한국컴퓨터정보학회지
제24권 제1호, 2016. 6.

의료영상정보 관리 방법

• 안일영(서정대학교 인터넷정보과)
• 김영천(서정대학교 인터넷정보과)

I. 서 론

컴퓨터에 의한 의료 정보처리와 고속 통신망을 통한 의료 정보 공유는 저가의 컴퓨팅 기술과 네트워킹 하드웨어의 보급에 따라 공통 관심사가 되어왔다. 현재 텍스트 파일이나 이미지와 같은 의료정보는 빠르고 신뢰성있는 저장장치와 복구를 위한 의료 데이터베이스 시스템에 저장되어 있다. 이외에도 이전에 획득한 필름으로 된 이미지나 수기된 문자도 디지털화되어 저장되었다. 별개의 정보 시스템을 운영하는 것 보다 통합된 시스템에서 이용 가능한 완전한 환자의 의료정보를 가지는 것이 편리하다. 원격 진료와 같은 의료적 응용은 불안전한 네트워크상에서 정보교환을 요구한다. 의료영상의 무결성과 신뢰성 보호는 환자의 의료기록 관리에 있어서의 이슈이다. 연성 워터마킹과 강성 워터마킹 기술들이 무결성 제어와 EPR (electronic patient record) 은닉을 위해 사용되어 왔다[1-4].

의료기관은 환자 중심의 의료서비스와 협진, 원격진료, 연구 등의 목적으로 의료정보의 교류가 빈번히 이루어지고 있으며, 디지털 영상 처리 등의 정보화 신기술의 등장, 네트워크의 광역화 및 무선 네트워크의 발달로 의료 정보화는 진화를 거듭하고 있다. 네트워크로 연결되어 연동되는 EMR(electric medical record), PACS(picture achieving and communication system), OCS(oder communication system) 등의 의료정보 시스템을 보호하고, 저장되어 있는 정보자산까지 안전하게 보호하기 위해서는 보안 기술의 적용이 필수적이다. 의료정보 시스템에서의 보안 위협의 현황 파악과 의료정보의 프라이버시 보호 및 보안을 위한 기술적 요구사항을 파악하여야 한다[5].

의료영상에 정보를 삽입하는 여러 가지 방법들은 의료 영상의 공유를 위해 각기 다른 보안 요구사항(신뢰성, 인증성, EPR 은닉 등)을 만족한다[6,7]. 이 방법들은 의료 영상의 정보보호를 위해 제안되었으며 다음과 같은 특징이 있다.

·EPR은 저장장치의 요구사항과 네트워크 대역폭을 줄이도록 의료영상에 삽입된다.

·공유 의료영상은 삽입된 정보가 보이지 않도록 하고 악의적 사용자의 주의를 끌지 않아야 한다.

·의료영상 수령자는 전송시에 의료영상이 변경되지 않는다는 것을 보장하기 위해 수신한 영상을 인증할 수 있다.

또한 미국의 HIPAA와 유럽의 EC 95/46 지침들에서 의료정보 보호는 엄격한 윤리적, 법적 규범으로 규정된다. 임상검사, 진단 기록, EPR에 중점을 둔 소견과 이미지 등에 따른 환자의 의료정보 기록을 중심으로 의료정보 기록의 3가지 필수적 특성은 다음과 같다[8].

·기밀성(confidentiality) : 인증된 사용자만이 그 정보에 접근할 수 있다.

·가용성(availability) : 정상적인 환경에서 정보 시스템을 사용할 수 있어야 한다.

·신뢰성 : 인증되지 않은 사람이 정보를 변경하지않을 것(무결성)이며 정보가 권한이 있는 자에 의해 만들어졌다는 증명(인증)이 가능하여야 한다.

의료정보 시스템에 있어서 5가지 보안 서비스(무결성, 가용성, 인증, 기밀성, 승인)를 통하여 이러한 특성들을 유지한다. 가용성, 무결성, 신뢰성 서비스가 보안의 관점에서 유사하다고 하면 인증 서비스는 전송, 메시지, 원본 또는 개인의 인증을 증명하는 방법이다. 승인 서비스는 전달의 증명과 메시지 전송자의 구별을 다룬다. 배포자를 추적하기 가능할 때 신뢰성은 추적성으로 확장할 수 있다.

