(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년09월06일
(11) 등록번호 10-0755934
(24) 등록일자 2007년08월30일

(51) Int. Cl.
G06K 9/00 (2006.01)
(21) 출원번호 10-2006-0035795
(22) 출원일자 2006년04월20일
심사청구일자 2006년04월20일
(56) 선행기술조사문헌
KR1020030072191 A
(뒷면에 계속)

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초4동 삼풍아파트 3동 405호
강전일
충남 공주시 옥룡동 284-1
(74) 대리인
이원희

전체 청구항 수 : 총 9 항 심사관 : 전창익

(54) 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한생체인식 시스템 및 방법

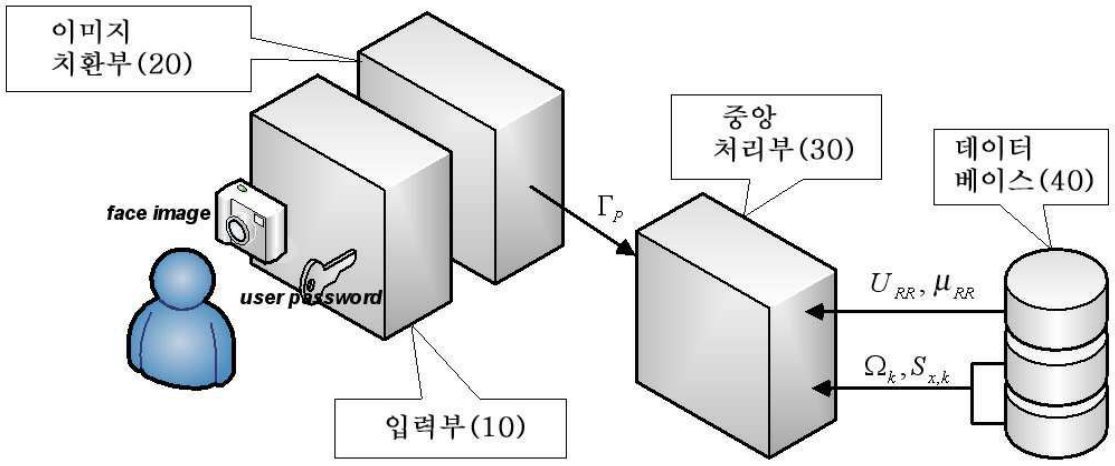
(57) 요 약

본 발명은 전역 변수 및 사용자 특정 가중치와 사용자 특정 치환 행렬을 생체인식을 위한 정보로 사용하며, 사용자 키워드를 바꾸는 것으로 사용자 특정 치환 행렬을 새롭게 갱신함으로써 생체정보를 취소할 수 있는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템 및 방법을 제공한다.

본 발명의 취소가능한 생체인식 방법은 사용자 특정 가중치와 사용자 특정 치환 행렬로 된 템플릿 및 소정 무작위 마스터 키로 치환된 전역 변수를 데이터베이스에 저장하는 제1단계; 입력부를 통해 입력되는 키워드를 무작위 키 문자열로 변환하며, 변환된 문자열로부터 치환 행렬을 얻어 상기 입력부를 통해 입력되는 사용자 생체정보 이미지의 치환된 이미지를 얻는 제2단계; 및 중앙처리부에서, 상기 제2단계에서 얻어진 치환된 이미지 정보와 상기 데이터베이스에 저장되어 있는 템플릿 및 전역 변수로부터 사용자를 인식하는 제3단계;를 포함한다.

이러한 본 발명은 기존 PCA나 LDA 등과 같은 데이터 구별 방법론을 사용하여 이미지를 인식하는 방법에서 취소 가능한 특징(Cancelable Feature)을 첨가하여 보안성을 갖출 수 있게 된다.

대표도 - 도5



(56) 선행기술조사문헌
KR1020030072192 A
KR1020050054394 A
KR1020050075272 A
KR1020050117624 A
US20030086593 A1

특허청구의 범위

청구항 1

사용자 생체정보 이미지 및 키워드를 입력하며, 입력된 키워드를 무작위 키 문자열로 변환하고, 변환된 문자열로부터 치환 행렬을 제공하는 입력부;

상기 입력부에서 제공되는 치환 행렬을 사용하여 상기 사용자 생체정보 이미지의 치환된 이미지를 얻는 이미지 치환부;

사용자 특정 가중치와 사용자 특정 치환 행렬로 된 템플릿 및 소정 무작위 마스터 키로 치환된 전역 변수가 저장되는 데이터베이스; 및

상기 이미지 치환부에서 얻어진 치환된 이미지 정보 및 상기 데이터베이스에 저장되어 있는 템플릿과 전역 변수로부터 사용자를 인식하는 중앙처리부;

를 포함하는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템.

청구항 2

제 1 항에 있어서, 상기 치환 행렬은

단위행렬 I를 무작위 키 문자열 RKS(Random Key String)을 이용하여 열이나 행으로 치환하여 얻는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템.

청구항 3

제 1 항에 있어서, 상기 전역 변수는

상기 무작위 마스터 키에 치환 행렬 추출함수(D_{Mx})를 사용하여 얻어낸 치환 행렬로 치환된 특성 벡터와, 무작위 마스터 키에 치환 행렬 추출함수(D_{Mx})를 사용하여 얻어낸 치환 행렬로 치환된 평균 얼굴 이미지로부터 생성되는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템.

청구항 4

제 1 항에 있어서, 상기 중앙처리부는

상기 데이터 베이스에 저장되어 있는 사용자 특정 가중치와 하기의 식(1)에 의해 생성되는 새로운 사용자 특정 가중치를 비교하여 사용자 인식을 행하는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템.

식(1) : $\Omega_k' = f_{c.k}(U^T)\{\Gamma_p - f_{r.k}(\mu)\}$

(여기서, Ω_k'는 새로운 사용자 특정 가중치, $f_{c.k}(A)$와 $f_{r.k}(A)$는 임의의 행렬 A를 각각 열과 행으로 치환하는 함수, U^T는 치환된 특성벡터, Γ_p는 치환된 이미지, μ는 평균 얼굴 이미지이다.)

청구항 5

제 1 항에 있어서, 상기 템플릿은

$D_{M_r}^{-1}()$ 가 무작위 키 문자열로부터 치환 행렬의 역행렬을 계산하는 함수일 때, 하기의 식(2)에 의해 취소될 수 있는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템.

