International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2285-2295
Journal homepage: http://iieta.org/journals/ijsse

MedRec-Secure: A Framework for Confidentiality Preservation in Medical Patient Records

Tigo S Yoga[1], Ntivuguruzwa Jean De La Croix[2,3,4], Tohari Ahmad[1*], Royyana Muslim Ijtihadie[1], Wahyu Suadi[1]

[1] Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya 60111, Indonesia
[2] Department of Business Information Technology, College of Business and Economics, University of Rwanda, Kigali 4285, Rwanda
[3] Department of Technology Innovation, SecureAI Laboratories, Kigali 6100, Rwanda
[4] Faculty of Computing and Information Science, University of Lay Adventist of Kigali (UNILAK), Kigali 6392, Rwanda

Corresponding Author Email: tohari@its.ac.id

https://doi.org/10.18280/ijsse.151109

Received: 23 October 2025
Revised: 24 November 2025
Accepted: 27 November 2025
Available online: 30 November 2025

Keywords:
Medical Patient Records, cyber security, data hiding, information hiding, information security, national security, ICT infrastructure

ABSTRACT

The digitization of healthcare has revolutionized patient data management through Medical Patient Records (MPRs), but has simultaneously introduced critical security vulnerabilities, as traditional cryptographic methods explicitly reveal the presence of sensitive information. This study introduces MedRec-Secure, a comprehensive data hiding scheme designed to enhance MPR confidentiality through a novel Dynamic Subtractor Selection Steganographic Framework (DSSSF) that conceals sensitive medical information within medical images while preserving diagnostic quality. The proposed framework operates on grayscale medical images divided into 4-pixel blocks, employing statistical analysis to select optimal reference pixels dynamically. A multi-zone embedding strategy categorizes pixels into three intensity zones, with tailored embedding rules for each zone. Experimental evaluation demonstrated superior performance, with a Peak Signal-to-Noise Ratio (PSNR) achieving a maximum of 75.43 dB across varying MPR payload sizes (1 kb to 100 kb). The Structural Similarity Index Measure (SSIM) achieved outstanding maximum values of 1.000, maintaining near-perfect similarity despite slight decreases with larger payloads. MedRec-Secure outperforms existing methods by 3.2 dB in PSNR performance, preserving diagnostic image integrity while enabling secure MPR transmission across healthcare networks.

1. INTRODUCTION

The digital revolution in healthcare has fundamentally transformed patient data management paradigms, with Electronic Health Records (EHRs) or Medical Patient Records (MPRs) emerging of modern medical information systems [1, 2]. This transformation has facilitated unprecedented improvements in healthcare delivery efficiency, clinical decision-making, and patient care coordination across diverse healthcare networks [3]. However, the exponential growth of digital health data, coupled with increasingly sophisticated cyber threats, has simultaneously introduced critical security vulnerabilities that threaten the confidentiality and integrity of sensitive medical records [4].

Healthcare environments face security challenges that extend beyond traditional data protection concerns. The interconnected nature of modern healthcare systems, where MPRs must traverse multiple networks and be accessible to various stakeholders, creates numerous potential attacks [5]. Data breaches in healthcare result in substantial financial losses and also compromise patient trust. This can potentially endanger patient safety when medical information is manipulated by unauthorized entities.

Traditional security methodologies, primarily relying on cryptographic techniques such as symmetric and asymmetric encryption algorithms, while providing essential data confidentiality, possess inherent limitations in the context of covert healthcare communications. Encrypted data explicitly advertises the presence of sensitive information, potentially attracting unwanted scrutiny from adversaries and increasing the likelihood of targeted decryption attempts [6]. Encryption methods do not address the growing need for secure communication channels that maintain operational covertness in potentially compromised network environments [7].

Steganography emerges as a complementary security paradigm that addresses these limitations by concealing confidential data rather than merely obscuring their content [8]. This technique provides security through obscurity by embedding sensitive information within carrier media, thereby enabling covert data transmission without raising suspicion [9]. In healthcare contexts, where medical images such as radiographs, computed tomography (CT) scans, and magnetic resonance imaging (MRI) data are routinely transmitted and stored, steganographic techniques offer unique opportunities for secure MPR distribution [10]. As depicted in Figure 1, the embedding process to put MPR into medical images

encompasses two fundamental stages: the embedding stage, where confidential medical information is concealed using Medical Data Embedding (MDE) algorithms, and the extraction stage, where the hidden MPR is reconstructed from the stego image.

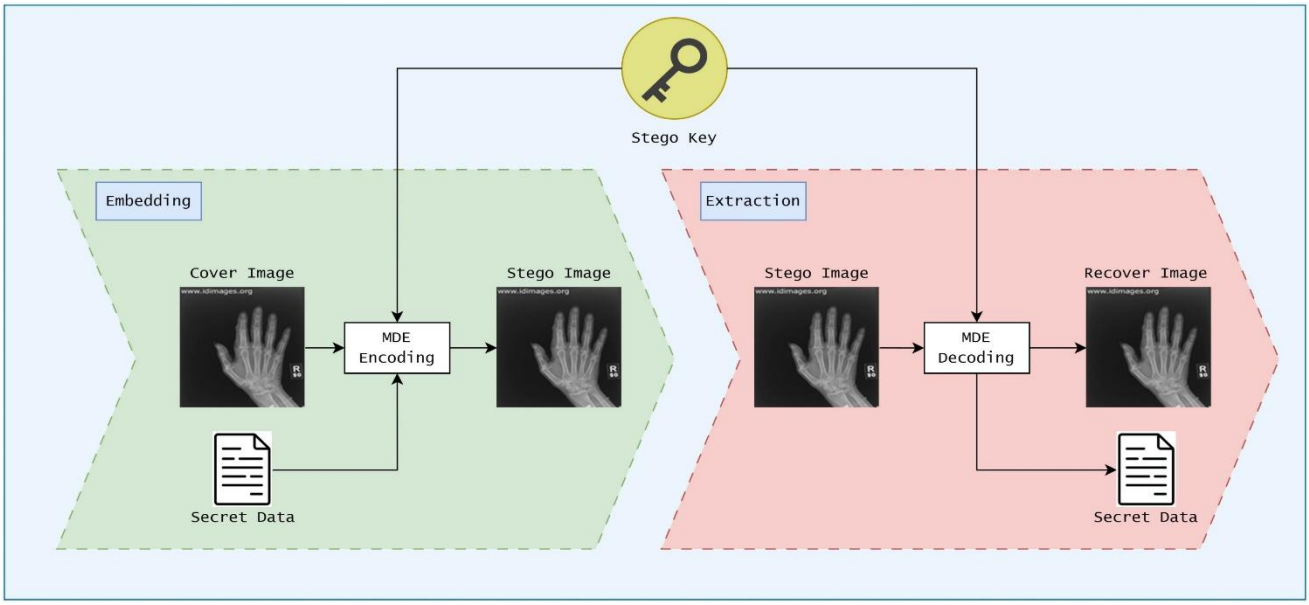

Figure 1. System architecture for steganographic Medical Patient Records (MPRs) data communication

The application of steganography to medical data protection presents distinctive challenges that differentiate it from conventional steganographic applications [11]. Medical images serve as carriers of hidden data for diagnostic tools afterwards. Consequently, any modification must maintain the integrity and visual quality of medical images while providing sufficient embedding capacity [12]. Small distortion in medical imagery can compromise diagnostic accuracy and potentially impact patient care outcomes.

