IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 5, October, 2025, pp. 2539-2547
Journal homepage: http://iieta.org/journals/ts

Fuzzy-Logic-Based Biometric Authentication for IoT Access Using Speech and ECG Signals

Ghada M. El-Banby[1], Safaa M. El-Gazar[2*], Walid El-Shafai[3], Rania M. Ghoniem[4], Fathi E. Abd El-Samie[4]

[1] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[2] Department of Information Systems, Osim Higher Institute for Administrative Sciences, Giza 12961, Egypt
[3] Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia
[4] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Corresponding Author Email: engsafaa2004@yahoo.com

https://doi.org/10.18280/ts.420508

Received: 27 April 2025
Revised: 10 June 2025
Accepted: 26 September 2025
Available online: 31 October 2025

Keywords:
biometric security, electrocardiogram signal, fuzzy system, Internet of Things

ABSTRACT

Authentication in the Internet of Things (IoT) is paramount, especially for individuals with disabilities, as it enables secure and seamless access to essential services and devices. Leveraging the distinctiveness of biometric signals like speech and electrocardiogram (ECG) signals has emerged as an effective approach to allow authentication, offering a convenient and unobtrusive means of identification. This paper presents a novel fuzzy system to generate cancelable biometric templates for access to IoT networks, significantly enhancing biometric security and user privacy and solving the ever-existing conflict between security and privacy. By transforming original biometric data templates into a non-reversible format, the fuzzy logic system protects these templates even in the event of a security breach. This approach not only meets the demand for robust IoT authentication for people with disabilities but also aligns with the trend towards more secure, user-friendly biometric authentication. Extensive simulation experiments under varying noise levels demonstrate the system resilience and strong performance.

1. INTRODUCTION

The rapid propagation of Internet of Things (IoT) devices has necessitated the development of advanced security frameworks, with a particular emphasis on biometric authentication mechanisms. Conventional biometric techniques, such as fingerprint and facial recognition, often pose accessibility challenges for individuals with disabilities. In this paper, we investigate the viability of voice and electrocardiogram (ECG) signals as alternative biometric modalities. The paper emphasizes the ability of voice- and ECG-based biometrics to enhance security within IoT ecosystems [1].

Biometric authentication relies on distinctive physiological or behavioral characteristics for the purpose of identity verification. In the IoT systems, such modalities enable secure access control across a wide spectrum of interconnected devices, including but not limited to smart home systems and wearable healthcare devices [2]. Conventional biometric recognition techniques—such as fingerprint recognition, facial recognition, and retinal scanning—often pose significant usability challenges for individuals with disabilities. For example, fingerprint-based systems may be ineffective for users with prosthetic limbs, and facial recognition may yield suboptimal performance in cases involving facial disfigurement or neurological impairments. Alternatively, voice and electrocardiogram (ECG)-based authentication modalities offer a promising combination of robust security and enhanced accessibility. However, their reliability can be influenced by external environmental noise and intrinsic physiological variability [3].

The integration of voice recognition technology into smart home environments represents a viable and effective approach to secure and user-friendly access control, particularly benefiting individuals with mobility impairments. Voice-based biometric authentication exploits the unique vocal features of individuals, such as pitch, timbre, and speaking style with voiceprints demonstrating a level of distinctiveness comparable to that of fingerprints, thereby establishing voice as a reliable biometric modality. Standard voice recognition systems operate by capturing audio samples, extracting distinctive features using digital signal processing techniques, and subsequently comparing these features to pre-enrolled voice templates for identity verification. Recent developments in machine learning and deep neural network architectures have markedly improved the precision and robustness of voice-based systems. Furthermore, voice authentication offers a contactless modality that is readily integrable into IoT devices equipped with microphones. This eliminates the requirement for physical interaction or sensor attachment, thereby enhancing usability and providing a more seamless, intuitive authentication experience [4, 5].

Cardiac signals offer a continuous, non-invasive modality for user authentication, presenting a seamless integration into

biometric security systems. Cardiac biometrics, particularly those derived from ECG and photoplethysmogram (PPG) signals, exploit the intrinsic electrical and hemodynamic characteristics of the human heart. These signals exhibit high individual specificity, serving as robust physiological identifiers.

Wearable technologies such as smart watches and fitness trackers embedded with ECG or PPG sensors facilitate the real-time acquisition of cardiac signals. Through the application of advanced signal processing and machine learning algorithms, distinctive biometric features are extracted to verify user identity, continuously.

The inherent complexity and uniqueness of cardiac waveforms render them exceedingly resistant to spoofing or replication. Unlike static biometrics (e.g., fingerprints or facial features), heart-based authentication enables persistent verification, ensuring that the legitimate user remains authenticated throughout system interaction rather than at a singular point of access.

This dual capability—resilience against impersonation and support for continuous verification—establishes cardiac biometrics as a promising approach for enhancing the security and reliability of modern authentication frameworks [6, 7].

The integration of vocal and cardiac signals in biometric authentication represents a promising strategy for enhancing both security and accessibility within IoT systems. These physiological modalities offer viable alternatives to conventional biometric techniques, particularly benefiting users with physical or cognitive impairments. By addressing the limitations of traditional systems and capitalizing on recent advancements in signal acquisition and processing, voice and heart-based biometrics can have the ability to foster more inclusive and secure IoT environments. This study aims to investigate and validate the effectiveness and inclusivity of employing vocal and cardiac signals as biometric identifiers within IoT-based authentication frameworks.

This paper makes several key contributions to the field of IoT authentication, with a focus on enhancing accessibility for individuals with disabilities, by addressing the following aspects:

• Emphasizing the importance of secure authentication methods in IoT systems for individuals with disabilities.

• Exploring the use of voice and ECG signals as viable modalities for access authentication.

• Introducing fuzzy systems to generate cancelable biometric templates for enhancing user privacy and biometric data security by transforming the original voice and ECG data into a non-reversible format. This transformation ensures that the original biometric data cannot be reconstructed, even if the templates are compromised.

