# A Frequency Domain Based Watermarking Scheme

Raymond H. Chan*, F. R. Lin†, and K. M. Yeung‡

January 15, 2001

**Abstract**

In this paper, we propose a frequency domain based watermarking scheme. We embed the watermark data by altering the magnitude of the Fourier coefficients of a sub-image of the given image. The embedded data can be extracted by a denoising process without the knowledge of the original image. Our tests show that our watermarking scheme is robust to various kinds of attacks, such as JPEG, blurring, sharpening, and GIF compression/decompression.

## 1 Introduction

A watermark for digital image is a sequence of information embedded in the image data. It can be embedded into the spatial domain (see for instance Lie and Chang [4] and Wu and Tsai [6]) or embedded into the frequency domain (see for instance Kim, Lee, and Lee [2], Koch, Rindfrey, and Jhao [3], and Ramkumar, Akansu, and Alatan [5]). The watermark should be invisible to the human. Furthermore, unauthorized removal and detection of the watermark must be impossible even if the watermarking scheme is partially known. Another characteristic of a watermark is that we should be able to retrieve the watermark even when the image has been attacked by some image processing operations, such as lossy compression and blurring. In recent years, watermarking has been used as a means of protecting copyrights on digitized media such as images, audio and multimedia data.

Watermarking technique has been a popular research topic in the signal processing area in the past few years. Lie and Chang [4] proposed an image watermarking method based on the human visual system. They studied the relation between the maximal bit position that can be changed and the intensity of the pixel. Koch, Rindfrey, and Jhao [3] proposed a frequency domain based watermarking scheme. They embedded the hidden data by modifying the coefficients of the discrete cosine transform of randomly chosen $8 \times 8$ blocks. This watermark is sensitive to noise or distortion. Kim, Lee, and Lee [2] discussed methods of embedding the hidden data into the frequency domain of the original image and extracting the embedded data. The watermark spreads out evenly to the whole image, so it is invisible to the human. To extract the watermark information (hidden bits), a prediction of the original value of the pixel containing the information is used. The watermark can be retrieved without the knowledge of the original images.

*Department of Mathematics, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong. Research supported in part by HKRGC grant CUHK4212/99P and CUHK DAG grant 2060183.

†Department of Mathematics, Shantou University, Shantou, Guangdong 515063, China.

‡Department of Mathematics, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong.

In this paper, we improve the watermarking scheme proposed by Kim, Lee, and Lee [2]. We consider embedding small rectangular binary seal images into the image data. The seal data will be inserted into the image data by a repetition code. That is, the watermark is a binary image which is formed by repeating the seal data. The watermark is embedded into the frequency domain of a sub-image of the original image. Repetition of the seal data makes the watermark more robust. Experimental results show that by using our scheme, one can retrieve the seal data even when the watermarked images are attacked by some operations, such as JPEG, GIF compression/decompression, blurring, and sharpening.

# 2 Watermarking approaches

## 2.1 The Embedding Process

In this subsection, we discuss the embedding of a small seal (binary image) of size $p \times q$ into an image (color or monochrome) of size $m \times n$. Let the seal data be denoted by $S$ with the marked pixels valued as 1's and the others as $-1$'s. The seal data $S$ will be embedded into the image data for a number of times. More precisely, the watermark to be inserted into the image data consists of the seal data repeated $r \times s$ times, where $1 \le r \le \left[\frac{m}{p}\right]$ and $1 \le s \le \left[\frac{n}{q}\right]$. For example, let the sizes of the seal and the original image be $32 \times 32$ and $128 \times 168$ respectively, then we can insert the seal data as many as $\left[\frac{128}{32}\right] \times \left[\frac{168}{32}\right] = 4 \times 5$ times. In this case, we can choose $(r, s) = (3, 3)$ or $(4, 5)$, and the resulted watermarks are

$$W = \begin{pmatrix} S & S & S \\ S & S & S \\ S & S & S \end{pmatrix} \quad \text{or} \quad W = \begin{pmatrix} S & S & S & S & S \\ S & S & S & S & S \\ S & S & S & S & S \\ S & S & S & S & S \end{pmatrix}$$

respectively. Thus, our watermark is usually smaller than the original image. We note that in [2], the seal data is embedded only for one time and therefore the watermarking scheme proposed by Kim, Lee and Lee is not as robust as ours.

