Securing Information Using Steganography

M Venkteswara Reddy[1], **M Lakshman Naik**[2]

[1]M.Tech Student, Department of PG (E&T), LITAM, JNTUK, A.P, India

[2]Assistant Professor, Department of ECE/CSE, LITAM, JNTUK, A.P, India

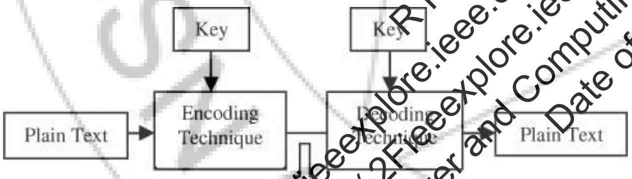
Abstract: *Now a day's the medium of communicating the information is through the internet and there are enough hackers to hack the information because the data has transferred through covert channels. The information will encrypt using cryptographic algorithms and the cipher text can see by a third - party adversary and by applying cryptanalysis the information can retrieve back. The major problem in applying cryptography is that, the cipher text is visible to unauthorized user. We can avoid this by using steganography. Different techniques are available to hide the information in steganography. Transformation techniques produce more noise in the image when the information has embedded. To avoid the noise distortion in the image, the LSB insertion method is used to insert the bits in an image by using random number generators. In this proposed technique before embedding the secret information into an image, the secret information has been compressed using the wavelet transform technique. The obtained bits after compression are encoded using quantum gates.*

Keywords: Information hiding, Steganography, Random number generator, Quantum computing, Transformation technique.

1. Introduction

Present days all the information is stored in the form of digital media. By using the internet as a medium lots of information is transferred from one person to another person. Every system can provide different security mechanisms for outgoing packets. The sender and receiver assumes that the is information is securely transferred. But the information is transferred over covert (insecure) channel, if anyone can get the encrypted information and by applying cryptanalysis on it, the intruder can get the original message, the adversary can even alter the information and pass to the receiver.

Two types of mechanisms are there to provide security for the information, they are cryptography and steganography. Cryptography means [1, 5, 8, 9] converting the text from readable format to unreadable format.



Cipher Text Figure: Block diagram for cryptography

But the encrypted text is visible to all, by applying cryptanalysis on cipher text, the intruder can get the original message, otherwise, he can alter the cipher text. Steganography is used for concealing the information in an image [1, 8, and 10]. The basic Stenographic model is shown below.

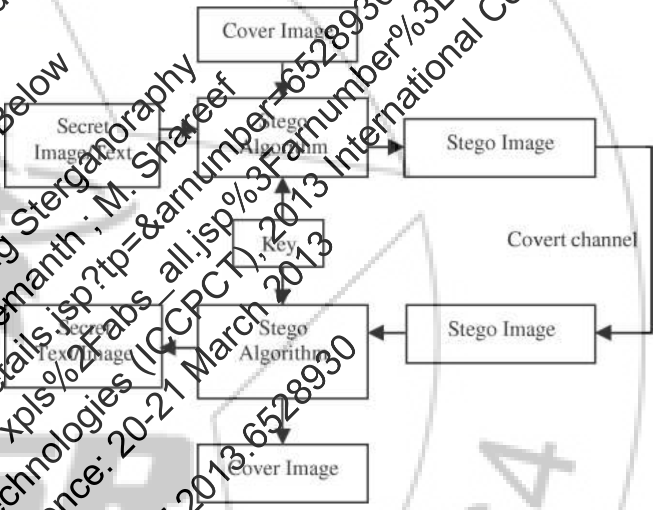


Figure: Block diagram for steganography

There are three different types of steganographic techniques are available for concealing the information in an image, that is Least Significant Bit Insertion, Masking, and Transformation techniques. The above three techniques having their own characteristics. Least significant bit insertion is the best technique for embedding the secret information in an image with less noise, but it is applicable only for a small amount of data. Transformation techniques are useful for embedding the large amount of data in an image, the main drawback in transformation technique is, it produces more noise in the stego image.

By using LSB insertion, large amount of data cannot be embedded in an image. Due to overcome this transformation techniques are performed on the secret information and then perform LSB insertion to embedded the transformed bits in an image.

Due to overcome this transformation techniques are performed on the secret information and then perform LSB insertion to embedded the transformed bits in an image. In the section 2, discussed about the background work of LSB insertion, CNOT gate, wavelet transformation, Random number generators. Section 3, the proposed technique has been discussed. In section 4 Experimental Results and final section 5 discuss about the conclusion.

2. Background Work

2.1 Least Significant Bit Insertion

Least significant bit (LSB) insertion is one of the technical approaches to embedding information in a cover image [3, 11]. In LSB insertion, information can be inserted in Chosen pixels.

