정당한 소유권 보호를 위한 DWT와 SVD기반의 디지털 워터마킹에 대한 연구

구대욱, 한수영, 이동규, 이두수
한양대 전자통신전파공학
전화 : 02-2290-0358 / 핸드폰 : 011-216-0796

A Study on SVD&DWT -based watermarking for protecting rightful ownership

Abstract

Digital watermarking is technique, which owner's information is inserted in digital image, with intention to protecting a copyright of digital image. In watermarking for copyright and authentication, watermark shouldn't be distorted or disappeared after general image processes like a compression and filtering. In this paper, we present a new digital image watermarking algorithm which combines the discrete wavelet transform (DWT) and the singular value decomposition (SVD). Simulation results show that the newly proposed algorithm is not only robust nevertheless variable attacks like noise, filtering and JPEG compression but also secure in application.

I. 서론

통신기술의 발달에 더불어 인터넷의 속도증가와 함께 기업내에서의 각종 OA(Office Automation)군을 이용한 업무의 디지털화가 이루어지고 있다. 기업 내에서 문서, 이미지, 서명 및 여러 가지 중요정보의 전송과 공유시 이러한 자료들의 보안문제를 해결하기 위해 여러 가지 방법들이 제공되고 있다. 이들 중 워터마킹은 자료의 유출, 복제 및 조작으로부터의 보안을 위해서 디지털 내용물 내부에 특정 정보를 은닉하여 데이터를 공유하는 방법으로 Steganography와 유사하게 정보를 은닉하기 위해서 내용물에 직접 부가적인 정보를 숨기는 방법으로 Steganography에 부가적인 견고성이 요구된다.

워터마킹은 일반적으로 은행이나 관공서의 문서, 법률 문서, 병원의 각종 임상 사진 등의 '원본 보호 및 증명'으로써 원본데이터의 보안과 관련된 신뢰성을 보장하거나 인터넷 컨텐츠의 저작권 보호를 위해 사용되어지고 있다.

삽입된 워터마크는 다음의 특징을 가져야 한다.

(1) 원본신호(host signal)에 삽입되어 질 때 눈에 띄지 말아야 한다.

(2) 저자권자의 워터마크 추출은 용이해야 하며, 또한 추출된 워터마크는 신뢰성을 주어야 한다.

(3) 불법적인 워터마크 추출이 불가능해야 한다.

(4) 적용에 따라서 필터링, 압축, 외부잡음인가, 기하학적 변형 등의 신호왜곡에 강인하거나 또는 깨지기 쉬워야 한다.

본 논문에서는 정지영상의 정당한 소유권 보호를 위해, DWT에 의해 주파수로 변환된 영역에서 SVD(Singular Value Decomposition:특이치분해)를 사용하여 강인한 워터마크를 삽입한다.

II. 제안된 워터마킹 기법

원본영상을 DWT를 사용하여 N 스케일 레벨로 분

해한다. 분해된 영상의 근사화 영상을 포함한 M레벨(M<N)이하의 저주파 대역의 웨이블릿 계수들을 선택하여 워터마크 삽입에 사용한다.

일반적으로 DWT를 사용한 워터마크 알고리듬에서는 화질의 열화를 막기 위해 근사화 영상을 제외한 나머지 고주파 부대역에 워터마크를 직접 삽입한다.

제안한 방법은 특이치분해를 사용하여 웨이블릿 계수들을 분해 후 워터마크를 삽입하므로, 근사화 영상을 사용하여도 화질의 열화를 막을 수 있다. 그리고 저주파 대역에 워터마크를 삽입함으로써 low-pass filtering에 대해 강인하다는 장점을 지닌다.

2.1 워터마크의 삽입

단계 1 : 선택된 웨이블릿 계수들을 $A \in F^{N\times N}$ (F: 실수 와 복소수 모두를 포함)라 놓으면, A의 특이치 분해는 다음과 같다.

$$A = X \wedge Y^T = \sum_{i=1}^{r} \lambda_i X_i Y_i^T \qquad (1)$$

(X,Y : $N\times N$ orthogonal matrices, $\wedge$: $N\times N$ diagonal matrix, λ_i : A의 SV(singular value))

A는 편의상 정사각행렬이라 가정하였지만, 정사각행렬이 아닌 경우에도 똑같은 방법으로 적용이 가능하다. 이것은 특이치분해가 지닌 장점의 하나이다.

