□ 기술해설 □

의료정보 시스템의 보안

광주보건대학 정현철*

1. 서 론

환자의 병력, 약제 정보, 치료 정보 등과 같은 다양한 의료정보가 증가하므로 인하여 의료분야는 정보화의 물결을 실감하고 있다. 의료정보 관리, 생체신호 처리, 혈액과 대소변 검사, 진료수가 청구, X-ray, CT, 초음파, MRI에 대한 의료영상 분석 등에서처럼 의료분야에서 컴퓨터의 응용은 매우 광범위하다.

특히, 컴퓨터가 의료기기에 응용되므로써 대량의 검사를 신속, 정확하게 처리하고 의료 데이타 취급의 실수를 감소시킨다. 그리고, 의료 데이타의 분석, 처리를 수월하게 하며 객관성을 향상시킨다. 컴퓨터 통신은 필요한 의료정보의 송수신을 가능하게 하므로써 검사 및 진료 시간, 인력과 비용을 절감시킨다.

컴퓨터에서 의료 데이타의 종합적 관리는 의료 데이타의 효율성을 증가시키고 정확한 데이타 처리로 의사의 진단 능력을 향상시킨다. 또한, 중복과 손실에 따른 의료 기능의 부담을 방지하고 환자의 병력 데이타를 참조하여 진료의 질을 향상시켜서 양질의 의료 서비스를 환자에게 제공할 수 있다.

컴퓨터의 다양한 의료정보 처리는 의료기술의 새로운 분야의 개발을 유도했으며 진료 및 진단 능력에 커다란 변화를 초래하고 있다.

본 논문의 2장에서는 의료정보 시스템의 정의와 목표를 기술하고 3장에서는 의료정보의 보안을 설명한다. 그리고 4장에서는 결론을 맺는다.

* 정회원

2. 의료정보 시스템

의료정보 시스템은 첫째, 병원내의 업무만을 처리하는 병원정보 시스템과 둘째, 병원을 비롯한 여러 의료기관에 있는 모든 의료정보를 종합하여 업무를 수행할 수 있도록 의료 데이타 은행, 의료정보 센타로 구성되는 광역 의료정보 시스템으로 크게 구분할 수 있다[1].

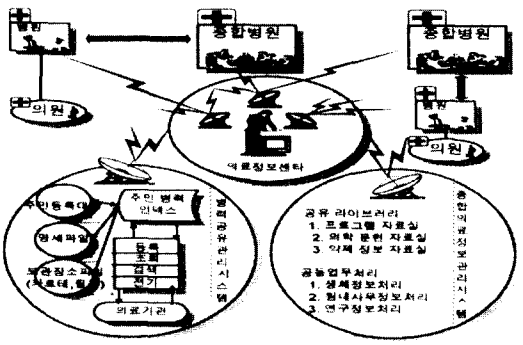


그림 1 의료정보 시스템

의료정보 시스템이 구축되면 컴퓨터 통신으로 환자의 데이타를 전송하여 원격지의 환자 검진이 가능하므로 지역, 광역 및 벽지 의료 서비스가 가능하다. 또, 각종 의료기관, 의학연구소에 소속되어 있는 의료관련 종사자들에게 의료정보 센타에 기억되어 있는 정보를 이용할 수 있게 한다. 의료정보 시스템에서는 모든 환자의 정보를 공동으로 등록 및 조회하여 데이타를 수집하고 개인의 사생활를 보장하기 위하여 이러한 의료 데이타를 보호하는 것이 아주 중요한 요소가 된다. 컴퓨터화된 환자 진료 데이타는 필요하다면 환자의 침대 또는 진료실에

서 직접 활용할 수 있다. 의료정보 시스템은 높은 성능이 보장되어야 하므로 빠른 응답성과 신뢰성을 고려해야 하고 환자의 프라이버시 보호를 위하여 의료 데이타를 활용할 수 있는 권한을 가진 의료 관계자만이 접근할 수 있도록 보안성을 고려해야 한다. 따라서, 본 논문에서는 이러한 여러 목표 중 보안 문제를 해결하기 위해 미국 스탠포드대학교 의과대학에서 진행하고 있는 TIHI(Trusted Interoperation of Healthcare Information) 시스템과 TIDE (Text Information Detection and Elimination) 시스템을 기술한다.

