Image-Data Watermarking by Embedding a Fresnel-Transformed Pattern

(フレネル変換パターンの埋め込みによる電子透かし法)

Seok Kang[†], Yoshinao Aoki (member)[†]

Abstract Watermarking techniques embed hidden information imperceptibly in data which represents images and sounds. The original image is generally transformed so that coded watermark data can be embedded in the frequency domain. In this paper, we outline a new method for embedding watermarks in image data by using a Fresnel transform. The watermark image is Fresnel-transformed and the resulting intensity pattern is embedded in the original image. Our watermarking model allows flexibility in hiding the watermark. It is possible to get many embedding patterns from a single watermark image by using various distance parameters with the Fresnel transform. All kinds of image models, such as shapes, letters and photos, can be used as watermark data. Watermarking experiments have shown the validity of our system and its robustness in resisting attacks.

Key words: watermarking, steganography, Fresnel transform, Fourier transform, data embedding

1. Introduction

In recent years, the spread of the Internet and the advance in digital techniques for transmitting and storing information have made it possible to copy and edit images, audio, video and other types of multimedia data. Multimedia data by digital format can be duplicated without loss of quality and changed easily at low cost. These situations cause the illicit actions such as interception, duplication, misuse and unauthorized modification of information. One approach to address the problem is watermarking technique. The concept of digital Watermarking is associated with the data-hiding technique known as steganography¹⁾. Watermarking is a technique to embed hidden multimedia information such as images and sounds. Digital watermarking has been proposed as a way to identify the source, creator, owner, distributor, or authorized consumer of multimedia data.

The process of watermarking involves the modification of the original information data to embed watermark information. The embedding method must leave the original information data perceptually unchanged, yet watermark data should be detected by extraction

algorithm. And, the following conditions are requested for watermarking:

- Watermark data should be imperceptible so as not to affect the experience of viewing the image and readily detectable by the proper authorities, even if imperceptible to the average observer.
- The watermark data must survive image modifications that are common to typical applications, such as scaling and color requantization, commonly performed by a picture editor, or lossy compression techniques like JPEG, used for transmission and storage.
- It must be difficult or impossible to remove watermark data, at least without visibly degrading the original image.

Various watermarking techniques have been developed. However, these techniques can be grouped into two classes: spatial domain methods and frequency domain methods. The spatial domain techniques are to embed the watermarking data by directly modifying the pixel values of the original images (the lower bit of image's intensity, brightness, geometric transformation, R.G.B color image, etc). The simplest watermarking technique is to just flip the lowest-order bit of chosen pixels in a gray-scale(8-bit) or color(24-bit) image. This works well only if the image will not be subject to any modification, such as color modification done by a photo editor. Another technique embeds a more robust watermark in much the same way as a watermark is added to paper: A

Received October 29, 1999; Revised February 24, 2000; Accepted March 9, 2000

[†]Graduate School of Electronics and Information Engineering, Hokkaido University
(N13 W8, Kita-ku, Sapporo, Hokkaido 060-8628, Japan)

watermark symbol is superimposed over an area of the image and some fixed intensity value for the watermark to the varied pixel values of the image is added. One disadvantage of spatial domain watermarks is that a common picture-cropping process can eliminate the watermark. In the case of the frequency domain techniques, where original digital data are transformed into frequency components, watermark information are embedded into particular frequency regions of original data. A representative research based on spread spectrum made a further advance in this class²⁾. Also DFT, DCT, or wavelet-based methods are proposed^{3) 4) 5) 6) 7)}. The advantage of frequency domain method is that the watermark is spreaded throughout the whole image or sound and hence is resistant to cropping or cutting. However, a standard frequency filter or a lossy compression algorithm, which usually filters out the less significant frequencies, could damage the watermark information.

In this paper, we propose a new watermarking technique using Fresnel transform and address new method to embed an image as watermark data. Our watermarking system is different from other frequency domain watermarking methods. It does not need to transform original information data. Transformed pattern of watermark data is embedded into original data. So our technique has the characteristics of spatial domain and frequency domain methods. Since Fresnel transform is based on Fresnel diffraction from the viewpoint of the optical processing theory, it shows that our method can provide multi-observable surfaces for getting many embedding patterns.

