지문을 이용한 생체 인증방식의 동향

김형균*, 황정연**, 김수형* **, 진승헌* **
*과학기술연합대학원대학교 정보보호공학
**한국전자통신 연구원
e-mail:kyun91@etri.re.kr

A Review of Biometric authentication using Fingerprint

Hyung-Kyun Kim*, Jung-Yeon Hwang**, Soo-hyung Kim* **,
Seung-Hun Jin* **
*Division of information security, University Of Science and Technology
**Electronics and Telecommunications Research InstituteDept of Computer

요 약

최근 기존에 사용하던 패스워드, PIN의 취약성으로 인해 개인정보 유출, 도난 등 다양한 문제가 발생하고 있다. 이를 대체할 목적으로 사람의 신체를 이용한 바이오 인증 기술이 떠오르고 있으며, 많은 연구를 거치고 있다. 그러나 사람의 바이오 정보는 외부에 노출 될 시, 이를 복구할 방법이 없기 때문에 개인정보 보호가 필수적이다. 본 논문에서는 바이오 인식 기술 중 지문을 기반으로 사용자 매칭 기법과 개인 프라이버시 보호를 위한 템플릿 구성방법에 대한 동향을 살펴본다.

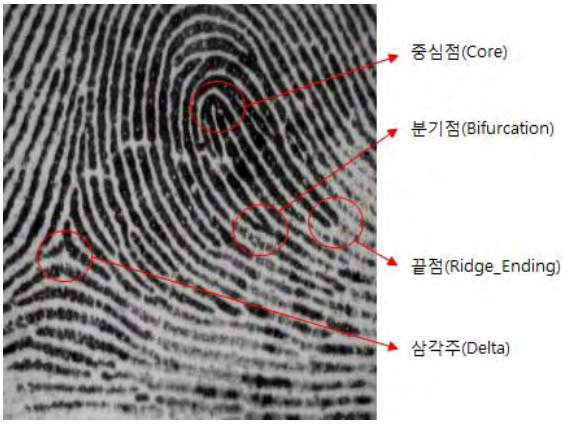
1. 서론

사회가 점차 고도화된 정보화 사회를 향해 거쳐 가면서 인터넷을 통해 사람들이 얻고자 하는 정보에 접근하는 방법도 편리해졌다. 이에 따라, 사람들이 자주 사용하는 카드정보, 개인 정보들이 온라인상에서 도난당하는 경우가 급증하였으며, 기존에 사용하는 PIN번호, 패스워드 등의 사용자 인증 방법으로는 더 이상 정보를 안전하게 보관할 수 없게 되었다. 이를 방지하기 위해 최근 떠오르는 방법으로는 사용자의 바이오 정보를 이용하여 자신을 인증 하는 것이다. 바이오 인증에는 다양한 신체 정보 또는 행동 패턴 정보를 사용할 수 있는데 예로는 사람의 정맥, 얼굴 모양, 음성, 홍채, 지문 등 여러 신체부위가 존재 하고, 사람의 걷는 패턴, 키스트로크 등이 있다. 바이오 인증은 다음과 같은 편리함이 있다. 신체의 부위와 행동 패턴을 사용함으로서 기억할 필요가 없으며 타인에게 도난당할 위험이 없다. 그러나 타인에게 자신의 바이오 정보가 누출되었을 시에는 심각한 위험이 된다. 사용자의 바이오 정보는 임의로 변경이 불가능하기 때문에 타인에게 누출 시, 누출된 정보는 재사용 할 수 없다. 따라서 사용자의 바이오 정보는 안전하게 가공, 처리, 보관이 이루어져야 한다.

본 논문에서는 바이오 정보 중 지문 정보에 대한 처리 기법과 보관 기법에 대해 최근 연구 동향을 설명한다.

2.. 지문 정보

지문 정보는 개개인의 고유한 신체적 특징이다. 지문이란 손가락 끝마디 안쪽에 있는 땀샘이 융기하여 생겨난 소용돌이 모양의 패턴이다. 국제표준화기구 ISO/IEC 19794-2에 따르면 지문 특징 정보는 다음과 같이 나타 낼 수 있다.



