IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image

MohanrajArumugam[1]and Rabindra Kumar Singh[2]

**[1] Information Technology, Hindustan University,
Chennai, Tamilnadu,603103, India**

**[2]Assistant Professor, Information Technology, Hindustan University,
Chennai, Tamilnadu,603103, India**

Abstract

Encryption is an effective and popular means of privacy protection. Reversible (lossless) data embedding (hiding) has drawn lots of interest recently. Being reversible, the original cover content can be completely restored. This paper proposes a novel reversible data hiding scheme with a lower computational complexity and can be used in applications where both the image and the hidden information is highly confidential. This work presents a new method that combines cryptography and steganography technique for data hiding and safe image transmission purpose. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. This work proposes a novel scheme for separable reversible data hiding in encrypted image. The content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may embed the additional data in encrypted image; data will be encrypted before embedding it ensures security over the hidden data.

Keywords:*Cryptography, Steganography, Image Encryption, Decryption.*

1. Introduction

The amount of digital images has increased rapidly on the internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. Two main groups of technologies have been developed for this purpose.The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. In this group, proper decryption of data requires a key. The second group bases the protectiondata hiding, aimed at secretly embedding a message into the data.

These two technologies can be used complementary and mutually commutative. Valuable secret information is vulnerable while in storage and during transmission over a network by unauthorized access. In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed a need to protect information from passing before curious eyes or, more importantly, from falling into wrong hands. Thus, multimedia security is much to consider in distributing digital information safety.

2. Literature Review

2.1 Cryptography

Cryptography is a technique for keeping message secure and free from attacks. Cryptography provides encryption techniques for a secure communication. In cryptography secret message is scrambled [8]. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Communication security of data can be accomplished by means of standard symmetric key cryptography.Such important data can be treated as binary sequence and the

whole data can be encrypted using a cryptosystem.Secret keys are used to encrypt the data into cipher data. Symmetric or Asymmetric keys are used for apply cryptography in data.

2.2Steganography

Steganography is the other technique for secured communication. Steganography involves hiding information so it appears that no information is hidden at all [3]. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography is the process of hiding a secret message within cover medium such as image, video, text, audio. Image steganography has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Image steganography allows for two parties to communicate secretly and covertly.

3. Proposed Scheme

The proposed scheme is made up of image encryption, data encryption, data embedding and data extraction or image recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data [1], before embedding the additional data would be encrypt using the key. At the receiver side, the data that embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered. Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media [10], such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

3.1 Image Encryption

Assume the original image with a size of N_1 x N_2 is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0}$, $b_{i,j,1}$,….$b_{i,j,7}$where $1 \le i \le N_1$ and $1 \le i \le N_2$, the gray value as $p_{i,j}$, and the number of pixels as $N(N = N_1 \times N_2)$. That implies

$$b_{i,j,u} = [\, p_{i,j} / 2^u \,] \bmod 2,\ u=0,1,\ldots,7 \qquad (1)$$

and

$$P_{i,,j} = \sum_{u=0}^{7} b_{i,j,u} \cdot 2^u \qquad (2)$$

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated

$$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u} \qquad (3)$$

Where $r_{i,j,u}$ are determined by an encryption key using a standard stream cipher. Then, $B_{i,j,u}$ are concatenated orderly as the encrypted data.

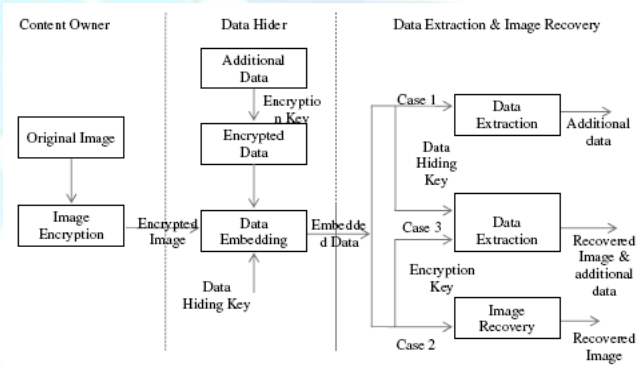

Fig. 1 Sketch of proposed scheme.

