한국지능정보시스템학회논문지 제9권 제3호 2003년 12월(pp.193~205)

인터넷 뱅킹의 사용자 인증을 위한 얼굴인식 시스템의 설계

배경율
상명대학교 소프트웨어학부
(jbae@smu.ac.kr)

본 논문에서는 인터넷 뱅킹의 사용자 인증에 있어 더 강인성(Robustness)을 갖춘 인증 시스템을 위해서 생체의 특징을 이용해 신분을 증명 또는 인증하는 생체인식 기술 중 지문이나 장문, 정맥, 홍채를 이용한 인식과 같이 장비에 접촉해야만 것과 달리 거부감이 없고, 별도의 전문 장비를 필요로 하지 않아 일반 대중들에 쉽게 접근할 수 있는 얼굴인식을 이용해 인증 시스템의 설계 및 구현을 제안한다. 얼굴인식 알고리즘은 얼굴 특징을 분석하는 방식에 따라 PCA (Principal Component Analysis), ICA (Independent Component Analysis), FDA (Fisher Discriminant Analysis) 등이 발표되어 있다. 이들 중 가장 기본적인 알고리즘이라 할 수 있는 PCA를 이용해 얼굴 특징을 분석하고 암호화된 형태의 생체 데이터를 전달해 분석한 결과를 원격지에 신속하고 정확하게 송수신할 수 있는 인터넷 뱅킹에서의 사용자 인증을 위한 얼굴인식 시스템의 설계 방법을 제안한다.

논문접수일 : 2003년 10월 게재확정일 : 2003년 12월 교신저자 : 배경율

1. 서론

인터넷 뱅킹과 사이버 머니등과 같이 인터넷 상의 데이터가 현금과 같이 이용되는 가치창출 수단이 되면서 개인의 정보가 중요한 사용자 증명수단으로서 활용됨에 따라 신뢰할 수 있는 인증수단이 요구되면서 최근에는 사람의 신체 일부를 비밀번호처럼 사용하는 생체인식 시스템에 대한 관심이 급증하고 있으며, 지문이나 장문, 홍채, 정맥, 얼굴인식의 경우 상용화되어 보안 분야에서 두각을 보이고 있다.

그러나 지문이나 장문, 홍채, 정맥인식의 경우 장비 또는 적외선에 접촉해야 하는 거부감이 있으며, 고가의 장비를 필요로 하기 때문에 일반 대중에 널리 활용하기 어려울 뿐만 아니라 등록 및 인식하는데 많은 시간이 요구돼 인터넷 상의 신분 증명 및 인증에서는 활성화되지 못하고 있는 실정이다.

반면에, 생체 인식기술 중에서도 개인얼굴의 특징을 이용하는 얼굴인식 기술은 특징점 추출이 용이하고 타 인식 기술에 비해 거부감이 없으며, 특히 고가의 전용 하드웨어가 아닌 범용 PC카메라(웹 캠)와 같이 사용자가 쉽게 접할 수 있는 장치를 이용하는 장점을 갖고 있으며, 접촉식이 아니므로 입력과 관련된 해킹에 대한 대비 및 사용자 편의성 측면에서 웹 적용에 가장 이상적인 시스템의 구현이 가능하다.

본 논문에서는 각종 생체인식기술의 인터넷

뱅킹에의 응용 가능성에 대하여 평가를 수행하고, 인터넷 뱅킹의 사용자 인증 측면에서 얼굴인식의 장점과 얼굴인식의 강인성을 보완할 수 있는 여러 분석법에 대해 살펴볼 것이다.

또한, 얼굴인식 기법 중 PCA 분석법으로부터 나온 얼굴 데이터를 인터넷 뱅킹에 이용할 수 있는 시스템을 설계하고자 한다.

2. 관련 연구

2.1. 생체인식 기술의 비교

일반적인 비밀번호 방식의 인증 시스템은 비밀번호가 노출될 경우 이를 쉽게 도용 및 남용할 수 있어 인증에 필수적 요소라 할 수 있는 비밀성, 무결성, 가용성 및 부인 방지의 기능을 만족시키지 못하고 있다(Bolle, R. M. et al. 1999).

은행 연합회의 보고서에 따르면 ATM에서의 타인 수락(False Acceptance)은 거의 30%에 이르고 있으며, 인터넷 뱅킹의 타인 수락으로 인한 손실도 하루에 수백 만 불에 달한다고 한다. 따라서, 최근에는 보다 안전하고 강화된 신분확인을 위한 기술로서 생체인식이 각광을 받고 있다.

