International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

ROI Based Steganography Method Using Two Bit LSB Replacement and Entropy Calculation

Harjeet Kaur, Dr. Amandeep Singh Sappal

Department of Electronics Engineering, Punjabi University, Patiala, Punjab, India

ABSTRACT

Different challenges in steganography are Imperceptibility, Robustness and Capacity. In this paper, all these points have been considered and a secure steganography method has been proposed to hide secret information. Self-embedding method has been adopted in which secret information has been taken from the Region of interest selected by a cropping tool. As MSB bits contain most of the information, only MSB bits has been embedded and rest of the LSB bits from the same chosen place can be used for embedding mechanism. Also two bit LSB replacement has been used for embedding data which is decided based on entropy information from a set of non-overlapping blocks of the input image. Maximum entropy has been chosen to select that block first which has maximum value among all. Entropy has been calculated only for MSB bits which results in same sorting sequence of blocks at the receiver side as well hence results in extraction of secret information in the same manner as embedding. XOR embedding has been implemented before embedding in order to secure the data. Proposed method has dual embedding capacity as two bit replacement has been used as compared to the existed method.

Keywords : Imperceptibility, Robustness, Steganography, Embedding, Entropy.

I. INTRODUCTION

Steganography deals with the art of hiding information with an interesting property of hiding the mere existence of the secret information. What makes steganography more preferable than cryptography is its extra layer of security provided by the non-detect ability of the presence of secret information. Cryptography is the practice of scrambling a message to an obscured form to prevent others from understanding it while steganography is the study of obscuring the message so that it cannot be seen [1]. Steganography requires two files – the cover/carrier file and the secret file. Various multimedia carriers like audio, video, text, image etc. can act as a cover media to carry the secret information. Also the secret can be of any type, which in most cases is converted into a bit stream. The resultant file after embedding can also be called as a stego-file. In image steganography the cover file will be an image and the secret may be plain text, cipher text (or another image).

Different challenges in steganography:

a) Imperceptibility
b) Robustness
c) Capacity.

Imperceptibility refers hiding data in such a way so that it cannot deviate the perceptibility of cover media.

Robustness of the secret data refers to preventing eavesdroppers from recovering the secret data until and unless they can able to sense the very existence of it [2].

Capacity, the third one means how much data can be embedded without hampering imperceptibility of cover media. Although these three are much related to each other but they should meet within the steganography without disturbing the other [3].

Most steganography methods uses a shared key to hide secret message and generate a stego[4] . To conceal the communication between two sides, stego should be statistically undetectable from the cover media. Increasing the size of the cover media after em-

bedding secret message, undetectability and the amount of distor- tion are three important points that should be consider in the pro- posed steganography methods because these points show the ca- pability of the algorithm in embedding process and diagnosis the histogram changes resistance against the histogram based attacks [5][6] .

II. LITERATURE SURVEY

Z. Y. Al-Omariet. al. (2017) proposed a new steganography approach for digital images in which the RGB coloring model was used. The efficiency of the proposed approach has been tested and evaluated.

ArefMiriet. al. (2017) chose the frequency space that is not constant according to the secret information and cover image, so the resemblance of secret information and cover image will be maximum. As a result, PSPNR of the cover image will be high after information injection. In this method an extra security layer is added to the algorithm, so the unauthorized receptor, willing to extract secret information, does not know to search information in which frequency space.

Xin Liao et. al. (2017) first investigate an adaptive strategy that synchronizes the modification directions for the same position of adjacent DCT blocks, and then the cost values are adjusted dynamically according to the modifications of inter-block neighbors in the embedding process. A novel medical JPEG image steganographic scheme is designed based on preserving the dependencies of inter-block DCT coefficients.

III. PROPOSED SYSTEM

Embedding Process

Step 1: Initially, read the image from the desired location, then crop the Region of interest need to be hide.
Step 2: Separate the Most Significant Bits and Least Significant Bits. So that MSB bits can be concatenated for embedding.
Step 3: Apply encryption process on concatenated data in order to increase security of data.
Step 4: Divide the image into non-overlapping blocks
Step 5: Evaluate the entropy of each block and sort the blocks according the entropy value
Step 6: Apply embedding procedure by taking two bits at a time from the secret data array and replace it with two LSBs bits of the block chosen for embedding
Step 7: After all bits are embedded recombine the blocks to make steganographed image.

