모바일 클라우드 컴퓨팅에서의 스마트 뱅킹 인증 시스템에 관한 연구

김민선*, 송양의**
*동국대학교 정보보호학과, **동국대학교 컴퓨터공학과
e-mail: minseon90@nate.com, redcroix@dongguk.edu

A Study on Smart-Banking Authentication System using Mobile Cloud Computing

Min-Seon Kim*, Yang-Eui Song**
*Dept of Information Security, Dongguk University,
**Dept of Computer Engineering, Dongguk University

요 약

스마트 뱅킹을 사용하는 인구가 늘어나고 있으며 보안상의 위협이 대두되고 있다. 스마트 뱅킹의 경우 작은 보안상의 위험이 큰 금전적인 피해를 줄 수 있기 때문에 강력한 보안이 요구된다.

본 논문에서는 2-Factor 인증과 클라우드에 저장된 인증서를 통해서 스마트 뱅킹 서비스를 안전하게 사용하는 방법을 제안하였다. 인증서 중복저장에 의한 문제점을 해결하고자 인증서를 클라우드 서비스를 통해 제공하고, 저장된 인증서의 제3자에 의한 접근을 막기 위해 2-Factor 인증 기법으로 사용자를 인증한다.

1. 서론

스마트폰의 보급이 확산되고 성능이 증가함에 따라 모바일에서 제공되는 서비스도 늘어나고 있다. 그 중에서 스마트 뱅킹은 금융 서비스를 제공하므로 작은 보안상의 위험이 큰 금전적인 피해를 줄 수 있기 때문에 강력한 보안이 요구된다.

기존에는 스마트 뱅킹을 하기 위해 공인인증서를 필수적으로 요구하는 데 모바일 기기에 공인인증서를 저장하면 단말기 분실, 악성코드로 인한 정보 유출 등의 위협에 노출될 수 있다.

우리나라에서는 방송통신위원회가 '전자금융거래 인증방법의 안전성 가이드라인'을 발표함에 따라 2010년 하반기부터 전자금융거래 시 공인인증서 외에 인증방법을 적용할 수 있게 되었다[1]. 그러나 아직까지도 공인인증서를 대체할 인증방법이 나타나지 않고 있다.

최근에는 스마트폰이 주도하는 모바일 열풍과 결합하면서 새롭게 모바일 클라우드 컴퓨팅이 관심사로 떠오르고 있다. 공인인증서를 모바일 클라우드 컴퓨팅을 이용하여 클라우드 상에 저장하면 분실 등으로 인한 유출 및 중복 저장을 방지할 수 있다.

본 논문에서는 2-Factor 인증과 클라우드에 저장된 인증서를 통해 보안을 강화할 수 있는 스마트 뱅킹 알고리즘을 제안한다.

본 논문의 2장에서는 관련 연구를 서술하였고, 3장에서는 기존의 문제점을 분석하였다. 4장에서는 제안된 모바일 클라우드 컴퓨팅에서의 스마트 뱅킹 인증 알고리즘을 소개하였다. 5장에서는 결론 및 향후 과제를 언급하였다.

2. 관련 연구

2.1. 모바일 클라우드 컴퓨팅

클라우드 컴퓨팅이란 인터넷 상에서 데이터 저장, 네트워크, 콘텐츠 사용 등 IT 자원들을 최소한의 관리 노력 또는 제공자의 상호협력으로 신속하게 제공하여 사용자가 언제 어디서나 사용하고 공유할 수 있는 컴퓨팅 환경 및 기술을 말하고, 모바일 클라우드 컴퓨팅이란 모바일 단말에서 처리해야할 작업 및 데이터 저장의 일부를 클라우드 컴퓨팅 환경으로 이동시켜 처리한 후 결과를 서비스로 제공하는 것 또는 서비스를 의미한다[2-4]. 즉, 클라우드 컴퓨팅 개념에 모바일 장치의 휴대성을 접목하여 사용자가 언제 어디서나 클라우드 서비스를 제공받을 수 있는 환경이며 단말 자원 재사용을 위한 디바이스로서의 서비스(Device as a Service)를 위한 클라우드 기술이다.

모바일 클라우드 컴퓨팅을 위해선 기존의 클라우드 컴퓨팅에 단말 이동성, 고도 안정성, 쉬운 접근성, 서비스 확장성 등의 요구사항이 추가적으로 필요하다[5].

