I. J. Computer Network and Information Security, **2018, 1, 1-9**
Published Online January 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.01.01

A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map

Sengul Dogan
Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: sdogan@firat.edu.tr

Received: 05 July 2017; Accepted: 11 November 2017; Published: 08 January 2018

***Abstract*—**In this paper, a new data hiding algorithm based on pixel pairs using chaotic map is proposed. Data hiding scheme is created by applying modulo function to pixel pairs. In here, pseudo random number generator (PRNG) is obtained from chaotic maps. The PRNG is very important for this algorithm since the data hiding coefficients are chosen by PRNG. For example, if the coefficient is 0, subtraction operator is used between pixel pairs. If coefficient is 1, summary operator is used for selected pixel pairs. The proposed algorithm is evaluated by embedding different sized secret data into different test images. This method is compared with the determined studies in the literature and the obtained results is evaluated. In this study, special rules are also defined to pixels which have boundary values for resolve overflow/underflow problem. Minimal changes are performed to reach the desired value of the pixel values. According to the results obtained, the proposed algorithm has high visual quality, good running time, secure and high payload capacity.

***Index Terms*—**Chaotic maps, data hiding, information security, pixel pairs, pixel selection.

I. INTRODUCTION

Rapidly developing and changing technology has led internet-connected electronic devices to be cheaper and commonly used [1]. While this situation facilitating access to information, it has become an important issue of ensuring information security. Information security is become important topic in digital world [2]. The main purpose of information security is to prevent the third-parties from capturing the digital data during storing and transmitting processes [3,4]. There are various methods in information security applications such as data hiding, cryptography etc. In this applications, data can be encrypted or its existence can be hidden by using a cover object. Cover object can be multimedia such as text, audio, video and image [5-7]. Multimedia data is frequently used in data hiding applications because of high payload capacity [8]. If small changes in cover object can't detected by human perception system, the application is considered as successful. Criteria such as bit error rate (BER) [9], peak signal-to-noise ratio (PSNR) [10, 11], structural similarity (SSIM) [12] are used to utilized success of data hiding application. A lot of data hiding methods are evaluated with this criteria [13-17]. There are two kind of data hiding application. The first data hiding application is spatial domain. Spatial domain applications changes pixel values, frequency domain applications use frequency coefficient for data hiding applications. Discrete Wavelet Transform, Discrete Fourier Transform and Discrete Cosine Transform are used to obtain frequency coefficients and these coefficients are modified for data hiding in frequency domain. If robustness against corruptive situation is important, frequency domain applications are preferred. For this reason, performing data hiding according to purpose of application increases performance of data hiding algorithm.

The paper is organized in 6 sections. The literature review about related works is given in section 2. In section 3, chaotic maps are introduced. the proposed method is described in section 4. In section 5, the obtained results are illustrated. Finally, conclusion of this paper is presented in section 6.

II. RELATED WORKS

There are a lot of studies about data hiding in literature. Chen [18] presented a Pixel Value Difference (*PVD*) method to safely hide data that is secure. The results demonstrated high capacity and cover object quality in comparison to other similar method. Shen and Huang [19] proposed a data hiding algorithm to increase embedding capacity based on pixel pairs. Their method demonstrated both to improve needed embedding capacity and to hold stego image quality. Qu and Kim [20] introduced a novel pixel-based pixel-value-ordering (*PVO*). Their obtained results indicated the good performance of the proposed pixel-based *PVO* method based on each predicted pixel. Wang et al [21] provided a new data hiding approach using *PVO* and dynamic pixel block partition. Their proposed scheme demonstrated a better capacity than current *PVO* based method. The method also tries to minimize distortion to the minimum. Lin and Hsueh [22] presented a reversible data hiding method used pixel pairs. This method embedded to ensure lossless a data into a cover object using pixel pairs in a three-pixel block. The average capacity of their proposed method for images measured with bpp (2.08 bit per pixel). Li et al [23] proposed a high accuracy reversible data hiding approach in test images based on *PVO* and prediction-error expansion (*PEE*) method measured by PSNR value which found about 51.14 dB. Tsai et al [24] come up with a new data hiding scheme in test images using the histogram method. This algorithm was obtained high embedding capacity and imperceptible distortion. Hong et al [25] presented a data hiding approach based on the diamond encoding (*DE*) technique. This method with the consideration of human visual system provides better quality and high embedding capacity. Yang et al [26] presented a new data hiding approach using pixel-value differencing (*PVD*) for increase the embedding capacity. Their experimental results were compared with other similar method. This method obtained better embedding capacity. Lee et al [27] proposed data hiding algorithm to increased capacity with quality recovery based on tri-way *PVD*. Their experimental results demonstrated a high resistance to dual statistics steganalysis. Peng et al [28] presented a data hiding approach based on *PVO* and *PEE*. This method obtained better embedding performance compared to similar methods. Chang et al [29] provided a hiding algorithm using a multilevel histogram-modification method using the difference of neighboring pixels. This method had better capacity and cover object quality.

