Proceedings of KFIS Spring Conference 2006 Vol. 16, No. 1.

암호이론을 이용한 다중생체데이터 전송상의 보안

Security Method on the Multi-modal Biometrics Data

고현주, 유병진, 김용민, 전명근

충북 청주시 충북대학교 전기전자컴퓨터공학부
E-mail: mgchun@chungbuk.ac.kr

요 약

생체인식은 정보처리시스템에 있어서 네트웍 보안, 시스템 보안, 어플리케이션 보안 등에 사용되는 개인인증 및 확인을 위한 하나의 기법으로 볼 수 있으며, 개인정보를 포함한 데이터의 보호를 위해서 본인이나 승인된 사용자만이 네트웍이나 물리적 접근 등을 통하여 접근하고자 하는 것이다. 본 논문에서는 얼굴인식과 홍채인식 시스템을 융합한 다중생체인식 시스템을 구현하였으며, 다중생체인식 시스템에서 구현된 생체데이터를 안전하게 전송할 수 있는 방법으로 블록 암호 알고리듬 ARIA를 침입에 대한 보안 방법으로 제안하였다. 이에 다중생체 특징벡터를 128비트의 블록 크기를 이용하여 암호화 하였으며, 생체 특징벡터를 이용하여 128비트의 키로 사용하였다.

Key Words : 다중생체인식, 전송 보안, 블록암호 알고리듬, ARIA

1. 서 론

정보통신 시스템과 네트워크가 개방되고, 용량과 성능, 연결성이 강화되는 추세에 인가 받지 않은 불법 사용자로 인한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통 등과 같은 정보화의 역기능이 증가할 것으로 예견되고 있다. 생체인식이란 넓은 의미에서 볼 때, 정보처리시스템에 있어서 네트웍 보안, 시스템 보안, 어플리케이션 보안 등에 사용되는 개인인증 및 확인을 위한 하나의 기법으로 볼 수 있으며, 개인정보를 포함한 데이터의 보호를 위해서 본인이나 승인된 사용자만이 네트웍이나 물리적 접근 등을 통하여 접근하고자 하는 것이다.

다중생체인식시스템의 구현방법은 동일한 생체특징에 대하여 서로 다른 특성을 갖는 다수의 센서로 측정하여 인식하는 방법인 다중센서, 인식 알고리듬의 최종 단계에 해당되는 매칭 과정에 서로 다른 알고리즘을 쓰는 경우인 다중매칭, 인식대상이 되는 생체특징을 다수의 대상으로부터 취득하여 인식하는 경우인 다중유니트, 동인한 생체인식 대상을 여러번 취득하여 인식하는 경우인 다중입력, 여러 개의 생체인식기법을 동시에 쓰는 것으로 다중생체특징을 들 수 있다[1].

생체인식의 적용분야는 크게 세가지 범주로 나눌 수 있다. 첫째는, 논리적 접근 통제로 컴퓨터나 컴퓨터의 네트웍을 통하여 데이터베이스나 컴퓨터의 자원의 접근을 통제하는 영역이며, 둘째는, 물리적 접근 통제로 출입이 통제되는 시설의 출입을 제어하기 위한 목적의 응용분야이다. 셋째는 신용적 접근 통제로 전자 상거래 등을 통한 금전적 거래의 개인 확인 분야를 들 수 있다.

한편, 합법적으로 취득된 생체정보에 대해서 이들이 중앙저장장치나 국부적 저장장치에 저장 되어있을 경우에 네트웍을 통한 불법 침입이나 인가 받지 않은 사용자로 인하여 이러한 데이터들이 불법으로 사용될 수 있다. 그림 1은 생체인식시스템의 구현 과정을 나타내고 있다[2].

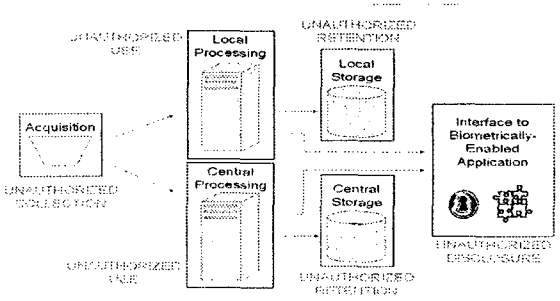


그림 1. 생체인식 시스템 구현 과정

생체데이터의 처리를 담당하는 중앙 처리부나 로컬 처리부에 있어서도 불법사용자에 의한 의도하지 않은 사용이나 당초의 목적 범위를 넘어서는 응용을 시도할 수 있으며, 시스템의 마지막 부분에 있으면서 생체정보에 기반 한 응용과의 인터페이스를 담당하는 부분에 있어서도 생체정보가 부당하게 공개 될 수 있는 위험이 있다.

