(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년02월10일
(11) 등록번호 10-0941372
(24) 등록일자 2010년02월02일

(51) Int. Cl.
G06K 9/52 (2006.01) *G06K 9/62* (2006.01)
G06K 9/80 (2006.01)
(21) 출원번호 10-2008-0034781
(22) 출원일자 2008년04월15일
심사청구일자 2008년04월15일
(65) 공개번호 10-2009-0109363
(43) 공개일자 2009년10월20일
(56) 선행기술조사문헌
WO02095657 A2
KR1020030072191 A
JP2001052127 A
JP11265350 A
전체 청구항 수 : 총 14 항

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울특별시 서초구 서초4동 삼풍아파트 3동 405호
강전일
충남 공주시 옥룡동 284-1
김군순
충남 서산시 읍내 1동 30번지
(74) 대리인
이원희

심사관 : 장기정

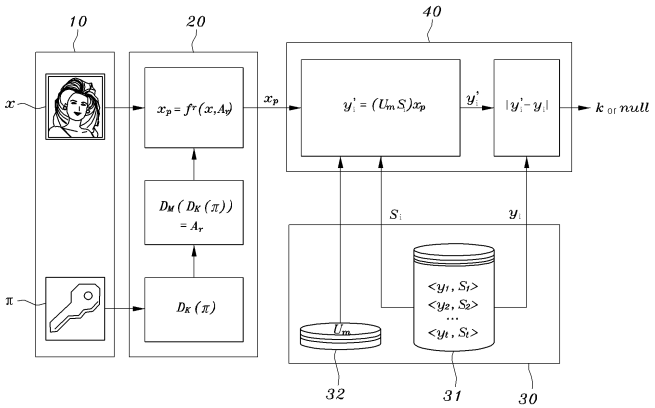
(54) 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식장치 및 방법

(57) 요 약

본 발명은 역행렬을 갖는 행렬을 치환행렬로 사용하는 취소 가능한 얼굴인식 장치 및 방법에 관한 것으로, 본 발명에 따른 얼굴인식 장치는,

사용자의 얼굴 이미지와 패스워드가 입력되는 입력부; 상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 이미지 치환부; 사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿 및 시스템 행렬이 저장되는 데이터베이스; 및, 상기 치환된 이미지와 상기 사용자 특정 치환행렬 및 상기 시스템 행렬을 이용하여 사용자 특정 가중치 후보를 산출하고, 상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 중앙처리부를 포함하는 것을 특징으로 한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

사용자의 얼굴 이미지와 패스워드가 입력되는 입력부;

상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 이미지 치환부;

사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿 및 시스템 행렬이 저장되는 데이터베이스; 및,

상기 치환된 이미지와 상기 사용자 특정 치환행렬 및 상기 시스템 행렬을 이용하여 사용자 특정 가중치 후보를 산출하고, 상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 중앙처리부

를 포함하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 2

청구항 1에 있어서,

상기 입력부는 역행렬을 갖지 않는 치환행렬을 생성하는 패스워드는 입력되지 않는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 3

청구항 1에 있어서,

상기 이미지 치환부는 상기 패스워드를 랜덤키 문자열로 변환하고, 상기 변환된 랜덤키 문자열로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 4

청구항 1에 있어서,

상기 시스템 행렬은 시스템 마스터 키를 이용하여 생성되는 행렬에 의해 사상 행렬로부터 치환되어 생성되는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 5

청구항 1에 있어서,

상기 사용자 특정 가중치 후보는 하기의 식에 의해 생성되는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치

식 : $y_i' = (U_m S_i)x_p$

(여기서, y_i'은 사용자 특정 가중치 후보, U_m은 시스템 행렬, S_i는 사용자 특정 치환행렬, x_p는 치환된 이미지이다.).

청구항 6

청구항 1에 있어서,

상기 이미지 치환부는 상기 패스워드로부터 사용자 지정 난수를 생성하는 난수 생성기를 더 포함하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 7

청구항 6에 있어서,

상기 이미지 치환부는 상기 난수 생성기에서 생성된 상기 사용자 지정 난수를 상기 역행렬을 갖는 치환행렬에

곱하여 각각 다른 사용자가 생성한 치환행렬이 서로 다른 평균을 갖도록 하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 8

사용자의 얼굴 이미지와 패스워드가 입력되는 입력부;

상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 이미지 치환부;

사용자 특정 가중치 또는 사용자 특정 치환행렬 중 어느 하나만이 상기 사용자의 얼굴 이미지 또는 상기 패스워드와 연관되어 구성되는, 연관 해제된 템플릿 및 시스템 행렬이 저장되는 데이터베이스; 및,

상기 치환된 이미지와 상기 사용자 특정 치환행렬 및 상기 시스템 행렬을 이용하여 사용자 특정 가중치 후보를 산출하고, 상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 중앙처리부

를 포함하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 9

청구항 8에 있어서,

상기 데이터베이스는 얼굴인식과는 무관한 더미 템플릿을 더 포함하여 공격자의 사전 탐색 횟수를 더 증가시키는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치.

