Journal of Korean Institute of Intelligent Systems, Vol. 23, No. 4, August 2013, pp. 310-316
http://dx.doi.org/10.5391/JKIIS.2013.23.4.310

실수형 퍼지볼트를 이용한 다중 바이오인식 시스템

Multimodal Biometric Recognition System using Real Fuzzy Vault

이대종* · 전명근*†
Dae-Jong Lee, and Myung-Geun Chun*†

*충북대학교 전자정보대학 전자공학부 컴퓨터정보통신연구소
† College of Electrical and Computer Engineering, Chungbuk National University

요 약

바이오인식 시스템은 변하지 않는 고유의 특성으로 인하여 범죄를 포함한 다양한 분야에서 널리 사용되고 있다. 그러나 바이오인식정보가 불법 사용자에게 누설되었을 때 많은 문제점을 지니고 있다. 본 논문에서는 지문과 얼굴 정보를 보호하기 위하여 실수형 오류정보 부호 코드화를 수행하는 실수형 퍼지 볼트를 이용한 다중 바이오 인식 시스템을 개발한다. 제안된 방법은 실수형 퍼지볼트를 이용함으로써 분실시 재생성할 수 없는 지문 및 얼굴 특징값과 달리 개인 킷값을 수시로 변경할 수 있다는 장점과 두 가지 바이오정보를 융합함으로써 보안이 강화된 바이오인식 시스템을 구현할 수 있다는 장점이 있다. 제안된 방법의 타당성을 검증하기 위하여 실험한 결과 기존 방법에 비하여 우수한 결과를 나타냈다.

키워드 : 퍼지 볼트, RN-ECC, 얼굴인식, 지문인식, 다중 바이오인식

Abstract

Biometric techniques have been widely used for various areas including criminal identification due to their reliability. However, they have some drawbacks when the biometric information is divulged to illegal users. This paper proposed multimodal biometric system using a real fuzzy vault by RN-ECC for protecting fingerprint and face template. This proposed method has some advantages to regenerate a key value compared with face or fingerprint based verification system having non-regenerative nature and to implement advanced biometric verification system by fusion of both fingerprint and face recognition. From the various experiments, we found that the proposed method shows high recognition rates comparing with the conventional methods

Key Words : Fuzzy Vault, RN-ECC, Face Verification, Biometrics

1. 서 론

얼굴, 지문 등을 이용하여 신분을 확인하는 바이오인식 기술은 비밀번호나 카드와 같은 인증 수단과 달리 불법 사용의 위험성이 없기 때문에 차세대 보안인증 기술로 각광을 받고 있다[1-3]. 그러나 얼굴, 지문 등의 개인 바이오 정보가 누설되었을 때 바이오 정보 그 자체를 변경할 수 없다는 치명적인 문제점을 지니고 있다. 따라서 바이오 인식 기술이 널리 적용되기 위해서는 바이오 정보를 담고 있는 템플릿을 보호하거나, 또는 바이오 정보가 유출되었다 하더라도 불법 사용자가 도용한 바이오 정보 자체만을 이용하여 사용할 수 없도록 처리하는 방법이 우선 개발되어야 한다.

기존에는 생체인식 시스템의 성능을 향상시키기 위하여 두 가지 이상의 생체정보를 융합한 다중 바이오인식 시스템 측면으로의 연구가 이루어졌으나[4-7], 최근에는 바이오 템플릿을 보호하기 위한 기법들이 국내외적으로 활발하게 이루어지고 있다[8][9]. 이들 기법들은 특징벡터 변환(feature transformation)과 바이오 암호시스템(Biometric Cryptosystem)으로 나누어진다. 특징벡터 변환 방법은 역변환 가능한 변환 함수를 쓰는 경우와 역변환이 가능하지 않은 방법을 사용하는지에 따라서 다시, BioHashing과 Robust Hashing 방법으로 나누어진다. 한편, 바이오 암호시스템(Biometric Cryptosystem)에 있어서는 암호화 키를 직접 바이오정보로부터 만들어 내는 방법(Key Generation)과 암호화 키를 바이오정보와 엮어서 보관한 후, 이를 필요한 경우에 바이오정보를 이용하여 다시 추출해 낼 수 있도

접수일자: 2013년 5월 20일
심사(수정)일자: 2013년 8월 5일
게재확정일자 : 2013년 8월 7일
† Corresponding author
이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0024037)

록 하는 Key Binding 방법이 있다[10].

특징벡터 변환 방법은 사용자가 지정한 키 값이나 패스워드로부터 정의되는 함수에 기초하게 된다. 특히, 역변환 가능한 경우에 있어서는 사용되는 키 값을 안전하게 보호해야 되는 부가적인 요구사항이 생기는 반면에, 공격자에게는 바이오인식 시스템을 해킹하기 위해서는 키 값과 함께 바이오정보도 요구하게 되어 시스템의 안전도는 높아질 수 있는 구조이다. 현재, 가장 많이 연구 되고 있는 형태는 랜덤한 직교좌표에 기반한 BioHashing 방법이 있다[11]. 입력된 특징 벡터는 사전에 랜덤하게 생성되어 토큰에 저장되어 있는 직교행렬들과 내적을 통하여 특정한 값을 산출하게 되고, 이를 지정된 임계값을 이용하여 이진화 하여 원하는 BioHash 값을 갖는 구조로 이루어 졌다. 실험 결과 낮은 오수락율(False Accept Rate) 등의 장점이 있으나, 다음과 같은 단점과 한계가 지적되고 있다.

첫 번째로, 변환함수에 사용된 사용자 지정 키값이 유출되었을 때, 역변환 가능한 함수일 경우에 원래의 원본 바이오 템플릿 정보를 얻을 수 있다는 점이다. 두 번째로, 매칭이 변환된 영역에서 이루어지므로, 인식률의 저하가 없기 위해서는, 변환 전 템플릿간의 유사도가 변환 후에도 유지될 수 있어야 한다. 따라서 변환 함수의 선택에 따라 인식성능이 크게 변할 수 있다는 점이다. 마지막 문제점으로 인식률을 높이기 위하여 크기가 큰 랜덤 행렬을 사용하는 경우, 바이오 정보에 의한 변별력 보다, 행렬 자체에 의한 변별력이 커져서 바이오 인식 알고리즘을 사용하는 장점자체가 없어지고, 따라서 타인 수락율이 커질 수 있는 위험이 있다는 점이다.

