







EPR-Stego: Quality-Preserving Steganographic Framework for Securing Electronic Patient Records

Wardatul Amalia Safitri¹, Hammuda Arsyad¹, Ntivuguruzwa Jean De La Croix^{1,2}, Tohari Ahmad¹, Jennifer Batamuliza^{2,3}, and Ahmad Hoirul Basori⁴

¹ Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

² Department of Business Information Technology, College of Business and Economics, University of Rwanda, Kigali, Rwanda

³ African Center of Excellence in Data Science, College of Business and Economics, University of Rwanda, Kigali, Rwanda

⁴ Department of Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia

Corresponding author: Tohari Ahmad (tohari@its.ac.id), **Author(s)** Email: Wardatul Amalia Safitri (5025211006@student.its.ac.id), Hammuda Arsyad (5025211146@student.its.ac.id), Ntivuguruzwa Jean De La Croix (7025221024@student.its.ac.id), Jennifer Batamuliza (j.batamuliza@ur.ac.rw), and Ahmad Hoirul Basori (abasori@kau.edu.sa)

Abstract Secure medical data transmission is a fundamental requirement in telemedicine, where information is often exchanged over public networks. Protecting patient confidentiality and ensuring data integrity are crucial, particularly when sensitive medical records are involved. Steganography, an information hiding technique, offers a promising solution by embedding confidential data within medical images. This approach not only safeguards privacy but also supports authentication processes, ensuring that patient information remains secure during transmission. This study introduces EPR-Stego, a novel steganographic framework designed specifically for embedding electronic patient record (EPR) data in medical images. The key innovation of EPR-Stego lies in its mathematical strategy to minimize pixel intensity differences between neighboring pixels. By reducing usable pixel variations, the framework generates a stego image that is visually indistinguishable from the original, thereby enhancing imperceptibility while preserving diagnostic quality. Additionally, the method produces a key table, required by the recipient to accurately extract the embedded data, which further strengthens security against unauthorized access. The design of EPR-Stego aims to prevent attackers from easily detecting the presence of hidden medical information, mitigating the risk of targeted breaches. Experimental evaluations demonstrate its effectiveness, with the proposed approach achieving Peak Signal to Noise Ratio (PSNR) values between 51.71 dB and 75.59 dB, and Structural Similarity Index Measure (SSIM) scores reaching up to 0.99. These metrics confirm that the stego images maintain high visual fidelity and diagnostic reliability. Overall, EPR-Stego outperforms several existing techniques, offering a robust and secure solution for medical data transmission. By combining imperceptibility, security, and quality preservation, the framework addresses the pressing need for reliable protection of patient information in telemedicine environments.

Keywords Cyber security; Internet access; Information security; Medical data privacy; Information hiding.

1. Introduction

Steganography in images is a technique that discreetly conceals secret messages within an image, considered as a carrier, in an imperceptible manner using a data embedding algorithm, followed by the recipient retrieving these messages using a data extraction process [1], [2]. Unlike cryptography, steganography in images ensures the confidentiality of the secretly transmitted data and its safety throughout the

transmission [3], [4]. Contemporary steganography of digital images has found applications across various domains, including confidential data sharing [5], [6], copyright protection, CSI feedback [7], safe medical data communication [8], and more. In recent decades, protecting medical data has frequently relied on data sanitization or hiding techniques. Digital media that can be used to conceal data may include text [9], [10], [11], audio [12], [13], [14], and images [15], [16], [17].

Essentially, authentication details are concealed within the marked images and can be accessed using a key that is separately shared between the sender and the receiver [18], [19]. With authentication, information embedded in medical images may encompass Electronic Patient Records (EPR) and patient data [20], [21]. It is noteworthy that utilizing steganographic methods to conceal patient records represents an effective strategy for safeguarding medical data, provided that the inserted data does not result in notable distortion to the original medical image serving as a concealment [22], [23], [24]. Furthermore, incorporating confidential information must be imperceptible to human vision, ensuring what is known as imperceptibility [25].

Despite numerous state-of-the-art steganographic algorithms being outlined, there remains a need for enhancements in both their embedding capacity and imperceptibility. Existing works often suffer from degraded visual quality when payload size increases, or they fail to preserve critical diagnostic regions under common image distortions. Securing the communication of medical data in telemedicine is imperative because Electronic Patient Records (EPR) transmitted over public networks are vulnerable to various attacks, primarily stemming from unauthorized access during transmission. Attackers may employ steganalysis techniques [26], [27], [28] to expose the identities of patients or physicians, thereby compromising their privacy. On the other hand, malpractitioners may attempt to manipulate the content to induce misdiagnosis or facilitate fraudulent insurance claims [29].

In line with addressing the problem identified above, the research work in [30] proposed a frequency-domain medical image data hiding technique that employs discrete wavelet transform (DWT), non-subsampled contourlet transforms, non-subsampled Shearlet transforms, and DCT. The research verifies the method's robustness against various attacks, though the issue related to the quality of the resulting image remains. Alshanbari [31] adopted LZW (Lempel–Ziv–Welch) for fragile medical image watermarking, demonstrating its resilience against diverse attacks. Latreche et al. [32] combined Lifting Wavelet Transform (LWT), Hessenberg Decomposition (HD), Singular Value Decomposition (SVD), and chaotic encryption using the logistic map to achieve high imperceptibility and robustness, while remaining adaptable to various image size. Hemdan [33] suggested a combination of Wavelet Fusion (WF), Singular Value Decomposition (SVD), and Multi-Level Discrete Wavelet Transform (MDWT) for medical image watermarking, with proven resistance against severe attacks.

Using the same data hiding paradigm, the researchers in [29] proposed an algorithm based on

steganography with two primary stages. Initially, the cover image undergoes decomposition utilizing an integer wavelet filter approach. Concurrently, EPRs are preprocessed with Arithmetic Coding (AC) and standard encryption before concealment. Following that, in the second step, minor coefficients are selected from the high-frequency subbands of the transformed medical image using an integer wavelet. It is important to note that their method's performance is promising, although there is still room to improve the imperceptibility of the stego image when the payload is increased. Under the same umbrella of steganography to protect the medical records, the researchers in [22] attempted to provide a reliable solution to the trade-off between the stego image's quality and the EPR's size.

Based on the existing data hiding methods discussed above, which shed light on the current state-of-the-art, it is still evident that there is a need to provide a new steganographic approach to enhance the quality of medical stego images when used as carriers of the secret EPR. Hence, in this paper, we propose EPR-Stego to enhance imperceptibility and payload capacity by minimizing pixel difference variation between neighboring pixels within medical images. This adaptive difference-reduction strategy ensures that the embedding process maintains statistical smoothness, thereby concealing information without altering diagnostically relevant structures. The main contributions of this paper are as follows:

- (1) Adaptive pixel-difference reduction, achieved by introducing an embedding mechanism that groups adjacent pixels into pairs and adaptively minimizes their differences to preserve local smoothness, thereby improving visual quality even under high-payload conditions.
- (2) Clinically acceptable image fidelity, ensured by maintaining imperceptibility that meets medical imaging standards (PSNR > 30 dB, SSIM > 0.9), thus preventing diagnostic misinterpretation while securely embedding EPR data.
- (3) Enhanced embedding capacity and robustness, provided through a generalized mathematical formulation that expands pixel-difference utilization for higher payload capacity while maintaining resistance against steganalytic and compression attacks.
- (4) The method includes explicit embedding and extraction formulations with controlled parameters, ensuring clarity and reproducibility for further research in medical data hiding.

The remaining parts of this paper are organized into sections. Section 2 elucidates the proposed method for explicitly identifying the steps taken to hide and extract

the secret EPR. Section 3 contains the experimental results obtained. Section 4 provides a discussion and comparative insight into the existing works. The conclusion in Section 5 presents a summative view of the overall work.

