Displays 41 (2016) 1–8

Contents lists available at ScienceDirect

Displays

journal homepage: www.elsevier.com/locate/displa

A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images

Türker Tuncer [a,*], Engin Avci [b]

[a] Department of Digital Forensic Engineering, Technology Faculty, Firat University, Elazig, Turkey
[b] Department of Software Engineering, Technology Faculty, Firat University, Elazig, Turkey

ARTICLE INFO

Article history:
Received 19 March 2015
Received in revised form 7 October 2015
Accepted 13 October 2015
Available online 22 October 2015

Keywords:
Data hiding
Probabilistic DNA-XOR secret sharing
Image steganography
Watermarking
Information security

ABSTRACT

In this paper, a new data hiding method is proposed based on secret sharing scheme with the DNA exclusive or (DNA-XOR) operator for color images. The DNA-XOR secret sharing scheme uses a DNA-XOR truth table. Each input value of truth table is evaluated and according to that evaluation, highest PSNR (Peak Signal-to-Noise Ratio) value is selected for secret sharing. These selected values are embedded into cover image. Cover image is used as an encryption key in the proposed secret sharing process. In this study, the hidden data are divided into three secret shares and embedded into the red, green and blue channels of a cover image respectively. In here, the DNA-XOR operator has been firstly used as secret sharing operator in data hiding literature. Our proposed data hiding method was compared with previous methods. The comparison of these methods shows that our proposed method gives the most successful result.

1. Introduction

Nowadays, in parallel to improvements in technology, information security techniques have been developed. Data hiding is one of these techniques [1]. Data hiding is a technique, which involves hidden data that is known only by the sender and the receiver. In this technique, hidden data is obtained only by a person who has stego key. Data can be hidden in seemingly innocent multimedia files (image, audio signal, video, etc.) with the condition not to exceed size of the cover data during transmission. If the receiver side knows the stego key, he/she can obtain the hidden data by operating embedding function in reverse [2,3].

Multimedia data (image, audio, video) has more size than plain text in computer environment. Therefore, images, audios, videos are very convenient to use as cover objects [4]. In order to prevent hidden data in cover object from third parties, embedding algorithm must satisfy some certain criteria. Not to be perceived by the human visual system is one of these criteria. At the same time to hide the data with embedding algorithm, data must be able to embed with appropriate capacity into cover data. In order to evaluate the success of data hiding algorithms the following points should be considered [5].

- The optimum way of embedding mechanism.
- The optimum way of extraction of embedded data.
- The optimum amount of data: Capacity.
- Robustness to attacks.
- Transparency.
- Reliability.

To ensure these criteria, various data hiding algorithms have been developed [6–9]. The data hiding algorithms usually examined in 3 groups, according to the domain of data hiding algorithm.

Spatial Domain: In this domain, Least Significant Bit (LSB) [10,11] method is widely used. The pixel values of the cover object are used for data hiding process.
Frequency Domain: Data hiding process is used by obtaining coefficients from conversions of Discrete Cosine Transform (DCT) [12,13], Discrete Wavelet Transform (DWT) [14] and Discrete Fourier Transform (DFT) [15].
Compression Domain: In this domain, Vector Quantization (VQ) method is used for data hiding [16].

Also, histogram shifting mechanism is used for data hiding and steganographic schemes [17].

Frequency domain is used for increasing durability [18,19]. Many studies are available for improving the data hiding algorithm by obtaining the coefficients of cover data in Frequency domain.

Recently, some researchers started to use the complementary rule of the DNA to ensure information security and data hiding.

* Corresponding author.
E-mail addresses: turkertuncer@firat.edu.tr (T. Tuncer), enginavci@firat.edu.tr (E. Avci).

http://dx.doi.org/10.1016/j.displa.2015.10.005
0141-9382/

Huang et al. [20] suggested a DNA-based data hiding technique with low modification. This method solved many problems of previous DNA based data hiding algorithms. Liu et al. [21] proposed a new data hiding method based on deoxyribonucleic acid (DNA) coding, which used a word document as a cover object. In their method, the plain message became a cipher sequence after being encoded to a DNA sequence and being encrypted by the addition operation. The cipher sequence was attached to a random DNA primer sequence and circularly shifted for finite times, then the whole sequence was embedded into a Word document through substituting each character's color. The plaintext was extracted according to the keys, and the key space was large enough to resist brute force attacks. Zhang et al. [22] presented a new image fusion encryption algorithm based on image fusion and DNA sequence operation and hyper-chaotic system. Two DNA sequence matrices were obtained by encoding the original image and the key image. Secondly, the chaotic sequences generated by Chen's hyper-chaotic maps were used to scramble the locations of elements in the DNA sequence matrices which were generated from the original images. Finally using a XOR operator matrix was embedded. Lee [18] addressed issues regarding watermarking DNA coding sequences in the frequency domain. Chang et al. [23] proposed two data hiding schemes. In their schemes, secret messages were hidden in a DNA sequence. The host DNA sequence could be reconstructed after the reverse operation. This property ensured the security of the secret data and preserved the functionality of the original DNA. Risca [24] presented an implementation of steganography using DNA molecules. This study showed that the steganographically hidden message was retrieved only by using the two secret primers, meaning that the only applicable cryptanalytic approach was a brute-force search for the two primer sequences. At the same time in the literature, there are many studies supported by the secret sharing method to improve the success of data hiding application. Liu et al. [25] presented a robust readable H.264/AVC data hiding algorithm without intra-frame distortion drift. They first divided the original embedded data into several groups by using the secret sharing technique. Then they used the BCH syndrome code (BCH code) technique to encode each grouping of data. Finally, they embed the encoded data into the paired-coefficients of the 4×4 Discrete Cosine Transform (DCT) block of the selected frames which meet our conditions to avert the distortion drift. Lee and Tsai [26] presented a new data hiding method via PNG images based on Shamir's (k,n)-threshold secret sharing scheme. Wei et al. [27] proposed new information hiding scheme for color images based on the concept of visual cryptography and the XOR operation. Three different schemes with noise-like, meaningful and binary shares were presented. Their proposed model could be extended from 256 colors to 65,536 or true color images by expanding the block size from 3×3 to 4×4 or 5×5. In this paper, for improving the success rate of data hiding techniques an efficient method is proposed based on DNA-XOR secret sharing. In Section 2, we briefly describe the basic concept of DNA encoding and decoding for color image. Section 3 contains a detailed explanation of the proposed algorithm. In Section 4, we describe the results of proposed method in the context of PSNR, bit error rate (BER), pixel distortion (PD) and structural similarity (SSIM). Finally, we present our conclusion in Section 5.

