# 인증과 무결성을 위한 DCT 기반 워터마킹

이혜란, 박지환

부경대학교 대학원 전자계산학과

# DCT Based Watermarking for Image Verification and Authentication

Hye-Ran Lee, Ji-Hwan Park

Dept. of Computer Science, PuKyong Nat'l University,

## 요 약

본 논문에서는 디지털 영상의 변조를 확인함과 동시에 변조의 위치를 확인하는 DCT 기반의 fragile watermarking을 제안한다. 디지털 영상의 인증과 무결성을 위해 기존의 Wong이 사용한 해쉬 함수와 비대칭키 암호 알고리즘을 사용하며, 영상에 DCT 변환을 함으로서 영상의 모든 픽셀에 워터마크를 삽입하지 않고서도 변조의 유무를 확인하는 것이 가능하다. 본 논문에서는 DCT 계수 중 일부 저주파 계수의 하위 비트에 워터마크를 삽입하여 워터마크의 비가시성과 연성을 만족하며 변조의 유무와 위치를 확인할 수 있게 된다.

## 1. 서론

최근에 통신망의 발달로 정보교환이 신속하게 이루어지고 있고, 멀티미디어 데이터의 사용이 증가되고 있다. 영상 데이터의 경우에도 기존의 데이터가 디지털화 됨에 따라 많은 편리성을 제공해 주고 있다. 하지만 디지털 영상은 복제가 용이하다는 것과 복제된 영상은 원 영상과 동일하다는 것, 디지털 영상에 대한 조작이 용이하다는 등의 부작용이 따르며 이에 따라 디지털 영상의 정보보호가 필요하게 되어진다.

디지털 영상의 정보보호는 크게 암호화 방법, 사이트 보호방법, 디지털 워터마킹 등이 있다. 암호화 방법은 공개키 방식의 암호 알고리즘 및 비밀키 방식의 암호 알고리즘이 메시지의 조작이나 변형을 방지하기 위하여 여러 분야에서 사용되고 있고, 디지털 워터마킹 방법은 사람의 눈으로 식별할 수 없는 정보를 영상 내에 삽입, 추출하는 과정으로 영상에 대하여 손실이 발생할 수 있지만 소유권자가 워터마크를 쉽게 추출하여 자신의 영상에 대한 소유권을 주장할 수 있는 방법을 제공한다. 또한 디지털 영상에 대한 인증(Authentication)과 무결성(Integrity)을 위한 디지털 워터마킹은 데이터의 내용이 조작되거나 변형되지 않았다는 것을 확인하면서 그 영상들의 송신자나 소유자의 확인이 가능한 방법을 제공한다[1].

디지털 워터마킹은 크게 공간 영역 워터마킹(spatial watermarking)과 주파수 영역 워터마킹(spectral watermarking)으로 분류할 수 있으며, 공간 영역 워터마킹 기술은 인간 시각이 영상의 밝기에 민감하지 않다는 것을 이용하여 영상의 픽셀 값에서 LSB를 조작하여 윤곽선의 밝기 값을 변화시키는 방법이다. 주파수 영역 워터마킹은 영상을 DCT, DWT, DFT 등으로 변화된 계수에 워터마킹하는 방법이다.

본 논문에서는 DCT를 이용한 주파수 영역 워터마

본 연구는 한국과학재단 지역대학 우수과학자 지원연구(과제번호:2000-1-51200-002-2)에 의해 수행된 결과의 일부임

킹 방법을 적용한다.

2장에서는 fragile watermarking에 대한 개념과 기존의 방법들에 대해 기술하고 3장에서는 DCT 변환을 이용하여 일부 저주파 계수의 하위 비트에 워터마크를 삽입하는 제안방법을 기술한다. 그리고 4장에서는 실험 결과를 통하여 제안방법을 평가하고 5장에서는 결론과 향후의 과제에 대하여 기술한다.

