[RACE: March 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

HIGHLY SECURED DOUBLE DATA HIDING TECHNIQUE: A REVIEW

Rubeena.T.P.[*1] & Shihabudeen.H.[2]

[*1]M tech scholar, College of Engineering, Thalassery

[2]Assistant professor, College of Engineering, Thalassery

ABSTRACT

This paper proposes a novel scheme of reversible data hiding (RDH) in encrypted images using distributed source coding (DSC). After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make room for the secret data. The selected bit series is Slepian-Wolf encoded using low density parity check (LDPC) codes. On the receiver side, the secret bits can be extracted if the image receiver has the embedding key only. In case the receiver has the encryption key only, he/she can recover the original image approximately with high quality using an image estimation algorithm. If the receiver has both the embedding and encryption keys, he/she can extract the secret data and perfectly recover the original image using the distributed source decoding. The proposed method outperforms previously published ones.

I. INTRODUCTION

Information processing in the encrypted domain has attracted considerable research interests in recent years. In many applications such as cloud computing and delegated calculation, the content owner needs to transmit data to a remote server for further processing. In some cases, the content owner may not trust the service supplier, and needs to encrypt the data before uploading. Thus, the service provider must be able to do the processing in the encrypted domain. Some works have been done for data processing in an encrypted domain, for example, compressing encrypted images, adding a watermark into the encrypted image, and reversibly hiding data into the encrypted image.

Unlike robust watermarking, reversible data hiding emphasizes perfect image reconstruction and data extraction, but not the robustness against malicious attacks. Many RDH methods for plaintext images have been proposed, for example, a common framework of redundancy compression, difference expansion (DE) and histogram shifting (HS) approaches. However, these are not applicable to encrypted images since the redundancy in the original image cannot be used directly after image encryption.

As a new trend, reversible data hiding in encrypted images allows the service provider to embed additional messages, e.g., image metadata, labels, notations or authentication information, into the encrypted images without accessing the original contents. The original image is required to be perfectly recovered and the hidden message completely extracted on the receiving side. Reversible data hiding in encrypted images is desirable. For example, in medical applications, a patient does not allow his/her medical images to be revealed to any outsiders, while the database administrator may need to embed medical records or the patient's information into the encrypted images. On the other hand, the original medical image for diagnosis must be recovered without error after decryption and retrieval of the hidden message.

This paper aims to enhance embedding payload in encrypted images. We propose a separable reversible data hiding method for encrypted images using Slepian-Wolf source encoding. The idea is inspired by the DSC, in which we encode the selected bits taken from the stream-ciphered image using LDPC codes into syndrome bits to make spare room to accommodate the secret data. With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. With both keys available, the hidden data can be completely extracted, and the original image perfectly recovered with the aid of some estimated side information. The proposed method

achieves a high embedding payload and good image reconstruction quality, and avoids the operations of room-reserving by the sender.

II. LITERATURE REVIEW

A. A Reversible Data Hiding Method for Encrypted Images

Methodology

The proposed system use Advanced Encryption Standard (AES) algorithm .The Advanced Encryption Standard (AES) algorithm consists of a set of processing steps repeated for a number of iterations called rounds.21 The number of rounds depends on the size of the key and the size of the data block. The AES algorithm can support several cipher modes: ECB (Electronic Code Book), CBC (Cipher Block Chaining), OFB (Output Feedback), CFB (Cipher Feedback) and CTR (Counter).22 The ECB mode is actually the basic AES algorithm. In this paper, for the proposed method, the ECB mode of AES algorithm has been chosen to encrypt the images. We used bit substitution-based data hiding method in order to embed the bits of the hidden message.

The decoding algorithm is also composed of two steps which are the extraction of the message and the decryption removing. The extraction of the message is very simple: it is just enough to read the bits of the pixels we have marked by using the secret key k and the same PRNG. But after the extraction, each marked cipher-text is still marked. The problem is then to decrypt the marked encrypted image. The decryption removing is done by analyzing the local standard deviation during the decryption of the marked encrypted images.

