HVS 기반 워터마킹에서 외부 공격에 강인한 방법에 관한 연구

심상흔, 정용주, 강호경, 노용만
한국정보통신대학원대학교 멀티미디어정보통신그룹
{ssheun, yro}@icu.ac.kr

A ROBUST WATERMARKING METHOD BASED ON HVS

Sang-Heun Shim Yong-Ju Jung Ho-Koung Kang Yong Man Ro
School of Engineering, Information and Communications University (ICU)

Abstract

In this paper, we utilize a HVS(Human Visual System) watermarking method where watermarks are embedded in a DFT domain. The HVS watermarking method is robust for attacks like JPEG, filtering, noise, etc. But, when images are attacked by basic geometric attacks as cropping, scaling, rotation, a watermarks may not be detected. In this paper, we introduce the HVS watermarking method that inserts references in a domain of LSB(Least Significant Bit) of image. Experimental results show that the proposed method based on HVS watermarking method gives more robustness to the basic geometric attacks compared with original HVS watermarking methods.

I. 서론

최근 인터넷의 급속한 확산 속에서 디지털 영상물의 불법 복제로 인한 소유권 문제가 중요하게 인식되고 있다. 이에 대한 해결책으로, 멀티미디어 데이터에 대한 소유권을 효과적으로 보호하고, 데이터의 불법 복제 및 배포를 제한할 수 있는 디지털 워터마크 기술이 활발히 연구되고 있다.

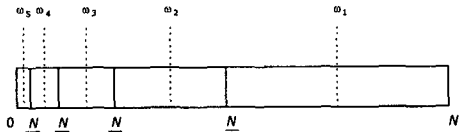
본 논문은 휴먼 비주얼 특성을 이용하여 DFT 영역에 워터마크를 삽입하는 HVS 워터마킹 방법을 바탕으로 한다[10]. HVS 워터마킹 방법은 공간 주파수 영역에서 각 밴드의 정보량에 따라 중요한 부분에 많은 워터마크를 삽입한다. 그리고, 이 방법은 휴먼 비주얼 특성을 이용함으로써 기존의 방법보다 압축, 필터링, 노이즈 등의 여러 공격에 강인함을 보인다. 그러나, 기본적인 기하적 공격인 크로핑, 스케일링, 회전 변환 후 워터마크 검출률이 현저히 떨어진다. 그래서, 본 논문은 영상의 LSB 영역에 기준영역을 삽입하여 크로핑, 스케일링, 회전 공격에 강인한 HVS 워터마킹 방법을 제시한다.

본 논문의 구성은 다음과 같다. II장에서 HVS 특성을 이용한 DFT 영역에서 워터마크 삽입 및 검출 알고리즘에 대해 기술하고, III장에서 LSB 기준영역을 이용하는, 기하적 공격에 강인한 워터마크 검출 알고리즘을 제시한다. 그리고, IV장에서 실험 방법과 결과를 보인다. 마지막으로 V장에서 본 논문의 결론을 맺는다.

II. HVS 워터마크 삽입 및 검출

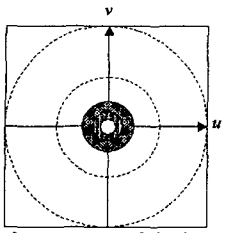
2.1 워터마크 삽입을 위한 HVS 구조

정신물리학을 통해 이제까지 알려진 가장 적절한 공간 주파수 분할은 각도 방향과 방사 방향을 기본 축으로 하며[9], 공간 주파수 영역에서 각도 방향으로는 동일한 각도 폭으로 180도의 전 각도 영역을 5~6개로 분할하고, 방사방향에서는 전체 주파수영역을 4~5개의 옥타브 밴드로 분할한다[8].



[그림 1] 방사방향으로 채널분할

이렇게 분할된 공간 주파수 영역은 [그림 2]와 같다. [그림 2]에서 보듯이, HVS 채널은 저주파 영역에서 조밀한 채널들로 구성되고 고주파 영역에서는 상대적으로 넓은 영역의 채널들로 구성된다. 즉, 시각 특성은 저주파 성분의 변화에 민감하고 고주파 성분의 변화에 둔감하다. 본 논문에서, 이러한 채널 특성에 기반하여 [그림 2]에 표시된 두 밴드에 워터마크를 효과적으로 삽입 및 검출한다.



[그림 2] HVS 주파수밴드분할

2.2 워터마크 삽입 알고리즘

본 논문에서 워터마크는 평균이 0인 1 또는 □ 1로 구성되며 DFT영역에 삽입된다. N x M 그레이스케일 원영상 I의 퓨리어 변환은 식(1)과 같다.

$$F(u,v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\exp\left[-j2\pi(ux/M+vy/N)\right] \quad (1)$$

$f(x,y)$가 실수이면 Fourier 변환은 공액대칭(conjugate symmetry)의 특성을 가지게 된다. 여기서 $F^*(u,v)$는 $F(u,v)$의 복소공액(complex conjugate)이다.

