Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 10, October 2018, pg.25 – 32

Image Steganography using K-LSB Embedding with Edge Detection and Chaotic Map

Karrar Abdalluh Mohammed

Department of Computer Sciences, College of Education for Girls, Kufa University, Iraq

karrara.habeeban@uokufa.edu.iq

Abstract: Steganography is the science of embedding secret data inside data so they can be sent to destination security. Image steganography is the most popular type of carrier to hold information. Many algorithms have been proposed to hide information into digital images; the least significant bit algorithm (LSB) is one of these algorithms that is widely used in steganography. In this paper, we introduced propose steganography method by using edge detection of 6 bits in the image by edge detection and chaotic map. In work, we use 1-LSB or 2-LSB embedding, it depends on the threshold for edge detection image. We use locations not serialized of the pixel to embedding information rely on tent map.

Keywords: image steganography, edge detection, LSB, chaotic map, Correlation Coefficient, SSIM, and histogram.

I. INTRODUCTION

The transmission of a large amount of data over network communications requires security to protect data. Therefore, steganography has an important role in secret communication. Steganographic processes can be classified into two categories: spatial and transform domains approaches [1]. Used digital images for steganography [2]; Image steganography techniques require two files: cover image, and the data (message) to be secretly hidden [3]. Steganography based information security is essential for confidential data transfer. There are three basic requirements in the field of digital steganography. The first requirement is capacity i.e. the number of secret bits that are to be embedded per cover pixel. Higher the capacity more data can be hidden in cover media. The second requirement is robustness that prevents hidden sensitive information data from being attacked. The third requirement is imperceptibility, usually calculated by peak signal to noise ratio. Thus, the stego-media is considered good when the imperceptibility is high. When steganography is employed as a method to conceal the existence of secret information during data transmission and communication, imperceptibility becomes the most important requirement while robustness [4]. There exist various methods to conduct steganography. One of the oldest methods is Least Significant Bit (LSB) where redundant bits of cover images are replaced by the covert information bits, it embeds the bit in the spatial domain of the image and less efficient in which it causes obvious distortion [5].

II. SPATIAL DOMAIN TECHNIQUE

There are many versions of spatial steganography, the most widely known steganography algorithm is based on hiding the secret message in the LSBs (sequentially or randomly) of pixel values without introducing visual traces[6].

III. DISTORTION TECHNIQUES

Distortion techniques need to know of the original cover image in the decoding process. It checks for differences between the original cover image and the stego-image in order to restore the secret message [7].

IV. TYPICAL CHAOTIC SYSTEMS

Chaos exists widely in nature. During the research and development of chaos theory, researchers found a lot of chaotic dynamics models, and some of them are typical for the chaos theory and application research, including discrete-time chaotic maps, continuous-time chaotic systems. Discrete-time chaotic Map: meaning is that chaos is generated by a discrete map described by a nonlinear difference equation, which can usually be achieved by a software program or sampler[8].

V. TENT MAP

Tent map another commonly used discrete chaotic map. The chaotic sequence generated by the tent map has been widely applied in the field of chaotic spread spectrum communication, chaotic encryption system, chaotic optimum algorithm, and so on.

Its equation is [9]:

$$x_{n+1} = \begin{cases} rx_n & x_n \in [0, 0.5) \\ r(1 - x_n) & , x_n \in [0.5, 1] \end{cases}$$

Where the system parameter $0 \leq r \leq 2$ and the variable $x_n \in \ (0,1)$.

