論文
5-1-16

얼굴정보를 이용한 사용자 인증 프로토콜 설계
Design of a User authentication Protocol Using Face Information

지은미(Eun-Mi Ji)[1)]

요 약

최근 들어 개인의 고유한 생체정보인 지문, 음성, 얼굴, 홍채, 손의 형태, 정맥분포 등을 사용자 인증에 이용하려는 이른바 생체 인식 및 인증 기술에 관한 연구에 관심이 모아지고 있다. 생체 인증 기술 중 얼굴 정보를 이용한 시스템은 비접촉식이므로 사용자의 거부감이 없고 컴퓨터에 기본으로 탑재되는 PC 카메라를 이용할 수 있다는 점에서 비용상 장점을 가진다. 그러나 얼굴 인증은 동일한 사람의 얼굴이라도 조명 변화, 표정 변화, 시점 변화, 머리 모양의 변화 등에 따라 다른 사람으로 인식될 수 있기 때문에 이러한 변화에 민감하지 않고 안정적인 성능을 갖는 시스템을 구현하는 것이 얼굴 인증 시스템의 목적이라고 할 수 있다.

이 연구에서는 사용자 정보의 기밀성 및 무결성을 제공하고 얼굴 인증시 발생하는 오 인증율(EER)을 최소화하기 위한 사용자 인증 프로토콜을 제안하였다.

Abstract

Consequently substantial research has been done on the development of the bio-metric recognition method as well as technical research in the field of authentication.

As a method of bio-metric recognition, personal and unique information such as fingerprints, voice, face, iris, hand-geometry and vein-pattern are used. The face image system in bio-metric recognition and information authentication reduces the denial response from the users because it is a non-contact system, the face image system operates through a PC camera attached to a computer base this makes the system economically viable as well as user friendly. Conversely, the face image system is very sensitive to illumination, hair style and appearance and consequently creates recognition errors easily, therefore we must build a stable authentication system which is not too sensitive to changes in appearance and light.

In this study, I proposed user authentication protocol to serve a confidentiality and integrity and to obtain a least Equal Error Rate to minimize the wrong authentication rate when it authenticates the user.

논문접수 : 2004. 1. 9.
심사완료 : 2004. 1.16.

1) 정회원 : 혜천대학 컴퓨터통신계열 조교수

* 본 논문은 2002년도 혜천대학 교내학술연구비 지원에 의해 수행된 것임

1. 서론

현재, 다양한 계층의 사용자가 컴퓨터 네트워크 망에 연결된 각 조직의 서버에 접속하여 원하는 정보를 얻고 있으며, 일부에서는 사용자에게 패스워드 등의 사용자 정보로 정당한 사용자에게 접근을 허용하는 등 사용자 인증 기능을 강화하고 있다.

현재까지 사용자 인증 수단으로 많이 사용되고 있는 패스워드 등은 분실되거나 타인에 의해 오용될 수 있어 재산상의 손실을 초래하는 심각한 문제가 야기되고 있다. 이에 따라 개인의 고유한 생체 정보인 지문, 음성, 얼굴, 홍채, 손의 형태, 정맥분포 등을 사용자 인증에 이용하려는 이른바 생체 인증 기술에 관한 연구에 관심이 모아지고 있다[1][2][3]. 생체 정보는 개인별로 고유한 것이므로 자신의 지문이나 홍채 패턴을 잊거나 집에 두고 올 수 없으며, 타인이 훔쳐갈 수 없으므로 생체 정보를 이용한 인증 기술은 패스워드 인증 기반의 문제점을 해결하기 위한 새로운 방법이 될 것이라 기대된다. 또한 이러한 생체 정보의 보호를 위해 등록 데이터를 중앙 데이터베이스에 저장하지 않고 보안 토큰 또는 IC 카드 등에 저장하는 방법이 연구되고 있다[4].

생체 인증 기술 중 지문 인증 기술은 가장 보편화되어 상용화되고 있으나, 지문 인증 기기에 따라 인증 결과가 종속되고, 사람의 직업에 따라 지문 인증 결과의 신뢰성이 낮아지는 등 한계가 있다. 반면에 얼굴 정보를 이용한 생체 인증 시스템은 비접촉식이므로 사용자에게 가장 자연스러운 방법이며 컴퓨터에 기본으로 탑재되는 PC 카메라를 이용할 수 있다는 점에서 장점을 가진다.

