Implementation of Embedding and Extracting Invisible Watermarking

Mustafa Sabah Mustafa
Al-Mansour University College
Computer science department

Abstract

The protection of ownership and prevention of unauthorized tampering with multimedia data (audio, video, image and text) have become important concerns. Image authentication verifies the originality of an image by detecting malicious manipulation; the ultimate goal to the watermark is retrieve the right owner information from the received data in a correct way. Digital watermarking is the process that embeds data called watermark into multimedia object such that watermark can be detected or extracted later only with appropriate decoding mechanism.

In this work, an image is taken from color image (24 bits) type and from BMP file type and is converted into gray scale image (256 bits) and then converted into binary file by using one of filters (Sobel, Prewitt, Robert) to find edge detection of original file. Data storage process is performed in original image in edge points corresponding to the same place in a binary image. These edges are specified randomly based on location of the edge mod 3 and then specifying one of values (R, G, B) randomly to store data in it. As a result of this paper work invisible watermark is not noticeable to viewer and without any degrade the quality of the content. The product invisible watermark is robust against distortions processes and resistant to intentional tampering solely intended to remove the watermark. The embed information is repeated three times that take 2400 bits to keep on the quality image and even undistinguished in any image the watermark is embed.

الخلاصة

إن حماية الخصوصية الشخصية ومنع الأشخاص الغير مخولين من التلاعب بأوساط البيانات المختلفة (صوت ،صورة ، فيلم والوثائق) أصبح من الأمور المهمة. والتخويل الصوري هو التحقق من أصالة الصورة بواسطة اكتشاف التغيرات الماكرة بصورة عامة الهدف الرئيسي لأبحاث العلامة المائية هو استرجاع المعلومات التي تخص المالك الشرعي من المعلومات المستلمة بصورة صحيحة. العلامة المائية هي العملية التي تخفى بيانات وتدعى علامة مائية إلى أحد الأوساط المتعددة حيث العلامة المائية يمكن أن تكتشف أو تستخلص أخيرا فقط مع آلية مناسبة لاستخلاص العلامة المائية.

في هذا البحث الصورة تأخذ من نوع الصور الملونة (24بت) و يكون الملف من نوع (BMP)حيث تحول هذه الصورة إلى صورة أحادية اللون (256بت) ثم تحول إلى صورة ثنائية بواسطة استخدام أحد المرشحات التالية (sobel, prewitt, robert) لإيجاد أو كشف الحواف للصورة الأصلية. عملية خزن البيانات هي منجزة في الصورة الأصلية في نقط الحواف المطابقة

لنفس مكان الحواف في الصورة الثنائية. هذه الحواف تكون محددة عشوائيا بلإعتماد على مبدأ باقي القسمة (MOD) حيث نأخذ رقم موقع الحافة مقسوم على(MOD 3) وثم نحدد أحد قيم الألوان (الأحمر ، الأخضر ، الأزرق) لغرض خزن البيانات فيها.يستنتج من هذه الأطروحة إن العلامة المائية الناتجة هي غير مرئية وغير ملحوظة وبدون أن تؤثر على محتويات وجودة الصورة . العلامة المائية الغير مرئية الناتجة هي قوية ضد عمليات التشويه و مقاومة لعمليات التلاعب التي تهدف إزالة العلامة المائية. يتم تكرار المعلومات المخفية في الصورة ثلاثة مرات حيث تأخذ أقصى حد للخزن(2400 بت) وذلك للحفاظ على جودة الصورة ولكي لا تميز الصورة التي تم خزن البيانات فيها حيث كلما ازدادت كمية البيانات المخزونة في الصورة تزداد احتمالية كشف و تشويه هذه الصورة مما يسهل عملية تمييز هذه الصورة.

Introduction:

The growth of high speed computer networks and that of Internet, in particular, has explored means of new business, scientific, entertainment, and social opportunities. Ironically, the cause for the growth is also of the apprehension- use of digital formatted data. Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various software products have been recently introduced in attempt to address these growing concerns. It is done by hiding data (information) within digital audio, images and video files. One way of such data hiding is digital signature, copyright label or digital watermark, that completely characterizes the person who applies it and, therefore, marks it as being his intellectual property. Digital Watermarking is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. Watermarking is either “visible” or “invisible”. Although visible and invisible are visual terms watermarking is not limited to images, it can also be used to protect other types of multimedia objects [1].

Digital Watermarking:

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection [2].
Watermarking technique is to hide secret information into the digital signals so as to discourage unauthorized copying or attest the origin of the media. The watermark is a digital code embedded in the image data and is invisible. A digital watermark is permanently embedded in the data, that is, it remains present within the original data after any distortion process. A watermark could be used to provide proof of authorship of a signal.
For digital watermarking of image, a number of different characteristics of the watermarking process and watermark are desirable [3]. These requirements are:

1. Invisible: The digital watermark embedded into the image data should be invisible to the human.
2. Security: Unauthorized removal and detection of the watermark must be impossible even if the basic scheme used for watermarking is known.
3. Robustness: It should be impossible to manipulate the watermark by intentional or unintentional operations without degrading the perceived quality of the image to the point of significantly reducing its commercial value. Such operations are, for example, filtering, and blurring.

From application point of view digital watermark could be as below.
1. Source based
2. Destination based.

Also the watermark can compare between attributes as follows [4, 5].

Visible watermark	Invisible watermark

The intention is for the presence of the watermark to be very obvious but equally to make it impossible to remove without destroying the image.	Can be used for any application and also resists any detection and decoding.
Complete watermark	**Incomplete watermark**
Doesn't need the original copy for the hidden message decoding.	This scheme needs the original copy for message decoding which means that it is strongly resistant to detection and decoding.
Robust watermark	**Fragile watermark**
These are designed to withstand accidental and malicious attack.	Have just the opposite characteristics and are used to detect tampering.

General Framework for Watermarking:

Watermarking is the process that embeds data called a watermark for digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. A simple example of a digital watermark would be a visible “seal” placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material. In general, any watermarking scheme (algorithm) consists of three parts.

