한국산학기술학회논문지
Vol. 8, No. 4, pp. 952-960, 2007

청소년을 위한 인증시스템의 설계에 관한 연구

홍기천[1*], 김은미[2]

A Study of Authentication Design for Youth

Ki-Cheon Hong[1] and Eun-Mi Kim[2]

요 약 현재의 대부분의 웹사이트에서는 본인확인을 위한 로그인 절차를 수행하고 있다. 그러나 아이디와 패스워드와 같은 간단한 특징은 도용의 우려가 많아서 본인 확인의 신뢰를 할 수 없다. 이 때문에 청소년들은 타인의 아이디와 패스워드를 가지고 불법매체 사이트를 쉽게 접근할 수 있다. 그래서 본 논문에서는 사용자 인증 시스템을 설계할 때, 적용 가능한 특징들을 알아보고, 이를 바탕으로 인증 시스템 설계를 제안한다. 인증 시스템은 저수준 인증 방법과 고수준 인증 방법으로 나누었다. 저수준 인증 방법은 핸드폰을 통한 인증번호 부여 방법과 요즘 많이 쓰이고 있는 공인 인증서를 이용하는 방법이다. 고수준 인증 방법은 아이디와 패스워드를 지문 인식, 문자 인식, 음성 인식, 영상 인식에서의 특징들과 결합하여 인증하는 방법이다. 이를 위해서 본 논문에서 알아본 특징은 지문인식, 얼굴인식, 홍채인식, 문자인식, 정맥인식, 음성인식에 사용 가능한 특징들이다. 이 특징들 중, 지문 인식, 문자 인식, 음성 인식, 영상 인식은 보편화된 개인용 컴퓨터에 저가의 장비만 있으면 인증 시스템을 구현할 수 있다. 이러한 다중특징을 이용하여 웹사이트를 구축하면 본인 확인에 대한 신뢰도를 한층 높일 수 있다.

Abstract Most Websites perform login process for authentication. But simple features like ID and Password have no trust because most people worry about appropriation. So the youth can easily access illegal media sites using other's ID and Password. Therefore this paper examine features be adaptable to authentication system, and propose a design of authentication system using multiple features. A proposed authentication system has two categories, such as low-level and high-level method. Low-level method consists of grant of authentication number through mobile phone from server and certificate from authority. High-level method combines ID/Password and features of fingerprint, character, voice, face recognition systems. For this, this paper surveys six recognition systems such as fingerprint, face, iris, character, vein, voice recognition system. Among these, fingerprint, character, voice, face recognition systems can be easily implemented in personal computer with low cost accessories. Usage of multiple features can improve reliability of authentication.

Key words : Authentication, Websites, Multiple Features

1. 서론

인터넷의 보급과 개인용 컴퓨터의 확산으로 인하여 가상세계인 사이버공간이 급속도로 확장하고 있다. 현재 만 7세 이상의 50%가 넘는 2200만명이 한달에 한번 인터넷을 사용하고 있다. 인터넷이 우리의 생활과 밀접하게 연관되어 있음은 누구도 부인하지 않는다[1].

지금까지 현실세계에서는 행동주체의 인증을 위하여 법적 효력을 갖는 신분증이나 신분을 증명할 수 있는 서류와 행동주체를 직접 눈으로 확인하였으나, 사이버공간에서의 행동주체는 현실세계에서처럼 직접 확인할 수가 없어 개인인증의 신뢰도에 약점을 가지고 있다[2].

인터넷상에서 현재 사용하고 있는 인증방법으로는 아이디와 패스워드를 입력하는 것이다. 이러한 텍스트 중심의 인증방법으로는 본인확인에 대한 신뢰성을 확보할 수 없다. 이러한 비신뢰성은 초등학생과 청소년들로 하여금 성인사이트, 폭력사이트, 자살사이트와 같은 인터넷 불건전 정보로부터 보호하기 어렵기 때문이다. 이러한 정보는 성장기의 청소년들에게 치명적인 해를 끼칠 수 있다고 사료된다.

[1]전주교육대학교 컴퓨터교육과
[2]호원대학교 컴퓨터게임학부
*교신저자: 홍기천(kchong@jnue.ac.kr)

표 1. 음란사이트 접속 횟수(1주 당)

횟수 / 연령별	1회	2~3회	4~5회	5회 이상
초등	91.7%	5.0%	1.7%	1.7%
중등	65.2%	21.5%	7.6%	5.7%

표 2. 폭력사이트 접속 횟수(1주 당)

횟수 / 연령별	1회	2~3회	4~5회	5회 이상
초등	85.9%	7.7%	3.2%	3.2%
중등	55.2%	22.4%	9.8%	12.6%

표 3. 자살사이트 접속 횟수(1주 당)

횟수 / 연령별	1회	2~3회	4~5회	5회 이상	이용안함
초등	2.6%	6.2%	0.9%	0.4%	89.9%
중등	45.5%	41.1%	9.8%	2.7%	0.9%

표 1~3은 청소년들이 불건전 정보에 접속한 사례를 보여준다[3].

