IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 October 2024, accepted 28 October 2024, date of publication 31 October 2024, date of current version 18 November 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3489452

RESEARCH ARTICLE

Securing X-Ray Images Into Cover Images Using Hybrid EBS Steganography With Five-Layer Cryptography

DIVYA SHARMA[1], CHANDER PRABHA[1], MD MEHEDI HASSAN[2], (Member, IEEE), SHAHAB ABDULLA[3], ANUPAM KUMAR BAIRAGI[2], (Senior Member, IEEE), SAMAH ALSHATHRI[4], AND WALID EL-SHAFAI[5,6], (Senior Member, IEEE)

[1]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab 140401, India
[2]Computer Science and Engineering Discipline, Khulna University, Khulna 9208, Bangladesh
[3]UniSQ College, University of Southern Queensland, Toowoomba, QLD 4305, Australia
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[5]Security Engineering Laboratory, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia
[6]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Corresponding authors: Md Mehedi Hassan (mehedihassan@ieee.org), Chander Prabha (prabhanice@gmail.com), Samah Alshathri (sealshathry@pnu.edu.sa), Walid El-Shafai (eng.waled.elshafai@gmail.com), and Divya Sharma (divya1007cse.phd21@chitkara.edu.in)

This work was supported by Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, through the Researchers Supporting Project PNURSP2024R197.

ABSTRACT Electronic Medical Images (*EMI*) have grown with the increase in population. *EMI* are used for medical diagnosis for medical emergencies hence, they should be correct and clear for accurate diagnosis. In general, *EMI* are of varying sizes and dimensions. The aim is to enhance the security and privacy of *EMI* with reduced computational time while dealing with a larger and varying-sized data set. Reducing computational time will make the method suitable for real-time applications (*RTA*). Hence, a data set of *5856* secret *X-ray* images all varying in dimensions, total sized up to *1.16 GB*, are applied with a hybrid of steganography and cryptography. Here, one *X-Ray* image is taken at a time then hidden into a single cover image using Edge-based steganography and then encrypted using five layers of cryptography. Various performance evaluation tests such as Structural Similarity Index Metrics (*SSIM*) achieved a value close to *1* which is the preferred value, Peak Signal-to-Noise Ratio (*PSNR*) is *82.51967* dB which is good, Mean Square Error (*MSE*) is *5.6E-09* which is close to zero indicating no addition of noise in the retrieved *X-ray* images, the Correlation (*R*) is *1*. Therefore, the extracted image is the same as the original *X-ray* images, while remaining tests such as *RMSE*, Entropy, *KLD, BER, SNR, CV, MAPE, PRD,* etc. achieved good results. The computational time is measured by the Encryption Time (*ET*) is *0.37* seconds while the Decryption Time (*DT*) is *3.9275* sec. Thus, it can be concluded that a hybrid method *(HM)* could be implemented for *RTA*.

INDEX TERMS Electronic medical images (EMI), security, privacy, cryptography, steganography.

I. INTRODUCTION

Electronic medical images *(EMI)* are growing with the growth in population. *EMI* users have also grown because of its features such as flexibility, scalability [1], easily accessible, reduced time [2], ease to use any time, any place, reduces retesting time, and cost, etc. *EMI* consists of confidential information such as body part, medical history, disease description, diagnosis, patient's personal and payment details which should be kept a secret [3]. Electronic Medical Images *(EMI)* are Magnetic resonance imaging *(MRI)* [4], *X-ray* [5], [6], computed tomography *(CT)* scan [4], Electrocardiogram *(ECG)* [7], [8], [9].

Doctors use *EMI* for medical diagnosis and researchers use them for the development of machine learning algorithm [3] which help in early prediction of diseases, etc. In Pharma

The associate editor coordinating the review of this manuscript and approving it for publication was Rahim Rahmani.

companies, researchers use them to enhance already available medical treatments. They are also used by insurance agencies, doctors, government agencies, academic researchers, and genome registry [10]. As such the *EMI* need to be accurate, correct, valid, readable, and understandable for correct diagnosis [11].

The authors in [10] discussed the potential risks/threats [12] faced by them such as phishing attacks, malware attacks, low vision spot encryption, cloud threats, and insider attacks [2], [13], [14], [15], [16], [17]. Thus, the security of *EMI* needs to be enhanced from hackers [17], [18] and attackers [3].

This research work is motivated as changes in retrieved *EMI* could lead to incorrect diagnosis or even death [11]. Hence, to enhance security while ensuring privacy [14], [19], [20] of *EMI* while reducing the encryption and decryption time [21], [22] is an important aspect [2]. As already existing algorithms lead to noisy *EMI* as output [23]. Therefore, an implementation of hybrid [22], [24], [25] of edge-based steganography [9], [26], [27] with five layers of cryptography on *EMI* were performed here.

A. RESEARCH CONTRIBUTIONS

The major contribution of this research work has been listed below:

- Tabular study of the recent literature work conducted for securing *EMI*.
- To deal with a larger data set of *EMI* without normalizing their size to such that would render them unclear or non-understandable for future medical diagnosis. Therefore, dealing with diverse, varied sized, and different dimensioned *EMI [2], [21]* which retains their quality after retrieval.
- Implementing a hybrid [1] of *EBS [27]* with five layers of cryptography on *EMI* while reducing computational time-based complexity [20], [28], [29]. Implementing a hybrid method will ensure that the properties of both cryptography and steganography have enhanced the security of *X-ray* images. Hence increased resistance against various kinds of attacks [16].
- As *EMI* image quality is important as they are often used to make decisions in medical emergencies. While reducing computational time and retaining *EMI* image quality helps practitioners timely make better and correct medical decisions.
- Checking the validity of the hybrid [24], [30] of *EBS* and five-layer cryptography method by performing various evaluation tests such as SSIM, PSNR, MSE, etc. [31], [32].

This research work is organised into the following sections: Section II gives a tabulated understanding of the current state of research work done for securing *EMI* with its details on the data set, and the programming language used by the researcher. Section III discusses the hybrid method *(HM)*algorithm with its flowchart. Section IV details the experimental results achieved after implementing *HM* on 6 cover images hidden with *5856* secret X-ray images based on the ET and DT. Section V the values achieved by *HM* for various performance evaluation tests such as *MSE, PSNR, SSIM, R,* etc. Finally, the conclusion and Future scope have been discussed.

TABLE 1. Research study based on programming language and used data set.

Cited as	Language	Data Set Details
HM	**MATLAB R2021a**	**Six cover images: 1080 × 1080 × 3 with a total size of 2.92 MB, Secret images: 5856 X-ray images of varying dimensions sized 1.16 GB: Data set from [32] All images were initially in JPEG format**.
[1]	Python	Secret: Block of characters "Rose Adee encrypted files" converted to ASCII, 3 cover images sized 1.2MB, 2.9, and 7.2MB.
[33]	MATLAB and Visual C++	Real electrocardiographs, photoplethysmography, and Holter cardio data recorded for up to 72 h.
[29]	MATLAB 2020b and Python	Grey-scale images 256 ×256.
[34]	MATLAB R2016b	Secret: 880 × 660 (pelvis and thorax), 256 × 256; Leg, Eye, Thorax, Pelvis, cover images: Lena, Baboon, Barbara, Cameraman.
[3]	MATLAB R2018a	Secret images: Human Brain 699 × 911, MRI 512 × 513, Lungs 425 × 425; 50 grey-scale and 50 RGB images, 512 × 512, cover image: Lena 512 × 512.
[17]	MATLAB R2018a	Secret data: Patient text file of 100 characters, including patient name, age, gender, address, etc. medical diagnosis sized 107 bytes, cover images: 6 abdominal CT 335 × 400, Heart CT-scan 412 × 800, Brain-MRI 1175 × 1332, Neck-MRI 315 × 560, Chest X-ray 174 × 290, Body X-ray 483 × 626.
[35]	MATLAB R2016a	Secret: images X-ray Foot 512×512, CT Brain 256×256, MRI Head 256×256, Ultrasound Fetus 512×512, PET Brain 256×256, Virus COVID-19 512×512, cover image: Lena 512×512, Normal image Peppers 256×256, output size 2.45 Mbps.
[36]	MATLAB R2020b	4 CT images 512 × 512, 2 MRI size 320 × 320 Grey and colour images 256×256 dimensions. Dataset from https://openmd.com, and https://medpix.nlm.nih.gov.
[37]	MATLAB	32 high-resolution CT scan images 677 × 598, size 364.2 KB. Size of 32 images 11.3 MB. Dataset from National Institute of Health.

II. LITERATURE STUDY

In Table 1 the literature is studied based on the programming language used in the hybrid method (*HM*) and by other researchers with details on the data set with sizes of EMI that have been secured.

In [11] Python programming language was used. Table 1 researchers of [4], [29], [35], [36], and [37] have normalized *EMI* to dimensions of *256 × 256, 512 × 512, 699 × 911*, and lesser. Here the data set which is originally of varying sizes

TABLE 2. Literature study.

Cited as	Research goal	Achieved	Proposed Technique	Future
[1]	Data security is based on cryptography and steganography in a cloud reducing security and privacy concerns such as data theft, and manipulation.	Ensures twice the protection of the cloud with more redundancy, flexibility, efficiency, and security by protecting data confidentiality, privacy, and integrity from attackers.	Rivest–Shamir Adleman, Advanced Encryption Standard, with identity-based encryption algorithms alongside Least Significant Bit steganography	More research is needed to improve the combination of steganography with cryptography and provide greater security for multimedia data.
[33]	Protect cardiac database against unauthorized access	Effective, secure, stable, and potential use in telemedicine	Daubechies wavelet transform then Energy Packing Efficiency-based compression	-
[29]	Security of image while in communication	Secure, efficient, and immune from attacks, ensures noise immunity due to more advantages of parallel SAE computations, and significantly reduces runtime complexity.	Stacked Auto-Encoder (SAE)	Deep learning algorithm with extraction from the region of interest in medical images then compression and multi-stage security comprise watermarking and hiding schemes with employee encryption for robust broadcasting in telemedicine IoT.
[34]	Secure transmission of medical information between practitioners	Good encryption performance, more efficient, secure, fast encryption, excellent resistance against differential attacks.	Cryptography using Logistic May (LM) and Henon Maps with SHA-256	-
[3]	To develop a new, fast, and secure medical image that withstands attacks	Fast computational time, efficient, can withstand cropping and noise attacks, implementable in RTA	The 1D logistic map associated with pseudo-random numbers	Randomness increased, RGB image can be encrypted using interleaving, diffusion-confusion.
[17]	Securing E-health images	Robust	LSB and key compression with six stages of chaotic maps: Chebyshev, Gauss, Henon, Logistic, Tent, and Piecewise maps then DNA encoded	Randomness increased, RGB image can be encrypted using interleaving, diffusion-confusion
[35]	Medical image transmission and storage quickly and securely	Good visual quality, high entropy, low adjacency correlation, low time complexity, uniformly distributed histogram, correlation between adjacent pixels is weak, information entropy close to ideal value 8 of cipher-images	Permutation then substitution enhanced 2-D logistic chaotic map with SHA-256	Implementing a combination of semi-selective image encryption with high information region and implementing the algorithm on different platforms.
[11]	Secure, authentic, confidential transmission of medical images over the Internet faces challenges of size and privacy	High security and good efficiency, image quality retained, free from statistical attacks, no noise addition in achieved medical image	7z-based lossless compression with public key encryption algorithm Elliptic Curve Cryptography (ECC)	-
[4]	Multiple medical image encryption	Good encryption effects, resistance to attacks, higher security, faster encryption speed, better performance, time efficiency, high efficiency	Logistic tent 1-D Lyapunov Exponent chaotic system with Fisher-Yates scrambling and diffusion algorithm	Generalizing the encryption algorithm to various types of medical images
[36]	Security from attackers and hackers of patient confidential records as the current solution lacks efficiency as high number of security breaches. Develop a more efficient, confidential, authentic algorithm which resists security threats while maintaining integrity	Secure transmission, high-security performance, high efficiency and robustness, low complexity, low processing speed	Hybrid optical based Discrete Wavelet Transform (DWT) based compression then Quantization process then encrypted using Rubik's cube-based cryptography with optical Double Random Phase Encoding (DRPE) technique then SHA-256 generating (Hash-based Message Authentication Code value (HMAC then Least Significant Bit (LSB) steganography	Other more complex attacks could be injected, other security techniques could be applied, and future deep learning-based encryption and authentication techniques, robustness and not detectable should also be measured.
[37]	Medical images carry sensitive patient data from unauthorized access over the Internet	The extracted image is of good quality, robust	Random phase with transposition method encrypted then phase grating on 32 cross-sectional CT-scan images	-

