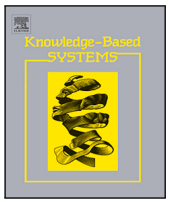
Knowledge-Based Systems 316 (2025) 113326

Contents lists available at ScienceDirect

Knowledge-Based Systems

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



A novel dictionary attack on ECG authentication system using adversarial optimization and clustering

Bonan Zhang [a,*], Lin Li [c], Chao Chen [a], Ickjai Lee [b], Kyungmi Lee [b], Tianqing Zhu [d], Kok-Leong Ong [a]

[a] RMIT, 124 La Trobe St, Melbourne, 3000, VIC, Australia
[b] James Cook University, 1 James Cook Dr, Townsville, 4814, QLD, Australia
[c] Southern Cross University, Gold Coast Airport, Gold Coast, 4225, QLD, Australia
[d] City University of Macau, Avenida Padre Tomás Pereira Taipa, 999078, Macao Special Administrative Region of China

ARTICLE INFO

Keywords:
ECG
Biometric
Authentication
Security

ABSTRACT

Electrocardiogram(ECG)-based biometric authentication has become a promising method to improve security in wearable devices due to its inherent uniqueness and difficulty to replicate. However, no studies currently demonstrate that ECG authentication can resist modern attack techniques employed against biometric authentication. In this paper, we present a novel dictionary attack against ECG authentication systems, which poses a significant threat. In contrast to conventional targeted attacks, this approach utilizes random pairing to breach a vast number of users, without requiring specific information about their biometric data. Our approach leverages adversarial optimization and clustering to generate synthetic ECG waveforms capable of bypassing authentication mechanisms of various systems, revealing critical vulnerabilities in the current implementation of ECG-based biometrics. We comprehensively evaluate the effectiveness of this attack across different ECG authentication models, demonstrating that despite the intrinsic uniqueness of ECG signals, a substantial number of users are vulnerable. Our attack method can bypass the authentication system of an average of 20% of users even at the most stringent false acceptance rate of 1%. With up to five attack attempts allowed, our method can bypass up to 62% of users' ECG authentication models.

1. Introduction

Biometric authentication has become the cornerstone of modern security systems due to its convenience and seamless integration. In particular, the use of biometric technology in mobile devices has greatly improved the user experience [1]. Unlike traditional methods such as passwords or PINs, biometric authentication offers enhanced security through traits that are inherent and difficult to replicate. Fingerprint recognition [2] and facial recognition [3] have become the most common authentication methods for current smart devices. Following extensive research over several years, both methods have been thoroughly validated regarding their authentication accuracy. Consequently, both approaches have gained widespread acceptance and utilization by the public. Nevertheless, incorporating fingerprint sensors or cameras into smartwatches and other wearables to support both authentication schemes poses challenges due to hardware limitations. Wearable devices, however, maintain proximity to the user's skin and gather physiological data about them. This permits applications like gait authentication [4], voice authentication [5], PPG authentication [6], and ECG authentication [7]. This research will mainly focus on ECG authentication.

User authentication via ECG signals offers unique advantages over other biometric modalities. The ECG records the heart's electrical activity, which is affected by the person's anatomical structure and physiological state, producing distinct and stable patterns over time [8]. ECG signals, in contrast to external biometrics, are dynamic and internal, which makes them challenging to duplicate or record without the individual's awareness. This intrinsic security reduces the risk of spoofing attacks. In addition, ECG-based authentication can be continuously monitored, providing continuous and seamless verification without active user participation [9]. This is particularly advantageous in environments with high security requirements or applications necessitating continuous authentication. Moreover, advancements in wearable technology have greatly enhanced the accessibility of acquiring ECG signals. Devices including smartwatches, fitness trackers, and

* Corresponding author.
E-mail address: bonan.zhang@rmit.edu.au (B. Zhang).

https://doi.org/10.1016/j.knosys.2025.113326
Received 26 December 2024; Received in revised form 5 March 2025; Accepted 9 March 2025
Available online 20 March 2025

specific medical wearables incorporate sensors that can acquire high-quality ECG data [10]. These devices detect the electrical activity of the heart through electrodes placed on the skin, which are then digitized and used for authentication of identity.

Although ECG-based authentication offers several promising security features, it is not entirely immune to presentation attacks, particularly those originating from external sources like replay attacks [11,12]. An attacker can break into a user's authentication system by stealing a fragment of the user's ECG signal and replaying this ECG fragment through an oscilloscope. However, two key assumptions are required to implement the replay attack: firstly, the attack is targeted at a specific user; and additionally, that the adversary possesses access to the user's ECG segment. The implementation of this attack approach encounters numerous technical challenges.

In this paper, we introduce a novel attack on the ECG authentication system. Our strategy, unlike conventional targeted attacks, does not target a specific individual. The scheme relies on pure chance matching to breach the authentication system of a significant portion of users without prior information about the victim. This method can be used to gain access to any stolen wearable devices. Our approach adversarially optimizes ECG signal samples for different authentication protocols. The attack poses a new threat to ECG authentication methods.

Recent studies have shown that dictionary attacks can effectively target biometric authentication systems, including fingerprint recognition [13], facial recognition [14], and speech recognition [15,16]. The theoretical basis of dictionary attacks is derived from the biometric menagerie, which categorizes users based on the authentication performance of their biometric data. According to this theory, the majority of users exhibit significant biometric differences from others. However, there are 'wolf' users whose biometrics can easily match with those of others, and 'lamb' users whose biometrics are easily matched by others [17]. The goal of a dictionary attack is to exploit this phenomenon by generating biometric examples that can match as many user templates as possible. This method could significantly influence the security of biometric authentication systems through its integration with evolving generative machine learning techniques.

In this paper, we comprehensively evaluate the impact of dictionary attacks on ECG authentication. The contributions of this paper are as follows.

- We propose a novel clustering-based dictionary attack method targeting ECG authentication, which leverages the similarity of ECG embedding features to achieve adversarial optimization.
- Through experiments, we demonstrate that this attack exhibits strong generalization capabilities against unseen user features. It can bypass the authentication of most users, even when facing state-of-the-art ECG recognition systems.
- Our experiments show that the ECG embedding features extracted through CNN architectures exhibit clustering characteristics among different users. This makes their authentication models highly susceptible to attacks targeting specific user groups.

The remainder of the paper is structured as follows. Section 2 reviews related work, including the implementation of ECG-based authentication methods and dictionary attacks against biometric authentication. Section 3 details the implementation of our attack scheme. Section 4 presents the details of the experimental setup. In Section 5, we evaluate the effectiveness of our proposed scheme. In Section 6, we summarize our work and discuss future directions.

2. Related work

In this section, we will summarize the existing ECG authentication schemes and the attack threats they face. This section will be divided into three subsections. First, we introduce the main ECG authentication schemes currently in use; second, we introduce the existing attack methods designed against ECG authentication. The last section presents the existing dictionary attack methods against biometric authentication.

2.1. ECG authentication modeling

ECG signals are used mainly to show the electrical changes that occur in the human heart. They are collected by placing electrodes on the body. Fig. 1 illustrates changes in cardiac voltage during a heartbeat cycle. Within a single heartbeat cycle, its waveform can be divided into five waves. Within a single cardiac cycle, the waveform can be divided into five waves. Atrial depolarization produces P waves; ventricular depolarization produces QRS wave clusters; and ventricular repolarization produces T waves [18]. To improve diagnostic accuracy in medical settings, electrodes are normally required to be placed in all 12 lead ECG configurations on the patient's body. Thanks to advances in wearable technology, modern devices, such as smartwatches and fitness trackers, are now capable of acquiring high-quality ECG signals. This advancement enables the establishment of ECG certification programs for these wearable devices [19].

Differences in lifestyle habits and heart weights between individuals result in significant variations in ECG signals, which contribute to their uniqueness [10]. Authentication models leverage the distinctive statistical properties of ECG waveforms to effectively identify or verify users. Compared to conventional methods like fingerprint and facial recognition, ECG authentication offers unique advantages. It is difficult to steal a user's heart template and it also enables continuous authentication. For fingerprint and facial recognition, attackers can obtain victim biometric information relatively easily using high-resolution cameras and other tools [20]. However, with ECG authentication, unless the attacker has direct physical contact with the victim, it is extremely difficult to obtain their ECG signal. This inherent difficulty in obtaining the signal significantly enhances the security of ECG-based authentication. In addition, ECG signals can be collected passively through electrodes, without requiring active user participation. This allows continuous verification, ensuring that the device user remains consistent over time [9].

