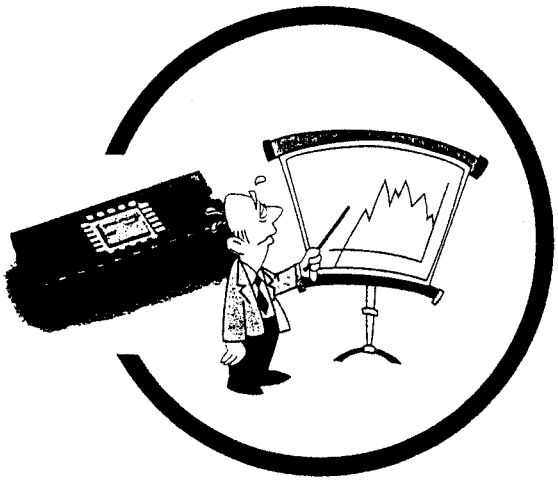


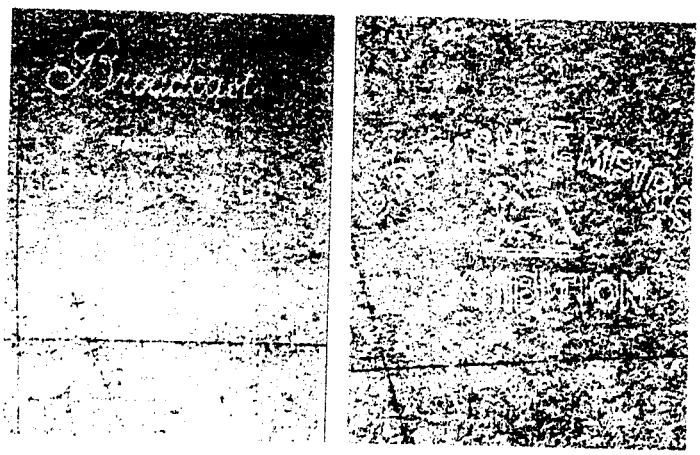
디지털 워터마킹 기술의 이해

호 요 성 교수
광주과학기술원
hoyo@kjist.ac.kr

- 디지털 워터마킹 기술의 이해
- 비디오 워터마킹 기술
- 디지털 오디오 워터마킹의 H/W 구현
- 디지털 방송과 IPMP 기술

1. 워터마크의 역사

워터마크(Watermark)의 기원은 1292년 가장 오래된 워터마크가 삽입된 종이가 발견된 이탈리아의 Fabriano 지방으로 거슬러 올라간다. 13세기말 대략 40개 정도의 제지 공장이 Fabriano 지방의 제지 시장을 공유하고 있었는데, 이들은 각기 다른 형태, 제질, 가격으로 종이를 생산하고 있었다. 그 당시 제지 공장들이 생산한 종이의 표면은 매우 거칠어서 무언가 기록하기에 적절하지 못했다. 이러한 종이를 전달받은 기술공들은 캘린더(Calender)라는 압착 롤러의 도움으로 표면을 매끄럽게 만들었다. 이렇게 가공된 종이는 상인들에게 팔렸으며, 이들은 높은 수익을 목적으로 거대한 창고에 저장하였다. 제지 공장들 뿐만 아니라, 기술공과 상인들 사이의 경쟁은 매우 치열했으며, 그들 중 누구도 종이의 출처, 즉 형태와 제질을 추적하기 어려웠다. 워터마크의 도입은 이러한 혼란을 해결할 수 있는 완벽한 방법이었다 (그림 1 참조 [1]). 그 이후 워터마크는 이탈리아와 유럽 전역으로 급속히 확산되었다. 워터마크는 초기에 종이의 상표나 제지 공장을 나타내는데 사용되었지만, 그 이후 종이의 형태, 제질, 강도를 나타낼 뿐만 아니라, 생산 날짜와 조작 여부를 가려내는 방법의 기반이 되었다 [2].