III. Chaotic Maps

Random numbers are required for perform various purposes in computer systems such as encryptions algorithms, game programing etc. For example, random numbers are very important for security and performance of encryptions algorithms. Random number generators (*RNG*) are used for generate this numbers. However, if seed values of *RNG* are estimated, this random numbers can be obtained. If generated numbers of *RNG* are same in each iteration, this is an undesirable situation especially for security applications. The main purpose of *RNG* is to generate a different seed value in each iteration. To avoid this undesirable situations new methods are developed for *RNG*. Chaotic maps are used as *RNG* for solving these problems. A chaotic system can be defined as system that sensitive to initial conditions and unpredictably complex. Small changes in initial conditions of chaotic systems cause big changes in this system. In this situation, chaotic systems become unpredictable.

A chaotic system describes in below.

- It is not random. It has an arrangement in itself.
- It is sensitively depended of initial conditions.

In parallel to this purposes, there are a lot of chaotic maps such as logistic map, gauss map and tent map. The widely used chaotic map is logistic maps. Logistic map developed by Robert MAY in 1976 was constructed on changes based on feedback of biological population [10, 30]. Logistic map is defined in Equation (1).

$$x_{n+1} = \rho x_n(1 - x_n), 0 < \rho \leq 4, x_n \in (0, 1) \qquad (1)$$

According to ρ parameter system behaves chaotic or not chaotic [31, 32]. x is the initial seed and ρ is control parameter. Bifurcation diagram of logistic map is given in Fig. 1 [33].

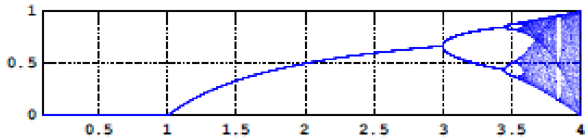


Fig.1. The Bifurcation Diagram of Logistic Map

IV. The Proposed Method

The purpose of proposed method is to increase visual quality and obtain a data hiding algorithm which has a short running time. This data hiding algorithm has high payload capacity. Modulo *4^b* operator is used for determine payload capacity. *b* expresses payload capacity. For example, if *1* bpp payload capacity is used, process is performed according to modulo *4*, if *2* bpp payload capacity is used, process is performed according to modulo *16*. One of the biggest advantages of this method according to *xLSBs* (x Least Significant Bits Insertion Method) is less distortion rate on cover image by using high data hiding capacity. Privacy of secret data is also ensured by using chaotic maps and the proposed method has better running time than *xLSBs* because *xLSBs* algorithms are commonly used decimal to binary transformation on each pixel value for data hiding. This situation creates *+1* iteration in algorithm. However, the proposed method doesn't need decimal to binary transformation on each pixel value.

Data hiding steps of proposed method in this paper is given in below.

Step 1: Generate chaotic map by using seed values. The chaotic map must be same size with secret data.

$$\begin{gathered} x_{i+1} = \rho x_i(1 - x_i), \rho = [3.57, 4], \\ x_i \in (0,1), x_i \neq 0.5, i = \{1,2,3, \dots, n\} \\ x_i \begin{cases} x_i < 0.5, x_i = 0 \\ x_i \geq 0.5, x_i = 1 \end{cases} \end{gathered} \qquad (2)$$

Step 2: Encode secret data by using modulo function. For example, if *1* bpp payload capacity is used, secret data is encoded with *2* bits, if *2* bpp payload capacity is used, secret data is encoded with 4 bits.

Step 3: Select operator according to value in chaotic map. If value is *0*, select subtraction operator, otherwise select summary operator for pixel pairs.

$$x_{i,j} \begin{cases} 0, d = \left|CI_{i,2j} - CI_{i,2j+1}\right| (mod4^b) \\ 1, t = CI_{i,2j} + CI_{i,2j+1} \, (mod4^b) \end{cases} \qquad (3)$$

$$i = \{0, 1, 2, \dots\ r-1\}, j = \{0, 1, 2, \dots \tfrac{c}{2} - 1\}$$

d is difference of pixel pairs, *CI* is cover image and *t* is summary of pixel pairs.

Step 4: Equal obtained *t* and *d* values to secret data. For example, random values which are obtained from chaotic map is $(1011)_2$, secret data is $(01111000)_2$ and cover image pixel values are given in Fig. 2. Data hiding process is applied in below.

128	133	117	85
250	25	0	255

Fig.2. The Sample Image Pixels

If value of chaotic map is *0*, subtraction operator is selected, otherwise summary operator is selected for pixel pairs.

$$x_{i,j} \begin{cases} 0, d = \left|SI_{i,2j} - SI_{i,2j+1}\right| \ (mod 4^b) \\ 1, t = SI_{i,2j} + SI_{i,2j+1} \ (mod 4^b) \end{cases} \quad (4)$$
$$i = \{0, 1, 2, \dots\ r-1\}, j = \{0, 1, 2, \dots \tfrac{c}{2} - 1\}$$

128+133 (mod 4) = $(01)_2$, 128 and 133 pixel values don't change because the first two bits of secret data is $(01)_2$.

|117-85| (mod 4) = $(00)_2$, and secret data is $(11)_2$. The small one of pixel pairs is increased by *1*. The obtained final values are 117, 86.

250+25 (mod 4) = $(11)_2$, and it is sufficient to decrease one of the pixel pairs by *1* because secret data is $(10)_2$. The obtained new values are 249, 25.

