논문 2010-47CI-1-8

의료영상을 위한 복원 가능한 정보 은닉 및 메시지 인증

(Reversible Data Hiding and Message Authentication for Medical Images)

김 천 식*, 윤 은 준**, 조 민 호***, 홍 유 식****

(Cheonshik Kim, Eun-Jun Yoon, Minho Jo, and You-Sik Hong)

요 약

오늘날 의료 기관에서는 수많은 의료 영상자료를 만들고 관리하고 있으며, 이러한 자료들 중에서는 환자의 프라이버시와 관련된 정보도 많다. 따라서 이러한 개인정보는 외부로 노출되어서는 안 되며, 철저한 관리가 필요하다. 본 논문에서는 이러한 프라이버시 관련 영상 자료에 환자의 상태 및 의료 처방 정보를 포함함으로서, 향후 영상자료의 관리 소홀로 인한 잘못된 의료처방 등을 방지할 수 있는 방안을 제안한다. 제안한 방법은 각 환자 정보에 대한 HMAC 기반의 해쉬 코드를 생성하고, 생성된 코드와 환자의 정보를 함께 이미지에 포함함으로서 향후 의사가 이 이미지로부터 추출한 데이터가 외부인에게 훼손되었는지 여부를 쉽게 감지함으로써, 환자의 정보를 보다 철저히 관리할 수 있도록 하는 것을 목적으로 한다. 또한, 환자의 의료정보를 이미지에 은닉하기 위해서 복원 가능한 데이터 은닉 기법인 DE(Difference Expansion) 알고리즘을 사용함으로서, 이미지로부터 데이터를 추출한 후 원 영상을 가지고, 환자의 상태를 쉽게 체크할 수 있게 되어 의사의 입장에서 매우 효율적인 방법으로 환자 상태를 평가할 수 있다. 제안한 방법은 뇌 영상을 촬영한 MRI 영상에서 실험한 결과 데이터은닉과 추출 그리고 영상의 복원 그리고 데이터 무결석 확인에 있어서 완벽한 성능을 보였다.

Abstract

Nowadays, most hospitals have been used to create MRI or CT and managed them. Doctors depend on fast access to images such as magnetic resonance imaging (MRIs), computerized tomography (CT) scans, and X-rays for accurate diagnoses. Those image data are related privacy of a patient. Therefore, it should be protected from hackers and managed perfectly. In this paper, we propose a data hiding method into MRI or CT related a condition and intervention of a patient, and it is suggested that how to authenticate patient information from an image. In this way, we create hash code using HMAC with patient information, and hash code and patient information is hided into an image. After then, doctor will check authentication using HMAC. In addition, we use a reversible data hiding DE(Difference Expansion) algorithm to hide patient information. This technique is possible to reconstruct the original image with stego image. Therefore, doctor can easily be possible to check condition of a patient. As a consequence of an experiment with MRI image, data hiding, extraction and reconstruct is shown compact performance.

Keywords: HMAC, authentication, data hiding, MRIS, Steganography

I. 서 론

스테가노그라피(Steganography)는 최근에 많은 연구자들이 관심을 갖고 연구하는 분야로서 이미지에 데이터를 은닉하는 기술이다. 이 기술은 다양한 멀티미디어 매체에 적용되고 활용되고 있다[1]. 예를 들어서, 워터마크 기술은 멀티미디어에 대한 소유권 정보를 연구하는 분야로서 지금도 연구되고 있는 분야이다[2]. 이러한 기술은 여러 분야에 활용될 수 있지만, 초기에는 안전한 통신에 대한 요구로서 출발하였다. 왜냐하면, 전자메일

* 정회원, 안양대학교 교양학부
(Division of Liberal Arts, Anyang University)
** 정회원, 경북대학교 전자전기컴퓨터학부
(School of Electrical Engineering and Computer Science, Kyungpook National University)
***정회원, 고려대학교 정보경영공학전문대학원
(Graduate school of Information Management & Security, Korea University)
****평생회원, 상지대학교 컴퓨터공학과
(Dept. of Computer Science, Sangji University)
접수일자: 2009년12월16일, 수정완료일: 2010년1월11일

이나 기타 인터넷을 이용한 통신에서는 암호화 되지 않은 상태에서 통신이 이루어지고, 간단한 로그인 아이디와 패스워드만으로 개인정보를 쉽게 알아낼 수 있기 때문이다. 아이디와 패스워드는 기존의 해킹 방법으로 간단히 알아낼 수 있으므로, 안전한 통신방법에 대한 연구로서 데이터 은닉(Data Hiding) 방법이 최근에 활발하게 연구되고 있다[1]. 다른 이유로서는 기존의 이미지 검색방법이 주로 메타 태그를 이용하였지만, 이미지에 주석을 처리함으로서 이미지 검색이 용이할 수 있다. 또한, 군사나 의료 분야에서 이미지에 직접 중요한 정보를 은닉함으로써, 정보를 더 안전하게 보호할 수 있는 장점이 있다.

