Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2017) 25: 461 – 473

doi:10.3906/elk-1506-189

A new efficient block matching data hiding method based on scanning order selection in medical images

Turgay AYDOĞAN[1,*], **Cüneyt BAYILMIŞ**[2]

[1]Institute of Science and Technology, Sakarya University, Sakarya, Turkey

[2]Department of Computer Engineering, Faculty of Computer and Information Sciences, Sakarya University, Sakarya, Turkey

Received: 22.06.2015 • **Accepted/Published Online:** 29.12.2015 • **Final Version:** 24.01.2017

Abstract: Digital technology and the widespread use of the Internet has increased the speeds at which digital data can be obtained and shared in daily life. In parallel to this, there are important concerns regarding the confidentiality of private data during data transmissions and the possibility that data might fall into the hands of third parties. Issues relating to data safety can also affect patients' medical images and other information relating to these images. In this study, we propose a new method based on block matching that can be used to hide the patient information in medical images. In this method, 8 scanning orders (6 of which are newly designed) are developed to provide high image quality. By diversifying the number of scanning orders, we aim to achieve the lowest number of bit changes. The performance of the developed method is measured using the number of bits subject to change, the peak signal-to-noise ratio and the mean structural similarity index measure image quality assessment metrics, and steganalysis attacks. The method we developed was found to be more effective in hiding data compared to the classical least significant bit method.

Key words: Steganography, data hiding, block matching, least significant bit, least significant bit replacement

1. Introduction

In parallel to the rapid developments in medical technologies, there has been an increase in the quantity of images, videos, and sound data generated and processed by medical devices [1]. Such data are expected to enhance the quality of health services and to facilitate the sharing of information between units/departments providing medical services. On the other hand, these medical data may contain highly critical and sensitive information, which can be threatened by third parties willing to access or retrieve them [2]. The protection of medical data against various security problems during their transmission through communication media has become an important issue for health services. These sensitive and personal medical data can be protected using steganography, which represents one of the major types of data hiding methods [3–5].

Etymologically, the word steganography is derived from Greek words meaning "covered writing". Steganography has been used in many different forms for thousands of years [6]. In steganography, the objects used for hiding the secret data are called cover objects, which can be text, image, video, sound data, etc. The combination of the cover object and the secret data hidden by it is called the stego object, which may appear as an ordinary text, image, video, or sound data [7–9].

Many steganographic methods have been developed in the past few decades. The simplest and most

*Correspondence: turgayaydogan@yahoo.com

commonly used of these methods is the least significant bit (LSB) method [8,10]. Attention must be paid to two features when designing a data hiding algorithm: one of these is the undetectability of the secret data, while the other is the data hiding capacity. For many data hiding applications, the most important demand is the undetectability of the data. It is possible to prevent the hidden data from being noticed by using a cover object that is visually or digitally similar to the secret data that are hidden [11].

An evaluation of the literature shows that there are numerous studies on medical images including the hidden patients' medical pasts, patient information, and patient reports. In a study conducted by Zhou et al., it is possible to see that patient-related data were hidden on breast radiography images. In the same study, Zhou et al. also concealed certain important information on these images, along with the digital signature information they had formed using mathematical techniques [12].

Luo et al. developed a data hiding method for medical images, designed for use in e-diagnosis applications. Within the medical image, they concealed all data relating to the patients, including the patients' personal information, history, tests, and diagnoses. For data hiding, they made use of the LSB_0, LSB_1, LSB_2, and LSB_3 bits [13]. Srinivasan et al. also developed a steganography method for the secure transmission of medical reports; to hide the patients' medical records, they applied bit plane complexity segmentation steganography to the patients' medical image [14]. Liu et al. developed a secure stenography method for medical images produced by health systems and devices. During the data hiding process, they employed a Hilbert filling curve instead of the zig-zag scanning or the raster scanning order, which are generally used for the scanning of images [3]. On the other hand, Taghipour et al. conducted studies for hiding pathology reports within pathology images. Using the differences that exist between a pixel and its neighboring pixels, they performed a data hiding process that involves increase or decrease of LSB values [15].

In this study, we aimed to develop a new method that would ensure the hiding of information in medical images by performing only a minimum number of bit changes. The data are hidden using an LSB-based approach. The main contribution of this research paper is that, for ensuring as few bit changes as possible, 8 scanning orders are used in a block matching process where 6 of these scanning orders are newly designed. In Section 2 of this article, we provide information regarding the LSB method, while in Section 3, a new method is proposed and described. In Section 4, we provide the performance results and assessments of the proposed method.

2. Classical LSB-based data hiding

The LSB-based data hiding approach is one of the most commonly used data hiding methods [16–18]. LSB-based data hiding approaches are categorized as LSB replacement steganography (LSBR) and LSB matching steganography (LSBM) [19]. When an image is taken as a cover object in LSB-based data hiding approaches, and in case the pixels of the cover image are not the same as the bits of the data that will be hidden using the LSB value, the pixels of the cover image will be manipulated to the LSB value. In data hiding performed using LSBR, the least significant bit of each pixel in the cover image will be substituted with the bit of the data to be hidden. On the other hand, in the LSBM method, if the bit of the cover image and the bit of the data to be hidden are not the same, addition or subtraction will be randomly performed on the pixel value of the cover image [20]. In a 24-bit color image, each red, green, and blue color channel of each pixel has 8 bits. Three bits of information can be hidden in a pixel of a color image. If we assume that the data to be hidden have $(100)_2$ bits, data hiding according to the LSBR will be performed as shown in Table 1. According to Table 1, if the color values of the pixel in which data hiding will be performed are accepted as 238, 216, and 195, and in

case we wish to hide the $(100)_2$ bits into these pixels, we will have to substitute the LSB values of the red and blue color channels by 1 and 0, respectively. As this substitution is performed on the LSB values of the color channels, it is relatively difficult for them to be perceived by the human visual system.

