논문 2007-44CI-6-1

휴대폰 환경에서 얼굴 및 홍채 정보를 이용한 암호화키 생성에 관한 연구

(A Study on Releasing Cryptographic Key by Using Face and Iris Information on mobile phones)

한 송 이*, 박 강 령**, 박 소 영**

(Song-yi Han, Kang Ryoung Park, and So-young Park)

요 약

최근 하나의 휴대폰에 여러 가지 미디어들이 복합적으로 장착됨에 따라 휴대폰에서 제공되는 서비스의 사용자 보안에 대한 요구가 증가되고 있다. 현재 이를 위하여 비밀번호와 인증과정을 통한 암호화 카드를 이용하여 본인을 인증한 후에 서비스를 제공할 수 있는 암호화키를 생성하고 있지만 이는 분실의 위험에 언제든지 노출되어 있다. 따라서 상대적으로 분실의 위험이 거의 존재하지 않는 생체정보를 이용하여 키를 생성하는 연구가 많이 진행되고 있다. 하지만 생체정보는 언제나 동일한 키를 생성해내야 하는 암호화키 생성 시스템의 요구사항과 달리 환경의 변화에 따라 본인이라도 특징 추출시마다 약간씩 다른 특징값이 추출되는 문제점을 가지고 있다. 따라서 본 연구에서는 생체 특징으로부터 직접적으로 키를 생성해내는 생체 정보 기반 키 생성 방법(Biometric-based key generation)이 아닌 생체 정보 매칭 기반 키 생성 방법(Biometric matching-based key release)을 이용하여 미리 정의해 놓은 키를 인식과정을 통하여 도출하고 또한 하나의 생체가 갖는 성능의 불안정성을 극복하기 위하여 얼굴과 홍채를 결정 레벨(Decision Level) 에서 결합함으로써 모바일 환경의 특성을 반영하며 안정된 성능 하에 암호화키가 생성될 수 있도록 하였다. 또한 휴대폰에 내장되어 있는 메가 픽셀 카메라를 이용함으로써 한 번의 영상 취득으로 얼굴과 홍채 인식이 동시에 이루어지는 편리함을 제공하였다. 본 논문에서 제안하는 키 생성 방법의 성능을 측정한 결과, 암호화키 생성에 있어 0.5%의 EER(Equal Error Rate) 성능을 얻었으며, FRR(False Rejection Rate : 본인의 생체 정보로 타인의 암호화키가 나올 에러율)을 25%로 설정하였을 때, FAR(False Acceptance Rate : 타인의 생체 정보로 본인의 암호화키가 나올 에러율)은 약 0.002%의 성능을 얻었다. 동시에 본 시스템에서는 임계 치에 따라 암호화키 생성의 FAR과 FRR값을 동적으로 제어할 수 있는 기능을 제공하였다.

Abstract

Recently, as a number of media are fused into a phone, the requirement of security of service provided on a mobile phone is increasing. For this, conventional cryptographic key based on password and security card is used in the mobile phone, but it has the characteristics which is easy to be vulnerable and to be illegally stolen. To overcome such a problem, the researches to generate key based on biometrics have been done. However, it has also the problem that biometric information is susceptible to the variation of environment, whereas conventional cryptographic system should generate invariant cryptographic key at any time. So, we propose new method of producing cryptographic key based on "Biometric matching-based key release" instead of "Biometric-based key generation" by using both face and iris information in order to overcome the unstability of uni-modal biometrics. Also, by using mega-pixel camera embedded on mobile phone, we can provide users with convenience that both face and iris recognition is possible at the same time. Experimental results showed that we could obtain the EER(Equal Error Rate) performance of 0.5% when producing cryptographic key. And FAR was shown as about 0.002% in case of FRR of 25%. In addition, our system can provide the functionality of controlling FAR and FRR based on threshold.

Keywords: Cryptographic Key. Biometric Matching-based Key Release, Face and Iris Information

* 학생회원, 상명대학교 일반대학원 컴퓨터과학과
(Dept. of Computer Science, Sangmyung University)
** 정회원, 상명대학교 디지털미디어학부
(Division of Digital Media Technology, Sangmyung University)
접수일자: 2007년1월3일, 수정완료일: 2007년11월4일

Ⅰ. 서 론

최근 하나의 휴대폰에 여러 가지 미디어들이 복합적으로 장착됨에 따라 휴대폰에서 제공되는 서비스의 사용자 보안에 대한 요구가 증가되고 있다. 이를 위한 인증 방법으로는 Miller에 의해 소개된 4가지의 방법이 있다[1]. 첫 번째는 소유(Possession)의 개념으로 인식에 사용되는 도구를 사용자가 직접 소유(have)하고 있는 것이다. 예를 들면 사용자 ID, 카드, 키와 같은 것으로 이것들은 타인과 공유하는 것이 가능하고 복사하거나 분실의 위험이 있는 특징이 있다. 두 번째는 기억(knowledge)의 개념으로 인식에 사용되는 것을 사용자가 직접 기억하고 있는 것이다. 이는 비밀번호와 같은 것으로 이 또한 타인과 공유하는 것이 가능하고 많은 비밀번호를 사용할 경우 혼란의 여지가 큰 특징이 있다. 세 번째는 소유하는 것과 기억하는 것을 혼합한 방법이다. 우리가 주변에서 흔히 사용하는 사용자ID와 비밀번호를 사용하거나 현금인출기에서 카드와 비밀번호를 사용하는 것을 의미한다. 이 또한 앞에서 제시한 방법들과 마찬가지로 분실과 공유하는 것이 가능한 특징을 갖고 있다. 네 번째는 사용자마다 유일하게 갖고 있는 생체정보(Biometric information)를 이용하는 방법이다. 지문, 홍채, 목소리, 얼굴 등을 이용하는 것으로 이는 타인과 공유하거나 복사할 수 없을 뿐 아니라 분실의 위험이 상대적으로 적은 특징을 갖고 있다. 이와 같은 인증 방법의 분류 아래, 현재 휴대폰에서 응용되고 있는 방법으로는 간단한 곳에서는 비밀번호를 이용하거나 모바일 뱅킹과 같이 높은 보안을 요구하는 서비스에서는 인증센터로부터 인증을 받은 뒤 본인에게만 부여된 보안카드의 코드 표를 이용하여 비밀번호보다는 좀 더 강화된 보안성을 제공해 주고 있다. 하지만 비밀번호와 마찬가지로 코드표가 타인에 의해 공유되거나 분실 될 경우 위험에 노출될 수 있는 단점을 가지고 있다.