(그림 1) 지문 특징 점과 특이 점

지문 정보는 2가지로 나눌 수 있다.[2] 특징 점과 특이 점이다. (그림 1)과 같이 2가지 특징 점으로 분기점, 끝점, 이 있고, 특이점으로는 중심점과 삼각주 2가지가 있다. 분기점은 융선 이 갈라지는 점이고, 끝점은 융선이 끊어지

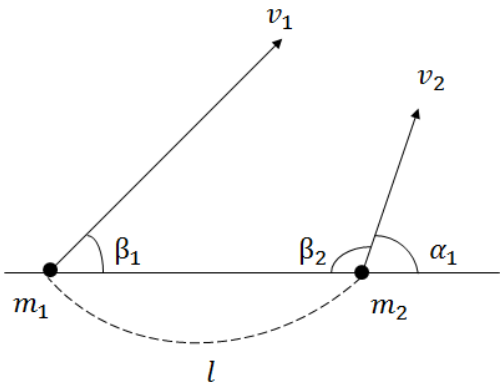
는 점이다. 분기점과 특이점을 또한 minutiae라 부르기도 한다. minutiae에는 다음과 같은 정보를 포함하고 있다. minutiae의 x좌표, y좌표, 수평선과 분기점 또는 끝점이 이루는 사이 각도, minutiae가 분기점인지 끝점인지를 구별하는 Type이 있다. 중심점은 굴곡이 위쪽으로 가장 큰 곳이며, 삼각주는 그림과 같이 융선이 세 가지 방향에서 모이는 곳이다. 특징 점과 특이 점 중 주로 특징점이 주가 되고 특이점이 보조로서 많이 사용되어진다.

3. 지문 정보 매칭 기법

본 장에서는 앞장에서 지문 이미지 정보로부터 얻은 지문 특징 점들을 이용하여 사용자 매칭을 하는 기법을 소개 한다. 사용자 매칭 기법에는 여러 기법들이 있다. 이 중 일부 매칭 기법을 소개한다.

3.1 Using Minutiae Triangulation 기법

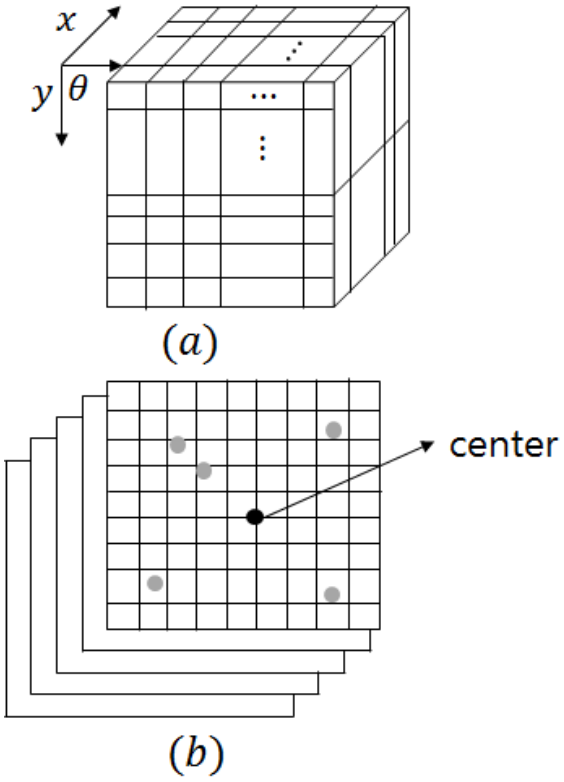
Minutiae Triangulation 기법[3]은 두 개의 minutiae들 간의 길이와 각도를 이용하는 기법이다. 그림()에서 $m1, m2$는 각각의 minutiae이다. 이 두 minutiae 사이의 픽셀 길이를 l이라 하고, l선분과 각 minutiae의 벡터 방향과의 각도를 β_1, β_2라 정의한다. 또한, α값은 v_1, v_2가 이루는 각도의 차이다. 위에서 구한 $l, \alpha, \beta_1, \beta_2$ 값을 이용해 일정 길이의 비트 스트링을 만들 수 있다. 비트 스트링의 개수는 총 n개의 minutiae가 존재한다고 가정할 때, ${}_nC_2$ 개의 수가 존재한다. 이를 비교하여 사용자의 지문 매칭 확인을 할 수 있다.



