INNOVARE JOURNAL OF ENGINEERING & TECHNOLOGY

Vol 3, Issue 1, 2015

ISSN - 2347-1573

Original Article

HIDING TEXT WITHIN LSB OF IMAGE PIXELS

RUPALI JAIN, DURGESH WADBUDE, JAYSHREE BOADDH*

Department of Computer Science Engineering, Mittal Institute of Technology, Navibagh, Bhopal 4620038 M.P. India. Email: rupalijain.aj@gmail.com

Received: 6 May 2015, Revised and Accepted: 30 May 2015

ABSTRACT

Data security is maintained by assuming the consistency and accuracy of data over its entire life cycle. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, data integrity and denial of service. Here, we are proposing a separable reversible data hiding technique in which data to be hidden is text. This technique proposed a way how to hide large amount of text behind an image. Process involves creating space after compressing least significant bits of the image. Later, the data is hidden in this space..

Keywords: Encryption technique, Reversible data hiding, hidden data, data hiding.

INTRODUCTION

Protecting data in the digital world is a must feature to be taken care of everywhere during private communication. Our data always need to be protected from intruders and people with the destructive motives. Data security is maintained by assuming the consistency and accuracy of data over its entire life cycle. We use cryptography all for secret writing and verifying the correctness of message that are intended for the recipient. The message is usually encrypted from intelligible form to unintelligible form. Later this message is retransformed at the receiver side back to its original form. On the other hand, Steganography conceal the existence of the message generally through character marking/ invisible ink/ pin punctures/ typewriter correction ribbon. Potential investigators find it very difficult to discover the hidden message. Cryptographic features can further be enhanced using data hiding. Data hiding does not easily allow access to the multimedia content. It provides various mechanisms to transmit secret messages which are hard to detect by the intruders.

Separable reversible data hiding technique

Reversible data hiding is the common name in the field of electronic media for transmitting hidden messages behind the host media like cover image or say master image. Reversible data hiding is a technique in which we first extract the hidden data and then we can losslesly recover the image carrying that data. The two keys that play the role are encryption key and the data hiding key. The separable reversible data hiding technique says that there are two separate activities that involves recovering the hidden data behind the cover image and later obtaining that image at the receiver side.

Motivation and Related work

Generally we find those separable reversible data hiding techniques to be used most of the times that does not involve compression-decompression methods and encryption-decryption procedure. If the channel is not secure to communicate or if the channel bandwidth is within the constraints then it is recommended to first compress the data and then encrypt it. But in [3] these steps are in reverse order. The work done involves introduction of compression technique over encrypted data.

Liu *et al* [1] showed that for encrypted real-world sources, such as images, the key to improve the compression efficiency is how the source dependency is exploited. Approaches in the literature that make use of Markov properties in the Slepian-Wolf decoder do not work well for grayscale images. In this correspondence, the author propose 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 local statistics based on it, and use the statistics to decode the next resolution level. Good performance is observed both theoretically and experimentally.

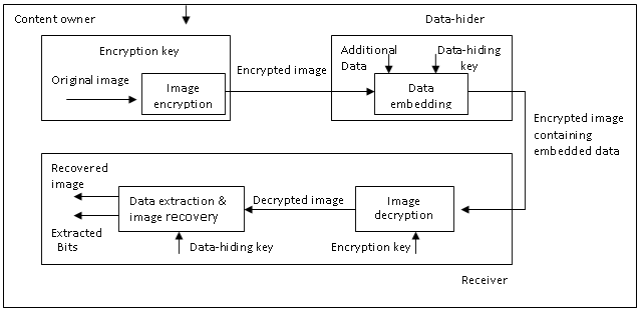


Fig1: Diagram for Non-Separable reversible data hiding technique

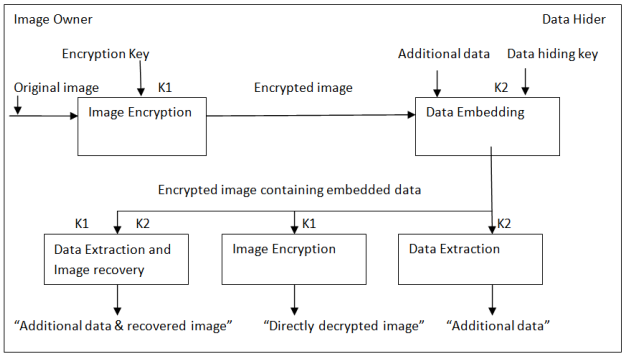


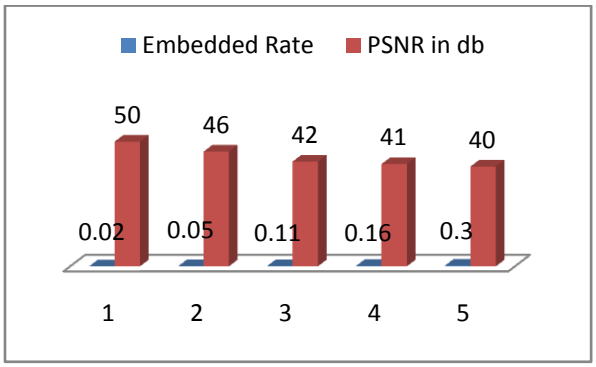
Fig 2: Diagram for Separable reversible data hiding technique

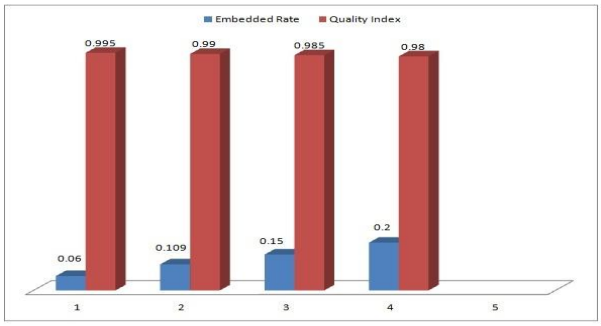
Zhang [2] proposes a novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image, and the encrypted

data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image.

