International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Data Hiding in Reviser Room for Embedded Before Encryption

Achuri Srilakshmi[1]& D. Vijay Kumar[2]
[1]M.Tech, Dept of ECE, VijayaEngineering College, Telangana,India.
Email:sriprasannaachuri@gmail.com
[2]Associate Professor, HOD, Dept of ECE,Vijaya Engineering college, Telangana,India,
Email: vkumar88.d@gmail.com

Abstract
Data hacking is very challenging problem in today's internet world. There are number of techniques to secure the data. So, the data hiding in the encrypted image comes into the picture, but occurrence of distortion at the time of data extraction is a main problem. So Reversible Data Hiding (RDH) in encrypted image is used. With this method original cover can be recovered. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method provides improved PSNR ratio and recovers image with its original quality.
Keywords: Reversible Data Hiding (RDH); image encryption; histogram shift

1. Introduction

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest.

In theoretical aspect, Kalker and Willems [1] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. Zhang *et al.* [2], [3] improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers.

In practical aspect, many RDH techniques have emerged in recent years. Fridrich*et al.* [4] constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE) [5], in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS) [6], in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods [7]–[11] usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance.

With regard to providing confidentiality for images, encryption [12] is an effective and popular means as it converts the original and meaningful content to incomprehensible one. In [13], Hwang *et al.* advocated a reputation-based trust-management scheme enhanced with data

coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data coloring technique based on encrypted data is preferred. In [16], Zhang divided the encrypted image into several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image. Hong *et al.* [17] ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve much lower error rate.

In the present paper, we propose a novel method for RDH in encrypted images, for which we do not "vacate room after encryption" as done in [16]–[18], but "reserve room before encryption". In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- ✓ Real reversibility is realized, that is, data extraction and image recovery are free of any error.
- ✓ For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

2. Related Work

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.

Reversible data hiding (RDH) in images is atechnique, by which the original cover can belosslessly recovered after the embedded message isextracted. This important technique is widely used inmedical imagery, military imagery and law forensics,where no distortion of the original cover is allowed.Since first introduced, RDH has attractedconsiderable research interest [1]. Kalker andWillems [2] established a rate-distortion model forRDH, through which they proved the rate-distortionbounds of RDH for memory less covers and proposeda recursive code construction which, however, doesnot approach the bound. Some attempts on RDH inencrypted images have been made.

As when data is embedded into the image then thereis occurrence of distortion in an image. So it isexpected that after the data extraction the imagequality should be maintained like the original image.But that image contains some distortions. With regardof distortion in image, Kalker and Willems[1]established a rate-distortion copy for RDH ,throughwhich they showed the rate-distortion bounds ofRDH for without memory covers and proposed

arecursive code development which, however, doesnot move towards the bound [3].

In this they usedtheencoding and decoding as, Another promisingstrategy for RDH is histogram shift (HS), in whichspace is saved for data embedding by shifting the binsof histogram of gray values. In this process the dataembedding process is done in three steps as first thehistogram is drawn then the peak point is taken intoconsideration then whole image is scanned row byrow. Then once again the image is scanned & thegrayscale value 154 is encountered then theembedded data sequence is checked & we get themarked image. Then the data extraction is done. Toget the original cover quality the process of histogramshift is applied again.

Then the original cover is getback. Basically data hiding is the process to hide thedata into some covering media. That is it is theconcatenation of two blocks of data, first isembedding data & second is covering media. But inmost of the cases the covering media gets distortedafter the data is embedded & the covering media isnot inverted back to its original form after data isremoved from it. So, to maintain the quality of animage reversible data hiding i.e. RDH techniques areused. Some reversible data hiding methods uses theconcept of differential expansion transform which is based on hoar wavelet transform. Another conceptused is the histogram shift. The differential expansion

2.1 Proposed Scheme:

As we know loss lessly vacating rooms from the encrypted images is comparatively intricate and at times unproductive, why are we still so fanatical to discover novel RDH techniques running directly for encrypted images? Imagine if we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side. The RDH tasks in encrypted images would be more natural and much easier which guide us to the novel framework, “reserving room before encryption (RRBE)”. As shown in Fig. 1(b), the content owner first reserves adequate space on original image. Then translate the image into its encrypted version with the encryption key. Now, the data embed-ding process in encrypted images is essentially reversible. Data hider only needs to have room for data into the spare space previous emptied out.