The remainder of this paper is organized as follows. Section 2 provides an overview of cancelable biometric systems based on speech and ECG signals. Section 3 describes the proposed cancelable biometric system. Section 4 introduces the experimental results. Finally, Section 5 gives the conclusion of the paper.

2. RELATED WORK

Biometric revocability refers to the capability of canceling and reissuing biometric templates if they are compromised, as in resetting a password if it is exposed. In traditional biometric systems, a compromised biometric template poses a security risk, as it cannot be easily exploited in several applications. This vulnerability could allow indefinite misuse of the compromised templates. To moderate this risk, cancelable biometric systems transform the original biometric templates into secure, non-invertible ones, which are then stored and used for authentication. If a transformed template is compromised, a new template can be generated by applying a different transformation to the original one. Cancelable biometric systems must meet certain key requirements, as stated below [8].

Transformation: The original biometric data is subjected to a transformation process using a secure algorithm. This transformation is designed to be non-invertible, meaning that it should be computationally infeasible to retrieve the original biometric data from a transformed template.

Diversity: Different transformations can be applied to the same biometric data to generate multiple, distinct templates. This allows template revocation and reissuance, providing flexibility in case of compromise.

Security: The security of the system relies on the robustness of the transformation algorithm. The transformation should ensure that even if a transformed template is compromised, it should not provide useful information about the original biometric data.

Performance: The transformation should maintain the discriminating features of the biometric data, meaning that the transformed templates should still allow accurate identification and authentication of individuals.

In recent years, there has been a growing interest in research on cancelable biometric systems, with the goal of enhancing the security of biometric data and the privacy of users. The concept of cancelable biometrics has been explored across different biometrics, including voice and ECG signals. This section provides a comprehensive overview of some relevant work in the area of cancelable biometrics.

Cepstral coefficients are extensively utilized in speaker recognition systems due to their high efficacy in capturing the distinctive vocal characteristics of individuals. These coefficients are extracted from speech signals, and they serve as the primary features for speaker identification. Costantini et al. [9] applied both deep learning and traditional machine learning techniques for speaker recognition. They developed a custom CNN model and also utilized pre-trained architectures such as AlexNet and GoogleNet. The input speech signals were represented as either spectrograms or Mel-frequency cepstral coefficients (MFCC) graphs, in both colored and grayscale formats. The authors also extracted a comprehensive set of features, including spectral, cepstral, prosodic, and perceptual descriptors. They applied a correlation-based feature selection (CFS) method and used a naïve Bayes classifier for recognition. The results showed that the custom CNN trained on grayscale spectrograms achieves the highest recognition accuracy of approximately 90.15%**,** while AlexNet also performs competitively with 89.28% accuracy on spectrograms and 83.43% accuracy on MFCC inputs. The traditional naïve Bayes approach achieved an accuracy of around 87.09%.

Furthermore, El-Gazar et al. [10] introduced a secure cancelable biometric system by applying an optical encryption technique to speech spectrograms. Specifically, they employed a two-stage encryption process comprising optical scanning holography (OSH) followed by double random phase encoding (DRPE), utilizing two random phase masks (RPMs). This method resulted in an exceptionally low equal error rate

(EER) of 3.23×10^{-7}. Another trend depends on employing optical encryption techniques to convert speech spectrograms into secure biometric templates. In particular, El Shafai et al. [11] implemented a combination of the 3D Jigsaw transform and the fractional Fourier transform (FrFT) to enhance the security and non-invertibility of the biometric data. Their proposed approach demonstrated strong performance, achieving an EER of 0.0035 on the evaluated dataset. Despite the promising performance of cancelable biometric systems utilizing optical encryption techniques, these techniques introduce significant computational complexity and hardware dependency, making them less practical for real-time or lightweight IoT applications.

A cancelable speaker verification system was introduced based on a two-step process to enhance privacy and security. It depends on transforming traditional I-vectors into binary representations and then further obscuring them through a shuffling scheme [12]. This shuffling scheme involves rearranging the order of the bits in the binary I-vectors. The system achieved an EER of 0.08. Although this approach improves data privacy, the binarization process may reduce the discriminatory power of the features, and the system robustness under noisy or real-world conditions remains insufficiently evaluated.

Sakr et al. [13] utilized deep transfer learning to leverage pre-trained models on large datasets, enhancing the feature extraction process from ECG signals. The extracted features are then encoded using DNA and amino acid representations, which add an additional layer of security in order to build a robust cancelable biometric system. A support vector machines (SVM) classifier is employed for authentication. The system achieved an average EER of 0.04. Unofrtunately, combining deep learning with biological encodings (DNA, amino acids) adds a significant computational burden that is not ideal for real-time or IoT devices.

Yang et al. [14] introduced a cancelable ECG recognition system employing 3D chaotic logistic map encryption, characterized by efficient random behavior with confusion and diffusion properties that aid in generating secure ECG templates. They noted that while chaotic systems offer high security, their sensitivity to initial conditions could potentially affect stability under signal variations.

El-Moneim Kabel et al. [15] introduced a cancelable ECG recognition system based on signal separation. A 2×2 blind signal separation module is applied to each ECG biometric signal along with an audio signal, resulting in two minimally correlated distorted outputs. The induced distortions ensure that the templates cannot be reversed to their original forms. In this system, a simple XOR encryption step is performed using a unique key for each user. The system achieved an average EER of 0.134. Unfortunately, the utilization of blind source separation techniques with audio signals may inadvertently introduce the required level of distortion for efficient cancelable biometric system performance.

Kim and Chun [16] presented a cancelable ECG biometric recognition system using a generalized likelihood ratio test (GLRT) based on a composite hypothesis testing in the compressive sensing (CS) domain. The system was developed and tested with a random row permutation revocation mechanism for its resistance to different attacks. The system achieved a probability of detection of 93.0% and an EER of 4.8%. While CS-GLRT offers privacy, it may be sensitive to natural fluctuations in ECG signals due to physiological variability.