본 논문에서는 지문과 얼굴 정보를 보호하기 위하여 실수형 오류정보 부호 코드화를 수행하는 실수형 퍼지볼트를 이용한 다중 바이오 인식 시스템을 개발한다. 본 논문에서 적용한 실수형 퍼지볼트는 기존에 널리 적용되는 CRC(Cyclic redundancy check)를 이용한 방법에 비하여 구현이 간단하고 바이오 인식 정보의 매칭을 위해 실수형의 매칭기를 사용할 수 있는 장점이 있다. 또한, 제안된 방법은 실수형 퍼지 볼트(Real fuzzy valut)를 이용함으로써 분실시 재성성할 수 없는 지문 및 얼굴과 달리 개인 킷값을 수시로 변경할 수 있다는 장점과 두 가지 바이오인식 정보를 융합함으로써 보안이 강화된 바이오인식 시스템을 구현할 수 있다는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 퍼지 볼트를 이용한 바이오인식 정보보호기법에 대하여 살펴본 후, 3장에서는 본 논문에서 실수형 퍼지 볼트 방법을 이용한 다중 바이오 인식시스템을 설명한다. 4장에서는 실험방법과 실험결과에 대한 분석을 하고. 마지막 5장에서는 결론을 맺는다.

2. 퍼지 볼트를 이용한 바이오정보 보호기법

퍼지 볼트는 중요한 정보를 보호하기 위해 Jules와 Sudan에 의해 제안된 방법으로 인코딩(Encoding)과 디코딩(Decoding)과정으로 이루어진다. 먼저 인코딩 과정을 살펴보자. Alice는 집합 A를 이용하여 비밀정보 S를 은닉하려고 한다. 그러면 비밀정보 S를 이용하여 변수 x에 대한 다항식 $P(x)$를 생성한다. 그리고 집합 A의 원소들을 다항식의 변수 x에 각각 대입하여 다항식 $P(x)$위에 존재하는 점들을 생성한다. 그리고 나서 공격자로부터 다항식 $P(x)$를 은닉하기 위해서 $P(x)$와 무관한 임의의 점들(chaff points)을 다항식 위의 점들에 삽입하여 볼트 V(Vault)를 생성함으로 인코딩 과정을 마친다.

이번에는 Bob이 집합 B를 이용하여 금고에 있는 S를 얻고자 한다. 만약 B의 원소들과 A의 원소들 사이에 일치하는 부분이 많다면, B는 V에서 다항식 $P(x)$위에 존재하는 대부분의 점들을 식별해내게 된다. 그러나 집합 B를 이용해 찾아낸 점들에는 다항식과 무관한 점들도 포함되어 있을 수 있다. 이러한 오류 점들은 오류정정부호(Error correcting code)를 통해 정정되고 Bob 은 정확하게 S를 얻어내게 된다. 반면에 B와 A가 거의 일치하지 않는다면 $P(x)$를 알아낼 수 없도록 방해하는 많은 점들(chaff points) 때문에 Bob 은 S에 접근할 수 없다. 퍼지볼트 알고리즘은 집합 B가 집합 A와 항상 정확하게 일치하지 않더라도 오류정정부호를 사용하기 때문에 열쇠가 갖는 모호성과 암호화 구조가 요구하는 정확성 사이의 틈을 줄여줄 수 있다. 또한 집합 A와 비밀정보 S는 다항식과 무관한 점들에 의해 동시에 보호된다. 이러한 퍼지볼트의 개념을 생체정보인 지문[12], 얼굴[13][14], 홍채[15] 등에 결합시킨 연구가 활발하게 이루어지고 있다.

그림 1은 전형적인 퍼지볼트 방법과 바이오 인식 시스템을 결합한 바이오인식 시스템을 나타냈다. 퍼지 볼트를 만드는 인코딩과정을 간략히 설명하며 다음과 같다. 사용자의 유사 식별자로 쓰일 K-비트로 구성된 PI인 S를 랜덤하게 생성한다. S는 균등하게 l-비트단위로 구성된 $(\{s_1,s_{2.}...,s_{K/l}\})$로 분할되었고, 이것들로 (K/l)개의 계수를 갖는 다항식 P의 계수로 구성한다. 계수들이 l-비트 값인 통상 퍼지볼트 시스템의 모든 수학적 연산이 유한계 $\mathrm{GF}(2^l)$에 근거하기 때문이다. 결론적으로, 다항식 P는 차수 $d=((K/l)-1)$, $P(x)=s_1+s_2x+\cdots+s_{(K/l)}x^{(K/l)-1}$로 표현된다. 퍼지 볼트를 위해서는 세 집합 (T,N,R)을 생성하는 것이 필요하다.

첫 번째 집합은 양자화된 바이오인식 특징값인 $A=\{a_1,a_2,...,a_A\}$을 사용하여 다항식 $P(x)$를 계산함으로써 형성된 사용자 볼트 집합 T $(T=\{(a_1,P(a_1)),(a_2,P(a_2)),...,(a_A,P(a_A))\}$이다. 사용자 볼트 집합 T의 모든 성분들은 볼트를 여는(unlock) 과정에서 다항식을 재구성하기 위해 사용된다. 따라서 생성되는 점들은 최소한 $(d+1)$이어야 한다. 여기서 집합 T는 A개의 점들로 구성된다고 본다.

