International Journal of Research in Advent Technology (IJRAT)
Vol. 1, No. 3, October 2013, ISSN: 2321–9637

SEPARABLE REVERSIBLE DATA HIDING TECHNIQUE BASED ON RGB-LSB METHOD

Vinit K Agham [1], Tareek M Pattewar [2]
[1] *Computer Engineering, Department*
[2] *Information Technology Department*
[1 2] *R C Patel institute of Technology,Shirpur.*
Email- [1] *vinitagham@gmail.com,* [2] *tarrekpattewar@gmail.com*

ABSTARCT:

Communication over the internet is facing some problem such as data security, copyright control, data size capacity, authentication etc. Here we introduce a novel scheme for separable reversible data hiding in encrypted domain in which we use image as a cover medium. This paper illustrates the various objectives of implementing separable reversible data hiding technique. The separable reversible data hiding is consists of three steps in the first step; a content owner encrypts the image using an encryption key. Then, a data-hider compresses the encrypted image using a data-hiding key. The third step is to extract the additional data and recover the original image. The activities i.e. extracting the additional data and recover the original images are depends upon which key the receiver has. There is separation of these two activities according to availability of keys. The scheme's main feature is the way of data embedding into the encrypted image using the different positions of LSB within image. Here we are concentrating on using RGB-LSB method for data embedding and finally verifies the performance of using RGB-LSB method in terms of data capacity, image quality etc.

Keywords: *Image encryption, RGB-LSB, image recovery, reversible data hiding.*

1. INTRODUCTION

Now a day the data security and integrity are the two challenging areas for research. There are numerous research is progressing on the field like internet security, steganography, cryptography Images used in military, medical science are the media in which we found certain distortion sometime which is un-acceptable. Hence for data hiding we have a technique using which we can extract data correctly and after that original cover content can be perfectly recovered. This technique is also known as reversible data hiding or it is also named as lossless, distortion free, or invertible data hiding technique [Ni Zhicheng and et al. (2006)].The author Xinpeng Zhang presented an exclusive reversible (lossless) data hiding technique which supports the exact recovery of the original cover medium with the extraction of the embedded information. And the process of this recovery with lossless data is nothing but the reversible data hiding. Generally the well-known LSB (least significant bit) method is used as the data embedding method. Reversible data hiding is a technique that is mainly used for the authentication of data like images, videos, electronic documents etc. Mainly the reversible data hiding is applicable for in IPR (Intellectual Property Rights) protection, authentication, and conditional access. In some application scenarios it is essential to provide security, authentication and privacy while communication or transferring data. To hide the data or to provide the data security we need some new approach in communication.

2. LITERATURE REVIEW

Mostly reversible data hiding techniques are not separable, not based on encryption-decryption domain, not based on RGB-LSB steganography. Here provides the small survey that expresses what techniques have been used for compression-decompression, encryption-decryption, data embedding etc.

Reversible data hiding technique includes following actions like compression-decompression, encryption-decryption, data embedding-data extracting, creating space at LSB in real world source like images, providing security, authentication using automatic key generation and etc. The customary way of transferring data is to first compress the data to reduce the redundancy and then to encrypt the compressed data. At the receiver side the decryption and decompression operations are orderly performed to recover the original cover data. However

in some applications a sender wants to transmit some data to the receiver and demands to keep the information confidential to a network operator who provides the channel resource for the transmission, means the sender should encrypt the original data i.e. image in this case and the network provider compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side to rebuild the original data, a decoder which integrates decompression and decryption functions will be used.

There are certain techniques for compressing/decompressing encrypted data have been developed. When it is anticipated to transmit redundant data over an insecure and bandwidth- constrained channel, it is customary to first compress the data and then encrypt it. Mark Johnson investigated the novelty of reversing the order of these steps that is first encrypting and then compressing without compromising either the compression efficiency or the security [Johnson Mark and et al. (2004)].

Wei Liu and et al. suggested a lossless compression method for encrypted gray image using resolution progressive decomposition. In this method they developed resolution progressive compression, which has been shown to have much better coding efficiency and less computational complexity. In this paper, he proposed a resolution progressive compression scheme which compresses an encrypted image progressively in resolution such that the decoder can observe a low-resolution version of the image study statistics based on it and use this statistics to decode the next resolution level and this process iterates until last level of resolution. He focused on the design and analysis of a practical lossless image codec where the image undergoes stream-cipher based encryption before compression [Liu Wei and et al. (2010)].

