AN ASSESSMENT ON THE DIFFERENT RECENT STEGANOGRAPHY METHODS

V.ARUNKUMAR[1], Dr. K. PADMANABAN[2]
[1]RESEARCH SCHOLAR, PERIYAR UNIVERSITY, SALEM, TAMILNADU, INDIA
[2]PRINCIPAL, VIVEKANANDHA COLLEGE FOR WOMEN, UNJANAI, TIRUCHENGODE, TAMILNADU, INDIA

ABSTRACT

The security for information is a real challenge when a large unit of data is transmitting the internet. The message can be send with top level security using Cryptography and Steganography. By the Cryptography, as the data can secured with cipher key for encryption and by the Steganography, the encrypted data can hide with another data such as images, Videos, Audios or Protocols. In this paper, take a survey about various techniques using for Steganography such as LSB (Least Significant Bits) and MSB (Most Significant Bits). But LSB is mostly used rather than MSB. Current trends of Steganography, we have used more techniques such as Retransmission Steganography (RSTEG), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Singular Value Decomposition (SVD) techniques for image Steganography. This survey paper is giving a platform for the beginners in steganography.

KEYWORDS-Steganography, Cryptography, DCT, DWT, LWT, SVD

1. INTRODUCTION

The main concept of this paper is to be sending the information with high security from one node to another node using internet. It cannot limit by geographical area. Steganography is very useful but high risk is related with secure the information during the transmission in the Internet. The information without secure, the hacker on the net can hack our information. The hacker can also misuse our personal information on the internet. Some hacker can destroy our information before reach our destination either can be corrupted them. So, nowadays, we are in need of protection of our information. The Steganography and Cryptography are giving the security to our data.

The word steganography is gotten from the Greek words steganos (which means covered up or secured) and the Greek root diagram (which means to compose).Definition of steganography from the Collins English Dictionary is the act of covering messages so that just the sender and the beneficiary realize that there is a message. In steganography, we can hide the information within an image or an audio file or a Video file. It is also possible to protect the information using Cryptography to encrypt our information. The main objective of both Steganography and Cryptography is fetching our information to destination without any loss. Good technology (difficult to detect hidden information) and sufficient data potential (efficiency of hidden information) are two properties which should be taken by all the steganography techniques.

This overview performed on different steganography systems which are exceptionally valuable for giving better assurance to data with some of cryptography strategies and some different methods, for example, LSB, MSB, RSTEG, DCT, DWT, LWT.

2.0 TYPES OF STEGANOGRAPHY

The Types of steganography is as follows

- Text steganography
- Image steganography
- Audio steganography
- Video Steganography

2.1 TEXT STEGANOGRAPHY

Content steganography can be accomplished by adjusting the content organizing, or by modifying certain qualities of literary components (e.g., Characters).

2.2 IMAGE STEGANOGRAPHY

The messages can convey into an Image. The most well known spread articles utilized in steganography is the Images.

2.3 AUDIO STEGANOGRAPHY

In sound steganography, incognito message is connected sound flag which result slight changing of double movement of the related sound document.

2.3 VIDEO STEGANOGRAPHY

In Video steganography, secret message is dug in into video flag which result minor fluctuating of paired movement of the related video record.

3.0 STEGANOGRAPHY TECHNIQUES

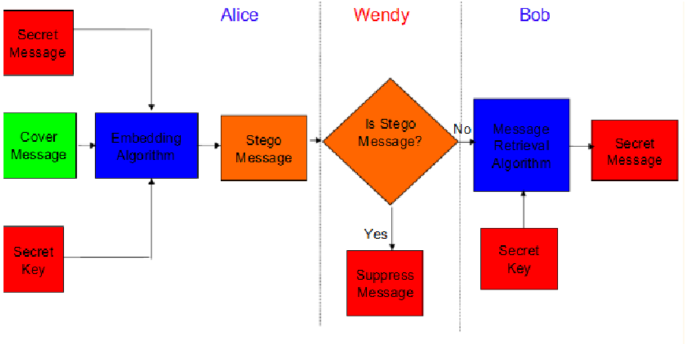


Fig 3.1 Steganography Techniques

4.0 LSB (LEAST SIGNIFICANT BITS)

The LSB is the Lowest Significant Bit in the byte estimation of the picture pixel. The LSB based picture steganography installs the incognito at all huge bits of pixel estimations of the spread picture. While applying LSB strategies to each byte of a 24 bit picture, three bits can be encoded into each pixel.

If the LSB of the pixel value of cover image C(i,j) is equal to the message bit SM of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding Procedure is given below:

$S(i,j) = C(i,j) - 1$, if $LSB(C(i,j)) = 1$ and $SM = 0$

$S(i,j) = C(i,j) + 1$, if $LSB(C(i,j)) = 0$ and $SM = 1$

$S(I,j) = C(i,j)$, if $LSB(C(i,j)) = SM$

Where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and “SM” is the next message bit to be Embedded. S(i,j) is the stego image.

4.1 DATA EMBEDDING ALGORITHM

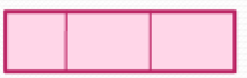
Step 1: Extract the pixels of the cover image.
Step 2: Extract the characters of the text le.
Step 3: Extract the characters from the Stego key.
Step 4: Choose first pixel and pick characters of the Stego key and place it in first component of pixel.
Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.
Step 6: Insert characters of text le in each RST component of next pixels by replacing it.
Step 7: Repeat step 6 till all the characters has been embedded.

4.2 DATA EXTRACTION ALGORITHM

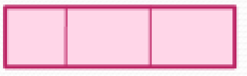
Step 1: Extract the pixels of the stego image.
Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.
Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.
Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.
Step 6: Extract secret message.

