情報保護學會論文誌
第18卷 第3號, 2008. 6

특성 벡터를 이용한 얼굴 인증 시스템에서 변환된 생체 정보 데이터의 가역성에 대한 보안 문제 분석*

김 군 순[1†], 강 전 일[1], 양 대 헌[1‡], 이 경 희[2]
[1]인하대학교 정보보호연구실, [2]수원대학교 전기공학과

The Security Problem Analysis for Reversibility of Transformed Biometric Information Data on Eigenvector-based Face Authentication*

KoonSoon Kim[1†], Jeonil Kang[1], DaeHun Nyang[1‡], KyungHee Lee[2]
[1]Information Security Research Laboratory, INHA University,
[2]Department of Electrical Engineering, The University of Suwon

요 약

생체 정보 인식은 사용자의 인증을 위한 수단으로써 많은 연구가 진행 되어 오고 있다. 그 중 얼굴 인식 분야에서 특성 벡터를 이용한 사용자의 얼굴 인식 기법이 존재한다. 이 기법은 전체 얼굴 데이터 집합에서 벡터 공간을 만들어 내고 생체 정보 템플릿을 사상시켜 추상화된 데이터를 생성하는 기법이다. 그러나 생체 정보의 보안성을 일컫는 개념인 취소 가능한 특성(Cancelable Feature)을 기대 할 수 는 없다. 이 논문에서는 특성 벡터를 이용한 얼굴 인증 시스템에서 변환된 생체 정보 데이터의 복원에 대한 보안 문제를 지적하고, 예상 가능한 공격 시나리오를 실험을 통해 보인다.

ABSTRACT

The biometrics has been researched as a means for authenticating user's identity. Among the biometrics schemes for face recognition, the eigenvector-based schemes, which use eigenvector made from training data for transforming test data to abstracted data, are widely adopted. From those schemes, however, it is hard to expect cancelable feature, which is a general concept for security in the biometrics. In this paper, we point out the security problem that is the recovery of valuable face information from the abstracted face data and consider a possible attack scenario by showing our experiment results.

Keywords : *Cancelable Biometrics, User Privacy*

접수일 : 2007년 10월 18일; 수정일 : 2008년 1월 29일;
채택일 : 2008년 2월 27일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0028)
† 주저자, soony@seclab.inha.ac.kr
‡ 교신저자, nyang@inha.ac.kr

Ⅰ. 서 론

사용자의 고유한 생체 정보를 이용한 인증은 그 자체가 지닌 휴대성과 더불어 강력한 위조 방지를 장점으로 한다. 하지만 이러한 특성은 단점으로 작용하여 보안에 취약한 인증 구조를 만들어 낸다. 이에 대한 연구 분야로 취소 가능한 특성을 지원하는 생체 정보 인식(Can-

celable Biometrics)[11] 이라는 분야가 연구 되었으나, 현재까지 그 수가 많지 않다[8,9,18,21,22]. 취소 가능성은 두 가지 특성을 만족해야 하는데, 첫째는 사용자의 생체 정보가 공격자에게 노출 되었을 때, 이를 재갱신할 수 있어야 하고, 둘째는 변환된 생체 정보 데이터가 원래의 생체 정보 템플릿으로 복원이 불가능(noninvertible)해야 한다[11].

기본적으로 생체 정보 인식은 동일 사용자의 생체 정보라고 할지라도, 생체 정보의 추출에 있어서 어느 정도의 편차가 존재하기 때문에 암호학적 인증 방식에서 사용되는 일방향 함수의 사용이 불가능하다. 따라서 여타의 인증 방식과는 달리 생체 정보 인증 방식은 다양한 패턴 인식 알고리즘에 기반 하여 구현된다. 그 중에서 특성 벡터(eigenvector)에 기반 하고 있는 알고리즘은 전체 데이터 집합으로부터 각 클래스들이 가지고 있는 정보들을 최대한 반영할 수 있는 벡터 공간을 생성하는 방법으로써 생체 정보 인식 분야에서는 얼굴 인증에 사용되고 있다[12]. 이외에도 신호 처리 및 압축 기법에도 사용되기도 하는데, 이는 데이터를 추상화시키는 특성과 함께 추상화된 데이터를 약간의 데이터 손실을 감수하며 원래의 데이터에 가까운 형태로 복원할 수 있기 때문이다. 그러나 생체 정보의 보안성을 일컫는 개념인 취소 가능한 특성(Cancelable Feature)을 기대 할 수 는 없다. 따라서 생체 정보 인식 시스템에 특성 벡터를 이용한 알고리즘을 그대로 사용하는 경우, 생체 정보 재갱신의 문제와 변환된 생체 정보 데이터의 역변환에 따른 보안 문제를 동시에 지니게 된다.

이 논문에서는 특성 벡터 알고리즘이 사용되는 얼굴 인증 시스템에서 생체 정보 템플릿 복원에 대한 보안 문제를 지적하고, 예상 가능한 공격 시나리오를 실험을 통해 보인다. II 장에서는 생체 정보 인식 보안 분야의 관련 연구를 설명하고, 이를 통해서 이 논문의 신규성을 제시한다. III 장에서는 특성 벡터 알고리즘을 이용한 얼굴 인증에 대해서 간략히 설명한다. IV 장에서는 변환된 생체 정보 데이터로부터 수식 변환을 통한 역변환 원리를 설명한다. V 장에서는 복원된 사용자 템플릿을 이용한 공격 시나리오를 설명한다. VI와 VII 장에서는 실험을 통하여 거짓 인증이 가능한 것을 증명한다.

