Received October 29, 2018, accepted November 27, 2018, date of publication December 13, 2018, date of current version March 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2886573

Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint

MOHAMED HAMMAD, YASHU LIU, AND KUANQUAN WANG, (Senior Member, IEEE)
School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China

Corresponding author: Kuanquan Wang (wangkq@hit.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61571165.

ABSTRACT A multimodal biometric system integrates information from more than one biometric modality to improve the performance of each individual biometric system and make the system robust to spoof attacks. In this paper, we propose a secure multimodal biometric system that uses convolution neural network (CNN) and Q-Gaussian multi support vector machine (QG-MSVM) based on a different level fusion. We developed two authentication systems with two different level fusion algorithms: a feature level fusion and a decision level fusion. The feature extraction for individual modalities is performed using CNN. In this step, we selected two layers from CNN that achieved the highest accuracy, in which each layer is regarded as separated feature descriptors. After that, we combined them using the proposed internal fusion to generate the biometric templates. In the next step, we applied one of the cancelable biometric techniques to protect these templates and increase the security of the proposed system. In the authentication stage, we applied QG-MSVM as a classifier for authentication to improve the performance. Our systems were tested on several publicly available databases for ECG and fingerprint. The experimental results show that the proposed multimodal systems are efficient, robust, and reliable than existing multimodal authentication systems.

INDEX TERMS Authentication, CNN, decision fusion, ECG, feature fusion, fingerprint, multimodal.

I. INTRODUCTION

Biometric system is a pattern recognition system that requires biometric data from individuals based on their physical and/or behavioral traits, such as a fingerprint, Electrocardiogram (ECG), iris, face, or voice pattern [1]. Unlike traditional methods such as passwords and tokens, biometrics cannot be copied, shared, lost, forgotten, manipulated or forged. Nowadays, biometrics are no longer confined to criminal law enforcement. In addition, more businesses use biometrics to regulate access to buildings and information systems. In real-world applications, there are several problems with unimodal biometric systems which operate on a single biometric modality such as noise in sensed data, intra-class variations, inter-class similarities, nonuniversality and spoof attacks. To address these drawbacks of unimodal systems, we proposed a novel multi-biometric system based on ECG and fingerprint. Our system overcomes the limitations of both single systems, improves the performance of the overall system and enhances the security, as in this system we combine two characteristics, one is physical (fingerprint) and the other is vital (ECG) which offers the advantage of liveness detection to the system that makes the system robust to spoof attacks. Unlike other multimodal biometric systems that would be very inconvenient (e.g. a face, ear and fingerprint-based multimodal biometric system), the ECG signals can easily be acquired from fingers, which make the system very convenient and efficient.

Several multimodal biometric systems based on conventional traits such as fingerprint and iris have been developed during past decades [2]–[4]; there are only a few works about a multimodal biometric system that includes ECG. Komeili *et al.* [5], fused ECG with a fingerprint for liveness detection and authentication. However, they focused on liveness detection rather than authentication and they did not focus on fingerprint authentication performance. Zhao *et al.* [6] suggested a multimodal biometric system with the finger-based ECG signal and fingerprint recordings but they did not evaluate this system. Manjunathswamy *et al.* [7], proposed an algorithm for biometric recognition using ECG and fingerprint. They used decision level fusion to fuse ECG with the fingerprint. However, they have worked on a low authentication threshold (75%), and they have not provided information on the number of users in the study. Singh *et al.* [8] also reported such a multimodal biometric system, but the ECG data they used was captured from the chest which disregards one of the main advantages of a compact finger-based system. However, in these studies Komeili *et al.* [5], Zhao *et al.* [6], Manjunathswamy *et al.* [7], Singh *et al.* [8] concentrated on the conventional machine learning approaches, which often suffer from overfitting and show lower performance when validated on a separate dataset. In this study, we did not follow the conventional process by building the proposed multimodal biometric system based on convolutional neural network (CNN).

Recently, CNN has been employed in multimodal biometric systems [9]–[11]. However, none of the previous multimodal systems based on CNN worked on ECG with the fingerprint for authentication.

In this paper, we proposed two multimodal systems using CNN based on a different level fusion of ECG and fingerprint for human authentication.

In the first system, we proposed a sequential multimodal system using CNN based on decision level fusion of ECG and fingerprint for human authentication. The feature extraction for individual modalities is performed using CNN and then biometric templates are generated from these features. After that, we have applied the improved Bio-Hashing technique, which is one of the cancelable biometric techniques and proposed by Lumini *et al.* [12] to protect these templates and increase the security of the proposed system. In the authentication stage, we proposed Q-Gaussian multi-class support vector machine (QG-MSVM) [13] as a classifier for authentication to improve the performance. Finally, we used decision level fusion to make the final decision.

In the second system, we proposed a parallel multimodal system using CNN based on feature level fusion of ECG and fingerprint for human authentication. The feature extraction for individual modalities is performed using CNN and then the output feature vectors of the ECG-CNN and fingerprint-CNN are fused based on the fusion method. In the authentication stage, we employed the same classifier (QG_MSVM) that used in the first system. In this study, we employed two ECG and two fingerprint databases to evaluate the performance of the proposed multimodal biometric system. The Physikalisch-Technische Bundesanstalt (PTB) database [14] and Check Your Biosignals Here initiative (CYBHi) database [15], which are employed for ECG, LivDet2015 database [16] and FVC 2004 database [17], which are employed for the fingerprint.

The main contributions of this paper can be summarized as follows:

- We employ the pre-trained deep CNN models for ECG and fingerprint authentication, where we use VGG-Net as a feature extractor by selecting valuable layers to get a good representation of ECG and fingerprint data, which achieves superior results compared with the previous hand-designed works.
- We are the first to propose a multimodal system based on ECG and fingerprint using CNN for human authentication, where all previous multimodal biometric systems that used CNN are worked on other biometrics.
- We are the first to apply the improved Bio-Hashing technique on ECG to protect the extracted deep features and to enhance the accuracy of authentication. Also, we applied it to protect the deep features of the fingerprint.
- We are the first to make internal feature fusion on ECG and fingerprint system. In this fusion, different layers of the CNN model are combined, where the output of each layer is supposed as a feature descriptor and combined to construct final feature representation of the input image. The internal deep feature fusion performs better than other previous hand-designed and current methods based on pre-trained CNN.

The rest of this paper is organized as follows: Section II explains the details of the first proposed approach including ECG authentication, fingerprint authentication, decision level fusion of ECG and fingerprint and template updating. In Section III, the details of the second proposed multi-biometric system are presented including ECG and fingerprint feature extraction using CNN, feature fusion of ECG and fingerprint and classification based on QG-MSVM. In Section IV, we describe all datasets used in the experiments and evaluate the proposed system on these datasets. The experimental results are analyzed in Section V. Finally, Section VI concludes the paper.

II. THE PROPOSED SEQUENTIAL MULTIMODAL SYSTEM USING CNN BASED ON DECISION LEVEL FUSION

This section presents the detail about the first proposed multimodal biometric system using CNN for human authentication. In the proposed sequential multimodal system, the system must begin with the ECG authentication to ensure the liveness detection. In other words, the ECG authentication is better at rejecting impostors and the fingerprint authentication is better at accepting genuine users. After the system has rejected the impostors and accepted the genuine users, it will authenticate the remaining subjects using the fusion of ECG and fingerprint as shown in Figure.1.

As shown in Figure.1 for authentication, the system will try to authenticate the user using its ECG (to ensure the liveness detection), if the user is rejected then that is the final decision of the overall system, however, the accepted users will be given to the fingerprint authentication. If the user is accepted at this stage, then that is the final decision for that user. The remaining rejected users will be given to the combination of the ECG and fingerprint multimodal biometric system which fuses the two at decision level to make the final decision.

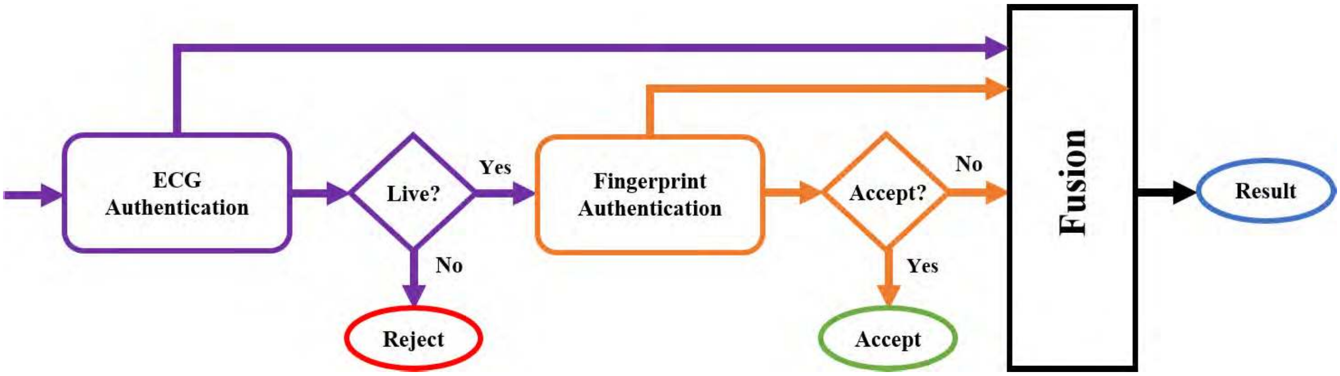

FIGURE 1. Block diagram of the first multimodal system.

