Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2022.017650

ARTICLE

Reversible Watermarking Method with Low Distortion for the Secure Transmission of Medical Images

Rizwan Taj[1], Feng Tao[1,*], Shahzada Khurram[2], Ateeq Ur Rehman[3], Syed Kamran Haider[4], Akber Abid Gardezi[5] and Saima Kanwal[1]

[1]School of Computer and Communication, Lanzhou University of Technology, Lanzhou, China

[2]Faculty of Computing, The Islamia University of Bahawalpur, Bahawalpur, Pakistan

[3]Department of Electrical Engineering, Government College University, Lahore, Pakistan

[4]College of Internet of Things Engineering, Hohai University, Changzhou, China

[5]Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan

[*]Corresponding Author: Feng Tao. Email: fengt@lut.cn

Received: 27 May 2021 Accepted: 14 September 2021

ABSTRACT

In telemedicine, the realization of reversible watermarking through information security is an emerging research field. However, adding watermarks hinders the distribution of pixels in the cover image because it creates distortions (which lead to an increase in the detection probability). In this article, we introduce a reversible watermarking method that can transmit medical images with minimal distortion and high security. The proposed method selects two adjacent gray pixels whose least significant bit (LSB) is different from the relevant message bit and then calculates the distortion degree. We use the LSB pairing method to embed the secret matrix of patient record into the cover image and exchange pixel values. Experimental results show that the designed method is robust to different attacks and has a high PSNR (peak signal-to-noise ratio) value. The MRI image quality and imperceptibility are verified by embedding a secret matrix of up to 262,688 bits to achieve an average PSNR of 51.657 dB. In addition, the proposed algorithm is tested against the latest technology on standard images, and it is found that the average PSNR of our proposed reversible watermarking technology is higher (i.e., 51.71 dB). Numerical results show that the algorithm can be extended to normal images and medical images.

KEYWORDS

LSB; reversible watermarking; medical images security; data distortion

1 Introduction

In the next few decades, digital life is expected to change the e-health care system. With the rapid development of Internet technology, high-speed digital communication increasingly requires more and more medical image transmission. In addition, digital devices must also deal with security vulnerabilities. The e-health system is angering possible security risks, such as eavesdropping and unauthorized access. With the passage of time, digital information has become

an important topic for data security researchers to ensure that this digital content is protected and reliable [1]. Digital watermarking system has been widely used as a data authentication method for transmitting medical data [2–5]. Watermarking technology has the following four key characteristics [6–8]. First, the embedded watermark is robust against various types of attacks. Second, the extracted watermark verifies the provability of copyright ownership by verifying the watermark information. Third, the security feature makes the watermark information unable to be operated by unauthorized personnel. Finally, confidentiality is because the cover image will not cause a large amount of data loss by encoding the watermark. However, the watermarking method may cause a certain amount of permanent image distortion. These deformations can lead to erroneous diagnosis. Image distortion is considered to be an important issue in the use of digital watermarking systems to transmit medical images. In order to solve the problems related to permanent distortion, reversible technology has been applied for watermarking and zero watermarking [9,10].

In the embedding stage, the cover image pixels are modified during the reversible watermark, but at the receiver, the cover image can be restored by extracting the watermark [11]. The watermark embedding method does not allow any changes to the pixels of the cover image in the zero watermark, several main features need to be taken out of the cover image and used as a guide during data authentication [12]. However, the limitation of the zero-watermark is that in order to perform potential data identity verification, the specific attributes extracted from each cover image must be kept secret. This encourages us to propose a new watermarking method, called the reversible zero watermarking technology, which combines the reversible watermarking method and the zero watermarking method together.

In [13], the authors proposed the difference between two adjacent pixels in the cover image and calculated the size of the secret information to be hidden. This method shows that the consistency of the embedded watermark is very small. In [14], the authors pointed out that in unbalanced parity check asymmetric information, LSB replacement is considered to produce an imbalance in the watermark image. Due to the imbalance, some of the techniques such as test analysis and RS attack are used to detect the watermark generated by LSB replacement [15,16]. In [14], the author found that the aforementioned detection can be resisted by reducing the histogram variation between the carrier image and the watermark image. In addition, in [17], the author proposed that reducing the histogram shift before and after steganography is a fact that resists the detection method. In [14], the authors propose to replace LSB with embedded DES (LSB-DES) encryption to reduce histogram changes. This scheme use DES in LSB-DES to encrypt the message, and then encode the ciphertext of the message in the carrier picture, while LSB replacement explicitly embeds the message in the carrier picture. More description of LSB-DES is provided in [14]. This paper proposes a new reversible watermarking algorithm based on the analysis idea, which aims to ensure the transmission security of certified medical images and reduce the distortion of medical watermark images. This new method can be used as an effective method to achieve robust watermarking with less distortion. In Fig. 1, we have shown the block diagram of the proposed method.