II. 생체 정보 템플릿 복원에 대한 기존의 관련 연구 분석

취소 가능한 특성을 지원하는 생체 정보 인식(Cancelable Biometrics)에 대한 최초의 언급은 Ratha의 논문 [11]이다. 이 논문은 생체 정보가 사용자의 인증을 위해서 사용되는 경우에 발생할 수 있는 프라이버시 침해 문제를 언급하고, 이를 해결하기 위한 방법론을 제시하였다. 논문에서 담고 있는 방법론은 암호학 분야에서 오래전부터 응용된 격자 변형(Grid Morphing)이나 블록 치환(Block Permutation)를 이용한 변형 함수를 제시하였고, 이상적으로는 비가역성(noninvertible)을 만족해야 한다는 전제를 달았다. 그러나 변형 함수를 실제로 구현하기 위한 구체적인 기법을 제시하지는 못한 채, 개념적인 언급 수준에서 그쳤다. 논문 [7]은 취소 가능한 특성을 지원하는 생체 정보 인식 시스템을 설계할 경우에 고려해야할 정책 사항을 다루고 있을 뿐, 어떤 변형 함수가 보다 효율적인지에 대한 통계적 근거조차 존재하지 않는다고 지적한 바 있다.

변형 함수에 대한 보다 구체적인 구현 사항을 다룬 연구는, PIN[8]과 Fuzzy Vault 기법[3,18,21] 그리고 바이오 해싱(Bio-Hashing)[9]이다. 생체 정보 보호를 위한 연구는 생체 정보로부터 일관된 사용자 키를 계산하여 저장하는 암호학적 접근(cryptographic approach)[3,9,18,21]과 생체 정보 자체를 안전하게 저장하고 이용하려는 생체 인식적 접근(biometrics approach)[8, 11]으로 나눌 수 있다.

Fuzzy Vault 기법은 사용자의 지문 생체 정보를 인증을 이용할 경우에, 지문 생체 정보(minutiae)를 임의의 Vault에 담고 있는 것으로 생체 정보를 안전하게 보호하는 기법이다. 또한 취소 가능한 특성의 지원이 필요한 경우 Vault를 다시 재생성 함으로써, 이를 해결할 수 있다. 그러나 이 기법은 지문에 국한된 경우이고, 얼굴에 적용된 실용적인 연구 결과는 발표되지 않았다.

바이오 해싱(Bio-Hashing)[9]은 얼굴 데이터 집합으로부터 특징을 추출하고 사용자 토큰(user token)을 이용하여 인증을 위한 일관된 키를 계산해내는 기법이다. 이론적으로는 변환된 도메인 상에서 키 정보를 비교하여 인증을 수행하면서, 사용자 토큰 정보를 변경함으로써 취소 가능한 특성의 지원을 기대할 수 있다. 그러나 사용자 인증에 대한 의존도가 사용자의 생체 정보에 의한 것인지 일종의 필터의 기능을 하는 사용자 토큰에 의한 것인지 증명된 바가 없다. 또한 비밀 키인 사용자 토큰 정보가 유출될 경우, 키 계산을 위한 한계치 변환의 역변환 과정에서 정보의 손실이 발생하지만 부분적으로 생체정보의 복원이 가능할 것으로 보인다.

한편 국내에서는, 사용자 패스워드를 이용하여 특성 행렬을 치환 변환하여 저장하는 취소 가능한 얼굴 인증 시스템을 제시한바 있다[1,2,22].

이처럼 취소 가능한 특성을 지원하는 생체 정보 인식에 대한 대부분의 연구들은, 사용자의 생체 정보가 공격자에게 노출 되었을 경우를 대비한 생체 정보 재갱신에 초점이 맞추어져 있고, 생체 정보의 복원에 대한 지적은 변형 함수가 역변환이 불가능해야한다는 상식적인 언급 수준에 불과할 뿐, 어떠한 실험적인 예를 보여준 적이 없다. 또한 생체 정보의 공격 방법에 대한 모델은 생체 정보 시스템의 전반적인 과정과 기기(device)상에서 발생할 수 있는 데이터 유출에 대한 지적이며[7,11], 생체 정보 인증 프로토콜의 고찰에 근거한 공격 기법을 제시한 연구 역시 발표되지 않았다.

이 논문은 특성 벡터를 이용한 얼굴 생체 정보 시스템에서 발생 가능한 템플릿 복원에 대한 보안 문제를 지적하고, 구체적인 실험을 통해서 보안 취약성의 문제를 분석한다.

Ⅲ. 특성 벡터를 이용한 얼굴 인증 기법

얼굴 인식을 위한 두 가지 기법이 존재한다. 하나는 선형 방식이고 다른 하나는 비선형 방식이다. 선형 방식은 전체 데이터 집합으로부터 특징을 추출하기 위하여 특성 벡터를 사용한다. 비선형 방식은 일반적으로 사람의 신경 구조를 모방한 신경망을 사용한다. 비선형 방식은 높은 인식률을 보이지만, 선형 방식에 비하여 샘플 데이터를 비교하는데 많은 시간을 필요로 한다. 이 논문에서 설명하는 특성 벡터 알고리즘은 선형 방식에 해당한다.

