Random Insertion Watermarking By Computing Angle Between Two Lines In Blue Components On Postage Stamp

Nada Mahdi al- Husseiny*

Received on: 20/7/2010
Accepted on: 7/4/2011

Abstract

This paper presents a new approach for watermarking by using geometric analytic and mathematical model providing robustness to embed the watermarking in postage stamp (ps) image, using the angle between two lines to insert the embedded information in blue component for pixels. Analytic geometry, also known as coordinate geometry, or Cartesian geometry, is the study of geometry using a coordinate system and analysis. The modern and advanced meaning refers to the geometry of analytic varieties, to develop a data-hiding method that has a good performance in color images. Furthermore, the watermark must be either robust or fragile; depending on the application. The expression "robust" in this paper refers to the capability of the watermark to resist manipulations of the media. Two types of watermarked attack was used; the JEPQ compression as lossy compression (where compressing and decompressing data retrieve hidden information that may be close enough to the original image), and the enhancement filter (mean filter). This proposed watermarking system refers to the watermark objective evaluation test or (WOET).

Keywords: digital watermarking, watermark evaluation, Analytic geometry, hidden information, attack watermarking.

الإدخال العشوائي لإخفاء معلومة باستخدام الزوايا في المكونات الزرقاء لنقاط الصورة على الطوابع البريدية

الخلاصة

هذا البحث تم استحداث طريقة جديدة لاخفاء المعلومات باستخدام التحليل الهندسي لمكونات نقاط الصور وباستخدام النموذج الرياضي لتوفير متانة جيدة لاخفاء رسالة معينة على صور الطوابع البريدية من خلال استحداث الزوايا بين خطين منتخبين ضمن الصورة لادخال المعلومة المخفية للمكون الازرق لنقاط الصورة.

ان التحليل الهندسي يعرف على انه هندسة الاحداثيات او الهندسة الديكارتية حيث يتم دراسة الهندسة باستخدام نظام الاحداثيات ومن ثم تحليلها. ان التعريف الحديث لهذا النموذج يشير الى التحليل الهندسي للنقاط المختلفة لتطوير طريقة جديدة لاخفاء المعلومات التي تمتلك اداء جيد للصور الملونة. اضافة الى ذلك فان طريقة الاخفاء قد تكون متينة او قابلة للاختراق وذلك يعتمد على نوع التطبيق المستخدم. ان مصطلح متين في هذا البحث يشير الى قدرة طرق الاخفاء على مقاومة التلاعب في الوسط البيئي المستخدم.

تم استخدام طريقتين لمهاجمة اخفاء المعلومة ، الاولى هي طريقة الضغط (JEPQ Compression) الذي يعرف على انه الانضغاط المفقود (حيث يتم ضغط البيانات ومن ثم فتحها يمكن من استرجاع المعلومات المخفية بصورة تكون قريبة جدا الى الصورة الاصلية) ، اما الطريقة الثانية فتتم باستخدام

*Building and Construction Engineering Department, University of Technology/Baghdad

https://doi.org/10.30684/ etj.29.7.7
University of Technology-Iraq, Baghdad, Iraq/2412-0758

المرشح المحسن (مرشح الوسط). الطريقة المقترحة في هذا البحث تشير الى فحص تقييم اهداف اخفاء المعلومات.

Introduction

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to be removed. The signal may be audio, picture or video, for example, if the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time [1]. The general watermarking system for image is explained in the figure (1).

Watermarks are embedded into images by changing some bits in image representation. Some methods operate on least significant bits, while others operate on embedded information into perceptually more significant image components [2].

Interest in digital watermarks has grown out of an increasing interest in intellectual property and copyright protection. The embedded information known as watermark can be provided by information about the media, the author, copyright, or license information. Digital watermarks may be perceptible (visible) or imperceptible (invisible) to human vision. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived (although it may be possible to detect that the information is hidden).

Visible watermarks, by nature, are more intrusive to the media and act to deter theft of the media, such as a Warning sign announces an alarm system even if one does not exist.

Examples of such watermarks can be seen easily on most network television stations by the station's logo in the corner of the viewable screen. These watermarks are typically confined to an area of the image, which is less intrusive to the overall image. Attackers have a visible target and can remove the watermark by cropping the image [3].

The basic requirements on the watermarking method include that the watermark is invisible and difficult to remove. Digital Watermarking is the practice of hiding a message in an image, audio, video or other digital media element. Since the late 1990s, there has been an explosion in the number of digital watermarking algorithms published. The sudden increase is mostly due to the increase in concern over copyright protection of content. Applications of watermarking include broadcast monitoring, owner identification, proof of ownership, transaction tracking, authentication, copy control, and device control [4].

In most cases, the hidden data is a collection of bits, which, depending on the application, may come from an encoded character string; the embedded data may form a perceptual source itself, such as the application of “image in image” and “video in video” [5].

The watermark is a key feature of the postage stamp, and often constitutes the difference between a common and

a rare stamp, Elephant head watermark used on early stamps of India. Watermarks were nearly universal on postage stamps in the 19th and early 20th centuries, but generally are used on modern issues.

2. The Proposed Watermarking System

Most process models use geometric shapes to represent variables of interest, and lines and arrows to show effects and relationships.

The present research used the Red, Green, Blue color model to insert embedded information for true color postage stamp image.

