Journal of Computer Science

Research Article

A Comparative Computational Efficiency Analysis of LSB and Hybrid Steganographic Methods

Divya Sharma and Chander Prabha

Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Article history
Received: 23-12-2024
Revised: 24-05-2025
Accepted: 11-06-2025

Corresponding Author:
Chander Prabha
Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
Email: prabhanice@gmail.com

Abstract: Electronic Medical Images (EMI) are of various types such as X-rays, CT scans, MRIs, etc. EMIs are generally large, but they vary in dimensions and sizes based on the body part to which they belong. Not much research has been done to secure EMIs due to their varied and large sizes, while ensuring their accessibility for real-time transmission. Where access and storage from third-party storage is performed. Enhancing the security and privacy of EMI while being transmitted or when saved on third-party storage is still a cause of concern. In this research paper, a comparative study is conducted on the Least Significant Bit (LSB) and the Hybrid Method (HM) based on their reduced computational time. In HM, Edge-Based Steganography (EBS) is applied, followed by five layers of cryptography, and separately, LSB steganography is performed to secure the same dataset of 5856 greyscale secret Chest X-ray images, each varying in dimensions and sizes. This paper also discusses EMI and its relevant topics. The HM took an encryption time (ET) of 0.0117 seconds, while the LSB took 5.916 minutes. The decryption time (DT) taken by HM is 0.0142 seconds; on the contrary, the LSB was 13.46 minutes. Concluding based on reduced computational time, making the data security method appropriate for real-time applications (RTA). Thus, ensuring better accessibility to data stored by HM than the LSB method when hiding greyscale Chest X-ray images in the colored cover image. HM performance tests values for Mean square error (MSE) are 0.0000000056, Peak Signal to Noise Ratio (PSNR) is 82.51967, Correlation (R) is 1, Structural Similarity Index Metrics (SSIM) is 1, Signal to Noise Ratio (SNR) is 0.049221, Entropy (E) is 7.8398, and the Number of Pixel Changing Rate (NPCR) is 95.59, which are close to the preferred and good values for Root Mean Square Error (RMSE), Bit Error Rate (BER), etc. Thus, based on computational time and performance tests, these HM values are far superior to the LSB. Therefore, the HM is more practical and can be implemented for real-time applications in the future.

Keywords: Least Significant Bit (LSB), Edge-based Steganography, Steganography, Cryptography, Hybrid Method (HM), Computational Complexity

Introduction

The advancements in technology, combined with the Internet, provide real-time access as part of a smart city lifestyle. This smart city lifestyle extends to various sectors of society, such as E-health care, farming, electricity, etc. (Ali *et al.*, 2021). The areas of applications are shown in Figure 1.

Smart health is part of the smart city lifestyle, which means real-time access to patient records and reports (Akkasaligar & Biradar, 2020; Ali *et al.*, 2022). Here, a patient's healthcare records are accessed in real-time while ensuring security. Electronic health care records (EHR) are composed of details such as the patient's name, age, gender, address, and patient's payment details, such as credit card, debit card details, etc. and Electronic Medical Images (EMI) (Sharma & Prabha, 2023). Generally, EMI comprises of X-rays, Ultrasounds, CT scans, MRIs, Endoscopies, ECGs, and PET scans.

These are commonly used by academic medical researchers, pharma companies, hospitals, insurance agencies, and government agencies, apart from the patient. EMIs are sensitive and need to be accurate for a correct diagnosis (Chowdhuri *et al.*, 2023). Ensuring

access to accurate and proper EMI promptly in case of medical emergencies would save patients' lives. EMI should be accessible in real-time while being clear, readable and understandable. Thus, it should not be modified or damaged by hackers or attackers while being stored or transmitted through a communication medium (Sharma & Prabha, 2024).

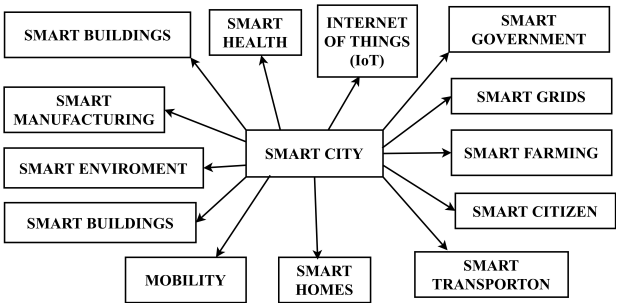

Fig. 1: Smart City Utilities and Areas of Application.

Data Hiding Techniques

The various types of data hiding techniques are, Steganography, the art of hiding a secret message in plain sight, and Cryptography, which converts a plain image into a non-understandable form; and Watermarking, making visible changes to the cover image. In Fig. 2(a), the process of cryptography is depicted, while Fig. 2(b) shows the working of steganography. In Table 1, the differences between cryptography and steganography is detailed based on various properties.

Table 1: Differences between cryptography and steganography

	Cryptography	Steganography
Input	Plain Text & Key	Cover image & secret image
Output	Cipher image	Stego-image
Definition	Converting into a non-understandable form	Hiding in plain sight
Attacks	Crypto-analysis	Stegano-analysis
Imperceptibility	The output is non-understandable	The output is understandable
Mathematical	It uses a mathematical transformation	It does not use a mathematical transformation
Visibility	Changes made are visible to all	Changes made are not visible to all
Techniques	AES, DES,	LSB, Spread spectrum
Popularity	More popular	Less popular
Property	Confidentiality, integrity, authentication, and non-repudiation	Capacity, imperceptibility, robustness, and security

Research Contribution

This paper makes several key contributions to the field of medical image steganography. It provides a comprehensive discussion of data hiding techniques, focusing on EMI and its associated advantages. The research includes a tabular analysis of previous literature that informed the current study's methodology. Additionally, the work implements the widely used LSB steganography technique and compares its performance against the HM method (Sharma & Prabha, 2024) using a dataset of 5856 X-ray images (Pixlr, 2021) embedded into identical cover images, evaluating both computational efficiency and performance metrics.