## 2. 관련연구

디지털 영상에서 fragile watermarking의 필요 조건은 다음과 같다.

① 영상의 변조 여부가 검출 가능해야 한다.
② 영상의 변조된 위치를 지정 가능해야 한다.
③ 원 영상 없이도 워터마크의 추출이 가능해야 한다.
④ 워터마크는 비가시적이어야 한다.

조건 ①과 ②는 robust watermarking과 구별되는 fragile watermarking의 특징이라고 할 수 있다.

디지털 영상의 인증은 수신된 영상이 전송도중 변형되었는지를 확인할 수 있는 기능으로 Digital Signature에 의한 방법과 Watermarking System에 의한 방법이 있다. Watermarking system은 영상을 다소 훼손시키는 단점은 있으나 다음의 장점을 가지고 있다.

① 워터마크는 영상에 직접 삽입되므로 부가적인 데이터를 보관할 필요가 없다.
② Digital Signature는 영상을 단순한 데이터 열로 간주하므로 영상의 독특한 구조를 활용하지 못하지만 워터마킹 시스템은 영상의 구조적인 특성을 활용할 수 있어 영상공간상 변조된 위치나 변조의 종류 등을 알 수 있다.

Yeung and Mintzer[2]에 의해 제안된 방법은 영상의 변조 유무 및 변조위치를 확인할 수 있다. 워터마크 검출시 원영상이 불필요하며 워터마크와 워터마크 검출함수로 워터마크 검출이 가능하다.

Fridrich[3]에 의해 제안된 방법은 robust watermark와 fragile watermark를 함께 삽입함으로서 악의에 의한 변조와 그렇지 않은 변조를 구분하는 것이 가능하다.

Wong[4]에 의해 제안된 방법은 영상의 조작여부 및 블록단위의 조작위치 확인이 가능하다.

1) 영상을 8×8블록으로 분할
2) 블록내 각 픽셀의 LSB를 떼어냄
3) 나머지 MSB비트와 영상의 크기정보를 입력으로 하여 해쉬함수 취함
4) 해쉬함수의 출력값과 watermark를 XOR 연산
5) 공개키 암호화한 후 영상의 LSB에 삽입

Scaling이나 Cropping등에 의한 영상의 크기변화의 검출이 가능하며, 정확한 공개키를 사용하면 해당 워터마크를 추출할 수 있다. 특정부위의 영상이 조작되면 워터마크 추출과정에서 해당 부위가 랜덤잡음과 같은 신호를 출력한다.

## 3. 제안 알고리즘

영상의 인증과 무결성을 위한 기존의 방법중 공개키 암호 알고리즘을 이용한 Wong의 방법이 있다. Wong의 방법은 영상을 인증하고 무결성을 증명하는 적합한 워터마킹 방법이지만 공간 영역에서의 워터마킹 기법을 사용하고 있으며, LSB에 워터마크가 삽입되어 LSB 공격에 취약하다는 단점을 가지게 된다. 제안 알고리즘은 기존의 Wong의 알고리즘에 DCT 변환을 적용하게 된다. 영상을 일정한 블록으로 나눈 후 DCT 변환을 하고, 저주파 계수의 하위 비트에 워터마크를 삽입하므로 블록내의 모든 픽셀에 워터마크를 삽입하지 않더라도 변조를 검출할 수 있다는 장점을 가지며, 영상의 화질도 상승시킬 수 있게 된다.

DC 성분에 워터마크를 삽입하는 것이 다른 주파수 성분에 워터마크를 삽입하는 것보다 더 강인하다는 결과가 있다[5]. DCT의 DC 성분에 워터마크를 넣는 것이 항상 가시적인 블록킹 현상을 유발하지는 않는다는 것과, 압축, 저역통과필터, A/D 변환등의 일반적인 영상처리에 대해 DC성분이 덜 영향을 받는 경향이 있다는 것이다. 본 알고리즘도 DC성분과 DC주위의 저주파 성분을 이용함으로서 변조의 검출이 용의할 뿐만 아니라 악의가 없는 영상처리에는 견고해 질 수 있다.

