Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2022.020255

ARTICLE

A Robust Data Hiding Reversible Technique for Improving the Security in e-Health Care System

Saima Kanwal[1], Feng Tao[1,*], Ahmad Almogren[2], Ateeq Ur Rehman[3], Rizwan Taj[1] and Ayman Radwan[4]

[1]School of Computer and Communication, Lanzhou University of Technology, Lanzhou, 730050, China

[2]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh, 11633, Saudi Arabia

[3]Department of Electrical Engineering, Government College University, Lahore, 54000, Pakistan

[4]Instituto de Telecomunicações and Universidade de Aveiro, Aveiro, 3810-193, Portugal

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

Received: 13 November 2021 Accepted: 28 March 2022

ABSTRACT

The authenticity and integrity of healthcare is the primary objective. Numerous reversible watermarking schemes have been developed to improve the primary objective but increasing the quantity of embedding data leads to covering image distortion and visual quality resulting in data security detection. A trade-off between robustness, imperceptibility, and embedded capacity is difficult to achieve with current algorithms due to limitations in their ability. Keeping this purpose insight, an improved reversibility watermarking methodology is proposed to maximize data embedding capacity and imperceptibility while maintaining data security as a primary concern. A key is generated by a random path with minimum bit flipping is selected in the 4 × 4 block to gain access to the data embedding patterns. The random path's complex structure ensures data security. Data of various sizes (8 KB, 16 KB, 32 KB) are used to analyze image imperceptibility and evaluate quality factors. The proposed reversible watermarking methodology performance is tested under standard structures PSNR, SSIM, and MSE. The results revealed that the MRI watermarked images are imperceptible, like the cover image when LSB is 3 bits plane. Our proposed reversible watermarking methodology outperforms other related techniques in terms of average PSNR (49.29). Experiment results show that the suggested reversible watermarking method improves data embedding capacity and imperceptibility compared to existing state-of-the-art approaches.

KEYWORDS

Medical images security; data hiding; LSB matching; hiding capacity; imperceptibility

1 Introduction

Over the decades, the exponential growth of the internet, digital communication expanded the capacity of internet multimedia networks with the processing of a massive volume of videos and images [1]. Many developments in the computing environment have threatened copyright security and material integrity, including hardware, software, and communication systems. In recent years, in the biomedical system, many changes and advancements have occurred regarding digital images of medical data, and it has become a significant field [2]. Besides the fast speed and highly efficient digital communication, security risks must be resolved in Internet Apps, e.g., military images are associated with the security of the entire country. Information security of digital communication affects everyone's peace of mind. Researchers have developed different techniques in digital image processing to authenticate the image information and identify image manipulation accurately and robustly. Medical images contain sensitive information about the patients, so security and privacy protections of the medical images become crucial while sending those images through the internet [3]. Due to the rapid growth in the electronic health industry, remote health monitoring of the patients has become possible using sensors, resulting in better patient care [4]. To ensure the privacy and security of information on the internet and avoid data leakage, data hiding technology (i.e., embedding data) has emerged. Steganography and watermarking are the two major types of data hiding methodologies. Steganography is generally used for secret communication so that the confidential data concealed in the cover object would not catch the public's attention. Steganography typically introduces a "peer-to-peer" secret communication. The content of the hidden message is only accessible to the sender and recipient, and the recipient can accurately extract the secret message. Digital watermarking is used to ensure that digital media such as documents and videos are authentic and copyright protected by embedding secret data in them. It is significant to mention that watermarking has numerous resemblances to steganography in terms of embedding data. The purpose of watermarking is to make it extremely difficult to extract hidden information to avoid the unauthorized copying of the data. Digital watermarking technology is divided into two categories: frequency domain and spatial domain [5]. The watermarking approach is implemented on the image's coefficient values in the frequency domain. There are three main types of spatial domain images in digital image processing: one is binary, the other is grayscale, and the third is colour images. In binary images, there are only two possible values for each pixel, and it is most commonly used in black and white, but it can also be used for any two colours. Greyscales images only contain the intensity data using a single sample value for each pixel. It is usually called black and white, and these images contain the different shades of grey (0 to 255), in which the black color is at 0, and it represents the weak intensity, while the white color is at 255, and it represents the vigorous-intensity whereas color images consist of three primary sets of colors red, green and blue ranging color from 0–255 [6]. However, in the spatial domain watermarking, the modification of cover image pixel with watermark image is applied. An ideal watermarking algorithm focuses solely on high visibility of source image, minimum complexity, data security, imperceptibility, and high embedding capacity. However, it is challenging to provide a data hiding approach that contains these characteristics simultaneously in most situations. In recent decades, researchers have progressed on data hiding algorithms that need low or medium computational capacity with adequate visual quality at a higher embedding capacity. In steganography, two main embedding techniques are used, one is the PVD (Pixel Value Difference), and the other one is LSB (Least Significant Bit) [7]. PVD technique has much better performance as compared to LSB because it provides stego images with high quality and hidden data with a high capacity [8]. Implementation ofthe PVD scheme as a new paradigm, spatial domain algorithms are being used, through which the iris implicit images data would be, inserted instantly into the cover pixel images [9]. The least significant bits (LSB [10–13], Exploiting Modification Direction (EMD) [14–16], and Pixel Value Difference (PVD) [17–21] are some of the most popular algorithms of watermarking in the spatial domain. Some researchers have combined two methodologies PVD, EMD with LSB substitutions, to obtain efficient results in data security, embedding capacity, and excellent visual quality [16,22–27]. The secret bits are encoded pairwise and then embedded in the cover LSB bits with very little changes to the reference image [28]. Wu et al. [29] proposed a methodology known as PDBD for low distortion in PVD and base decomposition. In the context of a pixel pair, the difference between pixels is determined first, and the corresponding degree is measured. Then certain bits of information are transformed by the base pair of the degree into two adjacent coefficients. Further, the pixel pair is formed by embedding coefficients. Traditionally, algorithms were commonly identified, and strategies in which information was directly encoded in the LSB planes of the host image were implemented. An acceptable extent of security and in contexts of data encoding, many of these algorithms have done reasonably well. Besides that, with the ever-growing computing capability of digital technologies, most strategies are noticed to be compromised. With this in perspective, algorithms for hiding data based on keys emerged into the field of research, and researchers also explored these using conventional digital signature attacks. In [30], the Hilbert curve methodology produces data embedding structures and a logistic map to encode a message signal to improve security with a high payload and better image quality. Some studies show higher security schemes were also implemented using the similarities of the pixel neighbourhood, redundancy, inherent features in the image, etc. [31–36]. Chaotic system-based various schemes have provided enhanced security performance. Such systems focus on secret keys generated by the chaotic map parameters [37,38]. The security of the data hiding algorithm relies greatly on the scale and accuracy of the secret keys used in the process. The histogram of watermarked images is well known to publicize the presence of hidden information, and this is especially true for algorithms that have a high data encoding capability. At the same point, imperceptibility is important for information security. Therefore, algorithms should also focus on significantly reducing the impact of encoding on histograms. We have proposed an efficient reversible watermarking system with improved patient records security and a high level of imperceptibility. An embedding pattern is implemented by generating the key using random paths in the pixel block to obtain maximum security. The patient record information is embedded in the cover image up to 3 bits plane without any indication of secret information for a third party.

The following are our main contributions:

- Implementation of the unique random path in blocks and rotation of pixels.
- Different math operations have been implemented for data embedding up to 3 bits plane LSB.
- Strategy for optimization to reduce bit flipping.
- An approach is implemented with impactful improvements in terms of maximum payload capacity and imperceptibility.
- Detailed evaluation and comparison with other similar state-of-the-art methodologies.

