情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

바이오정보 워터마킹을 이용한 전자여권 보안기술

이 용 준†
한국인터넷진흥원

e-Passport Security Technology using Biometric Information Watermarking

Yong-joon Lee†
Korea Internet Security Agency

요 약

국제적으로 통용되는 전자여권은 스마트카드, 공개키 기반 암호화, 바이오인식 등 최신의 보안기술이 융합되어 전자여권의 위조 복제 방지를 위해 사용되고 있다. 특히 전자여권의 사용되는 바이오정보는 개인의 가장 민감한 정보로써 위조·복제 되었을 때 가장 큰 피해가 예상되며 바이오정보의 복제 여부를 검증하는 보안기술이 필요하다. 본 논문에서는 전자여권내의 바이오정보 복제를 방지하기 위해 바이오정보 워터마킹을 이용한 전자여권 보안기술을 제안한다. 제안하는 바이오정보 워터마킹은 전자여권의 발급과 전자여권의 판독하는 과정에서 워터마크를 이용하여 바이오정보의 복제 여부를 검출한다. 본 논문은 국내 전자여권의 환경에서 발급 및 판독을 통해 실험결과를 제시하였으며 전자여권의 선택적인 보안기능으로 활용이 가능하다.

ABSTRACT

There has been significant research in security technology such as e-passport standards, as e-passports have been introduced internationally. E-passports combine the latest security technologies such as smart card, public key infrastructure, and biometric recognition, so that these technologies can prevent unauthorized copies and counterfeits. Biometric information stored in e-passports is the most sensitive personal information, and it is expected to bring the highest risk of damages in case of its forgery or duplication. The present e-passport standards cannot handle security features that verify whether its biometric information is copied or not. In this paper, we propose an e-passport security technology in which biometric watermarking is used to prevent the copy of biometric information in the e-passport. The proposed method, biometric watermarking, embeds the invisible date of acquisition into the original data during the e-passport issuing process so that the human visual system cannot perceive its invisibly watermarked information. Then the biometric sample, having its unauthorized copy, is retrieved at the moment of reading the e-passport from the issuing database. The previous e-passport security technology placed an emphasis on both access control readers and anti-cloning chip features, and it is expected that the proposed feature, copy protection of biometric information, will be demanded as the cases of biometric recognition to verify personal identity information has increased.

Keywords: e-Passport, Biometrics, Digital Watermarking

I. 서 론

국제적으로 전자여권 도입에 따라서 전자여권의 표준과 함께 보안기술에 대한 연구가 활발하게 진행되고 있다. 전자여권은 스마트카드, 공개키 기반 암호화, 바이오인식 등 최신의 보안기술의 융합되어 전자여권의 위조 복제 방지를 위해 사용되고 있다. 특히 전자여권에 저장되는 바이오정보는 개인의 가장 민감한 정보이며 위조, 복제 되었을 때 가장 큰 피해가 예상되

접수일(2011년 4월 4일), 게재확정일(2011년 7월 25일)
† 주저자, yjlee@kisa.or.kr

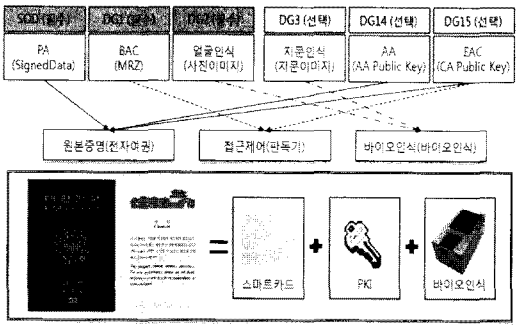
고 있지만 현재의 전자여권 표준은 바이오정보의 복제 여부를 검증하는 보안기능은 제공되지 않고 있다[1].

본 논문에서는 전자여권내의 바이오정보 복제를 방지하기 위해 바이오정보 워터마킹을 이용한 전자여권 보안기술을 제안한다. 제안하는 바이오정보 워터마킹은 전자여권의 발급하는 과정에서 획득일자를 육안으로 인지하지 못하게 삽입하고 전자여권의 판독하는 과정에서 워터마크를 추출함으로써 바이오정보의 복제 여부를 검출한다. 기존의 전자여권 보안기술은 판독기 접근제어, 칩복제 기능에 중점을 두었으며 전자여권의 신원확인을 위해 바이오인식을 채택하는 경우가 증가에 따라 제안하는 바이오정보 복제방지 기능이 요구될 것으로 사료된다.

II. 기존연구

2.1 전자여권의 개요

전자여권은 국제민간항공기구(ICAO : International Civil Aviation Organization)에서 전자여권 개념을 확립하고, 국제호환성을 확보하기 위한 국제 표준화 작업에 따라 비접촉식 스마트 기능의 IC(Integrated Circuit) 칩에 얼굴, 지문 이미지의 바이오정보와 전자여권 소지자의 개인정보, 그리고 전자여권 보안 프로토콜을 위한 보안키를 저장한다. 전자여권 칩의 데이터 개인정보에 대한 표준화된 논리적 데이터 구조(LDS : Logical Data Structure)에 맞게 각각의 데이터 그룹(DG : Data Group)에 개인 신상정보를 저장한다. 전자여권은 기존 여권을 이용한 출입국 관리 시스템의 단점을 보완하고, 여권 소지자의 편리성과 보안성을 고려한 차세대 출입국 관리 시스템이다. [그림 1]은 전자여권에 사용되는 원본증명, 접근제어, 바이오인식 등 융합보안기술에 대한 전체구성도를 나타낸다[3].