고속통신과 멀티미디어 환경이 급속도로 발달하고 있는 컴퓨팅 기술에 있어서 이에 적합한 바이오메트릭(biometric) 정보를 이용한 사용자 인증 방법을 사용한다. 바이오메트릭에서는 긍정적인 사용자 인증을 위하여 각 개인이 가지는 독특한 생리학적(physiological), 행동학적(behavioral), 형태학적(morphological) 등의 독특한 특성을 사용한다. 단, 이들 특성은 관찰될 수 있고, 정량화될 수 있어야 한다. 현재의 기술로 가능한 바이오메트릭은 망막패턴, 지문, 필체 및 서명, 음성, 얼굴 등이 있다. 실제로 인간에 의한 상대방의 인식은 많은 경우 상황에 따라서 필요한 바이오메트릭 정보를 사용한다고 볼 수 있다. 바이오매트릭 정보를 이용한 정보통신망 보안의 가능성은 인지되어 왔지만, 고가의 통신비용과 입력 장치비용으로 인하여 실용성을 인정받지 못하였다. 최근 초고속 통신망의 구축과 멀티미디어 기술의 발전으로 수년 내에 저렴한 비용으로 바이오메트릭 정보가 자유롭게 실시간 송수신이 가능하게 될 것이다. 현재의 기술수준으로 컴퓨터환경에서 사용 가능한 바이오메트릭 정보는 음성, 얼굴, 지문, 서명, 망막패턴을 들 수 있다. 일반적으로 멀티미디어 컴퓨터에는 음성과 영상 입출력 장치의 부착이 현실적이며, 사용자 인증을 위하여 지문, 서명, 망막, 패턴 인식을 위한 관련 장치를 부착하는 것은 경제성 면에서 볼 때에 아직 비현실적이다. 멀티미디어 기능을 갖춘 일반 개인용 컴퓨터에 음성과 시각정보처리 기능을 추가하는데 수십만 원 정도의 저렴한 비용이 들며, 영상회의 등의 수용에 의하여 일반화 될 예정이므로, 앞으로 이 비용은 더욱더 낮아질 것으로 예상된다[4].

2. 현 사용자 인증기술의 문제점

최근에 들어서 전 세계적으로 정보통신망이 구축되고, World Wide Web으로 대표되는 인터넷이 일반 사용자에게로 확산되고 있다. 이는 정보화 사회로 의 전환을 더욱 더 앞당길 것으로 예상되며, 이에 따른 적지 않은 문제점도 제기되고 있다. 그 중 중요한 문제는 정보통신망의 개방과 보안의 상호 모순적인 딜레마이다. 정보화 사회로의 발전을 위하여 정보의 유통을 원활하게 지원하여야 하고, 이를 위하여 정보통신망의 개방은 필연적이다. 현재 군사적인 긴장이 계속되고 있는 중동의 이스라엘도 정보통신망을 개방하겠다고 선언한 것을 보면, 정보통신망의 폐쇄로 인한 불이익이 얼마나 심각한지를 알 수 있다. 그러나, 개방시스템의 지향을 위한 정보통신망의 무분별한 개방은 보안상 심각한 문제를 야기할 수 있다는 것은 자명한 사실이다. 현재의 보안기술은 많은 문제점을 내포하고 있으며, 특히 사용자 인증에 있어서 주로 인위적인 ID, 패스워드에 의존하고 있으므로, 정보통신망을 통한 보안 사고가 발생하기 시작했으며, 확산될 가능성이 매우 높다. 특히, 최근에 들어 개인정보에 대한 보호문제가 심각하게 대두되고 있다. 이러한 정보통신망 관련 보안사고는 성공적인 정보화 사회로 넘어가기 위한 정보화 마인드 확립에 걸림돌이 되며, 실제로 경제, 사회에 혼란을 야기할 수도 있다[4].

컴퓨터 사용자의 정당성을 확인하거나, 요구하는 서비스에 대한 정당성을 확인하는 사용자 신분 확인의 메커니즘은 컴퓨터 시스템에 대한 접근 제어 및 중요 서비스 제공여부에 대한 판단 기법으로 현재 패스워드를 가장 많이 사용하고 있다. 그 이외의 신분 확인 기법으로 생체적인 방법, 동적인 패스워드 기법 등이 있는데 이들 중 네트워크 환경에서는 주로 일반 패스워드와 동적인 패스워드 기법이 사용되고 있다[5].

▶ 일반 패스워드

인터넷상에서 연결되어 있는 수많은 서버들 중에 유닉스 계열이 단연 제일 많다. 최근 윈도우즈 NT 등도 서버로써 구축되고 있으나 대부분의 시스템은 유닉스 기반의 전통적인 계정과 패스워드 메커니즘을 이용하여 사용자 신분을 확인하고 있다. 유닉스뿐만 아니라 네트웍에 연결되어 서비스를 제공하는 시스템에서 주로 사용하는 방식이 패스워드에 의한 방식이 일반적인데, 이 방식의 한계

점은 인간의 기억력에 의존하고 있으며 동일한 패스워드를 반복적으로 사용함으로써 노출될 위험성이 있으며 사용자가 패스워드를 분실하였을 경우 본인의 신분확인 방안이 인터넷과 같은 네트워크로는 불가능하다.

▶ 동적인 패스워드

매 회 접속 시마다 일정한 함수 관계에 의하여 패스워드를 새로 생성하는 기법으로 Codebook Challenge Response 방식 등이 있으며 주로 일 방향 함수를 이용한다. 일회용 패스워드 생성기와 같은 소프트웨어 혹은 하드웨어 장비가 필요한 경우가 많고 한번 동기화에 실패할 경우 복구에 문제점이 있으며 비용도 많이 드는 단점이 있다. 그러나 보다 안전한 시스템을 구성하기 위하여 최근에 많이 도입되고 있다.

3. 인증시스템에 적용 가능한 인식 이론

3.1 지문인식

생채인식 패턴 중, 지문인식은 각종 보안 구역의 통제, 시스템의 접근, 무선 단말기를 이용한 은행 업무 처리를 위한 인증 절차 등에 사용되고 있다. 지문 인식 기술은 매우 높은 정확도, 변별력을 보유하고 있지만 접촉식 생체 측정 수단으로서 친화성이 떨어지는 단점을 가지며 사용자가 매우 협조적인 자세를 가져야만 확인/인증 절차를 수행할 수 있는 단점을 가진다. 그러나 편의성, 소형화의 장점을 가지고 있어 현재 보편화된 컴퓨터 시스템에서 사용이 용이한 인식 방법이기 때문에 생체인식 시장의 높은 점유율을 차지하고 있다[2].

