Journal of Korea Multimedia Society Vol. 8, No. 11, November 2005(pp. 1462-1471)

ROI를 고려한 공개키 암호화 알고리즘 기반 의료영상 디지털 워터마킹

이형교[†], 김희정[††], 성택영[†††], 권기룡[††††], 이종극[†††††]

요 약

정보통신 기술 및 컴퓨터의 발달로 의료기기의 디지털화가 가능하게 되어 의료 영상 분야에 다양한 활용이 이루어지고 있다. DICOM 표준에 따른 PACS의 구축으로 의료 영상의 저장, 데이터베이스 검색 및 네트워크를 통한 원격 진료가 가능하게 됨으로써 의료 영상에 대한 불법복제, 소유권 및 데이터 인증 문제가 야기되고 있다. 본 논문에서는 무결성 인증을 위하여 공개 키 암호화 알고리즘을 기반한 새로운 의료 영상 디지털 워터마킹 기법을 제안한다. 이는 의료 영상 데이터를 원격으로 전송 후에 발생하는 불법적인 위/변조를 막기 위한 디지털 워터마킹 기법이다. 워터마크는 원 의료 영상을 웨이블릿 변환 후 비트플레인 값을 사용한다. 제안한 방법에서 삽입되는 영역은 ROI(region of interest)를 고려하여 랜덤하게 선택되도록 하고, MD5의 해쉬 함수는 디지털 서명을 생성하기 위하여 비밀 키로 사용한다. 실험 결과 제안한 알고리즘은 영상 처리에서도 워터마크 정보를 검출할 수 있으며 비가시성이 우수하다.

Digital Watermarking of Medical Image Based on Public Key Encryption Algorithm Considering ROI

Hyung-Kyo Lee[†], Hee-Jung Kim[††], Tack-Young Seong[†††], Ki-Ryong Kwon[††††], Jong-Keuk Lee[†††††]

ABSTRACT

Recently, the medical image has been digitized by the development of computer science and digitization of the medical devices. There are needs for database service of the medical image and long term storage because of the construction of PACS(picture archiving and communication system) following DICOM(digital imaging communications in medicine) standards, telemedicine, and et al. However, it also caused some kinds of problems, such as illegal reproduction of medical image, proprietary rights and data authentication. In this paper, we propose the new digital watermarking technique for medical image based on public key encryption algorithm for integrity verification. It prevents illegal forgery that can be caused after transmitting medical image data remotely. The watermark is the value of bit-plane in wavelet transform of the original image for certification method of integrity verification. We proposed the embedding regions are randomly chosen considering ROI, and a digital signature is made using hash function of MD5 which input is a secret key. The experimental results show that the watermark embedded by the proposed algorithm can survive successfully in image processing operations and that the watermark's invisibility is good.

Key words: PACS, DICOM, Digital Watermarking(디지털 워터마킹), Public Key Encryption Algorithm (공개키 암호화 알고리즘)

※ 교신저자(Corresponding Author) : 권기룡, 주소 : 부산광역시 남구 우암동 산 55-1(608-738), 전화 : 051)640-3176, FAX : 051)640-3428, E-mail : krkwon@pufs.ac.kr
접수일 : 2005년 9월 21일, 완료일 : 2005년 10월 28일
[†] 정회원, 안동과학대학 의료정보과 교수
(E-mail : hyungkyolee@hanmail.net)
[††] 준회원, 부산외국어대학교 교양연계부 초빙교수
(E-mail : khj@pufs.ac.kr)
[†††] 준회원, 부산외국어대학교 대학원 전자컴퓨터공학과 석사과정
(E-mail : sty76@hanmail.net)
[††††] 종신회원, 부산외국어대학교 디지털정보공학부 부교수
[†††††] 종신회원, 동의대학교 컴퓨터공학과 교수
(E-mail : jklee@deu.ac.kr)
※ 본 연구는 *2005년도 부산외국어대학교 학술연구조성비 및 **2004년도 Brain Busan 21 사업에 의하여 연구 되었음.

1. 서 론

최근 과학 기술의 발달로 의료 영상의 획득과 저장이 디지털화됨으로써 이러한 정보들을 데이터베이스화시켜 네트워크를 통한 원격 진료가 가능한 디지털 병원 시대를 맞이하고 있다.

PACS(picture archiving and communication system)는 각종 영상 촬영장치(modality)로 촬영한 영상들을 CR(computed radiography)를 통해 디지털화하여 하드 디스크와 같은 저장매체에 저장하고, 네트워크를 통해 각 단말기로 전송하여 진찰실, 병동 등의 워크스테이션이 있는 곳이면 어디에서든 실시간으로 환자의 영상을 조회할 수 있는 시스템이다. 이에 따라 의료정보시스템인 HIS(hospital information system)와 연계하여 병원의 의학 영상, 관련 임상정보, ADT(입퇴원, 전과)를 전산화하여 효율적으로 통합 관리 할 수 있다[1,2].

뿐만 아니라 초고속 네트워크의 발달로 이러한 의료 정보들을 인터넷과 같은 개방형 네트워크를 통하여 전송함으로써 원격 진료 및 원격 상담이 가능하며, 보험금 지급이나 병무청의 근거 서류로 사용될 수 있다. 이러한 시스템의 이용에 있어 의료 영상의 조작이나 훼손 혹은 영상 진단자의 인증 등의 의료정보의 보안 문제가 크게 대두되고 있다. 현재 환자에게 필름을 복사해서 주던 방식에서 CD 복제물로 제공함으로써 불법적인 위/변조로 진단서 재교부나 보험사기, 병역기피에의 악용 등의 취약점을 가지고 있다.