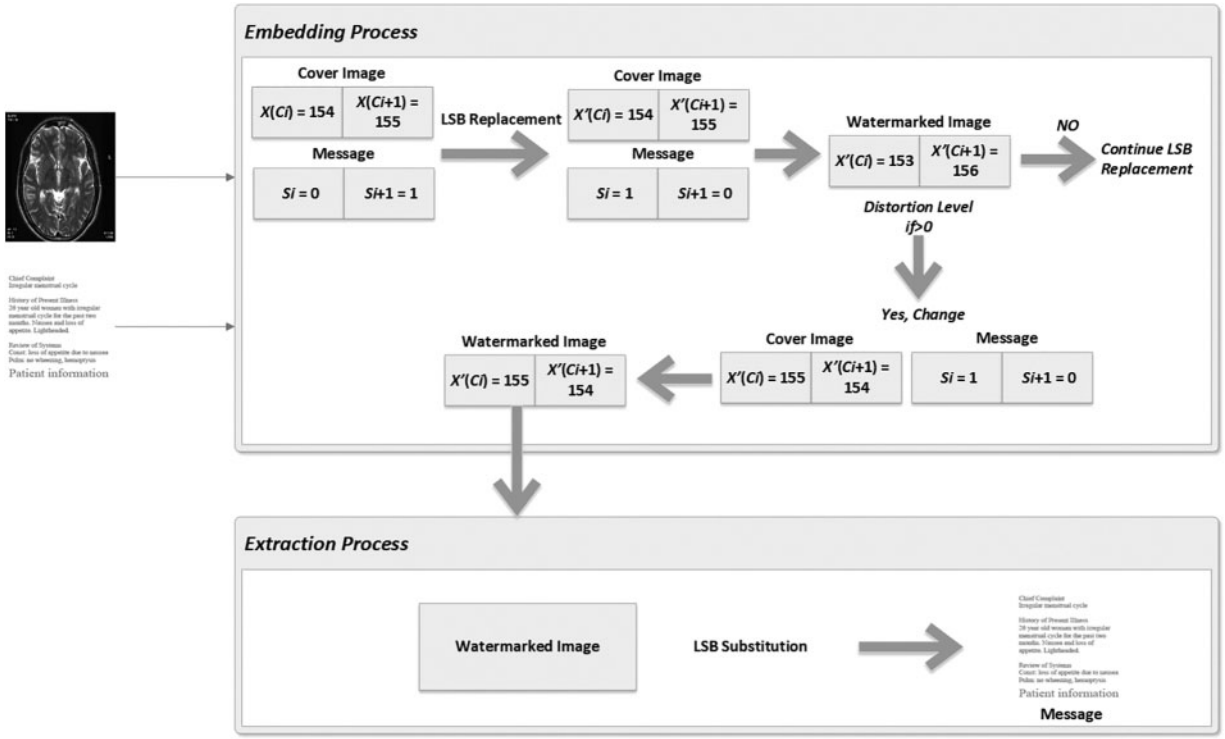

Figure 1: Block diagram of the proposed reversible watermarking methodology

The main contributions of the proposed method are:

- The proposed method aims to embed a larger payload into the cover image, thereby taking into account the imperceptibility of medical images.
- In order to better hide data and improve the security of medical images, the original LSB method is improved by reducing the distortion of watermarked images.
- The proposed method has been evaluated and compared in detail, and compared with other similar cutting-edge technologies.

The rest of this article is structured as follows. Section 2 summarizes the current state of reversible watermarking methods. Section 3 describes the proposed scheme and implementation experiment, which consists of the embedding and extraction stages of the reversible watermark. In Section 4, we discussed the experimental results. Section 5 is about conclusions and future work.

2 Related Work

Early reversible watermarking methods are divided into three parts: reversible watermarking through differential expansion, reversible watermarking through compression, and reversible watermarking through moving histograms [11]. In [18], a reversible watermarking appraoch with low distortion (HGW, watermark method based on histogram gap) is suggested. This method increases the standard histogram translation process and reduces the number of columns and distortion. We can find a lot of research work that applied classical histogram translation [19,20] and difference expansion [21,22] to predict errors. Reversible watermarking systems based on lossless data compression attempt to compress some cover images to create capacity for embedding

watermark bits. This basic principle has been used in compression-based systems and is described in [23,24].

In [25], a new LSB method is proposed, therein authors articulate that a higher peak signal-to-noise ratio (PSNR) can be obtained by embedding message bits and modifying the pixel pattern of the carrier image. LSB embedding is performed in units, because two pixels are paired into one unit in his algorithm. In [16], the authors suggested that coding distortion is easy to conceal analysis due to unbalanced distribution. In [26], it is found that when the secret message is embedded in the cover image, the original LSB digital watermark will have an imbalance of embedding distortion. In [14], a new embedding algorithm was proposed to check a pair of pixels, which revealed that the same amount of data can reduce the distortion of the cover image. It also shows that by minimizing image distortion, the resistance to watermark detection can be increased. In [27,28], the authors proposed an adaptive pixel pair matching (APPM) method, which uses pixel values to locate a pair of pixels near the embedded message bit based on them. However, when visualizing medical images, watermarking technology is still ineffective in e-Health care applications because it may cause incorrect diagnosis of treatment due to distortion.

3 Proposed Methodology

Our method relies on three main methods, including generating a secret matrix from a text file containing patient data, embedding and extracting. Textual data *Tmsg*, in the beginning, is loaded into the buffer and converted into its equivalent binary. By using the number conversion formula, the binary is converted into its equivalent decimal value. The *Tmsg* must be accompanied by 8-bit character encoding. Each character encoding scheme details how to interpret byte sequences as code points (in contrast, how to encode code points as byte sequences). The next step is to create a secret matrix *Smsg*. Every single character's decimal value represents a pixel.

$$\begin{aligned} &Smsg = \{b_ij,\ 0 \le i \le Mr,\ 0 \le j < Mc\} \\ &where, \\ &bij \in \{0, 1, \ldots, 255\} \end{aligned} \tag{1}$$

where *bi,j* is the intensity of pixel appereing at *i*-th row and *j*-th column, *Mr* is the number of rows in the Smsg, and *Mc* is the number of the columns in Smsg. The *Smsg* size sets automatically depending on the text length to be encoded.

3.1 Embedding Phase

In this process, we embed the secret matrix *Smsg* into the cover image to reduce the distortion of the watermark image. The cover image should be converted from a two-dimensional matrix to a one-dimensional matrix. Based on a one-dimensional matrix, it tries to find two adjacent LSB pairs of a pixel. In LSB substitution, the secret matrix bits are repeatedly embedded in the cover image, and one of the secret matrix bits is embedded in a pixel in a cycle. Embedding process of LSB pair for one loop can be summarized as the following steps:

Step 1. Two adjacent pixels C_i and C_{i+1}, are pair or not in the cover image. If yes, go to Step (2), else If not, do LSB substitution of current pixel C_i, then go to the next loop for the next pixel. To find LSB-pair pixels, following two conditions need to be satisfied:

$$\begin{aligned} &X(C_i) = X(C_{i+1}) + 1 \ or \ X(C_i) = X(C_{i+1}) - 1 \\ &LSB(X(C_i)) \neq S_i \ and \ LSB(X(C_{i+1})) \neq S_{i+1} \end{aligned} \tag{2}$$