식(2) : $P_{new}(P_{old})^{-1} = D_{M_r}(D_{F_r}(\text{새로운 키워드}))D_{M_p}^{-1}(D_{F_p}(\text{기존 키워드}))$

(여기서, 상기 D_k는 키워드 기반 키 추출함수, D_{Mr}은 치환행렬을 추출하는 함수, D_{Mr}^{-1}은 D_{Mr}의 역함수, P_{new} 및 P_{old}는 N×N 치환행렬이다.)

청구항 6

사용자 특정 가중치와 사용자 특정 치환 행렬로 된 템플릿 및 소정 무작위 마스터 키로 치환된 전역 변수를 데이터베이스에 저장하는 제1단계;

입력부를 통해 입력되는 키워드를 무작위 키 문자열로 변환하며, 변환된 문자열로부터 치환 행렬을 얻어 상기 입력부를 통해 입력되는 사용자 생체정보 이미지의 치환된 이미지를 얻는 제2단계; 및

중앙처리부에서, 상기 제2단계에서 얻어진 치환된 이미지 정보와 상기 데이터베이스에 저장되어 있는 템플릿 및 전역 변수로부터 사용자를 인식하는 제3단계;

를 포함하는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 방법.

청구항 7

제 6 항에 있어서, 상기 전역 변수는

상기 무작위 마스터 키에 치환 행렬 추출함수(D_{Mx})를 사용하여 얻어낸 치환 행렬로 치환된 특성 벡터와, 무작위 마스터 키에 치환 행렬 추출함수(D_{Mx})를 사용하여 얻어낸 치환 행렬로 치환된 평균 얼굴 이미지로부터 생성되는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 방법.

청구항 8

제 6 항에 있어서, 상기 제3단계에서

상기 데이터 베이스에 저장되어 있는 사용자 특정 가중치와 하기의 식(1)에 의해 생성되는 새로운 사용자 특정 가중치를 비교하여 사용자 인식을 행하는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 방법.

식(1) : $\Omega_k' = f_{c.k}(U^T)\{\Gamma_p - f_{r.k}(\mu)\}$

(여기서, Ω_k'는 새로운 사용자 특정 가중치, $f_{c.k}(A)$와 $f_{r.k}(A)$는 임의의 행렬 A를 각각 열과 행으로 치환하는 함수, U^T는 치환된 특성벡터, Γ_p는 치환된 이미지, μ는 평균 얼굴 이미지이다.)

청구항 9

제 6 항에 있어서, 상기 템플릿은

$D_{M_r}^{-1}()$ 가 무작위 키 문자열로부터 치환 행렬의 역행렬을 계산하는 함수일 때, 하기의 식(2)에 의해 취소될 수 있는 것을 특징으로 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 방법.

식(2) : $P_{new}(P_{old})^{-1} = D_{M_r}(D_k(\text{새로운 키워드}))D_{M_r}^{-1}(D_k(\text{기존 키워드}))$

(여기서, 상기 D_k는 키워드 기반 키 추출함수, D_{Mr}은 치환행렬을 추출하는 함수, D_{Mr}^{-1}은 D_{Mr}의 역함수, P_{new} 및 P_{old}는 N×N 치환행렬이다.)

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<10> 본 발명은 취소 가능한 생체인식 시스템 및 방법에 관한 것으로, 특히 전역 변수 및 사용자 특정 가중치와 사용자 특정 치환 행렬을 인식을 위한 정보로 사용하며, 키워드를 바꾸는 것으로 자신의 생체정보를 취소할 수 있도록 하는 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템 및 방법에 관한 것이다.

<11> 많은 생체인식기술들은 인간에게 주는 편리함을 유지하기 위하여 생체정보를 도난당하지 않도록 연구되어 왔다. 과거, 일반적으로 생체인식기술에서 매칭은 템플릿(Template)과 얻어진 이미지를 비교하는 작업이며, 그렇기 때문에 몇몇 인식기술에서 인증을 위한 생체정보는 템플릿을 이용하여 복원이 가능했다. 그러나 이러한 특징은 보안적인 측면에서는 약점으로 작용한다.

<12> 이러한 특징으로인해 데이터베이스로부터 인코딩된 정보를 취소한다는 N.K. Ratha의 취소가능한 생체인식기술(cancelable biometric)(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)의 개념이 필요하게 되었다.

<13> 이의 취소가능한 생체인식기술은 보안을 목적으로 사용자 인식을 위해 저장된 템플릿을 사용자가 임의로 취소할 수 있게 하는 취소 가능한 생체정보인식기술의 필요성에 대하여 논의하였다(도 1참조).

<14> 데이터베이스는 템플릿으로써 인코딩된 정보를 가지고 있고, 입력된 정보는 데이터베이스에서와 동일한 함수로 인코딩된 후, 이 원래의 정보와 얻어진 정보는 인코딩된 도메인 위에서 비교된다. 이 결과는 인코딩되지 않은 도메인에서 비교한 결과와 동일하다.

<15> 여기에서 인코딩 함수는 복원가능하지 않은 특징(또는 일방향성)을 갖고 있으면 더욱 좋다. 그러나 일반적으로 이러한 인코딩 작업도 이미지 처리를 기본으로 하기 때문에 비트 단위의 완전한 임의의 변환을 적용하기 힘들고, 그렇게 때문에 아직도 인코딩 함수에 암호학적 방법을 적용하기란 힘든 일이다.

<16> Mario Savvide의 기법(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)은 이러한 취소가능한 생체인식기술의 좋은 예이다.

<17> M. Braithwaite(Michael Braithwaite, Ulf Cahn von Seelen, James Cambier, John Daugman, Randy Glass, Russ moore, and lan Scott, "Application-Specific Biometric Templates", Iridian Technologies Inc., Proceedings of AutoID, pp.167-171,2002)는 템플릿을 취소가능하게 하기 위하여 어떠한 프레임위크를 가져야 하는지에 대하여 논의하였으며, 비록 어떤 종류의 함수인지 정의하지 않았지만, 매칭을 변환된 도메인 위에서 수행하는 아이디어를 제시하였다.

