Multimed Tools Appl (2019) 78:1857–1887
https://doi.org/10.1007/s11042-018-6300-2

Cancelable biometric authentication system based on ECG

Mohamed Hammad[1,2] · Gongning Luo[1] ·
Kuanquan Wang[1]

Received: 3 November 2017 / Revised: 10 June 2018 / Accepted: 22 June 2018 /
Published online: 3 July 2018

Abstract Biometrics are widely deployed in various security systems; however, they have drawbacks in the form of leakage or stealing, therefore numerous solutions have been proposed to secure biometric template such as cancelable biometric, which is one of the possible solutions for canceling and securing biometric template. However, this problem is still open and to the best of our knowledge, few previous studies have proposed a complete authentic system using the cancelable biometric techniques based on electrocardiogram (ECG). In this paper, we have applied two cancelable biometric techniques for developing a human authentication system based on ECG signals. The first one is an improved Bio-Hashing and the second one is matrix operation technique. The improved Bio-Hash technique solves the problem of accuracy loss, which is the main drawback of basic Bio-Hash technique. The protected feature vector (Bio-Hashed code) is generated from the inner product between the ECG features matrix and tokenize number matrix. While the matrix operation technique is applied on the ECG feature matrix to produce a transformed template which is irreversible to the original features of the ECG. In the authentication stage, Feed-Forward Neural Network (FFNN) is used to verify individuals. After applying the two cancelable techniques on three public available ECG databases, experimental results show that the proposed system performs better regarding authentication and outperforms state-of-the-art techniques considered.

Keywords ECG · Cancelable biometrics · Improved Bio-Hashing · Matrix operation · FFNN

✉ Mohamed Hammad
mohammed.adel@ci.menofia.edu.eg

[1] School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang, China

[2] Faculty of Computers and Information, Menoufia University, Menoufia, Egypt

1 Introduction

Electrocardiogram (ECG) is a picture of the electrical conduction of the heart. The ECG signal consists of three main components: P-wave, QRS-complex, and T-wave. The vital characteristics of the ECG signal depend upon its characteristic points' P, Q, R, S and T. The P-wave indicates atrial depolarization, the QRS-complex represents ventricular depolarization and the T-wave indicates ventricular repolarization. Recently, the use of ECG recordings in biometric recognition systems has increased, because ECG characteristics are suitable for human authentication for many reasons such as they are unique and available to all living beings. Some biometrics are unique but could not provide the assurance of the aliveness of the person such as fingerprint and palmprint. It has been observed that ECG based biometric authentication system detects the aliveness of the person, requires low computational cost and easy to record compared to other biometrics [39]. Therefore, ECG technology can be used in many vital applications, for example, physical access control, medical records management, bank accounts, credit cards management, government applications, and forensic applications [26, 32, 43]. A comparative study of different biometric modalities including ECG is presented in Table 1, which is taken according to [27, 44]. Where, there are a lot of privacy and security problems that need to be addressed, like, the loss of ECG data of an individual, ECG sensitivity, and ECG template protection. Because of such issues, an effective method to protect the ECG template is needed by storing it in a special format where the users cannot access them. To address the said issues, the transformation techniques or ECG template protection techniques are required to transform the original ECG data into a new format. There are two main types used for biometric template protection purpose, the cryptosystem which is developed to use a biometric key in cryptography and the cancelable biometric which is discussed in detail in the following section.

The concept of cancelable biometric was first introduced by Ratha et al. [34]. It refers to the intentional and repeatable distortion or transformation of biometric features to make sure the privacy of biometric data. This distortion is modified if cancelable features are compromised and the same biometric is mapped to a new template which could be reused for security applications. In short, such distortion is non-invertible. Therefore, the four objectives of designing any cancelable biometric approach are necessary to follow [3, 41]:

- Diversity: The same cancelable template could not be used across various applications; so many protected templates from the same biometric feature are required.
- Reusability (Revocability): To cancel the current template and reissue another one in case of compromise.
- Non-invertibility: To prevent recovery of original biometric data.
- Performance: The performance of authentication system using the protected template should not deteriorate the performance of authentication system using the unprotected template.

It is difficult to design a cancelable biometric system that satisfies the four objectives above, so template protection is a very challenging task. Nowadays, many solutions have been investigated to design template protection methods which can satisfy the four above objectives, however, this problem is still open, and to the best of our knowledge, few of the previous research has proposed a complete authentication system using the cancelable biometric technique based on ECG. In this paper, ECG features are extracted using Pan-Tompkins

Table 1 Comparative study of different biometric modalities

Biometrics	Uniqueness	Universality	Permanence	Performance	Acceptability
Fingerprint	H	M	H	H	M
Palmprint	H	M	H	H	M
Iris	H	H	H	H	L
Face	H	H	M	H	H
Voice	L	M	L	L	M
Signature	L	L	L	L	H
DNA	H	H	H	H	L
Keystroke	L	L	L	L	M
ECG	H	H	H	H	M

H High, *L* Low, *M* Medium

algorithm [33] and then the ECG template is generated from these features. Two methods are used to protect this ECG template, the first method is the improved Bio-Hashing algorithm, which is proposed by Nanni [28], we modified and applied it to the ECG template, the second algorithm is matrix operations algorithm [31], which is modified and then used for generating cancelable ECG template. The main contributions of this paper are as follows:

- We generated a novel cancelable ECG template for human authentication system based on two methods, improved Bio-Hashing and matrix operation, which are much more secure than other cancelable methods.
- We modified the improved Bio-Hashing method [28], by changing some details (discussed in Section 3.2) to enhance the accuracy, and then we applied it to the ECG template.
- We modified the matrix operation method [31], by changing some steps (discussed in Section 3.3) and then we used it for generating the cancelable ECG template.
- We overcome the main drawbacks of the Bio-Hashing method in the worst case that always an impostor steals the Hash key by using the improved Bio-Hashing method.
- We overcome the main drawbacks of the Improved Bio-Hashing method in case if an impostor tries to perform a "brute force attack" to cause a false accept by combining the Improved Bio-Hashing method with aliveness detection system (ECG system).
- We used Feed-Forward Neural Network (FFNN) classifier for authentication to improve the performance.

Finally, the proposed system based on the proposed two methods is compared with some existing approaches on ECG biometric and several biometric traits. Results show that the accuracy of the proposed method is better than other methods for authentication. The main advantage of this paper is that we combined a feature transformation method with aliveness detection system (ECG system) to avoid spoofing using fake data which is one of the main drawbacks of the Bio-Hashing and some improved Bio-Hashing algorithms, and in case if the imposter steals the Hash key and uses information about the transformation or if both the biometric data and the key are stolen, the matcher can be spoofed.

This paper is organized as follows: In Section 2 an overview of the existing approaches for cancelable biometric is given, Section 3 illustrates the proposed method on a cancelable biometric system based on the ECG signals, in Section 4 experimental results are presented and aimed at comparing the performance of state-of-the-art authentication techniques with our proposed method for testing the advantages in authentication system, finally, Section 5 concludes the paper with future work. The major symbols used in this paper are summarized in Table 2 for easy reference.

2 Related works

Cancelable biometric approaches have been categorized into two main types, referred to as biometric salting and non-invertible transformation.

2.1 Biometric salting

In the biometric salting, the original information can be recovered by applying the inverse transformation. This can be done by giving a key or password to the user. But it becomes less secure than non-invertible transformation.

Bio-Hashing is a method of biometric salting proposed by Teoh et al. [40], in which biometric features are combined with a Tokenized Random Number (TRN) to generate Bio-Hash codes. Figure 1 illustrates the Bio-Hashing process. At the enrolment stage, auxiliary data is used to generate a user specific random matrix. The columns of this matrix are ortho-normalized using Gram-Schmidt ortho-normalization process, and the original biometric feature is transformed by projecting it along the columns of the ortho-normalized random matrix. The transformed template is then binarized to generate Bio-Hash code by comparing it with a fixed threshold value. Instead of the original biometric, the generated Bio-Hash code is stored in the database, and the user-specific random data is provided to the enrollee as a token. For positive authentication a genuine user needs to provide his/her original biometric data and the token. In case the stored Bio-Hash code is intercepted, a new one can be generated by changing the token. An individual can have many Bio-Hash codes for different applications by having various tokens. Bio-Hashing was reported to achieve nearly zero Equal Error Rate (EER) for the modalities which are a substantial increase in performance. But, if an adversary gains access to the transformed template and random data (token stolen), he can generate a coarse approximation of the original template as this process is invertible. Hence, the security of the data may be compromised and performance regresses. To deal with the problems of Bio-

Table 2 Notations and symbols

Symbol	Definition
f	Input feature vector, $f \in \Re^n$
b	Bio-Hash code (bit vector), $b \in \{0, 1\}^m$
m	The length of the bit string ($m \leq n$)
r	A set of pseudo-random vectors $r_i \in \Re^n, i = 1, \ldots, m$
O_i	An orthonormal set of vectors, $i = 1, \ldots, m$
τ	A preset threshold.
N	The selected number of projection spaces or the iteration number of the Bio-Hashing method on the same ECG vector.
n	Feature vector dimension.
K	Hash key.
k	Number of ECG feature vectors.
C	ECG cancelable vector.
x	Test feature vector, $x \in \Re^n$

Hashing method, Lumini and Nanni [28] proposed several solutions leading to an improved version of the Bio-Hashing method as shown in Fig. 2.

The basic idea was to iterate N times the Bio-Hashing method to generate N Bio-Hash codes per user. Also, before applying the Bio-Hashing method, they normalized each biometric vector by its module. Moreover, they used several values for $\boldsymbol{\tau}$ instead of a fixed one. The result is compared to the Hamming distance and the verification task was performed by training a classifier for each Bio-Hash code and combining these classifiers by the sum rule.

