Complex & Intelligent Systems (2024) 10:435–454
https://doi.org/10.1007/s40747-023-01149-6

ORIGINAL ARTICLE

Security enhancement of the access control scheme in IoMT applications based on fuzzy logic processing and lightweight encryption

Ghada M. El-Banby[1] · Lamiaa A. Abou Elazm[2] · Walid El-Shafai[3] · Nirmeen A. El-Bahnasawy[4] · Fathi E. Abd El-Samie[3] · Atef Abou Elazm[3] · Ali I. Siam[5]

Received: 13 February 2023 / Accepted: 11 June 2023 / Published online: 25 July 2023

Abstract

Security of Internet-of-Medical-Things (IoMT) networks has evolved as a vital issue in recent years. The IoMT networks are designed to link patients with caregivers. All reports, data, and medical signals are transferred over these networks. Hence, these networks require robust and secure access strategies for patients to send their vital data or reports. Hence, hacking of these networks may lead to harmful effects on patients. One of the vulnerable points to hacking in these networks is the access point. Access to these networks could be performed with biometrics. The popular biometric traits for this purpose are biomedical signals such as Electrocardiogram (ECG) signals, as they are continuously monitored and measured for patients. A common thread between all biometric authentication systems is the possibility of losing the biometric traits forever if hacking attempts manage to concur the biometric template storage. A new trend in the field of biometric authentication is to avoid the utilization of original biometrics in access control processes. A possible alternative is to use cancelable biometrics instead. Cancelable biometrics can be generated through encryption schemes or non-invertible transforms. This paper adopts both strategies in a unified framework for cancelable ECG signal recognition that can be used in the access step of IoMT networks. The proposed framework begins with applying a non-invertible transformation on the ECG signals through fuzzy logic to change the dynamic range of the signals. As this process is non-invertible in nature, it prevents the recovery of the original ECG signals from the processed versions, which is the main target of cancelable biometric systems. After that, lightweight encryption through XOR operation with user-specific patterns is implemented. Here, the high complexity of full encryption schemes that need a large processing burden is eliminated. The addition of the encryption stage enhances the security of cancelable biometric traits, allowing a hybrid nature of the proposed cancelable biometric framework through the merging of non-invertible transforms and encryption algorithms. Moreover, an FPGA hardware implementation is introduced for real implementation of the proposed ECG-based cancelable biometric recognition framework. This hardware can accompany the user to allow access of the IoMT network when requested. Experimental results show a promising performance of the proposed framework with a large Area under the Receiver Operating Characteristic curve (AROC) of 99.5% and an Equal Error Rate (EER) of 0.058%.

Keywords IoMT · Access control · ECG signals · Cancelable biometrics · Fuzzy logic · FPGA

Introduction

The last decade has witnessed a revolution in the Internet-of-Things (IoT) field due to the advances in networking technologies and protocols. IoT applications are popular in the community, allowing users to control all their assets and peripherals. With this development, the idea of IoT has been extended to the field of healthcare. New networks, called the Internet-of-Medical-Things (IoMT), have been initiated to monitor the status of patients with chronic diseases [1, 2]. Both patients and caregivers should be connected to these IoMT networks for the exchange of biomedical measurements regularly and remote access to diagnosis and treatment if needed.

Security of IoMT networks is a large-scope research area as numerous attacks may be performed on these networks.

✉ Ali I. Siam
ali.siam@ai.kfs.edu.eg

Extended author information available on the last page of the article

These attacks range from fake users to fake nodes during the data transmission over IoMT networks [3, 4]. Moreover, attackers may intrude into IoMT networks to manage patient information in operations similar to SQL injection [1, 5]. It is clear that actions of this type threaten the patients' lives as they will be subject to incorrect diagnosis and treatment. The security of the IoMT networks begins by providing an answer to the question of "How can the patient access the network?". Xin et al. suggested biometric-based authentication as a basis for IoMT network access by patients [6]. They introduced a framework based on the fusion of features extracted from the face, fingerprint, and finger vein for the patients to access the IoMT networks.

In fact, IoMT networks are mainly designed to monitor the cases of patients with chronic diseases. Therefore, one of the biometrics related to the continuous measurements taken for the patients would be recommended. The ECG is a good candidate for this task. The ECG is the measurement of the electrical activities of the heart [7–9]. The ECG signal is obtained and measured on the chest. The autonomic nervous system controls the ECG waveform by a combination of sympathetic and parasympathetic factors. Hence, every time interval is relatively different for every subject, and thus difficult to mimic or reproduce. That is why ECG signals can be used for authentication purposes [10, 11]. They are more appropriate for authentication in IoMT networks as the patients will not be obliged to give other biometrics on scanners or cameras.

Furthermore, many modern access control systems, especially in the medical field, are primarily geared towards biometric authentication rather than passwords, credit cards, and token-based verification to reduce attack impacts. The ease of implementation of biometric-based authentication is considered an advantage to be exploited in many crucial applications. Biometric traits such as voice [12], ECG, Photoplethysmography (PPG) [13], Electroencephalography (EEG), face, hand geometry [14], and ear shape are permanently accompanying the user and cannot be replaced. Hence, it is easy for the user to use them in remote access systems. For the case of patient monitoring, ECG scanning has the benefit of continuously allowing ECG signals for patients. Hence, it becomes easy for patients to depend on these signals to connect to the healthcare system without their intervention, even in cases of exhaustion and inability to provide other biometric traits. Unfortunately, one of the weak points in the biometric system is the biometric acquisition, which is vulnerable to attacks and theft attempts. The main biometrics used in the access process should be secured to prevent attackers from impersonating other users' identities.

The main requirements of human biometrics to be used in biometric authentication systems, such as universality and permanence, are achieved with ECG signals. Universality is maintained as the ECG signals can be continuously monitored for all subjects. High permanence of ECG-based authentication systems is guaranteed through the invariant nature of the signals over a large period of time. In addition, aliveness detection is continuously guaranteed as long as ECG signals are recorded and transmitted. All these characteristics allow the utilization of ECG signals for biometric authentication over IoMT networks.

Unfortunately, biometric-based authentication systems require biometric attributes or features to be stored in databases. Any biometric system is vulnerable to attacks at different points, ranging from the biometric acquisition point to the decision-making point [15]. That is why the trend of cancelable biometrics has evolved. Through cancelable biometrics, the users are allowed to use different alternatives for their original biometric templates that can be generated with non-invertible transforms or encryption schemes. The objective of the utilization of cancelable biometrics is privacy preservation [16].

Through the deep investigation of the existing cancelable biometric schemes, we notice that the schemes that depend on non-invertible transforms may be subject to record multiplicity attacks, and also those that rely on encryption may be vulnerable to brute-force attacks [3, 15]. The elimination and avoidance of brute-force attacks require strong encryption mechanisms and the use of very long keys in the employed encryption process. They may be unsuitable for biomedical applications that need high speed. Therefore, an elegant solution for this problem is introducing a hybrid framework for cancelable biometrics that comprises a non-invertible transform and a lightweight encryption scheme. By cascading these two stages, we guarantee high privacy of users, and high speed of operation, while achieving high authentication accuracy.

It is clear that IoMT applications are emerging now. They need efficient and strong access mechanisms. Access through raw biometrics is not recommended, as these biometrics become vulnerable to hacking attempts. Unfortunately, there is currently a lack of research on the development of cancelable biometric recognition systems specifically tailored for use in IoMT applications. While cancelable biometrics and encryption-based algorithms have been studied extensively in other contexts, their use in the context of IoMT has not been fully explored. The problem with the current biometric recognition systems used in IoMT applications is that they may not be secure enough to prevent unauthorized access and misuse of sensitive health data. Traditional biometric systems store biometric data in a central database, which makes them vulnerable to security breaches and privacy violations. Therefore, there is a need for a secure and privacy-preserving biometric recognition system that can protect patient information, while providing reliable authentication. The proposed cancelable biometric recognition framework based on fuzzy logic and lightweight encryption has a secure and privacy-preserving mechanism for biometric recognition in IoMT applications.

An appropriate solution that achieves both security and privacy is to use the new trend of cancelable biometrics for access control in IoMT applications. The most suitable biometric traits for patients to deal with IoMT applications are the ECG signals, which are continuously monitored for these patients. The two main trends to build cancelable biometric systems, namely non-invertible transforms and encryption of biometrics, are not appropriate alone as they are subject to certain types of attacks. A suggested solution in this paper is to combine them together to enhance the security level of cancelable templates. A major requirement that needs to be considered in the combination process is to avoid high complexity. That is why the fuzzy logic processing is implemented as a non-invertible transform and lightweight encryption is adopted for more security. Each of them is simple in implementation, but their combination enhances the level of security.

The research motivations of this work can be summarized as follows:

- Security enhancement: A motivation behind this research is to provide a more secure and privacy-preserving method for biometric recognition in IoMT applications. Traditional biometric systems are vulnerable to attacks, and a cancelable biometric system can address this problem by generating a new biometric template for each authentication request.
- Privacy preservation: Another motivation for this research is to enhance the privacy of patients by ensuring that their sensitive health data is protected. Cancelable biometric systems ensure that biometric data cannot be reverse-engineered to reveal the original biometric features, which provides an additional layer of protection for sensitive data.
- Efficiency enhancement: Cancelable biometric systems can also improve the efficiency of authentication in IoMT applications. Traditional biometric systems require a centralized database to store biometric data, which may be time-consuming and expensive to manage. A cancelable biometric system, on the other hand, generates a new template for each authentication request, eliminating the need for a centralized database.
- Innovation: This research also aims to explore the potential of combining fuzzy logic processing with lightweight encryption for cancelable biometric recognition. This approach has not been studied in the context of IoMT applications, and the proposed framework could be a more effective and efficient tool for biometric authentication.
- Real-world application: Finally, an important motivation for this research is to develop a framework that can be applied in real-world IoMT applications, such as remote health monitoring and patient identification. A cancelable biometric recognition framework based on fuzzy logic processing and lightweight encryption has the potential to improve the security, privacy, and efficiency of these applications, ultimately leading to better patient care.

In this paper, we introduce a cancelable ECG recognition framework that begins with the ECG acquisition stage. After that, the ECG signal is reformulated to a 2D format, and fuzzy logic processing is implemented to induce a non-invertible dynamic range modification. This process resembles the one adopted in image enhancement. Then, a simple XOR encryption stage is implemented with a patient-specific code. This stage enhances the privacy of users. Each user can select his code in a simple way. In addition, his original ECG biometric is kept away from utilization in the system database. In case of hacking attempts on the database, the user can easily change his selected code or make some parameter changes in the fuzzy logic processing algorithm.

This paper mainly provides a trusted solution to guarantee aliveness through ECG signals used in IoMT authentication applications. This solution is more robust against attempts of tampering or stealing of original biometric templates by generating revocable and non-invertible one-way cancelable biometric templates to be stored in databases. Generally, a cancelable biometric system relays on designing a transformed, distorted version of the biometric data in a non-invertible way. The presented transformation is one-way and does not give any information about the actual biometric signal. The authenticity of the user is allowed by performing matching between the templates stored in the database and the new user transformed and distorted template.

