인증과 무결성을 위한 비밀키 워터마킹

우 찬 일† · 신 인 철††

요 약

디지털 워터마크는 멀티미디어 콘텐츠에 대한 지적권 보호와 인증의 목적으로 최근에 제안되었다. 워터마킹 기술은 공간 영역이나 주파수 영역에서 영상 내에 워터마킹 구조를 혼합하는 알고리즘으로 구성된다

본 논문에서는 디지털 영상의 인증과 무결성을 위한 새로운 워터마킹 방법을 제안하였고, 제안된 알고리즘은 MD5 해쉬 함수와 대칭키 암호 알고리즘을 사용하였다 원 영상에 삽입되는 워터마크의 위치와 픽셀 내의 비트 위치를 결정하기 위하여 비밀키를 MD5 해쉬 함수의 입력으로 사용하였다 시뮬레이션 결과는 제안하는 알고리즘이 삽입된 워터마크의 위치를 찾기 어려운 장점을 가지며, 워터마크 된 영상의 화질이 Wong의 방법과 비슷하게 유지됨을 보인다

A Secret Key Watermarking for Authentication and Integrity

Chan-Il Woo† · In-Chul Shin††

ABSTRACT

Digital watermarks have recently been proposed for the purposes of copyright protection and authentication for multimedia contents. A watermarking technique consists of an algorithm that incorporates a watermarking structure into an image in the spatial or frequency domains.

In this paper we proposed a new watermarking method for authentication and integrity of digital images and the proposed algorithm uses the MD5 hash function and a symmetric key encryption algorithm To decide the position of embedding watermark and the bit position in the original image, the secret key is used as an input of the MD5 hash function The simulation results show that the proposed algorithm has the advantage of difficulty to find positions of inserted watermarks, and keep the similar watermarked image quality with Wong's method

1. 서 론

최근 통신망이 확대 보급되면서 정보교환이 신속하게 이루어지고 있고, 컴퓨터 기술의 급속한 발전으로 인하여 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 등의 멀티미디어를 제공하는 환경으로 변하고 있다.

†준 회 원 : 단국대학교 대학원 전자공학과
††정 회 원 단국대학교 전자·컴퓨터공학과 교수
논문접수 2000년 6월 27일, 심사완료 : 2000년 11월 24일

따라서 인터넷 등의 대중 네트웍을 통하여 디지털 정보를 송, 수신하는데 있어서 정보의 보안성이 중요한 문제점으로 대두되고 있으며, 또한 자신의 정보를 제3의 사용자로부터 불법적으로 사용되어 지는 것이나 데이터의 변조를 막기 위한 수단으로 암호 기술이 개발되어 사용되었다 암호화 방법은 데이터를 특정한 키에 의하여 알 수 없는 정보로 암호화하여 전송하는 것으로 데이터를 송, 수신하는데 있어서 불법적인 사용자로부터 데이터를 안전하게 보호할 수 있는 방법을

제공하고 있으며, 영상이나 오디오 등의 멀티미디어에 대한 저작권을 부여할 수 있는 방법으로 워터마킹 방법이 제안되었다[1-4].

인터넷상에서 디지털 영상 정보를 보호하기 위한 방법으로는 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 미디어에 대한 소유권을 주장할 수 있는 방법을 제공한다. 또한 디지털 영상에 대한 인증(Authentication)과 무결성(Integrity)을 위한 디지털 워터마킹은 디지털 데이터의 내용이 조작되거나 변형되지 않았다는 것을 확인하면서 그 영상물의 송신자나 소유자를 확인할 수 있는 방법을 제공한다[4-9].

디지털 워터마크는 크게 공간 영역 워터마크(Spatial domain watermark)와 주파수 영역 워터마크(Frequency domain watermark)로 분류할 수 있으며, 주파수 영역 워터마크는 영상 데이터를 DCT domain, Wavelet domain, Fourier transform domain 등과 같은 변환으로 주파수 공간으로 변환하여 워터마크를 삽입한다. 그러나 고의적인 영상 변형, 손실압축, 필터링 등과 같은 영상 왜곡에 워터마크가 손실 될 수 있다.