The entries $w_{i,j}$ are then modulated by a binary pseudo-noise matrix $\Lambda$, where $\lambda_{i,j} \in \{-1, 1\}$. The pseudo-noise $\lambda_{i,j}$ serves for spreading the watermark evenly and is the secret key for embedding and retrieving of the watermark. In order that the average of the "noise" $\lambda_{i,j} w_{i,j}$ is zero, we adjust the entries of the watermark to

$$\tilde{w}_{i,j} = w_{i,j} \cdot \lambda_{i,j} - \overline{w},$$

where

$$\overline{w} = \sum_{i=1}^{p \cdot r} \sum_{j=1}^{q \cdot s} w_{i,j} \cdot \lambda_{i,j} / (p \cdot q \cdot r \cdot s).$$

Then $\tilde{w}_{i,j}$ is amplified with an adjustable amplitude factor $\alpha$. The parameter $\alpha$ is a constant determining the signature strength. It is obviously that $|\overline{w}| < 1$ and therefore the signs of $\tilde{w}_{i,j}$ and $w_{i,j}\lambda_{i,j}$ are the same. Therefore, from the sign of $\tilde{w}_{i,j}$ we can determine whether $w_{i,j} = 1$ or $w_{i,j} = -1$, which is sufficient for us to justify whether the $(i, j)$-pixel is marked.

The next step is to select a sub-image to embed the watermark. The sub-image is of the same size as the watermark. To make the watermark more robust, we can select the sub-image randomly so that attackers do not know the position where the watermark is applied. For monochrome

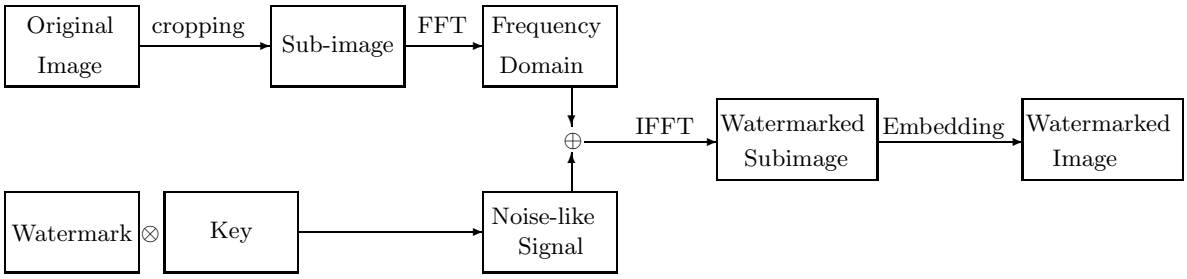


Figure 1: Embedding Steps

images, we apply the two-dimensional FFT to the matrix of pixel values directly. For color images, we represent the sub-image in YIQ color mode [1] and apply the two-dimensional FFT to the matrix of the intensity components. Let the frequency coefficients be denoted by

$$f_{i,j} = \sigma_{i,j} \exp(\beta_{i,j}\sqrt{-1}), \quad 1 \le i \le p \cdot r, 1 \le j \le q \cdot s,$$

where $\sigma_{i,j} \ge 0$ and $\beta_{i,j}$ are the magnitude and the phase angle of $f_{i,j}$ respectively. The watermark is embedded into the frequency domain of the sub-image by altering the magnitude of the frequency coefficients:

$$\tilde{f}_{i,j} = \tilde{\sigma}_{i,j} \exp(\beta_{i,j}\sqrt{-1}), \quad 1 \le i \le p \cdot r, 1 \le j \le q \cdot s,$$

where $\tilde{\sigma}_{i,j} = \sigma_{i,j} + \alpha\tilde{w}_{i,j}$. Then the inverse two-dimensional FFT is performed to obtain the watermarked sub-image. Finally, we get the watermarked image by embedding the watermarked sub-image into the original image.

The embedding process of the watermark is summarized in Figure 1.

