EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Fortifying Patient Data Security in the Digital Era: A Two-Layer Approach with Data Hiding and Electrocardiogram

Praveen Gupta*[1] and Ajay Prasad[2]

[1]Research Scholar, UPES, Dehradun, INDIA
[2]Department of Computer Science, UPES, Dehradun, INDIA

Abstract

In an era dominated by digital technology, the imperative of securing patient data cannot be overstated. The deployment of advanced protective measures, including encryption, firewalls, and robust authentication protocols, is an absolute necessity when it comes to preserving the confidentiality and integrity of sensitive patient information. Furthermore, the establishment of stringent access controls serves as a fundamental safeguard, ensuring that only authorized personnel are granted access to this invaluable data. An innovative development in the realm of patient data protection is the utilization of ElectroCardioGram (ECG) as a unique identifier for individuals. In the context of this study, ECG data is ingeniously embedded within cover images using a technique known as Reversible Data Hiding (RDH). RDH offers a distinctive advantage by ensuring that the original image can be fully restored without loss of data after extraction. This achievement is made possible through the application of inventive pixel interpolation and histogram shifting algorithms. Crucially, the study's simulations, conducted across a diverse array of images, underscore the enhanced embedding capacity of the RDH technique while maintaining a commendable balance in terms of the Peak Signal to Noise Ratio (PSNR) and boundary map. This empirical evidence corroborates the efficacy of the approach and its potential to provide an advanced level of security for patient data in the digital landscape.

Keywords: ECG, data embedding, RDH, PSNR

Received on 11 02 2024, accepted on 15 06 2024, published on 15 07 2024

doi: 10.4108/eetsis.5644

*Corresponding author. Email: guptapraveenphd@gmail.com

1. Introduction

The importance of safeguarding patient data in the digital age cannot be overstated. A myriad of security measures, such as encryption, firewalls, secure authentication, and access controls, have become pivotal components in fortifying patient information against unauthorized access and potential breaches [1-4]. In the realm of healthcare, the need for stringent control over who can access patient data is paramount. Only individuals with the proper credentials and authorization should be allowed to access and interact with this sensitive information. This not only upholds patient privacy but also ensures that medical records remain confidential and secure. To maintain the resilience of these security measures, regular security updates and audits are vital. These ongoing processes serve the critical function of identifying vulnerabilities and rectifying them promptly. Moreover, comprehensive staff training is imperative to prevent accidental data breaches, as human error remains a

significant factor in data security incidents. In the digital age, a holistic approach is indispensable for the protection of patient data. This comprehensive strategy encompasses various security layers to create a robust defense system against the evolving landscape of digital threats. The implementation of this multi-faceted approach ensures that patient data remains secure and intact.

One of the technological advancements enhancing patient care in the digital era is the deployment of Wireless Body Area Networks (WBANs). These networks efficiently monitor physiological data, contributing to the detection and treatment of chronic diseases [5]. By utilizing tiny sensors for real-time health data collection, WBANs have revolutionized medical care and wellness management. The data gathered from patients can be efficiently processed and transmitted over WBAN-based e-human services architecture, enabling rapid data delivery and remote examinations [1]. WBANs consist of sensor nodes responsible for collecting physiological data. This data is then processed by the Body Control Unit (BCU) before transmission [1]. The security of data transmitted within WBANs is of paramount importance due to the inherently sensitive nature of medical information. Robust security measures, such as encryption and authentication, are essential to prevent unauthorized access and tampering [4]. In resource-constrained environments like WBANs, lightweight security protocols are optimized to address scalability challenges, ensuring that security is not compromised [4]. The use of electrocardiogram (ECG) as a unique biometric identifier has gained prominence in the healthcare sector [6]. ECG offers non-invasive accuracy in patient identification, a feature of great value in healthcare. WBANs play a pivotal role in facilitating the accurate transmission of ECG data among sensors, thereby enhancing remote patient monitoring and healthcare delivery [5]. The protection of patient privacy and the secure handling of data from various sources are critical in healthcare settings [6]. Implementing systems that allow patients to control access to their personal health records not only builds trust but also ensures responsible data handling [7]. Robust security protocols and encryption methods are crucial for safeguarding data in communication networks and on servers [8, 9]. Notably, data can be hidden within host data without increasing its size or computing overhead [10-12]. This allows for secure data storage and transmission, either before or after the encryption process, ensuring that patient data remains confidential and intact [12].

In this paper, the authors propose a novel approach for patient identification by utilizing ECG (electrocardiogram) data. ECG is a widely used medical diagnostic tool that records the electrical activity of the heart over time. This method, as illustrated in Figure 1, introduces an innovative data security measure, the RDH mechanism, to safeguard ECG data. The fundamental idea behind this approach is to ensure that patient data, specifically their ECG records, remain confidential and secure throughout the identification process.

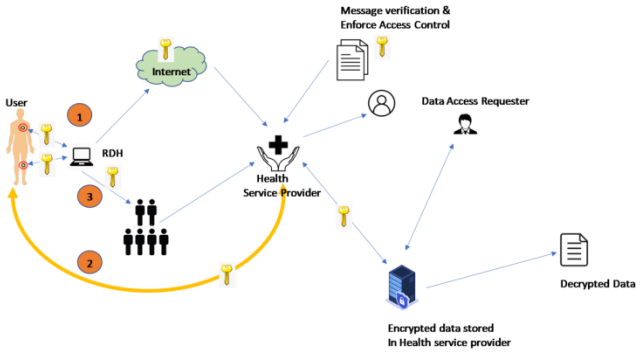

Figure 1. Schematic of RDH based secure data transfer mechanism

To achieve this, the RDH mechanism plays a pivotal role. RDH is a technique employed in information technology and data security, primarily focused on embedding data within other data while still allowing for the extraction of the original information. In this case, the RDH mechanism is applied to the ECG data. Before transmitting the RDH-embedded ECG data, an additional layer of protection is added. The RDH image is subjected to encryption. This encryption process ensures that the data is transformed into a format that is virtually impossible to decipher without the corresponding decryption keys. Thus, even if the transmitted data were intercepted by unauthorized parties, it would remain effectively unreadable and secure. The encryption keys serve as the critical tools for decrypting the RDH image. Only authorized individuals or entities possessing these decryption keys can successfully unlock and access the embedded ECG data. This guarantees that the patient's sensitive medical information remains protected from any potential security breaches or unauthorized access.

1.1 Motivation

The motivation behind the proposed concept stems from the pressing need to bolster patient data security within the increasingly digitized landscape of healthcare. With the proliferation of electronic health records and telemedicine, protecting sensitive medical information, such as electrocardiogram (ECG) data, has become paramount. Traditional encryption methods may provide some level of security but can be vulnerable to sophisticated cyber threats. Therefore, there is a strong motivation to explore innovative approaches that go beyond conventional encryption techniques to safeguard patient data effectively. By integrating ECG data into cover images using reversible data hiding (RDH), the proposed concept seeks to address this need by providing an alternative, yet robust, method for securing sensitive medical information. This approach not only enhances the security of ECG data but also ensures its confidentiality and integrity during transmission and storage, thereby motivating advancements in patient data security in the digital age.

1.2 Novelty and Contribution

The contribution of the proposed concept lies in its innovative integration of ECG data into cover images using RDH, which significantly enhances patient data security in the digital healthcare landscape. By leveraging RDH techniques, the concept enables the seamless embedding of ECG data into seemingly innocuous cover images without perceptible distortion, thus concealing sensitive medical information from unauthorized access. This novel approach not only enhances the confidentiality of ECG data but also ensures its tamper-resistance, as the embedded data can be extracted with minimal loss or distortion when required. Moreover, by employing cover images as carriers for ECG data, the concept offers an additional layer of security, as the embedded information remains camouflaged within the visual content, making it less susceptible to detection by potential attackers. Overall, the proposed concept makes a significant contribution to the field of patient data security by introducing a novel and effective method for safeguarding sensitive medical information in the digital realm.