[그림 1] 전자여권의 보안기술

전자여권을 이용한 개인 식별 기술은 전자여권 칩과 판독시스템 사이의 물리적인 접촉 없이 인식이 가능하다는 장점과 함께 도청 공격, 데이터 위·변조, 바이오정보 노출, 전자여권 복제 등의 개인 신원 정보 침해 문제를 발생 시킬 수 있다. 이러한 개인 신원 정보 침해 문제를 해결하기 위해서 전자여권은 스마트카드, PKI, 바이오인식의 융합 보안기술이 적용되어 있다.

2.2 전자여권의 보안위협

- 스키밍(Skimming) : 스키밍은 사용자가 인지하지 못하는 상태에서 비인가된 리더기로 RF 정보를 취득하는 적극적 공격 방식이다.
- 도청(Eavesdropping) : 도청은 인가된 리더기로 칩에 접근할 때 칩내 정보를 가로치는 공격이다. 도청 공격은 스키밍 공격과 대비하여 원거리에서 도청이 가능한 수동적 공격의 특징을 가진다.
- 추적(Tracking) : 공격자가 RF 칩 정보를 취득하여 전자여권 소지자를 추적할 수 있다. 취득된 RF 칩 정보로 동선을 추적하고 부가적인 정보와 결합하여 전자여권 소지자의 개인정보를 획득할 수 있다.
- 핫리스팅(Hotlisting) : 공격자는 핫리스팅을 이용하여 RF 칩 정보와 관련된 개인정보를 획득하여 추적 가능한 데이터베이스를 구축할 수 있다. 핫리스팅 정보는 개인 또는 소속된 그룹을 식별할 수 있는 정보로 사용될 수 있다. 공격자는 전자여권의 식별 정도로 소지자의 사진과 국적과 결합하여 개인을 식별할 수 있다[7].
- 신원 사칭(Identity Theft) : 신원 사칭는 부가적인 위험이다. RF 칩의 식별 정보가 암호화되지 않는 경우, 소지자 성명, 신원정보를 취득하여 공격자가 신원 사칭을 할 수 있다.
- 복제(Cloning) : 공격자는 RF 칩의 정보로 부터 신원 복제할 수 있다. 소지자가 인지하지 못하는 상태에서 복제된 전자여권은 실제 전자여권으로 사용이 가능하다.
- 바이오정보 유출(Biometric Data Leakage) : 전자여권은 사진과 지문과 같은 바이오정보를 저장하고 있다. 물리적으로 보안이 통제된 환경에서는 바이오정보가 암호화되지 않아도 되지만 현재의 전자여권 시스템은 자동화 뿐 아니라 출입국 담당자에 의해 확인하기 때문에 바이오정보

의 유출이 가능한 위험을 가지고 있다.

- 암호학적 약점(Cryptographic Weaknesses) : ICAO 표준은 전자여권과 리더기 간의 암호화 통신을 제공하기 위해 광학판독 방식을 제정하였다. 전자여권을 광학판독하여 성명, 생년월일, 전자여권 번호로 암호키를 생성한다. 전자여권 소지자는 외국에서 출입국하는 경우 전자여권의 키 정보를 제공해야 하지만 문제가 발생한 경우, 키를 폐지하는 메커니즘을 가지고 있지 않다[10].

2.3 전자여권 보안목표

- 신원확인(Identification) : 전자여권 프로토콜이 완료되면 전자여권과 판독시스템은 연계 시스템을 통해 신원을 확인해야 한다.
- 데이터 원본 확인(Data Origin Authentication) : 출입국 담당자가 판독에 의해서 전자여권내의 정보와 전자여권 책자의 MRZ와 사진정보로 원본임을 확인해야 한다.
- 무결성(Integrity) : 전자여권 프로토콜이 수행될 때 전자여권내의 데이터 무결성은 전자서명 검증으로 확인한다. 판독기는 전자여권내 SOD, LDS에 대한 전자서명을 검증하여 전자여권에 저장된 정보가 변경되지 않았음을 확인할 수 있다.
- 상호인증(Mutual Authentication) : 판독기는 전자여권을 인증해야 하며 개인정보는 제공하기 전에 전자여권 칩은 판독기를 인증해야 한다. 비인가된 판독기가 전자여권의 개인정보와 바이오정보를 획득하는 것을 방지해야 한다.
- 데이터 기밀성(Data Confidentiality) : 전자여권과 판독시스템간의 세션키 보안강도에 기반하여 전자여권 프로토콜은 통신간의 데이터 기밀성을 제공해야 한다. 비인가된 리더기는 전자여권내의 LDS와 보안키에 대해 접근할 수 없어야 한다. 전자여권과 판독기는 세션키 교환 프로토콜이 완료되면 해당 세션키는 외부에 노출되어서는 안된다.
- 데이터 인증(Data Authenticity) : 전자여권 프로토콜이 완료되면 전자여권과 판독시스템은 통신간의 메시지에 대하여 데이터 인증을 제공해야 한다.
- 프라이버시(Privacy) : 전자여권 프로토콜이 모두 완료된 이후 인가된 판독기를 통해서만 전자여권의 신원정보가 획득되어야 한다[5].
- 세션키 보안성(Session key security) : 전자여권과 판독기의 교환되는 세션키는 확률적인 보안성을 제공해야 한다.
- 부인방지 : 출입국 절차에서 전자여권 소지자의 신원을 확인할 수 있으나 향후 출입국의 부인방지 위해서 전자여권의 디지털 정보를 획득하여 추적가능해야 한다.
- 키 갱신과 키 무결성(Key Freshness and Key Integrity) : 판독기와 전자여권은 전자여권 프로토콜이 수행될 때 세션키의 갱신성과 무결성을 제공해야 한다. 이전에 사용된 폐기된 세션키가 검출되면 전자여권 프로토콜은 종료되어야 한다.
- 인증서 변경(Certificate Manipulation) : 판독기는 전자여권내의 인증서의 유효성 검증과 상태확인을 수행하여 인증서가 변경되지 않았음을 확인해야 한다.
- 포워드 비밀성(Forward Secrecy) : 세션키와 유도키(KENC, KMAC)가 유출되어도 이후의 통신을 훼손해서는 안된다[9].

