워터마킹 기법 및 공격기술에 관한 고찰

*김천윤 · *김윤호, **성경, **윤호군
*목원대학교 컴퓨터멀티미디어공학부, *목원대학교 컴퓨터교육학과

A Study About Watermarking Techniques and Attack Technology

*Cheon-yoon Kim · *Yoon-ho Kim,**Keong Seong · **Ho-kun Yoon
*Div. of Computer Multimedia Eng., Mokwon Univ.· **Computer Education. Mokwon Univ
E-mail : hidead@mokwon.ac.kr

요 약

디지털 워터마킹 기술은 이러한 저작권 보호기술의 하나로 원본 컨텐츠에 저작권자에 대한 정보를 은닉함으로써 저작권자를 확인시켜주고 불법복제나 유통여부를 가려주는 기술로 개발된 것이다. 디지털 워터마킹 기술이 필요한 정보를 은닉한다는 측면에서 정보은닉 기술의 하나이며, 이는 단순히 저작권 보호의 이외의 분야에 대해서도 응용이 가능하다는 것을 나타낸다. 본 논문에서는 워터마킹이 무엇인지 그리고 워터마킹의 공격방법의 유형을 정리하고, 기존에 제안한 워터마킹 기법에 대해 고찰한다.

키워드
워터마킹, 저작권 보호, 워터마크, 공격 기법

I. 서 론

우리는 인터넷과 멀티미디어 기술의 발달로 인하여 각종 그림, 음악, 동영상 등이 디지털화 되어가는 멀티미디어 디지털시대를 살고 있다. 보통 인터넷을 통하여 멀티미디어 자료들이 유통됨에 따라 디지털 저작물이 무제한적인 복제와 유통이 가능하며, 원본과는 구별이 불가능해 멀티미디어 자료에 대한 저작권의 보호나 불법복제 및 유통 방지를 위한 기술이 절실히 필요하게 되었다. 이러한 현상에 의해 훌륭한 콘텐츠에 대한 정당한 대우와 소유권을 보호하려면 멀티미디어 유통 과정에서 저작권의 보호나 불법복제 방지 기능들이 포함되어야 한다. 현재 멀티미디어 저작권 관리시스템들은 일반적으로 암호화, 접속 제어, 키 관리 등으로 이루어져 있으며 복제 방지, 저작권 지불 인터페이스 등을 포함하고 있다. 그러나 실제적으로 불법 복제 방지나 유통 제어를 구현하기에는 한계를 나타낸다. 이 한계를 극복하기 위해서 제안된 것이 개별 복사본에 대한 사용자 확인 및 역추적이다. 이것은 일종의 컴퓨터 소프트웨어의 일련번호와 비슷한 것으로 멀티미디어 자료에 대한 불법 복제는 억제 할 수 없지만 불법 복제된 멀티미디어 자료의 원본을 밝혀내는데 도움을 줄 수 있다. 이러한 불법 복제 가능성이 있는 데이터에 대한 정보의 확인을 위한 디지털콘텐츠 저작권 보호의 주요 기술로서 디지털 워터마킹 기술이 부각되고 있다. 초기의 연구되었던 워터마킹 기법은 공간 영역에 워터마크를 삽입하는 것으로 공간 영역 상에서 영상의 화소값을 직접 변화 시켜 워터마킹을 수행하는 방식이었다. 하지만 이러한 공간 영역에서의 워터마킹은 공격에 약한 단점을 가지게 되었다. 워터마킹의 기술이 발달함으로 워터마크 적용 영역이 공간영역에서 주파수 영역으로 옮겨지게 되었는데, 공간영역에서 적용되던 방식에 비해 공격에 강한 특성을 갖는다. 본 논문의 구성은 2장에서는 디지털 워터마킹에 대해 알아보고, 3장에서는 기존에 제안되어 있는 워터마킹 기법중에 몇 개만 추슬러서 이를 분석하고, 5장에서는 결과 및 향후 과제를 제시한다.

II. 디지털 워터마킹

디지털 워터마킹이란 멀티미디어 저작물을 보

호하기 위해 여기에 특별한 형태의 워터마크(저작권 정보, 로고, 인감, 일련번호 등)를 감추고 검출하는 모든 기술적 방법을 뜻한다. 워터마킹 기술의 초기에는 멀티미디어 저작물 자체에 대해서 은닉시키는 방법을 연구하였지만, 현재는 많은 기술적 변환방법을 이용한 강력한 워터마킹기술이 개발되고 있다.

