International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Review of Designing Secured Data Using a Combination of LZW Compression, RSA Encryption, and DCT Steganography

Sayli S. Relekar[1], V. B. Raskar[2]

[1]Pune University, Department of ENTC ICOER, Wagholi Pune, Maharashtra India

[2] Professor, Pune University, Department of ENTC ICOER, Wagholi Pune, Maharashtra India

Abstract: ***Now a days the use of internet has been increased very much. Confidential data is been exchange over internet and various media file are also been exchange over internet. To keep these confidential data and media file secure over internet, then the cryptography and steganography technique are used to secure the data. So in this paper we are use various cryptography technique and steganography technique. Cryptography technique is use to encrypt the data. Steganography technique is use to hide the data within the selected image. . For that, we first substitute the original message by using the fourteen square substitution algorithms. After the substitution of text, we then encrypt this text message using RSA algorithm. The encrypted message compressed by JPEG 2000 (Huffman coding) method, so it will reduce the size of the message that will be inserted and increase the capacity of messages that can be inserted. Messages that have been compressed and encrypted, is then hidden by DWT (Discrete Wavelet Transform) techniques. With the incorporation of encryption techniques, steganography, and compression, the acquired information is more secure and its capacity is larger. At the receivers end, same operations are performed to decrypt the original message in reverse order. It is found that here we are using the double ciphering techniques which makes the system very robust and secures it from known hacking attacks. It makes very difficult for the intruders to hack the image and then decrypt the message in a feasible amount of time thus securing it from many known network attacks.***

Keywords: Encryption, steganography, cryptography, compression technique, RSA

1. Introduction

The use of internet has been increase day by day. Everyone can accesses from any part of the world. Internet is mostly used for exchanging the data. The data can be of type of the file such audio, video, image or a document type. Some of them sends a confidential data over internet. But while sending the confidential data the sender should know whether the data is secured or not. Otherwise the data will be hack by the hacker or it may be destroy. There are various technique use to secure the data over internet. These technique are cryptography and steganography.

Cryptography and steganography plays an important role in the network security. Cryptography is use to encrypt data. Steganography is use to hide the data into image, video or in any multimedia file. Using such a technique the data is secured and transfer over internet without getting misplace or hack.

Cryptography is a science and study of secret writing. It is synonymous to the encryption technique. In cryptography data is been encrypted. And this encrypted data is known as the secret key. So the cryptography is called as the secret encryption or secret writing. The process of converting the plaintext into ciphertext is called as the encryption. And same in the reverse order converting ciphertext into plaintext is called as decryption.

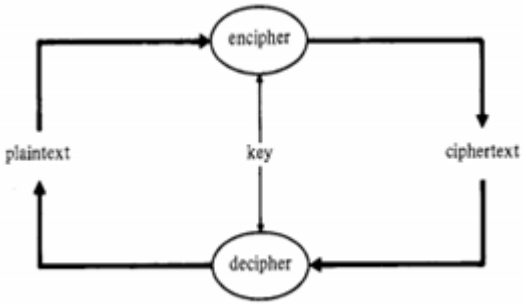

Figure 1: Cryptography process

Steganography is know as the invisible communication. The steganography techniques conceal the information in such as image, audio and video. The main aim of the steganography is to conceal the information between the sender and the receiver. The content is use to embed the information is called as the cover object. In this project the color image is taken to hide the information. The secret information and the stego key are embedded in the color image and hence we get the stego image. This stego image is unnoticeable to the hacker whether the secret information is hiden the image or not.

Figure 2: Steganography model

There are various research conducted on cryptography and steganography technique. But every research has some kind of draw back. To overcome these drawbacks we are just defined and implemented some technique. The least significant bit is used to hide the data. But only the least significant is not sufficient to hide the data or information. In the least significant bit the data is hide bit by bit. Only the use least significant bit (LSB) may not fully hide the data because while sending the data the image get some noise added to the image the data hide in that will get distorted and the data will also get distorted.

The discrete wavelength transform is also used for data hiding. Discrete wavelength transform is a steganography technique for embedding the message. Discrete wavelength transform is done within the frequency domain. In this two operation are perform horizontal and vertical operation. The horizontal operation scan from left to right and then perform sum and difference. The sum pixel are store at the top of the image and difference pixel are store at the bottom.

