□ 기술해설 □

디지탈 영상의 저작권 보호

동국대학교 원치선

1. 서 론

컴퓨터의 급속한 성능대비 가격하락과 WWW (World Wide Web) 등 컴퓨터 망의 확산으로 수많은 음성, 영상 및 비디오 데이타들이 디지탈화 되고 있다. 미디어에 대한 디지탈화의 추세는 디지탈 신호의 장점 (즉, 전송 및 저장시 발생되는 에러에 강하고, 편집 등 다기능이 용이) 때문에 더욱 가속화되고 있다. 그러나 신호의 디지탈화는 다음 두 가지의 새로운 문제를 발생시킨다. 첫번째 문제점은 영상, 특히 비디오 데이타를 디지탈화 하는 경우 발생되는 데이타 량이 폭발적으로 증가한다는 것과, 둘째, 정보를 디지탈화 하여 표현하므써 원본과 복사본 그리고 변형본의 구분이 불가능해 진다는 점이다. 첫번째 문제점은 영상데이타 압축기술과 함께 해결되고 있고, JPEG, MPEG-1, 2, 4 등의 국제적 표준안으로 결실을 맺고 있다. 그러나 두번째 문제인 디지탈 영상물의 저작권 보호와 인증(authentication)에 대한 해결책은 아직도 모두가 인정할 만한 방법이 제시되지 않고 있다.

디지탈 영상물의 정보보호를 위해 적용할 수 있는 보안책은 그림 1에서 보는 바와 같이 세 가지로 나눌 수 있다[1]. 첫번째 보안책은 기존의 공통키 또는 공개키 암호화 알고리즘을 이용하여 주어진 데이타를 암호화하는 것으로 영상을 원래의 데이타로 복원하려면 관련키를 알고 있어야 한다. 이 방법의 적용 예는 가입자 개념의 유료 방송 시스템(conditional access system)에서 찾아 볼 수 있다. 즉, 정당한 가입자들은 해독키를 갖고 있어 정상적인 영상을 볼 수 있으나, 비가입자들은 스크램블(scramble)된 비정상적인 영상밖에 볼 수 없다. 두번째 영상정보보호 방법으로 보호 대상 영상정보에 대한 접근제어용 방화벽(firewall)을 구축하는 것이다. 마지막으로 세번째 방법은 디지탈 영상의 불법적인 내용 조작을 막고, 영상의 소유권을 보장할 수 있는 디지탈 워터마크(watermark) 방법이다.

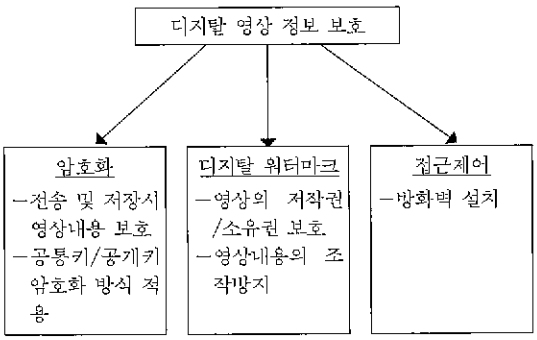


그림 1 디지탈 영상정보 보호의 분류

본고에서는 디지탈 영상 및 비디오의 저작권 보호와 인증에 대해 지금까지 제안된 기법들을 살펴보고 앞으로의 발전발향을 제시한다. 참고로 멀티미디어 환경에서 영상뿐만이 아니라 음성 및 문자 등의 데이타에 대해서도 저작권 보호와 인증의 방법이 똑같이 적용될 수 있으나, 본고에서는 특히 영상 및 비디오 데이타에 대해 한정해서 살펴보기로 한다.

