저작권 보호를 위한 견고한 이미지 워터마킹 기법

한창수[U*] 황재호** 홍충선* 이대영*
경희대학교 전자정보학부* 수원여자대학 전자상거래학과**
cshan@digital.kyunghee.ac.kr jaeho@suwon-c.ac.kr {cshong, dylee}@khu.ac.kr

Robust Digital Watermarking Algorithm For Copyright Protection

Chang Su Han[U*] Jae ho Whang** Choong Seon Hong* Dae Young Lee*
School of Electronics & Information. Kyung Hee University*
Department of electronic suwon women's College**

요 약

본 논문에서는 HVS을 이용하여 웨이브렛기반 이미지 워터마킹 기법을 제안한다. 웨이브렛 변환 된 각 밴드 중 최고 저주파 밴드에 인접한 3개의 밴드를 선택하여 각 밴드에 워터마크를 반복적으로 삽입하여 견고성을 높였다. 또한 밴드 안의 모든 계수 값에 워터마크를 삽입하지 않고 선택적으로 삽입함으로써 비가시성을 고려하였다. 저주파 영역에 워터마크를 삽입함으로서 가우시안 노이즈나 JPEG, 잘라내기등 여러 공격모델에 대해 견고성을 잘 보여주고 있다.

1. 서론

최근 급속한 인터넷의 성장과 그 이용률이 폭발적으로 증가하면서 디지털을 통한 멀티미디어 서비스가 급증하게 되었다. 특히 JPEG, MPEG와 같은 압축기술의 발달은 이러한 멀티미디어 컨텐츠의 인터넷을 통한 여러 서비스를 가능하게 만들었다. 디지털로 제작된 어떤 영상이나 오디오에 대해 저작권을 가진 자는 새로운 과금서비스나 보안서비스를 요구하게 되었다. 이런 디지털 콘텐츠를 보호하기 위한 기술적인 방법은 크게 3가지로 나눌 수 있다. 첫 번째는 권리가 없는 사용자에게 콘텐츠 접근을 막는 접근제어방법 두 번째는 암호화나 비밀키, 공개키를 이용하여 정당하지 않은 사용자의 콘텐츠사용을 막는 방법, 그리고 마지막으로 콘텐츠 내용에 보이지 않는 정보를 심어 저작권을 보호하고 불법적인 복제를 막는 내용제어이다. 오래 전부터 연구되어 오던 것 중 하나는 암호화를 통한 방법이나 저작권이나 진품여부를 판명하기에는 불충분하다. 워터마크는 내용제어에 해당하는 것으로 이미지, 오디오, 동영상등 멀티미디어 컨텐츠에 사람이 인식하지 못하는 신호를 넣어서 소유권을 주장하고자 하는 특정 데이터를 보장해주고 임의로 컨텐츠에 대해 조작을 못하게 하는 기술이다[2]

워터마크를 삽입하기 위한 고려사항이다[3].

Invisible : 워터마크는 사람의 시각에 인지되어서는 안 된다. 즉, 삽입된 신호가 본래 이미지에 시각적으로 영향을 미쳐서는 안 된다.

Robust : 워터마크는 외부의 요인으로 인하여 제거가 안되어야 한다. 일반적인 신호처리 즉, 디지털에서 아날로그로의 변환, 아날로그에서 디지털로의 변환, 샘플링, 양자화, 압축등과 같은 과정을 거치더라도 워터마크는 존재해야한다.

Capacity : 워터마크는 이미지의 질 저하 없이 최대한 많은 수의 워터마크를 넣어야한다.

위 세 가지는 서로 상호 보안(trade-off)관계에 있다. 사람 눈에 안보이게 하기 위해 작은 신호를 넣는다면 그 워터마크는 제거되기가 쉬울 것이다. 반대로 쉽게 제거되지 않게 하기 위해 큰 신호를 넣는다면 사람 눈에 잘 보이게 될 것이다.

이러한 워터마크의 응용분야로는 크게 저작권 증명, 브로드캐스팅 모니터링, 역추적시스템등에 이용할 수 있으며 특히 저작권 증명에 있어서 디지털 문화의 확산과 응용의 광범위함에 따라 그 중요성이 증가하고 있는 추세이다. 소리바다의 폐쇄가 그 대표적인 예라고 하겠다.

본 논문의 구성은 다음과 같다. 2절에서는 기존의 워터마크 기법에 대해 알아보고 3절에서는 제안한 알고리즘을 소개하며 4장에서는 실험결과, 5절에서는 결론을 맺고 향후 연구과제를 제시한다.

