생체정보 수집 시스템 설계 및 구현

고기남*, 이용섭*, 문남미**
*플레이스비(주) 뉴미디어연구소
**호서대학교 컴퓨터소프트웨어학전공
e-mail:gnko@placeb.com

A Design and Implementation of The Biometrics Collection System

Ginam Ko*, YongSub Lee*, Nammee Moon**
*placeB Inc. Newmedia Laboratories
**Dept. of Computer Software, Hoseo University

요 약

본 논문은 지문, 홍채, 얼굴 및 서명 이미지를 수집하고, 이를 기 수집된 생체정보들과 비교 분석하여 고유한 개인 정보를 생성함으로써, 회원 및 직원 등 소규모 단위뿐만 아니라, 국가 단위의 주민 정보에도 활용 가능한 생체정보 수집 시스템의 설계 및 구현에 관한 것이다.

제안 시스템은 개인정보 수집기, 생체정보 수집기(지문수집기, 홍채수집기, 얼굴수집기 및 서명 수집기), 생체정보 검증기(지문검증기, 홍채검증기)와 생체정보 관리기로 구성되어 있으며, 웹페이지 형태의 개인정보 수집기에서 Java로 구현된 생체정보 수집기의 호출 및 데이터 송수신을 위해, 최근 기술적 추세에 맞추어 자바애플릿 형태가 아닌 브라우저 플러그인 형태의 데이터 연동모듈을 구현하였다.

1. 서론

최근 생체정보 기술의 발달로 인해, 개인 식별, 전자여권 및 주민증, 출입 통제, 개인 정보보호 등 다양한 분야에서 생체인식(Biometrics) 기술이 활용되고 있으며, 이를 통해 기존의 사용자이름과 비밀번호 기반의 인증절차 등이 보다 손쉽고 안전하게 사용될 수 있도록 개선 및 보완이 요구되고 있다[1][2].

특히, 전자 여권 및 주민증의 경우에는 획득한 개인의 생체정보를 기반으로 각종 복지서비스 및 주민서비스 등 각종 전자정부서비스와 최근 주목받고 있는 핀테크(FinTech)와 접목하여 다양한 금융 서비스에 활용 가능하다. 또한, 현재 대다수의 국가에서 주민증(Identity Card)를 사용하고 있으며, 최근 기술발전으로 인해 RFID 칩이 내장된 전자주민증(Electronic Identity Card)으로 교체되거나 새롭게 도입되고 있다. 이러한 전자 여권 및 주민 시스템에서 개인 식별 및 인증을 위해서는 생체정보 기술의 활용이 필수적이다[3][4][5].

이에, 본 논문에서는 회원 및 직원 관리 등 중소규모 단위에서부터 전자정부포털과 연계된 국가 단위의 주민정보 시스템에서도 활용 가능한 생체정보 수집 시스템에 대해 설계하고 이를 구현하였다.

2. 관련연구

2.1. 전자 여권 및 주민증

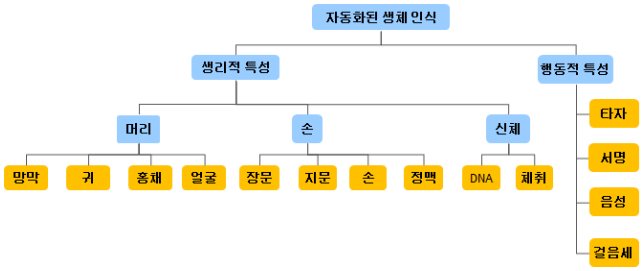
전세계 약 100여개 이상의 국가에서 국민들에게 주민증을 발급하고 있으며, 이는 여권과 동등하게 각 국가에서 국민들의 신분 증명에 활용된다. 또한 최근 기술 발전 추세에 맞춰 RFID 칩이 내장된 스마트카드의 형태로 발전되고 있으며, 유출에 민감한 개인정보 및 개인인증용 생체정보 등을 RFID 칩에 안전하게 보관하고, 다양한 서비스에서 인증 수단으로 활용 가능하다[2][4].