Example:

The letter 'C' is an ASCII code of 67 (decimal), which is 1000011 in binary. It needs three consecutive pixels for a 72-bit image to store a 'C':

The pixels before the LSB insertion are:		
10000000	10100100	10110101
10110101	11110011	10110111
11100111	10110011	00110011
Then their values after the insertion of an 'C' w		
10000001	10100100	10110100
10110100	11110010	10110110
11100111	10110011	00110011

After modifying the LSB bits in pixels, results are not completely different small modification was done. Modifications are not identified by the human eye, because pixel values are minutely changed. Then the secret image bits are successfully hidden in the cover image. The Sender sends the stego image to the receiver then the destination station can starts getting the secret message bits from the stego image. And then combined all secret message bits secret message will form receiver can able to read the secret message.

2.2 CNOT Gate

CNOT gate is also called as Controlled not gate [7]. It comes under quantum computer. It is essential for constructing a quantum computer. Inside the CNOT gate, first qbit is control bit and the second bit is a target bit [7].

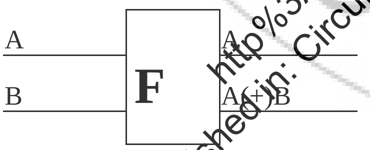


Figure: CNOT gate

Where, A be the control qbit, B be the target qbit, and (+) represents as EXOR. The truth table for CNOT gate is shown below. CNOT gate is completely different from the EX - OR gate. The EX-OR gate is irreversible gate, then the CNOT gate is reversible gate [7].

Wavelet Transformation:
Wavelet compressions are two types lossless or lossy. In lossless compression, the original data can be reconstructed from the compressed data, but in lossy compression the partial data can be reconstructed. Using wavelet transformation the data can be stored in less space, By doing so the memory space will be reduced and the data can be transferred easily [4]. Steps in wavelet compression: Load the image, perform wavelet decomposition of the image, and compress using fixed threshold.

Random Number Generators:
Blum Blum Shub generator is the pseudo random number generator. By using this random numbers are generated. The formula has shown below [6],

$X_{i+1}= (X_i)^2 \bmod n$ Where, X_i is the seed, and n be the range.

The pseudo random bit generator is used for generating random numbers in cryptography. Seed, two large prime numbers, and the range is the inputs for the pseudo random bit generators. The mathematical formulae has shown below, $X_{i+1} = (PX_i+Q) \bmod n$ Where P, Q are two large prime numbers, X_i is the seed n be the range.

3. Proposed Technique

3.1 Encryption Algorithm

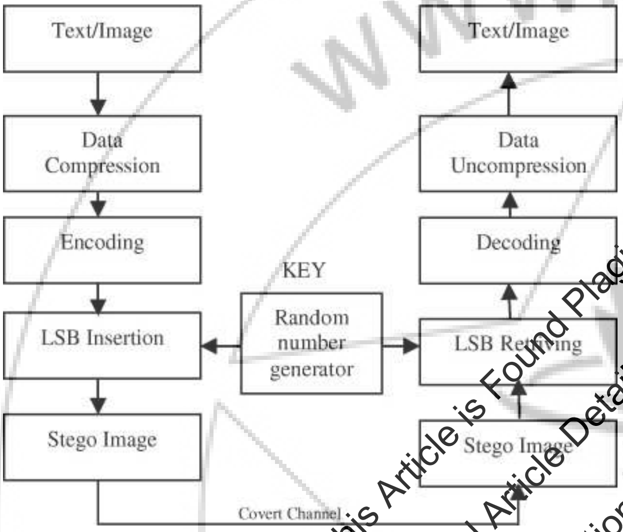
In this paper the secret information that can be in any form like text, image etc. is compressed by wavelet transform. The compressed text is now converted into its corresponding ASCII value, further the ASCII is converted into its 8-bit binary value. By using Control NOT gate, we are encoding the 8-bit binary value. Now these bits are ready to embedded into an image using LSB insertion.

The encrypted message is ready to be embedded in the cover image. Before embedding the message, the image is now converted into its corresponding pixel values. These values are arranged in the r x c matrix form, r and c represent rows and columns respectively. The bit of the secret information has to be embedded in the random positions in the cover image. To identify the random positions, Random number generators places a vital role. Random numbers act like a key in this technique. Blum Blum shub generator and Pseudo random number generator are used to select the random rows and columns respectively. Random numbers are generated by the generator, using the key (seed). Randomness will be varying from generator to generator. The randomness is achieved by padding the bits in the sequence. After selecting the random positions in the image (pixel values) now the secret message is embedded in the corresponding bits using the LSB insertion technique. After performing the above process the cover image is now converted into stego image in which the secret information has been embedded, along with the stego image the sender will send the key (seed) using some secure key exchange techniques.

3.2 Decryption Process

Decryption is the repeal process of the encryption process. After receiving the stego image, the receiver will convert the image into its corresponding pixels (matrix form). With the help of Key (seed) the receiver will be generating the random number using the random generators to identify in which positions the bits have been embedded. After getting the pixel positions, applying reverse LSB insertion technique will give the encoded bits. Applying the Control NOT gates on the encoded bits, the compressed text is retrieved. By applying wavelet, transformation technique (decompression) the original secret information is retrieved.