<18> 상기와 같은 취소 가능한 생체정보인식기술에 대한 개념과 그에 대한 프레임워크가 나온 이후, 이러한 기술을 구현하기 위해서 노력하고 있으나, 현재 대부분의 취소 가능한 생체정보인식기술은 이미지 처리를 이용한 노이즈의 삽입이나 형태의 변형을 통한 방법이 사용되어 왔다.

<19> 그러나 보안적인 측면에서 보았을 때, 이는 충분히 안전하다고 볼 수 없기 때문에 이미 오랜 기간 검증을 거친 암호학적인 방법이 사용되어야만 한다.

<20> 한편, 현재 생체인식을 위한 기술로 PCA(Principle Component Analysis) 기법, FLD(Fisher's Linear Discriminant) 기법 등을 들 수 있다.

<21> 상기 PCA기법은 학습을 위한 이미지가 $\Gamma_1, \Gamma_2, \cdots, \Gamma_M$이고, μ를 이들의 전체 평균이라고 할 때, 전체 이미지에 대한 전체 스캐터 매트릭스(total scatter matrix)를 S_T라고 하고 다음과 같이 정의한다.

<22> $$S_T = \sum_{i=1}^{M} (\Gamma_i - \mu)(\Gamma_i - \mu)^T$$

<23> 새로운 특징 벡터를 $y_k=U^T x_k$라고 정의할 때 y_k위로 사상되는 전체 스캐터 매트릭스는 $U^T S_T U$가 된다. 이때 $U^T S_T U$의 determinant를 최대로 하는 U를 고유벡터(Eigen Vectors)로써 사용하고 있다.

<24> $$U_{opt}=\arg\max_U |U^T S_T U|$$

<25> 상기 FLD기법은 학습하려는 이미지가 몇 개의 클래스로 구별될 수 있을 때, μ_i를 j번째 클래스의 평균이라고 하고, x_i는 그 클래스의 하나의 원소라고 하고, N을 그 클래스의 원소의 개수, c를 클래스의 개수라고 할 때, Between-class 스캐터 매트릭스를 S_B라고 하고 다음과 같이 정의한다.

<26> $$S_B=\sum_{j=1}^{c}\sum_{i=1}^{N}(x_i-\mu_j)(x_i-\mu_j)^T$$

<27> 또한, Within-class 스캐터 매트릭스를 S_W라고 하고 다음과 같이 정의한다.

<28> $$S_W=\sum_{j=1}^{c}(\mu_j-\mu)(\mu_j-\mu)^T$$

<29> 이때, S_B대 S_W의 비율을 최대로 하는 U를 고유벡터로써 사용하고 있다.

<30> $$U_{opt}=\arg\max_U \frac{|U^T S_B U|}{|U^T S_W U|}$$

<31> 그리고 각각의 얼굴 이미지(클래스)에 대해서 고유벡터가 기여하는 가중치를 다음과 같이 계산할 수 있다.

<32> $$\Omega_k=U_{opt}^T(\Gamma_k-\mu)$$

<33> 만약, 어떠한 이미지 Γ가 입력되었을 때, Γ에 따른 가중치를 다음과 같이 계산할 수 있다.

<34> $$\Omega=U_{opt}^T(\Gamma-\mu)$$

<35> 이후, 각각의 계산된 가중치 Ω_k중에서 유클리디언 거리(Euclidean Distance)가 어떠한 한계 값 Θ_ε보다 작으며, 또한 그 중에서 가장 작은 클래스를 선택한다.

<36> $$\varepsilon_k=\| \Omega-\Omega_k \| \leq \Theta_\varepsilon$$

<37> 만약 $\varepsilon_k>\Theta_\varepsilon$라면 이 이미지는 "알 수 없음"으로 분류하고 있다.

<38> 따라서 본 발명은 상기에서 기술된 PCA나 LDA 등과 같은 데이터 구별 방법론과 함께 암호학적으로 충분히 검증받은 방법을 사용하지만 취소가능한 특성을 만족할 수 있는 취소 가능한 생체인식기술을 제시하고자 한다.

발명이 이루고자 하는 기술적 과제

<39> 본 발명은 이러한 점을 감안한 것으로, 본 발명의 목적은 전역 변수 및 사용자 특정 가중치와 사용자 특정 치환 행렬을 생체인식을 위한 정보로 사용하며, 사용자 키워드를 바꾸는 것으로 사용자 특정 치환 행렬을 새롭게 갱신함으로써 자신의 생체정보를 취소할 수 있도록 한 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템 및 방법을 제공함에 있다.

발명의 구성 및 작용

<40> 상기 목적을 달성하기 위한 본 발명에 따른 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한

생체인식 시스템은, 사용자 생체정보 이미지 및 키워드를 입력하며, 입력된 키워드를 무작위 키 문자열로 변환하고, 변환된 문자열로부터 치환 행렬을 제공하는 입력부; 상기 입력부에서 제공되는 치환 행렬을 사용하여 상기 사용자 생체정보 이미지의 치환된 이미지를 얻는 이미지 치환부; 사용자 특정 가중치와 사용자 특정 치환 행렬로 된 템플릿 및 소정 무작위 마스터 키로 치환된 전역 변수가 저장되는 데이터베이스; 및 상기 이미지 치환부에서 얻어진 치환된 이미지 정보 및 상기 데이터베이스에 저장되어 있는 템플릿과 전역 변수로부터 사용자를 인식하는 중앙처리부;를 포함하는 것을 특징으로 한다.

<41> 상기 치환 행렬은 단위행렬 I를 무작위 키 문자열 RKS(Random Key String)을 이용하여 열이나 행으로 치환하여 얻으며, 상기 전역 변수는 상기 무작위 마스터 키와 특성 벡터 및 상기 생체정보 평균 이미지로부터 얻는다.

<42> 상기 목적을 달성하기 위한 본 발명에 따른 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 방법은, 사용자 특정 가중치와 사용자 특정 치환 행렬로 된 템플릿 및 소정 무작위 마스터 키로 치환된 전역 변수를 데이터베이스에 저장하는 제1단계; 입력부를 통해 입력되는 키워드를 무작위 키 문자열로 변환하며, 변환된 문자열로부터 치환 행렬을 얻어 상기 입력부를 통해 입력되는 사용자 생체정보 이미지의 치환된 이미지를 얻는 제2단계; 및 중앙처리부에서, 상기 제2단계에서 얻어진 치환된 이미지 정보와 상기 데이터베이스에 저장되어 있는 템플릿 및 전역 변수로부터 사용자를 인식하는 제3단계;를 포함하는 것을 특징으로 한다.

