COLOR IMAGE WATERMARKING FOR COPYRIGHT PROTECTION

Oleh

Chua Tiong Kin

Disertasi ini dikemukakan kepada
UNIVERSITI SAINS MALAYSIA

Sebagai memenuhi sebahagian daripada syarat keperluan
untuk ijazah dengan kepujian

SARJANA MUDA KEJURUTERAAN (KEJURUTERAAN ELEKTRONIK)

Pusat Pengajian Kejuruteraan
Elektrik dan Elektronik
Universiti Sains Malaysia **Mac 2005**

ABSTRACT:

Watermarking is an effective and potential method for copyright protection in digital audio, image and video data. One of the media is digital image, where it can be copied and displayed widely while still maintaining the quality. Protections to these images become more and more important. One of the simple methods is to hide the data and then get back the data by owner itself, with certain secret key. The main objective of my project is to find out which color model representation is suitable apply the digital image watermarking for copyright protection. One of the watermarking techniques in frequency domain is applied. At the same time, the robustness of the implemented algorithm to the common image processing operation, example, filtering attack, noise attack, rotation attack, and lossy JPEG compression. Some images are used in the testing. Detailed description of every resulted image and watermark is show out in this report. Quality evaluation to the images is carried out and comparison is made. The quality metrics used in this project is PSNR.

ACKNOWLEDGEMNENT:

I wish to take this opportunity to express my appreciations to all people that have helped me in completing my project successfully.

First of all, I would like to thank my supervisor, Dr Khoo Bee Ee for giving me a lot of useful advices in doing this project well. She checks my project and her kindness in helping me to solve some problems in this project. .She also gives many useful ideal for complete my final year project.

Beside that, I also wish to express my appreciations to Mr. Lim Say Yarn, a Master student under Dr. Khoo Bee Ee. He teaches me and solves my problems. He also give many information and useful advices when I doing my project. Without his valuable assistance, this project could not be done smoothly and on time.

Not forgotten also to thank to all my friends and roommates that had given advices and supports to me for completing this project successfully.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER 1 : INTRODUCTION

1.1 Digital Watermarking:

Usage of digital media has witnessed a tremendous growth during the last decades as a result of ease of manipulation and transmission. However these features make digital media vulnerable to copyright infringement, tampering and unauthorized distribution. In the last few years, the protection of digital information has received significant attention within the digital media community, and a number of techniques that try to address the problem by hiding appropriate information within digital media have been proposed.

1.1.1 History:

The idea to communicate secretly is as old as communication itself. First stories, which can be interpreted as early records of covert communication, appear in the old Greek literature (Frank Hartung and Martin Kutter, 1999).

Paper watermarks appeared in the art of handmade papermaking nearly 700 years ago (Frank Hartung and Martin Kutter, 1999).The oldest watermarked paper found in archives dates back to 1292 and has its origin in Fabriano, Italy, which is considered the birthplace of watermarks. At the end of the thirteenth century, about 40 paper mills were sharing the paper marked in Fabriano and producing paper with different format, quality, and price. They produced raw, coarse paper which was smoothed and post processed by artisans and sold by merchants. Competition not only among the paper mills but also among the artisans and merchants was very high, and it was difficult to keep track of paper provenance and thus format and quality identification. The introduction of watermarks helped avoiding any possibility of confusion. After their invention, watermarks quickly spread over Italy and then over Europe, and although originally used to indicate the paper brand or paper mill, they later served as indication for paper format, quality, and strength and were also used to date and authenticate paper

The idea of digital image watermarking arose independently in 1990 and around 1993; Tirkel *et al.* coined the word “water mark” which became “watermark” later on. It took a few more years until 1996 before watermarking received remarkable attention. Since then, digital watermarking has gained a lot of attention and has evolved very quickly, and while there are a lot of topics open for further research, practical working methods and systems have been developed.

1.1.2 Watermarking Applications:

Digital watermarking has seven applications (Ingemar.Cox et. Al, 2000). The applications are broadcast monitoring, owner identification, proof of ownership, authentication, transactional watermarks, copy control and covert communication. Watermarking technique not only use at the images, but also at data of videos and audios. I will briefly discuss the applications of watermarking.

Broadcast Monitoring:

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.

Owner Identification:

A digital watermarking provides complementary copyright marking functionality and become an integral part. The Digimare corporation has marketed a watermarking system whereby bundled with photo shop. Its detector will find out a watermarking then contact a central database to identify the watermark owner.

