



MedProtect: Protecting Electronic Patient Data Using Interpolation-Based Medical Image Steganography

Aditya Rizki Muhammad¹, Irsyad Fikriansyah Ramadhan¹, Ntivuguruzwa Jean De La Croix^{1,2}, Tohari Ahmad¹, Dieudonne Uwizeye³, and Evelyne Kantarama^{4,5}

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

² African Center of Excellence in Internet of Things, College of Science and Technology, University of Rwanda, Kigali, Rwanda

³ Department of Development Studies, College of Arts and Social Sciences, University of Rwanda, Kigali, Rwanda

⁴ Department of Clinical Biology, College of Medicine and Health Sciences, University of Rwanda, Kigali, Rwanda

⁵ Department of Pathology, The University Teaching Hospital of Kigali, Kigali, Rwanda

Corresponding author: Tohari Ahmad. (e-mail: tohari@its.ac.id; tohari@if.its.ac.id); Author(s) Email:

Aditya Rizki Muhammad (e-mail: 5025221272@student.its.ac.id), Irsyad Fikriansyah Ramadhan: (e-mail:

5025211149@student.its.ac.id); Ntivuguruzwa Jean De La Croix (e-mail: 7025221024@student.its.ac.id);

Dieudonne Uwizeye (e-mail: d.uwizeye@ur.ac.rw); Evelyne Kantarama (e-mail: ekantarama@cartafrica.org)

Abstract Electronic Patient Records (EPRS) represent critical elements of digital healthcare systems, as they contain confidential and sensitive medical information essential for patient care and clinical decision-making. Due to their sensitive nature, EPRs frequently face threats from unauthorized intrusions, security breaches and malicious attacks. Safeguarding such information has emerged as an urgent concern in medical data security. Steganography offers a compelling solution by hiding confidential data within conventional carrier objects like medical imagery. Unlike traditional cryptographic methods that merely alter the data representation, steganography conceals the existence of the information itself, thereby providing discretion, security, and resilience against unauthorized disclosure. However, embedding patient information inside medical images introduces a new challenge. The method must maintain the image's visual fidelity to prevent compromising diagnostic precision, while ensuring reversibility for complete restoration of both original imagery and concealed information. To address these challenges, this research proposes MedProtect, a reversible steganographic framework customized for medical applications. MedProtect procedure integrates pixel interpolation techniques and center-folding-based data transformation to insert sensitive records into medical imagery. This method combination ensures accurate data recovery of the original image while maintaining the image quality of the resulting image. To clarify the performance of MedProtect, this study evaluates two well-established image quality metrics, Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). The discovery shows that the framework achieves PSNR values of 48.190 to 53.808 dB and SSIM scores between 0.9956 and 0.9980. These outcomes display the high level of visual fidelity and imperceptibility achieved by the proposed method, underscoring its effectiveness as a secure approach for protecting electronic patient records within medical imaging systems.

Keywords cyber security; data hiding; electronic patient records; information hiding; information security; medical data protection; steganography.

1. Introduction

As information technology continues to evolve rapidly, the medical industry has significantly benefited from these advancements, particularly in the efficient management and secure transmission of Electronic Patient Records (EPRs). These records encapsulate highly sensitive data, including patient demographics,

clinical notes, and diagnostic outputs from imaging tools such as X-rays, MRIs, and CT scans. EPRs play a central role in enabling healthcare professionals to make informed decisions, improve diagnostic accuracy, and deliver personalized treatment plans [1], [2], [3]. However, due to their critical nature and confidentiality, EPRs have become increasingly

attractive targets for cybercriminals seeking unauthorized access. Although standards such as the Fast Healthcare Interoperability Resources (FHIR), developed by HL7, have improved interoperability and streamlined data exchange across healthcare systems, they do not directly address data-level security. FHIR focuses on structuring and formatting health data for seamless communication, but delegates the responsibility of securing that data to the underlying system environment. FHIR does not embed encryption mechanisms within its framework. Instead, it relies on external security protocols, such as HTTPS and OAuth 2.0, to protect data in transit and during authentication [4], [5].

This design leaves a potential vulnerability, primarily when EPRs are transmitted over less secure networks or stored in distributed environments. Therefore, it is imperative to explore complementary security mechanisms, such as encryption, watermarking, and steganography, that provide intrinsic protection at the data level. These methods can ensure confidentiality, integrity, and resilience against unauthorized access regardless of the external transmission protocols, addressing a critical gap in healthcare data protection strategies.

Recent advances in the state of the art have highlighted information hiding as a vital component in securing sensitive data during transmission, particularly in domains requiring confidentiality, such as healthcare [6], [7], [8]. Among the most prominent techniques are cryptography and steganography. Cryptography ensures data confidentiality by converting readable information into an encrypted format that only authorized users with a valid decryption key can access [9]. However, despite its effectiveness, the visibly scrambled nature of encrypted content may raise suspicion and invite attempts at unauthorized analysis. Steganography addresses this limitation by concealing the very existence of the message, embedding it within seemingly innocuous cover media such as images, audio, video, or text files, resulting in a stego object [10]. Its key strength lies in imperceptibility, allowing sensitive data to be transmitted without alerting potential adversaries to its presence [11].

Steganographic techniques generally fall into two categories: spatial domain and transform domain methods. Transform domain approaches apply mathematical transformations, such as the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), to the cover medium prior to data embedding to enhance robustness against compression, noise, and signal processing attacks. However, they often incur higher computational costs. In contrast, spatial domain techniques embed secret data by directly modifying the pixel intensity values of

the image. These methods are generally more straightforward, faster and computationally efficient, but they are often less resistant to image processing and statistical attacks [12], [13], [14], [15]. Although selecting an appropriate steganographic method requires a careful trade-off between imperceptibility, robustness, and computational efficiency, the spatial domain is mainly preferred in medical data protection due to its adaptiveness and robustness in resisting steganalysis attacks [16].

Sensitive Electronic Patient Records (EPRs) are routinely exchanged across institutional boundaries and often traverse untrusted networks, particularly in telemedicine, remote diagnostics, and mobile health contexts. Medical images used in these workflows have unique and strict requirements such as embedded data must be concealed securely, both the payload and the host image must remain confidential, and the original image must be perfectly recoverable to preserve diagnostic fidelity [16]. Yet, existing reversible steganography methods face practical limitations in this context, including capacity-fidelity trade-offs, visible artifacts around edges, overflow/underflow risks in higher bit-depth modalities, and reliance on cryptographic keys to ensure data recoverability. While keys can help control access and recovery, key management itself introduces operational complexity and potential failure when secure key distribution cannot be guaranteed [17]. These factors motivate medical image-tailored, efficient, and reversible schemes that guarantee lossless recovery of both the hidden data and the original image while minimizing clinical risk and integration overhead.

Researchers have explored interpolation-based embedding and center folding method, motivated by these requirements. Interpolation, widely used for image upscaling, estimates new pixel values based on known reference pixels. In steganographic use, these interpolated pixels become embedding sites while the original reference pixels remain untouched, thereby increasing capacity and enabling exact, high-quality reconstruction as shown in prior work [18], [19]. Center folding, on the other hand, maps pixel intensities toward a central reference before embedding to create headroom, preventing overflow/underflow and reducing visible changes at very dark or bright regions. During extraction, this mapping is precisely inverted [18], [19].

Building on existing interpolation-based approaches for securing EPRs, this research proposes MedProtect, a novel keyless reversible steganography method that combines image interpolation techniques and center folding strategy. The main contributions of this study are:

1. This study develops a new method that integrates a center folding strategy to preserve the fidelity of

- medical images while embedding sensitive information. This approach achieves excellent visual quality of the medical image and maintains imperceptibility, as demonstrated by a Peak Signal-to-Noise Ratio (PSNR) of 53.808 dB achieved on a chest X-ray image.
- By leveraging image interpolation, MedProtect generates additional embedding space within interpolated pixels of the original medical image, thereby increasing the capacity of the EPRs to be concealed in a single image. At the same time, MedProtect adopts a keyless reversible embedding approach. By eliminating the reliance on secret keys, the method further reduces the likelihood of key interception during transmission and strengthens the overall security of the embedded data.

The paper is organized as follows: Section 2 reviews the recent related work from the state-of-the-art. Section 3 details the approach proposed for MedProtect. Section 4 presents experimental results. Section 5 concludes the study with suggestions for possible future work.

II. State-of-the-art

Effective healthcare data management plays a vital role in supporting accurate clinical decisions and safeguarding patient well-being. Despite its importance, several obstacles persist, including data acquisition variability, data integrity challenges, and the necessity for secure data exchange. Addressing these issues is essential to utilize the potential of healthcare information fully. Ensuring data consistency and quality is fundamental to trustworthy decision-making processes. According to Mavrogiorgos et al. [20], integrating data from diverse sources, such as EPRs, clinical systems, and medical devices, often results in fragmented, redundant, or incomplete datasets.