The proposed method is applied on different true color bitmap cover images of 256×256 in size. Thereafter a new class of watermarking schemes is used, by choosing the random generator location to embed the watermark into one of the RGB components for each pixel. We embed multiple bits using the angle between two lines to insert sequences of characters in text hiding depending on the angle's value; the insertion at different location depend on the type of image and the value of angle between any two lines in the entire image. The values of three color channels are dependent on the imaging. In this research the saving of the hidden information was done using blue component, because of its least influence of the image.

In this proposed watermarking system refer to the watermark objective evaluation test or (WOET) by compute the measurements MSE, PSNR and distortion to evaluate the watermarking algorithm after inserting embedded text in stamps and all the results show very good and acceptable agreement [6]. This work will greatly stimulate new research in watermarking and data hiding by allowing the demonstrating of new techniques. Postage Stamps are used to represent digital media. Invisible watermarks have an advantage over visible watermarks, where their location may be unknown; a common practice is to distribute the watermark (or watermarks) across the entire image. Every watermarking system consists of at least two different parts: watermark embedding unit and watermark detection and extraction unit. This provides some protection against cropping attacks.

The proposed system in this paper is composed of the following stages, as shown in figure (2).

1. Convert (2D to 1D) true color Bitmap image.
2. The Insertion of embedded information is known as watermark in image according to mathematic model.
3. Using Objective Evaluation to measure the performance of proposed watermark system.
4. Watermarking Attacks.
5. Decoding the hidden information.
6. Display the hidden information.

2.1 Transform 2D To 1D True Color Image.

The next step for random generation is transforming the 2d true color bitmap image into 1d

true color bitmap image; as shown in the algorithm below:

Input: original true color bitmap (256*256) image as 2D.

Output: 1D true color bitmap image (256*256).

1) transform 2d matrix which represents the location

Corresponding to pixels with the elements values, as the equation (1)

$$location\_1dim=[(No of row-1)*depth+No of depth location \quad \ldots\ldots (1)$$

2) Repeat step 1 until obtain 1 d matrix representing the location

Corresponding to all pixels with the elements values which represents the experimental images.

2.2. Random Generator Location

Random generator location is used to generate random insertion for hidden information in the watermarking image and it works as shown in the steps below:

Input: 1D true color bitmap image

Output: 1D true color bitmap image with random _location.

1) Compute the max _ location for the input image as shown in the equation (2).

$$\max\_location = width \times height \quad \ldots\ldots. (2)$$

2) First seed _random location= seed_ random (max location)

$$\max\_location = \max\_lcation - 1 \quad \ldots. (3)$$

3) Exchange the max _location with first seed _random Location.

4) Repeat steps (2, 3).

5)in end of this process, obtain the sequence of random location for original Image.

The random sequence was selected in the algorithm above to facilitate the process of obtaining lines between two adjacent pixels, where these pixels not necessarily being adjacent in the original image, to prohibit drawing identical lines.

The end of this process obtains the random sequence of location to be used in the next step.

2.3. Mathematical Model:

Mathematics is the study of quantity, structure, space, and change. When engineers analyze a system to be controlled or optimized, they use a mathematical model. In analysis, engineers can build a descriptive model of the system as a hypothesis of how the system could work, or try to estimate how an unforeseeable event could affect the system. Similarly, in control of a system, engineers can try out different control approaches in simulations.

A mathematical model usually describes a system by a set of variables and a set of equations that establish relationships between the variables. The values of the variables can be practically anything; real or integer numbers, Boolean values or strings, for example. The actual model is the set of functions that describe the relations between the different variables [7].

The mathematical model used in this research includes the geometric analysis for embedded information; the steps of this model are listed below

2.3.1. Distance Between Two Pixels (with known coordinates)**:**

In analytic geometry, geometric notions such as distance and angle measure, these definitions are designed

to be consistent with the underlying Euclidean geometry. For example, using Cartesian coordinates in the x-y plane, the distance (D) between two points (x_1, y_1) and (x_2, y_2) is defined by Eq. (4)

$$D = \sqrt{dx^2 + dy^2} \qquad \text{..... (4)}$$

Where dx is the difference between the x-coordinates of the points, dy is the difference between the y-coordinates of the points.

A line can be drawn by two adjacent pixels in the 1D matrix obtained by the random generator locations; these two pixels may not be adjacent in the original 2D matrix.

This operation is repeated for each two adjacent pixels in the whole 1D matrix, the lines created intersect with each other obtaining angles between them.

The formula in Eq.(4) above can be used to find the distance between two points with known coordinates. This distance is also the length of the line segment linking these two points [8].

2.3.2. The Slope and the Angle between Two Lines

Analytic geometry, also known as coordinate geometry or Cartesian geometry, is the study of geometry using coordinate system and the principles of algebra and analysis. This contrasts with the synthetic approach of Euclidean geometry, which treats certain geometric notions as primitive, and uses deductive reasoning based on axioms and theorems to derive truth. Analytic geometry is the foundation of most modern fields of geometry, including algebraic geometry, differential geometry, and discrete and computational geometry, and is widely used in physics and engineering.

In geometry, an angle is formed by two rays sharing a common endpoint, called the vertex of the angle. The magnitude of the angle is the "amount of rotation" that separates the two rays, and can be measured by considering the length of circular arc swept out when one ray is rotated about the vertex to coincide with the other. Where there is no possibility of confusion, the term "angle" is used interchangeably for both the geometric configuration itself and for its angular magnitude (which is simply a numerical quantity).Euclid defines a plane angle as the inclination to each other, in a plane, of two lines which meet each other, and do not lie straight with respect to each other.