The first ECG-based biometric authentication method was proposed in 2001 [21]. During the past two decades, a substantial amount of literature has explored how to design various authentication schemes [22,23]. These schemes typically consist of the following components: filtering, segmentation, feature extraction, and template matching. Upon acquiring ECG signals through electrodes, the system initially employs a pre-established filtering model to eliminate noise from the signal. Subsequently, the ECG is divided into various segments corresponding to the heartbeat cycle. The features are then extracted individually from each segment. In the registration phase, features from multiple heartbeat cycles are aggregated and stored as the user's template. During authentication, the input signal undergoes filtering, segmentation, and feature extraction, then is compared to the stored template. A matching algorithm determines whether the test template sufficiently matches the registered template to verify the user's identity [10].

In an authentication model, two fundamental tasks are identification and verification [24]. Identification aims to determine the user associated with a given heartbeat signal by comparing it to registered ECG samples. Meanwhile, the verification task seeks to confirm whether the input signal corresponds to the user's declared identity.

The current state-of-the-art ECG authentication models are mainly implemented using Deep Neural Networks (DNNs). Compared to traditional machine learning methods, DNN models often achieve better performance due to their ability to automatically learn complex features from ECG signals. For closed-set identification tasks, DNNs are trained as classifiers to recognize user identities. In open-set verification tasks, the DNN's classification head is discarded and features are extracted from its intermediate layers to represent the signal. Verification is then achieved by comparing the features of the registered template with those of the input signal.

During the enrollment phase, multiple heartbeat cycles of the user's signal are typically required to generate a template. There are two strategies for template generation: using the average of the registered signal features as the template or saving all feature templates of the registered signals. Generally, using the average embedding yields better performance, making it a more popular choice.

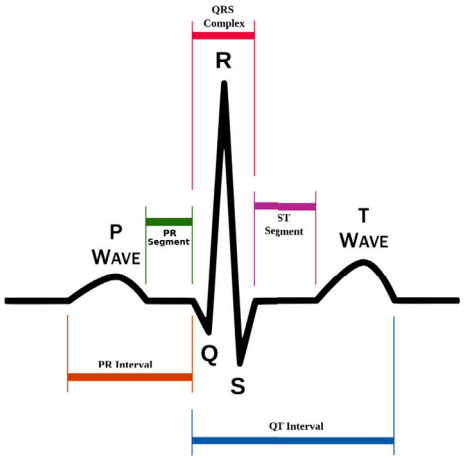


Fig. 1. An example of an ECG cycle.

2.2. Adversarial attack in ECG

Adversarial attacks were first proposed in the field of computer vision, where subtle, imperceptible perturbations are added to images to influence the model's prediction results. In the field of ECG authentication, existing adversarial attacks primarily focus on cross-device or cross-signal presentation attacks. Both of these methods assume that the attacker has access to the victim's biometric signals.

In cross-device attack scenarios, it is assumed that the attacker can obtain part of the victim's ECG signal, possibly by stealing medical records. However, ECG signals collected from different devices often vary significantly due to differences in sensor quality or electrode placement, making it difficult for attackers to directly use stolen signal fragments. To carry out the attack successfully, the attacker must first construct an equation for converting ECG signals between different devices, allowing the stolen signal to be transformed into one recognizable by the authentication device. Simone et al. [11] first proposed a method to construct a transformation equation for ECG cross-device attacks. Nima et al. [12] improved this method by refining the transformation equation, resulting in better cross-device compatibility. They also introduced a mitigation strategy analyzing heart rate variability to determine if the ECG signal originates from a real person, as heart rate variability is difficult to replicate artificially.

Cross-signal attacks, recently introduced, are a novel approach that does not require attackers to have access to the victim's ECG fragments Instead, attackers have access to user's cardiovascular bio-signals related to ECG, such as PPG (Photoplethysmogram), BCG (Ballistocardiogram) or SCG (Seismocardiogram) signals, which are all generated by heart activity. Among these signals, the PPG is the simplest to acquire. Attackers can acquire PPG signals without direct contact with the victim, even through methods like video recording. Afterwards, the attacker can build a generative model to convert these signals into ECG signals that can be used to attack authentication devices. Veena et al. [25] demonstrated that cross-signal attacks could successfully bypass ECG authentication with a success rate of over 50% within 10 attempts.

These techniques, whether they are cross-device or cross-signal attacks, are aimed at a particular user. Executing these attacks requires the attacker to establish either direct or indirect contact with the victim to obtain their biometric signals, significantly increasing the complexity.

In our proposed attack method, the attacker can execute the attack without any prior information about the victim. This approach is a non-targeted dictionary attack, meaning it does not focus on a specific individual, fundamentally distinguishing it from traditional adversarial methods.

2.3. Dictionary attack in biometrics

Dictionary attacks were originally used to decrypt user passwords through brute force methods, leveraging pre-existing knowledge to bypass authentication. Historically, this method has been primarily used to break common passwords composed of easily guessed words. However, recent research has investigated its possible use in other areas of authentication [5,13,14]. In biometric authentication, dictionary attacks are fundamentally different from spoofing attacks such as presentation attacks. Dictionary attacks do not require specific information about the target; instead, they rely on accidental matches across a large user base.

In the context of biometric authentication, the prior knowledge used for dictionary attacks comes from the concept of "biometric menagerie". If attackers identify biometric data with a high likelihood of matching others, they can build an effective attack dictionary [17]. Moreover, the implementation of biometric authentication systems typically involves a compromise between security and usability, which may elevate the risk of successful dictionary attacks.

The feasibility of dictionary attacks in biometric authentication was first demonstrated in fingerprint recognition [13]. Subsequent research demonstrated that facial recognition [14,26] and voice recognition [5] face similar threats. The typical approach begins by selecting the fingerprint with the highest impostor success rate. Subsequently, an algorithm for first-order hill climbing was employed to incrementally enhance the 'master fingerprint' enabling it to bypass an increased number of users' fingerprint authentication mechanisms. A significant limitation of this approach is its susceptibility to becoming trapped in local optima [13].

In recent years, with the advancement of generative models such as GANs, more dictionary attack methods have used generated biometric signals for attacks. These generative models overcome the limitations of traditional optimization by producing more versatile biometric data, making attacks more effective across a broader user base.

3. Attack strategy and framework

In this section, we discuss the construction of ECG authentication systems using DNNs, along with the attack model we developed. The overview of the proposed framework we designed is illustrated in Fig. 2. The process is divided into four parts. First is the preprocessing of the ECG signal, where the noise is removed and the signal is segmented according to the heartbeat cycle. The second step involves training a CNN model and discarding the classification head to extract embedded features. In the third step, a clustering method is used to select the dataset for optimization and to choose the seed signals to be optimized. The final step involves adversarial optimization of the seed signals to increase the success rate of impersonation. The specific details of each step will be elaborated in the following subsections.

3.1. DNN ECG certification process

Most DNN-based ECG authentication models extract embedded features by analyzing ECG signals from a single heartbeat cycle. This study adopts a similar approach for model construction. The construction of the authentication model is divided into two parts: feature extraction and registration template generation. We will offer comprehensive elucidations of the implementation of each component.

