ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 10 || October– 2014 ||
International Journal of Computational Engineering Research (IJCER)

Reversible Data Hiding in Encrypted color images by Reserving Room before Encryption with LSB Method

[1] Sabeena O.M, [2] Rosna P. Haroon
[1]*Dept. of CSE Ilahia College Of Engineering and Technology, Kerala,India*
[2]*Assistant Professor Dept. of CSE Ilahia College Of Engineering and Technology, Kerala, India*

ABSTRACT
Reversible data hiding is the technique in which data in the cover image reversibly can retrieve after the extraction of hidden data in it. The technique provides the secrecy for a data, and also for its cover image. Ancestor methods of reversible data hiding were vacates room for data hiding after encryption, which leads to some errors at the time of data extraction and image recovery. Here describes a novel method of reversible data hiding in which, Reserving room before encryption in images, so that image extraction is subjected to free of errors. Here we are proposing an LSB plane method for the data hiding, which will result more space for embedded secret data. Moreover the usage of colour images as cover images will helps to store more data in different channels.

KEY WORDS*— reversible data hiding, LSB plane method*

I. INTRODUCTION

In most cases of data hiding, the cover images will experience some distortion due to data hiding and cannot be inverted back to the original form. That is, some permanent distortion has occurred to the cover image even after the hidden data have been extracted out. In a wide range of applications like medical, military and law forensic fields, distortion of cover images does not allowed. So reversible data hiding is essential for these cases. In this technique the cover image can losslessly recover after the extraction of hidden data. So many RDH techniques have introduced in recent years. One of a general framework for RDH is first extracting compressible features of original cover and then compressing them losslessly, more space can be saved for embedding auxiliary data. Another popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded like multiplication by even numbers. Then the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another considerable strategy for RDH is histogram shift (HS), in which space is surplus for data embedding by shifting the highest possible value of histogram of gray values. Encryption is an effective and popular means of privacy protection. A content owner can encrypt his message before sending to another person as it converts the original and meaningful content to abstruse one. In some applications a block. This process is performing with the help of spatial correlation in decrypted image. In another method, at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique, which provides much lower error rate. These two methods mentioned above rely on spatial correlation of original image to extract data. Implies that, decryption must be done in the encrypted before data extraction. All the above methods try to vacate room from the encrypted images directly. Because of the entropy of encrypted images has been maximized, these techniques can only obtain small payloads or generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration. Some methods can use error correcting codes, also pure payload can consume. In this paper, we proposes a novel method for RDH in encrypted color images, for which we do not "vacate room after encryption", but "reserve room before encryption" [1]. We can first empty out spaces by embedding LSBs of some pixels into other pixels with a LSB plane method and then encrypt the image, so the place of these LSBs in the encrypted image can be used to hide data bits. This method separate data extraction from image decryption and data extraction and image recovery are free of any error.

II. RELATED WORKS

Reversible data hiding was first established as a technique of attaining the cover image after the extraction of hidden data. Here utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel gray scale values to embed data into the image [2]. The computational complexity for technique is low, but it is only applicable at gray scale images. Then the Reversible Data Hiding with Optimal Value Transfer emerges to find the optimal rule of value modification under a payload-distortion criterion.

An optimal value transfer matrix can be obtained by maximizing a target function using iterative algorithm, for a practical reversible data hiding scheme [3]. The technique undergoes the prediction so Computation complexity will be higher. Encryption is an effective and popular means of privacy protection. Through the work Reversible Data Hiding in Encrypted Image proposes a reversible data hiding scheme for encrypted image. Then the additional data can be embedded into the image by modifying a small portion of encrypted data, after encrypting the entire data of a gray image [5]. The received image provides original image through decryption using encryption key and data using data hiding key. For encrypted images, the compression efficiency can be improved as how the source dependency is exploited. So a work developed as Efficient Compression of Encrypted Gray scale Images. The paper proposes a resolution progressive compression scheme which compresses the encrypted image progressively in resolution, such that the decoder can attain low-resolution version of the image [4]. The statistics can be used to analyze next resolution level. An Improved method of Reversible Data Hiding in Encrypted Images is Using Side Match. Here proposes an improved data extraction and image recovery method over Zhang's work. The Zhang's work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels [6]. Thus leads to estimation of new algorithm for better calculation of smoothness of image blocks. According to the descending order of the absolute smoothness difference between two candidate blocks, the extraction and recovery of blocks are performed. Also side match technique reduces the error rate.

