THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 4 Article 8

12-2017

A DATA HIDING SCHEME BASED ON CHAOTIC MAP AND PIXEL PAIRS

Sengul DOGAN SD
Firat University, senguldgn@gmail.com

Recommended Citation

DOGAN, Sengul SD (2017) "A DATA HIDING SCHEME BASED ON CHAOTIC MAP AND PIXEL PAIRS," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 4 , Article 8.
DOI: https://doi.org/10.15394/jdfsl.2017.1456
Available at: https://commons.erau.edu/jdfsl/vol12/iss4/8

A DATA HIDING SCHEME BASED ON CHAOTIC MAP AND PIXEL PAIRS

Sengul Dogan
Firat University, Turkey

ABSTRACT

Information security is one of the most common areas of study today. In the literature, there are many algorithms developed in the information security. The Least Significant Bit (LSB) method is the most known of these algorithms. The LSB method is easy to apply; however, it is not effective on providing data privacy and robustness. In spite of all its disadvantages, LSB is the most frequently used algorithm in literature, due to providing high visual quality. In this study, an effective data hiding scheme alternative to LSB, 2LSBs, 3LSBs and 4LSBs algorithms (known as xLSBs), is proposed. In this method, random numbers which are to be used as indices of pixels of the cover image are obtained from chaotic maps and data hiding process is applied on the values of these pixels by using modulo function. Calculated values are embedded in cover image as hidden data. Success of the proposed data hiding scheme is assessed by Peak Signal-to-Noise Ratio (PSNR), payload capacity and quality.

1. INTRODUCTION

The development of technology, especially in communication systems, greatly facilitates human life. The progress in communication technologies enables us to use electronic devices such as smartphones and tablets without time and place concerns, thanks to mobility and wide-area networks. But as technology continues to improve, electronic data security has become an important issue in daily life [1,2]. Main purpose of data security is to prevent unauthorized copying, changing or damaging of any data whether it is stored in a storage device or internet. Precautions are needed to provide data security [3]. Several methods such as Data Hiding [4-6], Cryptography [7-9] and Watermarking [10,11] are used to provide data security. All these methods need to have three base qualities which are listed below [12].

- Identity: There must not be an identity problem between sender and receiver.
- Integrity: There must not be any change in data during transmission process.
- Privacy: Data must not be seen by any party other than the receiver.

Watermarking is used for determining ownership of data which is in a network or World Wide Web. Watermark is embedded into a data such as image, an audio or a video by the owner of data. Anyone who has an extraction function to decode the watermark, gets the ownership information of the data [13]. In cryptography method, data transformed a different format by the way of encryption. Thus, any third-party who gets the encrypted data needs to have the crypto key or any means to decipher the code, in order to

have the raw data [7]. The main purpose of data hiding algorithms is to ensure transmission of data with a seemingly innocent cover object. At the end of data hiding process, less the cover object changes, more successful is the algorithm [5, 6]. Data hiding methods can be performed in spatial domain, frequency domain and compression domain. Vector Quantization (VQ) is one of the most widely used methods in compression domain [14]. Also, the most popular method among developed methods is LSB in spatial domain. In LSB method, secret data is embedded into least significant bits of cover object as shown in Table 1 [15].

Table 1.
Data Hiding Process with LSB Method

Secret message	Pixel value of cover image	Binary value of cover image	Binary value of stego image	Pixel value of stego image
11	$CI_{i,j}$=108 $CI_{i,j+1}$= 111	1101100 1101111	1101101 1101111	$SI_{i,j}$=109 $SI_{i,j+1}$=111

In the frequency domain, the specific coefficients are obtained by applying methods such as Discrete Wavelet Transform (DWT) [16], Discrete Cosine Transform (DCT) [17], and Discrete Fourier Transform (DFT) [18]. The obtained coefficients from these methods are embedded in secret data. DFT, widely used in image processing, is capable of distinguishing the frequency components of a picture from each other. Thus, low and high-pass filtering operations are provided at different ratios. DWT is another technique used in the frequency domain. in this technique an image is passed through the low and high pass filter to obtain the sub-bands. LL, LH, HL, HH sub-bands obtained from DWT method are shown in Figure 1.

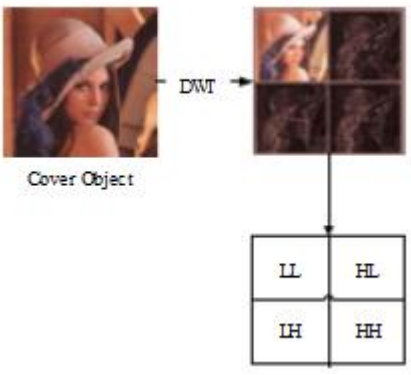


Figure 1. DWT Sub-bands of Cover Image

DCT transmits the pixel values to the frequency domain by splitting the image into blocks of 8 x 8 size. Robustness of cover image is increased by embedding secret data into coefficients of these subbands [16].