2. 워터마크를 이용한 디지탈 영상의 저작권 보호

2.1 워터마크의 정의 및 구비 조건

워터마크는 저작권 보호를 위해 영상 데이타에 표시한 보이지 않는 마크를 말한다. 즉, 주어진 원 영상 I에 라벨(label) $S=\{S_1, S_2, \cdots,\}$를 부호화 과정 E를 통해 부착하면 워터마크가 찍힌 영상 $\hat{I}=E(I, S)$를 얻을 수 있다[2] [3]. 이때 라벨 S는 영상에 표시된 워터마크가 된다. 테스트 영상 J(워터마크가 찍혔거나, 안 찍혔거나, 혹은 훼손된 영상)에 대한 소유권을 판정하는 과정은 워터마크 삽입과정의 역과정으로 J나 원영상 I를 입력으로 받아 복호화 과정 D를 통해 라벨 $S'=D(I, J)$를 추출한다. 추출된 라벨 S'는 소유권을 주장하는 자가 비밀로 보관하고 있는 라벨 S와 비교기 $C_\delta(S', S)$에 입력하여 소유권의 유무가 판정된다. 이때 비교기 $C_\delta(S', S)$는 두 라벨의 상관관계를 계산하는 것으로 계산된 유사도가 δ를 넘으면 소유권자로 판정한다. 따라서 워터마킹의 구성요소는 (E, D, C_δ)가 되며 이들 구성요소들을 각각 어떻게 설정하느냐에 따라 여러 가지의 워터마킹(watermarking) 방법이 존재하게 된다. 이들 가능한 워터마킹 기법들은 다음의 기본적인 요구조건을 만족해야 한다[4] [5] [6].

i) 무감지성(Invisibility) : 디지탈 영상에 찍힌 워터마크를 육안으로 확인할 수 없어야 한다. 즉, I와 $\hat{I}$는 육안으로 구분될 수 없어야 한다.

ii) 보안성(Security) : 워터마크의 삽입과정이 알려져 있다 해도 관련된 파라미터 값들을 알고 있지 않는한 불법적으로 워터마크를 삭제하려는 시도는 불가능해야 한다.

iii) 강인성(Robustness) : 워터마크가 찍힌 영상은 그 이후의 다양한 의도적 또는 비의도적 영상변형에 의해 삭제되어서는 안된다. 예를 들어, 전송 및 저장시 발생되는 에러나 손실압축 환경에서 발생하는 압축에러, 그리고 필터링(filtering), 크로핑(cropping) 등의 영상처리 과정에 의해 워터마크가 지워져서는 안된다.

iv) 명확성(Unambiguity) : 워터마크가 찍힌 영상에 대해 명확히 소유권을 증명할 수 있는 방법이 있어야 한다. 때에 따라 여러 불법 사용자들이 자신이 임의로 만든 워터마크를 워터마크가 이미 찍힌 영상에 재삽입하여 소유권을 주장하는 충돌이 발생하는 경우에도 영상의 실제 소유권자를 구별할 수 있어야 한다.

2.2 공간 영역에서의 워터마크

원 영상의 밝기의 세기를 변화시키거나 영상내 임의의 패턴을 삽입하는 공간영역의 워터마킹 기법중에 가장 간단한 방법은 각 픽셀에서의 그레이레블(gray-level) 값의 LSB(Least Significant Bit)를 발생된 난수에 의해 바꾸므로써 영상공간내 밝기 값의 LSB에 서명문양을 숨기는 방법이다. 그러나 이 간단한 방법은 워터마크가 찍힌 영상에 대한 압축손실, 전송에러, 편집, 및 특수처리 등에 아주 약하다는 단점을 갖고 있다. 즉, LSB에 워터마크를 삽입한 영상을 DCT(Discrete Cosine Transform) 등을 사용하는 손실 압축 부호화를 행하면 DCT 계수의 양자 화에 의해 LSB에 삽입된 워터마크가 삭제될 수 있다. 이 단점을 극복하기 위해 인간의 시각 특성을 활용할 수 있다. 즉, 인간 시각의 마스킹(masking) 효과[6] [7] [8]에 의해 영상 내에 텍스쳐(texture) 영역이나 윤곽선 둘레의 밝기 값의 변화를 육안으로 잘 구별할 수 없다는 점을 이용하여 그 부분에 대해 영상밝기 값을 특별히 더 많이 변화시킴으로써 워터마크 검출시 신뢰도를 높이는 효과를 얻는다. 좀 더 복잡한 방법으로 영상 소유권자만 알고 있는 이진 패턴에 의해 이진수 "1"을 갖는 픽셀 위치의 밝기 값만 변형을 가하는 방법으로, 고주파성분을 제거하므로써 압축효과를 얻는 압축방법에 의한 압축손실에 강하게 하기 위해 픽셀이 아닌 블록 단위로 패턴을 만들고 블록내 평균 밝기 값을 변형시키는 방법[9]과 블록의 특성분류를 이용하는 방법[10] 등이 있다.

