通信情報保護學會誌
第2卷 第4號, 1992. 12

개체의 특징에 의한 신분인증에 관한 고찰

A Study of Identity Verfication by Biometrcs

이필중* · 조주연**

1. 서 론

정보화 사회를 추구하는 현대에 이르러서는 사회의 대부분의 정보의 교류들이 컴퓨터 네트워크를 통하여 이루어지고 있을 뿐만 아니라 개인 및 단체의 주요 정보들이 컴퓨터 시스템을 매개로 저장, 관리되고 있다. 이에 따라 타인의 불법적인 침입, 임의변경 그리고 데이타 조작으로부터 자신의 정보를 보호받고자 하는 요구 또는 점점 절실해 지고 있는 실정이다. 더구나 현대사회같은 고도의 익명성을 가지는 사회일수록 한번의 노출이 초래하는 손실의 결과는 엄청난 것이라 할 수 있다. 이와같은 정보보호의 필요성에 부응하기 위해 정보보안 시스템의 개발이 가속화되고 있으며 그 중 가장 기본적이면서도 무엇보다 필요한 것이 바로 사용자의 신분인증 시스템의 개발이다. 현대의 컴퓨터 시스템은 공개적인 네트워크를 통하여 노출되기 마련이며 그럼에도 불구하고 적법한 사용권을 가진 사용자만이 이를 이용할 수 있게 하기 위해서는 무엇보다 시스템의 접근제어가 기본적인 요구조건이기 때문이다.

이를 위하여 기존의 대부분의 방식에서는 사용자가 기억하고 있는 지식을 확인하거나 소유한 물건을 확인함으로써 적법성을 인증하는 방법을 택하였다. 이를테면 패스워드를 입력하게 한다든지 열쇠나 토큰 그리고 카드 등을 통하여 인증하게 하는 방법이 그것이다. 그러나 이 방식은 인증이 간편하고 비용이 저렴한 장점을 지니는 반면 위조, 도난 등에 의한 불법적인 침입에 약하다는 위험이 따르며 하드웨어의 기술이 발달할 수록 그 위험도는 증가하고 있다. 또한 사용자의 소유물이 마모나 훼손, 분실에 의해 적법성을 잃을 경우에도 재발급을 위한 많은 번거로운 절차가 수반되어야 한다.

그런 의미에서 본 논문에서는 보다 안전도가 높을 뿐만 아니라 분실의 염려가 없는 개체의 특징을 통한 신분인증 방식에 대하여 고찰하고 그 장단점을 설명하며 인증 시스템의 설계시에 고려하여야 할 점들을 분석해 보고자 한다. 신분인증은 시스템의 접근을 적법한 사용자에게만 허용하는 적극적 의미에서의 인증과 원하는 사용자의 요청에 의하여 그 사용자의 정보만을 보호하기 위한 소극적 의미에서의 인증을 모두 포함한다. 아직까지 이런 방식의 현실화가 가시적으로 드러나 있지는 않으나 현대사회가 점점 정보화를 추구할 수록 그 효능이 중요한 가치를 띠게 될 것이며 그에 따른 제반기술의 발전은 필요에 의해 수반되는 것이므로 이런 인증방식을 비교 분석하는 것은 정보사회의 구현을 위해 중요한 의의를 지니는 것이라 하겠다.