Proof of Ownership:

Multimedia owners may want to use watermark not just to identify copyright ownership, but to actually prove ownership. Alice creates an image and put it on her website, it is possible for Alice to use a watermark embedded in the image to prove that she owns it when someone steals the image, and then claims to own the copyright himself

Authentication:

A preferable solution is to embed the signature directly into the image using watermarking. The new signature shall be embedded into the image using watermarking to avoid interference with the last signature and to authenticate the image.

Transactional Watermarks (Fingerprinting):

One application of transactional watermarks is in the distribution of movie dailies. A unique transactional watermark can easily identify the source of the leak of movie dailies. Also, with transactional watermark, DIVX Corporation can track illegal copies of movie to the source.

Copy Control:

A transactional watermark does 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 signal. In this way, a recording device might inhibit recording of a signal if it detects a watermark that indicates recording is prohibited.

Covert Communication:

One of the earliest applications of watermarking, or more precisely, data hiding, is as a method of sending secret messages. For example, the messages relate to a plan for escape. The solution is to disguise the escape-plan messages by hiding them in innocuous messages.

1.1.3 Objective:

Unlimited number of replicas of original content can be made from unprotected digital content. This makes the content creators and owner more anxious about the copyrights management of their digital contents. Digital watermarking is one of the methods that embedded unique data for copyright protection. There are several attacks likes noise attacks, rotation, and filtering attack. These attacks will damage the quality of watermarked image. Objective of my project is to find out which color model representation is suitable to apply the digital image watermarking for copyright protection.

1.2 Color Model:

The purpose of a color model is to facilitate the specification of colors in some standard, generally accepted way. In essence, a color model is a specification of a coordinate system and a subspace within that system where each color is represented by a single point. (Rafael C. Gonzalez, 2004)

RGB Color Model:

Each color appears in its primary spectral components of red (R), green (G) and blue (B). Model is based on Cartesians coordinate system. Images represented in the RGB color model consist of three component images, one for each primary color. When fed into RGB monitor, these images combine on the phosphor screen to produce a composite color image. The number of bits used to represent each pixel in RGB space is called the pixel depth. Consider an RGB image in which each of the red, green and blue images is an 8-bit image. Under these conditions each RGB color pixel is said to have a depth of 24 bits.

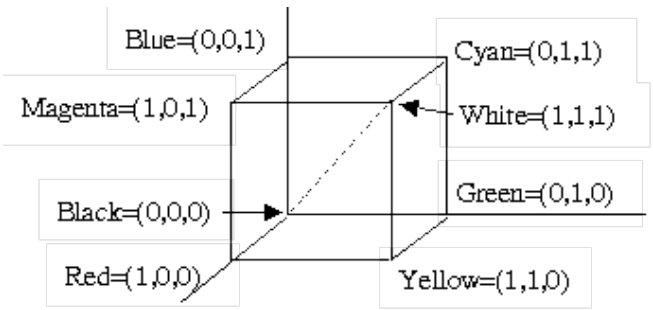

Figure 1.1: RGB color cube

CMY Color Model:

Cyan(C), magenta (M), and yellow(Y) are the secondary color of light or, alternatively the primary color of pigments. When surface coated with cyan pigment is illuminated with white light, no red light is reflect from surface. Pure magenta does not reflect green, and pure yellow does not reflect blue. Equal amount of the pigment primaries, cyan, magenta and yellow should produce black.

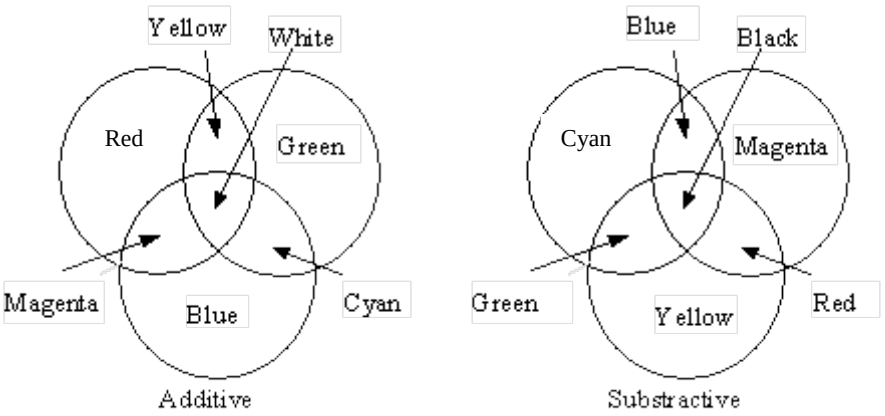

Figure 1.2: Additive colors and subtractive colors

HSI Color Model:

When humans view a color object, we describe it by its hue, saturation and brightness. Hue is a color attribute to which a pure color, saturation gives a measure of the degree to which a pure color is diluted by white light. Brightness is a subjective descriptor that is practically impossible to measure. Intensity is one of the key factors in describing color sensation. Intensity (gray level) is a most useful descriptor of monochromatic image, measurable and easily interpretable .HSI model is an ideal tool for developing image processing algorithms based on color descriptions that are natural and intuitive to humans.