A. ECG AUTHENTICATION

In this work, we proposed the ECG authentication system using CNN without performing any noise filtering or segmentation techniques. The proposed ECG authentication system comprises four main stages: First, transform the one-dimensional ECG signals into two-dimensional ECG images, unlike most of the previous algorithms which used noise filtering or segmentation and cause a loss of information about the ECG waveform, specifically about the variability of the ECG signal. Also, data augmentation can apply to the trained ECG images to improve the classification accuracy, which is difficult to be applied on a one-dimensional ECG signal. Second, the feature template is generated using the proposed CNN model. After that, the improved Bio-Hashing technique applies to protect this template. Finally, QG-MSVM classifier is proposed for classification. The proposed CNN model and each aspect of the proposed system is described in more details in the following sections.

B. ECG SIGNAL TRANSFORMATION

We transformed the one-dimensional ECG signal to two-dimensional ECG image by plotting each ECG signal as an individual 224 × 224 gray-scale image as in [18]. The reason we applied 2D CNN by converting the ECG signal into ECG image form in this paper is that 2D convolutional and pooling layers are more suitable for filtering the spatial locality of the ECG images. As a result, higher ECG authentication accuracy can be obtained [18]. Moreover, unlike most of the previous algorithms, we did not need to use noise filtering or segmentation, where using it causes a loss of information about the ECG waveform, specifically about the variability of the ECG signal. Also, it is easy to apply data augmentation to the trained ECG images to improve the performance, which is difficult to be applied on a one-dimensional ECG signal.

C. FINGERPRINT AUTHENTICATION

In this section, we describe the proposed system for fingerprint authentication using VGG-Net as a feature extractor. Our proposed system consists of the following four main steps: 1) preprocessing the fingerprint image; 2) feature extraction with VGG-Net; 3) using the improved Bio-Hashing method to protect the feature template; 4) using QG-MSVM as a classifier for fingerprint classification.

We adopt the procedure in [19] for the preprocessing algorithm, which consists of three steps: image enhancement, binarization and thinning. After the preprocessing stage, the features are extracted from the thinned fingerprint image using the proposed CNN model.

D. THE PROPOSED CNN MODAL

CNN is a fundamental example of deep learning where the structure consists of many hidden layers and parameters [20]. CNN has been applied in image processing [21], natural language processing [22] and other kinds of cognitive tasks [23], [24]. Recently, numerous CNN models have been developed for large-scale image classification such as Caffe-Net [25], Alex-Net [26], and VGG-Net [27]. The proposed algorithm is based on the VGG-Net for feature extraction because it has a much deeper architecture than other models, hence it can provide more informative features. The VGG-Net outperforms the previous generation of CNN models, which is trained with the public ImageNet dataset and achieves the second place in the detection task of the ImageNet 2014 challenge [28]. Different from most previous algorithms, which are based on low-level features, our system is based on the internal fusion of the features learned by the VGG-Net. In this study, the first and the second output fully connected layers are supposed as a feature descriptor of the ECG and fingerprint for authentication to describe it with informative features.

Figure.2 describe the architecture of VGG-Net that used in this study to generate the feature templates of ECG and fingerprint. It comprises five convolutional layers, where each one followed by a pooling layer, three fully connected layers and a soft-max layer, where the input images are resized to $224 \times 224 \times 3$. The configuration of the fully connected layers is the same in all networks. All hidden layers are supplied with the rectified linear unit (ReLU) activation function and do not contain local response normalization (LRN), as it does not improve the performance on our ECG signal dataset,

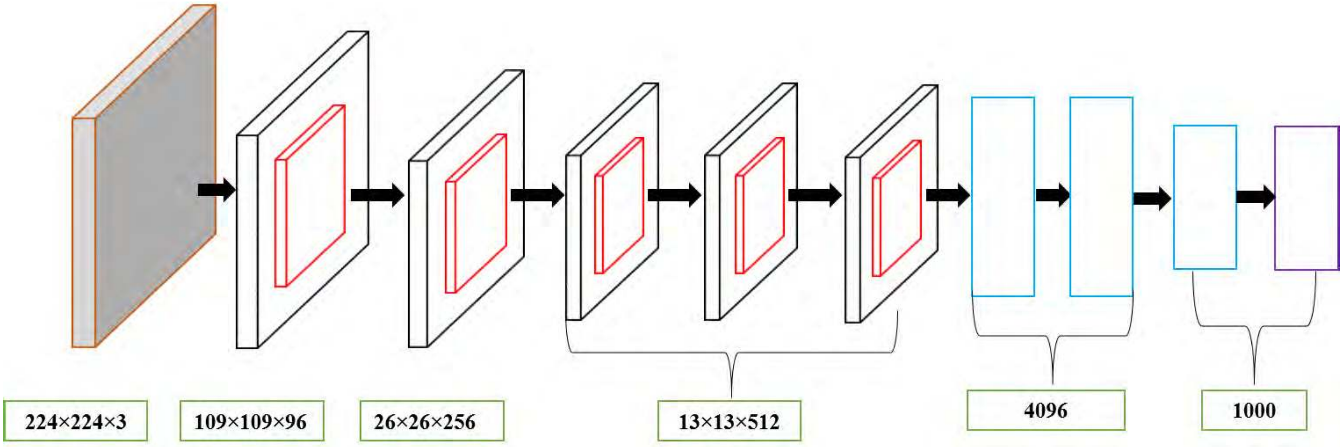

FIGURE 2. Architecture of the VGG-net. The boxes show the size of each feature layer, fully connected layers, and the size of the output.

instead, it leads to increase the time complexity and the memory consumption. The mathematical form of ReLU function is as follows:

$$f(x) = max(0, x) \tag{1}$$

where x is the input to a neuron. This is also known as a ramp function. This activation function makes the network converge much faster also; it is computationally efficient because it is implemented using a simple threshold. The final layer in the proposed model is a soft-max layer.

E. UPDATING OF ECG AND FINGERPRINT TEMPLATES (CANCELABLE METHOD)

In this paper, we utilized the improved Bio-Hashing method, which is one of the cancelable biometric techniques to protect the ECG and fingerprint features template and increase the authentication accuracy of the system. Lumini *et al.* [12] proposed an improved Bio-Hashing method, which is an updated version of Bio-Hashing method [29]. In [12], they proposed several solutions leading to an improved version of the Bio-Hashing method and overcoming most of the Bio-Hashing problems.

The basic idea of the improved Bio-Hashing method is 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 threshold (τ) instead of a fixed one. In this paper, we applied the improved Bio-Hashing technique to protect the deep features from ECG and fingerprint by producing a transformed template of ECG and fingerprint which is irrevocable to the original features, whereas we applied the cancelable method on the features from the fusion of the first and the second fully-connected layer from the ECG-CNN and fingerprint-CNN. We use the following steps to apply this method to protect the deep features of ECG and fingerprint:

- Each feature vector was normalized using the Gram–Schmidt ortho-normalization to produce the normalization feature matrix [30].
- Blum-Blum-Shub method is used to produce a set of pseudo-random vectors with the uniform distribution 30].

N-normalize

- vectors were generated from the pseudo-random vectors.
- The inner product was computed between the normalized feature matrix and the normalized random matrix to generate the cancelable matrix template.

In this study, after lots of experiments, we found that the following parameters are given the best results after applying it to the proposed system: $m = 4096$; $\tau_{\max} = 0.1$; $\tau_{\min} = -0.1$; $p = 5$; $k = 5$; $q = 5$. Where: m is the length of a bit string, τ is a present threshold between $\tau_{\min}$ and $\tau_{\max}$, p is the number of threshold steps, k is the selected number of projection spaces and q is a bit vector used for feature permutations.

F. CLASSIFICATION

In this study, Q-Gaussian multi-class support vector machine (QG-MSVM) was applied to classify ECG and fingerprint for authentication, where the Q-Gaussian function is incorporated into SVM as a kernel function. In our previous work [13], we used QG-MSVM to classify fingerprints, and achieved a good result comparing to other SVM kernels. In this work, we modified the QG-MSVM to classify ECG besides using it to classify fingerprint. The Q-Gaussian function is employed by replacing exponential expression in standard Gaussian function with Q-exponential expression while maximizing entropy under certain constraints as in (2):

$$K(x, x_i) = e_q\left(-\frac{\|x - x_i\|^2}{(3-q)\,\sigma^2}\right) \tag{2}$$

where $\boldsymbol{q}$ is a real valued parameter and e_q is $\boldsymbol{q}$-exponential function defined in [31] and given by (3):

$$e_q = (1-(q-1))^{\frac{-1}{q-1}}, \quad if \;\; (1-(q-1)) \geq 0 \qquad (3)$$

The equation in (2) can be rewritten as (4):

$$k\,(x, x_i) = \left(1 + \frac{q-1}{(3-q)\,\sigma^2}\,\|x - x_i\|^2\right)^{\frac{1}{1-q}} \qquad (4)$$

In this work we used the same values in our previous work [13], which give the best results comparing to other SVM kernels: $\frac{\mathbf{1}}{\boldsymbol{\sigma}^{\mathbf{2}}}$ is assigned to 0.5 and $\boldsymbol{q}$ to 1.5.

In addition, we employed a ten-fold cross-validation approach [32]. Therefore, the total ECG and fingerprint images were divided into ten equal parts. Nine out of ten parts were used for training and the remaining were used for testing. This method was repeated ten times by shifting the testing part. In each fold, the performance of the system was evaluated. The average of all ten-folds gives the total performance of the system.

G. INTERNAL FUSION

This study proposed an internal fusion, which is fused the internal features of each biometric. In this case, for both systems (ECG and fingerprint), we used the first and second outputs of fully connected layers as the feature descriptor of the ECG and fingerprint for authentication. Figure.3 shows the criterion of considering the selected layers by selecting the two layers that achieve the highest accuracy comparing to other layers in the proposed model.

