Journal of Korea Multimedia Society Vol. 7, No. 9, September 2004(pp. 1294-1303)

LUT 기반의 블록 연성 워터마킹

주은경[†], 강현호[††], 박지환[†††]

요 약

본 논문에서는 기존의 픽셀 기반 방식과 블록 기반 방식의 개념을 도입하여 영상의 인증과 무결성을 위한 새로운 블록 연성 워터마킹을 제안하였다. 제안 방식은 원 영상의 각 픽셀과 해당 블록의 정보로 LUT(Look Up Table)을 선택하여 원 영상을 이진화 한 값과 워터마크를 비교하여 원 영상을 수정하면서 워터마크를 삽입하였다. 그 결과 기존 방식의 약점으로 지적된 collage 공격 등을 방지하면서도 워터마크된 영상에서 워터마크인 이진로고를 추출하여 시각적으로 편리하게 소유권 확인과 변조 위치를 픽셀 단위 또는 블록 단위로 검출할 수 있었다.

Block Fragile Watermarking Based on LUT

Eun-Kyong Joo[†], Hyun-Ho Kang[††], Ji-Hwan Park[†††]

ABSTRACT

This paper proposes new block fragile watermarking for image authentication and integrity by using the existing pixel-based scheme and block-based scheme. The proposed scheme is performed as follows. First, we choose LUT(Look Up Table) from each pixel of original image and information of the corresponding block. Next, we insert a watermark, modifying original image with values to compare binary original image with the watermark to be embedded. As a result, we provide the means to overcome some weakness of the existing scheme. Binary logo as watermark can be detected from watermarked image and altered location can also be detected by the unit of pixel or that of block in our scheme.

Key words: Fragile Watermarking(연성 워터마킹), Image Authentication(영상 인증)

1. 서 론

최근 컴퓨터의 발전과 인터넷 보급에 따라 음악, 영상, 동영상 등과 같은 여러 형태의 멀티미디어 데이터가 디지털 화되어 누구나 쉽게 저장 및 전송을 할 수 있게 되었다. 전송 받은 디지털 데이터는 컴퓨터에서 원본의 손상 없이 대량 복사가 가능하고, 각종 편집도구를 이용하여 다양하게 변형 할 수 있다. 따라서 누구든지 저자의 동의 없이 이러한 디지털 데이터의 불법 복제 및 배포가 가능한 것이다. 따라서 이러한 불법 복제를 방지하거나 저작권을 보호하기 위한 기술에 대한 요구가 커지고 있다.

일반적으로 디지털 데이터를 보호하기 위한 기법으로는 크게 세 가지를 생각할 수가 있다. 첫째는 사용자 인증이라는 기법으로 적법한 사용자만이 디지털 데이터에 접근이 가능하도록 하는 것이며, 둘째는 키를 이용한 암호화 기법으로 디지털 데이터를 암호화하여 전송하면 적법한 사용자만이 복호화해서 디지털 데이터를 사용할 수 있도록 하는 것이다. 셋째는 디지털 데이터에 직접적으로 저작권 정보를 삽입하는 디지털 워터마킹(Digital Watermarking) 기법이 있다. 인증이나 암호화라는 기법은 일단 디지털

※ 교신저자(Corresponding Author) : 주은경, 주소 : 부산시 남구 대연3동 부경대학교 5214A, 전화 : 051)620-6392, FAX : 051)620-6390, E-mail : jooek@pknu.ac.kr
접수일 : 2003년 12월 31일, 완료일 : 2004년 4월 7일
[†] 준회원, 부경대학교 산업대학원 전산정보학과
[††] 준회원, 부경대학교 대학원 전자계산학과
(E-mail : hhkang@shannon.pknu.ac.kr)
[†††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부
(E-mail : jpark@pknu.ac.kr)

데이터에 접근하게 되면 복제와 배포가 자유롭고, 저작권 정보를 파악할 수 없는 반면에 디지털 워터마킹 기법은 디지털 데이터 자체에 저작권 정보를 포함하고 있으므로 불법 복제나 유통을 방지하는데 유용하게 활용할 수 있는 기술이다.

디지털 워터마킹 기법은 음악, 정지영상, 동영상 등의 디지털 데이터에 원 소유주만이 아는 마크를 사람의 육안이나 귀로는 구별할 수 없게 삽입하여 자신의 디지털 데이터에 대하여 저작권을 주장할 수 있는 방법을 제공한다. 이러한 디지털 워터마킹 기법은 견고성에 따라 강인한 워터마킹(robust watermarking)과[1,2] 연성 워터마킹(fragile watermarking)으로[3-7,10,11] 분류할 수 있다. 강인한 워터마킹은 원래 디지털 데이터를 파괴할 정도로 공격을 가하지 않는 통상적인 영상처리 기법에 의해 워터마크가 잘 지워지지 않는 특성을 갖는다. 이러한 특성을 가지면서 비지각성의 특성을 가지려면 인간 시각에 둔감한 데이터 영역에 적절한 강도로 워터마크를 삽입하여 해야 한다. 연성 워터마킹은 디지털 데이터가 변경될 경우에는 워터마크가 손상되어 법정에서 데이터의 무결성을 증명하거나 그 외에 불법 복제나 유통의 목적으로 가해진 공격을 파악하는데 사용될 수 있다. 즉, 디지털 영상에 대한 인증(authentication)과 무결성(integrity)을 위한 연성 워터마킹 기법은 디지털 데이터의 내용이 조작되거나 변형되지 않았다는 것을 확인하면서 그 영상물의 송신자나 소유자를 확인할 수 있는 방법을 제공해야 한다.