Extraction process
Step 1: Receive the steganographed image and divide into non-overlapping blocks.
Step 2: As entropy of MSB bits will not change after embedding entropy has been calculated for each block using MSB bits only.
Step 3: Then sort the blocks according to maximum entropy first in decreasing order
Step 4: Extract information by taking only LSB bits.
Step 5: As the extracted bits are in encrypted form, apply reverse XOR operation to get decrypted data.
Step 6: Insert the extracted MSB bits back into the same location from which it was cropped first.
Step 7: Resulted image is the output image after extraction process.

Least-Significant Bit (LSB) Insertion [10]
It is the simplest steganographic algorithm [11]. Let us assume that x[i] □ x= {0,…., 2n-1} is a sequence of integers where n denotes the number of bits and x[i] refers to the pixel or intensity value at the ith pixel in an 8-bit grayscaleimage (n=8) or a quantized DCT coefficient in a JPEG file. Depending on the image format and the bit depth selected for representing the isolated values, each x[i] can be represented by n bits b[i,1],….,b[i,n],

$$x[i] = \sum_{k=1}^{n} b[i,k] * 2^{n-k} \qquad (1)$$

The series (b [i, 1],…….,b[i, n]) is the binary representation of x[i] in big-endian form. LSB embedding as its name suggests, works by replacing the LSBs of x[i] by all of the message bits m[i], obtaining in the behavior the stego image y[i].LSB embedding follow the class of steganographic algorithm that abide each message bit at one cover element. In other words, each bit is situated at an actual element. The embedding proceed by visiting individual cover elements and applying the embedding operation (flipping the LSB) if imminent, to relate the LSB with the message bit (Fig.1.).The message is inserted sequentially in pixels of an image. The embedding reaction of flipping the LSB can be written mathematically as:

$$LSBflip(x) = x + 1 - 2(x \bmod 2) \quad (2)$$

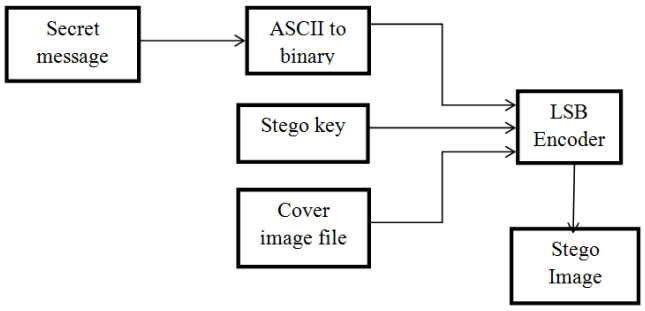

Figure 1: LSB Insertion Mechanism

Where x could be the light intensity at the ith pixel in an 8-bit grayscale image (n=8) or a quantized DCT coefficient in a JPEG file.

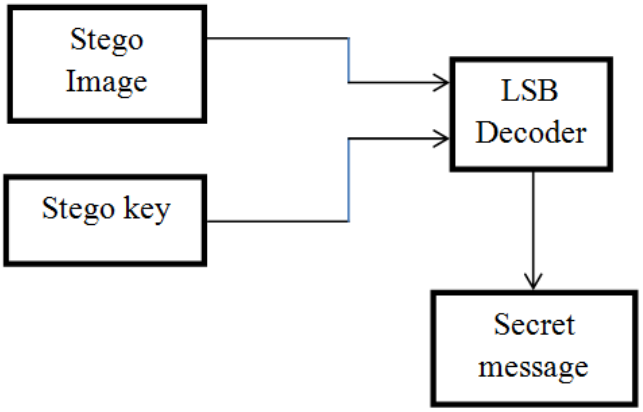

Figure 2: LSB Extraction Mechanism

IV. RESULTS AND DISCUSSION

The table 1 shows the MSE, PSNR (DB) and Embedding Capacity for Koala image

Table 1 : MSE, PSNR and Embedding Capacity for koala image

MSE	PSNR (DB)	Embedding Capacity
0.3366	52.89	1.22
0.3653	52.53	1.83
0.2621	53.97	5.17
0.3884	52.27	7.68
0.8465	48.88	16.82
1.1294	47.63	22.33
1.6764	45.92	33.30

Figure 3: shows the bar graph for MSE parameter. As seen above the MSE values increases along with increase in payload.

