정보 및 제어 심포지엄(ICS'04) 2004. 5. 22

손혈관 인식 시스템의 경쟁기술현황과 전망

Forecast and Present Technology of Hand Vascular Pattern Recognition System

김 재 우, 여 운 동, 배 상 진, 성 경 모
(Kim Jae Woo, Yeo Woon Dong, Bae Sang Jin, Seong Kyung Mo)

Abstract - Biometrics consist of technologies that support automatic identification or verification of identity based on behavioral or physical traits. Biometrics can authenticate identities since they measure unique individual characteristics including fingerprints, hand geometry, iris, hand vascular patterns and facial characteristics. we review the state of the hand vascular patterns identificatin technology and compare other competitive authentication technologies such as cryptography, electronic signature and PKI.

Key Words : 생체인식, 손혈관, 정맥인식

1. 국내외 기술개발 동향

손혈관 인식 시스템 기술은 영국의 NEU Science와 BTG 등의 연구기관을 중심으로 정맥인식을 이용한 개인인증에 관한 연구가 시작된 이래, 정맥 영상추출의 우수한 식별성 때문에 연구가 활발히 진행 중에 있다. 특히 이 분야는 국내 벤처기업인 넥스턴(BK 시스템)이 BK100, BK200이라는 제품을 세계 최초로 상용화하였으며 특허를 보유하고 있다.

해외 생체인식기술을 분야별로 보면, 지문이 48.8%, 얼굴이 15.4%, 장문이 10.4%, 홍채 6.2%로 지난 3년 동안 지문인식 부문이 전체 생체인식 중에서 가장 큰 비중을 차지하고 있다.

앞으로 생체인식 분야의 발전 추세는 보다 안정적인 사용성(Usability), 사용자 편의성, 안정된 성능을 제공하는 생체인식 시스템의 개발로 진행되고 있다. 다양한 특징의 융합(Multimodal or Fusion)을 이용하여, 각 생체인식시스템에서 발생되는 단점을 서로가 보완하여 장점만을 부각할 수 있는 시스템이 개발되고 있다.

생체인식기술 관련 국내의 연구는 대부분 지문인식과 얼굴인식에 편중되고 있다. 대규모 실용화를 위한 기술 수준에 도달하지는 못한 상태이다. 생체인식 기기 중에서 지문인식기가 그 주류이고, 그중 주로 출입통제용을 연구 및 출시하고 있다.

BSP의 국제현황을 살펴보면, SVAPI(Speaker Verification API)가 처음으로 개발되었고, 1997년 초에 HA-API(Human Authentication API)가 개발되었으며, 1997년 12월에 HA-API V.1.03, 1998년 4월에 V.2.0이 발표되었다. 1998년 I/O Software: low-level BAPI 발표되었고, 1998년 4월에는 BioAPI Consortium이 결성되었다. 다중 레벨의 산업계표준 생체인식 API를 만들기 위하여 6개 회사가 연합되었고, 1999년 3월에는 45개회사 연합한 HA-API, BAPI, BioAPI group BioAPI Consortium이 결성되었다. 1999년 12월에는 BioAPI Consortium이 결성되어 High-level 사양 초안을 배포하였다. 2000년 3월에는 BioAPI Consortium Specification V.1.0을 발표하였고, 2001년 3월에는 BioAPI Consortium Specification V.1.1 발표되었다.

BSP의 국내현황을 살펴보면, 인식 알고리즘 및 최신 기술 동향에 관한 연구를 수행하는 Biometric 연구회가 있다. 업계에서는 지문, 홍채, 정맥 인식에서 독자적인 기술 개발을 수행할 예정이다. 국내에서도 2001년 2월 한국생체인식협의회가 발족되었으며, 향후에는 단일 생체인식의 한계 극복을 위하여 다중생체 기술을 이용한 생체인식 기술과 국제 표준과의 연계된 기술을 필요로 하고 있다.

2. 대체기술 및 경쟁 기술 동향

전자상거래 확산에 따라 생체인식에 따른 인증 뿐만 아니라 대체기술과 경쟁기술로서 전자서명, 키관리, 인증서비스가 새롭게 부상하고 있으며, 이에 적용하기 위한 인터넷 보안 기반 기술인 정보보호 기반 기술로서는 암호화기술, 인증기술, 전자서명, PKI 및 WPKI 등이 있다.