2. 생체 특징에 근거한 신분인증

* 포항공과대학 전자전기공학과 부교수
** 포항공과대학 전자전기공학과 석사과정

2.1. 개 요

어떤 개체는 타 개체들과 자신을 구별할 수 있는, 자신에게 유일한 신체상의 특징을 가진다. 이를테면 사람의 얼굴이나 목소리가 그러하며 널리 알려진 지문도 이런 특징 중의 하나이다. 개체의 특징을 이용한 신분인증 시스템은 이런 각 개체가 가지는 여러가지 생체상의 특징들을 근거로 하여 자신의 신분을 자동적으로 인증받을 수 있게하는 시스템이다. 인증 시스템을 이용하는 모든 사용자는 먼저 사전등록을 통하여 자신의 특징에 대한 데이타를 인증 시스템에 제공해야 하고 이 때 시스템 관리자는 각 개체들의 생체 측정 데이타들을 모아 이를 각 사용자의 인증을 위한 생체 측정 자료(biometric templet)로 보관한다. 이 자료는 개체의 특징으로부터 다양한 요소들을 측정하되 이를 여러번 반복하여 평균한 값으로 전적으로 신뢰할 수 있어야 한다. 시스템에 접근하려는 사용자들의 신분인증은 인증받고자하는 사용자와 인증 시스템의 측정기계 사이에서 자동적으로 이루어진다. 먼저 각 사용자들은 자신의 이름을 키보드로 입력하거나 자신의 신원이 기록된 메모리 카드를 측정기에 제시하고 자신의 특징을 생체 측정하는 과정을 거치면 측정기는 측정 데이타와 미리 등록시에 보관되어 있던 인증자의 biometric templet와 비교하여 인증 여부를 판정하게 되는 것이다.

각 객체가 타 개체와 구별할 수 있는 특징은 무수히 많으며 실제적으로 인증 수단화되고 있는 대표적인 것으로는 손으로 쓰여진 서명(handwritten signature)이나 지문(fingerprint), 그리고 성문(voice print)등이 있고 이 외에도 두상 모양(head bump), 입술무늬(lip print), 발무늬(feet print), 손이나 손목의 정맥의 모양, 그리고 물리적인 자극에 의한 뼈의 반응 등도 개체에게 독특한 특징들이다. 그러나 이 특징들을 인증 수단으로 선택할 때에는 인증의 정확도의 문제 이외에도 측정방법의 문제가 중요하게 고려되어야 한다. 예를 들어 입술무늬를 측정하기 위해서는 측정기와 입술접촉이 필요한데 이는 사용자들에게 거부감을 줄 우려가 크기 때문이다. 그러므로 보다 효과적인 인증을 위하여 측정대상화 할 수 있는 특징들은 다음과 같은 조건을 갖추어야 한다.

1. 한 개체의 특징을 다른 개체들의 특징으로 부터 쉽게 구별해 낼 수 있게 하여야 한다(large interperson variation). 이를 위해 각 개체들의 특징 중에서 통계적으로 타 개체와 차이가 뚜렷한 요소들을 다양하게 선택하여 측정자료화 하여야 한다.
2. 임의의 개체에 대하여 반복하여 측정하여도 데이타의 변화가 작은 특징을 측정대상으로 선택하여야 한다(small intraperson variation). 인증자의 신체의 상태나 감정의 변화에 따라 오차가 심한 특징은 피하여야 한다.
3. 생체 측정에 거부감이 생기지 않아야 한다. 인증 시스템은 무엇보다 사용자 중심의 설계를 하여야 하며 위험하거나 혐오스러운 측정 방법은 배제되어야 하고 인증을 위한 사용자의 노력을 최소화할 수 있어야 한다.
4. 물리적 혹은 화학적인 자극에 의한 생체 측정을 피하고 되도록 전자 시스템을 통하여 개체의 특징을 측정하여야 한다.

또한 불법적인 침입자가 인증에 실패했을 경우에 감수해야 하는 위험도를 높이는 방법 역시 중요하게 고려해야 할 사항이다. 이를 위해 인증을 무한히 되풀이할 수 없게 하여야 할 뿐 아니라 되풀이 되는 인증 실패의 경우 경보장치를 가동시켜 불법침입의 여부를 확인할 수 있게 하여야 한다.

2.2. 인증 오류

개체의 특징을 통한 신분인증 방식은 개체의 특징들이 소유물이나 기억하고 있는 비밀정보들처럼 분실 혹은 도난 당하거나 망각될 염려가 없고 지속적이며 또 인증의 오류를 범할 확률도 이들보다 상대적으로 낮다는 장점을 가진다. 그러나 일단 등록시의 개체의 생체 측정 자료를 가지고 현재 개체의 인증여부를 비교 판단하는 만큼 다음과 같은 두 가지 종류의 오류를 범할 가능성이 항상 존재한다.