모바일 클라우드는 클라우드 컴퓨팅과 동일하게 서비스의 종류에 따라 IaaS, PaaS, SaaS로 구분되고 개방 여부에 따라 Private, Public, Hybrid로 분류된다[6].

2.2. 2-Factor 인증

2-Factor 인증이란 2가지 인증 요소를 조합하여 본인 여부를 판단하는 것으로써 안전성을 향상시키는 방법을 말한다. 기존 로그인 방식의 낮은 보안성, 비사용, 재사용, 공유, 망각, 도난, 입력 어려움, 키 로깅, 중간자 공격(MITM: Man-In-The-Middle) 취약점 등 다양한 보안상의 문제를 해결하기 위하여 이러한 Multi-factor인증(Authentication)방식의 도입이 요구된다.
강력한 인증 1가지를 사용하는 것보다 낮은 2가지를 조합하는 것이 더욱 안전한 인증이 된다.

인증 구분	설명	기반	종류
Type Ⅰ 인증	Something you know	지식	Password, PIN
Type Ⅱ 인증	Something you have	소유	스마트 카드, Token
Type Ⅲ 인증	Something you are	존재	얼굴, 홍채, 지문, 정맥
Type Ⅳ 인증	Something you do	행동	음성, 서명, keystroke

(그림 1) 인증 방식 종류 및 예

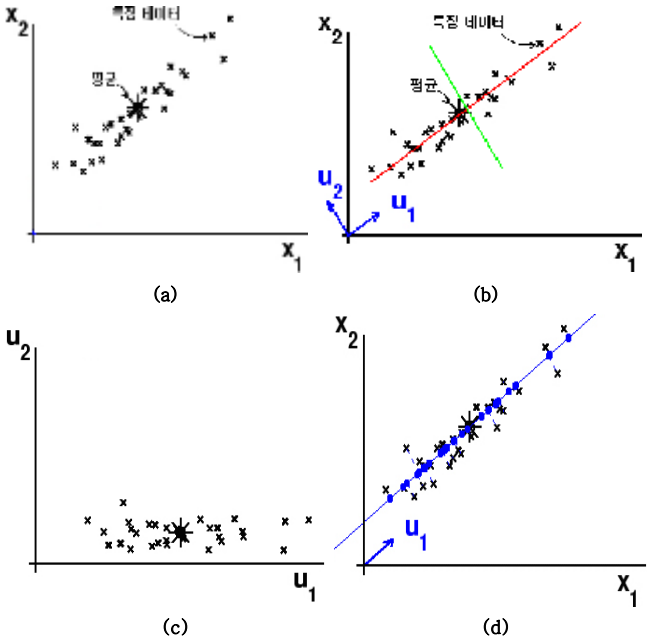
2.3. 얼굴 인식 기술

개인 정보 보안의 중요성이 증대함에 따라 사람의 신원을 확인하기 위하여 많은 기술이 개발되고 있다. 그 중에서도 단연 생체 인식이 각광을 받고 있다. 사람의 신체를 이용한 생체 인식은 분실할 위험이 없고, 잊어버릴 위험이 없으며 도용하기도 힘들어 그 중요성을 높이 인정받고 있다.

최근 생체 인식 중에서도 얼굴 인식(Face Recognition)은 여러 장점으로 인해 가장 활발히 연구가 진행되고 있다. 얼굴 인식은 타 인식(지문, 홍채, 정맥 등) 기술과 달리 고가의 전용 생체 인식 장비를 쓰지 않아도 스마트폰에 기본으로 장착되어있는 카메라로 인식할 수 있기 때문에 추가적인 비용이 들지 않는다. 또한 인식 대상의 특별한 동작이나 행위에 대한 요구 없이 카메라를 통해 얼굴에서 중요 부분(눈, 코, 입)들을 추출하여 영상으로 인식하는 비 접촉식이므로 자연스럽게 신원을 확인하고 인식 대상으로 하여금 거부감을 줄일 수 있다[7].