2.1 암호화 기술

2.1.1 암호화 기술 개요

암호 기술이란 합법적 참여자들간에 메시지 변/복조 규칙에 대한 약속을 정하고 이 규칙에 따라 송신하려는 메시지를 변조시켜 전달하고, 메시지 수신시 또는 접근 권한이 있는 사람이 필요에 따라 이를 복조하도록 하는 기술을 말한다. 다시 말해서 메시지를 암호화함으로써 암호규칙을 모르거나 암호화나 복호화에 필요한 핵심적 정보를 알지 못하는 사람

저자 소개
* 金 載 佑 : 韓國科學技術正報硏究院
** 呂 雲 東 : 韓國科學技術情報硏究院
*** 裵 相 鎭 : 韓國科學技術正報硏究院
****成 京 摸 : 韓國科學技術正報硏究院

은 해독할 수 없도록 하여 메시지를 원래 형태로 복원하지 못하도록 함으로써 제 3자로부터 메시지 내용을 보호할 수 있다.

2.1.2 비밀키 암호시스템

이 기법은 정보의 암호화나 복호화 시 같은 키를 사용하는 알고리즘 방식으로서 고전적인 모든 암호기법은 여기에 속하며, 공개키 암호방식이 나오기 전까지 모든 암호시스템에서 이용해왔다. 공개키 알고리즘에 비해 알고리즘이 매우 간단하여 속도가 빠르며, 소프트웨어 구성 시 파일크기를 작게할 수 있으므로 하드웨어로 구현하는 경우 회로가 간단해지는 등 경제적 이점 때문에 널리 이용되고 있다. 비밀키 암호방식을 위한 알고리즘 종류에는 데이터 취급 단위 크기에 따라 데이터를 큰 블록으로 나누어 암호화하는 블록 사이퍼 방식과 비트 혹은 단위로 암호화하는 스트림 사이퍼 방식으로 나눈다. 현재 대표적인 비밀키 알고리즘은 1977년 공표된 DES(Data Encryption Standard)로서 UNIX 운영체제의 패스워드를 암호화하는 'crypt'에 이용되며, 특히 미국과 유럽은행에 의해 EFT(Electronic Fund Transfer)시스템에 이용되는 등 광범위하게 사용되고 있다.

2.1.3 공개키 암호시스템

중요한 정보의 안전한 보호를 위해 고대로부터 사용되어온 암호의 최대난제는 암호화과정에서 사용되는 키를 안전하게 분배시키는 일이다. 이의 해결방안으로 등장한 것이 1976년 Diffie와 Hellman이 제안한 공개키 암호기법으로 키에 관한 정보를 공개함으로써 키관리의 어려움을 해결하고자 하였다.

2.1.4 암호기술동향

1977년 미국 상무부 산하 국가표준국이 대칭 키 방식의 암호 알고리즘인 DES를 국가표준으로 채택하여 민간에 보급한 이래, 유럽에서는 1992년도에 128비트 암호 알고리즘 IDEA를 개발, 유럽 표준으로 채택하고 이를 국제통상 등의 업무에 활용되고 있다. 미국에서는 키 복구 기능을 제공하는 제품을 1997년부터 상용화하여 시판 중에 있으며, 정부와 상업적인 용도로 모두 사용할 수 있다. 유럽은 2000년부터 NESSIE 프로젝트를 추진하여 암호프리미티브 전반에 걸쳐 유럽 표준 암호 알고리즘을 개발하였다. 이스라엘은 정보보호 분야를 전략적 기술 개발 분야로 설정하고 암호 기술에서 선도 기술을 보유하고 있으며, 일본은 128비트 암호 알고리즘 MISTY를 1996년에 개발하였고, 이의 변형인 KASUMI 블록 암호 알고리즘을 2000년에 IMT-2000 표준으로 채택하였다. 이처럼 최근 선진 각 국에서는 유, 무선 네트워크 분야에 적합한 보안 프로토콜과 암호 솔루션 개발에 많은 투자를 하고 있으며, 이들의 핵심 연산 요소로 독립형 및 내장형 고속 암호 프로세서가 사용되는 추세이다. 인텔, BroardCom 등 미국의 선진 반도체 회사들은 암호 알고리즘의 고속 처리 프로세서를 네트워크 프로세서 형태로 개발하였거나 개발중이다.

국내에서는 1997년 KCDSA 전자서명 알고리즘, 1998년 HAS-160 해시함수, 1999년 128비트 블록 암호알고리즘인 SEED 등을 자체 개발하여 표준으로 보급하고 있다. 그러나 국내의 고속 암호 프로세서 설계 기술은 매우 낙후된 실정으로 일부 연구소와 기업에서 부분적인 기술을 확보하고 있고 또한 공개키 기반구조 환경이 구비되어 있으나 기밀성을 지원하는 암호키 관리 기반 구조는 아직 구축되고 있지 못한 실정이다. 시큐어피아의 Crypto Engine, 아라리온의 Cipher, 퓨처시스템의 Secure Gate 2000, 텔레시큐어 CNISTTM, 시큐리티테크놀로지스의 SCC101, CryptoXL 등이 있으며 성능 면에서는 외국제품과 많은 차이를 보이고 있다.