3.1.1. Extract embedding feature

During the signal acquisition phase, a continuous ECG signal from the user is gathered to either generate the registration template or perform authentication. Initially, the ECG signal is divided into ECG fragments of equal length according to the heartbeat cycle. Following the segmentation, each fragment is normalized using the z-score method. The fixed-length ECG embedded features from each fragment

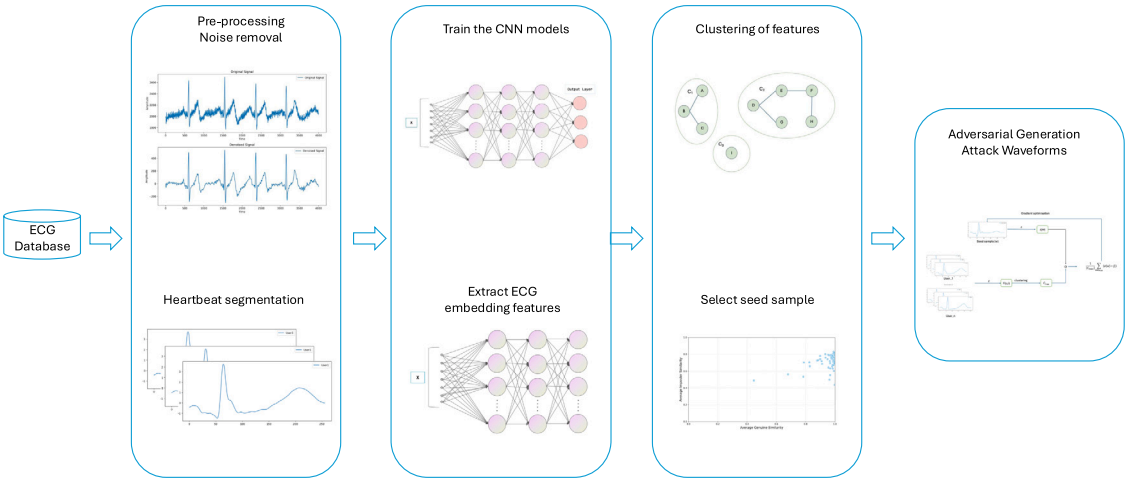


Fig. 2. Overview of the proposed framework.

are then extracted using a pre-trained encoder. The entire process can be represented by the following equations:

$$W \rightarrow \{w_i\}_{i=1}^{N}, \tag{1}$$

$$\hat{w}_i = \frac{w_i - \mu(w_i)}{\sigma(w_i)}, \tag{2}$$

$$\hat{w}_i \xrightarrow{\mathcal{E}} f(\hat{w}_i), \tag{3}$$

where W is the original ECG signal, and w_i represents each segmented ECG fragment. $\mathcal{E}$ represents an ECG encoder trained on waveforms and f is the embedding feature extracted from the ECG segment.

The model $\mathcal{E}$ is generally pre-trained on an ECG dataset to develop a fully supervised ECG signal classification model. Once training is complete, the classification head is removed and the earlier layers are used to extract ECG embedding features.

3.1.2. Enrollment and verification strategy

During the enrollment phase, the system collects multiple ECG signal segments from the user, extracts their corresponding embedding features, and stores them as an authentication template $F = f_i$, where i represents the index of consecutive samples. Each user takes the same number n of ECG fragments during the enrollment phase to generate the template. During the verification process, the system compares the features extracted from the input signal with the features of the registered template to determine whether the input signal belongs to the registered user.

$$v_{\rho,\tau}(W_t, F) := v_{\rho,\tau}(\mu(f_t), F) \rightarrow \{0, 1\}, \tag{4}$$

where W_t represents the input ECG signal to be verified. For most models, using a single heartbeat cycle is insufficient to achieve good performance, and multiple heartbeat cycles are typically needed for authentication. Therefore, the input ECG signal is segmented again according to the heartbeat cycle, and embedded features are extracted from each segment. f_t denotes the corresponding generated embedded features. The verification process, represented as $v_{\rho,\tau}$, involves comparing the mean of the features f_t with the stored template.

The authentication process can employ various scoring schemes ρ and thresholds τ, depending on the configuration of the model. In this study, we chose two widely used scoring strategies for our experiments: the Any-n strategy and the Avg-n strategy.

Any-n strategy: This approach involves comparing the features obtained from the input ECG signal with the embedded features of the n registered signals. Authentication is regarded as successful if any feature pair exhibits a similarity that exceeds the threshold. The aim of this approach is to identify at least one strong match between the input and stored signals.

Avg-n strategy: This method assesses the similarity between the features extracted from the input signal and the mean embedded features of all n registered signals. When the similarity score reaches or exceeds the set threshold, authentication is deemed successful. This method evaluates the overall consistency of the input signal with the template.

$$v_{any,\tau}(\mu(f_t), F) := \text{any}\left(\mu(f_t) \circ f_i > \tau \mid i = 1, \ldots, n\right), \tag{5}$$

$$v_{avg,\tau}(\mu(f_t), F) := \mu(f_t) \circ \mu(F) > \tau. \tag{6}$$

In this context, $\mu(f_t) \circ f_i$ denotes the computation of the similarity between the two features. The method for determining similarity will also differ based on the model configuration.

3.2. Dictionary attack method

Unlike traditional user-specific spoof attacks, the goal of a dictionary attack is to bypass the authentication system of a broad set of users. In this context, the goal is to identify a master ECG waveform sample w_m capable of bypassing the ECG authentication systems for most users. For a total of N users, the formula for finding the master ECG waveform can be represented as follows:

$$\arg\max_{w} \sum_{n=1}^{N} \left[v_{\rho,\tau}(w, F_n)\right]. \tag{7}$$

When the attacker is allowed multiple authentication attempts, the dictionary attack can be expanded by creating a collection of master ECG waveforms. This collection, or "dictionary", enhances the likelihood of successful attacks. The following equation describes the process for developing a dictionary of master ECG waveforms:

$$\arg\max_{\{w_k\}_{k=1}^{M}} \sum_{n=1}^{N} \left[v_{\rho,\tau}(w_1, F_n) \vee \ldots \vee v_{\rho,\tau}(w_k, F_n)\right]. \tag{8}$$

When multiple attacks are allowed, the attacker can independently optimize each master waveform. By selecting distinct user groups for training each master waveform, the attacker can improve the success rate of circumventing authentication. This approach makes each master waveform suitable for a specific subset of users, which can effectively improve the breakthrough success rate.

Rather than optimizing a single waveform for the entire user base, the attacker segments the users into groups. Each waveform is then optimized for a specific subset, thereby increasing the overall success rate of the dictionary attack. Once the waveforms are generated, we

assess the impostor effect of each one and compute the impostor matrix. First, we construct a matrix of size $M \times N$, where N is the number of users in the database and M is the number of generated ECG waveform segments. If waveform w_m is able to successfully spoof the authentication model of user n, the matrix entry at position (m, n) is set to 1; otherwise, it remains 0. The formula for calculating the impostor matrix is as follows:

$$\mathbf{B}_{M\times N} = \begin{bmatrix} v_{\rho,\tau}(w_1, F_1) & \cdots & v_{\rho,\tau}(w_1, F_N) \\ \cdots & \cdots & \cdots \\ v_{\rho,\tau}(w_M, F_N) & \cdots & v_{\rho,\tau}(w_M, F_N) \end{bmatrix}. \tag{9}$$

Using this matrix, we can calculate the impostor success rate, which measures how effective each ECG segment in the dictionary is at spoofing users. The impostor success rate for a segment is defined as the proportion of users that the segment can successfully spoof. The formula for calculating the success rate of the impostor for a segment w_m is as follows:

$$\mathrm{IR}(w_m) = \frac{1}{|N|} \sum_{n\in N} v_{\rho,\tau}(w_m, F_n). \tag{10}$$

3.3. Attack implementation

In the practical application of the attack, our goal is to execute adversarial optimization against the targeted algorithm in order to create a master ECG waveform capable of circumventing the authentication models for the largest possible number of users.

In this research, our attack focuses on users who are more easily matched by others. Initially, we implement connected components clustering using cosine similarity to group user ECG datasets, which are utilized for optimizing the master waveform. Subsequently, we choose the cluster that contains the highest number of users to direct our optimization efforts for the adversarial waveform. The comprehensive procedure and mathematical formulation are detailed below:

- Computation of Cosine Similarity: The cosine similarity between each pair of user ECG feature vectors f_i and f_j is determined by employing:

$$\mathrm{CosSim}(f_i, f_j) = \frac{f_i \cdot f_j}{\|f_i\|\|f_j\|}. \tag{11}$$

- Build Adjacency Matrix: Based on the cosine similarity scores, an adjacency matrix is created by applying the threshold θ.

$$A_{ij} = \begin{cases} 1 & \text{if } \mathrm{CosSim}(f_i, f_j) > \theta \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

- Connected Components Clustering: With the adjacency matrix A, we determine the connected components within the graph. Each connected component signifies a set of users whose ECG features exhibit high similarity.
- Cluster Selection: Once the clusters are identified, we choose the cluster $C_{\max}$ that encompasses the greatest quantity of ECG fragments.

$$C_{\max} = \arg\max_k |C_k|, \tag{13}$$

where $|C_k|$ represents the number of users in cluster C_k.

