

*Republic of Iraq
Ministry of Higher Education and Scientific Research
Al-Nahrain University
College of Science*

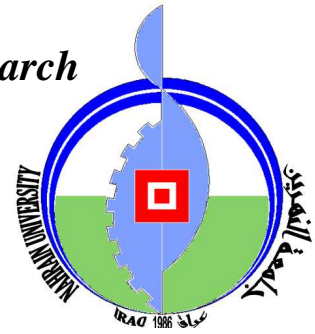


Image Authentication by Using Logo Embedding

A Thesis

*Submitted to the College of Science, Al-Nahrain University
In Partial Fulfillment of the Requirements for
The Degree of Master of Science in Computer Science*

**By
Zainab Hussain Kadhim
(B.Sc. 2005)**

**Supervised By
Dr. Ali Kadhim Mousa**

April 2008

Rabye Al-Awal 1429



جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم

وثوقية الصور باستخدام العلامة المطمورة

رسالة مقدمة الى كلية العلوم في جامعة النهرين وهي جزء من متطلبات
نيل شهادة الماجستير في علم الحاسوب

من قبل

زينب حسين كاظم

(بكالوريوس جامعة النهرين ٢٠٠٥)

أشرف

د. علي كاظم موسى

ربيع الأول ١٤٢٩

نيسان ٢٠٠٨

Supervisor Certification

I certify that this thesis was prepared under our supervision at the Department of Computer Science/College of Science/Al-Nahrain University, by **Zainab Hussain Kadhim Al-Timimi** as partial fulfillment of the requirements for the degree of Master of Science in Computer Science.

Signature:

Name : **Dr. Ali K. Mousa**

Title : **Lecturer**

Date : / / **2008**

In view of the available recommendations, I forward this thesis for debate by the examination committee.

Signature:

Name : **Dr. Taha S. Bashaga**

Title : **Head of the department of Computer Science,
Al-Nahrain University.**

Date : / / **2008**

Certification of the Examination Committee

We certify, as an examining committee, that we have studied this thesis titled "**Image Authentication by Using Logo Embedding**" presented by the student **Zainab Hussain Kadhim Al-Timimi** and examined her in its contents and what is related to it, and found that the thesis meets the standard for the degree of Master of Science in Computer Science.

Signature:

Name: **Dr. Abdul Monem S. Rahma**

Title : **Assist. Professor**

Date : / /2008

(Chairman)

Signature:

Name: **Dr. Bushra K. AL-Abudi**

Title : **Assist. Professor**

Date : / /2008

(Member)

Signature:

Name: **Dr. Abeer M. Yousif**

Title : **Lecturer**

Date : / /2008

(Member)

Signature:

Name: **Dr. Ali K. Mousa**

Title : **Lecturer**

Date : / /2008

(Supervisor)

Approved by the Dean of the Collage of Science, Al-Nahrain University.

Signature:

Name: **Dr. Laith Abdul Aziz Al-Ani**

Title : **Assist. Professor**

Date : / /2008

(Dean of Collage of Science)

Dedicated To...

My Parents

My Sisters

My Brothers

To everyone

Taught me a letter

Zainab



Acknowledgment

I would like to express my sincere appreciation to my supervisor, Dr. Ali K. Mousa, for giving me the major steps to go on to explore the subject, sharing with me the ideas in my research “Image Authentication by Using Logo Embedding” and discuss the points that I felt they are important.

Grateful thanks for the Head of Department of Computer Science, Dr. Taha S. Bashaga .

Special thank to Dr. Ban N. Thanoon for her continuous supports during the period of my studies.

Also, I wish to thank the staff of Computer Science Department at Al-Nahrain University for their help.

Finally, my very special thanks to my friends especially, M.Sc. group for their continuous supports and encouragement.

المستخلص

بات من السهولة التلاعب بالصور الرقمية باستخدام طرائق يصعب اكتشافها. في هذه الرسالة نقدم أسلوب استخدام العلامة المائية سهلة الكسر نسبياً مع الصور الرقمية الملونة في صيغتها المكانية. حيث يجري تقسيم الصورة إلى عدد من الأجزاء ، في كل جزء يجري طمر علامة وثوقية خاصة بهذا الجزء تفيدنا هذه العلامات غير المرئية لاحقاً في تحديد الأجزاء التي جرى التلاعب بها.

الهدف الأول المطلوب تحقيقه هو إيجاد أفضل عدد من التقسيمات للوصول إلى أفضل علامة مائية حيث جرى اختبار زيادة التقسيمات مع مراقبة مقياس التشوهات التي تحصل في الصورة كي يبقى ضمن الحدود المقبولة.

الهدف الثاني من البحث هو إيجاد أفضل موقع من بين المواقع الأربعة الأولى للقيمة اللونية في صيغتها الثنائية والذي يمكن استخدامه كمضيف لأحد أجزاء العلامة المائية بالشكل الذي يحقق أعلى سرية ممكنة.

الهدف الثالث هو إيجاد أفضل موديل لوني للصور يمكن أن يلائم النظام المقترح ، حيث جرى اختبار أشهر الموديلات اللونية المعروفة (RGB ، YUV ، YIQ ، YCbCr₁ ، YCbCr₂).

في هذا العمل إن الأخطاء المتولدة نتيجة التحويلات الرياضية المستخدمة للتحويل بين نظم الألوان جرى احتسابها وأخذها بنظر الاعتبار عند تقويم النتائج . بينت نتائج الاختبار أن نظام الألوان YUV يمثل الأفضل بين النظم اللونية المختبرة لإغراض إخفاء المعلومات في الصور الملونة.

في النظام المقترح يجري التحقق من وثوقية الصورة دون الحاجة إلى وجود الصورة الأصلية. بينت نتائج البحث إن الصورة المعلمة احتفظت بجودتها العالية إضافة إلى مقاومة العلامة المائية لبعض التغييرات غير المقصودة كأنواع معروفة من برمجيات الضغط (ZIP ، WINRAR) وبعض التحويلات التي يمكن أن تجري لتغيير هيئة خزن الصورة

(PDF ، PICT ، TIFF)

Abstract

It is becoming easier to tamper with digital images in ways that are difficult to detect. In this work a *semi-fragile* watermarking scheme is presented. This scheme is applied to digital color image in *spatial domain*. The image is divided into parts, each part has its authentication mark embedded in it, It would be able to be insure which parts of the image are authentic and which parts have been modified.

First objective is to find the best *number of partitions*; this achieved by increasing the number of partitions. But *Peak signal to noise ratio (PSNR)* measure should be kept in a predefined quality range, while tuning the watermark strength parameter.

Second objective is to find the best *least significant bits (LSB's) positions*, because one bit of authentication mark is embedded into one of first four LSB's according to embedding function to increase secrecy.

Third objective is to find the most suitable *color model* for the proposed system. It has been tested the most commonly used color models; *RGB, YUV, YIQ, YCbCr₁* and *YCbCr₂*.

In this work it has been taken into consideration the value of errors that generated during transformations among color models. The results show *YUV* color model is the best for information hiding in color images.

The authentication process carried out without need for the original image (*Blind method*). The results show the quality of the watermarked image remains *very good* by keeping *Mean Square Error (MSE)* and (*PSNR*) in an acceptable quality range. The proposed watermark survives some types of unintended modification such as familiar compression software like (*WINRAR* and *ZIP*) with a *high* ratio. Also it survives some types of image transformation format like (*TIFF, PICT, and PDF*).

Chapter One

General Introduction

1.1 Introduction

The digital revolution, the explosion of communication networks, and the increasingly growing passion of the general public for new information technologies lead to exponential growth of multimedia document traffic (image, text, audio, video, etc.). This phenomenon is now so important that insuring protection and control of the exchanged data have become a major issue. Indeed, from their digital nature, multimedia documents can be duplicated, modified, transformed, and diffused very easily. In this context, it is important to develop systems for authentication of content, and protection against manipulation.

On the other hand, because of the rapid development of internet, digital media has been widely distributed on the network recently. It leads to an acute need for media authentication because such digital content can be easily edited or modified by certain software or tools. As a new solution for content authentication, digital watermarking, is drawing considerable attention and has become an active research field [Cox02-1].

1.2 Watermarking

Watermarking describes techniques which are used to convey information in a hidden manner by embedding the information into some cover. Although watermarks are usually imperceptible, there are also visible watermarks. Typically, this information is required to be robust

against intentional removal by malicious parties. In contrast to cryptography, where the existence of watermarks but not their meaning should be known, watermarking aims to hide the existence of the information from any potential eavesdropper. Watermarking has existed since approximately 15th century, and in the past watermarks were mainly used on papers to identify the mill that made them. These kinds of watermarks are called physical watermarks because they exist in a physical media. Nowadays, physical watermarks are commonly used to authenticate important documents, for example, banknotes and passports.

Watermarking seems to be the alternative solution for reinforcing the security of multimedia documents. The aim of watermarking is to include subliminal information (i.e., imperceptible) in a multimedia document to ensure a security service or simply a labeling application. It would be then possible to recover the embedded message at any time. [Chr02].

Digital watermarking is a technique that embeds information into host multimedia signals in an imperceptible way and promises to be the enabling technology for intellectual property rights protection and data security [Cox02-1].

1.2.1 Watermarking Terminology [Ali04]

Over the years, researchers have coined numerous terms to describe and classify watermarking techniques. These terms are clarified in this section as follows:

1. The image into which it have been hiding the information is called the *host* or *cover data*, and the hidden information is referred to as the *payload*.
2. Most image watermarking systems involve making *imperceptible*

alterations to the host image to convey the hidden information, but there also exist *visible* watermarks, which are visible patterns (like company logos) overlaid on top of an image. However, this thesis will concentrate on *invisible* watermarks and it should be *imperceptible* to refer to *invisible* watermarks.

3. If the original, *unwatermarked* image is required in order to retrieve the watermark, the system is known as *non-blind* or *non-oblivious*, otherwise it is known as *blind* or *oblivious*.
4. Watermarking systems typically require the use of a *key* (like that used in the cryptographic sense) for retrieving the embedded *watermark*. If the *same* key as in the watermark embedder must be used for retrieving the watermark, the scheme is known as *private*, because only the person who has the key can read the watermark. If a different key is needed to read the watermark, the scheme is known as *public*. Public watermarking is sometimes also known as *asymmetric* watermarking.
5. Watermarking systems can be *robust* or *fragile*. Robust watermarks are required to resist any modifications which do not decrease the commercial value of the cover image. On the contrary, fragile watermarks are designed to fail when the cover image is modified.

1.2.2 Digital Watermarking for Images

The solution to the problem of authenticity of digital images is explored through digital watermarking. This process attempts to add some small digital structure to a host image that cannot then be perceived or removed unless by the owner. With the greater reliance on digital media in work, research, and entertainment the rather difficult question arises: how can we assign ownership to confirm the authenticity

of protected media from duplication or alteration of digital media? A large body in research has focused on techniques that embed an imperceptible symbol to the original media that will “mark” ownership of it and authenticate it [Kun97], [Pit96], and [Swa96]. This symbol is called a digital watermark.

It is important to note that watermarking is not similar to encryption because the embedding is meant to be unnoticeable [Swa96], and the original media, in this case images, are still viewable. The criteria for digital watermarking, as noted in [Cox95] and similarly elsewhere, assert that the digital watermark must be:

1. visually imperceptible within the host image so that there is no visual interference.
2. discreet or statistically invisible to prevent unauthorized removal.
3. easily extracted, and unambiguously identify the owner.
4. robust to incidental and intention distortions of the watermarked image including:
 - I. signal processing manipulations such as compression.
 - II. geometric distortions that include rotation, translation, cropping, and scaling.
 - III. subterfuge or attacks to change or destroy watermark for collusion or forgery.

As can be expected, many of the criteria seem to be in direct conflict. This fact simply brings to light the overwhelming complexity of the issue. However, in spite of the challenge, the need for copyrighting and authenticating digital work is extremely necessary in an increasing digital workplace.

1.3 Difference and Relationship between Watermarking and Steganography [Mou01]

Both Steganography and Watermarking describe techniques that are used to imperceptibly convey information by embedding it into the cover data; however steganography typically relates to convert point to point communication between two parties. Thus Steganography is not robust against modification of data, or has only limited robustness and protects the embedded information against technical modifications that may occur during transmission and storage like format conversion, compression, and digital to analog conversion.

Watermarking on the other hand, has additional notion of resilience against attempts to remove the hidden data. Thus, watermarking rather than steganography principles are used whenever the cover data is available to parties who know the existence of the hidden data and may have an interest removing it.

1.4 Authentication

In the past decade, there has been exponential growth in the use of digital multimedia contents. The wideband networks made the exchange of multimedia contents, easy and fast. On the other hand, the availability of powerful image processing tools made it easy for user to do even imperceptible changes in the original work. As a result image authenticity has become greatly threatened. [Hua05].