두 번째 집합은 몇 개의 chaff 점들로 구성된 한 집합 N이다. 이러한 점들은 사용자 볼트 집합 T를 숨기는데 중요한 역할을 한다. $N=\{(v_1,w_1),(v_2,w_2),...,(v_g,w_g)\}$(여기서 v_i는 다항식의 입력에 해당되는 x값이고, w_i는 y 값으로 여기서 사용되는 x값은 집합 T 를 구성하는 x값들과 겹치지 말아야하며 즉, $(v_i \neq a_j, i=1,2,...,g, j=1,2,...,A)$이고, 다항식 $P(x)(w_i \neq P(v_i), i=1,2,...,g)$에 위치하지 않는다는 조건을 만족하면서 유한계의 범위에서 임의로 생성되었다. 이렇게 구성되는 집합 A와 집합 N을 임의로 섞어서 최종적인 볼트인 V를 만들게 된다. 이렇게 하면 등록 과정은 모두 마치게 되며, 구해진 볼트는 스마트카드나 USB 저장장치에 저장됨으로서 개인의 프라이버시를 보호 할 수 있다.

볼트를 여는 과정은 두 개의 입력, 볼트(V)와 테스트 B

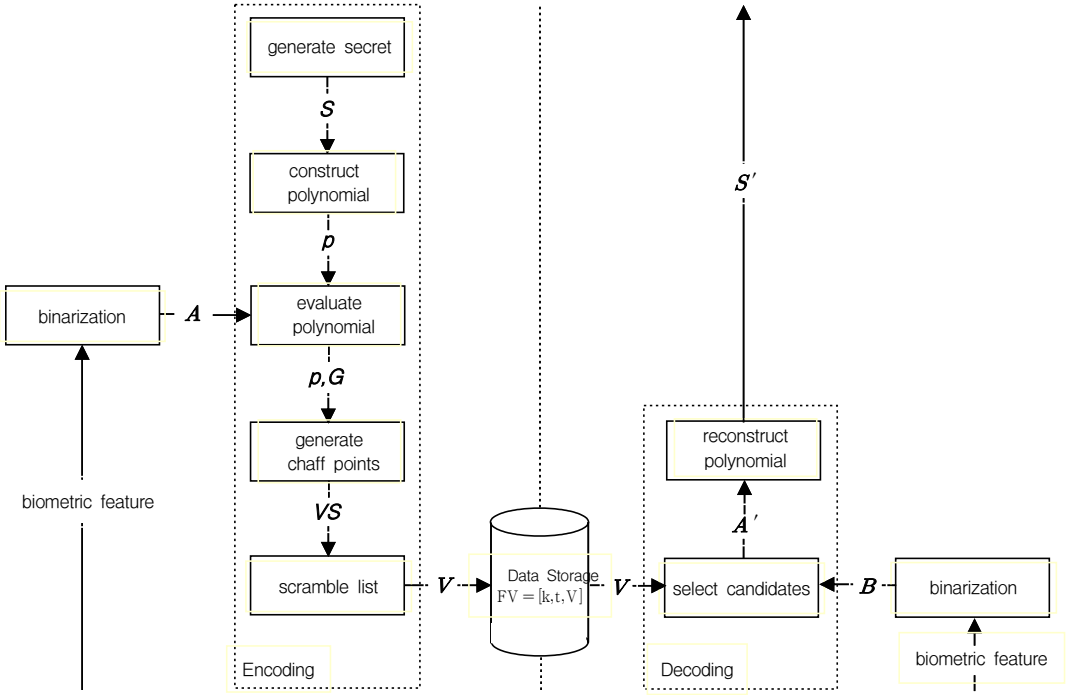


그림 1. 퍼지볼트를 이용한 바이오인식
Fig. 1. Biometrics by fuzzy vault scheme

를 필요로 한다. 볼트(V)는 저장장치로부터 얻어지고, 테스트 B는 위에서 보인 바와 같이, B개의 바이오특징을 취득하여 얻어진다. B를 이용하여 주어진 다항식의 계수를 Lagrange 보간법을 이용하여 추정하게 된다. 그러나 위와 같은 과정은 실제적인 바이오인식 시스템에 적용할 때 주요 문제가 있었다. 첫 번째로, 지문이나 얼굴과 같은 바이오정보는 취득할 때 마다, 외부적 변동요인에 의해서 특징값이 달라지므로 위의 과정에서와 같이 집합 A와 B가 정확하게 일치하는 경우는 드물다. 또한, 등록과정에서 만들어진 유사식별자 S에 대해서 Lagrange 보간에 의해서 만들어지는 재구성된 유사식별자 S^*와의 오차검출이나 수정을 위한 오류검출 및 정정코드(error correcting code)가 반드시 필요하다.

오류정정부호코드는 1948년, Shannon이 그의 논문에서 오류정정부호를 통해 정보를 손실 없이 전송 하거나 저장할 수 있다는 개념을 소개한 이후로 다양한 연구가 활발하게 진행되어 오고 있다. 이들 중에서 퍼지 볼트 연구 분야에 가장 많이 쓰이는 것이 Reed-Solomon 코드이다[16]. Reed-Solomon(RS)코드는 1960년 Irving Reed와 Gus Solomon에 의해 개발된 오류정정코드로써 다원 BCH(Bose-Chaudhuri-Hoquenghem) 코드의 한 범주에 속한다. RS코드는 GaloisField $GF(q)$의 원소로 코드워드가 구성되고 $GF(q)$상의 심볼 단위로 인코딩 되고 디코딩 되기 때문에 통신 선로 상에서 발생하는 산발오류(random error)와 연집오류(burst error)를 정정할 수 있기 때문에 각종 디지털 통신 시스템 및 데이터 저장 시스템의 신뢰성 향상을 위해 광범위하게 사용되는 오류정정 코드이다.

