, pp 220–237