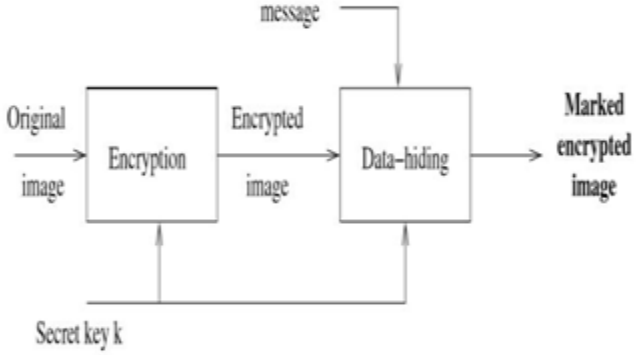


Fig. 1: Architecture of encoding method

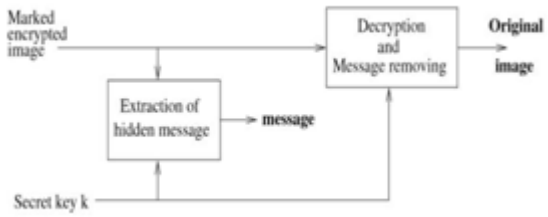


Fig. 2: Architecture of decoding method

Disadvantage

- If there is not enough white pixels, then it is not possible to embed an useful message in the image.
- It is thus not possible to use high capacity reversible data hiding method16 for encrypted images.
- Efficiency is not much enough to handle higher payload.

ISSN 2348 – 8034
Impact Factor- 4.022

B. Reversible Data Hiding in Encrypted Image

Methodology

This work proposes a novel reversible data hiding scheme for encrypted image, which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered.

In this work, a novel reversible data hiding scheme for encrypted image with a low computation complexity is proposed, which consists of image encryption, data embedding and data extraction/image-recovery phases. The data of original image are entirely encrypted by a stream cipher. Although a data-hider does not know the original content, he can embed additional data into the encrypted image by modifying a part of encrypted data. With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be correctly extracted while the original image can be perfectly recovered.

Assume the original image is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as

$$b_{i,j,0}, b_{i,j,1}, \ldots, b_{i,j,7}$$

$$b_{i,j,k} = \left\lfloor \frac{p_{i,j}}{2^k} \right\rfloor \mod 2, \quad k = 0, 1, \ldots, 7$$

$$p_{i,j} = \sum_{u=0}^{7} b_{i,j,k} \cdot 2^k.$$

In encryption phase, the exclusive-or results of the original bits and pseudo random bits are calculated. Where ri,j,k are determined by an encryption key using a standardstream cipher. Then, are concatenated orderly as the encrypted data. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data

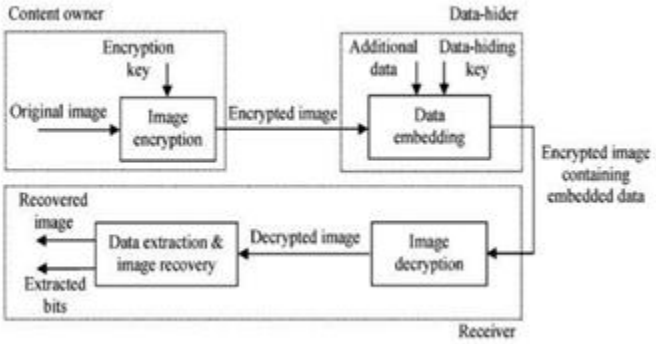


Fig. 3: Architecture of the Proposed System

Disadvantage

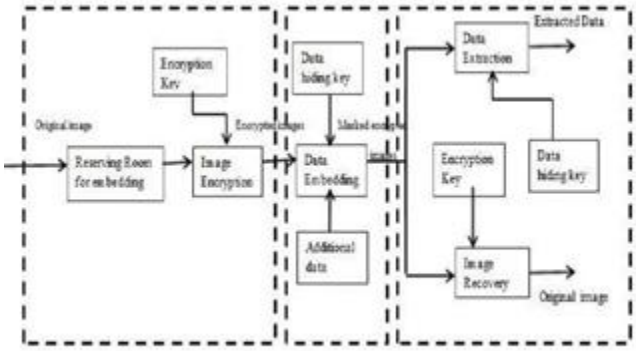
- In the proposed scheme, the smaller the block size, the more additional data can be embedded. However, the risk of defeat of bit extraction and image recovery rises.
- Incorrect bit-extraction occurred.
- The extracted-bit error rate is equivalent to the rate of unsuccessful block recovery.

C. Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption

Methodology

Here, a novel method is proposed so as to reserve 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. The proposed method can achieve real reversibility, i.e., data extraction and image recovery are free of an error.

Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may subject to some errors on data extraction and/or image restoration. Here, a novel method is proposed so as to reserve 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. The proposed method can achieve real reversibility, i.e., data extraction and image recovery are free of any error.



(b)

Fig. 4: Framework RRBE

Disadvantage

- The quality of image is reduce drastically.
- All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.
- The method is difficult to implement.

III. SYSTEM DESIGN

The proposed system is sketched in Fig. 5, which consists three phases: image encryption, data embedding, and data extraction/image recovery. In phase I, the sender encrypts the original image into an encrypted image using a stream cipher and an encryption key. In phase II, the data-hider selects and compresses some MSB of the secret image using LDPC codes to generate a spare space, and embeds additional bits into the encrypted image using an embedding key. In phase III, the receiver extracts the secret bits using the embedding key. If he/she has the encryption key, the original image can be approximately reconstructed via image decryption and estimation. When both the encryption and embedding keys are available, the receiver can extract the compressed bits, and implement the distributed source decoding using the estimated image as side information to perfectly recover the original

image.

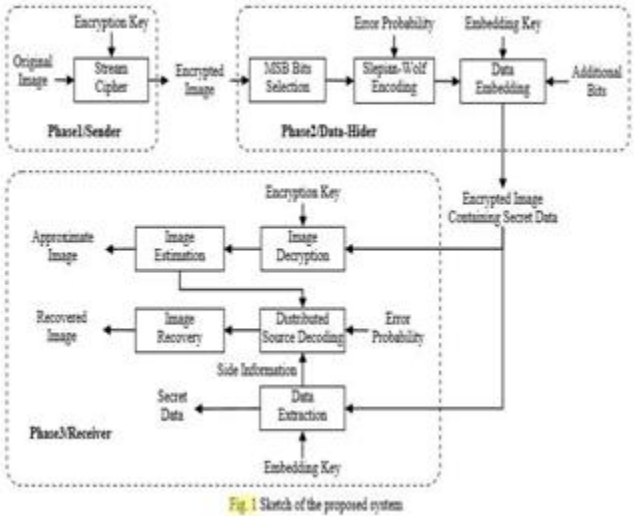


Fig. 5: Sketch of the proposed system

A. Image Encryption

Without loss of generality, we assume the original image O is a grayscale image with all pixel values falling into [0, 255], and the image size is M×N where both M and N are power of 2.

$$b_{i,j,u} = \left\lfloor O_{i,j} / 2^{u} \right\rfloor \bmod 2, \quad u = 0, 1, 2, \ldots, 7 \qquad (1)$$

where Oi,j are pixels of the original image, 1≤i≤M, 1≤j≤N.

The owner then chooses an encryption key KENC to generate pseudo-random bits using a stream cipher function (e.g., RC4 or SEAL), and encrypts the bitstream of the original image by

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

where ki,j,u are the key stream bits, ei,j,u the generated cipher text, and denotes exclusive OR. Accordingly, the encrypted image E can be constructed by

$$E_{i,j} = \sum_{u=0}^{7} e_{i,j,u} \cdot 2^{u} \qquad (3)$$

Ei,j are pixel values of the encrypted image, 1≤i≤M, 1≤j≤N. Note that the stream cipher in (2) only scrambles pixel values but does not shuffle pixel locations.

IV. CONCLUSION

This paper proposes a scheme of reversible data hiding in encrypted images using distributed source coding. After encrypting the original image with a stream cipher, some bits of MSB planes are selected and compressed to make room 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. With the idea of DSC, the proposed method substantially increases the payload as compared with the existing VRAE methods. An LDPC parity-check matrix is used to generate corresponding

syndromes. Associated with the estimated image generated from the proposed estimation algorithm, the receiver can decode these syndromes back to the original bits using iterative BPA decoding. 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 an/d recovery are protected by the encryption and embedding keys, an adversary is unable to break into the system without these keys.

REFERENCES

[1] *"A Reversible Data Hiding Method for Encrypted Images", W. Puech, M. Chaumont and O. Strauss*
[2] *"Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption", X. Zhang*
[3] *"Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption", K. Ma, W. Zhang*