지문 생체알고리즘을 통한 개인 인증 연구

Thank with CA mothed of biologic algorithm

정 지문, 신 정길, 장 동 진*, 최 성

Ji-Moon Jung, Jung-Gil, Jang-Dong Jin, Sung Choi

남서울 대학교 컴퓨터학과

Department of Computer Science Southern Seoul University

개 요

오늘날 많은 국가들이 전자상거래 부문을 세계 여러 국가들 보다 빨리 선점하기 위해서 많이 노력하고 있다. 그리고 전자상거래가 활성화된 국가에서는 앞선 기술로서 가상공간에서의 자국의 위치를 높이고 있다. 우리 나라도 전자상거래가 활성화되는 과정에 있다. 그러나 가상공간 즉, 인터넷에서 해결되지 못한 문제들이 많이 있다. 그 중에서도 세계 여러 나라들도 해결하지 못한 문제 바로 보안에 관한 문제이다. 인터넷에서의 보안문제는 여러 가지 문제들이 있다. 그러나 본 논문에서는 개인 인증에 관하여 중점적으로 다루려 한다. 개인 인증 방법에는 PKI 개념에서 RSA 암호알고리즘과, 전자서명 등이 있다. 그리고 공인 인증기관에서 개인에 대한 인증을 해 주는 경우가 있다. 현재 이러한 인증방법에 대해서 알아보고, 문제점과 함께 해결방안으로 생체알고리즘을 통한 인증 방법, 특히 지문에 대해서 개인 인증 방법을 다루려 한다 특히 지문을 통한 생체알고리즘은 패턴 인식방향 보다 이미지에 대한 직접적인 의미 부여를 통해서 전송속도와 전송량을 줄이려고 노력했다. 이런 방식으로 얻어낸 이미지를 전자주민 카드 지문 시스템과 상호 호환이 될 수 있도록 연구하였다.

I. 서론

국내외로 전자상거래에 대한 사회적 국가적 인식이 커지고 관심도 높아지게 되었다. 이런 전자상거래 시장의 양적 팽창은 괄목한 수준까지 오게 되었다. 그러나 전자상거래에서 아직 취약한 부분이 많이 존재 하고 있다. 그런 부분들 가운데 개인 인증에 대한 문제에 대해서 본 논문에서 다루려고 한다.

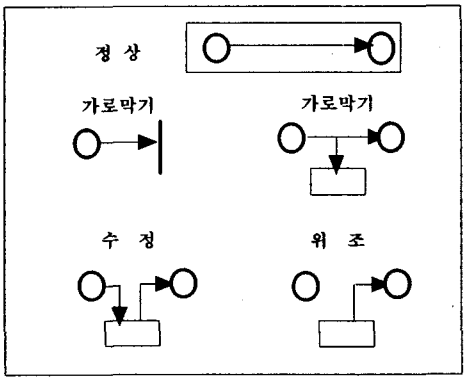
현재 많은 사용자들이 개인 자료 누출에 대한 꺼려로 전자상거래의 활성화를 이끌지 못하는 경우가 많다. 그리고 판매자 입장에서도 고객의 정보의 사실여부를 판다하기 어려울 것이다. 그래서 현재 사용되고 있는 인증 방법에 대해서 알아보고 그에 해당하는 문제점을 생각해 보고 문제점을 해결 할 수 있는 생체 알고리즘을 통해 문제점들을 해결 하고자 한다. 그러나 본 논문에서는 직접적인 Programming을 통한 구현을 미처 하지 못한 문제점을 가지고 있다. 그래서 이런 알고리즘을 연구하였다.

II. 본론

1. 인터넷상에서 보안피해

인터넷은 개방된 시스템으로써 전세계에 펼쳐 있는 거대한 네트워크이자 소비자에게는 새로운 소비패턴을 판매자에게는 수많은 새로운 고객들이 발생하는 경제적 효과를 가져오게 했다. 그런 긍정적인 부분이외에 부정

적인 측면으로 해커들에 의한 개인 자료누출 또는 자료변조, 사칭, 자료차단 등의 여러 문제들을 갖고 있다. 그래서 개인과 단체, 기업들의 피해가 속출하고 있다. 그림 [1-1]에서는 인터넷 상에서 발생할 수 있는 보안위협에 대해 도식화 하였다. 정상적인 흐름에 비해 보안상 위협을 받을 때에는 자료의 흐름이 변조되는 것을 알 수 있다.