The following are some of the most relevant approaches belonging to cancelable biometric type using the Bio-Hashing technique. Teoh et al. [14] proposed a Bio-Hashing method based on iterated inner products between the tokenized pseudo-random number and the user-specific fingerprint features. By using this method, there is no deterministic way to get the user-specific code without both tokens with random data and user fingerprint feature, thereby providing high protection to the biometric and external factors. Connie et al. [4] proposed palm-hashing (palmprint + hashing) technique for cancelable biometric to solve the non-revocable biometric issue. For which, hashing method is applied on palmprint template with a set of pseudo-random keys to generate palm-hash code that can be stored in many portable devices for verification. The literature on cancelable biometric approaches is vast; however, there is very little research working on cancelable ECG using biometric salting method. One of the previous methods that generated Bio-Hashing code from ECG features was proposed by Dey et al. [7]. This algorithm can be detailed as follows:

A. Detect P, QRS and T peaks by modifying Pan-Tompkins algorithm.
B. Extract and measure ECG features (time duration) from the detected peaks are P-P, Q-Q, R-R, P-R, S-S, T-T, Q-T, Q-Tc and QRS complex.
C. Generate the feature matrix with size 6 × 8 from the ECG detected features, where number 6 refers to the number of input ECG signals and number 8 refers to the number of features shown in Table 1.
D. A tokenized number is randomly generated.
E. Compute the inner product between the ECG feature matrix and the matrix of tokenized number.
F. Finally, compute the Bio-Hash code from the result of the inner product as

$$b_i = \left\{ \begin{array}{ll} 0 & \text{if } \mathrm{prod_i} \leq \tau \\ 1 & \text{if } \mathrm{prod_i} > \tau \end{array} \right\}$$

Where the resulting bit vector $\boldsymbol{b}$ is the Bio-Hash code, **prod** is the result of inner product vector and $\boldsymbol{\tau}$ is a pre-defined threshold.

Thus, the Bio-Hash code can perform authentication of the subjects. According to authors, this method is less susceptible to noise, however, the database used was small and it would be useful to apply this method to a larger set of records to prove its performance. Besides, they do not present results regarding the authentication performance. Also, in [8], Dey et al. generated Bio-Hashing code from ECG features but the inner product is performed between the ECG features matrices that are obtained from two different individuals located remotely. These methods based on Bio-Hashing have various drawbacks [29, 42]. One of the main drawbacks of Bio-Hashing method is the low accuracy in the case when the Hash key is stolen by an imposter. Recently, several methods have been proposed to solve this limitation by improving the Bio-Hash method as in [28].

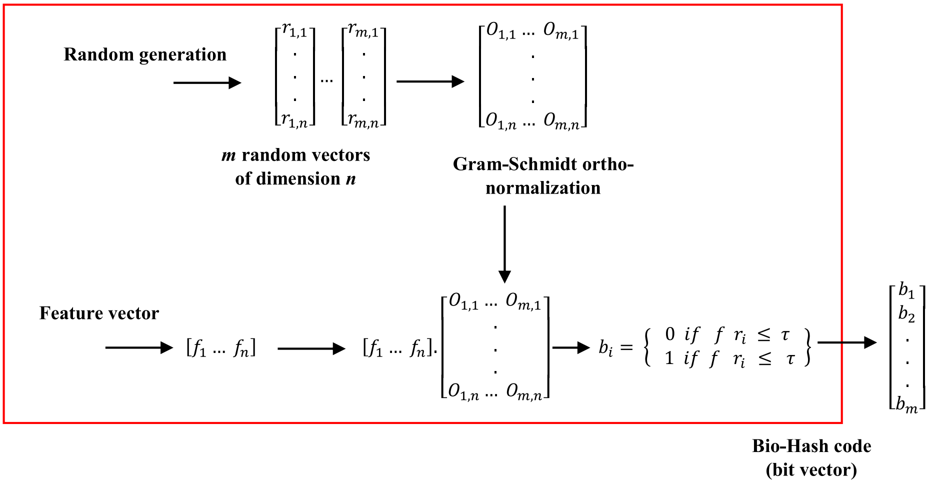

Random generation
m random vectors of dimension n
Gram-Schmidt ortho-normalization
Feature vector
$[f_1 \dots f_n]$
$b_i = \{ 0 \text{ if } f\ r_i \le \tau;\ 1 \text{ if } f\ r_i \le \tau \}$
Bio-Hash code (bit vector)

Fig. 1 The bio-hashing method

2.2 Non-invertible transformation

In non-invertible transformation, the whole recognition process is performed in transformation space and not in the original space. If the transformation is compromised, it is still difficult to reconstruct the biometric data by an impostor.

One of the non-invertible transformation method is matrix operation method [31]. The main aim of using matrix operation method for generating cancelable biometric template is the production of a reliable revocable biometric template. This method consists of three matrices operations, inverse operation, the elementary row operations (ERO) and the Kronecker product (KP) operation. These operations are used to protect and authorize personal information from

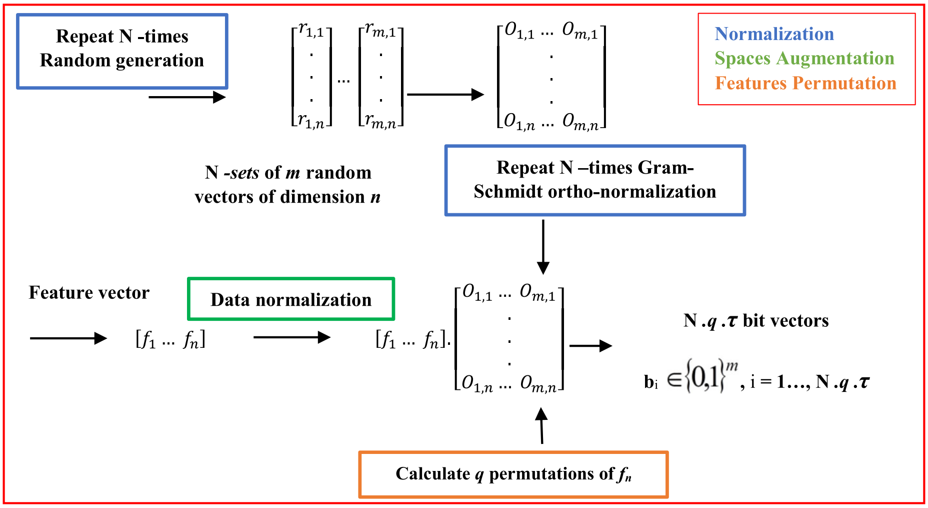

Repeat N -times Random generation
N -sets of m random vectors of dimension n
Repeat N –times Gram-Schmidt ortho-normalization
Normalization
Spaces Augmentation
Features Permutation
Feature vector
Data normalization
$[f_1 \dots f_n]$
N .q .τ bit vectors
$b_i \in \{0,1\}^m$, i = 1…, N .q .τ
Calculate q permutations of f_n

Fig. 2 The Improved bio-hashing method

an impostor by randomizing the original biometric feature to generate a cancelable biometric template. The three operations are able to satisfy the three requirements of non-invertible matrices:

A. At least one row of the matrix should be of zero value.
B. It must be ensured that there is a row that is a multiple of another row.
C. Finally, the original matrix must be modified into a non-square matrix form.

Points 'A' and 'B' can be achieved using ERO, where the selected row is multiplied by zero to achieve the point A. Meanwhile, for the point B, it is rare to find a row which is a multiple of another row; hence, it can be created using ERO. The Kronecker product (KP) operation is used [13] to meet the last point for the non-invertible matrix, this can be achieved by multiplying each element of the transformed matrix with an arbitrary matrix/element. The process to build the cancelable biometrics template using an input matrix *A* are as follows: Firstly, matrix *A* will be inverted. In the next step, the inverted matrix goes through a KP operation to produce a KP matrix. In this KP operation, the inverted matrix will be multiplied by a tensor factor that can be in the form of a matrix or integer with a constant value called B. After that, the ERO is used to determine how many zero rows to achieve the required maximum non-invertible matrix and also used to create rows that are the multiples of other rows. After implementing the ERO operation, the result of this process will be a cancelable matrix of matrix A (a cancelable template). The outline of the matrix operation method is as shown in Fig. 3.

Many previous approaches worked on cancelable biometric using non-invertible transformation method, such as the approach presented by Ratha et al. [34], which uses three non-invertible transformation functions (Cartesian transformation, polar transformation and surface folding transformation) to transform the fingerprint data. Leng et al. [20], proposed a method called $(2D)^2$RP (two-directional two-dimensional random projection) for feature extraction of face and palmprint. They also fused this method with principal component analysis (PCA) and linear discriminant analysis (LDA), which can play complementary advantages. Although this method has much less storage and computational cost, it requires more coefficients and computational time than our method. Leng et al. [22], also proposed two-dimensional (2D) cancelable biometric scheme namely $(2D)^2$FSRP and $(2D)^2$PSRP to generate 2D cancelable face and palmprint, which play complementary advantages by fusing 2DSRP and 2DPCA/2DLDA. Although the computational cost of this method is less than one-dimensional methods, it needs a mass of coefficients to represent cancelable biometric template. Besides, the verification performance of this method is less than our method. Ang et al. [2] generated cancelable fingerprint templates based on geometric transformation. Sadhya et al. [35] proposed a cancelable biometric template protection for fingerprints based on cryptographic hash functions and other state-of-art cancelable biometrics [11, 16, 17, 21, 23, 24, 25]. However, few previous studies have worked on cancelable ECG using non-invertible transformation method. One of these studies is Kim et al. [19], which proposed a cancelable ECG biometrics using generalized likelihood ratio test (GLRT), also they proposed a guided filtering (GF) with irreversible guide signal for performance degradation due to the cancelable scheme. In this work, we focus on one of the biometric salting method called improved Bio-Hashing and a non-invertible method using mathematical operations, which discussed in the following section.

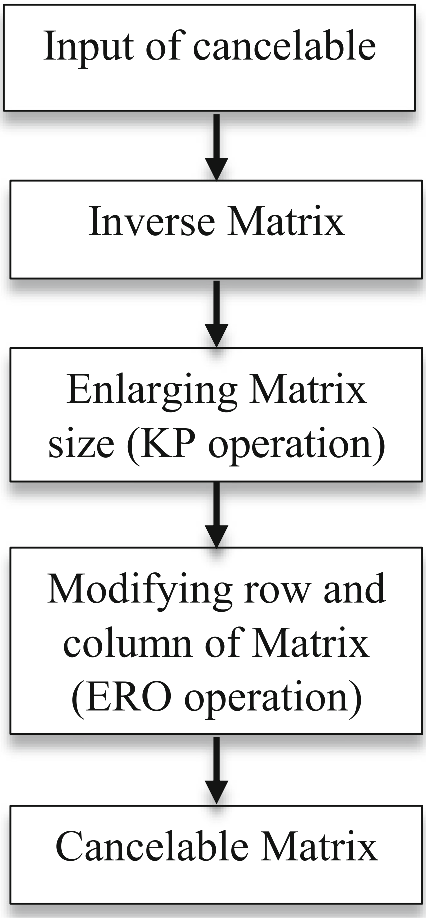

Input of cancelable
Inverse Matrix
Enlarging Matrix size (KP operation)
Modifying row and column of Matrix (ERO operation)
Cancelable Matrix

Fig. 3 The outline of matrix operation method

3 Proposed cancelable biometric system based on ECG

This section presents the detail about the proposed cancelable biometric system using ECG signals for human authentication. First, to extract the features of ECG signals, efficient feature extraction algorithms have been proposed in recent years and a good overview of existing features and analysis of their performances could be found in [12]. However, we used the same feature extraction algorithm (Pan-Tompkins algorithm [33]) used in the work of Dey et al. [7] and extract the same features with different sizes to get an actual comparison term between this algorithm and the proposed algorithm. Second, after extracting the features, we used two techniques the improved Bio-Hashing and the matrix operation to protect the ECG features template. Finally, FFNN is used to complete the authentication system.

