Asian Journal of Science and Applied Technology (AJSAT)
Vol.2.No.1 2014pp 33-37
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

LOSSLESS DATA EXTRACTION BY RESERVING ROOM BEFORE ENCRYPTION WITH REVERSIBLE EMBEDDING TECHNIQUE

P.Kanchanamala, **MrP.S.Thumilvannan**
ArulmiguMeenakshi Amman College of Engg
ThiruvannamalaiDt

ABSTRACT

Reversible Data hiding enables the exact recovery of the image upon the extraction of embedding information . The constructed system is to reserve room before encryption with Reversible data hiding technique can achieve real reversibility and then extract the original data and image recovery without any error. The technique can be utilize in reversible data hiding is Histogram shift technique. The Histogram Shift technique in which the space is saved for data hiding by shifting the bins of histogram of gray values. The content owner and then reserve enough space on original image and then convert the image in to its encrypted version with encryption key. The data embedding process in encrypted image is reversible for data hider needs to accommodate data in to sparse space then the data can be extracted and recover the image. If the receiver has the data-hiding key, can extract the additional data though the receiver does not know the image content. If the receiver has the image encryption key, can decrypt the imageThe Reversible data Hiding technique used in medical imagery, military imagery and law forensic.

Keywords–Reversible Data Hiding,Histogram shift,image Encryption.

I. INTRODUCTION

Reversibledatahiding(RDH)hasthe capability toremove the distortion introduced by Embedding processaftercover restoration.Itisanimportant property thatcanbeused for manyscenarios,suchasmedicalimagery,military imageryandlawforensics.Formost of thisreason,RDHbecomes an importanttopicandisextensivelystudiedoverthe years. Recently manyRDHtechniqueshavebeenproposed basedon3fundamentalstrategies:losslesscompression-appending scheme [1],differenceexpansion(DE) [3] and histogramshift(HS) [5]. Recentlycombinedthe strategiestoresidualsoftheimagesuchaspredictionerrors (PE) [6] toachieve thebetterperformance.Almostallstate of the artRDHalgorithmsconsistoftwosteps.Thefirststep generateahostsequencewiththe smallentropy,i.e.,thehost has asharphistogramwhichusuallycanberealizedbyusing PE combinedwiththesortingtechnique [10] orpixelselection . Theseconds stepreversiblyembedsthemessageinthehostsequenceby modifyingthehistogramwithmethodslike Histogram Shift andDE.

In 2003, proposed the lossless watermarking algorithm based on circular interpretation ofbijective transformation [2]. In this approach, the histograms of pixel values are mapped to a circle. The comparative orientation of the histograms of 2 groups of pixels hide only 1 bit of an hiding message. Therefore, the scheme can achieve the hiding capacity is low. Later, Tian [3] proposed a scheme for reversible data hiding referreddifference expansion (DE) based on the addition rather than replacement. In this scheme theredundancy between the two neighboring pixels was determined and the secret data to beembedded, with the difference value and expanding the new difference value by2.

In 2004, Alattar[11] proposed a reversible watermarking for color images by using an integer transform for the DE. Kamstra et al. [7] improved the DE scheme byusing sorting method to increase the efficiency of lossless compression. Thodi[4] proposed aprediction-error expansion approach that can bebetter for exploit the correlation inherent in theneighboring of a pixel than the DE scheme.

In 2006, Ni et al. [5] proposed a RDH technique based on histogramshifting. The scheme used the minimapoint and peak point of the histogram of image to hidethe message and achieved reversibility. In 2008, Lin et al.[8] proposed a reversible data hiding based on histogrammodification of difference of image pixel is generated from the linear prediction scheme. They also proposed to apply the technique for many times in order to achieve high embeddingcapacity.

2. PREVIOUS ARTS

In previousmethods of [12]–[14], the encrypted 8bit grayscale imagesare generated by encryption domain every bit-planes with a streamcipher. The method in [12] segments the encrypted image into anumber of nonoverlapping blocks sized by a x a ; each block isused to carry 1 additional bit. To do this, pixels in each blockare pseudo-randomly divided into two sets S1 and S2 accordingto a data hiding key. If the additional bit 0 is to be embedded, flip the 3 LSBs of each encrypted pixel in S1, or else flipthe 3 encrypted LSBs of pixels inS2 . For data extraction andimage recovery, the receiver flips all the 3 LSBs of pixels into form a new decrypted block, and flips all the three LSBsof pixels in to form another new block; one of them willbe decrypted to the original block. Due to the spatial correlation innatural images, original block is to be much smootherthan interfered block and embedded data can be extracted correspondingly.However, there is a risk of defeat of data extractionand image recovery when divided block is to relatively small (e.g., a=8) or has much fine-detailed textures.

