이미지 워터마킹을 위한 Fresnel 변환을 이용한 데이타 삽입 기법

(A Data Embedding Technique for Image Watermarking using Fresnel Transform)

강 석 † 아오끼 요시나오 ††
(Seok Kang) (Yoshinao Aoki)

요 약 디지털 워터마킹은 이미지, 사운드와 같은 멀티미디어 데이타에 지각할 수 없도록 비밀 정보를 삽입하는 기법이다. 일반적으로 주파수 영역 워터마킹 기법에서는 원 이미지에 대해 주파수 변환을 하고, 그 변환 면에 부호화된 워터마크 데이타를 삽입한다. 본 논문에서 우리는 Fresnel 변환을 이용한 새로운 워터마크 데이타 삽입 기법을 제안한다. 워터마크 이미지를 Fresnel 변환시켜 얻은 패턴의 값들을 원 이미지에 삽입한다. 본 워터마킹 모델은, 하나의 워터마크 이미지로부터 Fresnel 변환의 거리 파라미터의 값에 변화를 줌으로써 다양한 삽입 패턴을 얻을 수 있음으로 인해 데이타 삽입에 있어서 유연성을 가진다. 또한 도형, 문자, 사진과 같은 모든 종류의 이미지를 워터마크 데이타로 사용하는 것이 가능하다. 제안된 기법의 유효성을 검증하기 위한 실험 결과, 손실 압축, 필터링, 기하학적 변환 등의 공격에 대해 내성을 지니고 있음을 보였다.

키워드 : 워터마킹, 퓨리에 변환, Fresnel 변환, 데이타 은닉

Abstract Digital watermarking is a technique embedding hidden information into multimedia data imperceptibly such as images and sounds. Generally an original image is transformed and coded watermark data is embedded in frequency domain watermarking models. In this paper, We propose a new data embedding method using Fresnel transform. A watermark image is Fresnel-transformed and the intensity of transformed pattern is embedded into original image. Our watermarking model has the flexibility in data embedding. It is possible to get many embedding patterns from a single watermark image by using various distance parameters with Fresnel transform. All kinds of image models such as shape, letter and photo can be used as a watermark data. The watermarking experiments were conducted to show the validity of the proposed method, and the results show that our method has the robustness against lossy compression, filtering and geometric transformation.

Key words : Watermarking, Fourier Transform, Fresnel Transform, Data Embedding

1. Introduction

Digital watermarking, a technique to embed hidden information has been proposed as a method to protect digital data (e.g. audio, images, video, etc.) against the illicit actions such as interception, duplication, misuse and unauthorized modification of digital information over the past few years.

The concept of digital watermarking is associated with the data-hiding technique known as steganography[1]. The process of watermarking involves the modification of the original information data to embed a watermark information. The embedding method must leave the original information data perceptually unchanged, yet watermark data should be detected by extraction algorithm.

- *It must be difficult or impossible to remove*

† 정 회 원 : 충북대학교 전기전자컴퓨터공학부 및 컴퓨터정보통신연구소
kssrh@cbucc.chungbuk.ac.kr
†† 비 회 원 : 북해도대학교 공학연구과 교수
aoki@media.eng.hokudai.ac.jp

논문접수 : 2002년 2월 21일
심사완료 : 2002년 10월 10일

watermark data, at least without visibly degrading the original image.

- The watermark data must survive image modifications that are common to typical applications, such as scaling and color requanti zation, commonly performed by a picture editor, or lossy compression techniques lie JPEG, used for transmission and storage.
- 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.

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). These techniques can be easily attacked by the illicit image processing. In the case of the frequency domain techniques, where original digital data are transformed into frequency components, watermark informations are embedded into particular frequency regions of original data. A representative research based on spread spectrum made a further advance in this class[2]. Also DFT, DCT or WT(Wavelet Transform) 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. Our water marking system is different from other frequency domain watermarking methods. Original information data does not need to be transformed. Transformed pattern of watermark data is embedded into original data. In the next section we review the numerical Fresnel transform. In Section 3, the proposed watermarking system is introduced. Experimental results are given in Section 4 and 5, and show the validity of our method. We provide conclusion in Section 6.

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 equation[8].

$$F(x_2,y_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s(x_1,y_1)\exp\left[-\frac{j\pi}{D}\left[(x_2-x_1)^2+(y_2-y_1)^2\right]\right]dx_1dy_1 \qquad (1)$$

where D is a distance 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.

$$D = \lambda z \qquad (2)$$

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

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

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.

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

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

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

where μ and ν are spatial frequencies. The calculation of numerical Fresnel transform is performed by the flow of Fig. 2.

