IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331,
PP 58-63
www.iosrjournals.org

Reversible Data Hiding in Encrypted Image with Logistic Substitution Encoding

Sruthi K V[1], Sreetha Sreedhar[2]
[1](Electronics and Communication Engineering, Malabar Institute of Technology, India)
[2](Electronics and Communication Engineering, Malabar Institute of Technology, India)

Abstract: *A scheme is proposed to implement reversible data hiding (RDH) in encrypted images using logistic substitution encoding. The original image is encrypted by the content owner using logistic substitution encoding. Then the data hider modifies the bits taken from the encrypted image to accommodate the secret data. On the receiver side, the secret data can be extracted if the receiver is available with the embedding key only. If the receiver has the encryption key only, original image can be recovered. If both the embedding and encryption keys are available at the receiver side, he/she can extract the secret data and recover the original image using logistic substitution decoding. The scheme is a good choice for secure image transmission.*
Keywords: *Image encryption, image recovery, image transmission, reversible data hiding.*

I. Introduction

With the rapid development of Internet technology, such media data as images, audios or videos are used more and more widely in human's daily life. This makes media data not only easy to be transmitted, but also easy to be copied and spread out. Thus, the legal issue rises that some media data should be protected against unauthorized users or operations.

In some cases, the content owner may not trust the service supplier, and needs to encrypt the data before uploading. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Some works have been done for data processing in encrypted domain, such as, compressing encrypted images [1],[3]adding a watermark into the encrypted images [2], and reversibly hiding data into the encrypted image [4-7]. The reversible data hiding in encrypted images allows the service supplier to embed additional messages such as image metadata, labels, notations or authentication information inside the encrypted images without accessing the original image. The original image along with the secret data is required to be recovered at the receiving side. Reversible data hiding is desirable. For example, to protect the patient's privacy, content of the medical image might be unavailable for the technician who embeds the information into the medical image.

In this paper, we propose a separable reversible data hiding method for encrypted images using logistic substitution encoding. With the two different keys, the system is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed using the encryption key. With both keys available, the hidden data can be completely extracted, and the original image perfectly recovered. The proposed method avoids the operations of room-reserving by the sender.

The rest of the paper is organized as follows. Previous works of RDH in encrypted images are surveyed in Section II. The proposed system is described in section III, which presents the procedure of image encryption, data embedding, data extraction and image recovery. Section IV presents the experimental results. Section V concludes the paper.

II. Previous Works

The security of images has been extensively studied. These studies are briefly described as follows.
The existing methods of reversible data hiding can be mainly classified into two types: "vacating room after encryption (VRAE)" and "vacating room before encryption (VRBE)" [7]. RDH for encrypted image are usuall

designed for the applications in which the content owner and the service data hider are not the same person. The original image is encrypted directly by the sender and data hider adds the secret bits by modifying some bits of the encrypted data. This is the method of VRAE. In [4], the owner encrypts the original image by Advanced Encryption Scheme (AES), and the data hider embeds one bit in each block. On the receiving side, data extraction and image recovery are realized by analyzing the local standard deviation during decryption of encrypted image. Here data extraction and image decryption are inseparable.
In [7], Zhang divides the encrypted image into blocks, and embeds one bit into each block by flipping 3

LSBs of the half pixels in the block. Hong et al. [6] provided an improved version of Zhang's method, by exploiting the correlation of the border of neighboring blocks, and using the side match algorithm to achieve a lower error rate. To resolve the problem of inseparability, Zhang further proposed a separable RDH scheme for encrypted image by compressing the encrypted data using source coding with side information [8], which guarantees the data extraction independent from image encryption.

In [5], Ma et al. provided a RDH idea in encrypted images by reserving room before encryption. This method empties out room by embedding LSBs of some pixels into other pixels with the traditional RDH method and then encrypts the image on the sender side, and as a result, positions of these LSBs in the encrypted image can be used for data hiding by the data hider. Although this method greatly improved the embedding capacity, an additional RDH has to be implemented by the sender, which might be impossible to the users, because RDH in encrypted image always requires the sender to do nothing except encryption and the embedding tasks are always supposed to be accomplished by the data-hider.

The methods in both VRAE and VRBE categories are effective for RDH in encrypted images. However, there are some limitations. In VRAE RDH methods for encrypted images, estimation technique is necessary for the receiver, because no prior information of original image is available. Although VRBE can achieve a higher embedding payload, it requires that the sender must perform an additional RDH before image encryption.

III. Proposed System

Sketch of the proposed system is shown in Fig. 1. The system mainly consists of three phases: image encryption, data embedding and data retrieval/image recovery. In the first phase, the original image is encrypted to form the encrypted data using an encryption key. The encrypted data are sent to the data hider who embeds the secret data into the encrypted data using an embedding key in the second phase. There are three cases for the receiver to extract secret bits or recover the image. In the third phase, if the receiver has only the embedding key, he/she can extract the secret data independently. If he has only the encryption key, he can approximately recover the original image. If both the embedding key and the encryption keys are available for the receiver, the secret bits can be extracted and the original image can be perfectly recovered. Details of the procedure are as follows.