얼굴을 인증하는 방법은 웨이블렛 변환을 통하여 추출한 얼굴의 특징을 이용하여 그래프 매칭 기법으로 인증하는 방법[5], 얼굴 구성요소의 특징과 관계를 이용한 기하학적인 모델에 의해 인증하는 방법[6], 주성분 분석으로 추출한 특징 벡터를 이용하여 인증 여부를 판별하는 방법[7][8][9] 등이 있다.

이 논문은 사무실 환경의 개인 컴퓨터에서 권한이 제한된 서버에 접속하는 사용자 관리, 사이버 교육 사이트에서 학생의 신분 확인, 성인 사이트에서 타인의 ID를 도용하는 미성년자의 접속 거부 등을 위한 사용자 인증 시스템의 기반 기술에 관한 연구이다.

본 논제의 2장은 생체 정보를 이용한 인증 기술의 연구 동향, 3장은 생체 정보중 얼굴을 이용한 인증 기술에 관하여 기술하며, 4장은 사용자 인증 프로토콜 그리고 5장은 결론을 기술한다.

2. 생체 정보를 이용한 인증 기술의 연구 동향

생체 정보를 이용하여 인증 한다는 것은 살아있는 사람의 신원을 생물학적 또는 행동 특징을 기반으로 인증 하는 것을 말한다. 현재 인증에 사용하기 위하여 연구되고 있거나 실용화된 시스템에서 사용하고 있는 생체 정보는 지문, 홍채, 음성, 망막, 얼굴 등의 생물학적 특징과 서명, 키보드 치는 습관 등과 같은 행동학적 특징 등이 있다[10]. 사용자 인증을 위해 생체 정보를 이용하는 이유는 다음과 같다.

- 홍채, 지문, 얼굴 등의 생체 정보는 개인별로 고유한 것이므로 위조하거나 변조하기 어렵다.
- ID 카드나 패스워드 등은 항상 지참하고 암기해야 하고 분실 또는 오용될 수 있으나 자신의 생체 패턴은 망각하거나 분실할 염려가 없고 편리하다.
- 생체 정보의 등록 시 중앙 데이터베이스에 저장하지 않고 프로세서가 내장된 IC카드에 등록하여 인증할 경우 네트웍 공격으로부터 안전하다.

그러나 이러한 장점 외에 장치가 크고 비싸며 사용자에게 거부감을 줄 수 있다는 단점도 가지고 있으므로 이러한 단점을 보완할 수 있는 기법에 관한 연구가 요구된다.

[표 1]은 생체 인증 시스템을 정확도, 비용, 노력, 강요성 등의 관점에서 비교 분석한 것[11]으로 ★이 많을수록 좋은 특성을 갖으며 ☆는 2002년 현재 시스템의 정확도가 개선되었음을 의미한다. [표 1]은 여러 가지 생체 인증 시스템 중에서 지문과 얼굴을 이용한 시스템이 여러 가지 면에서 비교적 좋은 특성을 갖고 있으며, 홍채와 망막은 정확도 면에서 우수하지만 비용이나 강요성 면에서 비효율적이며 음성은 정확도 면에서 현저하게 떨어짐을 보여주고 있다.

[표 59] 생체 인증 시스템별 비교
[Table 1] Comparison of bio-metric certification system

	정확도 (Accuracy)	비용 (Cost)	노력 (Effort)	강요성 (Intrusiveness)
지문	★★★	★★★★	★★★	★★★
홍채	★★★★★	★	★★★★★	★★
얼굴	★★☆	★★★★	★★★★	★★★★
음성	★	★★★★★	★★★	★★★★★
망막	★★★★	★★	★	★

[표 1]에서 보는 바와 같이 얼굴 정보를 이용한 생체 인증 시스템은 영상 획득시 비접촉으로 획득할 수 있으므로 사용자가 불편함을 느끼지 않으며, 비용 면에서 경제적이고 또한 정확도가 비교적 높으므로 사이버 교육 사이트에서 학생 신분의 확인, 인터넷 사이트에서 회원의 확인, 권한이 제한된 서버에 접속하는 사용자의 관리 등과 같이 저가형 인증 시스템을 구현하는데 적합하다.

