정보학연구 제9권 제4호 2006년 12월(pp.49-55)
The Journal of Information Technology, Vol.9, No.4

산술부호화를 이용한 연성 워터마킹 기법

박성일* · 백승은** · 한승수***

목 차

Ⅰ. 서론

인터넷과 컴퓨터 네트워크가 널리 사용되면서 시공간을 초월하여 다양한 디지털 데이터들을 주고받는 것이 매우 손쉽게 이루어지게 되었다. 이러한 환경은 기존의 아날로그 환경에서 불가능하다고 여겼던 다양한 디지털 콘텐츠(오디오, 이미지, 비디오, 문서 등)의 창작과 조작을 가능하게 만들었다. 이러한 네트워크를 통한 디지털 데이터의 교류 활성화는 긍정적인 측면과 함께 부정적인 측면을 유발하게 되었는데 불법적으로 복제된 콘텐츠(contents)가 인터넷을 통해서 매우 빠른 속도로 많은 사람들에게 퍼져나가면서 콘텐츠 제공자의 수익 구조를 해치고 창작의욕을 떨어뜨리는 결과를 가져오게 되었다. 인터넷을 통한 다양한 콘텐츠의 유료서비스를 계획하거나 시행하기 위해서는 콘텐츠의 보안에 대한 요구가 증대되고 있으며, 몇 가지 방법을 이용하여 보안을 시도하고 있다.

대표적인 콘텐츠 저작권 보호기술로서 암호화 기술과 디지털 워터마킹 기술이 있다. 암호화 기술은 적법한 사용자에게만 암호화된 콘텐츠를 재생할 수 있도록 하는 기술로서 역시 복호화된 콘텐츠에 대해서는 보호할 방법이 없다. 워터마킹 기술은 콘텐츠 자체에 다양한 정보를 은닉하기 때문에 콘텐츠에 항상 따라다니는 정보라는 장점을 갖고 있다. 즉 워터마킹된 멀티미디어 콘텐츠를 암호화한 후 배포함으로써 복호화된 콘텐츠의 보호도 가능하게 되었다. 워터마킹 기술이 사용되는 응용분야는 다양하다. 삽입되는 워터마크의 용도에 따라서 저작권 정보를 워터마크로써 삽입하여 추후 법정에서 자신의 소유권을 주장할 수 있는 저작권인증, 콘텐츠의 불법 배포자를 찾아

* 명지대학교 정보공학과 박사수료
** 명지대학교 정보공학과 박사수료
*** 명지대학교 정보공학과 교수

내기 위한 핑거프린팅, 콘텐츠의 위변조 식별을 위한 콘텐츠인증, 불법적인 복제를 원천적으로 막는 복제방지, 워터마크를 기기제어를 위해 사용하는 기기제어 등으로 구분된다.

현재 연구되고 있는 디지털 워터마킹은 워터마크를 삽입하기 위한 방법이나 응용의 목적에 따라 크게 다음과 같이 분류할 수 있다.

워터마크의 삽입에 따른 변환식의 사용여부에 따라서 공간영역(Spatial Domain) 워터마킹과 주파수 영역(Frequency Domain) 워터마킹으로 나눌 수 있다.

그리고 워터마크 추출 시 원영상의 사용 여부에 따라서 원영상 없이 추출 가능한 블라인더(Blind) 워터마킹과 원영상과 워터마킹영상 둘 다 있어야 워터마크가 추출 가능한 넌 블라인더(Non Blind) 워터마킹 기법이 있다.

또 삽입된 워터마크의 강인성에 따라서 소유권 증명에 주로 사용되는 강인한(Robust) 워터마킹과 데이터 인증 기능 등에 응용되는 연약한(Fragile) 워터마킹이 있다.

그리고 삽입된 워터마크의 시각화에 따라 보이는(Visible) 워터마킹과 보이지 않는(Invisible) 워터마킹이 있다. 워터마킹 삽입 대상(콘텐츠)에 따라 이미지(Image), 오디오(Audio), 비디오(Video), 텍스트(Text), 2D/3D벡터(Vector) 워터마킹 등으로 분류하기도 한다.