and dimensions *X-ray* images [38] are normalized if their dimensions are greater than $500 \times NAN$. It can be deduced that most of the previous researchers have used MATLAB as their programming language except for [1] where Python was used. Table 1 summarises that [17] has used *6 EMI*, [3] used *50 EMI*, [34] used *5 EMI*, [37] with *32 EMI*, etc. which are lesser in number compared to *5856 X-ray* images used in this research work. Authors of [4] have mentioned the need for a method which could deal with a large number of different-sized *EMI*. The literature study that helps formulate hybrid method *(HM)* has been tabulated in Table 2 based on the research goal that led to their research, results achieved after implementing the proposed method, proposed work that they have implemented, and future suggestions made by them.

Table 2 shows that previous researchers worked towards enhancing the security of *EMI* while it is being transmitted or stored on third-party storage. Conventional methods such as the Rivest-Shamir algorithm (*RSA*), stacked autoencoder (*SAE*), secure hash algorithm (*SHA*), advanced encryption algorithm (*AES*) elliptic curve cryptography (*ECC*), Discreet wavelet transform (*DWT*), and least significant bit (*LSB*). These conventional methods are well known to all, easy to detect, and vulnerable to attacks but are time-consuming and thus complex to implement [39].

The total time taken to hide *5856 X-ray* images into cover image using Edge-based steganography (*EBS*) was *2.0514* minutes while Block-based steganography (*BBS*) was *9.112* min [27]. This research is motivated to reduce computational time-based complexity hence *EBS* is selected.

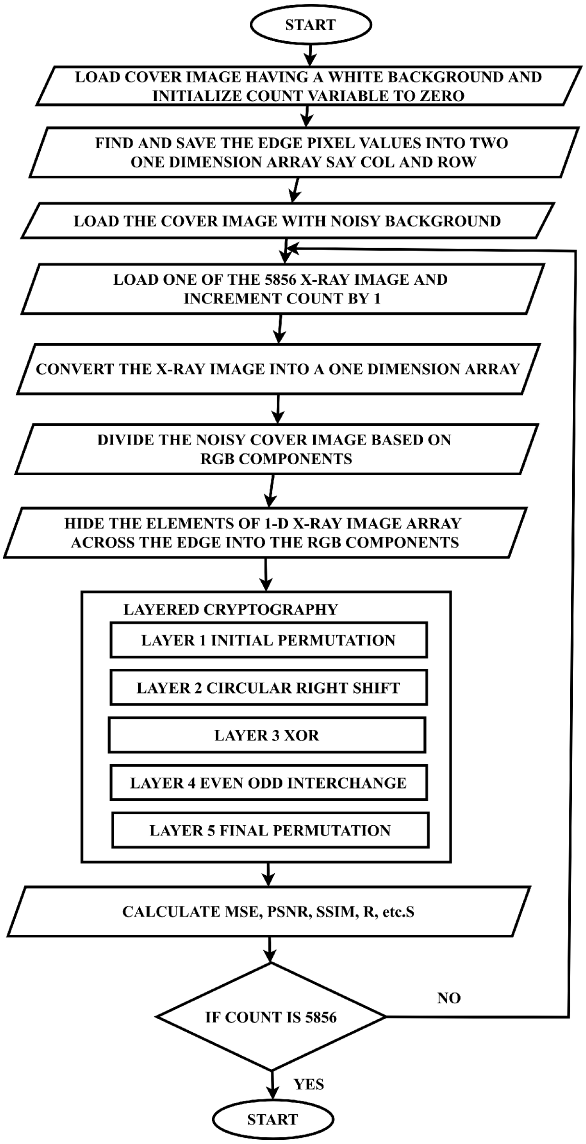

FIGURE 1. Flowchart of hybrid method.

The combination of *(EBS)* with five-layered cryptography enhances the security and privacy of *EMI*. Reducing time-based complexity will help its users to refer *X-ray* images in real-time.

III. HYBRID METHOD (HM)

HM method combines *(EBS)* with five layers of cryptography. The working, of *EBS* with five layers has been explained in this section. Implementing steganography enacts the properties of steganography such as tamper resistance, robustness, imperceptibility, payload capacity, and secrecy while cryptography ensures authenticity, integrity, confidentiality, non-repudiation, privacy, and reliability properties [40]. The noisy and white background cover images were created using the online photo editing tool Pixlr.com available online at *[41]*. *HM* algorithm is discussed in Algorithm *1* while its flowchart is shown in Figure 1.

A. DATA SET USED

This research deals with *5856* secret *X-ray* images in *JPEG* format differing in dimensions and sizes. These have been downloaded from the online database Mendeley [38]. A few *X-ray* images are shown in Figure 2. The *6 JPEG* cover images are shown in Figure 3. These cover images were downloaded from the online public database.

B. EDGE-BASED STEGANOGRAPHY (EBS)

For edge detection, the green component of the white background cover image is loaded. With the help of MATLAB's inbuilt edge function, the method "Prewitt" is used at threshold *0.025* the edge pixel values are found. These pixel values are saved into two *1D* arrays say row and column. Figure 4 shows a cover image in a white and noisy background. It also highlights the edge position on the white cover image. These edge positions are used on the noisy coloured cover image to locate the edge pixel and is the same across all *RGB* components. The condition for *HM* is that the cover image should have more region of interest towards the y-axis. Therefore occupying more area vertically.

The noisy cover image is loaded into variable array say *A*. *A* is further divided based on *RGB* components and saved into variable arrays *AR, AG,* and *AB*. One of the *5856* greyscale *X-ray* image is loaded into *2D* array say *X*. Then *X* is resized to *500* to *NAN* with respect to the aspect ratio of the original image. This is done when the row size is greater than 500. *X* is converted into a *1D* array say *XA*. Then one row and column value are used to pinpoint the same edge position on all three components. The data is hidden from the edge position towards the noisy background in the cover image. An equal amount of data from *XA* is hidden across all components for all edge positions.

After hiding all the elements of *XA*. The three components are combined into one coloured image. This stego-image is encrypted using five layers of cryptography.

C. FIVE LAYERS OF CRYPTOGRAPHY

The stego-image generated after *EBS* is applied with five layers of cryptography. Here these five unique layers of cryptography have been discussed in detail.

Layer 1: Initial Permutation *(IP)*: In *IP* a random row wise scrambled array of size *1080* × *1080* is created. It has *1080* rows and *1080* columns. Each row has index values ranging from *1:1080*. Each row values are randomized and the table created is called *IP* table. The *IP* table is used as a substitution table for the previous stego-image. This layer causes diffusion [42] of pixel values. IP table is obtained once initially and used for all components and all *5856* X-ray images. This *IP* table will be sent to the receiver to retrieve the hidden X-ray images. In Figure 5 a *6* × *6*-pixel values table is used as an example to illustrate the proper working of *IP* layer. It should be noted that the actual dimensions of the stego-images are *1080* × *1080* × *3* while the *IP* table is *1080* × *1080*. The *3* is for the *RGB* components of the

FIGURE 2. Few X-ray images from the data set of 5856 X-ray images.

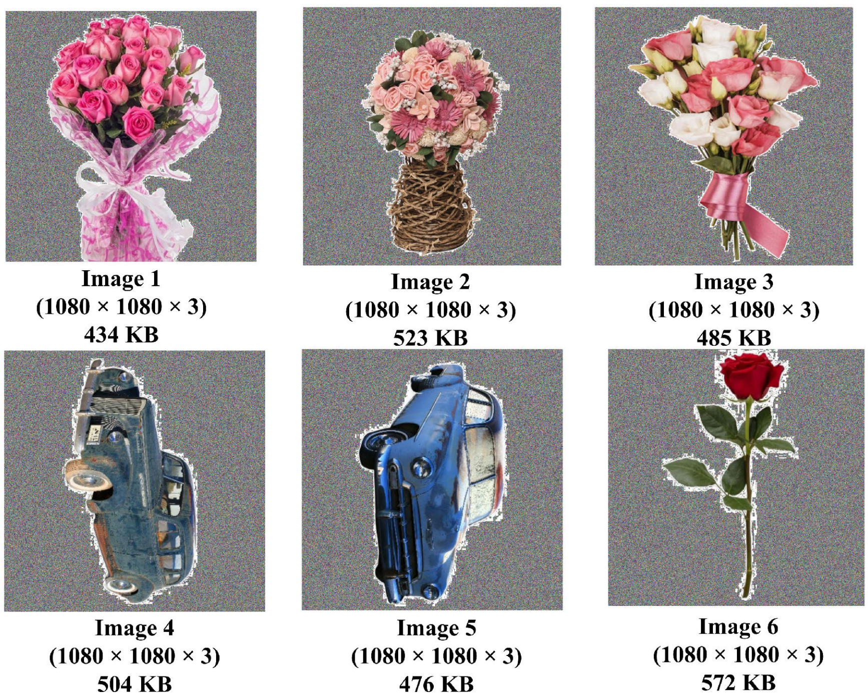

FIGURE 3. 6 Cover images used for hiding the X-ray images.

coloured stego-image. The same *IP* table will be used on all components as well as for all *5856* X-ray images hidden one at a time into the cover image. But the *IP* table will vary for the different cover images.

Layer 2: Circular Right Shift *(CRC)*: The output image achieved after implementing layer *1* acts as input. The image components are divided into left half and right half each dimension *540* × *1080*. Here *540* is the number of columns whereas *1080* is the number of rows. Thus, a total of 6 halves are created. The first four columns on the left side of all *6* halves are shifted circularly right. Figure 6 for a matrix size *6* × *6* is applied with a circular right shift by *4* columns.

