Fresnel 변환 패턴의 삽입에 의한 컬러 이미지 워터마킹 기법

A Color Image Watermarking Technique by Embedding a Fresnel-Transformed Pattern

이창조*, 강 석**

우송대학교 게임멀티미디어학과*, 북해도대학 정보과학연구과**

Chang-Jo Lee(cjlee@wsu.ac.kr)*, Seok Kang(kssrh@mcm.ist.hokudai.ac.jp)**

요약

디지털 워터마킹은 이미지, 사운드와 같은 멀티미디어 데이터에 지각할 수 없도록 비밀 정보를 삽입하는 기법이다. 일반적으로 주파수 영역 워터마킹 기법에서는 원 이미지에 대해 주파수 변환을 하고, 그 변환 면에 부호화된 워터마크 데이터를 삽입한다. 본 논문에서 우리는 Fresnel 변환을 이용한 새로운 컬러 이미지 워터마킹 기법을 제안한다. 워터마크 이미지를 Fresnel 변환시켜 얻은 패턴의 값들을 컬러 이미지에 삽입한다. 본 워터마킹 모델은, 컬러 이미지에 대한 워터마크 삽입을 위해 원 이미지를 RGB 성분에서 YCrCb 성분으로 분해를 한 후 Y 성분에 워터마크 이미지의 Fresnel 변환된 패턴의 실수와 허수 값을 삽입하는 기법이다. 제안된 기법의 유효성을 검증하기 위한 워터마크 삽입 추출 실험 결과 유효성을 입증할 PSNR 값을 나타냈으며, 또한 JPEG와 같은 손실 압축 공격에 대해 내성을 지니고 있음을 보였다.

■ 중심어 : | 워터마킹 | 퓨리에 변환 | Fresnel 변환 | 데이터 삽입 |

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 color image watermarking technique using Fresnel transform. A watermark image is Fresnel-transformed and the intensity of transformed pattern is embedded into color image. In our watermarking model, an original image is converted from RGB components into YCrCb components and then the values of real number and imaginary number of a Fresnel-transformed pattern of a watermark image are embedded into Y component. The watermarking experiments were conducted to show the validity of the proposed method using PSNR value, and the results show that our method has the robustness against lossy compression like JPEG.

■ keyword : | Watermarking | Fourier Transform | Fresnel Transform | Data Embedding |

접수번호 : #060613-002

접수일자 : 2006년 06월 13일

심사완료일 : 2006년 06월 27일

교신저자 : 이창조, e-mail : cjlee@wsu.ac.kr

I. 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* 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 requantization, 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 based methods are proposed [3-7]. 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 color image watermarking technique based on the former grey-scaled image watermarking technique[8] to recover the weak points of [9](needs extra imaginary number data to extract watermark 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 show the validity of our method. We provide conclusion in Section 5.

II. 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.

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[10].

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

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].

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

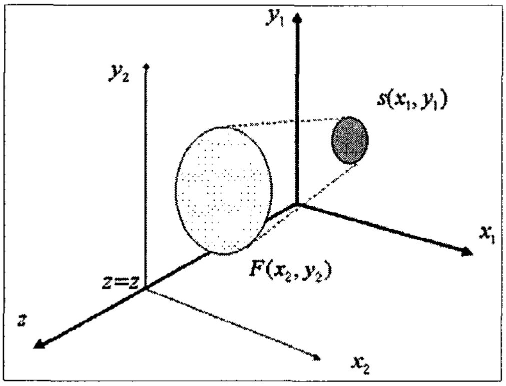


Fig. 1. Fresnel transform of a 2-D model

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 $p(x, y)$.

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

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.

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

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

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

where μ and ν are spatial frequencies. The calculation of numerical Fresnel transform 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:

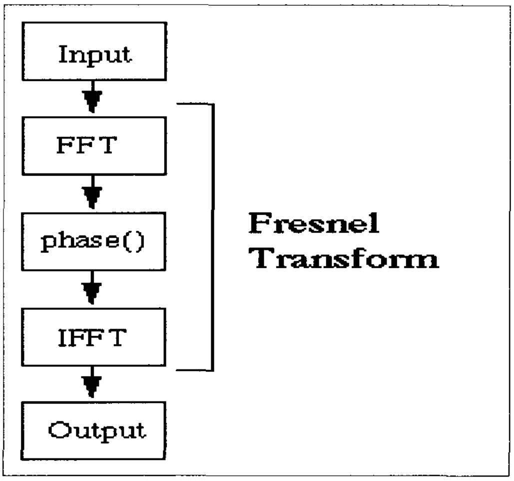


Fig. 2. The flow of calculation of Fresnel transform

$$F(x_1,y_1) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s(x_2,y_2)\exp[-\frac{j\pi}{D}[(x_1-x_2)^2 + (y_1-y_2)^2]]dx_1 dy_1 \quad (6)$$