2. DNA sequence

A DNA sequence consists of DNA molecules. DNA sequence is essential information for living, surviving and reproducing [28]. A DNA sequence is formed by four nucleic acids which are A (adenine), C (cytosine), G (guanine), T (thymine). A, T and G, C are complementary like 0 and 1 in binary. DNA sequencing is important for biological research [29].

Table 1
Eight kinds of schemes encoding map rule of DNA sequence.

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

Table 2
XOR operator for DNA sequences.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

2.1. DNA encoding and decoding for color image

In a DNA sequence, there are four different nucleic acids which are, A (adenine), T (thymine), C (cytosine), and G (guanine). Therefore, Watson–Crick complement rule is valid in here [30]. Table 1 shows encoding and decoding map by using DNA sequence in this paper.

The Watson–Crick complementarity rule gives fundamental information which can be transferred to daily life. Firstly, a color image is separated to RGB channels. Secondly, these RGB channels are converted to binary coding. Then, each pixel of RGB channels can be expressed as a DNA sequence. For example, the binary code of the pixel value of blue channel image is [11001001]. DNA sequence of this binary code is [TACG] according to definition of first column in Table 1 [31].

A x-bit color image, which has $m \times n$ size and can be defined as a three-dimensional (Red, Green and Blue) binary matrix, which is denoted as $A = [s_{i,j,k}]_{m \times n \times k}$. Where $s_{i,j,k} \in \{0,1\}$, and $(i,j,k) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\} \times \{0,1,\ldots,k-1\}$.

The XOR operation for R, G, B channels of the image are defined in Eq. (1):

$$\mathrm{R} \oplus \mathrm{G} \oplus \mathrm{B} = \left[s_{i,j,1} \oplus s_{i,j,2} \oplus s_{i,j,3}\right]_{m \times n \times k} \tag{1}$$

Binary code of the represented value of pixel $A_{i,j}$ at point (i,j) can be converted to a decimal number by using Eq. (2) [32].

$$A_{i,j} = a_{i,j,k-1}2^{k-1} + a_{i,j,k-2}2^{k-2} + \ldots + a_{i,j,1}2^{1} + a_{i,j,0}2^{0} \tag{2}$$

In DNA computing, biological and mathematical operators based on DNA sequences are used. XOR operator has been widely utilized in DNA computing. Table 2 shows the DNA-XOR rules [30].

Fig. 1 illustrates the deterministic finite automata of XOR operator for DNA sequences using a state diagram [33].

3. The proposed method

In this study, the secret data is divided into three secret shares with using DNA-XOR operator. Each part of hidden data is embedded into each channel of color image. Cover images size is $512 \times 512 \times 3$. Size of each secret share is 512×1024 (524,288) bits which is embedded into the cover image.

3.1. Probabilistic DNA-XOR secret sharing scheme

Secret sharing based methods have been introduced to protect the reliability of the encryption key or data. Shamir's (k,n) threshold method is the best known of these methods. Purpose of secret sharing is to provide the key reliability. In the literature, many

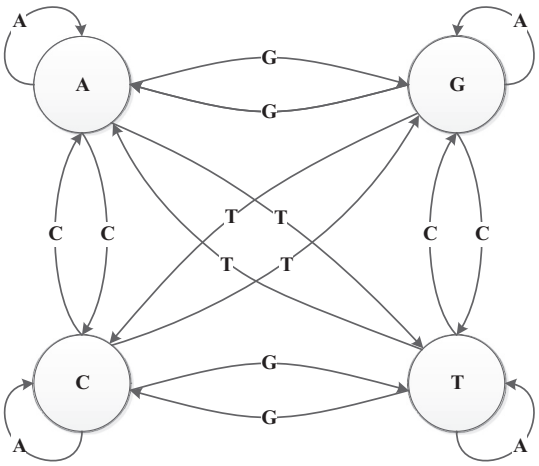


Fig. 1. The automata of XOR operator for DNA sequences.

Let A be the binary matrix representing the secret image.

Distribution phase.
The dealer:

- generates $n-1$ random matrices $B_1, \ldots, B_{n-1}$;
- distributes the n shares $A_1, \ldots, A_n$ where $A_1 = B_1$, $A_i = B_{i-1} \oplus B_i$, and $A_n = B_{n-1} \oplus A$.

