情報保護學會論文誌
第16卷 第1號, 2006. 2

# 두 가지 보안 요소를 사용하는 취소 가능한 얼굴 인증 기술

강 전 일,[1†] 양 대 헌,[1‡] 이 경 희[2]
[1]인하대학교 정보보호연구실, [2]수원대학교 전자공학과

# Two Factor Face Authentication Scheme with Cancelable Feature

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

생체정보를 이용하는 인증은 사람에게 편리하지만, 개인 생체 정보의 유출과 같은 보안 문제들은 심각할 수 있다. 이러한 문제 해결을 위해서 취소 가능한 생체 인식 기술을 사용할 수 있지만, 현재까지 단지 몇몇의 인증 시스템만이 알려졌을 뿐이다. 이 논문에서는 패스워드와 얼굴 이미지를 사용하는 얼굴 인증 기술에 대해서 제시한다. 변환된 도메인에서의 매칭 알고리즘을 사용하여, 이 기술은 변환 및 가중치 벡터로 이루어진 템플릿을 자유롭게 바꿀 수 있도록 설계 되었다.

ABSTRACT

Though authentication using biometric techniques has conveniences for people, security problems like the leakage of personal bio-information would be serious. Even if cancelable biometric is a good solution for the problems, only a few biometric authentication scheme with cancelable feature has been published. In this paper, we suggest a face authentication scheme with two security factors: password and face image. Using matching algorithm in the permuted domain, our scheme is designed to be cancelable in the sense that templates that is composed of permutation and weight vector can be changed freely.

**Keywords** : *Biometric, Cancelable, Eigenface, PCA*

## Ⅰ. 서 론

많은 생체 인식 기술들은 인간에게 주는 편리함을 유지하기 위하여 생체 정보를 도난당하지 않도록 연구 되어 왔다. 과거, 일반적으로 생체 인식 기술에서 '매칭'은 템플릿(template)과 얻어진 이미지를 비교하는 작업이며, 그렇기 때문에 몇몇 인식 기술에서 인증을 위한 생체 정보는 템플릿을 이용하여 복원이 가능했다. 하지만 이러한 특징은 보안적인 측면에서 보자면 약점으로 작용한다.

이러한 특징으로 말미암아, 데이터베이스로부터 인코딩된 정보를 취소한다는 N. K. Ratha의 '취소 가능한 생체 인식 기술(cancelable biometric)'[1],

접수일 : 2005년 8월 25일 ; 채택일 : 2005년 12월 9일
† 주저자 : dreamx@seclab.inha.ac.kr
‡ 교신저자 : nyang@inha.ac.kr

의 개념이 필요하게 되었다. 데이터베이스는 템플릿으로써 인코딩된 정보를 가지고 있고, 입력된 정보는 데이터베이스에서와 동일한 함수로 인코딩된 후 이 원래의 정보와 얻어진 정보는 인코딩된 도메인 위에서 비교된다. 이 결과는 인코딩 되지 않은 도메인에서 비교한 결과와 동일하다. 여기에서 인코딩 함수는 복원가능하지 않은 특징(또는, 일방향성)을 갖고 있으면 더욱 좋다. 하지만, 일반적으로 이러한 인코딩 작업도 이미지 처리를 기본으로 하기 때문에 비트 단위의 완전한 임의의 변환을 적용하기 힘들고, 그렇기 때문에 아직도 인코딩 함수에 암호학적 방법을 적용하기란 힘든 일이다. Mario Savvide의 기법[8]은 이러한 취소 가능한 생체 인식 기술의 좋은 예이다.

M. Braithwaite는 비록 어떤 종류의 함수인지 정의하지 않았지만, 매칭을 변환된 도메인 위에서 수행하는 아이디어를 제시하였다. 이 논문에서는 이러한 개념의 예시를 제시할 것이며, 이는 PCA (Principal Component Analysis)[3-6]와 PBKDF (Password-Based Key Derivation Function)[7]을 혼합한 형태의 취소 가능한 생체 인증 기법이 될 것이다. 기본적으로 이 기법은 로컬 시스템 위에서 동작하지만, 이것이 원격 시스템을 통한 인증에서도 적용 가능할 것으로 기대한다.

## II. 특성 얼굴(Eigenface)을 이용한 얼굴 인식

1991년, Mattew A. Turk는 PCA를 기반으로 하는 얼굴 인식 기법[3,4]을 발표하였다. PCA는 데이터의 패턴을 인식하고, 그것들의 유사점과 차이점을 더욱 강조하는 데이터 분석 기법이다[6]. 특성 얼굴(Eigenface)는 PCA 기법을 사용하여 샘플 얼굴 이미지들을 분석하여 얻은 얼굴 공간(face space)이며, 얻은 이미지가 얼굴인지, 얼굴이라면 누구의 얼굴인지에 대해서 구별할 수 있는 특징을 담고 있다.