255+0 (mod 4) = $(11)_2$ and secret data is $(00)_2$. Increasing one of the pixel pairs by *1* is required to equal summary value to $(00)_2$. The big pixel value is *255*, for this reason this value is not increased. The small value is increased by *1* and the obtained new values are *1*, *255*.

Secret data is embedded as $(01111000)_2$ and the obtained pixel values are shown in Fig. 3.

128	133	117	86
249	25	1	255

Fig.3. The Pixel Values of Stego Image

Data extraction steps are given in below.

Step 1: Generate chaotic maps by using seed values.
Step 2: Apply Equation (4) to pixel pairs of stego image and obtain secret data.

d is difference of pixel pairs, *b* is payload capacity, *SI* is stego image and *t* is summary of pixel pairs. For example, chaotic map is generated by using seed values to obtain data which is embedded into pixel values and 1011 is obtained by receiver from chaotic maps.

SD1=128+133 mod 4 = $(01)_2$
SD2=|117-86| mod 4 = $(11)_2$
SD3=249+25 mod 4 = $(10)_2$
SD4= 1+255 mod 4 = $(00)_2$

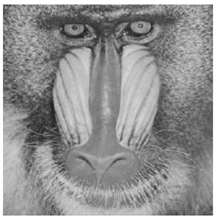
$(01111000)_2$ is obtained from stego image after steps in above.

V. Experimental Result

The proposed method is evaluated on a computer with Windows8.1 operating system. The obtained results are utilized using MATLAB 2014a. In this study, after secret data in different sizes are embedded into test images, test images [34] and Kodak image data set [35] are evaluated according to the widely used criteria in the literature These images given in Fig. 4 are *512x512* sized and gray-scale. These test images are named as Lena, F16, Baboon, Barbara, Boat, Pepper, House, Sailboat, Elaine, Tiffany, Goldhill, Toys and Zelda. PSNR [36] and Quality (Q) [37] given Equation 5-12 are used to utilized the result of proposed method.

(a)

(b)


(c)

(d)

(e)

(f) (g) (h) (i) (j)

(k) (l) (m)

Fig. 4. The test images (a) Lena, (b) F16, (c) Baboon, (d) Barbara, (e) Boat, (f) Pepper, (g) House, (h) Sailboat, (i) Elaine, (j) Tiffany, (k) Goldhill, (l) Toys, (m) Zelda

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - SI_{i,j})^2 \quad (5)$$

$$PSNR = 10\log\frac{Max(CI_{i,j}^2)}{MSE} \quad (6)$$

$$Q = \frac{4\sigma_{xy}\,\overline{x}\times\overline{y}}{(\sigma_x^2+\sigma_y^2)[\,\overline{x}^2+\overline{y}^2\,]} \quad (7)$$

$$\overline{x} = \frac{1}{m\,x\,n}\sum_{i=1}^{m}\sum_{j=1}^{n}CI_{i,j} \quad (8)$$

$$\overline{y} = \frac{1}{m\,x\,n}\sum_{i=1}^{m}\sum_{j=1}^{n}SI_{i,j} \quad (9)$$

$$\sigma_x^2 = \frac{1}{m\,x\,n-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - \bar{x})^2 \quad (10)$$

$$\sigma_x^2 = \frac{1}{m\,x\,n-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - \bar{x})^2 \quad (11)$$

$$\sigma_{xy} = \frac{1}{m\,x\,n-1}\sum_{i=1}^{m}\sum_{j}^{n}(CI_{i,j} - \bar{x})(SI_{i,j} - \bar{y}) \quad (12)$$

Here,

$CI_{i,j}$ – Cover image

$SI_{i,j}$ – Stego image

m – Weight of cover/stego image

n – Height of cover/stego image

$\overline{x},\overline{y}$ – The mean value of cover image, stego image, respectively

σ_x^2,σ_y^2 – The variance of cover image, stego image

σ_{xy} – The covariance of the values from the stego image and cover image

The proposed method is compared for *10.000* bits and *20.000* bits sized secret data by using test images and Kodak images data set. The obtained results are shown in Table 1-2.

Table 1. The obtained In Terms of PSNR (dB) the Proposed Method with the Embedding Capacity of 10,000 and 20,000 bits

Image	10,000 bits	20,000 bits	Image	10,000 bits	20,000 bits
Lena	63.0	60.0	Barbara	63.2	60.2
Baboon	63.2	60.0	Tiffany	63.1	60.1
F16	63.4	60.2	Elaine	62.9	59.9
Boat	63.2	60.0	Sailboat	63.3	60.1
Pepper	63.3	60.0	House	63.4	60.5

Table 2. The obtained of Kodak Image Data Set in Terms of PSNR (dB) for the Proposed Method with the Embedding Capacity of 10,000 and 20,000 bits

Image	10,000 bits	20,000 bits	Image	10,000 bits	20,000 bits
kodim01	64.76	61.64	kodim13	64.77	61.61
kodim02	64.91	61.76	kodim14	64.86	61.75
kodim03	64.75	61.96	kodim15	64.66	61.78
kodim04	64.96	61.83	kodim16	64.80	62.00
kodim05	64.95	61.83	kodim17	64.89	61.92
kodim06	63.54	61.35	kodim18	64.85	61.73
kodim07	64.71	61.97	kodim19	64.79	61.86
kodim08	64.82	61.66	kodim20	63.55	61.37
kodim09	64.77	61.76	kodim21	64.86	61.88
kodim10	64.84	61.83	kodim22	65.17	61.97
kodim11	64.26	61.81	kodim23	65.07	62.17
kodim12	64.91	61.94	kodim24	63.78	61.19

The proposed method is compared with Shen and Huang method [19] and obtained results is given in Table 3.

