IJARSE, Vol. No.4, Special Issue (03), March 2015 ISSN-2319-8354(E)

IMAGE STEGNOGRAPHY USING SEPERABLE REVERSIBLE APPROACH

Saranya J[1], Prof. R. Srinivasan[2], Prof. V Saravanan[3]

[1]Student , [2]Professor and Head, [3]Asst Professor

IT Department P.S.V College of Engg& Tech, Krishnagiri, (India)

ABSTRACT

This paper proposes an advanced technique of data hiding in encrypted images by using data hiding key and the encryption key. In this approach, a content owner intending to send a data in a secured manner can encrypt the original uncompressed gray scale image using an encryption key. After encrypting the image, the data which needs to be sent will be embedded by compressing the least significant bit of the encrypted image using a data hiding key. By this way if the receiver has a decryption key of the image, then they can extract the image alone without being able to get the data. Similarly the receiver can get the data alone without the image if they have the data hiding key.

1. INTRODUCTION

In recent years signal processing in encryption has attracted researches to a great extend. For privacy of data the encryption is handled which makes the signals are changed into unintelligible signals. As a result the original signal processing takes place before encryption and after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired.

Stegnagrophy literally “hidden writing.”Nowadays stegnagrophy is most often associated with embedding data in some form of electronic media. The difference between stegnagrophy and the more commonly used cryptography is that while cryptography scrambles and unclear data that can then be accessed publicly (without consequence), stegnagrophy conceals the data altogether. Data from a “covert or source file is hidden by altering insignificant bits of information in an “overt,” or host file. For example, an algorithm designed to embed an audio file might replace information describing frequencies inaudible to the human ear.

For instance, when the secret data to be transmitted are encrypted, a channel resource. 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.

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, 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. In 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 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.

An anonymous fingerprinting scheme that improves the enciphering rate by exploiting the Okamoto-Uchiyama encryption method has been proposed. By introducing the composite signal overhead and the large communication bandwidth due to homomorphic public-key encryption are also significantly reduced. 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.

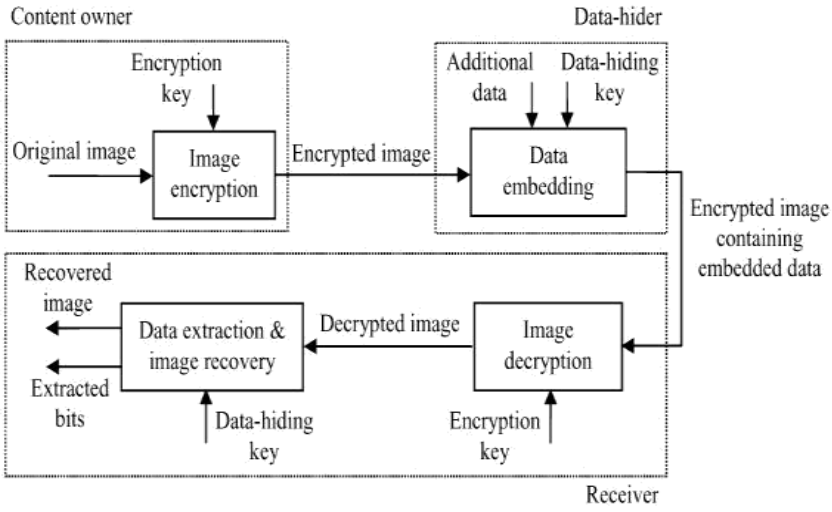

Fig1: Non Separable Reversible Data Hiding

For example 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 the cover data in higher and lower bit-planes of transform domain are respectively encrypted and watermarked. In 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 contains fingerprints are generated for the users.

The reversible data hiding is based mainly on the data embedding/data hiding which is done in a spatial manner. But in some application if someone needs to append message such as origin information or the authentication data within the encrypted image though he does not know the image content he can do that using the data hiding key. The original content is recovered without any error after image decryption in receiver side. Fig 1gives the sketch of reversible data hiding. A content owner encrypts the original image using encryption key and data hider embeds the additional data in encrypted image using data hiding key. In this method the data extraction is not separable that means only after the image decryption we can find the additional data. So first we need to encrypt the image using the encryption key and to add the additional data we need to use data hiding key all these are done in the sender side, and in the receiver side first he needs to decrypt the image using encryption key and then only he can retrieve the additional data using the data hiding key. This is known as non separable approach of data hiding.

This paper approaches a novel scheme for 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 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.

II EXISTING SYSTEM

In some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. 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. 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.

III PROPOSED SYSTEM

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. 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 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.

3.1 Image Encryption

In Image Encryption phase the original uncompressed image is first changed into gray scale image since we use gray scale image for the distortion to be less and the encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and the decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. Scientific community have seen strong interest in image transmission. Because of the illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption /decryption is essential, furthermore.