공간영역 워터마킹 기술은 인간의 시각이 영상의 밝기에 민감하지 않다는 것을 이용하여 영상의 픽셀 값에서 LSB를 조작하여 윤곽선의 밝기 값을 변화시키는 방법으로 원 영상에 시각적으로 인식할 수 없는 워터마크를 삽입하는데 효과적이다. 그러나 제3자에 의하여 고의적으로 워터마크가 삽입된 영상의 LSB를 삭제하여 자신의 워터마크를 삽입할 수 있는 단점이 있다[1, 2, 9].

본 논문에서는 공간영역 워터마킹 기술을 사용하여 워터마크가 삽입되는 위치를 숨기고 디지털 영상의 인증 및 무결성을 확인하기 위한 방법을 제시하였다. 이를 위하여 기존에 나와 있는 방법을 살펴보고 이들의 장단점을 살펴본 뒤 기존의 방법이 가지는 문제점을 해결할 수 있는 방법을 MD5 해쉬 함수와 대칭키 암호를 사용하여 제안한다.

2. 디지털 워터마킹

워터마크(watermark)의 사전적 의미는 "물이 흔들릴 때 밝게 빛나는 부분", "종이나 서류에 투명한 표시를 하여 빛에 밝게 비추어 보면 나타나는 무늬 문양"이다[10]. 따라서 워터마크란 음성, 영상 등의 디지털 데이터에 삽입되는 정보를 말하고, 이러한 기술을 적용한 것을 디지털 워터마킹이라 한다. 일반적으로 디지털 워터마킹은 저작권(copyright)의 보호나 인증(authentication)을 위한 정보를 디지털 데이터에 삽입하는 것이다[11-16].

2.1 디지털 워터마크의 분류.

디지털 워터마크 기술은 관점에 따라 여러 가지 방법으로 나눌 수 있는데 일반적으로 다음과 같이 분류할 수 있다[1, 2].

2.2.1 견고성에 의한 분류

- Fragile 워터마킹 : 영상에 대한 사소한 변화에 대해 워터마크가 쉽게 지워짐.
- Semi-Fragile 워터마킹 : 사용자가 규정한 한계 치를 초과하는 경우 워터마크 손상.
- Robust 워터마킹 : 통상적인 영상처리 기법에 의해 워터마크가 잘 지워지지 않음

2.2.2 영역에 의한 분류

- Spatial 워터마킹 : 공간영역에서의 워터마킹
- Spectral 워터마킹 : 주파수 영역에서의 워터마킹

2.2.3 가시성에 의한 분류

- Visible : 삽입된 워터마크가 시각적으로 관찰됨.
- Invisible : 삽입된 워터마크를 시각적으로 구분할 수 없음

2.2.4 기타

- Public 워터마킹 : 사용자가 워터마크 검출 필요시 검출 알고리즘 공개.
- Private 워터마킹 : 사용자가 워터마크 검출 불 필요시 검출 알고리즘 비공개.
- Blind 워터마킹 : 원영상을 사용하지 않고 워터마크를 검증할 수 있는 기술
- Image Adaptive 워터마킹 : 인간시각 특성을 이용하여 영상의 내용에 따라 워터마크의 강도를 적응적으로 설정

2.2 주파수 영역 워터마킹.

