웹상의 BioAPI에 기반한 서명 다중 인증 시스템

(A Multiple Signature Authentication System Based on BioAPI for WWW)

윤 성 근 † 김 성 훈 †† 전 병 환 †††

(Sung Keun Yun) (Seong Hoon Kim) (Byung Hwan Jun)

요 약 차세대 보안 시장을 이끌어갈 신기술로 생체 인증 기술이 부상하고 있으나, 기존 시스템들은 대부분 생체 특징에 따라 개별 단위의 인증 방식을 제공하고 있다. 최근에는 이러한 개별 시스템들을 통합할 수 있도록 표준화하기 위한 연구가 활발히 이루어지고 있다. 본 논문에서는 생체 인증 기술의 표준화를 위해서 BioAPI 협회에서 발표한 BioAPI 명세서를 따르면서, 필기 서명이라는 단일 생체측정에 대해 함수적, 매개변수적, 구조적 접근법의 서로 다른 세 가지 검증기를 적용한 웹기반 인증 시스템을 제안한다. 시스템은 클라이언트-서버 구조이고, 클라이언트와 서버는 각각 BioAPI 규격에 따라 크게 세 계층으로 구성된다. 제안한 웹기반 단일 생체측정의 다중 인증 시스템은 사용자의 인증 거부율이 다소 증가되더라도 별도의 여러 생체측정을 요구하지 않으면서도 인증의 신뢰도를 크게 향상시킬 수 있다. 즉 세 가지 서명 검증기를 결합한 경우, 사용자의 인증 거부율(FRR)이 약 2.7배 증가하였지만 오류 승인률(FAR)은 4만분의 1로 감소하는 것으로 나타났다. 따라서 제안한 방법은 개방형 네트워크인 인터넷에서의 효과적인 신원확인 방법으로 활용될 수 있으며, 또한 다양한 생체측정을 이용하는 시스템으로 쉽게 확장될 수 있다.

키워드 : BioAPI, 서명 인식, 생체 인증, 보안 시스템

Abstract *Biometric authentication is rising technology for the security market of the next generation. But most of biometric systems are developed using only one of various biological features. Recently, there is a vigorous research for the standardization of various biometric systems. In this paper, we propose a web-based authentication system using three other verifiers based on functional, parametric, and structural approaches for one biometrics of handwritten signature, which is conformable to a specification of BioAPI introduced by BioAPI Consortium for a standardization of biometric technology. This system is developed with a client-server structure, and clients and servers consist of three layers according to the BioAPI structure. The proposed web-based multiple authentication system of one biometrics can be used to highly increase confidence degree of authentication without additional several biological measurements, although rejection rate is a little increased. That is, the false accept rate(FAR) decreases on the scale of about 1:40,000, although false reject rate(FRR) increases about 2.7 times in the case of combining above three signature verifiers. So the proposed approach can be used as an effective identification method on the internet of an open network. Also, it can be easily extended to a security system using multimodal biometrics.*

Key words : BioAPI, signature verification, biometric authentication, security system

1. 서 론

개인용 컴퓨터와 통신망이 급속히 발달되어 인간과 컴퓨터의 상호작용은 다양한 방법으로 발전되어 왔다. 사용자들은 관공서에서의 민원, 신용카드 또는 전자화폐를 이용한 전자상거래, 온라인 뱅킹을 통한 입·출금 등과 같이 기존에 사람이 직접 찾아다니며 처리해야 했던 일들을 웹상에서 처리하고자 하고 있으며, 이러한 요구는 거래의 기밀성(confidentiality), 무결성(integrity), 부인 방지(non-repudiation)를 위해 웹에서 개인 신원의 확인 절차를 중시하게 했다[1,2]. 기존에 개인 인증의 도

· 본 연구는 한국과학재단 지정 공주대학교 자원재활용 신소재 연구센터의 지원에 의한 것입니다.

† 비 회 원 : (주)투루게이트
patterny@truegate.net
†† 비 회 원 : 영동대학교 컴퓨터공학과 교수
escher@youngdong.ac.kr
††† 종신회원 : 공주대학교 정보통신공학부 교수
bhjun@kongju.ac.kr

