한국지능정보시스템학회논문지 제10권 제1호 2004년 6월(pp.65~75)

분산형 인공지능 얼굴인증 시스템의 설계 및 구현*

배경율
상명대학교 소프트웨어학부
(jbae@smu.ac.kr)

네트워크로 연결된 환경에서 PIN 번호를 이용해 사용자의 신분을 증명하고 인증하는 방식이 일반적으로 활용되고 있다. 그러나, 아이디나 비밀번호가 해킹을 통해 유출되면 금전적인 피해뿐만 아니라 개인의 사생활까지도 침해받게 된다. 본 논문에서는 아이디나 비밀번호가 유출될 염려가 없는 안전한 인증방식으로 얼굴인식을 채택하였다. 또한, 2-Tier 간의 인증방식이 아닌 점점 분산화 되어 가는 네트워크 시스템을 고려해 3-Tier이상의 분산된 환경에서 원격으로 신분을 증명하고 인증할 수 있는 시스템을 제안하였다. 본 인증시스템의 얼굴인식 알고리즘으로는 최근 분류(Classification)와 특징추출(Feature Extraction)에서 빠른 속도와 정확성을 보이는 SVM(Support Vector Machine)과 PCA를 이용해 얼굴 특징을 분석하고, 분산된 환경에서 인공지능 기법을 활용해 인식속도 및 정확성을 높일 수 있는 분산형 인공지능 얼굴인증 모듈을 구현하였다.

논문접수일 : 2004년 3월 게재확정일 : 2004년 5월 교신저자 : 배경율

1. 서론

과거에는 인터넷과 같은 네트워크 환경에서 클라이언트에게 정보를 전달하기 위해서는 클라이언트/서버 방식이 가장 보편적이고, 유용한 도구였다. 그러나 이제 하드웨어 기반의 표준화와 시장 활성화보다는 하드웨어·소프트웨어·서비스가 결합되어 플랫폼에 종속되지 않는 컴포넌트 기반 기술, 서비스 지향 표준화가 주류를 이룰 것이고 이를 위해 네트워크 환경 역시 유연성과 확장성을 갖춘 분산된 환경으로 전환되는 추세이다. 특히 서비스를 처리하는 시스템이 분산될 경우 정보를 안전하게 유지하고, 처리할 수 있는 보안 시스템을 필요로 하게 된다. 분산된 환경에서 데이터를 보호하고, 인증을 처리하기 위해서 사람의 신체 일부를 비밀번호처럼 사용하는 생체인식 시스템이 최근 이슈가 되고 있으며, 이를 위해 지문이나 장문, 홍채, 정맥, 얼굴인식에 대한 적용 가능성 여부를 두고 많은 비교평가가 이루어지고 있다. 이 중에서, 얼굴인식 기술은 장비에 접촉할 필요가 없어 입력과 관련된 해킹에 대비할 수 있고, 일반적으로 화상채팅이나 화상회의에 활용되는 PC카메라를 이용할 수 있어 경제적인 면을 갖추고 있다. 또한, 타 인식기술에 비해 특징추출 시간이 짧기 때문에 인식과 등록 시간을 단축할 수 있어 멀티 클라이언트나 분산 서버 환경에서의

* 본 연구는 상명대학교 소프트웨어·미디어연구소의 2004년 교내 연구비에 의해서 지원되었음.

신분 증명, 인증에 대한 보안(Security Level) 및 성능(Performance)을 높일 수 있다(Bellovin, S.M. 1989).

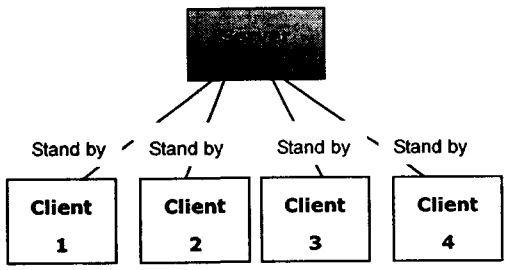
본 논문의 2장에서는 분산환경에 인증 서비스를 구성해보고, 3장에서 얼굴을 인식하기 위한 방법을 제시하였다. 그리고, 4장에서는 분산된 네트워크 환경에서의 특징데이터 전달방법에 대해 살펴보고, 5장에서는 인공지능 기법을 활용해 추출된 생체 정보를 분산 환경에서 수집 및 처리하는 얼굴인증 시스템에 대해 제안하고자 한다.

