
# Digital Image watermarking

**---------An overview**

**Mentor : C.V.Jawahar**

**Faculty IIIT –Hyderabad.**

**(Indian Institute of Information Technology)**

**jawahar@iiit.net**

**Done by: Gaurav Jain**

**Roll no :98014**

**Student ,IIIT –Hyderabad.**

**gaurav@gdit.iiit.net ,**

**gjain_iiit@chequemail.com**

**T. Srinivas Choudary**

**Roll no :98041**

**Student ,IIIT –Hyderabad.**

**srinivas@gdit.iiit.net , srinu001@hotmail.com**

## Watermarking history

Watermarks made their first appearance in the thirteenth century in Italy. Most notables adopted their own watermarks, and letters preserved from that time still bear their author's coats of arms and royal crests. Like wax seal, a watermark was an emblem of prestige, and also guarded the security of personal correspondence.

Like the finest papers, the true watermark remains a thing of rare craftsmanship, changed little in its manufacture in over seven centuries. With today's improved paper machines, watermarks are now clearer, and are used in most of the world's banknotes as they are difficult to forge without the craftsmanship required to produce the genuine article.

## Introduction:

In our Information Age, more and more textual, image, and audio data find their way from traditional media, e.g. paper or vinyl discs, to digital media. Digital representation of media potentially improves the accessibility, portability, efficiency, and accuracy of the data. Undesirable effects of the accessibility include an increased opportunity for violation of copyright or modification of content. Data hiding (or steganography) tries to solve some of these undesirable effects by embedding data, such as copyright information, into various forms of media with a minimum amount of perceivable degradation of the original signal.

Since the advent of computers there has been a vast dissemination of information, some of which needs to be kept private, some of which does not. The information may be hidden in two ways.

- Steganography techniques
- Cryptography techniques

(Since the theme of this document is steganography and watermarking we would like to discuss very little about the cryptographic techniques but deal in detail about the steganographic techniques.)

**Cryptography techniques:**

The methods of cryptography on the other hand don't conceal the presence of secret information but make it unintelligible by applying various transformations. The cryptologist is the entity that performs cryptography. With cryptography there is always the possibility of cracking the code.

**Steganography techniques:**

Steganography is a science, which dates back to ancient times. Ordinary people, governments, armies, spies and rulers have used it. Information has been hidden in writings ,drawings (images in the current context) and in speech etc.

Steganography is derived from two Greek words stego which means roof or cover and graphy which means writing. So steganograpy means cover writing.

The methods of steganography conceal the very fact of the existence of the secret information. It is one of various **data hiding techniques**, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. With steganography there is the possibility that the existence of the secret information in the image or writing can be discovered. The stegator is the entity that performs steganography. On the other hand the cryptanalyst is the one who tries to break the cryptographic code or find the steganographic information.

If there is vast quantity of information that needs to be kept secret there is no use of applying steganographic techniques. The main use of steganography is in sending or hiding short messages that needs to be secure.

On computer systems there are lots of examples of random looking data like graphical image files, compressed files; sound and audio files etc .It is this randomness that can be exploited to conceal the presence of the message. If data looks and random and the randomness of the data doesn’t change the randomness then steganography is achieved.

Steganographic data in JPEG image is harder to detect with naked eye than with the same data in raw 8 bit or 24 bit image files.

A typical example can be stated as follows:

A PC disk file can contain bad sectors. These sectors are marked as unusable in the FAT. The data in an unformatted disk is random and is different from disk to disk .A steganographic application can be developed that would describe some sectors that are readable as bad in FAT and use these to hold the sensitive data.
Blocks of deleted executable files can also be used to store the sensitive data.

## Data hiding in various media

Data Hiding in Text:

Soft-copy text has a relatively lack of redundant information compared to image or sound files. A reader, even only a period, can easily notice newly added text. Therefore, date hiding techniques focus to the discovery of modifications that are not noticed by readers. Three major methods can be distinguished:

1. **open space methods** that encode messages through manipulation of the white space and unused space on the page,
2. **syntactic methods** that utilize punctuation, and
3. **Semantic methods** that manipulate the words themselves.

Syntactic and semantic methods generally do not interfere with the open space methods, thus these can be applied in parallel. We will give an overview of some techniques for encoding with these three methods.

Open Space Methods:

This methods exploit inter-sentence spacing, end-of -line space, and inter-word spacing in justified text , and they are a to some programs which may remove extra spacing (e.g. sendmail), or programs which automatically modify spacing (e.g. word-processors which set a space after periods.)

A first method with low bandwidth encodes a binary message into a text by placing either one space for `0` or two spaces for `1` after each terminating character. The language justifies the terminating characters e.g. period for English text, semicolon for C-code, etc.

A second method with higher bandwidth is to insert spaces at the end of each line. The number of spaces is predetermined,

Syntactic methods:

Syntactic methods make use of ambiguous punctuation, and changing the text without changing the meaning. The former should be used with caution since inconsistent use of punctuation is noticeable, and might impact clarity or even meaning. The latter are more transparent.

As an example of exploiting ambiguous punctuation consider the phrases

*Bread, butter, and milk*
*Bread, butter and milk*

Which are both considered correct usage of commas in a list. Alternation between these two forms can encode binary data.

As an example of changing text without changing the meaning, the phrase

*Before the night is over, I will have finished*

could be stated as

*I will have finished, before the night is over.*

These methods encode information in the word usage. An online thesaurus like WordNet groups synonymous words into senses. Take as en example a synonym set:

*{propensity, predilection, penchant, proclivity}*

These words are interchangeable in a certain context. The choice to use one of these four words to represent the sense can encode two bits of data. Of course, the problem of selecting the right synonym set according to the context (word-sense disambiguation) becomes very important for using this technique.

Data Hiding in Images:

Data hiding in images presents a variety of possibilities due to the way the Human Visual System (HVS) works. Many attributes of the HVS are potential candidates for exploitations such as our varying sensitivity to contrast as a function of spatial frequency and the masking effect of edges (both in brightness and color). Moreover a typical Cathode Ray Tube (CRT) display or printer has a limited dynamic range because of technical limitations.

Data Hiding in Images is the basic theme of this document and will be discussed in detail subsequently.

Data Hiding in Audio:

The Human Auditory System (HAS) operates over a wider dynamic range than the HVS, consequently data hiding in audio signals is especially challenging. Perturbations in a sound file can be detected as low as one part in ten million (-80 dB).

While HAS has a large dynamic range, it has a small differential range, and as a result, loud sounds tend to mask quiet ones. Additionally, the HAS does not perceive absolute phase, but only relative phase. Finally there are some environmental distortions so common as to be ignored by the listener in most cases. These "holes" can be exploited by data hiding techniques.

There are 2 parameters in the digital representation of sound: sample quantization and sampling rate. Typically, quantization is linear 16-bit or logarithmic 8-bit. Sampling rate varies from 8kHz to 44.1kHz (CD quality). According to the theorem of Nyquist the maximum usable sound frequency is bounded by sampling-rate/2. These characteristics of the digital signal play an important role in the data hiding techniques.

The transmission environment of the signal has an impact on data hiding. Four transmission environments can be distinguished:

- **digital**. The signal is copied from source to destination without any modifications.
- **re-sampled**. The signal is re-sampled to higher or lower sampling rate. Signal magnitude and phase are usually preserved, but quantization might not.

- **analog**. The signal is transformed to analog, transmitted over an analog channel, and re-sampled again at the destination. Sampling rate, magnitude, and quantization are not preserved. In general, phase will be preserved.
- **over-the-air**. In this case the signal is played "over the air" and it is re-sampled with a microphone. None of the original signal's characteristics are preserved.

Some data hiding techniques for audio,

Low Bit Encoding:

Low-bit encoding is practically useful only in digital transmission environments and introduces audible noise.

By replacing the least significant bit of every sample by a coded binary string, a large amount of data can be encoded, ideally 1 Kbps per 1 kHz of sampling rate.

This method has poor immunity to manipulation, but it can be improved by using redundancy.

Phase Coding:

Phase Coding is one of the most effective data hiding methods in terms of signal-to-perceived-noise ratio. It encodes data by substituting the phase of an initial audio (frequency) segment with a reference phase that represents the data. This method offers a typical bandwidth of 8 to 32 bps. Distortion is introduced due to phase dispersion, a break in the

relationship of the phases between each of the frequency segments. Minimizing phase dispersion constrains the data rate.

Spread Spectrum:

The basic Spread Spectrum technique is designed to encode a stream of information by spreading as much as possible the encoded data across the frequency spectrum. This allows the signal reception, even if there is interference on some frequencies. The technique offers low data rate with a typical value of 4 bps.

Echo Data Hiding:

Echo Data Hiding embeds data into audio signals by introducing an echo. There are three parameters of the echo: initial amplitude, delay, and decay rate. Echo's which have a very short delay (typically less than 1 msec) are indistinguishable by the HAS. Two different short delay times are used to represent the binary 0 and 1. To ensure further inaudibility, the initial amplitude and decay rate are adjusted below the audible threshold of the human ear.

Experiments have shown that it is possible to encode and decode information using Echo Data Hiding with minimal alteration to the original signal at approximately 16 bps.

**Data Hiding (Watermarking) in the java source code:**

It is a well-known fact that the java class files can be decompiled to get the original source code (Decafe, Jade etc are java decompilers). This is possible because of the specific structure used by the java compiler to create the class file. With java becoming a very popular language and many applications being developed through out the world, the need to protect the copyright of the java applications (or tools) has arisen. Though anti-decompilers are available, they are not very popular. So watermarking has been suggested as a solution for this problem. The source code is watermarked and then converted to a class file or the class file is watermarked. This establishes the copyright of the author in the programs (or applications) thus protecting the intellectual property rights of a work.

SandMark is a system for embedding a watermark in a Java program. It modifies the application source code to make it build a structure at execution time that encodes a watermark. Dumping and analyzing the Java heap recognize the watermark.

The ultimate goal is to produce application watermarks that an adversary can remove only through careful analysis, not through automated means. SandMark makes changes to the application programs that are easily spotted. For a robust system it would be necessary to obfuscate the resulting program to obscure the SandMark modifications.

Two different applications of steganography are:

- Classical steganography – the aim here is to transmit a message by another innocent or casual looking system.

- Watermarking –the aim here is to access the ownership or integrity of some pieces of information named after the watermarks.

