랜덤한 점분포를 가진 영상을 사용한 워터마킹의 견고성

(A Robustness of Watermarking Using Random Dot Distribute Image)

이 인정*

In Jung Lee

요 약 삽입하려는 암호영상이 원본 전체 이미지 내에 랜덤하게 분포할수록 삽입과 추출성능이 좋아지는데 본 논문에서는 랜덤성이 우수한 오토스테레오그램을 삽입암호영상으로 사용하여 워터마크 하였을 때 복원과 추출성능이 양호함을 알아보았고 이를 이용하여 로고영상을 워터마크하려는 영상의 전 영역에 랜덤하게 고루 분포 하게 하여 워터마크한 후 역으로 변환하여 로고를 찾았다. 영상이 많이 손상되었을 때도 추출된 로고가 육안으로 식별할 수 있을 정도로 견고성이 우수함을 알아보았다.

Abstract In Generally, a imbedding and extracting is good as watermark using a random dot image. In this paper, when the autostreogram which has some randomness is used watermark image, distortion rate is low and extraction rate is high. Using this quality, when any logo image is transformed to same image domain randomly, distortion rate is low and extraction rate is high, more over the robustness is good in spite of hard clipping.

1.서론

정지영상, 오디오, 동영상, 문서 등은 고유성과 독창성 및 원 소유주의 권리가 결여 될 가능성이 매우 크다. 그 이유 중 한 가지가 바로 소유주의 동의 없이 대량의 복사와 무단 배포가 가능한 것이다. 이러한 복사를 방지하는 기술 중에 영상에 암호를 삽입하여 소유권을 주장할 수 있는 기술로 워터마크 기술을 들 수 있다. 워터마크 기술은 텍스트, 이미지, 동영상, 오디오 등의 데이터에 원 소유주만이 알수 있는 마크(Mark)를 삽입하여 사람의 육안이나 청력으로 구별할 수 없게 삽입하여 제공하는 기술을 말한다. 워터마크 삽입 시 다음과 같은 두 가지 경우가 발생한다. 첫째, 많은 양의 데이터를 워터마크로 삽입하게 되면 원 이미지가 깨어지는 현상이 생기고, 이와 반대로 적은 양의 데이터를 워터마크로 삽입하면 워터마크 추출에 문제점이 있다. 둘째, 각종 이미지가 디지털 조작(JPEG압축, MP3 압축 등)에 의하여 삽입된 워터마크가 손상되면, 워터마크를 추출하여 저작권을 주장하는데 문제점이 있기 때문에 이를 원본에 가깝게 복원하는 기술이 절대적으로 필요하다[6,9]. 워터마크를 삽입하는 데 있어서 여러 방법이 제안되고 있으나 그 중에서 가장 널

*호서대학교 컴퓨터공학부 교수

리 사용되고 있는 Cox의 방법은 다음과 같은 방법으로 watermark를 삽입하였다[1,2,10,11].

$$v_i' = v_i + \alpha x_i \quad \text{(식 1)}$$

여기서, $V = \{v_1, v_2, \ldots, v_n\}$

: 원 이미지를 DCT 또는 FFT로 변형한 값.