1. The watermark.
2. The encoder (insertion or embedding algorithm).
3. The decoder and comparator (verification or extraction or detection algorithm).

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporate the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object [2].

Requirements of digital watermarks:

Depending on the watermarking application and purpose, different requirements arise resulting in various design issues. Watermark imperceptibility is a common requirement and independent of the application purpose. Additional requirements have to be taken into consideration when designing watermarking techniques [4].

Recovery with or without the original data, depending on the application, the original data is or is not available to the watermark recovery system. If the original is available, it is usually advantageous to use it, since systems that use the original for recovery are typically more robust.

Robustness: Robustness of the watermarked image against modifications or malicious attacks is one of the key requirements in watermarking. Robust watermarking schemes can withstand common content- altering operations.

Security issues and use of keys. The conditions for key management differ greatly depending on the application [6].

Image Authentication Techniques:

In the past, several techniques and concepts based on data hiding or stegannography have been introduced as a means for tamper detection in digital image and for image authentication fragile watermarks, semi fragile watermarks, robust watermark [7, 8].

The visual redundancy of typical images enables us to insert imperceptible additional information and make the images capable of authentication themselves without accessing the originals. The goal is to prevent creating a forgery that goes undetected

Image Representation [9]:

We have seen that the human visual system receives an input image as a collection of spatially distributed light energy; this form is called an optical image. Optical images are the types we deal with everyday- cameras capture them, monitors display them, and we see them. We know that these optical images are represented as video information in the form of analog electrical signals and have seen how these are sampled to generate the digital image I(r,c).

The digital image I(r,c) is represented as a two-dimensional array of data, where each pixel value corresponds to the brightness of the image at the point (r,c). In linear algebra terms, a two-dimensional

array like our image model I(r,c) is referred to as a matrix, and one row (or column) is called a vector.
The image types we will consider are: (1) color image (2) gray-scale image (3) binary image.

Edge Detection[9]:.

Edge detection methods are used as a first step in the line detection process. Edge detection is also used to find complex object boundaries by marking potential edge points corresponding to places in an image where rapid changes in brightness occur. After these edge points have been marked, they can be merged to form lines and object outlines.
With many of these operators, noise in the image can create problems. That is why it is best to preprocess the image to eliminate, or at least minimize, noise effects. To deal with noise effects, we must make tradeoffs between the sensitivity and the accuracy of an edge detector. For example, if the parameters are set so that the edge detector is very sensitive, it will tend to find many potential edge points that are attributable to noise. If we make it less sensitive, it may miss valid edges. The parameters that we can set include the size of the edge detection mask and the value of the gray-level threshold. A larger mask is less sensitive to noise: a lower gray-level threshold will tend to reduce noise effects.
Edge detection operators are based on the idea that edge information in an image is found by looking at the relationship a pixel has with its neighbors. If a pixel's gray-level value is similar to those around it, there is probably not an edge at that point. However, if a pixel has neighbors with widely varying gray levels, it may represent an edge point. In other words, an edge is defined by a discontinuity in gray-level values. Ideally, an edge separates two distinct objects. In practice, apparent edges are caused by changes in color or texture or by the specific lighting conditions present during the image acquisition process.

Roberts Operator:

The Roberts operator marks edge points only; it does not return any information about the edge orientation. It is the simplest of the edge detection operators and will work best with binary images (gray-level images can be made binary by a threshold operation). There are two forms of the Roberts operator. The first

consists of the square root of the sum of the differences of the diagonal neighbors squared, as follows:

$$\sqrt{[I(r,c)-I(r-l,c-l)]^2+[(I(r,c-l)-I(r-l,c)]^2} \quad \text{.....(1)}$$

The second form of the Roberts operator is the sum of the magnitude of the differences of the diagonal neighbors, as follows:

|I(r,c) - I(r-l,c-l)| + |I(r,c -l) - I(r-l,c)| .....(2)

The second form of the equation is often used in practice due to its computational efficiency- it is typically faster for a computer to find an absolute value than to find square roots.

Sobel Operator:

The Sobel edge detection masks look for edges in both the horizontal and vertical directions and then combine this information into a single metric. The masks are as follows:

ROW MASK

$$\begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix}$$

COLUMN MASK

$$\begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}$$

At each pixel location we now have two numbers: s1, corresponding to the result from the row mask, and s2, from the column mask. We use these numbers to compute two metrics, the edge magnitude and the edge direction, which are defined as follows:

EDGE MAGNITUDE

$$\sqrt{s_1^2 - s_2^2} \quad \text{.....(3)}$$

EDGE DIRECTION

$$\tan^{1}\left[\frac{s_1}{s_2}\right] \quad \text{.....(4)}$$

The edge direction is perpendicular to the edge itself because the direction specified is the direction of the gradient, along which the gray levels are changing.

Prewitt Operator:

The Prewitt is similar to the Sobel, but with different mask coefficients. The masks are defined as follows:

ROW MASK COLUMN MASK

$$\begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

These masks are each convolved with the image. At each pixel location we find two numbers: p1, corresponding to the result from the row mask, and p2, from the column mask. We use these results to determine two metrics, the edge magnitude and the edge direction, which are defined as follows:

EDGE MAGNITUDE = $\sqrt{p_1^2 + p_2^2}$ …… (5)

EDGE DIRECTION = $\tan^{-1}\left[\frac{p_1}{p_2}\right]$ …….. (3.6)

As with the Sobel edge detector, the direction lies 90o from the apparent direction of the edge.

The Mean Filter:

The mean filters are essentially averaging filters. They operate on local groups of pixels called neighborhoods and replace the center pixel with an average of the pixels in the neighborhood. This replacement is done with a convolution mask such as the following 3x3 mask:

$$\begin{bmatrix} 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \end{bmatrix}$$

Note that the coefficients of this mask sum to one, so the image brightness will be retained, and the coefficients are all positive, so it will tend to blur the image.