이 방법은 DCT, Wavelet, Fourier Transform된 계수에 워터마크를 삽입하는 것으로 압축에러에도 워터마크가 존재하기 위해서는 인간시각의 민감한 부위에 워터마크를 삽입해야 한다. 그러나 invisible 워터마크의 조건과 상충되므로, 이를 해결할 수 있는 방법으로 영상 내의 워터마크를 시각적으로 감지할 수 없도록 하면서 시각적으로 중요하고 민감한 부분에 워터마크를 삽입할 수 있는 주파수 확산 워터마킹 방법이 있다. 주파수 확산 워터마킹 방법은 워터마크를 영상이 가지고 있는 넓은 주파수 대역으로 확산하여 이런 특정 주파수 성분에 부착된 워터마크의 에너지는 감지할 수 없을 정도로 작지만 워터마크가 찍힌 주파수의 위치와 변화량을 알고 있는 소유자에 의해 산재해 있는 워터마크 성분을 모으면 높은 신호대 잡음비로 워터마크를 검출할 수 있다. 주파수 확산 워터마킹 방법은 여러 가지 에러환경에서 강인한 특성을 가지며 저작권 정보를 추출하는데 원 영상이 필요하지 않다는 장점을 가지고 있다[1, 2, 14-16].

2.3 인증과 무결성을 위한 워터마킹

2.3.1 공개키 암호 알고리즘을 이용한 방법[17,18]

공개키 암호 알고리즘은 이미지 전체를 암호화하지 않고서도 이미지에 대한 인증을 수행할 수 있는 방법을 제공한다. 이미지에 대한 인증을 수행하는 절차는 아래와 같다.

① 인증에 사용될 digital signature를 생성한다. Digital signature는 암호학적 해쉬 함수를 사용해서 만들어진다.
signature = hash(image)
② 비밀키(private key)를 사용해서 digital signature를 암호화한다.
authenticator = 공개키암호(signature)
③ 암호화된 authenticator와 image를 전송한다.
④ 수신자는 공개키(public key)를 사용해서 암호화된 authenticator를 복호화하고, 송신자에게서 받은 image에 대한 해쉬 함수 값을 구한다. 그리고 원 영상의 해쉬 값과 수신된 해쉬 값을 비교하면 이미지가 변경되었는지 확인할 수 있게 되고, 송신자의 공개키를 사용해서 복호화 했으므로 송신자가 누구인가를 알 수 있게된다

2.3.2 TimeStamp 사용[7, 17]

TimeStamp를 사용하는 방법은 누군가가 영상을 소유했다는 것을 증명하기 위해서 영상에 스탬프를 찍는 방법이다. 이를 위해서 이미지의 소유자는 믿을 수 있는 제3의 기관을 통해서 그 영상의 해쉬 함수 값과 날짜를 등록하게 된다.

2.3.3 Yeung and Mintzer 알고리즘[1]

영상의 조작여부를 확인할 수 있을 뿐만 아니라 조작된 위치도 확인 가능한 Fragile 워터마킹 방법으로 원 영상 없이 워터마크와 워터마크 추출함수로 워터마크를 검출할 수 있다.

2.3.4 Wong 알고리즘[1, 9]

Wong의 알고리즘은 올바른 비밀키를 사용해야 인증 및 무결성을 확인할 수 있고, 또한 영상의 조작여부 및 블록단위의 조작위치가 확인 가능한 장점이 있다. 그러나 워터마크가 삽입되는 위치가 노출되어 쉽게 워터마크를 추출하여 제거할 수 있다는 단점이 있다. 알고리즘의 수행 절차는 다음과 같다

① 영상을 8×8 크기를 가지는 여러 블록으로 분할.
② 블록내 각 픽셀의 LSB 제거.
③ 나머지 MSBs 비트와 영상의 크기정보를 해쉬 함수의 입력으로 하여 디지털 서명(digital signature)을 생성한 후 워터마크와 XOR 연산 수행.
④ XOR 연산된 데이터를 사용자의 비밀키로 암호화한 후 영상의 LSB에 삽입.