The $X(C_i)$ sign indicates the grayscale value of C_i pixels. C_i represents a certain pixel in the cover image, with a sequential number indicating i in the data, where

$$\{0 \leq X(C_i) \leq 255\} \tag{3}$$

When transforming secret matrix message into binary, the ith binary value of this secret matrix is indicated by Si, where Si is represented by 0 or 1. Si and Si+1 are the respectively Ci and Ci+1 message bits. Finally, the LS $B(X(C_i))$ symbolization represents the 8th bit of gray level value for a pixel. Let's say that if the gray value of the 28th pixel was 152, the LS B(X(C28)) = 0 LSB pixel could be used to represent the 28th pixel. We had LS B(X(C29)) equal to 1 If the gray level of the 29th pixel was 153. The next phase is to identify how the variation changes when you embed the secret matrix message in LSB pairs. Since each pixel is 8 bits in the grayscale image, To represent image energy the distribution, we can use a range of 256 ordered variables. Every variable means a particular gray level frequency. The sequence of distortions can be viewed as:

$$V = (v_0, v_1, v_2, , , , v_{253}, v_{254}, v_{255}) \tag{4}$$

The variation between the cover image and watermarked image can be measured by $V' = v_2 - v_1$ where v1 represents cover image distortion, and v2 represents watermarked image distortion. There are two different conditions in which secret matrix messages are embedded when using the LSB pair procedure.

First condition. Consider two pixels are: $X(C_i) = 154$, $X(C_{i+1}) = 155$ and secret matrix message bits: $S_i = 1$, $S_{i+1} = 0$. A calculation is possible to obtain the LSB value of these two pixels: $LS\ B(X(Ci)) = 0$, $LSB(X(C_{i+1})) = 1$. These pixels are considered to be a pair as they satisfy the requirements.

Second condition. $X(C_i) = 155,\ X(C_{i+1}) = 156,\ S_i = 0, S_{i+1} = 1.$ (5)

Step 2. Determine the distortion variation $V'_{after} - V_{before}$ for regular LSB substitution; if it is larger than 0, go to Step (3); else, go to Step (4).

Step 1 First condition. Let assume the distortion variation before doing LSB replacement is:

$$V'_{before} = (\ldots, v_{154} = w, v_{155} = x, \ldots) \tag{6}$$

We obtained new $X'(C_i)$ and V'_{after} after embedding the i-th message bit into the cover image:

$$X'(C_i) = 155 \tag{7}$$

$$V'_{after} = (\ldots, v_{154} = w - 1, v_{155} = x + 1, \ldots) \tag{8}$$

Then $(i+1)^{\text{th}}$ secret matrix message bit is embedded into the cover image. We obtained new $X'(C_{i+1})$ and $D'after$:

$$X'(C_{i+1}) = 124 \tag{9}$$

$$\begin{aligned} V'_{after} &= (\ldots, v_{154} = w - 1 + 1, v_{155} = x + 1 - 1, \ldots) \\ &= (\ldots, v_{154} = w, v_{155} = x, \ldots) \\ &= V'_{before} \\ &\Rightarrow V'_{after} - V'_{before} = 0 \end{aligned} \tag{10}$$

At this location, distortion changes 0 mean that distortion is not modified after embedding watermarking messages.

Step 1 Second condition. Assume the distortion change before watermarking is $V'_{before} = (\ldots, v_{154} = w, v_{155} = x, v_{156} = y, v_{157} = z, \ldots)$. Then using the LSB replacement method to embed message, we

$$\begin{aligned} X'(C_i) &= 154 \\ X'(C_{i+1}) &= 157 \end{aligned} \tag{11}$$

$$V'_{after} = (\ldots, v_{154} = w+1, v_{155} = x-1, v_{156} = y-1, v_{157} = z+1, \ldots) \tag{12}$$

After that, calculating the distortion variations:

$$V'after - V'before = (|w+1| - |w|) + (|x-1| - |x|) + (|y-1| - |y|) + (|z+1| - |z|) \tag{13}$$

Based on the current description, $V'after - V'before < 0$ implies that the image distortion is minimized after embedding a message and vice versa. Suppose w > 0, x < 0, y < 0 and z > 0, thus we obtain

$$\begin{aligned} V'_{after} - V'_{before} &= (|w+1| - |w|) + (|x-1| - |x|) + (|y-1| - |y|) + (|z+1| - |z|) \\ &= (w+1-w) + (1-x+x) + (1-y+y) + (z+1-z) \\ &= 1+1+1+1 \\ &= 4 > 0 \end{aligned} \tag{14}$$

However, when $w + 1 < 0;\ x - 1 > 0;\ y - 1 > 0$ *and* $z + 1 < 0$

$$\begin{aligned} V'_{after} - V'_{before} &= (|w+1| - |w|) + (|x-1| - |x|) + (|y-1| - |y|) + (|z+1| - |z|) \\ &= (-1-w+w) + (x-1-x) + (y-1-y) + (-1-z+z) \\ &= -1-1-1-1 \\ &= -4 < 0 \end{aligned} \tag{15}$$

Furthermore, the distortion change can be 0 in some conditions. Numerous permutations and combinations of the value of w, x, y, and z are possible. In this system, only two interesting states: increasing variation in distortion or decreasing variation. We are only interested in whether if the value $V'_{after} - V'_{before}$ is positive or negative in LSB-pair methods.

Step 3. Shift the value of two pixels, then move to the next loop, go to one after the succeeding loop. From the first condition, gray level value 154 and 155 does not alter. After embedding, we get $X'(C_i) = 155, X'(C_{i+1}) = 154$ what looks like these adjacent pixels swap their values because before embedding values were $X(C_i) = 154$, $X(C_{i+1}) = 155$. Fig. 2 points us to an elucidation to the second condition because after embedding, it looks like two pixels swap their position. From the second condition, before embedding, if we swap the value of two pixels $X(C_i) = 155$; $X(C_{i+1}) = 156$; $S_i = 0$; $S_{i+1} = 1$, the result will be: $X'(C_i) = 154, X'(C_{i+1}) = 157$. Alternatively, the modification in distortion may be both positive and negative for applying a normal LSB substitution for the second case explicitly as in Fig. 3. When variation modification is negative, it indicates applying regular LSB replacement, and when the variation modification is positive, LSB-pair is swapping pixels before using LSB replacement.