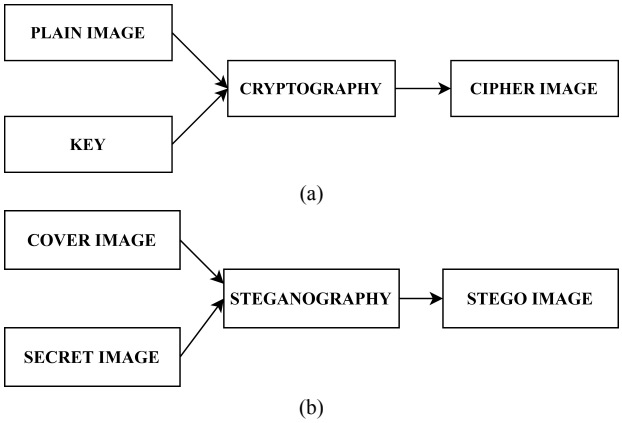

Fig. 2: Process of (a) Cryptography and (b) Steganography

Literature Review

The previous literature studied during this research work is presented in Table 2. The study is done based on the research goal that led previous researchers, the results they achieved, the techniques they proposed, the programming language on which they implemented their proposed methods, the data set details that were used, and the future scope, if mentioned.

Table 2 helps deduce that LSB steganography is still currently popularly implemented. This may be because LSB is simple to implement and understand, which is also a major drawback of LSB.

Table 2 concludes that previous researchers have aimed to secure EMI. Previous researchers have pointed out the need to increase the embedding capacity of the cover and to hide 3-D medical images as a secret image. A 3-D medical image in JPEG will have 3 basic components: Red, Green, and Blue (RGB). Therefore, the amount of data to be hidden will increase significantly. LSB has limited capacity for hiding the data, as only the least significant bit is used in the cover to hide the secret image.

Due to the popularity of the LSB technique, it was implemented for hiding 5856 X-ray images in the same cover image as the HM one at a time. Both methods, computational time and performance test values, are compared in this research work. Table 2 concludes that MATLAB is the most commonly used PL, and the same has been used in this research. The database's previous research used varied methods. Commonly, the data set on which the proposed technique was applied was small in size, but (Abdul, 2022) used 1,12,120 cover images for

hiding a 16 × 16 matrix in them. Hence, the size of the data set of the secret image was smaller. Here a data of 5856 greyscale Chest X-ray secret images is hidden in the cover image.

Table 2: Literature Study Based on Proposed Technique

Referred As	Research Goal / Achieved / PL / Database / Data Set Details	Proposed Methods / Future Scope
Mahalakshmi *et al*., 2023	For the safety of medical images from data leaks when transferred on an unsafe network/ Easy execution/ -/-/ MRI and CT scan images (914 ×1100) with the cover image Lena (512 ×512	LSB embeds using Particle Swarm Optimiser (PSO)/ A new LSB technique should be developed, which enhances embedding capacity, PSNR, and MSE values
Desai *et al*., 2022	Patient data security over network communication,/ Image quality is retained/ -/-/ Chest X Ray image with a cover image of natural scenery.	Deep neural network-based steganography where LSB, with Discrete Coefficient Transfer (DCT), Discrete Wavelet Transfer (DWT) and Binary Pattern Complexity/ One shall experiment to hide multiple medical images in one natural scene image as a future scope. The model can be tested for scalability by training it on a larger dataset and using a high-performance computing GPU system.
Aleisa, 2022	Reliable and confidential internet-based exchange of EMR, EMI, and diagnosis of patients geographically distant. / Better PSNR, MSE, R, secure, imperceptible, enhanced confidentiality/ -/-/ Secret text with up to 8 and 192 digits with cover image 512 × 512 bitmap grayscale images reduced to 256 × 256.	LSB of integer wavelet transform/ -
Mohsin *et al*., 2021	Secure and efficient transmission and sharing of medical information amongst hospitals while maintaining confidentiality and integrity, while addressing the need for data availability in a decentralised environment/ Confidentiality, high embedding capacity, high image quality, secure, and data availability/ -/-/ Medical data with a greyscale cover image	Particle swarm optimisation (PSO) algorithm, then hashing secret Covid-19 data, followed by LSB / could be implemented in the voting system.
Al-Shaarani & Gutub, 2021	Privacy and confidentiality of data with the growth of online transfer of information / Simple, intuitive, secure, robust, no quality deterioration/ MATLAB/Kaggle (2021) and USC-SIPI/ 1-bit and 2-bit, 50 images with 4 images of Baboon, Deer, Flower, Fruit (32 Bits,64 Bits	Secret collective agreement, counting-based and matrix-based secret sharing with LSB and DWT XOR encryption / Applied to audio, video, offering high capacity
Abdul, 2022	Secure & private communication over an insecure medium for IoMT/ Robustness against filter, JPEG compression, addition of noise attacks, 100% payload retrieval extraction after low pass filter attack, robust against AWGN attacks, Imperceptible, achieved secrecy, extraction possible in case of severe degradation/-/ NIH-Clinical Centre chest X-ray data set/ 16 × 16 pseudo-random matrix, 16 ×16 bit with 1,12120 cover X-Ray images; 30,805 patients having 14 disease labels (1024 × 1024 PNG).	Zero steganography, LSB/DCT transform / could be applied to 3D medical images.
Singhal *et al*., 2020	Secure classified information steganography maintains visual quality/ Enhanced level of security, quality retained, secure, undetectable, robust, secure from hackers, more security layers, imperceptible/ -/-/Data (196608 bits (= 24576 bytes), 2 bit with butterfly (176 KB, 386 ×395), Mario(22.1KB, 219 ×150), penguin(47.1KB, 386 ×395) cover images (256 × 256	AES-256, SHA-256 with LSB steganography/ Higher security and confidentiality are needed
Lishomwa & Zimba, 2023	Confidentiality of healthcare records with secure transmission using steganography and cryptography/ Faster, minimal image distortion, more secure/ -/-/Text " this is the test string" with Bitmap (BMP) images in PNG and WAV files.	Privacy-preserving hybrid AES-128 with Diffie-Hellman encryption, then LSB steganography/ -
Awadh *et al*., 2022	Security of the image and capacity concerns when being transmitted by the Internet, thus cryptography and steganography/with good image quality of 68%, solve security and capacity concerns, and the output images are distortion-free/ Visual Basic .NET language/ Lena image (65536 Bits) with landscape Image & 40 different-sized cover images (393216 Bytes)	Security by hybrid layers, where the image is compressed using Discrete Wavelet Transform (DWT), followed by AES-128 encryption, and then LSB steganography, / A more secure hybrid method, followed by a random hiding algorithm, could be implemented on other languages.
Olvera-Martinez *et al*., 2022	Security, confidentiality and integrity of medical images from malicious users for timely and successful diagnosis/ high hiding capacity, lower distortion in visual quality, and maintaining the integrity/MATLAB/ Instituto Mexicano del Seguro Social (IMSS)/10 images DICOM file hiding, medical images in greyscale: head and brain (4095 depth 12 bits/pixel) in a cover image, patient identification photo (255 × 255)	Extended visual cryptography with hash-like function circular shift encryption (CRE), then LSB MSB, and SHA 256/ Should be applied to colour images while increasing security and embedding capacity, and other medical image modalities further to 3-D medical imaging.