2. LITERATURE REVIEW

There are many studies about data hiding in literature. Zhao et al. [19] propose an enhanced data hiding scheme based on modulus function (MF) and pixel-value differencing (PVD) using indeterminate equation. Their study ensures higher embedding than modulus function-PVD and PVD methods. Gholampour and Khosravi [20] introduce a data hiding method using multiple q-ary schemes. Their results provide less corruption and high security. Pan et al. [21] perform an effective data hiding method using side-match distortion based on joint neighboring coding. According to the results obtained, higher embedding capacity and image quality than comparable methods. Hong and Chen [22] present a data hiding scheme using adaptive pixel pair matching (APPM). Their experimental results provide higher performance than between optimal pixel adjustment process and diamond encoding. Their method also provides high security for known steganalysis methods. Weng et al. [23] propose an improved hiding method using pairwise difference adjustment (PDA) on pixel pairs. In this method, PDA tries to arrange the embedding process according to this value by setting a threshold value to minimize the distortion of the pixel pairs. Thus, PDA allows to increase the embedding capacity and solve overflow- underflow problems. Thus, a higher PSNR value is obtained. Tai et al. [24] introduce a new data hiding scheme using histogram modification. Their experimental results ensure large embedding capacity by reducing distortion. Yang et al. [25] present an improved data hiding method in edge areas of images with least-significant-bit domain using PVD. The embedding capacity is increased for gray images with their proposed method.

In this paper, a data hiding scheme based on pixel pairs is proposed. Chaotic maps are described in section 2. The proposed method is presented in section 3. In section 4, the results are given. Finally, conclusion of this study is presented in section 5.

3. CHAOTIC MAPS

Chaos theory is a mathematical technique which aims to define a system under chaos. According to the rules of chaos theory [3,26]:

- Chaotic systems are not linear.
- They are complex.
- They exist in structure of nature.
- They have feedback mechanism.
- They are extremely sensitive to initial conditions.

Chaotic theory has many uses in areas such as education, science, social studies, and engineering. For instance, random numbers which are needed by several security algorithms in computer systems, can be generated by random number generators (RNG) [27,28]. However, these RNGs may generate the same numbers in a specific iteration which is not desirable. To solve this problem, chaotic maps may be used instead of RNGs [29,30]. Random numbers generated by chaotic maps has an order in their own disarray. Widely used equations of chaotic maps in literature are presented in Table 2 [29,31].

Table 2.
The Most Commonly used Chaotic Maps and Equations

Chaotic maps	**Equations**
Logistic map	$x_{n+1} = rx_n(1-x_n) \quad 3.57 \le r \le 4, \quad x_n \in (0,1)$
Tent map	$x_{n+1} = \begin{cases} \frac{x_n}{0.7} & x_n < 0.7 \\ \frac{10}{3}x_n(1-x_n), & otherwise \end{cases} \quad x_n \in (0,1)$
Chebyshev map	$x_{n+1} = \cos(r\cos^{-1}x_n) \quad r > 0, x_n \in [-1,1]$
Circle map	$x_{n+1} = x_n + \varphi - \left(\frac{\tau}{2\pi}\right)\sin 2\pi x_n \quad mod(1) \quad x_n \in (0,1)$
Cubic map	$x_{n+1} = rx_n(1-x_n^2) \quad x_n \in (0,1)$
Gauss map	$x_{n+1} = \begin{cases} 0 & x_n = 0 \\ \frac{1}{x_n} - \left[\frac{1}{x_n}\right] & x_n \neq 0 \end{cases} \quad x_n \in (0,1)$
Henon map	$x_{n+1} = 1 - \propto x_n^2] + \beta y_n$ $y_{n+1} = x_n$
Icmic map	$x_{n+1} = \sin\frac{\propto}{x_n} \quad \propto \in (0,\infty), \ x_n \in (-1,1)$
Sinusodial map	$x_{n+1} = \sin(\pi x_n)\ x_n \ \in (0,1)$
Sinus map	$x_{n+1} = 2.3(x_n)^{2\sin(\pi x_n)}$

4. THE PROPOSED SCHEME

The proposed method is similar to data hiding algorithms based on pixel pairs. This algorithm carries out data hiding process by using a single pixel and random numbers which are the virtual pairs of this pixel. Chaotic maps are used as deterministic RNGs. Data hiding steps of this method is given below.

Step 1: Generate random numbers as much as the number of pixels in the cover image. Chaotic maps are used for generating random numbers. Equation of logistic map, as being the most frequently used chaotic map, is given in Equation 1.

$$x_{t+1} = rx_t(1-x_t), t = \{1,2,\dots,mn\}, \quad x \neq 0.5, x \in (0,1), r \in [3.57,4] \tag{1}$$

$r \rightarrow$ logistic map multiplier
$t \rightarrow$ iteration number
$x_t \rightarrow$t. chaotic number

Step 2: Convert numbers obtained in step 1 into two dimensions and encode these numbers in user specified range.