Beyond ensuring data accuracy and integrity, safeguarding the transmission of Electronic Patient

Records (EPRs) is a crucial aspect of digital healthcare. Since EPRs contain highly sensitive patient information, any compromise during data transfer can lead to severe privacy breaches and legal issues. As healthcare systems increasingly adopt digital technologies, robust security mechanisms become indispensable. One such approach is steganography, which enhances transmission security by concealing confidential EPR data within medical images, thereby reducing the risk of unauthorized access [6]. Steganography is a data hiding technique that involves concealing sensitive information within a cover medium to protect it from unauthorized access. Fig. 1 illustrates steganography in medical images, where a standard medical image is used to embed secret data, such as Electronic Patient Records (EPRs). A steganographic data concealment process ensures that the hidden information remains imperceptible, preserving the visual integrity of the image while securely embedding the data. The resulting output, known as a stego image, is then transmitted or stored without revealing the presence of embedded data. Only authorized users with the appropriate extraction mechanism can retrieve the concealed information, making steganography an effective tool for enhancing data privacy and security in digital healthcare systems [10].

In recent years, various steganographic algorithms have been developed to strengthen the security of EPRs. However, many of these methods still face challenges related to image quality degradation, which can raise concerns about the reliability of clinical interpretations derived from the altered images [17]. To address this limitation, researchers in medical image steganography have adopted pixel interpolation to enhance data embedding. As illustrated in Fig. 2, interpolation is a core image processing technique used to estimate pixel values when resizing or scaling images. Within the context of steganography, interpolated pixels offer additional embedding locations, helping to maintain the visual integrity of the stego image. Standard interpolation methods include nearest neighbor, bilinear, and bicubic interpolation,



Fig. 1. General concept of steganography in medical images

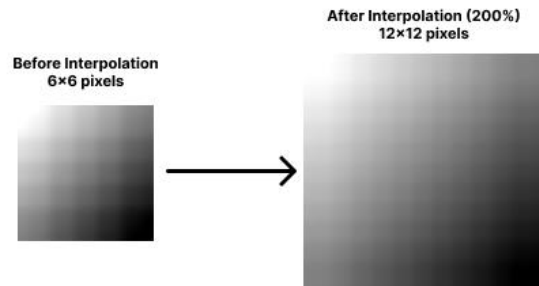


Fig. 2. Interpolation concept

each balancing processing complexity and image fidelity differently [21].

In steganography, interpolation techniques are commonly employed to upscale images and create new pixel values that serve as potential embedding sites for secret data. A foundational contribution in this domain was made by Jung and Yoo [22], who introduced a data hiding method based on Neighbor Mean Interpolation (NMI). Their approach involves initially downscaling the original image to one-quarter of its size, followed by upscaling using NMI to produce an interpolated image suitable for data embedding. This method achieved low computational complexity while preserving acceptable image quality. Building on this work, Lee and Huang [23] proposed the Interpolation by Neighboring Pixels (INP) technique to enhance the visual fidelity of stego images. By employing more accurate neighbor pixel references during the interpolation process, their method improved the precision of pixel value estimation, resulting in better preservation of image quality after data embedding.

Further advancements in interpolation-based steganography were introduced, which developed an extended interpolation method that maximized pixel value differences between neighboring regions. This enhancement significantly increased the embedding capacity while preserving acceptable image quality. Building on this foundation, recent studies have continued to refine interpolation techniques to improve steganographic performance. For instance, Malik et al. [24] utilized the Pixel Intensity Range (PIR) within interpolated images to achieve high Peak Signal-to-Noise Ratio (PSNR) values, indicating strong visual

fidelity. In another contribution, Punia et al. [25] proposed an interpolation-driven steganographic approach specifically designed for Internet of Things (IoT) applications. Their method demonstrated both high payload capacity and superior PSNR, making it particularly effective in resource-constrained and bandwidth-sensitive environments. These studies highlight the potential of interpolation techniques to improve data embedding efficiency while preserving image integrity. They provide the theoretical basis for our proposed steganographic model, which incorporates interpolation to support reversible data hiding with minimal visual distortion.

To significantly enhance the imperceptibility of stego images, Lu et al. [18] proposed a reversible data hiding (RDH) scheme based on center folding with dual images. In this method, secret data is preprocessed by dividing it into k -bit segments, each converted into a decimal value and then folded into a reduced range centered around zero. These folded values are subsequently split into two components and embedded into dual stego images using a reversible averaging technique. While this approach improves security and reversibility of the original image by requiring both stego images for complete data extraction, this method introduces a problem in transmission overhead due to the generation of two stego images instead of one.

Building upon this theoretical foundation, MedProtect proposes a novel interpolation-based medical image steganography to protect the electronic patient record. Based on the benefits of interpolation techniques and center folding strategy, MedProtect aims to ensure secure, reversible data hiding with minimal visual distortion, thus safeguarding patient

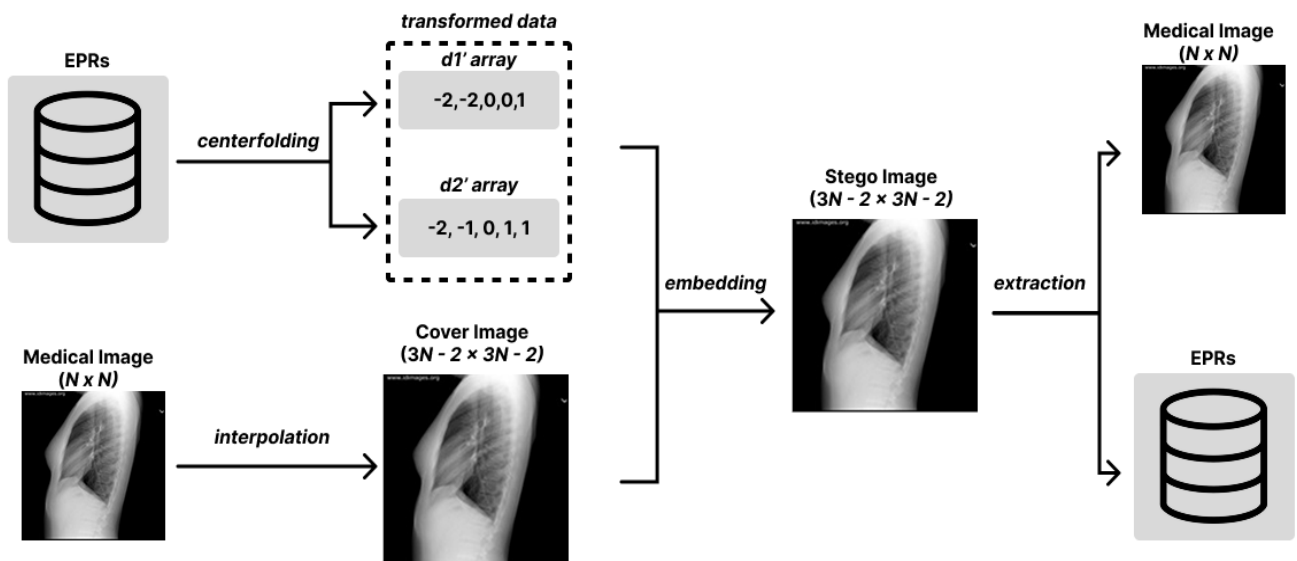


Fig. 3. Example of data embedding in a $N \times N$ medical image using the proposed method.

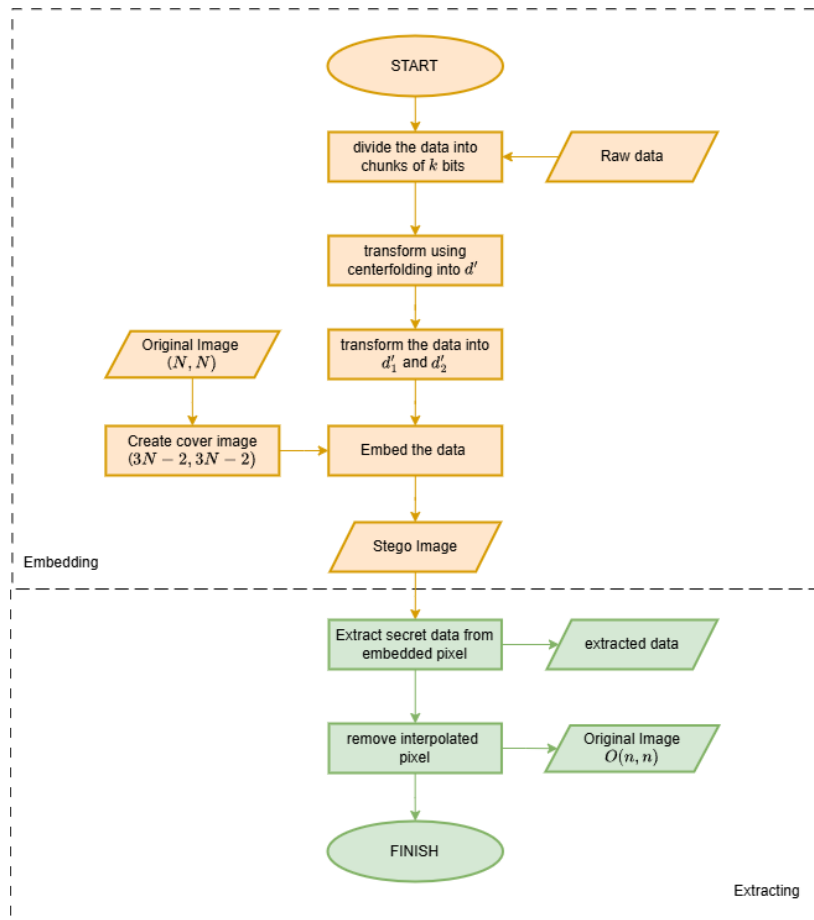


Fig. 4. Flowchart for embedding and extracting process

privacy without compromising the diagnostic quality of medical images. MedProtect is well-aligned with the need for robust, efficient, and clinically viable data protection mechanisms in digital healthcare systems.