따라서 이러한 의료영상의 무결성(integrity) 및 저작권 보호(copyright protection)를 위한 새로운 대안으로 멀티미디어 콘텐츠에 대한 소유권 및 내용 인증(authentication)을 제공하는 디지털 워터마킹 기술을 적용하여 의료영상 보호시스템을 구현하는 연구가 활발히 진행중이다[3-8].

디지털 콘텐츠의 정보보호 기법은 일반적으로 키(key)를 이용한 암호화 방법 및 디지털 워터마킹 방법을 사용한다. 암호화 방법은 데이터를 특정한 키에 의하여 알 수 없는 정보로 암호화하여 전송하는 것으로 데이터를 송·수신하는데 있어 불법적인 사용자로부터 데이터를 안전하게 보호할 수 있는 방법을 제공하나 암호가 해킹을 당한 경우 정보보호가 사실상 어렵게 된다. 디지털 워터마킹은 사람의 눈에 식별할 수 없는 정보를 콘텐츠 내에 삽입, 추출하는 것으로 디지털 데이터에 대한 소유권자가 워터마크를 추출하여 자신의 저작권을 주장할 수 있는 방법으로 이러한 디지털 워터마킹 기법은 목적과 용도에 따라 소유권 주장을 위한 강인한 워터마킹(robust watermarking)과 영상의 변질검증을 위한 연성 워터마킹(fragile watermarking)으로 나눌 수 있다.

소유권 주장을 위한 워터마킹은 일반적인 워터마킹의 방법으로 창작자의 디지털 미디어 콘텐츠에 대한 소유 관계를 주장을 위해 워터마크를 사용하는 것이다. 이 방법은 영상에 대한 압축, 확대, 축소 및 포맷 변환 등과 같은 일반적인 영상처리 수행 후에도 워터마크가 존재해야 하는 것으로 워터마크의 강인성(robustness)이 요구된다. 또한 워터마킹된 영상은 워터마크가 시각적으로 인지되지 않는 비가시성(invisibility)을 만족해야하며, 삽입되는 워터마크는 추출되었을 때 저작권의 판단이 가능한 비모호성(unambiguousness)이 만족되어야 한다.

영상의 변질 검증을 위한 것은 멀티미디어 콘텐츠가 법적인 용도, 의학적인 용도, 뉴스 혹은 상업적인 용도로 사용되는 경우 콘텐츠가 훼손되거나 수정되지 않음을 확인 하는 것이다. 이를 위해 영상의 어떤 부분이 변질되었는지를 시각적으로 명백히 판단할 수 있는 방법이 필요하며 영상의 변질 여부를 검증하기 위한 요구사항은 다음과 같다. 첫째, 영상의 변조 여부를 추출된 워터마크를 통해 확인 할 수 있어야 하고, 두 번째로 영상이 변조된 경우 영상의 어느 위치가 변조되었는지를 검출할 수 있어야 한다. 세 번째로는 원 영상 없이 워터마크를 추출할 수 있어야하고 마지막으로 워터마크는 인간의 시각에 의해 인지되지 않아야 한다.

이러한 연성 워터마킹의 삽입은 공간 영역(spatial domain) 워터마크와 주파수 영역 워터마크로 분류할 수 있으며, 주파수 영역의 워터마크는 영상 데이터를 FFT(fast fourier transform), DCT(discrete cosine transform), DWT(discrete wavelet transform) 등과 같은 주파수 공간으로 변환하여 워터마크를 삽입한다. 그러나 고의적인 영상 변형, 손실 압축, 필터링과 같은 영상 왜곡에 워터마크가 손실 될 수 있다.

공간영역 워터마킹 기술은 인간의 시각이 영상의 밝기에 민감하지 않다는 것을 이용하여 영상의 픽셀 값에서 LSB(least significant bit)를 조작하여 윤곽

선의 밝기 값을 변화시키는 방법으로 원 영상에 시각적으로 인식할 수 없는 워터마크를 삽입하는데 효과적이다. 그러나 제 3자에 의하여 고의적으로 워터마크가 삽입된 영상의 LSB를 삭제하여 자신의 워터마크를 삽입할 수 있는 단점이 있다.

인증과 무결성을 위한 기존의 워터마킹 기법으로 누군가가 영상을 소유했다는 것을 증명하기 위해서 영상에 스탬프를 찍는 방법이 있다. 이는 영상의 소유권자가 믿을 수 있는 제 3의 기관을 통해서 그 영상의 해쉬 함수 값과 날짜를 등록한다. 또한 영상의 전체를 암호화 하지 않고 영상에 대한 인증을 하는 방법으로 공개 키 암호 알고리즘을 사용한다[9,10].

Wong[11,12]은 인증 및 무결성을 확인하기 위하여 워터마크를 영상의 LSB에만 삽입하는 방식을 제시하였다. 이 방법은 영상의 조작여부 및 블록 단위의 조작 위치를 확인할 수 있는 장점이 있으나, 워터마크가 삽입되는 위치가 노출되어 쉽게 워터마크를 추출하여 제거할 수 있는 문제점이 있다.

