Received: September 3, 2021. Revised: October 7, 2021. 678

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Reversible Watermarking Using Hyperchaotic System for Secure Image Transmission

Veena Seenappa[1,3*] Narayanappa Chikkajala Krishnappa[1] Pradeep Kumar Mallesh[2,3]

[1]*Department of Medical electronics, MS Ramaiah Institute of Technology, Bangalore, India*
[2]*Department of Electrical and Computer Engineering, Indian Institute of Science, Bangalore, India*
[3]*S.J.C. Institute of Technology, Chickballapur, India*
* Corresponding author's Email: veenasdl@gmail.com

Abstract: In telemedicine applications, the images pertaining to medicines and diseases can undergo tampering and forging, where it increases risk in diagnosis. The reversible watermarking technique is capable to extract the embedded information and retrieve the original images completely from watermarked images. It has some specific features like lower distortion of images and high capacity of payload. To solve such an issue, a reversible watermarking method is proposed to provide security for the medical images using hyperchaotic with Deoxyribonucleic Acid (DNA) sequence. The proposed reversible watermarking method utilized standard images (lena, Barbara, boat and medical images) for encryption and decryption. Discrete Wavelet Transform (DWT) and Inverse Discrete Wavelet Transform (IDWT) are used to compress the cover images and to decompress the stego images. Further, the thresholding with morphological transform is employed for segmentation of Region of Interest (RoI) in secret images. In addition, the encryption and decryption of secret image is done by hyperchaotic system with DNA sequence. Lastly, the embedding and extraction of secret images and cover images from the stego images is performed by reversible watermarking with differential expansion and modulus function. Simulation result shows that the proposed reversible watermarking method achieved Peak Signal to Noise Ratio (PSNR) of 99 dB for secret image construction, which is better compared to other traditional watermarking techniques.

Keywords: Hyperchaotic, Medical images, Reversible watermarking, Security, Telemedicine.

1. Introduction

In recent times, Telemedicine potentially provide convenient medical services to patients. However, the medical images (transmitted via network) present in the application can easily be forged or tampered, thereby increasing the risk of misdiagnosis [1, 2]. So, data protection is needed during the transmission through an unsecured medium. Information hiding is the art of protecting the information in a secured manner. Steganography and watermarking methods are two main categories of Information hiding [3, 4]. The watermarking is considered a process of making information imperceptible, where it changes a work to embed information related to the particular work. In medical image, watermarking is quite challenging. Some essential constraints must be considered while executing watermarking process. The embedding information in the host image causes distortion. This might make medical images imprudent for the physicians [5, 6]. So, encryption methods are widely used to protect confidential information, some of the desirable functionality might be un-realizable for data encryption [7, 8].

Watermarking technique has two classes – one can be reversed while the other one is irreversible. In irreversible watermarking, lossless recovery of host image is impossible, but the lossless recovery of host image is possible in reversible watermarking, where host images are recovered to their pristine state [9]. Hence, the reversible watermarking is more suitable for medical images [10, 11], where it can extract the embedded sentence and completely retrieve the original image from an image, which is watermarked. It also has some desirable features such as low image

distortion and high payload capacity [12]. Although, the reversible watermarking schemes are easy to implement, the compression rate of Least Significant Bits (LSBs) are less and it confines the embedding capacity. [13].

To solve this problem, a reversible watermarking method is proposed for constructing stego images and reconstructing cover and secret images. Though, the major contributions of this study are given as follows. In this work, medical images and multimedia images like lena, pepper, boat, barbara, and cameraman are considered as input images. Further, DWT method is used to compress the cover image and IDWT method is used to decompress the stego image. In this study, the DWT coefficient is same as host image, so it is easy to compress the images that reduces the system complexity. Next, thresholding with morphological transform is used for the RoI segmentation of secret images to achieve better watermarking performance. Further, hyperchaotic system with DNA sequence is used for image encryption and decryption process. In addition to this, the extraction of secret image and cover image from the stego image is carried out using reversible watermarking with differential expansion and modulus function. Uncertainty and randomness are improved in the hyperchaotic process, which is simple and more efficient. In this work, the key space becomes large, while the intricacy of security systems increases, so it provides better protection with DNA sequences. A few papers on image watermarking are reviewed in Section 2. Mathematical explanation of the proposed model is given in Section 3. In Section 4, quantitative and comparative evaluation of the proposed model is given. In Section 5, Conclusion of this research work is detailed.

2. Literature review

In telemedicine, medical images are required to be transmitted without any loss along with maintaining the data privacy. Reversible watermarking technique is applied to protect the data privacy of medical and multimedia images. Some recent notable researches in reversible watermarking methods are reviewed in this section.

Selvam [14] developed a new reversible watermarking technique for medical images without any additional key information. The hybrid reversible watermarking algorithm was applied for increasing the embedding capacity. The Discrete Gould Transform (DGT) and Integer Wavelet Transform (IWT) were employed to secure watermarking of the medical images. On the sender side, the DGT was used to embed watermark information within wavelet subband. On the receiver side, the embedded watermark was extracted. The results showed that the developed method has higher robustness, capacity, and reversibility. The slightest increase in the rate of embedding embedded sharply decreases the PSNR value of the hybrid method.

Liu [15] applied Recursive Dither Modulation (RDM) method to avoid any kind of influence on the diagnosis of the reversible watermarking method. Singular value decomposition and slantlet transform were applied with RDM to provide a reliable solution for protecting the image authenticity. The watermark was embedded in all the medical images to avoid risk caused by spatially segmenting images. Simulation result showed that the developed method has better performance in reversible watermarking techniques. Embedding capacity of the developed method was low, where the robustness of the method was required to be increased.