Hong *et al.* [13] reduced the error rate of Zhang'smethod [12]by fully exploiting the pixels in calculating the smoothness ofeach block by using the side match technique. The extraction and recovery ofblocks are well performed according to the

2) For embedding rate of RDH , the PSNR of decrypted image containing the embedded data are significantly to be improved; and for the acceptable PSNR, range of the embedding rates is greatly enlarged.

The content owner reserves enoughspace on the original image and then converts the image into its encrypteddomain with the encryption key. Further the data hiding process in encrypted images is reversible for thedata hider only needs toaccommodate data into the sparse space previous method emptied out. The data extraction and image recoveryare identical to that of Previous work. Obviously, standard RDH technique

descending order of theabsolute smoothness difference between two

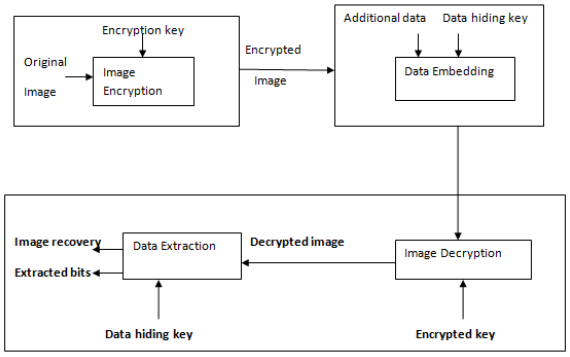

Fig 1 RDH in Encrypted image with non overlapping block

candidate blocksand recovered blocks can further be used to calculate the smoothnessof unrecovered blocks, which is meant by side match.Zhang's method in [14] pseudo-randomly permuted and dividedencrypted image into a number of groups with size ofL. The P LSB-planes of each group are compressed with aparitycheck matrix and the vacated room is used to embed data.

The method try to vacate room from the encrypted image directly.

3. PROPOSED METHOD

The Proposed method for RDH ,"Reserve room before encryption". Here we first empty out room by embedding the LSBs of some pixels inimage partition into other pixels with a traditional RDH method and then encrypt the image, The positions of these LSBs in the encrypted image can be used to hide the data. Not only the proposed method is toseparate data extraction from image decryption but also achieve the excellent performance in 2 different prospects: 1)Real reversibility can be realized, data extraction and image recovery are free of error.

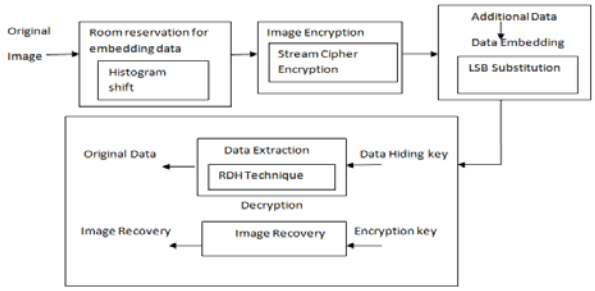

Fig 2 .Architecture Diagram for "Room Reservation Before Encryption"

are the ideal operator for room reserving before encryption and can be easily applied to RRBE to achieve the better performance compared with side match technique. The proposed method based on the "Room reservation before Encryption", which consists of five stages :Image partition,Self reversibleembedding process, image encryption, data extraction and image recovery.

4. IMPLEMENTATION

1.Image Partition :

Reserving room before encryption is a traditional RDH technique ,so the goal of partitioning the image is to construct a smoother area B.The content owner who has select the particular block with the highest to be A and put it to the front of the image concatenated by the rest part of the B with fewer textured areas.

2.Self Reversible Embedding

Selfreversible embedding is to embed the LSB-planes of A into B by employing Histogram shift technique. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. To implement the data embedding scheme to accommodate the additional data.

Steps:

1. Assume the original image is an 8 bits representation of gray scale image with its size MxN .
2. Check the pixel $C_{i,j} \in [0,255]$, $1 \le i \le M, 1 \le j \le N$.
3. First, the owner has to extracts from the original image, along the rows, several overlapping blocks whose number is determined by the size of to be embedded messages, denoted by l.
4. Every block consists of m rows, where m=l/N and the number of blocks can be computed .
5.For each block to measure its first order smoothness.

