Steganalysis Using Wavelet Transform

Prof. Dr. Waleed A. Mahmud Al-Jouhar
University of Baghdad
Dr. Talib M. Jawad Abbas Al-Talib
University of Al-Nahrain
Hussam Juma'a Nayma Al-Bahadly
University of Baghdad

Abstract

Techniques and applications for information hiding have become increasingly more sophisticated and widespread. With high-resolution digital images as carriers, detecting the presence of hidden messages has also become considerably more difficult. It is sometimes possible, nevertheless, to detect (but not necessarily decipher) the presence of embedded messages. The basic approach taken here works by finding predictable higher-order statistics of "natural" images within a multi-scale decomposition, and then showing that embedded messages alter these statistics.

The decomposition of images using basis functions that are localized in spatial position, orientation, and scale (such as wavelets) has proven extremely useful in a range of applications. One reason for this is that such decompositions exhibit statistical regularities that can be exploited.

The proposed algorithm consist of three stages: Image feature extraction (IFE) stage, training stage, and testing stage. In IFE the image decomposes to four level wavelet. Set of statistics (mean, skewness, second set of statistics collected is based on the errors in an optimal linear predictor of coefficient magnitude. In this predictor, the subband coefficients are correlated to their spatial, orientation and scale neighbors.

The steganalysis technique was tested on samples of images processed with most commercial steganographic software products.

1. Introduction

Hiding information within electronic media requires alterations of the media properties that may introduce some form of the degradation or unusual characteristics. These characteristics may act as signatures that broadcast the existence of the embedded message, thus defeating the purpose of steganography [1].

Steganalysis is an area of study where ways of detecting and defeating steganography are examined. Discovering a hidden message is the first step in steganalysis and is considered an "attack" on the hidden information. There are many ways steganography can be attacked [2].

The broad goal of steganalysis is to understand the effects of hiding data into a medium. This knowledge is typically used to either strengthen the hiding system or detect the use of data hiding [1].

Attack against hidden information involve identifying patterns and characteristics the embedding processes have on the carries. From these characteristics, methods for attacking hidden information (steganalysis) are defined and executed. These attacks are used to document the break points of various tools for embedding information and to identify the limitations of steganography tools [3].

The detection of steganographic communication is a very important application of steganalysis. The loss of sensitive data, by both civilian and military entities is very undesirable. As steganography provides a means for covertly transferring information, it is especially well suited to an insider sneaking information out [4].

Recent years have seen many different steganalysis techniques will be proposed hereunder.

a. Some of earliest work in this regard was reported by **Johnson** and **Jajodia** [5]. They pointed out that steganographic methods for palette images that preprocess the palette before embedding are very vulnerable. Several steganographic programs create clusters of close palette colors that can be swapped for each other to embed message bits. These programs decrease the colors depth and then it to 256 by small perturbations to the colors. This preprocessing, however, will create suspicious pairs (clusters) of colors that can be easily detected.

b. Fridrich [6,7] introduced the dual statistics steganalytic method for detection of LSB embedding in uncompressed formats. For high quality images taken with a digital camera or a scanner, the dual statistics steganalysis indicates that the safe bit rate is less than 0.005 bits per sample, providing a surprisingly stringent upper bound on steganographic capacity of simple LSB embedding.

c. **Onkar D., Kenneth S., and Upamanyu M [8].** They apply the theory of hypothesis testing to the *steganalysis*, or detection of hidden data, in the least significant bit (LSB) of a host image. The hiding rate (if data is hidden) and host probability mass function (PMF) are unknown. Their main results are as follows: (1) Two types of tests are derived: a universal (over choices of host PMF) method that has certain asymptotic optimality properties and methods that are based on knowledge or estimation of the host PMF and, hence, an appropriate likelihood ratio (LR). (2) For a known host PMF, it is shown that the composite hypothesis-testing problem corresponding to an unknown hiding rate reduces to a worst-case simple hypothesis-testing problem. (3) Using the results for a known host PMF, practical tests based on the estimation of the host PMF are obtained. These are shown to be superior to the state of the art in terms of receiver operating characteristics as well as self-calibration across different host images. Estimators for the hiding rate are also developed.

d. **Mohammad Ali Bani Youns and Aman Jantan** [9]. They proposed a new steganography approach for data hiding. This approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Experimental results show that the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy have not changed, the method offers a good concealment for data in the encrypted image, and reduces the chance of the encrypted image being detected. The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after extracting it and hence the original image can be reproduced by the inverse of the transformation and encryption processes.

2. Propose Steganalysis Using Wavelet Transform

The techniques presented here are novel and to the best of our knowledge, the first attempt at designing general purpose tools that use wavelet decomposition for steganalysis. General detection techniques as applied to steganography have not been devised and methods beyond visual inspection and specific statistical tests for individual techniques are not present in the section one above. Since too many images have to be inspected visually to sense hidden messages, the development of a technique to automate the detection process will be very valuable to the steganalyst.

Our approach is based on the fact that the natural images have strong higher-order statistical regularities within wavelet decomposition. Hiding information in digital media requires alterations of these properties that introduce some form of degradation, no matter how small. These degradations can act as signatures that could be used to reveal the existence of a hidden message.