In the first phase, a content owner encrypts the original image using a key. Then, a data-hider may vacates some spare space by performing compression on least significant bits using a data-hiding key to accommodate some additional data. Using Separable Reversible Data Hiding in Encrypted Image, with an encrypted image containing additional data, even receiver does not know the image content he can extract the additional data using data hiding key [7]. Also receiver can decrypt the received data to obtain an image similar to the original one using encryption key, but cannot extract the additional data. Receiver can recover the original content and extract additional data without any error using the encryption key and data-hiding key. Watermarking embeds information into a digital signal. After the hidden data is extracted, receiver can restorethe original image without any distortion. Reversible Image Watermarking is a scheme using an interpolation technique, which can embed a large amount of data into images with unknowable modification [8]. Here assigns the interpolation-error. Due to lesser modification of pixels, quality of image will be higher. Reversible Watermarking Algorithm Using Sorting and Prediction is another algorithm without using a location map is used for reversible watermarking. This algorithm employs prediction errors to hide data into an image. To record the prophesy errors based on magnitude of its local variances a sorting technique is used [9]. Using sorted prophesies errors and a reduced size location map allows us to hide more data in the image with less distortion.

Then improved a Reversible Data Hiding Scheme Via Optimal Codes for Binary Covers. It improves the recursive construction to approach the rate–distortion bound. Also they generalize the method using a decompression algorithm as the coding scheme to hide data and prove that the generalized codes can reach the rate–distortion bound [10]. Also proves the compression algorithm reaches entropy. By the proposed binary codes, they improve three RDH schemes that use binary feature sequence as covers. Reversible Data Embedding Using Difference Expansion is a novel reversible data embedding method for digital images. They explore the redundancy in digital images to achieve very high overwhelming capacity, and keep the distortion low. Here needs to access location map and also can be performed at gray image only.

III. PROPOSED SYSTEM

The proposed architecture consists of a Reserving Room Before Encryption (RRBE) method for the data hiding in color images and also allows the reversible extraction of cover image. The architecture shown below in figure 1 is architecture of RRBE. VRAE images are sometimes inefficient and difficult to extract data, we like to reverse the order of encryption and vacating room, i.e., reserving room before image encryption at content owner side, becomes a novel framework "reserving room before encryption (RRBE)" which leads to the more natural and much easier Reversible data hiding tasks in encrypted images. Here the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data hiding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previously reserved. The data extraction and image recovery are identical to VRAE. Using color images as the cover images, more data can become hidden. We can reserve more space from three channels of colour image.