2 본론

앞에서도 언급했지만 워터마킹에 관한 연구는 주파수 도메인에서가 대부분이다. 그 중에서도 가장 많은 연구가 되고 있는 부분은 DCT(discrete cosine transform)와 DWT(discrete wavelet transform)을 이용한 기법들이다. 이번 절에서는 워터마크 기법들을 살펴보고 특징을 분석해 본다.

다음은 워터마크를 삽입하고 추출하는 일반적인 그림이다.[1]

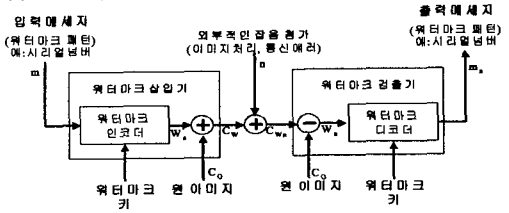

그림 1 워터마크 삽입과 추출

Fig 1 Watermark embedding and extraction

2.1 DCT기반 워터마크 기법

주파수 도메인에서의 워터마크 기법은 여러 가지가 있다. 그 중에서도 DCT를 이용한 방법은 가장 많이 연구되어지는 것 중 하나이다. DCT는 계산량이 적고 JPEG, MPEG과 같은 국제 표준에서도 많이 이용되고 있다는 점에서 이득을 얻을 수 있다.[4] 은 다른 논문들은 주로 중간대역에 워터마크를 삽입했다. 다른 말로하면 DCT의 AC성분에 워터마크를 삽입하는 것이다.[2,5] DC성분에 워터마크를 안 넣는 이유는 DC성분은

이미지 질에 감소를 가져오기 때문이다. 그러나 견고성 관점에서 보면 AC성분보다 DC성분에 워터마크를 삽입하는 것이 유리하다. 단 워터마크의 비가시성을 유지해야 하므로 아주 작은 신호가 더해 질 것이다. DC 성분에 워터마크를 삽입 할 경우 작은 신호라도 압축이나 샘플링을 통해 제거되지 않는다. 보통 DC성분에는 이미지의 중요한 정보가 들어있기 때문이다. 보통 AC계수값들보다 DC계수값들은 크다. DCT기반 워터마크 기법을 간단히 소개하면 8×8 블럭단위로 DCT를 하고 Brightness와 Texture성분을 블록단위로 계산한다. 임계값을 기준으로 밝은 부분과 texture부분을 나눠어 각각에 다른 크기의 워터마크를 삽입한다. 워터마크 추출은 워터마크가 삽입된 이미지에서 본래의 이미지를 뺀 다음 나온 값을 블록 DCT를 한다. 여기서 워터마크를 추출하고 원래 삽입된 워터마크와 유사성(correlation)을 측정해 워터마크의 유무를 판단한다[5].

2.2 DWT기반 워터마크 기법

현재 JPEG2000의 표준화는 DCT에서 웨이브렛 기반 이미지 압축의 방법을 사용하면서 웨이브렛의 관심이 늘어가고 있다. 웨이브렛 코딩은 이미지압축이나 워터마크의 응용에서 많은 이점을 주고 있다.[6]

1) Space-frequency localization

웨이브렛 도메인은 공간과 주파수 성분을 나타낼 수 있다. 이는 에지와 텍스처 부분을 잘 해석할 수 있게 하여 견고하고 눈에 안 보이는 워터마크를 삽입할 수 있다.

2) Multi-resolution representation

Harr, Daubechies-4, 7/9-biorthorgonal filter를 통해 세 번이나 네 번의 분해 과정을 거치면 다른 크기(scale)로 이미지를 표현하게 한다.

3) Coefficient selection

워터마킹 과정에서 계수 값을 선택하는 것은 삽입하는 알고리즘이나 워터마크의 응용분야에 따라 다르다.

최고 저주파부분에 삽입하는 방법으로 다시 말해서 LL부분에 워터마크 신호를 삽입하는 방법이다. 3개의 레벨로 분해된 LL은 8×8 블록 단위 DCT의 DC성분과 같은 의미를 가진다. 즉, 이미지의 낮은 주파수성분이 LL에 위치하게 되는 것이다. 중국의 Liang과 Ohnishi는 pseudo-random Gaussian sequence를 각각의 계수값에 더하여 워터마크를 삽입했다. 이는 큰 크기를 갖는 신호를 삽입하게 될 경우 사람 눈에 보일 수가 있고 LL성분에 넣는 이유는 robustness를 강화하기 위한 알고리즘이다[8,9].