연성 워터마킹은 다음과 같은 조건이 고려되고 있는데, 그 중 첫 번째와 두 번째 조건은 일반적인 워터마킹 기법과 구별되는 연성 워터마킹 기법만의 특별한 조건이다.

(1) 변조 여부 : 영상의 변조 여부를 추출된 워터마크를 통해 확인할 수 있어야 한다.

(2) 변조 위치 : 영상이 변조된 경우에는 영상의 어느 위치가 변조되었는지를 검출할 수 있어야 한다.

(3) 원 영상 불필요 : 원 영상 없이 워터마크를 추출할 수 있어야 한다.

(4) 무감지성 : 워터마크는 인간의 시각에 의해 인지되지 않아야 한다.

연성 워터마킹의 기법은 크게 두 가지 형태로 발전되어 왔다. 첫 번째 형태는 공간영역에 워터마크를 삽입하는 방법으로 영상 데이터의 픽셀 값에 워터마크를 삽입하는 기술이며, 두 번째 형태는 DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT(Discrete Fourier Transform) 등의 변환을 이용하여 주파수 계수들을 워터마크에 따라 변경하여 워터마크를 삽입하는 기술이다.

본 논문에서는 영상의 인증과 무결성을 목적으로 원 영상의 공간영역에 이진로고를 워터마크로 삽입한다. 제안하는 방식은 원 영상과 워터마크 없이 워터마크가 추출되며, 추출된 워터마크인 이진로고를 통하여 시각적으로 영상의 변조 여부 및 변조 위치를 픽셀 단위 및 블록 단위로 검출할 수 있다.

본 논문은 다음과 같은 내용으로 구성된다. 먼저 2장에서는 기존의 연성 워터마킹 기법에 대해 간략히 소개하고 문제점을 지적한다. 3장에서는 영상의 인증과 무결성을 위한 새로운 블록 연성 워터마킹 기법을 제안한다. 제안된 방법을 4장에서 실험을 통하여 결과를 확인하고, 마지막으로 5장에서는 결과를 정리한다.

2. 기존의 연성 워터마킹 기법

본 장에서는 영상의 인증과 무결성을 위한 기존의 연성 워터마킹 기법에 대하여 설명하고 이에 대한 문제점을 살펴본다.

2.1 Yeung의 방식

Yeung은 영상의 소유권 정보 표시와 검증을 위하여 원 영상의 각 픽셀에 대하여 워터마크로 이진로고를 삽입하여 화질이 좋으면서 눈에 보이지 않는 워터마킹을 제안하였다[5]. 이 방식은 다음의 그림 1과

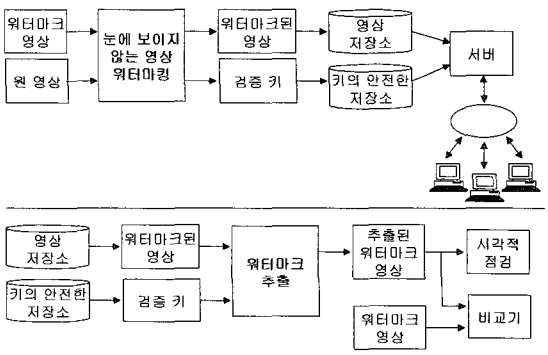


그림 1. 영상검증시스템의 블록 다이어그램

같이 눈에 보이지 않는 영상 워터마킹 처리와 워터마크 추출 처리로 구성된다. 눈에 보이지 않는 워터마킹은 원 영상에 워터마크를 삽입하면서 검증키를 생기게 하며, 워터마크 추출은 검증키를 사용하여 워터마크된 영상으로부터 삽입된 워터마크를 추출한다.

이 방식은 워터마크로 추출된 이진로고를 통해서 시각적으로 영상의 변조 여부 및 픽셀 단위로 변조 위치를 검출하는데 좋은 성능을 가지고 있다. 그러나 같은 비밀키와 이진로고를 사용하여 여러 영상에 워터마크를 삽입한 경우에는 다음과 같은 문제점이 있다. 첫 번째는 여러 다른 워터마크된 영상에서의 워터마크 비트 위치가 대응되는 픽셀 값을 이진화한 값의 위치이므로 공격자가 이진로고와 이진함수를 쉽게 추정하여 워터마크된 영상을 수정하거나 위조할 수 있다. 두 번째는 워터마크 비트가 원 영상에 종속적이지 않고 각 픽셀 값에 종속적이므로 공격자가 워터마크된 여러 다른 영상으로부터 각 영상 내의 상대적인 위치를 유지하면서 영상의 일부분을 잘라내고 결합해서 정상적으로 인증이 되도록 하는 collage 공격에 약한 점이다[8,9].