The proposed algorithm works with any type of images format like (GRAY SCALE, BMP and GIF file format). Using fisher linear discriminator (FLD) in the classifier enables us to train the algorithm with several type of steganogrphic algorithm. This feature makes us know not only if the image contain a secret message or not but also the type of the steganographic algorithm.

3. Steganalysis Algorithm Structure

The steganalysis algorithm contains two phases, training phase and testing phase. In both phases a vector, called feature vector of the image, in the image feature extraction stage, represents the image. The process is illustrated generally in Fig.(1) which shows the stages involved. Each stage will be discussed in the next sections.

In the image feature extractions stage, image statistics (mean, skewness and kurtosis) are calculated, and stored as a feature vector, for a large number of images use the wavelet transforms. The feature vectors of the training image are used in second stage to train the classifier , in this work FLD is used. Finally, to the test new image, determine its statistics as in the first stage and use the result of second stage to classify the image.

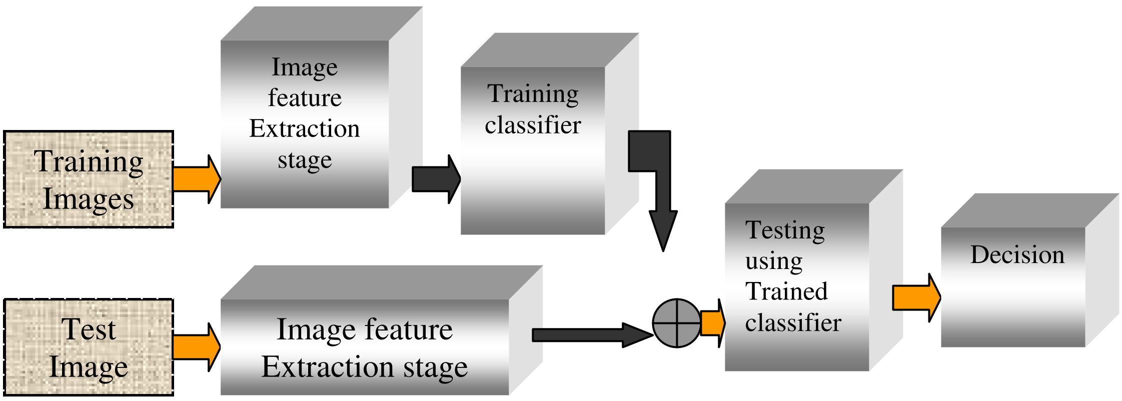

Figure (1): general block diagram to the steganalysis system

3.1 Image Feature Extraction

The decomposition of images using basis functions that are localized in spatial position, orientation, and scale as wavelets are found useful in the steganalysis application. One reason for this is that such decompositions exhibit statistical regularities that can be exploited. Fig.(2) describe the collection statistics set from this decomposition.

Given image decomposition, the statistical model is composed of, the mean, skewness and kurtosis of the subband coefficients at each orientation and at scales i = 1,…,(n-1) where n=4. These statistics characterize the basic coefficient distributions. The second set of statistics collected is based on the errors in an optimal linear predictor of coefficient magnitude.

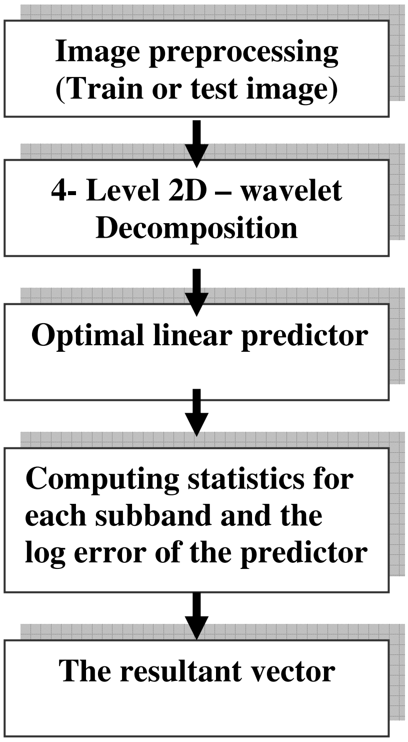

Figure (2): Main stages of image feature extraction

The details of implementation of these steps are given in the coming sub-section.

3.1.1 The Image Preprocessing Step

Image preprocessing is the first stage in the proposed algorithm in which a database of images is built for training and a part of it is for testing. The data used in the process are 200 images. 150 images are used for training and the rest 50 images are used in the testing. These images are collected through the following procedure. First image is compressed using Jsteg (with no stego message) to average size of 250 kb (quality 75). Next, convert the images from RGB to 8-bit grayscale (gray=0.299R+0.587G+0.114B) and convert them to a color pallet in another set. The above images are used as cover images to hide the given message. Each message consists of a central 256x256 portion of random selected image from the same database. Note that, two type of steganography are used which are S-Tool [10], LSB that uses wavelet transform[11]. As result four sets of images will be produced hence the images will be 200x4=800. Two of them contain host images, one set for grayscale images and the other for pallet images, the remaining two sets are classified as one for each type of steganographic algorithms given above (S-Tool and LSB that uses wavelet transform).