III. Proposed Method

This section introduces MedProtect and its end-to-end workflow, as shown in Fig. 3. Briefly, we center-fold the EPR payload to limit distortion and generate embedding sites via image interpolation. At the receiver, these steps are exactly inverted to recover both the payload and the original image. The following subsections detail each stage and the associated parameter.

A. EPR data embedding into the cover medical image

In the embedding process, the proposed approach to conceal the data involves eight steps, from the inputs to the transmissible outputs. To enhance clarity and reproducibility, the pseudocode of the embedding process is presented in Algorithm 1, and the corresponding flowchart is illustrated in Fig. 4. The sequence of the process is detailed below:

Step 1: Load the EPRs into their binary forms (d) and divide the data into chunks of k Bits, as depicted in Fig. 5.

Step 2: Using every chunk from the previous steps, MedProtect transforms the chunks using the center folding strategy, as stated in Eq. (1) [18], [26]. The d is the decimal value of the chunk, and d' is the result. This process aims to reduce the distortion in stego images.

Step 3: MedProtect splits d' by creating d'_1 and d'_2 using Eq. (2) [18] and Eq. (3) [18], [27], respectively. This value is used to create the medical stego image. After obtaining the d'_1 and d'_2 , MedProtect continues



Fig. 5. secret data chunk with k = 3

the bits concealment process by interpolating the original medical image to be further used for data

<i>A</i>	<i>b</i>	<i>c</i>	<i>D</i>
<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>
<i>i</i>	<i>j</i>	<i>k</i>	<i>l</i>
<i>M</i>	<i>n</i>	<i>o</i>	<i>P</i>

Fig. 6. Cover array produced from original image with the size $N = 2$.

concealment.

$$d' = d - 2^{k-1} \quad (1)$$

$$d'_1 = \left\lfloor \frac{d'}{2} \right\rfloor \quad (2)$$

$$d'_2 = \left\lfloor \frac{d'}{2} \right\rfloor \quad (3)$$

Step 4: MedProtect creates a new medical cover image array with a size of $(3N - 2 \times 3N - 2)$ where N equals the width and the height of the original medical image. Fig. 6 illustrates the array created from the original medical image with N equals two.

Step 5: At this step, the MedProtect approach continues by allocating every pixel from the original image into the cover image array. As illustrated in Fig. 6, the variables A, D, M , and P represent the location where the original pixel is placed in the new cover medical image.

Step 6: MedProtect then calculates the pixel pairs that lie horizontally and vertically between the original pixels by taking the average of the two surrounding original pixels. Referring to Fig. 6, to calculate the values of b and c , there is a computation of the average of A and D , then assigning the value to both b and c . Similarly, to calculate the values of e and i , average the values of A and M . Likewise, the values of h and l are obtained by averaging D and P , and assigned to both h and l . For n and o , the average of M and P is computed and assigned to both n and o . These interpolated pixel pairs are then used to represent the bits of the EPRs, following the process outlined in Step 8.

Step 7: To complete the interpolation process, MedProtect assigns the remaining empty pixels using the average of their surrounding pixels. For example, the new values in f, g, j, k are computed by averaging the values of b, c, e, g, i, j, k . For averaging purposes, any surrounding pixel that is unavailable has a value of 0.

Algorithm 1. Embedding Process

- (1) Load binary data
- (2) Split binary data into chunks of size k
- (3) Initialize empty lists d', d'_1, d'_2
- (4) **For** each chunk **do**:
- (5) Convert chunk to decimal value d
- (6) Append $(d - 2^{k-1})$ to d'
- (7) Append $\left\lfloor \frac{d'}{2} \right\rfloor$ to d'_1
- (8) Append $\left\lfloor \frac{d'}{2} \right\rfloor$ to d'_2
- (9) **End for**
- (10) Load original image $O[N, N]$
- (11) Create cover image $C[3N - 2, 3N - 2]$ initialized with zeroes
- (12) Place original pixels at scaled positions $(i \times 3, j \times 3)$
Perform horizontal interpolation:
- (13) **For** every row with original pixels in $C(i = 0, 3, 6, \dots)$ **do**:
- (14) Fill the gaps between the horizontal original pixels with the average of original pixels
- (15) **End for**
Perform vertical interpolation:
- (16) **For** every column in C **do**:
- (17) Fill the gaps between the vertical original pixels with the average of original pixels
- (18) **End for**
- (19) **For** every zeroes value in C **do**:
- (20) Fill with the average of 3×3 area
- (21) **End for**
- (22) **For** every horizontal and vertical pixel in between the original pixels **do**:
- (23) $pixel = pixel + d'_1$
- (24) $pixel = pixel - d'_2$
- (25) **End for**
- (26) Create stego image from C

Step 8: In this final stage of the EPRs sensitive data concealment, for each pixel pair produced from Step 6, update the first and second-pixel values only if their values are in the numerical range of $[2^{k-1}, 256 - 2^{k-1}]$ (to prevent overflow/underflow) using Eq. (4) [18], [28] and Eq. (5) [18] respectively. In this equation, the S_{val1} and S_{val2} are the resulting stego pixel values from adjusting the first pixel pair (P_{val1}) and the second pixel pair (P_{val2}) respectively. Applying these updates across all pairs produces the final stego image for transmission.

$$S_{val1} = P_{val1} + d'_1 \quad (4)$$

$$S_{val2} = P_{val2} - d'_2 \quad (5)$$

B. Extracting the embedded EPRs data and restoration of the original medical image

To validate the integrity of the proposed embedding process, both the hidden EPR data and the original

Algorithm 2. Extraction Process

```

(1) Load the stego image  $S$ 
(2) Initialize empty array  $sdb$ 
(3) For  $i \leftarrow 0$  to  $height(S)$  in steps of 3 do:
(4)   For  $j \leftarrow 0$  to  $width(S) - 3$  in steps of 3 do:
(5)      $a \leftarrow S[i, j + 1], b \leftarrow S[i, j + 2]$ 
(6)      $D = |a - b|$ 
(7)     If  $D > 0$  do:
(8)       Append  $sdb$  with binary form of
(9)        $D + 2^{(k-1)}$ 
(10)    Else do:
(11)      Continue
(12)    End if
(13)  End for
(14) For  $j \leftarrow 0$  to  $width(S)$  in steps of 3 do:
(15)   For  $i \leftarrow 0$  to  $height(S) - 3$  in steps of 3 do:
(16)      $a \leftarrow S[i + 1, j], b \leftarrow S[i + 2, j]$ 
(17)      $D = |a - b|$ 
(18)     If  $D > 0$  do:
(19)       Append  $sdb$  with binary form of
(20)        $D + 2^{(k-1)}$ 
(21)    Else do:
(22)      Continue
(23)    End if
(24)  End for
(25) Initialize original image array  $O \left[ \frac{(N+2)}{3}, \frac{(N+2)}{3} \right]$ 
(26) For  $i \leftarrow 0$  to  $height(S)$  do:
(27)   For  $j \leftarrow 0$  to  $width(S)$  do:
(28)      $O[i, j] = S[3 \times i, 3 \times j]$ 
(29)   End for
(30) End for
(31) Create original image from  $O$ 
(32) Return the extracted data in  $sdb$ 

```

medical image are extracted and assessed. The pseudocode for the extraction process is provided in Algorithm 2 to illustrate the steps involved clearly. The extraction process begins by loading the stego image and identifying the pixel pairs that were interpolated between the original pixels during the embedding process. These interpolated pairs are critical, as they serve as the locations where data may have been embedded.