Layer 3: *XOR*: Here the left half is *XOR* with the right half of the output from layer *2*. This resulting image will

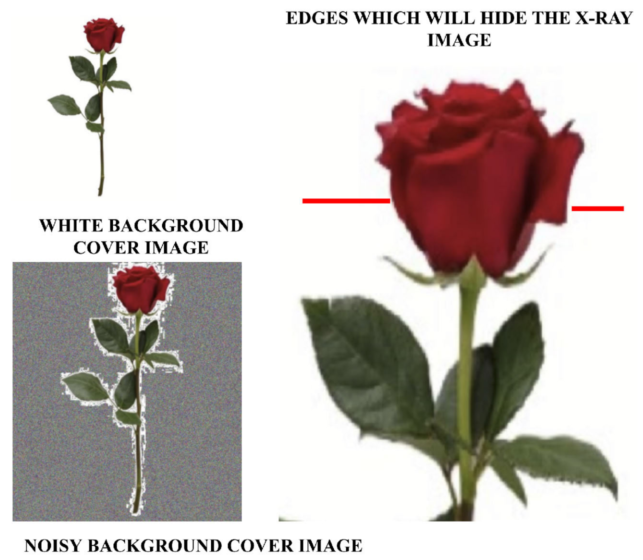

FIGURE 4. White and noisy background cover images, the edge's locations.

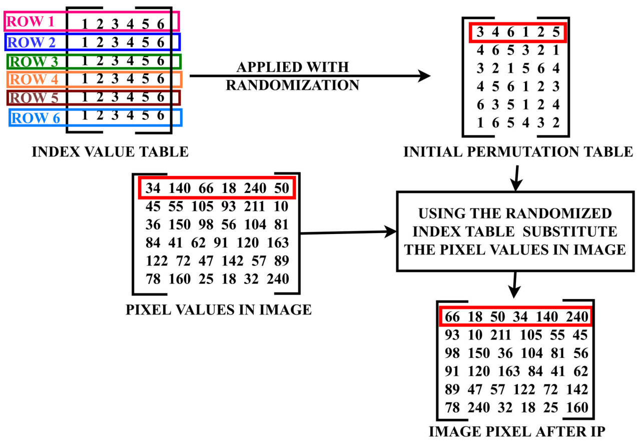

FIGURE 5. Showing the IP table and method implemented in the layer 1.

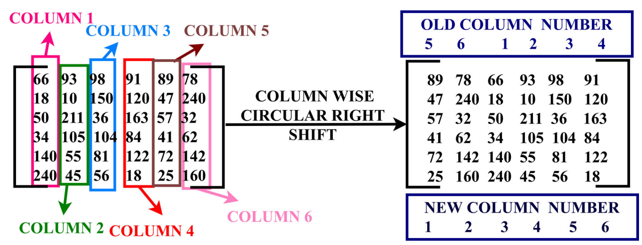

FIGURE 6. Working of layer 2 cryptography.

now become the new left half. The old left half will become the new right half. This is repeated for the remaining two components. A diagrammatic explanation of *XOR* can be seen in Figure 7.

Layer 4: Even-Odd Interchange: Here the new left and new right half of the image are combined into one component having a size of 1080×1080. The remaining component halves are combined into one component. Then each even column is interchanged with odd columns and vice-versa. This is done to all components. Figure 8 simplifies the working of this layer.

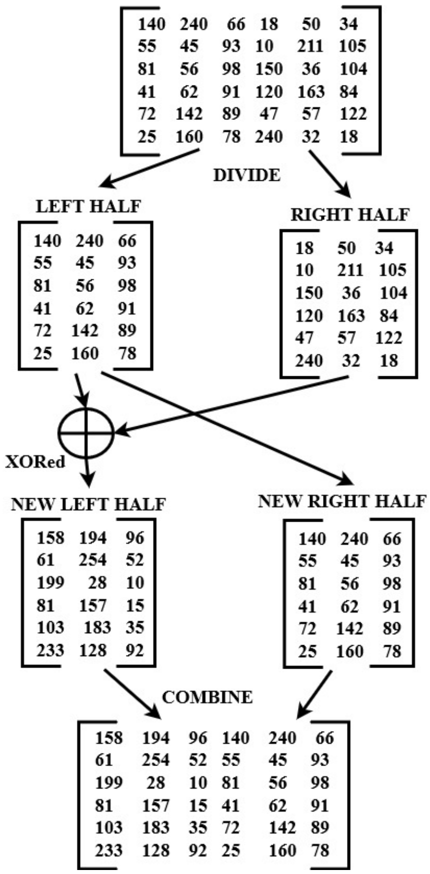

FIGURE 7. Working of layer 3 of cryptography.

FIGURE 8. Working of layer 4.

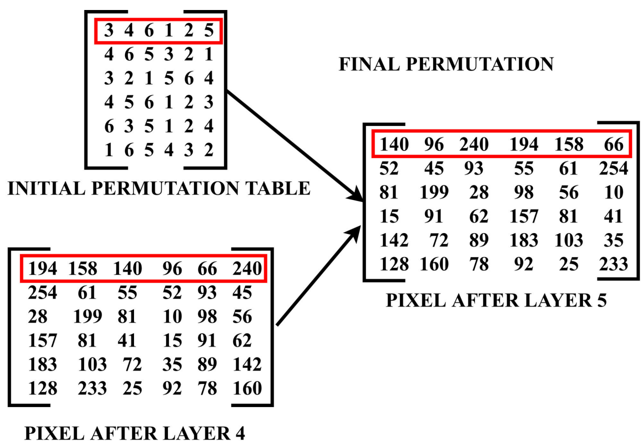

FIGURE 9. Layer 5 of cryptography.

Algorithm 1 HM Algorithm

Input: 6 Cover Images C_i $(i = 1, 2, \ldots, 6)$ each of size $1080 \times 1080 \times 3$, 5856 Secret X-ray images X_j $(j = 1, 2, \ldots, 5856)$ of varying sizes, all in JPEG format

Output: 5856 stego-crypto images S_j $(j = 1, 2, \ldots, 5856)$ as noisy images in PNG format

Step 1: Load a white cover image C. Find the edges towards the noisy region and save them into array variables `row` and `column`. Initialize `count` $\leftarrow 0$.
Step 2: Load an X-ray image X from the dataset of 5856 X-ray images. Convert X into a 1-D array **h**. Increment `count` $\leftarrow$ `count` $+ 1$.
Step 3: Load a noisy cover image C. Divide it into Red, Green, and Blue (RGB) components: **tr**, **tg**, and **tb**.
Step 4: Find the edge by using one pixel position across `row` $\times$ `column`. Hide a group of elements of **h** into the edges towards the same rows of **tr** components on the left side, then continue the same for **tg** and **tb** on the right side.
Step 5: Implement five layers of cryptography:
(a) Initial Permutation (IP): Use a random row-based substitution table to diffuse pixel values.
(b) Circular Right Shift (CRC): Divide into left half and right half, then perform CRC by four columns on these halves.
(c) XOR: Create the new left half by XORing the previous left and right half, while the new right half is the old left half.
(d) Even-Odd Interchange: Interchange even columns of the image with the odd columns to introduce confusion [43].
(e) Final Permutation (FP): Perform the substitution using the reverse of the IP table.
Step 6: The final image generated is a stego-crypto image S.
Step 7: If `count` < 5856, go to Step 2.
Step 8: End.

Layer 5: Final Permutation *(FP)*: Here the same *IP* table of layer *1* is used again as a substitution table. The working of this process can be better understood with the help of Figure 9.

The above hybrid of steganography and cryptography will generate crypto-stego images which can be saved on insecure storage or transmitted over insecure communication channels. A few of these crypto-stego images are shown in Figure 10. These crypto-stego images are applied with the reverse of HM to retrieve back the *X-ray* images.

IV. EXPERIMENTAL RESULTS

The experiment results were achieved using Matlab*R2021a* programming language on *12*th Gen Intel Core *i 7*, *2.30 GHz*, *RAM 16.0 GB*, and Windows *11*. Table 3 shows cover images with the same *X-ray* images as the secret image, the output of implementing the *HM*, and the extracted *X-ray* image.

A. ASSUMPTIONS

All six cover images are coloured in *JPEG* format. Their dimensions are increased to *1080* × *1080* × *3* using the online photo-editing tool Pixlr [41]. Each cover image has more region of interest in the vertical direction, this condition is necessary for smooth implementation of *HM* (Thus, the area of the cover image should be lengthier towards the y-axis than the x-axis.). On changing the cover image dimensions *HM*, the secret *X-ray* image in some cases, is not properly hidden or will result in secret image quality loss. X-ray images are used for medical emergencies thus loss in the quality of X-ray images would render them useless for medical diagnosis. After testing it was found that changing the dimensions of the cover image decreases its embedding capacity significantly while the dimensions *1080* × *1080* × *3* is an optimal choice for the cover image. Two sets of cover images are created one on a white background and the other on a noisy background.

The *5856* secret *X-ray* images are downloaded from Mendeley [38] and are all in *JPEG* format. Before embedding if their size is greater than (*500* × *NAN*) (NAN is used to show that only one dimension is considered) then they are normalized to the same and are applied with *HM*. At a time only one X-ray image is hidden in the cover image. In case the number of input *X-ray* images is increased beyond *5856*. Then the total time which was earlier in minutes could increase to a few more minutes or even an hour as per the increase in count. The largest dimension of *X-ray* image is *1408* × *1304* if it is also increased then during *EBS* the dimensions would be normalized. The *HM* will work properly for both cases and yield results appropriately.

B. COMPUTATIONAL TIME

The computational time of *HM* measures the time-based complexity of the algorithm. In Table 4 average encryption and decryption time for *5856 X-ray* is tabulated for all *6* cover images.

1) ENCRYPTION TIME (ET)

ET is the time taken to implement *HM*. Thus, time taken to generate crypto-stego images.

2) DECRYPTION TIME (DT)

DT is the time taken to retrieve back the secret *X-ray* image from the cover image or reversing *HM*.

The maximum(Max.), minimum (Min.), average(Avg.), and total *ET* and *DT* have been mentioned in Table 4. Table 4 it can be concluded that for cover image *1* the least amount of time is taken to perform *HM* encryption and decryption.

Table 4 it can be deduced that image *1* has significantly reduced encryption and decryption time. Thus, the time-based complexity for cover image *1* is less than the

FIGURE 10. **Crypto-stego images after hybrid method (HM).**

remaining *5* cover images. Table 5 compares [1], [3], [17], [29], [34], [35], [36] with *HM* based on average values.

It is to be noted that all papers cited in Table 5 have mentioned average time. The average value of the cited papers is compared with the minimum average value of HM achieved for all *6* cover images. In Table 5 the computational time *ET* and *DT* are mentioned in seconds(sec). The average *ET* for *HM* is *0.37* sec while the *DT* is *3.9275* sec which is good. The *HM* retrieved back the *X-ray* image and that too in the original dimensions. As *HM* was able to reduce the time taken. Thus, *HM* can be implemented for securing *EMI* in real-time through real-time applications on the Internet. *EMI* which will be accessed in case of medical emergencies will retain their image quality and would result in correct diagnosis.