< 그림 1-1 보안 위협 유형 >

2. 인증

2.1 인증의 정의

인증(Certification) 정보나 통신시스템에서 사용자, 주변장치, 혹은 다른 실체의 주장된 신원의 정당성을 확립하는 기능으로 정의 할 수 있다. 이러한 인증은 다음과 같이 수행할 수 있다.

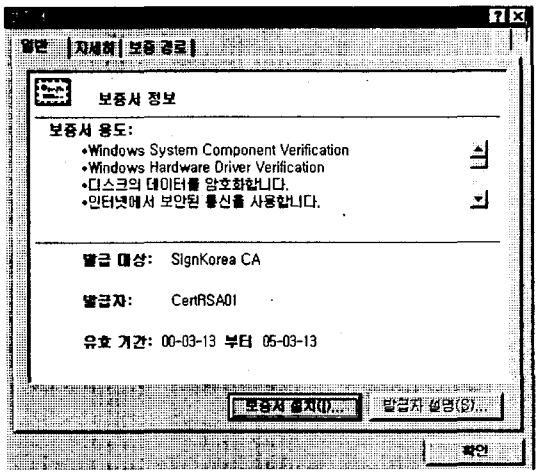
- 문제의 사용자가 이전에 등록된 사람임을 확인하는 행위. 이것은 사용자의 서명이나 사용자의 지문, 망막형태 등을 포함하는 다양한 생체적 방법을 사용하여 수행된다.
- 어떤 사실이나 문장이 사실이라는 보장
- 어떤 거론된 사실의 진실성을 증명하는 문서
- 어떤 것이나 어떤 사람의 신뢰성을 검증
- 통신상에서 비 대면 원칙에 따라 개개인 인증에 따른 신뢰성을 검증

2.2 현재 사용되고 있는 인증방법

ID, Pass Word 방법과 인증기관에서 발행한 인증서(Certificate)를 통해 개인의 인증을 하고 있다.

2.3 인증서

인증서(Certificate)는 SET 기반의 전자상거래에서는 자신의 신원을 알리는 신분증과 같은 것이다. SET 기반의 전자상거래에 참여하는 모든 주체들 즉, 구매자(Cardholder), 상점 (Merchant), 지불게이트웨이(Payment Gateway)는 각각 자신의 인증서를 가지고 전자상거래에 참여함으로써 자신의 신원이 믿을 만하다는 것을 거래 상대방에게 알리게 된다. [그림 2-1] 인증서는 한국 증권전산에서 발행한 인증서이다. 개인에 대한 인증서를 인증기관에 등록함으로써 인증을 요구하는 곳에서 개인의 인증서를 발행한 기관에서 보여줌으로써 개인 인증단계를 받게 된다.



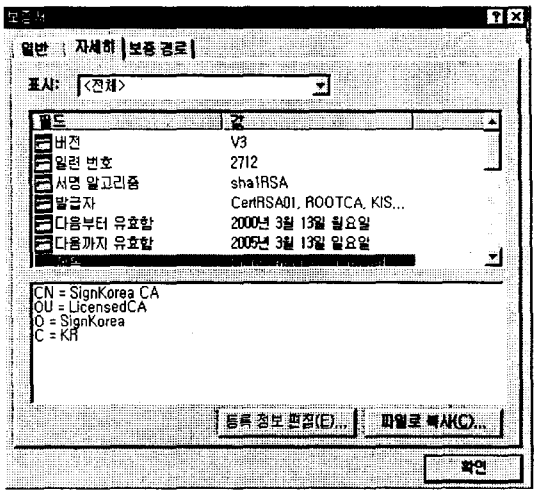
< 그림 2-1 사용중인 인증서 >

2.3.1 인증서는 기본적인 내용

- 인증서 소유자의 신원정보
- 인증서의 일련번호
- 인증서의 만기일자
- 인증서 소유자의 공개키
- 인증서가 적절한 기관에 의해 발급되었음을 증명하는 인증기관 신원정보와 전자서명

결국 인증서는 정부가 발행하는 운전면허증 또는 은행계좌에 연결되는 카드와 같은 기능을 한다. 인증서는 실제생활에서의 신분증 내지는 신용카드와 동일한 기능을 하지만 물리적인 실체를 가진 것이 아니며 구매자(Cardholder)의 경우에는 구매자가 사용하게

될 소프트웨어인 전자지갑(Wallet)에 설치되어지기 때문에 실제로 볼 수 있는 것은 아니다.