The main contributions of this paper are as follows:

- Proposal of a novel cancelable biometric recognition framework based on fuzzy logic processing and lightweight encryption for IoMT applications to ensure the security and privacy of biometric data.
- Presentation of novel non-invertible cancelable ECG templates for human authentication based on the fuzzy transformation method, which cannot be inverted to obtain the original templates back. The fuzzy logic processing can handle imprecise and uncertain data that is commonly encountered in biometric recognition applications.
- Development of lightweight encryption through XOR operation with user-specific patterns to increase the security and privacy levels. The lightweight encryption algorithm used in the proposed framework is designed to minimize the computational and storage requirements, making the suggested framework suitable for resource-constrained IoMT devices.
- Introduction of an FPGA hardware implementation of the proposed cancelable biometric authentication system.

- Evaluation of the proposed framework on different ECG databases. The results showed that it achieves high recognition accuracy and low computational cost, while maintaining high levels of security and privacy.

Finally, the proposed framework is compared with some previous cancelable ECG recognition systems. Results prove that the accuracy of the proposed framework is better than those of other previous systems. Another main advantage of this work is that aliveness verification is guaranteed.

The paper is organized as follows. Some recent related works are discussed in section "Related work". The proposed cancelable ECG recognition framework is explained in section "Proposed cancelable ECG recognition framework". The simulation results and discussion are provided in section "Experiments". The hardware implementation of the proposed framework is given in section "Hardware implementation". The concluding remarks are summarized in section "Conclusions and future work".

Related work

Several studies have been introduced in the literature for person identification based on ECG signals. Zhang et al. [17] proposed an approach for human authentication based on ECG signals captured from two-finger electrodes associated with a smartphone application. They adopted fiducial feature extraction and used Discrete Cosine Transform (DCT) for feature dimensionality reduction due to its energy compaction property. They tested the performance of their approach using Support Vector Machine (SVM) and Neural Network (NN) classifiers. They achieved accuracy levels up to 97.6% and 96.6%, respectively. The implementation of this approach needs 20 s to register a new user and 4 s for authentication.

Lee and Kwak introduced an algorithm for person identification from ECG signals [18]. Their main work concentrated on Eigenvalue decomposition and principal component analysis. This algorithm is well-known for its ability to tolerate noise effects. The authors managed to achieve classification accuracies up to 98.25%.

Barros et al. [19] presented a scheme for ECG-based identification that comprises pre-processing prior to the identification process. The pre-processing steps include noise removal, QRS complex segmentation, and outlier removal to concentrate on the most representative component of ECG signal to be used in the identification process. The authors worked on signal segments of 3 s. They adopted a feature extraction strategy with a bulk of features, including twenty two features. They validated their work over the PhysioNet Computing in Cardiology 2018 dataset [20] using Random Forest (RF) classifier. This work achieved a 92% precision on 1500 subjects and an 80% accuracy on 1200 subjects.

Huang et al. introduced an ECG recognition scheme based on sparse feature representations [21]. Similarity tests are performed on sparse feature patterns for users in a general optimization framework. Certain constraints and a regularization problem are adopted in the recognition task. This scheme was intended for authentication through a smartphone application. The complexity of this scheme is relatively high due to the need to perform Eigenvalue decomposition of matrices in addition to solving an optimization problem.

Zhao et al. [22] presented an ECG-based human authentication scheme based on Convolutional Neural Networks (CNNs) and the generalized S-transformation. The ECG signal is segmented blindly, and then the S-transform is applied to the segments to get the ECG signal trajectories in the form of images. These trajectories are then fed to the CNN as input images to further identify the corresponding subjects. The authors used noisy and clean ECG signals from three different databases. This work achieved accuracy levels up to 96.6%.

To follow the new trend of biometrics, namely cancelable biometrics, some authors have begun to investigate this trend in ECG signal identification. The objective in this scenario is to enhance the privacy of users. Hammad et al. [23] applied two techniques for developing a cancelable ECG recognition system. Their proposed techniques are improved Bio-Hashing and matrix manipulation. Bio-Hashing generally depends on generating irreversible binary codes from the feature vectors. On the other hand, the matrix manipulation technique has operations such as row and column permutations, mixing and matrix inversion. In [23], the authors employed the Pan-Tompkins algorithm to extract the ECG features first and an Artificial Neural Network (ANN) for authentication. The obtained EER values are 0.20 and 0.06 for the first and second techniques, respectively.

Using randomly-selected hypothesis testing, Kim et al. [24] proposed a cancelable ECG recognition system based on a Generalized Likelihood Ratio Test (GLRT). They also proposed Guided Filtering (GF) to create an irreversibly-transformed version of the ECG signal. Finally, they evaluated the system on the ECG-ID database. It achieved a performance index of 94.3%, higher than that of the conventional Euclidean detector.

Bugdol et al. [25] combined ECG and sound signals to build a behavior-based multi-modal biometric system. This system depends on measuring the human reactions in response to the given stimulations. The R–R distance between successive R peaks in the ECG signal and the Mel-Frequeny Cepstral Coefficients (MFCCs) extracted from the voice are taken as discriminant features for the multi-modal system. The authors adopted the K-Nearest Neighbors

(KNN) and NN classifiers to evaluate the system, and the average accuracies were 75% and 77%, respectively.

Su et al. [26] combined ECG with finger veins for robust human identification. They adopted Canonical Correlation Analysis (CCA) and Discriminant Correlation Analysis (DCA) for fusing the features extracted from every database. EER and the ROC curve are adopted as assessment tools to evaluate the performance of their model. This model achieved a 0.144% EER. It proved superiority over two other individual unimodal systems in terms of both recognition accuracy and security.

Blasco et al. [27] implemented a prototype of low-cost wearable sensors to acquire the ECG, PPG, and Galvanic Skin Response (GSR) signals to build a multi-modal biometric system for user verification. In this system, each signal is filtered, and then split into 2-s windows. Ninety-six coefficients (64 from the Walsh–Hadamard transform and 32 from the Fourier transform) are extracted from the ECG and PPG windows, and four statistical features are extracted from the GSR window. The authors adopted the Gaussian model-based density estimation classifier, which achieved an 0.99 AROC and an 0.02 EER. The related works in the literature are summarized in Table 1.

Most of the existing and previous cancelable biometric recognition systems introduced acceptable results. Still, they have several noticeable limitations that could motivate the development of new systems. Here is the summary of most limitations of the existing systems:

- ***Security:*** Existing cancelable biometric recognition systems may not provide adequate security levels, leading to risks such as unauthorized access, identity theft, and data breaches.
- ***Complexity:*** Some cancelable biometric recognition systems may require complex hardware or software, making them difficult to implement or use.
- ***Scalability:*** Some cancelable biometric recognition systems are neither scalable nor adaptable to different devices or systems, limiting their usefulness and adoption.
- ***Recognition Performance:*** Some cancelable biometric recognition systems not always perform well in terms of accuracy or speed, leading to inconvenience or frustration for users.
- ***Usability:*** Some cancelable biometric recognition systems are not always user-friendly or intuitive, leading to usability issues.

Thus, the common thread between most of the presented ECG recognition systems, whether open or cancelable, is the relatively high complexity of segmentation and classification algorithms. To access the IoMT networks, the patient needs an interactive system to deal with through the simple acquisition and ECG signal deformation strategy. In addition, a hardware implementation is required to perform these tasks automatically without user intervention. The rule of the user is only to set a patient-specific code or identifier that can be altered in hacking scenarios. That is what we will introduce in the following sections that present the details of the proposed framework, its analysis and discussions, and its superior performance compared to other related studies.

Proposed cancelable ECG recognition framework

This part presents the proposed framework to generate the cancelable ECG templates. The main desired property of a cancelable biometric system is the ability to generate cancelable templates from the original ones that cannot be used to recover the original templates again. This maintains the privacy of users. Another important desirable property is the ability to change the cancelable templates in hacking scenarios. The simplicity of implementation and the high classification accuracy are also majorly required.

The proposed framework is hybrid in nature. It comprises a non-invertible transform represented by signal dynamic range modification with Intuitionistic Fuzzy Logic (IFL) and lightweight encryption represented by binary XOR operation with a user-specific code, as shown in Fig. 1. The purpose of using this structure is to allow the non-invertibility of biometric templates with an enhanced level of privacy through lightweight encryption that is implemented at a low cost.

Transforming the signal into the fuzzy domain guarantees the non-invertibility of the transformed signal, and hence we ensure a sufficient level of distortion to hide the significant features of the original biometrics. Furthermore, the generation of a user-specific secret code with the same length as that of the ECG signal supports the process of lightweight encryption. The developed framework provides secure cancelable ECG templates that can be used for access to IoMT networks. In the proposed framework, the acquired ECG biometric signal is first filtered to eliminate the unwanted power line noise, baseline drift, or other high-frequency noise to produce an acceptable-quality ECG signal for further operations. The subsequent step is to transform the 1-D ECG signal into a 2-D matrix form, where the IFS is used to modify the signal dynamic range to generate the distorted ECG signal. Finally, for more privacy of users, the output ECG signal is converted into binary format and XORed with a user-specific binary code to obtain the final cancelable ECG template.

The steps of the proposed framework can be summarized as follows:

1. Getting the pre-processed ECG biometric signal.
2. Transformation of the ECG signal vector into a 2-D matrix.

3. Application of IFS with a selected α to generate the modified ECG template matrix.
4. Transformation of the new matrix into a 1-D vector format.
5. Binarization of the ECG vector.
6. XORing of the obtained binary vector with a user-specific code to generate the cancelable template.

