Research Journal of Applied Sciences, Engineering and Technology 5(2): 553-557, 2013
ISSN: 2040-7459; E-ISSN: 2040-7467

Submitted: May 16, 2012 Accepted: June 06, 2012 Published: January 11, 2013

Gray Level Image Hiding by Using Mackey-Glass Series

[1]Rasul Enayatifar, [1]Abdul Hanan Abdullah, [2]Abdulrahman A. Mirza and [2]Maqsood Mahmud
[1]Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, Malaysia
[2]Department of Information System, CCIS, King Saud University, Saudi Arabia

Abstract: In this study a new method for Steganography is proposed. This method is base on Mackey-Glass series. This series is used to determine the position of every bit of secret image in the cover image. The main advantage of this method is the homogenous distribution of the secret image pixels in the cover image pixels that it causes the stability of the proposed result against common attacks to increase. Stability review of proposed method against type of damages such as corrupted, cutting and noise from image, also high amount of PSNR (approximately 45) in this method is represented high performance of this method.

Keywords: Chaotic function, cover image, image encryption, secret image

INTRODUCTION

As a new kind of secret communication technology, steganography is mainly used to convey messages secretly by concealing their very existence. Data security over the Internet is becoming more critical (Cheng and Huang, 2001) because of the digitization of data and networking of communications. The Internet is by and large an open channel in which modification, interception, falsification, as well as other forms of distortion can occur. To reach this goal, steganography offers different approaches to transmitting secret messages (Anderson and Petitcolas, 1998; Petitcolas *et al*., 1999). The most common and well-known steganographic method is called Least Significant Bit (LSB) substitution, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly (Bender *et al*., 1996). Many optimized LSB methods have been proposed to improve this study (Wang *et al*., 2001; Chan and Chen, 2004; Lin *et al*., 2009). Wu and Tsai (2003) proposed a novel steganographic method that uses the difference value between two neighboring pixels to determine how many secret bits should be embedded (Wu and Tsai, 2003). Another method based on wavelet is proposed in (Kwok and Tang, 2007), which puts the pixels of secret image in the cover image sequentially. Therefore this method has weakness against cutting attack. In the recent years researchers has concentrated on the methods that distribute pixels in cover image homogeneously (Chu and Chan, 2004; Bin *et al*., 2006; Chang *et al*., 2006).

In this study a new method based on Mackey-Glass series method is proposed that can distribute pixels of secret image in cover image homogeneously. In fact chaotic feature of Mackey-Glass series is used to determine each pixel of secret image position in cover image. In the experimental result section, stability of this method against common attacks is represented.

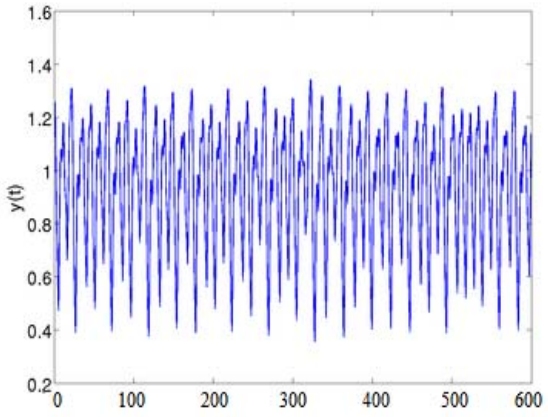


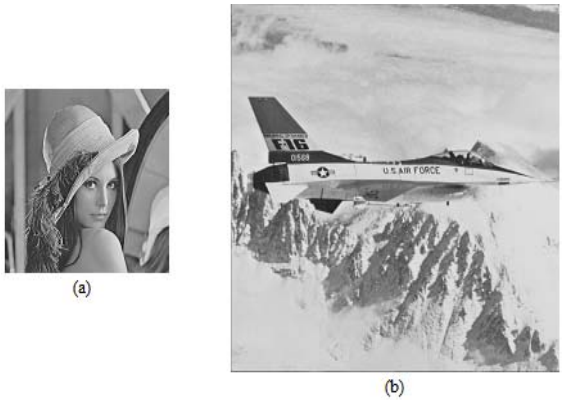
Fig. 1: Dynamics in the mackey-glass equation, Eq. (1), for $\tau > 17$

The rest of the study is organized as follows. First Mackey-Glass series will be introduced, then propose method is explained. Experimental results and conclusion are described finally.