3. 얼굴 인증 기술

3. 1 얼굴 검출 기법

얼굴 인증 시스템은 주로 2차원 영상으로 획득되는 얼굴 데이터에서 다른 사람의 얼굴 영상과의 미세한 차이를 구별하고, 같은 사람의 얼굴 영상의 경우 작은 변화에도 불구하고 동일한 특징을 찾아내는 기술에 기반하고 있다. 그러나 얼굴 인증은 동일한 사람의 얼굴이라도 조명 변화, 표정 변화, 시점 변화, 머리 모양의 변화 등에 따라 인증이 거부될 수 있기 때문에 이러한 변화에 민감하지 않고 안정적인 성능을 갖는 시스템을 구현하는 것이 얼굴 인증 시스템의 목적이라고 할 수 있다.

얼굴 인증 시스템은 크게 얼굴 영역의 검출, 얼굴 영역으로부터 얼굴 특징 추출, 추출된 특징을 이용한 얼굴 인증으로 구성된다[12]. 얼굴 인증 기술의 전처리 과정이라 할 수 있는 얼굴 영역 검출과 얼굴 특징 추출은 배경과 영상에서 얼굴이 차지하는 크기나 방향 등에 대한 제약을 가지고 있으므로, 얼굴에 대한 인증율을 높이기 위해서는 첫 번째 과정인 얼굴 영역 검출이 효과적으로 이루어져야 한다[13]. 초기의 얼굴 영역 검출 방법들은 주로 연구실 환경 내에서, 얼굴 영역만을 포함하며, 단일 색조의 배경만이 존재한다는 가정하에서 이루어졌다[14][15]. 그러나 실용화를 목표로 하는 얼굴 인증 시스템을 개발 할 때는 배경, 조명 상태, 얼굴과 카메라의 거리, 입력 얼굴의 상하좌우 각도, 얼굴 표정, 카메라의 입력 특성 등의 다양한 환경에서 강인한 얼굴 검출 결과를 얻을 수 있어야 한다.

얼굴 영역을 검출하는 방법으로는 색상 정보를 이용하는 방법[16], 에지 맵을 구성하여 경계선을 연결하고 이를 Hough 변환을 통해 얼굴 영역을 분리하는 방법[17], 주성분 분석으로 추출한 고유 얼굴을 이용하는 방법[18], 색 정보와 동영상을 이용하는 방법[19], 신경망을 이용하는 방법[20], 얼굴에 대한 표준적인 형판을 만들고 입력 영상에 대하여 탐색 윈도우를 적용하여 윈도우내의 영상과 형판을 비교하여 얼굴 영역을 찾아내는 방법[21] 등이 있다.

위에 제시된 방법들은 다음과 같은 문제점을 갖고 있다. 첫째 색상 정보를 이용하는 경우에는 살색과 유사한 색상이 배경에 존재하는 영상에 대해 얼굴 영역을 검출하기 어렵다. 둘째 신경망을 이용하는 경우에는 동일한 크기의 얼굴에 대해서는 정확도가 높은 반면 얼굴 크기에 민감하기 때문에 실제 환경과 같이 얼굴 크기가 다양한 경우 학습 데이터 및 오류가 증가한다. 셋째 템플릿을 이용하는 경우 템플릿의 대표성을 부여하기 어렵기 때문에 여러 개의 템플릿을 사용할 경우 연산 량이 증가한다. 이러한 단점 외에 위에 제시한 모든 방법들은 공통적으로 입력 영상의 조명변화, 배경변화, 표정변화, 안경 유무에 따라 검출 결과가 크게 좌우되므로 이러한 변화에 민감하지 않은 얼굴 검출 방법에 관한 연구가 필요하다. 본 연구에서는 에지 정보와 컬러 정보를 결합한 얼굴 영역 검출 방법[22]를 이용하여 얼굴 영역 검출, 크기 정규화, 기울기 교정 등의 작업을 수행하였으며 이를 이용하여 얼굴 인증 시스템을 구현하고자 한다.

3.2 인증 알고리즘의 비교

고성능 컴퓨터의 가격이 저렴해지고 컴퓨터

비젼 연구가 활발해짐에 따라 얼굴 인증을 위한 효과적인 기술이 개발되었다.

1998년 보고된 실험결과[23]는 FERET 데이터베이스[24]를 대상으로 각 대학과 기업에서 제안한 얼굴 인식 및 인증 알고리즘의 성능을 평가하였다. 여기서 알고리즘의 성능을 평가한다는 것은 질의 집합 Q에 있는 임의의 영상 q_i 와 목적 집합 T에 있는 등록 영상 t_k 간의 유사도 측정치 $s_i(k)$를 구하는 것이다.