2.2 인증 기술

인증은 어떤 사실을 증명하거나 확인하기 위해 사용되는 기능으로서 전자상거래에 있어서 인증 서비스의 목표는 크게 안전한 전자상거래의 보장, 개인 및 기업의 비밀보장, 거래사실에 대한 증명으로 분류된다.

2.2.1 인증의 유형

통신 상대방 한쪽에 대해서만 인증을 하는 단방향 인증과 통신 상대방 서로에 대하여 쌍방향으로 인증을 행하는 상호 인증으로 분류할 수 있다. 그리고 전산망에서는 서로 통신망에 연결된 실체가 적법한 상대인가를 인증하는 사용자 인증과 발신 데이타가 변조되지 않고 전달되었는가에 대해 인증을 하는 메시지 인증으로 분류할 수 있다. 사용자 인증은 사용자가 터미널을 통하여 컴퓨터시스템에 들어가기를 원하거나 혹은 일괄작업의 실행을 요구할 때 사용자의 신분을 확인하기 위한 방법이다. 메시지 인증은 특별한 데이터 항목의 근원에 대한 본질성을 제공하며, 데이터 항목이 그 출처를 떠난 이후 수정되지 않았다는 보증이 있어야 한다.

2.2.2 인증 기반 기술

ITU에서는 인증에 대한 표준으로 X.509를 제정하였으며, X.509를 이용한 인증시스템 구성은 최종사용자가 인증서 및 CRL 저장소와의 운영 및 관리업무를 기본으로 하여, CA와 인증서 및 CRL 배포 등 각각의 CA와는 관리업무를 주고받는 것으로 되어 있다. 그리고 IETF에서는 PKIX(Public Key Infrastructure(X.509))라는 그룹을 결성하여 공개키 기반의 인증 시스템에 대한 표준화 작업을 추진하고 있다. 또한 전자서명 등 공개키 암호화 기술의 활용에 대해서는 RSA사에서 제안한 PKCS(Public-Key Cryptography Standards)가 표준으로 수용되고 있다.

2.2.3 인증기관의 분류

인증기관은 인증서를 발급하는 기관으로 다양한 분야에 존재할 수 있고, 서로 다른 인증기관의 인증서를 가지고 있는 서로가 거래할 수 있다. 이러한 인증서에는 이용범위에 따라 Public Certificate와 Private Certificate로 구분할 수 있다. 이와 마찬가지로 CA(Certification Authority)구축에 있어서도 인터넷과 같은 공공네트워크에서 인증서를 사용할 목적으로 CA를 구축한 경우와 조직 내에서 이용할 목적으로 인증서를

발행하고 CA를 구축한 경우로 구분된다. 이를 각각 Public CA와 Private CA라 칭한다. 대표적 Public CA는 VeriSign, Private CA는 Frontier Technology사 e-Cert가 있다.

2.2.4 인증기술 주요 동향

공개키 알고리즘인 RSA를 이용한 서명 및 인증기법이 산업표준으로 널리 이용되고 있고, 1994년에 미국정부가 전자서명 방식인 DSS를 표준으로 채택하여 정부기관이 사용되고 있다. 미국, 유럽 등 선진국에서는 안전한 전자상거래를 위하여 PKI를 구축하여 키 복구 등의 키 관리에 활용하고 있다.

2.3 전자 서명

이의 생성은 데이터축약 알고리즘을 사용하여 전자서명을 요약한 일정한 길이의 축약정보인 해시값을 생성한다. 그리고 전자서명 생성 알고리즘과 서명자의 서명 생성키를 사용하여 전자문서의 축약정보에 전자서명을 하고 서명문을 생성한다. 전자 서명은 알고리즘에 따라 처리할 수 있는 서명문의 크기는 다르지만 각 알고리즘마다 고정된 크기의 서명문을 요구한다. 실제로 서명해야할 문서는 이보다 긴 문서일 경우가 대부분이며, 이때 전체 문서를 서명 가능한 크기로 나누어 각각에 대해서 디지털 서명을 생성하는 것은 여러 가지 면에서 비효율적이다. 이러한 문제를 해결하기 위해 임의의 길이 입력에 대해 고정된 길이의 출력을 생성하는 함수로 서명문에 대한 압축을 수행하는 함수인 해시함수를 이용한다.

2.4 PKI와 WPKI

전자 상거래와 정보 유통의 안전성과 신뢰성을 확보하기 위한 시스템으로 상대방의 신원을 확인하고 정보내용의 변경 확인과 비밀유지 기능을 갖는 지식 정보화 사회의 핵심기술인 공개키 기반구조(Public Key Infrastructure)와 무선 환경에서 필요한 무선 공개키 기반구조(Wireless PKI)가 있다.