## 2.2 The Retrieval Process

The watermark we embedded in the frequency domain of the sub-image is a noise-like signal. Therefore denoising processes can be used to recover the watermark without the knowledge of the original image. One denoising method is to blur the magnitudes of the frequency domain. For simplicity, we approximate the magnitude of the Fourier coefficients $\sigma_{i,j}$ of the original sub-image by the average of the magnitudes of the $(2c+1) \times (2c+1)$ neighborhood centered at $(i, j)$:

$$\hat{\sigma}_{i,j} = \frac{1}{(2c+1)^2} \sum_{r=i-c}^{i+c} \sum_{s=j-c}^{j+c} \tilde{\sigma}_{r,s}.$$

Then we compare the values of $\hat{\sigma}_{i,j}$ and $\tilde{\sigma}_{i,j}$: if $\hat{\sigma}_{i,j} > \tilde{\sigma}_{i,j}$, which indicates that the magnitude at $(i, j)$ becomes smaller after embedding the watermark, then $\tilde{w}_{i,j} < 0$, otherwise we have $\tilde{w}_{i,j} > 0$. From the sign of $\tilde{w}_{i,j}$, we predict that the embedded bit is

$$\lambda_{i,j}\hat{w}_{i,j} = \begin{cases} -1, & \tilde{w}_{i,j} < 0, \\ 1, & \tilde{w}_{i,j} > 0. \end{cases}$$

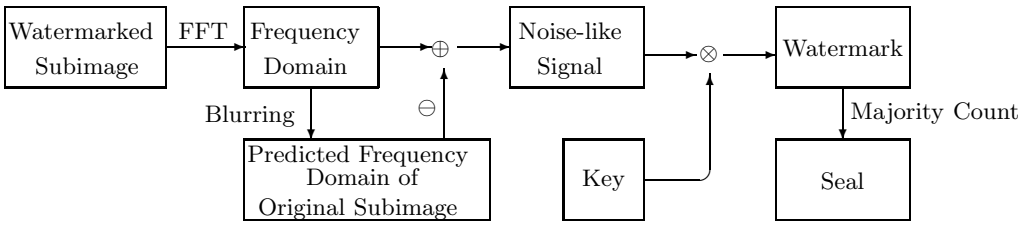


Figure 2: Extracting Steps

Finally, $\hat{w}_{i,j}$ can be obtained by dividing $\lambda_{i,j}$ by the embedded bit.

The predicted value $\hat{w}_{i,j}$ of $w_{i,j}$ may be correct or incorrect. Since the embedding of $w_{i,j}$ are repeated for $r \times s$ times, we have $r \times s$ predicted values for $w_{i,j}$. In order to make the retrieving process more reliable, we use the rule of majority count. That is, the bits of the retrieved seal is determined by

$$\hat{s}_{i,j} = \begin{cases} 1, & \sum_{k=1}^{r} \sum_{l=1}^{s} \hat{w}_{(k-1)p+i,(l-1)q+j} > 0, \\ -1, & \sum_{k=1}^{r} \sum_{l=1}^{s} \hat{w}_{(k-1)p+i,(l-1)q+j} < 0, \end{cases} \qquad 1 \le i \le p,\ 1 \le j \le q.$$

We note that the pseudo-noise matrix $\Lambda$ plays an important role in the retrieval of the watermark. If a wrong pseudo-random sequence is used, the scheme does not work, and it is impossible to figure out the seal image from the recovered data $[\hat{s}_{i,j}]_{i,j=1}^{p,q}$. This further protects the watermark from malicious attacks.

The retrieving process is summarized in Figure 2.

After retrieving the seal, users can compare the results with the referenced seal subjectively. A similarity measure of the extracted and the referenced watermarks can be defined as:

$$\textit{Correlation Value } (CV) = \frac{X}{pq},$$

where $X$ denotes the number of matched bits between the extracted seal and the referenced seal.

# 3 Experimental Results

The experiments are conducted on both 24-bit color images and 8-bit monochrome images. Six $512 \times 512$ images are tested. They are: Lena (color and monochrome), Peppers (color), Airplane (color), Baboon (color) and Fishing boat (monochrome). All testing images can be found in [8]. We use a $10 \times 20$ binary image "SPIE" as our seal for all images. The seal image and all testing images are shown in Figure 3.

