REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE WITH LOGISTIC SWAP ENCODING

V.V. Vinoth
Research Scholar
Department of ECE
Bharath University, Chennai
India
E-mail:vinothvv.velaian@gmail.com

Dr. B. Karthik
Associate Professor
Department of ECE
Bharath University, Chennai,
India
E-mail: karthik.ece@bharathuniv.ac.in

Abstract- **In this method the logistic swap encoding is used to proposed the implement reversible data hiding (RDH) in encrypted images. Using logistic swap encoding the original image is encrypted by the content owner. To accommodate the secret data, the data hider modifies the bits taken from the encrypted image. 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. Public can extract the secret data and recover the original image using logistic swap decoding, when the embedding and encryption keys are available at the receiver side . The scheme is a good choice for secure image transmission.**

Index Terms- **Image encryption, image recovery, image transmission, and 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. Only authorized parties can access the process of encoding a message n such a way that it. Encryption denies the intelligible content to a would-be interceptor; it does not of itself prevent interference. In an encryption method, the encryption algorithm is used to encryptthe future message referred to as plaintext, generating cipher text that can only be read if decrypted. For technical reasons, an encryption method usually uses a pseudo-random encryption key generated by an algorithm. Without possessing the key then the principle possible to decrypt the message, but for a well designed encryption scheme, considerable computational resources and skills are required. When the originator provided the key to recipient, an authorized recipient can easily decrypt the message but not to unauthorized users.

Compressing encrypted images, adding a watermark into the encrypted images, and reversibly hiding data into the encrypted image are done by the data processing. Without accessing the original image, 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. Theoriginal image along with the secret data is required to be recovered at the receiving side. Reversible data hiding is desirable. For example, who embeds the information into the medical image to protect the patient's privacy content of the medical image might be unavailable for the technician who embeds the information into themedical image.

A separable reversible data hiding method for encrypted images using logistic swap encoding is proposed in this paper. With the two different keys, the system is separable. The original image can be approximately reconstructed and hidden data can be completely extracted using the encryption key. With both keys available, the original image perfectly recovered and the hidden data can be completely extracted. The proposedmethod avoids the operations of room-reserving by the sender. The break of the paper is organized as follows. Previous works of RDH in encrypted images are surveyed in Section II. The proposed system is describes image encryption, data embedding, data extraction and image recovery in section III,. 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. "Vacating Room After Encryption (VRAE)" and " Vacating Room Before Encryption (VRBE)" are the

main two types of existing methods of reversible data hiding. The content owner and the service data hider are not the same person in RDH for encrypted image are usually designed for the applications. Sender encrypts the original image directly and data hider adds the secret bits by modifying some bits of the encrypted data. This is the method of VRAE. Advanced Encryption Scheme (AES) is used to encrypt the original image by the owner, and the data hider embeds one bit in each block. On the receiving side, data extraction and image recovery arerealized during decryption of encrypted image by analyzing the local standard deviation. Here data extraction and image decryption are inseparable.

Zhang divides the encrypted image into blocks, and embeds one bit into each blocks by flipping 3 LSBs of the half pixels in the block. Hong et al 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, using source coding with side information Zhang proposed separable RDH scheme for encrypted image by compressing the encrypted data, which guarantees the data extraction independent from image encryption.

Ma et al provided a RDH idea in encrypted images by reserving room before encryption. This method with the traditional RDH method empties out room by embedding LSBs of some pixels into other pixels 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.

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

III.PROPOSED SYSTEM

Image encryption, data embedding and data retrieval/image recovery are the main three phases of the system. In the first phase, using an encryption key the original image is encrypted form the encrypted data. In the second phase encrypted data are sent to the data hider who embeds the secret data into the encrypted data using an embedding key. There are three cases for the receiver to extract secret bits or recover theimage. 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. The secret bits can be extracted and theoriginal image can be perfectly recovered, if both the embedding key and the encryption keys are available for the receiver. Details of the procedure are as follows.

A. 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.

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

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

$$x' = a * x * (1 - x) \qquad (2)$$

Now the stream cipher encrypts the bit stream of the original image by

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

Where $K_{i,\,j,u} \in x'$, are the key stream bits, *ei, j, u* the generated cipher text, and $\oplus$ denotes Exclusive OR.