논문접수 : 2003년 4월 2일
심사완료 : 2004년 6월 29일

구로 주로 사용되고 있는 것은 비밀번호(password)와 전자 서명(digital signature)을 이용한 방식이 있다. 그러나 비밀 번호나 전자 서명 등은 암기하거나 소지해야 하는 부담이 있고, 도용될 가능성이 높아 막대한 손실을 입을 수 있다. 그러므로 이러한 단점을 줄이기 위해 신원 확인의 신뢰성 증대를 위한 연구와 노력이 계속되고 있다. 이의 일환으로 차세대 보안 시장을 이끌어갈 신기술로 생체인식 기술이 부상하고 있으며, 이러한 생체인식 기술은 사람이 가진 신체적 습관 혹은 신체 일부를 이용하여 개인을 식별하는 기술이므로 소지나 암기의 부담이 없다. 기술은 주로 서명, 필체, 지문, 손바닥, 손등의 정맥, 손 모양, 얼굴, 음성, 홍채, 망막, 키보드 타이핑 습관, 걸음걸이 습관, 귀, 냄새 등을 이용하고 있다[3-7]. 생체인식 기술의 편리성과 보안성이 부각되면서 마우스의 지문 인식을 통한 개인용 컴퓨터의 보안, 기존의 열쇠를 대신하는 출입문에서의 잠금장치, 출·퇴근 시스템에 사용하는 등 여러 가지에 적용되기 시작했다.

그러나 대부분의 생체인증 시스템은 단일 생체 정보를 이용하므로 지문의 경우에서처럼 전체 인구의 5%가 신체장애 및 기타요인으로 생체 데이타를 사용할 수 없는 문제점을 가지고 있으며, 낮은 인식 오류율을 극복하기도 어렵다. 이때, 오류율은 크게 등록되지 않은 사람을 등록된 사용자로 인식하는 오인식율(False Acceptance Rate; FAR)과 등록된 사용자를 거부하는 오거부율(False Rejection Rate; FRR)로 구분된다.

최근의 생체인식 연구는 오인식률을 줄이고자 다수의 인식기를 사용하는 인증 시스템에 초점이 맞춰지고 있다. 그러나 상호 보유한 기술에 대한 이해가 부족한 상황에서 서로 다른 벤더에서 개발한 생체인식 기술을 결합한 다중 생체인증 시스템을 개발하는 것은 쉽지 않기 때문에, 대부분 두 가지의 생체 인식 기술이 합해진 시스템에 그치고 있는 실정이다.

이러한 문제점을 극복하기 위해, 최근에는 이러한 개별 시스템들을 통합하여 표준화하기 위한 많은 연구가 이루어지고 있다. 그 대표적인 예로 BioAPI 컨소시엄(consortium)에서 BioAPI 명세 버전(specification version) 1.1[8]을 통해 150개 이상 세분화된 생체 인식 하드웨어와 소프트웨어 벤더에 각기 다른 인터페이스, 알고리즘, 자료구조를 통합하기 위한 생체 인식기술의 표준화와 상호 보완적인 두 가지 이상 기술 활용에 대한 연구를 활발히 하고 있으며, 벤더별로 상이한 시스템에 표준화를 위해 일반적 인터페이스를 제공하여 서로 다른 생체인식 기술의 접목에 편리성 및 통합성을 제공하고 있다[9,10].

본 논문에서는 BioAPI의 표준을 따르면서, 그림 1과 같이, 웹상에서의 본인 인증을 위해 필기서명 생체측정을 사용하고 서로 다른 세 가지 서명 검증기를 통해 인증하는 시스템을 제안한다. 이러한 방식은 별도의 여러 생체측정을 요구하지 않으면서도 인증의 신뢰도를 크게 향상시킬 수 있으며, 특성이 다른 각 생체인증 기술을 손쉽게 대체하거나 확장시킬 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 BioAPI와 생체 인증을 위한 서명 검증기에 대해 다루고, 3장에서는 웹 다중 인증 시스템의 구성을 다룬다. 4장에서는 세 가지 서명 검증기를 이용하여 통합 판정한 결과를 분석하고, 5장에서는 결론 및 향후 연구 방향을 제시한다.

2. BioAPI와 생체 인증을 위한 서명 검증기

BioAPI 컨소시엄은 플랫폼 독립을 위해 2~4의 다계층 구조의 BioAPI[8]를 제안하고 있다. 최상위 레벨은 다음과 같은 기능을 제공한다. 그러나 본 논문에서는 개인 인증이 주목적이기에 식별은 고려하지 않는다.

- 등록(enrollment): 개인의 입력된 생체측정 데이타로부터 고유 정보의 생성 및 저장
- 인증(verification): 개인에 대해 등록된 샘플과 입력된 생체측정 샘플의 일대일 비교
- 식별(identification): 기존 DB에 등록되어 있는 샘플들과 입력된 생체측정 샘플의 일대다 비교

입력 장치의 설정에 대한 제어와 기술 의존적인 것은 하향식으로 접근하게 된다. 응용은 단지 상위레벨에 대한 사항만을 선택하여 사용하므로, 세부 기술적인 복잡한 것이나 서로 다른 인증 기술에 대해 자세하게 알아야 하는 필요성은 감소된다. 반대로 단일 기술을 가진 응용은 계층의 단계를 줄여 생체 인증 처리 또는 장치

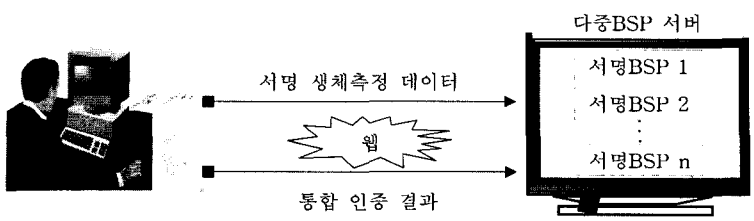


그림 1 웹상에서의 다중 서명 인증

제어의 기능을 증가시켜 하위 레벨의 접근을 정교하게 한다.