따라서 본 연구에서는 분실의 위험이 없는 생체정보를 이용한 암호화키의 생성 방법에 대한 연구를 진행하였다. 인식에 사용될 수 있는 여러 생체 가운데 휴대폰 환경에서 인증 또는 암호화를 위하여 쉽게 사용될 수 있는 것은 홍채, 얼굴, 지문 등이 있다. 그러나 지문 인식의 경우는 별도의 지문센서를 부착해야하므로 휴대폰의 부피가 커지고 가격이 상승하는 문제점이 있다. 이러한 예로 지문인식을 이용한 휴대폰(LP3550)[2]이 출시되었지만 DSP(Digital Signal Processing)칩의 장착과 지문을 입력받는 센서 공간의 추가로 비용과 크기 면에서 사용자들에게 대중화되지 못하였다. 최근 휴대폰 카메라의 발달에 따라 화소 수는 증가하면서 가격은 하락하며 거의 모든 휴대폰에 고 해상도의 메가 픽셀(Mega-pixel) 카메라가 내장되어 출시되고 있다. 이러한 환경에 발맞추어 휴대폰의 내장형 카메라를 이용한 얼굴 인식과 홍채 인식에 대한 연구가 빠른 속도로 진행되고 있다. 얼굴 인식과 홍채 인식은 다른 부가적인 칩의 부착 없이 휴대폰의 내장된 메가 픽셀 카메라를 통하여 인식 가능하기 때문에 지문 인식 휴대폰이 대중화되지 못한 문제점을 극복하고 대중화의 요소를 충분히 가지고 있다.

홍채 인식은 생체 인식 중에 비교적 높은 인식 성능을 갖는 것으로 알려져 있지만, 안경 면에 발생되는 조명 반사광이 홍채의 일부분을 가리거나 영상의 초점이 맞지 않은 경우. 선천적으로 눈이 작은 사람의 경우 인식 성능이 현저하게 떨어지는 문제점을 갖고 있다.

얼굴 인식은 홍채인식에 비하여 낮은 인식 성능을 갖지만 사용자의 거부감 없이 쉽게 영상을 취득할 수 있다는 장점을 가지고 있다. 메가 픽셀 휴대폰 카메라로부터 얼굴 영상을 취득하면 얼굴 인식 뿐 아니라 홍채 인식을 위한 충분한 해상도를 지원하고 한 번의 영상 취득 과정을 통하여 얼굴 인식과 홍채 인식의 다중 생체 인식이 가능하게 된다[13, 16].

이러한 생체의 장점을 이용하여 생체를 이용한 암호화키의 생성방법에 대한 연구가 많이 진행되어 왔다[4~6, 18]. 하지만 대다수의 연구가 하나의 생체로부터 키를 생성하는 방법이며 생체의 특징으로부터 매칭과정 없이 직접적으로 생체 정보로부터 키를 생성해 내기 때문에 항상 동일한 값이어야 하는 암호화키의 속성을 만족시키지 못하는 경우가 자주 발생하게 된다. 따라서 본 연구에서는 위에서 제시한 홍채와 얼굴의 두 가지 생체를 이용하여 하나의 생체에서 오는 성능의 불안정성을 최소화하고 각 생체의 장점을 극대화시켜, 휴대폰 환경에서의 얼굴인식과 홍채인식 알고리즘을 바탕으로 한 매칭 기반 암호화키 생성에 대한 방법을 제안한다. Ⅱ장 관련연구에서는 기존의 생채정보를 이용한 키 생성에 관한 연구를 살펴보고, Ⅲ장에서는 본 연구에서 제안한 얼굴과 홍채를 이용한 생체 키 생성 방법에 대하여 소개한다. 마지막으로 Ⅳ장에서는 실험 구현 및 실험결과를 나타낸다.

Ⅱ. 관련 연구

생체를 이용하여 키를 생성하는 방법은 생체의 특징으로부터 별도의 매칭 과정 없이 직접적으로 키 값을 추출해 내는 방법인 "생체 정보 기반 키 생성" 방법(Biometric-based key generation)과 미리 정의 되어 있는 키 값이 생체정보 매칭을 통하여 도출되는 방법인 "생체 정보 매칭 기반 키 생성" 방법 (Biometric matching-based key release)으로 분류 할 수 있다. 생체 정보 기반 키 생성 방법의 하나로 Monrose *et al.*은 key-stroke를 이용한 키 생성 방법을 제안하였다[4]. 키보드를 치는 움직임으로부터 특징을 추출하고 견고한 키의 생성을 위하여 사용자의 비밀번호와 혼합하여 사용하였다. 이 때 각 특징들은 하나의 비트로 연결되기 때문에 특징의 변화에 대한 오차를 갖고 있게 되며, 각 비트들은 하나로 연결되어 최종적인 키로 만들어지게 된다. 또 다른 연구로 Monrose *et al.*은 음성을 이용한 키 생성 방법을 제안하였다[5]. Monrose의 이전 연구와 유사한 방법으로 음성의 특징을 추출하고 그것을 기반으로 키를 생성하였는데 기존 12비트의 키에서 46비트의 키로 확장시켰으며 False Reject Error는 48.4%에서 20%로 감소시켰다. Feng Hao *et al.*에 의해 제안된 방법은 홍채를 이용하여 키를 생성해내는 것이다[6]. 홍채 코드내의 에러 비트를 정정하기 위하여 Hadamard, Reed-Solomon codes를 사용하면서 성공적으로 140비트의 키를 생성하고 False Reject Error를 0.47%로 감소시켰다. 위에 제시한 방법들은 모두 생체의 특징을 기반으로 하여 키를 생성해내는 방법들로 키를 저장하거나 영상을 저장하지 않아도 되기 때문에 키를 분실하거나 생체 영상을 분실하게 되는 가능성이 적지만 매번 생체 특징 추출 시 마다 특징 값이 동일하지 않고 변화도를 갖는 성질로 동일한 키를 생성해 내는데 어려움을 갖게 된다. 또한 알고리즘이 상대적으로 복잡하고 많은 프로세싱 파워를 요구하기 때문에 적은 프로세싱 파워를 제공하는 휴대폰 환경에서는 구현의 어려움이 존재하게 된다.

