Information Sciences 585 (2022) 127–143

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication

Ahmed S. Sakr [a], Paweł Pławiak [b,c,*], Ryszard Tadeusiewicz [d], Mohamed Hammad [e]

[a] Department of Information System, Faculty of Computers and Information, Menoufia University, Egypt
[b] Department of Computer Science, Faculty of Computer Science and Telecommunications, Cracow University of Technology, Warszawska 24, 31-155 Krakow, Poland
[c] Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland
[d] AGH University of Science and Technology, Department of Biocybernetics and Biomedical Engineering, Krakow, Poland
[e] Department of Information Technology, Faculty of Computers and Information, Menoufia University, Menoufia, Egypt

ARTICLE INFO

Article history:
Received 15 August 2021
Received in revised form 21 November 2021
Accepted 22 November 2021
Available online 27 November 2021

Keywords:
Authentication
Amino Acid
Biometrics
Cancelable
Deep Transfer Learning
DNA
ECG
Template Protection
SVM

ABSTRACT

Recently, electrocardiogram (ECG) signals have received a high level of attention as a physiological signal in the field of biometrics. It has presented great possibilities for its strength against counterfeit. However, the ECG feature templates are irreplaceable, and a compromised template implies a permanent loss of identity. Therefore, several studies have been introduced biometric template protection techniques such as cancelable techniques to protect the original template in case it is stolen or lost. In this research, a cancelable ECG approach is proposed to protect the ECG feature template for human authentication. In our system, we first employed some image processing techniques for preprocessing the input ECG signals. Then, a deep transfer learning approach is employed to extract the deep ECG features. Later, the proposed cancelable approach based on DNA and amino acid is applied to protect the deep feature templates. Lastly, a Support Vector Machine (SVM) is employed for authentication. Extensive experiments on two commonly used datasets coupled with comprehensive theoretical analysis demonstrate the highest accuracy of the proposed system and the strong resilience of the system to various security and privacy attacks. Results show that the proposed cancelable method meets all requirements of cancelable biometrics such as *irreversibility*, *revocability*, and *unlinkability*.

1. Introduction

Biometric systems are becoming one of the most favorable and dependable technologies for human authentication. Biometric authentication systems analyze individual traits by extracting biometric data to perform authentication [1]. Biometric identifiers are the distinguishing and assessable characteristics used to name and describe every individual. Biometric determinants are classified as physiological characteristics that are related to body shape such as Electrocardiogram (ECG), Electroencephalogram (EEG), DNA, fingerprints, face recognition, palm print, iris, and smell recognition. Behavioral characteristics that are related to a person's behavior pattern such as voice, typing rhythm, signature, keystroke and behav-

* Corresponding author.

https://doi.org/10.1016/j.ins.2021.11.066
0020-0255/

ioral profiling. Several researchers have coined the term "behavioral measurements" to define the latter category of biometrics [2].

Traditional methods of access control such as passport or driver's license, and password or PIN. Because of the uniqueness of biometric identifiers to every individual, they outperform these traditional authentication methods; however, the gathering of biometric identifiers increases confidentiality concerns about the end use of this information [3]. In addition, biometric templates stored in plaintext are immutable and irreplaceable, and a compromised template implies a permanent loss of identity. Therefore, cancelable biometrics is introduced to make the system more secure and private and to enable the regeneration of the original biometric feature [4]. Cancelable biometrics is devised to conceal the user's true pattern by using an intentionally transformed template through a non-invertible transform, which must fulfill the following criteria: *Unlinkability, Revocability*, *Non-invertibility*, and *Performance* [5].

- ***Unlinkability***: Infeasibility of distinguishing whether multiple transformed instances are extracted from the same ECG. This property prevents cross-matching between multiple databases.
- ***Revocability***: Revocation of the transformation and reissue of a new one in case it has been compromised.
- ***Non-invertibility***: One-way transformation of the template, to prevent computational recovery of ECG data.
- ***Performance***: The recognition accuracy of the cancelable templates should be preserved or improved compared to their unprotected counterparts.

It is rather difficult to develop a template protection algorithm that satisfies the above-mentioned criteria. Therefore, in this paper, we satisfy most of these criteria by proposing a new cancelable technique based on a combination of a deep transfer learning approach with a method inspired by DNA and Amino Acid.

There are two types to design cancelable biometrics such as biometric salting and non-invertible transform methods [6]. Biometric salting utilizes an external factor to derive a transformation matrix that can be used to mix with biometric templates. On the other hand, a non-invertible transform is a privacy-preserving biometric authentication solution by using a one-way transformation to ensconce the original biometric.

This paper focused on a non-invertible transform technique based on ECG signals for authentication. The ECG is an effective test to measure the electrical activity of the heart and its rate. This test is done using electrodes placed on the chest, hands and feet and fixed using adhesive cloth patches, and its results are shown on a screen or paper. The heart is divided into four chambers: two uppers and two lowers. The two upper chambers create the first electrical wave, which is called the "P wave". Then comes a straight line until it reaches the two lower chambers that make the other wave, which is called the QRS complex. And there is the last wave called the "T wave", which represents the return to the resting position of the two lower chambers. The ECG authentication systems extract unique behavioral patterns to verify the user. In addition, compared to other biometrics the ECG signals are more robust against noises, as a result, ECG became more desirable as a biometric system [7].

Recently, DNA and Amino Acid are used for encryption in the information security field because of their capabilities [8], however, as far as we know, this is the first study that employed DNA and Amino Acid for this issue. In biology, DNA is the hereditary material in humans that contains the biological instructions that make each gender unique. DNA stores information as a code, which is made of *four* chemical elements: adenine (A), guanine (G), cytosine (C), and thymine (T). Amino acids are the monomers that make up proteins. In this study, the cancelable code is generated using the sequence of the information code in DNA and the sequence of amino acids in proteins.

Several recent studies are proposed to protect the template of ECG authentication [9–21]. However, no previous study satisfies all cancelable criteria. In this paper, we proposed a method that meets all the requirements of cancelable techniques. In addition, some early works that used cancelable techniques for ECG signals were primary and incomplete [9], however, our method is more comprehensive. Moreover, some ECG cancelable techniques are non-uniformly and lightly distributed, which executes an unwanted constraint on the search space. The proposed cancelable method can be used to secure any other biometrics such as EEG and fingerprint. Furthermore, no previous ECG cancelable systems used deep learning approaches according to the recent review studies in [22,23], which faces many problems such as working on big data and overfitting problems. Deep learning approaches can solve these previous problems and achieve state-of-the-art accuracy, sometimes exceeding the performance of human-level. To our knowledge, only two studies [15,16] used deep learning with cancelable ECG, however, these studies focus on authentication not template protection and also the main aim of this studies is to propose multi-model biometric system based on ECG and fingerprint. This study considered the *first* study that focused on using deep learning approach for cancelable ECG signals, which overcome most of the previous traditional machine learning methods.

The major contributions of this study are cleared as follows:

- We are the first to employ the combination of biological properties and deep learning approaches for cancelable ECG biometrics.
- We are the first to propose a novel cancelable ECG method using DNA and Amino Acid method combined with deep learning, which satisfies all cancelable requirements (*unlinkability*, *revocability*, *non-invertibility*, and *performance*). Unlike other previous cancelable ECG systems that did not satisfy all cancelable requirements.

- We proposed the first cancelable ECG system that employed deep learning for human authentication, which overcome the problems that faced most of the previous traditional machine learning cancelable methods.
- This is the first study to combine such different fields as biometrics, signal processing, biology and artificial intelligence (AI). As a result, increase productivity and increase the flexibility of our system to use it in different fields of science.
- A comprehensive and theoretical analysis of authentication aspects (e.g., different types of attack) are given both qualitatively and quantitatively to justify the proposed method.
- We evaluate our approach on two different datasets PTB [24] and ECG-ID [25], which are the most important datasets used for ECG authentication purposes in the literature. Results show that our methodology outperforms other approaches in terms of authentication *accuracy*, *recall*, *precision*, *f1-score* and *equal error rate* (*EER*). Part of our source code is available at: https://github.com/assakr/DNA-Cancelable

Following is the remainder of this paper. The previous work is discussed in Section 2. Section 3 describes the proposed approach. In Section 4, the experimental results are reported along with the performance analysis. The results are discussed and compared with related works in Section 5. Finally, Section 6 shows the conclusion of the study.

2. Related work

In this section, several related works for ECG template protection methods are reviewed [9–13]. In addition, we summarized some previous methods that used DNA and Amino Acid for encryption [26–28]. Finally, for a full-fledged understanding of cancelable biometrics, several comprehensive review papers [22,23] are available online.