Type I 오류 : 인증 시스템이 마땅히 인증해 주어야 할 개체를 인식하지 못하는 오류(false reject)

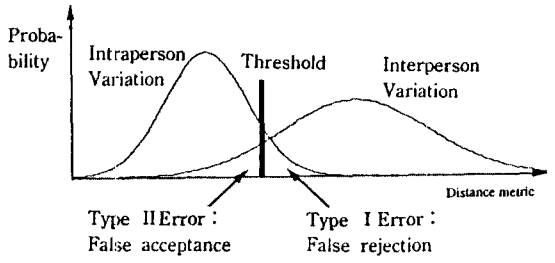


그림 1. 개체의 특징에 의한 신분인증의 오류율

Type II 오류 : 인증 시스템이 받아들이지 말아야 할 개체를 다른 개체로 잘못 인식하여 받아들이는 오류(false acceptance)

개체의 특징도 변화의 가능성을 항상 배제할 수 없을 뿐만 아니라 측정 당시의 상태에 따른 오차도 있을 수 있다. 앞 절에서 제시했던 small intraperson variation의 조건이 충족되지 않을 경우 Type 1 오류가 유발되며 large interperson variation이 만족되지 않을 경우에는 Type II 오류가 발생하게 된다. 이 두 가지 오류의 가능성이 완전히 배제될 수는 없으며 또한 그림 1에서 보듯이 두 오류율 사이에는 한가지 오류율을 감소시키기 위해서 다른 한 가지 오류율의 증가를 감수해야 하는 상호 보정(trade-off) 문제가 있다. 그러므로 응용되는 시스템에 따라서 위의 두 가지 오류 가능성들 사이에서 최적의 오차 허용도를 갖도록 시스템 설계가 이루어져야 한다.

2.3. 오류율과 오차 허용도

인증 시스템이 인증 수단으로 선택한 생체 특징은 그림 1에서 보듯이 개체간 편차의 확률분포와 개체 특징의 시간적 편차의 확률분포로 그 특성을 나타낼 수 있다. 앞절에서 제시한 두 가지 형태의 오류의 가능성은 피할 수 없을 뿐더러 서로간에 trade-off가 존재하므로 인증 시스템에서는 두 가지 오류에 대하여 적절한 오류율을 정하여 시스템의 신뢰도를 나타내게 할 수 있다.

등록할 때에 개체의 생체 특징 자료로서 시스템에 제공되었던 인증 자료들의 평균을 m, 표준편차를 σ라고 한다면 인증시에 측정되는 데이타 x에 대하여 오차허용도 t는 다음과 같은 조건을 가진다.

$$|x - m| / \sigma < t$$

즉 인증시에 측정되는 데이타들의 측정오차를 표준편차로 정규화하고 오차 허용도와 비교하여 인증 여부를 판단하다. 이 때 오차 허용도 t는 각 오류율의 합이 최소가 되는 점에서 선정하는 것이 일반적으로 바람직하다. 그러나 인증 시스템의 응용에 따라 두 가지 형태의 오류율 중에서 특히 어느 한쪽 오류형태에 보다 엄밀한 인증을 요구할 수 있기 때문에 두 가지 오류율에 각각 비중치를 두어 응용 시스템의 측면에서 최소의 오류율을 제공하는 측정 대상들을 선정한다. 그림 1에서는 false rejection error, 즉 적법한 개체를 불법하다고 잘못 인증하는 Type II 의 오류에 대하여 Type I 의 오류보다 더 오류율을 낮출 수 있도록 오차 허용도 t를 정한 예이다.

적법한 사용자를 불법하다고 판정하는 Type I 오류율을 줄이기 위하여 인증자에게 다수의 인증방식을 제시하고 인증자가 그 중에서 하나만 통과하여도 적법성을 인증하도록 하는 방법이 많은 인증 시스템에서 쓰이고 있다. 또한 측정 대상인 개체의 특징에 따라 어떤 사용자에게는 가변적인 요소가 있을 수 있으며 이런 경우 사칭의 위험이 크다. 이를테면 노인들의 수서명은 신체조건에 따라 상당히 가변적이다. 따라서 이는 사용자에게 미리 경고됨은 물론 다른 인증방식이 제시되어야 한다.