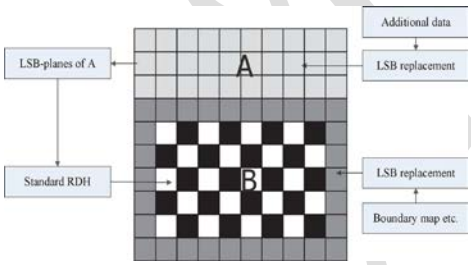

Fig.3 Partitioning Image and self reversible embedding.

Histogram shift Modification:

The Reversible data hiding scheme based on histogram shift modification technique. The technique which has toconstruct the histogram based on the neighbor pixel differences instead of the host image's histogram .

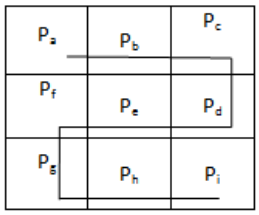

Fig .4 Pixel of inverse 'S' scan of 3 x 3 image block.

The estimating error $e_{i,j}$ is calculated and then some data can be embedded in to the estimating errorsequence with histogram shift. After that, To calculate the estimating errors of black pixels with the help of surrounding white pixels that may have been modified. Then another estimating error sequence is generated which can accommodate messages as well. Histogram shift, some messages can beembedded.

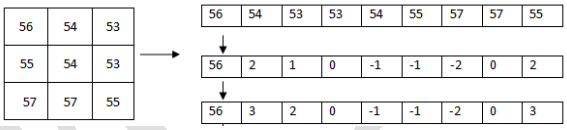

Fig .5 Example for Pixel scan

3.ImageEncryption

The reversible data hiding in encrypted image is investigated in [14]. Most of the work on reversible data hiding focuses on the data embedding or extracting on the plain spatial domain. A content owner encrypts the original image with the help of an encryption key, and a data-hider can embed additional data into the encrypted image with the help of a data-hiding key though he does not know the original content.

After rearrange the self reversible embedded image ,denoted by b. The owner can encrypt b to construct the encrypted image B. Assume the image with a size of N1 * N2 is and each pixel with gray value falling into [0, 255] which has represented by 8 bits.

By denote the bits of a pixel as $b_{i,j,0}$,$b_{i,j,1\ldots}$,$b_{i,j,7}$ where $1 \le i \le N1$ and $1 \le j \le N2$, the gray value as $P_{i,j}$ and the number of pixels as N (N= N1 * N2).

In encryption phase, the X-OR results of the original bits and pseudorandom bits are calculated$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u}$

where $r_{i,j,u}$ are determined by an encryption key using a standard stream cipher. Then,$B_{i,j,u}$ are concatenated orderly as the encrypted data.

4. DATA EMBEDDING

In the data embedding phase, parameters are embedded into a small number of encrypted pixels. Once the data hider acquires the encrypted image, the data hider can embed some data into it, though he does not get access to the original image. The embedding

process starts with locating the encrypted domain of A which has denoted by A_E. Since A_E has been rearranged to the top of E, it is effortless for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After that knowing how many bit planes and rows of pixels the hider can modify,simply adopts LSB replacement to substitute the available bit planes with additional data . Finally, the data hider sets a label following m to point out the end position of embedding process and further encrypts m according to the data hiding key to formulate marked encrypted image.

In [5],Ni et al, introduced a reversible data hiding scheme based on histogram modification using pairs of peak point and zero points. Let P be the value of peak point and Z be the value of zero point. The range of the histogram,P+1, Z-1,is shifted to the right hand side by 1. Once a pixel with value P is encountered, if the message bit is "1",the pixel value is increased by 1.Otherwise, no modification is needed.

Steps for Histogram Shift Modification

1. Input an image of size M×N with the pixel grayscale values y, y∈ [0,255] .
2. Generate its histogram H(y).
3. Find a peak point (k) and a minimum point (b) in the generated histogram H(y). The peak point corresponds to the pixel value which has the largest occurrence in the image and the minimum point corresponds to the gray value which has the least occurrence in the image.
4. The whole image is scanned inverse s order. The scale values of the pixels between the peak (k) and zero point (b) are incremented by 1,i.e. the histogram is shifted to the right by 1 unit leaving the gray value b.
5. The whole image is scanned once again in the same order. If the gray value of a pixelequal to the peak value (k) is encountered the secret data bit is embedded into it. If the process to be embedded bit is '1', then the pixel value is incremented, i.e. 'k+1', otherwise, if it is '0'the pixel value is retained, i.e. 'a'.