학습을 위한 얼굴 이미지를 $\Gamma_1$, $\Gamma_2$, $\cdots$, $\Gamma_M$ 라고 하자. 이러한 학습 이미지의 평균을 $\Psi=(\sum_{n=1}^{M}\Gamma_n)/M$ 라 하고, 각각의 편차를 $\Phi_i=\Gamma_i-\Psi$ 라 한다. 행렬 $A=[\Phi_1\Phi_2\cdots\Phi_M]$라 할 때, 얼굴 벡터에 대한 공분산(covariance) 행렬 $C$ 를 구할 수 있다.

$$C=\frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T=AA^T \tag{1}$$

만약 얼굴 이미지의 크기가 $N\times N$ 이라면, 행렬 $C$의 크기는 $N^2\times N^2$가 된다. $N^2$개의 특성 벡터(eigenvector)와 특성 값(eigen value)는 구하는데 너무 어려우므로, $C$를 수학적인 트릭을 사용하여 $M\times M$ 행렬로 바꾸어야만 한다. 이 때 $M$은 $N^2$ 에 비하여 매우 작다. (더 자세한 부분은 [4]에서 볼 수 있다.) 이제, $i=1,\cdots,M$이라고 하고, $M'$ 이 얼굴 탐색을 위해서 경험적으로 얻어진 값이라고 할 때 ($M\le M'$), $u_i$는 특성 벡터를 의미하고, $U=[u_1u_2\cdots u_{M'}]$이다.

$k=1,2,\cdots,N_c$ ($N_c$ 는 얼굴 종류)라고 할 때, 각각의 편차 $\Phi_k$는 특성 벡터 $u_i$의 선형적인 조합으로써 표현할 수 있다.

$$\Omega_k=U^T\Phi_k=U^T(\Gamma_k-\Psi) \tag{2}$$

따라서 각각의 표준화(normalized)된 학습 얼굴 $\Phi_k$는 벡터 $\Omega_k=[u_1^ku_2^k\cdots u_{M'}^k]^T$로 표현할 수 있다.

주어진 알 수 없는 얼굴 이미지 $\Gamma$는 표준화되고, 특성 얼굴 공간에 투영된다.

$$\Omega=U^T(\Gamma-\Psi) \tag{3}$$

벡터 $\Omega=[w_1w_2\cdots w_{M'}]^T$는 입력 얼굴 이미지를 표현하기 위한 각각의 특성 얼굴의 기여도를 의미한다. 어떤 얼굴 부류가 입력 얼굴 이미지를 가장 잘 기술하는지 결정하기 위한 간단한 방법은 어떠한 주어진 한계 값(threshold) $\theta_\epsilon$보다 작은 가장 작으면서 유클리드 거리(Euclidean distance)를 갖는 얼굴 부류 $k$를 찾아내는 것이다.

$$\epsilon_k=\|\Omega-\Omega_k\| \tag{4}$$

만약 $\epsilon_k>\theta_\epsilon$라면, 그 입력 이미지는 '알 수 없음'으로 분류한다.

## III. 변환된 도메인에서의 매칭 작업

이 절에서는 취소 가능한 특징을 갖는 얼굴 인증 기법에 대해서 설명하고자 한다. 이 취소 가능한 특징은 변환된 도메인에서의 매칭 작업을 수행함으로써 구현할 수 있다. 생체 정보는 인증 시스템에서 변환된 형태로 저장되고, 치환 행렬 자체는 어디에도 저장되지 않는다. 그래서 만약 사용자의 템플릿이 공격자에게 노출되었다고 하더라도, 다른 시스템에서 이를 사용하여 인증 받을 수 없다. 또한 공격

자는 템플릿을 저장하고 있던 바로 그 시스템에서도 치환 행렬을 생성하는 사용자 패스워드를 모른다면 이를 이용하여 인증 받을 수 없다. 그런 이유 때문에, 이러한 기법은 패스워드와 얼굴 이미지, '두 가지 보안 요소를 사용하는 인증 시스템'이라고 말한다.

만약 사용자가 생체 정보를 취소하고 싶다면, 사용자는 패스워드를 바꾸는 것으로 자신의 생체 정보를 취소할 수 있다. 더 정확하게, 패스워드를 바꿈으로써 사용자는 생체 정보를 바꿀 수는 없지만 시스템에 저장된 인증 정보를 바꿀 수 있다. 공격자가 원래 얼굴 이미지를 얻는다고 하더라도, 공격자는 각각의 시스템에 맞는 패스워드를 알아내지 않고는 그 시스템에서 인증 받을 수 없다.