3. 의료정보의 보안

의사와 의료기록 부서, 회계원과 의료기록 부서, 공중보건 기관과 병원, 보험회사와 병원은 서로 협력하여 업무를 수행한다. TIHI 프로젝트[2]는 모든 의료정보가 공유되지 않더라도 의료정보의 일부가 의료관계 협력자들에게 공유될 때 발생하는 보안 문제를 다룬다. 협력자들의 정보 교환이 필수적일지라도 데이타와 정보 자원을 전적으로 공유할 수 없다. 적대자에게 정보를 거절하기보다는 협력자들간에 공유하는 정보를 보호하는 것이다.

3.1 보안 중재자(Security mediator)

환자에 대한 정보는 인증받은 의료관계자가 부분적으로 접근할 수 있도록 허용된다. 어떤 정보는 보험회사, 어떤 정보는 공중보건 모니터링에 이용된다. 그래서 고객에 대한 모든 정보는 개별적으로 제어되어야 한다. 예를 들면, 심장병 환자의 의료기록은 심장병 연구자가 소유하며 이 기록에는 노출되지 않아야 할 에이즈 바이러스(HIV)의 진단 기록이 포함되어 있다. 부적절한 정보의 영역(domain) 이탈 방지를 보장하기 위하여 책임과 권위를 갖는 보안 사무원(security officer)이 있다. 방화벽(fire wall)은 침입자에 대해서 영역을 보호한다. 각 보안 사무원이 소유하고 제어하는 별개의 컴퓨터 시스템인 게이트웨이는 영역의 입출력에 대해서 합법적인 루트만 제공한다. 이러한 시스템을 그림 2의 보안 중재자(security mediator)라고 한다[3].

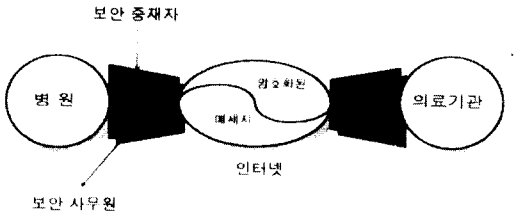


그림 2 보안 중재자 설정

보안 중재자가 설정한 보안 정책은 보안 사무원의 상호작용과 제어하에서 구현된다. 보안 중재자는 외부 요구에 대해서 통신 보안과 인증을 사용한다.