청구항 10

사용자의 얼굴 이미지와 패스워드를 입력하는 단계;

상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하는 단계;

상기 역행렬을 갖는 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 단계;

사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿 및 시스템 행렬이 저장된 데이터베이스에서 추출된 사용자 특정 치환행렬 및 시스템 행렬과, 상기 치환된 이미지를 이용하여 사용자 특정 가중치 후보를 산출하는 단계;

상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 단계

를 포함하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 방법.

청구항 11

청구항 10에 있어서,

상기 치환된 이미지를 생성하는 단계는 상기 패스워드를 랜덤키 문자열로 변환하고, 상기 변환된 랜덤키 문자열로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 방법.

청구항 12

청구항 10에 있어서,

상기 사용자 특정 가중치 후보는 하기의 식에 의해 생성되는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 방법

식 : $y_i' = (U_m S_i)x_p$

(여기서, y_i'은 사용자 특정 가중치 후보, U_m은 시스템 행렬, S_i는 사용자 특정 치환행렬, x_p는 치환된 이미지이다.).

청구항 13

청구항 10에 있어서,

상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하는 단계는 상기 패스워드로부터 사용자 지정 난수를 생성하는 단계를 더 포함하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 방법.

청구항 14

청구항 13에 있어서,

상기 사용자 지정 난수를 상기 역행렬을 갖는 치환행렬에 곱하여 각각 다른 사용자가 생성한 치환행렬이 서로 다른 평균을 갖도록 하는 것을 특징으로 하는 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 취소 가능한 얼굴인식 장치 및 방법에 관한 것으로, 특히 역행렬을 갖는 행렬을 치환행렬로 사용하는 취소 가능한 얼굴인식 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 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.

[0003] 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.

[0004] 이의 취소가능한 생체인식기술은 보안을 목적으로 사용자 인식을 위해 저장된 템플릿을 사용자가 임의로 취소할 수 있게 하는 취소 가능한 생체정보인식기술의 필요성에 대하여 논의하였다.

[0005] 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.

[0006] 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.

[0007] 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.

[0008] M. Braithwaite(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)는 템플릿을 취소가능하게 하기 위하여 어떠한 프레임위크를 가져야 하는지에 대하여 논의하였으며, 비록 어떤 종류의 함수인지 정의하지 않았지만, 매칭을 변환된 도메인 위에서 수행하는 아이디어를 제시하였다.

[0009] 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.

[0010] 그러나 보안적인 측면에서 보았을 때, 이는 충분히 안전하다고 볼 수 없기 때문에 이미 오랜 기간 검증을 거친 암호학적인 방법이 사용되어야만 한다.

[0011] 한편, 현재 생체인식을 위한 기술로 PCA(Principle Component Analysis) 기법, FLD(Fisher's Linear Discriminant) 기법 등을 들 수 있으며, 이에 대해 본 출원의 발명자들은 PCA나 LDA 등과 같은 데이터 구별 방법론과 함께 암호학적으로 충분히 검증받은 방법을 사용하지만 취소가능한 특성을 만족할 수 있는 취소 가능한 생체인식기술을 제시한 바가 있다.(한국특허출원 제10-2006-35795호)

[0012] 상기 특허출원에서는 특수하게 디자인된 치환행렬을 생성하여 선형 얼굴 인증 시스템에서 보안을 강화하면서도 기존과 동일한 인증효과를 도출할 수 있었다.

발명의 내용

해결 하고자하는 과제

[0013] 본 발명의 출원인들은 상기 특허출원의 기술적 내용을 보완하여 특수하게 디자인된 치환행렬을 생성하지 않고서도 보다 간소한 방법으로도 보안을 강화할 수 있는 취소 가능한 얼굴인식 장치 및 방법을 제공하고자 한다.

과제 해결수단

[0014] 상기와 같은 본 발명의 목적을 달성하기 위한 본 발명에 따른 취소 가능한 얼굴인식 장치는,

[0015] 사용자의 얼굴 이미지와 패스워드가 입력되는 입력부; 상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 이미지 치환부; 사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿 및 시스템 행렬이 저장되는 데이터베이스; 및, 상기 치환된 이미지와 상기 사용자 특정 치환행렬 및 상기 시스템 행렬을 이용하여 사용자 특정 가중치 후보를 산출하고, 상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 중앙처리부를 포함하는 것을 특징으로 한다.