2.4. 생체 측정 방식의 선택

◆오류율

오류율은 인증 시스템의 신뢰도를 결정하는 중요한 요소이다. 우선 되도록 개체의 다양한 특징들을 모두 선택하고 많은 개체의 측정을 통하여 그림 1과 같은 확률 분포를 구한다. 생체 측정 방식은 각 특징들의 오류율이 최소가 되는 방식을 선택하되 두 가지 형태의 오류 중에서 한 가지 오류율이 주어진다면 다른 한 가지의 오류율을 최소화하는 방식을 선택한다.

◆생체 측정 방법

신분인증을 위한 생체측정은 측정기계와 대상인 개체 사이에서 이루어지기 때문에 측정방법이 사용자에게 혐오감이나 신체상의 위험을 주어서는 안되며 또한 측정을 위해 사용자에게 요구하는 노력과 이에 소요되는 시간이 지나쳐서는 안된다.

◆등록작업 및 인증시간

초기에 신분인증 시스템을 구성하기 위하여 적법한 사용자들로부터 정확한 생체 측정 자료를 얻어야 하는데 이를 위해 과도한 시간과 비용, 노력을 사용자에게 요구하여서는 곤란하다. 생체 측정 결과를 분석하고 인증여부를 판정하기까지의 시간과 비용에 있어서도 생체 측정의 판별은 정확해야 하지만 처리속도 역시 신속한 것이 바람직하다. 이 문제 역시 두 가지 상반되는 요구조건을 고려하여 시스템의 신뢰도를 정하게 하는 요소이다.

2.5. 생체 측정의 종류

생체 측정은 다른 개체와 구별할 수 있는 다양한 개체의 특징 중에서 어떤 부분을 인증 수단으로 응용하느냐에 따라 여러가지로 나눌 수 있다. 현재까지 대표적으로 생체 측정대상이 되고 있는 개체의 특징들과 측정방법들을 차례로 설명하면 다음과 같다.

(1) 지문(fingerprint)

지문의 형태는 일생동안 변하지 않는다고 알려져 있으며 잉크를 통하여 미세한 자국까지도 쉽게 남길 수 있고 또 판별하기가 용이한 장점이 있으므로 오래전부터 사용되어 온 인증 수단의 하나이다. 인증 시스템에서 사용하는 측정방법으로는 잉크로 지문을 찍어 자국을 남기는 방법 보다 빛을 쏘아 그 반사광을

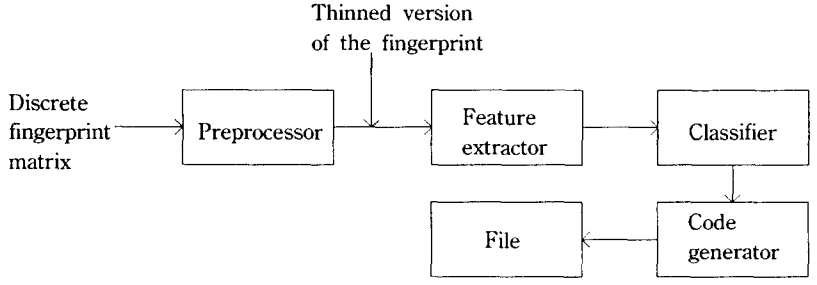


그림 2. 지문 화상처리를 위한 Block diagram

받아서 지문에서의 선들의 위치를 찾는 방법을 주로 사용한다. 그림 2는 지문을 디지탈 화상으로 처리하고 저장하는 과정을 간단히 나타낸 것이다[1].