3.1.2 Wavelet Decomposition [12,13,14]

Wavelet coefficients are calculated following special algorithm introduced for purpose here. It is implemented to give strong higher-order statistical regularities and these statistics are significantly altered when a message is embedded with an image. It is tested across a broad range of natural images. The filters of the wavelet used here are a special

lowpass filter = [0.02807382 –0.060944743 -0.073386624 0.41472545 0.7973934 0.41472545 -0.73386224 -0.060944743 0.02807382]'. The highpass filter may be constructed from the lowpass filter by:

Step1: modulating (multiplying) by (-1)^n (equivalent to shifting by pi in the Fourier domain).

Step2: flipping (i.e., reversing the order of the taps).

Step3: spatially shifting by one sample.

To compute 2-D Discrete Wavelet Transform using QMF9 filters of NxN image matrix, the next step should be followed:

1. Checking image dimensions: Image matrix should be a square matrix, NxN matrix, where n must power of 2 (here is 512). So that the first step of the transform procedure is checking input image dimensions. If image is not a square matrix some operation must be done to the image like resizing the image or adding rows or columns of zeros to get a square matrix.
2. Constructing the filters: Use the QMF9 lowpass filter above and then compute the highpass filter using the same way described above.
3. Transformation of image columns: transformation of image columns can be done in two steps:

   i. Correlate the columns of the image with the lowpass filter coefficients moving [2 1] steps.

   ii. Correlate the columns of the image with the highpss filter coefficients moving [2 1] steps as another output.
4. Transformation of image rows: transformation of image rows can be done in four steps:

   i. Correlate the rows of the result in part (*i*) of step3 above with transpose lowpass filter coefficients moving [1 2] steps. This process gives the LoLo (approximation) subband.

   ii . Correlate the rows of the result in part (*i*) of step3 above with transpose highpass filter coefficients moving [1 2] steps. This process gives the LoHi (horizontal) subband.

   iii. Correlate the rows of the result in part (*ii*) of step3 above with transpose lowpass filter coefficients moving [1 2] steps. This process gives the HiLo (vertical) subband.

   iv. Correlate the rows of the result in part (*ii*) of step3 above with transpose highpass filter coefficients moving [1 2] steps. This process gives the HiHi (diagonal) subband.

5. The same process is applied to the LoLo subband to get second orientation and so on.

3.1.3 The Implemented Optimal Linear Predictor

There are relationships between the magnitudes of large-amplitudes coefficients. Large-magnitude coefficients tend to occur at neighboring spatial locations, and at the same relative spatial location of subbands at adjacent scales and orientations.

The coefficients magnitude of the implemented optimal linear predictor is calculated as a function of a subset of the potential conditioning neighbors. For purposes of illustration, consider first a vertical subband, $Vi(x,y)$, at scale i. A linear predictor for the magnitude of these coefficients in a subset of all possible neighbors is given by:

$$Vi(x,y) = w1Vi(x-1,y) + w2Vi(x+1,y) + w3Vi(x,y-1) + w4Vi(x,y+1) + w5Vi+1(xl2,yl2) + w6Di(x,y) \ldots \quad (1) + w7Di+1(xl2,yl2)$$

Where Wk denotes scalar weighting values. This linear relationship may be expressed more compactly in matrix form as:

$$\vec{V} = Q\vec{W} \quad \ldots\ldots.. (2)$$

Where the column vector $\vec{w} = (w1, w2, ..., w7)^T$, the vector $\vec{V}$ contains the coefficient magnitudes of $Vi(x,y)$ strung out into a column vector and the columns of the matrix Q contain the neighboring coefficient magnitudes also strung out into column vectors. The coefficients that minimize the squared error of the estimator are:

$$\vec{w} = (Q^T Q)^{-1} Q^T \vec{V} \quad \ldots\ldots\ldots. (3)$$

The log error in the linear predictor is then given by:

$$\vec{E}v = \log_2(V) - \log_2(|Q\vec{w}|) \ldots (4)$$

It is from this error that additional statistics are collected. This process is repeated for each vertical subband at scales i = 1,…,n-1, where at each scale a new linear predictor is estimated. A similar process is repeated for the horizontal and diagonal subbands. The linear predictor for the horizontal subbands is of the form:

$$Hi(x,y) = w1Hi(x-1,y) + w2Hi(x+1,y) + w3Hi(x,y-1) + w4Hi(x,y+1) + w5Hi+1(xl2,yl2) + w6Di(x,y) + w7Di+1(xl2,yl2) \ldots (5)$$

and for the diagonal subbands:

$$Di(x,y) = w1Di(x-1,y) + w2Di(x+1,y) + w3Di(x,y-1) + w4Di(x,y+1) + w5Di+1(xl2,yl2) + w6Hi(x,y) + w7Vi+1(x,y) \quad \text{……… (6)}$$

The same error metric, Equation (4), and error statistics computed for the vertical subbands, are computed for the horizontal and diagonal subbands, for 9(n-1) error statistics [15]

3.1.4 The Statistics Computation of The Image

Two sets of statistics has been collected to characterize the image, the first set is composed of, mean, skewness and kurtosis of the subband coefficients at each orientation and scales i=1, ---, n-1 (where n=4). The **first set** contains 9(n-1) coefficient statistics. The statistics are calculated by using the equations:

The mean calculates the sample average

$$\vec{\mu} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{………... (7)}$$

Where n is the number of samples of (x). The skewness of a distribution is defined as

$$y = \frac{E(x-\mu)^3}{\sigma^3} \quad \text{………… (8)}$$

Where μ the mean of is x, σ is the standard deviation of x, and $E(t)$ represents the expected value of the quantity t. The kurtosis of a distribution is defined as

$$k = \frac{E(x-\mu)^4}{\sigma^4} \quad \text{………. (9)}$$

Where the mean of is x, σ is the standard deviation of x, and $E(t)$ represents the expected value of the quantity t.