Rahman [16] applied a chaotic key to select some of the pixels from the host image to generate the watermark chaotically embedded in the image. The Residual Number System (RNS) was used to convert the rest of the pixels to residual. The polynomial was applied to represent chaotically selected images. The obtained remainder was operated using the XOR gate and the watermark. Lastly, it was appended along with the images. On the receiver's side, the appended received messages that were divided with a similar primitive polynomial and calculates the remainder. The results showed that the developed method has higher performance, due to the four keys used in a chaotic map. The simulation analysis showed that embedded capacity of the presented method was low.

Balsamy [17] applied wavelet decomposition and Particle Swarm Optimization (PSO) for medical image authentication. The medical image was treated with wavelet transformation with the other image, which was treated with a tent map and a hash function for protecting the secret watermark. The chaotic map encryption sequences were operated on the binary-coded image, where PSO provides optimal balance among embedding capacity. The developed method has the advantage of identifying the optimal wavelet coefficient based on PSO and apply features to embed the watermark. Developed model has watermarking with low distortion for secrete information. The PSO has the limitation of a trap into local optima.

Lee [18] developed a new reversible watermarking method for the medical system to preserve the quality of medical images. The object and background region was segmented and estimated by the error expansion that was applied for reverse watermarking method. After extraction of a watermark, the original image was reconstructed without any quality degradation. A technique of pre-

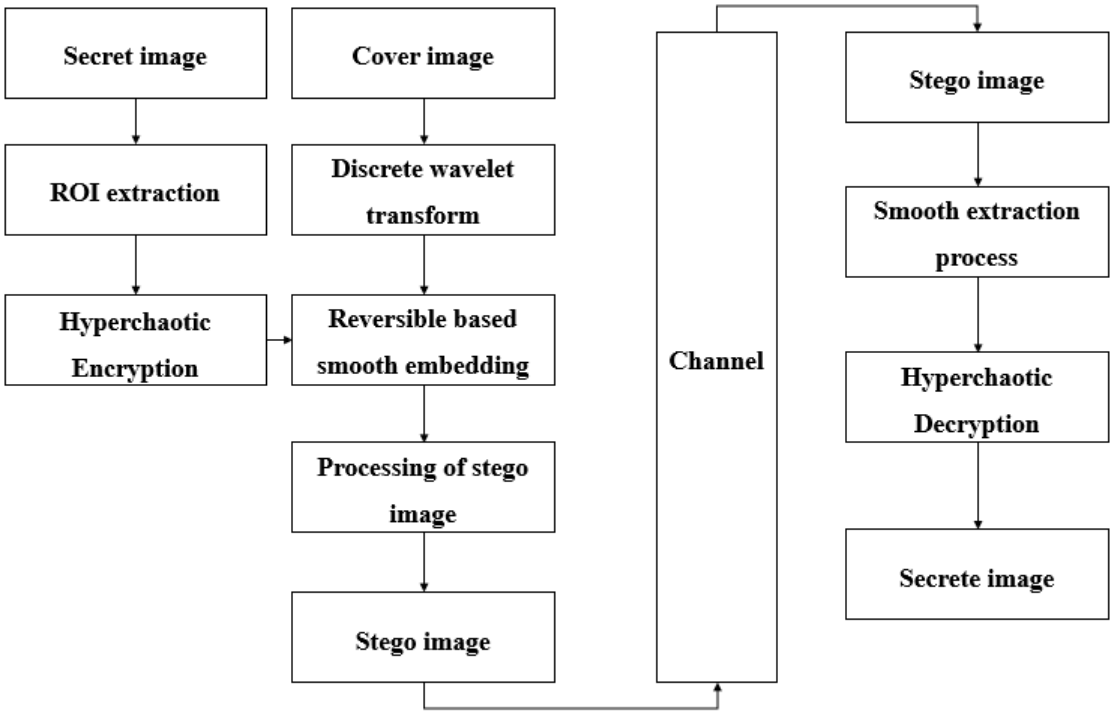

Figure. 1 Block diagram of proposed reversible water marking method

compensation of errors was used to solve inherent over and underflow problems. The result showed that the developed model has higher performance in medical images. Still, the quality of reconstructed image was required to be improved.

Venugopal and Reddy [19] presented a multipurpose watermarking technique for an effective encryption. Initially, the cover image was converted into wavelet domain using IWT technique. Then, a chaotic logistic map was used to encrypt the images, and then rivest–shamir–adleman and LSB were utilized to locate the watermarked region and to enhance the security with higher computation efficiency and better embedding capacity. Setyono and Setiadi [20] has combined two transformations such as tchebichefand singular value decomposition and Arnold's technique for improving the visual ability and security of the images. Arnold's technique was applied in the cover images in order to spread watermark, and further the cover images were categorized into smaller block and transformed using Tchebichef. The low coefficient of every Tchebichef block was collected in a matrix for decomposition, and then the watermark was embedded in the singular matrix. The main problem in the developed methods were stealth effects in the presence of message. For addressing the aforementioned issues, a new model is proposed in this research paper.

3. Proposed methodology

For secure transmission of images, a reversible watermarking method is proposed for constructing stego images and reconstructing cover as well as secret images. The standard database like Lena, Pepper, Boat, Barbara, Cameraman, and medical images are considered as cover images and secret images. Uncertainty and randomness are improved in the hyperchaotic process, it not only simpler but efficient. Here, the key spaces are larger and the security of a system is intricate. Due to this, better protection with DNA sequence is obtained. The block diagram for construction of stego image and reconstruction of cover and secret image from stego image is shown in Fig. 1.

