http://dx.doi.org/10.14400/JDC.2014.12.6.317

지문인식기술과 암호화된 QR코드를 이용한 안전한 신분증 연구

송충건, 이근호
백석대학교 정보통신학부

A Study on Safe Identification Card Using Fingerprint Recognition and Encrypted QR

Chung-Geon Song, Keun-Ho Lee
Dept. of Information and Commnunication, Beakseok University

요 약 현재 국내에서 국민들을 식별하기 위해 사용되는 주민등록증은 지문정보를 구체적으로 표시하고 있어 도난 당할 시 이를 활용한 2차 피해를 초례할 수 있다. 이러한 문제점을 해결하기 위해서는 식별정보에 기밀성을 유지하면서 비용측면의 만족해야하며, 현재 국가가 보유하고 있는 지문 DB를 활용할 수 있는 형태의 신분증이 요구되고 이다. 이러한 시점에서 암호화된 QR코드와 지문정보를 활용한 안전한 신분증 형태를 제안하고자 한다.

주제어 : 전자신분증, 지문정보, 바이오메트릭스, QR 코드

Abstract The registration cards that are currently used to identify the people of Korea may cause secondary damage once stolen because they contain very specifically expressed fingerprint information. In order to solve this problem, in ID is required that can utilize the state-owned fingerprint DB, while while maintaining confidentiality of the identification information and satisfying the cost as well. At this point accordingly, a secure form of ID, which uses the encrypted QR code and fingerprint information, is proposed.

Key Words : e-ID, Finger Print, Biometric, QR Code

1. 서론

국내에서 국민들을 식별하기 위해 사용되는 주민등록증은 카드 외부에 여러 가지 개인정보가 구체적으로 명시되어 있어 다양한 사회적 문제를 야기한다[1][2]. 대표적으로 신분증을 불법으로 위조하여 타인의 신분으로 위장하고 악의적인 행위를 하는 경우가 있다. 이는 범죄자에게 익명성을 보장할 뿐 아니라 변조 대상이 된 무고한 사람에게 피해가 갈 수 있어 빠른 시일 내에 해결되어야 하는 시급한 사안으로 여겨지고 있다.

또한 다양한 산업에서 신분증을 통해 신원확인을 수행할 시 단순히 카드의 표면에 명시된 개인정보를 기준으로 인증을 수행한다. 이러한 개인정보는 공중망을 통해 이동하는 주민등록증의 사본을 이용하여 수집할 수 있을 뿐 아니라 최근 늘어나고 있는 대형 웹사이트에서 발생하는 개인정보 유출사고를 통해 제 3자가 개인정보

Received 14 April 2014, Revised 20 May 2014
Accepted 20 June 2014
Corresponding Author: Keun-Ho Lee(Division of Information and Commnunication, Beakseok University)
Email: root1004@bu.ac.kr

ISSN: 1738-1916

를 소유할 수 있는 원인을 제공하고 있다.

이러한 문제를 해결하기 위해 최근에는 지문인식 기술을 이용하여 신원확인 수단으로 활용하는 신분증 진위확인 솔루션이 개발되어 보급되고 있다[3]. 지문은 그 사람의 신체적 특징을 인증의 수단으로 활용하는 생체인증 기술 중 가장 보편화 된 기술이다[4]. 이러한 지문인식은 가치가 높은 정보나 장소에 대한 접근제어를 수행할 시 많이 활용되고 있다. 또한 대학민국 정부에서 신분증 제작 시 국민 개개인의 지문정보를 수집하여 보관하고 있어 신뢰도 있는 신용평가기관에서 지문정보를 기준으로 신원을 확인해 주는 서비스도 개발되어 보급되고 있다.

또한 지문정보는 ID/PW를 대체하는 편리한 사용자 인증수단으로 여겨지며 차세대 인증기술로 각광 받고 있다. 최근 스마트폰과 같은 다양한 디바이스에 하드웨어적으로 지문인식 센서가 내장되어 지문인식에 대한 수요가 점차 늘어날 것으로 예상된다.