Both classical steganography and digital watermarking are based on a fundamental assumption: *it is quite easy to foil the human senses*

This fundamental assumption gives rise to a simple formula

$$D+I < T$$

Where D: original piece of data

T: the threshold below which any changes made to the data cannot be perceived by the human eye.

I: affordable change that can be made on D.

The formula can be replaced with the entropy function H().

Assuming that the message we insert is perfectly encrypted, then it is indistinguishable from random data, so the entropy will be strictly additive. The entropy of the stego-medium S will be given by the sum of the entropy of the cover C and of the embedded message M:

$$H(S) = H(C) + H(M)$$

And the embedded message would be undetectable if:

- The entropy H(M) is much less than the uncertainty in the attacker's measurement of H()
- H(C) is reduced by some means before processing, so it is restored by adding H(M)

As a rule of thumb the attacker must be given very little data.

A tradeoff exists between the ratio of hidden information over the normal ones, and the subsequent robustness of the embedded message. So a  simple formula can be derived when given a piece of information in which we want to hide some data and being sure that the data is ideally undetectable,

$$amount\_of\_hidden\_data \times robustness = constant$$

So the amount of hidden data can only be increased only at the expense of robustness

Classical steganography is used as a service, which is important for both the transmitter and the receiver. Hence we'll want to push up as much as we can the amount of data hidden, and eventually losing robustness.

But we have a different setting with the watermarking perspective, the watermark is to be inserted by the transmitter and it must avoid any counterfeit or destruction at the receiver (by any person) .This demands the robustness of the embedded data. i.e., the data we need to insert in an image or audio (any data) must be robust, and it leaves us with a little freedom on the amount of data that can be embedded in any data and the watermarking data must be as small as possible.

**Watermarking in detail:**

The topics covered subsequently will deal with image watermarking .It has to be assumed that the watermarking is in images unless explicitly stated. (as audio watermarking ,video watermarking etc).

The large diffusion of multimedia products distributed both through CD-ROMs (off-line) and through Internet (on-line) that can be observed in the present years, is raising many concerns among the authors regarding the preservation of their rights. On the other side, such new publications appear to be very attractive for increasing business opportunities. The problem of electronic management of copyright has thus become very important. Traditional laws on IPR (Intellectual Property Rights) protection do not seem suitable to solve all the problems raised by this technological revolution. Just the fact that each work could be easily digitized, stored and transmitted without loss of quality an almost uncountable number of times, is causing, at the international level, the revision of the concept of IPR(Intellectual Property Rights) protection itself.

In particular, two technological revolutions have made the problem of IPR protection so new and challenging today. The first is the advent of digital techniques, and the second the explosion of

telematic networks. The possibility to represent every kind of work (being text, picture, video, music, …) in a digital format has given birth to a new type of creation, i.e. multimedia creations, where different kind of data can be integrated to produce a new composite object. This possibility offer a big chance to authors to better express their creativity, but, on the other side, the IPR problem becomes quite complex: in order to compose the new object, all its components have to be licensed by respective authors.

Digital watermarking is a very recent research area, therefore its intrinsic limits are not well understood yet. On the other hand, more insight into the technical possibility of satisfying the requirements imposed by practical applications is needed, if the practical possibility of using watermarking for copyright protection is to be evaluated. Some of the most common limits shared by digital watermarking schemes are as follows. Unlike encryption watermark does not restrict access to an image.

- Even if the evaluation of the maximum number of information bits that can be hidden within a piece of data of a given size plays an important role, such an issue has not been satisfactorily addressed yet. Existing works addressing this problem model the watermarking process as a communication task. According to Smith and Comiskey and Servetto et al. the watermark-channel is modeled as an AWGN channel, so that the corresponding capacity theorem can be used; such an analysis, however, can only be applied to particular cases. In the work of Barni et al. an appropriate statistical model for the watermark-channel is obtained and the relative capacity is

then calculated, but the presented results do not take into account attacks.

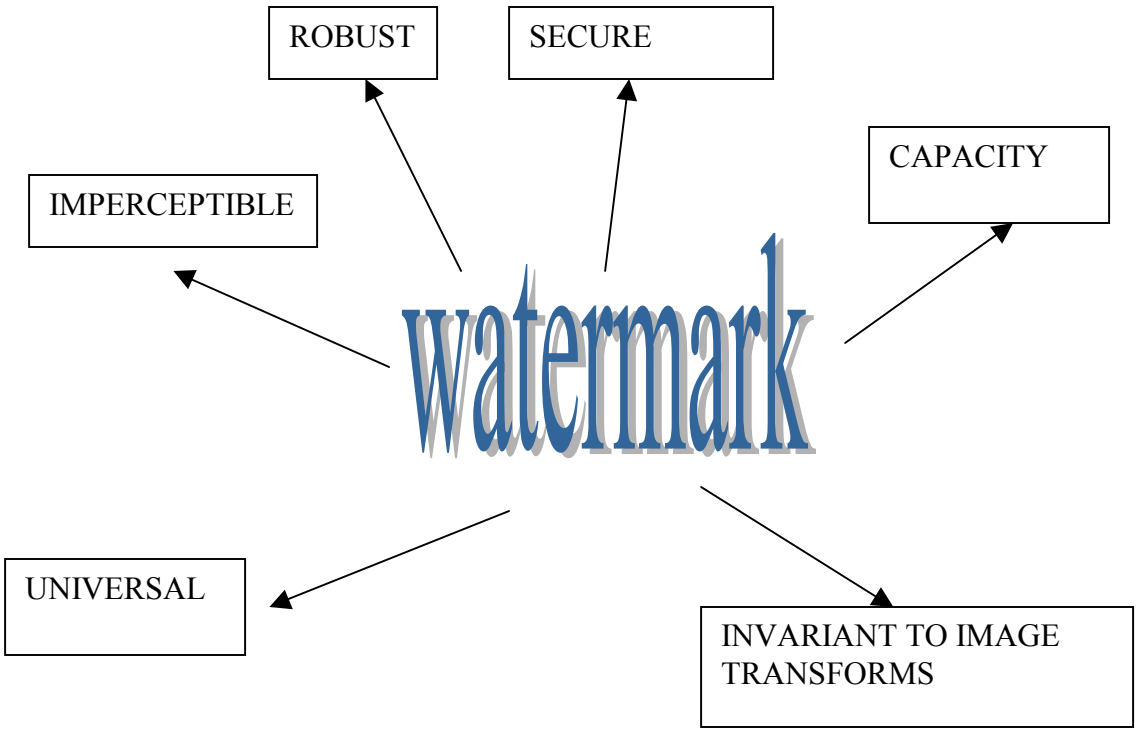
- A blind watermarking algorithm that is really robust does not exist yet. In the image case, robustness is still an open issue. More specifically, resistance to geometric manipulations such as cropping, is recognized as a very difficult goal to achieve in a computationally efficient way. But there exists many solutions to watermarking that can solve a specific set of problems but not resistant to all the types of attacks. (A good number of watermarking algorithms will be discussed later).
- Owners can erase the mark: virtually all the blind watermarking schemes proposed so far are reversible. In other words, by knowing the exact content of the watermark, and the algorithms used to embed and retrieve it, it is always possible to make it unreadable without any significant degradation of the data. In addition, the reversibility of the algorithms proposed so far, raises severe doubts on the possibility of developing a public watermarking technique, which is also robust against tampering. As a matter of fact, if anyone is allowed to read the watermark, then anyone can erase it once the embedding algorithm is known.

**Features a watermark should have:**

In order to be effective a watermark

- Should be unobtrusive ( perceptually invisible)

- Should be robust
- Should be universal i.e., should be applicable to all three media under consideration
- Should be resilient to common signal processing and geometric distortions and intentional attacks. Intentional attacks include forgery and attacks using one or more watermarked copies of a document.
- Should be invariant to complex transformations like cropping ,mosaicing ,inversion and other simple geometric transformations like rotation, scaling and translation.
- Should not be destroyed by image compression.
- Should be secure
- Should have high capacity


ROBUST
SECURE
CAPACITY
IMPERCEPTIBLE
watermark
UNIVERSAL
INVARIANT TO IMAGE TRANSFORMS

***WATERMARK FEATURES***

high imperceptibility
universally applicability
invariance to image transforms
capacity should be high
highly secure
highly robust

Watermarks can be embedded in different domains , can be of different sizes ,can be extracted in different ways .So a classification of different types of watermarking is essential .Although these can be classified in various from , we will try to cover  a lot of them .But all kinds of classifications may not be possible to deal with. So we restrict our discussion with a few classifications and specify as many as possible from the rest.

## Types of watermarking:

A broad classification of watermarking (Other classifications based on some other fields will be discussed subsequently).

- Visible: Perceptible

- Invisible: Perceptually transparent
    - Fragile: breaks down by slightest image alteration.

- Robust: Survives severe manipulation and tampering
    - Private: requires original or reference image for watermark detection
    - Public: Doesn't require the original image for detection

## **Visible watermarking**:

The embedded watermark will be visible. The image shown below shows an image watermarked with a visible stamp (can be seen as a light background).

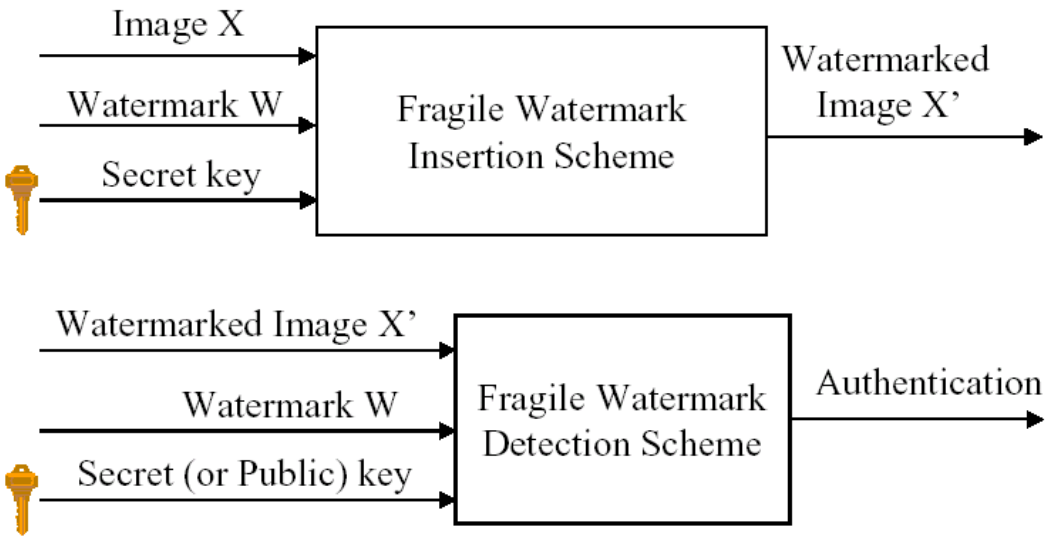
source: IBM website

*Don't copy the image, download it from the IBM website

# Invisible watermarking:

## *Fragile watermarking:*

The slightest alteration of the image destroys the watermark. Used for authentication at a pixel or small block level.




