ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

Survey on Efficient Reversible Data Hiding in Encrypted Images Transformation

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

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

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

ABSTRACT: With the regard of outsourcing data to the cloud,it is protect the confidentiality of data and support the cloud server to simply achieve the data at the same time. Under such strains, reversible data hiding in encrypted images (RDH-EI) invites more and more scientists' attention. In this paper, we propose a novel framework for RDH-EI based on reversible image transformation (RIT). Different from all earlier encryption-based frameworks, in which the cipher texts may interest the system of the snooping cloud, RIT-based framework allows the user to transform the content of new image into the content of another object image with the same size. The transformed image, which looks like the target image, is used as the "encrypted image," and is outsourced to the cloud. Therefore, the cloud server can simplyembed data into the "encrypted image" by any RDH methods for plaintext images. And thus a client-free scheme for RDH-EI can be recognized, that is, the data-embedding development executed by the cloud server is irrelevant with the processes of both encryption and decryption.

KEYWORDS: RDH, Image encryption, Secure communication, Cloud, Reversible image transformation (RIT).

I. INTRODUCTION

The expanse of digital images has increased quickly on the Internet. Image security becomes gradually important for many applications, e.g., confidential transmission, video investigation, army and medical uses. For example, the requirement of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily uses routine and it is necessary to find an effective way to transmit them over systems. To decrease the communication time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding processes. Since few years, a difficult is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were suggested in to associationimage encryption and compression. Two main sets of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are some methods to encrypt binary images or gray level images.

The next group bases the protection on data hiding, designed at secretly embedding a message into the data. Nowadays, a new task consists to embed data in encrypted images. Earlier work proposed to embed data in an encrypted image by using an irreversible method of data hiding or data hiding, intended at secretly embedding a message into the data. A originalknowledge is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Latest reversible data hiding methods have been proposed with high size, but these methods are not applicable on encrypted images.

Data security basically means protection of data from illegal users or hackers and providing high security to check data medication. This area of data security has gained more attention over the recent period of time due to the huge increase in data transmission rate over the network. In order to recover the security types in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a technique to secrete information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image.

On the other hand, cloud service for outsourced storage makes it challenging to protect the privacy of image contents. For instance, recently many private photos of Hollywood actress leaked from iCloud.Although RDH is helpful for managing the outsourced images, it cannot protect the image content. Encryption is the most popular technique for

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

protecting privacy. So it is interesting to implement RDH in encrypted images (RDHEI), by which the cloud server can reversibly embed data into the image but cannot get any knowledge about the image contents. Inspired by the needs of privacy protection, many methods have been presented to extend RDH methods to encryption domain. From the viewpoint of compression, these methods on RDH-EI belong to the next two frameworks: Framework I "vacating room after encryption (VRAE)" and Framework II "reserving room before encryption (RRBE)."In the framework 'VRAE," the cloud server inserts data by lossless vacating room from the encrypted images by using the idea of compressing encrypted images Compression of encrypted data can be communicated as source coding with side information at the decoder. Usually the side information is the correlation of plaintexts that is exploited for decompressionby the decoder. In divided the encrypted image into several 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 extraction and image retrieval proceed by finding which part has been reversed in one block. This process can be realized with the help of spatial association in the decrypted image. The decoder side by further exploiting the spatial correlationusing a different estimate equation and side match system. For both methods in decrypting image and extracting data must be jointly executed. Recentlyproposed a novel RDH-EI method for joint decryption and extraction, in which the correlation of plaintexts is further exploited by distinguishing the encrypted and non-encrypted pixel blocks. The set of paper is systematized as follows. In section ii, Related work and summarize the main contributions novel frame work. A method of RDH in encrypted image elaborated in section iii, and Section iv RIT method are proposed, The paper is conclude in section v.

II. RELATED WORK

The reversibly embed the message into the host sequence by modifying its histogram with methods like histogram shifting [8] or difference expansion. Recently, Zhang et al. proposedthe optimal histogram modification algorithm [4], for RDH by estimating the optimal modification probability.

Zhang divided the encrypted image into several 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 extraction and image recovery proceed by finding which part has been flicked 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 distinguishing the encrypted and non-encrypted pixel blocks with a two-class SVM classifier. To separate the data extraction from image decryption,

Zhang [7] 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.

Recently Weiming Zhang, Hui Wang, Dongdong Hou, and Nenghai Yu propose a novel framework [1], for RDH-EI based on reversible image transformation (RIT). Different from all previous encryption-based frameworks, in which the cipher texts may attract the notation of the curious cloud, RIT-based context allows the user to transform the contented of original image into the content of another object image with the same size. The transformed image that looks like the target image is used as the "encrypted 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.

III. REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

Data hiding is used for secure communication. In some uses, the embedded carriers are further encrypted to prevent the carrier from being studied to disclose the presence of the embedment. Other uses could be for when the owner of the carrier might not want the other one, including data hider, to know the content of the transferor before data hiding is actually performed, such as army images or personal medical images. In this case, the content holder has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded data and recover the original image. Many reversible data hiding techniques have been proposed newly .As is well known, encryption is an active and standard means of privacy protection. In order to securely share a private image with other person, a content holder may encrypt the image before transmission. In some application scenarios, an lessersupporter or a channel proprietor hopes to append some additional message, such as the origin data, image notation or verification data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for secure the patient privacy, a database administrator may goal to embed the personal data into the corresponding encrypted images.

It may be also encouraged that the unique content can be recovered without any error after decryption and retrieve of additional message at receiver side. Conventionally, data hiding is used for secret message. In some uses, the embedded carriers are further encrypted to prevent the carrier from being analyzed to expose the presence of the embedment. Other uses could be for when the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

vender of the transferor might not want the other person, including data hider, to know the contented of the carrier before data hiding is actually achieved, such as army images or private medical images.

In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. A major recent trend is to minimize the computational necessities for secure multimedia distribution by selective encryption where only parts of the data are encrypted. There are binary levels of security for digital image encryption: small level and big security encryption. In low-level security encryption, the encrypted image has corrupted visual quality compared to that of the original one, but the contented of the image is still visible and logical to the viewers. In the high-level security case, the content is completely twisted and the image just looks like random noise. In this case, the image is not clear to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a arithmetical image and yet confirming a protected encryption.

Reversible data hiding is a system to embed additional message into some distortion-unacceptable cover media, such as army or remedial images, with a reversible manner so that the new cover contented can be perfectly reconstructed after extraction of the hidden message. As an real and popular means for privacy protection, encryption transforms the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption. However, in some environments that a content owner does not trust the service provider, the capability to work the encrypted data when keeping the plain content secret is desired. When the secret data to be transferred are encrypted, a channel source without any knowledge of the cryptographic key may compress the translated data due to the restrictednetwork resource. Encryption is an active means of privacy protection. To share a secret data with other person, a content holder may encrypt the image before transmission. In some cases, a channel administrator needs to add some other message, such as the originaldata, image notation or verification data, within the encrypted image however he does not know the original image content. It may be also predictable that the real content can be recovered without any mistake after decryption and recover of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is required. Data hiding is mentioned to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data.

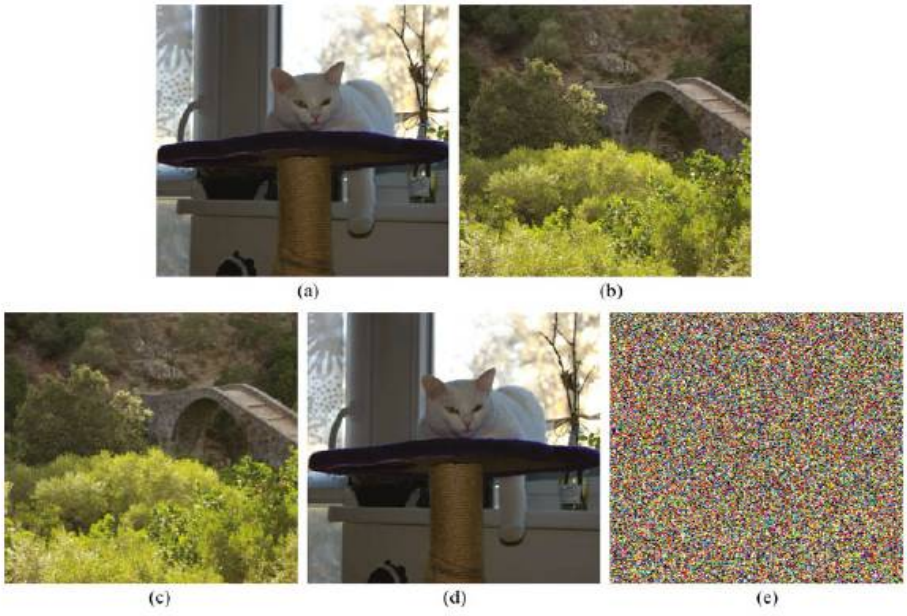

Figure.1. Experimental results of test images in Experiment A. (a)Original image. (b) Target image. (c) Encrypted image. (d) Decrypted image (right key). (e) Decrypted image (wrong key).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