최근 러시아에서는 주민증, 복지카드 및 국내 여권 기능과 함께 금융 서비스를 통합하여 활용 가능한 UEC(Universal Electronic Card)를 도입하는 등 다양한 서비스와 결합되어 적용되고 있고 있으며, 개인정보 및 금융 서비스를 안전하게 이용하기 위해 생체정보 기술을 필수적으로 사용하고 있다[3][4][8].

2.2. 생체인식

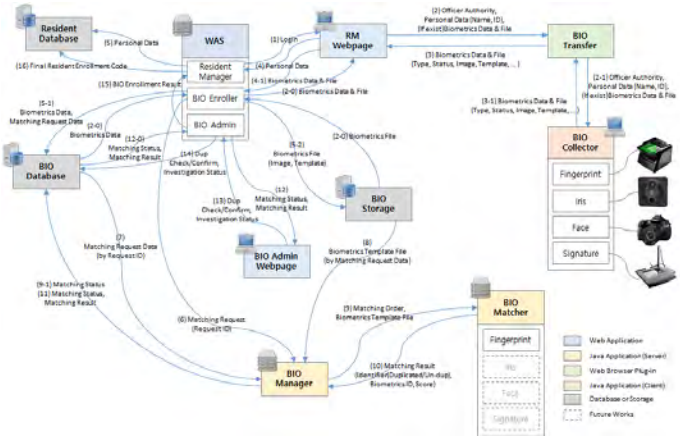
생체인식 기술은 생체정보를 템플릿(Template)의 형태로 수집 및 등록하여, 인증 시 센서로 취득한 정보와 비교하여 사용한다. 기존의 비밀번호 또는 열쇠 등 물건에 의한 인증 방식은 사용자의 망각이나 분실 또는 도난 등의 우려가 존재하나, 생체정보는 이러한 위험성이 낮고, 제3자가 인증하는 것을 방지할 수 있기 때문에 각종 서비스에서의 개인인증, 보안지역의 출입통제, 출입국 관리 및 전자여권 및 주민증을 통한 신원 인증, 금융서비스에서의 인증수단으로 널리 사용되고 있다[3][10].

생체인식에 사용되어지는 다양한 생체정보는 (그림 1)에서 나타내는 것과 같이, 생리적 특성과 행동적 특성으로 분류할 수 있으며, 망막, 귀, 홍채, 얼굴과 서명, 음성 및 걸음걸이 등 매우 다양하다. 이 중, 지문과 홍채는 가장 대중적으로 많이 사용되는 생체정보이다[1][10].



(그림 1) 생체인식의 종류

3. 생체정보 수집 시스템 설계



(그림 2) 생체정보 수집 시스템 구성

본 논문의 생체정보 수집 시스템(Biometrics Collection System)의 구성은 (그림 2)와 같으며, 전체 6개 애플리케이션이 10단계에 걸쳐서 개인정보 및 생체정보 수집 및 검증 작업을 수행한다.

첫 번째 단계로 사용자 관리기(Resident(Member) Manager)에서 사용자(주민)의 이름, 생년월일 등 개인 데이터를 입력하면 데이터 연동 모듈을 통해 클라이언트 PC의 생체정보 수집기(Biometrics Collector)를 호출하고 개인 데이터를 전달한다. 전달받은 개인 데이터를 기반으로 생체정보 수집 장치(지문 스캐너, 홍채 스캐너, 카메라 및 서명패드 등)를 활용하여, 사용자의 지문, 홍채, 얼굴 및 서명 이미지를 수집한 뒤, 이를 다시 데이터 연동 모듈(Biometrics Transfer)를 통해 사용자 관리기에게 전송한다. 사용자 관리기는 사용자로부터 입력받은 개인 데이터를 바탕으로 임시 사용자 정보를 생성하고, 생체정보 관리기(Biometrics Manager)에게 생체정보를 전달한다. 생체정보 관리기는 전달받은 생체정보 파일 중 템플릿 파일을 활용하여 생체정보 검증기(Biometrics Matcher)에게 검증을 요청한다. 이때, 검증기에 기 수집된 생체정보 중에서 중복되는 생체정보 존재 여부와 대상, 유사도 점수를 생체정보 관리기에게 전달한다. 생체정보 관리기는 전달받은 검증 결과를 생체정보 관리자(Biometrics Admin)에게 전달하며, 이때 중복되는 생체정보는 관리자가 최종적으로 재차 검증하게 된다. 재차 검증 후, 중복정보로 결정되면 검증 결과를 “등록거절(Denied)”로 사용자 관리기에 전달하고, 해당 개인정보는 중복데이터로 처리하여 등록이 거절된다.