본 논문에서는 영상의 인증과 무결성을 보장하는 연약한(Fragile)워터마킹 새로운 알고리즘을 제안하였다. 영상의 인증과 무결성에 사용되는 워터마킹 기술은 많은 연구자들에 의해서 개발되어져 왔다. 대표적인 방법으로는 Wong[1][2]등에 의해 제안된 암호학적 해쉬함수를 이용한 워터마킹 방법이다. 무결성을 보장하는 해쉬값을 계산하려면 법, 보수, 시프트, XOR 등 많은 논리 연산이 필요하다. 본 논문에서는 해쉬함수 대신에 곱셈에 의하여 계산되는 산술부호화를 사용하여 그 값을 무결성을 보장하는데 사용하였다. 그리고 또한 산술부호화는 영상압축분야에서 많이 사용하고 있으므로 직접 사용가능하다.

제안한 방법의 우수성을 검증하기 위하여 실험을 하였고, 해쉬함수를 이용한 워터마킹 방법과 비교하였다.

II. 본론

2.1. 산술부호화 기법

산술부호화기법[3][4][5]는 무손실압축에 흔히 사용하는 기법이다. 아래의 그림은 산술부호화 기법의 설명도이다.

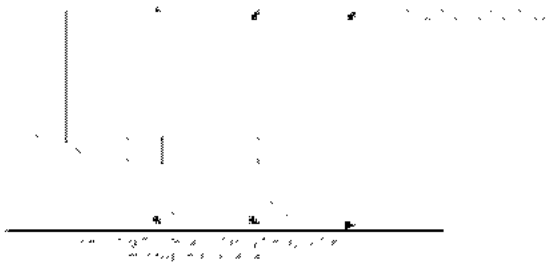

그림 1. 산술부호화 기법
fig 1. Arithmetic coding technique

그림에서 $a_1, a_2, a_3, \ldots$는 기호(symbol)이고 $F_{X(i)}$는 각 기호들의 확률($P(a_i)$)의 누적확률이다. 아래의 수식으로 누적확률을 계산한다.

$$P(X=i)=P(a_i) \quad (1)$$

$$F_{X(i)}=\sum_{k=i}^{i} P(X=k) \quad (2)$$

그림1에서 보면 입력되는 심벌(symbol)들의 확률구간을 계속적으로 곱하여 결과적으로 얻어지는 누적확률구간을 출력한다. 출력되는 누적확률구간은 각 기호들의 초기 확률과 입력되는 데이터에 순서에 의하여 결정된다. 만약 각 심벌이 초기 확률과 입력되는 순서를 key 값에 의하여 발생하게 되면 출력되는 누적확률구간도 key 값에 의존하게 된다. 본 논문은 key 값에 의존하는 산술부호화를 이용하여 해쉬함수 대신에 사용하였다.

2.2. Fragile Watermarking 요구조건

Fragile 워터마킹은 불법적인 조작으로부터 무결성을 증명할 수 있고, 불법조작의 정확한 위치 등을 알아낼 수 있게 하기위하여 다음과 같은 다양한 특성 및 요구조건을 만족해야 한다.

비가시성(Invisibility) : 삽입 후에도 원본의 변화가 거의 없고, 워터마크의 삽입여부를 감지할 수 없어야 한다. 이는 콘텐츠의 품질을 저하시키지 않는 특성으로 삽입된 워터마크가 시각적으로 보이지 않아야 한다. 특별히 의료영상은 화질 저하가 생기면 사람의 생명에 위험을 줄 수 있다. 객관적인 판단 수단으로는 신호 대 잡음비율(PSNR, Peak Signal to Noise Ratio)을 사용한다.

취약성(Fragile): 환경변화에 따라서 의도적으로 워터마크가 잘 깨져서 콘텐츠의 무결성을 판단하고, 불법 조작의 정확한 위치등도 알아낼 수 있어야 한다.

원본 없이 추출(Blindness) : 원본 영상 없이 워터마킹된 영상만으로 워터마크를 검출해야 한다. 이는 워터마킹 기법을 온라인상이나 다양한 응용분야의 적용에 있어, 올바른 소유권자를 구별할 수 있어야 하는 현실성을 고려할 때 반드시 가능해야 한다.

보안성(Security) : 관련된 키값 등을 알고 있을 경우에 워터마크의 확인이 가능해야 된다.

