Reversible Data Hiding Technique

Adona Antony, Angel Maria Savio
Dept. of Electronics and Communication Engineering
Amal Jyothi College of Engineering
Kanjirappally- Kottayam

Anusree B K, Emil Maria Chacko
Dept. of Electronics and Communication Engineering
Amal Jyothi College of Engineering
Kanjirappally- Kottayam

***Abstract*— By Reversible Data Hiding Technique (RDH), the original cover image can be recovered back from the marked media. This allows a secret image to be hidden in an original image which can be retrieved as and when required. The multimedia content can be made secure by the process of encryption. Thus content owner encrypts the original uncompressed image by the process of Stream Cipher encryption using an encryption key. The encrypted image is then compressed to reduce the amount of data required for representing the image which further reduces the transmission time. Compression technique used is wavelet compression. The data hider can hide the secret image using a data hiding key. The receiver does all these processes in reverse to extract the secret image as well as the original cover image. Thus the data hiding key is used to extract the secret image, and then the cover image is decompressed and finally decrypted using the encryption key. Thus this paper focuses on achieving better security.**

Keywords*— *RDH, Stream Cipher Encryption, Wavelet Compression, Secret image Embedding.

I. INTRODUCTION

In this era of technology, security is a big issue and securing important data is very essential, so that the data cannot be intercepted or misused for illegal purposes. So different cryptographic methods are being used by different organizations and government institutions to protect their data online.

In applications like law enforcement, medical image systems, remote sensing and military imaging, the original image needs to be recovered back. Reversibility of original media is thus required in such cases. This type of data hiding is termed lossless data hiding or Reversible Data Hiding (RDH) [1].

Image encryption is the process of scrambling the data. It is a popular means of information protection. It is a form of cryptographic measure. Though the process of cryptography and steganography aims in providing security against various threats, these two are conceptually different. The former just scrambles the data whereas the latter imposes data hiding. Cryptography and steganography when combined together offers improved authentication.

Cryptography can be divided into two types : 1)Symmetric key cryptography

2)Private key cryptography

In Symmetric key cryptography, same key is used for both encryption as well as decryption whereas in Public key cryptography, one key is used for encryption and another publically generated key is used for decryption. In symmetric key, it is easier for the whole process as same key is used for both encryption and decryption. Public key cryptography is more popular because of its security but still these methods are also susceptible to attacks like 'brute force key search attack'.

The key used for encryption is produced by a pseudorandom number generator. Encryption can be classified based on how they process on the given input data. Block cipher is a method where inputs are being processed on a block by block basis whereas Stream cipher is a method by which inputs are being processed bitwise. In stream cipher, the cipher text is obtained by performing Ex-or operation between the pixels of original image and the pseudorandom number generated which is a key. Since the operation of Ex-or seems easier, stream cipher method is faster than block cipher method.

Every image, being encrypted or unencrypted contains some amount of redundant data. This redundancy is being reduced by means of data compression. Image compression thus minimizes the size of multimedia files in bytes without degrading the image quality [2]. Discrete Cosine Transformation is one well known form of image compression
which does lossy type of compression with higher compression rate. Other form of wavelet compression is achieved through wavelet transforms. Wavelets are mathematical tools for decomposing an image hierarchically. Wavelet compression offers more advantages than DCT compression techniques [2].

In data embedding phase, the pixels of the secret image are embedded into the LSB of the compressed image. Data hiding has many applications such as authentication, copyright, ownership of digital images, fraud detection, adding caption to images, additional information such as subtitles to video etc. Thus these methods provide high security and authentication to the transmitted data.

II. PROPOSED SCHEME

A. Encryption

Cryptography finds applications in the security of ATM cards and computer passwords [3]. Encryption is a cryptographic method. This paper uses stream cipher for encryption. Stream cipher is produced with pseudo randomly generated key values, which makes hacking difficult. Stream ciphers are generated by Ex-oring the contents of original image pixels with the key value maintaining the integrity of specifications.

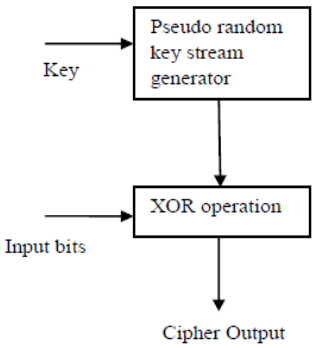

Fig 1. Stream Cipher Generation

The process of generating a stream cipher output is shown above. The input image bits is Ex-ored with the key values to generate cipher output [5]. To generate a stream cipher, a key is input to the random no generator. For improved security the key stream is unpredictable without knowing the key value. The key stream is completely independent of the original image.