지문 인식의 절차는 크게 지문 영상 획득, 특징 추출, 지문 영상 인식의 3 단계로 나뉜다. 지문 영상 획득은 스캐너 입력, 잡음 제거, 융선 보정과 같은 단계를 거쳐서 정확하고 깨끗한 지문 영상을 획득한다. 특징 추출 단계에서는 각 개인들이 가지는 고유한 특징을 추출하는 단계이다. 그림 1은 지문의 형태를 보여준다. 검정부분을 융선(ridge)이라하고, 밝은 부분을 골(valley)이라고 한다. 그리고 특징 추출에 사용되는 특징점으로는 분기점, 끝점, 중심점, 삼각주와 같은 정보를 사용한다[6].

지문인식 알고리즘은 크게 융선의 특징점을 이용하는 방법과 땀구멍(sweat glands/pores)을 이용하는 방법으로 나눌 수 있다. 전자의 방법이 입력 센서의 가격도 저렴하고 가장 많이 사용하는 방법이다. 후자의 방법은 해상도 1000dpi 이상의 고해상도 센서를 요구하기 때문에 가격이 비싸다는 점과 땀샘은 고해상도의 센서에서만 추출이 가능하므로 가짜 지문을 쉽게 구분할 수 있는 점이 있다.

그림 1. 지문의 형태[19]

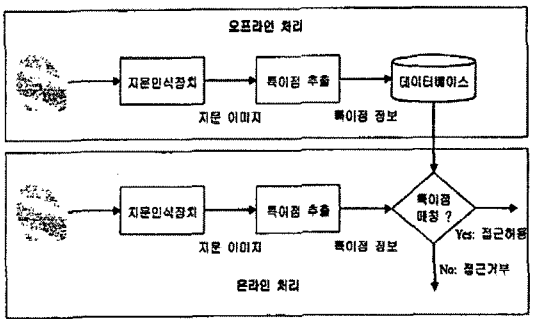


그림 2. 지문 처리 절차

3.2 얼굴인식

최근 생체인식 기술로서 변별 능력이 탁월하고 활용성 및 편리성이 뛰어난 얼굴 인식 기술이 부각되고 있다. 얼굴 인식 기술은 얼굴 검출 기술과 인식 기능으로 구분된다. 얼굴 인식 기능은 검출된 얼굴을 이용하여 사람을 인식하는 시스템이다. 따라서 얼굴 검출 시스템의 성능에 의해 그 인식 및 검증 성능이 영향을 많이 받는다. 얼굴 추출 기술은 얼굴 및 표정 인식을 위한 필수적인 전 처리 기술이다 [8].

얼굴 인식 인증의 장점은 다음과 같다[7].

(1) 자신만의 고유 생체 정보를 사용하여 도용, 분실의 위험이 없다.
(2) 얼굴 정보의 이용으로 문제 발생 시, 사후 대처가 용이하다.
(3) 타 생체 정보와 비교하여 부가적인 하드웨어 장비 필요 없다. 일반 PC사양에 일반 PC 카메라를 사용할 수 있기 때문이다.

얼굴 검출 기술이란 배경으로부터 얼굴 영역을 추출하는 기술이다. 여기에 쓰이는 알고리즘으로는 특징 기반 알고리즘과 영상 기반 알고리즘으로 나뉜다 [8]. 특징 기반 알고리즘은 인간의 경험 정보(Heuristic)에서 비롯된

알고리즘이다. 사용하는 특징들로는 얼굴 윤곽(edge), 눈썹이나 눈동자와 같은 그레이(Gray) 정보, 객체의 외향을 구분하기위한 컬러(Color) 정보, 비디오상에서의 움직임(Motion) 정보 등과 같은 특징을 사용하는 알고리즘이다. 그러나 이 방법은 얼굴 외양이나 환경 조건의 비예측성 때문에 어려움을 내포하고 있다. 영상 기반 알고리즘은 이런 비예측성을 통계학적인 차원에서 접근한 방법이다. 즉, 얼굴의 위치를 통계적으로 표현한 방법이다. 신경망 방법, 통계적 방법이 여기에 속한다.

그림 3은 얼굴 영역 추출 과정을 단계별로 보여준다[9].

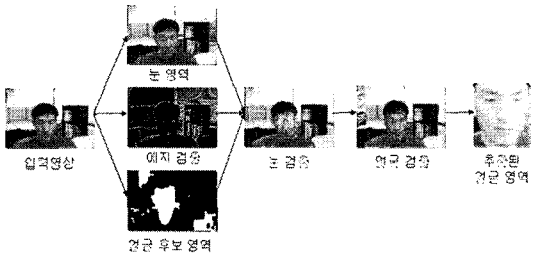


그림 3. 얼굴 영역 추출 과정

3.3 문자인식

문자인식 기술은 온라인 인식과 오프라인 인식으로 나뉜다. 온라인 인식은 사용자가 PDA나 테블렛과 같은 입력기에 문자를 입력하면 곧바로 인식되는 방법이고[10], 오프라인 인식은 종이에 문자를 기입하고, 이 문자를 스캐너를 이용하여 그림으로 저장한 후, 인식하는 방법이다[11, 12, 13]. 온라인 인식보다 오프라인 인식이 훨씬 어렵다. 아직까지도 오프라인 문자 인식은 계속 연구되어진다.