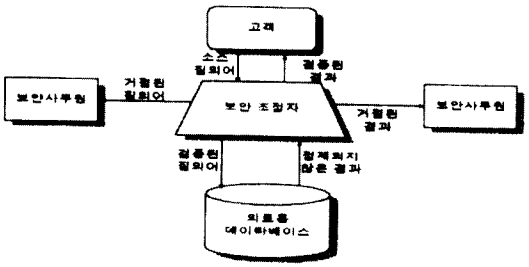


그림 3 양방향 정보 내용 검증

그림 3에서처럼 통신 내용의 검증이 질의와 응답 모두에 대해서 이뤄지는 것은 중요하다. 심장병 연구자가 심장병 환자에 대해서 HIV의 진단 기록을 포함한 모든 기록의 접근을 허용하는 것은 부적당하다. 접근 통제와 정보 보안의 보장 처리를 자동화하기 위하여 보안 사무원은 시스템으로 규칙을 넣고 보안 중재자는 모든 질의어의 검증과 정보의 보급에 적합한 결정을 하기 위하여 이 규칙을 사용한다. 질의어가 규칙을 위배하면 에러 메세지는 보안 사무원에게 보내지고 에러 메시지는 추론이 가능하므로 사용자에게는 보내지지 않는다. 모든 질의어와 에러는 회계감사를 위하여 시스템에 로그된다. 보안 중재자는 결과를 역시 검사하고 결과가 규칙을 위배하면 에러 메세지는 보안 사무원에게 보낸다. 뷰 기반 강제적 접근 제어를 위하여 질의어는 분석되고 뷰에 있는 데이타가 뷰를 접근하기 위하여 인증된 사용자의 접근 가능을 보장하도록 응답은 필터링된다. 두 타입의 질의어 분석[4]이 있다. 첫째는

단일 질의어 분석이다. 강제적 접근 제어를 시행하는 가장 쉬운 방법은 질의어의 발행자가 권한을 갖는 뷰의 관점에서 질의어를 형식화하는 것이다. 둘째는 질의어 열의 분석이다. 사용자가 발행되는 모든 질의어에 권한을 갖더라도 접근 권한을 갖지 않는 뷰에 있는 데이타를 유도하기 위하여 질의어 열로부터 응답을 결합할 수 있다.

3.2 웹 보안(Web security)

인터넷에서 의료 데이타로의 접근은 정보를 공유하는데 매우 용이하다. 보안 중재자는 고객, 질의어, 결과의 내용을 스크린에 보임으로써 데이타베이스에 있는 정보의 접근을 규칙화한다.

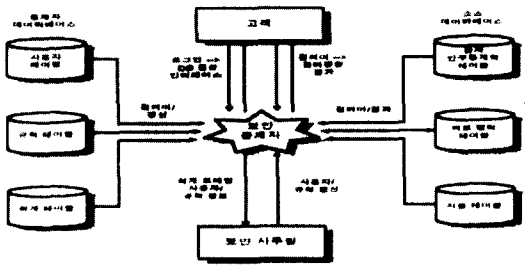


그림 4 웹 시스템의 구조

그림 4에서 후반부(back-end)는 고객의 관심이 있는 정보를 갖는 소스 데이타베이스다. 이 정보는 의료기관 내부에서 인증된 사람이 접근할 수 있도록 중앙 컴퓨터에 상주한다. 또 다른 요소는 중재자 데이타베이스다. 