1.3 Organization of Paper

The remaining sections of the paper are as follows: Section 2 provides an overview of related and recent notable works. Section 3 outlines the proposed approach for data hiding. In Section 4, simulation results, including PSNR and bit embedding capacity, are presented. The key findings are summarized finally in section 5.

2. Literature Survey

This section of the paper focuses on an extensive exploration of research and developments pertaining to the crucial domains of data hiding and patient identification using ECG data.

2.1 RDH Schemes

Early methods like compression [10], histogram equalization [11], and difference expansion [12] had limited embedding capacity. Compression involved a minor cover image compression to embed data, resulting in low capacity [10]. Histogram equalization used peak points for embedding but suffered from overflow and underflow issues, and limited peak locations reduced capacity [11]. Wang et.al introduced a new method based on Difference Expansion (DE) [12], increasing capacity and lowering complexity but still having low bit per pixel capacity. Subsequent modifications by researchers such as Wu et al. [13], Hou et al. [14], Chang et al. [15], and He et al. [16] aimed to enhance embedding capacity and image quality in RDH schemes, with a focus on histogram modification. Jhong et al. introduced histogram shifting for data embedding, using peak points [17]. Shaik et al. combined wavelet and histogram shifting to obtain more peak points [18]. Khan A. et al. improved capacity with histogram shifting, down sampling, and block selection [19]. Pan et al. proposed multi-dimensional and multi-level embedding [20]. Tai et al. based their method on histogram shifting and neighboring pixel differences [21]. Lin et al. used histogram difference for additional data embedding space [22]. Hu et al. employed neighboring pixel correlation and difference expansion for embedding [23]. Abadi et al. suggested interpolation error and histogram shifting [24], which was extended by Thodi and Rodriguez to Prediction Error Expansion (PEE) [25]. Recently, reversible methods focusing on image interpolation with a reversible cover image have gained attention. The interpolation process scales a 2M×2N image to M×N pixels, forming the final 2M×2N cover image. Various interpolation strategies have been proposed, where pixels values are interpolated using the surrounding pixels [26-32] Ma et al. introduced a method combining pixel interpolation and histogram shifting with good capacity but faced overflow and underflow issues, mitigated by the introduction of boundary maps [27]. Sah et al. [28] improved Ma et al.'s work by reducing the boundary map's size to enhance capacity while maintaining the histogram shifting procedure [27]. In this study, further enhancements are suggested, incorporating the Discrete Cosine Transform (DCT) and a novel interpolation scheme while keeping the histogram shifting approach similar to Ma et al.'s method [27]. Tripathi et al. [29] modified the interpolation scheme to further improve the results.

2.2 ECG Based Patient Identification

Wang and his colleagues (referenced as [33]) introduced an innovative biometric recognition technique centered on an ECG feature vector, which utilizes a pooling layer to handle beat signals of varying lengths. This method's efficacy and resilience are thoroughly assessed across a range of datasets, encompassing the ECG-ID database, the MITDB arrhythmia database, and a USSTDB database, a proprietary resource containing ECG recordings from 60 volunteers before and after physical exertion. Furthermore, this method exhibits strong recognition capabilities when subjected to cross-database tests. Mehdi et.al [34] proposed leveraging ECG signals, readily available in digital healthcare systems, for authentication purposes. The proposed solution utilizes an Ensemble Siamese Network (ESN) capable of handling minor variations in ECG signals. We further enhance the model's performance by incorporating preprocessing techniques for feature extraction. Through extensive training on benchmark datasets such as ECG-ID and PTB, our model achieves remarkable results, boasting an accuracy of 93.6% and 96.8%, respectively. In their research, Islam and colleagues (cited as [35]) introduced a novel feature known as "heartbeat shape" (HBS) for ECG-based biometric applications. This feature is derived from the morphology of

segmented heartbeats. To evaluate its effectiveness, the proposed feature was extensively tested on two publicly available databases: one containing data from 76 subjects and another from 26 subjects. It was assessed for both identification and verification purposes. Notably, the second database included subjects with clinically confirmed cardiac irregularities, specifically atrial premature contraction arrhythmia. The experimental results on both databases revealed impressive outcomes, with high identification accuracy (98% and 99.85%, respectively). Additionally, in their work, Islam and colleagues (mentioned as [36]) put forth an unsupervised outlier detection method designed to identify the most regular heartbeats from a given dataset. To address the impact of heart rate variability (HRV), they aligned the morphology of the selected heartbeats using a piecewise-uniform approach. Subsequently, they constructed a template by averaging the aligned heartbeats and represented it in a lower-dimensional space through principal component analysis (PCA). The authentication performance of this template was thoroughly evaluated using a database consisting of data from 112 individuals collected across multiple sessions with a handheld ECG device. The experimental results demonstrated that the proposed template surpassed all other templates in terms of authentication accuracy.

3. Proposed Method

The proposed method's block diagram, as depicted in Figure 2, is a comprehensive approach designed for the secure transmission and extraction of ECG (Electrocardiogram) data over a network. At the beginning of the process, an ECG signal is recorded from a patient. This ECG signal represents the electrical activity of the heart and is a critical component in diagnosing various cardiac conditions. The recorded ECG signal is concealed within a cover image using a technique known as RDH. RDH allows for the embedding of data (in this case, the ECG signal) into another medium (the cover image) in such a way that the original cover image can be completely recovered. This step essentially combines the visual data (the cover image) with the ECG data. After hiding the ECG signal within the cover image, the combined image is encrypted using a secure encryption algorithm. Encryption ensures that the data is protected during transmission, making it challenging for unauthorized parties to access or tamper with the information. The encrypted image, which now contains the ECG data in a concealed form, is transmitted over a network. This network could be a local hospital network or a secure channel for telemedicine applications. The encryption ensures the confidentiality and integrity of the data during transit. At the receiver's end, the inverse operations are performed to retrieve the ECG image and subsequently identify the patient. The receiver applies the inverse of the encryption algorithm to decrypt the received image, revealing the hidden ECG signal and the original cover image. To identify the patient from the extracted ECG image, a RESNET-50 model is employed. RESNET-50 is a pre-trained deep learning model, typically used for image classification tasks. In this case, it is utilized as a template matching or pattern recognition tool. The RESNET-50 model compares the received ECG image with a set of template ECG images stored in its database. These template images serve as references for patient identification. The model's neural network architecture helps in recognizing patterns and features within the ECG image, which are then compared to the template images. Based on the comparison, the system produces a patient identification result. If a match is found between the received ECG image and a template ECG image, the patient is positively identified. This can be useful for maintaining patient records, ensuring data privacy, and confirming the identity of the patient associated with the ECG data.

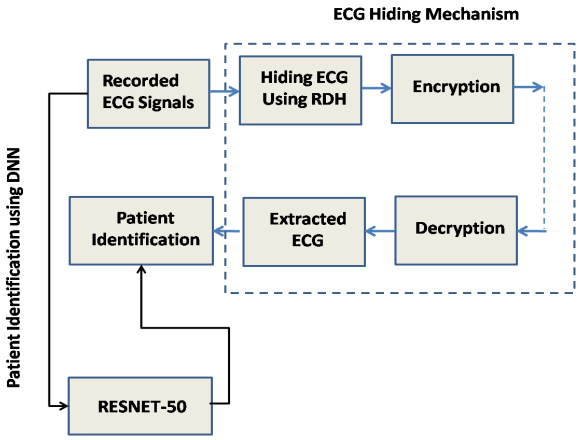

Figure 2. Block diagram of the proposed ECG based patient identification with RDH scheme

3.1 Reversible Data Hiding Mechanism

In the proposed method, ECG is used as confidential data, combined with sensor data, and incorporated into the ECG image. Given that ECG and other data are concealed within the cover image, it's imperative that the embedding capacity remains high without compromising the cover image's quality. This work introduces a reversible data hiding technique with excellent PSNR and embedding capacity for concealing ECG and sensor data.