2.3.1. 주성분 분석(Principal Component Analysis)

KL(Karhunen-Loeve, 카루넨-루베)변환 또는 Hotelling(호텔링) 변환[8]이라고 불리는 주성분 분석(PCA: Principal Component Analysis)은 템플릿 정합 방식의 대표적인 방식 중의 하나로 고유 얼굴(Eigenface)의 가중치 조합을 통해 원본 영상에 가깝게 영상을 복원할 수 있다는 점에서 가장 효율적인 기법으로 인식되고 있다[9]. 이 PCA는 현재 얼굴 인식 분야에서 가장 널리 알려져 있고, 많이 쓰이는 기법이다. 원래의 데이터를 완전히 표현하기 위해 n개의 주성분(N차원)이 필요하지만 정보의 손실이 최소가 되도록 k개의 주성분(K차원)으로 요약함으로써 차원을 줄이되, 원본 데이터와의 차이를 최소화 할 수 있다. 또한 PCA 기법은 얼굴의 전체적인 형태를 잘 반영한다[10].



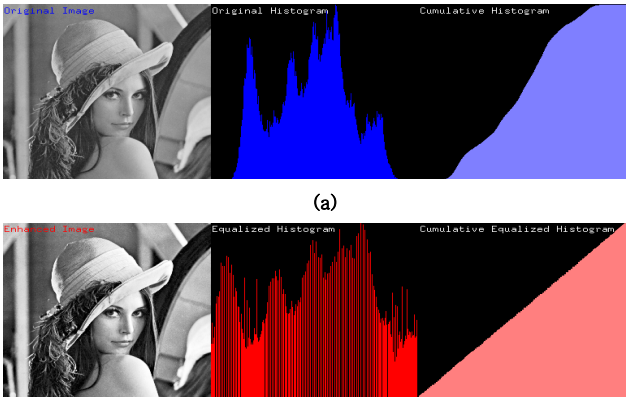
(그림 2) Principal Component Analysis

(그림 2)는 2차원의 데이터를 1차원의 데이터로 축소하는 과정을 나타낸 것이다. (a)는 데이터 간의 관계를 알아내어 특징을 뽑아낸 원본 PCA 데이터이고, (b)는 주성분 계산 및 주축을 확인하는 과정이다. (c)는 주성분이 주축을 이루도록 데이터를 회전을 한 결과이며, (d)는 원본 데이터를 주성분으로 사영(projection)시켜 1차원 데이터로 차원을 축소한 결과이다.

2.3.2. 히스토그램 평활화(Histogram Equalization)

히스토그램 평활화(Histogram Equalization)는 영상 픽셀 값의 동적 영역을 변경시키는 방법 중 하나이다. 히스토그램 평활화는 히스토그램을 평균화하는 것이 아니라 명암도의 분포를 균일하게 해주는 것으로써, 명암도 분포가 고르지 않고 한쪽으로 치우쳐 있는 히스토그램을 인위적으로 재분배 과정을 통해 일정한 분포를 가진 히스토그램으로 만드는 알고리즘이다[9].

히스토그램 평활화는 궁극적으로 평탄한 분포를 가지는 히스토그램을 생성하기 위한 것이다. 그러나 히스토그램 변환 함수에 너무 의존한 나머지 변환 영상의 밝기 값이 과도하게 변한다는 문제점이 발생한다. 즉, 원 영상 내에서 어두운 부분에 대하여 변환함수를 적용할 땐 유용하나, 밝은 부분에 대하여 변환함수를 적용했을 때에는 오히려 화질이 떨어지는 역효과를 일으킨다.

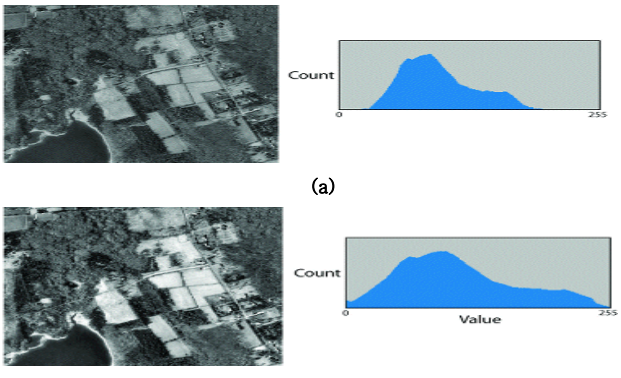


(그림 3) (a) 원 영상, (b) Histogram Equalization을 적용한 결과 영상

2.3.3. 명암대비 스트레칭(Contrast Stretching)

명암대비 스트레칭(Contrast Stretching)은 영상의 명암대비를 조절하여 눈, 코, 입 등의 특징 부분을 강조할 수 있다. 영상의 명암도 분포를 최대한 활용하도록 히스토그램 픽셀 분포를 펼쳐주는 역할을 한다.