재차 검증 후, 기 수집 생체정보와 중복되지 않는 고유한 데이터로 검증되면, 검증 결과를 “등록(Enrolled)”으로 사용자 관리기에 전달하고, 최종적으로 해당 사용자를 사용자 목록에 등록 처리하게 된다. 이러한 과정을 통해 중복되지 않는 고유한 사용자(주민) 정보를 수집할 수 있으며, 다양한 개인 식별 응용서비스에 활용 가능하다.

(그림 3), (그림 4), (그림 5), (그림 6)은 각각 지문수집기, 서명수집기, 홍채수집기 및 얼굴수집기의 UI 설계를 나타낸 것으로, 각 수집기는 생체정보 뷰어(Viewer)와 캡쳐(Capture) 모듈로 구성된다. 기 수집된 생체정보가 있다면 뷰어에서 확인 가능하며, 새로 수집하여 교체할 수 있다. 또한, 기 수집된 생체정보가 없는 경우 시작(Start) 버튼을 클릭하여 새로 수집할 수 있다.

얼굴수집기의 경우, 생체인식 국제표준인 ISO/IEC 29109 및 국제민간항공기구 (ICAO: International Civil Aviation Organization) 표준을 준수하기 위해, 수집한 얼굴 이미지를 평가 및 확인하는 작업을 추가로 수행할 수 있다[12][13][14].

(그림 3) 지문수집기 UI 설계

(그림 4) 서명수집기 UI 설계

(그림 5) 홍채수집기 UI 설계

(그림 6) 얼굴수집기 UI 설계

4. 생체정보 수집 시스템 구현

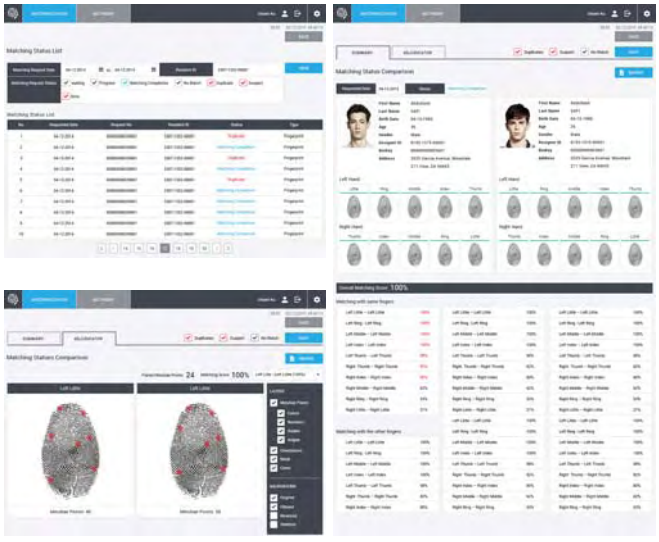
본 생체정보 시스템의 사용자 관리기 및 생체정보 관리자를 구현하기 위한 서버 환경은 CentOS6.5, WebLogic 12c (12.1.3) 및 Oracle 12c (12.1.0.2.0)를 사용하여 WAS(Web Application Server)와 DB 서버를 구성하였으며, Java 8 및 Spring F/W를 사용하여 구현하였다. 또한 사용자 환경은 Windows 10에서 파이어폭스(Firefox) 40.0을 사용하여 구성하였다.