온라인 인식 방법은 PDA 또는 태블릿에 펜으로 입력하면서 곧바로 인식하는 방법이다. 한글을 입력할 때, 시작점과 끝점, 획의 순서등과 같은 특징을 이용하여 인식하는 방법이다. 상용화된 온라인 인식 기술은 거의 100%에 가까울 정도의 인식률을 자랑하고 있다.

오프라인 인식 방법은 인쇄체 문자 인식과 필기체 문자 인식으로 나뉜다.

인쇄체 인식은 프린터로 프린트된 문자를 인식하는 것이고, 필기체 인식은 사람이 직접 종이에 기입한 내용을 인식하는 것이다. 이 방법은 종이에 기입된 문자를 인식하는 방법이므로 온라인 인식 방법에서 사용하던 특징들에 대한 정보가 전혀 없다. 단지 배경은 흰색이고 글자는 검정색이라는 정보밖에 없다.

문자인식의 응용으로는 자동차 번호판 자동 인식, 서명 인증, 우편물 자동 분류 등의 분야를 들 수 있다. 그림 4는 자동차 번호판 자동 인식의 단계를 보여준다[14].

3.4 홍채인식

지문인식의 경우는 타인의 지문을 특수 테입에 복사하여 사용하는 경우 이를 막을 수 없으며, 음성인식의 경우도 타인의 음성을 녹음하여 사용하는 경우 동일한 상황이 된다. 얼굴인식의 경우 때에 따라 각 개인의 표정 및 형태가 변화가 가능한데, 이를 수용하기 쉽지 않으며, 타인의 얼굴을 모방하는 경우 식별할 수 있는 정확도가 높지 않다는 것이 지금까지의 연구 결과이다. 망막인식의 경우도 최근 질병이 생기는 경우 망막의 형상이 변하는 것이 밝혀지면서 최근에는 사용이 중단되고 있다.

그림 5에서 보는 바와 같이 사람 눈의 동공과 흰 부위 사이에 존재하는 영역을 홍채라고 하며 홍채의 특징은 안과학자들로 부터의 눈이 지문이라 불리며 1961년과 1965년에 학계에 보고되었다. 이렇게 각 사람들이 다르게 가지는 홍채의 특징을 추출하고 그 정보를 이용하여 개개인을 인식하는 것을 홍채인식 이라한다 [15].

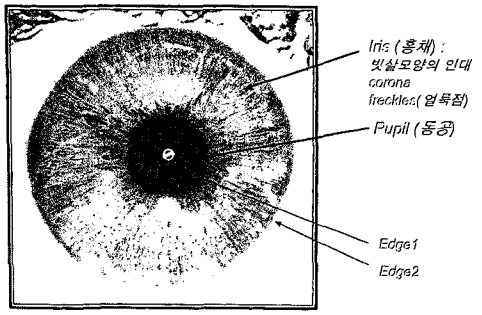
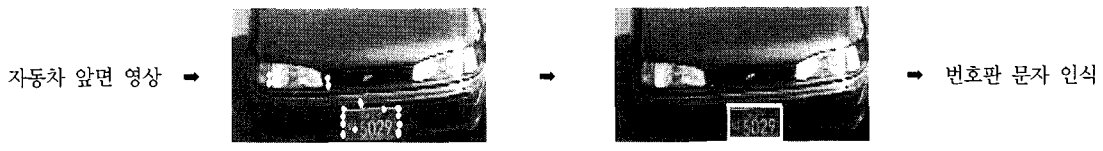


그림 5. 홍채의 영상



(a) 자동차 번호판 후보 영역 추출 (b) 자동차 번호판 영역 추출

그림 4. 자동차 번호판 인식 단계

홍채인식 시스템의 구성도는 그림 6과 같다. 먼저 CCD 카메라로 안구 영상을 획득하고, 이미지 전처리 과정을 거쳐서 웨이블렛 알고리즘을 이용하여 특징을 추출한다. 이 특징을 신경망 알고리즘을 이용하여 인식한다 [15]. 그림 7은 안구 영상에서 홍채와 내,외부 경계를 보여준다 [16].

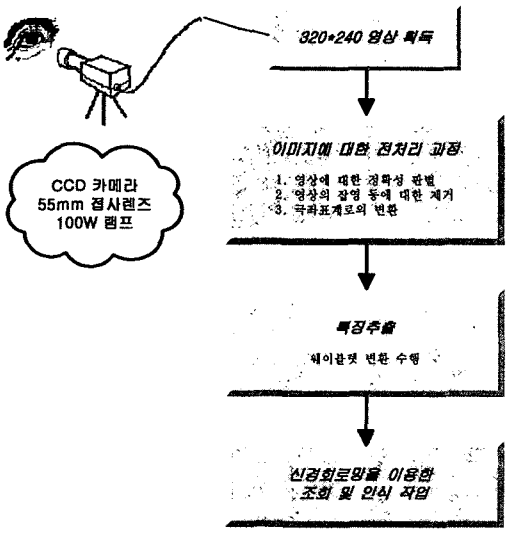


그림 6. 홍채인식의 시스템 흐름도

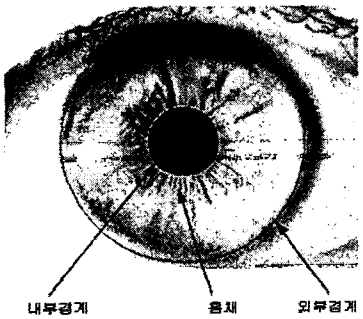


그림 7. 홍채와 내·외부 경계의 모습

3.5 음성인식

음성 인식 기술 및 화자 인식 기술은 HMI(Human-Machine Interface) 기술 중 인간에게 가장 편리한 인터페이스 핵심 기술 중의 하나이다. 음성 인식 및 화자 인증 기술은 현재의 기술 수준이 완벽한 단계는 아니며 기술적 한계를 많이 가지고 있다. 그럼에도 불구하고 상용화가 활발히 진행되고 있으며 활용 분야는 점차 넓어지고 있다. 현재 주로 상용화되고 있는 기술은 화자독립 고립 가변어 인식 기술이며 점차 연속어로 진화하고 있는 단계이다[17].