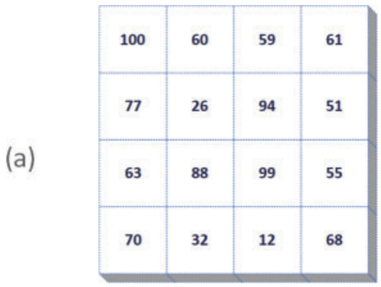
The Breakdown structure of the paper is as follows: Section 2 represents different state-of-the-art reversible algorithms. Section 3 delves into the proposed methodology in detail with embedding and extracting watermark steps. The experimental results of the study and discussion are found in Section 4. Finally, Section 5 presents the conclusion and future work.

2 Preliminaries

Different studies have used image steganography methodologies to conceal confidential information, the images' visual quality, and data embedding capacity. Gndu et al. [39–42] explained the reverse connection between MSE and PSNR. They depicted that higher values of PSNR represent the high-quality image (better), and the PVD method stores a greater number of bits for the message than the LSB method. They showed a better quality result of LSB images after embedding as compared to PVD. However, the PVD method can store a larger number of data bits without losing the image quality, while an LSB can store a large number of data bits but degrades the image quality. Mansor et al. [6] proposed the technique of 2D discrete wavelet transforms in two levels for embedding patients' data in a cover medium. For cover images, they used colour images and grayscale images. They employed conventional procedures to encrypt the textual data before embedding it in the cover medium. To validate the cover medium imperceptibility, they applied different algorithms and statistical tests. They achieved better statistical scores for hidden textual material than similar existing techniques and proposed various state-of-the-art image stenographic methodologies. Among them, the LSB modification of [31] is one of the most common methods to modify the lower order bits of the pixel values that will be unnoticeable, even with multiple steganalysis methods [43,44]. Several LSB-based information hiding techniques provide high data encoding with an acceptable level of imperceptibility. Even so, it can be noticed that many other spatial domain steganalysis techniques lack this primary objective, as histograms can easily decipher the appearance of concealed data. In [45], the authors proposed the inter-block coefficient dependency method for embedding purposes. The difference in the coefficients is calculated employing adjacent discrete transform cosine (DCT) blocks with identical locations. However, this technique is particularly for JPEG medical images to conceal patient data. The methodology of reversible data hiding based on histogram shifting is used to embed data via histogram modification [46]. The original image histogram's peak and zero/minimum points are employed, where the peak point has the maximum number of grayscale pixels and the zero/minimum point has the minimum pixel value. Each pixel with a peak point value is used to convey a bit of a hidden message. The histogram shifting approach has low computational requirements, minimal distortion in the original image and a high PSNR ratio between the original and watermarked images. However, this technique limits hiding capacity by the histogram's peak points. Sahu et al. [47] described the image steganography approach, in which they employed distinct pixels from various sub-blocks to improve the Peak Signal to Noise Ratio (PSNR) and Embedding Capacity (EC) of the image. This method was divided into two sections, the first was OPVD (Overlapped Pixel Value Difference), and the second was OPVDMF (Overlapped Pixel Value Differencing with Module Function). It brings significant improvement in resist, security, and RS analysis test. In [48], the author proposed a high-quality and straightforward reversible watermarking approach focused on difference expansion and using redundancy of digital content to obtain reversibility. The pixel value difference between pairs of the host image is expended by two in this technique. The least significant bits embed hidden messages as the even number is calculated from the expanded difference. After the least significant bits, a watermark bit is embedded to obtain the watermarked image. The compressed location map and payload are concatenated with actual least significant bit values for identical image retrieval. High embedding capacity is achieved by this method; however, because a location map is required, not much of the capacity is used to embed data. Furthermore, this approach introduces unfavorable distortion. In [49], the authors implemented a Hamiltonian path to minimize distortion between LSB pixels and embedded data. LSB equivalent encoding method is changed specifically rather than blindly to improve image steganography. However, several visual objects in the stego-images can be identified in the suggested model. Their methodology is robust against the soft margin SVM based on the second-order SPAM. In [50], the authors suggested a new approach that divides the cover image into non-overlapping blocks. Hamilton's path for each block first modifies the structure of the block's pixels. Next, they evaluate the pixels whose LSB is not equivalent to the hidden data. The path that results in minimal distortion is selected, and both its binary code and the mismatched pixels are counted. The pixels that should be changed during data embedding and a binary key containing codes of the best Hamiltonian path in all blocks are calculated by repeating this procedure. Then, with reference to the compressed key, the latest value of the second LSB of the modifiable pixels is computed using writing on the wet paper method. Finally, the value computed for the second LSB±1 is applied to each changeable pixel [13]. Siddiqui et al. [2] proposed steganography techniques to hide the secreted data in the image, the N-rightmost bit is replaced, and its main objective is Peak Signal to Noise Ratio (PSNR), which improves the quality of the image. The EC (Embedding Capacity) benefit from transmitting a considerable quantity of data between the sender and the receiver, avoiding the FOBP (Fall Boundary Problem), which enhance the security in salt, resist pepper noise, and RS attack. Sahu et al. [51] describes another work in which two approaches were used for RDH (Reversible Data Hiding). In the first approach, to achieve reversibility, they extend the matching of LSB (Least Significant Bit) in dual images. In the second approach for the secret data embedding, they used the four identical cover images, and then the secret data of cover images were embedded in two phases. In the first phase, the N-RMB (NRightmost Bit replacement) techniques were used, and in the second phase, the MPVD (Modified Pixel Value Differencing) technique they used in [52], 1D adaptive Bernoulli map, ideal for encryption, is suggested for correlation coefficients. The revolutionary image encryption technique was implemented focused on the recent chaotic map. The permutation process was understood by creating a randomly Hamiltonian path implemented over different bit planes. Then, in the diffusion process (XOR procedures were conducted on pixels), the concept of the random Hamiltonian path was applied to substitute for grey levels.

3 Proposed Methodology

The desired methodology takes the cover image and patient record information as inputs and generates the watermarked image by implementing numerous operations at the pixel level. The patient record has all the details about the individual, the patient's details, the disease under which the patient suffers, and the physician who diagnoses the disease. The fundamental concept of the scheme is to maximize the imperceptibility and robustness against different attacks of the cover image. A cover image of 512 × 512 is divided into non-overlapping disjoint square pixel blocks of the same size. The patient record information is embedded in the LSB planes of the pixel blocks by pursuing a sequence created by the random path. Fig. 1 provides an example of three random paths with minimum bit flipping described in a 4 × 4 block. Once the random path has been chosen, the embedding procedure is carried out by considering four ideal sequence directions and pixel rotation (0°; 90°; 180°; 270°), and the path with minimum bit flipping is selected for the patient record embedding. The random path selected for data embedding is implemented on all blocks. The workflow of the proposed algorithm is defined in Fig. 2.



