

모바일 원격의료 클라우드 환경에서 QRcode를 이용한 사용자 검증 시스템 연구

김영혁*, 임일권*, 이준우*, 이계귀*, 이재광*
*한남대학교 컴퓨터공학과
e-mail:yhkim@netwk.hannam.ac.kr

User Verification System using QRcode in Mobile Telemedicine Cloud Environment

Young-Hyuk Kim*, Il-Kwon Lim*, Jun-Woo Lee*, LiQiGui*, Jae-Kwang Lee*
*Dept of Computer Engineering, Han-Nam University

요 약

Smart Society로 나아가는 핵심으로 손꼽히는 모바일의 급속한 확산은 교육, 교통, 경제뿐만 아니라 건강에도 큰 영향을 미치고 있다. 그동안 발전이 미진했던 u-Health 기술 및 시장 역시 모바일로 인해 새로운 서비스 모델을 제시함으로써 발전하고 있다. 본 논문은 제안하는 시스템은 u-Health 서비스 중 sensor를 이용하여 원격지 환자의 생체정보를 수집하고, 실시간으로 병원의 클라우드 서버에 전송하는 시스템에서 사용자 검증에 대하여 연구하였다. 여기서 사용자란 클라우드 서버에 접속하는 의사를 말하며, 환자의 생체정보를 보기 위하여 시스템 접속함에 있어 공인인증서나 기타 인증 시스템과 비교해 간편하고, 네트워크 트래픽이 적은 사용자 검증 시스템을 목표로 한다. 그리하여 QRcode를 3개 생성하고, 각 클라우드 서버에 분산 분배 후 서로 섞음으로써 기존의 QRcode와 전혀 다른 인증용 QRcode를 생성할 수 있었다. 이것을 3차원 인덱스를 통해 원본 사용자 QRcode와 대조함으로써 사용자 검증 과정을 수행시킴으로써 절차를 간소화하고 네트워크 트래픽을 약 15% 감소시킬 수 있었다.

1. 서론

u-Health 서비스는 사후 치료에서 사전 예방 및 관리 중심의 의료서비스 패러다임을 가져왔으며, 특히 만성질환자, 고령자, 고위험군 및 일반인의 신체 가까이 휴대 단말기를 두어 장착된 센서를 통해 생체정보를 측정해 원격지에 있는 병원의 서버에 전송을 하고, 의료진은 서버에 접속함으로써 모바일로 환자의 상태를 ‘언제, ‘어디서나’ 살펴 볼 수 있게 하는 실시간 원격 환자 모니터링 시스템이 전 세계적으로 많은 연구가 진행되고 있다.[1-3]

u-Health 원격의료 서비스란 예방, 진단, 치료, 사후 관리 등에 대한 의료 서비스를 원격지에서 관리/감독할 수 있도록 제공하는 것이다. 자세히는, 유/무선 측정 장치로부터 수집된 생체 정보(체중, 혈당, 운동량, 심전도, 호흡, 체온, 콜레스테롤, 산소포화도 등)를 유/무선 네트워크(3G/WiFi/WiBro 등)를 통해 원격지에 있는 건강 관리사나, 주치의에게 원격으로 건강관리 및 의료 서비스를 제공할 수 있도록 하는 것이다. 이러한 u-Health 모니터링 서비스를 위해서는 크게 4가지의 기술의 융합이 필요하다. 이는 각종 건강 기기로부터 생체정보를 센싱 하는 센싱 기술, 센싱된 정보를 취합하여 유/무선 통신을 통해 전송하는 취합 및 전송 기술, 수집된 개인 생체 정보를 분석하는 분석 기술, 마지막으로 이를 분석하여 건강 상태의 변화를 사용자에게 알려주는 피드백 기술이다[4].

본 논문에서 최종적으로 목표로 하는 시스템은 원격지 환자의 생체정보가 최종 수신기관인 의료기관의 클라우드 서버에 저장되고, 의료진이 스마트 모바일 기기를 이용해 ‘언제, 어디서나’ 환자의 상태를 확인하는 시스템이다. 클라우드 컴퓨팅, 모바일 클라우드 컴퓨팅은 IT 자산을 타 사용자와 공유함으로써 얻은 효율성 증대와 그로 인한 비용절감의 장점은 있지만 자산이라 할 수 있는 데이터를 타 사용자와 공유함으로써 데이터의 무결성 및 서버의 인증 문제가 발생할 수 있다[3]. 모바일 클라우드 컴퓨팅 환경에서는 사용자가 필요한 자원의 일부 또는 전부를 서버로부터 직접 공급받기 위해서 서버는 모바일 클라우드 서비스의 인증 시스템을 활용하고 있으며, 모바일 클라우드 컴퓨팅 환경에서 서버가 다수의 클라이언트를 인증하기 위해서는 수천 비트의 상태 비트 정보가 필요하다. 여기서 상태 비트 정보란 서버에서 동일한 클라이언트까지 가는 여러 경로 중 연결되어있는 링크(인터페이스)의 상태변화 정보를 의미한다. 이러한 수천 비트의 상태 비트 정보는 중앙 검증자에 의해 중앙의 권한으로부터 검색되어야하며 검색 과정은 높은 네트워크 대역폭과 지연 그리고 네트워크 혼잡을 야기한다[4].