2.1. Recent cancelable ECG biometric

Recently, several traditional machine learning approaches have been presented for cancelable ECG biometrics [9–14]. These approaches depend on extracting numerous features benchmarks from the ECG signal such as P, QRS and T waves and the features related to the amplitude and time intervals [29]. After that, they used a cancelable technique to protect these features. Finally, they test some classifiers according to these features and choose the suitable classifier that achieved the highest accuracy [30]. The main limitations of these methods are the inability of working with noisy ECG signals; the inability of working on big data; using a small number of features, which affect the overall accuracy of the system, and the overfitting problem.

The first cancelable ECG method is proposed by Dey *et al.* [9]. They used the Bio-Hashing algorithm to generate the cancelable code from the ECG features. However, this method gives low accuracy with a high false acceptance rate (FAR). In addition, they only implemented the cancelable stage and did not present a complete authentication system. In 2019, Hammad *et al.* [10], proposed the first completed cancelable system based on ECG. In their system, they overcome most of the limitations of the Dey *et al.* [9] method by presenting an improving version of the Bio-Hash method. Finally, they completed the system by using Feed-Forward Neural Network (FFNN) as a classifier for authentication. However, this system [10] also gives low authentication performance. After that, several cancelable ECG methods are proposed [11–15]. Kim *et al.* [11], presented a cancelable ECG biometric based on a detector called generalized likelihood ratio test (GLRT). In addition, they presented a guide filter (GF) to generate irreversible ECG signals. They obtained the best performance for non-invertibility evaluation with an EER of 2.6%. In this method, they only presented a way for the irreversible transformation of the ECG template and did not use it for secure biometrics. Chen *et al.* [12], presented a cancelable ECG scheme based on multi-lead ECG. To solve the problem of subspace overlapping, they used the multiple signal classification (MUSIC), which controls the individuality of an unknown beat. They obtained the best recognition rate of 97.58 % under some testing conditions. Kim and Chun [13], presented the same cancelable ECG as in their previous study [11]. The difference is using compressive sensing (GS) instead of GF. They obtained the best performance for non-invertibility evaluation with an EER of 3.8%.

To overcome the disadvantages of the traditional approaches, consequently, deep learning approaches were investigated. Numerous deep learning approaches have also been presented for ECG authentication [15–21,49,50], however, none of these methods have focused on cancelable ECG biometric. Labati *et al.* [49], used CNN to deploy an authentication algorithm based on the use of more than one ECG lead. Their algorithm recorded an EER of 1.36% for authentication using the PTB database. Li *et al.* [50], presented a CNN protocol for identifying humans based on ECGs. They employed two CNN models, one for feature extraction and another for identification a combination that recorded an average identification accuracy of 94.3%. In authentication, the deep learning methods have demonstrated much greater accuracy compared to the traditional machine learning approaches [15,16]. Therefore, we employed deep learning approaches in our system.

2.2. Recent DNA and amino acid approaches for encryption

Reddy *et al.* [26], presented an encryption system based on a key generation approach and DNA. In this method, firstly, the text is transmitted in 16-bit blocks. After that, they performed block-wise to replicate the noise of random binary using bidirectional associative memory neural network. Finally, they XORed the encoded sequence and the DNA was used for encryption. Kalsi *et al.* [27], introduced DNA sequence and deep learning for key generation using GA and Needleman-Wunsch (NW)

algorithm. This study also proved that DNA can be used as an encryption method with high performance. Another study presented by Basu *et al.* [28], which proves that DNA can use in encryption and decryption algorithms. They employed Bidirectional Associative Memory Neural Network (BAMNN) as a key generation with a high level of security compared with conventional cryptography algorithms. Sakr *et al.* [48], presented an amino acid encryption model for key generation using GA. They generated *two* keys, *one* is generated using GA, and the *second* key is by converting DNA to a protein message. The model is tested over different attacks and proved that DNA with amino acids can be used for encryption tasks. According to the mentioned studies [26–28,48], which prove that DNA and amino acid can be used for encryption, we proposed our system using DNA with an amino acid as a non-invertible transform method based on ECG for human authentication.

3. The proposed authentication system

This section introduces the proposed cancelable ECG technique for human authentication. The general block diagram of the proposed system is shown in Fig. 1, which is consists of the following stages: preprocessing stage to remove the noise of each ECG signal and prepares it for the next stage, feature extraction stage to extract the main features of each signal using a pre-trained CNN model, the proposed cancelable stage to protect the features from the previous stage and finally, the authentication stage to decide whether the user is accepted or rejected.

3.1. Databases

To assess the proposed method, we consider *two* different publicly available databases, which are the most significant databases used in ECG authentication in the literature [9–21]. In addition, we employed these datasets with the same number of records that were used in the previous works to make a fair comparison.

- Ecg-ID:

This dataset [25] is developed for authentication tasks and considered the best choice for working with ECG biometric. This database recorded from 90 persons (46 women and 44 men) and each record is *twenty* seconds from lead I. Each signal was 12-bit resolution and digitized at 500 Hz. The records of each subject were collected from 2 to 20 session data. In this study, we worked on *two* sessions for each subject to avoid any data imbalance problem [31].

- Ptb:

This dataset [24] made up 549 records from 290 subjects and each subject has a duration between *one* to *five* records, of which 52 persons are healthy and used for authentication in the literature [10,15–17,19,20]. Each signal was digitized at 1000 Hz with 16-bit resolution. The database contains recorded from *fifteen* leads (*twelve* regular leads and *three* Frank leads (vx, vy, vz)). In this study, we worked on ECG signals from the Frank leads.

The *two* databases were resampled to 500 Hz and collected from PhysioNet [32]. All these datasets were passed to the preprocessing stage to remove artifacts and noise. Table 1. presents an overview of the *two* databases.

3.2. Preprocessing stage

We start with the preprocessing stage to remove the noise and the baseline wander of the input ECG signal. We use the method in [33] to remove the baseline wander. Next, we use a Savitzky-Golay Smoothing Filter [34] to remove the remaining noise. The filter configuration filters the signal *four* times to offer an improved filtration while preserving the unique features

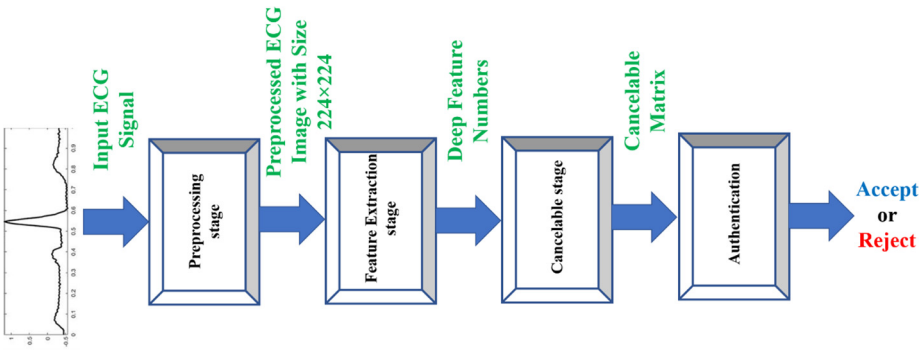


Fig. 1. Block Diagram of our authentication system.

Table 1
Overview of the used databases.

Database	Sample Rate	Subjects	Health Condition	Ref.
ECG-ID	500 Hz	90	Healthy	[25]
PTB	1000 Hz	290	Mixed	[24]

of the ECG signal. Finally, to make the ECG signals suitable for the deep model we converted each signal to an image according to the algorithm in [17] and resize each image to 224 × 224.