1.4.1 What is The Authentication?

Generally image authentication verifies the integrity of a digital image. In the past, digital watermarking gave promising solutions for

issues related to digital content authentication and copyright protection including images, audio, video and text and it is still in infancy. This area has welcomed researchers from signal & image processing, information security, computer and electrical engineering and mathematics [Min97]. Furthermore, the robustness requirements may change depending on the data type and application. Nevertheless, among all possible watermarking applications, authentication watermarks require the lowest level of robustness by definition. It should be noted that new approaches have emerged in which data attributes, such as block average or edge characteristics are embedded and check if the received image still has the same attributes. It is clear that such schemes may require a higher robustness if identification of the modified areas is of interest [Kat00].

1.4.2 Why Use The Authentication?

In authentication applications, the objective is to detect modifications of the data, this can be achieved with so called "fragile watermarks" that have a low robustness to certain modifications like compression but are impaired by other modifications.

Indeed, an active authentication scheme should have the following desirable features [Bed98]:

1. To be able to determine whether an image has been altered or not;
2. To be able to locate any alteration made on the image;
3. To be able to integrate authentication data with host image rather than as a separate data file;
4. The embedded authentication data is invisible under normal viewing conditions;

5. To allow the watermarked image be stored in lossy-compression format.

1.5 Related Work (Literature Survey)

Different techniques were developed and appeared in literature that attempt to meet most previous criteria both successfully and optimally. Various techniques are presented for digital watermarking, primarily focusing on still images. The breadth of this survey hopefully allows gaining an understanding of basic watermarking ideas from published research and the applications and needs for watermarking in real work. To give some historical perspective, the main interest in digital watermarking started in the 1990's. The main thrust of this work appears to have started around 1994 through conferences and technical reports. Traditionally, these methods have been grouped into two categories:

1. Spatial domain methods: The digital watermark is embedded into the host image without any transformation. These methods appeared first, and are still an active area of research. Of these, [Wal95], [Pit96], [Fri99], and others, fall into this category. Most use a (LSB) technique to embed the watermark into the least important parts of the host image to minimize detection.

2. Transform domain methods: The host image and watermark are transformed to a different domain (frequency, wavelet, etc.) before embedding. These techniques vary greatly. Some are styled after spread spectrum communications and DCT transforms [Cox95], and DCT transforms [Fri99]. On the other hand, still other watermarking schemes

use the discrete wavelet transform (DWT) domain to embed the watermark [Kun97], [Lin 98].

As noted previously, spatial domain methods embed the watermark directly into the host image pixels. The techniques proposed are:

1. Walton, (1995), [Wal95], presented an early scheme for image authentication where checksums of image are computed in combination with a seal, The proposed algorithm consists in selecting, according to a secret key, pseudorandom groups of pixels. The checksum value is obtained by summing the numbers determined by the 7th most significant bits (MSB) of selected pixels. Then the check-sum bits are embedded in the LSB. Then it generates the watermark that votes for authentication later on.
2. Pitas, (1996), [Pit96], proposed a technique based on ideas from statistics processes. The process first splits the original image's pixels into two equal subsets, one (A) to contain the watermark and the other (B) does not. Then, to the watermark subset, (A), an integer factor (k) is added to the pixel values, creating a new subset, (C). The constraints on choosing the integer value (k) have to take into account visibility of the watermark, and so it should be small compared to the pixel value it is to be added to detect the watermark, the means and variances of (B) and (C) are calculated and compared to a threshold.
3. Wolfgang, et al (1996), [Wol96], suggested Block-based watermarking which techniques consist in dividing the image into

blocks of about 64×64 pixels and inserting a “robust” mark into each block. To check the integrity of an image, the authenticator tests the presence or absence of the mark in all blocks. If the mark is present with a high probability in each block, we can affirm that the tested image is authentic. The variable-watermark two-dimensional technique (VW2D) is based on the principle described previously. A binary watermark $W(b)$ is embedded in each block b of an image X . to generate the mark. The use of m - sequences is justified by the fact that they have excellent auto-correlation properties, as well as a very good robustness with noise addition.

4. Yeung, et al (1997), [Yeu97], proposed an efficient and easily computed method that embeds a binary logo in an image in order to detect possible alterations in the image and at the same time provide some information about the image owner.

5. Rey, et al (2000), [Rey00], point out that the basic idea of Feature-based-watermark method consists in first extracting features from the original image, and hiding them within a robust and invisible watermark. Then, in order to check whether an image has been altered, its features are simply compared with those of the original image recovered from the watermark. If the features are identical, this will mean that the image was not tampered with, otherwise the differences will indicate the altered areas. The choice of image features used will directly affect the type of image alterations to be detected. Additionally, those features will depend on the type of image under consideration (paintings, satellite images, medical images, and so on). The features are typically selected so that

invariant properties are maintained under weak image alterations (lossy compression) and broken for malicious manipulations. These features could be also used to partially restore the tampered regions of the image. Typical features used to provide image authentication are edges, colors, gradient, luminance, or combinations of these features.

6. Gilani, et al (2006), [Gil06], proposed a semi-fragile watermarking scheme for color image authentication. In this particular scheme, the color image is first transformed from RGB to YST color space, The Y channel corresponds to the luminance component while S and T channels correspond to the chrominance component of color image. It is suitable for watermarking the color media. Each channel is divided into 4×4 non-overlapping blocks and its each 2×2 sub-block is selected. The embedding space is created by setting the two LSBs of selected sub-block to zero, which will hold the authentication and recovery information.

In the transform domain methods the host must be transformed to one of transform domain methods before any embedding process. These techniques are as follows:

7. Lin, et al (1998), [Lin 98], proposed wavelet-based image authentication. The principle of the Lin and Chang method consists in first choosing a wavelet basis and a pseudo-noise pattern (e.g., a 16×16 pixels pattern spatially repeated in the horizontal and vertical directions) selected according to a secret key. The image is then decomposed into four sub-bands, LL, LH,

HL, and HH, using the previously designated wavelet basis. The HH sub-band is substituted by the pseudo-noise pattern. Lastly, the watermarked image is obtained after applying the inverse wavelet transformation. Note that the embedding process changes only the HH sub-band of the image (i.e., high frequencies) and that it does not introduce important visual degradation to the image.

8. Fridrich, et al (1999), [Fri99], proposed an original method for self-embedding an image into itself as a mean of protecting the image content. This method also allows the regions of the image that have been tampered with, cropped, or replaced, to be partially repaired. The basic principle of this method is to embed a compressed version of the image into the LSB of its pixels. As in all watermarking methods based on LSB embedding of the watermark, this method does not introduce visible artifacts. The algorithm consists in dividing the image into (8×8) blocks, setting the LSB of each pixel to zero and then calculating a DCT (discrete cosines transform) for each block. The DCT matrix is quantified with the quantization matrix corresponding to a 50% JPEG quality. The result is encoded using only 64 bits and the code is inserted into the LSB of another block. The watermarked block must be sufficiently distant from the protected block to prevent simultaneous deterioration of the image and the recovery data during local image tampering. The quality of the recovered regions of the image is somewhat worse than a 50% JPEG quality, but sufficient to inform the user of the original content of these areas.

9. Lin, et al (2000), [Lin00], proposed a semi-fragile watermarking algorithm that accepts JPEG lossy compression and rejects malicious attacks. They have highlighted and shown two invariance properties of DCT coefficients with respect to JPEG compression. The first property shows that if we modify a DCT coefficient to an integral multiple of a quantization step Q_m , which is larger than the steps used in later JPEG compressions, then this coefficient can be exactly reconstructed after JPEG compression. The second is an invariant relationship between two homologous coefficients in a block pair before and after JPEG compression. The authentication system proposed by Lin and Chang is based on those two properties. The first one is used to embed the signature and the other is used to generate the authentication bits.

1.6 The Aim of Thesis

The general objective of this work is to build and apply efficient algorithms to verify the authenticity of color images by logo embedding. It uses the semi-fragile watermark technique to achieve these algorithms.

The main advantage of this project is the ability for verifying the slightest changes or tampering that might occur in the image and localize the altered regions such as cropping or pixel modification.

1.7 Thesis Layout

Besides this chapter the remaining part of thesis consists of the following four chapters:

- **Chapter Two:** This chapter contains background of Information Hiding and its issues. It includes watermarking technique, with its classification, properties, and applications. The generic image authentication and requirements in image authentication algorithms are also presented.

- **Chapter Three:** This chapter includes details of designed image authentication technique; the developed algorithms and corresponding block diagrams are presented for proposed technique.

- **Chapter Four:** This chapter gives the results of the conducted tests on some samples of images in this work. This chapter tries to find the optimal color model for proposed authentication system. The used performance criteria (MSE, PSNR). Also it computes the error values generated during color transformations process and their effects on the results.

- **Chapter Five:** This chapter includes the derived conclusions and some suggestions for future work.

Chapter Two

Information Hiding

2.1 Introduction to Information Hiding

Sometimes it is better hide messages than encipher them. In fact, the main purpose of cryptography is to make message incomprehensible, so that people, who do not possess secret keys, cannot recover the message. Instead, the data hiding uses binary files with certain degree of irrelevancy and redundancy to hide data. Digital books, images, videos, and audio tracks are ideal for this purpose. Digital representation of signals brings many advantages when compared to analog representation, and these advantages are [Cac00]:

1. Lossless recording and copying.
2. Convenient distribution.
3. Easy editing and modification.
4. Easily searchable archival.
5. Durable.
6. Cheap.

Against these advantages some serious problems appear:

1. Wide spread copyright violation.
2. Illegal copying and distribution.
3. Problematic authentication.
4. Easy forging.

The general definitions of hiding data in other data can be described as follows: the embedded data is the message that a person wishes to send secretly. This message must be concealed in a normal message as a cover-text, or cover-image, or cover-audio, or in general a cover-object, producing the stego-object or the marked-object. In particular, a stego-key is necessary to control the hiding process, to restrict detection and recovery of the embedded data to unauthorized people. The hidden data may have no relationship with (or may provide important information about) the cover-object, in which it is embedded [Cac00]. The classification of data hiding techniques is presented in Figure (2.1).

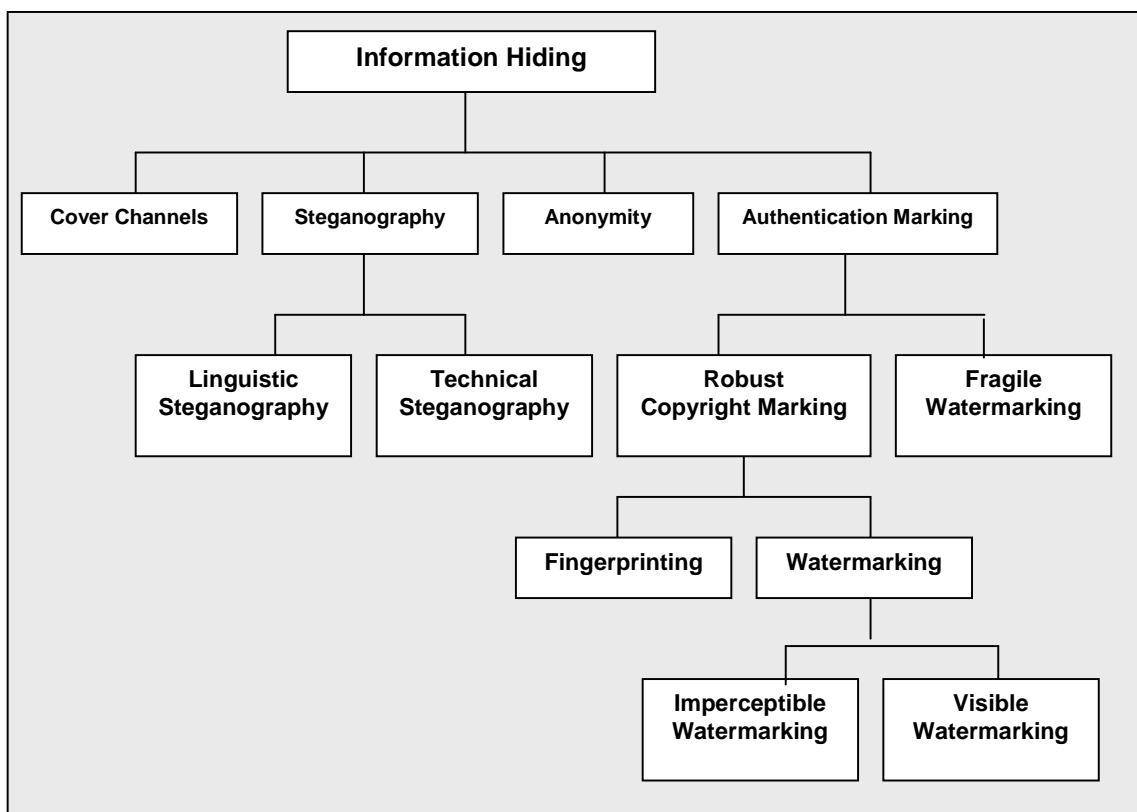


Figure (2.1) A classification of Information Hiding Techniques [CF00].