The inverse Fresnel transform means a Fresnel transform of Fresnel diffraction pattern with the distance parameter -D and its equation can be expressed as follows:

$$F(x_1, y_1) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s(x_2, y_2) \; [-\frac{j\pi}{D}[(x_1-x_2)^2 + (y_1-y_2)^2]]\, dx_2 dy_2 \tag{6}$$

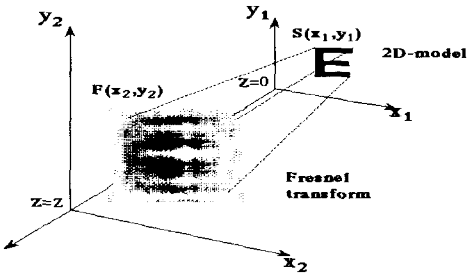


Fig. 1 Fresnel transform of a 2-D model

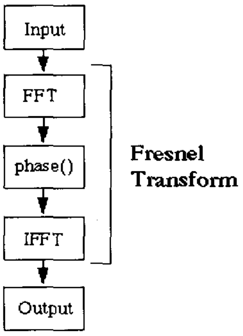
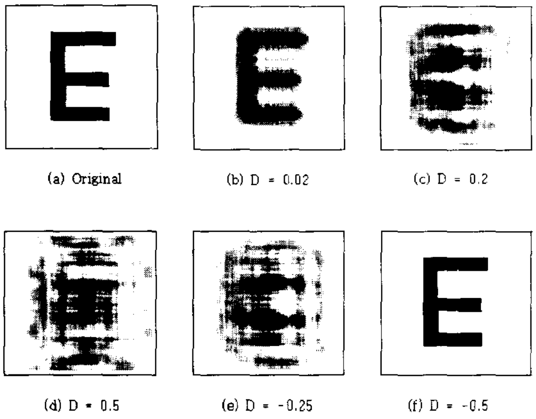


Fig. 2 The flow of calculation of Fresnel transform

2.2 Fresnel transform of image

If z in Eq.(2) becomes smaller, the distance 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 distance parameter D 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(d) is transformed image of Fig. 3(a) with the value of parameter D=0.5. Fig. 3(e) and (f) are inverse transformed images of Fig. 3(d).


(a) Original (b) D = 0.02 (c) D = 0.2

(d) D = 0.5 (e) D = -0.25 (f) D = -0.5

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

3. Watermarking using Fresnel Transform

Fourier transform provides only one spectrum plane for embedding data, so the embedded information can be removed easily. To increase the flexibility in data hiding, we propose a new technique using Fresnel transform.

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

- Generic embedding process: Given an original image O, a watermark W and a key K(usually the seed of a random number generator), the embedding process can be defined as a mapping of the form: $I \times K \times W \rightarrow I'$ and is common to all watermarking methods.
- Generic detection process: Output is either the recovered watermark W or some kind of confidence measure indication how likely it is for a given

watermark at the input to be present in the image I'' under inspection.

Our watermarking system, diagrammed in Fig. 4 is a kind of frequency domain method which embeds a data stream by modulating the transform domain coefficients. Whereas generally original model is transformed and coded watermark is embedded, in our watermarking system just transformed watermark data is embedded. It does not need to transform an original image.

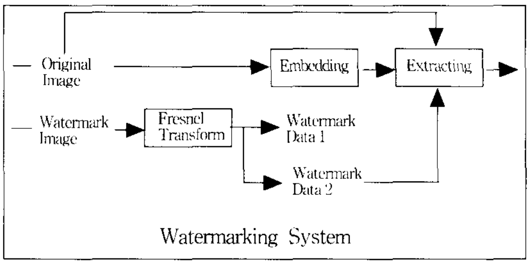


Fig. 4 Watermarking system block diagram

3.1 Fresnel Transform and Watermarking

There are two flexibilities using Fresnel transform in watermarking. The first one is to provide many transform planes for many different types of embedding patterns with various distance parameters of Fresnel transform from a watermark image. The second one is the flexibility in extraction of watermark data by inverse Fresnel transform. As shown in Fig. 3, it is possible to extract watermark data from transformed pattern. It is the simplest and the most powerful way to embed an image into original data.