In our tests, we set $r = \left\lfloor \frac{m}{2p} \right\rfloor = 25$ and $s = \left\lfloor \frac{n}{2q} \right\rfloor = 12$. Thus, we repeat the seal 300 times and the size of the watermark is $250 \times 240$. For simplicity, all sub-images to which the watermark are applied start at the pixel $\left(\left\lfloor \frac{m}{4} \right\rfloor + 1, \left\lfloor \frac{n}{4} \right\rfloor + 1\right)$, i.e. $(129, 129)$. Other parameters are set as follows: the amplitude factor $\alpha$ is 1000, the secret key is 37 (i.e., the entries of the binary pseudo-noise signal $\Lambda$ is generated by seed 37) and $c = 1$. The parameters $r$, $s$, the start position of sub-image,

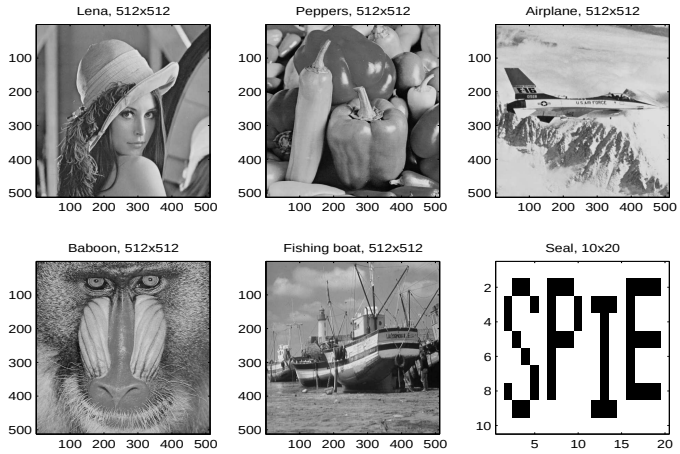


Figure 3: The Seal and the Original Images

| | *Lena* (*color*) | *Lena* (*monochrome*) | *Peppers* | *Airplane* | *Baboon* | *Fishing boat* |
|---|---|---|---|---|---|---|
| *No Operation* | 1 | 1 | 1 | 1 | 1 | 1 |
| *JPEG 70* | 0.9100 | 0.9300 | 0.9000 | 0.8500 | 0.8750 | 0.9050 |
| *JPEG 85* | 0.9950 | 1 | 0.9950 | 0.9850 | 1 | 0.9800 |
| *Blurring* | 0.9900 | 0.9850 | 0.9950 | 0.9900 | 0.9900 | 0.9900 |
| *Sharpening* | 1 | 1 | 1 | 0.9950 | 0.9900 | 1 |
| *GIF* | 1 | 1 | 1 | 1 | 1 | 1 |

Table 1: $CV$ Values

and the secret key are required to extract the watermark. The users should keep these parameters. The parameter $\alpha$ is not required and $c$ can be assigned to other values in the retrieval process.

The amplitude we select is quite small and therefore the watermarked images are of high quality. All watermarked images are shown in Figure 4. We refer to readers to [7] for the watermarked digital images. The relation between the amplitude and the PNSRs of watermarked images is shown in Table 2. We can see that the watermarked images become worse rapidly as the amplitude becomes larger. We test the robustness of our watermarking scheme under the following common attacks: JPEG (with quality factor 70 and 85 respectively), GIF compression/decompression, blurring (mask size $3 \times 3$) and sharpening (enhancement factor 75%). The $CV$ values are shown in Table 1.

We observe from Table 1 that for all testing images, at least 170 bits of 200 bits are recovered by our scheme and the watermark embedded in Airplane is the most fragile. Therefore, we plot the retrieved seals of Airplane. In Figure 5, we plot the graylevel of the retrieved seal

$$s_{i,j} = \text{uint8}\left(\frac{255}{rs}\sum_{k=1}^{r}\sum_{l=1}^{s}\hat{w}_{(k-1)p+i,(l-1)q+j}\right)$$

for the embedded bits of Airplane. We can clearly figure out the seal "SPIE" for all cases.