II장에서는 의료 영상정보의 표준인 DICOM과 HL7에 대하여 기술하고 III장에서는 의료영상 정보 관리에 대한 여러 가지 방법에 대하여 고찰한다. 디지털 시그네쳐와 환자의 데이터를 의료 이미지에 삽입하는 방법, 환자의 개인정보 보호를 위해 불법적으로 배포된 의료 이미지를 추적하는 방법, 의료 이미지의 용도에 따라 다중 워터마크를 삽입하는 방법들이 있다. 마지막으로 IV장에서는 결론을 기술한다.

II. 표준화 동향

1. DICOM

DICOM 표준은 네트워크를 통한 통신을 위한 프로토콜이다. 프로코콜을 사용하여 교환할 수 있는 구문과 관련 정보, 미디어 통신에 대하여 이미지 접근을 손쉽게 하는 파일 포맷과 의료 디렉토리 구조뿐만 아니라 미디어 저장 서비스 같은 사항을 기술하여 의료영상 장비의 호환을 촉진한다. 이러한 표준은 방사선학 등 다양한 의료 관련 분야에 적용함으로써 진단 의료영상에 비중을 두고 개발되어 왔다. DICOM 표준의 내용은 다음과 같다.

1) 적합성(conformance) : 적합성에 따라 구현함으로써 만족해야 하는 일반적 요구사항을 기술한다. 적합성 명세의 구조와 나타내야 할 정보를 기술한다. 구현의 적합성을 평가하기 위한 검증 수순은 기술하지 않는다.

2) 정보객체 정의 : 디지털 의료영상과 관련된 정보의 통신에 응용할 수 있는 현실세계 엔티티를 정의한다. 정규화 정보객체 클래스는 현실세계에서 고유의 속성만을 포함한다. 이것은 이미지 데이터와 연관 데이터가 밀접하게 연관될 필요가 있는 이미지의 통신 요구사항을 표현하기 위한 프레임 워크를 제공한다.

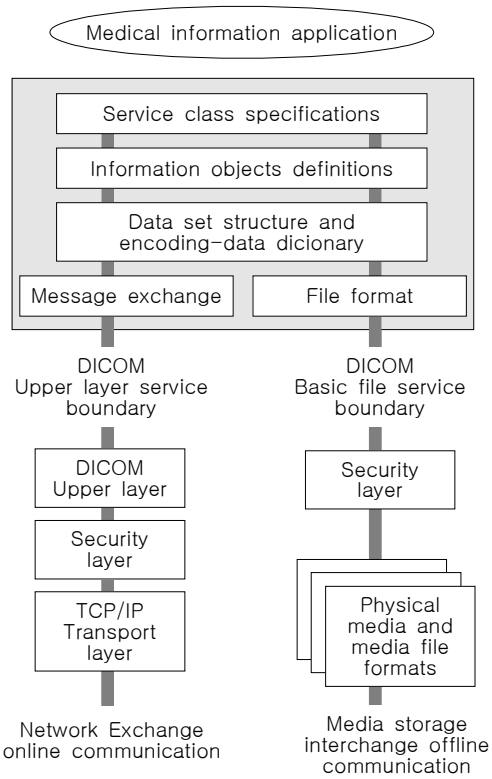

Fig. 1. DICOM 통신 모델

3) 서비스 클래스 명세 : 서비스 클래스 명세는 명령 요소의 요구사항과 명령들이 어떻게 정보객체에 적용되는지 기술한다. 통신 서비스 공급자와 사용자 둘 모두에 대한 요구사항을 기술한다. 이것은 모든 서비스 클래스와 공유되는 특성을 정의하고 개별적인 서비스 클래스에 대한 적합성 명세를 어떻게 구성할지 정의한다.