In mathematics, the angle from the first to the second coordinate axis of a coordinate system is considered as positive. Therefore, angles given a sign are positive angles if measured anticlockwise, and negative angles if measured clockwise, from a given line. If no line is specified, it can be assumed to be the first coordinate axis (x-axis) in the Cartesian plane. In many geometrical situations, a negative angle of $-\theta$ is effectively equivalent to a positive angle of "one full rotation less θ". For example, a clockwise rotation of 45° (that is, an angle of −45°) is often effectively equivalent to an anticlockwise rotation of 360° − 45° (that is, an angle of 315°).

In three dimensional geometry, "clockwise" and "anticlockwise" have no absolute meaning, so the direction of positive and negative angles must be

defined relative to some reference, which is typically a vector passing through the angle's vertex and perpendicular to the plane in which the rays of the angle lie.

Consider a line L in the xy plane. It forms an angle of inclination α ($0 \leq \alpha \prec \pi$), with the positive x axis. The slope m of L is $\tan\alpha$. (If $\alpha = \pi/2$, the slope is not defined) Consider two lines L and L', with angles of inclination α and α', and slopes m and m', respectively, as shown in figure (3)

The angle between these lines can be computed according to the Eq. (5)

$$\theta = \alpha - \alpha' \qquad \text{..... (5)}$$

If L and L' are parallel, define (θ) to be 0.

figure (4) and figure (5) show the angle (θ) for some typical L and L'. In each case (θ) is the counterclockwise angle from L' to L. note that (θ) depends on the choice of the x-axis that $0 \leq \theta \prec \pi$ [9].

The Formula for obtaining the slope of a straight line going through the points (x_1, y_1) and (x_2, y_2) is given by the Eq.(6)[10].

$$m = \frac{y_{2-}y_1}{x_2 - x_1} \qquad \text{..... (6)}$$

In mathematics, The slope is defined as the" rise" divided by" run" between two points on a line, as shown in figures (6,7), or in other words, the ratio of the altitude change to the horizontal distance between any two points on the line, as explained in Eq. (7).

$$m = \frac{rise}{run} = \frac{change.i.n\_y}{change.in.\_x} = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{..... (7)}$$

Rise means how many units up or down from point to point. On the graph that would be a **change in the *y* values**.

Run means how far left or right from point to point. On the graph, that would mean a **change of *x* values**. [11]

Any location in image is represented by pixel, and each pixel of these color images has three channels; red, green and blue. Let *Rl ,m, Gl ,m , Bl ,m* be the pixel values in Red(R), Green(G) and Blue(B) channels of the postage stamp color image on the coordinate (*l,m*) respectively.

We took the (red, green) components of two pixels from random sequence was considered, and by Assume the difference between two pixels for the red component related to Δy, and the difference between the same pixels for the green component related to Δx; as shown in Eq. (8).

$$m = \frac{\Delta y}{\Delta x} = \frac{Rp_2 - Rp_1}{Gp_2 - Gp_1} \qquad \text{... (8)}$$

Where the

Rp1…… red component for pixel 1,
Rp2…… red component for pixel 2,
GP1……Green component for pixel and GP2……Green component for pixel 2.

The tangent of (θ) is easily expressed in terms of the slopes *m* and m'.as shows in equation (9).

$$\tan\theta = \tan(\alpha - \alpha') \quad .... (9)$$

By the identity for tan (A-B) ,shows in equation (10).

$$\tan\theta = \frac{\tan\alpha - \tan\alpha'}{1 + \tan\alpha \tan\alpha'} \quad \dots (10)$$

Equation for tangent of angle between two lines in terms of their slopes is shown in Eq. (11).

$$\tan\theta = \frac{m - m'}{1 + mm'} \quad \dots\dots (11)$$

Where m is the slope of the line with larger angle of inclination $mm' = -1,$ then $\theta = \pi/2$; This corresponds to the fact that, as $mm' \to -1, |\tan\theta| \to \infty$ The procedure mentioned above is explained in the steps below:

1) Compute the angles between each two lines intersected in the image with dimension (256*256) as 24–bitmap; excluding the parallel lines, as in equations(9,10,11).
2) Compute the summation of all angles (θ) in image.

Find the average value for the angles in the image according to Eqs (12 and 13).

$$averageAngle = \frac{\sum_{1}^{N} angles}{No.angle} \quad \dots (12)$$

Where

$$N = \frac{width_{imge} * depth_{image}}{4} \dots (13)$$

2.3.3. Encoding Watermarking Image

Disabling a watermark or embedded message is easy in employ the LS.B of images. The previous steps compute the average value for angles and the next steps explain the algorithm to insert hidden information and encoding watermarking image:

1) Transform the hidden information to the sequence of bits (0 or 1), and one byte for each character embedded on the watermarked image.

2) Save every bit of hidden information in the watermarking image as a sequence, this process is done as follows:

a) Repeat the previous section to calculate all angles (θ) in cover Image.

b) Compare between each angle's values with the average.

If the angle value (θ) is more than the average then:

Save one bit (0 or 1) in L.S.B in blue component of this location, or using a threshold to represent hidden information bit Else, ignore this value .

c) Ending the algorithm when reaching the end of the Saving as a sequence of bits.

Because of its least influence, the blue component was used for saving the

message or string. The mark is embedded in each angle, when its value (θ) was more than the average, the message is of n-bit-long stream and $M = \{0,1\}^n$ and is modulated in the watermark, they are usually referred to as multiple bit watermarking schemes. The proposed system in this paper used two methods to save the hidden information: the first method is saving in the (L.S.B) in the blue component as one bit (0 or1) depending on the value of the information. This method may be changeable by lossy compression or small amounts of image processing. Using the attack process such as JPEQ compression leads to converting value of the bit saved in the L.S.B, leading to loosing the watermarking information, therefore this process must be repeated three times by using perfect algorithm.