Reconstruction phase. The n participants reconstruct the secret image as follows:

- superimpose their shares executing binary XOR operation to obtain $A' = A_1 \oplus A_2 \cdots \oplus A_n$.

Fig. 2. Boolean (XOR) based probabilistic secret sharing scheme (n,n) [34].

secret sharing based data hiding algorithms are proposed. To achieve an optimum data hiding scheme, a new probabilistic secret sharing method is proposed [34,35].

In this paper, we presented a new probabilistic secret sharing scheme based on DNA-XOR operator. This scheme is similar to Wang's scheme. Construction of Wang's scheme is given in Fig. 2 [34].

The probabilistic DNA-XOR secret sharing scheme is applied on a test image. The test image is divided into secret shares by using the probabilistic DNA-XOR secret sharing scheme and results are given in Fig. 3.

3.2. Embedding procedure of the proposed data hiding algorithm

The flow diagram of embedding procedure is given in Fig. 4.

Step 1: Transform cover image into R, G and B channels.
Step 2: Convert secret data to binary form.
Step 3: Convert binary data to the DNA form of the hidden data.
Step 4: Apply the DNA XOR secret sharing operator to the hidden data.
Step 5: Calculate all MSE (Mean Square Error) of all probabilities.
Step 6: Select the best triple combination which has minimum MSE as secret shares and embed secret shares into the cover image.

For example, combinations of A are shown in Table 3. These combinations are obtained from DNA-XOR truth table.

The embedding function is modulo and its equation is given in Eq. (3). For example, if secret data is A and the best combination is TTG. Thus, T $\oplus$ T $\oplus$ G $=$ *A*. T, T, G are embedded into channels of the color images, respectively.

$$bits_{i,j,k} = \lfloor A_{i,j,k} \ mod \ 2^2 \rfloor \quad i = 1,2,\ldots,m, \ j = 1,2,\ldots,m, \ k = 1,2,3 \tag{3}$$

An example of the proposed data embedding is shown in Fig. 5.

As shown in Fig. 5, G, G and A is the secret shares which have minimum MSE values. These values are embedded into cover channels of the cover image respectively. As a result of the embedding process, there has not been any changing in the pixel values. For this reason, a higher PSNR value is obtained. If multiple values have the minimum MSE, one of these values is randomly selected. In Fig. 5, there has been no change in the pixel values because of minimum value of MSE is zero.

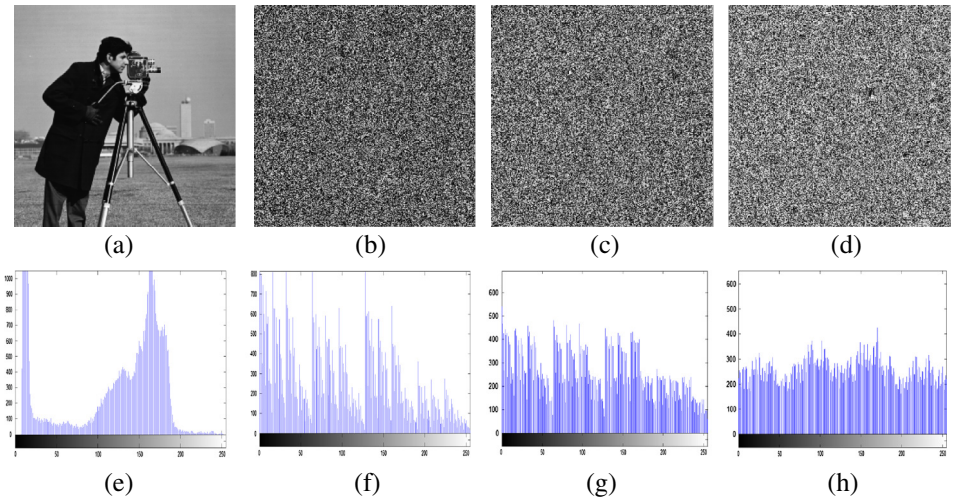


Fig. 3. Probabilistic DNA-XOR secret sharing scheme. (a) Original image. (b) First secret share of cameraman. (c) Second secret share of cameraman. (d) Third secret share of cameraman. (e) Histogram of original image. (f) Histogram of first secret share of cameraman. (g) Histogram of second secret share of cameraman. (h) Histogram of third secret share of cameraman.