2.2 Fridrich의 방식

Fridrich는 Yeung의 방식을 기반으로 하여 LUT 대신에 블록 암호를 사용하여 안전성에 문제가 없는 새로운 방식을 제안하였다[10]. 이 방식은 블록의 개념을 도입하여 각 픽셀의 이웃하는 픽셀들을 결합하여 원 영상에 종속적으로 워터마크를 삽입한다. 먼저 카메라 키로 블록 암호 알고리즘 E_k를 위한 비밀키를 생성하고, 생성된 비밀키로 원 영상의 블록 내에서 픽셀의 위치를 섞는다. 각 픽셀에 대하여 a×a 정사각형 내에서 $g_{i-u\,j-v} \mid 0 \le u,\ v \le a-1$로 구성된 이웃하는 픽셀 값들을 암호화한다. 여기에서 a는 정수(a≈5)이고, 워터마크가 삽입될 각 픽셀은 a×a 정사각형 내에서 가장 오른쪽 아래 코너에 위치하게 된다. 워터마크를 삽입하기 위하여 원 영상의 각 픽셀 값을 아래의 식(1)을 이용하여 이진화 한다.

$$L_{(i,j)} = Parity(E_k(g_{i-u\,j-v} \mid 0 \le u,\ v \le a-1)) \quad (1)$$

여기에서 $L_{(i,j)}$은 원 영상을 이진화한 값이고, $E_k(g_{i-u\,j-v} \mid 0 \le u,\ v \le a-1)$는 암호화된 비트 스트림인데 각 픽셀 값은 암호화 함수인 E_k에 적용되기 전에 이진 스트림으로 변환되어야 한다. Parity는 암호화된 비트 스트림에 XOR 연산을 수행한 것이다. 식(1)의 결과인 원 영상을 이진화한 값 L과 워터마크인 이진로고 W를 비교하여 원 영상의 각 픽셀 값을 수정하면서 워터마크를 삽입한다.

이 방식은 Yeung의 방식에서 언급한 공격[8,9]을 방지하면서 영상의 변조 여부 및 변조 위치를 블록 단위로 검출할 수 있다. 그러나 픽셀 단위로는 변조 위치 검출이 불가능하고 각 픽셀에 워터마크를 삽입 시 계산량이 많은 문제점이 있다.

2.3 Zhong의 방식

Zhong은 워터마킹 알고리즘의 안전성을 높이고 변조 위치를 픽셀 단위로 검출하기 위하여 각 영상별로 특성을 나타내는 블록을 선택하여 원 영상에 종속적으로 워터마크를 삽입하는 방식을 제안하였다[11]. 이 방식은 원 영상의 특성을 가장 잘 나타내는 블록(예: Lena 영상의 오른쪽 눈)을 선택하여 카메라 키와 같이 해쉬하여 비밀키를 생성한다. 이렇게 생성된 비밀키에 의존적인 암호화 매트릭스인 $\{B_{ij}\}$를 원 영상의 크기와 동일하게 생성한다. 워터마크를 삽입하기 위하여 원 영상의 각 픽셀 값에 대하여 아래의 식(2)를 이용하여 이진화 한다.

$$L_{(i,j)} = f(g_{(i,j)}) \oplus B_{(i,j)} \quad (2)$$

여기에서 $L_{(i,j)}$은 원 영상을 이진화한 값이고, $g_{(i,j)}$는 원 영상의 픽셀 값이다. f는 이진함수로서, f: {0, 1, …, 255} → {0, 1}, 0에서 255까지의 픽셀 값을 0 또는 1의 이진 값으로 사상하는 함수이고, $B_{(i,j)}$는 원 영상에 종속적인 암호화 매트릭스이다. 식(2)의 결과인 원 영상을 이진화한 값 L과 워터마크인 이진로고 W를 비교하여 원 영상의 픽셀 값을 수정하면서 워터마크를 삽입한다.

이 방식은 Yeung의 방식에서 언급한 공격[8,9]을 방지하면서 영상의 변조 여부 및 픽셀 단위로 변조 위치를 검출할 수 있다. 그러나 영상의 특성으로 선택된 블록이 변조되면 워터마크는 전혀 추출되지 않는 문제점이 있다.

3. 새로운 블록 연성 워터마킹 제안

본 장에서는 영상의 인증과 무결성을 위한 연성 워터마킹의 기존 방법들을 기반으로 하여 위에서 지

적된 두 공격을 효과적으로 방지하면서도 원 영상의 변조시에 워터마크를 추출하면 픽셀 단위 및 블록 단위로 변조 위치의 검출이 가능하고 알고리즘이 비교적 간단한 새로운 블록 연성 워터마킹을 제안한다.

3.1 워터마크 삽입

제안방식에서는 8-bit 그레이 스케일 영상을 기준으로 워터마크가 삽입과 추출이 되며, 원 영상 I의 크기는 M×N이다. 삽입될 워터마크 W는 원 영상과 동일한 M×N의 크기를 가지는 이진로고 영상이다. 워터마크의 삽입 과정에서 LUT를 4개 사용하여 안전성을 높이고, 원 영상을 m×n 크기의 블록으로 나누어 해당 블록의 모든 픽셀의 MSB(Most Significant Bit)정보를 이용하여 워터마크가 원 영상에 종속적으로 삽입이 되도록 한다. 첫 번째 단계는 비밀키 K에 의존적인 8-bit 그레이 스케일×4(256×4)인 1024 크기의 이진 비트열(bs: bit stream)을 의사 난수 생성기를 통해 표 1과 같이 생성시킨다. 이진 비트열을 생성시에 8-bit 그레이 스케일인 256 크기에 4를 곱하는 이유는 LUT를 4개 생성하기 위해서이다.