100	60	59	61
77	26	94	51
63	88	99	55
70	32	12	68

Figure 1: (Continued)

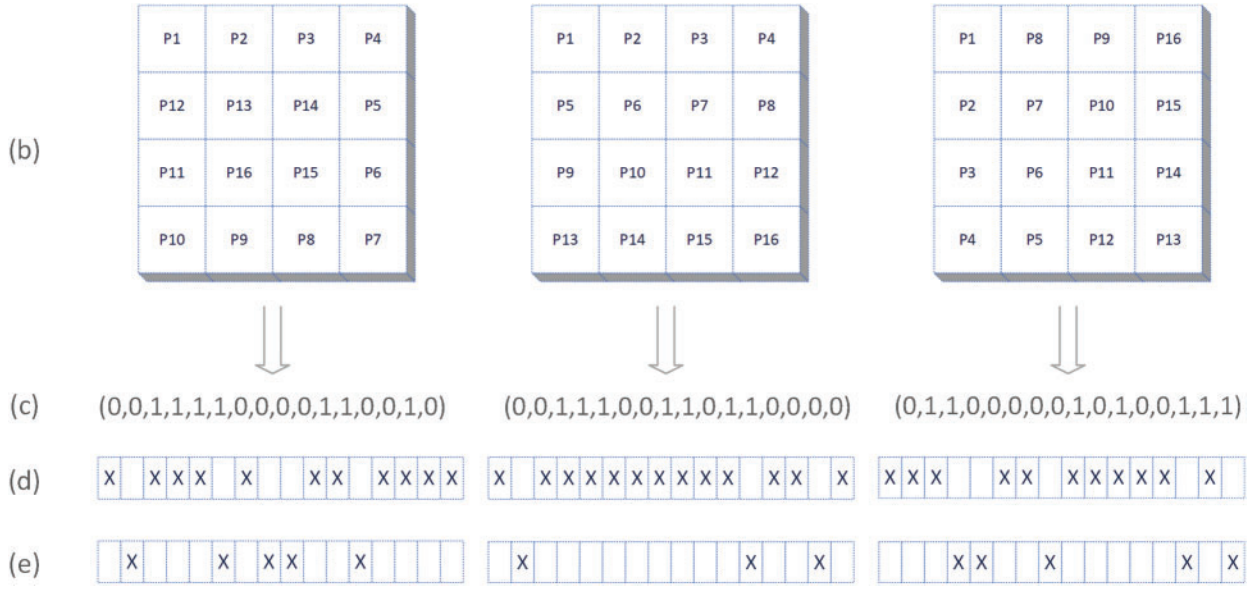


Figure 1: (a) An example of a 4 × 4 block (b) Random path in 4 × 4 block (c) LSB Sequence according to the random path (d) The distortion caused by matching every sequence to the data sample $(1000011001011101)_2$ and the distinct pixels (e) The distortion caused by matching every sequence to the complement of the data sample and the distinct pixels

3.1 Random Path Generation

We describe an explanation of finding the ideal random path in 4 × 4 non-overlapping blocks. Every pixel in the block will be accessed once starting from the top-left pixel. In the case of the proposed 4 × 4 blocks, one can choose a random path from a set of 20 possible paths using the combinatorics approach in 1.

$$\frac{(m+n-2)!}{(n-1)!\,(m-1)!} \tag{1}$$

Assume the patient data is $(1000011001011101)_2$. As seen in example Fig. 1, there are three different random paths in a 4 × 4 block. As shown in Fig. 1c from left to right, a matrix of the pixel's LSB is generated by tracing each path. The pixels in which LSBs do not match the respective hidden data bit or sample data complement are depicted in Figs. 1d and 1e, respectively. The block distortion is counted by the amount of non-matching pixels, as shown in these figures. The path with the least distortion is identified as the ideal random path in this block.

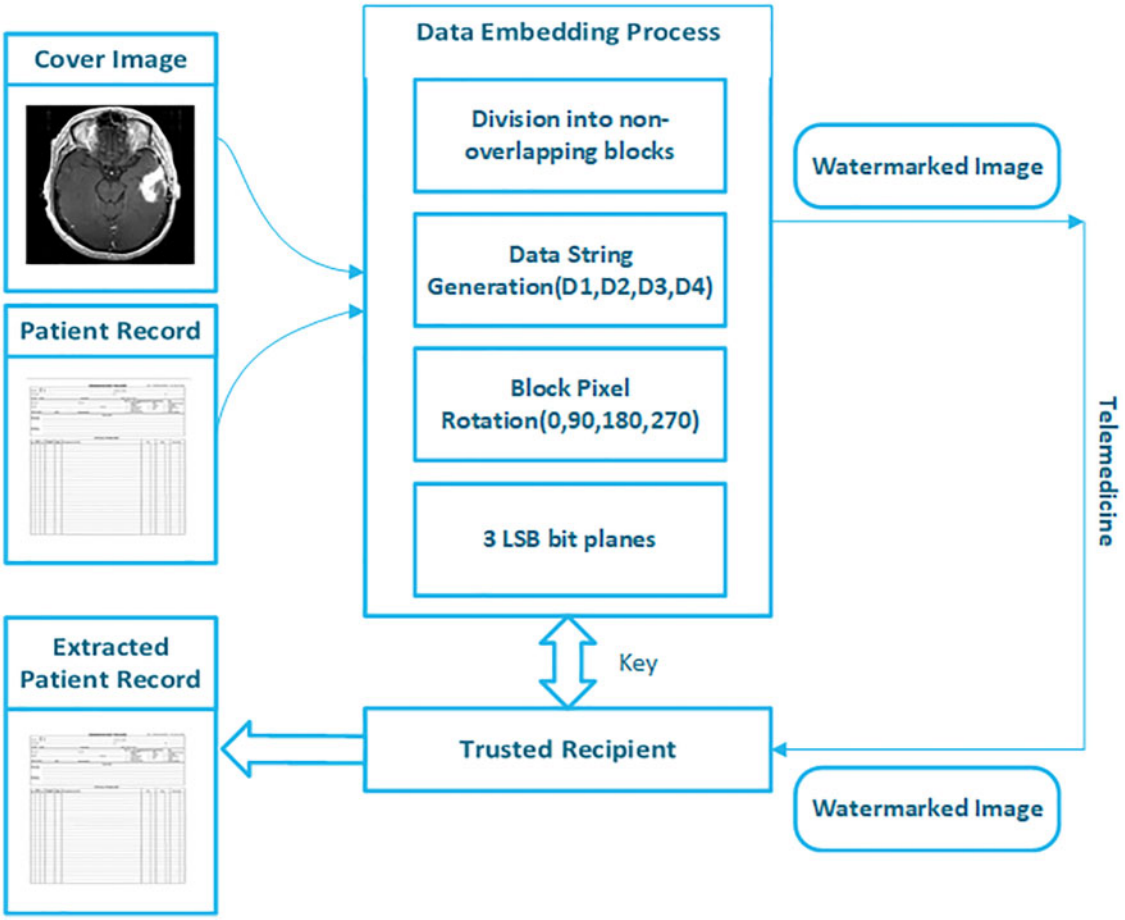


Figure 2: Proposed reversible watermarking system block diagram

3.2 Effective Embedding Capacity

Block size determines the effective embedding capacity; besides rotation bits data as explained in the embedding process, the number of bits required for embedding data is bl^2-2 for the block size of *l*. where

$$4 \leq l \leq min(\frac{m}{2}, \frac{n}{2}) \tag{2}$$

The effective embedding capacity will be

$$\frac{bl^2 - 2}{bl^2} \tag{3}$$

b denotes the number of bitplanes used for embedding, and *l* represents the block size. Data embedding is done using the three least significant bit planes in the proposed methodology. As explained in the data embedding process, two bits b1b2 will be placed at the upper left side of the selected block least significant bit concerning each block rotation. In the case of 4 × 4 block size, the total number of pixels available in the block is 16, so the maximum number of embedding bits available is 16 × 3 = 48 as the last three bits are used for embedding, 46 Effective Embedding bits are available, and .958 is effective embedding.

3.3 Embedding Phase

3.3.1 Cover Image Block

The first phase in embedding the patient data is determining the number of bytes available for modification in the cover image. The embedding phase will begin If the number of cover image bytes available for embedding is higher than or equal to the number of patient records; otherwise, an error message will appear. The cover image C_{image} of size 512 × 512 is divided into 4 × 4 non-overlapping blocks to minimize the complexity of the location map.