preprocessor는 주로 화상 잡음을 제거하는 역할을 한다. 지문의 겹쳐진 부분에 의해 생기는 불규칙성이나 골(ridge)의 두께의 가변성 등에서 화상 잡음을 초래하게 되며 이를 부드럽게 이어주고(smoothing) 골의 두께를 얇게 하는(thinning) 역할을 한다. 그런 다음 feature extractor에서는 지문의 주요한 특성들을 추출한다. 주로 지문에서의 선들의 끝점, 갈라지는 점, 동그랗게 말린 점 등의 상대적인 위치와 방향이 지문을 특징짓는 주요한 기준이 된다. 하나의 지문에서 약 50개 내지 200개 정도의 특징들을 잡을 수 있으며 그 중에서 20여가지 정도의 특징으로서 개체의 인증여부를 판정할 수 있다. classifier에서는 지문의 각 부위를 기본적으로 whorl, loop, arch등의 형태로 분류하는 역할을 한다. 등록시에는 이런 방식으로 추출된 지문의 특성이 생체자료로 저장되며 인증을 위한 측정시에는 보관된 자료와 측정된 생체 데이타가 비교되어 인증 여부를 판정하게 되는 것이다.

같은 지문을 가진 사람은 거의 없다고 알려져 있으므로 오류율은 작으나 측정기의 가격이 비교적 높은 편이다. 또한 측정 방법이 위험하지는 않으나 사용자로 하여금 거부감을 줄 우려가 있다[2].

(2) 수서명(handwritten signature)

오래전부터 신분인증을 위한 수단으로서 사용되고 있는 개체의 특징의 하나이다. 흔히 필기된 서명을 감식하여 인증여부를 판단하는 방법이 많이 쓰이나 이와 더불어 서명할 당시의 동작 역시 사용자에 대한 중요한 자료가 된다. 이를 위하여 흔히 쓰이는 필기되는 서명수단과는 달리 특수한 바닥에 특수 펜으로 수서명하게 할 필요가 있다. 이 방식은 서명 자체의 길이나 곡선도 등의 서명의 특징과 서명할 때의 손의 움직임의 특징을 이용하기 때문에 눈으로 판별하는 필기된 수서명보다 훨씬 정확하다[3].

서명을 모방하는 방법은 세 가지 정도로 분류할 수 있는데 freehand forgery, simulated forgery, traced forgery가 그것이다[4]. freehand forgery는 서명자의 서명동작에 대한 지식이 없이 이미 필기된 서명을 보고 모방하는 경우이며 이에 대한 검사는 주로 전체 서명의 가로와 세로의 비, 정사각 등이나 특이한 문자에 대한 비교를 통하여 이루어진다[5]. 그러나 simulated forgery, traced forgery와 같이 모방자가 서명자의 서명 동작에 대한 지식이 있을 경우에는 위와 같은 검사방법으로 진위를 판단하기 어려우며 이에 대해서는 서명 동작을 통한 검사가 이루어져야 한다. 서명할 때의 펜의 속도, 손이 누르는 압력, 리듬, 서명시간, 그리고 손이 바닥에 접촉하는 점의 좌표 등이 주요한 측정 대상이며 사용자가 등록할 때에 이에 대한 반복된 측정을 통하여 통계적인 생체 자료를 만든다. 실제로 이러한 방식을 이용하여 미국의 NPL(National Physical Laboratory)에서 VERISIGN이라는 수서명 인증시스템을 개발한 바 있는데 여기에서는 약 10가지 서명상의 특징을 측정대상으로 이용하고 CHIT라는 특수 패드를 측정수단으로 사용한다. 이 패드는 분리된 이중막 구조를 가지고 있으며 사용자가 수서명을 할 때 두 막이 접촉하는 좌표를 초당 50회 측정하여 저장한다. 또한 Autosig Systems, Inc에서도 Sign/On이라는 인증 시스템을 개발한 바 있다.

서명자의 정확한 인증을 위해서는 등록시에 사용자의 필기된 서명에 대한 많은 샘플을 모아서 특징들을 추출해야 하며 서명자의 서명동작에 따른 특징 역시 통계적인 방법을 통하여 가장 편차가 작은 부분들을 선별하여야 한다. 또한 서명자의 서명습관도 시간에 따라 서서히 변하므로 인증 시스템 역시 이에 적응하여 인증할 때마다 측정되는 데이타를 그 사용자의 새로운 생체자료로 활용할 수 있도록 설계되어야 한다.