생체정보 수집기는 각 수집 장치의 작동 환경, 드라이버 관련 문제로 인해 웹 애플리케이션으로의 구현이 불가능하고, 리눅스(Linux) 및 OS X 드라이버를 지원하지 않기 때문에, 본 논문에서는 윈도우즈 환경만을 지원하며, 자바(Java) 네이티브(Native) 애플리케이션으로 구현하였다. 수집기의 구현에는 Neurotechnology의 MegaMatcher 6.0 SDK와 MegaMatcher Accelerator 7.2를 사용하였으며, 생체정보 검증기를 위해 Intel i7, RAM 16GB의 서버를 구성하였다.

웹 기반의 사용자 관리기에서 사용자 개인정보 수집과 함께 생체정보 수집을 위해 생체정보 수집기의 호출 및 상호 데이터 송수신을 위해 웹브라우저의 플러그인 형태의 데이터 연동 모듈을 구현하여 활용한다.

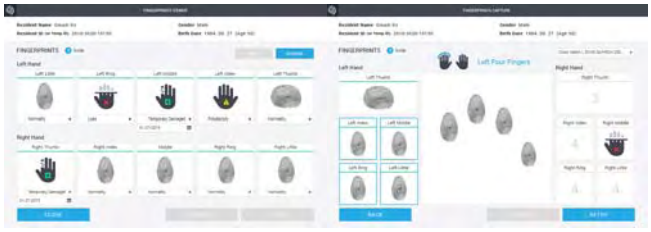
본 시스템에서 각 애플리케이션(또는 모듈)간 개인정보 및 생체정보 전송 시에는 사전에 AES 256 알고리즘을 통해 암호화(Encryption)를 수행한 뒤 전송함으로써, 개인정보와 유출 시 변경이 불가능한 생체정보가 유출되지 않도록 하였으며, 지문 이미지 파일의 경우, 기존의 JPEG, PNG, BMP 등의 이미지 포맷보다 지문에 특화된 이미지 포맷인 WSQ를 활용하였다[11].

본 논문에서는 보다 널리 활용되어지고 있는 지문 및 홍채를 활용한 생체정보 검증만을 구현하였으며, 얼굴 및 서명을 통한 검증은 추후 구현할 계획이다.

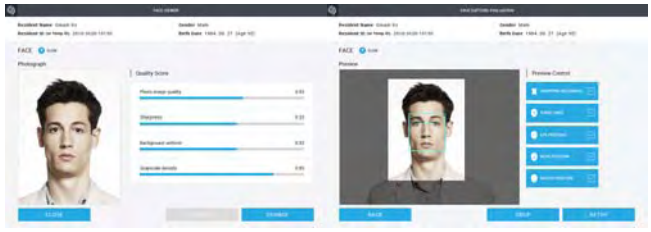


(그림 7) 생체정보 관리자 구현 화면

(그림 7)은 생체정보 관리자의 구현 화면이며, 좌측 상단부터 시계방향으로 검증상태 목록, 중복결과 보고서, 지문 상세 비교 화면이다.



(그림 8) 지문수집기 구현 화면



(그림 9) 얼굴수집기 구현 화면

(그림 10) 서명수집기 구현 화면

(그림 11) 홍채수집기 구현 화면

(그림 8)은 지문수집기 구현화면을 나타내며, 다른 생체정보와 달리 손가락 10개에 대한 상태를 입력한 뒤 지문 데이터를 수집한다. (그림 9)는 얼굴 수집기의 구현화면이며, 좌측부터 ISO, ICAO 표준안에 따른 얼굴 이미지의 밝기, 선명도 및 비율 등을 수치로 표시하였으며, 우측은 촬영 이미지에서 표준에 따른 추출 이미지를 검증하는 화면이다.

마지막으로, (그림 10)과 (그림 11)은 각각 서명수집기와 홍채수집기의 구현화면이며, 서명수집기는 와콤(Wacom) 서명패드를 활용하여 수집한다. 홍채의 경우 전용 스캐너와 일반 카메라를 모두 지원한다.

