CHAPTER III
PROBLEM ANALYSIS

III.1 Techniques of Digital Watermarking

Digital Watermarking techniques can be classified into two domains:

1. Spatial Domain Watermarking
2. Frequency Domain Watermarking

A. Spatial Domain Watermarking

Spatial Domain Technique is a technique of watermark embedding achieved by directly modifying the pixel values of the host image. There are two techniques in SDW:

1. Least Significant Bit (LSB) Technique

   LSB is one of old popular technique embeds the watermark in the least significant bit of pixels. This method is easy to implement and doesn't generate serious distortion to the image. However, this techniques is not robust from attack.

   This technique of watermark may be embedded inside the picture. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits.

   For example, in the binary number: 10111001, the least significant bit is the far right 1.

Fig 3.1 *Example of Bit used in LSB*

Source: www.bham.ac.uk

2. Correlation-Based Techniques

   Correlation-Based is the correlation properties of additive pseudo-random noise patterns as applied to an image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If he correlation exceeds a certain threshold T, the watermark is detected, and a single bit set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block.

B. Frequency Domain Watermarking

This technique is also known as transform domain. In this technique values of certain frequencies are changed from original values. There are various methods which are used in transform technique.

1. Discrete Wavelet Transforms (DWT)

   Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical, and diagonal. Hence wavelet reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The DWT is used in a signal processing applications such as audio and video compression and simulation of wireless antenna distribution. DWT is preferred because it provide both a simultaneous spatial and frequency spread of watermark within the host image.

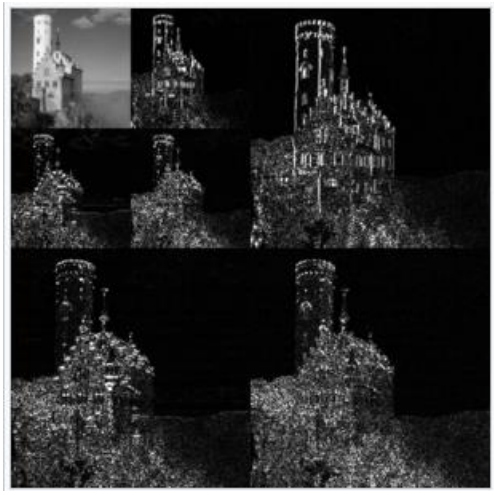

Fig 3.2 *an example of the 2D discrete wavelet transform that is used in JPEG 2000.*

Src: Wikipedia.com

2. Discrete Cosine Transform

   DCT like a Fourier transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive the light, so that the part are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness, and contrast adjustment, blurring etc. However they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.

Fig 3.2 *Image which build with DCT Technique*

Src: sourceforge.net

3. Discrete Fourier Transform

   Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

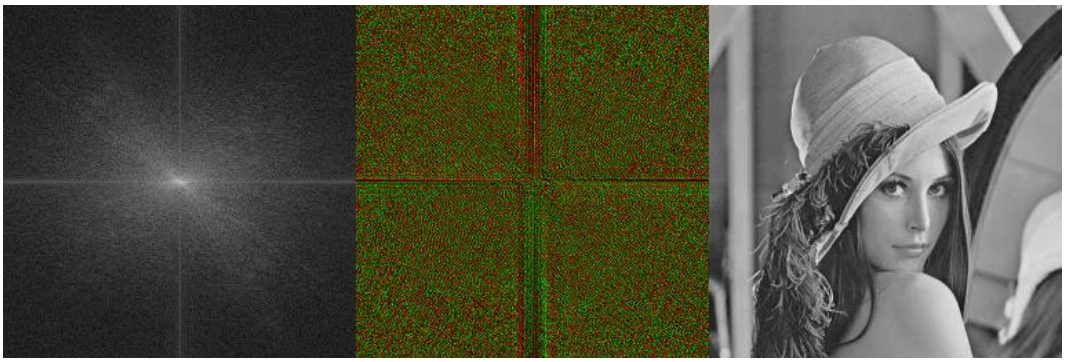

Fig 3.3 Left: Magnitude of DCF. Middle: Phase of DCF. Right: Input image
src: http://boofcv.org

III.1 Advantages and Disadvantages of Digital Watermarking

Digital Watermarking has some of advantages. Besides Digital Watermarking also have some of disadvantages

Advantages

1. It can't be easily understand by the people

   With Digital Watermarking we hidden the message inside the watermark. The message which hidden inside the watermark can't be easily understand by the people. Because there are several techniques to hidden the message inside the watermark and the message is encrypted with a lot of method. The images which encrypted with watermark is just like a normal images with a watermark to sign the creator of the picture owner.

   Imagine, if someone send a picture with watermark and uploaded in a Pinterest. The picture is just like a normal picture. But the fact there are a hidden message inside the picture and it can be understand to people who has role as receiver. People who saw the picture just think about the meaning of the picture and the essence of the picture. But

people who has role as receiver will decrypt the message inside the watermark. It can be a camouflage to the people.

2. The cost is cheap

   The cost of digital watermarking are not expensive because it can be easily embedded in the picture. It's only need editor of photo and give some effect there. So the cost of digital watermarking are cheap and easy to do. Imagine if a company want to send a hidden message but scared to be decrypted or hijacked by unauthorized people so they choose digital watermarking to safe their message inside a picture.

Disadvantages

1. The security is not very safety

   Because digital watermark can be seen in the picture. Some of several people can guess the mean of the message inside watermark. However if the message is not hidden with a good encryption. It can be easily guess by hackers. Besides if the sender always send the digital watermark with the same style it can also be guess by the hackers that the sender has a message inside the picture.

   As example, if the sender upload in a social media such as pinterest. It can be downloaded by the all of the people.