< 그림 2-2 인증서 내용 >

2.3.2 인증서(Certificate)의 역할

① 전자상거래 모든 참여자들의 신원을 확인하는 수단이 된다

② 전자상거래 참여자들은 서로 얼굴을 보지 못하는 상태이므로 그들의 신원을 공식적으로 확인해줄 공신력있는 기관으로부터 발급된 신원 증명이 필요한데 인증서가 그러한 역할을 하게 한다.

③암호화 과정에 필요한 공개키를 전달하는 역할을 한다

④ 타인으로부터 보호받아야 하는 거래정보의 안전을 위하여 SET 기반의 전자상거래에서는 암호화 기법을 사용하게 되는데 이 암호화과정에서 사용되어지는 비밀키/공개키의 쌍(pair)중에서 공개키를 포함하고 있어서 그러한 공개키를 전달하는 역할을 한다.

2.3.3 인증기관(Certificate Authority)의 역할

① 인증기관은 SET 기반의 전자상거래에 참여하는 구매자/상점/지불게이트웨이의 신원을 서로에게 보장하는 역할을 하는 인증서를 발급한다.

② 자신이 발급한 인증서에 대해 인증기관은 인증서의 만료 또는 실효와 같은 경우가 있을 때 그러한 사실을 알리는 역할을 한다.

③ 인증기관은 신원정보에 대한 책임을 지므로 인증서 요청자의 신원정보를 확인할 수 있는 금융기관이나 금융기관의 의뢰를 받은 제3의 기관에 의해 운영되어 진다.

④ SET 기반의 전자상거래에서는 인증기관도 계층적인 구조를 가지고 있어서 가장 상위의 인증기관이 자신의 하위에 있는 인증기관을 승인하여 인증기관의 역할을 하도록 한다.

⑤ 구매자/상점/지불게이트웨이는 각각 자신의 정보를 가지고 있는 인증기관으로부터 인증서를 발급받게 된다.

2.3.4 인증처리 방법

SET을 통한 개인 인증의 방법에서는 다음과 같은 질의를 통해서 개인의 인증서를 확인하게 된다.

- 사용자는 발행처에서 발행한 하나뿐인 카드인가?
- 이 카드는 인증받은 상점에서 사용중 인가?
- 이 상점은 발행자와 취급자 모두에게 등록 되었는가?
- 취급 은행으로 전송가능 한가?

2.4 문제점

개인의 ID와 Pass Word 도난 했거나, 인증서도 개인이 발급받은 인증서를 도난했거나, 타인이 몰래 사용해 개인 사칭할 경우 손 쓸 방법이 없으며 어떠한 해결 방법이 없다. 이러한 문제점을 해결하기 위해서 생체 알고리즘을 통해서 개인의 인증 여부를 판단하고자 한다.

3. 생체알고리즘을 통한 인증

3.1 생체알고리즘의 정의

인간의 신체적 또는 행동상의 특징을 이용하여 자동화된 방법으로 개인을 식별하는 것이다. 생체측정인식의 예로써 지문, 음성, 얼

굴, 망막, 홍채, 필체, 손금 등을 들 수 있다. 생체측정인식 기능은 "조회"와 "확인"의 2가지 모드로 나누어질 수 있다. "조회" 모드에서는 생체측정 시스템이 등록된 전체인구의 데이터베이스를 검색하여 동일한 사람을 찾아낸다. "확인" 모드에서는 생체측정 시스템이 사전에 등록된 데이터와 동일한 사람임을 증명해 준다.