4) 데이터 구조와 구문 : 이 표준은 정보객체 정의와 서비스 클래스 명세 표준에서 정의된 정보 객체와 서비스 클래스와 관련한 데이터 셋을 DICOM 응용이 어떻게 구성하고 암호화하는지 기술한다. JPEG과 같은 여러 가지 표준 이미지 압축기술과 데이터 스트림을 구성하기 위한 암호화 규칙을 기술한다.

5) 데이터 사전 : DICOM 데이터 요소의 집합을 정의하는 중앙집중된 레지스트리이다. 각 요소에 대하여 그룹과 요소 번호로 구성된 태그, 이름, 값 등을 기술하고 구분된 항목에 대하여는 수치 값, 이름, 데이터 전송을 위해 부호화 정의인 정보객체 클래스나 정보객체 인스턴스 등을 기술한다.

6) 메시지 교환 : 통신망을 통하여 메시지를 교환하기 위

한 의료 이미징 환경에 있어서 응용에 사용된 서비스와 프로토콜을 기술한다. 명령 요청과 응답의 교환을 관리하는 규칙, 커맨드 스트림과 메시지를 구성하기 위해 필요한 부호화 규칙 등을 기술한다.

이외에도 메시지 교환을 위한 네트워크 통신 지원, 미디어 스토리지와 파일 포맷, 미디어 스토리지 응용 프로파일, 데이터 교환을 위한 스토리지 기능과 매체 포맷, 그레이 스캐일 이미지 표현, 보안과 시스템 관리 등에 대한 표준이 있다.

2. HL7

HL7(health level 7)은 분산된 의료정보 처리를 위하여 시스템간 자료 전송을 효율적으로 수행하고 전송 오류를 최소화할 수 있는 표준을 정립하고 있다. 또한 전자 건강정보의 교환, 통합, 공유, 복구에 대한 프레임 워크를 제공한다. 시스템간 어떻게 정보를 주고 받는지 끊김없는 통합을 위한 구조와 데이터 타입 설정 등을 정의한다.

1) 1차 표준 : 시스템 통합, 운용성, 적합성을 위한 표준이며 가장 많이 사용된다.

2) 기본적 표준 : 기본적 도구와 HL7 표준의 구현을 다루어야하는 기술을 정의한다.

3) 임상과 관리적 영역 : 임상적 특수성과 그룹에 대한 도큐먼트 표준을 정의하는데 일단 1차 표준에서 보통 구현한다.

4) EHR(electronic health record) 프로파일 : 건강기록 관리를 위한 모델과 프로파일을 제공한다.

5) 구현 가이드 : 구현에 대한 지침이며 현재의 표준에 대한 보충 자료이다.

6) 규칙과 참조 : 기술적 사양, 프로그래밍 구조, 소프트웨어와 표준개발을 위한 가이드 라인을 정의한다.

7) 교육 : HL7에 대한 채택, 보충 이해에 대한 도구 등을 제공한다.

III. 관련 연구

공개키 암호화 방법의 주요한 응용으로서 F. Cao 등은 DICOM 이미지 헤더로부터 복호화된 환자 정보와 이미지의 디지털 시그네쳐(digital signature)를 포함하는 정보를 사용하여 의료 이미지에 메시지를 삽입하였다[11]. 그림2와 같이 의료 이미지를 구성하는 사각 영역 바깥 부분에 디지털 시그네쳐와 환자 정보를 덧붙여 삽입한다. 이 이미지를 공개키로 암호화하여 전송하고 수신측에서는 비밀키로 복호화한다. 수신된 이미지를 구성하는 사각 영역이외에서 디지털 시그네쳐를 검출한다. 이것을 원 이미지의 디지털 시그네쳐와 비교하여 전송된 이미지가 손상되지 않았는지 판단할 수 있다.