특히 병원 등 의료 기관에서 촬영되는 많은 CT 및 MRI 영상 등은 때때로 다른 사람의 CT 영상과 구분이 되지 않는 문제와 공격자에 의한 고의적인 영상 조작 변경 등의 심각한 일이 발생할 수 있다. 이에 이러한 영상정보를 안전하게 관리하고 해당 영상에 필요한 필수 정보를 저장하는 등의 방법을 통하여 위와 같은 문제점을 해결하는 기술들이 연구 개발되어야 할 필요성이 있다.

따라서 본 논문에서는 의료 MRI영상에 환자에 대한 중요한 정보를 저장하고, 필요할 때 의사가 환자의 의료 정보를 안전하고 쉽게 볼 수 있도록 프라이버시 제공 및 접근 제한을 할 뿐만 아니라, 데이터의 무결성을 유지함으로써 안전한 환자정보 관리를 할 수 있는 효율적인 인증 기법을 제안한다. 제안한 기법에서는 Tian[5]이 제안한 복원가능 데이터 은닉(Reversible Data Hiding)[2~9] 알고리즘을 적용하여 영상에 보관된 환자 인증 정보를 추출한 후에는 원 영상으로 복원이 가능하도록 하여 환자와 관련된 중요한 정보의 손실이 없도록 설계하였다. 기존의 의료영상 보안 기법들과 비교하여 제안한 방법의 가장 큰 장점은 첫째, 은닉 정보를 복원한 후에는 원본 영상이 숨기기 전의 원영상으로 완벽한 복원이 이루어져 원영상 훼손이 전혀 없으며, 둘째, 영상 정보의 위변조 여부를 *HMAC* 검증 과정을 통해 효율적이며 안전하게 수행 할 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 관련 연구로 복원가능 데이터 은닉 알고리즘의 원리에 관해 설명한다. Ⅲ장에서는 제안한 데이터 은닉과 접근제어 방법의 원리를 설명하며 Ⅳ장에서 실험 및 분석 결과를 보여주고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 제안한 방법에서 사용되고 있는 복원가능 데이터 은닉 알고리즘에 관해 설명한다.

1. 복원가능 데이터 은닉(Reversible Data Hiding)

데이터를 멀티미디어 매체에 은닉하면 필연적으로 매체의 질(Quality)이 나빠진다. 예를 들어서 이미지에 데이터를 은닉하면 이미지의 질이 숨기는 데이터의 양에 따라서 상대적으로 나빠지는 관계가 있다. 즉, 은닉하는 데이터가 많아지면 많아질수록 이미지의 질은 현저하게 떨어지게 된다. 따라서 많은 양의 데이터를 이미지에 은닉 할 경우 원 영상의 훼손 문제가 발생할 수 있는 문제를 원천적으로 해결하기 위한 방법으로 숨긴 데이터를 원 영상으로 추출한 후 완벽하게 원 영상으로 복원할 수 있는 복원가능 데이터 은닉 기법에 관한 연구가 최근에 활발히 연구되어지고 있다[2~7].

가장 대표적인 연구로서 두 픽셀에 대해서 정수 연산을 통해서 값을 저장하고 복원하는 기술[5~6]과 히스토그램을 이용하는 방법[7~9] 그리고 VQ-index를 이용하여 원래 이미지를 복원하는 벡터 양자화(Vector Quantization)[10]를 이용한 방법 등이 있다. 특히 히스토그램을 이용하는 방법은 이미지에 대한 히스토그램 분포가 특정 픽셀은 높고 어떤 부분은 낮은 부분이 있게 되는데 이러한 차이를 이용해서 데이터를 은닉하는 방법이다. 하지만 이 방법의 단점은 은닉하기 위해서 이동한 히스토그램 이동 위치를 표시해야 하며 나중에 복원할 때 이 정보를 다시 활용해야 하기 때문에 부가정보 저장 및 관리가 필요하다.

2. Tian 의 복원 데이터 은닉 알고리즘[5]

*Tian*이 제안한 복원 데이터 은닉 방법은 두 픽셀 값의 차이를 이용하여 수식 (1)~(3)과 같은 간단한 수식을 통해서 한 비트의 비밀 정보를 은닉하는 방법이다.

$$Avg = \left\lfloor \frac{x+y}{2} \right\rfloor, \quad diff = x - y. \tag{1}$$

$$diff' = 2 \times diff + b \tag{2}$$

$$x' = avg + \left\lfloor \frac{diff+1}{2} \right\rfloor, \quad y' = avg + \left\lfloor \frac{diff}{2} \right\rfloor \tag{3}$$