In decoding process, after using the attack technique (JPEQ compression), if the returned values were two of (0 or black) value and one of (1 or white) value then the value is definitely black. The second method for saving hidden information, is by using a level or threshold such as (3,-3); (to save one bit of hidden information, three bits are needed from the blue component, two bits to represent number 3 and one bit to represent the sign bit), when the bit wanted to be inserted as water marking having the sequence of bits as (1 or white), the highest value of the threshold, (3), must be added to the value of blue component, and if the bit of watermarking inserted is (0 or black), the value of the blue component must be added to the value of the lowest threshold, (-3), this method is robust for JEPQ compression in attack process.

The result for system encoding watermarking is shown in figure(8), which display the select image (original) and the output for watermarking image with hidden information, while figure (9) shows the experimental images.

2.4. Objective Evaluation Measurements:

Mean Square Error Module, Peak Signal to Noise Ratio (PSNR) and Distortion Measurement were used on all experimental images (Postage Stamps) for evaluation, Table (1), it can be concluded that the proposed method of watermarking is preferable, since it produces less MSE , distortion values and more PSNR value, The greatest advantage of the proposed method is it can hide an image of equal size of cover image.

2.4.1. **Mean Square Error Module**

One important performance measure is fidelity. Fidelity is the perceptual similarity between the original image and the watermarked image. We currently measure the fidelity in terms of Mean Square Error (MSE). Mean Square Error is obtained as follows:

$$MSE = \frac{1}{MN}\sum_{I=1}^{M}\sum_{J=1}^{N}(P(i,j)\hat{p}(i,j))^2 \quad \ldots\ldots. (14)$$

Where M is the number of color components, N is the number of pixels; p is the original image (cover image) and $\hat{p}$ is the watermarking image. We implemented a plug-in that takes two same size images as input, and outputs the mean square error and the difference image. It is most easily

defined via the mean squared error (MSE) is defined as the equation (14); MSE is the average summation of the squares of the difference between the relative positioned pixels of cover & watermarked images. An image that has less MSE value is more preferable for transfer of the secret text. By this, minute errors can be detected easily by MSE.

2.4.2. Peak Signal to Noise Ratio (PSNR)

The phrase peak signal-to-noise ratio ,For color images with three RGB values per pixel, the definition of PSNR, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the (or codec type) and same content. PSNR is very common in image processing.Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, where higher is better. When the two images are identical, the MSE will be equal to zero, resulting in an infinite PSNR

The equation (15); displays the PSNR (peak signal-to-noise ratio) between two images. The answer is in decibels (dB). A sample use is in the comparison between an original image and a coded/decoded image.

$$PSNR = 10 \times \log_{10}\left(\frac{L}{MSE}\right)^2 \quad \ldots (15)$$

Where

L is the peak signal value of the cover image. *PSNR* is usually expressed in terms of the logarithmic decibel scale. It is the square of ratio of maximum pixel value i.e. 255 to the *MSE* value. Images having high *PSNR* value are preferable. A little color distortion (even with a higher *PSNR* value) could be apparently appeared on resulting mixed images.

2.4.4. Distortion measurement

The difference between cover and watermarked image is referred to as embedding distortion. In the present research more than (60) postage images were detected without distortion after hiding information. The distortion is usually introduced by the embedding process. The allowable change introduced by embedding may be smaller, sometimes, much smaller.

The Distortion measurement between the cover true color bitmap image (original image), and the watermarking image (hidden information), can be computed as the difference between the blue components value of the relative positioned pixels in watermarked and cover images respectively, as shown in Eq.(16). Then by computing the summation of all difference values of blue components in watermarked image Eq. (17), and finally dividing it by the size of image, Eq. (18), the value obtained must be very low (less than 1).

$$diff = value\_blue_w - value\_blue_{cover} \quad .. (16)$$

$$sum\_diff = \sum_1^N diff \quad \ldots (17)$$

$$disoration = \frac{\sum_1^N diff}{256 * 256} \quad \ldots (18)$$

2.5. Attack with JPEG ompression Techniques and Enhancement Filter.

Image processing and transforming are commonly employed to create and apply watermarks.

Objectives of attacks against watermarks and embedded information include rendering a watermark unreadable, revealing the existence of hidden information, or confusing the reader as to the authenticity of the watermark. Attacks on watermarks may be accidental or intentional. Testing the robustness and security of a data hiding system via attacks is as important as the design process and can be viewed as its inseparable element in a broad sense.

In this paper, two methods are used to attack the watermarking image, these methods are:

1. JEPQ Compression.
2. Mean Filter.

Many owners of watermarked works do not want the watermark to interfere with the use of the work by others. They therefore require that the watermark be imperceptible to the human sensory system. This requirement works against the robustness of a watermark. Attacks on transform watermarks are typically aimed against the watermark reader .An attack may be to replace, remove, or distort watermark, and an attack may cause the reader to recognize a forged or counterfeited watermark, Images may also be altered so the reader cannot see a watermark at all. Attacks on watermark may not necessarily remove the watermark, but disable its readability. The performance of the presented scheme is evaluated after JPEG compression, geometrical attack and transformations. The proposed approach can be applied to compress image using JPEG or other compression techniques, and the watermarked image can be kept in the compressed format, by using the level (or threshold) to represent the (0 or 1) of the water marking embedded information, is robustness, because the information was kept in image and not removed or change. But when the L.S.B is used to insert the embedded information, the value of blue component for pixels may be removed or changed, meaning that the information is lost.