정보의 수집, 처리, 저장, 검색, 송수신 과정에서 그 정보가 훼손, 변조되거나 불법적으로 유출되는 것을 방지하고, 정보처리 시스템 내에 저장되거나 통신망을 통하여 송수신되는 정보를 각종 위험으로부터 보호하여 시스템의 가용성을 보장하기 위한 많은 정보보호 서비스들은 암호알고리즘을 바탕으로 구현된다. 이에 본 연구에서는 다중생체인식 시스템에서 구현된 생체데이터를 안전하게 전송할 수 있는 방법으로 블록 암호 알고리듬 ARIA를 사용하고자 한다. 블록 암호 알고리듬 ARIA는 128비트 데이터 블록을 처리하는 알고리즘으로 128, 192, 256 비트 암호키로 사용될 수 있으며 요구되는 안전성 기준에 따라 용도가 구분될 수 있다. 또한, 암호키의 길이에 따라 ARIA-128, ARIA-192, ARIA-256으로 구분하여 표기한다.

본 논문의 구성은 1장의 서론과 2장의 얼굴과 홍채를 이용한 다중생체인식 시스템에 대하여 논하고, 3장에서는 암호이론을 이용한 다중생체 데이터 보안에 대하여 설명한다. 마지막으로 4장에서는 결론을 맺는다.

2. 얼굴과 홍채를 이용한 다중생체인식 시스템 구현

단일 생체인식 방법 중 얼굴인식 시스템은 이미 잘 알려져 있는 PCA, ICA LDA 방법을 이용할 수 있다. 이는 얼굴인식의 다양한 방법들로 입력 벡터가 한 클래스에 할당되어질 때 그 클래스에서 소속의 정도를 0 또는 1로서 나타낸다. 따라서 이러한 방법들은 얼굴영상들이 조명이나 보는 각도로 인해 변형이 생기는 경우에 인식률이 저하되는 문제가 있다. 따라서 주성분 분석 기법에 의해 변환된 특징벡터에 퍼지 소속도를 할당하여 이를 개선하고자 한다.

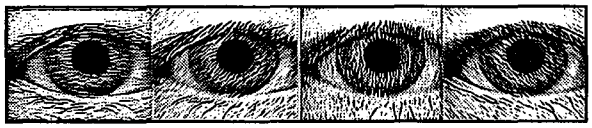
주성분 분석기법에 의해 변환된 특징벡터의 집합 $X=(x_1, x_2, \cdots, x_N)$이 주어질 때 이 벡터들의 퍼지분할 행렬은 c 클래스에서 각 벡터의 소속도로서 특성화되며, $c \times N$의 행렬 U로 표현한다. 여기서 $\mu_{ij}=\mu_i(x_j)$, $i=1,2,\cdots,c$, $j=1,2,\cdots,N$는 클래스 i에서 x_j의 소속도이다. 퍼지 분할 행렬 U는 다음과 같은 식들을 만족해야 한다. c 클래스에서 특징 벡터의 퍼지 소속도의 합은 항상 1이어야한다[3].

$$\sum_{i=1}^{c}\mu_{ij}=1 \tag{1}$$

$$0<\sum_{j=1}^{N}\mu_{ij}<N \tag{2}$$

$$\mu_{ij}\in[0,1] \tag{3}$$

한편, 홍채인식은 가버 웨이블릿을 이용하여 방향성 및 주파수 선택의 특징을 갖는 밴드패스 필터로 공간주파수 영역에서 최적의 집합 분석력을 갖고 있다. 그림 2는 가버 웨이블릿을 사용한 후의 홍채영상을 나타낸 것으로, 본 연구에서는 4개의 방향(0도, 45도, 90도, 135도)의 가버 웨이블릿을 사용하였다.



(a) 0도 (b) 45도 (c) 90도 (d) 135도

그림 2. 가버 웨이블릿 변환 후의 영상

홍채패턴에서의 특징을 찾아내기 위한 방법으로 동공의 바깥쪽 경계선과 홍채 패턴이 몰려있는 부분의 바깥쪽 경계선을 이용하여 도넛 모양을 그려낼 수 있는데, 동공의 크기에 따라 변화하는 홍채의 패턴이 많이 몰려 있는 부분을 검출하였다.

