JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-11 E-ISSN: 2347-2693

Distinct Revocable Data Hiding In Ciphered Image

Anamika Patil[1*], Pooja Bafna[2], Mona Pounikar[3], Pranjal Badgujar[4]

[1*,2,3,4]Department of Computer, MET BKC IOE, Nashik, India

www.ijcaonline.org

Received: Oct/22/2014 Revised: Nov/02/2014 Accepted: Nov/20/2014 Published: Nov/30/2014

Abstract— The rapid development of data transmission through internet made it easy to send the data at faster rate to the destination. This work proposes a scheme for distinct revocable data hiding in ciphered images. At first, a content owner encrypts the original image with help of the encryption key. Then, the LSB of the encrypted image are compressed using a data-hiding key by the data hider to create a space to include some data. If a receiver has the data-hiding key, the additional data can be retrieved easily. And if the receiver has the encryption key, he can easily decrypt the received data to get the image similar to the original one, but cannot obtain the data. In case if the receiver has both the data-hiding key as well as the encryption key, he can obtain the data and regain the original image content. Hence, in order to transfer the data securely to the destination without any modifications, there are many techniques like cryptography and about the various steganographic algorithms like Least Significant Bit (LSB) algorithm.

Keywords- *Data hiding; Crptography; Steganography*

I. Introduction

In the recent trends of the world, the technologies have advanced so much that every individual prefer using the internet as the primary source to transfer data across the world. However, one of the main problems with sending data over the internet is the security threat. Data security basically means protection of data from unauthorized users or hackers and providing security to prevent data modification. Therefore it becomes very vital to take data security into consideration, as it is one of the most important factors that require attention during the process of data transfer. Distinct revocable data hiding in ciphered image also means hiding data reversibly in encrypted image in separable manner. Nowadays data transmission over internet has increased tremendously so image security has become an important factor to be considered for e.g., video and confidential transmission, medical and military applications. As in medical field the necessity of fast and secure diagnosis is very important in the medical world. To reduce the transmission time over network, the data compression has become necessary.

Reversible data hiding (RDH) in images is a method, by which the original image can be losslessly recovered after the embedded message is extracted from it. In order to provide confidentiality for images, encryption is a popular mean as it converts the original content to incomprehensible one. There are some applications in RDH that can be applied to encrypted images. This process of extracting data from image requires compression of encrypted images and space for data hiding. Compression of encrypted data can be considered as source code with some side information at the decoder, in which the typical method is to generate the compressed data in reversible manner by exploiting the syndromes of parity-check matrix of channel codes [4]**.** In this paper we propose a scheme which achieves real reversibility by reserving room before encryption with a RDH algorithm, then encrypting the data and embedding the data in the encrypted image. This method can achieve real reversibility that is data extraction and image recoveries are error free.

Corresponding Author: Anamika Patil

II. Reversible Data Hiding

Reversible data hiding in images is a method that hides data in images for secret and secured communication. It is a technique to hide additional data into cover media in a reversible way so that the original cover content can be recovered after obtaining the hidden information. Data hiding is used for secret as well as secured communication. In many applications, the embedded carriers are encrypted to protect the carrier from being analyzed to show the presence of the embedded information. Other applications could be used when the owner of the carrier might not want the other person, to know the content of the carrier before data hiding is done. The two levels of security for digital image encryption are: low level and high-level security encryption. In low-level, the image has low visual quality compared to that of the original image. In the high-level, the content of image is completely scrambled and the image looks like random noise. Selective encryption aims at avoiding the encryption of all bits of a digital image and also ensures a secure encryption standard [5].

In our method, we first empty the memory space by embedding LSBs of pixels into other pixels with a RDH method and then apply encryption on the image, so the positions of these LSBs in the encrypted image can then be used to embed data. Not only does this method separate data extraction from image decryption but it also achieves better performance in a different way that is real reversibility is realized, so that we can say data extraction is error free. Most of the work on reversible data hiding focuses on the data embedding and data extracting. But, in some applications, the owner appends some additional message, image notation within the encrypted image though he does not know the original image content. And also it is hopeful that the original content should be recovered without any error after image decryption and message extraction on receiver side is completed. Reversible data embedding is a secret communication medium since reversible data embedding can also be used as a data carrier. Reversible data embedding embeds data into image in a reversible way. Amazing feature of reversible data embedding is the reversibility that is we can remove the embedded data in order to recover the original image. Reversible data embedding hides some data in image in such a way that only the authorized party can decode the hidden information and also recover the image.