전체 데이터 집합에서 구해지는 특성 벡터는 두 가지 역활을 한다. 데이터 특성을 유지하면서 데이터를 추상화된 데이터로 변환하여 데이터의 크기를 줄이는 동시에 벡터 간의 유사도 측정을 위하여 거리 측정이 수행될 때 발생하는 연산 비용을 줄인다. 또한 분류(classifier)의 역할로서 전체 데이터 집합에서 각 클래스 간의 유사도를 증가시키고 상대적으로 다른 클래스 간의 차이를 두드러지게 한다. 이러한 특성 벡터 U를 구하기 위한 방법으로 PCA(Principal Component Analysis)[12-14]와 LDA(Linear Discriminant Analysis)[4,6,10,16,17,19,20]를 사용할 수 있다.

$X=\{\Gamma_1, \Gamma_2, \Gamma_3, \ldots \Gamma_N\}$를 N개의 샘플 이미지 집합이라고 하자. 각 샘플 이미지는 n-차원 벡터로 나타낼 수 있다. 그리고 m-차원의 특징 행렬 $Y \in \mathbb{R}^{m \times N}$은 다음과 같이 정의한다.

$$Y = UX \tag{1}$$

그러면 $U \in \mathbb{R}^{m \times n}$는 n-차원의 이미지 공간을 m-차원의 이미지 공간으로 변환시키는 사상 행렬(Projection Matrix)이다. 각 테스트 이미지 $\Gamma_i \in \mathbb{R}^n$는 특징을 대변하는 $\Omega_i \in \mathbb{R}^m$를 가진다.

$$\Omega_i = U\Gamma_i \tag{2}$$

이때 사상 행렬 U를 만드는 다양한 방법이 존재한다. ICA(Independent Component Analysis)[12] 또는 PCA는 수집된 데이터로부터 일반적인 특징을 추출함으로서, 얼굴 데이터로부터 불필요한 정보를 줄이는데 사용될 수 있다. 전체 분산 행렬 S_t는 다음과 같이 정의된다.

$$S_t = \sum_{i=1}^{N} (\Gamma_i - \Psi)(\Gamma_i - \Psi)^T \tag{3}$$

$\Psi \in \mathbb{R}^n$는 모든 샘플 이미지의 평균 이미지이다. 그리고 PCA를 사용하여 얻어지는 U는 변환된 특징 행렬 $|U^T S_t U|$를 최대화하는 기능을 한다.

$$U_{opt} = \arg\max_U |U^T S_t U| = [u_1, u_2, \ldots, u_m] \tag{4}$$

u_i는 S_t의 m개의 큰 특성값(eigenvalue)과 일치하는, n-차원의 특성 벡터 집합이다, FLD(Fisher's Linear Discriminant)[17] 또는 LDA는 다른 클래스간의 거리를 최대화하고, 같은 클래스 내 이미지들 간의 거리를 최소화한다. $X=\{X_i\}_{i=1}^{C}$는 C개의 샘플 클래스의 집합이고, $X_i=\{\Gamma_{ij}\}_{j=1}^{C_i}$는 각 C_i의 샘플 이미지들의 클래스이다. 전체 샘플 이미지의 수는 $N=\sum_{i=1}^{C} C_i$ 이다.

LDA에서는 다른 클래스 간의 분산 행렬 S_b와 같은 클래스내의 분산 행렬 S_w는 다음과 같이 정의한다.

$$S_b = \frac{1}{N}\sum_{i=1}^{C} C_i(\Gamma_i - \Psi)(\Gamma_i - \Psi)^T \tag{5}$$

$$S_w = \frac{1}{N}\sum_{i=1}^{C}\sum_{j=1}^{C_i}(\Gamma_{ij}-\Psi_i)(\Gamma_{ij}-\Psi_i)^T \quad (6)$$

Ψ_i는 i번째 클래스 X_i의 평균이다. LDA에서 최적의 U는 같은 클래스내의 분산 행렬분에 다른 클래스 간의 분산 행렬의 비율을 최대화함으로서 구할 수 있다.

$$U_{opt} = \arg\max_U \frac{|U^T S_b U|}{|U^T S_w U|} = [u_1, u_2, \ldots, u_m] \quad (7)$$

특성 벡터 U가 구해지고 나면, 각 샘플 이미지 Γ에서 모든 샘플 이미지의 평균 Ψ를 뺀 벡터를 U^T의 공간에 사상시킨다. 계산된 Ω는 추상화 된 생체 정보의 데이터다.

$$U^T(\Gamma-\Psi) = \Omega \quad (8)$$

Ω_i와 Ω간의 모든 거리를 계산한 후, Ω_i와 Ω간의 거리가 가장 근접한 값을 찾아서 테스트 이미지 Γ에 대한 j-번째 이미지를 구할 수 있다. 이 때 만약 어떠한 한계치 값 θ_ϵ에 대해서 $\| \Omega_i - \Omega \| > \theta_\epsilon$ 라면, 테스트 이미지 Γ를 '알 수 없음'으로 분류한다.