예를 들어 두 픽셀이 $x=102, y=100$라고 가정하면, 수식 (1)을 적용하여 다음과 같이 평균(Avg)과 차이($diff$)를 각각 계산한다.

$$Avg = \left\lfloor \frac{102+100}{2} \right\rfloor = 101,\ diff = 102-100$$

수식 (2)에서 b는 은닉을 위한 바이너리 데이터이고 1비트를 의미한다. $diff'$는 수식 (2)와 같이 $diff$값에 두 배한 값에 b를 더한 값이다. b를 1이라고 가정하면, 다음과 같이 5가된다.

$$diff' = 2\times diff + b = 2\times 2 + 1 = 5$$

지금까지 구한 값을 수식 (3)에 적용 하면 아래와 같이 b값이 은닉된 픽셀 값이 만들어 지게 된다.

$$x' = 101 + \left\lfloor \frac{2+1}{2} \right\rfloor = 102,$$
$$y' = 101 - \left\lfloor \frac{2}{2} \right\rfloor = 100$$

즉, x'는 102가 되고 y'는 100이 된다. 이러한 과정을 나머지 픽셀 쌍들에 대해서도 적용을 하여 최종적으로 스테고(Stego)된 이미지가 만들어지게 된다.

완성된 스테고 이미지로부터 원래의 이미지로 복원하기 위해서는 데이터 은닉과 같이 한 쌍의 두 픽셀을 가져와서 평균(Avg)과 차이($diff$) 값을 구하고 차이 값에서 은닉한 비트 값을 추출한 후, $diff'$값을 알아내고, 수식 (3)을 적용하면 원래의 이미지로 복원이 되는 것이다.

Ⅲ. 제안한 정보 은닉과 메시지 인증 기법

본 장에서는 제안한 의료영상을 위한 복원 가능한 정보 은닉 및 메시지 인증 기법에 관해 설명한다. 제안한 스킴은 데이터 은닉 처리 과정(Data hiding procedure)와 *MAC*인증 절차 기반의 무결성 확인을 위한 데이터 추출 및 인증 과정(Data extracting and authentication)으로 구성된다.

1. *MAC* 인증절차

의료영상 이미지에서 실질적으로 고려해야 할 부분은 영상에 대한 인증(Authentication)이다. 예를 들면 고의 또는 오류로 타인의 의료영상을 해당 환자로 잘못 판단하는 문제 등을 해결하기 위해 영상 이미지 내에 환자식별 정보, 서명 정보, 환자 상태 정보 등을 기록하는 작업을 해주어야 한다. 더 나아가 해당 개인의 프라이버시와 연관된 영상 데이터를 아무나 보거나 접속할 수 없도록 안전하게 관리하기 위한 인증키는 필수적으로 요구된다.

일반적으로 메시지 무결성과 인증을 보장하기 위해서는 수신자가 메시지가 바뀌었는지 여부를 쉽게 판별 및 확인 할 수 있는 방법이 있어야 한다. 이러한 기능을 제공하기 위해서는 수신자가 수신한 영상 이미지를 이용하여 무결성 검증 및 인증을 수행할 수 있는 기술이 필요하다. 즉 수신자는 영상 이미지 검증을 위해 영상 정보 이외의 부가적인 정보를 송신자로부터 얻을 수 있어야 한다.

검증을 위한 이러한 부가적인 정보를 일반적으로 암호 체크섬(Cryptographic Checksum) 또는 메시지 인증 코드(Message Authentication Code, *MAC*)라고 부른다. *MAC*은 기본적으로 비밀 키를 입력 파라미터로 사용한 충돌 저항성을 가지는 안전한 일 방향 해쉬 함수(Secure One-way Hash Function)를 통해 얻어 지는 값을 의미한다[11~13].

MAC 인증은 암호 알고리즘과 송신자와 수신자가 공유하는 비밀 키를 기초로 한다. *MAC* 인증을 위해 송신자는 원본 메시지뿐만 아니라 그에 대응하는 *MAC*을 함께 수신자에게 보낸다. 그림 1과 같은 *MAC*은 비밀키 k를 이용하여 일방향 해쉬 함수 A로부터 임의의 메시지 m에 대한 다음 값을 메시지 무결성 검증 값으로 계산할 수 있다.

$$MAC = A_k(m)$$

일반적으로 *MAC*의 목적은 메시지 M에 대한 비밀 보장 문제가 아니기 때문에 메시지 M을 암호화하지 않을 수도 있다. 만약 송신자가 메시지 M을 비밀리에 전달하고 싶을 때는 M과 *MAC*을 3DES, AES 등의 대칭키 암호 시스템 또는 RSA, ECC 등의 비대칭키 암호 시스템을 이용하여 암호화하여 송신할 수도 있다.