Threshold:

After the edge detection operation has been performed, the next step is to threshold the results. One method to do this is to consider the histogram of the edge detection results. Often, the histogram of an image that has been operated on by an edge detector is unimodal (one peak); so it may be difficult to find a good valley. This method works best with a bimodal histogram. Another method that provides reasonable results is to use the average value for the threshold.

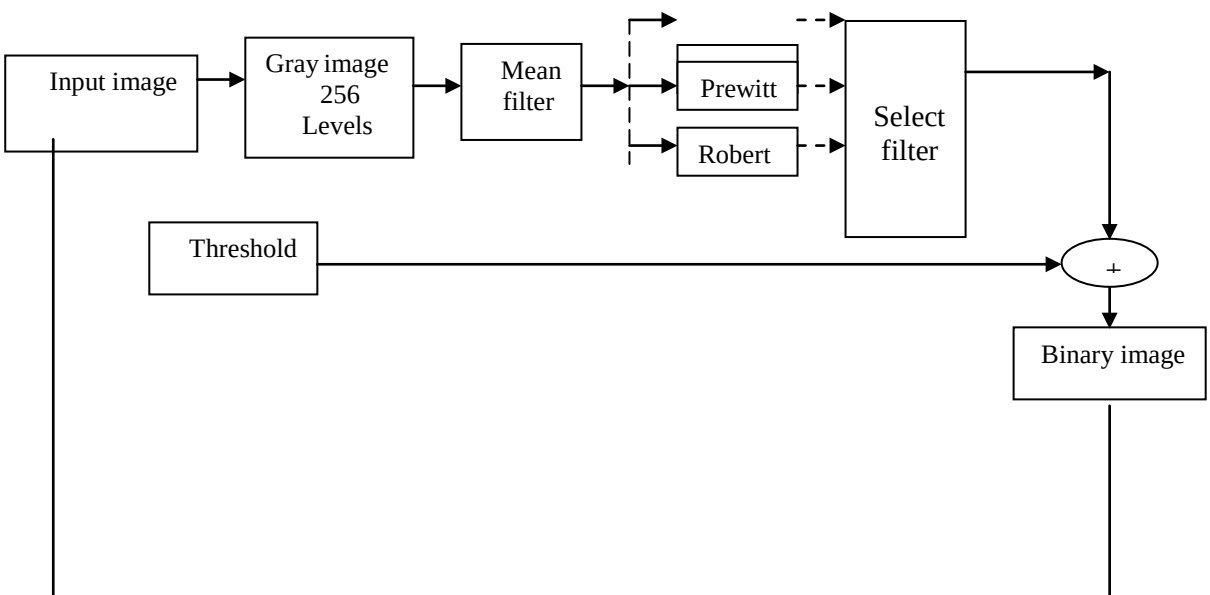
After we have determined a threshold for the edge detection, we need to merge the existing edge segments into boundaries. This is done by edge linking. The simplest approach to edge linking involves looking at each point that has passed the threshold test and connecting it to all other such points that are within a maximum distance. This method tends to connect many points and is not useful for images where too many points have been marked; it is most applicable to simple images [9]. Use following equation to compute threshold.

$$T = \frac{\sum_{I=0}^{N}\sum_{J=0}^{M}\left(X_{ij}, Y_{ij}\right)}{Z} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(7)$$

Where T is threshold and N is number of row and M is number of column and (Xij ,Yij) pixels values to the image and Z is size of image (N*M).

System Implementation

This paper will focus on the implementation of watermark embedding process and watermark extracting process. Data storage process is performed in original image in edge points corresponding to the same place in a binary image. These edges are specified based on location of the edge point mod 3 and then specifying one of values (R, G, B) to store data in it. Figure (1) shows the block diagram for watermark embedding process.



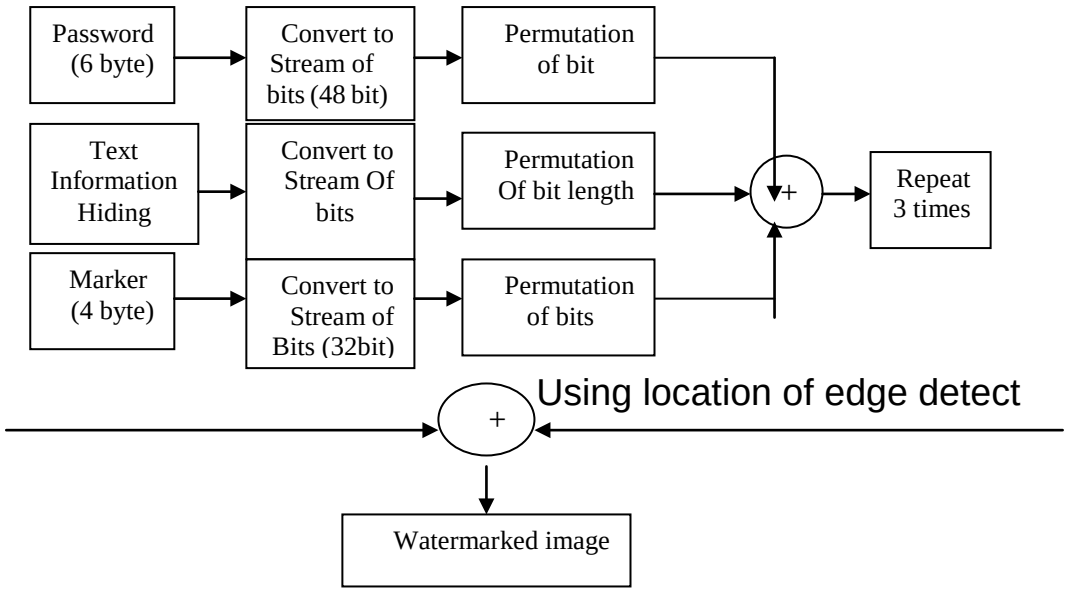
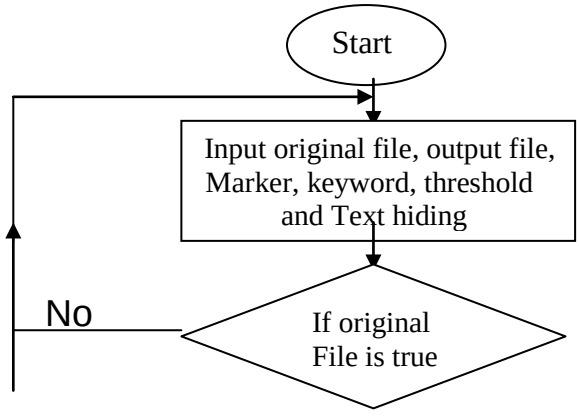