Ⅳ. 변환된 생체 정보 데이터의 역변환 과정

공격자가 U와 Ω 그리고 Ψ를 얻을 수 있다면, 수식 (8)에서부터 변환된 수식 (9)을 통하여 원본에 가까운 생체 정보 템플릿 Γ를 복원할 수 있다. 이때 U는 정방 행렬이 아니므로, $(U^T)^{-1}$를 구하기 위해서는 의사 역 변환(pseudo inverse) 연산을 수행해야 한다.

$$(U^T)^{-1}\Omega + \Psi = \Gamma_i \quad (9)$$

Ω는 각 템플릿의 특징을 반영하는 추상화한 데이터이기 때문에, 본래의 템플릿 Γ의 형태로 복원하기 위해서는 데이터 손실이 발생하게 된다. 손실률의 정도에 따라서 복원된 템플릿을 거짓 인증에 이용할 수 있을지가 결정된다.

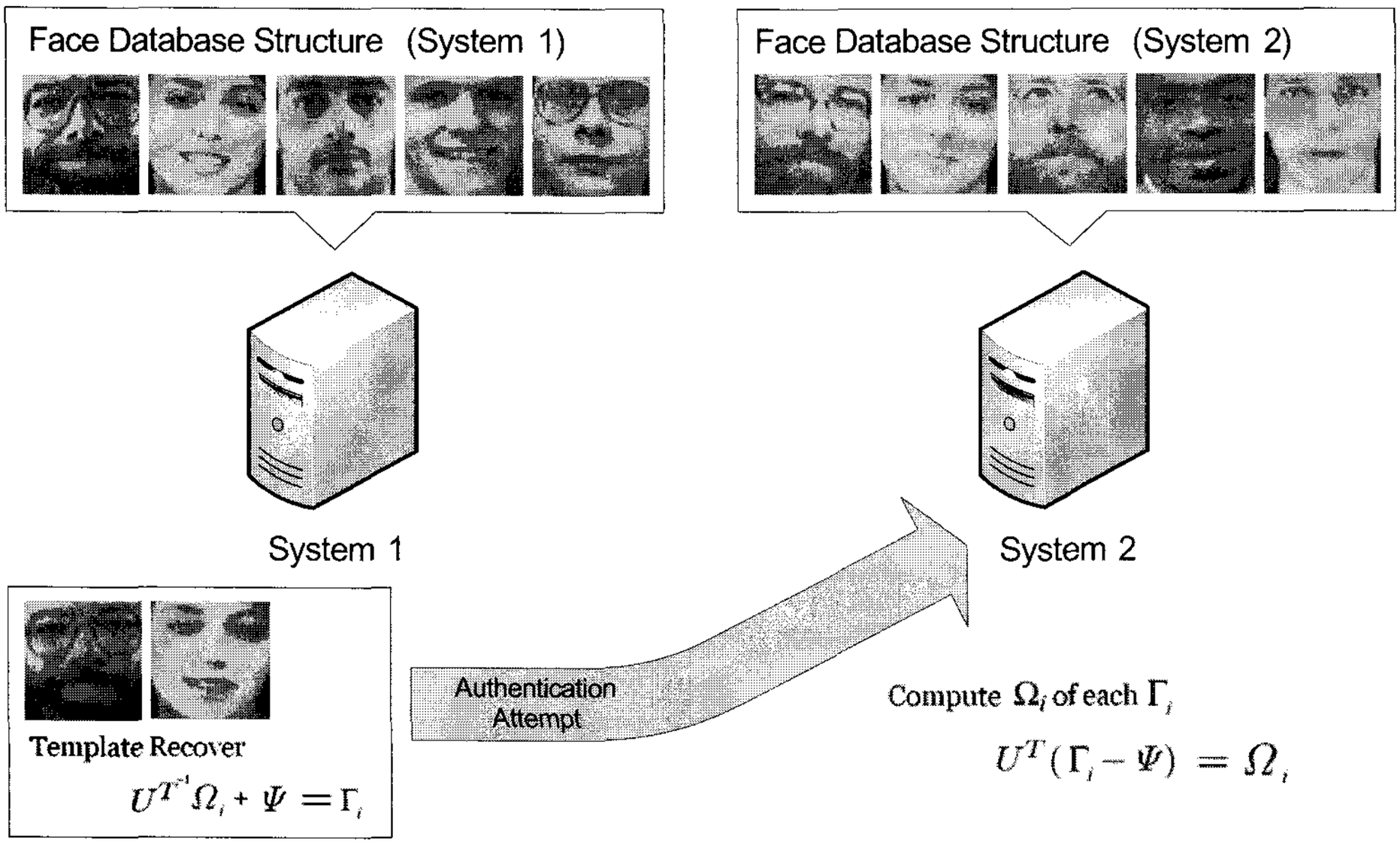
[그림 1]은 ORL 데이터베이스의 원본 템플릿과 복원시킨 템플릿이다. 복원된 템플릿을 생성하기 위해서, ORL 데이터베이스의 전체 템플릿 데이터에 대한 특성 벡터 U를 계산해 내고, 이에 원본 데이터 템플릿 Γ에 평균 데이터 Ψ를 뺀 데이터를 사상시켜 각각의 추상화된 데이터 Ω를 얻는다. 이 후에, 수식 (9)의 과정을 거쳐서, 전체 데이터 수만큼의 복원된 템플릿을 생성하였다. [그림 1]의 복원된 템플릿은 그 중에서 앞의 10명의 임의 자세를 선정하여 보였다. 이 때, 특성 벡터 U를 계산하기 위한 방법으로, PCA와 R-LDA를 사용하고 복원 템플릿의 결과를 비교하였다.