(그림 2) Features extracted from minutiae

3.2 Minutiae-based bit-string 기법

Minutiae-based bit-string 기법[4]은 minutiae의 4가지 정보(x좌표, y좌표, 각도, Type)를 이용한 방법이다. (그림 3)과 같이 지문 이미지의 가로길이와 세로길이를 2배, 깊이 2π의 길이를 가진 3차원 직육면체 T ($W \times H \times Z$)를 생성한다. 생성된 직육면체를 일정 크기의 3차원 직육면체 $T'(w \times h \times z)$로 나눈다. 나누어진 직육면체 T를 위에서 바라보았을 때, 하나의 minutiae를 선택하여 가지고 있는 각도 벡터를 x축과 평행시킨 후, 가장 정 가운데 위치시킨다. 정 가운데 있는 minutiae를 기준으로 다른 minutiae들을 각각 x좌표, y좌표, 각도 방향으로 각 차원 깊이에 위치시킨다. 나누어진 직육면체 T들 안에 minutiae가 존재하면 '1' 그렇지 않으면 '0'의 값을 가지게 한다. 직육면체 T를 3차원 배열이라 하였을 때, 이를 1차원 배열로 나누어 배열안의 값을 비트 스트링으로 나타낸다. 나타내어진 비트 스트링은 사용자의 PIN번호에 따라 다시 재배열 되며 이를 이용하여 추후 사용자의 지문 매칭에 필요한 비트 스트링 패턴에 사용된다.



(그림 3) (a) The 3 dimensional array
(b) The Transformation of minutiae base on reference minutia

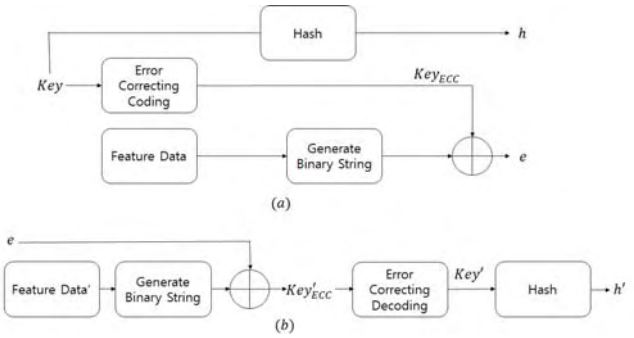
4. 지문 정보 저장 기법

바이오 정보 데이터들은 사용자로부터 데이터를 입력받을 때마다 일정의 잡음이 존재한다. 이런 잡음을 감안하여 바이오 정보들은 등록 시, 템플릿 화 되어 데이터베이스에 저장 된다.[1] 인증 시에는 등록된 템플릿들과 인증 사용자로부터 바이오 데이터들을 비교하여 인증절차를 밟게 된다. 데이터베이스에 저장되는 템플릿들은 도난당하거나 송수신과정에서 누출 될 수 있기 때문에 사용자의 정보를 숨겨 안전한 템플릿을 요구하게 된다. 이러한 방법에는 다음과 같은 3가지 방법이 주로 사용된다. Fuzzy Commitment, Fuzzy Vault, Fuzzy Extractor. 본 장에서는 지문 바이오 데이터들을 템플릿으로 만드는 과정을 설명

한다. 과정에는 등록과정과 인증과정이 있으며 위에 소개된 3가지 기법(Fuzzy Commitment, Fuzzy Vault, Fuzzy Extractor)을 설명한다.

4.1 Fuzzy Commitment Scheme

Fuzzy Commitment[5]는 ECC(Error Correction Code) 개념을 이용한 기법이다. ECC에는 Reed-Solomon(RS)과 Bose-Chaudhuri- Hocguenghem(BCH)을 사용할 수 있다. Fuzzy Commitment기법은 (그림 4)와 같다.



