논문 2007-44SP-2-4

통계적 형상 기반의 얼굴인식을 위한 가변얼굴템플릿 생성방법

(A Method of Generating Changeable Face Template for Statistical Appearance-Based Face Recognition)

이 철 한*, 정 민 이*, 김 종 선*, 최 정 윤*, 김 재 희*

(Chulhan Lee, MinYi Jung, Jongsun Kim, Jeung-Yoon Choi, and Jaihie Kim)

요 약

가변생체인식(Changeable Biometrics)이란 생체정보의 도난이나 도용 시 개인의 프라이버시를 보호하기 위해 원 생체정보를 사용하지 않고, 생체정보를 변환하여 변환된 생체정보로 개인을 인증하는 방법이다. 본 논문은 통계적 형상 기반의 얼굴인식(Statistical appearance based face recognition)에 적용될 수 있는 가변얼굴템플릿 생성 방법에 대해 제안한다. 상이한 두 개의 통계적 형상 기반의 얼굴특징 방법을 이용하여 두 개의 얼굴특징벡터를 추출하고, 추출된 두 개의 얼굴특징벡터를 정규화 후 각 특징벡터들의 요소의 순서를 재배열 시킨다. 가변얼굴템플릿은 정규화 되고 순서가 재배열된 특징벡터들의 가중 합으로 생성된다. 두 개의 서로 다른 얼굴특징벡터의 가중 합으로 하나의 가변얼굴템플릿을 생성하므로, 가중 합의 방법과 생성된 가변얼굴템플릿을 알더라도 원 얼굴 특징벡터를 복원할 수 없다. 또한, 생성된 가변얼굴템플릿의 도난 시 새로운 가변얼굴템플릿의 생성은 각 벡터의 순서를 재배열시키는 규칙을 변경함으로써 가능하다. 그러므로 제안한 가변얼굴템플릿을 이용하여 개인 인증 시, 개인의 얼굴템플릿을 도난당하더라도 원 얼굴특징정보를 복원 할 수 없고 또한 새로운 가변얼굴템플릿으로 대체 할 수 있어 생체정보의 도난 시 발생할 수 있는 프라이버시 침해의 문제를 해결 할 수 있다. 제안한 방법은 AR-face DB를 이용하여 성능과 보안성에 대해 평가 하였다.

Abstract

Changeable biometrics identify a person using transformed biometric data instead of original biometric data in order to enhance privacy and security in biometrics when biometric data is compromised. In this paper, a novel scheme which generates changeable face templates for statistical appearance-based face recognition is proposed. Two different original face feature vectors are extracted from two different appearance-based approaches, respectively, each original feature vector is normalized, and its elements are re-ordered. Finally a changeable face template is generated by weighted addition between two normalized and scrambled feature vectors. Since the two feature vectors are combined into one by a two to one mapping, the original two feature vectors are not easily recovered from the changeable face template even if the combining rule is known. Also, when we need to make new changeable face template for a person, we change the re-ordering rule for the person and make a new feature vector for the person. Therefore, the security and privacy in biometric system can be enhanced by using the proposed changeable face templates. In our experiments, we analyze the proposed method with respect to performance and security using an AR-face database.

Keywords : Changeable Biometrics, Face Recognition, Security and privacy concerns

I. 서 론

생체인식은 개인의 생체정보를 이용하여 개인을 인증하는 방법이다. 생체정보가 개인 인증의 수단으로써 사용될 수 있는 가장 큰 이유는, 생체정보는 개인마다 다르다는 고유성(Uniqueness)과, 시간의 흐름에도 크게 변하지 않는다는 불변성(Permanence) 때문이다. 하지만 이러한 생체정보의 고유성과 불변성은 개인 생체정보의 도난이나 도용 시 심각한 프라이버시 침해의 문제를 야기 시킬 수 있다. 전통적인 개인 인증 방법인 신분증이나 패스워드의 경우 도난이나 도용 시 새로운

* 정회원, 연세대학교 생체인식 연구센터
(Biometric Engineering Research Center, Yonsei University)

※ 본 연구는 한국과학재단 지정 생체인식 연구센터 (BERC)의 지원을 받아 이루어졌습니다.
접수일자: 2006년9월4일, 수정완료일: 2007년2월20일

신분증이나 패스워드를 재발급하면 문제를 해결 할 수 있으나, 생체정보의 경우 새로운 생체정보를 재 생성하는 것은 불가능하다. 또한 생체인식을 이용한 개인 인증방법이 활성화 되면서 개인의 생체정보가 범죄수사와 같은 수사기관이나 은행 또는 기타 인터넷을 이용하는 다른 상업적인 기업체와 공유될 수 있고 이로 인해 개인의 생체정보가 도용될 수 있는 문제점이 있다. 이러한 문제점을 해결하기 위해 최근에 생체정보를 변환 후 변환된 생체정보를 이용해 개인을 인증 하는 가변생체인식(Changeable Biometrics)의 개념이 소개 되었다[1][2]. 이러한 가변생체인식이 만족해야 될 조건은 다음과 같다. i) 변환된 생체정보는 원 생체정보와 달라야한다(변환성). ii) 변환된 생체정보와 변환 방법을 알더라도 원 생체정보의 복원이 쉽지 않아야 한다(비가역성). iii) 다수의 변환된 생체정보의 생성이 가능해야 한다(재생산성). iv) 변환된 생체정보를 사용하더라도 인식성능의 저하가 적어야 한다. 기존의 가변 얼굴 가변생체인식 방법들은 이러한 조건을 모두 만족하지 않는다. 고로 본 논문에서는 이러한 조건을 모두 만족하는 방법에 대해 제안하고 이를 실험적으로 증명한다.

1. 기존 가변생체인식 방법

가변생체인식 개념을 처음 소개한 Ratha[1][2]는 가변생체인식을 입력생체신호 자체를 변환하는 방법(Signal domain transform)과 입력된 생체신호에서 추출된 특징을 변환하는 방법(Feature domain transform)으로 구분하였다. 이 논문에서도 Ratha의 분류방법을 이용하여 기존논문들을 재정리 하였다.