Table 3. Comparisons of Test Images In Terms of PSNR (dB) for Shen and Huang Method and the Proposed Method

Image	PSNR	Capacity	Error
Shen and Huang Method 2015			
Lena	42.46	402.485	0
Baboon	38.88	443.472	0
Barbara	40.15	425.340	0
Elaine	42.98	398.250	0
Goldhill	41.80	405.956	0
Boat	41.60	408.777	0
Sailboat	41.29	411.306	0
Toys	42.52	402.011	0
House	41.16	412.354	0
Zelda	43.43	396.553	0
Average	**41.63**	**410.650**	**0**
The proposed method			
Lena	44.2868	450.240	0
Baboon	44.2969	450.240	0
Barbara	44.3053	450.240	0
Elaine	44.3123	450.240	0
Goldhill	44.3073	450.240	0
Boat	44.3212	450.240	0
Sailboat	44.2960	450.240	0
Toys	44.2800	450.240	0
House	44.2999	450.240	0
Zelda	44.3195	450.240	0
Average	**44.3000**	**450.240**	**0**

The proposed method is also compared with other data hiding methods [38, 39, 19] based on pixel pairs in literature in terms of Quality metric and the obtained results are shown in Table 4.

Table 4. Comparisons of other Methods [38, 39, 19] and the Proposed Method for Quality

Cover Image	hang and Lu method (2006)		Lu et al. method (2014) (|B|=4)		Lu et al. method (2014) (|B|=8)		Shen and Huang method (2015)	The proposed method
	Q,(T=15)	Q,(T=42)	Q,(T=3)	Q,(T=18)	Q,(T=3)	Q,(T=18)	Q	Q
Baboon	0.9913	0.9297	0.9955	0.9807	0.9858	0.9768	0.9977	0.9996
Lena	0.9951	0.9914	0.9978	0.9943	0.9934	0.9910	0.9992	0.9997
F16	0.9948	0.9815	0.9971	0.9923	0.9914	0.9863	0.9990	0.9996
Pepper	0.9960	0.9892	0.9983	0.9963	0.9951	0.9938	0.9995	0.9995
Average	**0,9943**	**0,97295**	**0,9971**	**0,9909**	**0,9914**	**0,9869**	**0,9988**	**0,9996**

The PSNR change rates obtained from test images are given in Fig. 5 for *1* bpp payload capacity.

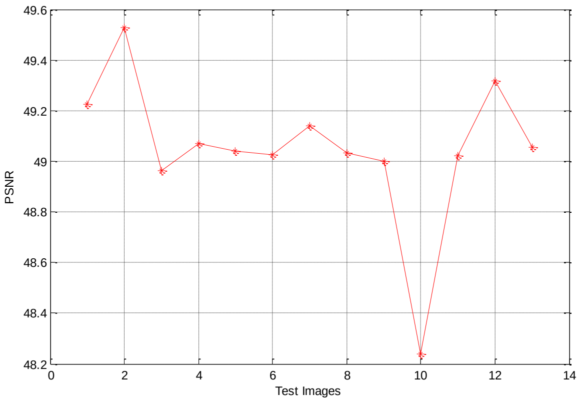


Fig.5. PSNR Values of Test Images for 1bpp Payload Capacity

The Quality change rates obtained from test images are presented in Fig. 6 for *1* bpp payload capacity.

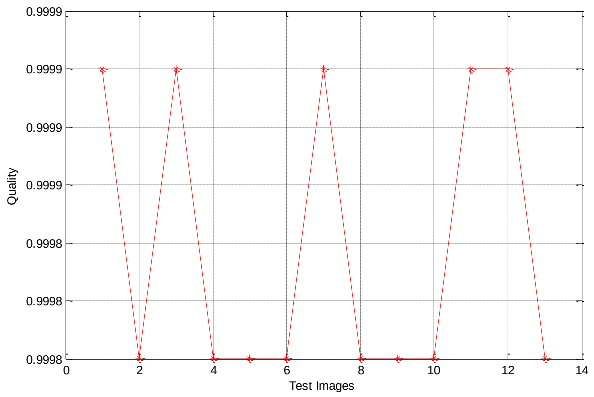


Fig.6. Q Values of Test Images for 1bpp Payload Capacity

The PSNR change rates obtained from test images are given in Fig. 7 for *2* bpp payload capacity.