A random key is used to build  a look up table that maps image pixel values to a binary value. The watermark is a binary image with the same dimensions as the original image. For every pixel in the image the value of the LUT is found (with that pixel value as input) and compared to the watermark binary value at that location:

- If the same ,pixel value is left unchanged
- If different the pixel value is altered by the smallest amount needed to create the desired output.

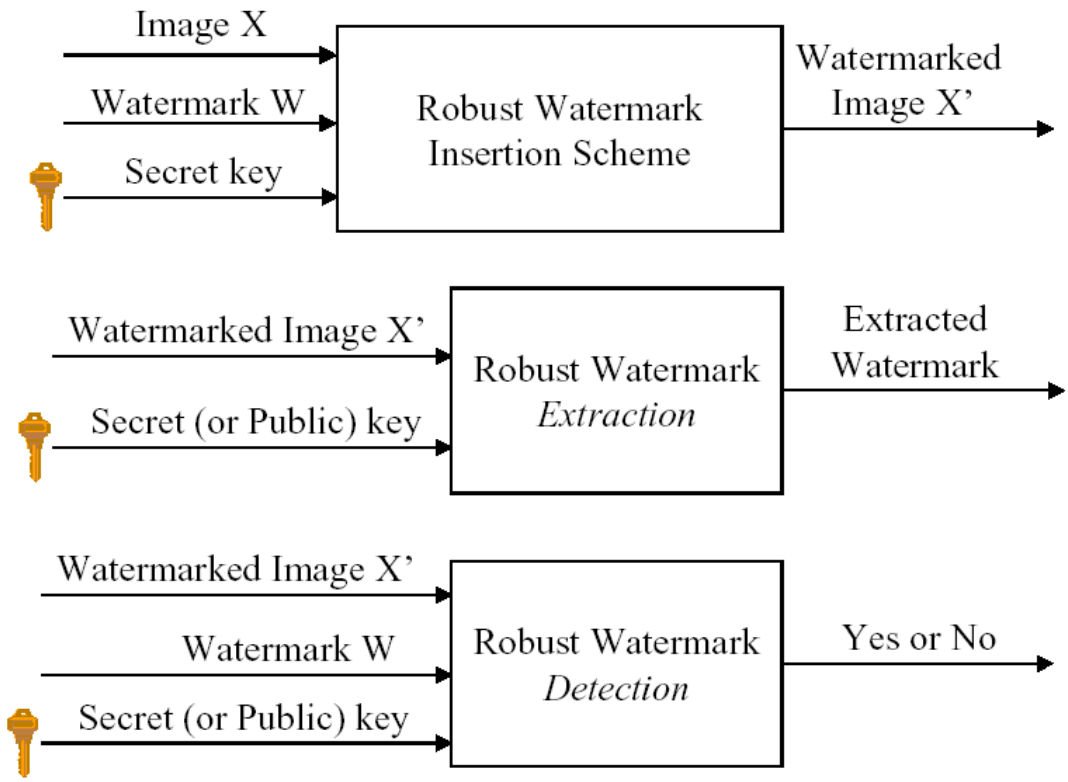
Advantages:

- Authentication is done on a pixel-by-pixel basis.

Disadvantages:

- Difficult to adapt to applications where JPEG compression (or any other lossy compression )is used.
- The original image after watermarking may be perceptually different.

## ***Robust watermarking:***




The desirable properties of a robust watermarking are

- Perceptual transparency
- Data capacity
- Robustness to unintentional image processing operations (e.g., compression, linear and non linear filtering ,random noise ,rotation and scale , cropping and analog conversion).
- Tamper resistance: difficult for an attacker to destroy and remove or alter or forge a message once it has been embedded in an image.
- Computational complexity
- Need for an original image

Robust watermarking techniques can be further divided

## Spatial domain techniques:

The watermark is embedded in the spatial domain i.e. in the two dimensional space of an image. Most popular technique is embedding the watermark in the LSB of the image. The original 8-bit image is adaptively histogram manipulated and is compressed to 7 bits. The resultant image is practically indistinguishable from the original .This process enables the LSB of the image to carry the watermark information. The watermark can be decoded by comparing the LSB bit pattern with the stored counterpart. The watermark may be spread through out the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed.

There are more advanced methods of spatial domain techniques like

Patchwork technique

Digimarc algorithm (proprietary)

### ***Patch work method:***

A secret key is used to randomly select a subset of pixels from an image and then divide it into two distinct sets. The brightness of one set of pixels is shifted by a positive number while the brightness of those in the other set are shifted by the corresponding negative number.

Detection: Detection procedure consists of partitioning the image into the corresponding sets using the secret key and computing the mean

intensities of the pixels in each group and finding their difference (the difference is almost equal to zero for an unmarked image ).

Restriction: Only a limited amount of data can be embedded , even if the image is divided into several sets and a different bit is embedded in each set.

***Watermarking Insertion technique of Digimarc:***

To embed N bits of information , N sequence of random numbers ,each with the same dimension as that of the image are generated ( a user private key can be used to generate Gaussian random numbers). The random numbers in each sequence are multiplied by their corresponding message bit values and added together to create a message image. The amplitude of the message image is attenuated down to acceptable perceived noise amplitude to create the watermark image, which is then added to the original image.

Extraction of the watermark:

The original image is needed for watermark extraction. The image in question is first normalized both in scale and in RMS sense and is then subtracted from the original. The signal is cross correlated with each of the N embedded message bits and the peak cross correlation value is recorded and used to decide the presence of 0 or 1.

M-Sequences:

A linear feedback shift register with n stages can form pseudo random binary sequences with periods as large as pow(2,n)-1. m sequences achieve this maximum period and have excellent randomness and auto-correlation properties .To generate the watermark a binary sequence is mapped from {1,0 } to {1,-1}, arranged into a suitable block, and added to the image pixel values.

Advantages of M-Sequence watermarks:

- Multiple watermarks can overlap with each other and will not change the average value(brightness) of the image. Successive watermarks treat the watermarked image as the original image.
- An attacker can only swap pixels with the same m-sequence bit without affecting the correlation properties.
  This requires knowledge of the private embedded sequence to successfully forge any reasonable area of the image.

Disadvantages of M-Sequence watermarks:

- An attacker could compute an entire watermark block if *2n* consecutive bits are known. More secure nonlinear codes, such as the Gold or Kasami codes, address this problem.
- This method does not specifically protect the DC value of the pixels covered by an individual block.
- If the watermark covers the entire image, an attacker must merely guess if a given pixel has increased or decreased by one gray level to identify a particular bit in the watermark.

There are many other techniques developed for proprietary usage by many commercial organizations whose details will not be discussed. An example of this kind is the method developed by Kodak. (Kodak watermarking algorithm).

***Spread Spectrum technique : (frequency domain)***

The most popular algorithm in this domain is Cox et al spread spectrum watermarking technique. The details of Cox et al algorithm follows.

Compute the full frame DCT of the original image. (For larger finding the DCT of a whole image may bean uphill task .So a fast implementation of the DCT like 2D FFT (fast Fourier transform ) can be used. This improves the performance of the algorithm (in terms of speed) to a large extent.

After finding the DCT or FFT of the image, perceptually significant coefficients of the image have to be found (usually 1000 coefficients are chosen).The perceptually significant coefficients are the coefficients with highest absolute value among the coefficients. The first coefficient (i.e. the DC coefficient will not be considered). But why do we need to select the perceptually significant regions only????
This is to stop the attackers from removing the watermark from the image without degrading the quality of the image. Even slightest changes made to the perceptually significant regions will affect the quality of the image since the changes can be easily perceived.
The watermark is constructed as

$$X = x_1, x_2, \ldots, x_n,$$

where each

each $x_i$

is chosen according to a gaussian distribution with mean and variance generated with a user private key.

The watermark is inserted into the DCT domain by modifying the DCT coefficient

$v_i$

according to :

$$v_i \leftarrow v_i(1+\alpha_i x_i).$$

where

$\alpha_i$

is the scaling factor.

The inversed DCT (or FFT) of the modified image gives the transparently watermarked image.

Normally X = x1, x2 ,x3 ……..xn can be a sequence of real numbers but if the noise (watermark) is normally distributed then the watermark is difficult to break. Normally distributed noise is chosen so that the mean is zero and variance is one. The choice of n dictates the degree to which the watermark is spread out among the relevant

components of the image. If the number of altered components are increased then the extent to which they must be altered decreases.

Advantages: (as claimed by Cox et al)

- The technique is analogous to spread spectrum communication, hiding a narrow band signal (here watermark ) in a wide band channel (here image data).So the watermark is hard to remove.
- Robust to common signal and geometric distortions such as
    - digital to analog conversion and analog to digital conversion
    - resampling
    - quantization
    - dithering
    - compression
    - rotation
    - translation
    - cropping and
    - scaling
- The same digital watermarking algorithm can be applied to all the three media with minor modifications.
- Since gaussian watermarks are used the probability of destroying the watermark is very low.
- Multiple sequential watermarking is an added advantage. A watermarked image can be watermarked with another watermark as if the image is not previously watermarked .That is adding noise to the watermarked frequency bins is not a disadvantage. This

proves that additive noise is not harmful to the technique.