2.4 전자여권의 보안 프로토콜

[표 1]은 전자여권 표준에서 채택한 전자여권 보안 프로토콜을 나타낸다[4].

- BAC(Basic Access Control) : LDS를 제공할 때 전자여권은 판독기에게 전자여권의 MRZ (전자여권 일련번호, 소지자 생년월일, 전자여권 만료일자)로 유도된 접근키를 요구한다. 전자여권의 소유자가 제시한 전자여권의 물리적 책자에 있는 정보를 이용하여 접근키를 유도함으로써 접법한 절차임을 확인한다. BAC는 소지자가 인식하지 못하게 전자여권에 접근하는 스키밍 공격을 방어한다[2].
- EAC(Extended Access Control) : 전자여권에는 바이오정보와 같은 가장 민감한 개인정보를 포함하고 있다. 비인가된 판독기로부터 바이오정보를 보호하기 위해서 BAC이외에 부가적으로 EAC 프로토콜을 수행한다. 전자여권 발행국가의 DVC (Document Verifier Certificate) 인증서를 보유하고 있는 판독기에서만 EAC 프로토콜을 수행할 수 있다.
- Passive Authentication(PA) : 전자여권에는 LDS에 있는 모든 데이터 그룹에 대한 해쉬값

이 포함된 SOD(Security Of Document)를 저장하고 있다. SOD는 DS(Document Signing) 개인키로 전자서명하고 DSC(Document Signing Public Key Certificate)로만 검증할 수 있다. 판독기가 DSC를 획득하는 방법은 SOD에 포함시켜서 검증하는 방식과 발행국의 PKD(Public Key Directory)에서 다운로드 받는 방식이 있다. PA는 LDS 정보의 변조 여부를 검증한다.

- Active Authentication (AA) : 판독기는 전자여권내 개인키가 생성한 전자서명으로 인증을 수행한다. 판독기는 전자여권의 DG14에 있는 공개키를 획득하여 전자여권이 생성한 전자서명을 검증한다. DG14는 SOD 해쉬값에 포함되어 판독기에서 전자서명 검증으로 무결성을 확인할 수 있다. 공격자는 전자여권으로부터 개인키를 획득할 수 없기 때문에 AA 는 전자여권의 복제 여부를 검출할 수 있다.

2.5 전자여권 보안 프로토콜 수행절차

미국의 AA 메커니즘을 따르는 전자여권 소지자는 출입국 담당자에게 자신의 전자여권을 제출하면 판독기는 다음과 같이 3단계로 프로토콜을 수행한다.

(1) BAC 프로토콜(선택) : 전자여권과 판독기간의 암호화 통신을 제공한다.
(2) PA 프로토콜(필수) : 출입국 담당자는 전자여권를 읽어 데이터 변조여부를 검증한다.
(3) AA 프로토콜(선택) : 전자여권의 복제여부를 검증한다.

〔표 1〕 전자여권 보안 프로토콜

	PA	AA	BAC	EAC
적용 단계	필수적용	선택적용	선택적용	선택적용
보안 목적	데이터 변조 방지	칩복제 방지	전자여권과 판독기 구간의 보안통신 채널 형성으로 도청 방지	민감한 바이오 정보에 대한 접근통제
공격 방법	공격자가 전자여권내 정보를 변경하는 경우	공격자가 전자여권과 동일한 칩을 복제하는 경우	공격자가 전자여권칩의 정보에 대해 도청을 시도하는 경우	공격자가 전자여권 칩내의 민감한 바이오 정보를 획득하고자 하는 경우
보안 기능	전자여권내 정보를 발행국에서 전자서명하여 칩에 저장하고 판독기에서 검증	전자여권 보안 메모리 영역의 개인키로 전자서명 수행 후 판독기에서 검증	판독기에서 여권책자의 BAC로 접근키 생성하여 전자여권에서 검증	국가간 협정을 통해 판독기는 전자여권 발행국에서 발급받은 개인키로 전자서명 수행 후 전자여권에서 검증

유럽의 EAC 메커니즘은 AA를 대체한 CA(Chip Authentication)과 TA(Terminal Authentication)의 2가지 프로토콜이 추가적으로 포함하여 4단계로 수행한다[6].

(1) BAC 프로토콜(선택) : 전자여권과 판독기간의 암호화 통신을 제공한다.
(2) CA 프로토콜(선택) : AA와 동일한 기능으로 전자여권의 복제여부를 검증한다.
(3) PA 프로토콜(필수) : 출입국 담당자는 전자여권를 읽어 데이터 변조여부를 검증한다.
(4) TA 프로토콜(선택) : 판독기가 전자여권 발행국의 DVC 인증서를 보유하고 있는지를 전자여권이 검증한다. 프로토콜이 완료되면 바이오정보의 민감한 개인정보를 판독기에 제공한다.

2.6 전자여권의 보안취약점

2.6.1 전자여권 보안 프로토콜의 보안취약점

- BAC 보안취약점 : BAC는 전자여권과 판독기간에 3DES 암호화 통신을 수행한다. 세션키는 전자여권 책자의 MRZ로부터 유도가 되며 MRZ는 전자여권의 사용기간인 10년동안 사용된다. MRZ는 생년월일, 유효기간, 전자여권 일련번호로 구성되며 생년월일과 유효기간은 6자리로 전자여권 일련번호는 숫자와 문자로 구성된다. ICAO는 세션키를 유도할 때 56 비트 이상의 보안강도를 권고하고 있으나 실제 전자여권의 경우는 56비트 이하의 비트 보안강도를 가지는 것으로 조사되었다. 그 원인으로 전자여권의 일련번호는 단순한 발행수의 증가이며 소지자의 생년월일은 추측이 가능하고 10년간의 전자여권 사용기간을 고려하면 실질적인 보안강도는 35 비트로 분석된다. 인가된 판독기와 전자여권간의 통신에서 무작위공격으로 정보를 획득하는 실험을 통해 BAC 프로토콜의 문제점이 제기되었다.