실험 대상 알고리즘은 얼굴 영상에서 눈의 좌표가 주어지는 반자동화 인증 알고리즘으로 주성분 분석, Correlation[25][9], Excalibur Corp.(Carlsbad, CA), MIT Media Lab.[26], Michigan State University(MSU)[27], Rutgers University[28], University of Maryland(UMD)[29], University of Southern California (USC)[30] 등이다. 주성분 분석 기반의 알고리즘은 눈의 중심점이 정해진 화소에 놓이도록 그 크기와 위치가 정규화 되었고 배경과 머리카락이 제거되었으며 얼굴 영역은 히스토그램이 균등하게 분포 되도록 평활화(equalization) 하였다. 또한 훈련집합의 영상은 500개로 이루어졌으며 고유 얼굴은 200개를 선택하였고 인증의 성공 여부를 결정하는 분류자(classifier)는 L_1을 사용하여 얻은 $s_i(k)$를 가지고 $s_i(k)$<=c 일 경우 인증 실패, $s_i(k)$>c 일 경우 인증 성공으로 결정하였다.

인증 성공율은 P_V, 인증 실패율은 P_F로 나타내며 인증의 성공여부를 결정하기 위한 L_1의 크기는 Neyman-Person 이론[31]을 적용하였다. 또한 임계값 c를 변화시키면서 인증 성공율 P_V와 인증 실패율 P_F을 얻었으며 이를 ROC(receiver operating characteristic) 그래프[31]와 EER로 나타내었다. [표 2][23]는 10가지 방법의 성능 평가 결과이다. FB 는 두 종류 즉, 표정이 약간 다른 2개의 정면 영상을 획득하여 하나는 갤러리에 저장하고 나머지 영상들은 실험 영상으로 사용한 경우, duplicate 1은 갤러리에 저장된 영상의 각 개인을 1년 이내에 재 촬영하여 실험 영상으로 사용한 경우, fc는 갤러리 영상과 같은 날 획득하였으나 카메라와 조명을 변경한 경우, duplicate II는 duplicate I과 같으나 2년 이내에 재 촬영하여 실험 영상으로 사용한 경우이다.

[표 2] 의 결과에 따르면 UMD의 LDA(Linear Discriminant Analysis)[29] 방법과 USC의 번치 그래프 매칭(bunch graph matching)[30] 방법이 비교적 높은 EER을 나타내었으며, 모든 방법이 FB에 대해서는 좋은 인증율을 보이고 있지만 fc, duplicate I, duplicate II에 대해서는 EER이 떨어짐을 나타내고 있다. 이는 실험 대상인 얼굴 인증 알고리즘이 표정에 강하지만, 카메라나 조명 변화, 시간이 경과된 얼굴 영상에 대해서는 인증율이 떨어진다는 것을 의미한다. 따라서 주성분 분석 방법의 경우 조명변화에 민감하지 않도록 첫 번째 고유 얼굴을 제거하여 사용하거나, 일정한 시간이 지나면 새로운 영상을 등록 영상에 추가하는 것도 인증율을 높일 수 있는 하나의 방법이 될 것이다.

[표 2] 얼굴 인증 알고리즘의 성능 평가 결과

[Table 2] Performance evaluation of face certification algorithm

얼굴인증 알고리즘	EER(Equal error rate) (%)			
	FB	Duplicate I	fc	Duplicate II
Baseline PCA	7	19	15	22
Baseline correlation	4	21	23	27
Excalibur	5	16	14	24
MIT Mar95	5	20	25	26
MIT Sep96	4	20	26	26
MSU	3	23	11	31
Rutgers	6	18	17	21
UMD Sep96	7	22	16	23
UMD Mar97	1	12	8	14
USC	2	14	6	17
평균 EER	4	19	16	23
최소 EER	1	12	6	14

4. 인증 프로토콜

인터넷은 서로를 직접 확인할 수 없는 가상공간이라는 특성을 지니고 있어서 클라이언트(사용자)와 서버(서비스 제공자)는 서로에 대한 신뢰를 확보하기 어

렵다. 따라서 서버에 접근하는 사용자들을 통제하기 위해 클라이언트를 식별할 수 있는 기법이 필요한데 이것은 인증 서비스를 통해 가능하다. 인증 프로토콜은 데이터를 주고받는 송수신 양자간의 상호 식별을 위한 상호 인증 프로토콜과 단지 서버가 클라언트를 식별하는 일방향 인증 프로토콜이 있다.