생체인식 기술을 인터넷 뱅킹에 도입시 고려해야 할 가장 중요한 사항으로는 타인 수락을 철저히 예방할 수 있는 신뢰성(Reliability)이며, 사용자의 생체정보를 등록하고 인증하는 과정에 있어 간편성과 시스템의 편의성이 수반되어야만 한다(Michael. K. and L. Sirovich, 1990). 지나친 보안을 강조하게 되면 시스템의 구조가 복잡해지고 등록 및 인증에 많은 시간을 허비해야 하므로 서비스 시간이 증가하게 되어 신속한 인증 처리와 서비스 이용을 위한 인터넷 뱅킹의 특성에 부합하지 않게 된다. 이에 대한 각 생체인식 유형별 보안성 및 등록, 인증 편의성의 비교는 <표 1>과 같다.

두 번째 고려사항으로는 사용자의 아이디나 비밀번호는 자의적으로 수정을 가하지 않는 한 종생불변하게 된다(Blackburn et al. 2001). 이와 마찬가지로 등록된 생체정보는 생리적 변화나 물리적인 변경이 없는 한 변경되어서는 안되며, 주민등록번호와 같이 유일해야만 하는 특성을 강인성(robustness)이라 한다. 이 특성에 대한 생체인식 유형별 비교는 <표 2>와 같다.

2.2. 얼굴 인식 기술

얼굴인식 기술에는 여러 가지가 있다. 첫째로 주성분분석(PCA: Principal Component Analysis)

<표 1> 생체인식 유형별 특징 비교 [6]

분 류	얼굴	지문	홍채	정맥
보안성	보통	보통	높음	보통
등록 용이성	높음	높음	보통	보통
등록 및 인증속도	높음	높음	높음	보통
인증방법의 적응성	높음	높음	높음	높음
사용자 거부감	낮음	보통	높음	보통
전용장비의 필요성	무	유	유	유
강제성	낮음	높음	보통	높음

<표 2> 생체인식 유형별 강인성 비교 [6]

분류	얼굴	지문	홍채	정맥
종생불변	낮음	높음	높음	보통
유일무이	보통	높음	높음	보통
변화요인	얼굴의 심한 변형 유전적 요인	지문의 손상 지문의 변형	장님 또는 안구 손상, 변형	정맥 패턴의 유사 또는 변형

이 있다. PCA 분석법은 벡터표현의 통계적 특성을 기반으로 한 방법으로 Karhunen-Loeve 근사법으로 부르기도 하며, 통계적으로 변화가 있는 N차원의 M개의 벡터를 공분산(Covariance) 행렬에 의해 고유 벡터(EigenVector)로 표현한다. 이 분석법은 서로 다른 공간의 차원을 줄여서 간단히 표현하는 실용적인 방법으로 널리 알려져 있다.

PCA의 기본적인 아이디어는 전체 영상공간에서 얼굴을 가장 잘 표현할 수 있는 벡터를 찾는데 있다. 다시 말해서 원래의 얼굴 영상에서 일치하는 공분산 행렬의 고유벡터(EigenVector)를 찾는 것이다. 여기서 고유벡터는 얼굴처럼 표현되기 때문에 고유얼굴(EigenFace)이라는 용어를 사용하며, 주성분은 얼굴의 눈, 코, 입과 같은 세부적인 표현이 아닌 얼굴 전체에 대한 표현이므로 국부적 특징 추출에 있어서는 응용하기 어려운 단점을 갖고 있다(Turk and Pentland, 1991).

둘째로 얼굴의 국부적 특징을 다른 얼굴로부터 잘 분리해 표현할 수 있도록 만들어진 방법이 바로 FDA(Fisher Discriminant Analysis)분석법이다. PCA분석법이 인식에 적용될 경우 가장 큰 단점은 영상의 변화가 객체(Object)의 변화인지 아니면 객체 외의 환경변화 즉, 조명이나 표정의 변화 때문인지를 명확히 구분하지 못하는데 있다. 특히, 인터넷 뱅킹은 가정이나 회사와 같이 다양한 장소에서 인증을 시도하게 되므로 조명이나 환경변화에 민감하게 된다. FDA분석법은 바로 객체의 변화와 그 밖에 다른 요인에 의한 변화를 판별할 수 있도록 하자는 것이다. 따라서, 어떤 객체(사람)가 등록할 때와 다른 조명에서 인증을 시도하였을 경우 변화의 요인은 조명의 변화이므로 객체는 동일하다는 사실을 구분 지을 수 있도록 하자는데 그 목적이 있다. 이때, 분석법의 효율성을 높이기 위해서는 인식을 원하는 객체마다 조명이나 표정 등이 다른 다양한 영상을 되도록 많이 보유하는 것이 중요하다.

셋째로 ICA(Independent Component Analysis)가 있다. ICA분석법은 특징의 차원이 커서 분류하기 어려운 문제를 해결하기 위해 특징분류에 있어 중요한 영향을 미치는 특징만을 고른다는 점에서는 PCA분석법과 비슷하다고 할 수 있다. 그러나, 기존의 주어진 특징만으로는 전체얼굴 이외의 특정영역에 대한 분류가 어렵기 때문에 ICA분석법에서는 주어진 특징으로부터 새로운 특징을 추출해내는 방식을 취한다. 분류되지 않은 특징들 중 확률적으로 독립(independent) 성분을 충분히 포함하고 있는 새로운 특징을 추출함으로써 PCA분석법의 단점을 보완할 수 있다(Swets and Weng, 1996).