2. Numerical Fresnel Transform

A Fresnel transform describes the wave propagation in the Fresnel diffraction region, whereas Fourier transform describes the Fraunhofer diffraction in the far field.

2.1 Theory of Fresnel Transform

When the model under watermarking is supposed to have a 2-D object pattern $s(x_1, y_1)$ located on the object plane $x_1 - y_1$, the Fresnel diffraction pattern $F(x_2, y_2)$ on the observed plane $x_2 - y_2$ can be expressed by the following equation⁸⁾ based on the Fresnel approximation.

$$F(x_2, y_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} s(x_1, y_1) \exp \left[-\frac{j\pi}{d} [(x_2 - x_1)^2 + (y_2 - y_1)^2] \right] dx_1 dy_1 \quad (1)$$

where d is a parameter as expressed by Eq.(2) with the distance z between the object and observing planes and a wavelength λ as shown in **Fig.1**.

Fig. 1 Fresnel transform of a 2-D model

$$d = \lambda z \quad (2)$$

Eq.(1) can be indicated as the integral of the convolution of function $s(x, y)$ and the following phase function $p(x, y)$ called as propagator.

$$p(x, y) = \exp \left[-\frac{j\pi}{d} (x^2 + y^2) \right] \quad (3)$$

A conventional method as adopted in the numerical image reconstruction technique in long-wavelength holographies is discussed to calculate Eq.(1) by computer, where the Fresnel transform is calculated by two-times of Fourier transforms according to Eq.(4). Let $\mathcal{F}$ and $\mathcal{F}^{-1}$ denote Fourier and inverse Fourier transforms respectively. Eq.(1) can be expressed as follows by the convolution theorem.

$$F = \mathcal{F}^{-1} [\mathcal{F}[s] \mathcal{F}[p]] \quad (4)$$

The Fourier transform $P(\mu, \nu) = \mathcal{F}[p]$ of the phase function p of Eq.(3) is obtained analytically as follows:

$$\begin{aligned} P(\mu, \nu) &= \mathcal{F}[p] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \exp \left[-\frac{j\pi}{d} (x^2 + y^2) \right] \\ &\quad \times \exp [-j2\pi(\mu x + \nu y)] dx dy \\ &= -jd \exp [j\pi d(\mu^2 + \nu^2)] \end{aligned} \quad (5)$$

where μ and ν are spatial frequencies. The calculation of numerical Fresnel transform using FFT algorithm is performed by the flow of **Fig.2**. The inverse Fresnel transform means a Fresnel transform of Fresnel diffraction pattern with the value of the parameter $-d$ and its equation can be expressed as follows:

$$F(x_1, y_1) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} s(x_2, y_2) \exp \left[-\frac{j\pi}{d} [(x_1 - x_2)^2 + (y_1 - y_2)^2] \right] dx_2 dy_2 \quad (6)$$

2.2 Sampling condition in numerical Fresnel transform

When Fresnel transform is calculated numerically, it

Fig. 2 The flow of calculation of Fresnel transform

needs to perform sampling and discretion of phase function P in Eq.(5). Let $L \times L$ is the square aperture of the object plane and N is the sampling numbers with respect to each side of this aperture, P in Eq.(5) is sampled with the sampling intervals $1/L$ by virtue of the DFT algorithm and aperture of spectrum plane is $-(1/L)(N/2) \sim (1/L)(N/2)$. Therefore the discrete phase function of Eq.(5) in the spectrum plane is expressed as follows:

$$P = \exp \left[j \frac{\pi d N^2}{L^2 N^2} (I^2 + J^2) \right] \text{ (Let } d' = \frac{d N^2}{L^2} \text{)}$$

$$= \exp \left[j \frac{\pi d'}{N^2} (I^2 + J^2) \right] \quad (7)$$

From the Eq.(7), the phase change at the 1 sampling interval of aperture having length $L/2$ in the spectrum plane is obtained as follows:

$$\frac{\pi d'}{N^2} \left[\left(\frac{N}{2} \right)^2 - \left(\frac{N}{2} - 1 \right)^2 \right] \approx \frac{\pi d'}{N} \quad (8)$$