위에서 생성한 이진 비트열을 8-bit 그레이 스케일인 256 크기로 4등분하여 이진함수 f_1, f_2, f_3, f_4을 생성하여 LUT_{00}, LUT_{01}, LUT_{10}, LUT_{11}을 표 2와 같이 작성한다. 여기에서 이진함수란 각 bs_i내에서의 생성순서인 0에서부터 255까지의 위치 값(index)을 8-bit 그레이 스케일의 픽셀 값으로 두어 이를 첫 번째 단계에서 생성한 이진 비트열의 0 또는 1의 이진 값으로 사상하는 함수이고, 이를 표로 나타낸 것이 LUT이다.

원 영상의 각 픽셀의 MSB값(b_1)과 원 영상을 m×n으로 나눈 해당 블록별로 모든 픽셀의 MSB를 Parity한 값(b_2)으로 해당 LUT를 표 3과 같이 선택한다. 이렇게 각 픽셀별로 선택된 LUT로 원 영상의 각 픽셀 값을 이진화 하여 이를 워터마크인 이진로고 영상의 이진 값과 비교하여 원 영상을 수정하면서 워터마크를 삽입한다. 원 영상을 이진화한 값과 이진 워터마크의 값이 동일할 경우에는 원 영상의 해당 픽셀 값을 그대로 두고 다음 픽셀로 넘어간다. 만약, 두 값이 다를 경우에는 원 영상의 해당 픽셀 값을 추출되어질 워터마크의 이진 값과 같아지도록 해당 LUT에서 가장 가까운 픽셀 값을 찾아서 원 영상의 픽셀 값을 수정한다. 워터마크의 삽입 과정을 다음의 그림 2와 같이 개괄적으로 나타내었다.

표 1. 의사 무작위 이진 비트열

bs 구분(bs_i)	bs_i의 위치(index)	bs_i의 이진비트열	비고
bs_1	bs{ 0, 1, … ,255}	0 1 … 0	f_1
bs_2	bs{256, 257, … ,511}	1 0 … 1	f_2
bs_3	bs{512, 513, … ,767}	0 0 … 1	f_3
bs_4	bs{768, 769, …,1023}	1 1 … 0	f_4

표 2. 이진함수와 LUT

이진 함수	사상 함수	해당 LUT	비고
f_1	{0, 1, …. 255} → {0, 1}	LUT_{00}	bs_1
f_2	{0, 1, …. 255} → {0, 1}	LUT_{01}	bs_2
f_3	{0, 1, …. 255} → {0, 1}	LUT_{10}	bs_3
f_4	{0, 1, …. 255} → {0, 1}	LUT_{11}	bs_4

표 3. 워터마크 삽입시 LUT의 선택

해당 LUT	b_1값	b_2값	비 고
LUT_{00}	0	0	bs_1
LUT_{01}	0	1	bs_2
LUT_{10}	1	0	bs_3
LUT_{11}	1	1	bs_4

b_1값 = $b_1(g_{(i,j)'s\ MSB})$.
b_2값 = $b_2(\text{Parity}(g'_{s\ MSB},\cdots,g_{m\times n's\ MSB}))$, 여기서 $g_{(i,j)}$는 원 영상 i행 j열의 픽셀 값, Parity는 Exclusive OR.

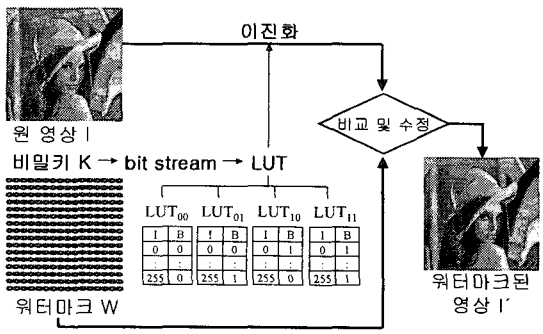


그림 2. 워터마크 삽입 과정(제안 방식)

3.2 워터마크 추출

워터마크를 추출하기 위해서 먼저 비밀키 K에 의존적인 1024 크기의 이진 비트열을 의사 난수 생성기를 통해 앞의 표 1과 같이 생성시킨다. 생성된 이진 비트열을 8-bit 그레이 스케일인 256 크기로 4등분하

여 이진함수 f_1, f_2, f_3, f_4을 생성하여 LUT_{00}, LUT_{01}, LUT_{10}, LUT_{11}을 앞의 표 2와 같이 작성한다. 워터마크된 영상의 각 픽셀별로 해당 픽셀의 MSB값(b_1)과 워터마크된 영상을 m×n으로 나눈 해당 블록별로 모든 픽셀의 MSB를 Parity한 값(b_2)으로 해당 LUT를 아래의 표 4와 같이 선택한다. 이렇게 각 픽셀별로 선택된 LUT로 워터마크된 영상의 각 픽셀 값을 이진화 하면 워터마크인 이진로고가 추출된다. 워터마크의 추출 과정을 다음의 그림 3과 같이 개괄적으로 나타내었다.

워터마크된 영상에 올바른 비밀키로 워터마크를 추출하면 이진로고가 추출되어 소유권을 주장할 수 있으나, 올바르지 않은 비밀키로 워터마크를 추출하면 이진함수 및 LUT의 구성 내용이 달라져서 전혀 알아볼 수 없는 영상이 추출되어 소유권을 주장할 수 없게 된다. 워터마크된 영상을 변조하면 변조된 픽셀들은 각 픽셀 값의 해당 LUT의 변조된 픽셀 값으로 이진 값을 추출하거나 아예 다른 LUT에서 변조된 픽셀 값으로 이진 값을 추출하므로 워터마크인 이진로고가 손상되어 변조 유무 확인 및 변조 위치를 검출할 수 있다.