Step 3: Determine data hiding capacity. If data will be embedded with b bit capacity, secret data must be encoded with b bits.

Step 4: Perform processes below to determine which operator (+, -) will be used

$$h = \begin{cases} -1, x_{i,j} \bmod 2 = 0 \\ +1, x_{i,j} \bmod 2 = 1' \end{cases}, \; i = \{1, 2, \dots, m\}, \; j = \{1, 2, \dots, n\} \quad (2)$$

Step 5: Apply the equation below for data hiding process

$$GV_{i,j} = SI_{i,j} + hx_{i,j} \bmod 2^b, \; i = \{1, 2, \dots, m\}, \; j = \{1, 2, \dots, n\} \quad (3)$$

$h \rightarrow$ -1, +1
$GV_{i,j} \rightarrow$ Secret data set
$SI_{i,j} \rightarrow$ Selected pixel value of stego image
$OI_{i,j} \rightarrow$ Selected pixel value of original image

If the equation is not ensured, pixel values are changed according to determined rules and equation is ensured. For example, if 1 bit per pixel (bpp) data will be embedded into cover image, $GV_{i,j} = SI_{i,j} \pm x_{i,j} \bmod 2$ equation must be ensured. To ensure this equation, pixel values of cover image is increased by one or are not changed. For instance, if it is assumed $b = 1$, $x_{i,j} = 45$, $OI_{i,j} = 125$ and $GV_{i,j} = 1$, the processes below are performed.

Due to $45 \bmod 2 = 1$, addition operator is used.

$(125 + 45) \bmod 2^1 = 0$ but this value must be equal to $GV_{i,j}$. For this reason, process below is performed.

Because of $SI_{i,j} = OI_{i,j} + 1$ process, new value of pixel will be 126. Thus, data hiding process is performed by ensuring $126 + 45 \bmod 2^1 = 1$ equation.

As given in the example, the pixel values of the cover image are increased by one or are not changed for embedding 1 bpp in the proposed method. Namely, the pixel value set is expressed with R= {0, 1} for embedding 1 bpp. The pixel value set is expressed with R= {-1, 0, 1} when the same process is performed with LSB. While there are two values in change set of the proposed method, there are three values in change set of LSB. If data hiding is performed with the proposed method, pixel values remain unchanged by P=0.5 probability, but this probability value is 0.33 in LSB. These values mathematically prove that the proposed algorithm decreases quality of cover image less than LSB. If 2LSBs is used for data hiding process, pixel values remain unchanged by 1/7 probability in 2LSBs but this probability in the proposed method is 1/4. The pixel values of cover image change between [-7, 7] range in 3LSBs but pixel values change between [-4, 3] range in the proposed method. Also, the pixel values of the cover image change between [-15, 15] range in 4LSBs but pixel values change between [-8, 7] range in the proposed method. Comparison of these probability results are shown in Table 3.

Table 3.
The Comparison of Probabilities

Methods	1bpp	2bpp	3bpp	4bpp
LSB	1/3	1/7	1/15	1/31
The proposed algorithm	1/2	1/4	1/8	1/16

Taking Table 3 and the examples into consideration, the probability of unchangeably of cover image is expressed with Equation 4 and 5.

$$P_{lsb} = \frac{1}{2^{b+1} - 1} \quad (4)$$

$$P_{pm} = \frac{1}{2^{b}} \quad (5)$$

The most important advantage of the proposed method is to optimize the selection of pixel pairs embedding data in accordance with the xLSBs and minimize the change in the cover image. The disadvantage of the proposed method is also overflow problem. In order to solve overflow problem, either normalization process is performed or pixels which will not cause overflow is collected and data hiding process is performed on these pixels. The pseudo code of the proposed method is given in Figure 2.

```
Input: Cover image, Logistic map, Secret data
Output: Stego image
for i=1 to m do
    for j=1 to n do
        sg=GV_{i,j};
        pd=x_{i,j}+CI_{i,j} mod 2^b
        for ll=0 to 2^{b-1} do
            if sg=ll then
                if sg=1+ll mod 2^b then
                    SI_{i,j}=OI_{i,j-1};
                else if sg=2+ll mod 2^b then
                    SI_{i,j}=OI_{i,j}-2;
                .
                    .
                else if sg=2^b -2+ll mod 2^b then
                    SI_{i,j}=OI_{i,j}+2;
                else if sg=2^b -2+ll mod 2^b then
                    SI_{i,j}=OI_{i,j}+1;
                else
                    SI_{i,j}=OI_{i,j};
                end
            end
        end
    end
end
```