2. 분산환경에서 인증 서비스의 구성

지금의 통신환경은 원격지에 위치한 시스템간의 협업을 통해 서로의 자원을 공유하거나, 필요한 정보를 주고받는 분산 컴퓨팅 방식으로 변화하고 있다. 통신망을 통한 작업 범위 또한 WWW을 통한 인터넷 환경이 주목을 받게 되면서 전세계적으로 그 규모가 확장되어 가고 있다. 이러한 분산환경에서의 인증 서비스는 클라이언트가 서버에 본인임을 입증할 수 있는 고유 정보를 미리 등록시켜두고, 인증이 필요한 시점에 요청하면 등록된 정보와 새로 요청된 정보와의 인증 작업을 자체 수행하거나 그 결과를 클라이언트에 보내게 된다. 분산된 환경에서 인증서비스를 제공하기 위한 가장 대표적인 구조로는 단일 인증서버 방식(Client/Server based Service)과 다중 인증서버 방식(Multi-Enroll/Authentication Service)으로 나눌 수 있다.

2.1 단일 인증서버의 시스템 구조

다수의 클라이언트가 하나의 서버를 통해 등록 및 인증되는 방식으로, 소수의 클라이언트로 구성된 인증 서비스에 이용되고 있다. 단일 인증서버 방식은 다수의 클라이언트들이 서버와 직접 연결된 대기상태(Standby Status)로 유지되기 때문에 키 분배 및 인증처리가 쉽고 단순한 구조를 갖는다. 반면에 서버에서 처리하는 데이터의 양이 증가함에 따라 클라이언트와 서버 간의 시간 동기화(Time Synchronization)나 병목현상(Bottleneck), 교착상태(Deadlock), 동시성(Concurrency)과 같은 문제를 피할 수 없다. 서버가 멀티스레딩(Multi-threading)을 지원한다 하더라도 단일 서버에서 처리되는 스레딩 역시 부하의 크기는 클라이언트 수에 비례할 수 밖에 없다. <그림 1>은 단일 인증서버 방식의 개략도를 나타낸 것이다.



<그림 1> 단일 인증서버 방식의 Service 개략도

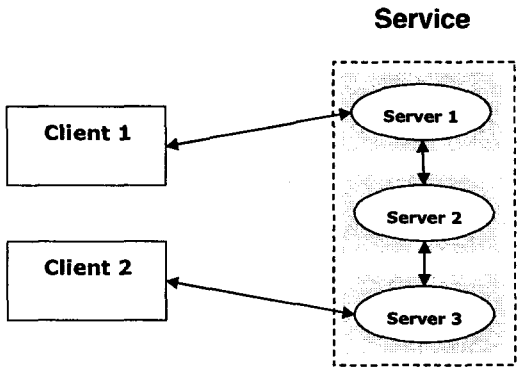
2.2 다중 인증서버를 갖춘 시스템 구조

앞서 살펴본 단일 인증서버 방식의 시스템은 다수의 이용자가 서버에 집중하게 되면 서버에 Lack현상을 일으킬 수 있고, 심지어는 시스템이 다운돼 서비스 이용이 중단되는 심각한 상황에까지 이를 수 있어서 다중 사용자에 대한 인증 서비스를 제공하는 분야에 적용하기 어렵다. 서비스를 제공하는 관리자 측면에서도 이러한 현상을 예방하기 위해서 많은 비용을 들여 서버를 증설해야

만 한다. 따라서, 단일 인증서버 기반의 문제점을 해결하고, 서버의 의존성을 최소화시키는 방법으로 다중 서버를 상호 연결시킴으로써 클라이언트의 접속을 조정하고, 서버의 기능을 분산시키는 방식을 설계하였다. 다중 서버방식은 서버 의존성 및 역할에 따라 대칭 인증서버(Symmetric Authentication Server)와 비대칭 인증서버(Asymmetric Authentication Server)로 나뉜다.