C. SIZE COMPARISON

In this research work, a size-based comparison of the before and after implementation of *HM*. The *5856* images had a size of *1236482806*. These images are then applied with *HM* and saved in *PNG* format. The size achieved has been tabulated in Table 6.

V. PERFORMANCE EVALUATION TESTS

Various performance evaluation tests such as Mean square error *(MSE)*, Peak signal to noise ratio *(PSNR)*, Structural similarity index metrics*(SSIM)*, Signal to noise ratio *(SNR)*, Number of pixel change rate *(NPCR)*, Unified average changing intensity *(UACI)*, Root mean square error *(RMSE)*, Embedding rate *(ER)*, Pearson correlation *(R)*, Kullback-leibler divergence *(KLD)*, Bit error rate *(BER)*, Entropy *(E)*, Mean absolute percentage error *(MAPE)*, Percentage residual difference *(PRD)*, and Co-efficient of variation *(CV)* are tested out for the validation of the *HM*. These tests have been discussed in this section along with their attained values.

A. MEAN SQUARE ERROR (MSE)

$$MSE = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{c_1(i,j) - c_2(i,j)}{m \times n} \tag{1}$$

In (1), (2), (3), (4), (5), (6), (7), (8), (9), (10), (11), (13), (14), (15), (16), (17) here *c1* is the original *X-ray* image while *c2* is the extracted *X-ray* image, L is $M \times N$ where M and N in (8) are the dimensions of the *X-ray* image. Thus, in (11), (13) L is the total number of pixels in *X-ray* image. In (2) max is the highest possible pixel value in the original image. In (3), (9) μ_x, μ_y are the averages of the decipher and original *X-ray* image, while σ_x, σ_y measure the variance in the deciphered and original images. In (12) *P(ci)* represent the probability. (1) to (17) are used using *HM* method taking *6* cover images for various performance test which are plotted in Figure 11, Figure 12, Figure 13, Figure 14, Figure 15, Figure 16, Figure 17, Figure 18, Figure 19, Figure 20, Figure 21, Figure 22, Figure 23, Figure 24, Figure 25 below.

Figure 11 below shows the *MSE* value for the *6* cover images. While Table 7 compares the *MSE* values of *HM* with [3], [17], and [33]. Table 7 compares the original and extracted *X-ray* images one at a time for a set of *5856* X-ray images for *HM*. Achieving *UACI* value is *7.43E-10*, *NPCR* is *95.59*, Entropy is *7.84*, *MSE* is *5.6E-09*, *PSNR* is *SSIM* is *0.9999*, and *R* is *1*. This paper compares the retrieved with its original while cited papers have compared the stego-image with the cover image to achieve *UACI* and *NPCR* test values.

TABLE 3. X-ray images with 6 cover images before and after implementing HM.

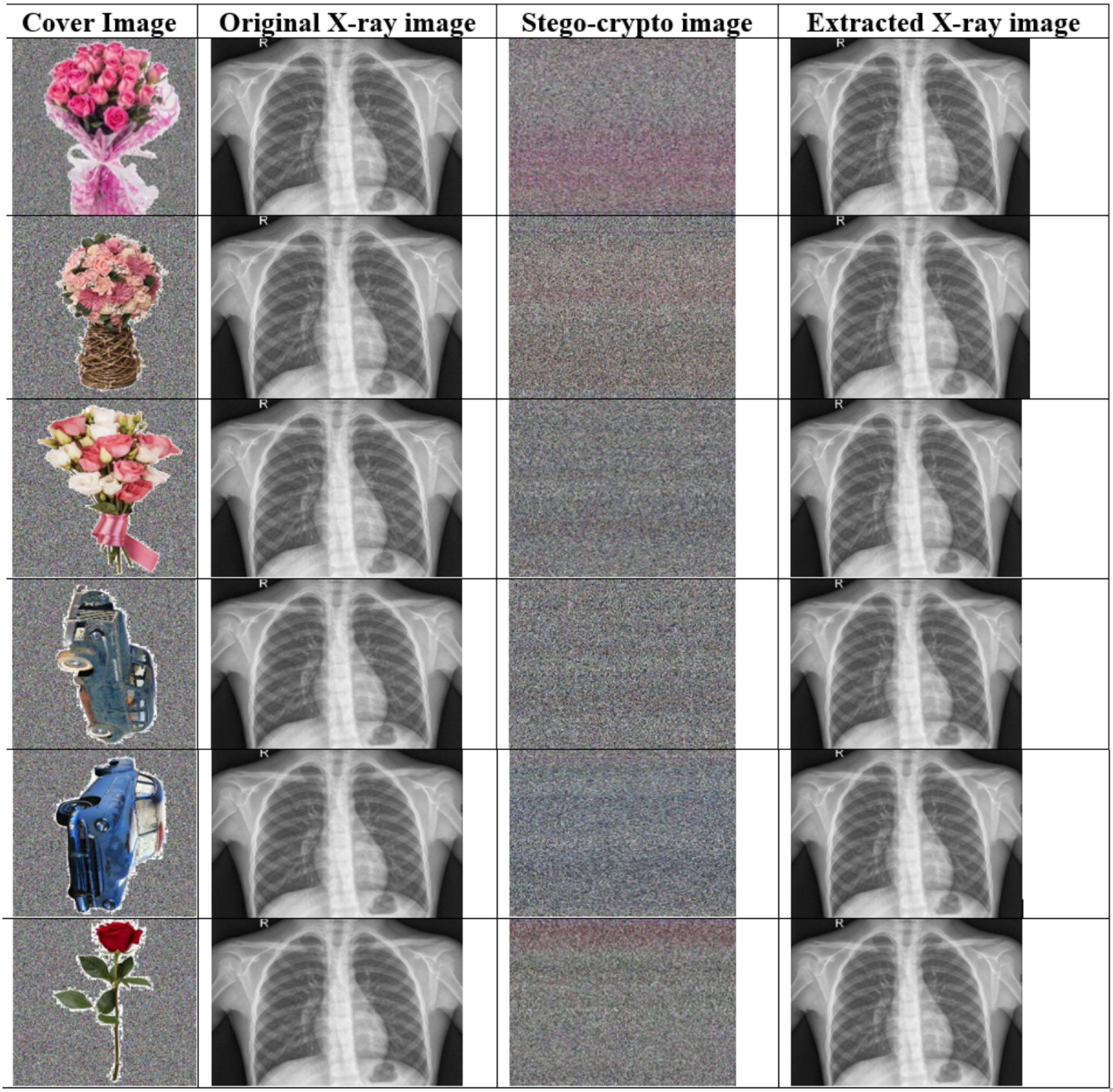

TABLE 4. Computational time comparison achieved after implementing hm on 6 cover images.

Cover Image	Encryption Time (ET)				Decryption Time (DT)			
	Total Time	Max. Time	Min. Time	Avg. Time	Total Time	Max. Time	Min. Time	Avg. Time
Image 1	2.0514 Min	0.074 Sec	0.0117 Sec	0.021 Sec	4.3094 Min	0.1095 Sec	0.0142 Sec	0.044 Sec
Image 2	18.735 Min	1.3815 Sec	0.1712 Sec	0.192 Sec	9.1995 Hrs	6.069 Sec	1.649 Sec	5.656 Sec
Image 3	56.57 Min	1.445 Sec	0.1783 Sec	0.58 Sec	9.456 Hrs	6.047 Sec	1.667 Sec	5.81 Sec
Image 4	27.293 Min	2.136 Sec	0.1759 Sec	0.279 Sec	4.004 Hrs	6.08 Sec	1.681 Sec	2.461 Sec
Image 5	49.976 Min	1.359 Sec	0.1804 Sec	0.512 Sec	7.929 Hrs	12.04min	1.693 Sec	4.874 Sec
Image 6	1.028 Hrs	2.065 Sec	0.181 Sec	0.632 Sec	7.681 Hrs	6.03 Sec	1.66 Sec	4.72 Sec

MSE value is achieved by comparing the original *X-ray* with the extracted *X-ray* image. Here extraction means reversing five layers of cryptography and then reversing *EBS*. Lower *MSE* value is preferred. Image *5* has the lowest *MSE* value of *5.6E-09* as depicted in Figure 11 below. As [3] had achieved the preferred value for *HM MSE* value is *5.6E-0.9* is also great. *MSE* indicates that retrieved and original X-ray images are the same.

TABLE 5. Computational time-based comparison with cited work.

Cited As	HM	[1]	[29]	[34]	[3]	[17]	[35]	[36]
Computational Time	**ET=0.37sec, DT=3.9275sec**	ET=17.196 sec, DT=2.177 sec	ET and DT = 2.2468sec	ET=0.7316sec, 0.5575sec	ET=0.0327 sec	ET=8.35 sec, DT=10.03sec	ET=0.492sec, DT=0.592 sec	CPU time=1.735sec

TABLE 6. Size comparison of data set of 5856 X-ray images after implementing HM.

IMAGE NO	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	IMAGE 6
TOTAL SIZE AFTER HM	16822655443	20532948837	20532546307	20532726089	20532855647	20531904400

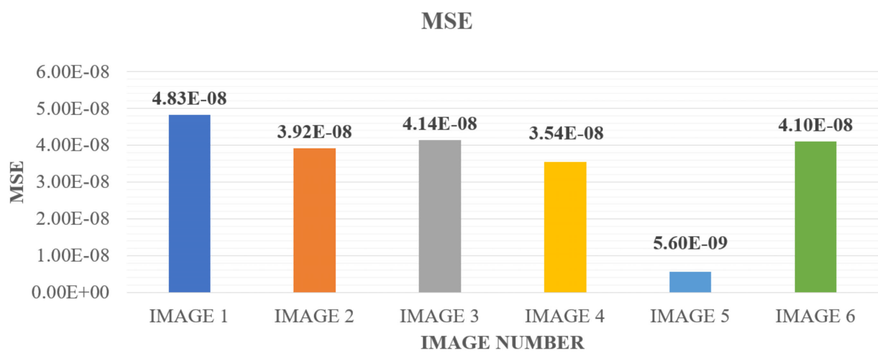

FIGURE 11. Minimum MSE value plot for 6 cover images using HM.

TABLE 7. , NPCR E, MSE, PSNR, SSIM, and R values comparison with the cited paper.