### 1. 변환된 도메인에서의 얼굴 인식

특성 얼굴을 사용하는 인증 기법에서 평균 얼굴 $\Psi$, 특성 벡터 $U$, 각각의 가중치 $\Omega_k$는 행렬(matrix) 형태로 다시 표현될 수 있다. 이것들은 미리 계산되어 얼굴 인식 시스템의 데이터베이스에 저장 된다. 만약 인증 시스템에 특성 얼굴 기법이 사용되고, $\Omega_k$가 노출되었다면, 이를 이용하여 누군가 $\epsilon$ 값을 0(영)으로 만들면서 특정한 개인으로 인증을 받을 수도 있을 것이다. 이러기 위해서는, 그는 $\Omega_k$가 $\Gamma_k$에서 계산되기 때문에 $\Gamma_k$를 시스템에게 제공해야만 할 것이다.

하지만, 만약 $\Psi$ , $U$ , $\Omega_k$가 한 번에 노출된다면, 공격자는 얼굴 이미지를 (2)부터 얻어낼 수 있다.

$$\Gamma_k = (UU^T)^{-1} U\Omega_k + \Psi \tag{5}$$

그래서 이것들은 암호학적 해시 함수와 같은 방법으로 안전하게 인코딩 된 후에야 데이터베이스에 저장할 수 있다. 하지만 암호학적 연산은 얼굴 인증 알고리즘이 정확히 얼굴을 매칭 하는 것을 방해한다. 이 문제를 해결하기 위해서 변환된 도메인 위에서라도 매칭 작업에 어떠한 영향을 주지 않는 변환 작업이 필요하다. 특성 얼굴 기법을 사용하는 인증 방법에서, 치환(permutation)은 좋은 선택이다.

**정의 1.** *$f_{c,k}(A)$ 와 $f_{r,k}(A)$ 를 어떠한 행렬 $A$ 를 동일한 방법으로 각각 열(column)과 행(row)으로써 치환하는 함수라고 하자. 여기서 $k$ 는 사용자의 인덱스(index)이다.*

*$P_{c,k}$ 과 $P_{r,k}$ 를 $N\times N$ 치환 행렬이라고 하고, $A$ 를 $N\times 1$ 행렬이라고 하자. 그러면 정의 1에 기술된 함수를 다음과 같이 다시 표현할 수 있다.*

$$f_{c,k}(A) = P_{c,k}A \tag{6}$$

$$f_{r,k}(A) = P_{r,k}A \tag{7}$$

*또한, $P_{c,k}$ 과 $P_{r,k}$ 는 $T$ 를 행렬의 회전이라고 하면 다음과 같은 연관이 있다.*

$$P_{c,k}^T = P_{r,k} \tag{8}$$

**보조정리 1.** *만약 주어진 얼굴 이미지 $\Gamma$, 평균 얼굴 이미지 $\Psi$, 특성 벡터 $U$가 (3)과 같은 관계가 있다면 다음을 만족한다.*

$$U^T(\Gamma-\Psi) = f_{c,k}(U^T)\{f_{r,k}(\Gamma) - f_{r,k}(\Psi)\} \tag{9}$$

**증명.** *$A$와 $B$를 $N\times 1$ 행렬이라 하고, $D$를 $M\times N$ 행렬이라고 하자. 그러면 행렬 연산의 특징에 의해서 다음과 같이 말할 수 있다.*

$$\begin{aligned} f_{r,k}(A-B) &= P_{r,k}(A-B) \\ &= P_{r,k}A - P_{r,k}B \\ &= f_{r,k}(A) - f_{r,k}(B) \end{aligned} \tag{10}$$

*또한, 행렬 $D$ 와 $A$ 를 곱할 때, 이 둘 모두가 $f_{c,k}()$ 나 $f_{r,k}()$ 에 의해서 치환 된다고 하더라도, 같은 치환 순서를 가지고 있기 때문에, $D_{ij}$ (행렬 $D$ 의 행으로 $i$ 번째, 열로 $j$ 번째 원소)는 언제나 $A_i$ (행렬 $A$ 의 $i$ 번째 원소)와 곱해진다. 그래서*

$$DA = f_{c,k}(D)f_{r,k}(A) \tag{11}$$

*식 (10)과 (11)로부터 다음과 같은 식을 얻을 수 있다.*

$$\begin{aligned} D(A-B) &= f_{c,k}(D)f_{r,k}(A-B) \\ &= f_{c,k}\{f_{r,k}(A) - f_{r,k}(B)\} \end{aligned} \tag{12}$$

□

보조정리 1에 따르면, 인증 시스템은 얼굴 이미지와 매칭을 위해서 치환되지 않은 $\Gamma_k$ 대신 치환된 $\Gamma_k$를 사용할 수 있다. 하지만 $\Omega_k$는 다른 행렬들과 차원(dimension)이 다르기 때문에 $f_{c,k}()$나 $f_{r,k}()$으로 치환될 수 없다는 사실에 유의해야 한다. (즉, $U$ 는 $N^2\times M$, $\Psi$와 $\Gamma_k$는 $N^2\times 1$ 이지만, $\Omega_k$는 $M\times 1$ 이다.)