지금까지의 모든 대부분의 퍼지 볼트 연구에서는 RS 코드를 사용하였다. 그러나 이를 적용하기 위해서는 모든 변수나 입력값들이 GaloisField $GF(q)$상의 값들로 표현 되어야 하고 따라서, 지문이나 얼굴에서 추출되는 실수(real number)값을 갖는 특징값을 바로 사용 할 수 없다. 더욱이 다항식의 역변환을 구함에 있어서도, 기존의 대수학에서 널리 사용하고 있는 일반적인 역변화(genealized inverse)를 사용할 수 없는 제약이 있다. 이러한 제약은 보안의 측면에서 보면, 주어지는 PI가 이진 비트열로만 주어지고, 이때의 길이는 사용하는 갈로아 유한체(Galois Field)의 크기에 따라 제한되므로 고정도의 보안을 위해 실수형의 PI를 발급할 수 있는 유사식별자의 발급이 불가능하다. 또한 최종적으로 추출된 PI*와 PI에 대한 매칭값도 퍼지논리 등에서 정의된 다양한 유사도 값을 사용하지 못하는 단점이 있다. 이에 본 연구에서는 실수형 오류정보 부호화 기법(RN-ECC; ,Real Number Error Correcting Code)[17][18]에 기반한 퍼지 볼트를 지문 및 얼굴로 구성된 다중 바이오 인증 시스템에 적용하고자 한다.

3. 실수형 퍼지볼트를 이용한 다중 바이오 인식시스템

3.1 RN-ECC에 기반한 실수형 퍼지 볼트 방법

본 논문에서는 지문 및 얼굴 템플릿의 특징값에 대해서 실수형 오류정보 부호 코드화를 수행하는 실수형 퍼지 볼트 방법을 적용하였다[20][21]. 기존에 단순한 유한체 다항식에 기초하여, 다항식에 계수에 키를 Bind하여 이를 바이오 정보를 이용하여 추출하는 경우, 바이오 정보의 변동을 극복하기 위하여 에러 수정 코드나 CRC(Cyclic redundancy check)를 이용하였다. 그러나 앞에서 지적 하였다시피, 이럴 경우 구현이 복잡할 뿐더러, 오차 수정 코드로 매칭을 하는 경우에 바이오 인식 정보의 매칭을 위해 개발된 실수

형의 매칭기를 사용할 수 없는 단점이 있다. 따라서 이를 극복하고자 실수형 다항식의 근사화 특성을 가지는 RN(Real number) ECC(오류정정코드)를 적용하였다. 여기서는 간략히 중요한 개념만을 언급하고자 한다.

랜덤 키 값인 실수형 데이터 K개로 구성된 $\{x_i\}$는 길이 K인 열벡터 $\boldsymbol{x}=[x_0,x_1,\cdots,x_{K-1}]$로 표현된다. 그리고 길이 N인 코드벡터는 $\boldsymbol{y}=[y_0,y_1,\cdots,y_{N-1}]$로 표시하기로 하면, 두 벡터 간의 관계는 다음과 같이 표현할 수 있다.

$$\boldsymbol{y}=\boldsymbol{x}\boldsymbol{G} \tag{1}$$

여기서, $\boldsymbol{G}$는 rank가 K인 $K\times N$ 발생행렬(generator matrix)이다. 이러한 관계는 블록코드(block code)는 (N,K) 코드로 표시할 수 있다. 양자화잡음과 채널오차를 각각 $\boldsymbol{q}$와 $\boldsymbol{e}$로 표기하자. 행렬 $\boldsymbol{G}$는 양자화 잡음과 정정할 수 없는 오차들이 없을 경우 $\boldsymbol{x}$가 정확히 복원될 수 있도록 하는 다음의 식을 만족하는 $\boldsymbol{G}$의 $N\times K$인 오른쪽 역행렬(right inverse)이다.

$$\boldsymbol{G}\boldsymbol{G}^{-1}=\boldsymbol{I}_K \tag{2}$$

Rank $N-K$인 $(N-K)\times N$ 패리티 검사 행렬 $\boldsymbol{H}$는 켤레전치(conjugate transpose) $*$를 이용하여 다음과 같이 정의된다.

$$\boldsymbol{G}\boldsymbol{H}^{*}=0 \tag{3}$$

추정하고자 하는 코드벡터 $\boldsymbol{r}$은 식 (4)와 같다.

$$\boldsymbol{r}=\boldsymbol{y}+\boldsymbol{e} \tag{4}$$

그러면 수신된 벡터 $\boldsymbol{r}$의 신드롬(syndrome) $\boldsymbol{s}$는 다음과 같이 계산된다.

$$\boldsymbol{s}=\boldsymbol{r}\boldsymbol{H}^{*}=(\boldsymbol{y}+\boldsymbol{e})\boldsymbol{H}^{*}=\boldsymbol{e}\boldsymbol{H}^{*} \tag{5}$$

여기서 $\boldsymbol{e}$는 차원 N의 알려지지 않은 오차 패턴이며, $\boldsymbol{e}=\boldsymbol{r}-\boldsymbol{y}$ 와 같다. 따라서 오차값 $\boldsymbol{e}$가 매우 적다면 신드롬 $\boldsymbol{s}$는 매우 작은 값을 갖게 된다. 전송된 코드벡터 $\boldsymbol{y}$와 추정하고자 하는 코드벡터 $\boldsymbol{r}$이 동일한 이상적인 경우에 신드롬 $\boldsymbol{s}$는 0이 된다. 신드롬 $\boldsymbol{s}$가 0에 근접할 경우 최종적으로 구하고자 하는 열벡터 $\hat{\boldsymbol{x}}$는 식 (6)에 의해 추정된다.

$$\hat{\boldsymbol{x}}=\boldsymbol{r}\,\boldsymbol{G}^{T}(\boldsymbol{G}\boldsymbol{G}^{T})^{-1} \tag{6}$$