2.2.1 대칭 인증서버 구조(Symmetric Authentication Server Architecture)

대칭 인증서버 구조는 서버가 처리해야 하는 부담을 동일한 기능을 갖는 한 대 이상의 서버에 분배함으로써 서비스를 원활히 하도록 설계하였다. 한 서버에 서비스가 집중될 경우 충돌 경고점(Crash Alert Point)을 설정해두고, 임계치(Threshold)가 경고점에 다다르게 되면 서버와 상호 연결된 서브 인증서버에 서비스를 넘겨주므로 한 서버에 작업이 집중되는 현상을 방지할 수 있다. 아래 <그림 2>는 대칭 인증서버 방식의 서비스를 개략적으로 나타낸 것이다.

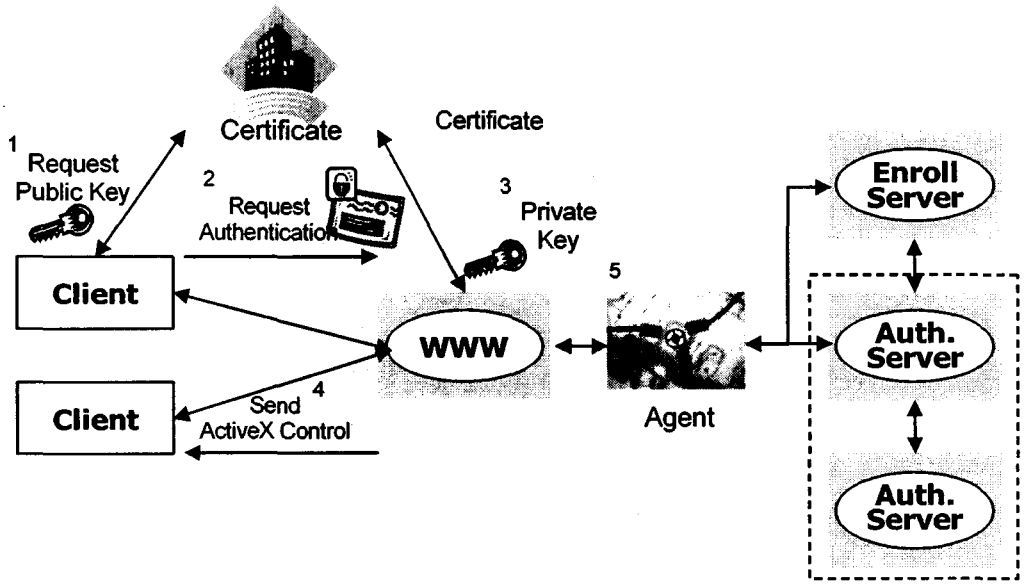


<그림 2> 대칭 인증서버 방식의 Service 개략도

대칭 인증방식은 다수의 클라이언트에 대해서 동일한 기능을 수행하는 서버가 다수 존재해야 하므로 서비스 공급자의 규모가 커지고, 충돌 경고점을 실시간으로 탐지하는 Agent가 각각의 서버에 존재해야 한다. 또한, 단일 인증서버에서 발생하는 시간 동기화처럼 대칭 인증방식에서는 키 분배 및 서비스권을 넘겨주는 과정에서 서버간 동기화가 발생할 수 있기 때문에 서비스권을 관할하는 서버 Agent의 오류 제어가 중요한 성능 지표가 된다. 따라서 Agent의 동기화 문제를 방지할 수 있는 대안으로 비대칭 인증서버 방식을 설계하였다. 비대칭 인증서버는 대칭 인증서버와 동일한 서버 아키텍처를 갖고 있으나 서버의 기능을 분류한 클러스터(Cluster)간 연결을 통해 서버와 Agent의 부담을 동시에 줄일 수 있다.

2.2.2 비대칭 인증서버 구조(Asymmetric Authentication Server Architecture)

