Key Dependent Image Steganography Using Edge Detection

Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad
Department of Computer Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi-110025, INDIA
{shahzad5alam, vipin.kumar, was.jmi}@gmail.com

***Abstract*–Steganography is the science of invisible communication. It aims at hiding sensitive information in digital media in a way to conceal the existence of information. In this paper, we aimed to propose an improved secured image steganography scheme recently given by Chen *et al.* The improved scheme is secret key based random LSB substitution. It also takes the advantages of edge detection based pixel dependency to achieve high embedding data capacity. The experiment results show that the proposed scheme also achieves high embedding capacity. High scores of PSNR reveal that there is no noticeable difference between cover image and stego-image. Moreover, the proposed improved scheme is robust and can protect effectively the embedded message from being steganalysis due to the inception of randomness, pixel dependency and key dependency.**

Keywords*—*Steganography, edge detection, security, chaotic systems, imperceptibility.

I. INTRODUCTION

Steganography technologies are very significant for the transmission of concealed sensitive information over the attack prone networks. Digital steganography research is primarily driven by the lack of strength in cryptographic systems and the desire to have complete secrecy in an open-systems environment. Almost any digital plain-text data whether it be texts, images or any other media can be hidden in a digital cover media. Due to the continued growth and usage of strong image based graphics in communication, the research being put into image based steganography, this field is continued to grow at a very rapid pace. When dealing with digital images for use in steganography [4], gray-scale and color pixel image files are typically used. Image steganography techniques require two files: cover image, and the data (message) to be secretly hidden. The one major merit of digital images over videos is their size, makes their more frequently utilization than the much large and redundant sized digital videos when communicated over low bandwidth networks [9].

The standard and concept of ‘‘What You See Is What You Get’’, which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a stenographer as it does not always hold true. Image can be more than that what we see with our human visual system (HVS). 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 [7] and possibly capacity can be sacrificed [3]. A strong and efficient steganographic scheme carefully regards all the three requirements effectively.

LSB substitution steganography is one of the most commonly and extensively used method, where the least significant bits of each pixel are replaced with bits of secret message until message finishes. Although, it is a simple techniques but the probability of detecting the hidden data is high which threats its security. To tackle this problem, a simple and effective method employing the concept of hybrid edge detection technique for LSB substitution is proposed by Chen *et al.* [1]. Their scheme is key independent and number of embedded bits depends on the edges of the cover image pixels. In this work, a key dependent random LSB substitution based image steganography scheme with edge detection technique is proposed. The random LSB substitution is based on secret key and also on pixel values to increase robustness. The experimental results show that the improved scheme inherits the merits of Chen *et al.* scheme. In addition, the improved edge detection based steganography scheme is effective and robust against the unauthorized steganalysis.

II. PRELIMINARIES

To develop a new key dependent LSB steganography scheme using edge detection technique that can resist steganalysis, we modify the Chen et al scheme. The modification involves the inception of key dependency and randomness. In each cover image pixel, the modified mechanism allows selecting random number of LSBs based on secret key which are used to replace secret message. The bits to be embedded are first encrypted with the equal number of most significant bits (MSBs) of the same pixel.

978-1-4799-4910-6/14 $31.00 © 2014 IEEE
DOI 10.1109/ACCT.2014.72

This modification not only helps in improving imperceptibility but also focuses randomness, pixels dependency and key dependency to achieve robustness along with high embedding payload. The chaotic logistic map employed for random sequence generation and canny edge detector to extract the edges of cover image are described as follows.

A. *Chaotic 1D Logistic Map*

The one-dimensional Logistic map proposed by R. M. May [10] is one of the simplest nonlinear chaotic discrete systems that exhibit chaotic behavior; it is governed by the following equation.

$$w(n+1)=\lambda w(n)(1- w(n)) \quad (1)$$

Where $w(0)$ is initial condition, λ is the system parameter and n is the number of iterations. The research shows that the map is chaotic for $3.57 < \lambda < 4$ and $w(n+1) \in (0, 1)$ for all n.

B. *Canny Edge Detection*

An edge is characterized by significant dissimilarity in gray levels being used to indicate boundary between two regions in an image. Edge detection is a fundamental tool in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extraction. Canny edge detector is considered the most rigorously defined and widely used operator. The Canny edge operator has three characteristics [2]: (1) no important edges should be missed, and there should be no false edges (2) the distance between the actual and located position of the edge should be minimal and (3) there is only one response to a single edge.

III. PROPOSED METHOD

The proposed scheme is an improvement over the scheme suggested by Chen *et al.* [1]. Our scheme not only inherits the high data embedding capacity feature of the existing scheme and good imperceptibility of stego-image but also focus on robustness of the scheme against steganalysis by statistical analysis which was not considered by Chen *et al.* [1]. The scheme uses secret key random number generation using chaotic logistic map for random LSB substitution based on cover image pixels edges. The initial value $w(0)$, used in chaotic formula, acts as secret key for random selection of message bits amount to be embedded in a pixel. The robustness is achieved by encrypting the message bits with the pixel's most significant bits.