Nasir Memon and Ping Wah Wong worked on a buyer-seller watermarking protocol which is the concept of digital watermarking. In this protocol they indicated that the seller does not get to know the exact watermarked copy that the buyer receives. Hence the seller cannot create duplicates of the original content containing the buyer's watermark. However, in case the seller finds an unauthorized copy, he can identify the buyer from whom this unauthorized copy has originated and furthermore also prove this fact to a third party by means of dispute resolution protocol. The watermark embedding protocol is based on public key cryptography and has little overhead in terms of the total data communicated between the buyer and the seller [Memon Nasir and Wong, P. W. (2001)]. Nasir Memon and Ping Wong indicated the concept of hiding the data in encrypted form of the data. Here seller is doing data (fingerprint/Watermark in this case.) embedding while he does not know the original data content thus invisible watermarking. The original data content is in the encrypted form.

Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. But in some applications it is important to append some additional message within the encrypted image however data hider does not know the original image content. And it is also expected that the original content should be recovered without any error after image decryption and message extraction at receiver side.

Xinpeng Zhang presented a practical scheme satisfying the above-mentioned requirements. A content owner encrypts the original cover image using an encryption key and a data-hider could embed additional data into the encrypted image using a data-hiding key although he does not know the original content. Having an encrypted image containing additional data a receiver first decrypts it according to the encryption key, and then extracts the embedded data and recovers the original image according to the data-hiding key. In the scheme the procedure of data extraction is not separable from the content decryption. In other words, the payload must be extracted from the decrypted image thus the principal content of original image is revealed before payload extraction, and, if someone has the data-hiding key only but not the encryption key he is unable to extract any information from the encrypted image containing additional data [Zhang Xinpeng (2011)]. Xinpeng Zhang also presented a newel practical scheme in which the procedure of data extraction is separable from the content decryption. In other words if someone has the data-hiding key only but not the encryption key he is able to extract any information from the encrypted image containing additional data [Zhang Xinpeng (2012)].

Jun Tian developed a simple and efficient reversible data-embedding method for digital images in which he explored the redundancy in the digital content to achieve reversibility. He concentrates specially on parameters like the payload capacity limit and the visual quality of embedded images. As a basic requirement; He achieved the policy that quality degradation on the image after data embedding should be low. [Tian Jun(2003)]

3. Objectives

This paper illustrates the various objectives of implementing separable reversible data hiding technique. Why we need to have such methodology? Why we are interested in achieving the most modern concept of separable data hiding technique. So following are some objectives which could be defined for this paper.

1. We attempt to implement data hiding technique in encryption-decryption domain rather than plain spatial domain i.e. trying to join steganography with cryptography. The cover media we use is the real world source image.

2. We attempt to execute data hiding technique using the sequence encryption-compression then decompression-decryption not the sequence compression-encryption then decryption –decompression.

3. The main theme of the literature is to implement the idea i.e. separable in which the two activities cover media decryption and hidden data extractions are separated according to keys. We are trying to implement this separable reversible data hiding scheme in this paper. The practical conception of this scheme is described in the section 4 in this paper.

4.The author Xinpeng Zhang suggests the method of separable reversible data hiding in encrypted domain he also notes that the amount of data to embed in the image(cover media) must be small in size here we are trying to vary this size[Zhang Xinpeng (2012)]. The author used LSB of the pixel value while here we are trying to use LSB of the pixel position values as well as LSB of RGB values. Usage of LSB of red, green and blue parameters of the image allows hiding much enough data in the image.

5. After embedding the data we are focusing on PSNR values of the decrypted image it should be more for ideal case. So this is our one of the target to have larger PSNR value.

4. Proposed Scheme

There are two kinds of reversible data hiding techniques (according to key distribution) separable reversible data hiding technique and non-reversible data hiding technique (also called as reversible data hiding). In non-separable technique i.e. reversible data hiding scheme, a content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image and then a data-hider embeds additional data into the encrypted image using a data-hiding key. Having an encrypted image containing additional data a receiver firstly decrypt it using the encryption key and can further extract the embedded data. Thus in non-separable technique it is compulsory to have both the keys i.e. encryption key and the data-hiding key for retrieving data [Zhang Xinpeng (2011)]. But in separable technique it is not compulsory to have both the keys for retrieving data here if the receiver has a data hiding key only then he can extract the embedded or hidden data from the encrypted image containing additional data. Here we are separating two activities i.e. cover image decryption and pay load data extraction [Zhang Xinpeng (2012)].