생체 키를 추출하는 두 번째 방법으로 "생체 정보 매칭 기반 키 생성" 방법은 이와는 다른 특징을 갖고 있다. Fengling han et al.[7]은 현금 자동 인출기 시스템을 위하여 지문과 스마트카드를 혼합하여 사용하는 방법을 제안하였다. 총 두 단계로 이루어져 있는 이 시스템은 첫 번째 단계를 통과하기 위하여 스마트카드를 사용하였고 두 번째 단계를 통과하기 위하여 지문인식을 사용하였다. 인식을 위한 매칭 후, 매칭이 성공하면 그 다음 절차를 진행하고 그렇지 않으면 공격자로 간주하고 절차를 멈추는 방법을 사용하였다. 직접적으로 생체로부터 키를 추출하는 방법 대신에 "생체 정보 매칭 기반 키 생성" 방법을 사용하였으며 미리 정의 된 키는 생체 샘플들과 함께 암호화 되고 높은 성능을 가지고 인식한 뒤에 미리 정의되어 있는 키를 도출할 수 있도록 하였다. 이러한 "생체 정보 매칭 기반 키 생성" 방법은 암호화키를 미리 정의해 놓고 사용하기 때문에 첫 번째 방법인 "생체 정보 기반 키 생성" 방법에서 생성된 키가 동일하지 않을 수 있는 가능성을 제거하였다. 또한

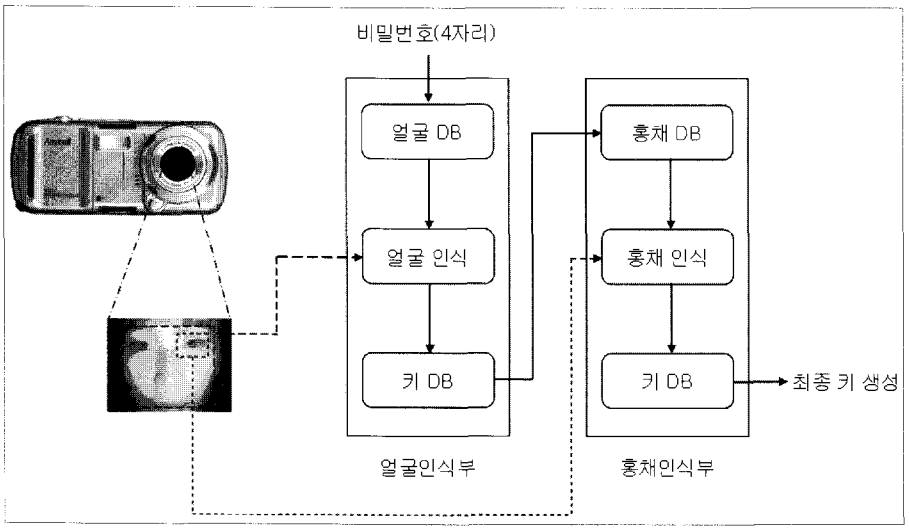


그림 1. 휴대폰에서의 다중 생체 기반 암호화키 생성 과정

Fig. 1. process of generating cryptographic key on mobile phone based on multi-modal biometrics.

알고리즘이 간단하고 구현이 상대적으로 복잡하지 않아 휴대폰과 같이 낮은 프로세싱 파워를 요구하는 응용프로그램에 적합하다. 하지만 미리 정의된 키와 인식에 사용할 영상을 저장해 놓고 있어 분실의 위험이 존재한다. 또한 인식의 결과로 키가 도출되는 것이기 때문에 성능이 높은 생체를 사용해야 한다.

기존에 Fengling han et al은 지문과 카드를 이용하여 미리 생성해 놓은 키를 도출하는 방법을 연구하였다[7]. 하지만 Fengling han et al은 단일 생체, 즉 지문 정보만을 이용하여 인식에 사용하였기 때문에 시스템에 대한 공격이 시도되었을 때 본 연구에서와 같이 다중 생체를 이용하는 것 보다 키가 잘못 유출될 수 있는 가능성이 큰 단점을 갖고 있다.

또한, 기존에 얼굴과 홍채를 feature level 및 score level에서 각각 결합한 연구들은 있었으나[22~23], 모두 얼굴 및 홍채 DB에 대한 보안문제는 고려하지 않았다. 이러한 문제를 해결하기 위하여 본 연구에서는 얼굴 DB는 사용자 정의 비밀번호로, 홍채 DB는 얼굴 매칭 결과 생성된 키로 각각 암호화함으로써, 휴대폰 환경에서 홍채/얼굴 인식의 결합 및 홍채/얼굴 DB의 보안문제를 같이 해결하는 방식을 제안하였다.

즉, 본 논문에서는 하나의 생체가 가지는 인식의 불안정성을 극복하기 위하여 두 개의 생체를 사용하는 다중생체 인식과 "생체 정보 매칭 기반 키 생성"을 결합함으로써 키를 도출하는 방법을 제안하였다.

이처럼 기존에 "단일 생체 정보 매칭 기반 키 생성 방법"과 "홍채와 얼굴을 다중 인식"하는 방법들은 각각 연구되었으나, 이 두 가지를 결합하여 본 연구에서와 같이 휴대폰 환경에서 홍채 및 얼굴의 다중 인식 기반 키 생성 방법에 관한 연구는 조사된 바 없다.