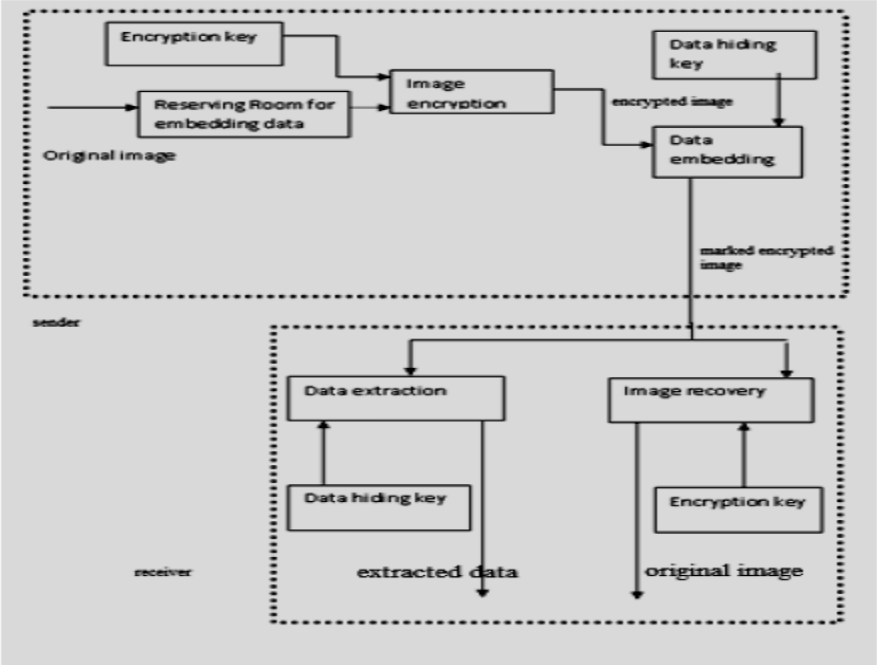

Figure 1. Architecture of RRBE

IV. SOLUTION METHODOLOGY

Here in the proposed architecture a practical framework based on "RRBE" method in color image, which primarily consists of following stages: reserving room in image, encryption of image, data hiding, data extraction and image recovery.

A. Reserving Room in Image

Actually the first stage can divide into two parts, image partition and self reversible embedding.

1.*Image partition*:

Here we uses the LSB planes for the reserving room operation, so the goal of image partition is to construct a smoother area [1], on which standard RDH algorithms can achieve better performance. To do that, without loss of ordinarily, take the 3 channels of original image as 8 bits gray-scale images with its size is M X N and pixels Ci,j belongs to [0,255]. 1<=i<=M, 1<=j<=N. so we have to perform every operation to the three channels of the image. First, the content owner extracts from the original image, along the rows, Discrete overlapping blocks whose number is determined by the size of to-be-embedded messages, denoted by *l*[1]. In detail, every block consists of *m* rows, where *m = [l/N]* and the number of blocks can be computed through *n=M-m+1[1]*. An important thing is that each block is overlapped by pervious or sub sequential blocks along the rows. The content owner, selects the particular block with the highest smoothness to be A, and puts it to the front of the image concatenated by the rest part B with fewer textured areas as shown below.To find smoother area we can use histogram of the cover image [1].

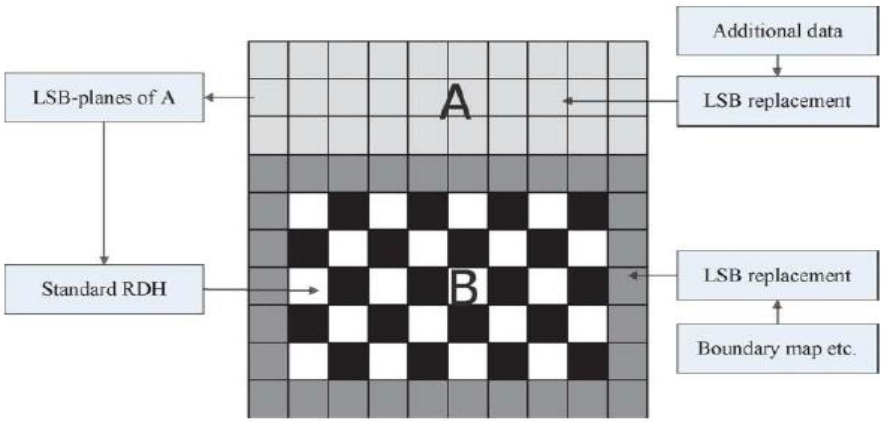

Fig. 2. Illustration of image partition and embedding process[1].

2..Self-Reversible Embedding:

The goal of self-reversible embedding is to embed the LSB-planes of A into B. Pixels in the rest of image B are first categorized into two sets: white pixels with its indices i and j satisfying (i+j)mod2 = 0 and black pixels whose indices meet (i+j)mod2 = 1, as shown in Fig. 2 Then, each white pixel, Bi,j is estimated by the interpolation value[1] obtained with the four black pixels surrounding it as follows

$$B'_{i,j} = w_1 B_{i-1,j} + w_2 B_{i+1,j} + w_3 B_{i,j-1} + w_4 B_{,j+1}$$

Where the weight *w*i, 1<= i<=4. The estimating error is calculated via ei,j = Bi,j - B'i,j and then some data can be embedded into the estimating error sequence. Also the same steps have to do for the black pixels and find ei,j.

