Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure and Authenticated Reversible Data Hiding in Encrypted Image

C.Anuradha,
Assistant Professor,
Department of CSE,
Bharath University, India.

S.Lavanya,
PG Student,
Department of CSE,
Bharath University,India.

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 the 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. It is also a drawback because if the receiver has any one key as known, and then he can take any one information from the encrypted data. In order to achieve authentication SHA-1 algorithm is being used.

Index Terms— Image encryption, Data embedding, Image extraction, Reversible data hiding.

I. Introduction

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images.

II. Background

For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource [1], a lossless compression method for encrypted gray image using progressive decompose and rate-compatible turbo codes is developed in [2]. With the lossy compression method presented in [3], an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied. Based on the homomorphic properties of the underlying cryptosystem, the discrete Fourier transform in the encrypted domain can be implemented [4]. In [5], a composite signal representation method packing together a number of signal samples and processing them as a unique sample is used to reduce the complexity of computation and the size of encrypted data. There are also a number of works on data hiding in the encrypted domain. In a buyer–seller watermarking protocol [6], 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.

By introducing the composite signal representation mechanism, both the computational overhead and the large communication bandwidth due to the homomorphic public key encryption are also significantly reduced [8]. For example [9], the intraprediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients. In [10], the cover data in higher and lower bit-planes of transform domain are respectively encrypted and watermarked. In [11], the content owner encrypts the signs of host DCT coefficients and each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints are generated for the users. The reversible data hiding in encrypted image is investigated in [12]. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain [13]–[14]. 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, receiver cannot extract any information from the encrypted image containing additional data.

III. Proposed Works

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. This paper proposes a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using 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 receiver does not know the image content. If receiver 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.

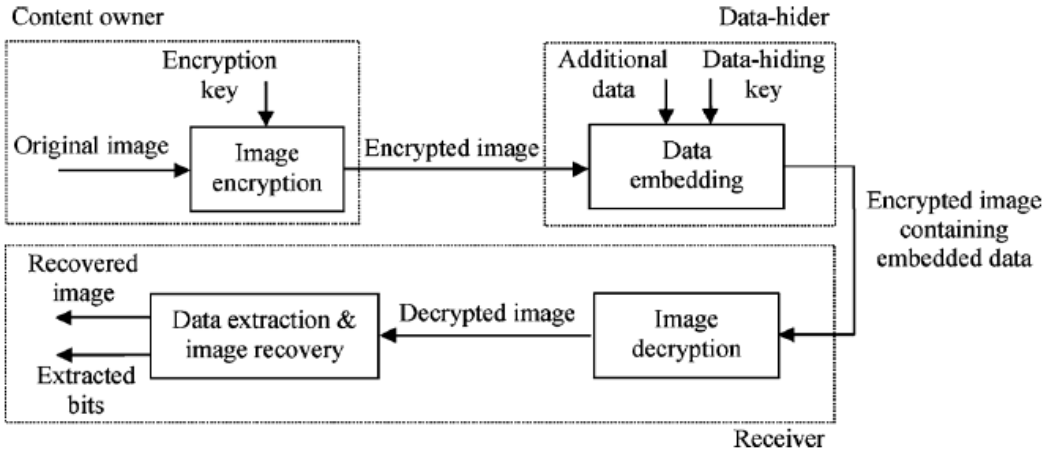

Fig1. Non-separable reversible data hiding in encrypted Image

The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the 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. Fig. 2 shows the three cases at the receiver side.

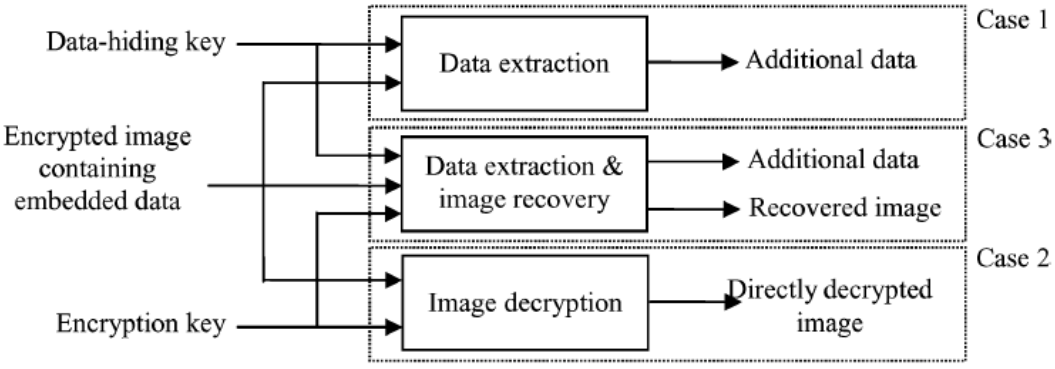

Fig 2. Three cases at receiver side of the proposed separable scheme

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 by exploiting the spatial correlation in natural image.