Table 2 (Continued): Literature Study Based on Proposed Technique

Referred As	Research Goal / Achieved / PL / Database / Data Set Details	Proposed Methods / Future Scope
Karawia, 2021	Information hiding in medical image secure transmission on communication medium/ Imperceptible, image quality retained, resistant to chi-square attacks/ MATLAB/-/ Head (4 secret images) in cove: Lena, baboon, pepper, & Airplane (512 × 512).	LSB steganography with a 1D piecewise tent chaotic map, then a 2D piecewise smooth chaotic map (2DPSCM), then secret key encryption
El-Shafai *et al*., 2023	Security from attackers and hackers attempting to steal patient confidential records, as the current solution lacks efficiency a high number of security breaches. Develop a more efficient algorithm which achieves authenticity, confidentiality, and integrity while resisting security threats/ Secure transmission, high-security performance, high efficiency and robustness against channel noise and attacks, low complexity, and low processing speed low complexity/ MATLAB/ Openmd & Medpix/ Grey & colour medical images (256×256)	Hybrid optical-based Discrete Wavelet Transform (DWT) based compression, then quantisation process, then encrypted using Rubik's cube-based cryptography. Simultaneously optical Double Random Phase Encoding (DRPE) technique is followed by SHA-256 and then a Hash-based Message Authentication Code value (HMAC) digest, and finally steganography/ The method could be checked against more complex attacks, with other security techniques could be applied; future deep learning-based encryption and authentication techniques, robustness and undetectability should also be measured.

The causes of concern pointed out by the previous researchers were: The attacker tries to modify the consistency of the medical image, a collusion attack to harm the sensitive patient data, while the blockchain approach lacks flexibility for cross-organisational application (Ali, *et al.* 2021). 2-D chaotic cat map suffers from brute force attack due to its key size and exhaustive key space attack, while the chaotic map is highly dependent on the initial condition (Akkasaligar & Biradar, 2020). Also showing that DNA, RSA, and chaotic require more time. Cloud-based security models suffer from data loss, theft, and security attacks (Ali *et al.* 2022).

Support Vector Machine (SVM) underperforms for a large set of data with high initial computational complexity (Chowdhuri *et al.* 2023). Previous researchers have emphasised the need to increase the payload capacity, imperceptibility, and enhance security (Abdul, 2022).

Materials and Methods

All the secret greyscale X-ray images are normalised across the row dimension to 500 while maintaining the original aspect ratio. A few assumptions are that the colored cover image dimensions should be 1080 × 1080 × 3, with most of the image's region of interest towards the vertical axis, thus the y-axis. This paper implements LSB and HM.

Least Significant Bit (LSB)

The LSB (Karawia, 2021) of the image is used for hiding the secret image. The cover image is divided based on RGB components. A pixel value from the cover is selected and converted into a binary value. In the least significant bit value of the cover image, the bit value of the secret image is hidden.