This paper is stating one of the types of reversible data hiding method i.e. separable reversible data hiding method which is consists of three main procedures

- Image encryption
- Data embedding
- Data extraction/image recovery.

As shown in figure 1. In separable scheme, the content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then using a data-hiding key the data-hider compresses the least significant bits (LSB) of the encrypted image to create some space to accommodate the additional data. At the receiver side the data embedded can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. As the data embedding only affects the LSB a decryption with the encryption key may result in an image similar to the original version.

Here at the receiver side there exists three cases as shown in figure 2.With an encrypted image containing additional data which is hidden case one is when the receiver has only the data- hiding key, he is able to extract the additional data even if he does not know the image content. Case two is if he has only the encryption key, he can decrypt the received data i.e. encrypted image to obtain an image similar to the original cover media, but cannot extract the embedded additional data. Case three is if the receiver has both the keys i.e. data-hiding key and the encryption key, he can extract the additional data and recovers the original image without any error. The

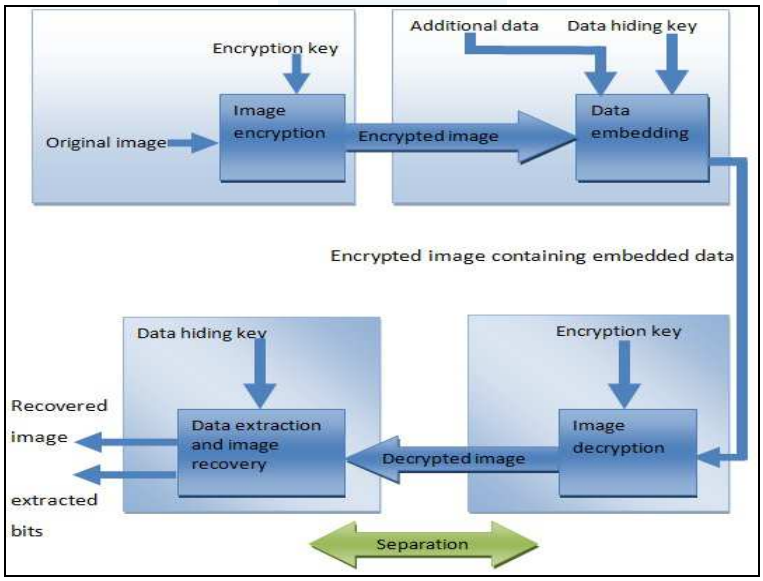

Fig. 1. Separable reversible data hiding in encrypted image.

proposed scheme is describing the method in which the concept of separable reversible data hiding is executed using RGB-LSB method [Zhang Xinpeng (2012)].

This part of the literature expose on implementing separable reversible data hiding schemes in encrypted image based on RGB-LSB method. The existing approach of using separable reversible data hiding involve simple LSB method in which the least significant bits of the pixel position value(representing one pixel as one byte or eight bits) is used for creating space. The space creation is for making room for external/additional confidential information which is to be hide/embedded. The author xinpeng zang uses this simple LSB based