Figure 2. The Pseudo Code of the Proposed Method

In the proposed method, data extraction step consists of the following 3 steps:
Step 1: Obtain the size of the secret data and the value of RNG from stego-key.
Step 2: Generate RNG whose seed values are obtained.
Step 3: Obtain secret data by using Equation 6.

$$GV_{i,j} = SI_{i,j} + hx_{i,j} \; mod \; 2^{b} \quad (6)$$

5. RESULTS AND DISCUSSIONS

In this study, the obtained results are evaluated using MATLAB 2014a with Windows 10 operating system. In this paper, Kodak image dataset [32] and test images [33] are used and varied sized secret data are embedded into both of the image sets. Test images which are named as Lena, F16, Baboon, Barbara, Boat, Pepper, House, Sailboat, Elaine, Tiffany, Toys, and Zelda are 512x512 sized and gray-scale. In Figure 3, these test images are shown.

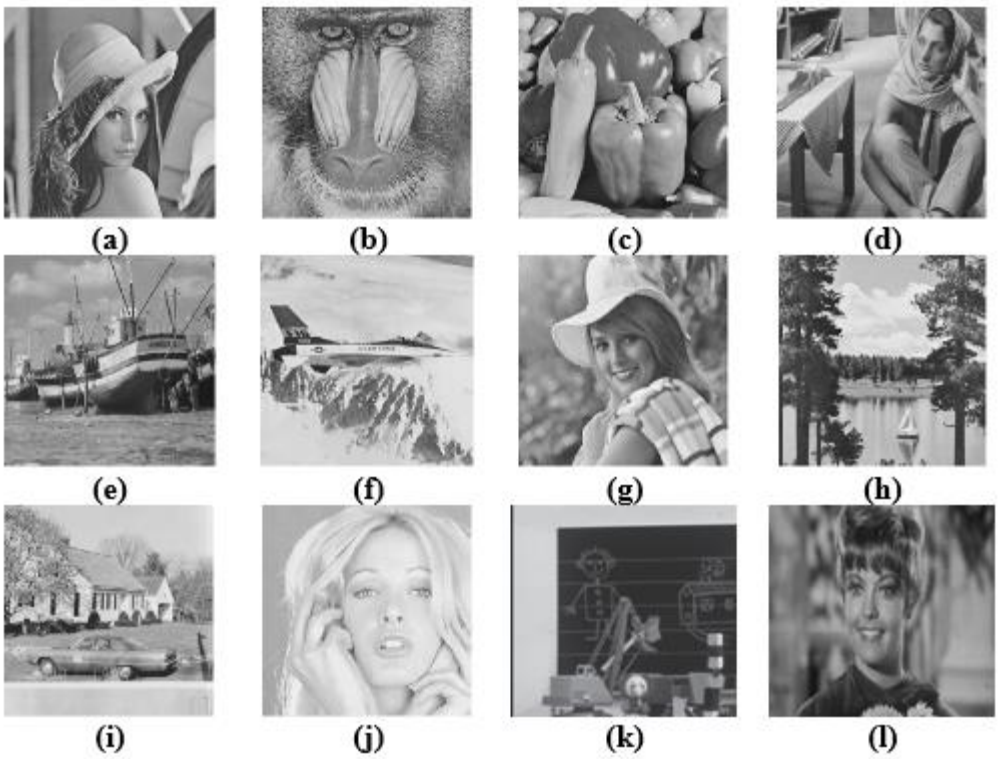


Figure 3. The Test Images
(a) Lena (b) Baboon (c) Pepper (d) Barbara (e) Boat (f) F16 (g) Elaine (h) Sailboat (i) House (j) Tiffany (k) Toys (l) Zelda

The proposed method is assessed by PSNR [34] and Quality values [35]. PSNR equations are given in Equation 7, 8.

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - SI_{i,j})^2 \tag{7}$$

$$PSNR = 10\log\frac{Max(CI_{i,j}^2)}{MSE} \tag{8}$$

$CI_{i,j}\rightarrow$ Cover image
$SI_{i,j}\rightarrow$ Stego image
$m \rightarrow$ Line number of cover/stego image
$n \rightarrow$ Column number of cover/stego image

PSNR and Capacity values of the proposed method for test images are given in Figure 4.