Mackey-glass series: The Mackey-Glass is one of the most famous series that has been successfully used in different problems such as weather forecasting. The Equation of this series is described as follow:

$$x(t) = \frac{0.2x(t-\tau)}{1+x^{10}(t-\tau)} - 0.1x(t) \quad (1)$$

Corresponding Author: Rasul Enayatifar, Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, Malaysia



(a) (b)

Fig. 2: a) Secret image, b) cover image

Though Mackey-Glass is behaving similar to noise, it has a certain value. It means that it can be reproduced having the initial value and the corresponding function. Another advantage of this method is its high sensitivity to the initial value. A small variation in the initial value of the function causes a great change in the result of the function.

It has been proven that Mackey-Glass series has a chaotic behavior for $\tau > 17$. The value of this function for $\tau > 17$ is demonstrated in Fig. 1.

THE PROPOSED METHODOLOGY

Overall explain: The grey level of every pixel of secret image (Fig. 2a) is converted to binary mode and Mackey-Glass series is used to determine the position of every bit of this cover image (Fig. 2b). Three low value bit of a pixel chosen from the cover image is used for hiding a pixel of secret image.

The detail description: For determining the initial value of the Mackey-Glass series, a 80-bit key is implemented. This key is described as Ascii form as follows:

$$K = K_0, K_1, \ldots\ldots, K_9 \ (Ascii) \quad (2)$$

K_i is representing a 8-bit block of the mentioned key. The key is converted to binary form using the Eq. (3):

$$K_{i=0,j=1,\ldots,8}, K_{i=1,j=1,\ldots,8}, \ldots, K_{i=9,j=1,\ldots,8} \quad (3)$$

where,

K_{ij} = The j^{th} bit of the i^{th} block of the key

The initial value is calculated by Eq. (4):

$$X_0 = \frac{K_{0,1}{}^9 + K_{1,1}{}^8 + K_{2,1}{}^7 + \cdots + K_{9,1}{}^0}{2^{10}} \quad (4)$$

where, $X_0 \in (0,1)$

As it can be seen in Fig. 1 the variation of the Mackey-Glass is in the range of (0.4, 1.4) and the maximum variation of this signal is in the range of (0.6-1.2) which is used in the current study.

Step 1: The series that is shown in formula 5 obtained after converting a pixel of secret image to binary mode:

$$B = B_7, B_6, B_5, B_4, B_3, B_2, B_1, B_0 (Binary) \quad (5)$$

All the pixels of the secret image are converted to binary code and arranged as series.

Step 2: According to the Eq. (1) and X_0 a new value is created for the Mackey-Glass.

Restriction: If the created value is not in the prescribed range, a new value is recreated.

Step 3: In this stage, a pixel from the cover image is selected for hiding the bits of the pixels of the secret image using the Mackey-Glass series. The Eq. (6) and (7) are used to determine the position of this pixel:

$$R_{Cover_{Image}} = (X_i - Mackey_{min}) \times \frac{R_L}{Mackey_{min}} \quad (6)$$

$$C_{Cover_{Image}} = (X_i - Mackey_{min}) \times \frac{C_L}{Mackey_{min}} \quad (7)$$

where,

$Mackey_{min} = 0.6$

X_i = The value from the Mackey-Glass series

R_{Cover_Image} = The row position of the pixel in the cover image

C_{Cover_Image} = Column position of the pixel in the cover image

R_L = The number of rows of the cover image

C_L = Columns of the cover image

Step 4: In this stage, 3 bits of the secret image are replaced in 3 low-value bits of the cover image with the row and column positions of R_{Cover_Image} and C_{Cover_Image} respectively which are obtained in stage 2.