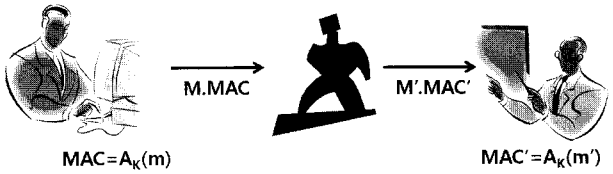


그림 1. MAC 인증절차
Fig. 1. MAC authentication procedure.

그림 1에서 공격자 X는 송신자가 보내는 메시지 M과 MAC을 도청하여 이를 변조한 M'과 MAC'로 바꾸어 수신자에게 전송 할 수 있다.

하지만 이러한 변조는 수신자의입장에서 생각해 보면 MAC을 통한 메시지 무결성 검증을 통해 간단히 위변조 여부를 판별할 수 있다.

즉, 수신한 메시지가 진짜로 송신자가 보낸 것인지 여부를 확인하려면, 수신자는 송신자가 수행했던 공유 비밀 키 k를 이용한 MAC 생성 과정을 똑같이 수행하여 수신한 M'에 대한 MAC을 생성해보면 쉽게 위변조 여부를 식별할 수 있다. 다시 말해 키 k를 이용하여 수신한 메시지 M'을 동일한 해쉬 알고리즘 A에 적용하여 출력된 그 결과가 수신한 메시지 인증 코드 MAC'와 일치하는지 여부를 확인하면 된다[12].

만약 $A_k(M') = MAC'$이면 수신한 메시지가 중간에 공격자 등에 의해 변형되지 않았음을 수신자는 쉽게 확인할 수 있다. 물론 이러한 과정은 해쉬 알고리즘 A와 비밀 키의 안전성(Security)에 기반을 두게 된다. 수신자는 메시지의 변경여부만 판단하기 때문에 만약 메시지가 변경되었다면 원래의 메시지로 복구 할 수 없다. 이 경우에는 송신자에게 메시지를 다시 송신해 달라고 요청하게 된다. 특히 MAC은 응용 목적에 따라 메시지 무결성과 메시지 인증을 동시에 확인할 수도 있다. 즉 송신자와 수신자 간에만 공유된 비밀 키 k로 메지시 M에 대한 무결성 검증을 하게 되면, 비밀 키 k를 모르는 임의의 어떤 사용자도 송신자가 보낸 메시지에 대한 무결성 검증을 할 수 없음으로 이런 경우 수신자는 송신자에 대한 인증도 함께 달성되어 지게 된다.

암호학적 해쉬 함수인 키-기반 메시지 인증 코드 HMAC(Keyed-Hash Message Authentication Code)은 안전한 공유 비밀 키를 기반으로 하여 임의의 메시지에 대한 MD-5, SHA-1, SHA-256 등의 암호학적 해쉬 알고리즘을 사용한다. 비밀 키 k를 기반으로 한 MAC을 사용함으로서 데이터의 무결성 보장뿐만 아니라 메시지 및 개체 인증도 가능하게 된다[11~13].

$HMAC(k,m)$은 다음의 수식 (4)와 같이 정의된다.

$$HMAC(k,m) = H((k_o \oplus opad) \| H((k_i \oplus ipad) \| m)) \quad (4)$$

여기에서 $H(\cdot)$는 암호학적 해시함수를 의미하고, k_o와 k_i는 비밀 키 k로부터 유도된 외부/내부키이며 해시함수의 블록 크기에 맞추기 위해서 여분의 공간은 0으로 채운다. $\|$은 결합 연산자이고, $\oplus$는 비트 단위 배타적 논리합(Exclusive Or, XOR)연산이며, opad와 ipad는 각각 외부/내부 패딩을 의미한다[11~13].

2. 데이터 은닉 처리 과정

제안한 데이터 은닉 처리과정에서는 비밀 데이터를 이미지에 은닉한 결과 이미지로 부터 그 비밀 데이터를 다시 추출하는 과정에서 완벽하게 원본 이미지로 복원 가능하도록 하기 위해 DE(Difference Expansion) 알고리즘을 사용하였다. 또한 의료 영상 데이터 내에 환자의 아이디 및 상태 정보를 기록하고, 이 데이터가 훼손되었는지를 빨리 판단하기 위한 방법으로 $HMAC$을 사용하였다. 이때 송·수신자 간에 공유된 비밀 키를 활용함으로서, 영상데이터에 대한 무결성을 쉽게 확인 할 수 있도록 설계하였다.

제안한 데이터 은닉 처리 과정은 그림 2와 같이 수행되며 단계별 순서는 다음과 같다.

단계 1: 수식 (5)를 이용하여 환자의 정보를 입력 값으로 한 해쉬 값을 생성시킨다. 이때 비밀 키 k를 사용하여 메시지의 무결성을 유지시킨다. 즉 다음과 같이 메시지 인증 코드 값 HV를 계산한다.

$$HV = HMAC_k(PI)$$

여기에서 PI는 환자의 정보이고 $HMAC$는 키-기반 암호학적 해쉬 함수이다.