The initial step involves image partitioning into two distinct segments, denoted as A and B. Subsequently, the Least Significant Bits (LSB) of segment A are embedded into segment B using the RDH process. This enables the utilization of segment B as a vessel for the concealed data. Finally, the restructured image undergoes an encryption process to enhance its security (see Figure 3). To provide a more comprehensive understanding, let's delve into the specific details of each of these processes:

3.1.1 Image Partitioning

The original image is divided into two separate parts, labelled as segments A and B. This partitioning is a critical initial step that separates the image into distinct components to facilitate the subsequent data embedding process. Take into consideration a distinctive image denoted as 'I.' This image is an 8-bit gray-scale representation, where each pixel '$P_{u,v}$' falls within the range of values from 0 to 255. The image has dimensions M×N. As a starting point, this image is divided into overlapping blocks, with each block being overlapped by both the preceding and subsequent blocks. The level of smoothness inherent to each individual block is quantified through the following expression:

$$S=\sum_{u=2}^{r}\sum_{v=2}^{N-1}\left|P_{u,v}-\frac{P_{u-1,v-1}+P_{u-1,v}+P_{u-1,v+1}+P_{u,v-1}+P_{u,v+1}+P_{u+1,v-1}+P_{u+1,v}+P_{u+1,v+1}}{8}\right| \quad (1)$$

The parameter 'S' serves as an indicator of texture characteristics within the image. Specifically, when 'S' assumes a value of 0, it signifies a uniform and consistent texture across the block. Conversely, higher 'S' values indicate the presence of more intricate and complex textures. Among these blocks, the one exhibiting the highest 'S' value is designated as 'A' and is positioned ahead of another block referred to as 'B,' as visually depicted in Figure 3.

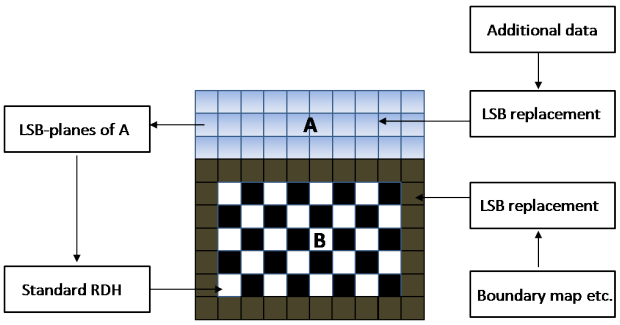

Figure 3. Image partitioning and embedding process diagram

3.1.2 LSB Embedding Using RDH

In this stage, the Least Significant Bits (LSB) of segment 'A' are discreetly embedded into segment 'B' through a process known as RDH. RDH is a technique that allows data to be hidden within an image in a manner that permits complete restoration of the original image without any loss of data. This process ensures that segment 'B' can function as a container for concealed data, while still preserving the integrity of both segments 'A' and 'B' (Figure 3).

3.1.3 Image Rearrangement

After the LSB embedding is completed, the image undergoes a reconfiguration process. This step ensures that the image is appropriately restructured, taking into account the changes made during the embedding process (Figure 3). It is crucial to maintain the overall structure and visual quality of the image while accommodating the embedded data.

3.1.4 Image Encryption

To bolster the security of the concealed data and the entire image, encryption is applied. This process involves the transformation of the image data into a coded format, making it accessible only to authorized individuals with the decryption key. Image encryption adds an additional layer of protection to safeguard both the concealed information and the integrity of the image. By meticulously following these steps, the proposed method achieves the seamless embedding of data into images while preserving data integrity, ensuring security, and enabling the subsequent retrieval of the concealed information without any loss or distortion. These processes collectively contribute to the effectiveness and reliability of the data hiding technique.

3.1.5 Self-Reversible Embedding in part B of image

This procedure relies on estimating pixel errors and performing histogram shifts. During this step, the least significant bits (LSB) of A are incorporated into B through the employment of the RDH mechanism. The interpolation value plays a pivotal role in the calculation of each white pixel. This interpolation value is obtained as

$$P'_{u,v}=W_1P_{u-1,v}+W_2P_{u+1,v}+W_3P_{u,v-1}+W_4P_{u,v+1} \quad (2)$$

The error is evaluated as

$$\varepsilon_{u,v}=P_{u,v}-P'_{u,v} \quad (3)$$

where the weight W_i, $1\le i\le 4$.

In general, the error for any pixel value $P_{u,v}$ is evaluated using $\varepsilon_{u,v}=P_{u,v}-P'_{u,v}$, next histogram shifting is done to embed data.

3.1.6 Histogram Shift Process in part B of image

Next, the estimation errors of the black pixels are determined by considering the neighbouring white pixels. Subsequently, a fresh estimation error sequence is produced, capable of accommodating the messages. In the considered interpolation method, a pixel's value from its surrounding

pixels is first estimated and interpolation errors is evaluated as

$$\varepsilon = P - P' \tag{4}$$

The interpolation values of pixels P are represented by parameter P' in the above equation.

The shifted Histogram is first divided into two distinct parts. Assume that γ_{LP} and γ_{RP} are the corresponding values of the two interpolation-errors histogram peak points, respectively, and are expressed as

$$\begin{cases} \gamma_{LP} = \arg \max\limits_{\varepsilon \in E} hist(\varepsilon) \\ \gamma_{RP} = \arg \max\limits_{\varepsilon \in E - \{\gamma_{LP}\}} hist(\varepsilon) \end{cases} \tag{5}$$

where, hist(ε) is histogram of ε, and E is the ensemble of interpolation-error. Considering, $\gamma_{LP} < \gamma_{RP}$ and dividing interpolation-errors as Right and left interpolation-errors depending on $\varepsilon \geq \Omega_{RP}$ or $\varepsilon \geq \Omega_{LP}$ respectively.

The additive interpolation-error expansion (ε') can be written as

$$\varepsilon' = \begin{cases} \varepsilon + sign(\varepsilon) \times b, & \varepsilon = \gamma_{LP} \text{ or } \gamma_{RP} \\ \varepsilon + sign(\varepsilon) \times 1, & \varepsilon \in (\gamma_{LP}, \gamma_{LN}) \cup (\gamma_{RP}, \gamma_{RN}) \\ \varepsilon, & else \end{cases} \tag{6}$$

where,

$$\begin{cases} \gamma_{LN} = \arg \min\limits_{\varepsilon \in LE} hist(\varepsilon) \\ \gamma_{RN} = \arg \min\limits_{\varepsilon \in RE} hist(\varepsilon) \end{cases} \tag{7}$$

And where b is the bit to be embedded, e' is the expanded interpolation-error, and sign(.) function takes value +1 in case of right interpolation-errors (RE) and -1 in case of left interpolation-errors (LE).

The interpolation errors are increased, and the watermarked pixels are transformed into

$$P'' = P' + \varepsilon' \tag{8}$$

Once γ_{LP}, γ_{LN}, γ_{RP} and γ_{RN} are evaluated, secret data can be recovered as

$$b = \begin{cases} 0, & \varepsilon' = \gamma_{LP} \text{ or } \gamma_{RP} \\ 1, & \varepsilon' = \gamma_{LP} - 1 \text{ or } \gamma_{RP} + 1 \end{cases} \tag{9}$$

The initial interpolation errors can be restored by employing

$$\varepsilon = \begin{cases} \varepsilon' - sign(\varepsilon') \times b, & \varepsilon' \in [\gamma_{LP} - 1, \gamma_{LP}] \cup [\gamma_{RP}, \gamma_{RP} + 1] \\ \varepsilon' - sign(\varepsilon') \times 1, & \varepsilon' \in [\gamma_{LN}, \gamma_{LP} - 1] \cup [\gamma_{RP} + 1, \gamma_{RN}] \\ \varepsilon, & else \end{cases} \tag{10}$$

The original pixel value is evaluated as

$$P = P' + \varepsilon \tag{11}$$

In this work, in the interpolation pixels at angles 0^0, 45^0, 90^0 and 135^0 are considered.