낮은 명암 대비에서 히스토그램의 화소가 양 끝 또는 중앙에 밀집되어 나타나거나, 높은 명암 대비에서 히스토그램의 왼쪽과 오른쪽에 큰 마루가 생기는 데 이런 경우에 Contrast Stretching을 사용하여 히스토그램의 분포를 넓힐 수 있다[11].



(그림 4) (a) 원영상, (b) Contrast Stretching을 적용한 결과 영상

Contrast Stretching은 크게 기본 명암 대비 스트레칭과 엔드-인 탐색 기법(End-In Search)이 있다. 기본 명암 대비 스트레칭은 특정 부분에 명암도가 치우쳐있는 영상에 적용하는 기법이고, 엔드-인 탐색기법은 영상의 명암도가 넓게 분포하고 있지만 히스토그램에서 특정한 골이나 마루가 있을 때 사용하는 기법이다[12].

3. 문제점 분석

3.1. 기존 스마트 뱅킹의 문제점

① 분실/도난에 의한 문제점

PC 상의 인터넷 뱅킹과 달리 스마트 뱅킹은 스마트폰의 휴대성(이동성)으로 인해 분실/도난의 위험이 크다. 스마트폰의 분실/도난에 따른 직접적인 경제적 피해와 더불어 스마트폰에 저장된 개인 정보들이 유출될 수 있다[13]. 특히 공인인증서의 유출로 인해 2차적인 금융 피해가 발생할 수 있어 문제가 되고 있다.

② 악성코드에 의한 문제점

스마트폰은 사용자가 원하는 어플리케이션의 다운로드와 실행이 자유롭다는 특징이 있다. 또한 디바이스가 항상 켜져 있고 무선 인터넷에 빈번하게 연결하는 등으로 인해 해킹 및 바이러스에 대한 노출이 잦다. 스마트폰의 또 다른 특징인 개방성은 일반 폰과는 다르게 외부 인터페이스를 개방하여 제공하고 있고 앱 개발 시 시스템 자원의 사용을 위해 SDK를 이용하여 API를 제공하고 있다. 이는 악성코드 전파 경로의 다양성을 제공하고 악의적인 목적을 가진 개발자가 악성코드가 은닉된 모바일 앱(어플리케이션)을 제작하는 데 용이하게 만드는 취약점을 가지고 있다. 악성 앱을 정상적인 앱으로 가장하여 배포할 경우 사용자의 스마트폰에서 주소록, 전화번호, 인증서 정보 등의 개인정보들이 유출될 수 있고 원하지 않는 서비스를 이용한다거나 좀비폰으로 사용될 위험성이 존재한다[13,14].

③ 중복 저장에 의한 문제점

스마트 뱅킹을 하려면 공인인증서를 요구하게 된다. 하지만 MS 기반의 플랫폼을 제외한 다른 플랫폼 기반 스마트폰은 자체적으로 공인인증서를 사용할 수 없기 때문에 각 금융 서비스 제공업체가 앱 형태로 인증서 모듈과 인증서를 저장하여 배포하면 사용자는 그 앱을 설치한 후 금융 서비스를 받을 수 있다. 사용자가 여러 은행과 거래할 경우 금융 서비스를 받기 위하여 다수의 앱과 인증서를 저장해야한다. 이 때 스마트폰에서 어플리케이션 간의 공간은 서로 독립적이기 때문에 불필요하게 다수의 인증서가 메모리에 저장되므로 공간이 낭비된다는 문제점이 있다[15].