3.1 ECG feature extraction algorithm

Pan-Tompkins algorithm is used to extract the features of ECG signals. This algorithm comprises the following steps to extract the ECG features. First, the band-pass filter is used to reduce the effect of noise on the ECG. Second, we obtained the high slope using differentiation equation. The next step performed squaring the signal to detect QRS-complex (the high-frequency component), P and T waves (the low-frequency components). Finally, we performed integration sum to extract the slope of R-wave. In this study, we used the same features in [7] to provide a fair comparison between the proposed method and the work in [7]. Table 3 shows the description of all features that used in this paper. The feature matrix is generated with size M × 8 features, where M is the number of input ECG signals.

3.2 Cancelable ECG using improved bio-hashing

In this paper, as a solution to the problem of Bio-Hash algorithm that was proposed by Dey et al. [7] and to make the Bio-Hashing procedure more robust against the possible stealing of the Hash key by an impostor, we modified the improved version of Bio-Hashing based on the ensemble of matchers [28]. The modification is done by changing some details as follows:

- We modified the Improved Bio-Hashing method to fit the ECG based authentication, which decreases the false acceptance that happens when the impostor tries to perform a "brute force attack".
- We neglected the step "Features Permutation", which decreases the implementation time.
- We compared the results by Feed Forward Neural Network (FFNN) algorithm instead of using Hamming distance to improve the performance.

As well some changes in the methodology reported above [7] and these changes are as follows:

1. We used the modified improved Bio-Hashing method instead of the base Bio-Hashing method.
2. We applied this method to a larger data records.
3. Unlike the work in [7], we presented results regarding the authentication performance and the Equal Error Rate (EER) was computed.

After doing the previous modifications, the proposed system is summarized as below:

A. Pan-Tompkins algorithm was applied to detect and extract QRS-peaks, Q-T, R-R, P-R, S-S, P-P, Q-Q and T-T intervals.
B. Using Blum-Blum-Shub method to generate pseudo-random bit/number.
C. Iterate N times the Bio-Hashing method to generate N Bio-Hash codes per user.

Table 3 Description of ECG features

Feature Number	Description of features
1	P-P intervals
2	P-R intervals
3	Q-Q intervals
4	R-R intervals
5	Q-T intervals
6	S-S intervals
7	T-T intervals
8	QRS complex

D. Normalize each biometric vector by its module before applying the Bio-Hashing procedure.
E. The verification task was performed using Feed Forward Neural Network (FFNN) algorithm to verify the individuals.
F. Using larger database and the Equal Error Rate (EER) was computed.

Figure 4 shows the proposed cancelable authentication system using improved Bio-Hashing method, step (a) shows the enrollment stage to generate the cancelable matrix for the input features and store it in the database, step (b) shows the authentication stage for one test ECG signal and compare it with the cancelable template using FFNN to decide if this individual accepts or rejects. In enrollment stage, the features of the ECG signals (input signals) were extracted using Pan-Tompkins algorithm. Then, each feature vector was normalized using the Gram–Schmidt ortho-normalization to transform the feature vector into an ortho-normal set of vectors (or$_n$) and produce the normalization feature matrix. After that, N-sequences of real numbers were generated using Blum-Blum-Shub method to produce a set of pseudo-random vectors with the uniform distribution. The Blum-Blum-Shub generator appears to be as secure as other encryption techniques, such as RSA encryption [9]. Moreover, this method is robust and very sensitive to small changes in key so even with the knowledge of the key approximate values; there is no possibility for the attacker to get the features. In this work, $d = 7603$ and $a = 7487$ were used to calculate $z = d \times a = 56{,}923{,}661$, and $s = 7817$ used to calculate $x_0 = s^2 \ mod \ z$. Where, d and a, are two k-bit random prime numbers and $s \in R[1, z - 1]$ is the random seed. The next step, N-normalize vectors were generated from the pseudo-random vectors. Lastly, the inner product was computed between the normalized feature matrix and the normalized random matrix to generate the cancelable matrix template. The Hash key (K) was given to a user during enrollment and was different among different users. In authentication stage, the individual who needs to verify should enter the personal Hash key (K), then the feature vector was extracted from the ECG signal (the test signal) and normalization was done on this vector. The inner product was computed between the normalized feature vector and the personal Hash key (K), and the result of the product was compared with the cancelable template. Finally, authentication was performed using FFNN, and then decided if this user is accepted or rejected.

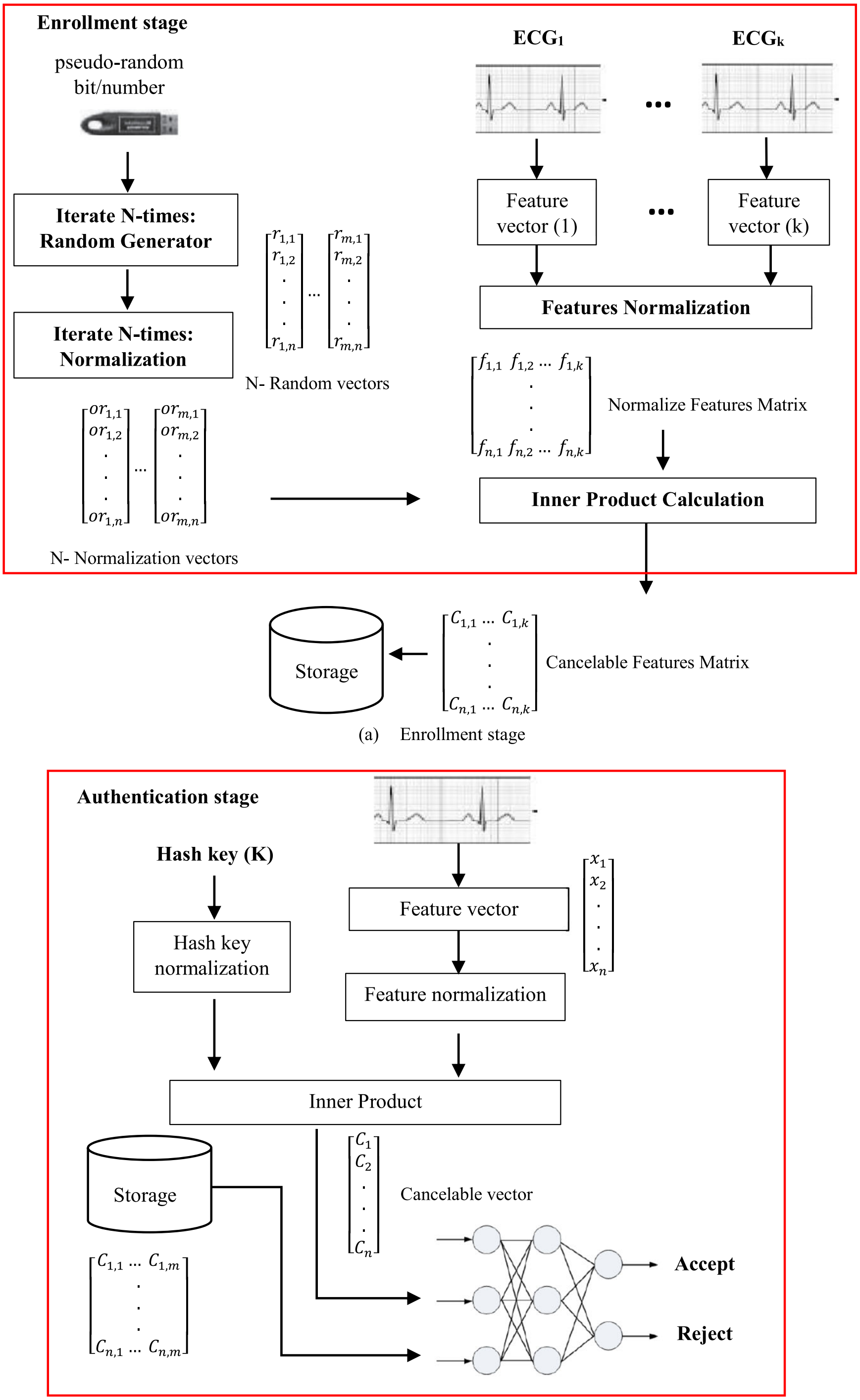
3.2.1 Gram–Schmidt ortho-normalization

In this paper after lots of experiments, we found that Gram-Schmidt ortho-normalization is the optimal normalization method for ECG data and has much less time cost than other methods such as Z-score normalization, Min–max normalization and Median normalization [6]. We apply the Gram-Schmidt process to the features (x) and normalize it into interval [−1,1], we can compute the orthogonal function as follows:

Let V be a vector space with an inner product. Suppose $x_1, x_2, \ldots, x_n$ is a basis for V then,

$$\begin{gathered} V_1 = x_1, \\ V_2 = x_2 - \frac{x_2 . V_1}{V_1 . V_1} V_1, \\ \cdots \\ V_n = x_n - \frac{x_n . V_{n-1}}{V_{n-1} . V_{n-1}} V_{n-1} \end{gathered} \tag{1}$$

Where, $V_1, V_2, \ldots, V_n$ is an orthogonal basis for V.