가. 입력생체신호 변환 방법

Ratha et al.[1][2]은 입력생체신호의 변환 방법으로 모핑(Morphing)과 블록 섞기(Block Permutation)의 방법을 소개하였다. 모핑을 이용한 방법은 입력생체영상을 모핑함수로 왜곡을 주어 변환하는 방법이고, 블록 섞기는 입력생체영상을 블록으로 나눈 후 그 블록들을 섞어 변환된 생체영상을 생성하는 방법이다. 이에 대한 예로 얼굴영상의 모핑과 지문영상의 블록 섞기를 소개하였다. 생체정보의 도난시 모핑함수와 블록 섞기의 규칙을 변경함으로써 새로운 생체영상을 생성 할 수 있다. 하지만 이 방법의 경우 모핑함수 혹은 블록 섞기의 규칙을 알면 원 생체영상으로 복원이 가능하다는 단점이 있다.

Savvides et al.[3]은 MACE(Minimum Average Correlation Energy) 필터를 이용하여 얼굴인식을 하는 방법에 적용될 수 있는 얼굴정보변환 방법에 대해 제안하였다. 학습과정에서 학습영상들을 랜덤커널(Random Kernel)과 콘볼루션(Convolution) 후 변형된 학습 영상을 생성하고 이를 이용하여 MACE필터를 생성한다. 이 랜덤커널은 사용자의 키(Key)를 초기(Seed)로 해서 생성된다. 검증과정에서는 입력영상을 학습과정과 동일한 랜덤커널로 콘볼루션을 하고 콘볼루션된 입력영상을 학습과정에서 생성된 MACE필터와 상관관계(Correlation)로 인증을 실시한다. Savvides et al. 은 랜덤커널의 사용이 인증 성능에 영향이 없다는 것을 분석적으로 실험적으로 보였다. 하지만 이 방법은 기존의 통계적 형상기반의 얼굴인식에는 적용할 수 없고 램덤커널을 아는 경우 원 영상이 복원 될 수 있다.

나. 생체특징 변환 방법

Teoh et al.[4]은 생체특징벡터를 랜덤패턴과 내적시켜 생체코드를 생성하는 BioHashing 방법을 제안하였다. 입력 생체신호에서 $n \times 1$의 생체특징벡터를 추출하고 이를 $n \times m (n \geq m)$ 랜덤패턴과 내적 시킨다. 여기서 랜덤패턴은 사용자의 토큰(token)을 초기로 랜덤생성기에서 생성된 랜덤행렬을 Gram-Schmidt 방법으로 생성한 직교(Orthonomal)행렬이다. 내적 시킨 값이 특정 값(Threshold) 보다 크면 1 작으면 0 으로 이진화 시켜 m-bit 생체코드(Biocode)를 생성하고, 이 코드를 이용하여 개인을 인증한다. 저장된 생체코드의 도난 시에는 램덤패턴을 변경시켜 새로운 생체코드를 재생성할 수 있다. 이러한 BioHashing 방법을 응용하여 얼굴[5][6], 지문[4], 장문[7][8], 홍채[9]에 적용하였다. 하지만 이 방법은 성능이 랜덤행렬의 보안성에 너무 의존적이라는 단점이 있다.[10]

Kang et al.[11]은 PBKDF(Password-Based Key Derivation Function)과 PCA를 이용한 가변얼굴생체인식 방법에 대해 제안하였다. 이 방법은 우선 마스터 키(Master key)로부터 순열행렬을 생성하여 PCA의 기저와 평균영상의 순서를 재배열 시킨 후 생성된 순열행렬을 제거함으로써 원 기저와 평균영상의 누출을 불가능하게 한다. 또 다른 순열행렬을 사용자의 패스워드에서 생성하고 이를 이용하여 입력영상의 순서를 재배열 시키고, 순서가 이미 재배열된 PCA 기저와 평균영상을 다시 재배열시킨다. 이렇게 생성된 PCA의 기저, 평균영상, 입력영상을 이용하여 얼굴특징벡터를 추출하고 이것으로 개인을 인증하는 방법이다. 이 방법은 입력얼굴영상과 PCA기저의 순서가 동일하지 않으므로 인식 성능을 저하시킬 수 있지만, 실제 얼굴영상을 이용한 실험평가는 이

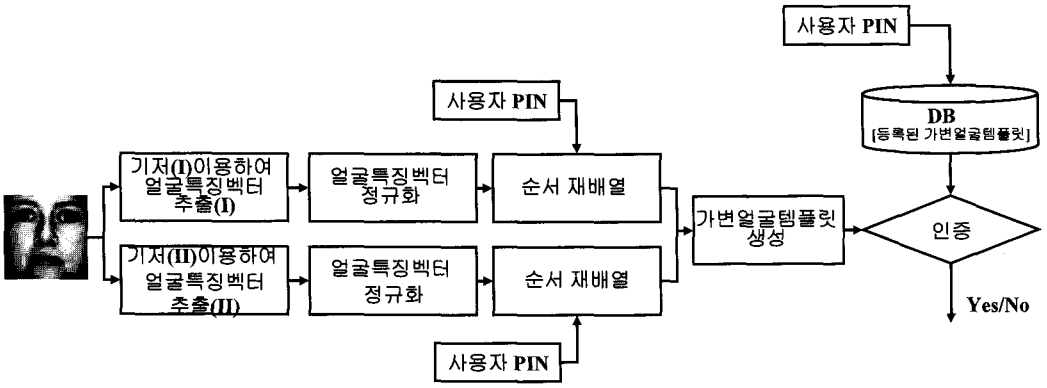


그림 1. 제안방법의 전체과정
Fig. 1. Overall block diagram of proposed method.

루어 지지 않았다.

Ang et al.[12]은 지문 특징점을 변환하여 가변지문정보를 생성하는 방법에 대해 제안하였다. 이 방법은 지문의 중심점(Core point)을 지나는 선을 사용자의 키(Key)로 기울기를 설정해서 구한 후, 그 선 아래의 지문 특징점을 선위로 반영(Reflect)시켜 변환된 지문 특징점을 생성하는 방법이다. 하지만 이방법의 경우 설정한 선 위의 특징점에는 변화가 없어 원 특징점의 정보가 변환 후에도 상당수 유지되는 단점이 있다.