For each extracted pixel pair (p_i, p_j) , the absolute difference $D = |p_i - p_j|$ is calculated. If $D = 0$, no data was embedded at that location. Otherwise, the embedded bit(s) for the EPRs are recovered using a predefined extraction function in Eq. (6) [18]. In this equation the S_{val1} and S_{val2} are the extracted stego pixel pair from the stego image, the k , is the chunk size used in the embedding process. After all data bits have

been retrieved, the original medical image is reconstructed by discarding the interpolated pixels and retaining only those located at the original coordinate positions. This restoration ensures the reversibility of the process, preserving the diagnostic quality of the image without introducing visual artifacts.

$$d = |S_{val1} - S_{val2}| + 2^{(k-1)} \quad (6)$$

IV. Experiments and Results**A. Experimental Dataset and Evaluation Metrics**

To evaluate the proposed MedProtect, we used cover images from the CT Medical Images dataset provided in TCGA-LUAD - The Cancer Imaging Archive (TCIA) [29] and from MIDAS/National Alliance for Medical Image Computing (NAMIC) [30], along with secret data of varying sizes (ranging from 1 to 100 kb) generated using the Lorem Ipsum text source [31]. All images were normalized to 512 x 512 pixels and converted to 8-bit greyscale to ensure dataset uniformity and reduce computational complexity, as shown in Fig. 7.

Moreover, MedProtect is assessed using PSNR and structural similarity index measure (SSIM), which are the key evaluation metrics in steganographic methods evaluation. The equation for PSNR is stated in Eq. (7) [32], which depends on the mean squared error (MSE) formula in Eq. (8) [33], [34]. The SSIM formula that evaluates the similarity between the cover and stego image is stated in Eq. (9) [35], [36]. The cover medical image is represented by the variable C , and the medical stego image is referred to as S . The v and w variable are the dimension of the image. The variables x_i and x_j represent the average pixel intensity, v_i and v_j represent the intensity variance, with $v_{i,j}$ representing the covariance. To assess robustness under commonly encountered lossy conditions. In addition to these quality-based metrics, we report the Bit Error Rate (BER) by counting the number of incorrectly extracted bits after the images were subjected to JPEG Compression. Furthermore, we are incorporating an independent two-sample t-test to statistically evaluate the differences in pixel distributions between cover and stego images.

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right) \quad (7)$$

$$MSE = \frac{1}{v \times w} \sum_{i=1}^v \sum_{j=1}^w (C(i, j) - S(i, j))^2 \quad (8)$$

$$SSIM = \frac{(2x_i x_j + C_1)(2v_{i,j} + C_2)}{(x_i^2 + x_j^2 + C_1)(v_i^2 + v_j^2 + C_2)} \quad (9)$$

B. Experimental results

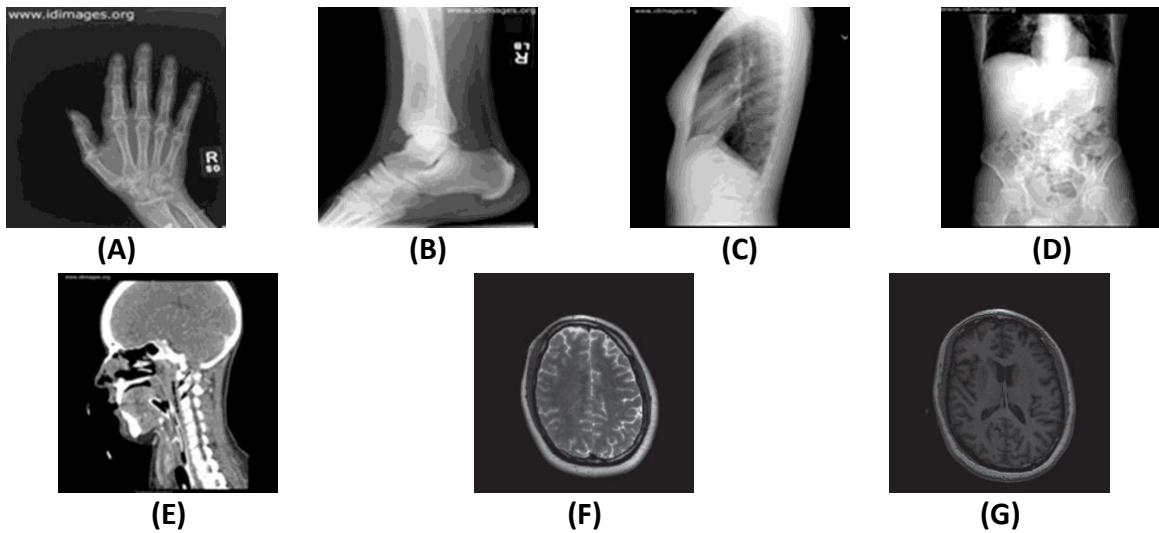


Fig. 7. Illustration of sample cover medical images. A: Hand, B: Leg, C: Chest, D: Abdominal, E: Head, F: Brain1, and G: Brain2

Table 1. Experimental results in PSNR with $k = 3$

Cover Image	Test payload sizes in kilobits (kb)										
	1	10	20	30	40	50	60	70	80	90	100
Hand	53.497	53.440	53.375	53.313	53.266	53.205	53.147	53.076	53.019	52.969	52.919
Leg	53.992	53.929	53.860	53.797	53.736	53.654	53.601	53.539	53.472	53.411	53.351
Chest	54.143	54.079	54.010	53.939	53.874	53.800	53.735	53.677	53.603	53.549	53.482
Head	48.279	48.262	48.244	48.226	48.208	48.190	48.169	48.153	48.135	48.118	48.102
Abdominal	53.149	53.099	53.041	52.986	52.933	52.875	52.828	52.776	52.715	52.673	52.621
Brain1	48.971	48.951	48.928	48.907	48.885	48.862	48.841	48.820	48.797	48.776	48.754
Brain2	49.384	49.361	49.337	49.313	49.290	49.264	49.242	49.218	49.193	49.170	49.146

Table 2. Experimental results in SSIM with $k = 3$

Cover Image	Test payload sizes in kilobits (kb)										
	1	10	20	30	40	50	60	70	80	90	100
Hand	0.9982	0.9981	0.9981	0.9980	0.9980	0.9979	0.9979	0.9978	0.9977	0.9977	0.9976
Leg	0.9983	0.9982	0.9982	0.9981	0.9981	0.9980	0.9979	0.9978	0.9978	0.9977	0.9976
Chest	0.9982	0.9982	0.9981	0.9981	0.9980	0.9979	0.9979	0.9978	0.9978	0.9977	0.9976
Head	0.9970	0.9970	0.9969	0.9969	0.9968	0.9967	0.9967	0.9966	0.9966	0.9965	0.9965
Abdominal	0.9975	0.9974	0.9974	0.9973	0.9973	0.9972	0.9972	0.9971	0.9971	0.9970	0.9970
Brain1	0.9966	0.9966	0.9965	0.9964	0.9964	0.9963	0.9962	0.9961	0.9961	0.9960	0.9959
Brain2	0.9960	0.9959	0.9959	0.9958	0.9957	0.9956	0.9956	0.9955	0.9954	0.9953	0.9953

The results in Table 1 and Fig. 8 demonstrate the effectiveness of the proposed method in maintaining high visual fidelity, particularly in less complex anatomical regions, such as the chest and legs. As presented in Table 1, the PSNR values (in dB), reflecting a closer similarity between the cover and stego medical images generated by MedProtect. These values are reported for seven anatomical image

Table 3. MSE obtained from the experimentation of the MedProtect with k = 3

Cover Image	Test payload sizes in kilobits (kb)										
	1	10	20	30	40	50	60	70	80	90	100
Hand	0.2907	0.2945	0.2989	0.3032	0.3065	0.3108	0.3150	0.3203	0.3244	0.3282	0.3320
Leg	0.2594	0.2632	0.2674	0.2713	0.2751	0.2803	0.2838	0.2879	0.2924	0.2965	0.3006
Chest	0.2505	0.2542	0.2583	0.2625	0.2665	0.2711	0.2752	0.2789	0.2836	0.2872	0.2917
Head	0.9664	0.9702	0.9743	0.9783	0.9824	0.9866	0.9912	0.9949	0.9990	1.0029	1.0067
Abdominal	0.3149	0.3185	0.3229	0.3270	0.3310	0.3354	0.3391	0.3432	0.3480	0.3514	0.3556
Brain1	0.8241	0.8280	0.8322	0.8364	0.8405	0.8450	0.8491	0.8533	0.8578	0.8619	0.8663
Brain2	0.7494	0.7532	0.7575	0.7616	0.7658	0.7703	0.7743	0.7786	0.7830	0.7871	0.7915

Table 4. BER obtained from the JPEG compression (%)

Cover Image	Test payload sizes in kilobits (kb)											
	1	10	20	30	40	50	60	70	80	90	100	Average
Hand	12.58	12.86	12.03	12.73	12.41	12.45	12.02	12.20	12.03	12.12	12.93	12.40
Leg	12.15	12.76	12.60	12.08	12.11	12.42	12.82	12.37	12.30	12.12	12.58	12.39
Chest	12.14	12.42	12.58	12.85	12.49	12.58	12.07	12.11	12.75	12.45	12.13	12.42
Head	12.40	12.56	12.25	12.53	12.61	12.22	12.47	12.05	12.32	12.38	12.41	12.38
Abdominal	12.95	12.20	12.83	12.25	12.90	12.38	12.14	12.76	12.19	12.63	12.73	12.54
Brain1	12.79	12.17	12.03	12.37	13.00	12.50	12.90	12.18	12.38	12.91	12.53	12.52
Brain2	12.15	12.76	12.60	12.08	12.11	12.42	12.82	12.37	12.30	12.12	12.58	12.43

categories: Hand, Leg, Chest, Head, Abdominal, Brain1, and Brain2, under varying payload sizes ranging from 1 to 100 kb. For all tested images, the PSNR values remain promising, as they are still within the admissible steganographic range (>30 dB).

