ISSN 2277-3061

Implementation of Detachable Reversible Data Hiding in Image Encryption

D Srilatha, Musham Pradeep
Assistant Professor, Sreenidhi Institute of Technology and Science,
Ghatkesar, Hyderabad, A.P. India
doddisrilatha@gmail.com
M. Tech. Student, Sreenidhi Institute of Technology and Science,
Ghatkesar, Hyderabad, A.P. India
pradeep.musham88@gmail.com

ABSTRACT

This paper proposes a scheme for detachable reversible data hiding in image encryption. In which the sender encrypts an image using encryption key. Then, the data is appended to the encrypted image using a data-hiding key. 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 content of the image. If the receiver has the encryption key, he can decrypt the encrypted image and get an image similar to the original one, but he cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original image without any error.

Indexing terms/Keywords

Image encryption, detachable, reversible data hiding

Academic Discipline And Sub-Disciplines

Computer Science – Software Engineering

SUBJECT CLASSIFICATION

Network Security

ISSN 2277-3061

INTRODUCTION

Signal processing in the encrypted domain has attracted considerable research interest recently. As an effective and popular means for privacy protection, encryption converts the ordinary signal into meaningless data, so that the traditional signal processing usually takes place before encryption or after decryption. Detachable reversible data hiding is a technique to embed additional message into some distortion less cover media, i.e., image with detachable and reversible manner [1] so that the original cover content can be perfectly restored after extraction of the appended message. A number of reversible data hiding methods have been proposed in recent years. This is the novel scheme that separates the data extraction and image decryption. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients

There are also a number of works on data hiding in the encrypted domain. In a buyer–seller watermarking protocol [2], the seller of digital multimedia product encrypts the original data using a public key, and then permutes and embeds an encrypted fingerprint provided by the buyer in the encrypted domain. After decryption with a private key, the buyer can obtain a watermarked product. This protocol ensures that the seller cannot know the buyer's watermarked version while the buyer cannot know the original version. In another type of joint data-hiding and encryption schemes, a part of cover data is used to carry the additional message and the rest of the data are encrypted, so that both the copyright and the privacy can be protected.

The reversible data hiding in encrypted image is developed in [1]. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain [3]–[8]. But, in some applications, sender hopes to append some additional message, within the encrypted image. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. Reference [1] presents a practical scheme satisfying the above mentioned requirements and Fig.1. Sender encrypts the original image using an encryption key, and embeds additional data into the encrypted image using a data-hiding key. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data according to the data-hiding key. 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 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.

This paper proposes a scheme for detachable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data is embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original image without any error when the amount of additional data is not too large.

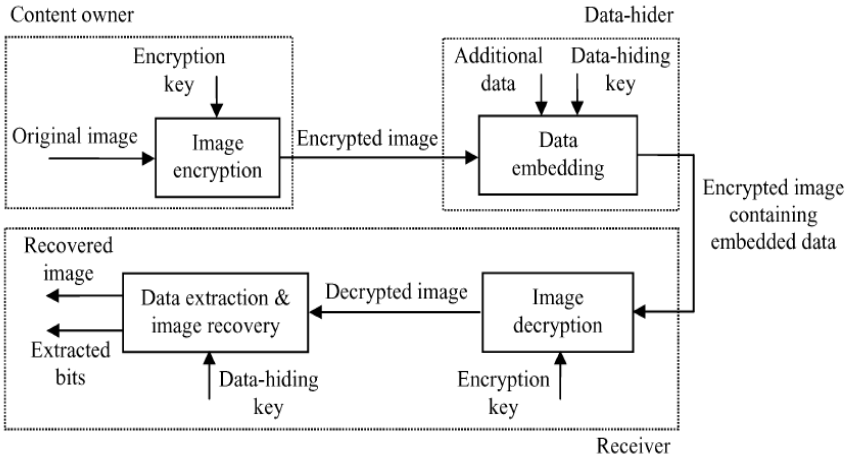

Fig.1. Sketch of reversible data hiding in encrypted image.