Data hiding techniques should be capable of embedding data in a host signal with the following restrictions and features [Ben96]:

1. The host signal should be non-objectionably degraded, and the embedded data should be minimally perceptible. This means that the observer should not notice the presence of the data, even if it is perceptible.
2. The embedded data should be directly encoded into the media, rather than into a header, so the data remain intact across varying data file formats.
3. The embedded data should be immune to modifications ranging from intentional and intelligent removal attempts, to anticipated manipulations, e.g., channel noise, resampling, encoding, lossy compressing, digital-to-analog(D/A) conversion, etc.
4. Asymmetrical coding of embedded data is desirable, since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make the data difficult to access.
5. Error correction coding should be used to ensure data integrity. It is inevitable that there will be some degradation in the embedded data when the host signal is modified.
6. The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can be recovered when only fragments of the host signal are available.

2.2 Issues in Information Hiding [Joh99]

There are issues in information hiding must be take in consideration, these are:

2.2.1 Level of Visibility: (Perceptible or Imperceptible)

Method of embedding information may result in the embed data being perceptible or imperceptible. Imperceptible data can not be detected by the human senses, but can be read by a computer. On the other hand, advertising the presence of digital watermark may pose an invitation to attempts of altering or disabling the watermark. Both view points have merit; but determination must be made by the owner of the images and depends on the intended use of the work. Raising the visibility of the embedded information makes it more robust to manipulation but it also distorts the perceptibility of the media.

2.2.2 Robustness vs. Payload

Various ways of hiding data may include the process of adding redundancy to the data being embedded. These methods of redundant pattern encoding may employ patchwork (like a digital quilt), pattern block encoding , or spread spectrum concepts as mean to help protect the embedded information against some types of image processing such as cropping and rotating. The patchwork approach uses a pseudo-random technique to select multiple areas (or patches) of an image for marking. Each patch may contain embedded data, so if one is destroyed or cropped, the other may survive.

2.2.3 Spatial or Transform Domain

Digital watermarking tools take advantage of the transform domain image signal to embed information. Tools are used in the space domain,

bitwise techniques such as least significant bit (LSB) or noise insertion manipulation. Patterns placed in the image and relationships between images components are other additive embedded information (such as the visible watermark).

The transform domain class includes tools that manipulate transforms or signals, early work in this area considered the possible dithering process used for image quantization may use discrete cosine transform (DCT) and wavelet transform are applied to determine the location and intensity of embedded information. Many variations on these approaches exist, ranging from applying the transform to entire image to applying it to blocks of the image or applying methods similar to those used in JPEG image compression, these methods hide messages in relatively significant areas of cover.

2.2.4 File Format Dependence

Some methods employed to hide information depend upon characteristics specific to a carrier type or format while other method may work without relying on specific file format. From the previous subsection, spatial domain process that add patterns to image such as a network logo, are fairly independent of image file format.

2.2.5 Image Modeling

Image modeling can be used to describe the parts of areas of images that can be manipulated to hide information. Image model has four basic components: image noise, texture, clutters (scene noise), and signal. A

common set of techniques for hiding data (that of embedding in the lower bits of images) are categorized under the (image) noise domain ; these include bitwise watermarking techniques, they are sensitive to small amounts of image processing or lossy compression.

2.3 Watermarking

Digital information revolution has brought about many advantages and new issues. It has recently become a vital requirement in the area of production of digital data in this Internet age.

Indeed, with the ease of editing and perfect reproduction and the prevention of unauthorized manipulation of digital audio, image, and video materials become important concerns. Digital watermarking, a scheme to embed special labels in digital sources, has made considerable progress in recent years [Min97].

2.3.1 Watermarking Classification

In this section, digital watermarks can be classified according to their application as presented by Cox [Cox02-2].

1. *Robust watermark.* The robust watermark survives when the watermarked digital content is severely attacked and thus can be applied in copyright protection.
2. *Fragile watermark.* The fragile watermark will be destroyed even if the change in the marked digital media is minute
3. *Semi-fragile watermark.* Because of the fragile property, image authentication becomes a prospective application of it. As a tradeoff of

robustness and fragility, semi-fragile watermark that can resist “content preserving” operations (such as compression operation) and be sensitive to “content altering” transforms (such as feature replacement) is more practicable than fragile watermark in image authentication.

In this section, watermarking classification criterion has been presented by Loo [Loo99]. Watermarking algorithms can be distinguished in terms of:

1. the embedding / extraction domain;
 - I. Spatial Domain.
 - II. Discrete Fourier transform (DFT) domain
 - III. Discrete cosine transform (DCT) domain.
 - IV. Discrete wavelet transform (DWT) domain.
 - V. Miscellaneous domains: e.g. fractal domain, complex wavelet transform (CWT) domain.
2. the availability of reference data (e.g. the original host image) for watermark extraction;
 - I. Oblivious (blind).
 - II. Semi-blind.
 - III. Non-oblivious (non blind).
3. the host data modification method;
 - I. Linear addition of spread spectrum signal.

- II. Image fusion (embedding of a 'logo').
 - III. Non-linear quantization-and-replace strategy.
4. the perceptual modeling strategy;
- I. No modeling.
 - II. Implicit modeling via transform domain properties.
 - III. Explicit HVS modeling.
5. the purpose of the watermarking application;
- I. Copyright protection, circulation tracking.
 - II. Image data verification, image authentication and tamper detection.
 - III. Data hiding and image labeling.
6. and the host media type;
- I. Still image.
 - II. Video.
 - III. Special multimedia format such as cartoon, map image.

2.3.2 Watermarking Properties

There are a number of papers that have discussed the characteristics of watermarks [Cox97] [Kut99] [Pet99] [Wo199] .Some of the properties discussed are robustness, tamper resistance, amount of embedded information, fidelity, and computational cost. In practice, it is probably impossible to design a watermarking system that excels all of these. Thus, it is necessary to make tradeoffs between them, and those tradeoffs must be

chosen with careful analysis of application [Cox02-2]. In addition, the application can affect the very definition of a property. In the following subsections, we look at each of the five properties listed above.

1. Robustness

A watermark is said to be robust if it survives against common signal processing operations (such as lossy compression and digital-to-analog-to-digital conversions). More recently, there has been an increased concern that video and still image watermarks also are robust to geometric transformations. Robustness is often thought of as a single-dimensional value, but this is incorrect. A watermark that is robust against one process may be very fragile against another. In many applications, robustness to all possible processing is excessive and unnecessary [Cox02-2].

2. Amount of Embedded Information

This is an important parameter since it directly influences the watermark robustness. The more information one wants to embed; the lower is the watermark robustness. The information to be hidden depends on the application. It seems reasonable to assume that one wants to embed a number similar to the one used for ISBN¹ (roughly 10 digits) or better ISRC² (roughly 12 alphanumeric characters). On top of this, one should also add the year of copyright, the permission granted on the work and rating for it.

¹ International Standard Book Numbering.

² International Standard Recording Code.

This means that at least 70 bits of information should be embedded in an image [Cox98].

3. Tamper Resistance

Tamper resistance refers to a watermarking system's resistance to hostile attacks. There are several types of tamper resistance. Depending on the application, certain types of attacks are more important than the others. In fact, there several applications in which the watermark has no hostile enemies, and tamper resistance is irrelevant. Some basic types of attacks are:

- I. *Active attacks*. Here the hacker tries to remove the watermark or make it undetectable .this type of attack is critical for many applications, including owner identification, proof of ownership, fingerprinting and copy control ,in which the purpose of the mark is defeated when it cannot be detected [Cox98].
- II. *Passive attacks*. In this case, the hacker is not trying to remove the watermark, but is simply trying to determine whether a mark is present, i.e. is trying to identify a covert communication. Most of scenarios mentioned are not concerned with this type of attack. In fact, they might even advertise the presence of the mark so that it can serve as a deterrent but for covert communication, the primary interest is to prevent the watermark from being observed.
- III. *Collusion attacks*. This kind of attacks can be considered as special case of active attacks, in which the hacker uses several copies of one piece of media, each with a different watermark, to construct a copy with no watermark. Resistance to collusion attacks can be critical in a

fingerprinting application, which entails putting a different mark in each copy of piece of media. However, the number of copies that we can expect the hacker to obtain varies greatly from application to application [Cox97-2].

IV. *Forgery attack*. Here, the hacker tries to embed a valid watermark, rather than remove one. This is main security concern in authentication application, since; if hackers can embed valid authentication marks they can cause the watermark detector to accept bogus or modified media. In addition, as pointed out by Memon et al, this type of attack is a serious concern in proof of ownership [Mem98].

4. Fidelity

Fidelity of a watermarking system is the perceptual similarity between the unwatermarked and watermarked image at the point when they are presented to a consumer. A watermark is said to have high fidelity if degradation it causes is very difficult for viewer to perceive. However, it only needs to be imperceptible at the time that the media are viewed [Cox02-2].

5. Computational Cost

Different applications require the embedders and detectors to work at different speeds. In broadcast monitoring, both embedders and detectors must work in (at least) real time. The embedders must not slowdown the media protection schedule, and the detectors must keep up with real-time broadcasts. On the other hand, a detector for proof of ownership will be valuable even if it takes days to find a watermark. Such a detector will only

be used during ownership disputes, which are rare, and its conclusion about whether the watermark is present is important enough that the user will be willing to wait [Cox02-2].

2.3.3 Watermarking Application

This section describes seven applications of watermarking: broadcast monitoring, owner identification, proof of ownership, authentication, transactional watermarks, copy control and convert communication.

1. Broadcast Monitoring

It can use watermarks for broadcast monitoring by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks. Identifying when and where each clip appears [Abb68] [Sol77].

2. Owner Identification

Although a copyright notice is no longer necessary to guarantee copy rights, it is still recommended. The form of the copyright notice is usually "©date, owner". On books and photographs, the copyright is placed in plane sight. A digital watermark can be used to provide complementary copyright marking functionality because it becomes an integral part of the content. The Digmarc Corporation has marketed a watermarking system designed for this application. Their watermark embedder and detector are bundled with Adobe's popular image processing program (Photoshop).

When the detector finds a watermark, it contacts a central database to identify the watermark's owner [Cox02-2].

3. Proof of Ownership

Multimedia owners may want to use watermarks not just to identify copyright ownership, but to actually prove ownership [Cox02-2].

4. Image Authentication and Data Integrity

Another application of watermarking is “image authentication” and “tamper detection”, digital photographs are being used more and more often as court evidence nowadays. Here, watermarking is used to detect significant modification of the image. Digital images are susceptible seamless modifications from sophisticated image processing applications. Watermarks can be used here as mean to verify the genuineness of an image (Figure 2.2). Verification watermarks are required to be fragile; so that any modification to the image will destroy (or detectable alter) the mark. Unlike cryptographic message digests which can only validate identical copies, watermarking for image authentication should tolerate some well defined image distortion (e.g. file format conversion, resampling).

5. Transactional Watermarks (Fingerprinting)

Monitoring and owner identification applications place the same watermark in all copies of the same content. However, electronic distribution of content allows each copy distributed to be customized for each recipient. This capability allows a unique watermark to be embedded

in each individual copy. Transactional watermarks, also called fingerprints, allow a content owner or content distributor to identify the source of illegal copy.

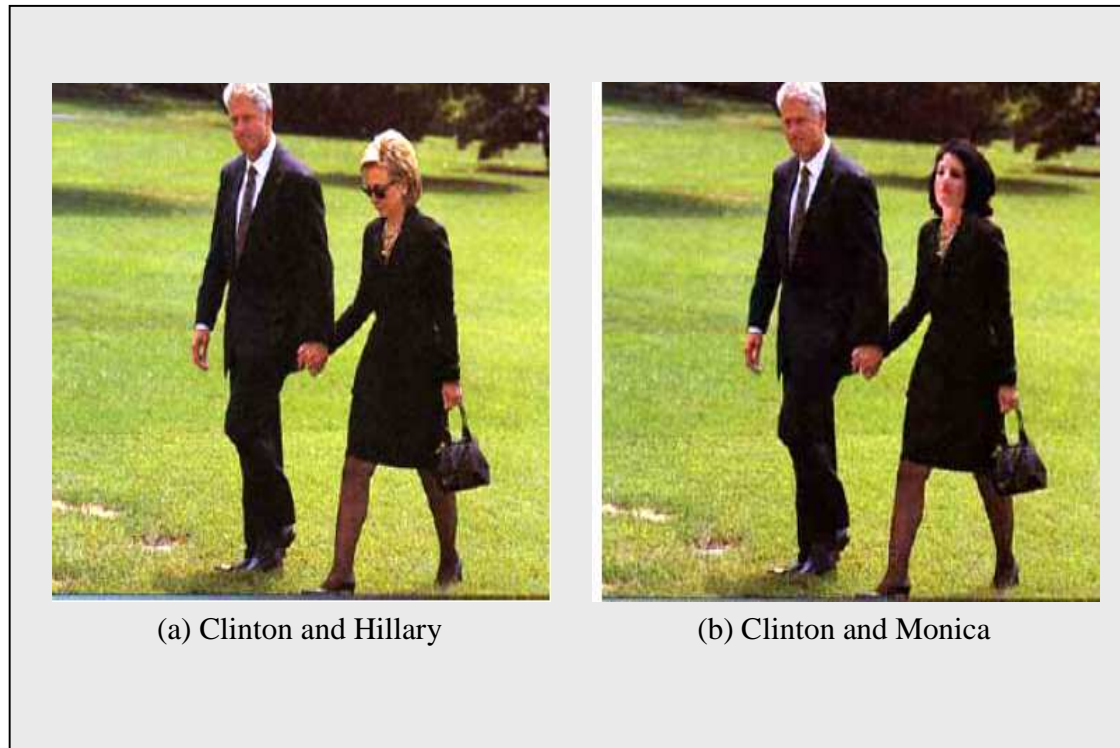


Figure (2.2) Data integrity: hard to judge is (a) or (b) trustworthy photography? (Image by Ching-yang Lin, see <http://www.Ctr.colombia.edu/~cylin/auth/.html>.)