Table 1 Summary of the related works

Method and reference	Number of subjects	Acquisition method or database	Classifier	Metrics	Limitations
Zhang et al. [17]	85	3 public ECG databases	Matching process	Accuracy = 97.6%	It does not consider noise on ECG signals It uses the original ECG templates It needs 20 s to register a subject and 4 s to authenticate it
Lee and Kwak [18]	100	CU-ECG DB	EECGNet-based SVM	Accuracy = 98.25%	It uses only 2 datasets It uses the original ECG templates
	290	PTB-ECG DB			It uses Deep Learning (DL) and converts the ECG signal to an image, adding more complexity
Barros et al. [19]	1500 100	PhysioNet Computing in Cardiology 2018 Database	RF classifier	Accuracy = 92% Accuracy = 95%	It uses only 1 ECG dataset It uses the original ECG templates It does not consider noise on ECG signals
Zhao et al. [22]	50	Physionet ECG database	CNN	Accuracy = 99%	It uses only 1 dataset It uses the original ECG templates It does not consider noise on ECG signals It uses DL and converts the ECG signals to images, adding more complexity
Hammad et al. [23]	25 males, and 22 females	MIT-BIH arrhythmia dataset	Feed-Forward Neural Network (FFNN)	EER = 0.06	It does not consider noise on ECG signals
	290	PTB dataset		EER = 0.14	
	65 subjects (49 males and 16 females)	CYBHi dataset		EER = 0.09	
Kim et al. [24]	89	ECG-ID database	Euclidean detector	Accuracy = 94.3%	It uses only 1 ECG dataset It does not consider noise on ECG signals
Bugdol et al. [25]	30	Voice-ECG database	KNN classifier	Accuracy = 89%	It uses only 1 ECG dataset It uses the original ECG templates It does not consider noise on ECG signals
Su et al. [26]	NaN	VeinECG obtained from FVPolyU finger vein dataset and ECG-ID dataset	DCA	Accuracy = 94%	It uses only 1 ECG dataset It uses the original ECG templates It does not consider noise on ECG signals
Blasco et al. [27]	25	Low-cost sensor dataset	One-class classifier density estimation	Accuracy = 99% EER = 0.16	It uses only 1 dataset It uses the original ECG templates It does not consider noise on ECG signals

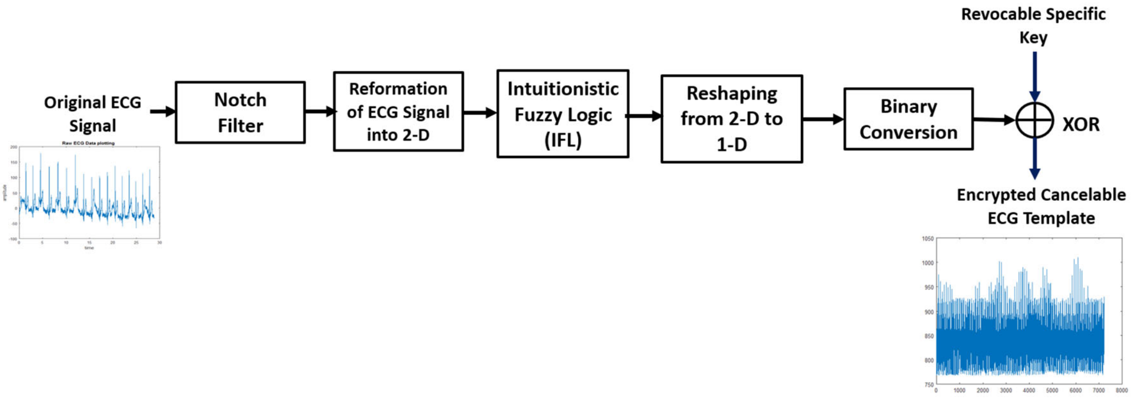


Fig. 1 Steps of the proposed cancelable ECG recognition framework

The ECG signals may be subjected to noise originating from the surrounding environment or systems mismatch during the acquisition process. Thus, the first step of the proposed framework is to remove the noise prior to further processing steps. On the other hand, to match the proposed framework with different real scenarios, its performance is examined using noisy signals with different Signal-to-Noise Ratios (SNRs). The noise affecting the signals is Additive White Gaussian Noise (AWGN) with SNRs of 10 dB, 5 dB, and 0.01 dB.

Fuzzy image processing attempts to solve the dynamic range ambiguity in 2D matrices using a membership function [28]. Due to the inherent fuzziness, uncertainty, or imperfect data of the sample values, fuzzy logic processing offers an effective framework to manage these issues. Zadeh introduced the idea of fuzzy sets in 1965 [29]. His idea presented a membership grade of any element of a certain set rather than crisp classical sets with two grades, zero or one. Therefore, the membership function is essential in all systems that use the fuzziness concept. Generally, the fuzzy logic framework consists of basic stages. The first stage is signal fuzzification, a type of non-linear signal processing to convert the signal from the time domain into a membership plane using membership functions with various shapes, which may be Gaussian, triangular, exponential, and others with grades between zero and one.

In contrast, the defuzzification stage is applied to convert the fuzzy samples into crisp gray values. An IFS and an advanced fuzzy set were proposed by Atanassov [30] to consider two degrees of uncertainty: membership and non-membership. As the selection of the type of membership function depends on the choice of the user, hesitation degree is taken into consideration in the IFS. Due to this hesitation degree, the non-membership degree is less than or equal to the complement of the membership degree [31–35]. In this paper, we use the non-linearity and non-invertibility of IFS to distort the ECG signal to perform accurate and effective dynamic range modification of the ECG signal, which prevents the inversion process.

For an image F, the IFS representation can be described mathematically as [33]:

$$F = \{< u, \mu_F(u), \upsilon_F(u) > | u \in U\} \tag{1}$$

where $\mu_F(u) : U \to [0, 1]$ refers to the degree of membership of sample value u in a finite set U and $\upsilon_F(u)$ can be estimated using Eq. (2).

$$\upsilon_F(u) = 1 - \mu_s(u) \tag{2}$$

$\upsilon_F(u)$ refers to the non-membership degree of the sample value u in a finite set U that satisfies the relation in Eq. (3).

$$0 \le \mu_F(u) + \upsilon_F(u) \le 1 \tag{3}$$

The hesitation degree π_F is described by Eq. (4):

$$\pi_F(u) = 1 - \mu_F(u) - \upsilon_F(u) \tag{4}$$

where $0 \le \pi_F(u) \le 1$ for each $u \in U$.

To transform the input 2-D matrix into the fuzzy domain to generate the two membership functions for each value in the matrix, Vlachos and Sergiadis [35] suggested the following relation to represent the required functions:

$$\mu_F(u) = \frac{u - u_{\min}}{u_{\max} - u_{\min}} \tag{5}$$

where u is the intensity value of the original signal F, u_{min} and u_{max} are the minimum and maximum intensity levels of F, respectively.

The membership function degree of the IFS of F is computed according to Eq. (6).

$$\mu_{\text{ifs}}(u; \lambda) = 1 - (1 - \mu_F(u))^{\lambda - 1} \tag{6}$$

In addition, the non-membership function degree of the IFS of F is calculated using the equation below:

$$v_{\text{ifs}}(u;\lambda) = (1 - \mu_{\text{Iifs}}(u;\lambda))^{\lambda} \tag{7}$$

Consequently, the hesitation degree of the IFS of F will be determined by:

$$\pi_{\text{ifs}}(u;\lambda) = (1 - \mu_{\text{ifs}}(u;\lambda) - v_{\text{ifs}}(u;\lambda)) \tag{8}$$

where $\lambda \geq 1$.

The converted 2-D ECG source matrix can be represented in the form of an IFS matrix as:

$$F_{\text{ifs}} = \{< u, \mu_F(u,\lambda), v_F(u,\lambda) > |u \in 0, \ldots\ldots, l-1\} \tag{9}$$

Finally, we convert the IFS matrix from the membership domain into the time domain using Eqs. (10) and (11) [28, 30],

$$u^{'} = (l-1)\mu_{D_{\text{ifs}}}(u) \tag{10}$$

and

$$\mu_{D_{\text{ifs}}}(u) = \alpha + (1-\alpha)\mu_F(u,\lambda) - \alpha v_F(u,\lambda) \tag{11}$$

where $u^{'}$ represents the final defuzzified value of each element in the 2D matrix, and α is a constant in the range of [0, 1].

The fuzzy 2-D processing based on IFS concept is shown in Fig. 2. We choose α to guarantee the generation of a completely-distorted signal prior to the subsequent encryption step.

Experiments

This section describes the methodology, metrics, and results used to evaluate the proposed framework based on ECG signal identification.

ECG datasets

To evaluate the performance of the proposed cancelable biometric recognition framework based on ECG signals, three publicly-available ECG datasets are involved in the study, namely ECG-ID [36–38], MIT-BIH [39–41], and Low-cost wearable sensors [27, 42] biometric datasets.

Using a single-lead ECG sensor, the ECG-ID dataset was generated containing 310 ECG records obtained for 90 persons (44 males and 46 females). Each record has a 20-s duration, and was sampled at 500 Hz with 12-bit resolution. The dataset also contains some demographic information, like age, gender, and recording date.

The MIT-BIH dataset contains 48 two-channel ECG recordings, each for a half-hour duration. The recordings were acquired for 47 subjects. The recordings were sampled at 360 Hz per channel with 11-bit resolution.

The low-cost wearable sensors dataset is a multi-modal biometric dataset that contains various signals, like ECG, PPG, ACC, and GSR. Data were captured for 25 subjects (16 males and 9 females) during different activities: seated at resting state, walking, and seated after a gentle stroll, cumulating a recording duration of 13 min. The ECG data were recorded using a single-lead sensor with a sampling frequency of 100 Hz.

Simulation steps

The process flow for the cancelable ECG signal generation is shown below in Fig. 3. The main steps of the entire authentication process are summarized as follows:

a. ECG signal acquisition.
b. Pre-processing and noise removal.
c. Production of cancelable ECG templates.
d. Classification and verification through correlation estimation and thresholding processes.

ECG signal acquisition

The first step for full authentication is to obtain the signals using an ECG sensor. The collected raw signals are processed and then stored in the database, which is later used for matching.

Pre-processing of ECG

The ECG signals may be subjected to some noise during the acquisition process originating from either the surrounding environment or system mismatch. Thus, a digital notch filter is applied to eliminate the power line interference, which may reduce the efficiency of the authentication process.

Production of cancelable ECG templates

After the pre-processing step, the following step is the creation of non-invertible cancelable ECG templates based on the fuzzy transformation method, which is non-invertible. In addition, lightweight encryption through XOR operation with user-specific patterns is used to increase the template security level.

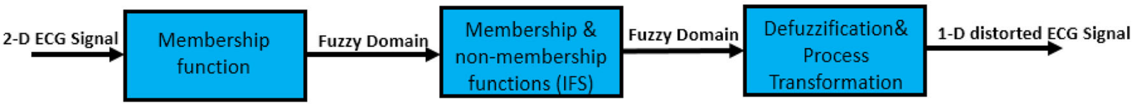

2-D ECG Signal
Membership function
Fuzzy Domain
Membership & non-membership functions (IFS)
Fuzzy Domain
Defuzzification& Process Transformation
1-D distorted ECG Signal

Fig. 2 Fuzzy 2-D processing framework based on IFS

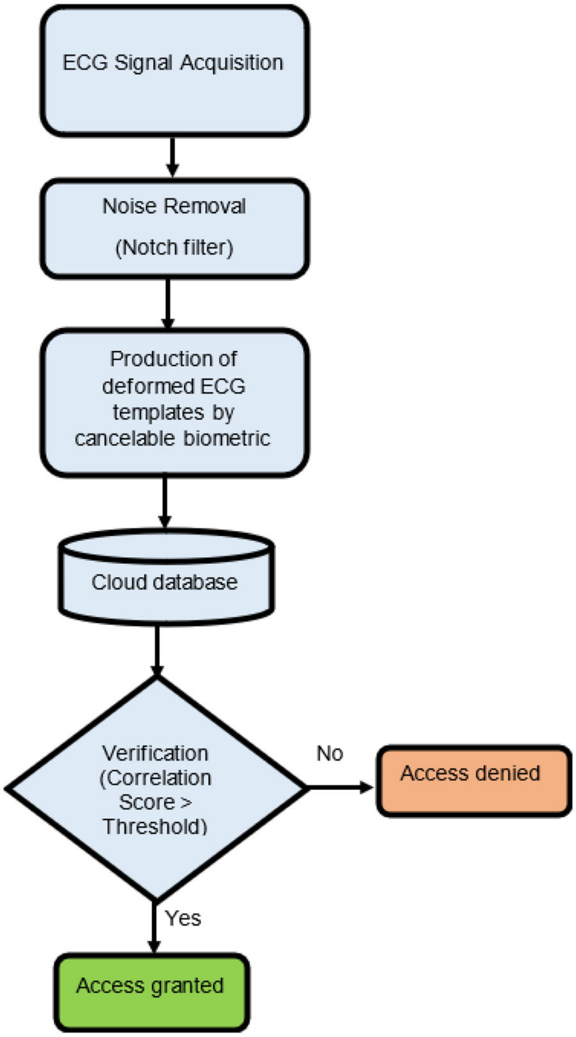

ECG Signal Acquisition
Noise Removal
(Notch filter)
Production of deformed ECG templates by cancelable biometric
Cloud database
Verification (Correlation Score > Threshold)
No
Access denied
Yes
Access granted

Fig. 3 Process flow for cancelable ECG signal authentication

Classification and verification through correlation

The goal of classification is to authenticate a valid user or to verify a user claim. The similarity score between the query and the stored biometric templates is used to produce a matching result. The authenticity of a user is determined based on the result of the matching process. The similarity score is the correlation score. The correlation estimation is performed between the query template and the corresponding ones in the database. A high correlation score means that there is a large similarity between the two encrypted templates and that belong to the same user.

