CHAPTER 2 THEORETICAL ISSUE

This chapter describes about background of digital watermarking. Also, the development of the digital watermarking scheme was proposed in the past.

2.1 Digital Watermarking

Digital watermarking has been widely studied and implemented throughout the world. Conceptually, digital watermarking is a method used to provide an electronic proof of ownership and/or receipt in distributed copies of digital media. Technically, a watermark signal is an owner's secret data embedded into a host media in such a way that the changes in watermarked media cannot be noticed by human perceptual system. Moreover, this embedded watermark will be securely attached to every made copy, and can later be reliably recovered for the use of identifying the original ownership of that media. Decent watermarking methods should provide efficient watermark retrieval even if the watermarked media is intentionally attacked. Apart from imperceptibility, reliability, security and robustness, a decent watermarking method should provide a blind detection property, so that watermark recovery can be achieved without the need of an original image.

Watermarking methods can be divided into two categories depending on the domain of watermark embedding, i.e. in spatial and frequency domains. The spatial domain watermarking was formerly developed by directly embedding the watermark into image pixels, while the frequency one was later developed by embedding the watermark into image coefficients in transformed domain. The main advantage gained from the spatial domain based approach is that the embedding methods used are more straightforward and less computationally expensive than the ones using transforms, while the frequency

domain based approach normally offers a higher degree of robustness, especially against most image compression schemes e.g. JPEG compression standard.

2.2 Literature Review

In the past, the watermarking scheme was proposed, which consisted of two main processes, i.e. the embedded process and the retrieval process. Both of them affected performance of the watermarking scheme. The embedded process was developed to improve the scheme. Also, the prediction of an original pixel value technique was developed to improve the scheme.

In 1997, C.Podichuk and W. Zeng [13] proposed Perceptual Watermarking of Still Images that based on utilizing a visual model which was developed in the context of image compression. They described a general framework for the watermark encoding scheme which consisted of a frequency decomposition based on an 8 x 8 DCT framework followed by JND calculation and watermark insertion. The block-based approach provided local control which allowed them to incorporate local visual masking effects. Such a scheme also allowed for the direct watermarking of the JPEG bit stream.

In 1998, C.Podichuk and W. Zeng proposed Image-Adaptive Watermarking using visual models. They named their new issue Image adaptive watermarking using visual model [10]. They embedded the watermark with Watson's model masking in the adaptive way. The results of the experiments were good but the detection was based on a classical detection theory. The original image was subtracted from the watermarked image. At the moment this method is called the non-blind detection.

In 1998, J.F. Delaigle, C. De Vleeschouwer and B.Macq [11] proposed an HVS masking which was built in the Fast Fourier Transform (FFT) domain with setting the

threshold on a band pass filter. Their major part of the watermark was concentrated in the horizontal component only. But there were ringing effects around the edge of the watermarked image. Later in 2001, B.T. Hannigan and Friends [12] combined the directional edge detection and the contrast measurement together; trying to avoid the effect from Delaigle's work but their work could not deal with the salt and pepper noise.

In 1998, Kutter proposed Digital Signature of color images using amplitude modulation, which was the first efficient image watermarking based on amplitude modulation, the embedded process could be achieved by modifying the pixel value in the blue channel of the color image, which was the prediction of the original pixel value technique based on linear combination neighbor pixel in cross shape. Numbers of pixels were calculated equal to 4c; c was size of cross shape, for c was 1 half of neighbor pixels which were calculated. In case of having the most differing pixel, the probability to correctly retrieve the watermark would decrease. Their method was proved to be robust against several of attacks, including blurring, JPEG encoding/decoding, rotation, composition with another image, pixel spreading, pixelizing, color quantization, translation, cropping, and despeckling (median filtering).

In 2001, Puertpan proposed a method to improve the retrieval performance. Gaussian pixel weighing mask was used in the embedded process, by averaging luminance of its own pixel and neighbor pixel. Also, Gaussian pixel weighing mask was used as a factor in the existing watermark embedding method, which was the prediction of the original pixel value technique using the average neighbor pixel around the embedded pixel. The retrieval process was based on linear combination neighbor pixel in cross shape and subtracted by center pixel value. In case of having the most differing pixel, the prediction of original pixel value performance will be slightly improved.