표 4. 워터마크 추출시 LUT의 선택

해당 LUT	b_1값	b_2값	비 고
LUT_{00}	0	0	bs_1
LUT_{01}	0	1	bs_2
LUT_{10}	1	0	bs_3
LUT_{11}	1	1	bs_4

b_1값 = $b_1(g_{(i,j)\text{'s MSB}})$.

b_2값 = $b_2(\text{Parity}(g'_{\text{s MSB}},\cdots,g_{m\times n\text{'s MSB}}))$, 여기서 $g_{(i,j)}$는 워터마크된 영상 i행 j열의 픽셀 값, Parity는 Exclusive OR.

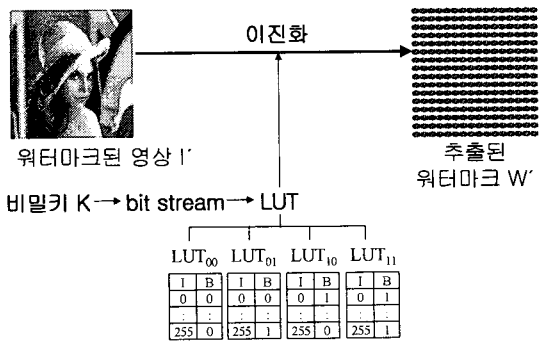


그림 3. 워터마크 추출 과정(제안 방식)

제안 방식의 이해를 돕고자 다음의 그림 4와 그림 5와 같이 예를 들어 나타내었다. 그림 4의 삽입 예를 보면 원 영상 I의 일부분인 픽셀 값 1, 2, 131, 132에 워터마크 W의 일부분인 0, 0, 1, 1을 삽입하기 위하여 원 영상의 각 픽셀 값을 LUT을 사용하여 이진화 한다. 각 LUT는 0에서 255까지의 픽셀 값을 0 또는 1의 값으로 사상하는 표이고, 생성된 4개의 LUT 중 하나를 선택하는 기준은 b_1과 b_2함수이다. b_1함수는 각 픽셀 $g_{(i,j)}$의 MSB이며, b_2 함수는 m×n의 크기인 각 블록의 모든 픽셀의 MSB를 Parity한 것인데 여기서는 b_2함수의 값은 0으로 가정한다.

원 영상의 첫 번째와 두 번째 픽셀 값의 MSB는 0이고 b_2의 값은 0으로 가정하였으므로 LUT_{00}을 선택하게 되어 첫 번째 픽셀 값 1은 0으로 두 번째 픽셀 값 2는 1로 이진화 되고, 세 번째 와 네 번째 픽셀 값의 MSB는 1이고 b_2의 값은 0으로 가정하였으므로 LUT_{10}을 선택하게 되어 세 번째 픽셀 값 131은 0으로, 네 번째 픽셀 값 132는 1로 이진화 되었다.

이렇게 이진화된 원 영상과 이진 워터마크의 이진

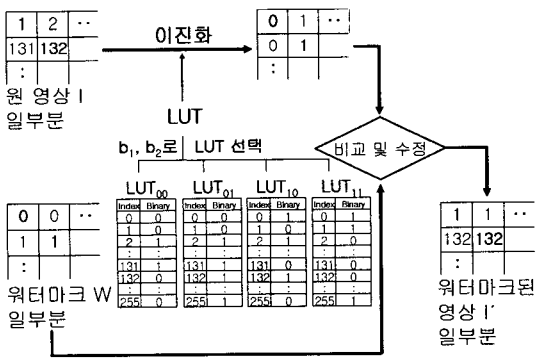


그림 4. 워터마크 삽입의 예

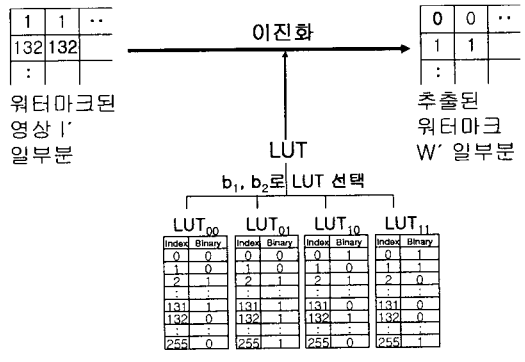


그림 5. 워터마크 추출의 예

값을 비교 및 수정하여 워터마크를 삽입하게 되는데 첫 번째와 네 번째 픽셀의 경우 원 영상을 이진화한 값과 워터마크의 이진 값이 같으면 원 영상을 수정을 하지 않고 바로 다음 픽셀로 넘어가고, 두 번째와 세 번째 픽셀의 경우와 같이 두 이진 값이 다를 경우에는 추출되어질 워터마크의 이진 값에 원 영상의 픽셀 값을 맞출 수 있도록 원 영상의 픽셀 값을 해당 LUT에서 가장 가까운 픽셀 값으로 수정한다. 픽셀 값 2의 경우에는 LUT_{00}에서 워터마크인 0의 값에 맞출 수 있도록 가장 가까운 1로 원 영상의 픽셀 값을 수정하고, 픽셀 값 131의 경우에는 LUT_{10}에서 워터마크인 1의 값에 맞출 수 있도록 가장 가까운 132로 원 영상의 픽셀 값을 수정하여 워터마크된 영상 I′를 얻게 된다.