이외에도 영상의 LSB 부분에 checksum을 삽입하는 방법등이 있다

3. 해쉬 함수

해쉬 함수는 임의의 크기의 입력 비트 열에 대하여 항상 고정된 길이의 출력 비트 열(해쉬 코드)을 생성한다. 이러한 해쉬 함수는 생성된 해쉬 코드에 대하여 이 해쉬 코드를 생성하는데 사용한 입력 데이터 스트링을 찾아내는 것이 계산상 실행 불가능하며, 주어진 입력 비트 열에 대하여 같은 해쉬 코드를 생성하는 또 다른 데이터 스트링을 찾아내는 것은 계산상 불가능하다는 두 가지 성질을 만족하는 함수를 말한다[17, 18].

해쉬 함수 h는 다음과 같은 네 조건을 만족해야 한다.

- h는 임의의 크기의 입력 메시지 M에 적용할 수 있을 것.
- h는 일정한 크기의 출력 $H=h(M)$를 낼 것.
- h와 메시지 M이 주어졌을 때 $H=h(M)$을 계산하기 쉬울 것.
- $H=h(M)$가 주어졌을 때 메시지 M을 구하는 역의 계산이 불가능 할 것.

3.1 MD5 해쉬 함수

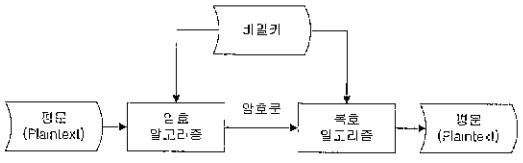
Ron Rivest에 의하여 개발된 MD4 해쉬 함수는 통상적인 해쉬 함수의 안전성을 확보하고 있고, 32비트의 기반 구조를 가진 빠른 알고리즘으로 구성되어 실행 속도에 효율성을 확보하고 있는 특징이 있다. 그러나 MD4의 마지막 두 라운드가 해독되었고, DC 공격에 의해서도 해독되어 MD5를 제안하였다.

MD4와 MD5의 차이점은 다음과 같다.

- MD4는 16단계의 3라운드를 사용하나, MD5는 16단계의 4라운드를 사용한다.
- MD4는 각 라운드에서 한 번씩 3개의 기약함수를 사용하고, MD5는 각 라운드에서 한번씩 4개의 기약 논리 함수를 사용한다.
- MD5의 각 단계는 이전 단계의 결과에 부가된다.

3.2 대칭형 암호 시스템

암호화를 이용한 보안 서비스를 제공하는 암호시스템은 송, 수신자 양측이 같은 키를 사용하는 DES(data encryption standard)와 같은 대칭형 암호시스템과 송, 수신자가 각각 다른 키를 사용하는 RSA(Rivest-Shamir-Adleman)와 같은 공개키 암호 시스템으로 대별된다. 암호화 과정은 암호 알고리즘과 키로 구성되는데 키는 알고리즘을 제어하는 평문과 무관하게 독립된 값을 사용하며 암호 알고리즘은 사용된 특정키에 따라 상이한 결과를 생성한다. 따라서 대칭형 암호 방식에서 생성된 암호문은 복호 알고리즘과 암호화에 사용했던 것과 동일한 키를 사용하여 평문으로 재 변환된다.



(그림 1) 대칭형 암호

4. 제안알고리즘

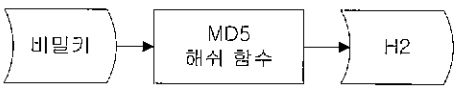
데이터에 대한 인증과 무결성을 체크하는 기존의 방법 중 공개키 암호 알고리즘을 이용한 Wong의 방법이 인증과 무결성을 위한 워터마크 방법으로 가장 적합하다. 특히 Wong의 방법은 암호학적 해쉬 함수를 사용하므로 워터마킹 알고리즘의 안전성이 암호학적 해쉬 함수의 안전성에 의존하게 된다. 그러나 워터마크가 삽입된 이미지를 공개하는 경우 제3자가 영상내의 LSB를 삭제하고 자신의 비밀키를 사용해서 서명을 만든 뒤 LSB 부분에 삽입 할 수 있는 단점이 있다[1, 9].