The steps of the proposed methodology are as follows:

Step 1: Apply canny edge detection to obtain edge image B from gray scale image G.

Step 2: Divide the gray scale image into set of blocks, each block containing n-pixels. Here we use P1 pixel to store status of other pixel. The status of each pixel Pi, is defined as '1' if it is a edge pixel. Otherwise is '0' if non-edge pixel. The status of pixels from P2 to Pn is stored inside P1 by LSBs substitution operation. To preserve the quality of pixel P1 as well as to increase the embedding payload, based on the experimental results, we suggest assigning the values of n as 3, 4.

Step 3: For a non edge pixel in a block we embed 'x' bits of message XOR with 'x' MSBs of the pixel by LSB substitution. To maintain the quality of the stego image, the value of x here is 1 or 2.

Step 4: For an edge pixel in a block, we embed 'y' bits of message XOR with 'y' MSBs of the pixel by LSB substitution. The value of 'y' is generated randomly for each pixel using chaotic map. To maintain the quality of stego image, the value of y is generated between 1 and 4.

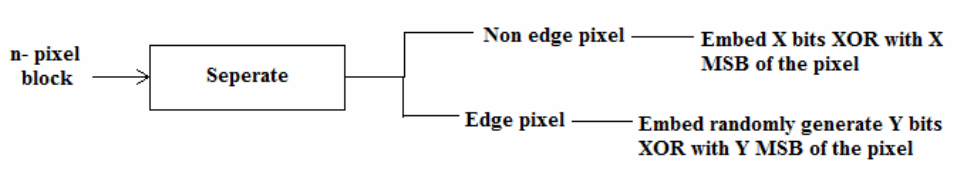


Figure 1. Classification and embedding of pixels

For example, let us consider an image A having four pixel as {[1 0 1 0 1 0 1 0], [10 0 0 0 0 0 0], [1 1 1 1 1 1 0 0], [0 0 0 0 1 1 1 1]} corresponding to P1, P2, P3 and P4 with the secret message M = '0 1 1 0 1 0 1 0'. The image A is considered to be a four-pixel block. Let us assume that, based on the canny edge detector; we determine that P2 and P4 are edge pixels. Obviously, the status of P2, P3 and P4 is '101'. Replace 3 LSBs in pixel P1 with '101'. Thus, the pixel P1 receives the new value of [1 0 1 0 1 1 0 1] and becomes pixel P1'.

Further, we assume that the value of parameter 'x' is 1 and that of 'y' generated randomly by chaotic map is 4 for pixel P2. Now, we XOR the 'y' bits of message with the 'y' MSBs of the pixel2 i.e. 'z'= b8b7b6b5 XOR m1m2m3m4 as shown in fig 1. Herein, we replace 'y' LSBs in pixel P2 with the secret 'z' bits. Also, we replace one LSB in pixel3 with 'z'=b8XORm1. Similarly, we replace new randomly generated 'y' LSBs in pixel P4 with secret 'z' bits, where 'z' in general represent 'y MSBs of a pixel XOR with y bits of

message'. For pixel P4 let the value of 'y' be 3. The new values of pixels P2, P3, P4 are {[1 0 0 0 1 1 1 0], [1 1 1 1 1 1 0 0], [0 0 0 0 1 0 1 0]}.

In the extraction process the secret key, the *w(0)* of chaotic map, plays a very important role. If the key used during embedding and extraction are same then only we can get the same value of embedded bits in each edge pixels. Otherwise, the message cannot be extracted correctly. This is where the robustness of our algorithm lies. The steps of extraction process are as follows.

Step 1: Similar to the dividing operation presented in the previous procedure. Divide the stego image into n-pixels block.

Step 2: Based on the (n - 1) LSBs in pixel P1', we obtain the status of the remaining pixels from P2' to Pn'. From this status value, we can identify two categories corresponding to the non-edge pixel category and the edge pixels category.

Step 3: From non-edge pixel, based on the value of 'x' used in embedding process, extract the 'x' LSBs of the pixel and XOR it with the 'x' MSBs of the pixel to obtain the bits of original message.

Step 4: From edge pixel, based on the value of 'y' generated randomly, extract 'y' LSBs of the pixel and XOR it with the 'y' MSBs of the pixel to achieve part of message. The value of 'y' generated will be same for a pixel in embedding & extraction if the secret key i.e. initial value *w(0)* of chaotic map is same on sender & receiver side.