3.2 제안된 방법

그림 2에서는 본 연구에서 제안한 지문 및 얼굴에 대한 실수형 퍼지볼트를 이용한 다중 바이오인식 시스템을 나타냈다. 우선 등록과정에서는 등록 개인에 랜덤하게 발생된 랜덤 키 $\boldsymbol{x}$를 부여하고, 발생행렬(generator matrix) $\boldsymbol{G}$와 패리티 검사 행렬 $\boldsymbol{H}$를 DCT 행렬에 기반을 둔 기저함수를 이용하여 생성하고, 생성된 발생행렬 $\boldsymbol{G}$와 키 값인 $\boldsymbol{x}$ 이를 이용하여 코드벡터 $\boldsymbol{y}$를 생성한다. 본 연구에서 코드벡터 $\boldsymbol{y}$는 다항식 $p(x)$를 발생시키기 위한 다항식 계수값을 의미한다. 다음 단계로 생성된 다항식 계수값과 지문 및 얼굴정보에 대한 특징값을 이용하여 다항식 $p(x)$를 산출한다. 마지막 단계에서 지문 및 얼굴 특징을 보호하기 위하여 거짓 특징점을 이용한 거짓 다항식값인 chaff point를 생성하여 퍼지 볼트 템플릿을 구축한다. 퍼지 볼트 템플릿에서는 계수의 차수에 해당하는 입력부분과 출력항인 다항식으로 구성되어 있다.

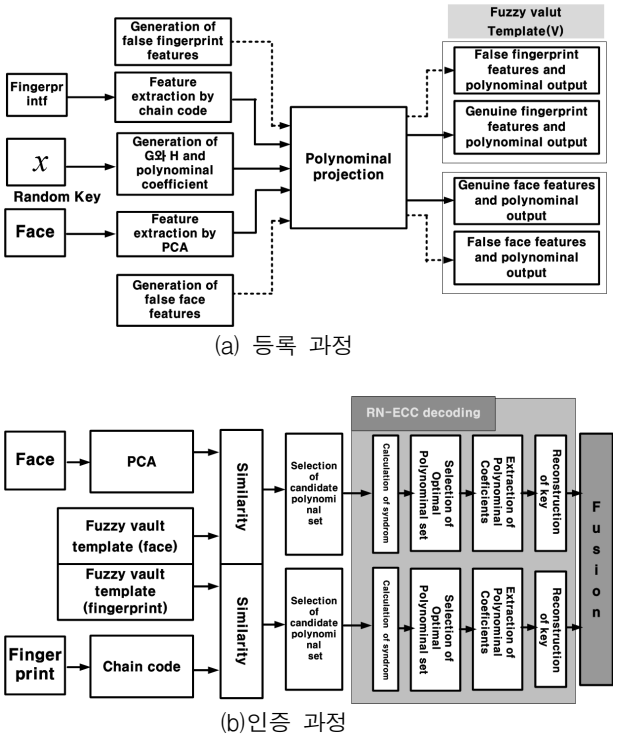


그림 2. RN-ECC에 기반한 실수형 퍼지 볼트 방법을 이용한 다중 바이오인식 시스템

Fig. 2. Multi-modal biometric system using real fuzzy vault method based on RN-ECC
(a) Registration process (b)Verification process

인증과정에서는 우선, 검증 영상에 대한 지문 및 얼굴의 특징을 추출하고 추출된 특징값과 등록과정에서 생성된 퍼지 볼트 템플릿을 비교하여 유사도가 높은 후보 다항식 집합을 선택한다. 선택된 후보 다항식 집합에는 등록시 사용된 지문 및 얼굴특징에 해당하는 다항식 집합뿐만 아니라 거짓 지문 및 얼굴 특징에 의해 생성된 다항식 집합도 포함되어 있다. 이러한 후보 다항식 집합에서 본인의 지문 특징 및 얼굴 특징에 해당하는 집합들을 선택하기 위하여 RN-ECC 디코딩 과정이 수행된다. RN-ECC 디코딩 과정은 선택된 후보 다항식 집합에서 $\boldsymbol{r}$로 표현된 다항식 계수값을 추출하기 위해 필요한 모든 집합을 구성한 후, 구성된 모든 조합에 대하여 다항식 계수값 $\hat{\boldsymbol{r}}$ 값을 추정하고 식 (5)에 의해 신드롬 $\boldsymbol{s}$값을 계산한다. 최종적으로 계산된 신드롬 $\boldsymbol{s}$값 중에서 가장 최소값을 갖는 집합에서 계산된 계수값 $\hat{\boldsymbol{r}}$ 값을 선택하고, 선택된 계수값 $\hat{\boldsymbol{r}}$과 등록과정에서 생성한 발생행렬(generator matrix) $\boldsymbol{G}$를 이용한 식 (6)에 의해 개인 키 값인 $\hat{\boldsymbol{x}}$를 복원하고, 등록과정에서 생성된 키값인 $\boldsymbol{x}$와 비교하여 최종 개인 인증을 하게 된다.

제안된 방법의 장점으로는 분실시 재생성할 수 없는 지문과 달리 개인 키 값인 $\boldsymbol{x}$값을 수시로 변경시킬 수 있음으로 주기적으로 키값을 변경할 수 있다는 점이다. 또한, 인증시 사용되는 퍼지 볼트 템플릿에는 개인의 지문 및 얼굴 정보뿐만 아니라 거짓 정보를 담고 있는 정보도 포함되어 있음으로 퍼지 볼트 템플릿이 분실되었다 하더라도 등록된 개인의 바이오 정보를 추출하기 어렵다는 장점이 있다.

4. 실험 결과 및 분석

본 연구에서 제안된 RN-ECC를 이용한 다중 바이오 인식시스템의 성능을 평가하기 위하여 40명에 대하여 개인당 6개의 지문을 취득한 지문 데이터와 ORL 얼굴 데이터를 이용하였다. ORL 얼굴 데이터베이스는 서로 다른 환경에서 40명에 대하여 개인당 10개의 얼굴영상을 포함하고 있다. 그러나 지문과의 일대일 매칭을 개인당 6개의 얼굴 데이터만을 이용하였다. 퍼지볼트 구축을 위한 학습용으로는 개인당 3장의 데이터를 이용하였고, 나머지 영상을 이용하여 검증을 하였다.