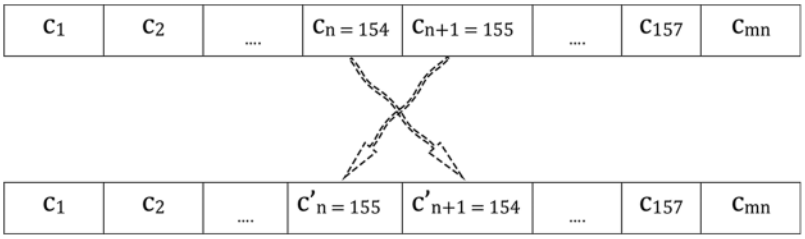

Figure 2: Swap pixels value before embedding

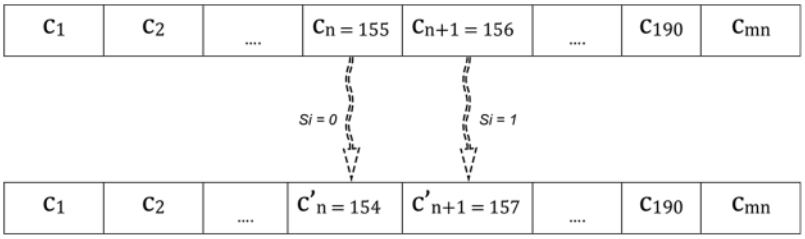

Figure 3: Swap pixels value after embedding

Algorithm 1: LSBs Extraction

Require: Watermarked image
Step 1: Initialize load watermarked image
Step 2: cols:= n;
Step 3: rows:= n;
Step 4: for each i: = 1 do rows
for each j: = 1 do cols
ExtractedPixels;
Nextpixel;
end for
end for
Step 5: *Transform Binary to Decimal*;
Step 6: *Transform to String*;
Ensure: Secret matrix message

3.2 Extraction Phase

- Read a watermarked image after embedding a secret matrix message.
- Loop through every pixel in the image, one pixel at a time.
- The Least Significant Bit(LSB) location is stored in an array of extracted bits for each pixel.
- After the LSBs have been extracted from the requisite pixels, we must take each 8-bit extracted bits and transform them into the proper text.

4 Results and Discussion

To evaluate the proposed algorithm level of performance, experimental analyses were executed on MATLAB R2016a, Windows 10 development environment, 3.5-GHz CPU with 4 GB RAM. We testedour methodology on a variety of medical images with dimensions of 512 × 512 using

MRI cover images from a well-known data source[1]. There are 38 directories in the data source folder which contains data for different patients.MRI images of two examinations are taken, one after the disease, and the second images were taken after six months of disease as shown in Fig. 4. The proposed algorithm is evaluated under randomly selected MRI images.

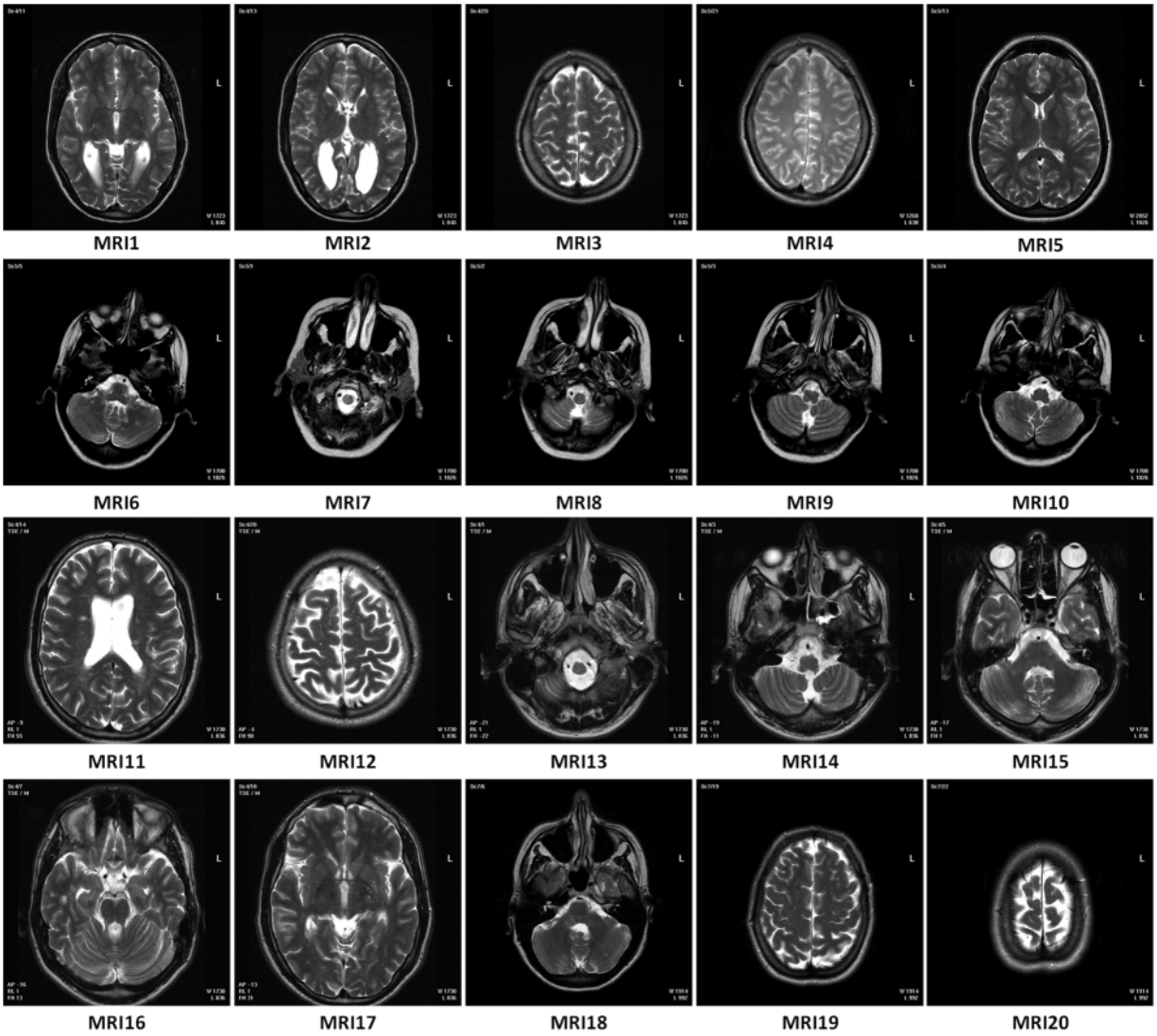

Figure 4: MRI grayscale images dataset

4.1 Performance Evaluation

Embedding a watermark into the cover image introduces distortion. The performance of the proposed methodology is evaluated by comparing the level of distortion and secret data detectability to the public. To measure the level of distortion added into the cover image, the algorithm is evaluated using quality metrics Peak signal to noise ratio (PSNR), structural similarity index