(3) 망막의 무늬(retinal pattern)

눈의 망막에 있는 실핏줄의 형태가 각 사람마다 독특하다. 미국의 Eyedentify Inc.(Portland, Oregon)에서는 망막 실핏줄의 다양성은 지문을 능가하며 전 세계에 단 한명도 같은 망막 실핏줄 무늬를 갖고 있지 않다고 주장한다. 또한 약 200만명의 등록된 사용자들의 측정실험에서 Type I 이나 Type II 오류율이 거의 0에 가까왔으며 측정에 소요된 시간도 몇 초에 불과했다고 실험결과를 보고한 바 있다[6].

측정할 때는 아주 약한 레이저 빛을 망막에 쏘아 동공을 중심으로 정해진 범위의 영역에 있는 실핏줄의 무늬를 관찰하고 주로 실핏줄의 갈라진 곳, 끊어진 곳 등의 상대적 위치를 등록되어 있는 자료와 비교하여 인증자의 진위를 판정하는 근거로 삼는다. 그러나 측정 방법이 위험하지는 않지만 사용자로 하여금 거부감을 줄 우려가 있으며 맹인의 경우에는 이 방법이 적절하지 못하다.

(4) 성문(voice print)

음성 인식은 다양한 분야에서 응용되고 있으며 그 기술 수준도 높은 편이다. 그러나 성문을 통한 인증 시스템은 음성을 문자로 인식할 수 있어야 할 뿐만 아니라 각 사용자의 생체 자료와 비교하여 동일성 여부를 판별할 수 있어야 한다. 이를 위해서는 우선 등록시에 사용자의 정확한 성문 자료를 만들기 위한 여러가지 조건이 필요하다. 측정공간은 각종 왜곡(distortion)과 잡음의 요소가 배제되어야 하고 잔향(reverberation)이 거의 없는 특수한 장소를 선택한다. 그리고 측정할 어휘로 사용자의 성문 특징을 가장 잘 드러낼 수 있는 몇개의 단어로 된 구절을 선택하여야 하며 사용자의 이름은 적당하지 않을 경우가 많다. 측정 단어들을 여러번 반복하여 입력하게 한 후 입력된 음성으로부터 여러 주파수 성분의

시간적인 변화 특성들을 찾는다. 그런 다음 여러 음성입력들로부터 모은 특성들을 통계처리하여 생체 측정 자료로 만든다[7]. 음성신호의 길이가 길어질수록 오류율은 확률적으로 줄어드나 그만큼 등록할 때에 성문 특성 검출에 소요되는 시간이 늘어날 뿐 아니라 인증을 위해 필요한 시간 역시 증가하는 trade-off가 있으므로 인증 시스템의 안전성과 신뢰도를 고려하여 결정해야 한다.

성문을 통한 인증 시스템은 등록과 측정 과정에서 시간이 많이 소요된다는 점과 인증자의 신체 상태에 따라 성문의 특성에 편차가 많으므로 오류가 발생할 우려가 크다는 약점이 있다. 그러나 만약 측정되는 음성이 그 개체만이 아는 비밀어이고 노출될 가능성이 없는 공간에서 측정이 이루어진다면 개체의 특징을 확인함과 동시에 비밀어를 알고 있는지의 여부를 확인함으로써 인증의 정확도를 높일 수 있다.

(5) 타자 리듬(typing rhythm, key-stroke dynamics)

많은 인증 시스템에서 사용자의 신분인증을 위해 사용자가 비밀정보를 알고 있는가를 확인하는 방법을 사용한다. 이는 대부분 키보드를 통하여 패스워드의 입력을 요구하는데 이 때 사용자가 키보드를 두드리는 리듬을 인증을 위한 수단의 하나로 이용할 수 있다. key pad나 자판에 숫자나 단어 등을 입력할 때 누르고 있는 시간이나 누르는 압력, 그리고 누르는 순간 사이의 간격 등은 사용자 마다 다르다. 그러므로 이 리듬을 찾아내어 생체 자료로 활용하는 것이다. 이는 사용자의 생체 상태에 따라 측정값에 변화가 많으므로 오류율은 상대적으로 높은 편이다. 그러나 측정을 위하여 어차피 PIN(personal identification number)이나 패스워드 등을 입력하므로 따로 특별한 기계의 도움없이 타자 리듬을 찾아낼 수 있는 작은 기판 하나를 늘 사용하는 컴퓨터에 끼워 넣기만 하면 인증 시스템으로 충분할 뿐만 아니라 신분인증을 위해 그 개체만이 알고 있는 지식측정과 더불어 개체의 행위적 특징의 측정이라는 인증요소를 쉽게 포함시킬 수 있으므로 응용 가능성이 높다[8].