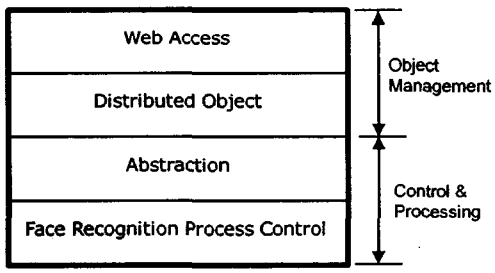
비대칭 인증서버는 단일 서버의 서비스 부담을 줄이기 위해 다중 서버를 이용해 서비스권을 분할해 처리한다는 서비스적 관점에서는 대칭 인증서버와 유사하다. 그러나 등록과 인증을 클러스터로 분류함으로써 동시에 두 기능을 처리해야 하는 대칭 인증서버 방식과 달리 단일 기능을 갖는 서버들을 비대칭으로 연결함으로써 키 분배, 등록 및 인증에 대한 판단, 서비스 권한 호출(Call)/분배(Distribution)와 같은 기능을 수행해야 했던 Agent를 보다 가볍게(Lightweight Agent) 만들 수 있다. 추가적으로 클라이언트와 서버의 기능 분담을 통해 서버 작업량을 줄일 수 있었던 다중 키 분산(Multi-key Distribution) 접근법(배경율, 2003)을 적용할 경우 인증서버의 처리량을 최적화할 수 있게 된다. 다중키 분산 방식의 설계는



<그림 3> 비대칭 인증서버 방식과 다중키 분산 Service 개략도

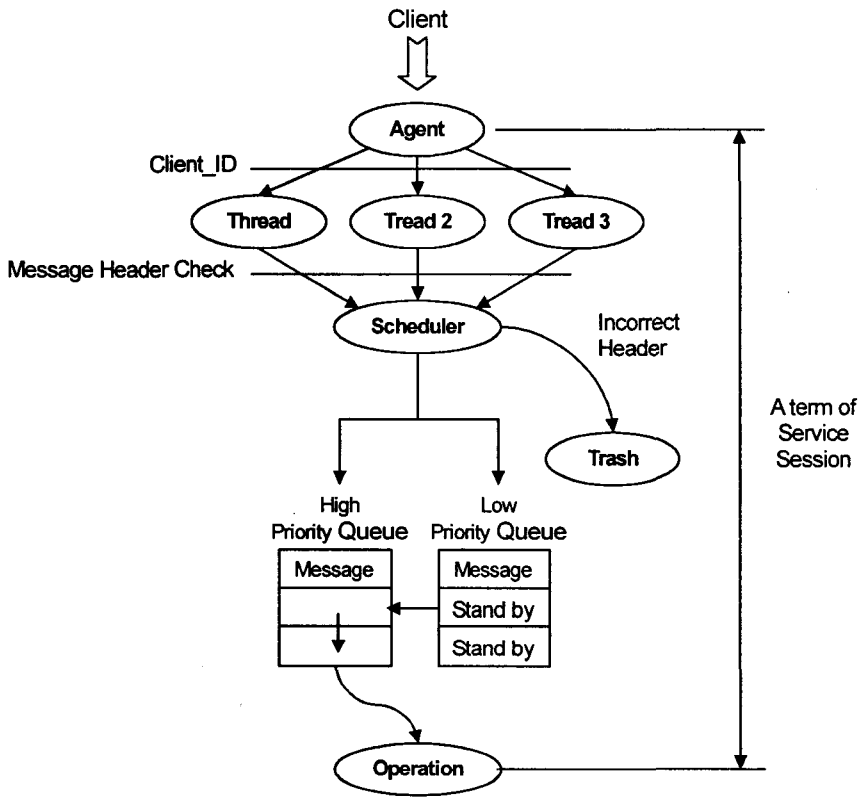
(배경율, 2003)에서 자세히 소개하였으므로 본 논문에서는 간략하게 흐름에 대한 방향성만 표시하였다. <그림 3>에서는 비대칭 인증서버 방식과 다중키 분산 접근법을 혼합한 최적 얼굴인증 서비스 개략도를 나타내었다.

<그림 3>에서와 같이 클라이언트는 인증기관에 서비스 제공자와 협약된 공개키를 요청하고, 그 공개키로 생체 데이터를 암호화해서 전자인증서 형태로 서비스 제공자(WWW Server)에 전달한다. 서비스 제공자는 전달받은 암호화된 생체 데이터를 인증기관으로부터 받은 개인키로 복호화하고, 복호화된 생체 데이터를 다시 서버 관리 Agent에 보낸다. 데이터를 처리하는 각 층에 대한 구조와 Agent가 위치하는 레이어의 형태는 <그림 4>와 같이 표현할 수 있다. 다음 Pseudo 코드는 Agent의 데이터 처리 프로세스를 표현한 것이다.