본 논문에서 제안하는 알고리즘은 영상 픽셀(pixel)내의 LSB에 워터마크가 삽입되어 제3자가 삽입된 워터마크를 쉽게 추출 및 제거할 수 있는 단점을 가진 Wong의 알고리즘을 보완하여, 워터마크가 삽입되는 위치를 랜덤하게 선택해서 삽입되는 위치를 알지 못하도록 하는 것이다. 이를 위하여 비밀키를 해쉬 함수의 입력으로 주어 디지털 서명을 만든 후 워터마크가 삽입되는 픽셀의 위치와 선택된 픽셀내의 특정 비트를 선택하여 워터마크를 삽입 및 추출하는 방법을 제안한다.

4.1 워터마크 삽입 알고리즘

4.1.1 해쉬 코드 생성

원 영상에 워터마크가 삽입되는 위치를 계산하기 위하여 비밀키를 MD5 해쉬 함수의 입력으로 사용하여 128비트 해쉬 출력 코드(H2)를 생성한다.



(그림 2) 해쉬 코드 생성

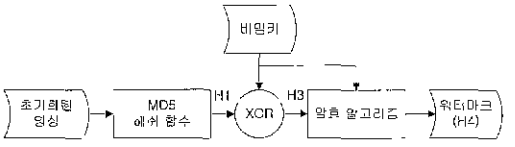
4.1.2 삽입 위치 결정

비밀키의 해쉬 출력 코드(H2)를 각각 N비트 블록과 M비트 블록으로 나누어 저장한 후, M비트 블록 값과 N비트 블록 값을 곱하여 워터마크가 삽입될 원 영상의 픽셀을 선택한다 그리고 선택된 픽셀 내에서 워터마크의 1비트를 삽입하기 위하여 N비트 블록 값으로 픽셀 내의 특정 비트를 선택한다. 본 논문에서 M과 N 비트 블록은 각각 4비트와 2비트로 선정하였다.

4.1.3 워터마크 생성

M과 N의 곱에 의해 선택된 원 영상의 비트들을 "0"

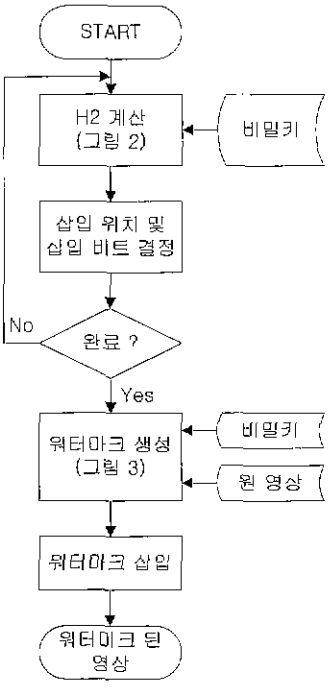
으로 초기화한 후 MD5 해쉬 함수의 입력으로 주어 128비트 출력(H1)을 생성한다. 그리고 H1과 비밀키를 XOR하여 생성된 결과(H3)를 비밀키로 암호화하여 워터마크(H4)를 생성한다.



(그림 3) 워터마크 생성과정

4.1.4 워터마크 삽입

M비트 블록과 N비트 블록을 곱하여 원 영상에서 워터마크가 삽입될 픽셀을 선택하고, 선택된 픽셀 내에서 워터마크의 1비트를 삽입하기 위하여 N비트 블록 값으로 임의의 비트를 선택하여 워터마크를 삽입한다.



