چهارمین کنفرانس ماشین بینایی و پردازش تصویر ایران
۲۶-۲۵ بهمن ماه ۱۳۸۵

Image Steganalysis Based on Wavelet Transformation

S. B. Sadkhan
Babylon University – Iraq
drengsattar@yahoo.com

N. A. Abbas
Babylon University –Iraq
nidaa_muhsin@yahoo.com

Abstract: *Techniques for information hiding have become increasingly more sophisticated and widespread. Steganalysis has recently received a great deal of attention both from law enforcement and the media. Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information.*
This paper provides wavelet based approach for image Steganalysis. The detection scheme of the system can be separated in two parts. In the first part, extraction a set of statistics, called the feature vector, for the investigated image. The second part, using a classification algorithm to separate original images from stego images by means of their feature vectors.

Keywords: *Image steganalysis, Wavelet, Statistical parameters, steganography, information hiding*

1 Introduction

In today's digital world, much more versatile and practical covers for hiding messages digital documents, images, video, and audio files have replaced invisible ink and paper. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a "cover" to hide secret messages.
Information hiding is a recently developed technique in the information security field and has received significant attention from both industry and academia. There are two main branches for information hiding–steganography and digital watermarking. The main purpose of steganography is to convey messages secretly by concealing the very existence of messages, while digital watermarking is mainly used for copyright protection of electronic product [1].
There are many approaches to hiding the embedded file. The embedded image bits can be inserted in any order ***substitution*** replaces cover file bits with embedded file bits. Such substitution bits techniques will be more detectable than the replacement of others, a smart decision has to be made as to which bits would make the best candidates for substitution [3]. One of the more common approaches to substitution is to replace the least significant bits (LSBs) in the cover file. This approach is justified by the simple observation that changing the LSB results in the smallest change in the value of the byte [7].
The Discrete Cosine Transform (DCT) is the keystone for JPEG compression and it can be exploited for information hiding. For such technique, specific DCT coefficients are used as the basis of the embedded file hiding. The coefficients correspond to locations of equal values in the quantization table. The embedded file bit is encoded in the relative difference between the coefficients [4].
Other Steganographic techniques, including spread spectrum, statistical Steganography, distortion, and cover generation, are described in detail in [5].
Detection of Steganography, estimation of message length[6], and its extraction belong to the field of steganalysis. Steganalysis has recently received a great deal of attention both from law enforcement and the media. Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attacker may also embed counter information over the existing hidden information[11]. With digital images as carriers, the detection of the presence of hidden messages poses significant challenges. Although the presence of embedded messages is often imperceptible to the human eye, it may nevertheless disturb the statistics of an image[12].

Research in steganalysis is still in its infancy. The main reason for this is that in its full generality, steganalysis is an ill-posed problem: the original host data is unknown, the rate of hiding is unknown, and the number of steganography scheme is large. A review of the view currently available steganalysis tools is given in [10]. Unfortunately, even the most promising existing approaches, such as Stegdetect [12] and the supervised learning framework[8], have drawbacks that limit their practical use; which are: -

- Existing steganalysis methods are based on heuristics, and the given steganography method, there is no systematic approach for designing a steganalysis method.
- Every steganalysis method has some parameters to be chosen, which determine the performance of the method. Ideally, the test parameters should be chosen purely on the basis of the data to meet the required performance.
- Due to the lack of a theoretical foundation, it is not known how current steganalysis test compare with "optimum" test.

The aim of this paper is to provide wavelet based approach for image Steganalysis. The detection scheme of the system can be separated in two parts. In the first part, extraction a set of statistics, called the feature vector, for the investigated image. The second part, using a classification algorithm to separate original images from stego images by means of their feature vectors.

2 The Proposed System for Image Steganalysis

The Proposed System given in Figure 1 can be divided up to three parts as follows:-

(1). Stego Image Preprocessing
(2). Features Extraction and Analysis Processes
(3). Discrimination Processes

In our system, we considered the LSB steganography approach to be used in implementing the information hiding task, hence the input signal to our system is the suspected signal resulted from hiding process.