To verify the proposed reversible watermarking method, the standard database like Lena, Pepper, Boat, Barbara, Cameraman and medical images are considered as cover images and secret images. The processes of construction of stego images and reconstruction of cover as well as secret images are explained below.

3.1 Compression and decompression

The DWT is utilized in the proposed method to compress the cover images. The IDWT is utilized to decompress the stego images so that the cover image

is obtained. The lifting process is based on the spatial construction of wavelet that includes three steps like splitting, predicting, updating the lift process and normalization. The lifting wavelet is also known as second form of wavelet where the principle is to break the multiple phase of matrices. For filters of wavelet to the sequence of lower and upper triangular matrices that converts the implementation into banded multiplications of a matrix. The finite response of impulsive filter wavelet is divided into lifting process and lifting step. The lifting process is a non-unique process.

Let $\bar{h}(z)$ and $\bar{g}(z)$ denotes low pass and high pass filters of analysis, $h(z)$ and $g(z)$ which are the low and high pass synthesis filters. The compression phase and reconstruction phase are carried out using Eqs. (1, 2).

$$\bar{p}(z) = \begin{bmatrix} \overline{h_e}(z) & \overline{h_o}(z) \\ \overline{g_e}(z) & \overline{g_o}(z) \end{bmatrix} \quad (1)$$

$$p(z) = \begin{bmatrix} h_e(z) & h_o(z) \\ g_e(z) & g_o(z) \end{bmatrix} \quad (2)$$

where, $h_e(z)$ and $h_o(z)$ represent the even and odd parts of the low pass of wavelet filters. If $\overline{g_e}(z)$ and $\overline{g_o}(z)$ are the pair of complementary filters for each other and $\bar{p}(z)$is factorized by the process of lifting by using Eq. (3).

$$\bar{p}(z) = \begin{pmatrix} K & 0 \\ 0 & \frac{1}{K} \end{pmatrix} \prod_{i=1}^{m} \left\{ \begin{pmatrix} 1 & s_i(z) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ f_i(z) & 1 \end{pmatrix} \right\} \quad (3)$$

where K is a constant. It is considered as a scaling factor, i.e., equal to 1. $s_i(z)$ and $f_i(z)$ are equal to $(1 \leq i \leq m)$ which are Laurent polynomials in the lower order. The evaluation of the upper triangular matrix is called primal lifting which is referred to as lifting of lower pass sub-bands by utilizing higher pass sub-band.

3.2 Segmentation

The secret images are considered into the process of Region of Interest which is segmentation using thresholding with morphological transform. To extract the region of interest from the images, the process is to break up the images into segments that can be considered for further processing that is called as segmentation. Morphological transformation operations are carried out based on image shape which is performed on binary images. The functions used in morphological transformations are erosion, dilation, and hit or miss transformation. The cascaded applications are the special cases in morphological transformation. The operations are based on binary images in the pixels like 0 or 1 where the images are 0 is black and 1 is white. The morphological operations are utilized on the grayscale images of the dataset.

Dilation is the relation between image X and structuring element Bin. One element from the images is added to another single element in set B, in the process of vector addition. After the process of dilation, the process of extra boundary is included in the object which is utilized to reduce the noise of internal features.

Erosion is the relation between image X and structuring element B in where every element from the images are subtracted with all the elements in B set which vector subtraction. After the process of erosion, the extra boundary is added to the object by removing dilation to reduce the external noise. The procedure involved in the process of morphological transformation with thresholding is explained below:

- The foreground region/forefront object is labeled with one color and the background region/subject is labeled with another color. The regions which are not sure of anything labeled it with 0 which is a marker.
- Finally, the marker will be updated with the labels and the boundaries of objects will have a value of -1.

3.3 Encryption and decryption

The process of the secret image of encryption and decryption are encrypted by secret images takes place using the hyperchaotic system with DNA sequence. The hyperchaotic is developed from the chaos. The difference between both of them is that the hyperchaotic process includes two or more Lyapunov exponents which are not seen in the former process. The uncertainty and randomness are improved in the hyperchaotic process which is simpler and highly efficient where the key spaces are larger and complexity of security is more which results in higher security protection with DNA sequence. Due to the presence of larger space for key and non-linearity behavior, more complexity was seen. The hyperchaotic system is adopted using the following non-linear Eqs. (4-7).

$$x_1 = a(x_2) + \lambda_1 x_4 \quad (4)$$

$$x_2 = \varepsilon x_1 - x_1 x_3 + \lambda_2 x_4 \quad (5)$$

$$x_3 = -\beta x_3 + x_1 x_2 + \lambda_3 x_4 \quad (6)$$

$$x_4 = -\tau x_1 \quad (7)$$

where, the x_1, x_2, x_3 and x_4 are the non-linear function of hyperchaotic systems. The parameters a, ε, β, τ, λ_1, λ_2 and λ_3 are the systems control parameters.

In DNA encoding, the sequence of DNA includes four nuclei acid bases like Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). A and T, C and G are interrelated with each other due to the binary digits such as 1 and 0 also complementary and utilize two bits of binary digits to represent the base of DNA. There are 24 types of rules to represent in that only 8 types of rules satisfy the complement rule of Watson-crick. In DNA computing the process of addition and subtraction is carried out using the traditional approach of binary addition and subtraction. The pseudo-randomness of the hyperchaotic system is stronger and the sequence includes good statistical properties. The generation of hyperchaotic sequence system includes four steps which are explained in the following:

Step 1: The system of hyperchaotic is iterated again for the N_o times in order to delete the effects adversely and to improve security.