Ratha et al.[1][2]은 고차다항식을 이용하여 생체특징을 변환하는 방법에 대해 소개 하였다. 고차다항식의 입력을 원 생체특징 값으로 하고 이에 대한 출력을 변환된 생체특징 값으로 하여 변환된 생체특징을 생성한다. 고차다항식을 사용하므로 변환된 생체특징에서 원 생체특징으로는 일대다의 매핑이 되어, 변환된 생체특징을 알더라도 원 생체특징의 복원이 불가능하다. 하지만 실제 생체정보에 이 방법을 적용 시 적합한 고차다항식의 파라미터와 차수의 결정이 필요한데 이에 대한 언급은 하지 않았다.

우리의 이전 논문[13]에서는 통계적 형상기반의 얼굴인식에 적용될 수 있는 가변얼굴인식 방법에 대해 소개하였다. PCA와 ICA Arch. 1 만을 이용하여 두 얼굴특징벡터의 단순 합으로 가변얼굴템플릿을 생성하는 방법에 대해 설명하였고, 가변얼굴템플릿의 보안성에 대한 평가는 이루어지지 않았다. 본 논문에서는 PCA, ICA Arch. 1, 뿐 아니라 ICA Arch. 2, NMF에서 추출된 얼굴특징벡터의 가중 합으로 가변얼굴템플릿을 생성하고, 가중치에 따른 성능과 보안성을 분석한다. Ⅱ 장에서는 제안방법에 대해 설명하고, Ⅲ에서 제안방법의 성능과 보안성에 대해 AR-FACE DB를 이용하여 평가한다.

Ⅱ. 가변얼굴템플릿 생성방법

이 장에서는 제안하는 가변얼굴템플릿 생성방법에 대해 설명한다. 가변얼굴템플릿은 두개의 얼굴특징벡터의 가중 합으로 생성되는데, 두개의 얼굴특징벡터는 서로 다른 통계적 형상기반의 얼굴특징추출 방법에 의해 구해진다. 통계적 형상기반의 얼굴특징추출 방법으로는 PCA (Principal Component Analysis)[14], ICA(Independent Component Analysis)[15][16], NMF(Nonnegative Matrix Factoriztion)[17] 등이 있다. 구해진 두 특징벡터는 우선 정규화(Normalization)되고 두 특징벡터 요소의 순서를 재배열 시킨 후 가중 합으로 가변얼굴템플릿을 생성한다.

얼굴특징벡터의 정규화는 두 얼굴특징벡터들의 요소값의 범위를 비슷하게 만들어 가중 합으로 생성된 가변얼굴템플릿에서 원 얼굴특징벡터의 정보를 추출하기 어렵게 만들기 위해 실시한다(Ⅱ. 2 장). 얼굴특징벡터의 재배열은 다 수의 가변얼굴템플릿의 생성을 위해 실시한다. 단순히 두 얼굴특징벡터들의 가중 합으로 가변얼굴템플릿을 생성할 경우 하나의 가변얼굴템플릿만이 생성될 수 있다. 이 경우 가변얼굴템플릿의 도난 시 새로운 가변얼굴템플릿으로 대치 될 수 없다. 이를 해결하기 위해 두개의 얼굴특징벡터의 가중 합 전에 각 얼굴특징벡터의 요소를 서로 다르게 재배열시킨다(Ⅱ. 3장). 재배열규칙은 사용자의 PIN에 의해 결정된다. 그러므로 가변얼굴템플릿의 도난 시 새로운 가변얼굴템플릿은 사용자의 PIN을 변경시킴으로써 재 생성될 수 있고, 동일 사용자의 경우 같은 재배열 순서가 적용되고 타인사용자와는 다른 재배열순서가 적용된다. 그림 1은 제안하는 방법의 전체과정을 보여준다.

1. 얼굴특징벡터 추출

두개의 N-차원 얼굴특징벡터(v_I,v_{II})는 입력얼굴영상을 서로 다른 기저(Basis)에 내적 시켜 아래와 같이 구해진다.

$$v_I = B_I x$$
$$v_{II} = B_{II} x \quad (1)$$

여기서 x는 M $\times$1 입력 얼굴영상이고, v_I 와 v_{II}는 N $\times$M의 서로 다른 기저행렬 B_I과 B_{II}에 의해 구해지는 얼굴특징벡터이다.

2. 얼굴특징벡터 정규화

가변얼굴템플릿은 두 개의 얼굴특징백터의 가중 합으로 생성되므로 원 얼굴특징벡터의 정보 보호를 위해서는 정규화 과정이 필요하다. 예를 들어 얼굴특징벡터 v_I의 요소 값이 v_{II}의 요소 값 보다 매우 클 경우 두 얼굴특징벡터를 더해 생성된 가변얼굴템플릿에는 v_{II}의 요소 값이 무시될 수 있어 얼굴특징벡터 v_I의 정보가 생성된 가변얼굴템플릿에 노출 될 수 있다. 얼굴특징벡터의 정규화는 다음과 같이 구해진다.

$$\hat{v} = v/|v| = \{v_1/|v|, v_2/|v|, \ldots v_n/|v|\} \quad (2)$$

여기서 |v|는 얼굴특징벡터 v의 놈(Norm)이다.

3. 순서 재배열

가변얼굴템플릿의 도난 시 새로운 가변얼굴템플릿 생성을 위해 정규화 된 두개의 얼굴특징벡터 요소를 서로 다르게 재배열 시킨다. N×N 순열행렬 (Permutation Matrix) Θ 와 Φ를 이용하여 순서가 재배열된 얼굴특징벡터는 다음과 같이 구해진다.

$$\tilde{v_I} = \Theta \hat{v_I}$$
$$\tilde{v_{II}} = \Phi \hat{v_{II}} \quad (3)$$

여기서 $\hat{v_I}$와 $\hat{v_{II}}$는 정규화 된 얼굴특징벡터이다. 두개의 순열행렬은 사용자의 PIN을 초기로 램덤하게 생성된다.