The 12 square algorithm consist of 12 square. These consist of the alphabet number. The alphabet consist upper case and lower case. But the alphabet P and Q are absent in the square. The alphabet P and Q does not encrypt so it remain as it is. So to overcome these drawback.

2. Literature Survey

Gandharba Swain, Saroj Kumar Lenka, [1] "Steganography using the Twelve Square Substitution Cipher and Index Variable",IEEE transactions on Image Processing, 2011, pp. 84-88. In this paper twelve square algorithm is present where first six square content the alphabet and remain six square content number and special charter. It encrypt the content small and capital alphabet, digit , number and special charter. The square matrix consist of 5 by 5 row and column.

In twelve square algorithm first six square content alphabets. In these six square twenty five alphabets are arranged. Square 1 content twenty five alphabet. In square 2 is same as the square 1 only first row is shifted to the last in square 2. Square 3 is same as the square 2 only the first row of square 2 is shifted to the last in the square 3. Similarly square 4 and square 5 are arrange.

Square-1	Square-2	Square-3
a b c d e f g h i j k l m n o p r s t u v w x y z	f g h i j k l m n o p r s t u v w x y z a b c d e	k l m n o p r s t u v w x y z a b c d e f g h i j
Square-4	**Square-5**	**Square-6**
g m r i t a b c d e f h j k l n o p s u v w x y z	a b c d e f h j k l g m r i t n o p s u v w x y z	a b c d e f h j k l n o p s u v w x y z g m r i t

Figure 3: plain text and cipher text of alphabet

Square 6 onwards the squares consist of the number and special charters. Square 6 content six rows and seven column. Square 7 is same as the square 6 in this the first row of the square 6 is shifted to the last. Similarly to the square 8 and square 9 are arranged. Square 10 is created from the square 7 by arranging the rows into column. Square 11 is same as the square 10 the first row is shifted to the third row of the square 11. And similarly the square 12 is arrange.

Square-7	Square-8	Square-9
0 1 2 3 4 5 6 7 8 9 ' ~ ! @ # $ % ^ & * ( ) _ - + = { [}] ; : " ' \ | < , > . ? / 0 1 2 3 4 5 6	7 8 9 ' ~ ! @ # $ % ^ & * ( ) _ - + = { [}] ; : " ' \ | < , > . ? / 0 1 2 3 4 5 6 7 8 9 ' ~ ! @	# $ % ^ & * ( ) _ - + = { [}] ; : " ' \ | < , > . ? / 0 1 2 3 4 5 6 7 8 9 ' ~ ! @
Square-10	**Square-11**	**Square-12**
0 6 ! & + ; < 1 7 @ * = : , 2 8 # ({ " > 3 9 $) [' . 4 ` % _ } \ ? 5 ~ ^ -] | /	1 7 @ * = : , 2 8 # ({ " > 0 6 ! & + ; < 3 9 $) [' . 4 ` % _ } \ ? 5 ~ ^ -] | /	1 7 @ * = : , 2 8 # ({ " > 3 9 $) [' . 4 ` % _ } \ ? 5 ~ ^ -] | / 0 6 ! & + ; <

Figure 4: plain text and cipher text of numbers and special character

Saleh Saraireh.[2] "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013. In this paper the secure communication is done using cryptography and steganography and transmitted secret information over non secure channel. In this paper the filter banks are used for high speed and level security. Embedding process is done using discrete wavelet transform. There four main stages encryption, decryption, embedding and extraction. Algorithm: (Embedding process)

Begin
1. Message
2. Encrypting Message
3. Implementation of DWT
4. Embedding process
5. Stego image
6. Extracting the message
7. Encrypting the message
8. Decrypting the message
9. Original message

End

The encryption and decryption process are same but only the process is vis versa. In the encryption and decryption process the filter banks are used. It consist of the two layers. First layer diffusion layer, it represent the analysis filter for high diffusion rate. Second is the substitution layer, it represent the lifting scheme.