〈그림 1〉 종이에 삽입된 워터마크의 예 (1924년 대영제국 전시회 샘플

은행권이나 인지에 사용되던 워터마크는 디지털 컨텐츠에 "워터마크"라는 개념을 사용할 수 있도록 고무하였다 [3]. 디지털 영상의 워터마킹에 초점을 맞추었던 최초의 논문이 1990년 Tanaka et al. [4], 1993년 Caronni [5]와 Tirkel et al. [3]에 의해 발표되었다.

1995년 이래 디지털 워터마킹은 관심이 고조되어 매우 빠르게 발전되어 왔으며, 실제적인 동작 방법과 시스템이 개발되고 있다. 디지털 워터마킹은 여전히 발전될 여지가 다분히 남아있다.

2. 워터마킹의 정의와 워터마킹의 필요성

최근 오디오, 정지영상, 등영상과 같은 디지털 컨텐츠의 저작권 보호의 필요성이 대두됨에 따라 워터마킹에 대한 관심이 고조되고 있다. 디지털 컨텐츠는 다양한 이점들을 제공해 주지만, 원본과 동일한 대량의 복사본이 불법적으로 배포될 수 있다는 사실은 저작권 보호에 심각한 위협이 되고 있다. 워터마킹은 소유자 확인(Owner Identification), 특허권 사용료 지불(Royalty Payment), 원본 조작 여부 인증(Authentication)에 사용된다.

여기서 워터마킹이란 오디오, 정지영상, 비디오 신호 등의 멀티미디어 데이터에 귀에 들리거나 눈에 보이지 않도록 데이터의 소유권 정보를 삽입하는 과정으로, 일단 워터마킹된 데이터는 권한이 없는 사용자에게 통계적으로 소유권 정보의 검출이 불가능해야 하며, 신호처리 필터링이나 정보압축 동작에 의해 신호가 변형되더라도 소유자에 의해서는 소유권 정보의 검출이 가능해야 한다.

3. 워터마킹의 분류

시각적 워터마크(Visible Watermark)는 로고와 같이 정지영상이나 비디오 신호에 삽입되거나 중첩되는 시각적인 패턴으로 기존의 로고와는 달리 신호의 일부분을 간단하게 잘라냄(Cropping)으로 워터마크가 제거되지 않도록 보호되어 있다. 이러한 시각적 워터마크는 원본의 화질을 열화시키며, 관련되는 프로그램이나 장치를 이용하여 자동으로 검출될 수 없고, 단지 시각적으로 워터마크의 존재 여부를 확인할 수 있다는 단점을 가지고 있다. 그러나, 지도, 그래픽, 소프트웨어 사용자 인터페이스 등과 같은 특별한 컨텐츠에 널리 사용되고 있다 [6].

반면, 비시각적 워터마크(Invisible Watermark)는 열화가 생기지 않도록 투명하게 컨텐츠에 삽입된다. 눈에 띄지 않도록 정보를 삽입하려면 삽입되는 데이터의 양이 제한되는데, 이때 인간의 시각 모델(Human Visual Model)을 이용하여 그 최대량을 예측한다 [7, 8].

영상 신호에 데이터를 숨기는 원리는 화소값, DCT (Discrete Cosine Transform) 계수 [9, 10], 웨이블릿 계수 [11, 7], 프랙탈, 비디오 신호의 움직임 벡터 등과 같은 신호 특성의 일부분을 수정하는 것이다.

공개 워터마크(Public Watermark)는 사용된 알고리즘만 안다면 잠재적으로 판독될 수 있다. 이러한 종류의 워터마크의 보안은 단순히 그 기술의 모호성에 달려있다. 따라서, 누군가 그 알고리즘에 대한 충분한 정보를 얻는다면, 전체적인 시스템은 잠재적으로 공개되고 만다. 공개 워터마크는 정