음성 인식을 위한 기술에는 Hidden Markov Model(이하 HMM), Neural Network, Dynamic Time Warpping, Knowledge Based Method 등 여러 방법들이 있다. 이들 방법 중 대용량, 가변어휘 인식에는 HMM이 가장 좋은 성능을 나타낸다. HMM은 연속적인 시간선상에서 나타나는 음성 신호의 특징들을 통계적인 방법을 통해 분석하여 인식하는 방법이며, 음성 인식의 다른 방법들과 마찬가지로 크게 학습 과정과 인식 과정의 두 가지 과정으로 나눌 수 있다. 그림 8에 HMM을 이용한 음성인식의 개략적 과정을 나타내었다[17].

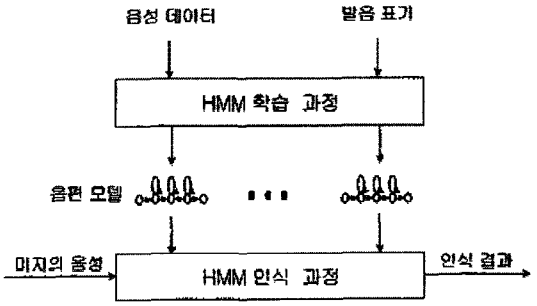


그림 8. HMM을 이용한 음성인식 과정

3.6 정맥인식

생체측정학을 이용하여 개인식별 또는 인증을 자동적으로 해 주는 장치를 생체측정시스템(Biometric System)이라 한다. 생체인식시스템으로는 개인의 신분을 인식하기 위해 신체적(physiological characteristic)또는 행위적 특징(behavioral characteristic)을 추출하여 자동적으로 인식하는 시스템으로 구분되어진다. 신체적 특징을 이용한 생체인식시스템의 예로는 지문, 얼굴, 망막의 혈관패턴, 홍채, 손 형상, 손등의 정맥 분포패턴 등이 있으며 행위적 특징을 이용한 생체인식시스템으로는 서명, 성문(음성) 등이 있다. 이와 같은 특징들을 이용한 많은 종류의 생체인식시스템이 개발되어 시장을 개척하고 있으나 각각의 시스템이 장단점을 가지고 있어 어떤 제품이 향후 시장을 석권하리라는 식의 예측은 아직 미지수다 [18].

현재 안정적인 생체특징으로 새롭게 부각되는 특징으로는 피하에 위치하는 혈관패턴을 인식하여 본인여부를 판별하는 기술이며, 피하에 위치하는 생체특징에서 얻을 수 있는 장점으로는 여타의 생체인식시스템에서 발생되는 오염, 상처, 시간경과에 따른 생체특징의 변형 등에 거의 영향을 받지 않는다는 점이다 [18]. 그림 9는 정맥 패

턴 영상에서 전처리 과정을 거쳐 추출된 정맥 패턴을 단계별로 보여준다.

그림 9. 정맥패턴 추출 알고리즘의 각 단계별 과정

4. 다중 특징을 이용한 인증 시스템 설계

앞서 3장에서는 인증 시스템의 특징에 대해서 알아보았다. 현재의 웹사이트는 아이디와 패스워드와 같은 특징으로는 신뢰도가 높은 인증이 어렵기 때문에 기존의 특징과 결합된 방법으로 인증 방법을 설계해야 한다. 그래서 본 논문에서는 저수준 인증 방법과 고수준 인증 방법을 제안한다.

4.1 저수준 인증(Low-level Authentication)

저수준 인증 방법에는 2가지가 있을 수 있다. 첫 번째 방법은 인증번호를 통한 인증 방법이고, 두 번째 방법은 공인 인증서를 이용한 방법이다.

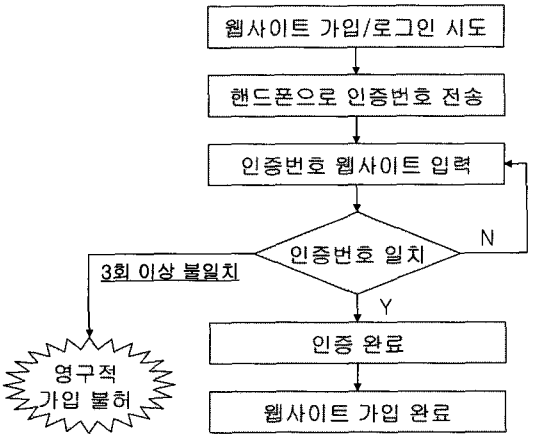


그림 10. 핸드폰 인증번호를 이용한 방법

첫 번째 방법은 가입자가 웹사이트 가입을 할 때, 입력 필드에 인증번호를 입력하게 하는 방법이다. 이 인증번호는 가입자 핸드폰으로 메시지가 전송되며, 이 인증번호는 서버에서 무작위로 조합된 숫자열, 문자열, 숫자-문자열 등의 형태로 만들어진다. 가입자는 전송된 인증번호를 웹사이트의 입력 필드에 입력하면 된다. 만약 전송된 인증번호와 입력된 인증번호가 일치하지 않는 경우에는 가입을 취소시킨다. 만약 이러한 경우를 3회 이상 실시하였을 경우에는 도용의 경우로 판단하여 서버에서는 더 이상의 인증번호를 전송하지 않도록 한다. 그러나 이 방법은 도용의 여지가 아직 남아있다. 만약 청소년이 부모의 핸드폰을 휴대하고 있다면 이 방법은 무용지물이기 때문이다. 그림 10은 핸드폰 인증번호를 이용한 방법의 순서도를 보여준다.

