IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. III (Jan. 2014), PP 70-73
www.iosrjournals.org

A Survey Paper on Steganalysis F5 Algorithm

Sneha Mehta[1], Amit Maru[2], Pravesh Kumar Goel[3]
[1](*Computer Science & Engineering Department, B. H. Gardi college of engineering and technology, Rajkot, India)*
[2](*Assistant Professor in Computer Science & Engineering Department, B. H. Gardi college of engineering and technology, Rajkot, India)*
[3](*Assistant Professor in Information Technology Department, B. H. Gardi college of engineering and technology, Rajkot, India)*

Abstract: *Steganography is a technique which used for securing the secret information from the illegal activity. Steganalysis is technique of finding the hidden text from the stego image. A Steganalysis based on the DCT value of the image is proposed in this paper. Steganography F5 algorithm is greater secure than other algorithm. In this paper survey on Steganalysis algorithm for attacking on F5 steganography algorithm is presented. When embedding rate is decreased from 10% to 5% then its accuracy is decreased that needs to improve and also need to decrease the processing time for that algorithm. Proposed techniques also discussed in this paper.*

Keywords: *Digital image, information hiding, Steganalysis, Steganography, f5, histogram, dct.*

I. INTRODUCTION

The Cryptography is used for protecting information security from illegal activity by making message illegible. But in cryptography the data which exist is not hidden. Steganography refers to the technique of hiding data in media (audio, image, video) in order to keep secret (hide) the existence of the information. Steganography hide the data which is existing to be observed. The media which contain with and without information are called the stego image and cover image [1].

Images are the digital media which is widely used and exchanged through the internet. Images are the best cover media to hide secret information inside. Secret information bits are inserted in an area of the cover file (image) that is not to be observed by an eye. Steganography communication system consists of an algorithm for embedding and an extraction. To provide a secret message, the original image is slightly modified by the embedding algorithm. Through which, the stego-image is acquire [4].

Steganography can be used for both illegal and legal purpose. Civilians may use it for protecting privacy while terrorists may use it for spreading terrorism [1]. It is new technique for establishing a secure communication [2]. In past null cipher technique is used as a Steganography communication. But in that method simple algorithm is used for the data transfer. Steganalysis, from an opponent's perspective, is an art of detecting stego image and avoiding from innocent ones. In first step it is need to determine whether a message is hidden within the image. Then find the type of Steganography algorithm used for producing the secret image. Then estimating the length of the message and then try to estimate the message is hidden behind the stego image. This paper will try to give survey on current Steganalysis algorithm [2]. Also discussed proposed work and also given some implementation part (histogram of image).

II. RELATED WORK

There are no of algorithm discussed in paper [2] which gives idea in detail regarding Steganography and Steganalysis. Such as 1) LSB algorithm: It works by replacing the LSBs of randomly selected pixels in the original (cover) image with the secret message bits [1, 5]. 2) F5: The F5 algorithm embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to hide a message of certain length. In the embedding process, the message length and the number of non-zero AC coefficients are used to determine the best matrix embedding that minimizes the number of modifications of the cover image [3, 4]. 3) Outguess: Firstly, OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0's and 1's. After embedding, corrections are made to the coefficients, which are not selected during embedding, to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be detected by chi-square attack [1]. 4) JSteg/JPHide: JSteg embeds secret information into a cover image by successively replacing the LSBs of non-zero quantized DCT coefficients with secret message bits. Unlike JSteg, the quantized DCT coefficients that will be used to hide secret message bits in JPHide are selected at random by a pseudo-random number generator, which may be controlled by a key. Moreover, JPHide modifies not only the LSBs of the selected

coefficients; it can also switch to a mode where the bits of the second least significant bit-plane are modified Steganalysis [1].

First step of Steganalysis is to find the image, which is stego image or cover image. Then after try to find the information is whether hidden behind the cover image or not. Next step is to find the true length of the hidden information behind the image. And at last if possible then try to what information is hidden within the cover image [1]. Different types of algorithm are used for the Steganalysis purpose such as Attack on LSB algorithm, Attack on F5 algorithm, Attack on outguess algorithm, Attack on JSteg/JP Hide algorithm[1].