Barros et al. [17] introduced an ECG-based identification system based on sparse feature representations. User sparse feature patterns are subjected to similarity tests. In the recognition process, a regularization problem and a set of constraints are considered. The system relies on solving a regularization problem subject to a set of constraints during the recognition process, which can introduce significant computational complexity and limit the system feasibility for real-time applications.

Despite significant advancements in cancelable biometric systems using speech and ECG signals, current methods reveal several critical limitations that hinder their practical deployment in accessible, secure IoT environments. For instance, optical-encryption-based systems offer strong security through techniques like the 3D Jigsaw transform and FrFT. However, they rely heavily on complex computations and specialized hardware, making them not suited for real-time or resource-constrained IoT applications. Similarly, the system based on binary I-vector and bit-shuffling has some limitations. While promising in terms of template security, the conversion to binary format may reduce the ability of discrimination between users.

Although the combination of deep transfer learning with DNA and amino acid encoding is innovative, it suffers from high computational overhead and limited transparency in feature interpretation, which may complicate the IoT access process. In addition, the 3D chaotic encryption of ECG offers randomness and confusion, but it is often sensitive to small changes in initial parameters, which could degrade recognition stability and reproducibility. Moreover, the system based on blind signal separation between ECG and auxiliary signals creates sufficiently distorted templates, but at the cost of increased system complexity and possible degradation in signal fidelity.

Furthermore, the adoption of compressive sensing with GLRT in a cancelable ECG framework achieves reasonable performance metrics, but the system becomes vulnerable to physiological variability. In addition, reliance on compressive sensing may result in information loss under low SNR conditions. Notably, most of these methods also lack thorough analysis of real-world threats, such as replay attacks and environmental noise interference—factors that are particularly relevant for deployment in accessible IoT settings.

These gaps indicate a pressing need for a cancelable biometric framework that not only ensures high security and privacy but also addresses accessibility, adaptability to varying input quality, and practical usability in diverse real-world scenarios. The fuzzy-logic-based transformation approach proposed in this study aims to bridge this gap by offering a lightweight, non-invertible, and noise-resilient transformation method that maintains both recognition accuracy and user accessibility.

3. PROPOSED SYSTEM METHODOLOGY

An authentication system, particularly one using biometrics like voice or speech, typically involves several key stages to ensure secure and accurate identity verification. The main stages of a biometric authentication system are enrollment and authentication. The enrollment stage includes biometric acquisition, pre-processing, feature extraction, cancelable template generation, and template saving. During the authentication phase, a new biometric sample is captured,

preprocessed, features are extracted and a new template is generated in the same manner as that used in enrollment [10]. The newly generated biometric template is compared to the stored template(s) in the database to verify the user's identity. Similarity scores are calculated between the new template and the stored templates. A predefined threshold is used to decide if a similarity score indicates a matching. If the similarity score exceeds the threshold, the user is authenticated. Otherwise, authentication fails.

Cancelable template generation is designed to enhance the security of biometric data and the privacy of users by transforming the original biometric templates into different, non-reversible formats. This transformation ensures that if the template is compromised, it can be canceled and replaced without compromising the original biometric data. A fuzzy system is used to generate the cancelable templates. This system depends on fuzzy logic principles to get distorted templates from the original ones, while maintaining the uniqueness of the templates.

3.1 Methodology to generate cancelable templates

This section introduces the proposed framework for generating cancelable biometric templates. Fuzzy logic techniques are applied to the signals to introduce controlled levels of ambiguity [18-21], making the data less susceptible to direct interpretation. By fuzzifying signals, such as ECG signals, we can create secure, non-invertible templates, which in turn enhances user privacy. This fuzzification process plays a crucial role in obscuring exact values, enabling the generation of the cancelable and secure biometric templates that protect sensitive information from unauthorized access.

To generate a cancelable template, the following preprocessing and transformation steps will be applied to the biometric signal:

(1) Biometric signal normalization: The original signal is first normalized to convert its values to the range [0, 1]. This step involved min-max normalization as follows:

$$s_n = \frac{s - s_{min}}{s_{max} - s_{min}} \tag{1}$$

where, s_n is the normalized signal, s is the original signal, s_{min} is the minimum value of the original signal, and s_{max} is the maximum value of the original signal.

This scaling ensures that the signal is consistent for further processing and reduces variability across signals.

(2) Fuzzification level setting: A specific fuzzification level l is selected to control the degree of transformation applied to the biometric signal. This parameter can be adjusted to tailor the fuzziness introduced to the signal, impacting the balance between template security and signal integrity.

(3) Applying fuzzification (fuzzy modification): A triangular fuzzy membership function is used to modify the normalized biometric signal, leading to a fuzzified version of the original signal. This fuzzification is defined by the following equation:

$$\mu = 1 - e^{(-l * abs(s_n - 0.5))} \tag{2}$$

where, μ is the degree of the membership value. This step introduces a layer of obfuscation to the biometric signal by applying a transformation based on a triangular membership function, which attenuates minor variations around the central membership value (0.5). This transformation plays a vital role in producing a cancelable biometric template that preserves the signal discriminative characteristics, while enhancing security and resistance to attacks.

For the proposed cancelable biometric system, the triangular function is chosen for the following reasons:

• The triangular function is mathematically simple. It only involves basic arithmetic operations (addition, subtraction, division). This simplicity enables fast execution and requires minimal processing power, making the triangular function highly suitable for real-time applications and resource-constrained environments.

• Cancelable biometrics require the transformation to be non-invertible. Triangular functions help construct fuzzy systems that map biometric signals into regions, making it difficult for an attacker to retrieve the original data.

• In cancelable biometrics, one of the key goals is to achieve revocability and diversity, meaning the ability to generate multiple, unique templates from the same biometric data. This ensures that if one template is compromised, it can be revoked and replaced with a new one, without needing to recapture the user's biometric.

• The triangular membership function supports this by allowing flexible adjustments to its parameters, such as the base and peak points, which makes it easy to create alternative fuzzy encodings of the same biometric template. All obtained versions still represent the same identity but with different templates, enhancing both security and template revocability.