6. Copy Control

Transactional watermarks as well as watermarks for monitoring, identification, and proof of ownership do not prevent illegal copying. Rather, they serve as powerful deterrents and investigative tools. However, it is also possible for recording and playback devices to react to embedded signals. In this way, a recording device might inhibit recording of a signal if

it detects a watermark that indicates recording is prohibited. Of course, for such a system to work, all manufactured recorders must include watermark detection circuitry. Such systems are currently being developed for DVD video [Blo99] and for digital music distribution [Bel99].

7. Covert Communication

One of the earliest applications of watermarking, or more precisely, data hiding, is as a method of sending secret message.

2.4 Authentication

Nowadays it is rather difficult to tell if a picture has been taken by a camera or if it is a fake. Since it is so easy to tamper pictures with the help of a computer, pictures cannot be considered trustworthy anymore. This credibility crisis is getting bigger and bigger in the future, because the production of analog cameras will sooner or later stop. The prices of digital cameras are coming down. Graphic software becomes more sophisticated. Less and less skill is required by the user to tamper an image without leaving a visible trace [Pal05].

2.4.1 Generic Image Authentication System

Various formulations have been proposed by Liu and Wu [Liu98], Lin and Chang [Lin00]. However, they propose a generic image authentication system.

To be effective, a system must satisfy the following criteria [Bed98]:

- 1. Sensitivity.** The system must be sensitive to malicious manipulations (e.g., modifying the image meaning) such as cropping or altering the image in specific areas.
- 2. Tolerance.** The system must tolerate some loss of information (originating from lossy compression algorithms) and more generally non malicious manipulations (generated, e.g., by multimedia providers or fair users).
- 3. Localization of Altered Regions.** The system should be able to locate precisely any malicious alteration made to the image and verify other areas as authentic.
- 4. Reconstruction of Altered Regions.** The system may need the ability to restore, even partially, altered or destroyed regions in order to allow the user to know what the original content of the manipulated areas was.

In addition, some technical features must be taken into account:

- 1. Storage.** Authentication data should be embedded in the image, such as a watermark, rather than in a separate file, as is the case with an external signature.
- 2. Mode of Extraction.** Depending on whether authentication data is dependent or not on the image, a full-blind or a semi-blind mode of extraction is required. It is quite obvious that a non-blind mode of extraction does not make sense for an authentication service, since the original image is necessary.
- 3. Asymmetrical Algorithm.** Contrary to classical security services such as copyright protection, an authentication service requires an asymmetrical watermarking (or encryption) algorithm (i.e., only the

author of an image can secure it, but any user must be able to check the authenticity of an image).

- 4. Visibility.** Authentication data should be invisible under normal observation. It is a question of making sure that the visual impact of watermarking is as weak as possible so that the watermarked image remains faithful to the original. Recently, a new approach based on invertible algorithms has been proposed by J. Fridrich et al [Fri01]. The basic idea is to be able to remove the distortions due to the watermarking process to obtain the original image data. Obviously perfect in terms of visibility, it is important to note that such an approach could create a very attractive context for attackers.
- 5. Robustness and Security.** It must not be possible for authentication data to be forged or manipulated.
- 6. Protocols.** Protocols are an important aspect of any image authentication system; in particular avoid protecting a corrupted picture. It is obvious that any algorithm alone can not guarantee the security of the system. It is necessary to define a set of scenario and specifications describing the operation and rules of the system, such as the management of the keys or the communication protocols between owner, seller, client, and so forth.

2.4.2 The Requirements in Image Authentication Algorithms

A modern image authentication algorithm should have the following properties [Pal05]:

1. **Integrity:** The algorithm should be able to detect malicious modifications of the image data.
2. **Embedding:** The embedding of the authentication data into the image allows file conversions.
3. **Robustness:** The embedded data should be robust to non-malicious alterations of the image.
4. **Visibility:** The embedding induced image modification should not be visible to a human being.
5. **Image dependence:** The authentication data should be image dependent to prevent tampering.
6. **Blindness:** The integrity verification algorithm should not require the original image file.
7. **Verification:** Public verification must be allowed. No third party should be needed.
8. **Security & Updatability:** The integrity of the image data should not have an expiration date. Since the security of an encryption scheme cannot be guaranteed forever, it must be possible to update the encryption scheme without degrading the quality of the image in the future.
9. **Reproduction:** The camera should record the position (longitude, latitude, and altitude), direction; date and time of a shot (see Figure 2.3). This information has to be added to the image authentication data and encrypted. This would deter the forger from photographing fake sceneries.
10. **Access:** The attacker should be denied access to the raw image data or the embedding algorithm.

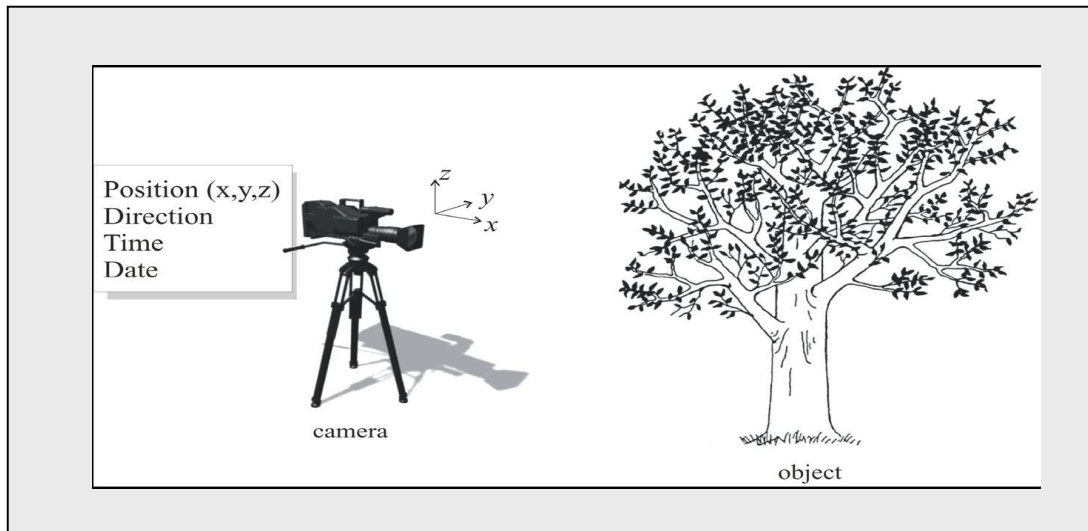


Figure (2.3): Additional information required for authenticity check of a picture.

2.4.3 Locations of Embedding Authentication Information

In this section, different type of authenticated information can be stored in different locations, as presented by Palfner et al [Pal05] which are:

1. External Authentication Data

The location of authentication data could be extern or intern. If the authentication data is stored in a separate file, two files have to be managed. For example, strict authentication algorithms are based on conventional *cryptographic hash functions* (e.g. MD2, MD5, SHA-1 and SHA-256). These hash functions are sensitive to single bit changes. If even one bit of the input signal is modified, the output of a classical hash function alters dramatically and hence no verification is possible. Therefore, they are only suited for strict authentication. The hash value is usually stored externally in a separate file.

To allow signal processing operations, which preserve the content of an image, non-strict authentication algorithms are required. One possibility is that, before the hash is calculated, features of the image are extracted. These features must represent the image content and be invariant to global content-preserving signal processing operations. Another often used solution is the use of *robust hash functions*. Since it is quite easy to lose this external authentication data, it is a better solution to store it inside the image file for easy storage and maintenance. This can be done by adding authentication data as metadata to the image file or by embedding the authentication data as a watermark inside the image.

2. Embedding Authentication Information as Metadata in JPEG2000 Data Stream

The advantage of storing the authentication data internally as metadata is, that the image quality is not degraded. The drawback of this approach used in JPEG2000 is, however, that the authentication data is usually lost after the image is converted into different file formats. Since it is quite common to convert the images into different file formats, it is better to insert the authentication data as a watermark directly into the image.

3. Embedding Authentication Information in the Wavelet Domain

As opposed to the other approaches described before, the authentication data becomes an integral part of the image. The authentication data does not get lost during format conversion operations.

The image is only slightly modified. Therefore, the image cannot be reconstructed perfectly. The small degradation of the image quality due to

the embedding process should not be visible to the human eye. Hence, the data embedded in the wavelet domain and so use one special effect of the human visual system (HVS) that the human eye is less sensitive to changes of higher image frequencies. The discrete wavelet transforms (DWT) works as a kind of frequency decomposition of an image.

2.5 Evaluating Perceptual Impact of Watermarks

One of The most important characteristics of watermarking is its imperceptibility. This raises an important question. How is watermark's perceptibility measured?

In the evaluation of watermarking systems, there are two subtly different types of perceptibility that may be judged: *fidelity* and *quality*. Quality an absolute measure of appeal. For some watermarking applications, however, there are applications of watermarking for which quality, rather than fidelity, is the primary perceptual concern [Cox02-2].

There are two approaches for evaluation of watermark's perceptibility, the first uses Human Visual System (HVS), while the second uses mathematical criteria.

Few watermarking systems produce watermarks that are perfectly imperceptible. However, the perceptibility of a given system's watermarks may be high or low in comparison with other watermarking system or other types of processing, such as compression. In this section, we address the question of how to measure that perceptibility, so that such comparisons can be made. Two types of perceptibility measurement techniques will be discussed, they are:

2.5.1 Human Evaluation Measurement Techniques

Although the claim of imperceptibility is often made in the watermarking literatures, rigorous perceptual quality and fidelity studies involving human observers are rare. However, many claims are based on a single observer's judgments constructed from a small number of trials. These empirical data points are not sufficient for proper perceptual evaluation or comparison of watermarking algorithms [Cox02-2].

In studies that involve the judgment of human beings, it is important to recognize that visual sensitivities can vary significantly from person to person. These sensitivities also change over time for any person. Therefore, it is common that studies involving human evaluation use a large number of subjects and perform a large number of trials.

Perhaps the most important point to note herein is that the experiments are statistical in nature. Different observers will behave differently. One observer might claim to see a difference in a pair of images, whereas another observer may not. Sometimes these discrepancies are random. Other times, the discrepancies reflect the very different perceptual abilities of observers. In fact, it is well known that a small percentage of people have extremely acute vision. In the movie industry these people are often referred to as *golden eyes*, and they are commonly employed at quality control points in the production process.

A classical experimental paradigm for measuring perceptual phenomena is the *two alternative, forced choices* (2AFC) [Gre74]. In this procedure, observers are asked to give one of two alternative responses to each of several trial stimuli. For example, to test the quality impact of a

watermarking algorithm, each trial of the experiment might present the observer with two versions of one image. One version of the image would be the original, the other would be watermarked. The observer, unaware of the differences between the images, must decide which one has higher quality.

2.5.2 Quality Metrics Measurement Techniques

For fair benchmarking and performance evaluation, the visual degradation due to the embedding is an important issue. Since there is no universal metric, this section reviews the most popular pixel based distortion criteria which take into consideration the performance of the human visual system (HVS). Most distortion measures or quality metrics used in visual information processing, belong to the group of difference measures. These measures are all based on the difference between the original, undistorted and the modified, distorted image [Say96].

2.6 Color Models

A color model is a mathematical representation of a set of colors. The most popular color models are RGB (used in computer graphics), YUV, YIQ, or $YCbCr$ (used in video systems). However, none of these color spaces is directly related to the intuitive notions of hue, saturation, and brightness. This resulted in the temporary pursuit of other models, such as HSI and HSV, to simplify programming, processing, and end-user manipulation. All of the color spaces can be derived from the RGB information supplied by devices such as cameras and scanners.

