EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Blockchain Enabled Interpolation Based Reversible Data Hiding Mechanism for Protecting Records

Abhinandan Tripathi[1,*], Jay Prakash[2]

[1]Department of Information Technology & Computer Application, Madan Mohan Malaviya University of Technology, Gorakhpur, India, abhinandan2787@gmail.com
[2]Department of Information Technology & Computer Application, Madan Mohan Malaviya University of Technology, Gorakhpur, India, jpr_1998@yahoo.co.in

Abstract

A diagnosis can be made using a lot of the crucial information contained in medical snaps. Medical images have become a target for malicious attacks due to the requirement for regular communication in order to provide flexibility and accurate diagnosis. In order to protect medical images, encryption algorithms are used. Because of this, medical photos are encrypted before being transmitted; yet, this is only one layer of security. Reversible Data Hiding (RDH) techniques have recently been used to incorporate private data into medical images. This enables efficient and safe communication, and the secretly contained information—such as personal and medical records—is highly helpful for making medical diagnosis. However, the limited embedding capacity of current RDH systems continues to limit their usefulness. In this study, a Reversible Data Hiding method based on a histogram shifting and interpolation scheme is highlighted. The achievable embedding capacity (EC) for the suggested technique is one bit per pixel (bpp) for both digital and medical images. A blockchain-based system based on three keys is used to encrypt the images. The proposed blockchain mechanism is secure against outside threats. To verify the utility of the suggested strategy, the outcomes are compared to cutting-edge techniques for both digital and medical photos. Along with the hash value of the actual medicinal snaps, the private information is preserved on the blockchain. Due to this, all medical photos transmitted through the suggested blockchain network may be monitored. The experiments and analysis are shows that the proposed scheme has excellent security has attained during the entire process. It also achieved high embedding capacity, PSNR, rate and low SSIM throughout the process of data concealing.

Keywords: PSNR, SSIM, RDH, Blockchain

Received on 14 December 2022, accepted on 07 April 2023, published on 24 May 2023

doi: 10.4108/eetsis.v10i4.2934

*Corresponding author. Email: abhinandan2787@gmail.com

1. Introduction

Current era has emphasized on digitalization, since a huge amount of medicinal records are kept in the digital form and also transferred digitally from one end to another end. It is very important to keep medical health record (MHR) confidential because it has personal information related to patient's medical report & their diagnosis. Generally, MHR contains patient's personal information, their medical history, reports and their diagnosis details on the basis of their reports. Now a days, every person has used to telemedicine technology by which patients and doctor exchange their medical reports & diagnosis. One of the crucial pieces of data in MHR that reveals a significant amount of sensitive information is the medical image. This data must be safeguarded against unauthorized intrusion.

In contrast to watermarking, accurately recovering the original image is of the utmost importance [1]. It has

become increasingly important in conventional fields like the military, healthcare, and law where individuals seek the highest degree of consistency between the original image and the decrypted image. RDH allows for the recovery of embedded bits while still allowing for the accurate reconstruction of the original image. The recipient can properly restore the original cover content following data extraction when data concealment is done using a reversible technique. The majority of previous information hidingtechniques directly embeds the extra bits into the original images.

To protect MHR (including medical photos) effectively we use conventional cryptography algorithms. For illustration, a system for distributing healthcare data has proposed by author Alam et al. [1] in which Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) have been used to encrypting medical data. Currently, RDH methods are mostly used to hide the private information in to medical images. The paper [2, 3] indicate that RHD systems have found some applications to medical pictures. This demonstrates that RDH is a promising contender for protecting medical images because it also has the ability to include sensitive data, which is absent from conventional cryptographic algorithms.

RDH method is a method by which we can extract original input data and hidden data. Normally, the hidden messages are sensitive data or personal data. For example, in the scenario of medicative icons, this could contain the individual information of patients, the diagnosis report, and a summary of prior medical records associated with the medical photos. An adaptable RDH scheme relies on quad-tree and pixel value ordering (PVO) was explained by J Lee et al. [4] to take advantage of the similarity between nearby pixels and conceal more data. An approach that disregards the differences between adjacent pixels in an image was proposed by F Aziz [5]. Instead, they change the image's columns and rows to enhance the smooth areas, which boost the image's embedding capability. The encryption and data hiding process has been shown in figure 1.

Recently, many researchers have attracted towards RDH on the encrypted image (RDHEI). This is done to guarantee that the transmitted image's security and privacy are upheld. These advanced proposed RDHEI methods can transmit images and concealed data safely, but they are still susceptible to some harmful actions. In particular, it should be noticed if someone attempts to change the pixel values of a medicinal snap that is encrypted. In other words, it is necessary to assess the reliability of RDHEI schemes, and this is currently an unsolved research issue. Additionally, the records of medical data exchange are not adequately preserved, making it difficult to trace and track such communication. The RDH method can be utilised in many different applications, including webometrics [6], digital forensic [7], e-health record transfer [8], and transfer of digital money [9].

Previously, several encryption and data embedding techniques are used & every scheme has its own merits and demerits. The original cover image, which can be of low quality or contain some superfluous information that can be removed, is used for data embedding in the previous systems. To achieve this, high-content image data embedding is done. The innovative interpolation technique is used for data embedding, together with a histogram shifting mechanism, and finally blockchain technology is employed to encrypt the images. The following are the inspiration and significance of the suggested scheme:

1. The existing interpolation techniques are considered either four neighbour pixels or eight neighbour pixels while estimating the value of center pixel, which is not very efficient and secure. The suggested interpolation scheme divides the pixels values in to two different regions for estimating the value of pixels. In experimental results, the proposed interpolation scheme shows that the quality of the interpolated image is better to ones obtained using existing techniques.

2. The suggested data concealing strategy considers how the HVS functions to conceal the personal data in the picture cells of the cover image. The approach alters the pixel values in a way that is adaptable and invisible to the human eye.

3. The experimental findings further demonstrate that the suggested approach performs best in terms of the capacity to hide data and the calibre of the produced images for all test shots. The suggested hiding strategy is also one of the easiest data hiding approach since it merely substitutes the personal data bits for the LSBs.

4. The suggested data hiding method is also reversible because it merely alters the interpolated picture cell values while concealing the private data. At the receiving end, the suggested interpolation approach can restore the interpolated pixel values.

5. Various encryption and data embedding techniques have been employed in the past, and each one has its own advantages and disadvantages. In earlier systems, data embedding used the original cover image, which could be of poor quality or contain some unnecessary information that could be removed. To achieve this, high-content image data embedding is done. The advanced interpolation technique is used for data embedding, combined with a histogram shifting mechanism, and ultimately blockchain technology is employed to encrypt the cover image.

The remaining part of this paper is structured as follows. Introduction to blockchain technology is covered in section 2. The associated works are considered in Section 3. Section 4 discusses the suggested approach and performance parameters are covered in section 5. Investigated outputs are discussed in section 6 and Section 7 serves as the paper's conclusion.

2. Blockchain Technology

Numerous image encryption techniques have been presented in the past. Still, approaches that work well for medical purposes are being investigated. The blockchain is a cutting-edge encryption method that is secure and has many uses in the technology and engineering areas. Blockchain is a new

technology whose objective is to substitute or remunerate for conventional centralised systems. It can be thought of as a Distributed Ledger Technology (DLT), where data storage

and transactions are carried out in a dispersed way. In this way, the blockchain network can be recognized even if there is no credibility between these entities who are communicating. The interconnection between all the data maintained in the chain by a cryptographic algorithm is one of the most crucial characteristics of the blockchain that makes tampering with the data very expensive (or nearly impossible). Recently, blockchain technology was used in the healthcare system to increase security. For example Z Wang et al. [7] suggested a concept of Gaurdhealth in which a decentralised blockchain system is used for sharing data and protecting privacy in the medical sector.

Additionally, blockchain provides a cryptographic hash to link all of the transaction details together, which is a distinctive characteristic. Figure 2 illustrates all legitimate transactions are gathered into a block within a predetermined time frame. Based on these transactional specifics and the previous block's hash, a new hash value is created. The consensus procedure (such as Proof of Work (PoW)) is used to approve the transaction comes next. During the consensus

time frame. Based on these transactional specifics and the previous block's hash, a new hash value is created. The consensus procedure (such as Proof of Work (PoW)) is used to approve the transaction comes next. During the consensus process, only such node that effectively resolved the predetermined challenging puzzle is able to add another block to the already-existent blockchain. Each transaction block's hash generation is connected to the block's prior

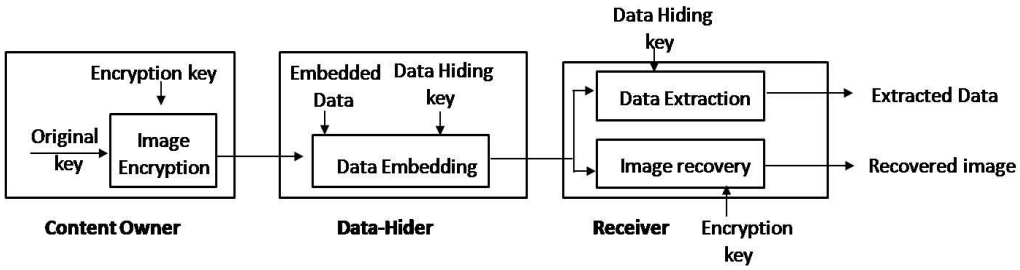


Figure 1. Encryption & Data Hiding Process

block's hash. A large number of legitimate blocks must be generated through the consensus process, and then the succeeding blocks must be overwritten, in order to change one of the transaction entries on the blockchain. Blockchain is an immutable solution for many applications because it is typical to build a large number of novel blocks quickly due to the time-consuming PoW procedure.

A blockchain is comprised of linked blocks joined together by previously created hash values. All information stored here is unalterable and immutable. We will have a sequence of blocks. Blockchain is a peer-to-peer network; it lacks centralised control. A complete copy of the entire sequence is sent to each blockchain node, and nodes utilise this copy to check the integrity and authenticity of the block. Since each block has a timestamp, it is quite difficult to alter the data. Each node in the chain receives a copy of the newly produced block as soon as it is formed. Every node establishes a consensus after confirming that this block hasn't been manipulated (Figure 3).