BioAPI는 응용이나 BSP(BioAPI Service Provider) 둘 중 하나에 생체측정 데이타를 저장하도록 하고 있는데, 대부분의 경우 BSP에 생체측정 데이타를 보관하여 서버의 안정성을 추구하고 있다. 본 논문에서도 이와 같은 구조를 유지하는데 그 이유는 알고리듬이 보다 안전한 환경에서 수행되어야 하고, 통합적인 이용자 DB 관리가 용이하며, 클라이언트 PC의 관리 문제를 줄일 수 있기 때문이다.

생체인증을 위해 사용가능한 신체 부위, 개인 특징, 그리고 데이타 획득 방법은 무수히 많다. 그러나 적합한 생체측정은 다음과 같은 특성을 지니고 있어야 한다[11,12].

- 보편성(universality): 모든 사람이 가지고 있는 특징
- 독특성(uniqueness): 개인별로 고유한 특징
- 영구성(permanence): 특징이 변화하지 않음
- 획득성(collectability): 특징을 센서가 쉽게 획득할 수 있고 정량화 가능

그러나 생체인증 시스템의 설계는 위의 특성을 모두 만족하는 생체측정이라고 해서 항상 적합한 것은 아니며, 다음과 같은 특성이 추가로 고려되어야 한다.

- 성능(performance): 시스템의 정확도, 속도, 강건성(robustness), 컴퓨터 자원 요구 등
- 수용성(acceptability): 일상적으로 사람들이 시스템에 거부감을 갖지 않는 정도
- 기만성(circumvention): 부정사용으로 시스템을 속이기가 용이한 정도

서명 검증 시스템은 서명을 입력하는 방법에 따라 두 가지로 구분된다. 하나는 종이에 쓴 서명을 카메라나 스캐너를 통해 입력하여 진위 여부를 판별하는 오프라인 방식이고, 다른 방법은 태블릿과 전자펜을 이용하여 실시간으로 데이타를 얻어 판별하는 온라인 방식이다[13]. 본 논문에서는 함수적, 매개변수적, 구조적 접근방법의 서로 다른 세 가지 온라인 서명 검증기를 생체 인증 시스템 구축에 사용한다.

2.1 함수적 접근법의 서명 검증기

함수적 접근은 입력된 서명 신호를 시간에 대한 특징 함수로 나타내고, 대응하는 특징값의 차이를 누적시켜 비교하는 방식이다[14]. 입력장치를 통해 입력된 데이타는 비교 알고리듬에 입력되는 시간에 대한 특징열을 구하는 특징 추출 과정을 거치게 되며, 사용될 수 있는 특징으로는 속력, 속도, 압력, 가속도, 거리 등이 있다.

2.2 매개변수적 접근법의 서명 검증기

매개변수적 접근법은 입력된 서명 신호에서 서명의 특징이 될 매개변수를 추출하고, 이것을 매개변수 공간에 대응시켜 등록된 서명을 대표하는 중심값과의 특징 공간상의 거리로써 참, 거짓을 판별하는 방법이다[15]. 매개변수적 접근의 서명 검증에 사용될 수 있는 특징은 크게 눈에 보이는 외부적 모양을 반영하는 특징과 눈에 보이지 않는 속도나 속력, 가속도 등의 내부적 속성을 반영하는 특징으로 구분된다. 서명의 특징을 반영하는 특징들에는 서명의 상하 좌우의 거리비, 중심으로부터의 거리 비율 등이 있으며, 이들 특징은 서명의 회전, 크기, 위치 등에 무관하도록 추출 과정에서 서명에 대해 정규화가 이루어진 후에 계산된다. 매개변수적 접근에서 이러한 특징들이 모두 서명 검증에 유용하게 사용되는 것은 아니며, 일반적으로 전향, 후향 탐색 방법을 이용한 특징 선택의 과정을 통하여 서명 검증에 특징을 선택하여 사용한다.