2.6.1 RGB Color Model

The red, green, and blue (*RGB*) color space is widely used throughout computer graphics and image processing. Since color cameras, scanners and displays are most often provided with direct *RGB* signal input or output, this color model is the basic one, which is, if necessary, transformed into other color models. *Red*, *green*, and *blue* are three primary additive colors (individual components are added together to form a desired color) and are represented by a three-dimensional, Cartesian coordinate system (as shown in Figure 2.4). The diagonal of the cube, with equal amount of each primary component, represents the shade of gray levels.

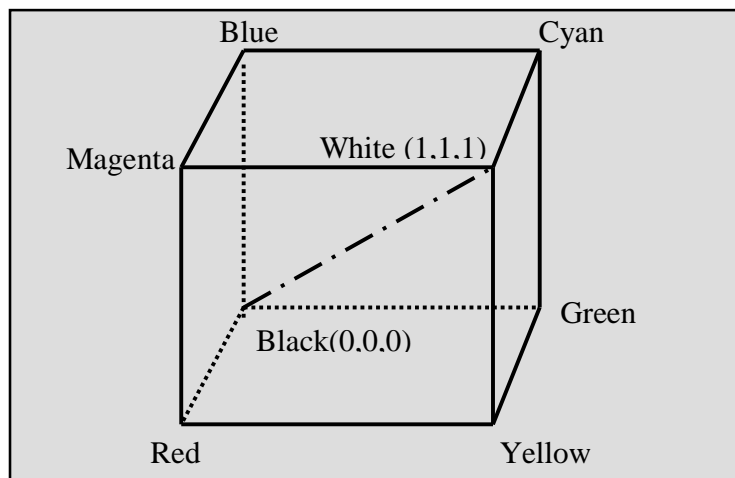


Figure 2.4: The RGB Color Cube [San98].

Table (2. 1): The components of the RGB color bars [San98].

	National Range	White	Yellow	Cyan	Green	Magenta	Red	Blue	Black
R	0 to 255	255	255	0	0	255	255	0	0
G	0 to 255	255	255	255	255	0	0	0	0
B	0 to 255	255	0	255	0	255	0	255	0

Table (2.1) presents the *RGB* values for the color bars with (100% amplitude, 100% saturated), i.e., the common video test signal.

2.6.2 YUV Color Model

The *YUV* color space is used by the PAL (Phase Alternation Line), NTSC (National Television System Committee), and SECAM (Sequential Color with Memory) composite color video standards. The black-and-white system uses only luminance (*Y*) information; color information (*U* and *V*) was added in such a way that a black-and-white receiver would still display a normal black-and-white picture. Color receivers decode the additional color information to display a color picture. [San98]. The simple linear transform of the *RGB* to *YUV* is performed as follows:

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.1 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

2.6.3 YIQ Color Model

The *YIQ* color space is derived from the *YUV* color space and is optionally used by the NTSC composite color video standard. (The “*I*” stand for “inphase” and “*Q*” for “quadrature” which is the modulation method used to transmit the color information.).

The given color image is split into its three components in the *YIQ* color space, where the *Y* component represents the luminance and the *I* and *Q* components represent the chrominance respectively. The *I* and *Q* components are used to jointly represent saturation and hue. The *YIQ* color space is suitable for information hiding as it splits information into a luminance component which contains a large component of the visual content as well as two chrominance components which contain less perceptual information [ITU02]. The simple linear transform of the RGB to YIQ is performed as follows:

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.321 \\ 0.596 & -0.275 & -0.114 \\ 0.212 & -0.523 & 0.311 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

2.6.4 YCbCr₁ Color Model

This color model is closely related to YUV model. It is appropriate for digital coding standard TV images. This color model is used in the process of video sequences encoding on videodisks [San98]. Other current applications in image compression (e.g. JPEG format) which often employ

YCbCr₁ model as quantization model. The simple linear transform of the RGB to YCbCr₁ is performed as follows:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.298 & 0.586 & 0.114 \\ -0.168 & -0.33 & 0.498 \\ 0.498 & -0.417 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

2.6.5 YCbCr₂ Color Model

The YC_bCr_2 color space was developed as part of ITU-R BT.601 during the development of a world-wide digital component video standard [ITU95]. YC_bCr_2 is a scaled and offset version of the YUV color space. Y is defined to have a nominal 8-bit range of (16-235); C_b and C_r are defined to have a nominal range of (16-240). YC_bCr_2 is used in image compression (e.g. JPEG format). [ITU02]. The simple linear transform of the RGB to YCbCr₂ is performed as follows:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.212 & 0.715 & 0.072 \\ -0.114 & -0.384 & 0.498 \\ 0.498 & -0.452 & -0.046 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

*Republic of Iraq
Ministry of Higher Education and Scientific Research
Al-Nahrain University
College of Science*

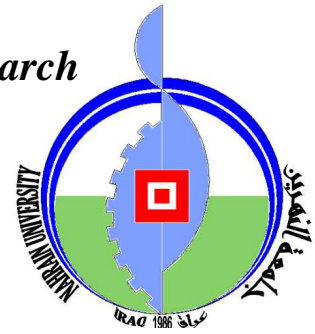


Image Authentication by Using Logo Embedding

A Thesis

*Submitted to the College of Science, Al-Nahrain University
In Partial Fulfillment of the Requirements for
The Degree of Master of Science in Computer Science*

**By
Zainab Hussain Kadhim
(B.Sc. 2005)**

**Supervised By
Dr. Ali Kadhim Mousa**

April 2008

Rabye Al-Awal 1429

Chapter Four

Test and Results

4.1 Introduction

This chapter is devoted to present the results of the conducted tests to study the effect of essential keys required for Embedding module and Extracting module. Some of the well known difference distortion metrics measures (i.e. *MSE*, *PSNR*) have been used to assess the quality of the watermarked images.

The watermarked images have been tested to resist some types of famous compression software which are (*WINRAR* and *ZIP*) and some types of image transformation format such as (*GIF* and *TIFF*).

The developed technique has been established by using Visual Basic (version 6.0) programming language under windows *XP* operating system. The tests have been conducted by using personal computer (processor Pentium 4, 2.40 GHz) with dual cash memory.

4.2 The Importance of Image Properties

Number of images have been taken as test samples, each image consists of different properties such as categories (painted or photo etc), nature of the image (smooth or texture) etc. The properties of the image are important; where the quality of some images are degraded in noticeable way after embedding watermark in it, because of these properties .Figure (4.1) shows the importance of image property when embed a watermark in image has high white color ratio. Table (4.1) shows these properties .Figure (4.2) shows some selected images used for test.

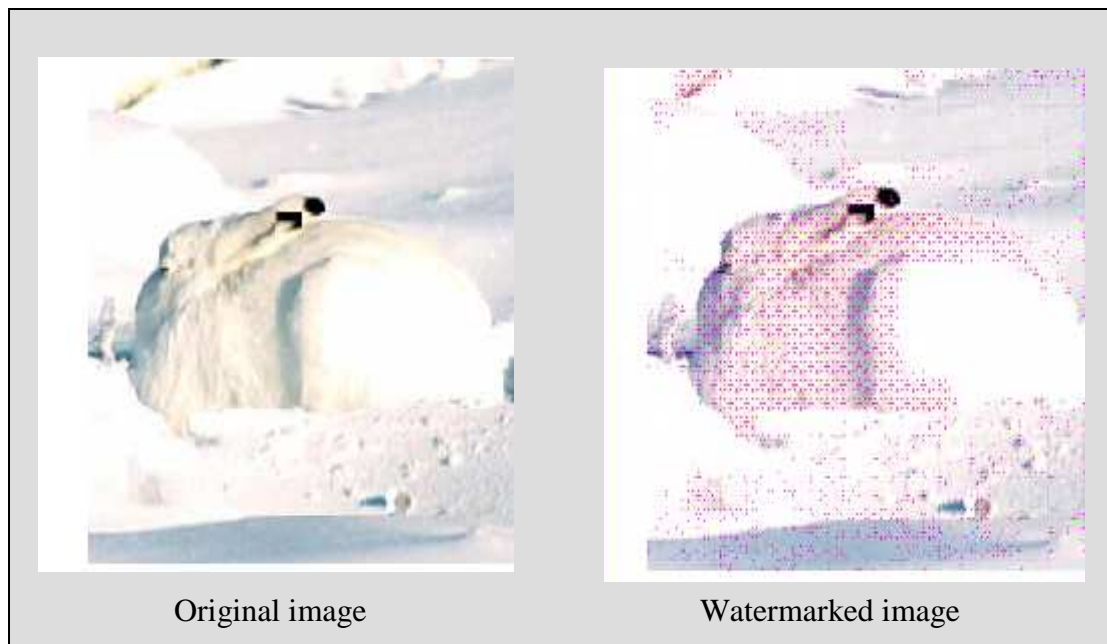


Figure (4.1): Comparison in quality before and after watermarking.

Table (4.1) shows numerous BMP images with various properties for each. All specimens' size is (256 x 256) pixels.

Table (4.1): Various Image properties.

Image Name	Categories
Baboon	High texture
Child	By scanner
Kids	Photo
Lena	Smoothed & texture
Monaliza	Painted
Arctic Hare	High smoothed

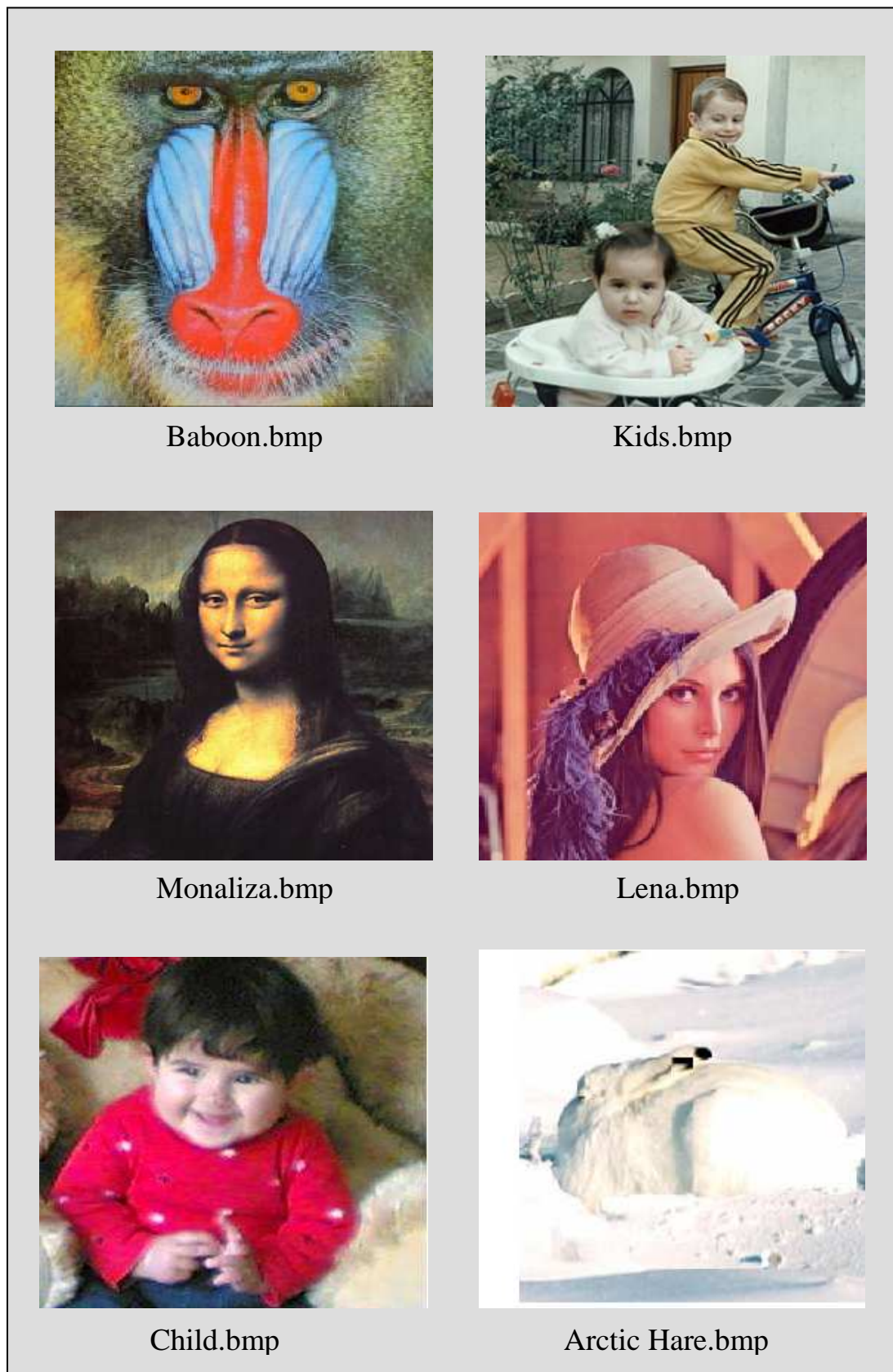


Figure (4.2): Image specimens used in the test work .

