생체 정보를 이용한 암호화 키 생성 장치 및 방법

대표발명자 : 신지선 교수

생체 정보를 이용한 암호화 키 생성 장치 및 방법

□ 기술개요

○ 본 발명은 생체 정보를 이용하여 암호화 키를 생성하는 기술임

○ 데이터 샘플에 포함된 각 사용자들(u_n)에 대한 데이터들의 각 특징(f_i)별 평균(M_i), 및 상기 평균(M_i)에 대한 상기 각 사용자들(u_n)에 대한 데이터들의 각 특징(f_i)별 표준편차(std^i_n)를 계산하고, 각 표준편차(std^i_n)의 평균($meanstd_i$), 및 각 표준편차(std^i_n) 중 최대값($maxstd_i$)을 계산하며, 새로운 사용자에 대한 생체 정보(w)를 입력 받고, 데이터 샘플에 포함된 각 사용자들(u_n)의 평균(M_i), 각 표준편차(std^i_n)의 평균($meanstd_i$), 및 최대값($maxstd_i$) 중 하나 이상을 이용하여 새로운 사용자의 생체 정보(w)를 고유한(unique) 정수값(w_n)으로 변환하며, 변환된 정수값(w_n)에 대응되는 비밀키(sk)를 생성함.

○ 여기서, 새로운 사용자의 생체 정보(w)를 고유한(unique) 정수값(w_n)으로 변환하는 것은, 아래의 수학식 1을 이용하여 생체 정보(w)를 고유값(w_u)으로 변환하고 고유값(w_u)에 기초하여 정수값(w_n)을 생성함.

[수학식 1]

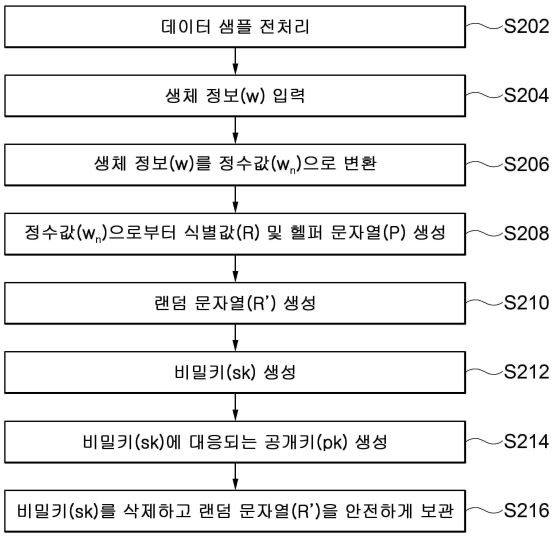
$$\text{if} \quad w = (x_1, \ldots, x_k),$$

$$W_u = \left(\frac{(x_1 - M_1)}{\alpha * meanstd_1}, \frac{(x_2 - M_2)}{\alpha * meanstd_2}, \ldots, \frac{(x_k - M_k)}{\alpha * meanstd_k}\right)$$

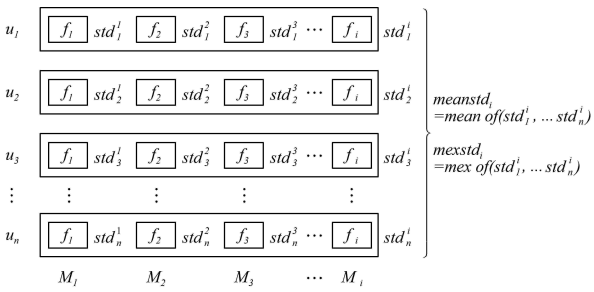
(여기서, x_k는 특징 k에 대 한 생체 정보를 나타내며, α는 양의 정수값을 갖는 계수임)

□ 대표도면

200



<암호화 키 생성 방법>



<데이터 샘플 및 데이터 샘플의 전처리 과정 >

□ 기술의 특징 및 우수성

○ 본 기술은 데이터 샘플에 포함된 각 사용자들에 대한 데이터들의 각 특징별 평균 및 평균에 대한 각 사용자들의 각 특징별 표준편차를 계산하고, 이를 기초로 새롭게 입력되는 생체 정보를 고유한 정수값으로 변환하고 정수값에 대응하는 비밀킬를 생성함에 따라, 생체 정보 기반의 암호화 시스템을 구현할 수 있게 됨.

