A Novel Approach for Reversible Data Hiding in Encrypted Images Using Key Based Pixel Selection

Mala R
PG Scholar, Department of CSE
CMR Institute of Technology
Bangalore, India

Mrs. Manimozi I
Associate Professor, Department of CSE
CMR Institute of Technology
Bangalore, India

Abstract—In this paper a new steganographic approach is proposed to increase the confidentiality of the hidden data in RGB images by placing the data randomly across the encrypted images. By using the secret key provided to the users, key based pixel selection approach is applied in order to randomize the pixel selection. In order to make the retrieved image and data free from error, space is reserved before image encryption. LSB replacement method is used to embed the data in the encrypted image. The basic idea in the newly proposed method is to embed the data into the least significant bits of pixels of red plane which are placed diagonally within the cover image. Replacing the Least Significant bits in a single RGB plane does not provide any distortion to the restored image which can be visible to human eye.

Keywords- LSB, Key Based Pixel Selection, Steganography, Histogram, Steganalysis.

I. INTRODUCTION

Over the recent years many data hiding techniques have been proposed and implemented to accomplish the goal of using steganography. Steganography is an art of hiding data into larger objects such that the changes are not easily detectable by the human eyes. Reversible data hiding is a stegnographic technique in which the data is hidden in digital media like images, audio, video etc and the original image and data are extracted in a lossless manner. In order to make the information invisible and undetectable to an intruder, information can be placed in some order or into specific places, successful data hiding should be such that the observer should not notice the presence of data and data should be directly encoded. Different methods have been proposed, among which Least Significant Bit (LSB) is most widely used and effective technique [1, 2], using the LSB based approach a pseudo random number generator function is proposed which uses the shared key to generate a random number to randomize the pixel selection, these pixels are used to embed the data [3].Some applications require that confidentiality be provided to the embedded data. Based on the textual key provided by the user a new encryption algorithm was proposed to make the message more secure [4] which further extended the MSA algorithm [5].

Furthermore applications like buyer-seller watermarking protocol [6] requires for data hiding in encrypted domain, for which the original image is encrypted with encryption key and data encryption is done with the data hiding key receiver. A person possessing both the keys can extract data and obtain the original image, here the LSB's of encrypted image is compressed to accommodate the data [7] this approach performed well if the amount of data was not too large. Due to maximization of entropy in encrypted images compressing and vacating room in encrypted images directly resulted in error rates after image restoration or data extraction with poor quality for large payloads. Reserving room before encryption emptied out space by reversibly embedding the LSB's of high contour pixels into low contour pixels in addition it also separated the data extraction from image decryption [8].Data was embedded into the rearranged pixels which were placed sequentially starting from the first row of the image, as it is easy to guess the position of the data this approach is subject to crypt analytic attacks compromising the security of the images.

In this paper, we present a novel steganographic approach to increase the confidentiality of the hidden data in RGB images. The basic idea here is to select the pixels based on the secret key shared with the receiver and the sender, the data is embedded into the RGB planes of these pixels. In this project we choose to embed data into the least significant bits of red plane. Since the selections of pixels are comparably random based on the secret key, this key based pixel selection method provides protection over visually detectable threats like cryptanalytic attacks. In addition to randomizing the pixel selection, space to hide the data is reserved before encryption of the image to make the process of image extraction lossless. The remainder of the paper is organized as follows. Section II explains the proposed scheme. Evaluation of image quality is represented in Section III. In Section IV

experimental analysis is shown along with the results. Finally, Section V concludes the work and discusses some future directions.

II. PROPOSED SYSTEM

The proposed scheme contains image encryption, data embedding and data-extraction/image-recovery phases.