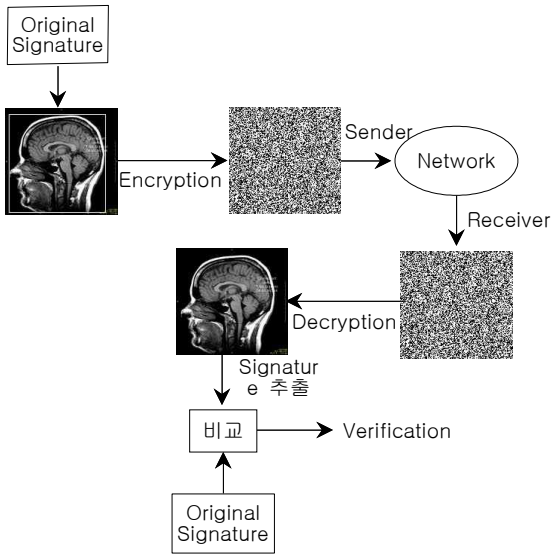

Fig. 2. 시그네쳐를 이용한 의료 이미지의 검증

전처리는 배경 제거와 분할로 구성된다. 그 목적은 필요한 이미지 크기를 줄여 이미지 처리속도를 높이는 것이고 이미지의 바깥 영역에 데이터를 삽입하도록 하는 것이다. 방사선 이미지에서 환자 이름, ID, 기타 비진료 관련 정보 등 진단과 무관한 부분은 제거한다. 유방 방사선 이미지에서는 최소 사각영역 알고리즘을 적용할 수 있으나 그 외 방사선 이미지는 이미지의 최하위 비트에 정보를 삽입한다. 단층 이미지에서는 배경 제거가 필요없다. 최소 사각 영역으로 분할한 이미지 바깥영역의 픽셀은 진단에 무관하므로 시그네쳐 등을 삽입한다.

이미지 해쉬 값을 계산하고 이것을 송신측의 비밀키로 암호화하여 시그네쳐를 생성한다. 수신한 이미지에 대하여 같은 알고리즘으로 이미지 해쉬 값을 계산한다. 송신측의 공개키로 시그네쳐를 복호화하여 소유자에 의해 계산된 해쉬 값과 비교한다. 입력 이미지의 한 개의 데이터 비트의 변화에서도 해쉬 값은 달라지므로 두 개의 해쉬 값이 같다면 수신측은

이미지가 비밀 키를 가진 소유자에 의해 서명되었으며 그 이미지는 서명된 이후 변경되지 않았다는 것을 보장한다. 이미지에 삽입한 정보는 이미지의 디지털 시그네쳐와 환자 데이터를 연결시켜 수신측의 공개키를 사용한 암호화로 생성된다. 여기서 생성된 정보는 데이터의 비밀성 뿐만 아니라 이미지 인증과 무결성을 보장한다. 수신측에서 인가된 사람만이 비밀키로 액세스하기 때문에 인가된 사람만이 시그네쳐를 볼 수 있다. 이미지 시그네쳐와 환자 데이터를 공개키로 암호화하는 방법은 PACS 환경에서 이미지 보안에 효과적이다.

데이터 삽입은 화질이 손상되지 않도록 이미지에 정보를 숨기는 형태이다. 데이터를 삽입하기 위해 전체 세그멘트 이미지에 랜덤 시퀀스(random sequence)를 만든다. 이 랜덤 시퀀스를 따라서 한 비트씩 랜덤하게 선택한 픽셀마다 LSB를 교체한다. DICOM 이미지 헤더에 암호화된 정보를 넣음으로써 삽입된 정보를 이미지에서 검출하기 어렵다. 또한 헤더가 이미 삽입되었으므로 DICOM 이미지 헤더를 따로 전송할 필요가 없다. 이미지에서 분리된 DICOM 헤더의 정보는 쉽게 삭제되고 헤커에 의해 조작될 수 있다.

M. Li 등은 환자의 개인정보 보호를 위해 인증되지 않은 의료 이미지의 배포자를 추적하는 방법을 연구하였다[12]. 의료 이미지에 있어서 워터마크에 의한 왜곡이나 이미지 압축은 진단 값을 손상하지 않도록 최소화되어야 한다. 고충실도에 대한 요구는 의료 이미지 워터마킹에 있어서 보다 높은 시각적인 왜곡을 허용하는 멀티미디어 응용보다 엄격하다. 의료 이미지는 40-50dB의 최소 PSNR(peak signal to noise ratio)이 요구되며 멀티미디어 응용은 20-30dB의 PSNR이 허용된다. 워터마크는 의료 이미지의 진단의 질을 향상시키기 위한 LPF, HPF와 같은 표준 영상처리와 JPEG 압축, 절단, 평균화 공격과 같은 고의적 공격에 살아남아야 한다.