The blockchain's PoW algorithm requires a lengthy consensus procedure, which slows down transactions. Another option is to use a consortium blockchain, which has already a predefined enumeration of reliable participants. A simple consensus procedure like Practical Byzantine Fault Tolerance (PBZT) [8] can be applied in this situation. This enables quicker exchange of information among the nodes sharing a consortium blockchain without compromising the blockchain's essential security properties (such as auditability, traceability, and integrity).

3. Related Work

Two additional sub-sections were added to this section. Contemporary methods for RDH processes are reviewed in the first subsection, and state-of-the-art methods for encryption techniques are discussed in the next subsection.

3.1 RDH Schemes

Histogram Based

Histogram equalization and histogram stretching are used to improve the histogram. In histogram based method peaks are used for data embedding. To incorporate data, K Hwang et al. [9] use the location map and the picture histogram's peak point, and they slightly change the pixel values. This approach uses the location map and picture histogram peak points; therefore no additional data needs to be communicated to the receiving side. Additionally, virtually imperceptible visuals can be produced by slightly altering pixel values. By retaining the bit map of the minima point's coordinates rather than the actual coordinates, Kuo et al [10] work's enhances that of Hwang et al. Based on PEE of several histograms, an effective RDH technique is suggested by Li et al. [11]. A number of histograms are created by

measuring the prediction-errors for various levels of complexity after each pixel's prediction value and complexity measurement which has been calculated based on its context.

Finally, this suggested embedding approach based on multiple histograms modification data embedding is carried out. This technique raised quality, but it had embedding capacity restrictions. The Dynamic Neighboring Pixels (DNP) predictor [12] generates the prediction technique adaptively for the current pixel's four gradient areas (gradient zone with horizontal/vertical/rhombus/plane axes). The creation of several histograms is introduced using fuzzy C-means (FCM) clustering. Fuzzy C-means (FCM) clustering [13], is used to create the various histograms. To categorize the cover carriers, the FCM with specially built features is used.

Difference Expansion

In DE method discrepancies between adjacent pixel values are computed and a few difference values should be chosen for the difference expansion. Initially, Tian et al. [15] proposed DE method in which enlarged difference and the two pixels' mean value were used to generate the updated values for the hidden image. Despite reducing stego image distortion, the method's embedding capacity was decreased to less than 50% of the total image's pixels. Alattar et al. [14] introduced an approach in which embed three bits when quads of adjacent pixels are expanded using the difference method.

The author proposed a reduced location map and adaptive DE-based reversible stegano graphic system with bilinear interpolation [16]. W Wang [17] suggested a SBDE-based method to split pixels into HSB and LSB for greater pixel correlation. In order to create a more correlated sequence of pixel pairs, it takes advantage of the higher pixel-bit planes that are significant within a small neighbourhood. This solution also tackles the issue of how to appropriately divide the pixels into pairs for pair wise SBDE.

Compression Based Scheme

By using an embedding process to compress a frequency of bits from the actual wrap image, this scheme conceals both the secret data and the shrinked data in the cover image. Vector quantization is used to compress the image by Lu et al. [18]. Now, only blocks with highly connected pixels have

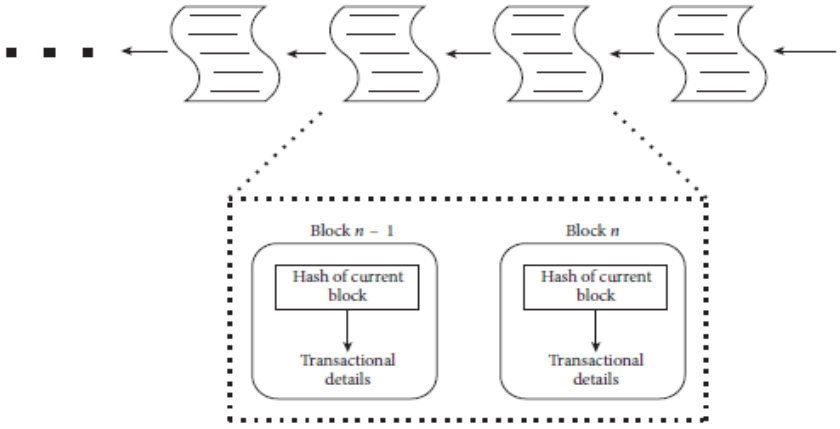


Figure 2. Blockchain data structure

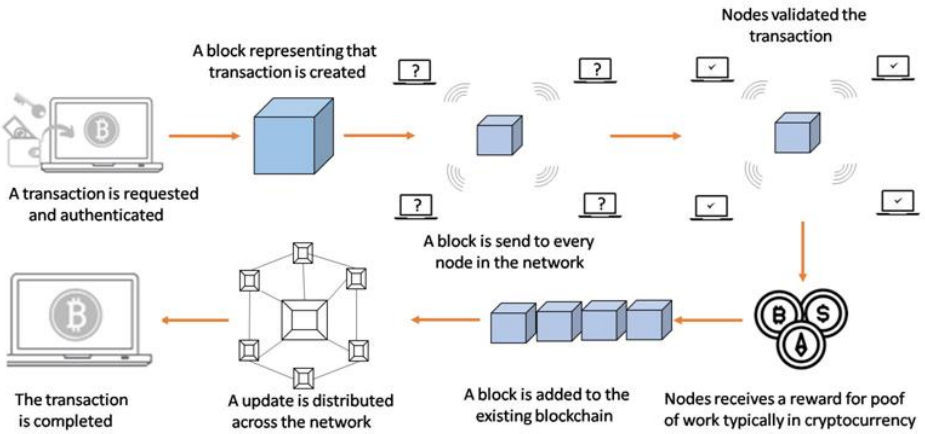


Figure 3. Network Diagram for Decentralized Blockchains

the secret data and the shrinked data in the cover image. Vector quantization is used to compress the image by Lu et al. [18]. Chang et al. [19] introduces another compression-based scheme which uses block truncation coding (BTC) for color images. In order to improve the rate of compaction, instead of employing three ones on every colour picture block, this method uses a GA to obtain an approximation of the ideal common bitmap. In contrast to using just the pixel value, the author provides a novel RDH approach for AMBTC-compressed images [20]. To assess if a block of AMBTC-compressed photos can be embedded or not, we examine the redundancy in the block.

Singh et al. [44] utilised a variety of techniques for various datasets. The authors conducted psychometric analysis with the LIWC15 tool, sentiment analysis with the MeaningCloud tool and SPSS software used to perform a descriptivestatistical analysis on the check-in data in order to identifysignificant trends and gain a better knowledge of how people behave in the city. To maintain the security and privacy ofthe Individually controlled EHR system, Vimalachandran et al. [45] developed an idea called "Log-in-Pair".Yong-Feng Ge et al. [46] clearly defines the multitasking database fragmentation problem for privacy preservation needs. Chentharaet al. [47] suggested an approach to create a framework for protecting privacy called Healthchain, which is built on Blockchain technology and upholds the security, privacy, scalability, and integrity of e-health data. To improve link prediction accuracy, Yin et al. [48] suggested a modality-aware graph convolutional network (MAGCN) module.

Interpolation-based Scheme

The confidential bits are situated in the interpolated pixels without altering the actual pixels in the interpolation-based RDH systems, which enlarge the image through interpolation methods. The quality and embedding capability of the interpolation-based approach are its key benefits.There is some interpolation based method like Adjacent Mean Interpolation (AMI) [21] Interpolation using Adjacent Pixels (IAP) [22], Improved Adjacent Mean Interpolation (IAMI) [23], and Updated Adjacent Mean Interpolation (UAMI) [24] are existed. In AMI technique, mean value is calculated by using neighbouring pixel values and these estimated mean value is placed into a pixel that has not yet been assigned. The IAP method is improvement over AMI method which included large embedding capacity, minimal computing complexity, and high image quality. Another interpolation method used for data hiding is IAMI in which histogram modification is used after embedding process. The method enables some changes to be concealed in a picture without being noticed by the human vision system (HVS). A Malik et al. has proposed UAMI method which estimates the pixel intensity by assigning more weight to the closer pixels. This interpolation has several advantages, over AMI & IAMI method while IAP is an extension of AMI which has low computational cost.

Table 1. Several RDH Schemes

Schemes	References	Concepts
HS	Kim et al.[9], Jiang et al.[10], Zhang et al. [11], Gao et al.[12], Mao et al.[13]	The maximum points are used for data embedding
Difference Expansion	Tian et al. [15], Alattar et al. [14], Wu et al. [17], Wang et al. [16]	For data embedding, discrepancies between neighbouring pixels are used
Compression-Based Schemes	Lu et al. [19], Chang et al. [18], Lin et al. [20]	Data embedding has taken compression into consideration.
Interpolation-Based Schemes	Jung et al. [22], Lee et al. [21], Chang et al. [24], Zhang et al. [23]	Data embedding has done through interpolation technique

3.2 Medical Image Encryption Schemes

Strong encryption methods are essential for protecting the medical data stored in the cloud. Image quality is maintained while achieving outstanding encryption outcomes using region of interest (ROI)-based approaches. Table 2 includes a list of the prominent medical picture encryption techniques. Jin et al. [39] emphasis on blockchain-based strategies, which analyses the most advanced medical data sharing protocols over the past years that are secure and privacy-preserving. The author Alvi et al. [40] proposes an adaptive noise removal technique that works well with impulsive noises and doesn't blur the edges of the input image. With a focus on medical imaging applications, In addition to discussing potential attack vectors and upcoming opportunities in medical imaging and other fields, Kaissis et al. [41] provide an overview of current and next-generation solutions for federated, secure, and privacy-preserving artificial intelligence.The authors Alvi et al. [42] put up a suggestion for an effective fuzzy logic technique for de-noising digital grayscale images. The Fuzzy Inference System (FIS) is used by this exiting algorithm to determine the membership value and nearly reproduces the original noise-free image. To implement the secure recommendation on the encrypted medical data, Zhang et al. [43] offer forth a medical treatment recommendation protocol and a privacy-preserving medical graph creation strategy.