A. Image Encryption

Assuming the size of image to be MxN, made of pixels with gray value ranging between [0,225].With 8 bits it can be represented as $O_{i,j}(0),O_{i,j}(1)\ldots\ldots O_{i,j}(7)$, which implies

$$O_{i,j}(u)= \lfloor (O_{i,j})/2^k \rfloor \bmod 2 \qquad \text{where } u=0,1\ldots7 \qquad (1)$$

$$E_{i,j}(u)= O_{i,j}(u) \oplus K_{i,j}(u) \qquad (2)$$

Here $K_{i,j}(u)$ is determined by an encryption key using a standard cipher. Exclusive-or operation is carried out between the original image bits and the encryption key bits to obtain the encrypted image. With the use of a separate encryption key for data the confidentiality of the image is protected as the data hider cannot access the contents of the image file without knowing the encryption key. Space to embed data is reserved before encryption of image and which achieved by the matrix construction method explained in the next section.

B. Data Hiding

The process of data hiding is divided into two steps: matrix construction followed by pixel selection.

1) Matrix Construction: This mainly involves the creation of a binary matrix from the chosen original image, considering the original image to be an RGB image of size MxN, the binary matrix of size MxN is constructed by mapping the 8 bit binary converted value of the encryption key, pseudocode for matrix creation is given below:

a) Initialize a binary matrix of size MxN.

b) Obtain the 8 bit binary value of the encryption key.

c) Initialize the index of the binary key for the first byte

d) Scan the image row wise for m=M

e) If m mod 2 is zero extract the MSB of binary key and create a 2x2 matrix across row i and i+1

f) Increase the column count j+2, if m mod 2 is not equal to zero create the matrix with LSB bits of key

g) Repeat the procedure until the end of binary matrix

h) Exit

2) Pixel Selection: The second step in data hiding process is selection of the pixels for hiding the message. The placement of the data in the pixels plays an important role, in sequential approach the message bits are sequentially embedded in the pixels, the major disadvantage is as the messages are encoded in image file sequentially, it is possible to find clusters of embedded bits, which results in abrupt changes in the bit statistics thus making the detection easier [3].While in the image encryption phase we will be encrypting the pixels at index where $M_{i,j}(u)=0$.For data hiding, pixels $E_{i,j}(u)$ in the encrypted image are selected by: scanning the binary image for which the value in the indices i and j is $M_{i,j}(u)=1$.Data is inserted using the traditional RDH approach of LSB replacement, message bits are embedded into the last 4 LSB bits of the pixels placed in red plane in the 8 bit RGB image. This proposed approach randomizes the pixels selection making it difficult to visually identify clusters of bits and hence a better approach in terms of confidentially in comparison with the sequential embedding.

C. Image Recovery and Message Extraction

In encryption phase we encrypted the image pixels for which the binary image matrix contained a value 0.This process is reversed in the image decryption phase. For data extracttion we consider the pixel values for which the corresponding value in the binary matrix holds a binary value 1. Based on the order of the image recovery and message extraction the practical applicability varies:

1) Data Extrcation from Encrypted Images: Few applications require that access be provided only to data without the image being displayed example in commercial applications like medical imaging which require updating of patients personal information which hiding the image, medical personals may get access only to data where the data is extracted using the data hiding key in such case provided the algorithm the user can run the algorithm with encryption key D_k as the input and retrieve the image.

2) Image recovery: If the user has only the encryption key E_k without access to the data hiding key then image. Decryption process is a reverse process of encryption done to recover the image.