의료정보 공유를 위한 시나리오는 다음과 같다. 환자는 주치의를 방문한다. 협진이 필요하면 의사는 다른 과의 전문의와 팀을 이룬다. 주치의는 데이터베이스에서 환자와 관련된 EHR(특히 이미지)을 검색하고 리뷰를 위해 다른 의사에게 EHR을 전달한다. 각 의사들은 자신의 의견을 기록하고 전체 그룹에 발송한다. 모든 보고서를 수령하여 주치의는 환자에 대한 치료 방법을 결정한다. 멀티캐스트 통신의 효율성을 가지는 반면 의료 이미지 추적은 미흡하다. 멀티캐스트 통신에서 다중의 수신자는 동일한 복사 이미지를 받는다. 누출 소스를 추적하기 위해 동시에 각 사용자에 대한 유일한 코드를 이미지에 삽입한다. 따라서 여러 사용자에 대한 별개의 코드를 가진 이미지가 생성된다. 이러한 이미지를 멀티캐스트하는 문제가 있다.

시스템 관리자는 원 이미지와 워터마크 키의 생성, 관리, 이미지 추적의 권리를 가진다. 이러한 관리자는 모든 사용자 i의 워터마크 시퀀스 w_i와 사용자 i의 워터마크 시퀀스를 제외한 각기 다른 사용자의 워터마크 시퀀스에 화이트 노이즈를 추가한 워터마크 키 Yi 생성, 배포한다. 워터마크 키 Ys를 가진 송신자 s는 이미지 X에 송신자의 워터마크 키를 더하여 전체 사용자에 전송한다. 수신자 워터마크 키 Yr를 가진 수신자는 수신한 이미지 X에 송신자의 워터마크 키에 수신자의 워터마크 키를 뺀다. 즉 수신한 이미지에 수신자의 워터마크 시퀀스에 송신자의 워터마크 시퀀스를 빼서 수신한 이미지 X를 얻는다. 그 식은 다음과 같다.

$$X+\alpha(Y_s-Y_r)=X+\alpha(w_r-w_s)$$

여기서 α는 가중치 값이다.

이미지 배포자를 추적하기 위해 시스템 관리자는 수신한 이미지에서 워터마크를 추출하여 모든 사용자의 워터마크 w_i와 추출한 워터마크와 상관관계를 계산한다. 이 값이 임계값보다 큰 w_i를 찾아낼 수 있다.

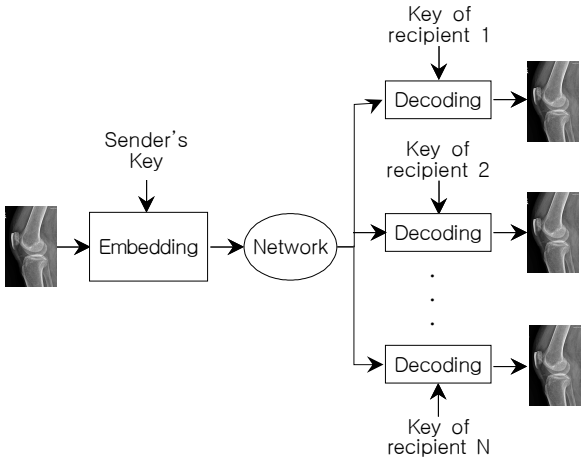

Fig. 3. 멀티캐스트 환경에서의 이미지 추적

그룹당 개인당 하나의 워터마크 키를 채용하여 다대다 멀티캐스트 모드에서 사용자 코드가 삽입된 이미지를 얻을 수 있다. N개의 송신자가 있는 다대다 시나리오로 확장하는 것은 N개의 각 사용자에 대한 키 저장장치의 요구사항을 증가

시킨다. 일대다 모드는 진찰후 각 전문가 그룹에 보내는 응용에 대하여 바람직한 통신 모드이다. 수신한 이미지는 수신자의 시그네쳐 wr뿐만 아니라 송신자의 시그네쳐 ws를 지닌다. 시스템 관리자는 수신 이미지의 워터마크와 모든 사용자 워터마크 사이 상관관계를 계산하여 수신자뿐만 아니라 원 송신자를 구별할 수 있다. 가장 큰 양수 값과 가장 작은 음수 값에 대한 상관관계의 절대값이 임계값 보다 크면 양수 값은 수신자, 음수 값은 송신자를 가르킨다.