Step 2: After reiterating N_o times, again the system is undergone iteration for $m \times n$ time. The j is utilized to describe the index of iteration. In every j iteration the values of four states like $\{x_1^j, x_2^j, x_3^j, x_4^j\}$are stored.

Step 3: At the time of iteration, every value of state x_i^j are utilized in order to develop the two key unique values like $(S_i^a)^j \in [0,255]$, where i=1, 2, 3, 4 and $\left(S_i^b\right) \in [0,255]$ which are evaluated by utilizing the Eqs. (8-9).

$$(S_i^a)^j = mod\{[[(|x_i^j| - |x_i^j|]) \times 10^{15}]/10^8]\ ], 256\}, \mathrm{i} = 1,2,3,4 \quad (8)$$

$$\left(S_i^b\right)^j = mod\{[[(|x_i^j| - |x_i^j|]) \times 10^{15}]/10^8]\ ], 256\}, \mathrm{i} = 1,2,3,4 \quad (9)$$

where, x_i^j is the iteration value of states, $mod(.)$ describes the modulus operation. $[.]$ describes flooring operation which rounds off the elements with the closest integer towards minus and infinity. The values of a key are joined by utilizing the Eq. (10)

$$S^j = [(S_1^a)^j, (S_2^a)^j, (S_3^a)^j, (S_4^a)^j, \left(S_1^b\right)^j, \left(S_2^b\right)^j, \left(S_3^b\right)^j, \left(S_4^b\right)^j \quad (10)$$

where, S_i^a and S_i^b are the two unique key values obtained by Eqs. (8) and (9).

Step 4: After completing the entire process, the concatenations of sequence are undergone using the Eq. (11) to get the k value.

$$k = \{S^1, S^2, \ldots, S^{m \times n}) \quad (11)$$

The process of image encryption is caste by the procedure of following seven steps:

Step 1: The '$m \times n$' describes the size of input image. Scrambling of global bit is carried out by utilizing image *P*in order to get the sequence of b^1 binary.

Step 2: b^1 is encoded to a DNA sequence d^1 by the first DNA coding rule. Additionally, the DNA on each element of d^1 is performed to obtain d^2 using Eqs. (12, 13).

$$d_1^2 = d_0 + d_1^1 \quad (12)$$

$$d_i^2 = d_{i-1}^2 d_i^1, i \in [2,4,mn] \quad (13)$$

where, $+$ indicates the addition process on DNA and d_0 is a specific value of initial terms.

Step 3: The sequence of $k^s = [k_1, k_2, \ldots., k_{mn}]$ is mined from the$k$, and the sequence of decimal k^s are transformed into the digits of binary such as b^k. The b^k is again encoded into d^k through the third step of the DNA encoding procedure. The addition of DNA among d^2 and d^k are undergone to get a sequence of d^3.

Step 4: The$f(z)$ is the threshold function that is defined by utilizing the Eq. (14).

$$f(z) = \begin{cases} 0, 0 \le \frac{z}{255} \le 0.5 \\ 1, 0.5 < \frac{z}{255} \le 1 \end{cases} \quad (14)$$

A cut sequence of , $[k_1, k_2, \ldots., \mathrm{k}_{4\mathrm{mn}}]$ are formed to mask the sequence of z by utilizing the Eq. (14). The masking of z sequence and d^3 is done to construct d^4 in such a way that whenever $w_i will\ become$ 1 , c d_i^3 will be complemented to get d_i^4 . Otherwise, no change occurs. By this process, d_4 A DNA sequence is obtained.

Step 5: The initial coding rule of DNA is utilized to decode the d_4 to obtain a b_2 a sequence in binary format.

Step 6: The bitwise XOR operation is carried out among the b^2 and b^k to get the binary sequence in cipher format for b^3.

Step 7: The b^3 a binary sequence is transformed into an image of cipher Q.

The process of decryption is similar to the encryption process but in reverse order.

3.4 Embedding and Extraction

Embedding of secret encrypted images and the cover image is done to get stego image. Similarly, the extraction of secret images and cover images from stego images is carried out using reversible watermarking with differential expansion and modulus function.

To store stego quality, secret information will not be hidden with values that are out among both ranges. The process of embedding is considered from a differential equation where the algorithms for the process of extraction are unique. The modulus functions are combined with the established extraction method to obtain the outcome of the process straightly. The proposed method removes the complexity by hiding secret information. To evaluate the effectiveness of the proposed approach, specific steps are needed to maintain the secrecy of the information while extracting it. For the data hiding process, an algorithm of embedding is an essential step in the established method. The complete process is explained below:

Step 1: Segmenting the cover images into the blocks such as 2×1 in the size.

Step 2: Calculating the difference among pixels in every block which preserves the values in d_{arr}array by utilizing the Eq. (15). The z and$y$ are the pair that describes pixels in every block and $d$is the difference that is analyzed.

$$d = z - y \tag{15}$$

where, d is the difference between the blocks, z and y are the pixel pairs in every blocks.

Step 3: Iteration of an array in sequential order to obtain each value that satisfies the embedding condition. To find every value to satisfy the initial condition such as $(0 \leq d \leq 2)$ and the second condition such as$(-1 \geq d \geq -2)$. The initial and second conditions are simplified by $(-2 \leq d \leq 2)$ and discarded the value of difference that is out of range.