The data extraction and image recovery are indistinguishable to that of Framework VRAE. Noticeably, standard RDH algorithms are the best operator for reserving room before encryption. This can be effortlessly applied to Framework RRBE to realize better performance compared with techniques from Framework VRAE. Reason is, in this new framework, we pursue the customary idea that first losslessly compresses the unneeded image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy. In the proposed method (Fig 1(b)),

1. We first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method.

2. Then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data.

This proposed method does below:-

1. Separate data extraction from image decryption

2. Achieves excellent performance in two different prospects:

a. Real reversibility is realized, that is, data extraction and image recovery are free of any error.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

b. For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is significantly enlarged.

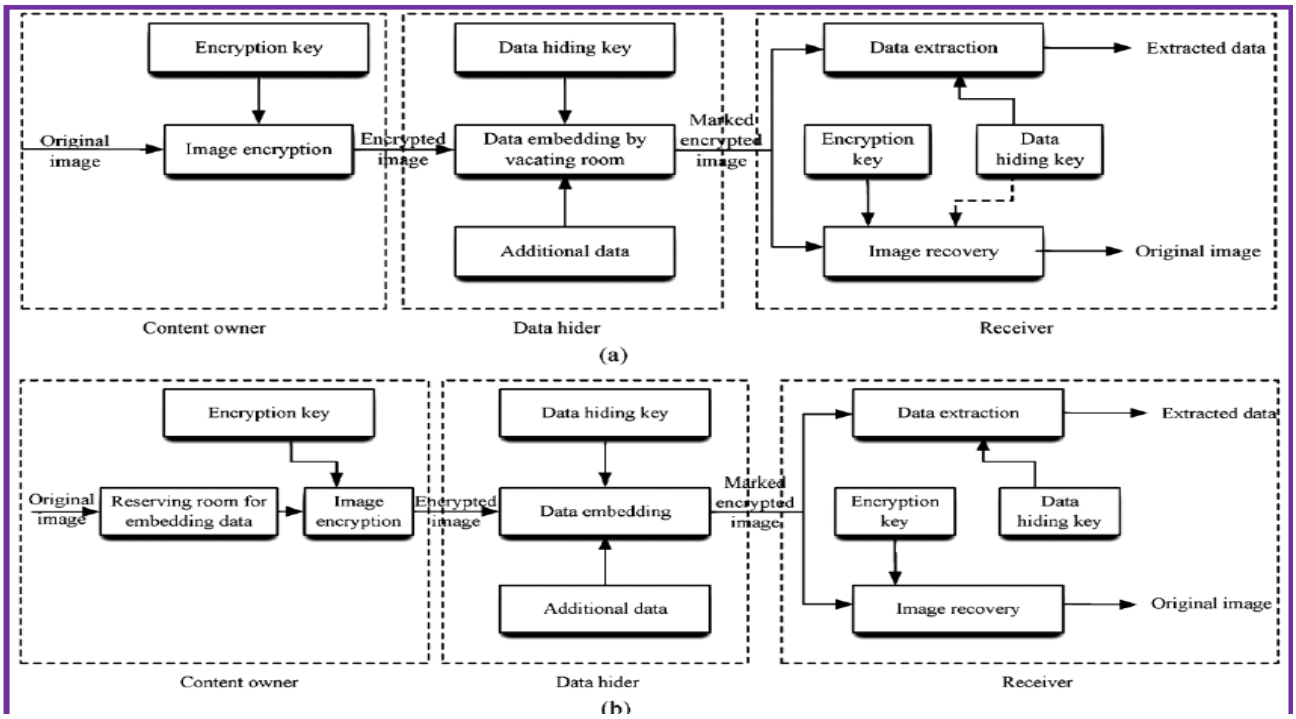

Fig 1: Framework: "vacating room after encryption (VRAE)" versus framework: "reserving room before encryption (RRBE)." (Dashed line in (a) states that the need of data hiding key in image recovery varies in different practical methods). (a) Framework VRAE. (b) Framework RRBE.