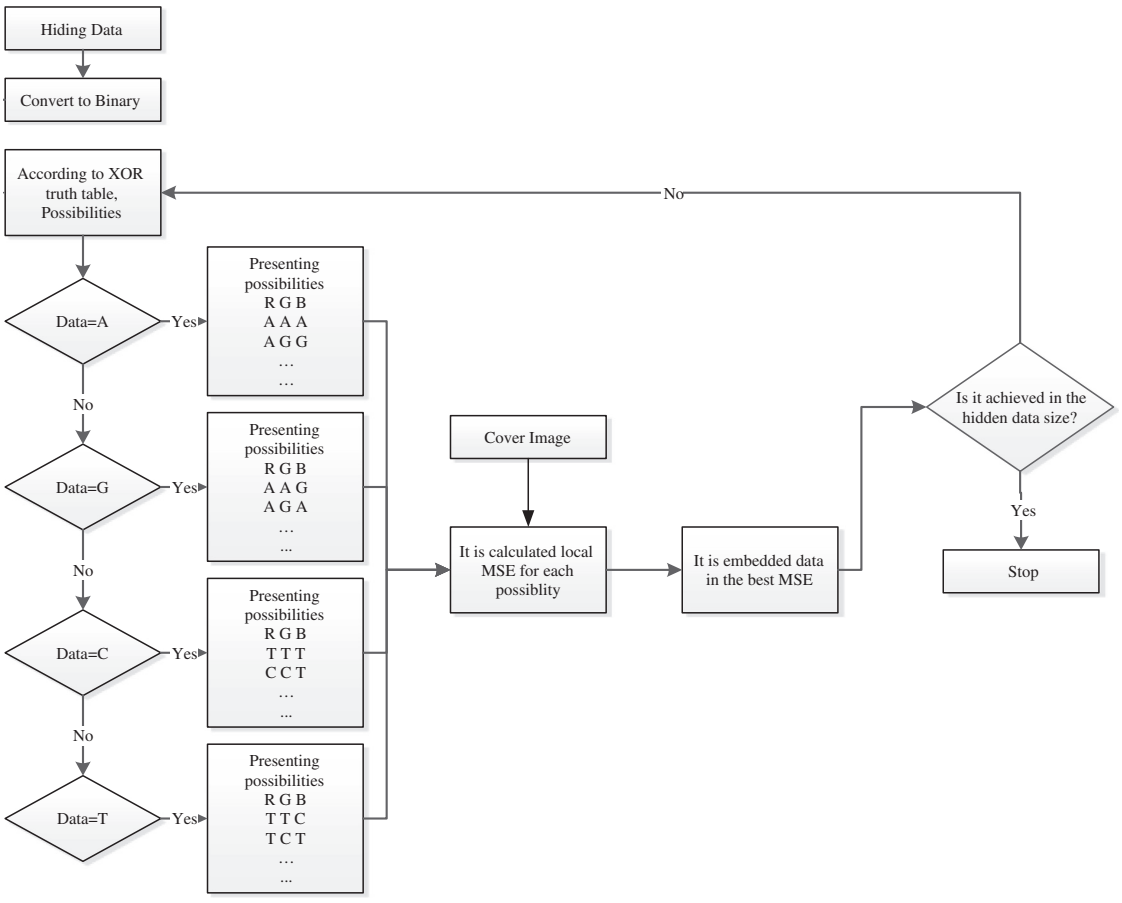


Fig. 4. The flow diagram of embedding procedure with DNA-XOR operation.

Table 3
Triple DNA-XOR truth table for adenine.

1	0 A	0	0 A	0	0 A	0	9	1 C	0	0 A	0	1 T	1
2	0 A	0	0 G	1	0 G	1	10	1 C	0	0 G	1	1 C	0
3	0 A	0	1 C	0	1 C	0	11	1 C	0	1 C	0	0 G	1
4	0 A	0	1 T	1	1 T	1	12	1 C	0	1 T	1	0 A	0
5	0 G	1	0 A	0	0 G	1	13	1 T	1	0 A	0	1 C	0
6	0 G	1	0 G	1	0 A	0	14	1 T	1	0 G	1	1 T	1
7	0 G	1	1 C	0	1 T	1	15	1 T	1	1 C	0	0 A	0
8	0 G	1	1 T	1	1 C	0	16	1 T	1	1 T	1	0 G	1

3.3. Extraction procedure of the proposed data hiding algorithm

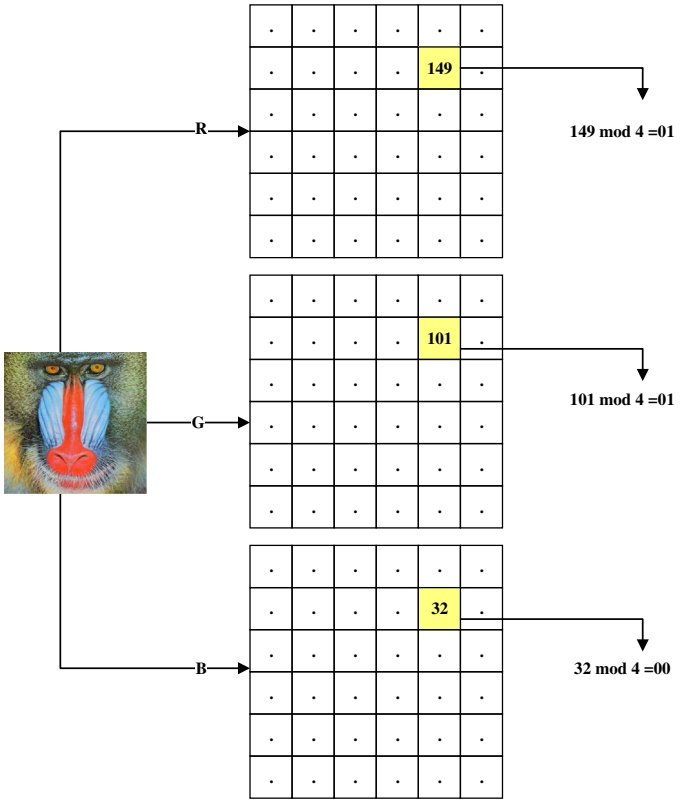
The extraction algorithm is given below.