2.3. 기존의 워터마킹 방법

Wong의 제안한 방법이 인증과 무결성을 위한 워터마크 방법에서 가장 적합하다. 이 방법은 암호학적 해쉬함수인 MD5를 사용한 방법을 제안했다. 먼저 이미지는 I*J 픽셀 크기를 가지는 여러 블록들로 나눈 다음. 아래의 그림 2와 같이 워터마크를 삽입한다. 워터마킹 추출과정은 삽입과정의 역 과정으로써 아래의 그림3과 같다.

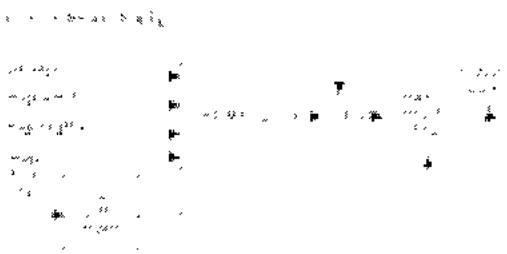

그림 2. Wong의 워터마크 삽입과정
fig 2. Watermark insertion of Wong's method

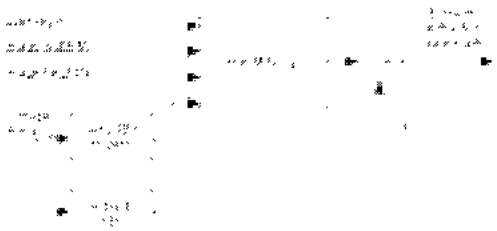

그림 3. Wong이 워터마크 추출과정
fig 3. Watermark extraction of Wong's method

2.4. 새로 제안하는 알고리즘

본 논문에서는 해쉬함수 MD5 대신에 산술부호화를 사용하였다. 워터마크 삽입방법은 아래 그림 4와 같다.

A. 먼저 이미지를 8*8블록으로 나누고, LSB's를 zero로 한다.
B. Key K2를 사용하여 X'_R의 입력순서를 바꾼다.
C. Key K1을 사용하여 각 기호들의 누적확률을 초기화한다.
D. 누적확률과 입력되는 기호를 이용하여 산술부호화 시킨다.
F. 산술부호화에서 산생되는 2진 스트링과 watermark bitmap B_R을 XOR 연산을 한 다음 LSB에 삽입하여 워터마크된 영상을 얻는다.

그림 4. 워터마크 삽입과정 블록도
fig 4. Block diagram of watermark insertion

워터마크 추출과정은 삽입과정의 역 과정으로서 그림 5와 같다.

A. 먼저 워터마크된 이미지를 8*8블록으로 나누고, LSB을 검출하고, 다시 LSB's를 zero로 한다.
B. Key K2를 사용하여 X'_R의 입력순서를 바꾼다.
C. Key K1을 사용하여 각 기호들의 누적확률을 초기화한다.
D. 누적확률과 입력되는 기호를 이용하여 산술부호화 시킨다.
F. 산술부호화에서 산생되는 2진 스트링과 검출한 LSB를 XOR 연산을 하여 워터마크를 검출한다.

그림 5. 워터마크 추출과정 블록도
fig 5. Block diagram of watermark extraction

III. 실험결과

제안한 방법의 성능을 실험적으로 보이기 위해서 그림6과 같이 256×256 8비트 Lena, Boat, Car and APCs등 영상에 대하여 실험하였고. 블록의 크기는 8×8이다. 동일한 PC와 동일한 조건하에서 모든 실험을 하였고, 실험은 MATLAB6.5로 구현을 하였다.

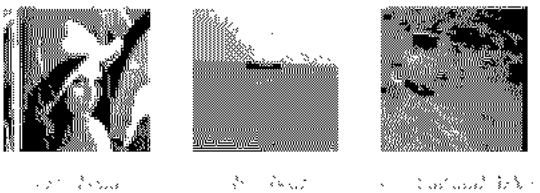

그림 6. 실험영상
fig 6. Test image

워터마크가 삽입된 영상에 대한 화질평가는 PSNR(peak signal to noise ratio)을 이용한 객관적인 방법으로 수행한다. 표1은 동일한 조건하에서 실

험을 했을 때 무결성을 입증하는데 소요되는 시간과 PSNR를 보여준다. 그림 7은 워터마크된 영상을 나타내며, 화질이 저하가 없다. 실험수치에 의하여 symbol수가 적으면 적을수록 무결성을 판단하는데 시간이 더 적게 소요됨을 알 수 있다. 픽셀 값과 1:1대응관계를 가지는 256개의 심벌을 가지고 실험한 결과 검출하는데 소요시간은 39.92초로서 해쉬함수를 사용한 Wong이 방법의 1/3시간 된다. 그림 8은 워터마크된 영상을 불법으로 조작한 영상이다. 그리고 그림9는 영상의 무결성을 검증한 것으로서, 영상의 조작된 위치를 아주 정확히 검출하였다(조작된 위치는 검정색 부분임). 그리고 PSNR이 50.15dB이상으로서 아주 우수함을 알 수 있다.