다른 방법으로는 고주파 부분에 워터마크를 삽입하는 기술이 있다. 즉 LH, HL HH부분에 사람의 눈이 둔감한 고주파 지역에 워터마크를 삽입하는 기술이다.[10] 대부분의 계수값들은 0에 가깝고 몇몇의 계수 값들만 큰 값을 갖는 특징이 있다. 삽입되는 워터마크 크기는 서브 밴드의 에너지와 분해 레벨에 따라 달라진다. Xia는 DWT계수값들을 이용하여 최고 저주파부분에 랜덤 가우시안 분포를 갖는 값을 삽입하던 방법과 같이 sub-band에 삽입하는 방법을 제안했다. 지각적으로 인식되지 않기 위하여 분해된 레벨에 따라 다른 크기의 워터마크를 삽입하였다.

3. 제안한 알고리즘

본 논문에서는 워터마크를 삽입하기 위하여 DWT을 이용하였고 LL성분과 가장 인접한 고주파부분을 선택하여 여러 이미지 처리과정에 견고하도록 하였다. 선택된 밴드 안에서도 모든 계수 값에 워터마크를 삽입하지 않았으며 연속하는 네 개의 계수 값을 비교하여 에너지가 가장 큰 것에 워터마크를 넣어서 비가시적인 면을 고려하였다. 본인이 제안한 알고리즘은 다음과 같다.

1) 원래 이미지 호출

워터마크를 삽입하고자 하는 이미지의 크기는 여러 가지가 될 수 있다. 본 논문에서는 512×512의 크기를 가지는 레나 영상으로 하였다.

2) 웨이브렛 변환 및 삽입 될 밴드 선택

우선 워터마크를 삽입하기 위해서 몇 레벨로 웨이브렛 분해를 할 것인지 결정하고 어떤 밴드에 워터마크를 삽입할 것인가를 결정하고 이를 키로 저장한다.

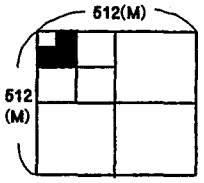

그림 2 세 개의 웨이브 렛 변환과 밴드 선택

Fig 2 three wavelet decomposition and band selection

위 그림은 3개의 레벨로 웨이브렛 변환이 되었고 그중 빨간색 부분의 밴드를 선택하였음을 나타내고 있다.

3) 워터마크 개수 결정

워터마크가 삽입될 개수는 아래 식에 의해서 결정한다

$$N(W_0)=\frac{M^2}{2^{2l+2}} \quad (1)$$

밴드 안의 모든 계수에 워터마크를 삽입하는 것은 아무래도 원 이미지 질에 훼손을 가져오게 마련이다. 위의 식을 이용하여 워터마크 개수를 결정하고 선택된 계수에만 워터마크를 삽입함으로써 원 이미지 훼손을 저하시킬 수 있다.

4) N개의 랜덤넘버 생성

워터마크의 개수가 결정되면 그 개수만큼 씨드(seed) 값을 이용하여 랜덤넘버를 생성하고 이것이 곧 워터마크의 모태가 된다.

$$W_0=\{x_1,x_2,x_3,\cdots\cdots,x_N\} \quad (2)$$

각각의 값은 0에서 1사이의 값을 가지는 랜덤 수이고 씨드 값은 저장한다.

5) 워터마크가 삽입될 계수 결정

우선 선택된 밴드를 1차원 벡터로 배열하고 연속하는 4개의 계수 값 중 큰 값을 선택한다. 큰 계수 값은 큰 크기의 워터마크를 삽입할 수 있고 보다 더 견고해지기 때문이다.

$$C[l,\theta]=\{c_1,c_2,c_3,\cdots\cdots c_N\}$$

$$a_{4i}\le c_{i+1}\le a_{4i+3} \quad (3)$$

여기서 i는 0,1,2,.....N-1을 가지고 a_i 는 선택된 밴드의 1차원 벡터를 나타낸다.