4.3 Performance Parameters

A lot of key parameters have been utilized in the literature to describe the performance of various watermarking methods. In this research the distortion measures (*MSE* and *PSNR*) before and after watermarking have been used to evaluate the performance of the proposed Image Authentication system under different embedding conditions. The watermark survival after exposed to compression operations.

4.3.1 Distortion Measures [Kut99-2]

Most distortion measures used in visual information processing belong to group of difference measures. These measures are all based on the difference between the original, undistorted and modified image. When we refer to a “perceptual model”, we mean more precisely a function that gives a measure of distance between the original image, O , and the watermarked image, R . One of the simplest distance functions is the mean squared error (*MSE*). This is defined as

$$MSE = \frac{\sum_{x,y} [O(x,y) - R(x,y)]^2}{W * H} \dots\dots\dots(4.1)$$

where $O(x,y)$ represents a pixel, whose coordinates are (x,y) , in the original (undistorted image), and $R(x,y)$ represents a pixel, whose coordinates are (x,y) , in the watermarked image. W and H represent the width and height of image respectively.

Nowadays, the most popular distortion measure in the field of image and video coding and compression is the *Peak Signal to Noise*

Ratio (PSNR). Its popularity is very likely due to the simplicity of the metric .It is defined as:

$$PSNR=10\log_{10}\frac{(255)^2}{MSE} \dots\dots\dots(4.2)$$

4.3.2 Compression Compactness [Umb98]

Although there are different measures to describe the achieved reduction in data size due to compression (like compression ratio, compression factor, and bit rate), in this work the compression ratio (C_r) has been adopted.

Compression ratio refers to the degree of image file size reduction due to compression process. This measure is determined as the ratio between the sizes of the original uncompressed image file to the size of the overall compressed data file.

$$C_r = \frac{\text{uncompression file size}}{\text{compression file size}} \dots\dots\dots(4.3)$$

The (C_r) parameter is an indicator for the compactness ability of the compression process.

4.4 Testing Strategy

The testing operations have been implemented on the image specimens shown in Figure (4.2).The test strategy of the proposed system is based on studying the effect of essential keys (color model, color components, number of partitions, LSB's position) on the quality of these images and their resistance against unintentional modifications then we will try to find the optimal of them.

Experimental results give *PSNR* much higher measurements than (38 dB) .This is considered as very acceptable, since the casual observer cannot notice any visual differences between the original and the watermarked image. The effectiveness of these keys on the operation of watermarking will be described as follows:

4.4.1 The Effect of Partition Number

The second essential key used in *Embedding* and *Extraction* module is the number of partitions. The question is, what is the preferable number of partitions should we divide the image?

If we increase the number of partitions by repartitioning the image until (32x32) parts, then finer altered regions can be defined. It should be noticed that as the number of partitions is increased, the payload of authentication mark is increased and this leads to finer altered region which can be specified, but this will lead to degradation in the quality of marked image as shown in Table (4.2) where *PSNR* decreases as partitions number increases (**numbers in Table (4.2) refer to PSNR values**).

The effect of increment the partitions number to localize the altered regions can be seen in Figure (3.4).

Table (4.2): The effect of partition number on PSNR values.

		Image Name						
		Baboon	Monaliza	Child	Kids	Lena	Arctic Hare	
Type of partitions	4x4	R	82.678	82.145	82.145	80.980	81.244	80.980
		G	80.167	80.980	81.110	81.824	83.742	80.613
		B	80.384	80.384	81.981	80.732	81.244	80.384
	8x8	R	73.530	73.508	73.417	73.135	73.577	73.508
		G	72.951	73.307	73.417	73.890	73.485	73.328
		B	73.199	73.600	73.350	73.417	73.767	73.417
	16x16	R	66.222	66.163	66.071	66.158	66.260	66.121
		G	66.158	66.218	66.213	66.218	66.248	66.096
		B	66.308	66.260	66.313	66.256	66.112	66.038
	32x32	R	59.178	59.213	59.218	59.197	59.196	59.109
		G	59.186	59.217	59.164	59.172	59.192	59.075
		B	59.158	59.251	59.191	59.230	59.220	59.117

Table (4.2) shows the optimal partition number is (32x32) parts (by depending on PSNR values), because it gives the best tamper localization while *PSNR* values are still more than (38 dB) which are acceptable.

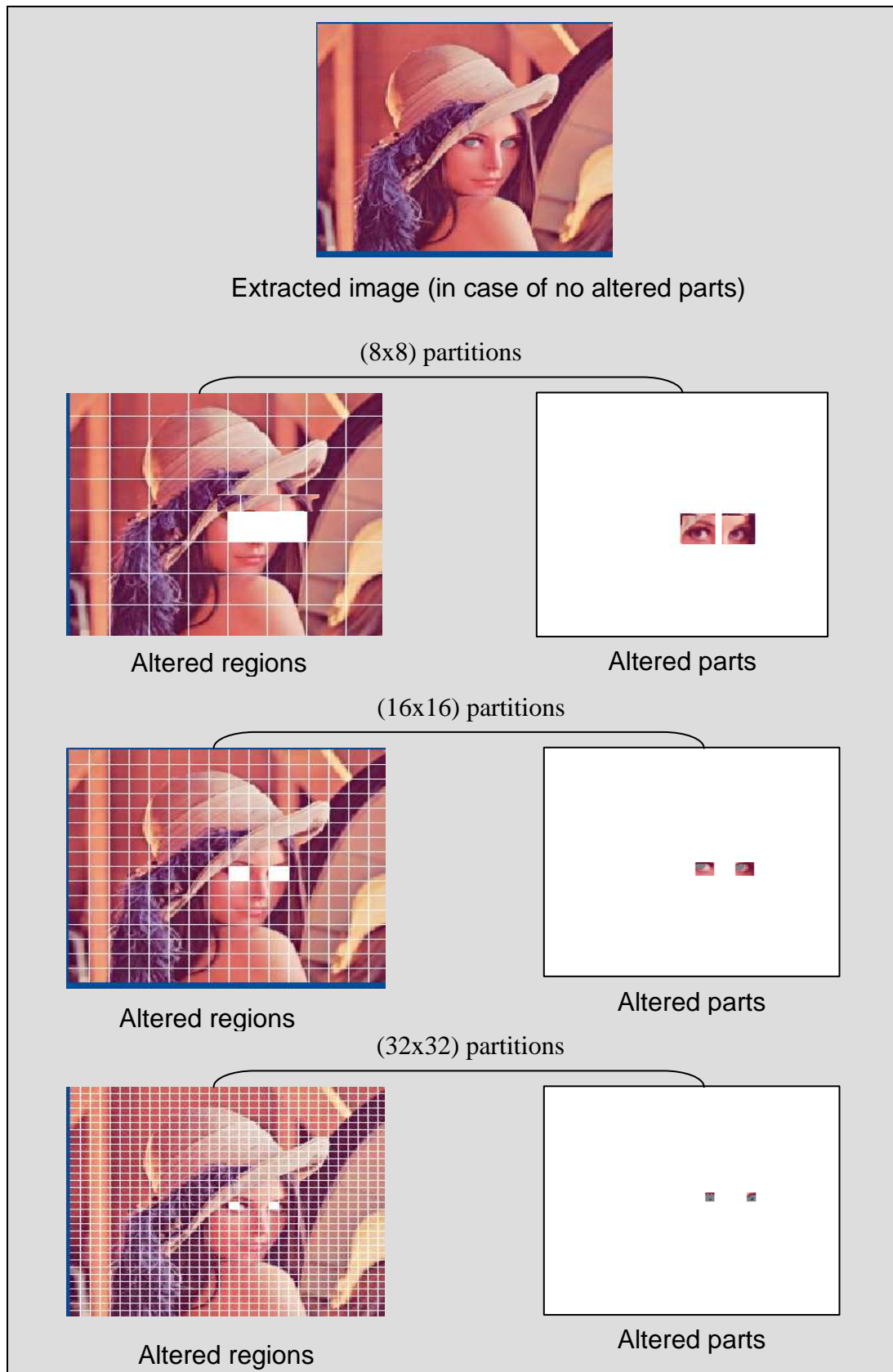


Figure (4.3): Increasing the partition number lead to finer localization.

4.4.2 The Effect of LSB's Position.

The third essential key used in Embedding module and required for Extraction module is LSB's position. Variable host bit locations from (1st LSB's) to (4th LSB's) were tested. The host bit is shifted from first LSB's toward the MSB this leads to increasing the robustness of authentication mark versus decreasing in image quality. Table (4.3) shows the effect of LSB's positions on quality of marked image partitioned to (32x32) parts (**numbers in Table (4.2) refer to PSNR values**).

Table (4.3): The effect of LSB's positions on PSNR values of marked images.

			Image Name					
			Baboon	Monaliza	Child	Kids	Lena	Arctic Hare
Type of LSB's Positions	1 st LSB	R	59.178	59.213	59.218	59.197	59.196	59.109
		G	59.186	59.217	59.164	59.172	59.192	59.075
		B	59.158	59.251	59.191	59.230	59.220	59.117
	2 nd LSB	R	53.194	53.137	53.248	53.181	53.127	53.140
		G	53.185	53.238	53.242	53.172	53.099	53.178
		B	53.211	53.168	53.173	53.242	53.245	53.204
	3 rd LSB	R	47.176	47.123	47.194	47.182	47.216	47.177
		G	47.208	47.166	47.163	47.168	47.134	47.171
		B	47.168	47.209	47.499	47.114	47.142	47.174
	4 th LSB	R	41.082	41.158	41.209	41.194	41.103	41.041
		G	41.213	41.225	41.052	41.215	41.206	41.089
		B	41.175	41.211	41.175	41.161	41.111	41.105

From Table (4.3), it is found the optimal LSB's position is the fourth, because *PSNR* values are still more than (38 dB) and give marked image robustness against unintentional modifications (compression and transformation).

4.4.3 The Effect of Color Component

The fourth key required for *Embedding* and *Extraction* processes is the color component used for hosting. Table (4.2) and Table (4.3) show that there is no obvious difference of *PSNR* measurements among the color components do RGB. And that is expected in this color model with the criteria used for evaluation. But next section will show some things different for other color models.

4.4.4 The Effect of Color Models (Optimal Color Models).

One of the most important issues in watermarking techniques is the color model of host image. In present work the effort has been put in finding the most suitable color model for the application of information hiding in color images. We test the most commonly used color models; RGB, YIQ, YUV, YCbCr₁ and YCbCr₂. The same set of embedding and detection procedures was applied so as to achieve the best comparison among them, and to decide which one of them is more appropriate for our suggested watermarking technique.

It has been discovered in this work that it has been taken into consideration the value of errors that generated during transformations among color models.

1. Evaluating Color Models Impact of Watermarks

In image watermarking researches, there are various attitudes about the preferable color model for embedding a watermark. Some of these are:

- I. Elisa, et al, [Say98] report that “ In general, it is better to watermark the RGB color components than the luminance components”
- II. Chae, et al, [Cha98] indicate that a robust data embedding scheme can be achieved in YUV color space.
- III. Patrizio, et al, [Pat01] state that “The YIQ color space is ideal for watermarking color image ”
- IV. Ekram, et al, [Kha02] distribute the watermark over YUV components.
- V. Gilani, et al, [Gil02] indicate that “it is found that linear and uncorrelated color transforms YUV & YIQ are most suitable for watermarking”.
- VI. Ali Kadhim, [Ali04] report that “RGB color model is found to be most suitable for watermarking applications in color images”.

New attitude about the preferable color model for embedding a watermark in proposed authentication technique may be found in next sections.

2. Errors in Color Models Transformations

During the forward and backward processes of color model transformation; there are some errors have been registered, Table (5.2) shows the values of these errors. In fact these errors appear because of the nature of mathematical equations of color transformation systems

Table (4.4): Error values result from color model transformation with RGB











Image Name	Color Model				
	RGB	YUV	YIQ	YCbCr1	YCbCr2
Monaliza	0	266	230	279	248
Kids	0	260	266	254	254
Lena	0	239	241	166	250
Child	0	222	237	141	250
Baboon	0	210	239	127	254
Arctic Hare	0	181	178	160	135
Average of Errors	0	229.667	231.833	187.833	231.833


3. The Optimal Color Model


We put in consideration these errors mentioned in section (2) as a noise, so we exclude them when MSE is calculated.

Table (4.5) shows PSNR values for the first band of each color model where the embedded identification numbers are totally retrieved. These PSNR values are shown with and without errors generated through color model transformations.