Ⅲ. 얼굴과 홍채를 이용한 생체 키 생성 방법

1. 키 생성 방법 알고리즘

본 논문에서 제안하는 키 생성 방법은 하나의 생체가 갖는 인식 성능의 약점을 극복하기 위하여 동시에 영상을 취득할 수 있는 얼굴과 홍채를 결합한 다중생체인식을 사용하고, 생체의 특징으로부터 직접 키를 생성하는 "생체 정보 기반 키 생성" 방법의 약점을 극복하기 위하여 매칭 후 미리 저장된 키를 생성하는 "생체 정보 매칭 기반 키 생성" 방법을 결합한 것이다. 본 논문에서 제안하는 키 생성 방법의 과정은 그림 1과 같다.

실험에서 사용한 700만 화소의 카메라는 그림 2에서 보이는 바와 같이 얼굴의 눈썹에서 입술까지의 영역을 포함할 수 있는 해상도(3,072×2,304 픽셀)를 지원한다. 따라서 한 번의 영상 촬영 과정을 통하여 촬영된 영상은 얼굴 인식과 홍채 인식에 사용될 영상으로 분할되어 각 인식 과정을 위한 입력 영상으로 사용된다.

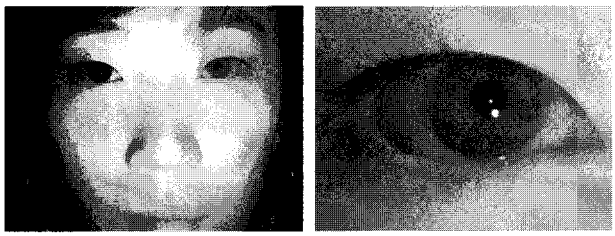


그림 2. 메가 픽셀 휴대폰 카메라로 촬영된 얼굴 영상과 홍채 영상

Fig. 2. Face image and iris image captured by mega-pixel camera in mobile phone.

일반적으로 홍채인식을 위해서는 홍채 직경이 200 픽셀 이상의 크기로 잡아야한다. 그러므로 일반적으로 홍채 카메라는 눈 영역만 확대해서 취득하는 협각(Narrow view) 카메라를 사용하고, 반면 얼굴인식을 위해서는 얼굴 전체 영역을 취득하는 광각(Wide view)카메라를 사용한다. 이처럼 2 카메라의 화각이 서로 틀리므로, 기존에는 2개 이상의 카메라를 사용하여 얼굴과 홍채 영상을 별도로 취득했습니다.

반면 최근 휴대폰의 고사양화에 따라 700만화소급 카메라가 휴대폰에 손쉽게 장착되어 출시되고 있다. 본 연구에서 사용한 카메라 휴대폰 역시, 700만 화소 카메라가 내장되어 있는 삼성전자에서 개발한 휴대폰(SCH-V770)[17]이며, 현재 출시되어 상용화되고 있다.

본 연구에서 제안하는 방법은 그림 1과 같이 총 두 단계로 진행된다. 첫 번째는 얼굴 인식을 통하여 1차 키를 생성하는 과정이고 두 번째는 홍채 인식을 통하여 2차 키, 즉 최종 암호화키를 생성하는 과정이다. 그림 1에서처럼, 휴대폰 카메라로 얼굴 영역이 추출되면 조명에 의한 각막 반사광을 이용하여 눈 위치를 찾게 된다.

이를 기준으로 양 눈 및 입까지의 비율 정보를 이용하여 양 눈과 입술이 포함된 얼굴 영역을 취득하게 된다[8, 13]. 추출된 얼굴 영역은 휴대폰 내부에 미리 저장된 얼굴 DB와 매칭 하게 된다[8]. 이때, 얼굴 DB의 보안성을 높이기 위해 사용자 비밀번호에 의해 얼굴 DB는 암호화된 상태로 유지되며, 올바른 비밀번호가 입력되는 경우에 얼굴 DB가 복호화 되어 입력 얼굴 영상과 매칭하게 된다. 얼굴 DB와의 매칭이 성공하게 되면 얼굴 DB에 이미 생성되어 있던 키가 도출되고, 이 키를 이용

하여 홍채 DB를 복호화하게 된다.

그러면 그림 2에서와 같이 메가 픽셀 얼굴 영상에서 취득한 홍채 입력 영상과 저장되어 있는 홍채 DB와의 2차 매칭을 수행한다[13~16]. 그림 1에서와 같이 매칭이 성공적으로 끝나는 경우, 홍채 DB에 이미 생성되어 있던 최종적인 암호화키가 도출되게 된다. 본 연구에서는 일반적인 PKI(Public Key Infrastructure)에서 사용하는 개인키(Private Key)를 대상으로 하여 128 비트를 생성하도록 하였다.

2. 얼굴인식 알고리즘

본 장에서는 그림 1의 입력 영상과 미리 저장된 얼굴 DB와의 인식 방법에 관한 부분을 설명한다. 얼굴인식은 얼굴의 수많은 특징들과 조명, 표정 변화 등 다양한 환경에 의한 영향으로 다른 생체에 비하여 낮은 성능을 보임에도 불구하고 인식 시에 사람들이 얼굴에 갖고 있는 친근감과 편리함으로 많은 곳에서 사용되어 지고 있다. 현재는 2D 뿐 아니라 3D를 이용한 기술을 얼굴 인식에 도입하면서 성능이 많이 향상되고 안정화되고 있다. 본 논문에서 사용한 얼굴인식은 휴대폰 환경이라는 매우 제한된 환경 아래 수행되기 때문에 일반적인 환경에서 수행되는 얼굴 인식과는 차별적인 특징이 있다[8]. 휴대폰 환경은 일반적으로 느린 프로세싱 파워와 실수 연산을 지원하지 않기 때문에 이런 환경을 반영한 얼굴 인식 알고리즘을 사용할 필요가 있다[19]. 그림 3은 본 논문에서 사용한 얼굴 인식 과정을 나타낸다. 기존의 얼굴 인식 알고리즘을 기반으로 각 단계별로 휴대폰 환경에 적합하게 변경된 알고리즘을 사용하였다. 입력 영상에서 얼굴 영역을 검출하기 위하여 조명으로 인해 발생하는 동공 및 홍채의 반사광(Specular Reflection)을 중심으로 얼굴 영역을 검출하는 방법을 사용하였다[13]. 입력 영상을 취득할 때에 홍채인식과의 다중생체인식을 고려하여 사용한 적외선 조명은 휴대폰의 특성상 가까운 근접 촬영으로 인하여 밝기포화 (Brightness Saturation)와 부분 그림자 (Local Shading)를 발생시킨다. 따라서 이를 보정해 주는 조명 정규화(Normali- zation)과정이 필요하다. 기존 연구로써 적외선 조명의 영향을 최소화