$$X = \{x_1, x_2, \ldots, x_n\}$$

: watermarking sequence

$$V' = \{v_1', v_2', \ldots, v_n'\}$$

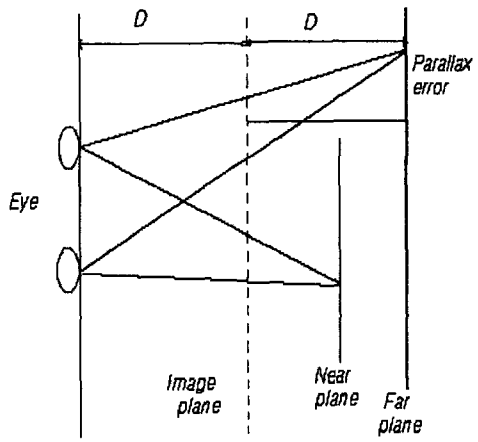
: adjusted sequence

α : scaling parameter

위의 (식 1)에서 파라메타 α의 값을 결정하는데 있어서 원본 데이터의 품질을 유지하면서 워터마크 데이터 추출 시 워터마크 정보 추출의 최대화를 기대할 수 있어야 한다. 본 논문에서는 (식 1)을 사용하였고, watermarking sequence로는 오토스테레오그램 영상을 DCT 변환한 값과 임의의 로고를 변환하여 워터마크하려는 이미지의 전 영역에 고루 분포하도록 만든 영상을 사용하였다[3,4,5]. 본 논문에서는 오토스테레오그램이나 변환된 로고영상이 클리핑에 대해 아주 견고함을 알아보았다.

2. 오토스테레오그램과 포인트 랜덤분포 이미지

여기서 사용한 오토스테레오그램 영상은 우리가 어떤 목표 사물을 볼 때 발생하는 두 눈의 시각적 오차 값을 이용하여 평면의 사물이 마치 입체에 형상이 이루어지는 것처럼 인간의 착시 현상을 말하는 것이다. 이러한 원리는 그림1.에서 보는 바와 같이 두 개의 눈은 적당한 거리(약 2.5inch)에 위치하고 두눈의 시각선은 고정된 사물을 서로 다른 방향에서 관측되게 된다. 즉 두 개의 서로 다른 눈은 고정된 목적물을 하나의 물체로 마치 목적물 위의 유리 위에 보이는 것 처럼 보이게 되는 현상을 말한다.

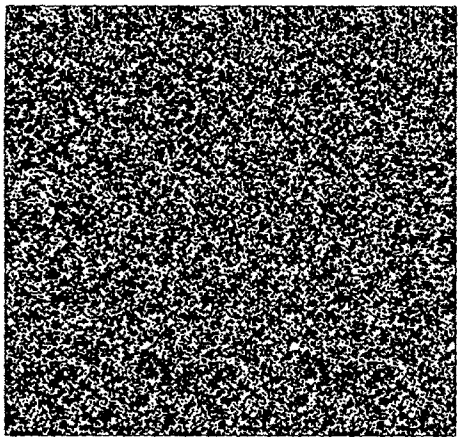


<그림1> Principals of Autostereogram

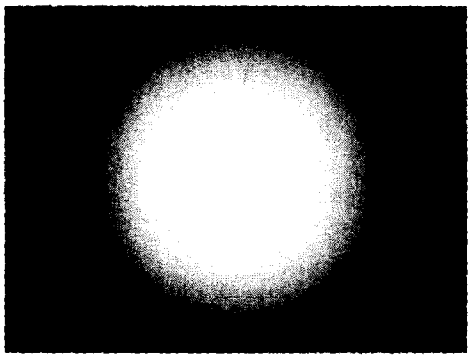
오토스테레오그램은 평면에 사물을 표현할 때 사물을 구성하는 점들에 이웃하는 유사한 점들을 추가하여 목적물을 일반적 시각으로 관찰하였을 때는 알 수 없고 두 눈의 초점을 하나의 교차점에 일치 시켜 입체적 반응을 기대하는 기법으로 오토 스테레오그램 생성 프로그램을 이용하였고 [8] 그림2.에 그 예를 보였다. 오토스테레오그램은 양안시차를 이용하여 보는 것이기 때문에 어떤 영상인지 표면에 나타나지 않기 때문에 오토스테레오그램에서 원영상의 형태를 짐작하기가 쉽지 않다. 두 눈 사이의 거리에 인치당 픽셀수를 계산하여 오토스테레오 그램에서 원 영상을 찾아본 결과를 그림3.에 보였다.