3.3.2 Cover Image Pixel Sequence

After splitting the cover image into blocks, the preceding steps are performed for each block. The pixel sequence is defined by a unique random path in the block. [log l^2] bits are required to display the final block sequence number leading to l^2 [log l^2] bits to define each element unique in a block of size *lxl*. These bits are part of the hidden key. The integrated data bits information for each block will be only accessible to the authorized receivers. b bitplanes can be used for embedding patient records in medical image pixels. This quantity *b* is based on the size of the concealed data, but to minimize the distortion of the medical image within an acceptable level, a maximum of four-bit planes are employed for the embedding procedure. The patient record information is transformed from text to bits, and The bit string is further equally grouped into the size of bl^2-2 substrings data, Data strings D_0; D_1; D_2; D_3 of four bits long bl^2 will be generated from each substring of data bl^2-c bits. The data bit string will be modified as

$$D_1, D_2, \ldots, D_{l^2}, D_{l^2+1}, \ldots, D_{2l^2}, \ldots, D_{(b-1)l^2+1}, \ldots, D_{bl^2} \tag{4}$$

3.3.3 Cover Image Block Rotation

After embedding b1b2 at the ideal location, keeping in mind the security perspective, every four rotations will be evaluated employing numerous objective functions, and the optimum performance will be preferred. Two bits b1b2 (00; 01; 10; 11) denotes the pixel rotation in each block with four angels (0^0; 90^0; 180^0; 270^0), respectively. These bits would be positioned in the concealed data string such that they embed in the least significant bits of two upper left corners pixel in the block. These bits b1b2 determine the efficient and effective embedding capacity based on the block size. When the data set of bits for the patient record and pixel sequence of the block are determined, we add ±1 to each modifiable pixel to embed the patient record in the cover image. The value of a pixel's LSB measured by the algorithm specifies the appropriate additive value for that pixel in the block.

Algorithm 1: Data Embedding Process

```
Input: Cover image, patient record, key
Output: Watermarked image
1: Create a $4 \times 4$ block size of the cover image
2: Create chunks of patient record $bl^2$-c, where b represent LSB bit planes, $c = 2$
3: Create data string $D_0$; $D_1$; $D_2$; $D_3$
4: Locate ideal path in block
```

(Continued)

Algorithm 1: (Continued)

```
5: Find pixel rotation in block (0°; 90°; 180°; 270°)
6: Calculate each pixel's additive value (+1 or –1)
7: Embed data
```

3.4 Extraction Phase

The data extraction process is much simpler than the data embedding process. As explained earlier, the maximum block size of an image 512 × 512 can have 256. As a result, the initial eight bits of the string indicate the pixel block size in the key. Therefore the very first eight bits are dissociated from the key. The preceding three bits indicate the count of bit planes selected during the embedding process and are thus dissociated from the key. The rest of the key bits determine the random path specified for the data embedding. We stated that the rotation bits (b1b2) are located in the top-left pixels of LSB in the block at the embedding phase. The block is rotated back in the extraction process by an angle defined by rotation bits. Pixels are then positioned in the exact order as the key dictates, and data from the LSB bit planes of every block can be recovered.

Algorithm 2: Data Embedding Process

```
Input: Watermarked image, key
Output: Patient record information
1: Get key information
2: Find the random path of each block
3: Block rotation based on rotation bits
4: Pixel order indicated by the key
5: Extract data
```

4 Results and Discussion

This section discusses the proposed methodology performance analysis, comparing the detailed studies with numerous traditional algorithms to verify the efficiency of this proposed model. "MATLAB 2020a" is used in this research for the implementation of experiments. PC with Windows 10, 3.5-GHz CPU, and 4 GB of RAM.

4.1 Data Set

We tested different sample images from a data archive1 to evaluate our methodology. Fig. 3 represents patients' images for cancer from n1–n10 that are negative cases, whereas images from y1–y2 are positive cases. The sample images are medical images of an 8-bit depth grayscale. The patient record sizes are 8 KB, 16 KB, and 32 KB.

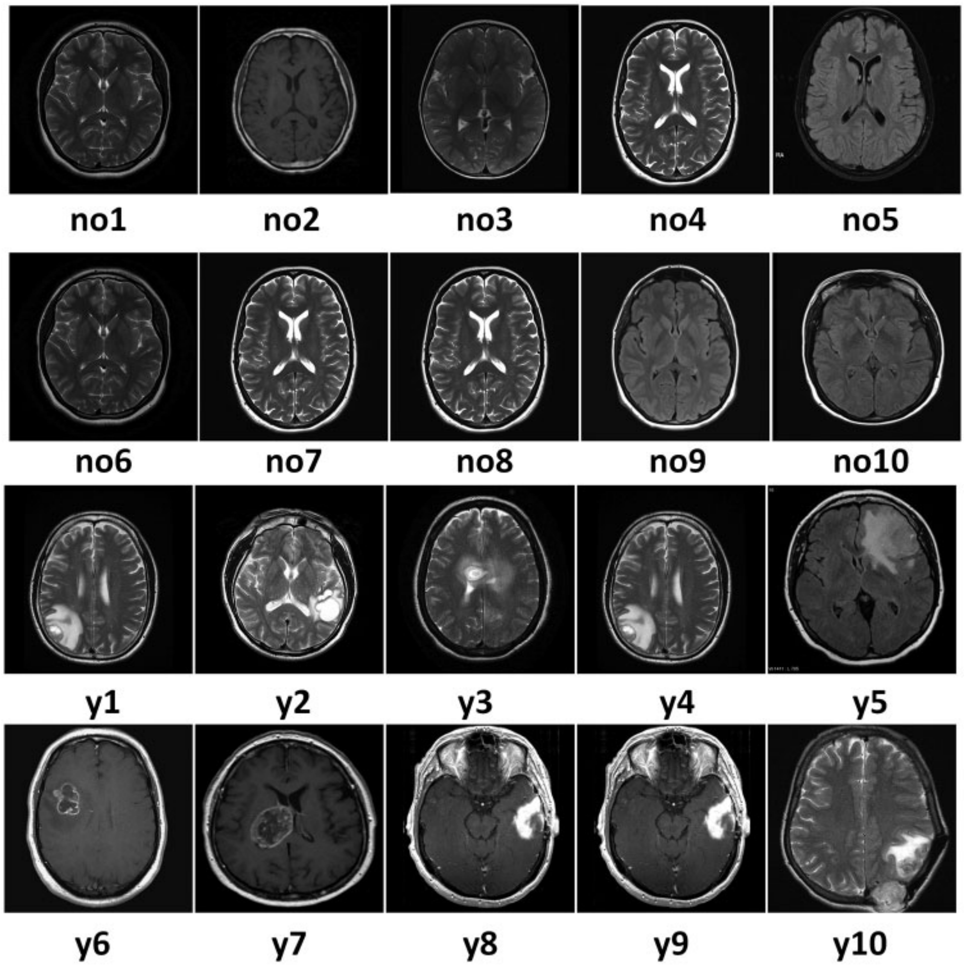


Figure 3: The collection of MRI grayscale BMP cover images for experiments. Cancer images with the normal condition are represented from n1–n10, and cancer images with the abnormal condition are represented from y1–y2

4.2 Performance Metrics

Peak signal-to-noise ratio (PSNR), mean square error (MSE), and structural similarity index metrics (SSIM) are used to assess perceptual invisibility. PSNR analyzes the cover image with the watermarked image in terms of the maximum possible value (power). An image with a PSNR of infinity is identical, whereas any PSNR higher than 35 dB is acceptable, and higher is preferred.

$$PSNR = 20log_{10}\left(\frac{Max}{\sqrt{MSE}}\right) \tag{5}$$

MAX denotes the maximum pixel value of the image. The mean square error (MSE) is defined as follows:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\left(O(i,j) - W(i,j)\right)^2 \tag{6}$$

where m, n denotes the size of the pixels, and O and W denote the original and cover images, respectively. The Structural Similarity Index is defined as follows:

$$SSIM(o,w) = [l(o,w)]^{\alpha} \cdot [c(o,w)]^{\beta} \cdot [s(o,w)]^{\gamma} \tag{7}$$