2.1F5 Steganography algorithm

Step 1: Input one RGB color cover-image.
Step 2: Calculate 2D DCT value of 8*8 image blocks.
Step 3: Apply quantization to DCT coefficients in each block of the image. The quality factor Q is used to build quantization table.
Step 4: Capture a password from the user as a seed to generate random embedding positions in a DCT block (8 x 8).
Step 5: Choose available coefficients to hide messages.
Step 6: Implement entropy coding algorithm.
Step 7: Save the stego-image in JPEG format with a given Q.[7]

2.2 F5 Steganalysis Algorithm

F5 Steganalysis attack is mainly used for estimating the true message length. Some of the characteristics of the histogram of DCT coefficients, like the symmetry and monotonicity are retain by the F5 Steganography algorithm. But the F5 Steganography algorithm modifies the shape of the histogram of DCT coefficients. This drawback of the Steganography algorithm is used for the Steganalysis attack.

The procedure for the Steganalysis algorithm (procedure for getting the cover image from stego image). First the stego image is decompressed to spatial domain. After that this decompressed image is cropped by 4 columns from all sides and then re-compressed it using the same quantization parameters as that of the stego image. Before the re-compressed operation a (blurring operation) low pass filter is applied (as a preprocessing step) to remove possible jpeg blocking artifacts from the cropped image. Then the resulting DCT coefficients will provide the estimation of the cover image histograms. Then the probability of none zero AC coefficient being modified, denoted by β, may be estimated by the least square approximation minimizing the square error between the stego image histograms.

Steps for the F5 Steganalysis algorithm [3][4][6].

Step 1: Input the stego image for performing Steganalysis.
Step 2: Decompressed the stego image.
Step 3: Crop the image by 4x4 column from all sides.
Step 4: Apply blurring operation to remove artifacts.
Step 5: Then re- compressed the image.
Step 6: Count the different histogram value for the stego image and cover image.
Step 7: Calculate the difference
Difference = stego image value – cover image value.

III. PROPOSED WORK

As discussed above in related work following is my proposed method which can be implemented to increase the detection rate.

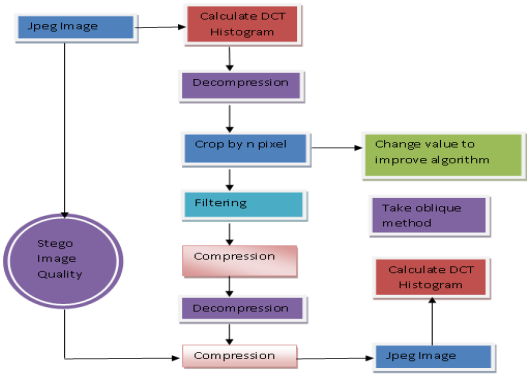

Fig.1: flow of proposed work

In already implemented algorithm the detection rate decrease as the embedding rate is decrease from 10% to 5% so in proposed work try to decrease this problem though using oblique method in place of the column wise cropping method.

Another problem need to solve is the processing time is much for applying Steganalysis attack on the F5 steganography this need to decrease in proposed work.

Steps for the proposed Steganalysis algorithm

Step 1: Input the stego image for performing Steganalysis.
Step 2: Decompressed the stego image.
Step 3: Crop image by N x N columns from all sides.
Oblique method will be used to crop the image
Step 4: Apply blurring operation to remove artifacts.
Step 5: Then re- compressed the image.
Step 6: Count the different histogram value for the stego image and cover image.
Step 7: Calculate the difference.

IV. ANALYSIS

By using above proposed algorithm detection rate can be increased and processing time can be decreased. As per [8] following rates are there.