Generating the cancelable template: The final cancelable biometric template is generated by combining the original biometric signal with the fuzzified signal using an element-wise multiplication operation. The formula used is:

$$s_c = s_n * \mu * z \tag{3}$$

where, s_c is the cancelable template, and z is an additional noise factor, which can be random or predetermined, enhancing the template uniqueness and further complicating reversibility.

Correlation Measurement: To evaluate the similarity between two biometric templates, a correlation coefficient is computed. The correlation formula between two templates x and y is given as follows:

$$R_{xy} = \frac{C_v(x,y)}{\sigma_x \sigma_y} \tag{4}$$

where, C_v indicates the covariance between the templates. The variables σ_x and σ_y refer to the standard deviations of these templates.

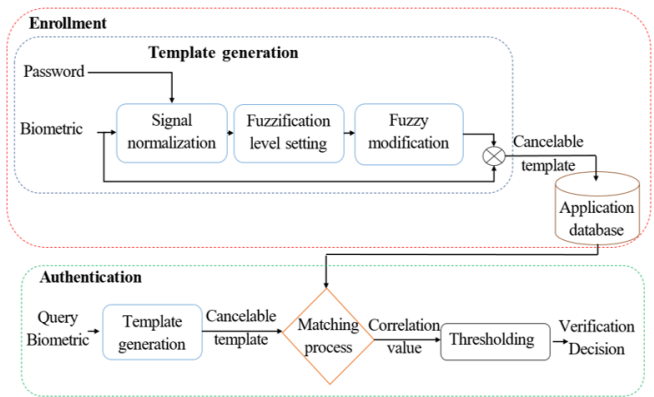


Figure 1. The proposed system block diagram

This system offers a structured approach to convert biometric signals into cancelable biometric templates, maintaining signal distinctiveness, while enhancing privacy. As shown in Figure 1, through normalization and fuzzification, the system effectively generates secure and non-invertible representations of biometric signals.

3.2 Fuzzification level setting

The fuzzification level can be determined using a password given by the user as follows:

The password is converted to an encrypted value using the MD5 message digest hash function algorithm.

The MD5 algorithm produces a 128-bit (16-byte) hash value, typically expressed as a 32-character hexadecimal number.

The MD5 begins with a 32-digit hexadecimal number which is converted to 128 bits. The first 32 bits of the 128 bits are used to obtain the MD5 initial values d_1, d_2, d_3 and d_4. Each of them is represented by 8 bits, and then the binary initial values are converted to decimal values. The initial value can be obtained using the following equation:

$$x_n = mod(d_1 \oplus d_2 \oplus d_3 \oplus d_4, 256)/255 \quad (5)$$

The obtained value is used as the logistic chaotic map initial value. This map is an iterative map expressed as follows:

$$x_{n+1} = \rho x_n (1 - x_n) \quad (6)$$

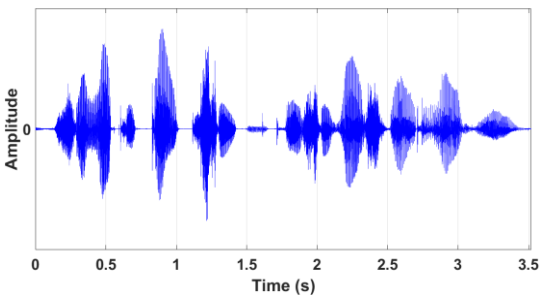
where, ρ is the logistic map control parameter. It can be set as 3.99999999.

Then, the fuzzification level can be obtained using the following equation:

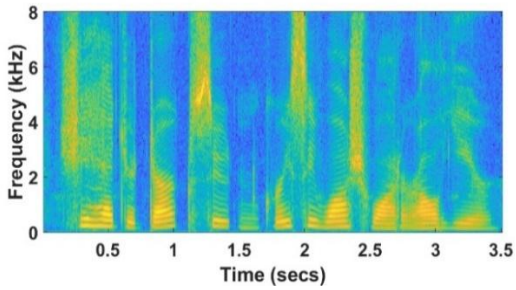
$$F_L = \lfloor x_{n+1} \times 5 \rfloor + 1 \quad (7)$$

4. SIMULATION RESULTS

This section presents the results of the proposed cancelable biometric system. The simulation experiments were performed on a workstation with an Intel 2.7 GHz processor, 16.00GB RAM, Windows 7, 64-bit operating system, and MATLAB R2018b. The proposed system has been applied to speech and ECG signals. The datasets used in the tests are the Texas Instruments (TI) Massachusetts Institute of Technology (MIT) for speech signal [22] and the ECG-ID database (ECGIDDB) [23]. The generated cancelable templates are one-dimension signals of 7200 samples. The average processing time for template generation is 0.5638 sec; and for the verification process, it is 1.77427 sec.

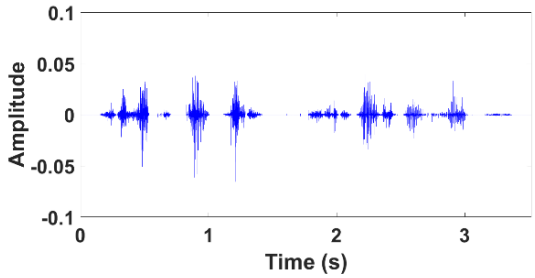


(a) Original speech signal

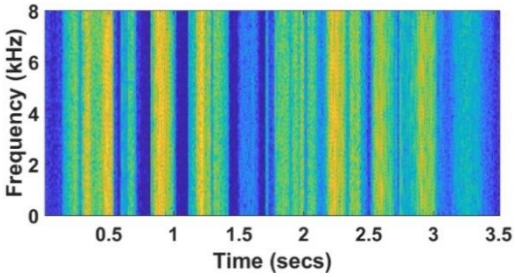


(b) Original speech spectrogram

Figure 2. Original speech signal and its spectrogram [24]