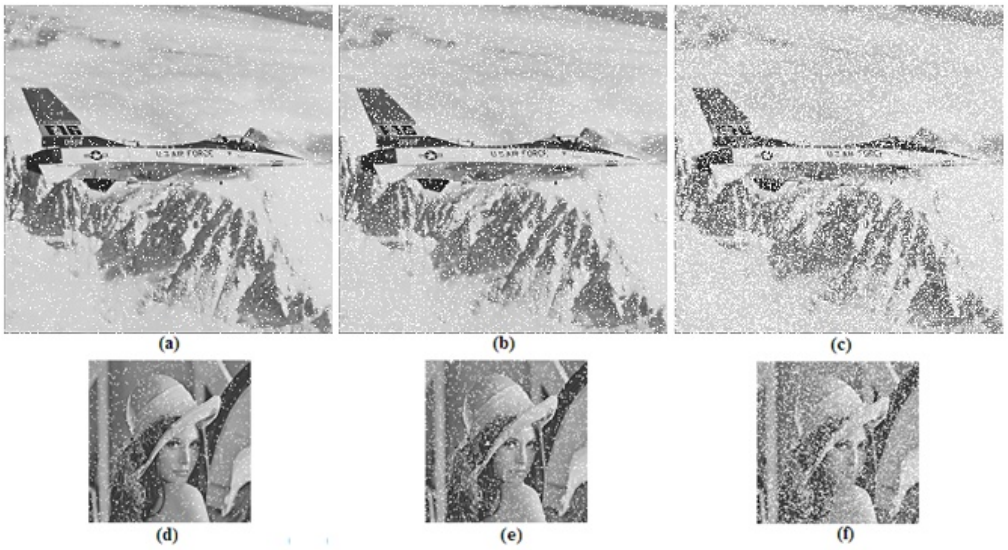


Fig. 3: (a, b, c) Stego-image after 5, 10, 30%, respectively noise, (d, e, f) secret image after extracing from stego-image

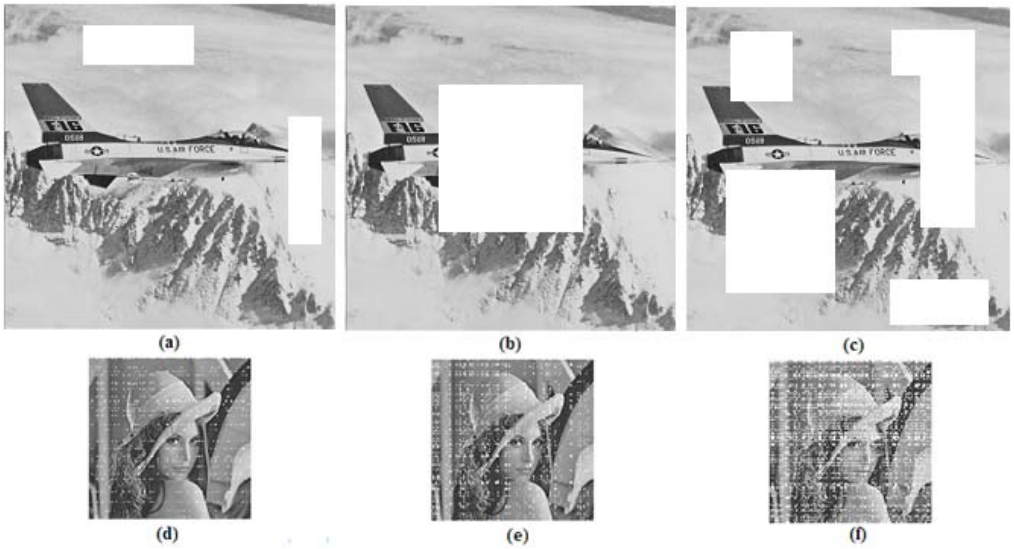


Fig. 4: (a, b, c) Stego-image after 5, 10, 30%, respectively cutting, (d, e, f) secret image after extracting from stego-image

Step 5: The stage 2 to 4 is carried out for all the pixels of the secret image considering the below restriction.

Restriction: If in the stage 3 a pixel is selected which had been chosen already, it should be neglected.