2.3 구조적 접근법의 서명 검증기

구조적 서명 검증은 서명으로부터 다양한 정보를 끌어내어 사용하기 위해 서명을 필기의 구성 요소들로 표현하고, 서명 검증에서 국부적으로 중요한 부분을 선택적으로 사용하는 방법이다[16]. 서명의 구조적 표현을 위해서 최소 속력점을 분할점으로 하여 얻어지는 부분을 기본요소로 정의하고, 필기의 방향변화에 의해 얻어지는 단순 회전형, 첨형, 종형 성분의 세 가지 종류를 서브 패턴으로 정의하여 서명을 구조적으로 표현하며, 정합을 위해서는 서브 패턴을 기본 단위로 한 동적 프로그래밍 기법에 병합 연산을 추가하여 서브 패턴의 변형을 흡수할 수 있도록 한다. 이를 바탕으로 국부적인 부분에 대해 학습 샘플들로부터 변화도와 복잡도를 추출하여 참조 패턴의 학습과 진위 판단 임계치를 설정한다.

3. 웹 다중 생체 인증 시스템

BioAPI 환경에서 전체 시스템은, 그림 2와 같이, 크게 인증이 필요한 웹 사이트와 서버, 클라이언트의 세 부분으로 구성된다. 클라이언트에서는 웹상에서의 인터페이스를 위해 ActiveX 컴포넌트로 등록 혹은 인증용 온라인 필기 서명을 입력받아 생체 식별 레코드(Biometric Identification Record; BIR)를 만들어 서버로 보낸다. 서버에서는 클라이언트로부터 받은 BIR을 개별 BSP에 보내 신규로 등록하거나 기존의 생체 데이타와 비교하여 인증 결과를 통보한다. 이와 같은 시스템은 사용자가 각 생체 정보별 BSP를 제공하는 업체 혹은 기관을 통해 개별 생체 정보를 등록한 후에 웹을 통해 전자상거래 또는 인터넷 뱅킹과 같은 개인 인증이 필요한 웹 사이트의 컨텐츠를 이용할 경우에 사용될 수 있다.

3.1 클라이언트 구성

실제 사용자가 이용하는 클라이언트의 구성은, 그림 3

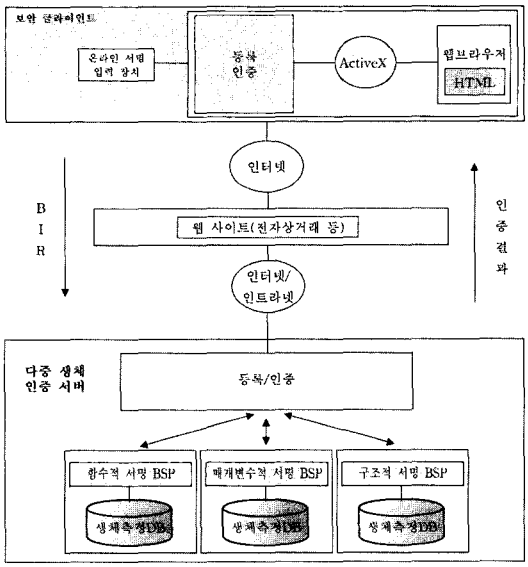


그림 2 전체 시스템 구성도

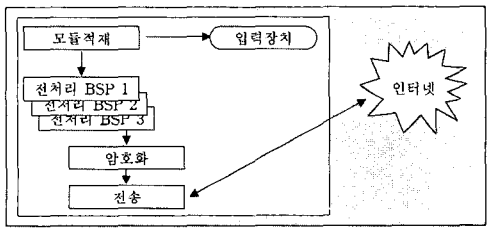


그림 3 생체인증 클라이언트 구성도

과 같이, 등록과 인증을 위한 인터페이스로 구성된다. 모든 기능이 웹상에서 제공되어야 하므로 ActiveX 컴포넌트로 표현되고 다음과 같은 기능들로 구성된다.

○ 등록 및 인증

- 모듈적재: BSP와 입력 장치의 동적인 부착
- 전처리 BSP: 원 생체 데이타에서 특징데이타를 추출하는 전처리
- 암호화: 전처리된 데이타의 암호화
- 전송: 생체 인증의 내역 및 데이타 전송

등록과 인증은 BioAPI의 표준 인터페이스 제공기능을 토대로 하여 모듈을 호출하는 이벤트를 발생시킨다. 모듈적재는 등록과 인증에 의해 발생된 이벤트에 따라 사용자 인터페이스와 입력장치, 그리고 BSP 모듈을 적재하고 설정한다. 전처리 BSP는 입력된 원 생체 데이타를 받아 BSP의 인증 알고리듬에서 필요로 하는 생체 데이타를 산출하여 BIR을 생성한다. 생성된 BIR을 네트워크 상에서 보호하기 위해 암호화 모듈을 거치며, 전송 모듈이 인증 내역을 BIR에 추가하여 웹을 통해 전송한다. 또한, 인증결과를 서버로부터 전송받는다. 클라이

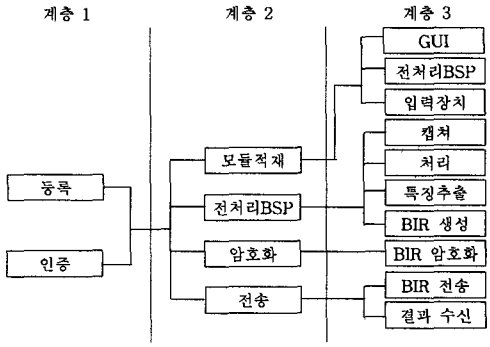


그림 4 생체인증 클라이언트 계층도

언트의 구조를 BioAPI의 계층으로 표현하면 그림 4와 같다.