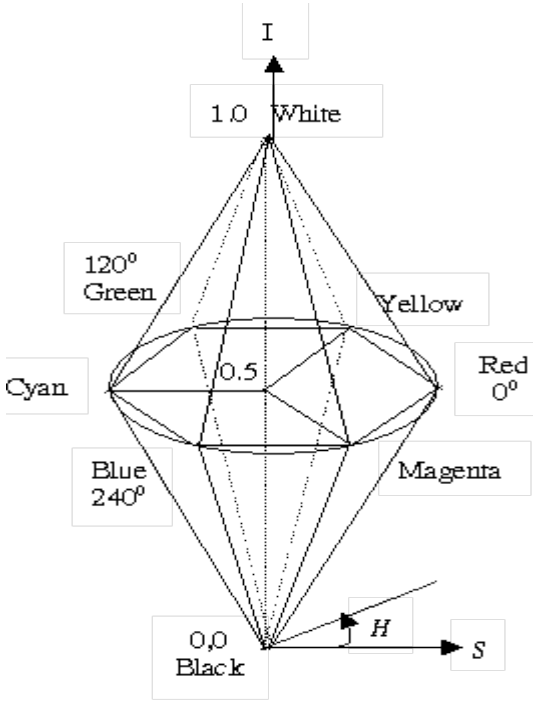

Figure 1.3: Double cone model of HSI color space

YIQ Color Model:

YIQ is a color space used in television signal. YIQ is used predominantly by the NTSC television standard for encoding color information. It is used to encode luminance information and is the only component used by black and white television receivers. I and Q signals contain the actual color information (chromatic properties). Y component represent the intensity.

YUV Color Model:

YUV is very similar to the YIQ color space and both proposed to be used with the NSTC standard. YIQ is more popular than YUV in using color space in the television signal. YIQ is chosen because YIQ need a lower bandwidth that YUV.Y stands for the luminance component (the Brightness) U and V are the chrominance component.

CIELAB Color Model:

CIE (Commission International de I'Eclairage) color system was developed to represent perceptual uniformity, and thus meets the psychophysical need for a human observer. The image in RGB color model will change to XYZ color model first. Then change the XYZ color model to the CIElab color model.

CHAPTER 2 : THEORY

2.1 Properties of Watermarking

A desirable watermarking technique may has the following properties (Frank Hartung and Martin Kutter, 1999).

1. **Imperceptibility**

   One of the main requirements for watermarking is the perceptual transparency. The data embedding process should not introduce any perceptible artifacts into the host data.

2. **Robustness**

   In the design of any watermarking scheme, watermark robustness is typically one of the main issues, watermarking is robustness to common signal processing operation, such as lossy compression , half toning, spatial filtering, printing and scanning, and geometric distortion.

3. **Watermark Security and Keys**

   Secrecy of the embedded information is required, one or several secret and cryptographically secure keys have to be used for the embedding and extraction process. Security keys are used for watermark's safety.

4. **Watermark Extraction or Verification of Presence for a Given Watermark**

   Watermark can accurately detect from a watermarked image. Extracted watermark can determine the true owner of the image based on the security key.

5. **Watermark Recovery With or Without the Original Data**

   If data original is use for process extractions watermark. The extracted data is more robust than watermark which extracted without original data. With the original data, extraction process allows the detection and inversion of distortions which change the data geometry.

2.2. Basic Watermarking Principles

The basic idea in watermarking (Frank Hartung and Martin Kutter, 1999) is a technique to embed invisible data to the original data to be watermarked data. The watermark signal is secure in the watermarked data. The watermark signal can be partly or fully extracted from watermarked data, when the actual security keys are used.

To ensure imperceptibility of the watermark after the watermark embedded, a perceptibility criterion is used. The individual samples that are used for watermark embedding can only be modified by an amount relatively small to their average amplitude.