3. 인터넷 뱅킹을 위한 생체인식 기술

생체인식 기술을 인터넷 뱅킹의 인증시스템에 적용하기 위해서는 웹의 특성에 부합하는가에 대한 검토가 필요하다. 각 유형의 생체인식 시스템들은 나름대로 장단점을 가지며, 유형별로 웹과 연관하여 성능 및 적용가능성을 포함해 고려해야 하는 사항을 <표 3>에서와 같이 분류할 수 있다.

3.1. 생체정보 인식속도 및 인식용 템플릿 크기 비교

앞의 관련연구에서 설명한 강인성은 생체인식 시스템의 인증 정확성과 생체정보에 대한 신뢰성을 높이는 측면에서 중요한 요인이 된다. 그러나, 강인성을 갖추기 위해서는 복잡한 계산과정의 증가로 인해 등록 및 인증의 편의성이 떨어지며 (Liu, C. and H. Wechsler,2000), 보다 정확한 생체정보의 송수신을 요함으로써 원격지에서 뱅킹 서버로 전달되는 생체정보의 템플릿 크기가 증가하고, 송수신 속도의 저하를 가져오게 된다.

따라서, 강인성과 함께 생체정보의 전달 속도 및 전달 생체정보의 크기를 함께 수용할 수 있는 생체인식 시스템의 설계가 중요하다. <표 4>는 생체인식 유형별 생체정보의 인식 속도 및 인식용 템플릿의 크기를 비교한 것이다.

원격지에서 사용자의 신분을 확인하는 인증서버 또는 인증기관과의 송수신에 소요되는 시간은 인식속도와 생체 템플릿 크기에 비례한다. 즉, 인식속도가 빠르면 빠를수록, 생체 템플릿 크기가 작으면 작을수록 송수신에 소요되는 시간은 줄어들게 된다. 다만 네트워크 트래픽과 인증서버 또는 인증기관의 처리율에 따라 평균송수신 속도에 영향을 줄 수 있다.

기존의 인터넷 뱅킹 인증 시스템은 별도의 장비없이 소프트웨어로만 처리로 가능하기 때문에

<표 3> 생체인식 적용시 고려사항

웹의 특성	고려 사항
사용의 편의성	생체정보 등록 및 인증의 편의성
사용자 친화성	등록 및 인증시 사용자 거부감
정보의 불변성	생체정보의 강인성(Robustness)
정보 이동의 신속성	생체정보 송수신 속도
정보 이용의 저비용성	생체정보 획득장비 및 시스템 크기
하이퍼링크 개념	장소의 제약성
데이터의 은닉성	생체정보의 은닉성 및 보안성

<표 4> 인식속도 및 인식용 템플릿 크기 비교 [6]

분류	얼굴	지문	홍채	정맥
인식속도	1.8-3초 이내	2-3초 이내	3-5초 이내	2-3초 이내
템플릿 크기	84-1,300 (byte)	250-1,200 (byte)	512 (byte)	256-512 (byte)

<표 5> 생체인식 시스템 및 장비 비교 [6]

분류	얼굴	지문	홍채	정맥
시스템크기	작음	작음	보통	큼
객체획득 장비	PC 캠 카메라 30만 화소 이상	지문 스캐너	CCD 카메라, Frame Grabber	적외선 조명, CCD 카메라, Frame Grabber

하드웨어와는 독립적인 형태를 보인다. 생체인증 역시 생체데이터를 얻기 위해 소프트웨어를 통한 전처리 과정을 거친다. 그러나, 생체 인식 시스템은 전처리 과정 이전에 객체(Object)를 인식하기 위한 별도의 하드웨어 장비가 필요하다. 또한, 각 인식 유형별로 전처리 과정을 위한 시스템 크기가 달라진다. 요구되는 장비와 시스템 크기에 대한 비교 결과는 위의 <표 5>를 통해 확인할 수 있다.

인터넷 뱅킹 상의 인증처리를 위한 생체인식 시스템의 크기는 생체정보의 송수신 속도에 영향을 준다. 전처리 과정에 소요되는 시간이 길면 길수록 인증 전체에 소요되는 시간이 증가하게 되고, 이는 사용자 편의성을 떨어뜨리고, 사용자로 하여금 거부감을 증가시킨다.