Evaluation and results

The proposed framework has been tested and evaluated based on three effective metrics. The correlation coefficient score gives the correlation between the cancelable ECG templates stored in the database and the new cancelable template. It is computed mathematically as follows:

$$R_{xy} = \frac{C(x,\ y)}{\sigma_x \sigma_y} \tag{12}$$

where C is the covariance between the cancelable ECG template stored in the database represented by x and the new version in the authentication phase represented by y. σ_x and σ_y represent the standard deviations of the templates.

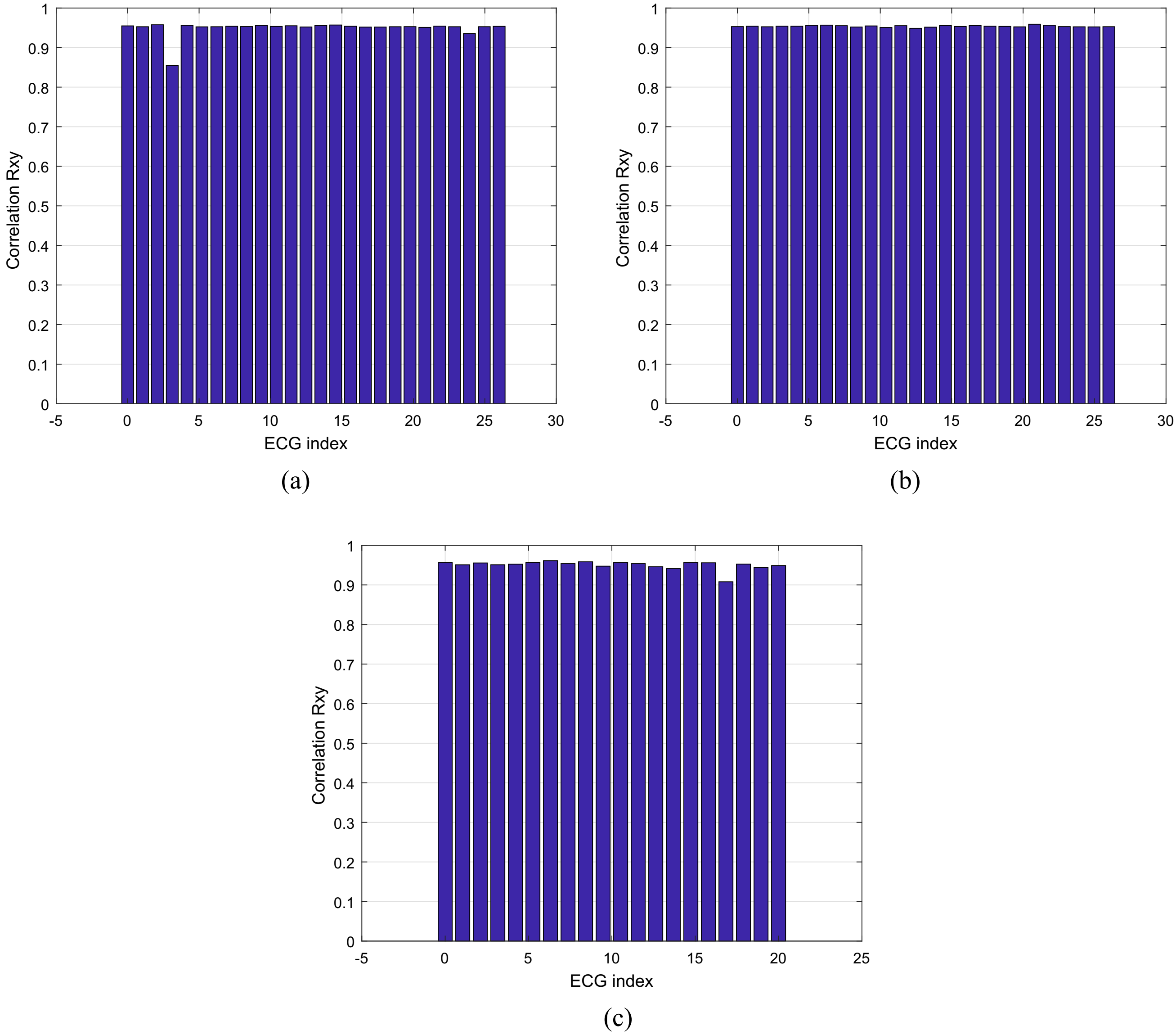
Receiver Operating Characteristic (ROC) curve and the Area under the ROC curve (AROC) are important evaluation metrics that are used to assess the authentication system performance [43–45]. The ROC curve is a plot of the False Positive Rate (FPR) against the True Positive Rate (TPR), indicating the accuracy of the classifier. The TPR represents the probability of correctly-classified states, and it is an indicator of system sensitivity. The FPR represents the probability of falsely-rejected states. TPR and FPR can be represented by the following equations [45]:

$$\text{TPR} = \frac{\text{True positive}}{\text{Total number of positives}} \tag{13}$$

$$\text{FPR} = \frac{\text{False positive}}{\text{Total number of negatives}} \tag{14}$$

Figure 4 shows the correlation scores calculated between the authorized encrypted templates in the presence of noise and their corresponding templates stored in the database. Similarly, Fig. 5 introduces the correlation scores computed for an unauthorized template with all templates stored in the database. It is clear from both figures that all correlation scores for authorized templates are higher than 0.8, while those for unauthorized templates are less than 0.08. Therefore, a threshold value can be easily adjusted in the range from 0.08 to 0.8 to discriminate between authorized and unauthorized templates. This guarantees a high security level of the proposed framework.

Moreover, to give more trust in the results, the probability distributions of the correlation scores of the authorized (genuine) and unauthorized (imposter) tests are displayed in Fig. 6. Another indicator of the efficiency of the proposed



(a)

(b)

(c)

Fig. 4 Correlation scores for authorized ECG biometric templates: **a** for the ECG-ID dataset, **b** for the MIT-BIH dataset, and **c** for the low-cost sensors biometrics dataset

framework is the AROC. As shown in Fig. 7, the higher the value of AROC, the higher the performance of the system is. The EER value is displayed for classification on all three datasets as the point obtained by intersecting the ROC curve with the diagonal of the unit square ensures a low value on the *x*-axis that reflects high accuracy of classification.

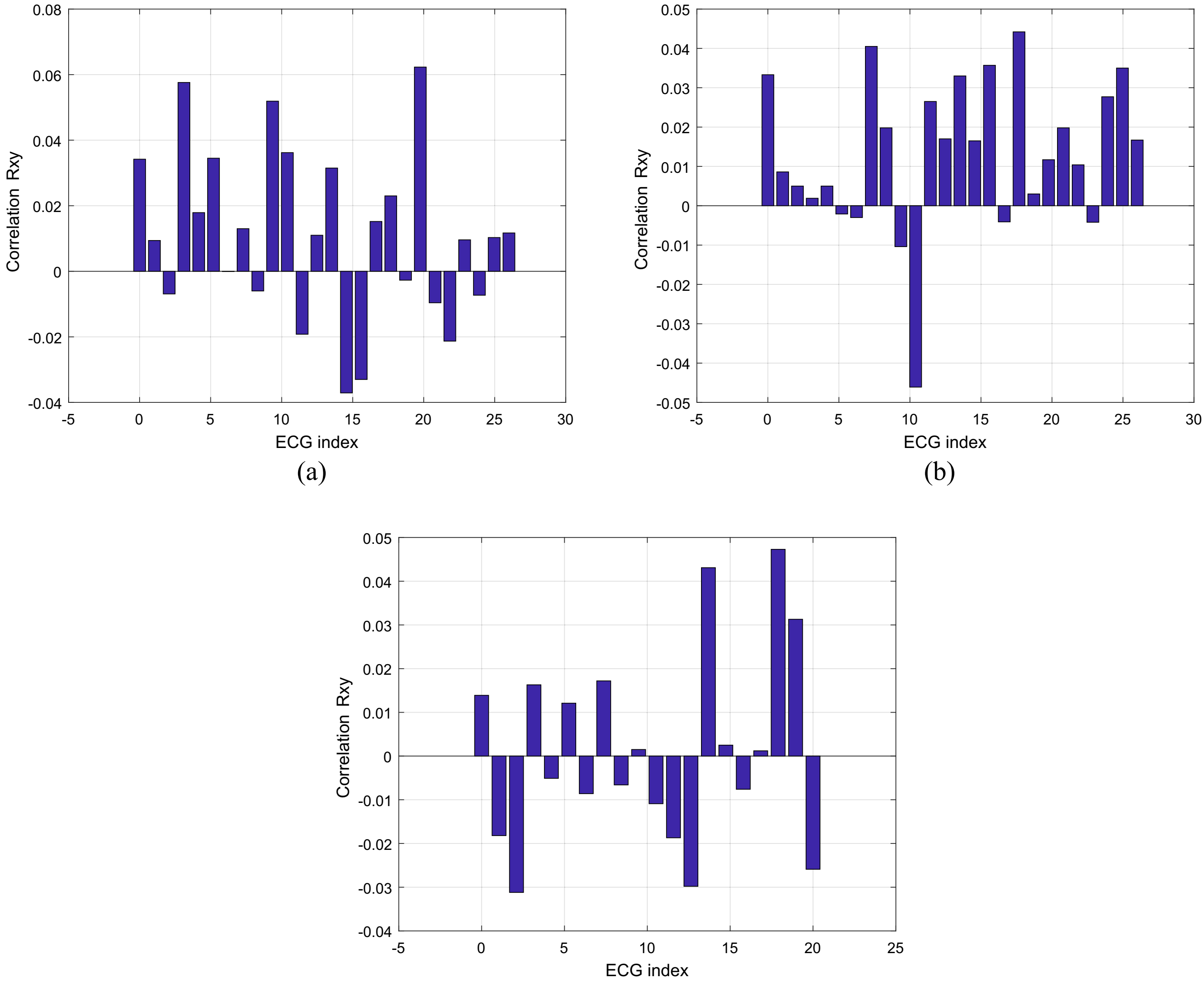
The average execution runtimes required to implement the proposed cancelable ECG recognition framework are recorded in Table 2. These times are acceptable, since the process of generating cancelable templates is implemented offline.

