Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Encryption of Medical Images with Steganography Method

Gagandeep Singh[1] & Navpreet Kaur[2]
[1] pursuing M.Tech, Electronics & Communication Engineering
[2]Assistant Professor, ASRA College of Engg. And Tech
Bhawanigarh, Punjab

Abstract : *The Least Significant Bit (LSB) hiding is the most common methodology to implement steganography. LSB-based steganography is based on manipulating the LSBs of some or all pixels of the cover image to embed the message. There are many techniques existed which use LSB's method for embedding but they all embed information depending upon some parameters i.e. Entropy, DWT coefficients etc. are used to select the pixels which can be modified so that output should be imperceptible in nature. Many methods use edge pixels to embed the image, as edges have maximum entropy values but they mostly use filters i.e. canny, Soble, prewitt etc. to locate the pixels for embedding. The problem with these filters is that they produce random outputs on pixel locations hence causes loss in extracted data while extraction process. To overcome this, block based corner pixel selection idea has been chosen for this work in which some pixels are used to detect edges and some are used for embedding the data. It causes the system fully reversible in nature. To increase the embedding capacity we have used multiple locations in a block along with encryption of secret data by pseudo random generator based encoding which scramble the secret bits into random fashion. Experimental results show high embedding capacity of the algorithm along with data security of secret information.*

Keywords: LSB, data hiding, image, XOR, encryption

1. Introduction

Image steganography is used to hide secret information within an image [1]. Two major approaches used are reversible and irreversible image steganography.

In reversible image steganography the cover image can be reconstructed accurately while extracting the payload from the stego image. The stego image is the image obtained after embedding the secret message in cover image. Most of the existing reversible image steganography schemes are very complex and achieve small embedding capacity . Embedding capacity can be increased by adaptive embedding of payload near sharper edges. More bits can be accommodated in sharper edges using adaptive selection.

Irreversible image steganography schemes achieve higher embedding capacity with minimum computation time. Detection of hidden information in stego image resulting from irreversible stego system is straightforward. Many steganalytic schemes [2], [3] have been proposed in literature, which can accurately detect the presence of secret information embedded using irreversible image steganography. These methods are prone to easy detection of the embedded information. Even though irreversible image steganography schemes achieve low computation time, low level of security degrades the performance of such system. Encryption of secret information could be one of the solutions. However, inclusion of encryption spoils the use of steganography as the fundamental need of image steganography is to eradicate the suspicion of hidden data.

In this paper an adaptive image steganography technique which bears high embedding rate is proposed. Adaptive nature of the embedding process increases the embedding rate without increasing the detectability. Binary payload is embedded in edge area of a grayscale cover image. Grayscales of the cover image are used to embed binary payload in selected area based on some threshold which determines the number of bits to be embedded.

2. Related work

There are many reversible image steganography schemes proposed in the literature which employ encryption to achieve higher level of security. Wu et al. proposed a reversible image steganography scheme [4], where the secret message is encrypted using either AES or DES. The encrypted bits are then embedded in a code tree computed from the frequency of absolute error values. Error values are computed using MED predictor [4].

Scheme proposed in [5] generates an intermediate image by converting a pair of pixel values of secret image into four hexadecimal values and then four

hexadecimal values are converted to three decimal values. This intermediate image is then distributed and embedded into n cover images. To recover the secret image one has to gather all n stego images. The steganography scheme used in this method is straightforward. Detection of hidden information is so trivial that any steganalysis scheme can detect the presence of hidden information with more than 80 % accuracy.

A data hiding based on side-match vector quantization (SMVQ) has been proposed by Chang et al. [6]. For each block of cover image codeword is generated using SMVQ. These codeword are used to embed the secret data. If secret bit is equal to 0, the closest codeword generated by SMVQ is encoded. For a secret bit 1 the approximation of the first closest codeword and the second closest codeword is computed to replace the closest codeword. Even though the proposed scheme effectively encodes the secret message, for a large payload the size of transformed index table can increase the space complexity of the steganography system. Moreover, the embedding capacity of the scheme is low compared to other existing image steganography schemes.

High embedding rate of irreversible image steganography draws researchers to work in this area. Level of security is a concern in irreversible image steganography. Easy detection of hidden data is possible with some powerful steganalytic tools.

Least Significant Bit (LSB) replacement is the most common irreversible steganography scheme. The binary bits of the secret data are hidden in the cover image by replacing the LSBs of the cover image with the secret binary bits [7]. The method is so trivial that an attacker can easily detect the presence of hidden information.