4. 인터넷 뱅킹을 위한 얼굴인식 기술의 제안

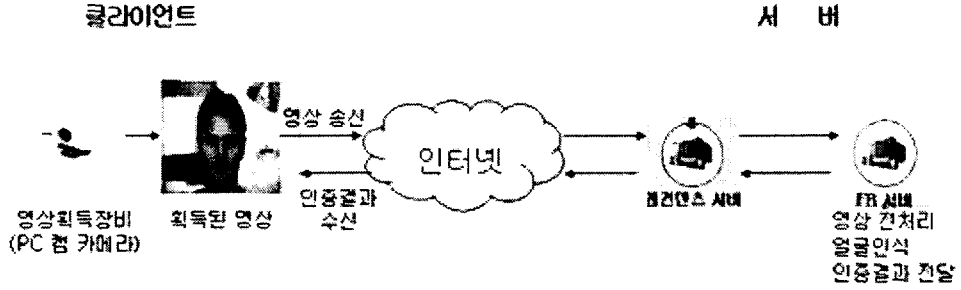
앞에서 살펴본 바와 같이 얼굴인식 기술이 인터넷 뱅킹에 적용하기에 효율적인 기술임을 살펴보았다. 원격지에 위치한 클라이언트의 얼굴을 인증해 현금 서비스를 제공하기 위해서는 크게 세 가지 방식으로 접근할 수 있다. 첫째, 서버 중심 접근법(Server Centric Approach)과 둘째로, 클라이언트-서버 분산 접근법(Distributed Client-Server Approach)이 있으며, 셋째로 보안을 강화한 다중 키 분산 접근법(Multi-key Distribution Approach)이 있다

4.1. 서버중심 접근법

서버 중심 접근법은 원격지에 위치한 클라이언트에 대해서 금융사와 직접 연결돼 인증하는 가장 기본적인 방법이라 할 수 있다. 즉, 영상획득장비로부터 입력된 인증 요청자의 영상을 인터넷을 통해 얼굴인증을 처리하는 뱅킹 서버로 전송하는 방식으로 인증 요청자의 시스템이 저 사양일 경우에 유리하다. 클라이언트 PC에서 처리되는 비중이 낮기 때문에 클라이언트PC의 리소스를 최소화할 수 있기 때문이다.

그러나, 클라이언트로부터 송신된 영상이 인증처리하기에 충분히 좋은 품질을 지녔는지 알 수 없고, 송신된 영상을 얼굴인식 모듈로 처리하기 이전에 전처리하는 과정이 필요하다. 이때 인증을 요청하는 사용자의 수가 증가할수록 전처리에 소요되는 시간과 얼굴을 인식해서 인증결과를 전송하는 시간이 비례해서 증가하므로 인증속도 및 서비스 제공 효율이 급격히 저하되는 문제가 발생하게 된다. 아래의 <그림 1>에서는 서버 중심 접근법의 간략한 구조를 나타내었다.

<그림 1>에서 보듯이 클라이언트의 영상획득 장비로부터 정확히 얼굴영상이 획득된 좋은 품질의 영상이고, 등록된 영상 역시 좋은 품질로 등



<그림 1> 서버중심 접근법의 구조

록되었을 경우는 인증이 쉽게 이루어진다. 그러나, 획득된 영상이 얼굴이 아니거나 저품질의 영상일 경우는 인증이 성공할 때까지 반복적으로 인증처리를 위해 송수신 되는 횟수가 증가하게 되고, 이로 인한 인증속도의 저하와 다른 사용자의 인증 대기시간이 증가하는 커다란 결함을 갖게 된다. 또한, 획득된 고품질의 영상(최소 226KB 크기의 BMP 영상파일)을 서버에 전달해야 하므로 네트워크 트래픽 양이 증가해 병목(Bottle-neck)현상을 일으킬 수 있는 단점을 갖고 있다. 특히, 금융권의 서버 동결(Frost) 상태는 기업의 관점에서는 엄청난 손실을 입게 된다.

4.2. 클라이언트-서버 분산 접근법

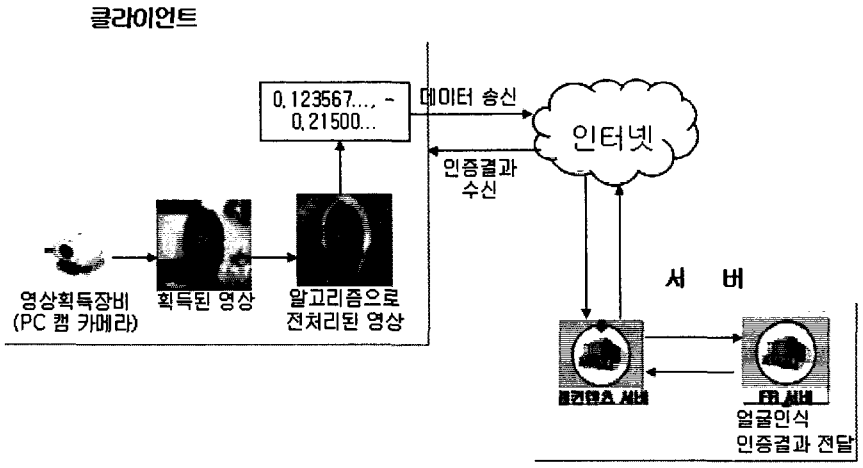
두 번째 접근법인 클라이언트-서버 분산 접근법은 인증절차의 일부 즉, 영상 전처리 과정을 클라이언트에 처리하도록 함으로써 클라이언트의 리소스를 활용하는 방안이다. 여기서의 전처리란, 얼굴을 검색하고 얼굴인식 알고리즘을 이용해 클라이언트 영상정보를 이미지가 아닌 데이터 템플릿으로 인코딩(Encoding)하는 과정을 말한다.