In our approach to waveform optimization, we drew upon the methodology introduced by Mirko et al. [16], employing Stochastic Gradient Descent (SGD) to conduct adversarial optimization of the ECG waveform. By using the optimized cluster C_{max} selected in the previous step, adversarial optimization of the master ECG waveform is performed. The purpose of the optimization is to enhance the average similarity between the embedded features of the master ECG waveform and those of the users in $C_{\max}$. The optimization objective can be expressed as follows:

$$\arg\max_w \frac{1}{|C_{\max}|} \sum_{i\in C_{\max}} (\mathcal{E}(w) \circ f_i). \tag{14}$$

In Fig. 3, we present the implementation process of our attack. The overall procedure can be segmented into the following stages. Initially, a seed ECG waveform sample w_0 is chosen. Subsequently, the embedding feature of this seed sample is computed using the ECG encoder $\mathcal{E}$. The succeeding step involves computing the average similarity between the seed's feature and the embedded features of the optimization group C_{max}. Thereafter, optimization of the seed waveform is performed according to the gradient of the similarity score. The update mechanism generally adheres to the following equation:

$$v_{t+1} = v_t + \eta \nabla_v \frac{1}{|C_{\max}|} \sum_{i\in C_{\max}} (\mathcal{E}(G(w_0, v_t)) \circ f_i), \tag{15}$$

$$w_* = G(w_0, v_t), \tag{16}$$

$$G(w, v) = w + v. \tag{17}$$

Algorithm 1 ECG Master Waveform Optimization

Input: User features $f_1, \ldots, f_n$, threshold θ, seed waveform w_0, learning rate η, iterations T
▷ Step 1: Compute Cosine Similarity
for each pair (f_i, f_j) **do**
  $S[i][j] \leftarrow \mathrm{cosine\_similarity}(f_i, f_j)$
end for
▷ Step 2: Build Adjacency Matrix
for each element $S[i][j]$ **do**
  if $S[i][j] >= \theta$ **then**
    $A[i][j] \leftarrow 1$
  else
    $A[i][j] \leftarrow 0$
  end if
end for
▷ Step 3: Connected Components Clustering
Identify clusters $C_1, \ldots, C_k$ using A
▷ Step 4: Cluster Selection
$C_{\max} \leftarrow \arg\max_k |C_k|$
▷ Step 5: Waveform Optimization
Initialize $v_0 \leftarrow 0$
for $t = 0$ to T **do**
  $g \leftarrow \frac{1}{|C_{\max}|} \sum_{i\in C_{\max}} \nabla_v (\mathcal{E}(G(w_0, v_t)) \circ f_i)$
  $v_{t+1} \leftarrow v_t + \eta \cdot g$
end for
Output: Optimized waveform $w_* \leftarrow G(w_0, v_T)$

The procedure of our optimization algorithm is shown in Algorithm 1. The objective of our attack is to identify adversarial waveforms within the waveform domain. The function $G(w, v)$ is responsible for generating waveforms based on the attack vector v. The attack initiates with a seed ECG sample, followed by optimization via the addition of the attack vector to the initial waveform.

4. Experimental setup

This section will provide a comprehensive overview of experimental datasets, ECG authentication schemes, and the methodology for processing ECG signals used in our research. In addition, we will present a detailed evaluation of the authentication performance of the different schemes.

4.1. ECG datasets

In this work, we mainly used two public datasets to evaluate performance: the ECG-ID [27] and the PTB Diagnostic ECG Database [28].

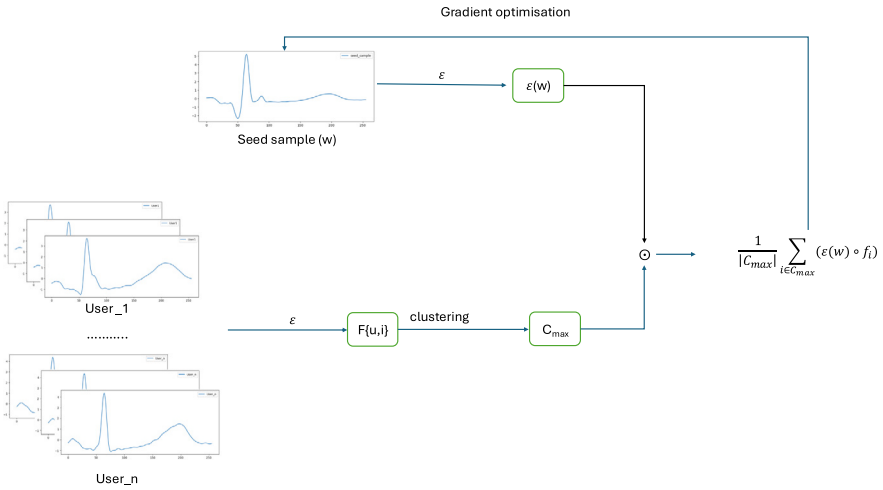


Fig. 3. Adversarial attack process.

Both datasets are widely used in the development of ECG authentication algorithms.

- ECG-ID: This dataset contains a total of 310 ECG recordings from 90 users. The subjects include 44 men and 46 women, with an age range of 13 to 75 years. The ECG signals were recorded using electrodes placed on the patients' wrists. This dataset is frequently used for personal identification and authentication tasks.
- PTB Diagnostic ECG Database: This dataset comprises 549 ECG recordings derived from 290 individuals, aged between 17 and 87 years. Among these subjects, there are 209 males and 81 females. The ECG signals were obtained using electrodes placed on the chest and limbs of the patients. The PTB Diagnostic ECG Database is extensively utilized in medical diagnostics and ECG signal analysis, offering a diverse assortment of signals from a wide-ranging cohort of subjects.
- MIT-BIH Arrhythmia dataset: This database comprises 48 half-hour ECG recordings from 47 subjects, all of whom suffer from arrhythmia. The ECG signals were collected using electrodes placed on the chest [29]. This database was chosen because it is widely used to evaluate the effectiveness of ECG authentication algorithms [19,30]
- MIT-BIH NSRDB: This database contains long-term ECG recordings from 18 subjects, including 5 males and 13 females, with ages ranging from 20 to 50 [29]. It is also widely used to validate the effectiveness of various ECG authentication algorithms [19,30].

In this study, subjects from the ECG-ID database were randomly split into two equal groups. One group was used to train the ECG signal encoder and the other was employed to evaluate the encoder's authentication performance. For the other three databases, 20% of the users in each database were randomly selected to train the main ECG waveforms, while the other 80% were used to create registration templates to evaluate the effectiveness of the attacks. Table 1 presents a comprehensive summary of the data distribution employed in the experiments.

In this experiment, as the sampling frequencies of the two datasets differ, we initially resampled the PTB Diagnostic ECG Database, MIT-BIH Arrhythmia Database and MIT-BIH NSRDB to align with the 500 Hz sampling rate of the ECG-ID database.

4.2. Preprocessing

During the acquisition of ECG data from subjects, noise is unavoidably introduced due to elements such as muscle activity and electrical power line interference. Additionally, because most ECG authentication algorithms extract features from individual heartbeats, it is crucial to segment the ECG signals accordingly.

In this experiment, to eliminate noise from the ECG signals, we employed a combination of filters. The filter system consists of four components: wavelet drift correction (to correct baseline drift), an adaptive notch filter (to remove power line interference), a low-pass filter (to eliminate high-frequency noise), and a smoothing filter [27]. Fig. 4 shows the differences between the ECG waveform before and after noise reduction, highlighting the impact of filtering on signal clarity. Following noise removal, the waveforms are segmented according to individual heartbeat cycles.

In our segmentation process, we initially employed the Pan-Tompkins algorithm [31] to identify the R-peaks within individual heartbeat cycles. Nevertheless, this algorithm's position indications can exhibit minor inaccuracies. Following the identification of R-peaks, we enhanced precision by pinpointing the local maxima in proximity to the initial points to fine-tune the R-peak locations.

During the experiment, each waveform's window size was fixed at 256 samples. The segmentation approach included selecting 64 samples preceding the R-peak and 192 samples succeeding the R-peak. Furthermore, Z-score normalization was applied to standardize the extracted heartbeat signals, promoting data uniformity across various samples.

4.3. ECG authentication scheme

In this experiment, we reproduced three ECG authentication algorithms based on Convolutional Neural Networks (CNNs). We chose algorithms that have been notably cited over the last five years, reflecting the current state-of-the-art in the domain. To maintain the precision of our reproductive studies, we focused on selecting publications that offer open-source code.