그러나 신분증에 명시된 지문정보는 이진화 단계의 이미지로 인증의 목적에 활용될 수 있을 만큼 정교한 데이터를 제공한다. 지문정보가 유출될 경우 지문의 특징을 인증수단으로 활용하는 인증 시스템의 인증키가 유출된 것과 같은 상황이 된다.

또한 인증에 활용되는 생체정보는 인간의 고유한 특징으로 한평생 변하지 않는 특징을 가지고 있다. 이와 같은 특징을 가진 생체정보가 마스터키로 활용될 경우 이는 그 사람의 권한을 제거하지 않는 이상 평생 마스터 권한을 타인과 공유하는 결과를 초례할 수 있는 문제점을 가지고 있다.

위와 같은 주민등록증의 지문인식의 단점을 IC칩에 내장된 디지털서명 기술로 대체할 경우 마스터키를 변경할 수 있어 부분적인 문제를 해결할 수 있지만 비용의 이슈가 발생하고 현재 국가가 보유하고 있는 국민 지문 데이터의 활용가치가 사라진다.

이러한 배경에서 플라스틱 카드에 원본을 유추할 수 없는 알고리즘을 통해 처리된 지문정보를 넣어 지문인식의 장점을 살리고 2차원적으로 출력이 가능한 암호화된 QR코드를 활용하여 전 국민을 대상으로 하는 신분증을 제안하고자 한다.

2. 관련연구

2.1 신분증 인증키 보관유형

신분증이란 본인의 신원을 확인하는 수단으로 다양한 형태로 발전되어 왔다. 신분증은 신원을 확인을 위한 그 사람의 고유한 정보가 들어있으며 나라마다 신분증에서 보유하고 있는 방식이나 보유하고 있는 데이터의 종류가 다양하다. 현재 유럽에서 전자신분증을 도입하는 나라가 늘어나고 있으며[5] 국내에서는 2008년 안행부에서 전자주민등록증 도입 추진방안을 발표하여 도입 방향을 제시하였다[6]. 신분증의 데이터 보관형태는 다음과 같이 이차평면 출력 형태와 e-ID 형태가 있다.

2.1.1 이차평면 출력

이차평면 출력형태는 고적적인 신분증 형태로 카드에 출력된 개인정보를 이용하여 신원확인을 수행한다. 카드의 규격은 ISO/IEC 7810 방식을 따르며 출력되는 데이터는 ID카드의 목적에 따라 결정된다. 현재 주민등록증의 경우 성명, 사진, 주소, 발행일, 주민등록기관 등이 표시된다[1].

2.1.1 E-ID

E-ID는 전자적인 형태로 신원확인 데이터를 저장하는 신분증을 말한다. E-ID에서 개인을 식별하는 기준은 스마트카드에 저장된 데이터이며 이러한 데이터의 안전성을 위해서는 강도 높은 암호기술을 요구된다[7]. 또한 범국가적인 신분증을 만들시 비용적인 측면이 고려되고 작은 크기에 암호강도가 높은 HEIGHT나 ECC와 같은 경량암호 알고리즘이 요구된다.

2.2 QR 코드

QR 코드는 1994년 일본의 덴소웨이브사에서 개발된 2차원 정보 마킹기법이다. QR 코드의 국제표준으로는 2000년 6월 채택된 ISO/IEC18004이 있다. 이를 시점으로 전 세계 다양한 분야에서 활용되기 시작하였다. QR코드의 다양한 출력 형태는 <Table 1>과 같다[8].

〈Table 1〉 QR Code type

QR Code type	Image	Feature
QR Code Model 1 Model 2	Model 1  Model 2 	Model1 is the type made at the initial stage of QR code, and Model 2 is made by improving Model 1 so that a code can be recognized without problem even when the code is deformed. Now QR code Model2 is most widely used in general.
Micro QR Code		Position symbol is a QR code that enables printing possible in a small space.
iQR Code		It is a 2-dimensional code of matrix type that enables the formation of a square or a rectangle. It can take more data than any other QR codes.
SQRC		It is the QR code that has the function of recognition restriction. It can be used for the management of personal information or in-house information, but security is not assured.
LogoQ		LogoQ is the QR code in which visuality is enhanced by the insertion of letters or pictures into a QR code.