3. Implementation

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.

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 $C_{i,j}$ 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

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

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].

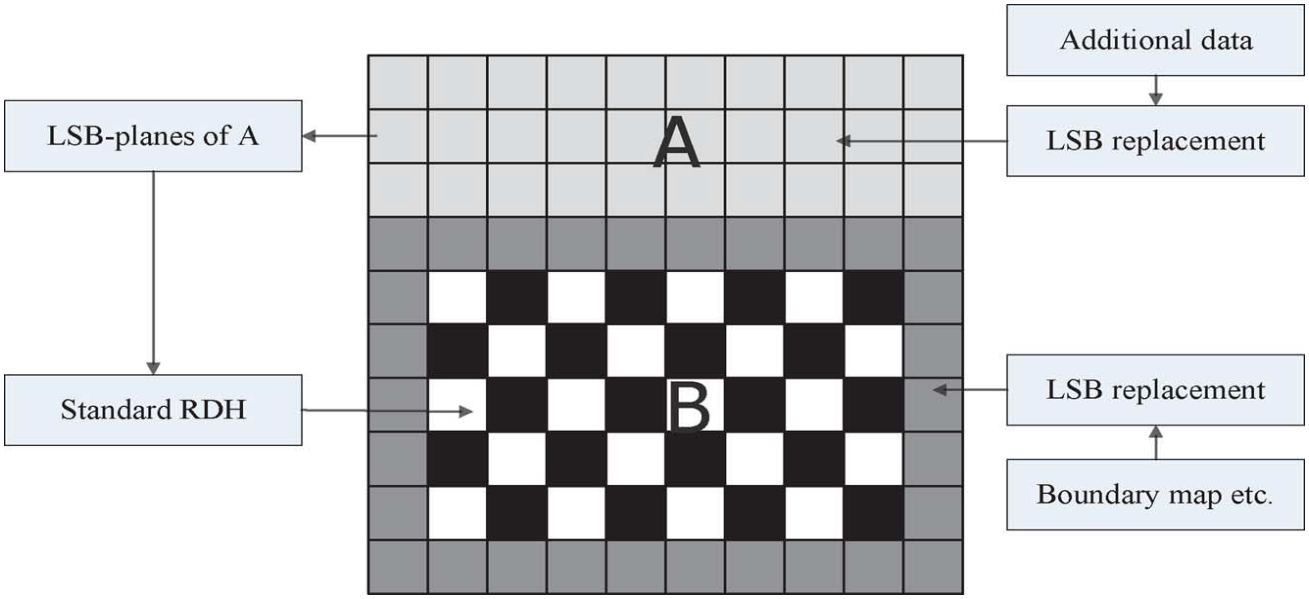

Fig 2: Illustration of image partition and embedding process[1].

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 asfollows

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

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

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

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 Xi,j(k)=[Xi,j/2k]mod2, k=0,1,….7 Exclusive- or operation can be used for obtaining encrypted bits

$$E_{i,j}(k) = \bar{X}_{i,j}(k) \oplus r_{i,j}(k)$$

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,

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

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

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

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].

4. Experimental Results

(a) (b) (c) (d)

Fig.(a) Original image, (b) encrypted image, (c) decrypted image containing messages (embedding rate 0.1 bpp), (d) recovery version.

5 Conclusion

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

6. References

[1] 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.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for Reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," In Proc. SPIE Proc. Photonics West, Electronic Imaging, Security And Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

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

[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] 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.

[7] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking Based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process. vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

ACHURI SRILAKSHMI pursuing her M.Tech, from Vijaya Engineering College, Telangana, India. Email:sriprasannaachuri@gmail.com

D. Vijay Kumar completed his M.Techand working as a Associate Professor, HOD,HOD,14-years ExperiencefromVijaya Engineering college, Telangana,India, Email: vkumar88.d@gmail.com