To ensure robustness despite the small allowed changes, the watermark signal is usually redundantly distributed over many samples (e.g., pixels) of the host data, thus providing a “holographic” robustness, which means that the watermark can usually be recovered from a small fraction of the watermarked data, but the recovery is more robust if more of the watermarked data are available for recovery.

As said before, watermark systems do in general use one or more cryptographically secure keys for security purpose like to ensure watermark against manipulation and erasure of the watermark.

2.3 Algorithms of Watermarking

Digital watermarking is a technique that embedding personal data or signature in the original data. The technique can embed watermark using two domains. They are spatial domain and frequency domain. Because embedding watermark in spatial domain is claimed to be not robust enough for the use of copyright protection. So, in this project frequency domain will be used. Besides, some of the spatial domain watermarking scheme are unable to detect the embedded watermark (Lim Say Yarn and Khoo Bee Ee, 2004). For frequency domain, I will discuss about Discrete Wavelet Transform and Stationary Wavelet Transform as below:

2.3.1 Discrete Wavelet Transform:

In Discrete Wavelet Transform (DWT), the signal is decomposed to two components, high frequency component and low frequency component. The high frequency component is margin component of signal. The low frequency is decomposed to two components again, high frequency and low frequency.

Watermarking using DWT domain has two parts, embedding and extracting watermark. In embedding part, we decompose the image into low-low (LL), low-high (LH), high-low (HL), and high-high (HH) bands, which is shown in the Figure 2.1 (Quan Yuan et. al, 2002). To obtain the next coarser scaled wavelet coefficients, the LL band is further decomposed and sub-sampled. This process is repeated, which is dependent on the user's requirement. From these DWT coefficients, the original image can be reconstructed using Inverse Discrete Wavelet Transform (IDWT).

In embedding part, we only decompose the image twice; it means that we take the LL band to decompose the band to LL2, LH2, HL2, HH2 bands. The LH2 and HL2 bands are used to embed watermark. Because the watermark embedded in the LL band is robust to attack while it will cause degeneration of the image quality. The watermark embedded in the HH band is not detectable to human eyes but it is vulnerable to attacks (Quan Yuan et. al, 2002).

Watermark Embedding Method:

Step 1:

The watermark image must be binary image, mean every pixel of watermark only contain value 0 or 1. The original image is decomposed into two levels. Watermark is embedded in LH2 and HL2.

Step 2:

The thresholds T for small coefficients are set as the magnitude of the largest coefficient in the smallest one out of three parts of all coefficients in the LH2 and HL2 bands. S and D are set as a fixed step and a fixed divisor. The watermark is embedded into the LH2 and HL2 bands redundantly until all the coefficients are quantized. At the location (i,j) the coefficient is quantized according to one bit of the watermark. If the bit is 1, the coefficient is rounded to the nearest odd number; otherwise, the coefficient is round to the nearest even number. The algorithm of embedding watermark is below:

```
For  all the LH2 and HL2 coefficients
    If   absolute value of LH2(i,j) and absolute value of HL2(i,j) are both smaller
         than T
        Quantize LH2 (i,j) and HL2(i,j)  by a fixed step S;
    Esle
        If  absolute value of LH2(i,j) bigger than absolute value of HL2(i,j)
            Maxcoef = absolute value of LH2(i,j);
        Else
            Maxcoef = absolute value of HL2(i,j);
        End If
        If  Maxcoef = absolute value of LH2(i,j)
            Quantize HL2(i,j) by Maxcoef / D;
        Else
            Quantize LH2(i,j) by Maxcoef / D;
        End If
    End If
End For
```

Step 3: Get the watermarked image after take two-dimensional IDWT.

Watermark Extraction Method:

The image is decomposed into two level using DWT. The coefficient of the middle frequency bands (LH2 and HL2) are divided to several parts. The watermark is added redundantly to the host image. Each part has the same number of coefficients as that of bits in the watermark. B(i,j) stand for the mark bit extracted at (i,j) in middle band wavelet coefficients.

```
For all the LH2 and HL2 coefficients
    If absolute value of LH2(i,j) and absolute value of HL2(i,j) are both smaller than T
        B(i,j) = ( LH(i,j) /S mod 2 + HL2(i,j)/S mod 2 )/2
    Else
        If absolute value of LH2(i,j) bigger than absolute value of HL2(i,j)
            Maxcoef = absolute value of LH2(i,j);
        Else
            Maxcoef = absolute value of HL2(i,j);
        End If
        Step = Maxcoef /D;
        If Maxcoef = absolute value of LH2(i,j)
            B(i,j) = HL2(i,j)/Step mod 2;
        Else
            B(i,j) = LH2(i,j)/Step mod 2;
        End If
    End If
End For
```