이것은 등록 고객의 암호와 사용자 이름을 갖는 사용자 테이블, 로그인, 질의 결과 스크린을 제어하는 정책 규칙이 있는규칙 테이블과 날짜, 시간 사용자 ID, 질의어, 결과, 규칙 위반 문장을 갖는 모든 트랜잭션의 기록인 회계감사 테이블을 저장한다. 이 데이타베이스는 다단계 보안 시스템에 의해서 보호되는 유닉스 웍스테이션에 상주한다. 보안 중재자와의 통신은 웹 기반 고객과 보안 사무원 인터페이스이다. 고객 인터페이스는 고객이 질의어를 제출하고 WWW을 연결하도록 지원하여 원격 지역에서 결과를 검색할 수 있게 한다. 고객 인터페이스는 로그인, 고객의 의료용 데이타베이스 접근, 결과 스크린으로 구성된다. 접근과 결과 스크린은 로그인 프로세서, 질의 프로세서, 결과 프로세서가 제어한다. 로그인 프로세서는 사용자 이름, 멤버십 그룹, 로그인 스크린에서 암호를 읽고 규칙 테이블에서 고객의 그룹과 관련된 설정(setup) 규칙을 검색한다. 규칙 위반이 탐지될 때, HTML에서 로그인 프로세서는 표준 에러 스크린을 생성하여 고객에게 반환한다. 설정 규칙을 모두 통과하면 고객 데이타베이스 접근 스크린을 고객에게 제공한다. 고객과 그룹에 대한 정보와 질의어는 HTML 형식을 통하여 질의 프로세서로 보내진다. 질의 프로세서는 고객의 그룹에 관련된 질의어 처리를 한다. 질의어가 모든 관련된 규칙을 통과하면 그때 결과는 받아지고 결과 프로세서가 처리한다. 성공적 질의는 모두 회계감사 테이블에 기록된다. 비성공적인 질의는 리뷰 큐로 보내진다. 성공적인 질의는 중재자가 해당 결과를 검색하고 결과 프로세서를 사용해서 스크린하도록 한다. 결과처리 규칙은 규칙 테이블에서 검색되고 결과에 적용된다. 규칙 위반이 발생하지 않으면 결과는 HTML 형식으로 고객에게 보내진다. 규칙 위반은 리뷰 큐로 보내진다. 사용자 이름, 그룹, 질의어, 위반된 규칙은 리뷰 큐의 엔트리로 저장된다. 보안 사무원은 각 엔트리를 검사하고 질의어가 허용되는지의 여부를 조사한다. 보안 사무원 인터페이스에서 보안 사무원은 그룹과 규칙 집합을 구축하고 시스템 사용을 모니터하며, 질의어와 보안 중재자가 불허한 결과를 찬성하거나 거절한다. 보안 사무원 HTML 인터페이스 홈 페이지에서는 보안 사무원에게 시스템 모니터링과 일반적 유지 기능을 제공한다[5].