Cited As	UACI	NPCR	ENTROPY	MSE	PSNR	SSIM	R
HM	**7.43E-10**	**95.58653**	**7.8398**	**5.60E-09**	**82.51967**	**0.999995**	**1**
[2]	0.3329	0.9987	7.846	739.098	5.72	-	0.0198
[30]	-	-	-	-	47.8	0.92	-
[33]	-	-	-	0.043	49.108	-	-
[29]	33.31	99.62	7.92	-	7.98	0.00462	0.0357
[34]	33.43	99.61	-	-	-	-	-
[3]	33.5727	99.5989	7.9974	0	7.4232		0.99906
[17]	33.124	99.618	7.94	13743	26.7	0.0067	0.02392
[35]	0.3337	0.9962	7.9974	-	-	-	0.002778
[4]	33.4681	99.6143	7.9994	-	-	-	0.0011
[36]	33.55	99.63	7.9989	-	9.33	0.0026	0.03097
[37]	-	-	-	-	38.98	-	0.996
[24]	–	–	–	0.001992	75.1375	-	-
[13]	33.5688	99.8069	7.9993	7.927483	39.948	0.9273	0
[7]	-	-	-	NA	76.909	-	-

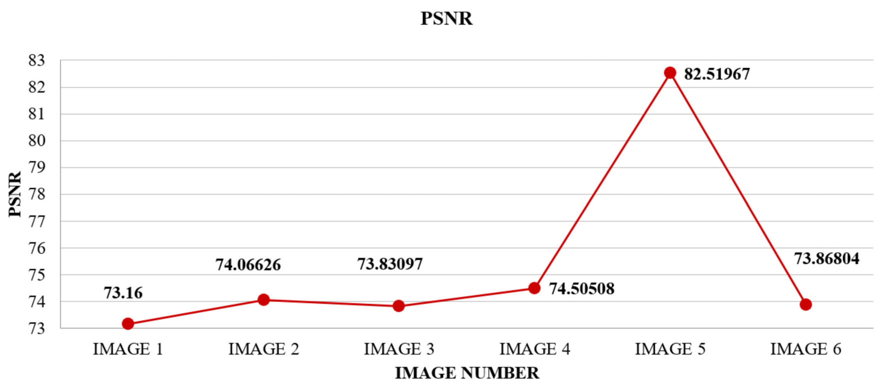

FIGURE 12. Maximum PSNR value plot for 6 cover images.

B. PEAK SIGNAL TO NOISE RATIO (PSNR)

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

Figure 12 below plots the comparisons of *6* cover images for *HM*. Table 7 and Table 8 depicts the statistical test values of *HM* and compares them with cited work [3], [17], [29], [33], [36]. A high value of *PSNR* is preferred [29].

TABLE 8. MAE, PRD, CR, SNR, RMSE, BER, KLD, FSIM, and Cv comparison of the HM with cited literature.

Cited As	MAE	PRD	CR	SNR	RMSE	BER	KLD	FSIM	Cv
HM	**1.89E-07**	**2.42E-05**	**0.995064**	**0.049221**	**7.48E-05**	**9.66E-06**	**-8.80E-06**	**-**	**690636.3**
[33]	0.0041 +- 0.001 (%)	0.164425	3.87 (for PPG) to 5.07 (for Holter)	31.83 to 46.37	0.2074	0.005	0.002	–	–
[29]	-	-	-	-	-	-	-	0.33532	-
[36]	-	-	-	-	-	-	-	0.4105	-
[7]	0.1985	0.3009	-	63.974	0.3341	-	-	-	-

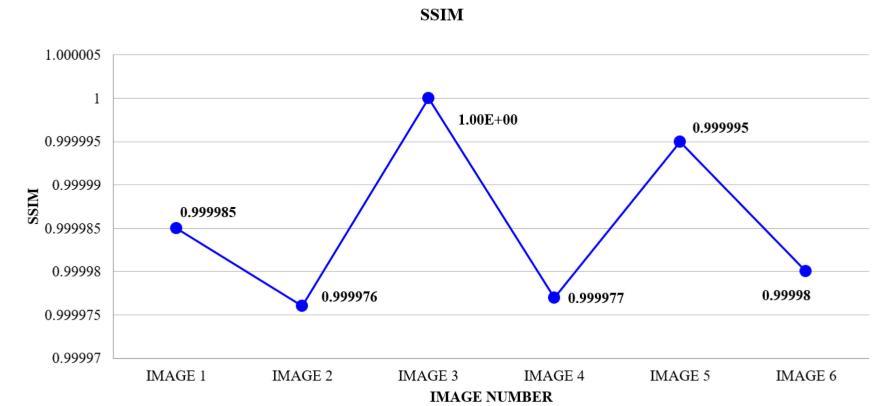

FIGURE 13. 6 cover images SSIM value plot.

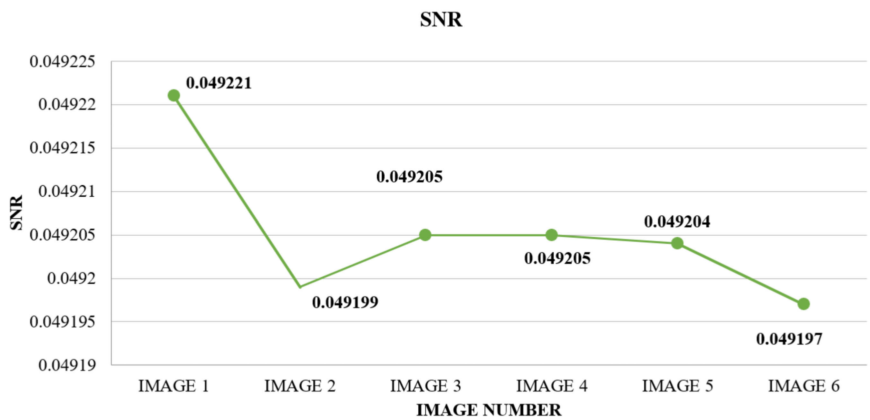

FIGURE 14. SNR value comparison for the 6 cover images for the same data set.

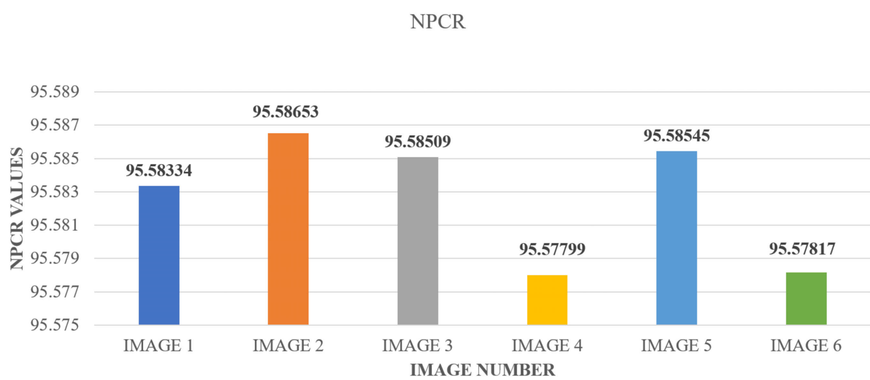

FIGURE 15. Maximum NPCR value for 6 cover images.

As per Figure 12 depicts the cover image *5* has good *PSNR* value of *82.51967* dB. Table 7 the *HM* has better *PSNR* value of *82.52*. Hence the retrieved X-ray image has some noise added to it but is far better when compared to other cited works. In [3], [29], and [36] the *PSNR* value is achieved by comparing the stego-image with the cover image.

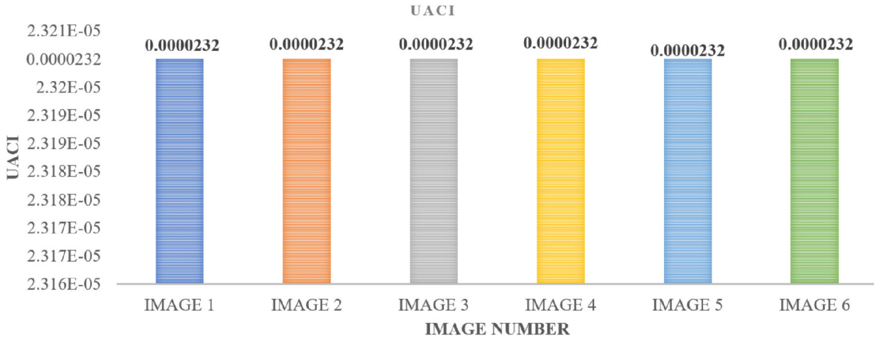

FIGURE 16. UACI value comparison for 6 cover images.

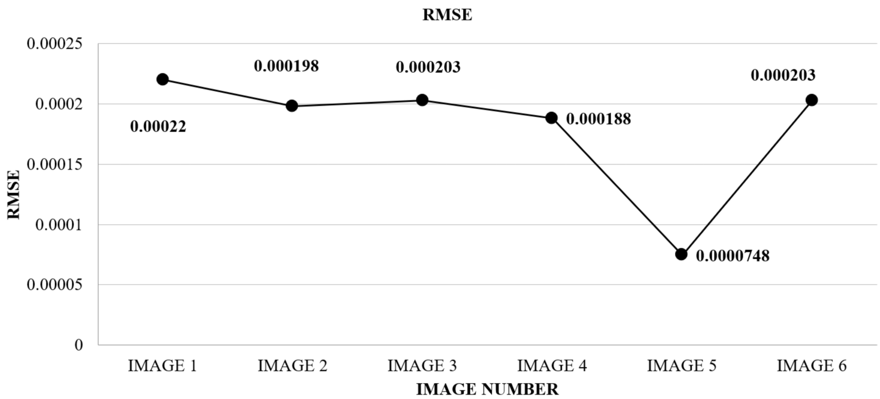

FIGURE 17. RMSE value comparison for the 6 cover images on the same data set.

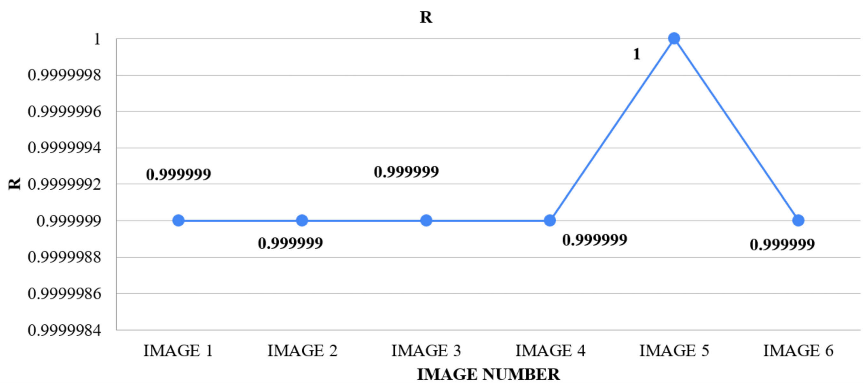

FIGURE 18. R values comparison for the 6 cover images for the same data set.

C. STRUCTURAL SIMILARITY INDEX MATRIX (SSIM)

$$SSIM\ (x, y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2\mu_y^2 + c_2\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{3}$$

Figure 13 plots *SSIM* of *6* cover images for *HM* which are all close to preferred value of 1. Figure 13 shows that image *3* has the best *SSIM* value of *1*. Table 7 it can be deduce that *HM* achieved better *SSIM* value than [17], [29], and [36].

D. SIGNAL TO NOISE RATIO (SNR)

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^{L} (c_1\ (i) - c_2\ (i))^2}{\sum_{i=1}^{L} \left(c_1\ (i)^2\right)} \tag{4}$$

Figure 14 depicts the minimum *SNR* values of *6* cover images after implementing *HM*. Here cover image *6* achieved the best value. Table 8 compares test values for various tests such as *BER, MAPE, RMSE, SNR, PRD, CR, FSIM, KLD,* and *Cv*.