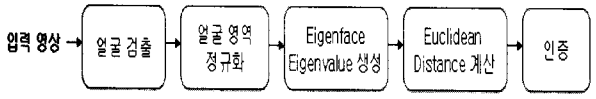


그림 3. 얼굴 인식 과정
Fig. 3. Procedure of face recognition.

하기 위한 정규화 방법은 대표적으로 homomorphic[9] 방법이 있지만 이것은 FFT연산을 주로 하여 실수연산과 많은 처리 시간을 필요로 하기 때문에 휴대폰 환경에 적합하지 않다. 따라서 본 논문에서 조명 정규화를 위하여 간단하지만 성능을 향상시킬 수 있는 저연산 Look-up table기반 Logarithm 변환 정규화 방법을 사용하였다[8]. Logarithm 변환 정규화 방법을 사용함으로써 기존의 정규화 방법을 사용하지 않았을 때의 정확도(EER) 16.43%에서 14.79%로 향상된 결과를 얻을 수 있었다. 다음 단계로, 정규화 된 영상의 특징을 추출하기 위하여 정수기반의 PCA(Principal Component Analysis)를 사용하였다[8, 10]. 이미 보편적으로 사용되고 있는 훈련 알고리즘에는 PCA, ICA(Independent Component Analysis)[11], LDA(Linear Discriminant Analysis)[12]등이 있지만 가시광선이 아닌 적외선 조명 아래 휴대폰으로 영상을 취득하여 영상을 훈련시켜야 하는 특징을 고려하여 볼 때 많은 훈련 영상을 취득할 수 없다는 점과 느린 프로세싱 파워의 환경에서 PCA가 가장 적합한 알고리즘이라는 것이 실험을 통하여 입증되었다[8]. 하지만 기존의 PCA 방법에는 실수 연산이 포함되어 있기 때문에 휴대폰 환경에 적합한 PCA 알고리즘으로 변경해주는 과정이 필요하다. 따라서 실수 연산을 정수 연산으로 변경하고 최적화 시킨 정수기반의 PCA를 사용하였다[8]. 정수기반의 PCA를 사용함으로써 기존 실수 연산 PCA를 사용했을 때의 정확도(EER) 14.79%에서 14.65%로 거의 비슷한 정확도를 나타냈다.

PDA(CPU: Intel PXA270, CPU clock : 624MHz, Memory : 128MB)에서 처리 속도를 측정하였을 때 정수 기반의 PCA를 사용한 것이 57.57ms로 실수 연산이 포함된 PCA를 사용할 때의 233.68ms 보다 훨씬 빠른 처리속도를 나타냈다[8].

휴대폰 환경에서 성능을 최대화시키기 위해 전술한 방법을 통하여 휴대폰 환경에서도 데스크 탑에서의 성능과 유사한 인식 성능 결과를 획득하였고 또한 휴대폰 환경에서 정수기반의 PCA를 사용함으로써 기존 실수연산의 PCA보다 약 4배 빠른 처리속도를 나타내었다. 입력 얼굴 영상에서 추출된 PCA 계수는 유클리디안 거리(Euclidean Distance)를 이용하여 얼굴 DB와 유사도를 계산하였다[8].

3. 홍채인식 알고리즘

홍채인식은 여러 가지 생체 중에서도 특히 인식성능이 좋은 것으로 알려져 있기 때문에 높은 보안을 요구

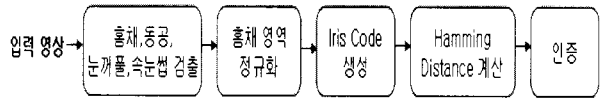


그림 4. 홍채 인식 과정
Fig. 4. Procedure of iris recognition.

하는 많은 응용프로그램에서 홍채 인식을 도입하여 활용하고 있다. 최근 메가 픽셀 카메라가 휴대폰에 장착되어 출시됨에 따라 고 배율의 줌렌즈나 초점 렌즈 없이도 홍채인식을 위한 해상도를 지원하게 되었다. 즉, 메가 픽셀 카메라 폰을 사용하여 사용자로부터 비교적 원거리에서 취득한 얼굴영상에서의 홍채 영역이 홍채인식을 위한 충분한 픽셀정보를 가지게 된 것이다.

그림 4는 본 논문에서 사용한 홍채 인식 과정을 나타낸다. 홍채 인식 알고리즘 역시 기존의 홍채 인식 알고리즘을 휴대폰 환경에 적합하게 변경한 뒤 사용하였다. 먼저, 입력영상에서 태양광의 존재유무와 흐림 현상(Optical & Motion Blur)을 판단하기 위해 조명을 연속적으로 On/Off 시키는 방법을 사용하여 각막에 반사되는 조명반사광의 밝기와 크기를 추정하는 이론적 배경을 바탕으로 고 해상도의 얼굴 영상에서 홍채의 위치를 찾는다. 이때의 모든 실수연산을 정수연산으로 변환하여 Embedded Board(CPU : StrongARM, CPU clock : 206MHz, Memory : 32MB)에서 처리속도를 측정하였을 때 12.02ms로 PDA(CPU : Intel PXA 270, CPU clock : 624MHz, Memory : 128MB)에서 실수연산의 처리시간을 측정한 값 21.98ms 보다 적은 처리 속도를 나타냈다. 이렇게 검출된 홍채의 위치를 가지고 홍채 영역을 분리하기 위하여 Dal-ho Cho *et al*[14]에 의해 제안된 동공, 홍채 영역 검출 알고리즘을 사용하여 입력 영상 내에서 고속으로 동공과 홍채의 영역을 검출하였다. 또한 눈꺼풀을 찾기 위하여 장영균 등[15]에 의해 제안된 눈꺼풀 검출 알고리즘을 사용하였으며, 속눈썹을 검출하기 위

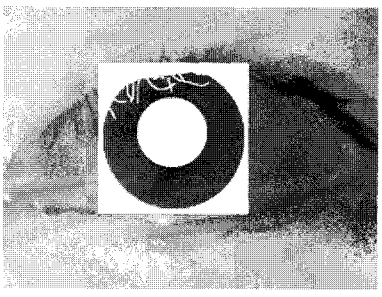


그림 5. 검출 된 홍채 영역
Fig. 5. detected the iris region.