3.3 이미지 보안(Image security)

진보된 의료장비가 질병의 진단과 관리에 사용될 때 환자 보고서, 의료 기록과 같은 전통적인 텍스트 데이타는 X-ray, MRI, CT, 3D volumn, 그리고 비디오 스트림으로 바뀐다. 의료영상이 온라인으로 제공되기에 앞서 환자의 프라이버시 보호 측면에서 영상에 나타난 환자 확인 정보를 제거할 필요성이 있다. 보안이 필요한 의료영상에 대해서 TIDE 시스템에서는

디지탈 의료영상내에서 텍스트의 정보에 대한 부분을 탐지하고 제거하기 위하여 도베치스 웨이블릿(Daubechies' wavelet)을 사용한다. 웨이블릿 변환은 영상을 몇 개의 해상도로 분해하기 때문에 웨이블릿 계수는 최초 영상의 연속적인 근접치를 형성한다. 도베치스 웨이블릿 변환을 사용해서 디지탈 의료영상에 대한 텍스트 정보를 탐지하고 제거하는 시스템 구조는 그림 5와 같다[6, 7].

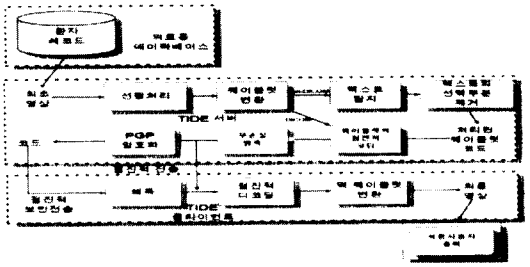


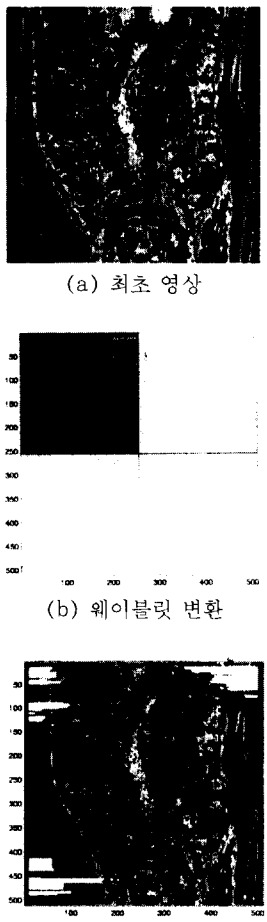
그림 5 TIDE의 기본 구조

① 선행처리 단계

현재 사용중인 많은 의료영상 형식 즉, DICOM, PPM, GIF, JPEG, TIFF는 가장 광범위하게 사용되는 형식이다. 의료영상이 다른 형식이기 때문에 먼저 계산을 위해 데이타를 정규화해야 한다. 칼라 의료영상은 방정식 WB=(R+G+B)/3을 사용해서 그레이 스케일로 전환된다. R, G, B는 RGB 칼라 공간에 있는 픽셀의 값이고 WB는 그레이 스케일에 있는 이 픽셀의 값이다. 이 시점에서 의료영상에 웨이블릿 변환을 적용한다. 도베치스 Symlet-8 웨이블릿 혹은 도베치스-8 웨이블릿을 사용하여 그레이스케일 PPM 영상을 변환하므로써 프로세스를 시작한다. 4개의 주파수 대역(frequency bands)로 영상을 분할한다. 저주파수(low frequency)는 L, 고주파수(high frequency)는 H로 표시한다. 좌상단 밴드는 LL 밴드라 하는데 행과 열방향 모두에서 저주파수정보를 갖기 때문이다. LH 밴드는 수평 선분에 대해서 민감하고 HL 밴드는 수직 선분, HH 밴드는 사선 선분에 대해서 민감하다. 의료영상에 대해서 HH 밴드는 텍스트가 있는 부분과 없는 부분을 잘 구분한다. 후행처리를 위해 HH 밴드만 유지한다.

② 후행처리 단계

후행처리는 텍스트 없는 영상 부분의 부적절한 제거를 방지해야 한다. 최초영상의 크기가 2n×2n이다면, 웨이블릿 변환의 크기는 2n×2n인 행렬이다. 후행처리 단계에서는 HH(1:n, 1:n) 행렬를 처리한다. 이진행렬B(1:n, 1:n)은 HH 행렬에서 가장 큰 M=O(n) 계수가 1로 대치되고 다른 모든 계수가 0으로 대치되도록 HH 행렬에서 얻어진다. 이때 이진행렬에서 고립된 포인트를 결정하기 위하여 이동 윈도우(moving win- dow)에 있는 0이 아닌 포인트의 최소 수에 대해 경계를 설정하므로써 약 20×20 픽셀의 정사각형 이동 윈도우 행렬을 사용한다. 이때 고립된 포인트들은 제거된다. B(1:n, 1:n)에서 변환된 고립 포인트 없는 행



(a) 최초 영상

(b) 웨이블릿 변환

(c) 최종영상

그림 6 동일 의료영상의 웨이블릿 변환

렬인 B'(1:n, 1:n)에서 탐지된 텍스트 부분을 갖는 Mask(1:n, 1:n)를 형성하기 위하여 남아 있는 포인트를 그룹지운다. 마지막으로 Mask (1:n, 1:n)를 2n×2n으로 다시 스케일하고 최종영상을 얻기 위하여 이것을 최초영상에 적용한다. 그림 6은 최초 영상에 도베치스 웨이블릿 변환을 수행하여 후행처리한 최종 영상을 보인다[7, 8]. TIDE 시스템의 제약점으로는 민감한 텍스트 정보 부분의 위치를 정확히 알 수 없다면 의료영상 전체를 사용해야 하는 것이다.

