논문 2010-47SP-1-10

보조정보에 기반한 가변 얼굴템플릿의 이진화 방법의 연구

(A Study on A Biometric Bits Extraction Method of A Cancelable face Template based on A Helper Data)

이 형 구*, 김 재 희*

(Hyunggu Lee and Jaihie Kim)

요 약

가변생체인식 방법 (Cancelable Biometrics)은 생체정보의 도난이나 도용으로부터 강인하며 재생성 가능한 생체템플릿을 제공하는 높은 보안성을 갖는 생체 인식방법이다. 본 논문은 가변얼굴인식 방법의 하나로써 얼굴생체템플릿을 나머지에 기반하여 이진화하는 방법을 제안한다. 이진화를 위한 입력 값으로, 우리의 기존 연구 결과로서의 가변얼굴템플릿을 이용하였다. 이 가변얼굴템플릿은 상이한 두 개의 형상 기반의 얼굴특징추출 방법 (Appearance based face recognition)을 이용하여 두 개의 얼굴특징벡터를 추출하고, 추출된 두 개의 얼굴특징벡터를 재배열 후 합하여 얻어진다. 우리의 기존방법으로 얻어진 얼굴특징벡터는 실수 값을 갖기 때문에 저장 시 기존의 암호화 방법과의 접목이 힘들며 원래의 생체정보 노출에 대한 잠정적인 위협이 될 수 있다. 본 논문의 나머지에 기반한 이진화 방법은 우리의 기존 가변얼굴템플릿에서 부분정보인 나머지를 이용하여 이진비트열을 생성하므로 향상된 보안성을 제공한다. 또한 본 논문의 이진화 기법은 합해진 특징벡터의 통계적인 특징으로부터 정의된 보조정보 (Helper data)를 이용하여 높은 인식 성능을 갖는다. 제안방법은 보조정보가 노출된 경우에서도 이진화된 가변얼굴템플릿이 원 얼굴특징벡터보다 향상된 인식성능을 보장한다. 제안하는 방법은 the extended YALEB face database를 이용하여 성능과 보안성에 대하여 평가 하였다.

Abstract

Cancelable biometrics is a robust and secure biometric recognition method using revocable biometric template in order to prevent possible compromisation of the original biometric data. In this paper, we present a new cancelable bits extraction method for the facial data. We use our previous cancelable feature template for the bits extraction. The adopted cancelable template is generated from two different original face feature vectors extracted from two different appearance-based approaches. Each element of feature vectors is re-ordered, and the scrambled features are added. With the added feature, biometric bits string is extracted using helper data based method. In this technique, helper data is generated using statistical property of the added feature vector, which can be easily replaced with straightforward revocation. Because, the helper data only utilizes partial information of the added feature, our proposed method is a more secure method than our previous one. The proposed method utilizes the helper data to reduce feature variance within the same individual and increase the distinctiveness of bit strings of different individuals for good recognition performance. For a security evaluation of our proposed method, a scenario in which the system is compromised by an adversary is also considered. In our experiments, we analyze the proposed method with respect to performance and security using the extended YALEB face database

Keywords: Cancelable biometrics, bits string extraction, appearance based face recognition, helper data.

I. 서 론

생체인식의 장점은 타고난 생체특징이 분실의 염려가 없고 타인간에 서로 다르다는 것에 있다. 또한 각 개인의 생체특징은 고유성을 가지며 이를 이용해 부인

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

※ 본 연구는 2002년도 정부(교육과학기술부)의 재원으로 한국연구재단 지정 생체인식연구센터의 지원을 받아 이루어졌습니다.(2009-0062997)

접수일자: 2009년7월6일, 수정완료일: 2009년12월28일

방지 (non-repudiation)에도 이용되고 있다. 그러나 역으로 이러한 생체정보의 특성은 심각한 보안상의 문제를 가져올 수 있다. 만일 유일한 생체정보가 도난 당하였을 경우 이러한 생체정보를 대신할 수 있는 대체생체정보를 생성하는 것은 사실상 불가능하다. 따라서 생체정보를 그대로 운용할 경우 복구 불가능한 개인정보의 손실을 초래할 수 있다. 이와 같은 문제를 해결하기 위해 제안된 방법이 변환된 생체정보를 통해 개인인증을 하는 가변생체인식 (Cancelable Biometrics) 방법이다. 가변생체인식은 원 생체정보와 다른 변환된 생체정보를 생성하여 이를 생체인식에 이용하는 방법이다. 인식성능에 있어서 변환된 생체정보는 원 생체정보와 비교하여 성능의 저하가 적어야 하며, 보안성에 있어서 변환방법이 알려지더라도 변환된 생체정보로부터 원 생체정보의 복원이 어려워야 한다. 본 논문에서는 이러한 가변 생체인식의 한 방법으로써 생체정보의 이진화 방법을 제안한다. 생체정보는 본질적으로 취득환경, 개인의 움직임 및 생체의 변화 등에 의해 그 값이 일정하지 않은 특성을 갖고 있다. 생체정보 이진화 방법은 변화를 포함하고 있는 취득된 생체정보로부터 변화하지 않는 일관성 있는 이진화된 생체템플릿을 생성하는 과정이다. 제안하는 방법은 생체정보의 통계적 특성으로부터 보조정보를 추출하고 이를 이용하여 생체정보를 이진화 하였다. 이러한 가변생체인식 방법으로써의 생체정보 이진화 방법이 가져야 할 특성을 다음과 같이 정리하였다.