일반적으로 홍채영상은 매우 고차원의 패턴으로 표현되기 때문에 특징 추출과 분류를 위해서는 저차원의 데이터로 표현되는 것이 요구된다. 선형판별분석기법은 클래스 내의 분산을 나타내는 행렬과 클래스 간 분산을 나타내는 행렬의 비율이 최대가 되도록 하는 선형 변환 방법으로, 주성분 분석기법은 영상 공간에서 저차원의 특징 공간으로의 선형 사영을 기초로 하므로 전체 데이터베이스의 모든 홍채 영상을 최대화하는 사영 방향을 찾아낸다. 본 연구에서는 입력홍채영상에 대하여 주성분 분석기법을 적용하여 저차원으로 축소한 후 퍼지 선형 판별 분석 기법을 이용하여 특징벡터를 획득하는 방법을 사용하였다[4].

얼굴과 홍채를 이용한 다중생체인식기법은 단일생체인식기법으로부터 얻은 각각의 특징값으로부터 균등화 과정을 거쳐 융합 하는 것으로, 저장하고 있는 템플릿(학습데이터에 의한 템플릿)과의 매칭값을 통해 수용/거부의 여부를 결정하는 방법이다. 이때, 융합하는 시점에 따라, 특징추출 단계에서의 융합하는 방법이 있을 수 있고, 각각 단일 생체인식 시스템에서 얻어진 매칭값을 융합함으로서 수용/거부의 여부를 결정하는 방법이 있을 수 있으며, 융합후

의 과정에서 수용/거부의 결과를 결정하는 방법이 있을 수 있다. 본 논문에서 제안한 다중생체인식 시스템은 두 번째로 언급한 방법으로 단일 생체인식 시스템의 매칭값을 균등화 과정을 거친 후 가중치 합(Weight sum rule) 방식을 적용하여 최종 결과를 얻는 시스템으로 구현하였다.

가중치합 방식은 두 개 이상의 데이터 값 융합에 일반적으로 쓰이는 방식으로, 두가지의 데이터 중 신뢰성이 높은 데이터에 높은 가중치를 주고 신뢰성이 낮은 경우에도 버리지 않고 낮은 수준의 가중치를 줌으로써 신뢰도만큼의 역할을 할 수 있도록 하는 방식이다. 이러한 가중치 합은 다음과 같은 식 (4)으로 나타낼 수 있다.

$$f=\sum_{i=1}^{N_E} w_i o_i \qquad (4)$$

여기서, o_i는 각 데이터의 출력값이고, w_i는 각 데이터의 신뢰도를 나타낸다. 이와 같이 융합된 결과 값들 중 일정한 임계값(threshold)을 기준으로 허용/거절(Acess/Reject)을 판단하게 된다. 그림 3은 정규화 과정을 포함한 다중생체인식 시스템의 처리과정을 보이고 있다.

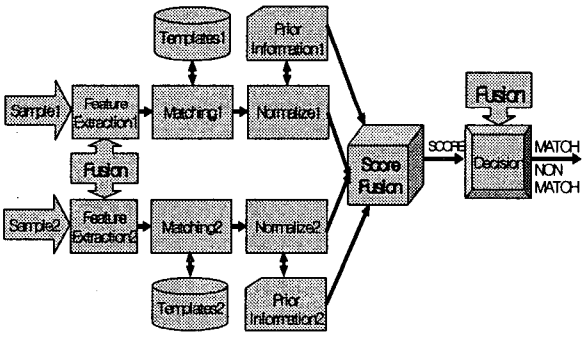


그림 3 정규화 과정을 포함한 다중 생체 인식 시스템의 처리 과정

본 논문에서는 다중생체 데이터를 전송하기 위해 특징벡터를 암호화 하는 방법에 대하여 두 가지를 제안하고자 한다. 첫 번째는, 입력 얼굴영상에 대하여 홍채의 특징벡터를 숨기는 스테가노그라피(Steganography) 영상을 만들어, 블록암호 알고리듬 ARIA를 이용하여 전송하는 방법에 대하여 연구하였다. 이를 위한 방법으로는 입력 얼굴영상에 대하여 이산웨이블렛 변환 계수를 이용하였으며, 홍채영상에 대하여는 앞에서 설명된 방법과 같이 Fuzzy-LDA를 이용한 특징벡터를 사용하였다. 또한 스테가노그라피 영상을 암호화하여 전송하기 위해 사용된 키는 홍채영상에 PCA를 이용하여 얻은 특징벡터를 사용하였다. 이와 같은 방법을 그림 4에 나타내었다.