Examining a 3×3 section of an image, where the pixel values range from P1 to P9, and considering four directions: 0°, 45°, 90°, and 135° (as shown in Figure 4), the objective is to estimate the pixel value at position "x" using an estimated value of "y." The mean value of surrounding pixel of P_5 is

$$P_{mean} = \frac{1}{8}\left[\sum_{i=1, i\neq 5}^{9} P_i\right] \tag{12}$$

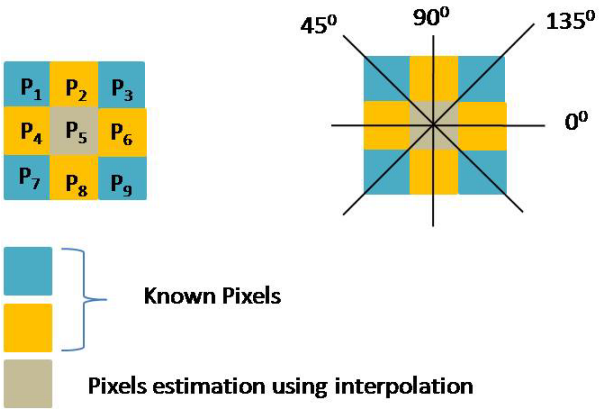

Figure 4. Determination of the central pixel by utilizing the neighbouring pixels

Defining average value in 0^0, 45^0, 90^0 and 135^0 degree respectively as

$$P_0 = \frac{1}{2}[P_4 + P_6], \; P_{45} = \frac{1}{2}[P_1 + P_9], \; P_{90} = \frac{1}{2}[P_2 + P_8]$$

$$\text{and } P_{135} = \frac{1}{2}[P_3 + P_7] \tag{13}$$

Defining sets in various directions as

$$S_0 = [P_4, P_6, P_0], \; S_{45} = [P_1, P_9, P_{45}], \; S_{90} = [P_2, P_8, P_{90}]$$

$$\text{and } S_{135} = [P_3, P_7, P_{135}] \tag{14}$$

The variance in 0^0, 45^0, 90^0 and 135^0 directions are

$$\sigma^2(e_0) = \frac{1}{3}\sum_{u=1}^{3}\left(S_0(u) - P_{mean}\right)^2$$

$$\sigma^2(e_{45}) = \frac{1}{3}\sum_{u=1}^{3}\left(S_{45}(u) - P_{mean}\right)^2$$

$$\sigma^2(e_{90}) = \frac{1}{3}\sum_{u=1}^{3}\left(S_{90}(u) - P_{mean}\right)^2$$

$$\sigma^2(e_{135}) = \frac{1}{3}\sum_{u=1}^{3}\left(S_{135}(u) - P_{mean}\right)^2 \tag{15}$$

The weight in 0^0, 45^0, 90^0 and 135^0 is given by

$$w_0 = \frac{\sigma_{90}^2}{\sigma_0^2 + \sigma_{90}^2}, \; w_{45} = \frac{\sigma_{135}^2}{\sigma_{45}^2 + \sigma_{135}^2}, \; w_{90} = \frac{\sigma_0^2}{\sigma_0^2 + \sigma_{90}^2}$$

$$\text{and } w_{135} = \frac{\sigma_{45}^2}{\sigma_{45}^2 + \sigma_{135}^2} \tag{16}$$

We can acquire the approximated pixel value using

$$\hat{P} = w_0 P_0 + w_{45} P_{45} + w_{90} P_{90} + w_{135} P_{135} \quad (17)$$

The estimated error is

$$e = P - P' \quad (18)$$

3.1.7 Image Encryption

After completing the rearrangement of the self-embedded image, represented by ***I***, we can encrypt ***I*** to form the encrypted image, denoted by Ξ. The encryption version of ***I*** is effectively obtained with the aid of a stream cypher. Consider the case where a grey image with pixels varying from 0 to 255 can be expressed by 8 bits. $I_{i,j}(0), I_{i,j}(1)$, ..., $I_{i,j}(7)$ in such a manner that

$$I_{i,j}(z) = \left\lfloor \frac{I_{i,j}}{2^z} \right\rfloor \bmod 2, \qquad z = 0,1,...,7. \quad (19)$$

Exclusive-or operation can be used to estimate the encrypted bits.

$$\Xi_{i,j}(z) = I_{i,j}(z) \oplus r_{i,j}(z) \quad (20)$$

In above, $r_{i,j}(z)$ is generated using basic encryption cipher.

3.1.8 Generation of Decrypted Image

The decrypted image I'' which is made up of A'' and B'' can be decrypted using steps below:

Step 1: The owner decrypts the image using the encryption key while leaving the LSB-planes of A_E (encrypted version of A).The decrypted form of Ξ' can be calculated by

$$I''_{i,j}(z) = \Xi'_{i,j}(z) \oplus r_{i,j}(z) \quad (21)$$

and

$$I''_{i,j} = \sum_{z=0}^{7} I''_{i,j}(z) \times 2^z, \quad (22)$$

Above the parameters $\Xi'_{i,j}(z)$ and $I''_{i,j}(z)$ represents the binary bits of $\Xi'_{i,j}(z)$ and $I''_{i,j}(z)$, acquired through (19) respectively.

Step 2: In the marginal zone of B'' extract Ω_{SR} and Ω_{ER} .The data embedded plain image is generated by rearranging A'' and B'' it to its original form. With the exception of the LSB-planes of A, the annotated decrypted image is indistinguishable from changed I. In comparison to the original image I'' it preserves perceptual transparency.

3.1.9 Image Restoration and Data Extraction

Using the procedure given below, original image and embedding data can be extracted using the steps given below:

Step 1: First LSB-planes of A'' is decoded, along with data hiding key; this process is continued till the end label.

Step 2: Extract γ_{LN}, γ_{RN}, γ_{LP}, γ_{RP} *R*, *I*, and boundary map using the LSB of the marginal area of, B'' After that, scan to complete the steps mentioned below.

Step 3: Proceed to Step 5 if *R*= 0, indicating that black pixels are not involved in the data embedding operation.

Step 4: Evaluate the black pixels' $B''_{i,j}$ estimating errors $\varepsilon'_{i,j}$. If $B''_{i,j} \in [1,254]$ and $\varepsilon'_{i,j}$ equals to any one of them γ_{LN}, γ_{RN}, γ_{LP}, γ_{RP} retrieve the estimating error and initial pixel value in extract the data embedding bits. If, $B''_{i,j} \in \{0,255\}$ this belongs to the boundary map'sfor bit *b*. If the value of bit *b* is zero 0, leave this step otherwise, proceed as before for $B''_{i,j} \in [1,254]$ do this process until all of the ECG payload has been removed.

Step 5: Repeat step 4, for white pixels and if the removed bits are pixels LSBs in the marginal region, restore themat that time only.

Step 6: Repeat Step 2 through 5*I*-1 rounds, merging each extracted bit to create A's LSB-planes it is done before B is fully recovered.

Step 7: For recovering the original cover image *I*, replace A'', LSB-planes with the B'' original extracted bits OF ECG data.

Once the cover image and hidden ECG data have been successfully extracted, the subsequent step involves leveraging advanced machine learning techniques for ECG patient identification. In this context, the RESNET 50 model, a state-of-the-art deep learning architecture renowned for its exceptional performance in image recognition tasks, emerges as a pivotal tool. The RESNET 50 model, comprising numerous layers of neural networks, possesses the capability to discern intricate patterns and features within images with remarkable accuracy. By feeding the extracted ECG data into the RESNET 50 model, the system can effectively analyze and identify unique patient characteristics encoded within the electrocardiogram signals.

The utilization of the RESNET 50 model in ECG patient identification represents a significant advancement in healthcare technology, offering unparalleled precision and reliability in discerning individual cardiac signatures. Through its sophisticated algorithms and extensive training on vast datasets, the RESNET 50 model can discern subtle

variations in ECG waveforms that serve as distinctive markers for each patient. These distinctive features encompass a myriad of factors, including heart rate variability, waveform morphology, and rhythm irregularities, among others.