시각적인 결과를 미루어볼 때, PCA를 이용한 경우의 복원된 템플릿의 왜곡이 근소하게 적다. 인식을 하는 경우에는 LDA가 PCA보다 높은 인식률을 나타내지만, 템플릿 복원의 경우에는 PCA가 보다 나은 방법일 수 있다. 이는 PCA가 데이터의 최적 표현의 견지에서 데이터를 축소하는 방법인데 반하여, LDA는 데이터의 최적 분류의 견지에서 데이터를 축소하는 방법이기 때문이다[10].

Ⅴ. 가능한 공격 시나리오

얼굴 인증 시스템은 여러 곳에서 도입할 수 있기 때문에, 특정 사용자의 생체 정보가 여러 인증 시스템에 등록 되어 있을 수 있다. 따라서 복원된 템플릿을 이용

〔그림 1〕 ORL 데이터 베이스의 원본 템플릿과 복원된 템플릿



〔그림 2〕 복원된 사용자의 얼굴 템플릿을 이용한 거짓 인증 시나리오

한 인증 공격은 단순히 해당 시스템에만 국한된 것이 아니라, 다른 인증 시스템에서도 가능하다. [그림 2]는 가능한 공격 시나리오를 나타낸다. 공격자가 보안이 취약한 시스템에서 특정 사용자의 생체 정보 템플릿을 복원할 수 있다면, 복원된 템플릿이 중복 구성되어 있는 다른 시스템에도 거짓 인증을 시도할 수 있다. 이 경우 두 시스템 간의 데이터 구성에 차이가 존재하므로, 인증 과정에서 다른 데이터 집합에서 구해진 특성 벡터 U가 추상화 된 데이터 Ω의 편차를 크게 만들어서 거짓 인증을 막을 수 있을지는 전적으로 U의 분류(classification) 역할에 달려있다.

특성 벡터 U는 전체 데이터 집합의 공통된 특징을 추출한 값이기 때문에, 각기 다른 클래스 집합으로 구성되어 있는 시스템일수록 계산된 U의 편차가 크다. 반대로 분산된 시스템 간의 데이터 집합의 유사 정도가 높아질수록 U의 유사도가 높아지기 때문에, 복원된 템플릿을 이용한 인증 공격 시에 더 높은 인증 성공률을 보일 것으로 추정할 수 있다.

따라서 특성 벡터 알고리즘의 데이터 가역성을 이용한 거짓 인증이 성공하기 위해서는, 템플릿의 역변환 과정에서 발생하는 순수한 손실률과 분산된 인증 시스템의 특성 벡터 U의 편차를 인증에 유효한 수준으로 극복할 수 있어야 한다. 이 논문에서는 실험을 통해서 이러한 공격 시나리오가 가능한지를 보인다.

Ⅵ. 실험 조건

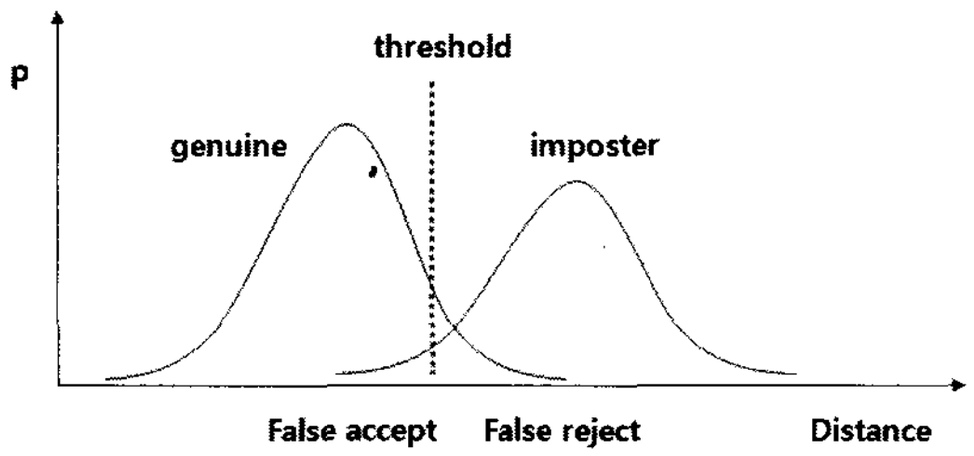
실험은 특성 벡터 추출 알고리즘 중 하나인 R-LDA[17]를 이용한 얼굴 인증 시스템을 가정하였다. 얼굴 데이터베이스는 ORL(Olivetti Research Lab) 데이터베이스를 사용하되, 인증의 일관성을 적용하기 위하여 얼굴 부분만을 50×픽셀로 잘라낸 이미지를 사용하였다. ORL 데이터베이스는 40명의 사용자 클래스로 이루어져 있으며, 각 클래스는 10개의 자세(pose)를 포함하고 있다.