(6) 얼굴 형태(profile)

사진 혹은 비디오 카메라로 잡은 영상으로부터 얼굴의 특징들을 찾는다. 눈, 코, 귀, 입의 크기, 이들간의 거리 등에서 약 100여개의 특징을 잡을 수 있다. 그러나 영상으로 잡힌 얼굴의 각도가 항상 일정하지 않기 때문에 오류율이 높은 편이다[9].

(7) 손모양(hand geometry)

유리판 위에 손을 정해진 위치에 올려 놓으면 손모양을 측정하는 기구는 빛을 쏘아 그 반사광을 받아서 손가락 마디들과 손바닥의 길이, 굵기, 굴곡 등으로부터 특징을 찾는다. 단 올바른 측정을 위하여 손바닥 모양의 틀 위에 손바닥을 두게 한다. 비교적 가격도 싸고 오류율도 높지 않으나 측정기구가 상당히 큰 편이다.

2.6. 안전성 분석

생체 측정은 크게 신체적 특성 측정과 행위적 특성 측정으로 구분할 수 있다. 지문, 망막의 무늬, 손모양, 얼굴 모양 등이 전자에 해당하고 수서명, 타자 리듬, 성문 등이 후자에 해당한다. 초기에 등록작업을 할 때 일반적으로 신체적 특징을 이용하는 것에 비하여 행위적 특징을 이용하여 신분인증을 하는 경우가 더 오랜 시간이 소요된다. 또한 행위적 특징들은 신체적 특징들에 비해 개체 사이에 차이가 크며(large intraperson variation) 개체의 생체 상태에 따라 측정 데이타의 변화가 생길 수 있으므로 오류율도 높은 편이다. 그러나 앞에서 설명한 바와 같이 행위적 특징을 이용하는 신분인증 방법은 지식을 확인하는 방법과 자연적으로 겸하여 사용할 수 있다는 장점이 있으므로 이를 적절히 결합하면 오류율을 낮출 수 있다.

한편 어떤 개체의 신체적인 특징들도 시간이 흘러감에 따라 서서히 변해간다. 따라서 개체의 자연적인 변화에 따른 생체 측정 자료의 수정이 자동적으로 이루어질 수 있도록 하여야 한다. 이를 위해 개체가 시스템에 접근하려고 할 때마다 측정되는 적법한 데이타를 개인 생체 자료와 통합하여 개체의 신체상의 변화에 자동적인 적응이 가능하도록 하여야 한다. 물론 급격한 신체적 변화에 대해서는 재등록

을 통한 새로운 생체 측정 자료를 마련하여야 할 것이다.