QR코드는 대용량의 정보를 2차 평면 형태의 출력물로 보관할 뿐만 아니라 뛰어난 복원력으로 전 세계 다양한 응용 분야에서 효용성을 인정받고 있다. <Table 2>는 다양한 속성의 QR코드가 가진 사양을 나타내고 있다[8].

〈Table 2〉 QR code specifications

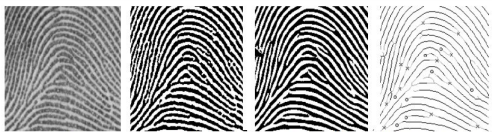
QR Code size	21×21 cell ~ 177×177 cell	
Type and amount of information	Number Alphanumeric 8bit byte English	Maximum of 7,089 characters Maximum of 4,296 characters Maximum of 2,953 characters Maximum of 1,817 characters
Error recovery	Level L Level M Level Q Level H	Approximately 7% Approximately 15% Approximately 25% Approximately 30%
Cord connection	Maximum of 16 split	

2.3 Encrypted QR

암호화된 QR은 암호기술이 적용된 QR코드를 말한다. QR코드는 SQRC(Security QR Code)를 통해서 개인정보나 사내정보를 보호할 수 있으나 보안의 강도가 약하여 전사적 공격에 쉽게 깨질 수 있다. 그러므로 중요한 정보자산을 QR코드에 넣을 시 암호기술이 적용된 데이터를 QR코드에 넣는 암호화된 QR 기술이 사용된다. 이를 통해 정보의 접근제어와 디지털 서명 기술이 증가하므로 사람이나 사물에 대한 인증이 가능하다[9].

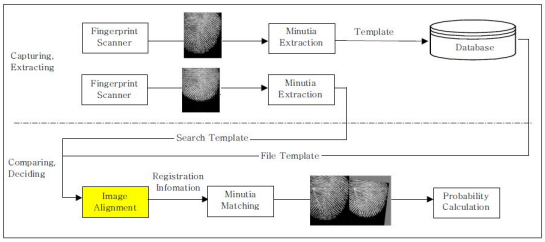
2.4 지문인식 시스템

지문인식을 생체인식 기술을 대표하는 기술로 가장 오래되고 가장 보편적으로 사용되는 사용자 인증기술이다. 이러한 지문인식 기술은 대한민국 주민등록증에도 활용되고 있다. 주민등록증에 출력되는 지문 이미지는 [Fig. 1]과 같이 다양한 형태의 변환 과정을 통해 특징점을 추출하게 된다. 현재 주민등록증에는 이진화가 수행된 지문이미지가 출력되어 있다[10].



[Fig. 1] Process of fingerprint data conversion

지문이미지는 위와 같은 변환과정을 거치고 [Fig. 2]과 같은 다양한 알고리즘을 통해 사용자 인증을 수행하게 된다[8]. 지문정보와 같은 Biometric 기술은 PKI에 활용될 암호화키를 생성할 수 있으며[11], 전자서명 기법도 연구된 바 있다[12].



[Fig. 2] Algorithms fingerprint authentication

3. 제안 신분증

3.1 제안 신분증의 구성요소

3.1.1 QR 생성기

QR 생성기는 영상캡처 장비를 통해 수집한 이진화 상태의 지문정보에서 특징점을 추출한다. 이러한 특징점은 알고리즘을 이용하여 지문의 원본 데이터를 유추할 수 없도록 변경한다. 이렇게 처리된 데이터를 최종적으로 암호화 후 QR코드로 만든다. QR 코드는 무료로 공개된 방식으로 자유롭게 QR 생성 알고리즘을 사용할 수 있다. 이러한 특징으로 인해 바코드에서 한 단계 발전한 차세대 마킹 기법으로 각광받고 있다. 제안 신분증에서의 핵심 구성요소로 QR를 생성한 시점에서 카드에 출력되어 Something you have적 인증 성격을 가지고 사용자에 의해 관리된다.

3.1.2 QR 리더기

QR 리더기는 2차 평면 출력 형태의 이미지를 읽어 디지털 데이터로 변환하는 기능을 수행한다. 최근 스마트폰 어플 형태의 보급으로 누구나 QR을 읽을 수 있어 마케팅 용도로 활성화되어 있다. 제안 신분증에서 카드에 명시된 QR을 읽어 암호문 상태의 QR을 신뢰도 있는 공공기간에 보내 인증을 요청하는 역할을 담당한다.