Yeung[13]은 원 영상의 각 화소에 대하여 이진 로고의 워터마크를 삽입하여 화질이 좋으면서 눈에 보이지 않는 워터마크를 제안하였다. 이 방식은 워터마크로 추출된 이진로고를 통해서 시각적으로 영상의 변조 여부 및 픽셀 단위로 변조 위치를 검출하는데 좋은 성능을 가지고 있다. 그러나 같은 비밀 키와 이진로고를 사용하여 여러 영상에 워터마크를 삽입한 경우에는 공격자가 이진로고와 이진함수를 쉽게 추정하여 워터마크된 영상을 수정하거나 위조 할 수 있는 문제점 있고, Collage 공격에 약하다는 단점이 있다[14,15].

Fridrich[16]는 Yeung의 방식을 기반으로 LUT (look-up table) 대신 블록 암호를 사용하여 안전성에 문제가 없는 방식을 제시하였다. 이 방식은 블록의 개념을 도입하여 각 픽셀의 이웃하는 픽셀들을 결합하여 원 영상에 종속적으로 워터마크를 삽입한다. 그러나 이 방식은 영상의 변조 여부 및 변조 위치를 블록 단위로 검출 할 수 있으나 픽셀 단위로는 변조 위치 검출이 불가능하고 각 픽셀에 워터마크를 삽입시 계산량이 많아지는 문제점이 있다.

Deepthid 등[17]은 의료영상의 워터마킹을 위해 공간 영역의 그레이 레벨 픽셀의 중요도가 낮은 비트인 LSB에 텍스트 문서와 E.C.G와 같은 데이터를 함께 암호화하여 CT 사진과 같은 의료 영상 사이에 끼워 넣는 워터마킹 방법을 제안하였다. Akiyoshi [18]는 압축된 서명 영상을 이용하여 의료 영상의 ROI(region of interest) 주변 영역에 워터마크를 삽입하는 방법을 제안하였다. 이는 원 영상을 ROI 영역으로 구분하고 점진코드에 의해 서명을 압축한 다음 중요도에 따라 비트 스트림을 발생한다. 이를 ROI 주변 픽셀에 나선형으로 삽입을 시키고 HS(hierarchical segmentation)알고리즘[19]으로 압축하는 방식이다.

본 논문에서는 ROI를 고려한 새로운 방법의 공개키 암호화 알고리즘 기반 의료영상 디지털 워터마킹 기법을 제안한다. 제안한 방법은 워터마크를 생성하기 위하여 원 영상을 웨이블릿 변환하여 최저주파 영상을 비트 플레인으로 분해한 다음 로고영상과 매핑(mapping)하여 이것을 랜덤치환(permutation)한다. 또한 워터마크를 삽입하기 위하여 원 영상을 블록화 시켜 각 블록마다 워터마크의 삽입 위치를 랜덤하게 지정한다. 선택된 블록에서 워터마크가 삽입될 위치의 비트 플레인을 0으로 초기화 시킨 다음 해쉬 함수를 사용하여 워터마크 정보와 XOR한다. 삽입된 워터마크 영상은 보다 강인한 무결성 인증을 위하여 공개 키 암호화 알고리즘을 사용한다. 제안한 방법의 실험 결과 기존의 방법보다 비가시성이 뛰어나며 강인한 무결성 검증을 확인하였다.

2. 제안한 워터마킹 알고리즘

2.1 워터마크의 삽입

본 논문에서는 영상의 변질 검증을 위한 워터마크를 사용하는 기법으로 원래의 의료영상 정보를 워터마크 정보로 만들어 사용함으로써 시각적으로 워터마크를 인지할 수 있도록 설계하고 불법적인 위/변조 검증이 가능하여 무결성 검증을 할 수 있도록 한다.

데이터에 대한 인증과 무결성을 체크하는 기존의 방법 중 공개키 암호 알고리즘인 해쉬 함수를 사용한 Wong의 방법이 적당하다. 이는 암호학적인 해쉬 함수를 사용하므로 워터마킹 알고리즘의 안전성이 암호학적 해쉬 함수의 안전성에 의존하게 된다. 그런데 암호학적 해쉬 함수의 특징 중의 하나가 바로 암호학적 해쉬 함수를 깨는 것이 아주 어렵다는 것이므로 Wong이 제안한 방법은 안전하게 되는 것이다. 그러나 제 3자가 영상내의 LSB를 삭제하고 자신의 비밀

키를 사용해서 서명을 만든 뒤 LSB 부분에 삽입할 수 있는 단점이 있는 이 방법을 보완하여 워터마크가 삽입되는 위치를 블록별로 랜덤하게 선택해서 삽입되는 위치를 알지 못하도록 한다. 비밀 키를 해쉬 함수의 입력한 MD5의 사용으로 디지털 서명을 만든 후 워터마크가 삽입되는 픽셀의 위치와 선택된 픽셀 내의 특정 비트를 선택하여 워터마크를 삽입 및 추출하는 방법을 제안한다.