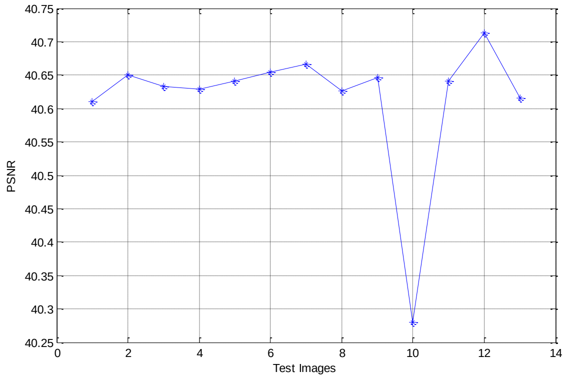


Fig. 7. PSNR Values of Test Images for 2bpp Payload Capacity

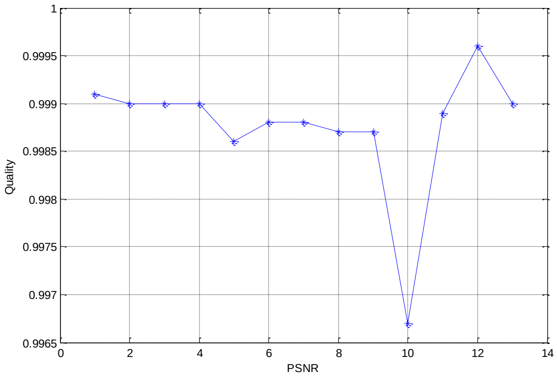
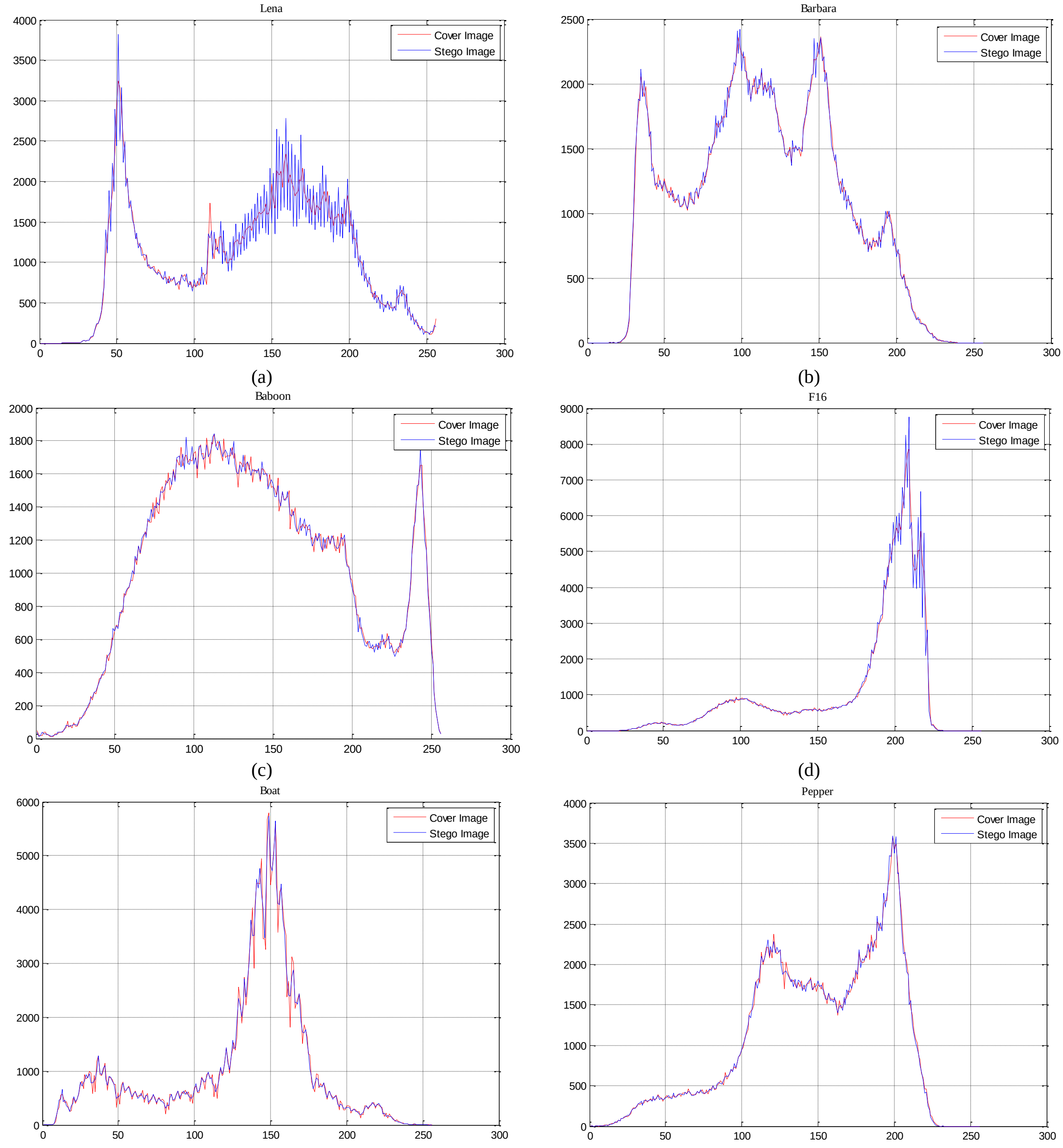


Fig. 8. Q Values of Test Images for 2bpp Payload Capacity

The Quality change rates obtained from test images are shown in Fig. 8 for *2* bpp payload capacity.