4. 가변얼굴템플릿 생성

가변얼굴템플릿은 정규화 및 순서가 재배열된 두개의 얼굴특징벡터 $\tilde{v_I}$와 $\tilde{v_{II}}$의 가중 합으로 아래와 같이 구해진다.

$$t = r\tilde{v_I} + (1-r)\tilde{v_{II}} \quad 0 \le r \le 1 \quad (4)$$

여기서 r은 가중치를 나타낸다. 이렇게 생성된 가변얼굴템플릿(t)은 사용자의 PIN과 함께 얼굴템플릿DB에 저장되고 새로운 입력 얼굴영상에서 생성된 가변얼굴템플릿과 비교함으로써 개인을 인증한다.

* 제안방법의 비가역성(Invertibility of proposed method)

가변생체인식은 변환된 생체정보와 변환 방법을 알더라도 원 생체정보의 복원이 쉽지 않아야 한다(비가역성). 생성된 가변얼굴템플릿은 원 얼굴특징벡터 v_I과 v_{II}를 이용하여 다음과 같이 표현될 수 있다.

$$t = r\tilde{v_I} + (1-r)\tilde{v_{II}} = r\lambda\Theta v_I + (1-r)\eta\Phi v_{II} \quad (5)$$

여기서 λ와 η는 $\frac{1}{|v_I|}$ 와 $\frac{1}{|v_{II}|}$로 시스템에 저장되지 않고 얼굴특징벡터 v_I과 v_{II}에서 구해지는 요소이다. 시스템이 해커에 의해 침입당하면, 가변얼굴템플릿(t), 생성방법, 두개의 순열행렬(Θ, Φ), 가중치(r)가 노출될 수 있다. 하지만 이들 정보를 모두 알더라도 미지수의 개수는 2N+2 (2N은 두 개 얼굴특징벡터, 2는 λ 와 η)이고 방정식의 수는 N이 된다. 고로 가변얼굴템플릿 t와, 변환방법을 알더라도, 가변얼굴템플릿에서 원 얼굴특징벡터를 추출하는 것은 쉽지 않다.

* 제안방법의 재생산성

가변생체인식 방법은 다수의 변환된 생체정보의 생성이 가능해야 한다(재생산성). 제안하는 방법은 사용자의 PIN를 변경함으로써, 순열행렬을 변경하여 새로운 가변얼굴템플릿을 생성할 수 있다. 재생성이 가능한 가변얼굴템플릿의 개수는 얼굴특징벡터의 차원에 의해 결정된다. 수학적으로 N-차원의 얼굴특징벡터를 사용하면 N! 개의 새로운 가변얼굴템플릿이 재 생성될 수 있다. 예를 들어 두 개의 50차원의 얼굴특징벡터를 사용하여 50차원의 가변얼굴템플릿을 생성할 경우 제안 방법은 50! ($\cong 3\times10^{64}$)개의 새로운 가변템플릿을 생성할 수 있다.

Ⅲ. 실 험

1. 실험 방법 및 평가 항목

제안 방법의 평가를 위해 AR-face DB[18]를 사용하였

다. AR-face DB는 가림, 표정변화, 조명변화에 따른 얼굴영상들을 포함하고 있다. 이중에서 본 논문에서는 가림과 절규(Scream) 표정을 제외한 100명분 600장의 얼굴영상들을 이용하여 평가하였다. 이중 50명분 300장은 학습을 위해 사용하였고, 나머지 50명분 300장은 평가를 위해 사용하였다. 학습에서는 Turk[14]의 방법으로 PCA의 기저를 구하였고, FAST-ICA[16] 방법으로 ICA Arch. 1 과 ICA Arch. 2의 기저를 구하였고, Lee[17]의 방법으로 NMF의 기저를 구하였다. 등록 얼굴템플릿과 입력 얼굴템플릿과의 유사도는 L_2거리를 사용하였다. 가변얼굴템플릿은 PCA와 ICA Arch. 1에서 추출된 특징벡터의 가중 합, PCA와 ICA Arch. 2에서 추출된 특징벡터의 가중 합, PCA와 NMF에서 추출된 특징벡터의 가중 합의 세 경우에 대해 생성하고 아래와 같은 항목을 평가 하였다.

(i) 성능비교: 원 얼굴특징벡터(PCA, ICA Arch. 1, ICA Arch. 2, NMF)를 사용할 때와 두 얼굴특징벡터의 가중 합으로 생성된 가변얼굴템플릿을 사용할 때의 성능을 EER(Equal Error Rate)로 비교 하였다. EER은 타인을 본인이라 판단하는 오류율 (FAR: False Accept Rate)과 본인을 본인이라 판단하지 않는 오류율 (FRR: False Reject Ratio)이 같을 때의 오류율을 나타낸다. 제안한 가변얼굴템플릿을 사용할 경우는 모든 사용자가 고유의 사용자 PIN 갖고 있는 경우와, 모든 사용자가 같은 사용자 PIN을 갖고 있는 경우로 나누어서 EER을 구하였다.

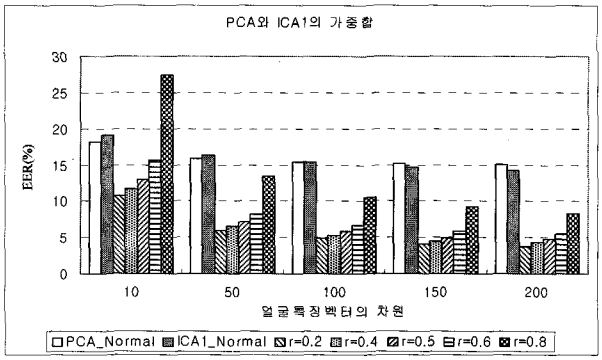
(ii) 변환성 평가: 생성된 가변얼굴템플릿은 원 얼굴특징벡터와 달라야 한다. 이를 평가하기 위해 같은 얼굴영상에서 생성된 가변얼굴템플릿과 정규화된 원 얼굴특징벡터와의 L_2거리를 측정하고, 이 L_2거리가 시스템 임계치 보다 작은 것들의 비율을 오류성공률(False Success Rate)로 정의하여 계산하였다. 오류성공률은 얼굴특징벡터가 제안한 방법으로 변환이 되어도 정규화된 원 얼굴특징벡터와 정합되는 경우의 비율이다. 또한 저장된 가변얼굴템플릿의 도난 시 새로운 가변얼굴템플릿으로 대치되어야 하는데, 이때 두 가변얼굴템플릿은 서로 정합이 되어서는 안 된다. 이 경우는 도난 된 가변얼굴템플릿으로 시스템을 공격하는 상황과 같다. 이를 평가하기 위해 같은 얼굴영상에서 사용자의 PIN을 다르게 하여 생성된 서로 다른 가변얼굴템플릿간의 L_2거리를 구하고, 이를 이용하여 오류성공률(False Success Rate)을 구하였다. 여기서 오류성공률은 서로 다른 가변얼굴템플릿이 같은 가변얼굴템플릿으로 잘못 정합되는 비율이다.