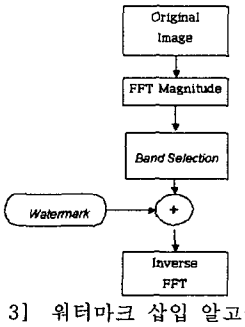
$$F(u,v)=F^*(-u,-v) \quad (2)$$

이러한 특성으로 인해 변환 영역에서 대칭적으로 워터마크가 삽입된다. $M(u,v)$는 I의 퓨리어 변환 진폭(Magnitude)이고, $W(u,v)$는 워터마크이다.

본 논문에서 사용된 워터마크 삽입 알고리즘은 [그림 3]과 같다. [그림 3]의 밴드선택 부분에서 워터마크 삽입 위치를 결정한다. 이렇게 선택된 위치에 식(3)을 이용해 워터마크가 삽입된다. 식 (3)에서, M`(u,v)는 워터마크가 삽입된 원영상 I의 퓨리어 변환 진폭이다.

$$M'(u,v)=M(u,v)+aW(u,v) \quad (3)$$

식(3)에서, a는 워터마크의 삽입 강도를 조절하는 스케일 팩터로 기본값은 0.3이다. 각 밴드별로 이 값을 조절함으로써 이미지의 화질 저하와 워터마크의 강인함을 적절히 절충할 수 있다. HVS에 따른 주파수밴드 분할에 의해 분할된 각 밴드에 비슷한 개수의 워터마크를 삽입함으로써 [그림 2]에서 결과적으로 안쪽 즉 저주파쪽에 상대적으로 많은 양의 워터마크가 삽입되는 효과를 가져온다. 이는 공격에도 많은 양의 정보가 살아 남게 되므로 강인함의 요구조건을 충족한다.



[그림 3] 워터마크 삽입 알고리즘

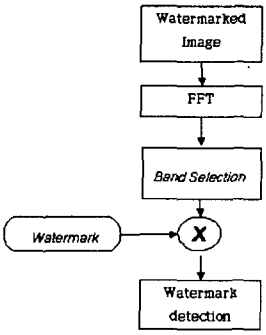
2.3 워터마크 검출

워터마크 검출은 원영상을 필요로 하지 않으며, 그 과정은 [그림 4]와 같다.

워터마크 검출을 위한 유사도 측정은 밴드 내에서 워터마크가 삽입된 위치의 진폭 M`과 워터마크 W와의 상관계수(correlation coefficient) c를 통해 구하게 된다. 이 과정은 식(4)와 같다.

$$c=\frac{1}{L}\sum_{u=1}^{N}\sum_{v=1}^{N}W(u,v)M'(u,v) \quad (4)$$

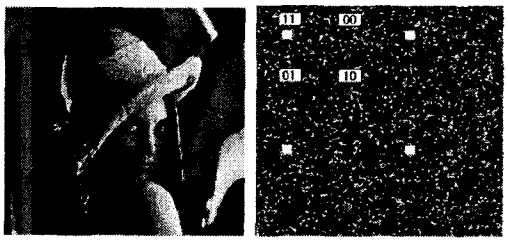
본 논문에서는 [그림 2]에서 안쪽 저주파를 제외한 두개의 표시된 밴드만 워터마크를 삽입하고 검출하는데 이용했다. 물론, 스케일 팩터를 조절해서 나머지 밴드에도 워터마크를 삽입할 수 있다.



[그림 4] 워터마크 검출 알고리즘

III. 기하적 공격에 대한 워터마크 검출

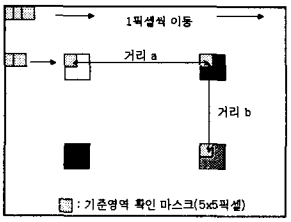
기하적 공격에 대한 워터마크 검출을 위해서, 워터마크 삽입 시 256 x 256 블록의 공간 영역에 4개의 기준영역을 삽입한다. 기준영역은 픽셀 위치 (64,64), (64,192), (192,64), (64,192)을 중심으로 가로, 세로 20 픽셀의 정사각형 영역에 LSB 2비트의 값이 11, 01, 00, 10이 되게 함으로써 형성된다. [그림 5]는 가시성을 위해서 각 픽셀의 LSB 2bit 값에 80을 곱한 기준영역들을 보인다.