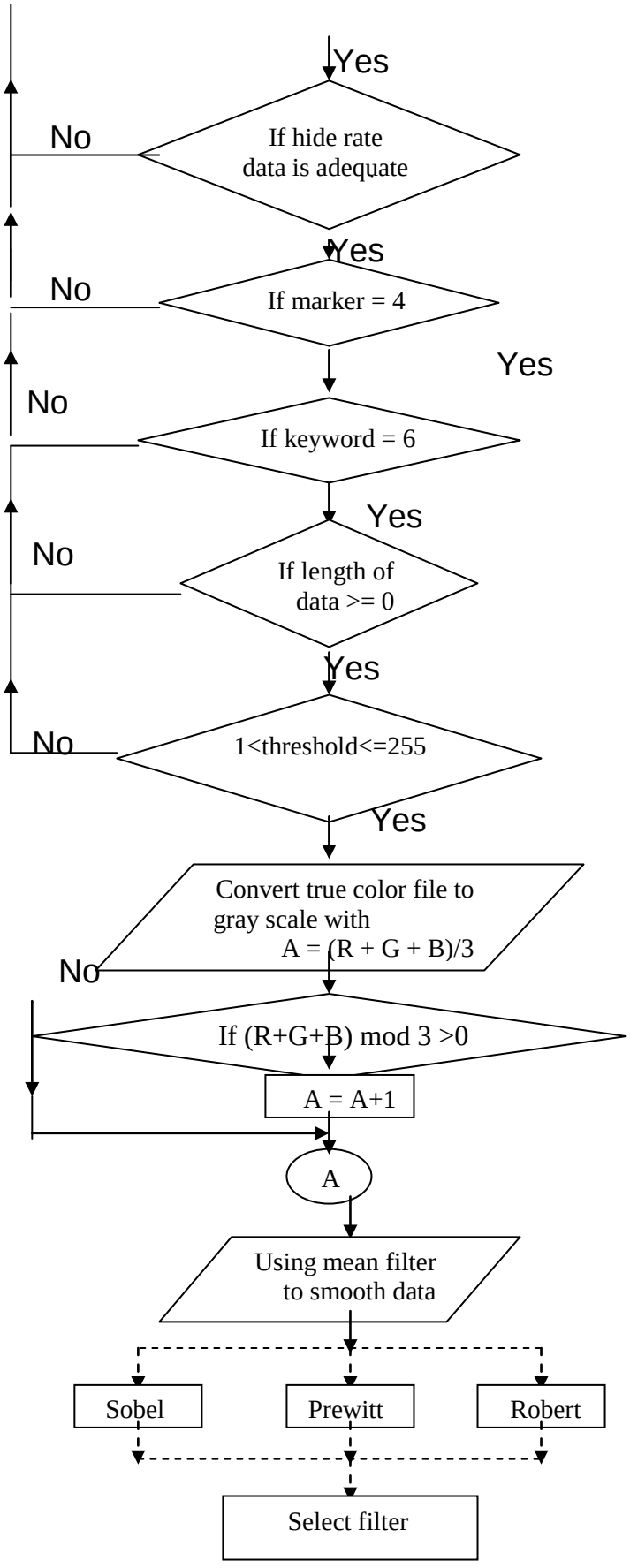
Figure (1): The block diagram for watermark embedding process.

Watermarked Embedding Process:

To generate a watermark first an image from type bmp (24 bit) must be available and then we perform the following steps. Figure (2) shows the flowchart of the embedding process.

1- Convert the true image from (24 bits) into grayscale (256 bits).
2- Use the mean filter to remove noise from the gray scale image.
3- Find edges detection of the original image by selecting one of filters (Sobel, Prewitt, Robert), and then obtain binary file.
4- Then obtain on binary file available image to store data.
5- From binary file specify location of edges to store data in the same position as the edge in the original image.
6- Embed in original image (text, marker, and password) that convert it to stream of bits, store this data three times.




Yes
If hide rate
data is adequate
No
Yes
If marker = 4
No
Yes
If keyword = 6
No
Yes
If length of
data >= 0
No
Yes
1<threshold<=255
No
Yes
Convert true color file to
gray scale with
A = (R + G + B)/3
No
If (R+G+B) mod 3 >0
A = A+1
A
Using mean filter
to smooth data
Sobel
Prewitt
Robert
Select filter