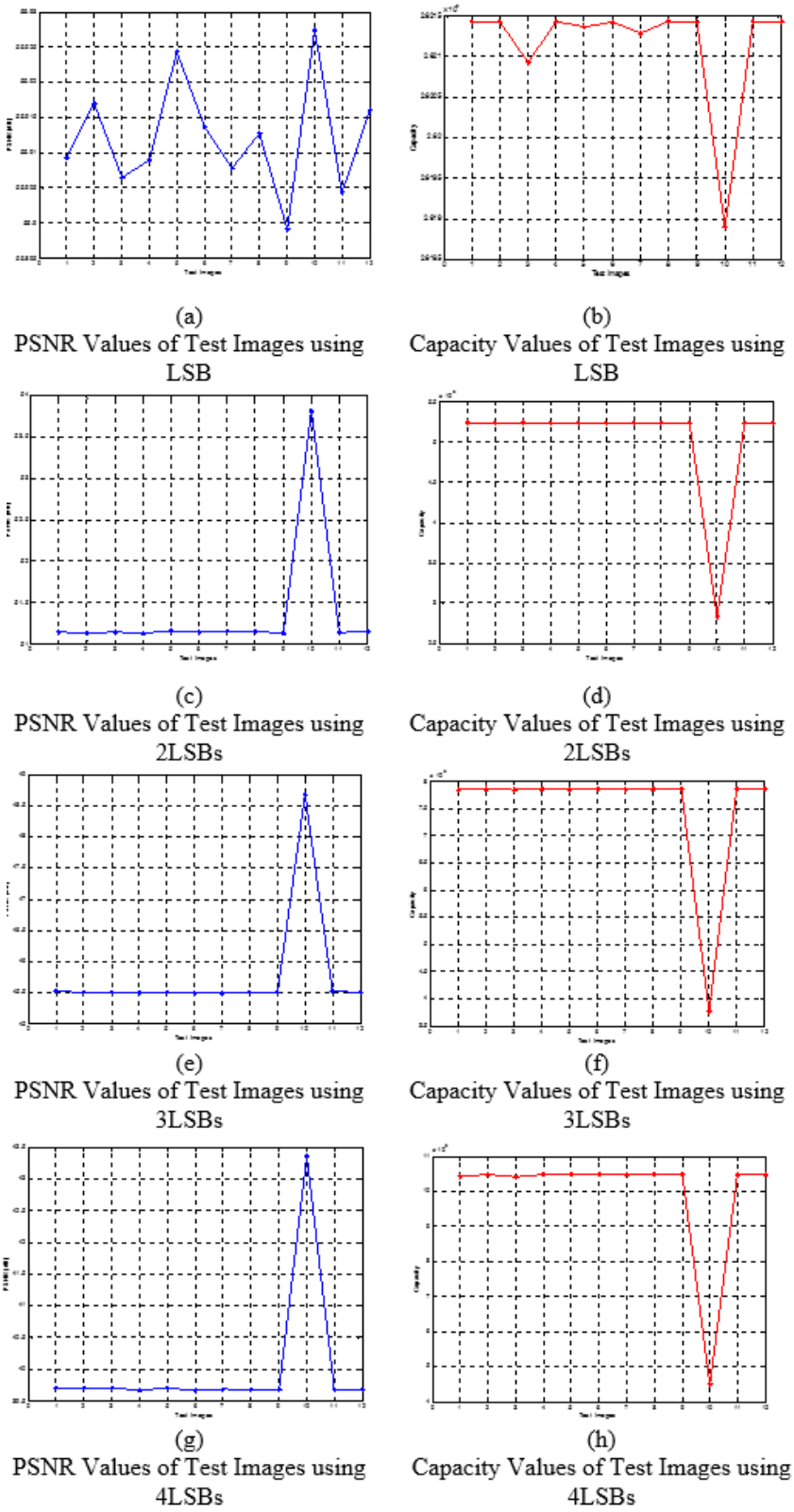
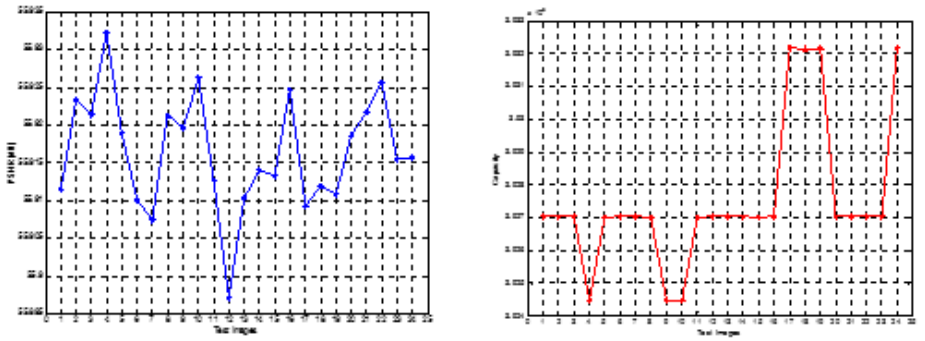


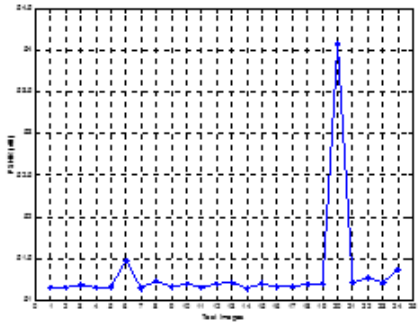
Figure 4. PSNR and Capacity Values for Test Images

In the results obtained in Figure 4, test images are numbered as [1-Lena, 2-F16 3-Baboon 4-Barbara 5-Boat 6-Pepper 7-House 8-Sailboat 9-Elaine 10-Tiffany 11-Toys 12-Zelda]. PSNR and Capacity values of the proposed method for Kodak data set are given in Figure 5.