(iii) 무차별 공격(Brute force attack): 생체인식은 무차별 공격에 노출 될 수 있다.[19] 제안한 시스템의 무차별 공격에 대한 강인성은 랜덤하게 생성된 얼굴특징벡를 이용하여 모조가변얼굴템플릿(Pseudo changeable face template)을 생성하고 이를 얼굴영상에서 생성된 가변얼굴템플릿과 비교하여 평가하였다.

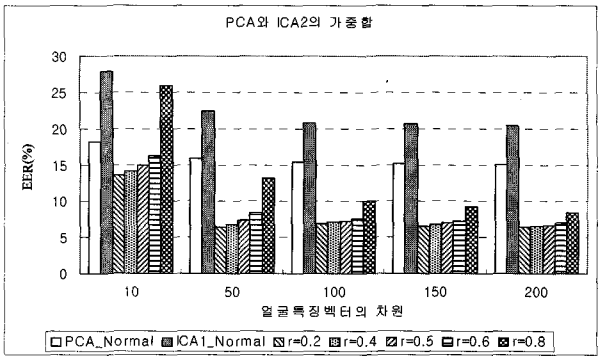
2. 성능비교 평가.

제안한 가변얼굴템플릿을 이용하여 개인을 인증하는 경우와 정규화 된 원 얼굴특징벡터($\hat{v}_I$, $\hat{v}_{II}$)를 이용하여 개인을 인증하는 경우의 성능을 EER(Equal Error Rate)로 비교 평가하였다. 가변얼굴템플릿을 이용하여 개인을 인증할 경우는 모든 사용자가 고유의 사용자 PIN을 사용할 때와, 모든 사용자가 같은 사용자 PIN을 공유할 때로 나누어 평가 하였다. 얼굴특징벡터의 순서 재배열 방법이 사용자 PIN을 초기로 랜덤하게 결정되므로 100개의 다른 사용자 PIN을 이용하여 100개의 가변템플릿을 만들고 이에 대한 평균 EER을 구하였다. 각각의 경우 얼굴특징벡터의 차원이 10, 50, 100, 150, 200일 때, 가중치 r이 0.2, 0.4, 0.5, 0.6, 0.8인 경우에 대한 성능을 구하였다. 그림 2는 모든 사용자가 고유의 사용자 PIN을 사용할 경우의 성능을 나타내고, 그림 3은 모든 사용자가 같은 사용자 PIN을 사용할 경우의 성능을 나타낸다.

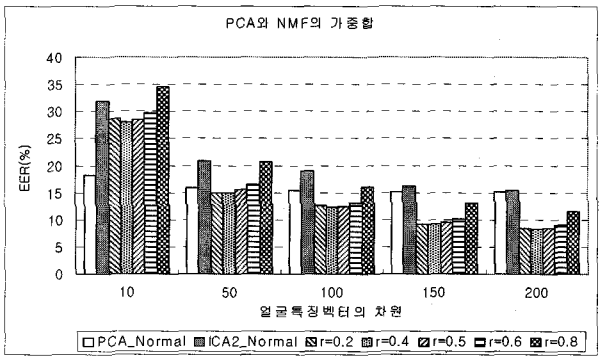
각 사용자가 고유의 사용자 PIN을 사용하는 경우는, 사용자마다 서로 다른 재배열 방법이 가변얼굴템플릿 생성 시 적용되므로 본인과 타인과의 구분력이 커져, 정규화 된 원 얼굴특징벡터를 사용하는 경우보다 가변템플릿을 사용하는 경우가 성능이 향상됨을 볼 수 있다. 모든 사용자가 같은 사용자 PIN을 사용할 경우는 가변얼굴템플릿을 사용 할 때의 성능이 정규화 된 원 얼굴특징벡터를 사용하는 경우 보다 약간 저하되었다. 변환성(III. 3) 및 무차별 공격(III, 4)에 대한 평가를 위해 Th-Dim을 정의한다. Th-Dim 은 Dim-차원의 가변얼굴템플릿을 이용해 매칭 시 EER이 계산되는 시스템 임계치(Threshold)이다. 즉 FAR(False Accept Rate)과 FRR(False Reject Rate)이 같아질 때의 L2 거리이다. 고로 두 가변얼굴템플릿간의 L2 거리가 Th-Dim보다 작으면, 두 가변얼굴템플릿은 같은 얼굴영상에서 생성된 것으로 판단되고, Th-Dim 보다 크면 두 가변얼굴템플릿은 다른 영굴영상에서 생성 된 것으로 판단되는 얼굴검증의 기준이 된다.