3.2 다중 생체 인증 서버 구성

서버는 클라이언트를 통해 요청받은 등록과 인증 모두를 수행한다. 그림 5는 이러한 서버의 개념을 보여주고 있으며 주요 기능은 다음과 같다.

○ 등록 및 인증

- 전송: 생체 데이타 수신 및 결과 송신
- 복호화: 암호화된 BIR의 복원
- 데이타 복원: BIR로부터 전처리된 생체 데이타의 복원
- BSP 수행: 다중 인증기에 의한 DB로의 등록 및 DB에서의 인증

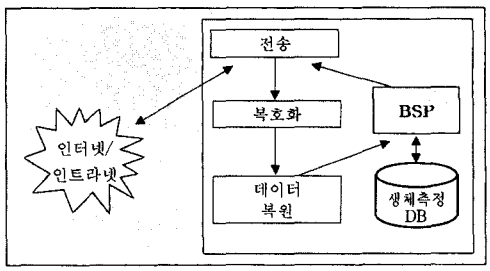


그림 5 생체인증 서버 구성도

전송 모듈은 인터넷 또는 인트라넷을 통해 클라이언트로부터 생체 데이타의 암호화된 BIR을 수신한다. 복호화 모듈은 암호화된 BIR을 해독하며, 생체 데이타 복원 모듈에서는 BIR로부터 전처리 BSP에서 추출된 생체 데이타를 복원한다. 복원된 생체 데이타는 실제 인증 알고리듬이 있는 BSP에 의해 DB에 신규 등록되거나 기존 DB와 비교하여 인증한다. 또한 인증 결과는 전송 모듈을 통해 클라이언트로 반환된다. 서버의 구조를 계층적으로 표현하면 그림 6과 같다.

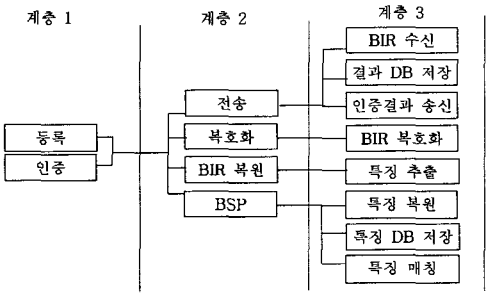


그림 6 생체인증 서버 계층도

4. 결과 및 분석

4.1 시스템 환경

본 논문에서는 생체 인증 시스템을 구축하기 위하여 ID와 세 가지 서명 BSP를 사용한다. 시스템 서버를 PentiumⅡ 300MHz Dual 상에서 구축하고, 클라이언트는 PentiumⅢ 450MHz 상에서 구축하여 생체 입력 장치 Wacom Intuos 4×5를 사용하여 사용자의 생체 데이타를 취득하며, Visual C++ 6.0으로 알고리즘을 구현하였다.

4.2 등록 과정

사용자 등록은 웹상에서도 적용이 용이한 ActiveX와 DLL로 구현하였다. 그림 7의 (a)는 필기 서명 인증을 사용하는 웹 사이트이고, (b)는 이의 HTML 코드를 나타낸다.

그림 8은 서명 등록 과정을 보여준다. 웹 페이지에서 ID 입력 후 '생체 서명 등록' 버튼을 누르면, (a)와 같이 타블렛을 통해 서명을 입력하게 된다. 서명의 등록은 총 3회 입력함으로써 수행된다. (b)는 서명이 등록된 기본 결과 화면이며, (c)는 각 서명 검증기에 등록된 서명들 간의 상이도에 대한 표준편차인 오차율을 자세하게 보여주고 있는 결과 화면이다.

4.3 인증 과정

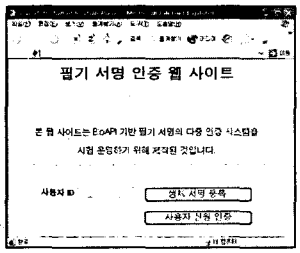
사용자의 인증을 위해서도 등록과 동일한 ID와 서명 입력을 수행한다. 이때, '사용자 신원 인증'을 선택한 후 단 1회의 서명 생체 데이타를 입력으로 받는다. 그러면, 클라이언트에서 전처리 BSP를 통해 처리된 데이타를 서버로 보내고 그 후 인증 결과를 받게 된다. 그림 9는 인증 결과를 보여준다. (a)는 인증 결과만을 보여주며, (b)는 각 서명 검증기별 인증률을 보여준다.