[표] 기술의 특징 및 우수성

종래기술 문제점	• 생체 정보를 암호화 키로 사용하고자 하는 시도가 증가하고 있으나, 기존에는 **생체 정보가 한 번 노출되면 복구가 불가능**하다는 문제가 있음 • 생체 정보와 같은 퍼지 데이터(fuzzy data)의 경우 노이즈가 포함되거나 그 특성상 입력 시 그 값이 조금씩 달라질 수 있으므로, **입력되는 생체 정보로부터 일정한 값을 얻어낼 필요**가 있음.
해결방안	• 데이터 샘플에 포함된 각 사용자들에 대한 데이터들의 각 특징별 평균, 및 각 특징별 평균에 대한 각 사용자들에 대한 데이터들의 각 특징별 표준 편차에 기초하여 새롭게 입력된 생체 정보를 고유한 정수값으로 변환할 수 있으며, 이에 따라 생체 정보 기반의 비밀키를 생성할 수 있음.
기술의 특징 및 우수성	• **생체 정보가 노출되더라도 비밀키의 안전성을 지킬 수 있음.** • **퍼지 추출기를 통해 입력된 생체 정보의 노이즈를 제거하여 유니크한 값을 생성할 수 있음**

□ 기술의 효과

○ 본 기술은 생체 정보를 비밀키로 하는 공개키 기반 암호화 시스템에서 생체 정보가 노출되더라도 비밀키의 안정성을 지킬 수 있어 암호화 시스템의 보안성을 높일 수 있음.

○ 입력되는 생체 정보를 퍼지 추출기를 통해 노이즈를 제거함으로써, 유니크한 값을 생성할 수 있으며, 데이터 샘플의 전처리 과정에서 입력된 생체 정보로부터 일정한 값을 얻어 낼 수 있음.

□ 기술의 완성도(TRL)

기초 연구 단계		실험 단계		시작품 단계		제품화 단계		사업화
기본원리 파악	기본개념 정립	기능 및 개념 검증	연구실환경 테스트	유사환경 테스트	파일럿현장 테스트	상용모델 개발	실제 환경 최종테스트	상용운영
		●						

□ 기술 키워드

한글키워드	생체 정보, 암호화, 키
영문키워드	biometric information, cryptographic, key

□ 기술의 적용분야

○ 본 기술은 사용자 인증 분야에 사용될 수 있으며, 특히 생체 정보를 이용한 인증 기술에서 암호화 키를 생성하는 분야에 사용 가능함

[표] 적용분야

인증 기술	생체 인증
사용자 인증	암호화 키 생성

□ 기술경쟁력

○ 생체 인식 분야에서 생체 정보가 노출되어도 비밀키의 안정성을 지킬 수 있어 암호화 시스템의 보안성이 높음.

□ 기술실시에 따른 기업에서의 이점

○ 사용자 인증 및 보안 업체에서 생체 정보가 노출되어도 비밀키의 안전성을 지킬 수 있는 바, 다른 생체 인증 보안 시스템과 대비하여 보안성에 대해 우수한 경쟁력을 가질 수 있음.

[표] 국내 생체 인증 분야의 SWOT 분석

강점(Strength)	약점(Weakness)
• 전자상거래 활성화로 바이오 인식에 의한 인증 수단 요구 증가 • 인터넷 대중화로 ID 도용 등 사이버 위협 증가에 따른 새로운 인증 수단 요구	• 얼굴, 홍채인식 등의 원천기술 부족 • 시민 단체 반발 등 바이오 정보 거부감 • 협소한 내수시장 및 업체간 과열 경쟁
기회요인(Opportunity)	**위협요인(Threat)**
• 국제통용 ID 카드 도입 확산과 전 세계적인 관심 고조 • 공공보안을 위한 신원확인 수요급증과 함께 바이오인식 시장의 높은 성장률 • 이동, 편리, 보안이 우수한 신원확인 수단으로 바이오 인식 정착화 추세	• 미국, 유럽, 일본 등 조기도입에 따른 일부 국가와 기업제품의 독점 우려 • 국가안보차원에서 선진국 정부마다 바이오 인식 분야에 대한 강력한 지원 • 국외 일부 국가 및 기업에서 핵심 원천기술에 대한 기술적 우위선점

□ 특허현황

구분	발명의 명칭	출원번호 (출원일)	등록번호 (등록일)	출원 국가
1	생체 정보를 이용한 암호화 키 생성 장치 및 방법	10-2018-0038572 (2018.04.03.)	10-1984033 (2019.05.24.)	한국