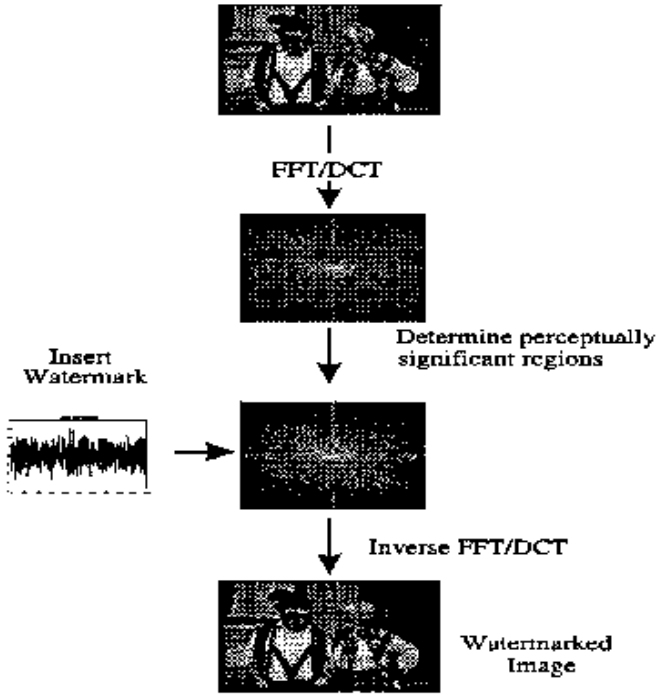



Figure 1: Stages of watermark insertion procedure.

Extraction of the watermark:

The DCT /FFT of the original image is taken. The DCT/FFT of the corrupted image is taken. Their difference is calculated. If the difference is similar to the watermark inserted then, the image is not corrupted or else it is corrupted .How is the similarity measured ??? If X is the original watermark embedded and X* is the extracted watermark then similar(X, X*) = (X.X*) / (sqrt(X*.X*)).

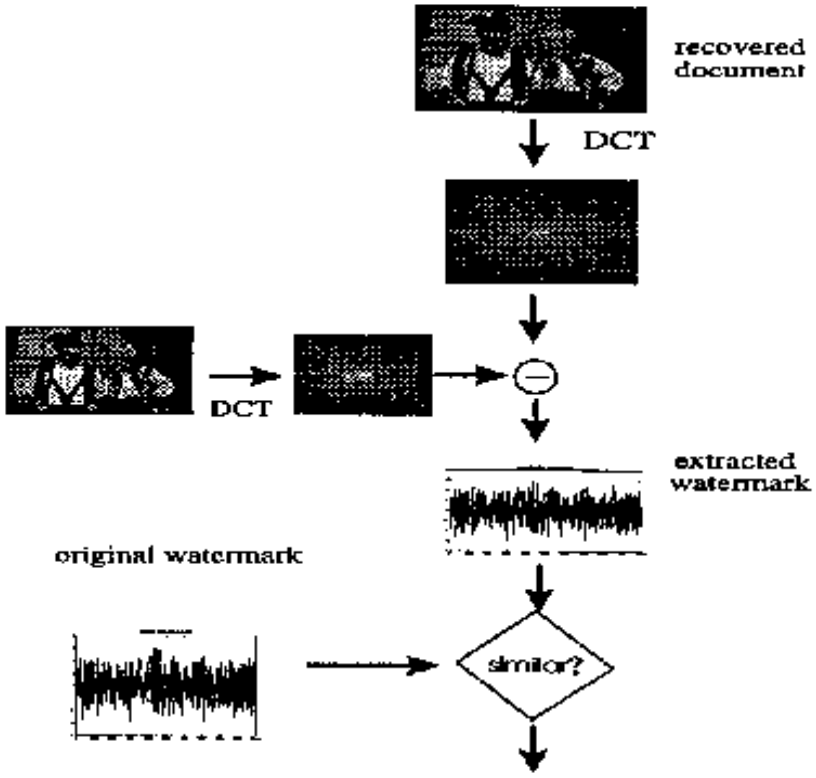



Figure 2: Stages of watermark extraction procedure.

The watermark that needs to be embedded must be normally distributed. Because normally distributed watermarks are resistant to multiple document attacks that use t multiple watermarked copies D1,D2,D3,D4……..Dt of a watermarked document D to get an unwatermarked document D*.So gaussian watermarks are better than ordinary watermarks when the size of watermark is large.

Suggested improvements:

Instead of choosing the 1000 most perceptually significant regions , an adaptive mechanism for choosing the highly perceptible components can be used based on the properties of the "human visual system" and an analysis of the image ,but that means sufficient amount of heuristics need to be assumed.

Extensions:

The same algorithm may be extended to the line-art and text images. Can also be extended to the video and audio sequences ,but the time varying nature of the video and audio signals must be taken care of.

Transparent robust image watermarking:

(by Mitchell D Swanson et al )

The watermarking scheme discussed below exploits the HVS characteristics.

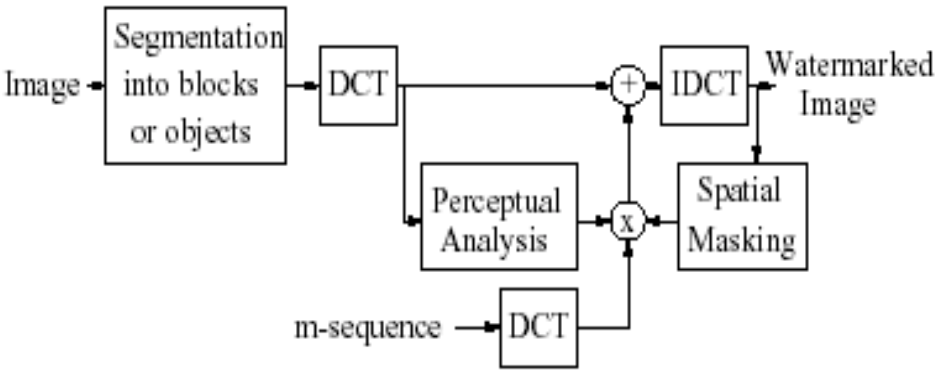
The image is segmented into blocks. The blocks may be n X n (e.g. 8X8 like JPEG).The image may also be segmented into texture regions or objects. DCT is applied to each block and a frequency mask is generated .The resulting perceptual mask is scaled and multiplied by the DCT of the maximal length pseudo noise sequence ( any key ).For each image block a different pseudo noise sequence is used. This watermark is then added to the corresponding DCT block. The watermarked image is obtained by assembling the inverse DCT of each block. Spatial masking is used to verify that the watermark is invisible and to control the scaling factor.

PN (pseudo noise) sequences are used as signatures because of their noise like characteristics, resistance to interference and their good

auto-correlation properties. They are noise like binary sequences generated by length m linear shift register.

Visual masking models are used to modify the watermarking key. Visual masking refers to a situation where a signal raises the visual threshold for other signals around it. The masking employed may be spatial or frequency or a combination of both.

Block diagram for the above watermarking technique




A model can be expressed as follows:
The contrast threshold at frequency f as a function of f,
the masking frequency

$$f_m$$

the masking contrast

$$c_m$$

$$c(f, f_m) = c_0(f) \cdot Max\{1, [k(f/f_m)c_m]^{\alpha}\},$$

where

$c_0(f)$ is the detection threshold at frequency f.

To find the contrast threshold c(f) at a frequency f in an image the DCT of the image is found out .Now the contrast at each of the frequencies is found .

A summation rule of the form

$$c(f) = [\sum_{f_m} c(f, f_m)^\beta]^{1/\beta}.$$

can be used.

If the contrast error at f is less than c(f) ,the model predicts that the error is invisible to the human eye. After adding the watermark in the frequency domain spatial masking is checked. (Why is this done???). The spatial model is used to verify that the watermark designed with the frequency masking model is invisible to the local spatial models.

To keep it simple without any mathematics it is to say that "Each watermark coefficient is compared with the tolerable error level obtained to assure that it is invisible".

Watermark detection:

Detection is assumed through hypotheses testing

H(0) = X = R – S =N (no watermark)

H(1) = X = R – S =W' + N (watermark)

Where R is pirated signal and W' is the modified watermark and N is the noise. The correct hypothesis is obtained by applying a correlating detector on X with W and comparing with the threshold.

Many variations of the HVS model can be implemented.

There are many variants of frequency domain watermarking techniques that have been found and experimentally implemented, but it is hard to discuss elaborately about all those techniques. But, a brief discussion of a few of them need a mention in this context.

A watermarking model using DCT constraints:

(by Adrian G Borg et al)

Certain blocks in the image are selected based on a gaussian network classifier. The pixel values of the selected blocks are modified such that their DCT coefficients fulfill a constraint imposed by the watermark code.

Two constraints can be considered

The first approach consists of embedding a linear constraint among selected DCT coefficients and the second one defines circular detection regions in the DCT domain.

Image watermarking using spread spectrum technique in log-2 spatio domain:

The advantage of embedding the watermark in log-2 spatio domain is to ensure the amplitude of the watermark depends on the intensity of the pixels. If the amplitude of the watermark depends on the intensities, the SNR will not be too low. We choose only the regions consisting mainly of mid-band frequency to embed the bit sequence. In the embedded process, a map is generated to describe the locations

where the bit sequence will be embedded and the map is estimated in the decoding process.

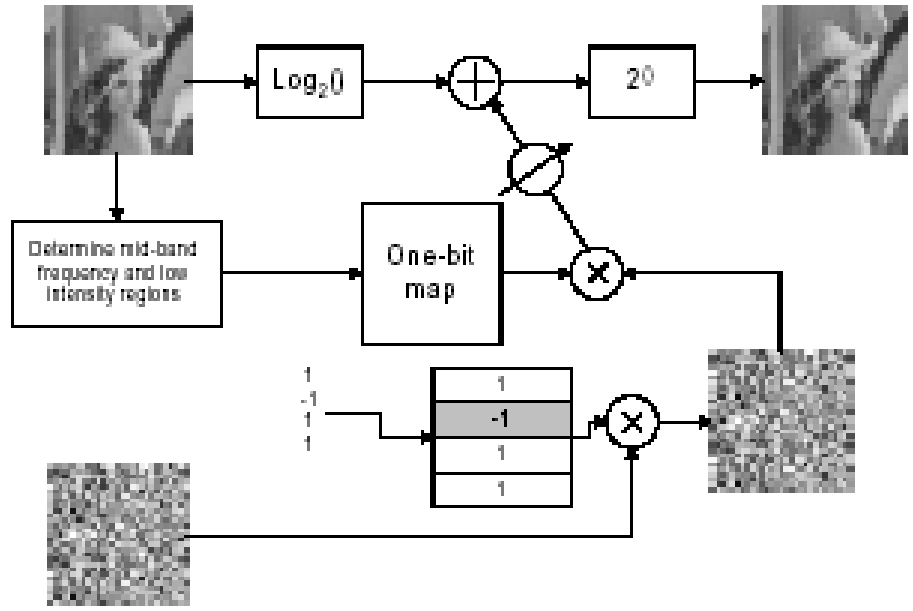



Figure 2: Visualization of the watermark embedding process in log-2-spatio domain