두 번째 방법은 공인된 인증서를 사용하는 방법이다. 요즘에는 인터넷 뱅킹, 폰 뱅킹과 같은 서비스를 이용할 때, 공인된 인증서를 부여받는다. 이 인증서에는 가입자에 대한 많은 정보를 포함되어 있기 때문에 첫 번째 방법보다는 훨씬 안전한 시도 방법이라고 사료된다. 이 방법은 가입자가 웹사이트에 접속하여 가입을 시도할 때, 입력 필드에 가입자 본인의 공인 인증서 패스워드를 입력하게 하는 방법이다. 이 패스워드는 대부분 사용자의 머릿속으로 기억하고 있기 때문에 안전한 방법이라고 하겠다. 그림 11은 공인 인증서를 이용한 방법의 순서도를 보여준다.

첫 번째 방법과 두 번째 방법 모두 가입과 로그인 과정에 그대로 적용된다.

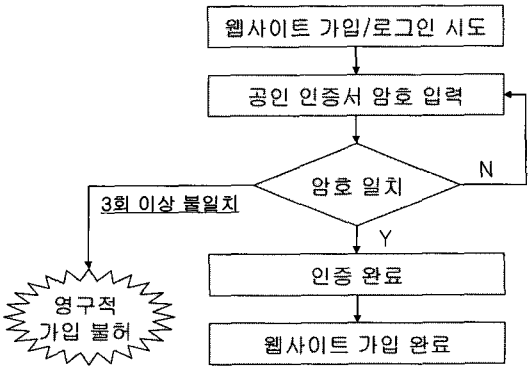


그림 11. 공인 인증서를 이용한 방법

4.2 고수준 인증(High-level Authentication)

3장에서 기술한 6가지의 인식 방법 중, 지문 인식, 문자 인식, 음성 인식, 얼굴 인식은 현재 보편화된 개인용 컴퓨터에서 저가의 장비 구입으로도 충분히 구현될 수 있다. 홍채 인식, 정맥 인식에는 고가의 장비가 구비되어야 하므로 개인용 컴퓨터에 구현하기에는 불가능하다. 고수준 인증 시스템은 아이디, 패스워드를 지문 인식, 문자 인식, 음성 인식, 얼굴 인식 기술과 병행하는 것이다. 그림 12는 다중 특징을 이용한 인증 시스템 흐름도를 보여

준다.

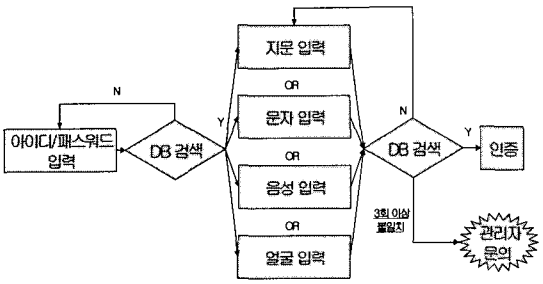


그림 12. 다중 특징을 이용한 인증 시스템 흐름도

그림 12에서 보는 바와 같이 이미 가입된 사용자가 웹사이트에 로그인을 하기 위해서는 먼저 아이디와 패스워드를 입력하고, 이를 데이터베이스에서 검색한다. 만약 불일치하면 계속 입력하게 하고, 일치하면 위의 지문, 문자, 음성, 얼굴등을 입력한다.

4.2.1 지문 입력을 선택한 경우

3.1에서 지문인식에서 언급된 바와 같이, 땀샘이 융기되어 일정한 흐름이 만들어진 지문은 그 모양이 개개인마다 다르다는 특징을 가지고 있다. 요즘은 노트북, 태블릿 PC에 지문인식 기술을 도입하여 지문인식 장치가 내장되어 나오는 경우가 많다. 그래서 사용자의 컴퓨터에 지문인식 장치만 부착이 되어 있다면 안전하게 사용할 수 있는 인식 방법이다. 이 노트북은 사용자의 지문을 입력받아서 부팅 및 웹사이트 로그인시 사용할 수 있도록 하고있다. 최근에는 USB메모리에도 지문 인식 기술을 사용하고 있다. USB메모리는 분실하기 쉽기 때문에 보안에 취약하기 때문이다.

4.2.2 문자 입력을 선택한 경우

문자 입력의 경우, 100명의 사용자에게 같은 글자를 쓰게 한다면 아마 100가지 형태의 글자가 나온다. 이렇듯 사용자마다 글씨를 쓰는 특징이 있기 때문에 사용자를 구별할 수 있는 좋은 방법이다. 현재까지 온라인 필기체 인식률은 95%이상을 자랑하고 있기 때문에 PDA와 같이 키보드가 없는 장비인 경우에는 이미 사용되어지고 있다. 이를 위해서는 기존의 사용자 컴퓨터에 있는 마우스이외에 태블릿 또는 터치 스크린과 같은 장비가 장착되어야만 한다. 태블릿은 태블릿의 판위에 웹사이트에서 요구하는 문자열을 입력하게 하면 된다. 터치 스크린은 기존의 컴퓨터 모니터에 터치 판넬을 장착하여 터치 스크린으로 만든다. 그래서 사용자는 웹사이트에서 요구하는 문자열을 모니터에 터치 스크린용 펜을 이용하여 직접 입력하게 한다. 터치 스크린은 은행의 현금지급기, 학교의 자동발급기등에 이미 설치되어 사용되고 있다. 그러나 터치 판넬을 유리로 만들어져 있기 때문에 무겁기도 하고 감도가 떨어진다는 단점이 있다. 그래서 개인적으로는 태블릿을 사용하는것을 권장한다.

