Design and Implementation of Information Hiding Detector Using Wavelet Transformation (Steganalysis)

L.A. Hiba Jebbar Aleqabie/ Kerbala University

Abstract

This research aims to design and implement a Steganalysis system that scan and test images, each of 24-bit, to find out if it contains hidden information. Using of wavelet transformation of Haar wavelet type to transform the images from the spatial domain to the frequency domain to produce feature vectors of coefficients, these coefficients are mapped, then using the ability of Probability Density Function (PDF) to minimize the features to extract the most important features that will be used as an input to the statistical tests in both The Standard statistics and the first order statistics

The Standard statistics are Absolute Value Differences (AD), Mean Square Error (MSE), Signal- to- Noise Ratio (SNR), Peak Signal- to- Noise Ratio (PSNR), Normalized Cross – Correlation (NCC), Correlation Quality (CQ).and the order statistics Mean, Variance, Skewness, Kurtosis. These tools are useful in examine the difference and similarity between the origin image and the suspected image.

The images that had been tested are 12 BMP images with different sizes, which had information hiding both Steganography and watermarked. Each BMP image of 24-bit. The stego objects(hidden information) are embedded using S-Toll, and Developed Steganography tool that modifying Least Significant Bit (LSB) of the pixel, some were detected and some were not, 6 images had information hiding and 6 were clear, 3 of 12 (i.e. 33%)were pass as they were clear, while 2 images were not. The others were detected. The developed system is implemented using Visual Basic programming language version 6, provides by Windows environments (XP, Me), and the resulted obtained are encouraging.

الخلاصـــة //

يهدف هذا البحث للتطوير و تنفيذ طريقة تحليل الاغمار من خلال الفحص الدقيق للصور المشكوك باحتوائها على معلومات مخفية (كصور ال BMP) , لتحديد فيما لو كانت تحتوي على اخفاء ولا تحتوي.

تم اغمار المعلومات المخفية باستخدام نوعين من الاغمار . النوع الاول نسخدم (S-Tool)و هو احد طرائق الاغمار المعروفة ,و طريقة مطورة تتعلق باغمار المعلومات باستخدام طريقة LSB.

و بالاعتماد على طريقة تحليل المويجة نوع هار (Harr Wavelet) كطريقة للتحويل الى المجال الترددي ثم استخلاص متجه المعالم (Feature Vector) الذي يحتوي على معلومات خاصة تتم معالجتها لاحقا,ثم استخدام امكانية دالة كثافة التوزيع(Probability Density Function) لاختزال المعلومات و تقليص عدد المعاملات اعتمادا على عمل الدالة حيث ستتم معالجة المعاملات في الاختبارات الاحصائية و التي هي على نوعين:طرائق تقليدية و طريقة مطورةو كالاتي:

الطريقة التقليدية هي عبارة عن عدة اختبارات هي: AD فرق القمة المطلقة ,MSE معدل مربع الخطا, SNRنسبة الاشار الى الضوضاء , PSNR نسبة الاشار الى الضوضاء القمية,NCCالرتباط المتقاطع الموزون,CQ نوعية الارتباط.

و في الطرقة المطورة تم استخدام الاختبارات الاتية : Mean المتوسط , Variance الت, Skewness معامل الالتواء , Kurtosis مقياس التفلطح.

تم اخبار عدة نماذج من الصور (كصور ال BMP) و باحجام مختلفة تحتوي على معلومات مخفية و اغمار مائي,لقد تم اختبار 12 صورة مختلفة بعضها تم تمييزه و اكتشاف احتواءه على اخفاء.4 من 12 (33%) دخلت النظام و لم تكتشف وكانها خالية من اي اضافة , بينما الاصل هو 1 خالية و الاخر حاوية على اخفاء .تم بناء النموذج باستخدام (Visual Basic 6) المجهز بواسطة بيئة النوافذ . و تم اختبار النموذج في بيئة نوافذ XP و نوافذ ME و قد اثبت النظام كفاءة مشجعة نسبيا.

1. Introduction to Information Hiding(Steganography)

Steganography is the art of hiding the presence of information by embedding secret messages into innocuous looking cover documents, such as digital images. Detection of Steganography, estimation of message length, and its extraction belong to the field of Steganalysis [9].

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 [11].

There are many approaches to hide the embedded file. The embedded file bits can be inserted in any order, concentrated in specific areas that might be less detectable, dispersed throughout the cover file, or repeated in many places. Careful selection of the cover file type and composition will contribute to successful embedding [3].