본 논문에서 제안하는 워터마킹은 삽입의 전체 구성도는 그림 1과 같다. 먼저 워터마크의 정보를 생성하기 위해 원 영상을 2-Level로 DWT을 수행한다. 여기서 구해진 기저 영역인 LL2를 이진 비트로 만들기 위해 8-bit 비트 플랜(bit-Plane)을 구성한다. 비트 플랜 재구성을 위해서 m비트 명암도를 기저가 2인 다항식의 형태인 (1)로 나타낼 수 있다[20].

$$a_{m-1}2^{m-1}+a_{m-2}2^{m-2}+\cdots+a_1 2^1+a_0 2^0 \qquad (1)$$

구해진 비트 플랜 정보들을 원 영상과 같은 크기에 매핑을 시킨다. 이때, LSB에 해당하는 비트 플랜 값 대신에 학교 로고를 삽입하여 워터마크 추출시 소유권자의 소속을 밝히도록 한다. 나머지 상위 7비트에 해당하는 각 비트 플랜 정보를 두 번에 걸쳐 반복하여 넣음으로써 워터마크의 무결성 여부를 판단할 수 있는 비교의 경우 수를 확장시키고 그 다음 각각의 비트에 따른 비트 플랜 정보의 보안을 위하여 (2)에서와 같이 랜덤치환을 수행하는데 여기서 M과 $\frac{M}{2}$은 512와 256으로 두 영역으로 각각 따로 랜덤치환을 수행하여 얻어진 랜덤 노이즈 형태를 워터마크 정보로 사용하도록 한다.

$$W_p = permutation(W) = \left\{ w_p(i,j) = w(i',j') \mid 0 \le i,\ i' < M \text{and} 0 \le j, j' < \frac{M}{2} \right\} \qquad (2)$$

워터마크의 삽입 위치는 원 영상의 하위 3비트 이내에 랜덤하게 선택된 영상 블록으로 설정을 하되 ROI 영역은 LSB가 될 수 있도록 설계를 한다. 이는 의료 영상의 특성상 워터마크 정보의 삽입으로 오진의 문제를 방지하기 위함이다. ROI 영역은 일반적인 경우 영상의 가장 중앙 영역을 대상으로 하고 특수한 경우 지정하여 사용할 수 있도록 한다.

이렇게 랜덤하게 선택된 워터마크 삽입 블록 X_R의 해당영역을 0으로 초기화 시킨 X_R'과 영상의 가로 세로 크기 값인 M과 N을 MD5 암호 해쉬 함수 $H(\cdot)$에 통과 시켜 나온 P_R을 (3)과 같이 비트 스트림으로 나타낼 수 있으며 이를 워터마크 정보 B_R과 exclusive-OR를 수행한 것이 (4)이다. 수행 결과로 나온 W_R은 공용 키 암호 시스템에 의하여 (5)와 같이 암호화된다. 여기서 $E_{K'}(\cdot)$는 공용 키 암호화 시스템

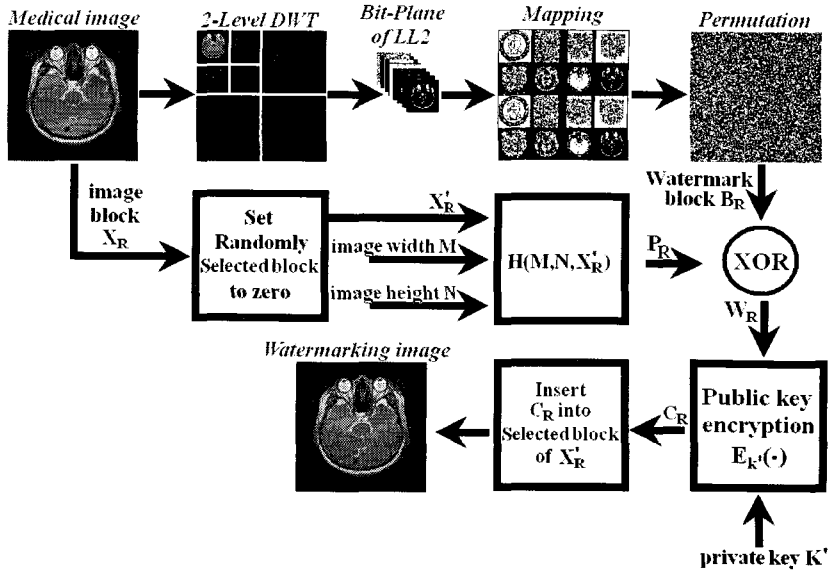


그림 1. 제안한 워터마크 삽입 블록도

이며 K'는 개인 키이다. 이렇게 만들어진 데이터 C_R은 X_R'에 삽입되고 그 결과 워터마크된 영상을 구하게 된다.

$$H(M, N, X_R') = (p_1^R, p_2^R, \cdots, p_s^R), s = 128 \quad (3)$$

$$W_R = P_R \oplus B_R \quad (4)$$

$$C_R = E_{K'}(W_R) \quad (5)$$

그림 1에 대한 워터마크의 삽입 순서는 다음과 같다.

【삽입순서】

① 워터마크의 정보를 생성하기 위해 원 영상을 2-level로 DWT을 수행

② LL2를 이진 비트로 만들기 위해 8-bit 비트 플랜을 구성

③ 비트 플랜 정보들을 원 영상과 같은 크기에 매핑. (단, LSB에 해당하는 비트 플랜 값 대 신에 학교 로고를 삽입하여 워터마크 추출시 소유권자의 소속을 밝힘)

④ 각각의 비트에 따른 비트 플랜 정보의 보안을 위하여 M과 N은 512와 256으로 두 영역 으로 각각 따로 랜덤치환을 수행

⑤ 워터마크의 삽입 위치는 원 영상의 하위 3비트 이내에 랜덤하게 선택된 영상 블록으 로 설정을 하되 ROI 영역은 LSB가 될 수 있도록 설계

⑥ 선택된 영상 블록의 초기화

⑦ 영상의 가로 세로 크기 값인 M과 N과 X_R'을 MD5 암호 해쉬 함수에 입력

⑧ 워터마크 정보와 ⑦에서 생성된 P_R의 exclusive-OR 수행

⑨ exclusive-OR 수행 결과로 나온 W_R은 공용키 암호 시스템에 의하여 암호화. (단, K'는 개인 키)

