ISSN:0975-9646

Hidding secured information into secured image

[1]J.Sabthami, [2] N.Nivetha, [3] P.Maheswari, [4] S.Janani

[1]Student, [2] Student, [3] Student, Assistant professor, Department of Computer Science and Engineering
Kamaraj college of Engineering College,Virudhunagar, India

***Abstract* – Information Security play a major problem in day-to-day lives. The information which has to be send in secured manner is embedded into the encrypted image using Least significant bit algorithm. The uncompressed image is encrypted using as key and data is embedded into a encrypted image using different key. To improve the security image protection is included. In the receiver side if the encryption key is alone known the image can be extracted which is similar to the original image. If the data hiding key is alone known only the data hidden can be extracted. Only both image and data hidden can be extracted if both the key is known.**

Keywords-Information security, key, encryption, uncompressed, data hiding .

I. INTRODUCTION

In recent technological world the usage of internet have been increased among people. The data transfer also increased as terabytes, petabytes and so on. But the security is a problem to transfer a image or a data in a secure manner. Many of the military related information, medical data, medical image, and all other secured information are hacked and modified by various attacks and threats. Various techniques are successfully implemented for data transfer and storage of large data but security play a important problem.

Information security is very useful for protecting the valuable secured data from unauthorized hackers. The information security is used to prevent modification of data. Cryptography and steganography is the main area which is used for securing the information by various methods using encryption, decryption, keys.

Steganography and watermarking which are the main areas of information hiding. Steganography means the data which is embedded into image cannot be detected. Watermarking is similar to steganography but the data embedded into the image can be seen but cannot be modified.

When larger images of greater bit has to be transmitted through internet image compression techniques used for to transmit the image at faster speed by reducing the size of the image. The image compression method is used for creating space for embedding secure data inside the image.

The owner compresses the encrypted image by changing the LSB bit [1][3][6] to create a space to embed the additional data . Only the last bits are modified to create a space to accommodate the data to be embedded.

The encryption is performed using secret key to improve the security. The user without the decryption key cannot read the information. Different keys are used for image encryption and data hiding. Cryptography is based on the sender and receiver of a data who use the same secret key. The sender uses the secret key to encrypt the message into a unreadable form, and the receiver uses the same secret key to decrypt the hidden message. This method is known as secret-key cryptography which is one form of protection of data.

Reversible data hiding is a technique to embed additional secret data into some distortion-unacceptable content [2], such as military images or medical images, with a reversible manner in such a way that the original content can be perfectly restored after extraction of the hidden message[4][5]. The image encrypted can be restored with small amount of changes using decryption key. The content of the data hidden can be extracted using data hiding key. Only if both data hiding and encryption key is known the data and image can be extracted.

II. PROPOSED SCHEME

The proposed method consist of Image encryption, data hiding, image protection and data recovery and image extraction. The original uncompressed image is encrypted by owner using image encryption key and the data is embedded inside the spare space of image which is by compression technique. LSB based compression method is used for compressing the image by change the binary value of the LSB bit. Image protection is used to enhance the security. The image protection is the first step in the receiver side before decryption process. The block diagram of the proposed method is given in Figure 1.

A. Image Encryption

Encryption is part of cryptography, which converts the image into unreadable from. Encryption is a task used to protect the image from access of unauthorized author. The encryption is the process of converting plain text into cipher text using secrete key.