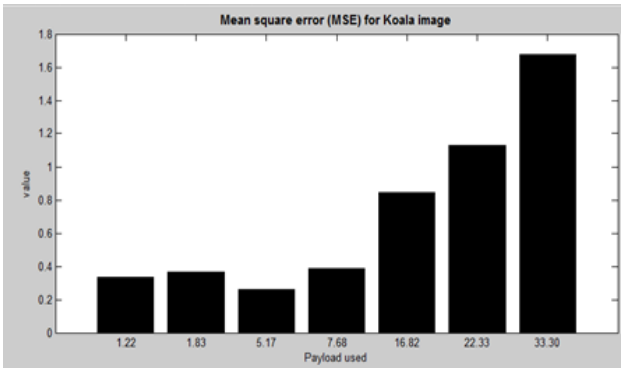

Figure 3:MSE values for koala image at different embedding capacity

Figure 4: shows PSNR values.

It has been found that slight decrease comes in PSNR values with the increase in payload. But as the bit selection varies with payload size, bit replacement also depends upon the selection pixel LSB values which results in almost similar PSNR values even with increase in payload.

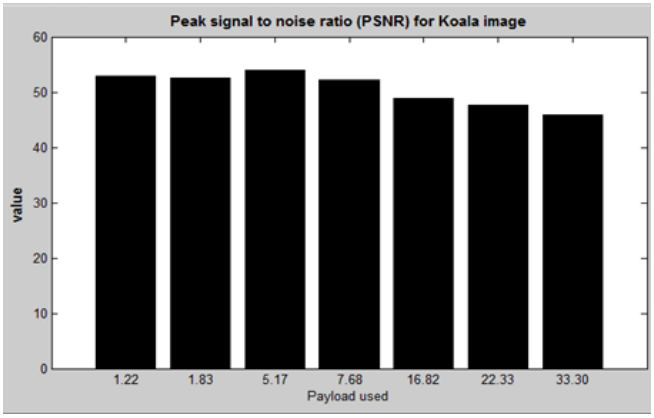

Figure 4: PSNR values for koala image at different embedding capacity

V. CONCLUSION

LSB (least significant bits) is one of the most well-known algorithms in spatial domain that replaces secret message bits with cover media's LSB which has been adopted for embedding. Two bit replacement has been

considered to increase the embedding capacity. Methods start by cropping the region of interest needed for self -embedding which is further separated into two matrices of LSB and MSB bits. MSB bits are then XOR encrypted in order to secure the data. MSB bits from whole image has been then used in which whole image is converted to non-overlapping blocks and entropy has been calculated for each block. Then blocks have been sorted based on maximum entropy value and blocks has been chosen for embedding process. Same criteria have been chosen on extraction side as entropy of MSB bits remain in same pattern. Proposed method scramble the bits in random fashion which are then embedded results in securing of data. Also MSB bit selection for embedding and two bit LSB replacement increases the embedding capacity by double. Hence 50% of the image can be used as region of interest for embedding.

VI. REFERENCES

[1]. Mansi S. Subhedara, Vijay H. Mankarb, "Current status and key issues in image steganography: A survey", ScienceDirect, computer science review 13-14 (2014) 95 - 113.

[2]. Dunbar B. Steganographic techniques and their use in an Open-Systems environment. SANS Institute; January 2002.

[3]. Artz D. Digital Steganography: Hiding Data within Data. IEEE Internet Computing Journal; June 2001.

[4]. Li F , Zhang X , Cheng H , Yu J . Digital image steganalysis based on local textural features and double dimensionality reduction. SecurCommunNetw2014 .

[5]. Wang X-T , Li M-C , Wang S-T , Chang C-C "Reversible data hiding exploiting high-correlation regulation for high-quality images"SecurCommunNetw 2015;8(7):1408-21 .

[6]. SubhedarMS ,Mankar VH . Current status and key issues in image steganography: a survey. ComputSci Rev 2014;13:95-113 .

[7]. Z. Y. Al-Omari and A. T. Al-Taani, "Secure LSB steganography for colored images using character-color mapping," 2017 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2017, pp. 104-110.

[8]. Aref Miri, Karim Faez , " Adaptive image steganography based on transform domain via genetic algorithm " Published in :Optik - International Journal for Light and Electron Optics Volume 145, September 2017, Pages 158-168

[9]. Xin Liao , Jiaojiao Yin , SujingGuo , Xiong Li , Arun Kumar Sangaiah , " Medical JPEG image steganography based on preserving inter-block dependencies " Published in : Computers & Electrical Engineering Available online 25 August 2017

[10]. P.Malathi, T.Gireeshkumar" Relating the embedding efficiency of LSB Steganography techniques in Spatial and Transform domains " published in : Procedia Computer Science Volume 93, 2016, Pages 878-885

[11]. Rao, J.B., Kuna, R.K. and Kasi, M.K., 2015, January "LSB matching steganalysis based on feature analysis approach" In Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on (pp. 1-5). IEEE