4.4 다중 생체 인증기의 통합 판정

각 서명 인증기 V_i에 대해 다음과 같은 수식이 성립한다.

$$t_i + frr_i + f_i + far_i = 1.0 \qquad (1)$$

이때, t_i는 진서명을 승인한 확률, frr_i는 진서명을 거

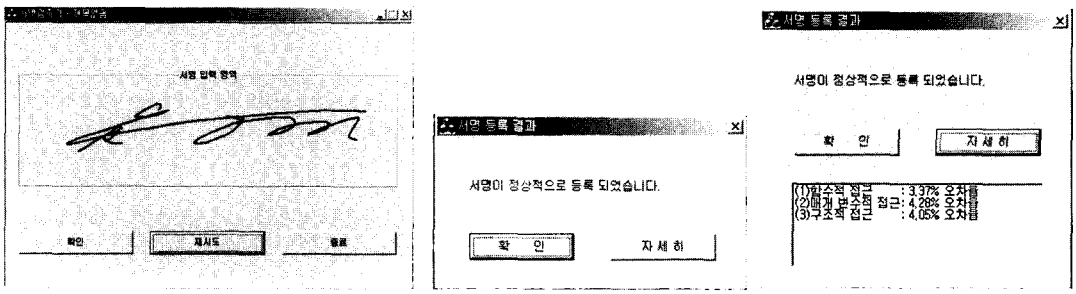


(a) 홈페이지 화면

```
<HTML>
<HEAD>
        <META name="GENERATOR" content="Microsoft Visual
Studio 6.0">
        <TITLE>Signature Authentication Page</TITLE>
        <OBJECT
classid="CLSID:9AB9F00A-FE75-4DBC-BF50-17DBA2D1A610"
codebase="/SignActiveX.ocx#Version=1,0,0,0"
                height=0 id=secuActiveX style="LEFT: 0px; TOP:
0px" width=0>
                <PARAM name="_Version" value="65536">
                <PARAM name="_ExtentX" value="26">
                <PARAM name="_ExtentY" value="26">
                <PARAM name="_StockProps" value="0">
        </OBJECT>
</HEAD>

<BODY >
        <P align=center>
        <FONT size=4 face=Verdana><LABEL><FONT size="6"
face="돋움"><b>필기 서명 인증 웹 사이트</b></FONT><br><br>
</LABEL>
<HR size=1 width=90%></P> 
<table border="1"  width="542" align=center>
    <tr>
    <td width="532" height="95"> <p align="center"><span
style="line-height:230%;"><font face="돋움" size="4">
    본 웹 사이트는 BioAPI 기반 필기 서명의 다중 인증 시스템을 <br>시험
    운영하기 위해 제작된 것입니다.  </font></span> </p></td>
    </tr>
    </table>
<div align="left"><br><br>
</div>
<table align="center" border="0" width="464">
    <tr>
    <td width="221" valign="top"> <p><font face="돋움"
size="3"><strong>사용자 ID</strong></font>
        <input name=szUserID style="LEFT: 271px; TOP: 273px"
size="16">
      </P></td>
    <td width="233"> <FORM name='formSGRegistration' method=post
action='./sgRegistration.asp' onsubmit='return Register()'>
        <p>
            <input name=btnRegister2 type=submit value="  생체 서명 등록
" style="font-family:돋움; font-size:14pt;">
            <br>
            <input name=btnRegister type=submit value=" 사용자 신원 인증
" style="font-family:돋움; font-size:14pt;">
        </p>
        </FORM></td>
    </tr>
</table>

<FORM name='formSGRegistration' method=post
action='./sgRegistration.asp' onsubmit='return Register()'>

<SCRIPT language=javascript>
<!--
self.focus();
//document.formFPRegistration.szUserID.focus();
-->
</SCRIPT>

<SCRIPT language='VBScript'>
<!--
Function Register
        Dim lReturn
        Dim szUserID
        Dim szOSPLocation
        Dim szTokenType
        On Error Resume Next
        szUserID = Trim(document.formFPRegistration.szUserID.value)
        if (Len(szUserID) = 0) then
          MsgBox("Please input UserID field first!")
          Register = FALSE
            Exit Function
        end if
 szOSPLocation  = top.location.host
szTokenType     = "REGISTRATION"
lReturn = document.secuActiveX.SetWBEConfig("WBE_HTTP_SSL"     , "")
lReturn = document.secuActiveX.SetWBEConfig("WBE_HTTP_PORT"    ,
"80")
lReturn = document.secuActiveX.SetWBEConfig("WBE_HTTP_ADDRESS",
szOSPLocation)
lReturn = document.secuActiveX.makeWBEToken(szTokenType, szUserID)
If Err > 0 then
        MsgBox("SecuWBE terminated abnormally")
    Register = FALSE
Exit Function
end If
if (lReturn <> 0) then
        MsgBox(document.secuActiveX.szErrorMsg)
Register = FALSE
Exit Function
end if
document.formFPRegistration.szRegistrationToken.value=document.secuActive
X.szReturnToken
Register = TRUE
End Function
-->
</SCRIPT>
</FORM>
</BODY>
</HTML>
```