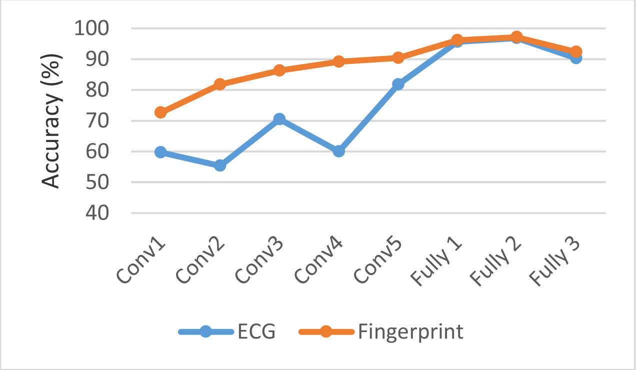

FIGURE 3. **Effect of the CNN layers on the classification accuracy on the two biometrics.**

We calculate the new transformation of those features based on the concatenation and the addition method. After that, the composite feature vector was then used for the classification process (as in the first system) or applied the external feature fusion on it (as in the second system). Figure.4 describes the procedure followed for internal features fusion in each biometric where we used CNN to extract deep features from the input ECG and fingerprint images. Then, we selected two feature sets from the two fully connected layers. After that, we combined (concatenation/addition) the features to represent the input images by single informative features.

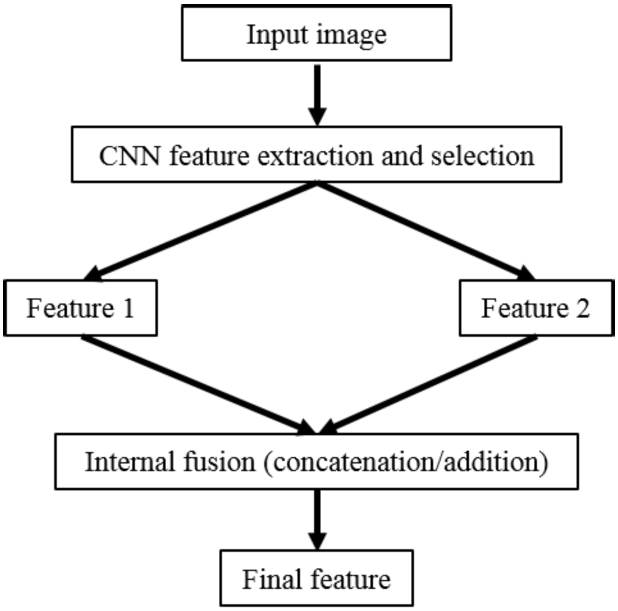
Input image
CNN feature extraction and selection
Feature 1
Feature 2
Internal fusion (concatenation/addition)
Final feature

FIGURE 4. **Internal fusion based on concatenation and addition technique.**

H. DECISION FUSION OF ECG AND FINGERPRINT

We investigated the fusion of ECG and fingerprint for human authentication. Fusions in multi-biometric systems can be classified into different levels: (1) sensor level fusion, (2) feature extraction level fusion, (3) matching level fusion, and (4) decision level fusion. We have chosen the decision-based fusion strategy by combining the final Boolean result obtained from the ECG authentication system and the one obtained from the fingerprint authentication system. In a multi-biometric authentication system, the simplest method of combining decision outputs by the different matchers (QG-MSVM in our case) is to use the "AND" and "OR" rules. The system output accepted the user using "AND" rule only when the result of all the biometric matchers (ECG and fingerprint classifiers) are accepted. On the contrary, the system output accepted the user using "OR" rule when at least the result of one biometric matcher (ECG or fingerprint classifiers) is accepted. In this paper, after the system has rejected the impostors and accepted the genuine users, it authenticates the remaining subjects using the "OR" rule to get the final decision of the proposed sequential multimodal system as shown in Figure 5. We used "OR" rule because the proposed system is started with ECG authentication then fingerprint authentication where the ECG authentication is better at rejecting impostors and the fingerprint authentication is better at accepting genuine users thus, "OR" rule is used to get the best performance.

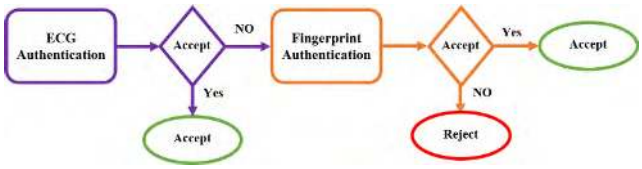

FIGURE 5. Decision fusion used "OR" rule of the proposed sequential multimodal system.

I. DATA AUGMENTATION

Data augmentation is a technique to generate artificial data samples from the original ones. It is used to make the proposed model more robust for overfitting. It has been successfully used in previous works in computer vision [33], [34].

Our dataset augmentation implementation is similar to the one presented in [35]. Moreover, we implemented addition augmentation as expand to the work in [36], such as color manipulation. Therefore, we obtained a database that is 10 times larger than the original one: 4 times are due to reflections, 4 times are due to translations and 2 times color manipulation.

III. THE PROPOSED PARALLEL MULTIMODAL SYSTEM USING CNN BASED ON FEATURE LEVEL FUSION

The proposed parallel multimodal biometric authentication system for ECG and fingerprint is shown in Figure.6.

In this system, all users are required to perform authentication using their ECG and fingerprint, unlike the first system which does not require performing authentication using both biometrics. In a verification setting, each user presents his ECG and fingerprint to the respective sensors and claims his identity. During this system, we employed the same CNN that used in the first system and then applied the feature level fusion. The output feature vectors of the ECG-CNN and fingerprint-CNN are fused as shown in Figure.7.

From Figure.7, we selected the feature set from the first and second fully connected layers of ECG-CNN and fingerprint-CNN. After that, we calculated the new transformation of those features (Fusion-fc) based on the fusion method. Finally, the fused feature vector was fed to the QG-MSVM classifier for authentication.

A. FEATURE FUSION OF ECG AND FINGERPRINT

Fusion can be done in different levels of multimodal biometric systems, such as the feature level, the score level, and the decision level. In the proposed parallel system, we used feature level fusion, which is believed to be very promising as feature sets can provide more information about the input biometrics than other levels. This fusion is done by combining the feature vector that extracted from the input ECG image with the feature vector that extracted from the input fingerprint image and creates a new feature vector to represent the individual. We calculate the new transformation of those features based on the concatenation method. After that, the composite feature vector is then used for the classification process.

In the concatenation method, two set of features are concatenated into one feature. It supposes that f_1 and f_2 are two features extracted from an input image with v_1, v_2 vector dimension, respectively, and then the fused feature is z with size equal to $(v_1 + v_2)$.

IV. EXPERIMENTAL SETUP AND RESULTS

We have evaluated our algorithm on a PC workstation with 2.7-GHz CPU with 32 GB of memory and a moderate

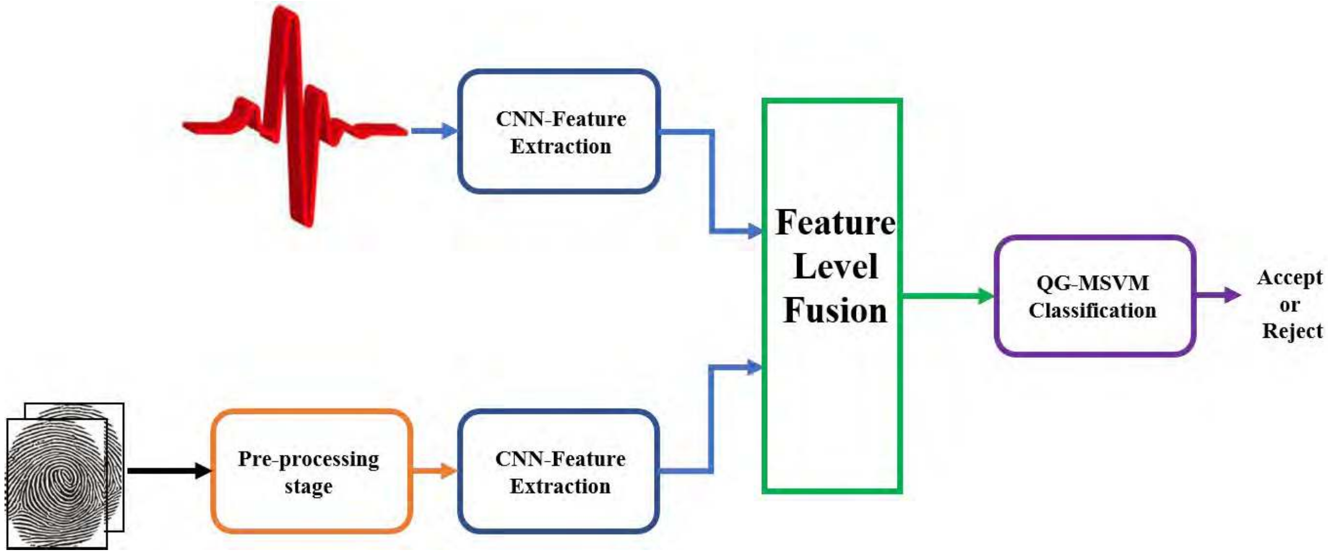

FIGURE 6. Block diagram of the second multimodal system.