Table 8 *SNR* value of 0.0492 indicates negligible addition of noise in the retrieved X-ray image compared [7], [33].

E. NUMBER OF PIXEL CHANGE RATE (NPCR)

$$d\ (i, j) = \begin{cases} 0 & c_1\ (i, j) = c_2\ (i, j) \\ 1 & otherwise \end{cases} \tag{5}$$

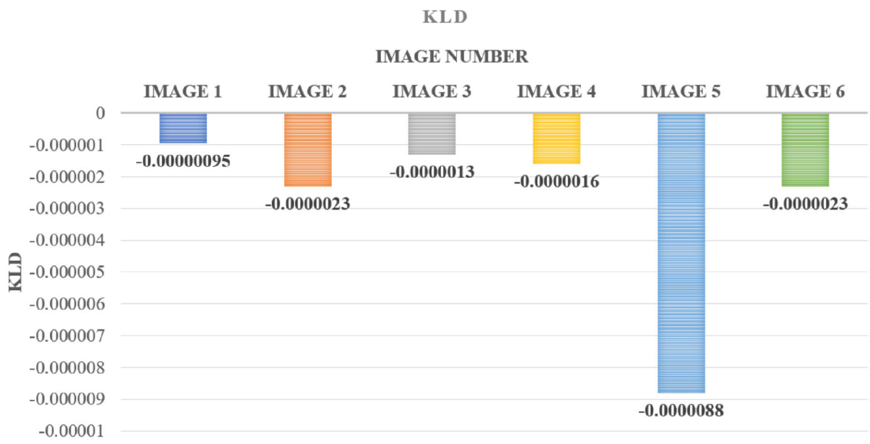

FIGURE 19. KLD value comparison for the 6 cover images for the same data set.

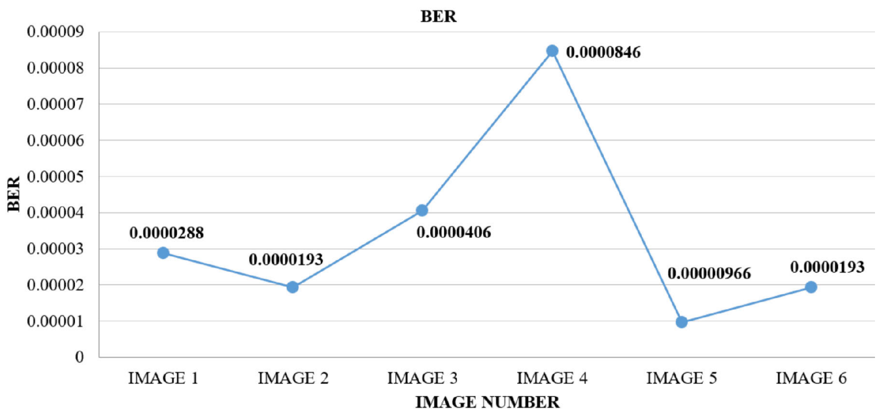

FIGURE 20. BER values for the 6 cover images.

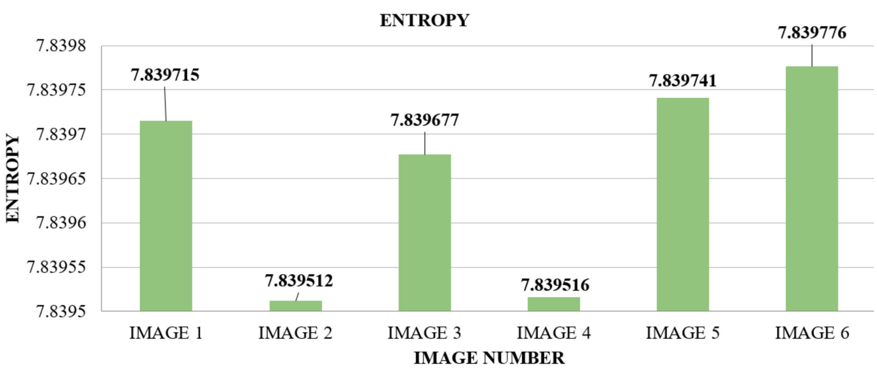

FIGURE 21. Entropy values comparison for the 6 cover images for the same data set.

$$NPCR = \frac{\sum_{(i,j)} D(i,j)}{m \times n} \times 100 \tag{6}$$

Figure 15 shows *NPCR* values of *6* cover images achieved after implementing *HM*. Table 7 tabulates *NPCR* values for *HM* compared with [3], [4], [17], [29], [34], [35], and [36].

Preferred value of *NPCR* which is greater than *99 %*. *HM* achieved a value close to 95.5.

F. UNIFIED AVERAGE CHANGING INTENSITY (UACI)

$$UACI = \frac{1}{m \times n}\left(\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right) \times 100 \tag{7}$$

In Figure 16 plots *UACI* values achieved after implementing *HM* on *6* cover images. Table 7 quotes *UACI* values for the cited work [3], [4], [17], [29], [34], [35], [36] where able to achieve preferred value of *33*.

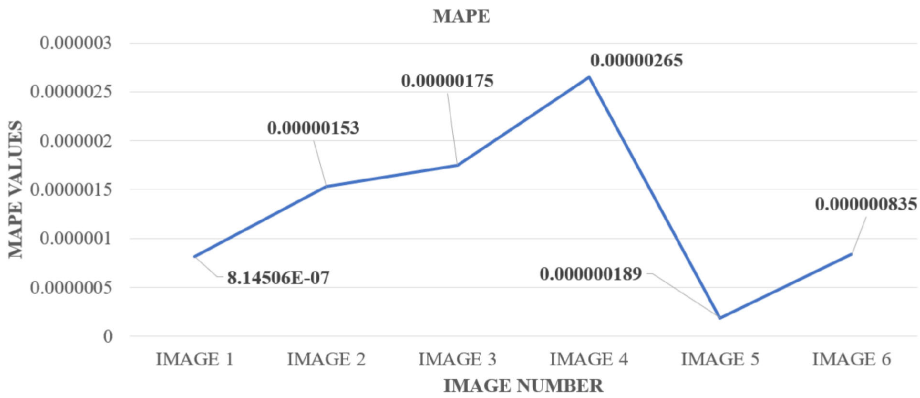

FIGURE 22. MAPE value for 6 cover images.

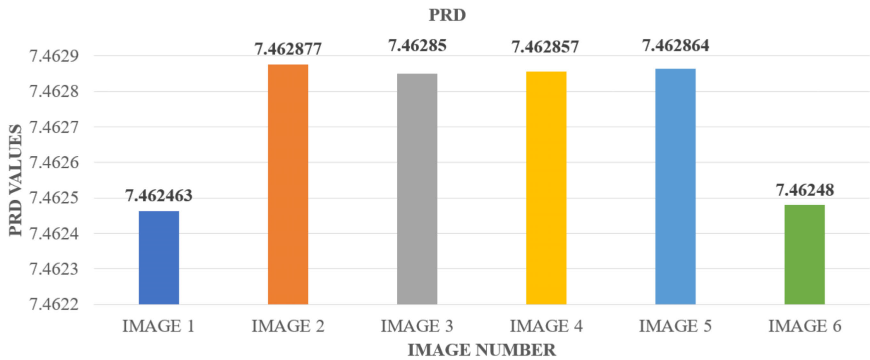

FIGURE 23. PRD values for the 6 cover images.

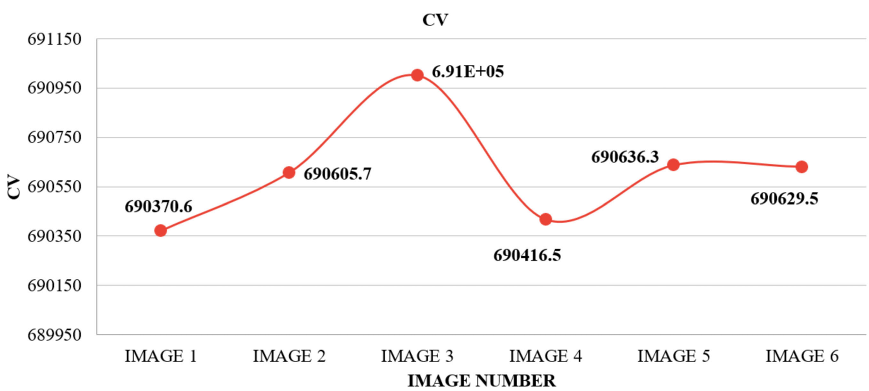

FIGURE 24. CV value comparison for the 6 cover images.

G. ROOT MEAN SQUARE ERROR (RMSE)

$$RMSE = \sqrt{MSE} \tag{8}$$

RMSE value of *7.48E-05* was achieved in Table 8.

H. PEARSON CORRELATION (R)

$$R\left(A_c, R_e\right) = \frac{Cov\left(A_c, R_e\right)}{\sigma_{Ac}\sigma_{Re}} \tag{9}$$

Figure 18 plots *R* values for *HM* method for *6* cover images. Table 7 compares *HM* with the cited work [3], [4], [17], [29], [35], [36], [37] for *R* values.

I. KULLBACK-LEIBLER DIVERGENCE (KLD)

$$KLD = \int c_2\left(x\right) \log \frac{c_1\left(x\right)}{c_2\left(x\right)} \tag{10}$$

Figure 19 *KLD* values for the *6* cover images for *HM*. Table 8 *KLD* values are compared with [33].

J. BIT ERROR RATE (BER)

$$BER = \frac{\sum_i c_1 \bigotimes c_2}{L} \tag{11}$$

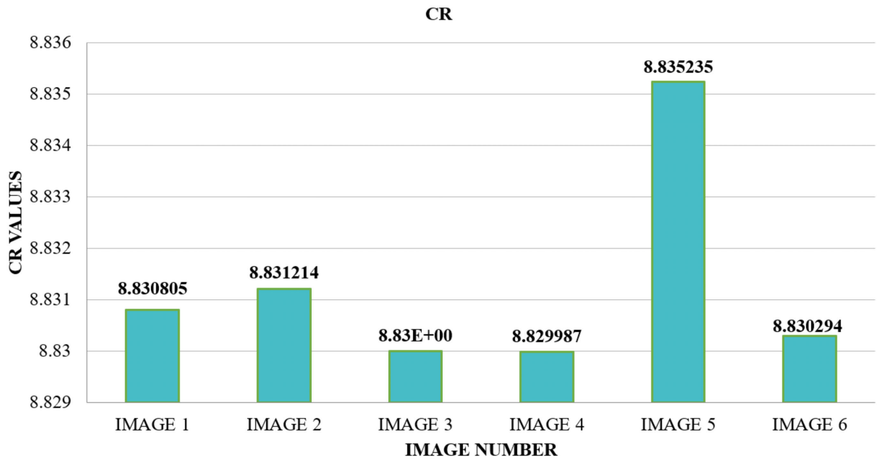

FIGURE 25. CR values comparison for the 6 cover images.