i) 변환된 생체정보는 보다 향상된 인식성능을 가져야 한다. ii) 변환된 생체정보는 원 생체정보와 다르며 다수의 변환방법을 제공하여야 한다 (변환성/재생산성). iii) 보조정보와 변환된 생체정보로부터 원 생체정보의 복원이 쉽지 않아야 한다 (불가역성). 본 논문의 제안방법은 위 조건들을 모두 만족하며 이를 실험적으로 검증하였다.

1. 기존 생체정보 이진화 방법

생체정보 이진화 방법은 크게 개인정보에 의한 방법 (user-specific quantization)과 임계값을 이용한 방법 (thresholding approaches)으로 분류하였으며, 기존 연구들을 이 기준에 따라 분석하였다.

가. 개인정보에 의한 이진화 방법

Linnartz와 Tuyls[1]는 보조정보 (helper data)를 이용한 생체정보의 이진화 방법을 제안하였는데 이 방법은 양자화 색인 변조 (Quantization Index Modulation (QIM))[2]라는 방식에 기반한 것이다. 등록단계에서 이용자는 비밀 비트정보 S와 생체정보 X 를 이용하여 보조정보 W 를 계산한다. 비밀 비트정보인 S의 값이 '0' 또는 '1' 인지의 여부에 따라 보조정보 W 는 달리 계산되며 그 값은 생체정보 X와 보조정보 W의 합이 할당된 '0' 또는 '1'의 비트를 생성하도록 조정된다. W의 값은 다음과 같이 정의된다:

$$W=\begin{cases}(2n+\frac{1}{2})q-X & \text{if } S=1\\ (2n-\frac{1}{2})q-X & \text{if } S=0\end{cases} \quad (1)$$

여기서 n 은 $-q<W<q$을 만족시키는 자연수이며 양자화 단위 q 는 각 개인의 생체정보 X 로부터 얻어진 표준편차로 계산된다. 인증 시에는 입력된 생체정보 Y와 보조정보 W 를 이용해 추정된 비밀 비트정보 S' 를 계산한다. 이 방법은 보조정보 W의 도난시 비밀 비트정보인 S의 값을 바꾸어 보조정보 W 를 다시 생성함으로써, 이를 이용해 쉽게 이진 생체 템플릿을 재생성 할 수 있는 방법이다. 그러나 저자들은 이 방법을 실제 생체 데이터에 적용한 구체적인 실험 결과를 제시하지 못했다.

Vielhauer et al.[3]은 서명인식방법을 통한 생체정보 이진화 방법을 제안하였다. 각 개인의 입력된 서명 특징 성분들에 대하여 각 특징의 값이 분포할 수 있는 범위를 하한과 상한으로 제한하여 이진화 시키는 방법이다. 그들은 50개의 특징성분들을 이용하였고 11명의 사용자들에 대해 인식률 기준으로 0%의 FAR과 7.05%의 FRR을 갖는 성능을 보여주었다. Qi Han et. al은 유사한 방법으로 각 개인마다 비균등한 이진화 영역을 정의하여 생체정보를 이진화하는 방법을 제안하였고 양자화 단위를 개인의 표준편차를 근거로 결정하였다[4]. 또한 Chen et. al은 가능도 비 (likelihood ratio)에 근거한 생체정보 이진화 방법을 제안하였다[5]. 이것은 각 개인에 대하여 가능도 비가 일정 값보다 큰 구간을 이진화 구간으로 지정하여 생체정보의 분포정보를 근거로 이진화 시키는 방법이다. 그러나 위 방법들은 각 개인마다 생체특징을 이진화하기 위한 영역이 고정되어 있기 때문에 이진화를 위해 생성된 정보가 노출되었을 때 이 정보를 변경 및 재생산을 하지 못하는 단점이 있다.