사람의 신원을 증명하는데 사용되는 생체 측정학은 기존의 보안 시스템 보다 뛰어난 장점을 제공한다. 생체 측정학으로 사람이 본래 갖추고 있는 부분을 토대로 확인을 할 수 있습니다. 스마트 카드, 마그네틱 줄무늬 카드, 열쇠와 같은 물건은 분실 , 도난 , 복사의 위험이 있으며 패스워드는 잊어버리거나 공유되거나 우연히 제3자가 알게 될 수도 있습니다. 반면에 생체측정 기술은 안전성과 편리함 모두를 제공한다. 정보시대가 되면서 온라인 기술과 기타 공유 자원에 대한 의존도 증가에 따라 전자상거래를 완성시키는 방법이 빠르게 발전되어가고 있다. 시간이 흐를수록 일상적인 행위들이 점차 전자적으로 처리되고 있으며, 이러한 전자 상거래의 증가로 빠르고 정확한 사용자 신원조회와 확인 방법에 대한 요구는 날로 증가하고 있다. 생체측정 기술은 정확하면서도 빠르고 편리하게 신원을 증명해 줄 것이다.

3.2 인증

우리가 비즈니스나 개인 일로 사람들을 접촉할 때에, 일상적으로 서로를 소개하고 신뢰감을 쌓는 일을 우선적으로 수행한다. 마찬가지로 사이버 공간에서도 서로를 확인하는 과정이 요구된다. 그런데, 실질 공간에서는 실물 확인이 가능하지만, 물리적 접촉이 불가능한 사이버 공간에서는 신분을 확인하는 과정이 다소 복잡하다. 인증은 여러 기법으로 신분(Identity)을 입증하는 프로세스를 의미하며, 스푸핑 이나 위장 공격에 대해 대응할 수 있다.

인증은 그 대상에 따라 실체 (Entity) 인증과 근원지 (Data origin) 인증으로 분류된다. 전자는 시스템에 접근하는 주체가 다른 신분으로 위장된 것은 아닌지를 밝혀 내고, 후자는 문서를 받았을 때 이 문서를 보낸 근원지, 즉 송신자의 실체를 확인한다.

3.3 지문을 사용하는 이유

지문 생체알고리즘을 사용의 장점

- 사람마다 수십가지의 특징을 지녀 확연한 구분이 가능하다
- 손상되거나 닳아 없어질 염려가 없다.
- 판별기준 데이터의 양이 수십 byte로 저가 시스템의 구축이 쉽다.
- 다른 생체알고리즘에 비해 사용 편리하다.
- 다른 시스템에 비해 경제성이 높아 응용분야가 넓음
- 휴대용으로 이동시 장소에 관계없이 사용가능

< 표 3-1 각 생체알고리즘 분석 >

구 분	얼굴인식 시스템	홍채인식 시스템
생체인증 운용 방식	카메라를 통해 사용자의 얼굴 확인 후 등록된 사용자와 일치하는지를 비교하는 시스템	홍채의 특징을 추출하여 본인 여부를 판별하는 시스템
타인 수락율	0 %	0.3 - 0.7 %
본인 거부율	2.8 %	3 %

구 분	핸드스캐닝 시스템	지문인식 시스템
생체인증 운용 방식	손의 기하학적 구조의 특징을 추출하여 본인 여부를 판별하는 시스템	지문의 특징을 추출하여 본인 여부를 판별하는 시스템
타인 수락율	0.001 %	0 %
본인 거부율	0.1 % 미만	0.0001 %