Enrollment stage
pseudo-random bit/number
Iterate N-times: Random Generator
Iterate N-times: Normalization
$r_{1,1}$ $r_{1,2}$ $r_{1,n}$ … $r_{m,1}$ $r_{m,2}$ $r_{m,n}$
N- Random vectors
$or_{1,1}$ $or_{1,2}$ $or_{1,n}$ … $or_{m,1}$ $or_{m,2}$ $or_{m,n}$
N- Normalization vectors
ECG₁
ECGₖ
Feature vector (1)
Feature vector (k)
Features Normalization
$f_{1,1}$ $f_{1,2}$ … $f_{1,k}$ $f_{n,1}$ $f_{n,2}$ … $f_{n,k}$
Normalize Features Matrix
Inner Product Calculation
Storage
$C_{1,1}$ … $C_{1,k}$ $C_{n,1}$ … $C_{n,k}$
Cancelable Features Matrix
Authentication stage
Hash key (K)
Hash key normalization
Feature vector
x_1 x_2 x_n
Feature normalization
Inner Product
Storage
$C_{1,1}$ … $C_{1,m}$ $C_{n,1}$ … $C_{n,m}$
C_1 C_2 C_n
Cancelable vector
Accept
Reject

(a) Enrollment stage

(b) Authentication stage

Fig. 4 Block diagram of the proposed system using improved bio-hashing method

3.3 Build cancelable ECG using an input feature matrix

In this study, we modified the matrix operation method by changing and adding some steps as follows:

- We utilized the matrix operations for generating the cancelable ECG template.
- We started with ERO operation instead of KP operation, which gives better performance.
- We presented results regarding the authentication performance and EER was computed.

The matrix operations were used on the ECG to produce a transformed template of ECG which is irrevocable to the original signal of ECG. The proposed matrix operation method is shown in Fig. 5, whereas the input of cancelable is the ECG features matrix from the feature extraction algorithm.

We built the cancelable ECG system using an input features matrix *I* by the following steps:

- First, matrix *I* will be inverted to change the original features using the pseudo-inverse algorithm.
- Apply ERO to the inverted matrix to obtain a zero-value row.
- Create rows that are the multiples of other rows using ERO.
- Create tensor factor.
- Doing KP operation between the output matrix after doing ERO and the tensor factor to produce a KP matrix.
- The result will be the cancelable matrix of the input features matrix *I*.
- Finally, the authentication task is performed by training the cancelable matrix with FFNN and the EER is computed.

Figure 6 shows the original features of an ECG signal in plot (a) and the cancelable features of an ECG signal in plot (b) using Matrix operation algorithm.

3.3.1 Inverse operation

Moore–Penrose pseudo-inverse described by E. H. Moore [1] is used to inverse the input ECG feature matrix. The pseudo-inverse is applied to all matrices (square and non-square matrices) whose entries are real or complex numbers. So, square form of input feature matrix does not need to be processed in all matrices operations. The calculation of right inverse matrix can be computed as eq. 2:

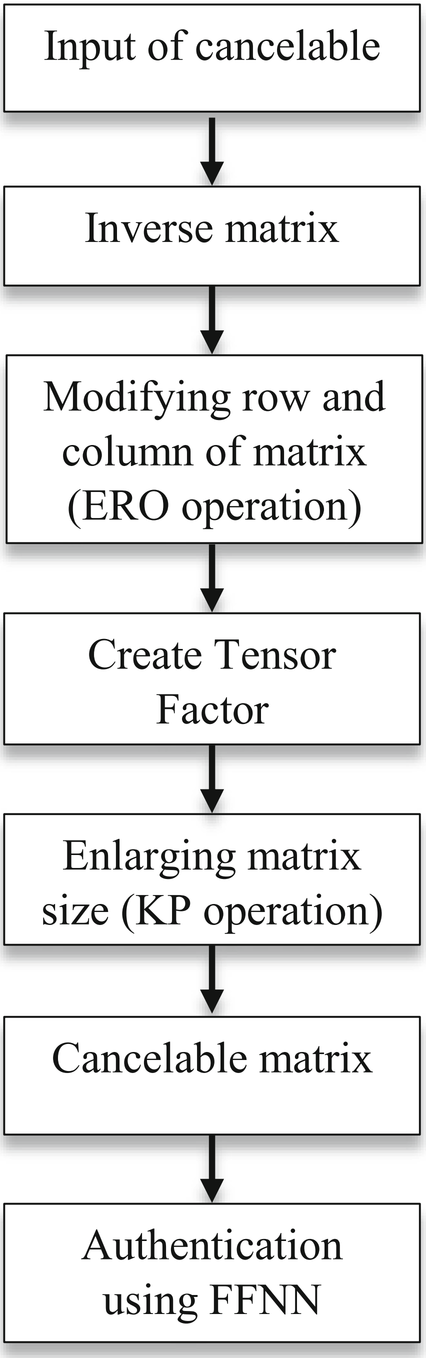
$$A^{-1} = A^T\left(AA^T\right)^{-1} \tag{2}$$

Where A^{-1} is the input matrix after inverse and A^T is the transpose of the input matrix *A*.

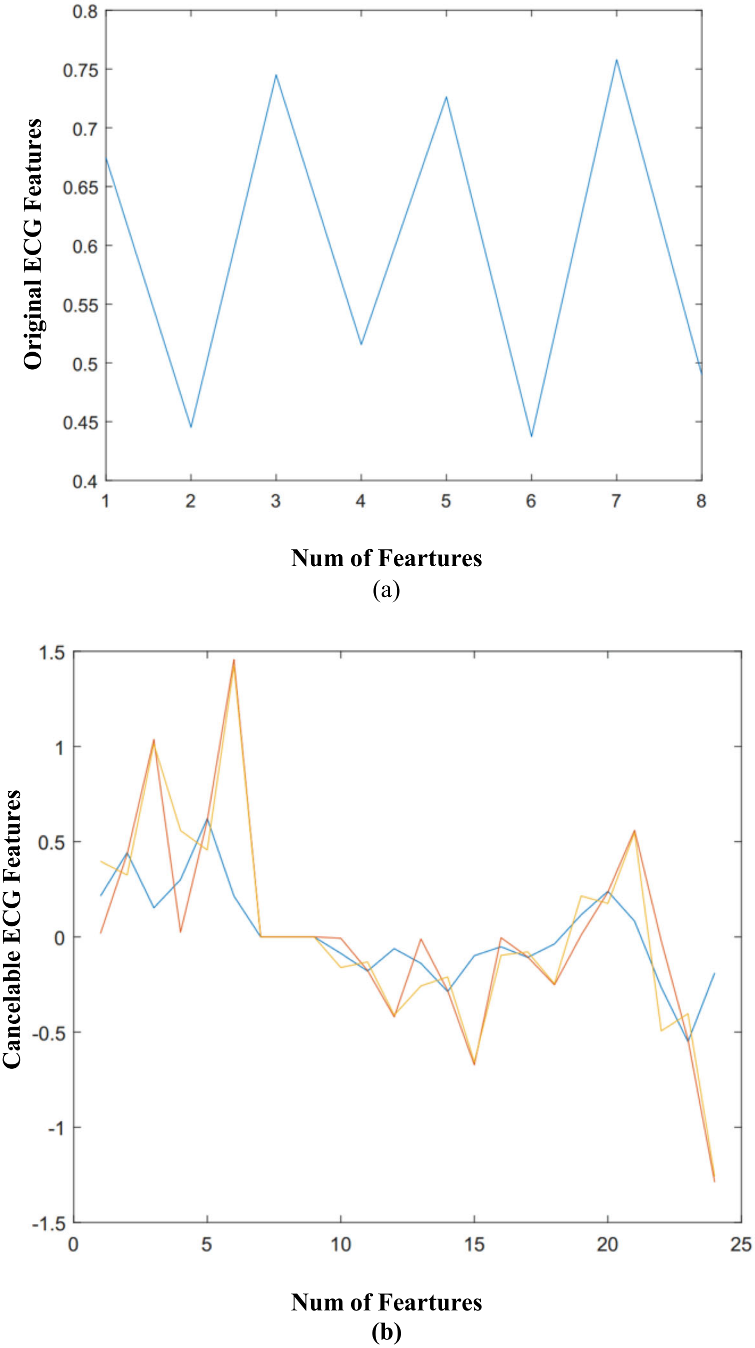
3.3.2 Elementary row operations (ERO)

Generally, Elementary Row Operations (ERO) can be defined as a multiplication and addition force that is imposed on the matrix rows. The three operations corresponding to the operations in rows of EROs are multiplied in the following:

Fig. 5 The proposed system using matrix operation method


Input of cancelable
Inverse matrix
Modifying row and column of matrix (ERO operation)
Create Tensor Factor
Enlarging matrix size (KP operation)
Cancelable matrix
Authentication using FFNN

a. Multiply a row by a non-zero constant.
b. Interchange two rows
c. Add constant m times one row to another.



(a)

(b)

Fig. 6 The original features in (a) and the cancelable features in (b) using matrix operations method

The purpose of these operations is to acquire a solution in algebra or to obtain a new form of a matrix.

3.3.3 Kronecker product (KP)

Given $m \times n$ matrix A and a $p \times q$ matrix B, their Kronecker product $R = A \otimes B$, also called their matrix direct product, is an $(m\,p) \times (n\,q)$ matrix with elements defined as the matrix:

$$R = \begin{bmatrix} a_{11}B \ldots a_{1n}B \\ \vdots \\ a_{m1}B \ldots a_{mn}B \end{bmatrix} \in R^{mp \times nq}$$

Where B ⊗ A ≠ A ⊗ B.

Figure 7 shows the result of KP operation between two square matrices (A and B) and between one square and one non-square matrix (A and C).