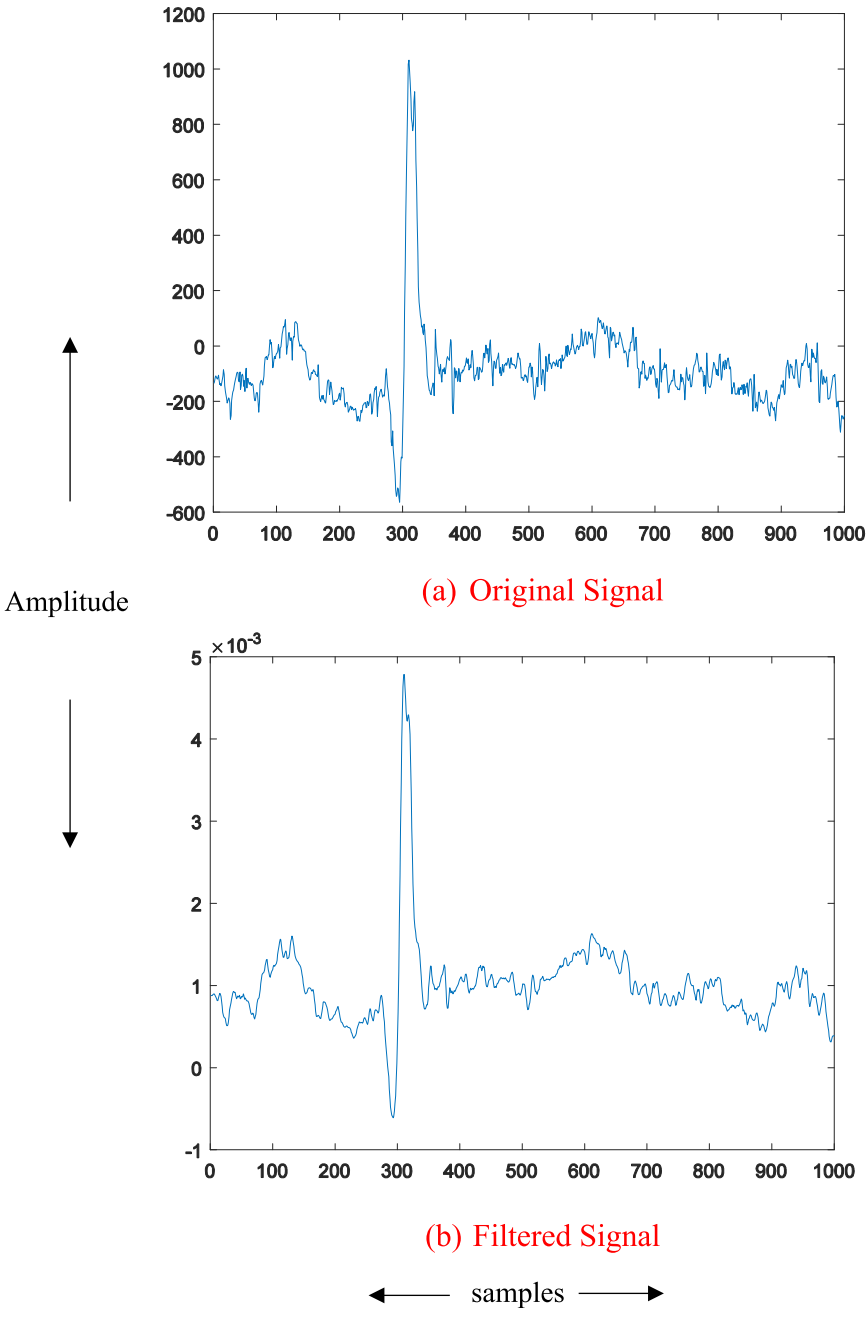


Fig. 2. The effect of using the Filter on an ECG signal.

Fig. 2 shows the result of the preprocessing on one signal from the PTB database, where (a and b) show the original ECG signal and the signal after applying the filter, respectively.

3.3. Deep feature extraction stage

In this study, the deep learning approach is used for extracting the deep features from the preprocessed ECG signals. According to the literature and our discussion in Section 1, we show that deep learning approaches established greater accuracy in authentication compared to the traditional methods. Therefore, we employed deep learning in our system. Deep learning applications are used in different fields such as medical fields [35,36], pattern recognition, electronics, and many other fields [37].

To implement the system quickly with high performance, to reduce the cost of implementation and to use cases from transfer learning, prediction, and feature extraction, we employed pre-trained deep models [38]. These models have already learned to extract informative and powerful ECG features. There are several available pre-trained networks trained such as resnet [39], googlenet [40], xception [41] and vgg [42]. In this study, we worked on vgg-16 pre-train model [42]. VGG-16 is not deep compared to other models such as vgg-19 and this will be useful for our case as the data is very different from the original data. In addition, another benefit of using vgg-16 is negligible the training time of the dense layer with superior accuracy [43].

For our system, we employed the vgg-16 as a feature extraction by removing the output layer in the original model and using the whole network as a feature extractor for the novel database. We start with the 2D convolutional layers with 64 filters and its size increases sequentially to 512 filters in the last layers (to extract more features from the input). The filter size is set at 3×3 with a stepwise stride. The output of every convolutional layer is also pooled at a stride of (2,2). Further,

Table 2
Architecture of the vgg-16 model.

Layer	Output shape	Kernel size	Parameter No.	Others
Input	(224, 224, 3)	–	0	–
Convolution (conv1-1)	(224, 224, 64)	$3 \times 3 \times 3$	1792	Stride [1 1]padding [1 1 1 1]
ReLU (relu1-1)	–	–	0	–
Convolution (conv1-2)	(224, 224, 64)	$3 \times 3 \times 64$	36,928	Stride [1 1]padding [1 1 1 1]
ReLU (relu1-2)	–	–	0	–
Maxpool (pool1)	(112, 112, 64)	2×2	0	Stride [2 2]padding [0 0 0 0]
Convolution (conv2-1)	(112, 112, 128)	$3 \times 3 \times 64$	73,856	padding [1 1 1 1]Stride [1 1]
ReLU (relu2-1)	–	–	0	–
Convolution (conv2-2)	(112, 112, 128)	$3 \times 3 \times 128$	147,584	Stride [1 1]padding [1 1 1 1]
ReLU (relu2-2)	–	–	0	–
Maxpool (pool2)	(56, 56, 128)	2×2	0	Stride [2 2]padding [0 0 0 0]
Convolution (conv3-1)	(56, 56, 256)	$3 \times 3 \times 128$	295,168	padding [1 1 1 1]Stride [1 1]
ReLU (relu3-1)	–	–	0	–
Convolution (conv3-2)	(56, 56, 256)	$3 \times 3 \times 256$	590,080	Stride [1 1]padding [1 1 1 1]
ReLU (relu3-2)	–	–	0	–
Convolution (conv3-3)	(56, 56, 256)	$3 \times 3 \times 256$	590,080	Stride [1 1]padding [1 1 1 1]
ReLU (relu3-3)	–	–	0	–
Maxpool (pool3)	(28, 28, 256)	2×2	0	Stride [2 2]padding [0 0 0 0]
Convolution (conv4-1)	(28, 28, 512)	$3 \times 3 \times 256$	1,180,160	padding [1 1 1 1]Stride [1 1]
ReLU (relu4-1)	–	–	0	–
Convolution (conv4-2)	(28, 28, 512)	$3 \times 3 \times 512$	2,359,808	Stride [1 1]padding [1 1 1 1]
ReLU (relu4-2)	–	–	0	–
Convolution (conv4-3)	(28, 28, 512)	$3 \times 3 \times 512$	2,359,808	Stride [1 1]padding [1 1 1 1]
ReLU (relu4-3)	–	–	0	–
Maxpool (pool4)	(14, 14, 512)	2×2	0	Stride [2 2]padding [0 0 0 0]
Convolution (conv5-1)	(14, 14, 512)	$3 \times 3 \times 512$	2,359,808	padding [1 1 1 1]Stride [1 1]
ReLU (relu5-1)	–	–	0	–
Convolution (conv5-2)	(14, 14, 512)	$3 \times 3 \times 512$	2,359,808	Stride [1 1]padding [1 1 1 1]
ReLU (relu5-2)	–	–	0	–
Convolution (conv5-3)	(14, 14, 512)	$3 \times 3 \times 512$	2,359,808	Stride [1 1]padding [1 1 1 1]
ReLU (relu5-3)	–	–	0	–
Maxpool (pool5)	(7, 7, 512)	2×2	0	Stride [2 2]padding [0 0 0 0]
Flatten (flatten)	25,088	–	0	–
Fully connected (fc1)	4096	–	102,764,544	–
ReLU (relu6)	–	–	0	–
Dropout (drop1)	–	–	0	50% dropout
Fully connected (fc2)	4096	–	16,781,312	–
ReLU (relu7)	–	–	0	–
Dropout (drop2)	–	–	0	50% dropout
Fully connected (fc3)	1000	–	4,097,000	–
Softmax	–	–	0	–

the dropout technique with a 0.5 probability rate is employed to avoid overfitting by ignoring some randomly selected neurons during the training. The dropout is important in large networks that have complex fitting but few labeled samples. In addition to serving as a classifier, the fully connected layer maps the dimensions (i.e., high to low). In our case, we selected the last fully connect layer as a feature extractor for the new data and to pass it to the next stage. Table 2 shows the architecture of the vgg-16 model employed in this paper.

According to Table 2, we selected the output of the last fully connected layer (fc3), which is 1000, and pass it to the next stage (cancelable stage). Finally, we obtained the feature matrix with size D $\times$ 1000, where D is the number of input ECG data.