2.4.1 PKI

공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 복합적인 보안 시스템 환경으로 암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템이다. 이는 전자상거래나 정보유통의 안전성과 신뢰성을 확보하기 위한 것으로 상대방의 신원 확인, 정보 내용의 변경확인, 비밀유지 기능 등을 갖는다. 이의 암호화 시스템은 암호화와 복호화키가 다르므로 데이터를 암호화하고 이를 다 풀 수 있는 열쇠가 달라 거의 완벽한 데이터보안이 가능하고 정보유출의 가능성이 적은 시스템이다. 이 시스템은 인터넷상의 보안을 위한 광범위한 기업응용 프로그램에 웹 보안, 전자우편 보안, 원격접속, 전자문서, 전자상거래 응용 등 보안솔루션을 제공한다.

PKI 구성요소로서 인증기관(CA), 등록기관(RA), 디렉토리 서비스(DS), 사용자, 인증서로 구성되며, 사용자의 신분과 공개키를 연결해주는 문서인 인증서는 인증기관의 비밀키로 전자 서명하여 생성된다.

2.4.2 WPKI

최근 휴대폰 등 이동 단말기를 이용한 무선인터넷 사용이 급증하면서 모바일 뱅킹, 증권거래, 인터넷 쇼핑몰에서도 무선인터넷을 통한 전자상거래가 확산되고 있다. 무선환경에서도 기밀성, 무결성 등을 가능하게 할 수 있는 정보보호서비스가 필요하며, 유선인터넷과 동일하게 요구되고 있다. 그러나 무선 환경에서는 낮은 대역폭과 단말기 제한으로 인한 차이점과 시간지연, 연결의 불안전성 등의 네트워크 문제와 적은 메모리, 배터리, 작은 디스플레이, 입력장치 등 유선환경에 비해 많은 제약사항을 가지고 있다. 무선 인터넷 기술은 노키아, 에릭슨, 모토롤라 등 세계 이동통신 회사가 주축이 된 WAP(Wireless Application Protocol) Forum에서 주창한 WAP방식과 MS사의 ME(Mobile Exploror)방식으로 양분되어 무선 PKI기술도 WAP과 ME 두 방식으로 구분된다.

3. 향후기술 전망

현재 BSP는 지문인식 시스템 위주로 개발되고 있다. 하지만 지문인식 시스템은 제한된 사용성으로 인해 제품보급이 지연되고 있어, 안정적인 시스템 성능과 사용성을 제공하는 혈관인식시스템에 대한 관심이 높아질 것으로 예상된다.

사람의 손(등)은 수년 동안 생체인식과 같은 정보의 소스로서 사용되어 왔으나 손 인식 제품을 생산하는 업체는 아직 매우 적다. 이와 같은 현상의 주된 이유는 손 인식 도구가 컴퓨터 기반의 응용에는 적절하지 못하기 때문이다. 대신 물리적 접근 제어, 이주나 이민관련, 법질서관련 응용분야에서는 여전히 사용될 것이다.

생체인식 기술을 응용한 컴퓨터부문의 응용분야 전망을 살펴보면, 기존 보안관리가 물리적 접근제어 측면에서 주로 이루어져왔던 것에서 전자상거래나 네트워크/PC보안 등으로 옮겨감에 따라 생체인식 응용분야 또한 이에 병행하여 변할 것으로 보인다. 앞으로 구현될 수 있는 제품은 혈관 인식 인터넷 개인 인증 및 보안 인증 서비스 시스템으로 인터넷을 통한 실시간 개인 인증시스템이다. 이는 정부주도의 시범사업과 금융권/카드사 등 대규모 인증시스템에 활용될 수 있다. 다음은 혈관 인식 인터넷 개인 인증 및 보안 인증 서비스 SDK이다. 이 시스템은 프로그램 개발자에게 안정적인 혈관인식 SDK를 제공한다. 또한 개별 생체 인식 장비의 특성을 파악할 필요 없이 신속하고 안정적인 프로그램 개발 가능하고, 다수의 생체인식 연동이 가능할 것이다.

참 고 문 헌

[1] 최환수, "손의 혈관분포패턴을 이용한 생체인식 기술", 정보과학회지, Vol.19, No. 7, 2001.7

[2] 길민정, "생체인식산업동향 세계 생체인식 시장 및 기술 전망", 한국정보보호진흥원, 2001.12

[3] 김지회, 전준철, "인터넷 기반 조합형 바이오 메트릭 인증 시스템 설계", 인터넷 정보학회 춘계학술발표 논문집, 2000.