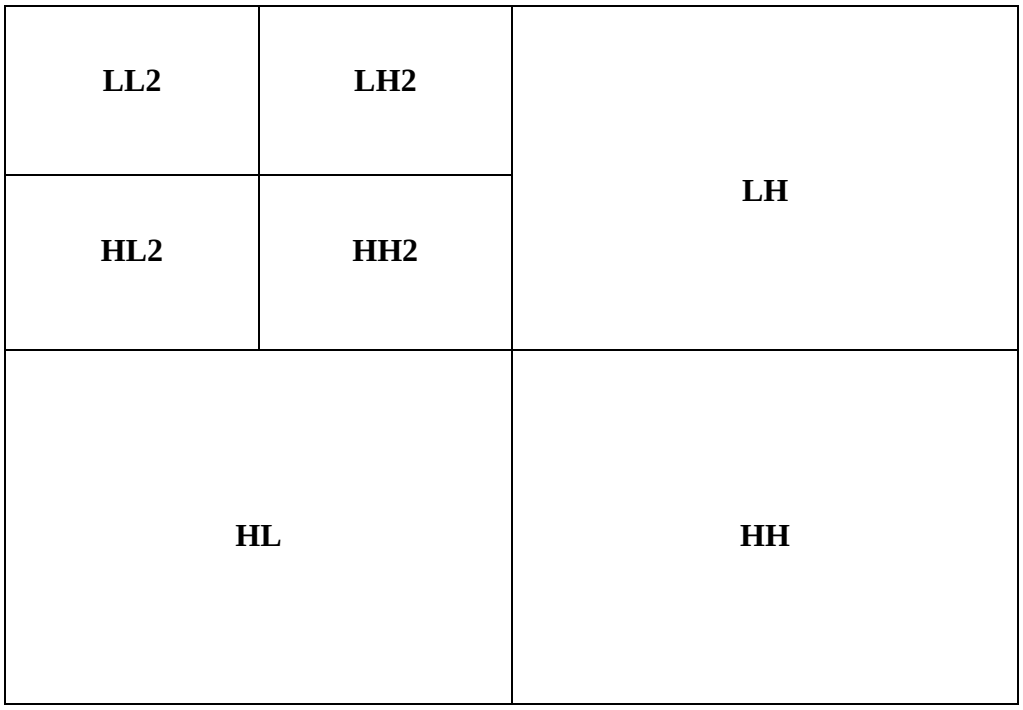

Figure 2.1: Twice Wavelet Decomposition of Image

2.3.2 Stationary Wavelet Transform:

We embedded watermark into the stationary wavelet transform coefficient of host image. The advantage of using SWT (Stationary Wavelet Transform) is the size of the decomposed coefficient is equivalent to the size of the original image. The watermark image is binary image. Thus, the extracted watermark can easily be seen by humans' eyes. The watermark embedded into certain coefficients of host image, these are suitable for the coefficients that will not noticeable to human eyes at watermarked image. The watermark permutation process, watermark embedding and extraction process are described below (Lim Say Yarn and Khoo Bee Ee, 2004).

Watermark Permutation Process:

The watermark is binary image. The logo is first permuted into scrambled data before insertion process. This watermark permutation process prevents the watermark from tampering or unauthorized access by attackers.

Watermark Embedding Process:

The original image is decomposed into frequency domain using SWT. Because, the decomposed coefficients is equivalent to the size of the original image .So that, the number of coefficients than can embed one bit watermark is increased. For the purpose of imperceptibility of watermark, the watermark is embedded into the middle and high frequency band of SWT coefficients. A block of SWT coefficient is selected for embedding a bit of watermark pixel value. The watermark insertion method is described as follow:

1. Decompose host image into SWT coefficients. Select a block, P size n x n SWT coefficients. The block is seeded randomly; the location of the block selected is seed value k.
2. Get the average value Pmean, maximum value Pmax, and minimal value Pmin , and standard deviation σ of the block P.
3. Separate every coefficient in block P into 2 categories, Zh and Zl, using Pmean:

   Cij is element of Zh if Cij bigger than Pmean

   Cij is element of Zl if Cij smaller than Pmean

   Where cij is the SWT coefficient of the block P.

4. Get the mean value, highest value Mh and lowest value of Ml of the Zh and Zl categories.
5. Modify the SWT coefficient in block P according the value of watermar, bw.