2.3 주파수 영역에서의 워터마크

인간시각의 마스킹(masking) 효과를 더 효율적으로 활용하기 위해서는 공간영역의 그레이레블 값을 이용하는 것보다 주파수 영역에서 주파수의 범위에 따른 인간시각의 서로 다른 특성을 이용하는 것이 더 유용하다. 즉, DCT(Discrete Cosine Transform)나 DFT(Discrete Fourier Transform), 혹은 웨이브릿 변

환(Wavelet Transform)을 통해 얻은 주파수 성분의 계수에 워터마크를 삽입하므로써 영상내 텍스쳐(texture) 영역과 같이 시각적으로 덜 민감한 고주파 성분에 적응적으로 워터마크를 삽입할 수 있다[11]. 또한 단일 주파수 성분을 변환시키므로써 변환블록내 밝기의 값 전체에 영향이 파급되고, 따라서 불법적인 공격에 강한 워터마크를 만들 수 있다. 그러나 텍스쳐 영역과 같이 인간 시각적으로 덜 민감한 부분에 워터마크를 삽입하는 방법은 오히려 압축손실이나 필터링(filtering)에 의해 쉽게 제거될 수 있다. 기존의 영상압축 기법이 인간시각에 덜 민감한 고주파 성분을 많이 압축한다는 점을 고려할 때, 오히려 워터마크가 감지될 수 있는 위험이 있지만 시각적으로 민감하고 중요한 영상데이타에 워터마크를 삽입하는 것이 더 압축손실에 강하다[5]. 문제는 영상의 변화를 감지할 수 없도록 하면서 어떻게 워터마크를 시각적으로 중요한 영역에 삽입하는냐는 것이다. 이 문제를 해결하기 위해 영상 데이타와 같은 주파수 대역(spectrum)을 갖는 통신채널에 워터마크가 신호로서 통과한다고 간주하면 워터마크(즉, 신호)에 대한 불법적 공격이나 필터링 및 압축손실 등은 통신채널에 가해지는 잡음(noise)으로 모델링할 수 있으며, 이들 잡음을 극복할 수 있는 효과적인 전송 방식은 대역확산통신(spread spectrum communication) 방식을 도입하는 것이다[5]. 즉, 신호(워터마크)를 전송 채널(영상)이 갖고 있는 여러 주파수 영역으로 확산하므로써 어떤 특정 주파수 대역의 에너지는 감지할 수 없을 정도로 작지만 주파수의 위치와 변화량을 알고 있는 소유권자에 의해 산재해 있는 주파수 성분을 모으면 높은 신호 대 잡음 비로 신호(워터마크)를 검출할 수 있다. 이와 같이 워터마크를 영상의 대역폭내 스펙트럼에 확산시키므로써 워터마크가 존재하는 위치가 불분명해지고 시각적으로 중요한 주파수 성분에도 워터마크를 넣을 수 있어 더욱 강인한 워터마크를 만들 수 있다.

2.4 압축공간에서의 워터마크

급속히 증가하는 디지탈 비디오물을 저장하는데 필요한 엄청난 데이타 량을 고려하여 디지탈 비디오는 MPEG-2와 같은 압축기법에 의해 압축된 형태로 저장해야 한다. 이와 같이 대부분의 디지탈 비디오 데이타가 압축된 형태로 저장 및 전송될 것으로 예상되므로 압축된 데이타를 복호화하여 얻은 비압축된 영상에 워터마크를 찍고 다시 압축하여 전송하는 것은 복호화 및 부호화 과정을 추가적으로 요구하므로 바람직하지 못하다. 따라서 압축된 비트 스트림에 직접 워터마크를 삽입하는 방법이 필요하다. 워터마크를 압축된 비트 스트림에 직접 삽입하는 문제는 기존의 공간영역에서의 워터마크 삽입 문제와는 달리 새로운 요구조건을 만족시켜야 한다. 즉,

i) 일정 비트 율의 유지 : 압축 비트 스트림에 워터마크를 가하는 것이 비트 율을 증가시켜서는 안된다. 만약 워터마크의 삽입이 압축 비트 스트림의 비트 율을 증가시키면 디코더(decoder) 하드웨어에 있는 버퍼(buffer)가 넘칠 수도 있고, 오디오와 비디오 사이의 동기도 흐트러질 수 있다.