Based on this foundation, the data also highlight a fundamental steganographic trade-off: PSNR predictably decreases across all medical images as payload size increases. This inverse correlation emphasizes the necessary compromise between steganographic capacity and image quality. For example, Chest images consistently achieve the highest PSNR, starting at 54.143 dB for 1 kb and decreasing slightly to 53.482 dB for 100 kb. While this reduction may appear modest, it exemplifies a limitation where the more EPR embedded will result in image degradation.

Anatomical characteristic further modulates this trend. In contrast to the Chest results, Head and Brain1 yield the lowest PSNR values, remaining nearly constant at 48.190 and 48.863. This suggests the method minorunderperforms when embedding occurs in bright, near-saturated regions with limited intensity headroom, resulting in small modifications that become more conspicuous and reduce fidelity. Performance is further hindered by large smooth, low-texture areas that offer little local variance or mid-high frequency energy, weakening perceptual masking and constraining embedding strength. These factors

explain the reduced performance observed for the Head and Brain1 images. Nevertheless, the PSNR values resulted from MedProtect remain high in absolute terms, showing that visual fidelity is still well preserved despite the decline.

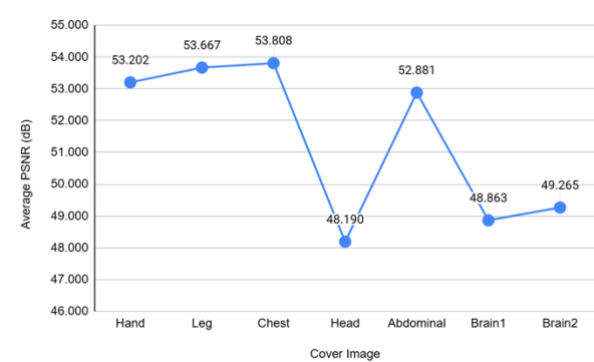


Fig. 8. Average PSNR for all images under the MedProtect

The graph in Fig. 8 demonstrates how the proposed MedProtect method consistently maintains high visual quality after embedding EPRs. Chest images achieved the highest average PSNR (53.808 dB), followed closely by Leg (53.667 dB), Hand (53.202 dB). On the Abdominal image where overlapping organs create edge intersection, the method slightly has a lower result at 52.881 dB. However, due to its high density from intricate bone trabecular patterns and detailed anatomical structures, the head image exhibits

performance degradation resulting in a PSNR of 48.190. Subsequently, followed by Brain1 and Brain2, characterized by their anatomical details, yield PSNR values of 48.863 and 49.265 respectively. Although the values showing lower PSNR than other objects, the results still remain within an acceptable diagnostic range.

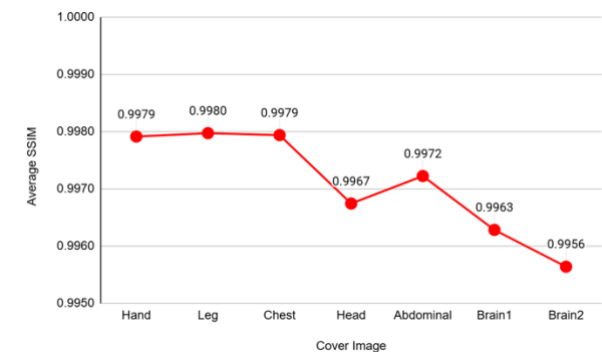


Fig. 9. Average PSNR for all images under the MedProtect

The SSIM result, as reported in Table 2, demonstrates high structural fidelity across all image types. As illustrated in Fig. 9, the highest average SSIM is observed in Leg images (0.9980), followed closely by Chest and Hand images (both 0.9979), Abdominal images (0.9972) and Head images (0.9967). Brain

imaging shows progressive decline with Brain1 (0.9963) and Brain2 achieving the lowest average SSIM (0.9956), though these values still indicate minimal perceptual distortion.

As seen in Fig. 9, all categories maintain SSIM values above 0.995, highlighting the method's ability to preserve anatomical structure even at high payload levels. The preservation of SSIM close to unity across all anatomical images demonstrates the suitability of MedProtect for medical applications, where structural integrity is crucial for accurate diagnosis and clinical use. Table 3 presents the MSE values for the considered test cover medical images under increasing payload sizes (1–100 kb).

The proposed MedProtect method consistently maintains low MSE values across all test cases, demonstrating its capacity to embed EPRs with minimal distortion. Chest images exhibit the lowest overall MSE (ranging from 0.2505 to 0.2917), followed closely by Leg (0.2594 to 0.3006) and Hand images (0.2907 to 0.3320). While Abdominal images show slightly higher MSE values (up to 0.3556), they remain within an acceptable range for clinical use. Brain2 demonstrates moderate MSE values (0.7494 to 0.7915), while Brain1 shows higher values (0.8241 to 0.8663). The Head images show the highest MSE values (0.9664 to 1.0067), which aligns with earlier PSNR and SSIM results, indicating that this region is more sensitive to data embedding.

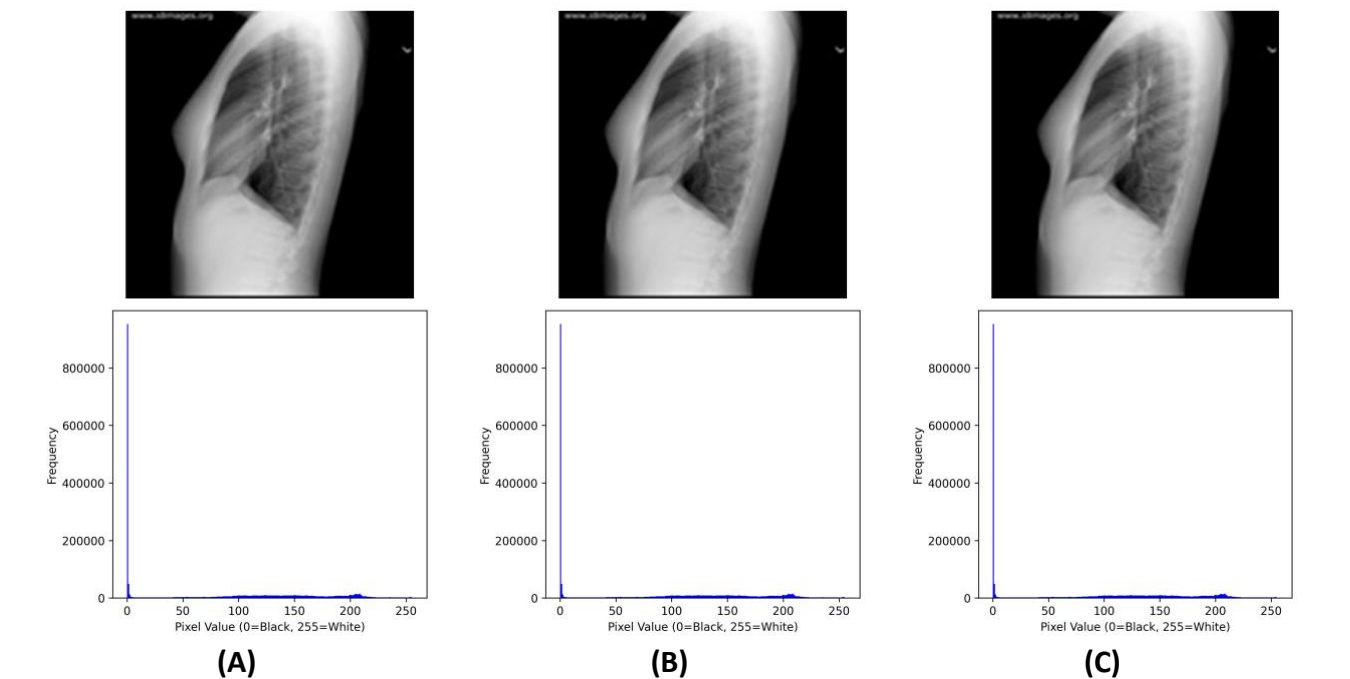


Fig. 10. Comparison of histogram for the cover and stego medical image. A: Cover Image, B: Stego image under 1 kb data, C: Stego image under 100 kb data.