(a) (b)

[그림 5] (a) 워터마크가 삽입된 영상 (b) LSB 영상

기하적 공격에 대한 워터마크 검출을 위해서, 5x5 픽셀의 기준영역 확인 마스크를 [그림 6]과 같이 워터마킹된 영상에 대해서 1픽셀 씩 이동하면서 삽입된 기준영역을 찾는다. 찾아진 기준영역의 크기, 형태, 위치로 가해진 공격을 파악한다.



[그림 6] 기하적 공격에 대한 기준영역 확인

크로핑 공격은 기준영역을 변형시키지 않는다. 그래서, 기준영역의 크기 및 형태가 변화되지 않으면, 워터마킹된 영상에 크로핑 공격이 가해진 것이다. 크로핑 공격에 대한 워터마크 검출은 4개의 원 기준영역이 남아있는 완벽한 256x256 블록들을 찾아 하나씩 워터마크 검출을 실행한다.

삽입된 기준영역의 가로, 세로 길이가 변하면, 영상에 스케일링 공격이 가해진 것이다. 스케일된 영상의 워터마크 검출을 위해서, LSB 2bit의 값이 11, 00, 10인 기준영역 간의 거리 a와 b를 워터마크 삽입 시 기준영역 간의 거리 128로 나눠서 가로, 세로 스케일링비를 구한다. 이 비를 이용해, 영상을 원래의 크기로 복원한 후 워터마크 검출을 실행한다.

$$\text{가로 스케일링비} = a/128 \qquad (5)$$

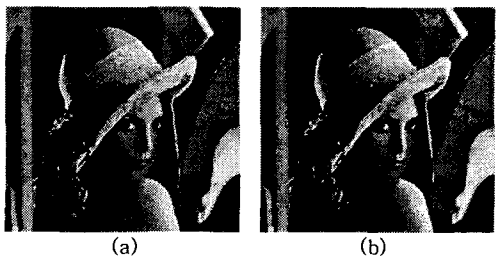
$$\text{세로 스케일링비} = b/128$$

영상에 회전 공격이 가해지면 기준영역 간의 위치가 변한다. 기준영역 간의 위치로 90도 단위의 회전각도를 찾는다. 시계 또는 반시계 방향으로 90도, 270도 회전된 영상은 시계 방향으로 90도 회전시킨 후 워터마크 검출을 실행한다. 180도 회전된 영상은 그대로 워터마크를 검출한다. 이 90도 단위 회전 공격에 대한 워터마크 검출은 DFT 주파수 영역의 대칭성을 이용한다.

IV. 시뮬레이션 및 결과

본 논문에서 제안된 방법을 많은 영상에 실험해 보았다. 실험에 사용된 파라미터들은 N=M=256, 워터마크 길이 L=4816, 여기서 안쪽(Band A)과 바깥쪽(Band B) 밴드에 각각 같은 수의 개수, 그리고 a=0.3이다. [그림 7]은 원영상과 워터마크가 삽입된 영상을 나타내고, [그림 8]은 워터마크가 삽입된 영상의 검출 값을 보인다.

[그림 8]에서 보듯이 삽입된 20번째의 워터마크에서 반응이 옴을 볼 수 있다. 검출 시, 삽입된 워터마크와 20번째의 워터마크의 검출 상관 계수 값이 다른 랜덤 워터마크와의 검출 상관 계수 값보다 40이상 크면, 워터마크가 검출된 것이다. 여기서, 값 40은 실험적으로 정해졌다.



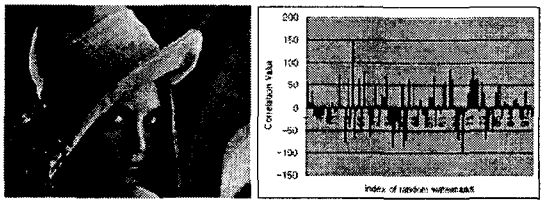
(a) (b)

[그림 7] (a) 원영상 (b)워터마크가 삽입된 영상

[그림 8] 워터마크 검출 상관계수

[표 1] 크로핑 공격에 대한 워터마크 검출

크로핑된 영상의 크기	Lena(768x768)		
	First peak	Second peak	Third peak
768x768(원영상)	162.69	-54.18	-47.22
640x640(중심기준)	148.50	92.59	90.51
512x512(중심기준)	145.73	-95.14	93.35
640x640(임의기준)	147.67	93.58	92.93
640x512(임의기준)	146.54	-94.88	88.49
512x640(임의기준)	146.98	92.73	-89.38
512x512(임의기준)	144.92	94.77	89.25