An improvement over LSB is achieved in LSB matching (LSBM) where a +1 or −1 is added to the pixel of the cover image if the corresponding LSB matches with the secret bit. In LSBM as the probability of increasing or decreasing the number of odd or even pixel is same, the usual asymmetry introduced in LSB is avoided. Steganalytic schemes which work for LSB replacement fails to detect the presence of secret message, if LSBM is used.

Modification rate is further reduced in LSB matching revisited (LSBMR) [8] [9]. A pair of pixel is used to embed the secret bits. A secret bit is added to the first pixel of the pair and another bit is embedded using the relationship of the pair of pixels. As only one pixel of the pair is modified to embed two secret bits the modification rate reduces to 0.375 bit per pixel (bpp) [9]. General asymmetry introduced in LSB does not exist in LSBMR hence detection of the presence of secret bits is difficult. There are some edge adaptive methods proposed in literature such as hide behind corner (HBC) [10]. Edge adaptive irreversible image steganography proposed by Lou et al. [11] embeds secret data adaptively in the selected regions of the cover image. Method proposed in [11] extends LSBMR [9] and embeds secret data in edge areas of the cover image baring smoother areas. To embed the secret data cover image is first rotated using a specific key. Edge areas of the modified cover are identified to embed the secret information adaptively. This method is highly secure as percentage accuracy of detection of most of the statistical analysis used on the stego images, generated using the method proposed by Luo et al. [11], is less. The method proposed in [11] identifies an edge as the difference between two consecutive pixels. Data is embedded only in those areas where a vertical edge exists. A single bit is embedded in two consecutive pixels. Even though this method selects edge area adaptively it is done using a single threshold value. Hence the method proposed in [11] is not at all adaptive when it comes to embedding. The proposed method tries to identify vertical as well as horizontal edges to embed the secret data, which intern increases the embedding capacity of the proposed scheme. EDGE effectively predicts horizontal as well as vertical edges. Edges are classified into three categories using three levels of threshold. More bits are embedded in sharper edges, which again increase the embedding rate. Result analysis shows that the proposed method achieves better results with respect to embedding rate and lesser percentage accuracy of detection compared to most of the state of the art steganography methods. [13] used DC components for hiding secret bits sequentially in Least significant Bits (LSBs) (1-LSB & 2-LSB).Work in [14] used he pixels where secret data is to be embedded is selected randomly using a pseudo random key. In the selected pixels the last 2 or 3bits are used for hiding. it is not advisable to use short data sequence and key lengths because by using powerful software‟s one can hack the short keys very easily and able to break the system. Once one can determine the failure rate of keys then encryption process takes place. All the keys are based upon the mathematical properties and their strength decreases wrt time. So, basically it is a tradeoff between key length and security level. For the task the optimal selection of keys makes the model optimized. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data.[15]

3. Proposed method

Proposed method has two major phases; embedding and recovery as shown in Fig. 1 and 2. To embed the secret message S, EDGE predictor is used to compute

the edge image from the cover image. Region selector divides the edge image into nonoverlapping Z × Z blocks. Predicted error greater than a particular threshold, are selected from each block for capacity estimation. Capacity of each block is measured by computing the number of bits that can be embedded into a particular block. In each block for a particular predictive error one, two or three bits of the secret message can be embedded into the corresponding grayscale of the original cover depending on the threshold. Capacity is computed by adding the number of bits that can be embedded in a particular grayscale of a block. If the capacity of the block is not enough to accommodate the secret data region selector re-computes the region for embedding. There are certain additional information required for extraction of the secret data such as block size (Z) and threshold (Tk) which are embedded in those regions which are not used for data embedding.

To extract the secret message edge image is computed from the cover image and auxiliary information such as threshold and block size are extracted from the stego image. Based on threshold and block size the regions containing the secret information are identified. Extraction process then extracts secret information from the selected regions.