To transform the image to log-2-spatio domain, the intensity of each pixel in the spatio domain is passed to a log2 function. The result of the function is called the log-2-spatio domain intensity. Assuming the intensity range in the spatio domain to be [1,256] for common 8-bit image, the intensity range of the log-2- spatio domain should be [0,8]. To achieve robustness of the algorithm to JPEG compression, only the local regions with mainly mid-band frequency components are chosen. To ensure invisibility and robustness to JPEG compression, a one-bit map to locate where the bit sequence is embedded will be chosen. The dimension of the one-bit map should have the same spatio resolution. The map is generated according to the following procedures:

1. The one-bit map consists of all zeros initially.
2. The image is filtered by a band pass filter all regions such as edges.
3. Each pixel in the band passed image is compared with a threshold *T1*. If it is larger than *T1*, the corresponding bit in the one-bit map is set to one.
4. Consider now the pixel intensity of the original image. If the intensity is between *R1* and *R2*, then set the corresponding bit in the one-bit map to one. If this bit has been set to one in step 3, keep the value.
5. The one-bit map is low pass filtered. Each location of the low passed map is compared with another threshold *T2*. If it is greater than *T2*, the location is used to embed the watermark information. The reason to low pass filter the map is to ensure the watermark will not be embedded in small regions such as edges.

Estimation of map in decoding process:

1. The one-bit map is initially consists of all zeros.
2. The watermarked image is filtered by the same band pass filter used in the embedding process.
3. Each pixel in the band passed image is compared with *T1*. If it is larger than *T1*, the corresponding location in the one-bit map is set to one.
4. Consider now the pixel intensity of the original image. If the intensity is between $0.95 \acute{} R1$ and $1.05 \acute{} R2$, then set the corresponding bit in the one bit map to one. If this bit has been set to one already in step 3, keep the value unchanged.

**5.** The one-bit map is low pass filtered. Each location of the low pass filtered map is compared with *T2*. If it is greater than *T2*, the location is used to embed the watermark information.

Some watermarking algorithms in the frequency domain ,insert the watermark in many DCT coefficients rather than in the perceptually significant components. The watermark is spread over a large number of DCT coefficients. For example DCT based watermark by Piva et al leaves out the top 16000 coefficients and inserts the watermark in the next 25000 coefficients. Watermark detection is performed by correlating the 25000 components with the original copy of the watermark.

***Wavelet Domain watermarking***:

Advantages of embedding the watermark in the wavelet domain are as follows

- Watermarking in the wavelet domain is compatible with the jpeg 2000 compression standard.
- Wavelet domain provides good space-frequency localization for analyzing image features such as edges or textured areas.
- The dyadic frequency decomposition of the wavelet transform resembles the signal processing of the HVS and thus permits to excite the different perceptual bands individually. Watermarking as well as image compression can benefit from this.
- Wavelet transform has linear computational complexity of O(log n) compared to the DCT complexity which is of order O(n*log (n)).The difference is important only when the DCT is applied to

the whole image (as in Cox ) ,but when compared to a block based DCT wavelet transform is more expensive.

- The wavelet transform is flexible and can adapt to a given set of images or a particular type of application.
- Complex wavelet transform can be applied to watermark the images to attain better diagonal selectivity.

A new wavelet based scheme for watermarking images:

(by rakesh dugad , narendra ahuja et al)

A three level DWT (discrete wavelet transform) with a Daubechies 8 tap filter. The low pass sub band is left out and all the coefficients in the other sub bands, which are above a given threshold (T1). Watermark is added to these coefficients only. Though the watermark is added to only a few significant coefficients an image size watermark will be taken. The watermark at a particular location in the image is fixed, it doesn't depend on the order of the significant coefficients. Since detection is a correlation process, order independence is a crucial factor.

Smooth images like lena have a few values above the threshold T1, where as images like baboon have large number of values above the threshold T1. It is found that small coefficients in the DWT domain are more susceptible to be corrupted by compression and other image manipulations like denoising as compared to the large coefficients.

Visual masking is implicit due to the time-frequency localization properties of the DWT. High pass bands, where the watermark is

added, typically contain edge related information of the image. Further more, each coefficient in the high frequency bands affects only a spatially limited portion of the image. Thus, adding the watermark to significant coefficients in the high frequency bands is equivalent to adding the watermark to only the edge areas of the image, which makes the watermark invisible to the human visual system.

Watermark detection:

During watermark detection all high pass coefficients above the threshold T2 (T2 >T1 ,because during manipulation some coefficients just below T1 may have become just more than T1)are taken and correlated with the original value of the watermark.(for example if T1 = 40 ,T2 is chosen as 50).

The equation used in watermark casting is similar to the Cox technique

$$V_i' = V_i + \alpha \left| V_i \right| x_i$$

V'(i) = V(i) +alpha* |V(i)|* x(i);

where "i" runs allover DWT coefficients >T1

V(i) denotes the corresponding DWT coefficient of the original image and V'(i) denotes the DWT coefficient of the watermarked image. x(i) is generated from a uniform distribution of zero mean and unit variance.

The correlation "z" between DWT coefficients V1 of the corrupted watermarked image and a possibly different watermark Y is obtained by the following relation.

z = 1/M (sigma v1(i).y(i) ) where "I" runs over all coefficients >T2>T1 and M is the number of such coefficients.

The threshold S is defined as

S = (alpha/2*M) (sigma | V1(i)|) where "I" runs over all coefficients >T2>T1.

Piva et al uses a 3M coefficient in the denominator instead of 2M.The threshold is a bit more because the mutual correlation in most cases is found to be equivalent to the theoretical value.

Digital watermarking using Daubechies ' wavelets and error correcting codes: (by James G Wang et al )

The watermark is adaptively applied to different frequency bands and different areas of the image based on the smoothness of the areas , to increase robustness within the limits of perception.
The use of Daubechies advanced wavelets makes the watermarked images more perceptively faithful than the images marked with other wavelet methods. Daubechies wavelet transforms the image into clean low and high frequency parts. Many experiments revealed that Daubechies wavelets are more suited for general purpose images (the details are out of the scope of the document).

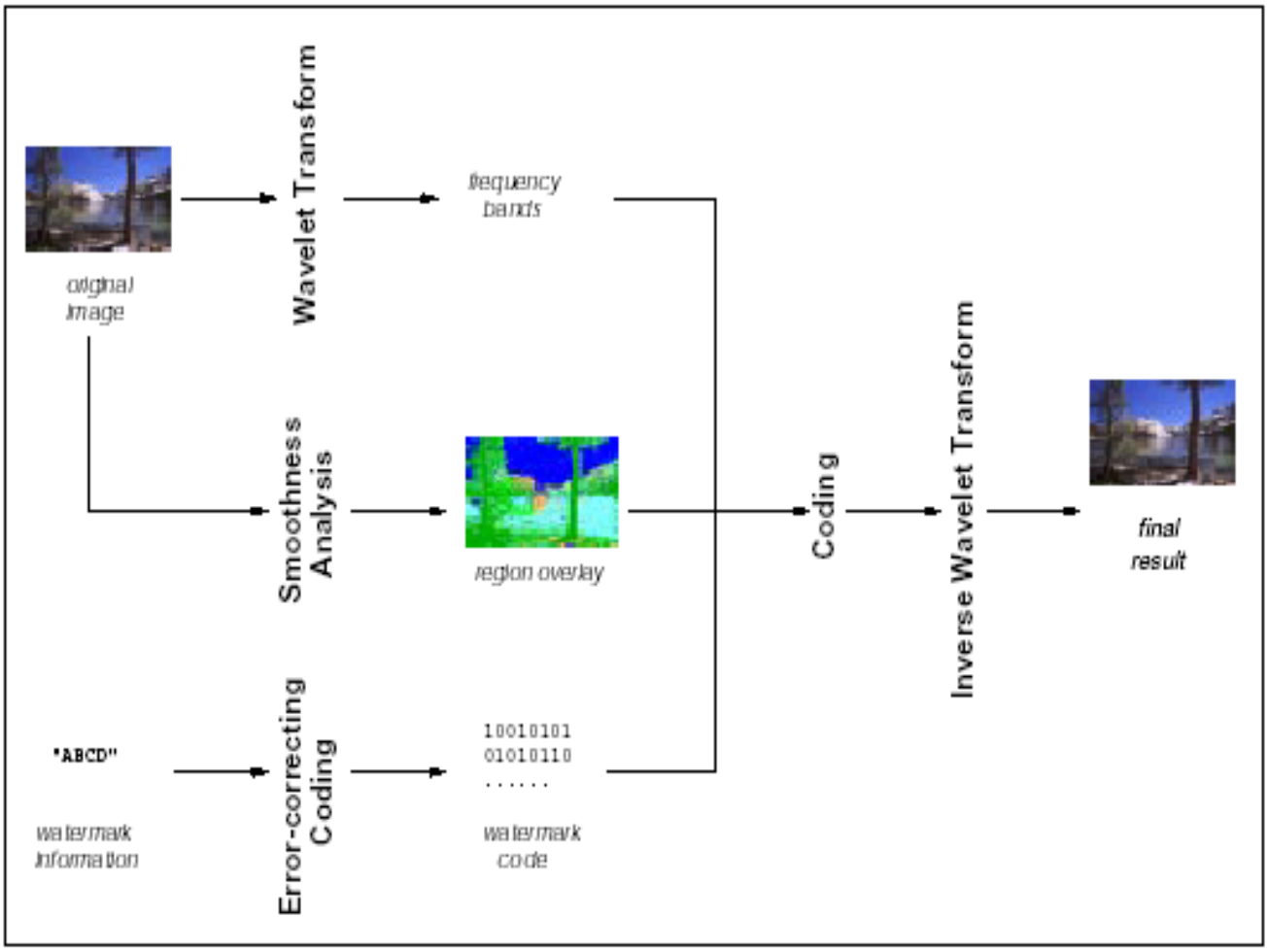
Procedure:
For each color component a 4-level wavelet transform using Daubechies 4 wavelet is performed.
Smoothness Analysis: The image is classified into different regions based on the smoothness. And watermark with the lower strength is applied to regions classified as highly smooth regions because watermark coding with higher strength in those regions introduces noticeable distortion.