Step 1: Obtain RGB channels of the stego image.
Step 2: Find embedded indices using the stego-key.
Step 3: Obtain embedded location for each channel and apply invert bit with modulo 2^2.
Step 4: Convert extracted bits to DNA-code.
Step 5: Apply DNA-XOR operation to DNA code of each channel as shown in Eq. (1).
Step 6: Extract DNA sequence and convert to appropriate form.

4. Experimental results

In this section, performance of the proposed method is evaluated according to 6 performance metrics and these metrics are given below.

The optimum way of embedding mechanism: LSB or modulo function based methods are used as data hiding functions in the proposed method. These data hiding functions are widely used and these functions have the optimum way of embedding mechanism. In this study, we used the optimum data hiding functions and the DNA-XOR secret sharing scheme together.
The optimum way of extraction of embedded data: Firstly, image is divided into R, G and B layers and then modulo function is used with the DNA-XOR operator to extract the secret data. This method is the optimum way for data extraction.
The optimum amount of data: The proposed method allows data hiding with high payload capacity. In this paper, 2 bpp (bit per pixel) payload capacity is used.
Robustness to attacks: Data hiding algorithms based on secret sharing are used for image authentication. For this reason, the proposed algorithm is fragile.



	Probabilities	Local MSE		Probabilities	Local MSE
1	0 0 0 0 0 0 / A A A	0,67	9	1 0 0 0 1 1 / C A T	3,67
2	0 0 0 1 0 1 / A G G	0,67	10	1 0 0 1 1 0 / C G C	1,67
3	0 0 1 0 1 0 / A C C	2	11	1 0 1 0 0 1 / C C G	1
4	0 0 1 1 1 1 / A T T	4,67	12	1 0 1 1 0 0 / C T A	1,67
5	0 1 0 0 0 1 / G A G	0,67	13	1 1 0 0 1 0 / T A C	3
6	0 1 0 1 0 0 / G G A	0	14	1 1 0 1 1 1 / T G T	4,33
7	0 1 1 0 1 1 / G C T	3,33	15	1 1 1 0 0 0 / T C A	1,67
8	0 1 1 1 1 0 / G T C	2,67	16	1 1 1 1 0 1 / T T G	3

The best value for selected pixel of Adenine

Fig. 5. Data hiding A (00) with the proposed method.

Transparency: The DNA-XOR secret sharing scheme uses the DNA-XOR truth table and multiple values are obtained for one secret share. The proposed algorithm selects the optimum value for embedding. For this reason, transparency of the proposed algorithm is very high.

Reliability: The DNA-XOR secret sharing scheme divides the secret data into secret shares and this scheme is uses image as an encryption key. The DNA-XOR operator uses 8 different encoding techniques. Reliability of the secret data is provided by using the DNA-XOR secret sharing scheme in the proposed data hiding algorithm.

Experimental results are offered for comparing the performance of the proposed method with the previously selected methods. In the experiments, eight general test images with the size of $512 \times 512 \times 3$ are used as cover images, namely, "Lena", "Peppers", "Tiffany", "Goldhill", "Baboon", "Jet", "Barbara" and "House". These test images are shown in Fig. 6.

The operating system is Windows 8.1 and the proposed algorithm is programmed in Matlab 2013a. The payload capacity is 2 bpp. To compare visual quality, MSE, PSNR, BER, PD and SSIM are defined in Eqs. (4)–(8) respectively [35–43].

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i,j}\left(\mathrm{CI}_{i,j} - \mathrm{SI}_{i,j}\right)^2 \tag{4}$$

$$\mathrm{PSNR} = 10\log\frac{Max(\mathrm{CI}_{i,j}^2)}{\mathrm{MSE}} \tag{5}$$

$$\mathrm{PD} = \frac{\text{total number of bits changes}}{\text{total number of bits embedded}} \tag{6}$$

$$\mathrm{BER} = \frac{\text{total number of bit changes}}{\text{total number of bits}} \tag{7}$$

$$\mathrm{SSIM}(\mathrm{CI},\mathrm{SI}) = \frac{(2\mu_{\mathrm{CI}}\mu_{\mathrm{SI}} + c_1)(2\sigma_{\mathrm{CISI}} + c_2)}{(\mu_{\mathrm{CI}}^2 + \mu_{\mathrm{SI}}^2 + c_1)(\sigma_{\mathrm{CI}}^2 + \sigma_{\mathrm{SI}}^2 + c_2)} \tag{8}$$

CI is cover image, SI is stego-image, μ_{CI} is the average of cover image, μ_{SI} is the average of stego image, σ_{CI}^2 is the variance of cover image, σ_{SI}^2 is the variance of stego image, σ_{CI} is the covariance of cover image and stego image, c_1;$(k_1L)^2$, c_2;$(k_2L)^2$, L: dynamic range of pixel values, $k1$; 0.01 and $k2$; 0.03 by default in SSIM equation [38–42].

The results of the proposed method are given in Table 4 for test images.

The PSNR/Capacity change rate of the proposed algorithm is shown in Fig. 7.

The proposed method is compared with Lin and Tsai's method [40], Yang et al.'s method [41], Chang et al.'s method [42], Wu et al.'s method [43] and Kanan and Nazeri's method [44]. The obtained results for the test images are shown in Table 5.

Yuan has also proposed to secret sharing methods for natural images based on multi-cover adaptive steganography in 2014 [10]. Our proposed method is also compared to Yuan's method and obtained results as shown in Table 6.