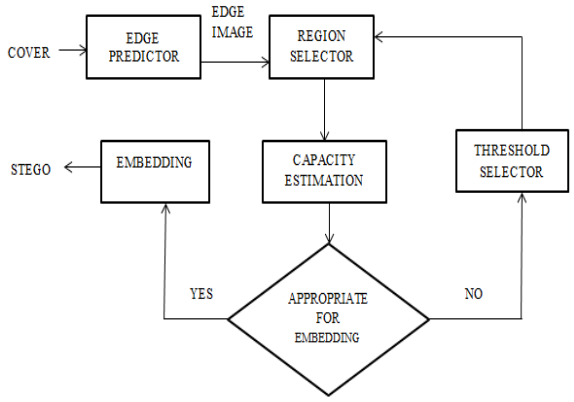

Figure 1: Flowchart for embedding process

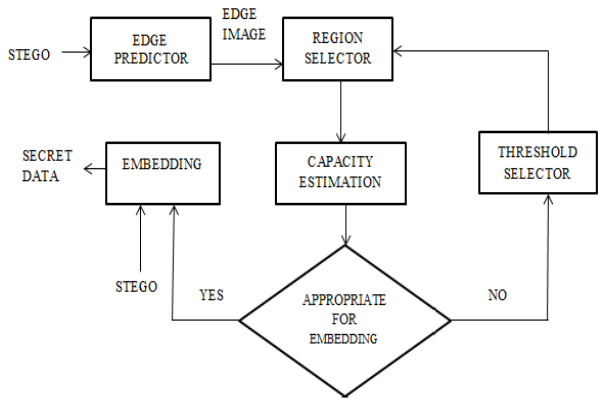

Figure 2: Flowchart for Extraction process

4. Results and discussions

First of all, the image to be embedded is selected. Self –embedding is required when the image contain sensitive material that should not be shown to the general public for example in court cases. Then edge predictor is applied to get the edges in the image

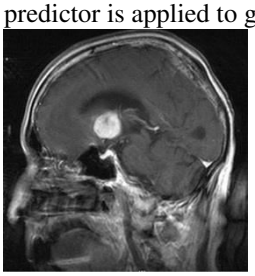

Figure 3: Input Cover image

After that, embedding has been carried out on LSB bits of those blocks which are found as edge blocks as described in previous chapter. Below is the image produced after embedding process. bit LSB steganography is used to embed the encrypted MSB bits into the block having highest entropy first. Human visual system is less sensitive to changes in sharp contrast area (edges) compared to uniform area of the image. Proposed system is reversible. Stego image can be converted back into original image. During extraction, Same edge blocks has been found. Decryption algorithm is applied to the extracted bits and resulted image bits are stored to the original location. Performance evaluation of proposed work has been carried out by pSNR and MSE metrics as described below.

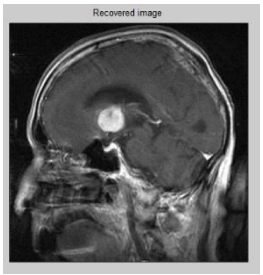

Figure 4: Recovered original image

Mean Square Error (MSE): The MSE signifies the cumulative squared error between the input and the output image. To compute the PSNR, we first calculate the mean squared error. It is calculated by the following equation (1).

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(m,n)]^2}{M * N} \quad \textbf{(1)}$$

Where N and M are the number of columns and rows in the input images, respectively and I1 (m, n) is the input image, I2 (m, n) is the sanitized image.

Peak Signal-to-Noise Ratio (PSNR): Signal–to-noise ratio (SNR) is a mathematical measure of image quality. It is based on the pixel difference between two images. The SNR measure is an estimate of quality of reconstructed image compared with original image. PSNR is defined by the following equation (2)

$$PSNR = 10\log_{10}\left[\frac{R^2}{MSE}\right] \quad \textbf{(2)}$$

The PSNR takes the signal strength into consideration. The values were used to evaluate the quality of the image. Where R represents maximum fluctuation or value in the image, its value is 255 for 8 bit unsigned number.

Table 1: Result Table for Proposed method

Threshold	MSE	PSNR
Existed work		
25	0.0155	66.2173
20	0.0156	66.1958
15	0.0154	66.2334
10	0.0156	66.1969
5	0.0154	66.2356
Proposed work		
25	0.0221	64.67195
20	0.02206	64.69460
15	0.02153	64.80032
10	0.02191	64.7242
5	0.02174	64.7571