그리하여 환자에게 특별한 처방과 지시를 하는 것이 아닌 단순히 기준 수치 값과 비교해 상태등급(위험/주시/주의/일반) 정보를 요청하는 수준의 간단한 정보 제공에 대

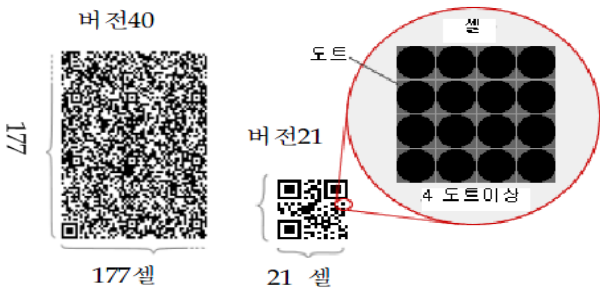
해서는 사용자적 입장에서 인증의 절차나 검증이 간편하고, 네트워크 트래픽 발생을 최소화시키기 위하여 QRcode를 이용한 사용자 검증 시스템을 제안한다. 2장에서는 QRcode의 기술 분석과 관련 연구를 살펴보고, 3장에서는 시스템을 설계한다. 4장에서 구현을 통해 공인인증서 방식과 네트워크 트래픽 발생량 부분에서만 비교함으로써 5장에서 결론과 향후 연구를 정의하여 마무리한다.

2. 관련 연구

2.1 QRcode

2D코드는 막대형태 이미지보다는 집합적 점이나 모자이크의 흑백 이미지로, 컬러코드를 포함하여 2D이미지코드로 총칭하는 것이 더 적합할지 모른다. 2D이미지코드 형태는 아스텍 코드, 데이터매트릭스 코드, 맥시코드, PDF-417 코드, QRcode, 트릴코드, 킥 마크, 슛 코드, 엠코드, 비 태그, 마이크로소프트 태그, 스노우 플레이크 코드 등으로 다양하다. 이러한 2D이미지코드는 발전초기 1D바코드의 다중 적합형태에서 2D의 적층형 구조 및 매트릭스 형태로 발전하여 일본에서는 QRcode가 미국에서는 PDF 417, 데이터매트릭스, 맥시코드 등이 대표적인 코드가 되었다[5].

QRcode란 1차원 코드인 바코드가 가지는 정보 저장 및 표현의 한계를 극복하기 위해 발전된 2차원 코드로서, 일본의 Denso Wave에 의해서 개발되었으며 대중적인 사용을 위해 특허권을 행사하지 않겠다고 선언하고 1994년에 배포되었다. QR은 Quick Response의 약자로, matrix 형태의 바코드이고 특징으로는 빠른 디코딩이 가능하며, 기존 사용되어지던 바코드에 비해 대용량, 많은 기록, 고밀도, Reed-Solomon 오류정정(8bits/codewords) 방식을 사용하고 있다. 그리하여 모바일 환경에서 빠른 인식과 데이터처리가 가능한 장점으로 최근 QRcode를 적용한 관련 서비스들이 활성화되고 있는 상황이다.



(그림 1) QRcode 구조

QRcode는 (그림 1)과 같이 작은 사각형 내의 x, y 방향으로 점자, 또는 모자이크식의 형태로 표현한 코드이며 360도 방향에서 인식된다. 기존 1차원 바코드보다 고밀도의 대량정보의 저장이 가능하고 데이터베이스 없이 그 자체로 해당정보 파악이 가능하다.