Step 4: Assigning values to trace the variables to separate every pair is carried out. When the initial and second conditions are satisfied with the bit value of 0 which is assigned for values to trace the variables. 1 bit is utilized to find the pairs that are not able to change or the pairs that include values that are out of range.

Step 5: Obtaining the secret messages is stored in a text file.

Step 6: Using values obtained from step 3, the secret hidden information by utilizing Eq. (16) and modified the differences d^1, in which the b describe the bit of secret data that is concealed by the zero and one such as$b \rightarrow \{0,1\}$.

$$d^1 = d + b \tag{16}$$

Where, d^1 is the modified difference value and b is the secret bit value.

Step 7: Calculated the new z pixel which includes secret bits by utilizing the Eq. (17). The z pixels are utilized to develop the stego image further.

$$z^1 = d^1 + z \tag{17}$$

Where, z^1 is the new pixel value containing bits and d^1 is the modified difference value

The process of extracting hidden data is carried out by utilizing the variables of tracing, estimated in the process of embedding. Initially, for the embedding process, the stego image is segmented into blocks of similar size such as 2×1. The difference among every pair of pixels is calculated by utilizing the Eq. (18). When all values are obtained, the secret information is extracted by utilizing modulus functions and tracing the variables. The cover images are required to be developed again, in the initial condition in Eq. (16) by recovering the original values during variable tracing value of 0 or the next part in the equation is utilized. The original values of pixels are similar to the values of stego pixels. The concealed information and original values of pixels are recovered by employing Eq. (18-20). This is carried out by the initial condition in which the scenarios are a reversal of the one evaluated by the process of embedding. The encrypted and decrypted images are graphically depicted in Fig 2.

$$d^{11} = z^1 - y^1 \tag{18}$$

$$b = d^{11} \; mod \; 2, if \; tracing \; variable = 0 \tag{19}$$

$$\begin{cases} z = z^1 - \left[\dfrac{z^1 - y^1}{2}\right], if \; tracing \; variable = 0 \\ z = z^1 \quad , \quad otherwise \end{cases} \tag{20}$$

3 Results and discussions

In this research, a reversible watermarking

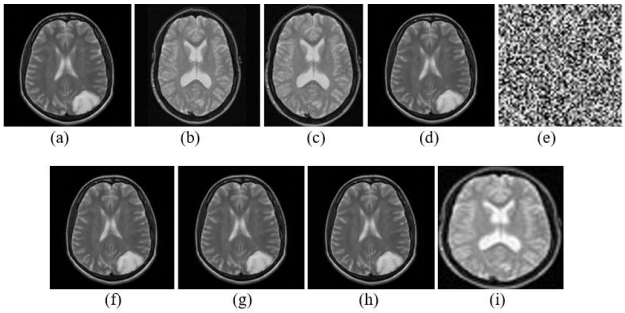

Figure. 2: (a) Cover image, (b) secrete image, (c) segmented secrete image, (d) compressed cover image, (e) encrypted secrete image, (f) stego image, (g) decompressed image, (h) decrypted cover image, and (i) decrypted secrete image

approach is presented for the construction and reconstruction of cover and secret images. The dataset like Lena, Pepper, Boat, Barbara, Cameraman and medical images are considered. The proposed method is evaluated by the MATLAB in windows 10, i7 core processor, 16 GB RAM, and 6 GB 2080Ti NVDIA GTX edition GPU environments. Several performance metrics are considered to evaluate the proposed method, where the quantitative and comparative analysis of the proposed reversible watermarking method is explained in this section.

4.1 Performance metrics

The parameters, considered to evaluate the proposed method for the construction of stego image and reconstruction of cover and secret images are explained below:

Mean square error (MSE)

Mean square error is a common and simple measure for distortion. The MSE among reference which processed image is expressed using Eq. (21).

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ij} - B_{ij}\right)^2 \quad (21)$$

where, A_{ij} and B_{ij} are the value of processed image and reference images, the lesser value of MSE describes the better result.

Peak signal to noise ratio (PSNR)

PSNR is the ratio of the maximum power signal to the power of corrupting noise which is represented in decibel. The higher value of PSNR indicates the reconstruction of higher quality which is represented using Eq. (22).

$$PSNR(db) = 10\log\left(\frac{255^2}{MSE}\right) \quad (22)$$

Structural content (SC)

The structural content metric is used to measure the quality of the reconstructed image. A higher value of SC indicates poor quality and is calculated using Eq. (23).

$$SC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ij}\right)^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(B_{ij}\right)^2} \quad (23)$$

Normalized cross-correlation (NCC)

NCC is the metric used to compare the processed image with a reconstructed image which is expressed using Eq. (24).

$$NCC = \sum_{i=1}^{m}\sum_{i=1}^{n}\frac{A_{ij}\times B_{ij}}{A_{ij}^2} \quad (24)$$

Average difference (AD)

AD is the average change regarding refined image and original image. AD, ideally, needs to be zero. It is calculated by using Eq. (25).

$$AD = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij} - B_{ij}) \quad (25)$$

Normalized absolute error (NAE)

NAE is a measure of quality. A higher value of NAE shows that the image is having of poor quality. It is expressed by using Eq. (26).

$$NAE = \left(\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij}-B_{ij})}{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij})}\right) \quad (26)$$

4.2 Quantitative analysis

The quantitative analysis of the reversible watermarking method (for construction of the stego image and reconstruction of secret image and cover image) is described in this section. The metrics used to analyze the proposed reversible watermarking methods are peak signal to noise ratio, mean square error, average difference, normalized cross-correlation, structural content and normalized absolute error. Table 1 shows the quantitative analysis performance of the proposed reversible watermarking method with a standard dataset.