3.2 Data Embedding and Extracting Process

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 data embedding and extracting can be described as follows:

Extractmbedding calculation formula :

Selection of $D_{embedding}$:

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

$$W' \in (\mathrm{R}, \mathrm{I})$$

$$W'_{code} = R$$

$$E = O + W_{code} * w$$

where

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

W' : Fresnel-transformed pattern of watermark image;

R : real number data of W' ;

I : imaginary number data of W' ;

W'_{code} : embedding pattern coded into original image;

w : embedding parameter;

O : original image;

E : embedded image;

Extracting calculation formula :

Selection of $D_{extraction}$:

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

$$W'' = IFRESNEL(W''_{code}, D)$$

where

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

O : original image;

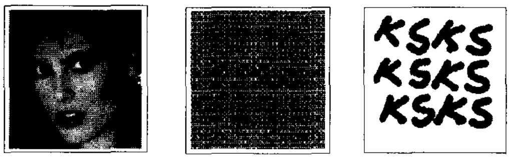
E : embedded image;

W''_{code} : extracted coding data;

W'' : extracted watermark image;

4. Embedding and Extraction Results

In order to confirm the validity of the proposed method, we implemented the some experiments with a pattern image and a signature image(as watermark data) as shown in Fig. 5 and 256 × 256 sampling points are chosen.



(a) Original (b) Image1 (C) Image2

Fig. 5 Original image and watermark images

The upper side of Fig. 6 shows the watermarking versions of original image, where the distance parameters are chosen as $D_{embedding} = 0.1$ for the image 1 and image 2 from left to right respectively and embedding parameter is chosen as w = 0.05 for all experiments. The lower side of Fig. 6 shows the extracted images from watermarked versions, where the distance parameters are chosen as $D_{extraction} = -0.1$.

And for our experiments we simply used the PSNR(Peak Signal to Noise Ratio) and it is given by:

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

where MSE is Mean Square Error.

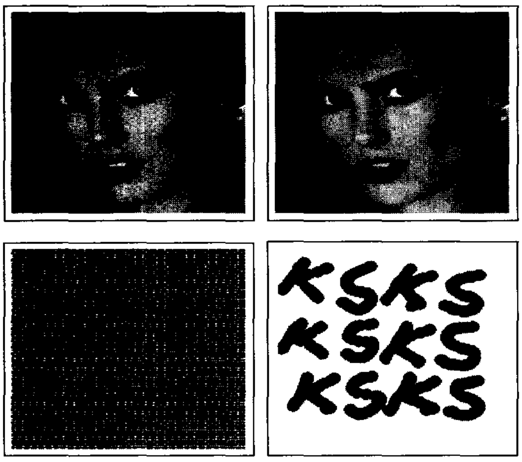


Fig. 6 Watermarked versions and extracted versions with distance parmeter D=0.1

The PSNR performance of embedding and extracting results at several distance parameters D are given in Table 1 and 2 for the image 1 and image 2, respectively. The results of Fig. 6 and Table 1-2 verify the validity of our proposed technique and show the flexibility of data hiding in watermarking using Fresnel transform.

From the Table 1 and 2, we can find out the fact the parameter $D_{embedding}$ has no influence on the quality of embedding and extraction results(maximum difference value is within 2). The qualities of watermarked versions and extracted versions depend on the embedding parameter w determine the strength of intensity of embedding pattern. The range of the values of $D_{embedding}$ chosen is depend on the sampling condition of numerical Fresnel transform, and its condition is $D \leq N$(where N is the sampling numbers)[8].

Table 1 The PSNR performance of embedding results

$D_{embedding}$	0.1	0.5	1.0	5.0	10
image1	27.71	28.15	26.50	26.78	26.58
image2	27.45	27.44	27.45	27.45	27.45

Table 2 The PSNR performance of extracting results

$D_{extraction}$	-0.1	-0.5	-1.0	-5.0	-10
image1	32.29	31.00	31.64	31.29	30.68
image2	28.35	28.41	28.29	28.49	28.36

5. Robustness Experiments

Watermark robustness under image modification is an essential topic for copyright protection.

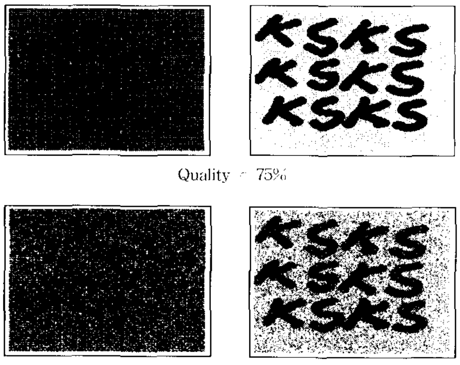
Any user can modify an original image to increase quality, compress data, edit digitally, and so on. We conducted three experiments to inspect the robustness of our watermarking system against compression, filtering and geometric modification, and all images are generated by StirMark[9] for the test 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. 7 and Table 3 show the robustness about image compression by JPEG.