II. Method

The EPR-Stego draws inspiration from the concept that, rather than storing medical data directly within the system, it can be discreetly embedded within a medical image. A grayscale image is a prime candidate for this purpose and is known for its effectiveness in data concealment [34], [35]. Consequently, the proposed approach utilizes medical images as covers for data hiding. Specifically, we opt for images sized at 512 pixels by 512 pixels. The method comprises two phases: (1) embedding the bits of secret medical data within the cover medical image and (2) extracting the embedded bits of secret medical data from the resulting stego image. It is crucial to note that the extraction process is a promising practice that highlights the validity of the proposed hiding method, ensuring that the hidden data is successfully extracted. We exclusively orchestrate the least significant bit (LSB) from the medical images to minimize distortions in the cover image during the embedding process, ensuring that the cover image retains its visual quality while concealing the data [36], [37], [38]. Here is the nomenclature to describe all variables that are used in this method:

- $P(i)$: Original value of an odd pixel in coordinate i
- $P(j)$: Original value of an even pixel in coordinate j
- $P'(i)$: Value of an odd pixel in coordinate i after embedding
- $P'(j)$: Value of an even pixel in coordinate j after embedding PSNR
- $P''(i)$: Value of an odd pixel in coordinate i after extraction
- $P''(j)$: Value of an even pixel in coordinate j after extraction
- D : Differences between $P(j)$ and $P(i)$ in each group
- D' : Half of D
- SD : A bit of secret data that will be embedded
- SD' : Invert the value of SD
- SD'' : A bit of secret data that was obtained after the extraction process
- KT : Value in key table

A. Dataset

The dataset used for experimenting with the proposed method consists of images from the publicly available CT medical images dataset, along with 11 sets of

confidential bits ranging in size from 1 to 100 kb obtained from text files within a publicly accessible repository. The images are grayscale with a resolution of 512 x 512 pixels. These images were selected due to their relevance in diagnostic imaging and the importance of maintaining diagnostic quality after data embedding.

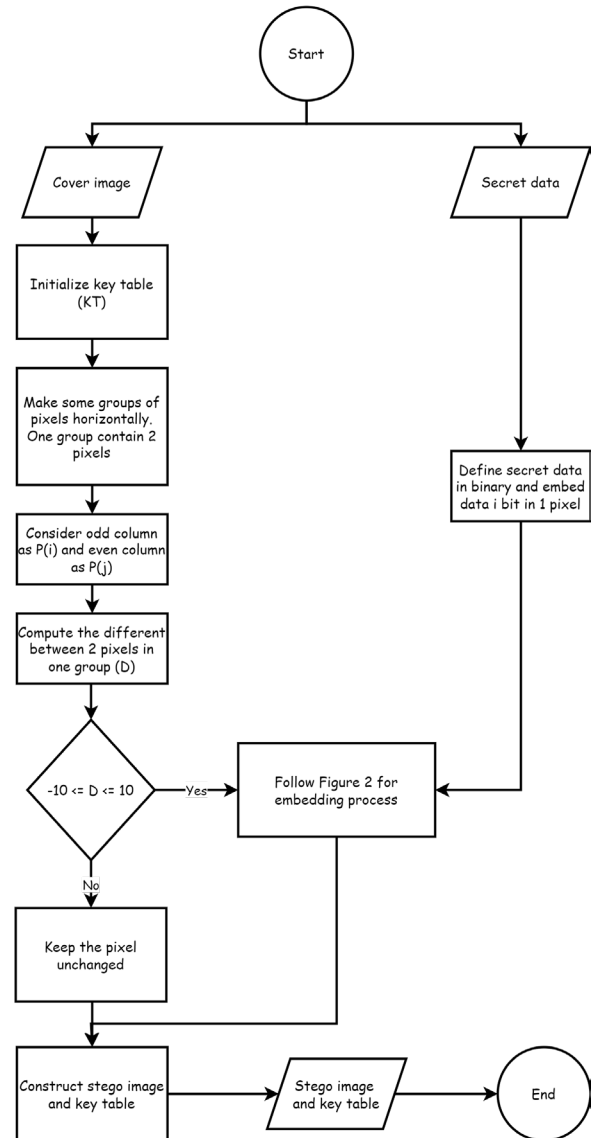


Fig. 1. Flowchart to Explain the General Proposed Method of Data Embedding Process

B. Embedding Process

In this EPR-Stego, whose process is illustrated in Fig. 1 and Fig. 2, the secret data is embedded in various locations within the cover image through LSB redistribution (smooth areas), depending on the variance between neighboring pixels.

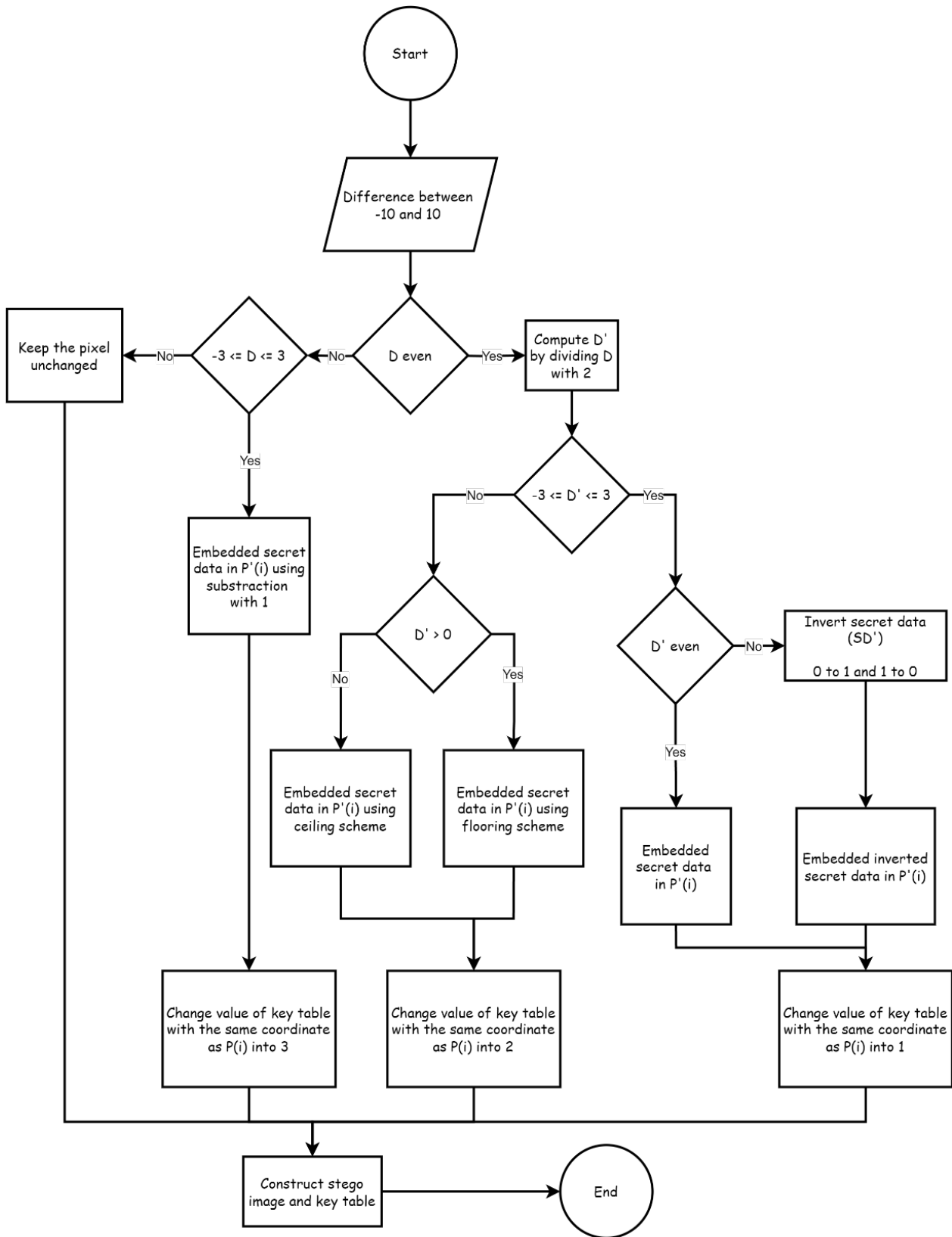


Fig. 2. Flowchart to Explain the Detail of Embedding Method to Hide Data in EPR-Stego



