Volume 4, No. 4, April 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

INDEPENDENT CHANGEABLE INFORMATION HIDING IN ENCRYPTED IMAGES

Lavanya.S, Anuradha.C
PG Student, Computer Science and Engineering, Bharath University, Chennai, India
Lavanya.pranav@gmail.com
Asst.Prof, Computer Science and Engineering, Bharath University, Chennai, India
Anuradha.ak23@gmail.com

Abstract **—**This work proposes a Secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then , a data hider may compress the least significant bits of the encrypted image 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, receiver can extract the additional data though receiver does not know the image content. If the receiver has encryption key, can decrypt the received data to obtain an image similar to the original one , but cannot extract the additional data. If the receiver has both the data hiding key and the encryption key, 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.

Key Words—data hiding, data embedding, data extraction, image encryption, reversible data hiding.

INTRODUCTION

Military and medical images are media having some distortion is un-acceptable. Hence for data hiding we have technique using which we can extract data correctly and after that original cover content can be perfectly recovered. This technique so known as reversible data hiding [4]. There are many reversible techniques such as expansion method and histogram shift method. Another kind of method makes use of redundancy n a cover by performing lossless compression to create a spare space for data embedding [1].

Encryption is well known for privacy protection. For securely transmission of image content owner encrypt it be for e-transmit it to other person. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images. It may be also hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable [1]. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data in to the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, are ceiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image 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 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.

This paper proposed new scheme of data hiding it is also known as separable reversible data hiding. Content owner can encrypt this image be for e-transmission by using encryption key. And additional data can be added using the data hiding key. At the receiver side if receiver has only data hide key, he can only extract the data from image. If receiver has encryption key then he can decrypt the image. But if receiver has both, data hiding and encryption key then he can extract hided data and as well as can recover image [2].

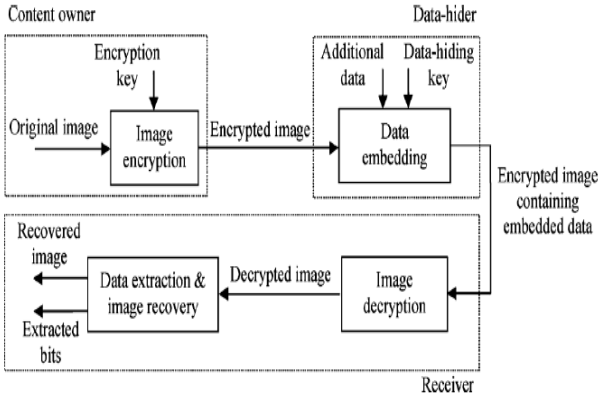

Figure: 1 Proposed System[1]

PROPOSED SYSTEM

Proposed system has three main phases:

A. Image Encryption:
B. Data embedding:
C. Data extraction and image recovery:

Using encryption key content owner encrypt image. Then data hider creates parse space for hiding data by replacing least significant bits (LSB) in encrypt image using data hiding key. At the receiver side embedded data at sparse space can retrieved from encrypted image using data hiding key. As data hiding affects only on LSB, hence after decryption original image can be correctly retrieved. When using both of the encryption and data-hiding keys, the embedded data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.Fig.2 shows the three cases at the receiver side.

***Image Encryption* [4], [2]:**

Assume the original image is in un compressed format and each pixel with gray value fall in gin to[0,255]is represented by8bits.Denotethebitsofapixelas$b_{i,j,0}$,$b_{i,j,1}$,……,$b_{i,j,7}$ where (i,j) in dicates the pixel position, and the gray valueas $p_{i,j}$.Thus

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

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

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated.

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k} \qquad (3)$$

Where $r_{i,j,k}$ are determined by an encryption key using a standard stream cipher. Then, $B_{i,j,k}$a reconatenated orderly as the encrypted data. A number of secure stream cipher method scan be used 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.

Data Embedding [4], [2]:

With the encrypted data, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data. Firstly, the data-hider segments then crypted image into a number of non-over lapping blocks size dbys×*s*. In other words, the encrypted bits *bi ,j,* satisfying (m-1)+*s* +*1*≤ *I*≤ *m*+*s*,*(n-1)* +*s*+*1*≤*j*≤ *n* +*s and0*≤ *k* ≤*7(mand nare positive integers)* are within as am block. Then, each block will be used to carry one additional bit. For each block, pseudo-random ly divide the s^2 pixels into two sets S_0 *and* S_1 according to a data-hiding key. Here, the probability that a pixel belongs to S_0 *or* S_1 is1/2. If the additional bit to beembeddedis0, flip the3 least sign if I can tb its (LSB) of each encrypted pixel in S_0,

$$B'_{i,j,k} = B'_{i,j,k'} \quad (i,j) \epsilon S_0 \text{ and } = 0,1, \quad 2 \qquad (4)$$

If the additional bit is1,flip the 3 encrypted LSB of pixel sinS_1,

$$B'_{i,j,k} = B'_{i,j,k'} \quad (i,j) \epsilon S_1 \text{ and } k = 0, \quad 1, \quad 2. \qquad (5)$$

The other encrypted data are not changed.