2. Fresnel Transform of Image

If z in Eq.(2) becomes smaller, the distance parameter D approaches 0, and the value of exp $[j\pi iD(\mu^2+\nu^2)]$ 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.

III. Watermarking using Fresnel Transform

We propose a color image watermarking technique by embedding both data real number and imaginary number of Fresnel-transformed pattern of a watermark image into original image, and it is based on the former technique[8]. Our watermarking system, diagrammed in [Fig. 3], is a watermarking scheme having characteristics of spatial domain method and frequency domain method. In [Fig. 3], Re and Im 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 technique just transformed pattern of watermark data is embedded.

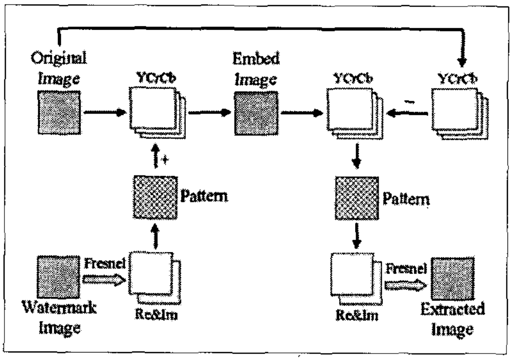


Fig. 3. Watermarking system block diagram

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.

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:

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 $m=2n$.

Embedding calculation formula :

Selection of $D_{embedding}$:

$$W' = Fresnel(W, D)$$
$$W' \in (R_{nm}, I_{nm})$$
$$W'_{code} \in (A, B)$$
$$E = O + (W'_{code}) * w$$

where

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

W' : Fresnel-transformed pattern of watermark image;

R_{m} : real number data of W';

I_{m} : imaginary number data of W';

A : an embedding data block consists of R_{nm} and I_{nm}

$$A = n\overset{2n}{\begin{pmatrix} R_{11}I_{11} & \cdots & R_{1(n/2)}I_{1(n/2)} & R_{1(n/2+1)}I_{1(n/2+1)} & \cdots & R_{1n}I_{1n} \\ I_{21}R_{21} & \cdots & I_{2(n/2)}R_{2(n/2)} & I_{2(n/2+1)}R_{2(n/2+1)} & \cdots & I_{2n}R_{2n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ R_{n1}I_{n1} & \cdots & R_{n(n/2)}I_{n(n/2)} & R_{n(n/2+1)}I_{n(n/2+1)} & \cdots & R_{nn}I_{nn} \end{pmatrix}}$$

B : an embedding data block consists of R_{nm} and I_{nm}

$$B = n\overset{2n}{\begin{pmatrix} R_{1(n/2+1)}I_{1(n/2+1)} & \cdots & R_{1n}I_{1n} & R_{11}I_{11} & \cdots & R_{1(n/2)}I_{1(n/2)} \\ I_{2(n/2+1)}R_{2(n/2+1)} & \cdots & I_{2n}R_{2n} & I_{21}R_{21} & \cdots & I_{2(n/2)}R_{2(n/2)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ I_{n(n/2+1)}R_{n(n/2+1)} & \cdots & I_{nn}R_{nn} & I_{n1}R_{n1} & \cdots & I_{n(n/2)}R_{n(n/2)} \end{pmatrix}}$$

w : embedding parameter;

O : original image;

E : embedded image;

W_{code} : embedding pattern coded into original image and having the structure as shown in the left side of [Fig. 4], and the right side of [Fig. 4] shows the real pattern embedded into an original image(in the case of letter F model);