Fig. 11. Representative visual comparisons. A: Cover image, B: Stego Image

Moreover, as shown in Fig. 10, the histograms of the stego medical images resemble the original cover image, demonstrating the visual and statistical consistency maintained by the proposed MedProtect 12.43%, resulting in a total average across the image at 12.44%. This stability across both image types and payload sizes indicates the robustness of MedProtect under lossy recompression scenarios.

Table 5. Two-sample t-Test result comparing cover image and stego image

Two Sample t-Test				
Cover Image	H	P-value	CI - Lower	CI - Upper
Hand	0	0.8637	-0.0853	0.0716
Leg	0	0.9273	-0.1398	0.1274
Chest	0	0.8202	-0.1643	0.1301
Head	0	0.8895	-0.1586	0.1376
Abdominal	0	0.9152	-0.1781	0.1597
Brain1	0	0.9208	-0.0730	0.0660
Brain2	0	0.8140	-0.0447	0.0351

method. Next, Fig. 11 showcases the comparison between the cover and stego image. The similarity of these figures indicates that the embedding process introduces negligible alterations to the pixel value distribution, ensuring that the perceptual quality of the medical images remains intact. Such preservation is crucial in clinical settings, where even minor distortions can affect diagnostic outcomes. The consistency across all histograms confirms that MedProtect is highly suitable for EPRs, enabling secure data embedding without compromising the diagnostic reliability of the host images.

To simulate lossy conditions typical of clinical storage and transmission, we compressed the stego images using JPEG and measured the bit error rate (BER) after the extraction across payloads from 1-100 kb. The proposed method achieved the result as shown in Table 4. The calculated average BER per cover image remains tightly concentrated with Hand at 12.40%, Leg 12.39%, Chest 12.42%, Head 12.38%, Abdominal 12.54%, Brain1 12.52%, and Brain2

In addition to other evaluations, an independent two-sample t-test was employed to statistically compare the pixel intensity distributions of each pair of cover and stego images. As shown in Table 5, the null hypothesis ($H = 0$) was retained for all image types, with p-values ranging from 0.8140 to 0.9273, all far above the 0.05 significance threshold. The 95% confidence intervals for the mean differences in each case spanned zero (e.g., Hand: -0.0853 to 0.0716), indicating that any observed differences in pixel values could be due to random artifacts rather than a well-designed change introduced by the embedding process. Overall, the evaluation results affirm that the proposed method is well-suited for medical applications, where maintaining visual and statistical characteristics of images is important.

C. Results Comparisons

Fig. 12 presents a comparative analysis of the PSNR performance of the proposed MedProtect method against Aminy et al. [37], Ananti et al. [38], Malik et al. [24], Karakus and Avci [39], and Hussain and Khoder

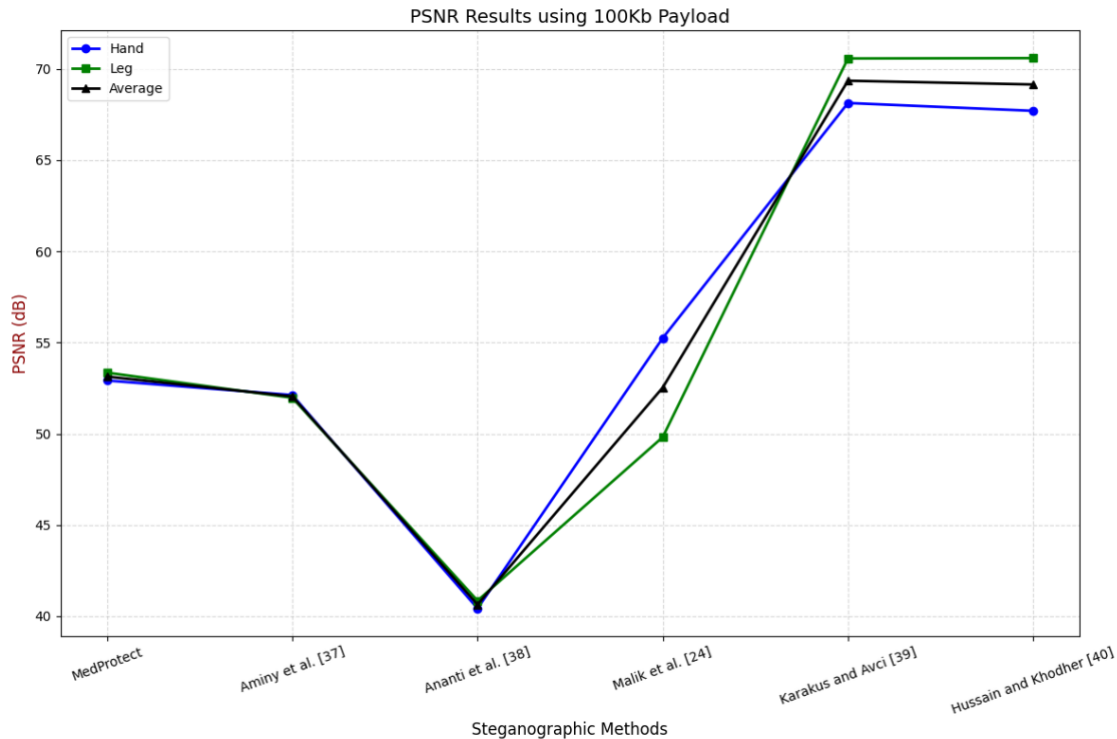


Fig. 12. Comparison of the PSNR performance of the proposed MedProtect and the existing methods

[40]. Five existing steganographic techniques. The evaluation focuses on two anatomical image categories, Hand and Leg, as well as their overall average, offering a comprehensive assessment of visual fidelity after data embedding.

Based on Fig. 12, Ananti et al. show the most significant limitation with average PSNR at 40.639 dB, followed by Aminy et al. [37] with an average PSNR of 52.046 dB, indicating visual degradation that could potentially harm the diagnostic reliability. While Malik et al demonstrate improving PSNR with Hand at 55.245 dB, Leg at 49.816, and an average of 52.530, the result still showcases inconsistencies across different anatomical regions. Following that, Karakus and Avci [39]Hussain and Khoder [40] achieve higher average PSNR values of 69.360 dB and 69.145 dB, respectively.

Despite the MedProtect achieving consistent PSNR values of 53 dB across both Hand and Leg, which positions it competitively within the evaluated methods, it demonstrates an advantage through its keyless-reversible steganography approach that enables complete restoration of the original medical image without requiring additional encryption keys. This keyless recovery eliminates the critical vulnerability of key management while ensuring perfect reconstruction of diagnostic images.

D. Discussion

This study aims to develop a new steganography method, MedProtect, to strengthen data transmission in the medical domain. The proposed method was tested on 7 different medical images and payload sizes ranging from 1kb to 100kb. Each medical image used was resized to 512 x 512 pixels and converted to 8-bit greyscale prior to embedding.

The performance of the proposed method is assessed using PSNR, SSIM, and MSE. As shown in Fig. 8 and Fig. 9, MedProtect achieve the highest average PSNR at 53.808 dB for Chest image, and the highest average SSIM at 0.9980 for Leg image. The MSE resulted from the experiment further confirmed this, with the Chest image yielding the lowest error at 0.2505 for 1 kb payload and only increasing slightly to 0.2917 for 100 kb payload, indicating stable performance as the payload grows.

To verify the robustness of MedProtect under lossy conditions, we provide the results of the bit error rate (BER) after the stego image is compressed under JPEG compression, as shown in Table 4. The results shows that BER remained stable, averaging at 12.44% with no significant increase as payload increases, demonstrating resilience against compression. Moreover, to compare the pixel intensity distribution between the cover image and the stego image, the method is evaluated with a two-sample t-test. From Table 5 the method achieves H = 0 for all tested

images. This value indicates that there is no significant difference between the cover image and the stego image. The p-values that achieved at range 0.8140 to 0.9208 further validate this claim. The confidence intervals (CI - Lower and CI - Upper), which spanned zero for every case, show that any observed difference in pixel values could be due to random artifacts rather than an intentional change from the embedding process.

Despite these strengths, MedProtect tends to perform less effectively in bright, near-saturated regions where intensity headroom is limited. Even small alterations become more noticeable in such areas, leading to reduced visual fidelity. This condition happened in an image such as Head image, where it consists of dense bone regions with very bright areas, resulting in the lowest PSNR value among all the tested images at average of 48.190 dB. Similarly, in the Brain1 image consisting of low texture with limited local variation, the method underperforms, resulting in a PSNR value of 48.863 dB. This can be explained because modifications are more easily detected in the low-texture area. Moreover, the increasing size of embedded data further influences the overall image quality.