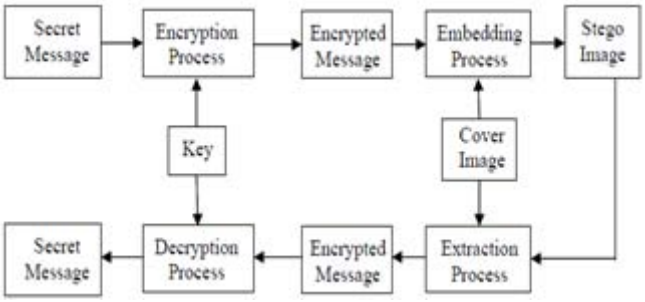

Figure 4: encryption and decryption process

Embedding is based on the discrete wavelet transform. This discrete wavelet transform is use to hide message using Haar wavelet. This transform is use to convert the spatial domain into frequency domain. In this the cover image is divided into four sub images that is approximate coefficient, vertical coefficient, horizontal coefficient and diagonal coefficient.

The extraction process is use to retrieve the original message to the receiver. It extract the stego image to retrieve the original message.

Geeta Kasana , Kulbir Singh [3] "Steganography Technique for JPEG2000 Compressed Images Using Histogram in Wavelet Domain" Vol.8, No.6 (2014). In this paper the steganography technique JPEG 2000 compressed image which provide the high embedding capacity and good visual quality of the stego image. JPEG 2000 is based on the wavelet transform for compression standard.

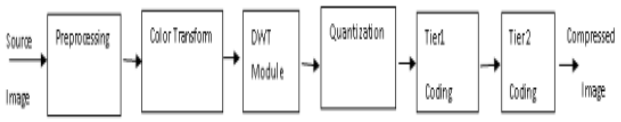

Figure 5: JPEG2000 encoder

The figure shows the JPEG2000 encoding process. First pre-processing is process on the source image for JPEG2000 encoder. The pre processing is use to tilling and shifting of the pixel image. Shifting is use for the high compression. Then the irreversible and reversible transform takes place on the pre process image to get the transformed image. After the transform is applied the lossy or lossless wavelet transform is applied to get the wavelet subband. If it is lossy compression then CDF 9/7 wavelet filters are used. And if it is the lossless compression is required then LeGall 5/3 wavelet filters are used. The quantization is performed on the discrete wavelet transform coefficients of a subband to decrease their precision.

Quantization is present only in lossy compression . Quantized wavelet coefficients are divided into two code blocks that is Tier-1. The tier-1 coding is performed on the code blocks. Each code block is passes through three different encoding passes which are significant propagation pass, refinement pass and cleanup pass. Tire-2 performs the post compression rate distortion optimization coding. It is use to discard the output of Tier-1. If the number of bytes in the tire-1 are more than it required bytes in the bit stream. Then these compressed bit stream is converted into packets. Then these packets are combined to produce the compressed image in JPEG2000 format.

This project we are hiding the text massage in the color image using the encryption technique. In this we are taking the color image in that we are going to hide the text massage. The encryption of this text is first process by the 14 square algorithm. And after encrypting by 14 square algorithm we are again encrypting by the RSA encryption technique. In this project we are dual encryption is done for higher level of security. After encryption process we are going to compression technique, which is JPEG2000 compression, in this the size of the image is compress.

3. Conclusions

Here we have seen the literature survey of papers. To overcome these drawback we are implementing compression technique and encryption technique. The compression technique is use to increase the capacity compress data. The encryption is is use to increase the security level and also increase the efficiency.

Reference

[1] Gandharba Swain, Saroj Kumar Lenka, "Steganography using the Twelve Square Substitution Cipher and Index Variable",IEEE transactions on Image Processing, 2011.
[2] Saleh Saraireh. "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.
[3] Geeta Kasana , Kulbir Singh "Steganography Technique for JPEG2000 Compressed Images Using Histogram in Wavelet Domain" Vol.8, No.6 (2014).

Author Profile

Mrs. Sayli S. Relekar has Completed B.E in Electronics and Tele-Communication in Savitribai Phule Womens College of Engineering, Aurangabad and pursuing ME in ICOER JSPM Wagholi, Pune.

Prof.V. B. Raskar, Professor in ICOER JSPM Wagholi, Pune.