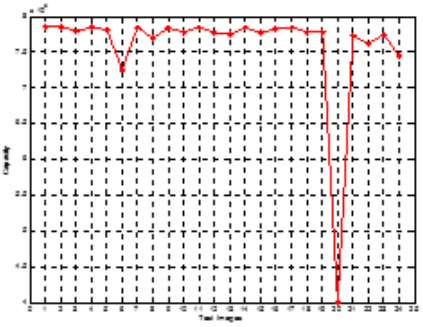


(a) PSNR Values of Kodak Dataset using LSB

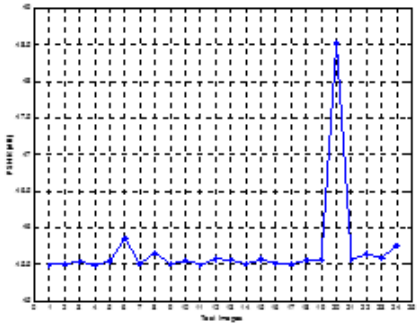
(b) Capacity Values of Kodak Dataset using LSB



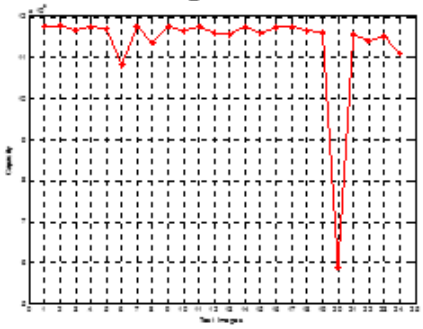
(c) PSNR Values of Kodak Dataset using 2LSBs



(d) Capacity Values of Kodak Dataset using 2LSBs

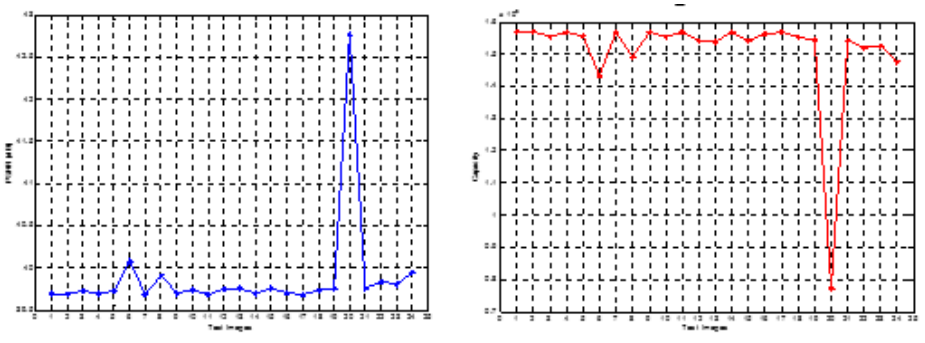


(e) PSNR Values of Kodak Dataset using 3LSBs



(f) Capacity Values of Kodak Dataset using 3LSBs

Figure 5 continued below.



(g) PSNR Values of Kodak Dataset using 4LSBs

(h) Capacity Values of Kodak Dataset using 4LSBs

Figure 5. PSNR and Capacity Values for KODAK Dataset

The capacity and PSNR values given in Figure 5 are presented for the 25 selected images from the Kodak data set. The obtained average PSNR value is 58.34 dB with the payload of 50,000 bits for test images (Lena, House, Baboon, Peppers, Barbara, Airplane). Also, the obtained average PSNR value is 64.86 dB with the payload of 50,000 bits for Kodak image dataset. In the proposed method, when the results obtained in Figures 4 and 5 are evaluated, it is seen that close PSNR values are obtained for the same payload capacity. Besides, considering experimental results, the proposed algorithm has high data hiding capacity and visual quality.