[0016] 이 때, 상기 입력부는 역행렬을 갖지 않는 치환행렬을 생성하는 패스워드는 입력되지 않는다.

[0017] 또한, 상기 이미지 치환부는 상기 패스워드를 랜덤키 문자열로 변환하고, 상기 변환된 랜덤키 문자열로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 것을 특징으로 한다.

[0018] 또한, 상기 시스템 행렬은 시스템 마스터 키를 이용하여 생성되는 행렬에 의해 사상 행렬로부터 치환되어 생성되는 것을 특징으로 한다.

[0019] 또한, 상기 사용자 특정 가중치 후보는 하기의 식에 의해 생성되는 것을 특징으로 한다.

[0020] 식 : $y_i' = (U_m S_i)x_p$

[0021] (여기서, y_i'은 사용자 특정 가중치 후보, U_m은 시스템 행렬, S_i는 사용자 특정 치환행렬, x_p는 치환된 이미지이다.).

[0022] 또한, 상기 이미지 치환부는 상기 패스워드로부터 사용자 지정 난수를 생성하는 난수 생성기를 더 포함하는 것을 특징으로 한다.

[0023] 또한, 상기 이미지 치환부는 상기 난수 생성기에서 생성된 상기 사용자 지정 난수를 상기 역행렬을 갖는 치환행렬에 곱하여 각각 다른 사용자가 생성한 치환행렬이 서로 다른 평균을 갖도록 하는 것을 특징으로 한다.

[0024] 본 발명의 또 다른 실시예에 따른 취소 가능한 얼굴인식 장치는,

[0025] 사용자의 얼굴 이미지와 패스워드가 입력되는 입력부; 상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 이미지 치환부; 사용자 특정 가중치 또는 사용자 특정 치환행렬 중 어느 하나만이 상기 사용자의 얼굴 이미지 또는 상기 패스워드와 연관되어 구성되는, 연관 해제된 템플릿 및 시스템 행렬이 저장되는 데이터베이스; 및, 상기 치환된 이미지와 상기 사용자 특정 치환행렬 및 상기 시스템 행렬을 이용하여 사용자 특정 가중치 후보를 산출하고, 상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 중앙처리부를 포함하는 것을 특

징으로 한다.

[0026] 또한, 상기 데이터베이스는 얼굴인식과는 무관한 더미 템플릿을 더 포함하여 공격자의 사전 탐색 횟수를 더 증가시켜서 보안을 강화할 수 있다.

[0027] 본 발명에 따른 취소 가능한 얼굴인식 방법은,

[0028] 사용자의 얼굴 이미지와 패스워드를 입력하는 단계; 상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하는 단계; 상기 역행렬을 갖는 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 단계; 사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿 및 시스템 행렬이 저장된 데이터베이스에서 추출된 사용자 특정 치환행렬 및 시스템 행렬과, 상기 치환된 이미지를 이용하여 사용자 특정 가중치 후보를 산출하는 단계; 상기 사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식하는 단계를 포함하는 것을 특징으로 한다.

[0029] 또한, 상기 치환된 이미지를 생성하는 단계는 상기 패스워드를 랜덤키 문자열로 변환하고, 상기 변환된 랜덤키 문자열로부터 역행렬을 갖는 치환행렬을 생성하며, 상기 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성하는 것을 특징으로 한다.

[0030] 또한, 상기 사용자 특정 가중치 후보는 하기의 식에 의해 생성되는 것을 특징으로 한다.

[0031] 식 : $y_i' = (U_m S_i)x_p$

[0032] (여기서, y_i'은 사용자 특정 가중치 후보, U_m은 시스템 행렬, S_i는 사용자 특정 치환행렬, x_p는 치환된 이미지이다.).

[0033] 또한, 상기 패스워드로부터 역행렬을 갖는 치환행렬을 생성하는 단계는 상기 패스워드로부터 사용자 지정 난수를 생성하는 단계를 더 포함하는 것을 특징으로 한다.

[0034] 또한, 상기 사용자 지정 난수를 상기 역행렬을 갖는 치환행렬에 곱하여 각각 다른 사용자가 생성한 치환행렬이 서로 다른 평균을 갖도록 하는 것을 특징으로 한다.