3.1.3 신용평가기관

신용평가기관은 실제 키관리 서버에 접근할 수 있는 권한을 가진 신뢰도 있는 기관을 말한다. 신용평가기관은 신원확인 신분증 인증요청을 받아 키관리 서버에 해당 키를 요청받고 키를 이용해 신원확인을 수행한다. 또한 요청받은 키를 QR 리더기 단말에 전송하여 결과를 알려준다. 이러한 신용평가기관은 공공기관이나 신용평가 전문 기업이 될 수 있다. 이러한 신용평가기관은 제안 신분증 인증구조에서 QR과 키관리 서버를 이어주는 다리 역할을 수행한다.

3.1.4 키관리 서버

키관리 서버는 암호화된 QR을 생성할 시 대칭키 암호화 함수에 사용된 키를 관리하는 서버로 신용평가기관의 요청에 복호화 키를 제공하는 기능을 가지고 있다. 신용평가기관과 키관리 서버 사이에 연결된 네트워크는 폐쇄망 형태로 구축하여 보안을 강화하도록 해야한다. 키관리 서버는 제인 인증구조에서 신용평가기관에 대한 인증을 PKI 인증을 수행하여 CA가 인증한 기관에 대해서만 복호화 키를 제공한다.

3.2 제안 신분증의 데이터 처리

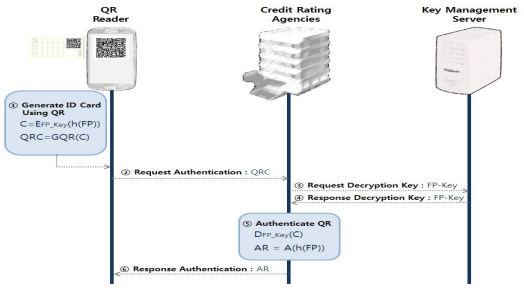
제안 신분증 구조에서는 2단계의 데이터 처리가 요구된다. 첫 번째 단계는 수집한 지문의 원본 데이터를 보호하기 위해 알고리즘을 통해 변형하는 과정이며 두 번째 단계는 지문정보에 대한 인증을 위해 디지털 서명을 수행하는 것이다.

3.3 제안 기법의 프로세스

〈Table 3〉 Matrix rules

Data rules	FP	Original prints
	FP-Key	Fingerprint encryption key
	QRC	QR Code fingerprint form
	C	Secure fingerprint
	AR	Authentication Result
Function rules	h()	One-way function
	E()	Encryption function
	D()	Decryption function
	GQR()	QR Code generating function
	A()	Authentication function

제안 신분증 구조에서 이루어지는 전체적인 프로세스를 설명하기 위해 요구되는 데이터의 유형에 기호를 부여하고 <Table 3>에 정리하였다. [Fig. 3] 에서는 인증이 이루어지는 단계를 크게 5단계로 나누고 시퀀스 다이어그램으로 가시화 하였다. [Fig. 3]의 구성요소는 크게 QR Reader, Credit Rating Agencies, Key Management Server로 나누어 명세하였으며, 데이터 들이 이동하는 네트워크에서 암호기술을 이용해 기밀성을 보장한다는 가정 하에 명세하였다.



[Fig. 3] Proposed ID authentication process

3.3.1 QR을 이용한 신분증 생성

가공된 지문이미지의 특징점을 암호화 한 데이터를 기반으로 QR코드를 생성한 후 주민등록증에 출력한다. 지문의 특징점을 추출할 경우 지문 원본을 추출할 수 없어야 한다.

3.3.2 신용평가기관에 인증 요청

인증을 요구하는 회사나 기관은 QR 리더기를 통해 QR을 리딩한 후 이 정보를 공공기관에 보낸다. 암호화된 QR코드를 읽을 수 있는 복호화키는 키관리 서버에서 관리되고 서버에 대한 접근은 신뢰도 있는 공공기관을 통에서 수행한다. 공공기관은 복호화키를 요구하는 리더기 소유자에 대한 관리가 가능하다.