In addition to the execution time tests, we also performed a complexity analysis in terms of *O*-notation for steps to perform each operation as follows:

Table 2 Execution time (in seconds)

ECG dataset	Execution time (s)
ECG-ID dataset	7.48
MIT-BIH dataset	8.17
Low-cost sensors biometrics dataset	9.866

1. ($O(1)$) to register the current ECG signal;
2. ($O(n \times (M \times N))$) to perform the first distortion process using the IFS transformation with M and N as the dimensions of the 2-D matrix to be processed;



(a)

(b)

(c)

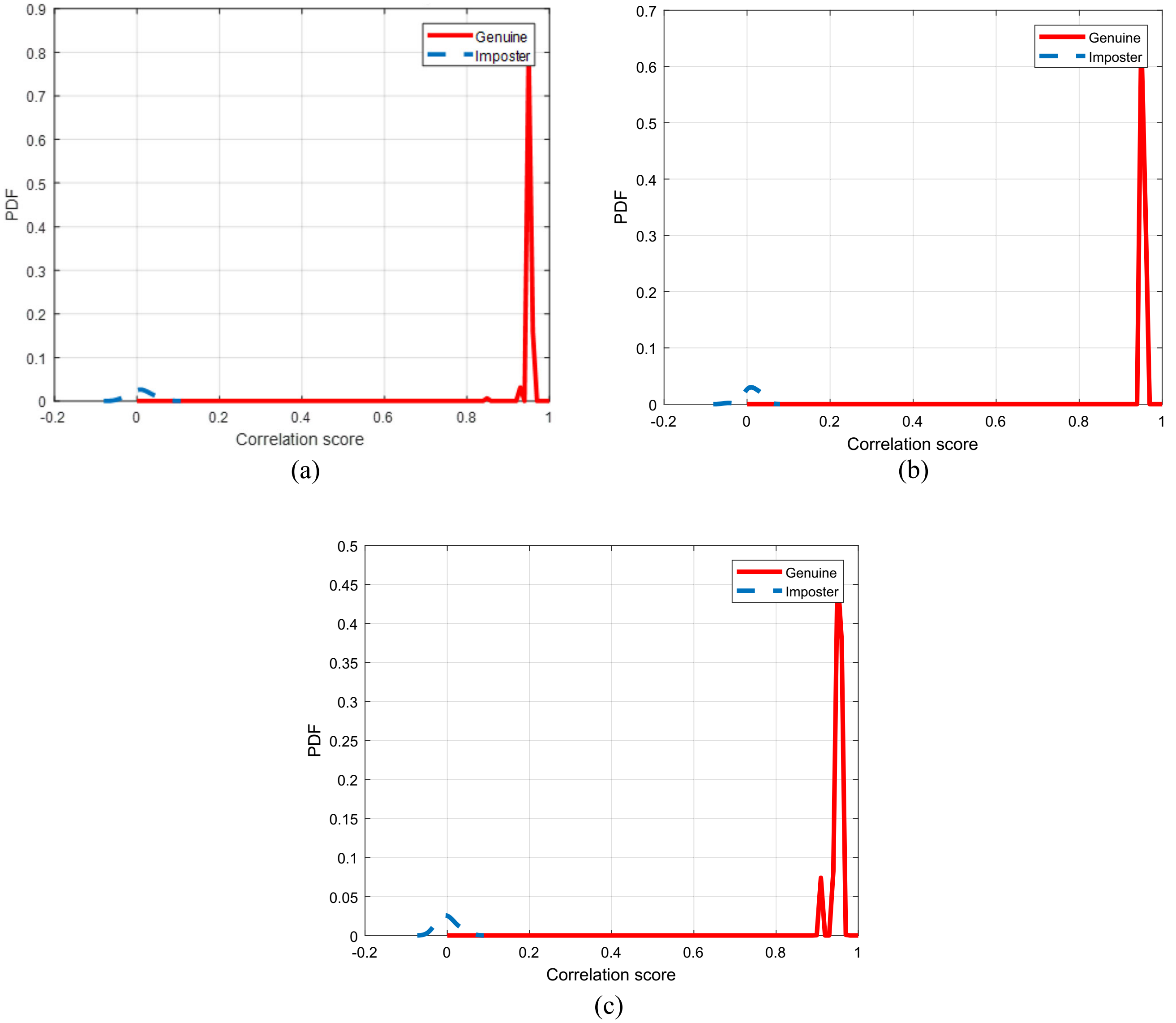
Fig. 5 Correlation scores for unauthorized imposter ECG biometric templates: **a** for the ECG-ID dataset, **b** for the MIT-BIH dataset, and **c** for the low-cost sensors biometrics dataset

3. ($O(\log_2(n/2^n))$) to perform lightweight encryption through XOR operation with n as the order of the vector space;
4. ($O(1)$) to compute the correlation coefficient between the cancelable template of the current user and any one stored in the database;
5. ($O(n)$) to execute the authentication process producing an outcome, whether granted or declined user based on the value of the correlation score.

Table 3 introduces a comparative study with other cancelable ECG recognition systems. In addition, the table shows the performance of the proposed framework at different noise levels. The results reveal that the proposed framework demonstrates superiority over the previous cancelable biometric systems. Furthermore, the high accuracy value of 99.5% at different noise levels and the corresponding low EER value of 0.058% affirm the strength of the proposed framework.

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

- The overall performance of the proposed framework is better than those of the previous systems from the authentication perspective.
- The proposed cancelable biometric recognition framework based on ECG signals overcomes most of the limitations of the existing systems related to accuracy levels.
- The resulting correlation scores in the fuzzy domain are better than those obtained in the original time domain.
- In the final step of the proposed framework, the output encrypted templates are represented in vector format, and



(a)

(b)

(c)

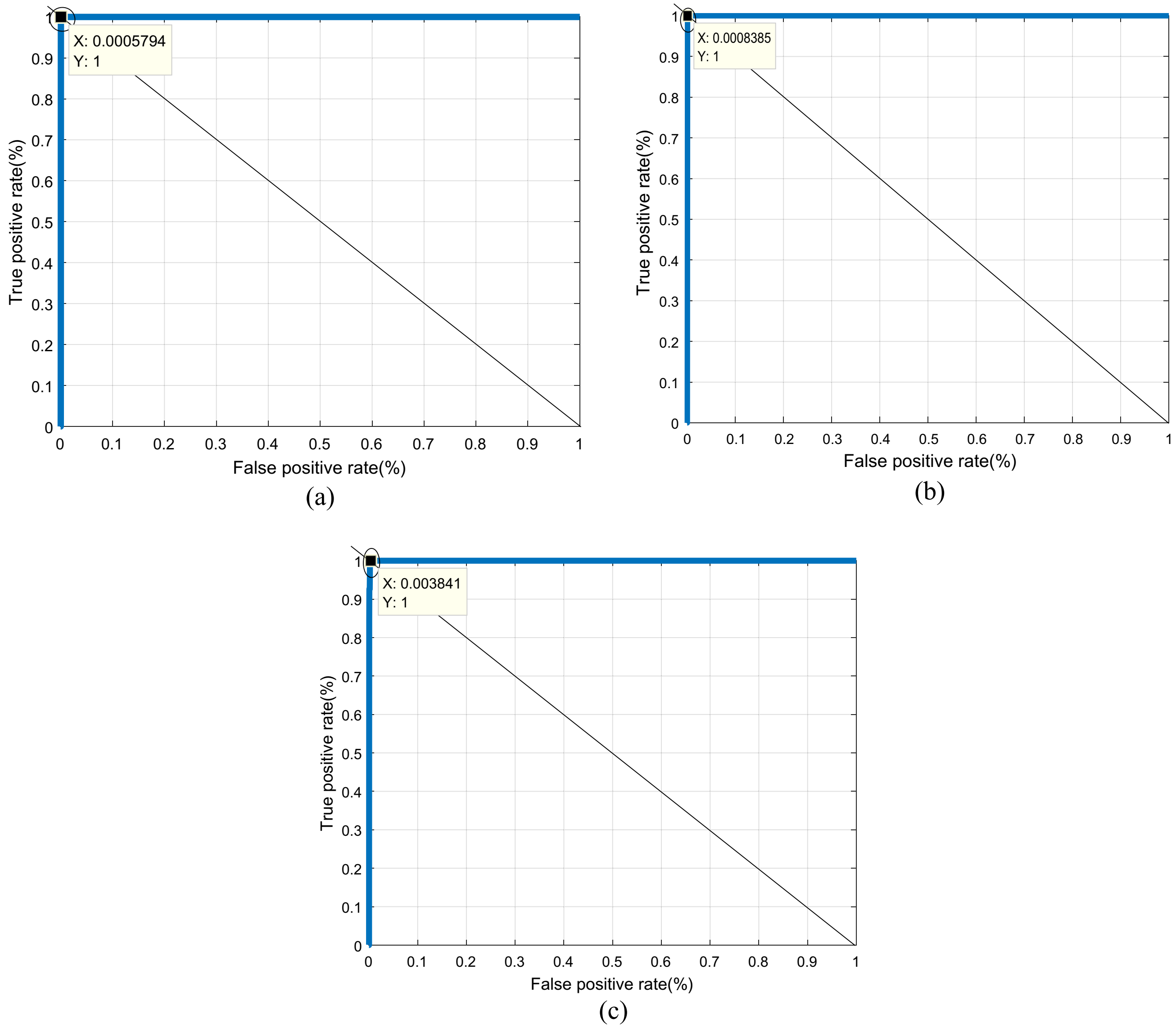
Fig. 6 Probability distributions for the cancelable ECG recognition framework: **a** for the ECG-ID dataset, **b** for the MIT-BIH dataset, and **c** for the low-cost sensors biometrics dataset

hence it could be used with many state-of-the-art classifiers for more accurate classification results.

Hardware implementation

The hardware implementation of the proposed cancelable ECG recognition framework is important, as it allows the patient to have an accompanying hardware that can carry out the task of cancelable template generation without his intervention to save his time and effort. The presented hardware for this task should be as accurate as the suggested software algorithm. The proposed framework is implemented on FPGA using Xilinx System Generator with MATLAB Simulink. The first stage in this hardware is the notch filter, which is realized as a fixed-point Infinite Impulse Response (IIR) filter, as shown in Fig. 8. This realization is selected to optimize the filter performance and minimize finite-word-length effects, such as the register overflow and arithmetic-round-off errors. Figure 8 shows the Simulink model for the whole proposed cancelable ECG recognition framework, including the fuzzy logic processing and the lightweight encryption.