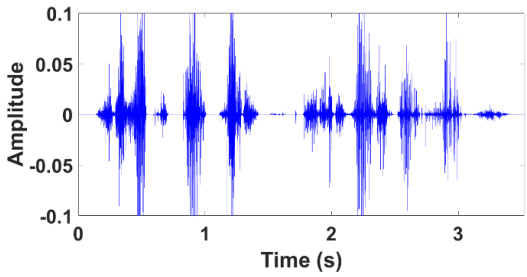


(a) Cancelable template

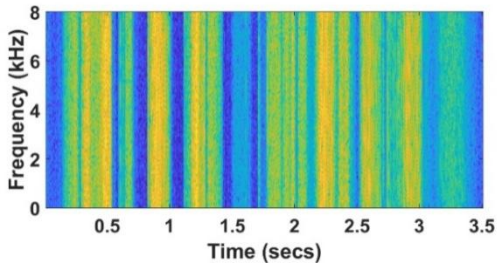


(b) Cancelable template spectrogram

Figure 3. Cancelable speech signal template and its spectrogram with the first fuzzification level having R_{xy} value equal to 0.0056

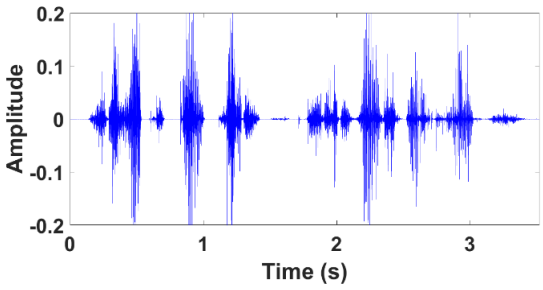


(a) Cancelable template

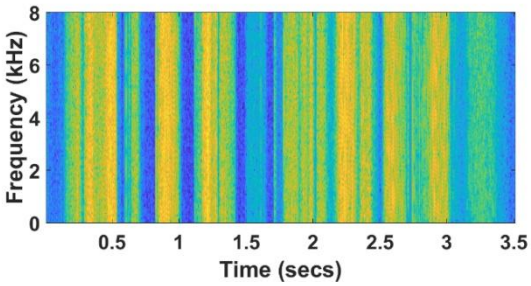


(b) Cancelable template spectrogram

Figure 4. Cancelable speech signal template and its spectrogram with the third fuzzification level having R_{xy} value equal to 0.0072



(a) Cancelable template



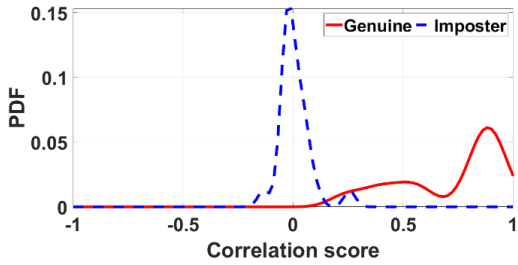
(b) Cancelable template spectrogram

Figure 5. Cancelable speech signal template and its spectrogram with the fifth fuzzification level having R_{xy} value equal to 0.0084

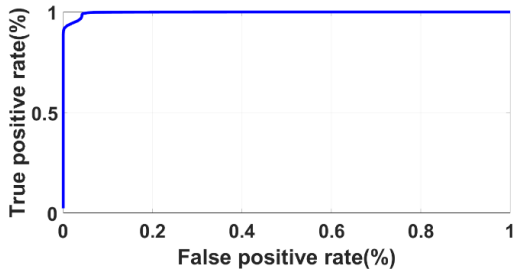
The proposed system depends on signal fuzzification to generate the cancelable templates. The correlation coefficient R_{xy} given in Eq. (4) is used to evaluate the correlation between the original and cancelable templates. The lower the R_{xy} is, the higher the cancelable template robustness. Figure 2 shows the original speech signal and its spectrogram. Figures 3-5 show the obtained cancelable templates at first, third, and fifth fuzzification levels for the speech signal, respectively.

In the authentication, the cancelable biometric template of the query user is generated using the same steps as in the enrolment. Then, it is compared to the templates that have been saved in the application database. The correlation values are compared with a threshold value to determine the authorized users. The threshold value is estimated as follows. Initially, a number of true tests is performed and the obtained correlation scores are regarded as random variable values. The probability distribution function (PDF) for the genuine test is estimated. Similarly, multiple tests are performed for fake users, and the correlation scores are obtained. The PDF of the imposter test is then estimated. The threshold value is determined at the point where the correlation distribution curves for the genuine and imposter tests meet together. Figure 6(a) shows the distribution curves for genuine and imposter tests for the proposed cancelable speaker identification system. It is clear that the threshold is at a correlation score equal to 0.18. This means that when the correlation value between the saved and query templates is larger than 0.18, the user is considered as an authorized user. Figure 6(b) shows the receiver operating characteristic (ROC) curve for the proposed system. This ROC curve is a graphical representation used to evaluate the system performance.

Figure 7 shows the original ECG signal template and its spectrogram. Figures 8-10 show the obtained cancelable templates at the first, third, and fifth fuzzification levels of the original ECG signal template, respectively. It is clear that the higher the fuzzification level is, the higher the correlation between original and obtained templates, and thus the greater the similarity between the original and the cancelable templates.