From the fact that the maximum phase change of Eq.(8) must be smaller than π , the following condition is obtained:

$$\pi d' \leq \pi N \quad (9)$$

And we determine a new parameter as a distance parameter of Fresnel transform as follows:

$$D = \pi d' \quad (10)$$

2.3 Fresnel transform of image

If z in Eq.(2) becomes smaller, the parameter d approaches 0, and the value of $\exp[j\pi d(\mu^2 + \nu^2)]$ can be approximated by 1. Under this condition, the expression reduces to $F = -jd\mathcal{F}^{-1}\mathcal{F}[s] = -jds$ in Eq.(4) and the diffraction pattern keeps the shape of the original model s . Its intensity distribution becomes localized (that is, the intensity distribution becomes close to that of the original image). On the other hand, as the parameter d

Fig. 3 Letter E model and its Fresnel transform and inverse Fresnel transform patterns

increases, the Fresnel diffraction pattern becomes conspicuous and the transformed image deviates from the original image with a wide-spread intensity distribution as shown in the upper side of Fig.3 and 128×128 sampling points are chosen. The lower side of Fig.3 is the simulation result of inverse Fresnel transform of Letter model E . Fig.3(b) and (c) are transformed images of Fig.3(a) and Fig.3(e) and (f) are inverse transformed images of Fig.3(d).

3. Watermarking by Fresnel transform

Before explain our watermarking system, we first look at the generic watermarking embedding and extracting schemes.

- **Generic embedding process:** Given an original image I , a watermark W , a key K (usually the seed of a random number generator) and a watermarked version $\hat{I}$, the embedding process can be defined as a mapping of the form: $I \times K \times W \rightarrow \hat{I}$ and is common to all watermarking methods (where the operator $\times$ means arbitrary operation).

- **Generic detection process:** Output is either the recovered watermark W or some kind of confidence measure indicating how likely it is for a given watermark at the input to be present in the image $\hat{I}'$ under inspection. Several watermarking systems are defined by their inputs and outputs of detection process⁹⁾:

- **Private watermarking:**

- Type I: $\hat{I}' \times I \times K \rightarrow W$

- Type II: $\hat{I}' \times I \times K \times W \rightarrow 0, 1$

- **Semi-private watermarking:** $\hat{I}' \times K \times W \rightarrow 0, 1$

- **Public watermarking:** $\hat{I}' \times K \rightarrow W$

- **asymmetric watermarking:** any user can read the watermark without being able to remove it

Fig. 4 Watermarking system block diagram

We propose a new watermarking system by embedding both data real number and imaginary number of Fresnel-transformed pattern of a watermark image into original image. Our watermarking system, diagrammed in Fig.4, is a watermarking scheme having characteristics of spatial domain method and frequency domain method. In Fig.4 Watermark Data 1 and 2 are real number data and imaginary number data of Fresnel transform respectively. Whereas original model is transformed and coded watermark data is embedded into transformed pattern of original data in the general frequency domain watermarking systems, in our watermarking system just transformed pattern of watermark data is embedded.

3.1 Data embedding and extracting

According to Fresnel transform characteristics, our watermarking scheme provides many patterns of embedded images with an original image and a watermark image by the flexibility of the distance parameter D of Fresnel transform. The algorithms of our watermarking system can be described as follows:

Let the size of original image is $m \times m$ and the size of watermark image is $n \times n$.

Condition of the size of a watermark image:

$m = 2^p * n$ (p is positive integer) is a sufficient condition to embed both real and imaginary number data of Fresnel-transformed pattern of a watermark image.

Here explain algorithm with the condition $m = 4n$.