The authors Parah et al. [28] introduced a novel large capacity and RDH method for e-healthcare applications. In this, the Pixel to Block (PTB) conversion approach has been employed as a viable and computationally affordable substitute for interpolation to guarantee reversibility of medical images. In this scheme, the EPR, watermark data, and checksum data have been embedded using Intermediate

Significant Bit Substitution (ISBS). ISBS is used to prevent the widely utilised LSB removal/replacement attack. Chen and Chi [29] proposed a new data-hiding methodology based on the block truncation coding (BTC) is used. This methodology shrinks the size of the image and improves security. Loan et al. [30] proposed a scalable data hiding strategy for medical pictures based on the Pixel Repetition Method (PRM) and Heterogeneous Edge Identification (HEI) is described. The tiny image was scaled up using PRM, and HEI makes sure that no essential edge information is neglected. Geetha et al. [31] introduces a Rhombus Mean Interpolation approach instead of PTB conversion process to forecast the interpolated points in the cover image. Yang et al. [32] proposed an adaptive threshold scheme to separate ROI and NROI in medical image then stretching the gray scale improves the contrast in the ROI region while embedding the data into the peak bins of the expanded histogram does not increase the histogram bins. The remaining necessary huge amounts of data are integrated into the NROI region, despite of their quality. The suggested algorithm [33] divides medicinal icons into ROIs and NROI. It naturally expands the ROI's gray scale histogram in order to increase both the ROI's embedding capacity and improve the contrast of the image. Balasamy et al. [34] presented a method for watermarking medical images which uses wavelet modification to insert an encrypted watermark and a fuzzy-based ROI selection. Liu et al. [35] proposed a model in which an actual medical image is first divided into a ROI and NROI, and then it is encrypted using an encryption key by a content owner. The LSB of the encrypted ROI and EPR are concatenated by a data-hider, who then uses the LSB substitution algorithm to embed the concatenated data into the encrypted picture. Zhang et al. [36] used a hyper chaotic system in which

Table 2. Encryption Techniques (Notable Methods)

References	Method	Features
Parah et al. [28]	Intermediate Significant Bit Substitution (ISBS)	Ability to localise the tampered block and count the number of modified blocks
Chen and Chi [29]	Block Truncation Coding	Payload and the number of blocks increases when the block size lowers, but the image quality declines. For various threshold values, it achieves the maximum payload and the best image quality.
Loan et al. [30]	Pixel Repetition Method (PRM)	Offers a high capacity, good imperceptivity, and is totally reversible with respect to the seed picture.
Geetha & Geetha [31]	Rhombus Mean Interpolation	It is more effective for localisation, tamper detection, and data embedding.
Yang et al [32]	Histogram modification	Improve the visual quality of medical photographs and produce more contrast enhancement effects & also prevent the overflow and underflow issues.
Gao et al. [33]	Difference Expansion	Improved visual perception and reduced distortion while maintaining the similarity and brightness of the source images.
Balasamy and Suganyadevi[34]	Wavelet Transformation + Fuzzy Logic	Increased resilience and enhanced security for the watermarked image against several types of attacks
Liu et al. [35]	LSB substitution	Achieve ROI reversibility and a significant improvement in the quality of images that have been directly decrypted.
Zhang et. al [36]	Hyperchaotic	Combines encryption and watermarking, and it has both a large secret key storage area and a big capacity for embedding watermarks.
Ahmad and Alam [37]	Elliptic Curve Cryptography (ECC)	Improve the e-commerce security through PGP with double security
Horng et.al [27]	Blockchain	Build a blockchain system on top of the RDH for encrypted image to give an integrity check.

personal information about patients is included into ROI in medical imaging with a large capacity difference. Following that, hyper chaotic systems are used to encrypt the watermarked medical photos and at the receiver end identical images can be achieved for diagnosis by deciphering theimage using the receiver's encryption key. Using the AES and ECC, Ahmad et al. [37] devised a method for encryptingdata. RDH techniques are now being used to insert private information into medical images. Hong et al. [46] outlined a plan based on histogram shifting and imaging block-wise encryption to enhance the embedding capacity of encrypted images. It is suggested to implement RDHEI using a blockchain, where the hash value would be produced from the output and kept on the blockchain. This makes it possible to quickly identify any attempt to manipulate with the medical photos. This study also examines how blockchain technology can be used to improve the reliableness and traceability of the RDHEI system with the goal of protecting medical data.

4. Proposed Method

In this paper, we have presented a novel interpolation scheme and histogram shifting technique. The histogram shifting process is similar to [25]. In this proposed method, initially data embedding has done using interpolation technique after that encryption process has applied to the stego image using blockchain technology.
Several steps of this proposed scheme has explained below:

4.1. Image Partition

Initially, the image is divided in to two distinct segments A & B, the LSB of segment A is embedded into the segment B reversibly by using RDH technique so that LSB of A can be used for handling the messages. Finally, encryption has done on regrouped image.

Suppose the actual image P is an 8-bit gray-scale image. The image P has dimension R×S and pixels $P_{k,l}\epsilon\,[0,255]\,, 0 < k \leq R, 0 < l \leq S$. The content owner first removes many overlapping blocks along the rows of the actual image, the number of blocks is defined by the size of the messages that will be embedded, which is denoted by $'L'$. Every block has r rows, where $r = \lceil L/S \rceil$, and the total number of overlapped blocks may be calculated using the formula $n = R - r + 1$. The fact that previous and subsequent blocks are overlapping one another along the rows is a crucial thing to note. Here, it is necessary to create a function for each block with the aim of estimating its first-order smoothness, which is the just difference between the present pixels and the mean of the eight nearby pixels.

$$\eta = \sum_{k=2}^{r}\sum_{l=2}^{N-1}\left|IM_{k,l} - \frac{IM_{k-1,l} + IM_{k+1,l} + IM_{k,l+1} + IM_{k,l-1} + IM_{k-1,l-1} + IM_{k+1,l+1} + IM_{k-1,l+1} + IM_{k+1,l-1}}{8}\right| \quad (1)$$

In this case, the function η checks the disparity between the pixel intensity and those of the surrounding pixels in 0^0, 45^0,90^0 and 135^0. This process has applied on all the pixels excluding boundary pixels. If the value of η is zero then surface is complete smooth and higher the value of η suggested the concerned block has complex texture. As a result, the content owner chooses the specific block with the highest η to be A and positions it in front of the image, which is joined by the remaining of part B, which has fewer textured areas, as illustrated in figure 4.

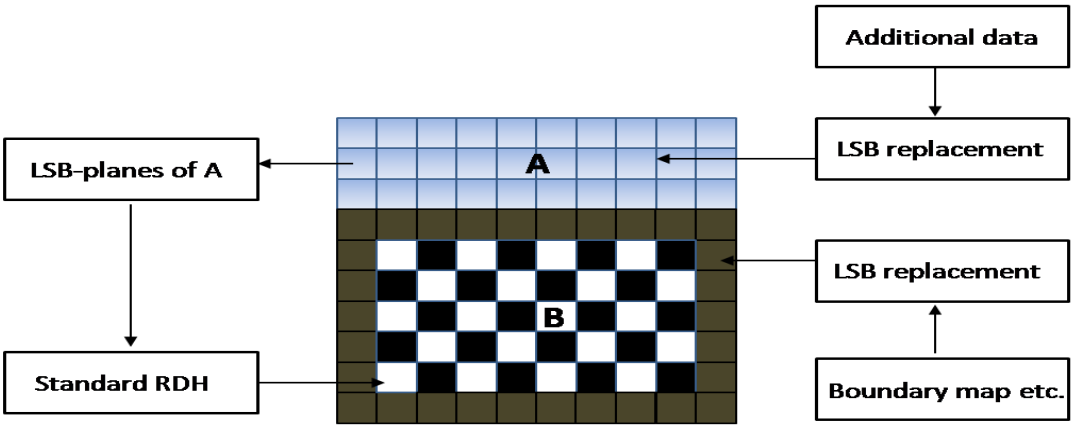


Figure 4. A visual illustration of the picture partitioning and data embedding method

4.2. Self Reversible Embedding (SRE)

The main objective of SRE is to LSB of A is incorporated into B through RDH technique which is shown in step 1. The SRE method relies on histogram shifting and pixel approximation error.

Step 1: In partition of B, pixels are black and white which is defined as

(k+l) mod 2 = 0 for white pixel
(k+l) mod 2 = 1 for black pixel

Here, k & l are the indices of pixels.

The interpolation value ($IM'_{k,l}$) for a pixel $IM_{k,l}$ gained through eight pixels that surround it as represented in the equation below:

$$IM'_{k,l} = W_1 IM_{k-1,l} + W_2 IM_{k+1,l} + W_3 IM_{k,l+1} + W_4 IM_{k,l-1} + W_5 IM_{k-1,l-1} + W_6 IM_{k+1,l+1} + W_7 IM_{k-1,l+1} + W_8 IM_{k+1,l-1} \quad (2)$$

As a result, the estimated pixel intensities depend on both the values of the pixels around them and the weights (W_i) of the corresponding pixel. Where, $0 < i \leq 8$.

The error is computed as [26]

$$E_{k,l} = IM_{k,l} - IM'_{k,l} \quad (3)$$

The assessing error for any pixel value $IM_{k,l}$ is often calculated using $E_{k,l} = IM_{k,l} - IM'_{k,l}$ and then those data can be incorporated into the evaluating error arrangement using HS as outlined below

4.3. Histogram Shifting

The inaccuracies of estimated pixels are calculated using nearby pixels that have been altered. A new estimated error sequence (e) is generated, which can be utilized in data embedding. The same data embedding procedure can be used to create multilayer embedding by treating the updated image B as the "original" picture. In order to utilize all pixels of B, two estimated error sequences are finally concatenated to embed messages in all single-layer embedding techniques. Data can be added to each error sequence using the HS method. Some messages can be incorporated on each error sequence using bidirectional histogram shift. The histogram of the error sequence is separated into two sections whose named are left part and right part. The right half contains the value zero and above & left half contains the negative values. The highest point in left part is denoted by μ_{max} and the peak point in right part is denoted by π_{max}. Similarly, zero point in left part is denoted by μ_{min} and the zero point in right part is denoted by π_{min}.