2.1 Stego Image Preprocessing

Preprocessing algorithm, techniques and operators are used to perform initial processing that makes the primary data reduction and analysis task easier. In our system it represent opening the suspected image that will be tested in the system as the input image. The images are saved as BMP format. *Generally,* Images come in different sizes and different Aspect ratio; therefore, we will scale the images into uniform size. Each image will be scaled to power of two (i.e. 48*48) so to put in a uniform size, and for both the suspected and the original image.

The data at the BMP file is stored as reverse sequence; we can notice them when viewing the BMP image it will appear from the bottom of the image. So reordering the data to make it appropriate to processing.

2.2 Feature Extraction and analysis Processes

Feature extraction refers to the process of forming a new set of features from the original and suspected features set, and find a mapping that reduces the dimensionality of pattern by extraction some numerical measurements from raw input pattern. There is no well-develop theory feature extraction; most is application oriented.

The extraction of feature vector are derived from the wavelet transformation process, For each suspected and original image, theses features are coefficients produced in this transformation and assumed to be fixed, do not changed after several image processing operation.

There are different types of wavelet transformations depending on the bases functions used in the transformation, in our work, Haar transformation is used to implement wavelet transformation. The Haar bases vectors are:- Lowpass : $\frac{1}{\sqrt{2}}[1,1]$,Highpass : $\frac{1}{\sqrt{2}}[1,-1]$.

Decompose a given image with 2-D wavelet transform into 4 images, as indicated in Figure 2.a the image is divided into four subbands after wavelet transform: horizontal, vertical, diagonal subimages, and low resolution subimages, which can be viewed as tree in Figure 2.b.

2.3 Discrimination Processes

After specifying the features vector by performing feature extraction and analysis, methods for comparing two features vectors need to be determined. These methods are either to measure the differences between the two or measure the similarity. These are the Statistical Tests.

3 Experimental Results and Discussion

This part concerned with experimental results for samples of images being tested (as discussed previously, several images are taken as shown

Figure 3, where these images have different sizes and type BMP with 24-BPP.The test is done on BMP cover image and BMP image as stego object in the LSB modification And a text file in the S-Tool . These BMP are 24 bits true color. Types of hiding were used LSB and S-Tool and adding a simple noise.

Firstly the system were tested with several samples, the images are Sandy bell that has a stego object using (LSB),Sandy bell2 has a stego object using (Stool) [9],Duck with no hidden information, drip with noise and some images with LSB, S-Tool ,clear …etc. Table 1 shows the result of the comparisons of several images.

In the first step Table 1 represent the statistical tests (AD, MSE, SNR, PSNR, NCC, CQ), these test are applied on different stego objects and the result are differ from image to image depending on the Steganography algorithm that used on insertion.

Then the Figure 4 shows the order statistics (Mean, Variance, Kurtosis, Skewness) for the Image Sandy that has hidden information using LSB modification .You can notice the differences between those two images. Where the statistics is little different and seems to be the same but when you focus you can notice it.

4 Conclusions

The following are some concluded remarks of the proposed system:-

1. Using statistical test is a good idea to detect the changing in image when original image is available.
2. The system needs to save only the features vectors that need only several kilobytes per image.
3. Using wavelet features give better results.

References

[1] Jacob T., Gregg H., Roger L., and Gary B., Blind Steganography Detection Using a Computational Immune System: A Work in Progress, International Journal of Digital Evidence Winter 2003, Issue 1, Volume 4.

[2] Roman T., Robert B., Johannes B. and Andre K., Steganographic System Based on Higher-Order Statistics, University of Erlanger-Nuremberg, Cauerstr. 7, D-91058, Erlanger, Germany.

[3] Johnson N., Duric Z. and Jajodia S., Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, Boston: Kluwer Academic Publishers, 2001.

[4] Fabien A., Ross J. and Markus G., Information Hiding – A Survey, Proceeding of the IEEE , Vol. 87, No. 7, July 1999.

[5] Katzenbeisser S. and Petitcolas F., Information Hiding Techniques for Steganography and Digital Watermarking. Boston: Artech House, 2000.