지문의 특징점 추출은 체인코드 윤곽선(Chain code contour)기법을 이용하였다[19]. 체인코드에 의해 지문에서 추출된 특징점은 위치, 각도, 그리고 종류로 나타내며 $m_i = (x_i, y_i, \theta_i, t_i)$로 표현되고, 두 개의 좌표인 x, y와 각도 θ를 갖는다. 얼굴의 특징점 추출은 주성분분석기법을 이용하여 36차를 갖는 얼굴특징을 추출하였다[20]. 그러나 36차의 얼굴 특징 한 개만으로는 다항식에 기반한 퍼지볼트를 적용할 수 없기 때문에 36차의 벡터를 3차원을 갖는 12개의 벡터로 재구성하였다. 또한 지문 및 얼굴 특징 템플릿은 지문 및 얼굴의 실제 특징값 뿐만 아니라 지문 및 얼굴 특징 정보를 보호하기 위한 거짓 특징점도 포함되어 있다. 거짓 특징점의 삽입 위치가 실제 지문 및 얼굴의 특징점의 위치와 매우 근접해 있다면 인식률의 성능이 저하된다. 따라서 본 연구에서는 가짜 특징점의 위치를 실제 특징점의 위치보다 일정 간격 떨어진 점에 있는 특징점들을 랜덤하게 선택하였다. 그림 3에서는 지문 및 얼굴에 대한 실제 특징점과 삽입된 가짜 특징점을 나타냈다.

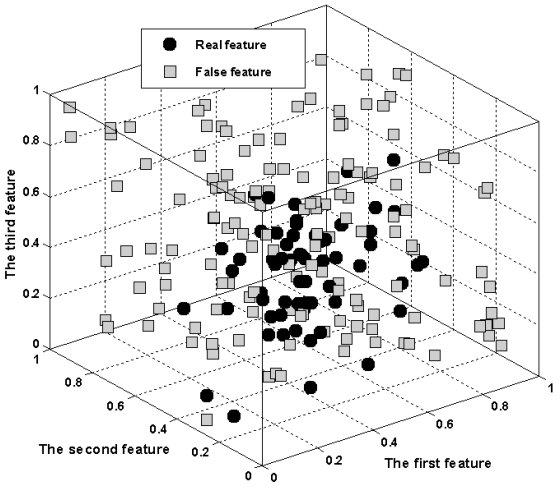
퍼지 볼트 템플릿에는 지문 및 얼굴의 특징점 뿐만 아니라 인증과정에서 필요한 키 값을 복원하는데 필요한 다항식 출력값이 필요하다. 이를 위해 3차원으로 재구성된 지문 및 얼굴의 특징점 (f_{i1}, f_{i2}, f_{i3})과 식 (7)에 나타낸 다항식을 이용하여 다항식 출력값 $p_i(x)$를 생성하게 된다.

$$p_i(x) = a_0 + a_1 f_{i1} + a_2 f_{i2} + a_3 f_{i3} + a_4 f_{i1} f_{i2} + a_5 f_{i1} f_{i3} + a_6 f_{i2} f_{i3} + a_7 f_{i1}^2 + a_8 f_{i2}^2 + a_9 f_{i3}^2 \quad (7)$$

식 (7)에 나타낸 다항식 계수 a_i를 계산하기 위해서는 랜덤키 $\boldsymbol{x}$와 발생행렬 $\boldsymbol{G}$, 그리고 인증과정에서 계수값을 복원하는데 사용될 패리티 검사행렬 $\boldsymbol{H}$가 필요하다. 본 논문에서는 랜덤 키 $\boldsymbol{x} = [11, 22, 33, 44, 55, 44, 33, 22]$로 임의로 설정하였고, 발생행렬 $\boldsymbol{G}$와 패리티 검사행렬 $\boldsymbol{H}$는 DCT(Discrete cosine transform)행렬에 기반을 둔 기저함수를 이용하여 생성하였다[20].

지문 및 얼굴 특징정보를 보호하기 위하여 퍼지 볼트 템플릿에는 얼굴 특징점과 랜덤하게 발생시킨 거짓 얼굴 특징점 뿐만 아니라 인증과정에서 키 값을 복원하는데 필요한 다항식 $p_i(x)$값이 포함되어 있다. 지문 및 얼굴 특징점에 대해서는 식 (7)에 의해 다항식값을 산출하지만, 랜덤하게 발생시킨 거짓 특징점에 대해서는 식 (7)에 의해 산출된 다항식 $p_i(x)$ 대신에 임의의 Chaff Point를 삽입하게 된다. 이를 위해 거짓 특징점에 대한 다항식 $p_i(x)$값은 식 (7)에 의해 계산된 다항식 출력값에 $\pm 25\%$ 이내에 존재하는 랜덤 값을 합산하여 Chaff Point를 발생시켰다.

(a). 거짓 특징값이 포함된 지문 영상



(b) 거짓 특징값이 포함된 얼굴 특징

그림 3. 거짓 특징값이 포함된 지문 및 얼굴 특징
Fig. 3. Fingerprint and face features including false features

제안된 방법에 의한 지문 및 얼굴정보를 이용한 인식과정은 다음과 같다. 우선 인증하고자 하는 지문 및 얼굴의 특징과 거짓 특징점이 포함된 템플릿과의 비교를 통해 유사도가 높은 순서대로 퍼지 볼트 템플릿에서 12개의 다항식 집합을 선택한다. 인식하고자 하는 지문 및 얼굴정보에 대한 특징값의 차원은 36차원이다. 즉 지문은 지문당 (x, y, θ)로 구성된 12개의 특징점을 가지고 있으며, 얼굴의 경우 얼

굴영상당 3차원을 갖는 12개의 특징점을 가지고 있다. 식(7)로부터 키 값을 복원하기 위해서는 최소한 10개의 데이터 집합이 필요하다. 본 논문에서는 입력 영상에 대한 특징과 퍼지 볼트내의 데이터 집합과의 비교를 통하여 유사도가 높은 12개의 다항식 집합을 추출하였다. 따라서 12개의 다항식 집합 중에서 최적의 다항식 집합 10개를 선택하여야 한다. 본 논문에서는 모든 조합에 대한 전수조사를 실시하고, 이를 통하여 계산된 신드롬값을 이용하여 최적의 다항식 집합을 선택하였다. 즉 일차적으로 선택된 다항식 집합의 수가 12임으로 신드롬값 계산을 위해 $C(12,10)=66$의 다항식 집합에 대한 신드롬값을 계산하고 신드롬 값이 가장 낮은 다항식 집합을 선택하여 계수값을 복원한 후, 복원된 계수값을 이용하여 키 값을 추정하게 된다.