Hybrid Method (HM)

In the HM method, firstly, edge-based steganography and then five layers of cryptography (Sharma & Prabha, 2024). HM is the same as HM performed in Sharma & Prabha, (2024); it can also be better understood with the help of the flowchart shown in Figure 3(a) and Figure 3(b). The cover image is downloaded from a publicly available website. It is then opened in the Online Photo editing tool Pixlr (Pixlr, 2021), where the dimensions of the cover image are increased to 1080 × 1080 × 3.

Using the magic wand tool in Pixlr, the background region in the cover image is replaced with a noisy and white background. Following this, EBS is implemented as illustrated in Algorithm 1. The white background cover image will help detect the edges easily. A secret Chest X-ray image is hidden across the edges of the region of interest (ROI) in the noisy background cover image. This process is called Edge-based steganography (EBS).

Algorithm 1: Edge-Based Steganography (EBS) in RONI

Input: White background cover image and noisy background cover image

Secret Image: 5856 X-ray images

Output: 5856 Stego-Images.

Step 1 Load the white background cover image into a 3D array C dimensioned (1080 × 1080 × 3). Divide C based on RGB components, forming three 2D arrays CR, CG, and CB (1080 × 1080). Use the green component CG of the cover image for edge detection. Save all edge pixel positions into two 1D arrays: *row* and *column*.

Step 2 Load the noisy background-colored cover image into a 3D array I (1080 × 1080 × 3). Divide I into RGB components IR, IG, and IB (1080 × 1080) and initialise *count* to 0.

Step 3 Load one of the 5856 X-ray images and increment *count* by 1. Apply Algorithm 1 X-ray image normalisation.

Step 4 Convert the X-ray image into a 1D array X.

Step 5 Using the edge pixel position values calculated in Step 1, embed the elements of X equally across IR, IG, and IB toward the noisy background.

Step 6 If *count* = 5856, proceed to Step 7; otherwise return to Step 3.

Step 7 Stop.

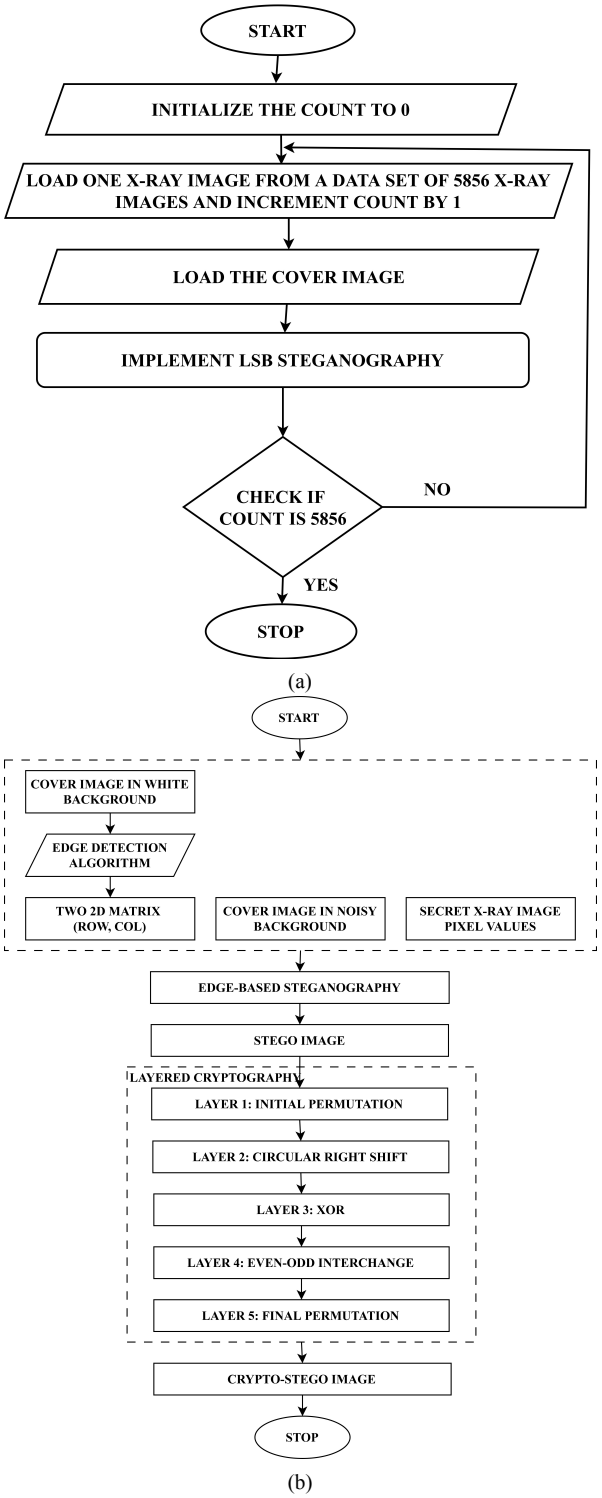

Fig. 3: Working of (a) LSB and (b) HM

Results

The results of the proposed method were achieved in MATLAB. The details of the data set used are: the normalized colored cover image is dimensioned 1080 × 1080 × 3 size is 720 KB. The 5856-secret greyscale, varied-sized Chest X-ray images were downloaded from Mendeley (Kermany *et al.*, 2018). Their details are as follows: the total number of images is 5856, all are in JPEG format, all are Chest X-ray images, with a total size of 1.16 GB. They are all greyscale images, while each varies in dimensions and size.