그룹 멤버가 브로드캐스트 이미지를 받지 못하는 경우 송신자는 이미지를 재전송하거나 그들에게 이미지를 중계하기 위해 사용자 m을 명시한다. 중계가 일어나면 사용자 m은 브로드캐스트 이미지에서 워터마크 키 Ym을 빼는

$$X+\alpha(Y_s-Y_m)=X+\alpha(w_m-w_s)$$

과정으로 복사본을 복호화한다. 송신자로서의 사용자 m은 이미지를 포워딩하기 전 복호화된 이미지에 워터마크 키 Ym을 더하여

$$X+\alpha(w_m-w_s+Y_m)=X+\alpha Y_s$$

을 계산한다. 이것은 원래의 수신된 이미지 X+αYs를 포워딩하는 것과 동일하다. 전송 체인 시퀀스의 경우에서 중계 노드들은 이미지 상에 각 노드의 워터마크들을 남겨 놓지 않을 것이고 원래의 송신자의 워터마크와 마지막 수신자의 워터마크만 이미지에 남는다. 주어진 시간에서 두 개의 워터마크가 복호화된 이미지에 나타날 뿐이므로 수신측에서의 이미지 화질은 통제가능하다.

Giakoumake 등은 제안한 워터마킹 방법은 건강 관리 시스템에 있어서 의료 이미지에 대한 엄격한 비가시성의 요구사항을 만족하면서 의료기밀 보호, 데이터 무결성, 접근제어, 효율적인 데이터 관리와 복구 등이 가능하도록 한다. 특히 4가지 다른 워터마크를 다른 목적으로 동시에 삽입한다[13].

1) 의사의 ID 등으로 사용하는 시스네쳐 워터마크는 수령자의 소스 인증을 위해 사용한다.

2) 데이터베이스 쿼리에 따라 이미지 복구를 위해 사용될 수 있는 키워드인 인덱스 워터마크는 별개의 워터마크로 삽입된다.

3) 환자 개인정보와 진단, 환자의 인구통계, 건강 이력, 진단 보고서 등의 부가 데이터에는 캡션 워터마크를 삽입한다.

4) 데이터 무결성 제어와 조작위치 검출의 목적으로 모든 분해 레벨에 연성 워터마크를 삽입한다.

CT, MRI, 초음파 등 서로 다른 의료 이미지 획득 시스템을 통합하여 원격진단과 병원내의 효과적인 의료 데이터 관리, 기록, 열람까지의 응용에 사용될 수 있다. 이미지 획득시 의사는 ID, 환자 개인정보, 검사 데이터, 이미지 검색을 위한 키워드, 다른 의사의 지시에 대한 부가정보를 삽입한다. 이미지에 이러한 데이터와 함께 워터마킹한 후 병원 데이터베이스에 저장된다. 데이터베이스에 접근하는 과정은 키를 가지고 인가된 의료 종사자가 삽입한 워터마크를 추출하여 환자의 데이터와 이미지나 진단한 의사의 ID 등의 정보를 알 수 있다. 연성 워터마크를 추출하여 이미지의 무결성을 검사한다.