Moreover, the integration of the RESNET 50 model into the ECG patient identification process enhances not only the accuracy but also the efficiency of the overall system. By automating the identification process, healthcare professionals can expedite diagnosis and treatment decisions, thereby improving patient outcomes and reducing healthcare costs. Additionally, the RESNET 50 model's ability to adapt and learn from new data ensures continuous improvement in identification accuracy over time, further enhancing the reliability of the system.

3.2 RESNET-50 for Patient Identification

In this work, ResNet-50 model is used for patient identification using ECG employing CNN architecture as shown in Figure 5. ResNet-50 is a specific variant of the ResNet (Residual Network) architecture that has 50 layers, making it deep and capable of capturing intricate features in ECG images. The ResNet-50 architecture is known for its deep structure, featuring 50 layers or more, and it incorporates a specialized building block called a "residual block." This block includes a convolution operation that plays a central role in the network's ability to learn and represent complex features from input images.

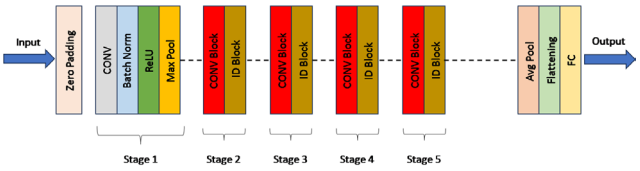

Figure 5. Detailed diagram of ResNet 50 architecture

Convolution Layer

The convolution operation in ResNet-50 is primarily associated with convolutional layers, which are the foundational building blocks for processing image data. Convolutional layers are used to detect various patterns, textures, and features within an image. The primary objective of convolution is to apply a set of learnable filters (kernels) to the input image. Here input data is differentiated ECG which is added in vector form.

Feature Extraction

In ResNet-50, the convolutional layers extract low-level to high-level features from the ECG data. As the network progresses through its layers, it learns to identify increasingly abstract and informative features which are helpful in patient identification.

Stacked Residual Blocks

One of the key innovations in the ResNet architecture is the use of residual blocks. These blocks are designed to make it easier for the network to learn and optimize deep representations. Each residual block typically contains multiple convolutional layers and batch normalization. The convolution operation within these blocks is responsible for learning a residual function.

Residual Learning

The central idea behind residual blocks is residual learning. In a standard deep neural network, each layer is expected to learn the underlying mapping directly. In contrast, a residual block learns the residual mapping—the difference between the input and the desired output. The convolution operation within the residual block is used to model this residual function. Mathematically, this is expressed as:

$$F(x) = H(x) - x \tag{23}$$

where, F(x) is the learned residual function, H(x) is the desired output and x is the input.

Shortcut Connections

To facilitate residual learning, ResNet-50 employs "shortcut connections" or "skip connections" that directly connects the input to the output of a residual block. This connection allows gradients to flow more easily during training, which is particularly important in very deep networks.

End-to-End Training

The entire ResNet-50 network, including its convolutional layers, residual blocks, and fully connected layers, is trained end-to-end using a loss function and a large dataset. The convolution operations in each residual block contribute to the network's ability to represent and learn features effectively.

Loss Function

Binary cross-entropy is a loss function commonly used in various binary classification tasks, including ECG-based patient identification. In this context, binary cross-entropy serves as a fundamental component of the training and evaluation of machine learning and deep learning models. ECG-based patient identification typically involves determining whether an ECG signal corresponds to a specific patient or not. In this binary classification task, the two classes are often labeled as "patient X" and "not patient X." Binary cross-entropy is used as the loss function during the training process. Here's how it works:

1. For each ECG signal, the model predicts a probability that the signal belongs to "patient X." This probability typically ranges between 0 and 1.

2. The binary cross-entropy loss function quantifies the dissimilarity between the predicted probabilities and the actual binary labels. It measures how well the model's predictions match the true labels.
3.

The binary cross-entropy loss for a single data point is calculated as follows:

$$L(y,\hat{y}) = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1-y_i)\log(1-\hat{y}_i)] \quad (24)$$

$L(y,\hat{y})$ is the binary cross-entropy loss. y is the true binary label (1 for "patient X," 0 for "not patient X"). $\hat{y}$ is the predicted probability that the ECG signal belongs to "patient X." Binary cross-entropy is well-suited for ECG-based patient identification because it quantifies the alignment of predicted probabilities with binary labels, allowing models to effectively distinguish between different patients based on their ECG signals.

4. Results

In the first results section, RDH scheme results are detailed, whilst in the second section, ECG-based patient identification results are detailed.

4.1 RDH Scheme Results

The methodology outlined in this research paper will undergo testing using publicly accessible standard image databases for RDH scheme, as in [27-28]. These image databases consist of images, each having a resolution of 512×512 pixels with an 8-bit colour depth. To assess the efficacy and performance of the proposed scheme, several performance metrics will be employed. These metrics are essential for quantitatively evaluating the quality and effectiveness of the proposed method. The specific performance metrics that will be used include:

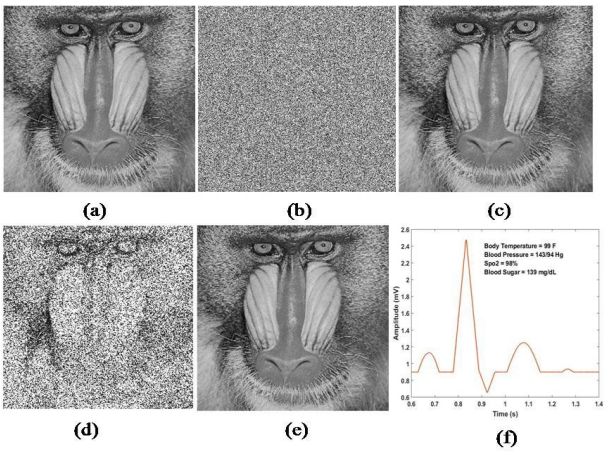

Figure 6. Image hiding and recovery using RDH process

Figure 6 provides a comprehensive visual representation of the various stages involved in the data embedding and retrieval process, particularly focusing on the encryption and decryption of images, as well as the extraction of the hidden ECG image. The original considered Baboon image is shown in Figure 6(a), the image in figure 76(b) represents the Baboon image after undergoing the data embedding and encryption process to protect its contents. After decryption, the image is restored to its original form, as shown in figure 6(c). The image in figure 6(d) showcases the differences between the original and decrypted images, highlighting any variations that may have occurred during encryption and decryption. In figure 6(e) image displays the successful recovery of the original image after decryption, illustrating that the decryption process has been executed accurately. Finally, in figure 6(f) the recovered ECG image is shown.

In figure 7, PSNR for various images at different bit per pixel (bpp) rates are shown. PSNR is a crucial metric used to evaluate the quality and fidelity of images after undergoing data embedding. The results indicate that for lower embedding rates, such as 0.05 bpp, the PSNR values are generally high, hovering around 60 dB for most images. However, the 'Baboon' image exhibits a slightly lower PSNR of around 54.5 dB at this embedding rate. As the bpp rate increases to 0.5, the PSNR values decrease, averaging around 46 dB. This reduction in PSNR is expected as more data is embedded, potentially introducing noise or artifacts into the images. For 'Baboon' and 'Pepper' images, the maximum allowable embedding bpp rates are noted. 'Baboon' image PSNR falls below 25 dB if the bpp exceeds 0.9, indicating a significant loss in image quality. Similarly, the 'Pepper' image has a maximum allowable embedding bpp rate of 0.9. These findings highlight the trade-off between data embedding capacity and image quality, with higher bpp rates leading to reduced PSNR values, which may impact image fidelity. Careful consideration of the desired balance between data capacity and image quality is essential when employing data embedding techniques.