μ_{max} and π_{max} are obtained as

$$\begin{cases} \mu_{max} = \arg \max_{\xi \epsilon E} hist(\xi) \\ \pi_{max} = \arg \max_{\xi \epsilon E - \{\mu_{min}\}} hist(\xi) \end{cases} \quad (4)$$

In the above equation (4) hist (ξ) represents the number of times the interpolation-error equals to ξ and E is the set of interpolation error. Further, interpolation error are categorized into two category, the left interpolation error as μ_e and the right interpolation error as π_e and by considering $\mu_{max} < \pi_{max}$

1. Left interpolation-error (μ_e): If interpolation error $\boldsymbol{\xi \leq \mu_{max}}$
2. Right interpolation-error (π_e): If interpolation error $\boldsymbol{\xi \geq \pi_{max}}$

The notion of additive interpolation-error extension is shown below.

$$\xi' = \begin{cases} \boldsymbol{\xi + sign\,(\xi) \times t}, & \boldsymbol{\xi = \mu_{max} \text{ or } \pi_{max}} \\ \boldsymbol{\xi + sign\,(\xi) \times 1}, & \boldsymbol{\xi \in (\mu_{max}, \mu_{min}) \cup (\pi_{max}, \pi_{min})} \\ \boldsymbol{\xi} & \textbf{else} \end{cases} \quad (5)$$

In the above equation (5), ξ' indicate the expanded interpolation-error, t is the bit to be embedded and sign () is the signum function which is defines as

$$\mathbf{sign}(\xi) = \begin{cases} \mathbf{1} & \boldsymbol{\xi \epsilon \pi_e} \\ \mathbf{-1} & \boldsymbol{\xi \epsilon \mu_e} \end{cases} \quad (6)$$

The terms left zero (μ_{min}) and right zero (π_{min}) in equation (5) could be defined as

$$\begin{cases} \boldsymbol{\mu_{min} = \arg \min_{\xi \epsilon \mu_e} hist(\xi)} \\ \boldsymbol{\pi_{min} = \arg \min_{\xi \epsilon \pi_e} hist(\xi)} \end{cases} \quad (7)$$

Similar interpolation calculations might be used in the extraction system; it is possible to have the past interpolation values and IM', the interpolation errors by using the equation shown below

$$\mathbf{IM''} = \mathbf{IM'} - \boldsymbol{\xi'} \quad (8)$$

When performing the extraction procedure, we can have homogenous interpolation values IM' and the related interpolation-errors by using the same interpolation mechanism.

$$\xi' = \mathrm{IM''} - \mathrm{IM'} \quad (9)$$

Finally, it is possible to retrieve the original pixels by using

$$\mathrm{IM} = \mathrm{IM'} + \xi \quad (12)$$

To embed messages into positions with an computing error which is equal to π_{max} , adjust all error values between $\pi_{max} + 1$ and $\pi_{min} - 1$ with one step toward right, and then, we can represent the bit 0 with π_{max} and the bit 1 with $\pi_{max} + 1$. Similar to the right part's embedding procedure, the left component shifts left and is accomplished by deducting 1 from the relevant pixel values. The technique was repeated until all the data had been incorporated.

The overflow problem occurs when natural boundary pixels shift from 255 to 256 and underflow problem occurs when natural boundary shifts from 0 to -1, similar to other RDH techniques. We only incorporate data into estimating errors with matching pixels valued between 1 and 254 to avoid overflow and underflow problems. However, uncertainties persist when non-boundary pixels are altered from 1 to 0 or from 254 to 255 during the embedding process. Pseudo-boundary pixels are those boundary pixels that were

The embedded data can be extracted with the help of parameters μ_{max} , μ_{min} , π_{max} , π_{min} and t which is used in equation 5.

$$\mathbf{t} = \begin{cases} \mathbf{0}, & \boldsymbol{\xi'} = \boldsymbol{\mu}_{\mathbf{max}} \ \mathbf{or} \ \boldsymbol{\pi}_{\mathbf{max}} \\ \mathbf{1}, & \boldsymbol{\xi'} = \boldsymbol{\mu}_{\mathbf{max}} - \mathbf{1} \ \mathbf{or} \ \boldsymbol{\pi}_{\mathbf{max}} - \mathbf{1} \end{cases} \quad (10)$$

We can utilize the inverse function of additive interpolation-error expansion to recover real interpolation errors as a result, and we obtain,

$$\boldsymbol{\xi} = \begin{cases} \boldsymbol{\xi'} - \mathbf{sign}(\boldsymbol{\xi'}) \times \mathbf{t}, \ \boldsymbol{\xi'} \boldsymbol{\varepsilon} \left[\boldsymbol{\mu}_{\mathbf{max}} - \mathbf{1}, \boldsymbol{\mu}_{\mathbf{max}}\right] \cup \left[\boldsymbol{\pi}_{\mathbf{max}}, \boldsymbol{\pi}_{\mathbf{max}} + \mathbf{1}\right] \\ \boldsymbol{\xi'} - \mathbf{sign}(\boldsymbol{\xi'}) \times \mathbf{1}, \ \boldsymbol{\xi'} \boldsymbol{\varepsilon} \left[\boldsymbol{\mu}_{\mathbf{min}}, \boldsymbol{\mu}_{\mathbf{max}} - \mathbf{1}\right] \cup \left[\boldsymbol{\pi}_{\mathbf{max}} + \mathbf{1}, \boldsymbol{\pi}_{\mathbf{min}}\right] \\ \boldsymbol{\xi}, \qquad \mathbf{otherwise} \end{cases} \quad (11)$$

produced during the embedding procedure. As a result, a boundary map is developed to indicate whether the boundary pixel is 0 or 1. Bit "0" stands for a pixel's natural border, while Bit "1" stands for a pixel's pseudo-boundary in a binary sequence. Since calculating errors for B's marginal area cannot be estimated using (2), in order to best utilize B, we set the border map there and use LSB replacement to embed it which is shown in figure 4. Messages, or LSB-planes, are built with the original LSBs of the marginal area and reversibly inserted therein. Most of the time, even with a high embedding rate; the length of the border map is extremely small; as a result, the marginal area of A is large enough to accommodate it. If, after a reasonable amount of embedding, some of the message is still visible, we can choose a portion of the error sequence that has adequate peak points. These correct points are designated by the letters LPP and RPP.

4.4. Proposed Interpolation Method

In this proposed work, we consider 3×3 part of an image,

Figure 5. Estimation of the center pixel through pixels in the neighbourhoods

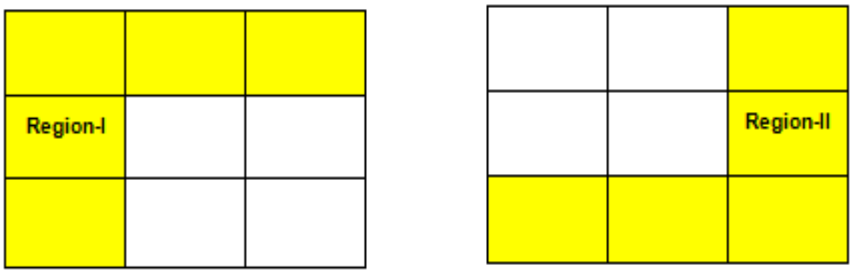


Figure 6. Estimation of the center pixel using pixels in the neighbourhoods in region I & region II

whose pixel values are lies between $IM_{k-1,l-1}$ to $IM_{k+1,l+1}$ as shown in figure 5. We have taken regional values instead of any proper direction pixel intensities. The partition of region is shown in figure 6. Assume that we have to estimate $IM_{k,l}$ with estimated value $IM'_{k,l}$.

The mean value of adjacent pixels of $IM_{k,l}$ are

$$IM^1_{mean} = \frac{1}{4}\left[IM_{k-1,l} + IM_{k+1,l} + IM_{k,l+1} + IM_{k,l-1}\right]$$

$$\mathbf{IM^2_{mean}} = \mathbf{\frac{1}{4}\left[IM_{k-1,l-1} + IM_{k+1,l+1} + IM_{k-1,l+1} + IM_{k+1,l-1}\right]} \quad (13)$$

Defining average value in region I and region II as

$$IM_I = \frac{1}{5}\left[IM_{k-1,l-1} + IM_{k-1,l} + IM_{k-1,l+1} + IM_{k,l-1} + IM_{k+1,l-1}\right]$$

$$IM_{II} = \frac{1}{5}\left[IM_{k+1,l-1} + IM_{k+1,l} + IM_{k+1,l+1} + IM_{k,l+1} + IM_{k-1,l+1}\right] \quad (14)$$

Defining sets in various regions as

$$S_I = [IM_{k,l-1}, IM_{k,l+1}, IM_I]$$

$$S_{II} = [IM_{k-1,l}, IM_{k+1,l}, IM_{II}] \quad (15)$$

The variance in region I and region II as

$$\sigma^2(e_I) = \frac{1}{3}\sum_{t=1}^{3}(S_I(t) - IM^1_{mean})^2$$

$$\sigma^2(e_{II}) = \frac{1}{3}\sum_{t=1}^{3}(S_{II}(t) - IM^2_{mean})^2 \quad (16)$$

The weight in regions I and II is determined by

$$\omega_I = \frac{\sigma^2_{II}}{\sigma^2_I + \sigma^2_{II}} \quad \text{and} \quad \mathbf{\omega_{II} = \frac{\sigma^2_I}{\sigma^2_I + \sigma^2_{II}}} \quad (17)$$

The approximated pixel value is calculated using

$$IM' = \omega_I IM_I + \omega_{II} IM_{II} \quad (18)$$

The estimated error is

$$e = IM - IM' \quad (19)$$

4.5. Encryption of Image

This section outlines the planned blockchain system, which aims to provide integrity and traceability. The suggested blockchain technology, which enables secure medical picture exchange between doctors D_1 and D_2 in hospital H_1 & H_2 , respectively as shown in figure 7. Before generating the encrypted stego medical image (ESMI), doctor D_1 first encrypts the EPR. The ESMI and enciphered health document both are kept in directory of hospital H_1 and the blockchain is updated with a new transaction block. In this blockchain method, if anyone is interested in exchanging medicinal document then the accuracy of data that was sent can verify at receiver side. Let the ESMI is shared by Doctor D_1 to the Doctor D_2 and Medical Institute H_2. Doctor D_2 initially calculates the hash value of the received ESMI and differentiate it to the blockchain to ensure its accuracy. He then uses a valid key to extract the concealed medical records and a legal key to decrypt the records. Medical Institute H_2 performs a comparable procedure.