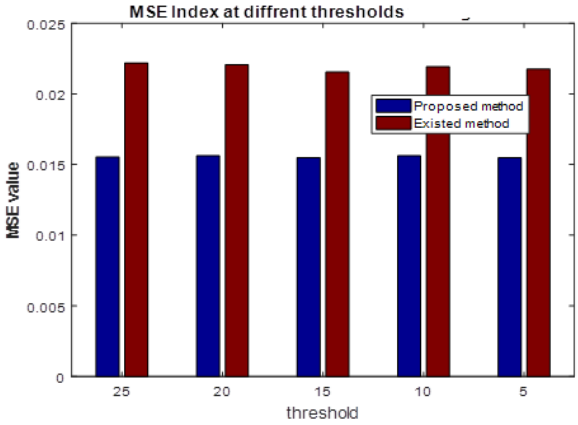

Figure 5: MSE Index at different thresholds

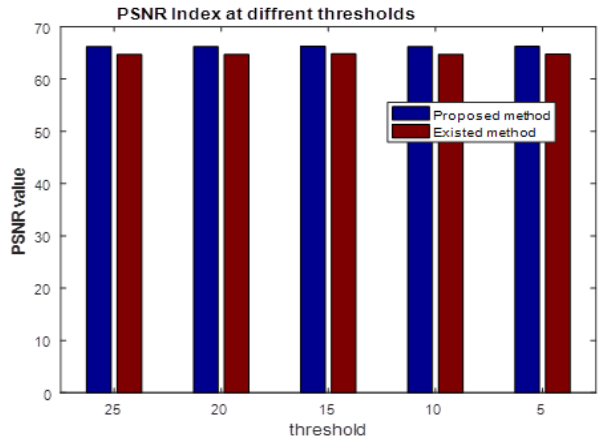

Figure 6: PSNR Index at different thresholds

5. Conclusion

The utilization of edge detection in image steganography has been considered by a number of researchers. Due to sensitivity of the human eye to changes in smooth areas of the image compared to sharp contrast areas, it is logical to focus on sharp edges when embedding the secret message. However, the main obstacle to applying traditional edge detection methods in image steganography is the correct identification of edge pixels in the stego image that need to exactly match the original edge pixels in the cover image. This problem arises from the fact that the embedding process introduces minor changes to the stego image, which may make the produced stego image not identical with the cover image, and this can affect the message extraction process. To solve this problem in the proposed steganography method, we did not use popular edge detection algorithm i.e. Canny, Soble etc. and uses an effective edge detection method which do not fail in detection of accurate edge location. The methods used non-overlapping blocks of size 3*3 and horizontal, vertical and diagonal edges has been found out using four corner pixels at the edges of

block. Then XOR based embedding algorithm has been used to embed data in the remaining pixel locations which are not used in edge detection phase. This will not effective the edge detection process at receiver side and same edge locations can be found at both sender and receiving end. To increase embedding capacity, not all eight bits are user for the secret location but only MSB bits are used hence cause in more area embedding than the full value embedding processes.

References

[1] Cheddad, Condell J, Curran K, McKevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752

[2] Huang F, Li B, Huang J (2007) Attack LSB matching steganography by counting alteration rate of the number of neighborhood gray levels. IEEE Image Process Conf Proc 1:401–404

[3] Ker D (2005) Steganalysis of LSB matching in grayscale images. IEEE Signal Process Lett 12(6):441–444

[4] Wu HC, Wang HC, Tsai CS, Wang CM (2010) Reversible image steganographic scheme via predictive coding. Displays 31:35–43

[5] Ulutas G, Ulutas M, Nabiyev VV (2012) Secret image sharing with reversible capabilities. International Journal of Internet Technology and Secured Transactions 4(1):1–11

[6] Chang CC, Tai WL, Lin CC (2006) A reversible data hiding scheme based on side-match vector quantization. IEEE Trans Circuits Syst Video Technol 16(10):1301–1308

[7] Walton S (1995) Image authentication for a slippery new age. Dr Dobbs J Softw Tools Prof Program 20:18–26

[8] Huang F, Zhong Y, Huang J (2014) Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm. Digital-forensics and watermarking. Lect Notes Comput Sci 8389:19–31

[9] Mielikainen J (2006) LSB matching revisited. IEEE Signal Process Lett 13(5):285–287

[10] Hempstalk K (2006) Hiding behind corners: using edges in images for better steganography. In: Computing Women's Congress Proceedings, Hamilton, New Zealand

[11] Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. IEEE Trans Inf Forensics Secur 5(2):201–214

[12] Alattar M (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156

[13] Sahar A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information" Published in: Computers & Electrical Engineering Available online 19 September 2016

[14] Saleema. A, Dr. T. Amarunnishad, "A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks" Published in: Procedia Technology Volume 24, 2016, Pages 1566-1574

[15] Ajay Kakkar, ML Singh, PK Bansal (2012) "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication" International Journal of Engineering and Technology Volume 2 No. 1, January, 2012 pp 87-92