Hiding Data in Encrypted Image with LSB Substitution

M. C. Padma[1], Yashaswini. J[2]

[1]Professor and HOD, Department of CSE, PES College of Engineering, Mandya, Karnataka-571401, India

[2]M.Tech 2nd year, Department CSE, PES college of Engineering, Mandya, Karnataka-571401, India

Abstract: ***Using data hiding technique one can send the information to the accurate user without noticing to third person. Data can be hidden using different cover Medias, like video, audio, images or text. As an Internet based communications of images have increased, encryption of images has become very important way to protect images especially on the Internet. This work proposes a new scheme for hiding data in encrypted image with LSB substitution. It consists of image encryption, data embedding and data-extraction/image-recovery phases. A content owner encrypts the original image using an encryption key. A data-hider changes the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. At the receiver side, the data that is embedded in the created space can be easily retrieved from the encrypted image using 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.***

Keywords: Data hiding, data extraction, image encryption, reversible data hiding.

1. Introduction

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. The common way to do this is to transform the secret data into another form, which is called Encryption. Steganography is the art of hiding data within data. Steganography is a means of storing information in a way that hides that information's existence and it can be used to carry out hidden exchange. Steganography can also enhance individual privacy.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, 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. A number of reversible data hiding methods have been proposed in recent years. In difference expansion method [1], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [2].

Encryption is well known for privacy protection. For securely transmission of image a content owner encrypt the image before transmitting it to another person. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images. It may be also hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable [3]. Figure 1 gives the sketch of reversible data hiding scheme for encrypted image.

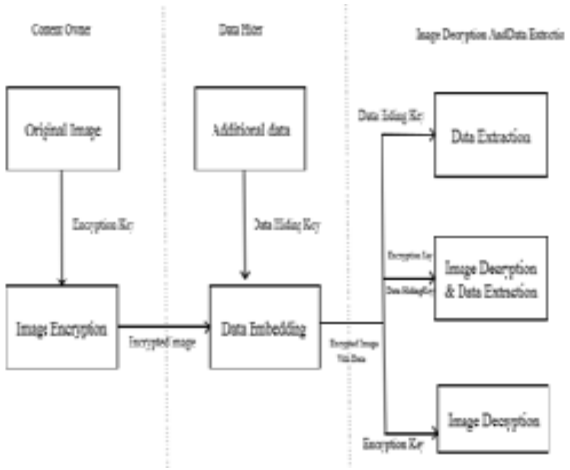

Figure 1: Sketch of existing system

A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In this scheme, the data extraction is not separate from the image decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any

information from the encrypted image containing additional data.

This paper proposes new scheme for data hiding into an encrypted image. A content owner encrypts his image before transmission by using encryption key. An additional data can be added to this encrypted image using the data hiding key. At the receiver side if receiver has only data hide key, he can only extract the data from image. If receiver has encryption key then he can decrypt the image. But if receiver has both, data hiding and encryption key then he can extract data and as well as can recover image when the amount of data is not too large [4].

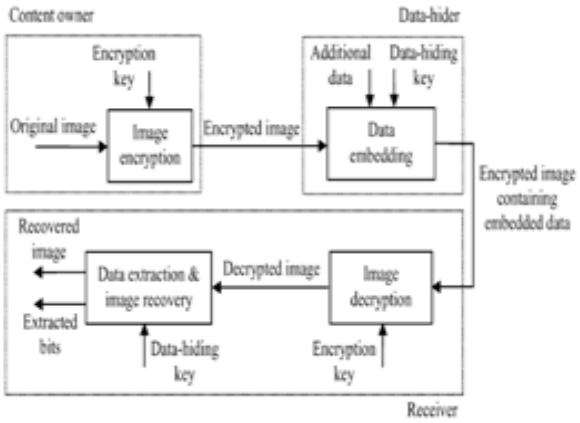

Figure 2: Sketch of proposed system

2. Proposed Model

The proposed scheme consists of image encryption, data embedding and data extraction/image-recovery phases. The content owner encrypts the original image using an encryption key to produce an encrypted image. Then, the data-hider Changes the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data 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. Figure 2 gives the sketch of the proposed scheme. The three phases of the proposed model is explained below,

2.1 Image Encryption

Assume the original image with a size of N1 x N2 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 bi,j,0, bi,j,1,….bi,j,7where $1 \le i \le N1$ and $1 \le i \le N2$, the gray value as pi,j, and the number of pixels as N(N = N1 x N2). That implies

$$B_{i,j,k} = [\, pi,j / 2^k] \bmod 2,\ k=0,1,\ldots,7$$

In encryption phase, the exclusive-or results of the original bits and the random bits generated by the encryption key are calculated.

$$Bi,j,k = b_{i,j,k} \oplus r_{i,j,k}$$

Where $r_{i,j,k}$ are determined by an encryption key using a standard stream cipher.

2.2 Data Embedding

In this scheme data embedding to encrypted key is done by changing the LSB of the encrypted image using data hiding key. Least Significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity [5]. 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 colour. A basic algorithm for LSB substitution is to take the first N cover a pixel where N is the first letter 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. 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
11000100 00001100 11010010 10101101

Byte-5 Byte-6 Byte-7 Byte-8
00101101 00011100 11011100 1010011

Suppose a message ‘a’ is to embed in the above bit pattern.

Now the ASCII representation of a is 01000001. 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 01000001. The Table 1.1 shows what happens to image file after embedding the binary value 01000001 of message ‘a’ in the LSB of all 8 bytes. In this way every pixel’s last bit is replaced by the remaining message bits.