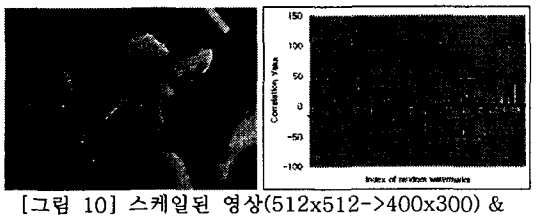


[그림 9] 임의 기준 크로핑(768x768->640x512) & 검출 상관계수

[표 2] 스케일링 공격에 대한 워터마크 검출

스케일된 영상의 크기	Lena(512 x 512)		
	First peak	Second peak	Third peak
256 x 256	147.87	79.90	65.48
384 x 384	157.24	82.62	-67.08
640 x 640	167.86	-111.82	-70.82
768 x 768	183.16	84.68	76.34
896 x 896	176.16	-78.36	-66.30
1024 x 1024	183.16	-79.07	-72.30

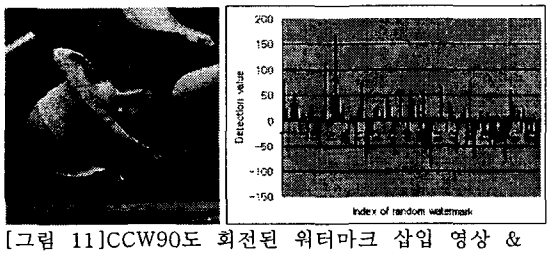
400 x 300	127.35	-65.80	-61.61
480 x 640	155.61	79.81	61.12
640 x 480	156.03	92.87	-61.70
800 x 600	144.52	-82.40	-82.58
1024 x 788	183.16	73.84	70.17



[그림 10] 스케일된 영상(512x512->400x300) & 검출 상관 계수

[표 3] 회전 공격에 대한 워터마크 검출

회전각도	Lena(512x512)		
	First peak	Second peak	Third peak
0도(원영상)	183.16	62.00	-58.06
CW 90도	165.39	114.94	-92.64
CCW 90도	159.80	102.94	-96.88
CW 180도	143.04	93.18	89.77



[그림 11]CCW90도 회전된 워터마크 삽입 영상 & 검출 상관 계수

V. 결론

최근, 디지털 워터마크 기술은 디지털 영상물의 불법 복제로 인한 저작권 및 소유권 문제에 대한 해결책으로 중요하게 인식되고 있다.

본 논문은 휴먼 비주얼 특성을 이용하여 DFT 영역에 워터마크를 삽입하는 HVS 워터마킹 방법의 기하적 공격에 대한 취약성을 해결하기 위해서, 영상의 LSB 영역에 기준영역을 삽입하였다. 그리고, 삽입된 기준 영역의 크기, 형태, 위치의 변화를 이용해, 가해진 기하적 공격을 파악하고, 변형된 영상을 복원하여 워터마크를 효과적으로 검출하였다.

향후 연구과제로 임의의 각도 회전에 의한 기하적 공격에도 워터마크를 검출할 수 있는 방법이 연구되어야 한다[5][6].

참고문헌

[1] I.J.Cox, J.Kilian, F.T.Leighton, and T.Shamoon. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, September 1996.

[2] V. Solachidis and I.Pitas, Circularly symmetric watermark embedding in 2-D DFT domain. IEEE, 1999.

[3] A.Piva, M.Barni, F.Bartolini, V.Cappellini. DCT-based watermark recovering without resorting to the uncorrupted original image. Proceedings of ICIP'97,Santa Barbara, CA, USA, Oct., 26-29, vol. I, pp.520-523, 1997.

[4] Hisashi INOUE, Akio MIYAZAKI, Takashi KATSURA, An image watermarking method based on the wavelet transform. IEEE 1999.

[5] J. O Ruanaidh and T.Pun. Rotation, scale and translation invariant digital image watermarking. In Proceedings of ICIP'97 volume I, pages 536-539, Atlanta, USA, October 1997.

[6] M. Kutter. Watermarking resisting to translation, rotation, and scaling. In Proceedings of SPIE International Symposium on Voice, Video, and Data Communications, November 1998.

[7] M. Kutter, S.K.Bhattacharjee, T.Ebrahimi. Towards Second Generation Watermarking Schemes, In Proceedings of ICIP'99 volume I, pages:320-323, 1999.

[8] J.G. Daugman, High Confidence Visual Recognition of Persons by a Test of Statistical Independence, *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol.15, no.11, pp.1148-1161, November, 1993

[9] J. G. Daugman, Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression, *IEEE Trans. ASSP*, vol.36, pp.1160-1179, July, 1988

[10] 정용주, 강호경, 노용만, 휴먼 비주얼 시스템의 공간 주파수 밴드분할을 이용한 디지털 워터마킹 방법, JCM2000, June, 2000