The **second set** of the statistics collected is based on the errors in the optimal linear predictor of coefficient magnitude, in other words the output of Eq.(4). The second set is the most important here because its depends on the higher order statistical regularities of the image in the multi-resolution decomposition. The same statistics mean, skewness and kurtosis are computed for each subbands error, which gives 9(n-1) error statistics. Combining these statistics with 9(n-1) coefficient statistics yields a total of 18(n-1) statistics that form a "feature" vector [16].

3.1.5 The Resultant Vector

The statistics are computed for each subband of, the wavelet decomposition and errors coefficient magnitude in the optimal linear predictor as shown in the previous step therefore they are needed to arrange in a vector form to be able to use them in the classifier stage. The length of it is 54-coefficient as shown in Fig.(3). This vector is named "feature" vector which is used to discriminate between images that contain hidden messages and that do not.

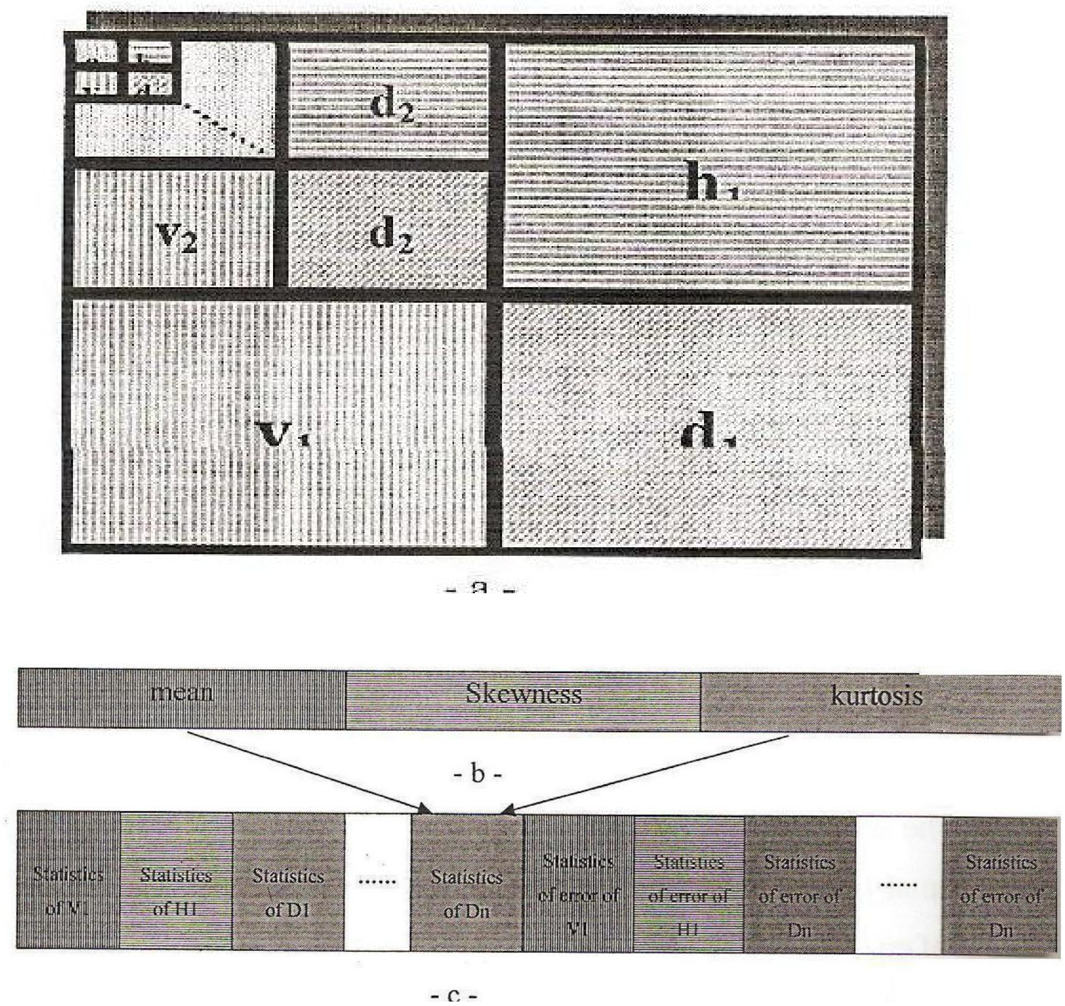

Fig (3): (a) N-Level 2D-DW representation of an image
(b) Statistics of each subband
(c) Feature vector form of image statistics

Algorithm 1: image feature extraction

Input: Image
Output: statistics coefficients "feature vector"

Step1: *Select the image.*
Step2: *Input the wavelet basis function.*
Step3: *Apply 4-level wavelet decomposition to the image.*
Step4: *Compute the statistics coefficient using the equations eq.(7),eq.(8),eq.(9).*
Step5: *Compute the log error of the optimal linear predictor for each subband using the eq.(1) to eq.(6).*
Step6: *Determine the error statistics using the equations eq.(7),eq.(8),eq.(9).*
Step7: *Arrange the total statistics into a vector form named feature vector as shown in fig.(3) which length is 54-statistics.*
Step8: *End.*

3.2 The Training Stage in The Proposed Algorithm

This stage uses image feature vectors of the training images sets of the host images set and stego images sets of all types of steganogrphic algorithms to learn the classifier algorithm and the training set contains 150 feature vectors for different images.

