A Technique For Audio Steganography

Charandeep Singh Bedi, Ramandeep kaur
Assistant Professor, Computer Department, Baba Farid college of Engineering & Tech, Punjab, India
Student, Computer Department, Baba Farid college of Engineering & Tech, Punjab, India

***ggAbstract*—Steganography and steganalysis received a great deal of attention from media and law enforcement. Many powerful and robust methods of steganography and steganalysis have been developed. In this paper we are considering the methods of steganalysis that are to be used for this processes. Paper giving some idea about the steganalysis and its method.**

***Keywords*— Steganography, Steganalysis, Audio, Fuzzy, N-Queen**

Introduction

Steganography is a technique of information security that hides secret information within a normal carrier media. The most widely used carrier media's are digital image, audio and video, etc. An unauthorized way of detecting and extracting the hidden secret information from stego is known as steganalysis. If any steganalysis algorithm can detect the presence of hidden message in a carrier then the steganography algorithm is considered to be broken. It has been assumpted that if the feature is visible it becomes possible to attack the hidden data. Thus the goal of the steganography here is always to conceal the existence of the hidden data.

Steganography can be used in a large amount of data formats. The most popular data formats are .bmp, .doc, .gif, .jpg, .mp3, .txt and .wav. Steganography tools make use of these data format because of their popularity on the internet and their ease of use. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message[3].

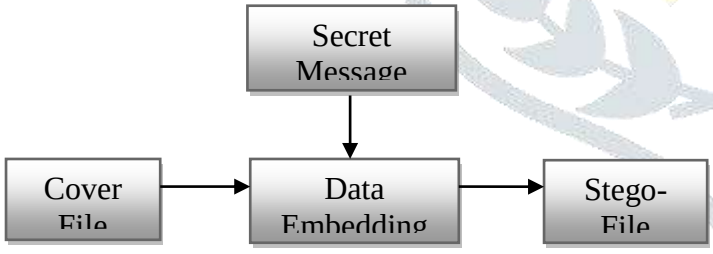


Figure 1 : Steganography Block Diagram

Steganography has various useful applications. However, it can be used for ill intentions like any other science. It has been found as a forefront of security techniques that are used currently by the remarkable growth in computational power, the awareness of increase in security, e.g., individuals, agencies, government, groups and through various intellectual pursuit. The ultimate objectives of steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. These are the main factors that distinguished it from related techniques like watermarking and cryptography. This research work involves the review and analysis of the different existing methodology used in steganography along with some common standards and guidelines drawn from the literature

I. Related Work

Much work has been done on steganalyzing LSB steganography in the initial stage of the development of steganalysis. Many steganalytic methods toward LSB steganography have been proved most successful, such as Chi-square statistical attack [2], RS analysis, sample pair analysis (SPA) analysis, weighted stego (WS) analysis, and structural steganalysis etc.

Many other steganalytic techniques [1] have been proposed in recent years. Some steganalytic methods, for example, the Chi-square attack, are effective to LSB steganography for spatial images as well as JPEG images. The fact that LSB steganography is vulnerable to attack implies that high imperceptivity does not guarantee a high security level. The first ever statistical steganalysis was proposed by Westfeld and Pfitzmann [3]. There approach is specific to LSB embedding and is based on powerful first order statistical analysis. It identifies Pairs of Values (POVs) that consist of pixel values, quantized DCT coefficients or palette indices which get mapped to one another on LSB flipping. After the message embedding, the total number of occurrence of two members of certain POV remains the same. This concept of pair wise dependencies is leads to design a statistical Chi-square test to detect the hidden messages [4]. A technique in grayscale images is proposed by Zhang and Ping [5].This technique uses different image histogram as the statistical analysis tool. Measure of the weak correlation between the LSB plane and the rest of the planes is done by the translation coefficients between different image histograms. This algorithm can identify the existence of secret messages embedded using sequential or random LSB replacement in images and also can estimate the amount of secret messages. This algorithm shows a better performance and computation speed than RS analysis method. Benton and Chu [6] proposed a soft computing approach to steganalysis specific to LSB. Decision trees and neural networks are used independently for detection purpose. The features are extracted from images which are based on the variables for estimating the embedding probability in the RS method. This approach different from original RS method. The goal of this method is to decide whether the image contains hidden data but not to estimate the embedding probability. Xiang-dong Chen, et al. [7] a proposed a steganalysis technique based on bit plane randomness tests. Two binary sequences are obtained by scanning the 7_{th} and 8_{th} bit planes of the image with Hilbert scan. The randomness of these two sequences is tested individually by 14 kinds of randomness tests. The results of these tests form a vector and are used to construct a SVM classifier to distinguish stego images from the clean ones. In [8] , Andrew D. Ker , proposed steganalysis methods for extensions of least-significant bit overwriting to both of the two lowest bit planes in digital images.There are two distinct embedding paradigms. He investigates how detectors for standard LSB replacement can be tailored to such embedding, and how the methods of "structural steganalysis",

