International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-4, April 2015

Image Encryption Using Reversible Data Hiding by Reserving Room before Encryption

Shubhangi Kolhe, Chaitrali Dhumal, Pratik Kumar, Achal Badgujar

Abstract— This work proposes a novel scheme for reversible data hiding in encrypted images reserving room before encryption. In the first phase, a content owner performs the image partition and creates space for data accommodation and then encrypts the image using an encryption key. Then, a data-hider accommodates the data inside the image and hide it using data-hiding key to encrypt it. 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. 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. This project deals with the image steganography as well as with the different security issues, general overview of cryptography approaches and about the different steganography algorithms like Least Significant Bit (LSB) algorithm and blow fish algorithms. It also compares those algorithms in means of speed, accuracy and security.

Keywords: encrypted image containing additional data, data-hiding key, modifications, cryptography and steganography, Least Significant Bit (LSB) algorithm.

I. INTRODUCTION

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Some promising applications can be generated if RDH can be applied to encrypted images.

Manuscript published on 30 April 2015.
***** Correspondence Author (s)
Shubhangi Kolhe, Department of Information Technology, Pune University (Dr. D Y Patil, Pimpri), Pune, India.
Chaitrali Dhumal, Department of Information Technology, Pune University (Dr. D Y Patil, Pimpri), Pune, India.
Pratik Kumar, Department of Information Technology, Pune University (Dr. D Y Patil, Pimpri), Pune, India.
Achal Badgujar, Department of Information Technology, Pune University (Dr. D Y Patil, Pimpri), Pune, India.

Suppose a medical image database stored in a data center, notations can be embedded into the encrypted version of a medical image through a RDH technique by a server in the data center. The server can manage the image or verify its integrity by using the notations without having the knowledge of the original content. This will protect the patient's privacy. At the same time, a doctor can decrypt and restore the image for further diagnosing by using the cryptographic key. In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the "security threat" it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal 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 or other formats.

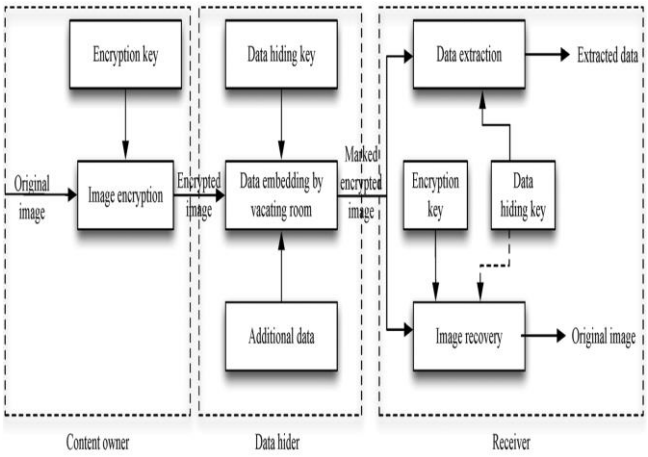
II. PREVIOUS SYSTEM

In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

Disadvantages:

The hackers recover the embedding data in original image because the data placed in particular bit position.

Previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.



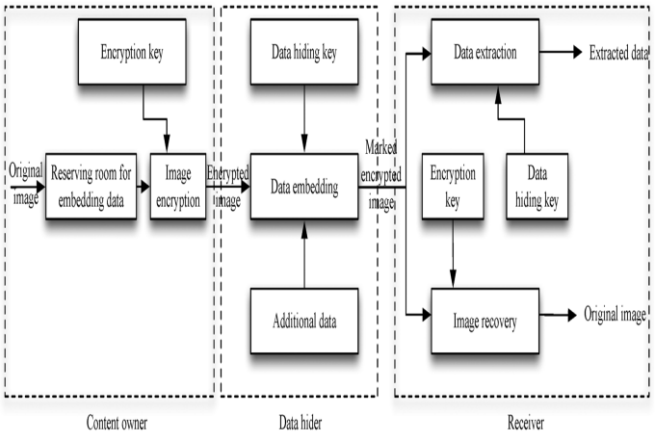
III. PROPOSED SYSTEM

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find novel RDH techniques working directly for encrypted images? If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)".

Therefore in this system we vacant the room before encrypting the image and use *watermarking* to specify the image, by using *watermarking* the owner authentication can be done.