데이터 구성에 따른 U의 편차가 인증 성공률에 미치는 영향력을 측정하기 위하여, ORL 데이터베이스의 구성을 다양하게 적용하였다. 전체 데이터베이스 집합을 20개씩의 클래스로 두 개의 집합으로 나누고, 공유된 클래스의 수를 1부터 9까지 증가시키면서 인증 성공률을 측정하였다. 이 때 클래스에 같은 자세가 중복되지 않도록 5개씩 나누어 공유하였다.

벡터간의 거리 측정 방법은 시티 블록 거리(City Block Distance)[5]를 사용하였다. 시티 블록 거리는 다음과 같이 정의한다.

$$d(a,b) = |a-b| = \sum_{i=1}^{k} |a_i - b_i| \tag{10}$$

인식 기법은 인식을 시도하려는 실험 집합으로 제공



〔그림 3〕 한계치 설정을 위한 데이터 집합의 거리 분포도

되는 클래스(Test Set)와 등록된 모든 클래스 집합(Train Set)의 벡터간 거리가 최소인 것을 찾아내는데 반하여, 인증 기법에서는 인증을 시도하려는 클래스와 등록되어 있는 해당 클래스 집합의 벡터간 거리를 구하고, 구해진 거리가 학습된 한계치(threshold) 내에 포함되어 있는지를 판별한다. 인증 기법은 벡터간의 거리 측정 이후에 필수적으로 한계치 적용을 필요로 한다. 이는 어떠한 보안 기법이 적용되지 않은 상태에서 거짓 인증의 시도를 막는 유일한 방법이다. 또한 인식 기법은 모든 클래스 집합을 검색해야 하기 때문에 본질적으로 클래스의 수와 자세의 수가 많은 데이터베이스에 적용시키기 어려운 문제점을 가지고 있다. 따라서 이 논문에서는 특성 벡터 알고리즘에 인증 기법을 적용하여 실험을 진행하였다.

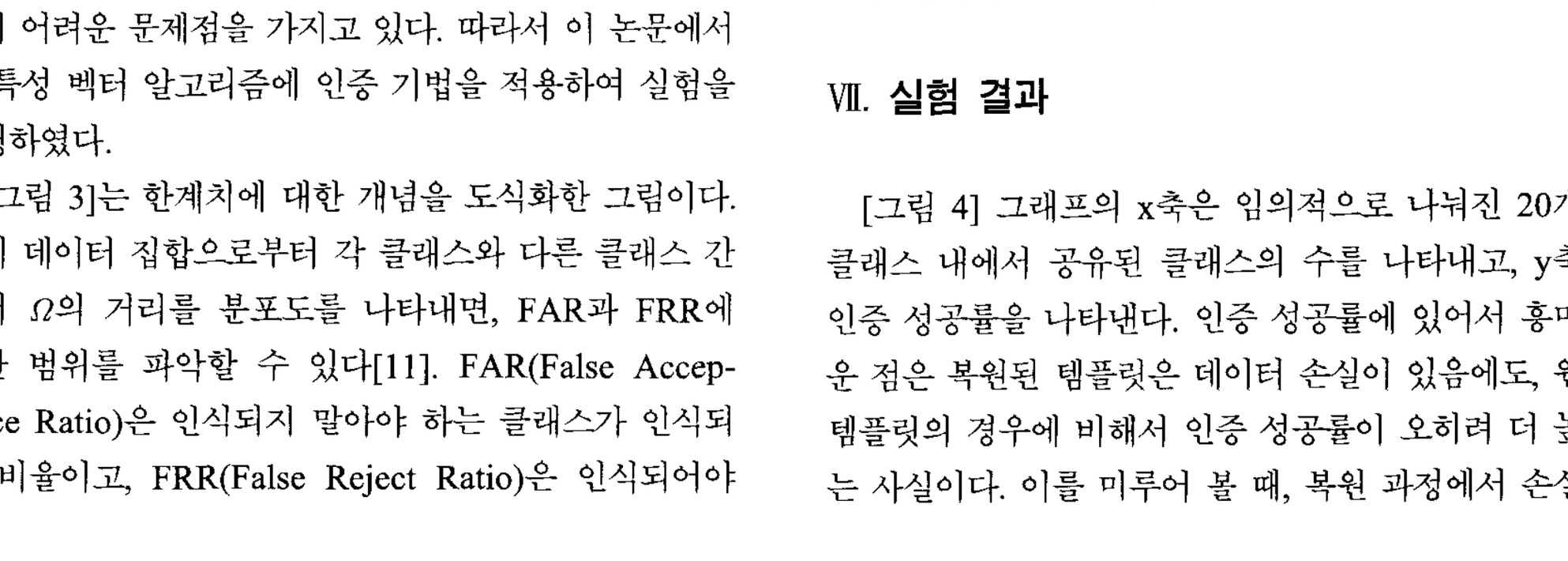
[그림 3]는 한계치에 대한 개념을 도식화한 그림이다. 전체 데이터 집합으로부터 각 클래스와 다른 클래스 간 벡터 Ω의 거리를 분포도를 나타내면, FAR과 FRR에 대한 범위를 파악할 수 있다[11]. FAR(False Acceptance Ratio)은 인식되지 말아야 하는 클래스가 인식되는 비율이고, FRR(False Reject Ratio)은 인식되어야 하는 클래스가 인식되지 못하는 비율이다. 이 범위 내에서 한계치에 대한 조정을 함으로써 인증 성공률을 조정할 수 있다.

