International Journal of Research in Advent Technology, Vol.3, No.4, April 2015
E-ISSN: 2321-9637

Data Embedding in Encrypted Images

Prajakta Jagtap[1], Atharva Joshi[2],Shamsundar Vyas[3]
Computer Department[1], Computer Department[2], Computer Department[3]
NBN Sinhgad School of Engineering[1], NBN Sinhgad School of Engineering[2], NBN Sinhgad School of Engineering[3]
prajaktakjagtap@gmail.com[1],aaj5956@gmail.com[2],shamsundarvyas@gmail.com[3]

Abstract - The following paper proposes a novel scheme of reversible data embedding in encrypted image. This work presents a new method that combines cryptography and steganography technique for data hiding and safe image transmission purpose. In order to securely share a secrete image with other person, a content owner may encrypt the image before transmission. 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 images using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if receiver has the data hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he 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, he 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.

Keywords— Encryption, Decryption, lossless data

1. INTRODUCTION

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption is an effective and popular means of privacy protection. Reversible (lossless) data embedding (hiding) has drawn lots of interest recently. Encryption is an effective and popular means of privacy protection. Reversible (lossless) data embedding (hiding) has drawn lots of interest recently. Being reversible, the original cover content can be completely restored. This work proposes a novel scheme for separable reversible data hiding in encrypted images. This work presents a new method that combines cryptography and steganography technique for data hiding and safe image transmission purpose.

In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. 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, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he 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, he 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.

Our scope is to limit unauthorized access and provide better security during message transmission. To meet the requirements, we use the simple and basic approach of steganography and cryptography. Now we will study how the image encryption and image decryption is done.

Image Encryption, illegal data or image access has become more easy and prevalent in wireless and general communication networks .Information security becomes a challenging issue. In order to protect valuable data or image from undesirable readers, Data or image encryption/decryption is essential, further more. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels.

Digital images, accounting for 70% of the information transmission on the internet, is an important parts of network exchanges .However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixel

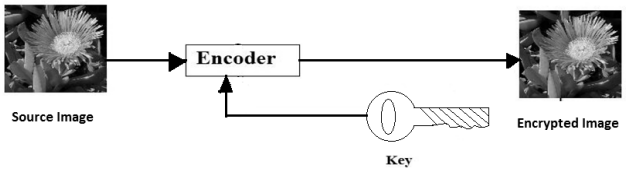

Fig.1

Image Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

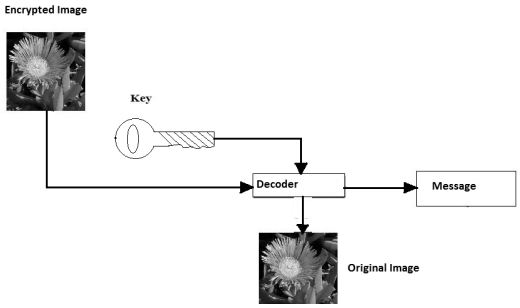

Fig.2

Now we will study the terms cryptography and steganography. They are explained as follow,

Cryptography is derived from two Greek words which mean “secret writing”. Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others. The original text, or plaintext, is converted into a coded equivalent called cipher text.Cryptography is an effective way to protect the information that is transmitting through the network communication paths. Cryptology is the science that deals about cryptography and cryptanalysis. Cryptography is the approach of sending the messages secretly and securely to the destination. Cryptanalysis is the method of obtaining the embedded messages into original texts. In general, cryptography is transferring data from source to destination by altering it through a secret code.

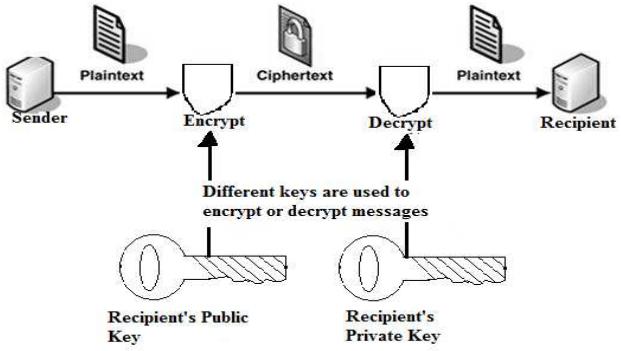

Fig.4: General model of cryptographic system.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word Steganography is of Greek origin and means "concealed writing "meaning "covered or protected", Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is high security technique for long data transmission. Steganography is the process of hiding the one information into other sources of information like text, image so that it is not visible to the natural view.