Table 1: comparison for different detection rate

Embedding Rate (%)	Detection Rate (%) SHDFT
100	96.42
78	89.87
5	86.78

As per the table contents when embedding rate is 100%, detection rate will be 96.42. This rate can be increased by above proposed algorithm. Let us take one example, suppose your input image is as shown in given below:

Fig. 2: input image

Histogram of above input image is given below:

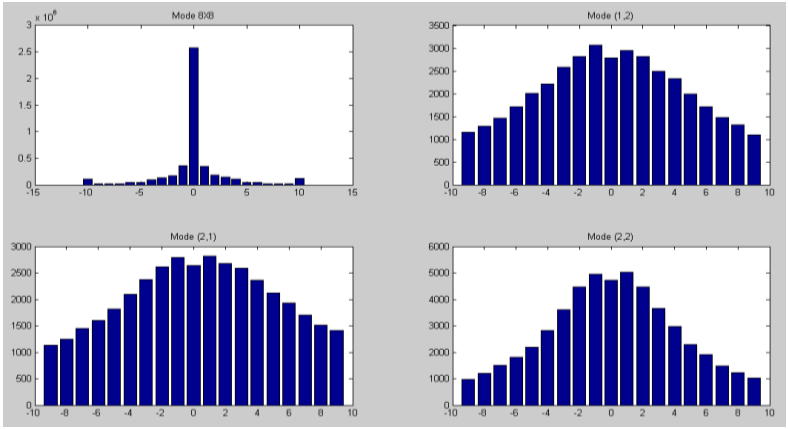

Fig. 3: a) the histogram values of all 8X8 AC DCT coefficients. b) The histogram values of the frequency [1,2] DCT coefficients. c) The histogram values of the frequency [2, 2] DCT coefficients. d) The histogram values of the frequency [2, 1] DCT coefficients.

V. CONCLUSION

Steganalysis F5 algorithm is mainly used for detecting the secret information hidden by the steganography f5 algorithm. When the steganography F5 algorithm is applied on the image at that time the statics of the image is changed, based on that Steganalysis F5 algorithm is applied to take the DCT and histogram analysis of the cover image and stego image and compare them based on that we can find the image is stego or not. In Future the implementation of F5 algorithm will be done. When embedding rate is decreased from 10% to 5% then its accuracy is decreased that needs to improve and also need to decrease the processing time for that algorithm. Steganalysis F5 algorithm will be implemented using re-implementation of image instead of double compression.

REFERENCES

[1] Bin LiA , Junhui He, Jiwu Huang, Yun Qing Shi "A Survey on Image Steganography and Steganalysis"Journal of Information Hiding and Multimedia Signal Processing Volume 2, Number 2, April 2011.

[2] Hatim aboalsamh, hassan mathkour, sami dokheekh, mona mursi, ghazyas- sassa "An Improved Steganalysis Approach for Breaking the F5 Algorithm "WSEAS TRANSACTIONS on COMPUTERS , Issue 9, Volume 7, September 2008,pp1447-1456.

[3] Mingwei TANG, Mingyu FAN, Wen SONG, YajunDU "A steganalysis of information hiding for f5" Journal of Computational Information Systems6:vol 1(2010) pp. 55-62.

[4] Jessica Fridrich, Miroslav Goljan, Dorin Hogea "Steganalysis of JPEG Images: Breaking the F5 Algorithm" Springer Berlin Heidelberg , volume 8 ,2003, pp 310-323.

[5] Mohit Kr. Srivastava , Sharad Kr. Gupta, Sushil Kushwaha, Brishket S. Tripathi "Steganalysis Of Lsb Insertion Method In Uncommpressed Images Using Matlab" Available online from: http://www.tutorialspoint.com/white-papers/124.pdf.

[6] Briffa, Johann A. "Has F5 Really Been Broken?" Crime Detection and Prevention (ICDP 2009), 3rd International Conference (IEEE) , volume 1, 3-3 Dec. 2009 ,pp.1 – 5.

[7] Hatim aboalsamh, hassan mathkour, sami dokheekh, mona mursi, ghazyas- sassa "An Improved Steganalysis Approach for Breaking the F5 Algorithm "WSEAS TRANSACTIONS on COMPUTERS , Issue 9, Volume 7, September 2008,pp1447-1456.

[8] T. H. Manjula Devi, H.S.Manjunatha Reddy, K. B. Raja,Venugopal K. R, and L. M. Patnaik "Detecting original image using histogram, dft and svm"International Journal of Recent Trends in Engineering Vol. 1, No. 1, May 2009,. 367-371.