우리가 신용카드를 위해서 사용하는 서명도 문자 인식의 연구 대상이다. 필적의 개인차가 존재한다는 전제에 기초하여 서명을 사전에 등록해 놓고 그 데이터와 서명을 조회하여 인증하는 방법이다. 서명 인식은 신용카드를 도난당하여 타인이 서명하였을 때 사용하기 좋은 방법이다. 서명 인식은 필순, 필압, 운필속도 등의 필기 운동의 정보를 사용한다. 아직까지는 서명 인식이 상용화되지 못하고 있다. 그 이유는 서명이 음성 인식과 마찬가지로 쉽게 복제가 가능하다는 신뢰도 문제가 있기 때문이다. 그래서 이러한 문제점을 보완하기 위해서 다른 인증 기술과 병행하는 추세이다.

4.2.3 음성 입력을 선택한 경우

음성의 경우도 지문이나 홍채처럼 각 개인마다 다르고 음성의 상대적 불변성으로 인하여 목소리 변조가 불가능하다. 흔히 감기나 흥분시에 귀로는 목소리가 변해 들린다고 느끼지만 일반적으로 영향을 받지 않는 것이 특징이다. 그래서 요즘은 핸드폰에 음성을 이용하여 메뉴를 선택하는 기능이 내장되어 있다. 운전중에도 핸드폰으로 해결해야할 부분이 있기 때문이다. 또한 요즘 자동차에는 사고 예방을 위해서 핸즈프리를 의무적으로 장착하도록 되어있다. 음성을 웹사이트에서 인증 방법으로 사용하기 위해서는 멀티미디어 헤드셋만 있으면 된다. 마이크를 이용하여 웹사이트에서 요구하는 문자열을 읽어주기만 하면 된다. 그러나 주의할 점은 마이크에 사용자 목소리 이외에 다른 잡음이 들어가서는 안되기 때문에 요즘 나오는 고성능 마이크가 있어야 한다.

4.2.4 얼굴 입력을 선택한 경우

얼굴 인식은 아직 실용화의 초기단계에 있고, 현재 대학 및 연구소를 중심으로 활발하게 연구중인 기술이다. 현재까지의 실용화 단계는 주로 현금 자동인출기의 고객 확인등에 사용되고 있고 점차 다른 분야로의 확대가 이루어질 계획이다. 이 기술의 주요응용분야는 현금자동인출기, 범죄자검색시스템, 국경의 통해자 검색 시스템등에 적용될 수 있다. 이 기술은 제한된 데이터베이스에서는 최고 95~98%의 정확성을 갖지만 얼굴의 특성과 주변 환경에 따른 변화 때문에 높지 않은 편이다[24]. 얼굴을 인증시스템의 특징으로 사용하기 위해서는 웹카메라만 있으면 된다. 웹카메라를 통해서 사진을 찍어서 데이터베이스와 비교하는 방식이다.

4.2.5 그 외의 경우

앞서 기술한 4가지 인식 이론들 이외에 정맥 인식과 홍채 인식의 특징을 개인용 컴퓨터 환경하에서 사용이 완전히 불가능한 것은 아니다. 정맥이나 홍채도 영상의 형태로 서버에 전송을 하는 방법이므로 정맥 영상이나 홍채 영상을 PC카메라로 촬영하여 입력하면 된다. 그러나 정맥이나 홍채와 같은 패턴은 해상도가 높은 특수한 카메라가 있어야만 효과를 제대로 발휘할 수 있다. 그러나 앞으로는 해상도 높은 특수한 카메라도 가격이 저렴하게 되어 PC카메라같이 우리 안방에서 사용할 수 있을 것이다.

다중 특징을 이용하여 인증 시스템을 설계하려면 사용자는 번거로움을 느낄 수 있다. 그러나 투명하고 건전한 인터넷 문화를 이끌어 나가기 위해서는 감수를 해야한다. 또한 지문 영상, 문자 영상, 얼굴 영상, 음성을 웹사이트의 데이터베이스에 저장하기 때문에, 해당 웹사이트는 보안에 신경을 많이 써야한다. 그러기 위해서는 데이터의 최첨단 암호화 방식을 채택하여 사용자들로 하여금 해당 사이트의 신뢰도를 높여야 한다.

5. 결론 및 제언

인터넷 시대에는 실세계의 모든 현상들이 디지털화되어 가고 있다. 그러나 이러한 추세에는 순기능과 역기능이 항상 존재한다. 실세계의 모든 현상에 자동화가 도입이 된다는 점에서는 바람직하다. 그러나 인간의 사회적 역할의 감소, 보안 및 감시, 범죄의 지능화고도화, 청소년 문제등과 같은 사회적인 부작용을 낳고 있다. 특히 미래를 짊어지고 갈 청소년들의 디지털 방황은 더욱 심각하다. 앞서 서론에서 알아보았듯이 청소년의 이러한 방황은 날로 늘어가고 있는 추세다.