한계치를 인증 과정에 정확하게 적용하기 위해서는 각 클래스마다 개별적인 한계치를 구한다. 전체 얼굴 데이터 집합을 학습 집합(Train Set)과 실험 집합(Test Set)으로 나눈 후에 특성 벡터 알고리즘을 통해 구해진 벡터 Ω간의 거리를 구하고 이를 통해서 각 클래스와 다른 클래스 간의 거리 분포도를 구한다. 그리고 클래스별로 구해진 거리 분포도에서 한계치로 설정하고자 하는 해당 거리 지점을 한계치로 설정한다. 이러한 연산을 반복적으로 수행하여 각 클래스의 특징을 반영하는 평균치에 근접한 한계치를 구한다.

이 논문에서 한계치의 설정은 임의적으로 세 가지의 조건으로 정했다. 각 클래스별로 거리 분포도를 구한 이후, 거리차가 0인 곳에서부터 해당 클래스 분포의 90% 지점, 80% 지점 그리고 70% 지점을 한계치로 설정하였다. 한계치의 적용이 엄격할 경우에, 거짓 인증의 시도를 막을 수 있을 것으로 기대 하였고, 실험을 통해서 인증 결과의 변화 추이를 지켜보았다.

Ⅶ. 실험 결과

[그림 4] 그래프의 x축은 임의적으로 나눠진 20개의 클래스 내에서 공유된 클래스의 수를 나타내고, y축은 인증 성공률을 나타낸다. 인증 성공률에 있어서 흥미로운 점은 복원된 템플릿은 데이터 손실이 있음에도, 원본 템플릿의 경우에 비해서 인증 성공률이 오히려 더 높다는 사실이다. 이를 미루어 볼 때, 복원 과정에서 손실된



(a) 원본 템플릿의 인증 성공률 (b) 복원 템플릿의 인증 성공률

〔그림 4〕 한계치 적용 단계에 따른 원본 템플릿과 복원 템플릿 간의 인증 성공률 비교

데이터 자체는 인증 과정에서 불필요한 노이즈로 작용하여 인증에 좋지 않은 영향을 미치는 것을 알 수 있다. 그리고 예상한 바와 같이 두 시스템의 데이터 집합의 유사도가 높을수록 인증 성공률이 높게 나타나는 것을 알 수 있다.

공격 시나리오에 따라 복원된 템플릿을 이용하여 다른 시스템에 인증을 시도할 때 본래의 인증 성공률 이상의 수준으로 인증이 가능하다. 따라서 추가적으로 보안 알고리즘[22]을 특성 벡터 기반의 얼굴 인증 시스템에 적용해야만 이러한 종류의 공격에 대비할 수 있을 것이다.

Ⅷ. 결 론

이 논문에서는 특성 벡터 알고리즘에서 수식 변환을 통한 데이터의 가역성이 얼굴 인증 시스템에서 보안 문제로 작용할 수 있음을 지적하고 실험을 통하여 이를 증명하였다. 이러한 보안 문제의 해결 방안인 변환된 생체 정보 데이터의 비가역성에 대한 연구는 취소 가능한 특성을 지원하는 생체 정보 인식 연구에 속하는 분야이다.

특정 사용자가 공유된 데이터 집합을 가지고 있는 두 개의 얼굴 인증 시스템으로 가정하고, 한 쪽의 시스템에서 특정 사용자의 데이터를 복원시켜, 이를 원래의 데이터와 함께 다른 데이터 시스템에 인증을 시도하였다. 실험 결과에서 나타난 것처럼 복원된 사용자 데이터의 인증 성공률은 원래의 사용자 데이터의 인증 성공률과 동일하거나 그 이상의 수준으로 가능하기 때문에, 특성 벡터 알고리즘을 이용한 얼굴 인증 시스템에서는 이러한 보안 문제를 고려해야 할 것이다.

참고문헌

[1] 강전일, 이경희, 양대헌, "두 가지 보안요소를 사용하는 취소 가능한 얼굴인증 기술", 정보보호학회논문지, 17권 3호, pp. 55-67, 2007. 06

[2] 김군순, 강전일, 이경희, 양대헌, "취소 가능한 얼굴 인식을 지원하는 치환 변환 기법에 대한 고찰", 정보보호학회논문지, 16권 6호, pp. 37-46, 2006. 12

[3] Ari Juels and Madhu Sudan. "A fuzzy commitment scheme." In ACM Conference on Comptuter and Communications Security, page 28-36, 1999.

[4] L. Chen, H. Liao, M. Ko, J. Lin and G. Yu. "A new LDAbased face recognition system which can solve the small sample size problem", Pattern Recognition, Vol.33, No.10, pp. 1713-1726, 2000.

[5] Wedndy S. Yambor, Bruce A. Draper and J. Ross Beveridge. "Analyzing PCAbased Face Recognition Algorithms : Eigenvector Selection and Distance Measures", 2nd Workshop on Empirical Evaluation in Computer Vision, 2000.