B. Encryption of image

We can create encrypted image E by performing the encryption on rearranged self-embedded image, denoted by X. Encryption of X can easily obtain using a stream cipher. For a color image, we take the three channels as three grayscale images. For example, a gray value Xi,j ranging from 0 to 255 can be represented by 8 bits, Xi,j(0), Xi,j(1),…… Xi,j(7) [1], such that

$X_{i,j}(k)=[X_{i,j}/2^k]\bmod 2$, k=0,1,….7

Exclusive- or operation can be used for obtaining encrypted bits

$$E_{i,j}(k)= X_{i,j}(k) \oplus r_{i,j}(k)$$

Where ri,j(k) is generated by a standard stream cipher determined by the encryption key. At last, we embed 10 bits information into LSBs of first 10 pixels in encrypted version of A to tell data hider the number of rows and the number of bit-planes [1] he can embed information into After image encryption to provide the privacy of the content owner being protected, any third party cannot see the content without using encryption key.

C. Data hiding

Data hider will not be provided with the original image. He can embed data to the encrypted image. The embedding process can start at AE which is encrypted version of A. The data hider read 10 bits information in LSBs of first 10 encrypted pixels, as it is arranged at the top of encrypted image. After knowing how many bit-planes and rows of pixels he can modify, he can simply adopt LSB replacement to substitute the available bit-planes with additional data m. The data hider analyzes additional data and the hiding process proceeds with that information. Every pixel values will be converted to binary form and binaries of data bits appended to last bit of pixel values. So a new image will be generated. Anyone who does not having the data hiding key could not extract the additional data.

D. Data extraction and image recovery

Data extraction can do completely independent from image decryption. So the order of them implies two different practical applications.

1) Case 1*: Extracting Data From Encrypted Images [1]:* To manage and update personal information of images which are encrypted for protecting clients' privacy, a poor database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The feasibility of work is when following the order of data extraction before image decryption.

The database manager gets the data hiding key for decrypting the LSB-planes of AE and extract the additional data m by directly reading the decrypted version. Leakage of original content avoids because the whole process is entirely operated on encrypted domain.

2) Case 2: *Extracting Data From Decrypted Images:* we can proceed with the following scenarios,

a) Generating the Marked Decrypted Image: To form the marked decrypted image X'' which is made up of A'' and B'', the content owner should do following two steps [1].

• Step 1. With the encryption key, the content owner decrypts the image except the LSB-planes of AE[1]. The decrypted version of E' containing the embedded data can be calculated by

$$X''_{i,j}(k)= E'_{i,j}(k) \oplus r_{i,j}(k)[1]$$

And

$$X''_{i,j}= \mathrm{Sum}(X''_{i,j}(k) \oplus r_{i,j}(k) \times 2^k)[1]$$

 Step 2. Extract SR and ER in marginal area of B''. By rearranging A''[1] and B'' to its original state, the plain image containing embedded data is obtained.

b) Data Extraction and Image Restoration* [1]*: After generating the marked decrypted image, the content owner can further extract the data and recover original image[1].

V.CONCLUSION AND FUTURE WORK

Reverse data hiding for colored images are proposed here in this paper. Previous methods have implemented several techniques for data hiding for Gray scale images only. For encrypted images, RDH is done by reserving room before encryption, by using LSB Plane Method as opposed to the one which have proposed Histogram Shifting. Thus the data hider can benefit from the extra space in each channel of the color image. Time delay may arise for color images when reserving room before encryption. By resizing the image we can remedied it out but we have to compensate for the extra space utilization.

VI.ACKNOWLEDGMENT

The authors wish to thank the Management and Principal and Head of the Department(CSE) of Ilahia College of Engineering and Technology for the support and help in completing this work.

REFERENCES

[1]. Kede Ma, Weiming Zhang, Xianfeng Zhao,, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL:8 NO:3 YEAR March 2013

[2]. Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[3]. T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Processing (DSP2002)*, 2002, pp. 71–76.

[4]. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[5]. X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[6]. W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol.

[7]. X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[8]. L. Luo *et al*., "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[9]. W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[10]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[11]. J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.