[6] Fridrich J. and Soukal D. and Goljan M., Maximum likelihood estimation of length of secret message embedded using ±K Steganography in spatial domain, SUNY Binghamton, Department of Electrical Engineering, Binghamton, NY 13902-6000,2004.

[7] Provos N., Defending Against Statistical Steganalysis, *10th USENIX Security Symposium*, Washington, DC, 2001.

[8] Farid H., Detecting Steganographic Messages in Digital Images, Department of Computer Science, Dartmouth College, Hanover NH 03755, 2001.

[9] Westfeld A. and Pfitzmann A., Attacks on Steganographic Systems - Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools - and Some Lessons Learned, *Lecture Notes in Computer Science*, 1768:61–75, 2000.

[10] Fridrich J. and Goljan M.," Practical Steganalysis of Digital Images – State of the Art ", in Proceeding of SPIE, 2002, vol. 4675.

[11] Dabeer O. , Sullivan K., and Madhow U., Detecting of Hiding in the Least Significant Bit, 2003 Conference on Information Science and Systems, The John Hopkins University, March 12-14, 2003.

[12] Provos N. and Honeyman P., Detecting steganographic content on the internet ISOC NDSS'02, San Diego, CA, 2002. see http://www.outguess.org/.

Table 1: comparison of several tested images in the proposed system

No.	*Image*	*Tests*	*R*	*G*	*B*
1	Sandy bell+ Sandy bell1	AD	0.00515	0.0055	0.0044
2	=	MSE	0.0205	0.02221	0.0178
3	=	SNR	1210115.2760	1576468.8434	2281166.91780
4	=	PSNR	6502.5333	6002.33843	7482.3670
5	=	NCC	0.999	0.9999	0.9999
6	=	CQ	212.8974	195.2398	213.5197
7	Sandy bell+ Sandy bell2	AD	2.88391	0.00299	0.00311
8	=	*MSE*	2.88391	0.00299	0.00311
9	=	*SNR*	8605264.1851	11710911.4081	13060798.8235
10	=	*PSNR*	46240.2368	44588.7997	42840.2193
11	=	*NCC*	0.99999	0.999999	0.9996467125979
12	=	*CQ*	212.9011	195.24367	213.5230
13	Guitar+ Guitar1	AD	0	10.2478	
14	=	*MSE*	0	513.30425	0
15	=	*SNR*	Overflow	overflow	overflow
16	=	*PSNR*	Division by zero	Division by zero	Division by zero
17	=	*NCC*	1	0.930604	1
18	=	*CQ*	163.6459	144.9521	148.2131

Appendix (I)

Mean = μ = $\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} I(i,\ j)$

Variance = $\sigma^2 = \frac{1}{MN}\sum_{j=0}^{N-1}\sum_{i=0}^{M-1}\left(I_{(i,j)} - m\right)^2$

Skewness = $\varsigma = \frac{1}{MN}\sum_{j=0}^{N-1}\sum_{i=0}^{M-1}\left(\frac{I_{(i,j)} - m}{s_x}\right)^3$

Kurtosis = $k = \frac{1}{MN}\sum_{j=0}^{N-1}\sum_{i=0}^{M-1}\left(\frac{I_{(i,j)} - m_x}{s_x}\right)^4$

