ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Reversible Data Hiding With Lossless Data Embedding Technique for Data Security

Reshmi R., Sheeja Agustin

Department of Computer Science, Marian Engineering College, Kerala University, Kerala, India

ABSTRACT: Reversible data hiding in encrypted images has attracted considerable attention from the communities of privacy security and protection. Reversible data hiding in encrypted images (RDH-EI) has got some promising applications in cloud storage, medical imaging, forensics etc. It has gained considerable research interest in recent years. In this project, we proposed LFSR based pseudo random key generation. Security is achieved in this by using Boolean functions to combine the state bits of the LFSR key stream generator. This approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Our proposed system gives security of the system by providing secret data with key. Finally, we perform a theoretical analysis including correctness and security of LFSR management key system and also present a performance comparison of the proposed scheme with existing ones. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR=55 dB.

KEYWORDS: Image encryption, image recovery, reversible data hiding in encrypted images

I. INTRODUCTION

Data hiding is the general term for embedding message into the covers such as image, audio and video files. The term hiding means making the information imperceptible or keeping the existence of the information secret which is used for integrity, authentication, media notation, etc. The image that will be embedded the secret data is called the cover image or otherwise called as the stego image. A reversible data hiding, which is also called a distortion-free or lossless data hiding, is a technique that not only embeds the secret data into cover images, but also used for restoring the original images from the stego images after the embedded data have been extracted. In our previous work, many reversible data hiding schemes were proposed, and most of them use the following techniques: lossless compression technique, difference expansion technique (DE), histogram shifting technique (HS), Interpolation technique are introduced.. 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. In practical aspect, many RDH techniques have emerged in recent years.

Fiddich et al. [1] 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) [2], 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. M. Johnson, P. Ishwar proposed the Compressing Encrypted Data[3] .In this first encrypting and then compressing the encrypted source. The compressor does not have access to the cryptographic key, so it must be able to compress the encrypted data (also called cipher text) without any knowledge of the original source[3]and Z. Ni, S. Wei, proposed “Reversible data hiding" technique[4]., 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. D.M. Thodi and J. J. Rodriguez proposed the “Expansion embedding techniques for reversible watermarking"[5]. Digital watermarking is a method of embedding useful information into a digital work (especially, thus, audio, image, or video) for the purpose of copy control, content authentication, distribution tracking, broadcast monitoring, etc. The distortion introduced by embedding the watermark is often constrained so that the host and the watermarked work are perceptually equivalent. 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 grey values. The state-of-art methods [2]–[6] 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 is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images have beenpublished yet, there are some promising applications if RDH can be applied to encrypted images.

Some attempts on RDH in encrypted images have been made. Zhang, proposed “Reversible data hiding in encrypted images[7][8][9]".Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. In difference expansion method, differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. A data hider can also perform reversible data hiding using a histogram shift mechanism, which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel grey values to embed data into the image.

In [8], 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. [9] ameliorated Zhang’s method can be summarized as the framework, “vacating room after encryption (VRAE)”, In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

II. RELATED WORK

To separate the data extraction from image decryption RDH in encrypted images, for which we do not “vacate room after encryption” as done in [9]. But “reserve room before encryption” [10]. In these, 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 these 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

However, there is a risk of defeat of bit extraction and image recovery when divided block is relatively small (e.g.,) or has much fine-detailed textures. Using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data.

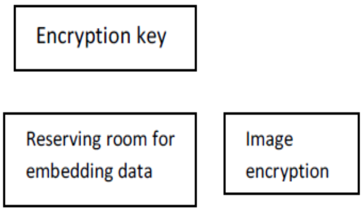

Fig 1: framework reserving room before encryption (RRBE)

If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large [10].Here data hiding key is not safe .If anybody or unauthorized know the about the encryption key can easily decrypted the image and access the secrete data .so that it has many limitations, lot of time consumption and some distortion will happened into the original image after the data is extracted.

III. PROPOSED ALGORITHM

Here, we take all advantages of RDH and “reserving room before encryption (RRBE)” [10] techniques are used. By analysing all previous techniques, we can understand that the security of keys is very less. So in order to improve the security of keys, we use LFSER (Linear Feedback Shift Register) techniques. Next, we elaborate a practical method based on the Framework “RRBE”, which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. Note that the reserving operation we adopt in the proposed method is a traditional RDH approach. As shown in Fig. 2, the content owner first reserves enough room for data hiding and encrypt the original image using an encryption key, and a data hider use LFSR for generating LFSR code. LFSER (Linear Feedback Shift Register) is popularly known as pseudo-random number generator. The random number repeats itself after 2^n-1 clock cycles (Wheren is thenumber bits in the LFSR).