Decompression the image after JPEG compression and transforming into bitmap image, leads to easily detecting the watermark. The compression method would change all pixels element in image. And the watermarking system should still be able to detect and extract the watermark. But the experimental results were good for most of the postage stamp images as shown in figures (10, 11 and 12); they differ in the quality factor (the quality factor represents the percentage of lost information to the total information after JPEG compression).

The tested image which can be extracted without error even when the image is JPEG compressed. The embedding rate can be higher for images containing more complex contents. The image with lower PSNR is stronger in watermarking for images with more textures.

Another method applied to the experimental image by using the mean filter to attack the algorithm for hidden information as watermarking. The mean filters are essentially averaging filters. They operate on local groups of pixels called neighborhood and replace the center pixels with an average of pixels in this neighborhood. This replacement is done with a convolution mask such as the following 3*3 mask: as shown in Eq.(19).

$$\begin{bmatrix} 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \end{bmatrix} \quad \ldots\ldots (19)$$

The mean filter method would lessen the change of all pixels element in image as shown in figures (14 and 15 with different mask). This attack could cause much distortion in watermark signal but the method used in this paper is still robust and detected the watermark successfully. The watermarking system should still be able to detect and extract the watermark. The experimental results were acceptable for most of the stamp image, neglecting all the effects of the filter on the image such as blurring it or changing its brightness, the mean filter used was a linear filter and with different window sizes [12].

2.6. The Algorithm of Decoding Watermarking

The detector tries to decode the hidden data using least significant bit for blue component in watermarked image or using the threshold to embed data on the postage stamp image and compare it with the cove image (original image). The decoded bits are approximately independent of each other and are "1" or "0". If the total number of bits for representing an image do not change during the embedding process, one bit is logically reallocated from representing the image to representing the embedded data, even though there may be more than one bits physically related to the embedded data.

An important characteristic of an image-based watermark should be robust to common image processing and compression techniques, as with many watermark verification techniques, this method requires the availability of the original image for comparison. There are two major classes of detection in a watermarking system: blind detection, which does not need the original image for detecting the mark and non-blind detection that uses the original image in the detection process. A new non-blind watermarking scheme is proposed for true color bitmap image as shown in figure (13 and 14).

A technique was used which embeds data into a color true image by modifying the least-significant bits (LSB) of the image. The insertions watermark or embedded bit is related to the LSB (least significant), was weak in the attack process, using the JPEQ compression caused to the loss of the [LSB], in this case saving it three times helps in ignoring the bad case regarding losing or changing the information as water marking; the proposed method gave results that 80% of the water marking embedded

information could be detected and read.

Using the other method (level or threshold generally set between (3 and -3)) for a maximal detection, the marked image was then compressed using JPEQ compression. If the result in decoding algorithm for threshold or level from subtracting the value of blue component corresponding to the stamp cover image (original stamp image) from that of the watermarking stamp image, was positive integer as shown in equation(20), (the positive part represents a '1' and the negative part Represents a '0'), that means the value of threshold was one in binary number, then the bit of embedded information was (1 or white), and if the result in decoding algorithm for threshold or level was negative integer, that means the value of threshold was zero in binary number, then the bit of embedded information was (0 or black).

Then the original image must be available to make the comparison as shown in the following steps:

1. If the value of $\theta \succ$ the value of average, then there must be hidden information saved using [LSB] or threshold, then do the comparison.

2. Comparing between the original and the watermarking images for the threshold method is according to the equation (20):

Level $_{[threshold]}$ = blue component $_{(w)}$ - blue component $_{(cover)}$ …...(20)

The difference between the blue components value of the relative positioned pixels in cover and watermarked images. Obtaining a sequence of bits for hidden information, then easily transforming it into bytes, the information could be detected and readable.

$0 \prec level \prec 3$ Then the bit for information hiding is $\rightarrow 1$ or

$0 \succ level \succ -3$ Then the bit for information hiding is $\rightarrow 0$

3. If the LSB method was used, then in the decoding algorithm the watermarking of hidden information for the bitmap image can be read or detected, when receiving the stamp image to the receiver, using the algorithm for decoding, the blue component of pixels in stamp image can be detected as the equation (21), if the result was (1) in binary number then the bit of the embedded information must be one and otherwise for (0) in binary number.

$$value_{bit} = value\ of\ blue\ component \bmod 2 \quad \ldots.(21)$$

3. Conclusion and Future Work

In this paper, a new color image watermarking method is proposed, by using the analytic geometric for three channel of pixels (Red, Green, Blue) for cover image (original image); and watermark information was embedded invisibly in all the blue components of the cover color image. The watermarking technique works for true bitmap color images at image size 256*256; with (60) experimental postage images.

After completing the entire watermarking process, image watermarking is robust to JPEQ compression. In this paper, geometrical analysis for hiding Data and watermarking system has been introduced by using methods or tools, which can show the impact of different kinds of attacks on the performance of the watermarking system.

The results of this analysis and tools provided for estimation, gave a good performance for the data hiding and watermarking schemes,

The experimental results show no visible distortions in the watermarked images and hidden information was still even with 85% lossy JEPQ compression.

There are still many open research problems in the field of watermarking for image. A theoretical approach to the study of watermarking techniques will produce immediate benefits, as shown in this paper.