III. EXISTING SYSTEM

In Reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded in to the image by using the data hiding key. At the receiver side he first need to extract the image using the encryption key in order to extract the data and after that he'll use data hiding key to extract the additional embedded data. It is a serial process, not a separable process. Steganography is the art and science of writing hidden messages in such a way that no one, apart the sender and receiver, knows about the existence of the message.

The word Steganography is a Greek word which means "concealed writing". The messages will appear to be something else: images, articles, lists, or some other text and the hidden message may be in invisible ink between the visible lines of a letter. Steganography is the process of hiding the one information into other sources of information like text, image so that it is not visible. There are varieties of stenographic techniques available to hide the data depending upon the carriers.

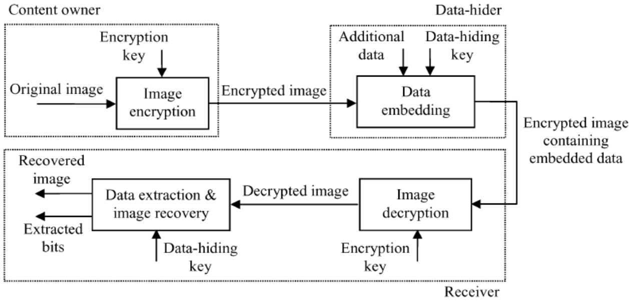

Fig. 1. Sketch of non-separable reversible data hiding in encrypted image.

In the existing system, the image is compressed and encrypted using the encryption key and the data to be hidden is embedded in to the image using the data hiding key. The owner encrypts the original image using an encryption key, the data-hider can then embed additional data into the encrypted image using a data-hiding key. With an encrypted image containing additional data, a receiver should first decrypt the image, and then he can extract the embedded data and thus recover the original image by using the data-hiding key [2]. Here data extraction and data decryption are not separable, i.e the data must be extracted from the decrypted image, so that the principal content of our original image is known before data is extracted, and, if anyone has the data-hiding key but not the encryption key, then he cannot extract any data from the encrypted image containing additional data as shown in Fig 1.

IV. PROPOSED SYSTEM

Here, the transactions will occur in a secured format between various clients over network. It provides flexibility to the user to transfer the data through the network very easily by compressing the large amount of information. It will identify the user and provide the communication according to the security standards. The user who is going to receive the file will do the operations like de-embedding, decryption, and uncompression in their level of hierarchy and get the information. Compressing the data will increase the performance of data transfer and embedding the encrypted data will assure the security while the transferring data over network.

The proposed scheme consists of image encryption, data embedding and data-extraction or image-recovery. The content owner first encrypts the original image using an encryption key to obtain an encrypted image. Then, the least significant bits (LSB) of the encrypted image are compressed using a data-hiding key in order to create a sparse space to accommodate some additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image according to the data-hiding key. Since the data embedding only affects the LSB, a decryption using an encryption key can then give us an image similar to the original one. By using both the encryption as well as the data-hiding key, the embedded additional data can be successfully retrieved and also the original image can be perfectly recovered [2].

This paper proposes a method for distinct revocable data hiding in ciphered image. As shown in Fig. 2, the content owner initially reserve enough space on original image to embed data and then converts the image into its encrypted form using an encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider as he only needs to accommodate data into the created space. The data extraction phase and image recovery phase are similar to that of Framework Vacating room after encryption. In the new framework, we follow the idea that first reversibly compresses the redundant image content and then encrypts in order to protect privacy and maintain security. Next, we consider a practical method based on the Framework Reserving space before encryption, which contains four stages: initially creating an encrypted image, data hiding in that encrypted image, then data extraction and image recovery.

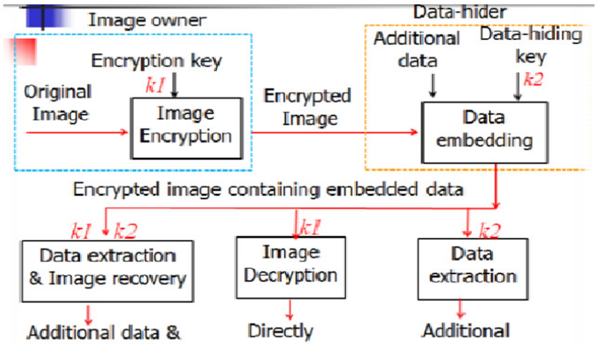

Fig 2. Sketch of distinct revocable data hiding in ciphered image

Advantages:

- If the receiver only has the data-hiding key, he can extract the additional data also if he does not know the image content.
- If he has only the encryption key and not the data hiding key he can easily decrypt the received data to obtain an image similar to the original image, but cannot obtain the additional data.
- If he receiver has both the data-hiding key as well as the encryption key, can extract the additional data and also recover the original image without any error when the additional data is not too large

V. IMAGE ENCRYPTION

The user will initially encrypt the image, then the system will auto generate an encryption key for encryption. Encryption applies special mathematical algorithms and keys so as to transform digital data into cipher text before they are transmitted further and then decryption applies mathematical algorithms and keys to get back the original data from cipher text. As information privacy becomes a challenging issue thus in order to protect valuable and secret data or image from unauthorized users, data or image encryption or image decryption is important.