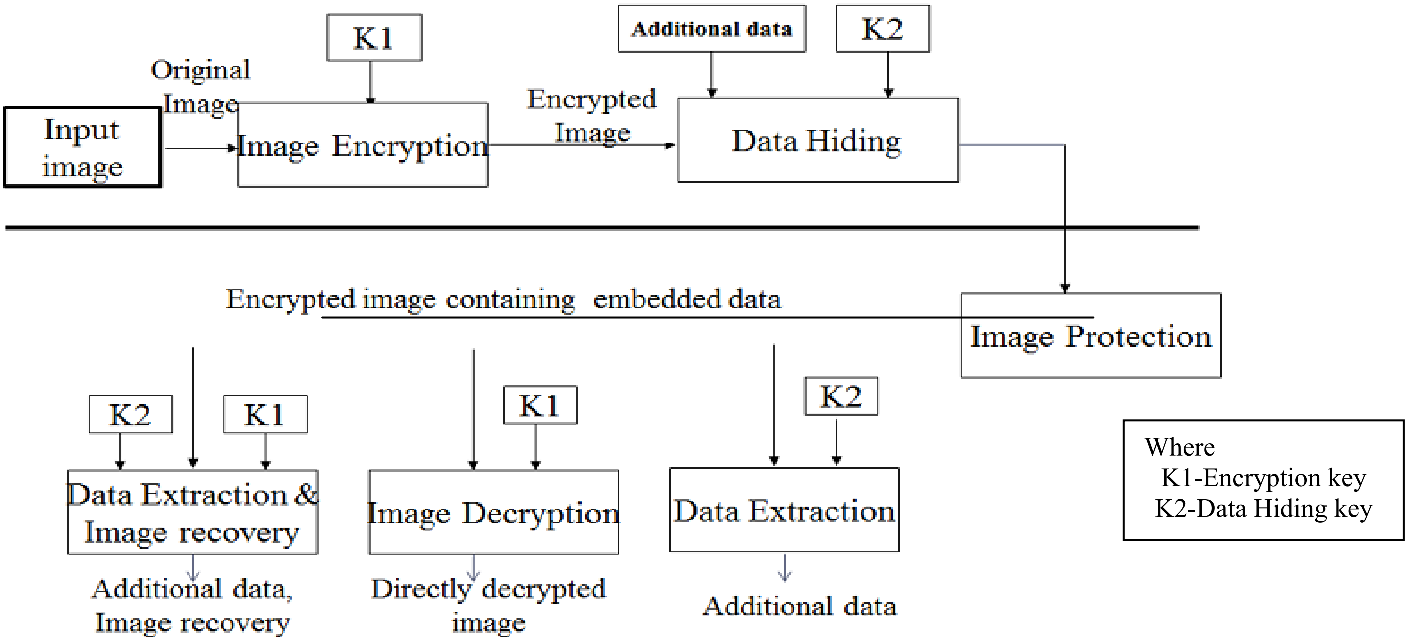


Figure 1.Block diagram for Proposed System

The purpose of encryption is to hide the data from the unauthorized, unintended person. The original uncompressed image with size of N1 x N2 and each pixel with gray value falling into [0-255] is represented by 8 bit (u) [13]. The image encryption is given in Figure 2.

The encrypted bit can be calculated by

$$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u}$$

Where $b_{i,j,u}$ - bits of a pixel

$r_{i,j,u}$ - pseudo random bits

$1 \leq i \leq N1, \; 1 \leq j \leq N2, \; 0 \leq u \leq 7$

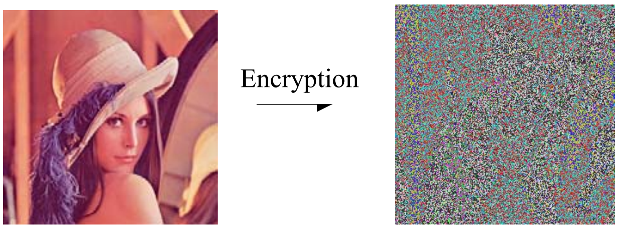


Figure 2. Image encryption

B. Data hiding

The data to be send in secured manner is embedded in the uncompressed image by changing the LSB bits[7]. The data hiding is done using a data hiding key which is different from the image encryption key. During the data hiding process the MSB (Most significant bit) of the encrypted image is not changed.

Original encrypted image is compressed using LSB (least significant bit) scheme for accommodating additional data. The compression is done in such a way that the there is no loss of information called as lossless compression[10] [11]. From each pixel group collect the N least significant bits of the O pixels and it is denoted as,

$$B(k,1), B(k,2), \ldots\ldots B(k,N,O)$$

Where k is a group index.

Data is inserted into M least significant bits. The result of data hiding is given in Figure 3.

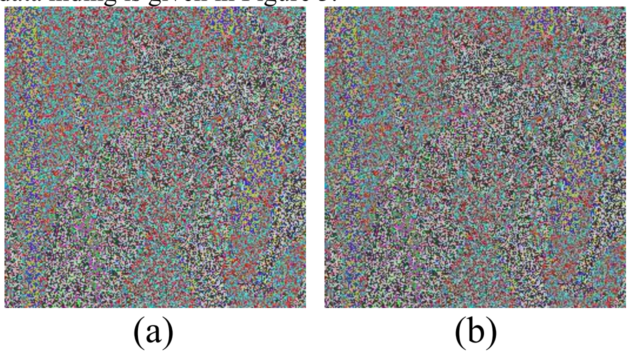


Figure 3. Result for Data Hiding (a) Encrypted image (b) Image after embedding.

For example 24 bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 120, which binary representation is 11110000, is embedded into the least significant bits of this part of the image, the resulting is as follows:

(0010110**1** 0001110**1** 1101110**1**)
(1010011**1** 1100010**0** 0000110**0**)
(1101001**0** 1010110**0** 0110001**0**)

Bit masking is done for embedding the data after encryption. The bit masking is done by using bit wise operations include AND (&) OR (|) Left Shift (<<) and Right Shift (>>).

C. Image protection

The security is enhanced by image protection technique. The source image is protected by using Pattern guessing technique. An image is separated into subparts and the user need to click on the image in specific sequence. The image is split into NxN (eg.4x4) subparts. The sequence has to be defined by owner. If the sequence is correct then the source image will be opened for further decryption. The image protection is shown in figure 4.