3.4. Proposed cancelable method

The proposed cancelable method is discussed in this Section. After extracting the features from the previous stage, we check if all numeric values of the features are positive or not. If the numbers are not positive, we get the absolute value of these numbers and get the integer part of the number. In the next step, we converted each number in the feature matrix to an 8-bit binary number to convert it to a DNA sequence according to the values in Table 3.

After converting each 8-bit binary number to DNA, we converted each DNA to protein (PM), which is called an amino acid. Finally, we converted each amino acid alphabet to a positive integer number and add the final numbers to the cancelable matrix. When converted DNA to protein it must be converted to RNA first then convert the RNA to protein. Table 4 shows how to convert the DNA to RNA (the corresponding alphabet of RNA). Fig. 3 shows a block diagram of all steps in the proposed cancelable method during the enrollment and authentication stage. During the enrollment stage, all deep features extracted from the deep model are passed through the proposed cancelable method (as discussed early in this Section) and generated positive integer numbers. After that, we generated a pseudo-random vector using the Blum-Blum-Shub generator with a uniform distribution [45]. We employed the same specifications of the generator as in the method [10]. Finally, we computed the inner product between the generated positive integer numbers and N-normalized pseudo-random number from the generator to generate the cancelable matrix and stored it in the database.

Fig. 4 shows an example for all steps of the proposed cancelable algorithm on one numeric value.

Different cancelable keys were given to each individual in the enrollment stage for using it in the authentication stage. During the authentication stage, each individual should enter the key for the authentication. After that, the deep feature is extracted from the ECG test image and passed through the proposed cancelable method to generate the positive integer number. Next, we compute the inner product between the key and the positive number to generate the cancelable feature vector. Finally, we employed support vector machine (SVM) to perform the authentication and make the final decision (Accept or Reject). The details of the authentication stage are discussed in the next subsection.

3.5. Authentication stage

For authentication, we performed *ten*-fold cross-validation using 60–20-20 training-validation-testing split. Therefore, the data were distributed and passed to the classifier for training. In the enrollment stage, the cancelable template is stored in a database. In the authentication stage, the cancelable template is fed to the ECG classifier and compared with the stored template. The distributions of the data (genuine and impostor) in training, validation, and testing cases (our baseline from the databases) in each fold are shown in Table 5 Where G and I refer to genuine and impostor, respectively.

In this stage, a separated classifier is used such as SVM, K-nearest neighbor (KNN), neural network, and others [44]. In this study, we selected SVM as a classifier to perform the authentication task and to achieve better authentication accuracy. The cancelable feature matrix is fed to the SVM to make the final decision (Accept or Reject). We selected the SVM classifier as it performs better for ECG authentication features than other classifiers and does not suffer from overfitting [46].

In the initial tests, we worked on the polynomial, linear, and radial basis function (RBF) kernels [47]. The RBF kernel executed better for our authentication system. The equation of the RBF kernel is:

$$K(x, x_i) = e^{-\|x - x_i\|^2} \tag{1}$$

where, x is the stored feature vector and x_i is the feature vector corresponding to the individual that attempting authentication and the || term is Euclidean distance. The main motivation for using the RBF kernel is to do calculations in any d-dimensional space. In addition, this kernel makes our regression line infinitely powerful.

Table 3
Converting binary number to DNA base.

DNA base	Binary sequence
A	01
C	00
G	11
T	10

Table 4
Converting DNA to corresponding RNA.

DNA base	RNA base
A	A
C	C
G	G
T	U

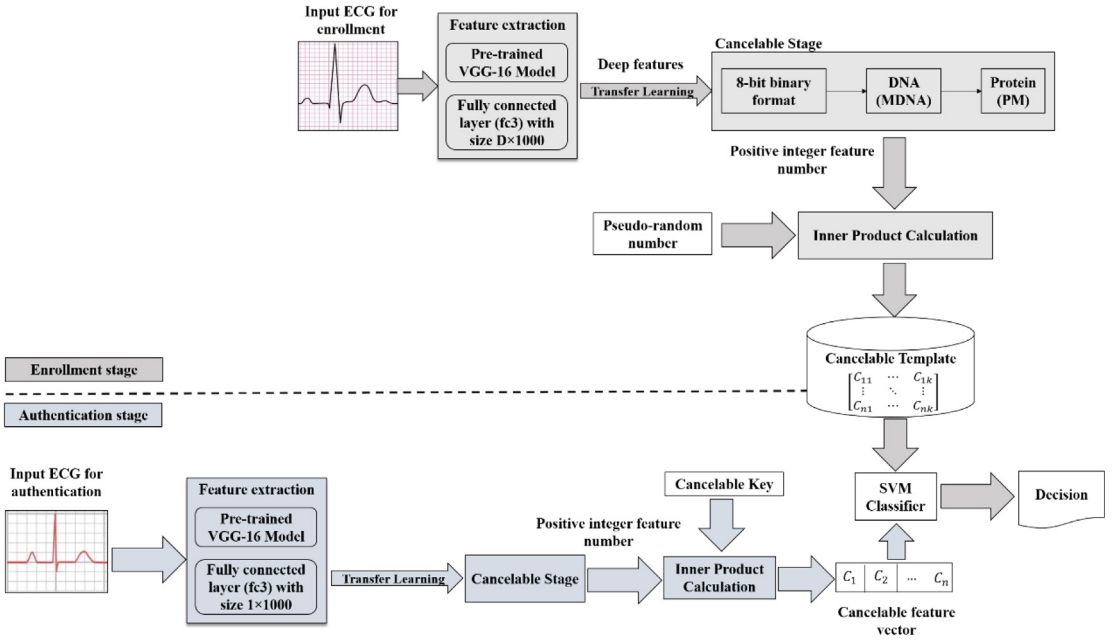


Fig. 3. Illustration of the proposed Authentication system based on our proposed Cancelable Method during: a) enrollment stage (above part) and b) authentication stage (below part).

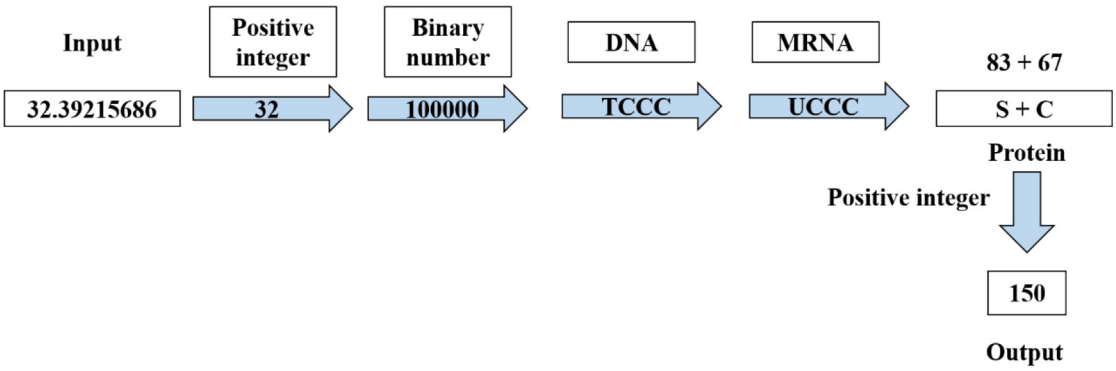


Fig. 4. An example for all steps of the proposed cancelable algorithm on one numeric value of the extracted features.

4. Results

Our system was executed on an Intel® Core (TM) i7-6800 K CPU and 16 GB RAM workstation equipped with MATLAB R2018a open-source for the preprocessing and feature extraction stages, and we employed Python programming language for the cancelable stage.

Table 5
Distributions of the baseline data from the used databases.

Database	Fold	Train		Validation		Test	
		G	I	G	I	G	I
ECG-ID	1	30	24	10	8	10	8
	2	24	30	13	5	13	5
	3	20	34	15	3	15	3
	4	36	18	7	11	7	11
	5	30	24	10	8	10	8
	6	20	34	15	3	15	3
	7	46	8	2	16	2	16
	8	40	14	5	13	5	13
	9	30	24	10	8	10	8
	10	24	30	13	5	13	5
PTB	1	99	75	33	25	33	25
	2	109	65	28	30	28	30
	3	89	85	38	20	38	20
	4	79	95	43	15	43	15
	5	95	79	35	23	35	23
	6	119	55	23	35	23	35
	7	129	45	18	40	18	40
	8	109	65	28	30	28	30
	9	99	75	33	25	33	25
	10	89	85	38	20	38	20

4.1. Evaluation metrics

The system was evaluated using the standard evaluation metrics, namely Accuracy, Precision, Recall, F1-Score, false rejection rate (FRR), false acceptance rate (FAR), and EER were computed.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

$$F1 - Score = \frac{2}{\frac{1}{Precision} + \frac{1}{Recall}} \tag{5}$$

If the system verifies two ECGs from different persons as a match, it is called a FAR, whereas if two samples of the same ECG are not matched by the system, it is called FRR. The EER is the location on a ROC curve where the FAR and FRR are equal. The higher the EER value, the lower the accuracy of the authentication system. Where, TP and TN correspond to the true positive and true negative predictions, respectively. In addition, FP and FN correspond to false positive, and false negative predictions, respectively.