인코딩된 데이터 템플릿은 전송해야 하는 추가정보의 크기와 알고리즘으로부터 생성된 데이터 크기에 따라 84byte에서 1,300byte까지 다양하게 전달할 수 있다. 클라이언트가 직접 획득된 영상의 품질을 확인한 뒤 전송하게 되므로 본인거부율(FRR; False Reject Rate)을 최소화할 수 있으며, 잘못된 생체데이터를 등록하는 등록 오차율(FEE; False Enrollment Error)도 줄일 수 있다.

이 외에도 획득영상 그대로가 아닌 축소된 크기의 데이터를 전송하기 때문에 서버 중심 접근법의 병목현상이나 '래그(Lag)' 문제, 서버 동결 현상을 동시에 해결하고, 서버의 데이터베이스에 저장될 생체데이터의 크기도 줄일 수 있으며, 서버의 리소스를 최적화할 수 있으므로 금융 서비스를 요청하는 다중 사용자에 대한 신속한 인증처리가 가능하게 되어 서비스 효율성을 극대화시킬 수 있다.

다만, 이러한 클라이언트-서버 분산 접근방식을 구현하기 위해서는 클라이언트측에 전처리할 수 있는 기능이 포함되어야 하므로 어느 정도 클라이언트측의 리소스가 요구된다.

<그림 2>는 클라이언트-서버 분산 접근법의 구조를 나타낸 것이다.

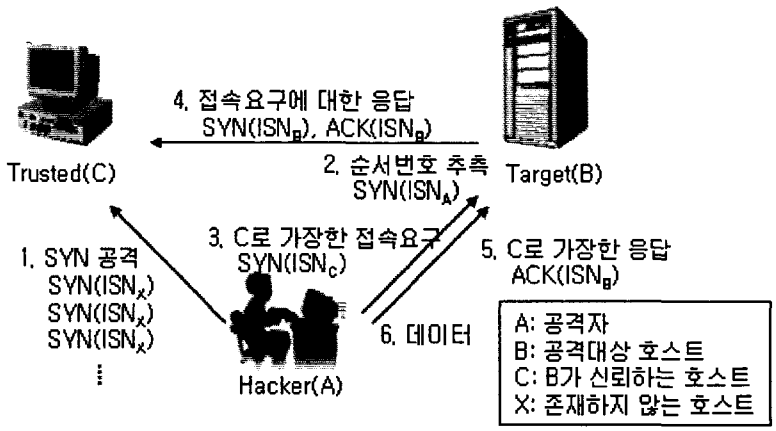


<그림 2> 클라이언트-서버 분산 접근법의 구조

4.3. 다중 키 분산 접근법

앞서 설명한 두 접근법은 얼굴 특징 데이터가 압축되지 않은 순수 데이터(raw data)의 형태로 네트워크를 통해 전달되므로, 고의적으로 얼굴 마스크를 이용하거나 클라이언트와 서버 사이에서 클라이언트로 가장한 해커의 공격인 IP 스푸핑(Spoofing), PC상에서 키보드 입력을 가로채는 후킹(Hooking) 공격에 그대로 노출되어 있다. 아래 <그림 3>은 IP 스푸핑의 예를 설명한 것이다.

아래 <그림 3>에서와 같이 공격자 'A'는 Target 'B'에 대해서 사용자 권한을 소유하고 있는 Trusted 'C'를 공격해 'C'의 권한을 획득하고, 'B'에 대한 인증 권한을 얻어낸다. 인증 권한을 얻게 된 공격자'A'는 'B'에 데이터를 수신할 수 있고, 필요한 개인 정보를 획득할 수 있게 된다. 여기서 Target 'B'가 인터넷 뱅킹 서버라 가정했