Computational Time

The computational time-based complexity is a measure of the time taken to perform the encryption and decryption. Here, encryption time (ET) amounts to the time taken to embed the secret image one at a time in the cover image. Decryption time (DT) evaluates the time taken to retrieve the secret image hidden in the cover image. Both ET and DT are found after implementing LSB and HM for the above-mentioned data set, and the values achieved are mentioned in Table 3.

Table 3: Comparison Based on Computational Time

Method	Total Time	Max. Time	Min. Time	Avg. Time
Encryption Time (ET)				
HM	2.0514 min	0.074 sec	0.0117 sec	0.021 sec
LSB	22.52733 Days	3.0519 Hrs	5.915788 min	24.91502 min
Decryption Time (DT)				
HM	4.3094 min	0.1095 sec	0.0142 sec	0.044 sec
LSB	10.4447 Hrs	16.9373 min	13.4578 min	29.0246 min

From Table 3, it can be deduced that HM is a more practical solution than the LSB. The HM was implemented on a total of 5856 X-ray images, which were hidden one at a time in the cover image, taking a total ET of 2.0514 minutes, while the average ET is 0.021 seconds, with a minimum ET of 0.0117 sec, while the total DT is 4.3094 min. with a minimum time of 0.0142 sec. It should be noted that the solution is a more practical solution than LSB, which took a total ET of 22.52 Days and an average ET of 24.91 minutes for encrypting 1302 images out of 5856 images. Therefore, it can be understood that the ET and DT for HM are feasible and real-time compared to LSB.

Table 4: Comparison analysis for previous research work based on Computational Time

Cited As	Time
HM	ET = 0.0117 sec, DT = 0.0142 sec
LSB	ET= 5.915788 min, DT = 13.4578 sec
Ali *et al.*, 2021	For 150 transactions, it is less than 75 microseconds
Akkasaligar & Biradar, 2020)	ET = 0.22 sec., DT = 0.36 sec
Lishomwa & Zimba, 2023)	ET= 2 sec, DT= 0 sec
Awadh *et al.*, 2022	ET = 4.596 seconds
El-Shafai *et al.*, 2023	Avg. CPU time=1.735sec

In Table 4, it can be observed that HM took the least amount of computational time to perform encryption and decryption compared with the literature studied. It is also noted that most researchers have not previously mentioned the computational time taken by their proposed technique and have not used a big data set of 5856 secret Chest X-ray images, in which each image varies in size and dimensions.

DOI: 10.3844/jcssp.2025.2256.2264

From Table 4, it can be concluded that compared to LSB and other researchers' proposed techniques, HM took less ET and DT. Hence, the computational time-based complexity of HM is less.

Performance Test

The performance test formulas and their results are presented. These values were attained by comparing 314 retrieved X-ray images with their original for the LSB method, while for HM, all 5856 X-ray images were retrieved timely. The formulas mentioned below were implemented in MATLAB, and values were obtained.

Mean Squared Error (MSE)

$$\mathrm{MSE} = \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{N} \frac{(\mathrm{I(i,j)} - \mathrm{SI(i,j)})^2}{\mathrm{M} \times \mathrm{N}} \tag{1}$$

In Eq. 1 the MSE value compares the original X-ray image with the retrieved X-ray images. In Eqs. 1 and 16, *I* represents the original image, and *SI* is the retrieved image. The desirable value for MSE is close to 0 for HM is 5.6E-09, while for LSB is 1.90E-05.

Peak Signal to Noise Ratio (PSNR)

$$\mathrm{PSNR} = 10\log_{10} \frac{\mathrm{max}^2}{\mathrm{MSE}} \tag{2}$$

In Eq. 2, variable max is the maximum value at any pixel position in the secret image. HM, the PSNR value is 82.51967, LSB is 32.391. Hence, the HM has attained good results. PSNR preferred value is high.

Root Mean Square Error (RMSE)

$$RMSE = \sqrt{MSE} \tag{3}$$

RMSE value for HM is 0.0000748 while LSB is 0.00435. A low value is desirable. Hence, HM is highly preferred over LSB.

Structural Similarity Index Metrics (SSIM)

$$\mathrm{SSIM}\,(\mathrm{x}, \mathrm{y}) = \frac{(2\mu_{Ac}\mu_{Re} + \mathrm{c}_1)(2\sigma_{\mathrm{AcRe}} + \mathrm{c}_2)}{\left(\mu_{\mathrm{Ac}}^2 + \mu_{Re}^2 + \mathrm{c}_1\right)\left(\sigma_{Ac}^2 + \sigma_{\mathrm{Re}}^2 + \mathrm{c}_2\right)} \tag{4}$$

The similarity of the original and retrieved X-ray image is measured with the SSIM value for HM is 1, which is also the preferred, while for LSB is 0.78891. In Eq. 4, c_1 and c_2 are two constants, $\mathrm{A_c}$ and $\mathrm{R_e}$ are actual and retrieved X-ray secret images, respectively, for Eqs. 4, 6, 7, 9 and 13. In Eqs. 4, 7, 8 and 9, μ represents the mean value, while σ in Eqs. 4, 6, 7, and 9 represents the standard deviation.

Embedding Ratio (ER)

$$ER = \frac{p}{M \times N} \tag{5}$$

Pearson Coefficient (R)

$$\mathrm{R}\,(\mathrm{Ac}, \mathrm{Re}) = \frac{\mathrm{Cov(Ac,Re)}}{\sigma_{\mathrm{Ac}}\sigma_{\mathrm{Re}}} \tag{6}$$

The desirable value for R is 1, which is achieved by HM, while for the LSB method it is 0.98949.