The number of bits in the cover file that get replaced will also affect the success of this method. In general, with each additional bit that is replaced the odd of detection increases, but in many cases more than one bit per cover file byte can be replaced successfully. Combining the correct selection of bits with analysis of the maximum number of bits to replace should result in the smallest possible impact to the statistical properties of the cover file [3].

2. Steganography VS. Steganalysis

Steganography is the art of invisible communication. Its purpose is to hide the very presence of communication by embedding messages into innocuous-looking cover objects. 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 [9].

Classical Steganographic systems depend on keeping the encoding system secret, modern Steganography tries to be undetectable unless secret information is known, namely, a secret key [10].

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 [5][6].

Though the first goal of Steganalysis is detection, there can be additional goals such as disabling, extraction, and confusion. Detection of Stenography, estimation of message length, and its extraction belong to the field of Steganalysis. Detection is more difficult than disabling in most cases, because disabling techniques can be applied to all files regardless of whether or not they are suspected of containing an embedded file. However, if only a minute portion of all files is suspected to have embedded files then disabling in this manner is not very efficient [7].

3. Steganalysis Techniques

a) One of Steganalysis technique is "the visible detection", which includes human observers detecting minute changes between a cover file and a stego file, or it can be done automatically. Additionally, since many Steganography tools take advantage of close colors or create their own close color groups, many similar colors in an image palette may make the image become suspect[8] [9].

b) Steganalysis can also involve the use of "statistical techniques". By analyzing changes in an image's close color pairs, the steganalyst can determine if LSB substitution was used. Close color pairs consist of two colors whose binary values differ only in the LSB. The sum of occurrences of each color in a close color pair does not change between the cover file and the stego file . This fact, along with the observation that LSB substitution merely flips some of the LSBs, causes the number of occurrences of each color in a close color pair in a stego file to approach the average number of occurrences for that pair. These statistical techniques benefit from the fact that the embedding process alters the original statistics of the cover file and in many cases these first-order statistics will show trends that can raise suspicion of Steganography[8].

c) "Universal blind Steganalysis" is a detection method(technique) in the sense that it can be adjusted, after training on original and stego-images, to detect any Steganographic method regardless of the embedding domain. The trick is to find an appropriate set of sensitive statistical quantities (a feature vector) with “distinguishing” capabilities. Neural networks, clustering algorithms, Statistical methods, and other tools of soft computing can then be used to find the right thresholds and construct the detection model from the collected experimental data [9] [5].

In this research the statistical techniques were used in cooperative with the Wavelet Transform.

4. Wavelet Transformation

Wavelets are mathematical functions that cut up data into different frequency components, and then study each component with a resolution matched to its scale [10].

Wavelet theory is based on analyzing signals to their components by using a set of basis functions. One important characteristic of the wavelet basis functions is that they relate to each other by simple scaling and translation. The original wavelet function, known as mother wavelet, which is generally designed based on some desired characteristics associated to that function, is used to generate all basis functions [9].

In most wavelet transform applications, it is required that the original signal be synthesized from the wavelet coefficients. This condition is referred to as perfect reconstruction. In some cases, however, like pattern recognition type of applications, this requirement can be relaxed. In the case of perfect reconstruction, in order to use same set of wavelets for both analysis and synthesis, and compactly represent the signal, the wavelets should also satisfy orthogonality condition. By choosing two different sets of wavelets, one for analysis and the other for synthesis, the two sets should satisfy the biorthogonality condition to achieve perfect reconstruction[9][10].

In general, the goal of most modern wavelet research is to create a mother wavelet function that will give an informative, efficient, and useful description of the signal of interest. It is not easy to design a uniform procedure for developing the best mother wavelet or wavelet transform for a given class of signals. However, based on several general characteristics of the wavelet functions, it is possible to determine which wavelet is more suitable for a given application [9].

They have advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities and sharp spikes. Wavelets were developed independently in the fields of mathematics, quantum physics, electrical engineering, and seismic geology. Interchanges between these fields during the last ten years have led to many new wavelet applications such as image compression, turbulence, human vision, radar, and earthquake prediction[11][8].

5. Histogram and Probability Density Function

In statistics, a **histogram** is a graphical display of tabulated frequencies. That is, a histogram is the graphical version of a table which shows what proportion of cases fall into each of several or many specified categories. The categories are usually specified as nonoverlapping intervals of some variable.