1. 워터마크 기본 원리

(그림 1)은 멀티미디어 컨텐츠에 Mark를 삽입/추출하는 과정이다. 주어진 영상 I, 마크 M, 키 K (보통 난수 발생기의 시드)에 대해서 삽입 과정은 다음의 매핑으로 정의된다.

$$I \times M \times K \rightarrow I\square\square \quad (식\ 1)$$

검파기의 출력은 추출된 워터마크 M이 될 수도 있고, 어떤 확증을 위한 측정값일 수도 있다.

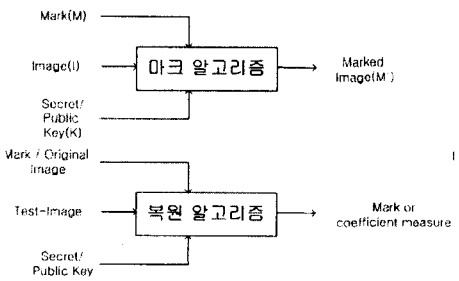

그림 1. 워터마킹의 기본 구조

2. 워터마크가 가져야 할 특성

이러한 워터마크가 가져야 할 특성은 여러 가지가 있다. 그중에서 크게 4가지로 구분하면 다음과 같다.

가. 비가시성(invisiblity) : 워터마크가 삽입 후에도 원본의 변화가 거의 없고, 삽입된 신호가 원 이미지에 시각적으로 영향을 미쳐서는 안 된다.

나. 강인성(robustness) : 멀티미디어 콘텐츠는 여러 가지 형태의 변형이 가해질 수 있다. 즉 콘텐츠를 압축할 수도 있고, A/D, D/A 변환시킬 수 있다. 그리고 확대/축소 이동, 자르기, 회전 등의 변형을 줄 수도 있다. 이러한 여러 가지 형태의 변형에 워터마크가 쉽게 깨지지 않게 되어야 한다.

다. 명확성(Unambiguity) : 노이즈나 여러 가지 형태의 변형과 공격에도 추출이 가능해 추출된 워터마크가 확실한 소유권을 주장할 수 있도록 공격에 대해 정확성을 유지가 필요하다.

라. 용량성(Capacity) : 워터마크는 이미지의 질저하 없이 최대한 많은 수의 워터마크가 삽입되어야 한다.

III. 워터마킹 공격방법

워터마킹을 무효화시키는 공격 기술에는 rotation, scale, translation, JPEG (MPEG) compression 등과 같은 기본적인 신호처리 기술이 있지

분 류	특성 및 용도
강성(Robust) 워터마킹	- 원본 이미지에 고유의 표식으로 워터마크를 삽입하여 저작권 증명 및 보호에 사용 - 삽입된 워터마크를 지우거나 무력화 시키려는 공격에 견딜 수 있는 내성(Robutness)이 가장 중요 - 현재 모든 공격에 대해 강성을 제공하기 어려움
연성(Fragile) 워터마킹	- 원본과 조금이라도 다르면 워터마크가 깨지며 원본이미지가 손상되게 설계 - 강성 워터마킹 기술과 달리 워터마크가 얼마나 잘 깨어질수 있는냐가 척도 - 복제되어서는 안되는 데이터 보호를 위해 활용 - 은행이나 관공서 문서, 법률 문서, 병원의 각종 임상사진 등 원본보호 및 증명에 사용
핑거프린팅 (Figer Printing)	- 지문과 같은 고유정보를 파일에 삽입하고 그 정보를 다양하게 활용할 수 있도록 함 - 바코드(bar code)대체, 정보의 전송경로/배포경로 확인, 물류사업에서 제품의 분류 작업에도 이용가능
스테가노 그래픽 (Steganography)	- 정보를 은닉하거나 다른 형태로 위장하여 주고 받을 수 있게 기능을 가지며 주로 군사적인 목적으로 사용 - 암호화(encryption) 형태보다 한층 진보된 암호통신

표 1. 워터마크 기술의 용도에 따른 분류

만 여기서는 복합적인 기술을 알아 보기로 한다.

1. Filtering Attack

많은 워터마크 신호는 spread spectrum 기술을 이용함으로써 멀티미디어 콘텐츠에 noise와 비슷한 형태로 처리되는데 이 Filtering attack은 lowpass filtering으로 멀티미디어 콘텐츠에 대한 노이즈를 없애듯이 멀티미디어 콘텐츠의 워터마크 정보를 없애는 공격 방법이다.

2. Copy Attack

워터마크가 삽입된 멀티미디어 콘텐츠에서 wiener filtering과 같은 방법을 통해 삽입된 워터마크를 확인하고, 확인된 워터마크에 워터마킹 되지 않은 임의의 정보를 추가하여 워터마크 검출기로 하여금 원 워터마크가 아닌 새로운 워터마크를 검출 하게 함으로써 false positive rate를 높이는 기술이다.