그림 5의 추출 예를 보면 워터마크된 영상 I′의 일부분인 픽셀 값 1, 1, 132, 132에서 워터마크를 추출하는 과정을 보인다. 여기서 워터마크된 영상의 각 픽셀 값을 이진화 하는데 LUT를 사용하며, 워터마크된 영상의 첫 번째와 두 번째 픽셀 값의 MSB는 0이고 b_2의 값은 0으로 가정하였으므로, LUT_{00}을 선택하게 되어 첫 번째와 두 번째 픽셀 값 1은 0으로 이진화 되고, 세 번째 와 네 번째 픽셀 값의 MSB는 1이고 b_2의 값은 0으로 가정하였으므로 LUT_{10}을 선택하게 되어 세 번째 와 네 번째 픽셀 값 132는 1로 이진화 되었다. 이렇게 이진화된 영상이 추출된 워터마크 W′이다.

3.3 기존방식과 비교

기존의 방식과 제안방식을 표 5와 같이 비교하여 나타내었다. 제안방식은 기존의 픽셀 기반 방식의 장점인 LUT을 여러 개 사용하였으며, 블록 기반 방식의 장점인 원 영상에 종속적으로 워터마크를 삽입할 수 있도록 MSB를 이용하였다. 이에 따라 영상이 변경되면 MSB의 변경 유무에 따라 블록 단위 또는 픽셀 단위로 변조 위치가 검출되어 기존의 방식에 비하여 큰 성과를 볼 수 있었다.

4. 실험 및 결과

본 논문에서 제안한 방식의 효율성을 확인하기 위해 MATLAB을 이용하여 구현하였고, 실험에 사용한 원 영상을 그림 6과 그림 7에 나타내었다. 원 영상은 256×256 크기의 Lena 및 House 8-bit 그레이 영상을 각각 원 영상 I 과 원 영상 II로 사용하였다. 16×16 크기의 이진로고인 그림 8을 256×256 크기로 그림 9와 같이 만들어 워터마크로 사용하였다. 워터마크 삽입 과정에서 LUT을 선택하기 위한 b_2 함수에서 MSB를 Parity하기 위한 한 블록의 크기는 32×32 크기로 실험하였다. 각 픽셀별로 LUT를 선택하기 위하여 가장 변경될 가능성이 적은 해당 픽셀의 MSB 정보를 사용하였고, 워터마킹 알고리즘에서 MSB는 변경되지 않도록 구현하였다.

워터마크된 영상인 그림 10과 그림 11은 시각적으

그림 6. 원 영상 I (Lena) 그림 7. 원 영상 II (House)

표 5. 기존의 방식과 제안방식의 비교

방식 / 비교	Yeung 방식	Fridrich 방식	Zhong 방식	제안 방식
변조위치 검출단위	픽셀 단위	블록 단위	픽셀 단위	픽셀 단위 및 블록 단위
블록개념 도입방식	해당사항 없음	이웃하는 픽셀 값의 암호화	원 영상의 특정 영역에 기반한 암호화 매트릭스	이웃하는 픽셀들의 MSB 값을 Parity 취함
중요 알고리즘	LUT	블록 암호	원 영상의 특정 영역 선택	4개의 LUT 중에서 선택
평가	블록 기반의 공격(collage 공격 등) 가능	픽셀 단위로 변조위치 검출 불가	선택된 특정 영역의 변조 시 워터마크 추출 불가	collage 공격에 강인하면서 픽셀단위로 검출가능

그림 8. 이진로고

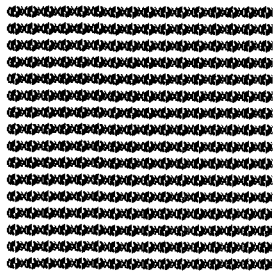


그림 9. 워터마크

그림 10. 워터마크된 영상 I

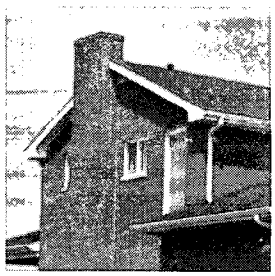


그림 11. 워터마크된 영상II

로 워터마크의 삽입을 구별하기 어려우며, 객관적인 화질평가를 나타내는 PSNR(Peak Signal to Noise Ratio)을 계산하면 그림 10은 43.00[dB], 그림 11은 43.32[dB]로 원 영상과의 화질 차이가 크지 않다는 것을 알 수 있다.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} [dB] \quad (3)$$

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x(i,j) - x'(i,j))^2$$

식(3)에서 M과 N은 원 영상의 너비와 높이 크기이고, $x(i,j)$는 원 영상의 픽셀값이며 $x'(i,j)$는 워터마크된 영상의 픽셀값이다. PSNR의 결과값이 클수록 원 영상과 화질의 차이가 적음을 나타낸다.

워터마크된 영상 I 로부터 올바른 비밀키로 추출된 워터마크인 그림 12의 오른쪽 상단은 원래의 삽입한 로고임을 지각할 수 있으므로 소유권 주장이 가능하다. 그러나, 올바르지 않은 비밀키로 워터마크를 추출하면 그림 12의 오른쪽 하단과 같이 전혀 알아볼 수 없는 영상이 추출되어 제3자는 영상의 소유권을 주장할 수 없게 된다.