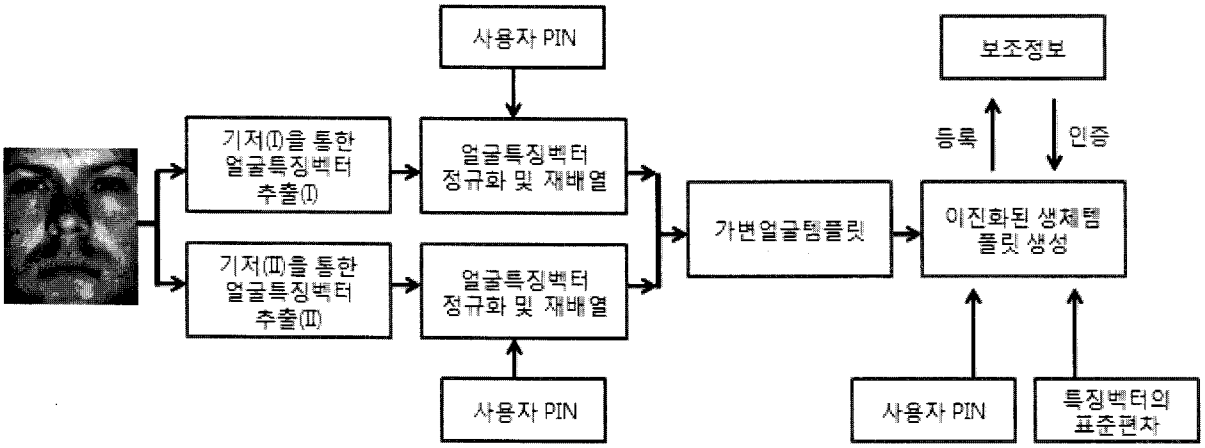


그림 1. 제안방법의 전체과정
Fig. 1. Overall block diagram of proposed method.

나. 임계값을 이용한 이진화 방법

Teoh et al.[6]은 BioHash로 명명된 변환생체인식 기술로서 생체정보 이진화 방법을 제안하였다. 이 방법은 난수발생기를 통해 생성된 난수 (pseudo-random numbers (PRN))를 이용하여 각 개인마다 투영 행렬(projection matrix)을 생성한다. 입력 생체특징을 생성된 투영 행렬에 대하여 투영 후 결과 값을 특정 값(threshold)을 기준으로 이진화 시켜 생체정보를 이진화 시킨다. 이진화 된 생체정보의 도난 시 투영행렬을 변경시켜 새로운 이진화 값을 재생성 할 수 있다. 그러나 이 방식은 투영 행렬이 도난 되었을 경우 (stolen-token scenario) 성능의 저하가 크다는 단점을 가지고 있다.

Tuyls et al.[7]은 각 개인의 생체특징들 중에서 신호대 잡음 비가 높은 특징들을 선택하여 이진화 시키는 방법을 제안하였다. 이진화 방법으로는 특징 값의 평균 값을 기준으로 이진화 하는 방법을 선택하였고 이진화 된 값은 BCH 오류정정부호를 통해 오류를 보정하였다. 그들의 방법은 두 개의 지문 데이터베이스에 대해 실험되었고 인식률 오류 기준으로 4.5%와 4.2%의 오류율을 보였다. 이 방법은 이진화를 위한 값이 특징 값들의 평균을 이용하기 때문에 이진화된 생체정보가 도난 되었을 경우 새로운 이진화된 생체 코드를 재생성하지 못하는 문제점이 있다.

기존의 생체정보 이진화 방법에 관한 연구들은 이진화 방법 자체만을 중점적으로 고려하여 상대적으로 이진화를 위한 보조정보나 부가정보가 도난 당하였을 때의 경우가 고려되지 않았다. Teoh et. al.이 보여준 바와 같이 개인의 보조정보가 도난 되었을 때 인식 성능의 큰 저하가 발생할 수 있다[6, 8]. 본 논문에서는 두 얼굴 특징벡터들을 합한 값에 대하여 보조정보를 적용해 보다 강인한 이진화된 생체정보 값을 얻는 방법에 대해서 제안한다. 또한 본 논문에서는 보조정보가 도난 되었을 경우에서도 제안방법이 원 생체정보보다 향상된 성능을 가지는 것을 보여준다. Ⅱ 장에서는 제안방법을 설명하고, Ⅲ장에서 제안방법의 성능과 보안성에 대해 확장된 YALEB 얼굴 데이터베이스 (The extended YALEB face database)를 통해 평가한다.

Ⅱ. 가변 얼굴생체정보 이진화 방법

이 장에서는 가변 얼굴생체정보의 이진화 방법에 대해 설명한다. 제안방법은 크게 두 가지 과정으로 나뉘어진다. 첫 번째 과정은 가변얼굴템플릿의 생성과정이다. 이 과정은 서로 다른 형상기반의 얼굴특징추출 방법에 의해 구해진 얼굴특징벡터들을 이용한다. 형상기반의 얼굴특징추출 방법으로는 PCA(Principal Component Analysis), ICA(Independent Component Analysis), 그리고 NMF(Nonnegative Matrix Factorization)등이 있다[9~11]. 구해진 두 특징벡터는 우선 정규화 (Normalization)되고 두 특징벡터의 요소를 재배열하고 합하여 가변얼굴템플릿이 만들어진다. 이 과정은 기존 연구방법에 의해 구해졌다[12~13]. 두 번째 과정은 생성된 가변얼굴템플릿을 제안하는 보조정보에 기반하여 이진화 시키는 과정이다. 이전 과정에서 생성된 가변얼굴템플릿이 서로 다른 두 특징벡터의 합으로 구해졌기 때문에 특징벡터들 각각의 통계적 특성을 고