Existing steganographic approaches for healthcare applications predominantly employ static embedding strategies that lack adaptability to varying image characteristics and data payload requirements [13]. These methods often suffer from limited embedding capacity, rendering them unsuitable for medical applications. Moreover, current techniques may fail to provide adequate resistance against modern steganalysis methods, limiting their practical applicability.

To address these critical limitations, this research introduces MedRec-Secure, a comprehensive data hiding scheme specifically designed to enhance MPR confidentiality. The MedRec-Secure operates on the principle of intelligent reference pixel selection within image blocks, where statistical analysis determines the most suitable subtractor pixels for embedding operations. This dynamic approach, combined with a sophisticated multi-zone embedding strategy that categorizes pixels based on intensity ranges, enables the system to maximize data hiding capacity while minimizing visual artifacts and preserving diagnostic image quality. The primary contributions of this research can be described as follows:

1. Development of an adaptive reference pixel selection algorithm that analyzes local statistical properties, including mean values and standard deviations, to identify optimal subtractor pixels within image blocks. This mechanism enhances embedding adaptability and reduces predictable patterns.
2. Introduction of an intelligent embedding approach that categorizes pixel intensities into three distinct zones (Zone 1: 0-85, Zone 2: 86-171, Zone 3: 172-254) with tailored embedding rules and conditions for each zone. This optimizes embedding capacity while minimizing visual distortion through zone-specific modification formulas.
3. Development of embedding algorithms optimized explicitly for medical imaging applications.

The next parts of this paper are organized as follows: Section 2 presents the literature review covering advances in healthcare data security and existing steganographic techniques for medical applications. Section 3 details the implementation flow of the proposed MedRec-Secure. The results of the experiments are explicitly reported in Section 4, and Section 5 concludes this study.

2. RELATED WORKS

Steganography in medical contexts presents unique challenges and opportunities compared to conventional digital steganography applications [14]. Spatial domain steganographic methods represent the most widely researched category of medical steganography techniques due to their computational efficiency and relative simplicity of implementation [15, 16]. The foundational Least Significant Bit (LSB) substitution method, while offering high embedding capacity, is vulnerable to statistical attacks and can introduce detectable patterns in medical images [17]. A previous study developed one of the early medical steganography applications, embedding electroencephalogram (EEG) and prescription data within medical images using enhanced LSB techniques with pixel similarity metrics [18]. Their approach achieved embedding capacities of up to 0.25 bits per pixel while maintaining acceptable visual quality. However, subsequent analysis demonstrated that the method was susceptible to histogram-based steganalysis techniques commonly used in forensic analysis [19].

Pixel Value Differencing (PVD) techniques have shown promise in medical image steganography due to their adaptive nature and improved resistance to statistical attacks. Huang et al. [20] proposed a modified PVD approach designed explicitly for radiographic images, utilizing region classification to vary embedding strategies based on clinical importance. Their method achieved superior imperceptibility in critical diagnostic regions while maximizing embedding capacity in non-critical areas. The approach demonstrated embedding capacities ranging from 0.18 to 0.31 bits per pixel, depending on image content, with PSNR values consistently above 45 dB for radiographic images.

The Difference Expansion (DE) technique has been adapted for medical applications, with a particular focus on the reversibility requirements essential for clinical environments. Wang and Fun developed a reversible DE steganography method for images, which was able to restore the original image after information extraction [21]. This approach is particularly valuable in medical contexts where the integrity of images must be maintained. Their method achieved embedding capacities of up to 0.22 bits per pixel while maintaining reversibility and PSNR values above 48 dB.

Transform domain steganographic approaches operate on frequency representations of medical images, offering potential advantages in terms of robustness and imperceptibility. Discrete Cosine Transform (DCT) based steganography has been investigated for medical applications, with particular focus on JPEG-compressed medical images commonly used in Picture Archiving and Communication Systems (PACS). Mohammed et al. proposed a DCT-based steganographic framework for embedding patient metadata within JPEG-compressed radiographic images [22]. Their approach utilized quantization table modification to embed information while maintaining JPEG compatibility. The method demonstrated good resistance to compression attacks but suffered from a limited embedding capacity (0.08-0.15 bits per pixel) and potential degradation in diagnostic quality in high-frequency image regions.

Discrete Wavelet Transform (DWT) techniques have shown promise for medical steganography due to their multi-resolution analysis capabilities. Soundrapandiyan et al. [23] developed a DWT-based embedding system that analyzes wavelet coefficients to identify optimal embedding locations. Their approach achieved improved imperceptibility compared to spatial domain methods with PSNR values above 52 dB, but required higher computational resources for embedding and extraction operations. The method demonstrated embedding capacities of 0.19-0.28 bits per pixel, depending on the selected wavelet basis and decomposition levels.

Adaptive and intelligent steganographic systems represent the latest advancement in medical steganography research, incorporating machine learning and optimization techniques. Chen et al. proposed a deep learning-based steganographic system for medical images that utilizes convolutional neural networks to identify optimal embedding regions [24]. Their approach depicted superior performance in terms of imperceptibility and embedding capacity compared to traditional methods, achieving PSNR values above 54 dB and embedding capacities up to 0.35 bits per pixel. However, the system required extensive training datasets and significant computational resources, which limited its practical deployment in resource-constrained healthcare environments.

Despite significant advances in medical steganography research, several critical limitations persist in existing approaches that limit their practical applicability in healthcare environments, including LSB-based approaches such as those in studies [25, 26]. A comprehensive analysis of the current literature, as reported in Table 1, reveals systematic gaps that require innovative solutions to enable the widespread adoption of steganographic techniques in medical contexts.

Table 1. Related works in medical data security and steganography

Aspect	References	Year	Findings
Medical Data Security	Peng et al. [27]	2024	Healthcare data security requires advanced encryption and steganographic protection methods.
Medical Image Integrity	Yan et al. [28]	2025	Medical image integrity is crucial for accurate diagnosis and preventing unauthorized alterations.
Medical Steganography Limitation	Hua et al. [29]	2023	Medical steganography faces cropping attacks and transmission distortion vulnerabilities.
Medical Data Preprocessing	Chahid et al. [30]	2023	Medical data preprocessing requires robust privacy protection mechanisms for sensitive patient information.
Proposed Method in MedRec-Secure	Employing dynamic steganographic approaches with adaptive embedding strategies to protect sensitive medical information while maintaining image fidelity for effective clinical decision making.		

3. PROPOSED METOD

The MedRec-Secure framework is designed for imperceptible embedding of MPR data into grayscale medical images. Unlike existing steganographic approaches that employ static embedding strategies, the proposed framework introduces a Dynamic Subtractor Selection Steganographic Framework (DSSSF) that adapts to local image characteristics while maintaining optimal trade-offs between embedding capacity, imperceptibility, and security.