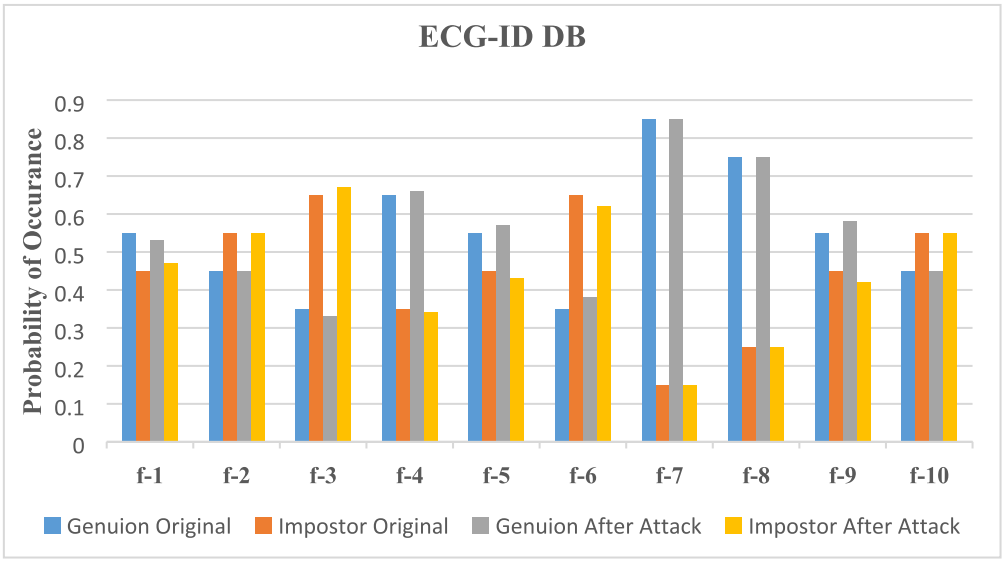
4.2. Authentication results

To assess the requirements of cancelable ECG templates (mentioned in the Introduction Section), we analyze our system's behavior according to *five* aspects: stolen-key scenario, performance, unlinkability, revocability, and irreversibility.

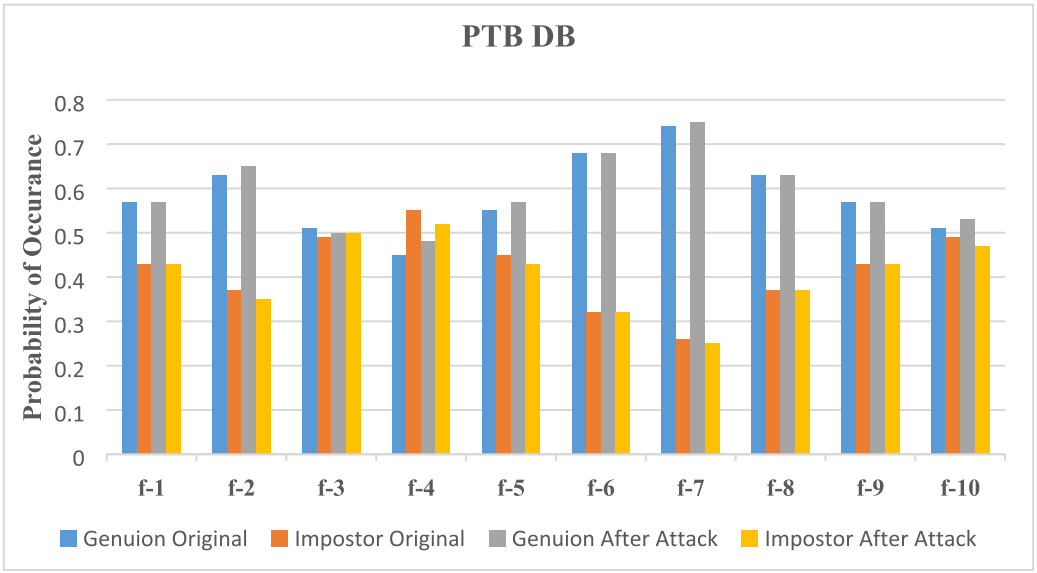
4.2.1. Stolen-key scenario

The usage of biometrics became meaningless if the proposed system depends only on cancelable keys. Therefore, we evaluated our system under this scenario (stolen-key scenario), where the imposters have obtained a valid key. In this scenario, we assigned the same key for all users in the database. Fig. 5 shows a comparison between the original distributions curves of the genuine vs impostor for the two datasets and the results after using this scenario in each fold (f) of the *ten*-fold. Where the original means that the distributions of the genuine and impostors according to the baseline from the database (as shown in Table 5).

From Fig. 5, we can find that the impostor and genuine population distributions in normal cases are almost the same impostor and genuine population distributions in case stolen the cancelable key among all folds. This proves that the proposed authentication system was able to differentiate correctly between the impostor and genuine even in the stolen key scenario. In addition, Fig. 6 presents the ROC curves for the proposed system for this scenario in each fold for both databases.



(a)



(b)

Fig. 5. Genuine vs Impostor distributions for (a) ECG-ID database, (b) PTB database.

4.2.2. Performance

Table 6 and Table 7 present the authentication results for the proposed system per fold for the *two* datasets by computing the accuracy, precision, recall, and F1-Score in each fold. Moreover, Fig. 7 presents the ROC curves for the proposed system for this scenario in each fold for both databases, while the variation in the EER for our proposed model during the ten-fold validation is presented in Fig. 8.

As noticed from Table 6, the average authentication accuracy of the system using the ECG-ID database is 98.60%. Also, Table 7 reported that the average authentication accuracy of the system using the PTB database is 98.85%. In addition, from Fig. 8, it is noteworthy that an average EERs of 0.44% and 0.40% are reported for the proposed method using ECG-ID and PTB databases, respectively.

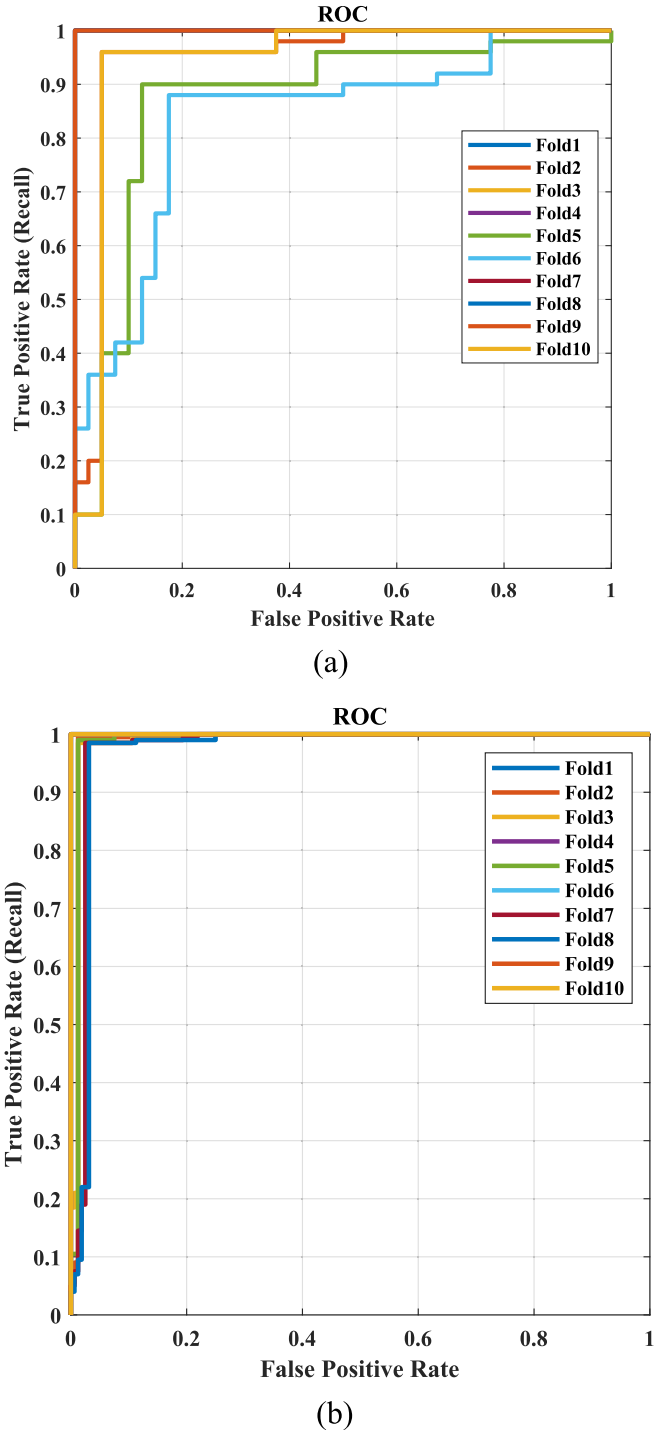


Fig. 6. ROC curves of the proposed method when stolen the cancelable key for each fold in both database: a) the ECG-ID database and b) The PTB database.