The flow of transaction in blockchain is shown in figure 8. Initially, a symmetric key mechanism is used to encrypt

the medical records of patient with the help of following equation:

$$\zeta_{\mathrm{PMR}} = \mathrm{Encryption}\ (\mathrm{k}', \mathrm{PMR}) \quad (20)$$

Where, ζ_{PMR} is resultant cipher text medical record, k' is symmetric key and PMR is patient medical record. Further, we produce another key $\mathrm{k}'' = \mathrm{key}_1 \parallel \mathrm{key}_2 \parallel \mathrm{key}_3$, where key_1 is sender's key, key_2 is encryption key and key_3 is data hiding key where, key_1, key_2 and key_3 are used in the proposed RDH scheme. By utilising the suggested RDH technique, we create an ESMI by embedding the encrypted patient's medical records ζ_{PMR}within the medical image.

The hash value of existing block is computed by concatenating the hash value of the previous block (γ_{Prev}) and ESMI. The following calculation produces the hash value of the current block:

$$\boldsymbol{\gamma_{\mathrm{current}} = \mathrm{Hash}(\gamma_{\mathrm{previous}} \parallel \mathrm{ESMI})} \quad (21)$$

Where, Hash can be any widely used cryptographic hash algorithm (SHA-256) & $\gamma_{current}$ is the current block's hash value. The blockchain network receives the newly created block for the consensus process. Once the peers have approved this block, it joins the blockchain network. To confirm the authenticity of the obtained ESMI, the receiver

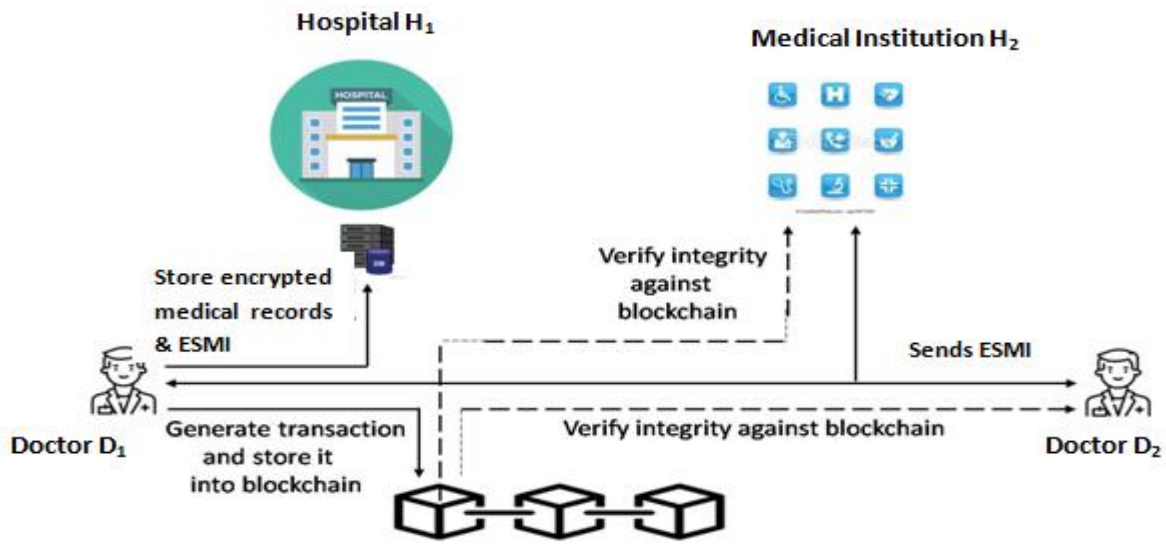


Figure 7. An illustration of the suggested Blockchain-based medical data exchange system

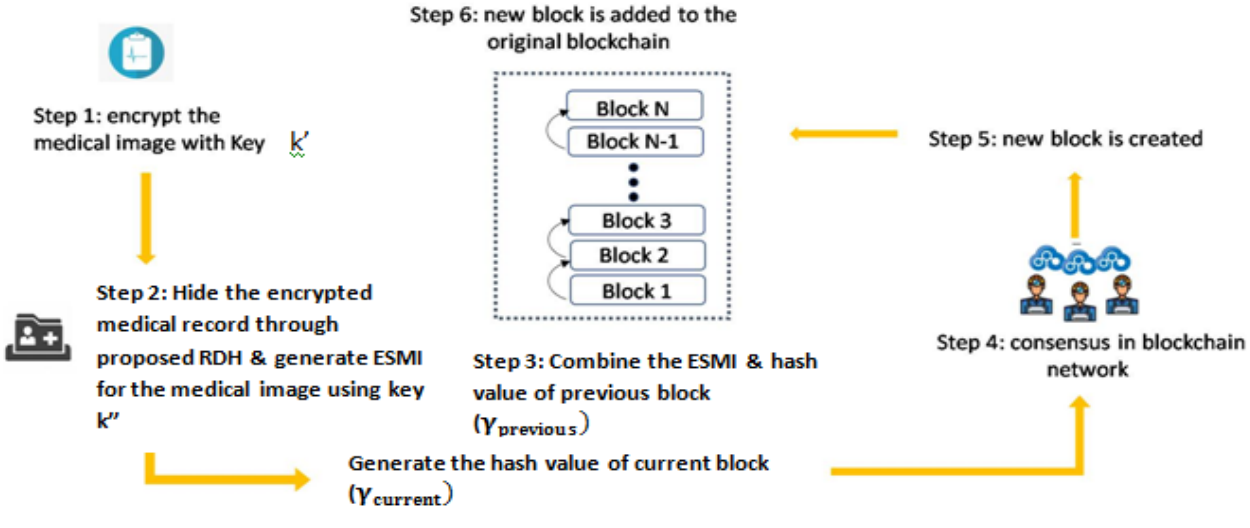


Figure 8. An illustration of the Blockchain system's transaction

generates a new hash value using the previously used cryptographic hash function (SHA-256). We can compute the new hash value at receiver end by following equation:

$$\gamma'_{\text{current}} = \text{Hash}(\gamma_{\text{previous}} \parallel \text{ESMI}) \quad (22)$$

Finally, $\gamma'_{current}$ is compared with the hash value of the present block in blockchain ($\gamma_{current}$). If $\gamma_{current} = \gamma'_{current}$ then the received block is unaltered otherwise block is modified.

Any well-known blockchain framework, such as Ethereum
and Hyperledger Fabric, can be used to create the suggested blockchain system. Step 1 can encrypt data using an industry-standard block cipher such as AES, and Step 2 can be completed using my proposed RDH scheme. Steps 3-6, which are common actions seen in a typical blockchain architecture, can be readily executed.

Security Analysis: With consideration of several attacker scenarios, a security analysis of this blockchain system is offered in this section.

1. This blockchain system can protect the confidentiality of patient's medical health record. Even with access to ESMI, an attacker cannot access a patient's medical record because he is not familiar with key_1, key_2 and key_3.

2. Integrity can be attained by this blockchain system. It's also feasible that the malicious attacker is more concerned with fabricating ESMI and generate fake keys: key_1, key_2 and key_3. However, in this instance, the hash value of the current block will differ from the hash value stored in the blockchain. In order to compromise the block chain, the attacker would need to have access to more than 50% of all nodes, which is impractical in a real-world scenario. However, referring to equation (20), each new block's hash value is influenced by the prior block. Similar to the previous scenario, the attacker would need a tremendous amount of computing power and time to calculate the hash values of all the blocks before it in order to modify just one record in the blockchain. Consequently, the suggested system is protected from malicious attempts that aim to damage its integrity.

3. The steganography of medical image prevents attackers from recovering them. The ESMI is kept in the hospital's database under this proposed system. Even if a harmful attacker gains access to the ESMI, he will be unable to decode the medical image steganography (SMI). He cannot successfully recover the SMI because he does not hold key_2. Additionally, he is unable to ever obtain the patient's medical records from ESMI.

4.6. Extraction & Restoration

To produce an error sequence, the blockchain decrypted image is first subtracted from the interpolated picture from the cover image interpolation. It is possible to recover the embedded bits by using:

$$b = \begin{cases} 0, & e' = \mu_{min} \; or \; \pi_{min} \\ 1, & e' = \mu_{min} - 1 \; or \; \pi_{min} - 1 \end{cases} \quad (23)$$

After the data bits are deleted, the remaining error sequence is added to the interpolated image to recover the original image. The extraction procedure is identical to that employed by K Ma et al. [26].

5. Performance Matrices

PSNR could be defined as a measurement of visual quality of an image which is interpreted as

$$\text{PSNR} = 10 \log_{10} \frac{(255)^2}{\text{MSE}} \quad (24)$$

The parameter MSE in the above equation is an estimation of the pixel difference between the actual image and embedded image. The maximum possible value of PSNR is ∞.

The second parameter is structural similarity (SSIM) which evaluates changes in contrast, brightness and structure of an image. Modelling brightness is done using average pixel intensity, modelling contrast is done using variance between the reference and distorted image, and modelling structural similarity is done using cross-correlation between the two images.

$$\text{SSIM}(u, v) = \frac{(2\mu_u + c_1)(2\sigma_{uv} + c_2)}{(\mu_u^2 + \mu_v^2 + c_1)(\sigma_u^2 + \sigma_v^2 + c_2)} \quad (25)$$

In the above equation, original image is denoted by 'u' and embedded image as 'v'. The actual image's mean and variance are represented by the parameters μ_u and σ_u^2 in the above equation. The distorted image's mean and variance are represented by the parameters μ_v and σ_v^2, and the parameter σ_{uv} is used to determine the cross-covariance between the two images, c_1 and c_2 are constants. The maximum possible value of SSIM is 1.

6. Results

The suggested technique will be examined using a standard image database that is openly accessible [25–26], as illustrated in Figure 9. The resolution of each image is $512 \times 512 \times 8$ pixels. The state-of-art method takes there images. The medical images which are taken from the link of MIDAS/National Alliance for Medical Image Computing (NAMIC) [27] also considered for the comparison of the state-of-the-art methods. In order to evaluate performance, PSNR and SSIM are utilized.