The MedRec-Secure framework operates on the principle of intelligent pixel block processing, where medical images are divided into fixed-size blocks and statistical analysis determines the most suitable reference pixels (subtractors) for embedding operations, which does not adaptively work on the clinical importance (e.g., [20]) or extends the pixel difference within a block (e.g., [21]). This dynamic approach, combined with a multi-zone embedding strategy that categorizes pixels based on intensity ranges, enables the system to maximize data hiding capacity while minimizing visual artifacts and preserving diagnostic image quality essential for medical applications.

MedRec-Secure consists of three main phases: dynamic subtractor selection within pixel blocks, zone-based embedding with adaptive conditions, and secure key

generation for reliable extraction. The framework processes 8-bit grayscale medical images by converting them into 1D pixel arrays and organizing these arrays into blocks of 4 pixels each. For each block, statistical analysis, including calculations of mean and standard deviation, identifies the optimal subtractor pixel. The remaining pixels undergo zone-based evaluation for embedding eligibility, based on their intensity values and the difference relationships with the selected subtractor.

3.1 Embedding process

The embedding process, as illustrated in Figure 2, constitutes the core functionality of the MedRec-Secure framework, transforming cover medical images into stego images that contain hidden MPR data through a systematic sequence of operations. The process takes as input the cover medical image and secret MPR bits, producing a stego image and secret keys required for extraction.

1. *Convert and Divide Cover Image into Processing Blocks*: Start by converting the cover image from its original 2D matrix format to a 1D pixel array for efficient processing. Divide the pixel array into non-overlapping blocks of four pixels each.
2. *Determine Optimal Subtractor Pixel through Statistical Analysis*: Calculate the mean (μ) and standard deviation (σ) for each pixel block, where μ represents the average intensity and σ indicates the intensity variation of pixels $p(i)$ within the block. Apply a weighted selection criterion to identify the most suitable subtractor pixel through the selection score function (S) defined in Eq. (1), where the subtractor weight parameter (w) is empirically set to 0.05 for optimal performance.

$$S(p(i)) = |p(i) - \mu| + w|p(i) - \sigma| \tag{1}$$

Identify the pixel with the minimum selection score as the designated subtractor using Eq. (2) and Eq. (3). It is to establish the reference point for subsequent embedding operations.

$$S_{idx} = argmin(S(p(i))) \tag{2}$$

$$S_{val} = block[S_{idx}] \tag{3}$$

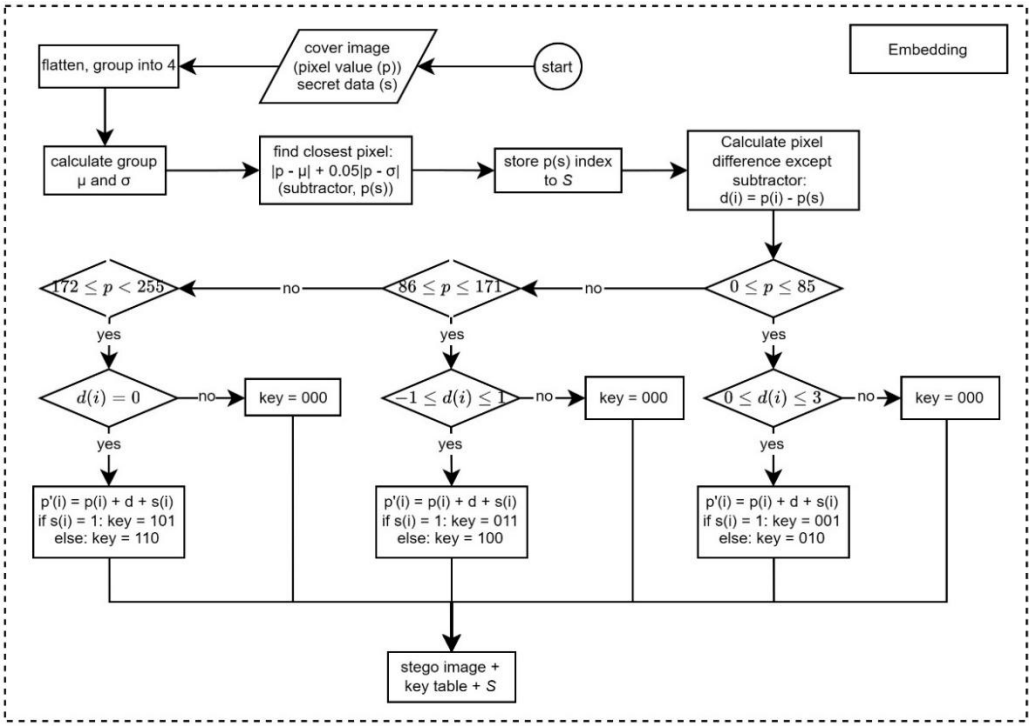

Figure 2. The embedding process

3. *Classify Pixels into Multi-Zone Categories and Embed Secret Data*: Perform zone classification for each non-subtractor pixel based on intensity values and calculated difference (d), establishing specific embedding conditions for three distinct regions using Eq. (4). The difference parameter (d) represents the deviation between pixel value and subtractor value. Apply zone-specific embedding rules where Zone A represents the dark region ($0 \le p(i) \le 85$), Zone B covers the mid-tone region ($86 \le p(i) \le 171$), and Zone C encompasses the bright region ($172 \le p(i) \le 255$). The secret data is embedded using the relation in Eq. (5), where $p'(i)$ denotes the resulting stego pixel and $b(i)$ represents the secret bit embedded. The corresponding secret keys are generated using the relations in Eqs. (6)-(8).

$$Zone = \begin{cases} A, if\ 0 \le p(i) \le 85, 0 \le d(i) \le 5 \\ B, if\ 86 \le p(i) \le 171, -2 \le d(i) \le 2 \\ C, if\ 172 \le p(i) \le 255, d(i) = 2 \end{cases} \tag{4}$$

$$p'(i) = p(i) + d(i) + b(i) \tag{5}$$

For Zone A:

$$\begin{cases} key = 001, b(i) = 1 \\ key = 010, b(i) = 0 \end{cases} \tag{6}$$

For Zone B:

$$\begin{cases} key = 011, b(i) = 1 \\ key = 100, b(i) = 0 \end{cases} \quad (7)$$

For Zone C:

$$\begin{cases} key = 101, b(i) = 1 \\ key = 110, b(i) = 0 \end{cases} \quad (8)$$

4. *Construct Final Steganographic Image*: Build the final steganographic image by replacing original pixel values with the modified values obtained from the embedding process. Reshape the processed 1D pixel array back to the original 2D image dimensions. It aims to ensure the stego image maintains the same structural properties as the cover image while successfully concealing the secret data within the specified embedding constraints.

3.2 Extraction process

Figure 3, contextualizing the extraction process, performs the inverse operations of embedding, systematically recovering both the original medical image and the hidden MPR data using the secret keys and subtractor indices obtained from the embedding stage. These are as follows.