4.1 클라이언트 프로토콜

클라이언트 프로토콜은 권한이 제한된 서버에 사용자의 가중치 벡터와 사용자 ID를 서버에 전송하여 인증을 받는 프로토콜로서 입력영상으로부터 생성한 가중치 벡터를 인증 서버에 전송할 때 가중치 벡터의 기밀성(confidentiality) 유지 및 무결성 확인, 사용자 확인을 위해 공개키 기반의 암호화 기법을 이용하여 암호화한다.

공개키 기반의 암호화 기법은 비밀키 암호 기법의 단점인 키 분배의 문제를 해결한 방법으로, 비밀키 암호 시스템과 달리 한쌍의 키 즉, 암호화 키와 복호화 키를 갖는 시스템이다. 이때 하나의 키는 비밀키(secret key) 또는 개인 키(private key)라 하여 사용자 자신만 보관하고 다른 사람에게는 절대로 공개하지 않으며, 나머지 키는 공개키(public key)라 하여 모두에게 공개한다.

A의 공개키로 암호화된 암호문은 A의 비밀키를 사용해야만 복호화 될 수 있으며 A의 비밀키로 암호화된 암호문은 A의 공개키를 사용해야만 복호화 할 수 있다. 따라서 A의 비밀키로 암호화된 암호문은 A의 공개키를 가지고 있는 사람은 모두 복호화 할 수 있게 되어, 이 경우 문서의 기밀성은 이룰 수 없으며, 단지 A의 비밀키를 이용하여 암호화되었다는 것 즉, A가 전송한 메시지라는 것을 증명할 수 있게 된다. 즉 메시지를 보낸 사람이 A라는 것을 증명할 수 있으므로 이러한 기능을 전자서명이라 하며 인증을 위해 사용한다.

따라서 메시지의 기밀성을 유지하고 메시지를 보내는 송신자를 확인할 수 있도록 전자 서명을 첨부하고 메시지를 받는 수신측의 공개키로 암호화하여 전송한다.

다음은 가중치 벡터의 무결성 및 기밀성 유지, 사용자 확인을 위해 클라이언트에서 만든 메시지이다.

$C \Rightarrow AS: E_{KU_{as}} [ID_c \| M_0 \| E_{KR_c} [H(M_0)]]$

여기서 C는 인증을 받고자 하는 사용자, AS는 인증 서버, KU_{as} 는 인증 서버의 공개키, ID_c 는 사용자 C의 ID, KR_c 는 사용자 C의 비밀키, M_0 는 클라이언트가 전송하는 첫 번째 가중치 벡터를 각각 의미하며 E_{KR_c} 는 사용자의 비밀키 KR_c 로 암호화됨을 의미한다.

① 사용자의 신분과 가중치 벡터의 무결성 확인

클라이언트는 가중치 벡터를 전송할 때 서버가 사용자 C의 신분을 확인할 수 있도록 C의 서명을 추가한다. 서명을 추가하는 방법은 가중치 벡터 M_0 를 해쉬한 후 C의 비밀키를 이용하여 암호화하는 것이다. 여기에 다음과 같이 가중치 벡터 M_0 를 함께 보내며, 해쉬 함수로는 MD4 알고리즘에 기반을 두고 있는 SHA(secure hash algorithm)나 MD5를 사용할 수 있다.

$C \Rightarrow AS: M_0 \| E_{KR_c}[H(M_0)]$

② 가중치 벡터의 무결성 확인

①에서 사용자의 서명을 첨부하게 되면 사용자 확인 및 가중치 벡터의 무결성은 확인할 수 있지만 가중치 벡터 M_0 가 노출되므로 이를 막기 위해 다음과 같이 인증서버의 공개키를 이용하여 ①의 메시지를 암호화한다. 이때 사용자 C의 ID를 함께 전송한다.

$C \Rightarrow AS: E_{KU_{as}} [ID_c \| M_0 \| E_{KR_c} [H(M_0)]]$

③ 거부 제어(reject control)

클라이언트는 서버로부터 전송 받은 메시지를 사용자 C의 비밀키로 복호화 하여, 그 결과가 Reject일 경우 거부 제어 횟수만큼 사용자의 얼굴 영상을 재 입력받아 이로부터 가중치 벡터를 계산하여 전송할 수 있다. 여기서 거부 제어 횟수는 실험을 통해서 결정한다.

4.2 서버 프로토콜

서버 프로토콜은 권한이 제한된 서버에 접근하려는 클라이언트의 접근 제어를 위해 인증 서버가 클라이언트의 사용자를 확인하는 일방향 인증 프로토콜이다.