<그림 4> 분산 시스템의 계층(Layer) 구조

분산 객체 레이어(Distributed Object Layer)에 위치하는 에이전트(Agent)는 독립된 프로세스와 권한을 가지고, 메시지의 속성(Message Attributes) 및 기능 분배(Function Distribution)의 역할을 담당한다. 에이전트는 한 서비스의 세션 동안 수신된 메시지를 분석한 뒤 우선순위를 정한 후 기능에 맞는 서버로 그 메시지를 넘겨주고, 프로세스 충돌의 위험을 방지하기 위한 관리



<그림 5> 서버 Agent의 데이터 처리를 위한 프로세스 모형

기능을 제공하게 된다. Agent의 데이터 처리를 위한 프로세스의 모형은 <그림 5>와 같이 구성된다.

3. 얼굴인식 기술(Face Recognition Technology)

분산 환경에서 클라이언트의 얼굴을 효율적으로 인식하기 위해서는 클라이언트와 서버 간의 기능분리가 어느 정도 필요하다(배경율, 2003). 본 연구에서도 클라이언트와 서버 간 기능을 분리해서 처리하였으며, 클라이언트에는 얼굴 탐지와 특징 정보 추출을 위한 전처리 기법이 적용되었고, 추출된 데이터는 네트워크를 통해 서버로 전달되어 서버 레이어의 얼굴인식 콘트롤에서 등록된 특징 데이터와 전달받은 특징 데이터 간 매칭(Matching)기능이 수행된다.

3.1 얼굴 후보 영역의 탐지

<그림 3>의 4번 과정과 같이 클라이언트는 얼굴 탐지 및 특징 추출 기능은 ActiveX Control 형태로 구현하였다. 본 연구에서 구현한 얼굴 탐지는 얼굴 영역이 피부색을 가진다는 정보와 얼굴 크기의 비율정보를 사용하였다. 피부색은 컬러 모

델에서 특정한 영역에 분포되며, 이 영역은 RGB 칼라 모델에서 보면 3차원 정보로 표현되지만 YCbCr 컬러 모델에서는 밝기 성분인 Y를 제거하고 CbCr만의 2차원 정보로 단순화해서 표현할 수 있다. 클라이언트의 카메라로부터 획득된 RGB 컬러 영상을 YCbCr로 변환한 후 밝기 Y를 제거한 CbCr 도메인에서 피부색 영역을 모델링하기 위해 피부영역만 분리해내서 저장한다. 피부색 영역만 분리된 영상은 필터링을 통해 노이즈를 제거(Blurring)하고 가로 세로 비율로 얼굴 후보영역을 검출한다. 이 단계로 얻어진 피부색 영역과 비 피부색 영역을 이진화(Thresholding)하고, 이진화된 영상 내에서 1-D recursive filter(Deriche, 1988)를 적용한다. 마지막 단계로 후보지 영역 내에서 Labeling(Ishiyama, Y. et al., 1992)을 이용해 크기가 임계치보다 작거나 가로의 크기가 큰 영역은 노이즈로 판단하여 제거한다. <그림 6>의 (a)는 입력 영상이고, (b)는 (a)를 전처리해 탐지된 얼굴 후보 영역이다(Ming-Hsuan Y. et al., 2002).

3.2 SVM과 PCA를 이용한 얼굴 특징 추출

- SVM(Support Vector Machine)

SVM(Support Vector Machine)은 일반화(Generalization) 오류의 상한값을 최소화시키는 방법으로 찾아낸 얼굴 영역을 CbCr 컬러로 변환하여 그 분포로 피부색 영역을 업데이트하여 다음 프레임에서 획득된 영상내에서 얼굴영역을 추적하는데 활용되었다(Nello, C. and J., Shawe-Taylor, 2000). 얼굴 영역을 찾기 위해 훈련 데이터 $\{(x_i, y_i)\}$ $i=1,2,\cdots, K, N$ 에서 x_i는 얼굴 또는 비 얼굴 클래스 중 하나이며, $y_i \in \{-1, 1\}$는 해당 클래스의 레이블, $K(x_i, y_j)$은 커널 함수이다. SVM에서의 학습은 선형 제한 조건하에서 **식 1**을 통해 풀 수 있으며, 이 때 변수의 개수는 데이터의 개수와 동일하다(Alex J.S. and B., Schölkopf, 2003).