3.2 Text Encryption

The data hider uses the data encryption key to encrypt the message and hide the secret message into the encrypted image [3][5]. The Advanced Encryption Standard (AES), which is used to encrypt the text. AES algorithm is not only for the text data, it can applied for the images, usually image processing deals with a image, which is composed of many image points. The image points, namely pixels, spatial co-ordinates that indicate the position of the points in the image and intensity values. AES comes in three favors, namely AES - 128, AES - 192, and AES-256, with the number in each case representing the size (in bits) of the key used [7].The algorithm begins with an Add round key stage followed by nine rounds of four stages and a

tenth round of three stages which applies for both encryption and decryption algorithm.

These rounds are governed by the following four stages:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The tenth round Mix columns stage is not included. The first nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

Substitute Bytes: Is a non linear byte substitution, using a substation table (S-box) each byte from the input state is replaced by another byte. The substitution is invertible and is constructed by the composition of two transformations.

Shift rows: In the Shift Rows transformation, the first row of the state array remains unchanged. The bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the left, respectively.

Inverse Shift rows: Is the inverse of the shift rows, the first row of the state array remains unchanged. The bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the right, respectively.

Mix columns: In the Mix Columns transformation, every column of the state array is considered as polynomial over GF (28) that is used in the AES.

Addroundkey: The AddRoundKey operation is a simple XOR operation between the State and the Round Key. The Round Key is derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element. There are three steps, in each Key schedule round.

- **Keyrotate:** The function Keyrotate takes a four-byte word and rotates one byte to the left.

- **Keysubytes:** The Keysubytes operation takes four-byte input word by substituting each byte in the input to another byte according to the S-Box.

KeyRcon: The first byte of a word is XORed with the round constant. Each value of the Rcon table is a member of the Rinjdael finite field. Add round key is same for the both encryption and decryption.possible.

3.3 Data Embedding

Least Significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity [7]. The fundamental idea here is to insert the secret message in the least significant bits of the images. This actually works because the human visual system is not sensitive enough to pick out changes in color where as changes in luminance are much better picked out. A basic algorithm for LSB substitution is to take the first N cover a pixel where N is the total length of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits.

Table 1: Illustration of LSB techniques

Before Replacement	After Replacement	Bit inserted	Remarks
1011101	00101101	1	No Change
00011100	00011101	1	Change in bit Pattern
11011100	11011100	0	No Change
10100110	10100110	0	No Change
11000100	11000101	1	Change in bit Pattern
00001100	00001100	0	No Change
11010010	11010010	0	No Change

Least significant bit (LSB) insertion is a common, simple approach for embedding information in a cover image. The LSB or in other words 8-th bit of some or all the bytes inside an image is changed to a bit of the secret message. Let us consider a cover image contains the following bit patterns:

Byte-1 Byte-2 Byte-3 Byte-4

00101101 00011100 11011100 10100110

Byte-5 Byte-6 Byte-7 Byte-8

11000100 00001100 11010010 10101101

Suppose a number 200 is to embed in the above bit pattern. Now the binary representation of 200 is 11001000. To embed this information at least 8 bytes in cover file is needed. Hence taken 8 bytes in the cover file. Now modify

the LSB of each byte of the cover file by each of the bit of embed text 11001000. The Table 1.1 shows what happens to cover file text after embedding 11001000 in the LSB of all 8 bytes.

3.4 Data Extraction and Image recovery

According to the availability of the key data extraction or image recovery has performed or both. The receiver may have both key or image encryption either data encryption key. When the user have the image recovery key the encrypted image will able decrypt, but it still keep the hidden message. So the decrypted image may contain some noise. When the user has the data encryption key user can decrypt the encrypted data. Actually the data encryption key is acts also as a data embedding key so using the data encryption key the hidden data is extracted from the encrypted image and then it decode the encrypted data into actual data. If the user have the both the data encryption key and the image encryption key they can able to access both the hidden data and the image. The decrypted image doesn't contain any noise in it, because the hidden data is extracted from the image.