그림2. a)에서 보듯이 오토스테레오그램 된 이미지는 점들이 이미지의 전 영역에 고루 분포함을

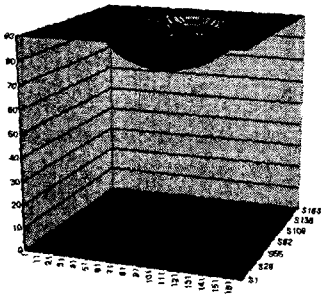
알 수 있고 이러한 특성이 워터마크의 삽입과 추출에 좋은 영향을 주는 것을 표1.을 보면 알 수 있다.



a) 반구를 오토스테레오그램화 한것



<그림2> b)영상깊이에 따라 반구를 표현한 것



<그림3> hemisphere에 대한 오토스테레오그램에서 다시 찾은 원영상

3. 보안성과 견고성

워터마킹은 모든 미디어에 기본적으로 적용되는 기술로 인식되고 있다. 저작물에 대한 정당한 보호와 권리를 주장하기 위해 워터마크 정보를 사용한다. 이러한 것을 보장하기 위해서 워터마크 기술은 다음과 같은 공통적인 요구사항을 만족해야 한다. 보안성(security), 무감지성(invisibility), 견고성(robustness), 삽입정보량, 낮은 오차 확률, 검출을 위한 원본 데이터 유지 등이 요구되어진다. 워터마킹의 안정성이 워터마킹 알고리즘의 비밀에 의해서 유지되어 지지는 않는다. 그러나 일반적인 워터마킹 상용물 들은 일반적으로 워터마킹 알고리즘을 비공개 하는 것에 기반을 두고 있다. 암호화 분야에서 공개키 기반의 암호화 기술이 효과 적인 것은 잘 알려진 사실이다. 워터마킹 기술에 있어서도 해적이 삽입된 워터마크가 어떠한 알고리즘에 의해서 삽입되었는지 모른다는 가정 하에서 워터마킹의 효율성이나, 안정성에 대하여 논한다는 것은 무의미하고 또 매우 위험한 일이 될 것이다. 워터마크에 대한 비밀이 일단 알려지면 지금 까지 만들어진 워터마킹에 대한 공격은 이루 말 할 수 없이 이루어 질 것이다. 예를 들면 워터마크의 제거, 워터마크 정보를 변조하여 저작권의 상실, 등이 이루어져 워터마킹 알고리즘을 변경해야 만 되는 경우도 발생할 것이다. 또한 실제 업무에 참여한 자의 업무 정보 유출도 발생할 것이다. 이러한 모든 사항을 고려하여 안정성을 유지하고 보증 받을 수 있는 워터마킹 절차가 이루어져야할 것이다. 워터마킹은 현재 멀티미디어 모든 매체에 적용을 하고 있다. 예를 들어 음악이나 사운드 정보에 워터마크 정보를 삽입했을 때 원래의 소리와 워터마크 소리가 같이 청취된다면 정보의 가치가 떨어지고 청취자가 워터마크를 인식할 수 있어 워터마킹의 가치를 잃을 것이고, 비디오 데이터에도 마찬가지일 것이다. 이러한 현상으로 멀티미디어 소비자들로부터 당연히 외면을 받을 것이다. 화상정보의 워터마킹은 영상속에 워터마크 정보를 일반적인 유관 관찰로는 보이지 않게 하는 방법을 사용한다. 이러한 방법은 저작권 소유와 영상물의 질을 저하시키지 않기 때문이다. 워터마킹의 무감지성은 해적의 공격

으로부터 강인성을 보장해주는 요소 중에 한 가지이다.

<표 1> The mean, sd., of randomness 20-sample image and it's distorsion limit

No.	Mean	Sd.	Distorsion Limit	No.	Mean	Sd.	Distorsion Limit
1	134	196	0.19	11	78	48	0.19
2	59	16	0.12	12	145	168	0.18
3	236	38	0.16	13	167	128	0.17
4	123	189	0.18	14	178	146	0.14
5	156	196	0.17	15	143	122	0.19
6	178	98	0.18	16	88	18	0.19
7	189	67	0.15	17	246	22	0.18
8	206	24	0.09	18	174	146	0.21
9	204	28	0.11	19	124	164	0.18
10	243	45	0.17	20	206	34	0.19

디지털 멀티미디어 정보는 손실 부호화, 필터링, 크기 변환(resizing) , 회전(rotating) , 클로핑(cropping) , 대비강조(contrastenhancement) 등과 같은 신호처리에 의해 쉽게 변형될 수 있다. 워터마크의 견고성은 앞서 서술한 신호처리에 대하여 견고성을 갖고 워터마크 정보 추출이 가능해야 한다. 이러한 워터마크 견고성을 보장하기 위해서는 워터마크 신호가 중요한 부분에 삽입이 이루어져야 한다는 것이 일반적 경향이다[7].