that gives the most responsive detectors for standard LSB replacement, He also compares the detectability of standard LSB embedding with the two methods of embedding in the lower two bit planes. In paper [9], they described a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. By inspecting the differences in the number of regular and singular groups for the LSB and the "shifted LSB plane", we can reliably detect messages as short as 0.03bpp. In a image, neighbor pixels have a high cross correlation. This is also true for LSB planes of close pixels. Inserting random bits using LSB method alleviates naturally the said correlations. Based on these feature, a method is proposed in [10] to detect LSB stego images by using 2-D autocorrelation coefficients of image. Since matrix of autocorrelation is symmetric, just some of its coefficients are used. These features are applied for classifying the stego image and natural image .The results show that this new method has a high performance, and is more effective than other methods. Jan Kodovský et al. [11], constructed a new quantitative steganalyzers for steganographic techniques which hide data using LSB embedding in quantized DCT coefficients of a JPEG file. They have explored two approaches: change-rate estimation using the maximum likelihood principle with a pre cover model and a heuristic approach based on minimizing a penalty functional obtained from a combined analysis of the embedding operation and properties of natural images. The techniques are applied to Jsteg and its modified version called symmetric Jsteg. Experiments are used to compare the new methods with current state of the art. **H.B.Kekre et al.** [12], proposesd a steganalysis technique for both grayscale and color images. Feature vectors derived from gray level co-occurrence matrix (GLCM) in spatial domain, which is sensitive to data embedding process has been used. Difference between the features of stego and non-stego images is used for steganalysis. Distance measures like Absolute distance and Euclidean distance are used for classification. Experimental results demonstrate that the proposed scheme outperforms the existing steganalysis techniques in attacking LSB steganographic schemes applied to spatial domain. LSB matching steganalysis method detects the existence of secret messages embedded by LSB matching steganography in digital media.LSB matching may be modeled in the context of additive noise independent of the cover image. The result of additive noise steganography to the image histogram is alike to a convolution of the histogram of the cover image and stego-noise PMF. LSB matching more difficult and hard to detect as compared to simple LSB replacement. This study presents a survey of LSB matching steganalysis for digital image. Andew D. Ker et al. proposed a steganalysis technique for LSB matching in [13]. The technique works for grayscale images. It was observed that the down sampling operation affects the center of mass of the HCF of stego image and this variation was used as the discriminator. These techniques produced reliable detectors for LSB matching in grayscale images. But the embedded message length highly affects the results. Q. Liu et al. [14] proposed a scheme for steganalysis of LSB matching steganography .It is based on feature extraction and pattern recognition techniques. The correlation features are extracted for color images.Statistical pattern recognition algorithms are applied to train and classify the feature sets. This scheme is highly efficient for colour images and reasonably efficient for grayscale images. In paper [15] Fangjun Huang, proposes a new technique for attacking the LSB matching based steganography. The least two or more significant bit-planes of the cover image will be changed during the embedding in LSB matching steganography .So the pairs of values do not exist in stego image. In the proposed method, they got an image by combining the least two significant bit-planes and divide it into 3×3 overlapped sub images. The sub images are grouped into four types. Embedding a random sequence by LSB matching and then calculating the alteration rate of the number of elements, they found that the alteration rate is higher in cover image than in the corresponding stego image. Experimental results show that the proposed algorithm is competent to detect the LSB matching stegonagraphy on uncompressed gray scale images. In [16], they expand the LSB matching image steganography and proposed an edge adaptive scheme which can choose the embedding regions according to the size of covert message and the difference between two consecutive pixels in the cover image.The results show that the new scheme can enhance the security significantly compared with typical LSB-based approaches while maintainning higher visual quality of stego images at the same time. Zhihua XIA et al. presented the detection of spatial domain least significant bit (LSB) matching steganography in gray images [17]. Three features, which are based on image histogram, neighborhood degree histogram and run-length histogram, are extracted first. Then, support vector machine is utilized to learn and distinguish the difference of features between cover and stego images. Experimental results show that the proposed method gives reliable detection ability and outperforms the two previous state-of-the-art methods.