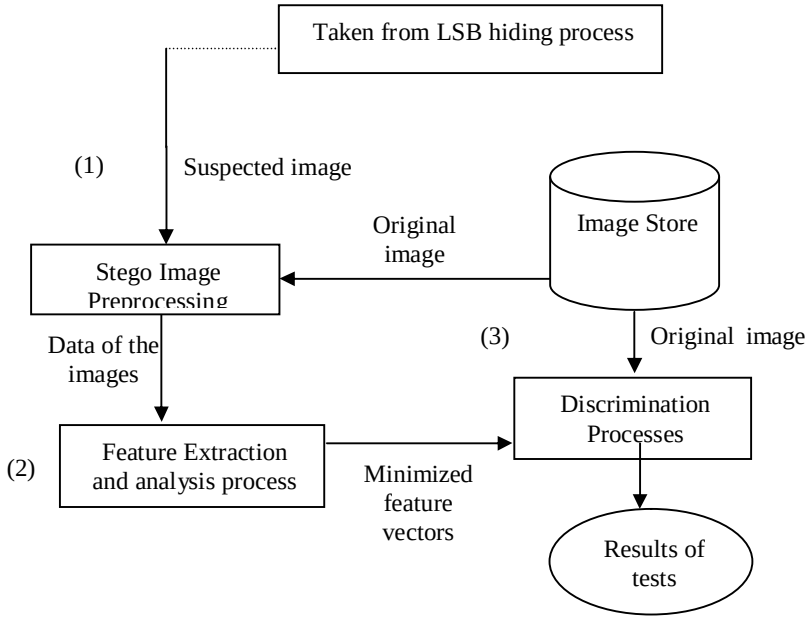

Figure 1: The overall Proposed System Model.

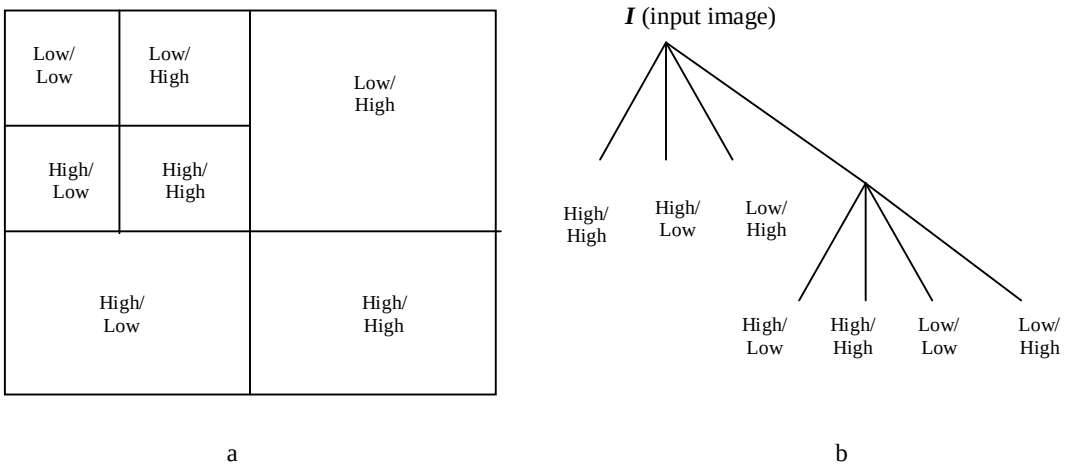

Figure 2: a. 2-D wavelet Transform, b. Tree presentation of 2-D wavelet Transform.

Figure 3: Set of images

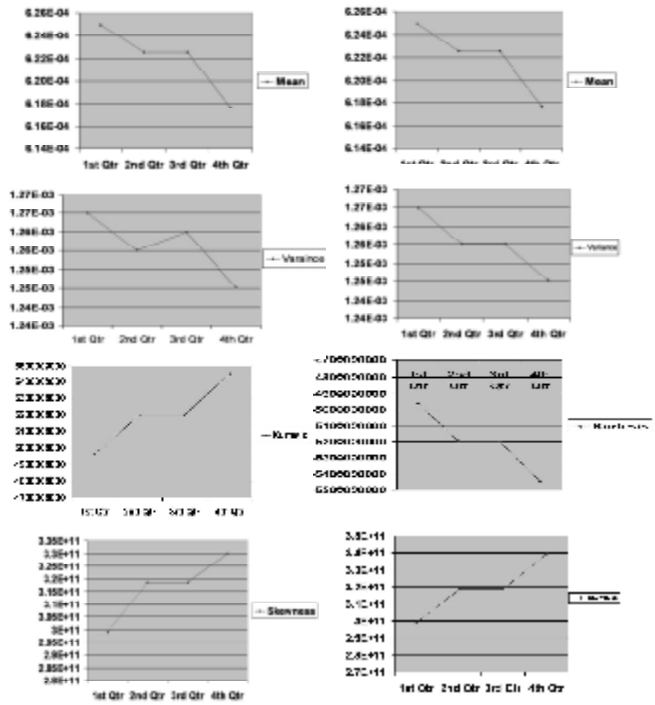

Figure 4: the order statistics