단계 2: 생성된 메시지 인증 코드 값 HV를 이진 숫자로 변환한다. 추가적으로 환자의 정보도 이진 숫자로 변환한다. 변환된 각각의 이진 데이터를 수식 (5)과 같이 결합(Concatenation)하여 커버이미지에 삽입할 준비를 한다.

$$Data = str2bin(HV) \| str2bin(PI) \quad (5)$$

단계 3: 위 DE 알고리즘의 수식 (1), (2), (3)을 이용하여 다음과 같이 새로운 x'와 y'를 구하여 원본 영상 이미지 GI의 픽셀 값들을 새로운 픽셀 값들로 대치시

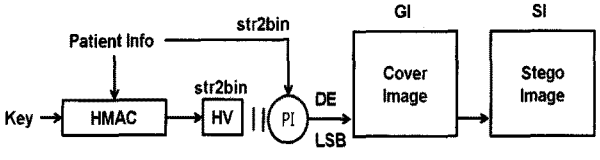


그림 2. 정보 은닉 과정
Fig. 2. Data hiding procedure.

킨다. 그 결과로서 데이터 은닉 처리된 스테고(Stego) 이미지 SI가 생성된다.

$$diff' = 2 \times diff + Data(count_1^n)$$

$$x' = avg + \left\lfloor \frac{diff+1}{2} \right\rfloor,$$
$$y' = avg + \left\lfloor \frac{diff}{2} \right\rfloor$$

3. 데이터 추출 및 인증을 통한 무결성 확인 과정

위 데이터 은닉 처리된 스테고 이미지 SI는 환자의 정보가 포함된 영상자료이다. 이 영상자료로부터 환자의 정보를 추출한 후 추출된 자료의 훼손 및 조작 여부를 $HMAC$을 통해서 확인한 후 최종적으로 $HMAC$ 처리되기 이전의 본래의 원본 이미지를 복원되도록 하는 것이 본 데이터 추출 및 인증을 통한 무결성 확인 과정의 목적이다. 제안한 데이터 추출 및 인증을 통한 무결성 확인 과정은 그림 3과 같이 수행되며 단계별 순서는 다음과 같다.

단계 1: 먼저 데이터 은닉 처리된 스테고 이미지 SI로부터 두 픽셀 단위로 읽어서 DE 알고리즘의 수식 (1)을 적용한다. 그 결과로 1비트의 은닉 데이터를 추출할 수 있다. 추출한 후 원래의 $diff$을 수식 (2)를 통하여 구하고 수식 (3)을 적용함으로써 원래의 두 픽셀을 복원하게 된다. 이러한 과정을 스테고 이미지 SI의 크기만큼 반복 적용하여 모든 은닉 데이터를 추출한다. 그 결과로 원본 이미지 GI를 완벽하게 복원할 수 있을 뿐만 아니라 삽입한 은닉 데이터 모두를 추출할 수 있게 된다.

단계 2: SI로부터 추출한 은닉 데이터를 PI'라 할 때, 이것으로부터 수식 (5)을 기반으로 HV와 PI를 분리한다.

단계 3: PI를 수식 (4)에 적용하여 $HMAC$을 구한 후 그 결과 값이 HV와 동일한지 여부를 비교한다. 만약 두 비교의 결과가 일치하면 해당 영상 자료로부터 추출한 환자의 의료 정보는 오류가 없는 것으로 판단하여 안전하게 사용한다. 만약 두 $HMAC$ 비교 값이 일치하지 않는다면 해당 영상은 조작 또는 오류가 있음을 인지하게 되어 폐기 또는 사용하지 않는다.

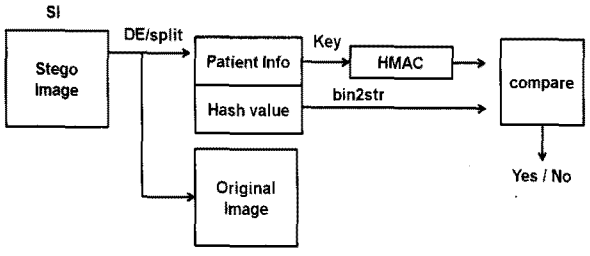


그림 3. 정보 추출 과정
Fig. 3. Data extracting procedure.

IV. 실험 및 분석

본 논문에서 실험을 위해서 의료 영상 MRI 자료를 구글 검색엔진을 통해서 얻었다. 수집한 의료 영상 이미지에 표 1과 같은 환자 의료 정보를 기록한다. 표 1에서 환자의 상태(Conditions)는 병명 혹은 징후를 의미한다. 환자에 대한 처방(Interventions)은 약, 백신 등의 투여 혹은 정밀 검사가 가능하다. 모든 환자들은 환자들의 상태에 따라서 단계(Phase)별 처치가 다르다.