3. 1 Image Encryption

The password for encryption is chosen by the content owner as encryption key. The original image **O** is a grayscale image with all pixel values falling into [0, 255], and the image size is $M \times N$ where both M and N are power of 2. Primarily, the image owner turns the original image into plain bits by decomposing each pixel into 8 bits using the equation (1):

$$b_{i,j,u} \quad [O_{i,j} / 2^{u}] \bmod 2 , \qquad u = 0, 1, 2, \ldots, 7 \tag{1}$$

A chaotic map is created using logistic substitution encoding using the equation (2):

$$x' \quad a * x * (1 - x) \tag{2}$$

Now the stream cipher encrypts the bit stream of the original image by equation (3):

$$e_{i,j,u} \quad b_{i,j,u} \approx k_{i,j,u} , \qquad u = 0, 1, 2, \ldots, 7 \tag{3}$$

Where $k_{i,j,u} \in x'$, are the key stream bits, $e_{i,j,u}$ the generated cipher text, and $\oplus$ denotes exclusive OR.
The encrypted image **E** can be constructed by equation (4):

$$E_{i,j} \quad \hat{\sum}_{u=0} e_{i,j,u} \, 2^{u} \tag{4}$$

$E_{i,j}$ are pixel values of encrypted image, $1 \le i \le M$, $1 \le j \le N$.

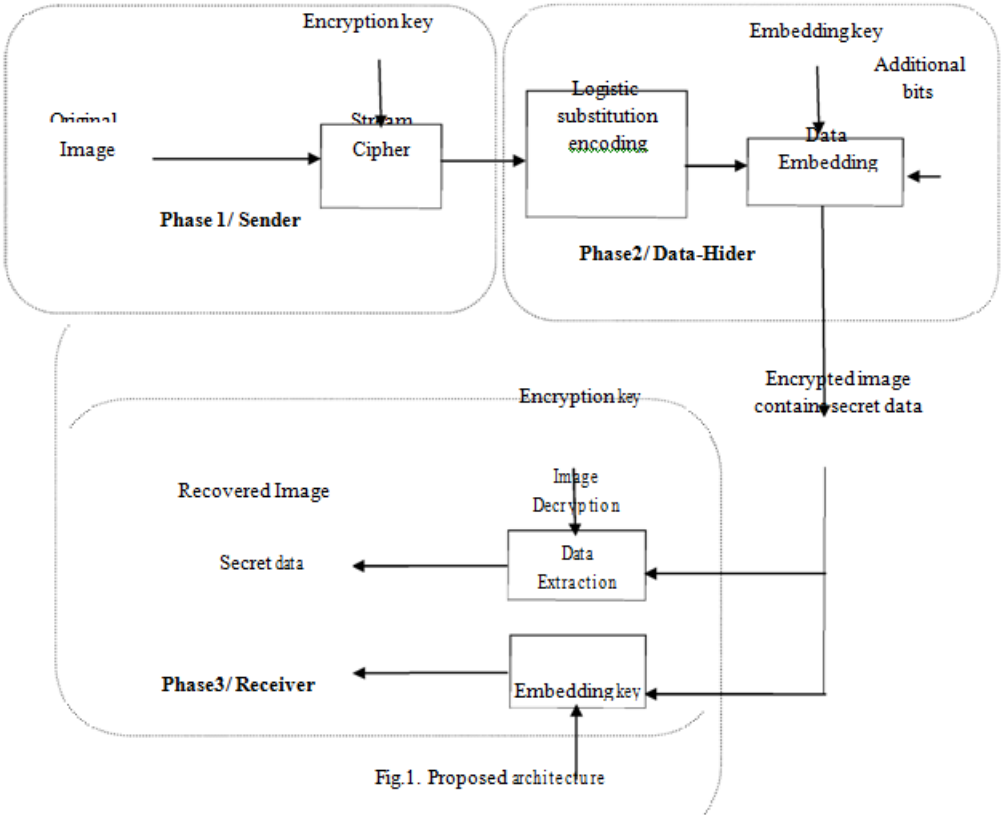

Fig.1. Proposed architecture

3.2 Data Embedding

After creating the encrypted form of original image, the content owner sends the encrypted image to the data-hider. An embedding key is chosen by the data hider for the secrecy of the data. The size of the data is calculated and it should be less than the encrypted image. The data is now embedded in the encrypted image by resizing the encrypted image.

3.3 Data Extraction and Image Recovery

On the receiving end, the encrypted image contains data is available. If the encryption key is available, image recovery is done by the logistic substitution decoding. This is the reversal process of Section A. If the embedding key is available at the end, data extraction is done by subtracting the values from the processed image, which is the reverse of Section B.

IV. Experimental Results

Our proposed method is verified using standard gray images and color images, all sized (256×256).