- AA 보안취약점 : AA 프로토콜은 AA 공개키는 칩내에 저장한 후 SOD로 무결성을 제공하고 AA 개인키는 칩내의 보안메모리 영역에 저장한다. 판독기는 64 비트의 랜던값을 생성해서 전자여권에 전송하면 AA의 개인키로 전자서명을 수행하여 응답하여 전자여권의 복제여부를 검증한다. 그러나 전자여권내의 AA 개인키를 보안메모리에서 실행을 위해 불러올 때 획득하거나, 공격자에 의한 키충돌 방식을 통해 AA 개인키 획득이 가능하다. 또한, AA 프로토콜을 우회할 수 있는 공격이 보고되었다. 전자여권 속성을 나타내는 지정자 파일이 SOD에 포함되어 있지 않기 때문에 속성 지정자의 변경이 가능하다. AA 프로토콜의 실행가능 속성에 대한 지정자를 제거함으로써 판독기는 AA 프로토콜을 수행하지 않는 검증절차를 수행하게 된다. 따라서 AA 개인키 획득 또는 AA를 수행하지 않도록 하여 원본 전자여권에 대한 복제가 가능하다.
- PA 보안취약점 : PA는 전자여권의 데이터 진위여부는 검증할 수 있지만 복제여부는 판별하지 못한다. 이러한 문제로 ICAO는 전자여권 책자에 대한 물리적인 검증을 포함하도록 하고 있으나 최근에는 자동화된 출입국 시스템을 도입하는 국가가 증가하고 있기 때문에 위조에 대한 문제가 존재한다. PA의 다른 문제점은 공개키 배포에 문제가 있다. 전자여권의 PA를 검증하기 위해 사용되는 발행국의 인증서는 국가간의 별도방식에 의해 교환되거나 PKD를 통해 공개되어야 한다. 만약 보안 표준을 낮게 적용한 국가의 개인키가 유출되는 경우 적법하게 위조되는 전자여권을 발행할 수 있는 문제점을 가지고 있다.
- EAC 보안취약점 : EAC는 BAC가 실행된 이후에 민감한 개인정보를 보호하기 위해 제안되는 프로토콜이다. 그러나 BAC 프로토콜이 수행된 이후에 SOD 파일은 판독기에 획득이 된다. SOD 파일에는 지문이미지의 해쉬값을 포함하고 있기 때문에 기존의 지문이미지에 대한 해쉬값을 가지고 있는 경우 무차별공격을 통해 지문정보의 획득이 가능하게 된다.

2.6.2 전자여권 바이오인식의 보안취약점

- 바이오인식률 : 전자여권에 저장된 사진, 지문 정보는 출입국 과정에서 본인임을 증명하기 위한 바이오인식으로 사용된다. 최근 바이오인식 기술이 발전이 되었으나 지문인식의 경우 지문이 획득되지 않거나 지문이 훼손된 사용자는 바이오인식 수행하지 못하게 된다. 지문과 얼굴인식은 오인식률과 본인거부율을 가지고 있는 한계가 있다. 특히 얼굴인식의 경우는 기타 바이오인식에 비해 성능이 현저히 낮기 때문에 전자여권 판독에 있어서는 출입국 담당자의 육안확인을 기본으로 하고 있다.
- 바이오정보 등록 : 전자여권을 발급하기 위해서 얼굴과 지문정보를 등록해야 한다. 바이오정보의 품질은 향후 바이오인식을 수행할 때 인식률에 성능을 끼치기 때문에 바이오인식에서 사용할 수 있는 고품질의 이미지를 검출해야 한다. 낮은 품질의 이미지가 등록된 경우 오인식률이나 오거부가 발생하여 소지자의 신원확인에 보안문제가 발생한다. 또한 등록된 바이오정보는 전자여권에 발급되기 위해서 일정기간 저장소에 이미지를 저장하는데 통신 또는 저장소의 바이오정보가 변경되는 문제가 발생할 수 있다. 기존의 암호화 통신은 바이오정보 자체에 보안기능을 제공할 수 없는 한계가 있다.
- 바이오인식의 자동화 : 출입국 속도를 개선하고 전자여권 소지자의 편의성을 제공하기 위해 무인 출입국 시스템이 도입되고 있다. 무인 출입국 시스템은 바이오인식이 자동화로 수행되기 때문에 출입국 담당자의 감독없이 수행됨으로 높은 수준의 바이오인식에 대한 검증이 요구된다. 지문이 탑재된 전자여권의 경우 동일한 지문을 제시하면 자동으로 출입국이 가능하다. 따라서 전자여권내의 바이오정보에 대한 원본임을 입증하기 위한 강화된 보안이 요구된다[8].