본 논문에서는 이미지에 의료 정보를 저장한 이미지와 원래의 이미지를 비교하여 비밀 데이터를 저장한 이미지의 질(Quality)이 이미지를 사용하는 사람에게 어느 정도 허용 가능한가를 측정하는 방법으로 PSNR(Peak Signal-to-noise ratio)[3~4]을 측정하여 사용하였다. PSNR 측정값을 기준으로 하면 일반적으로 허용 가능한 이미지 질은 통상 30dB이상이면 시각적으로 이미지 훼손 여부를 쉽게 구분할 수 없다. PSNR은 신호의 최대 출력과 오류 잡음의 출력간의 비율을 의미하는데, 통상적으로 PSNR은 손실 압축 코덱의 재생의 질을 측정하는데 사용된다. 압축 코덱을 비교할 때, PSNR은 사람의 시각인식 재생에 대한 추측에 사용된다. 그러므로 어떤 경우에는 재생이 원래의 이미지에 근접한 결과를 보일 수 있다. 이것은 이미지 크기 $m \times n$의 이미지 I 와 K에 대한 평균 제곱 에러(MSE)로 정의할 수 있다. 이중 한 이미지는 다른 이미지의 노이즈로 다음 수식 (6)과 같이 정의한다.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \| I(i,j) - K(i,j) \|^2 \qquad (6)$$

PSNR 수식의 정의는 다음과 같다.

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \qquad (7)$$

여기서 MAX_I는 이미지의 가능한 최대 픽셀 값을 의미한다. 손실 이미지와 비디오 압축에서 PSNR을 위한

표 1. 차트와 관련한 의료 정보
Table 1. Medical information related chart.

Conditions	Interventions	Phase
Brain Stem Neoplasms, Primary Neoplasms, Brain Stem	Drug: Carboplatin Drug: Thalomid Procedure: External Beam Radiation Therapy	Phase II

<Name> Christina Applegate
<ID> PI00001
<Condition> Brain Stem Neoplasms, Primary Neoplasms, Brain Stem
<Intervention> Drug: Carbonation
Drug: Thalomid
Procedure: External Beam Radiation Therapy
<Phrase> 2
<Hash>6e0572dab0727addedf1afbeb51a6af7

그림 4. 환자의 의료정보
Fig. 4. Patient medical information.

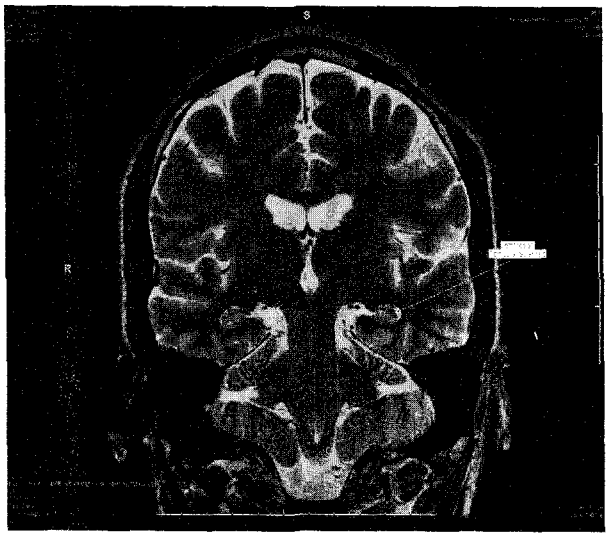


그림 5. 뇌 MRI (원본 영상, 999×1274)
Fig. 5. Brain MRI (original image, 999×1274).

전형적인 값은 30dB에서 50dB의 범위에 있다. 여기서는 숫자가 큰 것이 높은 이미지 질을 의미한다. 환자의 정보는 환자의 이름, 아이디, 그리고 표 1의 정보를 이용하여 실험하였다. 이때 저장할 환자의 정보와 메시지 인증 코드 *HMAC*에 대한 최대 비트수는 1912비트로 정의하였다.

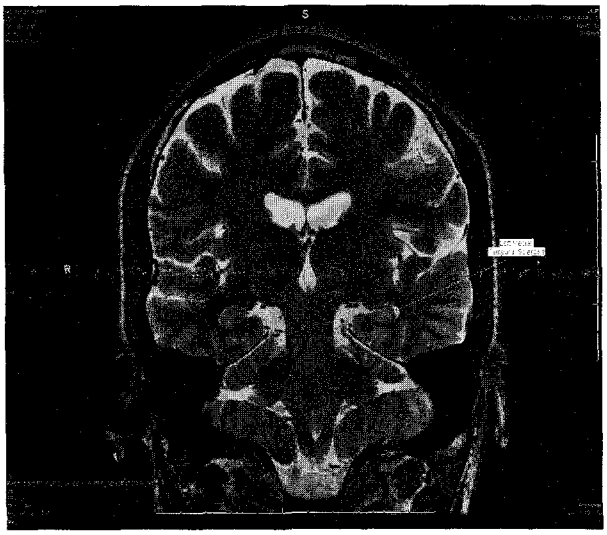


그림 6. 뇌 MRI (스테고 영상, 999×1274)
Fig. 6. Brain MRI (stego image, 999×1274).