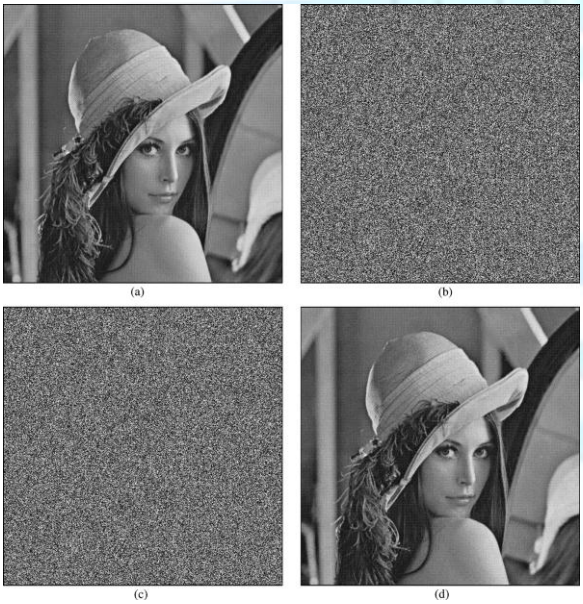

Fig. 2. (a) Original image, (b) its encrypted image, (c) encrypted image containing embedded data and (d) directly decrypted image.

3. Results and Discussion

In steganography following factor are considered after embedding secret message in the cover medium

A. Utilization factor

The utilization factor denotes the amount of cover image that has been utilized to embed the secret message into it,and it is given by x

*Utilization Factor = secret message size (bits)/ cover medium size (bits)*100* (1)

B. PSNR value

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of a logarithmic decibel scale. A higher PSNR value indicates that the reconstruction is of higher quality.PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codes. The signal in this case is the original data, and the noise is the error due to hiding. The PSNR value is calculated by,

$$PSNR(dB) = 10 * \log \frac{255^2}{MSE} \quad (2)$$

Where MSE: Mean-Square error Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image and is given by Eqn.3.

$$MSE = \sum_{i=1}^{x} = \sum_{j=1}^{y} \frac{(|A_{i,j} - B_{i,j}|)}{x + y} \quad (3)$$

Where x- width of image; y- height; x*y- number of pixels.

5. Conclusion

In this paper, a novel scheme for separable reversible data hiding in encrypted image is used, which consists of image encryption, data encryption, data embedding and data extraction / image recovery phases. In the first phase, the content owner encrypts the original image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data before that the additional data can be encrypt. With an encrypted image containing additional encrypted data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error.

References

[1] Chaitanya Kommini, Kamalesh Ellanti, Srinivasulu Asadi, "Image Based Secret Communication Using Double Compression", International Journal of Computer Applications, Volume 21, no.7, pp. 6-9, May 2011.

[2] Hamida M. Almangush, "A Novel Reversible Data Hiding Technique with High Capacity and Less Overhead Information", International Journal of Computer Applications, Volume 43, no.19, pp. 42-47, April 2012.

[3] Harshitha K M, "Secure Data Hiding Algorithm Using Encrypted Secret message", International Journal of Scientific and Research Publications, Volume 2, Issue 6, pp. 1-4, June 2012.

[4] Jobi.V.Das , "Data Hiding using a Novel Reversible Method for Encrypted Image", International Journal of Advanced Research in Technology, Vol. 2 Issue 5, pp. 28-32, May 2012.

[5] Kishore Reddy, "Encrypted Data Hiding in Encrypted Images", International Journal of Research in Engineering & Applied Sciences, Volume 2, Issue 9, pp. 50-59, September 2012.

[6] Manjula N Harihar," Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, pp. 290-294, June 2012..

[7] Vikas Tyagi,"Data Hiding in Image Using Least Significant bit with Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, pp. 120-123, pp. 290-294, April 2012.

[8] Vinay pandey , Angad Singh, Manish Shrivastava, "Medical Image Protection by Using Cryptography Data-Hiding and Steganography", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, pp. 106-109, January 2012.

[9] Wien Hong, "Reversible Data Embedding for High Quality Images Using Interpolation and Reference Pixel Distribution Mechanism", Science Direct, www.elsevier.com/ locate/ jvci, J. Vis. Commun. Image R. 22, pp. 131-140, 2011.

[10] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE Transactions on Information Forensics and Security, Vol.7, no. 2, pp. 826-832, April 2012.