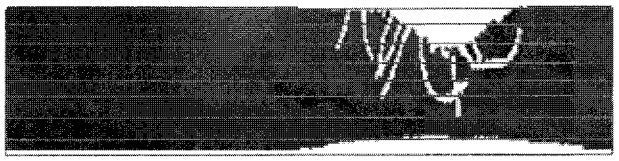


그림 6. 정규화 된 홍채 영상
Fig. 6. normalized iris image.

하여 강병준 등[20]의 연구결과를 이용하였다.

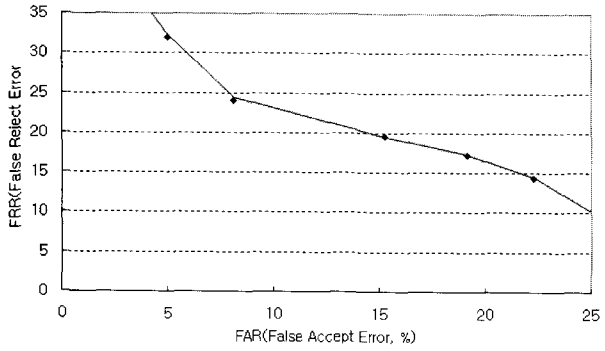
그림 5는 검출 된 홍채 영역을 나타낸다. 이렇게 검출 된 영역은 휴대폰 환경에 적합한 고속의 홍채 특징 추출[16]을 위하여 그림 6과 같이 직사각형으로 펼친 후에 8개의 트랙(track)으로 나누어 가로방향으로는 1차원의 가버 웨이블릿 커널을, 세로방향으로는 1차원의 가우시안 커널을 적용하여 특징을 추출하였다[16]. 이때 가우시안 커널을 적용하는 이유는 동공 및 홍채 영역 검출의 오차를 줄이기 위해서 이다. 8개 트랙의 총 256 위치에서 가버 웨이블릿을 적용하여 계산된 위상 값(Phase)을 0과 1의 비트로 변환하고, 이를 미리 저장된 홍채 코드 비트열과의 해밍 거리(Hamming Distance)를 계산함으로써 매칭 과정을 수행하게 된다[16, 21]. 이때 iris code 생성, Gabor를 적용하는 과정에서 발생하는 실수연산과 cos, sin 값을 정수연산 및 정수 값으로 변형하여 사용함으로써 실수연산으로 Embedded Board에서 처리속도를 측정하였을 때, 실수연산 시에 2,628ms의 값이 정수연산 시 1,471ms로 감소하여 향상된 처리 속도를 나타냈다.

Ⅳ. 실험 및 실험 결과

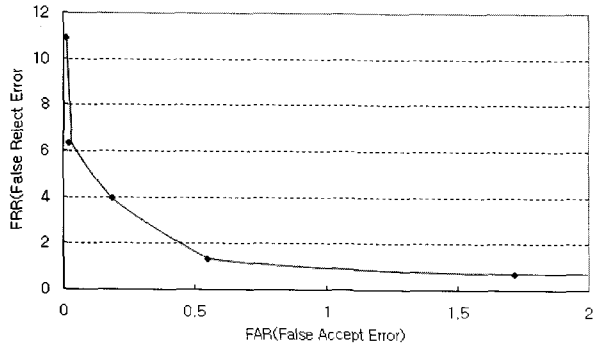
본 연구에서는 실험을 위하여 700만 화소 카메라가 내장되어 있는 삼성전자에서 개발한 휴대폰(SCH-V770)[17]을 사용하여 총 40명으로부터 취득된 506장의 영상을 이용하였다. 먼저 얼굴인식과 홍채인식의 EER(Error Equal Rate), FAR(False Accept Rate) 그리고 FRR(False Reject Rate)를 측정한 뒤 본 논문에서 제안하는 암호화키 생성 방법의 FAR와 FRR를 측정하여 성능을 분석하였다.

인식과정에서와는 조금 다른 개념으로 암호화키 생성에서의 FAR은 타인의 얼굴 및 홍채 정보로 본인의 암호화키가 나올 확률을, 그리고 FRR은 본인의 얼굴 및 홍채 정보로 타인의 암호화키가 나올 확률을 의미한다.

일반적으로 금융권 등 높은 성능의 보안 시스템을 구현하기 위해서는 FAR과 FRR이 동일한 EER을 적용하



(a)



(b)

그림 7. ROC(receiver operating characteristic) 곡선
(a) 얼굴인식의 ROC 곡선
(b) 홍채인식의 ROC 곡선

Fig. 7. ROC(receiver operating characteristic) curve.
(a). ROC curve of face (b). ROC curve of iris

는 것 보다는 FRR이 높게 나타나더라도 적은 FAR의 값을 갖도록 설정해 주는 것이 필요하다. 그리고 이외의 일반적인 시스템에서는 EER이 최소가 되도록 임계치 값을 설정해 주는 것이 필요하다. 그러므로 본 연구에서는 고 보안 시스템의 경우를 대비하여 FRR을 25%정도로 간주 했을 때 FAR값을, 그리고 기타 일반적인 보안 시스템을 대상으로 하였을 때 EER이 최소가 되는 경우의 FAR과 FRR을 각각 구하였다.