단계 2 : 구해진 $\wedge$에 워터마크 $W \in F^{N\times N}$ 를 더한 후 이를 특이치분해 한다.

$$\mathbf{T} = \wedge + \alpha W, \qquad T = X_W \wedge_W Y_W^T \qquad (2)$$

(α : 삽입강도)

λ_i 의 미세한 변화가 원본 이미지에 미치는 영향은 시각적으로 확연히 드러나지 않는다.

$\wedge$ 와 X_W, Y_W 는 워터마크 추출을 위해 저장해 두어야 한다.

단계 3 : $\wedge_W$ 와 X,Y를 사용해 워터마크가 삽입된 웨이블릿 계수를 구한다.

$$A_W = X \wedge_W Y^T \qquad (3)$$

단계 4 : 워터마크가 삽입된 웨이블릿 계수들과 사용되지 않은 나머지 웨이블릿 계수들로 IDWT를 사용하여 영상을 복원한다.

2.2 워터마크의 추출

위에 설명된 워터마크 삽입 과정을 역행함으로써 워터마크(W^*)를 추출 할 수 있다.

$$A_W^* = X^* \wedge_W^* Y^{*T}$$

(A_W^*: 훼손된 영상에서 선택된 웨이블릿 계수들)

$$D^* = X_W \wedge_W^* Y_W^T$$

$$W^* = \frac{1}{\alpha}(D^* - \wedge) \qquad (4)$$

2.3 워터마크의 위조와 소유권의 보호

2.3.1 만약 부적절한 사용자가 워터마크 혹은 원본 이미지를 추출하고자 한다는 것은 워터마크에 일정한 제한 조건을 걸어둘 경우 계산상 실행 불가능한 일이 된다.

a) $\wedge_W$만 알 경우, 즉 (3)의 A_W만 알고 있는 경우
: (2)에 대입하여도 $\wedge$와 W의 유일해를 구할 수 없어 원본이미지와 원래의 워터마크를 구할 수 없다.

b) $\wedge_W$와 $\wedge$만 알 경우, 즉 원본이미지 까지 알고 있는 경우
: (2)는 N^2개의 미지수를 지닌 다항식이 되지만, 알고 있는 constraints는 2N개이므로 원래의 워터마크를 구할 수 없다.

c) $\wedge_W$ 와 W를 알 경우, 즉 원래의 워터마크만 알 경우
: 이 경우 (2)의 $\wedge$의 유일해를 구할 수 있다. 하지만, (1)의 X,Y는 $\wedge$에 대한 고차원이면서 복잡한 비선형 문제이다. 때문에 $\wedge$를 구하기는 실제적으로 아주 어려운 일이 된다. 따라서 원래의 이미지를 구하는 일 또한 어렵다.

2.3.2 만약 워터마크에 일정한 제한 조건을 걸어둘 경우, 부적절한 사용자가 위조된 워터마크를 삽입하고자 하는 것은 아주 힘든 일이 된다.

a) 원래의 워터마크가 삽입된 영상 A_W만 가지고, 부적절한 사용자가 삽입하기를 원하는 위조된 워터마크 W_F로 원본이미지를 구하는 것은 아주 어렵다. 2.3.1 (a)와 같은 경우이다. 원본 이미지가 없기에 설사 위조된 워터마크를 삽입한다 한다 해도, 추출을 할 수가 없다.

b) $\wedge_W$와 $\wedge_F$를 알 경우, 즉 $\wedge_W$에 임의의 조작을 가해 $\wedge_F$로 만들 경우, $\wedge_F$에 종속적인 W_F를

쉽게 구할 수 있다.

$$X \wedge_W Y^T = XX^T_{F,W}(\wedge_F + \alpha W_F) Y_{F,W} Y^T$$

$$\wedge_W = X^T_{F,W}(\wedge_F + \alpha W_F) Y_{F,W}$$

$$U_{F,W} S_W V^T_{F,W} = S_F + \alpha W_F \quad (5)$$

하지만 W_F에 일정한 제약을 부여한다면, 반대로 W_F에 종속적인 $\wedge_F$를 만들기는 사실상 불가능하다.