워터마크에 대한 해적의 공격은 워터마크 자체만을 제거, 변형하는데 목적을 둔다. 그래서 대부분의 경우 육안으로 관측이 가능한 저주파 대역 필터(low pass filter)를 사용하거나, 압축과정을 수행한 후 고주파 대역 성분을 제거하는 방법으로 해적이 이루어진다. 따라서 신호의 중요한 부분에 워터마크를 삽입함으로서 강인성을 보장받아 해적으로부터 공격을 피할 수 있을 것이다. 또한 변환(transform), 변위(translation), 크리핑, 크기변환 등의 기하학적 변환(geometric transform)이 영상에 가해질 경우 워터마크의 견고성은 없어질 수가 있다. 워터마킹의 견고성은 곧 바로 저작권 보장과 직결될 수 있어 견고성은 무엇보다도 중요한 요건이다. 이러한 견고성을 고려하여 오토스테레오그램을 워터마크 정보로 사용하였고 또한 그 특성을 이용하여 임의의 로고를 랜덤분포 하게하여 결과를 제시하였다. 워터마크 검출 과정은 워터마크 추출 시 원 영상을 필요로 하며 워터마크의 검출은 워터마킹된 영상(손실 영상)과 원 영상의 DCT 계수차를 구한 다음 역 변환하여 스케일 파라미터의 역을 곱하여 영상을 구체화 시켜서 구한다. 견고성을 측정하기위해 두 이미지의 유사성을 비교하는 식을 정의한다. X, Y를 비교하려고 하는 두 이미지 라 할 때 $Sim(X,Y)$ 를 다음과 같이 정의 한다.

for each pixel $x_i \in X$, $y_i \in Y$,

$$Sim(X,Y) = 1/\left(\sum_i (x_i - y_i)^2\right)$$

삽입한 오토스테레오그램과 추출한 오토스테레오그램의 유사성을 보기위해

for each pixel $a_i \in I$, $a_i' \in I'$

$$Sim(I,I') = 1/\left(\sum_i (a_i - a'_i)^2\right)$$

여기서 I 는 original autostereogram 이고 I'는 extracted autostreogram이다. WY 를 watermarked image라 하고 OX 를 original image라하면

$$WY = IDCT\ (DCT(OX) + DCT(\alpha I))$$
$$= OX + IDCT\ (DCT(\alpha I)$$
$$WY - OX = IDCT\ (DCT(\alpha I))$$