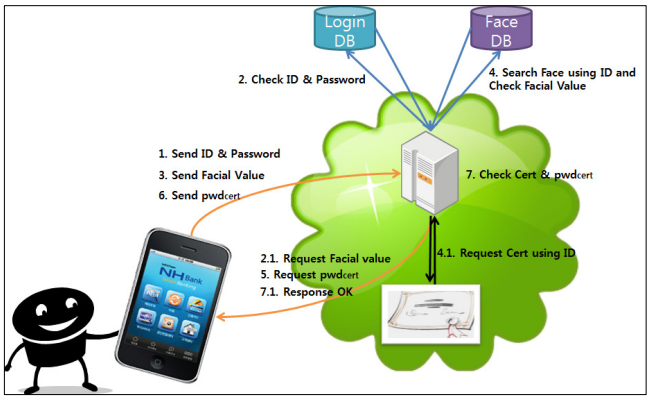
3.2. 얼굴 인식의 문제점

얼굴 인식은 앞에서 언급한 바와 같이 뛰어난 장점들을 지니고 있으나 실제로 응용되기에는 몇 가지 문제점을 지니고 있다. 예를 들어 낮, 밤과 같이 조명의 차이에 의한 변화는 같은 얼굴 임에도 불구하고 인식을 못하는 경우가 발생한다. 또한 얼굴의 표정, 변장(화장, 안경, 마스크, 모자), 주변 환경 등에 민감하고 카메라와 인식 대상 간의 거리, 인식 대상의 자세에 따라 얼굴의 크기와 회전 그리고 위치의 이동 등 인식 대상의 가변성이 커서 인식률이 낮아지는 단점이 있다[10]. 이는 정상적인 사용자임에도 불구하고 인식이 되지 않는 문제점이 발생하여 사용자 편의성을 저해할 우려가 있다. 보안성 측면에서는 카메라에 사람 얼굴이 아닌 사진을 대고 인식을 해도 인증이 될 수 있으므로 큰 위험이 있다.

4. 제안 시스템 설계

4.1. 스마트 뱅킹 인증 시스템 및 알고리즘

본 논문에서 제안하는 모바일 클라우드 컴퓨팅에서의 스마트 뱅킹 인증 시스템의 구성도와 알고리즘은 (그림 5), (그림 6)과 같다.



(그림 5) 모바일 클라우드 컴퓨팅에서의 스마트 뱅킹 인증 시스템

1. 클라우드에 로그인하기 위하여 ID와 Password를 입력한 후 인증 서버에 전송한다.
2. 클라우드 인증 서버에서 ID와 Password가 맞는지 확인한다.
   2.1. ID와 비밀번호가 일치하면 사용자에게 얼굴값을 요청한다.
   2.2. ID와 비밀번호가 맞지 않으면 로그인 화면으로 돌아간다.
3. 사용자는 모바일 기기의 카메라를 이용하여 얼굴 영상을 전송한다.
4. 클라우드 인증 서버에서 사용자가 보낸 얼굴과 데이터베이스에 저장되어 있는 얼굴을 비교하여 일치하는 지 확인한다.
   4.1. 일치할 경우 인증이 되면 해당 사용자의 공인인증서를 공인인증센터에서 요청하여 가져온다.
   4.2. 일치하지 않을 경우 로그인 화면으로 돌아간다.
5. 사용자에게 공인인증서 비밀번호를 입력하도록 요구한다.
6. 모바일 뱅킹 인증 서버에 공인인증서 비밀번호를 전송한다.
7. 인증서버에서 공인인증서 비밀번호가 맞는 지 확인한다.
   7.1. 인증이 되면 모바일 뱅킹의 기능을 사용한다.
   7.2. 인증이 되지 않으면 공인인증서 비밀번호를 다시 요구한다.

(그림 6) 스마트 뱅킹 알고리즘

(그림 5)의 Login DB에는 사용자의 ID와 비밀번호가 저장되어 있고 Face DB에는 사용자 ID 별로 얼굴값이 저장되어 있으며 클라우드 저장소에 공인인증서가 저장되어 있다. 인증 서버는 ID&Password 인증 및 얼굴 인식, 공인인증서 인증 등 모든 인증을 담당하는 서버이다.

사용자가 스마트 뱅킹 앱에 접속하여 조회, 이체, 환전 등의 업무를 선택했을 때, 클라우드 내에 있는 공인인증서를 사용하기 위하여 두 가지 인증을 사용함으로써 제3자의 공인인증서 도용을 막는 등 보안성을 강화할 수 있다.

4.2. 얼굴 인식 알고리즘 및 시스템

3.2.에서 언급한 얼굴 인식의 문제점을 스마트 뱅킹 인증용 데이터의 특성과 함께 고려했을 때, 얼굴 인식 시스템에 그대로 적용하면 좋은 성능을 기대하기 어려울 뿐만 아니라 보안성과 사용자 편의성을 크게 해칠 우려가 있다. 그러므로 사진일 경우 인증하지 못하게 하고 PCA를 기반으로 하되 주변 환경의 영향을 최소화하면서 조명 문제까지 해결할 수 있는 알고리즘을 고려해야 한다.