[6] Hua Yu and Jie Yang. "A Direct LDA Algorithm for High-DimensionalData - with Application to Face Recognition", Pattern Recognition, Vol.34, No.10, pp. 2067-2070, Oct. 2001

[7] Michael Braithwaite, Ulf Cahn von Seeln, James Cambier, John Daugman, Randy Glass, Russ Moore, and Ian Scott. "Application-specific bio-metrics templates", In IEEE Workshop on Automatic Identification Advanced Techno- log-ies, pages 167-171, 2002

[8] Mario Savvides, B.V.K. Vijaya Kumar and P.K. Khosla. "Cancelable biometric filters for face recognition", Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th Interna-tional Conference on Vol.3, pp. 922- 925, Aug. 2004

[9] Alwyn Goh and David Ngo Chek Ling. "Computation of cryptographic keys from face biometrics." Communications and Multimedia Security, volume 2828 of Lecture Notes in Computer Science, pages 1-13, Springer, 2003.

[10] Peter N. Belhumeur, Joao P. Hespanha and David J. Kriegman. "Eigenfaces vs. Fisherfaces : Recognition Using Class Specific Linear Projection". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.19, No.7, pp. 711-720, July 1997

[11] N.K. Ratha, J.K. Connell and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems

Journal, Vol.40, No.3, pp. 614-634, 2001

[12] Mattew A. Turk and Alex P. Pentland. "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, Vol. 3, No. 1, pp. 71-86, 1991.

[13] Mattew A. Turk and Alex P. Pentland. "Face Recognition Using Eigenfaces", Computer Vision and Pattern Recognition, 1991. Proceedings CVPR "91., IEEE Computer Society Conference on 3-6 pp. 586 - 591, June 1991

[14] Zhuji and Y.L. Yu. "Face recognition with eigenfaces", Industrial Technology, 1994. Proceedings of the IEEE International Conference on 5-9, pp. 434 - 438, Dec. 1994

[15] Marian Stewart Bartlett, Javier R. Movellan and Terrence J. Sejnowski. "Face Recognition by Independent Component Analysis", IEEE Transactions on Neural Networks, Vol.13, No.6, pp. 1450-1464, Nov. 2002

[16] Juwei Lu, Kostantinos N. Plataniotis and Anastasios N. Venetsanopoulos. "Face Recognition Using LDA-Based Algorithms", IEEE Transactions on Neural Networks, Vol.14, No.1, pp.195-200, Jan. 2003

[17] R. Lotlikar and R. Kothari. "Fractional-step dimensionality reduction", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.22, pp. 623-627, June 2000

[18] Umu Uludag, Sharath Pankanti, and Anil K. Jain. "Fuzzy vault for fingerprints.", AVBPA, volume 3546 of Lecture Notes in Computer Science, page 310-319. Springer, 2005.

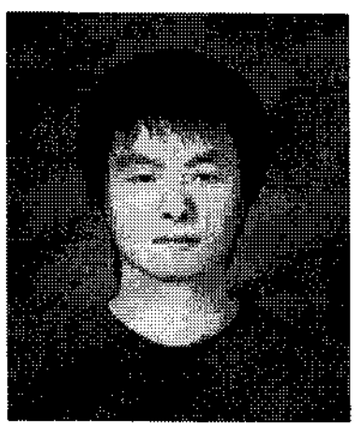
[19] Aleix M. Martinez, and Avinash C. Kak. "PCA versus LDA", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.23, No.2, pp. 228-233, Feb. 2001

[20] Juwei Lu, Kostantinos N. Plataniotis and Anastasios N. Venetsanopoulos. "Regularization Studies of Linear Discriminant Analysis in Small Sample Size Scenarios with Application to Face Recognition", Elsevier Science Inc., Pattern Recognition Letters, Vol.26, Issue 2, pp. 181-191, Jan. 2005

[21] Shenglin Yang and Ingrid M. Verbauwhede. "Secure fuzzy vault based fingerprint verification system." In 38th Asilomar Conference on Signals, Systems, and COmputers, volume 1, page 577-581, Nov. 2004.

[22] Jeonil Kang, DaeHun Nyang and KyungHee Lee, "Two Factor Face Authentication Scheme with Cancelable Feature", the Proceeding of IWBRS 2005, LNCS 3781, pp. 67-75, Oct. 2005

〈著者紹介〉



김 군 순 (KoonSoon Kim) 학생회원
2006년 8월 : 인하대학교 컴퓨터 공학과 졸업
2006년 9월~현재 : 인하대학교 정보통신대학원 석사
<관심분야> 생체 인식 보안, 패턴 인식, HCI

강 전 일 (Jeonil Kang) 학생회원
2003년 2월 : 인하대학교 컴퓨터 공학과 졸업
2006년 2월 : 인하대학교 정보통신대학원 석사
2006년 3월~현재 : 인하대학교 정보통신공학과 박사 과정
<관심분야> RFID 보안, 생체 인식 보안, 무선 센서 네트워크, 무선 인터넷 보안, 웹 인증 보안

양 대 헌 (DaeHun Nyang) 종신회원
1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 정보통신대학원 조교수
<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 경 희 (KyungHee Lee) 정회원
1989년 : 서울대학교 식품영양학과 학사
1993년 : 연세대학교 전산과학과 학사
1998년 : 연세대학교 컴퓨터과학과 석사
2004년 : 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월 : LG소프트(주) 연구원
2000년 12월~2005년 2월 : 한국전자통신연구원 선임연구원
2005년 3월~현재 : 수원대학교 조교수
<관심분야> 영상처리, 컴퓨터비젼, 인공지능, 패턴인식, 생체인식, 얼굴인식, 다중생체인식