3.4 FFNN

Artificial Neural Networks (ANNs) is well-suited for the construction of an authentication system based on it. In the proposed system, the neural network was assembled using the pattern recognition toolbox in MATLAB software. The network used for authentication is Feed-Forward Neural Network (FFNN) as shown in Fig. 8. In this network, tangent-sigmoid function is used as a transfer function for the hidden layer and the linear function is used as a transfer function for the output layer, these functions work better in Neural Network (NN) where speed is more important. The Levenberg-Marquardt algorithm is used to train the network, where this algorithm supports training with validation and test vectors. The validation vectors are used to stop training early when the network is reached to the maximum epochs or to the performance that is minimized to the goal, the test vectors are used to check whether the network generalizes well. As shown in Fig. 8, the best validation performance in this network achieved at iteration 7. The input layer consisted of input nodes for each input of the corresponding ECG signals from the dataset. The number of nodes in the hidden layer was altered for optimization through trial-and-error. The output layer consisted of two output nodes that correspond to each of the specific conditions being examined. To choose the number of nodes in the hidden layer and how it affects our experimental results, we compute the mean-squared error (MSE) of the network analysis corresponds to the number of nodes in the hidden layer for different networks as shown in Fig. 9. From Fig. 9, we observed that the MSE was minimized when the hidden layer was composed of 5 nodes. The proposed network is created

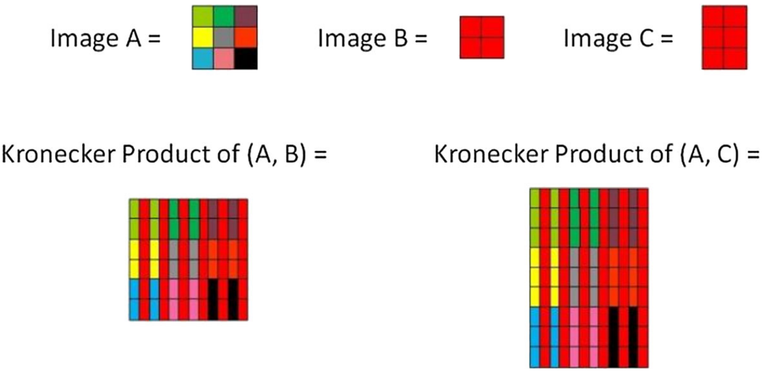
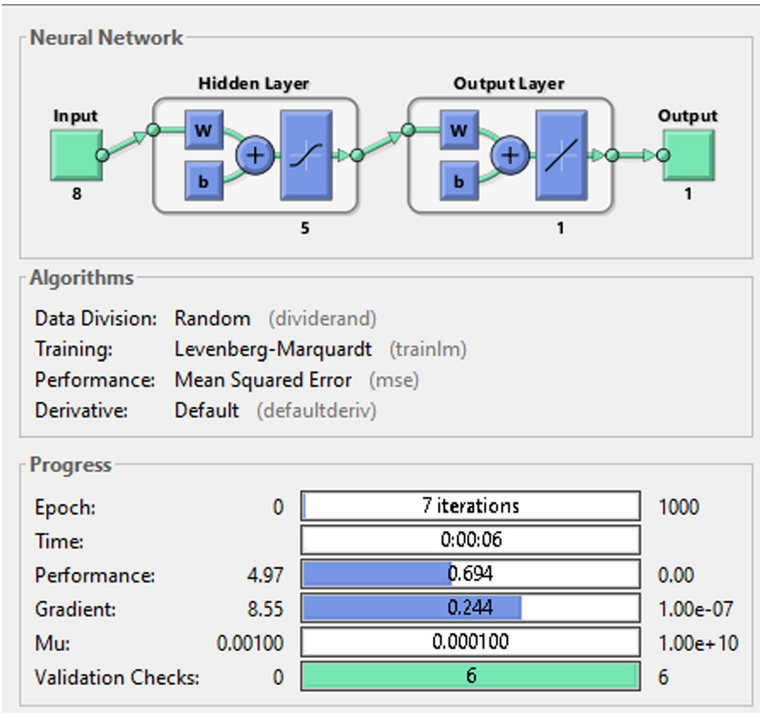


Fig. 7 KP operation



Algorithms

Data Division:	Random (dividerand)
Training:	Levenberg-Marquardt (trainlm)
Performance:	Mean Squared Error (mse)
Derivative:	Default (defaultderiv)

Progress

Epoch:	0	7 iterations	1000
Time:		0:00:06	
Performance:	4.97	0.694	0.00
Gradient:	8.55	0.244	1.00e-07
Mu:	0.00100	0.000100	1.00e+10
Validation Checks:	0	6	6

Fig. 8 The proposed neural network

with 8 features for input layer, one hidden layer of 5 nodes and one output layer with two nodes (accept or reject), the network is simulated and trained for 70 epochs. In this study, we

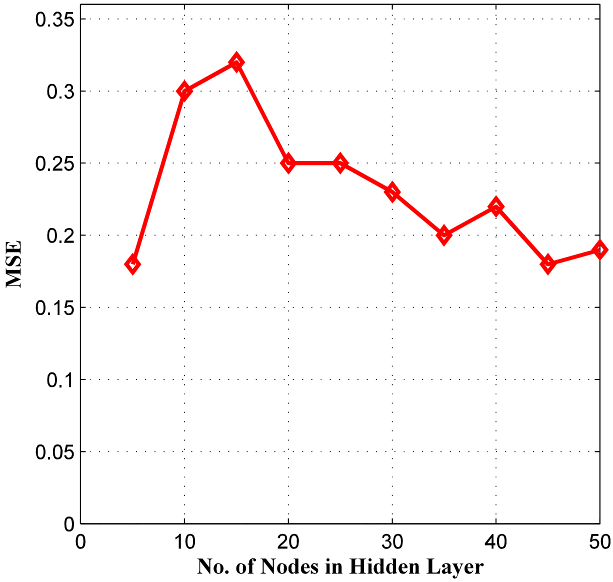


Fig. 9 MSE of different number of nodes in hidden layer

worked on 5 nodes hidden layer because it takes the lowest MSE value comparing with other cases. Figure 10 shows the structure of the proposed multilayer perceptron network with one hidden layer, in this Figure, the activation function (g) is used in the hidden layer and the activation function (P) is used in output layers [30]. The superscript of ***n***, ***θ***, or ***w*** refers to the first layer (hidden layer) or the second layer (output layer) in Fig. 10. The output, $\boldsymbol{y_i}$, $\boldsymbol{i}$ = 1 or 2, the network is calculated as eq. 3:

$$y_i = P\left[\sum_{j=1}^{5} w_{ij}^{(2)}\, g\left(n_j^{(1)}\right) + \theta_i^{(2)}\right] = P\left[\sum_{j=1}^{5} w_{ij}^{(2)}\, g\left(\sum_{k=1}^{8} w_{ij}^{(1)}\, x_k + \theta_j^{(1)}\right) + \theta_i^{(2)}\right] \quad (3)$$

4 Experimental results

In this section, we evaluate the performance of the proposed system for authentication and prove that the proposed system is better than the previous system in [7]. All the experiments are executed in a PC with 4 Intel Core i5 CPUs (2.50GHz) and 4 GB RAM and the algorithm was implemented using MATLAB software R2016a. The capability of using the proposed cancelable system was examined on three databases to show that the proposed cancelable system is not restricted for a single database. We randomly selected the ECG samples for the training and the testing data sets and we evaluated the final statistical results after 5 runs.

4.1 Dataset

4.1.1 MIT-BIH arrhythmia dataset

It contains forty-eight records obtained from forty-seven subjects. The subjects were 25 men aged thirty-two to eighty-nine years, and 22 women aged twenty-three to eighty-nine years. The recordings were digitized at 360 samples every second per channel with 11-bit resolution over a 10-mV range [10]. Table 4 shows the number of beats in each record from this database.

4.1.2 PTB dataset

The database contains 549 records from 290 subjects. Each subject is represented by one to five records. Each record includes 15 simultaneously measured signals: the conventional 12 leads together with the 3 Frank lead ECG signals. Each signal is digitized at 1000 samples per second, with 16-bit resolution over a range of ±16.384 mV. On special request to the contributors of the database, recordings may be available at sampling rates up to 10 KHz [10].

4.1.3 CYBHi dataset

This database is provided by the Check Your Biosignals Here initiative [5]. Collecting data from 65 subjects (49 males and 16 females) with an average age of 31.1 ± 9.46 years. Subjects were only asked to rest their left/right hands in a setup built for this proposes. The recordings available at sampling rates 1 KHz 12-bit resolution. Table 5 summarizes the specifications of the three databases that used in this paper.

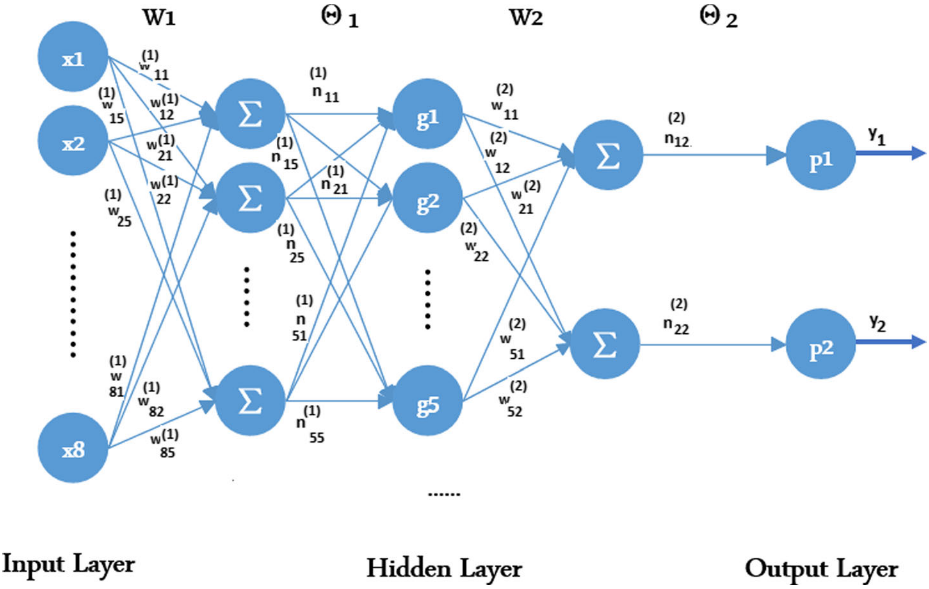


Fig. 10 Multilayer perceptron network with one hidden layer

4.2 Performance analysis

To evaluate the performance of authentication, the following metrics are used:

- False Acceptance Rate (FAR): It is the probability of an imposter being accepted as an authorized user and defined as the ratio of the number of False Acceptances to the number of authentication attempts at eq. 4:

$$FAR = \frac{FP}{TN + FP} \tag{4}$$

- False Rejection Rate (FRR): It is the probability of a legitimate user being rejected as an imposter and defined as the ratio of the number of False Rejections to the number of authentication attempts at eq. 5:

$$FRR = \frac{FN}{TP + FN} \tag{5}$$

- Precision: Represents the proportion of true positives retrieved amongst all classified positives, which defined as:

$$Precision = \frac{TP}{TN + FP} \tag{6}$$

- Recall: Represents the proportion of true positives retrieved amongst all the real positives, which defined as:

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

- Equal Error Rate (EER): is a biometric security system algorithm used to predetermining the threshold values for its false acceptance rate and its false rejection rate.