[1] http://www.ehealthlab.cs.ucy.ac.cy/index.php/facilities/32-software/218-datasets.

(SSIM), and mean squared error (MSE). The efficiency of the proposed methodology is properly analyzed by exposing it to different attacks.PSNR is primarily concerned with the pixel intensity between the cover image and watermarked image. The high PSNR value reveals that the cover image has undergone less distortion and improved the image's quality. In [3], PSNR between the cover and watermarked image is calculated as:

$$PSNR = 20\log_{10}\left(\frac{Max}{\sqrt{MSE}}\right) \tag{16}$$

where MSE is the mean square error, which is calculated in [3] as follows:

$$MSE = \frac{1}{mnm}\sum_{0}^{m-1}\sum_{0}^{n-1}(O(i,j) - S(i,j))^2 \tag{17}$$

where m, n represents pixels size, O and S represent original and cover image, respectively. SSIM calculates cover image and watermarked image structural similarity, and It contains three functions, specifically: luminance (l), contrast (c), and structural (s) are used to compare similarity. SSIM value should ideally be similar to unity. SSIM is defined mathematically in [3] as:

$$SSIM(S, Sw) = [l(S, Sw)]^{\alpha} \cdot [c(S, Sw)]^{\beta} \cdot [s(S, Sw)]^{\gamma} \tag{18}$$

Cover image and watermarked image are represented by the letters 'S' and 'S_w'. Normalized correlation (NC) aims to determine the robustness of the suggested reversible watermarking methodology by calculating similarities between the cover image and recovered watermarks when disclosed to an attack. This value should be more than 0.9 to retain attacks easily. In [3], we can find calculation of NC as,

$$NC(stg, stg^*) = \frac{\sum_{p_1=1}^{K}\sum_{p_2=1}^{K}\left[\left(stg(p1,p2) - \overline{stg}\right)\left(stg^*(p1,p2) - \overline{stg}^*\right)\right]}{\sqrt{\sum_{p_1=1}^{K}\sum_{p_2=1}^{K}\left[\left(stg(p1,p2) - \overline{stg}\right)^2\right]}\sqrt{\sum_{p_1=1}^{K}\sum_{p_2=1}^{K}\left[\left(stg^*(p1,p2) - \overline{stg}^*\right)^2\right]}} \tag{19}$$

where stg indicates cover image and stg^* indicates watermarked image while the mean value of stg and stg^* is represented by $\overline{stg}$ and $\overline{stg^*}$, respectively.

4.2 Quantitative Performance Comparison

This section provides a detailed analysis of the suggested approach with other existing methodologies, including the traditional LSB algorithm. The experimental process was conducted by random images chosen from the data source and five standard images. Table 1 presents the performance metrics for 20 MRI medical images. The experiment of the PSNR, SSIM, and MSE reveals that watermarked images cannot be discriminated against by the human eye and are relatively imperceptible. The average PSNR value of 51.657 dB of twenty images shows an ideal performance, and the visual trend is represented in Fig. 6. SSIM values are similar to 1, indicating high structural similarity between original and watermarked images. MRI5 attains a peak value of SSIM 0.988, and the average value of SSIM is 0.984. The average value of MSE is 0.444.NC is used to calculate the correlation of the cover image to the recovered watermark image. NC results are very close to 1, which represents the proposed approach resistance to attacks. Table 2

determines the suggested algorithm strength to various attacks. The table contains PSNR, SSIM, and NC metrics for randomly selected images 'Image 1', 'Image 9', 'Image 11', and 'Image 19' subject to numerous attacks. The SSIM value of 'Image 19' for cropping attack is 0.078, the comparison of the proposed scheme with the existing methodology. Table 3 shows the comparison of proposed scheme with existing methodology. The techniques have been compared with the methodology developed by Bailey et al. [29], Jassim [30], Karim et al. [31], Muhammad et al. [32], Rehman et al. [33], Siddiqui et al. [34], and Wazirali et al. [35]. Bailey et al. [29–34] employ 104,857 bits to calculate the PSNR value. The performance of the watermarking is identified by embedding large secret data with a higher PSNR.

Table 1: Results of watermarked images of 512 × 512 dimension, having 32 KB embedding data size

Image name	PSNR (dB)	SSIM	MSE
MRII	51.685	0.993	0.441
MRI2	51.685	0.993	0.441
MRI3	51.680	0.921	0.442
MRI4	51.687	0.990	0.440
MRI5	51.682	0.988	0.441
MRI6	51.599	0.974	0.449
MRI7	51.604	0.976	0.450
MRI8	51.606	0.976	0.449
MRI9	51.596	0.975	0.450
MRI10	51.610	0.974	0.449
MRI11	51.683	0.996	0.441
MRI12	51.678	0.996	0.442
MRI13	51.679	0.996	0.442
MRI14	51.696	0.996	0.440
MRI15	51.680	0.996	0.442
MRI16	51.673	0.996	0.442
MRI17	51.690	0.996	0.441
MRI18	51.647	0.985	0.445
MRI19	51.646	0.983	0.445
MRI20	51.635	0.981	0.446
Average	51.657	0.984	0.444