We have to compute EC, embedding rate (ER) in bpp, PSNR and SSIM for the images Airplane, Baboon, Barbara, Lenna, Boat and Peppers. In the table 3, shows the comparison between proposed work and the recent work by J Hoeng [27], Zhang et.al [38] and Geeta et.al [31] in terms of EC, ER, PSNR and SSIM. The maximum possible rate and PSNR in [27] is 0.73 and 33.15, 0.78 and 34.28 in [38] &

0.83 and 32.18 in [31] for airplane image. The obtained SSIM is 0.9821 in [27],0.9356 in [38] & 0.9551 in [31]. In the proposed work maximum possible rate is 0.94 and PSNR is 35.12. SSIM in proposed work is 0.9132. The maximum possible capacity and PSNR in [27] is 163427 and 25.10, 145694 and 21.36 in [38] & 166494 and 25.60 in [31] for 'baboon' while in the proposed work it is 173262 and 31.80. In the case of 'barbara' maximum possible ER and SSIM is 0.81 and 0.9801 in previous work while it is 0.89 and 35.14 respectively in this current work. In case of 'lena' PSNR and SSIM are 37.42 and 0.9898 in the Horng's work [27] while in proposed work this value is 39.95 and 0.9162. Embedding Capacity is 211102 for 'boat' and 218242 for 'pepper' in [27], 221235 and 213658 in [38] & 202215 and 226178 in [31] while 235421 and 246249 in proposed works. Additionally, it is clear that Horng et al. work's performs better with SSIM than the suggested work, which indicates that the embedding-related distortion in their work is reduced. It is also observed that ER is much less in previous works as compared to our work. The EC is calculated using $M \times N \times ER$ in the previous work [27] [38] [31], whereas in the proposed work, it is calculated as $M \times N \times ER - M4$ where M4 denotes the size of the boundary map where data is not stored. The table 3 also shows that the capacity in our approach is superior to [27], [38] and [31].

Comparison for medical images X & Y (shown in figure 10) of size 256×256 are represented in table 4.The maximum possible capacity and rate for medical image X is 60457 and 0.93 respectively in previous work [31] while in proposed work it is 62236 and 1.The PSNR and SSIM is obtained the value 36.14 and 0.9931 in [27], 37.62 and 0.9754 in [38] & 36.25 and 0.9804 in [31] while in our work it would be 39.12 and 0.9624 for image X. Similarly, the capacity, ER and PSNR are increases in the proposed work while SSIM is decreases as compared to [27], [38] and [31] for medical

Image Y. Therefore, it is clear that the suggested methodology is more effective than the current approaches in terms of EC while also having an acceptable PSNR and SSIM.

Figure 11 (from (a)-(d)), shows the comparison of capacity, ER, SSIM & PSNR between exiting schemes and proposed scheme for the digital image. Figure 12 (from (a)-(d)), shows the comparison of capacity, PSNR, ER & SSIM between exiting schemes and proposed scheme for the medical image X & Y.

7. Conclusion

For e-health applications, secure patient medical data transfer techniques are required. In this research, a secure patient data transfer system is suggested, employing

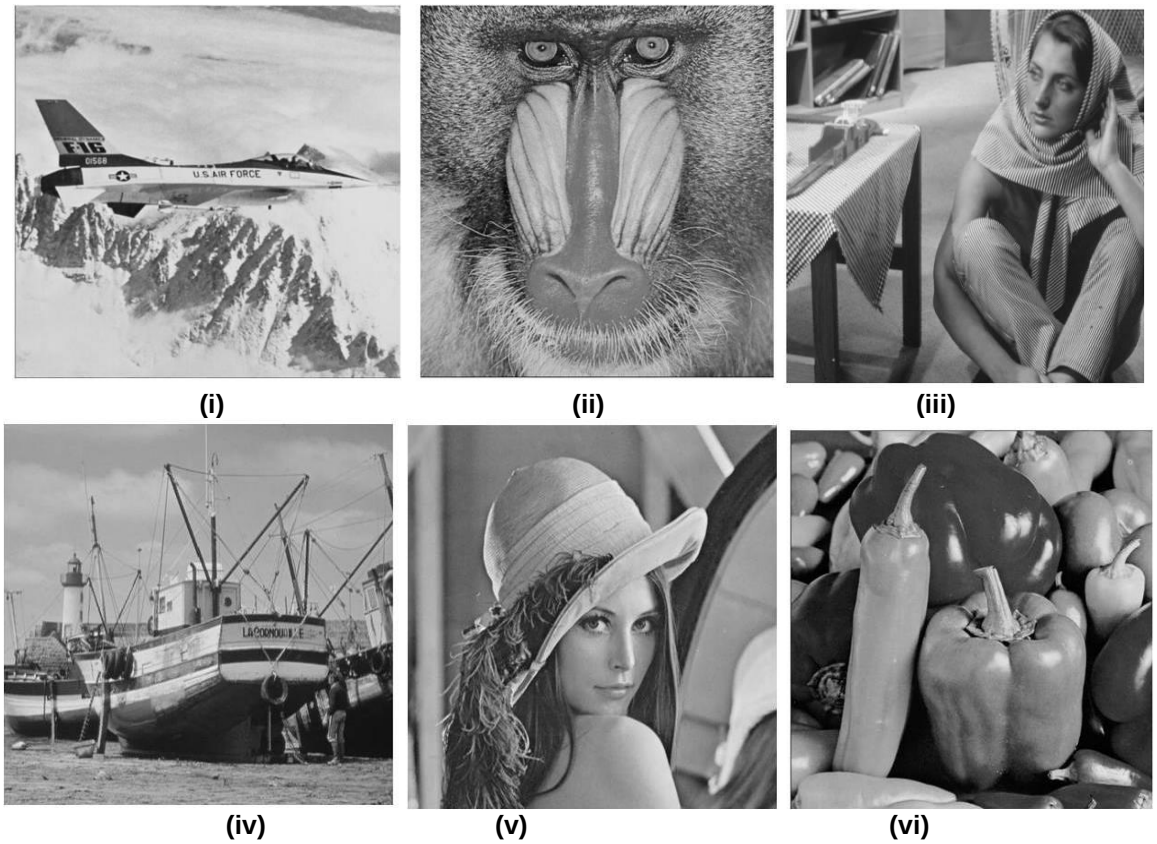


Figure 9. (i) Airplane (ii) Baboon (iii) Barbara (iv) Boat (v) Lenna (vi) Peppers

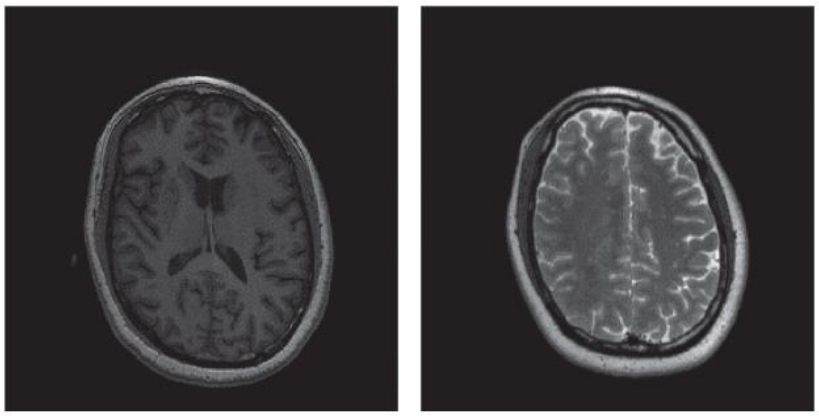
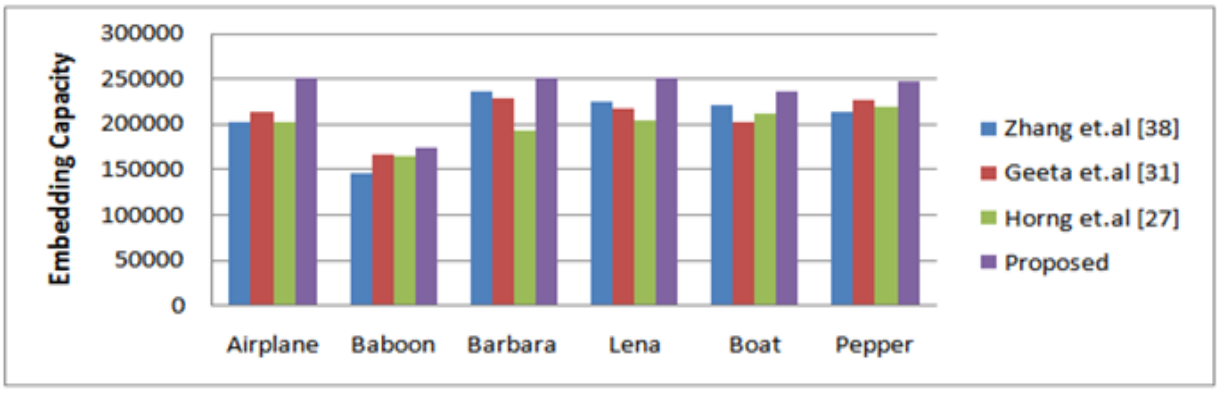


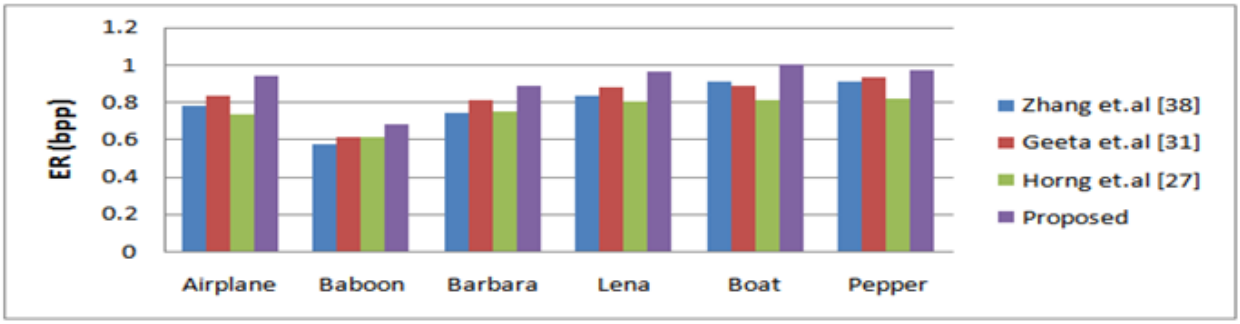
Figure 10. (i) Medical Image X (ii) Medical Image Y