$$MaxQ(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j K(x_i, x_j)$$

$$(1)\ \sum_{i=1}^{N} \alpha_i y_i = 0 \qquad \text{수식 (1)}$$

$$(2)\ 0 \le \alpha_i \le C \ \text{ where C is a positive.}$$

위 식을 이용해 현재 프레임에서 SVM에 위해 검증된 얼굴 영역을 찾을 수 있었고, 이 영역은 다음 프레임에서 얼굴 영역과 크기, 위치 변화가 임계치 이하일 경우 계속 탐지하게 된다. 즉, 얼굴 영역을 둘러싼 사각형의 각 모서리끼리의 좌표 변화의 합에 대한 **식 (2)**가 임계치 이하이면 탐지를 계속한다(Sobottka, K. and I. Pitas, 1996). 이는 피부색 영역에 포함되지만 얼굴 영역으로 검증되지 못한 경우에 효과적이다(Xin X. et al., 2000).

$$Y(i) = \sum_{j} \left\| p(i+1)_j - p(i)_j \right\| \qquad \text{수식 (2)}$$

이렇게 처리된 얼굴 영역은 다시 PCA (Principal Component Analysis)에 의해 고차원 영상을 저차원으로 줄일 수 있다(Turk, M. and A. Pentland; 1991).

- PCA(Principal Component Analysis)

PCA(Principal Component Analysis)는 다변량 분석 방법으로, 전체 영상의 데이터를 데이터 분산이 큰 몇 개의 고유방향(Eigenfaces)에 대한 축으로 선형 투사시켜 데이터의 차원을 줄인다. 특히, 서로 다른 클래스의 차원을 줄여 간단히 표현할 수 있는 체계적이고 실용적인 얼굴인식 알고

리즘이라 할 수 있다(Givens G. et al., 2003).

SVM에 의해 탐지된 얼굴 영상에 Eigenface 메소드를 적용시키려면 얼굴 영상을 2차원의 벡터(Vector)로 표현해야 하며, N x N 크기의 얼굴 영상은 픽셀의 좌표에 해당하는 I(x,y)라 할 수 있으므로 벡터의 크기는 N2이 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 얼굴을 구하는 식과 얼굴 특징 데이터를 추출해서 전송하는 방법은 (배경율, 2003)에서 소개하였으므로 본 논문에서는 생략하였다.

4. 실험 결과 및 결론

실험 환경은 클라이언트 측이 펜웨스트社의 Lebeca 웹 캠(CMOS센서, 30만화소급)과 Notebook Pentium-III 1.0Ghz로 구성하였으며, 얼굴 등록 및 인증을 위한 서버와 인증서를 발급하는 인증기관에 해당하는 서버는 Pentium-IV 2.0Ghz급으로 구성하였다. SVM 및 PCA 학습은 상명대학교 소프트웨어학부생 192명으로부터 제공된 학습 집단(Training Set)이 적용되었다. 각 입력 영상은 학생들을 실시간으로 추출하여 유무선 인터넷 환경에서 등록 및 인증을 실험하였다. <그림 6>은 SVM과 PCA를 통해 추출된 영역과 결과값을 표현한 것이다.