려해 이진화 방법을 변형 후 적용한다. 생성된 얼굴생체템플릿의 도난이 발생할 경우 이를 대체할 새로운 얼굴템플릿을 재생성하며, 이를 위해 첫 번째 과정에서 특징벡터 요소의 재배열 방법을 바꾸거나 두 번째 과정에서 이진화를 위한 보조정보를 바꾸는 방법이 가능하다. 그림 1은 제안하는 방법의 전체과정을 보여준다.

1. 얼굴특징벡터 추출

서로 다른 얼굴특징 벡터 (c_I, c_{II})는 서로 다른 기저(Basis)를 통해 아래와 같은 방식으로 계산된다.

$$\begin{aligned} c_I &= B_I x \\ c_{II} &= B_{II} x \end{aligned} \tag{2}$$

이때 x 값은 입력생체정보 이며, B_I, B_{II}는 각기 다른 형상기반 얼굴특징추출 방법에 해당되는 기저 행렬이다.

2. 얼굴특징벡터 정규화 및 재배열

가변얼굴템플릿은 서로 다른 얼굴특징벡터들의 합으로 구성되며 이를 위해 다음의 정규화 과정을 거친다.

$$\begin{aligned} \hat{c_I} &= c_I/|c_I| \\ \hat{c_{II}} &= c_{II}/|c_{II}| \end{aligned} \tag{3}$$

정규화된 $\hat{c_I}, \hat{c_{II}}$은 구성요소의 재배열을 거치며 그 과정은 다음과 같다.

$$\begin{aligned} \tilde{c_I} &= S_I(\hat{c_I}) \\ \tilde{c_{II}} &= S_{II}(\hat{c_{II}}) \end{aligned} \tag{4}$$

이때 구성요소의 재배열을 위한 규칙 S_I, S_{II}는 각 개인의 PIN을 기준으로 생성된다.

3. 가변얼굴템플릿 생성

얼굴생체정보의 이진화를 위한 입력으로써 가변얼굴템플릿이 이용된다. 가변얼굴템플릿은 정규화되고 재배열된 얼굴특징벡터들의 합이며 계산과정은 다음과 같다.

$$t = \tilde{c_I} + \tilde{c_{II}} \tag{5}$$

4. 보조정보의 생성과 이진화 과정

생성된 가변얼굴템플릿 t가 이진화 되며, 벡터 t의 각 요소별로 보조정보를 생성하며 이진화에 이용한다. 이진화 과정은 수식 (1)의 과정을 이용한다.

$$W = \begin{cases} (2n + \frac{1}{2})q - t & \text{if } S = 1 \\ (2n - \frac{1}{2})q - t & \text{if } S = 0 \end{cases}$$

여기서 n 은 $-q < W < q$을 만족시키는 자연수이며 t가 $\tilde{c_I}, \tilde{c_{II}}$의 합이므로 $\tilde{c_I}, \tilde{c_{II}}$의 통계적 특성인 표준편차 값들을 근거로 양자화 단위 q가 결정된다. 양자화 단위 q의 결정은 다음의 수식에 따른다.

$$q = \sqrt{(q_I)^2 + (q_{II})^2} \tag{6}$$

여기서 q 는 $t = \tilde{c_I} + \tilde{c_{II}}$의 양자화 단위이며 q_I, q_{II}은 각각 $\tilde{c_I}, \tilde{c_{II}}$의 양자화 단위이다. q_I은 $\tilde{c_I}$의 표준편차로 계산되며 q_{II}은 $\tilde{c_{II}}$의 표준편차로 계산된다. 양자화 단위 q 역시 t의 표준편차를 기준으로 결정할 수 있으며 수식 (6)의 형태를 가진다. 이것은 서로 독립인 $\tilde{c_I}, \tilde{c_{II}}$의 합으로 구성된 t의 표준편차를 $\tilde{c_I}, \tilde{c_{II}}$의 표준편차들로 표현한 것이다.