II. PROBLEM FORMULATION

Steganography is a technique which leads to hiding content of one format to another or within the same format. In case of an image steganography, a lot of work has been done in the same context. The techniques have been proved to a revolutionary step in the field of data hiding. As the technology advances, the need to increase the complexity of hiding the data also increases. We also need to enhance the security of the base image (refers to the image in which we are hiding the data), so that if the image gets hacked the hacker is not able to detect that some data has been hidden into the base image just by looking at the image. To achieve the same, a lot of previous algorithms have been proposed like DWT, DCT and so many other algorithms. This gives rise to our problem statement. Our problem statement involves applying hybrid cryptography techniques by making use of RSA, AES and Blowfish algorithm on secret data and applying hop-field neural network on cover image and quantized image is generated The encrypted data is then embedded in this quantized image by using Least Significant Bit (LSB) and n-queen problem embedding in such a way that the Image quality which is measured in terms of PSNR increases and the data remains safe within the image.

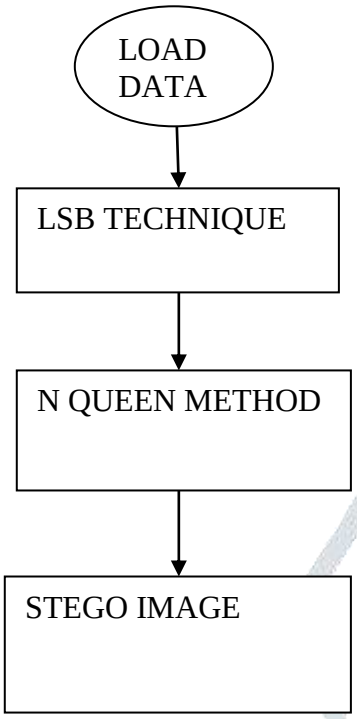
III. METHODOLOGY

In order to achieve the set goals, our proposed work aims at developing a better technique for Image Steganography that will maintain the high level of security, robustness and undetectability of hidden messages. In this proposed work steganography is combined with cryptography and implemented in MATLAB.

The proposed work is divided into two steps:

i) Encryption and embedding of the secret data

ii) Extraction and decryption of the secret data.



i)Embedding: The resulting image is used to hide the encrypted secret data by using the Least significant Bit embedding technique. After embedding, a stego- image is generated which contains the secret data in encrypted form.

Step 1: The image of any format is taken. It can be .jpg, .bmp, .png. It acts as a cover image.

Step 2: In this step, the cover image is quantized by using DCT. In the quantized image, it become easy to find the filled and vacant location within the image so that it become easy to embed the data.

Step 3: In this step, the secret encrypted data is embedded behind the quantized cover image by using Least Significant Bit and n-queen problem.

Step 4: The Stego- image is created as the result of embedding.

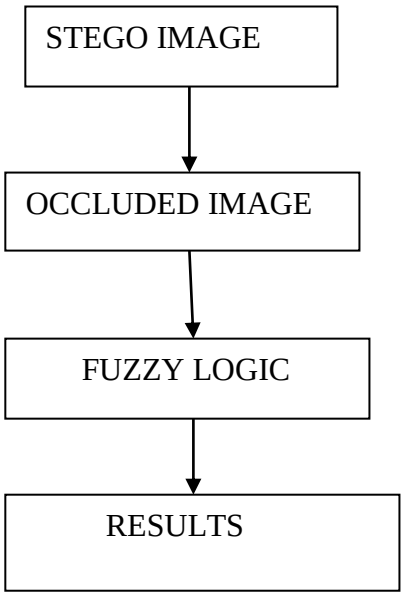


Figure 3: Flow Diagram Of Embedding

Extraction and decryption: During extraction, the secret data is extracted from the stego-image. As the extracted data is in encrypted form. So, decryption is done for getting the original hidden data. All the algorithms are executed in reversed order to get the original data.

Step 1: In this step, the encrypted embedded data is extracted from the Stego- image using the inverse LSB+(n-queen) techniques.

Step 2: in this step, the extracted encrypted message is decrypted using RSA and AES in reverse order.

Step 3: In this step, the original secret message is created after the execution of step 2.

As discussed above any type of image formats can be used in work. We have taken the following images as cover images viz. Lena, tulip, cameraman and babara.

Figure 4: Results

Figure 4 is the resultant window which is generated after the embedding of the message image into cover image.

IV. COMPARATIVE TABLE FOR DIFFERENT IMAGES

This table states that five various parameters measure the efficacy of the occluded image and size of image is constant and occlusion vary from 10%, 20%, 30%, 40% and 50%.

PSNR	MSE	CON.	SPCC	SSIM
28.1013	5.0931	.031315	.23726	1.0921
28.7334	5.0992	.030626	.23729	1.0923
36.7289	5.0998	.023959	.22757	1.0937
37.3004	5.6812	.023592	.21298	1.0939
44.813	5.9578	.19635	.20309	1.0954

V. CONCLUSION

We performed the research work on different types of images. These images are used as a cover image in which the secret data is embedded. Any image format or extensions can be used here. But mostly used extensions in this research work are .jpg, .png, .bmp. Stego – image for all these image format

are generated. The effectiveness of the research work depends upon the various paramaters used for measuring the quality of stego-image. These parameters are PSNR, MSE, Capacit. The experimentally calculated parameter of PSNR for different images are observed and compared with the existing techniques. It has been found the PSNR value of stego- image of our research work shows the better results in comparison with other existing steganography techniques viz. Image steganography based on join LSB and n-queen technique and Image steganography based on RSA encryption.