Error correcting coding: A Hamming code is used to add redundancy to the bits so that the errors can be detected or corrected to an extent. Hamming code is a linear block code. The main advantage of the linear block code is their simplicity in implementation and low computational complexity. A linear block code is usually composed of two parts. The first part contains the information bits, which are the original bits to be transmitted. The second part contains the parity checking bits, which are obtained by summing over a subset of the information bits. A linear block code with length n and k information bits is denoted as a (n; k) code.

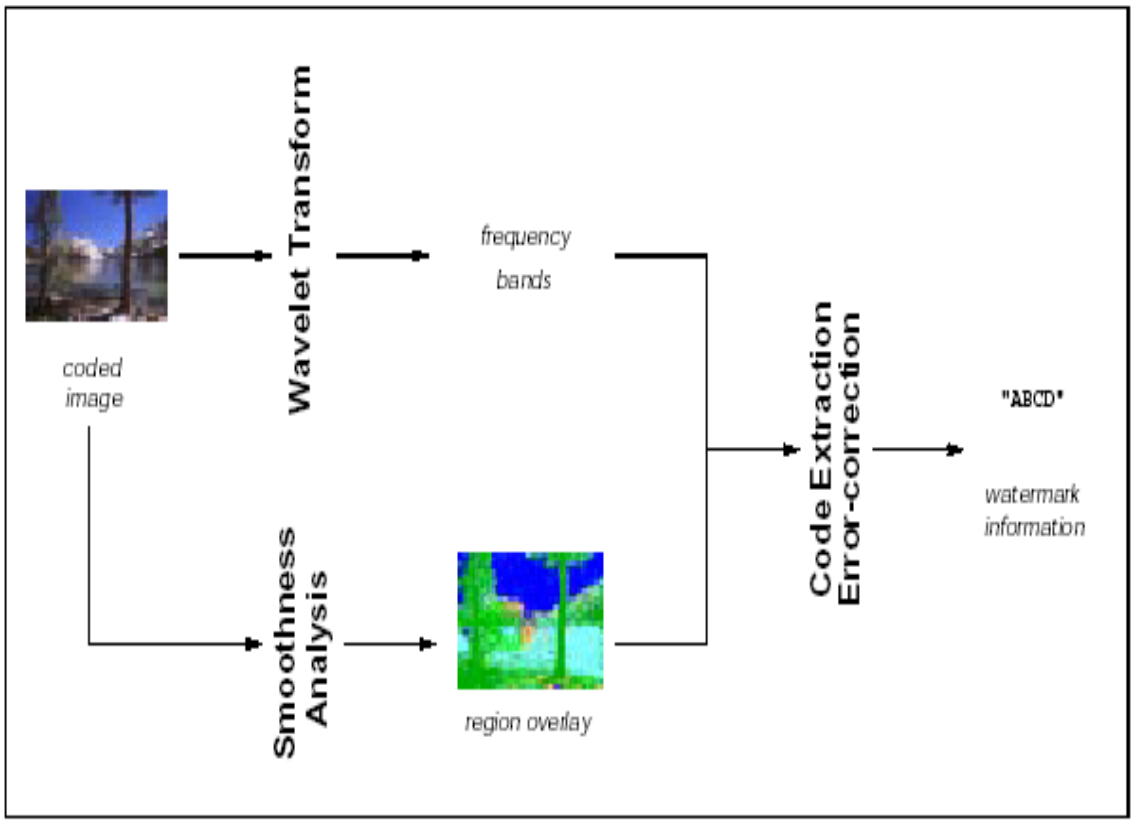
The lower bits of the coefficients according to the frequency represented in the band, the smoothness region overlay, and the encoded watermark code are altered. For the lower frequency bands of coefficients, watermark coding with higher strength is applied. That is, higher order bits in these bands are altered. Similarly, higher order bits are altered in regions with higher variations.

This method sustains image alterations such as compression, additive noise and even some intentional disturbances. It is not suited to handle rescaling, aspect ratio changes and rotational transformations.

# *ENCODER BLOCK DIAGRAM*



# *DECODER BLOCK DIAGRAM*



Data hiding (watermarking) techniques can also be classified with respect to the extraction process:

- *cover escrow* methods need both the original piece of information and the encoded one in order to extract the embedded data.
- *blind or oblivious* schemes can recover the hidden message by means only of the encoded data.

Blind data hiding is usually preferred nowadays, since it is usually impractical to distribute certified copies of the original medium.

Cover escrow methods:

Cox et al Spread Spectrum watermarking

Rakesh Dugad et al digital wavelet watermarking

Watermarking schemes with m-sequences as watermarks

Etc

Blind scheme:

Image watermark using spread spectrum technique in log-2 spatio domain by Peter. H. Wong et al.

Etc.

They have numerous applications like automatic detection of stolen images, intelligent internet browsers filtering out inappropriate information to a particular user etc.

Division based on the copyright problems:

In the copyright protection problem, one can distinguish between proper watermarking or fingerprinting.

In proper watermarking the entity that embeds the data wants only to be able to show its ownership over it, so basically it inserts the same message in every copy of the information.

A typical example of proper watermarking application is that a museum wants to display its images but doesn't allow for replication.

In fingerprinting the same entity wants to be able to tell who between the recipient of the data misused it, so it embeds personalized messages in every issued copy.

A typical example of fingerprinting application is that a company wants to sell its artistic pictures and want to find out any misuse by any of it's customers.

**Probable attacks on the watermarks:**

The attacks can be both intentional and unintentional. They can be broadly divided as

Jitter attack

Stirmark attacks

Mosaic attack: overlapping different parts of a photograph or different images to create a new one

Filtering attacks: applying median filter, blurring etc

Cropping: cropping cuts out the other areas leaving just the interesting areas of the image

Testing tools for new algorithms or implementations:

It is really hard to apply all the attacking techniques on a watermarked image manually or one by one. To overcome this problem and to set a standard in the watermarking community a tool called stirmark is developed to help the students and researchers in the watermarking world.

A word about stirmark:

Stirmark is a generic tool developed for simple robustness testing of image marking algorithms and other steganographic techniques. Stirmark simulates the following attacks

- Resampling process - introduces same kind of errors into an image as printing it on a high quality printer and then scanning it again.
- Applies minor geometric distortion – the image is slightly stretched, sheared, shifted, rotated by an unnoticeable random amount.

## Comparison of the watermarking techniques in different domains:

Spatial domain techniques act directly on the image .They can be easily detected and embedded. They are more prone to attacks . A simple correlation of a few images may lead to the detection of the weakly embedded watermark. They are the primitive techniques for watermark and not are not popular these days.

Frequency domain techniques are very popular. They embed the watermark in the frequency domain( by converting the image into frequency domain and then inserting the watermark and then converting back to the original image). Since the watermark is embedded in the perceptually significant components of the signal even slight changes made to these coefficients will effect quality of the image. These are more safe than the spatial domain techniques. Spread spectrum technique of Cox et al and other DCT based methods are very popular.

Wavelet domain techniques are becoming very popular because of the developments in the wavelet stream in the recent years. Wavelet based compression is used in the jpeg2000 compression ,this feature can be exploited in embedding the watermark. Wavelets use the similarity feature and exploit the time and frequency localization feature while frequency domain techniques could only exploit the frequency localization. Daubechies continuous time wavelet transforms are very popular and many watermarking techniques evolved in the recent years using this wavelet. There is a great future for these techniques because of the features.

## References :

J. R. Smith, and B. O. Comiskey, "Modulation and information hiding in images", Proc. of First Intern. Workshop on Information Hiding, R. Anderson, Lecture notes in Computer Science, Vol. 1174, pp. 207-226, 1996.

[17] S. D. Servetto and C. I. Podilchuk and K. Ramchandran, "Capacity issues in digital image watermarking", Proc. Of ICIP'98, pp. 445-449, Chicago, Illinois, 1998.

[18] M. Barni, F. Bartolini, A. De Rosa, A. Piva, "Capacity of the watermarking-channel: how many bits can be hidden within a digital image ", Security and Watermarking of Multimedia Contents, Proceedings of SPIE, Wong, Delp, Vol. 3657, pp. 437-448, San Jose, CA, 1999.
Majid Rabbani Eastman and Kodak company

Secure Spread Spectrum technique for watermarking images audio and video by Ingemar Cox ,Joe Kilian ,Tom Lieghton and Talal Shamoon

A survey of wavelet domain watermarking algorithms by peter meerwald and Andreas Uhl

*Images: courtesy –various resource on the internet and many more which are a worth mention but couldn't be mentioned because of certain limitations.

# Hardware Implementation Of Watermarking

An overview

**Mentor :** **C.V.Jawahar**

**Faculty IIIT –Hyderabad**

**(Indian Institute of Information Technology)**

**jawahar@iiit.net**

**Done by:** Gaurav Jain

**Student, IIIT**

**Roll no: 98014**

**gaurav@gdit.iiit.net**

**T. Srinivas Choudary**

**Student, IIIT**

**Roll no: 98041**

**srinivas@gdit.iiit.net**

## Hardware implementation of watermarking:

An implementation of any of the exiting watermarking algorithms is not a very difficult task. But the speed/ease of embedding a watermark into an image decreases as the complexity of the algorithm grows on.

A satellite may need to send some images (say of weather report or other resources on the surface of the earth) to the ground station. In this case it is safe to implement the copyright mechanism in the hardware of the digital camera of the satellite rather than the ground station watermarking all the images after receiving them from the satellite. Anything may happen in the transmission between the satellite and the ground station. So implementing the copyrighting mechanism in the hardware provides a new and promising dimension.

To provide flexibility to the users who wants to copyright their images taken through a digital camera it is better to provide the watermarking scheme in the digital camera itself rather than through a software procedure. This reduces the complexity of producing a copyrighted image (taking an image and then passing it through watermarking software to get the image copyrighted).

In digital cameras "jpeg" is the most popular standard. An image is captured and directly converted to a jpeg compressed image. Jpeg image occupies less space on hard disk and provides good and perceptibly high quality pictures. So it has become popular image format through out the world. Hence it is better if a watermark is embedded in the image when the conversion to the jpeg format is in progress in the digital camera. To understand this mechanism of

inserting a watermark with hardware support a detailed study of hardware of the digital camera is to be understood.