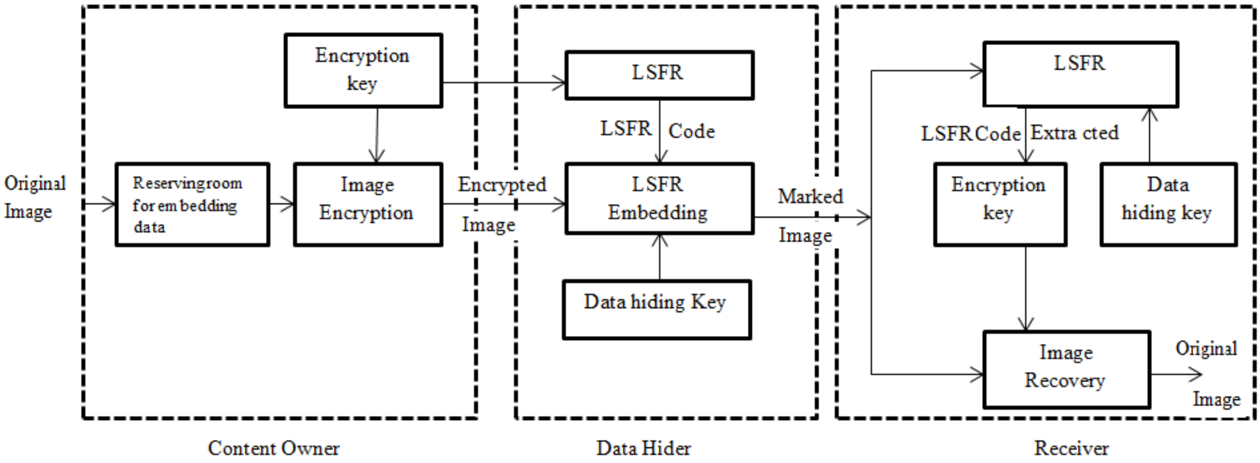

Fig 2.Frame work for RRBE using LFSR

Here, the LFSR code is the additional data. The data hider can embed additional data into the encrypted image using another data-hiding key though he does not know the original content. The LFSR method is also contain in the receiver side also. With an encrypted image containing additional data, a receiver may first decrypt LFSR code according to the data hiding key, and then extract the embedded LFSR code data and recover the original image according to the data-hiding key. For example, the content owner will encrypting the image by using the key as 12 .Then these key is implement into the LFSR method and get LFSR code is 2054.The data hider will hide these LFSR code into the encrypted image. In the scheme, the data extraction is not separable from the content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data hiding key but not the encryption key, he cannot extract any information from the encrypted image containing additional data. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version.

Linear Feedback Shift Register (LFSR)

LFSR is an acronym for Linear Feedback Shift Register. Due to LFSR is easy to constructed and implemented by software and hardware, so that it can be used to as a Good key Stream generator. A LFSR consists a shift register and a linear feedback function of its previous states. As shown in Figure the shift register is sequence of M flip flops, BM to BM-1, where each flip flop holds a single bit. The flip flops are initialized to an M-bit word called the Seed. As shown in Fig 3, BM is a linear function of B0, B1, B2… BM-1. Shift register can be divided according to its type of inputs and outputs. For example serial inputs and parallel outputs or parallel inputs and serial inputs.

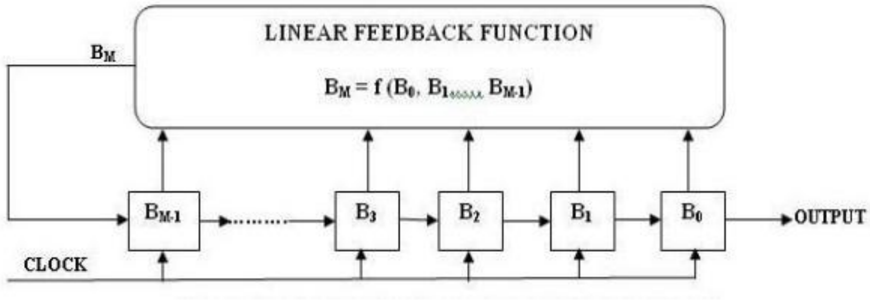

Fig 3. Block Diagram of LFSR Design

.