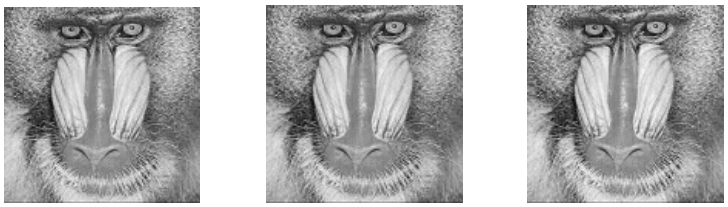
As an example, consider a stego-image A' having four pixels as {[1 0 1 0 1 1 0 1], [1 0 0 0 1 1 1 0], [1 1 1 1 1 1 0 0], [0 0 0 0 1 0 1 0]} corresponding to four pixels P1', P2', P3' and P4'. Obtain (n -1) = 3 LSBs in the first pixel, we get three bits as '1 0 1'. Thus the second and the fourth pixels are edge pixels and, the third pixel is a non- edge pixel. Based on the embedding procedure, we will extract four LSBs and MSBs from pixel P2', and XOR them. Next, we will take three LSBs from P4' and three MSBs of P4', and XOR them. Next we will extract one LSB from P3' pixel and first MSB of P3' pixel, and finally XOR them. The extracted bits from the pixel P2' are '0110'. The extracted bit from the pixel P3' is '1'. The extracted bits from the pixel P4' are '010'. Be appending these extracted bits, we obtain the secret message as M='0 1 1 0 1 0 1 0'.

IV. EXPERIMENTAL RESULTS

The scheme proposed in [1] focuses on achieving high embedding capacity & good quality stego image but on the cost of robustness. Our scheme not only focuses on high capacity & high imperceptibility but also take robustness into consideration. The robustness is provided in two ways in our scheme, (a) using random LSBs substitution based on secret key, (b) encrypting the n-bits of message with n- MSBs of the pixel. The strength of our proposed scheme lies in the secret key which makes the scheme to be robust against steganalysis. To conduct our experiment we used 128×128 gray scale images. The experimental results, to demonstrate the performance of our scheme, are shown in Fig. 2-3 and Table I for *Lena* and *Baboon* images. The stego-image quality is considered from the viewpoint of PSNR. We also compare the quality of stego image to that of cover image as seen by human visual system. The PSNR measures are higher than 40 dB which demonstrates the satisfactory performance of the proposed improved key dependent edge based image steganography algorithm.

(a) (b) (c)

Figure 2. Lena images (a) original image (b) stego-image with 2037 embedded bits (c) stego-image with 11074 embedded bits



(a) (b) (c)

Figure 3. Baboon images (a) original baboon image (b) stego-image with 4886 embedded bits (c) stego-image with 11074 embedded bits

TABLE I. PSNR OF STEGO-IMAGES WITH DIFFERENT EMBEDDING CAPACITY

Bits embedded in *Lena* image	2037	4302	4998	7167	8365	9912	11074	12929
PSNR (in dB)	41.000	40.939	40.931	40.910	40.879	40.835	40.822	40.795
Bits embedded in *Baboon* image	1400	2912	4886	6944	8022	9772	11074	12012
PSNR (in dB)	40.915	40.867	40.754	40.728	40.662	40.611	40.571	40.522

V. CONCLUSION

In this paper, we have proposed an improved key dependant image steganography scheme which is based on random LSB steganography mechanism and employ a canny edge detector. The canny edge detector assists in generating a better quality stego image. Experimental results confirm that the proposed scheme is successful in achieving high payload as well as a good quality stego image. The contents of the message have been recovered successfully by the extraction process. Moreover, due to random and encrypted LSB steganography the scheme is robust to attack and message cannot be recovered without knowing the key.

REFERENCES

[1] W. J. Chen, C. C. Chang, and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, vol. 37, no. 4, pp 3292-3301, 2010.

[2] Z. Nanning, "Computer visualization and pattern recognition", National Defense Industry Press, vol. 2, pp. 1069–1074, 1998.

[3] K. Wang, Z. M. Lu, and Y. J. Hu, "A high capacity lossless data hiding scheme for JPEG images", The Journal of Systems and Software, vol. 86, no. 7, pp. 1965-1975, 2013.

[4] 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.

[5] D. L. Hostalot, and D. Megıas, "LSB matching steganalysis based on patterns of pixel differences and random embedding", Computers & Security, vol. 32, pp. 192-206, 2013.

[6] A. Kanso, and H. S. Own, "Steganographic algorithm based on chaotic map", Communication in Nonlinear Science and Numerical Simulations, vol. 17, no. 8, pp. 3287-3302, 2012.

[7] 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.

[8] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure and high capacity image steganography technique", Signal and Image Processing: An International Journal, vol. 4, no.1, 2013.

[9] 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.

[10] R. M. May, "Simple mathematical model with very complicated dynamics", Nature, vol. 261, pp. 459–467, 1967.