- Deep-ECG [24]: This method, proposed by Labati et al. is one of the earliest approaches to use deep convolutional networks for ECG-based biometric recognition. The approach employs a multilayer CNN model trained for closed-set identification tasks. Once the training is complete, the classification head is removed, leaving the rest of the network to be employed for extracting ECG embedding features. The method has undergone thorough evaluation across various tasks, including authentication, closed-set identification, and cross-time recognition, showcasing its adaptability in diverse ECG-based recognition scenarios.
- EDITH [30]: The technique introduced by Ibtehaz et al. employs a CNN model trained via closed-set identification tasks to derive embeddings for ECG signals. The main advantage of this approach lies in its capacity to maintain high authentication accuracy while requiring fewer heartbeats compared to previous methods.

Table 1
Dataset partition.

Dataset	Subjects	Sampling Rate	Electrode Placement	Scope
ECG-ID Dev	45	500 Hz	Wrist	Encoder-train
ECG-ID Test	45	500 Hz	Wrist	Encoder-eval
PTB Train	58	100 Hz	Chest+Limbs	MW-Opt
PTB Test	232	100 Hz	Chest+Limbs	MW-eval
MIT-BIH Arrhythmia train	9	360 hz	Chest	MW-Opt
MIT-BIH Arrhythmia test	38	360 hz	Chest	MW-eval
MIT-BIH NSRDB train	4	360 hz	Chest	MW-Opt
MIT-BIH NSRDB test	14	360 hz	Chest	MW-eval

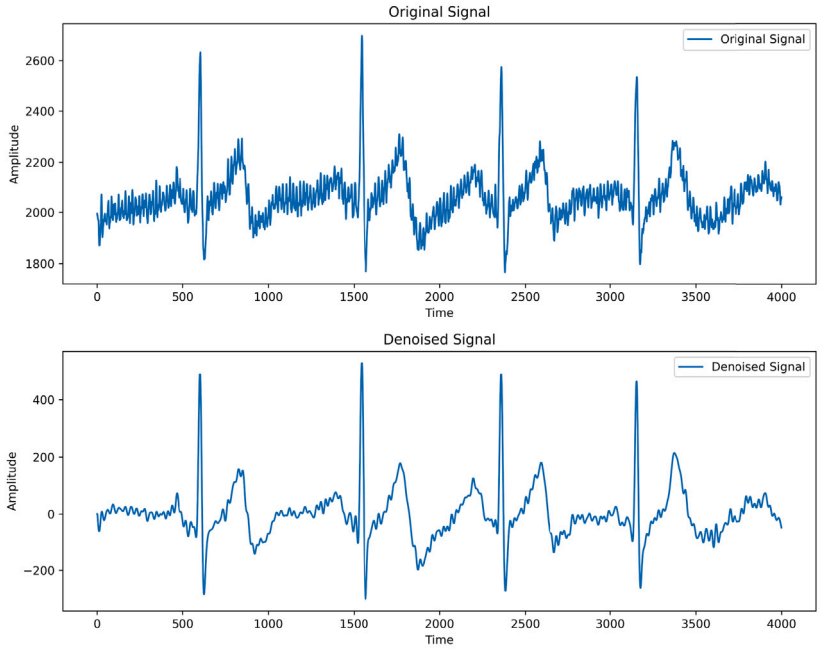


Fig. 4. Electrocardiogram signal de-noising.

- ECGIoT [32]: Introduced by Guoxin et al. this approach is a CNN-based ECG authentication algorithm tailored for IoT devices with constrained computational capabilities. The primary difference between ECGIoT and previous methods is its focus on enabling ECG authentication in resource-constrained environments. The method achieves fast authentication with minimal computational resources, making it highly suitable for IoT endpoints where efficiency and speed are crucial without sacrificing accuracy.

In order to assess the effectiveness of our reproduction attempts, we carried out a comprehensive performance evaluation of the three replicated authentication methods. In this experiment, for the Deep-ECG and EDITH methods, each user is enrolled using 10 consecutive heartbeat cycles, and an authentication template is generated. During the authentication phase, the features are extracted from 5 consecutive heartbeat cycles, and their average is used for authentication. Authentication is accomplished by computing the cosine similarity between the input ECG features and the stored template for authentication.

The ECGIoT approach is distinct from the other two methods as it does not extract features from individual heartbeat cycles. Instead, it considers five consecutive cycles as a unified entity for feature extraction. Consequently, the any-10 or avg-10 authentication techniques we developed were not applicable. In this experiment, we set the system to use the average of 5 sets of consecutive 5-heartbeat cycle features to generate the authentication template. Similarly, in the authentication phase, 5 consecutive heartbeats are used to extract features and compare with the authentication template via similarity comparison.

Table 2
ECG authentication model and their performance (transposed).

	ECGIoT	Deep-ECG	EDITH
AUC (any-10)		98.45%	99.63%
AUC (avg-10)	99.4%	98.52%	99.71%
EER (any-10)		5.69%	3.04%
EER (avg-10)	2.10%	5.43%	2.69%
FRR @ FAR 1% (any-10)		19.76%	9.5%
FRR @ FAR 1% (avg-10)	8.287%	15.85%	8.34%

The results of the evaluation conducted in this phase were utilized for threshold calibration in later experiments. In this experiment, the Equal Error Rates (EER) of the implemented authentication algorithms varied between 2.1% and 5.43%, aligning with the performance in published literature. The performance of our authentication model is shown in Table 2.

In this experiment, we focus on the threshold setting in the case of False Acceptance Rate (FAR) = 1% and EER. The results indicate that employing avg-10 as the authentication policy surpasses the performance of using any-10. This difference in performance is more notable when the FAR is set at 1%.

4.4. Dictionary attack

In this research, we utilized ECG data from 20% of the users within the each ECG databases to optimize and test the master ECG. The objective of choosing this subset is to emulate real-world situations,

where an attacker has access to substantially less ECG data compared to registered users.

We first conducted biometric analyses of three distinct authentication methods across three different databases to evaluate the system's robustness and to understand the specific differences among users. This analysis focused on two key metrics: intra-user similarity and inter-user similarity. Intra-user similarity is the mean similarity of features derived from various heartbeat cycles belonging to the same individual. An elevated similarity within a user's ECG signals suggests a consistent pattern over time, essential for dependable authentication. Inter-user similarity is the average similarity between a user's ECG features and those of other users. A low similarity among users means that the ECG characteristics are unique enough to thwart impersonation by unauthorized individuals. For a robust authentication model, it is essential to achieve high intra-user similarity and low inter-user similarity. This balance ensures that legitimate users are accurately recognized while unauthorized access is effectively prevented.

Fig. 5 presents that the three authentication algorithms produced similar results across the different databases, displaying analogous data distribution characteristics. Moreover, all three authentication algorithms achieved high intra-user feature similarity while maintaining a significant gap from inter-user feature similarity in every database. This substantial gap offers flexibility in adjusting the decision thresholds for authentication.

The initial stage of optimizing the primary ECG waveform involves selecting a seed ECG waveform. In this study, the waveform from the user with the greatest inter-user similarity was chosen as the seed for optimization. The rationale behind this choice is that a waveform already similar to many users' ECG signals serves as a strong starting point for creating an adversarial example that can potentially bypass multiple users' authentication checks. Although there is potential to enhance the attack success rate through the refinement of the seed selection process, we chose this methodology to streamline the experimental setup and concentrate on illustrating the attack's feasibility.

During the optimization process, we employed SGD to reduce the optimization time. SGD is particularly effective for large-scale optimization problems due to its ability to update parameters incrementally through subsets of the dataset, thereby facilitating quicker convergence than traditional gradient descent methods. To maintain stability and avoid overshooting minima during optimization, we applied gradient normalization before updating the attack vector. This normalization of gradients is crucial to managing step sizes efficiently.

We carried out comprehensive experiments to establish the ideal step size by evaluating different configurations to pinpoint the most appropriate setup. By fine-tuning the step size, we aimed to achieve a balance between rapid convergence and a high attack success rate.

5. Performance evaluation of proposed methods

In this section, we comprehensively evaluate the performance of the proposed attack method. The evaluation is divided into the following five parts:

- Resource requirements: We thoroughly evaluated the resource consumption required for the optimization process, thereby providing a comprehensive assessment of the feasibility of this attack method.
- Step Size Settings and Gradient Normalization in the Optimization Process: we investigated how various step sizes and gradient normalization strategies affect the optimization process. This analysis was instrumental in identifying the optimal setup to effectively optimize the attack vector.
- Authentication Performance for Various Authentication Methods: We evaluated the efficacy of the attack on multiple authentication strategies, examining the performance of the proposed method under different conditions of authentication models.