Embedding calculation formula:

Selection of $D_{embedding}$:

$$W' = \text{FRESNEL}(W)$$

$$W' \in (R_{nn}, I_{nn})$$

$$W'_{code} \in (A_k, B_l)$$

$$E = O + W'_{code} * w$$

where

$D_{embedding}$: the distance parameter of Fresnel transform in embedding process;

W : watermark image;

W' : Fresnel transformed-pattern of watermark image;

R_{nn} : real number data of W'

I_{nn} : imaginary number data of W'

A_k is a embedding data block consist of R_{nn} and I_{nn} ($k = 1, 2, 3, 4, 5, 6$):

$$A_k = \begin{matrix} & & & 2n \\ n & \begin{pmatrix} R_{11} & I_{11} & \dots & R_{1n} & I_{1n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ R_{n1} & I_{n1} & \dots & R_{nn} & I_{nn} \end{pmatrix} \end{matrix}$$

B_l is a embedding data block consist of R_{nn} and I_{nn} ($l = 1, 2$):

$$B_l = \begin{matrix} & & n \\ 2n & \begin{pmatrix} R_{11} & \dots & R_{1n} \\ I_{11} & \dots & I_{1n} \\ \vdots & \ddots & \vdots \\ R_{n1} & \dots & R_{nn} \\ I_{n1} & \dots & I_{nn} \end{pmatrix} \end{matrix}$$

w : embedding parameter;

O : original image;

E : embedded image;

W'_{code} : embedding pattern coded into original image and having the structure in Fig.5 and its structure could be variable by arranging A_k and B_l (here we choose the structure of Fig.5 for the cropping attack);

Extraction calculation formula:

Selection of $D_{extraction}$:

$$W''_{code} = (E - O) * \frac{1}{w}$$

Choose A'_k or B'_l from W''_{code}

$$A'_k \in (R'_{nn}, I'_{nn})$$

$$B'_l \in (R'_{nn}, I'_{nn})$$

$$W'' = \text{IFRESNEL}(R'_{nn}, I'_{nn})$$

where

$D_{extraction}$: the distance parameter of Fresnel transform in extraction process ($D_{embedding} + D_{extraction} = 0$);

O : original image;

E : embedded image;

W''_{code} : extracted embedding pattern;

w : embedding parameter;

A'_k, B'_l : a extracted embedding data block and has same structure as A_k, B_l ;

R'_{nn}, I'_{nn} : real number data and imaginary data from A'_k or B'_l for inverse Fresnel transform and each one

Fig. 5 Structure of embedding pattern

Fig. 6 Original image and watermark image

is extracted from arbitrary embedding data block(here extracted from A'_1 except cropping attack);
 W'' : extracted watermark image;

4. Experimental results

In order to confirm the validity of the proposed method, we conducted experiments with a photo image as an original image and a signature image as a watermark image as shown in Fig.6(512×512 and 128×128 sampling points are chosen for an original image and a watermark image respectively and having 256 grey-scaled levels). And for our experiments we simply used the $PSNR$ (Peak Signal to Noise Ratio)¹⁰ and it is given by:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (11)$$

where MSE is Mean Square Error.

4.1 Embedding and extraction results

Our experiments are performed by changing the values of two parameters w and D . Fig.7(a)-(c) shows the watermarked versions of an original image, where the distance parameters of Fresnel transform are chosen as $D_{embedding} = 0.1$ and embedding parameters are chosen as $w = 0.01, 0.05, 0.1$ respectively. Fig.8 shows the extracted images from watermarked versions of Fig.7, where the distance parameters for the inverse Fresnel

Fig. 7 Watermarked versions of an original image

Fig. 8 Extracted versions from watermarked versions

Fig. 9 PSNR performance changing of the value of w

transform are chosen as $D_{extraction} = -0.1$. Some noises in Fig.8 are caused by the error of conversion of embedded data from *float* to *unsigned char* when a watermarked image is saved as an image file and rescaling error when watermark data are extracted by the parameter w . Fig.9 shows the $PSNR$ performance of experimental results changing the value of the parameter w and it can be said that the qualities of watermarked versions and extracted versions depend on the embedding parameter w . The $PSNR$ performance of embedding and extracting results with several distance parameters $D_{embedding}$ are given in Table 1. From the Table 1 we can find out the fact the parameter $D_{embedding}$ has no influence on the quality of embedding result. But it is very important to use correct value of parameter $D_{extraction}$ in extraction step as compared in Fig.10. So it is possible to use $D_{extraction}$ as a hidden key in extraction process.

The results of Fig.7, 8 and Table 1 verify the validity of our watermarking system and show the flexibility of data hiding in watermarking using Fresnel transform.