Fisher linear discriminator analysis (FLD) is a class specific method for pattern recognition [17]. The training images are required to pass through Fisher linear discriminator which is used to discriminate between two Fisher linear discriminator analysis (FLD) is class specific method different classes therefore training the algorithm must be separate for each type of steganographic algorithm. It starts after computing the feature vectors of the host images as the first set and stego images that have the same steganographic algorithm as the second set, this classifier is implemented through the following procedure:

Denote column vectors $\vec{x}_i$, i=1,…,N_x and $\vec{y}_j$, j=1,..,N_Y as exemplars from each of two classes from the training set. The within-class means are defined as:

$$\vec{\mu}_x = \frac{1}{N_x}\sum_{i=1}^{N_X}\vec{x}_i \quad \text{and} \quad \vec{\mu}_y = \frac{1}{N_y}\sum_{i=1}^{N_y}\vec{y}_i \qquad \text{……….(10)}$$

The between-class mean is defined as:

$$\vec{\mu} = \frac{1}{N_x+N_y}\left(\sum_{i=1}^{N_x}\vec{x}_i + \sum_{j=1}^{N_y}\vec{y}_j\right) \qquad \text{……….(11)}$$

The within-class scatter matrix is defined as:

$$S_w = M_x M_x^T + M_y M_y^T \qquad \text{……….(12)}$$

Where the i^{th} column of matrix M_x contains the zero-meaned i^{th} exemplar given by $\vec{x}_i - \vec{\mu}_x$. Similarly, the j^{th} column of matrix M_y contains $\vec{y}_j - \vec{\mu}_y$. The between-class scatter matrix is defined as:

$$S_b = N_x(\vec{\mu}_x - \vec{\mu})(\vec{\mu}_x - \vec{\mu})^T + N_y(\vec{\mu}_y - \vec{\mu})^T \qquad \text{………(13)}$$

Finally, let $\vec{e}$ be the maximal generalized eigenvalue-eigenvector of S_b and S_w (i.e., $S_b\vec{e} = \lambda S_w\vec{e}$).

When the training exemplars $\vec{x}_i$ and $\vec{y}_j$ are projected onto the one-dimensional linear subspace defined by $\vec{e}$ (i.e., $\vec{x}_i^T\vec{e}$ and $\vec{y}_j^T\vec{e}$), the within-class scatter is minimized and the between-class scatter maximized, Figure(4). For the purpose of pattern recognition, such a projection is clearly desirable as it simultaneously reduces the dimensionality of the data and preserves discriminability.

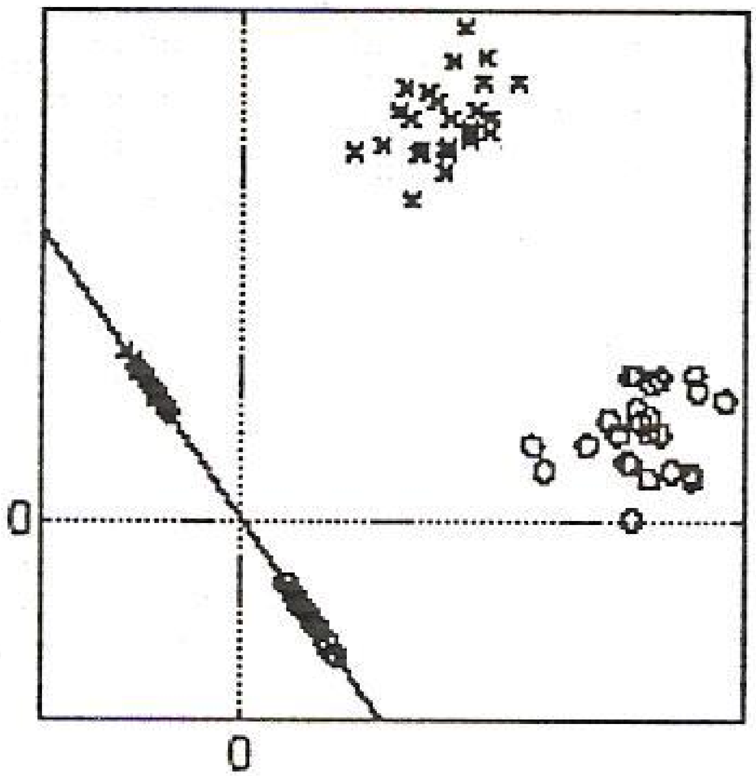

Fig (4): Shown are training exemplars from one of two classes ('x's and '0's) in an initially two-dimensional space. These exemplars are projected onto the FLD projection axis (solid line) to minimize within-class scatter and maximize between-class scatter. Novel exemplars projected onto the same axis can be, in this example, categorized depending on which side of the origin they project.