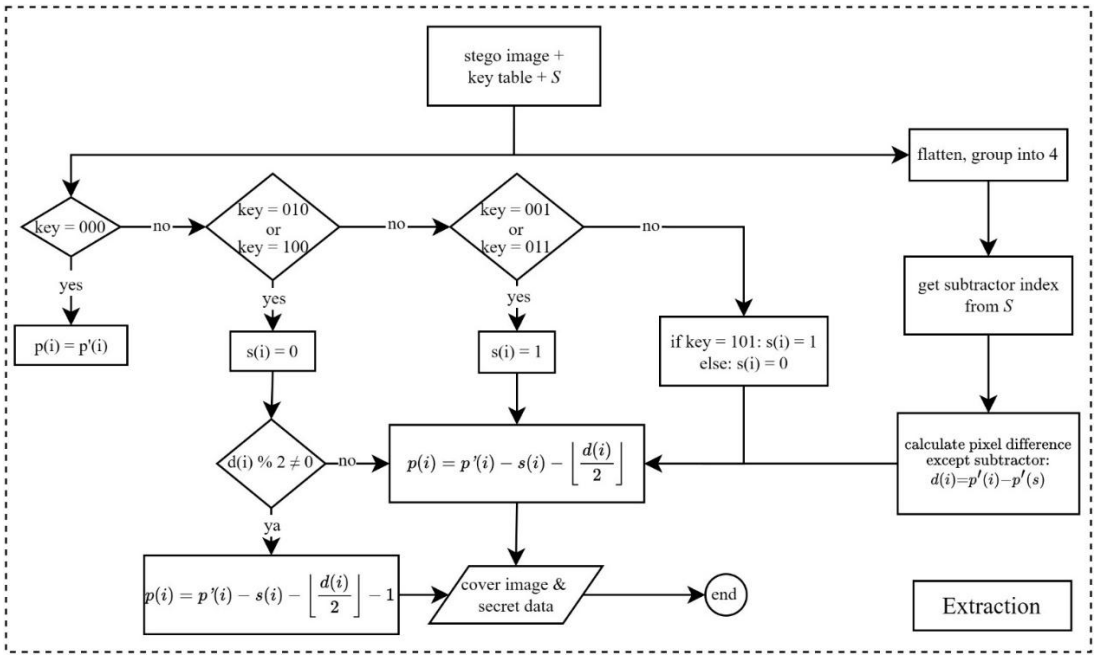

Figure 3. The extraction process

1. *Load Steganographic Image and Initialize Block Structure*: Load the steganographic image, along with the subtractor indices array and secret keys array, required for the extraction process. Convert the stego image from a 2D matrix format into a 1D pixel array, then divide it into separate blocks containing four pixels each. This block structure must match the one used during the data embedding process to ensure accurate data recovery.
2. *Identify Subtractor Pixels and Analyze Secret Keys*: Extract the subtractor pixel for each block using the stored subtractor indices ($I[j]$) from the embedding phase using Eq. (9). Based on the key, the location of the secret data is recognized. Analyze each pixel's corresponding secret key to determine the presence and characteristics of embedded data for subsequent extraction operations.
3. *Extract Embedded Bits and Recover Original Pixel Values*: Perform bit extraction when the secret key indicates the presence of embedded data ($k \neq$ '000'). To recover the cover image, Eq. (10) helps get the cover image that the embedding process has not modified. We apply Eq. (11) for the pixels with the secret data.

$$S_{val} = block[I[j]] \quad (9)$$

$$p(i) = p'(i) \quad (10)$$

$$p(i) = p'(i) - b(i) - \left\lfloor \frac{d(i)}{2} \right\rfloor \quad (11)$$

4. *Reconstruct Original Image and Concatenate Secret Data*: Validate and constrain all recovered pixel values to the valid intensity range [0, 255] to prevent invalid pixel values. Construct the original image by assembling the recovered pixel values generated from the extraction stage. Reshape the processed 1D pixel array back to the original 2D image dimensions, ensuring the recovered image maintains the same structural properties as the original cover image while successfully extracting the concealed secret data from the steganographic image.

3.3 Practical Implementation using MedRec-Secure

From this perspective, the relevance of the proposed dynamic subtractor selection approach is shown through practical implementation using a single pixel block, provided in Algorithm 1. The selection process employs statistical analysis to identify the optimal reference pixel that minimizes the weighted combination of mean deviation and standard deviation distance.

Algorithm 1. Dynamic Subtractor Selection Process

Notation:
- P = pixel_group → Group of pixels in 1 block
- μ → Mean value of pixel group
- σ → Standard deviation of pixel group
- w → Subtractor weight parameter (0.05)
- $d\_\mu(i)$ → Mean deviation distance for pixel i
- $d\_\sigma(i)$ → Standard deviation distance for pixel i
- $S(i)$ → Selection score for pixel i
- sub → Selected subtractor pixel value

Input: Group of pixels in 1 block
Output: Subtractor pixel value

1) Start
2) Calculate μ = MEAN(P)
3) Calculate σ = STD_DEV(P)
4) Initialize min_score = ∞
5) **for** each pixel in P **do**
6) Calculate $d\_\mu(i) = |P(i) - \mu|$
7) Calculate $d\_\sigma(i) = |P(i) - \sigma|$
8) Calculate $S(i) = d\_\mu(i) + w \times d\_\sigma(i)$
9) **if** $S(i)$ < min_score **then**
10) min_score = $S(i)$
11) sub = $P(i)$
12) Return sub
13) End

The algorithm begins with a pixel block containing values [75, 78, 73, 80]. First, the average (mean) value of the block is calculated, resulting in:

$$\mu = 76.5$$

Next, the standard deviation is computed as:

$$\sigma = 2.89$$

For each pixel in the block, the algorithm evaluates a weighted selection score. Pixel 0, with value 75, has a mean distance of 1.5 and a standard deviation distance of 72.11, producing a selection score of:

$$Score_0 = 1.5 + 0.05 \times 72.11 = 5.11$$

Pixel 1 with value 78 shows a mean distance of 1.5 and a standard deviation distance of 75.11, resulting in a score of:

$$Score_1 = 1.5 + 0.05 \times 75.11 = 5.26$$

Pixel 2 with value 73 exhibits a larger mean distance of 3.5 and standard deviation distance of 70.11, generating a higher score of:

$$Score_2 = 3.5 + 0.05 \times 70.11 = 7.01$$

Similarly, pixel 3 with value 80 has a mean distance of 3.5 and a standard deviation distance of 77.11, producing the highest score of:

$$Score_3 = 3.5 + 0.05 \times 77.11 = 7.36$$

The algorithm identifies the pixel with the minimum score as the optimal subtractor. In this case, pixel 0 with value 75 achieves the lowest score of 5.11, making it the selected subtractor for the block. This selection demonstrates the effectiveness of the weighted criterion in balancing statistical measures to determine the most representative pixel within the processing block.