References

[1] Neil F. Johnson1, Zoran Duric2, Sushil Jajodia1 "A Role for Digital Watermarking in Electronic Commerce", Center for Secure Information Systems,George Mason University, http://isse.gmu.edu/_csis, Accepted for publication ACM Computing Surveys in January 1999. Publication TBA.

[2] Min Wu "multimedia data hiding", a dissertation presented to the faculty of Princeton University in candidacy for the degree of doctor of philosophy recommended for acceptance by the department of electrical engineering June 2001, Copyright 2001 by Min Wu All rights reserved.

[3] Fernando P´erez-Gonz´alez and Juan R. Hern´andez "A tutorial on digital watermarking",Dept. Tecnolog´ıas de las Comunicaciones, Jan 2009

[4] Neil F. Johnson2, Zoran Duric1, and Sushil Jajodia2" Recovery of Watermarks from Distorted Images", Center for Secure Information Systems ,George Mason University, http://ise.gmu.edu/csis, 1 October 1999.

[5] P. Bas, J-M. Chassery and B. Macq; P. Bas, J-M. Chassery: "Geometrically Invariant Watermarking UsingFeature Points" This work was supported by the European IST Aspis project and the National RNRT Aquamars project, Nov 2002

[6] Hyung Cook Kim, Hakeem Third edition 1982, pages (562-564).

[10] Purple math company Ogunleye, Oriol Guitart and Edward J." The Watermark Evaluation testbed (WET)", University,West Lafayette, Indiana USA, this work was supported by the Air Force Research Laboratory, Information Directorate, 2004.

[7] http://en.wikipedia.org/wiki/ Examples_of_Mathematical_mod el

[8] http://www.tpub.com, " Distance between two points"

[9] Sherman k. stein, McGraw hill companies,"calculus and analytic geometry",

, "Slope of a Straight Line", http://www.purplemath. com/modules/slope.htm

[11] "Purple Math Company, "slop formula", http://cs.selu.edu/~rbyrd/math/slope

[12] scott EUmbaugh,ph.D.Prentice Hall PTR,Upper Saddl River ,NJ O7458,Computer Vision and image processing,pages (51-52),1993

Table (1): Shows the Watermark Objective Evaluation Test (WOET) in some of Experimental Postage Stamps Images

Name of stamps image	MSE	PSNR	DISTORSION
Bu-1	**0.020915**	**56.926317**	**0.000437**
Bu-2	**0.020670**	**47.926317**	**0.000437**
Bu-3	**0.021036**	**54.901213**	**0.000443**
Bu-4	**0.019531**	**65.223503**	**0.000381**
Face-man1	**0.021749**	**47.756395**	**0.000473**
king	**0.019401**	**65.252651**	**0.000376**
cat	**0.020793**	**64.951715**	**0.000432**
H2	**0.033672**	**53.858147**	**0.001134**
Wm-1	**0.020793**	**34.951715**	**0.000432**
Wm-face2	**0.021156**	**23.876396**	**0.000448**
Face-man2	**0.021866**	**34.733170**	**0.000478**