The metric SSIM (Structural Similarity Index) extracts three main attributes from an image: Luminance, Contrast, and Structure. For the two images O and W, these are computed as follows:

$$l(o,w) = \left(\frac{2\mu o\mu w + c1}{\mu_o^2 + \mu_w^2 + c1}\right) \tag{8}$$

$$c(o,w) = \left(\frac{2\sigma_o\sigma_w + c2}{\sigma_o^2 + \sigma_w^2 + c2}\right) \tag{9}$$

$$s(o,w) = \left(\frac{\sigma_{ow} + c3}{\sigma_o\sigma_w + c3}\right) \tag{10}$$

4.3 Results and Analysis

We analyzed our methodology at the cover image's maximum payload capacity to ensure that it is efficient. The numerical results of PSNR, SSIM, and MSE reveal that the watermark images are imperceptible and that human eyes are unable to discriminate between visual variations in the watermark images. The suggested methodology attains the average PSNR value of 44.22 dB on 512 × 512 dimensions with data embedding up to 32 KB and employing all three LSBs. Table 1 displays the cover image quality measures for 8 KB, 16 KB, and 32 KB. Fig. 4 displays a graphical representation of the proposed algorithm. The desired scheme performance is carefully analyzed by subjecting it to numerous attacks. Normalized correlation (NC) is used to assess the robustness of the implemented watermarking methodology under filtering, geometric, enhancement, compression, and noise attacks. This NC value should be greater than 0.9 to ensure that the method will resist attacks. Table 2 represents the proposed algorithm strength for various attacks—the SSIM values for geometric attacks and 0.19 for cropping attacks for y3 and y4 images. PSNR value for histogram equalization of no8 image is highest 49.30 dB, and y3 image has the lowest PSNR of 8.7 dB. The minimum NC value calculated from all attacks is 0.97. The watermarked image was exposed to various filtering attacks. The cover images were exposed to Gaussian(3 × 3), median (3 × 3), and wiener filter (3 × 3). The average NC value of filter attack is 0.99, y3 image has the highest PSNR value of 47.58 for Gaussian attack, whereas wiener attack has the lowest value of PSNR 21.16 for y3 cover image.

Table 1: Results of having 8 KB, 16 KB, and 32 KB embedding data size watermarked images of 512 × 512 dimensions

		8 KB			16 KB			32 KB	
Image	PSNR	SSIM	MSE	PSNR	SSIM	MSE	PSNR	SSIM	MSE
nol	45.36	0.999	0.75	42.36	0.999	0.75	38.36	0.99	4.75
no2	49.61	0.993	0.84	46.61	0.993	0.84	41.65	0.99	4.84
no3	52.54	0.993	0.84	50.54	0.993	0.84	43.54	0.97	2.87
no4	52.37	0.999	0.37	52.37	0.999	0.37	48.1	0.98	0.4

(Continued)

Table 1 (continued)

	8 KB			16 KB			32 KB		
Image	PSNR	SSIM	MSE	PSNR	SSIM	MSE	PSNR	SSIM	MSE
no5	54.37	0.999	0.37	54.37	0.999	0.37	52.1	0.98	0.3
no6	45.36	0.99	0.75	45.36	0.99	0.75	41.36	0.99	4.7
no7	52.37	0.999	0.37	51.37	0.999	0.37	50.1	0.97	0.6
no8	46.74	0.995	0.37	46.74	0.995	0.37	46.74	0.96	1.37
no9	50.5	0.999	0.57	50.5	0.999	0.57	46.74	0.99	1.37
no10	45.79	0.999	0.3	41.79	0.999	0.8	41.79	0.99	4.3
y1	50.5	0.999	0.57	48.5	0.999	0.57	48.5	0.98	0.57
y2	50.5	0.999	0.57	51.5	0.999	0.57	44.5	0.98	0.57
y3	50.5	0.999	0.57	47.5	0.999	0.57	43.5	0.98	0.56
y4	50.5	0.999	0.57	50.5	0.999	0.57	48.5	0.97	0.8
y5	50.54	0.999	0.57	48.54	0.99	0.57	41.61	0.97	4.84
y6	43.87	0.99	0.66	43.87	0.99	2.66	39.54	0.99	2.87
y7	50.5	0.99	0.57	47.5	0.99	0.57	45.1	0.99	0.4
y8	50.5	0.999	0.57	45.5	0.97	0.57	43.1	0.99	0.4
y9	50.5	0.999	0.57	48.5	0.91	0.57	41.36	0.99	4.7
y10	44.18	0.994	0.48	41.18	0.98	2.48	38.1	0.98	0.4
Average	49.355	0.9966	0.5615	47.755	0.98955	0.7865	44.2145	0.98	2.08

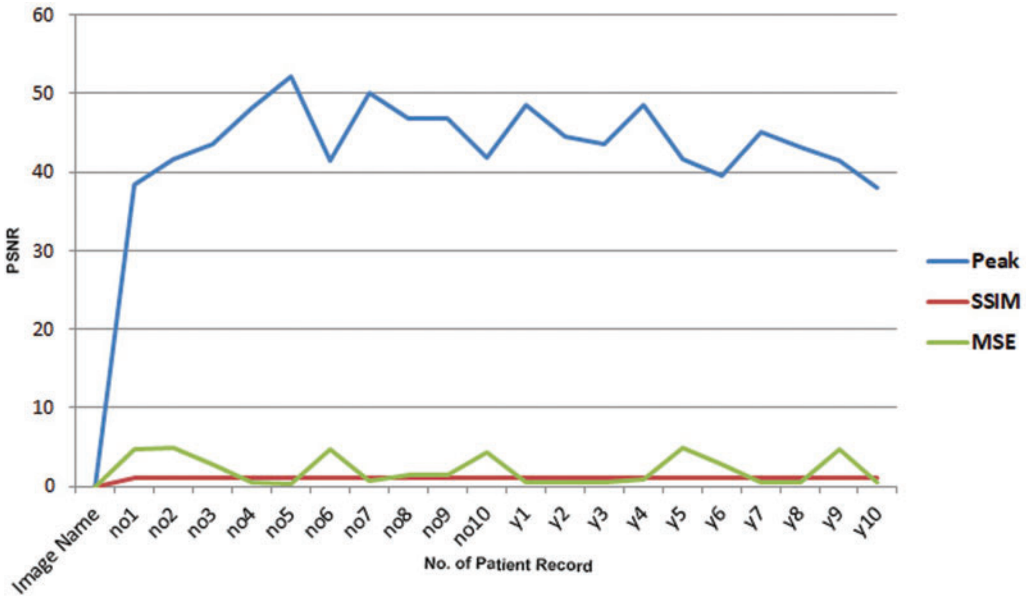


Figure 4: Graphical representation of PSNR, SSIM, and MSE at 32 KB patient record after implementing the proposed algorithm

Table 2: Robustness and imperceptibility analysis of watermark under different attacks