If bw = 1;

Cij = Pmax if Cij > Mh ,

Cij = Pmean if Ml ≤ Cij < Pmean ,

Cij = Cij + σ otherwise ,

If bw = 0;

Cij = Pmin if Cij < Ml ,

Cij = Pmean if Pmean ≤ Cij < Mh ,

Cij = Cij - σ otherwise ,

Where Cij is the modified SWT coefficient.

6. The new block of SWT coefficients, Pnew is then positioned to the same location as from the host image.
7. If want embedded another watermark at difference place by changing different seed value k. The seed value k and key used in watermark permutation process are security key.
8. The watermarked image can get from composing the new set of SWT coefficients using Inverse Stationary Wavelet Transform (ISWT).

Watermark Extraction Process

The extraction process is the reverse order of the embedding process. In the extraction process, the original image is required. The embedded watermark was extracted base on the security keys. The sum of the SWT coefficients of host image and watermarked image, So and Sw respectively, in the block are computed. So and Sw are use for retrieved watermark bit value. The watermark bit value is obtained from the below algorithms:

bw = 1 if Sw > So;

bw = 0 Otherwise.

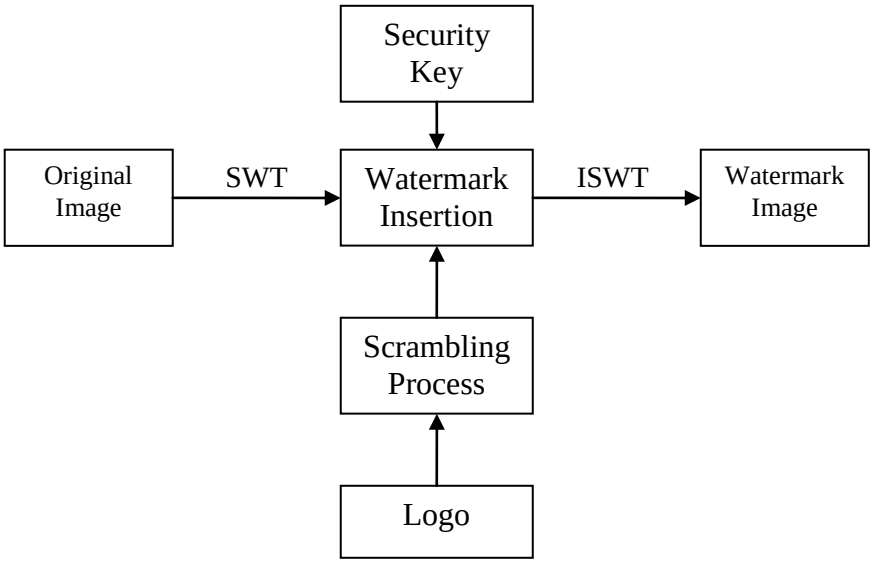

Figure 2.2: Watermark Embedding Process.

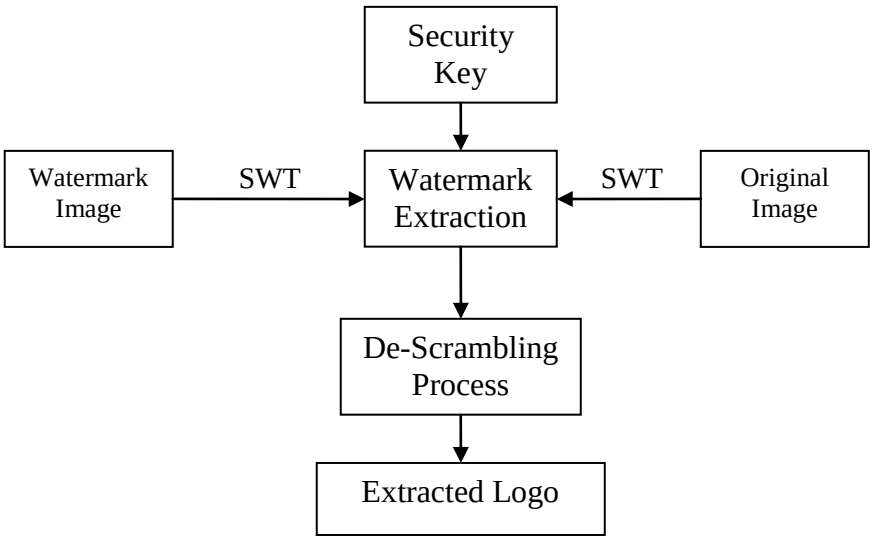

Figure 2.3: Watermark Extraction Process**.**

2.4 Watermarking Attacks:

As the result of rapid usage of internet and widespread distribution of digital media and image over the internet, the copyright protection becomes more important. Digital watermarking becomes technique that is frequently used for copyright protection.