4.3 EXAMPLE:

We can use images to hide things if we replace the last bit of every color's byte with a bit from the message.



Message A-01000001
Image with 3 pixels
Pixel 01: 11111000 11001001 00000011
Pixel 02: 11111000 11001001 00000011
Pixel 03: 11111000 11001001 00000011
Now we hide our message in the image.
Our Message: 01000001
Pixel 01: 1111100**0** 1100100**1** 0000001**0**
Pixel 02: 1111100**0** 1100100**0** 0000001**0**
Pixel 03: 1111100**0** 1100100**1** 00000011
New Image:



5.0 RETRANSMISSION STEGANOGRAPHY (RSTEG)

The new steganographic strategy called RSTEG (Retransmission Steganography), which is proposed for a wide class of conventions that abuses retransmission instruments. The fundamental target of Retransmission Steganography is to not recognize an effectively gotten bundle. Since, purposefully summon retransmission. At that point, the retransmitted bundle conveys a steganography document rather than genuine information in the payload field. RSTEG is exhibited in the wide setting of system steganography, and the use of RSTEG for TCP (transmission control protocol) retransmission components is portrayed in detail.

Reproduction results are additionally given the principle point of estimating and looking at the steganographic data transfer capacity of the proposed technique for various TCP retransmission instruments, just as to decide the impact of RSTEG on the system retransmission level.

6.0 TRANSFORM DOMAIN TECHNIQUES

It is more dynamic against a range of attacks such as cropping, density, etc as it uses the important region of the cover image to hide the information. There are number of transform domain concepts such as DCT, DWT etc.

6.1 DCT (DISCREET COSINE TRANSFORMS)

DCT (Discreet Cosine Transforms) is mathematical transformation. DCT obtains a signal and transforms it from spatial domain to frequency domain. The JEPG images compressed using DCT coefficients. The image separates into differing importance parts. It transforms a signal or image from spatial domain to frequency domain. It can separate the image into high, middle and low frequency components.

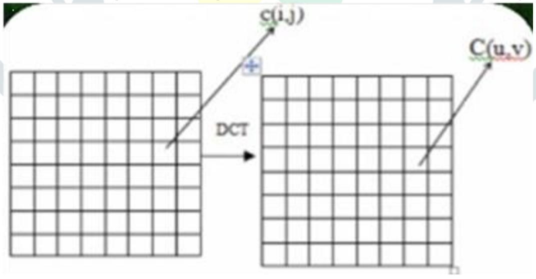


Fig 5.1 Discreet Cosine Transforms of an image

6.2 DWT (DISCRETE WAVELET TRANSFORM)

Wavelets are scientific capacities for picture pressure and advanced flag preparing. Utilized in the JPEG2000 standard. Wavelets are preferred for higher pressure levels over the DCT technique. By and large wavelets are increasingly hearty and are a decent method for concealing information. Wavelets are utilized to store the "detail" in pictures. They store the high recurrence data while the low recurrence data is put away independently. This takes into consideration high pressure as the detail is never lost but the low recurrence picture parts can be packed persistently. Same strategies as utilized with DCT amid the quantized advance.

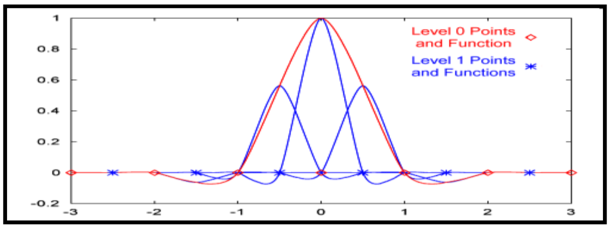


Fig 5.2 Discreet Wavelet Transforms of an image

7.0 CHARACTERISTICS OF STEGANOGRAPHY

A steganography system, in general, is expected to meet three key requirements, explicitly, imperceptibility of Embedding, exact recuperation of embedded information, and Payload (Payload is the bits that get delivered to the end user at the destination). An successful steganographic proposal should have the following preferred characteristics.

Secrecy: A person should not be able to extort the covert data from the host medium without the knowledge of the appropriate secret key used in the extracting procedure.
***Imperceptibility*:** The medium after being embedded with the secret data should be imperceptible from the original medium. One should not become apprehensive of the existence of the secret data within the medium.
High capacity: The maximum length of the secret message that can be embedded should be as long as possible
***Resistance*:** The secret data should be competent to endure when the host medium has been maneuver.
Accurate extraction: The extraction of the secret data from the medium should be perfect and consistent.

8.0 CONCLUSION

The steganography and Cryptography are using to protect our information during transmission over the internet. This survey shows various types of Steganography and the techniques what are using in the image steganography.

9.0 REFERENCES

[1] Jayaram.P, Ranganatha.H.R, Anupama.H.S, "Data Hiding Using Audio Steganography – A Survey" in The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[2] Mrs. Kavitha.M, Kavita.Kadam, Ashwini.Koshti, Priya.Dunghav "Steganography Using Least Significant Bit Algorithm" International Journal of Engineering Research &Applications (IJERA) ISSN: 22489622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012,

[3] Pratap Chandra Mandal Modern "Steganographic technique: A survey" in International Journal of Computer Science & Engineering Technology (IJCSET).

[4] Sheelu, Babita Ahuja "An Overview of Steganography" in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 1 (May. - Jun. 2013), PP 15-19

[5] K. B. Rajaa, C. R. Chowdari, K. R. Venugobal, and L. M. Patnaik, "A secure image steganography using LSB, DWT and Compression techniques on raw images" Intelligent 14-17 Dec. 2005.

[6] Implementation of LSB Steganography and its Evaluation for Various File Formats. Int. J. Advanced Networking and Applications 868.