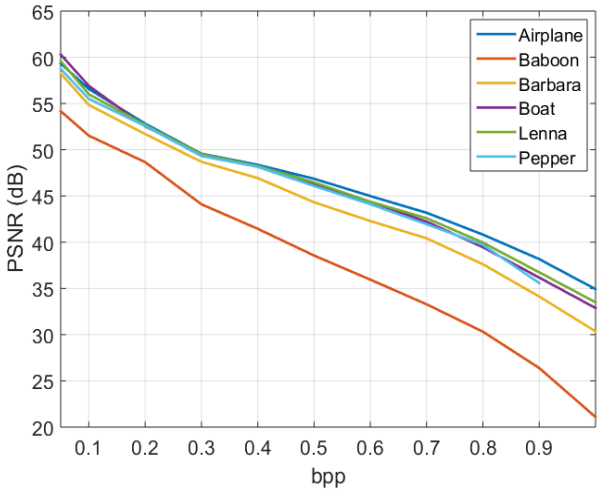

Figure 7. PSNR (dB) vs. bpp for all six images

In Figure 8, the boundary map is presented for the considered images. Up to a bpp of 0.8, the boundary map remains at 0 for the 'Airplane,' 'Barbara,' 'Boat,' and 'Lenna' images. It's worth mentioning that in the considered method, the marginal area has a size of 512×4×4=8192 bits. Therefore, for the 'Baboon' image, the maximum allowable bpp is 0.9 Similarly, for the 'Peppers' image, the maximum bpp is 0.8. To put this into context, the maximum allowable bpp is compared to previous works. In the work of Ma et al. [27], the maximum bpp is 0.5. In Sah et al.'s work [28], it is 0.75 while in case of Tripathi et. al [29] it is 0.95. In this current work, the maximum allowable bpp has been extended to 1. This indicates that the proposed method offers a higher data embedding capacity while maintaining acceptable image quality, making it suitable for various applications where a balance between data capacity and image fidelity is required.

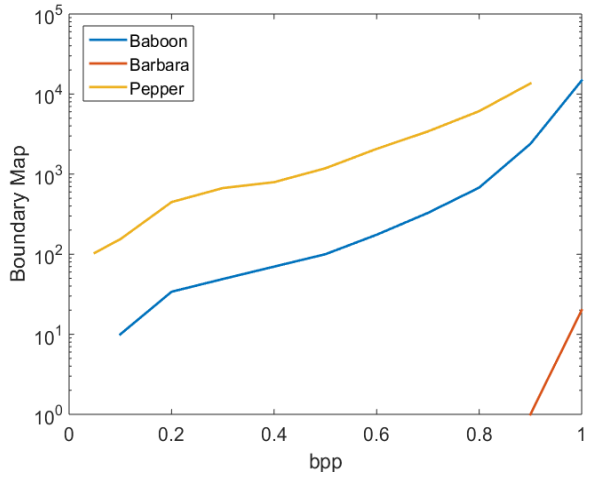

Figure 8. Boundary map vs. bpp for all six images

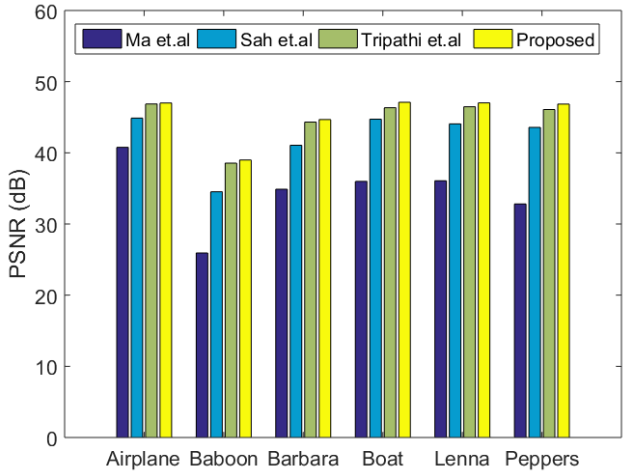

Figure 9. PSNR vs. all six images (bpp=0.5)

Figure 9 provides a comprehensive overview of the for all six images while comparing the results with those obtained from the works of Kede Ma et al. [27], Sah et al. [28] and Tripathi et. al [29]. The PSNR values are specifically presented at a bit per pixel (bpp) rate of 0.5. In this comparison, we observe significant differences in PSNR values between the proposed method and Kede Ma et al.'s work [27]. Notably, for the 'Baboon' and 'Peppers' images, the PSNR difference is more than 10 dB, indicating a substantial improvement in image quality in favour of the proposed approach. Furthermore, when comparing with Sah et al.'s work [28], the difference in PSNR is approximately 3 dB, signifying a notable enhancement in image quality while maintaining competitive performance.

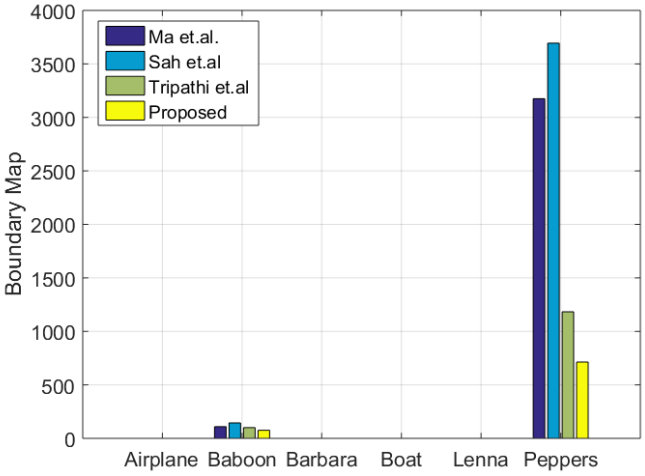

Figure 10. Boundary Map vs. all six images (bpp=0.5)

Figure 10 provides an insightful view of the boundary map results for all six images, offering a comparative analysis with the works of Kede Ma et al. [27] , Sah et al. [28] and Tripathi [29]. In the case of the 'Airplane,' 'Boat,' 'Barbara,' and 'Lenna' images, all three schemes, including the proposed approach, exhibit a boundary map value of zero. This indicates that the boundary area remains unaffected in these scenarios, emphasizing the effectiveness of each method in preserving the integrity of the image's outer regions. However, when considering the 'Baboon' image, Kede Ma et al.'s work [27] yields a boundary map value of 109, Sah et al.'s work [28] results in a value of 196, and the proposed method achieves a boundary map value of 100. This demonstrates that the proposed approach maintains a competitive boundary map value while ensuring a good balance between data embedding capacity and image quality. Similarly, for the 'Peppers' image, Kede Ma et al.'s work [27] produces a boundary map value of 3,175, Sah et al.'s work [28] results in a value of 3,694, and the proposed method attains a boundary map value of 1,183. These findings underscore the effectiveness of the proposed method in significantly reducing the boundary map value, indicating a notable improvement in image preservation near the image boundaries.

Figure 11 provides valuable insights into the average runtime of all six images when considering the maximum allowed embedding rate. The results are compared with the runtimes achieved by Ma et al.'s work [27] and Sah et al.'s work [28]. In Ma et al.'s work [27], the average runtime for

the selected images is recorded as 13.41 seconds, while in Sah et al.'s work [28], and it is slightly lower at 13.29 seconds. In the case of Tripathi et al. [29] the runtime is 9.73 seconds. However, the proposed scheme demonstrates significantly reduced runtime, with an average of 9.11 seconds. The improved runtime efficiency in the proposed scheme can be attributed to the utilization of compressed cover and secret images. These compressed images result in faster processing, contributing to the overall reduction in runtime.

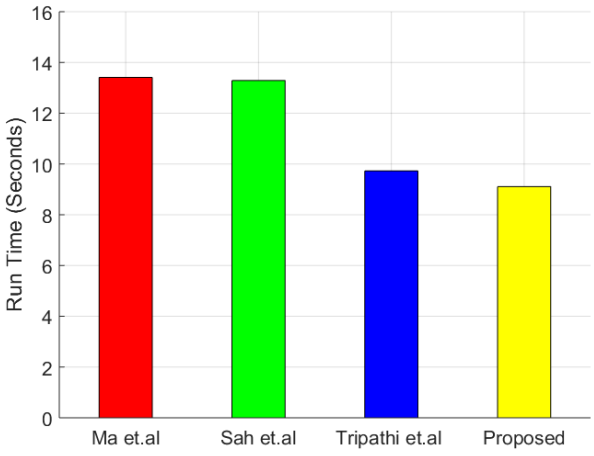

Figure 11. Run time comparison

In summary, the proposed scheme outperforms the compared methods in terms of runtime efficiency, highlighting its effectiveness and practicality for data embedding applications.