Table 1.1: Illustration of hiding data in encrypted image

Bits before inserted	*Bit inserted*	*Bits after inserted*	*Status*
11000100	0	11000100	No change
00001100	1	00001101	Bit changed
11010010	0	11010010	No change
10101101	0	10101100	Bit changed
00101101	0	00101100	Bit changed
00011100	0	00011100	No change
11011100	0	11011100	No change
10100110	1	10100111	Bit changed

2.3 Image Recovery and Data Extraction

According to the availability of the key, the data extraction, image recovery or both can be performed. The receiver may have both key and either image encryption or data hiding key. When the user has the image encryption key then the encrypted image will able to be decrypted, but it still keep the hidden message. If the user has data hiding key then he can able to retrieve the data. If the user has both the data hiding key and the image encryption key they can able to access both the hidden data and the image.

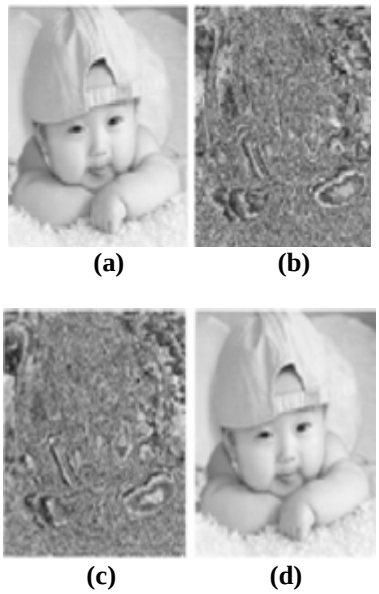

Figure 3: (a) Original image (b) Encrypted image (c) Encrypted image with data (d) Decrypted image

3. Results and Discussion

Figure 3 shows the result of the proposed scheme.

- AES algorithm takes more execution time. Here we are using a stream cipher for image encryption, so we can reduce the execution time for the encryption process. The comparison chart of advance encryption standard and a stream cipher is shown below,

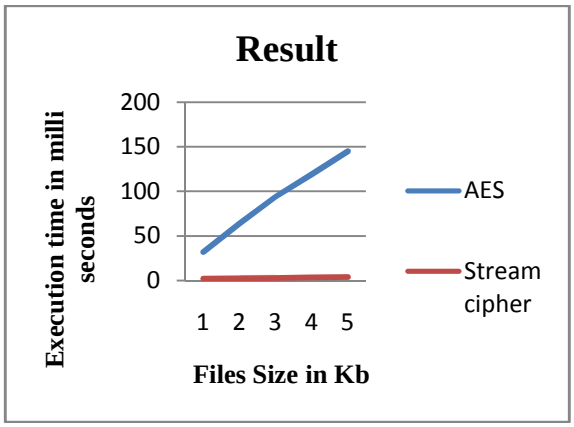

Figure 4: Execution time for AES and Stream Cipher

- To compare the original and decrypted image a PSNR value can be used. PSNR is Peak Signal Noise Ratio, and it is a 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,

$$PSNR=10*\log (255^2/MSE)$$

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

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

Where x- width of image, y- height, x*y- number of pixels

File size	*AES*	*Stream Cipher*
1kb	32	2
2kb	64	2.5
3kb	94	3
4kb	119	3.5
5kb	145	4

- 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,

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

4. Conclusion

In this paper, a new scheme for hiding a data in encrypted image is proposed, which consists of image encryption, data embedding and image recovery/data-extraction phases. A content owner encrypts the original image using an image encryption key by a stream cipher. To this encrypted image a user can embed the additional data by changing the LSB of the encrypted image using the data hiding key. At the receiver side, if he has the data hiding key then he can retrieve the data that is hided in the encrypted image. If the receiver has the encryption key then the decryption of the encrypted image can result in an image similar to the original version because data embedding only affects the LSB of the encrypted image. If the receiver has both keys, then using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image is also decrypted when the amount of the data is not too large. The original and decrypted image can be compared by calculating PSNR value.

References

[1] Manikandan R and Uma M,MahalakshmiPreethi S M, “Reversible Data Hiding for Encrypted Image”, Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-1, February 10, 2012.
[2] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol. , vol. 13, no. 8, pp. 890–896, Aug. 2003
[3] Xinpeng Zhang, “Reversible Data Hiding in Encrypted Image” IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011.
[4] Xinpeng Zhang,”Separable Reversible Data Hiding in Encrypted Image” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.
[5] 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.
[6] M.U.Celik,G.Sharma,A.M.Tekalp,andE.Saber,"Lossless generalized-LSB data embedding," IEEE Trans. Image Process. ,vol.14, no. 2, pp. 253–266, Feb. 2005.
[7] Mohanrajarumugam and Rabindra kumar," Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image", International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013

Author Profile

Dr. M. C. Padma received her B.E. Degree in Computer Science and Engineering and M.Sc. Tech. by Research degree from University of Mysore, Mysore, India and Ph.D. from Visvesvaraya Technological University, Belgaum. She is currently working as Professor in the department of Computer Science and Engineering, PES College of Engineering, Mandya, Karnataka. Her main research interests are in the area of image processing, pattern recognition, data base management system, data structures, natural language processing, data mining, document image processing, network security and cryptography.

Yashaswini. J received her B.E degree in Information Science from Coorg institute of Technology, Visvesvaraya Technological University, Belgaum, India in 2010.Now pursuing M Tech degree in Computer Science and Engineering from PES College of engineering, Mandya, India. She is currently doing project work under the guidance of Dr. M. C. Padma. Her research interests are web services, network security and cryptography.