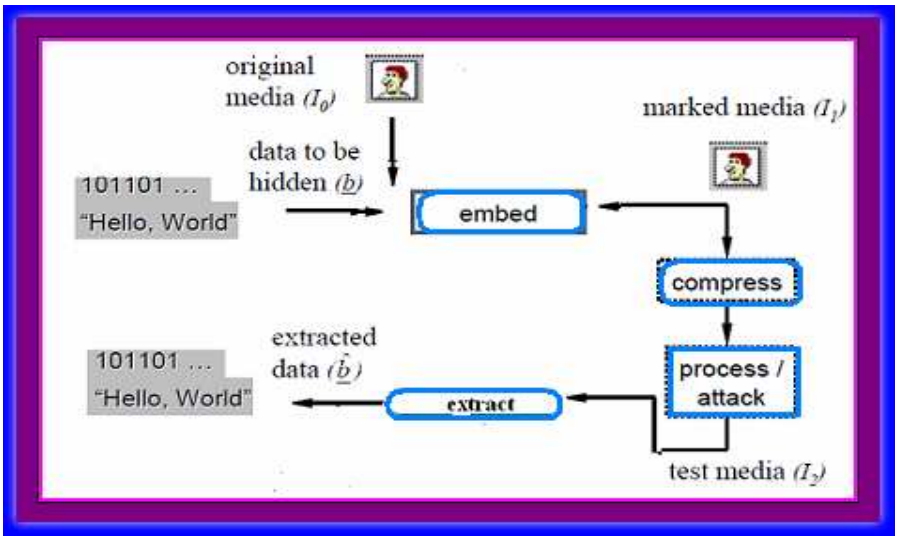

Figure (1): The Steps of General Watermarking System in **Images.**

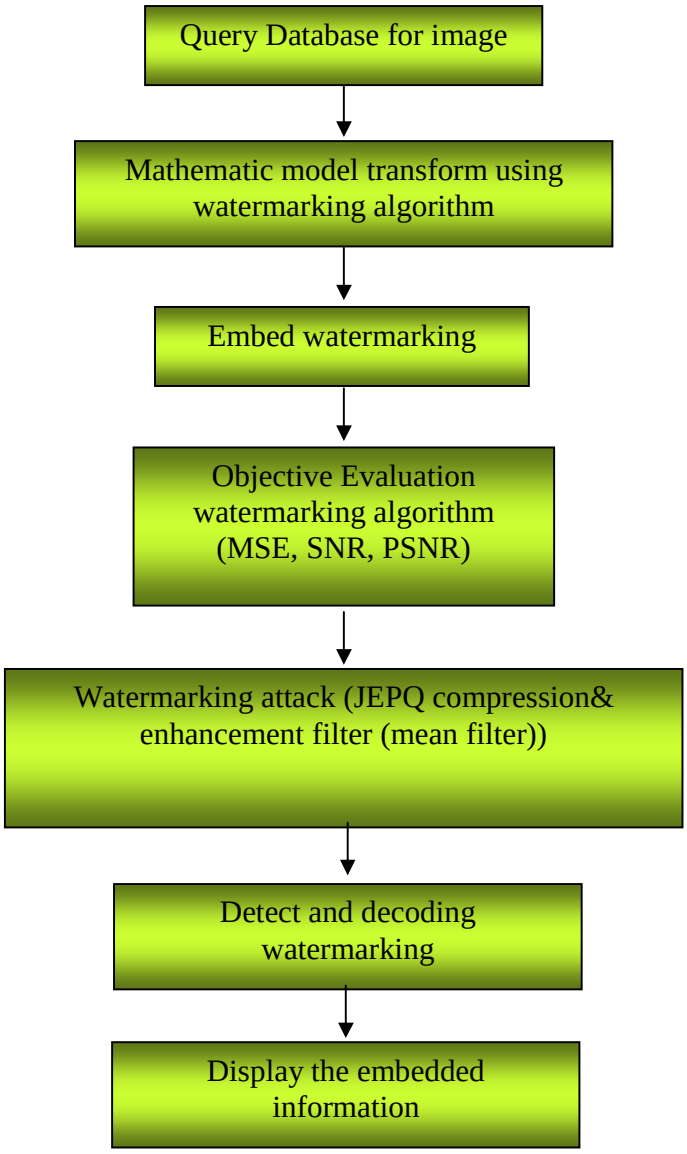

Figure (2): The Proposed Image Watermarking System

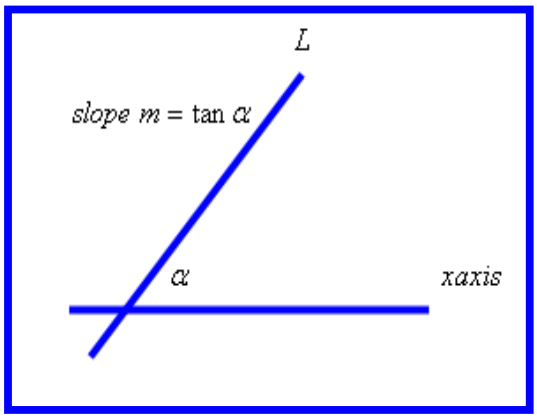

Figure (3): show the slop equation for line

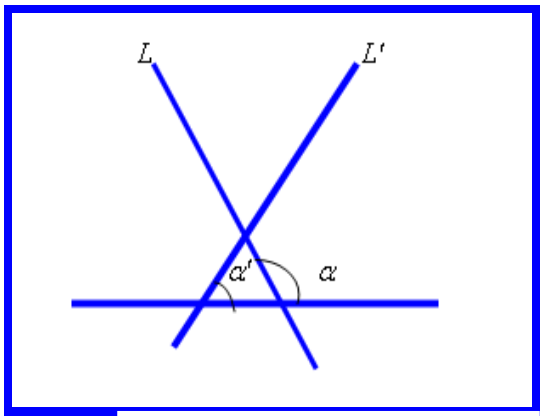

Figure (4): show the angle equation between two lines

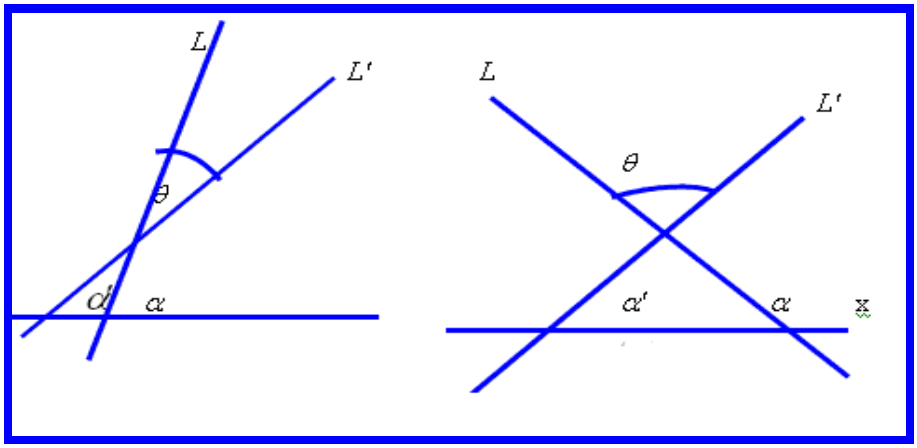

Figure (5): shows (θ) for some typical *L* and L'

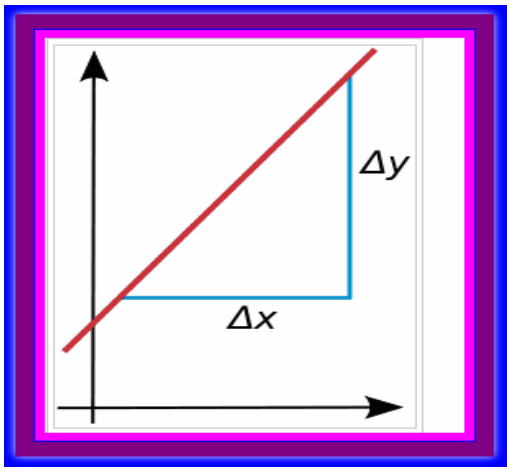

Figure (6): Explain the Slope of a Line Is Defined As the Rise over the Run, $m = \Delta y / \Delta x$