효 과

[0035] 상기한 바와 같은 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치 및 방법에 의하면,

[0036] 기존의 얼굴인식 장치 및 방법에 비해 보다 간단한 방법으로도 보안을 강화할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0037] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 우선, 도면들 중 동일한 구성요소 또는 부품들은 가능한 한 동일한 참조부호를 나타내고 있음에 유의해야 한다. 본 발명을 설명함에 있어서 관련된 공지기능 혹은 구성에 대한 구체적인 설명은 본 발명의 요지를 모호하게 하지 않기 위해 생략한다.

[0038] 도 1은 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치를 도시한 개념도이다.

[0039] 도 1을 참조하면, 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치는 크게 입력부(10), 이미지 치환부(20), 데이터 베이스(30), 중앙처리부(40)를 포함한다.

[0040] 상기 입력부(10)에서는 사용자의 얼굴 이미지(x)와 패스워드(π)가 입력된다. 사용자의 얼굴이미지(x)는 본 발명의 얼굴인식 장치에 부착된 카메라나 이와 유사한 기능을 수행하는 감지센서 등에 의해 감지되어 입력되고, 패스워드(π)는 컴퓨터 자판 등과 같은 입력장치에 의해 입력된다. 이때, 상기 입력부는 역행렬을 갖지 않는 치환행렬을 생성하는 패스워드는 입력되지 않게 하며, 이는 본 발명의 얼굴인식 장치에 의해 사용자에게 강제할 수 있다.

[0041] 상기 이미지 치환부(20)는 상기 패스워드(π)를 랜덤키 문자열($D_K(\pi)$)로 변환하고, 치환행렬 생성함수($D_M(D_K(\pi))$)를 이용하여 상기 변환된 랜덤키 문자열로부터 역행렬을 갖는 치환행렬(P_r)을 생성하며, 상기 치환행렬(P_r)과 상기 사용자의 얼굴 이미지(x)를 이용하여 치환된 이미지(x_p)를 생성한다.

[0042] 상기 데이터베이스(30)는 사용자 특정가중치(y_i)와 사용자 특정치환행렬(S_i)이 저장된 사용자 템플릿 데이터 베이스(31)와 시스템 행렬(U_m)이 저장되는 시스템 행렬 데이터 베이스(32)로 구성된다. 상기 시스템 행렬은 시스템 마스터 키를 이용하여 생성되는 행렬에 의해 사상 행렬(projection matrix)로부터 치환되어 생성된다. 또한, 상기 시스템 마스터 키는 랜덤 비트 스트링(random bit string)에서 형성되며, 시스템 관리자가 외장 메모리 장치를 이용하여 상기 시스템 마스터 키를 운반해야 하도록 하고, 필요한 때에 상기 시스템 마스터 키가 제공되도록 한다.

[0043] 이때, 본 발명의 일 실시예에 따른 얼굴인식 장치는 사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿이 데이터베이스에 저장되지만, 후술하는 다른 실시예에 따른 얼굴인식 장치에서는 사용자 특정 가중치 또는 사용자 특정 치환행렬 중 어느 하나만이 상기 사용자의 얼굴 이미지 또는 상기 패스워드와 연관되어 구성된 템플릿이 데이터베이스에 저장된다.

[0044] 상기 중앙처리부(40)는 상기 데이터베이스로부터 사용자 특정치환행렬(S_i), 사용자 특정가중치(y_i), 시스템 행렬(U_m)을 제공받고, 상기 치환된 이미지(x_p)와 상기 사용자 특정 치환행렬(S_i) 및 상기 시스템 행렬(U_m)을 이용하여 사용자 특정 가중치 후보(y_i')를 산출하고, 상기 사용자 특정 가중치(y_i)와 상기 사용자 특정 가중치 후보(y_i')로부터 사용자를 인식하기 위한 정보(k or null)를 제공한다. 여기서, 'k'는 특정 사용자를 인식한 경우이고, 'null'은 사용자 인식이 되지 않은 경우를 의미한다.

[0045] 이때, 상기 사용자 특정 가중치 후보(y_i')는 $y_i' = (U_m S_i)x_p$에 의해 생성되며, 여기서, y_i'은 사용자 특정 가중치 후보, U_m은 시스템 행렬, S_i는 사용자 특정 치환행렬, x_p는 치환된 이미지이다.

[0046] 상기와 같이 구성된 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치의 동작 알고리즘에 대한 설명은 다음과 같다.

[0047] 어떠한 테스트 얼굴 이미지 $x \in R^n$는 학습 얼굴 집합 $X=\{x_1, x_2, ..x_N\}$으로부터 추출한 특성 벡터의 전치(Transpose) $U \in R^{m \times n}$행렬 에 의해서 가중치 벡터 $y \in R^m$로 선형적으로 변환될 수 있다.