만약 인증 시스템이 누군가에 의해서 해킹 당해서 $\Omega_k$이 노출당한다면, 어떤 사람은 $\Omega_k$이 치환되지 않았다는 부주의함과 다른 데이터베이스에서 사람 별로 $\Omega_k$이 동일할 가능성 때문에 발생할 수 있는 보안 문제에 대해서 염려할지도 모른다. 하지만 $\Omega_k$는 얼굴 이미지 $\Gamma_k$, 특성 얼굴 $U$, 평균 얼굴 $\Psi$들에 의해서 결정되기 때문에, 만약 다른 시스템에서 다른 $\Gamma_k$, $U$, $\Psi$를 사용하게 된다면, 하나의 시스템에서 갖는 $\Omega_k$의 값은 다른 시스템에서 갖는 값과 달라질 것이다.

Mattew A. Turk는 그의 논문[3]에서 "$M$=16인 얼굴 이미지들을 사용한 많은 우리의 실험에서 $M$=7개의 특성 얼굴이 사용되었다. 사용된 특성 얼굴의 수는 특성 값에 의하여 경험적으로 선택되었다."라고 말했다. 만약 $M$=7을 사용할 때 $\Omega_k$을 치환하는 경우, 모든 가능한 $\Omega_k$의 치환 방법은 5040(=7!)가지이고, 이는 전혀 안전하지 않다. 보안 강도를 충분한 수준까지 증가시키기 위해서는 최소한 34나 35가지 정도의 학습 이미지나 특성 값을 사용해야만 한다. ($34! < 2^{128} < 35!$) 하지만 이는 많은 연산을 필요로 하게 된다. 따라서 이 논문에서는 $\Omega_k$을 치환하여 저장하지 않는다.

### 2. 사용자 패스워드로부터 치환 행렬의 추출

시스템은 치환 그 자체에 대해서는 아무런 정보도 가지고 있지 않기 때문에, 얼굴 이미지 입력 장치(acquiring device)는 시스템에게 치환된 얼굴 이미지를 보내주어야 한다는 이야기와 같다. 얼굴 이미지를 치환시키기 위해서, 입력 장치는 사용자로부터 패스워드를 얻고 치환 행렬을 제공해주어야 한다.

안전한 치환 행렬을 얻기 위해서 사용자 패스워드는 PKCS#5[7]에 기술되어 있는 PBKDF (Password-Based Key Derivation Function)와 같은 암호학적 방법을 사용하여 높은 복잡도를 갖는 문자열로 바꾸어야 한다.

**정의 2.** *$D_K()$는 패스워드 기반 키 추출 함수를 의미하고, 이 함수는 무작위의 키 문자열을 반환한다.*

무작위 키 문자열 = $D_K$(사용자 패스워드)

$D_K()$는 완전하게 PKCS#5의 PBKDF를 사용한다. 기본적으로 PKCS#5의 함수들은 해시 함수나 의사 난수 생성기 함수로 이루어져 있고, 이의 역을 구하는 것은 불가능하다.

**정의 3.** *$D_{M_x}()$는 무작위 키 문자열에서부터의 치환 행렬 추출 함수를 의미하고, 이 함수는 $x$의 값에 따라서 열이나 행 단위로 치환된 행렬을 반환한다. $x$는 $r$이나 $c$ 가 될 수 있다. $M$는 어떠한 행렬을 의미한다.*

치환 행렬 = $D_{M_x}$(무작위 키 문자열)

치환 행렬은 단위행렬 $I$를 무작위 키 문자열 *RKS* (Random Key String)를 이용하여 열이나 행으로 치환해서 얻는다. $RKS_{\langle i,j \rangle}$ (RKS⟨i..j⟩라고 표시한다.) 를 무작위 키 문자열에서 정수 형태로 인식할 수 있는 $i$부터 $j$까지의 비트열이라고 하면, 치환 행렬 추출 함수 $D_{M_x}()$는 다음과 같이 동작한다.

```
// RKS : random key string, input
// n : image height * image width
// m : larger integer then upper bound lg n

loop i := 0 to n
 j := RKS⟨i..i+m-1⟩
 if j ⟩= n
 j := j % n
 if x = r
  swap(the i-th row of I, the j-th row of I)
else if x = c
  swap(the i-th column of I, the j-th column of I)
return I
```