Watermarking is a technique that embeds personal information into the signal and then extracted out to prove the ownership. However, watermarked signal often undergo processing operation. This processing is lossy compression, improve the data of the signal or change the signal like digital to analog conversion and analog to digital conversion. All of these are referred as attack of watermarking. Attack is a process that aims to detect and damage the watermark or information delivered by watermark.

Now, there are four attack classes. They are removal attacks, presentation attacks, protocol attacks and cryptographic attacks (A. Nikolaidis et. al, 2001). These attacks will be described below:

Removal Attacks:

Removal attacks aim to remove the watermark without degrading the perceptual quality of the image. This kind of attack occurs in common processing operation by user or system like compression, filtering, resizing, printing, and scanning, or occurs when noise added to the watermarked image to weaken the strength of the watermark, or the collusion attack which tries to combine the watermark in same image to generate an average image that is very similar to host image, thus reducing strength of watermark or remove the watermark totally.

Presentation Attacks:

These attacks did not remove the watermark but manipulating the content in such a way that detector cannot extract the watermark. So that the technique use for this category is different from pervious category. Mosaic attack is an example of presentation attacks. Under mosaic attack, the watermarked image is divided into part and reassembled using proper HTML. Thus the detector cannot detect the watermark at the watermarked image. Other example of such attacks is rotation, enlargement, and affine transformations.

Protocol Attacks:

The aim of this attack makes the watermark unreliable. Example, attacker can make a counterfeit of original data after subtracting a counterfeit watermark from a watermarked image. Then, the attacker can claim that the new watermarked image contains his own watermark, so that he is the owner of the image.

Cryptographic Attacks:

Brute force attack is an example of this category attack. The attack is aim to find out security information of the watermark. Watermarking scheme use security keys to embed and extract watermark into host image, so that, information about the keys are very important in watermarking scheme. Another example is Oracle attack which use to make an image without watermark when the watermark detected in the watermarked image.

2.5 Measurement Quality of Watermarking

Besides of method for watermarking process, measurement also is an important thing. Not only measure the robustness of watermark, but also measure how many quality of the image change after watermark embedded. The measurement quality of watermarked image measure the difference between watermarked images compare with original image. I choose method Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) for measurement quality of watermarked image, because these methods are common and easy for used. The MSE method is used to calculate PSNR value. A color image consisting of three layers, these are layer red (R), green (G), and blue (B). When read the value data on the color image, we get a three dimension matrix. The MSE value can calculate from the below equation (Y. Fisher et. al, 1995):

$$MSE = [\sum_{i=1}^{k} \sum_{j=1}^{l} [(Rij - R'ij)^2 + (Gij - G'ij)^2 + (Bij - B'ij)^2]] \div (3 \times k \times l) \quad (2.1)$$

Where Rij and R'ij is layer red value of original image and watermarked image ,

Gij and G'ij is layer green value of original image and watermarked image

Bij and B'ij is layer blue value of original image and watermarked image

The PSNR value can be calculated by using the equation below (Ming Shin Hsieh et. al, 2001):

$$PSNR = 10 \log_{10} (255^2 \div MSE) \quad (2.2)$$

For the extracted watermark, I use the correlation coefficient measurement to measure how similar the extracted watermark to the original watermark I embedded. The formula is show at below (Lim Say Yarn and Khoo Bee Ee, 2004):

$$T = \frac{\sum_m \sum_n \left(A_{mn} - \overline{A}\right)\left(B_{mn} - \overline{B}\right)}{\sqrt{\left(\sum_m \sum_n \left(A_{mn} - \overline{A}\right)^2\right)\left(\sum_m \sum_n \left(B_{mn} - \overline{B}\right)^2\right)}} \quad (2.3)$$

Where A_{mn} and $\overline{A}$ are the extracted watermark value and watermark average value respectively, B_{mn} and $\overline{B}$ are the original watermark value and its average value respectively.

2.6 Conversion of Color Model:

In this section, I will discuss about conversion between the color model, like RGB to CMY and back, RGB to YIQ and back, RGB to YUV and back (Paul Bourke, 1994) ,RGB to HSI and back (Rafael C. Gonzalez et. al, 2004) and RGB to CIELAB (Christine Connolly and Thomas Fliess, 1997):

RGB to CMY conversion:

Given an image in RGB color format, the each component of CMY of each RGB pixel is obtained using the below equation:

$$\begin{bmatrix} C \\ M \\ Y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.4}$$

CMY to RGB conversion:

Given an image in CMY color format, the each component of RGB pixel is obtained using the below equation:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} C \\ M \\ Y \end{bmatrix} \tag{2.5}$$

Where again the assumption is that all color value have been normalized to the range [0,1].Mean that , 1 represented 255 value.