Table 1 shows the quantitative analysis of the proposed method for a standard dataset like Lena, Barbara, pepper and boat for the construction of stego image and reconstruction of cover as well as secret image.

The result shows that the proposed reversible watermarking method showed PSNR of 61.08 dB for the cover image and 99 dB for a secret image using the lena dataset. Similarly, the proposed reversible

Table 1. The quantitative analysis of the proposed reversible watermarking method for a standard dataset

Standard images		PSNR	MSE	NCC	AD	SC	NAE
Lena	Cover image	61.0839	0.0581	0.9956	**0.0160**	**0.9899**	**0.0059**
	Secret Image	99.0065	0.0082	0.9900	**0.0017**	**0.9950**	**0.0064**
Barbara	Cover image	63.9803	0.0298	0.9938	**0.0148**	**0.9942**	**0.0094**
	Secret Image	99.0054	0.0035	0.9994	**0.0018**	**0.9951**	**0.0010**
Pepper	Cover image	61.0409	0.0545	0.9956	**0.0176**	**0.9937**	**0.0061**
	Secret Image	99.0026	0.0023	0.9998	**0.0079**	**0.9961**	**0.0000**
Boat	Cover image	67.9842	0.0145	0.9970	**0.0001**	**0.9926**	**0.0005**
	Secret Image	99.0076	0.0053	0.9929	**0.0031**	**0.9987**	**0.0034**
Boat	Cover image	63.9928	0.0353	0.9955	**0.0091**	**0.9953**	**0.0055**
	Secret Image	99.0031	0.0092	0.9964	**0.0053**	**0.9930**	**0.0038**

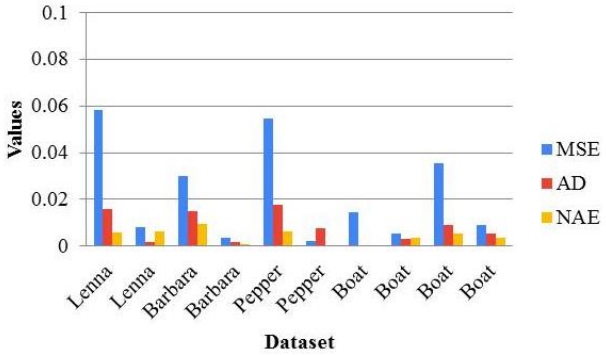

Figure. 3 The quantitative analysis of the proposed reversible watermarking method for a standard dataset in terms of MSE, AD and NAE

Table 2. The quantitative analysis of proposed reversible watermarking method for medical images

Medical Images		PSNR	MSE	NCC	AD	SC	NAE
Ab_1	Cover image	61.0135	0.0539	0.9969	0.0185	0.9920	0.0119
	Secret Image	99.0024	0.0005	0.9906	0.0089	0.9946	0.0021
Ab_2	Cover image	67.9771	0.0188	0.9923	0.0083	0.9940	0.0041
	Secret Image	99.0047	0.0023	0.9994	0.0037	0.9926	0.0033
Ab_3	Cover image	61.0408	0.0526	0.9957	0.0137	0.9949	0.0063
	Secret Image	99.0024	0.0060	0.9918	0.0066	0.9932	0.0025
Boat	Cover image	63.9823	0.0329	0.9944	0.0143	0.9928	0.0063
	Secret Image	99.0092	0.0090	0.9957	0.0037	0.9960	0.0066
Boat	Cover image	61.0547	0.0605	0.9914	0.0187	0.9940	0.0097
	Secret Image	99.0010	0.0052	0.9964	0.0021	0.9957	0.0011

watermarking method achieved an MSE of 0.0581 for the cover image and 0.082 for the secret image of the lena dataset. Then, the NCC of the reversible watermarking method is 0.9956 for the cover image and 0.990 for the secret image, for the lena dataset. The AD shown by the proposed reversible watermarking method, for a cover image is 0.0160 and the secret image is 0.0017. The SC shown by the proposed reversible watermarking method for a cover image is 0.9899 and 0.9950 for a secret image. The NAE shown by the proposed reversible watermarking is 0.0059 for the cover image and 0.0064 for lena standard dataset. The graphical representation of quantitative analysis of the proposed reversible watermarking method for MSE, AD, and NAE with the standard dataset is shown in Fig. 3.

Table 2 shows the quantitative analysis of proposed methods for a medical dataset like Ab_1, Ab_2, and boat for the construction of stego image and reconstruction of cover as well as secret image. This result shows that the proposed reversible watermarking method showed a PSNR of 61.0135 for the cover image and 99.0024 for a secret image using a medical dataset. Similarly, the proposed reversible watermarking method achieved an MSE of 0.0539 for the cover image and 0.0005 for the secret image, for a medical dataset. Then, the NCC of the proposed

Table 3. The quantitative analysis of proposed reversible watermarking method for attacks