그림 7은 각각 본 연구에서 사용한 얼굴인식[8]과 홍채인식[13~16]의 ROC 곡선을 나타낸 것이다. 실험결과 얼굴 인식과 홍채 인식의 EER은 각각 16%와 0.8%의 성능을 나타냈다. 이를 기반으로 최종적인 암호화키 생성의 FAR과 FRR은 식 (1)을 통하여 얻을 수 있다.

$$FAR_t = FAR_u * FAR_f * FAR_i$$
$$FRR_t = 1-(1-FRR_u)*(1-FRR_f)*(1-FRR_i) \quad (1)$$

식(1)에서 FAR_t과 FRR_t 은 각각 최종적인 암호화키 생성의 FAR과 FRR을 의미한다. 또한 FAR_u과 FRR_u은 각각 4자리 사용자 비밀번호를 입력할 때의 FAR과 FRR을 의미한다. 그리고 FAR_f 과 FRR_f, FAR_i 과 FRR_i 은 각각 얼굴 인식과 홍채 인식의 FAR과 FRR을 나타낸다. 그림 1에서와 같이 사용자 비밀번호 입력, 얼굴 인식 및 홍채 인식이 모두 성공해야 최종적인 암호화키가 나오게 되므로 모두 AND rule로 결합하여 최종적인 FAR_t과 FRR_t은 식 (1)과 같이 표현된다. 식 (1)에서 사용자 비밀번호는 타인에 의해 쉽게 도용된다고 가정하고 비밀번호 입력에 대한 FAR_u은 1로 가정한다. 또한 본인이 자신의 비밀번호를 잊지 않고 입력할 때 오류가 없다고 가정하면, 비밀번호 입력에 대한 FRR_u은 0이 된다. 이로부터 식 (1)은 식 (2)와 같이 다시 표현될 수 있다.

$$FAR_t = FAR_f * FAR_i$$
$$FRR_t = 1-(1-FRR_f)*(1-FRR_i) \quad (2)$$

식 (2)와 같이 AND rule로 결합되는 경우, 확률의 곱 형태로 표현되므로 FRR_t 보다는 FAR_t이 일반적으로 작아지게 된다. 그림 7의 FAR 및 FRR을 식 (2)에 대입하여 계산한 결과, 암호화키 생성에 있어서 0.5%의 EER(Equal Error Rate) 성능을 얻을 수 있었다. 이는 200명중 1명에게서 부정확한 인식 성능이 나타날 수 있음을 의미하는 수치이다. 또한, 일반적으로 FRR을 25%로 잡았을 때 사용자의 불편도가 그렇게 크지 않다고 가정하고, FRR(False Rejection Rate : 본인의 생체 정보로 타인의 암호화키가 나올 에러율)을 25% 로 설정하였을 때, FAR(False Acceptance Rate : 타인의 생체 정보로 본인의 암호화키가 나올 에러율) 약 0.002%의 성능을 이론적 및 실험적으로 얻을 수 있었다. 이는 50,000명중 1명에게서 부정확한 인식 성능이 나타날 수 있음을 의미하는 수치이다. 표 1은 그림 7의 홍채와 얼굴 ROC곡선에서 구해진 FAR 및 FRR을 식(2)에 대입하여 구한 암호화 키 생성의 FRR과 FAR값을 나타낸 것이다.

표 1. 암호화키 생성의 FAR과 FRR
Table 1. FAR and FRR of generating cryptographic key.

FRR_t (%)	FAR_t(%)
40	0.00001
30	0.001
25	0.002
20	0.03
10	0.07
5	0.09
1	0.1

동시에 본 시스템에서는 얼굴 및 홍채 인식의 임계치(threshold)에 따라 암호화키 생성의 FAR과 FRR값을 동적으로 제어할 수 있는 기능을 제공한다. 즉, 요구되어지는 FRR_t과 FAR_t의 수치가 주어졌을 때, 식 (2) 및 임계치에 의해 얼굴 인식 및 홍채 인식의 FAR과 FRR을 조정함으로써 요구사항을 만족할 수 있게 된다.
단일생체 정보를 이용한 암호화키 생성법과 비교했을 때, 일반적으로 단일 생체를 사용하는 것보다는 다중 생체를 이용하여 인식할 경우 인식의 성능이 보다 안정화되고 향상된다는 점은 이전의 많은 연구들에 의해 이미 입증되어 다[3].

또한, 식 (2)로 부터 단일생체 정보(얼굴 혹은 홍채)만을 이용했을 때의 FAR_t과 FRR_t은 각각, $FAR_t = FAR_f$ (혹은 $FAR_t = FAR_i$) 및 $FRR_t = 1-(1-FRR_f)$(혹은 $FRR_t = 1-(1-FRR_i)$)이 된다. 식 (2)와 비교해 보았을 때, 단일생체만을 이용했을 때는 다중생체보다 FAR이 커지고, FRR은 작아짐을 알 수 있다.

본 연구에서와 같이 암호화키를 생성하는 시스템에서는 본인 거부율(FRR) 보다는 타인에 의해 본인의 암호화 키가 잘못 생성되는 오류율(FAR)이 더욱 심각한 문제이므로, 본 연구에서와 같이 다중 생체 정보를 이용하는 것이 보다 더 안정적인 성능을 낸다고 할 수 있다.

V. 결 론

본 논문에서는 저 연산 휴대폰환경에 적합한 얼굴 및 홍채 다중 생체인식을 통한 암호화키 생성 방법을 제안하였다. 암호화키를 미리 저장해 놓고 사용하는 "생체정보 매칭 기반 키 시스템"을 사용함으로써 생체의 특징으로부터 직접 키를 생성해 내는 방법의 문제점을 극복하였고, 다중 생체를 이용함으로써 하나의 생체를 이용하여 생체 정보 매칭 기반 키 시스템을 적용한 시스템이 갖는 생체 인식의 불안정함을 좀 더 안정화 시킬 수 있었다. 또한, 요구되어지는 암호화키 생성에 대한 FAR과 FRR의 수치가 주어졌을 때, 얼굴 인식 및 홍채 인식의 FAR과 FRR을 조정함으로써 요구사항을 만족할 수 있게 하는 기능 역시 제공 하였다.