4.3. Privacy and security analysis

Privacy analysis focuses on the capability of the proposed system repelling against the regeneration of the original ECG information from the transformed version, while Security analysis focuses on the capability of the proposed system to prevent illegal access.

Table 6
Authentication results per fold on ECG-ID database.

Number of folds	Accuracy (%)	Precision (%)	Recall (%)	F1- Score (%)
1	99.56	99.56	99.56	99.56
2	100	100	100	100
3	99.30	99.60	99.98	99.40
4	97.78	100	96.15	98.03
5	98.72	98.90	99.98	99.40
6	97.78	98	97.50	97.74
7	100	100	100	100
8	100	100	100	100
9	99.5	99.78	99.99	99.80
10	100	100	100	100
Overall/Average	99.26	99.58	99.31	99.44

Table 7
Authentication results per fold on PTB database.

Number of folds	Accuracy (%)	Precision (%)	Recall (%)	F1- Score (%)
1	99.78	100	99.85	99.92
2	100	100	100	100
3	98.28	98.88	97.78	98.32
4	100	100	100	100
5	99.50	100	99.60	99.80
6	98.70	98.90	99.98	99.40
7	100	100	100	100
8	100	100	100	100
9	100	100	100	100
10	97.70	97.75	97.75	97.75
Overall/Average	99.39	99.55	99.49	99.52

4.3.1. Unlinkability

This property states that the transformed templates obtained from the same subject should be indistinguishable as if they were created from different ECGs. This property prevents cross-matching between multiple databases. In our case, we employed a Blum-Blum-Shub generator, which we can generate several cancelable templates from the same subject. Hence, different templates can generate from different ECGs as if they were created from the same subject. As a result, it suggests that the proposed method serves as a fully unlinkable system.

4.3.2. Revocability

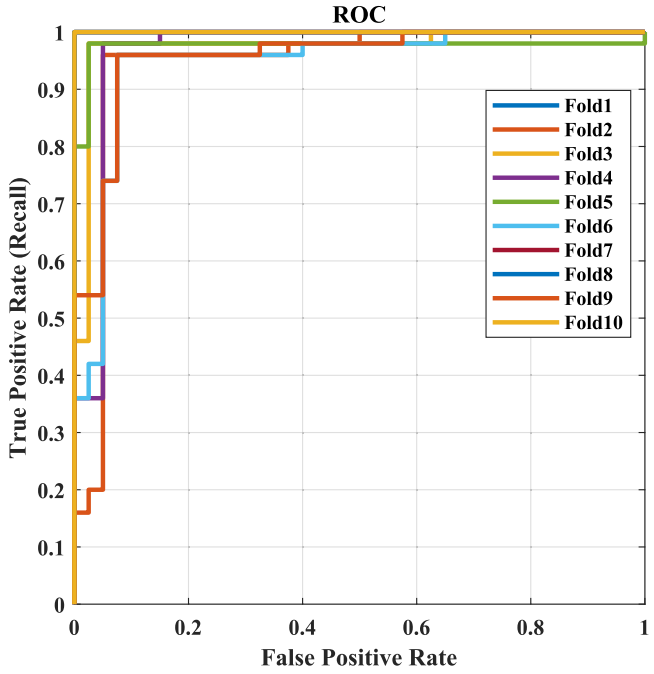
This property should evaluate whether there is any correlation between multiple templates generated from the same ECG. Here, in our case, the similarity is very low between the old and the new cancelable template. As a result, if the old cancelable template is compromised, we can reissue a new cancelable template easily.

4.3.3. Irreversibility

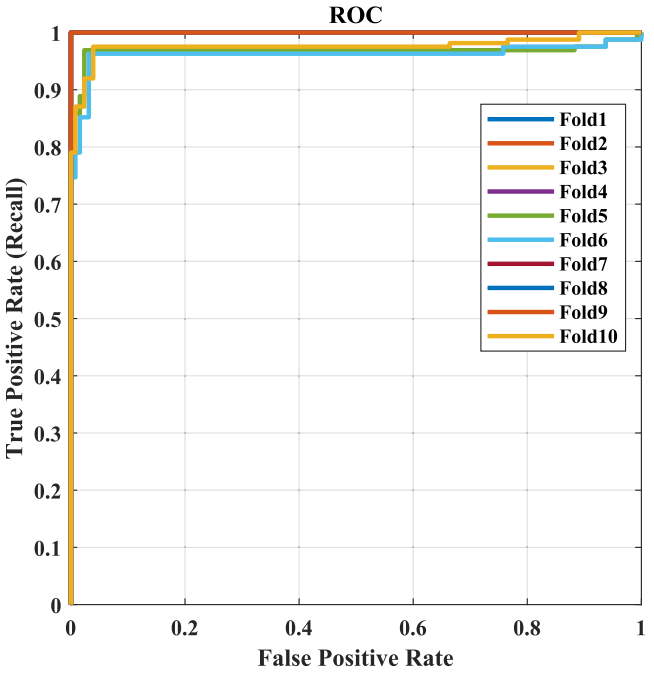
This property indicates the possibility of recovering the original feature template from the transformed template. In our case, the original features cannot be recovered when using the proposed cancelable method. For example, the proposed cancelable is irreversible in the worst case, if the imposter steals both the cancelable key and biometric data and if the imposter understands that the generated data is an amino acid. From the example in Fig. 4, if the imposter obtained the positive value (150) that results from the proposed method. The question is how the imposter can divide this value? Dose the imposter divides it into two numbers or three numbers or more? If for example two numbers, which two numbers from numerous numbers that give 150? (e.g., 100 and 50 or 70 and 80, etc.). Therefore, in our case, the security analysis of this property can be addressed in the proposed system.

5. Discussion

The analysis of the results shows that the proposed system achieved high authentication performance in different cancelable key scenarios and meets all cancelable requirements. From Figs. 5 and 6 we can observe that the proposed method in case of stolen the cancelable key achieved high authentication accuracy compared with the baseline data (very small difference), which satisfies the privacy requirement for ECG authentication. In the case of using different keys, we obtained an average accuracy of 99.62%, average precision of 99.58%, average recall of 99.31%, and average f1-score of 99.44% using the ECG-ID database as shown in Table 6. The results from Table 6 also show that the proposed authentication method can correctly authenticate 99.31% of all ECG images from the ECG-ID dataset and 0.69% of all ECG images from the database are wrongly rejected from our system. When using the PTB database, we achieved an average accuracy of 99.39%, average



(a)



(b)

Fig. 7. ROC curves of the proposed method when using different cancelable keys for each fold in both database: a) the ECG-ID database and b) The PTB database.

precision of 99.55%, average recall of 99.49% and average f1-score of 99.52% as shown in Table 7. The results from Table 7 also show that the proposed authentication method can correctly authenticate 99.49% of all ECG images from the ECG-ID dataset

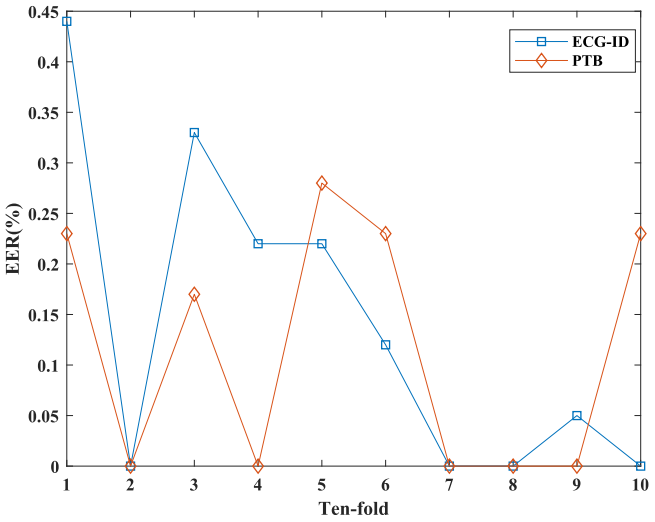


Fig. 8. Variation in the EER for our proposed model during the ten-fold validation in both databases.

and 0.51% of all ECG images from the database are wrongly rejected from our system. From the ROC curves in Fig. 7 and the variation of EER in Fig. 8, we can show that the proposed system achieved high accuracy in both datasets (slightly different in the accuracy of 0.13%), which mean that the proposed system overcome the overfitting problem and can fit with the new data with high accuracy. The results show the high performance of the proposed system, which satisfies the performance requirement for cancelable ECG.