Where, False Positive (FP) is the number of imposter acceptance, True Negative (TN) is the number of imposter rejection, False Negative (FN) is the number of legitimate rejection and True Positive (TP) is the number of legitimate acceptance.

4.2.1 Evaluation of improved bio-hash algorithm requirement

Number of Iterations (N) This parameter is considered in the performance of the system using improved Bio-Hash algorithm. The Bio-Hashing method is iterated N time on the same ECG vector to obtain N bit vectors b_i, $i = 1, \ldots, N$. In this paper, after doing a lot of tests using different values of N ($N = 3,4,5$ and 6) we found that the best performance of the algorithm is when the iteration number is at $N = 5$. Table 6 shows the EER and FAR of the algorithm using different N values in case of training data 70 and 30% for testing data, where FRR = 0.

The parameter (m) This parameter is critical to maximize the performance of the system using improved Bio-Hash algorithm. The performance improves by increasing **m** as shown in Fig. 11. The parameter **m** is bounded by the dimension **n** of the biometric feature, so it cannot be increased to be more than **n**. In this study, we found that the best performance of the algorithm is at **m** = 8.

4.2.2 Evaluation of matrix operation algorithm requirement

Zero row of ERO operation In this paper, we choose one row to be zero because the increase of zero rows would lose some detailed information about the ECG input features. We selected the row number to be n/3 according to [31] where n is the number of rows of input ECG features.

Tensor factor The tensor factor can be in the form of a matrix or integer with a constant value. The reason for determining the suitable size of the tensor factor is the size of that matrix could affect the implementation time; therefore, we tested different matrix size to check its influence on the time is taken for the running of the process for the databases. After lots of experiments, we found that the suitable size of the tensor factor that is used to produce a cancelable feature for ECG is 3 × 3 as shown in Fig. 12 and more details shown in Fig. 13 on MIT-BIH database.

4.3 Results

Four objectives are used to assess the performance of the proposed cancelable system:

(1) **Performance**: Two scenarios are used in this paper, the first scenario is the best testing, where imposters never steal the Hash key, the second scenario is the worst testing, where imposters always steal the Hash key. EER is calculated in both scenarios and the comparison is done between four algorithms (The original algorithm with the original

Table 4 Number of beats on MIT-BIH database

Record No.	No. of beats
100	2273
101	1865
102	2187
103	2084
104	2229
105	2572
106	2027
107	2137
108	1763
109	2532
111	2124
112	2539
113	1795
114	1879
115	1953
116	2412
117	1535
118	2278
119	1987
121	1863
122	2476
123	1518
124	1619
200	2601
201	1963
202	2136
203	2980
205	2656
207	2332
208	2955
209	3005
210	2650
212	2748
213	3251
214	2262
215	3363
217	2208
219	2154
220	2048
221	2427
222	2483
223	2605
228	2053
230	2256
231	1571
232	1780
233	3079
234	2753
48 records	109,966

template, base Bio-Hash algorithm, improved Bio-Hash algorithm and the algorithm using matrix operations) on the three databases. Tables 7, 8 and 9 are showing EER and FAR values of all algorithms on the three databases with $N = 5$ and $\mathrm{m} = 8$ for improved Bio-Hash algorithm and tensor factor 3×3 for the matrix operation algorithm and all results in both scenarios. In the original algorithm, we used the same features of the other

Table 5 Description of the three databases

Database	No. of beats	No. of subjects	Sampling rate	Resolution
MIT-BIH	109,966	48	360 Hz	11-bit
PTB	420,850	50	10 kHz	16-bit
CYBHi	222,390	65	1 kHz	12-bit

algorithms but without using any of template protection methods and then the authentication is done using FFNN on the original template.

Figure 14 shows the comparison of ROC curve of the experiments performed in the worst testing on the three databases. The ROC curve plot is a function of the decision threshold, which plots the rate of the False Positive Rate on the x-axis against the True Positive Rate on the y-axis, a lower value of EER is desirable for practical systems [36].

From Fig. 14 we found that the performance of matrix operation method is better than other methods in worst case on all databases. The matrix operation method is more robust than other algorithms in case the imposter steals both the key and the biometric data, where the features that result from KP operation are fully different than original features. The improved Bio-Hashing method also has ideal performance in worst case comparing with the Bio-Hashing and original methods on all databases and in some cases gives better performance than matrix operation method. The original method gives better performance than Bio-Hash in worst case on CYBHi database, where this database has the largest number of records.

(2) **Reusability (Revocability):** The similarity between the new and old cancelable templates generated by the proposed system is very low and it is easy to reissue a new cancelable template in case if the old template is compromised.
(3) **Diversity:** The key was given to a user during enrollment and was different among different users to generate the pseudo-random number; also we can generate many cancelable templates by mixing different random numbers with the same original biometric. Therefore, many different ECG cancelable biometric can be used in various applications.
(4) **Non-invertibility:** When using the proposed improved Bio-Hashing and matrix operation method the original biometric template cannot be recovered in case if the imposter steals the key and uses information about the transformation or if both the biometric data and the key are stolen.

In this paper, a comparison is done between our cancelable method and the work in [7], and to get an actual comparison term we used the same feature extraction algorithm and extract the same features. Moreover, we applied this method on one of the databases used in this paper,

Table 6 EER and FAR for different N values

Iteration Number (N)	EER	FAR (FRR =0)
N = 3	0.50	0.72
$N = 4$	0.46	0.66
N = 5	0.26	0.38
$N = 6$	0.38	0.55

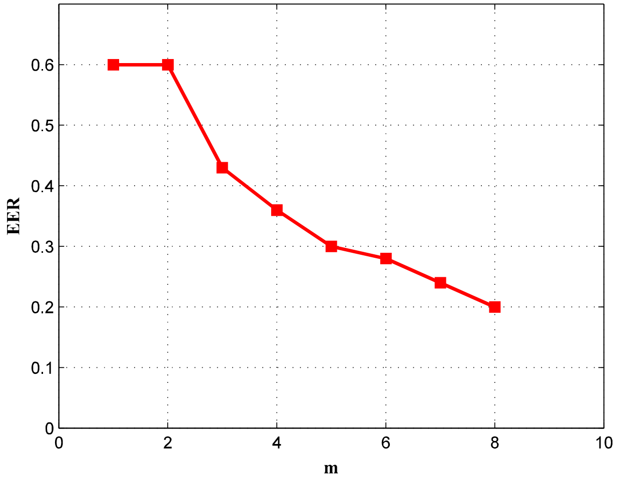


Fig. 11 EER obtained by the Improved Bio-Hashing method varying the parameter (**m**)

which is CYBHi database. Figures 15 and 16 are shown the ROC curve and Precision-Recall curve respectively between the proposed method and the work in [7].

Figures 15 and 16 are shown that the proposed two methods presented a better performance than the one proposed by [7] when using the same features and the same database.

Authentication is performed between the proposed algorithm and previous state-of-the-art cancelable algorithms and authentication algorithms without any protection templates. The comparison of previous state-of-the-art algorithms with the proposed algorithm are shown in Table 10.

It is evident that our proposed methods are more robust as compared to state-of-art works mentioned in Table 10, which make the security of the proposed system higher than others.

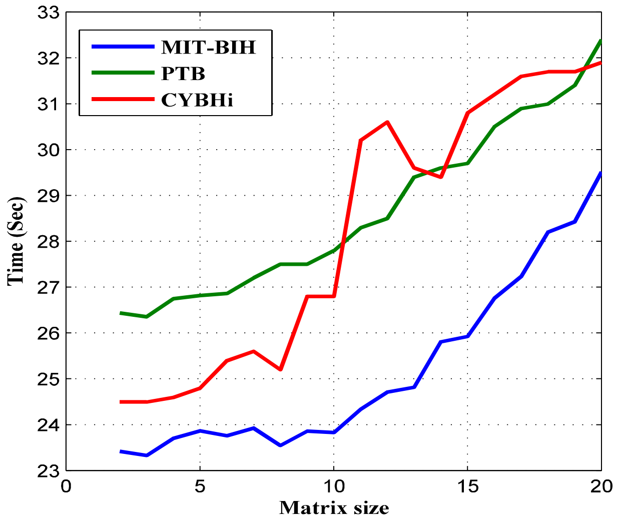


Fig. 12 The correlation between the size of the tensor factor and the time on the three databases

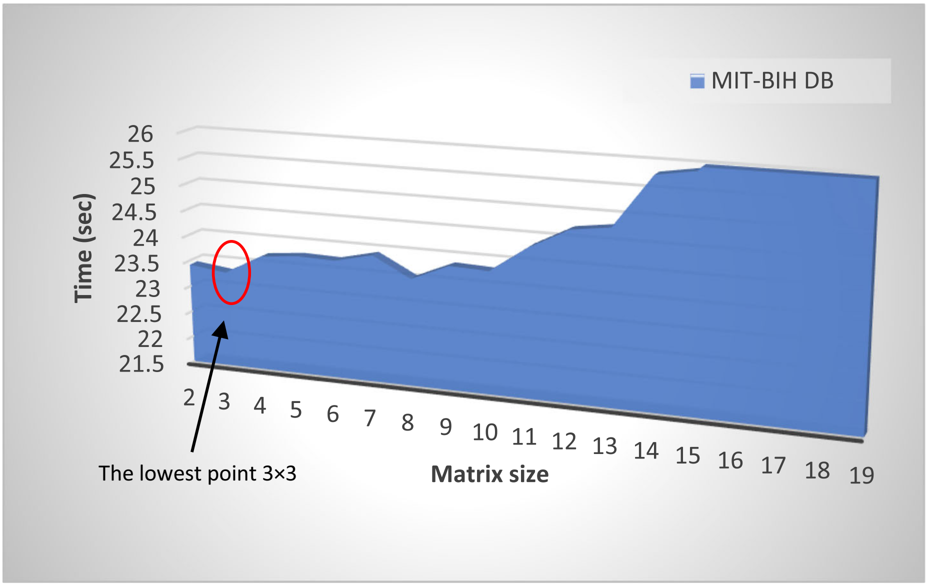


Fig. 13 The correlation between the size of the tensor factor and the time in detail on MIT-BIH

Kim et al. [19], proposed a cancelable ECG biometrics using generalized likelihood ratio test (GLRT). They achieved good accuracy when using a small number of samples, but when using a high number of samples leads to decrease the accuracy. Besides, this method protects the original ECG information but not saving it. Karegar et al. [15], proposed an ECG-based authentication system using some nonlinear features. This method also worked on a small number of samples and gives the lowest accuracy with a high number. Keshishzade et al. [18], proposed a convolution-based method and a wave shape-based method for beat extraction and Nearest Neighbor Based Data Description (NNDD) to perform the authentication. This method needs a large number of features for the training, which effects on the system performance and increase the processing time. Unlike the previous methods, our method worked on large number of records and achieves high accuracy. Also, the proposed method protects and saves the original ECG signal.