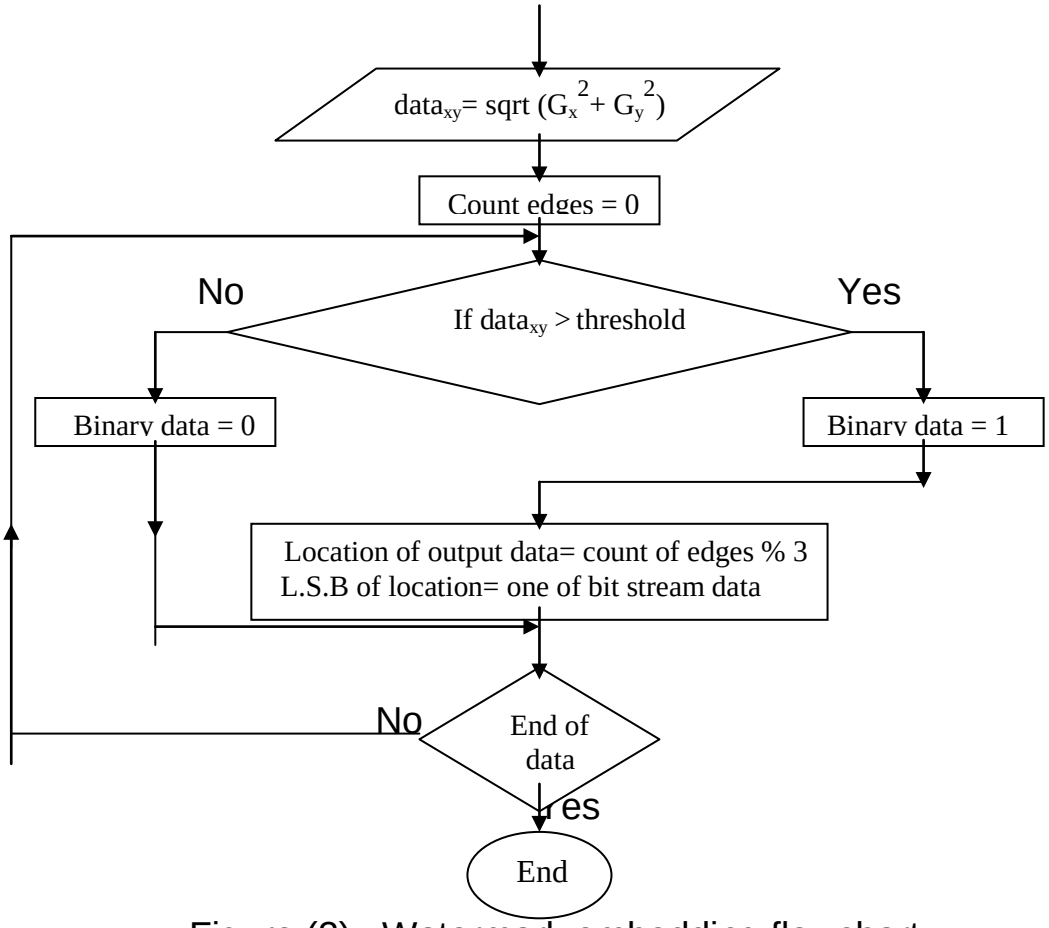


Figure (2): Watermark embedding flowchart

Result of Watermark Embedding:

Using images from true color type and from BMP file type want to convert it to watermark and storage data in it.

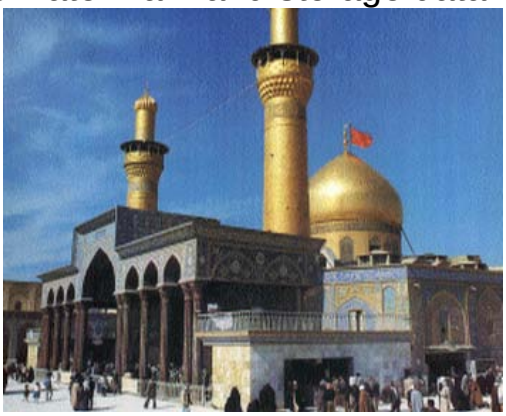


Figure (3 a): Original Al Hussein grave image 352×288×24b (298kB) bmp

Figure (3 b): Original tree image 352×288×24b (298kB) bmp
Figure (3): The original image bmp file

1. Convert the image from true color (24-bit) into gray scale (256 levels) to ready for convert into binary image.

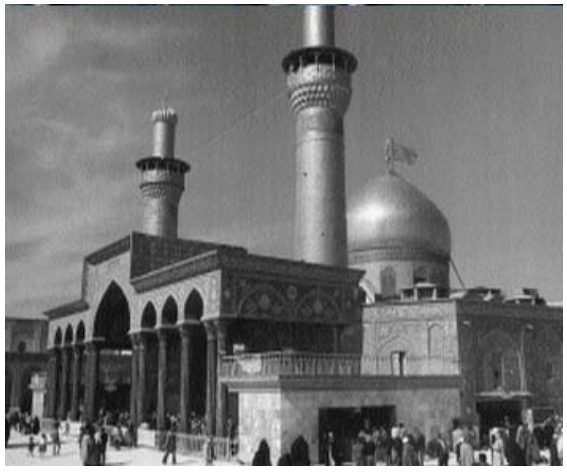


Figure (4 a): Al Hussein grave image 352×288×256(101kb) bmp

Figure (4 b): Tree image 352×288×256(101kb) bmp

Figure (4): The gray scale image

2. Convert the gray scale image into binary image by using one from three filters (Sobel, Prewitt, Robert) depending on the threshold to ready for embed information in the image.

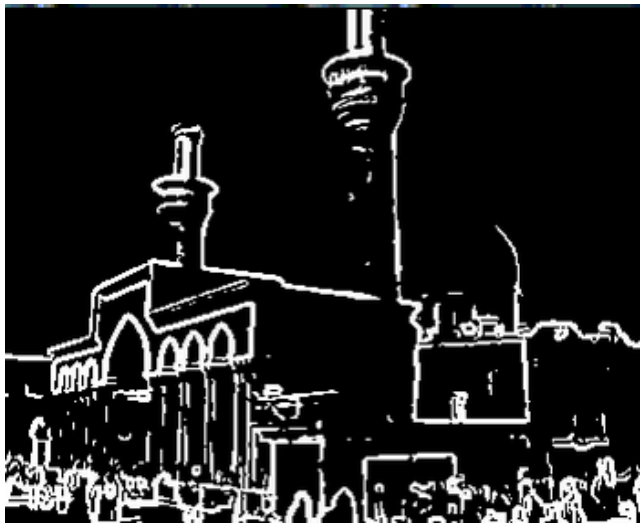
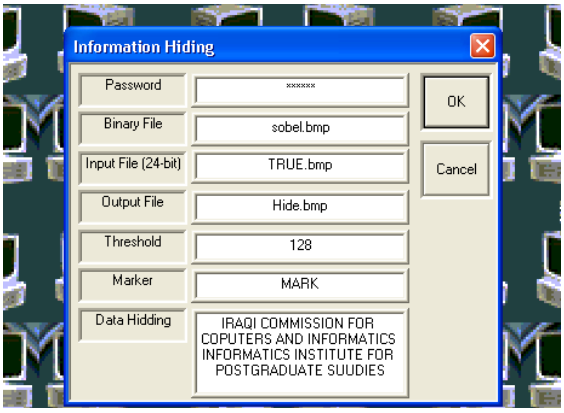