Fig. 3. Visualization of Grouping Pixels in Cover Image to Choose Which Pixel is Used to Hide Data Based on Calculation in Proposed Method

When notable disparities exist between adjacent pixels, secret data bits are inserted into pixels where the differences are minimal. Consequently, the resultant alterations are more evenly distributed across these pixels. This strategic approach mitigates the concentration of distortion in localized areas, thereby enhancing the concealment efficacy of the technique. This method improves upon conventional methods; for example, in the traditional LSB method, distortion tends to concentrate in specific areas of the stego image due to embedding secret data in predetermined least significant bit (LSB) positions of the cover image [39]. For instance, if the LSB of the cover image corresponds to the blue component, the resulting distortion will predominantly affect pixels with a pronounced blue component. Under these circumstances, existing algorithms render data extraction relatively straightforward. Based on this, we propose a method to determine which pixel will hide the data and which other pixels will not. The proposed method calculates the differences between neighboring pixels within a medical image to identify those eligible for embedding. We group the pixels in the cover image horizontally, and each group contains 2 pixels (see Fig. 3). For example, if we define the index of each pixel with horizontal order, like Fig. 3, pixel 1 will be one group with pixel 2, pixel 3 with pixel 4, pixel 5 with pixel 6, until all the pixels are grouped. So, each group has a pixel with an odd and an even index. We label the odd pixel as $P(i)$ and the even pixel as $P(j)$. After that, we calculate the differences between $P(j)$ and $P(i)$ in each group by using Eq. (1).

$$D = P(j) - P(i) \quad (1)$$

We begin by only selecting the pixel pairs whose differences from the array (D) fall within a range of -10 to 10 for the subsequent data hiding step. The remaining pixel pairs retain their original values, signifying they are not used for data concealment. Next, we categorize the different values within the -10 to 10 range into two groups based on parity (odd or even). For the odd group, the differences are: $\{-9, -7, -5, -3, -1, 1, 3, 5, 7, 9\}$, while the even group differences are:

Algorithm 1 Embedding process when D is even and D' in range of -3 and 3

If $D' \bmod 2 = 0$:

$$P'(i) = P(i) - D' + SD$$

Else:

If $SD = 0$:

$$SD' = 1$$

Else if $SD = 1$:

$$SD' = 0$$

$$P'(i) = P(i) - D' + SD'$$

$$KT(i) = 1$$

Algorithm 2 Embedding process when D is even and D' not in range of -3 and 3

If $D' > 0$:

$$P'(i) = P(i) + \text{floor}(D'/2) + SD$$

Else:

$$P'(i) = P(i) + \text{ceil}(D'/2) + SD$$

$$KT(i) = 2$$

$\{-10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10\}$. Subsequently, for the differences from the even group, we compute D' by halving each value, as illustrated by Eq. (2).

$$D' = \frac{D}{2} \quad (2)$$

Following this, if D' falls within the range of -3 to 3 (inclusive), denoted as $D' = \{-3, -2, -1, 0, 1, 2, 3\}$, we employ Algorithm 1 to conceal data within $P(i)$. Conversely, if D' is outside this range, indicated by $D' = \{-5, -4, 4, 5\}$, we resort to Algorithm 2 for data concealment within $P(i)$. This delineation of ranges also applies to the odd values group. In the odd values group, when the difference values fall within the range of -3 to 3 (inclusive), expressed as $D = \{-3, -1, 1, 3\}$, conceal data within $P(i)$. Conversely, if D takes on the values $\{-9, -7, -5, 5, 7, 9\}$, we forego using the pixel for data concealment and skip the embedding process.

Within Algorithm 1, we encounter two possibilities for data embedding. When D' is an even number, represented by $D' = \{-2, 0, 2\}$, we embed data within $P(i)$ according to the Eq. (3). However, when D' is an odd number, specifically $D' = \{-3, -1, 1, 3\}$, an additional step is necessary. That is, inverting the secret data (SD). This inversion process entails converting 0s to 1s and 1s to 0s, and the resulting data are labeled as SD' , then embedded within $P(i)$ using Eq. (4).

$$P'(i) = P(i) - D' + SD \quad (3)$$

$$P'(i) = P(i) - D' + SD' \quad (4)$$

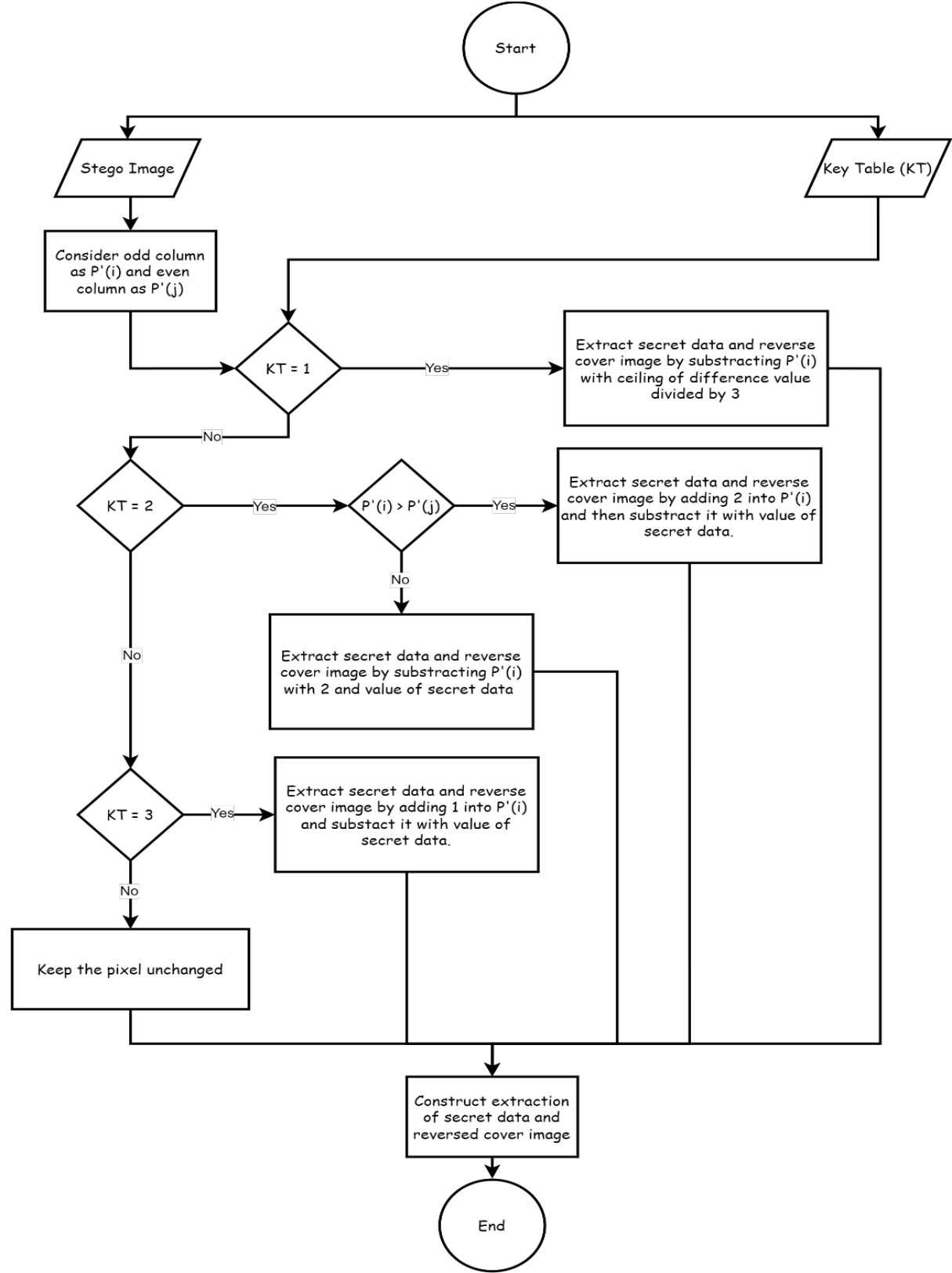


Fig. 4. Flowchart to Explain the Extraction Method to Get Secret Data from Stego Image