Ⅳ. 결 론

본 논문에서는 의료 이미지 정보의 관리를 위한 방법을 고찰한다. 디지털 시그네쳐와 환자의 데이터를 혼합한 정보를 의료 이미지에 삽입하는 방법, 의료 정보공유를 위해 인증되지 않은 의료 이미지 배포자를 추적하는 방법, 의료 이미지의 용도에 따라 4가지의 다른 워터마크를 삽입하는 방법들이 있다. 첫 번째 방법은 진단을 위한 이미지 영역 바깥쪽에 이미지 시그네쳐와 환자 데이터를 공개키로 암호화하여 삽입한다. 수신측에서 인가된 사람만이 비밀키로 액세스하기 때문에 인가된 사람만이 시그네쳐를 볼 수 있다. 이 방법은 PACS 환경에서 이미지 보안에 효과적이다. 두 번째 방법은 이미지 배포자를 추적하기 위한 방법으로 시스템 관리자는 수신한 이미지에서 워터마크를 추출한다. 모든 사용자의 워터마크 시퀀스 w_i와 수신 이미지에서 추출한 워터마크 시퀀스와의 상관관계를 계산한다. 이 값이 임계값보다 큰 w_i를 찾아낼 수 있다. 세 번째 방법은 용도가 다른 4가지의 워터마크를 이미지에 삽입한다. 이 방법은 의료 이미지에 대한 엄격한 비가시성의 요구사항을 만족하면서 의료기밀 보호, 데이터 무결성, 접근제어, 효율적인 데이터 관리와 복구 등이 가능하도록 한다. 향후 생체 정보 등과 같은 민감한 개인정보 보호를 위한 의료정보관리 방법에 대한 연구가 필요하다.

참 고 문 헌

[1] M. Ulutas, G. Ulutas, V. Nabiyev, “Medical Image Security and EPR hiding using Shamir's secret sharing scheme”, Journal of Systems and Software 84(2011), pp.341-353

[2] I. J. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, 2001.

[3] I. Cox, J. Kilian, T. Leighton, T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Trans. on Image Processing, vol.6 no.12, pp.1673-1687, Dec 1997.

[4] F. Petitcolas, R. Anderson and M. Kuhn, “Information Hiding-A Survey,” Proc. of the IEEE vol.87, no.7, pp.1062-1078, 1999

[5] “건강정보보호 및 보안체계 개발”보고서, https://www.hins.or.kr/ EgovPageLink.do, 사회보장정보원,2009

[6] D. C. Lou, M. C. Hu, J. L. Liu, “Multiple layer data hiding scheme for medical images”, Computer Standards and Interfaces 31, pp.329-335

[7] J. Hu, F. Han, “A pixel based scrambling scheme for digital medical images protection”, Journal of Network and Computer Applications 32, pp.788-794

[8] G. Coatrieux, L. Lecornu, B.Sankur, “A Review Image Watermarking Application in Healthcare”, Proceedings of the 28th IEEE EMBS Annual International Conference, 2006, pp.4691-4694

[9] Health Level Seven International, http://www.hl7.org/index.cfm

[10] National Electrical Manufacturers Association, http://dicom.nema.org/

[11] F. Cao, H. K. Huang, X. Q. Zhou, “Medical image security in a HIPAA mandated PACS environment”, Computerized Medical Imaging and Graphics 27(2003), pp.185-196

[12] M. Li, R. Poovendran and S. Narayanan, “Protecting patient privacy against unauthorized release of medical images in a group communication environment”, Computerized Medical Imaging and Graphics 29, 2005, pp.367-383

[13] A. Giakoumake, S. Pavlopoulos and D. Koutsouris, “Multiple image watermarking applied to health information management”, IEEE Trans. on Information Technology in Biomedicine, vol.10, no.4, October 2006. pp.722-732

저 자 소 개

안일영

1983년 한양대 전자공학과 졸업
1988년 한양대 대학원 전자공학과 졸업(공학석사)
2004년 한양대 대학원 전자계산학과 졸업
(공학박사)
2009년 ~ 현재 서정대학교 인터넷정보과 교수
※ 관심분야 : 영상처리, 영상압축

김영천

1992년 광주대 전자계산학과 졸업
1996년 조선대 컴퓨터공학과 졸업(공학석사)
2002년 조선대 전자계산학과 졸업(이학박사)
2003년 ~ 현재 서정대학교 인터넷정보과 교수
※ 관심분야 : 정보검색, 소프트웨어공학, 웹개발, RFID