There are different ways to display the same table, and two kinds of histograms are there. One shows the number of cases per unit interval, so that the area under the curve is the total number of cases. Other shows the number of cases per unit interval divided by the total number of cases, so that the area under the curve is exactly In mathematics, a Probability Density Function (PDF) serves to represent a probability distribution in terms of integrals. Any function that is everywhere non-negative and whose integral from $-\infty$ to $+\infty$ is equal to 1 is a probability density function.

6. Statistical Testes

The statistical Test is very useful for detection of embedded data in an image. These analysis or test can expose abnormality in an image that is not visible to human eyes.

These tests need the original and the suspected images for getting the correct results. Denoting I as the original Image, I' as the Suspected Image, M as the height, N as the width, x, y are indexes**.**

a) Average Absolute Difference(AD)test

The average of the difference between color of pixels in original image and suspected image can be calculated as:

$$AD = \frac{1}{MN} \sum_{x,y} \left| I_{x,y} - I`_{x,y} \right| \qquad \text{.....(1)}$$

The absolute values used for difference to get accurate result of summation difference output.

b) Mean Squared Error(MSE)Test

To calculate the MSE between the original and the suspected images, we must et the difference of pixel color in the two images. The resulted will be the square amount of error depending on the size of these images, as shown:

$$MSE = \frac{1}{MN} \sum_{x,y} \left(I_{x,y} - I`_{x,y} \right)^2 \qquad \text{.....(2)}$$

c) Signal-to-Noise Ratio(SNR)Test

$$SNR = \sum_{x,y} I^2{}_{x,y} \Big/ \sum_{x,y} \left(I_{x,y} - I`_{x,y} \right)^2 \qquad \text{.....(3)}$$

d) Peak Signal-to-Noise Ratio(PSNR)Test

We use (PSNR) to calculate the maximum peak signal -to- noise ratio between two images as follows

$$PSNR = MN * \max * (I^2{}_{x,y} \Big/ \sum_{x,y} \left(I_{x,y} - I`_{x,y} \right)^2 \qquad \text{.....(4)}$$

e) Normalize Cross Correlation (NCC)

This metrics is important for see the amount the correlation between the original and suspected images.

$$NCC = \sum_{x,y} I_{x,y} * (I`_{x,y} \Big/ \sum_{x,y} I^2_{x,y}) \quad \text{.....(5)}$$

f) *Correlation Quality (CQ) Test*

Quality of correlation can be measured between the original images and the suspected images depending on the size of these images by using the equation:

$$CQ = \sum_{x,y} I_{x,y} * (I`_{x,y} \Big/ \sum_{x,y} I_{x,y}) \quad \text{.....(6)}$$

The first order statistic Tests

a) Mean **μ:**

Mean is a simple, intuitive and easy to implement method of *smoothing* images, *i.e.* reducing the amount of intensity variation between one pixel and the next. It is often used to reduce noise in images.

The mean of input image I (m x n) is define as the total of its brightness over the product of the dimensions M an N.

$$\mu = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} I(i,j) \quad \text{Or} = \frac{1}{MN} \sum_{i=0}^{255} i * His(i) \quad \text{.....(7)}$$

b) Variance σ^2**:** measures the average of the squared summations of frequencies.

$$\sigma^2 = \frac{1}{MN} \sum_{j=0}^{N-1} \sum_{i=0}^{M-1} \left(I_{(i,j)} - \mu \right)^2 \quad \text{Or} \quad \text{.....(8)}$$

$$\sigma^2 = \frac{1}{MN} \sum_{i=0}^{255} (i - \mu)^2 His(i)$$

c) ***Skewness*** **ς:** Skewness is the deviation of the frequencies distribution curve over similarity

$$\varsigma = \frac{1}{MN} \sum_{j=0}^{N-1} \sum_{i=0}^{M-1} \left(\frac{I_{(i,j)} - \mu}{\sigma_x} \right)^3 \quad \text{.....(9)}$$

d) ***Kurtosis*** κ**:** Kurtosis is the deviation of the top of the frequencies distribution curve over similarity.

$$\kappa = \frac{1}{MN} \sum_{j=0}^{N-1} \sum_{i=0}^{M-1} \left(\frac{I_{(i,j)} - \mu_x}{\sigma_x} \right)^4 \qquad \text{.....(10)}$$

7. The Proposed System

The Proposed System as shown in Fig 1 can be divided up to four parts as:-

a) Hiding process.
b) Preprocessing.
c) Features Extraction and Analysis Processes.
d) Discrimination Processes.