Coefficient of Variation (Cov)

$$\sigma_{Ac} = \sqrt{\frac{(\sum(\mathrm{Ac} - \mu))^2}{\mathrm{L}}} \tag{7}$$

$$\mu_{Ac} = \frac{\sum \mathrm{Ac}}{\mathrm{L}} \tag{8}$$

$$\mathrm{Cov}\,(\mathrm{Ac}, \mathrm{Re}) = \frac{\sum(Ac - \mu_{Ac}) \times (Re - \mu_{Re})}{L} \tag{9}$$

A higher value of Cov is preferred.

Number of Pixel Changing Rate (NPCR)

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{i,j}}^{N,M} \mathrm{D(i,j)}}{\mathrm{M} \times \mathrm{N}} \times 100 \tag{10}$$

$$\mathrm{D}\,(\mathrm{i}, \mathrm{j}) = \begin{cases} 0 if \mathrm{c}_1\,(\mathrm{i}, \mathrm{j}) = \mathrm{c}_2\,(i, j) \\ 1 otherwise \end{cases} \tag{11}$$

Preferred value for NPCR is greater than 99 %, HM attained 95.59, while LSB 17.5999.

Compression Ratio (CR)

$$\mathrm{CR} = \frac{|Ac|}{|Re|} \tag{13}$$

CR should have a high value. CR for HM was 8.83, while for LSB it is 1.018.

Unified Average Changing Intensity (UACI)

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N}} \left(\sum_{\mathrm{i,j}}^{N,M} \frac{|\mathrm{c}_1\mathrm{(i,j)} - \mathrm{c}_2\mathrm{(i,j)}|}{255} \right) \times 100 \tag{12}$$

In Eqs. 12, 15, 17, 18 and 19 c_1 represents the original X-ray image compared with, c_2 the retrieved image. The *i* and *j* are the image pixel positions, while 255 is the maximum value in the image. Here, N and M are the maximum row and column pixel positions. UACI desirable value is 33 here, HM value is 2.30E-05, while LSB is 4.10E-06.

Entropy (E)

$$E = -\sum_{i=1}^{N} P\,(Re) \log_2 P\,(Re) \tag{14}$$

For HM the Entropy (E) value is 7.8398 while LSB is 6.59199. The E value close to 8 is preferred hence HM value is better. The $\mathrm{P(R_e)}$ in Eq. 14 represents the probability of the retrieved image.

Kullback–Leibler Divergence (KLD)

$$KLD = \int c_2\,(x) \times \log \frac{c_1(x)}{c_2(x)} d\,(x) \tag{15}$$

A low value of KLD is preferred.

Bit Error Rate (BER)

$$BER = \frac{\sum_{i,j}^{N,M} I(i,j) \otimes S(i,j)}{L} \tag{16}$$

A lower BER value is desirable.

Mean Absolute Percentage Error (MAPE)

$$\mathrm{MAPE} = \frac{1}{\mathrm{L}} \sum_{\mathrm{i}=1}^{\mathrm{L}} \left(\frac{|\mathrm{c}_1\mathrm{(i)} - \mathrm{c}_2\mathrm{(i)}|}{\mathrm{c}_1\mathrm{(i)}} \right) \times 100\% \tag{17}$$

DOI: 10.3844/jcssp.2025.2256.2264

MAPE value for LSB is 0.00106 while HM is 1.89E-07 as per Eq. 17. The preferred value for MAPE test should be 0, therefore, HM achieved better results.

Signal to Noise Ratio (SNR)

$$SNR = 10\log_{10}\frac{\sum_{i=1}^{L}(c_1(i)-c_2(i))^2}{\sum_{i=1}^{L}(c_1(i))^2} \quad (18)$$

SNR, a lower value is desirable.

Percentage Residual Difference (PRD)

$$PRD = \sqrt{\frac{\sum_{i=1}^{L}(c_1(i)-c_2(i))^2}{\sum_{i=1}^{L}(c_1(i))^2}} \times 100\% \quad (19)$$

PRD value for LSB is 0.20375, HM is 7.463, a low value is desirable as achieved by LSB for Eq. 19. The values achieved after implementing LSB and HM are compared based on various performance test values that were achieved (Table 5). The HM has better performance compared to LSB while dealing with the same data set of secret and cover images. The performance test values for E, R, SSIM, PSNR, MSE, RMSE, NPCR, and MAE were considerably better for HM in comparison with LSB.

Figure 4 shows the graphical depiction of the various performance test values. A low value of MSE is preferred in Figure 4(a). HM achieved the lowest value of 5.6E-09. Figure 4(b). for R values depicted that HM (Aleisa, 2022; Al-Shaarani & Gutub, 2021) has attained the best value of 1. A high value of PSNR is desired as per in Figure 4(c).