⑩ C_R은 X_R'에 삽입하여 워터마킹된 영상 획득

2.2 워터마크의 추출

그림 2는 워터마크가 삽입된 영상에서 워터마크를 추출하는 과정을 도식적으로 나타낸 것이다. 먼저 워터마킹 영상에서 워터마크가 삽입된 블록 Z_R을 0으로 초기화 시킨 Z_R'와 워터마크 값이 들어 있는 블록인 두 개의 영역으로 구분을 한다. Z_R'와 영상 크기인 M, N과의 해쉬 값을 통해 64비트의 Q_R을 만들고 워터마크 정보가 들어 있는 블록 G_R은 (6)에서와 같이 공용 키로 복호화 한 후 이를 (7)과 같이 exclusive-OR를 수행하면 삽입한 랜덤 노이즈 형태의 워터마크 정보가 추출 된다.

$$U_R = D_K(Z_R) \quad (6)$$

$$O_R = Q_R \oplus U_R \quad (7)$$

이때 만약 워터마킹된 영상에 조작을 하였다면 변질된 부분이 표시가 된다. 그러나 랜덤 노이즈의 패턴이므로 심하게 공격을 하지 않으면 변질 부분이 제대로 안 보일 수 있다. 완벽한 무결성 검증을 위해서 역(inverse) 랜덤치환을 수행하여 7비트의 비트플랜 형태로 만든 후 이를 다시 취합하여 영상을 구성

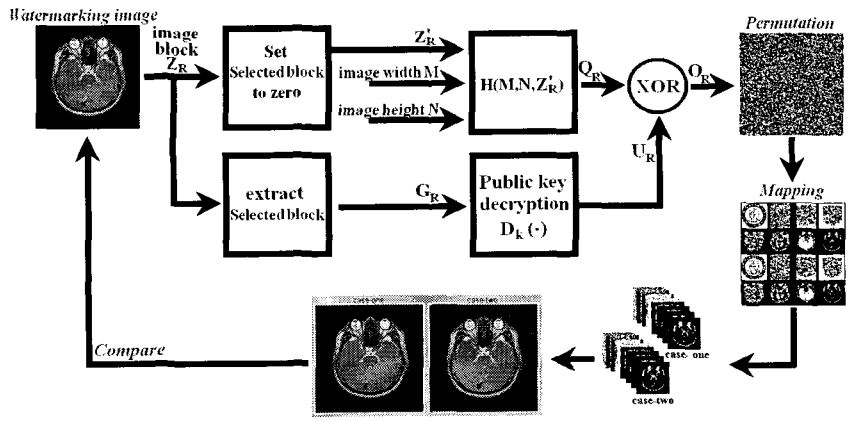


그림 2. 워터마크의 추출 과정

한다. 가장 하위 비트에 해당하는 LSB 위치의 정보는 학교 로고로 소유권자의 소속을 알아내고, 구해진 두 개의 비교 영상과 워터마킹된 영상과의 검증으로 무결성을 판단 할 수 있다. 만약 워터마킹된 영상에 어떠한 영역에 조작을 했다면 취합된 두 개의 비교 영상을 통해 문제를 일으킨 영역을 알 수 있어 왜곡된 영상과의 비교로 무결성 여부를 알 수 있다.

그림 2에 대한 워터마크의 추출 순서는 다음과 같다.