$D_{M_x}()$를 사용하여, $P_{ck}$와 $P_{rk}$를 얻을 수 있으며, 치환 함수 $f_{ck}()$와 $f_{rk}()$를 계산할 수 있다. 여기서, 식 (6)과 (7)는 다음과 같이 다시 쓸 수 있다.

$$f_{xk}(A) = D_{M_x}(D_K(\text{사용자 패스워드}))A \qquad (13)$$

## Ⅳ. 취소 가능한 생체 인식 기술을 사용하는 얼굴 인증 기법

### 1. 시스템 요구 사항

만약 시스템에 치환된 $U^{\#}$와 치환된 $\Psi$를 저장한

표 1. 전역 변수와 그에 대한 설명

| 변수 | 설 명 |
|---|---|
| $U_{RR}^{T}$ | $MRK$ 에 $D_{P_r}()$ 를 사용하여 얻어낸 치환 행렬로 치환된 특성 벡터의 모임 |
| $\Psi_{RR}$ | $MRK$ 에 $D_{P_r}()$ 를 사용하여 얻어낸 치환 행렬로 치환된 평균 얼굴 이미지 |

다면, 특성 얼굴 기반 매칭 알고리즘은 치환된 입력 얼굴 이미지들과 함께 잘 동작할 것이다. 그러나 이 경우, 특정 사용자 정보를 저장하기 위해서 요구되는 메모리 용량이 매우 크게 된다. 그래서 시스템에 어떠한 무작위 마스터 키(master random key)로 치환된 하나의 전역 $U_{RR}^{T}$과 $\Psi_{RR}$을 저장하면 특정 사용자 정보는 한 사용자 당 하나의 치환 정보를 저장하는 것으로 충분하다. 이렇게 함으로써, 많은 메모리를 절약할 수 있다. 아래 표에 보이고 있는 전역 변수들은 시스템에 저장되지도 않으며 어떠한 방법으로도 얻어낼 수 없는 $MRK$ (Master Random Key)로 만들어진 치환 행렬로 치환되어 안전하다.

또한 아래 표에 보이고 있는 사용자 계정은 사용자 특정 가중치와 치환 행렬로 이루어져 있다.

결과적으로, 몇 가지 앞에서 기술하였던 식의 변형을 생각해 볼 수 있다.

$$U_{RR}^{T} = D_{M_r}(MRK)\,U^{T} \tag{14}$$

$$\Psi_{RR} = D_{M_r}(MRK)\,\Psi \tag{15}$$

만약, 행렬 $f_{\sigma k}(U^{T})$ 와 $f_{\tau k}(\Psi)$ 이 사용자 패스워드로 생성된 치환 행렬로 치환된 행렬 사용자 특정 행렬이라면

표 2. 사용자 계정 변수와 그에 대한 설명

| 변수 | 설 명 |
|---|---|
| $\Omega_k$ | '사용자 특정 가중치(user specific weight factor)'로, 특성 벡터 $U$와 평균 얼굴 $\Psi$를 사용하여 어떻게 원래의 얼굴 이미지를 복원해내는지 가리키는 값이다. |
| $S_{\tau,k}$ | 얼굴 인식 단계에 사용되는 '사용자 특정 치환 행렬'을 뜻하며 전역 변수들과 곱해져 사용자 특정 변수들을 만들 수 있다. 추가적으로 많은 영(0) 원소를 포함하고 있으므로 압축을 통해서 사이즈를 더 줄일 수도 있다. 또한 $S_{\sigma k}^{T} = S_{\tau k}$의 관계가 있다. |

$$f_{\sigma k}(U^{T}) = D_{M_r}(D_K(\text{사용자 패스워드}))\,U^{T} = S_{\sigma k}\,U_{RR}^{T} \tag{16}$$

$$f_{\tau k}(\Psi) = D_{M_r}(D_K(\text{사용자 패스워드}))\,\Psi = S_{\tau k}\,\Psi_{RR} \tag{17}$$

이다. 따라서 저장해야만 하는 사용자 특정 데이터는 $\Omega_k$와 $S_k$이다.

## 2. 얼굴 인식

이러한 기법을 적용한 시스템에서 사용자가 인증을 받고자 할 때, 그는 그의 얼굴 이미지와 그의 패스워드를 입력 부분(acquiring part)에 제공해야만 한다. 그러한 얼굴 이미지를 $\Gamma$라고 하고 얼굴 이미지 치환 부분(face image permutation part)은 치환된 얼굴 이미지 $\Gamma_P$를 계산해야만 한다.