5. Conclusion

In this paper, a new high quality, secure, reversible, simple and applicable data hiding algorithm is proposed. The proposed data hiding algorithm provides an optimum way of embedding mechanism, an optimum way of extraction of embedded data, high payload capacity, high visual quality and reliability of the secret data for data hiding. In the proposed scheme, the hidden data is embedded by modulo function and the DNA-XOR operator is used for secret sharing. As we know there has been no proposed secret sharing scheme in the literature, which uses DNA-XOR operator.

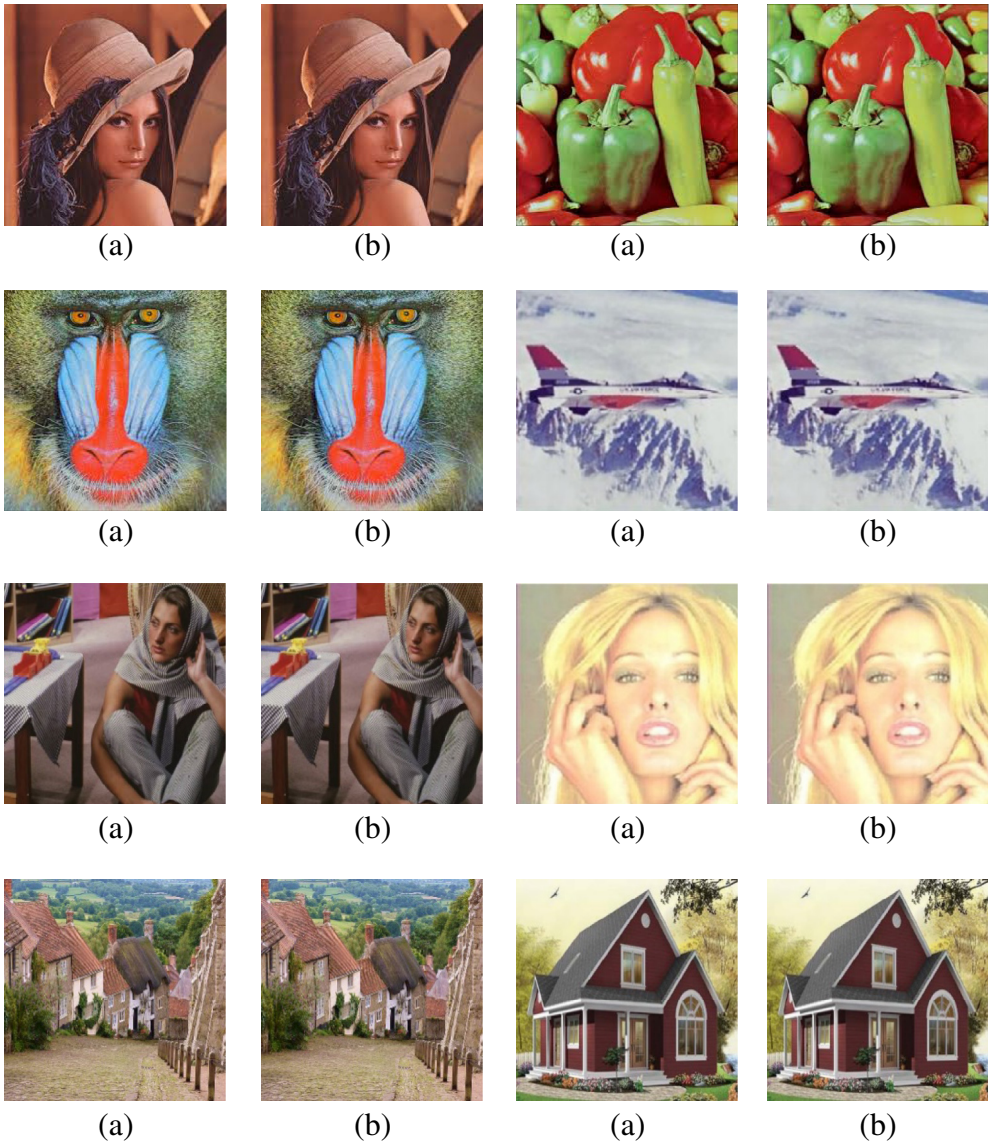


Fig. 6. Test images used in the experiment. (a) Original image. (b) Stego-image.

Table 4
Experimental results of the proposed method for different test images.

Image	PSNR	BER	PD	SSIM
Lena	52.24	0.0153	0.0110	0.9996
Peppers	52.16	0.0154	0.0112	0.9996
Baboon	52.18	0.0155	0.0112	0.9996
Jet	52.18	0.0153	0.0110	0.9996
Barbara	52.31	0.0153	0.0111	0.9996
Tiffany	52.11	0.0154	0.0110	0.9996
Goldhill	52.27	0.0152	0.0110	0.9996
House	52.11	0.0155	0.0110	0.9996

The proposed method is compared to previously popular approaches from the viewpoint of data hiding effectiveness and visual quality parameters. Although the capacity is 2 bpp (bit per pixel), the average PSNR of our proposed method is greater than 52 dB ($52 > 48.13$ dB ($10\log_{10}255^2/1$)). Therefore, this result clarified that the best PSNR values are obtained by using our proposed methods.