Table 3
Optimization resource requirement.

Authentication model	Deep-ECG	EDITH	ECGIoT
Memory usage	20.97 MB	12.12 MB	22.14 MB
Time consuming	0.0368 s	0.0561 s	0.00431 s

- Transferability experiment: we evaluated the transfer possibilities of the attack model between different authentication models. We explored whether the main ECG waveform, after adversarial optimization, can achieve the same attack effect in other authentication models that are not involved in the optimization.
- Attack Performance with Multiple Attempt Allowance: we evaluated the attack's success rate when multiple authentication attempts were allowed. This part of the experiment evaluates the attack performance of the method in real scenarios.

5.1. Resource requirements

In this attack method, the focus is on gradually optimizing the waveform. The primary computational load in each optimization step is the extraction of features by inputting the signal into the model and comparing the obtained features with others using cosine similarity. The overall computational complexity mainly depends on the size of the authentication model and the number of features. In this experiment, we evaluated the memory consumption and the average time per optimization step under three different authentication algorithms. This experiment was conducted on the Google Colab platform using an L4 GPU.

Table 3 summarizes the memory requirements and the optimization time per step for each algorithm. As can be seen from the table, the attack method requires very few resources, and the optimization time is also minimal. This is because various authentication algorithms are designed with relatively small models to ensure a short authentication time, allowing us to quickly optimize the waveform.

5.2. Impact of parameter settings

In this experiment, our first task was to identify the appropriate gradient normalization method and setting the step size. We tested two different gradient optimization approaches: $L2$ normalization and L_∞ normalization. For this stage of the experiment, we used the EDITH authentication algorithm and the evaluation was conducted in the FAR = 1% setting, using the any-10 authentication strategy.

Fig. 6 shows the changes in impostor success rate under different step size settings for both $L2$ and L_∞ normalization. From the figure, we can observe that both normalization methods achieved similar impostor success rates. After 100 epochs, both methods reached around a 25% impostor success rate. On the other hand, for both normalization methods, choosing a larger step size does not lead to effective adversarial optimization.

For the $L2$ normalization, the best optimization results were obtained with a step size in the range of 0.1 to 0.01. In contrast, for L_∞ normalization, the optimal range for the step size was between 0.01 and 0.001. Based on the results of this section of the experiment, we chose to use $L2$ normalization in subsequent experiments and set the step size to 0.1 for adversarially optimizing the master ECG waveform. This configuration was selected because it yielded the most effective optimization in terms of impostor success rate, balancing the speed of convergence and the overall effectiveness of the attack.

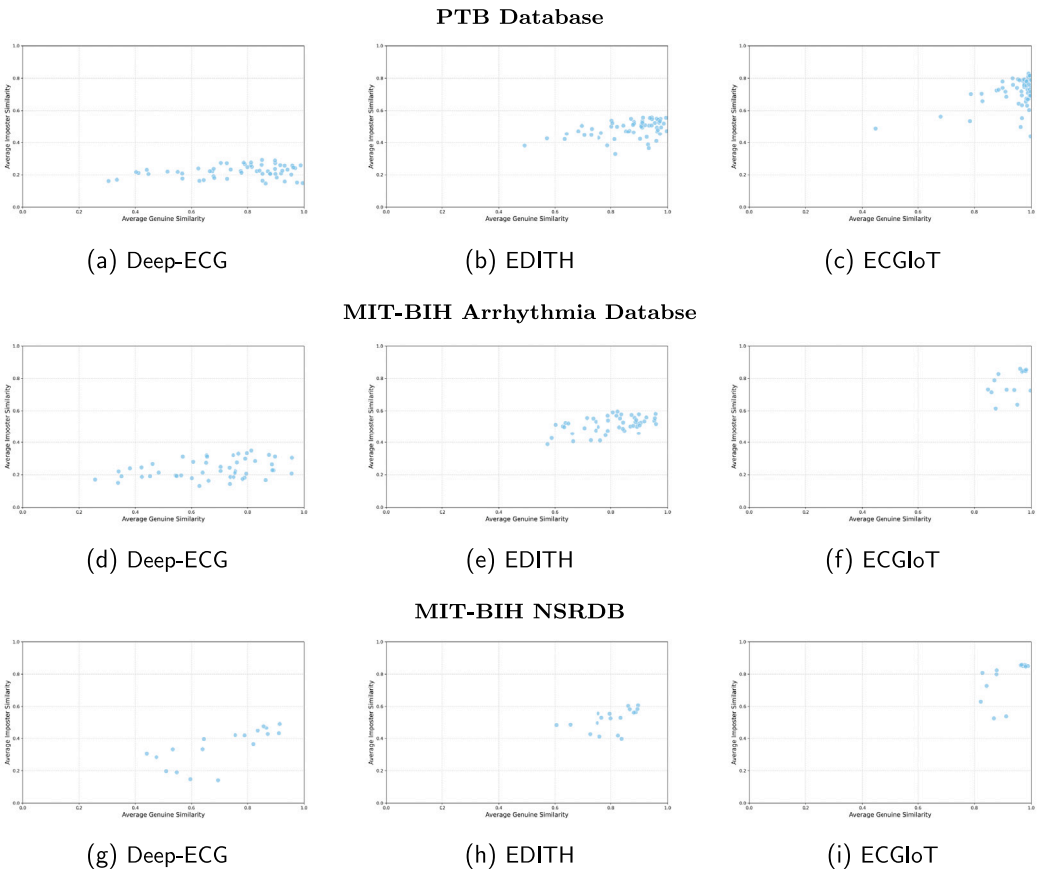


Fig. 5. Menagerie analysis plots.

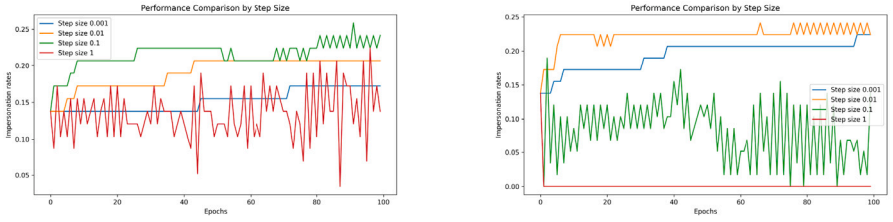


Fig. 6. Changes in impostor rate at different steps.

5.3. Performance of proposed method

In this section, we tested the impostor success rate of our designed attack method with different authentication methods and strategies. The threshold of the authentication model was set based on the FAR = 1% and EER conditions. Table 4 represents the impostor success rate of our method for the case of different models and different authentication policies in PTB databases. Table 5 presents the results of applying the same attack method to the other two databases.

Table 4 reveals that the proposed attack approach attains remarkable outcomes for various authentication algorithms and strategic configurations. Under the strict condition of a 1% FAR, our method achieved an average success rate of 20% when attacking ECG authentication systems for users unseen during the training process. When the authentication criterion is applied to the EER, our technique achieved an impersonation success rate of over 30%. Furthermore, the success rate for targeting the ECGIoT algorithm was nearly 50%. By comparing the success rates of the seed sample and the optimized master sample, it is clear that our optimization method significantly improves the success rate of impersonation attacks. This underscores the efficacy of our adversarial optimization approach in enhancing the attack's influence on ECG authentication systems.

When attacking the other databases, the results in Table 5 also demonstrated similar effectiveness. Compared to the attack results on the PTB database, our waveform optimization method improved the impersonation success rate. However, the improvement was not as pronounced as in the PTB database. This is because the number of users available for optimization in the other two databases is much smaller than in the PTB database, making it challenging for the optimized waveform to capture the broader population's characteristics. It is worth noting that even with a limited training dataset, our method can, on average, breach the authentication systems of more than 15% of unseen users.

Table 4
Impersonation success rate under different models with different threshold settings. S: Seed sample. M: Master sample.