PROPOSED SCHEME

The proposed scheme is made up of encode and decode phases. The sender encrypts the original image using an encryption key to produce an encrypted image. Then, the data compressed in the least significant bits (LSB) of the encrypted image using a data-hiding key. At the receiver side, the data embedded in the encrypted image can be easily retrieved using data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered. Fig. 2 shows the three

cases at the receiver side and Fig. 3 shows the process of implementation of detachable reversible data hiding in image encryption

A. Encode

Let the image with a size of N_1xN_2 and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0},b_{i,j,1} \ldots b_{i,j,7}$ where $1 \leq i \leq N_1$ and $1 \leq j \leq N_2$, the gray value as $p_{i,j}$, and the number of pixels as ($N=N_1xN_2$). During encryption, the exclusive-or of the original bits and pseudo-random bits are calculated

$$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u}$$

where $r_{i,j,u}$ are determined by an encryption key. Then, $B_{i,j,u}$ are concatenated result of encryption key and image pixel bits. Then the data that is given is embedded with the encrypted image.

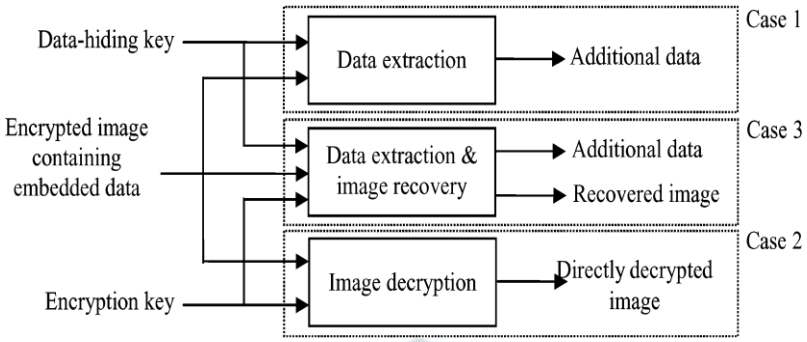

Fig.2. Three cases at receiver side of the proposed separable scheme.

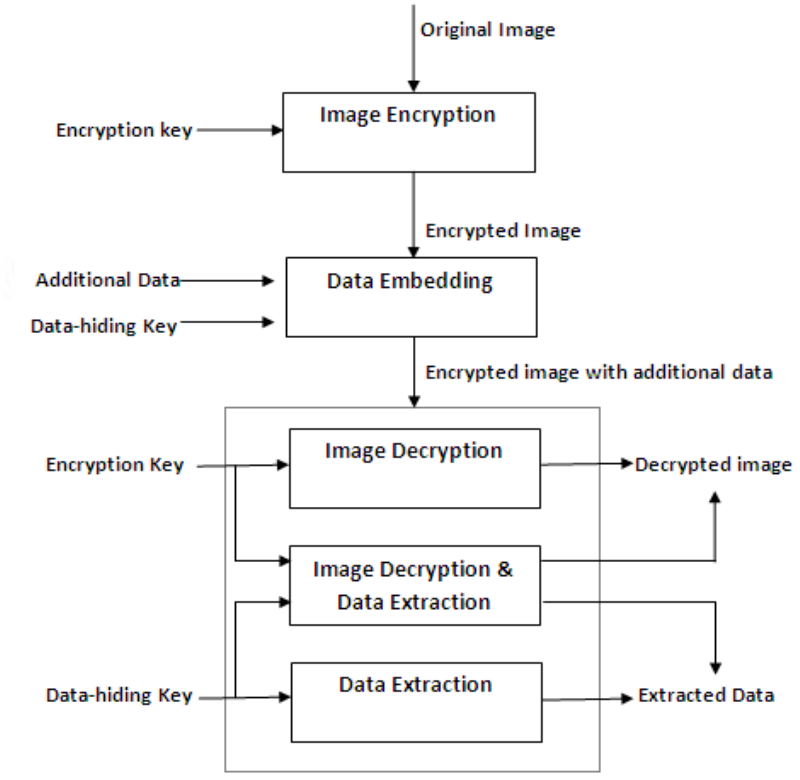

Fig.3. Process of Implementation of detachable reversible data hiding in image encryption.

B. Decode

In this phase, we will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters from the LSB. although the receiver having

the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

Consider the case that the receiver has the encryption key but does not know the data-hiding key. Clearly, he cannot obtain the values of parameters and cannot extract the embedded data. However, the original image content can be roughly recovered. Denoting the bits of pixels in the encrypted image containing embedded data as $B'_{i,j,0}, B'_{i,j,1}, \ldots\ldots, B'_{i,j,7}$ ($1 \le i \le N1$ and $1 \le j \le N2$), the receiver can decrypt the received data

$$b'_{i,j,u} = B'_{i,j,u} \oplus r_{i,j,u}$$

where $r_{i,j,u}$ derived from the encryption key.

If the receiver has both the data-hiding and the encryption keys, he may aim to extract the embedded data and recover the original image.

RESULTS

The test image shown in Fig. 4(a) was used as the original image. After image encryption, the eight encrypted bits of each pixel are converted into a gray value to generate an encrypted image and we also embed additional bits into the encrypted image. The encrypted image containing the embedded data is shown in Fig. 4(b). With an encrypted image containing embedded data, we can extract the additional data using the data-hiding key. If we directly decrypted the encrypted image containing embedded data using the encryption key, it gives the decrypted image as Fig. 4(d). By using both the data-hiding and the encryption keys, the embedded data could be successfully extracted and the original image could be perfectly recovered from the encrypted image containing embedded data.

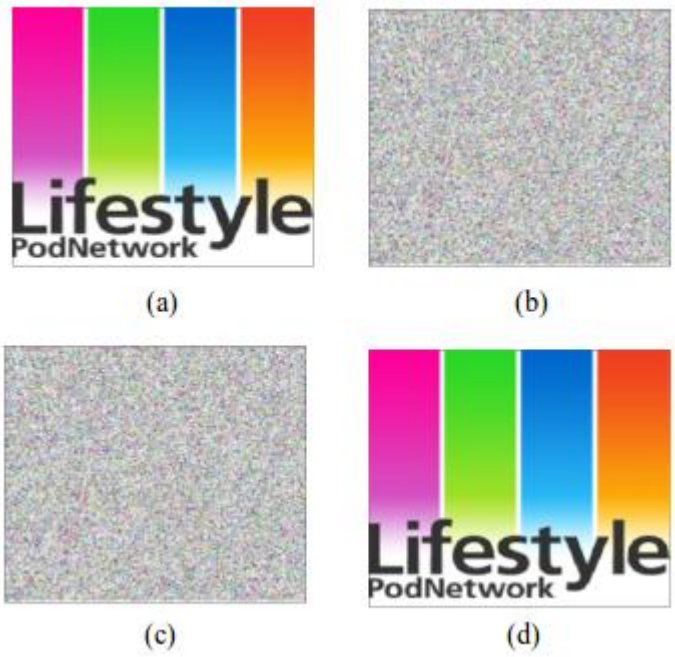

Fig.4. (a) Original Image, (b)&(c) Encrypted image containing embedded data, and (d) Decrypted image.

CONCLUSION

In this paper, a novel scheme for detachable reversible data hiding in image encryption is proposed, which consists of encode and decode phases. In the first phase, the sender encrypts the original image using an encryption key. Then the data is appended to the LSB of the encrypted image using a data-hiding key. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error. In the future, it can be done using different algorithms.

REFERENCES

[1] X. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[2] N. Memon and P. W. Wong, “A buyer-seller watermarking protocol,” IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

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

[4] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[5] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[6] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, “A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification,” Signal Process., vol. 90, pp. 2911–2922, 2010.

[7] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, “Reversible data-embedding scheme using differences between original and predicted pixel values,” IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.

[8] Xinpeng Zhang, “Separable Reversible Data Hiding in Encrypted Image,” IEEE Trans. Information Forensics and security., vol. 7, no. 2, pp 826-832, Apr. 2012.

Author Profile

Ms. D. Srilatha presently working as Assistant Professor in CSE Department in Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, India. She has completed her M.Tech from JNTU Hyderabad and her areas of interests are Network Security, Data Mining and Cloud Computing.

Musham Pradeep is a M.Tech Student in Software Engineering at Sreenidhi Institutue of Science and Technology, Ghatkesar, Hyderabad, India.