4. RESULTS AND DISCUSSIONS

4.1 Experimental environment

The MedRec-Secure framework was implemented and evaluated on system equipped with an Intel Core i9 processor operating at 3.2 GHz and 32 GB of RAM. The development environment utilized MATLAB R2023b for algorithmic implementation and Python 3.9 with the OpenCV library for image processing operations. Visual Studio Code served as the primary integrated development environment, chosen for its robust debugging capabilities and efficient code management features, which are essential for developing steganographic algorithms.

The experimental evaluation employed two comprehensive datasets to ensure thorough validation of the DSSSF. The primary dataset consisted of medical images obtained from the DICOM Library, similar to the study by Elhadad et al. [12], comprising high-resolution grayscale medical images with dimensions of 512 × 512 pixels. These images included various medical imaging modalities such as X-rays, CT scans, and MRI images, as illustrated in Figure 4. It has diverse textural characteristics essential for comprehensive steganographic evaluation. The secondary validation dataset incorporated images from the CT Medical Images database (https://www.kaggle.com/datasets/kmader/siim-medical-images), offering additional medical image samples with varying complexity levels and anatomical structures. To maintain consistency in image labeling, all images are uniformly labeled from Cover 1 to Cover 10, as presented in Table 2.

The MPRs' data utilized for embedding experiments was structured according to international healthcare standards, incorporating patient demographics, medical history, diagnostic information, treatment records, and clinical observations. The MPR dataset comprised six interconnected entities following relational database principles: Patient records containing personal identifiers, demographic information, and contact details; Medical History encompassing previous diagnoses, surgical procedures, and chronic conditions; Current Diagnosis including present medical conditions, severity assessments, and diagnostic confidence levels; Treatment Plans detailing prescribed medications, therapeutic interventions, and follow-up schedules; Laboratory Results containing test outcomes, reference ranges, and clinical interpretations; and Clinical Notes documenting physician observations, patient complaints, and treatment responses.

The synthetic MPR dataset was generated using medical data simulation tools based on realistic clinical scenarios. The dataset encompasses 500 patient records with varying complexity levels, ranging from basic demographic information to comprehensive medical histories with multiple diagnostic episodes. Individual MPR sizes varied from 1 kb for basic records to 100 kb for complex multi-speciality cases.

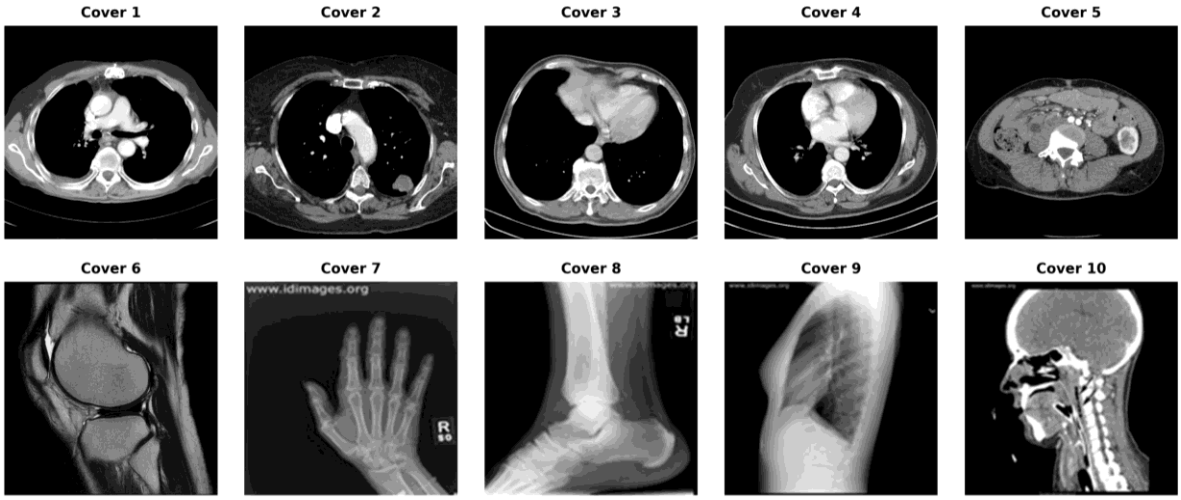

Figure 4. Sample cover images dataset taken from DICOM Library
Note: available at https://www.dicomlibrary.com/.

Table 2. Datasets filename

Image Name	File Name
Cover 1	ID_0001_AGE_0069_CONTRAST_1_CT
Cover 2	ID_0002_AGE_0074_CONTRAST_1_CT
Cover 3	ID_0003_AGE_0075_CONTRAST_1_CT
Cover 4	ID_0004_AGE_0056_CONTRAST_1_CT
Cover 5	ID_0005_AGE_0005_CONTRAST_1_CT
Cover 6	ID_0006_AGE_0010_CONTRAST_1_CT
Cover 7	Hand
Cover 8	Leg
Cover 9	Chest
Cover 10	Head

4.2 Experimental results

The PSNR evaluation results, as illustrated in Figure 5, shown the framework's superior ability to preserve image quality across varying MPR payload sizes and different medical image datasets. For MPR data ranging from 1 kb to 100 kb, the MedRec framework achieved remarkable PSNR values with significant variations depending on image characteristics and payload complexity.

The experimental results reveal that smaller payload sizes consistently achieve higher PSNR values across all tested images. At a 1 kb payload, all images achieved the maximum PSNR of 75.43 dB, demonstrating relatively acceptable imperceptibility for minimal data embedding. As payload sizes increase, the framework maintains performance, with Image 3 showing the highest average PSNR of 59.70 dB, followed closely by Image 5 with 59.57 dB and Image 4 with 59.36 dB. These results indicate that the dynamic subtractor selection mechanism effectively adapts to different structures and imaging characteristics.

Notably, Image 6 presents unique challenges with an average PSNR of 53.48 dB, showing more significant degradation at higher payload sizes (49.51 dB at 100 kb). This variation suggests that specific medical image characteristics, such as uniform intensity regions or specific structures, may require specialized embedding strategies within the DSSSF framework. Despite this variation, all images maintained PSNR scores higher than the predefined threshold for medical imaging applications.

The comparative analysis with state-of-the-art methods, as presented in Figure 6, demonstrates the superior performance of the proposed MedRec-Secure framework across different regions. When compared against the methods proposed by Hameed et al. [25], and Hussain and Khodher [26], the MedRec-Secure framework shows advantages in chest and hand medical images. For chest images, the proposed method achieved 69.292 dB compared to 65.295 dB [25] and 67.280 dB [26] representing improvements of 6.1% and 3.0% respectively. Similarly, for hand images, the framework achieved 69.997 dB, compared to 67.995 dB [25] and 67.700 dB [26], demonstrating consistent superiority.