In the realization in Fig. 9, fixed-point numbers are used to avoid the overflow problem, which increases quantization errors. The issue of register overflow occurs, when the signal dynamic range requires registers with values



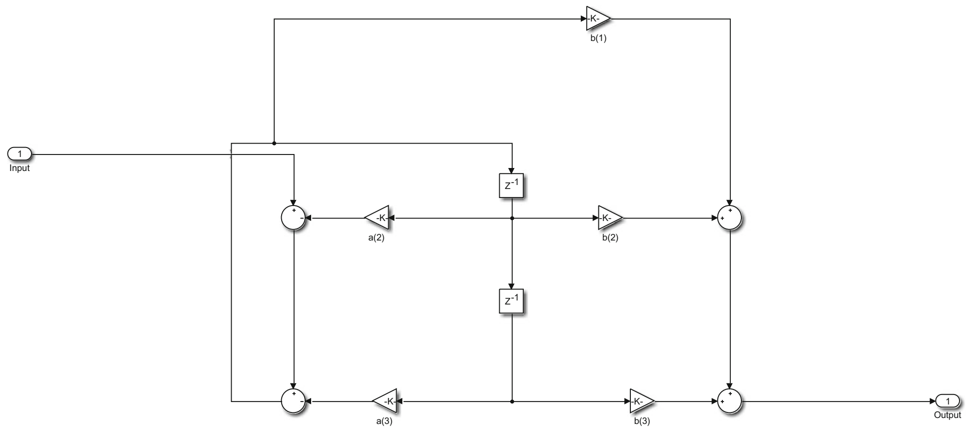
(a)

(b)

(c)

Fig. 7 Receiver operating characteristic (ROC) curves for the cancelable ECG recognition framework: **a** for the ECG-ID dataset, **b** for the MIT-BIH dataset, and **c** for the low-cost sensors biometrics dataset

Fig. 8 Simulink model of the direct form II IIR notch filter



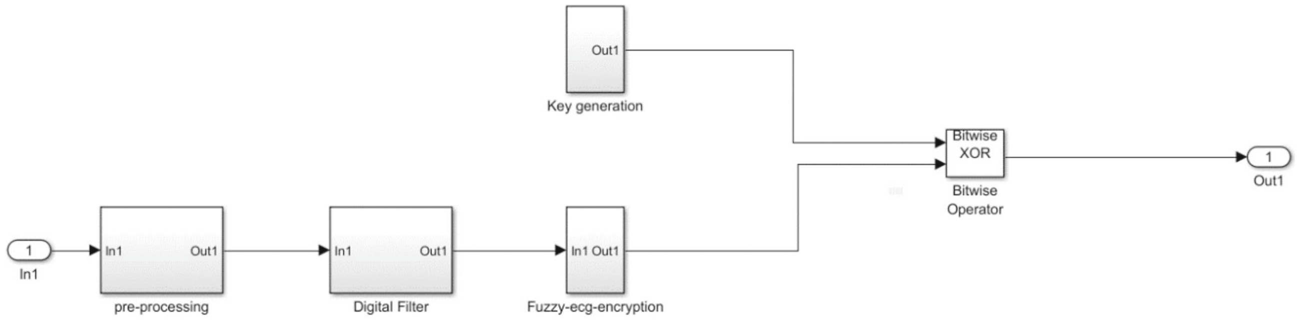


Fig. 9 Simulink model for the proposed cancelable ECG recognition framework

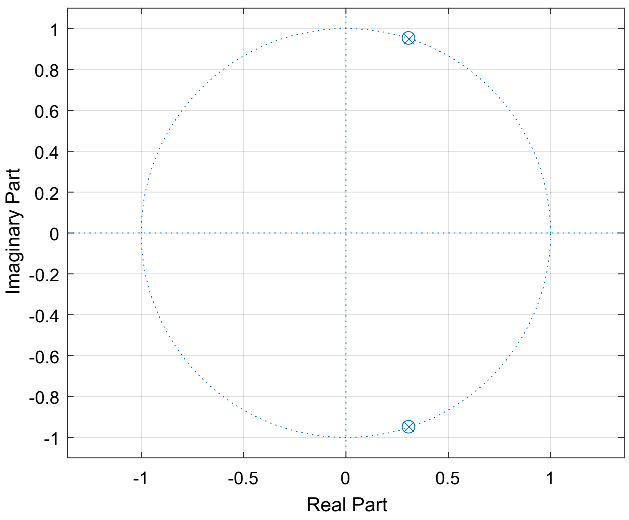


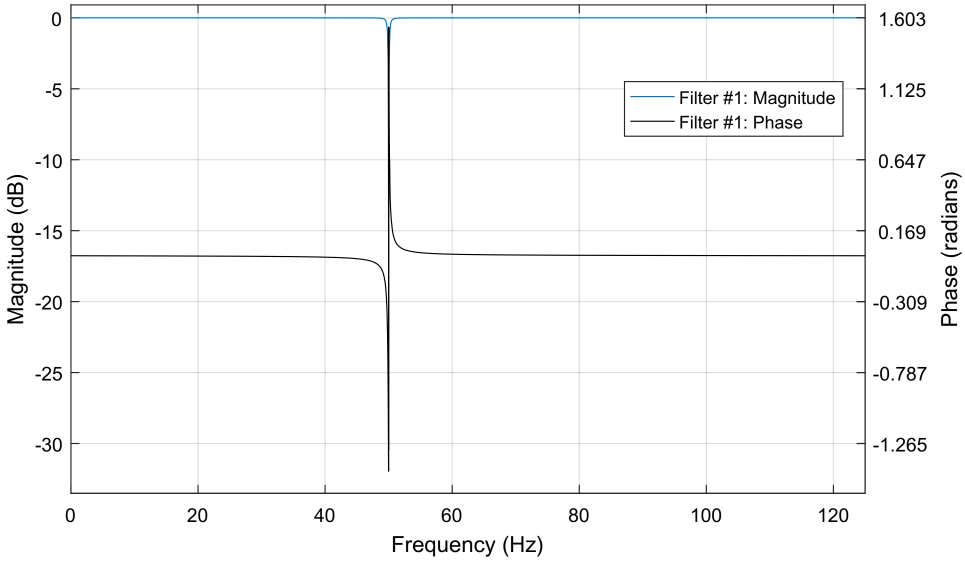
Fig. 10 IIR filter pole/zero diagram

exceeding the limited dynamic range of fixed-point registers. Hence, the overflow causes the system to behave in an unpredictable, non-linear manner, producing potentially-large runtime errors. The use of the arithmetic-round-off operation makes the system behave linearly with degraded precision due to the accumulation of various arithmetic errors within the filter [46].

As shown in Fig. 8, an IIR notch filter in direct form II is used [47]. The IIR filter gives a better frequency response for low orders than that obtained with the FIR filter [48]. It also reduces the calculations per time step and has non-linear phase characteristics. According to the desired requirements, the filter has a sampling frequency of 250 Hz, a notch frequency of 50 Hz, and a bandwidth of 0.4. The characteristics of the proposed IIR notch filter are shown in Figs. 10, 11, and 12. The hardware implementation units required for filter realization are summarized in Table 4. It is clear that the hardware cost is acceptable.

Figures 13, 14, and 15 illustrate the Simulink models for the fuzzy logic processing building units. It is clear that the hardware complexity of the fuzzy logic processing units is still acceptable. Figure 16 shows a cancelable ECG template generated with the suggested hardware. Numerical metrics

Fig. 11 IIR filter magnitude and phase responses



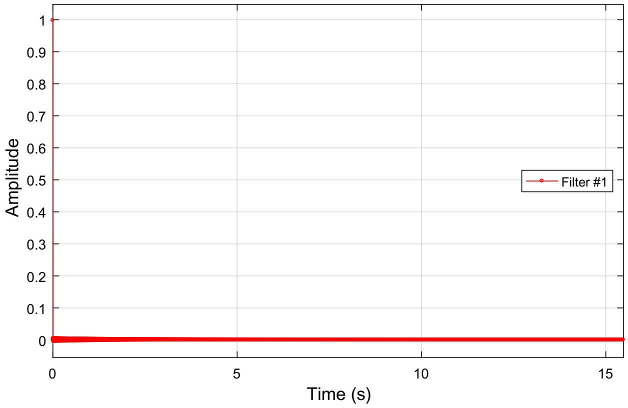


Fig. 12 IIR filter impulse response

show that the Mean Square Error (MSE) between the distorted cancelable ECG template and the original one is very large, while the correlation coefficient is very low. Moreover, the proposed cancelable ECG recognition framework has been completely implemented with the suggested hardware. The results of this implementation are illustrated in Figs. 17 and 18, showing an EER = 0.008. These results ensure the high accuracy of the introduced hardware compared to the presented software implementation.

Conclusions and future work

This study has been concerned with the issue of securing IoMT networks at the access point. Users are allowed to access the IoMT networks with cancelable templates generated from their unique ECG signals. Hence, their privacy is preserved. The introduced cancelable ECG recognition framework is simple in implementation due to the utilization of a hybrid structure that comprises fuzzy dynamic range modification of ECG signals and lightweight encryption. Through this cascaded structure, the low complexity is guaranteed to save the time and effort of users during the access process. Moreover, the proposed framework has been implemented with a hardware that can accompany the user or the patient to automate the whole access process to be as fast and simple as possible. Quantitative and qualitative results from simulations and comparisons with the previous systems ensure low EER values and high AROC values for the proposed cancelable ECG recognition framework at different noise levels.

The security of IoMT networks is an interesting research topic that has the potential to be developed further in the future. Here are some future research directions for the security of IoMT networks:

- Improvement of recognition performance: Future work can focus on improving the recognition performance of the proposed framework. This can be done by using more advanced machine learning algorithms or by incorporating other biometric modalities to enhance the recognition accuracy.
- Security enhancement: Although the proposed framework is secure, further work can be done to enhance the security level. Stronger encryption methods and more complex fuzzy logic algorithms can be used for this task.
- Evaluation of the system usability and acceptability: As biometric systems become more prevalent in healthcare and medical applications, it is essential to understand how users interact with them. Future research could investigate the usability and acceptability of the cancelable biometric recognition framework based on fuzzy logic processing and lightweight encryption for IoMT applications. So, usability testing can be conducted to evaluate the ease of use and user satisfaction with the proposed framework. This would help identify areas for improvement and ensure that the framework is user-friendly.
- Development of a standard framework for evaluating biometric systems: With the proliferation of biometric systems, there is a need to establish a standard framework for evaluating their effectiveness and security. Future research could focus on developing a framework for evaluating the performance and security of the cancelable biometric recognition systems, especially the one based on fuzzy logic processing and lightweight encryption.
- Extending the framework to other healthcare applications: The proposed cancelable biometric recognition framework has the potential to be extended to other healthcare applications beyond the IoMT. Future research could explore its applicability in areas such as patient identification, medical record management, and healthcare payment systems.
- Investigating the framework resistance to attacks: The proposed cancelable biometric recognition framework is designed to be resilient to attacks such as brute-force and dictionary attacks. Future research could focus on investigating the system resistance to more advanced attacks, such as machine-learning-based attacks or attacks that target specific vulnerabilities.
- Integration with blockchain technology: The integration of the proposed cancelable biometric recognition framework with blockchain technology can provide an added layer of security to the authentication process. Future works can focus on exploring how the blockchain can be used to store biometric data securely and how the cancelable biometric recognition framework can benefit from the blockchain to enhance users' security and privacy.
- Integration with existing systems: The proposed framework can be integrated with existing IoMT systems to enhance their security and reliability. This would involve developing a standard protocol for this integration.