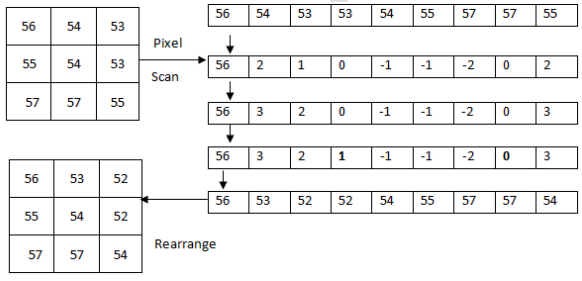

Fig.7 Example for Data Embedding

5.DATA EXTRACTION AND IMAGE RECOVERY

Both embedding and extraction of the data are manipulated in encrypted image. On the other hand, there is a different situation that the user wants to extract the image first by image encryption key or user want to extract data first by data encryption key when it is needed. Consider the three cases that the receiver has only the datahiding key, only the encryption key, and both the datahiding and encryption keys, respectively. In data extraction if the receiver has data hiding key then extract the data or if receiver has encryption key then decrypt the image.

Extracting Data from Encrypted images

The order of data extraction before image decryption guarantees in this case. When the receiver gets the data hiding key, he can decrypt the LSB-planes of A_E and extract the additional data by directly reading the decrypted version. When requesting for update the information of encrypted images, the database manager, then updates information through LSB replacement and encrypts updated information according to the data- hiding key all over again. All the process is entirely operated on encrypted image, it avoids the leakage of original content.

Extracting Data from Decrypted images

In the above case, both embedding and extraction of the data are manipulated in encrypted image. In this example,P_1 is obtained first, and then P_2, P_3, . . ., P_9 are recovered consecutively.

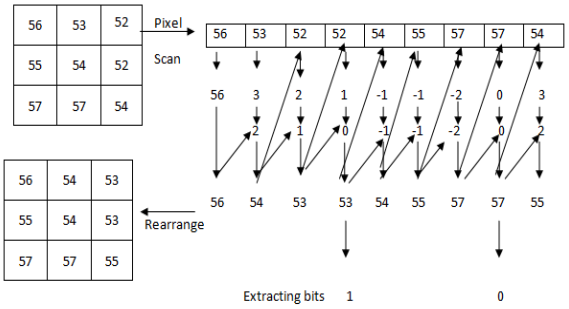

Fig : 8 Example of Data extraction and image recovery.

Steps for Data Extraction

Step 1 : The marked block is also inverse "S" ,scanned into a sequence first.

Step 2 :The first pixel is not changed during embedding, we have $P_1=P_1$ =56.

Step 3 : The difference $d_2=P_1-P_2$ =3. Obviously ,its counterpart d_2 =2. Thus the original pixel associated with P_2 is $P_2=P_1-d_2$ =54.

Step 4 : Next, to obtain $d_3=P_2-P_3$ =2, and its counterpart d_3 =1.Then $P_3=P_2-d_3$ =53.

Step 5 : Repeat these operations for the marked pixels and all the host pixels are recovered.

Step 6:One bit secret data "1" is extracted from P_3-P_4' = 1 and "0" is extracted from P_7-P_8' = 0.

6. CONCLUSION

Reversible data hiding by reserving room before encryption which consists of some phases. In the first phase the owner select the particular block of image for partition. The next phase using Histogram shift technique the space is saved for data embedding. After that using stream cipher the image has to be encrypted then the data hider hides the data in the partition of LSB plane. The next phase if a receiver has the data-hiding key, he can extract the additional data. If the receiver has the encryption key, he can decrypt to obtain the image similar to the original , but cannot extract the additional data.

REFERENCES

[1] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats,"inProc. SPIE Proc. Photonics West, San Jose, CA, USA,Jan. 2002, vol. 4675, pp. 572–583.

[2] C. D. Vleeschouwer, J.F. Delaigle and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Trans. on Multimedia, vol.5, no.1, pp.97–105,2003.

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

[4]D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3,pp. 721–730, Mar. 2007.

[5]. 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.

[6] P.Y. Tsai, Y.C. Hu, H.L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing 89 (6) (2009) 1129–1143.

[7] L. Kamstra and H. J. A .M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," IEEE Trans. on Image Processing, vol.14, no.12, pp.2082–2090, 2005.

[8]C.C. Lin, W.L. Tai, C.C. Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recognition .

[9] K. Kim, M. Lee, H. Lee, H. Lee, Reversible data hiding exploiting spatial correlation between sub-sampled images, Pattern Recognition 42 (11) (2009) 3083–3096.

[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. pp. 989–999, Jul. 2009.

[11] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Trans. Image Process., vol.13, no. 8, Aug. 2004.

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

[13] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol.19, no. 4, pp. 199–202, Apr. 2012.

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