From the analysis of the results the following conclusions can be drawn about the proposed methods:

Table 7 Comparison of performance between the proposed algorithm and other algorithms on MIT-BIH database using the following parameters: m = 8, N = 5 (Improved Bio-Hash) tensor factor = 3 × 3 (Matrix operation)

MIT-BIH database		Best Testing		Worst Testing	
		EER	FAR (FRR =0)	EER	FAR (FRR =0)
Methods	Original	0.34	0.49	0.34	0.49
	Bio-Hash	0.31	0.45	0.38	0.52
	Improved Bio-Hash	0.20	0.27	0.34	0.49
	Matrix Operations	0.06	0.02	0.06	0.02

Table 8 Comparison of performance between the proposed algorithm and other algorithms on PTB database using the following parameters: m = 8, N = 5 (Improved Bio-Hash) tensor factor = 3 × 3 (Matrix operation)

PTB database		Best Testing		Worst Testing	
		EER	FAR (FRR =0)	EER	FAR (FRR =0)
Methods	Original	0.35	0.50	0.35	0.50
	Bio-Hash	0.21	0.30	0.36	0.51
	Improved Bio-Hash	0.19	0.28	0.32	0.46
	Matrix Operations	0.14	0.20	0.14	0.20

- One of the advantages of the improved Bio-Hashing algorithm is that, the data are represented in a vector space; hence it could be used in many state-of-the-art machine learning approaches for the authentication process.
- The main drawback of the Bio-Hashing algorithm is that, if the information about the transformation and the Hash key are stolen, the imposter can easily spoof (spoofing attack), unlike the matrix operation algorithm.
- The improved Bio-Hash algorithm obtains performance better than the base Bio-Hashing algorithm in *the worst testing*, where the imposters always steal the Hash key.
- The cancelable ECG algorithm using matrix operations with FFNN has the distinguish performance than the other algorithms.
- The resulting score in the transformed domain is better than that obtained in the original space.
- For authentication, experimental results show that the proposed algorithm using the two methods achieves competitive authentication performance with state-of-the-art ECG authentication methods in terms of EER.

Finally, we want to stress that a novel cancelable biometric authentication system based on ECG has been already confirmed.

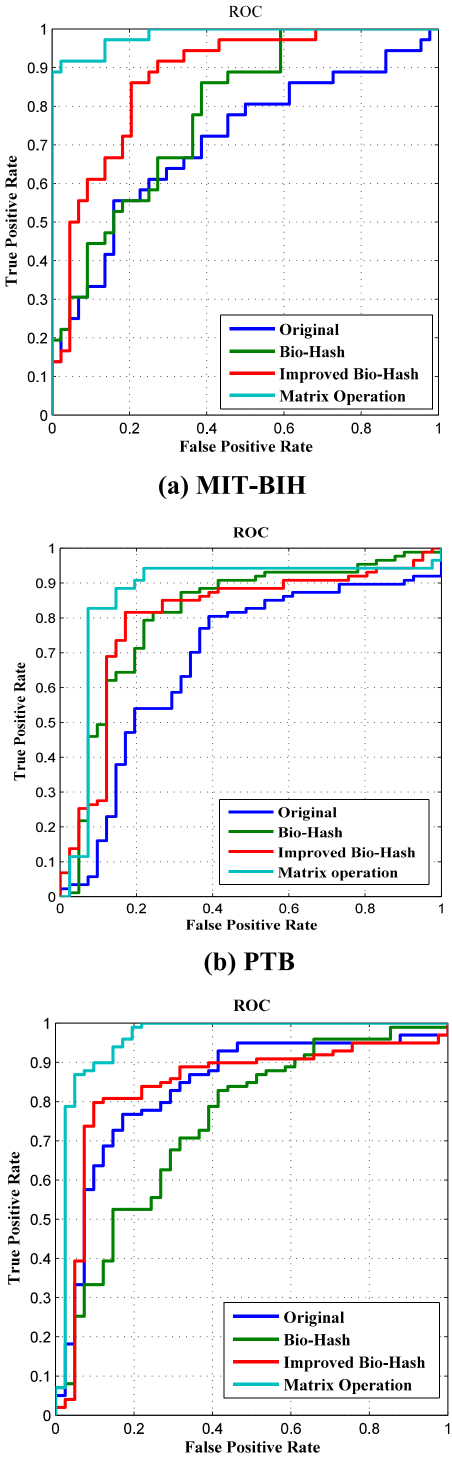
5 Conclusion and future work

This paper proposed a cancelable biometric authentication system based on ECG. Two cancelable biometric techniques applied to develop the proposed authentication system, the first technique is the improved Bio-Hashing technique, which overcomes most of the

Table 9 Comparison of performance between the proposed algorithm and other algorithms on CYBHi database using the following parameters: m = 8, N = 5 (Improved Bio-Hash) tensor factor = 3 × 3 (Matrix operation)

CYBHi database		Best Testing		Worst Testing	
		EER	FAR (FRR =0)	EER	FAR (FRR =0)
Methods	Original	0.21	0.30	0.21	0.30
	Bio-Hash	0.31	0.45	0.48	0.68
	Improved Bio-Hash	0.12	0.18	0.17	0.26
	Matrix Operations	0.09	0.04	0.09	0.04

Fig. 14 Comparison of ROC curve among cancelable biometrics on the three databases



(a) MIT-BIH

(b) PTB

(c) CYBHi

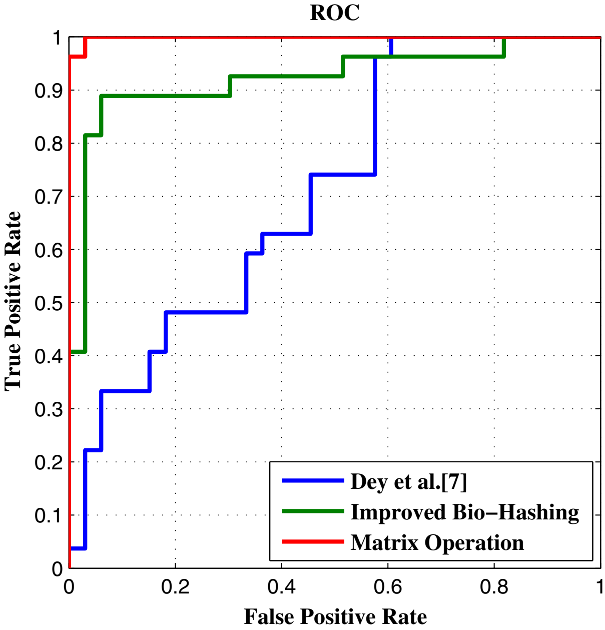


Fig. 15 Comparison of ROC curve among the proposed two methods and the work in [7]

limitations of the base Bio-Hashing technique such as losing accuracy, and the second technique is the matrix operation technique, which produced an irreversibly transformed template of ECG features. Pan-Tompkins algorithm is used for extracting the ECG features and ANN is used for authentication. The main advantage of this paper is that it overcomes the

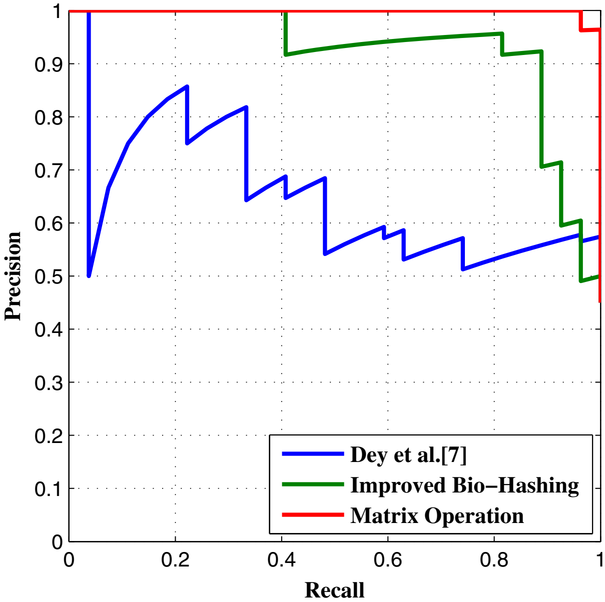


Fig. 16 Comparison of Precision-Recall curve among the proposed two methods and the work in [7]

Table 10 Comparison of previous authentication algorithms

Author	Year	Database	Biometric	Approach	Performance
Kim et al. [19]	2017	ECG-ID Database	ECG	GLRT	EER = 0.302 AUC = 0.775
Leng et al. [23]	2013	Palm-print-vein Database	Palmprint and Palm-vein	2DPHCs	Mean EER Worst = 0.2326 Best = 0.0499
Karegar et al. [15]	2017	MIT-BIH	ECG	RSA HFD DFA GHE RQA	EER = 4.88
Mukhaiyar et al. [31]	2015	FVC 2002 and 2004	Fingerprint	Matrix approaches	FVC 2002 Mean EER = 0.10 Mean FAR = 0.20 FVC 2004 Mean EER = 0.07 Mean FAR = 0.13
Salloum et al. [37]	2017	MIT-BIH	ECG	RNNs	EER = 3.5
Keshishzade et al. [18]	2015	MIT-BIH	ECG	FFS	EER = 2.34 AUC = 99.73
Singh et al. [38]	2012	MIT-BIH	ECG	delineated features	EER = 10.8
Proposed	2018	MIT-BIH PTB CYBHi	ECG	Improved Bio-Hashing Matrix operations	MIT-BIH EER = 0.34 (Improved) EER = 0.06 (Matrix) PTB EER = 0.32 (Improved) EER = 0.14 (Matrix) CYBHi EER = 0.17 (Improved) EER = 0.09 (Matrix)

GLRT Generalized likelihood ratio test, *2DPHCs* 2DPalmHash codes, *RSA* Rescaled range analysis, *HFD* Higuchi's fractal dimension, *DFA* Detrended fluctuation analysis, *GHE* Generalized hurst exponent, *RQA* Recurrence quantification analysis, *RNNs* Recurrent neural networks, *FFS* Feature forward selection, *EER* Equal error rate, *AUC* Area under ROC curve, *FAR* False acceptance rate spoofing attack in most biometrics that is done by combining a feature transformation method with aliveness detection system (ECG system). Results show that the second technique (matrix operations technique) is better than other techniques. The overall performance of the proposed system using the two cancelable techniques is better than the previous techniques regarding authentication. In future work, we can design a secure multi-biometric system using fusion techniques; also, we can design a cancelable system by combining the two techniques that used in the proposed algorithm. Finally, we can try to implement the proposed algorithm into different biometric technologies.