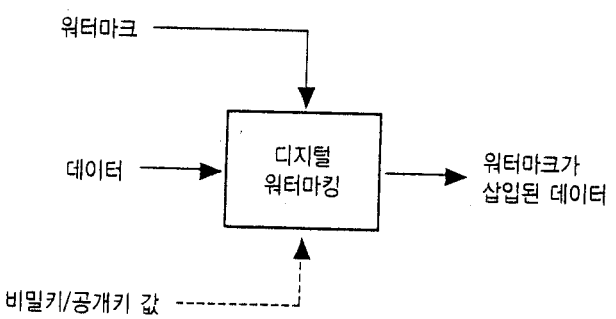
보의 보안은 사용된 알고리즘이 아니라 키 값에 달려있다고 하는 Kerckhoff 법칙에 따라 그 보안이 불투명하다.
조작이 불가능한 워터마크(Tamper-Proofing Watermark 또는 Fragile Watermark)는 컨텐츠의 무결정성(Integrity)을 입증할 수 있도록 해준다. 이 워터마크를 기반으로 한 무결정성 검사는 불법적인 목적으로 초래된 수정과 압축을 구별할 수 있다. 이 기술의 단점은 수정된 컨텐츠와 워터마크가 삽입되지 않은 컨텐츠를 구별하기 어렵다는 것이며 여전히 연구 과제로 남아있다.
비밀 워터마크(Private Watermark)는 비밀 키에 의해 보안이 유지된다. 비밀 키를 사용하지 않고 컨텐츠의 없이 비밀 워터마크를 제거하거나 변형시키는 것은 거의 불가능하다. 본 논문은 주로 비밀 워터마크에 초점을 맞출 것이다.

4. 워터마킹의 기본원리

워터마킹 시스템을 설계하는데 다음의 세 가지 주요 사항을 고려해야 한다 [12].

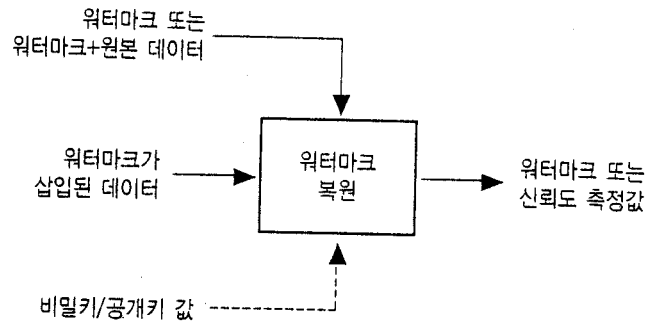
- 호스트 신호에 더해지는 워터마크 신호의 설계
- 워터마크 신호를 호스트 데이터에 삽입하는 알고리즘의 설계
- 키 값과 원본 데이터를 이용하여 워터마크가 삽입된 신호에서 워터마크 정보를 복원하는 검출 알고리즘의 설계

워터마크 신호 설계와 워터마크 신호 삽입 알고리즘 설계에 관한 처음 두 가지 고려사항은 삽입되는 워터마크가 호스트 신호에 따라 적응적으로 만들어질 때, 하나의 통합된 형태로 취급된다.
그림 1은 일반적인 워터마크 삽입 과정을 보여준다. 입력 신호는 워터마크, 호스트 데이터, 공개 또는 비밀키 값이다. 응용에 따라 호스트 데이터는 비압축 또는 압축된 형태이다. 대부분 제안된 방법들은 비압축 데이터 상에서 동작한다. 워터마크는 문자, 정지 영상 등과 같이 어떠한 형태도 가능하다. 비밀키 또는 공개키 값은 보완을 강화하는데 사용된다. 즉, 인증되지 않은 대상이 워터마크를 읽지 못하게 할 때, 키 값은 워터마크를 보호하는데 사용될 수 있다. 비밀키 또는 공개키 값과 조합되어 워터마킹 방법은 각각 비밀 워터마킹 또는 공개 워터마킹 방법으로 분류된다. 워터마크 삽입 알고리즘의 결과는 수정된, 즉 워터마크가 삽입된 데이터가 된다



〈그림1〉 워터마크 삽입 과정

그림 2는 일반적인 워터마크 복원 과정을 보여주고 있다. 입력 신호는 워터마크가 삽입된 데이터, 비밀키 또는 공개키 값, 워터마크 또는 워터마크와 원본 데이터이다. 워터마크 복원 알고리즘의 출력 신호는 복원된 워터마크 또는 원본 워터마크와 입력 데이터에 포함되어 있는 워터마크와의 유사성을 나타내는 신뢰도 측정값이 된다.