Table (4.5): PSNR values before / after removing errors

Color Model		Image Name						Average
		Baboon	Monaliza	Child	Kids	Lena	Arctic Hare	
RGB		59.178	59.213	59.218	59.197	59.196	59.109	59.185
		59.178	59.213	59.218	59.197	59.196	59.109	59.185
YUV		48.544	46.953	48.164	47.073	47.666	49.492	47.982
		65.891	67.962	66.158	67.318	66.719	64.897	66.490
YIQ		47.698	47.928	47.731	46.894	47.602	49.492	47.890
		67.013	66.434	66.719	67.318	66.719	64.22	66.403
YCbCr1		51.302	46.575	50.824	47.225	49.942	50.069	49.322
		62.282	67.962	63.006	67.013	64.005	63.392	64.610
YCbCr2		47.256	47.38	47.349	47.225	47.349	51.108	47.944
		67.318	66.719	67.013	67.013	67.013	63.006	66.347

: PSNR before excluding errors.

: PSNR after excluding errors.

1. From table (4.4), the values of color transformation errors are variant from one image to another according to the nature of image. The average shows the maximum error is in YIQ and YCbCr₂ color models then YUV, while the minimum values of error in YCbCr₁ (RGB color model is excluded).

2. From table (4.5), by depending on PSNR measurement evaluation we find YUV then YIQ color models are the most suitable color models for information hiding.

4.5 Unintentional Modifications

The watermarked images with semi-fragile watermark must have robustness against unintentional modification such as compression and some type of transformations; this concept has been satisfied with this proposed system.

4.5.1 Compression

Image compression addresses the problem of reducing the amount of data required to represent a digital image. The underlying basis of the reduction process is the removal of redundant data. From a mathematical point of view some transforms convert a 2D-pixel array into a statistically uncorrected data set [Gon00]. An effective authentication system should have desirable features; the most important of which is to allow the watermarked image to resist lossy-compression format in this work it has been concluded the authentication mark is extracted successfully when watermarked image is exposed to some types of famous compression software like *WINRAR* and *ZIP* with ratios exceeding 75% compression ratio under (32x32) partition number, 1st LSB position.

4.5.2 Transformations

If the marked image is transformed from BMP image format to other format; it has been found the watermark is retrieved from some images

under some transformation formats and not retrieved under others. As shown in Table (4.6).

Table (4.6): The status of watermark retrieving after transformation process.

Format	Baboon	Monaliza	Child	Kids	Lena	Arctic Hare
EPS	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
GIF	<i>Not retrieved</i>	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
JPEG	<i>Not retrieved</i>	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
JPEJ2000	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>
PCX	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
PDF¹	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
PDF²	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>
PNG	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
PXR	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
RAW	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
TGA	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
TIFF¹	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
TIFF²	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved	Retrieved
TIFF³	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>	<i>Not retrieved</i>

PDF¹: this type of transformation is done with *no* compression.

PDF²: this type of transformation is done with *JPEG* compression.

TIFF¹: this type of transformation is done with *LZW* compression.

TIFF²: this type of transformation is done with *ZIP* compression.

TIFF³: this type of transformation is done with *JPEG* compression.

Chapter Five

Conclusions and Suggestion for Future Works

5.1 Conclusions

The previous discussions have covered some remarks related to the behavior and performance of the suggested image authentication system. A summary of some important conclusions could be the following:

1. The results of the tests, conducted in this work, confirm the idea that spatial domain is suitable for watermark application, like Image Authentication.
2. The proposed method is providing the advantage of using it for the authentication of large volumes of digital images.
3. The optimal partition number is (32x32) parts, because it gives the best tamper localization while PSNR values are still more than (38 dB) which are acceptable.
4. The authentication mark is extracted successfully when the watermarked image is exposed to some type of famous compression software like *WINRAR* and *ZIP* and some image transformation formats like *TIFF*, *GIF* and *PDF*.
5. By depending on PSNR measurement evaluation the *YUV* then *YIQ* color models are the most suitable color models for information hiding. , but some of other color spaces could be used efficiently also.

6. The optimal LSB's position is the fourth, when *PSNR* values have been stilled more than (38 dB).

5.2 Suggestions for Future Works

The work done in this thesis can be extended along several interesting directions, among them are:

1. Apply authentication process on image format (e.g. *TIF*, *GIF* or *JPEG*) or other multimedia such as audio files.
2. Watermarking with transform domain instead of spatial domain like *DCT* or *DWT* to survive *JPEG2000*.
3. The owner of watermark analyzes the host image before embedding watermark to find the best places of image to conceal his watermark in away that satisfy increasing the imperceptibility.
4. Design an authentication system capable to retrieve corrupted parts of image.

List of Contents

Chapter One: General Introduction	Page No.
1.1 Introduction	1
1.2 Watermarking	1
1.2.1 Watermarking Terminology	2
1.2.2 Digital Watermarking for Images	3
1.3 Difference and Relationship between Watermarking and Steganography[Mou01]	5
1.4 Authentication	5
1.4.1 What is The Authentication?	5
1.4.2 Why Use The Authentication?	6
1.5 Related Work (literature survey)	7
1.6 The Aim of Thesis	12
1.7 Thesis Layout	12
Chapter Two : Information Hiding	
2.1 Introduction to Information Hiding	14
2.2 Issues in Information Hiding	16
2.2.1 Level of Visibility(Perceptible or Imperceptible)	17
2.2.2 Robustness vs. Payload	17
2.2.3 Spatial or Transform Domain	17
2.2.4 File Format Dependence	18
2.2.5 Image Modeling	18
2.3 Watermarking	19

2.3.1 Watermarking Classification	19
2.3.3 Watermarking Properties	21
2.3.4 Watermarking Application	25
2.4 Authentication	28
2.4.1 Generic Image Authentication System	28
2.4.2 The Requirements in Image Authentication Algorithms	30
2.4.3 Locations of Embedding Authentication Information	32
2.5 Evaluating Perceptual Impact of Watermarks	34
2.5.1 Human Evolution Measurement Techniques	35
2.5.2 Quality Metrics Measurement Techniques	36
2.6 Color Models	36
2.6.1 RGB Color Model	37
2.6.2 YUV Color Model	38
2.6.3 YIQ Color Model	39
2.6.4 YCbCr ₁ Color Model	39
2.6.5 YCbCr ₂ Color Model	40
Chapter Three : Proposed Authentication Technique	
3.1 Introduction	41
3.2 The Proposed Method	41
3.2.1 The Embedding Module	41
1.Color Separation Process	41
2.Color Transformation Process	45
3.Partitioning Process	55

5.Embedding Process	47
6.Saving Process	50

4.Finding Pixels Process	58
5.Embedding Process	60
6.Saving Process	63
3.2.2 Extraction Module	64
1. Extraction Process	64
2. Localization Process	66
Chapter Four :Test and Results	
4.1 Introduction	69
4.2 The Importance of Image properties	69
4.3 Performance Parameters	72
4.3 .1 Distortion Measures	72
4.3.2 Compression Compactness	73
4.4 Test Strategy	73
4.4.1 The Effect of Partition Number	74
4.4.2 The Effect of LSB's Position	77
4.4.3 The Effect of Color Component	78
4.4.4 The Effect of Color Models (Optimal Color Model)	78
1. Evaluating Color Space Impact of Watermark	79
2. Errors in Color Models Transformations	80
3. The Optimal Color Model	80
4.5 Unintentional Modifications	82
4.5.1 Compression	82
4.5.2 Transformations	82

Chapter Five: Conclusions and Suggestions for Future Works	
5.1 Conclusions	85
5.2 Suggestions for Future Works	86
References	I
Appendix A (BMP File Structure)	I

List of Algorithms

Algorithms Names	Page No.
Algorithm (3.1): Read BMP Image File	44
Algorithm (3.2): Convert image from RGB color model to YUV color model	45
Algorithm (3.3) :Convert YUV image data model to RGB color model	46
Algorithm (3.4) :Convert image from RGB color model to YIQ color model	47
Algorithm (3.5):Convert YIQ image data model to RGB color model	48
Algorithm (3.6):Convert image from RGB color model to YC_bC_{r1} color model	49
Algorithm (3.7):Convert YC_bC_{r1} image data model to RGB color model	50
Algorithm (3.8):Convert image from RGB color model to YCbCr2 color model	51
Algorithm (3.9):Convert YCbCr2 image data model to RGB color model	52
Algorithm (3.10): The image Partition	55
Algorithm (3.11): Finding pixels	58
Algorithm (3.12): The Embedding process	61
Algorithm (3.13): The Extraction process	66

List of Figures

Figures Names	Page No.
Figure (2.1): A Classification of Information Hiding Techniques.	15
Figure (2.2): Data integrity.	27
Figure (2.3): Additional information required for authenticity check of a picture.	32
Figure (2.4): The RGB Color Cube.	37
Figure (3.1): Block diagram of Embedding module.	42
Figure (3.2): Hunter image with separated color components.	43
Figure (3.3): Monaliza image in RGB & YUV models.	53
Figure (3.4): Monaliza image in YIQ & YCbCr1 models.	54
Figure (3.5): Hunter Image with Authentication Marks.	57
Figure (3.6): Details of Embedding process.	61
Figure (3.7): Block diagram of Extraction module.	65
Figure (4.1): Comparison in quality before and after watermarking	70
Figure (4.2): Image specimens used in the test work.	71
Figure (4.3): Increasing partition number lead to finer localization.	76

List of Abbreviations

Abbreviation	Meaning
BMP	Bitmap Image File
C_r	Compression Ratio
CWT	Complex Wavelet Transform
D/A	Digital-to-Analog conversion
dB	Decibels unit
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HH	High – High band coefficient
HL	High – Low band coefficient
HSI	(Hue, Saturation, Intensity) color space
HSV	(Hue, Saturation, Value) color space
HVS	Human Visual System
ISBN	International Standard Book Numbering
ISRC	International Standard Recording Code
MD	Message Digest algorithm
SHA	Secure Hash Algorithm
ITU-R	International Telecommunications Union-Radio
JPEG	Joint Photographic Experts Group
LH	Low – High band coefficient
LL	Low – Low band coefficient
LSB	Least Significant Bit
MSB	Most Significant Bit
MSE	Mean-Squared Error

NTSC	National Television System Committee
PAL	Phase Alternation Line
PDF	Probability Density Function
PSNR	Peak Signal-to-Noise Ratio
RGB	Red, Green, and Blue
SECAM	Sequential Color with Memory
VW2D	Variable Watermark Two Dimension of Technique
2AFC	Two Alternative, Forced Choice

List of Symbols

Symbol	Meaning
A	Sub set of original image's pixels contain a watermark
B	Sub set of original image's pixels doesn't contain a watermark
B(I,J)	8-bit pixel value of the blue component
C	New sub set of pixels produced after adding k-factor
f	General embedding/extraction function
f_G	The embedding function of Green band
f_R	The embedding function of Red band
f_B	The embedding function of Blue band
H	Height of image
K	An integer factor
(M,N)	Size of part (number of pixels in each part)
$O(x,y)$	Represents a pixel, whose coordinates are (x,y) , in the original (undistorted image)
PrtNo	Number of partitions in image
PxlsNo	Number of pixels in each part
Q-M	An integral quantization step
$R(x,y)$	Represents a pixel, whose coordinates are (x,y) in the watermarked image
W	Width of Image
W(b)	Binary Watermark

References

- [Abb68] Abbey, C.R. and Pursel, H. H. “*Data channel monitor*”, United States Patent, pp. (3,415,947), 1968.
- [Ali04] Ali, K., M.,”*Watermark Applications in Color Images Using Wavelet Transforms*”, Ph.D thesis, Informatics Institute for Postgraduate Studies, Baghdad, Iraq, April, 2004.
- [Bed98] Bede, L. and Min W.,”*Watermarking for Image Authentication*”, Department of Electronic Engineering, Princeton university, NJ08544, IEEE, Princeton, 0-8186-8821, USA, 1998.
- [Bel99] Bell, A.E. “*The Dynamic Digital Disk*”, IEEE Spectrum, vol. 36, no 10, pp. 28–35, 1999.
- [Ben96] Bender, W. "*Techniques for Data Hiding*", IBM system Journal; Vol. 35, no. 4, pp. 1-10, 1996.
- [Blo99] Bloom, J.A., Cox, I. J., and Miller, M. L, “*Copy Protection for DVD Video*”, Proceedings of the IEEE, vol. 87, no. 7, pp. 1267–1276, 1999.
- [Cac00] Cacciaguerra, S., and Ferretti, S., "*Data Hiding: Steganography and Copyright Marking*", department

References

of computer science, Paper, Bologna University, Italy, 2000.