TABLE 9. The minimum value achieved for HM on a data set of 5856 x-ray images while dealing with 6 cover images.

	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	IMAGE 6
MAE	8.15E-07	1.53E-06	1.75E-06	2.65E-06	1.89E-07	8.35E-07
PRD	6.37E-05	0.000104	3.47E-05	9.55E-05	2.42E-05	6.83E-05
CR	0.995064	0.995908	9.96E-01	0.995469	0.996006	0.995848
UACI	3.19E-09	5.99E-09	6.86E-09	1.04E-08	7.43E-10	3.27E-09
NPCR	0.002876	0.001933	4.06E-03	0.008456	0.000966	0.001933
ENTROPY	5.998852	5.999485	6.00E+00	5.99936	5.999273	5.998842
MSE	4.83E-08	3.92E-08	4.14E-08	3.54E-08	5.60E-09	4.10E-08
PSNR	24.79774	24.79901	2.48E+01	24.80275	24.80128	24.86517
SSIM	0.46264	0.462676	4.63E-01	0.462711	0.462646	0.462908
CV	895.2732	895.2804	8.95E+02	895.3043	894.5772	895.2712
R	0.976849	0.977266	9.77E-01	0.977097	0.977266	0.977476
SNR	-0.01595	-0.01632	-1.45E-02	-0.01659	-0.01738	-0.01655
RMSE	0.00022	0.000198	2.03E-04	0.000188	7.48E-05	0.000203
BER	2.88E-05	1.93E-05	4.06E-05	8.46E-05	9.66E-06	1.93E-05
KLD	-9.50E-07	-2.30E-06	-1.30E-06	-1.60E-06	-8.80E-06	-2.30E-06

TABLE 10. One of the maximum value achieved after implementing HM on data set of 5856 X-ray images for 6 cover images.

	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	IMAGE 6
MAE	0.04072	0.04072	0.04070	0.04072	0.04072	0.04067
PRD	7.46246	7.46288	7.46285	7.46286	7.46286	7.46248
CR	8.83081	8.83121	8.83000	8.82999	8.83524	8.83029
UACI	0.00016	0.00016	0.00016	0.00016	0.00016	0.00016
NPCR	95.5833	95.5865	95.60000	95.578	95.5855	95.5782
ENTROPY	7.83972	7.83951	7.84000	7.83952	7.83974	7.83978
MSE	0.00331	0.00331	0.00331	0.00331	0.00331	0.00326
PSNR	73.16	74.0663	73.80000	74.5051	82.5197	73.868
SSIM	0.99999	0.99998	1.00000	0.99998	1	0.99998
CV	690371	690606	691000	690417	690636	690630
R	1	1	1.00000	1	1	1
SNR	0.04922	0.0492	0.04920	0.04921	0.0492	0.0492
RMSE	0.05756	0.05755	0.05760	0.05753	0.05754	0.05711
BER	0.95583	0.95587	0.95600	0.95578	0.95586	0.95578
KLD	0.00026	0.00068	0.00026	0.00026	0.00068	0.00068

Table 8 shows that good result values were achieved for *BER*. While Figure 20 diagrammatically compares the result for *6* cover images.

K. ENTROPY (E)

$$E = -\sum_{i=1}^{n} P(c_i)\log_2 P(c_i) \tag{12}$$

In table 7 it can seen that *HM* achieved Entropy [44] value of 7.839. The best value for Entropy is close to 8 [2], [3], [4], [13], [17]. The 6 cover images comparative plot is shown in Figure 21.

L. MEAN ABSOLUTE PERCENTAGE ERROR (MAPE)

$$MAPE = \frac{1}{L}\sum_{i=1}^{L}\left(\frac{|c_1(i) - c_2(i)|}{c_i(i)}\right)100 \tag{13}$$

Figure 22 plots the *MAPE* values for the *6* cover images. Table 8 compares *HM* value with the cited work.

TABLE 11. Average values achieved after implementing HM one at a time on data set of 5856 secret X-ray images with 6 cover images.

	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	IMAGE 6
MAE	0.005914	0.005911	5.91E-03	0.005912	0.005911	0.005913
PRD	1.103065	1.102729	1.102986	1.102887	1.102763	1.102936
CR	1.945501	1.945428	1.95E+00	1.945486	1.945492	1.945492
UACI	2.32E-05	2.32E-05	2.32E-05	2.32E-05	2.32E-05	2.32E-05
NPCR	55.02185	55.0025	5.50E+01	55.00544	55.00285	55.00914
ENTROPY	7.282467	7.282502	7.28E+00	7.282506	7.282483	7.282518
MSE	0.000209	0.000208	2.09E-04	0.000209	0.00021	0.000209
PSNR	38.20109	38.1734	3.82E+01	38.1853	38.2452	38.17775
SSIM	0.945764	0.945788	9.46E-01	0.945775	0.945785	0.94577
CV	78295.71	78291.68	7.83E+04	78291.61	78291.71	78291.41
R	0.997956	0.997963	9.98E-01	0.997954	0.997958	0.997955
SNR	0.005469	0.00546	5.47E-03	0.005469	0.005466	0.005468
RMSE	0.013503	0.013488	1.35E-02	0.013509	0.013491	0.013513
BER	0.550218	0.550025	5.50E-01	0.550054	0.550029	0.550091
KLD	7.65E-05	6.96E-05	4.93E-05	4.68E-05	5.78E-05	0.000115

M. PERCENTAGE RESIDUAL DIFFERENCE (PRD)

$$PRD = \sqrt{\frac{\sum_{i=1}^{n} \left(c_2\left(i\right) - c_2\left(i\right)\right)^2}{\sum_{i=1}^{L} \left(c_1\left(i\right)\right)^2}} \times 100 \tag{14}$$

PRD is plotted in Figure 23 while its value is tabulated in Table 8.

N. COEFFICIENT OF VARIATION (CV)

$$std = \sqrt{\frac{\sum \left(A_c - \mu\right)}{n}} \tag{15}$$

$$mean = \frac{\sum A_c}{n} \tag{16}$$

$$CV = \frac{std(img)}{mean(img)} \tag{17}$$

Table 8 indicates a good value for *CV* test. In case the number of input *X-ray* images are increased beyond *5856*. Then total time which was in minutes could increase to a few more minutes or even an hour as per the increase in count. The largest dimension of *X-ray* image is 1408×1304 if it is also increased then during *EBS* its dimensions would be normalized. The *HM* will work properly for both cases and yield results appropriately. The results achieved for *6* cover images based on their minimum, maximum, and average performance test values are shown in Table 9, Table 10, and Table 11.

VI. CONCLUSION AND FUTURE SCOPE

HM enhanced the security and privacy of *EMI* on storage or while being transmitted on an insecure transmission channel from hackers and attacks. *HM* is reversible as all the *5856 X-ray images* were retrieved back. *HM*, combines edge-based steganography, with five layers of cryptography. Therefore, HM has properties of both steganography and cryptography methods such as confidentiality, integrity, payload capacity, etc. Confusion and diffusion properties of cryptography have enhanced the security of *HM*. *HM* took an average encryption time of *0.37* sec and a decryption time of *3.9275* sec. Thus, less computational time is taken to secure *EMI*. *EMI* secured using *HM* could be accessed in real-time through *RTA*. *HM* can be used in future by hospitals for real-time security of *EMI* while storing them on third-party cloud storage or while being communicated.

Further, *HM* achieves better value for standard performance tests such as *PSNR, SNR, SSIM, R, PRD, RMSE*, Entropy, *MAPE*, etc. Hence, enhancing the security and privacy of *EMI*. These tests help conclude that the secret *X-ray* images extracted after the reversal of *HM* are the same as the original X-ray images. Therefore, reliable, confidentiality, privacy, and enhanced security of *EMI*. In future, *3D* medical images can also be secured using the *HM* while incorporating it with an *AI* algorithm for edge detection which would work on all types of cover images. *3D* medical images are slices of images of the same body part from different angles which are taken to get a better diagnosis. Hence implementing *HM* could enhance their security. In future, a performance testing-based comparison study for the HM, LSB, and DWT could be implemented.

ACKNOWLEDGMENT

The authors would like to acknowledge Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R197), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Security Engineering Lab at Prince Sultan University for their support.

REFERENCES

[1] R. Adee and H. Mouratidis, "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography," *Sensors*, vol. 22, no. 3, p. 1109, Feb. 2022.

[2] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Inf. Secur. J., Global Perspective*, vol. 29, no. 2, pp. 91–101, Mar. 2020.

[3] M. Kumar and P. Gupta, "A new medical image encryption algorithm based on the 1D logistic map associated with pseudo-random numbers," *Multimedia Tools Appl.*, vol. 80, no. 12, pp. 18941–18967, May 2021.

[4] X. Wang and Y. Wang, "Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118924.

[5] S. Aggarwal, S. Gupta, A. Alhudhaif, D. Koundal, R. Gupta, and K. Polat, "Automated COVID-19 detection in chest X-ray images using fine-tuned deep learning architectures," *Expert Syst.*, vol. 39, no. 3, Mar. 2022, Art. no. e12749.

[6] P. Malhotra, S. Gupta, D. Koundal, A. Zaguia, M. Kaur, and H.-N. Lee, "Deep learning-based computer-aided pneumothorax detection using chest X-ray images," *Sensors*, vol. 22, no. 6, p. 2278, Mar. 2022.