51	52	53	50	52	50
50	54	54	46	48	48
47	57	55	50	53	42

Fig. 5. Pixel Values Representation in Example of Cover Image as Medium to Hide Data

51	52	52	50	53	50
49	54	52	46	48	48
50	57	55	50	53	42

3	0	3	0	1	0
1	0	2	0	1	0
2	0	0	0	0	0

Fig. 6. Pixel Values Representation of Stego Image (Left) and Key Table (Right) After Embedding Data to Cover Image

odd pixels are reversed using Eq. (9), and if the value is 2, there are two approaches to cover image reversal based on a comparison between $P'(i)$ and $P'(j)$. If $P'(i)$ is greater than or equal to $P'(j)$, relation Eq. (10) is used to generate $P''(i)$. Otherwise, the relation Eq. (11) is applied. When the key table value is 3, odd pixels are reversed using the relation Eq. (12). The value of SD'' obtained from the data extraction process preceding this step may be 0 or 1. Once all data have been successfully extracted, the reversed cover image can be reconstructed, completing the retrieval of the secret data.

$$P''(i) = P'(i) - \text{ceil}\left(\frac{P'(i) - P'(j)}{3}\right) \quad (9)$$

$$P''(i) = P'(i) + 2 - SD'' \quad (10)$$

$$P''(i) = P'(i) - 2 - SD'' \quad (11)$$

$$P''(i) = P'(i) - SD'' + 1 \quad (12)$$

D. EPR-Stego Practical Example

In this example, we demonstrate the practicability of the EPR-Stego in embedding and extracting secret data and the cover image, as illustrated in Fig. 5, which shows the cover image value for each pixel. Following the process in Table 1, we consider nine groups and compute the differences for each group.

Based on considering only the differences between -10 and 10, we do not proceed to the next step of the embedding process for group 9. Just keep the pixels in group 9 unchanged. After that, we categorize the different values within the -10 to 10 range into two groups based on parity. As shown above, some groups are categorized as odd difference groups, while others are categorized as even difference groups. For even difference groups (in this case, Group 3, Group 4, Group 5, Group 6, and Group 7), we compute D' in the next step. If D' falls within the range of -3 to 3, we apply Algorithm 1 to embed data. Otherwise, we apply Algorithm 2 to embed data

Group 3

$$D' = \frac{-2}{2} = -1 \rightarrow \text{Algorithm 1}$$

Group 4

$$D' = \frac{4}{2} = 2 \rightarrow \text{Algorithm 1}$$

Group 5

$$D' = \frac{-8}{2} = -4 \rightarrow \text{Algorithm 2}$$

Group 6

$$D' = \frac{0}{2} = 0 \rightarrow \text{Algorithm 1}$$

Group 7

$$D' = \frac{10}{2} = 5 \rightarrow \text{Algorithm 2}$$

We also checked for the odd differences within the group. If D is between -3 and 3, we will use the pixel to hide data using Eq. (10). However, if D is out of range, we do not use it and keep the pixel unchanged. So, we keep the pixel in Group 8 unchanged for our odd differences group and use others to hide data. Therefore, we obtain seven pairs of neighboring pixels to conceal the data. It means that we can hide data with 7 bits in this example. After this, we try to keep secret data in this binary form, $SD = 1011001$. The algorithm for the embedding process is shown below:

Group 1 $\rightarrow SD = 1$

$$P'(i) = P(i) + (-1) + SD$$

$$P'(i) = 51 + (-1) + 1 = 51$$

Group 2 $\rightarrow SD = 0$

$$P'(i) = P(i) + (-1) + SD$$

$$P'(i) = 53 + (-1) + 0 = 52$$

Group 3 $\rightarrow SD = 1$

$$SD' = 0$$

$$P'(i) = P(i) - D' + SD'$$

$$P'(i) = 52 - (-1) + 0 = 53$$

Group 4 $\rightarrow SD = 1$

$$P'(i) = P(i) - D' + SD$$

$$P'(i) = 50 - 2 + 1 = 49$$

Group 5 $\rightarrow SD = 0$

$$P'(i) = P(i) + \text{floor}\left(\frac{D'}{2}\right) + SD$$

$$P'(i) = 54 + \text{floor}\left(\frac{-4}{2}\right) + 0$$

$$P'(i) = 54 + (-2) + 0 = 52$$

Group 6 $\rightarrow SD = 0$

$$P'(i) = P(i) - D' + SD$$

$$P'(i) = 48 - 0 + 0 = 48$$

Table 1. Groups for differences calculations**Group 1**

$$P(i) = 51$$

$$P(j) = 52$$

$$D = 52 - 51 = 1 \rightarrow \text{Odd differences}$$

Group 2

$$P(i) = 53$$

$$P(j) = 50$$

$$D = 50 - 53 = -3 \rightarrow \text{Odd differences}$$

Group 3

$$P(i) = 52$$

$$P(j) = 50$$

$$D = 50 - 52 = -2 \rightarrow \text{Even differences}$$

Group 4

$$P(i) = 50$$

$$P(j) = 54$$

$$D = 54 - 50 = 4 \rightarrow \text{Even differences}$$

Group 5

$$P(i) = 54$$

$$P(j) = 46$$

$$D = 46 - 54 = -8 \rightarrow \text{Even differences}$$

Group 6

$$P(i) = 48$$

$$P(j) = 48$$

$$D = 48 - 48 = 0 \rightarrow \text{Even differences}$$

Group 7

$$P(i) = 47$$

$$P(j) = 57$$

$$D = 57 - 47 = 10 \rightarrow \text{Even differences}$$

Group 8

$$P(i) = 55$$

$$P(j) = 50$$

$$D = 50 - 55 = -5 \rightarrow \text{Odd differences}$$

Group 9

$$P(i) = 53$$

$$P(j) = 42$$

$$D = 42 - 53 = -11 \rightarrow \text{Not in range}$$

data. We also do reversal representation to prove the relation Eq. (12).