3. Mosaic Attack

워터마크 된 멀티미디어 콘텐츠를 워터마크가 검출 되기 전에 워터마크가 검출 되지 않을 정도의 크기로 작게 조각내어서 검출기를 통과한 후에 다시 조각을 맞추는 기술이다.

4. SWICO Attack

이는 Single Watermarked Image Counterfeit Original attack으로 타인 소유의 워터마크가 삽입된 멀티미디어 콘텐츠에 random noise와 비슷한 자신의 워터마크를 삽입하여, 각자의 검출기에서 각자의 워터마크를 검출할 수 있게 하여 소유권 분쟁을 일으키는 방법이다.

5. Template Attack

일종의 synchronization attack이다. 많은 워터마킹 기술들은 affine transformation 과정에도 불구하고 워터마크를 검출할 수 있도록 하기 위해 워터마크 정보 뿐만 아니라 이를 검출하기 위한 일종의 패턴을 삽입하는데, 이 공격은 이러한 패턴을 파괴함으로써 검출기로 하여금 워터마크 검출을 불가능하게 하는 방법이다.

IV. 대표적인 워터마킹 기법

워터마크에 대한 연구는 1990년대에 들어와 많은 연구가 진행되었다. 대표적으로 몇 가지 워터마킹 기법을 살펴보기로 한다.

1. G. Caronni가 제안한 기법

G. Caronni는 원 이미지에 사람이 인지 할수 없는 어두운 부분에 디지털화된 워터마크를 아주 작은 기하학적 패턴형식으로 삽입하는 방법을 제안했다. 이 기법은 공간적인 부분에 워터마크를 삽입하므로 필터링과 재디지털화에 의한 공격에 영향을 받기 쉬울 수 있다. 또한 기하학적 패턴들은 암호화된 정보와 함께 제안된 알파벳으로 제공함으로 크로핑과 같은 일반적인 기하학적 왜곡 현상들에 견고 할 수 없다[1].

2. B. M. Macq가 제안한 기법

B. M. Macq와 Quisquater는 주로 암호화와 디지털 TV상에서 워터마킹 디지털 이미지의 삽입하는 방법을 제안했다 이미지의 에지에 위치한 픽셀들의 LSB에 워터마크를 삽입하는 절차를 기술하였다. 이미지 에지 픽셀의 마지막 비트에 워터마크의 정보를 넣음으로써 구현이 쉽고 이미지에 최소한의 변형을 주는 것이지만 작은 이미지 변형에도 워터마크가 검출되지 않는다는 단점이 있다[2].

3. W. Bender가 제안한 기법

Bender는 두가지 워터마킹 기법을 제안하는데 이중에 한 방법은 패치워크라 불리는 통계적인 방법이다. 이 방법은 이진수로 랜덤 벡터를 생성한다. 이 랜덤 벡터에서 1의 정보를 나타날 때에는 삽입하고자 하는 픽셀에 더하고, 0의 정보를 나타날 때에는 삽입하고자 하는 픽셀에 빼기 연산을 하여 워터마크를 영상에 삽입한다. 이는 기하학적 왜곡에 안 좋은 결과를 나타내고 압축에서도 워터마크 검출율이 매우 낮다[3].

4. E. Koch가 제안한 기법

Koch, Rindfey와 Zhao는 이산 코사인 변환(DCT)을 이용한다. DCT 계수에 비트 스트림을 삽입하는 방법이다. JPEG압축 방법과 같이 8×8 블록으로 나눈 다음 각 블록에 대해 이산 코사인 변화 계수를 계산한다. 이 계수를 이미지의 질을 결정하는 Q-factor와 표준 양자화 행렬을 양자화하고 양자화 된 세 개의 블록을 비교하는데 세 번째 블록의 계수가 다른 두개의 블록의 계수보다 작을 경우에는 블록을 '1'로 부호화한다. 그러므로 주파수에 마스킹 하는 것과 같은 현상을 얻는 이 방법은 각각의 블록이 DCT 변환되면, 주파수 마스킹 모델을 이용하여 DCT 주파수 계수 각각의 최대 허용 변동 값을 계산하여 워터마크를 구조화 한다. 그러므로 다른 제 3자가 보기에 워터마크가 삽입되어 있는지 거의 알지 못하고 원 데이터의 주파수와 거의 같은 주파수를 삽입하여 보이지 않도록 구조화하는 방법이다[4].