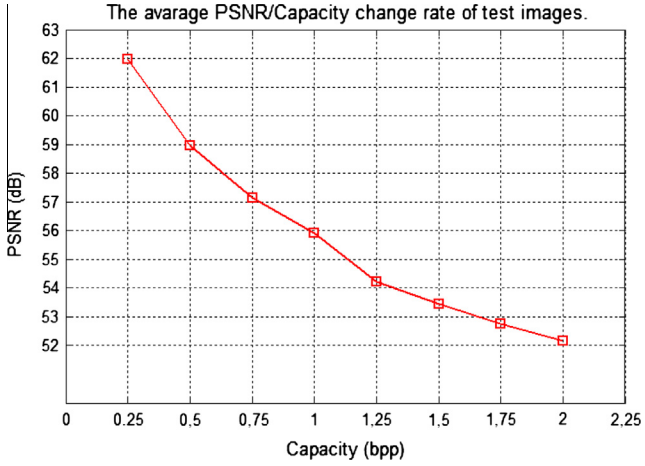


Fig. 7. The average PSNR/Capacity change rate of test images.

Table 5
The comparison of performances of the proposed method with previous methods.

Stego image	PSNR (dB)					
	Lin and Tsai's method [40]	Yang et al.'s method [41]	Chang et al.'s method [42]	Wu et al.'s method [43]	Kanan and Nazeri's method [44]	The proposed method
Lena	39.20	41.60	40.37	43.54	45.12	52.24
Jet	39.25	41.66	40.73	43.53	45.18	52.18
Peppers	39.17	41.56	39.30	43.56	45.13	52.12
Baboon	39.18	41.55	39.94	43.54	45.12	52.18
Average	39.2	41.59	40.08	43.54	45.14	52.18

Table 6
Comparative performance of proposed method and Yuan's method for 0.5 bpp payload capacity.

Image	Yuan's method [10]		The proposed method	
	PSNR	MSSIM	PSNR	MSSIM
Lena	55.46	0.9993	59.03	0.9999
Jet	55.70	0.9995	58.87	0.9999
Peppers	55.64	0.9993	58.97	0.9999
Bridge	51.46	0.9991	58.89	0.9999
Average	54.56	0.9993	58.69	0.9999

Acknowledgements

We thank reviewers for their positive comments, Fatih Özyurt, Mustafa Eriş and Hüseyin Yüce Kürüm for careful reading of the paper.