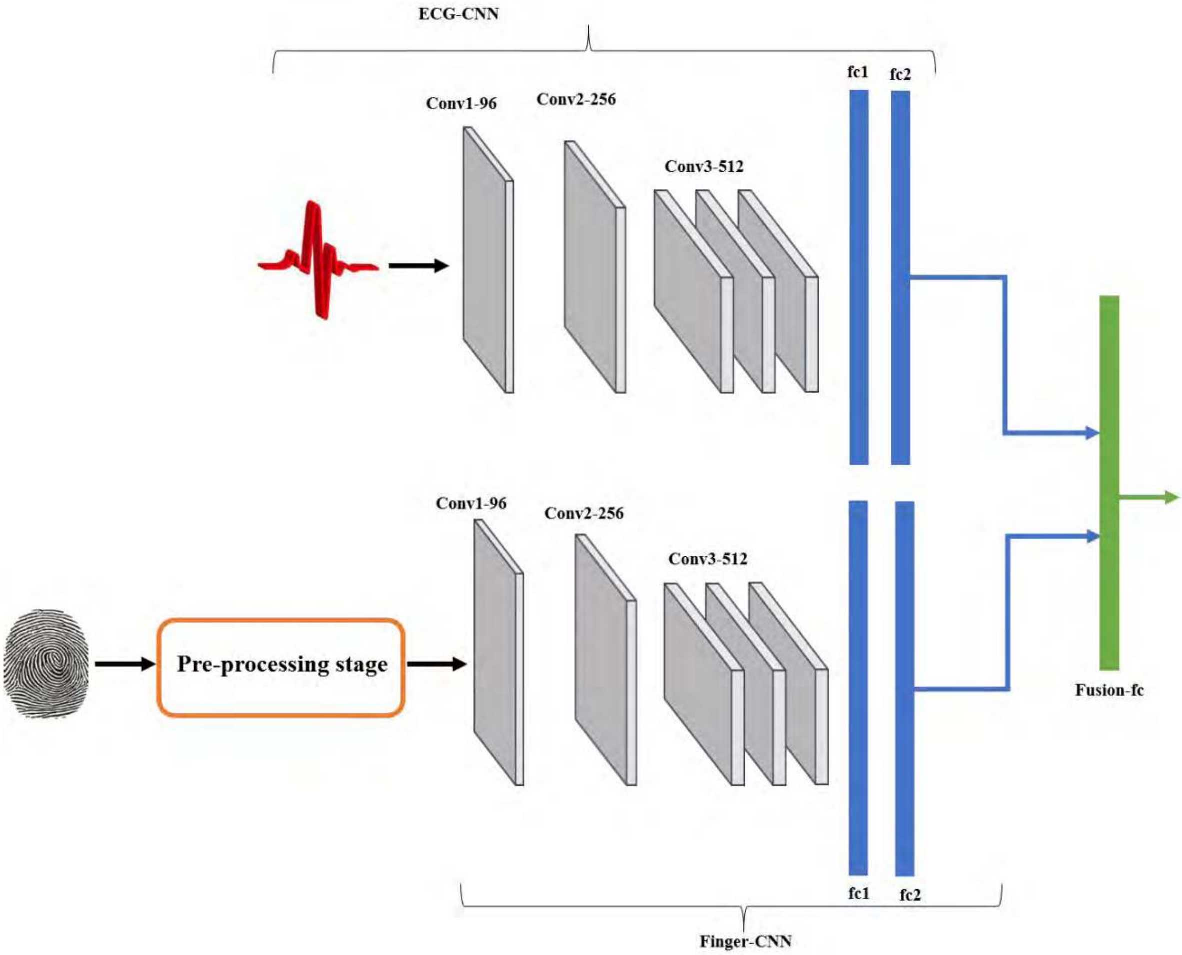

FIGURE 7. Proposed multi-CNN feature fusion.

GPU card. All methods have been implemented using Microsoft Windows 10 Pro 64-bit and MATLAB R2017a. The capability of using the proposed system was examined on two ECG databases: The PTB database and the CYBHi database and two fingerprint databases: The LivDet2015 database and FVC 2004 database. The description of the data sets has been given in the following section where we also analyze the parameters of the proposed system. And then the results are discussed.

A. DATASETS

Two different databases are used in this paper for ECG authentication. The first database is PTB database [14], which includes 290 subjects and uses one to five records to represent each subject. It contains 549 records such that each record includes 15 simultaneously measured signals, namely the conventional 12 leads together with the 3 Frank lead ECG. Each signal is digitized at 1000 samples per second, with 16-bit resolution over a range of ± 16.384 mV. In practice, the recordings may be available up to 10 KHz at sampling depending on the contributors' request of the database [14]. In this study, we used 200 ECG records of a two-second duration of Lead II obtained from 100 different subjects selected from PTB. We consider two records from each subject. Figure.8 shows an example of one record from PTB database.

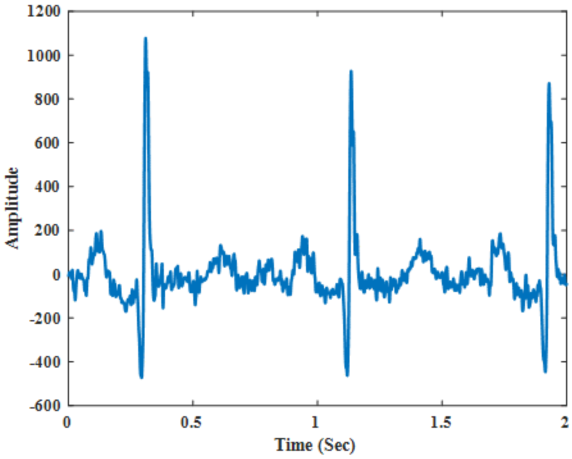

FIGURE 8. Example of one record from PTB database [14].

The second database is CYBHi database, which is provided by the Check Your Biosignals Here initiative [15]. In this database, two ECG sensors were used; one for the signals acquired with two dry electrodes at the palms and another acquired with Electrolycras at the index and middle fingers as shown in Figure.9. The data were collected from 65 volunteers (16 females and 49 males) with an average age between 21.64 and 40.56 years, where 63 subjects were recorded in a two-session in three months. The recordings are available with sampling rates 1 KHz and 12-bit resolution. We consider two records from each subject and each record is a two-second duration of ECG signals.

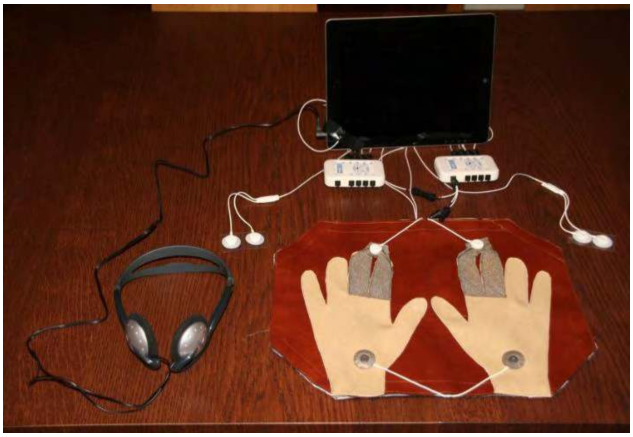

FIGURE 9. Full experimental setup to collect CYBHi database [15].

In addition, two different databases are used in this paper for fingerprint authentication. The first one is LivDet2015 fingerprint database [16] which includes 4 datasets corresponding to 4 different scanners: CrossMatch, DigitalPersona, GreenBit and Biometrika, each having approximately 2,000 images from fake and real fingerprints. This database is divided into two sets: training and testing. Fake samples were obtained from 6 different spoof materials including Ecoflex, Gelatine, Latex, WoodGlue, Liquid Ecoflex and RTV. We randomly selected 100 subjects and used only two samples for each subject. Figure.10 shows typical examples of real and fake fingerprint images that can be obtained from one dataset of the LivDet2015 database used in the experiments.

The second one is the FVC 2004 database [17], which is consisted of four different datasets (DB1, DB2, DB3 and DB4). In each dataset there are 110 fingers and 880 impressions (8 impressions per finger). Three different scanners were used to collect these fingerprints (Optical Sensor for DB1 and DB2, Thermal Sweeping Sensor for DB3 and Synthetic Generator for DB4). All fingerprint images are 8-Bit gray-level TIF files and the image resolution is 500dpi. We randomly selected 63 subjects and consider only two samples for each subject as shown in Figure 11.

In this study, we constructed two multimodal databases by combining the ECG and fingerprint datasets, and then we used these two databases for evaluation to show that our system is not restricted to a single database. In the first multimodal database (MDB1), we randomly assigned one subject from the PTB ECG database to a subject from the LivDet2015 fingerprint database. Finally, the MDB1 is collected from 100 subjects; each has two ECG and fingerprint samples.

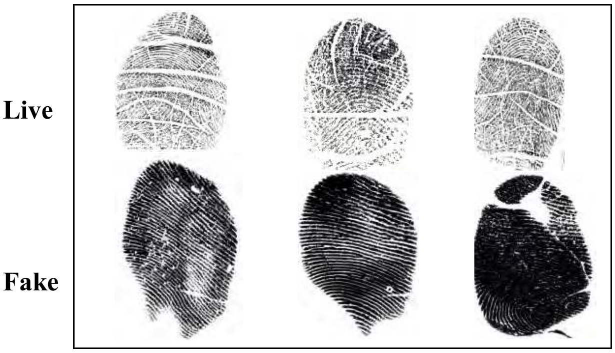

FIGURE 10. Typical examples of real and fake fingerprint images obtained from CrossMatch dataset in LivDet2015 database [16].

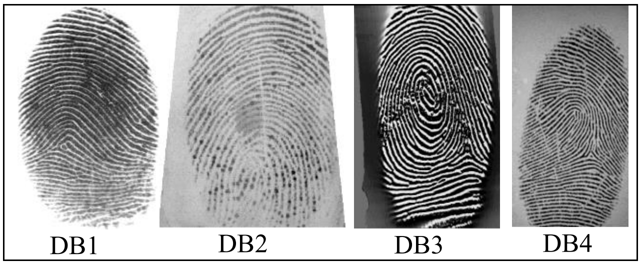

FIGURE 11. Sample image from each dataset on FVC 2004 database [17].

In the second multimodal database (MDB2), we randomly assigned one subject from the CYBHi ECG database to a subject from the FVC 2004 fingerprint database. Finally, the MDB2 is collected from 63 subjects; each has two ECG and fingerprint samples.