ii) 실시간 실행 : 압축된 데이타에 직접 워터마크를 삽입하고 검출하는 것은 계산시간이 많이 요구되는 복호화→워터마크 삽입→재압축의 과정을 거치지 않으려는 시도이므로 실시간 실행을 전제로 한다.

iii) 압축 안된 원 영상 데이타를 사용하지 않고도 워터마크의 추출이 가능해야 한다.

iv) 상호운용성 : 소유권 확인을 위한 워터마크 검출은 압축 및 비압축 비디오에 대해 모두 가능해야 한다.

MPEG-2 비트 스트림에는 사용자 데이타부(user-data)가 있어 워터마크를 이 사용자 데이타부에 부착할 수도 있으나, 이 경우 비트 전송율이 증가되고 사용자 데이타부가 전송 도중 비트열로 부터 제거될 수도 있으므로 압축된 데이타 열에 직접 워터마크를 삽입하는 것이 바람직하다. MPEG-2로 압축된 비트 스트림에 워터마크를 삽입하는 한가지 방법은 DCT 블록의 DC 계수들을 워터마크 신호의 DC 계수와 배타적 논리합을 취하는 것이다[12]. 즉, 변화에 민감한 움직임 벡터나 다른 부속 정보는 그대로 두고 DCT 계수 값들만 주

어진 워터마크의 DCT 계수들로 변형을 가한다. 이때 새롭게 바뀐 DCT 계수의 가변길이 부호화 결과가 워터마크 삽입 이전의 그것과 비교하여 길이가 늘어나지 않은 경우만 워터마크가 부착된 비트를 취하고 그렇지 않은 경우 일정 비트 율을 유지하기 위해 워터마크가 찍히지 않은 원래의 DCT 부호화 비트를 그대로 유지한다. MPEG-2 압축 방법은 움직임 보상 압축 기법을 기반으로 하므로 워터마크에 의한 DCT 계수에 대한 변화의 누적은 연속된 프레임에 영향을 줄 수 있다. 따라서 압축영역에서의 워터마크 기법은 이와 같은 드리프트(drift) 문제를 해결할 수 있어야 한다.

3. 영상 정보의 인증

디지탈 영상정보의 인증(authentication)은 수신된 영상이 전송 도중 불법으로 내용의 일부가 바뀌지 않았다는 것을 수신자로 하여금 확인할 수 있도록 하는 기법으로 수신된 영상의 전송자도 확인할 수 있는 추가적인 기능을 갖는다[13]. 즉, 워터마크가 영상을 만든 사람의 소유권을 보호하는데 비해 영상인증을 위한 서명(signature)은 수신자를 보호하려는 것이다[3]. 수신된 디지탈 영상정보가 전송도중 그 내용이 바뀌지 않았다는 것을 확인할 수 있는 가장 간단한 방법은 체크섬(checksum) 기법을 이용하는 것이다. 즉, 인증을 위한 서명 대상 데이타가 디지탈 영상인 경우 그것의 방대한 데이타량 때문에 모든 영상 데이타에 서명할 수 없고 체크섬 즉 해쉬값(Hash value)에 대해서만 서명하는 기법을 사용한다. 이때 서로 다른 두 영상이 같은 체크섬을 가질 확률은 체크섬에 할당된 비트 길이에 의해 결정되며 24비트인 경우 1/16,777.216이 된다. 원 영상으로부터 추출된 체크섬은 부가정보로서 원영상 데이타에 추가로 전송/저장되거나 체크섬값 자체를 마치 워터마크 처럼 원영상에 삽입하여 영상정보의 인증뿐만이 아니라 저작권 보호의 기능을 동시에 수행할 수 있다. 해쉬(Hash) 함수를 이용한 영상인증의 응용 예로 디지탈 카메라로 찍은 사진의 내용을 조작할 수 없도록 다음과 같은 과정을 통해 인증할 수 있다[14].