The histogram changes of selected test images are given in Fig. 9.



(a)

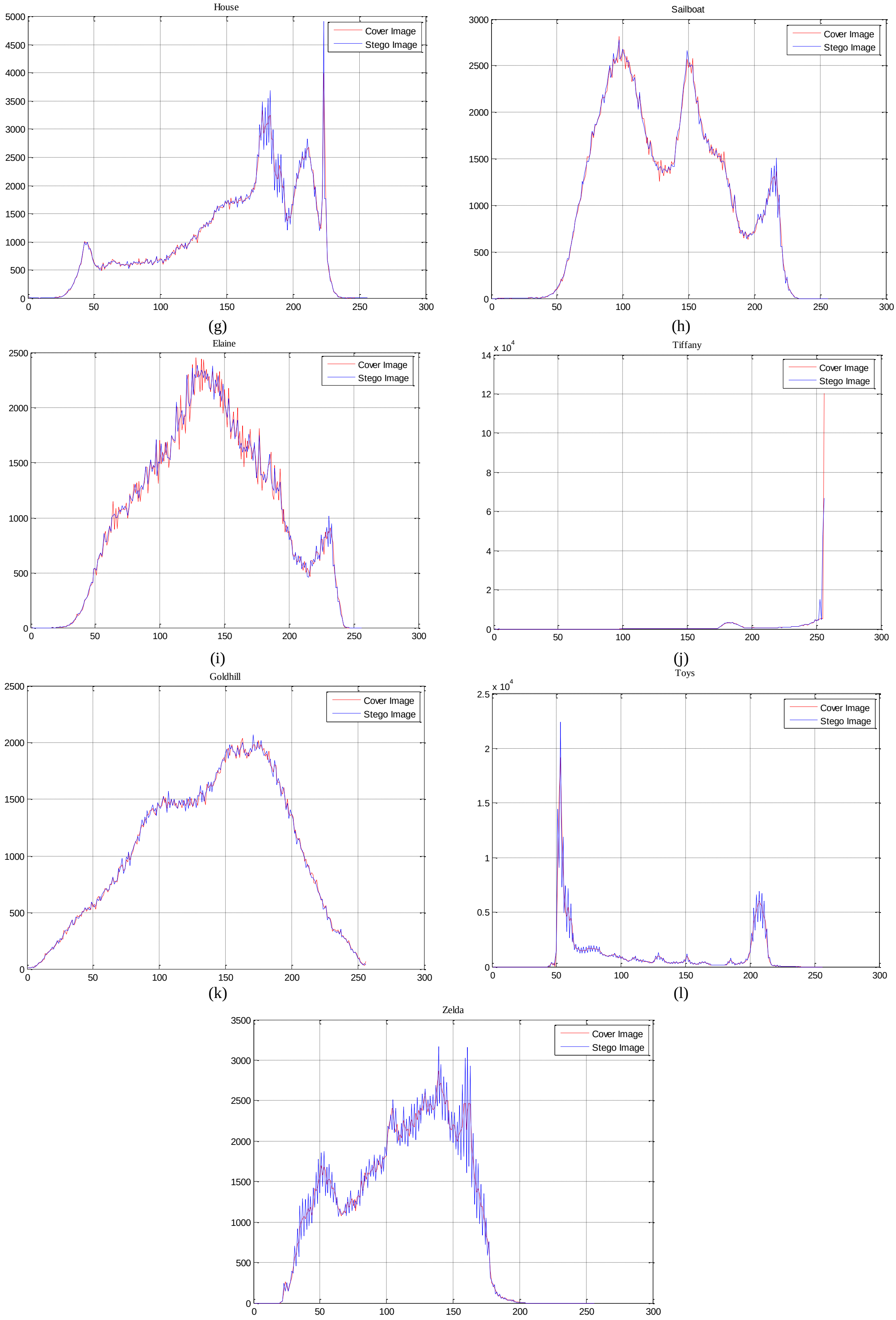
(b)

(c)

(d)

(e)

(f)



(g) (h)

(i) (j)

(k) (l)

(m)

Fig.9. The Histograms of Stego Image and Cover Image for Test Images
(a) Lena, (b) F16, (c) Baboon, (d) Barbara, (e) Boat, (f) Pepper, (g) House, (h) Sailboat, (i) Elaine, (j) Tiffany, (k) Goldhill, (l) Toys, (m) Zelda

Data embedding and data extracting processes running time of proposed method is also given in Table 5.