QRcode 자체에 문자, 숫자 등 텍스트는 물론, 그래픽, 사진, 음성, 지문, 서명 등 다양한 형태의 정보를 저장 할

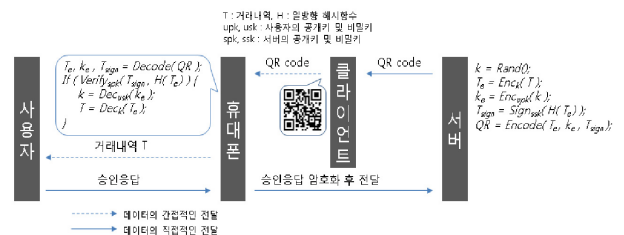
수 있어 인식하면 그 내용이 바로 디스플레이 된다. 서버나 DB와의 비 연동 데이터 파일이나 연결이 가능하여 정보저장매체로서의 이용도 가능하다. QRcode는 정보 훼손시의 복구 및 보안 인증기능으로 암호화가 가능해 신용기반 카드 등 각종 금융인증 및 지불 시스템으로도 활용가능하다. 또한 표준화된 기술로 코드인쇄 및 태그생성 비용이 저렴하고 확장성이 용이한 기술이다. QRcode의 크기는 데이터양, 문자 종류, 오류복원 수준에 따라 적용버전(코드크기)을 결정하고, 프린터나 스캐너의 해상도에 따라 셀을 설정 확정한다. 버전은 1 ~ 40으로 구성되어 있으며 각 버전마다 셀의 수가 정해져 있다. 셀은 QRcode를 구성하는 사각형의 점이다. 버전 1의 가로세로 (21개×21)개 셀로 시작하여 버전 증가 시 마다 4개 셀씩 늘어 버전40에는 (177×177)개 셀로 설정되어있다[6].

<표 1> 종류별 2차원 코드 비교 분석

	QR Code	PDF417	DataMatrix	MaxiCode
개발 (국가)	덴소웨이브 (Jap)	Symbol (USA)	CI Matrix (USA)	UPS (USA)
방식	Matrix	스콧쿠도 바코드	Matrix	Matrix
번호	7,089	2,710	3,116	138
숫자	4,296	1,850	2,355	93
이진	2,953	1,018	1,556	-
한자	1,817	554	778	-
주요 기능	대용량 공간 절약형 고속읽기	대용량	공간 절약형	고속읽기
주요 용도	전체분야	OA	FA	물류
규격화	AIM International JIS ISO	AIM Internation ISO	AIM Internation ISO	AIM Internation ISO

2.2 QRcode 활용 연구

1) 전자금융거래에서 QRcode를 활용한 승인방법



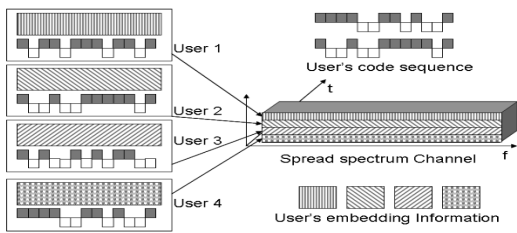
(그림 2) QRcode를 이용한 전자금융거래 승인방법

이 논문에서 제안하는 승인방법은 (그림 2)와 같이 휴대폰과 QRcode를 활용한 승인방법으로 QRcode에 표현될 데

이터는 거래내역(이체금액, 수신자, 은행명, 수신자 계좌번호, 수신사명 등)을 사용자 공인인증서의 공개키로 암호화하여 사용자에게 전달하는 것이다. 이와 같은 효과는 사람이 이미지를 인식하는 능력이 문자열을 인식하는 것보다 더 뛰어나기 때문이며, 그리하여 QRcode를 활용하고 있다.[7]

2) 2차원 바코드를 이용한 오디오 워터마킹 알고리즘

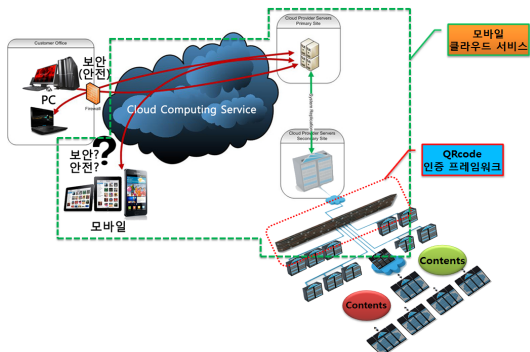
과거 데스크탑형 사용자 환경에서는 저작물을 보호하기 위해서 디지털 저작권 관리(DRM : Digital Rights Management) 기술과 같이 복잡한 암호·복호화 기술을 이용하여 보호하였으나 사용자 환경의 변화와 DRM 기술에 의한 호환성 문제로 DRM free 서비스로 전환되고 있다. 이러한 변화에 맞춰 최근에는 DRM을 대체할 수 있는 저작권보호 기술에 대한 관심이 높아지고 있다. DRM을 대체할 수 있는 기술로써는 디지털 워터마킹 기술과 디지털 핑거프린팅 기술을 들 수 있다. 디지털 워터마킹 기술은 저작권의 보호, 인증 및 권리를 검증할 수 있는 기술이며, 디지털 핑거프린팅 기술은 저작물의 불법유통 경로를 추적할 수 있는 기술로써 디지털 워터마킹 기술의 응용 기술이라 할 수 있다.