Table 2: Imperceptibility and robustness evaluation under attacks

Attacks	Image 1			Image 9			Image 11			Image 19		
	PSNR	SSIM	NC	PSNR	SSIM	NC	PSNR	SSIM	NC	PSNR	SSIM	NC
Salt & pepper noise (0.001)	33.586	0.969	0.997	33.335	0.951	0.995	34.010	0.971	0.999	34.117	0.961	0.996

(Continued)

Table 2 (Continued)

Attacks	Image 1			Image 9			Image 11			Image 19		
	PSNR	SSIM	NC	PSNR	SSIM	NC	PSNR	SSIM	NC	PSNR	SSIM	NC
Salt & pepper noise (0.0002)	39.726	0.987	0.999	38.014	0.967	0.998	41.264	0.992	0.999	39.855	0.978	0.999
Gaussian noise (0.0002)	37.296	0.894	0.999	38.349	0.759	0.998	37.042	0.906	0.999	38.175	0.798	0.998
Gaussian noise (0.010, 0.0002)	35.071	0.831	0.998	35.011	0.538	0.997	35.236	0.885	0.999	35.096	0.604	0.997
Speckle noise (0.0001)	46.706	0.990	1.000	47.887	0.974	0.999	45.032	0.990	0.999	47.323	0.981	0.999
Histogram equalization	8.696	0.285	0.866	5.891	0.115	0.641	11.324	0.462	0.927	7.042	0.170	0.748
Sharpening	35.134	0.964	0.998	35.701	0.962	0.997	36.588	0.975	0.999	38.276	0.965	0.998
Gaussian filter (3×3)	38.612	0.985	0.999	38.615	0.971	0.999	37.018	0.992	0.999	39.583	0.980	0.999
Median filter (3×3)	30.064	0.938	0.994	30.053	0.948	0.989	27.605	0.966	0.994	30.501	0.954	0.992
Wiener filter (3×3)	21.657	0.284	0.750	21.343	0.184	0.929	20.296	0.299	0.967	21.600	0.180	0.945
JPEG compression (80)	40.074	0.953	0.999	41.540	0.919	0.998	41.655	0.980	0.999	42.199	0.938	0.999
JPEG compression (90)	42.867	0.975	1.000	44.559	0.937	0.997	44.493	0.986	0.999	44.922	0.957	0.999
Rotattion2	16.656	0.545	0.853	16.429	0.661	0.745	15.044	0.460	0.885	17.819	0.677	0.856
Gamma correction (0.8)	25.784	0.827	0.994	28.970	0.810	0.996	24.650	0.885	0.994	27.383	0.819	0.994
Scaling	13.285	0.246	0.619	14.258	0.044	0.436	11.402	0.283	0.695	13.636	0.100	0.522
Cropping	9.656	0.170	0.609	9.734	0.123	0.377	4.309	0.184	0.746	9.697	0.078	0.539
Shearing	14.092	0.361	0.706	13.525	0.633	0.43	12.012	0.240	0.745	14.390	0.631	0.645
Motion blur	21.644	0.714	0.954	21.746	0.741	0.926	20.707	0.715	0.969	23.086	0.794	0.958
Translation	14.216	0.448	0.958	13.002	0.583	0.456	12.444	0.373	0.795	14.449	0.601	0.697

Table 3: PSNR results compared with the standard digital images when the image size is 512 × 512

Watermark image	Bailey et al. [29]	Jassim [30]	Karim et al. [31]	Muhammad et al. [32]	Rehman et al. [33]	Siddiqui et al. [34]	Wazirali et al. [35]	Proposed (32 KB)
Barbara	46.11	43.60	40.99	47.34	50.45	48.42	–	51.68
Baboon	44.67	44.75	44.66	49.10	52.00	50.08	51.37	51.71
Cameraman	44.59	45.21	41.56	48.02	50.98	47.88	–	51.71
Lena	44.12	44.93	42.95	50.01	51.05	49.83	–	51.72
Peppers	35.04	34.02	31.23	39.38	49.44	50.15	51.36	51.73
Average	42.90	42.50	40.28	46.77	50.78	49.27	51.37	51.71

In [35], authors proposed the reversible watermarking technique by maximizing the secret data to 180,000 bits. The PSNR value of [35] methodology for standard images baboon and peppers shows better results. We performed our experiments by embedding 262,688 bits of secret data than these methodologies, and our algorithm outperforms. The average value of PSNR on standard images shown in Fig. 5 Barbara, Baboon, Cameraman, Lena, and Peppers is 51.71 dB. Fig. 7 shows a visual representation of the proposed scheme with existing methodologies. The PSNR values in [29–34] are measured employing 104,857 bits, whereas [35] increases the embedding capacity by hiding 180,000 bits. We outperform the existing techniques by employing 32 KB of patient data.

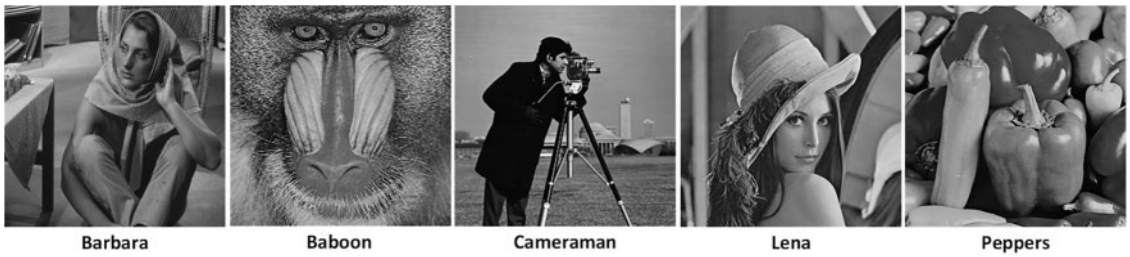

Figure 5: The sample set of standard cover images

Watermarking capacity quantifies the number of bits that can be embedded in a carrier image. According to distortion parameters, Fig. 8 evaluates some of the current state-of-the-art methodologies discussed in this research with the suggested scheme. The proposed scheme has a high embedding of data with low distortion. If we maximize the number of embedding data, the proposed scheme shows robustness and human eyes cannot detect it. Wazirali et al. [35] shows an average PSNR of 51.37 with a maximum embedding capacity of 32 KB, The proposed scheme achieved a PSNR of 51.4 when hiding 36 KB.