3.4 알고리즘의 방법

3.4.1 지문데이터의 구성

국내의 경우 전자주민증 사업이 진행되면서

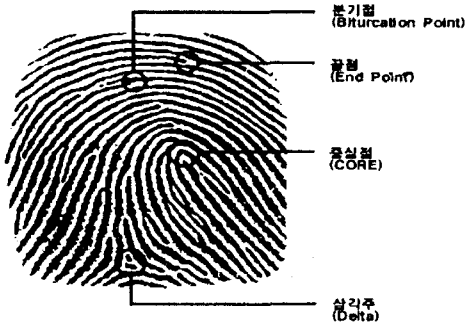
표준에 근접한 특징량 구성 방법이 정해진 바 있다. 이는 이미 대규모 데이터베이스를 구축할 경우를 위해 저장 공간의 효율을 높일 수 있도록 그 크기가 최소화된 상태이며, 이에 본 논문에서는 이와의 호환성만을 고려하여 특징량을 구성하고자 하였다 (전자주민증의 경우 스마트카드의 8K 바이트 저장 공간중에서 지문에 할당할 수 있는 공간이 불과 500바이트 정도이므로 효율적인 저장 방식은 매우 중요한 사항이다) 우선 저장될 개인별 지문 정보 크기는 500 바이트로 결정하였으며, 이들의 구조 및 내용은 다음 표 3-2와 같이 전자주민증의 경우와 유사하고, 다만 호환성을 잃지 않는 범위에서 일부 세부적인 항목의 용도만 변경하여 사용하게 된다. 그리고 이들 내용 중 손가락 번호의 경우, 각 손가락에 번호를 부여하여 구성한다.

< 표 3-2 전자주민증의 개인별 지문 정보 구조 >

항 목	내 용		옵셋	크기(바이트)
헤 더	손가락 번호		0	1
	중심점 좌표		1	4
	자료인식 번호		5	1
	특징점 개수		6	1
	여유 공간		7	1
	문 양 기준점	아래 중심점	8	2
		왼쪽 삼각주	10	2
		오른쪽 삼각주	12	2
	문양 기준점 부호		14	1
	분류 번호		15	1
	지문 양호 상태		16	1
여유공간	여유공간		17	43
특징점	지문 특징점 자료		60	440

3.4.2 지문의 구성요소

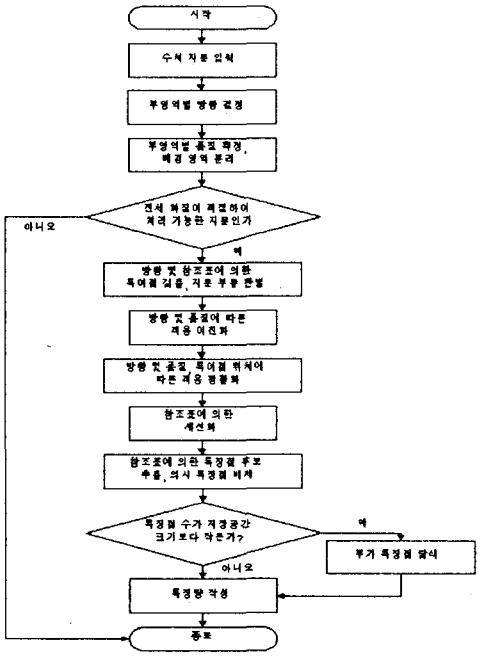
사람들의 지문은 다음과 같이 구성요소를 이루게 된다. 그리고 각각의 요소에 대한 패턴 인식을 검사하게 되고 그런 데이터를 중심으로 표 3-2 같이 구성하게 한다. 지문 구성요소는 그림 3-1과 같다.



< 그림 3-1 지문 구성요소 >

3.4.3 지문데이터 생성 알고리즘

지문은 특성상 수치 지문 획득시 발생한 기타 잡음이나 뒤틀림에 의한 왜곡, 상처에 의한 흉터 등을 제외하면 완만한 곡률 변화를 가지는 융선의 부드러운 흐름으로 볼 수 있다. 이러한 특성에 주목하고 이를 효과적으로 이용최소 크기의 융선들로 구성되어 있다고 하기 위해, 지문이 일정한 방향을 갖는 가정한 다음 이들의 방향을 구하여 특징 점 추출의 전체적인 특징량 추출 알고리즘은 그림과 같다.

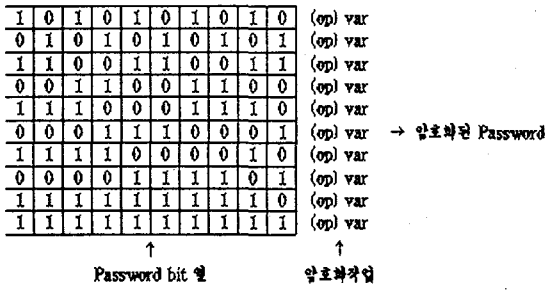


ⓐ 입력지문	ⓑ 패턴인식	ⓒ 결과지문

< 그림 3-2 지문데이터생성 알고리즘 >

< 그림 3-3 지문데이터 생성 과정 >

위의 알고리즘을 통해 입력 받은 지문은 다음과 같이 입력받아지게 된다. 그래서 ⓒ의 과정이 비로서 지문인식이 완료된 데이터의 모습을 하고 있다.ⓒ라는 이미지의 데이터는 그림 3-4와 같은 구조로 입력되어 통신상으로 전해지게 된다.