Table 3: Comparison with state-of-the-art method (6 images)

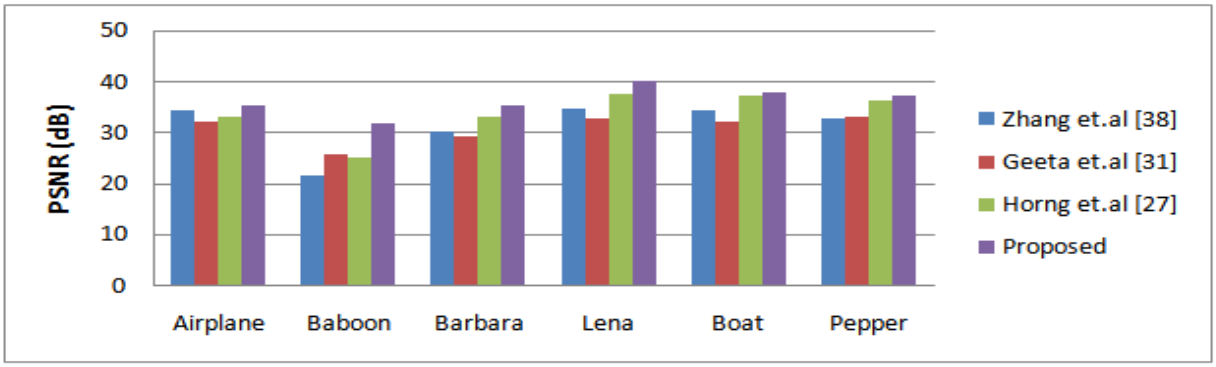
Image	Metrics	Zhang [38]	Geeta [31]	Horng [27]	Proposed
Airplane	EC	201456	212514	202715	250160
	ER(bpp)	0.78	0.83	0.73	0.94
	PSNR	34.28	32.18	33.15	35.12
	SSIM	0.9356	0.9551	0.9821	0.9132
Baboon	EC	145694	166494	163427	173262
	ER(bpp)	0.57	0.61	0.61	0.68
	PSNR	21.36	25.60	25.10	31.80
	SSIM	0.9648	0.9485	0.9520	0.9293
Barbara	EC	235894	228894	192703	251241
	ER(bpp)	0.74	0.81	0.75	0.89
	PSNR	30.23	29.31	33.12	35.14
	SSIM	0.9745	0.9451	0.9801	0.9112
Lena	EC	223698	216498	204345	251684
	ER(bpp)	0.83	0.88	0.80	0.96
	PSNR	34.56	32.61	37.42	39.95
	SSIM	0.9658	0.9781	0.9898	0.9162
Boat	EC	221235	202215	211102	235421
	ER(bpp)	0.91	0.89	0.81	1.00
	PSNR	34.21	32.02	37.15	37.89
	SSIM	0.9745	0.9651	0.9801	0.9398
Pepper	EC	213658	226178	218242	246249
	ER(bpp)	0.91	0.93	0.82	0.97
	PSNR	32.56	33.06	36.21	37.24
	SSIM	0.9785	0.9655	0.9921	0.9491



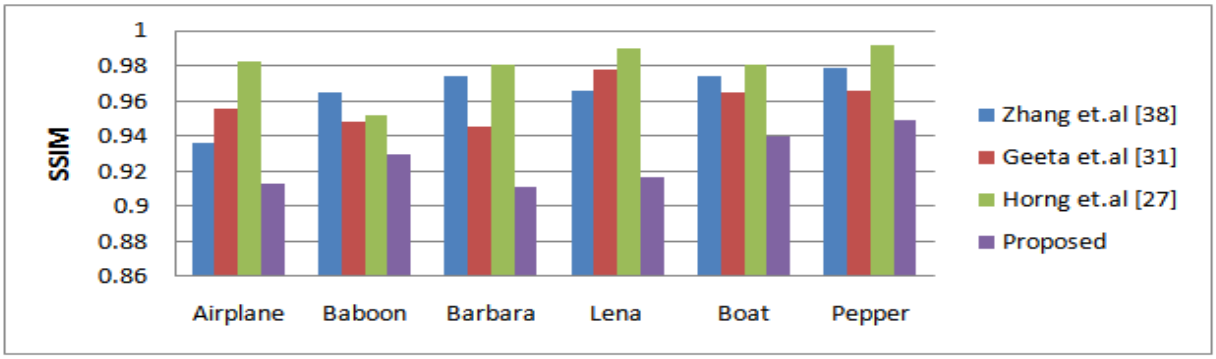
(a)



(b)



(c)



(d)

Figure 11. Comparison of (a) EC (b) ER (c) PSNR (d) SSIM for various images airplane, baboon, barbara, leena, boat and pepper

Table 4: Comparison with state-of-the-art method (Medical image)

Image	Metrics	Zhang [38]	Geeta [31]	Horng [27]	Proposed
Medical Image X	Capacity	56898	60457	57824	62236
	ER(bpp)	0.90	0.93	0.92	1
	PSNR	37.62	36.25	36.14	39.12
	SSIM	0.9754	0.9804	0.9931	0.9624
Medical Image Y	Capacity	56894	59914	55309	62938
	ER(bpp)	0.92	0.94	0.88	0.97
	PSNR	33.25	34.14	34.39	36.31
	SSIM	0.9854	0.9747	0.9893	0.9678

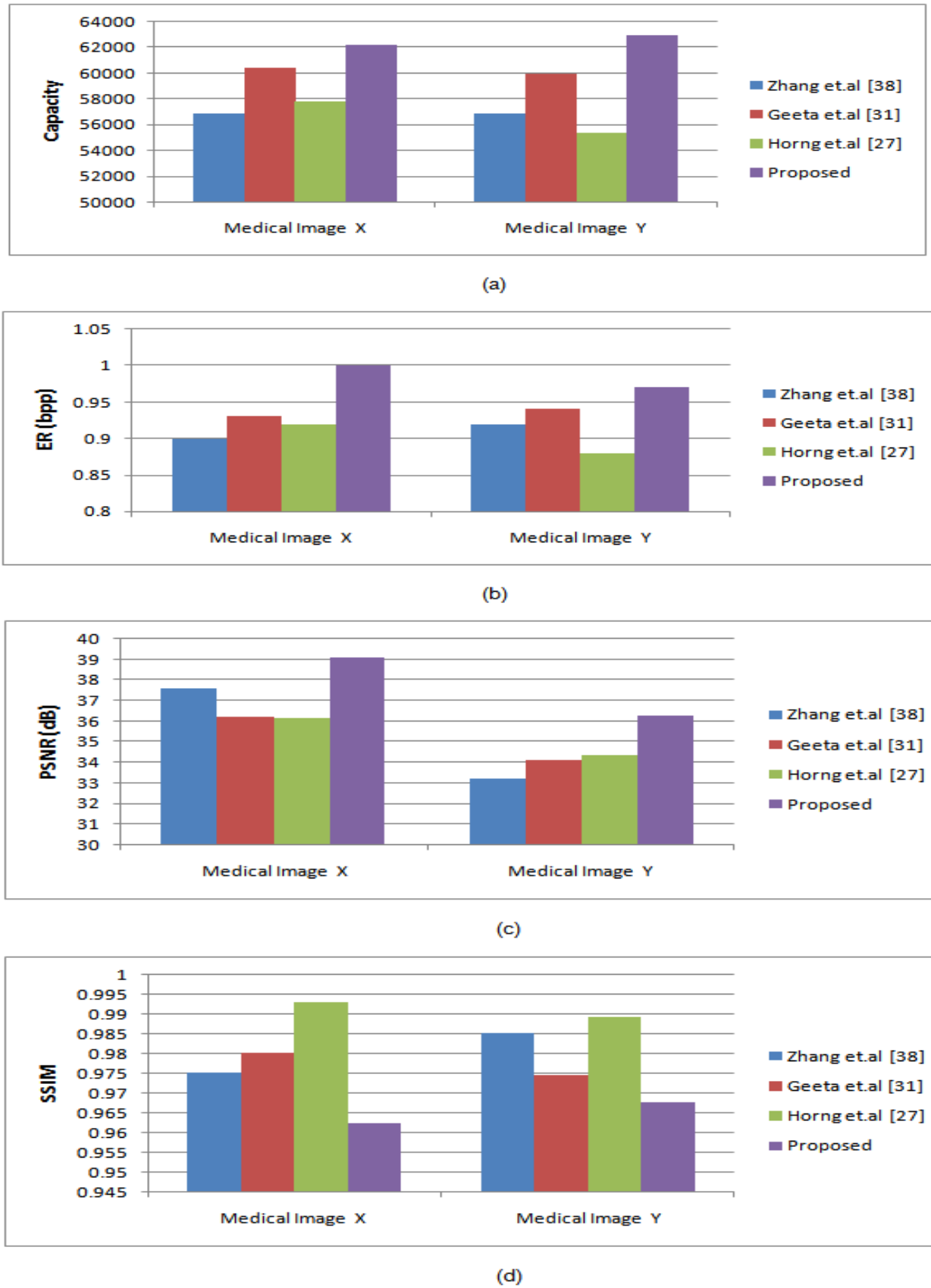


Figure 12. Comparison of (a) EC (b) ER (c) PSNR (d) SSIM for Medical Image A and B

blockchain technology for encryption and the proposed RDH mechanism to conceal patient electronic health records in the cover picture. The unique interpolation method and HS mechanism form the foundation of the suggested data hiding system. Three keys—key_1, key_2, and key_3—form the basis of the blockchain system. This makes the suggested system resistant to outside attack. .

The outcomes are displayed in a medical image as well as in a well-known image database. Various performance metrics are used to determine the results. It is found that the presented method is more effective than the state-of-the-art method in terms of EC, bpp, SSIM and PSNR. Future research can look into stronger interpolation techniques that could be combined with the HS process

References

[1] M. G. R. Alam, M. S. Munir, M. Z. Uddin, M. S. Alam,T. N. Dang, and C. S. Hong, "Edge-of-things computing

[2] framework for cost-effective provisioning of healthcare data,"*Journal of Parallel and Distributed Computing*, vol. 123,pp. 54–60, 2019.