Ma & Zhang [4] reported the use of a reverse data hiding traditional algorithm for reversibly vacating room before encrypting the image, to embed data in this space. Instead of embedding data in encrypted images directly, some pixels are estimated before encryption so that additional data can be embedded in the estimating errors. A benchmark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating errors.

Qian *et al* [5] proposed a framework of reversible data hiding (RDH) in an encrypted JPEG bitstream. Unlike existing RDH methods for encrypted spatial-domain images, the proposed method aims at encrypting a JPEG bitstream into a properly organized structure, and embedding a secret message into the encrypted bitstream by slightly modifying the JPEG stream. We identify usable bits suitable for data hiding so that the encrypted bitstream carrying secret data can be correctly decoded.





Qian & Zhang [6] proposed a novel scheme of reversible data hiding (RDH) in encrypted images using distributed source coding (DSC). After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make room for the secret data. The selected bit series is Slepian-Wolf encoded using low density parity check (LDPC) codes.

Methodology

This new approach of separable reversible data hiding method consists of 4 main procedures,

A. Image Selection

B. Image Encryption

C. Data Hiding

D. Extracting the data/ Obtain the image

A. Image Selection

The image selected can be of jpg, jpeg, png, gif, bmp etc format. We are assuming the pixels of the master image are ranging in [0,255] represented using 8 bits i.e 0 to 7 notation.

Mathematically

$$m_{p,q,r,s} = \lfloor w_{p,q,r} / 2^x \rfloor \bmod 2 \quad \text{where} \quad x = 0 \text{ to } 7 \qquad (1)$$

$$w_{p,q,r} = \sum m_{p,q,r,x} \cdot 2^x \qquad (2)$$

B. Image Encryption

For encrypting, we do the XORing of original bits with the randomly selected bits.

$$M_{p,q,r,x} = m_{p,q,r,x} \oplus n_{p,q,r,x} \qquad (3)$$

$n_{p,q,r,x}$ is actually obtained from the use of some cipher technique using the encryption key.

C. Data Hiding

Since the computer understands data in bits the data to be hidden is given as

M(b1,1), M(b1,2), ...,M(b1,8),....,M(bn,8).

b1 represents single character in the text

b2 represents two characters in the text

b3 represents three characters in the text

bn represents number of characters in the text.

Four Least Significant Bits of each of the two pixels of the image are thus covering the single character of the data to be hidden where LSB of each pixel is represented by $M_{p,q,r,x}$ with x= 5,6,7,8. Each character has got some ASCII value whose binary value in 8-bit notation is understood by the computer.

Rate of Embedding = text characters_count/pixels_count

D. Extracting the data and Obtaining the image

Data can be extracted in three ways at the destination:

When only E_k is known

E_k is the encryption key. Thus, when E_k is known at the destination then the data hidden can never be obtained but only the bits of the pixels containing the hidden data can be known. It can further be explained as the Most Significant bits of the pixels of the image are still the same after decryption therefore we know those bits which contain the hidden text i.e. M'p,q,r,0 , M'p,q,r,1..... M'p,q,r,7. The equation used to obtain the decrypt image is

$$m'_{p,q,r,x} = M'_{p,q,r,x} \oplus n_{p,q,r,x}$$

Thus, the master image can be roughly recovered.

When only H_k is known

From the LSB of the encrypted image, the receiver will extract the data contained using data hiding key. Four least significant bits of each of the two pixels (8bits) are used to hide each character of the text to be hidden. But we cannot obtain the image at the destination.

When both of the above keys are known

At the destination, he will obtain the hidden text and the master image using the H_k and E_k simultaneously.

Advantages of our proposed scheme over earlier methodology

The most advantageous point about this proposed methodology is using both the encryption and the hiding key the master image can be obtained without error and almost zero or zero distortion.

For such calculations, we calculate the PSNR values for the decrypted image. Higher the values of PSNR, less will be the loss in the image. The figures shown below can be observed. Also, earlier we saw that the amount of data we hide was not that much large but now we have extended its limit to quite larger size.

CONCLUSION

The paper consists of technique for separable reversible data hiding in encrypted image. The processes followed step by step for doing so are encryption of image, embedding the data and extracting the data with decryption of master image. First extract the hidden data and then we can lossless recover the image carrying that data. The two keys that play the role are encryption key and the data hiding key. The separable reversible data hiding technique says that there are two separate activities that involve recovering the hidden data behind the cover image and later obtaining that image at the receiver side.

REFERENCES

1. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted gray scale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097-1102, Apr. 2010.
2. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no.1, pp. 53-58, Feb. 2011.
3. Xinpeng Zhang “Separable Reversible Data Hiding in Encrypted Image” IEEE Trans. vol. 7, no. 2, Apr. 2012.
4. Kede Ma, Weiming Zhang, “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption” IEEE Trans. vol. 8, no. 3, Mar. 2013.
5. Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang, “Reversible Data Hiding in Encrypted JPEG Bitstream”, IEEE Trans. of Multimedia, vol. 16, no. 5, Aug. 2014
6. Z. Qian , X. Zhang, “Reversible Data Hiding in Encrypted Image with Distributed Source Encoding” IEEE Trans. VOL. PP, no. 9, Apr.2015