[0048] 식 (1) : $y = Ux$

[0049] 가중치 벡터 y는 같은 방식으로 학습 얼굴 집합 $X=\{x_1, x_2, ..x_N\}$으로부터 변환된 $y_1, y_2, ...y_N$와 거리를 비교함으로써 가장 유사한 하나의 학습 얼굴을 찾는데 사용된다.

[0050] 선형 얼굴 인식 기법은 선형적인 연산의 결과로써 가중치 벡터 y_i를 저장하기 때문에 설령 학습 얼굴 x_i를 시스템이 저장하지 않고 있다 하더라도 특성 벡터 U를 사용하여 가중치 벡터 yi로부터 원래의 학습 얼굴 x_i를 복원해 낼 수 있다. 이 때, 특성 벡터 U의 크기에 따라서 복원되는 정도가 다르지만 사람이 식별할 수 있고, 이를 이용하여 인증을 시도할 수 있을 만큼의 얼굴 정보는 복원된다.

[0051] 치환 변환 기법은 U를 행 방향으로, x를 열 방향으로 동일한 순서로 섞고, 사용자가 지정한 패스워드로부터 생성하는 '섞는 순서'에 대한 정보를 U와 결합된 형태로 시스템에 저장하여 사용자가 올바른 패스워드를 입력하였을 때에만 섞인 정보가 무효화가 되어 기존의 선형 인식 기법과 동일한 역할을 수행하도록 한 방법이다.

[0052] 동일한 순서로 섞인 행렬은 사용자 패스워드로부터 생성되는 특별하게 설계된 치환 행렬 P을 사용하여 U와 x에 각각 적용하여 얻을 수 있다. 따라서 다음과 같은 수식이 성립하게 된다.

[0053] 식 (2) : $y = Ux = UP^T \times Px$

[0054] 여기서 U는 시스템에서 삭제되고, 대신 각각의 사용자마다 하나씩 생성되는 UP^T가 서버에 저장된다. Px는 사용자가 패스워드와 자신의 얼굴 x를 입력함으로써 얻을 수 있으므로 올바른 패스워드와 얼굴을 입력했다면 시스템은 올바른 사용자를 찾아낼 수 있다.

[0055] 한편, UP^T에서 U나 P에 대한 정보가 없다면 시스템을 공격하여 모든 정보를 얻어온 공격자라 하더라도 이를 분해(Decompose)하는 것이 매우 어렵다.

[0056] 이때, 치환 행렬 P는 1보다 크거나 같고 n보다 작거나 같은 모든 i와 j에 대해서 다음과 같은 성질을 만족한다.

[0057] 식 (3) : $$\sum_{i=1}^{n} P_{\langle i,j\rangle} = 1, \sum_{j=1}^{n} P_{\langle i,j\rangle} = 1,\ P_{\langle i,j\rangle} \in \{0,1\}$$

[0058] 여기서, $P_{<i,j>}$는 P의 i번째 행, j번째 열에 위치한 원소를 의미한다.

[0059] 상기 치환 행렬은 한국특허출원 제10-2006-35795호에서 제안된 특수하게 치환된 행렬이다.

[0060] 한편, 상기 식 (3)을 만족하는 치환 행렬 P는 항상 다음 수식을 만족하는 특징이 있다.

[0061] 식 (4) : $P^T \times P = I$

[0062] 즉, $P^{-1} = P^T$를 만족한다. 따라서, 치환 변환 기법을 사용하기 위해서는 반드시 위와 같이 특수하게 설계된 치환 행렬을 사용하지 않고도 역행렬을 갖는 일반행렬 $A \in R^{n \times m}$를 치환 행렬로 사용 가능하다는 것을 알 수 있다. 즉, 다음의 식 (5)는 상기 식 (1)을 만족함을 알 수 있다.

[0063] 식 (5) : $y = Ux = UA^{-1} \times Ax$

[0064] 본 발명에 따른 상기 치환 행렬 A는 사용자가 제공하는 패스워드로부터 무작위로 생성될 수 있으며 원래의 치환 변환 기법과 동일한 절차를 거쳐 패스워드를 바꿈으로써 저장된 템플릿을 취소하고 새로운 템플릿을 저장할 수도 있다. 단, 역행렬을 갖지 않는 치환 행렬을 생성하는 패스워드는 사용되어서는 안 되며 이는 시스템에 의해서 사용자에게 강제로 의무화될 수 있다.

[0065] 본 발명에 따른 역행렬을 가지는 행렬을 취환 행렬로 사용하는 취소 가능한 얼굴 인식 장치에서, 상기 치환행렬 A는 패스워드-키 변환 함수 $D_K(\pi)$와 키-행렬 변환 함수 $D_M(D_K(\pi))$을 이용하여 패스워드(π)로부터 생성된다(식 (6)참조). 특히, 상기 패스워드-키 변환 함수 $D_K(\pi)$는 PBKDF(Password-Based Key Drrivation Function)를 사용한다.