<그림 3> IP Spoofing의 경로

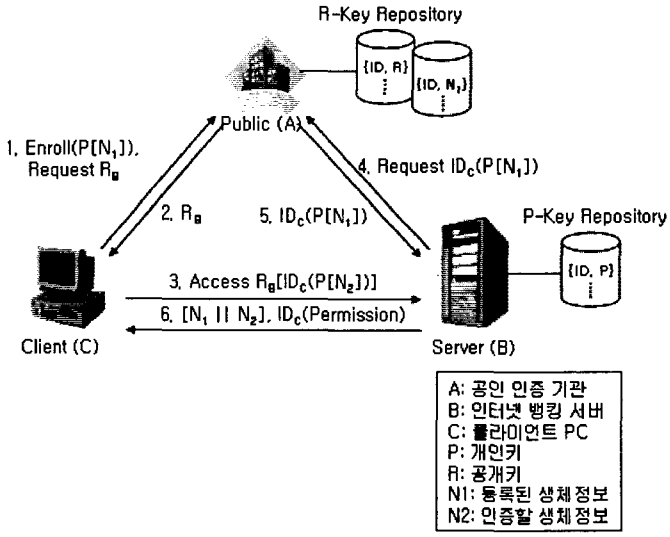
을 때, 공격자 'A'가 Trusted 'C'의 전자 인증서를 도용해 현금 서비스를 이용하게 되는 보안 취약성을 갖고 있다.

현, 금융권의 전자 인증서 발급 절차는 개인정보를 입력하고, 이중 삼중의 비밀번호 체계를 이용해 공인 인증기관으로부터 발급 받은 인증서를 개인의 PC에 저장하고 있다. 이렇게 비밀번호만으로 인증서 발급이 가능할 경우에는 위의 IP Spoofing을 이용한 공격이나 키보드 후킹(Hooking) 공격, 비밀번호가 누출될 경우에는 보안이 그대로 노출되는 문제점을 안고 있다.

그렇다면 앞서 설명한 두 생체인증 접근법을 이용하면 어떠한가? 이러한 생체인증 시스템은 비밀번호 누출이나 키보드 후킹 공격에 대한 방어는 가능하지만 생체정보를 중간에서 가로채는 하이재킹(Hijacking) 공격이나 인터넷의 패킷(Packet)을 변경해 추출된 특징점을 획득할 수 있는 스누핑(Snooping) 공격에는 무방비 상태가 된다. 이러한 취약점을 보완하기 위해서 생체정보를 암호화할 필요가 있으며, 얼굴인식을 인터넷 뱅킹 인증시스템으로 이용할 경우에는 타인수락율(FAR)을 낮추기 위한 방법으로 개인키(Private Key)와 신뢰할 수 있는 인증 기관에 등록된 공개키(Public Key)로 생체데이터를 암호화한 뒤 이를 이용하려면 두 키를 모두 소유하고 있을 때에만 복호화가 가능한 방식을 다중 키 분산 접근법(Multi-key Distribution Approach)이라 정의한다.

다중 키 분산 접근법을 이용하게 되면 하이재킹을 통해 생체정보를 획득하더라도 암호화된 상태이므로 정보 재사용이 불가능하며, 스누핑 공격 역시 개인이 소유한 키를 갖고 있지 않으므로 접근할 수 없게 되어 보안 취약성을 크게 개선시킬 수 있다.

<그림 4>는 다중 키 분산 접근법의 구조도를 표현한 것이다.



<그림 4> 다중 키 분산 접근법의 구조

5. 인터넷 뱅킹 얼굴인증 시스템의 설계

지금까지 생체인식을 인터넷 뱅킹의 사용자 인증에 적용할 수 있는 접근법들에 대해서 살펴보았다. 각 접근법 별로 나름대로의 장단점을 갖고 있으나 인터넷 뱅킹의 신뢰성과 시스템의 강인성 측면에서 서버 중심 접근법과 클라이언트-서버 분산 접근법을 그대로 이용하기에는 보안 취약점이 그대로 노출되는 문제가 있다. 본 논문에서는 순수 데이터를 전처리한 뒤 생체정보를 전달하는 접근법인 클라이언트-서버 분산 접근법을 이용해 서비스 시간 및 전달의 신속성을 유지하고, 안전한 생체인증을 보장하기 위해 다중키 분산 접근법을 혼용한 인터넷 뱅킹 얼굴인증 시스템 구조를 설계하고자 한다.

1차적으로, 그림 4에서와 같이 클라이언트(C)는 공인 인증 기관(A)에 생체정보(N_1)를 개인키(P)로 암호화해서 등록하고, 인증 기관(A)으로부터 뱅킹 서버(B)의 공개키(RB)를 획득한다. 클라이언트로부터 획득된 얼굴 영상을 PCA 알고리즘으로 분석하기 적합한 영상으로 재처리하고, 재처리된 영상으로부터 특징 데이터를 추출해 개인키로 암호화한 뒤 인증 서버에 전달해 준다. 획득된 영상으로부터 얼굴을 찾아내는 얼굴 탐지(Face Detection)는 많은 방법들이 존재하며, 이와 관련된 수많은 논문이 발표되어 있다(Givens, G., 2003, Liu and Wechsler, 2000, Michael et al., 2000, Samaria, 1994). 이러한 영상 처리를 거쳐 탐지된 얼굴 영상에 Eigenface 메소드를 적용시키려면 얼굴 영상을 2차원의 벡터(Vector)로 표현해야 하며, N x N크기의 얼굴 영상은 픽셀의 좌표에 해당하는 $I(x,y)$라 할 수 있으므로 벡터의 크기는 N^2이 된다.