RGB to YIQ conversion:

Given an image in RGB color format, the each component of YIQ of each RGB pixel is obtained using the equation:

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.212 & -0.523 & 0.311 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.6}$$

YIQ to RGB conversion:

Given an image in YIQ color format, the each component of RGB pixel is obtained using the below equation:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.0 & 0.956 & 0.621 \\ 1.0 & -0.272 & -0.647 \\ 1.0 & -1.105 & 1.702 \end{bmatrix} \times \begin{bmatrix} Y \\ I \\ Q \end{bmatrix} \tag{2.7}$$

RGB to YUV conversion:

Given an image in RGB color format, the each component of YUV of each RGB pixel is obtained using the below equation:

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.8}$$

Converting Color from YUV to RGB:

Given an image in YUV color format, the each component of RGB pixel is obtained using the below equation:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.164 & 0.0 & 1.596 \\ 1.164 & -0.813 & -0.391 \\ 1.164 & 2.018 & 0.0 \end{bmatrix} \begin{bmatrix} Y - 16 \\ U - 128 \\ V - 128 \end{bmatrix} \tag{2.9}$$

RGB to HSI conversion:

Given an image in RGB color format, the each component of HSI of each RGB pixel is obtained using the below equation:

$$I = (R + G + B) \div 3 \quad (2.10)$$

$$S = 1 - 3\{\min(R , G , B)\} \div (R + G + B) \quad (2.11)$$

$$\theta = \cos^{-1} [(R - G + R - B) \div \{2\times[(R - G)^2 + (R - B)\times(R - G)^{1/2}] \}] \quad (2.12)$$

If B is greater than G ,then

$$H = 360° - \theta \quad (2.13)$$

Otherwise ;

$$H = \theta \quad (2.14)$$

It is assumed that the RGB value have been normalized to the range[0,1], and the H is measured with respect to the red axis of the HSI space .Hue can be normalized to the range [0,1] by dividing by 360° all value resulting by equation. The other two HSI component already are in this range if the given RGB values are in the interval [0,1].

Color from HIS to RGB conversion:

Given values of HSI in the interval [0, 1]. The applicable equation depends on the values of H. There are three sectors of interest, corresponding to the 120° intervals in the separation of primaries. Begin by multiplying H by 360° which returns the hue to its original range of [0°, 360°].

RG sector($0° \leq H \leq 120°$): When H is in this sector, the RGB components are given by the equations

$$R = I \times [1 + (S \cos H) \div (\cos (60° - H))] \quad (2.15)$$

$$B = I \times (1 - S) \quad (2.16)$$

$$G = 3 \times I - R - B \quad (2.17)$$

GB sector (120°≤H≤240°):If the given value of H is in this sector, we first subtract 120° from it.

$$H = H - 120° \tag{2.18}$$

The RGB components are:

$$R = I \times (1 - S) \tag{2.19}$$

$$G = I \times [1 + (S \cos H) \div (\cos (60° - H))] \tag{2.20}$$

$$B = 3 \times I - R - G \tag{2.21}$$

BR sector (240°≤H≤360°) If the given value of H is in this sector, we first subtract 240° from it:

$$H = H - 240° \tag{2.22}$$

The RGB components are:

$$G = I \times (1 - S) \tag{2.23}$$

$$B = I \times [1 + (S \cos H) \div (\cos (60° - H))] \tag{2.24}$$

$$R = 3 \times I - G - B \tag{2.25}$$

RGB to CIELAB conversion:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.4303 & 0.3416 & 0.1784 \\ 0.2219 & 0.7068 & 0.0713 \\ 0.0202 & 0.1296 & 0.9393 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.26}$$

The CIELAB equation is then applied. This involves the evaluation of cube roots

$$L = 116f(Y/Yo) - 16 \tag{2.27}$$

$$A = 500[f(X/Xo) - f(Y/Yo)] \tag{2.28}$$

$$B = 200[f(Y/Yo) - f(Z/Zo)] \tag{2.29}$$

where

$f(q) = (q)^{1/3}$ $\quad q > 0.008856$

$f(q) = 7.787q + 16/116$ $\quad q \leq 0.008856$

Xo, Yo, Zo are X, Y Z values for the standard white.