【추출 순서】

① 워터마크가 삽입된 블록과 Z_R을 0으로 초기화 시킨 것으로 구분

② Z_R'와 영상 크기인 M, N과의 해쉬 값을 통해 64비트의 Q_R 생성

③ 워터마크가 삽입된 블록 G_R을 공용키로 복호화

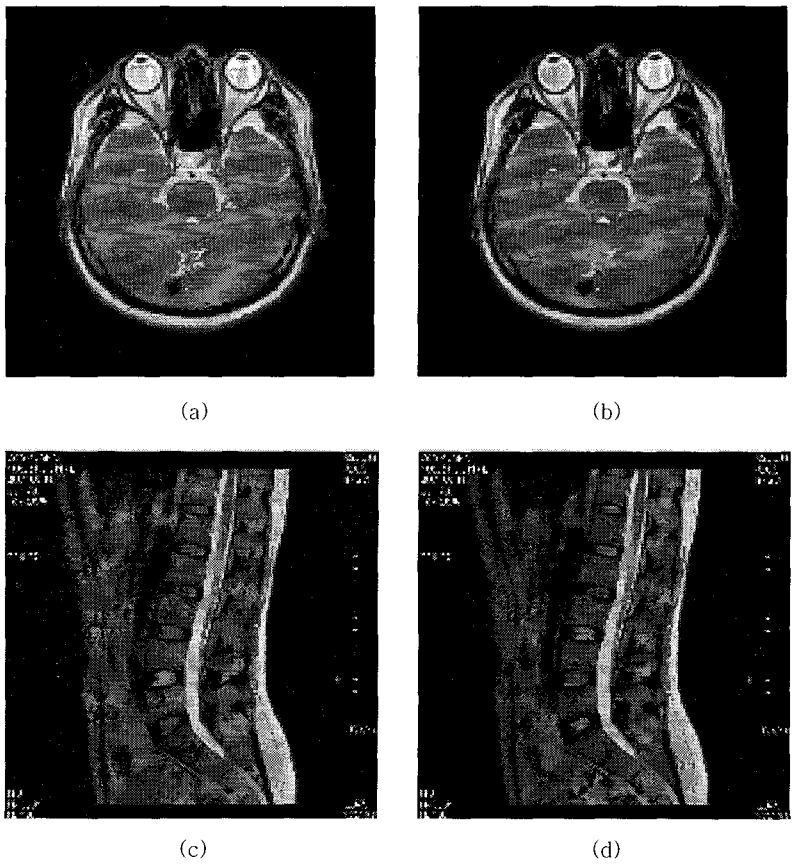
④ 해쉬 함수로 구해진 Q_R과 복호화된 U_R의 XOR

⑤ 역 랜덤치환을 수행하여 원 영상의 7비트의 비트플레인과 학교 로고의 패턴으로 생성하여 취합한 두개의 영상을 구성하고 이를 워터마킹된 영상과 비교

3. 실험 결과 및 고찰

의료 영상에서의 워터마킹 실험을 위해 Brain영상과 Spine을 사용하였다. 이 영상들은 http://www.infinitt.com/사에서 제공하는 PiView4.5 프로그램과 함께 설치되는 VisualGate 프로그램을 통하여 DICOM에서 지원하는 형식으로 저장된 파일을 일반 영상 데이터로 만들어 사용하였다.

그림 3 워터마크의 비가시성을 나타내는 것으로 (a)는 원 Brain 영상이며 (b)는 워터마킹된 영상으로 PSNR은 43.49[dB]이다. (c)는 원 Spine 영상으로 (d)



(a) (b)

(c) (d)

그림 3. 워터마크의 비가시성: (a) 원 영상, (b) 워터마크 영상, (c) 원 영상, (d) 워터마크 영상.

는 워터마킹된 영상으로 PSNR은 43.68[dB]이다. 표 1에서 보여지는바와 같이 제안한 워터마킹 기법은 Wong의 방법보다는 떨어지지만 우수한 비가시성을 나타냄을 알 수 있다. 비가시성의 척도로 (9)와 같이 *PSNR*(peak signal noise ratio)을 사용하였으며, (8)의 S는 root mean square이다. 여기서, $x(i,j)$은 원 영상, $\hat{x}(i,j)$은 추출된 영상을 나타낸다.

$$S=\frac{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\{x(i,j)-\hat{x}(i,j)\}^2}}{MN} \tag{8}$$

표 1. 제안한 방법과 Wong방법의 비가시성 평가

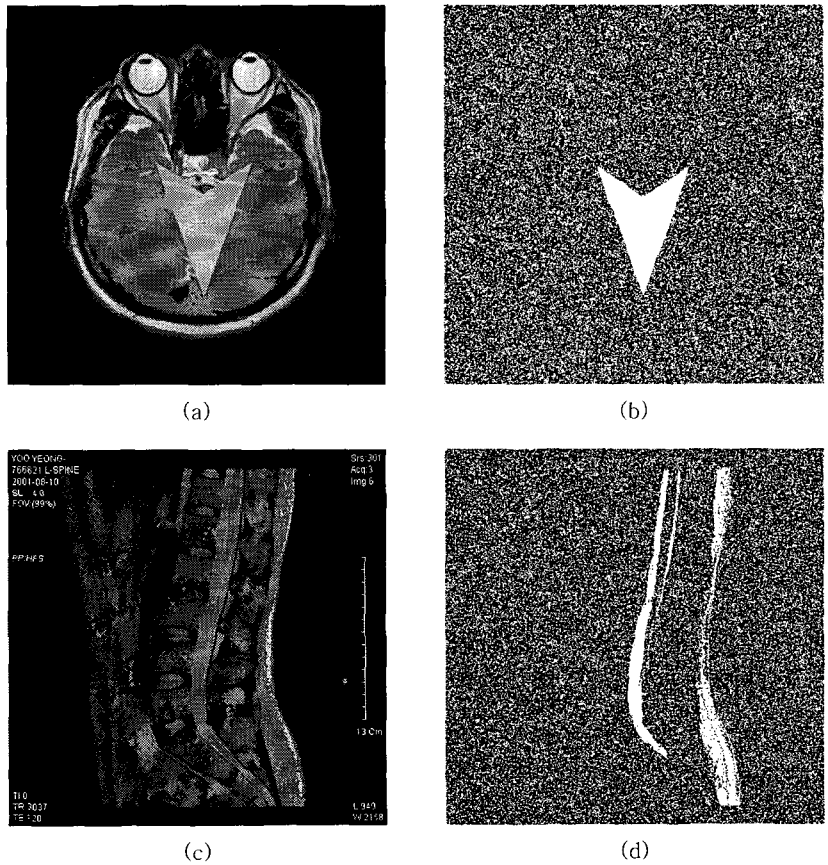
비가시성	Brain 영상	Spine 영상
제안한 방법	43.49[dB]	43.68[dB]
Wong의 방법	58.16[dB]	59.20[dB]

$$PSNR=20\log_{10}\left(\frac{255}{S}\right)=10\log_{10}\frac{255^2}{S^2} \tag{9}$$

아래의 (9)는 NC(normalized correlation)으로 워터마크의 견고성을 측정하는 것이다. 여기서 $W(i,j)$는 삽입한 워터마크를 나타내고, $\hat{W}(i,j)$는 추출한 워터마크를 나타낸다.