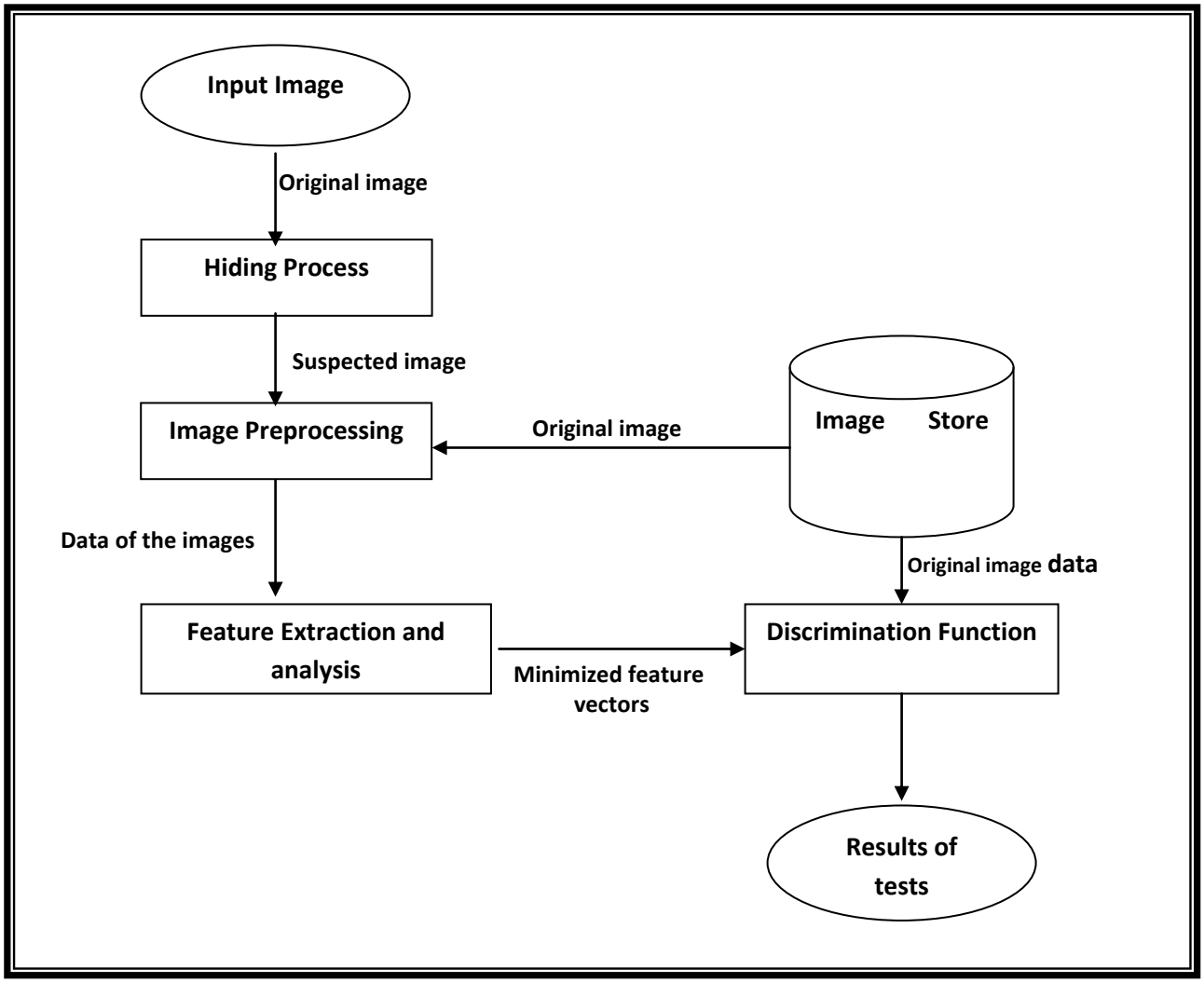


Fig 1 The Proposed System

a) Hiding process

In **LSB** modification, The embedded object is embedded in the spatial domain i.e. in two dimensional space of an image .At the beginning the color-plane (R, G, B, or all of them) is chosen, where the selected plane will carry the embedded object, by substitution the original bit with embedded bit.