III. 바이오정보 워터마킹을 이용한 전자여권 보안기술

3.1 전자여권 시스템의 바이오정보 관리의 문제점

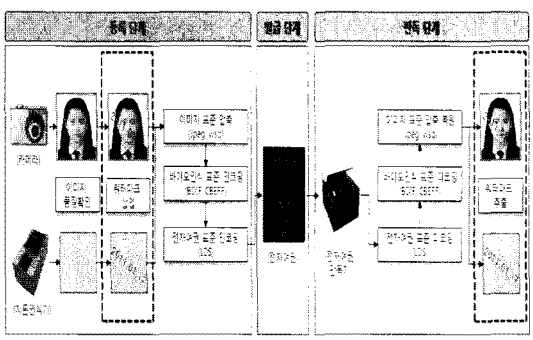
전자여권의 소지자를 확인하기 위해 저장된 사진, 지문정보는 가장 민감한 개인정보이기 때문에 ICAO는 강화된 전자여권 보안 프로토콜인 BAC와 EAC를 제안하였다. 판독기에서 사진정보에 대한 접근제어 방식인 BAC는 암호학적 복잡도가 낮은 한계를 가지고 있으며 지문정보에 대한 접근제어 방식은 EAC는 발

행국과 출입국 시스템간의 키관리에 대한 문제점을 가지고 있다. 전자여권에서 사용되는 바이오정보는 전자여권 발급과 무인 출입국 시스템에서 소지자의 신원확인을 위해 바이오인식을 수행하는 보안상 중요한 정보이다. 즉 바이오정보가 등록에서 출입국에서 사용되는 전단계에 걸쳐서 사진, 지문의 원본정보와 변조되지 않았음을 증명하기 위해 강화된 보안 프로토콜이 요구된다. ICAO가 제안한 PA 방식은 사진, 지문정보의 해쉬값에 전자서명을 이용하여 무결성을 보장하지만 바이오정보의 등록과정에서의 증명성을 보장하지 않는다. 따라서 본 제안에서는 바이오정보를 취득하는 시점에 워터마크를 원본에 삽입하고 출입국 시스템에서 바이오정보 원본의 워터마크를 추출함으로써 보다 강화된 바이오정보 보호 기능을 제공한다.

3.2 전자여권용 워터마킹 보안기능

본 논문에서 제안하는 워터마킹 기술은 얼굴과 지문 이미지를 대상으로 한다. 제안하는 전자여권용 바이오정보 워터마킹은 전자여권 등록과 판독하는 단계에서 [그림 2]와 같은 절차를 따른다. 얼굴정보는 전자여권 신청자로 부터 사진을 제출 받아 디지털스캐너를 통해 영상으로 획득되며 지문정보는 지문센서를 이용해 획득된다. 획득된 바이오정보는 등록일자를 워터마크 정보로 바이오정보 삽입된 후 압축 및 저장된다. 전자여권의 표준 바이오정보 압축 포맷에 따라서 얼굴영상은 JPEG와 지문은 WSQ 포맷으로 압축한다.

압축된 바이오정보는 바이오정보 DB로 전송되어 저장된다. 저장된 바이오정보는 전자여권 발급을 위한 통신하는 과정에서 원본영상 자체의 위변조를 검출하는데 사용된다. 동일한 방식으로 전자여권 칩에 저장된 사진영상 및 지문영상을 판독할 때 워터마크를 검출하여 무결성을 검증할 수 있다. 제안하는 전자여권



[그림 2] 전자여권의 바이오인식 워터마킹 처리절차

용 워터마킹은 다음과 같은 기술요구사항이 필요하다.

- 영상품질(Image Quality) : 바이오정보에 대한 워터마크 신호는 일종의 잡음으로 분류된다. 따라서 워터마크가 삽입된 바이오이미지는 영상품질이 왜곡된다. 일반적으로 사람의 눈으로 인지할 수 없는 정도의 워터마크를 삽입하게 되며 평가방법은 PSNR(Peak Signal-to-Noise Ratio)를 사용하며 워터마크 삽입 후 38dB 이상이면 품질을 만족한다고 판단한다. 제안방식은 전자여권 표준인 JPEG과 WSQ의 압축표준을 준수해야 하기 때문에 일반적인 기준보다 영상의 품질을 손상시키게 된다.
- 강인성(Robustness) : 강인성은 워터마크가 삽입된 바이오정보가 노이즈 환경에 노출 된 후 워터마크가 검출될 확률이며 Detection rate이라고도 한다. 전자여권 시스템에서 요구되는 워터마크의 강인성은 압축에 대한 강인성이다. 얼굴이나 지문에 사용되는 압축방법인 JPEG, WSQ는 손실압축(Lossy compression)이기 때문에 그 자체가 삽입된 워터마크를 제거하려는 시도가 된다. 제안하는 워터마크는 시나리오에서 요구하는 압축비(compression ratio)에 강인하도록 설계되어야 한다.
- 삽입량(Payload) : 삽입량은 얼굴이나 지문영상 대비 워터마크 정보량을 수용할 수 있는가를 나타내다. 제안하는 전자여권 시스템에서는 영상이 획득일자를 워터마크로 삽입한다.
- 검출률(False Negative Alarm) : 검출률은 삽입된 워터마크에 대해 정확히 검출히 가능한지를 나타내는 비율로 워터마크를 삽입한 총 영상에 대해 검출이 성공한 영상의 수를 백분율로 나타낸 것이다. 전자여권 시스템은 가장 높은 보안수준이 요구되기 때문에 100% 검출률을 지원해야 한다.
- 오검출률(False Positive Alarm) : 오검출률은 워터마크가 삽입되지 않은 영상에 대해 워터마크가 있다고 판별할 확률이다. 위,변조 된 바이오정보를 제대로 검출하기 위해서는 오검출률이 0.01% 이하로 매우 낮아야 한다.
- 제약사항(Restriction) : 제약사항은 전자여권 표준과 칩의 저장용량에 적합하도록 얼굴영상은 240x320 크기, 컬러, 24비트, JPEG압축, 용량 15KB 이하이고 지문영상의 포맷은 400x450 크기, 흑백, 8비트, WSQ압축, 용량 15KB 이하로

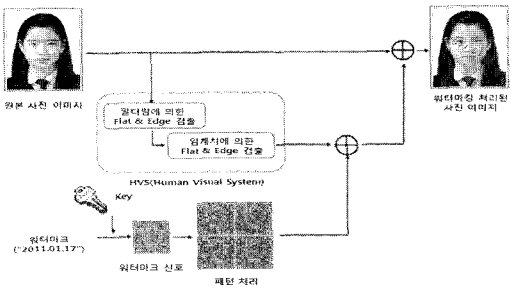
한정한다. 워터마크 삽입 후의 영상의 크기는 얼굴, 지문은 15KB 이하로 유지되어야 하며 이에 따른 평균 압축비는 각각 15:1(226K/15K), 11.8:1(177K/15K)이다. 강인성은 압축만 고려한다. 워터마킹 삽입 모듈은 워터마크를 삽입한 후 15Kbyte 이하로 압축한 후 저장해야 한다.