Another visual quality criterion in data hiding applications is Quality. Q measures the similarity of two images. The closer Q is to 1, the more two images are similar. Q equations are given in Equation 9-14.

$$Q = \frac{4\sigma_{xy}\,\overline{x} \times \overline{y}}{(\sigma_x^2 + \sigma_y^2)[\,\overline{x}^2 + \overline{y}^2\,]} \tag{9}$$

$$\overline{x} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n} CI_{i,j} \tag{10}$$

$$\overline{y} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n} SI_{i,j} \tag{11}$$

$$\sigma_x^2 = \frac{1}{mn-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(CI_{i,j} - \bar{x})^2 \tag{12}$$

$$\sigma_y^2 = \frac{1}{mn-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(SI_{i,j} - \bar{y})^2 \tag{13}$$

$$\sigma_{xy} = \frac{1}{mn-1}\sum_{i=1}^{m}\sum_{j}^{n}(CI_{i,j} - \bar{x})(SI_{i,j} - \bar{y}) \tag{14}$$

$\overline{x}$ → the mean value of cover image,
$\overline{y}$ → the mean value of stego image,
σ_x^2 →the variance of set cover image,
σ_y^2 →the variance of stego image,
σ_{xy} →the covariance of the values from the cover image and stego image

The proposed method for different payload capacity is evaluated in terms of Quality and the results are shown in Figure 6.

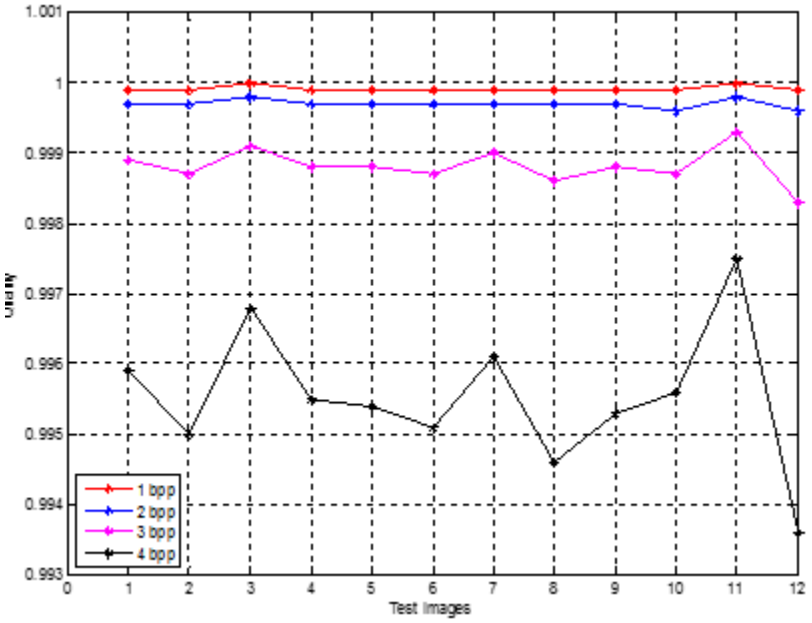


Figure 6 Quality Values of the Proposed Method

6. CONCLUSION

In this paper, a new data hiding scheme based on chaotic maps is presented. Chaotic maps and modulo function are used for data hiding in this method. Data privacy is provided by using random number generator based on chaos. It is shown that, this algorithm being fast and easy to perform, can be used instead of xLSBs. If the proposed algorithm is applied in frequency domain, robustness of the algorithm may be increased. In the future studies, to achieve the expected increase in robustness, this method will be performed in frequency domain and used for data hiding into other multimedia objects.

REFERENCES

[1] Celik, M. U., Sharma, G., Saber, E., & Tekalp, A. M. (2002). Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing*, *11*(6), 585-595.

[2] Warkentin, M., Bekkering, E., & Schmidt, M. B. (2008). Steganography: Forensic, security, and legal issues. *The Journal of Digital Forensics, Security and Law: JDFSL*, *3*(2), 17.

[3] Doğan, Ş. (2016). A new data hiding method based on chaos embedded genetic algorithm for color image. *Artificial Intelligence Review*, *46*(1), 129-143.

[4] Sutherland, I., Davies, G., Pringle, N., & Blyth, A. (2009). The impact of hard disk firmware steganography on computer forensics. *The Journal of Digital Forensics, Security and Law: JDFSL*, *4*(2), 73.

[5] Wang, X., Ding, J., & Pei, Q. (2015). A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition. *Information sciences*, *310*, 16-35.

[6] Dogan, S. (2017). A reversible data hiding scheme based on graph neighbourhood degree. *Journal of Experimental & Theoretical Artificial Intelligence*, *29*(4), 741-753.

[7] Kulkarni, A., Goldman, J., Nabholz, B., & Eyre, W. (2009). Detection of Steganography-Producing Software Artifacts on Crime-Related Seized Computers. *Journal of Digital Forensics, Security and Law*, *4*(2), 5-26.

[8] Ou, D., Sun, W., & Wu, X. (2015). Non-expansible XOR-based visual cryptography scheme with meaningful shares. *Signal Processing*, *108*, 604-621.