The encrypted image **E** can be constructed by

$$E_{i,j} = \sum_{u=0}^{7} e_{i,j,u} \cdot 2^u \qquad (4)$$

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

B. Data Embedding

After creating the encrypted form of original image, the content owner sends the encrypted image to the data-hider. The secrecy of the data can be access by the data hider using an embedding key .The size of the encrypted image is less when it is calculated. By resizing the encrypted image the data is now embedded in the encrypted image.

C. Data Extraction and Image Recovery

The encrypted image contains data on the receiving end. Image recovery is done by the logistic substitution decoding, if the encryption key is available. 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.

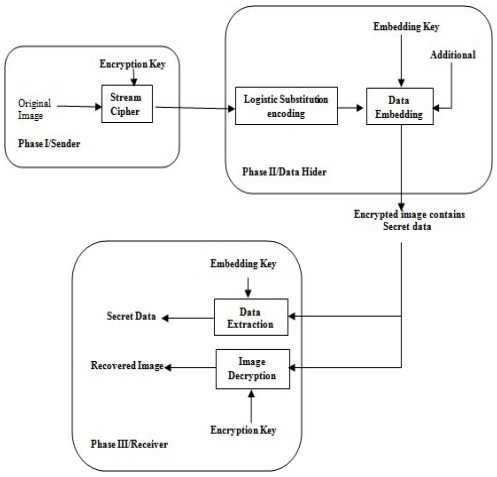

Fig.1. Proposed architecture

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 operation2. The resulting encrypted image containing secret bits respectively shows in Fig. 2(c). Fig. 3 shows the hidden text extract.

.

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). Using the hidden text, number of ASCII characters hidden ,length of the hidden text, number of bits available for data hiding, 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.

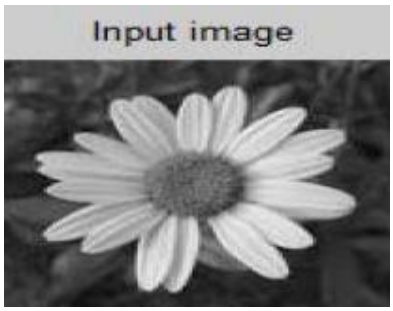

Fig 2. (a) Original image

For embedded message the data hider does not allow adversaries to crack the system. Using anencryption key, the original image is encrypted with a stream cipher.

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

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

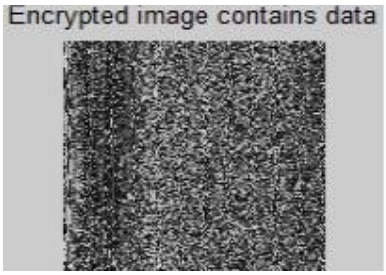

Fig..2 (c) Encrypted image contains secret data
Figure.2 Image encryption

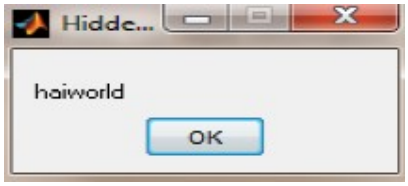

Fig..3 Extracted secret data

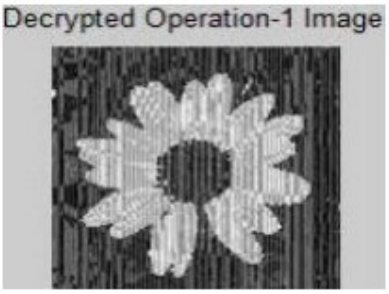

Fig..4 (a) Output of decryption-1

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

V.CONCLUSION

In this method the logistic swap encoding is used to propose the implement reversible data hiding (RDH) in encrypted images .Encrypted image is modified for the additional secret data after encrypting the original image with a stream cipher. On the receiver side, using the encryption key, all hidden data can be extracted with the embedding key, and the original image approximately recovered with high quality only. The hidden data can be extracted completely and the original image recovered perfectly, when both the embedding and encryption keys are available tothe receiver.

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

REFERENCES

[1] Zhenxing Qian, Xinpeng Zhang, “Reversible data hiding in encrypted image with distributed source encoding,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, pp. 636 - 646, April 2016.

[2] Z. Erkin, A. Piva, S. Katzenbeisser, et al., “Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing,” EURASIP Journal on Information Security 2007, 2008.

[3] 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. 201

[4] 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.

[5] 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.

[6] 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.

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