The embedding process requires the original image (I), the embedded object(S) and the three parameters (color plane, pixels position, bit position) as input, the output of embedding process are stego image (I),as will be seen in the Algorithm1 , the block of LSB modification is illustrated in Fig.2 , This operation is once performed .

```
INPUT
  I ( )   // image's data
  S ( )  //block of embedded object
  sz     //  size of block
OUTPUT
  I'( )  //   stego image
Begin
   Loop s=1 to sz
      I'(s).blue= I(s).blue And 254
      I'(s).blue= I(s).blue Or S(s)
    End Loop
End
```

Algorithm 1 LSB modification

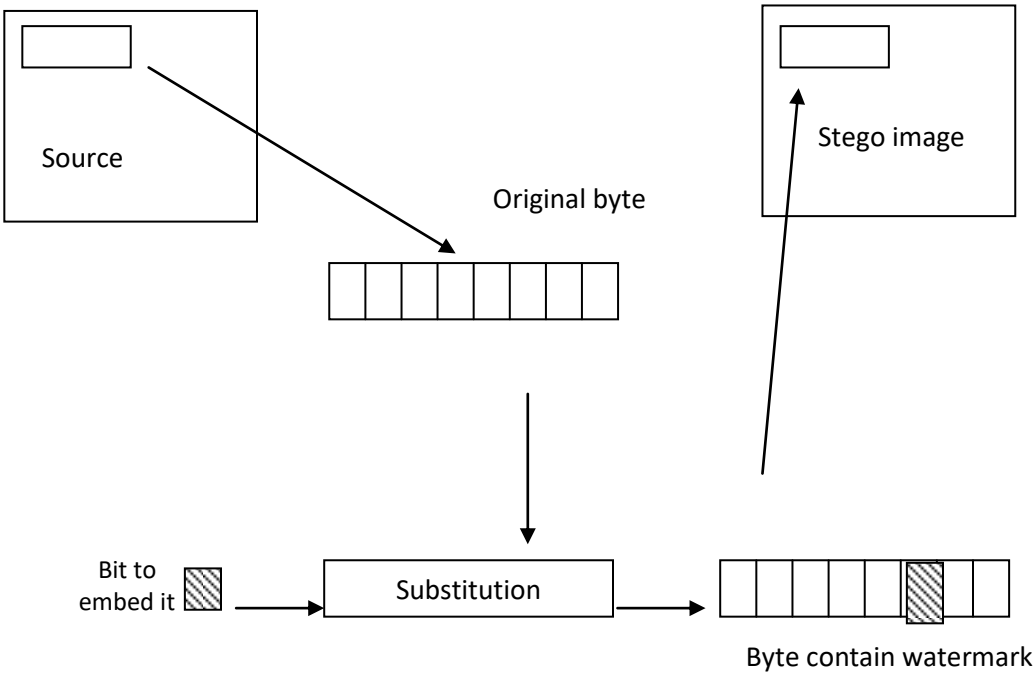


Fig.2 LSB modification

b) Preprocessing

Preprocessing is algorithms, techniques and operators are used to perform initial processing that makes the primary data reduction and analysis task easier. In the system it represents opening the suspected image that will be tested in the system as the input image. The images are saved as BMP format that start out with header followed by sequence of byte .The size of BMP header is 54 bytes and the data of the image is beginning from 55 to the end of the image pixel. The implemented image is describe as 24 bit per pixel, each pixel have three band (red, Green, Blue) , the detailed description of BMP is given at appendix A, Algorithm 1 search for the original image through the database folder assuming it's already exist. And save it bitmap data for the next process [11].

Generally, Images came 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 **I'** and the original image **I,** the algorithm 2 will be applied.

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. Reordering the bitmap data is stated in Algorithm 3.

```
INPUT
    I is the original image, I' is the suspected image.
 OUTPUT
    D ( )   //Array of one dimension of the bitmap data of the Original image
    D'( )  // Array of one dimension of the bitmap data of the Suspected image
Begin
    Search For the original image in the database and open it
    as I'.
For both  I and I' do
   Open I, I' file for read
    Read I, I' headers
    Read the bitmap data of I and I' as D and D' respectively
 End
```

Algorithm 2 Open BMP File

```
 INPUT
   Readimage with size N*M
 OUTPUT
Reordered image I
 // the pixel consist of three colors (Blue, Green ,Red)
(R,G,B)respectively, one byte is allocated to each color plane
Begin
For y = 1 to M
 For x = 1 to N
      I (h - y + 1, x).b = readimage (3 * x - 2, y)
      I (h - y + 1, x).g = readimage (3 * x - 1, y)
      I (h - y + 1, x).r = readimage (3 * x, y)
 End
```