$$NC=\frac{\sum_{i=0}^{(N/2)-1}\sum_{j=0}^{(N/2)-1}W(i,j)\hat{W}(i,j)}{\sum_{i=0}^{(N/2)-1}\sum_{j=0}^{(N/2)-1}[W(i,j)]^2} \tag{10}$$

그림 4는 워터마크의 무결성에 대한 실험으로 워터마킹된 영상에 (a)와 (c)와 같이 공격을 하였을 때 추출된 워터마크는 (b)와 (d)와 같으며 이때의 NC값은 각각 0.87과 0.81이며 추출된 워터마크에서도 알 수 있듯이 조작된 영역이 가시적으로 보이게 되어



(a) (b) (c) (d)

그림 4. 워터마크의 무결성 실험: (a) Brain 공격 영상, (b) 추출된 워터마크, (c) Spine 공격 영상, (d) 추출된 워터마크.

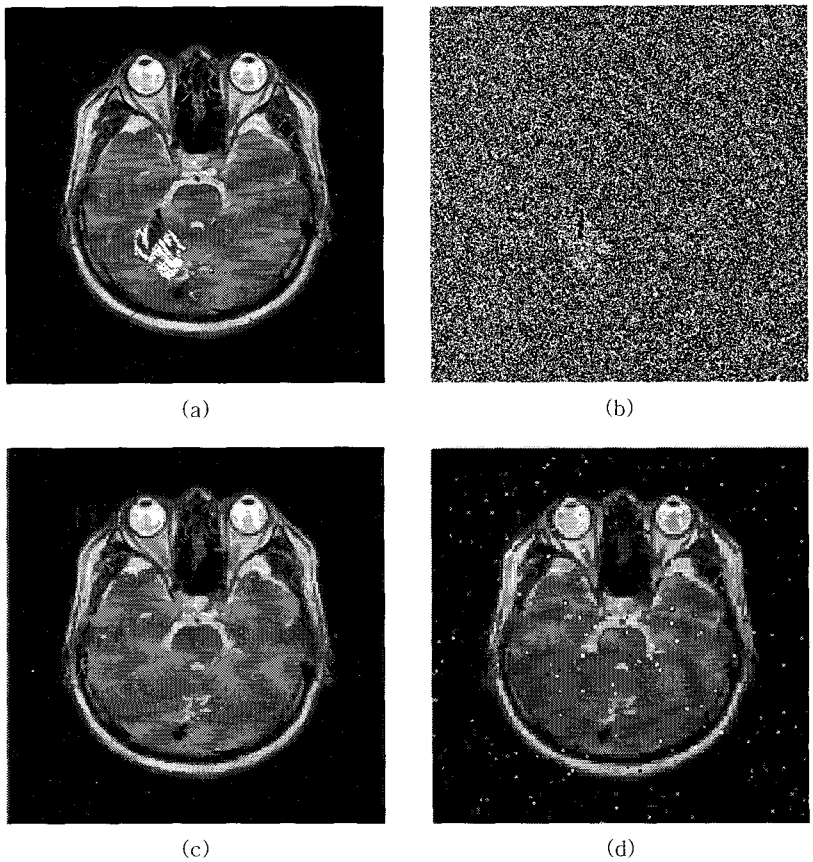
훼손이 된 영상임을 판단하여 무결성 검증을 할 수 있다.

그림 5는 그림 4와 같이 무결성 실험이다. 공격받은 워터마킹 영상인 (a)에서 추출한 워터마크 (b)가 그림 4에서와는 다르게 조작된 위치를 제대로 알 수 없을 때 원래의 형태로 역랜덤변환(inverse permutation)을 하여 구해진 이들 두 개의 비교 영상인 (c)와 (d)를 공격 영상인 (a)와의 비교 검증을 통해 조작된 (a)영상의 정확한 픽셀 위치를 알 수 있는 무결성 검증이 가능하다. 이와 같은 실험은 공격자가 눈에 잘 안 띄게 약간의 조작을 했다하더라도 해당 위치를 정확히 찾아 낼 수 장점이 있다.

4. 결 론

본 논문에서는 ROI를 고려한 공개키 암호화 알고리즘 기반 의료영상 디지털 워터마킹 기법을 제안하였다. 제안한 방법에서 ROI 영역은 LSB 영역에 워터마크를 삽입하고, 나머지 영역은 상위 비트에 랜덤하게 삽입한 워터마킹 기법이다. 이는 의료 영상의 특성상 워터마크 정보로 인한 오진의 문제가 발생할 수 있는 문제점을 고려한 것이다. DICOM에 의하여 저장된 영상을 온라인을 통하여 전송하거나, 혹은 CD-ROM과 같은 매체에 저장 했을 경우 어떠한 변형이나 훼손 등의 물리적인 변화가 생겼다고 의심이 될 때 워터마킹된 의료 영상의 인증과 무결성을 증명할 수 있도록 하였다.

제안한 방법은 암호학적 어려움을 기반으로 한 해쉬 함수와 공개키 암호 알고리즘을 사용한 Wong의 방법을 개선한 것으로서, 임의의 입력 비트열에 대하여 128비트의 안전한 출력 비트를 생성하는 MD5 해쉬 함수를 사용하여 영상내의 임의의 픽셀 블록을 선정하고 선택한 픽셀 내의 임의의 비트에 워터마크를 삽입 및 추출하였다.



(a) (b) (c) (d)

그림 5. 조작된 워터마킹 영상의 검증: (a) Brain 공격 영상, (b) 추출된 워터마크, (c) case-one,(d) case-two.