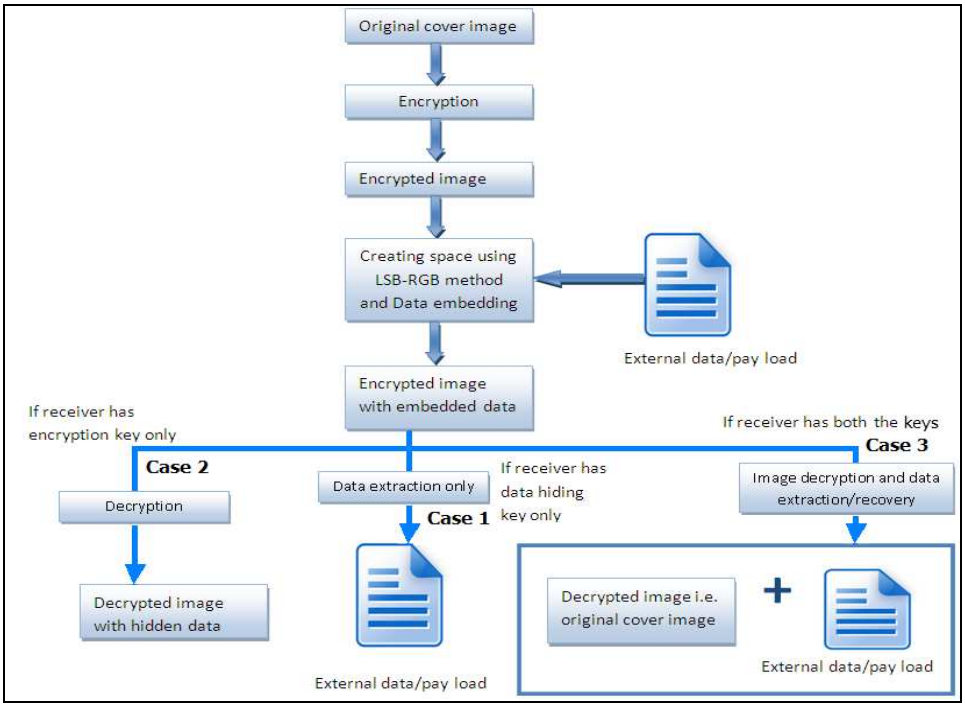

Fig. 2. Separable reversible data hiding with three cases.

compression .But this technique could not hide enough data the scheme is having limitation that at the receiver side receiver can extract the additional data and recover the original content without any error when the amount of additional data is not too large [Zhang Xinpeng (2012)]. Thus the scheme is not suitable if anyone wants to

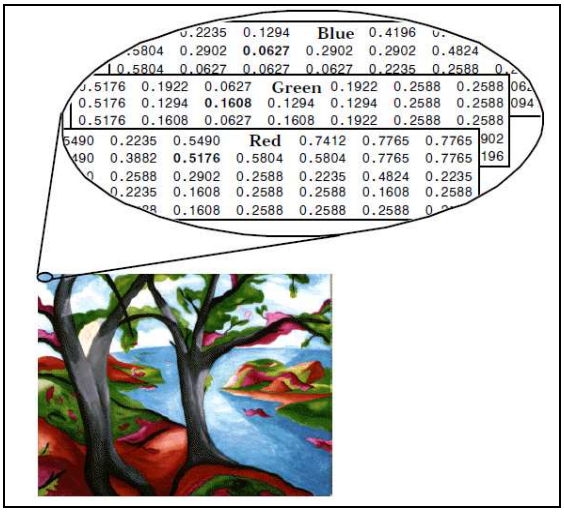

Fig. 3. RGB Matrix representation of cover image

embed the more data. So to overcome this problem we need a new method or new technique which can handle enough data to embed.

In general, in LSB methods, hidden information is stored into a specific position of LSB of image. In our paper, hidden information is stored into different position of LSB of image i.e. LSB of red color value, LSB of green color value and blue color value. Different positions of LSB of image means the LSB of RGB.The true color image is having five parameters two parameters represents the pixel position and three parameter represents red, green and blue color values. Actually these three colors are represented as three matrices red, green and blue as shown in figure.3. As a result, it is difficult to extract the hidden information knowing the retrieval methods. The proposed method results in LSB based image steganography using secret key which provides good security issue than general LSB based image steganography methods.

5. Conclusion

In this paper we proposed to implement the scheme of separable reversible data hiding using RGB-LSB method. In separable reversible data hiding at the receiver side when the receiver has data-hiding key only he can extract the confidential data and to recover the original content and extract the additional data the receiver must has both of the keys encryption key as well as data-hiding key. Also by using the novel RGB-LSB method for embedding the data, the size of the net payload can be increased sufficiently. That is we can hide the enough data into the encrypted image and also examined the performance of existing method and proposed method images in terms of parameters like PSNR values, data capacity, size of the cover image etc.

References

[1] Johnson Mark, and et al. (2004): On Compressing Encrypted Data, IEEE transactions on signal processing, vol. 52, no. 10,pp. 2992-3006.
[2] Liu Wei,and et al.(2010):Efficient compression of encrypted grayscale images, IEEE Transactions on Image Processing, vol. 19, no. 04,pp. 1097-1102.
[3] Memon Nasir ;Wong,P. W.(2001):A buyer-seller watermarking protocol, IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643-649.
[4] Ni Zhicheng, and et al. (2006): Reversible Data Hiding, IEEE transactions on circuits and systems for video technology, vol. 16, no. 3, pp. 354–362.
[5] Tian Jun(2003): Reversible data embedding using a difference expansion, IEEE Transactions Circuits Systems Video Technology, vol. 13, no. 8, pp. 890-896.
[6] Zhang Xinpeng, (2012): Separable Reversible Data Hiding in Encrypted Image,IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 826–832.
[7] Zhang Xinpeng,(2011) : Reversible data hiding in encrypted image ,IEEE Signal Processing, vol. 18, no. 4,pp. 255-778.