Algorithm 3 image Reordering

INPUT
Let image be $\mathbf{I_1}$ with size $h_1 * w_1$
OUTPUT
The scaled image $\mathbf{I_2}$ with size h2*w2
Begin
For each pixel (x_2,y_2)in $\mathbf{I_2}$ do
Find the corresponding pixel (x1,y1) in $\mathbf{I_1}$ to have the value of
$\mathbf{I_2}(x_1,y_1)$ pixel

$$X_1 = x_2 * ((w_1 - 1) / (w_2 - 1))$$
$$Y_1 = y_2 * ((h_1 - 1) / (h_2 - 1))$$

$\mathbf{I_2}(x_2,y_2) = \mathbf{I_1}(x_1,y_1)$
END

Algorithm 4 Resize the images (scaled image)

c) 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[11].

Feature vector is one method to represent an image. or part of an image. by finding measurements on a set features. The feature vector is an *n-dimensional* that contains these measurements. The vector provides us with high-level information.

Now we can consider methods to compare two feature vectors. The primary method either to measure the differences or measure the similarity .the difference measured by Euclidean distance is the most common metric for measure the distance of two vectors and giving by

$$\sum_{i=0}^{N} (a_i - b_i)^2$$

Where a_i is the original feature vector, b_i is the suspected feature vector

The histogram of an image plot of the gray-level values versus the number of pixels at that value. the shape of histogram provides us with information about the nature of the image, or subimage if we are considering an object within the image.

$$p(g) = \frac{N(g)}{M}$$

M is the number of pixels in image or subimage ,N(g)=number of pixels at gray level **g.** The features based on first order histogram are mean standard deviation, skew, energy, entropy. the Histogram, a simple graph that displays where all of the brightness levels contained in the scene are found, from the darkest to the brightest. These values are arrayed across the bottom of the graph from left (darkest) to right (brightest). The vertical axis (the height of points on the graph) shows how much of the image is found at any particular brightness level.

Then Apply "Probability Density function ", that Distribute the data using Probability density function as a way to minimize the feature vector in order to choose the best features that required and important in the work

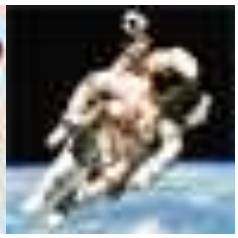
8 Conclusion and Discussions

This section concerned with experimental result for samples of images being tested, 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 24bits true color . Types of hiding were used LSB and S-Tool and adding a simple noise.


Picture 1


Picture 2


Picture3


Picture 4


Picture 5


Picture 6


Picture 7

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)),Duck with no hidden information, drip with noise and some images with LSB, S-Tool . Table1 shows the result of the comparisons of several images.
In the first step table1 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 , we can notice the differences
The AD represents the average of the difference between color of pixels in original image and suspected image.
The result for R byte of the image is 0.00515, for G byte of the image is 0.0055, B byte of the image is 0.0044.this means there is a difference between the pictures if there is no difference so there is no difference or no insertion in the image .
For the other statistics tests also if the results are zeros so there is no hidden information.

Table1 (the standard statistics between Sandybell and sandybell1 pictures)

Sandy bell and Sandy bell 1 ➔		R	G	B
	AD	0.00515	0.0055	0.0044
	MSE	0.0205	0.02221	0.0178
	SNR	1210115.2760	1576468.8434	2281166.91780
	PSNR	6502.5333	6002.33843	7482.3670
	NCC	0.999	0.9999	0.9999
	CQ	212.8974	195.2398	213.5197

if we take the Guitar and Guitar1 the resulted of

Table2 (the standard statistics between Guitar and Guitar1 pictures)

Guitar and Guitar1	➔	R	G	B
	AD	0	10.2478	
	MSE	0	513.30425	0
	SNR	overflow	overflow	Overflow
	PSNR	Division by zero	Division by zero	Division by zero
	NCC	1	0.930604	1
	CQ	163.6459	144.9521	148.2131

The result for R byte of the image is 0, for G byte of the image is 10.278 , B byte of the image is 0.this means there is no difference between the pictures at R byte of image ,but there is a difference at G byte of the image
For the other statistics tests also some are zeros and other is non zeros.
Some are overflowed and others are division by zeros.