(그림 4) 워터마크 삽입 과정

4.2 워터마크 추출 알고리즘

4.2.1 해쉬 코드 생성

수신자의 비밀키를 MD5 해쉬 함수의 입력으로 주어 128비트 해쉬 코드(H2)를 생성하고, H2를 각각 M비트 블록과 N비트 블록으로 나눈다

4.2.2 워터마크 추출

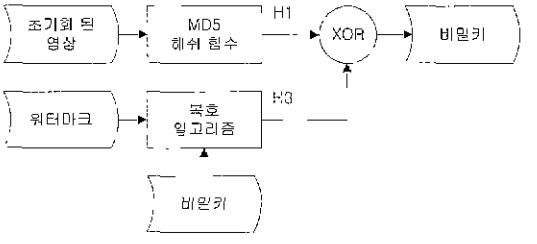
H2의 M비트와 N비트를 곱하여 워터마크가 삽입된 픽셀을 계산하고, N비트의 값으로 선택된 픽셀 내에 삽입된 비트를 선택한 후 워터마크를 추출한다. 추출된 워터마크는 수신자의 비밀키로 복호화 하여 H3를 생성한다

4.2.3 영상 초기화

워터마크가 삽입된 영상에서 워터마크를 추출한 후 워터마크 된 영상의 비트들을 "0"으로 초기화하고, 초기화된 영상을 MD5 해쉬 함수의 입력으로 주어 128비트 해쉬 출력 (H1)을 생성한다

4.3 인 증

초기화된 영상의 해쉬 출력 H1과 복호화 된 워터마크(H3)를 XOR하여 워터마크 생성에 사용된 비밀키를 추출한다. 그리고 추출된 비밀키와 복호화에 사용된 수신자의 비밀키를 비교하여 같으면 워터마크 된 영상에 대하여 어떠한 변형이 발생되지 않았음을 확인할 수 있고, 송신자에 대한 인증을 완료한다.



(그림 5) 인증 과정

5. 실험 및 결과

본 논문에서 제안한 알고리즘은 비밀키를 해쉬 함수의 입력으로 사용하여 생성된 해쉬 코드 128비트를 각각 M비트와 N비트 블록으로 나누어 원 영상에서 워터마크가 삽입될 픽셀을 선택하고 선택된 픽셀 내의 임의의 비트에 워터마크를 삽입하고 추출하였다. 실험에 사용된 워터마크를 생성하기 위하여 비밀키의 해쉬 출력(H2)의 M비트 블록과 N비트 블록을 곱하여 원

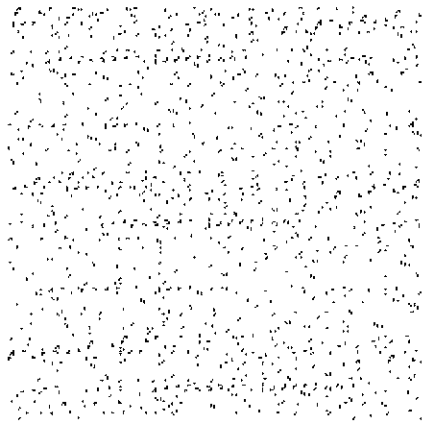
영상에서 픽셀을 선택하고, N비트 값에 의하여 선택된 픽셀 내의 특정 비트를 선택하여 "0"으로 초기화한다. 그리고 초기화된 영상을 해쉬 함수의 입력으로 사용하여 생성된 128비트 출력(H1)과 비밀키를 XOR 한 후 암호화하여 생성된 값을 사용하였다. 실험 결과로 원 영상과 워터마크가 삽입된 영상을 비교하여 (그림 6)과 (그림 7)에 나타내었으며 (그림 8)은 워터마크가 삽입된 위치들을 보여준다.