III. 실험 결과

제안된 알고리듬의 지각적 비가시도와 강인함을 확인하였다. 본 방법은 Cox에 의해 제안되 "Spread Spectrum Communication method"와 비교를 하였다. 사용된 DWT는 선형위상 9/7 필터를 사용하였고, 삽입강도는 α=0.3 이었다.

그림 1은 256×256Lena영상에 제안된 알고리듬을 사용하여 워터마크를 삽입한 결과를 보여준다. 그림 1.(c)는 원본이미지와 워터마크가 삽입된 이미지간의 절대오차를 뚜렷이 보여주기 위하여 64배의 스케일링을 하였다. 사용된 워터마크는 각종 이미지 처리에 대한 강인함을 보여주기 위하여, 그림 1.(d) 의 64×64 크기의 시각적 워터마크를 사용하였다.

지각적 비가시도는 원본 영상과 위에 설명된 가시적 워터마크를 삽입한 영상간의 PSNR(Peak Signal to Noise Ratio)를 계산하여 나타내었다. 제안된 방법의 PSNR은 45.0dB이었고, Cox의 방법의 PSNR은 41.43dB였다. Cox의 방법에 비해 비가시성에서 뛰어남을 알 수 있다.

그림 2는 Lena영상에 제안된 알고리듬을 사용하여 워터마크를 삽입한 후 각종 이미지 처리에 대한 강인함을 보여준다. (a)는 16×16 가우시안 low-pass filter를 거친 영상이다. (b)는 워터마크가 삽입된 후 평균이 0이고 분산이 0.05인 AGWN가 첨가된 영상이다. (c)는 왼쪽 절반이 제거된 영상이다. (d)는 JPEG 압축을 거쳐 JPEG 압축 퀄러티가 5인 영상이다. (e~h)는 각 영상에서 추출한 워터마크 로고이다. (e)와 원 워터마크의 상관도는 0.2473, (f)와 원 워터마크의 상관도는 0.5287, (g)와 원 워터마크의 상관도는 0.2606, (h)와 원 워터마크의 상관도는 0.9879 이다.

Cox의 방법으로 위와 동일한 과정을 거쳐 워터마크의 유사도를 측정하였다. (a~d)에 대응된 추출 워터마크의 유사도는, 0.11, 0.06, 0.08, 0.05, 0.10 로 나타났다. 이는 본 논문에서 제안된 방법이 가시적 워터마크 삽입과 추출에 있어서 Cox의 방법에 비해 월등함을 나타낸다.

이러한 실험 결과는 워터마크로 삽입된 로고(logo)가 각종 이미지 처리를 거친 후에도 추출 후 충분히 시각적으로 판별이 가능함을 알 수 있다.

IV. 결론

본 논문은 정지영상의 정당한 소유권을 보호하기 위하여 강인한 워터마크를 삽입하는 기법을 제안하였다. 제안된 기법은 기존의 워터마킹 알고리듬들이 크로핑(cropping)과 같은 영상의 물리적 손실에 상당히 취약한 단점을 상당부분 개선하였고, 다른 일반적으로 사용되는 이미지 처리에 있어서도 강인함을 보여주었다.

하지만, 최근의 기법들에 비해서는 영상의 훼손 정도가 조금 더 큰, 워터마킹의 비가시성을 해결해야 하는 문제가 남아있다. 그리고 워터마크의 위조를 막기 위해 워터마크에 걸어야 할 제약 조건에 대한 좀 더 구체적인 연구가 필요하다.

참고문헌

[1] S. Katzenbeisser, "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House.

[2] W. Bendor, D. Gruhl and N. Morimoto "Techniques for Data Hiding," Proc. SPIE, Feb. 1995

[3] Ingemar J. Cox, F. Thomson Leighton, and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," Image Processing, IEEE Trans. on, Dec, 1997

[4] Harry C. Andrews and Claude L. Patterson, "Singular Value Decomposition(SVD) Image Coding," Communications, IEEE Trans. on, Apr. 1976

[5] Ruizhen Liu and Tieniu Tan,"An SVD-Based Watermarking Scheme for Protecting," Multimedia, IEEE Trans.on, Mar. 2002