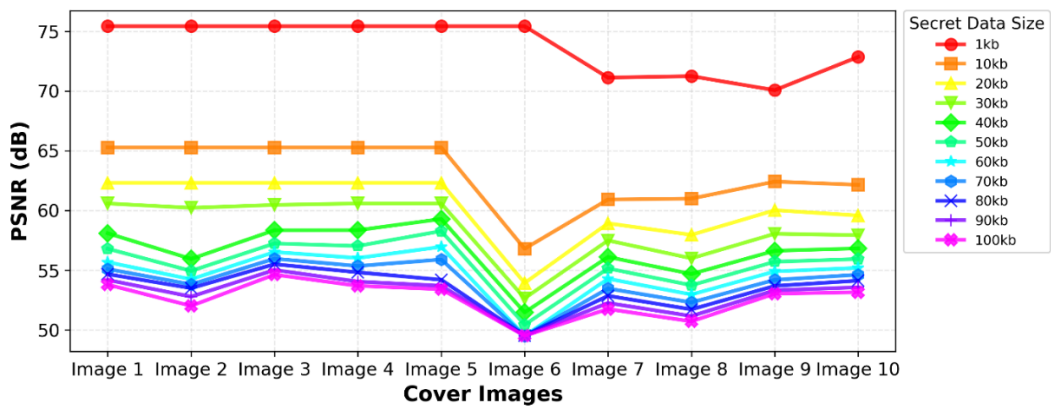

Figure 5. Peak Signal-to-Noise Ratio (PSNR) values from experiment across various datasets and secret data sizes

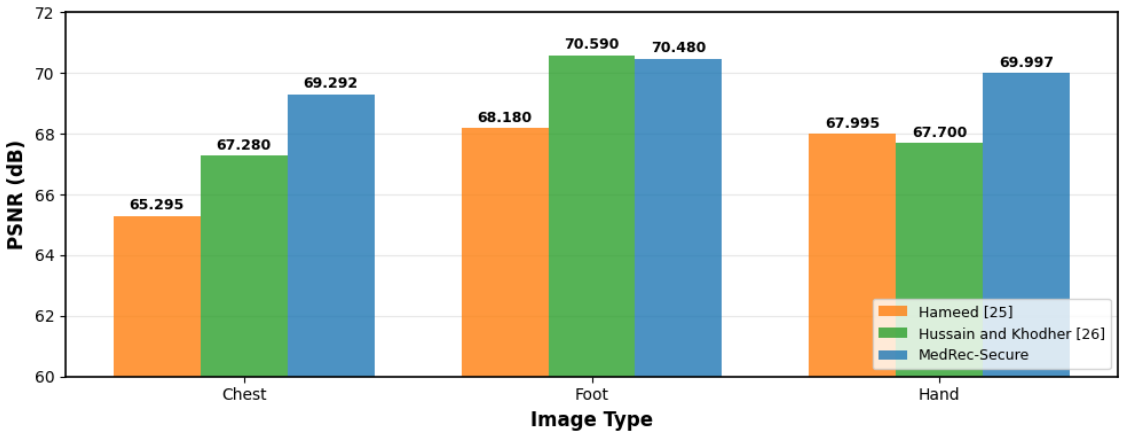

Figure 6. Peak Signal-to-Noise Ratio (PSNR) evaluation of the proposed approach against benchmark techniques

However, the framework shows slightly lower performance for foot images (70.480 dB) compared to [26] (70.590 dB), although it still outperforms [25] (68.180 dB). This difference of 0.16% suggests that certain structures with specific intensity patterns may benefit from alternative embedding strategies, indicating areas for future optimization within the DSSSF framework. Comprehensive statistical analysis confirmed the reliability and consistency of the MedRec-Secure framework across multiple evaluation sessions. Repeated experiments on identical image-payload combinations yielded coefficients of variation of 2.1% or less for PSNR measurements and 1.8% or less for Structural Similarity Index Measure (SSIM) evaluations. This statistical consistency validates the framework's suitability for operational healthcare environments.

The Mean Squared Error (MSE) evaluation results, detailed in Table 3, provide quantitative validation of the framework's minimal distortion characteristics. The MSE values have inverse correlation with PSNR results, confirming the reliability of the imperceptibility measurements. Image 3 achieved the lowest average MSE of 0.114, corresponding to its highest PSNR performance, while Image 6 showed the highest average MSE of 0.495, consistent with its more challenging embedding characteristics.

The MSE progression across payload sizes reveals predictable patterns, with values ranging from 0.002 at 1 kb (across most images) to maximum values of 0.728 at 100 kb for the most challenging image (Image 6). The majority of images maintained MSE values below 0.3 even at maximum payload capacity, indicating excellent preservation of image quality suitable for medical diagnostic purposes.

The SSIM evaluation results, presented in Table 4, confirm the framework's exceptional structural preservation capabilities. SSIM values are consistently above 0.9883 across all tested scenarios, with average values ranging from 0.9940 to 0.9982 across different images. Image 7 indicated the highest structural preservation, with an average SSIM of 0.9982, while Images 1-5 showed consistent performance, ranging from 0.9940 to 0.9941.

Table 3. Obtained Mean Squared Error (MSE) values

Cover Image	1 kb	10 kb	20 kb	30 kb	40 kb	50 kb	60 kb	70 kb	80 kb	90 kb	100 kb	Average MSE
Image 1	0.002	0.019	0.038	0.057	0.101	0.136	0.176	0.201	0.222	0.248	0.272	0.134
Image 2	0.002	0.019	0.038	0.062	0.165	0.208	0.245	0.271	0.291	0.342	0.409	0.187
Image 3	0.002	0.019	0.038	0.058	0.095	0.123	0.145	0.165	0.183	0.205	0.224	0.114
Image 4	0.002	0.019	0.038	0.057	0.095	0.129	0.163	0.190	0.214	0.256	0.278	0.131
Image 5	0.002	0.019	0.038	0.057	0.077	0.097	0.131	0.167	0.247	0.278	0.297	0.128
Image 6	0.002	0.136	0.263	0.353	0.464	0.589	0.730	0.729	0.725	0.729	0.728	0.495
Image 7	0.005	0.053	0.083	0.116	0.159	0.199	0.242	0.293	0.337	0.387	0.435	0.210
Image 8	0.005	0.052	0.104	0.164	0.221	0.275	0.329	0.383	0.438	0.498	0.552	0.275
Image 9	0.006	0.037	0.065	0.102	0.141	0.175	0.211	0.248	0.278	0.303	0.324	0.172
Image 10	0.003	0.040	0.072	0.105	0.135	0.166	0.197	0.224	0.252	0.286	0.314	0.163

Table 4. Obtained Structural Similarity Index Measure (SSIM) values

Cover Image	1 kb	10 kb	20 kb	30 kb	40 kb	50 kb	60 kb	70 kb	80 kb	90 kb	100 kb	Average SSIM
Image 1	1.000	0.9989	0.9975	0.9963	0.9950	0.9940	0.9927	0.9916	0.9906	0.9894	0.9885	0.9940
Image 2	1.000	0.9989	0.9975	0.9963	0.9952	0.9941	0.9928	0.9918	0.9907	0.9895	0.9886	0.9941
Image 3	1.0000	0.9989	0.9975	0.9963	0.9952	0.9942	0.9930	0.9919	0.9908	0.9894	0.9883	0.9941
Image 4	1.0000	0.9989	0.9975	0.9963	0.9950	0.9940	0.9928	0.9918	0.9907	0.9897	0.9887	0.9941
Image 5	1.0000	0.9989	0.9975	0.9963	0.9949	0.9936	0.9924	0.9916	0.9910	0.9896	0.9884	0.9940
Image 6	1.0000	0.9987	0.9973	0.9962	0.9949	0.9934	0.9921	0.9921	0.9922	0.9921	0.9921	0.9947
Image 7	1.0000	0.9996	0.9993	0.9990	0.9986	0.9982	0.9979	0.9974	0.9970	0.9966	0.9962	0.9982
Image 8	1.0000	0.9995	0.9990	0.9984	0.9978	0.9972	0.9966	0.9961	0.9955	0.9948	0.9942	0.9972
Image 9	1.0000	0.9989	0.9977	0.9966	0.9954	0.9943	0.9932	0.9921	0.9911	0.9900	0.9890	0.9944
Image 10	1.0000	0.9990	0.9979	0.9970	0.9960	0.9948	0.9935	0.9923	0.9912	0.9897	0.9884	0.9945