A look at the digital camera:

The key difference between a digital camera and a film-based camera is that the digital camera has no film. Instead, it has a sensor that converts light into electrical charges. All the fun and interesting features of digital cameras come as a direct result of this shift from recording an image on film to recording the image in digital form. The image sensor employed by most digital cameras is a charge coupled device (CCD). Some low-end cameras use complementary metal oxide semiconductor (CMOS) technology.

The CCD is a collection of tiny light-sensitive diodes, which convert photons (light) into electrons (electrical charge). These diodes are called photosites. In a nutshell, each photosite is sensitive to light -- the brighter the light that hits a single photosite, the greater the electrical charge that will accumulate at that site.

Both CCD and CMOS image sensors start at the same point -- they have to convert light into electrons at the photosites. A simplified way to think about the sensor used in a digital camera (or camcorder) is to think of it as having a 2-D array of thousands or millions of tiny solar cells, each of which transforms the light from one small portion of the image into electrons. Both CCD and CMOS devices perform this task using a variety of technologies. The next step is to read the value (accumulated charge) of each cell in the image. In a CCD device, the charge is actually transported across the chip and read at one corner of the array. An analog-to-digital converter turns

each pixel's value into a digital value. In most CMOS devices, there are several transistors at each pixel which amplify and move the charge using more traditional wires. The CMOS approach is more flexible because each pixel can be read individually.

Summarizing the differences between CCD and CMOS:

- CCD sensors create high-quality, low-noise images. CMOS sensors, traditionally, are more susceptible to noise.

- Because each pixel on a CMOS sensor has several transistors located next to it, the light sensitivity of a CMOS chip is lower. Many of the photons hitting the chip hit the transistors instead of the photodiode.

- CMOS sensors traditionally consume little power. Implementing a sensor in CMOS yields a low-power sensor.

- CCDs, on the other hand, use a special process that consumes lots of power. CCDs consume as much as 100 times more power than an equivalent CMOS sensor.

- CMOS chips can be fabricated on just about any standard silicon production line, so they tend to be extremely inexpensive compared to CCD sensors.

- CCD sensors have been mass produced for a longer period of time, so they are more mature. They tend to have higher quality

pixels, and more of them.

Light is converted to electrical charge, but the electrical charges that build up in the CCD are not digital signals that are ready to be used by your computer. In order to digitize the information, the signal must be passed through an analog-to-digital converter (ADC)

Compression: It takes a lot of memory to store a picture with 1.2 million pixels. Almost all the digital cameras have to use some sort of compression to make the files smaller.
Most of today's cameras store their images in JPEG format. Higher-end cameras may also support the TIFF format. While JPEG compresses the image, TIFF does not, so TIFF images take lots of space. The advantage of TIFF storage is that no data is lost to the compression process.
So the slot to embed the watermark in the digital camera has finally been arrived at. The watermark can be embedded while performing the jpeg compression rather than embedding the watermark in the jpeg compressed image .So the fine details of jpeg compression can be exploited to embed the watermark. This saves processing power and time. The subsequent sections try to provide some algorithms for embedding the watermark in jpeg file formats. Since jpeg compression hardware is widely available, just a slight modification of the hardware will do the watermarking task. The following section describes an algorithm that embeds the watermark in the 8-by-8 DCT block of the jpeg image.( digital cameras have a facility to convert an image into a jpeg image ,because of the universality of the jpeg images and it surely must have a mechanism for 8-by-8 DCT finding procedure. So

the watermark information can be embedded after arriving at the 8-by-8 DCT block).

Watermarking in jpeg compressed domain by DC coefficient modification: (by Peter. H. Wong et al).

One bit of the secret or watermarking information is embedded in an 8-by-8 block by modifying its quantized DC coefficients slightly. But all the blocks are not used because even the slightest change in the quantized DC coefficients can cause visual artifacts in the smooth regions. (For example shoulder of Lena). However in the texture rich portions of an image a small change in the quantized DC coefficients can be perceptually undetectable. So only the texture rich blocks are used to embed the watermark information.

Detection of texture rich blocks:

The image is band pass filtered using a 3-by-3 band pass filter. The boundaries of each block are treated as zero intensity. In each block the number of pixels that are greater than a particular threshold T1 are counted. If the number in a block is greater than T2, the block will be used to embed the watermark information.

One bit of secret information is embedded in the quantized DC coefficient of an 8-by-8 block as follows:

Let qDC(i) be the quantized DC coefficient of the block I, w(i) be the 1-bit information to be embedded in the block I and n(i) be the PN number which is uniformly distributed. Then qDC(i) is modified according to the following equation.

$$qDC'(i) = \text{round}( n(i).\text{round}((qDC(i))/n(i)))$$
$$\text{if } \text{mod}(\text{round } (qDC(i)/n(i))*2) = w(i).$$

qDC’(i) = round( n(i).round((qDC(i))/n(i)+beta(i)))

if mod(round (qDC(i)/n(i))*2) != w(i).

beta is chosen to be either -1 or 1 such that the modification process minimizes the absolute difference between the original DC coefficient and the quantized DC coefficient.

The above given technique can be easily implemented in the hardware. But to decode the watermark information the PN sequence is needed .So a unique key can be given to a piece of hardware. This establishes the ownership of any individual possessing the hardware. The hardware prices have rapidly come down following the Moore’s law and hardware for watermarking will not cost much compared to the other hardware. Hence price of hardware is not a constraint.

Mass production of these hardware chips can be more advantageous.

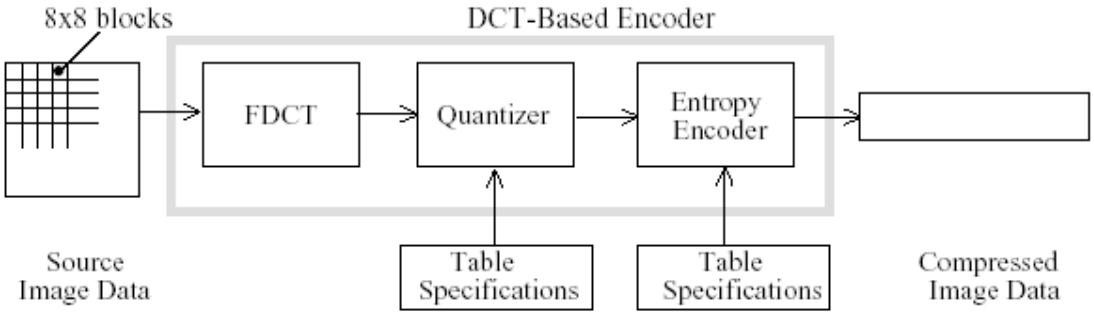



Figure 1. DCT-Based Encoder Processing Steps

The watermark bit embedding process can be included in the DCT – Based Encoder block shown above. An m-bit PN sequence generator can be added and a hardware filter mask can be added to the output of the 8-by-8 DCT generation unit. The filter mask finds the texture rich regions and orders the PN sequence generator block to quantize

the particular DCT coefficient. Thus the watermark is embedded into the DCT coefficients of the JPEG image.

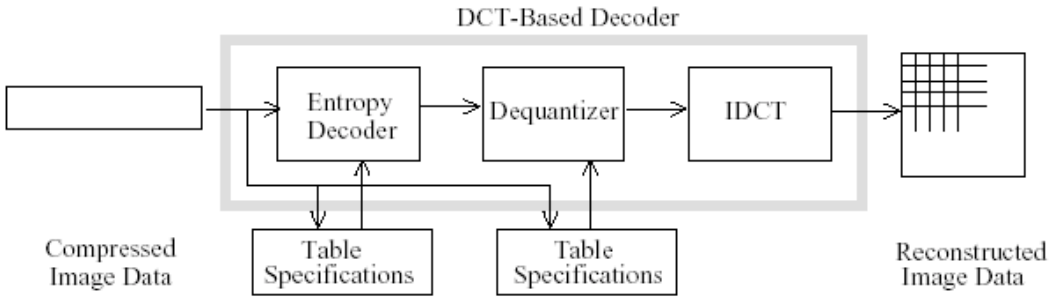



Figure 2. DCT-Based Decoder Processing Steps

The decoder does the reverse process of encoding. A better idea would be to go for the software implementation of the watermark detecting process because it needs to be done only in case of about the genuine nature of any image. This doesn't require mass production of hardware and associated costs with it.

A more detailed JPEG compression and decompression model can be depicted as follows. The names given to the various sub-blocks are in the block diagram are very relevant and need no explanation.
Two block diagrams, both showing the JPEG compression and decompression are shown but the second one presents a modified process of JPEG compression and decompression while the first one is the standard JPEG compression and decompression block diagram.