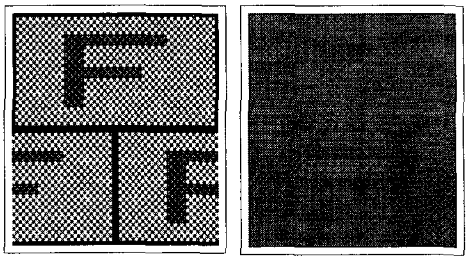


Fig. 4. An example of structure embedded data block and its real pattern embedded into original image

Extracting calculation formula :

Selection of $D_{extraction}$:

$$W'_{code} = (E - O)/w$$
$$W'_{code} \in (A', B')$$
$$A' \text{ or } B' \in (R'_{nm}, I'_{nm})$$
$$W' = InvFresnel(R'_{nm}, I'_{nm})$$

where

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

w : embedding parameter;

O : original image;

E : embedded image;

W'_{code} : extracted embedding pattern;

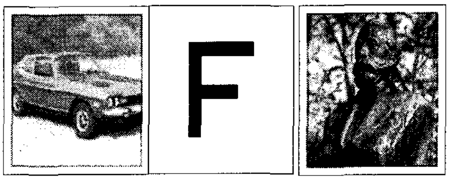
A', B' : an extracted embedding data block and has same structure as A B

R'_{nm}, I'_{nm} : real number data and imaginary number data from A' or B' for inverse Fresnel transform;

W'' : extracted watermark image;

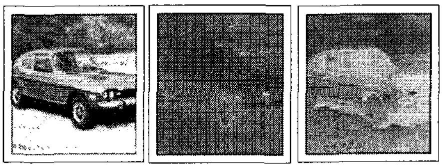
IV. Embedding and Extraction Results

In order to confirm the validity of the proposed method, we implemented the some experiments with a color image as an original image and a letter and photo image(as watermark data) as shown in [Fig. 5]. 256×256(24 bits color) and 128×128(8 bits binary and grey-scaled levels) sampling points are chosen for an original image and watermark images respectively and also [Fig. 6] shows the results of conversion of RGB components into YC_rC_b components.



(a) Original (b) Mark A (c) Mark B

Fig. 5. Original image and watermark images.



(a) Y (b) Cr (c) Cb

Fig. 6. Conversion of RGB into YC_rCb.

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.*

1. Embedding and extraction results

Our experiments are performed by changing the values of two parameters w and D The upper side of [Fig. 7] shows the watermarking versions of original image, where the distance parameters are chosen as $D_{embedding} = 0.1$ for the Mark A and B from left to right respectively and embedding parameter is chosen as $w = 0.05$ for all experiments. The lower side of [Fig. 7] shows the extracted images from watermarked versions, where the distance parameters are chosen as $D_{extraction} = -0.1$·

Fig. 7. Watermarked versions and extracted versions with distance parameter D = 0.1 and w = 0.05.

The PSNR performance of embedding and extracting results at several distance parameters D are given in [Table 1] and [Table 2] for the Mark A and B, respectively(The value of w is fixed as 0.05).

Table 1. Embedding and extraction results with mark A.

D	0.00	0.01	0.05	0.10	0.50
embed	30.15	30.01	30.08	29.60	29.68
extracted	25.06	26.45	25.37	35.92	33.54

Table 2. Embedding and extraction results with mark B.

D	0.00	0.01	0.05	0.10	0.50
embed	36.74	36.90	36.97	36.00	36.17
extracted	26.88	25.32	24.89	32.92	32.11

Also, [Table 3] and [Table 4] show the PSNR performance of embedding and extracting results changing the values of embedding parameter w ($D=0.50$).

Table 3. Embedding and extraction results with mark A.

w	0.010	0.025	0.050	0.075	0.100
embed	43.40	35.72	29.68	26.15	23.65
extracted	20.40	27.70	33.54	36.48	38.12

Table 4. Embedding and extraction results with mark B.