(그림 3) 워터마킹 알고리즘

이 논문에서는 두 가지 새로운 접근 방법을 동시에 적용하여 오디오 워터마킹 알고리즘(그림 3)을 개발하였다. 그 중 하나는 2차원 바코드를 삽입정보로 표현하여 바코드가 갖고 있는 코드자체의 에러 보정 능력을 이용하여 알고리즘의 견고성을 높였고, 다른 하나는 CDMA(Code Division Multiple Access)의 Chip Sequence 원리를 도입하여 각종 공격에 대한 대응 알고리즘을 구성하였다[8].

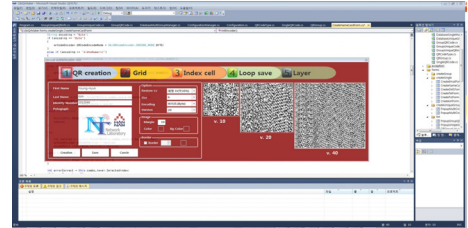
3. QRcode 사용자 검증 시스템 설계 및 구현



(그림 4) QRcode 사용자 검증 시스템 역할

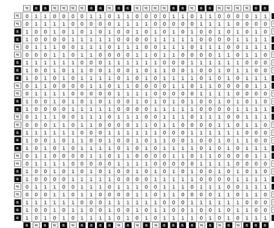
전체 모바일 클라우드 환경에서 본 QRcode 사용자 검증 시스템이 동작하는 부분은 (그림 4)에서 보이는 것과 같이 서비스를 제공해야 할 콘텐츠 서버 앞단에서 이루어지게 된다.

3.1 QRcode 생성 및 격자분할



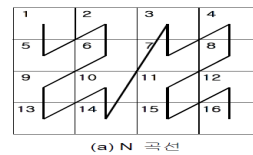
(그림 5) QRcode 생성 및 분할

QRcode를 통해 사용자 검증을 받기 위해서 먼저 본인의 사진과 고유ID, 소속부서명으로 3가지 버전(10, 20, 40)의 QRcode를 생성해낸다. (그림 5)와 같이 생성된 3가지의 QRcode는 흑/백 기준값(50%)에 의해 1/0 값으로 변환된다. 이렇게 변환된 바이너리 데이터를 4x4 배열로 구분하여 (그림 6)과 같이 격자화를 시키게 된다.

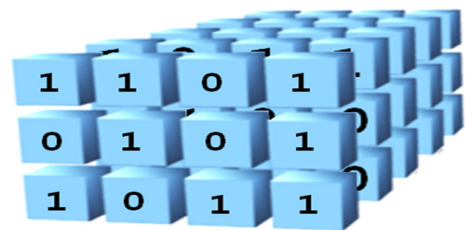


(그림 6) 격자화

3.2 3차원 Layer화 및 3차원 Index 생성



(그림 7) N-순서화 기법

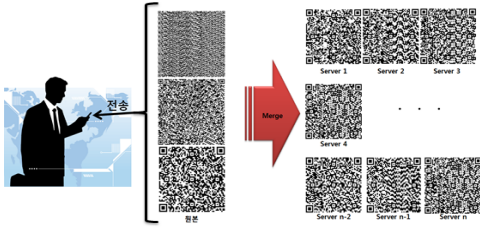


(그림 8) Z-Order를 활용한 3차원 Layer화

N-순서화 기법을 이용해 4x4 배열의 데이터를 1차적으로 섞고, 2차적으로 1차원 나열된 데이터들을 정방형태로 다시 재배열을 Z-order를 통해 한다. 3차원 정사각형으로 구성된 바이너리 데이터들은 (그림 8)과 같은 형태

를 가지며, 이렇게 3차원의 공간 값을 가지게 되는 QRcode의 각각의 요소 값들에 3차원 기준점 Index를 생성시켜 데이터베이스에 저장하게 된다.