Table 1. Data hiding with the LSBR method on a color image.

	Red	Green	Blue
Initial digital value of the pixel	238	216	195
Initial binary value of the pixel	11101110	11011000	11000011
LSB values of the pixel	0	0	1
The bit value of the data to be hidden	1	0	0
Binary value of the pixel after hiding	1110111**1**	1101100**0**	1100001**0**
Digital value of the pixel after hiding	239	216	194
Number of bits that have changed	1	0	1

The same LSBR method applied to 24-bit RGB images can also be used for 8-bit grayscale images. The only difference will be that, with the grayscale image, only 1 bit of data can be hidden in 1 pixel, in contrast to the RGB image where 3 bits of data can be hidden in 1 pixel.

In data hiding methods, determining the location on the image where the data will be hidden is an important step. In LSB-based methods, scanning methods such as raster scanning order, zig-zag scanning order, or Hilbert filling order are used to determine the data hiding order of the pixels in the image. The raster scanning order is the most commonly used method and involves the scanning of the image line by line, from left to right.

3. The proposed block matching method

Every new data hiding algorithm that is designed aims to increase the quality of the image as well as the capacity of data that can be hidden. Images that have hidden data will be subject to change and distortion. An increase in the level of distortion is associated with a decrease in image quality. High image quality means that the hidden data within the image will also be more secure [20].

With the method proposed in this study, we aim to increase the image quality and to render the image more secure by ensuring that the hidden data remain harder to discern and acquire by third parties. The method is developed using new scanning orders in order to ensure the minimum number of bit changes on the medical image. Figure 1 illustrates the data hiding, transmission, and data extracting processes.

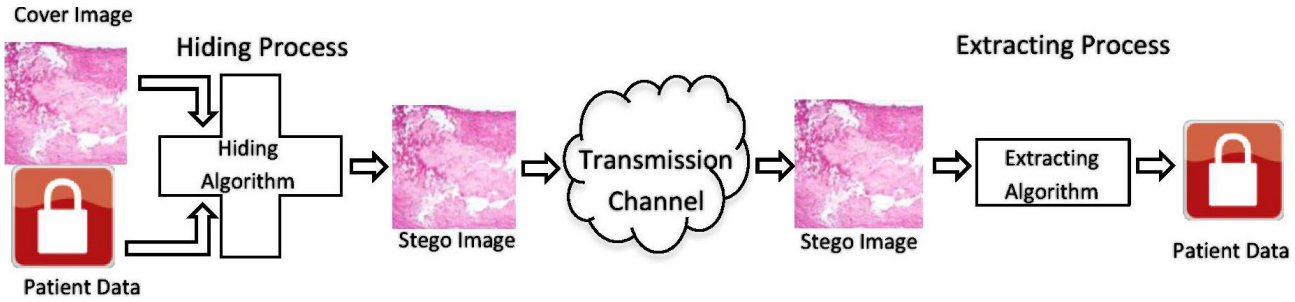


Figure 1. Data hiding processes.

The flow diagram for the algorithm of the data hiding method developed in this study is shown in Figure 2.

The data hiding algorithm consists of the data preparation, calculation of the similarity ratio, and data hiding stages. The processes, which are explained below, consist of 7 steps:

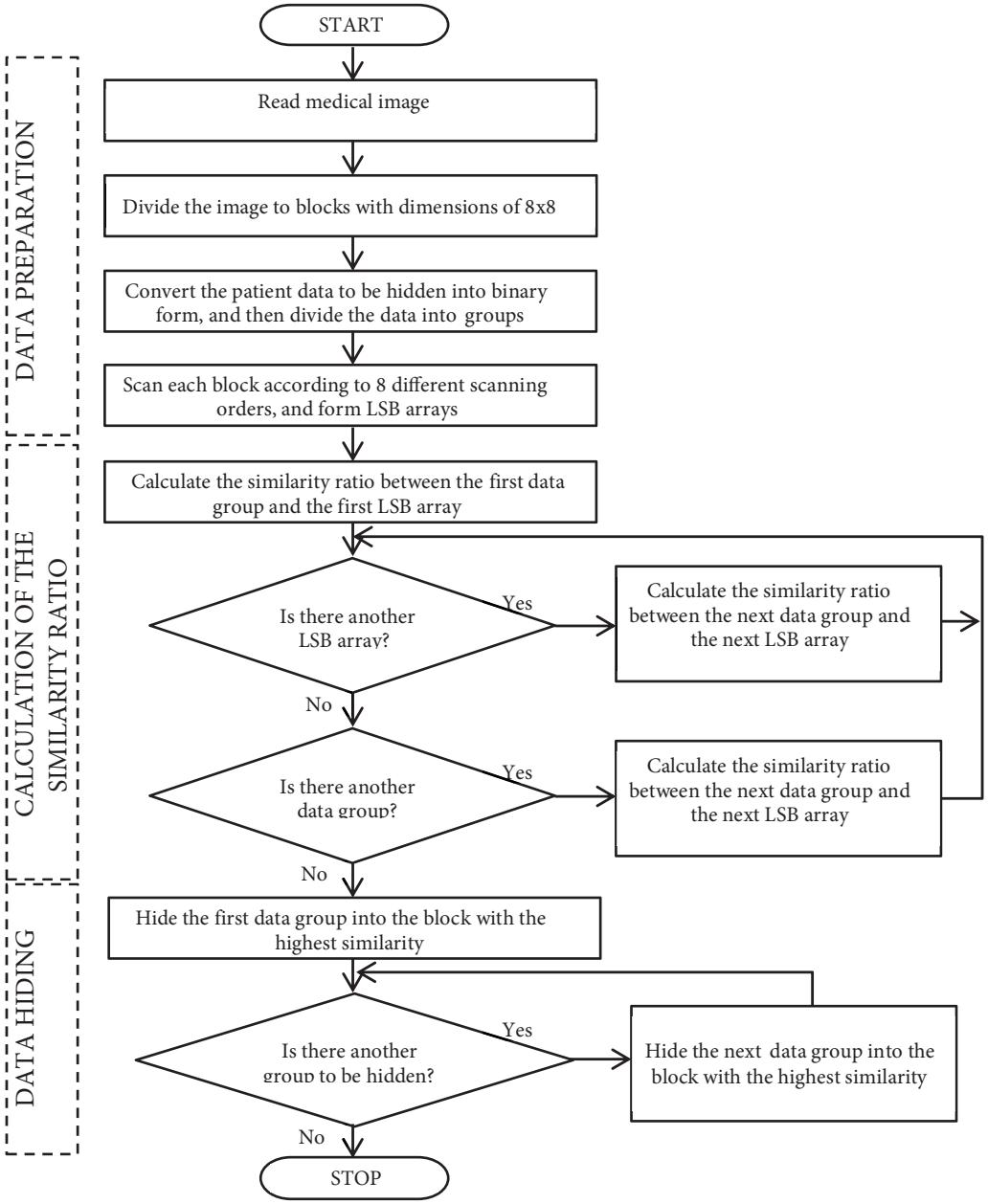
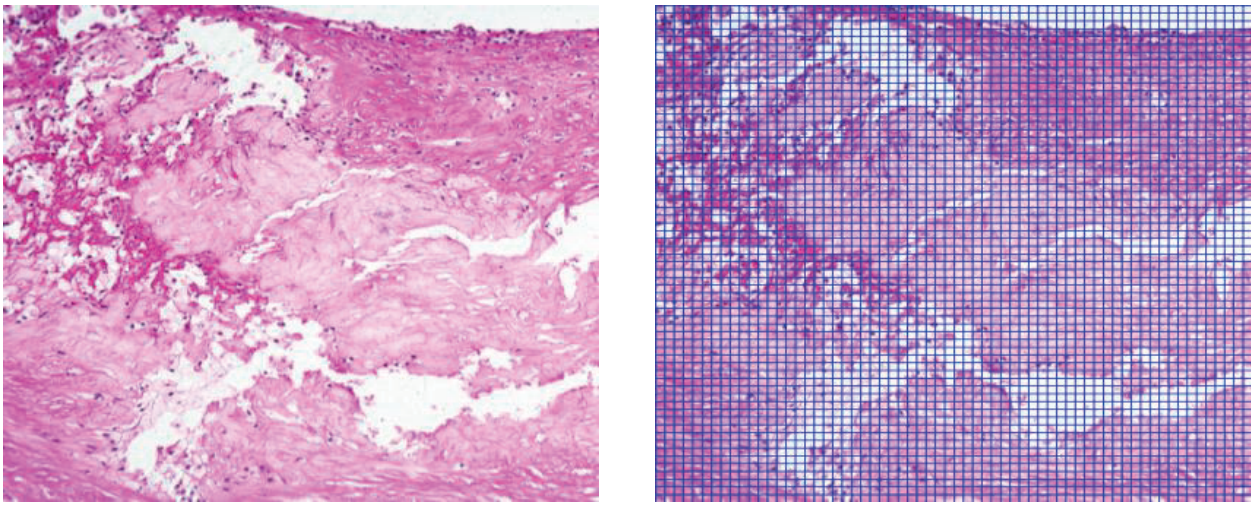


Figure 2. Flow diagram of the proposed method.

1. First, read a medical cover image with dimensions of 512 × 512.

2. Separate the medical cover image into different subblocks (subimages), each with a dimension of 8 × 8 pixels. Thus, 4096 blocks will be obtained, with each block consisting of 8 × 8 = 64 pixels (Figure 3).



(a) (b)

Figure 3. a) The medical cover image with dimensions of 512 × 512. b) Illustration of the medical cover image divided into blocks with dimensions of 8 × 8.

3. The data to be hidden are converted to binary form (1,0) and then separated into 64-bit data groups to form one-dimensional arrays.

4. To identify the most suitable pixel in which the data can be hidden, each block is scanned with 8 scanning orders, as shown in Figure 4. The first two of the scanning orders are the commonly used raster scanning order and zigzag scanning order. The others are the new scanning orders designed within the context of this study. After the 8 scanning orders are applied to each block, different LSB arrays are obtained in the form of 64-bit arrays. For 4096 blocks, 32,768 LSB arrays are formed. The aim of this study is to increase the number of scanning orders, to increase the likelihood of identifying blocks similar to the data groups to be hidden, and to thereby perform the minimum amount of change on the blocks within the medical cover image.

5. The one-dimensional data arrays formed in Step 3 and the 32,768 LSB arrays formed in Step 4 are compared element by element. Based on the comparison, with the number of similar elements in the arrays the similarity ratio is determined. Matched array pairs with high similarity ratios have fewer bit changes as a result of the data hiding process; this will reduce the level of distortion in the medical cover image.