획득된 영상의 고유 얼굴(Eigenface)을 구하기 위해서는 벡터화된 학습 영상(Γ) M개를 더한 뒤 그것의 평균을 구하면 획득된 영상과 비교할 평균 얼굴(Mean Face)를 구할 수 있다. 평균 얼굴의 집합(Ψ)은 다음과 같이 수식(1)로 표현된다.

$$\Psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n \qquad \text{수식 (1)}$$

각 학습 영상(Γ)과 평균 얼굴(Ψ)에 대한 벡터들의 차를 구한 것(Φ)들로 나타난다. 아래는 벡터의 차를 구하는 나타낸 수식(2)이다.

$$\Phi_i = \Gamma_i - \Psi \qquad \text{수식 (2)}$$

여기서 원래의 얼굴 영상에서 일치하는 공분산 행렬(C; Covariance Matrix)의 고유벡터(EigenVector)를 찾기 위해 벡터들의 차(Φ)를 이용해 다음과 같은 수식(3)으로 표현할 수 있다.

$$\begin{aligned} C &= \frac{1}{M}\sum_{i=1}^{M}\Phi_i\Phi_i^T \\ &= AA^T \\ A &= [\Phi_1\Phi_2 \ldots \Phi_M] \end{aligned} \qquad \text{수식 (3)}$$

그러나 AA^T 행렬은 그 크기가 N^2 x N^2으로 급격히 커지게 되어 계산이 어려워지므로 다음과 같이 표현하면 그 크기를 감소시킬 수 있다.

$$\begin{aligned} &(A^TA)v_i = \lambda_i v_i \\ &A(A^TA)v_i = A(\lambda_i v_i) \\ &AA^T(Av_i) = \lambda_i(Av_i) \end{aligned} \qquad \text{수식 (4)}$$

A^TA는 N x N행렬이므로 계산과정이 간단하다. 수식(4)에서 구해진 고유벡터를 고유값(υ)의 내림차순 정렬하면 하나의 고유벡터를 얻는데 이

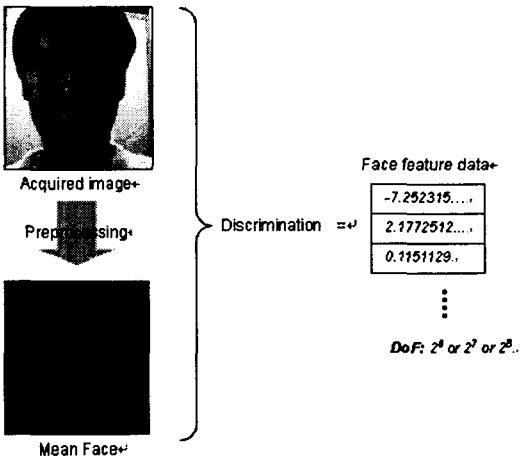
벡터공간을 고유공간(Eigenspace)라 하며 새로운 얼굴벡터(Ω)는 다음과 같이 표현된다.

$$\Omega^T = [w_1 w_2 \ldots w_{M'}] \qquad \text{수식 (5)}$$

<그림 5>는 획득된 얼굴 영상과 평균 얼굴의 차를 구해서 고유공간에 얼굴벡터로 표현한 것이다. <그림 5>에서처럼 얼굴 탐지(Face Detection)와 영상처리(Image processing)를 거쳐 PCA 방법이 적용된 평균 얼굴(실험 중에는 192명의 평균얼굴을 구함)과의 차(discrimination)로 $2^6 \sim 2^8$개 사이의 고유벡터 값 집합(Eigenvector Value Set)으로 표현되며, 이들이 바로 생체정보(N_1 or N_2)가 된다. 클라이언트 환경을 고려했을 때 인터넷 뱅킹의 사용자 인증을 위한 생체정보는 크기를 최소화해야 한다. 생체정보의 크기를 너무 많이 줄이게 되면 특징 템플릿의 자유도(DoF; Degree of Freedom = Number of features)가 떨어지며, 그 크기를 늘이는 경우 자유도는 높아지지만 비교해야 할 특성(feature)이 늘어나 인증속도를 저하시키게 된다.

얼굴 영상으로부터 추출된 생체 정보(N_1)는 공인 인증 기관에 사용자의 ID, 공개키(R-Key)와 더불어 정보 보관소(R-Key Repository)에 등록된다. 클라이언트(C)가 뱅킹 서버(A)를 통해서 사용자 인증을 요청할 경우 새롭게 추출된 생체정보(N_2)를 개인키(P-Key)로 암호화하고, 이를 다시 공개키(R-Key)로 암호화해서 뱅킹 서버(B)에 전달하면, 뱅킹 서버(B)에서는 클라이언트(C)로부터 전달 받은 암호화된 데이터를 공인 인증기관(A)에 클라이언트 공개키(R-Key)와 생체정보(N_1)를 요청해 복호화한 뒤, 이를 다시 개인키 저장소(P-Key Repository)에 등록된 클라이언트(C)의 개인키(P-Key)로 복호화한다.