VI. PROPOSED METHOD OF STEGANOGRAPHY

In the proposed method, we apply the edge detection on the image. We used sex bits to find the edge and leave the two least significant bits. We find the threshold of the edge detection image and compare the pixels of the cover image with the threshold if it is greater than the threshold then we two-bit embedding in the original image or if the pixels less than the threshold then we one-bit embedding in the original image, we used a random pixel to hidden information relies on tent map.

```
Algorithm: Embedding Information in K-LSB of Image
Input: color or gray image and information (message).
Output: Steganography image.
Step 1: Convert the message into binary.
Step 2: Split six bits from the original image and leave two least
        significant bits.
Step 3: Apply edge detection on six bits of the image.
Step 4: Compute threshold of edge detection image , where
        th=max(edge image)+min(edge image)/2 .
Step 5: Comparison pixels of edge detection image with the threshold
         if it is greater than the threshold then we used two bits for
         hidden information else we used one bit for hidden information.
Step 6: Compute tent map value according to equation (1).
Step 7: Ascending sorting of the tent map value and store index this value.
Step 8: Select random pixels from the original image to embedding bits
        according to the index of tent map value.
Step 9: Compute PSNR and MSE for Steganography and the original
        image.
Step 10: Apply similarity measure between Steganography and the
          original image and find the histogram.
```

VII. PERFORMANCE MEASUREMENT PARAMETERA

1. Mean Square Error(MSE): it represents the quality of the stego image. Its equation is[10]:

$$\text{MSE} = \sum_{i=1}^{N} \sum_{j=1}^{M} (S(i,j) - I(i,j))^2 \Big/ M * N$$

2. Peak Signal-to-Noise Ratio (PSNR): is the ratio of the maximum signal to noise in the stego image. PSNR value if large indicates the better quality of the image and lead to less distortion. Its equation is[10]:

$$\mathrm{PSNR} = 10 \log 10 \,(\mathrm{MAX}^{2} / \mathrm{MSE})$$

3. Correlation Coefficient: is give the 2-D correlation coefficient between image A and B. Its equation:

$$R = \frac{\sum_N \sum_M (A - \bar{A})(B - \bar{B})}{\sqrt{(\sum_N \sum_M (A - \bar{A})^2)(\sum_N \sum_M (B - \bar{B})^2)}}$$

Where $\bar{A}$ and $\bar{B}$ present mean of A and mean of B.

4. Structural Similarity Index (SSIM): it is a statistical measure and based on the computation of three terms, namely the luminance term, the contrast term and the structural term. It's equation[11]:

$$\mathrm{SSIM}(A, B) = \frac{(2\mu_A \mu_B + C_1)(2\sigma_{AB} + C_2)}{(\mu_A^2 + \mu_B^2 + C_1)(\sigma_A^2 + \sigma_B^2 + C_2)}$$

Where μ_A , μ_B is means of the images A and B, σ_A , $\sigma_B$is Standard Deviation of the Images A and B , σ_{AB} cross-covariance for images A and B, and C_1, C_2 is constant.

VIII. EXPERIMENTAL ANALYSIS AND RESULTS

This section introduces the experiment conducted to image steganography by using Sobel edge detection and K-LSB method. This method Apply on color or gray images. Figure 1: explain the edge detection of original images. Figure 2: explain the original, stego image and histograms of images; histogram is the number of the frequency of per color. We used set of measure explain in table 1: to give similarity images.

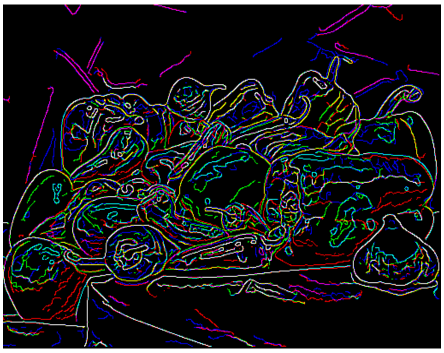
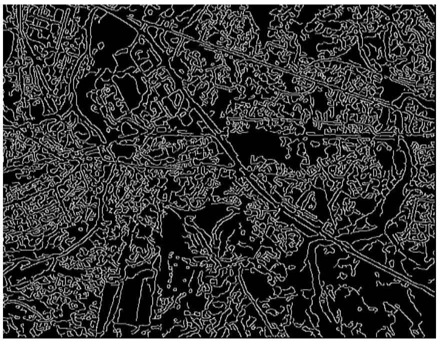
Edge detection of Peppers image	Edge detection of concordorthophoto
	

Figure 1: show edge detection images of original images.