EXPERIMENTAL RESULTS

The proposed method is evaluated in this section through some experiments to see its stability against common attacks.

The stability against cover image corruption: Furthermore, common damages of stego-image are investigated using this method. Three common attacks to stego-image are corrupted image, cutting image and noisy image.

Figure 3 is used to examine the stability of proposed method whereas Fig. 3a. Namely Airplane is the secret image (128*128) and Fig. 3b is cover image (256*256).

Figure 3, 4 and 5a, b, c are the resulting images of hiding Fig. 3a and 3b. With the proposed method and applying 5, 10, 30% noise, 5, 10, 30% cutting and 5, 10,

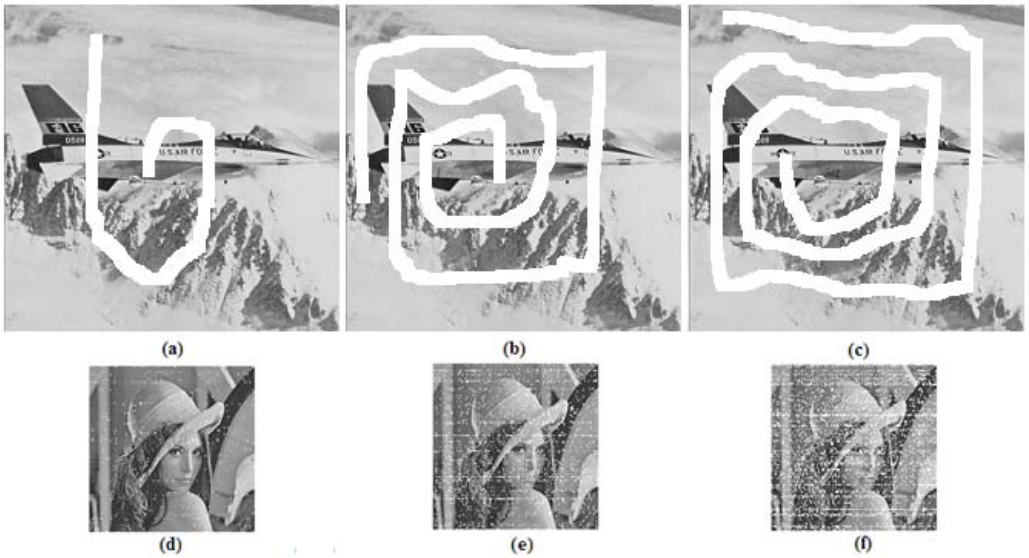


Fig. 5: (a, b, c) Stego-image after 5, 10, 30%, respectively corrupted, (d, e, f) secret image after extracting from stego-image

Table 1: Compare PSNR of other methods with proposed method

Secret image	Sheng *et al*. (2005)	Bin *et al*. (2006)	Chang and Huang (2001)	Proposed method
Airplane	39.36	41.86	44.14	44.32
House	41.64	41.88	41.93	43.91
Peppers	37.66	41.87	44.12	44.08
Boat	38.79	41.87	43.76	44.89

30% corruption, respectively. Figure 3d, e, f, 4d, e, f and 5d, e, f depict the resulting image of extracting the secret image from the cover image. In the entire resulting images Airplane image can be distinguished vividly. In all the mentioned attacks even in the most powerful one, just some minor details of the original image has been damaged which does not affect the recognition of the secret image. The main reason of this stability is the uniform distribution of the secret image's pixels in the cover image.

Peak Signal to Noise Ratio (PSNR): PSNR is used to scale the quality of Stego-image (Anderson and Petitcolas, 1998; Sheng *et al*., 2005). PSNR can be explained as follows:

$$PSNR = 10 * \log_{10}\left(\frac{255^2}{\frac{1}{W * H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(O_{ij} - D_{ij}\right)^2}\right) \quad (8)$$

In above Equation O_{ij} and D_{ij} denote the gray level of pixels of main image and Stego-Image respectively. H and W are height and width of the images.

To determine PSNR of the proposed method, four images namely Peppers, Lena, Boat and Woman are used as the covering image with (256*256) while Airplane, Tree and House are the secret images with (128*128). The results are demonstrated in Fig. 6.