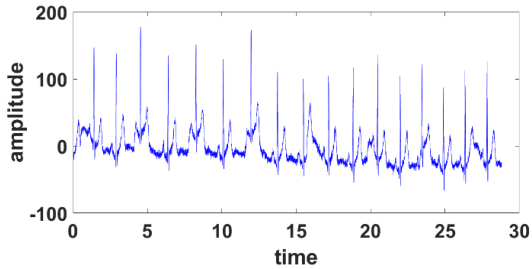


(a) PDFs for genuine and imposter tests

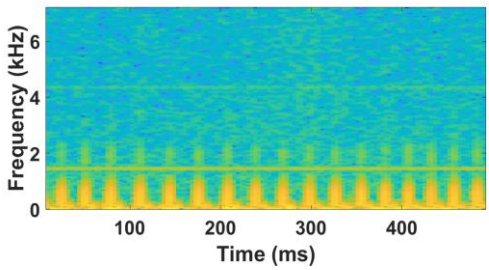


(b) ROC curve

Figure 6. PDFs for genuine and imposter tests and ROC curve for speech signals

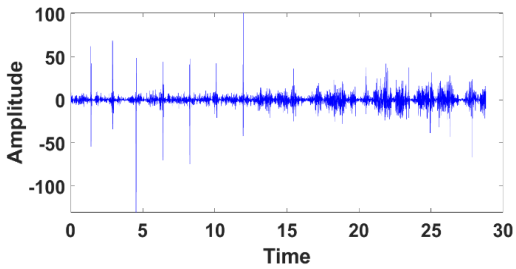


(a) Original ECG signal

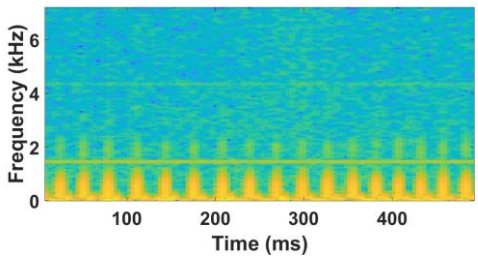


(b) Original ECG signal spectrogram

Figure 7. Original ECG signal and its spectrogram

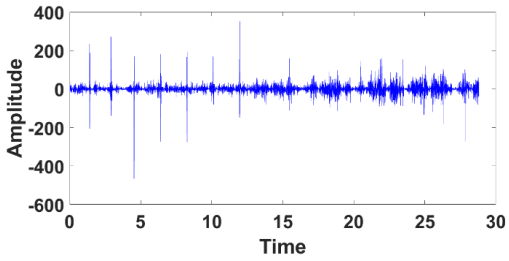


(a) Cancelable template

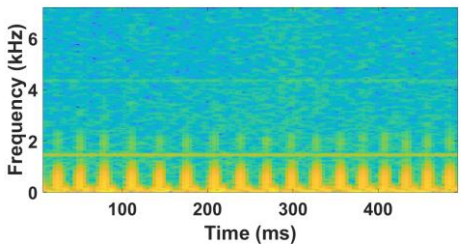


(b) Cancelable template spectrogram

Figure 8. Cancelable ECG signal template and its spectrogram with the first fuzzification level having R_{xy} value equal to 7.2141×10^{-4}

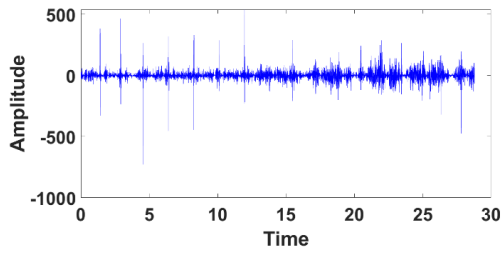


(a) Cancelable template

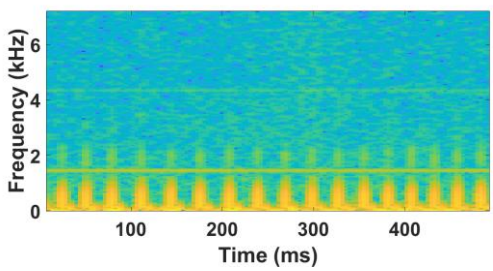


(b) Cancelable template spectrogram

Figure 9. Cancelable ECG signal template and its spectrogram with the third fuzzification level having R_{xy} value equal to 0.0058



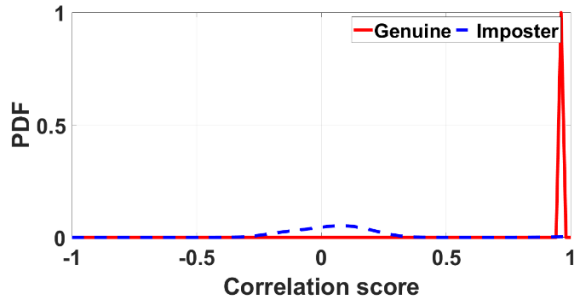
(a) Cancelable template



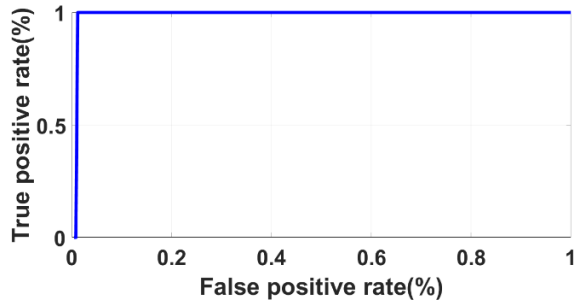
(b) Cancelable template spectrogram

Figure 10. Cancelable ECG signal template and its spectrogram with the fifth fuzzification level having R_{xy} value equal to 0.0.0098

Figure 11(a) shows the distribution curves for genuine and imposter tests on the cancelable ECG templates. The threshold value is considered as the midpoint between the distribution curves, and it can be estimated at a correlation score equal to 0.65. Figure 11(b) shows the ROC curve for the proposed system.



(a) PDFs of the genuine and imposter tests



(b) ROC curve

Figure 11. PDFs of genuine and imposter tests and ROC curve of the proposed system with ECG signals

Tables 1 and 2 give correlation values for imposter and genuine samples for the speech and ECG signals, respectively. Values given in the tables indicate that the genuine correlation values are around 0.8 and 0.9 for the speech and ECG signals, respectively, but the imposter correlation values are around 0.03 and 0.1 for the speech and ECG signals, respectively.