Advantages of stream cipher lies in the fact that the encrypted output is dependent on the pseudorandom key which offers improved security. They also offer implementation simplicity and higher speed [4].

B. Compression Technique

Digital images are comprised of an enormous amount of data. Reduction in the size of the image data for both storing and transmission of digital images are becoming increasingly important as they find more applications.

Image compression is a mapping from a higher dimensional space to a lower dimensional space. Image compression plays an important role in many multimedia applications, such as image storage and transmission. The basic goal of image compression is to represent an image with minimum number of bits of an acceptable image quality.

With the advanced development in internet, teleconferencing, multimedia and high definition television technologies, the amount of information that is handled by computers has grown exponentially over the past decades. Hence, storage and transmission of digital image component of multimedia systems is a major problem. The amount of data required to represent images at an acceptable level of quality is extremely large. High quality image data requires large amount of storage space and transmission bandwidth, something which the current technology is unable to handle technically and economically. One of the possible solution to this problem is to compress the information so that the storage space and transmission time can be reduced.

Here we are performing wavelet based image compression. The wavelet transform has the ability to de-correlate an image both in space and frequency, thereby distributing energy compactly into a few low frequency and a few high frequency coefficients.

The wavelet transform decomposes an image into a set of different resolution sub-images, corresponding to the various frequency bands. The main advantages of wavelet based image compression is summarised below:

(i) Wavelets have a non-uniform frequency spectra which facilitate multi scale analysis.

(ii) The multi-resolution property of the wavelet transform can be used to exploit the fact that the response of the human eye is different to high and low frequency component of an image.

One of the simplest wavelets is the Haar wavelet which is given by

$$\varphi(t) = \begin{cases} 1, 0 \le t < \frac{1}{2} \\ -1, \frac{1}{2} \le t < 1 \end{cases}$$

It is a bipolar step function. It is a real function, anti-symmetric with respect to t=1/2. The Haar wavelet is discontinuous in time.

1. Wavelet decomposition

The input image is sub divided into several frequency bands namely LL, LH, HL and HH by passing it through a set of consecutive low pass and high pass filters. The outputs of low pass filter are referred to as approximation coefficients and the outputs of high pass filter are referred to as detail coefficients.

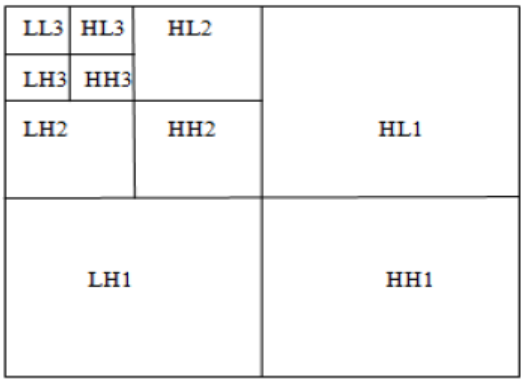

Fig 2. Structure of Wavelet Decomposition

2. Quantization and Encoding

Quantization involves representing the coefficients obtained as a result of decomposition by a finite number of

levels. Quantization, involves compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible.

Run-length encoding (RLE) is a very simple form of data compression in which runs of data, that is, sequences in which the same data value occurs in many consecutive data elements are stored as a single data value and count, rather than as the original run.

C. Secret Image Embedding

The compressed image is used as the medium for hiding the secret image. For this, we employ a data hiding key. The secret image can be extracted only if this data hiding key is known to the receiver.