Once the FLD projection axis is determined from the training set, a novel exemplar, $\vec{z}$ from the testing set is classified by first projecting onto the same subspace, $\vec{z}^T \vec{e}$. In the simplest case, the class to which this exemplar belongs is determined via a simple threshold, Figure (4). In the case of a two-class FLD, we are guaranteed to be able to project onto a one-dimensional subspace (i.e., there will be at most one nonzero eigenvalue).

Algorithm 2:Trainig Algorithm Using FLD
Input: Feature Vectors of host and specific type of steganographic algorithm. *Output :FLD projection axis and threshold*
***Step1:** Specify feature vectors of the host set and the stego set for specific steganographic*

algorithm.
Step2: *Compute the within-class means as in eq.(10).*
Step3: *Determine the between-class mean according to eq.(11) .*
Step4: *Calculate the within-scatter matrix and the between-scatter matrix using the equations eq.(12) and eq.(13) respectively .*
Step5: *The FLD projection axis is the maximal generalized eigenvalue-eigenvector of* S_b *and* S_w *(i.e.,* $S_b \vec{e} = \lambda S_w \vec{e}$*).*

Step6: *Compute the projection of the feature vectors of host images and stego images on the FLD projection axis.*
Step7:*Plot on the same chart the percent of images no. to its projection values for the host and stego sets.*
Step8: *The intersection point of the two curves is take as threshold.*
Step9:*End.*

3.3 Testing Stage of The Implemented Algorithm

Testing stage is the final stage in the proposed algorithm that decides if the novel image contains hidden message or not. Here the testing image set, which contain 50 images that are used to check the performance of the steganalysis algorithm.

Once the FLD projection axis is determined from the training set, a novel feature vector, $\vec{z}$ from the testing set is classified by first projecting onto the same subspace, $\vec{z}^T \vec{e}$. In the simplest case, the class to which this exemplar belongs is determined via a simple threshold.

3.4 Experimental Results

The proposed method can operate on palette images (color and gray scale) of JPG, BMP and GIF formats. All of the stego images used are the same size (512x512).

Algorithm 3:Testing Algorithm Using FLD

Input: Feature Vectors ofNovel image, FLD Projectin Axis and the Threshold.
Output: Decision.

Step1: *Determined the image feature vector of the novel(* $\vec{z}$ *).*

Step2: *Get the FLD projection axis and the threshold(* $\vec{e}$ *).*

Step3: *Multiply feature vector by the FLD projection axis (* $\vec{z}^T \vec{e}$ *).*
Step4: *Get the threshold from the training stage and compare the result from the step3 and the threshold to decide to which set the image belongs.*
Step5:*End.*

Two steganographic programs/tools are used to test the proposed algorithm. These are S-Tool and LSB using wavelet transform. Different types of hidden message are used here, first type is an image and the second is a text.

3.4.1 S-Tool Steganography Algorithm

Train the algorithm on the two sets, the first is the host images set and the second stego images that use S-Tool algorithm in the embedding. Then FLD projection axis is computed and the latter used to find the projection of the feature vectors on the FLD projection axis by multiplying the feature vectors by it. Figure (5) shows the results of the training and testing set, the training set is on the left of the vertical dashed line and the testing set is on the right. In this figure the '*' corresponds to 'no-stego' images and the '◊' corresponds to the 'stego' images. The threshold for classification (horizontal line) is selected using the Figure (6). Table (1) shown the result of the detection process.