The result for R byte of the image is 0, for G byte of the image is 10.278 , B byte of the image is 0.this means there is no difference between the pictures at R byte of image ,but there is a difference at G byte of the image .For the other statistics tests also some are zeros and other is non zeros. Some are overflowed and others are division by zeros.

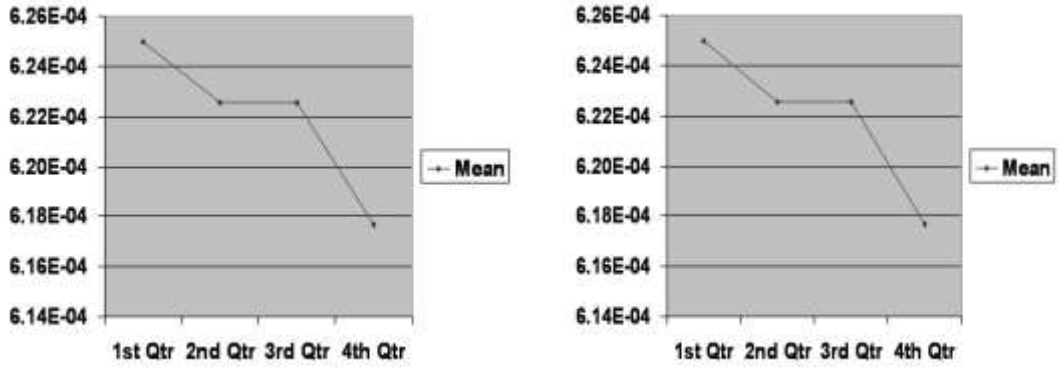


Fig 3 Mean Measurement for picture1 duck and duck1

Fig 3 represent the measurement of the first order statistics, the Mean which is the total of its brightness over the product of the dimensions M an N. will be applied on the original image and the suspected image. It can be noticed that there is no different for the tested images, it's clear according to mean measurement.

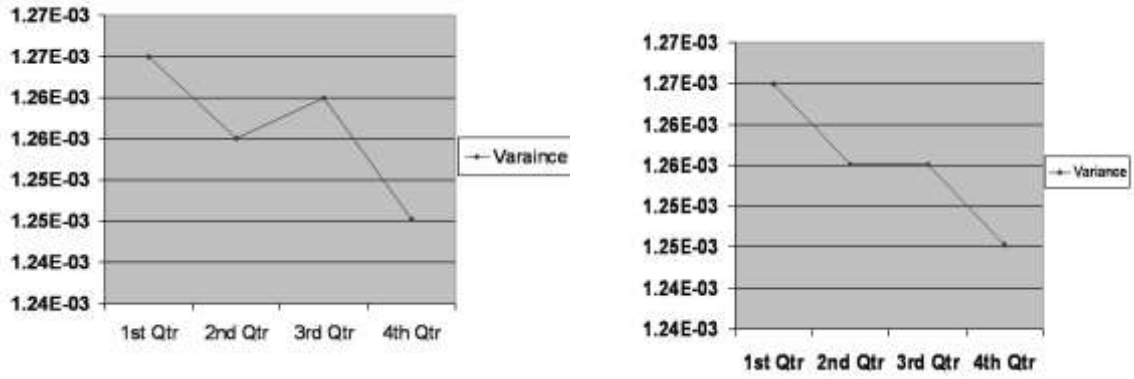


Fig 4 Variance Measurement for pictur31fly and fly1

Fig 4 represent the measurement of the first order statistics, measures the average of the squared summations of frequencies. will be applied on the original image and the suspected image. It can be noticed that there is a difference in the result if we focus on the fig3 and watch it its very clear for the tested images, it's not clear according to variance measurement.

Appendix A

The BMP file format

The BMP file format divides a graphics file into four major parts, these are:

- Bitmap file Header the bitmap file header is 14-bytes long and it formatted as :

UNIT bfType (hold the signature value 0x4D24,identifies the file as BMP)
DWORD bfSize (holds the file size)
UNIT bfReserved (not used, set to zero)
UNIT bfReserved (not used, set to zero)
WORD bfOffcet (specifies the offset, relative to the beginning of the file, where the datarepresenting the bitmap itself)

- Bitmap Information header the bitmap information header contains important information about the image .the windows format for this header is:

DWORD biSize (hold the header length in bytes)
LONG biWidth (identify the image width)
LONG biHight (identify the image Height)
WORD biPlanes
WORD biBitCount (identify number of bit/pixel in the image and thus the maximum number color that the bitmap can contain)
DWORD biCompression (identify the compression scheme that the bitmap employs. It will contain zeroif the bitmap uncompressed)
DWORD biSizeImage (set to zero for uncompressed image, else it holds size(in bytes)of the bitsrepresenting the bitmap image forcompressed image)
LONG biXpelsperMeter
LONG biYpelsperMeter
DWROD biClrUsed
DWORD biClrImportant

- Palette: The color table specifies the color used in bitmap. The BMP file comes in four color formats

1. 2-color one bit per pixel
2. 16-color four bit per pixel
3. 256-color eight bit per pixel
4. 16.7million-color 24bits per pixel

The number of bits per pixel can be determined from the biBitCount shown above. In the 2-color, 16-color, 256-color BMP format, the color table contains one entry for each color. Each entry specifies the intensities of color's red, green, and blue components and it is of 24-bytes long as shown below:

BYTE regBlue , BYTE regGreen,BYTE regRed BYTE regReserved

Each color-table entry can specify range or red, green, and blue values from 0 to 255. True color BMP files do not contain color table, because a single color table with 16.7million entries of 4-bytes each would require 64MB of storage space.

- Bitmap Bits: the bitmap bits are set of bits defining the image –the bitmap itself. In the 2-color, 16-color, and 256-color BMP formats, each entry in the bitmap is an index to the color table. In 16.7milion-color bitmap, where there is no color table, each bitmap entry directly specifies a color. These first 3-bytes in each 24-bit entry specify the pixel color and component, the second specifies green component, and the third specifies blue.

The bitmap bits representing a single line stored in left-to-right order, the same way that the pixel they represent line up on the screen. The first row pixel data in bitmap responds to the bottom row of pixel on the screen, the second row corresponds to the row of pixel second from the bottom, and on.
The size of one bitmap entry is determined by the number of bits per pixel as shown in the following table:

Number Of Color	Number Of bits Per Pixel Require
2	1
16	4 (1/2 byte)
256	8 (1 byte)
16.7million	24 (6 bytes)

References

[1] Jessica F. and Miroslav G. "**Practical Steganalysis of Digital Images – State of the Art",**SUNY Binghamton, Department of Electrical Engineering, Binghamton, NY 13902-6000 ,2000.

[2] Hany F., **"Detecting Hidden Messages Using Higher-Order Statistical Models"** Department of Computer Science, Dartmouth College, Hanover NH 03755,2001.

[3] Neil J. and Sushil J., "**Steganalysis: The Investigation of Hidden Information**", Proceedings of the 1998 IEEE Information Technology Conference, Syracuse, New York, USA, September 1st - 3rd, 1998.

[4] Niels P.**, "Defending Against Statistical Steganalysis**" Center for Information Technology Integration, University of Michigan, published in 10th NSENIX security Symposium, Washington DC, pp. 323-335,2001.

[5] Haider J.**"Wavelet-Base Steganography "**a M.SC. Thesis submitted to Al-Nahrain university ,computer science department ,2004 .

[6] Roman T., Robert B., Johannes B. , "**Steganographic System Based on Higher-Order Statistics"** University of Erlangen-Nuremberg, Cauerstr., D-91058 Erlangen, Germany. published in Proceedings of SPIE Vol. 5020, Security and Watermarking of Multimedia Contents V, Santa Clara, California, USA, 2003.

[7] Stefan K., Fabien. P., "**Information Hiding For Steganography And Digital Watermarking** ", ISBN 1-58053-035-4 , published in 2000.

[8] Jacob T. ,Gregg G., Roger C.,Gary B, **"Blind Steganography Detection Using a Computational Immune System",** International Journal of Digital Evidence Winter 2003, Issue 1, Volume 4 .

[9] Ali M. Reza," **Wavelet Characteristics, What Wavelet Should I use?",** an internet paper, Spire Lab, UWM,1999.privet communication through Internet .

[10] Burrus C. S. , Gopinath R. A., and H. Guo, **" Introduction to Wavelets and Wavelet Transforms: *A Primer*"**, Prentice Hall, Inc., 1998.

[11] Mustafa D. T. ," **Design of A Fingerprint Recognition System Using Wavelet Transformation**", a M.SC. Thesis submitted to Al-Nahrain university ,Computer science department Computer science, Al-Nahrain university, 2001.

[12] Hany F., **"Detecting Hidden Messages Using Higher-Order Statistical Models"** Department of Computer Science, Dartmouth College, Hanover NH 03755,2001.