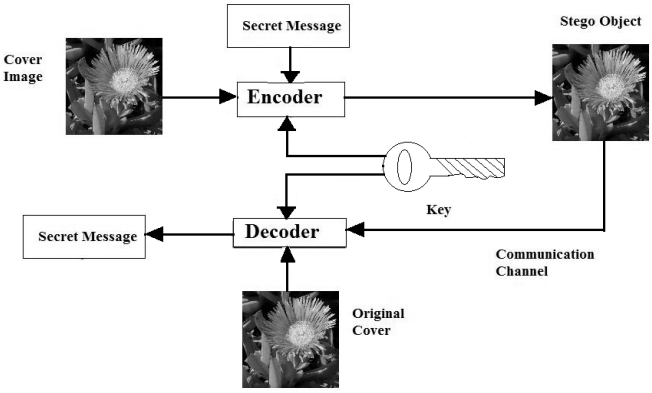

Fig.3 Block diagram of Steganography.

2. PROPOSED SCHEME

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 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.

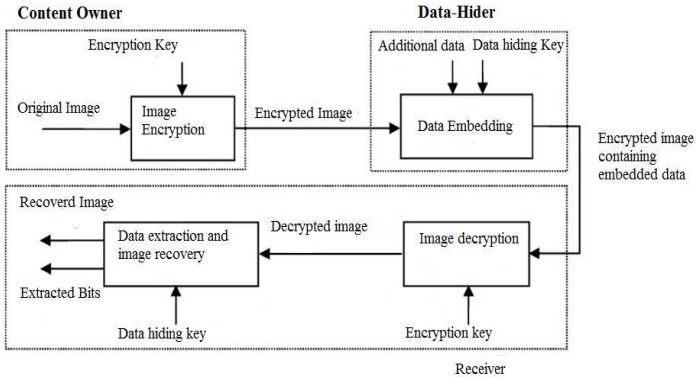

Fig.5

3. THE PROCESSING

Data is hidden in the encrypted images by allocating memory before encryption. It is used to recover the original data without any loss or errors. It is basically used in the medical institutes, military institutes and law forensics, where the distortion of the original image is not permitted.

In this process, the first step is to reserve the memory space in the image for embedding of data. This sort of reservation is beneficial because it saves time for creating space for data on time. The next step is image encryption in which the image is encrypted. There are a number of methods for encryption of images such as image partition in which image is divided into two parts. Then part A is reversibly embedded into the part B. That is least significant bits are embedded first in part B.

Then the process of data hiding is done using the separable reversible data hiding. 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. This additional data is restored back in image to get image with original quality at the receiver's end.

At the receiver end, two tasks are carried out viz. data extraction & image recovery. But, to extract the original cover from the encrypted image, an additional task known as image restoration needs to be carried out. In this additional step, the original key contents are restored in the image.

With an encrypted image containing extra data, if a user at the receiver's end has the key for decryption, he can extract the data even if he does not know the image content to extract the additional data. If the receiver has the key for encryption, he can decrypt the received data to get an image similar to the original image, but cannot extract the extra data.

If the user at the receiver's end has both the encryption as well as the decryption key then he/she can extract the extra data as well as the original image error-free by using the spatial correlation in normal image when the amount of additional data is not large.

4. ALGORITHM USED

LSB (Steganography) Algorithm:

Step 1:

Extract Bit set of Message ,
Bit={M0,M1,……, M65535 }

Step 2:

The Pixels of cover image ,
Pixel ={pixel0, pixel ,…, pixel65535}

Step 3:

Extract LSB-1 set of the cover image,
LSB1={A0, A1,…,A65535}.

Step 4:

Extract LSB-2 set of the cover image,
LSB2={B0, B1,…, B65535}.

Step 5:

For i=1 to message length do
{ If Mi= =Bi Then do nothing Else
{If Mi= =1 and Bi= =0 Then
{Bi=Mi; Ai=0; Pixel(i)-=1 }
Else If Mi= =0 and Bi= =1 Then
{Bi=Mi; Ai=1; Pixel(i)+=1 } } }

DES Algorithm:

Step1:

Fractioning of the text into 64-bit (8 octet) blocks;

Step2:

Initial permutation of blocks;

Step3:

Breakdown of the blocks intsssso two parts: left and right, named *L* and *R*;

Step3:

Permutation and substitution steps repeated 16 times (called rounds);

Step4:

Re-joining of the left and right parts then inverse initial permutation.

4. OBJECTIVE

The objective of this project is to provide an efficient data hiding technique and image Encryption in which the data and image can be retrieved independently. The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination .There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like cryptography and steganography.

5. CONCLUSION AND FUTURE SCOPE

In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data extraction/image recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption 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 one using only the encryption key.

The lossless compression method 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. However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

The future of encryption is brighter than ever before. Demand for control and protection of corporation information assets and third-party information is increasing now a days. Everyday large amount imformation is being communicated. Hence need for more effective information security products is growing at a higher rate.

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 gray scale 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. VideoTechnol.*, 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.