Table 1. Correlation scores for a cancelable speech signal template with true and false templates in the presence of AWGN at SNR equal to 10 dB

Speech Samples	R_{xy} with True Speech	R_{xy} with False Speech
Speech 1	0.8669	-0.0085
Speech 2	0.5208	0.0419
Speech 3	0.4301	0.0398
Speech 4	0.9749	0.0541
Speech 5	0.8592	0.0026

Table 2. Correlation scores for a cancelable ECG signal template with true and false templates in the presence of AWGN at SNR equal to 10 dB

ECG Samples	R_{xy} with True ECG	R_{xy} with False ECG
ECG 1	0.9537	-01664
ECG 2	0.9527	0.1255
ECG 3	0.9528	0.0340
ECG 4	0.9524	0.1388
ECG 5	0.9536	0.0445

System performance can be evaluated through numerical evaluation metrics such as EER, area under the ROC curve

(AROC), false acceptance rate (FAR) and false reject rate (FRR). Values of EER, FAR and FRR indicate the system error rate in the discrimination process between authenticated and unauthenticated users. So, they are better to be close to zero. The AROC summarizes the overall performance of the system, and it equals one for a perfect system. Table 3 gives the numerical values of the evaluation metrics in the presence of additive white Gaussian noise (AWGN) at different SNR values. The table indicates that the proposed system has a good performance in the presence of noise, where EER, FAR and FRR values are close to 0, while AROC values are close to 1.

Table 3. Numerical evaluation results for the proposed system

	SNR (dB)	EER	AROC	FAR	FRR
Speech	0 dB	0.0002	1	4.12×10^{-4}	1.3175×10^{-5}
	10 dB	0.0059	0.9973	0.0543	0.0070
	15 dB	0.023	0.8841	0.0779	0.1799
ECG	0 dB	0.0015	0.9903	0.0145	4.029×10^{-55}
	10 dB	0.0018	0.9941	0.0114	0
	15 dB	0.0015	0.9903	0.0145	4.029×10^{-55}

Table 4. Correlation scores between the original speech signal template and the corresponding cancelable template for different membership functions of fuzzification

Speech Samples	Triangular	Trapezoidal	Gaussian
Speech 1	0.0041	0.0116	0.0098
Speech 2	0.0113	-0.0054	-0.0136
Speech 3	0.0075	0.0043	0.0035
Speech 4	-0.0075	0.0336	-0.0498
Speech 5	0.0016	0.0241	0.0334
Processing time (Sec)	0.5638	2.2766	4.2217

Table 5. Correlation scores between the original ECG signal template and the corresponding cancelable template for different membership functions of fuzzification

ECG samples	Triangular	Trapezoidal	Gaussian
ECG 1	0.0098	0.0351	0.0289
ECG 2	-0.0025	0.0030	0.0066
ECG 3	0.0017	-0.0111	-0.0095
ECG 4	0.0211	0.0097	0.0124
ECG 5	0.0015	0.0139	0.0137
Processing time (Sec)	0.4782	2.3428	4.3112

Table 6. Numerical evaluation results for the proposed system with different membership functions of fuzzification in the presence of AWGN at an SNR equal to 10 dB

	Triangular		Trapezoidal		Gaussian	
	EER	AROC	EER	AROC	EER	AROC
Speech	0.0059	0.997	0.1033	0.4539	0.1016	0.4456
ECG	0.0018	0.994	2.6×10^{-36}	0.984	1.1×10^{-20}	0.995

Table 7. Comparison results between the proposed cancelable biometric systems and other state-of-the-art systems [10, 11, 13, 14]

Cancelable Biometric System	EER	AROC
Proposed system (speech)	0.0059	0.9973
Proposed system (ECG)	0.0018	0.9941
Ref [10]	1.95×10^{-20}	1
Ref [11]	0.0035	0.9958
Ref [13]	0.0044	
Ref [14]	0.134	

Different membership functions of fuzzification have been tested. System performance levels using trapezoidal and Gaussian functions have been compared. Tables 4 and 5 give the correlation scores between the original signal and the corresponding cancelable template using triangular, trapezoidal and Gaussian functions for the speech and ECG signals, respectively. It is clear from the tables that the triangular function gives the lowest correlation scores. In addition, it needs less processing times. Table 6 gives EER and AROC values using triangular, trapezoidal and Gaussian functions for the speech and ECG signals in the presence of AWGN with SNR equal to 10 dB.

Although trapezoidal function can achieve lower EER values compared to trangular function, it takes longer processing times, and this is not recommended in IoT applications. To ensure the effectiveness of the proposed cancelable biometric system, its results are compared to those of the recent state-of-the-art systems as given in Table 7.

5. CONCLUSION

In this paper, we have emphasized the critical importance of secure access to Internet of Things (IoT) systems, particularly for individuals with disabilities. We explored the use of speech and electrocardiogram (ECG) signals as biometric traits for authentication in the access process, leveraging their unique and stable characteristics to enhance both user convenience and security. A novel system has been introduced based on fuzzy logic processing to generate cancelable biometric templates. This is accomplished through transforming the original biometric data into a non-reversible format. This transformation ensures that even if the templates were compromised, the original biometric data could not be reconstructed. Fuzzy systems effectively handle variations and uncertainties in speech and ECG signals, while generating distorted versions form them. This feature enhances the system robustness to noise, signal variations, and fluctuations in the user's health status. Our proposed system for generating cancelable templates maintains high accuracy in biometric matching, while preserving user privacy. In conclusion, the adoption of cancelable templates generated using fuzzy systems for speech- and ECG-based authentication is a promising trend for future research and development.