## JPEG compression and decompression flow diagram

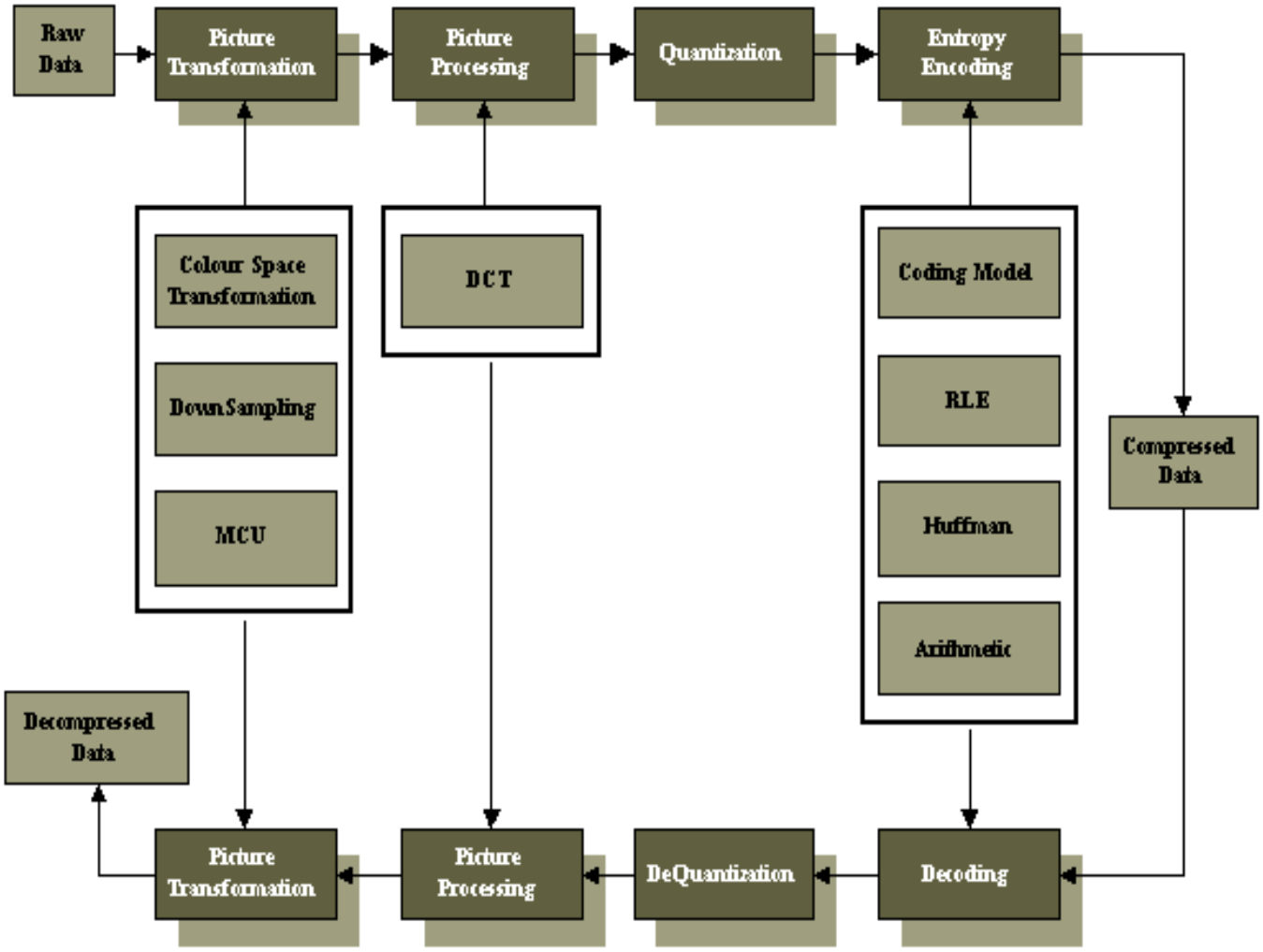



Figure 3.1 Process Flow of JPEG Compression and Decompression
(Based on Steinmetz and Nahrstedt, 1995, pg. 131)

## JPEG compression and decompression flow diagram(modified)

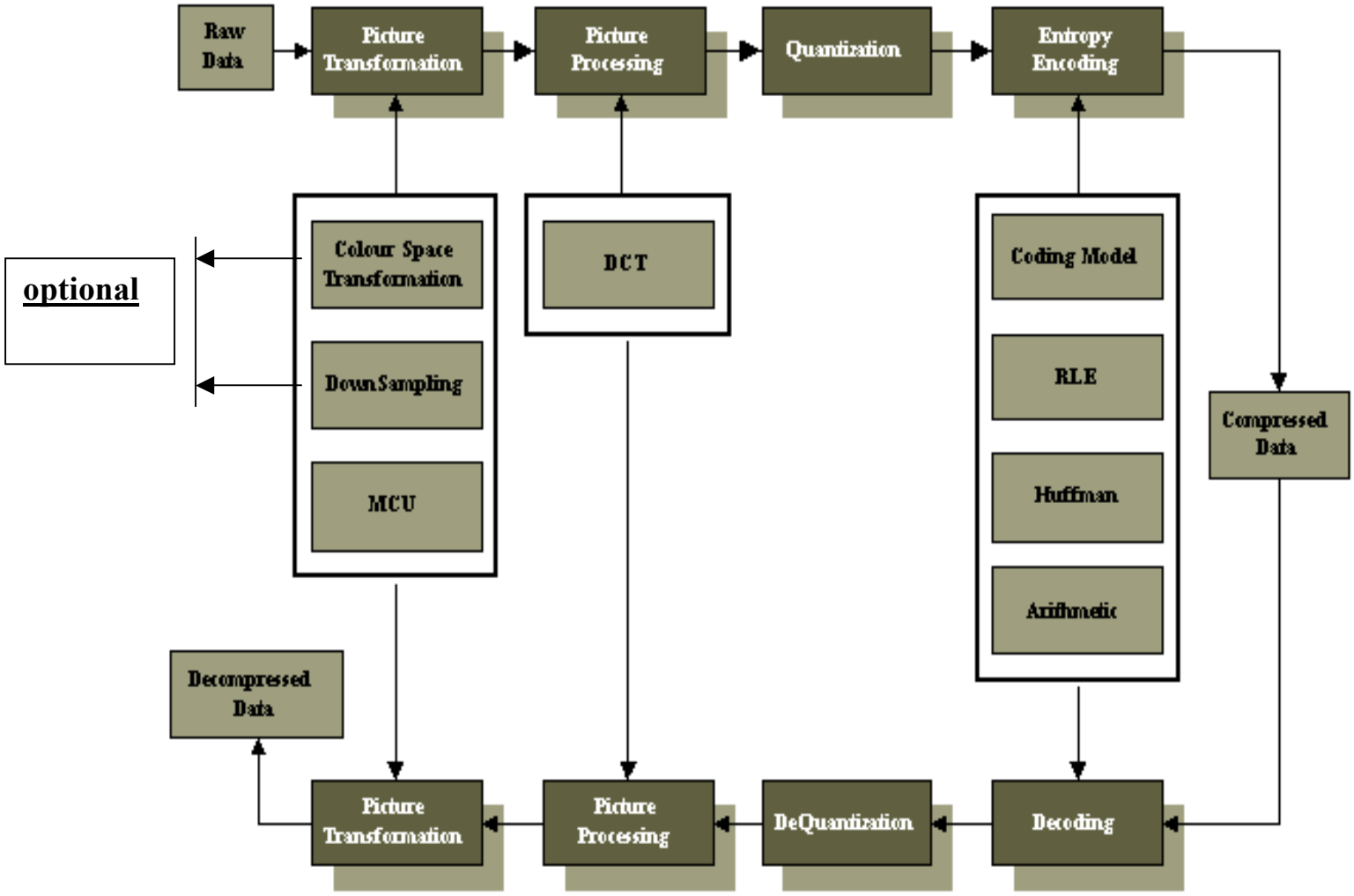
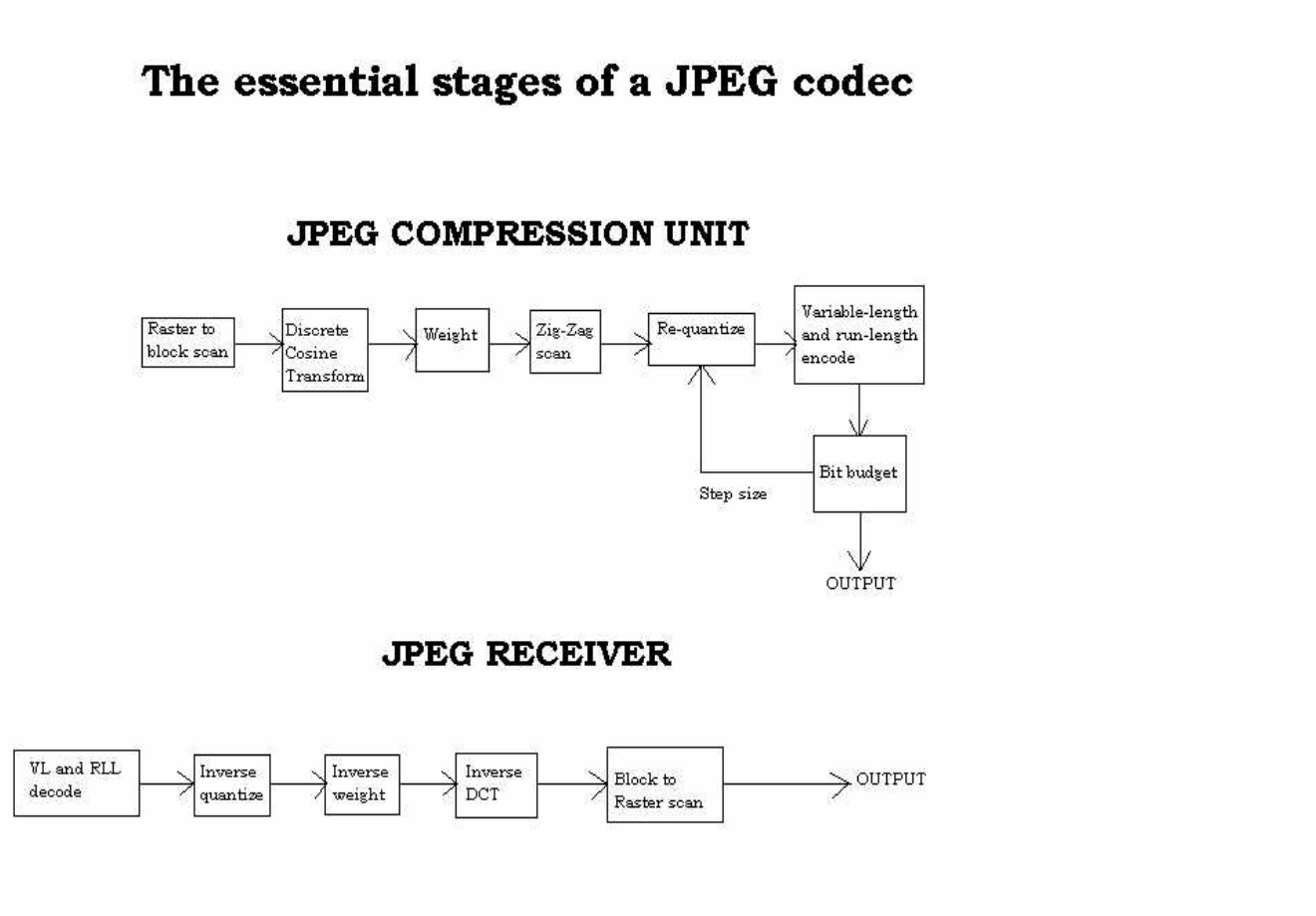



Figure 3.1 Process Flow of JPEG Compression and Decompression
(Based on Steinmetz and Nahrstedt, 1995, pg. 131)

A more simplified block diagram for showing the stages in the JPEG codec can be shown as follows.



***References:***

Watermark in jpeg compressed domain by DC coefficient modification *by Peter H Wong et al.*

*Images: courtesy -- jpeg resources on the internet.