Attacks	y3			no8			y4			no4		
	PSNR	SSIM	NC	PSNR	SSIM	NC	PSNR	SSIM	NC	PSNR	SSIM	NC
Salt & pepper noise(0.001)	34.12	0.97	0.99	33.47	0.96	0.98	31.13	0.97	0.99	33.85	0.97	0.99
Salt & pepper noise(0.0002)	41.5	0.99	0.99	40.74	0.99	0.99	41.90	1.00	0.99	43.30	0.99	0.99
Gaussian noise(0.0002)	37.72	0.86	0.99	36.71	0.87	0.99	36.72	0.87	0.99	38.54	0.87	0.99
Gaussian noise(0.010, 0.0002)	35.31	0.76	0.99	34.23	0.84	0.99	36.31	0.76	0.99	36.29	0.86	0.99
Speckle noise(0.0001)	47.63	0.99	0.99	45.17	0.99	0.99	47.63	1.00	0.99	47.55	0.97	0.99
Histogram equalization	48.7	0.31	0.99	49.30	0.35	0.99	48.73	0.31	0.99	44.83	0.81	0.99
Sharpening	39.52	0.98	0.99	39.32	0.99	0.99	39.52	0.98	0.99	47.19	0.99	0.99
Gaussian filter(3 × 3)	47.58	0.99	0.99	44.69	0.99	0.99	45.59	1.00	0.99	47.43	0.99	0.99
Median filter(3 × 3)	40.82	0.97	0.99	43.33	0.99	0.99	41.82	0.98	0.99	40.40	0.98	0.99
Wiener filter(3 × 3)	21.61	0.22	0.99	21.04	0.23	0.99	21.62	0.23	0.99	44.81	0.98	0.99
JPEG Compression(80)	43.45	0.98	0.99	43.76	0.99	0.99	43.46	0.98	0.99	42.94	0.98	0.99
JPEG Compression(90)	46.08	0.98	0.99	45.62	0.99	0.99	46.09	0.99	0.99	45.29	0.99	0.99
Rotation(2°)	16.68	0.55	0.99	14.69	0.65	0.99	13.69	0.55	0.98	18.27	0.65	0.98
Gamma correction(0.8)	25.25	0.91	0.99	24.33	0.85	0.99	23.25	0.91	0.99	24.69	0.98	0.99
Scaling(2, 0.5)	43.9	0.24	0.99	33.77	0.38	0.99	13.12	0.25	0.99	48.48	0.99	0.99
Cropping	8.7	0.19	0.99	11.05	0.32	0.99	10.50	0.19	0.99	17.40	0.81	0.99
Shearing(0.2, 0.2)	14.3	0.41	0.99	13.24	0.35	0.99	12.40	0.42	0.97	10.75	0.43	0.97
Motion blur	24	0.76	0.99	21.69	0.82	0.97	22.00	0.77	0.99	36.13	0.94	0.99
Translation [20,20]	14.52	0.46	0.99	13.77	0.57	0.99	12.50	0.47	0.99	14.71	0.59	0.99

4.4 Evaluation and Discussion

The proposed method was compared with the state-of-the-art technique [2] to determine its performance on UCID dataset2 as seen in Fig. 5, the collection of medical images were randomly chosen. Table 3 represents the calculated PSNR, SSIM values of selected images. The average PSNR and SSIM values of [2] are 43.23 and 0.92, respectively, whereas our methodology significantly improves PSNR of 45.00 and SSIM of 0.99. Table 4 represents the performance evaluation of the proposed methods with a standard dataset of images Barbara, Baboon, Cameraman, Lena, Peppers. The results of six different methodologies Bailey et al. [53], Jassim [54], Karim et al. [11], Muhammad et al. [55], Rehman et al. [56], and Siddiqui et al. [2], are displayed in Table 2. Since PSNR is always greater than 30 dB, human eyes cannot perceive distortion. The PSNR value of our proposed method as compared to [53–56] and Siddiqui et al. [2] shows better results on 857 bits.

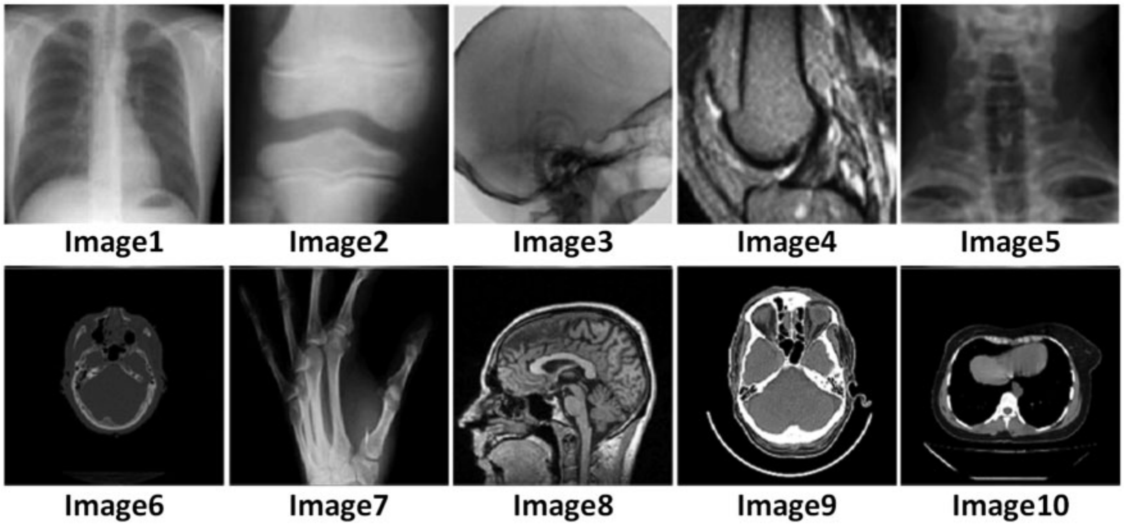


Figure 5: A set of 512 × 512 medical images randomly selected for comparison purposes

Table 3: PSNR and SSIM performance analysis with the state-of-the-art technique on a collection of randomly selected medical images

S. No.	Siddiqui et al. [2]		Proposed method	
	PSNR	SSIM	PSNR	SSIM
Image1	46.61	0.99	48.70	0.99
Image2	45.54	0.99	43.54	0.98
Image3	44.76	0.99	41.03	0.99
Image4	44.70	0.99	49.28	0.99
Image5	43.61	0.98	43.94	0.99
Image6	41.33	0.84	40.13	0.99
Image7	41.08	0.82	43.61	0.99
Image8	43.35	0.99	45.50	0.99
Image9	41.02	0.80	48.85	0.99
Image10	40.29	0.76	45.43	0.99
Average	43.23	0.92	45.00	0.99

Table 4: PSNR result of the standard set images with 512x512 dimensions at 104,847 embedding bits

Watermark image	Bailey et al. [53]	Jassim [54]	Karim et al. [11]	Muhammad et al. [55]	Rehman et al. [56]	Siddiqui et al. [2]	Proposed
Barbara	46.11	43.6	40.99	47.34	50.45	48.42	47.54
Baboon	44.67	44.75	44.66	49.1	52	50.08	49.34
Cameraman	44.59	45.21	41.56	48.02	50.98	47.88	50.58
Lena	44.12	44.93	42.95	50.01	51.05	49.83	48.3
Peppers	35.04	34.02	31.23	39.38	49.44	50.15	50.67
Average	42.9	42.5	40.28	46.77	50.78	49.27	49.29

We improved the effectiveness of the suggested approach with Rehman et al. [56] by increasing patient data to the maximum size of 235,929 bits since embedding a greater data size with a higher SNR indicates the performance of the watermarking strategy. The suggested scheme achieves the minimum PSNR value of 45.22 dB by hiding 235,929 and employing all three LSBs. Fig. 6 represents a graphical comparison of the proposed algorithm with the state of art methodologies.