〈그림2〉 워터마크 복원 과정

대부분의 워터마킹 방법들은 대역확산 통신과 유사한 방법을 이용하고 있다. 이 방법은 호스트 데이터에 비해 상대적으로 작은 크기의 의사잡음 시퀀스를 더하여 워터마크를 삽입한다. 의사잡음 시퀀스는 상관관계 수신기(Correlation Receiver) 또는 정합 필터(Matched Filter)를 이용하여 검출될 수 있다. 의사잡음 시퀀스를 적절히 선택하여 적용하면, 오경보 확률(False Alarm)을 낮출 수 있다.

5. 워터마킹 기술의 응용

워터마킹 시스템이 순응해야 할 요구사항은 그 응용에 따라서 다르기 때문에, 요구사항과 알고리즘 설계에 따른 고려사항을 다루기 전에 워터마킹의 응용을 먼저 살펴본다. 비록 워터마킹 방법은 일반적으로 강인해야 하지만, 그 응용에 따라 요구되는 강인성의 중요도는 서로 다를 수 있다.

(a) 저작권 보호 (Copyright Protection)
저작권 보호는 워터마킹의 가장 두드러진 응용이다. 그 목적은 컨텐츠와 저작권 소유자의 정보를 삽입하여 다른 이들이 함부로 저작권 주장을 하지 못하도록 하는 것이다. 따라서, 워터마크는 올바른 저작권 소유자를 결정하는데 사용되며, 요구되는 강인성의 중요도가 매우 높다. 예를 들면, 웹 상에 쉽게 이용 가능한 영상에 대해 그 소유자가 저작권을 보호받기 원하는 경우 이러한 응용이 적용될 수 있다. 강인성과 더불어 다른 이들이 부가적으로 워터마크를 삽입하는 경우에 대해서도 저작권 보호를 할 수 있도록 고려해야 한다.

(b) 불법 배포자 추적을 위한 지문 (Fingerprinting)
지문은 컨텐츠 정보가 아닌 합법적 사용자에 대한 정보를 전달할 목적으로, 주로 컨텐츠의 초본 복사 진의를 입증한다. 이러한 응용은 불법적으로 배포되고 있는 컨텐츠의 복사본을 감시하거나 추적하는데 유용하며, 소프트웨어 제품의 일련 번호(Serial Number)와도 흡사하다. 지문은 초본으로 배포되는 각 복사본에 개별적으로 삽입된다. 이러한 배포는 각 초본 복사본을 비교하여 삽입된 마크를 쉽게 검출할 수 있으므로 그러한 공모에 안전하도록 (Collusion-Secure) 설계되어야 한다 [13]. 또한, 예를 들면, 특정 웹 Crawler가 저작권이 침해된 워터마크가 삽입된 영상을 검색하는 WWW (World Wide Web) 응용에 대해 쉽고 복잡하지 않도록 워터마크가 검출되어야 한다. 이러한 응용은 불법적인 공격 뿐만 아니라, 신호의 압축 처리에 대해 매우 강인해야 한다.

(c) 복사 보호 (Copy Protection)
앞으로의 멀티미디어 배포 시스템은 미디어의 불법적인 복사를 막을 수 있는 복사 보호 메커니즘을 보유해야 한다. 복사 보호는 개방된 시스템에 대해 매우 힘들지만, 밀폐된 또는 개인적으로 관리되

는 시스템에 대해 가능하다. 그러한 시스템에 대해 데이터의 복사 여부를 나타내는 워터마크를 이용할 수 있다. 예를 들면, DVD의 경우 데이터에 워터마크를 이용하여 복사 정보가 삽입되어 있다. 그에 순응하는 DVD 재생기는 "복사 불가"라는 정보를 담고 있는 복사 데이터에 대해 재생할 수 없다. "일회 복사"라는 워터마크를 담고 있는 데이터는 일회의 복사가 가능하며 더 이상의 복사를 할 수 없다 [14].

