International Conference on Emerging Trends in Engineering, Technology, Science and Management
IIMT College of Engineering, Greater Noida, India (ICETETSM-17)
12th April 2017, www.conferenceworld.in ISBN: 978-93-86171-38-2

EFFICIENT DATA HIDING TECHNIQUE IN ENCRYPTED IMAGE

Chetan G. Tappe[1], Anil V. Deorankar[2]

[1]*P.G. Student, Department of Computer Engineering, Govt. College of Engineering, Amravati (India)*

[2]*Associate Professor, Department of Information Technology, Govt. College of Engineering, Amravati (India)*

ABSTRACT

This work proposes a novel revocable data hiding system for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With ancoded image containing additional data, one may to start with decrypt it using the encryption key, and the decrypted version is similar to the original image. Allowing to the data-hiding key, with the utility of spatial association in normal image, the inserted data can be successfully extracted and the original image can be perfectly recovered.

Keyword- Data hiding, encrypted image, embedded data, reversible image.

I. INTRODUCTION

This paper propose data hiding is a technique to embed added message into some distortion-unacceptable cover media, such as army or medical images, with a reversible manner so that the real cover content can be perfectly retrieve after extraction of the hidden message. A number of reversible data hiding methods have been suggested in recent years. In difference expansion method, differences between two adjacent pixels are crumpled to generate a new least significant bit (LSB) plane for accepting extra data. A data hider can also implement reversible data hiding using a histogram shift mechanism, which utilizes the zero and peak points of the histogram of an image and faintly change the pixel gray values to insert data into the image. Another kind of method makes use of dismissal in a cover by performing lossless compression to create a extra space for data embedding. Furthermore, various skills have been introduced into the typical reversible data hiding methods to improve the performance. As is well known, encryption is an in effect and popular means of secure protection. In order to securely share a secret image with other person, a data owner may encrypt the image before transmission. In some

application scenarios, an inferior assistant or a channel administrator hopes to append some added message, such as the origin data, image symbolization or secret data, within the encrypted image though he does not know the original image data. For example, when medical images have been encrypted for protecting the patient secrecy, a database manager may aim to embed the private information into the consistent encrypted images. It may be also confident that the original content can be retrieve without any error after decryption and recover of extra message at receiver side. That means a reversible data hiding scheme for encrypted image is necessary.

Data security basically means protection of data from illegal users or hackers and providing high safety to avoid data medication. This region of data safety has gained more consideration over the recent period of time due to

the enormous increase in data transmission rate over the internet. In order to increase the safety features in data transfers over the internet, many methods have been developed like: Cryptography, Steganography. While Cryptography is a process to conceal data by encrypting it to encryption texts and transmitting it to the proposed receiver using an unknown key, Steganography provides further security by beating the cipher text into a really invisible image or other formats.

In new years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and common means for confidentiality protection, encryption translates the ordinary signal into meaningless data, so that the modern signal processing usually takes place before encryption or after decryption. However, in some consequences that a content holder does not trust the processing service provider, the ability to work the encrypted data when keeping the basic content secret is preferred. For example, when the secret data to be transferred are encrypted, a channel provider without any knowledge of the cryptographic key may tend to wrapping the encrypted data due to the partial channel resource. While an encrypted second image can be compacted with a lossless manner by finding the syndromes of low-density parity-check codes. With the loss density method an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of numbers generated from orthogonal transform. When having the compressed data, a receiver may rebuild the basic content of original image by recovering the values of coefficients.

Data hiding is a technique that is recycled to hide info in numeral media such as images, audio, video etc. The data that is hidden depends upon the purpose of application. Owing to data hiding, some distortion may ensue in the unique cover medium and cannot be reversed back to the unique medium. Such a data hiding is called lossy data hiding. But in applications such as medical image system, law application, remote sensing, military imaging etc it is preferred to recover the original image gratified with greater accuracy for legal considerations. The data hiding scheme that satisfies this requirement is called revocable or lossless data hiding. Reversible data hiding was main proposed for verification and its important feature is reversibility. It hides the secret data in the alphanumeric image in such a way that only the legal person could decode the secret information and restore the original image. Several data hiding methods have been proposed. The routine of a reversible data embedding algorithm is measured by its load capacity, complexity, visual quality and security. Earlier methods have lower embedding capacity and lowly image quality. As the inserting capacity and image superiority improved, this method changed a covert communication channel. Not only should the data hiding algorithm be given importance. The image on which the data is hidden should also be highly secured.

II. LITERATURE WORK

Zhang separated the encrypted image into some blocks. By flipping 3 LSBs (least significant bits) of the half of pixels in each block, room can be vacated for the embedded bit. The data insertion and image retrieval proceed by finding which part has been flipped in one block. This process can be recognized with the help of spatial association in the decrypted image. The decoder side by further exploiting the spatial correlation using a dissimilar estimation equation and side match technique. For both methods in [2] and [3], decrypting image and extracting data must be jointly executed.

Recently, Zhou et al. [5] proposed a novel RDH-EI method for joint decryption and extraction, in which the correlation of plaintexts is further exploited by unique the scrambled and non-scrambled pixel blocks with a

two-class classifier. To separate the data extraction from image decryption, Zhang emptied out space for data embedding by directly using the typical manner of cipher text compression that is, compressing the encrypted pixels in a lossless manner by using the syndromes of parity-check matrix of channel codes.