3.3.3 키관리 서버에 복호화키 요청

신뢰도 있는 공공기관은 네트워크 망을 통해 키관리 서버에 복호화 키를 요청한다. 이 구간에서는 보안의 강화를 위해 스카다망 형태로 구성하는 것이 안전할 것이다.

3.3.4 신용평가기관에 복호화키 응답

공공기관은 키관리 서버에서 암호화된 QR을 복호화 할 수 있는 키를 부여받는다. 그 후 부여받은 복호화 수행 후 신원확인의 결과를 생성하게 된다.

3.3.5 복호화 수행 후 지문정보 인증수행

신용평가기관은 키관리 서버로부터 받은 복호화 키를 이용하여 암호화된 지문정보를 복호화할 수 있다. 그러므로 인증을 실제 수행하는 부분은 신용평가기관에서만 이루어질 수 있으며, 복호화된 지문정보를 보관하지 않는 것을 원칙으로 세부 사양이나 시스템을 설계하도록 한다.

3.3.6 QR 리더기에 인증결과 응답

사전에 키관리 서버와 통신을 하며 수행한 신원확인 결과를 인증을 요청한 기관에 응답하여 알려주는 최종 단계이다.

3.4 QR코드 복제방지

QR코드는 단순한 이차평면 형태의 이미지로 카메라나 스캐너로 복제가 용이한 단점을 가지고 있다. 이러한 단점을 해결하기 위해선 두 가지 방법을 활용할 수 있다. 첫 번째로 QR코드에 저장된 지문의 특징점과 현재 QR코드를 제출한 자의 지문을 실시간으로 비교하는 것이다. 이러한 방법은 확실한 복제방지를 이룰 수 있으나 사용자에게 지문인식을 요청해야하는 불편함을 요구하므로 상대적으로 중요한 신원확인 목적으로 활용한다. 다음으로 특정한 ID를 카드와 QR 내부에 저장하여 비교하는 것이다. 이는 리더기에 일시적으로 저장되는 과정에서 유출되는 사고를 막을 수 있다. 타인에게 QR코드가 넘어가도 동일한 ID가 출력된 카드가 없으면 신원이 확인되지 않는다. 그러나 물리적으로 카드를 탈취하여 ID를 복사할 경우는 예방할 수 없다. 그러므로 사용자의 불편함 없이 비교적 가벼운 신원확인에 활용할 수 있다.

또한 제안 신분증의 구조에서 인증을 위해서는 항상 키관리 서버에 대한 요청이 요구되기 때문에 요청에 대한 로그를 사용자가 확인할 수 있다. 만약 타인이 인증요청을 수행한 흔적인 발견된 경우 키를 변경하고 신용평가기관에서는 인증을 요청한 기관을 조사하여 불법 신원확인을 조사하고 차단할 수 있다.

4. 성능분석

본고에서 제안한 신분증은 지문인식이라는 바이오메트릭 기술과 암호화된 QR을 융합하여 다음과 같은 기능을 수행할 수 있으며 타 신분증 인증기법과의 비교되는 성능은 <Table 4>에 나타내었다. 성능분석은 미국의 개인신원검증 기준 FIPS 201-1 표준을 기준으로 구성하였다.

4.1 국민 지문정보 소유방지

현재 대한민국은 주민등록증 발급 시 개인의 양손에 엄지손가락 지문을 획득하도록 되어 있다. 현 시점에서 지문정보는 단순한 신원확인 용도로 활용되고 있지만 미래 다양한 정보와 장소에 대하여 주요한 접근제어 키로 이용될 경우 지문정보의 가치가 매우 상승할 것으로 예측된다. 그러므로 구체적인 지문정보를 저장하는 것을 매우 위험할 수 있다. 이러한 요구사항을 제안 신분증 구조가 만족시키며 정부가 국민을 철저하게 관리하는 빅브라더를 방지할 수 있다.

4.2 공중망을 통한 지문 데이터 유출방지

기존 신분증 사본을 인터넷으로 주고받는 경우 지문정보에 대한 구체적인 명시로 기밀성을 유지하기 힘들었다. 그러나 제안 신분증 구조로 제 3자에게 신분증 데이터가 들어가도 지문 정보를 획득하는 것이 불가능 하며 지문정보 처리 알고리즘을 기존 알고리즘과 다르게 수행하여 안전한 신분증을 재발급 받는 것이 가능하다.