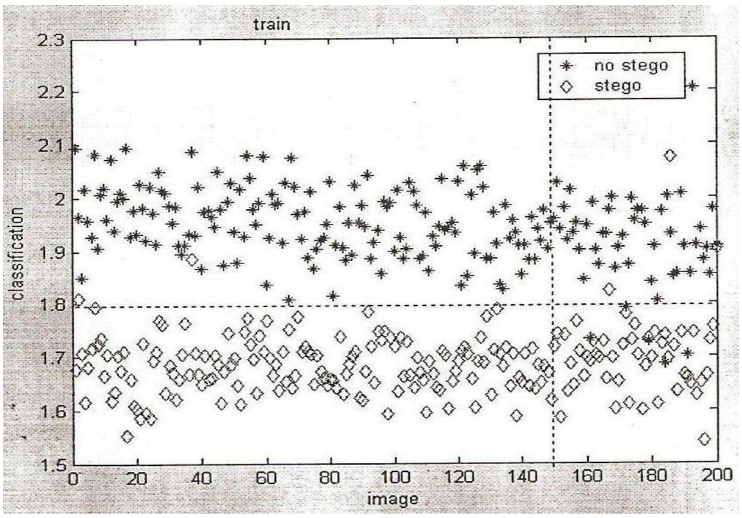

Fig (5): Result of training and testing images the threshold

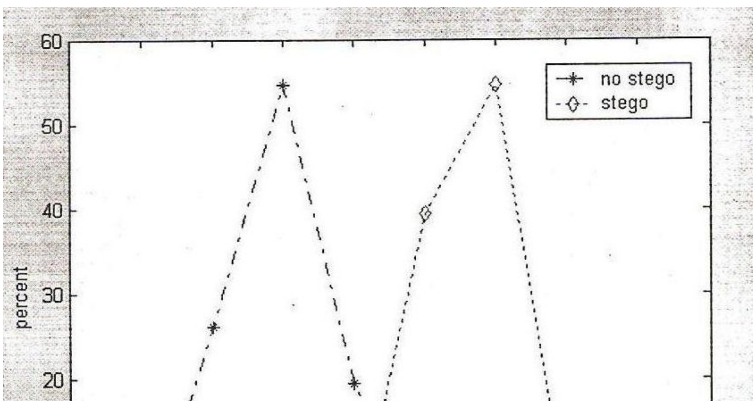

Fig (6): calculation of

3.4.2 LSB Using Wavelet Transform Steganography Algorithm

Here the FLD is trained for the host image set and stego images; the steganographic algorithm is based on wavelet. Shown in Figure (7) are the results of the training and testing sets. In this figure the '*' corresponds to 'no-stego' images and the '◊' corresponds to the 'stego' images. The threshold for classification (horizontal line) is selected using the Figure (8). Table (1) shown the result of the detection process.

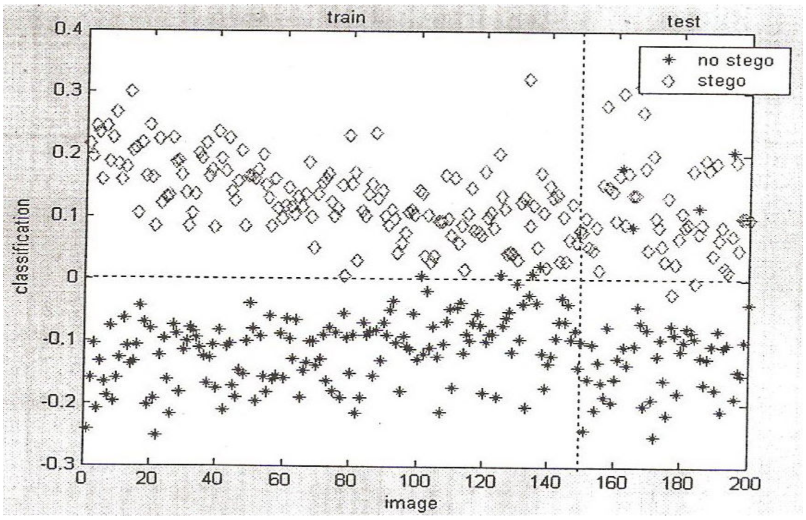

Fig (7): Result of training and testing images

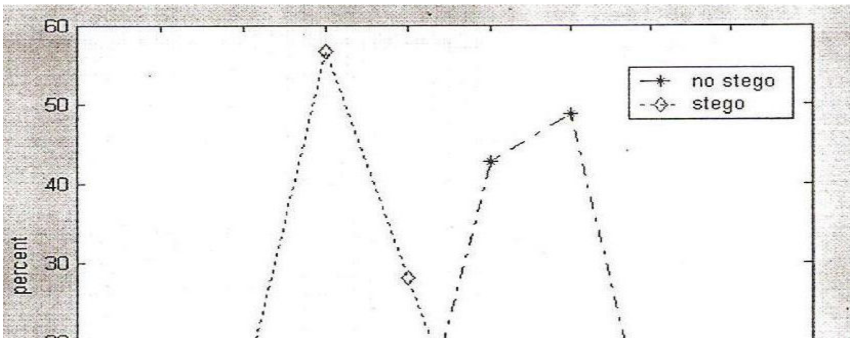

Fig (8): calculation of the threshold

Table(1): the result of the algorithms above

Lmage type / Stego type	No stego		Stego		threshold
	right	wrong	right	wrong	
S-TOOL	**90%**	**10%**	**94%**	**6%**	**1.7947**
WAVELET	**92%**	**8%**	**94%**	**6%**	**0.0064**

4. Conclusions

Messages can be embedded into digital images in ways that are imperceptible to the human eye, and yet these manipulations can fundamentally alter th underlying statistics of an image. To detect the presence of hidden messages a model based on statistics taken from a multi-scale decomposition has been employed. This model includes basic coefficient statistics as well as error statistics from an optimal linear predictor of coefficient magnitude. This higher-order statistics appear to capture certain properties of "natural" image, and more importantly, these statistics are significantly altered when a message is embedded within an image. As such, it is possible to detect, with high degree of accuracy, the presence of steganographic messages in digital images with format JPG or pallet like GIF (compressed or not). As the message size decreases, detection will become increasingly more difficult and less reliable.

Several directions should be explored in order to improve detection accuracy. The particular choice of statistics is some-what ad hoc, as suh it would be beneficial to optimize across a set of statistics that maximizes detection rates. By the classifier FLD, which simultaneously distinguishes between no-steg images and steg images generated from multiple programs, it becomes more accurate and it can identify the steg algorithm used. However convenient, FLD analysis is linear, and detection rates would almost certainly benefit from a more flexible non-linear classification scheme. Lastly, the indiscriminant comparison of image statistics across all images could be replaced with a class-based analysis, where, for example, indoor and outdoor scenes, or images with similar frequency content, are compared separately.

References

[1] Francesco Q.(**2000**), "Steganography in Image Final Communications Report",. eric.purpletree.org/file/Steganography%20In%20Images.pdf

[2] Silman J.(**2001**), "Steganography and Steganalysis: An Overview".