6. The identified similarity ratio, the order number of the data groups, the block number of the LSB arrays, and the number of the scanning order are used to form the similarity table.

7. For each data group, the information of the line with the highest similarity ratio in the similarity table is selected and used. Data group, block number, and number of scanning order info are the payloads of the present study. For hiding payload, the data group matched according to this information will then be hidden according to the scanning order compatible with the block in the medical cover image. This process is repeated until the last data group by ensuring that there is one data group hidden in each block.

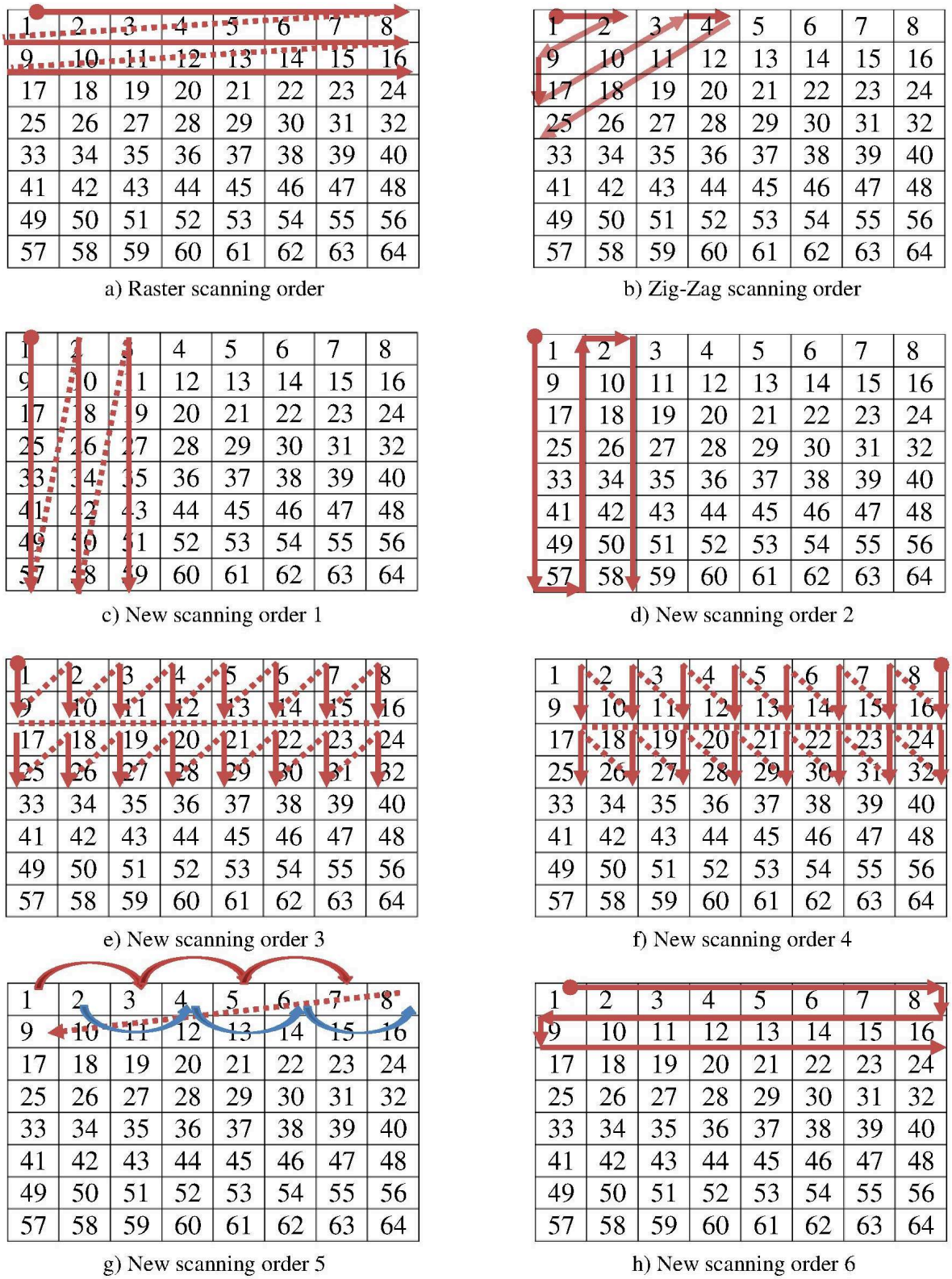


Figure 4. The scanning orders followed during data hiding in blocks: a) raster scan order, b) zig-zag scan order, c–h) new scan orders 1–6.

4. Performance evaluation of the proposed block matching data hiding method

The block matching data hiding method developed within the context of this study was analyzed based on the number of bits subject to change in the cover image, the image quality of the stego image, and the stego image's steganalysis attack versus its performance. During the analysis, test were performed by having data formed randomly at 1 KB, 2 KB, 4 KB, 8 KB, 16 KB, 24 KB, and 32 KB hidden into 24-bit medical images with dimensions of 512 × 512, and also into versions of these images that have been converted to 8-bit grayscale. In addition 24-bit RGB standard test images (Lena, Tiffany, House, Pepper, Baboon, Jet, and Lake) with sizes of 512 × 512 and their 8-bit grayscale versions were used.