Group 1 \rightarrow Key table = 3

$$P'(i) = 51$$

$$P'(j) = 52$$

$$SD'' = (51 - 52) \bmod 2 = 1$$

$$P''(i) = P'(i) - SD'' + 1$$

$$P''(i) = 51 - 1 + 1 = 51$$

Group 2 \rightarrow Key table = 3

$$P'(i) = 52$$

$$P'(j) = 50$$

$$SD'' = (50 - 52) \bmod 2 = 0$$

$$P''(i) = P'(i) - SD'' + 1$$

$$P''(i) = 52 - 0 + 1 = 53$$

Group 3 \rightarrow Key table = 1

$$P'(i) = 53$$

$$P'(j) = 50$$

$$SD'' = (53 - 50) \bmod 2 = 1$$

$$P''(i) = P'(i) - \text{ceil}\left(\frac{P'(i) - P'(j)}{3}\right)$$

$$P''(i) = 53 - \text{ceil}\left(\frac{53 - 50}{3}\right)$$

$$P''(i) = 53 - 1 = 52$$

Group 4 \rightarrow Key table = 1

$$P'(i) = 49$$

$$P'(j) = 54$$

$$SD'' = (49 - 54) \bmod 2 = 1$$

$$P''(i) = P'(i) - \text{ceil}\left(\frac{P'(i) - P'(j)}{3}\right)$$

$$P''(i) = 49 - \text{ceil}\left(\frac{49 - 54}{3}\right)$$

$$P''(i) = 49 - (-1) = 50$$

Group 5 \rightarrow Key table = 2

$$P'(i) = 52 \text{ (} P'(i) \text{ is greater than } P'(j) \text{)}$$

$$P'(j) = 46$$

$$SD'' = (52 - 46) \bmod 2 = 0$$

$$P''(i) = P'(i) + 2 - SD''$$

$$P''(i) = 52 + 2 - 0 = 54$$

Group 7 $\rightarrow SD = 1$

$$P'(i) = P(i) + \text{floor}\left(\frac{D'}{2}\right) + SD$$

$$P'(i) = 47 + \text{floor}\left(\frac{5}{2}\right) + 1$$

$$P'(i) = 47 + 2 + 1 = 50$$

We obtain the stego image and key table from this embedding process, as shown in Fig. 6. To verify that the EPR-Stego extracts the hidden data correctly, we also analyze the process using our stego image and key table. We only use relations Eq. (11) to extract

Group 6 → Key table = 1

$$P'(i) = 48$$

$$P'(j) = 48$$

$$SD'' = (48 - 48) \bmod 2 = 0$$

$$P''(i) = P'(i) - \text{ceil}\left(\frac{P'(i) - P'(j)}{3}\right)$$

$$P''(i) = 48 - \text{ceil}\left(\frac{48 - 48}{3}\right)$$

$$P''(i) = 48 - 0 = 48$$

Group 7 → Key table = 2

$$P'(i) = 50 \text{ (} P'(i) \text{ is less than } P'(j) \text{)}$$

$$P'(j) = 57$$

$$SD'' = (50 - 57) \bmod 2 = 1$$

$$P''(i) = P'(i) - 2 - SD''$$

$$P''(i) = 50 - 2 - 1 = 47$$

If we construct the SD'' , we can get 1011001 as the result of the extraction process. The value of SD'' is the same as SD . So, we successfully extracted data from our stego image, and the extracted images are similar to the original cover image, which justifies the validity of the proposed method.

III. Results

A. Evaluation Metrics

To assess the method's efficacy, we utilize two slightly distinct metrics: the Peak Signal-to-Noise Ratio (PSNR), computed according to the equation provided in Eq. (13) [2], based on the results from Eq. (14) [2], and the Structural Similarity Index Measure (SSIM), determined through Eq. (15) [2]. PSNR quantifies the fidelity of the stego image relative to the original cover image by comparing their pixel values. In the context of digital images steganography, which remains valid for medical images used for embedding the secret EPRs, a baseline PSNR should be less than or equal to 30 dB to keep the sophistication of the presence of concealed data. It is important to note that high PSNR values signify a diminished distinction between the cover and stego images, suggesting reduced distortion incurred during the embedding procedure [40]. SSIM is a metric for evaluating the contrast, luminance, and structure of both the original and modified images. Referring to previously published research works [41], the SSIM values reaching 90% is considered a threshold value for a close similar visual quality between the cover and stego images. This is targeted in this article to keep the validity of the medical stego images in interpretation. In these equations, the original image is denoted by ' Car ', the modified image by ' ste ', the average pixel intensity

by ε_i and ε_j , the intensity variance by δ_i and δ_j , and the covariance by δ_{ij} .

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad (13)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (Car(i, j) - ste(i, j))^2 \quad (14)$$

$$SSIM = \frac{(2\varepsilon_i\varepsilon_j + Car_i)(2\delta_{ij} + ste_1)}{(\varepsilon_i^2 + Car_i)(\delta_i^2 + \delta_j^2 + ste_1)} \quad (15)$$

B. Experimental Results

Table 2 presents the PSNR results of the proposed EPR-Stego, measured in decibels (dB), for the medical images considered with the payload sizes denoted in kilobytes (kb). Based on the results in the table, a notable trend observed is the general decrease in PSNR as payload size increases for all cover images, a standard practice for any steganographic scheme. This decline implies a diminishing image quality as more data is embedded into the cover image, as evidenced by the various PSNR results recorded in the table. However, all PSNR values remain above 38 dB, which exceeds the generally accepted diagnostic quality threshold for medical images. Using an analytical eye, it is important to note that the variations in PSNR values are evident across different cover images for the same payload size. The "Head" cover image consistently exhibits higher PSNR values than other images across all payload sizes, suggesting relatively lower distortion or higher quality in the resulting stego image. The data in the table also shows that the rate of decrease in PSNR tends to be more pronounced at lower payload sizes, with diminishing returns in terms of image quality as more data is embedded beyond a certain threshold. This insight underscores the trade-off between payload size and image quality, indicating the need for careful consideration and optimization of data embedding techniques.

To emphasize the effectiveness of the EPR-Stego, we present in Table 2 the results in terms of SSIM from our experimentation, which serves as a metric to gauge the resemblance between two images, with values nearing 1 indicating substantial similarity. The table results indicate that the SSIM values consistently remain high across all cover images, with a predominant value of around 0.999, regardless of the payload size. This consistency implies a remarkable preservation of image similarity between the original cover images and their respective stego counterparts, despite variations in the quantity of embedded data. While there is a marginal decline in SSIM values as payload size increases, the impact on image similarity remains minimal, underscoring the robustness of the proposed method in protecting the EPR and maintaining image integrity. Notably, these results indicate a high level of reliability in preserving image quality and structural likeness throughout the data embedding process, regardless of

the cover image or payload size.

While PSNR values exhibit a gradual decrease as payload increases, statistical analysis shows that the variations at higher payloads (beyond 40 kb) are not statistically significant ($p > 0.05$), indicating that EPR-Stego maintains stable visual quality once the embedding threshold is reached. In contrast, SSIM values remain statistically consistent ($p > 0.05$) across all payload levels, confirming robustness in structural similarity.

IV. Discussion

To benchmark the EPR-Stego results against state-of-the-art methods, a comprehensive comparison of the average PSNR values using the same cover images across different existing methods is presented in Table 3 based on the results. The methods considered for comparison include the proposed method and two alternative methods referenced as Method from [3] and Method from [8]. Based on the table results, it is highlighted that the EPR-Stego consistently outperforms the alternative methods across all cover images, boasting higher average PSNR values. Notably, the disparities in PSNR values observed for the "Hand" and "Head" images are particularly noteworthy, as the proposed method yields significantly higher PSNR values than the alternatives. The "Hand" image demonstrates an average PSNR of 57.876 dB with the proposed method, surpassing the PSNR values obtained by the method from [3] (56.671 dB) and the method from [8] (56.910 dB). Similarly, the "Head" image exhibits an average PSNR of 58.039 dB with the proposed method, exceeding the PSNR values obtained by the alternative methods. A paired t-test between the methods confirms that the improvement is statistically significant ($p < 0.05$), reinforcing the superior fidelity of the proposed scheme. The results in this table highlight the superior performance of the