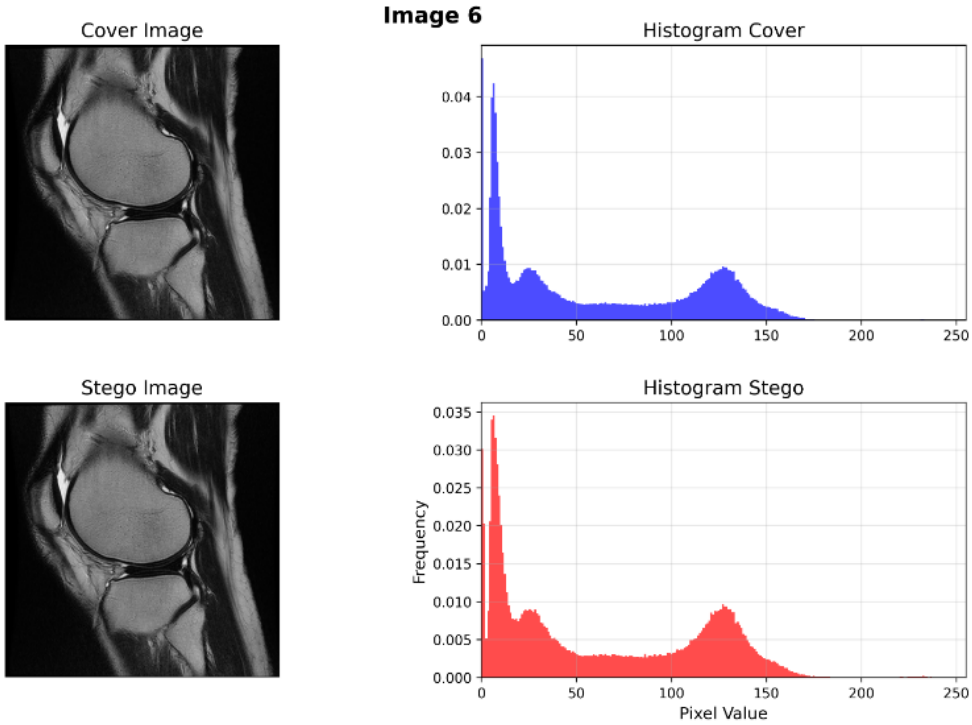

Figure 7. Cover and stego histogram comparison

The SSIM results indicate that the Dynamic Subtractor Selection mechanism effectively preserves critical structural information essential for medical diagnosis. Even at maximum payload capacity (100 kb), SSIM values are above 0.9883, which embedded MPR may not affect the diagnostic utility of medical images. This structural preservation is particularly crucial for medical applications where information details must be maintained.

The comprehensive histogram analysis comparing cover and stego images, as illustrated in Figure 7, specifically demonstrates Image 6 with a 100 kb payload embedding scenario. Despite being the most challenging case in terms of PSNR and MSE metrics, the histogram comparison reveals minimal distributional changes between the original and steganographic images. The pixel intensity distributions exhibit a similarity across all intensity ranges, with negligible variations in the frequency distribution patterns, despite the substantial data embedding capacity. This preservation of histogram characteristics ensures that the embedded MPR data is imperceptible to both visual and statistical analysis.

In its implementation to a real environment, the proposed method may be combined with cryptography. The payload is firstly encrypted using existing algorithms to increase its security, anticipating attackers obtain the hidden message. In this case, the security level improves, along with its complexity. However, the complexity expects to increase. Therefore, it needs to consider what the purpose and environment of the system, whether the processing time, payload reconstruction, robustness or other factors should be focused on. Overall, the complexity of the algorithm is essential to further analysis. It is also wort noting that, as spatial domain-based data hiding, this method is not robust again stego image manipulation, which can destroy the information in it.

The experimental findings indicate that the MedRec-Secure framework, with its DSSSF, signifies considerable enhancement in medical data steganography, providing trade-offs between embedding capacity and imperceptibility, which are essential for practical healthcare applications. Furthermore, it is still possible to increase the data security by integrating the federated learning framework [31] or blockchain mechanism [32] into the system.

5. CONCLUSIONS

This study proposes a data hiding framework, MedRec-Secure, which aims to hide MPRs within medical images by still considering imperceptibility and payload capacity. Implementing the DSSSF with a multi-zone embedding strategy, the framework generates protection for medical data while maintaining image quality. MedRec-Secure represents an advancement by addressing critical limitations in previous methods, particularly in adaptive embedding, imperceptibility, and payload capacity. The experimental results demonstrate its superior performance, achieving PSNR values ranging from 49.51 dB to 75.43 dB and SSIM values above 0.9883. The framework also exhibits notable improvements over state-of-the-art methods in chest and hand image scenarios, underscoring its adaptability across various anatomical structures and medical image types.

Future work will focus on expanding the DSSSF framework to support color medical images and three-dimensional datasets, which are increasingly prevalent in modern healthcare. Enhancements will also explore the integration of machine learning techniques for more intelligent subtractor selection and real-time optimization.

ACKNOWLEDGMENT

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).

The authors also 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.

REFERENCES

[1] D'Layla, A.W.C., De La Croix, N.J., Ahmad, T., Han, F. (2025). EHR-protect: A steganographic framework based on data-transformation to protect Electronic Health Records. Intelligent Systems with Applications, 26: 200493. https://doi.org/10.1016/j.iswa.2025.200493

[2] Chai, X.L., Cao, G.Y., Fu, Z.F., Gan, Z.H., Wang, B.J., Zhang, Y.S. (2024). High-capacity reversible data hiding in encrypted medical images using adaptive pixel-modulation and HBP-RMC. Biomedical Signal Processing and Control, 95(Part B): 106424. https://doi.org/10.1016/j.bspc.2024.106424

[3] De La Croix, N.J., Ahmad, T., Han, F. (2024). Comprehensive survey on image steganalysis using deep learning. Array, 22: 100353. https://doi.org/10.1016/j.array.2024.100353

[4] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., et al. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20: 146. https://doi.org/10.1186/s12911-020-01161-7

[5] Newaz, A. I., Sikder, A.K., Rahman, M.A., Uluagac, A.S. (2020). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. arXiv preprint arXiv:2005.07359. https://doi.org/10.48550/arXiv.2005.07359

[6] Alharbi, F., Sabra, M.N.A., Alharbe, N., Almajed, A.A. (2022). Towards a strategic IT GRC framework for healthcare organizations. International Journal of Advanced Computer Science and Applications, 13(1). https://doi.org/10.14569/IJACSA.2022.0130125

[7] Omotunde, H., Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of Cybersecurity, 2023: 115-133. https://doi.org/10.58496/mjcsc/2023/016

[8] Idakwo, M.A., Muazu, M.B., Adedokun, E.A., Sadiq, B.O. (2020). An extensive survey of digital image steganography: State of the art. ATBU Journal of Science, Technology and Education, 8(2): 40-54.