6) 선택된 계수의 HVS측정

웨이브렛 계수를 놓고 볼 때 사람의 시각적인 특성은 낮은 레벨, 높은 광도, 복잡한 텍스처성분에서 덜 민감하다.[]

위와 같은 특성을 고려하여 비쥬얼 팩터를 준다.

$$H[C(l,\theta)]=R(l,\theta)\cdot L(l,i)\cdot T(l,i)^{0.2} \quad (4)$$

여기서 l은 fp벨을 나타내고 θ는 밴드를 나타낸다.

$R(l,\theta)$에서 θ가 1이면(대각선 밴드)$\sqrt{2}\times 0.16$이고 θ 가 각각 0과 2이면 0.16의 값을 가진다. 여기서 0.16값은 레벨 l에 따라 값이 달라지는데 예를 들어 레벨이 1이면 1이고 2이면 0.32값을 가진다.

$$L(l,i)=\frac{1}{256}S(3,3)[C_i] \quad (5)$$

최고 저주파 부분에는 이미지의 대부분의 정보를 포함하고 있고 그 계수 값 역시 매우 크다. 트리형태로 아래 레벨로 내려가면 유사한 정보를 내포하게 되는데 이를 이용하여 광도 값을 계산한다.

$$T(l,i)=(\sum_{x=0}^{1}s(i+x)^2+\sum_{x=0}^{1}s(Ni+x)^2)\times Var\{S(3,3)c[i+x]\}_{x=0,1} \quad (6)$$

위의 식으로 텍스처 성분을 분석하여 H를 구한다.

다음은 최종적으로 워터마크를 삽입하는 식이다

$$I^*(l,\theta)=I(l,\theta)+\alpha\cdot W_0\cdot H(l,\theta) \quad (7)$$

I는 원 이미지이고 I^*는 워터마크가 삽입된 이미지이다. α는 임의의 팩터로 워터마크의 크기를 조절하는 상수이다.

워터마크 검출은 키를 이용하여 똑같은 방법으로 웨이브렛 분해를 하고 밴드를 추출한 후 원 이미지와의 차이를 가지고 삽입된 워터마크와 유사성을 가지고 워터마크 유무를 판별하게 된다. 다음은 유사성을 판별하는 식이다.[3]

$$\text{유사성}(W, W^*) = \frac{W^* \cdot W}{\sqrt{W^*} \cdot \sqrt{W^*}} \qquad (8)$$

어떤 임계값을 넘으면 이미지는 워터마크가 삽입된 걸로 간주하고 넘지 않으면 워터마크가 없는 걸로 간주하여 저작권을 인증하게 된다. W^*은 워터마크가 삽입되어 어떤 외부 작용에 의해 변형된 워터마크 값을 말하고 W는 원래 삽입되었던 워터마크를 말한다. 이렇게 식 (8)에 의해 얻어진 값은 워터마크 유무를 판별하는데 기준이 된다.

4. 실험 및 고찰

실험영상으로는 레나영상을 사용하였고 크기는 512×512로 하였다. 워터마크는 주어진 식(1)에 의하여 웨이브렛 변환의 분해 레벨과 선택밴드에 따라 결정되지만 여기선 세 개의 레벨과 최고 저주파 부분과 인접한 고주파 부분의 밴드를 선택함으로써 1096개의 워터마크를 생성한다. 고주파 밴드영역의 부분을 선택하게 되면 PSNR값은 더 높아지지만 압축 시에나 스무딩, 가우시안 노이즈 공격 시에 검출율은 더 낮아졌다. 본 논문은 견고한 워터마킹 시스템을 설계하기 위해 최대한 저주파 밴드 영역에 워터마크를 삽입하였으며 그 결과는 다음과 같다. α는 0.1로 하였고 가우시안노이즈 더하기, 잘라내기, 스무딩, JPEG압축비율을 달리해 가면서 유사성을 측정해 보았고 모두 성공적으로 워터마크를 검출할 수 있었다. 다음 그림은 원래의 레나 영상과 워터마크를 삽입한 후의 레나 영상이다.

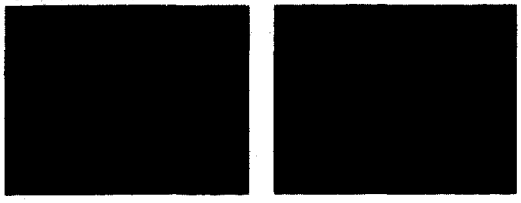

그림 3 원래 레나 영상과 워터마크가 삽입 된 후의 레나 영상 (PSNR = 40.98)

Fig 3 original lena image and watermarked lena image (PSNR = 40.98)

워터마크를 삽입한 후 PSNR을 측정한 결과 40.98이 나왔다. 다음 그림은 워터마크를 삽입하고 1000개의 다른 워터마크를 가지고 유사관계를 측정한 그림이다. 워터마크의 존재 유무의 임계값은 10으로 하였다.