(a) PCA와 ICA Arch. 1의 특징벡터의 가중 합으로 생성된 가변템플릿의 경우

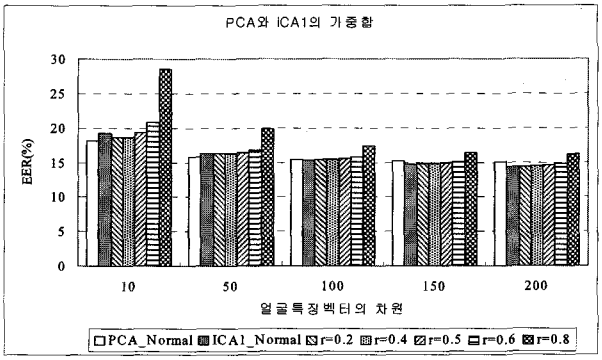


(b) PCA와 ICA Arch. 2의 특징벡터의 가중 합으로 생성된 가변템플릿의 경우

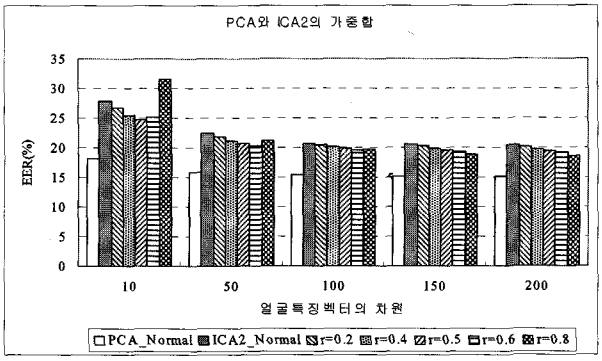


(c) PCA와 NMF의 특징벡터의 가중 합으로 생성된 가변템플릿의 경우

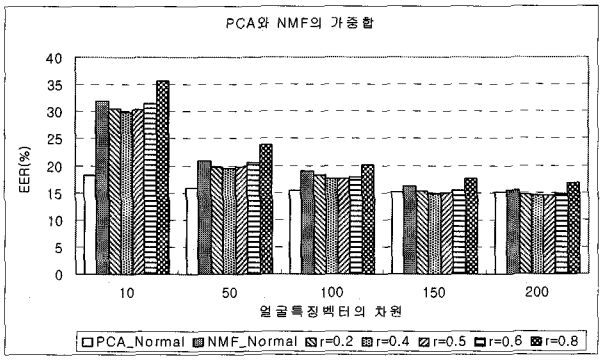
그림 2. 사용자 PIN이 다를 때 EER
Fig. 2. EER for different user's PIN.



(a) PCA와 ICA Arch. 1의 특징벡터의 가중 합으로 생성된 가변템플릿의 경우



(b) PCA와 ICA Arch. 2의 특징벡터의 가중 합으로 생성된 가변템플릿의 경우



(c) PCA와 NMF의 특징벡터의 가중 합으로 생성된 가변템플릿의 경우

그림 3. 사용자 PIN이 같을 때 EER(%)
Fig. 3. EER(%) for same user's PIN.

3. 변환성 평가

가변생체인식의 경우 원 생체정보와 변환된 생체정보는 달라야한다(변환성). 제안 방법의 변환성 평가를 위해 다음과 같은 실험을 실시하였다. (i) 입력된 얼굴영상에서 상이한 통계적 형상기반의 기법을 이용하여 두 개의 정규화 된 원 얼굴특징벡터($\hat{v_I}$, $\hat{v_{II}}$) 및 사용자 PIN을 변경하여 100개의 가변얼굴템플릿을 생성한다. (ii) 각 정규화 된 원 얼굴특징벡터와 가변얼굴템플릿간의 L_2거리를 구한다. (iii) 구한 L_2의 거리가 Th-Dim 보다 작은 경우의 개수를 구해, 전체에 대한 비율(오류성공률)을 구한다. 표 1은 위와 같은 방법으로 구한 얼굴특징벡터의 차원 및 가중치에 따른 오류성공률(False Success Rate)를 나타낸다. 오류성공률은 차원이 커질수록 낮아지고, 가중치가 한쪽 특징벡터에 크게 가중되면 커짐을 알 수 있다. 이는 한쪽 특징벡터에

표 1. 가변얼굴템플릿과 정규화 된 원 얼굴특징벡터간의 변환성
Table 1. Changeability between changeable face templates and normalized original face feature vectors.

(a) PCA와 ICA Arch.1의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA1}})$ 생성된 가변얼굴템플릿과 정규화 된 PCA 특징벡터와의 정합 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	0.770	1.248	2.64	5.434	15.482
50	0	0	0	0.002	0.477
100	0	0	0	0.042	0.4
150	0	0	0	0.008	0.224
200	0	0	0	0	0.04

(b) PCA와 ICA Arch.1의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA1}})$ 생성된 가변얼굴템플릿과 정규화 된 ICA Arch.1특징벡터와의 정합 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	16.253	4.805	2.109	1.016	0.778
50	0.456	0	0	0	0
100	0.010	0	0	0	0
150	0	0	0	0	0
200	0	0	0	0	0

(c) PCA와 ICA Arch.2의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA2}})$ 생성된 가변얼굴템플릿과 정규화 된 PCA 특징벡터와의 정합 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	0.149	0.362	1.290	4.290	16.965
50	0	0	0	0.0453	0.6
100	0	0	0	0	0.024
150	0	0	0	0	0.005
200	0	0	0	0	0.010

(d) PCA와 ICA Arch. 2의 특징벡터들의 가중 합 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA2}})$으로 생성된 가변얼굴템플릿과 정규화 된 ICA Arch. 2 특징벡터와의 정합 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	20.933	5.005	1.328	0.336	0.117
50	0.208	0	0	0	0
100	0	0	0	0	0
150	0	0	0	0	0
200	0	0	0	0	0

(e) PCA와 NMF의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{NMF}})$ 생성된 가변얼굴템플릿과 정규화 된 PCA 특징벡터와의 정합 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	8.525	7.834	8.872	11.192	18.725
50	0.146	0.058	0.112	0.226	1.248
100	0.037	0.013	0.072	0.218	0.584
150	0.002	0	0	0.008	0.162
200	0	0	0	0	0.008

(f) PCA와 NMF의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{NMF}})$ 생성된 가변얼굴템플릿과 정규화 된 NMF 특징벡터와의 정합 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	24.013	13.922	10.648	9.184	9.754
50	5.776	1.08	0.5013	0.277	0.261
100	1.114	0.093	0.024	0.008	0.026
150	0.416	0.002	0.002	0	0
200	0.096	0	0	0	0

가중치가 커지면, 가변얼굴템플릿에 가중치가 커진 특징벡터의 정보를 더 많이 포함되기 때문이다. 가중치가 0.5이고 가변얼굴템플릿의 차원이 50차원 이상이면 오류성공률은 0.6%미만으로 나타난다.