인증 서버는 자신의 비밀키로 전송 받은 메시지를 복호화 하여 사용자 ID를 얻고, 사용자의 공개키를 이용하여 가중치 벡터를 복호화 한다. 이렇게 복호화된

가중치 벡터와 데이터베이스에 등록된 가중치 벡터를 비교하여 인증 여부를 결정하되 가중치 벡터간의 거리가 커서 인증을 거부할 경우에는 n회에 걸쳐 새로운 가중치 벡터를 전송 받도록 한다. 이때 n 번째까지 가중치 벡터간의 거리가 임계값 이상일 경우에는 사용자 본인이 아니라고 판정하여 접속을 거부한다. n에 대한 구체적인 값은 실험을 통하여 결정할수 있다.

① 전송 받은 메시지의 복호화

인증 서버는 클라이언트로부터 전송받은 다음의 메시지를 자신의 비밀키로 복호화하여 사용자 ID와 메시지 M_0 를 얻고, M_0 를 해쉬하여 그 결과과 $H(M_0)$와 동일한가의 여부를 검사한다. 그 값이 서로 동일한 경우 가중치 벡터 M_0 의 무결성이 확인되는 것이다.

$$E_{KUas}\ [ID_c \parallel M_0 \parallel E_{KRc}\ [H(M_0)]]$$

② DB의 가중치 벡터 엑세스 및 가중치 벡터간의 거리 비교

DB에 등록된 가중치 백터 중에서 사용자 C의 가중치 백터 M_R을 가져와 ①에서 구한 가중치 벡터 M_0 와 비교하여 인증 여부를 결정한다.

③ 인증 결과의 암호화 및 전송

인증 여부 즉, *Accept* 또는 *Reject*를 사용자의 공개키로 암호화하여 클라이언트로 전송한다.

④ 거부 제어

전송받은 가중치 벡터와 등록된 가중치 벡터와의 거리가 임계값 이하인 경우에는 인증을 허락하고, 임계값보다 큰 경우에는 클라이언트에게 새로운 가중치 백터를 요구한다. 이때 거부 제어 횟수만큼 새로운 가중치 백터를 요구할 수 있다. 거부 제어 횟수가 초과한 경우에는 최종적으로 사용자의 인증을 거부한다.

4.3 얼굴 정보 기반의 사용자 인증 프로토콜

[표 3]은 사용자 인증 프로토콜에서 사용된 함수와 부호의 의미를 표시한다.

[표 3] 사용자 인증 프로토콜에서 사용되는 함수와 부호

[Table 3] Function and symbol used in user authentication protocol

기능	함수 및 부호	의미
정의문	MAX_Count	거부 제어 횟수
함수	Preprocess()	얼굴 영상을 획득하고 전 처리하는 함수
함수	Compute()	가중치 벡터를 계산하는 함수
복호화	$D_{KRas}(e_c)$	암호문장을 인증 서버의 비밀키로 복호화하는 함수
복호화	$D_{KUas}(e_s)$	암호문장을 인증서버의 공개키로 복호화하는 함수
암호화	E_{KUc}[Msg]	사용자 C의 공개키로 메시지를 암호화하는 함수
암호화	E_{KUas}[Msg]	인증 서버 AS의 공개키로 메시지를 암호화하는 함수
함수	Send()	메시지를 송신하는 함수
함수	Receive()	메시지를 수신하는 함수
함수	Access_DB()	DB에 등록된 가중치 벡터를 엑세스하는 함수
함수	Compare()	가중치 벡터간의 거리를 비교하는 함수
부호	M_{count}	몇 번째 가중치 벡터인가 표시
부호	e_c	클라이언트로부터 인증 서버로 전송하는 메시지
부호	e_s	인증 서버로부터 클라이언트로 전송하는 메시지

[그림 1] 은 연구에서 제안하는 공개키 기반의 사용자 인증 프로토콜로서 인증 서버 AS가 사용자 C를 인증하는 일방향 인증 과정을 표시하며 클라이언트에서 가중치 벡터의 기밀성 유지를 위해 그 값을 암호화하고 사용자 인증 및 가중치 백터의 무결성을 확인하기 위해 사용자의 전자 서명이 첨부되는 과정을 표시한다.