〈표 1〉 실험에 사용된 인수들

비 밀 키	3a ec d2 59 2b 58 c1 38 1c 2 9a 5e 33 3a 5d 8c
비밀키의 해 쉬 값	6 19 91 86 1b e7 51 6 e6 37 fb ec d1 bb a7 ef
M 비트 블록 값	0 6 1 9 9 1 8 6 1 b e 7 5 1 0 6 e 6 3 7 f b e c d 1 b b a 7 e f
N 비트 블록 값	0 0 1 2 0 1 2 1 2 1 0 1 2 0 1 2 0 1 2 3 3 2 1 3 1 1 0 1 0 0 1 2 3 2 1 2 0 3 1 3 3 3 2 3 3 2 3 0 3 1 0 1 2 3 2 3 2 2 1 3 3 2 3 3
워터마크	0 fe b4 53 7c 6f 30 6d 80 99 d0 93 5c 9a e5 7c

(그림 6) 256×256 Lena 영상.

(그림 7) 워터마크가 삽입된 영상



(그림 8) 워터마크 삽입 위치

〈표 2〉 워터마킹된 영상들의 PSNR

영 상	Lena	Airplane	Baboon	Peppers	Gul
PSNR	52.42	52.08	52.15	52.21	52.57

실험결과를 살펴보면 워터마크가 삽입된 영상은 인간의 시각으로 원 영상과의 차이점을 발견할 수 없으며, 워터마크가 삽입된 영상에 대하여 PSNR을 구한 결과를 <표 2>에 나타내었다. 실험결과에서 워터마크가 삽입되는 범위를 LSB에서 MSBs로 확장하더라도 128비트의 워터마크를 삽입하여 51.13dB의 PSNR을 나타내는 Wong의 알고리즘과 비교하여 이미지 훼손이 발생하지 않음을 알 수 있다. 또한 Wong 알고리즘의 경우 영상의 LSB 부분 모두를 워터마크가 삽입되는 위치로 사용하여 워터마크가 삽입되는 위치가 노출된다는 단점을 가진다. 하지만 본 논문에서 제안한 알고리즘의 경우, 영상 내의 어느 곳에 워터마크가 삽입되는지 알 수 없도록 픽셀 내의 비트를 LSB에서 MSBs로 확장하여 제3자에 의한 의도적인 워터마크 추출을 방지할 수 있다.

6. 결 론

인터넷이 널리 사용되고 있는 현 시점에서 디지털 영상 및 음성 등의 디지털 미디어를 보호하기 위해서 암호화 방법, 사이트 보호방법, 디지털 워터마킹 방법이 대안으로 떠오르고 있다.

본 논문에서는 워터마킹 방법을 사용하여 디지털

영상의 인증과 무결성을 위한 새로운 방법을 제안하였다. 제안된 알고리즘은 암호학적 어려움을 기반으로 한 해쉬 함수와 공개키 암호 알고리즘을 사용한 Wong의 알고리즘을 개선한 것으로, 임의의 입력 비트 열에 대하여 128비트의 안전한 출력 비트 열을 생성하는 MD5 해쉬 함수를 사용하여 영상내의 임의의 픽셀을 선정하고 선택된 픽셀 내의 임의의 비트에 워터마크를 삽입 및 추출하였다. MD5 해쉬 함수, 비밀키 암호 알고리즘 및 워터마크 삽입, 추출 알고리즘은 Pentium 450MHz PC상에서 C언어로 구현하여 그레이 레벨의 Lena 영상을 대상으로 실험하였다. 실험결과로 원 영상과 워터마크가 삽입된 영상에 대하여 PSNR을 구하여 Wong이 제시한 방법과 비교하였을 경우 워터마크의 삽입 위치가 LSB에서 MSBs로 확장되더라도 이미지 훼손이 발생하지 않음을 알 수 있다. 또한 Wong의 알고리즘은 워터마크를 영상의 LSB에 삽입하여 제3자가 쉽게 워터마크를 추출하여 제거가 용이한 반면, 본 논문에서 제안한 알고리즘의 경우 워터마크가 삽입되는 위치를 숨길 수 있다는 장점을 가지고 있다

향후 연구 과제로는 제안한 알고리즘이 디지털 영상의 인증과 무결성을 위한 목적 외에 저작권 보호를 위하여 Filtering이나 압축과 같은 영상 변형에도 안전하기 위하여 암호학적인 접근 외에 Wavelet, DCT 등의 영상처리 측면에서 폭넓은 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] 원치선, "NETSEC-KR '99", 한국정보보호센터, pp 155-170, 1999.