저장된 가변얼굴템플릿의 도난 시 새로운 가변템플릿은 사용자의 PIN을 다르게 하여 생성한 후 도난 된 가변템플릿을 대치한다. 이때 새로 생성된 가변템플릿은 도난된 가변템플릿과 정합되어서는 안된다. 이를 평가하기 위해 다음과 같은 실험을 실시하였다. (i) 입력된 얼굴영상에서 사용자의 PIN을 다르게 하며 100개의 가변얼굴템플릿을 생성한다. (ii) 서로 다른 사용자 PIN에서 생성된 가변얼굴템플릿의 L_2거리를 구한다. (iii) 구한 L_2의 거리가 Th-Dim 보다 작은 경우의 개수를 구해 전체에 대한 비율을 구한다(오류성공률). 표 2 는 위와 같은 방법으로 구한 오류성공률을 얼굴특징벡터의 차원 및 가중치에 따라 구한 것을 보여준다. 오류 성공률은 PCA와 NMF의 특징벡터들의 가중 합으로 가변얼굴템플릿을 생성하는 경우가 가장 높고, PCA와 ICA Arch. 1,2의 경우는 가중치가 0.5일 때 차원이 50차원 이상이면 0.2%미만의 오류성공률을 나타냈다. 가중치가 작으면 두 개의 서로 다른 가변템플릿간의 오류성공률은 낮아지지만, 표. 1에서 보인바와 같이 가중치가 한 쪽 특징벡터로 더 가중되므로 정규화 된 원 특징벡터와의 오류성공률은 증가된다.

3. 무차별 공격

제안 시스템의 무차별 공격에 대한 강인성을 평가하기 위해 다음과 같은 실험을 실시하였다. (i) 입력영상에서 제안한 가변얼굴템플릿을 생성한다. (ii) 두 개의

표 2. 서로 다른 두 가변얼굴템플릿간의 오류성공률
Table 2. False success rate between two different changeable face templates.

(a) PCA와 ICA Arch. 1의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA1}})$ 생성된 가변얼굴템플릿들 간의 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	3.085	4.712	7.754	13.496	30.482
50	0.002	0.021	0.186	0.834	9.445
100	0	0	0.024	0.154	3.437
150	0	0	0.008	0.032	2.437
200	0	0	0	0.005	1.370

(b) PCA와 ICA Arch. 2의 특징벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA2}})$ 생성된 가변얼굴템플릿들 간의 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	0.258	0.8987	2.114	5.938	22.32
50	0	0	0.005	0.112	6.248
100	0	0	0	0	1.498
150	0	0	0	0	0.442
200	0	0	0	0	0.064

(c) PCA와 INMF의 특징들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{NMF}})$ 생성된 가변얼굴템플릿들 간의 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	27.52	27.176	27.92267	28.984	33.866
50	10.498	10.922	11.864	13.754	19.194
100	5.773	5.677	6.346	7.288	11.76
150	2.962	2.986	3.504	4.485	8.672
200	1.405	1.416	1.818	2.634	6.125

랜덤벡터를 생성한다: 각 요소의 값은 -1에서 1값을 갖는다. (iii) 생성된 두 랜덤벡터를 이용하여 가중 합으로 모조가변얼굴템플릿을 생성한다. (iv) (i)에서 생성한 가변얼굴템플릿과 (iii)에서 생성한 모조 가변얼굴템플릿 간의 L_2거리를 구하고, Th-Dim보다 작은 L_2가 발생하는 경우의 개수를 이용하여 오류성공률을 구한다. 한 영상에서 100개의 가변얼굴템플릿에 대해 10000개의 모조 가변얼굴템플릿을 생성하여 정합을 실시하였다. 고로 한 영상에 대한 무차별 공격의 수는 백만 번이 된다. 표 3은 무차별 공격에 대한 오류성공률(%)을 나타낸다. 표. 3에서 알 수 있듯이 가변템플릿의 차원이 50차원 이상일 때 무차별 공격에 대한 오류 성공률이 0%임을 나타내어 제안한 가변얼굴템플릿은 무차별 공격에 강인함을 알 수 있다.

표 3. 무차별 공격에 대한 오류성공률(%)
Table 3. False success rate(%) for brute force attacks.

(a) PCA와 ICA Arch. 1의 특벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA1}})$ 생성된 가변얼굴템플릿에 대한 무차별 공격 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	0.051	0.246	0.557	0.982	1.516
50	0	0	0	0	0
100	0	0	0	0	0
150	0	0	0	0	0
200	0	0	0	0	0

(b) PCA와 ICA Arch. 2의 특벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{ICA2}})$ 가중 합으로 생성된 가변얼굴템플릿에 대한 무차별 공격 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	0.004	0.093	0.227	0.515	1.326
50	0	0	0	0	0
100	0	0	0	0	0
150	0	0	0	0	0
200	0	0	0	0	0

(c) PCA와 NMF의 특벡터들의 가중 합으로 $(r\mathrm{v}_{\mathrm{PCA}}+(1-r)\mathrm{v}_{\mathrm{NMF}})$ 가중 합으로 생성된 가변얼굴템플릿에 대한 무차별 공격 시 오류성공률(%)

차원 \ r	0.2	0.4	0.5	0.6	0.8
10	1.068	2.460	2.941	2.674	1.794
50	0	0	0	0	0
100	0	0	0	0	0
150	0	0	0	0	0
200	0	0	0	0	0

IV. 결 론

본 논문은 얼굴인식에서 얼굴정보의 도난 시 발생할 수 있는 개인의 프라이버시 보호를 위한 것으로, 얼굴생체정보의 보호를 위해 원 생체정보를 사용하지 않고 변환된 얼굴생체정보를 이용하여 개인을 인증하기 위한 가변얼굴템플릿을 생성하는 방법에 관한 것이다. 두 개의 얼굴특징벡터를 서로 다른 통계적 형상기반의 얼굴특징 추출 방법에서 추출하고, 추출된 두 개의 얼굴특징벡터를 정규화 시킨다. 정규화 된 얼굴특징벡터의 요소의 순서를 재배열 시킨 후 두 벡터의 가중 합으로 가변얼굴템

플릿을 생성한다. 이렇게 생성된 가변얼굴템플릿은 가중합의 방법과 재배열 순서를 알더라도 가변얼굴템플릿으로부터 원 얼굴특징벡터의 복원이 쉽지 않고, 재배열 순서를 변경시킴으로써 얼굴템플릿 도난 시에도 다수의 새로운 가변얼굴템플릿을 생성 할 수 있다. 고로 제안한 가변얼굴템플릿 사용하여 개인을 인증할 경우 얼굴템플릿의 도난 시에도 개인의 생체정보를 보호 할 수 있다. 실험을 통해 제안한 방법이 성능과 보안성 면에서 가변생체인식의 조건을 만족한다는 것을 보여 주었다.