3.3 QRcode 사용자 검증 방법



(그림 9) 사용자-서버 간 QRcode 검증

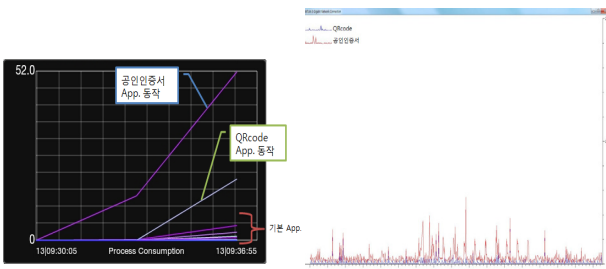
각 클라우드의 분산 서버들은 서로 다른 형태로 조합된 QRcode를 보유하고 있고, 사용자는 원본 QRcode를 보유하게 된다. 그리하여 사용자가 서버에 인증 요청시 해당 요청 서버 각각마다 보유한 QRcode를 통해 사용자를 확인/검증하게 된다.

4. 실험

실험은 안드로이드 OS 환경에서 QRcode 인증 시스템과 공인인증서 인증을 번갈아 하면서 발생한 네트워크 트래픽과 스마트폰 기기의 배터리 소모율을 측정하였다. 실험환경은 <표 2>와 같다.

<표 2> 종류별 2차원 코드 비교 분석

Server	SmartPhone	S/W
CPU: Intel Core2 Quad Q8400	CPU: 1.2GHz	CPU & RAM: Process Monitor
RAM: 4GB	RAM: 1GB	Network Traffic Android Traffic Grapher
Ethernet: 100Mbps	HSPA+ 21Mbps	Wireshark
OS: CDH CentOS	OS: Android 2.3	
DB: MySQL 5.1.41	-	-



(그림 10) CPU 사용량 비교 (그림 11) 네트워크 사용량

총 패킷 1,397 중 공인인증서의 접속부터 인증 완료 결과 값인 생체정보 표출까지 729, QRcode가 551, 나머지 117은 (그림 10)의 기본적으로 동작하는 App.들이 소모한 것으로 추정된다. 전체적으로 QRcode의 네트워크를 통한 사용자 검증시 전송되는 패킷의 크기가 작음을 알 수 있었다.

5. 결론

본 논문에서는 원격으로 환자의 생체정보를 클라우드 환경으로 구성되어진 원격의료기관의 서버에 수집/저장하고 활용하는 시스템의 사용자 검증 방법에 대한 연구를 진행하였다. 여기서 사용자란 원격지 환자의 정확한 생체정보 수치 값이 아닌 기준 수치 값과 비교해 상태등급(위험/주시/주의/일반) 정보를 요청하는 자를 의미하며, 이와 같은 정보를 요청시 사용자의 권한 검증, 사용자 본인 검증과 같은 수단으로 QRcode를 인증 수단으로 쓰는 방법에 대하여 제안하였다.

장점은 일반적인 인증 수단인 ID/비밀번호, 공인인증서 등의 수단 외에 인증이 이루어질 수 있는 시스템 모델을 제시하였다는 것과 공인인증서 방식과 비교했을 때 네트워크 트래픽의 사용량이 감소되었다는 것이다. 또한, 사용자는 원본의 QRcode의 보관만 주의하면 간편하게 인증이 가능해지지만, QRcode의 외부 유출시에 대한 대비가 현재의 논문에서는 제시되고 있지 않기 때문에 추후에는 반드시 사용자가 보관하는 원본 QRcode에 대한 보호 수단이 제시되어야만 한다.

"이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0013029)"

참고문헌

- [1] A. Lympers and A. Dittmar, "Advanced Wearable Health Systems and Applications, Research and Development Efforts in the European Union," IEEE Eng. Med. Biol. Mag., Vol.26, No.3, pp.29-33, May/June, 2007.
- [2] Y. Hao and R. Foster, "Wireless Body Sensor Networks for Health Monitoring Applications," Phys. Meas., Vol.29, pp.R27.R56, Nov., 2008.
- [3] V. Shnauder et al., "Sensor Networks for Medical Care," Harvard Univ. tech. rep. TR-08-05, Apr., 2005.
- [4] 천승만, 나재욱, 박종태, "M2M을 위한 U-헬스케어 응용 서비스 기반 IEEE 11073/HL7 변환 게이트웨이 설계 및 구현", 한국통신학회논문지, 제36권, 제3호, 2011.03.
- [5] 박종만, 박종규, "휴대전화의 2D 이미지코드 인식 기술동향", 한국통신학회논문지, 제36권, 제6호, 2011.06.
- [6] <http://www.qrcode.com/ko/images/QRcode.pdf>
- [7] 맹영재, 신동오, 김성호, 양대현, "전자금융거래에서의 문서변조 취약점 분석 및 대응방법 고찰", 한국정보보호학회지, 제20권, 제6호, 2010.12.
- [8] 배경율, "2차원 바코드를 이용한 오디오 워터마킹 알고리즘", 한국지능정보시스템학회 지능정보연구, 제17권, 제2호, 2011.06.