The performance of the proposed method compared with the previous authentication methods based on PTB and ECG-ID databases is presented in Table 8. In order to make fair comparisons, we employed the same datasets and the same performance metric (EER) that was used in the previous works for evaluation.

From Table 8, we can find that the proposed algorithm achieved the best authentication performance among other previous studies. There are three studies [14,18,20] that obtained high accuracy than our study, however, these studies did not use any template protection, which gives low secure representation for ECG and does not satisfy privacy requirements for ECG authentication. Other methods that used template protection techniques for authentication [10,13,15,16] obtained low authentication accuracy than the proposed system and some of these methods used traditional machine learning approaches, which have some disadvantages over the proposed method (as mentioned earlier in the paper). We highlighted the advantages of the proposed system as follow:

- Our method is less complex than other authentication methods, especially the methods that used deep learning approaches because we employed a pre-trained model and a very simple cancelable technique compared with other cancelable techniques (e.g., Bio-Hashing).
- The system satisfies all cancelable requirements such as irreversibility, revocability and, unlinkability with high authentication performance.

Table 8
Comparison between our system and other previous systems based on the same databases.

Authors/year	Database/s	Methodology	Template Protection	Performance
Hammad *et al.* [15]2018	PTB	2D-CNN	Yes	EER = 3.20%
Hammad *et al.* [10]2019	PTB	Improved Bio-Hashing, Matrix operation and FFNN	Yes	Best EER = 14%
Kim *et al.* [13]2019	ECG-ID	GLRTCS	Yes	EER = 3.8%
Hammad and Wang [16] 2019	PTB	1D-CNN	Yes	EER = 3.50%
Hammad *et al.* [17]2019	PTB	CNN	No	EER = 1.63%
Li *et al.* [14]2020	ECG-ID	GNMF and sparse representation	No	EER almost = 0%
Ihsanto *et al.* [18]2020	ECG-ID	Hamilton's method and RDSCNN	No	EER = 0%
Hammad *et al.* [19]2020	PTB	ResNet-Attention	No	EER = 1.39%
Srivastva *et al.* [20]2021	PTB	transfer learning and ensemble learning	No	EER = 0.34%
Lynn *et al.* [21]2021	ECG-ID	RNN and LSTM	No	EER = 0.70%
Proposed2021	PTBECG-ID	DNA, Amino Acid, Deep Transfer Learning and SVM	Yes	Avg. EER = 0.40% (PTB)Avg. EER = 0.44% (ECG-ID)

- Most of the previous studies did not use any template protection, which gives low secure representation for ECG and did not satisfy privacy requirements for ECG authentication. Unlike these methods, the proposed method focused on template protection.
- Other methods that used template protection techniques for authentication obtained low authentication accuracy than the proposed system and some of these methods used traditional machine learning approaches, which have several disadvantages over the proposed method.
- The system overcome the overfitting problem and achieved high accuracy with small data. Unlike most of the previous authentication methods based on deep learning that need huge amounts of data to attain high accuracy.
- The proposed system is more robust and effective compared with the previous authentication methods.

Lastly, we want to confirm that a novel cancelable ECG biometric based on a combination of deep transfer learning with DNA and amino acid approaches has been confirmed for human authentication.

- Computational complexity:

We computed the time of the CPU that is required to execute each stage to evaluate the computational complexity of the proposed system (see Table 9). We can observe from Table 9 that the cost of the proposed system amounts to $O(2^n)$, which is the same as other template protection methods. However, the cost of the proposed cancelable method is less than other cancelable methods, which achieves the highest accuracy. We can conclude that the proposed cancelable method is more efficient than other methods. Therefore, principally, there is a tradeoff between cost and the improvement of the authentication performance, which is considered depending on the application.

6. Conclusion and future work

The main objective of this paper is to propose a novel cancelable ECG based on DNA and amino acid to protect ECG templates in the authentication system. The proposed cancelable approach meets all cancelable requirements such as *irreversibility*, *revocability,* and *unlinkability*, which enables strong attack resistance and computational efficiency. Results were benchmarked using the ECG-ID and PTB databases with 0.44% and 0.4% of EER were reported, respectively. Finally, the proposed cancelable method can provide decent adaptability for other biometric modalities (e.g., fingerprint, iris, face, EEG, etc.). As part of its downsides, our method takes a long time for the training, once the train is finished it takes seconds to make the test. In addition, we employed a big number of features that fed to the classifier, which increase the cost and the time of the implementation. Finally, we implemented our work on small datasets, which did not satisfy the requirements of real-time applications that needs big data. We suggested several solutions for these limitations in our future work.

As for future work, several research directions can be studied to further push the disadvantages of the proposed method. First, we can employ one of the optimization methods to optimize the extracted features (e.g., genetic algorithm). Second, we can try to use the proposed method on big data to satisfy the real-time application requirements. Finally, we can integrate some advanced biometric cryptography applications (e.g., key generation) to enhance the security of the ECG templates.

CRediT authorship contribution statement

Ahmed S. Sakr: Methodology, Software, Validation, Writing – original draft. **Paweł Pławiak:** Supervision, Investigation, Writing – review & editing. **Ryszard Tadeusiewicz:** Supervision, Writing – review & editing. **Mohamed Hammad:** Conceptualization, Methodology, Data curation, Writing – original draft, Software, Validation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Table 9
Computational complexity of the proposed method comparing with other methods.

Stages	Proposed	Ref. [10]	Ref. [13]	Ref. [15]	Ref. [16]
Preprocessing	$O(n)$	$O(n)$	$O(n)$	$O(n)$	$O(n)$
Feature extraction	$O(n)$	$O(n)$	$O(n)$	$O(n)$	$O(n)$
Cancelable	$O(n)$	$O(2^n)$	$O(2^n)$	$O(n^2)$	$O(n^2)$
Classification	$O(2^n)$	$O(n^5)$	$O(n)$	$O(2^n)$	$O(2^n)$
Total time	$O(2^n)$	$O(2^n)$	$O(2^n)$	$O(2^n)$	$O(2^n)$