Fig. 2 illustrates a group of experimental results with Flower image. The original image in Fig. 2(a) is encrypted using stream cipher is shown in Fig. 2(b). It should be noted that, here the encryption process is carried out in two steps. Fig. 2(b)(i) shows the output of encryption operation-1 and Fig. 2(b)(ii) shows the output of the encryption operation-2. Fig. 2(c) shows the resulting encrypted image containing secret bits respectively. The hidden text (secret data) extracted is shown if Fig. 3

Similar to the encryption, decryption also performed in two stages. The output of decryption opration-1 and opration-2 is illustrated in Fig. 4(a) and 4(b). Along with the hidden text, length of the hidden text, number of bits available for data hiding, number of ASCII characters hidden also calculated. Because no operation is performed before image encryption, the proposed method is a kind of VRAE. With the encryption key only, an approximate image can be reconstructed with high quality. The two aspects of security is considered here. Security of the image content and the security of the additional message. The content owner does not allow the service supplier to access the original image. The data hider does not allow adversaries to crack the system for embedded message. The original image is encrypted with a stream cipher using an encryption key.

For the data hider, the additional bits are also protected with the embedding key. Data extraction and image reconstruction is separable in this method. The three different cases at the receiving end is hence solved here; with the encryption key only, with the embedding key only and with the two keys together.

Fig. 2(a) Original image

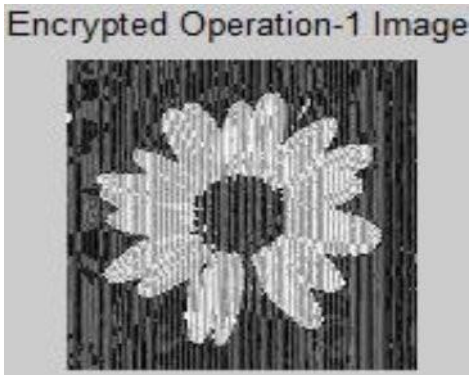

Fig. 2 (b)(i) Output of encryption opearation-1

Fig. 2 (b)(ii) Output of encryption operation-2

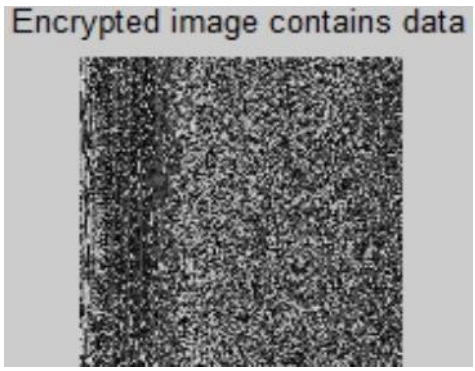

Fig. 2(c) Encrypted image contains secret data

Fig.2 Image encryption

Fig. 3 Extracted secret data

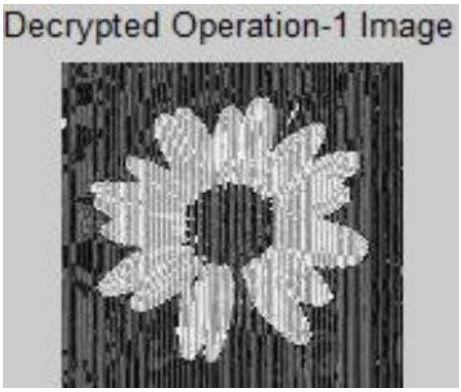

Fig. 4(a) Output of decryption-1

Fig. 4(b) Output of decryption-2
Fig.4 Image recovery

V. Conclusion

This paper proposes a system of reversible data hiding in encrypted images using logistic substitution encoding. After encrypting the original image with a stream cipher, encrypted image is modified for the additional secret data. On the receiver side, all hidden data can be extracted with the embedding key only, and the original image approximately recovered with high quality using the encryption key only. When both the embedding and encryption keys are available to the receiver, the hidden data can be extracted completely and the original image recovered perfectly.

Because embedding operations are performed to the encrypted data, the data-hider cannot access the contents of the original image. That ensures security of the contents in data hiding. As the embedding and recovery are protected by the encryption and embedding keys, an adversary is unable to break into the system without the two these keys.

Acknowledgements

This work was done at Malabar Institute Of Technology, Kannur. The authors would like to acknowledge the support from
Dr.C.Sorna Chandra Devadass (Principal, MIT) and Asst. Prof Jacob Zachariah (Head of the Department, Electronics And Communication
Engineering MIT) for their immense encouragement and support.

References

[1]. 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.

[2]. S. Lian, Z. Liu, Z. Ren, and H. Wang, *Commutative encryption and watermarking in video compression, IEEE Trans. Circuits Syst.Video Technol., vol. 17, no. 6*, pp. 774–778, Jun. 2007.

[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]. W. Puech, M. Chaumont and O. Strauss, *A reversible data hiding method for encrypted images, Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 68191E*, Feb. 26, 2008, doi:10.1117/12.766754.

[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. 19, no. 4*, pp. 199–202, Apr. 2012.

[7]. K. Ma, W. Zhang, et al. *Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption*, IEEE Trans. Inf.Forensics Security, vol. 8, no. 3, 553-562, 2013.

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