향후, 실제 휴대폰 환경에서 구동하여 처리 시간 등을 측정하여야 하며, 보다 많은 입력 데이터에 대하여 실험해야 할 것으로 요구된다.

참 고 문 헌

[1] Ruud Bolle, Jonathan Connell, Sharanthchandra Pankanti, Nalini Ratha, Andrew Senior "Guide to Biometrics" Springer Professional Computing. p20-21, 2003.

[2] http://www.lge.com (accessed on 2007. 08. 31)

[3] Arun Ross, Anil Jain, Jian-Zhong Qian, : Information Fusion in Biometrics. Pattern Recognition Letters, vol. 24, issue 13, p2115-2125, 2003.

[4] F. Monrose, M.K. Reiter and R. Wetzel, : Password hardening based on keystroke dynamics. Proceedings of sixth ACM Conference on Computer and Communications Security, CCCS, 1999.

[5] F. Monrose, M.K. Reiter, Q. Li and S. Wetzel, :Cryptographic key generation from voice. Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

[6] Feng Hao, Ross Anderson, John Daugman, : Combining Crypto with Biometrics Effectivel. IEEE Transactions on Computers archive, Volume55, p1081-1088, 2006.

[7] Fengling Han, Jiankun Hu, Xinhuo Yu, Yong Feng and Jie Zhou : A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications. ICB 2006, LNCS3832, p675-681, 2005.

[8] Songyi Han, Hyun-Ae Park, Dal-ho Cho, Kang Ryoung Park : Face Recognition Based on Near-Infrared Light using Mobile Phone, Lecture Notes in Computer Science (ICANNGA'2007), Warsaw, Poland, April 11 ~ 14, 2007, accepted for publication

[9] Wen-Hung Liao, Dai-Yun Li : Homomorphic processing techniques for near-infrared images. Proceedings of ICASSP, Vol.3 p461-464, 2003

[10] M. Turk, A. Pentland : Eigenfaces for Recognition. Journal of Cognitive Neuroscience, Vol. 3 , No. 1 p71-86, 1991.

[11] M. S. Barlett, J. R. Movellan, T.J. Sejnowski : Face Recognition by Independent Component Analysis. IEEE Trans. on Neural Networks, Vol. 13, No. 6 p1450-1464, 2002.

[12] P. Belhumeur, J. Hespanha, D.Kriegman : Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. IEEE Trans. on PAMI, Vol. 19, No. 7 p711-720, 1997.

[13] 박현애, 박강령 : 휴대폰에서의 홍채인식을 위한 고속 홍채검출에 관한 연구, 대한전자공학회 논문지, Vol. 43, SP, No. 2, p19 ~ 29, 2006. 3

[14] Dal-ho Cho, Kang Ryoung Park, Dae Woong Rhee, Yanggon Kim, Jonghoon Yang, : Pupil and Iris Localization for Iris Recognition in Mobile Phones, SNPD, Las Vegas Nevada, USA, June p19-20, 2006.
[15] 장영균, 강병준, 박강령, 홍채 인식을 위한 포물 허프 변환 기반 눈꺼풀 영역 검출 알고리즘, 대한전자공학회 논문지, 제44권 SP편 제 1호, 2006년 1월
[16] Hyun-Ae Park, Kang Ryoung Park, : Iris Recognition Based on Score Level Fusion by Using SVM. Pattern Recognition Letters, submitted
[17] http://land.anycall.com (accessed on 2007. 08. 31)
[18] 이연주, 박강령, 김재희, : 퍼지볼트 기반의 암호키 생성을 위한 불변 홍채코드 추출, 2006년 대한전자공학회 하계학술대회, 제주롯데호텔, 2006. 6. p21-23
[19] K. H. Pun et al., : A Face Authentication System for Mobile Devices: Optimization Techniques, Proceedings of SPIE, Vol. 5684, p 265-273, 2005.
[20] 강병준, 박강령, : 속눈썹 추출 방법을 이용한 홍채 인식 성능 향상 연구, 한국정보처리학회 논문지 B, 제12-B권, 제3호, p. 233~238, 2005년 6월
[21] J. G. Daugman : High Confidence Visual Recognition of Persons by a Test of Statistical Independence, IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 15, No. 11, p. 1148-1161, 1993.
[22] Byunjun Son, Yillbyung Lee : Biometric Authentication System Using Reduced Joint Feature Vetor of Iris and Face, Lecture Notes in Computer Science, LNCS 3546, pp.513~522, 2005
[23] Song-yi Han, Kang Ryoung Park : Multi-modal Near-IR Face and Iris Recognition by Hierarchical SVM for Mobile Phone, Electronics Letters, Submitted

저 자 소 개

한 송 이(학생회원)
2006년 2월 상명대학교 소프트웨어학과 학사 졸업
2006년 3월~현재 상명대학교 일반대학원 컴퓨터과학과 석사 과정

<주관심분야 : Biometric 영상처리, 패턴인식, Digital Watermarking>

박 소 영(정회원)
1997년 2월 상명대학교 전자계산학과 졸업
1999년 2월 고려대학교 컴퓨터학과 석사
2005년 2월 고려대학교 컴퓨터학과 박사
2005년 상명대학교 소프트웨어학부 초빙교수
2006년 고려대학교 BK21 연구전임강사
2007년~현재 상명대학교 디지털미디어학부 전임강사

<주관심분야 : 자연어처리, 지능형 대화시스템, 기계학습>

박 강 령(정회원-주저자, 교신저자)
1994년 2월 연세대학교 전자공학과 졸업
1996년 2월 연세대학교 전자공학과 석사
2000년 2월 연세대학교 전기·컴퓨터공학과 박사
2000년 3월~2003년 2월 LG 전자 기술원 Digital Vision Group 홍채 인식팀
2003년 3월~현재 상명대학교 소프트웨어대학 디지털미디어학부 조교수

<주관심분야 : Biometric 영상처리, 패턴인식, 컴퓨터 vision, 컴퓨터 그래픽스>