Proposed Technique Flow chart:



4. Experimental Results

In the above technique which we have discussed is implemented for different images and passwords, messages. For better quality of encryption, maximum large prime numbers should be chosen. The message has been compressed using a wavelet transform technique by using CNOT gate data is encoded and then embedded into the cover image using LSB insertion. The above process has been performed on the below images.

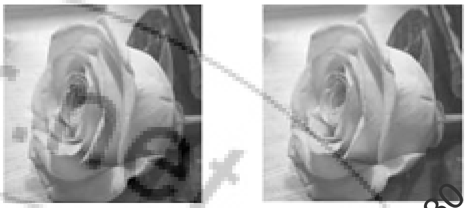


Figure: The left hand side figure shows cover image and right hand shows stego image.

We can compare the above cover image and stego image based on the histograms [2] by using MATLAB

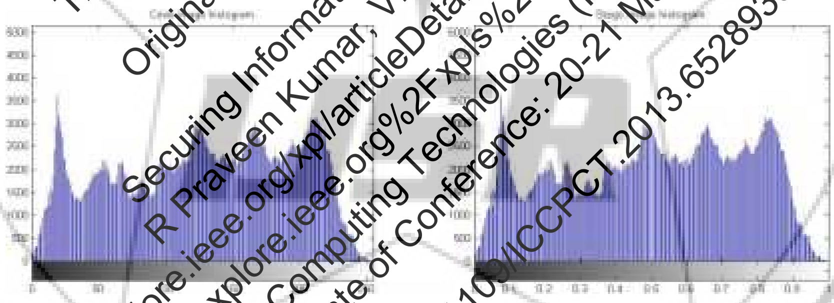


Figure: The left hand side figure shows an input image histogram and the right hand side image shows stego image histogram. The variations are very less comparing both cover and stego image histograms.

There are no changes between cover image histogram and stego image histogram. The very minute changes are identified. Here the resultant correlation coefficient for the above cover image and stego image is 0.9981

5. Conclusion

Using LSB technique, embedding huge amount of secret information in not possible. The basic idea of this paper is to embedded huge amount of secret information using LSB technique. To achieve this first the secret information is compressed using wavelet transforms. After compression the bits are encoded using a reversible quantum gate. LSB is one of the best techniques when compared to transformation techniques, because it reduces lots of noise distortion. In cryptography, the intruder can know the existence of the message transferring. By doing this process huge amount of information can be communicated in the covert channel and even the existence of the message is difficult to identify.

Equalize the length of your columns on the last page. If you are using *Word*, proceed as follows: Insert/Break/Continuous.

References

[1] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography”, IEEE Security and Privacy1(3) pp. 32-44,2003
[2] R. C. Gonzalez and R. E. Woods, “Digital Image Processing”, 2nd edition, Prentice Hall, Inc, 2002
[3] Venkatraman.S. Aiith Abraham. Marcin Paprzvcki. *“Significance of Steganography on Data Security”*, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC

04), ISBN: 0-7695-2108-8, IEEE 2004.

[4] Ivan W. Selesnick "Wavelet Transforms A Quick Study", Physics Today magazine, October, 2007.

[5] S. Song, J. Zhang, X. Liao, J. Du and O. Wen, "A *Novel Secure Communication Protocol Combining Steganography and Cryptography"*, Elsevier Inc, Advanced in Control Engineering and Information Science, Vol. 15, pp. 2767 - 2772, 2011.

[6] "Blum Blum Shub", From Wikipedia, http://en.wikipedia.org/wiki/Blum_Blum_Shub

[7]"Controlled NOT gate", From Wikipedia, http://en,wikipedia.org/wiki/Controlled_NOT _gate.

[8] P. Marwaha and P. Marwaha, "*Visual Cryptographic Steganography in Images*", in Proc. ICCCNT, 2010, pp. 1-6.

[9] S. Song, J. Zhang, *X*. Liao, J. Du and Q. Wen, "A *Novel Secure Communication Protocol Combining Steganography and Cryptography"*, Elsevier Inc, Advanced in Control Engineering and Information Science, Vol. 15, pp. 2767 - 2772, 2011.

[10] Changder. S.Ghosh. D and Debnath. N.C, "LCS based text steganography through Indian Languages", in Proc. ICCSIT 2010, pp. 53-57.

[11] Juneja. M, Sandhu. P.S, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption" , ARTCom 2009, pp 302-305.

Author Profile

M Venkteswara Reddy received B.Tech in electronics & communication engineering from Guntur engineering college, Guntur, AP in 2012 and present pursuing M.Tech in communication and signal processing in LITAM, JNTUK, AP, INDIA.

M Lakshman Naik received M.Tech in computer Science and engineering from JNTU Kakinada, and B.Tech in Electronics and communication engineering from V.R .Siddhartha Engineering College,Vijayawada,AP.Present he is working as assistant professor in ECE Dept in LITAM,JNTUK,AP.