Attacks		PSNR	MSE	NCC	AD	SC	NAE
Cropping	Cover image	23.1809	312.8723	0.8000	2.8561	1.2316	0.1760
	Secret Image	19.7320	693.0059	0.8725	2.3643	0.9185	0.1204
Salt & pepper noise	Cover image	26.9468	131.5823	0.9544	0.4277	0.9104	0.0456
	Secret Image	18.6458	888.2448	0.8432	4.1900	0.8672	0.1414
Histogram enhancement	Cover image	14.5139	2302.2489	0.9267	25.1863	0.2291	1.4678
	Secret Image	8.1002	10080.4230	0.3032	46.0117	0.3990	1.1062
Blur	Cover image	41.9933	4.1235	0.9964	0.0017	1.0083	0.0414
	Secret Image	8.1319	10004.0483	0.3072	47.9691	0.3885	1.1098
Rotation	Cover image	22.0277	408.4436	0.7449	0.4600	0.9982	0.4311
	Secret Image	8.0278	10256.4550	0.3002	46.2580	0.4007	1.1145

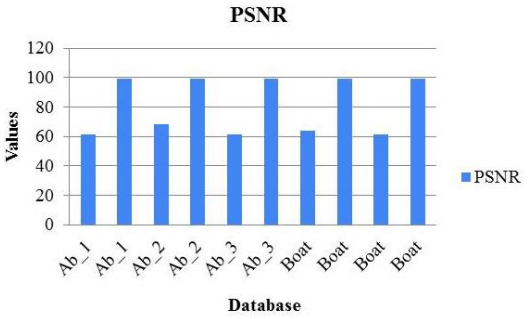

Figure. 4 The quantitative analysis of the proposed reversible watermarking method for a medical dataset in terms of PSNR

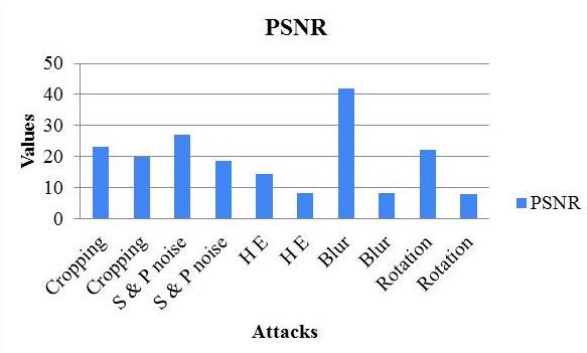

Figure. 5 The quantitative analysis of the proposed reversible watermarking method for attacks in terms of PSNR

reversible watermarking method is 0.9969 for the cover image and 0.9906 for the secret image medical dataset. The AD shown by the proposed reversible watermarking method for a cover image is 0.0185 and the secret image I s0.0089.

The SC shown by the proposed reversible watermarking method for a cover image is 0.9920and 0.9946for a secret image. The NAE shown by the proposed reversible watermarking is 0.0119for cover image and 0.0021for medical dataset. The graphical representation of quantitative analysis of the proposed reversible watermarking method for PSNR with the medical dataset is shown in Fig. 4.

Table 3 shows a quantitative analysis of the proposed method for attacks. Examples of attacks are Cropping, salt & pepper noise, histogram enhancement, blur and rotation. These are seen in the construction of the stego image and reconstruction of cover as well as secret image. This result shows that the proposed reversible watermarking method showed PSNR of 23.1809 for the cover image and 19.7320for the secret image in cropping attack. Similarly, the proposed reversible watermarking method showed an MSE of 131.5823 for the cover image and 888.2448 for a secret image in the case of salt & pepper noise attacks. Then, the NCC of the proposed reversible watermarking method is0.9267for cover image and 0.3032 for a secret image in histogram enhancement attack. The AD shown by the proposed reversible watermarking method for a cover image is 0.0017 where the secret image is47.9691 for blur attack. The SC shown by the proposed reversible watermarking method for a cover image is 0.9982and 0.4007 for a secret image in rotation. The graphical representation of quantitative analysis of the proposed reversible watermarking method for PSNR in attack is shown in Fig. 5.

4.3 Comparative Analysis

The comparative analysis of the proposed reversible watermarking method (for construction of the stego image and reconstruction of secret image and cover image) is compared with the existing methods in this section. Existing methods such as Liu [15], Rahman [16], Balsamy [17] and Venugopal and Reddy [19] are compared with the reversible watermarking method. The performance measures: NCC, MSE, PSNR and Structural Similarity Index (SSIM) are employed to compare the proposed method with existing methods. Tables 4 and 5 shows the comparative analysis of the proposed reversible watermarking method with the existing methods.

Tables 4 and 5 shows a comparative analysis of the proposed method with existing methods for

Table 4. Comparative analysis of proposed reversible watermarking method with the existing methods in terms of NCC and MSE

Metrics	Liu [15]	Rahman [16]	Balsamy [17]	**Proposed Method**
NCC	0.9624	-	0.9499	**0.9964**
MSE	0.0476	0.0728	4.98	**0.0052**

Table 5. Comparative analysis of proposed reversible watermarking method with the existing method in terms of PSNR and SSIM

Methods	PSNR (dB)	SSIM
Venugopal and Reddy [19]	36.25	0.67
Proposed Method	**99**	**0.93**

medical images. The existing Liu [15] method attained a NCC of 0.962 and MSE of 0.0476. Similarly, the existing Rahman[16] method achieved a MSE of 0.0728, and the existing Balsamy [17] method obtained a NCC result of 0.09499 and MSE of 4.98. Additional, the Venugopal and Reddy [19] method achieved a PSNR value of 36.25dB and SSIM of 0.67. However, the proposed method has achieved effective performance than the existing compared methods. The embedding capacity of the Liu [15] and Rahman [16] methods were low but the embedding capacity of the proposed method is effective and improved the roboustness of the system.