[0066] 식 (6) : $A = D_M(D_K(\pi))$

[0067] 본 발명에 따른 취소 가능한 얼굴인식 장치에서, 상기 이미지 치환부(20)는 상기 패스워드(π)로부터 사용자 지정 난수 v를 생성하는 난수 생성기를 더 포함할 수 있다.

[0068] 상기 난수 생성기에서 생성된 상기 사용자 지정 난수 v는 상기 역행렬을 갖는 치환행렬(P_r)에 곱해짐으로써 각각 다른 사용자가 생성한 치환행렬이 서로 다른 평균을 갖도록 할 수 있다. 이와 같이 사용자마다 생성된 치환행렬 값이 서로 다르게 하는 이유는 다음과 같다.

[0069] 무작위로 생성된 임의의 치환 행렬 A_i는 다른 치환 행렬 A_j와 유사한 평균값 (즉, $|A_i| \fallingdotseq |A_j|$)을 갖게 된다. 예를 든 것과 같은 단지 2개의 치환 행렬만이 유사한 평균을 갖는 것이 아니라, 모든 치환 행렬들이 유사한 평균을 갖게 된다. 이는 시스템 공격에 성공한 공격자로 하여금 특징적인 얼굴 정보를 가진 특정한 사용자를 알 수 있게 하는 빌미를 제공할 수 있다.

[0070] 따라서, 이를 방지하기 위하여 시스템은 각기 다른 사용자가 생성한 치환 행렬 A_i를 서로 다른 평균을 갖도록 할 필요가 있다. 이는 패스워드(π)로부터 생성된 난수 v를 아래의 식(a)와 같이, A_i^{-1}와 A_i에 v_i^{-1}와 v_i의 형태로 곱함으로써 해결할 수 있다. 이 때, 상기 v를 사용자 지정 난수라고 부른다.

[0071] 식 (a) : $y = Ux = v_i^{-1} U A_i^{-1} \times v_i A_i x$

[0072] 또한, 아래의 식 (b)와 같이 패스워드(π)로부터 생성된 난수 v_i를 모든 원소가 1인 행렬 $B(\in R^{n \times n})$에 곱한 후, A_i에 더하여 사용하고 $(v_iB + A_i)$의 역행렬을 이용할 수도 있다.

[0073] 식 (b) : $y = Ux = U(v_iB + A_i)^{-1} \times (v_iB + A_i)x$

[0074] 이러한 사용자 지정 난수는 결과적으로 시스템에 저장되는 UA^{-1}의 크기를 무작위로 변화시키는 역할을 하게 되어 공격자로 하여금 UA^{-1}만 가지고 특정한 사용자의 것임을 확신할 수 없게 하여, 보안성을 강화할 수 있다.

[0075] 본 명세서에서 개시된 바와 같이, 역행렬을 갖는 행렬을 치환 변환 기법에 적용하면 더 높은 얼굴 인식률을 갖게 된다. '얼굴 인식'은 다른 얼굴과 구별하는 과정이기 때문에 서로 일치하지 않는 $v_i^{-1}UA_i^{-1}$와 v_jA_jx가 만나게 되면 올바른 가중치 벡터 y가 생성되지 않기 때문이다. 이 과정에서 $v_i^{-1}A_i^{-1}\times v_jA_j$는 단위행렬이 아니게 되므로, 이 행렬이 노이즈로써 작용하여 인식 과정에 영향을 미치게 되고, 다른 계정의 가중치 벡터와의 거리를 넓히게 되므로 인식률을 높이는 결과를 가져오게 된다.

[0076] 기존의 치환 행렬 또한 $P_i^T\times P_j$는 역시 단위행렬은 아니지만, 이 경우 행렬 자체의 크기가 0에 가까워 가중치 벡터 자체의 크기를 줄이는 역할을 수행하며 다른 계정의 가중치 벡터와의 거리를 좁히게 된다. 결과적으로 인식률이 감소하게 된다.

[0077] 이렇게 인식률에 영향을 미치는 치환 행렬을 만듦에 있어서 오로지 사용자의 패스워드만이 정보로 사용되므로, 결과적으로는 패스워드가 인식률에 영향을 미친다고 할 수 있다. 즉, 역행렬을 갖는 행렬을 치환 행렬로써 사용할 때의 인식률의 증가는 패스워드가 인식을 위한 정보로써 사용되었음을 의미한다.