$$\Gamma_P = D_{M_r}(D_K(\text{사용자 패스워드}))\,\Gamma \tag{18}$$

그런 뒤, 이 치환된 얼굴 이미지는 각각의 사용자

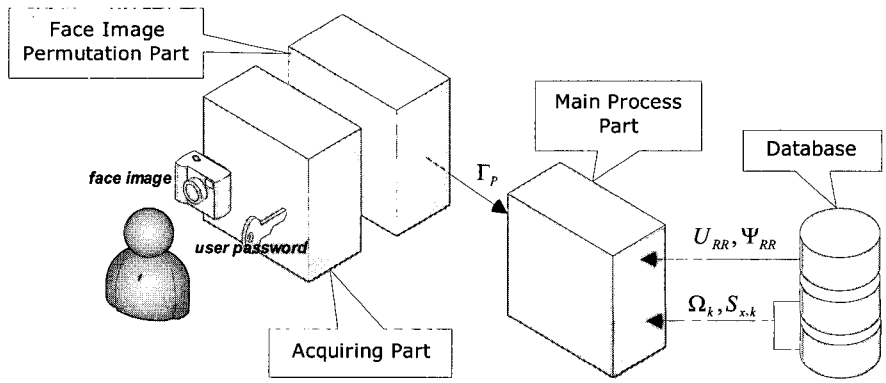


그림 1. 얼굴 인식 및 인증 시스템의 구성

계정을 뒤지며 사용자의 가중치 $\Omega$를 찾는 중앙 처리 부분(main process part)로 보내진다. 각각의 사용자 계정에 대해서, 중앙 처리 부분은 $\Omega$의 후보 $\Omega_k'$를 계산해야만 한다.

$$\begin{aligned}\Omega_k' &= f_{\circ k}(U^T)\{\Gamma_P - f_{\cdot k}(\Psi)\} \\ &= S_{\circ k} U_{RR}^T \{\Gamma_P - S_{\cdot k}\Psi_{RR}\}\end{aligned} \tag{19}$$

그러면 사용자 특정 가중치 $\Omega_k$와 위의 식을 통하여 얻은 $\Omega_k'$ 벡터들과 비교함으로써, 적합한 사용자 계정을 찾아낼 수 있을 것이다.

각각의 계정은 다른 치환 순서를 갖기 때문에, $\Omega_k'$와 $\Omega_k$ 유클리드 거리는 올바른 계정과 그렇지 않은 계정들 사이에 큰 차이를 보일 것이다.

### 3. 템플릿의 취소

여기서 제시되는 기법에서 템플릿은 $(S_{\cdot k},\ \Omega_k)$로 정의된다. 그래서 템플릿의 취소 작업은 $S_{\cdot k}$를 바꾸는 작업과도 같다. 이렇게 패스워드를 바꾸는 작업은 변환되는 과정에서 사용자 얼굴 이미지의 누출을 막기 위하여 어떠한 보안이 필요하다. 어떠한 보안 위협 때문에 사용자가 그의 패스워드를 바꾸고자 할 때, 그는 반드시 그의 패스워드를 시스템에게 새로운 $S_{\cdot k}$를 계산하도록 하기 위해서 제공해야한다. 하지만 만약 이러한 작업이 원격으로 이루어진다면 원형태의 사용자 패스워드나 $D_K$(사용자 패스워드), $D_{M_r}$($D_K$(사용자 패스워드))를 제공하는 행위는 매우 위험하다. 왜냐하면 $\Gamma = P_r^{-1}\Gamma_P$이고 $\Gamma_P$은 인증 과정을 관찰함으로써 얻을 수 있기 때문이다. 따라서 패스워드 정보는 어떠한 세션 키로 안전하게 암호화되었다고 가정한다.

더 나아가, 새로운 패스워드가 적용되는 경우를 생각해야한다. 만약 $U^T$와 $\Psi$이 이 작업 동안 복원된다면, $U^T$와 $\Psi$는 다른 누군가에게 노출될 가능성이 있기 때문에 위험하다. 따라서 다음과 같은 미리 계산된 행렬이 이러한 복원을 막기 위해서 제공되어져야만 할 것이다.

$$\begin{aligned}P_{\neq w}(P_{old})^{-1} = D_{M_r}(D_K(\text{새로운 패스워드})) \\ D_{M_r}^{-1}(D_K(\text{기존 패스워드}))\end{aligned} \tag{20}$$

$D_{M_r}^{-1}()$ 는 무작위 키 문자열로부터 치환 행렬의 역행렬을 계산하는 함수이다. $P_{\neq w}(P_{old})^{-1}$는 분리될 수 없으며 $U_{P_{old}}^T$를 $U_{P_{new}}^T$로, $\Psi_{P_{old}}$를 $\Psi_{P_{new}}$로 바로 바꾸어준다. 그러면, 시스템은 $U_{RR}^T$와 $U_{P_{new}}^T$나 $\Psi_{RR}$와 $\Psi_{P_{new}}$를 이용하여 새로운 $S_{\cdot k}$를 구해야만 한다. (17)에 의하여 다음과 같은 식이 만족한다.

$$\begin{aligned}S_{\circ k} &= U_{P_k}^T (U_{RR}^T)^{-1} \\ &= (\Psi_{P_k}(\Psi_{RR})^{-1})^T = (S_{\cdot k})^T\end{aligned} \tag{21}$$

## V. 보안성 분석

시스템에 참여하는 사용자의 올바른 얼굴을 모르는 공격자는 사용자의 얼굴 이미지를 얻기 위해서 노력하거나, 시스템을 다루기 위한 허가된 권한을 얻고자 할 것이다.