[9] Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A.A., Ahmed, A. (2023). A comprehensive study of digital image steganographic techniques. IEEE Access, 11: 6770-6791. https://doi.org/10.1109/access.2023.3237393

[10] Alzubaidy, H.K., Al-Shammary, D., Abed, M.H. (2022). A survey on patients privacy protection with stganography and visual encryption. arXiv preprint arXiv:2201.09388. https://doi.org/10.48550/arXiv.2201.09388

[11] Thangaraj, P., Salomi, M., Devipriya, A. (2020). Steganography Based Authenticated Data Sharing in Health Care. IJAICT India Publications, India, pp. 435-437. https://doi.org/10.46532/978-81-950008-1-4

[12] Elhadad, A., Ghareeb, A., Abbas, S. (2021). A blind and high-capacity data hiding of DICOM medical images based on fuzzification concepts. Alexandria Engineering Journal, 60(2): 2471-2482. https://doi.org/10.1016/j.aej.2020.12.050

[13] Siddiqui, G.F., Iqbal, M.Z., Saleem, K., Saeed, Z., Ahmed, A., Hameed, I.A., Khan, M.F. (2020). A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. IEEE Access, 8: 181893-181903. https://doi.org/10.1109/ACCESS.2020.3028315

[14] Haq, I.U., Ali, A., Qaisar, B.S., Adnan, H.M., Hussain, M., Nauman, M. (2023). Steganography techniques for medical images: A recommender paper. International Journal of Innovative Science and Research Technology, 8(9): 79-87. https://doi.org/10.5281/zenodo.8340603

[15] Alhomoud, A.M. (2021). Image steganography in spatial domain: Current status, techniques, and trends. Intelligent Automation & Soft Computing, 27(1): 69-88. https://doi.org/10.32604/iasc.2021.014773

[16] Sirisha, B.L., Mohan, B.C. (2021). Review on spatial domain image steganography techniques. Journal of Discrete Mathematical Sciences and Cryptography, 24(6): 1873-1883. https://doi.org/10.1080/09720529.2021.1962025

[17] Ogundokun, R.O., Abikoye, O.C. (2021). A safe and secured medical textual information using an improved LSB image steganography. International Journal of Digital Multimedia Broadcasting, 2021(1): 8827055. https://doi.org/10.1155/2021/8827055

[18] Karawia, A.A. (2021). Medical image steganographic algorithm via modified LSB method and chaotic map. IET Image Processing, 15(11): 2580-2590. https://doi.org/10.1049/ipr2.12246

[19] Jiang, W.J., Hu, D.H., Yu, C., Li, M., Zhao, Z.Q. (2020). A new steganography without embedding based on adversarial training. In Proceedings of the ACM Turing Celebration Conference - China (ACM TURC '20). Association for Computing Machinery, New York, NY, USA, pp. 219-223. https://doi.org/10.1145/3393527.3393564

[20] Huang, L.C., Chiou, S.F., Hwang, M.S. (2020). A reversible data hiding based on histogram shifting of prediction errors for two-tier medical images. Informatica, 32(1): 69-84. https://doi.org/10.15388/20-infor422

[21] Wang, J.J., Tan, S.F. (2021). Separable reversible data hiding in encryption image with two-tuples coding. Computers, 10(7): 86. https://doi.org/10.3390/computers10070086

[22] Mohammed, A.A., Jebur, B.A., Younus, K.M. (2021). Hybrid DCT-SVD based digital watermarking scheme with chaotic encryption for medical images. IOP Conference Series: Materials Science and Engineering, 1152(1): 012025. https://doi.org/10.1088/1757-899x/1152/1/012025

[23] Soundrapandiyan, R., Rajendiran, K., Gurunathan, A., Victor, A., Selvanambi, R. (2023). Analysis of DWT–DCT watermarking algorithm on digital medical imaging. Journal of Medical Imaging, 11(1): 014002. https://doi.org/10.1117/1.jmi.11.1.014002

[24] Chen, B.L., Luo, W.Q., Zheng, P.J., Huang, J.W. (2020). Universal stego post-processing for enhancing image steganography. Journal of Information Security and Applications, 55: 102664.

https://doi.org/10.1016/j.jisa.2020.102664
[25] Hameed, M.A., Abdel-Aleem, O.A., Hassaballah, M. (2023). A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. Journal of Ambient Intelligence and Humanized Computing, 14: 4639-4657. https://doi.org/10.1007/s12652-022-04366-y
[26] Hussain, A.Z., Khodher, M.A.A. (2024). Securing medical images using chaotic map encryption and LSB steganography. Revue d'Intelligence Artificielle, 38(1): 313-321. https://doi.org/10.18280/ria.380133
[27] Peng, Y.X., Fu, C., Zheng, Y., Tian, Y.J., Cao, G.X., Chen, J.X. (2024). Medical steganography: Enhanced security and image quality, and new S-Q assessment. Signal Processing, 223: 109546. https://doi.org/10.1016/j.sigpro.2024.109546
[28] Yan, F., Wang, Z.Q., Hirota, K. (2025). Dual medical image watermarking using SRU-enhanced network and EICC chaotic map. Complex & Intelligent Systems, 11: 101. https://doi.org/10.1007/s40747-024-01723-6
[29] Hua, C.J., Wu, Y., Shi, Y.Q., Hu, M.H., Xie, R., Zhai, G.T., Zhang, X.P. (2023). Steganography for medical record image. Computers in Biology and Medicine, 165: 107344. https://doi.org/10.1016/j.compbiomed.2023.107344
[30] Chahid, I., Elmiad, A.K., Badaoui, M. (2023). Data preprocessing for machine learning applications in healthcare: A review. In 2023 14th International Conference on Intelligent Systems: Theories and Applications (SITA), Casablanca, Morocco, pp. 1-6. https://doi.org/10.1109/SITA60746.2023.10373591
[31] Lim, S.J., Prabaharan, G., Mani, K. (2025). Privacy preservation of medical images through synthesized federated learning framework in healthcare. Traitement du Signal, 42(4): 2119-2130. https://doi.org/10.18280/ts.420424
[32] Mohammed, Z.Q., Aboody, C.H., Zaidan, O.H. (2025). Integrated framework for real-time cyber threat detection and mitigation in IoT and healthcare systems using deep learning and blockchain. International Journal of Safety and Security Engineering, 15(8): 1611-1625. https://doi.org/10.18280/ijsse.150807