4.2 ECG Based Patient Identification Results

MITDB, which stands for the MIT-BIH Arrhythmia Database [37], is a widely recognized and extensively utilized resource in the field of electrocardiography (ECG). This database comprises a rich collection of annotated ECG recordings, featuring various types of cardiac arrhythmias. ECG-ID and Heart-print are multisession database (Table 1). This takes into account variability in heart rhythms.

The MITDB original dataset comprises 47 subjects, and the algorithm's performance may be impacted when analyzing both healthy and arrhythmic subjects. This is because some recordings exhibit cardiac abnormalities affecting the QRS complex and influencing the P wave. Bassiouni et al. [40] and Tang et al. [41] employed artificial neural networks (ANN) as classifiers, achieving accuracy rates of 96.67% and 91.1%, respectively. Abdeldayem et al. [43] and Zhang et al. [42] utilized convolutional neural networks (CNN) as classifiers and obtained accuracy rates of 96.5% and 91.1%, respectively. In contrast, our proposed method boasts a PIDR accuracy of 99.98%.

The ECG-ID dataset, as presented by Zhao et al. [44] and AlDuwaile, and Islam [45], as well as the Heartprint dataset, reported by Islam et al. [39], offer valuable insights into the performance of various models in ECG-based biometric identification.

In the context of the ECG-ID dataset, several models underwent evaluation, including CNN, GoogLeNet, ResNet, EfficientNet, MobileNet, Small CNN, and LSTM. Among these models, ResNet and LSTM delivered robust performance, achieving accuracy rates of 97.28% and 97.69%, respectively. This suggests that deep learning models like ResNet and LSTM are well-suited for ECG-based identification tasks, possibly due to their capacity to capture intricate patterns within ECG signals. GoogLeNet also exhibited commendable accuracy at 93.87%.

Table 1: Comparison of the proposed method with state of arts methods under different databases

Author	Classification Method	Accuracy%
MITDB [37]		
Bassiouni et al. [40]	ANN	96.67
Tang et al. [41]	ANN	91.7
Zhang et al. [42]	CNN	91.1
Abdeldayemet al. [43]	CNN	96.5
Gupta and Awasthi [7]	LSTM	98.95
Proposed	RESNET-50	99.98
ECG-ID [38]		
Zhao et al. [44]	CNN	96.63
AlDuwaile, and Islam [45]	GoogLeNet	93.87
	ResNet	97.28
	EfficientNet	83.10
	MobileNet	87.51
	Small CNN	94.18
Gupta and Awasthi [7]	LSTM	98.94
Proposed	RESNET-50	99.94
Heartprint [39]		
Islam et al. [39]	CNN (Mixed Session)	100
	CNN (Cross Session)	69.35
Proposed	RESNET-50 (Mixed Session)	100
	RESNET-50 (Cross Session)	93.21

In contrast, EfficientNet and MobileNet yielded lower accuracy rates of 83.10% and 87.51%, respectively, indicating their limited effectiveness for this specific task.

In the case of the Heartprint dataset, the proposed models encompass CNN (Mixed Session), CNN (Cross Session), LSTM (Mixed Session), and LSTM (Cross Session). Remarkably, the CNN (Mixed Session) and LSTM (Mixed Session) models achieved flawless accuracy rates of 100%, underscoring their precision in identifying individuals across multiple sessions. However, when faced with a cross-session scenario, where the model must recognize individuals in sessions different from those used for training, accuracy rates dipped. Specifically, CNN (Cross Session) achieved an accuracy of 69.35%, while LSTM (Cross Session) demonstrated improved accuracy at 89.21%. These findings indicate that while some models excel in recognizing

individuals within the same session, cross-session identification poses a more challenging task.

The accuracy of person detection in ECG-based systems across multiple sessions can be compromised by several key factors. Firstly, the inherent variability in ECG signals between sessions, influenced by physiological fluctuations and environmental conditions, poses a significant challenge. This variability can manifest in differences in signal morphology and amplitude, hindering the accurate generalization of detection algorithms. Secondly, the presence of noise and artifacts in ECG signals, such as muscle noise or electrode motion artifacts, obscures the underlying waveform, impeding the identification of individual characteristics. Additionally, variations in signal quality due to factors like electrode contact and skin impedance can further degrade detection accuracy. Moreover, temporal misalignment between ECG signals from different sessions, stemming from differences in recording duration or sampling rate, introduces discrepancies in signal timing that complicate cross-session analysis. Furthermore, the non-stationary nature of ECG signals, characterized by changes in heart rate and physiological state, poses a challenge to establishing consistent features for person detection across sessions. Addressing these challenges requires robust preprocessing techniques, feature extraction methods that capture discriminative characteristics, and machine learning models trained on diverse datasets to improve generalization performance in cross-session analysis.

5. Conclusions

This paper proposes a multi-layered approach with reversible data hiding using ECG, which has provided valuable insights into the vital area of safeguarding patient data in the modern digital landscape. The research has demonstrated the efficacy of a multi-layered security approach incorporating reversible data hiding techniques leveraging Electrocardiogram (ECG) data. The findings from our investigation highlight the significance of protecting sensitive patient information and medical data, especially in the context of electronic health records and telemedicine, where data breaches and unauthorized access pose significant risks to patient privacy. Our study offers a promising solution by utilizing ECG data, which can serve as a unique and secure identifier, to enhance data security. The results presented in this paper showcase the effectiveness of various data embedding RDH mechanism and machine learning and deep learning models in ECG-based biometric identification. Notably, ResNet model exhibited remarkable accuracy rates, demonstrating their potential for robust patient data security solutions. Additionally, the performance differences in cross-session scenarios, as revealed by the Heartprint dataset, emphasize the challenges that must be addressed in securing patient data across various healthcare settings.

References

[1] Siraj, Muhammed, Mohd Izuan Hafez Ninggal, Nur Izura Udzir, Muhammad Daniel Hafiz Abdullah, and Aziah Asmawi. "Smart-Contract Privacy Preservation Mechanism." *EAI Endorsed Transactions on Scalable Information Systems* 10, no. 6 (2023).

[2] Gupta, Manish, and Rajendra Kumar Dwivedi. "Fortified MapReduce Layer: Elevating Security and Privacy in Big Data." *EAI Endorsed Transactions on Scalable Information Systems* 10, no. 6 (2023).

[3] Al-Jubori, Hussein N., and Izzat Al-Darraji. "Tools and Process of Defect Detection in Automated Manufacturing Systems." *EAI Endorsed Transactions on Scalable Information Systems* 10, no. 6 (2023).

[4] Pattnaik, Lal Mohan, Pratik Kumar Swain, Suneeta Satpathy, and Aditya N. Panda. "Cloud DDoS Attack Detection Model with Data Fusion & Machine Learning Classifiers." *EAI Endorsed Transactions on Scalable Information Systems* 10, no. 6 (2023).

[5] Saxena, Drishti, and Prabhat Patel. "Energy-efficient clustering and cooperative routing protocol for wireless body area networks (WBAN)." *Sādhanā* 48, no. 2 (2023): 71.

[6] Parveen, Nikhat, Manisha Gupta, Shirisha Kasireddy, Md Shamsul Haque Ansari, and Mohammad Nadeem Ahmed. "ECG based one-dimensional residual deep convolutional auto-encoder model for heart disease classification." *Multimedia Tools and Applications* (2024): 1-27.

[7] Gupta, Praveen Kumar, and Vinay Avasthi. "Person identification using electrocardiogram and deep long short term memory." *International Journal of Information Technology* 15, no. 3 (2023): 1709-1717.