클라이언트(C)		인증 서버(AS)
1 #define MAX_Count n count =0; r=Reject||ID_c;		#define Max_Count n count = 0;
2 while(r==Reject||ID_c && count < n) { Preprocess($FaceImage_{count}$); Compute(M_{count}); $e_c=E_{KUas}[ID_c\|\|M_0\|\|E_{KRc}[H(M_{count})]]$; Send($e_c$) count++; Receive($e_s$) r=$D_{KUas}(e_s)$; }	e_c → ← e_s	while(count < n) { Receive(e_c) $D_{KRas}(e_c)$; Access_DB(ID_c, M_R); r = Compare(M_0, M_R); $e_s=E_{KUc}[r\|\| ID_c]$; Send(e_s) count++; } if(cont >= n || r==Reject) $e_s= E_{KUc}[r\|\| ID_c]$;

[그림 1] 사용자 인증 프로토콜

[Fig. 1] Proposed user authentication protocol

얼굴 인증 시스템에서 오 인증이 발생했을 때는 새롭게 입력받은 얼굴 영상으로 인증을 시도한다. 따라서 얼굴 인증 과정은 [식 1]과 같이 이항 확률 분포의 성질을 만족하므로 반복 인증을 시도할 경우 성공 확률은 1에 근사하게 됨을 알 수 있다.

$$(p+q)^n = \sum_{x=0}^{n} \binom{n}{x} p^x q^{n-x} \quad [식\ 1]$$

[그림 1]의 사용자 인증 프로토콜에서 오인증율(EER)을 최소화하기 위해 사용한 거부 제어 횟수 n은 실험에 의해 평가하였다.

5. 결론

본 논제에서는 네트워상에서 사용자를 인증하기 위해 사용하는 생체 인증 기술중 얼굴 인증 기술에 관하여 기술하였다. 얼굴 정보를 이용한 이유는 생체 정보를 획득할 때 사용자가 거부감을 느끼지 않으며, 컴퓨터에 기본으로 탑재되는 PC 카메라를 이용하기 때문에 비용 면에서 장점을 갖기 때문이다. 사용자 인증 기술로는 정보의 양을 줄일 수 있고 비교적 정확도가 높은 주성분 분석을 이용하였다.

얼굴 정보를 이용하여 사용자를 인증할 때 발생하는 EER(equal error rate)을 최소화하고, 네트웍을 통해 전송되는 사용자 정보를 보호하기 위해 사용자 인증 프로토콜(user authentication protocol)을 제안하였다. 또한 가중치 벡터의 기밀성 및 무결성을 제공하였으며 제안된 사용자 인증 프로토콜을 사용하여 개선된 인증율을 얻었다.

참고 문헌

[1] Pankanti, R. Bolle, R., and Jain, A., "Biometrics: The Future of Identification, " *IEEE Computer*, vol. 33, pp. 46-49, 2000.

[2] Adams, J., *Survey: Biometrics and smart cards,* BTT. pp. 8-11, Aug. 2000.

[3] Liu, J., Lee., Y. T., "Graph-based method for face identification from a single 2D line drawing," *IEEE Transactions on Pattern Analysis & Machine Intelligence,* vol. 23, no. 10, Oct. 2001, pp. 1106-19. USA.

[4] 반성범, 정용화, 김호원, 박영수, "IC 카드를 이용한 생체인식 기술 개발 동향", **정보과학회지** 제19권, 제7호, pp. 14~21, 2001.

[5] Wiskott, L., Fellous, J., Kruger, N., Malsburg, C.,

"Face Recognition by Elastic Bunch Graph Matching," *Intelligent Biometric Technique in Fingerprint and Face Recognition*, 1999.

[6] Brunelli, R., Poggio, T., "Face Recognition through Geometrical Features," *Proc. ECCV92*, pp. 792-800, 1992.

[7] Liu, C., and Wechsler, H., "Enhanced Fisher Linear Discriminant Models for Face Recognition," *Proceedings of the 14th International Conference on Pattern Recognition*, vol. 2, pp. 1368-1372, 1998.

[8] 박준우, 이필규, "가보함수와 주성분 분석을 이용한 사용자 인증 시스템", **한국정보처리학회 춘계 학술발표논문집** 제8권 제1호, 2001.

[9] Moon, H., Phillips, J., *Analysis of PCA-based Face Recognition Algorithms, in Emprical Evaluation techniques in Computer Vision*, K. Boyer and J. Phillips, Editors. 1998, IEEE Computer Society Press: Los Alamitos, CA.