3.3 전자여권용 워터마크 삽입

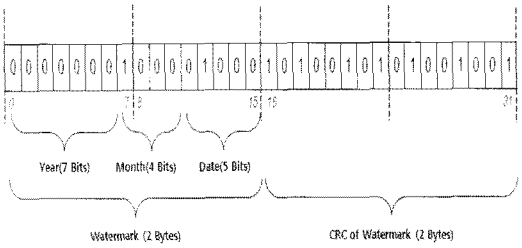
제안하는 전자여권용 워터마킹 보안기능은 지문, 얼굴 이미지를 획득한 이후, 품질확인을 거쳐서 보정불가인 바이오정보는 재획득하며 보정이 가능한 이미지는 보정작업을 수행하여 품질이 확보된 바이오이미지를 획득한다. [그림 3]과 같이 품질이 확보된 지문, 얼굴이미지에 소유기관을 명시하기 위해 워터마킹을 수행하고 지문은 WSQ로 얼굴은 JPEG로 압축을 수행한다.

워터마킹 시스템은 삽입 모듈과 추출 모듈로 구성된다. 삽입모듈에 대한 블록 다이어그램이 [그림 4]에 나타나 있다. 삽입과정은 크게 이미지의 휘도(Luminance)부분을 취하는 부분과 이미지의 육안 인지 시스템(Human Visual System)를 계산하는 부분, 일자 형태의 워터마크를 휘도 영역에 삽입 가능한 랜덤시퀀스(Random Sequence)신호로 바꿔주는 메시지 변환(Message Modulation) 부분으로 구성된다. 메시지 변환에 사용되는 키(Key)는 유일한 랜덤시퀀스를 발생시켜주도록 하는 시드(Seed)이며 추출시에도 사용된다. 워터마크 신호가 같더라도 시드값이 다르면 실제 다른 워터마크가 삽입된다. 키에 의해 생성된 랜덤시퀀스는 단위블록 형태가 되고 이 블록이 영상의 크기에 맞게 반복되어 삽입된다. 400x450의 얼굴 영상의 경우 워터마크 신호에 대한 단위블록의

[그림 3] 전자여권의 바이오인식 품질 확인



[그림 4] 바이오인식 워터마크 삽입



[그림 5] 워터마크 정보

크기는 120x160이며 이 블록이 4번 반복 삽입된다. 지문영상의 경우 같은 원리로 단위블록의 크기는 200x225이다. HVS함수는 워터마크가 삽입된 영상의 품질과 동시에 강인성을 결정하는 중요한 부분으로 랜덤시퀀스 형태의 워터마크 신호를 이미지의 특성을 고려하여 스케일링하는 역할을 한다.

3.3.1 워터마크 정보

[그림 5]와 같이 전자여권용 워터마킹에서는 일자정보를 입력으로 4bytes 워터마크를 생성한다. 획득일자 정보는 매핑테이블을 이용하여 2byte로 재배치된다. 나머지 2byte는 2byte의 획득일자 워터마크에 대한 무결성 검증을 위한 16bits CRC 값이다.

3.3.2 메시지 변환(Message Modulation)

생성된 4bytes 워터마크는 바이오이미지에 잡음의 형태로 삽입하게 되는데 복잡도를 증가시키기 위하여 랜덤시퀀스로 변환하게 된다. 메시지 변환은 랜덤값으로 4byte 워터마크 신호를 단위블록 크기의 2차원 랜덤시퀀스로 바꾸어 준다. 각각의 시퀀스는 주어진 키에 의해 4개의 서브키가 만들어지고 각각의 서브키로부터 단위블록 길이로 생성된다. 다음으로 생성된 랜

덤시퀀스는 각 byte의 값에 따라 환형 쉬프트한다. 각 바이트의 표현 범위가 0부터 255까지이므로 단위 블록 길이의 2차원 랜덤시퀀스는 16x16의 서브블록으로 논리적 분할이 이루어진다. 그 후 해당 서브블록의 위치로 시퀀스가 환형 쉬프트 된다. 바이트의 값이 블록의 위치로 표현되는 것이다. 이렇게 표현된 4장의 2차원 랜덤시퀀스는 최종적으로 합해져 그 사인(sign)값이 다시 취해진다. 최종적으로 4개의 신호를 포함한 1개의 2차원 랜덤시퀀스가 생성된다.

3.3.3 육안 인지 시스템(HVS : Human Visual System)

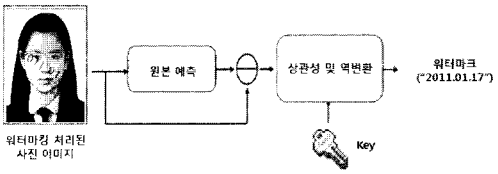
HVS는 워터마크를 삽입하는 강인성을 유지하면서 삽입하면서 비가성(im-perceptibility)을 유지하는 기술이다. 바이오이미지의 품질만을 우선시 한다면 이미지 전반에 약하게 삽입하는 방법이 사용되지만 왜곡에 대한 강인성을 고려한다면 사람이 인지하지 못하는 범위내에서 최대한 강하게 삽입해야 한다. HVS는 이미지의 어느 부분에 강하게 삽입해야 할지를 식별하는 함수이다. 사람이 인지할 수 있는 변화량은 주변픽셀에 따라 다르다는 법칙으로 주변픽셀에 따라는 삽입강도를 다르게 조절할 수 있다. 제안하는 전자여권용 워터마킹 보안기능에서는 바이오이미지의 주변값들 통계적 계산치인 주변값과의 표준편차를 주로 이용한다. 주변 픽셀과의 편차가 작은 평면(flat) 영역에는 편차값에 비례하여 약한 워터마크 삽입을 하고 반면 편차값이 큰 edge 또는 texture영역에는 강한 워터마크가 삽입된다.