<43> 상기 제3단계에서 Γ_p : 이미지 치환부에서 치환된 이미지로, $\Gamma_P = D_{M_r}(D_K(\text{사용자 키워드}))\Gamma$ 이며, $U^T_{RR}=U^T_{opt}D_{Mc}(MRK)$, $\mu_{RR}=D_{M_c}(MRK)\mu$, $f_{c,k}(U^T)=U^T(D_{Mc}(D_K(\text{사용자키워드})))^T=U^T_{RR}S_{c,k}$, $f_{r,k}(\mu)=D_{M_r}(D_K(\text{사용자 키워드}))\mu=S_{r,k}\mu_{RR}$ 일때, $\Omega_k'=f_{c,k}(U^T)\{\Gamma_p-f_{r,k}(\mu)\}=U^T_{RR}S_{c,k}(\Gamma_P-S_{r,k}\mu_{RR})$에 의해 새로운 사용자 특정 가중치를 얻어 상기 데이터베이스에 저장되어 있는 사용자 특정 가중치와 비교하여 사용자 인식을 행한다.

<44> 그리고 상기 템플릿은 $D^{-1}_{M_r}()$ 는 무작위 키 문자열로부터 치환 행렬의 역행렬을 계산하는 함수일 때, $P_{new}(P_{old})^{-1}=D_{M_r}(D_K(\text{새로운 키워드}))D^{-1}_{M_r}(D_K(\text{기존 키워드}))$ 에 의해 취소될 수 있다.

<45> 이하, 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 보다 상세하게 설명한다. 단, 하기 실시 예는 본 발명을 예시하는 것일 뿐 본 발명의 내용이 하기 실시 예에 한정되는 것은 아니다.

<46> 도 2는 본 발명에 따른 변환된 행렬의 벡터 곱과 키워드를 사용하는 취소 가능한 생체인식 시스템의 개념 구성도를 도시한 것으로, 본 발명이 사용자 키워드와 변환된 도메인에서의 벡터 곱의 두가지 요소를 사용하며, 사용자 키워드를 PBKDF(Password-Based Key Derivation Function)의 암호화 방식을 사용하여 무작위의 키 문자열로 변환하며, 이로부터 치환 행렬(Matrix Permutation) 추출 함수를 통해 치환 행렬을 얻고, 치환 행렬과 사용자의 생체정보(얼굴영상)를 이용하여 PCA나 LDA기법을 이용하여 인식하게 됨을 보여주고 있다.

<47> 1. 치환된 도메인에서의 인식

<48> 특성 얼굴을 사용하는 인증 기법에서 평균얼굴, 특성 벡터, 각각의 가중치는 행렬 형태로 다시 표현될 수 있다. 이것들은 미리 계산되어 인식 시스템의 데이터베이스에 저장된다. 만약, 인증 시스템에 특성 얼굴 기법이 사용되고, 가중치가 노출되었다면 이를 이용하여 누군가가 특정한 개인으로 인증을 받을 수도 있을 것이다.

<49> 이를 위해서는 가중치가 얼굴 이미지에서 계산되므로 얼굴 이미지를 시스템에 제공해야만 할 것이다. 그러나 만약, 평균 얼굴, 특성 벡터, 가중치가 한번에 노출된다면 공격자는 얼굴 이미지를 $\Omega_k = U_{opt}^T(\Gamma_k - \mu)$ 로부터 얻어낼 수 있다.

<50> 따라서 이것들은 암호학적 해시 함수와 같은 방법으로 안전하게 인코딩 된 후에야 데이터베이스에 저장

할 수 있다. 그러나 암호학적 연산은 얼굴 인증 알고리즘이 정확히 얼굴을 매칭하는 것을 방해한다. 이 문제를 해결하기 위해서 치환된 도메인 위에서라도 매칭 작업에 어떠한 영향을 주지 않는 변환 작업이 필요하다. 특성 얼굴기법을 사용하는 인증 방법에서 치환(Permutation)은 바람직한 선택이다.

<51>

<52> [정의 1] $f_{c,k}(A)$와 $f_{r,k}(A)$를 어떠한 행렬 A를 동일한 방법으로 각각 열(column)과 행(row)으로써 치환하는 함수라고 하자. 여기서, k는 사용자의 인덱스(index)이다.

<53> $p_{c,k}$과 $p_{r,k}$를 N×N치환 행렬이라고 하고, A를 N×1행렬이라고 하자. 그러면 정의 1에 기술된 함수를 다음과 같이 다시 표현할 수 있다.

<54> $f_{c,k}(A) = Ap_{c,k}$

<55> $f_{r,k}(A) = p_{r,k}A$

<56> 또한, $p_{c,k}$과 $p_{r,k}$는 다음과 같은 연관이 있다.

<57> $$P_{c,k}^{T} = P_{r,k}$$

<58> [보조정리 1] 주어진 이미지 Γ , 평균 이미지 μ , 특성 벡터 U_{opt}는 다음을 만족한다.

<59> $$U_{opt}^{T}(\Gamma-\mu)=f_{c,k}(U_{opt}^{T})\{f_{r,k}(\Gamma)-f_{r,k}(\mu)\}$$

<60> 도 3은 변환된 도메인에서의 벡터 곱의 결과를 나타낸 도로, 만약 N×M행렬과 M×L 행렬의 벡터 곱을 수행할 때, 각각 가로와 세로(즉, M개) 열을 동일한 방식으로 섞었을 때 섞지 않은 벡터의 곱과 동일한 결과를 얻을 수 있음을 보여주고 있다.

<61> 2. 사용자 키워드로부터 치환 행렬의 추출

<62> 시스템은 치환 그 자체에 대해서는 아무런 정보도 가지고 있지 않기 때문에, 얼굴 이미지 입력측에서는 시스템에게 치환된 얼굴 이미지를 보내주어야 한다는 이야기와 같다. 얼굴 이미지를 치환시키기 위해서, 입력측에서는 사용자로부터 키워드를 얻고 치환 행렬을 제공해주어야 한다.