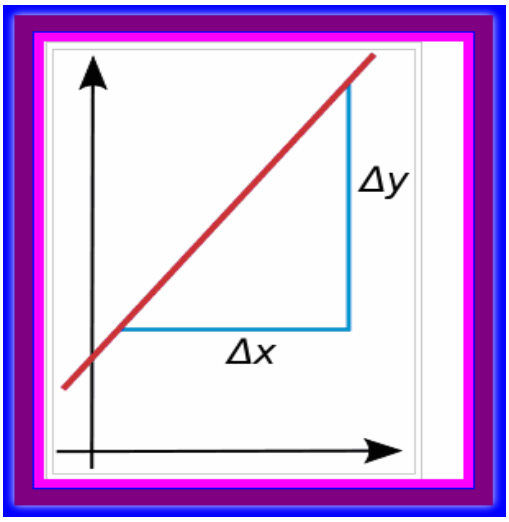

Figure (7): Explain the Slope of a Line Is Defined As the Rise over the Run, $m = \Delta y / \Delta x$

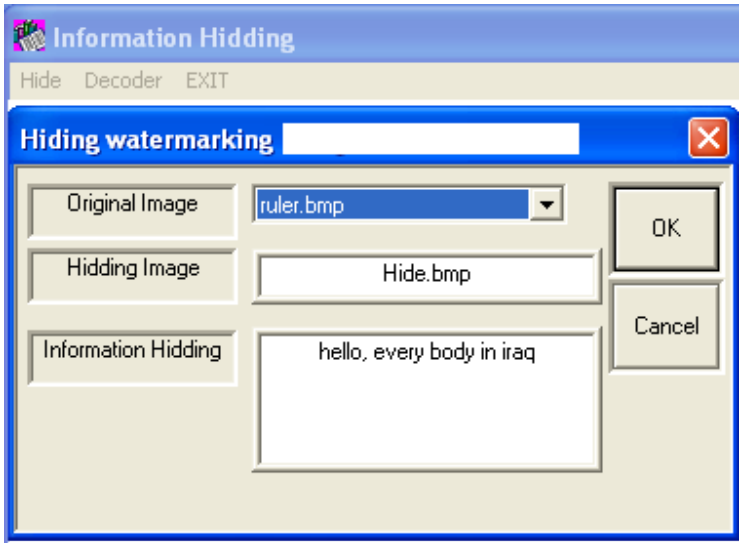

Figure (8): Shows the System Encoding Interface with Hidden Information in the Image.

Figure (9): Shows the Watermarking Performed on its RGB Components. a): Original Unmarked 256 × 256 Image , (b): Watermarked Image Stored in JPEG Format with a Quality Factor of (70%).100 characters was the embedded message.

Mj

a) b)

Figure (10): Shows the Watermarking Performed on its RGB Components. a): Original Unmarked 256 × 256 Image , (b): Watermarked Image Stored in JPEG Format with a Quality Factor of (70%).100 characters was the embedded message.

Figure (11): Examples of watermarking image after using mean filter with mask 5*5

Figure (12): Examples of watermarking image after using mean filter with mask 3*3

Figure (13): Shown the System Decoding Interface and Display the Information Hiding in the Postage Stamp Image.

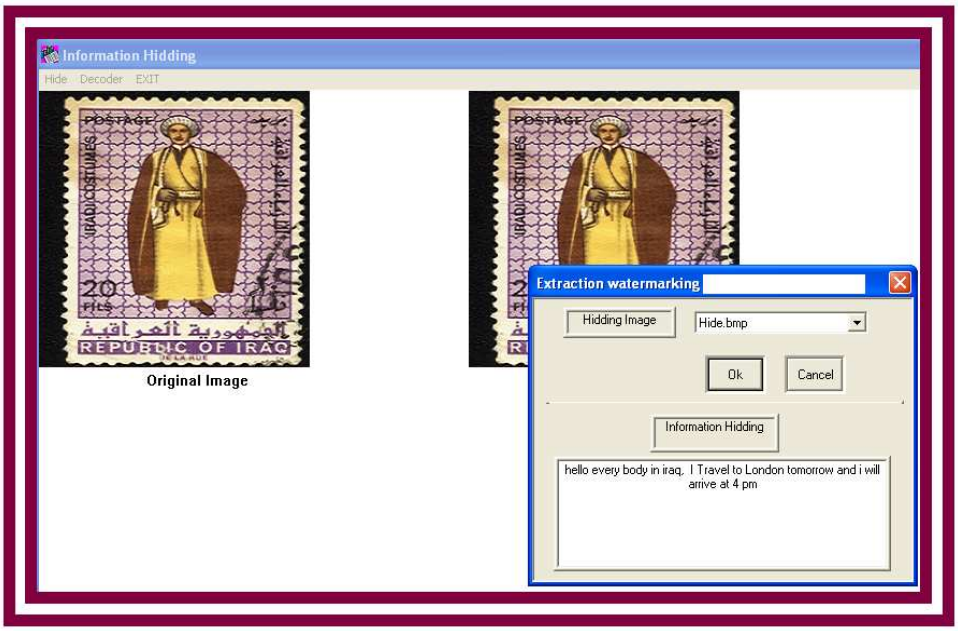

Figure (14): Shows Another Example of the System Decoding Interface and Display the Information Hiding in The Postage Stamp Image.