(그림 4) (a) Enrollment procedure
(b) Authentication procedure

등록 과정 :

비밀 키(KEY)를 입력 값으로 ECC를 통해 오류 정정이 가능한 결과 값(KEY_{ECC})을 구한다. 지문 바이오 데이터를 KEY_{ECC}값과 같은 비트 수의 이진 스트링으로 변환시켜 베타적 논리합으로 e를 도출시킨다. 또한, 비밀 키를 해쉬 함수의 입력 값으로 h를 도출한다.

인증 과정 :

등록과정에서와 마찬가지로 인증과정에서의 지문 바이오데이터를 이진 스트링으로 변환시켜 이를 등록과정의 결과 값(e)과 베타적 논리합으로 KEY'_{ECC}을 구한다. 구한 KEY'_{ECC} 값을 에러 정정 코드를 거쳐 비밀 키(KEY')를 구하고 이를 해쉬 함수를 거쳐 나온 값(h')과 등록과정의 해쉬 값(h)를 비교하여 인증을 시도한다.

4.2 Fuzzy Vault Scheme

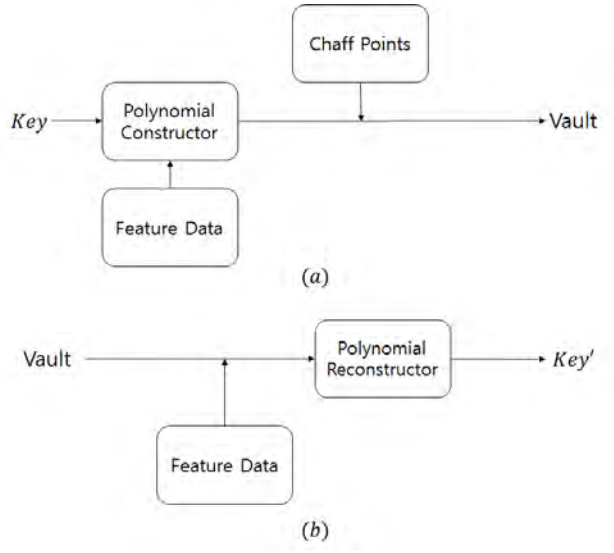
Fuzzy Vault기법은 (그림 5)와 같다.

등록 과정 :

Fuzzy Vaults[6]는 n차 다항식을 사용한다. n차 다항식의 계수는 비밀 키(KEY)가 된다. n차 다항식의 입력 값은 단일 변수로서 지문 바이오 데이터(m)를 이용한다. n차 다항식을 거쳐 나온 값들은 $(m, p(m))$ 형태의 결과 값이 생성되고 나온 결과 값과 거짓 값들, $chaff\ points(x,y)$을 합쳐 Vaults 템플릿을 만들게 된다.

인증 과정 :

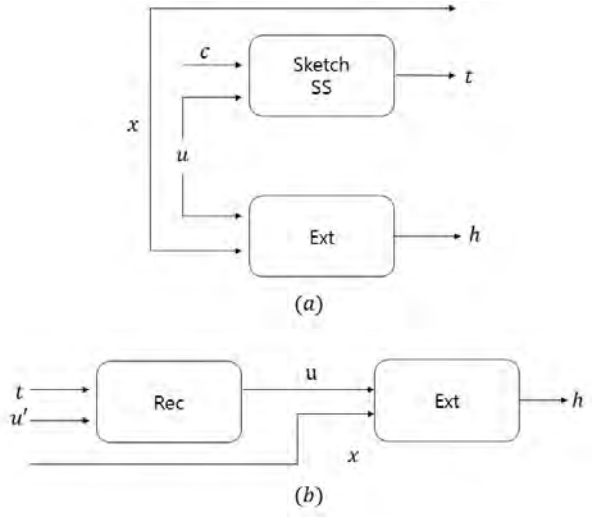
등록과정에서 얻은 Vaults 템플릿에서 많은 볼트 값들 중 인증 시의 지문 바이오 데이터(m')와 매칭 되는 $(m', p(m))$을 구한다. 구한 매칭 점들을 통해 n차 다항식 복원을 시도하여 비밀 키(KEY')값을 얻을 수 있다.