Nevertheless, MedProtect demonstrates competitive performance compared to existing methods in a 100kb payload size. For example, in the Hand and Leg images, MedProtect achieved PSNR values of 52.919 dB and 53.351 dB, respectively, while achieving an average of both images at 53.135 dB. This outperforms Ananti et al. [38], whose method achieved only 40.639 dB on average for the same images (40.426 dB for Hand and 40.852 dB for Leg), representing the lowest performance among the compared methods. Next, the method by Aminy et al. [37] reported a higher average result of 52.046 dB with values of 52.120 dB for the Hand image and 51.972 dB for the Leg image. Meanwhile, the interpolation steganography method by Malik [24] obtained slightly higher average result at 52.530 dB. Still, its results varied significantly between images, recording only 49.815 dB for the Leg image while reaching 55.245 dB for the Hand image. In contrast, MedProtect surpasses these averages and delivers more consistent performance across different images, highlighting its robustness and reliability compared to existing approaches. Although Karakus and Avci [39] and Husein and Khoder [40] reported higher PSNR values. Where Karakus and Avci sit at an average of 69.350 dB, Husein and Khoder at 69.145 dB for the average. MedProtect offers a distinct advantage through its keyless reversible steganography design. This feature is particularly valuable in the medical domain, where the ability to restore the original image perfectly is

essential for ensuring diagnostic reliability and clinical trust.

V. Conclusion

This study introduces MedProtect, a keyless reversible steganography method aims to embed EPRs within medical images while preserving diagnostic quality securely. By combining center folding principles with advanced interpolation techniques, MedProtect is able to achieve high average PSNR ranging from 48.190 dB to 53.808 dB across all the tested images, showing the robustness of the method. Although the PSNR tends to decrease as the EPRs data rises, comparative results confirm that MedProtect achieves competitive performance with existing methods while preserving image integrity through its reversible approach, demonstrating strong potential for real-world clinical deployment.

Future plans will include MedProtect to handle color and volumetric (3D) medical images, extending its usefulness across more imaging modalities. To enable deployment in time-sensitive healthcare workflows, further development will also optimize interpolation methods to speed up embedding and extraction while maintaining fidelity. Finally, further research will investigate more advanced transform-based approaches to conceal payloads better and reduce vulnerability to steganalysis, further enhancing security and perceptual transparency in medical data protection. This will bolster reliability, scalability, interoperability, and seamless clinical integration.

Acknowledgment

The authors thank all Cyber Security Research Group members, Net-Centric Computing Laboratory, Department of Informatics, ITS, for their support and discussion.

Funding

The research was supported by Institut Teknologi Sepuluh Nopember (ITS).

Author Contribution

Aditya Rizki Muhammad: Conceptualization, Software, Validation, Formal analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Visualization. Irsyad Fikriansyah Ramadhan: Methodology, Validation, Formal analysis, Resources, Writing - Original Draft, Visualization. Ntivuguruzwa Jean De La Croix: Conceptualization, Methodology, Formal analysis, Investigation, Writing - Review & Editing. Tohari Ahmad: Conceptualization, Methodology, Writing - Review & Editing, Supervision, Project administration, Funding acquisition. Dieudonne Uwizeye: Conceptualization, Methodology, Writing - Review & Editing. Evelyne Kantarama: Conceptualization, Methodology, Writing - Review & Editing.

Declaration**Ethical Approval**

This research uses public datasets from The Cancer Imaging Archive (TCIA) and MIDAS/National Alliance for Medical Image Computing (NAMIC).

Consent for Publication Participants

All participants gave consent for publication.

Competing Interests

The authors declare no competing interests.

References

- [1] S. T. Miller and R. G. Pickering, "CLINICAL CASE Use of Electronic Patient Data in Research Commentary," *American Medical Association Journal of Ethics*, vol. 13, pp. 148–151, 2011, Accessed: May 20, 2025. [Online]. Available: www.virtualmentor.org
- [2] A. O. Adeniyi, J. O. Arowoogun, R. Chidi, C. A. Okolo, and O. Babawarun, "The impact of electronic health records on patient care and outcomes: A comprehensive review," *World Journal of Advanced Research and Reviews*, vol. 21, no. 2, pp. 1446–1455, Feb. 2024, doi: 10.30574/wjarr.2024.21.2.0592.
- [3] E. Kim, S. M. Rubinstein, K. T. Nead, A. P. Wojcieszynski, P. E. Gabriel, and J. L. Warner, "The Evolving Use of Electronic Health Records (EHR) for Research," *Semin Radiat Oncol*, vol. 29, no. 4, pp. 354–361, Oct. 2019, doi: 10.1016/J.SEMRADONC.2019.05.010.
- [4] C. N. Vorisek, M. Lehne, S. A. I. Klopfenstein, P. J. Mayer, A. Bartschke, T. Haese, and S. Thun, "Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review," *JMIR Med Inform*, vol. 10, no. 7, Jul. 2022, doi: 10.2196/35724.
- [5] S. N. Duda, N. Kennedy, D. Conway, A. C. Cheng, V. Nguyen, T. Zayas-Cabán, and P. A. Harris, "HL7 FHIR-based tools and initiatives to support clinical research: a scoping review," *Journal of the American Medical Informatics Association*, vol. 29, no. 9, pp. 1642–1653, Aug. 2022, doi: 10.1093/JAMIA/OCAC105.
- [6] A. W. Chanda D'Layla, N. J. De La Croix, T. Ahmad, and F. Han, "EHR-protect: A steganographic framework based on data-transformation to protect electronic health records," *Intelligent Systems with Applications*, vol. 26, Jun. 2025, doi: 10.1016/j.iswa.2025.200493.
- [7] H. A. Khan, R. Abdulla, S. K. Selvaperumal, and A. Bathich, "IoT based on secure personal healthcare using RFID technology and steganography," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 4, pp. 3300–3309, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3300-3309.
- [8] M. M. Hashim, S. H. Rhaif, A. A. Abdulrazzaq, A. H. Ali, and M. S. Taha, "Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography," in *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, Aug. 2020, doi: 10.1088/1757-899X/881/1/012120.
- [9] K. Shimada, R. Suketomo, M. Misumi, M. Inagaki, and T. Kodama, "Physical security attacks on symbol masking schemes using time-spread cryptographic keys in digital coherent communication," *Opt Commun*, vol. 590, Oct. 2025, doi: 10.1016/j.optcom.2025.131986.
- [10] G. Kalaiaresi, B. Sudharani, S. C. Jonnalagadda, H. V. Battula, and B. Sanagala, "A Comprehensive Survey of Image Steganography," in *2nd International Conference on Sustainable Computing and Smart Systems, ICSCSS 2024 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1225–1229, doi: 10.1109/ICSCSS60660.2024.10625295.
- [11] I. F. Ramadhan, N. J. De La Croix, T. Ahmad, and A. Uzamurengera, "Huffman coding-based data reduction and quadristego logic for secure image steganography," *Engineering Science and Technology, an International Journal*, vol. 65, p. 102033, May 2025, doi: 10.1016/J.JESTCH.2025.102033.
- [12] R. Apau, M. Asante, F. Twum, J. Ben Hayfron-Acquah, and K. O. Peasah, "Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review," *PLoS One*, vol. 19, no. 9, p. e0308807, Sep. 2024, doi: 10.1371/journal.pone.0308807.
- [13] Z. Pakdaman, H. Nezamabadi-pour, and S. Saryazdi, "A new reversible data hiding in transform domain," *Multimed Tools Appl*, vol. 80, no. 6, pp. 8931–8955, Mar. 2021, doi: 10.1007/s11042-020-10058-6.
- [14] S. Hemalatha, U. D. Acharya, A. Renuka, P. R. Kamath, "A Secure Color Image Steganography in Transform Domain," *International Journal on Cryptography and Information Security*, vol. 3, no. 1, pp. 17–24, Mar. 2013, doi: 10.5121/ijcis.2013.3103.
- [15] H. Ye, K. Su, X. Cheng, and S. Huang, "Research on reversible image steganography of encrypted image based on image interpolation and difference histogram shift," *IET Image Process*, vol. 16, no. 7, pp. 1959–1972, May 2022, doi: 10.1049/ipr2.12461.

