IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-12, May 2019 E-ISSN: 2347-2693

Protection Reversible Data Hiding in Encrypted Images by Distributing Memory before Encryption

Sonali Jambhulkar[1*], Priyanka Dudhe[2]

[1,2]Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

[*]*Corresponding Author: sonali.jambhulkar7@gmail.com, Tel.: +91-9511856954*

Available online at: www.ijcseonline.org

Abstract— Electronic image and data inserting framework have number of critical interactive media applications. Now a days, consideration is paid to reversible data hiding (RDH) in encoded images is more, since it maintains the highest quality property that the original cover can be losslessly recovered after inserted data is extracted while securing the image content's confidentiality. RDH is a technology used to hide data inside image for high security and can fully recover the original image and private data . All earlier methods fixed data by reversibly vacating room from the encrypted images, which may result to some errors on data extraction and/or image restoration. In this paper, we put forward another method in which we simply encrypt an image without its header by using our new technique. Hence it is easy for the data hider to reversibly fixed data in the encrypted image. The projected technique can achieve real reversibility, that is, data extraction and image recovery are free of any error.

Keywords— Encryption, Decryption and Reversible Data hiding

I. INTRODUCTION

Now a days, privacy and security is very necessary. With the more and more wide reach of the Internet, communications via Internet are getting more frequent. Due to large number of threats against communications security, information security has become an important issue. Information embedding and data hiding systems play an extremely important role in dealing with couple of major challenges that have risen up from the widespread distribution of multimedia content over digital communication networks. Data hiding is referred to as a process to hide data into cover media. It links two sets of data such as embedded set of data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. Especially, these systems are enabling technologies for (1) enforcing and protecting copyrights (2) authenticating and detecting tampering of multimedia signals & image.

In theoretical aspect, Kalker and Willems [1] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory-less covers and proposed a recursive code construction which, however, does not approach the bound. Zhang *et al.* [2], [3] improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between information compression and RDH for binary covers.

II. RELATED WORK

In practical aspect, many RDH techniques have come out over the last few years. Fridrich *et al.* [4] constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding extra information. Another strategy for RDH is histogram shift (HS) [5], in which space is saved for data embedding by shifting the bins of histogram of gray values. In [6], Zhang divided the encrypted image into several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image restoration proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image. Hong *et al.* [7] ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to accomplish much lower error rate. These two methods mentioned above depend on spatial correlation of original image to gain data. That is, the encrypted image should be decrypted first before information extraction.

Our purpose is to develop a secure system to send the data over a network which consist of separate and reverse image encryption (like bmp image and txt file encryption), data embedding which prevents any third party access to the private data. In this method, with the help of symmetric key, we can achieve real reversibility, that is, data extraction and image recovery are free of any error. The output will be the original image file without any distortion.

The objectives behind this is to hide secret or confidential data in Encrypted image using Encrypting key and data hiding key and to achieve real reversibility, that is, data extraction and image recovery will be free of any errors.

III. METHODOLOGY

RDH is a technology used to hide data inside image for high security and can fully recover the original image and private data. In simple words, Reversible data hiding is a procedure to fixed extra message into some distortion-unacceptable cover media, such as military or medical images, with a reversible behaviour so that the original cover content can be flawlessly restored. Image is not visible after encryption not even readable by any image viewing software and also delete file header in between encryption. Normally changing image R, G, B in order to save information will not affect image but decrease the quality of the image. If we try to change single bit in encrypted image, we could not decrypt the image. But our main objective is to hide secret/confidential data or information in encrypted image and on other side that data should recover free from error i.e. real reversibility is done.

The proposed work is made up of image encryption, data embedding and data-extraction/image-recovery phases.This projected technique can accomplish real reversibility, that is, data extraction and image recovery are free of any error. This method proposes a separable reversible data hiding in encrypted image. In the proposed method, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using data-hiding key.

With an encrypted image containing additional data, if the receiver has only the data-hiding key, receiver can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, receiver can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data.

IV. RESULTS AND DISCUSSION

There are three steps in this experiment. Encryption, Data Hiding, Decryption and Recovery.

Encryption:

The first step is Encryption. This process contains the image to be encrypted , where we have to select the image in which we have to hide our secret information then Enter Encryption Key which is alphanumeric with special symbol. The output will be an Encrypted Image which is in unreadable format. The Encrypted format is also not readable by image viewing software.

Data Hiding:

The second step is Data Hiding. In this process we need a text file which is to be hidden and data hiding key which is also alphanumeric. The output of this process is Encrypted raw file which enclose text file into encrypted image. Raw file is a file that has no importance with unknown name.

Decryption and Recovery

The third step is Decryption and Recovery. Here, if we want to recover the hidden Information inside text file along with image, firstly we have to recover the Information in specific folder by applying recovery process on raw file with the help of data hiding key. Now in order to obtain original image, decrypt Encrypted image using the symmetric key i.e. encryption key from the first step. The output of the process will be exact original Image recover free of any error or any distortion.

V. CONCLUSION AND FUTURE SCOPE

This work presents a new technique of reversible data hiding for encrypted image , which consists of three phases via image encryption, data embedding and data-extraction/image-recovery. The embedded data can be correctly extracted while the original image can be perfectly recovered along with the data hidden inside the image which is free of any errors. Without knowledge of encryption key and data-hiding key, it is still impossible to extract the additional data and recover the original image by third party which is a safer way to send the message over a network.

In future, it is expected that this reversible data hiding technique will be deployed for a wide range of applications in the areas such as secure medical image data systems, and image authentication in the medical field and law enforcement, and the other fields where the rendering of the original images is needed or desired. Further research can be done on hiding very large amount of data in Encrypted image and hiding data in video.

REFERENCES

[1] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011),LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans.
[4] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[5] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[6] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[7] 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.
[8] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[9] 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. 562 IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013
[10] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010
[11] Miscelaneous Gray Level Images [Online]. Availabe:http://decsai.ugr.es/cvg/dbimagenes/g512.php

Authors Profile

Miss Sonali Kumar Jambhulkar pursed Bachelor of Engineering in Information Technology from JD College of Engineering, RTMNU University in 2014 and is currently a Master of Technology scholar from Rashtrasant Tukadoji Maharaj Nagpur University. Her main research work focuses on Protection Reversible Data Hiding In Encrypted Images by Distributing Memory Before Encryption.