B. EXPERIMENTAL SETUP

To analyze the authentication performance of the proposed two multimodal systems, we used CNN to extract the features from each biometric, which can provide many informative features. And then we selected two layers as two different feature descriptors. After that, we used two methods of internal fusion: 1) addition fusion and 2) concatenation fusion. Then, we utilized the improved Bio-Hashing method to protect these features template. In the classification task, we used QG-MSVM [13]. In addition, a ten-fold cross-validation approach [31] was employed. In the first system, decision level fusion of ECG and fingerprint was used. In the second system, we used feature level fusion of ECG and fingerprint.

C. PERFORMANCE METRICS

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

- **False Acceptance Rate (FAR)**: It is defined as the ratio of the number of false acceptances to the number of authentications attempts in formula (5):

$$FAR = \frac{FP}{TN + FP} \tag{5}$$

- **False Rejection Rate (FRR)**: It is defined as the ratio of the number of false rejections to the number of authentications attempts in formula (6):

$$FRR = \frac{FN}{TP + FN} \tag{6}$$

- **Accuracy** (**Acc**): It is the measure of overall system performance over all the available classes and is defined as formula (7):

$$Acc = \frac{TP + FP}{TP + FP + TN + FN} \tag{7}$$

- **Equal Error Rate (EER)**: This error rate equates to the point at which the FAR and FRR cross (the compromise between FAR and FRR).

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 acceptances.

D. ECG AUTHENTICATION

In this study, we suppose that the ECG authentication system has low false reject rates and reaches FRR of zero. Thus, we are sure that no genuine subject will be rejected as an impostor. In this stage, we are implicitly utilizing the liveness property of ECG to guarantee that the accepted subjects are alive.

In previous work [5], Komeili *et al.* reported that the accuracy of ECG was low when using it for authentication. In this study, we showed that the proposed ECG authentication system based on CNN achieved high accuracy compared with other previous authentication systems. To evaluate the performance of the proposed ECG system on the two databases, ten-fold cross-validation approach was used, which divided the total ECG images into ten equal parts, nine out of ten parts were used for training and the remaining were used for testing. In terms of authentication accuracies, we used internal fusions by addition and by concatenation respectively, and then compared our algorithm with previous authentication algorithms [36]–[39]. To the best of our knowledge, there are only two recent works on ECG authentication based on deep learning [40], [41], thus our study should be considered one of the first studies to build an ECG authentication system based on deep learning. The confusion matrix of the results for ECG authentication system using PTB and CYBHi databases is presented in Tables 1 and 2, respectively. It can be noted from the Table 1 that, Acc of 96.83% and FAR of 3.1% without using internal fusion, Acc of 97.50% and FAR of 2.5% using internal fusion by concatenation and Acc of 98.66% and FAR of 1.3% using internal fusion by addition. In this work, 3.1% of the impostors are wrongly identified as genuine when using the system without internal fusion, 2.5% of the impostors are wrongly identified as genuine when using the system with internal fusion by concatenation and 1.3% of the impostors are wrongly identified as genuine when using the system with internal fusion by addition. As well, from Table 2, it can be noted that Acc of 97.15%, 98.44% and 98.97% without using internal fusion, using concatenation internal fusion and using addition internal fusion, respectively.

TABLE 1. Confusion matrix obtained using ten-fold cross validation for ECG authentication system on PTB database.

ECG System	True/ Predicted	G	I	Acc (%)	FAR (%) (FRR=0)
Without Fusion	G	1600	0	96.83	3.1
	I	19	581		
With Concat Fusion	G	1600	0	97.50	2.5
	I	15	585		
With Addition Fusion	G	1600	0	98.66	1.3
	I	8	592		

G: Genuine, I: Impostor, Acc: Accuracy, FAR: False Acceptance Rate, FRR: False Rejection Rate.

TABLE 2. Confusion matrix obtained using ten-fold cross validation for ECG authentication system on CYBHi database.

ECG System	True/ Predicted	G	I	Acc (%)	FAR (%) (FRR=0)
Without Fusion	G	1000	0	97.15	2.8
	I	11	375		
With Concat Fusion	G	1000	0	98.44	1.5
	I	6	380		
With Addition Fusion	G	1000	0	98.97	1
	I	4	382		

We compared the authentication performance of the proposed ECG system with 1) different approaches based on handcrafted features including short-time Fourier transform (STFT) [36], DWT [37] and others [38], [39] and 2) with the only two recent works based on deep learning for ECG authentication [40], [41]. Table 3 shows the comparison between the proposed algorithm and other previous algorithms for ECG authentication.

From the Table 3, we can prove that the proposed ECG unimodal system can be used for authentication with acceptable authentication results. We compared the proposed method with works in [40] and [41], where these are the only two studies on ECG authentication based on deep learning as shown in Table 4.

From Table 4, the proposed algorithm with addition fusion achieved acceptable accuracy compared with the methods in [40] and [41]. Also, our algorithm is more robust than the algorithm in [40] and [41]. Unlike these algorithms [40], [41], no segmentation or QRS detection needed in our algorithm.

TABLE 3. Authentication accuracy of different ECG methods.

Approach	Database	Subjects	Performance (%)
STFT [36]	PTB	269	EER = 5.58%
DCT [37]	PTB	90	Acc = 97.7%
PAR [38]	PTB	112	EER Healthy = 9.89% EER Arrhythmia = 19.15%
AC/DCT [39]	PTB	30	Se: 97.25% Spe: 99.91% Avg. Recognition Rate: 97.31%
Proposed with Add fusion	**PTB** **CYBHi**	**100** **63**	**Acc = 98.66%** **Acc = 98.97%**

STFT: Short Time Fourier Transform, DCT: Discrete Cosine Transform, PAR: PAR = Pulse Active Ratio.

TABLE 4. Comparison between the proposed ECG system on PTB database and previous ECG authentication system based on deep learning.

Method	Feature size	No. of Layers	Performance (%)
Deep-ECG [40]	500	8	EER = 1.36%
CN-ECG [41]	100	10	EER = 1.33%
Proposed without fusion	4096	12	EER = 3.2%
Proposed with Concat fusion	8192	12	EER = 2.7%
Proposed with Add fusion	**4096**	**12**	**EER = 1.4%**

In addition, the proposed algorithm is insensitive to the quality of ECG images.

E. FINGERPRINT AUTHENTICATION

In our system, we suppose that the fingerprint authentication system has low false acceptance rates and reaches FAR of zero. Thus, we are sure that no impostor subject will be accepted as a genuine. To evaluate the performance of the fingerprint system on the two databases, the ten-fold cross-validation approach was used. In terms of authentication accuracies, we used internal fusion as in ECG system, then compared the algorithm with previous authentication algorithms [35], [42]–[44]. Tables 5 and 6 show the results for fingerprint authentication system using LivDet2015 and FVC 2004 databases, respectively. It can be noted from the Table 5 that, Acc of 97.12% and FRR of 2.8% without using internal fusion, Acc of 98.25% and FRR of 1.7% using internal fusion by concatenation and Acc of 98.81% and FRR of 1.1% using internal fusion by addition. Out of all fingerprint images, 2.8% are incorrectly identified as impostors without using internal fusion, 1.7% using internal fusion by concatenation and 1.1% using internal fusion by addition. Also, from Table 6 it can be noted that Acc of 96.70%, 97.40% and 98.20% without using internal fusion, using concatenation internal fusion and using addition internal fusion, respectively.

TABLE 5. Confusion matrix obtained using ten-fold cross validation for fingerprint authentication system on LivDet2015 database.

Fingerprint System	True/Predicted	G	I	Acc (%)	FRR (%) (FAR=0)
Without Fusion	**G**	1554	46	97.12	2.8
	I	0	600		
With Concat Fusion	**G**	1572	28	98.25	1.7
	I	0	600		
With Addition Fusion	**G**	1581	19	98.81	1.1
	I	0	600		

TABLE 6. Confusion matrix obtained using ten-fold cross validation for fingerprint authentication system on FVC 2004 database.

Fingerprint System	True/Predicted	G	I	Acc (%)	FRR (%) (FAR=0)
Without Fusion	**G**	967	33	96.70	3.3
	I	0	386		
With Concat Fusion	**G**	972	26	97.40	2.6
	I	0	386		
With Addition Fusion	**G**	982	18	98.20	1.8
	I	0	386		

We then compared the authentication performance of the system with previous fingerprint authentication systems as shown in Table 7.

TABLE 7. Authentication accuracy of different fingerprint systems.

Approach	Database	Performance (%)
Geometric Features [42]	neurotechnology database [45]	EER = 0.8%
Phase-Only Correlation [43]	FVC2000 DB2 [46]	EER = 1.70%
Contrast enhancement and CNN [44]	ATVS database [47]	Avg Acc = 99.8%
CNN [35]	LivDet 2009, 2011, and 2013 [48,49,50]	Acc = 97.1%
Proposed with Add fusion	**LivDet2015** **FVC 2004**	**Acc = 98.81%** **Acc = 98.20%**

From the previous Tables, it can be argued that the authentication result of the proposed fingerprint system with the internal fusion by addition is more robust and better than other previous algorithms that used CNN for fingerprint authentication. Also, we can prove that the proposed fingerprint system can be used for authentication with acceptable authentication results.

F. FUSION OF ECG AND FINGERPRINT (THE FIRST SYSTEM)

In this section, we present the results of the decision fusion of ECG and fingerprint for human authentication purpose. We worked on the two multimodal databases (MDB1 and MDB2) in all the experiments in this section.

TABLE 8. The overall authentication performance for the first multimodal system on MDB1.

Multimodal System 1	Acc (%)	FAR (%)	FRR
Without Fusion	99.12	1.2	0
With Concat Fusion	99.55	0.4	0
With Addition Fusion	99.83	0.2	0

Acc: Accuracy, FAR: False Acceptance Rate, FRR: False Rejection Rate.