[0078] 하지만 '얼굴 인증'의 경우 다른 계정의 영향을 받지 않기 때문에 치환 변환 기법의 경우 어떠한 치환 행렬을 사용한다 하더라도 원래의 얼굴 인증 기법과 동일한 결과를 얻어낼 수 있다.

[0079] 전술한 실시예에 따른 얼굴인식 장치는 사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿이 데이터베이스에 저장되지만, 본 발명의 다른 실시예에 따른 얼굴인식 장치에서는 사용자 특정 가중치 또는 사용자 특정 치환행렬 중 어느 하나만이 상기 사용자의 얼굴 이미지 또는 상기 패스워드와 연관되어 구성된 템플릿이 데이터베이스에 저장된다.

[0080] 치환 변환 기법의 경우, 시스템에 저장되는 템플릿이 다른 얼굴 인증 시스템과 다르게 $<U_m, S_i, y_i>$의 형태를 가지고 있다. 여기에서 U_m의 경우 모든 템플릿에 공통적으로 저장되는 정보이기 때문에 실제로는 $<S_i, y_i>$을 식별자(또는 ID)와 연관되는 템플릿 정보라고 볼 수 있다.

[0081] 시스템을 공격하여 템플릿 정보를 가져온 공격자는 한 번의 사전 탐색 공격(Dictionary Attack)을 수행함으로써, 모든 사용자의 얼굴 정보를 복원할 수 있다. 왜냐하면 S_i와 y_i가 연관되어 있기 때문에, 어떠한 연관된 S_k와 y_k를 사용하면, $P_kx_k \fallingdotseq (U_mS_k)^+y_k$ 처럼 올바르게 치환 변환된 P_kx_k를 구할 수 있고, 이에 대해서 사전 탐색 공격을 수행하여 P_k를 구하고, $U = U_mS_kP_k$를 이용해 U를 구할 수 있기 때문이다. U를 구할 수 있으면 U를 이용하여 모든 x_i를 계산해낼 수 있다.

[0082] 이러한 과정에서 사전 탐색 공격은 일반적인 사전 탐색 공격과 달리 $x_k' = (P_k^T)'P_kx_k$가 얼굴의 형태를 가지고 있는지 아닌지를 확인해야 한다. 따라서 공격자는 얼굴 탐지 프로그램을 가지고 있어야 한다. 얼굴 탐지 프로그램은 인터넷에서 얼마든지 구할 수 있다.

[0083] 따라서, 본 발명의 다른 실시예와 같이, 사용자 특정 치환행렬(S_i)와 사용자 특정 가중치(y_i)가 서로 연관이 되어 있지 않고, S_i또는 y_i 중 어느 한 쪽만 식별자와 연관되어 있다면 공격자는 올바른 연관을 찾아내기 위하여 최고 N(모든 템플릿의 수)번의 사전 탐색 공격을 수행하여야 한다.

[0084] 이는 노출된 템플릿의 보안성을 높여주는 역할을 한다. 물론, 연관되지 않은 템플릿을 사용하여 올바르게 인증하기 위해서는 모든 가능한 연관의 수를 고려해야하며 이때 필요한 연산의 양이 N배 증가하게 된다. 그러나 사전 공격은 일반적인 행렬 곱 연산에 비해서 매우 많은 연산을 필요로 한다.

[0085] 또한 이때, 임의의 M개의 더미 템플릿 $S_{N+1}, S_{N+2}, S_{N+3}, \ldots, S_{N+M}$을 데이터베이스에 삽입할 수 있다. 일반적인 연관이 유지되는 얼굴 인증 시스템에서는 더미 템플릿의 사용은 아무런 의미도 갖지 못하지만, 연관 해제된 템플릿에서 더미 템플릿은 실제 템플릿과 구별이 불가능하므로, 올바른 연관을 찾기 위한 경우의 수가 증가하게 되어 보안 수준을 높여주게 된다.

[0086] 이상과 같이 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치 및 방법을 예시한 도면을 참조로 하여 설명하였으나, 본 명세서에 개시된 실시예와 도면에 의해 본 발명이 한정되는 것은 아니며, 본 발명의 기술사상 범위내에서 당업자에 의해 다양한 변형이 이루어질 수 있음은 물론이다.

도면의 간단한 설명

[0087] 도 1은 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 장치를 도시한 블록도,

[0088] 도 2는 본 발명에 따른 역행렬을 갖는 치환행렬을 사용하는 취소 가능한 얼굴인식 방법을 도시한 순서도이다.