Table 5: Comparison HM with LSB Based on Performance Test

Metric	MAE	PRD	CR	UACI	NPCR	E	KLD	MSE	PSNR	SSIM	Cov	R	SNR	RMSE	BER
HM	1.89E-07	7.463	8.835235	2.30E-05	95.59	7.8398	-8.80E-06	5.6E-09	82.51967	1	690636.3	1	0.049221	0.0000748	9.66E-06
LSB	0.00106	0.20375	1.01772	4.10E-06	17.5999	6.59199	0	1.90E-05	32.391	0.78891	13393.09	0.98949	-0.0144	0.00435	0.176

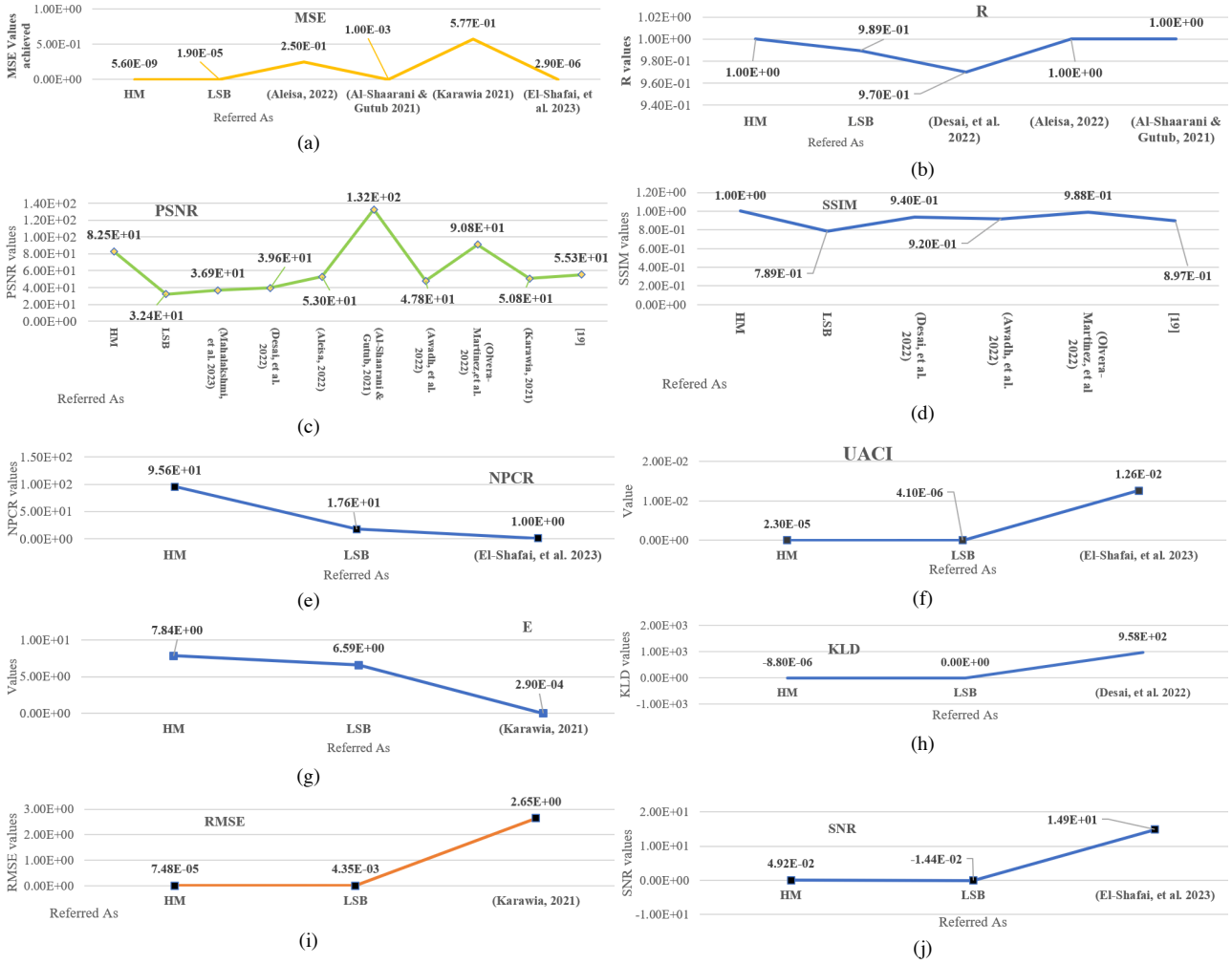

Fig. 4: Comparative plots for various performance tests (a) MSE, (b) R, (c) PSNR, (d) SSIM, (e) NPCR, (f) UACI, (g) E, (h) KLD, (i) RMSE, and (j) SNR

Olvera-Martinez *et al.* (2022) achieved a PSNR value of 90.8 and an HM value of 82.52, while Al-Shaarani & Gutub (2021) had 132.47, which is not valid. HM obtained the SSIM value of 1, which is preferred

compared to the referred work, as shown in Figure 4(d). Figure 4(e) for NPCR shows that the El-Shafai *et al.* (2023) value of 99.9, while HM attained 95.59. UACI, KLD, RMSE, and SNR values were plotted in Figure 4(f), Figure 4(h), Figure 4(i), and Figure 4(j). The preferred value for E is close to 8. The HM obtained a value of 7.84.

Discussion

EMI has grown with the increase in population. EMI security is a major issue of concern. Comparing the standard technique, LSB, with the HM based on reduced computational time. LSB steganography is still currently implemented widely in combination with other data-hiding techniques to increase security. The results indicate that LSB requires significantly more time than HM for embedding 5856 X-ray images in the cover image.

The following properties of the HM help understand why HM is more suitable for real-time applications. The HM is simple to understand, and can be used even by naive users while being usable on various types of devices (like Android, laptop, etc.). HM is high in performance as it is seconds to hide and extract an image, efficient to use as it does not require any high-power GPU, nor any kind of special resources. Neither the HM nor the LSB methods won't need training as per the dataset. The HM was able to encrypt and decrypt in 0.0117 sec and 0.0142 sec, respectively, compared to the LSB ET of 5.9159 min. and DT of 13.4578 min. Both techniques comply with HIPAA and GDPR. HM is practical to work with while dealing with data of varying sizes and dimensions.