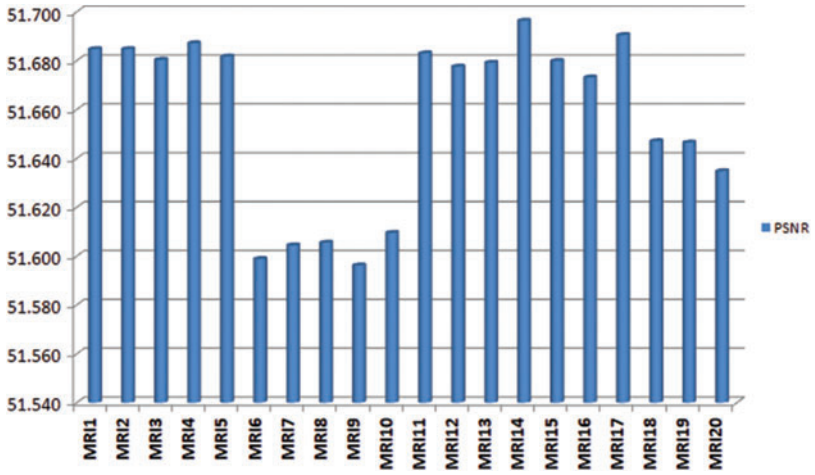

Figure 6: PSNR values visual presentation

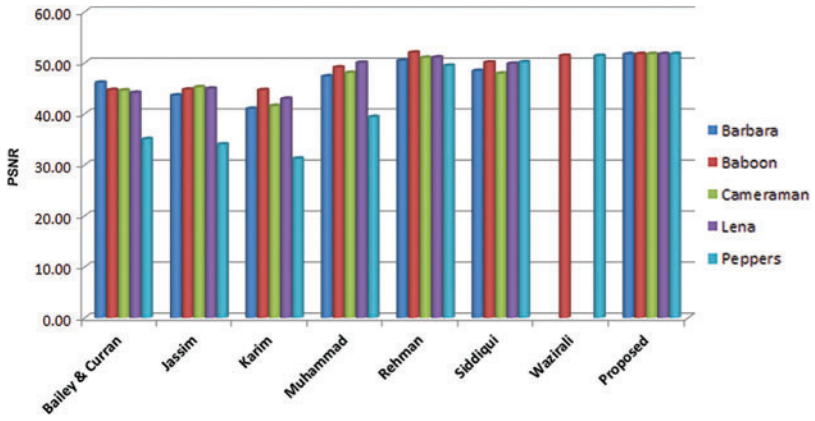

Figure 7: PSNR performance analysis visual representation of proposed scheme on the standard images with the state-of-the-art technique

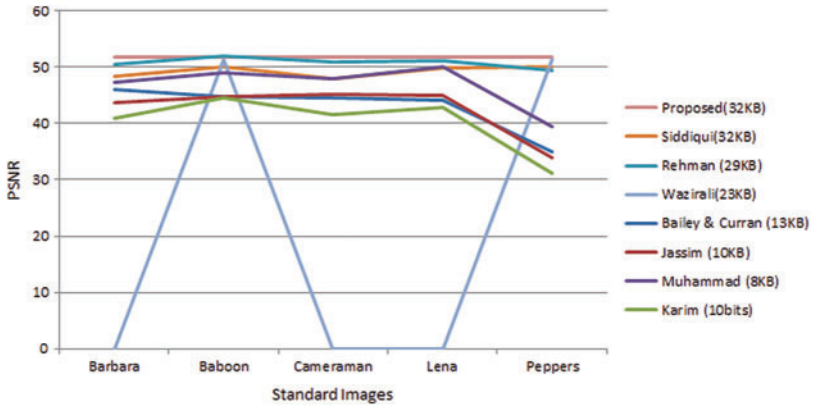

Figure 8: Disortation comparison of various schemes cited in the paper

5 Conclusions

This article introduces a low-distortion reversible watermarking method suitable for remote medical image transmission. The core component of our method is to convert text information into secret matrix messages, embed low-distortion messages and extract messages from watermarked images. The proposed method has lower computational requirements because all processes are implemented in the spatial domain rather than the transform or frequency domain. When subjected to different attacks, the algorithm shows ideal resistance. For an MRI image with a size of 512 × 512, the average PSNR value is 51.657. Therefore, it can be said with certainty that the proposed reversible watermarking method will be effective in the medical field. In future work, the suggested method can be enhanced for color images.

Funding Statement: This work is supported by the National Natural Science Foundation of China (Grant 61762060), Educational Commission of Gansu Province, China (Grant 2017C-05), Foundation for the Key Research and Development Program of Gansu Province, China (Grant 20YF3GA016).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Velpuru, M. S. (2021). Reversible watermarking techniques: Digital conent security. In: *Advancements in security and privacy initiatives for multimedia images,* pp. 114–132. IGI Global.
2. Anand, A., Singh, A. K. (2020). Watermarking techniques for medical data authentication: A survey. *Multimedia tools and applications,* pp. 1–33. Springer.
3. Zainol, Z., Teh, J. S., Alawida, M., Alabdulatif, A. (2021). Hybrid SVD-based imager26 watermarking schemes: A review. *IEEE Access, 9,* 32931–32968. DOI 10.1109/ACCESS.2021.3060861.
4. Bastani, A., Ahouz, F. (2020). High capacity and secure watermarking for medical images using Tchebichef moments. *Radioengineering, 29(4),* 636–643. DOI 10.13164/re.
5. Thabit, R. (2021). Review of medical image authentication techniques and their recent trends. *Multimedia Tools and Applications, 88(9),* 1–35.
6. Iftikhar, S., Kamran, M., Anwar, Z. (2014). RRW—A robust and reversible watermarking technique for relational data. *IEEE Transactions on Knowledge and Data Engineering, 27(4),* 1132–1145. DOI 10.1109/TKDE.2014.2349911.
7. Mo, Q., Yao, H., Cao, F., Chang, Z., Qin, C. (2019). Reversible data hiding in encrypted image based on block classification permutation. *Computers, Materials & Continua, 59(1),* 119–133. DOI 10.32604/cmc.2019.05770.
8. Liu, J., Li, J., Cheng, J., Ma, J., Sadiq, N. et al. (2019). A novel robust watermarking algorithm for encrypted medical image based on DTCWT-DCT and chaotic map. *Computers, Materials & Continua, 61(2),* 889–910. DOI 10.32604/cmc.2019.06034.
9. Guo, X., Zhuang, T. G. (2009). Lossless watermarking for verifying the integrity of medical images with tamper localization. *Journal of Digital Imaging, 22(6),* 620–628. DOI 10.1007/s10278-008-9120-5.
10. Wen, Q., Sun, T. F., Wang, S. X. (2003). Concept and application of zero-watermark. *Acta Electronica Sinica, 31(2),* 214–216.
11. Khan, A., Siddiqa, A., Munib, S., Malik, S. A. (2014). A recent survey of reversible watermarking techniques. *Information Sciences, 279(1),* 251–272. DOI 10.1016/j.ins.2014.03.118.
12. Seenivasagam, V., Velumani, R. (2013). A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud. *Computational and Mathematical Methods in Medicine, 2013(4),* 1–16. DOI 10.1155/2013/516465.