Table 1 The PSNR performance of embedding and extracting results($w = 0.05$)

$D_{embedding}$	0.1	0.5	1.0	5.0	10
embedding	30.63	30.63	30.63	30.63	30.63
extracting	28.45	26.43	28.89	24.34	24.05

(a) Correct value(-0.1) (b) Incorrect value(-0.5)

Fig. 10 Comparison the extraction results using correct value of $D_{extraction}$ or not from Fig.7(b)

Quality = 90% Quality = 60% Quality = 30%

Fig. 11 Extracted versions from compressed images

5. Robustness Experiments

Watermark robustness under image modification is an essential topic for copyright protection. Any user can modify an original image to increase quality, compress data, edit digitally, and so on. We conducted three experiments to inspect the robustness of our watermarking system against compression, filtering and geometric modifications, and all images are generated by Stir-Mark⁹⁾ for the test of robustness with the watermarked version($D = 0.1$ and $w = 0.05$).

5.1 Lossy compression

It is the most widely used procedure to store and send digital images. The JPEG algorithm provides a high compression ratio and the desired quality. However, lossy compression tends to remove invisible information related to the watermark. Therefore, watermarks should combine invisibility and robustness simultaneously. We extracted watermark data from reconverted images from JPEG to raw data. **Fig.11** and **Table 2** show the robustness about image compression by JPEG.

5.2 Filtering

Users apply filtering to remove noise or to improve

Table 2 The PSNR performance of extracting results from JPEG compressed images

Quality	30%	45%	60%	75%	90%
extracting	2.64	4.58	6.21	8.68	13.67

(a) Gaussian filter (b) Median filter

Fig. 12 Extracted versions from modified versions by gaussian filter and median filter

Fig. 13 Extracted versions from geometrically modified versions

the perceptual quality. This process can remove watermarks as well. Additionally, attackers may develop filters specifically designed for watermark removal. **Fig.12**(a) and (b) show the detecting results of watermark data from gaussian filtering version and median filtering version of watermarked version respectively.

5.3 Geometric modifications

Geometric modifications include flipping, rotation, cropping, reflection, line and column extraction or insertion, and combination of these. Watermark detection in geometrically modified products without resorting to the original product is a difficult task. **Fig.13** shows the extracted versions from the rotated($\frac{\pi}{2}$), flipped, and cropped(50%) images of watermark versions from the left side to the right side respectively. In addition, $PSNR$ performance of extracted watermark image from cropped version is 26.34 and extracted from cropped image size. From the robustness results of our watermarking system, it can be said that our technique has robustness against lossy compression and geometric modifications and filtering(even though extracted images are very rough in the case of filtering).

6. Discussion

6.1 Watermark data

Many types of data can be used as a watermark data in watermarking system. It depends on the algorithm of embedding process. In our system, where just transformed pattern is embedded into the original image, it is better to use image files as a watermark data than bit stream data. And a signature image used in our experiments has a property that nobody can make same one.

6.2 Fresnel transform and watermarking

As shown in Fig.3, a Fresnel-transformed pattern has spreaded type and it keeps the form of an original model. It can be investigated from two points of view robustness of our system using Fresnel transform to the attack. From the point of attackers, it must be difficult to attack transformed pattern because they have to consider full fields of transform plane. And the other side, keeping the form of original model, our method has robustness to attacks.

It is possible to perform our watermarking algorithm using Fourier transform and its results are given in Fig.14. *PSNR* performance of results of Fig.14(a)-(c) are 30.63, 4.42, 1.98 respectively and JPEG quality is 60%. From the comparison of Fresnel transform method and Fourier transform method, our method using Fresnel transform is more tolerant against data distortion.

Our watermarking method using Fresnel transform, where all frequency components of Fresnel transform are embedded into an original image, has tolerance against lossy compression like JPEG because even though the values of typical frequency regions are changed by JPEG algorithm, it is possible to reconstruct with remained frequency components. But in the case of attack by gaussian and median filtering, extracted watermark data are severely damaged. It is due to the distribution patterns of real number data and imaginary number data of Fresnel transform, where real number data are symmetrical to the Y axis and imaginary number data are symmetrical to the origin like Fourier transform. From the distribution patterns, it can be said that imaginary number data are damaged more than real number data by gaussian and median filtering. As we have to use both real and imaginary number data to perform inverse Fresnel transform, serious distortion of extracted watermark data occur of different change ratio between real number data and imaginary number data by gaussian and median filtering, and it could be

Fig. 14 Watermarking results by Fourier transform

a weak point of our method to embed both real and imaginary number data of Fresnel transform. However following problem depends on the structure of filtering operator to the other filtering attacks.