공격자가 워터마크된 영상 I 에 그림 13의 우측 하단부와 같이 변조를 가한 경우에는 추출된 워터마크에 변조된 위치가 픽셀 단위로 그림 14와 같이 손상되어 시각적으로 표시된다.

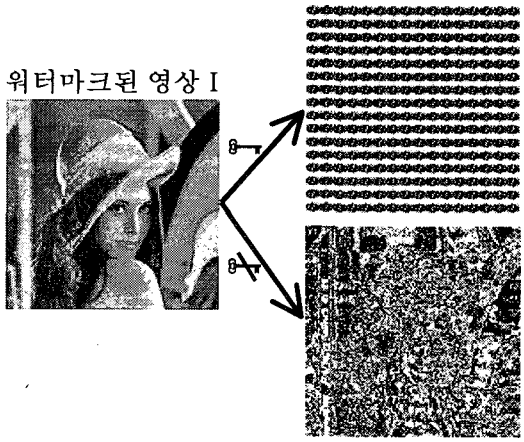


그림 12. 워터마크의 추출

그림 13. 변조 영상 I

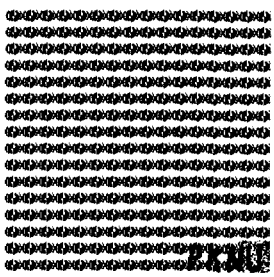


그림 14. 변조 영상 I 의 추출 워터마크

앞에서 언급된 공격[8,9] 중에서 워터마크된 여러 다른 영상으로부터 공격자가 이진로고와 이진함수를 추정하여 워터마크의 삽입을 위조하는 공격이 있다. 제안 방식에서는 픽셀값이 동일하더라도 이진함수의 수가 4개이므로 이를 추정하기가 Yeung의 방식에 비하여 매우 어렵다. 또한, 공격자가 워터마크된 여러 다른 영상으로부터 각 영상 내의 상대적인 위치를 유지하면서 영상의 일부분들을 잘라내고 붙여서 정상적으로 인증이 되도록 하는 collage 공격이 있다. 제안 방식에서는 해당 픽셀 및 블록의 MSB 정보로 LUT을 선택하여 워터마크가 원 영상에 종속적이게 삽입이 되므로 collage 공격을 방지할 수 있다. 이러한 collage 공격의 실험으로 원 영상 I 에 상대적 위치가 동일하게 원 영상 II의 일부분을 잘라내고 붙여서 그림 15를 만들었다. 이렇게 생성된 영상에서 추출된 워터마크는 그림 16과 같이 변조위치를 블록 단위로 검출할 수 있다.

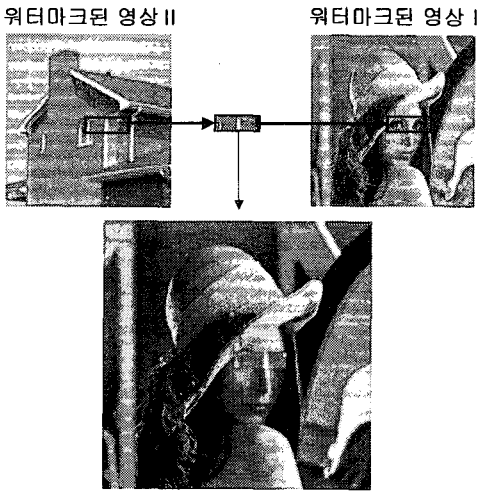


그림 15. collage 공격 영상

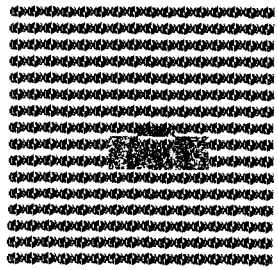


그림 16. collage 공격 영상의 추출 워터마크

제안방식을 컬러 영상에 실험하기 위하여 256×256 크기의 24-bit Lena 컬러 영상인 그림 17을 컬러 원 영상으로, 이진로고인 256×256 크기의 그림 9를 워터마크로 사용하였다. 제안 방식을 컬러 영상에 적용하기 위하여 24-bit 컬러 영상을 R성분, G성분, B성분으로 각각 8-bit씩 분리하여 이 중에서 한 성분에 워터마크를 삽입하였다. 워터마크 삽입 과정에서 LUT을 선택하기 위한 b_2 함수에서 MSB를 Parity하기 위한 한 블록의 크기는 그레이 영상의 실험과 마찬가지로 32×32 크기로 하였다.

그림 17의 컬러 원 영상에 워터마크를 삽입한 그림 18의 워터마크된 컬러 영상은 시각적으로 화질의 차이를 구별하기 어려우며, PSNR의 계산값은 43.06 [dB]이다. 워터마크된 컬러 영상에 다음의 그림 19의

그림 17. 컬러 원 영상(Lena) 그림 18. 워터마크된 컬러 영상

그림 19. 변조 컬러 영상

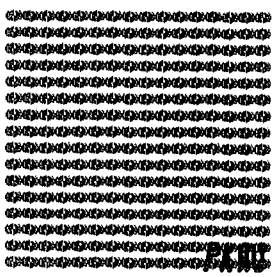


그림 20. 변조 컬러 영상의 추출 워터마크

우측 하단부와 같이 변조를 가한 경우에 워터마크를 추출하면 그림 20과 같이 그 변조된 위치가 픽셀 단위로 손상되어 시각적으로 확인이 가능하다.