1) MDB1

Table 8 shows the overall authentication performance for the proposed sequential multimodal authentication system on MDB1. It can be noted from the Table 8 that, Acc of 99.12%, FRR of 0 and FAR of 1.2% without using internal fusion, Acc of 99.55%, FRR of 0 and FAR of 0.4% using internal fusion by concatenation and Acc of 99.83%, FRR of 0 and FAR of 0.2% using internal fusion by addition.

A comparison is done between the proposed multimodal with the two internal fusion methods and each unimodal using internal fusion with addition as shown in the ROC curves in Figure.12. The ROC curve plot is a function of the decision threshold, which plots the rate of False Positive Rate on the x-axis, against the True Positive Rate on the y-axis.

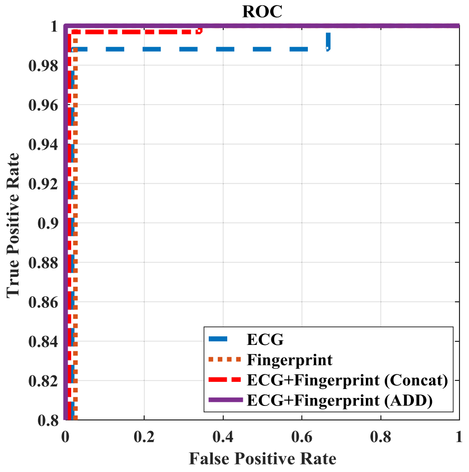

FIGURE 12. Comparison of ROC curves among the proposed sequential multimodal using MDB1 and other unimodal systems.

Figure.13 shows the variation of the EER of the proposed multimodal during different folds (ten-fold) on the two internal fusion methods.

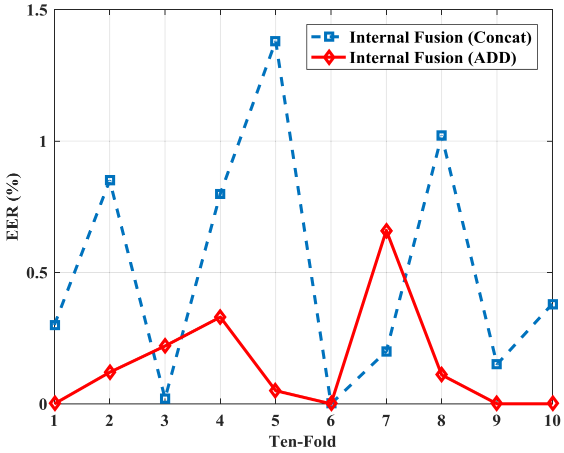

FIGURE 13. The variation of the EER during different folds (ten-fold) on the two-feature fusion method for the proposed sequential multimodal using MDB1.

2) MDB2

Table 9 shows the overall authentication performance for the proposed sequential multimodal authentication system on MDB2. It can be noted from the Table 9 that, Acc of 99.42%, FRR of 0 and FAR of 0.6% without using internal fusion, Acc of 99.82%, FRR of 0 and FAR of 0.2% using internal fusion by concatenation and Acc of 99.92%, FRR of 0 and FAR of 0.1% using internal fusion by addition.

TABLE 9. The overall authentication performance for the first multimodal system on MDB2.

Multimodal System 1	Acc (%)	FAR (%)	FRR
Without Fusion	99.42	0.6	0
With Concat Fusion	99.82	0.2	0
With Addition Fusion	99.92	0.1	0

Acc: Accuracy, FAR: False Acceptance Rate, FRR: False Rejection Rate.

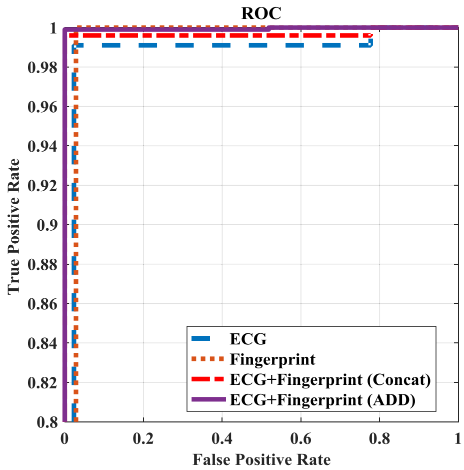

FIGURE 14. Comparison of ROC curves among the proposed sequential multimodal using MDB2 and other unimodal systems.

A comparison is done between the proposed multimodal with the two internal fusion methods and each unimodal using internal fusion with addition as shown in the ROC curves in Figure.14. Figure.15 shows the variation of the EER of the proposed multimodal during different folds (ten-fold) on the two internal fusion methods.

G. FUSION OF ECG AND FINGERPRINT (THE SECOND SYSTEM)

This section presents the results of the feature fusion of ECG and fingerprint for human authentication purpose. The feature vectors of ECG and fingerprint are extracted using the proposed CNN, and then the new transformation of those

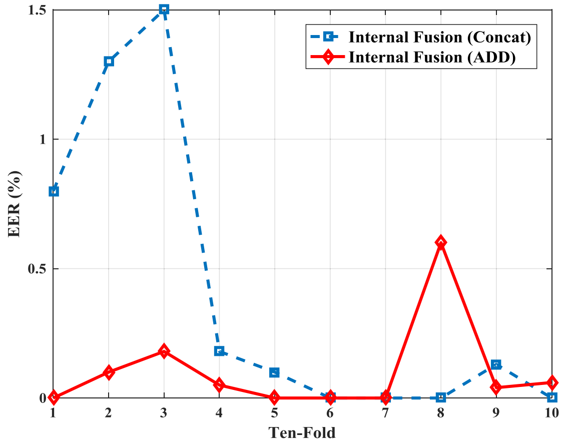

FIGURE 15. The variation of the EER during different folds (ten-fold) on the two-feature fusion method for the proposed sequential multimodal using MDB2.

features is calculated based on the concatenation and the addition method. Finally, the classification is done using QG-MSVM. We worked on the two multimodal databases (MDB1 and MDB2) in all the experiments in this section.

1) MDB1

Table 10 shows the overall authentication performance for the proposed parallel multimodal authentication system with feature fusion by addition and with feature fusion by concatenation. It can be noted from the Table 10 that, Acc of 99.37%, FRR of 0.6% and FAR of 0.8% for feature fusion by concatenation, and Acc of 99.68%, FRR of 0.3% and FAR of 0.4% for feature fusion by addition.

TABLE 10. The overall authentication performance for the second multimodal system on MDB1.

Multimodal System 1	Acc (%)	FAR (%)	FRR (%)
Without Fusion	98.94	1.7	1.1
With Concat Fusion	99.37	0.8	0.6
With Addition Fusion	99.68	0.3	0.4

Acc: Accuracy, FAR: False Acceptance Rate, FRR: False Rejection Rate.

A comparison is done between the proposed multimodal with the two feature fusion methods and each unimodal using internal fusion with addition as shown in the ROC curves in Figure.16.

Figure.17 shows the variation of the EER of the proposed multimodal during different folds (ten-fold) on the two-feature fusion method.

2) MDB2

Table 11 shows the overall authentication performance for the proposed parallel multimodal authentication system with feature fusion by addition and with feature fusion by concatenation. It can be noted from the Table 11 that, Acc of 99.57%, FRR of 0.5% and FAR of 0.4% for feature fusion by concatenation, and Acc of 99.74%, FRR of 0.2% and FAR of 0.3% for feature fusion by addition.

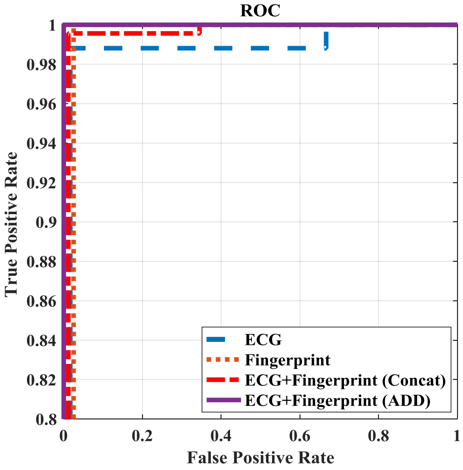

FIGURE 16. Comparison of ROC curves among the proposed parallel multimodal using MDB1 and other unimodal systems.

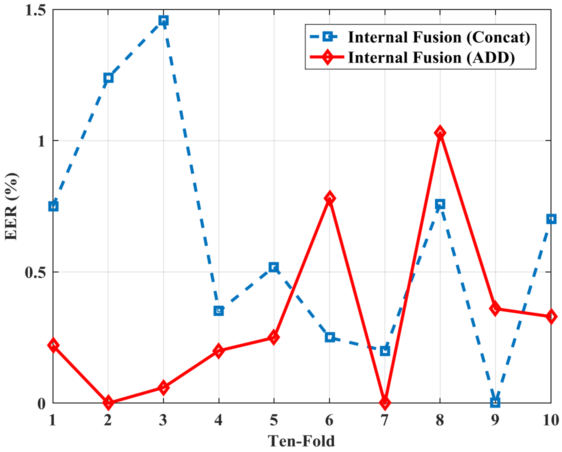

FIGURE 17. The variation of the EER during different folds (ten-fold) on the two-feature fusion method for the proposed parallel multimodal using MDB1.

TABLE 11. The overall authentication performance for the second multimodal system on MDB2.

Multimodal System 1	Acc (%)	FAR (%)	FRR (%)
Without Fusion	99.23	0.7	1
With Concat Fusion	99.57	0.4	0.5
With Addition Fusion	99.74	0.3	0.2

A comparison is done between the proposed multimodal with the two feature fusion methods and each unimodal using internal fusion with addition as shown in the ROC curves in Figure.18.

Figure.19 shows the variation of the EER of the proposed multimodal during different folds (ten-fold) on the two-feature fusion method.