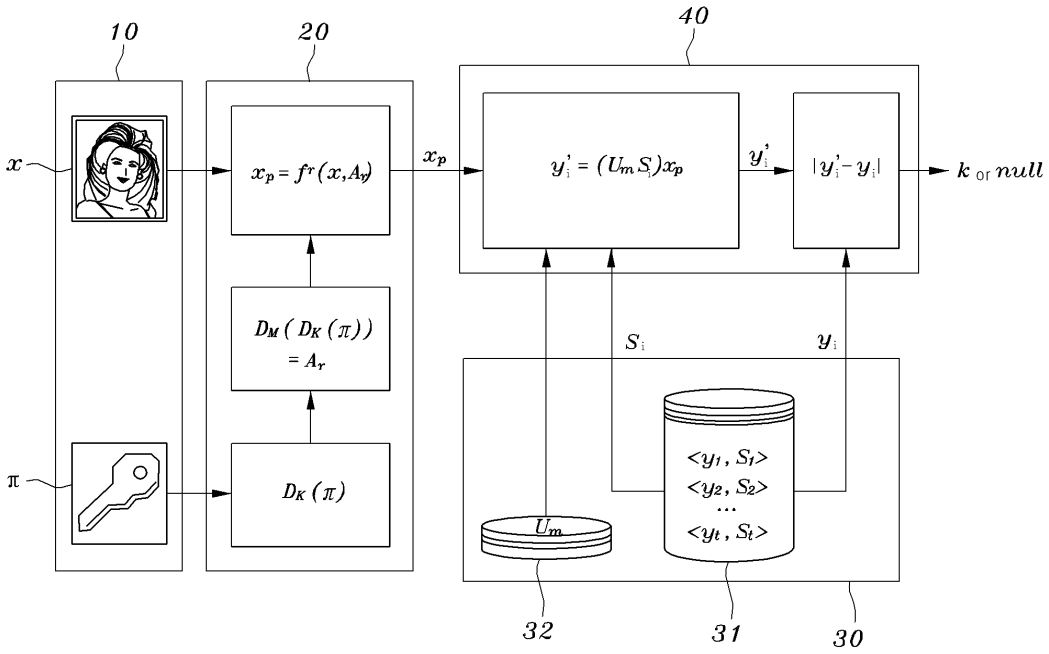
[0089] <도면의 주요부분에 대한 부호의 설명>

[0090] 10 : 입력부 20 : 이미지 치환부

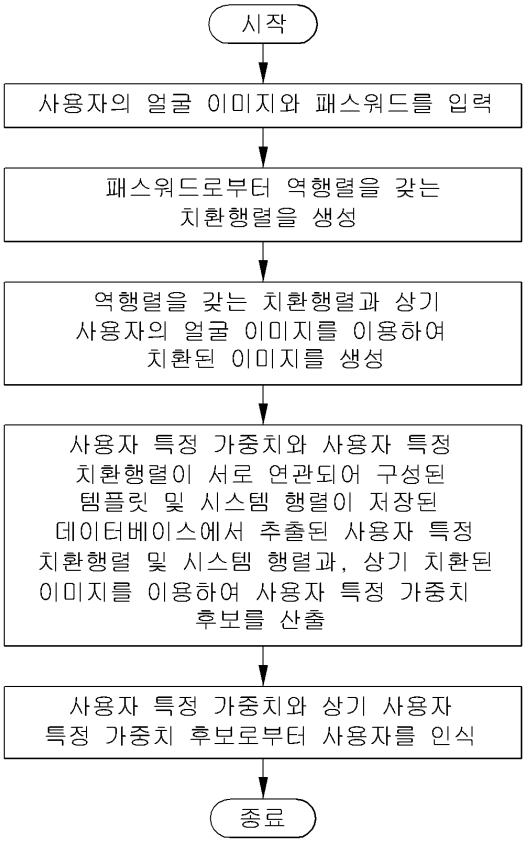
[0091] 30 : 데이터베이스 40 : 중앙 처리부

도면

도면1



도면2


시작
사용자의 얼굴 이미지와 패스워드를 입력
패스워드로부터 역행렬을 갖는 치환행렬을 생성
역행렬을 갖는 치환행렬과 상기 사용자의 얼굴 이미지를 이용하여 치환된 이미지를 생성
사용자 특정 가중치와 사용자 특정 치환행렬이 서로 연관되어 구성된 템플릿 및 시스템 행렬이 저장된 데이터베이스에서 추출된 사용자 특정 치환행렬 및 시스템 행렬과, 상기 치환된 이미지를 이용하여 사용자 특정 가중치 후보를 산출
사용자 특정 가중치와 상기 사용자 특정 가중치 후보로부터 사용자를 인식
종료