$$Sim(I,I') = 1/\left(\sum_i (a_i - a'_i)^2\right)$$

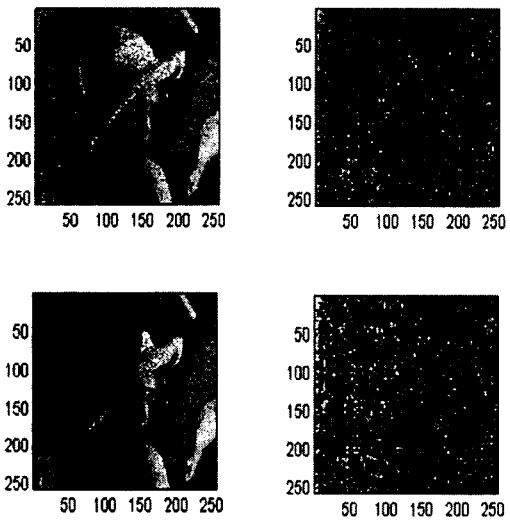
는 추출효율을 나타내며

$1/Sim(OX,WY)$

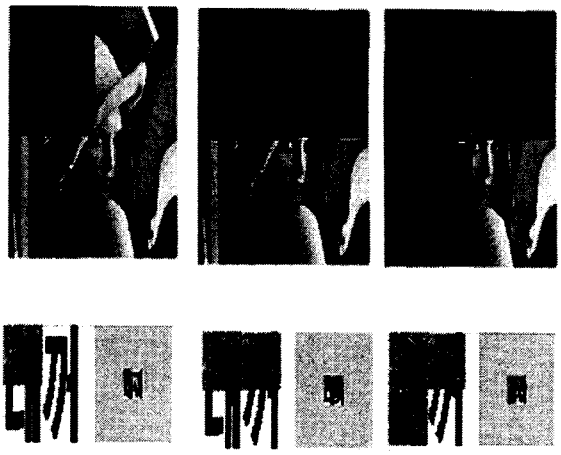
는 왜곡도를 나타내게 된다.

4. 실험결과와 결론

위에서 정의한 식을 사용하여 견고성에 대해 알아보았으며 실제 영상을 가지고 실험하여 얻은 결과는 그림4.,그림5.와 같다. 그림4.의 왼쪽 위는 노이즈가 워터마크된 영상에 가해진 영상이고 오른쪽 위는 찾아진 워터마크이며 아래는 일부분이 심하게 손상된 경우를 나타낸다. 그림3.에서 보듯이 노이즈를 가했을 때와 손상된 영상이라도 찾아진 워터마크가 매우 양호함을 알 수 있다. 그림5. 에서는 변환된 로고를 워터마크 한 것으로 절단된 그림이라도 육안으로 식별이 가능할 정도의 추출성능을 보였다.



<그림4> 왼쪽 위는 노이즈가 워터마크된 영상에 가해진 영상이고 오른쪽 위는 찾아진 워터마크이며 아래는 일부분이 심하게 손상된 경우를 나타낸다.



<그림5> 이미지의 절단이 각각 25%,50%,75% 일어났을 때 추출된 워터마크 이미지

결론적으로 오토스테레오그램과 같은 점들이 전 영역에 고루 분포하는 이미지를 워터마크하는 것은 삽입과 추출이 용이하고 견고성이 우수한 것으로 평가된다. 또한 랜덤성이 우수할수록 질 좋은 워터마크를 얻을 수 있음을 표1.을 통해 볼 수 있다.

참고문헌

[1] I. Cox et al. "Secure spread specturm watermarking for multimedia," IEEE Trans. On Image Processing, vol.6, no. 12, pp 1673-1687, Dec.1997.

[2] I.J. Cox, J. Kalian, T. Leighton, T. Shamoon, "A Secure, Robust Watermark for Multimedia," Workshop on Information Hiding, Newton Institute, Univ. of *Cambridge*, May, 1996.

[3] Brain et al., "DCT-domain system for robust image watermarking," Signal Processing.

[4] J. Fridrich, "On Digital Watermarks," *:http://ssie.binghamton.edu/~jirif/resume.html*

[5]J. Zhao, E. Koch, "Embedding Robust Labels into Images for Copyright Protection," *Proc. of*

the International Congress on Intellectual Property Rights for Specialize Information, Knowledge and New Technologies, Vienna, Austria, Aug. 1995.

[6] G. Caronni, "Assuring Ownership Rights for Digital Images," *Proc. of Reliable IT Systems, VIS '95*, Viewing Publishing Co., Germany, 1995.

[7] I.J. Cox, J. Kalian, T. Leighton, T. Shamoon, "A Secure, Robust Watermark for Multimedia," *Workshop on InformationNewton Institute, Univ. of Cambridge*, May, 1996.

[8] Harold W.Thimbleby, Stuart Inglis, Ian H.Witten, "Displaying 3D Images: Algorithms for Single-Image Random-Dot Stereograms", in Proc IEEE COMPUTER, pp38-48, October, 1994.

[9] Raymond B. Wolfgang, Christine I. Podilchuk "Perceptual Watermark for Digital Image and Video", Proc. of The IEEE, pp1108-1126, Vol. 87, No. 7, July, 1999.

[10] I.J Cox, M. L. Miller, J. A. Bloom, "Watermarking Applications and their properties", Conf. on Information Technology '2000, Las Vegas, 2000.

[11] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", M.I.T. Media Lab., Cambridge, Massachusetts, U.S.A., pp. 313-336, 1995