(그림 7)은 제안하는 스마트 뱅킹 시스템 중에서 보안을 강화하고 신뢰성을 높이기 위한 얼굴 인식 시스템의 알고리즘을 간략하게 나타낸 것이다.

1. 움직임을 최소화한 상태에서 사용자의 영상을 입력받은 후 얼굴 영역을 검출한다.
2. 연속된 프레임 간 차영상을 구하여 픽셀 값을 확인했을 때 차영상의 픽셀 값이 χ 이상일 경우 255, 미만일 경우 0으로 치환한 후 외곽을 검출한다.
   2.1. 외곽이 2개일 경우 눈 깜박임으로 인식하고 다음 단계로 간다.
   2.2. 외곽이 2개가 아닐 경우 다시 시도한다.
3. PCA를 이용해 데이터베이스에 있는 대조군과의 거리를 구한다.
   3.1. 구한 거리가 α값 내에 있으면 인증에 성공하고 종료한다.
   3.2. 구한 거리가 α값을 초과하면 다음 단계로 간다.
4. 입력된 영상에 Histogram Equalization을 수행한 후 데이터베이스에 있는 대조군과의 거리를 구한다.
   4.1. 구한 거리가 β값 내에 있으면 인증에 성공하고 종료한다.
   4.2. 구한 거리가 β값을 초과하면 다음 단계로 간다.
5. 입력된 영상에 Contrast Stretching을 수행한 후 데이터베이스에 있는 대조군과의 거리를 구한다.
   5.1. 구한 거리가 ɣ값 내에 있으면 인증에 성공하고 종료한다.
   5.2. 구한 거리가 ɣ값을 초과하면 인증에 실패하고 종료한다.

(그림 7) 얼굴 인식 알고리즘

제안한 얼굴 인식 알고리즘은 주변 환경의 영향을 최소화하기 위해 얼굴 영역만을 검출하고 연속된 영상 프레임의 픽셀 차를 이용하여 눈 깜박임을 인식한 후 테스트 영상을 데이터베이스에 저장되어있는 영상과 비교한다. 테스트 영상과 대조군의 유사도 값을 정량적으로 계산하여 지정된 Threshold 값(α, β, ɣ) 범위 내에 있으면 같은 사람이라고 판단하고, 그렇지 않으면 입력된 영상에 변화를 준다. 변경된 영상이 원본 영상에 가까워질수록 높은 상관관계를 가지므로 얼굴 인식률은 상대적으로 높아진다. 또한 눈 깜박임을 인식한 후 비교함으로써 사진이 아닌 살아있는 사람의 얼굴임을 증명할 수 있다.

픽셀 값을 치환하는 기준 값 χ는 외부 요인(예를 들면 밝기, 움직임, 잡음)을 고려하여 실험을 통해 정한다. 또, 최적의 threshold 값(α, β, ɣ)은 얼굴 인식률이 가장 높은 값을 뜻하며 이 최적의 Threshold 값을 찾기 위해 0.01단위로 세밀하게 실험을 실시한다. 알고리즘의 얼굴 인식률은 식(1)과 같이 평가한다.

$$\text{인식률} = \frac{Success}{Success + Failed} \times 100 \quad \cdots\cdots\cdots\cdots \text{식 (1)}$$

Success는 각 테스트 영상이 데이터베이스에 있는 각 대조군과 일치하는 데이터 개수이고, Failed는 일치하지 않는 데이터 개수이다. 이러한 실험을 각 Threshold 당 10회씩 실행하고, 그 평균으로 최종 인식률을 측정한다.

최적의 Threshold(α)는 PCA를 수행한 후 Histogram Equalization을 했을 때, 인식률을 가장 많이 향상시킬 수 있는 threshold 값이다. 최적의 Threshold(β)는 PCA, Histogram Equalization을 수행하고 난 후 Contrast Stretching을 수행했을 때, 인식률이 가장 향상될 수 있는 threshold 값이다. 즉, 앞에서 최적화 된 Threshold(α)를 찾았으므로 Threshold(α)를 고정시킨 후 실험을 진행하여 최적의 Threshold(β)를 찾는다. Threshold(ɣ)는 PCA, Histogram Equalization, Contrast Stretching을 모두 수행하고 난 후 인증 실패의 기준이 되는 값이다. 이 Threshold(ɣ)는 최적의 Threshold(α), Threshold(β)를 고정시킨 후 실험을 진행한다.