4.1. Number of bits subject to change in the cover image

The proposed method was compared with the commonly used LSBR method in order to assess both methods' performance with respect to the number of bits changed. Table 2 shows the average change that occurred in the bits of the image's pixels after data hiding was performed on 24-bit medical images. The developed method could hide 1 KB (8192 bits) of data by changing 2272 bit values by 0.036, while the LSBR method could hide the same amount of data by changing 4110 bit values by 0.065. In other words, compared to the commonly used LSBR method, the proposed method is able to hide data by performing changes with 45% less bit values. Thus, the new method caused 45% less distortion in the medical image in comparison to the LSB method.

Table 2. Average changes and effects in the bits of 24-bit RGB medical images' pixels.

Total number of bits in medical image	Hidden data		Developed method		LSBR		Ratio of bit changes between the developed method and LSBR	Scanning orders	
	Amount	Number of bits	Number of bits changed on the medical image	Ratio of bits changed on the medical image	Number of bits changed on the medical image	Ratio of bits changed on the medical image		Number of 1–2 scanning orders	Number of 3–8 scanning orders
6,291,456	1 KB	8192	2272	0.036	4110	0.065	–45%	33	95
6,291,456	2 KB	16,384	4514	0.071	8148	0.129	–45%	55	201
6,291,456	4 KB	32,768	9073	0.144	16,199	0.257	–44%	118	394
6,291,456	8 KB	65,536	18,268	0.290	32,699	0.519	–45%	276	748
6,291,456	16 KB	131,072	36,912	0.586	65,322	1.038	–44%	517	1531
6,291,456	24 KB	196,608	55,656	0.884	98,755	1.569	–44%	783	2289
6,291,456	32 KB	262,144	75,407	1.198	131,231	2.085	–43%	1054	3042

This increase in performance is associated with the use of 6 new scanning orders, which are developed to determine the most suitable block matching for the data groups to be hidden. This indicator directly affects the other performance analyses, as well. In the tests, we observed that the new scanning orders (3–8) were used 3 times more frequently than the common scanning orders (1–2).

As a result of the data hiding process described in Figure 5, matched blocks with the highest similarity are obtained. The data were hidden into blocks where the fewest changes occur.

Figure 6 shows the cover images before and after data hiding is performed with the proposed method.

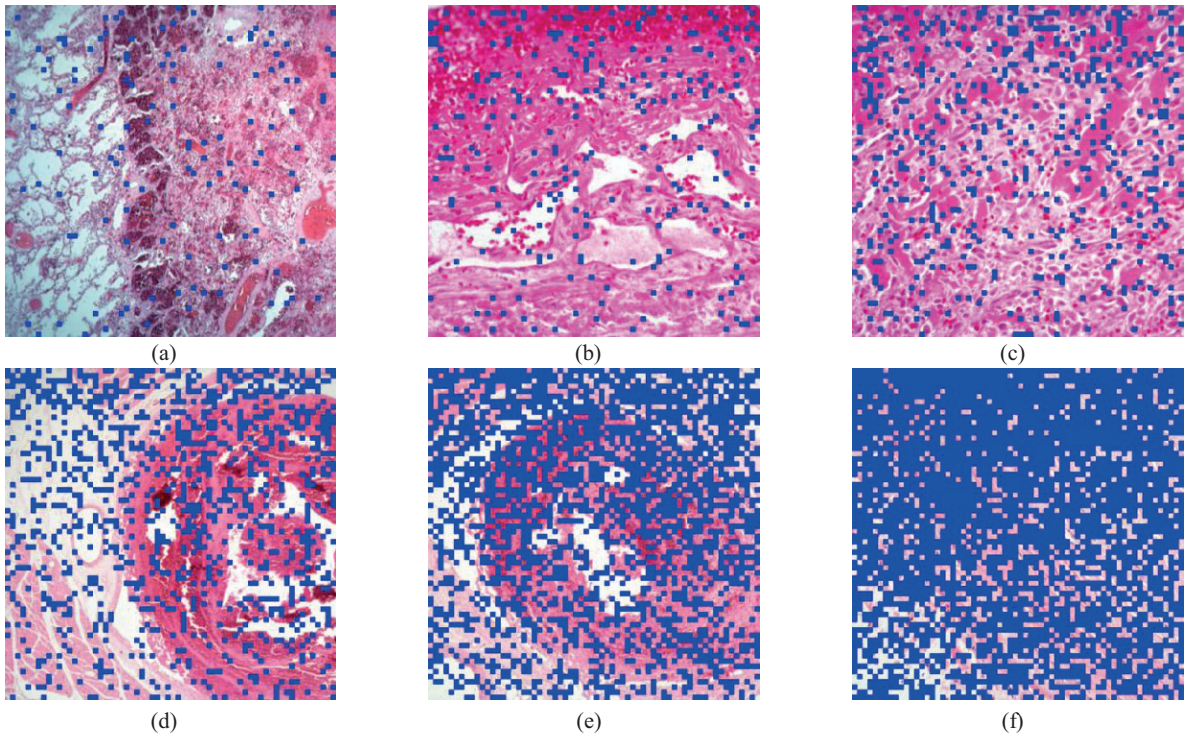


Figure 5. Illustration of the blocks in which the data are hidden: a) 1 KB, b) 2 KB, c) 4 KB, d) 8 KB, e)16 KB, f) 24 KB.