[8] Shiu, Chih-Wei, Yu-Chi Chen, and Wien Hong. "Encrypted image-based reversible data hiding with public key cryptography from difference expansion." *Signal Processing: Image Communication* 39 (2015): 226-233.

[9] Rakhra, Manik, Rajan Kumar, and Himdweep Walia. "A Review on Data hiding using Steganography and Cryptography." In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1-4. IEEE, 2021.

[10] Kumar, Sanjay, Anjana Gupta, and Gurjit Singh Walia. "Reversible data hiding: A contemporary survey of state-of-the-art, opportunities and challenges." *Applied Intelligence* (2022): 1-34.

[11] Gao, Guangyong, Shikun Tong, Zhihua Xia, Bin Wu, Liya Xu, and Zhiqiang Zhao. "Reversible data hiding with automatic contrast enhancement for medical images." *Signal Processing* 178 (2021): 107817.

[12] Wang, Weiqing. "A reversible data hiding algorithm based on bidirectional difference expansion." *Multimedia Tools and Applications* 79, no. 9 (2020): 5965-5988.

[13] Wu, Hao-Tian, Xin Cao, Ruoyan Jia, and Yiu-Ming Cheung. "Reversible data hiding with brightness preserving contrast enhancement by two-dimensional histogram modification." *IEEE Transactions on Circuits and Systems for Video Technology* 32, no. 11 (2022): 7605-7617.

[14] Hou, Jiacheng, Bo Ou, Huawei Tian, and Zheng Qin. "Reversible data hiding based on multiple histograms

modification and deep neural networks." *Signal Processing: Image Communication* 92 (2021): 116118.
[15] Chang, Qi, Xiaolong Li, and Yao Zhao. "Reversible data hiding for color images based on adaptive three-dimensional histogram modification." *IEEE Transactions on Circuits and Systems for Video Technology* 32, no. 9 (2022): 5725-5735.
[16] He, Wenguang, Gangqiang Xiong, and Yaomin Wang. "Reversible data hiding based on adaptive multiple histograms modification." *IEEE Transactions on Information Forensics and Security* 16 (2021): 3000-3012.
[17] Jhong, Chun-Liang, and Hsin-Lung Wu. "Grayscale-invariant reversible data hiding based on multiple histograms modification." *IEEE Transactions on Circuits and Systems for Video Technology* 32, no. 9 (2022): 5888-5901.
[18] Shaik, Ahmad, and V. Thanikaiselvan. "Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification." *Journal of King Saud University-Computer and Information Sciences* 33, no. 7 (2021): 878-889.
[19] Khan A. Kamran, A. Malik, A high capacity reversible watermarking approach for authenticating images: exploiting down-sampling, histogram processing, and block selection, Inf. Sci. 256 (2014) 162–183
[20] J.S. Pan, C.N. Yang, C.C. Lin, Z.H. Wang, C.C. Chang, M.L. Li, et al., Multidimensional and multi-level histogram-shifting-imitated reversible data hiding scheme, Adv. Intell. Syst. Appl. 2 (2013) 149–158. Springer, Berlin Heidelberg.
[21] W. Tai, C. Yeh, C. Chang, Reversible data hiding based on histogram modification of pixel differences, IEEE Trans. Circuits Syst. Video Technol. 19(6) (2009) 906–910.
[22] C.C. Lin, W.L. Tai, C.C. Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recogn. 41 (12) (2008) 3582–3591.
[23] Hu, Runwen, and Shijun Xiang. "CNN prediction based reversible data hiding." *IEEE Signal Processing Letters* 28 (2021): 464-468.
[24] Abadi MAM, Danyali H, Helfroush MS (2010) Reversible watermarking based on interpolation error histogram shifting. 5th International Symposium on Telecommunications (IST), Kish Island, Iran, p 840–845.
[25] D.M. Thodi, J.J. Rodriguez, Prediction-error based reversible watermarking, in: International Conference on Image Processing, 2004, pp. 1549–1552.
[26] Hassan, Fatuma Saeid, and Adnan Gutub. "Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme." *Journal of King Saud University-Computer and Information Sciences* 34, no. 5 (2022): 2017-2030.
[27] Ma, Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li. "Reversible data hiding in encrypted images by reserving room before encryption." *IEEE Transactions on information forensics and security* 8, no. 3 (2013): 553-562.
[28] Sah, Basant, and Vijay Kumar Jha. "Reversible data hiding technique using novel interpolation technique and discrete cosine transform." *International Journal of Integrated Engineering* 11, no. 1 (2019).
[29] Tripathi, Abhinandan, and Jay Prakash. "Blockchain Enabled Interpolation Based Reversible Data Hiding Mechanism for Protecting Records." *EAI Endorsed Transactions on Scalable Information Systems* (2023):
[30] Mohammad, Ahmad A. "A high quality interpolation-based reversible data hiding technique using dual images." *Multimedia Tools and Applications* 82, no. 24 (2023): 36713-36737.
[31] Punia, Riya, Aruna Malik, and Samayveer Singh. "Innovative image interpolation based reversible data hiding for secure communication." *Discover Internet of Things* 3, no. 1 (2023): 22.
[32] H. Jie, L. Tianrui, Reversible steganography using extended image interpolation technique, Comput. Electr. Eng. (2015): http://dx.doi.org/10.1016/j.compeleceng.2015.04.01.
[33] Wang, Xuan, Wenjie Cai, and Mingjie Wang. "A novel approach for biometric recognition based on ECG feature vectors." *Biomedical Signal Processing and Control* 86 (2023): 104922.
[34] Hazratifard, Mehdi, Vibhav Agrawal, Fayez Gebali, Haytham Elmiligi, and Mohammad Mamun. "Ensemble Siamese Network (ESN) Using ECG Signals for Human Authentication in Smart Healthcare System." *Sensors* 23, no. 10 (2023): 4727.
[35] Islam, Md Saiful, Naif Alajlan, Yakoub Bazi, and Haikel S. Hichri. "HBS: a novel biometric feature based on heartbeat morphology." *IEEE transactions on Information Technology in Biomedicine* 16, no. 3 (2012): 445-453.
[36] Islam, Md Saiful, and Naif Alajlan. "Biometric template extraction from a heartbeat signal captured from fingers." *Multimedia Tools and Applications* 76 (2017): 12709-12733.
[37] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45–50, 2001.
[38] Islam, Md Saiful, Haikel Alhichri, Yakoub Bazi, Nassim Ammour, Naif Alajlan, and Rami M. Jomaa. "Heartprint: A Dataset of Multisession ECG Signal with Long Interval Captured from Fingers for Biometric Recognition." *Data* 7, no. 10 (2022): 141.
[39] https://archive.physionet.org/physiobank/database/ecgiddb/
[40] M. Bassiouni, W. Khaleefa, E. ElDahshan, and A.-B. M. Salem, "A machine learning technique for person identification using ECG signals," *Journal of Applied Physics*, vol. 1, pp. 37–41, 2016.
[41] X. Tang and L. Shu, "Classification of electrocardiogram signals with RS and quantum neural networks," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 2, pp. 363–372,2014.
[42] Q. Zhang, D. Zhou, and X. Zeng, "HeartID: a multiresolution convolutional neural network for ECG-based biometric human identification in smart health applications," *IEEE Access*, vol. 5, pp. 11 805–11 816, 2017.
[43] Abdeldayem, Sara S., and Thirimachos Bourlai. "A novel approach for ECG-based human identification using spectral correlation and deep learning." *IEEE Transactions on Biometrics, Behavior, and Identity Science* 2, no. 1 (2019): 1-14.
[44] Zhao, Zhidong, Yefei Zhang, Yanjun Deng, and Xiaohong Zhang. "ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation." *Computers in biology and medicine* 102 (2018): 168-179.
[45] AlDuwaile, Dalal A., and Md Saiful Islam. "Using convolutional neural network and a single heartbeat for ECG biometric recognition." *Entropy* 23, no. 6 (2021): 733.