Consider an original image with a size of Q1 * Q2 which is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. We can denote the bits of a pixel as bij0,bij1,....bij7 where 1<i<Q1 and 1<j<Q2, represent the gray value as P i ,j and the number of pixels as Q (Q= Q1 * Q2).In encryption phase, we calculate the pseudo-random bits and exclusive-or the results of the bits, where

$$Bi,j,u \ = bi,j,u \ \oplus \ ri,j,u$$

r, i, j, u can be determined by using an encryption key. Then B, i, j, u, are concatenated in an ordered manner as in encrypted data.

VI. DATA EMBEDDING

In data embedding process, user will hide the encrypted data in encrypted image and system will then automatically generate data hiding key. In this stage, we embed few parameters into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a sparse space for so that we can accomodate the additional data and the original data at the positions obtained by the parameters. The data-hider will randomly select Np encrypted pixels using a data hiding key that will be used to carry the parameters for data hiding. Np is a small positive integer, for example, Np=20. The remaining (N-Np) encrypted pixels are permuted and divided into a number of groups, each group will contain L pixels. We can determine the permutation way by using the data-hiding key. For each pixel-group, for L pixels select the M least significant bits, and represent them as B (k,1) , B (k,2) B(k,M*L) where k represents a group index within [1,(N-Np)/L] and M represents a positive integer less than 5. The data-hider generates a matrix G, which is made up of two parts. The left part represents identity matrix and the right part represents pseudo-random binary matrix which is obtained from the data-hiding key. Now for each group, which is product with the G matrix to form a matrix of size (M * L-S), that has a sparse bit of size S, in which the data is embedded and the pixels are then arranged into the original form and re-permutated to form an original image.

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

VII. IMAGE DECRYPTION

The user will firstly browse data that he wish to send to receiver and then encrypt the original data and the system will auto generate the data encryption key. The content owner encrypts the original image using an encryption key. Even if the data-hider does not know the original content, he can easily compress the least significant bits of the encrypted image using a data-hiding key to create some space so as to accommodate the additional data. Now with an encrypted image containing additional data, by using a data hiding key receiver can obtain the additional data, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys with him, he can extract the additional data as well as he can recover the original content without any error. Having an encrypted image containing embedded data, using encryption key receiver first generate ri,j,k, and then calculates the exclusive-or of the received data and ri,j,kso as to decrypt the image. We can denote the decrypted bits as bri,j,k.

The original most significant bits (MSB) are retrieved correctly without any errors. Now for a certain pixel, if the embedded bit which is in the block including the pixel is zero and the pixel is belonging to D1, or if the embedded bit is 1 and the pixel that is belonging to D0, then the data-hiding will not affect any encrypted bits of the pixel. So, the three LSB which are decrypted must be same as the original LSB, which implies that the decrypted gray value of the pixel is correct. In other way, if the embedded bit in the pixels block is zero and the pixel is belonging to D0, or the embedded bit is one and the pixel is belonging to D1, the decrypted LSB.

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

VIII. DATA EXTRACTION

As data extraction is totally independent from image decryption, the two different practical applications which are as follows:

1) Obtaining Data from Encrypted Images:

In order to update some personal information of images which are encrypted for protecting privacy, the database manager will only get access to the data hiding key and will have to calculate data in encrypted domain. Order of data extraction before image decryption will guaranty the feasibility of our work. When the database manager will get the data hiding key, then he will be able to decrypt the LSB-bits of encrypted image of A which is denoted by AE, and then obtain the additional data z by directly reading the decrypted image. When we request for updating information of encrypted images, the database manager, will then update information through LSB replacement and will encrypt updated information according to the data hiding key. Now the entire process is completely operated on encrypted domain, so it will avoid the leakage of original data.