5. 결론 및 향후 과제

본 논문에서는 스마트 뱅킹에서 공인인증서를 사용하기 위해 모바일 클라우드 컴퓨팅을 활용하는 방법을 제안했다. 이는 기존 시스템과 달리 공인인증서에 대한 별도의 플러그인 설치로 인한 번거로움, 공간의 낭비를 줄일 수 있으며, 공인인증서를 스마트폰 내에 저장하여 관리하는 것이 아니라 모바일 클라우드 상에 저장하고 관리하므로 스마트폰의 분실 또는 악성코드 감염 등의 위험으로부터 공인인증서를 보호할 수 있다. 또한 모바일 클라우드 컴퓨팅에서 보안 강도를 높이기 위하여 ID & Password 방식과 얼굴 인식을 결합한 2-Factor 인증 방식의 사용자 인증을 제안했다. 제안한 방식은 모바일 기기의 장점인 얼굴 인식을 위해 별도의 장비가 필요하지 않다는 점, 사용자 거부감을 줄일 수 있다는 점을 활용했다. 특히 보안성과 사용자 편의성 모두를 고려하기 위해 얼굴 인식률을 향상시켰다.

본 논문은 모바일 클라우드 자체는 신뢰성이 있다고 가정하고 있으므로 모바일 클라우드 서비스의 위협 요인인 서비스 불능, 가상화 기술 위협 등에 대해선 연구 과제로 남겨져 있다.

참고문헌

[1] 전자금융거래 시 인증방법에 대한 가이드라인
[2] 이강찬, 이승윤, “모바일 클라우드 표준화 동향 및 전략”, 한국통신학회지(정보와 통신) 제28권 제10호, 2011, 9월
[3] F.A.Samimi, P.K.McKinley, S.M.Sadjadi, “Mobile Service Clouds: A Self-managing Infrastructure for Autonomic Mobile Computing Services”, Proceedings of the Second International Workshop on Self-Managed Networks, Systems & Services (SelfMan 2006, June 2006, Dublin, Ireland)
[4] NIST, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, Sep. 2011
[5] 이강찬, “모바일 클라우드 개념과 기술 동향”, 한국정보통신기술협회, TTA 저널 139권, 2012, pp.54-58
[6]정보통신산업 진흥원, SaaS 시장 및 기술 동향 연구, 2009
[7] 배경율, "인터넷 뱅킹의 사용자 인증을 위한 얼굴인식 시스템의 설계", 한국지능정보시스템학회논문지, 2003, 12월, pp.193~205
[8] Z.Sun, G.Bebis, X.Yuan, S.J.Louis, "Genetic Feature Subset Selection for Gender Classification : A Comparison Study", Applications of Computer Vision, 2002(WACV 2002). Proceedings Sixth IEEE Workshop on, Dec.2002, pp.165-170
[9] 신상일, "PCA 기법과 히스토그램 평활화를 이용한 얼굴 인식에 관한 연구(A Study on the Face Recognition using PCA and Histogram Equalization)", 광운 대학교 정보 통신 대학원 컴퓨터 공학 전공, 석사학위 논문, 2006
[10] 경북대학교 전자기술 연구소, 초고속 통신망에서 인간 시각 시스템 특성에 기반한 신원확인 시스템 개발에 관한 연구, 1999
[11] 장준영, “미술품의 양식과 도상학의 분석을 위한 이미지 블랜딩”, 세종대학교대학원 디지털 콘텐츠 학과, 2008, pp.22-23
[12] 유명현, 박정선 등, “얼굴 기반 생체 인식 기술의 현황과 전망”, 정보과학회 논문지, 19권 7호(2001), 22-31
[13] 강동호 외 6명, “스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석 제 25권 제3호, 2010, 6월
[14] “모바일 클라우드 컴퓨팅을 이용한 스마트폰 뱅킹에서 공인인증서 관리 방안”, 대한전자공학회 하계학술대회, 2010
[15] 이상걸, “클라우드 환경에서의 모바일 뱅킹 시스템”, 2011, 6월