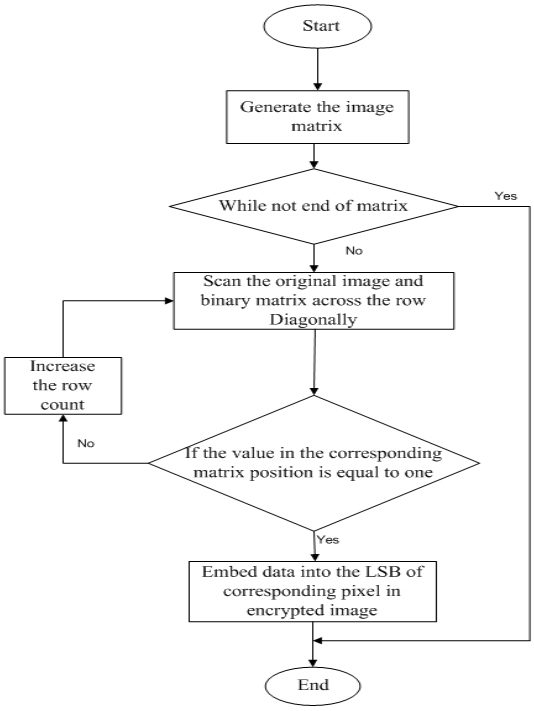

Fig. 1. Pixel Selection Algorithm

III. EVALUATION OF IMAGE QUALITY

Comparison of the recovered image with the original image is done by measuring the image quality in terms of PSNR (Peak Signal-to-Noise Ratio), MSE (Mean-Squared error) and histogram. Mean Squared Error (MSE) is used to check the error between the original image and the recovered image and is defined as in equation (3). Where O_{xy} is the original image, R_{xy} is the recovered image, x, y is the image coordinates and M, N is the dimensions of the image.

$$MSE = \frac{1}{MN}\sum_{X=1}^{M}\sum_{y=1}^{N}(O_{XY} - R_{XY}) \quad (3)$$

Peak Signal-to-Noise Ratio (PSNR) is used as a metric to evaluate the difference between the original and recovered images, as an approximation to the human perception of reconstruction quality it is measured using the mean squared error (MSE) represented by equation (4).

$$PSNR = 10 \log_{10} \left(\frac{P_{max}^2}{MSE}\right) \quad (4)$$

Where P_{max} is the maximum pixel value, for an 8 bit image the value would be 255.Table I shows the MSE and PSNR values calculated for different images.

TABLE I. PSNR FOR DIFFERENT IMAGE SIZES

PSNR results (dB)			
Image	**Size of cover image in KB**	**MSE**	**PSNR**
Girl	15.2	1.7958	45.5882
Flower	461	0.0674	59.8421

IV. EXPERIMENTAL ANALYSIS

Based on the proposed approach, a system was developed, which implemented the algorithm. The system is tested using the images shown in Fig. 1. And Fig. 2. The original images before encryption image are shown in Fig. 2(a) and Fig. 3(a), Fig. 2(b) and Fig. 3(b) depict the recovered image after image extraction. As it can be seen recovered image does not have a noticeable distortion on it visually as seen by human eyes.

(a) (b)

Fig. 2.Girl (a) Original Image, (b) Decrypted Image

(a) (b)

Fig. 3. Flower (a) Original Image, (b) Decrypted Image

Histogram analysis was carried out, in order to detect significant changes in frequency of appearance by comparing the original cover image with the recovered image. Fig. 4-Fig. 7 shows the generated histogram. It is evident from the histograms that there are no significant changes. Hence from this result it can all so be said that the proposed approach could be immune to attacks based on histogram analysis. Histogram in Fig. 4.shows the generated histogram for the image girl before encryption, in Fig. 5.it is visible the histogram of decrypted image is same as original image histogram as in Fig.4.

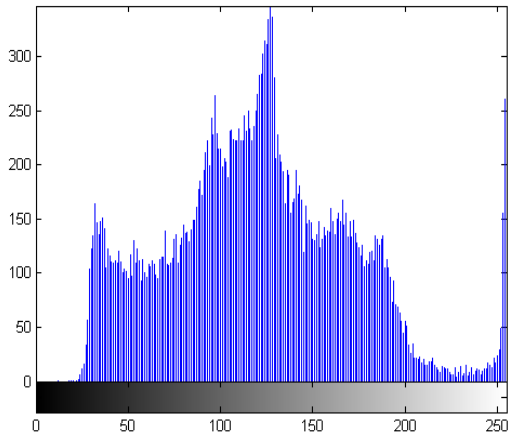

Fig. 4. Histogram Original Image (Girl)