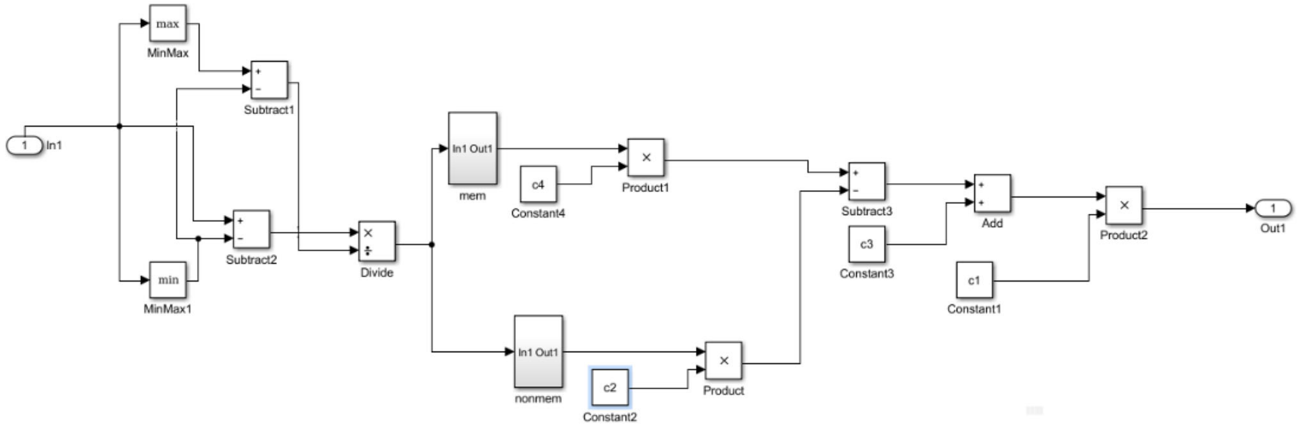


Fig. 13 Simulink model for fuzzy logic processing of ECG signals

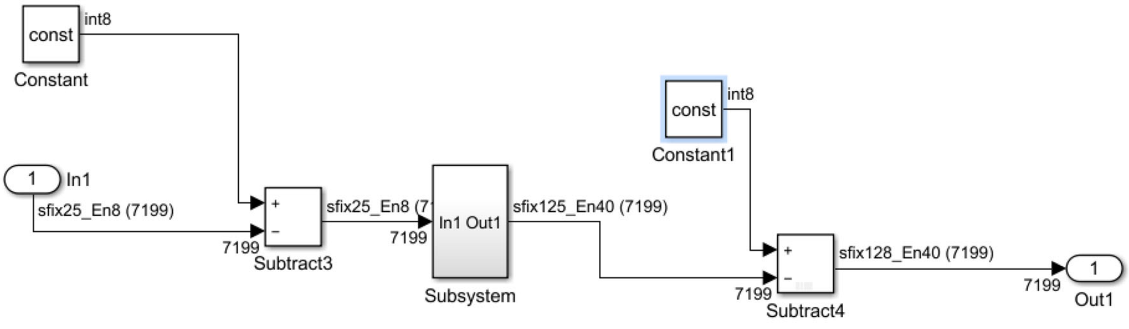


Fig. 14 Simulink model of the membership function

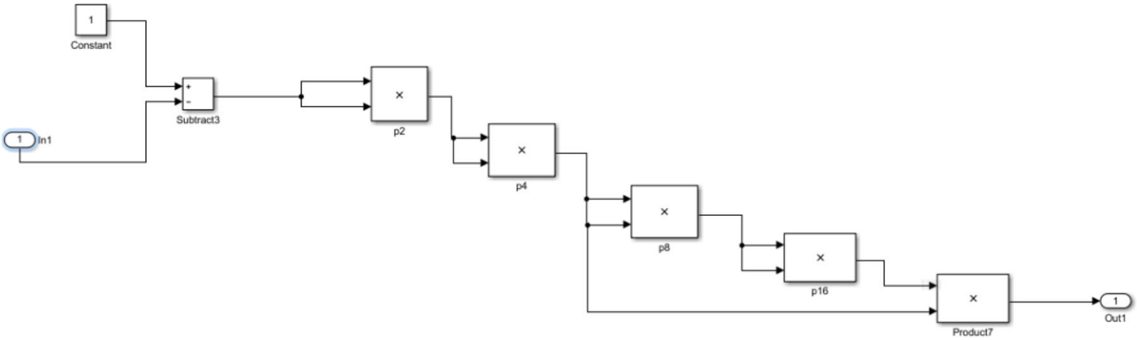


Fig. 15 Simulink model of the non-membership function

- Development of multi-modal biometric systems: The use of multiple biometric modalities can improve the accuracy and reliability of biometric systems. Future works can explore the possibility of integrating the proposed cancelable biometric recognition framework with other biometric modalities to enhance the overall performance.
- Real-time authentication: The proposed framework is designed to operate in batch mode. Future works can focus on exploring how the proposed framework can be adapted to provide real-time authentication, which is essential for many IoMT applications. So, it can be implemented in real time to provide instantaneous authentication and authorization for IoMT devices. This would require optimization of the used algorithms for real-time processing.
- Robustness to variability: Biometric systems may be affected by various factors such as changes in noise level and interference. Future works can focus on improving the robustness of the proposed cancelable biometric recognition framework to these factors by exploring different feature extraction techniques, fuzzy logic models, and lightweight encryption algorithms.

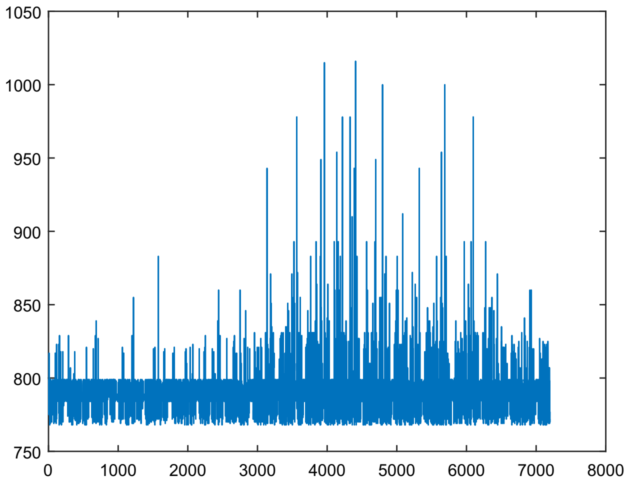


Fig. 16 Cancelable ECG template generated with the recommended hardware, MSE = 7.0608×10^5, and correlation with the original template = 0.0371

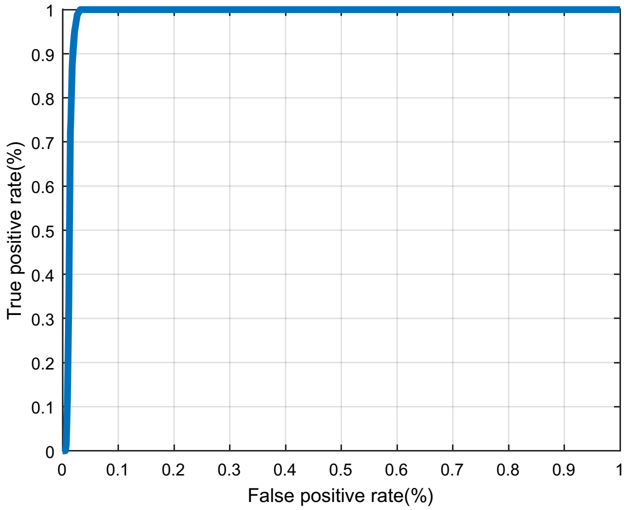


Fig. 17 ROC curves for the hardware implementation of the proposed cancelable ECG recognition framework

- Large-scale deployment: The proposed cancelable biometric recognition framework can be deployed in various healthcare settings, including hospitals, clinics, and remote healthcare systems. Future works can focus on exploring the scalability and feasibility of deploying this framework on a large scale and addressing the challenges associated with this deployment, such as user acceptance and integration with existing healthcare systems. This would help to reveal the effectiveness of the proposed framework in real-world scenarios.
- Privacy and ethical considerations: Future work can also focus on the user privacy and ethical considerations of the proposed framework. This would involve investigating the potential risks associated with the collection and storage

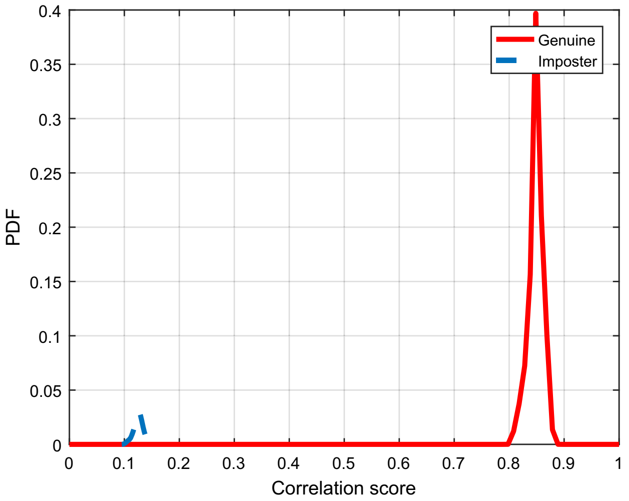


Fig. 18 Probability distributions of the hardware implementation of the proposed cancelable ECG recognition framework

Table 3 Summary of the performance evaluation metrics of the proposed framework compared to related systems

Work	Dataset	EER (%)	Accuracy (%)
Barros et al. [19]	PhysioNet	N/A	92
Su et al. [26]	ECG-ID	0.144	75.71
Zhang et al. [17]	ptbdb, mitdb, nsrdb	1.57	97.6
Hammad et al. [23]	MIT-BIH	6	N/A
Kim et al. [24]	ECG-ID	2.6	94.3
Zhao et al. [22]	ECG-ID	5.68	96.6
Blasco et al. [27]	Low-cost sensors biometrics	2	99
Proposed framework at SNR = 10 dB	ECG-ID	0.058	99.5
	MIT-BIH	0.083	99.4
	Low-cost sensors biometrics	0.38	99.4
Proposed framework at SNR = 5 dB	ECG-ID	1.3	99.4
	MIT-BIH	0.9	99.42
	Low-cost sensors biometrics	1.37	99.51
Proposed framework at SNR = 0.01 dB	ECG-ID	7	93.04
	MIT-BIH	6	93.59
	Low-cost sensors biometrics	11.26	90

Table 4 Implementation cost of the proposed filter

Parameter	Value
Number of multipliers	5
Number of adders	4
Number of states	2

of biometric data and ensuring that the framework is compliant with relevant privacy regulations.

By focusing on these suggested directions for future work, we can enhance the effectiveness and security of the proposed cancelable biometric recognition framework and expand its applicability to various IoMT applications.