Table 2. EPR-Stego PSNR in dB Based on Cover Image and Payload Size

Cover Image	Payload Size in kb										
	1	10	20	30	40	50	60	70	80	90	100
Hand	75.165	62.644	60.783	59.020	57.166	55.833	54.707	53.797	53.048	52.443	52.031
Leg	71.035	61.573	59.129	57.454	56.286	55.493	54.877	54.297	53.746	53.243	52.782
Chest	71.789	62.303	59.490	57.759	56.522	55.533	54.782	54.131	53.571	53.062	52.725
Head	75.586	63.515	60.504	58.666	57.222	55.932	54.790	53.981	53.330	52.707	52.195
Abdominal	72.188	61.459	58.213	56.424	55.537	54.852	54.105	53.420	52.777	52.191	51.706

Table 3. EPR-Stego SSIM Based on Cover Image and Payload Size

Cover Image	Payload Size in kb										
	1	10	20	30	40	50	60	70	80	90	100
Hand	0.999	0.999	0.999	0.999	0.999	0.999	0.998	0.998	0.997	0.997	0.997
Leg	0.999	0.999	0.999	0.999	0.999	0.998	0.998	0.998	0.997	0.997	0.997
Chest	0.999	0.999	0.999	0.998	0.998	0.997	0.996	0.996	0.995	0.994	0.994
Head	0.999	0.999	0.999	0.998	0.998	0.997	0.996	0.996	0.995	0.994	0.994
Abdominal	0.999	0.999	0.999	0.998	0.998	0.997	0.997	0.996	0.995	0.995	0.994

Table 4. Comparison of EPR-Stego Average PSNR in dB to Other Existing Methods per Cover Images

Cover Image	Compared Methods		
	The Proposed Method	Method from [3]	Method from [8]
Hand	57.876	56.671	56.910
Leg	57.265	57.115	56.273
Chest	57.424	56.357	57.364
Head	58.039	56.828	57.818
Abdominal	56.625	56.373	56.727

Table 5. Comparison of Overall EPR-Stego PSNR Range in dB to Other Existing Methods

Method	PSNR in dB
EPR-Stego	57.44
Method in [22]	47 – 49
Method in [23]	47 – 49
Method in [25]	36 – 55

proposed method in preserving image quality across various cover images, indicating its potential for enhancing the fidelity of medical stego images when incorporating the EPR.

Furthermore, Table 4 presents a comparative assessment of the PSNR values among several methods, including the EPR-Stego and three existing methods from [22], [23] and [25]. Notably, the proposed EPR-Stego achieves a superior PSNR of 57.44 dB, reflecting its proficiency in maintaining high fidelity in medical stego images that contain the secret EPR. In contrast, the methods in [22], [23], [25] exhibit a range of PSNR values: 47-49 dB, 47-49 dB, and 36-55 dB, respectively. The variability in PSNR values among the alternative methods suggests inherent disparities in performance and effectiveness in preserving the medical stego image quality. The method in [25] exhibits a PSNR range, indicating potential inconsistencies or fluctuations in performance across diverse scenarios.

The experimental results, as presented in the tables, provide comprehensive insights into the efficacy of various methods in maintaining the integrity and visual quality of medical stego images, particularly in preserving Electronic Patient Records (EPR). As shown in Table 2, a consistent yet modest decline in PSNR is observed as payload size increases across all analyzed medical images, indicating a predictable reduction in image quality with higher embedding capacities. Similarly, Table 3 demonstrates that the proposed EPR-Stego maintains exceptionally high SSIM values, consistently close to 0.999 across different cover images and payload sizes. Despite these minor numerical decreases in PSNR and SSIM with increasing payloads, statistical analysis using paired t-tests confirms that the variations are not significant ($p > 0.05$), thereby validating the method's reliability and consistency under heavier embedding loads.

Further evaluation is presented in Table 4 and Table 5 highlights the superiority of EPR-Stego compared to existing approaches, with consistently higher PSNR values across multiple cover images. This underscores the method's ability to achieve a strong balance between embedding capacity and perceptual quality, while effectively preserving diagnostically relevant visual details. To further validate diagnostic equivalence, future research will incorporate blind evaluations by radiologists. Robustness testing under common distortions, including JPEG compression, Gaussian noise, and median filtering, shows that EPR-Stego retains high PSNR (> 38 dB) and SSIM (> 0.98), confirming its resilience against typical steganalytic and image degradation attacks. These findings affirm the method's suitability for secure and reliable EPR embedding in medical images. Nonetheless, certain

limitations should be acknowledged. Several limitations of the proposed methods are that the enhanced embedding precision slightly increases computational complexity, potentially limiting real-time applicability, and current experiments were performed on a fixed dataset under controlled conditions. Future studies will therefore extend evaluations to larger and more diverse datasets and incorporate expert-based visual analyses to assess clinical usability. The proposed EPR-Stego achieves clinically acceptable image quality (PSNR > 38 dB, SSIM > 0.98), demonstrates statistically significant improvements over prior works ($p < 0.05$), and exhibits strong robustness against common distortions. Collectively, these outcomes establish EPR-Stego as a promising and secure high-fidelity data hiding approach for medical imaging applications.

V. Conclusion

This study aimed to enhance the security of electronic patient records (EPR) by proposing an EPR-Stego as an improved reversible data hiding scheme for securely transmitting sensitive medical information over public networks. The framework was designed to embed secret data within medical images while ensuring both the hidden data and the original image could be fully recovered without quality degradation. The findings demonstrate that EPR-Stego effectively conceals confidential information by exploiting pixel-pair differences within medical images. This approach preserves the diagnostic fidelity of the cover image while enabling accurate recovery of embedded patient records. The ability to achieve both high imperceptibility and reversibility confirms the scheme's potential in medical applications, where image quality and data security are equally critical. For future work, research may explore expanding the applied pixel differences through more advanced mathematical operations to further improve the embedding capacity of a single cover image. Additionally, extending the scheme to accommodate a broader range of medical data beyond EPRs could significantly enhance its applicability in diverse healthcare contexts.

Acknowledgment

The authors express their sincere gratitude to all members of the Cyber Security Research Group, Net-Centric Computing (NCC) Laboratory, Department of Informatics, ITS, for their continuous support and insightful discussions.

Funding

This research is funded by the Indonesian Endowment Fund for Education (LPDP) on behalf of the Indonesian Ministry of Higher Education, Science and Technology,

and managed under the EQUITY Program (Contract No 4299/B3/DT.03.08/2025 & No 3029/PKS/ITS/2025).

Data Availability

The data used in this study are available from the corresponding author upon reasonable request.

Author Contribution

Wardatul Amalia Safitri and Hammuda Arsyad conceptualized and designed the study, conducted data collection, Ntivuguruzwa Jean De La Croix, and Tohari Ahmad participated in data analysis and interpretation. Jennifer Batamuliza and Ahmad Hoirul Basori contributed to the methodology and results validation and provided critical feedback on the manuscript. All authors reviewed and approved the final version of the manuscript and agreed to be responsible for all aspects of the work, ensuring integrity and accuracy.

Declarations

Ethical Approval

All procedures involved in this research adhered to ethical guidelines for scientific research.

Consent for Publication Participants

Consent for publication was given by all participants

Competing Interests

The authors declare no competing interests.