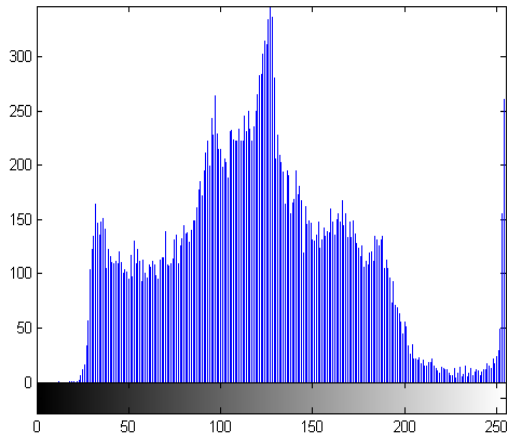

Fig. 5. Histogram Decrypted Image (Girl)

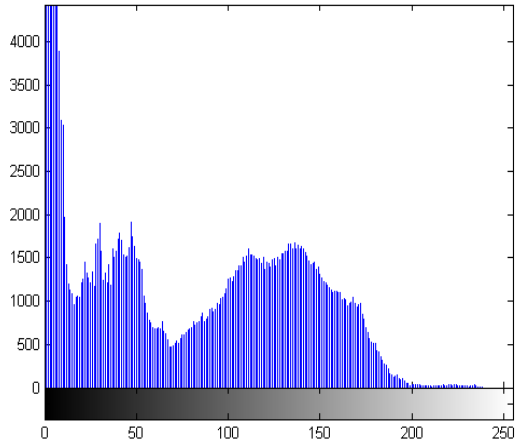

Fig. 6. Histogram Original Image (Flower)

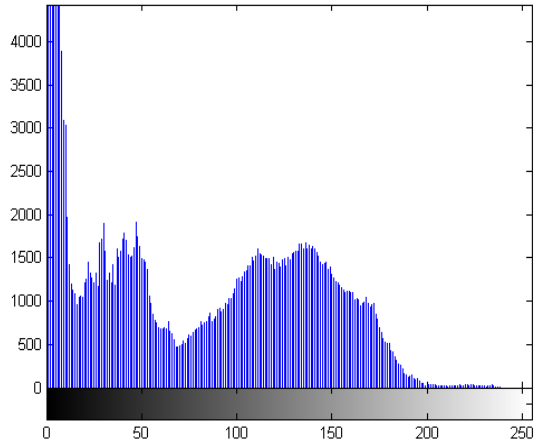

Fig. 7. Histogram Decrypted Image (Flower)

V. CONCLUSION AND FUTURE WORK

In this paper, a new approach is presented for securely hiding data in a digital cover image using stegnographic techniques, here the main focus is on increasing the security of the data for protecting it from steganalysis while reducing distortion rate in the recovered image. Traditionally proven RDH approaches like least significant bit replacement was used combined with the key based pixel selection approach which randomizes the position of data embedding. In this proposed method since the space is reserved for embedding data before image encryption complexity to hide data emptying the space from an encrypted image is reduced. The length of message that can be embedded depends on the size of the image and the encryption key. Furthermore this approach can be enhanced to increase the size of messages that can be embedded. Some aspects which have not been considered like higher encryption techniques for encrypting message and could be added to secure data while preserving the original features of the image.

REFERENCES

[1] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE,Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998.
[2] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image," David publishing, Computer Technology and Application 2 (2011) 102-108.
[3] Shamim Ahmed Laskar and Kattamanchi Hemachandran "Steganography based on random pixel selection for efficient data hiding," International journal of computer engineering & technology (ijcet), Volume 4, Issue 2, March – April (2013), pp. 31-44.
[4] Joyshree Nath and Asoke Nath, "Advanced Steganography Algorithm using Encrypted secret message," International Journal of Advanced Computer Science and Applications,Vol. 2, No.3, March 2011.
[5] A.Nath, S.Ghosh, M.A.Mallik, "Symmetric key cryptography using random key generator," Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.
[6] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, April 2001.
[7] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE transactions on information forensics and security, Vol. 7, No. 2, April 2012.
[8] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li , "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE transactions on information forensics and security, Vol. 8, No. 3, March 2013.
[9] Juan Jose Roque, "LSB: Improving the Steganographic Algorithm LSB," WOSIS, 2009, pp.57-66.