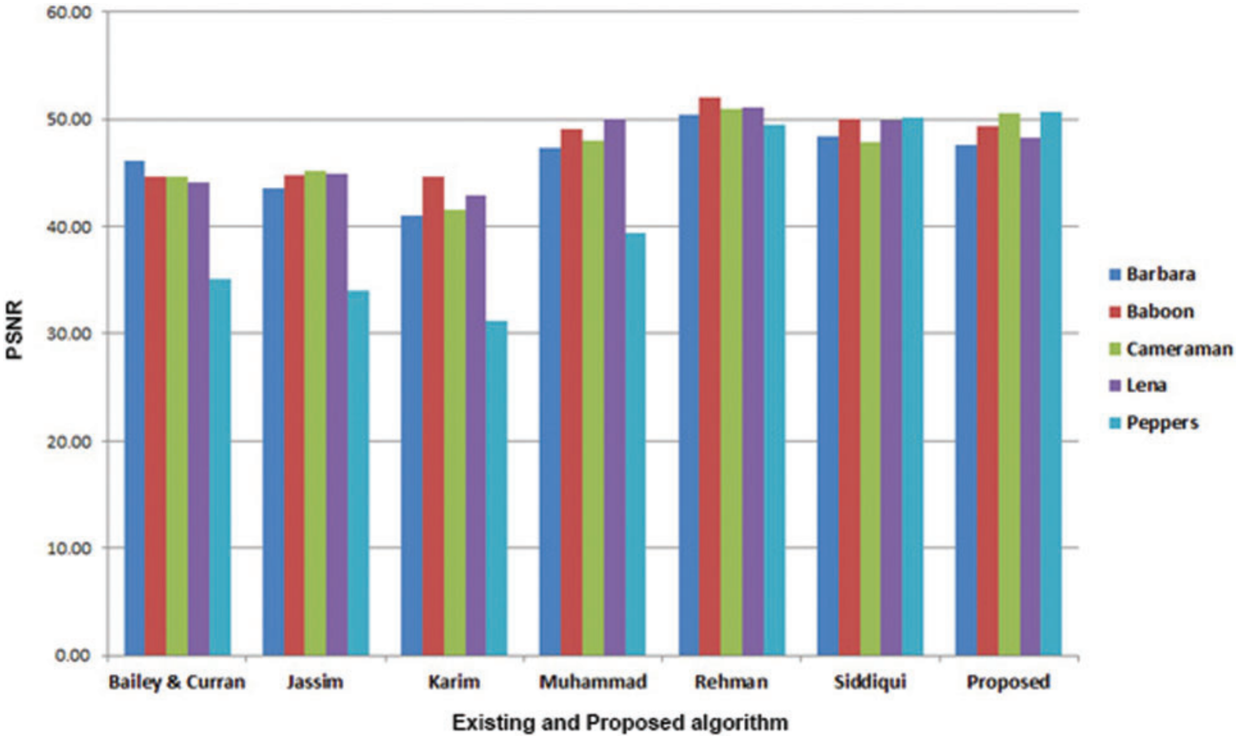


Figure 6: Graphical representation of proposed algorithm with state of art methodologies

4.5 Summary of Results

Based on the above experimental analyses, we can draw the conclusion:

- It is found that the suggested methodology performs better than other schemes. Compared to standard LSB and the other state-of-the-art watermarking systems based on reversible watermarking, the proposed method offers a higher PSNR.
- Even if the embedding capacity is increased, the suggested methodology produces high-quality watermarked images.
- It is noted that the visual quality of the watermarked image is undetectable. The human eye cannot differentiate between the cover image and watermarked image.

5 Conclusions

In this research paper, a novel reversible watermarking algorithm is proposed. The proposed algorithm is also evaluated under different attacks and shows better results, and it can be applied to medical images and standard images (Barbara, Baboon, Cameraman, Lena, Peppers) for reversible watermarking with better performance for medical images. The proposed algorithm generates an ideal random path among all paths for pixel blocks with minimum bit flipping to improve image imperceptibility. The embedding and extraction process is done by a key that contains information about the selected random path and pixel rotation in the blocks. The degradation of the image is proven by visual quality and structural similarity parameters PSNR, SSIM, and MSE. The calculated values of parameters always come in the acceptable range. In future research, we aim to develop a new framework of the reversible watermarking algorithm for color images.

Funding Statement: This work is supported by the National Natural Science Foundation of China (Grant No. 61762060), Educational Commission of Gansu Province, China (Grant No. 2017C-05), Foundation for the Key Research and Development Program of Gansu Province, China (Grant No. 20YF3GA016). This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project No. RSP-2022/184. The work of author Ayman Radwan was supported by FCT/MEC through Programa Operacional Regional do Centro and by the European Union through the European Social Fund (ESF) under Investigator FCT Grant (5G-AHEAD IF/FCT-IF/01393/2015/CP1310/CT0002).

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

References

1. Taj, R., Tao, F., Khurram, S., Rehman, A. U., Haider, S. K. et al. (2022). Reversible watermarking method with low distortion for the secure transmission of medical images. *Computer Modeling in Engineering & Sciences, 130(3),* 1309–1324. DOI 10.32604/cmes.2022.17650.
2. 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.6287639.
3. Almogren, A., Mohiuddin, I., Din, I. U., Almajed, H., Guizani, N. (2020). FTM-IoMT: Fuzzy-based trust management for preventing Sybil attacks in Internet of Medical Things. *IEEE Internet of Things Journal, 8(6),* 4485–4497. DOI 10.1109/JIoT.6488907.

4. Din, I. U., Almogren, A., Guizani, M., Zuair, M. (2019). A decade of Internet of Things: Analysis in the light of healthcare applications. *IEEE Access, 7,* 89967–89979. DOI 10.1109/Access.6287639.
5. Li, Y. M., Wei, D., Zhang, L. (2021). Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain. *Information Sciences, 551,* 205–227. DOI 10.1016/j.ins.2020.11.020.
6. Mansor, N. K., Asraf, S. M. H., Idrus, S. Z. S. (2020). Steganographic on pixel value differencing in iris biometric. *Journal of Physics: Conference Series, 1529(3),* 032078. DOI 10.1088/1742-6596/1529/3/032078.
7. Suman, D., Ranade, S. K. (2017). A secure steganographic method using modified lsb (least significant bit) substitution. *International Journal of Advanced Research in Computer Engineering & Technology, 6(8),* 1268–1273.
8. Douglas, M., Bailey, K., Leeney, M., Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications, 77(13),* 17333–17373. DOI 10.1007/s11042-017-5308-3.
9. Sahu, A. K., Swain, G., Babu, E. S. (2018). Digital image steganography using bit flipping. *Cybernetics and Information Technologies, 18(1),* 69–80. DOI 10.2478/cait-2018-0006.
10. Solak, S., Altınışık, U. (2019). Image steganography based on LSB substitution and encryption method: Adaptive LSB 3. *Journal of Electronic Imaging, 28(4),* 043025. DOI 10.1117/1.JEI.28.4.043025.
11. 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 (ICCIT 2011)*, pp. 286–291. Dhaka, Bangladesh.
12. Luo, W., Huang, F., Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security, 5(2),* 201–214. DOI 10.1109/TIFS.2010.2041812.
13. Sahu, A. K., Swain, G. (2019). A novel n-right most bit replacement image steganography technique. *3D Research, 10(1),* 1–18. DOI 10.1007/s13319-018-0211-x.
14. Ray, P. P., Chowhan, B., Kumar, N., Almogren, A. (2021). BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem. *IEEE Internet of Things Journal, 8(13),* 10857–10872. DOI 10.1109/JIOT.2021.3050703.
15. Liu, Y., Chang, C. C., Huang, P. C., Hsu, C. Y. (2018). Efficient information hiding based on theory of numbers. *Symmetry, 10(1),* 19. DOI 10.3390/sym10010019.
16. Leng, H. S., Tseng, H. W. (2019). Generalize the EMD scheme on an n-dimensional hypercube with maximum payload. *Multimedia Tools and Applications, 78(13),* 18363–18377. DOI 10.1007/s11042-019-7228-x.
17. Prasad, S., Pal, A. K. (2017). An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science, 4(4),* 161066. DOI 10.1098/rsos.161066.
18. Kim, P. H., Yoon, E. J., Ryu, K. W., Jung, K. H. (2019). Data-hiding scheme using multidirectional pixel-value differencing on colour images. *Security and Communication Networks, 2019,* 1–12. DOI 10.1155/2019/9038650.
19. Li, Z., He, Y. (2018). Steganography with pixel-value differencing and modulus function based on PSO. *Journal of Information Security and Applications, 43,* 47–52. DOI 10.1016/j.jisa.2018.10.006.
20. Yang, C. H., Weng, C. Y., Tso, H. K., Wang, S. J. (2011). A data hiding scheme using the varieties of pixel-value differencing in multimedia images. *Journal of Systems and Software, 84(4),* 669–678. DOI 10.1016/j.jss.2010.11.889.
21. 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.
22. Darabkh, K. A., Al-Dhamari, A. K., Jafar, I. F. (2017). A new steganographic algorithm based on multi directional PVD and modified LSB. *Information Technology and Control, 46(1),* 16–36. DOI 10.5755/j01.itc.46.1.15253.