(그림 5) (a) Enrollment procedure
(b) Authentication procedure

4.3 Fuzzy Extractor Scheme

Fuzzy Extractor[7]는 Secure sketch 기법을 이용한다. Secure Sketch는 두 가지 모듈을 사용한다. Sketch SS라는 모듈과 Rec라는 모듈이다.



(그림 6) (a) Enrollment procedure
(b) Authentication procedure

등록과정 :

Sketch SS에는 b라는 지문 바이오 데이터 비트 스트링이 들어가고 c에는 같은 비트 스트링 길이의 해밍길이가 $2s+1$인 코드가 들어간다. 이 둘을 XOR하여 얻은 값

이 t이다. Extractor모듈의 예로 해쉬 함수를 사용할 수 있다. (그림 6) 과 같이 공개된 값 x와 지문 바이오 데이터 b를 Ext 모듈에 넣어 h값을 도출한다.

인증과정 :

Rec모듈에는 Sketch SS의 결과 값 t와 새로운 지문 바이오 데이터 b'가 들어오고 Rec 모듈을 거친다. Rec모듈은 이 둘을 XOR 하여 새로운 c'을 구한다. 이때 c'의 비트 중 오류 비트가 s개 이하일시, $c = c'$이 가능해 진다. 새로 구해진 c와 t를 다시 XOR 하였을 시, 등록과정에서의 지문 바이오 데이터 b를 구할 수 있으며 공개된 값 x와 b를 Ext 모듈에 넣어 h'을 구한다. 그 후, 등록과정에서 받은 h와 비교를 통해 인증한다.

5. 결론

본 논문에서는 바이오 정보 중 지문 정보에 대해 처리기법과 보관기법에 대하여 설명하였다. 바이오 정보를 이용하는 것은 기존의 패스워드 방식에 비해 장점이 많다 잃어버릴 위험이 없으며 엔트로피도 기존의 패스워드 방식보다 크게 적용하여 보안성도 크다. 이러한 장점을 바탕으로 바이오 시장은 향후 대규모 시장 활성화를 이루어 낼 것으로 전망된다. 그러나 바이오 시장이 활성화하기 위해서는 개인정보 보호기법들을 이용한 안전한 보관기법이 필수적이다. 이와 같은 문제를 해결하고자 현재 반복 사용 가능하지만 복구가 불가능한 바이오 템플릿 생성연구들이 활발히 진행 중이다.

참고문헌

[1] Yong-Nyuo Shin, Yong Jun Lee, Myung Geun Chun. "Biometric Template Security for Personal Information Protection." Journal of Korean Institute of Intelligent Systems, 18.4 (2008.8): 437-444.

[2] S. Prabhakar, A. K. Jain, Jianguo Wang, S. Pankanti and R. Bolle, "Minutia verification and classification for fingerprint matching," Proceedings 15th International Conference on Pattern Recognition. ICPR-2000, Barcelona, 2000, pp. 25-29 vol.1.

[3] Parziale, Giuseppe, and Albert Niel. "A fingerprint matching using minutiae triangulation." Biometric Authentication. Springer Berlin Heidelberg, 2004. 241-248.

[4] Lee, Chulhan, and Jaihie Kim. "Cancelable fingerprint templates using minutiae-based bit-strings." Journal of Network and Computer Applications 33.3 (2010): 236-246.

[5] Juels, Ari, and Martin Wattenberg. "A fuzzy commitment scheme." Proceedings of the 6th ACM conference on Computer and communications security. ACM, 1999.

[6] Juels, Ari, and Madhu Sudan. "A fuzzy vault scheme." Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on. IEEE, 2002.

[7] Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." International conference on the theory and applications of cryptographic techniques. Springer Berlin Heidelberg, 2004.

[Acknowledgement]

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의

지원을 받아 수행된 연구임. (No. 2016-0-00097, 비대면 본인확인을 위한 바이오 공개키 기반구조 기술 개발)