Finally, to analyze the proposed two systems, a comparison is done between the proposed two multimodal systems using

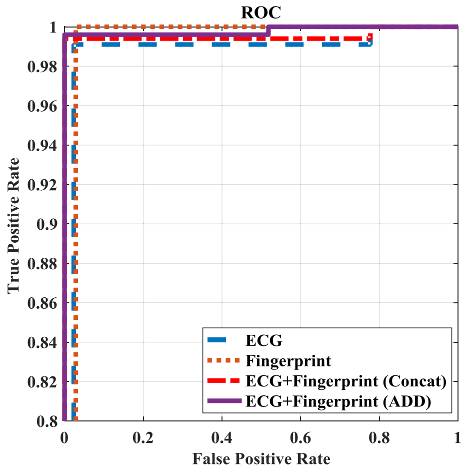

FIGURE 18. Comparison of ROC curves among the proposed parallel multimodal using MDB2 and other unimodal systems.

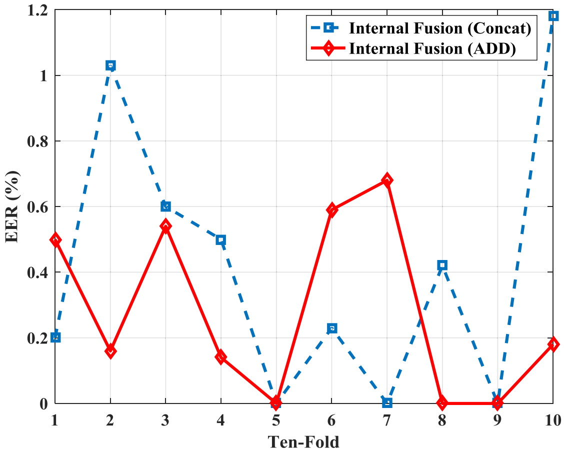

FIGURE 19. The variation of the EER during different folds (ten-fold) on the two-feature fusion method for the proposed parallel multimodal using MDB2.

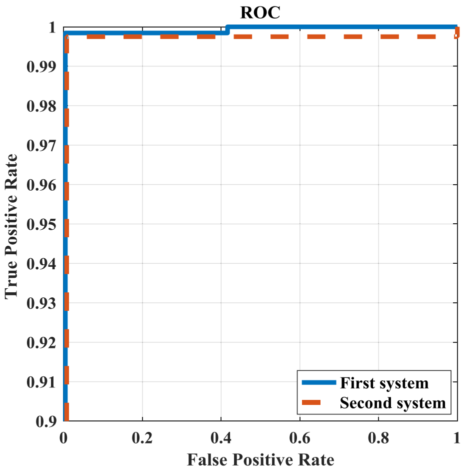

FIGURE 20. Comparison of ROC curves among the proposed two systems using internal fusion with addition on MDB1.

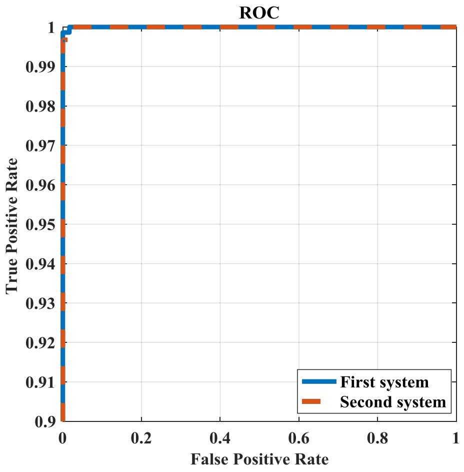

FIGURE 21. Comparison of ROC curves among the proposed two systems using internal fusion with addition on MDB2.

internal fusion with addition on the two multimodal databases and shown in Figures.20 and 21.

V. DISCUSSION

Based on the results yielded in Tables 1, 2, 5 and 6 it can be argued that the authentication results of ECG or fingerprint based on CNN is better than most previous hand-designed works. Also, Tables 1 and 2 show that the ECG as unimodal in addition using it for liveness detection it can be used for authentication with acceptable authentication accuracy. Figures 12,14,16 and 18 show that the proposed two multimodal systems are significantly efficient, robust and reliable than using unimodal based on CNN. Also, these Figures show that the proposed two multimodal systems are not restricted to a single database and give a high accuracy on different databases. As well, Figures 20 and 21 show that the performance of the proposed sequential system is better than the proposed parallel system. However, the computation time of the proposed parallel system is less than the proposed sequential system.

We compared the authentication performance of the proposed two multimodal systems with previous state-of-the-art multimodal authentication algorithms based on ECG and fingerprint. The comparison of previous state-of-the-art algorithms with the proposed two systems is shown in Table 12.

It is evident that our proposed systems are more efficient and robust as compared to the rest of the works mentioned in Table 12.

Table 13 shows the comparison between the proposed systems and other systems that used CNN on different biometrics.

From Table 13, we can show that the results of the proposed system are acceptable compared with other systems that using CNN on different biometrics.

The main highlights of our proposed systems are summarized below:

TABLE 12. Summary of previous state-of-the-art multibiometric authentication system based on ECG and fingerprint.

Reference (Year)	Methodology	Performance (%)
Komeili et al [5] 2018	Score based fusion Automatic template updating algorithm Linear SVM	Average EER = 2.9 %

Manjunathswamy et al [7]
2014
	Score based fusion	FRR = 0 %
		FAR = 2.5 %

Zhao et al [6] 2012	AC/LDA method	N/R
Singh et al [8] 2012	Transformation based score fusion Euclidean distance	EER = 1.52 %
The proposed sequential system	**Classifier-based decision fusion CNN Improved Bio-Hash method QG-MSVM**	**MDB1 EER = 0.14% MDB2 EER = 0.10%**
The proposed parallel system	**Feature fusion with addition CNN Improved Bio-Hash method QG-MSVM**	**MDB1 EER = 0.40% MDB2 EER = 0.32%**

- **SVM: Support Vector Machine, AC/LDA: Autocorrelation/ Linear Discriminant Analysis, QG-MSVM: Q-Gaussian multi-class support vector machine.**
- **EER: Equal Error Rate, FAR = False Acceptance Rate, FRR: False Rejection Rate, N/R: Not Reported.**

TABLE 13. Comparison between the proposed algorithm and previous state-of-the-art authentication algorithms on different biometrics.

Author	Year	Biometric	Approach	Performance (%)
Kurban et al. [9]	2017	Face + Gesture Energy	- Score fusion - CNN	EER = 1.4%
Al-Waisy et al. [10]	2017	irises	- Ranking fusion - CNN	EER = 0.13%
Talreja et al. [11]	2017	Face + irises	- Feature fusion - DNN	EER = 0.3%
This work	**2018**	**ECG + Fingerprint**	**Classifier-based decision fusion CNN Improved Bio-Hash method QG-MSVM**	**MDB1 EER = 0.14% MDB2 EER = 0.10%**

1. The proposed systems are invariant to translation for ECG images; therefore, no noise filtering or segmentation techniques are needed in this work.
2. Ten-fold cross-validation strategy is used in this work. Hence, the reported performance is robust.
3. The proposed multimodal authentication systems achieve superior results compared with the previous multimodal systems based on ECG and fingerprint.

According to the advantages of the proposed system, it can be deployed in real applications.

The main disadvantages of the proposed systems are:

- In the first system, the wait time for a user to be authenticated at least be the authentication time of the ECG authentication.
- In the second system, there is no guarantee that there is liveness detection which is a major flaw in this system.

A. EFFECT OF DATASET AUGMENTATION

Table 14 compares the effect of dataset augmentation on the two proposed multimodal systems. As shown in the Table, this technique helps to improve the accuracy of the proposed systems: the error was reduced by a factor of 4 in some cases.

TABLE 14. Average Error on the proposed two systems with and without augmentation technique.

System	Without Augmentation	With Augmentation
Sequential system	0.59%	0.14%
Parallel system	1.20%	0.40%

B. EFFECT OF TEMPLATE PROTECTION METHOD

Table 15 compares the effect of using the cancelable method on the two proposed multimodal system using MDB1. As shown in the Table, this method plays an important rule to increase the accuracy of the proposed system.

TABLE 15. Average Accuracy on the proposed two systems with and without cancelable method.

System	Without cancelable	With cancelable
Sequential system	98.42%	99.12%
Parallel system	98.11%	98.94%

C. COMPUTATIONAL COSTS

The computational cost of the proposed systems is relatively low. The algorithm is tested/trained in a computer with specifications of a 2.7-GHz CPU and 32 GB RAM. Moreover, the proposed systems only need pre-trained convolutions; hence implementation is economical and requires simple hardware. To extract the deep features, we used the GPU instances that allowed us to extract the features from the whole database in a few seconds (it takes around 30-50 seconds for each system). Training ECG data for authentication takes about 2.5747 seconds and training fingerprint data for authentication takes about 3.2668 seconds. The time for testing is very small and takes about 0.1263 seconds, so it can be neglected. Furthermore, the proposed systems can be deployed in real applications.

VI. CONCLUSIONS

This paper presented two multimodal authentication systems (sequential and parallel system) using CNN to fuse the ECG and the fingerprint based on a different level of fusion. These multimodal systems overcome most of the previous unimodal problems such as authentication accuracy loss and spoof attacks. CNN is used for extracting the features from the two biometrics. The improved Bio-Hashing technique is applied to protect the extracted features and to enhance the accuracy of authentication. Finally, QG-MSVM is proposed as a classifier for authentication to improve the performance. We proposed the internal fusion, which is fused the important features of each biometric to improve the authentication accuracy. The experimental results show that the proposed ECG and fingerprint unimodal system can be used for authentication with acceptable authentication results comparing with other methods. We also showed that the overall performance of the proposed multimodal systems is better than unimodal systems based on CNN and the previous multimodal regarding authentication. Data augmentation plays an important role in increasing the authentication accuracy, which reduced the error of the system by a factor of 4 in some cases. In the future, we suggest reducing the feature size of each biometric to speed up the authentication task, also we suggest testing the proposed systems on a real database.