In 2002, J.F. Dealigle and his group [14] proposed "Human Visual System Feature Enabling Watermarking". This thesis, they just only tried to understand HVS in a syntactic way and from an engineering perspective for a designer of a watermarking algorithm. They described about perceptual model such as JND, CSF and visual masking techniques, such as the spatial masking and the contrast or pattern masking.

In 2006, Irene G. Karybali and Kostas Berberidis proposed Efficient Spatial Image Watermarking via New Perceptual Masking and Blind Detection Schemes [17]. A new spatial perceptual mask was proposed, which was based on the least-squares prediction error sequence of images, of which matches used the HVS, In the smooth area, the errors would be smaller than errors which were in edges and textured areas. The robustness of the embedded watermark was proved by the denoising attack. The denoising attack is a base directly on the data; the proposed detector's improved performance has been justified for the case of linear filtering plus a noise attack, and has also been verified by the simulations. The theoretical analysis is independent of the proposed mask and is valid for any watermarking technique based on the spatial masking. In most cases, the detector performed better if the proposed mask was employed. The experimental results showed that the proposed watermarking scheme was robust against both linear filtering plus an additive white noise attack and several other attacks as well (nonlinear attacks, JPEG compression, etc.). The proposed mask was better performance compared to the existing ones. It increased the watermark strength while, at the same time, watermark visibility was decreased. In the detection procedure, the improved performance was more robust verified by the proposed embedding scheme.

In 2006, Amornraksa proposed Enhanced Images Watermarking Based on Amplitude Modulation. Three techniques were used to improve the watermark schemes, i.e. by

balancing the watermark around the embedded pixel, by properly tuning the strength of the watermark in the embedded process, and by modifying the linear combination of the neighbor pixel around the embedded pixel in the retrieval process. The prediction technique was based on two assumptions. First, any pixel value within an image was close to its surrounding neighbors, so that the embedded pixel value can be predicted by the average of its nearby pixel values. Second, the summation of w around the embedded pixel value was close to zero. To reduce the bias, removing most differing pixel technique was used in the retrieval process. The most differing pixel value is replaced with the embedded pixel, so it will reduce the bias. It can be seen that, in case of having two most different pixels, the prediction of the original pixel can detect one of them. So the prediction of the original pixel value performance will be slightly improved. However, their method was proved to be robust against several of attacks, including high pass filter, JPEG encoding/decoding, Gaussian distributed noise addition, brightness & contrast enhancement, rotation, cropping, and watermark counterfeit.

2.3 Digital Watermarking Based on Modification of Image Pixel

In the watermark embedding process, a unique binary bit-stream is generated and considered as a watermark $w(i, j) \in \{1,-1\}$ to be embedded into an image. It is then permuted, using XOR operation, with a pseudo-random bit-stream generated from a key-based stream cipher to improve the balance of w around (i, j), and the security of the embedded watermark. The watermark embedding is performed by modifying the blue component at a given coordinate (i, j), in a line scan fashion. Note that the blue component is selected to be watermarked because it is the one that a human eye is least sensitive to [7]. The modifications of the blue component in each pixel $B(i, j)$ are either

additive or subtractive, depending on $w(i, j)$, and proportional to the modification of luminance of the embedding pixel $L(i, j) = 0.299R(i, j) + 0.587G(i, j) + 0.114B(i, j)$. Due to the fact that changes in high luminance pixels are less perceptible to the human eye, the luminance value is hence considered and used for tuning the strength of the watermark, so that more energy of the watermark can be added to achieve a higher level of the robustness. Notice that the modification of the luminance $L'(i, j)$ is obtained from a Gaussian pixel weighting mask [8]. The watermarked pixel $B'(i, j)$ is expressed in equation (2.1).

$$B'(i,j)=B(i,j)+w(i,j)sL'(i,j) \tag{2.1}$$

Where s is watermark signal strength and is considered as a scaling factor applied to the whole image frame. In practice, s must be carefully selected to obtain the best trade-off between imperceptibility and robustness. Figure 2.1 illustrates the block diagram of the watermark embedding process.