3. 결 론

정보화되어 가는 현대 사회에서 신분인증이나 개인 식별의 문제는 정보 보호에 있어서 가장 기본적인 관건이 되는 문제이다. 현재 상용되고 있는 개인의 소유물에 의한 신분인증이나 기억하고 있는 지식에 의한 신분인증은 불법적인 조작이나 위조라는 부분에 취약한 약점이 있어 신분인증 방식으로서는 한계가 있다. 개체의 생체 특징에 근거한 신분인증 방식은 불법적인 위조나 가장(forgery)의 가능성을 거의 없앨 수 있어 정보의 보호라는 차원에서 중요한 의의를 가진다고 하겠다. 그러나 신분인증 시스템의 선택을 위해서는 무엇보다 안전성이 가장 중요한 요소이지만 이밖에도 경제적인 문제나 처리 속도, 측정 방법의 편의성 등의 문제가 같이 고려되어야 한다. 인증 시스템이 어떠한 분야에 응용되느냐에 따라 각 요소들에 대한 비중치가 달라져야 하기 때문이다. 또한 개체의 특징에 의한 신분인증 방식이 인증 오류를 범할 확률을 크게 낮추었다고 하지만 더욱 중요한 것은 그 운용의 문제로서 등록시에 신뢰할 수 있는 생체 측정 자료를 수집해야 하는 것은 물론 그 관리에도 허점이 노출되면 안된다. 또한 어떤 보안시스템에도 불법 침입의 여지가 존재하기 마련이므로 안전도가 높은 하나의 방식에 전체 시스템의 안전을 맡기기 보다는 여러 종류의 신분인증 방식들을 혼합하여 운용함으로써 각 방식들의 약점을 상호보완해 주도록 시스템을 구성하는 것이 바람직하다. 현대 사회가 정보화를 추구할수록 사용자의 신분인증 문제는 정보보호의 중요한 관건이 되고 있으며 이에 따라 인증의 오류가 거의 없는 개체의 특징에 의한 신분인증 방식에 대한 연구는 앞으로도 계속 진행되어야 할 것이다.

참 고 문 헌

1. K.Rao, "On fingerprint pattern recognition", *Pattern Recognition*, 10/1, 1978.

2. K.Rao and K. Balck, "Type classification of fingerprints : a syntactic approach", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, PAMI-2,3, May, 1980, pp.223-231.

3. C.N. Liu, N.M. Herbst and N.J. Anthony, "Automatic signature verification : system description and field test results", *IEEE Trans. on systems, Man, and Cybernetics*, SMC-9, No.1, Jan. 1979. pp.35-38.

4. R.N. Nagel, "Computer screening of handwritten signature : A proposal", *Comput. Sci. Center, Univ. of Maryland, College Park, Tech. Rep.* 220, Jan. 1973.

5. R.N. Nagel and A. Rosenfeld, "Computer detection of freehand forgeries", *IEEE Trans. on Computer*, C-26, No.9, Sep. 1977, pp.895-905.

6. D.W. Davies and W.L. Price, "Security for computer networks(2nd ed)", John Wiley & Sons, 1989.

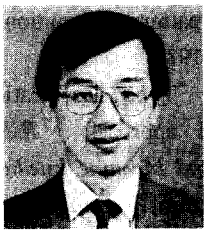
7. R.L. Kashyap, "Speaker recognition from an unknown utterance and speaker-speech interaction", *IEEE Trans. on Acoustics, Speech and Signal Processing*, ASSP-24, 6, Dec. 1976, pp. 481-488.

8. R. Joyce and G. Gupta, "Identity Authentication based on keystroke latencies", *Comm. of the ACM*, V.33, Feb. 1990. pp.168-176.

9. L.D. Harmon, L.D. Khan, M.K. Rasch and P.F.Ramig, "Machine identification of human faces", *Pattern Recognition*, 13/2, 1981.

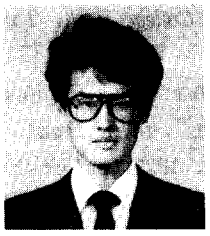
10. National Bureau of Standards, "Guidelines on evaluation of techniques for automated personal identification", *Federal Information Processing Standards Publication*, 48, 1977.

□ 著者紹介



李 弼 中(정회원)

1951년 12월생
1974년 2월 서울대학교 전자공학과 학사
1977년 2월 서울대학교 전자공학과 석사
1982년 6월 U.C.L.A. System Science, Engineer
1985년 6월 U.C.L.A. Electrical Engineering, Ph.D.
1980년 6월~1985년 8월 : Jet Propulsion Laboratory, Senior Engineer
1985년 8월~1990년 2월 : Bell Communications Research. M.T.S
1990년 2월~현재 : 포항공과대학 전자전기공학과, 부교수.



趙 柱 衍(학생회원)

1968년 11월생
1991년 2월 서울대학교 제어계측공학과 학사
1991년 3월~현재 : 포항공과대학 전자전기공학과 석사과정