REFERENCES

[1] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. New York, NY, USA: Springer-Verlag, 2004.

[2] Z. Wang, E. Wang, S. Wang, and Q. Ding, "Multimodal biometric system using face-iris fusion feature," *J. Comput.*, vol. 6, no. 5, pp. 931–938, 2011.

[3] D. Miao, M. Zhang, Z. Sun, T. Tan, and Z. He, "Bin-based classifier fusion of iris and face biometrics," *Neurocomputing*, vol. 224, pp. 105–118, Feb. 2017.

[4] H. Mehrotra, R. Singh, M. Vatsa, and B. Majhi, "Incremental granular relevance vector machine: A case study in multimodal biometrics," *Pattern Recognit.*, vol. 56, pp. 63–76, Aug. 2016.

[5] M. Komeili, N. Armanfard, and D. Hatzinakos, "Liveness detection and automatic template updating using fusion of ECG and fingerprint," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1810–1822, Jul. 2018.

[6] C. X. Zhao, T. Wysocki, F. Agrafioti, and D. Hatzinakos, "Securing handheld devices and fingerprint readers with ECG biometrics," in *Proc. IEEE 5th Int. Conf. IEEE Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2012, pp. 150–155.

[7] B. E. Manjunathswamy, A. M. Abhishek, J. Thriveni, K. R. Venugopal, and L. M. Patnaik, "Multimodel biometrics using ECG and fingerprint," in *Proc. Int. Conf. Adv. Commun. Netw. Comput.*, 2014.

[8] Y. N. Singh, S. K. Singh, and P. Gupta, "Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system," *Pattern Recognit. Lett.*, vol. 33, no. 14, pp. 1932–1941, 2012.

[9] O. C. Kurban, T. Yildirim, and A. Bilgiç, "A multi-biometric recognition system based on deep features of face and gesture energy image," in *Proc. IEEE Int. Conf. Innov. Intell. Syst. Appl.*, Jul. 2017, pp. 361–364.

[10] A. S. Al-Waisy, R. Qahwaji, S. Ipson, S. Al-Fahdawi, and T. A. M. Nagem, "A multi-biometric iris recognition system based on a deep learning approach," *Pattern Anal. Appl.*, vol. 21, no. 3, pp. 783–802, Aug. 2018.

[11] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Multibiometric secure system based on deep learning," in *Proc. GloablSIP*, Nov. 2017, pp. 298–302.

[12] R. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.

[13] H. Mohamed and K. Wang, "Fingerprint classification based on a Q-Gaussian multiclass support vector machine," in *Proc. Int. Conf. Biometrics Eng. Appl.*, 2017, pp. 39–44.

[14] A. L. Goldberger *et al.*, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, p. E215, 2000.

[15] H. P. Da Silva, A. Lourenço, A. Fred, N. Raposo, and M. Aires-de-Sousa, "Check your biosignals here: A new dataset for off-the-person ECG biometrics," *Comput. Methods Programs Biomed.*, vol. 113, no. 2, pp. 503–514, 2014.

[16] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," in *Proc. IEEE 7th Int. Conf. IEEE Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–6.

[17] *FVC2004—Third International Fingerprint Verification Competition*. [Online]. Available: http://bias.csr.unibo.it/fvc2004/download.asp

[18] T. J. Jun, H. M. Nguyen, D. Kang, D. Kim, D. Kim, and Y.-H. Kim. (Apr. 18, 2018). "ECG arrhythmia classification using a 2-D convolutional neural network." [Online]. Available: https://arxiv.org/abs/1804.06812

[19] A. Ali, R. Khan, I. Ullah, A. D. Khan, and A. Munir, "Minutiae based automatic fingerprint recognition: Machine learning approaches," in *Proc. IEEE Int. Conf. Comput. Inf. Technol., Ubiquitous Comput. Commun., Dependable, Autonomic Secure Comput., Pervasive Intell. Comput.*, Oct. 2015, pp. 1148–1153.

[20] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Netw.*, vol. 61, pp. 85–117, Jan. 2015.

[21] H. Li, Y. Huang, and Z. Zhang, "An improved faster R-CNN for same object retrieval," *IEEE Access*, vol. 5, pp. 13665–13676, 2017.

[22] X. Ren, Y. Zhou, Z. Huang, J. Sun, X. Yang, and K. Chen, "A novel text structure feature extractor for Chinese scene text detection and recognition," *IEEE Access*, vol. 5, pp. 3193–3204, 2017.

[23] M. Z. Uddin, W. Khaksar, and J. Torresen, "Facial expression recognition using salient features and convolutional neural network," *IEEE Access*, vol. 5, pp. 26146–26161, 2017.

[24] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Network traffic classifier with convolutional and recurrent neural networks for Internet of Things," *IEEE Access*, vol. 5, pp. 18042–18050, 2017.

[25] Y. Jia *et al.*, "Caffe: Convolutional architecture for fast feature embedding," in *Proc. MM*, 2014, pp. 675–678.

[26] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems*, vol. 25, F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, Eds. Red Hook, NY, USA: Curran & Assoc. Inc, 2012, pp. 1097–1105.

[27] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2014, pp. 580–587.

[28] O. Russakovsky *et al.*, "ImageNet large scale visual recognition challenge," *Int. J. Comput. Vis.*, vol. 115, no. 3, pp. 211–252, Dec. 2015.

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

[30] M. Hammad, G. Luo, and K. Wang, "Cancelable biometric authentication system based on ECG," *Multimedia Tools Appl.*, vol. 12, pp. 1–31, Jul. 2018.

[31] C. Tsallis, *What Are the Numbers that Experiments Provide?*. Rio de Janeiro, Brazil: Centro Brasileiro de Pesquisas Físicas, 1994.

[32] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. Hoboken, NJ, USA: Wiley, 2001, pp. 55–88.

[33] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 1097–1105.

[34] D. Ciresan, U. Meier, and J. Schmidhuber, "Multi-column deep neural networks for image classification," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2012, pp. 3642–3649.

[35] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.

[36] I. Odinaka *et al.*, "ECG biometrics: A robust short-time frequency analysis," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2010, pp. 1–6.

[37] M. M. Tantawi, K. Revett, A.-B. Salem, and M. F. Tolba, "A wavelet feature extraction method for electrocardiogram (ECG)-based biometric recognition," *Signal Image Video Process.*, vol. 9, no. 6, pp. 1271–1280, 2015.

[38] S. I. Safie, J. J. Soraghan, and L. Petropoulakis, "Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR)," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1315–1322, Dec. 2011.

[39] H. Gürkan, U. Guz, and B. S. Yarman, "A novel biometric authentication approach using electrocardiogram signals," in *Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2013, pp. 4259–4262.

[40] R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, "Deep-ECG: Convolutional neural networks for ECG biometric recognition," *Pattern Recognit. Lett.*, to be published.

[41] E. J. da Silva Luz, G. J. P. Moreira, L. S. Oliveira, W. R. Schwartz, and D. Menotti, "Learning deep off-the-person heart biometrics representations," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1258–1270, May 2018.

[42] K. K. M. Shreyas, S. Rajeev, K. Panetta, and S. S. Agaian, "Fingerprint authentication using geometric features," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2017, pp. 1–7.

[43] N. Shabrina, T. Isshiki, and H. Kunieda, "Fingerprint authentication on touch sensor using phase-only correlation method," in *Proc. 7th Int. Conf. Inf. Commun. Technol. Embedded Syst. (IC-ICTES)*, Mar. 2016, pp. 85–89.

[44] H.-U. Jang, H.-Y. Choi, D. Kim, J. Son, and H.-K. Lee, "Fingerprint spoof detection using contrast enhancement and convolutional neural networks," in *Proc. Int. Conf. Inf. Sci. Appl.* Singapore: Springer, 2017, pp. 331–338.

[45] Neurotechnology. (2016). *Download Biometric Algorithm Demo Software, SDK Trials, Product Brochures*. [Online]. Available: http://www.neurotechnology.com/download.html

[46] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 3, pp. 402–412, Mar. 2002.

[47] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.

[48] G. L. Marcialis *et al.*, "First international fingerprint liveness detection competition—LivDet 2009," in *Image Analysis and Processing*. Berlin, Germany: Springer, 2009, pp. 12–23.

[49] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011—Fingerprint liveness detection competition 2011," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar./Apr. 2012, pp. 208–215.

[50] L. Ghiani *et al.*, "LivDet 2013 fingerprint liveness detection competition 2013," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.

MOHAMED HAMMAD received the M.Sc. degree from the Information Technology Department, Faculty of Computers and Information, Menoufia University, Egypt, in 2015. He is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. He has been a Demonstrator and an Assistant Lecturer with the Faculty of Computers and Information, Menoufia University, Egypt, since 2012. His research interests include computer vision, machine learning, pattern recognition, and biometrics.

YASHU LIU is currently pursuing the Ph.D. degree with the Perception Computing Center, School of Computer Science and Technology, Harbin Institute of Technology. Her research interest is medical image processing, pattern recognition, and deep learning.

KUANQUAN WANG (M'01–SM'07) was an Associate Dean of the School of Computer Science and Technology, Harbin Institute of Technology (HIT), Harbin, and the Dean of the School of Computer Science and Technology, HIT, Weihai, from 2011 to 2014. He is currently a Full Professor and a Ph.D. Supervisor with the School of Computer Science and Technology, and the Deputy Director of the Research Center of Perception and Computing, HIT. He has published over 300 papers and six books, and has more than 10 patents. His research interests include image processing and pattern recognition, biometrics, biocomputing, modeling and simulation, virtual reality, and visualization. He is a Senior Member of the China Computer Federation, ACM, and the Chinese Society of Biomedical Engineering. He received the second prize of National Teaching Achievement.