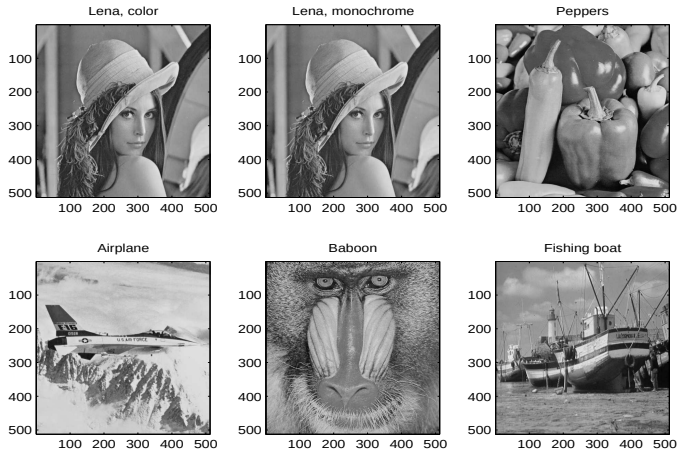


Figure 4: Watermarked Images

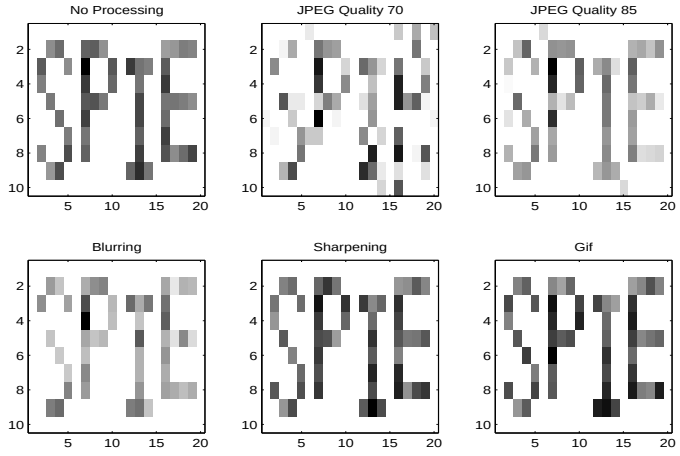


Figure 5: The Retrieved Seals from Watermarked Airplane

| $\alpha$ | *Lena* (*color*) | *Lena* (*monochrome*) | *Peppers* | *Airplane* | *Baboon* | *Fishing boat* |
|---|---|---|---|---|---|---|
| 1000 | 38.7699 | 38.3428 | 38.1468 | 38.0188 | 38.7540 | 37.7628 |
| 2000 | 32.8818 | 32.4524 | 32.2660 | 32.1260 | 32.8801 | 32.8725 |
| 4000 | 26.9333 | 26.4668 | 26.2902 | 26.1460 | 26.9775 | 26.8946 |
| 8000 | 21.0943 | 20.4905 | 20.3730 | 20.2523 | 21.1962 | 21.0212 |

Table 2: PSNR(dB) of Watermarked Sub-Images for Different Amplitudes

# 4 Concluding Remarks

In this paper, we have proposed a frequency domain based watermarking scheme. The watermarks are invisible and the watermarked images are of high quality. Our scheme is robust to common attacks such as JPEG, GIF compression/decompression, blurring, and sharpening. Repetition code is essential to make the watermark robust.

# References


[1] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Addison-Wesley Publishing Company, 1992.

[2] W. G. Kim, J. C. Lee, and W. D. Lee, *An image watermarking scheme with hidden signatures*, IEEE Proc. of the International Conference on Image Processing, Japan, October, 1999, II, pp. 206–210.

[3] E. Koch, J. Rindfrey, and J. Jhao, *Copyright protection for multimedia data*, Proc. of Int. Conf. on Digital Media and Electronic Publishing, 1994.

[4] W. N. Lie and L. C. Chang, *Data hiding in images with adaptive numbers of least significant bits based on the human visual system*, IEEE Proc. of the International Conference on Image Processing, Japan, October, 1999, II, pp. 286–290.

[5] M. Ramkumar, A. N. Akansu, and A A. Alatan, *A robust data hiding scheme for images using DFT*, IEEE Proc. of the International Conference on Image Processing, Japan, October, 1999, II, pp. 211–215.

[6] D. C. Wu and W. H. Tsai, *Image hiding in spatial domain using an image differencing approach*, Proc. of 1998 Workshop on Computer Vision, Graphics, and Image Processing, Taipei, Taiwan, pp. 280–287, 1998.

[7] See ftp://ftp.math.cuhk.edu.hk/report/2001-04/

[8] See http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/image_database.html