Moreover , in our research work the PSNR value for all the stego images shows the much better result then the existing techniques used for Image Steganography. Hence, the satisfactory security result can be maintained because it become impractical for the unauthorized used to detect the presence of hidden data behind the image.

We overall concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages . Neural Network has been found effective enough to find pixels to merge the data bits without much affecting the original pattern of the image. It has been also concluded that if we can encrypt the data up to some level before merging it to the image, it may enhance the chances of security into the image embedding.

Although the results are quite satisfactory but there is always a hope of improvement in the current work .Our current approach opens up a lot of premises of development for the future users of Neural Logics. The current work does not contain the noisy image. Future research workers can get to see how the current scheme goes with different levels of noise. The effect of different types of noise may also put some different effect on the approach. Also some other methods of Neural Network can be also tried.

VI. REFERENCES

[1] Bin Li, 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 ,pp.142-172

[2] Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal, " A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," Journal of Global Research in Computer Science, Volume 2, No. 4, April 2011,pp.1-15.

[3] A. Westfeld, A.Pfitzmann, " Attacks on steganographic systems," Proc. of Information Hiding, Third Int. Workshop, Dresden, Germany, September 28–October 1, 1999, pp. 61–75.

[4] N.F. Johnson, S. Jajodia, "Steganalys of images created using current steganography software, in: Lecture Notes in Computer Science," vol. 1525, Springer-Verlag, Berlin, 1998, pp. 273–289.

[5] T. Zhang, X. Ping, "Reliable detection of LSB steganography based on difference image histogram," in: Proc. ICASSP, vol. I, 2003, pp. 545–548.

[6] Ryan Benton, Henry Chu, "Soft computing approach to steganalysis of LSB embedding in digital images," in: 3rd Int. Conf. on Information Technology Research and Education, 27–30 June 2005, pp. 105–109.

[7] Xiang-dong Chen, "Detect LSB steganography with bit plane randomness tests," in: Proc. of 6th World Congress on Intelligent Control and Automation, China, June 21–23, 2006.

[8] Andrew D. Ker ," Steganalysis of Embedding in Two Least-Significant Bits , " Information Forensics and Security, IEEE Transactions on**,** Volume 2 **,** Issue 1, March 2007,pp.46 - 54

[9] Jessica Fridrich, Miroslav Goljan, Rui Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images"

[10] Arezoo Yadollahpour, Hossein Miar Naimi ,"Attack on LSB Steganography in Color and Grayscale Images Using Autocorrelation Coefficients," European Journal of Scientific Research ,ISSN 1450-216X Vol.31 No.2 © EuroJournals Publishing, Inc. 2009, pp.172-183

[11] Jan Kodovský, Jessica Fridrich, "Quantitative Steganalysis of LSB Embedding in JPEG Domain ," MM&Sec'10, September 9–10, 2010, Roma, Italy.

[12] H.B. Kekre, A.A. Athawale & S.A.Patki, " Steganalysis of LSB Embedded Images Using Gray Level Co- Occurrence Matrix," International Journal of Image Processing (IJIP), Volume 5 ,Issue 1: 2011

[13] A.D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett. 12 (6), June 2005,pp. 441–444.

[14] Qingzhong Liu, Andrew H. Sung, Jianyun Xu, Bernardete M. Ribeiro, Image complexity and feature extraction for steganalysis of LSB matching steganography," in: IEEE Int. Conf. on Pattern Recognition, vol. 2, 2006, pp. 267–270.

[15] Fangjun Huang, Bin Li, Jiwu Huang ,"ATTACK LSB MATCHING TEGANOGRAPHY BY COUNTING ALTERATION RATE OF THE NUMBER OF NEIGHBOURHOOD GRAY LEVELS," ©2007 IEEE I - 401 ICIP 2007

[16] Fangjun Huang, Jiwu Huang," Edge Adaptive Image Steganography Based on LSB Matching,"INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS, VOL. 5, NO. 2, JUNE 2010

[17] ZHIHUA XIA, ET AL.,"A LEARNING-BASED STEGANALYTIC METHOD AGAINST LSB ATCHING STEGANOGRAPHY RADIOENGINEERING," VOL. 20, NO. 1, APRIL 2011,pp102-109

[18] NOUHA KOBSI, HAYET FARIDA MEROUANI, "Neural Network Based Image Steganalysis: A Comparative Study",