ACKNOWLEDGMENT

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R138), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] Chanal, P.M., Kakkasageri, M.S. (2020). Security and privacy in IoT: A survey. Wireless Personal Communications, 115(2): 1667-1693. https://doi.org/10.1007/s11277-020-07649-9

[2] Sadhu, P.K, Yanambaka, V.P, Abdelgawad, A. (2022). Internet of things: Security and solutions survey. Sensors, 22(19): 7433. https://doi.org/10.3390/s22197433

[3] Abiodun, O.I., Abiodun, E.O., Alawida, M., Alkhawaldeh, R.S., Arshad, H. (2021). A review on the

security of the internet of things: Challenges and solutions. Wireless Personal Communications, 119(3): 2603-2637. https://doi.org/10.1007/s11277-021-08348-9

[4] Duraibi, S. (2020). Voice biometric identity authentication model for IoT devices. International Journal of Security, Privacy and Trust Management (IJSPTM), 9(1/2): 1-10. https://doi.org/10.5121/ijsptm.2020.9201

[5] Elshamy, E.M., Hussein, A.I., Hamed, H.F., Abdelghany, M.A., Kelash, H.M. (2021). Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem. Multimedia Tools and Applications, 80(7): 9877-9893. https://doi.org/10.1007/s11042-020-09986-0

[6] Bhuva, D.R. Kumar, S. (2023). A novel continuous authentication method using biometrics for IOT devices. Internet of Things, 24: 100927. https://doi.org/10.1016/j.iot.2023.100927

[7] Hammad, M., Iliyasu, A.M., Elgendy, I.A., Abd El-Latif, A.A. (2022). End-to-end data authentication deep learning model for securing IoT configurations. Human-Centric Computing and Information Sciences, 12: 4. https://doi.org/10.22967/HCIS.2022.12.004

[8] Bernal-Romero, J.C., Ramirez-Cortes, J.M., Rangel-Magdaleno, J.D.J., Gomez-Gil, P., Peregrina-Barreto, H., Cruz-Vega, I. (2023). A review on protection and cancelable techniques in biometric systems. IEEE Access, 11: 8531-8568. https://doi.org/10.1109/ACCESS.2023.3239387

[9] Costantini, G., Cesarini, V., Brenna, E. (2023). High-level CNN and machine learning methods for speaker recognition. Sensors, 23(7): 3461. https://doi.org/10.3390/s23073461

[10] El-Gazar, S., El Shafai, W., El Banby, G.M., Hamed, H., FA Salama, G.M., Abd-Elnaby, M., Abd El-Samie, F.E. (2022). Cancelable speaker identification system based on optical-like encryption algorithms. Computer Systems Science & Engineering, 43(1): 87-102. https://doi.org/10.32604/csse.2022.022722

[11] El Shafai, W., Elsayed, M.A., Rashwan, M.A., Dessouky, M.I., El-Fishawy, A.S., Soliman, N.F., Alhussan, A.A., Abd El-Samie, F.E. (2023). Optical ciphering scheme for cancellable speaker identification system. Computer Systems Science & Engineering, 45(1): 563-578. https://doi.org/10.32604/csse.2023.024375

[12] Mtibaa, A., Petrovska-Delacrétaz, D., Boudy, J., Ben Hamida, A. (2021). Privacy-preserving speaker verification system based on binary I-vectors. IET Biometrics, 10(3): 233-245. https://doi.org/10.1049/bme2.12013

[13] Sakr, A.S. Pławiak, P. Tadeusiewicz, R. Hammad, M. (2022). Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication. Information Sciences, 585: 127-143. https://doi.org/10.1016/j.ins.2021.11.066

[14] Yang, W.C., Wang, S., Hu, J.K., Tao, X.H., Li, Y. (2024). Feature extraction and learning approaches for cancellable biometrics: A survey. CAAI Transactions on Intelligence Technology, 9(1): 4-25. https://doi.org/10.1049/cit2.12283

[15] El-Moneim Kabel, S.A., El-Banby, G.M., Abou Elazm, L.A., El-Shafai, W., El-Bahnasawy, N.A., El-Samie, F.E.A., Elazm, A.A., Siam, A.I., Abdelhamed, M.A. (2024). Securing internet-of-medical-things networks using cancellable ECG recognition. Scientific Reports, 14(1): 10871. https://doi.org/10.1038/s41598-024-54830-2

[16] Kim, H., Chun, S.Y. (2019). Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test. IEEE Access, 7: 9232-9242. https://doi.org/10.1109/ACCESS.2019.2891817

[17] Barros, A., Resque, P., Almeida, J., Mota, R., Oliveira, H., Rosário, D., Cerqueira, E. (2020). Data improvement model based on ECG biometric for user authentication and identification. Sensors, 20(10): 2920. https://doi.org/10.3390/s20102920

[18] Ross, T.J. (2010). Fuzzy Logic with Engineering Applications. John Wiley & Sons. https://doi.org/10.1002/9781119994374

[19] Klir, G., Yuan, B. (1995). Fuzzy Sets and Fuzzy Logic: Theory and Applications. Prentice Hall. https://dml.cz/bitstream/handle/10338.dmlcz/124175/Kybernetika_32-1996-2_8.pdf.

[20] Chaira, T. (2015). Medical Image Processing: Advanced Fuzzy Set Theoretic Techniques. CRC Press. https://doi.org/10.1201/b18019

[21] Zadeh, L.A. (1999). Fuzzy sets as a basis for a theory of possibility. Fuzzy Sets and Systems, 100: 9-34. https://doi.org/10.1016/S0165-0114(99)80004-9

[22] Voice Biometrics: The Essential Guide. https://www.phonexia.com/knowledge-base/voice-biometrics-essential-guide/, accessed on Mar. 23, 2022.

[23] ECG-ID Database. https://physionet.org/content/ecgiddb/1.0.0/, accessed on Sep. 19, 2022.

[24] Singh, M.K. (2024). Feature extraction and classification efficiency analysis using machine learning approach for speech signal. Multimedia Tools and Applications, 83(16): 47069-47084. https://doi.org/10.1007/s11042-023-17368-5

NOMENCLATURE

s	Original signal intensity
s_{max}	Signal maximum intensity
s_{min}	Signal minimum intensity
l	Fuzzification level
z	Additional noise factor
R_{xy}	Correlation cooficient
C_v	Covariance between two templates
x	A biometric template, whether normal or cancelable
y	A biometric template, whether normal or cancelable
x_n	Logistic map initial value

Greek symbols

μ	Fuzzified version of the original signal
σ_x	Standard deviation of template *x*
σ_y	Standard deviation of template *y*
ρ	Logistic map control parameter