23. Swain, G. (2019). Very high capacity image steganography technique using quotient value differencing and LSB substitution. *Arabian Journal for Science and Engineering, 44(4),* 2995–3004. DOI 10.1007/s13369-018-3372-2.

24. Muhammad, S. M., Yasir, S., Ahmad, A., Jehangir, A., Mujataba, H. J. et al. (2022). Forensic analysis on internet of things (IoT) device using machine to machine (M2 M) framework. *Electronics, 11(7),* 1126. DOI 10.3390/electronics11071126.

25. Khan, S. R., Sikandar, M., Almogren, A., Din, I. U., Guerrieri, A. et al. (2020). IoMT–Based computational approach for detecting brain tumor. *Future Generation Computer Systems, 109,* 360–367. DOI 10.1016/j.future.2020.03.054.

26. Pradhan, A., Sekhar, K. R., Swain, G. (2018). Digital image steganography using LSB substitution, PVD, and EMD. *Mathematical Problems in Engineering, 2018(1),* 1–11. DOI 10.1155/2018/1804953.

27. Sahu, A. K., Swain, G. (2019). Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis. *International Journal of Electronic Security and Digital Forensics, 11(4),* 458–476. DOI 10.1504/IJESDF.2019.102567.

28. Maji, G., Mandal, S., Sen, S., Debnath, N. C. (2018). Dual image based LSB steganography. *2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, pp. 61–66. Ho Chi Minh City, Vietnam.

29. Wu, N. I., Wu, K. C., Wang, C. M. (2012). Exploring pixel-value differencing and base decomposition for low distortion data embedding. *Applied Soft Computing, 12(2),* 942–960. DOI 10.1016/j.asoc.2011.09.002.

30. Yadav, G. S., Ojha, A. (2018). A reversible data hiding scheme with high security and improved embedding capacity. *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, pp. 1555–1559. New York, NY, USA.

31. Chan, C. K., Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37(3),* 469–474. DOI 10.1016/j.patcog.2003.08.007.

32. Bibi, N., Sikandar, M., Din, I. U., Almogren, A., Ali, S. (2020). IoMT-Based automated detection and classification of leukemia using deep learning. *Journal of Healthcare Engineering, 2020,* 1–12. DOI 10.1155/2020/6648574.

33. Mohammadi, A., Nakhkash, M., Akhaee, M. A. (2020). A high-capacity reversible data hiding in encrypted images employing local difference predictor. *IEEE Transactions on Circuits and Systems for Video Technology, 30(8),* 2366–2376. DOI 10.1109/TCSVT.76.

34. Lin, C. C., Tsai, W. H. (2004). Secret image sharing with steganography and authentication. *Journal of Systems and Software, 73(3),* 405–414. DOI 10.1016/S0164-1212(03)00239-5.

35. Luo, X. Y., Wang, D. S., Wang, P., Liu, F. L. (2008). A review on blind detection for image steganography. *Signal Processing, 88(9),* 2138–2157. DOI 10.1016/j.sigpro.2008.03.016.

36. Yadav, G. S., Ojha, A. (2018). Secure data hiding scheme using shape generation algorithm: A key based approach. *Multimedia Tools and Applications, 77(13),* 16319–16345. DOI 10.1007/s11042-017-5200-1.

37. Liao, X., Hahsmi, M. A., Haider, R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. *Optik–International Journal for Light and Electron Optics, 153,* 117–134. DOI 10.1016/j.ijleo.2017.09.099.

38. Valandar, M. Y., Barani, M. J., Ayubi, P. (2019). A fast color image encryption technique based on three dimensional chaotic map. *Optik, 193,* 162921. DOI 10.1016/j.ijleo.2019.06.021.

39. Gndurc, J. (2015). State-of-the-art review on steganographic techniques. *International Journal of Signal Processing. Image Processing and Pattern Recognition, 8(7),* 161–170. DOI 10.14257/ijsip.

40. Rabara, V., Goswami, A. (2015). A survey of image based steganography. *International Journal of Computer Engineering and Sciences, 1(2),* 1–4. DOI 10.26472/ijces.v1i2.11.

41. Shaik, A., Thanikaiselvan, V., Amitharajan, R. (2017). Data security through data hiding in images: A review. *Journal of Artificial Intelligence, 10(1),* 1–21. DOI 10.3923/jai.2017.1.21.

42. Sahu, A. K., Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. *Indonesian Journal of Electrical Engineering and Computer Science, 2(3),* 712–719. DOI 10.11591/ijeecs.v2.i3.pp712-719.

43. Dumitrescu, S., Wu, X., Memon, N. (2002). On steganalysis of random LSB embedding in continuous-tone images. *Proc. International Conference on Image Processing*, pp. 641–644. Rochester, NY, USA.

44. Almogren, A. S. (2015). Developing a powerful and resilient smart body sensor network through hypercube interconnection. *International Journal of Distributed Sensor Networks, 11(10),* 609–715.

45. Liao, X., Yin, J., Guo, S., Li, X., Sangaiah, A. K. (2018). Medical JPEG image steganography based on preserving inter-block dependencies. *Computers & Electrical Engineering, 67,* 320–329. DOI 10.1016/j.compeleceng.2017.08.020.

46. Ni, Z., Shi, Y. Q., Ansari, N., Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology, 16(3),* 354–362. DOI 10.1109/TCSVT.2006.869964.

47. Sahu, A. K., Swain, G. (2018). Pixel overlapping image steganography using PVD and modulus function. *3D Research, 9(3),* 1–14. DOI 10.1007/s13319-018-0188-5.

48. Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology, 13(8),* 890–896. DOI 10.1109/TCSVT.2003.815962.

49. Iranpour, M. (2013). LSB–Based steganography using Hamiltonian paths. *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 586–589. Beijing, China.

50. Iranpour, M., Safabakhsh, R. (2015). Reducing the embedding impact in steganography using Hamiltonian paths and writing on wet paper. *Multimedia Tools and Applications, 74(17),* 6657–6670. DOI 10.1007/s11042-014-1921-6.

51. Sahu, A. K., Swain, G. (2019). High fidelity based reversible data hiding using modified LSB matching and pixel difference. *Journal of King Saud University–Computer and Information Sciences, 34(4),* 1395–1409. DOI 10.1016/j.jksuci.2019.07.004.

52. Zhang, W., Wang, S., Han, W., Yu, H., Zhu, Z. (2020). An image encryption algorithm based on random Hamiltonian path. *Entropy, 22(1),* 73. DOI 10.3390/e22010073.

53. 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.

54. Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.

55. 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. *KSII Transactions on Internet and Information Systems , 9(5),* 1938–1962. DOI 10.3837/tiis.2015.05.022.

56. 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.