Figure (5 a): Al Hussein grave image 352×288×256(101kb) bmp

Figure (5 b): Tree image 352×288×256(101kb) bmp

Figure (5): The binary image

3. Watermarked embedding process must be contain the following information to embed information in the image:



Figure(6):The information that must be available to create the watermarked image

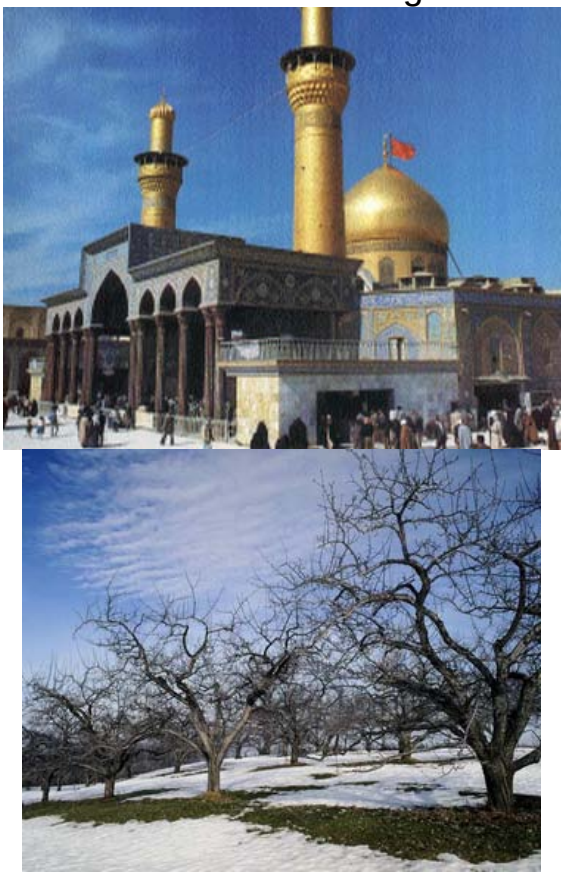
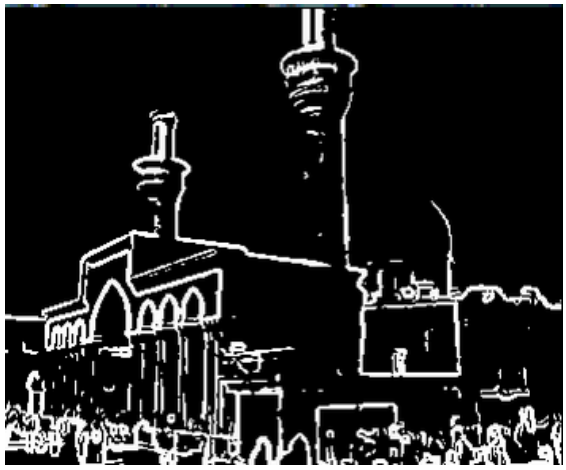
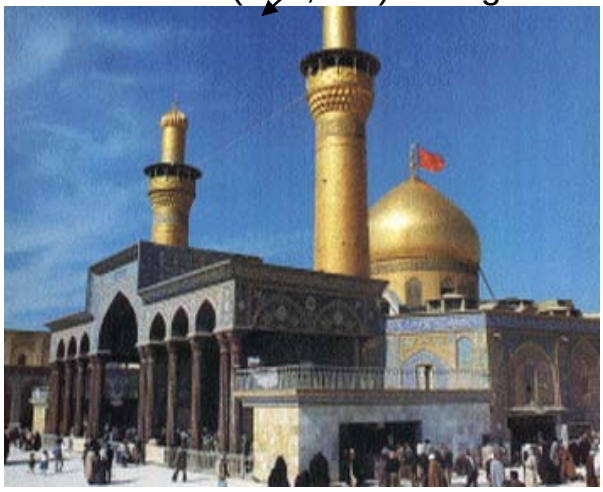


Figure (7): The hidden file 352×288×24b (298kB) bmp

Note: Two files are used in the embedded process, the first one is the BMP file to the original image and the other one is the binary file.



Point (230,249) is edge



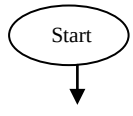
R G B

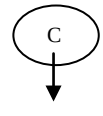
Figure (8): Illustrate the embedding process by select edge from Binary file and store only one bit in same location in original image after specified any byte from value(R, G, B) randomly to store data by using (number of edge mod 3) then select one byte from (R,G,B).