<63> 안전한 치환 행렬을 얻기 위해서 사용자 키워드는 PKCS#5에 기술되어 있는 PBKDF(Password-Based Key Derivation Function)와 같은 암호학적 방법을 사용하여 높은 복잡도를 갖는 문자열로 바꾸어야 한다.

<64>

<65> [정의 2] $D_k()$는 키워드 기반 키 추출 함수를 의미하고, 이 함수는 무작위의 키 문자열을 반환한다.

<66> $$\text{무작위키문자열}=D_K(\text{사용자키워드})$$

<67> $D_k()$는 완전하게 PKCS#5의 PBKDF를 사용한다. 기본적으로 PKCS#5의 함수들은 해시 함수나 의사 난수 생성기 함수로 이루어져 있고, 이의 역을 구하는 것은 불가능하다.

<68> [정의 3] $D_{M_x}()$ 는 무작위 키 문자열에서부터의 치환 행렬 추출 함수를 의미하고, 이 함수는 x의 값에 따라서 열이나 행 단위로 치환된 행렬을 반환한다. x는 r이나 c가 될 수 있다. M는 어떠한 행렬을 의미한다.

<69> $$\text{치환행렬}=D_{M_x}(\text{무작위키문자열})$$

<70> 치환 행렬은 단위행렬 I를 무작위 키 문자열 RKS(Random Key String)를 이용하여 열이나 행으로 치환해서 얻는다. $RKS_{<i..j>}$ (RKS<i..j>라고 표시한다.)를 무작위 키 문자열에서 정수 형태로 인식할 수

있는 i부터 j까지의 비트열이라고 하면, 치환 행렬 추출 함수 $D_{M_x}()$ 는 도 4와 같이 동작한다.

<71> $D_{M_x}()$ 를 사용하여 $P_{c,k}$와 $P_{r,k}$를 얻을 수 있으며, 치환 함수 $f_{c,k}()$와 $f_{r,k}()$를 계산할 수 있다. 그러면 다음과 같이 다시 쓸 수 있다.

<72> $f_{r,k}(A)=D_{Mr}(D_K(\text{사용자키워드}))A$, $fc_{,k}(A)=AD_{Mc}(D_K(\text{사용자키워드}))$

<73> 3. 취소 가능한 생체 인식 기술을 사용하는 얼굴 인증

<74> 3.1 시스템 요구사항

<75> 만약, 시스템에 치환된 U_{opt}^{T} 와 치환된 μ를 저장한다면, 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.

<76> 따라서 시스템에 어떠한 무작위 마스터 키(master random key)로 치환된 하나의 전역 U_{RR}^{T}과 μ_{RR}을 후술될 데이터베이스(40)에 저장하면 특정 사용자 정보는 한 사용자 당 하나의 치환 정보를 저장하는 것으로 충분하다. 여기서, 상기 마스터 키는 상기 무작위 키 문자열과 동일한 것이다.

<77> 이와 같이 함으로써 많은 메모리를 절약할 수 있다. 아래 표1에 보이고 있는 전역 변수들은 시스템에 저장되지도 않으며 어떠한 방법으로도 얻어낼 수 없는 MRK(Master Random Key)로 만들어진 치환 행렬로 치환되어 안전하다.

<78> **표 1.** 전역 변수와 그에 대한 설명

<79>

변수	설 명
U_{RR}^{T}	MRK 에 $D_{M_c}()$ 를 사용하여 얻어낸 치환 행렬로 치환된 특성 벡터의 모임
μ_{RR}	MRK 에 $D_{M_r}()$ 를 사용하여 얻어낸 치환 행렬로 치환된 평균 얼굴 이미지

<80> 또한, 다음의 표2에 보이고 있는 사용자 계정은 사용자 특정 가중치와 치환 행렬로 이루어져 있으며, 이 역시 데이터베이스(40)에 저장되어 있게 된다.

<81> **표 2.** 사용자 계정 변수와 그에 대한 설명

<82>

변수	설 명
Ω_k	'사용자 특정 가중치(user specific weight factor)'로, 특성 벡터 U 와 평균 μ 를 사용하여 어떻게 원래의 이미지를 복원해내는지 가리키는 값이다.
$S_{x,k}$	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 $S_{c,k}^{T}=S_{r,k}$의 관계가 있다.

<83> 결과적으로, 몇 가지 앞에서 기술하였던 식의 변형을 생각해 볼 수 있다.

<84> $U^{T}_{RR}=U^{T}_{opt}D_{Mc}(MRK)$

<85> $\mu_{\mu}=D_{M_c}(MRK)\mu$

<86> 만약, 행렬 $f_{c,k}(U^{T})$ 와 $f_{r,k}(\mu)$ 이 사용자 키워드로 생성된 치환 행렬로 치환된 행렬 사용자 특정 행렬이라면

<87> $f_{c,k}(U^T)=U^T(D_{Mc}(D_K(\text{사용자키워드})))^T=U^T_{RR}S_{c,k}$

<88> $$f_{r,k}(\mu)=D_{M_r}(D_K(\text{사용자 키워드}))\mu=S_{r,k}\mu_{RR}$$

<89> 이다. 따라서 저장해야만 하는 사용자 특정 데이터는 Ω_k와 S_k이다.

<90> 3.2 이미지 인식

<91> 도 5는 본 발명의 시스템 구성도를 도시한 것으로, 이러한 기법을 적용한 시스템에서 사용자가 인증을 받고자 할 때, 사용자는 사용자의 생체정보 이미지와 키워드를 입력부(Acquiring Part)(10)에 제공해야만 한다. 그러한 이미지를 Γ라고 하고, 이미지 치환 부분(Image Permutation Part)인 이미지 치환부(20)는 치환된 이미지 Γ_p를 계산해야만 한다.

<92> $$\Gamma_P=D_{M_r}(D_K(\text{사용자 키워드}))\Gamma$$

<93> 즉, 상기 입력부(10)는 사용자로부터 입력되는 키워드를 무작위 키 문자열로 변환하고, 변환된 문자열로부터 치환 행렬을 제공하며, 이미지 치환부(20)는 치환 행렬을 사용하여 사용자 생체정보 이미지의 치환된 이미지를 얻게 된다.