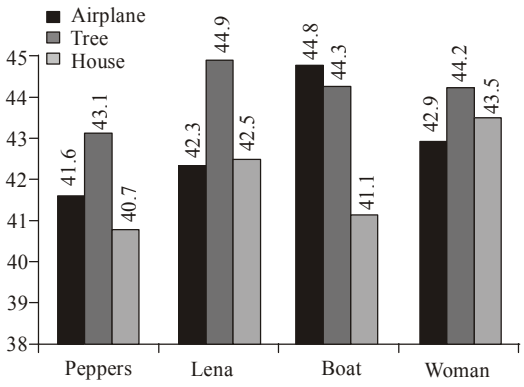


Fig. 6: PSNR for proposed method

To compare the PSNR of the proposed method with other methods (Bender *et al*., 1996; Wu *et al*., 2004; Yu *et al*., 2007), four images namely, Airplane, House, Peppers and Boat with dimension of (256*256) are used as the secret image. Lena image with dimension of (512*512) is used as the cover image. As it is seen in Table 1, the proposed method has completely better results comparing to the results of (Sheng *et al*., 2005; Bin *et al*., 2006) and better results than (Cheng and Huang, 2001) in most cases.

CONCLUSION

In this study a new method for Steganography is proposed. The main idea of this study is determining the position of the secret image pixels by using Mackey-Glass series. The main advantage of this method is the homogenous distribution of the secret image pixels in the cover image pixels. The inscription of every bits of the secret image with a bit from the key, before hiding the image, increases the security of the method.

As it was demonstrated in the result section, the above mentioned features cause the stability of the proposed result against common attacks to increase. The high amount of PSNR, approximately 45, is another proof of the efficiency of the proposed method.

ACKNOWLEDGMENT

This study was supported by the Research Center of College of Computer and Information Sciences, King Saud University. The authors are grateful for this support.

REFERENCES

Anderson, R.J. and F.A.P. Petitcolas, 1998. On the limits of steganography. IEEE J. Sel. Areas Commun., 16(4): 474-481.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35(3.5): 313-316.

Bin, L., L. Zhitang and T. Hao, 2006. An image encryption method based on bit plane hiding technology. Wuhan Univ. J. Natur. Sci., 11(5): 1283-1286.

Chan, C.K. and L.M. Chen, 2004. Hiding data in images by simple LSB substitution. Pattern Recogn., 37(3): 469-474.

Chang, C.C., C.S. Chan and Y.H. Fan, 2006. Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels. Pattern Recogn., 39(6): 1155-1167.

Cheng, Q. and T.S. Huang, 2001. An additive approach to transformdomain information hiding and optimum detection structure. IEEE Trans. Multimedia., 3(3): 273-284.

Chu, Y. P. and Y. K. Chan, 2004. Image hiding based on a hybrid technique of vq compression and discrete wavelet transformation. International Computer Symposium, Taipei, Taiwan, pp: 313-317.

Kwok, H.S. and W.K.S. Tang, 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Soliton. Fract., 32(4): 1518-1529.

Lin, I.C., Y.B. Lin and C.M. Wang, 2009. Hiding data in spatial domain images with distortion tolerance. Comput. Stand. Inter., 31(2): 458-464.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information Hidinga Survey. Pennsylvania State University, United States.

Sheng, L.N., G. Dong-Hui, W. Bo-Xi and G. Parr, 2005. A new images hiding scheme based on chaotic sequences. Wuhan Univer. J. Natur. Sci., 10(1): 303-306.

Wang, R.Z., C.F. Lin and J.C. Lin, 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn., 34(3): 671-683.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn., 24(9-10): 1613-1626.

Wu, Y.S., C.C. Thien and J.C. Lin, 2004. Sharing and hiding secret images with size constraint. Pattern Recogn., 37(7): 1377-1385.

Yu, Y.H., C.C. Chang and I.C. Lin, 2007. A new steganographic method for color and grayscale image hiding. Comput. Vision Image Und., 107(3): 183-194.