Table 5. Running Times of data Embedding and Data Extracting Processes for Test Images

Test Images (512x512)	Time (sec) for 1 bpp	
	Data Embedding	Data Extract
Lena	0.069168	0.048932
Barbara	0.064320	0.045023
Baboon	0.067654	0.043105
F16	0.069114	0.049731
Boat	0.069092	0.056022
Pepper	0.076035	0.053498
House	0.062452	0.037706
Sailboat	0.072378	0.052184
Elaine	0.070545	0.052636
Tiffany	0.065044	0.043495
Goldhill	0.066420	0.044093
Toys	0.068566	0.050303
Zelda	0.065619	0.043780
Average	**0.068185**	**0.047731**

Test Images (512x512)	Time (sec) for 2 bpp	
	Data Embedding	Data Extract
Lena	0.113872	0.047254
Barbara	0.108884	0.050283
Baboon	0.111490	0.051427
F16	0.109973	0.048256
Boat	0.108841	0.048606
Pepper	0.107190	0.048639
House	0.109721	0.049101
Sailboat	0.111420	0.049183
Elaine	0.109541	0.045971
Tiffany	0.110721	0.047532
Goldhill	0.111603	0.048779
Toys	0.106451	0.048197
Zelda	0.108448	0.047728
Average	**0.109858**	**0.048535**

VI. CONCLUSIONS

In this study, a data hiding algorithm based on pixel pairs and chaotic map is proposed. The obtained results by applying summary-modulo or subtraction-modulo operation to pixel pairs are equaled to secret data. Chaotic maps which have statistically powerful features are used in proposed method for providing privacy of secret data. The operation between the pixel pairs is selected according to chaotic maps. Thus, the randomness of processes and privacy of secret data are provided. To avoid overflow/underflow situations, different rules are described for boundary pixel values. *1* bpp and *2* bpp payload capacity are embedded into test images. The obtained results are compared using PSNR, capacity, quality, running time with previous selected similar methods. In test images, the average PSNR values are *63.2* and *60.1* for *10.000* and *20.000* payload capacity, respectively. The average PSNR values are *64.67* and *61.77* for *10.000* and *20.000* payload capacity in Kodak image data set, respectively. At the same time, the average capacity is *450.240* in selected test images. In test images (*512x512*), the average running times are *0.068185* and *0.047731* for data embedding and data extracting, respectively. According to the obtained results, the proposed method is obtained to be better than the comparative similar methods. The proposed algorithm has high payload capacity, high visual quality, good security and good running time. In the future time, a better data hiding algorithm can be performed by normalizing coefficients in frequency domain.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey”, *Proc.of the IEEE*, vol. 87(7), pp. 1062-1078, 1999.

[2] I. Vajda,"On Classical Cryptographic Protocols in Post-Quantum World", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.8, pp.1-8, 2017.DOI:10.5815/ijcnis.2017.08.01

[3] A. H. Lone, and M. Uddin, “A Novel Scheme for Image Authentication and Secret Data Sharing”. International Journal of Computer Network and Information Security, vol. 8(9), pp. 10, 2016.

[4] T. C. Lu, C. Y. Tseng, and J. H. Wu, “Dual imaging-based reversible hiding technique using LSB matching”, *Sig.Proc.*, vol. 108, pp. 77–89, 2015.

[5] Y. Liu, Z. Li, X. Ma, and J. Liu, “A robust data hiding algorithm for H.264/AVC video streams”, J. of Systems and Software, vol. 86(8), pp. 2174-2183, 2013.

[6] S. U. Maheswari, and D. J. Hemanth, “Image Steganography using Hybrid Edge Detector and Ridgelet Transform”. *Def.Sci.J.*, vol. 65(3), pp. 214-219, 2015.

[7] J. J. Garcia-Hernandez, R. Parra-Michel, C. Feregrino-Uribe, and R. Cumplido, “High payload data-hiding in audio signals based on a modified OFDM approach”, *Exp.Systems with App.*, vol. 40(8), pp. 3055-3064, 2013.

[8] Y. C. Chen, C. W. Shiu, and G. Horng, “Encrypted signal-based reversible data hiding with public key cryptosystem”, *J.of Visual Com. and Image Rep.*, vol. 25(5), pp. 1164-1170, 2014.

[9] N. Wang, H. Zhang, and C. Men, A high capacity reversible data hiding method for 2D vector maps based on virtual coordinates, *Comp.-Aided Design*, vol. 47, pp. 108-117, 2014.

[10] W. Hong, T. S. Chen, and J. Chen, “Reversible data hiding using Delaunay triangulation and selective embedment”, *Inf.Sciences*, vol. 308, pp. 140-154, 2015.

[11] S. Dogan, “A new data hiding method based on chaos embedded genetic algorithm for color image”, *Artificial Intell.Review*, vol. 46(1), pp. 129-143, 2016.

[12] P. V. S. Govind, and M. Wilscy, “A New Reversible Data Hiding Scheme with Improved Capacity Based on Directional Interpolation and Difference Expansion”, *Procedia Comp.Science*, vol. 46, pp. 491-498, 2015.

[13] R. Cogranne, and F. Retraint, “Application of hypothesis testing theory for optimal detection of LSB matching data hiding”, *Sig.Proc.*, vol. 93(7), pp. 1724-1737, 2013.

[14] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, “Image steganography using uncorrelated color space and its application for security of visual contents in online social networks”. *Fut.Gen.Computer Syst.*, http://dx.doi.org/10.1016/j.future.2016.11.029, 2016.

[15] S. Dogan, “A reversible data hiding scheme based on graph neighbourhood degree”. *J.of Experimental& Theoretical Artificial Intell.* vol. 29(4), pp. 741-753, 2016.