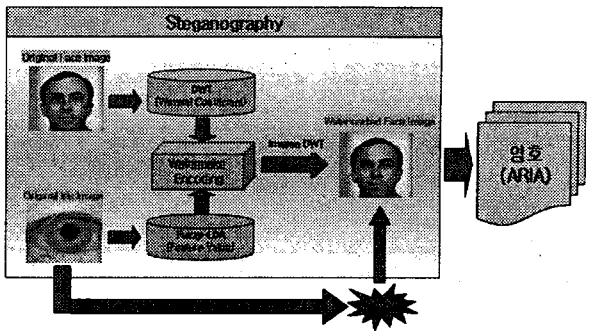


그림 4. 스테가노그라피를 이용한 다중생체데이터 전송 과정

두 번째는, 특징벡터를 획득하는 방법으로 앞장에서 설명된 방법과 같이 얼굴영상에 대하여 획득된 특징벡터와 홍채영상에 대하여 획득된 특징벡터를 1차원의 벡터로 연결한 후 이를 이산퓨리에 변환을 거쳐 계수의 크기와 위상을 획득하였다. 이때 크기성분인 계수 값을 암호화하기 위해 위상 값을 키로 사용하여 블록암호 알고리듬 ARIA로 암호화 하였다. 이와 같은 방법을 그림 5에 나타내었다.

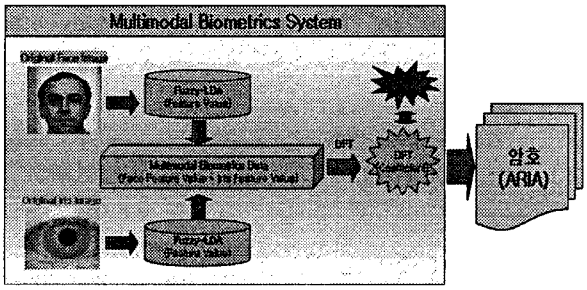


그림 5. 이산퓨리에 변환을 이용한 다중생체 특징벡터 전송 과정

3. 암호이론을 이용한 다중생체 데이터 보안

암호시스템을 이용한 인증은 정보보안의 중요한 역할을 하고 있으며, 인터넷상에서 행해지는 전자상거래에 있어서 이러한 보안 문제의 해결을 위해서는 암호기술을 이용한 인증이 매우 중요한 역할을 담당하고 있다. 아리아(ARIA)는 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안기술연구소(NSRI) 주도로 학계, 국가정보원 등의 암호기술 전문가들이 힘을 모아 개발한 국가 암호화 알고리즘이다. 또한, 민간 암호화 알고리즘 시드(SEED)와 함께 전자정부의 대국민행정서비스용으로 보급되고 있으며, 스마트카드 등의 초경량 환경 및 고성능 서버 환경 등에서 시드에 비하여 상대적인 장점을 가지고 있다. 국내 학계 및 산업계의 구현 결과에서 초경량 환경과 고성능 서버 환경에서는

아리아가 미국 암호화 알고리즘인 AES와 어깨를 나란히 할 수 있음이 밝혀졌으며, Pentium IV PC에서는 일본의 암호화 알고리즘인 카멜리아(Camellia)와 민간 암호화 알고리즘인 시드(SEED)보다 약 2배의 성능을 가짐이 AES를 개발한 벨기에 루벤 대학의 검증을 통하여 밝혀졌다. KS 표준은 국가의 대표 규격을 의미하므로, 아리아(ARIA)의 KS 표준 제정은 미국, 유럽, 일본의 암호화 알고리즘과 어깨를 나란히 할 수 있는 성능을 가진 아리아(ARIA)를 국가의 대표 알고리즘으로 승인함으로써 세계 최고의 네트워크 인프라를 가지고 있는 우리나라의 위상 제고에 큰 역할을 할 것으로 예상되고 있는 방법이다[5].

ARIA는 경량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용.블록 암호 알고리즘입니다. ARIA의 주요 특성은 128비트의 블록 크기를 가지며, 128/192/256비트(AES와 동일 규격)의 키 크기를 가진다. 또한, 전체 구조는 Involutional Substitution-Permutation Network이며, 라운드 수는 키 크기에 따라 12/14/16를 가진다. 특히, 경량 환경 및 하드웨어에서의 효율성 향상을 위해, ARIA가 사용하는 대부분의 연산은 XOR과 같은 단순한 바이트 단위 연산으로 구성되어 있습니다.