IV. Implementation Details

A. Image Encryption

While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes, a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in .With the lossy compression method presented in, an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the 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 by exploiting the spatial correlation in natural image.

B. Data Embedding

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

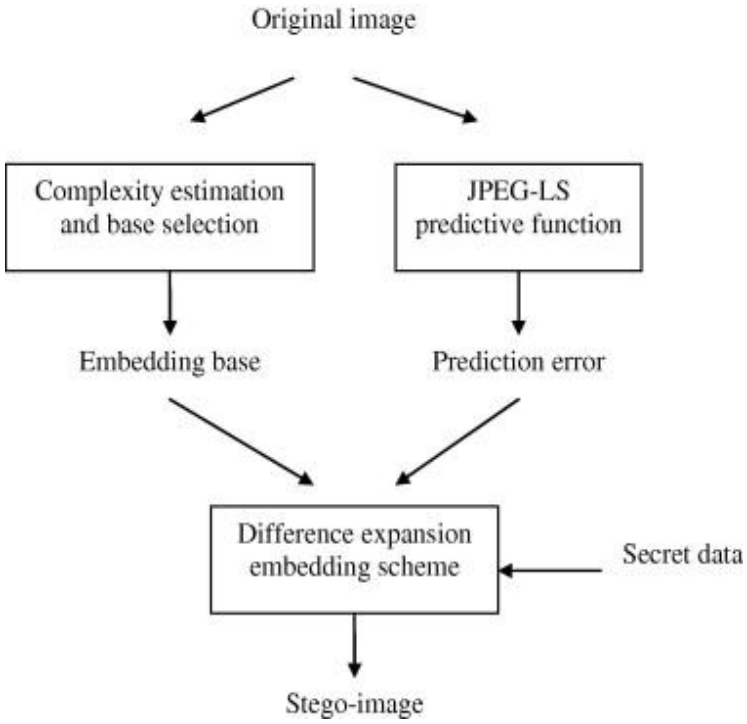

Fig 3. Data Embedding

According to the data hiding key, the data hider pseudo randomly selects N_P encrypted pixels that will be used to carry the parameters for data hiding. Here N_P is a small positive integer, for example N_P=20.The other encrypted pixels are pseudo-randomly permuted and divided into number of groups, each of which contain L pixels. The permutation way is also determined by the data-hiding key. For each pixel-group, collect the M least significant bits of the L pixels, and denote them as B (k,1) , B (k,2) …… B(k,M*L) where k is a group index within [1,(N-Np)/L] and M is a positive integer less than 5. The data-hider also generates a matrix G sized (M*L – S) * M*L, which is composed of two parts. The left part is the identity matrix and the right part is pseudo-random binary matrix derived from the data-hiding key. For each group, which is product with the G matrix to form a matrix of size (M * L-S). Which has sparse bits of size S, in which the data is embedded and arrange the pixels into the original form and permutated to form a original image.

C. Image Decryption

When having an encrypted image containing embedded data, a receiver firstly generates ri,j,k according to the

encryption key, and calculates the exclusive-or of the received data and ri,j,k to decrypt the image. We denote the decrypted bits as b1i,j,k . Clearly, the original five most significant bits (MSB) are retrieved correctly.

For a certain pixel, if the embedded bit in the block including the pixel is zero and the pixel belongs to S1, or the embedded bit is 1 and the pixel belongs to S0 , 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's block is 0 and the pixel belongs to S0, or the embedded bit is 1 and the pixel belongs to S1 , the decrypted LSB.That means the three decrypted LSB must be different from the original LSB.In this case:

$$b'_{i,j,k} + b_{i,j,k} = 1$$

On the other hand, if the embedded bit in the pixel's block is 0 and the pixel belongs to S0, or the embedded bit is 1 and the pixel belongs to S1, the decrypted LSB

D. Data Extraction

The receiver has both the data hiding, he may aim to extract the embedded data according to the data hiding key. The values of M, Land S, the original LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can be extracted from the encrypted image containing embedded data. By putting the Np LSB into their original positions, the encrypted data of the Np selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, it will recover the original gray values of the other (N-Np) pixels. 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.