[16] Y. K. Chan, W. T. Chen, S. S. Yu, Y. A. Ho, C. S. Tsai, and Y. P. Chu, “A HDWT-based reversible data hiding method”, *J.of Systems and Software,* vol. 82(3), pp.411-421, 2009.

[17] Y. K. Lin, “A data hiding scheme based upon DCT coefficient modification”, *Comp.Standards&Interfaces,* vol. 36(5), pp.855-862, 2014.

[18] J. Chen, “A PVD-based data hiding method with histogram preserving using pixel pair matching”, *Sig.Proc.: Image Communication,* vol. 29(3), pp.375-384, 2014.

[19] S. Y. Shen, and L. H. Huang, “A data hiding scheme using pixel value differencing and improving exploiting modification directions”, *Computers & Security,* vol. 48, pp. 131-141, 2015.

[20] X. Qu, and H. J. Kim, “Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding”, *Sig.Proc.,* vol. 111, 249-260, 2015.

[21] X. Wang, J. Ding, and Q. Pei, “A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition”, *Information Sciences,* vol. 310, pp.16-35, 2015.

[22] C. C. Lin, and N. L. Hsueh, “A lossless data hiding scheme based on three-pixel block differences”, *Pattern Recog.,* vol. 41(4), pp. 1415-1425, 2008.

[23] X. Li, J. Li, B. Li, and B. Yang, “High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion”, *Sig.Proc.,* vol. 93(1), pp.198-205, 2015.

[24] Y. Y. Tsai, D. S. Tsai, and C. L. Liu, “Reversible data hiding scheme based on neighboring pixel differences”, *Dig.Sig.Proc.,* vol. 23(3), pp. 919-927, 2013.

[25] W. Hong, T. S. Chen, and C. W. Luo, “Data embedding using pixel value differencing and diamond encoding with multiple-base notational system”, *J.of Systems and Software,* vol. 85(5), pp. 1166-1175, 2012.

[26] C. H. Yang, C. Y. Weng, H. K. Tso, and S. J. Wang, “A data hiding scheme using the varieties of pixel-value differencing in multimedia images”, *J.of Systems and Software,* vol. 84(4), pp. 669-678, 2011.

[27] Y. P. Lee, J. C. Lee, W. K. Chen, K. C. Chang, I. J. Su, and C. P. Chang, “High-payload image hiding with quality recovery using tri-way pixel-value differencing”, *Information Sciences,* vol. 191, pp. 214-225, 2012.

[28] F. Peng, X. Li, and B. Yang, “Improved PVO-based reversible data hiding”, *Dig.Sig.Proc.,* vol. 25**,** pp.255-265, 2014.

[29] C. C. Chang, Y. H. Huang, H. Y. Tsai, and C. Qin, “Prediction-based reversible data hiding using the difference of neighboring pixels”, *AEU – Inter. J.of Electronics and Com.,* vol. 66(9), pp.758-766, 2012.

[30] G. Chen, and Y. Huang, “Chaotic Maps Dynamics, Fractals, and Rapid Fluctuations”, Morgan & Claypool Publishers, 2011.

[31] A. Baykasoglu, “Design optimization with chaos embedded great deluge algorithm”, *App.Soft.Comp.,* vol. 12, pp. 1055–1067, 2012.

[32] R. Ye, W. Guo,"An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters", IJCNIS, vol.6, no.4, pp.37-45, 2014. DOI: 10.5815/ijcnis.2014.04.05

[33] L. Acho, “A discrete-time chaotic oscillator based on the logistic map: A secure communication scheme and a simple experiment using Arduino”, *J.of the Franklin Institute,* vol. 352 (8), pp. 3113–3121, 2015.

[34] SIPI Image Dataset, http://sipi.usc.edu/database/. (03.12.2014).

[35] Kodak Lossless True Color Image Suite, http://r0k.us/graphics/kodak/ (05.01.2015).

[36] W. Zhang, K. Ma, and N. Yu, “Reversibility improved data hiding in encrypted images”, *Sig.Proc.,* vol. 94, pp.118–127, 2014.

[37] Z. Wang, and A. C. Bovik, “A Universal Image Quality Index”, *IEEE Sig.Proc.Letters,* vol. 9(3), pp.1-4, 2002.

[38] C. C. Chang, and T. C. Lu, “A difference expansion oriented data hiding scheme for restoring the original host image”, *J.of Systems and Software,* vol. 79, pp.1754-1766, 2006.

[39] C. T. C. Lu, C. Chang, and Y. H. Huang, “High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting”, *Multimedia Tools and App.,* vol. 71(1), pp. 417-435, 2014.

Authors’ Profiles

Sengul Dogan received her Ph.D degree in Electrical and Electronic Engineering from the University of Firat, Elazig, Turkey, in 2011. She is currently an Assistant Professor in the Digital Forensics Engineering Department of Firat University. Her research interests cover Data Hiding, Information Security, Digital Forensics, Image Processing and Optimization Techniques.

How to cite this paper: Sengul Dogan,"A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.1, pp.1-9, 2018.DOI: 10.5815/ijcnis.2018.01.01