Advantages:

It is easy for the data hider to reversibly embed data in the encrypted image. This method can embed more than 10 times as large payloads for the same image quality as the previous methods.

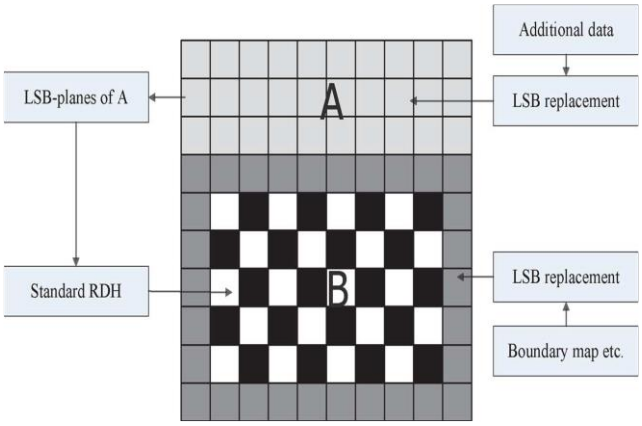


A) Generation of Encrypted Image

To generate an encrypted image first stage can be divided into three steps: image partition, self reversible embedding and image encryption.

i) Image portion

In this step we divide the image in two parts A and B using standard RDH algorithm LSB algorithm. The image is a 8-bit grey scale image, B is used to create a smoother area to minimize the image distortion and helps to reserve room before encryption. Reserving room before encryption helps to improve quality of image during image decryption.



ii) Self reversible imbedding

The bit locations of last 3 LSB are scuffled merged from portion A to B to make room for embedding data, which we want to hide behind the image by using traditional RDH algorithm.

iii) Image encryption

After rearranging the self embedded image, we encrypt the image using blow fish algorithm, and use watermarking in the image. Note that after image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

B) Data Hiding in Encrypted Image

When the data hider acquires the Encrypted image, he can embed some data in the image. The data hider checks the first 10 bits of image where image encrypted puts the information about the spaces available to put data in the image. By using the information provided in the first 10 bits of image the data hider puts the data in those locations.

C) Data Extraction and Image Recovery

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.

Case1:Extraction of data from Encrypted image:

In this case the image data and is still encrypted with the encrypted key; the user who wants the hidden information need to first decrypt the image and then the data to see the information hidden behind the image.

Case2:Extraction of data from Decrypted image:

In this case the Image is decrypted and the data is still encrypted; the user who wants to access the information hidden needs the decryption key for data to decrypt the data.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy- preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

REFERENCES

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, IEEE, Nenghai Yu, and Fenghua Li "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption",Mar 2013.
[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding",Mar. 2006.
[3] J. Tian, "Reversible data embedding using a difference expansion",Aug. 2003.
[4] X. Zhang, "Separable reversible data hiding in encrypted image",Apr. 2012.
[5] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images"2008 SPIE Digital Library.
[6] Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao, Efficient "Compression of Encrypted Grayscale Images", April 2010.
[7] Masoud Nosrati Ronak Karimi Mehdi Hariri "Reversible Data Hiding:Principles, Techniques, and Recent Studies",May 2012.
[8] T. Margaret "Reversible Data Hiding In Encrypted Images by XOR Ciphering Technique", Feb 2014.
[9] Fameela. K. A, Reshma. V.K "A Secure Data Transmission by Embedding Marked Encrypted Image on Cloak Image ",Mar-Apr 2014.
[10] Aparna Gopinath P.K, Grace John "A Review on Reversible Data Hiding Techniques",May-Jun 2014.
[11] Deepthi C. "Highly Secured Reversible Data Hiding in AES Encrypted Images by Reserving Room before Encryption with Authentication",May 2014.
[12] Sunita, Syeda Asra "Reversible Data Hiding For Embedding Data Securely in Encrypted Image by Reserving Room Before Encryption" IJEDR 2014.
[13] Harish G, Smitha Shekar B, Prajwal R, Sunil S Shetty "Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption",Jul 2014.
[14] Dipali P. Pethe , Tabassum Khan "A Reversible Data Hiding Scheme in Encrypted Image Using Concept of Reserving Room",2014.
[15] Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images",2008.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)