[10] http://www.evermedia.co.kr/kor/main.php?viewPage=tech, 2001.

[11] www.biometricgroup.com, 1998.

[12] Weng, J., Swets, D. L., "Face Recognition," *in Biometrics: Personal Identification in Networked Society(A. Jain, R. Bolle, and S. Pankanti, Eds.)*, pp. 67-86, Boston, MA: Kluwer Academic, 1999.

[13] Yang, M. H., Ahuja, N., Kriegman, D., "A survey on face detection methods," *Working paper, available at http://vision.ai.uiuc.edu/myyang/papers/survey.ps.gz*, 1999.

[14] Yang, G., and Huang, T., "Human face detection in a scene," *IEEE Int. Conference of Computer Vision and Pattern Recognition*, pp. 453-458, 1993.

[15] Govindaraju, V., Srihari, S. N., and Sher, D. B., "A computational model for face location," *IEEE Int. Conference of Computer Vision*, Osaka, Japan, pp. 718-721, 1990.

[16] Lee, C. H., Kim, J. S. and Park, K. H., "Automatic human face location in a complex background using motion and color information," *Pattern Recognition*, vol. 29, no. 11, pp. 1877-1889, 1996.

[17] Davies, E. R., *Machine Vision: Theory Algorithms*, Practicalities, 2nd Edition, Academic Press, San Diego, 1997.

[18] Moghaddam, B., Pentland, A., "Probablistic Visual Learning for Object Detection," *ICCV* 1995.

[19] Birchfield, S., "Elliptical Head Tracking Using Intensity Gradients and Color Histogram," *CVPR*, 1998.

[20] Rowley, H. A., Baluja, S. and Kanade, T., "Human Face Detection in Visual Scenes," *IEEE Conference on Computer Vision and Pattern Recognition*, 1998.

[21] 김도형, 이학만, 박재현, 차의영, "눈영역 추출과 개폐상태 인식에 관한 연구", **정보과학회 2001년 춘계학술대회** vol. 28 no. 01 pp. 0532-0534.

[22] 지은미, 윤호섭, 이상호, "컬러와 에지정보를 결합한 조명변화에 강인한 얼굴영역 검출방법", 정보과학회논문지, vol. 29, no. 11, pp. 809-817, 2002.

[23] Rizvi, S. A., Phillips, P. J., Moon, H., "The FERET Verification Testing Protocol for Face Recognition Algorithm," *Technical report 6281*, Oct. 1998.

[24] Phillips, P. J., Wechsler, H., Huang, J., Rauss, P., "The FERET databased and evaluation procedure for face-recognition algorithms," *Image and Vision Computing Journal*, vol. 5, pp. 295-306, 1998.

[25] Turk, M., Pentland, A., "Eigenfaces for recognition," *Journal for Cognitive Neuroscience* vol. 3, no. 1, pp. 71-79, 1991.

[26] Moghaddam, B., Nastar, C., Pentland, A., "Bayesian face recognition using deformable intensity surfaces," *In Proceedings Computer Vision and Pattern Recognition 96*, pp. 638-645, 1996.

[27] Swets, D., Weng, J., "Using discriminant eigenfeatures for image retrieval," *IEEE*

Trans. PAMI, vol. 8, pp. 831-836, 1996.

[28] Wilder, J., "Face recognition using transform coding of gray scale projection projections and the neural tree network," *In R.J. Mammone, editor, Artifical Neural Networks with Applications in Speech and Vision,* pp. 520-536, Chapman Hall, 1994.

[29] Etemad, K., and Chellappa, R., "Discriminant analysis for recognition of human face images," *J. Opt. Soc, Am. A,* vol. 14, pp. 1724-1733, Aug. 1997.

[30] Wiskott, L., Fellous, J-M., Kruger, N., Malsburg, C., "Face Recognition by Elastic Bunch Graph Matching," *IEEE Trans. on PAMI,* vol. 17, no. 7, pp. 775-779, 1997.

[31] Green, D., Swets, J., *Signal Detection Theory and Psychophysics,* John Wiley & Sons Ltd., 1966.

지은미

1988.2: 숭실대학교 전자계산학과 (학사)
1990.2: 숭실대학교 전자계산학과 (석사)
2003.2: 충북대학교 전자계산학과 (박사)
1991.4 - 1995.2 한국과학기술연구원 정보전자 연구부 연구원
1995.3 - 현재: 혜천대학 의료정보과 조교수
주관심분야: 정보보호, 영상처리, 데이터베이스