Newly Weiming Zhang, Hui Wang, DongdongHou, and Nenghai Yu proposition a novel context [1], for RDH-EI based on reversible image transformation (RIT). Different from all previous encryption-based contexts, in which the cipher texts may invite the representation of the snooping cloud, RIT-based context permits the user to transform the contented of real image into the content of another entity image with the same size. The converted image that looks like the target image is used as the scrambled image. Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide other message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

The proposed method is inspired by Lai and Tsai [6], they first uses the concept of mosaic image in the field of information security. The type of mosaic image used by them is secret fragment visible mosaic image that is formed by dividing the source image into small tiles or block and arranging these blocks in random position with respect to target image. The target image is required to be selected from database. The database plays a vital role for mosaic image creation so for better result the database should be sufficiently large in size. For target image selection we have to scan the database in search of image with highest similarity measure with respect to given secret image.

III. PROPOSE WORK

In existing system reversible data hiding technique the image is compacted and encrypted by using the encryption key and the data to hide is entrenched in to the image by using the data hiding key. At the receiver side he first need to source the image using the encryption key in order to mine the data and after that he'll use data hiding key to extract the inserted data. It is a serial process and is not a independent process.

With an encrypted image containing added data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is comparable to the unique image. Allowing to the data-hiding key, he can more abstract the inserted data and recover the unique image from the decrypted version.

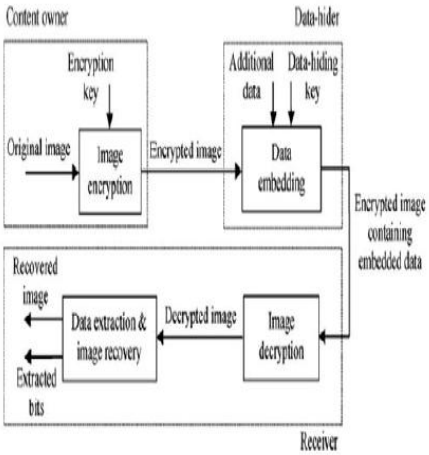

Fig. 1 Propose system

A. Least Significant Bits

The possibility of incorrect LSB-decryption is 1/2, when renovating an image using the decrypted data, the value of PSNR in the decrypted image is nearly

$$PSNR = 10\log_{10}\frac{255^2}{\frac{EA}{2}} \quad (1)$$

Then, the receiver will extract the inserted bits and convalesce the original content from the encrypted image. Allowing to the data-hiding key, he may section the decrypted image into blocks and split the pixels in each block into double sets in a same way. For each decrypted block, the receiver flips all the three LSB of pixels in to form aoriginal block, and flips all the three LSB of pixels in to form another innovative block. We denote the binary original blocks as and There must be that either or is the original block, and another one is more seriously

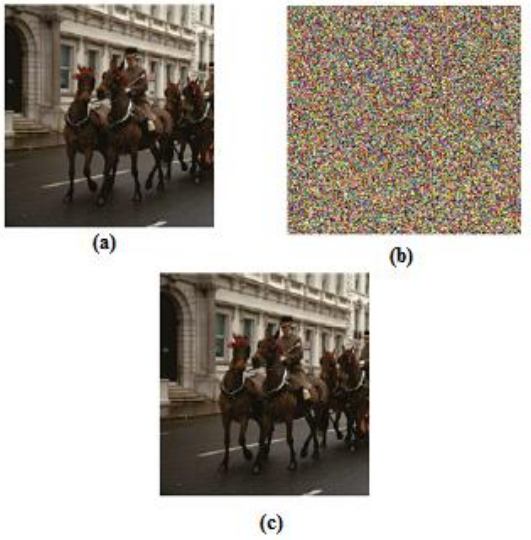

Fig.2. (a) Original image (b) Encrypted image(c) Decrypted original image.

Interfered due to the LSB flip operation. For the two blocks sized by define a function to measure the fluctuation in them

$$f = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p_{u,v}-\frac{p_{u-1,v}+p_{u,v-1}+p_{u+1,v}+p_{u,v+1}}{4}\right| \quad (2)$$

and denote the values of fluctuation function of and as and , respectively. Because of spatial association in normal image, the variation function of original block is generally inferiorthan that of a extremely interfered version. So, the receiver can execute data extraction and image retrieval by comparing and If regard as the unique content of the block and let the extracted bit be 0. Otherwise, respect as the original content of this block and extract a bit 1. Finally, concatenate the mined data to retrieve the added message and collect the recovered blocks to form the original image.

IV. CONCLUSION

The proposed system is improves the Reversible Data Hiding (RDH) scheme present in existing system. The improvement will be achieved using Reversible Encrypted Data Hiding in Encrypted Image in which the data and the image will be retrieved independently.

Used for the encrypted image containing embedded data, the additional data can be still extracted and the real content can be also recovered since the data compression does not modified the content of the encrypted image containing embedded data. Although a data-hider does not know the original content, he can compress the least significant bits of the encoded image using a data-hiding key to create a scrubby space to provide accommodations the added data. With an encrypted image containing extra data, the receiver may extract the extra data using only the data-hiding key, or obtain imagecomparable to the original one using only the encryption key.

REFERENCES

[1]. Weiming Zhang, Hui Wang, DongdongHou, and Nenghai Yu proposition a novel context for "RDH-EI based on reversible image transformation" IEEE Transactions On Multimedia, Vol. 18, No. 8, August 2016

[2]. Z. Ni,Y.-Q. Shi,N. Ansari, andW. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.

[3]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[4]. Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Image" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012

[5]. J. Zhou et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. Circuits Syst. Video Technol., vol. 26,

[6]. Lai and Wen. Tsai, "Secret-fragment-visible mosaic image-a new computer art and its application to information hiding," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 936–945, Sep. 2011.

[7]. 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