(d) 인증 (Authentication)

인증은 데이터의 수정 여부를 판단하는데 이용된다. 이러한 응용은 "조작이 불가능한 워터마크(Fragile Watermark)"를 통해 가능한데, 압축 처리에는 약간의 강인성이 있지만 다른 조작에 대해서는 손상되기 쉽다 [15]. 요구되는 강인성은 데이터의 형태나 응용에 따라 중요도가 다르지만, 워터마킹의 응용들 중에 강인성의 중요도가 가장 적다. 최근 인증에 관한 주목할만한 새로운 접근 방법들이 제안되고 있는데, 이 방법들은 블록 평균, 윤곽선 특성과 같은 데이터의 특성이 워터마크로 삽입되어 영상이 여전히 그러한 특성을 가지고 있는가를 검사한다. 수정된 영역의 확인이 중요하다면 이러한 방법들은 좀 더 높은 강인성을 요구한다.

6. 워터마킹의 요구사항

워터마킹의 응용과 목적에 따라 그 요구사항도 약간씩 다르다. 워터마크의 비지각성 (Imperceptibility)은 응용 목적에 관계없이 공통된 요구사항이다. 그 외의 요구사항들은 워터마킹 시스템을 설계할 때 고려되어야 한다.

(a) 비지각성 (Imperceptibility)

가장 중요한 요구사항 중에 하나는 워터마크의 지각적인 투명성으로 그 응용과 워터마킹 시스템의 목적에 무관하다. 워터마킹의 결과는 지각적으로 거슬릴 뿐만 아니라, 상업적 가치도 감소할 수 있다. 따라서, 인간의 시각 시스템(Human Visual System) 또는 인간의 청각 시스템(Human Auditory System)을 이용하여 비지각성을 유지하면서 워터마크의 에너지를 최대화 시킬 수 있는 방법을 설계하는 것이 매우 중요하다.

b) 강인성 (Robustness)

궁극적인 워터마킹 방법은 표준 압축 또는 불법적인 조작으로 발생되는 왜곡에 강인해야 한다. 실제적인 시스템은 강인성과 비지각성 또는 정보율과 같은 요구사항들과 적절한 타협을 해야 한다. 강인성의 중요도는 그 응용 목적에 따라 크게 영향을 받으며, 그 응용과 워터마킹의 요구사항에 관련하여 다음의 왜곡과 공격들이 고려될 수 있다.

- 신호 개선 (Signal Enhancement)
- 부가 잡음, 다중 잡음 (Additive or Multiplicative Noise)
- 선형 필터링 (Linear Filtering)
- 비선형 필터링 (Nonlinear Filtering)
- 손실 압축 (Lossy Compression)
- 국부 Affine 변환, 전역 Affine 변환
- 데이터 감소
- 데이터 혼합
- 이종 부호화 (Transcoding)
- D/A 변환, A/D 변환
- 다중 워터마킹 (Multiple Watermarking)
- 공모 공격 (Collusion Attack)
- 통계적 평균 (Statistical Averaging)
- 모자이크 공격 (Mosaic Attack)

워터마킹 설계의 기본 원리는 그러한 공격들에 충분히 강인해서 공격이 성공적으로 가해졌을 때 데이터의 상업적 가치에 손상되도록 하는 것이다.