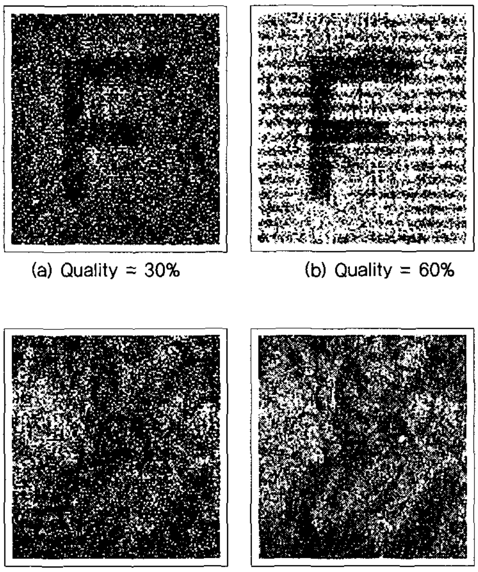
w	0.010	0.025	0.050	0.075	0.100
embed	48.98	42.07	36.17	32.65	30.15
extracted	18.81	26.28	32.11	35.46	37.84

From the [Table 1] and [Table 2], we can find out the fact the parameter D has less influence on the quality of embedding and extraction results(maximum difference value is within 1 in the case of embedding). 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 chosen is depend on the sampling condition of numerical Fresnel transform, and its condition is $D \leq N$ (where N is the sampling numbers)[10].

2. Robustness against JPEG 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. 8] shows the robustness about image compression by JPEG ($D=0.1, w=0.05$).

The result of [Fig. 8] shows that Mark A is stronger than Mark B against JPEG compression attack, because binary image has high contrast.



(a) Quality = 30% (b) Quality = 60%

(c) Quality = 70% (d) Quality = 90%

Fig. 8. Extracted images from compressed images

By the comparison with the results of [9], the quality of extracted image against JPEG attack is lower than the case of [9] using perfect imaginary data in extraction process. But it doesn't need to use extra data for extraction watermark data in this technique, and even though extracted image is rough, we can recognize "What it is" because of the redundancy of the image.

V. Conclusion

A new color image 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 binary and multi-scaled images in embedding process. Also the extracting results against JPEG compression show that our method has the resistance to lossy compression like JPEG, 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 or impossible to embed an image as watermark data in frequency domain methods because of low robustness against attacks[11]. 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.

참고문헌

[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, 1996.

[5] A. G. Bors and I. Pitas, "Image Watermarking Using DCT Domain Constraints," In Proc. of the ICIP'96, Vol.3, 1996.

[6] W. L. Tang and Y. Aoki, "A DCT-based Coding of Images In Watermarking," In Proc. of the ICICS'97 Vol.1, 1997.

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

[8] Seok Kang and Yoshinao Aoki, "Image-Data Watermarking by Embedding a Fresnel-Transformed Pattern," 映像情報メディア學會論文誌, Vol.54, No.5, pp.709-716, 2000.

[9] Seok Kang and Yoshinao Aoki, "Digital Image Watermarking by Fresnel Transform and Its Robustness," In Proc. of the ICIP'99, 1999.

[10] Y. Aoki, *Wave Signal Processing*, Morikita publisher(Tokyo), 1986.

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

저 자 소 개

이 창 조(Chang-Jo Lee) 정회원

- 1989년 2월 : 인하대 전자계산
- 1991년 2월 : 인하대 대학원 컴퓨터과학전공
- 1994년 2월 : 고려대 대학원 컴퓨터과학전공
- 1990년 11월~1994년 2월 : 한국과학기술연구원/시스템공학 연구소(KIST/SERI) 소프트웨어공학연구부 선임연구원(현, 한국전자통신연구원)
- 1994년 3월~1996년 2월 : 한국문화예술진흥원 문화정보사업본부 선임연구원
- 1996년 3월~현재 : 우송대학교 게임멀티미디어학과 교수
- 2004년 7월~현재 : 첨단영상게임산업전문인력양성(NURI) 사업팀장
- 2005년 8월~현재 : (재)한국게임산업개발원 대전게임아카데미 원장
- 2006년 1월~현재 : 대전광역시 정보화추진위 위원

<관심분야> : 게임기획, 컴퓨터그래픽, 디지털콘텐츠

강 석(Seok Kang) 정회원

- 1992년 2월 : 숭실대 전자계산
- 1997년 3월 : 북해도대학 대학원
- 2000년 9월 : 북해도대학 대학원 전자정보공학전공박사
- 2001년 4월~2003년 2월 : 충북대 BK21 사업단 초빙 전임강사
- 2003년 4월~현재 : 일본 북해도대학 대학원 정보과학연구과 조교수
- 2006년 4월~현재 : 우송대학교 게임멀티미디어학과 객원교수

<관심분야> : 정보보호, 디지털콘텐츠, 컴퓨터그래픽