4. 결 론

의료정보는 선택적으로 보호될 필요성이 있다. 오늘날 각종 의료 기관에서 환자의 프라이버시 보호는 권고되고 있지만 실제로 무시되며 많은 상황이 위험에 노출되어 있다. 본 논문에서는 의료정보의 보안을 위한 TIHI 시스템과 TIDE 시스템을 설명하였다. TIHI 시스템은 의료기관의 데이타를 안전하게 관리할 수 있는 해결책을 제공한다. 사용자 질의어를 엄격히 파싱하고 결과를 필터링하므로써 보안 중재자는 기본적인 데이타 조직과 기억장치에서 발견되는 보안의 헛점을 극복할 수 있게 한다. 또한 TIDE 시스템은 환자 이름 혹은 환자 확인 번호같은 환자의 사생활 정보에 관련된 텍스트를 보호하기 위하여 웨이블릿을 사용하여 디지탈 의료 영상내에서 텍스트의 정보에 대한 부분을 탐지하고 제거하였다. 오늘날 컴퓨터가 의료 분야에서 필수적이며 광범위하게 응용되고 있는 만큼 환자의 의료정보에 대한 보안의 중요성을 깊이 인식해야 한다.

참고문헌

[1] Derek Enlander, *Computers in Medicine an Introduction*, C.V. Mosley Company, 1980.

[2] Qian XioaLei, Gio Wiederhold, Michel Bilello, Andrea Chavez, and Vatsala Sarathy, "Trusted Interoperation of Healthcare Information(TIHI)", Stan- ford, 6 February 1996, abstract for the NSF challenge Workshop March pp. 20-23, 1996.

[3] Gio Wiederhold, Michel Bilello, Sarathy Vatsala, Qian XioaLei, "A Security Mediator of Health Care Information", In Proceedings of the American Medical Informatics Association Annual Fall Symposium, Octorber 1996.

[4] Gio Wiederhold, Michel Bilello, Sarathy Vatsala, Qian XioaLei, "Protec- tiong Collaboration", National Inform- ation System Security Conference, 21 October 1996; as Proceedings of the NISSC '96, Baltimore MD, pp. 561-569, Octber 1996.

[5] Gio Wiederhold, Michel Bilello, and Chris Donahue, "Web Implementation of a Security Mediator for Medical Databases", in T.Y. Lin and Shelly Qian: Database Security XI, status and Prospects, IFIP/Chapman&Hall, pp. 60-72, 1998.

[6] James Ze Wang, Gio Wiederhold, "System for Efficient and Secure Distribution of Medical Images on the Internet", In Proceedings of the 1998 American Medical Informatics Association (AMIA'98) Annual Fall Symposium, Orlando, Florida, Novem- ber, 1998.

[7] James Ze Wang, Gio Wiederhold, Jia Li, "Wavelet-based Progressive Transmission and Security Filtering for Medical Image Distribution", Advances in Biomedical Image Databases, S. Wong (Ed.), to appear, 1998.

[8] James Ze Wang, Michel Bilello, Gio Wiederhold, "Texual Information Detection and Elimination System for Secure Medical Image Distribution", In Proceedings of the 1997 American Medical Informatics Association(AM IA'97) Annual Fall Symposium, Nashville, Tennessee, October, 1997.

정 현 철

1987 조선대학교 자연과학대학 계산통계학과 학사
1990 중앙대학교 대학원 전산학과 석사
1991~1997 전남대학교 전산학과, 조선대학교 전산통계학과 시간강사
1997 전남대학교 대학원 전산학과 박사
1998~현재 광주보건대 의공학과 교수

관심분야 : 의료정보학, 데이타베이스 보안, 의료영상 처리, 이미지 보안, 실시간 처리
E-mail:hcjeong@www.kjhc-c.ac.kr

● ISAAC '98 ●

- 일 자 : 1998년 12월 14일(월)~16일(수)
- 장 소 : 대전 리베라호텔
- 주 최 : 컴퓨터이론연구회
- 문 의 처 : 한국과학기술원 전산학과 신찬수
  Tel. 042-869-3553 Fax. 042-869-3510
  E-mail : isaac98@jupiter.kaist.ac.kr

● 제6회 영남지부 학술논문발표회 ●

- 일 자 : 1998년 12월 18일(금)
- 장 소 : 포항공과대학교
- 주 최 : 영남지부
- 문 의 처 : 울산대학교 컴퓨터정보통신공학부 고재진 교수
  Tel. 052-259-2216