i) 디지탈 카메라로 촬영한 영상에 대해 카메라내에서 해쉬함수를 이용하여 영상 해쉬값을 얻는다.

ii) 영상 해쉬값을 디지탈 카메라 내에 안전하게 보관되어 있는 비밀키로 암호화하여 디지탈 서명 값을 얻는다.

iii) 디지탈 카메라로부터 취득한 영상을 외부의 저장 매체에 저장하거나 전송할 때는 영상데이타와 함께 암호화된 디지탈 서명 값도 같이 전송/저장한다.

iv) 주어진 테스트 영상이 해당 카메라로 촬영되어 내용이 변경/조작되지 않았음을 인증하기 위해 공개된 인증 프로그램을 실행한다.

v) 인증 프로그램은 인증 대상 영상과 그것의 디지탈 서명 값 그리고 카메라 외부에 기록된 공개키로 디지탈 서명을 해독한다.

vi) 해독된 디지탈 서명 값은 원 영상의 영상 해쉬값이며 이 값을 인증 대상 영상으로부터 직접 계산한 해쉬값과 비교한다.

vii) 두개의 영상 해쉬값이 서로 같으면 원영상의 내용이 변경/조작되지 않았음이 확인된다.

4. 결론 및 향후전망

점점 더 많은 비디오 데이타가 디지탈화되어 전송 및 저장되면서 멀티미디어 시대가 앞당겨지고 있지만, 이에 따른 저작권 및 내용인증 문제의 발생에도 대비해야 한다. 즉, 디지탈 비디오는 쉽게 복제되며, 복제물은 원영상과 동일하고, 복제된 영상물은 컴퓨터 망을 통해 쉽고 빠르게 불법 유통될 수 있다. 또한 디지탈 영상처리 기술의 발전으로 원영상의 내용을 간단하게 변경 또는 조작할 수도 있다. 이와 같이 예상되는 문제들을 해결하기 위해 디지탈 영상의 저작권을 보호하기 위한 워터마크를 삽입하고, 디지탈 영상물의 내용증명을 위해 인증방법이 도입되고 있다. 디지탈 영상의 저작권 보호를 위한 워터마크는 그림 2와 같이 디지탈 통신의 대역확산(spread spectrum) 개념을 이용한 워터마크 기법이 압축손실을 포함한 여러 영상 데이타 처리에 강하고 원영상 훼손

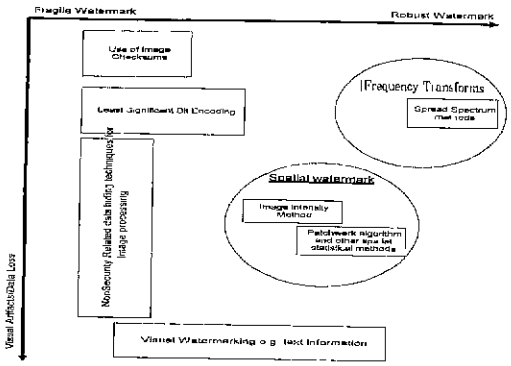


그림 2 디지탈 워터마크 기술의 원영상 손실 대비 강인성

정도에 따른 성능 면에서도 뛰어난 것으로 분류되어 이 기법이 앞으로 많이 활용될 것으로 기대되며, 저작권 보호와 더불어 내용인증을 동시에 수행할 수 있는 기법들도 제안되고 있다.