3.3.4 키 정의

랜덤시퀀스를 발생시키는 키(Key)는 램덤 넘버 생성기의 입력으로 시드(Seed) 넘버로 이용된다. 시드는 32bits로 그 범위는 0 부터 4,294,967,295 까지이다. 삽입 시 사용했던 키를 추출 시에 같이 사용해야만 추출이 가능하다. 기본적으로 워터마크 입력이 같더라도 할당된 키가 다르면 다른 정보가 워터마크로 삽입된다.

3.4 전자여권용 워터마크 추출

[그림 6]은 전자여권에 삽입된 워터마크를 추출하는 과정을 설명한다. 본 기술은 원본 없이 워터마킹된 이미지에서 바로 추출할 수 있는 기술을 제공하며



[그림 6] 바이오인식 워터마크 추출

추출 과정은 크게 원본예측 과정과 메시지 역 변환의 2가지 요소기술로 구분할 수 있다.

3.4.1 원본예측(Original Estimation)

원본예측기술은 노이즈와 같은 워터마크 신호를 이미지에서 분리하는 기술로 일반적으로 노이즈 제거 필터를 사용한다. 노이즈 제거 필터에 의해 제거된 노이즈에는 삽입한 핑거프린트 신호가 많이 포함되어 있다고 가정한다. 본 기술에서는 적응 위너(Adaptive Wiener) 필터를 사용하였다. 위너필터는 입력을 원하는 출력과 가능한 한 매우 근사하게 변환시켜주는 필터로써, 필터 출력과 원하는 결과의 차의 제곱의 합이 최소가 된다는 의미이다. 영상에서 e(x,y)가 최소가 되는 h(x,y)를 위너 필터를 이용하여 노이즈를 제거한다.

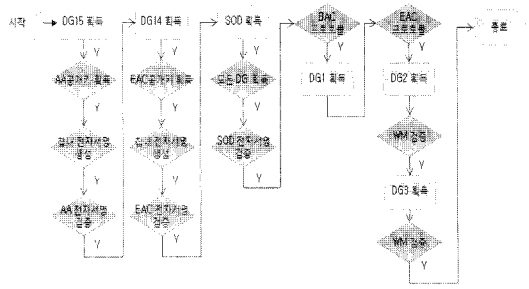
3.4.2 상호상관도와 메시지 역변환

상호상관도(Cross Correlation)는 두 신호간의 유사한 정도를 추정하는 표준 방법이다. 제안한 워터마킹 알고리즘에서는 상호상관계수를 구한 다음 계수들에서 최고값의 위치를 추출된 워터마크로 추출한다. 삽입 시 워터마크의 값에 따라 환상쉬프트가 이루어진 2차원 랜덤시퀀스는 환상쉬프트가 이루어지지 않은 시퀀스와 상호상관계수를 구할 경우 그 피크의 위치가 쉬프트한 서브블록의 위치가 된다. 따라서 피크가 나타난 서브블록의 인덱스가 워터마크 신호이다. 이렇게 4byte를 모두 추출한 후 처음 2 바이트의 16bits CRC를 계산한다. 계산한 CRC 값은 뒤의 2byte와 일치했을 경우에만 최종적으로 워터마크가 추출한다.

IV. 실험

본 제안의 실험을 위해서 국내 전자여권과 동일한 보안기능을 대상으로 실험을 수행하였다. 실험에서는 제안하는 워터마크가 삽입된 전자여권을 대상으로 판

〔그림 7〕 전자여권 보안기능 판독 테스트



〔그림 8〕 전자여권 판독 흐름도

독에 대한 실험을 수행하다. 판독에 사용된 노트북은 윈도우 XP, CPU 2.5 GHz, RAM 4G, HDD 300G 이며, 전자여권 판독기는 24 Bits 스캔이 가능한 국내 제품으로 테스트 하였다. 〔그림 7〕은 전자여권 보안기능의 판독과정을 나타낸다.

〔그림 8〕은 전자여권 판독과정의 전체 흐름도를 나타낸다.

전자여권 기본적인 보안기능 외에 제안하는 워터마크를 추출하는 과정을 수행하였으며 〔표 2〕에 결과를 나타내었다. 국내 전자여권의 바이오정보의 크기는 15K 미만으로 제한되어 있고, 판독과 워터마크를 추출하는 과정을 포함한 결과를 나타낸다.

본 제안방식이 6초가 소요되는 문제는 얼굴영상 JPEG 압축복원, 지문영상 WSQ 압축복원후 워터마크 검증하기 때문에 속도가 상대적으로 증가하였다. 실제 전자여권 판독시에는 심사자가 얼굴, 지문의 압축복원을 통해 확인하는 작업이 있으므로 실제 워터마킹으로 소요되는 시간은 2~3초 이내이다.

기존의 전자여권 보안기능은 전자여권과 판독기의 진위여부, 통신구간 암호화, 칩 복제 방지를 중점으로 채택되었으며 가장 민감한 정보인 바이오정보의 복제를 원천적으로 차단하기 어려웠다. 〔표 3〕과 같이 제안하는 바이오정보 워터마킹을 적용하는 경우, 바이오정보 자체에 워터마크를 삽입함으로써 기존의 PA, AA, BAC, EAC가 제공하지 못하는 바이오정보 복제 방지가 가능하다.