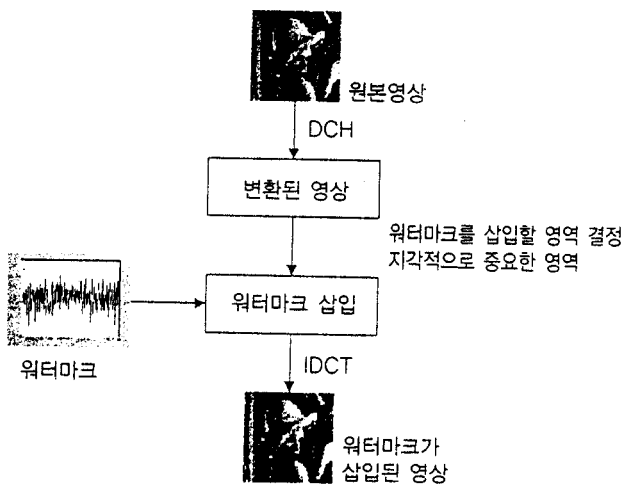
7. 워터마킹의 기본적인 방법

본 장에서는 워터마킹의 기본적인 방법으로 대역확산 워터마킹 기술을 소개한다. 대역확산 워터마킹 방법은 의사잡음(Pseudoran-dom Noise) 워터마크 패턴을 삽입하고, 상관성을 이용해 워터마크를 추출해 내는 방식이다. 즉, 워터마크를 영상이 가지고 있는 넓은 주파수 대역으로 확산하여, 어떤 특정 주파수 성분에서의 워터마크 에너지는 감지할 수 없을 정도로 매우 작다. 그러나 워터마크가 삽입된 위치와 내용을 알면, 산재되어 있는 워터마크 신호를 모아서 높은 신호 대 잡음 비 (Signal-To-Noise Ratio, SNR)를 가진 워터마크 신호로 검출 할 수 있다. 이렇게 영상의 스펙트럼 전역에 워터마크를 확산시키는 방식은 고의적 또는 비고의적인 공격에 대한 강한 강인성을 보장한다. 현재 많은 워터마킹 방법이 이 대역확산 워터마킹 방식을 사용하는데, 그 중 가장 잘 알려진 Cox 알고리즘 [9]을 살펴본다.

그림 3은 워터마크 삽입 과정을 나타낸다. 원래 영상 V에 워터 W마를를 삽입해서 워터마크가 삽입된 영상 V'를 얻는다. 이때 V'를 얻기 위해 삽입되는 스케일링 변수 ∂는 W가 V를 변화시키는 정도에 따라 결정된다.

$$v_i' = v_i(1+\partial w_i)$$

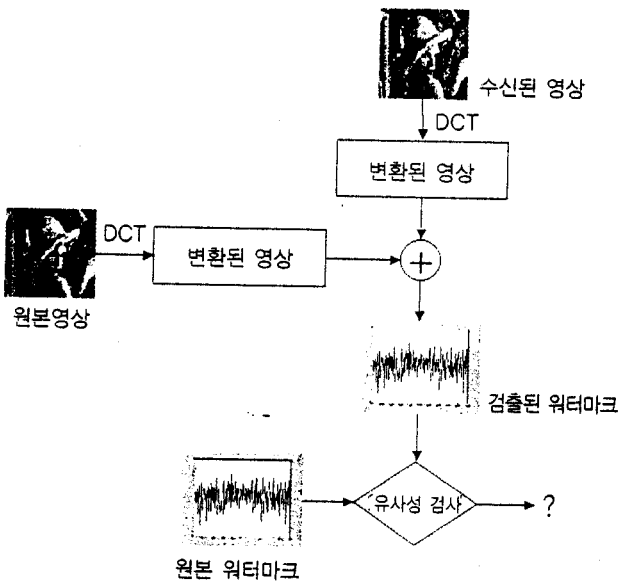
이때, v_i는 영상에서 지각적으로 중요한 주파수 성분을 나타낸다. 또한 워터마크 W는 연속된 실수 즉, $W=w_1,...,w_n$을 포함하며, 이것은 평균이 0이고 분산이 1인 정규 분로부터 독립적으로 선택된다.