- [16] G. Gao, S. Tong, Z. Xia, B. Wu, L. Xu, and Z. Zhao, "Reversible data hiding with automatic contrast enhancement for medical images," *Signal Processing*, vol. 178, p. 107817, Jan. 2021, doi: 10.1016/J.SIGPRO.2020.107817.
- [17] Q. Wang and R. K. Ward, "A new orientation-adaptive interpolation method," *IEEE Transactions on Image Processing*, vol. 16, no. 4, pp. 889–900, Apr. 2007, doi: 10.1109/TIP.2007.891794.
- [18] T. C. Lu, J. H. Wu, and C. C. Huang, "Dual-image-based reversible data hiding method using center folding strategy," *Signal Processing*, vol. 115, pp. 195–213, Oct. 2015, doi: 10.1016/J.SIGPRO.2015.03.017.
- [19] T. N. Vo and T. C. Lu, "Dynamic payload adjustment in image steganography through interpolation and center folding strategies," *Signal Processing*, vol. 235, p. 110030, Oct. 2025, doi: 10.1016/J.SIGPRO.2025.110030.
- [20] K. Mavrogiorgos, A. Kiourtis, A. Mavrogiorgou, S. Kleftakis, and D. Kyriazis, "A Multi-layer Approach for Data Cleaning in the Healthcare Domain," *ACM International Conference Proceeding Series*, pp. 22–28, Jan. 2022, doi: 10.1145/3512850.3512856.
- [21] S. J. Devaraj, "Emerging Paradigms in Transform-Based Medical Image Compression for Telemedicine Environment," *Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare*, pp. 15–29, Jan. 2019, doi: 10.1016/B978-0-12-816948-3.00002-7.
- [22] K. H. Jung and K. Y. Yoo, "Data hiding method using image interpolation," *Comput Stand Interfaces*, vol. 31, no. 2, pp. 465–470, Feb. 2009, doi: 10.1016/j.csi.2008.06.001.
- [23] C. F. Lee and Y. L. Huang, "An efficient image interpolation increasing payload in reversible data hiding," *Expert Syst Appl*, vol. 39, no. 8, pp. 6712–6719, Jun. 2012, doi: 10.1016/j.eswa.2011.12.019.
- [24] A. Malik, G. Sikka, and H. K. Verma, "A Reversible Data Hiding Scheme for Interpolated Images Based on Pixel Intensity Range," *Multimed Tools Appl*, vol. 79, no. 25–26, pp. 18005–18031, Jul. 2020, doi: 10.1007/s11042-020-08691-2.
- [25] R. Punia, A. Malik, and S. Singh, "An interpolation-based reversible data hiding scheme for internet of things applications," *Discover Internet of Things*, vol. 3, no. 1, pp. 1–16, Dec. 2023, doi: 10.1007/S43926-023-00048-Z/TABLES/4.
- [26] S. Solak and G. Tezcan, "A New Dual Image Based Reversible Data Hiding Method Using Most Significant Bits and Center Shifting Technique," *Applied Sciences* 2022, Vol. 12, Page 10933, vol. 12, no. 21, p. 10933, Oct. 2022, doi: 10.3390/APP122110933.
- [27] C. Shaji and I. Shatheesh Sam, "New Center Folding Strategy Encoding for Reversible Data Hiding in Dual Stego Images," 2021, pp. 83–89, doi: 10.1007/978-981-16-2248-9_9.
- [28] V. A. Pham, N. H. Nguyen, Q. H. Le, K. S. Nguyen, T. L. Cao, and M. T. Pham, "Reversible image authentication using a central folding strategy with two images," *Multimed Tools Appl*, vol. 83, no. 24, pp. 64441–64465, Jul. 2024, doi: 10.1007/s11042-024-18165-4.
- [29] B. Albertina, M. Watson, C. Holback, R. Jarosz, S. Kirk, Y. Lee, K. Rieger-Christ, and J. Lemmerman, "The Cancer Genome Atlas Lung Adenocarcinoma Collection (TCGA-LUAD) (Version 4) [Data set]." Accessed: Aug. 2025. [Online]. Available: <https://www.cancerimagingarchive.net/collection/tcga-luad/>
- [30] "National Alliance for Medical Image Computing." Accessed: Aug. 13, 2025. [Online]. Available: <https://www.na-mic.org/>
- [31] "Lorem Ipsum - All the facts - Lipsum generator." Accessed: May 19, 2025. [Online]. Available: <https://www.lipsum.com/>
- [32] C. Ding, M. Zhang and Y. Gu, "Study on image quality Control Method based on Gaussian Noise," *J Phys Conf Ser*, vol. 2029, no. 1, p. 012034, Sep. 2021, doi: 10.1088/1742-6596/2029/1/012034.
- [33] T. O. Hodson, T. M. Over, and S. S. Foks, "Mean Squared Error, Deconstructed," *J Adv Model Earth Syst*, vol. 13, no. 12, p. e2021MS002681, Dec. 2021, doi: 10.1029/2021MS002681.
- [34] D. S. K. Karunasingha, "Root mean square error or mean absolute error? Use their ratio as well," *Inf Sci (N Y)*, vol. 585, pp. 609–629, Mar. 2022, doi: 10.1016/J.INS.2021.11.036.
- [35] V. Mudeng, M. Kim, and S. W. Choe, "Prospects of Structural Similarity Index for Medical Image Analysis," *Applied Sciences* 2022, Vol. 12, Page 3754, vol. 12, no. 8, p. 3754, Apr. 2022, doi: 10.3390/APP12083754.
- [36] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimed Tools Appl*, vol. 80, no. 6, pp. 8423–8444, Mar. 2021, doi: 10.1007/s11042-020-10035-z.
- [37] M. R. H. Aminy, N. J. De La Croix, and T. Ahmad, "A Reversible Data Hiding Approach in Medical Images Using Difference Expansion," *Proceedings - 2023 15th IEEE International Conference on Computational Intelligence and Communication Networks, CICN 2023*, pp. 358–

- 362, 2023, doi: 10.1109/CICN59264.2023.10402139.
- [38] M. S. Ananti, A. W. C. D'Layla, N. J. D. La Croix, and T. Ahmad, "FuzzyStego: An Adaptive Steganographic Scheme Using Fuzzy Logic for Optimizing Embeddable Areas in Spatial Domain Images," *Computers, Materials & Continua*, vol. 0, no. 0, pp. 1–10, 2025, doi: 10.32604/cmc.2025.061246.
- [39] S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," *Med Hypotheses*, vol. 139, p. 109691, Jun. 2020, doi: 10.1016/J.MEHY.2020.109691.
- [40] A. Z. Hussain and M. A. A. Khoder, "Securing Medical Images Using Chaotic Map Encryption and LSB Steganography," *Revue d'Intelligence Artificielle*, vol. 38, no. 1, pp. 313–321, Feb. 2024, doi: 10.18280/RIA.380133.

Author Biography



Aditya Rizki Muhammad is a student in the Department of Informatics at Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia. His research interests include information security, which relates to steganography, with a particular emphasis on digital image processing, interpolation techniques, and transformation methods; and network security, specifically in intrusion detection systems and computer networks. Muhammad is active in the Net Centric Computing Laboratory, where he serves as an assistant managing the research, and coordinating the research activities. Additionally, he is also a member of the Cyber Security Research Group (CSRG), investigating how to protect secret or sensitive data.



Irsyad Fikriansyah Ramadhan is a student in the Department of Informatics at Institut Teknologi Sepuluh Nopember (ITS), Indonesia, where he has been enrolled since 2021 and is expected to graduate with a bachelor's degree in 2025. His research has led to several publications, including a paper presented at a conference and another published in a high-impact Q1 international journal. His primary research interests include steganography and botnet detection, particularly within information security. Motivated by the growing demand for secure and reliable systems, he

strives to develop innovative methods that integrate both practical applicability and academic rigor. In addition to his research, he has served as a teaching assistant in his department. He has contributed as a research assistant at the Net-Centric Computing Laboratory, where he supported colleagues and junior researchers in co-authoring publications.



Ntivuguruzwa Jean De La Croix (Member, IEEE) received a B.Sc. degree in computer science and systems from the National University of Rwanda, Rwanda, a master's degree in information technology from the University of Madras, India, a PGD 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 pursuing a PhD in computer science at Institut Teknologi Sepuluh Nopember (ITS), Indonesia. His current research interests include steganography, steganalysis, and deep learning for data security in public networks. He reviews for several journals from IEEE, Elsevier, Springer, and others.



Tohari Ahmad is a Professor of Computer Science at the Institut Teknologi Sepuluh Nopember (ITS), Indonesia. Prof. Ahmad was a consultant for several international companies before joining ITS in 2003. His research interests include network security, information security, data hiding, and computer networks. He is an active member of the IEEE and ACM and a reviewer for several high-impact international journals. Prof. Ahmad has received multiple honors, including the Hitachi Research Fellowship and the JICA Research Program, to support research activities in Japan. In 2024, he was recognized among the world's top 2% of scientists in the Elsevier global ranking.



Dieudonne Uwizeye is a professor of demography, currently working for the University of Rwanda as the Director of Research and Innovation at the College of Arts and Social Sciences. His research bridges population dynamics and health with a strong focus on access to healthcare and wellbeing, and resource distribution in low-income settings. He has led and collaborated on numerous national and international health-related research projects, published extensively in peer-reviewed journals, and

secured competitive grants to support evidence-based policy and practice in the medical and public health sectors. He is also a regular reviewer for several highly reputed international journals in public health, population studies, and social science research.



Evelyne Kantarama is a Rwandan biomedical scientist. She is a lecturer at the University of Rwanda's College of Medicine and Health Sciences, clinical pathology department, and a Clinical Biochemistry specialist at the University Teaching Hospital of Kigali-CHUK. Her research focuses

on cardiometabolic diseases, with particular interest in the molecular mechanisms underlying diabetes mellitus, dyslipidemia, systemic inflammation, hypertension, and obesity. Dr. Kantarama is actively involved in identifying biomarkers for early disease detection, risk stratification, and the development of personalized treatment approaches. She also serves as a reviewer for several high-ranking international journals in clinical biochemistry and medical sciences.