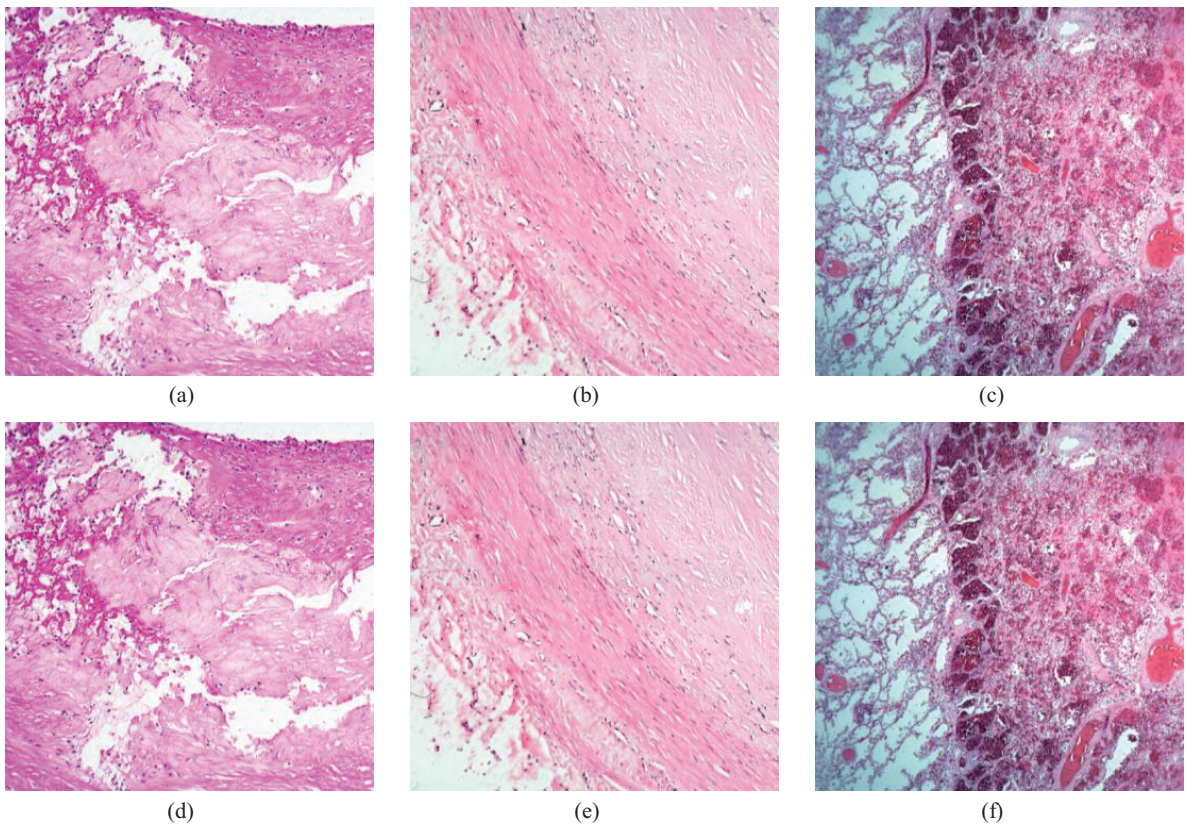


Figure 6. Reference test images (a, b, c) and versions of the same images with 32 KB of hidden data (d, e, f).

4.2. Image quality performance of the stego image

For analyzing the image quality of the stego image, the peak signal-to-noise ratio (PSNR) and the structural similarity index measure (SSIM) values, which are also commonly used in the literature, are employed. Furthermore, CQM color image quality measure was also used.

PSNR is a commonly used metric for determining the similarity between two images. At first, for the determination of the PSNR value, the mean squared error (MSE) is calculated [21]. Eq. (1) is used for the calculation of the MSE value.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|O(i,j) - C(i,j)\|^2 \tag{1}$$

Here O represents the initial or original image, while C represents the image with the hidden data, and the m and n values represent the row and column information.

After calculating the MSE value, the next step consists of calculating the PSNR value by using Eq. (2) [21]. The MAX value in the equation represents the highest value of the pixel.

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \tag{2}$$

Figure 7 shows the PSNR values of the cover images obtained after data hiding with the proposed method and the LSBR method. After all of the tests are performed, it is seen that the proposed algorithm provides the highest PSNR values. This result indicates that the proposed method provides images that are closer to the original one in comparison with LSBR. Despite the increasing ratio of hidden data, the proposed method continued to provide good results.

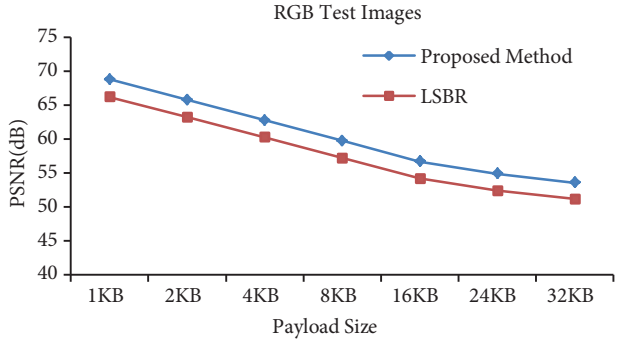


Figure 7. PSNR values of medical covered images.

The SSIM is another metric used for measuring the level of distortion in visual quality between the original image and the processed image [22]. The mean SSIM (MSSIM) is an image quality value with a minimum value of 0 and a maximum value of 1. Within the range of values between 0 and 1, the value of 1 represents the best quality [21]. The MSSIM is calculated from the SSIM using Eq. (3) [23]:

$$MSSIM(X,Y) = \frac{1}{M} \sum_{j=1}^{M} SSIM\,(x_j, y_j)\,, \tag{3}$$

where X and Y represent the original and the processed image, respectively; the M value represents the number of local windows used for determining the SSIM value; and x_j and y_j represent the j image content in M

number of local windows [23]. The MSSIM is calculated as the average of the SSIM values for M number of windows.