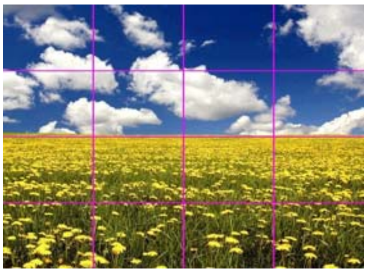


Figure 4. Image protection

Image protection is the first step of security in receiver side. After the sequence is correctly identified the page with option for image recovery, data extraction and both image and data extracted is displayed.

D. Data Extraction and Image Recovery

Image extraction and image recovery is by decryption process. Both image and data extraction is done by separable reversible process[8][9]. Decryption is a converse process of encryption. The encryption process converts the data into unreadable form and decryption process converts the unreadable data into readable form.

It follows three process

- If the image alone has to be extracted image encryption key should be known.
- If the data alone has to be extracted data hiding key should be known.
- If both data and image has to be extracted then both data hiding and image encryption key has to be known.

The decryption is done to receive the data using

$$b'_{i,j,u} = B'_{i,j,u} \oplus r_{i,j,u}$$

Where $r_{i,j,u}$ are derived from the encryption key.

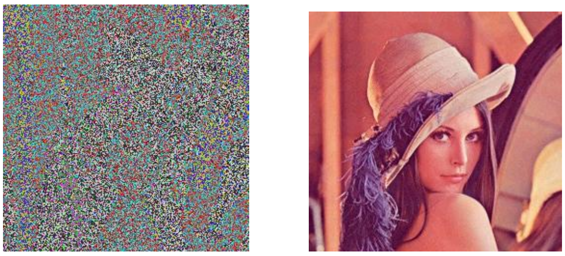
The gray values of decrypted pixels are

$$p'_{i,j} = \sum_{u=0}^{7} b'_{i,j,u} .2^{u}$$

The encryption and decryption combined is equal to one. Since it is a dual process

$$b'_{i,j,k} + b_{i,j,k} = 1$$

The data embedded by changing the LSB bit in the encrypted image. While decryption process the image extracted will have only very little distortion. The result of image recovery from the encrypted image is given in Figure 5



. (a) (b)

Figure 5. Result for (a) Encrypted image after data embedding (b) Image recovery

APPLICATION

This application is used in military application, Medical diagnosis and so on. For example in military application if a person has to send image of the equipment to only some people and usage of the equipment to some group of people and both image and data of the equipment to some people in secured manner.

CONCLUSION AND FUTURE WORK

In this paper, we build a system to provide security for data and image to be send in secured manner. The owner encrypts the image and embedded the data into the image for transfering the image in secured manner. The image protection is included to enhance the security. The data and image can be extracted only if the keys are known. The keys used for image and data extraction are both different. This system is used in day to day life because of the usage of internet is increased more. It follows separable reversible technique. The data alone can be extracted by knowing the data hiding key. The image alone can be extracted by knowing the image encryption key. Both the data and image can be extracted by knowing the both different keys.

In future work, it is planned still enhance the security level. And also use the MSB (Most significant bit) to embedded the bit when there is lot of changes in the pixels

ACKNOWLEDGMENT

The authors like to express the gratitude to Management and Principal of Kamaraj college of Engineering for providing support for carrying out this work.

REFERENCES

1. Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp(2005) developed “Lossless Generalised-LSB Data Embedding”..
2. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su,(2006) “Reversible Data Hiding”.
3. M. Johnson, P. Ishwar, V. M. Prabhakaran, D.Schonberg, and K.Ramchandran,(2004) “losseless compression”.
4. W. Puech, M. Chaumont and O. Strauss , (2008), “A Reversible Data Hiding Method for Encrypted Images”.
5. C.-C. Chang, C.-C. Lin, and Y.-H. Chen, (2008), “Reversible data-embedding scheme using differences between original and predicted pixel values”.
6. Hsien-Wen TSENG, Chin-Chen,(2004) ,“High Capacity Data Hiding in JPEG-Compressed Images”.
7. F. Cayre and P. Bas, (2008), “Kerckhoffs-based embedding security classes for a data hiding”.
8. Zhang,(2011),developed “Reversible data hiding in encrypted image”.
9. Xinpeng Zhang ,(2012),”Separable Reversible Data Hiding in Encrypted Image”.
10. V.Manjula, J.Rajani, K.Radhika,(2012)”A Secure Data Hiding Technique in Compressed Video Using a Secret Key”.
11. Xin-Peng Zhang,(2011),developed “Lossy Compression and Iterative Reconstruction for encrypted image”.
12. Wien Hong ,tung-shou chen developed,(2012), “An improved reversible data hiding in encryption image using side match”.
13. W. Liu, W. Zeng, L. Dong, and Q. Yao,(2010), “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process.