*제안방법의 비가역성

(Non-invertibility of the proposed method)

변환생체인식 방법은 변환된 생체정보나 변환방법을 알더라도 원래의 생체정보의 복원이 쉽지 않아야 한다. 이러한 변환생체정보의 비가역성을 위한 것 중 하나가 가변템플릿의 사용이다. 가변템플릿 t는 서로 다른 두 계수벡터 $\tilde{c_I}, \tilde{c_{II}}$의 합이므로 t로부터 $\tilde{c_I}, \tilde{c_{II}}$를 구하는 것이 불가능하다[13~14]. 뿐만 아니라 실수 값을 갖는 가변템플릿 t를 이진화 하는 과정에서 t의 나머지 정보만을 이용하기 때문에 보조정보 W로부터 t를 추정하는 것이 불가능 하다. 이것은 수식 (1)에서 W생성 시 원래 생체정보 중 정수부분에 해당하는 n은 저장되지 않기 때문이다. t의 정수분을 제외한 나머지 정보를 추정하는 것 역시 쉽지 않은데, 이것은 t의 각 요소에 대해서 어떠한 비밀비트정보 S값이 할당 되었는지 저장하지 않기 때문이다. 따라서 개인의 PIN과 보조정보를 알더라도, 개인의 비밀 비트열 정보를 알 수 없으며 원 생체정보의 추출 역시 쉽지 않다.

*제안방법의 재생산성

(Revocability of the proposed method)

변환생체인식 방법에서는 저장된 변환생체템플릿이 노출되더라도 새로운 변환생체템플릿을 다시 생성할 수 있어야 한다. 재생산성을 위한 장치는 크게 두 가지로 나뉘어 진다. 첫 번째는 PIN을 변경함으로써 가변얼굴템플릿을 생성하기 위한 재배열의 조합을 바꾸는 것이다. t의 차원이 N일 경우 총 $N!$의 조합이 재생산 가능하다. 만일 100차원의 얼굴특징벡터를 이용하여 가변얼굴템플릿을 만들 경우 $N! = 100! \cong 10^{158}$개의 서로 다른 조합의 변환생체템플릿을 생성할 수 있다. 생체정보의 이진화 방법 역시 임의의 비밀비트 값을 각 차원에 할당 가능하므로 100차원의 t에 대하여 $2^N = 2^{100} \cong 10^{30}$개의 조합이 가능하다. 따라서 제안방법의 재생산성은 100차원의 얼굴특징벡터를 이용할 경우 $N!2^N = 100!2^{100} \cong 10^{188}$개의 새로운 가변템플릿을 생성할 수 있다.

Ⅲ. 실 험

1. 실험 방법 및 평가 지표

제안된 가변얼굴템플릿의 이진화 방법을 검증하기 위해 확장된 YALEB 얼굴 데이터베이스가 이용되었다[15]. 이것은 YALEB 얼굴 데이터베이스[16]가 확장된 것으로 38명의 사람에 대하여 각각 조명변화와 자세변화를 포함하여 64장의 얼굴영상이 취득된 것이다. 기존의 YALEB 얼굴 데이터베이스가 10명의 정보만을 포함하고 있는 것을 감안하면 확장된 YALEB 얼굴 데이터베이스를 이용함으로써 더욱 신뢰성 높은 인식성능의 평가가 가능하다.

등록 시 제안된 이진화 방법을 위하여 보조정보의 생성이 필요하다. 이를 위해 각 사람의 64장의 얼굴영상에서 무작위로 15장의 영상을 취하여 얻은 특징벡터계수들로부터 표준편차를 구하고, 이것을 모든 사람에 대해 평균하여 이진화 과정의 양자화 단위로 이용하였다. 평가 시 각각의 사람으로부터 무작위로 10개의 얼굴영상을 선택하였다. 전체 사람의 수가 38명이므로 평가에 사용된 얼굴영상은 380장이다. 형상기반 얼굴특징 추출기법으로는 PCA, ICA, 그리고 NMF를 이용하였다. 가변얼굴 템플릿의 생성은 PCA와 ICA 벡터의 합과, PCA와 NMF 벡터의 합의 두 가지 조합을 고려하였다. 가변얼굴 템플릿을 제안하는 생체정보 이진화 방법으로 이진비트열로 변환하고 생성된 이진비트열에 대하여 성능을 평가하였다. 성능평가의 지표로 이용된 것은 인식성능으로써의 Equal Error Rate (EER), 개인정보가 노출되었을 경우에서의 인식성능, 그리고 가변생체템플릿으로써의 재생산성 (Revocability) 이다.

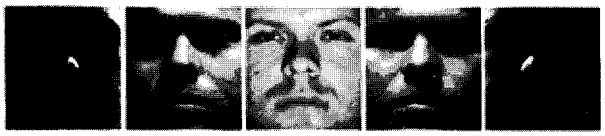


그림 2. 사용되어진 확장된 YALEB 얼굴 데이터베이스의 예시

Fig. 2. Examples of the illumination variation in images obtained from the extended YALEB face database.

2. 인식성능 평가 (Performance evaluation)

제안된 방법으로 변환얼굴템플릿으로부터 이진비트열을 생성하고, 생성된 각 개인의 이진비트열에 대한 인식성능을 입력 얼굴특징 벡터들 (PCA, ICA, NMF 계수벡터)의 인식성능과 비교하였다.

변환얼굴템플릿 생성 시 사용자마다 서로 다른 PIN 값을 사용하고 그에 따라 얼굴특징벡터들을 재배열 하였다. 또한 이진비트열 생성 시 비밀비트정보와 그에 따른 보조정보를 각 개인마다 서로 다르게 지정하였다. 표 1.에서 보여지는 바와 같이 해당 얼굴 데이터 (the extended YALEB face database)에서 추출된 입력특징벡터 (PCA, ICA, NMF 계수벡터)들의 인식 성능은 좋지 않다. 그러나 제안된 이진화 방법으로 생성된 이진비트열의 성능은 상대적으로 탁월한 성능을 보인다. 이러한 결과는 각 사용자마다 서로 다른 PIN을 할당하고 이진화에 이용되는 보조정보도 서로 다르게 지정하였기 때문에 가능하다. 따라서 이러한 PIN정보나 보조정보가 노출되었을 경우에 대한 고려 역시 필요하며 다음의 단락에서 상세히 다루었다.

표 1. 제안된 이진화 방법의 인식 성능

Table 1. Performance of the proposed method for the extended YALEB database.

	입력특징벡터			제안 이진화 방법	
	PCA	ICA	NMF	PCA+ICA	PCA+NMF
EER(%)	49.1	47	38.3	0.75	0.06

3. 개인정보가 도난 되었을 경우의 인식 성능 (peformance under the stolen-token scenario)

변환생체인식에서 일반적으로 개인정보가 노출되었을 경우 변환생체템플릿의 인식성능이 크게 저하된다. 이러한 인식성능의 저하는 개인마다 다르게 선택된 개인정보가 공격자에게 노출되어 각 개인의 변환생체템플릿에 대한 공격에 이용되기 때문이다. 본 논문에서 이용되는 개인정보는 PIN정보와 이진화를 위한 보조정보가 있다. 이 두 가지 정보 모두가 노출되었을 경우의 변환얼굴템플릿으로써의 이진비트열이 갖는 인식성능을 다음의 표 2.에서 다루었다.

표 2.에서 확인할 수 있듯이 개인정보가 노출된 경우 제안 이진화 방법으로 생성된 이진비트열은 개인정보가 유지된 표 1.의 경우보다 좋지 못한 성능을 가진다. 그러나 입력특징벡터를 기준으로 보았을 때 제안 이진화 방법은 인식성능상의 이점을 가진다. 제안된 방법은 개인정보가 노출된 경우에서도 30.6%와 33.1%의 EER을 각각 PCA+ICA 조합과 PCA+NMF 조합에서 보여준다. 입력특징벡터 중 가장 좋은 인식성능을 가지는 NMF벡터가 38.3%의 EER을 가지는 것을 고려할 때, 제안방법의 각 경우에서 7.7%와 5.2%의 EER 인식성능이 향상되었다.

표 2. 개인정보가 노출된 상황에서의 제안된 이진화 방법의 인식 성능

Table 2. Performance of the proposed method for the extended YALEB database under stolen-token scenario.

	입력특징벡터			제안 이진화 방법	
	PCA	ICA	NMF	PCA+ICA	PCA+NMF
EER(%)	49.1	47	38.3	30.6	33.1

4. 변환성 평가 (Revocability evaluation)

제안된 변환얼굴템플릿의 이진화 방법은 재생산 가능한 이진비트열을 생성한다. 이진비트열이 도난 당하였을 경우 새롭게 생성된 이진비트열은 도난 된 이진비트열과 정합되어선 안 된다. 이를 평가하기 위해 동일인에 대하여 서로 다른 여러 개의 PIN과 보조정보를 할당하고 평가입력들로부터 서로 다르게 변환된 이진비트열이 생성되는지 확인하였다. 이 경우 동일인으로부터 생성된 비트열들로부터 만들어진 분포를 pseudo genuine distribution이라 한다. 일반적으로 생체인식에서 이용되는 분포들로는 genuine distribution과 imposter distribution이 있다. 본 논문에서의 genuine distribution은 동일인으로부터 동일한 PIN과 보조정보를 이용하여 얻어진 비트열으로부터 만들어진 분포이며 imposter distribution은 서로 다른 PIN과 보조정보가 할당된 타인간의 비트열을 비교하여 만들어진 분포이다. 높은 변환성을 갖는 변환생체특징의 경우 pseudo genuine distributoin이 imposter distribution과 유사하며 동시에 genuine distribution과 차이를 보여야 한다. 이러한 특성을 이용하여 생성된 이진비트열의 변환성을 평가하기 위하여 pseudo genuine distribution과 imposter distribution사이의 Receiver Operating Characteristic (ROC) curve를 고려하였다. 이상적인 변환성을 갖는 경우 pseudo genuine distribution과

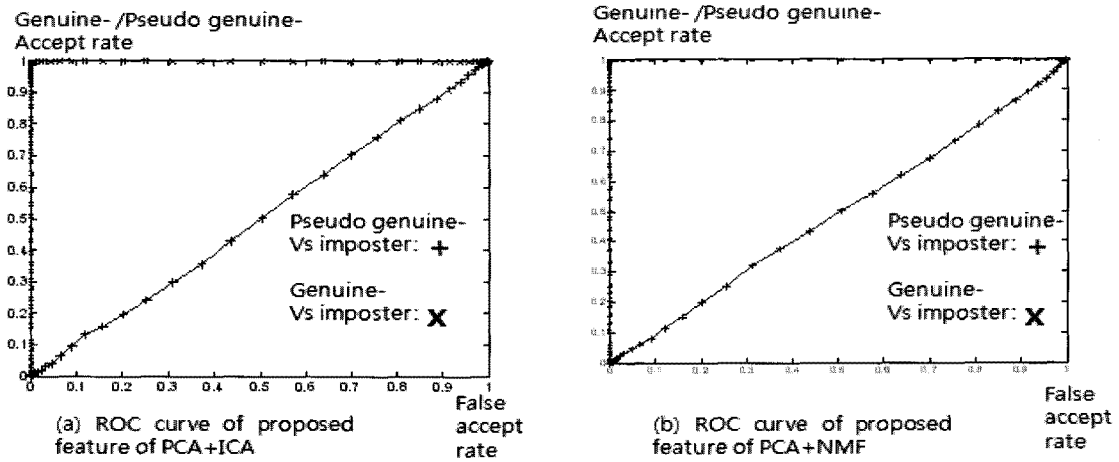


그림 3. 제안된 방법의 ROC curve를 통한 변환성 측정결과

Fig. 3. ROC curve between pseudo genuine Vs imposter distributions for the proposed method.

imposter distribution 사이에서 얻어진 ROC curve는 단조증가 형태의 대각성분으로 나타나게 된다. 이것은 pseudo genuine distribution과 imposter distribution이 비슷하여 pseudo genuine의 True Accept Rate (TAR)와 imposter의 False Accept Rate (FAR)가 유사해지기 때문이다. 제안방법의 변환성은 이상적인 형태를 가지며 그림 3.의 ROC curve로 확인할 수 있다.

Ⅳ. 결 론

본 논문은 얼굴인식에서 얼굴정보의 도난 시 개인의 얼굴생체정보를 보호하면서 동시에 높은 생체인식 성능을 보장하기 위한 것으로, 변환얼굴템플릿의 이진화 방법에 대해 제안하였다. 이를 위해 변환얼굴템플릿의 통계적 특성을 고려하여 이진화를 위한 보조정보를 생성한다. 이진화된 비트열은 동일인에 대하여 일관성이 있으며 타인간의 구분력을 더 높이도록 생성되었다. 제안된 방법은 기본적인 변환얼굴템플릿의 변환성에 더하여 이진화방법의 가변성으로 인해 다수의 변환 가능한 비트열을 생성할 수 있다. 따라서 생성된 비트열이 노출된 경우 쉽게 다른 비트열로 대체가 가능하다. 본 논문은 개인정보인 PIN과 이진화를 위한 보조정보가 노출된 경우에 대해서도 고려하였다. 일반적인 변환생체인식 방법들에서 이러한 개인정보 노출의 경우 공격자가 해당 생체정보에 유사한 값을 추측 함으로써 심각한 성능저하가 발생한다. Kong et al.[17]이 보였듯이 BioHash에서도 투영 행렬이 도난 되었을 경우 (stolen-token scenario) 원 생체보다 안좋은 인식성능을 보인다. 제안방법 역시 개인정보가 노출된 경우의 성능은 개인정보가 노출되지 않았을 경우 보다 좋지 않다. 그러나 개인정보가 노출된 경우에서도 원래의 얼굴생체정보의 복원이 쉽지 않으며, 이진화를 통해 생성된 비트열은 개인정보가 노출된 경우에서도 원 얼굴생체특징정보와 비교하여 향상된 인식성능을 보여준다. 추가적인 연구내용으로써, 본 논문의 생체정보 이진화 방법은 2차원으로 확장되어 위상영역 (phase domain)에서 비트열을 생성하는 방법도 연구되었으며 해당 연구내용은 국제저널지에 제출된 상태이다[18]. 이와 같은 생체정보 이진화 방법을 이용함으로써, 연속적인 실수 값을 갖는 얼굴생체정보를 이진화하여 생체정보의 보안성을 향상시키며 동시에 기존의 암호화 시스템과의 연계가 가능하다. 따라서 인터넷 뱅킹이나 전자상거래 등에 있어서 제안 방법을 통하여 생체인식에 기반한 보다 안전한 개인인증이 가능할 것으로 기대된다.

참 고 문 헌

[1] Jean-paul Linnartz and Pim Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," AVBPA, pp. 393-402, 2003.

[2] Brian Chen and Gregory W. Wornell, " Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," IEEE Trans. on Information Theory, vol. 47, no. 4, pp. 1423-1443, 2001.

[3] C. Vielhauer and R. Steinmetz, "Handwriting: feature correlation analysis for biometric hashes," EURASIP Journal on Applied Signal Processing, vol. 2004, no. 4, pp. 542 - 558, special issue on Biometric Signal Processing, 2004.

[4] Qi Han, Zhifang Wang, and Xiamu Niu, "A Non-uniform Quantizing Approach to Protect Biometric Templates," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP '06., pp. 693-698, 2006.

[5] Chen C., Veldhuis R.N.J., Kevenaar T.A.M., and Akkermans A.H.M., "Multi-Bits Biometric String Generation based on the Likelihood Ratio," First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007., 2007.

[6] Andrew Teoh, David Ngo and Alwyn Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data And Tokenised Random Number," Pattern Recognition, Vol. 37, Issue 11, pp. 2245-2255, 2004.

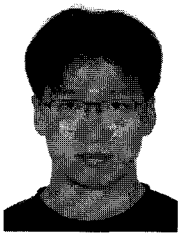
[7] Pim Tuyls, Anton H. M. Akkermans, Tom A. M. Kevenaar, Geert Jan Schrijen, Asker M. Bazen, and Raymond N. J. Veldhuis, "Practical Biometric Authentication with Template Protection," International conference on: Audio- and Video-Based Biometric Person Authentication. AVBPA, Vol. 3546, pp. 436-446, 2005.

[8] Andrew B. J. Teoh, Yip Wai Kuan, and Sangyoun Lee, "Cancellable biometrics and annotations on BioHash," Pattern Recognition, Vol. 41 , Issue 6, pp. 2034-2044, 2008.

[9] M.A. Turk and A.P. Pentland, "Eigenfaces for

Recognition," Cognitive Neuroscience, Vol. 3, No. 1, pp. 71-86, 1991.
[10] 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.
[11] D. D. Lee and H. S. Seung, "Learning the parts of objects by non-negative matrix factorization," Nature, vol. 401, pp. 788-791, 1999.
[12] 이철한, 정민이, 김종선, 최정윤, 김재희, "통계적 형상 기반의 얼굴인식을 위한 가변얼굴템플릿 생성방법," 대한전자공학회 논문지 제 44권 SP편 제 2호, pp. 27-36, 2007.
[13] M.Y. Jeong, C.H. Lee, J.S. Kim, J.Y. Choi, K.A. Toh, and J.H. Kim, "Changeable biometrics for appearance based face recognition," The Biometric Consortium Conference, pp. 1-5, 2006.
[14] Hyunggu Lee, Chulhan Lee, Jeung-yoon Choi, Jongsun Kim, and Jaihie Kim, "Changeable Face Representations Suitable for Human Recognition," International Conference on Biometrics, Vol. 4642, No. 1, pp. 557-565, 2007.
[15] K.C. Lee, J. Ho and D. Kriegman, "Acquiring Linear Subspaces for Face Recognition under Variable Lighting," IEEE Trans. Pattern Anal. Mach. Intelligence, Vol. 27, No. 5, pp. 684-698, 2005.
[16] Georghiades A.S., Belhumeur P.N., and Kriegman D.J., "From Few to Many: Illumination Cone Models for Face Recognition under Variable Lighting and Pose," IEEE Trans. Pattern Anal. Mach. Intelligence, vol. 23, no. 6, pp. 643-660, 2001, http://vision.ucsd.edu/~leekc/ExtYaleDatabase/ExtYaleB.html
[17] Kong et al., 2006 B. Kong, K. Cheung, D. Zhang, M. Kamel and J. You, "An analysis of BioHashing and its variants," Pattern Recognition vol. 39, no. 7, 2006, pp. 1359 - 1368.
[18] Hyunggu Lee, Andrew Beng Jin Teoh, and Jaihie Kim, "Biometric Bits Extraction through Phase Quantization based on Feature level fusion", submitted to the Special Issue on Biometric Systems and Applications in the Journal of Telecommunication Systems

저 자 소 개



이 형 구(정회원)
2003년 연세대학교 전기전자 공학과 학사 졸업.
2005년 연세대학교 전기전자 공학과 석사 졸업.
2009년 연세대학교 전기전자 공학과 박사 과정.
<주관심분야 : 생체인식, 컴퓨터 비젼, 패턴인식>

김 재 희(정회원)-교신저자
1979년 연세대학교 전자공학과 졸업.
1982년 Case Western Reserve University 전기공학 석사
1984년 Case Western Reserve University 전기공학 박사
2009년 연세대학교 전기전자공학부 교수
2009년 과학기술부 지정 생체인식 연구센터 소장
2009년 한국바이오인식포럼(KBA) 의장
<주관심분야 : 생체인식, 패턴인식, 컴퓨터 비젼, 영상인식>