Table 3 shows the MSSIM values obtained after 32 KB of data were hidden into a color cover image by using the proposed method. The results indicate that the proposed method provides very high perceptual invisibility.

Table 3. MSSIM and CQM values of the medical test images.

	Medical test images							
	1	2	3	4	5	6	7	8
MSSIM dB	0.999994	0.999991	0.999993	0.999977	0.999979	0.999986	0.999977	0.999988
CQM dB	77.6759	91.8711	97.7494	80.9558	99.8928	91.4529	99.8891	92.3598

CQM was proposed by Yalman and Ertürk [24]. CQM is a color image quality measure based on reversible luminance and chrominance (YUV) color transformation and PSNR. The CQM value is calculated by using Eq. (4) [24]:

$$CQM = (PSNR_Y \times R_W) + \left(\frac{PSNR_U + PSNR_V}{2}\right) \times C_W, \tag{4}$$

where PSNR_Y, PSNR_U, and PSNR_V represent the PSNR values of the Y, U, and V channels. R_W is the weight on the human perception of the cones and C_W is the weight on the human perception of the rods [24]. Table 3 shows the CQM values obtained after 32 KB of data were hidden in a color cover image by using the proposed method.

The closest method to the proposed method was performed by Liu et al. [3]. In that study, Liu et al. developed a secure steganography method for medical images. When testing their method, they also converted all color images to grayscale images. As the proposed method is applied to the grayscale medical images, the PSNR values are obtained and tabulated in Table 4. It is observed that the proposed method provides better results (nearly 1%–6%) than that of Liu et al. [3] and LSBR. Furthermore, as the proposed method is tested on images of Lena, Tiffany, House, Pepper, Baboon, Jet, and Lake, the PSNR value for 32 KB is 53.52–53.55 dB, while it is 51.12–51.15 dB for the LSBR method.

Table 4. Comparison of the proposed method's PSNR (dB) values (512 × 512 × 8).

Payload size	Proposed algorithm	Liu et al. [3]	LSBR
50%	56.65 dB	54.9621 dB	50.04 dB
100%	53.55 dB	52.8776 dB	51.14 dB

Table 5 shows the performances of the proposed method as well as the other 7 methods [7,25–30], which have been developed in recent years. Several images, sizes, and payloads units of the available literature have been used. The proposed method has shown better performance as it is employed with approximately similar image, size, and payload units.

Table 5. The comparison results according to PSNR values between the proposed method and different methods in the literature. In all methods grayscale cover images were used. Size of the cover image of the proposed method is 512 × 512.

	Different methods		Proposed method	
	Payload	PSNR (dB)	Payload	PSNR (dB)
Lou et al. [25]	90%	50.5139	100%	53.55
Akar et al. [7]	32 KB	51.16	32 KB	53.54
Kaan et al. [26]	0.5 bpp	54.30	0.5 bpp	56.65
Sarreshedari et al. [27]	0.5 bpp	52.9064	0.5 bpp	56.65
Al-Dmour et al. [28]	25%	57.99	25%	59.68
Sajasi et al. [29]	131,072 bits	54.33	131,072 bits	56.32
Li et al. [30]	10,000 bits	63.88	16,384 bits	65.69

4.3. Steganalysis performance of the stego image

Steganalysis is the process used for identifying hidden data within stego images [31]. There are a variety of different steganalysis tools that can be used for identifying the data hidden through data hiding algorithms. Stegdetect is one of the tools used to detect the presence of hidden data within digital images [32]. The results of steganalysis of stego images are shown in Table 6. In these results, "-" indicates the nondetection of hidden data within the stego object, while "+" indicates the detection of hidden data. As shown in Table 6, steganalysis could not detect 1 KB, 2 KB, 4 KB, 8 KB, 16 KB, and 24 KB of data hidden within the 512 × 512 medical image. However, when 32 KB of data were hidden with the proposed method, the hidden data could be detected in the stego image by steganalysis.

Table 6. Stegdetect steganalysis results of the proposed method.

Amount of hidden data	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB
Result	-	-	-	-	-	+

5. Conclusion

One of the goals of data hiding methods is to perform the minimum digital changes on the cover image and to thereby maintain the image quality as high as possible. In this context, the proposed method is a new data hiding method based on block matching and LSB. The novelty of the proposed is that the method selects and uses the most suitable one of eight scanning orders, rather than using only one scanning order. The results of the proposed method show that the newly designed scanning orders have been selected three times more frequently than the commonly used scanning orders, which validates the efficiency of data hiding. Moreover, the proposed method requires 45% fewer bit changes for data hiding than the LSBR-based data hiding method.

For analyzing the image quality of the stego images obtained using the proposed method, the PSNR was measured. It is observed that the proposed method provides better results (nearly 1%–6%) than the others. Furthermore, as the cover images and stego images have been examined according to the MSSIM and CQM image quality metrics, it is found that the proposed method provides very high perceptual invisibility.

The proposed data hiding method has been examined by the Stegdetect tool. The results have verified the robustness of the stego images with 1 KB, 2 KB, 4 KB, 8 KB, 16 KB, and 24 KB data payload sizes against detection attacks. Only data detection has occurred in the medical stego image with 32 KB data payload size.