	S (Train-sets)	M (Train-sets)	S (Test-sets)	M (Test-sets)
EDITH (any-EER)	20.69%	41.37%	19.82%	40.95%
EDITH (any-FAR)	13.79%	25.86%	9.91%	23.71%
EDITH (avg-EER)	15.51%	32.75%	13.79%	39.65%
EDITH (avg-FAR)	10.34%	22.41%	7.75%	22.84%
Deep-ECG (any-EER)	17.24%	27.58%	22.41%	32.75%
Deep-ECG (any-FAR)	5.17%	17.24%	4.31%	18.53%
Deep-ECG (avg-EER)	15.51%	25.86%	21.98%	31.46%
Deep-ECG (avg-FAR)	5.17%	12.06%	3.87%	18.53%
ECGIoT (EER)	25.86%	55.17%	16.81%	48.27%
ECGIoT (FAR)	13.79%	36.21%	6.47%	27.59%

Table 5
The impersonation success rates in the MIT-BIH Arrhythmia database and the MIT-BIH NSRDB; S: Seed sample, M: Master sample.

	S (Arrhythmia)	M (Arrhythmia)	S (NSRDB)	M (NSRDB)
EDITH (any-EER)	15.79%	23.68%	14.29%	21.43%
EDITH (any-FAR)	7.9%	15.79%	7.14%	7.14%
EDITH (avg-EER)	10.53%	18.42%	7.14%	12.29%
EDITH (avg-FAR)	7.9%	15.79%	7.14%	7.14%
Deep-ECG (any-EER)	31.57%	42.11%	21.43%	28.57%
Deep-ECG (any-FAR)	13.15%	18.42%	14.29%	14.29%
Deep-ECG (avg-EER)	23.68%	31.58%	21.43%	21.43%
Deep-ECG (avg-FAR)	10.52%	18.42%	7.14%	14.29%
ECGIoT (EER)	10.52%	44.74%	21.43%	42.86%
ECGIoT (FAR)	0%	31.58%	7.14%	42.86%

Table 6
Transferability possibility experiments for different authentication models.

test \ target	EDITH	Deep-ECG	ECG-IoT
EDITH	23.71%	0%	0.43%
Deep-ECG	0.86%	18.53%	18.53%
ECG-IoT	0%	0.86%	27.6%

Based on these experimental results, in subsequent experiments we will use only the PTB database and consider the any-10 authentication strategy under the condition of FAR = 1%.

5.4. Transferability experiment

For each of the three distinct ECG authentication models, we individually optimized the master ECG waveform. In every instance, the optimization was exclusively focused on one specific authentication model, devoid of any influence from the remaining models.

Once optimization was complete, the generated master ECG waveform was then transferred to the other two authentication models that had not participated in the optimization process. At this stage, no further optimization was performed; instead, we directly used the master ECG waveform to evaluate its attack success rate on the other two authentication models.

Table 6 presents the results of the transferability experiments in three ECG authentication models: EDITH, Deep-ECG, and ECG-IoT. Analyzing the outcomes, it is apparent that ECG signals optimized adversarially show limited transferability between various models. In most cases, the attack success rates are significantly lower when transferred to models other than the one for which they were optimized. However, there is one notable exception: the Deep-ECG model seems to have moderate transferability, achieving a relatively high success rate when transferred to the ECG-IoT model. We hypothesize that this is likely due to the structural similarity between the two models. The CNN structure of the ECG-IoT was derived from and modified based on the Deep-ECG model, which may explain the improved success rate when attacks are transferred between these two models.

5.5. Multiple presentation attack

For biological authentication models, users are generally allowed to make multiple attempts due to their false rejection rate. In this section, we evaluate the performance of our attack model in a scenario that allows multiple authentication attempts. We configured the system to allow for 5 attempts, and for each authentication algorithm, we optimized five distinct adversarial waveforms for the attack.

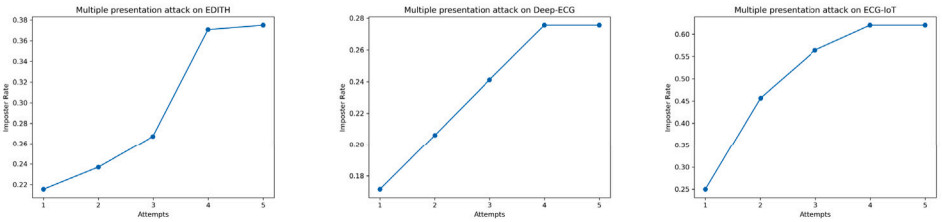
To ensure that each waveform is specifically designed for diverse user groups, we optimized the waveforms employing distinct data subsets. In prior experiments, we implemented connected component clustering to categorize the data, selecting the cluster with the highest number of data points for optimizing a single waveform. In this part, we increase the clustering threshold, which resulted in five distinct clusters, each containing a sufficient number of data points. Then these five clusters were used to optimize the five separate attack waveforms.

Fig. 7 presents the results of our experiments in which multiple attack attempts were allowed. The figure illustrates that for each algorithm, the success rate of our proposed attack method has notably increased after several attempts. Specifically, the results of the ECG-IoT algorithm are notable, revealing that after five attack attempts, the success rate for bypassing ECG authentication with unseen users exceeds 60%. This poses a substantial threat to ECG-based authentication systems, demonstrating that allowing multiple authentication attempts considerably increases the risk of adversarial attacks.

6. Discussion

In this study, we reveal the vulnerability of ECG authentication algorithms when confronted with dictionary attacks. We hypothesize that this vulnerability arises due to two key factors:

- High-Density Feature Regions from CNN model: Using CNN model to extract ECG features tends to create high-density regions in the feature space. These regions are populated by features that represent a large proportion of the user population.
- Robustness Challenges in ECG Authentication Systems: Existing ECG authentication techniques fail to possess the necessary robustness to distinguish between artificially generated (adversarial) signals and genuine, authentic signals. This facilitates the attack's ability to exploit unintended feature overlaps.



(a) EDITH (b) Deep-ECG (c) ECG-IoT

Fig. 7. Multiple presentation attacks.

In light of the issues currently affecting authentication algorithms, several potential mitigation strategies can be implemented as follows:

- Multi-factor authentication: When users authenticate on mobile devices, they will place their finger on an electrode to capture ECG signals. This approach can also concurrently gather fingerprint data or other biometric signals to enable multi-factor authentication [33–35]. Multi-factor authentication can significantly increase the difficulty for attackers, thereby ensuring secure authentication.
- Biometric template selection: Most existing authentication schemes generate registration templates by randomly selecting the signals provided by users. This method has been proven to carry inherent risks. Previous research in fingerprint authentication has demonstrated that systematic template selection can yield better authentication performance compared to random selection [36]. Moreover, this approach can effectively reduce feature similarity between different users.
- Developing anti-spoofing schemes: Existing algorithms consider only a single ECG signal when extracting features. However, there is an inherent relationship between the contexts of consecutive ECG signals. Incorporating heart rate variability into anti-spoofing strategies may serve as an effective means to mitigate dictionary attacks [12,37].

7. Conclusion and future work

In this research, we developed a dictionary attack technique aimed at ECG-based authentication systems. This method does not require any prior background information about the victim and relies on incidental matches to bypass the victim's authentication device. Our experimental findings indicate that our method can effectively compromise the authentication systems of a significant number of users. The method demonstrates a high level of generalizability and shows effectiveness across a range of ECG authentication algorithms. The experimental evaluation allows us to outline the following principal points:

- Effectiveness of the Dictionary Attack: Our proposed method achieves a high success rate in bypassing the ECG authentication systems, even without prior knowledge of the victim's specific ECG patterns. This shows the vulnerability of ECG-based authentication to incidental matches when using dictionary attacks.
- Cross-Population Transferability: In our experiments, the optimized waveforms achieved similar impersonation success rates in both the training set and the test set. This indicates that different populations share similar distributions of ECG features.
- Cluster-Based Optimization: The use of clustering techniques to optimize multiple attack waveforms significantly enhances the success rate. By targeting different user groups with specialized waveforms, the attack is able to cover a wider range of potential victims.

Although we achieved good results, our experiment still has some shortcomings. First, all of our experiments were conducted in a controlled laboratory environment. In real-world scenarios, the performance of our attack may be influenced by various factors. Secondly, numerous ECG synthesis algorithms are currently available and testing these algorithms could possibly boost the effectiveness of our attack. Particularly those employing generative models such as GANs (Generative Adversarial Networks) or VAEs (Variational Auto-Encoders) are capable of generating adversarial waveforms of superior quality that bear a closer resemblance to authentic physiological signals. We believe that our work will contribute to a deeper understanding of the mechanisms behind ECG authentication, thereby laying the groundwork for developing more secure ECG authentication systems in the future.