6.3 Robustness to the cropping

It must be required to resize cropped image as same size as an original image in other watermarking systems(original image is transformed) because frequency components are truncated. On the other hand, watermark can be extracted without resizing in our system because transformed pattern of watermark data is embedded into the spatial plane of an original image. And the condition of minimum size of cropped image is related to the size of embedding data block in Section 3.1. If the size of watermark data is $n \times n$, condition will be $2n \times n$ in the case of centralized cropping.

7. Conclusion

A new watermarking technique by Fresnel transform is proposed and experiments are done resulting in confirming the validity of the proposed technique. To vary our method is further subject to study in order to extend the proposed technique to the integrated system.

From the experimental result, it is said that our technique using Fresnel transform has a possibility to embed an image as a watermark data in watermarking and also the extracting results about robustness show that our method has the resistance to lossy compression like JPEG and geometric modifications and filtering.

It is difficult to comment on our system with other watermarking systems, because our system use an image as watermark data. It has been reported that it is difficult to embed an image as watermark data in frequency domain methods because of low robustness against attacks⁷⁾. But our simulation results cleared that weak point and from a practical use of view, our scheme is fit for the personal user level watermarking system and extraction watermark data in software level by the simplicity and clearness in authentication of watermark data.

[References]

- 1) Michiharu Niimi, Hideki Noda and Eiji Kawaguchi, "A study on the Steganography using Bit-Plane Complexity Segmentation," Image and Vision Computing New Zealand'98(IVCNZ'98), pp.151-156, Auckland, New Zealand, November 1998.
- 2) Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., "Watermarking for multimedia," NEC Research Institute Technical Report 95-10, 1995.
- 3) E.Koch, J.Rindfrey, and J.Zhao, "Copyright protection for multimedia data," In Proc. of the Int. Conf. on Digital Media and Electronic Publishing, 1994.
- 4) C.T Hsu and J.L Wu, "Hidden signatures in images," In Proc. of the ICIP-96, Vol.3.
- 5) A.G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," In Proc. of the ICIP-96, Vol.3.
- 6) W.L.Tang and Y.Aoki, "A DCT-based coding of images in watermarking," In Proc. of the ICICS'97 Vol.1.
- 7) J. Ohnishi and K. Matsui, "Image coding for copyright protection by using wavelet," Trans. of IPSJ, Vol.38, No.3, pp.534-539, 1997.
- 8) Y. Aoki, "Wave signal processing," Morikita publisher(Tokyo), 1986.
- 9) M. Kutter and F.A.P. Petitcolas, "A fair benchmark for image watermarking systems," Proc. of Electronic Imaging'99, Security and Watermarking of Multimedia Contents, Vol. 3657, Jan., 1999.
- 10) J. Ohnishi and S. Ozawa, "Watermark supports cropping attack via multiresolution analysis," Trans. IEICE, Vol.J81-D-II, No.10, pp.2321-2329, 1998.

Kang Seok received B.E. degree from Soongsil University, Seoul, Korea, in 1994 and M.E. degree in Electronic Information Engineering from Hokkaido University, Sapporo, Japan, in 1997. He is now a graduate student in the Doctoral Program of Electronic Information Engineering, Faculty of Engineering, Hokkaido University. He is currently engaged in research on image processing, computer graphics, and digital watermarking.

Aoki Yoshinao received B.E., M.E., and ph.D. degrees from Hokkaido University in 1964, 1966, and 1973, respectively. From 1967 to 1979, he was Assistant Professor, and since 1979, Professor of Electronic Engineering at Hokkaido University. He is engaged in research on long-wave holography, signal and image processing, computer graphics, and applications of communication satellites. He is a member of the Information Processing Society of Japan, and IEEE.