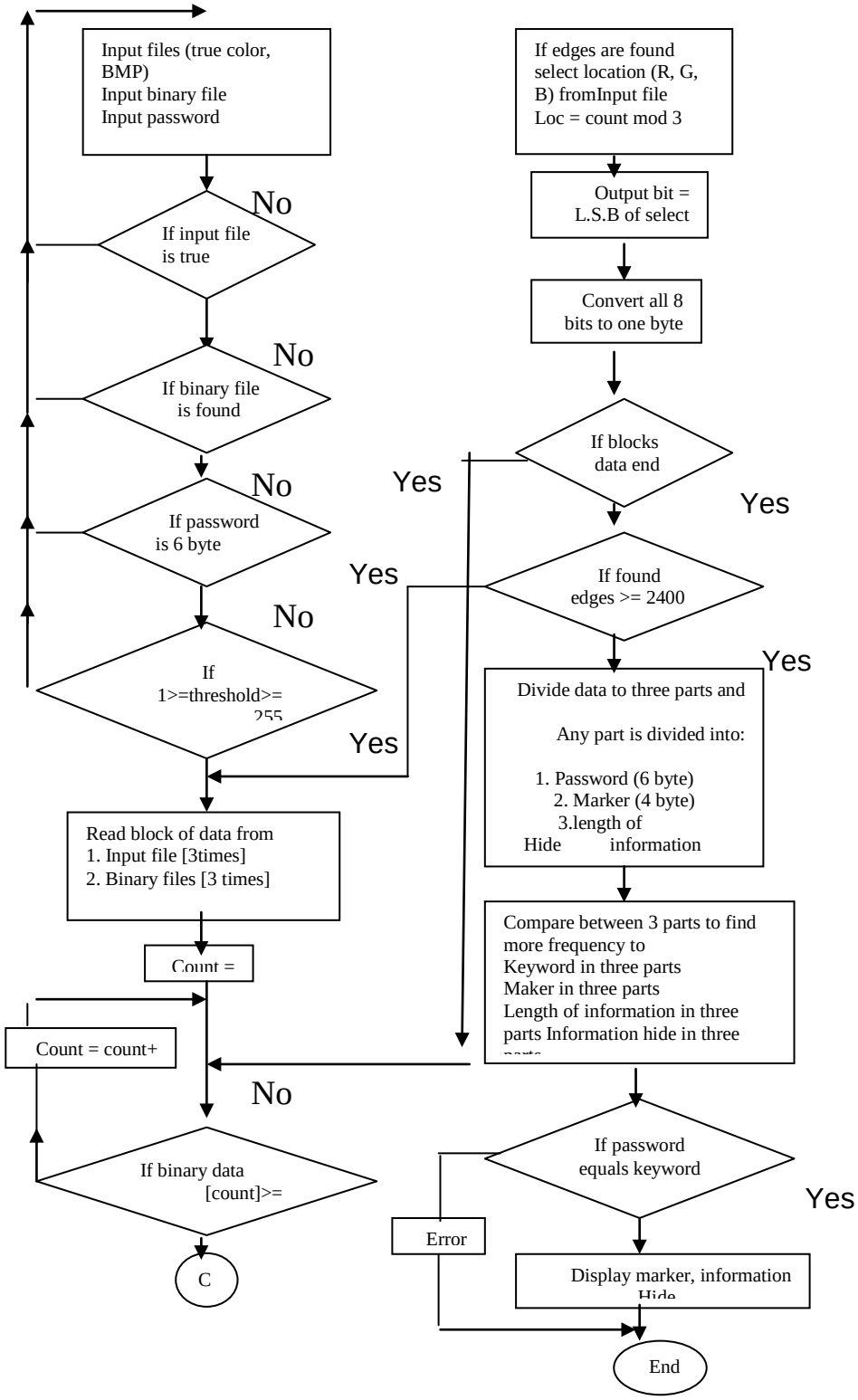
Watermark Extracting Process:

To extract the hidden information from the watermarked image the following steps must be performed. Figure (9) shows the flowchart of the extracting process.

1- The bmp to the watermarked image & binary file of the original image must be available two files.
2- The password must be known.
3- The input file must be known.
4- The binary file must be known.
5- The threshold must be known.
6- Read blocks of data (100 byte) from input file and binary file.
7- Compare password in first part with second and third parts to find the correct keyword.
8- Compare marker in first part with second and third parts to find correct the marker.
9- Compare information hiding in first part with second and third parts to find correct information hiding.
10- If this comparison is correct then give the marker and hidden information.







Result of Watermark Extracting:

1. In the extracting process two files BMP file must be available to the watermarked image and the binary file and without these files we cannot obtain the information hiding.

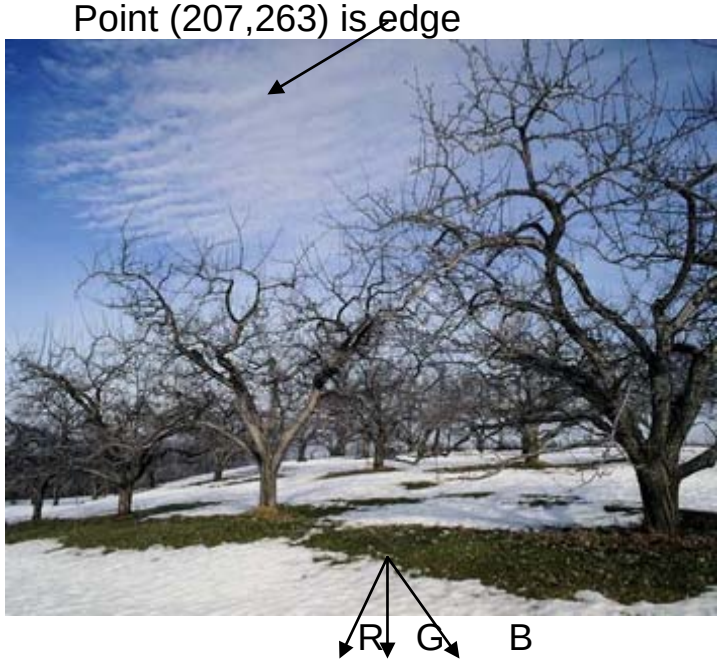


Figure (10): illustrates the extracting process by selecting edge from Binary file

and extract only one bit in the same location in hidden file after specified any byte from value(R, G, B) randomly contain data by using (number of edge mod 3) then selecting one byte from (R,G,B).

2. The following information must be entered to extract the embed information:

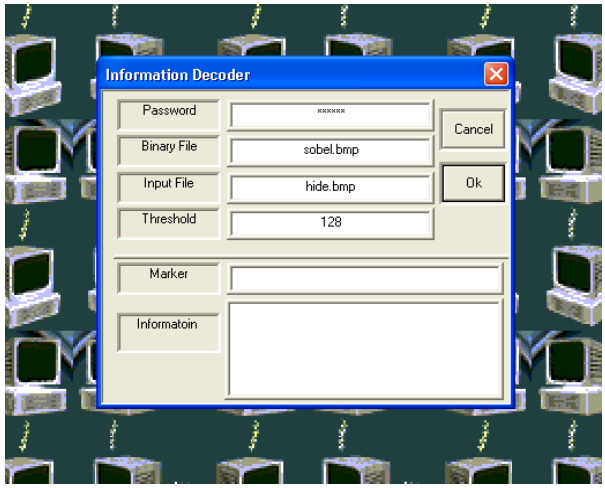


Figure (11.a): The information that must be available to obtain the hidden information.