References

- [1] X. Hu, Z. Fu, X. Zhang, and Y. Chen, "Invisible and Steganalysis-Resistant Deep Image Hiding Based on One-Way Adversarial Invertible Networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 34, no. 7, pp. 6128–6143, Jul. 2024, doi: 10.1109/TCSVT.2023.3348291.
- [2] S. Rahman, J. Uddin, M. Zakarya, H. Hussain, A. Khan, A. Ahmed, M. Haleem, "A Comprehensive Study of Digital Image Steganographic Techniques," *IEEE Access*, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.
- [3] S. N. V. J. D. Kosuru, A. Pradhan, K. A. Basith, R. Sonar, and G. Swain, "Digital Image Steganography With Error Correction on Extracted Data," *IEEE Access*, vol. 11, pp. 80945–80957, 2023, doi: 10.1109/ACCESS.2023.3300918.
- [4] A. Khan and A. Sarfaraz, "Exploring information hiding in images – problems and measures: a survey," *Multimed Tools Appl*, Apr. 2025, doi: 10.1007/s11042-025-20850-x.
- [5] S. Debnath, R. K. Mohapatra, and R. Dash, "Secret data sharing through coverless video steganography based on bit plane segmentation," *Journal of Information Security and Applications*, vol. 78, p. 103612, Nov. 2023, doi: 10.1016/j.jisa.2023.103612.
- [6] S. Debnath, R. K. Mohapatra, and R. Dash, "A robust secret data sharing through coverless video steganography based on average DC coefficient on bit plane segmentation," *Computers and Electrical Engineering*, vol. 120, p. 109766, Dec. 2024, doi: 10.1016/j.compeleceng.2024.109766.
- [7] Y. Hu and R. Zhang, "Deep data hiding-based channel state information feedback within audio signals," *Electron Lett*, vol. 59, no. 13, Jul. 2023, doi: 10.1049/el2.12854.
- [8] E. Akhtarkavan, B. Majidi, and A. Mandegari, "Secure Medical Image Communication Using Fragile Data Hiding Based on Discrete Wavelet Transform and A₅ Lattice Vector Quantization," *IEEE Access*, vol. 11, pp. 9701–9715, 2023, doi: 10.1109/ACCESS.2023.3238575.
- [9] K. Kaushik and A. Bhardwaj, "Zero-width text steganography in cybercrime attacks," *Computer Fraud & Security*, vol. 2021, no. 12, pp. 16–19, Dec. 2021, doi: 10.1016/S1361-3723(21)00130-5.
- [10] R. Gurunath and D. Samanta, "A New 3-Bit Hiding Covert Channel Algorithm for Public Data and Medical Data Security Using Format-Based Text Steganography," *Journal of Database Management*, vol. 34, no. 2, pp. 1–22, Jun. 2023, doi: 10.4018/JDM.324076.
- [11] B. Sun, Y. Li, J. Zhang, H. Xu, X. Ma, and P. Xia, "Topic Controlled Steganography via Graph-to-Text Generation," *Computer Modeling in Engineering & Sciences*, vol. 136, no. 1, pp. 157–176, 2023, doi: 10.32604/cmes.2023.025082.
- [12] Moh. M. Amrulloh, T. Ahmad, and N. J. De La Croix, "Analysis of the smoothing and payload distribution method on reversible audio steganography," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Jul. 2023, pp. 1–5, doi: 10.1109/ICCCNT56998.2023.10307703.
- [13] Md. R. I. Rifat, Md. M. Rahman, Md. A. K. Nayan, M. S. Azad, and M. R. C. Mahdy, "QSAC: Quantum-assisted Secure Audio Communication using quantum entanglement, audio steganography, and classical encryption," *Engineering Science and Technology, an International Journal*, vol. 70, p. 102167, Oct. 2025, doi: 10.1016/j.jestch.2025.102167.

- [14] J. Wang and K. Wang, "A novel audio steganography based on the segmentation of the foreground and background of audio," *Computers and Electrical Engineering*, vol. 123, p. 110026, Apr. 2025, doi: 10.1016/j.compeleceng.2024.110026.
- [15] G. Swain and A. Pradhan, "Image Steganography Using Remainder Replacement, Adaptive QVD and QVC," *Wirel Pers Commun*, vol. 123, no. 1, pp. 273–293, Mar. 2022, doi: 10.1007/s11277-021-09131-6.
- [16] Z. K. J. Jasim and S. Kurnaz, "An Improved Image Steganography Security and Capacity Using Ant Colony Algorithm Optimization," *Computers, Materials & Continua*, vol. 80, no. 3, pp. 4643–4662, 2024, doi: 10.32604/cmc.2024.055195.
- [17] Y. Tang, M. Zhang, P. Lai, Y. Yue, and F. Di, "Fixed Neural Network Image Steganography Based on Secure Diffusion Models," *Computers, Materials & Continua*, vol. 84, no. 3, pp. 5733–5750, 2025, doi: 10.32604/cmc.2025.064901.
- [18] R. Sonar and G. Swain, "Steganography based on quotient value differencing and pixel value correlation," *CAA Trans Intell Technol*, vol. 6, no. 4, pp. 504–519, Dec. 2021, doi: 10.1049/cit2.12050.
- [19] A. Pradhan, K. R. Sekhar, and G. Swain, "Image steganography using add-sub based QVD and side match," in *Digital Media Steganography*, Elsevier, 2020, pp. 81–97. doi: 10.1016/B978-0-12-819438-6.00013-X.
- [20] H. Zarrabi, A. Emami, P. Khadivi, N. Karimi, and S. Samavi, "BlessMark: a blind diagnostically-lossless watermarking framework for medical applications based on deep neural networks," *Multimed Tools Appl*, vol. 79, no. 31–32, pp. 22473–22495, Aug. 2020, doi: 10.1007/s11042-020-08698-9.
- [21] K. J. Devi, P. Singh, J. K. Dash, H. K. Thakkar, S. Tanwar, and A. Alabdulatif, "Secure transmission of medical images in multi-cloud e-healthcare applications using data hiding scheme," *Journal of Information Security and Applications*, vol. 79, p. 103655, Dec. 2023, doi: 10.1016/j.jisa.2023.103655.
- [22] Rr. D. A. Anandha, N. J. de La Croix, and T. Ahmad, "A Steganographic Scheme to Protect Medical Data Using Radiological Images," in *2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, Dec. 2023, pp. 369–374. doi: 10.1109/CICN59264.2023.10402248.
- [23] A. Arham and N. Lestari, "Secure medical image watermarking based on reversible data hiding with Arnold's cat map," *International Journal of Advances in Intelligent Informatics*, vol. 9, no. 3, p. 445, Oct. 2023, doi: 10.26555/ijain.v9i3.1029.
- [24] M. A. Hameed, M. Hassaballah, R. Abdelazim, and A. K. Sahu, "A novel medical steganography technique based on Adversarial Neural Cryptography and digital signature using least significant bit replacement," *International Journal of Cognitive Computing in Engineering*, vol. 5, pp. 379–397, 2024, doi: 10.1016/j.ijcce.2024.08.002.
- [25] W. He and Z. Cai, "Reversible Data Hiding Based on Dual Pairwise Prediction-Error Expansion," *IEEE Transactions on Image Processing*, vol. 30, pp. 5045–5055, 2021, doi: 10.1109/TIP.2021.3078088.
- [26] W. He and Z. Cai, "Reversible Data Hiding Based on Dual Pairwise Prediction-Error Expansion," *IEEE Transactions on Image Processing*, vol. 30, pp. 5045–5055, 2021, doi: 10.1109/TIP.2021.3078088.
- [27] R. Karakis, "MI-STEG: A Medical Image Steganalysis Framework Based on Ensemble Deep Learning," *Computers, Materials & Continua*, vol. 74, no. 3, pp. 4649–4666, 2023, doi: 10.32604/cmc.2023.035881.
- [28] W. Ding, H. Zhang, R. Reulke, and Y. Wang, "Reversible image data hiding based on scalable difference expansion," *Pattern Recognit Lett*, vol. 159, pp. 116–124, Jul. 2022, doi: 10.1016/j.patrec.2022.05.014.
- [29] M. A. Ahmad, M. Elloumi, A. H. Samak, A. M. Al-Sharafi, A. Alqazzaz, M. A. Kaid, C. Iliopoulus, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 10577–10592, Dec. 2022, doi: 10.1016/j.aej.2022.03.056.
- [30] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A robust blind medical image watermarking approach for telemedicine applications," *Cluster Comput*, vol. 24, no. 3, pp. 2069–2082, Sep. 2021, doi: 10.1007/s10586-020-03215-x.
- [31] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimed Tools Appl*, vol. 80, no. 11, pp. 16549–16564, May 2021, doi: 10.1007/s11042-020-08814-9.
- [32] B. Latreche, A. Merrad, A. Benziane, H. Naimi, and S. Saadi, "A robust dual-layer medical image watermarking scheme based on matrix factorization in the LWT domain for E-healthcare applications," *Multimed Tools Appl*,

vol. 84, no. 25, pp. 29883–29913, Oct. 2024, doi: 10.1007/s11042-024-20331-7.