[3] Niel F. Johnson, Dduric Z. and Jajodia S.(**2001**), "Information Hiding: steganography and Watermarking – Attack and Countermeasures", Kluwer Academic Publishers.

[4] Jacob T. Jackson, Gregg H. Gunsch, Roger L. Claypoole, Jr., Gary B., "Blind Steganography Detection Using a Computational Immune System Approach: a proposal", Lamont Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology.

[5] Johnson, N.F., Jajodia, S.(**1998**), "Steganalysis: The Investigation of Hidden Information", IEEE Information Technology Conference,September.

[6] Fridrich J., Goljan. M., and Du R.(**2001**), "Reliable Detection of LSB Steganography in Grayscale and Color Images", Proc. ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, December 5, pp. 27-30.

[7] Fridrich J., Goljan. M., and Du R.(**2001**), "Detecting LSB Steganography in Color and Gray-Scale Images", Magazine of IEEE Multimedia, Special Issue on Security, December-November Issue, PP. 22-28.

[8] Onkar D., Kenneth S., and Upamanyu M (**2004**), " Detection of Hiding in the Least Significant Bit", IEEE Transactions on Signal Processing, Vol. 52, No. 10. **vision.ece.ucsb.edu**/publications/04SigprocKen.pdf

[9] Mohammad Ali Bani Youns and Aman Jantan (**2008**), " A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6.

paper.ijcsns.org/07_book/2008 06/20080634.pdf.

[10] Johnson N. F. and Jajodia S (**1998**), "Steganalysis of Image Created Using Current Steganography Software", Lecture Notes in Computer Science. Proceeding Vol. 1525 , pp 273-289. www.**jjtc.com**/ihws98/jjgmu.html

[11] Haider T. H. AL-Haajy (**2001**), "Still Images Steganography Using Wavelet Transform", thesis M.s.c, Baghdad.

[12] Burrus G. S., Gopinath R. A., Guo H (**1998**)., "Introduction to Wavelets and Wavelet Transform", Upper saddle New Jersey: Prentice Hall.

[13] Woods J. W and Ed (**1991**), "Subband IMAG Coding", Boston: Kluwer.

[14] Vetterli M. and Herley C.(**1992**), "Wavelet and Filter Banks: Theory and Design", IEEE Trans. Signal Processing, Vol. 40, No. 9; pp. 2202-2232.

[15] Robert W. Buccigrossi and Eero P. Simoncelli (**1999**), "Image Compression via Joint Statistical Characterization in the Wavelet Domain", IEEE Transaction on Image Processing, 8(12): 1688-1701.

[16] Smoncelli E. P.(**1999**), "Modeling the Joint Statistics of Images in the Wavelet Domain", In Processing of the 44th Annual Meeting, Vol. 813, Denver, CO, USA.

[17] Duda R. and Hart P.(**1973**), "Pattern Classification and Scene Analysis", Wiley, New York, NY.

الكشف عن المعلومات المخفية داخل الصور بأستخدام تحويل المويجة

أ.د وليد آمين محمود الجوهر
جامعة بغداد
د.طالب محمد جواد عباس
جامعة النهرين/كلية الحقوق
حسام جمعة نعيمة ألبهادلي
جامعة بغداد

الملخص

التقنيات والتطبيقات لإخفاء المعلومات أصبحا جداً متطورةَ وواسعةا الانتشار. وباستعمال الصور الرقميةِ ذات درجة الوضوح العاليةِ كناقل، معرفة وجود معلومات مخفيةِ أصبحَ أكثر صعوبة إلى حدّ كبير أيضاً. على الرغم من هذا فمن المحتملُ أحياناً معرفة (ليس بلضرورة أن تفك شفرة المعلومات) وجود معلومات مخفية. الفكرة الرئيسية في هذه الخوارزمية هو إيجاد إحصائياتِ الطلب الأعلى المتوقعةِ من الصور "الطبيعيةِ" ضمن تحليل متعدد المقياس، وبعد ذلك تبيين أن المعلومات المخفية في الصور الطبيعية تغير هذه الإحصائيات.

إن تحليل الصور التي تَستعملُ دوال اساسية محلية في الموقع المكاني والتوجيه والمقياس (مثال على ذلك: تحليل المويجه) أثبتَ انها مفيدَ جداً في عدة تطبيقاتِ. أحد الأسباب لهذا بأن مثل هذا التحليل يبدي انتظام إحصائي الذي يُيمكنُ أن يُستَغلَّ. إنّ الخوارزمية المُقترَحة تَتضمنُ ثلاث مراحل: مرحلة استخلاص ميزات الصورة (IFE)، مرحلة التدريب، ومرحلة الاختبار. في مرحلة استخلاص ميزات الصورةُ إلى المستوى الرابع باستخدام تحليل المويجة. مجموعة الإحصائيات (mean، skewness، وkurtosis لكلَ subband) جمعت من هذا التحليل. إنَ المجموعة الثانية للإحصائيات تستند على الأخطاء في المتوقع الخطيَ المثالي لمقدار المعامل في هذا التحليل. في هذا المتوقع فأن المعاملات تَربط مع جيرانهم في المكان والتوجيه والمقياسَ. تقنية الكشف المقترحة اختبرت على عينات الصور عولجت بأكثر طرق الإخفاء التجارية.