CRediT authorship contribution statement

Bonan Zhang: Writing – original draft, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Lin Li:** Writing – review & editing. **Chao Chen:** Writing – review & editing, Supervision, Conceptualization. **Ickjai Lee:** Writing – review & editing, Supervision. **Kyungmi Lee:** Writing – review & editing, Supervision. **Tianqing Zhu:** Writing – review & editing. **Kok-Leong Ong:** Writing – review & editing, Supervision.

Declaration of competing interest

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

Data availability

The dataset used in this article is a public dataset. All readers have access to the dataset.

References

[1] A. Sarkar, B.K. Singh, A review on performance, security and various biometric template protection schemes for biometric authentication systems, Multimedia Tools Appl. 79 (37) (2020) 27721–27776.
[2] E. Rahmawati, M. Listyasari, A.S. Aziz, S. Sukaridhoto, F.A. Damastuti, M.M. Bachtiar, A. Sudarsono, Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone, in: 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), IEEE, 2017, pp. 234–238.
[3] P. Kaur, K. Krishan, S.K. Sharma, T. Kanchan, Facial-recognition algorithms: A literature review, Med. Sci. Law 60 (2) (2020) 131–139.
[4] D. Gafurov, E. Snekkenes, P. Bours, Gait authentication and identification using wearable accelerometer sensor, in: 2007 IEEE Workshop on Automatic Identification Advanced Technologies, IEEE, 2007, pp. 220–225.
[5] C. Shi, Y. Wang, Y. Chen, N. Saxena, C. Wang, Wearid: Low-effort wearable-assisted authentication of voice commands via cross-domain comparison without training, in: Proceedings of the 36th Annual Computer Security Applications Conference, 2020, pp. 829–842.
[6] Y. Cao, Q. Zhang, F. Li, S. Yang, Y. Wang, Ppgpass: Nonintrusive and secure mobile two-factor authentication via wearables, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications, IEEE, 2020, pp. 1917–1926.

[7] S.J. Kang, S.Y. Lee, H.I. Cho, H. Park, ECG authentication system design based on signal analysis in mobile and wearable devices, IEEE Signal Process. Lett. 23 (6) (2016) 805–808.
[8] F. Agrafioti, J. Gao, D. Hatzinakos, J. Yang, Heart biometrics: Theory, methods and applications, Biometrics 3 (199–216) (2011) 25.
[9] C. Camara, P. Peris-Lopez, L. Gonzalez-Manzano, J. Tapiador, Real-time electrocardiogram streams for continuous authentication, Appl. Soft Comput. 68 (2018) 784–794.
[10] A.S. Rathore, Z. Li, W. Zhu, Z. Jin, W. Xu, A survey on heart biometrics, ACM Comput. Surv. 53 (6) (2020) 1–38.
[11] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, A. Patané, Broken hearted: How to attack ECG biometrics, in: Network and Distributed System Security Symposium 2017, Internet Society, 2017.
[12] N. Karimian, D. Woodard, D. Forte, ECG biometric: Spoofing and countermeasures, IEEE Trans. Biom. Behav. Identity Sci. 2 (3) (2020) 257–270.
[13] A. Roy, N. Memon, A. Ross, Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems, IEEE Trans. Inf. Forensics Secur. 12 (9) (2017) 2013–2025.
[14] H.H. Nguyen, S. Marcel, J. Yamagishi, I. Echizen, Master face attacks on face recognition systems, IEEE Trans. Biom. Behav. Identity Sci. 4 (3) (2022) 398–411.
[15] M. Marras, P. Korus, N.D. Memon, G. Fenu, et al., Adversarial optimization for dictionary attacks on speaker verification, in: Interspeech, 2019, pp. 2913–2917.
[16] M. Marras, P. Korus, A. Jain, N. Memon, Dictionary attacks on speaker verification, IEEE Trans. Inf. Forensics Secur. 18 (2022) 773–788.
[17] N. Yager, T. Dunstone, The biometric menagerie, IEEE Trans. Pattern Anal. Mach. Intell. 32 (2) (2008) 220–230.
[18] L.S. Lilly, Pathophysiology of Heart Disease: a Collaborative Project of Medical Students and Faculty, Lippincott Williams & Wilkins, 2012.
[19] J.S. Arteaga-Falconi, H. Al Osman, A. El Saddik, ECG authentication for mobile devices, IEEE Trans. Instrum. Meas. 65 (3) (2015) 591–600.
[20] T. Fiebig, J. Krissler, R. Hänsch, Security impact of high resolution smartphone cameras, in: 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014.
[21] L. Biel, O. Pettersson, L. Philipson, P. Wide, ECG analysis: a new approach in human identification, IEEE Trans. Instrum. Meas. 50 (3) (2001) 808–812.
[22] M. Benouis, L. Mostefai, N. Costen, M. Regouid, ECG based biometric identification using one-dimensional local difference pattern, Biomed. Signal Process. Control. 64 (2021) 102226.
[23] B. Fatimah, P. Singh, A. Singhal, R.B. Pachori, Biometric identification from ECG signals using Fourier decomposition and machine learning, IEEE Trans. Instrum. Meas. 71 (2022) 1–9.
[24] R.D. Labati, E. Muñoz, V. Piuri, R. Sassi, F. Scotti, Deep-ECG: Convolutional neural networks for ECG biometric recognition, Pattern Recognit. Lett. 126 (2019) 78–85.
[25] V. Krish, N. Paoletti, M. Kazemi, S. Smolka, A. Rahmati, Biosignal authentication considered harmful today, in: 33rd USENIX Security Symposium (USENIX Security 24), 2024, pp. 5521–5536.
[26] H.H. Nguyen, J. Yamagishi, I. Echizen, S. Marcel, Generating master faces for use in performing wolf attacks on face recognition systems, in: 2020 IEEE International Joint Conference on Biometrics, IJCB, IEEE, 2020, pp. 1–10.
[27] N. Lugovaya, Biometric human identification based on ECG, Russ. Conf. Math. Methods Pattern Recognit. (2005).
[28] R. Bousseljot, D. Kreiseler, A. Schnabel, Nutzung der EKG-signaldatenbank CARDIODAT der PTB über das internet, Biomed. Tech. / Biomed. Eng. 40 (s1) (1995) 317–318.
[29] G.B. Moody, R.G. Mark, The impact of the MIT-bih arrhythmia database, IEEE Eng. Med. Biol. Mag. 20 (3) (2001) 45–50.
[30] N. Ibtehaz, M.E. Chowdhury, A. Khandakar, S. Kiranyaz, M.S. Rahman, A. Tahir, Y. Qiblawey, T. Rahman, EDITH: ECG biometrics aided by deep learning for reliable individual authentication, IEEE Trans. Emerg. Top. Comput. Intell. 6 (4) (2021) 928–940.
[31] J. Pan, W.J. Tompkins, A real-time QRS detection algorithm, IEEE Trans. Biomed. Eng. (3) (1985) 230–236.
[32] G. Wang, S. Shanker, A. Nag, Y. Lian, D. John, ECG biometric authentication using self-supervised learning for IoT edge sensors, IEEE J. Biomed. Heal. Inform. (2024).
[33] Y.N. Singh, S.K. Singh, P. Gupta, Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system, Pattern Recognit. Lett. 33 (14) (2012) 1932–1941.
[34] L. Bastos, T. Tavares, D. Rosário, E. Cerqueira, A. Santos, M. Nogueira, Double authentication model based on ppg and ecg signals, in: 2020 International Wireless Communications and Mobile Computing, IWCMC, IEEE, 2020, pp. 601–606.
[35] M. Komeili, N. Armanfard, D. Hatzinakos, Liveness detection and automatic template updating using fusion of ECG and fingerprint, IEEE Trans. Inf. Forensics Secur. 13 (7) (2018) 1810–1822.
[36] U. Uludag, A. Ross, A. Jain, Biometric template selection and update: a case study in fingerprints, Pattern Recognit. 37 (7) (2004) 1533–1542.
[37] T. Zhu, L. Fu, Q. Liu, Z. Lin, Y. Chen, T. Chen, One cycle attack: Fool sensor-based personal gait authentication with clustering, IEEE Trans. Inf. Forensics Secur. 16 (2020) 553–568.