Author contributions All authors equally contributed.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

Availability of data and materials All data are available upon request from the corresponding author.

Declarations

Conflict of interest The authors declare no conflict of interests.

References

1. Ghubaish A, Salman T, Zolanvari M et al (2021) Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet Things J 8:8707–8718. https://doi.org/10.1109/JIOT.2020.3045653
2. Gadekallu TR, Alazab M, Hemanth J, Wang W (2023) Guest editorial federated learning for privacy preservation of healthcare data in internet of medical things and patient monitoring. IEEE J Biomed Health Inform 27:648–651. https://doi.org/10.1109/JBHI.2023.3234604
3. Xiong H, Jin C, Alazab M et al (2022) On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT. IEEE J Biomed Health Inform 26:1977–1986. https://doi.org/10.1109/JBHI.2021.3112693
4. Almogren A, Mohiuddin I, Din IU et al (2021) FTM-IoMT: fuzzy-based trust management for preventing sybil attacks in internet of medical things. IEEE Internet Things J 8:4485–4497. https://doi.org/10.1109/JIOT.2020.3027440
5. Siam AI, El-khobby HA, Abd Elkader HS et al (2015) Enhanced data security model for cloud computing platform. Int J Sci Res Sci Eng Technol 1:450–460
6. Xin Y, Kong L, Liu Z et al (2018) Multimodal feature-level fusion for biometrics identification system on IoMT platform. IEEE Access 6:21418–21426. https://doi.org/10.1109/ACCESS.2018.2815540
7. Siam AI, El-Affendi MA, Abou Elazm A et al (2022) Portable and real-time IoT-based healthcare monitoring system for daily medical applications. IEEE Trans Comput Soc Syst. https://doi.org/10.1109/TCSS.2022.3207562
8. Siam AI, Almaiah MA, Al-Zahrani A et al (2021) Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Comput Intell Neurosci 2021:1–23. https://doi.org/10.1155/2021/8016525
9. Siam AI, Abou Elazm A, El-Bahnasawy NA et al (2019) Smart health monitoring system based on IoT and cloud computing. Menoufia J Electron Eng Res 28:37–42. https://doi.org/10.21608/mjeer.2019.76711
10. Uwaechia AN, Ramli DA (2021) A comprehensive survey on ECG signals as new biometric modality for human authentication: recent advances and future challenges. IEEE Access 9:97760–97802. https://doi.org/10.1109/ACCESS.2021.3095248
11. Siam AI, Abou Elazm A, El-Bahnasawy NA et al (2021) PPG-based human identification using Mel-frequency cepstral coefficients and neural networks. Multimed Tools Appl 80:26001–26019. https://doi.org/10.1007/s11042-021-10781-8
12. Siam AI, El-khobby HA, Abdelnaby MM et al (2019) A novel speech enhancement method using Fourier series decomposition and spectral subtraction for robust speaker identification. Wireless Pers Commun 108:1055–1068. https://doi.org/10.1007/s11277-019-06453-4
13. Sharma A, Tanwar RS, Singh Y et al (2022) Heart rate and blood pressure measurement based on photoplethysmogram signal using fast Fourier transform. Comput Electr Eng 101:108057. https://doi.org/10.1016/j.compeleceng.2022.108057
14. Mahmoud NM, Fouad H, Soliman AM (2021) Smart healthcare solutions using the internet of medical things for hand gesture recognition system. Complex Intell Syst 7:1253–1264. https://doi.org/10.1007/s40747-020-00194-9
15. Patel VM, Ratha NK, Chellappa R (2015) Cancelable biometrics: a review. IEEE Signal Process Mag 32:54–65. https://doi.org/10.1109/MSP.2015.2434151
16. Tran QN, Turnbull BP, Hu J (2021) Biometrics and privacy-preservation: how do they evolve? IEEE Open J Comput Soc 2:179–191. https://doi.org/10.1109/OJCS.2021.3068385
17. Zhang Y, Junjie Wu (2016) Practical human authentication method based on piecewise corrected Electrocardiogram. In: 2016 7th IEEE international conference on software engineering and service science (ICSESS). IEEE, pp 300–303
18. Lee J-N, Kwak K-C (2019) Personal identification using a robust eigen ECG network based on time-frequency representations of ECG signals. IEEE Access 7:48392–48404. https://doi.org/10.1109/ACCESS.2019.2904095
19. Barros A, Resque P, Almeida J et al (2020) Data improvement model based on ECG biometric for user authentication and identification. Sensors 20:2920. https://doi.org/10.3390/s20102920
20. Ghassemi M, Moody B, Lehman L, et al (2018) You snooze, you win: the physionet/computing in cardiology challenge 2018. In: 2018 Computing in cardiology conference (CinC). IEEE
21. Huang Y, Yang G, Wang K et al (2021) Learning joint and specific patterns: a unified sparse representation for off-the-person

ECG biometric recognition. IEEE Trans Inf Forensics Secur 16:147–160. https://doi.org/10.1109/TIFS.2020.3006384

22. Zhao Z, Zhang Y, Deng Y, Zhang X (2018) ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation. Comput Biol Med 102:168–179. https://doi.org/10.1016/j.compbiomed.2018.09.027
23. Hammad M, Luo G, Wang K (2019) Cancelable biometric authentication system based on ECG. Multimed Tools Appl 78:1857–1887. https://doi.org/10.1007/s11042-018-6300-2
24. Kim H, Nguyen MP, Chun SY (2017) 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). IEEE, pp 454–457
25. Bugdol MD, Mitas AW (2014) Multimodal biometric system combining ECG and sound signals. Pattern Recogn Lett 38:107–112. https://doi.org/10.1016/j.patrec.2013.11.014
26. Su K, Yang G, Wu B et al (2019) Human identification using finger vein and ECG signals. Neurocomputing 332:111–118. https://doi.org/10.1016/j.neucom.2018.12.015
27. Blasco J, Peris-Lopez P (2018) On the feasibility of low-cost wearable sensors for multi-modal biometric verification. Sensors 18:2782. https://doi.org/10.3390/s18092782
28. Chaira T (2015) Medical image processing: advanced fuzzy set theoretic techniques. CRC Press
29. Zadeh L (1978) Fuzzy sets as a basis for a theory of possibility. Fuzzy Sets Syst 1:3–28. https://doi.org/10.1016/0165-0114(78)90029-5
30. Atanassov K (2016) Intuitionistic fuzzy sets. Int J Bioautomation 20:1
31. Ejegwa PA, Akowe SO, Otene PM, Ikyule JM (2014) An overview on intuitionistic fuzzy sets. Int J Sci Technol Res 3:142–145
32. Verma H, Gupta A, Kumar D (2019) A modified intuitionistic fuzzy c-means algorithm incorporating hesitation degree. Pattern Recogn Lett 122:45–52. https://doi.org/10.1016/j.patrec.2019.02.017
33. Chaira T (2020) Intuitionistic fuzzy approach for enhancement of low contrast mammogram images. Int J Imaging Syst Technol 30:1162–1172
34. Kaushik R, Bajaj RK, Kumar T (2015) On intuitionistic fuzzy divergence measure with application to edge detection. Procedia Comput Sci 70:2–8. https://doi.org/10.1016/j.procs.2015.10.017
35. Vlachos IK, Sergiadis GD (2007) The role of entropy in intuitionistic fuzzy contrast enhancement. In: Foundations of fuzzy logic and soft computing: 12th international fuzzy systems association world congress, IFSA 2007, Cancun, Mexico, June 18–21, 2007. Proceedings 12. pp 104–113
36. Lugovaya TS (2005) Biometric human identification based on electrocardiogram. Master's thesis, Faculty of Computing Technologies and Informatics, Electrotechnical University 'LETI', Saint-Petersburg, Russian Federation
37. Lugovaya TS ECG-ID Database. https://physionet.org/content/ecgiddb/1.0.0/. Accessed 14 Apr 2023
38. Goldberger AL, Amaral LAN, Glass L et al (2000) PhysioBank, PhysioToolkit, and PhysioNet. Circulation. https://doi.org/10.1161/01.CIR.101.23.e215
39. Moody GB, Mark RG (2001) The impact of the MIT-BIH arrhythmia database. IEEE Eng Med Biol Mag 20:45–50. https://doi.org/10.1109/51.932724
40. Moody GB, Mark RG MIT-BIH arrhythmia database. https://physionet.org/content/mitdb/1.0.0/. Accessed 14 Apr 2023
41. Mark RG, Schluter PS, Moody G, et al (1982) An annotated ECG database for evaluating arrhythmia detectors. In: IEEE Transactions on Biomedical Engineering. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC, p 600
42. Blasco J, Peris-Lopez P Low-cost sensors biometrics dataset. https://www.dropbox.com/s/lei4a27fcgp0ygr/LowCostSensorsBiometrics.zip?dl=0. Accessed 14 Apr 2023
43. Siam AI, Sedik A, El-Shafai W et al (2021) Biosignal classification for human identification based on convolutional neural networks. Int J Commun Syst. https://doi.org/10.1002/dac.4685
44. Soliman RF, Amin M, Abd El-Samie FE (2018) A double random phase encoding approach for cancelable iris recognition. Opt Quant Electron 50:326. https://doi.org/10.1007/s11082-018-1591-0
45. Siam AI, Gamel SA, Talaat FM (2023) Automatic stress detection in car drivers based on non-invasive physiological signals using machine learning techniques. Neural Comput Appl. https://doi.org/10.1007/s00521-023-08428-w
46. Christensen M, Taylor FJ (2006) Fixed-point-IIR-filter challenges. EDN Netw 51:111–122
47. El-Shafai W, Mohamed FAHE, Elkamchouchi HMA et al (2021) Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. IEEE Access 9:77675–77692. https://doi.org/10.1109/ACCESS.2021.3082940
48. Chanukya PSVVN, Thivakaran TK (2020) Multimodal biometric cryptosystem for human authentication using fingerprint and ear. Multimed Tools Appl 79:659–673. https://doi.org/10.1007/s11042-019-08123-w

Author and Affiliations

Ghada M. El-Banby[1] · Lamiaa A. Abou Elazm[2] · Walid El-Shafai[3] · Nirmeen A. El-Bahnasawy[4] · Fathi E. Abd El-Samie[3] · Atef Abou Elazm[3] · Ali I. Siam[5]

Ghada M. El-Banby
ghadaelbanby75@gmail.com

Lamiaa A. Abou Elazm
lamiaa.abouelazm@gmail.com

Walid El-Shafai
eng.waled.elshafai@gmail.com

Nirmeen A. El-Bahnasawy
nirmeena.el-bahnasawy@el-eng.menofia.edu.eg

Fathi E. Abd El-Samie
fathi_sayed@yahoo.com

Atef Abou Elazm
abouelazm.atef@el-eng.menofia.edu.eg

[1] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Department of Microelectronics, Electronics Research Institute, Nozha, Giza, Egypt

[3] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[4] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[5] Department of Embedded Network Systems Technology, Faculty of Artificial Intelligence, Kafrelsheikh University, Kafr El-Shaikh, Egypt