〈그림3〉 워터마크 삽입과정

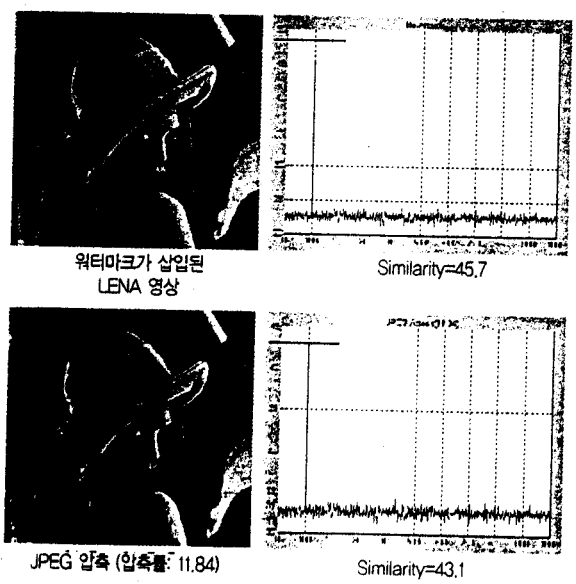
그림 4는 워터마크 추출 과정을 나타낸다. 원래 영상 V와 왜곡된 워터마크 삽입 영상 V^*로 왜곡된 워터마크 W^*를 추출할 수 있는데, 이 추출 과정은 워터마크를 영상에 삽입하는 것의 역 과정을 거친다. 만약 V^*가 V'와 다르면 (즉, 비고의적 왜곡이나 고의적인 공격을 받았을 경우), 추출된 워터마크 W^*는 원래 워터마크 W와 다를 것이다. 이때, W^*와 W^*의 유사성을 측정하기 위해 아래의 식을 사용한다.

$$sim(W, W^*) = \frac{W^* \cdot W}{\sqrt{W^* \cdot W^*}}$$



〈그림4〉 워터마크 추출과정

그림 5는 LENA 영상에 워터마크를 삽입했을 때의 영상과, 워터마크의 성능을 측정하기 위해 워터마크가 삽입된 영상을 JPEG 부호화를 했을 때의 영상, 그리고 그에 따른 워터마크 검출기의 반응(Watermark Detection Response)을 나타낸다. 이때 워터마크 검출기는 무작위로 발생시킨 1000개의 워터마크에 반응하도록 하였다. 그림 5에서 보듯이, 단지 한 개의 워터마크만이 검출되었으며, JPEG 부호화 후에도 여전히 워터마크가 남아 있음을 알 수 있다. 즉, 워터마크 삽입으로 인해 데이터의 손실 및 화질 열화가 발생하였지만, 공격에 대한 워터마크의 강인성을 어느 정도 보장할 수 있다.



〈그림 5〉 실험결과

참고문헌

[1] http://www.baph.freeserve.co.uk/watermarks/empire1924.html

[2] S. Katzenbeisser and F. Petitcolas, *Information HidingTechniques for Steganography and Digital Watermarking*, Artech House, MA, 2000.

[3] A. Tikel et al., "Electronic water mark," *Proc. DICTA 1993*, pp. 667-672, Dec. 1993.

[4] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multilevel image," *Proc. of the 1990 IEEE Military Commun. Conf.*, pp. 216-220, 1990.

[5] G. Caronni, "Ermitteln unauthorisierter Verteiler von maschinenlesbaren Daten," *Technical Report*, ETH Zurich, Switzerland, Aug. 1993.

[6] D. Augot et al, "Secure delivery of images over open networks," *Proc. of IEEE*, vol. 87, no. 7, pp. 1251-1266, July 1999.

[7] C. Podilchuk and W. Zeng, "Image-adaptive watermarks using visual model," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 525-540, May 1998.

[8] J. Delaigle, C. De Vleeschouwer, and B. Macq, "Watermarking algorithm based on a human visual model," *Signal Processing (Special Issue on Watermarking)*, vol. 66, no. 3, pp. 319-336, May 1998.

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

[10] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing (Special Issue on Watermarking)*, vol. 66, no. 3, pp. 283-302, May 1998.

[11] D. Kundur and D. Hatzinakos, "Toward a telltalt watermarking technique for tamper-proofing," *Proc. IEEE ICIP'98*, Chicago, IL, vol. 2, pp. 409-413, Oct. 1998.

[12] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. of IEEE*, vol. 87, no. 7, July 1999.

[13] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Trans. Inform. Theory, vol. 44, no. 5, pp. 1897-1905, 1998.

[14] J. Bloom et al, "Copy protection for DVD video," Proc. of IEEE, vol. 87, no. 7, July 1999.

[15] M. Schneider and S. Chang, "A robust content based digital signature for image authentication," *Proc. IEEE ICIP'96*, Lausanne, Switzerland, Sept. 1996.