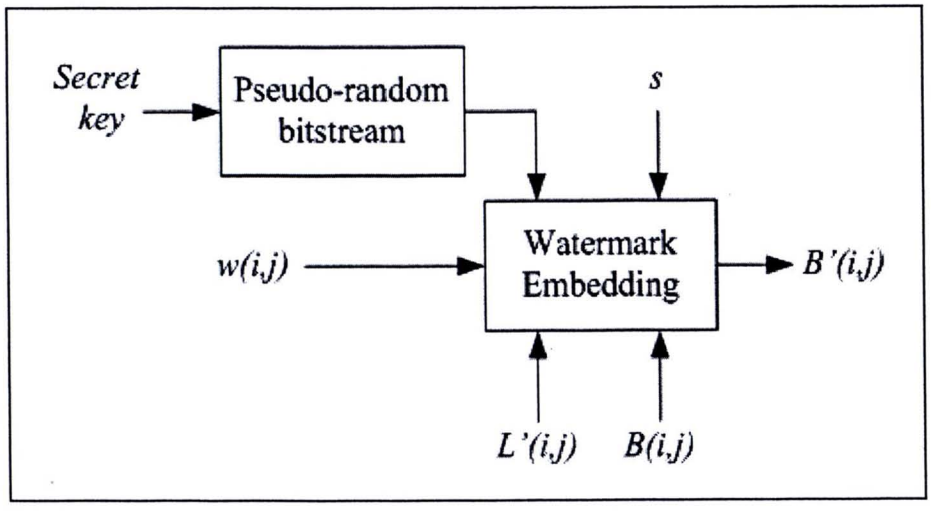

Figure 2.1 Watermark embedding process

In the watermark retrieval process, the embedded watermark can be recovered based on two assumptions. First, any pixel value within an image is close to its surrounding neighbors, so that a pixel value at a given coordinate (i, j) can be predicted by the average of its nearby pixel values. Second, the summation of w around (i, j) is close to zero, so that the original image pixel at (i, j) can be predicted by the following equation.

$$B''(i,j) = \frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} B'(i+m, j+n) \quad B'(m,n)\right) \tag{2.2}$$

Where *B''(i, j)* is the predicted original pixel. It was shown in [8] that the retrieval performance can be improved by removing one surrounding pixel *B'(m_max, n_max)* that most differs from *B'(i, j)*. The original image pixel at *(i, j)* can now be predicted by the following equation.

$$B''(i,j) = \frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} B'(i+m, j+n) \quad B'(m\_\max, n\_\max)\right) \tag{2.3}$$

After obtaining *B''(i, j)*, the estimation of the embedded bit *w'(i, j)* at *(i, j)* can be obtained by the following equation.

$$w'(i,j) = B'(i,j) \quad B''(i,j) \tag{2.4}$$

Since *w'(i, j)* can be either 1 and -1, the value of *w'(i, j)* = 0 is set as a threshold, and its sign is used to estimate the value of *w'(i, j)*. That is, if *w'(i, j)* is positive (or negative),

w'(i, j) is 1 (or -1, respectively). Notice that the magnitude of *w'(i, j)* reflects a confident level of estimating *w(i, j)*. Figure 2.2 illustrates the block diagram of the watermark retrieval process.

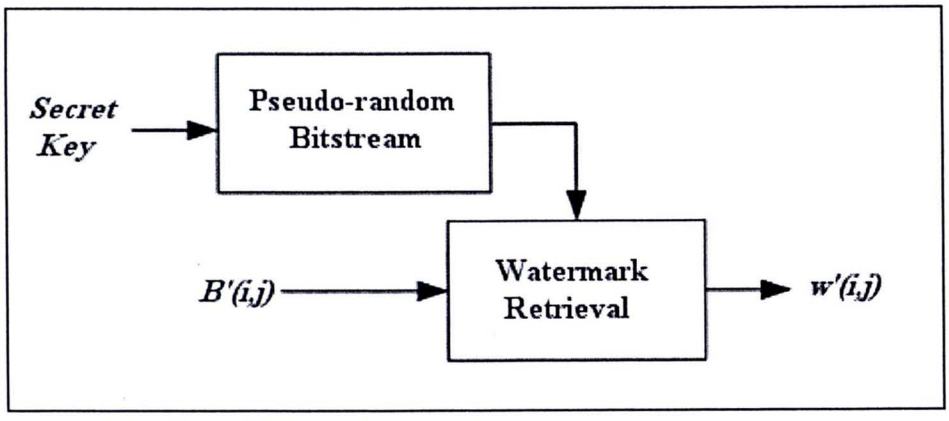

Figure 2.2 Watermark retrieval process