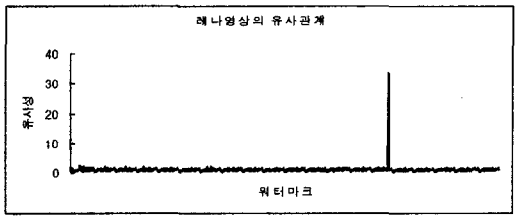

그림 4 워터마크가 삽입된 레나영상의 유사관계

Fig 4 correlation after watermarked lena image

다음 표는 영상처리 후 유사성을 측정해 보았다 JPEG 경우 압축률을 70%까지는 임계값 10을 넘었고 그 이후는 검출이 안되었다. 잘라내기의 경우도 영상의 60%까지 잘라냈을 경우 가능하였다.

표 1 영상처리후 유사관계

Table 1 correlation after image processing

	가우시안 노이즈	잘라내기 (30%)	스무딩	JPEG(30%)
유사성	20.8	20.3	22.4	16.1

5. 결론 및 향후 연구방향

워터마크를 삽입하는 데 있어 가장 중요한 것은 사람의 눈이나 귀에 인지되지 않는 신호를 압축이나 샘플링등을 하여도 삽입된 워터마크가 손상되지 않아야 한다. 기존에 많이 연구되어져 온 DCT기반 그 계수 값에 워터마크를 삽입하는 방법은 계산량이 작고 많은 압축 표준에서 사용하고 있다는 장점이 있으나 공간영역에서의 분석이 불가능하다는 단점이 있다. DWT를 기반으로 하는 연구는 현재 활발히 진행 중에 있으며 특히 HVS를 이용한 방법이 비가시성과 견고성, 용량성의 특성을 가장 잘 살릴 수 있는 방법이다. 본 논문에서 밴드 선택과 레벨 선택을 임의로 할 수 있게 하였고 한 밴드 안에 있는 모든 계수 값에 워터마크를 넣지 않고 네 개의 계수 중 특성이 보다 좋은 한 계수를 선택하여 넣음으로써 더 좋은 결과를 도출하였다. 물론 비가시적인 측면에서도 우수하였다. 본 실험에서는 최고저주파밴드에 인접한 고주파부분에 넣었으나 레벨이 낮은 밴드에 삽입하게 되면 비가시성은 더 우수할 것으로 보이나 견고성은 그만큼 더 떨어질 것으로 생각된다. 향후 연구 과제는 원 이미지가 사용되지 않는 방식의 검출 방식을 연구해야 한다. 원 이미지가 필요하다는 것은 결국 메모리 문제에 봉착하게 될 것이다. 워터마크에 대한 정보만 가지고 워터마크가 삽입된 이미지에서 워터마크를 추출할 수 있는 기술이 필요하다. 또한 공개키를 기반으로 워터마크를 삽입하는 방법도 현재 이슈 중 하나이다.

참고문헌

[1] J. Cox et al, "Digital Watermarking" p48 morgan kaufmann publishers

[2] A. Hanjalic et al"Image and Video Databases : Restoration, Watermarking and Retrieval" Elsevier Science, 2000

[3] J. Cox ed, "A secure, Robust Watermark for multimedia" Univ. of Cambridge 1996

[4] A. Piva, ed., "DCT-based watermark recovering without resorting to the uncorrupted original image" proceeding of ICIP, 1997

[5] J. Cox et, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing. vol 6, no. 12. pp. 1673-1687, 1997

[6] J. Cox et al, "Mulitiresolution Watermarking for Image and Video" IEEE Trans on circuitys and systems for video technology. vol.9, no.4 1999

[7] Y.J. ZHANG et al. "Embedding Watermarks into Both DC and AC Components of DCT" Proceedings of SPIE 2001

[8] J. Liang, et al. "A universal robust low frequency watermarking scheme," submitted to IEEE Trans. on Image Processing, 2000

[9] J. Ohnishi, et al. " A method of watermarking with multiresolution analysis and pseudo noise sequences," Systems and Computers in Japan 29, pp. 11-19, 1998

[10] X. G. Xia et al, "Wavelet transform based watermark for digital images," Optics Express3, p.497 1998