IV. RESULT AND DISCUSSION

In this module we compare the performance of the existing and the proposed system shows PSNR and Time consumption. PSNR is most easily defined via the mean squared error (*MSE*). Given a noise-free *m*×*n* monochrome image *I* and its noisy approximation *K*, *MSE* is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 10.\,log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

Here, 256 Gray scale images are used.

$$\text{PSNR}=10.\log_{10}\left(\frac{255 * 255}{MSE}\right)$$

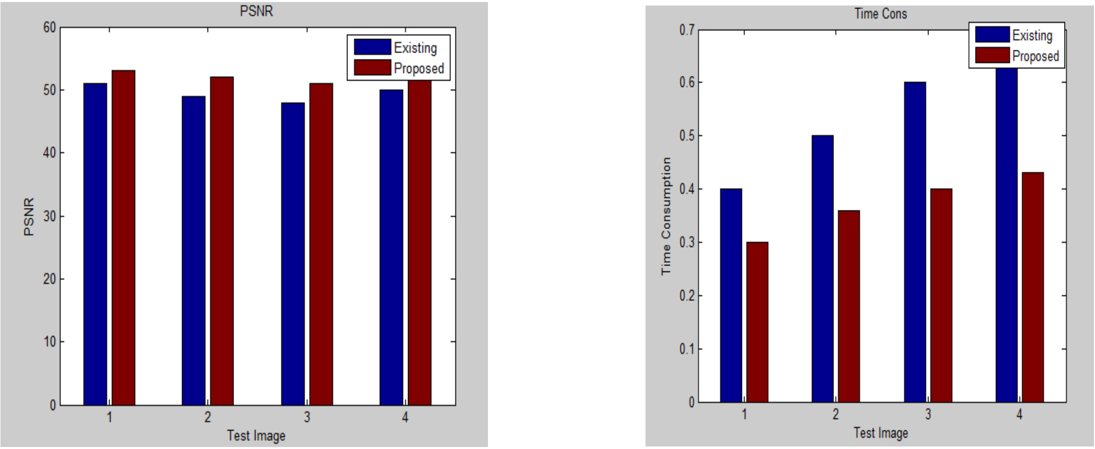

Fig 4(a) PSNR comparison and 4(b) Time consumption

Figures 4 shows, the comparison of PSNR and time consumption between the existing and this proposed system. By using the LFSR method, the time consumption is less in proposed system .Here, LFSR code is used as the data. So embedding rate of key is 0.2(bpp). Thus embed rate is less. On the receiver side also we have used LFSR method. So easily decrypted the data with in small time. From the graph 4(a), X-axis showed tested different images like Ship, Baboon, Barbara and Boat etc. and y-axis shows the corresponding the PSNR value of different test images. The graph 4(b),X-axis showed tested different images and y-axis shows the corresponding time consumption different test images. The highest PSNR value of existing system is 52.3 and the highest PSNR value of proposed system is 55.4 .The good quality of image contain high PSNR value. It is found that accuracy of data hiding capacity and PSNR is higher than existing system and the time consumption is relatively less.

V. Conclusion

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. The proposed method can take advantage of all traditional RDH techniques, “RRBE”and LFSR method for plain images and achieve excellent performance without loss of perfect secrecy. In this paper the image is taken from database and hiding the information or message is stored in that image for security purpose. After that it sends to the receiver. The receiver extracted that original message from stego image. I.e. the image with hiding data called as stego image. The proposed system increased the hiding capacity, key secrecy and PSNR value.

References

[1] 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.
[2] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
[3] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[4] 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.
[5] 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.
[6] P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” *Signal Process.*, vol. 89, pp. 1129–1143, 2009.
[7] L. Luo et al., “Reversible image watermarking using interpolation technique”,IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[8] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett, vol. 18, no. 4, pp. 255–258, Apr. 2011.
[9] W. Hong, T. Chen, and H.Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Letts, vol. 19, no. 4, pp. 199–202, Apr. 2012.
[10] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

BIOGRAPHY

Reshmi R is M Tech student in Department of Computer Science, Marian Engineering College, Kerala University, Kerala, India. She received Bachelor of Computer Science (BE) degree in 2011 from Anna University Chennai, Tamilnadu, India.

Sheeja Agustin is Associate professor in Department of Computer Science, Marian Engineering College, Kerala University, India.