**공격 1.** *$\Gamma_P$로부터의 사용자 얼굴 복원* : 공격자는 치환된 얼굴 이미지 $\Gamma_P$로부터 사용자의 얼굴 이미지를 복구하려고 할지도 모른다. 그러나 이러한 시도는 이미지의 사이즈가 $400(=20\times20)$이나 $900(=30\times30)$정도로 매우 크기 때문에 불가능하다. 이러한 경우와 같은 시도의 복잡도는 약 $400!(=6.4\times10^{865})$이나 $900!(=6.7\times10^{2269})$에 이른다.

**공격 2.** *$U_{RR}^T$ 등에서의 사용자 얼굴 복원* : 시스템을 침입한 해커는 $U_{RR}^T$, $\Psi_{RR}$, $\Omega_k$, $S_{\cdot k}$ 를 얻을 수 있다. (5)를 이용하여 그는 사용자의 얼굴을 복원하려고 할지도 모른다. 그러나 $(U_{RR}U_{RR}^T)^{-1}U_{RR}\Omega_k + \Psi_{RR}$는 치환된 얼굴 이미지 $\Gamma_P$와 동일하다.

**공격 3.** *$U_{RR}^T$ 등에서 변형되지 않은 형태의 $U$나 $\Psi$의 복원* : 만약 공격자가 변형되지 않은 형태의 $U$나 $\Psi$을 복원할 수 있다면, 그는 사용자의 얼굴 이미지를 복원해 낼 수 있을 것이다. 물론, 이러한 이미지는 $U$가 학습 이미지들에 대한 전체 정보를 담고 있지 않기 때문에 눈으로 식별하기에 좋은 이미지는 아니지만 인증을 받는데 무리가 없는 정보이다. 그러나 이러한 시도 또한 얼굴 이미지 $\Gamma_P$ 처럼 행렬의 사이즈가 매우 크기 때문에 불가능해 보인다.

이 논문에서 기술된 기법은 얼굴 이미지의 누출을

허용하지 않지만, 공격자는 시스템에 참여한 사용자의 얼굴 이미지를 다른 곳에서 얻어낼 수도 있을 것이다. 그러면 공격자는 다음과 같은 공격을 시도해 볼 수 있다.

**공격 4.** *사용자 패스워드에 대한 사전 공격* : 제안하는 기법은 사전 공격을 사용하여 사용자의 패스워드를 얻어낼 수 있을 것처럼 보인다. 그러나 이 공격은 로컬 시스템에서는 매우 힘들다. 왜냐하면 공격자는 시스템에 하나, 하나 사전 단어를 입력해야만 하기 때문이다. 여기에 더해서, 시스템 제조자는 사전 공격을 지연시키기 위해서 어떠한 방법을 강구할 수도 있다.

**공격 5.** *유사한 치환 행렬을 생성해내는 패스워드의 발견* : 만약 공격자가 원래의 것에서 몇 개의 열이나 행이 다른 유사한 치환 행렬을 알고 있다면 유클리드 거리의 특성을 이용하여 시스템에 합법적으로 접근할 수 있을 것이다. 그러나 필요한 검색 공간의 크기를 상당히 줄였다고 하더라도 그 크기가 $N$에 따라 유사한 치환 행렬이 2~100개 정도라고 가정했을 때 300!~398!이나 800!~898! 정도일 것이기 때문에 이러한 공격은 불가능하다. 따라서 공격자는 그의 준비된 사전에서 유사한 치환 행렬을 만들어내는 패스워드를 찾기를 기대할지도 모른다. 만약 그가 그러한 패스워드를 찾을 수 있다면, 사전 공격을 위한 시간을 대폭 줄일 수 있다. 하지만 불행하게도, $|Dict|$을 사전의 크기라고 하고 $ds$를 유사도를 결정하는 한계 값이라고 했을 때 그러한 패스워드를 찾는 확률은 불과 $(|Dict|\times(N^2-ds)!)^{-1}$ 이다. 이러한 확률을 가능하게 하는 것은 각각 크기가 다른 검색 공간 때문이다. 사전의 공간은 $|Dict|$, 무작위 키 문자열의 공간은 $2^{N^2+\log_2 N^2}$, 치환 공간은 $N^2!$ 의 크기를 가지며, $|Dict| \ll 2^{N^2+\log_2 N^2} \ll N^2!$ 와 같은 관계가 존재한다.