References

[1] Z. Rui, Z. Yan, A survey on biometric authentication: Toward secure and privacy-preserving identification, IEEE Access 7 (2019) 5994–6009.
[2] Oak, R. (2018). A literature survey on authentication using Behavioural biometric techniques. *Intelligent Computing and Information and Communication*, *Advances in Intelligent Systems and Computing*, 173-181, vol 673. Springer, Singapore. https://doi.org/10.1007/978-981-10-7245-1_18.
[3] J.A. Unar, W.C. Seng, A. Abbasi, A review of biometric technology along with trends and prospects, Pattern Recogn. 47 (8) (2014) 2673–2688.
[4] V.M. Patel, N.K. Ratha, R. Chellappa, Cancelable biometrics: A review, IEEE Signal Process Mag. 32 (5) (2015) 54–65.
[5] K. Nandakumar, A.K. Jain, Biometric template protection: Bridging the performance gap between theory and practice, IEEE Signal Process Mag. 32 (5) (2015) 88–100.
[6] H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recogn. Lett. 126 (2019) 31–40.
[7] S.A. Israel, J.M. Irvine, A. Cheng, M.D. Wiederhold, B.K. Wiederhold, ECG to identify individuals, Pattern Recogn. 38 (1) (2005) 133–142.
[8] M. Sabry, M. Hashem, T. Nazmy, M.E. Khalifa, A DNA and amino acids-based implementation of playfair cipher. *IJCSIS) International Journal of Computer Science and Information*, Security 8 (3) (2010) 129–136.
[9] N. Dey, B. Nandi, M. Dey, D. Biswas, A. Das, S.S. Chaudhuri, in: February). BioHash code generation from electrocardiogram features, IEEE, 2013, pp. 732–735.
[10] M. Hammad, G. Luo, K. Wang, Cancelable biometric authentication system based on ECG, Multimedia Tools and Applications 78 (2) (2019) 1857–1887.
[11] Kim, H., Nguyen, M. P., & Chun, S. Y. (2017, July). Cancelable ECG biometrics using GLRT and performance improvement using guided filter with irreversible guide signal. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (pp. 454-457). IEEE.
[12] Chen, P. T., Wu, S. C., & Hsieh, J. H. (2017, July). A cancelable biometric scheme based on multi-lead ECGs. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (pp. 3497-3500). IEEE.
[13] H. Kim, S.Y. Chun, Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test, IEEE Access 7 (2019) 9232–9242.
[14] R. Li, G. Yang, K. Wang, Y. Huang, F. Yuan, Y. Yin, Robust ECG biometrics using GNMF and sparse representation, Pattern Recogn. Lett. 129 (2020) 70–76.
[15] M. Hammad, Y. Liu, K. Wang, Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint, IEEE Access 7 (2019) 26527–26542.
[16] M. Hammad, K. Wang, Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network, Computers & Security 81 (2019) 107–122.
[17] M. Hammad, S. Zhang, K. Wang, A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication, Future Gener. Comput. Syst. 101 (2019) 180–196.
[18] E. Ihsanto, K. Ramli, D. Sudiana, T.S. Gunawan, Fast and accurate algorithm for ECG authentication using residual depthwise separable convolutional neural networks, Applied Sci. 10 (9) (2020) 3304.
[19] M. Hammad, P. Pławiak, K. Wang, U.R. Acharya, ResNet-Attention model for human authentication using ECG signals, Expert Systems e12547 (2020) 1–17.
[20] R. Srivastva, A. Singh, Y.N. Singh, PlexNet: A fast and robust ECG biometric system for human recognition, Inf. Sci. 558 (2021) 208–228.
[21] H.M. Lynn, S.B. Pan, P. Kim, A deep bidirectional GRU network model for biometric electrocardiogram classification based on recurrent neural networks, IEEE Access 7 (2019) 145395–145405.
[22] Manisha, N. Kumar, Cancelable biometrics: A comprehensive survey, Artif. Intell. Rev. 53 (5) (2020) 3403–3446.
[23] N. Karimian, D. Woodard, D. Forte, Ecg biometric: Spoofing and countermeasures, IEEE Trans. Biomet. Behav. Ident. Science 2 (3) (2020) 257–270.
[24] R. Bousseljot, D. Kreiseler, A. Schnabel, Nutzung der EKG-Signaldatenbank CARDIODAT der PTB über das Internet, Biomedizinische Technik, Band 40, Ergänzungsband 1 (1995) S 317.
[25] Lugovaya T.S. Biometric human identification based on electrocardiogram. [Master's thesis] Faculty of Computing Technologies and Informatics, Electrotechnical University "LETI", Saint-Petersburg, Russian Federation; June 2005.
[26] M.I. Reddy, A.S. Kumar, K.S. Reddy, A secured cryptographic system based on DNA and a hybrid key generation approach, Biosystems 197 (2020) 104207.
[27] S. Kalsi, H. Kaur, V. Chang, DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation, J. Med. Syst. 42 (1) (2018) 1–12.
[28] S. Basu, M. Karuppiah, M. Nasipuri, A.K. Halder, N. Radhakrishnan, Bio-inspired cryptosystem with DNA cryptography and neural networks, J. Syst. Archit. 94 (2019) 24–31.
[29] T.W.D. Shen, W.J. Tompkins, Y.H. Hu, Implementation of a one-lead ECG human identification system on a normal population, J. Eng. Comput. Innov. 2 (1) (2010) 12–21.
[30] M. Hammad, A. Maher, K. Wang, F. Jiang, M. Amrani, Detection of abnormal heart conditions based on characteristics of ECG signals, Measurement 125 (2018) 634–644.
[31] M. Hammad, M.H. Alkinani, B.B. Gupta, A.A. Abd El-Latif, Myocardial infarction detection based on deep neural network on imbalanced data, Multimedia Syst. 1–13 (2021), https://doi.org/10.1007/s00530-020-00728-8.
[32] A.L. Goldberger, L.A.N. Amaral, L. Glass, J.M. Hausdorff, P.C. Ivanov, R.G. Mark, J.E. Mietus, G.B. Moody, C.-K. Peng, H.E. Stanley, PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals, Circulation [Online]. 101 (23) (2000), https://doi.org/10.1161/01.CIR.101.23.e215.
[33] C. Figuera, U. Irusta, E. Morgado, E. Aramendi, U. Ayala, L. Wik, J.o. Kramer-Johansen, T. Eftestøl, F. Alonso-Atienza, A. Talkachova, Machine learning techniques for the detection of shockable rhythms in automated external defibrillators, PLoS ONE 11 (7) (2016) e0159654.
[34] W.H. Press, S.A. Teukolsky, Savitzky-Golay smoothing filters, Comput. Phys. 4 (6) (1990) 669–672.
[35] A. Sedik, M. Hammad, F.E. Abd El-Samie, B.B. Gupta, A.A. Abd El-Latif, Efficient deep learning approach for augmented detection of Coronavirus disease, Neural Comput. Appl. 1–18 (2021), https://doi.org/10.1007/s00521-020-05410-8.
[36] M. Hammad, A.M. Iliyasu, A. Subasi, E.S. Ho, A.A. Abd El-Latif, A multitier deep learning model for arrhythmia detection, IEEE Trans. Instrum. Meas. 70 (2020) 1–9.
[37] A. Sedik, Lo'Ai Tawalbeh, M. Hammad, A.A.A. El-Latif, G.M. El-Banby, A.A.M. Khalaf, F.E.A. El-Samie, A.M. Iliyasu, Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities, IEEE Access 9 (2021) 94780–94788.
[38] S. Tammina, Transfer learning using vgg-16 with deep convolutional neural network for classifying images, Int. J. Sci. Res Publ. (IJSRP) 9 (10) (2019) 143–150.
[39] Z. Wu, C. Shen, A. van den Hengel, Wider or deeper: Revisiting the resnet model for visual recognition, Pattern Recogn. 90 (2019) 119–133.
[40] H. Ran, S. Wen, K. Shi, T. Huang, Stable and compact design of Memristive GoogLeNet Neural Network, Neurocomputing 441 (2021) 52–63.
[41] G. Viswanatha Reddy, C.V.R. Dharma Savarni, S. Mukherjee, Facial expression recognition in the wild, by fusion of deep learnt and hand-crafted features, Cognit. Syst. Res. 62 (2020) 23–34.
[42] C. Sitaula, M.B. Hossain, Attention-based VGG-16 model for COVID-19 chest X-ray image classification, Appl. Intell. 51 (5) (2021) 2850–2863.
[43] Gupta, D., Jain, S., Shaikh, F., & Singh, G. (2017). Transfer learning & The art of using Pre-trained Models in Deep Learning. *Analytics Vidhya*.
[44] W. Książek, M. Hammad, P. Pławiak, U.R. Acharya, R. Tadeusiewicz, Development of novel ensemble model using stacking learning and evolutionary computation techniques for automated hepatocellular carcinoma detection, Biocybernet. Biomed. Eng. 40 (4) (2020) 1512–1524.
[45] C. Ding, Blum-blum-shub generator, Electron. Lett. 33 (8) (1997) 677, https://doi.org/10.1049/el:19970440.
[46] K.K. Patro, S.P.R. Reddi, S.K.E. Khalelulla, P. Rajesh Kumar, K. Shankar, ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm, J. Supercomput. 76 (2) (2020) 858–875.

[47] Hammad, M., & Wang, K. (2017, April). Fingerprint classification based on a Q-Gaussian multiclass support vector machine. In *Proceedings of the 2017 International Conference on biometrics engineering and application* (pp. 39-44)
[48] A.S. Sakr, M.Y. Shams, A. Mahmoud, M. Zidan, Amino Acid Encryption Method Using Genetic Algorithm for Key Generation, CMC-Comput. Materials & Cont. 70 (1) (2022) 123–134.
[49] Labati, Ruggero Donida, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. "Deep-ECG: Convolutional neural networks for ECG biometric recognition." *Pattern Recognition Letters*, 126 (2019): 78-85.
[50] Y. Li, Y. Pang, K. Wang, X. Li, Toward improving ECG biometric identification using cascaded convolutional neural networks, Neurocomputing 391 (2020) 83–95.