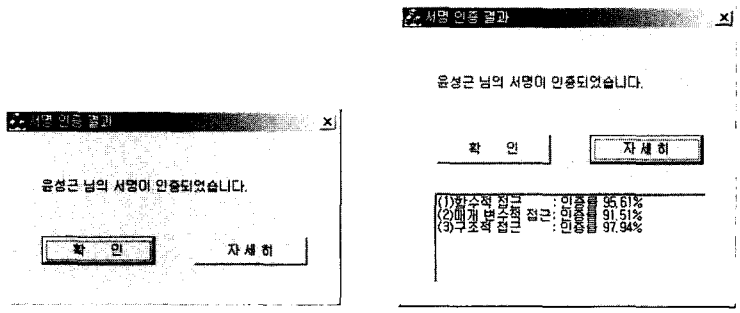
(b) HTML 코드

그림 7 필기 서명 인증 웹 사이트



(a) 서명 입력 (b) 기본 등록 결과 (c) 세부 등록 결과

그림 8 서명 등록 입력 및 결과



(a) 기본 인증 결과 (b) 세부 인증 결과

그림 9 서명 인증 결과

부한 확률(False Reject Rate; FRR), f_i는 거짓 서명을 거부한 확률, far_i는 거짓 서명을 승인한 확률(False Accept Rate; FAR)이다. 인증 결과가 참인 경우에는 t_i와 frr_i만 존재하고, 거짓인 경우에는 f_i와 far_i만 존재한다. 이때, frr_i 값이 크면 단지 사용자의 승인 재시도 횟수를 증가시킴으로서 다소의 불편함만이 초래되지만 인증의 신뢰도와는 무관한 요소이다. 그러므로 인증 시스템의 안전성은 far_i에 의해 결정된다고 말할 수 있다.

이제, 최종 판정을 위한 인식기의 통합 방법을 고려해 보자. 통합 판정은 크게 모든 검증기가 본인임을 인정해야 하는 방식, 다수결에 의한 방식, 적어도 하나의 검증기가 본인을 인정하는 방식 등을 고려할 수 있다. 보안 시스템에서는 신뢰도가 중요하기 때문에 일반적으로 모든 검증기가 인정해야 하는 AND 판정 방식이 사용된다.

AND 통합 검증기 V_{AND}가 거짓 서명을 승인할 확률 far_{AND}와 진서명을 거부할 확률 frr_{AND}는 다음과 같다.

$$far_{AND} = \prod_i far_i \tag{2}$$

$$frr_{AND} = 1 - t_{AND} = 1 - \prod_i t_i = 1 - \prod_i (1 - frr_i) \tag{3}$$

예로써, 함수적 검증기 V_f, 매개변수적 검증기 V_p, 구조적 검증기 V_s에 대해 frr_i가 모두 0.1일 때, 각각의 far_i와 통합 검증기 V_{AND}의 far_{AND}는 표 1과 같다.

표 1 통합 판정 결과

검증기 \ 확률	far_i	frr_i
V_f	0.016	0.1
V_p	0.025	0.1
V_s	0.012	0.1
V_{AND}	0.0000048	0.27

결과적으로, 다중 생체 인증을 통한 AND 판정의 경우 본인 거부율이 약 3배 높아져 사용자에게 다소의 불편을 끼치게 되지만, 보안에 있어 중요한 사항인 오승인률을 획기적으로 낮출 수 있음을 알 수 있다. 그러므로 별도의 추가적인 생체측정을 요구하지 않으면서도 다중 인증기를 사용함으로써 인증의 신뢰성을 크게 향상시킬 수 있다.

5. 결 론

본 논문에서는 생체 인식 기술을 적용하여 본인 인증을 하는데 있어 다양한 생체 기술의 응용과 보유 기술의 공유 그리고 손쉬운 생체 인증 시스템의 확장이 가

능한 방법을 제시하였다. 시스템의 요소기술로써 크게 웹 보안, 생체 인증, BioAPI를 사용하였으며, 생체 인증 기술의 표준화에 중점을 두었다.