References

[1] S.A. Parah, J.A. Sheikh, A.M. Hafiz, G.M. Bhat, Data hiding in scrambled images: a new double layer security data hiding technique, Comput. Electr. Eng. 40 (2014) 70–82.
[2] O. Cetin, A.T. Ozcerit, A new steganography algorithm based on color histograms for data embedding into raw video streams, Comput. Secur. 28 (7) (2009) 670–682.
[3] G. Kipper, Investigator's Guide to Steganography, Auerbach Publications A CRC Press Company, Boca Raton, London, New York, Washington, DC, 2004. pp. 20–26.
[4] S.Y. Shen, L.-H. Huang, A data hiding scheme using pixel value differencing and improving exploiting modification directions, Comput. Secur. 48 (2015) 131–141.
[5] H.T. Sencar, M. Ramkumar, A.N. Akansu, Data Hiding Fundamentals and Applications, Content Security in Digital Media, Elsevier Academic Press, 2004.
[6] I.J. Cox, J. Killian, T. Leighton, T. Shamoon, A secure robust watermark for multimedia, IEEE Trans. Image Process. 6 (12) (1997) 1673–1687.
[7] A. Phadikar, S.P. Maity, On protection of compressed image in fading channel using data hiding, Comput. Electr. Eng. 38 (5) (2012) 1278–1298.
[8] R.G. van Schyndel, A.Z. Tirkel, C.F. Osborne, A digital watermark, in: Proceedings of IEEE International Conference of Image Processing, vol. 2, Austin, Texas, November 1994, pp. 86–90.
[9] A. Piva, M. Barni, F. Barolini, V. Cappellini, DCT-based watermark recovering without resorting to the uncorrupted original image, in: Proceedings of IEEE International Conference of Image Processing, vol. 1, Santa Barbara, California, October 1997, pp. 520–523.
[10] H.D. Yuan, Secret sharing with multi-cover adaptive steganography, Inform. Sci. 254 (2014) 197–212.
[11] A. Miller, Least Significant Bit Embeddings: Implementation and Detection, May 2012.
[12] H. Noda, M. Niimi, E. Kawaguchi, High-performance JPEG steganography using quantization index modulation in DCT domain, Pattern Recogn. Lett. 27 (5) (2006) 455–461.
[13] P.C. Chang, K.L. Chung, J.J. Chen, C.H. Lin, T.J. Lin, A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames, J. Vis. Commun. Image Represent. 25 (2) (2014) 239–253.
[14] S.H. Lee, DWT based coding DNA watermarking for DNA copyright protection, Inform. Sci. 273 (2014) 263–286.
[15] B. Chen, G. Coatrieux, G. Chen, X. Sun, J.L. Coatrieux, H. Shu, Full 4-D quaternion discrete Fourier transform based watermarking for color images, Digit. Signal Process. 28 (2014) 106–119.
[16] C. Qin, C.-C. Chang, Y.-C. Chen, Efficient reversible data hiding for VQ-compressed images based on index mapping mechanism, Signal Process. 93 (9) (2013) 2687–2695.
[17] C. Qin, C.C. Chang, Y.H. Huang, L.T. Liao, An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism, IEEE Trans. Circ. Syst. Video Technol. 23 (7) (2013) 1109–1118.
[18] S.H. Lee, DWT based coding DNA watermarking for DNA copyright protection, Inform. Sci. 273 (2014) 263–286.
[19] F. Peng, X. Li, B. Yang, Adaptive reversible data hiding scheme based on integer transform, Signal Process. 92 (1) (2012) 54–62.
[20] Y.H. Huang, C.C. Chang, C.Y. Yu, A DNA-based data hiding technique with low modification rates, Multimed. Tools Appl. 70 (3) (2014) 1439–1451.
[21] H. Liu, D. Lin, A. Kadir, A novel data hiding method based on deoxyribonucleic acid coding, Comput. Electr. Eng. 39 (4) (2013) 1164–1173.
[22] Q. Zhang, L. Guo, X. Wei, A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 124 (2013) 3596–3600.
[23] C.C. Chang, T.C. Lu, Y.F. Chang, C.T. Lee, Reversible data hiding schemes for deoxyribonucleic acid (DNA) medium, Int. J. Innov. Comput. Inform. Control 3 (5) (2007).
[24] V.I. Risca, DNA-based steganography, Cryptologia 25 (2001) 37–49.
[25] Y. Liu, M. Hu, X. Ma, H. Zhao, A new robust data hiding method for H.264/AVC without intra-frame distortion drift, Neurocomputing 151 (3) (2015) 1076–1085.
[26] C.W. Lee, W.H. Tsai, A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, Signal Process. 93 (7) (2013) 2010–2025.
[27] S.C. Wei, Y.C. Hou, Y.C. Lu, A technique for sharing a digital image, Comput. Stand. Inter. 40 (2015) 53–61.
[28] X. Wei, L. Guoa, Q. Zhanga, J. Zhanga, S. Lianb, A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, J. Syst. Software 85 (2012) 290–299.
[29] L. Liu, Q. Zhang, X. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map, Comput. Electr. Eng. 38 (2012) 1240–1248.
[30] R. Enayatifar, A.H. Abdullah, I.F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Opt. Lasers Eng. 56 (2014) 83–93.
[31] O.D. King, P. Gaborit, Binary templates for comma-free DNA codes, Discrete Appl. Math. 155 (2007) 831–839.
[32] T. Xie, Y. Liu, J. Tang, Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 125 (2014) 7166–7169.
[33] J.H. Reif, S. Sahu, Autonomous programmable DNA nanorobotic devices using DNAzymes, Theor. Comput. Sci. 410 (2009) 1428–1439.
[34] D. Wang, X. Li, F. Yi, D. Wang, X. Li, F. Yi, Probabilistic (n,n) visual secret sharing scheme for grayscale images, in: Information Security and Cryptology, Lecture Notes in Computer Science, vol. 4990, Springer-Verlag, Berlin, 2007, pp. 192–200.
[35] A. Tanchenko, Visual-PSNR measure of image quality, J. Vis. Commun. Image R. 25 (2014) 874–878.
[36] C.C. Wang, Y.F. Chang, C.C. Chang, J.K. Jan, C.C. Lin, A high capacity data hiding scheme for binary images based on block patterns, J. Syst. Software 93 (2014) 152–162.
[37] M.M. A-Eldayem, A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine, Egypt. Inform. J. 14 (2013) 1–13.
[38] M. Zengzhen, Image quality assessment in multiband DCT domain based on SSIM, Optik 125 (2014) 6470–6473.
[39] L.University, UCID Image Dataset. <http://homepages.lboro.ac.uk/~cogs/datasets/ucid/ucid.html> (18.11.14).
[40] C.-C. Lin, W.-H. Tsai, Secret image sharing with steganography and authentication, J. Syst. Software 73 (3) (2004) 405–414.
[41] C.-N. Yang, T.-S. Chen, K.H. Yu, C.-C. Wang, Improvements of image sharing with steganography and authentication, J. Syst. Software 80 (7) (2007) 1070–1076.
[42] C.-C. Chang, Y.-P. Hsieh, C.-H. Lin, Sharing secrets in stego images with authentication, Pattern Recogn. 41 (10) (2008) 3130–3137.
[43] C.-C. Wu, S.-J. Kao, M.-S. Hwang, A high quality image sharing with steganography and adaptive authentication scheme, J. Syst. Software 84 (12) (2011) 2196–2207.
[44] H.R. Kanan, B. Nazeri, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Exp. Syst. Appl. 41 (2014) 6123–6130.

Türker Tuncer was born in Tunceli, Turkey in 1986. He received the B.S. degree from the Department of Electronics and Computer Education, Technical Education Faculty, the Firat University in 2009 and M.S. degree in Telecommunication Science from the Firat University in 2011. He is a Ph.D. student in the Department of Software Engineering at the Firat University. He works as a research assistant in the Department of Digital Forensic Engineering, the Firat University. His research interests include data hiding, visual cryptography, secret sharing, and image processing.

Engin Avci was born in Elazig, Turkey in 1978. He received the B.S. degree from the Department of Electronics and Computer Education, Technical Education Faculty, the Firat University in 2000, M.S. degree in Computer Science from the Firat University in 2002 and Ph.D. degree in Electrical and Electronical Engineering from the Firat University in 2005. He works as a professor doctor in the Department of Software Engineering, the Firat University. His research interests include pattern recognition techniques, communication, signal processing, radar target recognition, intelligent systems, data hiding and information security.