[7] S. Banerjee and G. K. Singh, "A new approach of ECG steganography and prediction using deep learning," *Biomed. Signal Process. Control*, vol. 64, Feb. 2021, Art. no. 102151.
[8] N. Soni, I. Saini, and B. Singh, "An integer wavelet transform and pixel value differencing based feature specific hybrid technique for 2D ECG steganography with high payload capacity," *Multimedia Tools Appl.*, vol. 80, no. 6, pp. 8505–8540, Mar. 2021.
[9] D. Sharma, C. Prabha, A. Goyal, M. Malik, and R. Kumar, "Enhanced security of EMI using an edge-based steganography with four-layered cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, nos. 2–8, pp. 775–784, 2024.
[10] D. Sharma and C. Prabha, "Security and privacy aspects of electronic health records: A review," in *Proc. Int. Conf. Advancement Comput. Comput. Technol. (InCACCT)*, May 2023, pp. 815–820.
[11] T. Ratheesh and V. Paul, "An effective mechanism for the secure transmission of medical images using compression and public key encryption mechanism," in *Proc. 4th Int. Conf. Smart Comput. Informat. Smart Comput. Techn. Appl.*, vol. 2. Cham, Switzerland: Springer, 2021, pp. 317–325.
[12] C. Gong, J. Zhang, Y. Yang, X. Yi, X. Zhao, and Y. Ma, "Detecting fingerprints of audio steganography software," *Forensic Sci. Int., Rep.*, vol. 2, Dec. 2020, Art. no. 100075.
[13] M. Yildirim, "Steganography-based voice hiding in medical images of COVID-19 patients," *Nonlinear Dyn.*, vol. 105, no. 3, pp. 2677–2692, Aug. 2021.
[14] A. Kore and S. Patil, "Cross layered cryptography based secure routing for IoT-enabled smart healthcare system," *Wireless Netw.*, vol. 28, no. 1, pp. 287–301, Jan. 2022.
[15] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.
[16] N. A. N. Adnan and S. Ariffin, "Big data security in the web-based cloud storage system using 3D-AES block cipher cryptography algorithm," in *Proc. Int. Conf. Soft Comput. Data Sci.*, Bangkok, Thailand. Cham, Switzerland: Springer, Aug. 2018, pp. 309–321.
[17] M. M. Elamir, W. I. Al-atabany, and M. S. Mabrouk, "Hybrid image encryption scheme for secure E-health systems," *Netw. Model. Anal. Health Informat. Bioinf.*, vol. 10, no. 1, p. 35, Dec. 2021.
[18] A. Saxena, D. Misra, R. Ganesamoorthy, J. L. Arias Gonzales, H. A. Almashaqbeh, and V. Tripathi, "Artificial intelligence wireless network data security system for medical records using cryptography management," in *Proc. 2nd Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, Apr. 2022, pp. 2555–2559.
[19] M. A. Nasr, W. El-Shafai, N. Abdel-Salam, E.-S.-M. El-Rabaie, A. S. El-Fishawy, and F. E. A. El-Samie, "Efficient information hiding in medical optical images based on piecewise linear chaotic maps," *J. Opt.*, vol. 52, no. 4, pp. 1852–1866, Dec. 2023.
[20] W. Al-Chaab, Z. A. Abduljabbar, E. W. Abood, V. O. Nyangaresi, H. M. Mohammed, and J. Ma, "Secure and low-complexity medical image exchange based on compressive sensing and LSB audio steganography," *Informatica*, vol. 47, no. 6, pp. 65–74, May 2023.
[21] Z. Zhang, N. Zhou, B. Sun, S. Banerjee, and J. Mou, "Multimedia healthcare cloud personal archives security system based on compressed sensing and multi-image encryption," *J. Franklin Inst.*, vol. 361, no. 8, May 2024, Art. no. 106844.
[22] M. Y. Shakor, N. M. S. Surameery, and Z. N. Khlaif, "Hybrid security model for medical image protection in cloud," *Diyala J. Eng. Sci.*, vol. 16, pp. 68–77, Mar. 2023.
[23] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 50, no. 1, pp. 73–80, Jan. 2020.
[24] R. Mothi and M. Karthikeyan, "Protection of bio medical Iris image using watermarking and cryptography with WPT," *Measurement*, vol. 136, pp. 67–73, Mar. 2019.
[25] F. Castro, D. Impedovo, and G. Pirlo, "A medical image encryption scheme for secure fingerprint-based authenticated transmission," *Appl. Sci.*, vol. 13, no. 10, p. 6099, May 2023.
[26] D. Sharma and C. Prabha, "Hybrid security of EMI using edge-based steganography and three-layered cryptography," in *Applied Data Science and Smart Systems*, 1st ed., J. Singh, S. Goyal, R. K. Kaushal, N. Kumar, and S. S. Sehra, Eds., London, U.K.: CRC Press, Jul. 2024, pp. 278–290.
[27] D. Sharma, C. Prabha, D. Gupta, S. Juneja, M. Abd-Elnaby, F. Alraddady, and A. Nauman, "Securing X-ray images in no interest region (NIR) of the normalized cover image by edge steganography," *IEEE Access*, early access, Sep. 24, 2024, doi: 10.1109/ACCESS.2024.3467167.
[28] R. L. R. Maata, R. S. Cordova, and A. Halibas, "Performance analysis of twofish cryptography algorithm in big data," in *Proc. 9th Int. Conf. Softw. Inf. Eng. (ICSIE)*, vol. 3, Nov. 2020, pp. 56–60.
[29] W. El-Shafai, F. Khallaf, E.-S.-M. El-Rabaie, and F. E. A. El-Samie, "Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications," *Neural Comput. Appl.*, vol. 34, no. 13, pp. 10629–10653, Jul. 2022.
[30] W. A. Awadh, A. S. Alasady, and A. K. Hamoud, "Hybrid information security system via combination of compression, cryptography, and image steganography," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 12, no. 6, p. 6574, Dec. 2022.
[31] O. F. Boyraz, E. Guleryuz, A. Akgul, M. Z. Yildiz, H. E. Kiran, and J. Ahmad, "A novel security and authentication method for infrared medical image with discrete time chaotic systems," *Optik*, vol. 267, Oct. 2022, Art. no. 169717.
[32] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Sci. Int.*, vol. 320, Mar. 2021, Art. no. 110691.
[33] G. Georgieva-Tsaneva, G. Bogdanova, and E. Gospodinova, "Mathematically based assessment of the accuracy of protection of cardiac data realized with the help of cryptography and steganography," *Mathematics*, vol. 10, no. 3, p. 390, Jan. 2022.
[34] L. M. H. Yepdia and A. Tiedeu, "Secure transmission of medical image for telemedicine," *Sens. Imag.*, vol. 22, no. 1, p. 17, Dec. 2021.
[35] B. Zhang, B. Rahmatullah, S. L. Wang, and Z. Liu, "A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map," *Multimedia Tools Appl.*, vol. 82, no. 10, pp. 15735–15762, Apr. 2023.
[36] W. El-Shafai, I. Almomani, A. Ara, and A. Alkhayer, "An optical-based encryption and authentication algorithm for color and grayscale medical images," *Multimedia Tools Appl.*, vol. 82, no. 15, pp. 23735–23770, Jun. 2023.
[37] A. Patra, A. Saha, and K. Bhattacharya, "Efficient storage and encryption of 32-slice CT scan images using phase grating," *Arabian J. Sci. Eng.*, vol. 48, no. 2, pp. 1757–1770, Feb. 2023.
[38] D. Kermany, K. Zhang, and M. Goldbaum, "Labeled optical coherence tomography (OCT) and chest X-ray images for classification," *Mendeley Data*, vol. 2, no. 2, p. 651, 2018.
[39] A. Ali, H. A. Rahim, J. Ali, M. F. Pasha, M. Masud, A. U. Rehman, C. Chen, and M. Baz, "A novel secure blockchain framework for accessing electronic health records using multiple certificate authority," *Appl. Sci.*, vol. 11, no. 21, p. 9999, Oct. 2021.
[40] D. Sharma and R. Kawatra, "Security techniques implementation on big data using steganography and cryptography," in *ICT Analysis and Applications*. Cham, Switzerland: Springer, 2022, pp. 279–302.
[41] *Pixlr.com/*. Accessed: Jul. 21, 2023. [Online]. Available: https://pixlr.com/
[42] N. Chidambaram, K. Thenmozhi, P. Raj, and R. Amirtharajan, "DNA-chaos governed cryptosystem for cloud-based medical image repository," *Cluster Comput.*, vol. 27, no. 4, pp. 4127–4144, Jul. 2024.
[43] K. Demla and A. Anand, "RISE: Rubik's cube and image segmentation based secure medical images encryption," *Multimedia Tools Appl.*, pp. 1–25, 2024.
[44] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm," *Artif. Intell. Rev.*, vol. 57, no. 4, p. 87, Mar. 2024.

DIVYA SHARMA is currently pursuing the Ph.D. degree in computer science and engineering with Chitkara University, Rajpura, Punjab, India. She is currently an Assistant Professor with the Department of Information Technology, PUSS-GRC, Hoshiarpur, India. Her research interests include steganography, cryptography, and multimedia data.

CHANDER PRABHA is currently with the Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India. Her area of specialization includes opportunistic networks, MANETs, data science, fog computing, SDN, and AIML. She has more than 20 years of teaching and research expertise.

MD MEHEDI HASSAN (Member, IEEE) received the B.Sc. degree in computer science and engineering from North Western University, Khulna, in 2022, and the Master of Science (M.Sc.) degree in computer science and engineering from Khulna University, Khulna, Bangladesh, in 2024. He is currently a Dedicated and Accomplished Researcher. As the Founder and the CEO of The Virtual BD IT Firm and VRD Research Laboratory, Bangladesh, he has established himself as a highly respected leader in the fields of biomedical engineering, data science, and expert systems. His research interests include important human diseases, such as oncology, cancer, and hepatitis, and human behavior analysis and mental health. He is highly skilled in association rule mining, predictive analysis, machine learning, and data analysis, with a particular focus on the biomedical sciences. As a Young Researcher, he has published 55 articles in various international top journals and conferences, which is a remarkable achievement. His work has been well-received by the research community and has significantly contributed to the advancement of knowledge in his field. Overall, he is a highly motivated and skilled researcher with a strong commitment to improving human health and well-being through cutting-edge scientific research. His accomplishments to date are impressive and his potential for future contributions to his field is very promising. Additionally, he serves as an Academic Editor of *PLOS One*, *PLOS Digital Health*, and *Discover Applied Sciences* (Springer) and a reviewer for 56 prestigious journals. He has filed more than three patents out of which three are granted to his name.

SHAHAB ABDULLA received the Ph.D. degree in computer science from the University of Southern Queensland (UniSQ). He is currently an Associate Professor with the UniSQ College, University of Southern Queensland, Toowoomba, QLD, Australia. His research interests include biomedical engineering, complex medical engineering, networked systems, intelligent control, and computer control systems.

ANUPAM KUMAR BAIRAGI (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science and engineering from Khulna University, Bangladesh, and the Ph.D. degree in computer engineering from Kyung Hee University, South Korea. He is a Professor in the discipline of Computer Science and Engineering, Khulna University. He has authored or co-authored more than 100 publications, including refereed IEEE/ACM journals, and conference papers. His research interests include wireless resource management in 5G, game theory, IIoT, health informatics, and agri informatics. He has served as a technical program committee member in different international conferences and also served as guest editor in special issues of different journals. He achieved Vice Chancellor's award 2023 for his contribution in research and academic excellence. Recently, he was also enlisted in the list of the world's top 2% scientists in 2024 published by Stanford University and Elsevier.

SAMAH ALSHATHRI received the Bachelor of Computer Science and Master of Computer Engineering degrees from King Saud University, Riyadh, Saudi Arabia, and the Ph.D. degree from the Department of Computer and Mathematics, Plymouth University, Plymouth, U.K. She is currently an Assistant Professor with the Department of Information technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University (PNU), Riyadh. Her research interests include wireless networks, cloud computing, fog computing, the IoT, data mining, machine learning, text analytics, image classification, and deep learning. She was the Chair of the Network and Communication Department and participated in organizing many international conferences. She has authored or co-authored many articles published in well-known journals in the research field.

WALID EL-SHAFAI (Senior Member, IEEE) was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the FEE, Menoufia University, in 2019. Since January 2021, he has been a Postdoctoral Research Fellow with the Security Engineering Laboratory (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently a Senior Cybersecurity Researcher with the SEL Laboratory and an Assistant Professor with the College of Computer Science and Information Systems. Also, he is an Associate Professor with the Department of Electronics and Communication Engineering (ECE), FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software-defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, malware and ransomware detection and analysis, deep learning in signal processing, and communication systems applications. He also serves as a reviewer for several international journals.