[2] 최윤식, "2000년대 화상처리 및 텔레비전 방송기술 발전 전망", 대한전자공학회지, 제27권 제2호, pp.38-45, 2000.

[3] L. Qian and K. Nahrstedt, "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights," Pre-print, 1998

[4] K S NG and L.M CHENG "Selective block assignment approach for robust digital image watermarking," Proc. of SPIE, Vol 3657, Jan, pp 14-20, 1999

[5] D Kundur, D Hatzinakos, "A Robust Digital Image Watermarking Method using Wavelet-Based Fusion," Proc. IEEE ICIP, Santa Barbara, California, Vol.1, pp.544-547, Oct, 1997

[6] R B Wolfgang, J D Edward, "Fragile Watermarking Using VW2D Watermark," Proc of SPIE, Vol 3657, Jan, pp 204-213, 1999

[7] Scott Craver, Nasir Memon, Boon-Lock Yeo and Minerva Yeung, "Can invisible watermarks resolve rightful ownership," Proc. of IS&T/SPIE, USA, Feb. 13-14, 1997, Vol 3022, pp.310-321

[8] D. Bearman, and J. Trant, "Authenticity of Digital Resources Towards a Statement of Requirements in the Research Process," D-Lib Magazine, June 1998.

[9] P. W. Wong, "A Public Key Watermark for Image Verification and Authentication," In Proc of ICIP, Oct. 1998.

[10] The American Heritage Dictionary, 3rd Edition. Dell publishing, pp.910, 1994.

[11] E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of Image Alterations Using Semi-Fragile Watermarks," Proc. SPIE, Vol.3971, Jan. 2000.

[12] M P. Queluz, "Content-based integrity protection of digital images," Proc. of SPIE, Vol.3657, Jan, pp.85-93, 1999.

[13] Norishige Morimoto, "Techniques for Data Hiding in Audio Files," MIT Master Thesis, June 1995.

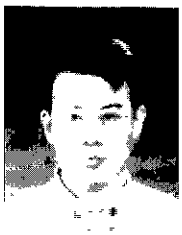
[14] M. D. Swanson, Bin Zhu, A. H. Tewfik, "Transparent Robust Image Watermarking," Proc. IEEE ICIP, Vol.3, Sep. pp.211-214, 1996.

[15] Keith T Knox, "Reversible Digital Image," Proc of SPIE, Jan. pp.397-401 1999.

[16] R B. Wolfgang, E. J. Delp, "A Watermark for Digital Image," Proc. of ICIP, Vol.3, pp 219-222, 1996.

[17] Bruce Schneier, *Applied Cryptography*, Willey, 1996.

[18] William Stallings, *Network and Internetwork Security*, Prentice Hall, 1995



우 찬 일

e-mail ciwoo@dankook.ac.kr

1993년 단국대학교 전자공학과 졸업(학사)

1995년 단국대학교 대학원 전자공학과 졸업(공학석사)

1997년~현재 단국대학교 대학원 전자공학과 박사과정

1995년~1997년 LG이노텍 연구원

관심분야 : 정보보안, 전자상거래, 디지털 워터마킹

신 인 철

e-mail : chai@dankook.ac.kr

1973년 고려대학교 전지공학과 졸업(학사)

1978년 고려대학교 대학원 전자공학과 졸업(공학석사)

1986년 고려대학교 대학원 전지공학과 졸업(공학박사)

1979~현재 단국대학교 전자·컴퓨터공학과 교수

관심분야 : 병렬처리, 정보보안, 스마트카드, 전자상거래, 디지털 워터마킹