### 3.1 워터마크 삽입과 추출

그레이 레벨 영상을 기준으로 워터마크가 삽입 및 추출이 되며, 영상 X의 크기는 M×N 이다. 삽입될 워터마크 이미지 B는 I×H의 크기를 가지는 2진 영상이다. I×H는 워터마크 삽입 량에 따라 결정되어 진다. 먼저, 영상 X를 일정한 크기의 블록으로 분할하고, 각 블록별로 워터마크를 삽입하고 추출한다.

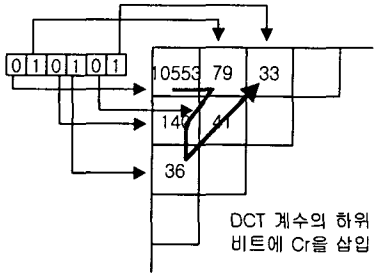
#### 3.1.1 워터마크 생성

원 영상을 일정한 크기의 블록으로 나누고 DCT 변환을 수행한다. DCT 계수 중 일부 저주파 계수의

하위 비트를 '0'으로 바꾸고, 그것을 X'로 표현한다. 영상의 크기 정보 M, N과 X'를 입력으로 하여 해쉬 함수를 적용하고, 해쉬 함수의 출력 값을 P라고 표현한다. 이진 워터마크 B와 P를 XOR하여 출력된 값 W를 가지고 공개키 암호화를 수행한다. 공개키 암호화를 통해 출력된 값 C가 영상에 삽입될 정보가 된다.

### 3.1.2 워터마크 삽입

영상 X의 각 블록을 DCT 변환해서 DCT 계수 중 일부 저주파 계수의 하위 비트를 '0'으로 바꿔 놓은 X'에 C를 삽입한다. 그림1은 저주파 계수의 하위 비트에 워터마크를 삽입하는 방법의 예를 보여준다.




10553 : 10100100111001 ← "0"

10100100111001=>10100100111
00010100100111000=>10552

그림2 DCT 계수의 하위비트에
워터마크를 삽입하는 예

블록에 IDCT를 하게되면 결국 워터마크된 영상 Y를 얻게 된다.

### 3.1.3 워터마크 추출

워터마크 추출은 먼저 각 블록에 DCT 변환을 한다. 일부 저주파 계수의 하위 비트를 추출하고 그것을 G라고 표시한다. 하위 비트를 추출하고 난 후 일부 저주파 계수의 하위 비트를 '0'으로 바꾸고, Z'라고 표시한다. 영상의 크기 정보와 Z'를 입력으로 하여 해쉬 함수를 수행하며 해쉬함수의 출력은 Q라고 나타낸다. G를 공개키로 복호화하여 U를 얻게 되며 Q와 U를 XOR하여 추출된 워터마크 O를 얻을 수 있다.

## 4. 실험 및 결과

본 논문에서 제안한 알고리즘의 효율성을 확인하기 위하여 그림2에 표시된 256×256 크기의 그레이 레벨 Lena(8bits/pixel) 영상을 원 영상으로 사용한다. 이진 워터마크 이미지는 128×64 크기의 로고 이미지로 그림3에 표시되어 있다. 실험을 위해서 MD5 해쉬 함수를 사용하며 RSA 공개키 암호화 알고리즘을 사용한다.

그림 2 원 영상

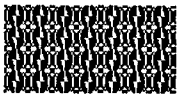


그림 3 워터마크

한 블록의 크기는 8×8로 하며 워터마크는 한 블록에 8비트, 4비트, 2비트, 1비트가 삽입된다. 워터마크가 삽입되는 위치는 DCT 계수를 지그재그 주사하는 순서로 선택되어 진다.