References

[1] Guo K, Zhang S. A semantic medical multimedia retrieval approach using ontology information hiding. Comput Math Method M 2013; 2013: 407917.

[2] Ahmed M, Ahamad M, Jaiswal T. Augmenting security and accountability within the eHealth Exchange. IBM J Res Dev 2014; 58: 8:1-8:11.

[3] Liu J, Tang G, Sun Y. A secure steganography for privacy protection in healthcare system. J Med Syst 2013; 37: 1-10.

[4] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding: a survey. P IEEE 1999; 87: 1062-1078.

[5] Raul RC, Claudia FU, Trinidad-BIas GDJ. Data hiding scheme for medical images. In: 17th International Conference on Electronics, Communications and Computers; 26–28 February 2007; Cholula, Mexico. New York, NY, USA: IEEE. pp. 32-32.

[6] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal Process 2010; 90: 727-752.

[7] Akar F, Yalman Y, Varol HS. Data hiding in digital images using a partial optimization technique based on the classical LSB method. Turk J Elec Eng & Comp Sci 2013; 21: 2037-2047.

[8] Chen SK, Wang RZ. High-payload image hiding scheme using k-way block matching. In: 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 15–17 October 2010; Darmstadt, Germany. New York, NY, USA: IEEE. pp. 70-73.

[9] Wang RZ, Chen YS. High-payload image steganography using two-way block matching. IEEE Signal Proc Let 2006; 13: 161-164.

[10] Kermani ZZ, Jamzad M. A robust steganography algorithm based on texture similarity using Gabor filter. In: Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology; 21 December 2005; Athens, Greece. New York, NY, USA: IEEE. pp. 578-582.

[11] Luo W, Huang F, Huang J. Edge adaptive image steganography based on LSB matching revisited. IEEE T Inf Foren Sec 2010; 5: 201-214.

[12] Zhou XQ, Huang HK, Lou SL. Authenticity and integrity of digital mammography images. IEEE T Med Imaging 2001; 20: 784-791.

[13] Luo X, Cheng Q, Tan J. A lossless data embedding scheme for medical images in application of e-diagnosis. In: Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society; 17–21 September 2003. New York, NY, USA: IEEE: pp. 852-855.

[14] Srinivasan Y, Nutter B, Mitra S, Phillips B, Ferris D. Secure transmission of medical records using high capacity steganography. In: 17th IEEE Symposium on Computer-Based Medical Systems; 24–25 June 2004. New York, NY, USA: IEEE. pp. 122-127.

[15] Taghipour H, Taghipour J, Esmaili HA. Embedding of pathology reports in pathology images. Annual Research & Review in Biology 2014; 4: 2228-2241.

[16] Iranpour M, Farokhian F. Minimal distortion steganography using well-defined functions. In: 10th International Conference on High Capacity Optical Networks and Enabling Technologies; 11–13 December 2013. New York, NY, USA: IEEE. pp. 21-24.

[17] Tang M, Hu J, Fan M, Song W. A steganalysis by adjacency pixel bits structure. Comput Electr Eng 2013; 39: 488-496.

[18] Zhu Z, Zhang T, Wan B. A special detector for the edge adaptive image steganography based on LSB matching revisited. In: 10th IEEE International Conference on Control and Automation; 12–14 June 2013; Hangzhou, China. New York, NY, USA: IEEE. pp. 1363-1366.

[19] Vashishtha LK, Dutta T, Sur A. Least significant bit matching steganalysis based on feature analysis. In: 2013 National Conference on Communications; 15–17 February 2013; New Delhi, India. New York, NY, USA: IEEE. pp. 1-5.

[20] Nayak DK, Bhagvati C. A threshold-LSB based information hiding scheme using digital images. In: 4th International Conference on Computer and Communication Technology; 20–22 September 2013; Allahabad, India. New York, NY, USA: IEEE. pp. 269-272.

[21] Coşkun İ, Akar F, Çetin Ö. A new digital image steganography algorithm based on visible wavelength. Turk J Elec Eng & Comp Sci 2013; 21: 548-564.

[22] Rad RM, Wong K, Guo JM. A unified data embedding and scrambling method. IEEE T Image Process 2014; 23: 1463-1475.

[23] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE T Image Process 2004; 13: 600-612.

[24] Yalman Y, Ertürk İ. A new color image quality measure based on YUV transformation and PSNR for human vision system. Turk J Elec Eng & Comp Sci 2013; 21: 603-612.

[25] Lou DC, Hu CH. LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis. Inform Sciences 2012; 188: 346-358.

[26] Kanan HR, Nazeri B. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst Appl 2014; 41: 6123-6130.

[27] Sarreshedari S, Akhaee MA. One-third probability embedding: a new ± 1 histogram compensating image least significant bit steganography. IET Image Process 2014; 8: 78-89.

[28] Al-Dmour H, Al-Ani A. A steganography embedding method based on edge identification and XOR coding. Expert Syst Appl 2016; 46: 293-306.

[29] Sajasi S, Moghamad AME. An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method. Appl Soft Comput 2015; 30: 375-389.

[30] Li X, Zhang W, Gui X, Yang B. Efficient reversible data hiding based on multiple histograms modification. IEEE T Inf Foren Sec 2015; 10: 2016-2027.

[31] Ker AD, Pevny T. The steganographer is the outlier: realistic large-scale steganalysis. IEEE T Inf Foren Sec 2014; 9: 1424-1435.

[32] Khalind OS, Hernandez-Castro JC, Aziz B. A study on the false positive rate of Stegdetect. Digit Invest 2013; 9: 235-245.