먼저, 세계 표준화 기관인 BioAPI 협회에서 제공하는 BioAPI 명세서를 기반으로 웹상에서 클라이언트-서버 방식의 생체 인증 시스템을 구성하였다. 쇼핑몰과 같은 웹 사이트에서 인증이 필요한 경우, 사용자가 클라이언트에서 입력 장치와 전처리 BSP를 통해 생체 정보를 생성하여 생체 인증 서버에 보내게 된다. 사용자와 서버 간의 신속하고 정확한 데이타의 전달을 위해 ActiveX 컴포넌트를 사용한다. 클라이언트와 서버 모두 BioAPI의 응용 프로그램 인터페이스를 사용하여 다양한 다른 생체 인식 기술의 손쉬운 적용이 가능하다. 특히, 본 논문에서는 서명 생체 데이타라는 단일 측정에 대해 세 개의 서로 다른 서명 검증기를 적용하여, 개별 인증시보다 재입력의 요구는 다소 증가되지만 인증의 신뢰도를 크게 향상시킬 수 있음을 증명하였다.

향후에는 다양한 생체 측정을 이용하는 인증 시스템에 관한 연구와 웹상에서의 실시간 처리 및 생체 데이타의 보안에 대한 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] S. S. Y. Shim, V. S. Pendyala, M. Sundaram, and J. Z. Gao, "Business-to-Business E-Commerce," *IEEE Computer*, Vol. 33, No. 10, pp.40-47, Oct. 2000.

[2] T. W. Sandholm, "Unenforced E-Commerce Transaction", IEEE Computer, Vol. 1, No. 6, pp.47-54, Nov. 1997.

[3] G. Lawton, "Biometrics: A New Era in Security," IEEE Computer, Vol. 31, No. 8, pp.16-18, Aug. 1998.

[4] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," IEEE Computer, Vol. 33, No. 2, pp.56-63, Feb. 2000.

[5] S. Pankanti, R. M. Bolle, and A. Jain, "Biometric: The Future of Identification," IEEE Computer, Vol. 31, No. 8, pp.46-49, Feb. 2000.

[6] J. L. Wayman, "Federal Biometric Technology Legislation," IEEE Computer, Vol. 33, No. 2, pp.76-80, Feb. 2000.

[7] R. Wildes, "Iris Recognition: An Emerging Biometric Technology," Proc. of the IEEE, Vol. 85, No. 9, pp.1347-1363, Sep. 1997.

[8] BioAPI Specification Version 1.1, BioAPI Consortium, Mar. 2001.

[9] C. J. Tilton, "An Emerging Biometric API Industry Standard," IEEE Computer, Vol. 33, No. 2, pp.130-132, Feb. 2000.

[10] T. Wessels and C. W. Omlin "A Hybrid System for Signature Verification," Proc. of the IEEE-INNS-ENNS IJCNN, 2000.

[11] Morris and K. Thompson, "Password Security: A Case History," *Communications of the ACM*, Vol. 22, No. 11, pp.594-597, Nov. 1979.

[12] A. Jain, L. Hong, and S. Pankanti, "Biometric Identification," *Communications of the ACM*, Vol. 43, No. 2, pp.91-98, Feb. 2000.

[13] R. Plamondon and S. N. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 22, No. 1, pp.63-84, Jan. 2000.

[14] 유재룡, 김성훈, 김재희, "다이나믹 프로그래밍을 사용하는 서명검증에서의 클래스 학습방법에 관한 연구", *전자공학회논문지*, 제32권, B편, 제2호, pp.154-161, 1995. 2.

[15] S. H. Kim, M. S. Park, and J. Kim, "Applying Personalized Weights to a Feature Set for On-line Signature Verification," *Proc. of 3rd Int'l Conf. on Document Analysis and Recognition*, IAPR, pp.882-885, Aug. 1995.

[16] 김성훈, 장문익, 김재희, "필기의 구조적 표현에 의한 온라인 자동 서명 검증 기법", *정보처리논문지*, 제5권, 제11호, pp.2884-2896, 1998. 5.

윤 성 근

2000년 영동대학교 컴퓨터공학과(공학사). 2002년 공주대학교 대학원 전자계산학과(이학석사). 2002년~현재 ㈜트루게이트 연구원. 관심분야는 생체보안

김 성 훈

1988년 서강대학교 전자공학과(공학사) 1990년 연세대학교 대학원 전자공학과(공학석사). 1996년 연세대학교 대학원 전자공학과(공학박사). 1996년~현재 영동대학교 컴퓨터공학과 부교수. 관심분야는 패턴인식, HCI

전 병 환

1989년 연세대학교 전자공학과(공학사) 1991년 연세대학교 대학원 전자공학과(공학석사). 1996년 연세대학교 대학원 전자공학과(공학박사). 2000년~2001년 ㈜모리아테크놀로지 연구소장. 1997년~현재 공주대학교 정보통신공학부 컴퓨터전공 부교수. 관심분야는 컴퓨터비전, 가상현실