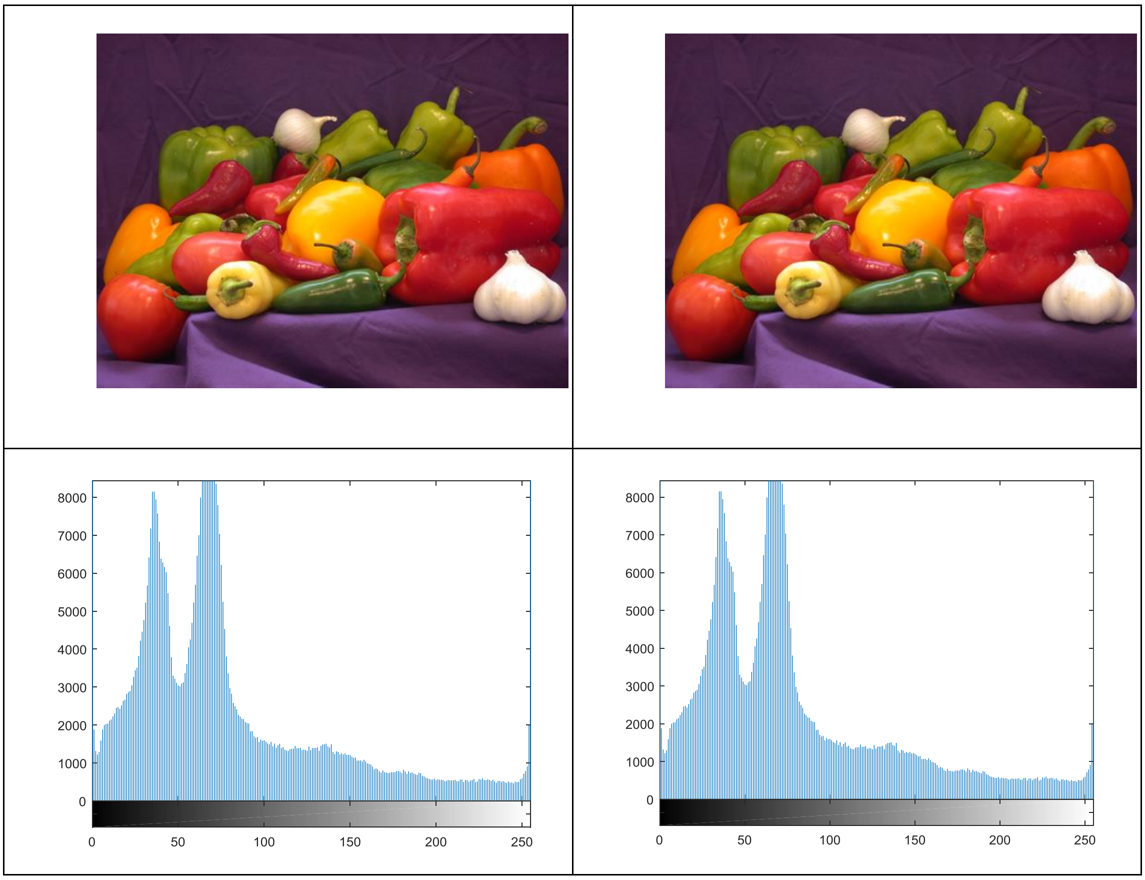


Figure 2: show original and stego images and histogram of images.