In this paper, a scheme based on encryption has been proposed for secure image transmission over channels. Assume the original image with a size of N1 * N2 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 bij0,bij1,....bij7 where 1<i<j and 1<j<N2 the gray value as P i ,j and the number of pixels as N (N= N1 * N2).In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated. where r,i,j,u are determined by an encryption key using a standard stream cipher. Then B,i,j,u, are concatenated orderly as the encrypted data:

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

3.2 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. According to a data-hiding key, the data-hider pseudo-randomly selects the encrypted pixels that will be used to carry the parameters for data hiding.

$$\begin{bmatrix} B'(k,1) \\ B'(k,2) \\ \vdots \\ B'(k,ML-S) \end{bmatrix} = \mathbf{G} \cdot \begin{bmatrix} B(k,1) \\ B(k,2) \\ \vdots \\ B(k,ML) \end{bmatrix}$$

Fig 2: Matrix Multiplication for sparse space

The procedure that is followed to do this data embedding is According to a data-hiding key, the data hider randomly selects Np encrypted pixels that will be used to carry the parameters for data hiding. Here, Np is a small positive integer, for example, Np=30. The other (N-Np) encrypted pixels are permuted and divided into a more groups, each of which contains L pixels. The permutation method is 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 , which is composed of two parts as in fig 2. 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 a sparse bit of size S, in which the data is embedded and arrange the pixels into the original form and re-permutated to form a original image.

3.3 Image Decryption

Since the data-embedding operation does not alter any MSB of encrypted image, the decrypted MSB must be same as the original MSB. So, the content of decrypted image is similar to that of original image. The encrypted data in the LSB-planes have been changed by the data-embedding operation, so that the decrypted data in the LSB-planes differ from the original data.

$$\begin{aligned} b'_{i,j,k} &= r_{i,j,k} \oplus B'_{i,j,k} \\ &= r_{i,j,k} \oplus \overline{B_{i,j,k}} \\ &= r_{i,j,k} \oplus \overline{b_{i,j,k} \oplus r_{i,j,k}} \\ &= \overline{b_{i,j,k}}, \qquad k = 0, 1, 2. \end{aligned}$$

On the other hand, if more neighbouring pixels and a smarter prediction method are used to estimate the gray values, the performance of content recovery will be better, but the computation complexity is higher. To keep a low computation complexity, we let *S* be less than ten and use only the four neighbouring pixels to calculate the estimated values. If the lossless compression method in is used for the encrypted image containing embedded data,

the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data.

When the 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 bri,j,k . Clearly, the original 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 pixels block is 0 and the pixel belongs to S0, or the embedded bit is 1 and the pixel belongs to S1 , the decrypted LSB.

3.4 Reversible Data Hiding

If 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,L and 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, we will recover the original gray values of the other (N-Np) pixels. . 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 as in Fig 3. 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 and from the LSB of the selected encrypted pixels.

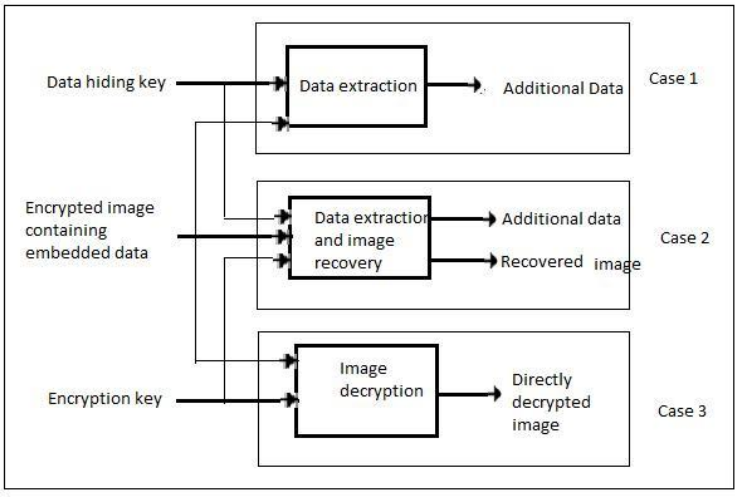

Fig 3: Separable Reversible Data Hiding

Then, the receiver permutes and divides the other pixels into groups and extracts the embedded bits from the LSB-planes of each group. When having the total no of extracted bits, the receiver can divide them into original LSB of

selected encrypted pixels and additional bits. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

IV CONCLUSION

Thus image stegnagrophy method using separable reversible approach will provide an efficient way of sending secured way of sending data over network leaving the hackers with no clues of the data being transmitted. In the first phase, the content owner encrypts the original uncompressed image using an encrypted key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key, to create a sparse space to accommodate the additional data.

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 content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image contains embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image contains embedded data.

However the lossy compression method is compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation.

V FUTURE ENHANCEMENT

In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation. The implemented a Novel Reversible method can be enhanced in future by using the following provisions A MLSB technique can also be applied after embedding when there is lot of change in the pixel to retain nearest to the original value.

VI ACKNOWLEDGMENT

This research is supported by Prof. R.SRINIVASAN, M.E, (Ph.D.), HOD of Information Technology in P.S.V College of Engg. & Technology, Prof. V. Saravanan, M.Sc,., M.C.A., M.Phil., M.E., (Ph.D).,AP/IT Department, P.S.V College Of Engineering And Technology, Krishnagiri. Thanks to my advisors and all researchers in this Department.

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] K. Porkumaran, S. Manimurugan, Pradeep P Mathew "An Assessment on Irrevocable Compression of Encrypted Grayscale Image "International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012

[3] Kuo-Liang Chung a,*, Yong-Huai Huang a, Wei-Ning Yang b, Yu-Chiao Hsu b, Chyou-Hwa Chen" Capacity maximization for reversible data hiding based on dynamic programming approach".

[4] Wei Liu,Wenjun Zeng,Lina Dong and Qiuming Yao"Resolution-Progressive Compression of Encrypted Grayscale Images"

[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] Nasir Memon,Polytechnic University,Ping Wah Wong Apalo.com" A Buyer-Seller Watermarking Protocol"

[7] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE*