논문 2007-44SP-6-3

독립성분 분석 계수의 합성에 의한 가변 얼굴 생체정보 생성 방법

(Generation of Changeable Face Template by Combining Independent Component Analysis Coefficients)

정 민 이*, 이 철 한*, 최 정 윤*, 김 재 희*

(MinYi Jeong, Chelhan Lee, Jeung-Yoon Choi, and Jaihie Kim)

요 약

개인 인증 방법 중 하나인 생체인식(Biometrics)은 개인 생체정보의 수가 한정되어 있기 때문에 생체정보의 도난 시 프라이버시 침해라는 문제를 가진다. 이 문제를 해결하기 위해 등장한 개념이 가변 생체인식(Changeable biometrics)이다. 가변 생체인식은 생체정보가 훼손당했을 경우 새로운 생체정보로 대체하기 어렵다는 생체인식의 가장 큰 단점을 보완하기 위한 방법으로 원 생체정보가 아닌 변환된 생체정보로 개인을 인증한다. 이 논문에서는 가변 생체인식 가운데 얼굴인식을 위한 가변 생체인식에 대해 제안한다. 기존에 알려진 얼굴인식의 방법 가운데 하나인 외형 기반 기법(Appearance-based method) 중 독립성분 분석(Independent Component Analysis)의 계수(coefficient)를 변형하는 방법을 제안한다. 제안된 얼굴 생체정보 생성 방법은 계수의 일부분을 가우시안 분포(Gaussian distribution)에 따른 임의의 값으로 치환한 후 계수의 순서를 임의로 변경하여 무수히 많은 가변 얼굴 정보를 생성할 수 있도록 하였고 서로 다르게 변경된 계수들을 서로 합성함으로써 비가역성(Non-invertibility)을 만족시키려고 시도했다.

Abstract

Changeable biometrics has been developed as a solution to problem of enhancing security and privacy. The idea is to transform a biometric signal or feature into a new one for the purposes of enrollment and matching. In this paper, we propose a changeable biometric system that can be applied to appearance based face recognition system. In the first step when using feature extraction, ICA(Independent Component Analysis) coefficient vectors extracted from an input face image are replaced randomly using their mean and variation. The transformed vectors by replacement are scrambled randomly and a new transformed face coefficient vector (transformed template) is generated by combination of the two transformed vectors. When this transformed template is compromised, it is replaced with new random numbers and a new scrambling rule. Because the transformed template is generated by the addition of two vectors, the original ICA coefficients could not be easily recovered from the transformed coefficients.

Keywords: Biometrics, Changeable biometrics, Face recognition, Independent component analysis

I. 서 론

생체인식[1~2]이란 지문, 홍채, 얼굴, 손등혈관, 손금, 걸음걸이 같은 개인의 독특한 생체정보를 사용하여 개인 인증을 하는 방법 중 하나이다. 이러한 생체인식은 개인의 특정 신체 정보를 사용하므로 쉽게 도난당할 수 없다는 점, 휴대의 불편함이 없다는 점, 잊어버리지 않는 다는 점 등 많은 장점이 있다. 그러한 반면에 몇 가지 문제점도 가지고 있다. 생체인식의 문제점이 되는 원인 중 하나는 개인의 생체특성을 이용한다는 것으로 이것은 생체인식의 큰 장점이기도 하지만 오히려 프라이버시 침해 문제를 야기 시킬 수 있다. 생체특성은 그 수가 한정되어 있기 때문에 도난이나 손상을 당했을 경

* 정회원, 연세대학교 생체인식 연구센터
(Biometric Engineering Research Center, Yonsei University)
※ 본 연구는 한국과학재단 지정 생체인식 연구센터 (BERC)의 지원을 받아 이루어졌습니다.
접수일자: 2007년2월23일, 수정완료일: 2007년10월29일

우 취소 또는 대체가 불가능하거나 그 횟수가 매우 제한된다. 게다가 한 사람이 가지는 생체특성은 고유하기 때문에 도난을 당한 한 가지 정보를 이용하여 여러 인식기를 공격 할 수 있다. 이런 문제는 생체인식이 비밀번호나 열쇠처럼 쉽게 취소하거나 변경할 수 없기 때문에 발생한다. 이런 프라이버시 문제는 최근에 생체인식 분야에서 큰 이슈(issue)가 되고 있다.

가변 생체인식[3]은 이런 생체인식 문제를 해결하기 위한 방법이다. 가변 생체인식은 '변경 가능하다'는 의미로, 저장된 생체정보를 도난당하면 등록 되어있던 생체정보를 취소하고 새롭게 변경하여 사용할 수 있음을 뜻한다. 가변 생체인식을 위해서는 먼저 변환 함수를 선택하여 생체정보를 변환하고, 변환된 생체정보를 실제 시스템을 위한 생체 정보로 사용하게 된다. 이 변환 함수는 사람에 따라 또는 시스템에 따라 다르게 주어지며, 만약 생체정보가 도난을 당했을 경우 기존의 생체정보는 제거를 하고 새로운 변환 함수를 할당 받아 새로운 생체정보를 다시 생성하게 된다. 이때 변경된 함수로 만들어진 생체정보는 이전의 생체정보와 전혀 상관성이 없으며 원본 생체정보로 복구하는 것도 불가능하다.

가변 생체인식을 위해서 우리는 4가지 고려사항을 제안한다[9]. 첫째, 변경된 생체정보를 알고 있다고 하더라도 이 데이터는 원본 영상으로 복원 되어서는 안 된다. 이것을 비가역성(Non-invertibility)이라고 지칭한다. 가변 생체인식의 가장 중요한 목적은 시스템에 저장되어있는 생체 정보를 도난 또는 훼손당했을 경우에도 개인의 고유한 원본 생체 정보에는 영향을 미치지 않음에 있다. 만약 어떠한 경우에도 원본 생체정보를 알아낼 수 없다는 비가역성을 만족한다면 프라이버시 문제는 해결된다. 둘째, 변형된 생체정보는 원본 영상과 충분히 달라야 하며, 변형 된 정보들도 서로 달라야 한다. 이것을 변화성(Changeability)이라고 지칭한다. 가변 생체인식은 원 생체 정보 또는 변환된 생체 정보와 전혀 관계없는 새로운 생체 정보로 변경을 하여 사용하는 데 그 목적이 있기 때문에 변화성은 가변 생체인식을 위해 고려되어야 할 중요한 요소 중 하나다. 셋째, 변환 함수는 무한히 생성될 수 있어야 한다. 가변 생체인식은 훼손을 당할 때마다 이전에 사용하던 생체정보를 취소하고 새로운 생체정보를 재등록 하여 사용하는 것 이므로 생체정보의 변형 가짓수는 무한하거나 또는 매우 많아야 한다. 이것을 재생산성(Reproducibility)이라고 지칭한다. 넷째, 변형 후의 인식률은 변형 전의 인식률을 유지하거나 저하가 적어야 한다. 가변 생체인식 또한 개인인증의 한 종류이므로 인증 성능에 큰 영향을 미쳐서는 안 된다. 이 논문에서 우리는 제안된 방법을 통한 실험결과를 위에서 서술한 고려사항을 통하여 성능 평가 및 분석을 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 얼굴 정보를 이용한 기존의 가변 생체인식 방법을 기술하고 Ⅲ장에서는 얼굴 정보를 추출하는 독립성분 분석 방법과 제안된 가변 생체인식 방법을 소개한다. Ⅳ장에서는 실험 및 분석, Ⅴ장에서는 결론으로 구성된다.

Ⅱ. 기존의 가변 얼굴 생체정보 생성 방법

생체정보 변환 방법을 소개한 Ratha et a.l[4]는 얼굴 생체신호 변환 방법으로 모핑(Morphing) 방법을 이용하였다. 이 방법은 입력 얼굴 영상을 모핑 함수로 변환시켜 새로운 얼굴 생체정보를 얻는다. 변환된 얼굴 정보가 도난이나 도용을 당했을 경우에는 새로운 모핑 함수를 이용하여 새롭게 변환된 생체정보를 획득할 수 있다. 하지만 악의적인 공격자가 모핑의 방법만 안다면 원 생체신호로의 복원이 가능하다는 심각한 문제점이 있다.

얼굴 생체신호를 변환하는 또 다른 방법으로MACE (Minimum Average Correlation Energy) 필터를 이용하는 방법이 있다[5]. 이는 랜덤 수 생성기(Random Number Generator)에서 생성된 랜덤 커널(Random Kernel)로 영상들을 변형 후 MACE 필터를 생성하여 인증하는 방법이다. 등록 과정에서 랜덤커널과 콘볼루션(Convolution)후 변형된 학습영상을 생성하고, 이 영상들에서 MACE필터를 생성한다. 만약 자신의 생체정보가 도난당하였을 경우, 새로운 랜덤 커널을 생성하여 생체정보를 재생성 시킬 수 있다. 그러나 이 방법은 MACE필터를 이용하는 얼굴인식 시스템에서만 적용이 가능하며 MACE필터와 변형된 영상을 알 경우 원 생체신호로 복원이 가능하다.

Teoh et al.[6]는 BioHashing 방법을 제안 하였다. 입력된 영상에서 FDA(Fisher Discriminant Analysis)를 이용하여 $m \times 1$ 특징벡터를 계산하고 계산된 특징 벡터를 $m \times n$ 랜덤 패턴과 내적을 시킨다. 여기서 랜덤 패턴은 랜덤 생성기로 랜덤 행렬을 생성 후 Gram-Schmidt 방법을 적용하여 직교행렬(Orthonormal Metrics)로 만든 행렬이다. 이러한 랜덤패턴과의 내적 후 특정 값(Threshold)보다 크면 1 작으면 0으로 이진

화 시켜 복원이 불가능한 코드를 생성하게 된다. 만약 도난이나 도용을 당할 경우 새롭게 생성해낸 랜덤패턴을 사용하여 만들어낸 새로운 생체 코드를 사용 할 수 있다. 이 논문의 실험 결과 FAR(False Accept Rate)과 FRR(False Reject Rate)이 0%가 나왔다. 하지만 이 논문의 결과는 Kong et al.[7]에 의해서 랜덤코드에 매우 의존적인 것으로 반증되었다.

Kang et al.[8]은 PCA(Principal Component Analysis)와 PBKDF(Password-Based Key Derivation Function)의 합성에 의한 가변 생체인식을 제안했다. 제안한 인증 시스템은 비밀번호와 얼굴 영상 두 요소를 사용한다. 변형함수는 PBKDF를 통한 비밀번호에 의해서 생성되며 시스템에는 변형 함수가 적용된 생체정보만이 저장된다. 생체정보 도난 시, 비밀번호의 변경에 의해 새로운 생체정보 생성이 가능하다. 그러나 이 시스템은 공격자가 변형된 생체정보와 변형 함수를 알고 있다면 원 생체정보의 복원이 가능하며, 성능에 대한 실험을 보이지 않았다.

Jeong et al.[9]은 외형 기반 기법을 이용하여 가변 생체인식을 시도하였다. PCA와 ICA를 이용하는 방법 은 한 영상에서 PCA와 ICA의 계수를 추출하고 각각을 평준화(normalization) 한 후 각 계수를 서로 다른 순서로 섞고 더한다. 이 방법은 두 개의 다른 계수를 사용하기 때문에 사용이 불편하며, 성능 이외의 가변 생체인식을 위한 평가 결과를 시행하지 않았다.

본 논문은 변형된 생체정보를 알고 있다고 하더라도 원 생체정보의 복원이 불가능하며, 가변 생체인식 시스템의 고려사항인 가변성과 재생산성에 대한 조건도 만족시키는 방법을 제안한다.

Ⅲ. 독립성분 분석의 합성에 의한 가변 얼굴 생체정보 생성 방법

1. 독립성분 분석을 이용한 얼굴 인식

얼굴 인식을 위해 널리 사용되는 방법 가운데 하나인 독립성분 분석은 주어진 데이터를 독립성을 가지는 변수에 대한 요소들의 선형 합으로 표시하는 고차통계에 기초한 다차원 변환기법이다. 이는 주성분 분석의 확장된 형태로써, 특정 신호를 구성하고 있는 독립된 성분들을 혼합된 신호로부터 분리해내는데 사용한다[10~14].

독립 성분 분석을 정의할 때에는 일반적으로 통계학적인 모델(Statistical model)이 사용되는데 n개의 관측된 랜덤 변수를 $x_1, x_2, \cdots, x_n$이라고 한다면 각각의 변수 x_i는 n개의 미지의 랜덤 변수 $s_1, s_2, \cdots, s_n$의 선형 결합으로 이루어진다고 가정한다. 관측된 변수 x_i를 $\vec{x} = [x_1, x_2, \cdots, x_n]^T$로 독립 성분들인 s_i를 $\vec{s} = [s_1, s_2, \cdots, s_n]^T$로 표기 할 때, $\vec{x}$와 $\vec{s}$의 관계는 다음 식으로 표현된다.

$$\vec{x} = \overrightarrow{As} = \sum_{i=1}^{n} a_i s_i \tag{1}$$

여기서 $\vec{A}$는 $n \times n$의 역행렬이 존재하는 정방행렬로써 혼합 행렬이며, $\vec{A}$의 열벡터인 $\vec{a_i}$는 독립 성분 분석의 기저벡터(Basis vector)라고 부른다. 만일 $\vec{s}$의 확률밀도함수가 독립 성분으로 표현될 때 원 신호는 혼합된 입력 데이터로부터 분리가 가능하다. 이런 통계적 모델을 독립성분 분석이라고 한다. 결국 독립성분 분석방법의 목적은 독립이 아닌 기저를 사용하는 입력 데이터 $\vec{x}$를 독립된 새로운 기저를 사용하는 좌표계로 변환해 주는 선형 변환 $\vec{W}$을 찾는 것이다. 찾고자 하는 원 신호의 추정 값을 $\vec{y}$라고 할 때 $\vec{y}$의 성분들을 최대한 독립적으로 만들어가며 $\vec{W}$를 추정한다. 그림 1은 독립성분 분석의 기저벡터를 이용하여 표현한 얼굴 영상을 보여준다.

2. 제안된 가변 얼굴 생체정보 생성 방법

이 장에서는 가변 생체인식을 위해서 얼굴 영상에서 추출한 독립성분 분석의 계수(ICA coefficient)를 변형하여 사용하는 방법을 제안한다. 제안된 방법은 두 개의 변형 함수를 통해 계수의 일부 값을 변형하고 순서

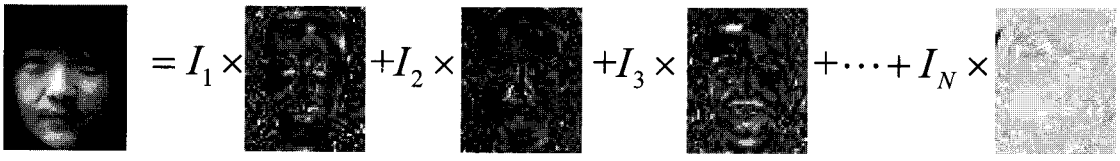


그림 1. 독립성분 분석의 기저벡터로 표현한 얼굴 영상
Fig. 1. Facial Image Representation Using ICA.

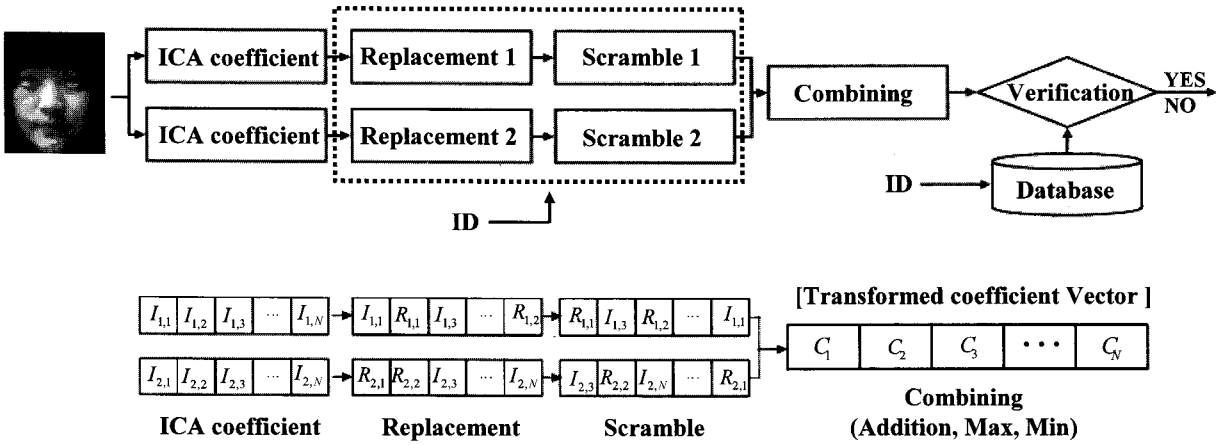


그림 2. 제안 방법의 전체적인 처리과정
Fig. 2. Overall Procedure of Proposed Method.

를 섞은 후 합성함으로써 가변 생체정보를 생성한다. 이 방법은 독립성분 분석 방법 이외의 외형 기반 기법도 적용 가능하다. 그림 2는 제안된 방법의 전체적인 처리 과정을 보여준다.

먼저, 한 영상에서 ICA를 이용하여 같은 방법으로 계수 $\vec{I}=[I_1,I_2,\cdots,I_N]$를 두 번 추출한다. 그리고 추출된 계수의 임의의 위치에 임의의 값(Random value)을 적용한다. 그림 2에서 이를 Replacement라고 지칭한다. 임의로 발생시킨 값과 추출된 계수와의 지나친 범위차를 없애기 위해 추출된 계수들의 평균과 분산에 따른 가우시안 분포에 의해 임의의 값을 얻는다. 이때 계수 값들의 치환을 위한 함수는 사용자의 ID에 의하여 결정되며 한 ID당 두 개의 치환 함수가 필요하다.

서로 다른 치환 함수에 의해 변형된 계수들은 변화성의 강화와 재생산성의 만족을 위해 스크램블링(Scrambling) 방법이 적용 된다. 각각의 계수는 임의의 스크램블링 방법이 적용되고 이 때 스크램블링 방법은 사용자의 ID에 의하여 결정된다. 우리는 두개의 스크램블링 함수를 다음과 같이 정의한다[10].

$$S_{ID}^{ICA}(\bullet),\ Z_{ID}^{ICA}(\bullet) \tag{2}$$

$S_{ID}^{ICA}(\bullet)$는 첫 번째 치환함수를 적용한 독립성분 분석 계수 $\vec{I_1}$를 위한 스크램블링 함수이고, $Z_{ID}^{ICA}(\bullet)$는 두 번째 치환함수를 적용한 독립성분 분석 계수 $\vec{I_2}$를 위한 스크램블링 함수이다. 스크램블링 방법이 적용된 후의 독립성분 분석 계수는 다음과 같이 표현 할 수 있다.

$$\begin{aligned}\vec{I_1^s}&=S_{ID}^{ICA}(\vec{I_1})\\ \vec{I_2^s}&=Z_{ID}^{ICA}(\vec{I_2})\end{aligned} \tag{3}$$

제안된 방법에서 두 변형 함수는 서로 다른 스크램블링 방법을 적용하므로 충분히 많은 재생산성이 보장된다. 만약 변형된 계수가 도난을 당하였을 경우, 스크램블링 방법과 적용 계수의 변경에 의한 새로운 함수를 이용하여 새롭게 변형된 계수를 생성 할 수 있다.

마지막으로, 서로 다른 변형 함수에 의해 변형된 계수들의 합성에 의해 가변 계수는 생성된다. 합성은 합, 최대, 최소의 방법을 선택할 수 있다.

$$\begin{aligned}C_{addition}&=\vec{I_1^s}+\vec{I_2^s}\\ &\text{or}\\ C_{\max}&=\max(\vec{I_1^s},\vec{I_2^s})\\ &\text{or}\\ C_{\min}&=\min(\vec{I_1^s},\vec{I_2^s})\end{aligned} \tag{4}$$

가변 생체인식의 조건을 만족하기 위해서, 변형된 생체정보는 원래 생체정보로 쉽게 복원이 되어서는 안 된다. 만약 침입자가 데이터베이스를 공격하여 정보를 가져간다고 하더라도 이 방법은 변형된 계수만을 저장하고 있고 변형 전의 계수들을 저장하지 않기 때문에 원 독립성분 분석 계수를 찾아내는 것은 불가능하다. 만약 침입자가 저장된 정보와 스크램블링 순서를 알고 있다고 하더라도 임의의 치환 값을 적용했기 때문에 완벽한 원 생체정보를 찾아낼 수 없다. 이 중 최대, 최소에 의한 합성을 했을 경우는 어떠한 경우에도 비가역성을 만족한다.

Ⅳ. 실험 및 분석

본 논문에서 성능 분석을 위해 AR Face 데이터베이스[15]를 사용하였다. 이 데이터베이스는 총 126명에 대한 3,200개의 정면 얼굴 영상으로 이루어졌고 각 영상은 부분 가림과 조명변화, 표정변화를 포함하며 2주에 걸쳐 획득되었다. 본 실험에서는 총 112명에 대해 6장의 표정 변화 영상만을 사용하였다. 그림 3은 실험에 사용된 영상을 보인다. 학습(Train)과 평가(Test)를 위하여 각각 336장의 영상이 사용되었다. 학습 영상들은 56명으로 구성되어있으며 나머지 56명에 대한 영상은 평가를 위해 사용되었다. 등록 템플릿과 입력 템플릿 간의 유사도 측정은 L_2거리를 사용하였다. 기저벡터의 개수(n)는 10개에서 300개까지 10개의 단위로 변경하면서 실험하였으며, 기저벡터의 20%에 해당하는 개수(r)의 계수를 평균과 분산에 의존적인 치환 값으로 랜덤하게 결정하여 치환하였다. 제안 방법은 스크램블링 함수와 치환 함수의 값이 랜덤이므로 결과 값이 매번 다르다. 그러므로 총 100번의 변경함수를 적용한 후 평균 성능을 최종 결과 값으로 보여준다. 가변 얼굴 생체정보를 사용했을 경우의 성능, 변화성, 재생산성에 대해 평가하였다.

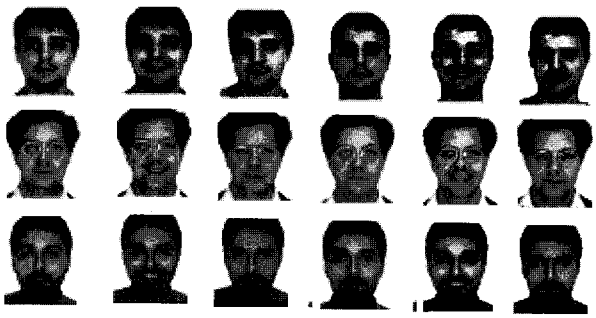


그림 3. 얼굴 DB 중 일부
Fig. 3. Sample images from the AR database.

1. 성능 비교 평가

제안한 가변 얼굴 생체정보를 이용하여 개인을 검증(Verification)하는 경우와 원 얼굴 특징정보(ICA coefficient)를 이용하여 개인을 인증하는 경우의 성능을 EER(Equal Error Rate)로 비교평가 하였다. 실험결과, 제안된 방법을 적용한 후의 EER은 원 생체정보를 이용하여 실험한 결과와 비교하여 성능의 큰 저하가 없음을 확인할 수 있었다. 특히 합에 의한 합성법은 최대, 최소에 의한 합성에 비해 좋은 성능을 보인다. 그림 4는 기저벡터 개수의 변화에 따른 EER 값의 그래프를 보여준다.

2. 변화성

변화성(변화성 1, 변화성 2)의 분석을 위하여 두 가지 실험을 하였다. 변화성 1을 위한 실험은 다음과 같다. 먼저 같은 영상에 대하여 변경 전의 계수와 변경 후의 계수를 얻는다. 이 계수들을 이용하여 L_2 거리 차를 구하고 이를 시스템 임계값(System threshold)을 기준으로 거리 차의 분포를 확인한다. 변화성 2의 실험에서는 같은 영상에 대해 서로 다른 변경 함수(변경 함수 1과 변경 함수 2)를 적용하여 얻어진 계수들을 이용하여 L_2 거리 차를 구하고 시스템 임계값을 기준으로 거리 차의 분포를 확인한다. 이때, 위 실험에 의한 거리 차이 분포를 pseudo-genuine 분포라고 지칭하며, 전체 pseudo-genuine 분포에 대해 시스템 임계값보다 오른쪽에

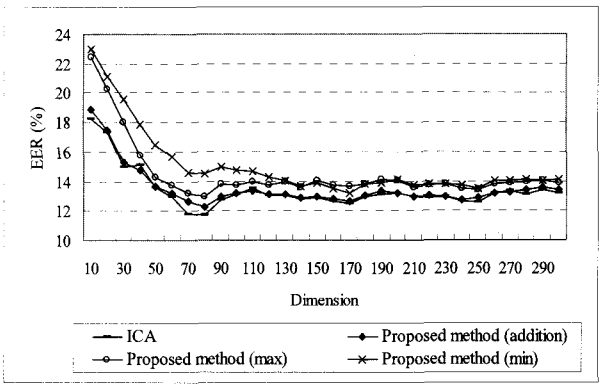


그림 4. 기저벡터 개수의 변화에 따른 ICA와 제안 방법의 인식률
Fig. 4. Recognition performance of ICA and proposed method in varying dimensions.

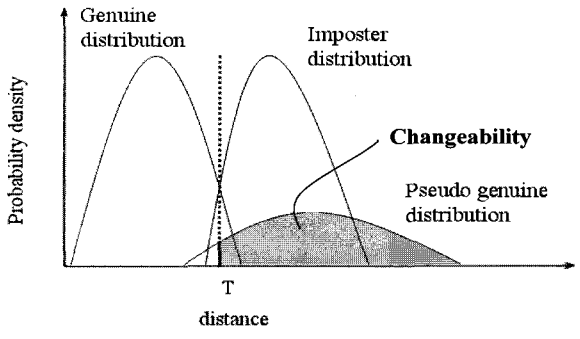
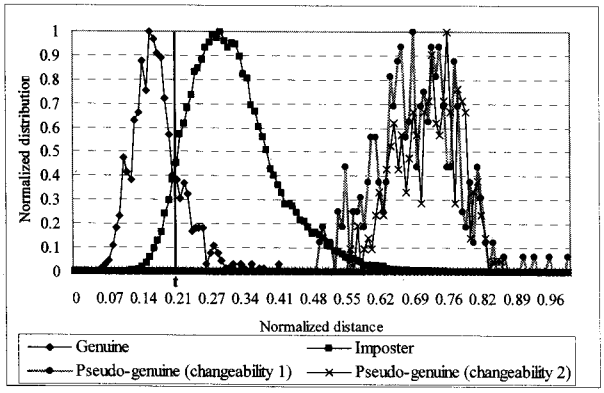
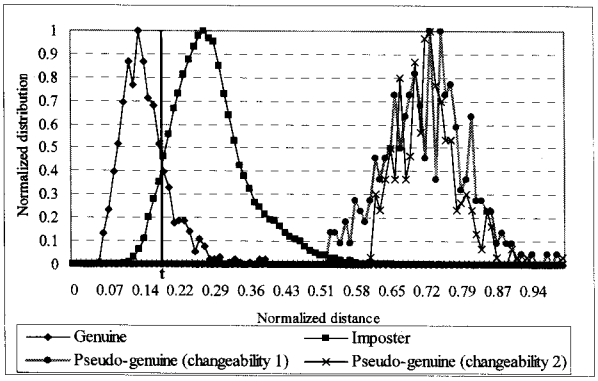


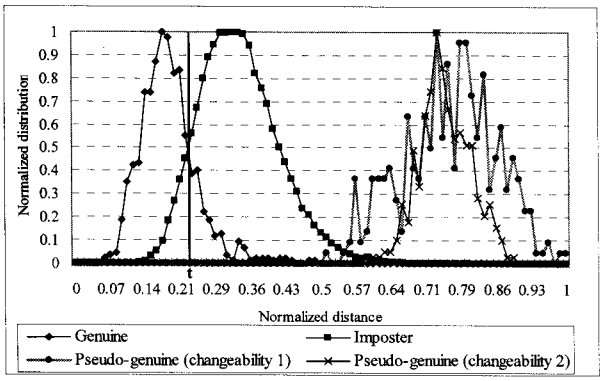
그림 5. Genuine 분포, imposter 분포, 그리고 pseudo genuine 분포의 예 (T: 시스템 임계값)
Fig. 5. The distance distributions: genuine, imposter, and pseudo genuine distribution (T: system threshold).



(a)



(b)



(c)

그림 6. 60개의 기저벡터를 사용하여 제안 방법 적용 후 Genuine, imposter, 그리고 pseudo genuine의 분포 (a) 합, (b) 최대, (c) 최소

Fig. 6. Genuine and imposter distribution, and pseudo genuine distribution applying the proposed method using number of 60 dimension (a) addition, (b) maximum, (c) minimum.

위치하는 pseudo-genuine 분포의 비율을 변화성(Changeability)이라고 한다.

Pseudo-genuine 분포가 오른쪽에 위치할수록 두 계수들 간의 거리차가 크다고 할 수 있으며, 이는 계수들이 동일인의 생체정보에서 생성되었음에도 서로 다른 생체정보로 인식함을 뜻한다. 그림 5[9]는 시스템 임계값 결정을 위한 genuine 분포와 imposter 분포, 그리고 pseudo-genuine 분포의 예를 보여준다. 시스템 임계값은 변경후의 얼굴 생체정보를 이용하여 얻은 genuine과 imposter 분포를 통해 결정하였다.

실험 결과, 기저벡터 변경에 따른 제안된 방법이 적용된 모든 분포는 시스템 임계값보다 오른쪽에 분포하였다. 그림 6은 n=60, r=12(20%)를 사용했을 경우, 합[그림 6(a)], 최대[그림 6(b)], 최소[그림 6(c)]의 합성 함수의 선택에 따른 변화성 1과 변화성 2에 대한 분포를 보여준다. 이는 제안된 방법을 적용한 후에는 동일인의 계수라고 할지라도 변경 전과 후 또는 변경 1과 변경 2의 계수들은 서로 다른 얼굴 생체정보로 판단함을 의미한다. 제안된 방법은 변화성을 충분히 만족함을 알 수 있다.

3. 재생산성

재생산성은 스크램블링 방법과 임의의 값 선택에 따른 경수의 수에 의해 계산 가능하다. 만약 총 n개의 계수의 사용하고 r개의 치환 값을 적용하였다면, 총 $\frac{n!}{r!(n-r)!}$의 경우의 수를 가질 수 있다. 여기에서 두 함수는 서로 다른 방법으로 스크램블링 되므로, 각각의 함수가 생성 될 수 있는 경우의 수는 $\frac{n!}{r!(n-r)!}\times n!$ 이다. 이때 두 변환함수의 치환함수와 스크램블링 함수가 일치할 경우를 제외하면 제안된 방법의 총 가짓수는 $(\frac{n!}{r!(n-r)!}\times n!)\times\left\{(\frac{n!}{r!(n-r)!}\times n!)-1\right\}$이다. 예를 들어 60개의 기저벡터(n=60)와 20%의 치환값(r=12)을 사용하였을 경우 총 1.80×10^{233}의 재생산이 가능하다. 따라서 이 방법은 가변 생체인식 시스템에 만족하는 재생산성을 가진다.

V. 결 론

본 논문에서는 생체인식을 이용한 개인 인증 시 나타날 수 있는 프라이버시 문제의 해결을 위하여 독립성분분석의 계수를 이용한 가변 얼굴 생체인식 구현 방법을 제안하였다. 제안된 얼굴 생체정보 생성 방법은 임의의 위치에 임의의 값으로 치환하고 각각의 계수의 순서를 임의로 변경하여 무한한 가변 얼굴 정보를 생성할 수 있도록 하였고 각 계수를 합성함으로써 비가역성을 만

족시키려고 시도했다. 제안된 방법을 이용한 실험 결과 가변 얼굴 생체정보를 사용해도 개인 인증의 성능이 유지됨을 확인 할 수 있었다. 또한 이 방법은 순서 변경을 위한 랜덤함수가 무한하므로 재생산성을 충분히 만족시키며, 계산이 간단하다. 게다가 변형된 고유계수들은 원 고유계수들의 값과 매우 다르므로 원 정보의 보호 기능을 가진다. 또한 임의의 상수와의 치환과 합성 연산(합, 최대, 최소)을 거쳤기 때문에 역변환이 불가능하다. 특히 최대, 최소 방법에 따라 합성을 하였을 경우 변경된 계수, 스크램블링 함수, 치환함수를 모두 도난당해도 역변환이 불가능하다. 또한 합에 의한 합성법은 최대, 최소 방법에 비해 좋은 성능을 보이므로 시스템 목적의 중요도에 따른 변형 함수의 선택이 가능하다.

참 고 문 헌

[1] A. K. Jain, R. Bolle, and S. Pankanti, *BIOMETRICS: Personal Identification in Networked Society,* Kluwer Academics Publishers, Norwel, MA, 1999.

[2] A. Pankanti, R. M. Bolle, and A. K. Jain, "Biometrics: the future of identification," *IEEE Computer*, Vol. 33, No. 2, pp.46-49, 2000.

[3] 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.

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

[5] 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 (ICPR 2004)*, 3, pp. 922-925, 2004.

[6] A. Teoh, D. Ngo and A. Goh, "An Integrated Dual Factor Authenticator Based on the Face Data and Tokenised Random Number," *International Conference on Bioinformatics and its Applications 2004*, LNCS 3072, pp. 117-123, 2004.

[7] 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.

[8] J. Kang, D. Nyang and K. Lee, "Two Factor Face Authentication Scheme with Cancelable Feature," *International Workshop on Biometric Recognition Systems (IWBRS)*, pp. 67-76, 2005.

[9] M.Y. Jeong, C. Lee, J. Kim, J.Y. Choi, K.A. Toh, J. Kim, "Changeable Biometrics for Appearance based Face Recognition," *Proc. of Biometric consortium conference*, September 2006.

[10] K. Bae, S. Noh, and J. Kim, "Iris Feature Extraction Using Independent Componet Analysis," *Lecture Notes on Computer Science 2688*, pp 838-844, Jun. 2003.

[11] 조용현, "조합형 고정점 알고리듬에 의한 신경망 기반 독립 성분 분석," *정보처리학회 논문지B*, 제9-B권, 제5호, pp643-652, 2002년

[12] A. Hyvrinen, and E. Oja, *Independent Component Analysis*, Wiley, 2001.

[13] A. Hyvrineni, "Fast and Robust Fixed-Point Algorithm for Independence Component Analysis," *IEEE Trans. on Neural Networks*, Vol. 10, No. 3, pp 626-634, 1999.

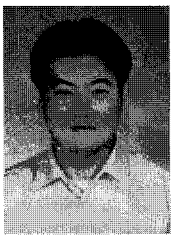
[14] 노승인, 배광혁, 박강령, 김재희, "독립 성분 분석 방법을 이용한 홍채 특징 추출," *대한전자공학회 논문지-SP* 제40권 6호, pp. 20-30, 2003년

[15] A. M. Martinez and R. Benavente, "The AR Face Database," CVC Technical Report #24, 1998.

저 자 소 개

정 민 이(정회원)
2005년 세종대학교 정보통신 공학과 학사 졸업.
2007년 연세대학교 생체인식협동 과정 석사 졸업.
2007년 연세대학교 전자공학과 박사 과정.
<주관심분야 : 생체인식, 컴퓨터 비젼, 패턴인식>

최 정 윤(정회원)
1992년 연세대학교 전자공학과 학사 졸업.
1994년 연세대학교 전자공학과 석사 졸업.
1999년 메사추세츠 공과대학 박사 졸업.
2005년 메사추세츠 공과대학 일리노이 주립대학 박사후 연구원
2006년 연세대학교 생체인식연구센터 연구교수
2007년 연세대학교 전기전자 공학부 교수
<주관심분야 : 신호처리, 음성인식, 생체인식>



이 철 한(정회원)
2000년 명지대학교 전자공학과 학사 졸업.
2002년 연세대학교 전기전자 공학과 석사 졸업.
2007년 연세대학교 전자공학과 박사 졸업.
2007년 삼성전자 SoC 연구소 책임 연구원
<주관심분야 : 생체인식, 컴퓨터 비젼, 패턴인식>

김 재 희(정회원)-교신저자
1979년 연세대학교 전자공학과 학사 졸업.
1982년 Case Western Reserve University 전기공학과 석사 졸업.
1984년 Case Western Reserve University 전자공학과 박사 졸업.
2007년 연세대학교 전기전자공학부 교수
2007년 (과학기술부/과학재단 지정 ERC) 생체인식 연구센터 소장
2007년 대한전자공학회 수석부회장/차기회장
<주관심분야 : 생체인식, 패턴인식, 컴퓨터 비젼, 영상인식>