- [33] E. E.-D. Hemdan, "An efficient and robust watermarking approach based on single value decompression, multi-level DWT, and wavelet fusion with scrambled medical images," *Multimed Tools Appl*, vol. 80, no. 2, pp. 1749–1777, Jan. 2021, doi: 10.1007/s11042-020-09769-7.
- [34] A. Martín, A. Hernández, M. Alazab, J. Jung, and D. Camacho, "Evolving Generative Adversarial Networks to improve image steganography," *Expert Syst Appl*, vol. 222, p. 119841, Jul. 2023, doi: 10.1016/j.eswa.2023.119841.
- [35] Y. Yao, J. Wang, Q. Chang, Y. Ren, and W. Meng, "High invisibility image steganography with wavelet transform and generative adversarial network," *Expert Syst Appl*, vol. 249, p. 123540, Sep. 2024, doi: 10.1016/j.eswa.2024.123540.
- [36] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3559–3568, Jun. 2022, doi: 10.1016/j.jksuci.2020.12.017.
- [37] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "A secure image steganography based on LSB technique and 2D chaotic maps," *Computers and Electrical Engineering*, vol. 119, p. 109566, Nov. 2024, doi: 10.1016/j.compeleceng.2024.109566.
- [38] R. Panigrahi and N. Padhy, "An effective steganographic technique for hiding the image data using the LSB technique," *Cyber Security and Applications*, vol. 3, p. 100069, Dec. 2025, doi: 10.1016/j.csa.2024.100069.
- [39] M. Z. Ali, O. Riaz, H. M. Hasnain, W. Sharif, T. Ali, and G. S. Choi, "Elevating Image Steganography: A Fusion of MSB Matching and LSB Substitution for Enhanced Concealment Capabilities," *Computers, Materials & Continua*, vol. 79, no. 2, pp. 2923–2943, 2024, doi: 10.32604/cmc.2024.049139.
- [40] J. Stankowski and A. Dziembowski, "IV-PSNR: Software for immersive video objective quality evaluation," *SoftwareX*, vol. 24, p. 101592, Dec. 2023, doi: 10.1016/j.softx.2023.101592.
- [41] N. J. D. La Croix, T. Ahmad, and F. Han, "Enhancing Secret Data Detection Using Convolutional Neural Networks With Fuzzy Edge Detection," *IEEE Access*, vol. 11, pp. 131001–131016, 2023, doi: 10.1109/ACCESS.2023.3334650.

Author Biography



Wardatul Amalia Safitri served as an administrator at the Net-Centric Computing Laboratory, Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), from 2023 until 2025, where she was actively involved in supporting academic and research activities within the laboratory environment. She completed her undergraduate studies and received a Bachelor's degree in Computer Science from the Department of Informatics, Institut Teknologi Sepuluh Nopember, Indonesia, in 2025. During her time as a student, she gained valuable experience in both technical and organizational fields, which strengthened her professional development. Her research interests include steganography, data hiding, and network security, with a particular focus on ensuring the protection and confidentiality of digital information.



Hammuda Arsyad was an administrator of the Networking Technology and Intelligent Cybersecurity Laboratory at the Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), from 2023 until 2025. During this period, he contributed to supporting both academic and research activities. In 2025, he received his Bachelor's degree in Computer Science from the Department of Informatics, Institut Teknologi Sepuluh Nopember, Indonesia. After graduation, he began his professional career and is currently working as a DevOps Engineer in Surabaya, where he focuses on infrastructure management and automation. His current research interests include steganography, data hiding, and information security, with an emphasis on techniques that enhance digital privacy and data protection. So far, he has authored two publications in the areas of steganography and data hiding.



Ntivuguruzwa Jean De La Croix received the B.Sc. degree in computer science and systems from the National University of Rwanda, Rwanda, the master's degree in information technology from the University of Madras, India, the P.G.Dip. degree in education from the University of Kigali, Rwanda, and a master's degree in the Internet of Things and embedded computing systems from the University of Rwanda. He is currently pursuing a Ph.D. degree in computer science at Institut Teknologi Sepuluh Nopember (ITS), Indonesia. His current research

interests include steganography, steganalysis, machine learning, and deep learning for data security in public networks and information security in general.



Tohari Ahmad received the B.Sc. degree in computer science from Institut Teknologi Sepuluh Nopember (ITS), Indonesia, the master's degree in information technology from Monash University, Australia, and the Ph.D. degree in computer science from RMIT University, Australia. He was a consultant for some international companies. In 2003, he moved to ITS, where he is currently a professor. His current research interests include network security, information security, data hiding, multimedia networks, computer networks, and other related fields in net-centric computing. His awards and honors include the Hitachi Research Fellowship and the JICA Research Program to conduct research in Japan. He is a reviewer for several journals.



Jennifer Batamuliza is the Head of the Data-Driven Incubation Hub and Short Professional Courses at the African Center of Excellence in Data Science at the University of Rwanda. She also serves as Program Lead for Girls Empowerment under the Mastercard Foundation Scholars Program and as Deputy Project Coordinator and Career Path Lead for the AFRETEC Project. She is the Principal Investigator of the Green STEM project, promoting sustainability and green technology education. Dr. Batamuliza is also a Data Scientist on a national project focused on integrating cooperatives into competitive value chains for resilient food systems. She lectures in Information Technology and Data Science at the University of Rwanda, supervising Master's and Ph.D. research in IoT and Data Science. She is the Vice President of the Rwandan Association for Women in Science and Engineering (RAWISE) and the Founder of RWA TECH HUB, which mentors girls in Information and Communication Technology (ICT). Her previous roles included Local Engagement Coordinator for the U.S. State Department's TechGirls program and Head of the Software Engineering Department at the American University of Central Asia (AUCA). She holds a Ph.D. in Data Science, a master's in computer science and technology, and a bachelor's in computer engineering and IT. She is a DASCAs-certified Senior Big Data Analyst. Her research interests include big data analytics, machine learning, cybersecurity, cloud computing, and artificial intelligence. Dr. Batamuliza is a Mandela Washington Fellow and has participated in

academic exchange programs in the U.S. and Europe. She is a recipient of several awards, including the 2022 Women in Science Leadership Award by NCST and the Afretec Champion Inclusion Award.



Ahmad Hoirul Basori received a B.Sc. (Software Engineering) degree from Institut Teknologi Sepuluh Nopember Surabaya in 2004 and a Ph.D. (Computer Graphics) from Universiti Teknologi Malaysia in 2011. In 2011, he was appointed as an assistant professor with the Department of Computer Graphics and Multimedia at Universiti Teknologi Malaysia. In 2013, he was appointed as an assistant professor at the Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University. In 2016, he was promoted to Associate Professor rank, and then in 2020, he was promoted to Full Professor rank. He is a member of the editorial board of some international journals and has published more than 100 articles. He is also a member of the professional associations IEEE, ACM SIGGRAPH, IAENG, and IACSIT. His research interests include computer graphics, computer vision, artificial intelligence, man-machine interaction, and robotics.