V. Experimental Results

The proposed reversible data hiding algorithm has been applied to many different types of images, including some commonly used images, medical images, texture images, aerial images, and all of the 1096 images in the Corel DRAW database, and has always achieved satisfactory results, thus demonstrating its general applicability. The proposed reversible data hiding technique is able to embed about 5–80 kb into a 512* 512 8 grayscale image while guaranteeing the PSNR of the marked image versus the original image to be above 48 dB. In addition, this algorithm can be applied to virtually all types of images.

In fact, it has been successfully applied to many frequently used images, medical images, texture images, aerial images, Furthermore, this algorithm is quite simple, and the execution time is rather short. Therefore, its overall performance is better than many existing reversible data hiding algorithms. It is expected that this reversible data hiding technique will be deployed for a wide range of applications in the areas such as secure medical image data systems, and image authentication in the medical field and law enforcement, and the other fields where the rendering of the original images is required or desired.

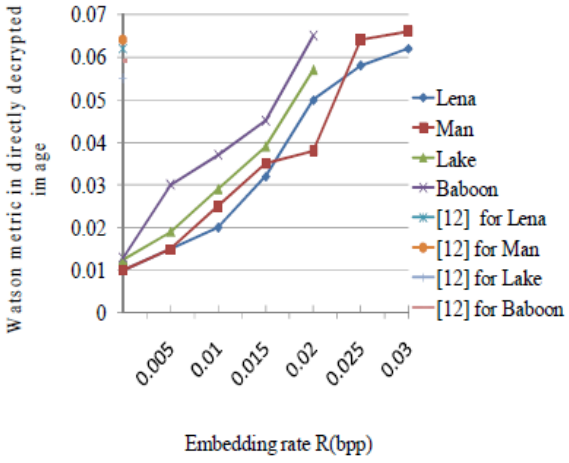

Fig4. Rate-Watson metric comparison between the proposed schemes

The rate distortion curves of the four images Lena, Man, Lake and Baboon. Here, three quality metrics were used to measure the distortion in directly decrypted image: PSNR, the Watson metric and a universal quality index Q. While PSNR simply indicates the energy of distortion caused by data hiding, the Watson metric is designed by using characteristics of the human visual system and measures the total perceptual error, which is DCT-based and takes into account three factors: contrast sensitivity, luminance masking and contrast masking.

Additionally, the quality index Q works in spatial domain, as a combination of correlation loss, luminance distortion and contrast distortion. Higher PSNR, lower Watson metric or higher Q means better quality. In these figures, while the

abscissa represents the embedding rate, the ordinate is the values of PSNR, Watson metric or quality index Q. The curves are derived from different L, M and S under a condition that the original content can be perfectly recovered using the data hiding and encryption keys. Since the spatial correlation is exploited for the content recovery, the rate-distortion performance in a smoother image is better.

The performance of the non separable method is also given in Figure. It can be seen that the performance of the proposed separable scheme is significantly better. It also compared the proposed scheme with the non-separable method over 100 images sized 2520 * 3776, which were captured with a digital camera and contain landscape and people. When meeting the perfect recovery condition, the proposed scheme has an average 203% gain of embedded data amount with same PSNR value in directly decrypted image, or an average gain of 8.7 dB of PSNR value in directly decrypted image with same embedded data amount.

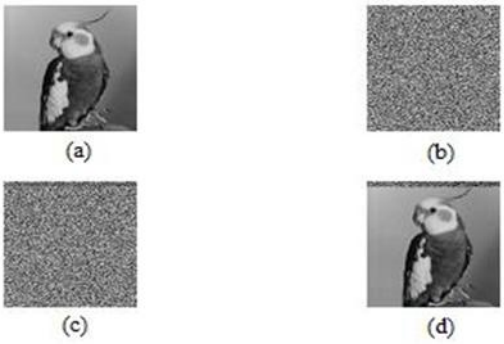

Fig 5: (a) Original image (b) Encrypted version (c) Encrypted image with message (d) Decrypted image.

VI. Conclusion And Future Work

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. Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB steganalytic methods, if he does not know the data hiding key, it is still impossible to extract the additional data and recover the original image. For ensuring the correct data extraction and the perfect image recovery, It may let the block side length be a big value or introduce error correction mechanism before data hiding to protect the additional data with a cost of payload reduction.

The implemented a reversible method can be enhanced in future by using the following provisions and MLSB technique can also be applied after embedding when there is lot of change in the pixel to retain nearest to the original value. It can be applied in networking and the keys are sent and received securely. The image produced by the reversible data hiding using two key has distortion. In order to remove distortion and to produce the image in a high quality using 3 key.

References

[1] 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.

[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. 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.

[9] 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.

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

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

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

[21] 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.