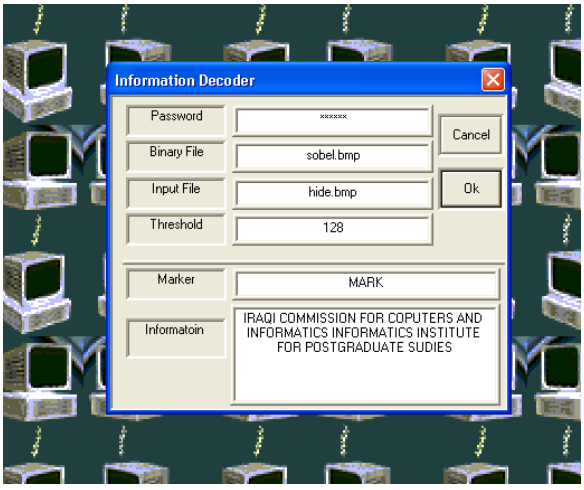


Figure (11.b): The result of the extracting process

Figure (11): Illustrates the extract information from the watermark.

Attack on the image:

The program "gws.exe" (graphics work show) is used to attack watermarked image to ensure the hidden information is not affected when convert it from BMP file format into any file format.

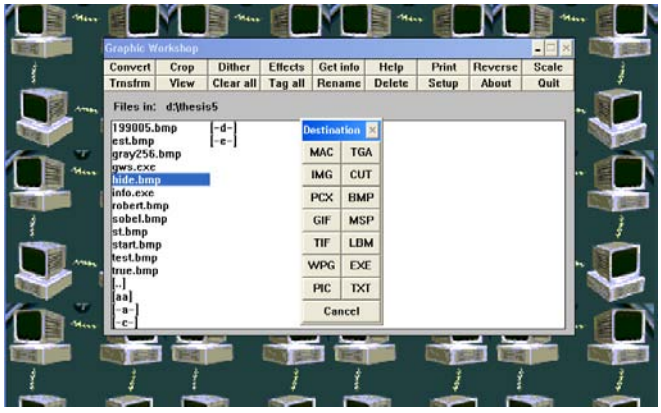


Figure (12): Illustrate convert process the BMP file into TIF file or PCX file

Example 1:

Convert watermarked image from BMP file format into TIF file format and then return it into BMP file format, in this state the hidden information didn't effect.

Figure (13.a): Al Hussein grave image352×288×24b (298kB) TIF

Figure (13.b): Tree image 352×288×24b (298kB) TIF

Figure (13): Watermarked image TIF file.

Example 2:

Convert watermarked image from BMP file format into PCX file format and then return it into BMP file format, in this state the hidden information didn't effect.

Figure (14.a): Al Hussein grave image 352×288×24b (298kB) PCX

Figure (14.b): Tree image 352×288×24b (298kB) PCX

Figure (14): Watermarked image PCX file.

Hide rate:

$$H = \frac{A}{Z} \quad \text{.....(8)}$$

Where H = Hide rate, A = Amount of embed data, Z = Size the image (N, M).

Name of image	Al-Huseen grave
Size the image	352*288
SNR	2069.097937
PSNR	72.438277
H	0.000155
ERMS	0.003709

Table: Fidelity criteria

Conclusions:

Based on the presented work the following points are put:

1. In this paper work invisible watermark is not noticeable to viewer and without any degrade the quality of the content.
2. Data storage process is based on the existence of the edges in the image. These edges or the storage location in the image is not specified but depends on characteristic of image.
3. The product invisible watermark is robust against distortions processes and resistant to intentional tampering solely intended to remove the watermark.
4. Returning information is impossible except when we know the type of used filter and used threshold value in case of converting image into binary image. In addition, we must know the password and watermarked image.
5. Watermarking provides the capability to specify the original image and ownership to this image and prevent counterfeits processes to this watermarking.

Suggestions for Future Work:

Based on the presented work the following points are put forward as future work.

1. The ability of using two filters or more which gives two binary files or more for the case of edge detection when the location of edge in the first binary file correspond to the same location of edge in second binary file. Then the location is specified to stored data in the original image.
2. Using one filter and two or more threshold values. Data storage process could be achieved after specifying the edge in the first binary file compared with same locations of this edge in the second binary file by using another threshold if the two edges were correspond in locations. After this, we are able to specify the location of data storage in the original image.

References

1. S. Katzenbeisser. F.A.P. P “Information Hiding Techniques for Steganography and Digital Watermarking” Artech House, INC., 2000.

2. Hal Berghel, “Watermarking Cyberspace”, Communications of the ACM, Nov. 1997, Vol.40, No.11, pp.19-24.

3. J.Neil, D. Zoran and J. Sushil, “Information Hiding Steganography and Watermarking“ Kluwer Academic Publishers, 2001,USA.

4. F. Jiri, “Application of Data Hiding in Digital Image“, Tutorial for ISPACS 98 Conference Melborne, Australia November 4-6,1998.

5. S.P.Mohanty, et al., “A Dual Watermarking Technique for Images”, Proc. 7th ACM International Multimedia Conference, ACM-MM’99, Part 2, pp.49-51, Orlando, USA, Oct.1999.

6. Elizabeth Ferrill and Matthew Moyer. “A Survey of Digital Watermarking". February 1999.

7. J. Fridrich, ” Method for Tamper Detection in Digital Image”, http@binghamton.edu, 2000.

8 Scott E Umbaugh, PH.D. “Computer Vision and Image Processing”. A Practical Approach Using CVIPtools. To join a Prentice Hall PTR mailing list, point to:http://www.prenhall.com/mail_list/