Table 3 The PSNR performance of extracting results from JPEG compressed images

Quality	15%	30%	45%	60%	75%
image1	4.44	6.00	6.97	7.87	9.96
image2	5.42	7.30	8.55	9.63	11.38

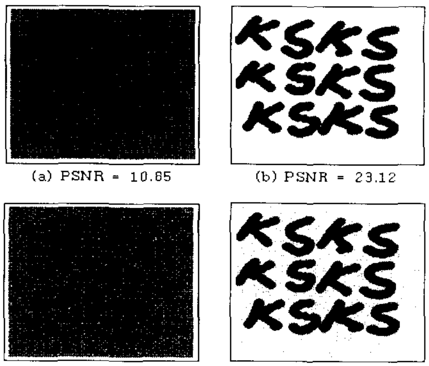

Quality = 75%

Quality = 15%

Fig. 7 Extracted versions from compressed images

5.2 Filtering

Users apply filtering to remove noise or to improve the perceptual quality. This process can remove watermarks as well. Additionally, attackers may develop filters specifically designed for watermark removal. Fig. 8 (a) and (b) show the detecting results of watermark data from gaussian filtering versions for the image 1, and 2 respectively, and (c) and (d) show the results from median filtering versions for the image 1 and 2 respectively.


(a) PSNR = 10.85

(b) PSNR = 23.12

(c) PSNR = 9.51

(d) PSNR = 15.38

Fig. 8 Extracted versions from modified versions by gaussian filtering and median filtering

5.3 Geometric Modifications

Geometric modifications include rotation, cropping, scaling, flipping, 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. 9 shows the extracted versions from the rotated $(\frac{\pi}{2})$, reduced (50%), and cropped (50%) images of water mark versions from the left side to the right side respectively for the image 1 and 2. From the robustness results of our watermarking system, it can be said that our watermarking system has the robustness against filtering and geometric modifications.

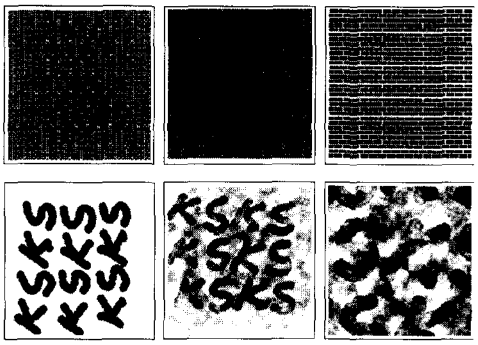


Fig. 9 Extracted versions from geometrically modified versions

6. Conclusion

A new watermarking technique by Fresnel transform is proposed and experiments are done resulting in confirming the validity of the proposed technique with some types of images as watermark images. To vary our method is further subject to study in order to extend the proposed technique to the public watermarking system. From the experimental results, it can be said that our technique using Fresnel transform has a possibility to embed image data in watermarking process. Also the extracting results from the some types of modified images show that our method has the resistance to lossy compression like JPEG, filtering and geometric transformation, because even though the values of typical regions are changed it is possible to reconstruct with remained components of Fresnel-transformed pattern.

It is difficult to comment on our system with other watermarking systems directly, 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 attacks[10]. 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] 김형중, "스테가노그라피의 이론적 배경과 검출기법", 정보보호학회지, 제12권, 제1호, pp.34-47, 2002.

[2] I. J. Cox, J. Kilian, T. Leighton. and T. Shamoon, *"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.

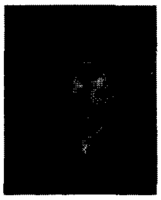
[6] W. L. Tang and Y. Aoki, *"A DCT-based Coding of Images In Watermarking,"* In Proc. of the ICICS'97 Vol.3.

[7] J. Ohnish and S. Ozawa, *"Watermark supports cropping attack via multiresolution analysis,"* Trans. IEICE, Vol.J81-D-2, No.10, pp.2321-2329, 1998.

[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. Ohnish and K. Matsui, *"Image coding for copyright protection by using wavelet,"* Trans. of IPSJ, Vol.38, No.3, pp.534-539, 1997.



Kang Seok
received B.E. degree from Soongsil University, Seoul, Korea, in 1994, and M.E. and ph.D degrees in Electronic Information Engineering from Hokkaido University, Sapporo, Japan, in 1997 and 2000, respectively. He is now a lecturer of School of Electrical & Computer Engineering at Chungbuk National University. He is currently engaged in research on image processing, 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