(a) 원 영상

(b) SVM 처리된 영상

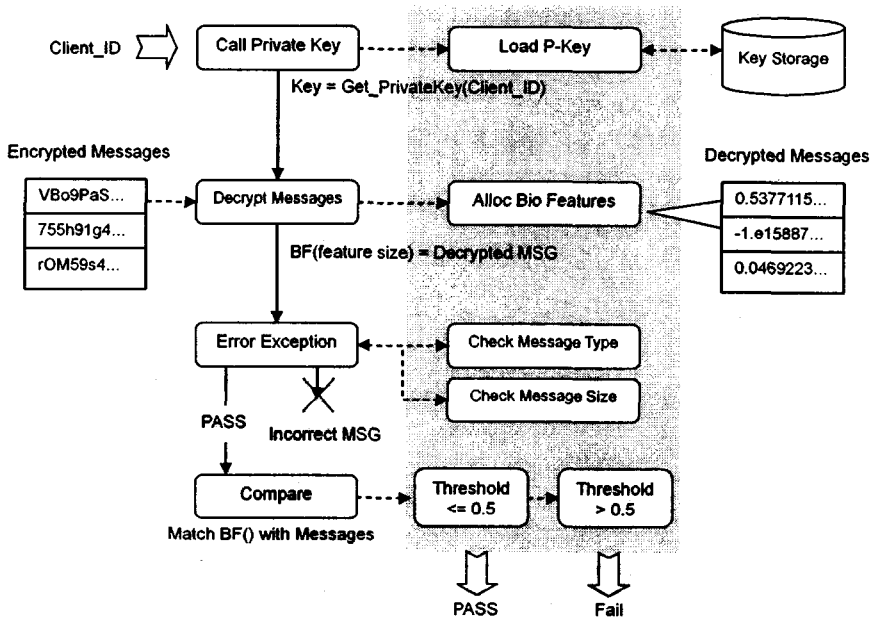
(c) SVM 마스킹 및 크기에 비례한 얼굴 영역 검출

(d) 원 영상에서 추출된 얼굴 영역

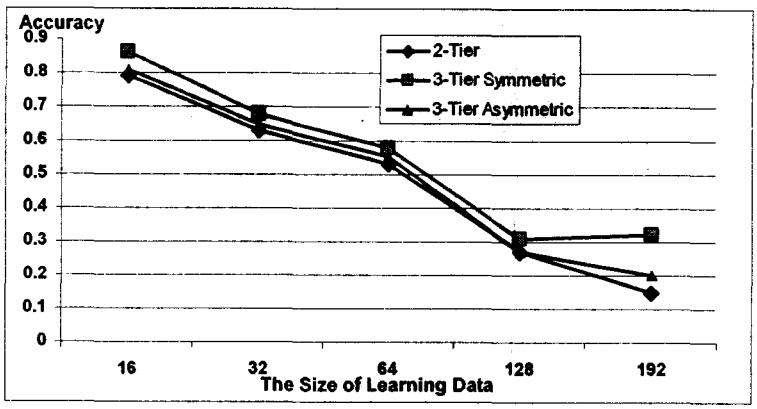
(e) Eigenface화된 얼굴 영상

<그림 6> 얼굴 후보 영역 탐지

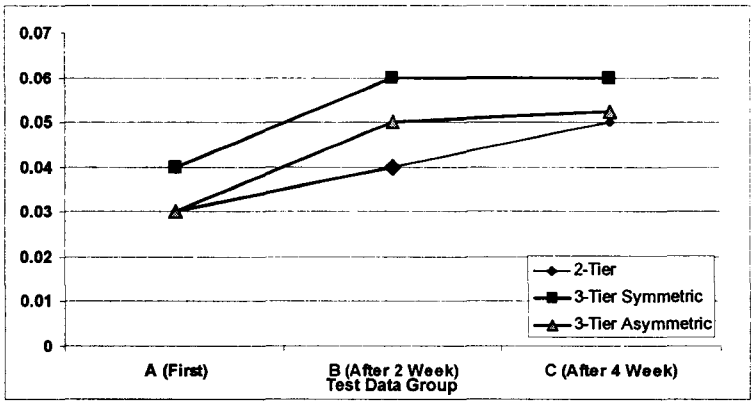
추출된 결과값은 인증기관으로부터 랜덤하게 생성된 공개키를 전달받아 대칭키 기반의 스트림 암호화 알고리즘인 RC4를 사용해 암호화된 상태로 서버에 전달된다. 전달된 데이터는 <그림 5>의 Agent 모형에 의해 처리되며, 메시지 큐에 메시지가 들어오면 Existed_MSG_In_Queue 함수를 호출하게 된다. 호출된 함수는 아래 <그림 7>의 Agent 프로세스와 같이 복호화 함수와 매칭



<그림 7> 생체 데이터 복호화 및 데이터 매칭을 위한 Agent 프로세스



<그림 8> 분산 계층수준에 따른 인증 정확성(Accuracy) 비교



<그림 9> 분산 계층수준에 따른 타인 수락율(FAR) 비교

함수에 의해 생체 데이터 간 매칭이 이루어지며, 준비된 샘플의 매칭 결과는 <그림 8>과 <그림 9>에 나타내었다. 인증 정확성의 범위는 0~1 사이이며, 0에 가까울수록 정확성이 높다.