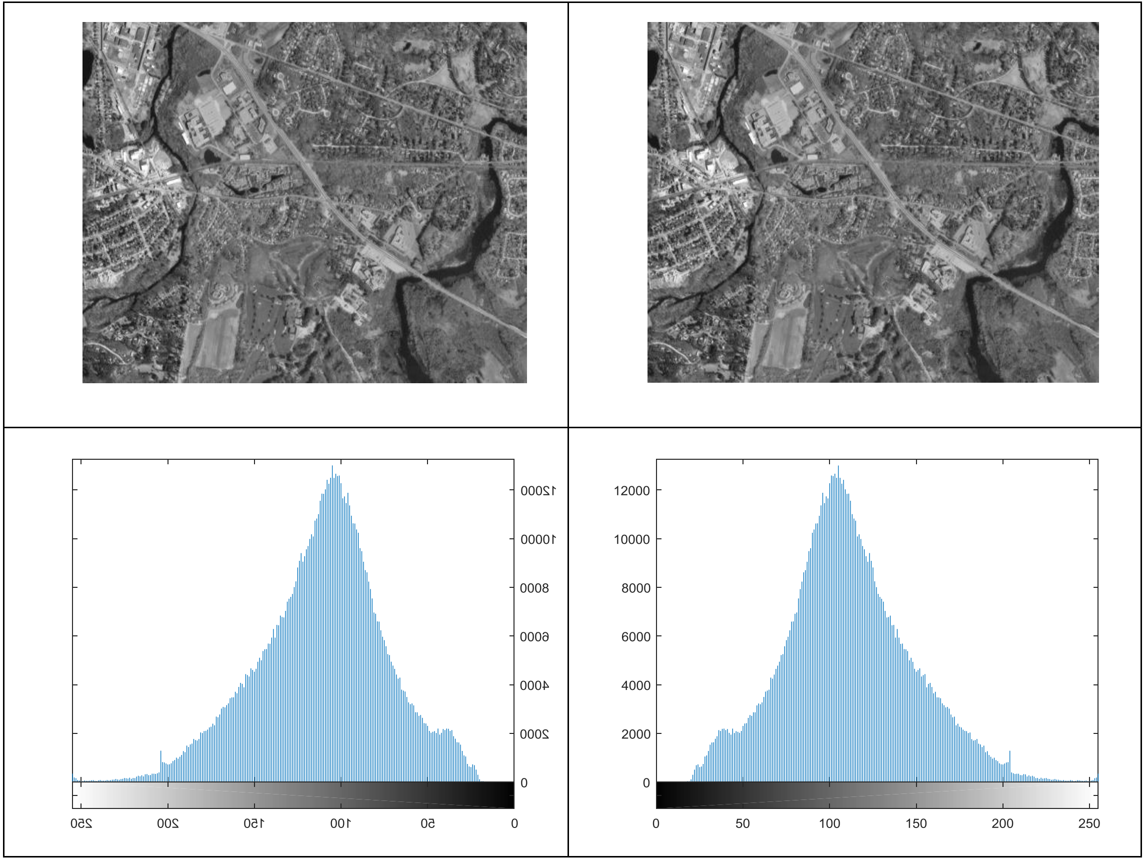


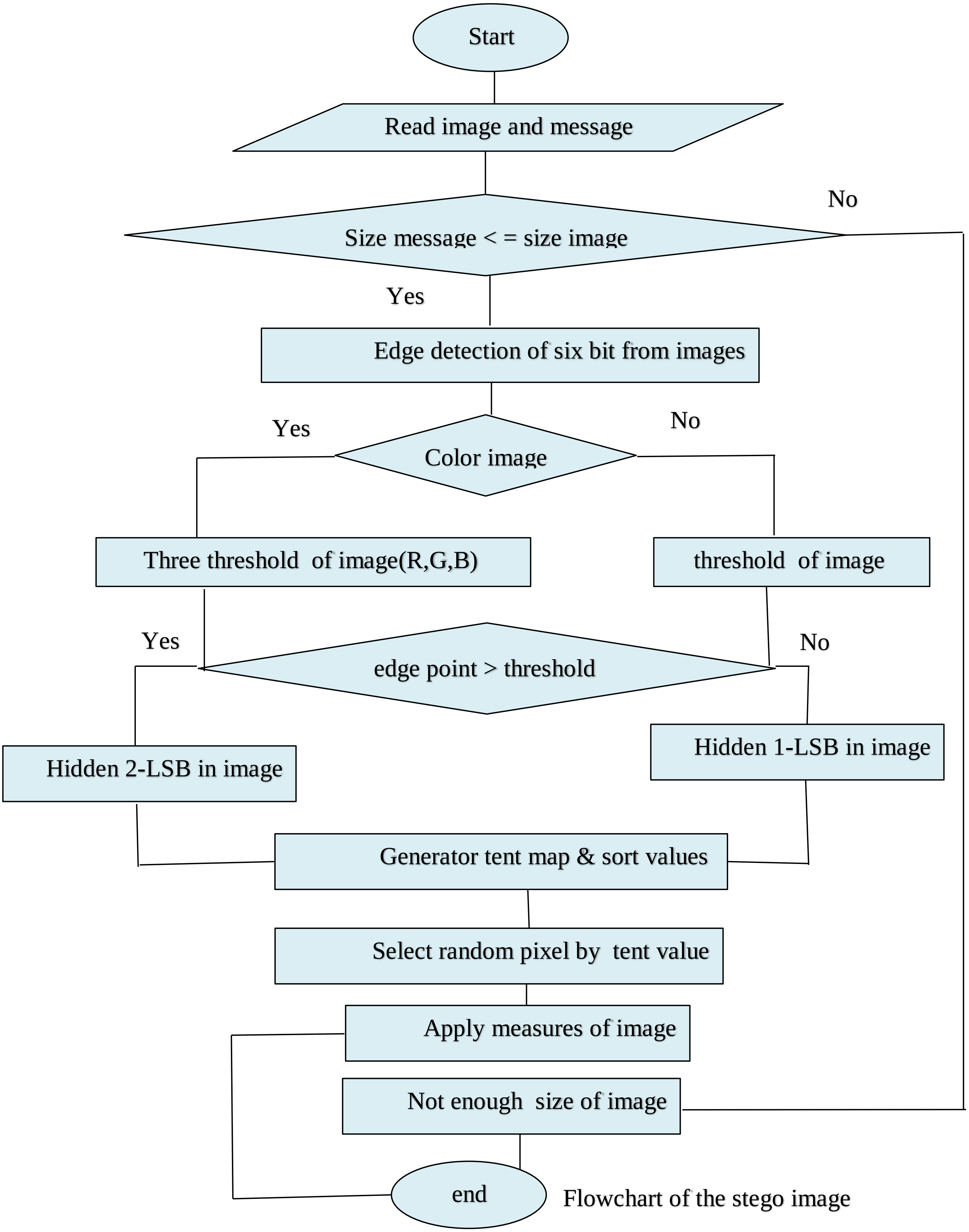
Figure 3: show original and stego images and histogram of images.

Table 1: show some the measures of similarity images.

Size of secret	Size of cover	PSNR	MSR	SSIM	correlation
63	384x512	91.8586	4.2386e-05	1.0000	1.0000
259	536x586	86.9736	1.3053e-04	1.0000	1.0000
245	600x903	89.2024	7.8135e-05	1.0000	1.0000
105	684x912	94.0401	2.5649e-05	1.0000	1.0000
364	684x912	88.1109	1.0046e-04	1.0000	1.0000

IX. CONCLUSION

The proposed method applies the edge detection technique on the cover image and chaotic map. We used edge detection technique such that Sobel filter, it is used to give a number of bits used in embedding. Also, we used tent map, it gives the location of pixels which used to embedding bits. The experiments and result conducted to confirm that stego-image embeds the two secret bits if pixel present edges or embeds the one secret bit if pixel, not the present edge. We used set of the measures to find ratio of noise between images.



Flowchart of the stego image

References

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods”, Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[2] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

[3] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 2073-4212, 2011.

[4] N. H. A. Mahdi, A. Yahya R. B. Ahmad, and O. M. Al-Qershib, "Secured and robust information hiding scheme", Procedia Engineering, vol. 53, pp. 463-471, 2013.

[5] Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." Computer 31, no. 2 (1998): 26-34.

[6] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). “Image steganography: Concepts and practice.” WSPC/Lecture Notes Series: 9in x 6in, [On line], April 2004, pp. 1-49.

[7] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. “Data masking: a secure-covert channel paradigm”, in IEEE Workshop on Multimedia Signal Processing, 2002, pp. 339-342.

[8] Kehui Sun, “Chaotic secure communication: principles and technologies,” Berlin Boston De Gruyter, 2016.

[9] S. Li, G. Chen, and X. etc., "On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps," International Journal of Bifurcation and Chaos, 2005.

[10] C. Science and B. Bridgeport, “A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes”, 2015.

[11] Zhou, W., A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. "Image Qualifty Assessment: From Error Visibility to Structural Similarity." *IEEE Transactions on Image Processing*. Vol. 13, Issue 4, April 2004, pp. 600–612.