- [Cha98] Chae, J.J., Mukherjee, D. and Manjunath B.S. “*Color Image Embedding using Multidimensional Lattice Structures*”, Proceedings of the IEEE, January, 1998.
- [Cox97] Cox, I., and Miller, M.L., “*A Review of Watermarking and The Importance of Perceptual Modeling*”, In Proceedings of SPIE, Human Vision & Electronic Imaging II, vol. 3016, pp. 92–99, 1997.
- [Cox97-2] Cox, I., Kilian, J., and Shamoon, T., “*Secure Spread Spectrum Watermarking for Multimedia*”, IEEE Trans. on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.
- [Cox98] Cox, I.J. and Linnartz, J.P., “*Some General Methods for Tampering with Watermarks*”, IEEE Trans. on Selected Areas of Communications, vol. 16, no. 4, pp. 587–593, 1998.
- [Cox02-1] Cox, I.J. and Miller, M.I., “*The first 50 Years of Electronic Watermarking*”, Journal of Applied Signal Processing, no.2, pp. 126-132, 2002.
- [Cox02-2] Cox, I.J., Miller, M.I. and B., “*Digital Watermarking*”, Morgan Kaufmann, 2002.

References

- [Fri99] Fridrich J., “*Methods for Tamper Detection in Digital Images*”, Multimedia and Security Workshop at ACM Multimedia 1999, Orlando, Florida, USA, Oct, 1999.
- [Gil02] Gilani, S.A.M., Kostopoulos, I. and Skodras, A.N., “*Color Image-Adaptive Watermarking*”, Proceedings of the IEEE, 0-7803-7503, 2002.
- [Gil06] Gilani, A. and Hassan, H., "A *Fragile Watermarking Scheme for Color Image Authentication* “, Transactions on Engineering Computing and Technology, WORLD ENFORMATIKA SOCIETY, vol. 13, ISSN 1305-5313 312 ,pp. 312-316, Pakistan, April, 2006.
- [Gon00] Gonzales, R. C., and Woods, R. E., “*Digital Image Processing*”, Addison-Wesley Publishing Company, 2000.
- [Gre74] Green, D.M., and Swets, J.A. “*Signal Detection Theory and Psychophysics*”, Huntington, New York, Robert E. Krieger Publisher Co., 1974.
- [Hem61] Hembrooke, E.F., “*Identification of sound and like signals*”, US patent, No. 3004104, 1961.
- [Hua05] Huang, J., Wu ,X., Hu, J., and Gu ,Z. , "A *Secure Semi-*

References

Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters, School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, 510275, P. R. China, 2005.

- [ITU95] International Telecommunications Union ITU-R BT., “*Studio Encoding Parameters of Digital Television*”, 601–5, 1995.
- [ITU02] International Telecommunications Union ITU-R BT., “*Parameter Values for the HDTV Standards for Production and International Program Exchange*” 709–5, 2002.
- [Joh99] Johnson, N. F., “*An Introduction to Watermark Recovery from Images*”, pp. 9-13, Virginia, USA, February, 1999.

Internet site: www.jjtc.com/pub/nfjidr99.pdf.

- [Kat00] Katzenbeisser, S., and Petitcolas, A.P., “*Information Hiding Techniques for Steganography and Digital Watermarking*”, Artech House, Inc., 2000.
- [Kha02] Khan, E., and Ghanbari, M., “*Embedded Color Image Coding With Visual SPIHT*”, Proceedings of the IEEE, 0-7803-7402, 2002.

References

- [Kun97] Kundur, D., and Hatzinakos, D., “*A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion*”, Proc. of Int. Conf. on Image Processing, no. 1, pp. 544–547, 1997.
- [Kut99-1] Kutter, M., and Hartung, F., “*Multimedia watermarking techniques*”, Proceedings of the IEEE, vol. 87, no. 7, pp. 1079–1107, 1999.
- [Kut99-2] Kutter, M., and Petitcolas, F.A., “*A Fair Benchmark for Image Watermarking Systems*”, Security and Watermarking of Multimedia Content, SPIE-3657, pp. 226-239, 1999.
- [Lin00] Lin, C.Y., and Hang, S.F., “*Semi-fragile Watermarking for Authenticating JPEG Visual Content*,” in Proc. SPIE International Conf. on Security and Watermarking of Multimedia Contents II, vol. 3971, San Jose, California, USA, January, 2000.
- [Loo99] Loo, P., and Kingsbury, N. G., “*Watermarking using Complex Wavelet*”, Technical report, Cambridge University, UK 1999.
- [Mem98] Memon, N., Craver, S., and Yeung, M., “*Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications*”,

References

- IEEE Trans. on Selected Areas of Communications, vol. 16 no. 4, pp. 573–586, 1998.
- [Min97] Mintzer, F., Braudaway, G. W., and Yeung, M. M., "Effective and Ineffective Digital Watermarks", ICIP, 1997.
 - [Mou01] Moulin, P., "The Role of Information Theory in Watermarking and its Application to Image Watermarking". Signal processing, Jun, 2001.
 - [Pal05] Palfner, T., Schlaueweg, M., and Muller, E., "A Secure Semi-fragile Watermarking Algorithm for Image Authentication in the Wavelet Domain of JPEG2000", Institute of Communications Engineering, University of Rostock, paper, Rostock, 2005.
 - [Pat01] Campsi, P., and Kundur, D., "Compressive Data Hiding: An Unconventional Approach for Improved Color Image Coding", Eurasia Journal on ASP, April, 2001.
 - [Pet99] Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G., "Information Hiding - a survey", Proc. of IEEE Special Issue on Identification and Protection of Multimedia Information, July-1999.
 - [Pit96] Pitas, I., "A Method for Signature Casting on Digital

References

- Images*”, Proc. of Int. Conf. on Image Processing, vol. 3, pp. 215–218, 1996.
- [Rey00] Rey ,C. ,and Dugelay , J. L., “*Blind detection of malicious alterations on still images using robust watermark*”,in *Secure Images and Image Authentication Colloquium*, IEE Electronics & Communications, London, UK, 2000.
 - [Rey02] Rey. C, and Dugelary J. L., "A Survey of Watermarking Algorithm for Image Authentication", EURASIP Journal on Applied signal processing, multimedia, Eurecom Institute, Sophia Antipolice, France, pp. 613-621, march-2002.
 - [San98] Sangwine, S.J., and Horne, R. E. N., “*The Color Image Processing Handbook*”, Chapman & Hall, London, 1998.
 - [Say96] Sayood, K., “*Introduction to Data Compression*”, Morgan Kaufmann Publisher, 1996.
 - [Say98] Sayrol, E., Vidal, J., Cabanillas, S., and Santamaria S. “*Optimum Watermark Detection in Color Images*”, polytechnic university, Spain, 1998.
 - [Sol77] Solar, C.M., and D.E.H., “*Automatic monitor for programs broadcast*”, United States Patent, 1977.

References

- [Soo01] Soongsathitanon, S., and Dlay, S. S., "A *New Orthogonal Logarithmic Search Algorithm for Fixed Block-Based Motion Estimation for Video Coding*", University of Newcastle, 2001.
- [Swa96] Swanson, M.D., Zhu, B., and Tewk, A.H., "Transparent Robust Image Watermarking", Proc. of Int. Conf. on Image Processing, no. 3, pp. 211–214, 1996.
- [Umb98] Umbaugh, S.E., "Computer Vision and Image Processing: A Practical Approach using CVIP Tools", Prentice Hall, Inc., 1998.
- [Wal95] Walton, S., "Image authentication for Slipper New Age", Journal of software Tools for professional programmers, vol.20, no. 4, pp. 18–26, April, 1995.
- [Wol96] Wolfgang, R. B. and Delp, E. J., "A watermark for digital images," In Proc. 1996 IEEE International Conference on Image Processing, vol. 3, pp. 219–222, Lausanne, Switzerland, September 1996.
- [Wol99] Wolfgang, R.B., Podilchuk, C.I., and Delp, E.J., "Perceptual Watermarks for Digital Images and Video", Proc. of the IEEE, vol. 87, no. 7, pp. 1108–1126, 1999.

References

- [Yeu97] Yeung, M., and Mintzer, F., “*An Invisible Watermarking Technique for Image Verification*”, Proc. ICIP 1997, Santa Barbara, California, Oct.1997.

Appendix A

The BMP file format

The bmp file structure is very simple and shown in Figure (A.1):

File Header	Image Header	Color Table	Pixel Data
--------------------	---------------------	--------------------	-------------------

Figure (A .1) BMP File Format

File Header

Every windows BMP begins with a BITMAPFILEHEADER structure whose layout is shown in Table (A.1) .the main structure of this structure is to serve as the signature that identifies that file format.

Table (A .1): Bit Map file header structure.

Field Name	Size In Bytes	Descriptions
bfType	2	Contains the character "BM" that identify the file type
bfSize	4	File Size
bfReserved1	2	Unused
bfReserved2	2	Unused
bfOffbits	4	Offset to start of pixel data

Three checks can be made to ensure that the file you are reading is in fact a BMP file:

- The first two bytes of the file must contain the ASCII characters "B" followed by "M".

- If you are using a file system where you can determine the exact file size in bytes, you can compare the file size with the value in the bfSize field.
- The bfReserved1 and bfReserved2 fields must be zero.

The file header also specifies the location of the pixel data in the file. When decoding a BMP file you must use the bfOffbits field to determine the offset from the beginning of the file to where the pixel data starts. Most applications place the pixel data immediately following the BITMAPINFOHEADER structure or palette, if it is present. However some applications place filler bytes between these structures and the pixel data so you must use the bfOffbits to determine the number of bytes from the BITMAPFILEHEADER structure to the pixel data.

Image Header

The image header immediately follows the BITMAPFILEHEADER structure. It comes in two distinct formats, defined by the BITMAPINFOHEADER and BITMAPCOREHEADER structures. BITMAPCOREHEADER represents the OS/2 BMP format and BITMAPINFOHEADER is the much more common windows format. Unfortunately, there is no version field in the BMP definitions. The only way to determine the type of image structure used in a particular file is to examine the structure's size field, which is the first 4 bytes of both structure types. The size of the BITMAPCOREHEADER structure is 12 bytes; the size of BITMAPINFOHEADER, at least 40 bytes

The layout of BITMAPINFOHEADER is shown in Table (A.2) this structure gives the dimensions and bit depth of the image and tells if the

image is compressed. Windows95 supports a BMP format that uses an enlarged version of this header. Few applications create BMP files using this format; however; a decoder should be implemented so that it knows that header sizes can be larger than 40 bytes. The image height is unsigned value. A negative value for the **biHieght** field specifies that pixel data is ordered from the top down rather than the normal bottom up. Images with a negative **biHeight** value may not be compressed.

Table (A.2) Bit Map info Header structure.

Field Name	Size	descriptions
bisize	4	Header size must be at least 40
biwidth	4	Image width
biHieght	4	Image height
biplanes	2	Must be 1
bibitcount	2	Bits per pixel:1,4,8,16,24, or 32
bicompression	4	Compression type :BI_RGB=0, BI_RLE8=1, BI_RLE4=2,or BI_BITFIELDS=3
bisizeimage	4	Image size: may be 0 if not compressed
bixpelspermeter	4	Preferred resolution in pixels per meter
biypelspermeter	4	Preferred resolution in pixels per meter
biclused	4	Number of entries in the color map that are actually used
biclrimportant	4	Number of significant color

The BIT MAPCOREHEADER structure is the other image header format. Its layout is shown in Table (A .3):

Table (A. 3): Bit Map Core Header structure.

Field Name	Size	Descriptions
bcSize	4	Header size must be 12
bcWidth	2	Image width
bcHieght	2	Image height
bcplanes	2	Must be 1
bcBitCount	2	Bit count : 1,4,8,or 24

Notice that it has fewer field and that all have analogous fields in the BITMAPINFOHEADER structure if the file uses BITMAPCOREHEADER rather than BITMAPINFOHEADER, the pixel data cannot be compressed.

Color Palette

The color palette immediately follows the file header and can be in one of three formats .the first two are used to map pixel data to RGB color values when the bit count is 1,4,or 8 (biBitCount fields). For BMP files in the Windows format, the palette consists of an array of 2 bitcount RGBQUAD structures Table (A.4). BMP files in OS/2 format use an array of RGBTRIPLE structures Table (A.5).

Table (A.4): BRGBQUAD structure.

Field Name	Size	Descriptions
rgbBlue	1	Blue color value
rgbGreen	1	Green color value
rgbRed	1	Red color value
rgbReserved	1	Must be zero

Table (A.5): BRGTRIPLE structure.

Field Name	Size	Description
rgbBlue	1	Blue color value
rgbGreen	1	Green color value
rgbRed	1	Red color value

الأسم: زينب حسين كاظم عباس التميمي.

سنة التخرج: بكالوريوس ٢٠٠٥.

التحصيل الدراسي: ماجستير - علوم حاسبات.

الجامعة: جامعة النهريين.

المواليد: ١٩٨٤.

العنوان: بغداد - العراق.

عنوان السكن: محله : ٧٢٦ ، الزقاق: ٥٥، الدار: ١/٨

تاريخ المناقشة : ٢٨-٥-٢٠٠٨

رقم الهاتف: لا يوجد

الايمل: ZHk_84@yahoo.com

اسم المشرف: د. علي كاظم موسى.

عنوان الاطروحة: وثوقية الصور باستخدام العلامة

المطمورة