The Balsamy [17] method has the limitation of a trap into local optimal with poor performance. However, the proposed method overcomes the issue of existing method and increased the roboutsness of proposed method. Compared to the Venugopal and Reddy [19] method, uncertainty and randomness are improved in the hyperchaotic process, which is simple and highly efficient. So, the key space become large and increase the intricacy of security system.

4 Conclusion

For safeguarding medical images, the reversible watermarking method is proposed for constructing stego images and reconstructing cover and secret images. The standard database like Lena, Pepper, Boat, Barbara, Cameraman and medical images are considered as cover and secret images. The DWT in the lifting scheme is utilized to compress the cover images and IDWT is utilized to decompress the stego images to get a cover image. The secret images are considered in the process of RoI segmentation using thresholding with morphological transform. The process of encrypting secret images and decrypting the same encrypted image takes place using a hyperchaotic system with a DNA sequence. The embedding of secret encrypted images and cover images to get stego images. Similarly, extraction of secret images and cover images from stego images is carried out using reversible watermarking with differential expansion and modulus function. This experimental result shows that the proposed method achieved a higher PSNR value by providing a higher quality of reconstructed images. In future work, the improved encryption and decryption method can be developed to provide more security for images.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first and third author.

The supervision, review of work and project administration, has been done by second author.

References

[1] X. Liu, J. Lou, H. Fang, Y. Chen, P. Ouyang, Y. Wang, B. Zou, and L. Wang, "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images", *IEEE Access*, Vol. 7, pp. 76580-76598, 2019.

[2] P. Selvam, S. Balachandran, S. P. Iyer, and R. Jayabal, "Hybrid transform based reversible watermarking technique for medical images in telemedicine applications", *Optik*, Vol. 145, pp. 655-671, 2017.

[3] M. Arsalan, A. S. Qureshi, A. Khan, and M. Rajarajan, "Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique", *Applied Soft Computing*, Vol. 51, pp.168-179, 2017.

[4] L. Meng, L. Liu, G. Tian, and X. Wang, "An adaptive reversible watermarking in IWT domain", *Multimedia Tools and Applications*, Vol. 80, No. 1, pp. 711-735, 2021.

[5] C. C. Chang, C. T. Li, and Y. Q. Shi, "Privacy-aware reversible watermarking in cloud computing environments", *IEEE Access*, Vol. 6, pp. 70720-70733, 2018.

[6] M. V. Malayil and M. Vedhanayagam, "A novel image scaling based reversible watermarking scheme for secure medical image transmission", *ISA transactions*, Vol. 108, pp. 269-281, 2021.

[7] M. Ishtiaq, W. Ali, W. Shahzad, M. A. Jaffar, and Y. Nam, "Hybrid predictor based four-phase

adaptive reversible watermarking", *IEEE Access*, Vol. 6, pp. 13213-13230, 2018.

[8] M. Ishtiaq, W. Ali, W. Shahzad, M. A. Jaffar, and Y. Nam, "Hybrid predictor based four-phase adaptive reversible watermarking", *IEEE Access*, Vol. 6, pp. 13213-13230, 2018.

[9] H. Zheng, C. Wang, J. Wang, and S. Xiang, "A new reversible watermarking scheme using the content-adaptive block size for prediction", *Signal Processing*, Vol. 164, pp. 74-83, 2018.

[10] M. R. Khosravi and M. Yazdi, "A lossless data hiding scheme for medical images using a hybrid solution based on IBRW error histogram computation and quartered interpolation with greedy weights", *Neural Computing and Applications*, Vol. 30, No. 7, pp. 2017-2028, 2018.

[11] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain", *Optik*, Vol. 208, pp. 164562, 2020.

[12] Z. Zainol, J. S. Teh, and M. Alawida, "A new chaotic image watermarking scheme based on SVD and IWT", *IEEE Access*, Vol. 8, pp. 43391-43406, 2020.

[13] M. Yamni, A. Daoui, H. Karmouni, M. Sayyouri, H. Qjidaa, and J. Flusser, "Fractional Charlier moments for image reconstruction and image watermarking", *Signal Processing*, Vol. 171, pp. 107509, 2020.

[14] P. Selvam, S. Balachandran, S. P. Iyer, and R. Jayabal, "Hybrid transform based reversible watermarking technique for medical images in telemedicine applications", *Optik*, Vol. 145, pp. 655-671, 2017.

[15] X. Liu, J. Lou, H. Fang, Y. Chen, P. Ouyang, Y. Wang, B. Zou, and L. Wang, "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images", *IEEE Access*, Vol. 7, pp. 76580-76598, 2018.

[16] K. Sultan, N. Aldhafferi, A. Alqahtani, and M. Mahmud, "Reversible and fragile watermarking for medical images", *Computational and mathematical methods in medicine*, 2018.

[17] K. Balasamy, and S. Ramakrishnan, "An intelligent reversible watermarking system for authenticating medical images using wavelet and PSO", *Cluster Computing*, Vol. 22, No. 2, pp. 4431-4442, 2019.

[18] H. Y. Lee, "Adaptive reversible watermarking for authentication and privacy protection of medical records", *Multimedia Tools and Applications*, Vol. 78, No. 14, pp. 19663-19680, 2019.

[19] T. Venugopal, and V. S. K. Reddy, "Image watermarking using two level encryption method based on chaotic logistic mapping and Rivest Shamir Adleman algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 6, pp. 271-281, 2018.

[20] A. Setyono and D. R. I. M. Setiadi, "An Image Watermarking Method Using Discrete Tchebichef Transform and Singular Value Decomposition Based on Chaos Embedding", *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 2, pp. 140-150, 2020.