5. Yu Jin Zhang가 제안한 기법

Zhang은 영상을 8×8 블록 DCT 후 고주파 성분(AC)와 저주파 성분(DC) 모두에 각 계수의 특성에 따라 워터마크의 크기를 조절하는 방법으로 워터마크를 삽입하였다. 크기를 조절하는 상수 α

제안자	장 점	단점
G. Caronni	- 기하학적 패턴 적용 - 복잡도가 낮은 알고리즘	- 필터링에 약함 - 재디지털화에 약함 - 크로핑에 약함
B. M. Macq	- 픽셀의 LSB 기반 - 복잡도가 낮은 알고리즘 - 이미지의 최소한의 변형	- 작은 이미지 변형에 대한 워터마크 손실 - 워터마크가 인지 가능성 높음
W. Bender	- 랜덤 벡터 기반 - 통계적 방법 적용	- 기하학적 왜곡에 워터마크 손실 - 재압축시 워터마크 검출률 낮아짐
E. Koch	- DCT 변환 기반 - DCT 계수 비트 스트림에 삽입 - Q-factor와 표준 양자화 행렬로 양자화 - 주파수 마스킹 모델	- 재 워터마크시 기존 워터마크와 새로운 워터마크 검출
Yu Jin Zhang	- 8×8 DCT 변환 기반 - AC 성분과 DC 성분 계수 사용	- 워터마크 크기 조절 가능한 상수에 의해 알고리즘의 한계 발생
Mohammed A. Al-Mohimeed	- 웨이블릿 기반 - 양자화 키 사용 - 다중 워터마크 삽입 가능	- 워터마크 최적의 크기에 대한 한계

표 2. 대표적인 워터마킹 기법의 장단점

와 β를 영상의 밝고 어두운 정도와 복잡도 특성을 우선 결정하고 이에 따라 워터마크를 삽입하였다. α와 β가 상수라는 점에서 알고리즘의 한계가 있다[5].

6. Mohammed A. Al-Mohimeed가 제안한 기법

Mohammed A. Al-Mohimeed는 웨이블릿 기반으로 워터마크를 삽입하는데 바이너리 워터마크를 사용하여 삽입될 워터마크가 1이면 값을 변화시키지 않고 0이면 양자화 키를 이용하여 워터마크 삽입한다. 워터마크가 삽입될 계수에 따라 양자화 키를 사용함으로써 각각 다른 크기의 워터마크를 삽입할 수 있다는 장점이 있으나 워터마크의 최적의 크기가 유도한 것은 아니므로 한계를 가진다[6].

V. 결 과

동영상에 대한 워터마킹 기술은 저작권 보호, 디지털 컨텐츠 복제 방지, 비디오의 실시간 모니터링 등에 활용 될 수 있다. 본 논문에서는 워터마킹이 무엇인지 알아보고 이 워터마킹에 대한 각종 공격 방법에 고찰하였다. 그리고 기존에 제안된 각종 워터마킹 기법을 살펴보았는데 여기서 알수 있는 것은 워터마크를 이미지 픽셀에 직접 공간 주파수 대역을 이용하여 워터마크를 삽입하는 것은 기본적인 신호 처리 기술 즉 rotation, scale, translation, JPEG (MPEG) compression에 쉽게 워터마크가 사라진다는 사실이다. 이는 (표 5-1)를 통해 알수 있다.

이는 G. Caronni의 기법과 B. M. Macq의 기법, W. Bender의 기법을 통해서 알수 있다. 이러한 사실에 따라 워터마크 삽입 밴드를 주파수 대역으로 옮겨지게 되었다.

최근에는 주파수 대역으로 워터마크 삽입하는 방법은 웨이블릿 기법이 많이 사용된다. 웨이블릿 변환 기법은 연속 신호와 이산 신호의 경우에 모두 적용 될 수 있으며 다양한 분야에서 그 응용 가능성을 인정받고 있다. 향후 과제로 워터마킹의 지녀야 할 특성인 비가시성과 강인성, 용량성 등을 모두 만족하는 웨이블릿 변환 워터마킹 기법을 적용한 기법에 대한 폭 넓은 연구가 수행되어야 할 것이다.

참고문헌

[1] G. Caronni, "Assuring ownership right for digital images.", Proc. Reliable IT Systems, VIS'95. Vieweg Publishing Company, 1995

[2] B.M.Macq and J-J Quisquater. "Cryptology for digital TV bradcasting." Proc. of the IEEE, 1995

[3] W. Bender, D. Gruhl, N. Morimoto. "Techniques for data hiding." Proc. of SPIE, Vol 2420, 1995

[4] E. Koch and Z. Zhao, "Copyright protection for multimedia data" Proceeedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, June 1995

[5] Yu Zin Zhang, Ting Chen, Juan Li, "Embedding Watermarks into Both DC and AC Components of DCT", Proceeding of SPIE, 2001

[6] Mohammed A. Al-Mohimeed, "Wavelet-Based Digital Watermarking", Proceeding of SPIE, 2001

[7] 강상익 "디지털 워터마킹 국내·국외 표준화 동향", TTA-저널, 제73권, pp. 138-145, 2001