위의 사양을 블록 단위(8 비트)로 정리하면 표 1과 같다. 이때, 입.출력 블록 크기를 Nb, 입력 키 블록 크기를 Nk, 그리고 라운드 수를 Nr로 나타내었다.

표 1. ARIA 사용

구 분	Nb	Nk	Nr
ARIA-128	16	16	12
ARIA-192	16	24	14
ARIA-256	16	32	16

ARIA의 라운드 함수는 다음과 같은 세 부분으로 구성되어 있다. 첫째는 라운드 키 덧셈(AddRound Key)으로 128-비트 라운드 키를 라운드 입력 128-비트와 비트별 XOR하며, 두 번째는 치환 계층(Subst Layer)으로 두 유형의 치환 계층이 있으며 각각은 2종의 8비트 입.출력 S-box와 그들의 역변환으로 구성된다. 세 번째는 환산 계층(DiffLayer)으로 간단한 16 × 16 involution 이진 행렬을 사용한 바이트 간의 확산 함수로 구성되어 있으며, 암호화 과정과 복호화 과정은 라운드 키를 제외하고 일치함을 알 수 있다. 이와 같은 방법을 이용한 암호화 과정과 복호와 과정을 그림 6에 나타내었다.

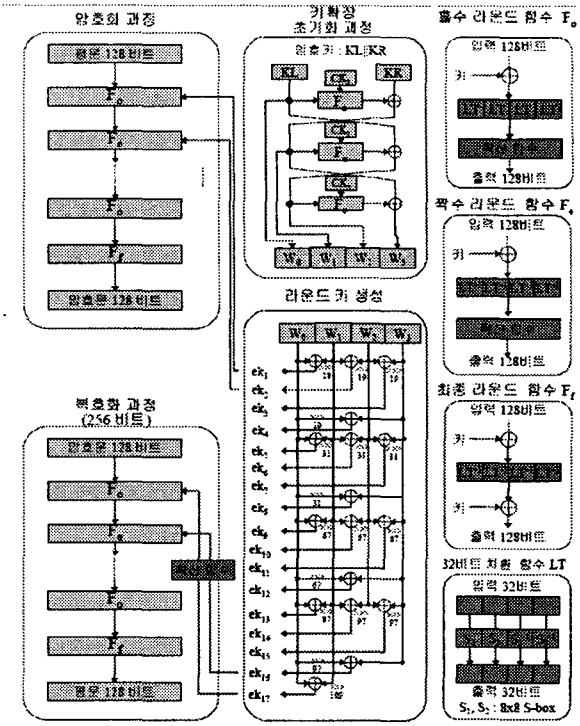


그림 6. 암호화 및 복호화 과정

4. 결 론

본 논문에서는 얼굴인식과 홍채인식 시스템을 융합한 다중생체인식 시스템을 구현하였으며, 다중생체인식 시스템에서 구현된 생체데이터를 안전하게 전송할 수 있는 방법으로 블록 암호 알고리듬 ARIA를 침입에 대한 보안 방법을 제안하였다. 이에 다중생체 특징벡터를 128비트의 블록 크기로 이용하여 암호화 하였으며, 생체특징벡터에 대하여 128비트의 키로 사용하였다.

향후 연구 과제로 제안하지 않은 특징벡터를 이용하여 암호화 하는 방법에 대하여 연구 및 구현이 요구된다.

참고문헌

[1] 전명근외, "다중 생체인식 시스템 성능 시험방법론 연구 개발", 한국정보보호진흥원 위탁과제, 2005
[2] 전명근외, "프라이버시 친화적 생체인식 시스템 구축 방안 연구", 한국전자통신연구원 위탁과제, 2005
[3] 곽근창, 고현주, 전명근, 퍼지 소속도를 갖는 Fisherface 방법을 이용한 얼굴인식, 한국정보과학회, 정보과학논문지, Vol 31, No 6, pp.784-791, 2004.
[4]고현주, 권만준, 전명근, "가버 웨이블릿과 퍼지 선형판별분석기법을 이용한 홍채인식", 정보과학회논문지, Vol 32, No 11, pp.1147-1155, 2005.
[5] 국가보안기술연구소, http://www.nsri.re.kr