[9] Lai, H., Xiao, J., Li, L., & Yang, Y. (2012). Recursive hiding of biometrics-based secret sharing scheme using adversary structure. *Information Processing Letters*, *112*(17), 683-687.

[10] Tuncer, T. (2017). A novel image authentication method based on singular value decomposition. *Journal of the Faculty of Engineering and Architecture of Gazi University, 32*(3), 877-886.

[11] Ahmed, A. M., & Day, D. D. (2004). Applications of the naturalness preserving transform to image watermarking and data hiding. *Digital Signal Processing*, *14*(6), 531-549.

[12] Faircloth, J. (2014). Chapter 5 – Information Security, *Enterprise Applications Administration*, 175-220.

[13] Vaishnavi, D., & Subashini, T. S. (2015). Robust and invisible image watermarking in RGB color space using SVD. *Procedia Computer Science*, *46*, 1770-1777.

[14] Chang, C. C., Tai, W. L., & Lin, C. C. (2006). A reversible data hiding scheme based on side match vector quantization. *IEEE Transactions on Circuits and Systems for Video Technology*, *16*(10), 1301-1308.

[15] Lin, Y. K. (2014). A data hiding scheme based upon DCT coefficient modification. *Computer Standards & Interfaces*, *36*(5), 855-862.

[16] Liu, T., & Qiu, Z. D. (2002, August). A DWT-based color image steganography scheme. In *Signal Processing, 2002 6th International Conference on* (Vol. 2, pp. 1568-1571). IEEE.

[17] Noda, H., Niimi, M., & Kawaguchi, E. (2006). High-performance JPEG

steganography using quantization index modulation in DCT domain. *Pattern Recognition Letters*, *27*(5), 455-461.

[18] Chen, W. Y. (2008). Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *Applied Mathematics and computation*, *196*(1), 40-54.

[19] Zhao, W., Jie, Z., Xin, L., & Qiaoyan, W. (2015). Data embedding based on pixel value differencing and modulus function using indeterminate equation. *The Journal of China Universities of Posts and Telecommunications*, *22*(1), 95-100.

[20] Gholampour, I., & Khosravi, K. (2015). Steganographic schemes with multiple q-ary changes per block of pixels. Signal Processing, 108, 206-219.

[21] Pan, Z., Hu, S., Ma, X., & Wang, L. (2015). A new lossless data hiding method based on joint neighboring coding. *Journal of Visual Communication and Image Representation*, *26*, 14-23.

[22] Hong, W., & Chen, T. S. (2012). A novel data embedding method using adaptive pixel pair matching. *IEEE transactions on information forensics and security*, *7*(1), 176-184.

[23] Weng, S., Zhao, Y., Pan, J. S., & Ni, R. (2008). Reversible watermarking based on invariability and adjustment on pixel pairs. *IEEE Signal Processing Letters*, *15*, 721-724.

[24] Tai, W. L., Yeh, C. M., & Chang, C. C. (2009). Reversible data hiding based on histogram modification of pixel differences. *IEEE Transactions on Circuits and Systems for Video technology*, *19*(6), 906-910.

[25] Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, *3*(3), 488-497.

[26] Lou, D. C., & Sung, C. H. (2004). A steganographic scheme for secure communications based on the chaos and Euler theorem. *IEEE Transactions on Multimedia*, *6*(3), 501-509.

[27] Yi, S., & Zhou, Y. (2017). Binary-block embedding for reversible data hiding in encrypted images. *Signal Processing*, *133*, 40-51.

[28] Bailey, J. P., Beal, A. N., Dean, R. N., Hamilton, M. C., & Tugnait, J. K. (2014). High-frequency reverse-time chaos generation using digital chaotic maps. *Electronics Letters*, *50*(23), 1683-1685.

[29] Baykasoglu, A. (2012). Design optimization with chaos embedded great deluge algorithm. *Applied Soft Computing*, *12*(3), 1055-1067.

[30] Roy, R., Sarkar, A., & Changder, S. (2013). Chaos based edge adaptive image steganography. *Procedia Technology*, *10*, 138-146.

[31] Arivazhagan, S., Jebarani, W. S. L., Kalyani, S. V., & Abinaya, A. D. (2017, March). Mixed chaotic maps based encryption for high crypto secrecy. In *Signal Processing, Communication and Networking (ICSCN), 2017 Fourth International Conference on* (pp. 1-6). IEEE.

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

[33] L. University, UCID Image Dataset, http://homepages.lboro.ac.uk/~cogs/datasets/ucid/ucid.html (18.11.2014).

[34] Zhang, W., Ma, K., & Yu, N. (2014). Reversibility improved data hiding in encrypted images. Signal Processing, 94, 118-127.

[35] Wang, Z., & Bovik, A. C. (2002). Image and Multidimensional Signal Processing-A Universal Image Quality Index. *IEEE Signal Processing Letters*, *9*(3), 81-84.