5. 결 론

디지털화된 음악, 영상, 동영상 등과 같은 멀티미디어 데이터의 사용 증가에 따라 저작권 침해 및 불법 위·변조 등과 같은 문제점들이 발생하고 있다. 이러한 디지털 멀티미디어 데이터를 보호하기 위한 새로운 방법으로 디지털 워터마킹 기술이 활발히 연구되고 있다. 이 기술은 디지털 데이터의 저작권 보호, 인증/무결성, 불법 유통자 추적 등의 다양한 응용이 가능하다.

본 논문에서는 영상의 인증과 무결성을 위한 새로운 블록 연성 워터마킹 방법을 제안하고, 그 유용성에 대하여 살펴보았다. 기존의 픽셀 기반 방식에서는 collage 공격 등이 가능하며, 기존의 블록 기반 방식에서 원 영상에서 한 픽셀만 변조되어도 워터마크를 추출하면 변조 위치가 블록 전체로만 추출되는 문제점이 있었다. 제안 방식에서는 기존의 픽셀 기반 방식의 LUT를 사용하고, 블록 기반의 방식의 블록의 개념을 도입하여 원 영상의 각 픽셀과 해당 블록의 정보로 LUT을 선택하여 원 영상을 이진화한 후 이 값과 워터마크를 각 픽셀별로 비교하여 원 영상을 수정하면서 워터마크를 삽입하였다.

그 결과 원 영상과 원 워터마크 없이 워터마크를 추출하여 소유권을 확인할 수 있었다. 또한, 기존의 문제점으로 지적된 collage 공격 등에 강인하여 안전성을 더하였으며, 원 영상의 변조 위치를 해당 블록의 MSB의 변경 유무에 따라 블록 단위 또는 픽셀 단위로 시각적으로 편리하게 확인이 가능하였다.

참 고 문 헌

[1] 신용달, 권성근, "DCT의 DC 계수에 워터마크를 삽입하는 디지털 워터마킹," 한국멀티미디어학회 논문지, Vol.6, No.6, pp.962-968, 2003.

[2] 김용훈, 이태홍, 이경훈, "웨이브릿 기반의 강인한 패턴 디지털 워터마킹 방법," 한국멀티미디어학회 논문지, Vol.7, No.1, pp.98-108, 2004.

[3] G.L. Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image," IEEE Trans. on Consumer Electronics, Vol.39, No.4, pp. 905-910, Nov. 1993.

[4] R.G. Schyndel, A.Z. Tirkel and C.F. Osborne, "A Digital Watermark," IEEE International Conference on Image Processing, ICIP'94, Vol.2, pp. 86-90. Nov. 1994.

[5] M.M. Yeung and F. Mintzer, "An Invisible Watermarking Technique for Image Verification," IEEE International Conference on Image Processing, ICIP'97, Vol.2, pp. 680-683, Oct. 1997.

[6] P.W. Wong, "A Watermark for Image Integrity and Ownership Verification," In Proc. of IS&T PIC Conference, May 1998.

[7] P.W. Wong, "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing ICIP'98, Oct 1998.

[8] J. Fridrich, M. Goljan and N. Memon, "Further Attacks on Yeung-Mintzer Watermarking Scheme," Proc. SPIE, Electronic Imaging 2000, Security and Watermarking of Multimedia Contents, pp.428-437, Jan. 2000.

[9] M. Holliman and N. Memon, "Counterfeiting Attacks on Oblivious Block-Wise Independent Invisible Watermarking Schemes," IEEE Trans. on Image Processing, Vol.9, No.3, pp. 432-441, Mar. 2000.

[10] J. Fridrich, M. Goljan and A.C. Baldoza, "New Fragile Authentication Watermark for Images," IEEE International Conference on Image Processing, ICIP'00, Vol.1, pp. 446-449, Sep. 2000.

[11] H. Zhong, F. Liu and L.C Jiao, "A New Fragile Watermarking Technique for Image Authentication," Int'l Conference on Signal Processing, Vol.1, pp.792-795, Aug. 2002.

주 은 경

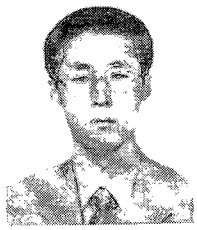
2001년 2월 경성대학교 컴퓨터과학과 (공학사)
2004년 2월 부경대학교 산업대학원 전산정보학과(공학석사)

관심분야 : 디지털 워터마킹

강 현 호

1999년 동의대학교 컴퓨터공학과 (공학사)
2001년 부경대학교 대학원 전자계산학과(이학석사)
2002년~현재 부경대학교 대학원 전자계산학과 박사과정

관심분야 : 디지털 워터마킹, 신호처리



박 지 환

1984년 경희대학교 전자공학과 (공학사)
1987년 일본 국립 전기통신대학 정보공학과(공학석사)
1990년 일본 요코하마국립대학 전자정보 공학과(공학박사)
1990년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
1996년~현재 동경대학 생산기술연구소 협력연구원
1997년~현재 한국정보보호학회 이사
1998년~현재 한국멀티미디어학회 운영위원 및 논문지 편집위원
1999년~현재 한국정보처리학회 논문지 편집위원
2002년~현재 한국정보보호학회 영남지부장 및 논문지 편집위원

관심분야 : 멀티미디어 컨텐츠 보호 및 응용, 암호학