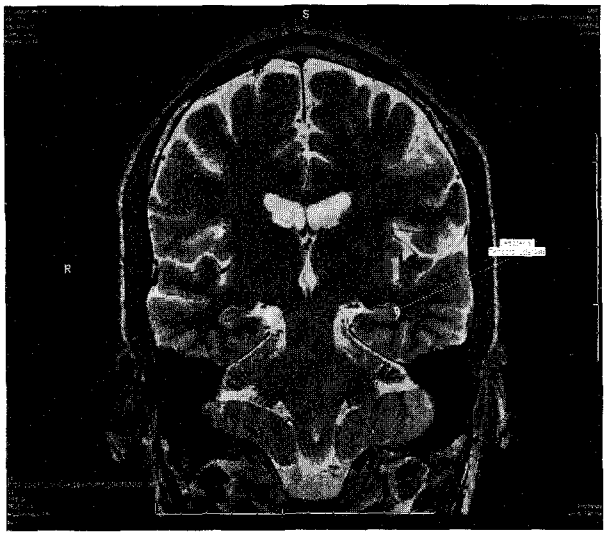


그림 7. 뇌 MRI (복원 영상, 999×1274)
Fig. 7. Brain MRI (recovered image, 999×1274).

그림 4의 환자 비밀 데이터를 그림 5의 의료 영상 이미지 내에 위 DE 알고리즘 수식 (1), (2), (3)을 이용하여 해당 환자 비밀 데이터를 은닉하였다. 그림 6의 PSNR은 48.3691dB로서 50dB에 근접한 높은 이미지 질의 보여주었다. 그림 7은 데이터 추출 알고리즘을 이용해서 복원한 이미지로서 그림 5의 원본 영상 이미지와 완벽히 동일하게 복원 되었을 뿐만 아니라 *HMAC* 검증 과정을 통해서 원본 데이터가 훼손되지 않은 처음 그대로의 데이터임을 증명할 수 있었다. 실험 결과로서 제안한 방법은 완벽하게 원본 영상으로 복원이 가능하였으며 영상 정보의 위변조 여부도 *HMAC* 검증 과정을 통해 효율적으로 수행할 수 있음을 확인하였다.

Ⅳ. 결 론

오늘날 대부분의 의료 기관에서는 환자의 의료 영상 자료의 관리를 위해서 영상자료의 상단 또는 하단 모서리 부분에 환자에 대한 관리정보를 누구든지 식별 가능하도록 기록 관리하고 있다. 이러한 방법은 간단하지만 환자의 프라이버시를 침해할 수 있으며, 악의적인 공격자에 의해 쉽게 수정 및 위변조가 가능할 뿐만 아니라 영상 관리자에 의한 생각지 못한 오류 기입 및 관리 부실로 인한 정보 삭제 등으로 인해 잘못된 의료처방을 시행하게 되어 의료 사고를 유발 시킬 수 있다.

위와 같은 문제점을 해결하기 위한 방법으로 본 논문에서는 의료 영상자료에 저장된 메시지 관리와 영상자료 자체를 효율적으로 관리할 수 있는 복원 가능한 정보 은닉 및 효율적인 메시지 인증 기법을 제안하였다. 기존의 의료영상 보안 기법들과 비교하여 제안한 방법의 가장 큰 장점은 첫째, 은닉 정보를 복원한 후에는 원본 영상이 숨기기 전의 원영상으로 완벽한 복원이 이루어져 원영상 훼손이 전혀 없으며, 둘째, 영상 정보의 위변조 여부를 *HMAC* 검증 과정을 통해 효율적이며 안전하게 수행 할 수 있다. 향후 연구 과제로는 제안한 방법에서 보다 다양한 비밀 키를 적용하여 접근 권한을 부여함으로써 의료기관 내부자라도 악의적인 영상 조작 등을 방지할 수 있은 방법을 연구하고자 한다.

참 고 문 헌

[1] Provos, N. Honeyman, P., Hide and seek: an introduction to steganography, Security & Privacy, IEEE, issue.3, pp.32-44, May 2003

[2] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq,"Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Trans. Multimedia, vol.5, pp.97 - 105, Mar. 2003.

[3] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol.14, pp.253 - 266, Feb. 2005.