IV. REVERSIBLE IMAGE TRANSFORMATION

In this section, we propose a method of RIT to encrypt spatial images, which is inspired by the technique of image transformation proposed by Lee and Tsai. Lee *et al.*'s method can transform the original image to a freely selected target image with the same size, yielding a secret-fragment-visible mosaic image defined [13]. But the original image cannot be restored in a lossless way. It is not reversible, so it is not suitable for the scenario of RDH EI. We will modify Lee *et al.*'s method to be reversible and obtain an encrypted image which looks like the target image. For color images, we transform the color channel R, G, and B respectively in the same manner. So we just take gray images (one channel) as an example to describe the method. For an original image *I*, we randomly select a target image *J* having the same size with *I* from an image database. Firstly, we divide the original image *I* and the target image *J* into *N* non-overlapping blocks respectively, and then pair the blocks of *I* and *J* as a sequence such that (B1, T1), . . . , (BN , TN), where Bi is an original block of I and Ti is the corresponding target block of J, $1 \leq i \leq N$. We will transform Bi toward Ti and generate a Ti similar to Ti . After that, we replace each Ti with Ti in the target image J to get the transformed image J. Finally we embed some accessorial information (AI) into J with an RDH method and generate the ultimate "encrypted image" E(I). These AI is necessary for recovering I from J. Before being embedded, these AI will be compressed and encrypted with a key K shared with the receiver, so only a receiver having K can decrypt E(I).s

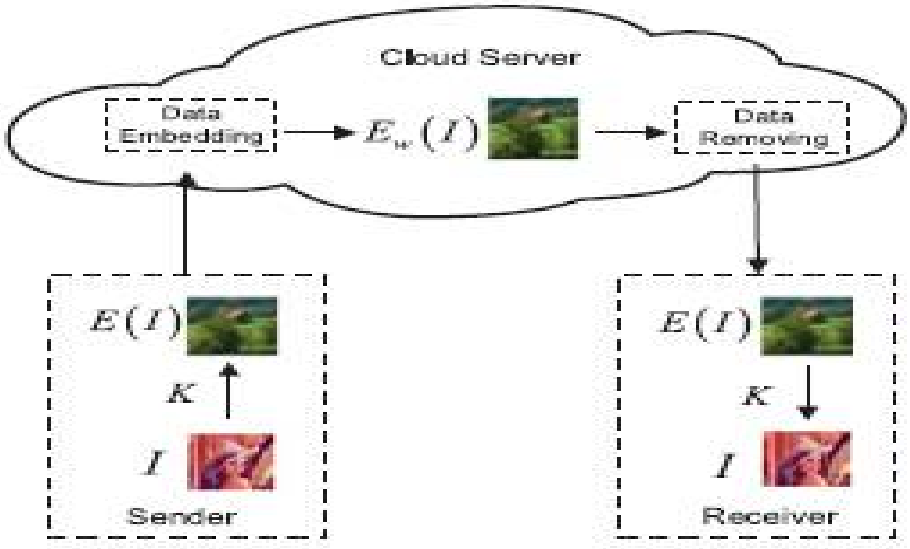

Figure.2.RIT-based framework.

V. CONCLUSION

Thus this paper provides a brief description of techniques used for reversible data hiding. All these techniques aim at reproducing the original image in which the data was hidden with maximum accuracy. We realize an RIT based method by improving the imagetransformation technique in to be reversible. By RIT, wecan transform the original image to an arbitrary selected targetimage with the same size, and restore the original image from theencrypted image in a lossless way.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 6, Special Issue 1, January 2017*

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

REFERENCES

[1] Weiming Zhang, Hui Wang, Dongdong Hou, and Nenghai Yu propose a novel framework for RDH-EI based on reversible image transformation IEEE Trans on Multimedia, vol.18,no.8,aug 2016.
[2] W. Liu,W. Zeng, L. Dong, andQ.Yao, "Efficient compression of encrypted gray scale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[3] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[4] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, 653–664, Mar. 2015.
[5] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785,Jul. 2013.
[6] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, 2009.
[7] X. Zhang, " data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[8] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779–1790, Apr. 2014.
[9] W. Hong, T. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[11] X. Hu et al., "Fast estimation of optimal marked-signal distribution for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 8, no. 5, pp. 779–788, May 2013.
[12] W. Zhang, X. Hu, and N. Yu, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," IEEE Trans. Image Process., vol. 24, no. 1, pp. 294–304, Jan. 2015.
[13] Y. Lee and W. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformation," IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 4, pp. 695–703, Apr. 2014..
[14] 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.