<94> 그런 뒤, 이 치환된 이미지는 각각의 사용자 계정을 뒤지며 사용자의 특정 가중치 Ω를 찾는 중앙처리부(main process part)(30)로 보내진다. 각각의 사용자 계정에 대해서, 중앙처리부(30)는 Ω의 후보 Ω_k'를 계산해야만 한다.

<95> $\Omega_k'=f_{c,k}(U^T)\{\Gamma_p-f_{r,k}(\mu)\}=U^T_{RR}S_{c,k}(\Gamma_P-S_{r,k}\mu_{RR})$

<96> 그러면 데이터베이스(40)에 저장되어 있는 사용자 특정 가중치 Ω_k와 위의 식을 통하여 얻은 Ω_k' 벡터들과 비교함으로써, 적합한 사용자 계정을 찾아낼 수 있게 된다.

<97> 각각의 계정은 다른 치환 순서를 갖기 때문에, Ω_k'와 Ω_k 유클리드 거리는 올바른 계정과 그렇지 않은 계정들 사이에 큰 차이를 보일 것이다.

<98> 3.3 템플릿의 취소

<99> 본 발명에서 템플릿은 ($S_{x,k}$, Ω_k)로 정의된다. 따라서 템플릿의 취소 작업은 $S_{x,k}$를 바꾸는 작업과도 같다. 이렇게 키워드를 바꾸는 작업은 변환되는 과정에서 사용자 이미지의 누출을 막기 위하여 어떠한 보안이 필요하다. 어떠한 보안 위협 때문에 사용자가 그의 키워드를 바꾸고자 할 때, 그는 반드시 그의 키워드를 시스템에게 새로운 $S_{x,k}$를 계산하도록 하기 위해서 제공해야한다.

<100> 그러나, 만약 이러한 작업이 원격으로 이루어진다면 원형태의 사용자 키워드나 $D_K(\text{사용자 키워드})$, $D_{M_r}(D_K(\text{사용자 키워드}))$를 제공하는 행위는 매우 위험하다. 왜냐하면 $\Gamma=P_r^{-1}\Gamma_P$ 이고 Γp은 인증 과정을 관찰함으로써 얻을 수 있기 때문이다. 따라서 키워드 정보는 어떠한 세션 키로 안전하게 암호화되었다고 가정한다.

<101> 더 나아가, 새로운 키워드가 적용되는 경우를 생각해야한다. 만약 U^T와 μ이 이 작업동안 복원된다면, U^T와 μ는 다른 누군가에게 노출될 가능성이 있기 때문에 위험하다. 따라서 다음과 같은 미리 계산된 행렬이 이러한 복원을 막기 위해서 제공되어져야만 할 것이다.

<102> $P_{new}(P_{old})^{-1}=D_{M_r}(D_K(\text{새로운 키워드}))D^{-1}_{M_r}(D_K(\text{기존 키워드}))$

<103> $D_{M_r}^{-1}()$ 는 무작위 키 문자열로부터 치환 행렬의 역행렬을 계산하는 함수이다.

<104> $P_{new}(P_{old})^{-1}$ 는 분리될 수 없으며 $U_{P_{old}}^{T}$ 를 $U_{P_{new}}^{T}$ 로, $\mu_{P_{old}}$ 를 $\mu_{P_{new}}$ 로 바로 바꾸어준다. 그러면, 시스템은 U_{RR}^{T} 와 $U_{P_{new}}^{T}$ 나 μ_{RR} 와 $\mu_{P_{new}}$ 를 이용하여 새로운 $S_{x,k}$ 를 구해야만 한다.

<105> $$S_{c,k}=U_{P_k}^{T}(U_{RR}^{T})^{-1}=(\mu_{P_k}(\mu_{RR})^{-1})^{T}=(S_{r,k})^{T}$$

<106> 그리고 구해진 새로운 $S_{x,k}$ 를 데이터베이스(40)에 저장하여 추후 인식시에 이용하게 된다.

<107> 도 6은 상기와 같은 본 발명의 전체적인 동작 흐름도를 도시한 것으로, 먼저 사용자 특정 가중치 Ω_k 와 사용자 특정 치환 행렬 $S_{x,k}$ 로 된 템플릿 및 소정 무작위 마스터 키로 치환된 상기 전역 변수 U_{RR}^{T}, μ_{RR} 를 데이터베이스(40)에 저장한다(S110).

<108> 그리고 상기 입력부(10)를 통해 입력되는 키워드를 무작위 키 문자열로 변환하며, 변환된 문자열로부터 상기 치환 행렬을 얻어 이미지 치환부(20)에서 사용자 생체정보의 치환된 이미지를 얻는다(S120),(S130). 이후, 상기 단계(S130)에서 얻어진 생체정보의 치환된 이미지와 상기 데이터베이스(40)에 저장되어 있는 템플릿 및 전역 변수로부터 사용자를 인식하게 된다(S140).

<109> 사용자 인식에는 상기와 같이 $\Omega_k'=f_{c,k}(U^{T})\{\Gamma_p-f_{r,k}(\mu)\}=U_{RR}^{T}S_{c,k}(\Gamma_P-S_{r,k}\mu_{RR})$ 를 이용하여 새로운 사용자 특정 가중치를 얻어 상기 데이터베이스(40)에 저장되어 있는 사용자 특정 가중치와 비교하여 사용자 인식을 행하게 되고, 상기 템플릿은 상기 $P_{new}(P_{old})^{-1}=D_{M_r}(D_K(\text{새로운 키워드}))D_{M_r}^{-1}(D_K(\text{기존 키워드}))$ 에 의해 취소될 수 있게 되는 것이다.

<110> 상기와 같이 본 발명의 취소 가능한 특징은 변환된 도메인에서의 매칭 작업을 수행함으로써 구현할 수 있다. 생체정보는 인증 시스템에서 변환된 형태로 저장되고, 치환행렬 자체는 어디에도 저장되지 않는다. 따라서 만약 사용자의 템플릿이 공격자에게 노출되었다고 하더라도 다른 시스템에서 이를 사용하여 인증받을 수는 없다.

<111> 또한, 공격자는 템플릿을 저장하고 있던 바로 그 시스템에서도 치환 행렬을 생성하는 사용자 키워드를 모른다면 이를 이용하여 인증받을 수 없다. 따라서 이러한 기법은 키워드와 얼굴 이미지의 두가지 보안 요소를 사용하는 인증 시스템이라고 할 수 있는 것이다.