표 1. 무결성 검출시간과 PSNR
Table 1. Detection time and PSNR

method	Wong	Arithmetic coding
검출 time (second)	123.65	39.92
PSNR (dB)	51.13	51.15

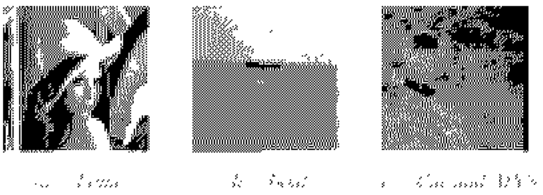

그림 7. 워터마크된 영상
fig 7. watermarked image

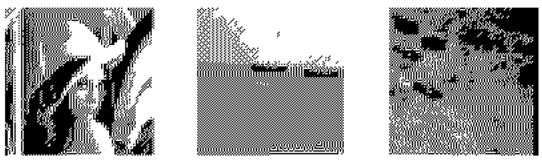

그림 8, 워터마크된 영상을 위조한 영상
fig 8. Forging watermarked image

그림 9. 위조된 부분을 검출
fig 9. Detection forged area

Ⅳ. 결과

새로 제안한 알고리즘은 암호학적 해쉬함수를 사용하지 않고, 산술부호화기법을 사용하였다. 산술부호화에서 산생된 누적확률구간은 Key 값에 의존함으로서 아주 안정하다. 그리고 여러 가지 복잡한 논리연산 대신에 간단한 곱셈만으로 값을 구하므로 검출하는데 소요되는 시간이 아주 적다. 그러므로 실시간 무결성 검출에 사용가능하다.

참고문헌

[1] P.W. Wong, "A watermark for image integrity and ownership verification," In *Proceedings of IS&TPIC Conference,* May 1998

[2] P.W, Wong, "A public key watermark for image verification and authentication," *In proceedings of ICIP.* Oct. 1998

[3] Howard, P.G. & Vitter, J.S. "Arithmetic coding for data compression," *Procee dings of the IEEE, 82*(6), June 1994, pp.857~865.

[4] P. Elias, "Universal codeword sets and representations of the integers," *IEEE*

Trans. Inform. Theory, 21, 1975, pp. 194 ~203.

[5] P. Elias, "Predictive codmg," *IRE Trans. Inform. Theory, IT l,* Mar. 1955, pp. 16 ~33, pp.30~33.

A Fragile Watermarking Scheme Using a Arithmetic Coding

Cheng-Ri, Piao* · Seung-Eun, Paek** · Seung-Soo, Han***

Abstract

In this paper, a new fragile watermarking algorithm for digital image is presented, which makes resolving the security and forgery problem of the digital image to be possible. The most suitable watermarking method that verifies the authentication and integrity of the digital image is the Wong's method, which invokes the hash function (MD5). The algorithm is safe because this meth od uses the hash function of the cryptology. The operations such as modulus, complement, shift, bitwise exclusive or, bitwise inclusive or are necessary for calculating the value of hash function. But, in this paper, an Arithmetic encoding method that only includes the multiplication operation is adopted. This technique prints out accumulative probability interval, which is obtained by multi plying the input symbol probability interval. In this paper, the initial probability interval is de termined according to the value of the key, and the input sequence of the symbols is adjusted ac cording to the key value so that the accumulative probability interval will depend on the key value. The integrity of the algorithm has been verified by experiment. The PSNR is above the 51.13db and the verifying time is 1/3~1/4 of the verifying time of using the hash function (MD5), so, it can be used in the real time system.

Key Words : Digital Image, Watermaking Algorithm

* Information engineering, MyungJi University
** Information engineering, MyungJi University
*** Professor, Dept. of Information engineering, MyungJi University