Conclusion

HM and LSB were implemented for hiding a larger set of 5856 greyscale Chest X-ray images, each of varying sizes. The computational time-based complexity of the LSB was very high compared to HM. In case LSB is combined with any other algorithm, such an implementation will only increase the computational time and complexity of the algorithm. The value for the various performance tests for HM showed good results in comparison to LSB. Hence, LSB is not a practical solution for hiding a secret image in a cover image. As EMI are accessed in real-time, security for EMI should be provided in real-time. Concluding that the HM is better than the LSB method in terms of computational time-based complexity. The validity of LSB and HM has been verified with the various performance tests. The suggested HM outperforms LSB and other referred methods. In the future, a comparison can be made with other conventional algorithms (like AES, DES, and T-DES) for hiding a secret image in a cover image. Furthermore, Continuous feedback could be incorporated into the HM to improve the technique as per real-time requirements. The HM can be extended to 3D medical images (like CT, MRI) or other types of digital data, such as colored images, audio signals, video, etc.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Authors Contribution

All authors equally contributed to this study.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all other authors have read and approved the manuscript, and no ethical issues are involved.

References

Abdul, W. (2022). Security of medical images over insecure communication channels using zero-steganography. *International Journal of Distributed Sensor Networks*, *18*(2), 155014772110063. https://doi.org/10.1177/15501477211006347

Akkasaligar, P. T., & Biradar, S. (2020). Selective medical image encryption using DNA cryptography. *Information Security Journal: A Global Perspective*, *29*(2), 91–101. https://doi.org/10.1080/19393555.2020.1718248

Aleisa, H. N. (2022). Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things. *Journal of Healthcare Engineering*, *2022*, 1–11. https://doi.org/10.1155/2022/7528583

Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. *Sensors*, *22*(2), 528. https://doi.org/10.3390/s22020528

Ali, A., Rahim, H. A., Ali, J., Pasha, M. F., Masud, M., Rehman, A. U., Chen, C., & Baz, M. (2021). A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority. *Applied Sciences*, *11*(21), 9999. https://doi.org/10.3390/app11219999

Al-Shaarani, F., & Gutub, A. (2022). Securing matrix counting-based secret-sharing involving crypto steganography. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6909–6924. https://doi.org/10.1016/j.jksuci.2021.09.009

Awadh, W. A., Alasady, A. S., & Hamoud, A. K. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. *International Journal of Electrical and Computer Engineering (IJECE)*, *12*(6), 6574. https://doi.org/10.11591/ijece.v12i6.pp6574-6584

Chowdhuri, P., Pal, P., & Si, T. (2023). A novel steganographic technique for medical image using SVM and IWT. *Multimedia Tools and Applications*, *82*(13), 20497–20516. https://doi.org/10.1007/s11042-022-14301-0

Desai, S. D., Patil, N., Nirmala, S. R., Kulkarni, S., Desai, P. D., & Shinde, D. (2022). Deep Neural Network based Medical Image Steganography. *2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*. https://doi.org/10.1109/icstsn53084.2022.9761321

El-Shafai, W., Almomani, I., Ara, A., & Alkhayer, A. (2023). An optical-based encryption and authentication algorithm for color and grayscale medical images. *Multimedia Tools and Applications*, *82*(15), 23735–23770. https://doi.org/10.1007/s11042-022-14093-3

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

Kermany, D. S., Zhang, K., & Goldbaum, M. (2018). Identifying medical diagnoses and treatable diseases by image-based deep learning. *Cell*, *172*(5), 1122–1131.e9.

Lishomwa, K., & Zimba, A. (2023). A Privacy-Preserving Scheme for Medical Diagnosis Records Based on Encrypted Image Steganography. *Zambia ICT Journal*, *7*(1), 23–28. https://doi.org/10.33260/zictjournal.v7i1.151

Mahalakshmi, G., Sarathambekai, S., & Vairam, T. (2023). Improving security using Swarm intelligence based optimal pixel selection in Image steganography-A Study. *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*. https://doi.org/10.1109/iciscois56541.2023.10100500

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Mohammed, K. I., Albahri, O. S., Albahri, A. S., & Alsalem, M. A. (2021). PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. *Multimedia Tools and Applications*, *80*(9), 14137–14161. https://doi.org/10.1007/s11042-020-10284-y

Olvera-Martinez, L. A., Cedillo-Hernandez, M. A. B., Diaz-Rodriguez, C. A. A., & Jimenez-Borgonio, E. T. A. (2022). Secure Exchange of Medical Images Via Extended Visual Cryptography. *Revista Mexicana de IngenieriaBiomedica, Sociedad Mexicana de IngenieriaBiomedica*, *43*, 64–77. https://doi.org/10.17488/RMIB.43.2.5

Sharma, D., & Prabha, C. (2023). Security and Privacy Aspects of Electronic Health Records: A Review. *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*. https://doi.org/10.1109/incacct57535.2023.10141814

Sharma, D., & Prabha, C. (2024). *Hybrid security of EMI using edge-based steganography and three-layered cryptography*. 278–290. https://doi.org/10.1201/9781003471059-37

Singhal, Mr. V., Shukla, Mr. Y. K., & Prakash, Dr. N. (2020). Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256. *International Journal of Innovative Technology and Exploring Engineering*, *9*(8), 641–648. https://doi.org/10.35940/ijitee.h6442.069820