[4] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding – new paradigm in digital watermarking," EURASIP J. Applied Signal Process., vol.2002, pp.185 - 196, Feb. 2002.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuit Syst. Video Technol., vol.13, pp.890 - 896, Aug. 2003.

[6] H.J. Kim, V. Sachnev, Y.Q. Shi, J. Nam, and H.- G. Choo, "A novel difference expansion transform for reversible data embedding," IEEE Trans. Inf. Forensics Security, vol.3, pp.456 - 465, Sep. 2008.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuit Syst. Video Technol., vol.16, pp.354 - 362, Mar. 2006.

[8] S. Han, M. Fujiyoshi, and H. Kiya, "A reversible image authentication method free from location map and parameter memorization," in Proc. IWAIT, 2009.

[9] Chia-Chen Lin, Wei-Liang Tai, Chin-Chen Chang, Multilevel reversible data hiding based on histogram modification of difference images ,Pattern Recognition, vol. 41, Issue 12, pp. 3582-3591, December 2008.

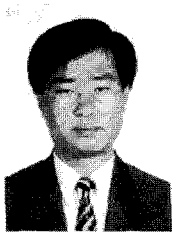
[10]Zhe-Ming Lua, Jun-Xiang Wang, Bei-Bei Liua, An improved lossless data hiding scheme based on image VQ-index residual value coding , Journal of Systems and Software, vol. 82, Issue 6, pp. 1016-1024 June 2009.

[11]L. Xie, G. R. Arce, R. F. Graveman, Approximate Image Message Authentication Codes, IEEE Transactions on multimedia, vol.3, no.2, june 2001.

[12]H. Krawczyk, HMAC: Keyed-Hashing for Message Authentication, RFC 2104, February 1997

[13]양종필, 이경현, 패스워드 추측공격에 강한 HMAC에 기반한 패스워드 인증, 정보통신진흥원, 정보통신연구진흥원 학술기사 Feb 2006.

저 자 소 개



김 천 식(정회원)

1997년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
2003년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
2000년~2003년 경동대학교 정보통신공학부 교수
2004년~현재 안양대학교 교수
2007년~2009년 대한전자공학회 컴퓨터소사이어티 멀티미디어 분과위원장
2006년~현재 인터넷 정보학회 학회편집위원
2006년~현재 대한교통학회 정회원
2007년~2008년 인터넷방송통신tv학회 상임이사
2005년~현재 한국데이터베이스학회 정회원
2008년~2009 ICHIT committee member
2009년 ACIIDS 2010 committee member
2009년 대한전자공학회 JUCT 영문저널 위원
2009년 2009 ICACT committee member
2009년 IEEE member
<주관심분야: 데이터베이스, 데이터마이닝, Steganography, 영상처리, e-Learning>

윤 은 준(정회원)

1995년 경일대학교 졸업 (공학사)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년~현재 경북대학교 전자전기컴퓨터학부 계약교수
2009년~현재 대한전자공학회 컴퓨터소사이어티 편집위원
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>

조 민 호(정회원)

1984년 조선대학교 산업공학과 (학사)
1994년 미국 Lehigh University 산업시스템공학과 (박사)
1994년~1997년 삼성전자 LCD Division 선임연구원
2008년~현재 고려대학교 정보경영공학전문대학원 연구교수
2009년~현재 Editor of IEEE Network
2007년~현재 Founding Editor-in-Chief of KSII Transactions on Internet & Information Systems
2007년~현재 Editor of Wireless Communications and Mobile Computing (Wiley & Sons)
2008년~현재 Editor of Security and Communication Networks (Wiley & Sons)
<주관심분야 : 네트워크보안, 무선 센서 네트워크, 무선 메쉬 네트워크, 소프트웨어시스템공학, RFID, MIMO Network Optimization, Ubiquitous Computing>

홍 유 식(정회원)

1984년 경희대학교 전자공학과 (학사)
1989년 뉴욕공과대학교 전산학과 (석사)
1997년 경희대학교 전자공학과 (박사)
1985년~1987년 대한항공(N.Y.지점 근무)
1989년~1990년 삼성전자 종합기술원 연구원
1991년~현재 상지대학교 컴퓨터공학부 교수
2000년~현재 한국 퍼지 및 지능시스템학회 이사
2001년~2003년 한국정보과학회 편집위원
2001년~2003년 한국컴퓨터교육산업학회 이사, 편집위원
2004년~현재 건설교통부 ITS 전문심사위원
2004년~현재 원주 시 인공지능신호등 심사위원
2005년~현재 정보처리학회 이사
2005년~현재 인터넷 정보학회 이사
2006년~현재 인터넷 방송통신 TV학회 상임이사
2010년~현재 대한전자공학회 컴퓨터소사이어티 회장
<주관심분야: 퍼지 시스템, 전문가시스템, 신경망, 교통제어>