<112> 만약, 사용자가 생체정보를 취소하고자 할 경우, 사용자는 키워드를 바꾸는 것으로 자신의 생체정보를 취소할 수 있다. 더 정확하게는 키워드를 바꿈으로써 사용자는 생체정보를 바꿀수는 없지만 시스템에 저장된 인증정보를 바꿀 수 있다. 공격자가 원래 얼굴 이미지를 얻는다고 하더라도 공격자는 각각의 시스템에 맞는 키워드를 알아내지 않고는 그 스스템에서 인증받을 수 없다.

<113> 상술한 바와 같이, 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 또는 변형하여 실시할 수 있다.

발명의 효과

<114> 이상에서 살펴본 바와 같이, 본 발명은 전역 변수 및 사용자 특정 가중치와 사용자 특정 치환 행렬을 생체인식을 위한 정보로 사용하여 인식을 행하며, 사용자 키워드를 바꾸는 것으로 사용자 특정 치환 행렬을 새롭게 갱신하여 자신의 인증을 위한 생체정보를 취소할 수 있도록 함으로써 기존의 PCA나 LDA 등과 같은 데이터 구별 방법론을 사용하여 이미지를 인식하는 방법에서 취소 가능한 특징(Cancelable Feature)을 첨가하여 보안성을 갖출 수 있도록 한 효과가 있다.

<115>

도면의 간단한 설명

<1> 도 1은 종래 보안을 위한 생체정보의 복원 불가능한 도메인으로서의 변환의 불가피성에 대한 도.

<2> 도 2는 본 발명에 따른 취소 가능한 생체인식 시스템의 개념 구성도.

<3> 도 3은 본 발명에 따른 변환된 도메인에서의 벡터 곱의 결과를 나타낸 도.

<4> 도 4는 본 발명에서 무작위한 비트 스트링으로부터 치환 행렬을 생성해내는 과정을 나타낸 도.

<5> 도 5는 본 발명에 따른 취소 가능한 생체인식 시스템의 상세 구성도.

<6> 도 6은 본 발명의 전체적인 동작 설명도.