[3] Y. Yang, X. Xiao, X. Cai, and W. Zhang, "A secure and high visual-quality framework for medical images by contrast enhancement reversible data hiding and homomorphic encryption,"*IEEE Access*, vol. 7, pp. 96900–96911, 2019..

[4] Y. Yang, X. Xiao, X. Cai, and W. Zhang, "A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images," *IEEE Signal Processing Letters*, vol. 27, pp. 256–260, 2020.

[5] J.-J. Li, C.-F. Lee, C.-C. Chang, J.-Y. Lin, and Y.-H. Wu, "Reversible data hiding scheme based on quad-tree and pixel value ordering," *IEEE Access*, vol. 7, pp. 142947–142962, 2019.

[6] F. Aziz, T. Ahmad, A. H. Malik, M. I. Uddin, S. Ahmad, and M. Sharaf, "Reversible data hiding techniques with high message embedding capacity in images," *PLoS One*, vol. 15, Article ID e0231602, 2020.

[7] Yaghobi, Shabnam Rahber, and Hedieh Sajedi. "Text steganography in webometrics." *International Journal of Information Technology* 13, no. 2 (2021): 621-635.

[8] Z. Wang, N. Luo, and P. Zhou, "Guardhealth: blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare," *Journal of Parallel and Distributed Computing*, vol. 142, pp. 1–12, 2020.

[9] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-PBFT: an EigenTrustbased practical Byzantine fault tolerance consensus algorithm,"*China Communications*, vol. 16, no. 12, pp. 111–123, 2019.

[10] Hwang, J.H., Kim, J.W., Choi, J.U., 2006. A reversible watermarking based on histogram shifting. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 4283 LNCS, 348–361. https://doi.org/10.1007/11922841_28.

[11] Kuo, W.C., Jiang, D.J., Huang, Y.C., 2007. Reversible data hiding based on histogram. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 4682 LNAI, 1152–1161. https://doi.org/10.1007/978-3-540- 74205-0_119.

[12] Li, X., Zhang, W., Gui, X., Yang, B., 2015. Efficient reversible data hiding based on multiple histograms modification. IEEE Trans. Inf. Forensics Secur. 10, 2016–2027. https://doi.org/10.1109/TIFS.2015.2444354.

[13] Pan, Z., Gao, X., Wang, L., Gao, E., 2020. Effective reversible data hiding using dynamic neighboring pixels prediction based on prediction-error histogram. Multimed. Tools Appl. 79, 12569–12595. https://doi.org/10.1007/s11042-019-08335-0.

[14] Wang, J., Mao, N., Chen, X., Ni, J., Wang, C., Shi, Y., 2019. Multiple histogramsbased reversible data hiding by using FCM clustering. Signal Process. 159, 193–203. https://doi.org/10.1016/j.sigpro.2019.02.013.

[15] Alattar, A.M., 2004. Reversible watermark using difference expansion of quads, in:ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing – Proceedings

[16] Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Technol. 13, 890–896. https://doi.org/10.1109/TCSVT.2003.815962

[17] Wang, W., Ye, J., Wang, T., Wang, W., 2017. Reversible data hiding scheme based on significant-bit-difference expansion. IET Image Process. 11, 1002–1014. https://doi.org/10.1049/iet-ipr.2017.0151.

[18] Liu, Y.C., Wu, H.C., Yu, S.S., 2011. Adaptive DE-based reversible Steganographic technique using bilinear interpolation and simplified location map. Multimed. Tools Appl. 52, 263–276. https://doi.org/10.1007/s11042-010-0496-0.

[19] Chang, C.C., Lin, C.Y., Fan, Y.H., 2008. Lossless data hiding for color images based on block truncation coding. Pattern Recogn. 41, 2347–2357. https://doi.org/10.1016/j.patcog.2007.12.009.

[20] Lu, Z.M., Wang, J.X., Liu, B.B., 2009. An improved lossless data hiding scheme based on image VQ-index residual value coding. J. Syst. Softw. 82, 1016–1024. https://doi.org/10.1016/j.jss.2009.01.010

[21] Lin, C.C., Liu, X.L., Tai, W.L., Yuan, S.M., 2015. A novel reversible data hiding scheme based on AMBTC compression technique. Multimed. Tools Appl. 74, 3823–3842. https://doi.org/10.1007/s11042-013-1801-5.

[22] Lee, C.F., Huang, Y.L., 2012. An efficient image interpolation increasing payload in reversible data hiding. Expert Syst. Appl. 39, 6712–6719. https://doi.org/10.1016/j.eswa.2011.12.019.

[23] Jung, K.H., Yoo, K.Y., 2009. Data hiding method using image interpolation. Comput.Stand. Interfaces 31, 465–470. https://doi.org/10.1016/j.csi.2008.06.001.

[24] Malik, A., Sikka, G., Verma, H.K., 2017. Image interpolation based high capacity reversible data hiding scheme. Multimed. Tools Appl. 76, 24107–24123. https://doi.org/10.1007/s11042-016-4186-4

[25] Chang, Y.T., Huang, C.T., Lee, C.F., Wang, S.J., 2013. Image interpolating based data hiding in conjunction with pixel-shifting of histogram. J. Supercomput. 66,1093–1110. https://doi.org/10.1007/s11227-013-1016-6.

[26] Sah, Basant, and Vijay Kumar Jha. "Reversible data hiding technique using novel interpolation technique and discrete

cosine transform." *International Journal of Integrated Engineering* 11, no. 1 (2019).
[27] Ma, Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li."Reversible data hiding in encrypted images by reserving room before encryption."*IEEE Transactions on information forensics and security* 8, no. 3 (2013): 553-562.
[28] Horng, Ji-Hwei, Ching-Chun Chang, Guan-Long Li, Wai-Kong Lee, and Seong Oun Hwang. "Blockchain-Based Reversible Data Hiding for Securing Medical Images." *Journal of Healthcare Engineering* 2021 (2021).
[29] Parah, Shabir A., Farhana Ahad, Javaid A. Sheikh, and Ghulam Mohiuddin Bhat. "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique." *Journal of biomedical informatics* 66 (2017): 214-230.
[30] Chen, Yung-Yao, and Kuan-Yu Chi. "Cloud image watermarking: high quality data hiding and blind decoding scheme based on block truncation coding." *Multimedia Systems* 25, no. 5 (2019): 551-563.
[31] Loan, Nazir A., Shabir A. Parah, Javaid A. Sheikh, Jahangir A. Akhoon, and Ghulam M. Bhat. "Hiding electronic patient record (EPR) in medical images: a high capacity and computationally efficient technique for e-healthcare applications." *Journal of biomedical informatics* 73 (2017): 125-136.
[32] Geetha, R., and S. Geetha. "Embedding electronic patient information in clinical images: an improved and efficient reversible data hiding technique." *Multimedia Tools and Applications* 79, no. 19 (2020): 12869-12890.
[33] Yang, Yang, Weiming Zhang, Dong Liang, and Nenghai Yu. "A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images." *Multimedia Tools and Applications* 77, no. 14 (2018): 18043-18065.
[34] Gao, Guangyong, Shikun Tong, Zhihua Xia, Bin Wu, Liya Xu, and Zhiqiang Zhao. "Reversible data hiding with automatic contrast enhancement for medical images." *Signal Processing* 178 (2021): 107817.
[35] Balasamy, K., and S. Suganyadevi. "A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD." *Multimedia tools and applications* 80, no. 5 (2021): 7167-7186.
[36] Liu, Yuling, Xinxin Qu, and Guojiang Xin. "A ROI-based reversible data hiding scheme in encrypted medical images." *Journal of Visual Communication and Image Representation* 39 (2016): 51-57.
[37] Zhang, Shun, Tiegang Gao, and Lin Gao. "A novel encryption frame for medical image with watermark based on hyperchaotic system." *Mathematical Problems in Engineering* 2014 (2014).
[38] Ahmad, Khaleel, and Md Shoaib Alam. "E-commerce security through elliptic curve cryptography." *Procedia Computer Science* 78 (2016): 867-873.
[39] Zhang, Ru, Chunjing Lu, and Jianyi Liu. "A high capacity reversible data hiding scheme for encrypted covers based on histogram shifting." Journal of Information Security and Applications 47 (2019): 199-207.
[40] Jin, Hao, et al. "A review of secure and privacy-preserving medical data sharing." IEEE Access 7 (2019): 61656-61669.
[41] Alvi, Ashik Mostafa, et al. "An adaptive image smoothing technique based on localization." Developments of Artificial Intelligence Technologies in Computation and Robotics: Proceedings of the 14th International FLINS Conference (FLINS 2020). 2020.
[42] Kaissis, Georgios A., et al. "Secure, privacy-preserving and federated machine learning in medical imaging." Nature Machine Intelligence 2.6 (2020): 305-311.
[43] Alvi, Ashik Mostafa, et al. "An adaptive grayscale image de-noising technique by fuzzy inference system." 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD). IEEE, 2017.
[44] Zhang, Mingwu, Yu Chen, and Jingqiang Lin. "A privacy-preserving optimization of neighborhood-based recommendation for medical-aided diagnosis and treatment." IEEE Internet of Things Journal 8.13 (2021): 10830-10842.
[45] Singh, Ravinder, et al. "Investigation of social behaviour patterns using location-based data–a melbourne case study." EAI Endorsed Transactions on Scalable Information Systems 8.31 (2020).
[46] Vimalachandran, Pasupathy, et al. "The Australian PCEHR system: ensuring privacy and security through an improved access control mechanism." arXiv preprint arXiv:1710.07778 (2017).
[47] Ge, Yong-Feng, et al. "MDDE: multitasking distributed differential evolution for privacy-preserving database fragmentation." The VLDB Journal 31.5 (2022): 957-975.
[48] Chenthara, Shekha, et al. "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology." Plos one 15.12 (2020): e0243043.
[49] Yin, Jiao, et al. "Knowledge-driven cybersecurity intelligence: software vulnerability co-exploitation behaviour discovery." IEEE Transactions on Industrial Informatics (2022).