Acknowledgements The authors would like to thank Dr. Loris Nanni for his helpful advice in implementing the improved Bio-Hash algorithm. This work was supported by the National Nature Science Foundation of China (NSFC) Grant No. 61571165.

Compliance with ethical standards

Conflicts of interest The authors declare that there is no conflict of interest regarding the publication of this article.

References

1. Albert A (1972) Regression and the moore-penrose pseudoinverse. Academic Press, New York
2. Ang R, Safavi-Naini R, McAven LF (2005) Cancelable key-based fingerprint templates. In: Boyd C, Gonzalez Nieto JM (eds) Australasian Conference on Information Security and Privacy. Springer, Germany, pp 242–252
3. Bolle RM, Connell JH, Ratha NK (2002) Biometric perils and patches. Pattern Recogn 35(12):2727–2738
4. Connie T, Teoh A, Goh M, Ngo D (2005) Palmhashing: a novel approach for cancelable biometrics. Inf Process Lett 93(1):1–5
5. Da Silva HP, Lourenço A, Fred A, Raposo N, Aires-de Sousa M (2014) Check your biosignals here: A new dataset for off-the-person ECG biometrics. Comput Methods Prog Biomed 113(2):503–514
6. Damer N, Opel A, Nouak A (2013). Performance anchored score normalization for multi-biometric fusion. In: International Symposium on Visual Computing, Springer, pp. 68-75
7. Dey N, Nandi B, Dey M, Biswas D, Das A, Chaudhuri SS (2013) BioHash code generation from electrocardiogram features. In: IEEE 3rd International Advance Computing Conference (IACC). IEEE, Ghaziabad
8. Dey M, Dey N, Mahata SK, Chakraborty S, Acharjee S, Das A (2014) Electrocardiogram feature based inter-human biometric authentication system. In: International Conference on Electronic Systems, Signal Processing and Computing Technologies. IEEE, Nagpur, pp 300–304
9. El-Khamy SE, Korany NO, El-Sherif MH (2017) A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and rsa encryption. Multimedia Tools and Applications 76(22):24091–24106
10. Goldberger AL, Amaral LAN, Glass L, Hausdorff JM, Ivanov PC, Mark RG et al (2000) Physiobank, physiotoolkit, and physionet components of a new research resource for complex physiologic signals. Circulation 101(23):E215
11. Islam MS, Alajlan N (2017) Biometric template extraction from a heartbeat signal captured from fingers. Multimedia Tools and Applications 76(10):12709–12733
12. Islam S, Ammour N, Alajlan N, Abdullah-Al-Wadud M (2017) Selection of heart-biometric templates for fusion. IEEE Access 5:1753–1761
13. Jain AK, Maltoni D, Miao D, Prabhakar A (2003) Handbook of fingerprint recognition. Springer-Verlag, New York
14. Jin ATB, Ling DNC, Goh A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn 37(11):2245–2255

15. Karegar FP, Fallah A, Rashidi S. (2017). Using recurrence quantification analysis and generalized hurst exponents of ECG for human authentication. In: Swarm Intelligence and Evolutionary Computation. IEEE, Kerman, pp 66–71
16. Kaur H, Khanna P (2016) Biometric template protection using cancelable biometrics and visual cryptography techniques. Multimedia Tools and Applications 75(23):1–29
17. Kaur H, Khanna P (2017) Cancelable features using log-Gabor filters for biometric authentication. Multimedia Tools and Applications 76(4):4673–4694
18. Keshishzadeh S, Rashidi S (2015) A system of biometric authentication based on ECG signal segmentation. In: 22nd Iranian Conference on Electrical Engineering (ICEE), vol. 6. IEEE, Tehran, pp 1873–1877
19. Kim H, Nguyen MP, Chun SY (2017) Cancelable ECG biometrics using GLRT and performance improvement using guided filter with irreversible guide signal. In: 39th Annual International Conference of the IEEE Conf Proc IEEE Engineering in Medicine and Biology Society (EMBC). IEEE, Seogwipo, pp 454–457
20. Leng L, Zhang J, Chen G, Khan MK, Alghathbar K (2011) Two-directional two-dimensional random projection and its variations for face and palmprint recognition. In: Murgante B, Gervasi O, Iglesias A, Taniar D, Apduhan BO (eds) Computational Science and Its Applications - ICCSA 2011. ICCSA 2011. Lecture Notes in Computer Science, vol 6786. Springer, Berlin
21. Leng L, Zhang J, Chen G, Khan MK, Bai P (2011) Two dimensional palmphasor enhanced by multi-orientation score level fusion. In: Park JJ, Lopez J, Yeo SS, Shon T, Taniar D (eds) Secure and Trust Computing, Data Management and Applications. STA 2011. Communications in Computer and Information Science, vol 186. Springer, Berlin, Heidelberg
22. Leng L, Zhang S, Bi X, Khan MK (2012) Two-dimensional cancelable biometric scheme. In: 2012 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR). IEEE, Xian, pp 164–169
23. Leng L, Li M, Teoh ABJ (2013) Conjugate 2DPalmHash code for secure palm-print-vein verification. In: International Congress on Image and Signal Processing, vol. 03. IEEE, Hangzhou, pp 1705–1710
24. Leng L, Teoh ABJ, Li M, Khan MK (2014) Analysis of correlation of 2dpalmhash code and orientation range suitable for transposition. Neurocomputing 131(9):377–387
25. Leng L, Teoh ABJ, Li M, Khan MK (2015) Orientation range of transposition for vertical correlation suppression of 2dpalmphasor code. Multimedia Tools and Applications 74(24):11683–11701
26. Li H, Tan J (2010) Heartbeat-driven medium-access control for body sensor networks. IEEE Trans Inf Technol Biomed 14(1):44–51
27. Li L, Correia PL, Hadid A (2018) Face recognition under spoofing attacks: countermeasures and research directions. IET Biometrics 7(1):3–14
28. Lumini A, Nanni L (2007) An improved biohashing for human authentication. Pattern Recogn 40(3):1057–1065
29. Maio D, Nanni L (2005) Multihashing, human authentication featuring biometrics data and tokenized random number: A case study fvc2004. Neurocomputing 69(1):242–249
30. Matlab, Neural Networks. [Online] Available from: http://www.mathworks.com/products/neural-network
31. Mukhaiyar R, Dlay SS, Woo WL (2015) Cancellable biometric using matrix approaches. Newcastle University, Newcastle upon Tyne
32. [Online] (Available from: https://www.techworld.com/news/developers/halifax-bank-trials-heart-rate-technology-authenticate-customers-3601753/
33. Pan J, Tompkins WJ (1985) A real-time qrs detection algorithm. IEEE Trans Biomed Eng 32(3):230–236
34. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis & Machine. Intelligence 29(4):561
35. Sadhya D, Singh SK (2017) Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions. Multimedia Tools and Applications 77(12):15113–15137
36. Safie SI, Soraghan JJ, Petropoulakis L (2011) Electrocardiogram (ECG) biometric authentication using pulse active ratio (par). IEEE Transactions on Information Forensics and Security 6(4):1315–1322
37. Salloum R, Kuo CCJ (2017). ECG-based biometrics using recurrent neural networks. In: Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on, IEEE, pp. 2062-2066
38. Singh YN, Singh SK (2012) Evaluation of electrocardiogram for biometric authentication. J Information Security 3(1):39–48
39. Singla SK, Sharma A (2010) ECG as biometric in the automated world. International Journal of Computer Science and Communication 1(2):281–283
40. Teoh ABJ, Goh A, Ngo DCL (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
41. Teoh AB, Kuan YW, Lee S (2008) Cancellable biometrics and annotations on biohash. Pattern Recogn 41(6):2034–2044
42. Teoh ABJ, Yip WK, Toh KA (2010) Cancellable biometrics and user dependent multi-state discretization in biohash. Pattern Anal Applic 13(3):301–307

43. Van Driest SL, Wells QS, Stallings S, Bush WS, Gordon A, Nickerson DA et al (2016) Association of arrhythmia-related genetic variants with phenotypes documented in electronic medical records. JAMA 315(1):47–57
44. Wyant RS, Nedjah N, Mourelle LM (2017) Efficient biometric palm-print matching on smart-cards. Multimedia Tools and Applications 8584(21):1–31

Mohamed Hammad received his MSc degree in 2015, Information Technology Department, Faculty of Computers and Information, Menoufia University, Egypt. He worked as a demonstrator and assistant lecturer in Faculty of Computers and Information, Menoufia University, Egypt since April 2012 till now. He is currently a PhD candidate at the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. His research interests include Computer Vision, Machine Learning, Pattern Recognition and Biometrics.

Gongning Luo received the B.Sc. degree in computer science from East China Jiao Tong University, Nanchang, China, in 2012, and received the M.Sc. degree in computer science from Harbin Institute of Technology, Harbin, China 2014. He is currently pursuing the Ph.D. degree from the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. His research interests include medical image processing and machine learning. He has published 9 papers and got 2 patents, and won National Scholarship for two times.

Wang Kuanquan is a full professor and PhD supervisor with School of Computer Science and Technology, and the deputy director of Research Center of Perception and Computing at Harbin Institute of Technology. Also, he was an associate dean of School of Computer Science and Technology, HIT at Harbin, and the dean of School of Computer Science and Technology, HIT at Weihai from 2011 to 2014. He is a senior member of IEEE, a senior member of China Computer Federation (CCF) and ACM, and a senior member of Chinese Society of Biomedical Engineering. His main research areas include Image Processing and Pattern Recognition, Biometrics, Biocomputing, Modelling and Simulation, Virtual Reality and Visualization.