〔표 3〕 전자여권 보안기능 비교

보안기능 \ 보안 프로토콜	PA	AA	BAC	EAC	WM
데이터 변조 방지	◆				
칩 복제 방지		◆		◆	
판독기 접근제어			◆	◆	
통신구간 암호화			◆	◆	
바이오정보 복제 방지					◆

제안하는 전자여권 워터마킹 기술은 전자여권내 주요 바이오정보인 지문과 얼굴에 사람이 인지할 수 없는 워터마크를 삽입하고 판독할 때 워터마크를 추출하는 단계를 통해 바이오정보의 복제를 방지한다. 바이오정보가 등록과 데이터베이스에 저장하는 동안 발생할 수 있는 바이오정보의 변경 가능성을 미연에 방지함으로써 전자여권의 보안강도를 높이는 결과를 보인다. 실험결과에서는 바이오정보에서 워터마크를 추출하는 과정에 기존보다 시간 소요가 되는데 이 부분은 바이오정보 압축해제와 워터마킹 검증을 동시에 수행하기 때문에 시간 소요가 발생하였다.

〔표 2〕 전자여권 보안기능 판독결과

단계	데이터 그룹	데이터 내용	알고리즘	데이터 크기	판독 시간
①	F.COM	헤더 파일		25 Bytes	0.03 s
②	DG15	AA 공개키	RSA	298 Bytes	0.05 s
③	DG14	EAC 공개키	ECC	480 Bytes	0.08 s
④	EF.SOD	PA 전자서명	RSA	1,863 Bytes	0.23 s
⑤	DG1	MRZ 정보	BAC	93 Bytes	0.03 s
⑥	DG2	얼굴(워터마크)	Watermarking	12,865 Bytes	3.53 s
⑦	DG3	지문(워터마크)	Watermarking	11,415 Bytes	3.36 s
총수행 결과				27,039 Bytes	7.31 s

V. 결 론

국제적으로 전자여권 도입에 따라서 전자여권의 표준과 함께 보안기술에 대한 연구가 활발하게 진행되고 있다. 전자여권은 스마트카드, 공개키 기반 암호화, 바이오인식 등 최신의 보안기술의 융합되어 전자여권의 위조, 복제 방지를 위해 사용되고 있다. 전자여권에 저장되는 바이오정보는 개인의 가장 민감한 정보이며 위조, 복제 되었을 때 가장 큰 피해가 예상되지만 현재의 전자여권 표준은 바이오정보의 복제 여부를 검증하는 보안기능은 제공되지 않고 있다.

본 논문에서는 전자여권내의 바이오정보 복제를 방지하기 위해 바이오정보 워터마킹을 이용한 전자여권 보안기술을 제안하였다. 제안하는 바이오정보 워터마킹은 전자여권의 발급하는 과정에서 획득일자을 육안으로 인지하지 못하게 삽입하고 전자여권의 판독하는 과정에서 워터마크를 추출함으로써 바이오정보의 복제 여부를 검출한다. 본 논문은 국내 전자여권을 대상으로 워터마크 발급 및 판독을 통해 실험결과를 제시하였으며 바이오정보의 보호를 위한 표준으로 활용이 가능할 것으로 기대한다.

참고문헌

[1] Ari Juels, David Molnar, and David Wagner, "Security and Privacy Issues in E-passports," Security and Privacy for Emerging Areas in Communications Networks, pp. 74-88, Mar. 2005.

[2] Y. Liu, T. Kasper, K. Lemke-Rust, and C. Paar, "E-Passport: Cracking Basic Access Control Keys," Proceedings of OTM Conferences, pp. 1531-1547, 2007.

[3] D. Lekkas and D. Gritzalis, "e-Passports as a means towards the first world-wide Public Key Infrastructure," In Proceedings of EuroPKI, pp. 34-48, 2007.

[4] Marci Meingast, Jennifer King and Deirdre K. Mulligan, "Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond," JCM, pp. 36-48, 2007.

[5] Serge Vaudenay, "E-Passport Threats," IEEE Security & Privacy. pp .61-64, 2007.

[6] J. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R.W. Schreur, "Crossing Borders: Security and Privacy Issues of the European e-Passport," In Proceedings of CoRR, 2008.

[7] V. Pasupathinathan, J. Pieprzyk, and H. Wang, "An On-Line Secure E-Passport Protocol," in Proceedings of ISPEC, pp. 14-28, 2008.

[8] B.A.M. Schouten and B. Jacobs, "Biometrics and their use in e-passports," Proceedings of Image Vision Comput., pp. 305-312, 2009.

[9] T. Chothia and V. Smirnov, "A Traceability Attack against e-Passports," In Proceedings of Financial Cryptography, pp .20-34, 2010.

[10] V. Auletta, C. Blundo, A.D. Caro, E.D. Cristofaro, G. Persiano, and I. Visconti, "Increasing Privacy Threats in the Cyberspace: The Case of Italian E-Passports," In Proceedings of Financial Cryptography Workshops, pp. 94-104, 2010.

〈著者紹介〉

이 용 준 (Yong-joon Lee) 정회원
2001년 ~ 2005년: 숭실대학교 컴퓨터학과 공학박사
2005년 ~ 2006년: 현대정보기술 바이오솔루션팀 과장
2007년 ~ 2009년: LG CNS 기술연구부문 부책임연구원
2010년 ~ 현재: 한국인터넷진흥원 인터넷침해대응센터 책임연구원
〈관심분야〉 인터넷침해대응, 전자신분증, 바이오인식, 공인인증