표 1에서는 실험결과를 나타냈다. 표 1에서 융합방법은 AND 연산과 OR 연산을 이용하였다. AND 연산은 지문과 얼굴에 대하여 모두 인증된 경우만 최종 승낙하는 구조로 구성하였으며, OR 연산은 지문과 얼굴 어느 한쪽이 인증된 경우 최종 승낙하는 구조로 구성하였다. 성능평가로는 오거부율(본인을 거부)을 나타내는 FRR과 오인식률(타인을 본인으로 인식)을 나타내는 FAR은을 기준으로 하였다. FRR을 위해 사용된 지문 및 얼굴의 수는 120개(40명×3개)이고, FAR을 위해 사용된 지문 및 얼굴의 수는 4680개(39명×3개×40set)이다. 또한 거짓 특징점의 개수는 200으로 설정하여 실험하였다[14]. 표 1에서 보는 바와 같이 지문은 본인 영상 120개 중에서 16개가 인식되지 않아 FRR이 13.33%로 나타났으며, 타인 영상 4680개 중에서 8개가 인식되어 FAR이 0.17%로 나타났다. 얼굴의 경우에는 본인 영상 120개 중에서 2개가 인식되지 않아 FRR이 1.67%로 나타났으며, FAR은 0%로 나타났다. 융합 방법으로 AND 연산한 결과 본인 영상 120개 중에서 18개가 인식되지 않아 FRR이 15%로 나타났으며, OR 연산인 경우 0%로 나타났다. FAR은 AND 연산이 0%, OR 연산이 0.17%로 나타났다. 표 1의 결과로부터 OR 연산이 AND 연산에 비하여 우수함을 알 수 있다.

표 1. 융합 결과
Table 1. Fusion result

Division	fingerprint	Face	Fusion	
			AND	OR
FRR	13.33%	1.67%	15%	0%
FAR	0.17%	0%	0%	0.17%

얼굴 영상의 경우 가장 문제시되는 것으로 잡음에 따른 영향을 들 수 있다. 즉, 잡음에 의해 PCA 특징벡터의 변화가 크게 나타나며, 이는 얼굴 인식률의 저하를 초래한다. 이러한 경우에 제안된 방법을 평가하기 위하여 salt&pepper 잡음을 첨가하여 잡음에 따른 특성을 분석하였으며, 그 결과를 표 2에 나타냈다. 표 2에서 보는 바와 같이 얼굴의 경우 잡음 밀도에 따라 인식률이 급격히 저하됨을 확인할 수 있다. 즉 잡음이 없을 때는 FRR이 1.67%이었으나 잡음 밀도가 15%인 경우 FRR이 41.67%로 급격이 오거부율이 증가하였다. 그러나 OR 연산에 의한 융합 결과 잡음이 없을 경우 0%에서 잡음 밀도가 15%인 경우 FRR이 6.67%로 얼굴정보만을 이용하였을 때보다 저하율이 크지 않았다. 즉 잡음 밀도가 15% 주었을 경우, 지문은 오거부율 영상이 16개, 얼굴의 경우 오거부율 영상이 40개로 나타났으며, 지문과 얼굴 모두 오거부율된 영상의 개수는 8개로 나타났다. 따라서 OR 연산한 결과 120개의 영상 중에서 8개만이 오거부율됨으로써 6.67%의 FRR을 나타냈다. 오인식률은 잡음 밀도에 관계없이 일관된 결과를 보였다.

표 2. 얼굴 영상의 조명 변화에 따른 융합 결과
Table 2. Fusion result according to illumination changes for face image

Noise density (mixed in face)	Division	fingerprint	Face	Fusion	
				AND	OR
5%	FRR	13.33%	3.33%	15.83	0.83%
	FAR	0.17%	0%	0%	0.17%
10%	FRR	13.33%	15%	24.16%	4.16%
	FAR	0.17%	0%	0%	0.17%
15%	FRR	13.33%	33.33%	40%	6.67%
	FAR	0.17%	0%	0%	0.17%

5. 결론 및 향후 연구

본 논문에서는 실수형 퍼지볼트를 이용하여 지문과 얼굴로 구성된 다중 바이오 인식시스템을 개발하였다. 제안된 방법은 개인의 바이오인식 특징뿐만 아니라 가짜 바이오인식 특징으로 구성된 퍼지볼트와 RN(Real number) ECC(오류정정코드)를 적용하여 지문 및 얼굴에 대하여 독립적으로 인증하며, 최종적으로 OR 연산에 의해 승낙하는 구조로 구성하였다. 실험결과 얼굴영상의 결과가 지문영상의 결과보다 우수하여 지문영상의 융합효과가 적게 나타났다. 그러나 얼굴 영상의 가장 큰 문제점으로 지적되어 온 잡음이 존재할 경우 AND 연산에 의한 융합결과에 의해 성능이 개선되었음을 확인하였다. 또한, 인식성능을 비교하지 않더라도 기존의 바이오 인식 방법은 개인의 바이오인식 정보를 보호없이 사용하기 때문에 분실시 다른 대책이 없는 반면에 제안방법은 퍼지 볼트 템플릿에 의해 진짜 얼굴특징 정보를 보호할 수 있을 뿐만 아니라 키 값의 변경에 의해 퍼지 볼트 템플릿에 포함된 다항식 집합을 수시로 변경할 수 있음으로 보호측면에서도 우수한 성능을 보임을 확인할 수 있다. 향후 제안된 방법을 얼굴, 지문 이외의 생체정보에 적용하여 그 유용성을 보이고자 한다.