5. 결론 및 향후 계획

본 논문의 생체정보 수집 시스템은 해당 시스템은 초당 1억개의 지문 또는 2억개의 홍채를 비교 가능하며, 이를 통해 중소규모의 회사 및 기관과 국가 단위에서 전국민을 대상으로한 대규모의 시스템에서도 활용 가능하도록 설계 및 구현하였다.

다만 현재 구현된 방식은 파이어폭스 브라우저만을 사

용환경으로 설정하여, 익스플로러, 엣지 또는 크롬 등과 같은 다른 브라우저에서는 사용할 수 없는 단점이 있다.

그러나, 최근의 NPAPI 배재 흐름에 따라, Java applet 또는 ActiveX 등이 아닌 브라우저 플러그인 방식을 통해 구현함으로써 보안성을 향상시키고, 기존의 인터넷 사용 경험자에게 친숙한 사용 환경을 제공할 수 있다.

향후에는 보다 다양한 브라우저를 지원하고, 국내에 비해 비교적 불안정한 네트워크 환경을 고려하여 보완한다면, 전자여권 및 전자주민증을 도입하고자 하는 다양한 개발도상국에 손쉽게 공급할 수 있을 것으로 예측된다.

또한, 해외에서 국내의 인감(도장)과 같은 효력을 가지고 있는 서명 검증을 바탕으로 개인인증이 가능하게 된다면, 전자 여권 및 주민증 뿐만 아닌 부동산 거래 및 각종 행정/사법 서비스에서도 활용할 수 있을 것으로 기대된다.

참고문헌

[1] 최성필, 정강훈, 문현중, “안드로이드 환경의 다중생체 인식 기술을 응용한 인증 성능 개선 연구”, Journal of Korea Multimedia Society, Vol. 16, No. 3, pp.302-308, 2013.03.

[2] Mariah Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith, “On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards“, Privacy Enhancing Technologies, pp. 245-264, 2013

[3] David D. Zhang, “Automated Biometrics Technologies and Systems”, Kluwer Academic Publishers, 2000

[4] Ozgur Dagdelen, “The Cryptographic Security of the German Electronic Identity Card“, Technische Universitat Darmstadt, Ph.D. Thesis, 2013

[5] Ulf Melin, Karin Axelsson, Fredrik Soderstrom, “Managing The Development Of Secure Identification - Investigating A National E-ID Initiative Within A Public E-Service Context”, Proceedings of the 21st European Conference on Information Systems, 2013

[6] 송충건, 이근호, “지문인식기술과 암호화된 QR코드를 이용한 안전한 신분증 연구”, Journal of Digital Convergence, Vol. 12, No. 6, 2014. 06.

[7] Tai-Pang Chen, Wei-Yun Yau, and Xudong Jiang, “Biometrics on Smart Card”, Biometrics: From Fiction to Practice, 2013

[8] https://en.wikipedia.org/wiki/Universal_electronic_card

[9] Leo F. Goodstadt, Regina Connolly, and Frank Bannister, “The hong Kong e-Identity Card: Examining the Reasons for Its Success When Other Cards Continue to Struggle”, Information Systems Management, Vol. 32, Issue 1, pp. 72-80, 2015

[10] https://ko.wikipedia.org/wiki/바이오메트릭스

[11] Natnicha Anurakphanawan, Poonlap Lamsrichan, “Fingerprint Recognition performance with WSQ, CAWDR, and JPEG2000 Compression”, 2015 6th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES), pp. 1-6, 2015. 04.

[12] “Information technology - Confermance testing methodology for biometric data interchange formats defined in ISO/IEC 19794”, Part 5: Face image data, ISO/IEC 29109-5, ISO/IEC, 3rd Edition, 2014. 04.

[13] “Machine Readable Travel Documents”, Doc 9303, Part 1: Machine Readable Passports, Vol. 1: Passports with Machine Readable Data Stored in Optical Character Recognition Format, ICAO (International Civil Aviation Organization), 6th Edition, 2006

[14] “Machine Readable Travel Documents”, Doc 9303, Part 1: Machine Readable Passports, Vol. 2: Specification for Electronically Enabled Passports with Biometric Identification Capabillity, ICAO (International Civil Aviation Organization), 6th Edition, 2006