실험 결과 워터마크의 삽입 위치가 LSB에서 MSBs로 확장되더라도 비가시성은 우수함을 확인하였고, 조작된 영상에서 삽입한 워터마크를 추출함으로써 무결성 검증을 할 수 있어 의료 영상의 불법적인 조작으로 인한 병역비리나 보험 사기와 같은 문제를 해결할 수 있다. 앞으로 JPEG 압축과 같은 다양한 영상처리 공격에서도 워터마크 추출이 가능한 후속 연구를 할 것이다.

참 고 문 헌

[1] C. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of Watermarking in Medical Imaging," *IEEE EMBS200 Conf. On Information Technology Applications in Biomedicine*, pp. 250-255, Nov. 2000.

[2] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "A medical image watermarking scheme based on wavelet transform," *In Proc. of the 25th Annual Int. Conf. of the IEEE-EMBS*, pp. 856-859, Cancun, Mexico, Sept. 2003.

[3] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Specturm watermarking for Multimedia," *IEEE Trans. on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.

[4] C. Podilchuk and W. Zeng, "Image Adaptive Watermarking Using Visual Models," *IEEE Journal on Selected Areas in Communication*, Vol. 16, No. 4. pp. 525-539, 1998.

[5] Stefan Katzenbeisser (Editor), Fabien, A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, pp. 103-105, Jan. 2000.

[6] M.L.Miller and J.A Bloom, "Computing the Probability of False Watermark Detection," *Proceeding of the Third International Workshop on Information Hiding*, pp. 146-158, 1999.

[7] Joseph J. K. Ruanaidh and Trierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking," *IEEE ICIP1997*, pp. 536-539, Santa Barbara, 1997.

[8] F. Y. Shih and Y. Wu, *Robust watermarking and compression for medical images based on genetic algorithms*, Information Sciences, In Press, Vol. 2005.

[9] Schneier and Bruce, *Applied Crytography*, Wiley, 1996.

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

[11] P.W. Wong, "A Watermark for Image Integrity and Ownership Verification," *IS&T PIC Conference*, May 1998.

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

[13] 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.

[14] 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.

[15] 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.

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

[17] Deepthi An and U.C.Niranjan, "Watermarking medical images with patient information," *in proc. IEEE/EMBS Conference*, Hong Kong, China, pp. 703-706, Oct. 1998.

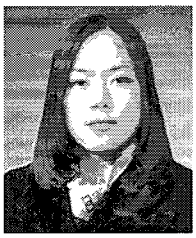
[18] Akiyoshi Wakatani, "Digital Watermarking for ROI Medical Images by Using Compresses Signature Image," *HICSS*, Vol. 157, 2002.

[19] Masaki Yamauchi and Akiyoshi Wakatani, "A New Lossless Compression Scheme for Medical Images by Hierarchical Segmentation," *Proc. Data Compression Conference,* 2001.

[20] Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing,* Prentice Hall, 2002.

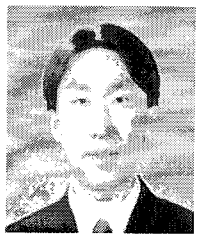
이 형 교

1976년 경북대학교 전자공학과 공학사
1996년 국민대학교 전자공학과 공학석사
2006년 동의대학교 컴퓨터공학과 박사졸업예정
1980년~1984년 한국전자통신연구원 연구원
1985년~1988년 (주)데이콤 주임연구원
1988년~1989년 호주 Datacraft사 연구원
1990년~1992년 (주)삼보컴퓨터 부장
1995년~2000년 부산백병원 전산실장
현재 안동과학대학 의료정보과 교수
관심분야 : 멀티미디어, 영상처리



김 희 정

1996년 2월 부산외국어대학교 컴퓨터공학과(공학사)
1999년 2월 부산외국어대학교 교육대학원 전산교육전공(교육학석사)
2004년 8월 부산외국어대학교 일반대학원 전자컴퓨터공학과(공학박사)
2003년 9월~2005년 2월 부산외국어대학교 교양연계학부 초빙교수
관심분야 : 워터마킹, 영상처리, 컴퓨터그래픽스, 3D 애니메이션



성 택 영

2004년 2월 부산외국어대학교 컴퓨터전자공학부(공학사)
2006년 2월 부산외국어대학교 대학원 전자컴퓨터공학과 졸업예정(공학석사)
관심분야 : 영상처리, 디지털워터마킹

권 기 룡

1986년 2월 경북대학교 전자공학과 졸업(공학사)
1990년 2월 경북대학교 대학원 전자공학과 졸업(공학석사)
1994년 8월 경북대학교 대학원 전자공학과 졸업(공학박사)
2000년 7월~2001년 8월 Univ. of Minnesota, Post-Doc. 과정
1996년 3월~현재 부산외국어대학교 디지털정보공학부 부교수
2005년 3월~현재 한국멀티미디어학회 논문지 편집위원장
관심분야 : 멀티미디어정보보호, 멀티미디어 통신, 웨이브릿 변환

이 종 극

1978년 2월 경북대학교 전자공학과(공학사)
1988년 2월 미국 North Carolina St. Universtiy(공학석사)
1993년 6월 미국 Texas A&M University(공학박사)
1988년 6월 Assistant Teaching
1994년~현재 동의대학교 컴퓨터응용공학부 교수
관심분야 : 컴퓨터 네트워크, 병렬처리