[6] A. B. Watson, G Y. Yang, J. A. Solomon, and

J. Villasenor, "Visibility of wavelet quantization
nosie," Image Processing, IEEE Trans on, vol 6, pp.
1164-1175, 1997
[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon,
"Secure spread spectrum watermarking for multimedia,"
IEEE Trans. Image Processing ,Dec. 1997

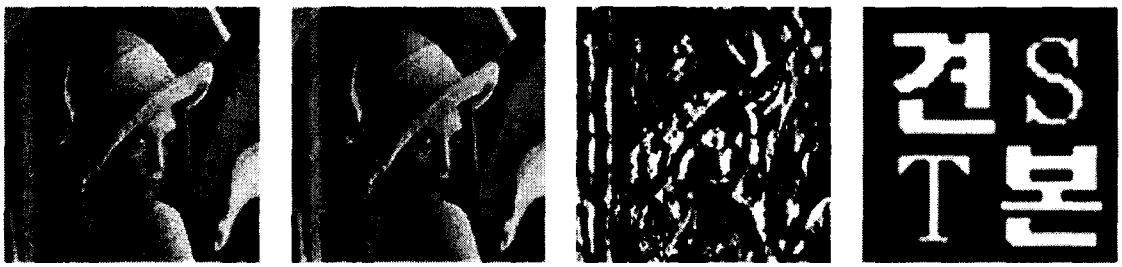

그림 1. (a)"Lena"원본영상, (b)워터마크가 삽입된 영상, (c)원본영상과 워터마크가 삽입된 영상과의 절대 에러값 영상, (d)삽입된 시각적 워터마크

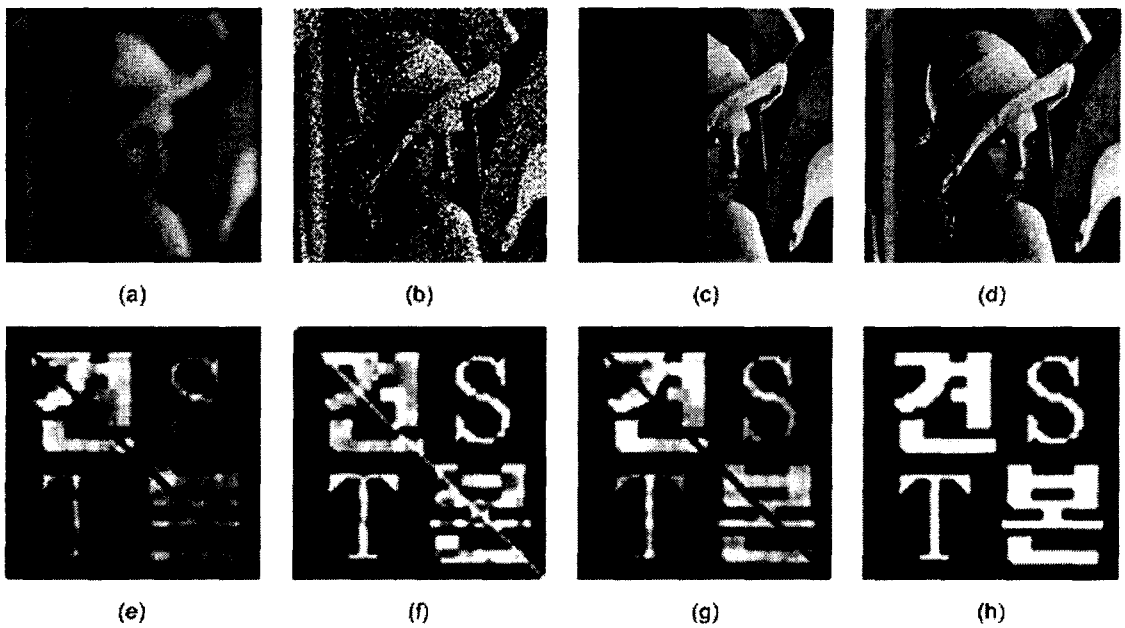

그림 2. 그림 1.(b)의 워터마크가 삽입된 영상에 (a)16×16가우시안 low-pass filtering한 이미지, (b)평균이 0이고 분산이 0.05인 AGWN첨가한 이미지, (c)좌측 절반이 없어진 이미지, (d)손실율 95% JPEG압축을 거친 이미지와, (e-h)각 이미지에서 추출한 워터마크 로고