4.3 지문원본 데이터에 기밀성 보호

지문정보는 인간의 고유한 특성으로 인증키로 활용할 경우 한평생 변하지 않는 단점으로 인해 원본을 유추할 수 없도록 변형하여 활용하고 있다. 제안 신분증 구조에서는 영상캡처 장비를 통해 얻은 지문의 원본을 특정 알고리즘으로 변형하여 지문의 원본 영상을 보호할 수 있다.

4.4 QR코드에 대한 무결성 검증

QR에 암호기술을 넣어 디지털 서명을 구현하여 개인의 신원을 확인하는 제안 시스템은 첫 단계로 Something you have 적 특징을 활용하고 있다. 이러한 특징은 키가 제 3자에게 유출될 경우 접근권한도 넘어가는 단점이 있어 유출여부를 활용할 수 있는 솔루션이 요구된다. 제안 신분증에서는 지문이라는 바이오메트릭스 기술을 접목해 심도 있는 보안이 요구되는 시점에서 실시간으로 지문인식을 수행하여 QR코드의 무결성을 검증할 수 있다.

〈Table 4〉 Comparison with other means of recognition

ID Authentication Scheme	Whether the key can be modified	Ease of key management	Key Security
E-ID	Possible	Bad	Average
Fingerprint	Impossible	Good	Average
Proposed Study	Possible	Good	Good

5. 결론

본 연구에서는 지문정보를 일방향 함수를 통해 원본 데이터를 보호하고 암호화 수행 후 복호화 키를 Key Management Server를 통해 관리하는 신분증 식별 데이터 관리 기법을 제안하였다. 따라서 공중망에서 이동하는 지문정보의 기밀성을 유지하며 다양한 개인정보 유출 위협으로 부 소중한 신체정보를 안전하게 보호할 수 있을 것이며, 제안 시스템을 통해 신뢰성과 편의성을 보장하는 차세대 신분증 도입에 기여할 것으로 기대한다.

REFERENCES

[1] Ministry of security and public administration, Promotion plan of Introduction of E-ID card

[2] S. K. Kim, A Constitutional Study on the Problems of the Current National ID Card and the Introduction of an Electronic ID Card, Public Law Journal, Vol. 12, Mo. 2, pp.105-131, 2011.

[3] Secret royal inspector: http://www.mapae.co.kr/

[4] A. Jain, R. Bolle, S. Pankanti, Biometrics-Personal Identification in Networked Society, Kluwer Academic Press, 1999.

[5] Ministry of security and public administration, Status of the introduction of OECD countries.

[6] G. B. Gwon, Legal Review of Scheme for e-ID Card, construction method Journal, Vol. 39, No. 2, pp.341-368, 2010.

[7] J. M. Cho, J. S. Hun, H. S. Jo, Status and Considerations of E-ID, KIISC, Vol. 21, No. 4, pp.32-39, 2011.

[8] QR Code: http://www.denso-wave.com/qrcode/

[9] Encrypted QR: http://qrworld.wordpress.com/

[10] S. B. Pan, J. H. Moon, Y. W. Chung, H. I. Kim, Technology trends of the fingerprint recognition, Electronics and Telecommunications Trends, Vol. 16, No 5, pp 46-54, 2001.

[11] H. W. Lee, S. H. Yun, K. Y. Moon, Y. S. Chung, Bio information based electronic signature and method of generating a digital key, KOCON, Vol. 5, No. 9, PP. 33-44, 2007.

[12] Peter Orvos, Biometric generation of digital keys, Mini Symposium, DMIS-BUTE, 2001.

송 충 건(Song, Chung Geon)

・2010년 3월 ~ 현재 : 백석대학교 정보통신학부(이학사)
・관심분야 : IoT, U-Healthcare, 개인정보 보호, 보안 컨설팅
・E-Mail : security0730@naver.com

이 근 호 (Lee, Keun Ho)

・2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
・2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
・2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
・관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
・E-Mail : root1004@bu.ac.kr