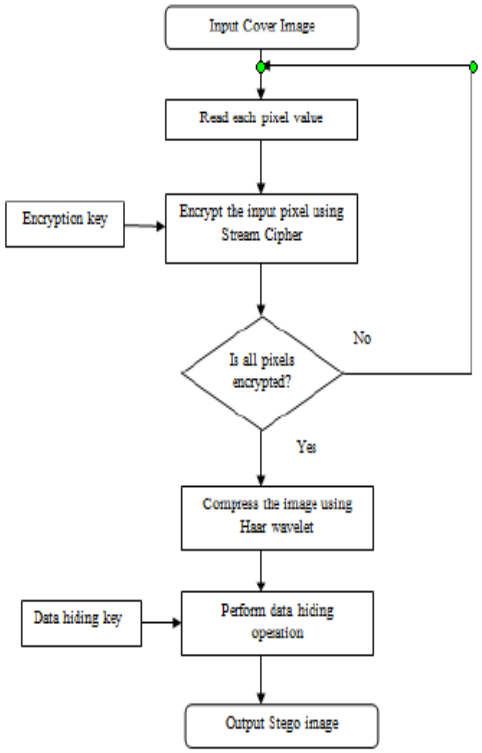

Fig 3. Flowchart of Data Hiding

D. Secret Image Extraction and Cover Image Recovery

At the receiver the secret image embedded in the created space can be easily retrieved from compressed image by using the data hiding key. Since the secret image embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both the encryption and data hiding keys, the secret image can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

III. EXPERIMENTAL RESULTS

The image Lena sized 512*512 is used as the cover image in the experiment. Secret image of size 64*64 is embedded into the compressed image using a secret key. The extraction procedure is then applied to retrieve the secret image and the original image is recovered by using the decryption key. This paper is implemented with the software MATLAB and the following results are obtained.

Fig 4. Cover Image

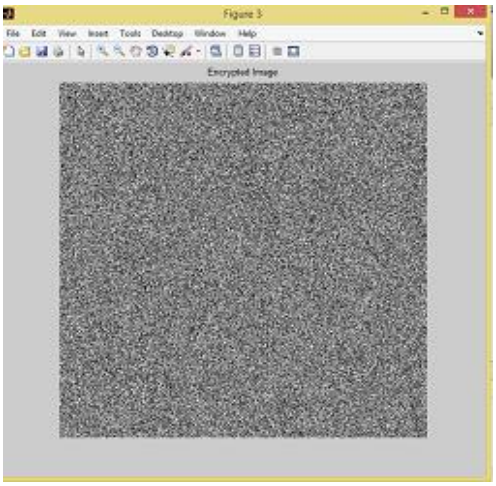

Fig 5. Encrypted Image

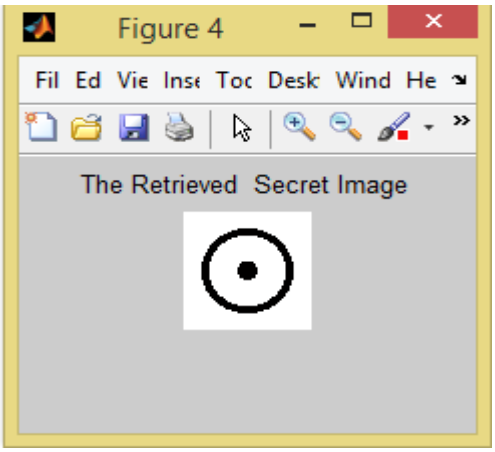

Fig 6. Secret Image

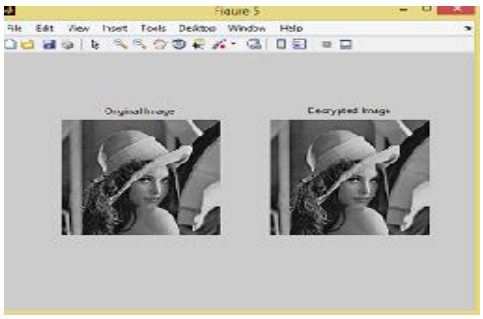

Fig 6. Recovered Image

IV. CONCLUSION

This method describes the technique for recovering back the original image from the marked media. By employing encryption key and data hiding key double protection is achieved. Haar wavelet transformed compression is used to improve the transmission rate.

REFERENCES

[1] Yun Q. Shi, "Reversible data hiding", New Jersey Institute of Technology, Newark, NJ 07102, USA.
[2] Kamrul Hasan Talukder and Koichi Harada, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image", IJAM_36_1_9.
[3] Musbah J.Aquel, Zid A Alqadi, Ibraheim M. El Emary, "Analysis of stream cipher security algorithm", Journal of Information and Computing Science,ISSN 1746-7659, vol.2,no.4,2007, pp. 288-298.
[4] C. Rengarajaswamy, K. Vel Murugan, "Separable Extraction of Concealed Data and Compressed Image".
[5] S. Imaculate Rosaline, C. Rengarajaswamy, "A Steganographic Substitution Technique using APPM for Encrypted pixels".