< 그림 3-4 지문데이터의 비트 데이터화 >

3.5 생체알고리즘의 문제점

아직 안정된 기술이 미개발 상태로 시스템 구축시 고비용 문제와 사용시의 심리적 거부감 존재하며, 각 기업에서 사용하는 기기간에 기술상의 차이로 인해서 오류 발생의 여지가 있다. 지문의 인식률이 미흡한 상황이다. 사용자나 기업주의 인증에 대한 인식부족으로 도입의 어려움, 그리고 지문 인식을 통한 새로운 시스템을 도입 해야하는 문제점을 갖고 있다.

III. 결론

현재 인터넷에서 발생하는 보안상의 문제는 개인 인증에 대한 문제점으로 귀속될 수 있다. 개인인증을 현재의 ID/Password 방식과 인증기관에서 발행하는 인증 방법은 어느 정도 개인인증에 대해 한계점에 왔다. 그래서 본 논문에서 알아 본 것과 같이 생체 알고리즘 특히 지문을 통한 개인 인증 방법은 지문의 인증방법에 대한 문제점을 해결 할 수 있다. 이런 방법으로 인증이 해결 된다면 인증뿐만 아니라 자동 지불수단 등으로 폭넓게 이용이 가능할 것이다.

그러나 이러한 지문 인식에 필요한 장비 도입이 되지 않았고, 기업들이 개인 인증에 대한 인식 변화와 사회의 인식 변화가 먼저 선행 되어야 할 문제이다.

IV. 참고자료

1. 전자상거래 보안 기술/ 이만영 외/ 생능 출판사/1999. 9. 10
2. 전자서명 및 인증제도/ 신일순 외 / 정보통신정책연구원 /1998. 12. 31
3. 21세기 전자상거래/ 김홍식 외 /경문사 /2000. 4. 5
4. 인터넷활용과 전자상거래/ 남태희 외 /글로벌 출판사 / 2000. 2. 29
5. 전자상거래와디지털경제/ 김상욱 외/홍릉과학출판사/ 2000. 2. 17
6. 전자상거래/ 김철환 외 /문원 출판사 /1999. 6. 5
7. 전자상거래 혁명/ 최인영 / 동일출판사 /1998. 8. 5
8. 인터넷과 전자상거래/ 고영국 /글로벌 출판사 /1998. 8. 25
9. 전자상거래 시스템운영 및 관리/전영일 /삼선 출판사 /2000. 4. 25
10. 칼스와 전자상거래/ 이남용 / 법영사 /1999. 6. 1
11. 전자상거래 정보보안/ 조찬식 /대한상공회의소 /1999. 12. 11
12. 신일순, "전자서명 및 인증제도의 필요성과 국내외 동향," 정보통신정책연구원/한국정보보호센터, 전자서명법 제정을 위한 토론회 발표논문집, 1998. 6
13. 김현, 김학일, "RSTI불변 지문인식 알고리즘", 전자공학회 논문지 제35권, s편, 제6호, 1998, 6.
14. 양지성, 안도성, 김학일, "자동 지문 인식을 위한 의사 특징점 제거 알고리즘", 대한전기학회 99년 추계학술대회 논문지 , 1999, 11
15. 김현 , "RSTI 불면 지문 특징량 추출 및 인식과 응용 (RSTI-invariant Feature Volume Extraction and Recognition of Fingerprints and Applications)" , 인하대학교 자동화 공학과 석사 학위 논문 , 1998년 2월
16. 양지성, "자동 지문 인식을 위한 의사 특징점 제거 알고리즘(False Minutiae Filtering Algorithm for Automatic Fingerprint Identification)", 인하대학교 자동화공학과 석사 학위 논문, 2000, 2