워터마크 기법의 또 한가지 연구방향은 복수의 저작권 소유 주장에 대한 해결 방안의 모색이다. 예를 들어, Alice에 의해 워터마크가 삽입된 영상에 대해 Bob이 다시 워터마크를 넣는 경우 Alice와 Bob은 모두 주어진 영상에서 자신의 서명라벨을 추출할 수 있으므로 소유권을 주장할 수 있다. 이 경우 Alice와 Bob중 어느 쪽이 진짜 소유자인지를 판가름 할 수 있어야 한다. 한 가지 방법은 Alice와 Bob이 각각 자신의 원영상을 갖고 있는 경우 Alice는 Bob에게 Bob이 소유하고 있는 원영상으로부터 Alice의 서명라벨을 추출하도록 하고, 반대로 Bob은 Alice에게 Alice가 갖고 있는 원영상에서 Bob의 서명라벨을 추출할 것을 요구하면 Bob이 소유하고 있는 원영상은 실제로는 Alice가 이미 워터마크를 삽입한 영상이므로 Bob의 원영상으로부터 Alice의 서명라벨이 검출되나, Alice의 원영상에서는 Bob의 서명라벨이 검출되지 않으므로 Alice가 진짜 소유권자임이 판명된다. 위의 경우와 같이 복수의 저작권 소유 주장에 Alice는 원영상을 소유하고 있으므로 이를 이용하여 소유권 주장을 할 수 있었다. 그렇다면, 보안을 확신할 수 있는 신뢰당국에 원영상을 등록 보관하면 소유권 주장을 할 수 있는데 구태여 워터마크를 도입하는 이유가 무엇인가. 이 의문에 대한 답변은 다음의 워터마크의 한 응용 예로부터 불식될 수 있다. 즉, 원영상의 소유권자(Alice)가 영상의 복사본을 판매할 때 각 영상에 서로 다른 워터마크를 삽입하므로써 후에 불법 복사물이 누구에 의해 불법 유통되었는지를 판정할 수 있다[2].

참고문헌

[1] Wong, S., "Image security", http : // www.ece.curtin.edu.au/~wongsc/digital.htm, 1997.

[2] Craver, S., el al., "Can invisible watermarks resolve rightful ownership?", *Proc. of SPIE*, vol 3022, pp. 310~321, 1997.

[3] Macq, B. M. and Quisquater, J. J., "Cryptology for digital TV broadcasting," *Proc. of IEEE*, vol. 83, No. 6, pp. 944~957, June 1995.

[4] Hartung, F. and Girod, B., "Copyright protection in video delivery networks by watermarking of pre-compressed video," *Lecture note in computer science*, vol. 1242, pp. 423~436, Springer, Heidelberg, 1997.

[5] Cox, I. J., et al., "Secure spread spectrum watermarking for multimedia," NEC Research Institute, Technical Report 95~10, 1995.

[6] Tewfik, A. H., "Data hiding for multimedia personalization, interaction, and protection," *IEEE Signal Processing Magazine*, pp. 41-44, July 1997.

[7] Bender, W., et al., "Techniques for data hiding," MIT Media laboratory, Cambridge, MA, USA, 1995.

[8] Goffin, F., et al., "A low cost perceptive digital picture watermarking method," *Proc. of SPIE*, vol. 3022, pp. 264~277, 1997.

[9] Nikolaidis, N. and Pitas, I., "Copyright protection of images using robust digi-

tal signatures," *Proc. of ICASSP*, vol. 4, pp. 9,168~9,171, May 1996.

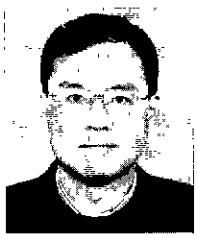
[10] 서정일, 우석훈, 원치선, "디지탈 영상의 저작권 보호를 위한 새로운 서명문양," 한국통신학회논문지, 제22권 제8호, pp. 1,814~1,822, 1997.

[11] ORuanaidh, J.J.K., et al., "Watermarking digital images for copy right protection," *IEE Proc. Vis. Image Signal Process.*, Vol. 143, No. 4, pp. 250~256, 1996.

[12] Hartung, F. and Girod, P., "Watermarking of MPEG-2 encoded video without decoding and re-encoding," *Proc. of SPIE*, vol. 3027, pp. 264~274. 1997.

[13] Walton, S., "Image authentication for a slippery new age," *Dr. Dobb's Journal*, pp. 18~26, 1995.

[14] Friedman, G.L., "The trustworthy digital camera : restoring credibility to the photographic image," *IEEE* 1993.



원 치 선

1982 고려대학교 전자공학과 졸업
1986 Univ. of Massachusetts/Amherst, 석사
1989~1992 금성사 선임연구원
1990 Univ. of Massachusetts/Amherst, 박사
1992~현재 동국대학교 전자공학과, 조교수, 부교수
관심분야 : 영상분할기반 영상압축, 디지탈 비디오 검색, 영상보안