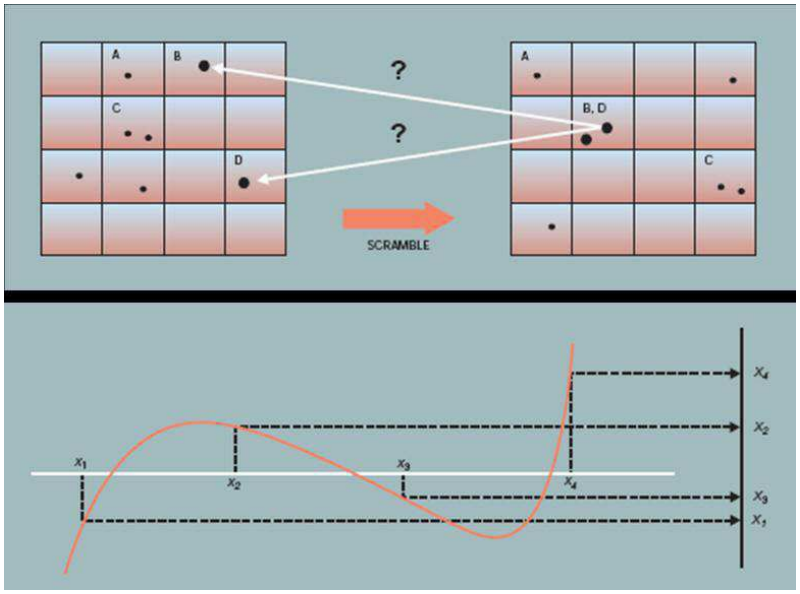
<7> <도면의 주요 부분에 대한 부호의 설명>

<8> 10 : 입력부 20 : 이미지 치환부

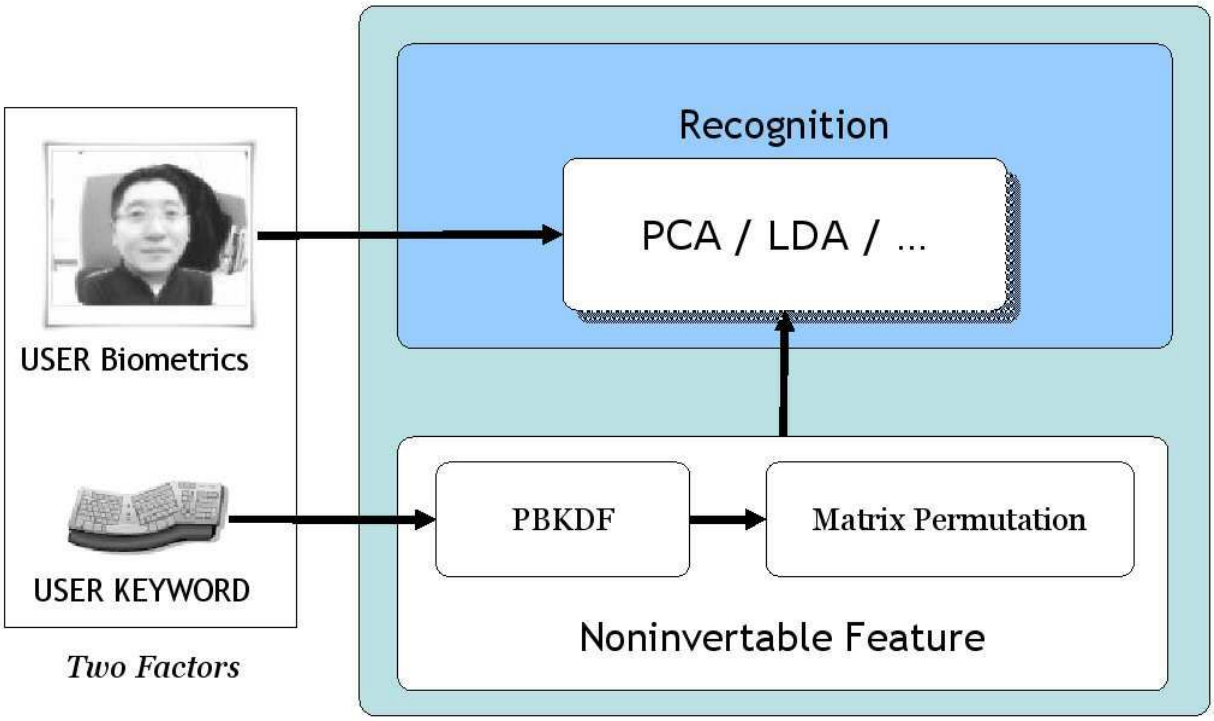
<9> 30 : 중앙처리부 40 : 데이터베이스

도면

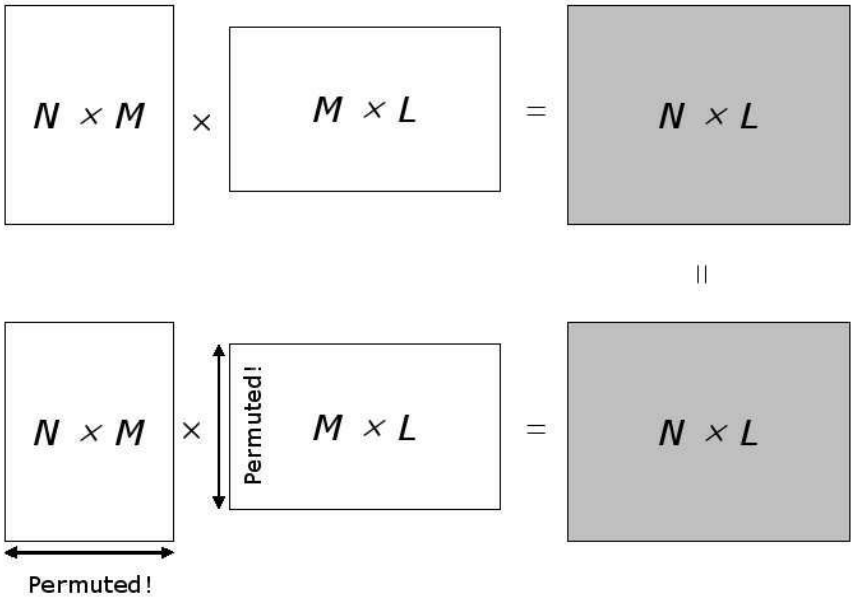
도면1



도면2


Recognition
PCA / LDA / ...
USER Biometrics
USER KEYWORD
PBKDF
Matrix Permutation
Noninvertable Feature
Two Factors

도면3

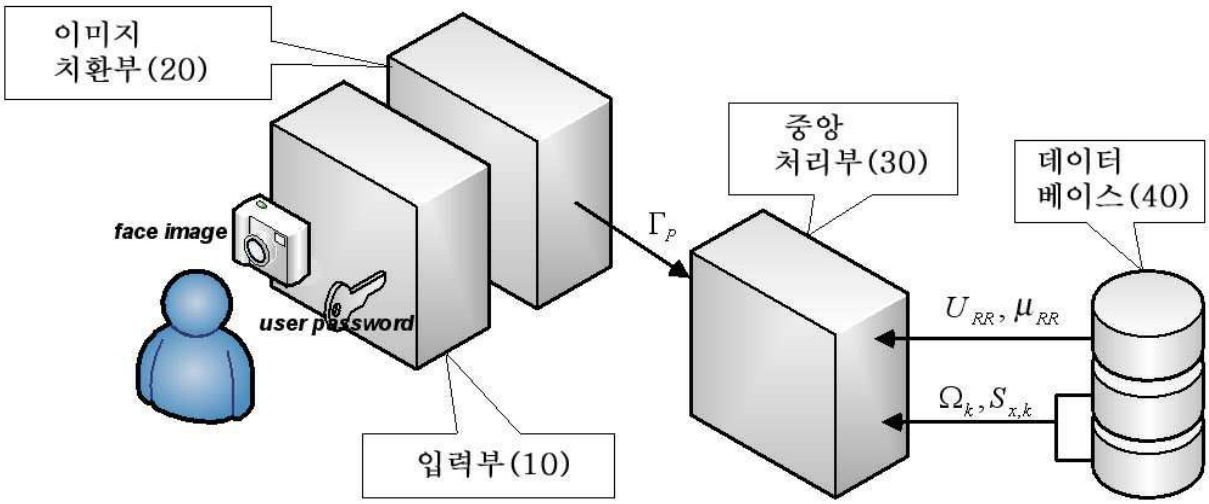

N × M
×
M × L
=
N × L
||
N × M
×
Permuted!
M × L
=
N × L
Permuted!

도면4

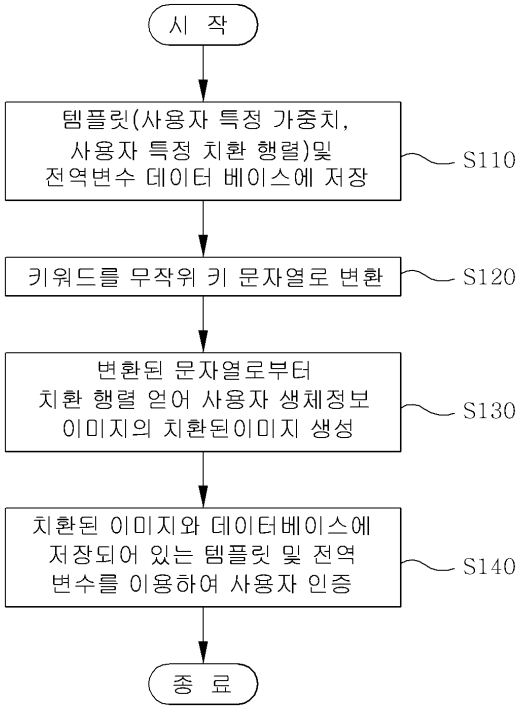
```
// RKS : random key string, input
// n : image height * image width
// m : larger integer then upper bound lg n

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
```

도면5



도면6


시 작
템플릿(사용자 특정 가중치,
사용자 특정 치환 행렬)및
전역변수 데이터 베이스에 저장
S110
키워드를 무작위 키 문자열로 변환
S120
변환된 문자열로부터
치환 행렬 얻어 사용자 생체정보
이미지의 치환된이미지 생성
S130
치환된 이미지와 데이터베이스에
저장되어 있는 템플릿 및 전역
변수를 이용하여 사용자 인증
S140
종 료