공개키(R-Key)와 개인키(P-Key)로 두 번 복호화된 생체정보(N_2)는 공인 인증 기관(A)으로부터 가져온 생체정보(N_1)와의 차이를 비교해 일정 임계치(Threshold)를 넘지 않는 경우에는 클라이언트(C)에게 인증 허가권(Permission)을 전달한다.



<그림 5> 획득된 이미지의 생체정보 추출과정

6. 결론 및 향후과제

본 논문에서는 생체인식 시스템 중 인터넷 뱅킹의 사용자 인증에 적합한 시스템을 설계하는 몇 가지 접근법을 제시하였다. 현재까지 생체인식의 여러 응용분야에서는 얼굴인식보다 지문인식이나 홍채인식이 앞서고 있으나 얼굴인식의 특징인 인식의 편의성, 비강제성, 비접촉성, 특징정보 추출의 용이성과 같은 장점을 살려 타 인식기술에 비해 부족한 보안 취약점을 보완할 수 있는 기술을 접목시켰을 때 인터넷 상에서의 활용도는 훨씬 높아질 것으로 예상된다.

그러나, 본 논문에서 충분히 다루지 못했던 인증과정의 암호화 처리 문제와 신뢰할 수 있는 공인 생체 인증 기관의 확보, 객체 집단을 동시에 처리해야 하는 문제, 그리고 타인 승락율과 본인 거부율에 대한 개선, 빛과 환경의 변화에 대한 처리가 앞으로 더 연구되어야 할 과제로 남아있다.

참고문헌

[1] Blackburn, D. M., J. M. Bone, and P. J. Phillips *FRVT 2000 Report*, http://www.ftvt.org, 2001.

[2] Bolle, R. M., N. K. Ratha, and S. Pankanti. "Evaluating authentication systems using bootstrap confidence intervals," *In Proc. 1999 IEEE Workshop on Automatic Identification Advanced Technologies,* Vol.2 , No.33(1999), 9-13.

[3] Givens, G., J. R. Beveridge, B. A. Draper, and D. Bolme. "A statistical assessment of subject factors in PCA recognition of human faces," *Conf. on Computer Vision and Pattern Recognition Workshop*, Vol.8, No.1(2003), 96.

[4] Liu, C. and H. Wechsler, "Evolutionary Pursuit and its Application to Face Recognition", *IEEE Trans. Patt. Analysis and Machine Intell.*, Vol.22, No.6(2000), 570-582.

[5] Michael. K and L. Sirovich, "Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces," *IEEE Transactions on Pattern Analysis and MachineIntelligence,* Vol.12 No.1(1990), 103-108.

[6] Michael J. L., J. Budynek and A. Plante, "Classifying Facial Attributes using a 2-D Gabor Wavelet Representation and Discriminant Analysis", *4th Int'l. Conf. on Automatic Face and Gesture Recognition,* Vol.1, No.4(2000), 202-207.

[7] Samaria F.S., *Face recognition using Hidden markov Models.* PhD thesis, Trinity College, Univ. of Cambridge, Cambridge, 1994.

[8] Swets, D.L. and J.J. Weng, "Using Discriminant Eigenfeatures for Image Retrieval", *IEEE Trans. Patt. Analysis and Machine Intell.*, Vol.18, No.8(1996), 831-836.

[9] Turk, M. and A. Pentland, "Eigenface for Recognition", *J. Cognitive Neuroscience*, Vol.3, No.1(1991), 71-86.

Abstract

Design of Face Recognition System for Authentication of Internet Banking User

Kyoung-Yul Bae*

In this paper, we suggest user authentication and authorization system for internet banking by face recognition. The system is one of Biometrics technology to verify and authorize personnel identification and is more unobtrusive than the other technologies, because they use physiological characteristics such as fingerprint, hand geometry, iris to their system that people have to touch it. Also, the face recognition system requires only a few devices such as a camera and keypad, so it is easy to apply it to the real world. The face recognition algorithms open to the public are separated by their analysis method differ from what characteristic of the human face use. There are PCA (Principal Component Analysis), ICA (Independent Component Analysis), FDA (Fisher Discriminant Analysis). Among these, physiological data of encrypted form is translated utilizing PCA which is the most fundamental algorithm that analyze face feature, and we suggests design method of user authentication system that can do send-receive fast and exactly.

Key words : Biometrics, Face Recognition, Bio-authentication system of Internet Banking User

* Dept. of Software, Sang-Myung University