각 블록당 8비트의 워터마크가 삽입된 영상은 그림4에 표시되어 있고 PSNR은 53.102[dB]로서 50.549[dB]를 나타내는 Wong의 PSNR보다 향상되었음을 알 수 있다.

그림 4 워터마크된
영상(8bit)
(PSNR:53.102)

그림5는 워터마크 된 영상의 간단한 변조로서 모자의 꽃 장식을 여러 개 복사해 놓은 것이다. 그림6은 변조된 이미지에서 추출한 워터마크이며, 특정 블록의 로고가 깨어진 것을 알 수 있다. 로고가 깨어진 부분을 영상의 블록으로 나타낸 것이 그림7과 그림8이다.

그림 5 변조된 이미지

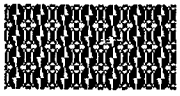


그림 6
추출된 워터마크

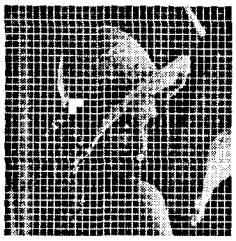


그림 7 이미지 블록의 변조 위치

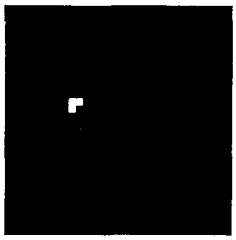


그림 9 변조 위치 측정

각 블록당 4비트, 2비트, 1비트의 워터마크가 삽입된 영상과 추출된 워터마크를 아래에 보여 주며 영상의 변조는 8비트 워터마크 삽입시와 동일하게 영상의 모자부분의 꽃 장식을 3개 복사한 것이다. 변조된 영상에서 추출된 워터마크로부터 변조된 블록이 깨어진 것을 알 수 있다.

그림 10 워터마크된 영상(4bit) PSNR:53.604

그림 11 추출된 워터마크

그림 12 변조된 영상으로부터 추출된 워터마크

그림 13 워터마크된 영상(2bit) PSNR:53.862

그림 15 추출된 워터마크

그림 14 변조된 영상으로부터 추출된 워터마크

그림 17 워터마크된 영상(1bit) PSNR:53.988



그림 16 추출된 워터마크

그림 18 변조된 영상으로부터 추출된 워터마크

각 블록당 8비트, 4비트, 2비트, 1비트의 워터마크를 삽입하여 영상의 변조 확인과 위치 측정이 가능한 것을 확인할 수 있음을 알 수 있다.

## 5. 결론

본 논문에서는 블록 내에 적은 양의 워터마크를 삽입하고도 변조의 유무와 위치를 측정할 수 있는 fragile watermarking 방법을 제안하였다. 단순히 하위 비트와 워터마크의 단순 대체가 아니라 영상에 DCT 변환을 통하여 적은 양의 워터마크를 영상의 중요한 정보를 가지는 영역으로 확산하는 방법을 제안하였다. 영상의 화질을 기존의 방법보다 향상시키면서 변조를 검출할 수 있는 방법이다. 향후의 과제로는 악의가 있는 변조에는 워터마크가 쉽게 깨어지면서 악의가 없는 영상 변형에는 워터마크가 견고해 질 수 있는 연구가 수행되어야 할 것이다.

## [참고문헌]


[1] D. Kundur and D. Hatzinakos, "Digital Watermarking for Telltale Tamper-Proofing and Authentication," Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87(7), pp. 1167-1180, July 1999.

[2] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in Proceedings of ICIP 97, pp. 680-683, 1997.

[3] J. Fridrich, "A Hybrid Watermark for Tamper Detection in Digital," Signal Processing and Its Applications, ISSPA, vol.1 pp. 301-304, 1999.

[4] P. W. Wong, "A public key watermark for image verification and authentication," in Proceedings of ICIP 98 (Chicago, IL), October. 1998.

[5] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding Image Watermarks in DC Components," IEEE trans. on CSVT, vol.10, no.6, pp.974-979, september. 2000.