References

[1] S. K. Oh, C. M. Ma, S. H. Yoo, "Design of Optimized pRBFBBs-based Face Recognition Algorithm Using Two-dimensional Image and ASM Algorithm," *Journal of Korean Institute of Intelligent Systems*, Vol. 21, No. 6, pp. 749-754, 2011.

[2] J. Y. Hur, L. X. Truong, S. K. Lee, "A study on Iris Recognition using Wavelet Transformation and Nonlinear Function," *Journal of Korean Institute of Intelligent Systems*, Vol. 15, No. 3, pp. 357-362, 2005.

[3] S. H. Choi, S. W. Cho, S. T. Chung, "Identification System Based on Partial Face Feature Extraction,"

Journal of Korean Institute of Intelligent Systems, Vol. 22, No. 2, pp. 168-173, 2012.
[4] J. H. Kim, S. R. Kwon, "A Study on the Development of Embedded Serial Multi-modal Biometrics Recognition System," *Journal of Korean Institute of Intelligent Systems*, Vol. 16, No. 1, pp. 49-54, 2006.
[5] M. J. Kwon, D. H. Yang, Y. S. Kim, D. J. Lee, M. G. Chun, "Multimodal Biometrics System Using PDA under Ubiquitous Environments," *Journal of Korean Institute of Intelligent Systems*, Vol. 16, No. 4, pp. 430-435, 2006.
[6] I. F. Nizami, S. G. An, S. J. Hong, H. S. Lee, E. T. Kim, M. N. Park, "Fusion Algorithm for Integrated Face and Gait Identification," *Journal of Korean Institute of Intelligent Systems,* Vol. 18, No. 1, pp. 72-77, 2008.
[7] H. J. Go, Y. T. Kim, M. G. Chun, " A Multimodal Emotion Recognition Using the Facial Image and Speech Signal," *International Journal of Fuzzy Logic and Intelligent Systems,* Vol. 5, No. 1, pp. 1-6, 2005.
[8] M. K. Muhammad, N. Marsono, Rabia Bakhteri. "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," *Future Generation Computer Systems,* Vol. 29, No. 3, pp. 800-810, 2013.
[9] A. Marinoa, F. H. Alvarezb, L. H. Encinasb, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," *Information Sciences,* Vol. 195, No. 15, pp. 91-102, 2012.
[10] E. C. Chang and S. Roy, "Robust Extraction of Secret Bits From Minutiae," *Proceedings of Second International Conference on Biometrics,* pp. 750 - 759, 2007,
[11] A. B. J. Teoh, Y. W. Kuan, S. LEE, "Cancellable Biometrics and Annotations on BioHash," *Pattern Recognition*, Vol. 41, No. 6, pp.2034-2044, 2008.
[12] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, J. Tian, "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme," *Journal of Network and Computer Applications*, Vol. 33, No. 3, pp. 207-220, 2010.
[13] Y. Wang, K. N. Plataniotis, "fuzzy vault for face based cryptographic key generation," *Proceedings of Biometrics Symposium,* pp. 1-6, 2007.
[14] F. Thomas, Z. Xuebing, B. Christoph, "Fuzzy Vault for 3D face recognition systems," *Int. Conf. on Intelligent information hiding and multimedia signal processing*, pp. 1069-1074, 2008.
[15] L. Yiun Joo, P. Kang Ryong, L. Sung Joo, B. Kwanghyuk, K. Jaihie, "A new method for generating an invariant iris private key based on the fuzzy vault system," *IEEE Trans. on System, Man, Cybernetics*, Vol. 38, No. 5, pp.1302-1313, 2008.
[16] K. Moon, Error Correcting Code:Mathematical Methods and Algorithm, *Wiley-Interscience*, 2005
[17] T. Marshall, "Coding of real-number sequences for error correction: a digital signal processing problem," *IEEE Journal of Selected Areas in Communication*, Vol. 2, No. 2, pp. 381-392, 1984.
[18] A. Kumar, A. Makur, "Improved coding-theoretic and subspace-based decoding algorithms for a wider class of DCT and DST codes", *IEEE Trans. on Signal Processing,* Vol. 58, No. 2, pp. 695-708, 2010.
[19] Dae Jong Lee, Yong-Nyuo Shin, Seon-Hong Park, Myung-Geun Chun, "RN-ECC Based Fuzzy Vault for Protecting Fingerprint Templates," *International Journal of Fuzzy Logic and Intelligent Systems,* vol. 11. no. 4, pp. 286-292, 2011.
[20] D. J. Lee, C. K. Song, S. M. Park, M. G. Chun, "Real Fuzzy Vault for Protecting Face Template," *Journal of Korean Institute of Intelligent Systems*, Vol. 23, No. 2, pp. 113-119, 2013.

저 자 소 개

이대종(Dae-Jong Lee)
1995년 : 충북대학교 전기공학과 공학사
1997년 : 충북대학교 전기정보공학과 공학석사
2002년 : 충북대학교 전기정보공학과 공학박사
2006년～2008년 : 충북대학교 충북정보기술 사업단 초빙 조교수

관심분야 : Biometrics, Recognition, Intelligent system
Phone : +82-43-261-2388
E-mail : bigbell@cbnu.ac.kr

전명근(Myung-Geun Chun)
1987년 : 부산대학교 전자공학과 공학사
1989년 : 한국과학기술원 전기및전자공학과 공학석사
1993년 : 한국과학기술원 전기및전자공학과 공학박사
1993년～1996년 : 삼성전자 자동화연구소 선임연구원
2000년～2001년 : University of Alberta 방문 교수
1996～현재: 충북대학교 전자공학부 교수
2008～현재: TTA PG505 표준위원회 의장

관심분야 : Biometrics, Recognition, Soft Computing
Phone : +82-43-261-2388
E-mail : mgchun@cbnu.ac.kr