2) Obtaining Data from Decrypted Images:

In 1, embedding and extraction of the data both are calculated in encrypted domain. In other way, there is another situation that the user will want to decrypt the image first and then obtain the data from the decrypted image when it will be required. The following example illustrates an application for such scenario. Consider Alice outsourced her images to a cloud server, and the images are encrypted in order to protect their data into the encrypted images, by embedding some notation the server will mark the images, including the identity of the images owner and the identity of the time stamps and the cloud server, so as to manage the encrypted images. The server has no authority to do any kind of permanent damage to the images. Only an authorized user, Bob who has the encryption key and the data hiding key with him, downloaded the images and then he decrypted the images. Bob marks decrypted images, so that decrypted images will include the notation, this notation can be used to trace the history and origin of the data. Order of image decryption before data extraction or without data extraction is suitable in this case.

If the receiver has both the data-hiding key and encryption key, he may hope to obtain the embedded data. Now according to the data-hiding key, the values of M,S and L, the LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can then be obtained from the encrypted image which containing embedded data. Now by placing the Np LSB into their original positions, the data which is encrypted of the Np selected pixels are retrieved, using the encryption keys their original gray values can be appropriately decrypted. We will recover the original gray values of the other (N-Np) pixels. This paper proposes a novel scheme for distinct revocable data hiding, that is, separable reversible data hiding in encrypted image.

In the proposed scheme, by using an encryption key we can encrypt the original image and by using a data hiding key the additional data can be added in to the encrypted image. Now along with an encrypted image containing additional data, if the receiver only has the data-hiding key, then he can only extract the additional data embedded inside the image even if he is not aware about the image content. If the receiver only has the encryption key, and not the data hiding key then he can decrypt the received data to obtain an image similar to the original image, but then he cannot extract the additional data. In other case, if the receiver has both the data-hiding key as well as the encryption key, then he can obtain the additional data and also recover the original image content without any error when the amount of additional data is considerably small.

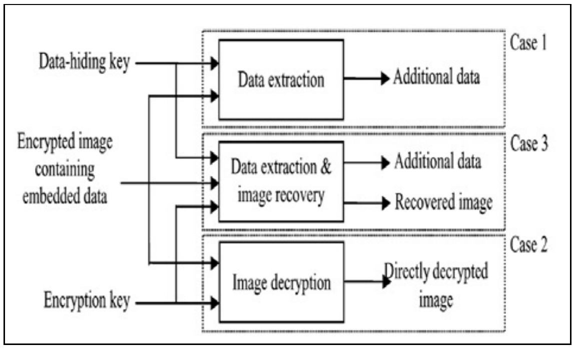

Fig 3. Three cases at receiver side

IX. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed a novel scheme for distinct revocable data hiding in ciphered image which consists of 3 phases: image encryption, data-extraction and data embedding. In the first stage, the content owner using an encryption key encrypts the original image. Although the data-hider does not know the original content, using a data-hiding key he can compress the least significant bits of the encrypted image so as to create a sparse space to embed the additional data into the encrypted image. With an encrypted image containing additional data, the receiver can extract the additional data using only the data hiding key, or obtain an image exactly similar to the original image using the encryption key. When the receiver has both the keys, the data hiding key as well as encryption key, he can extract the additional data and also recover the original content. If the lossless compression method is used for the encrypted image which contains embedded data, the additional data can still be 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.

The reversible compression method is used for the encrypted image containing embedded data, the additional data can be extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing additional data. Reversible data hiding in encrypted images is a new concept which attracts our attention due to the privacy-preserving requirements from cloud data management. This study helps constructing secure and secret transmission of secrete file in order to prevent any unauthorized party access information and security level of data is increased. We also provide protection for keys during decryption process so that even if any hacker attacks on system it should be secure. In further future, video, audio in case of image as cover for data hiding can also be used.

ACKNOWLEDGMENT

We wish to thank the Department of computer of MET BKC IOE College Nasik for providing the materials and their support during the course of this work.

REFERENCES

[1] Study On Separable Reversible Data Hiding In Encrypted Image, International Journal Of Advancements In Research & Technology, Volume 2, Issue 12, December-2013 223 ISSN 2278-7763.

[2] Xinpeng Zhang, Separable Reversible Data Hiding In Encrypted Image**,** IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[3] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, And Fenghua Li, Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013.

[4] Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade, Hide Inside-Separable Reversible Data Hiding In Encrypted Image, International Journal Of Innovative Technology And Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-9, February 2014.

[5] Jun Tian, Reversible Data Embedding Using A Difference Expansion, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 13, NO. 8, AUGUST.

[6] 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.

[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] Kede Ma, Weiming Zhang, Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption, IEEE Trans. VOL. 8, No. 3, Mar 2013.