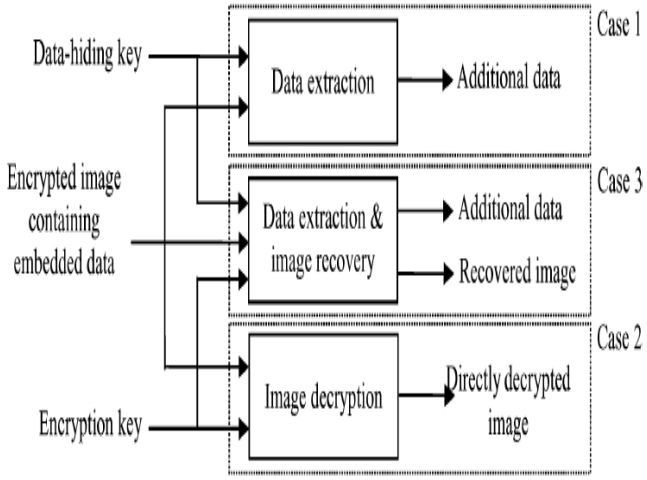

Figure 2: Three case sat the receiver side for the propose separable scheme [2]

Data Extraction and Image Recovery [4], [2]:

When having an encrypted image contain in gem bedded data, are ceiver first ly generates $r_{i,j,k}$ according to then cryption key, and calculates the exclusive-or of the received data $r_{i,j,k}$ and to decrypt the image. We denote the decrypted as. Clearly, the original five most significant bits (MSB) are retrieved correctly. For a certain pixel, if the embedded it in the block including the pixel is zero and the pixel belongs to S_1, or the embedded it is1 andthe pixel belongs to S_0, the data-hiding does not affect any encrypted bits of the pixel. So, the three decrypted LSB must be same as the original LSB, implying that the decrypted gray value of the pixel is correct. On the other hand, if the embedded bit in the pixel'sblockis0 and the pixel be longs to S_0, or the embedded bit is 1 and the pixel belongs to S_1, the decrypted LSB That

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

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

$$= r_{i,j,k} \oplus b'_{i,j,k} \oplus r'_{j,k}$$

= b'i,j,kk= 0, 1, 2(6)

That means the three decrypted LSB must be different from the original LSB. In this case:

b'i,j,k+ bi,j,k= 1, k= 0,1,2

So, the sum of decimal values of three decrypted LSB and three original LSB must be seven. The average energy of errors between the decrypted and original gray values is

$$E_A = \frac{1}{8} \sum_{u=0}^{7} [u - (7-u)]^2 = 21.$$

As the probability of incorrect LSB-decryptionis1/2, when reconstructing an image using the decrypted data, the value of PSNR in the decrypted image is approximately

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\frac{E_A}{2}} = 37.9 \text{ dB}.$$

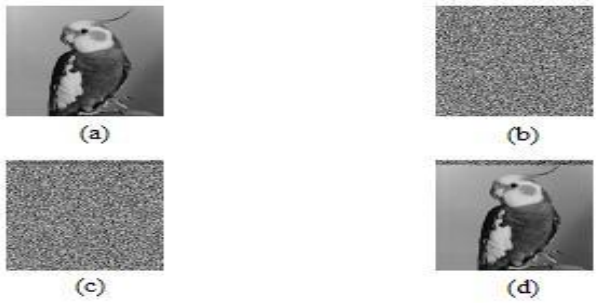

Figure 3:(a) Original image(b) Encrypted version (c) Encrypted image with message(d) Decrypted image

Then, the receiver will extract he embedded bits and recover the original content from then cryptic image. According to the data-hiding key, he may segment the decrypted image into blocks and divide the pixels in each block into two sets in as Amway. For each decrypted block, the receiver flips all the three LSB of pixel sin S_0 to form a new block, and flips all the three LSB of pixels in S_1 to form another new block. We denote the two new blocks asH_0 and H_1.There must be that either H_0 orH_1 is the original block, and another one is more seriously interfered due to the LSB flip operation. For the two blocks sized by $S \times S$, define a function to measure the fluctuation in them and de note the values of fluctuation function no fH_0 and H_1 as f_0 and f1respectively.Because of spatial correlation in natural image, the fluctuation function of original block is generally lower than that of seriously interfered version. So, the receiver can perform data extraction and image recovery by comparing f_0 and f_1. If $f_0 < f_1$, regard H_0 as the original content of the block and let the extracted it be 0. Otherwise, regard H_1 as the original content of this block and extract a bit1. Finally, concatenate the extracted bits to retrieve the additional message and collect the recovered blocks to form the original image [4], [2].

CONCLUSION

When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the loss less compression method in [6]or[7] is used for the en crypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the loss less compression does not change the content of the encrypted image containing embedded data [2]. However, the lossy compression method in [5] compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation [2].So, in future a complete mixture of image encryption and data hiding compatible with lossy compression demands further research.

REFERENCES

[1]. 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.

[2]. 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.

[3]. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011

[4]. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[5]. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180– 187, Feb. 2010.

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

[7]. M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., vol. 14, no. 12, pp. 2129–2139, Dec. 2005

[8]. M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

[9]. 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

[10]. M.Cancellaro, F.Battisti, M. Carli, G.Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Processing: Image Commun., vol. 26, no. 1, pp. 1– 12, 2011.

[11]. D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proceedings IEEE, vol. 92, no.6, pp. 918–932, Jun. 2004.

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

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