**공격 6.** *다른 사용자의 얼굴의 발견* : 만약 인증 시스템으로부터 모든 데이터베이스를 훔치는 데에 성공하고, 어떠한 의미에서 공격자가 특정 사용자의 패스워드를 발견해낸다면, 그는 패스워드로부터 치환 행렬의 역행렬을 구한 뒤 $U$와 $\Psi$를 복원해낼 수 있다. 그 뒤에 그는 이것들과 (5)를 이용하여 다른 사용자의 얼굴을 복원해 낼 수 있게 된다. 하지만 우리가 이러한 상황을 가정한다고 하더라도, 공격자는 이렇게 복원해낸 얼굴을 이용하여 같은 인증 방법을 사용하는 다른 시스템이나 바로 그 크랙 당한 시스템이라고 할지라도 공격자가 각각의 경우에 대해서 정확한 패스워드를 모를 경우 복원해낸 얼굴을 이용해서는 인증을 받을 수 없다.

## Ⅵ. 결 론

이 논문에서, 특성 얼굴 기법을 바탕으로 하는 취소 가능한 얼굴 인증 기법을 소개하였다. 이 기법은 생체 인증 시의 보안 문제를 강화하기 위하여 두 가지 보안 요소로 구성되었으며, 그는 각각 치환된 도메인에서의 비교와 사용자 패스워드로부터 생성된 치환 순서이다. 그 뒤 이 기법을 깰 수 있을지도 모르는 몇 가지 공격 방법에 대하여 생각해보았으며, 사용자 얼굴 이미지가 시스템을 해킹함으로써 노출되지 않는다는 가정 하에서 충분히 납득 가능한 어떠한 취약점도 찾아내지 못했다. 만약 사용자의 얼굴 이미지가 다른 곳에서 노출되었다고 하더라도, 공격자는 시스템을 붕괴시킬 정도의 성공적인 공격을 실행할 수 없다. 더 나아가 사용자 패스워드를 안전하게 바꿀 수 있는 방법에 대해서 제시하였다.

좋은 성능과 높은 보안성을 갖는 응용 모델을 만들기 위해서는 특별히 학습 얼굴 이미지의 결과물인 $U$나 $\Psi$에 대한 더 많고 깊은 연구와 확인 작업이 반드시 필요할 것으로 보인다. 왜냐하면 $U$나 $\Psi$는 다른 학습 그룹(즉, 연령, 나라, 인증 등)에 따라 다른 패턴을 가질 것이며, 학습 단계에서 유연성을 가지고 있기 때문이다.

## 참 고 문 헌

[1] N.K. Ratha, J.K. Connell, and R.M. Bolle, "Ehhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, Vol. 40, No. 3, pp. 614-634, 2001

[2] Michael Braithwaite, Ulf Cahn von Seelen, James Cambier, John Daugman, Randy Glass, Russ moore, and

Ian Scott, "Application-Specific Biometric Templates", Iridian Technologies Inc., Proceedings of AutoID, pp. 167-171, 2002

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

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

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

[6] Lindsay I Smith, "A tutorial on Principal Components Analysis", February 1994

[7] "PKCS#5 v2.0: Password-based Cryptography Standard", RSA Laboratories, March 25 1999

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

[9] Anil K. Jain, Umut Uludag and Rein-Lien Hsu, "Hiding a Face in a Fingerprint Image", Proceedings of ICPR, August 2004

[10] Biometric Consortium, http://www.biometrics.org

[11] 문지현, 김학일, "국내 생체 인식 시스템 성능 평가를 위한 표준안 연구", 정보보호학회 논문지 12권 2호 pp 92-101, 2002

[12] 문대성, 길연희, 안도성, 반성범, 정용화, 정교일, "지문 인증을 이용한 보안 토큰 시스템 구현", 정보보호학회논문지, 13권 4호 pp. 63-, 2003

[13] 손기욱, 최영철, 박상준, 원동호, "복구 가능한 패스워드 기반 키 분배 프로토콜", 11권 5호 pp. 89-97, 2001

## 〈著者紹介〉

**강 전 일 (Jeonil Kang) 학생회원**
2003년 2월 : 인하대학교 컴퓨터 공학과 졸업
2004년 3월~현재 : 인하대학교 정보통신대학원 석사과정
〈관심분야〉 RFID 보안

**양 대 헌 (DaeHun Nyang) 정회원**
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)**
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 전임강사
〈관심분야〉 영상처리, 컴퓨터비젼, 인공지능, 패턴인식, 생체인식, 얼굴인식, 다중생체인식