13. Wu, D. C., Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24(9–10),* 1613–1626. DOI 10.1016/S0167-8655(02)00402-6.
14. Mielikainen, J. (2006). LSB matching revisited. *IEEE Signal Processing Letters, 13(5),* 285–287. DOI 10.1109/LSP.2006.870357.
15. Westfeld, A., Pfitzmann, A. (1999). Attacks on steganographic systems. In: *International workshop on information hiding,* pp. 61–76. Berlin, Germany: Springer.
16. Fridrich, J., Goljan, M., Du, R. (2001). Detecting LSB steganography in color, and gray scale images. *IEEE Multimedia, 8(4),* 22–28. DOI 10.1109/93.959097.
17. Xi, L., Ping, X., Zhang, T. (2010). Improved LSB matching steganography resisting histogram attacks. *3rd International Conference on Computer Science and Information Technology*, vol. 1, pp. 203–206, Chengdu, China: IEEE.
18. Li, Y., Wang, J., Ge, S., Luo, X., Wang, B. (2019). A reversible database watermarking method with low distortion. *Mathematical Biosciences and Engineering, 16(5),* 4053–4068. DOI 10.3934/mbe.2019200.
19. Fu, D. S., Jing, Z. J., Zhao, S. G., Fan, J. (2014). Reversible data hiding based on prediction-error histogram shifting and EMD mechanism. *AEU-International Journal of Electronics and Communications, 68(10),* 933–943. DOI 10.1016/j.aeue.2014.04.015.
20. Jaara, E. N., Jafar, I. F. (2015). Reversible data hiding based on histogram shifting of prediction errors using two predictors. *Applied Electrical Engineering & Computing Technologies*, pp. 1–5. Amman, Jordan: IEEE.
21. Ou, B., Li, X., Zhao, Y., Ni, R., Shi, Y. Q. (2013). Pairwise prediction-error expansion for efficient reversible data hiding. *IEEE Transactions on Image Processing, 22(12),* 5010–5021. DOI 10.1109/TIP.2013.2281422.
22. Li, X., Li, J., Li, B., Yang, B. (2013). High-fidelity reversible data hiding scheme based on pixel-valueordering and prediction-error expansion. *Signal Processing, 93(1),* 198–205. DOI 10.1016/j.sigpro.2012.07.025.
23. Celik, M. U., Sharma, G., Tekalp, A. M., Saber, E. (2005). Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing, 14(2),* 253–266. DOI 10.1109/TIP.2004.840686.
24. Memon, N. A., Khan, A., Gilani, S., Ahmad, M. (2011). Reversible watermarking method based on adaptive thresholding and companding technique. *International Journal of Computer Mathematics, 88(8),* 1573–1594. DOI 10.1080/00207160.2010.509429.
25. Bamatraf A., Ibrahim, R., Salleh, M., Mohd, N. (2011). A new digital watermarking algorithm using combination of least significant bit (LSB) and an inverse bit. arXiv preprint arXiv: 1111.6727.
26. Ker, A. D. (2004). Improved detection of LSB steganography in grayscale images. In: *International Workshop on Information Hiding,* pp. 97–115. Springer, Berlin, Heidelberg.
27. Zhang, X., Wang, S. (2006). Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters, 10(11),* 781–783. DOI 10.1109/LCOMM.2006.060863.
28. Hong, W., Chen, T. S. (2011). A novel data embedding method using adaptive pixel pair matching. *IEEE Transactions on Information Forensics and Security, 7(1),* 176–184. DOI 10.1109/TIFS.2011.2155062.
29. Bailey, K., Curran, K. (2006). An evaluation of image based steganography methods. *Multimedia Tools and Applications, 30(1),* 55–88. DOI 10.1007/s11042-006-0008-4.
30. Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv: 1307.0642.
31. Karim, S. M., Rahman, M. S., Hossain, M. I. (2011). A new approach for LSB based image steganography using secret key. *14th International Conference on Computer and Information Technology*, pp. 286–291. Dhaka, Bangladesh.
32. Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M. et al. (2015). A secure method for color image steganography using gray-level modification and multi-level encryption. *TIIS Transactions on Internet and Information Systems, 9(5),* 1938–1962. DOI 10.3837/tiis.2015.05.022.
33. Rehman, A., Saba, T., Mahmood, T., Mehmood, Z., Shah, M. et al. (2019). Data hiding technique in steganography for information security using number theory. *Journal of Information Science, 45(6),* 767–778. DOI 10.1177/0165551518816303.

34. Siddiqui, G. F., Iqbal, M. Z., Saleem, K., Saeed, Z., Ahmed, A. et al. (2020). A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. *IEEE Access, 8,* 181893–181903. DOI 10.1109/ACCESS.2020.3028315.
35. Wazirali, R., Alasmary, W., Mahmoud, M. M., Alhindi, A. (2019). An optimized steganography hiding capacity and imperceptibly using genetic algorithms. *IEEE Access, 7,* 133496–133508. DOI 10.1109/ACCESS.2019.2941440.