참 고 문 헌

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, 2001.

[2] R. M. Bolle, J.H. Connel, and N.K. Ratha, "Biometrics Perils and Patches," *Pattern Recognition*, vol. 35, pp. 2727-2738, 2002.

[3] M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla, "Cancelable Biometric Filters for Face Recognition," *Proceedings of the 17th International Conference on Pattern Recognition*, 3, pp. 922-925, Cambridge, UK, 2004.

[4] A.B.J. Teoh, D.C.L. Ngo, and A. Goh, "BioHashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, pp. 22452255, November, 2004.

[5] A.B.J. Teoh, D.C.L. Ngo, and A. Goh, "Personalised cryptographic key generation based on FaceHashing," *Computers and Security*, vol. 23, no. 7, pp. 606-614, 2004.

[6] A.B.J. Teoh, and D.C.L. Ngo, "Cancellable biometrics featuring with tokenized random number," *Pattern Recognition Letter*, vol. 26, no. 10, pp. 14541460, 2005.

[7] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for dual-factor authentication," *Pattern Analysis and Applications*, vol. 7, no. 3, pp. 255 268, 2004.

[8] Y.H. Pang, A.B. J Teoh, and D.C.L. Ngo, "Palmprint based cancelable biometric authentication system," *International Journal of Signal Processing*, vol. 1, no. 2, pp. 98-104, 2004.

[9] C. S. Chin, A.B.J. Teoh, and D.C.L. Ngo, "High security Iris verificationsystem based on random secret integration," *Computer Vision and Image Understanding*, vol. 102, Iss. 2, pp. 169-177, 2006.

[10] A. Kong, K. H. Cheung, D. Zhang, M. Kamel and J. You, "An analysis of BioHashing and its variants," *Pattern Recognition*, In Press, Corrected Proof, Available online, 27 December 2005.

[11] J. N. Kang, D. H. Nyang and K. H. Lee, "Two Factor Face Authentication Scheme with Cancelable Feature," *Lecture notes in Computer Science* 3781, pp.67-76, Oct. 2005.

[12] R. Ang. R.Safavi-Naini, and L.McAven, "Cancelable Key-Based Fingerprint Templates," Information Security and Privacy: 10th Australasian Conference, ACISP, pp. 242-252, Brisbane, Australia, 2005.

[13] M. Y. Jung, C. H. Lee, J. S. Kim, J. Y. Chol, and J. H. Kim, "A Changeable Biometric System for Appearance-Based Face Recognition," Biometric Consortium Conference (BCC 2006), Baltimore, USA, 2006.

[14] M.A. Turk and A.P. Pentland, "Eigenfaces for Recognition," Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.

[15] M. S. Bartlett, J. R. Movellan, and T. J. Sejnowski, "Face Recognition by Independent Component Analysis," *IEEE Trans. Neural Networks*, vol. 13, no. 6, pp. 1450-1464, 2002.

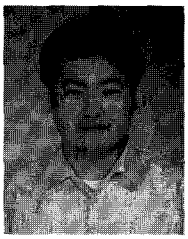
[16] A. Hyvarinen and E. Oja, "Independent component analysis: a tutorial," http://www.cis.hut.fi/~aapo/papers/IJCNN99_tutorialweb/, 1999.

[17] D. D. Lee and H. S. Seung, "Learning the parts of objects by non-negative matrix factorization," Nature, vol. 401, pp. 788-791, 1999.

[18] A.M. Martinez and R. Benavente, "The AR Face Database," CVC Tech, 1998.

[19] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, New York, 2003.

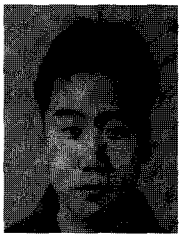
저 자 소 개



이 철 한(정회원)

2000년 명지대학교 전자공학과 학사 졸업
2002년 연세대학교 전기전자 공학과 석사 졸업
2007년 연세대학교 전기전자 공학과 박사 과정

<주관심분야 : 생체인식, 컴퓨터 비젼, 패턴인식>



김 종 선(정회원)

1999년 목포대학교 컴퓨터공학과 학사
2002년 성균관대학교 전기전자 및 컴퓨터공학부 석사
2006년 성균관대학교 전기전자 및 컴퓨터공학부 박사

2007년 연세대학교 생체인식연구센터 연구교수
<주관심분야 : 생체인식, 패턴인식, 컴퓨터 비젼, 영상인식>

김 재 희(정회원)

1979년 연세대학교 전자공학과 졸업
1982년 Case Western Reserve University 전기공학 석사
1984년 Case Western Reserve University 전기공학 박사

2007년 연세대학교 전기전자공학부 교수
2007년 과학기술부 지정 생체인식 연구센터 소장
<주관심분야 : 생체인식, 패턴인식, 컴퓨터 비젼, 영상인식>

정 민 이(정회원)

1997년 세종대학교 정보통신 공학과 학사
1999년 연세대학교 생체인식협동 과정 석사
2007년 연세대학교 전기전자 공학과 박사 과정

<주관심분야 : 생체인식, 컴퓨터 비젼, 패턴인식>

최 정 윤(정회원)

1992년 연세대학교 전자공학과 학사
1994년 연세대학교 전자공학과 석사
1999년 MIT 전기컴퓨터과 박사
2007년 연세대학교 전기전자 공학부 교수

<주관심분야: 신호처리, 음성인식, 생체인식, 인지과학>