본 논문에서는 인터넷상에서 사이트 인증 방법으로 적용될 수 있는 여러 가지 특징들을 알아보았다. 이 특징들이 연구된 배경으로는 6T를 논할 수 있다. 6T란 IT(Information Technology), BT(Bio Technology), NT (Nano Technology), ST(Space Technology), ET(Environment Technology), CT(Culture Technology)를 의미한다. 이 중 BT는 현재 대두되고 있는 이슈이다. 앞서 알아보았던 문자인식을 제외한 5가지의 특징들이 모두 BT에 속한다고 볼 수 있다. 이러한 특징들을 100% 구현하기에는 많은 과제들이 남아있다.

본 논문에서는 인증시스템에 사용가능한 저수준 인증 방법과 고수준 인증방법에 대해서 제안하였다. 저수준 인증 방법은 핸드폰 또는 공인인증서를 이용하는 방법이다. 이 방법은 청소년들과 부모들과의 정보화 격차를 감안한다면 그리 권장할 방법은 아니다. 왜냐하면 부모들이 공인인증서를 사용하면서 청소년인 자녀에게 비밀번호가 쉽게 노출이 된다는 것이다. 또한 핸드폰을 이용한 인증 방법도 마찬가지이다. 부모들이 집안 내부에서 핸드폰을 놓는 위치가 자녀들에게는 무방비로 노출되어 있기 때문이다. 이러한 저수준 인증 방법을 보완할 방법으로는 고수준 인증 방법이 있다.

고수준 인증 방법은 웹사이트에 로그인할 때 기존의 아이디/비밀번호 방식과 병행하여 지문인식 기술, 문자인식 기술, 얼굴인식 기술, 음성인식 기술과 같은 4가지 최신 기술을 도입하는 방법이다. 웹사이트 관리자 입장에서는 초기에 투자비용이 들겠지만 정보보호 차원에서 생각한다면 웹사이트의 대내외적 신뢰도를 향상시키는 방안이 될 수 있다. 그리고 사용자 입장에서는 4가지 기술을 사용하기 위해서 들어가는 추가 비용도 많지 않다는 것이다. 이러한 최근 기술에서 사용자가 구비해야할 장치로는 지문 인식 장치, 태블릿, 웹카메라, 멀티미디어 헤드셋 정도이다. 요즘은 저렴한 가격에 고성능을 갖는 장치들이 많이 나와 있기 때문에 사용자도 쉽게 접근할 수 있다.

나열한 특징 이외에도 현재 연구되어지고 있는 특징으로는 심장 박동 인식, DNA 인식, 치아 및 구강구조 인식, 손 모양 인식 등을 들 수 있다. 이러한 특징들이 많이 연구가 되어서 청소년들의 디지털 세상에 밝은 미래가 보였으면 하는 바람이다. 또한 인터넷에서 사용하고 있는 인증방법의 체계적인 검증의 노력이 있어야 하겠다.

참고문헌

[1] 한국인터넷정보센터, "국내인터넷사용자 현황", 한국인터넷정보센터, 2001.

[2] 이남일, "이기종 지문인식기를 통한 사용자인증시스템 개발", 정보통신부 보고서, 2003

[3] 한미정, "불건전정보 유통 및 이용실태", 정보통신부 보고서, 2002

[4] 이필규, "바이오메트릭 정보에 기반한 정보통신망 사용자 인증 시스템 개발", 정보통신부 보고서, 1999.

[5] 공병훈, "결함-허용 기법을 이용한 신분확인 방안", 정보통신연구진흥원 보고서, 2002

[6] 유영기, "지문이미지 획득장치 기술", 정보처리학회지, 제 6권 제 4호 pp. 32-43, 1999.

[7] 최종무, "얼굴 인식에 기반한 인터넷 사용자 인증 기술", 정보통신부 보고서, 2002

[8] 김영로, "얼굴 인식을 이용한 특정인 검색 및 출입통제 시스템 개발", 정보통신부 보고서, 2003

[9] 이성환, http://image.korea.ac.kr/korean/research.html, 2000.
[10] 김인광, "문자인식기능과 명함인식기능을 갖춘 펜형 PDA개발", 정보통신부 보고서, 2001
[11] 김수형, "한글이 포함된 필기체 문자열의 오프라인 인식에 관한 연구", 정보통신부 보고서, 1999.
[12] 남기완, "자동차 영상에서의 번호판 추출과 문자 인식에 관한 연구", 정보통신기반 신호처리 시스템 설계기술 워크샵, 2002.
[13] 김진형, "필기체 한글 주소 고속인식 방법론에 대한 연구", 한국전자통신연구원 보고서, 1999.
[14] 이효종, "도로 영상에서 차량 번호판 인식", 1999.
[15] 임성훈, "초고속망하에서 홍채인식을 이용한 지능형 신원확인 시스템 개발에 관한 연구", 정보통신부 보고서, 1998.
[16] 조성원, "저용량 고신뢰도 홍채인식 보안 시스템 개발", 정보통신부 보고서, 2002
[17] 이윤근, "IMT-2000용 음성 및 화자 인식 기술 개발", 정보통신부 보고서, 2000.
[18] 임상균, "임베디드 정맥인식 전용 하드웨어 개발", 정보통신부 보고서, 2003.
[19] 김창수, "지문인식시스템 보안취약성 분석 S/W 개발", 한국정보보호진흥원 보고서, 2001.

홍 기 천(Ki-Cheon Hong) **[정회원]**

- 2000년 8월 : 전북대학교 전산통계학과 이학박사
- 2001년 8월 ~ 현재 : 전주교육대학교 교수

<관심분야>
프로그래밍 언어 교육, 이러닝

김 은 미(Eun-Mi Kim) **[정회원]**

- 1997년 8월 : 일본 오사카 대학 정보공학과 졸업(공학박사)
- 1998년 8월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

<관심분야>
소프트웨어 품질평가, 객체지향 시스템