본 논문에서는 생체인식 시스템을 분산된 환경에 적용하기 위한 몇 가지 설계 구조에 대하여 제안하였다. 제안한 구조 중 비대칭 인증방식의 경우 2-Tier 인증과 비교했을 때 인증 속도 면에서 거의 비슷한 속도(평균 0.2초)를 나타내었고, 인증 정확성이 비대칭 인증방식에서 크게 개선되어 학습 데이터의 크기가 128일 때는 동일한 수준까지 도달하였다. 타인 수락율(FAR; False Acceptance Rate)은 매칭 수준을 0~1 사이 중 0.65에 두고 테스트를 한 결과, A그룹(최초 등록 시의 매칭 결과)과 C 그룹(4주 후의 매칭 결과)에 대해서는 2-Tier와 동일한 결과를 나타내었으며, 2주 후인 B 그룹에 대해서는 100명이 100번 인증 시도했을 경우 타인 승락율이 한 명 증가하는 성능을 보였다. 그러나, 학습 데이터의 크기가 크거나 더 낮은 경우에는 서비스 동기화 문제(잘못된 메시지 전달로 프로세스가 취소되는 현상)로 인해 인증 정확성에 차이를 보였다. 이러한 차이를 최소화하기 위해서는 메시지 전달 이전에 전달 메시지를 간소화해야 하는 과제가 남아 있으며, 얼굴인식의 단점이라 할 수 있는 빛과 장소이동으로 인한 환경 변화의 처리 등이 분산환경에서 인증율을 저하시키는 요인이 되고 있다. 이후 지속적인 연구를 통해 현 접근법의 개선과 이기종 시스템에 적용할 수 있는 표준안에 대해서도 대비해야 할 것이다.

참고문헌

[1] 배경율. "인터넷 뱅킹의 사용자 인증을 위한 얼굴인식 시스템의 설계," **한국지능정보시스템학회논문지**, 제9권 3호 (2003), 193-205.

[2] Alex J. S. and B., Schölkopf, *A Tutorial on Support Vector Regression*, the NeuroCOLT2 Technical Report, 2003.

[3] Bellovin S.M. "Security problems in the {TCP}/{IP} protocol suite," *Journal of Computer Communications Review*, Vol. 19 (1989), 32-48.

[4] Deriche R. "Fast algorithms for low-level vision,"*9th International Conference on Pattern Recognition,* vol.1 (1988), 434 -438.

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

[6] Ishiyama Y., C. Funaoka, F. Kubo, H. Takahashi and F. Tomita, "Labeling Board Based on Boundary Tracking," *Proceedings of International Conference on Pattern Recognition (IAPR),* Vol. 4 (1992), 34 -38.

[7] Ming-Hsuan Y., D., Kriegman, and N., Ahuja. "Detecting Faces in Images: A Survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI),* Vol. 24, Issue 1 (2002), 34-58.

[8] Nello C. and J., Shawe-Taylor. *An introduction to Support Vector Machines,* Cambridge University Press, 2000.

[9] Sobottka K. and I. Pitas. "Segmentation and tracking of faces in color images," *2nd International Conference on Automatic Face and Gesture-Recognition* (1996), 14-16.

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

[11] Xin X., L., Shen, K., Wang, and K., Jia. "Automatic Human Face Detection," *ISO/IECJTC1/SC29/WG11 MPEG99/m6144* (2000), 274-280.

Abstract

Implementation and Design of Artificial Intelligence Face Recognition in Distributed Environment

Kyoung-Yul Bae*

It is notorious that PIN(Personal Identification Number) is used widely for user verification and authentication in networked environment. But, when the user Identification and password are exposed by hacking, we can be damaged monetary damage as well as invasion of privacy. In this paper, we adopt face recognition-based authentication which have nothing to worry what the ID and password will be exposed. Also, we suggest the remote authentication and verification system by considering not only 2-Tier system but also 3-Tier system getting be distributed. In this research, we analyze the face feature data using the SVM(Support Vector Machine) and PCA(Principle Component Analysis), and implement artificial intelligence face recognition module in distributed environment which increase the authentication speed and heightens accuracy by utilizing artificial intelligence techniques.

Key words : Biometrics, Face Recognition, Distributed Artificial Intelligence Authentication System

* Dept. of Software, Sang-Myung University