情報保護學會論文誌
第15卷 第4號, 2005. 8

다중 생체인식 시스템에 적합한 워터마킹 알고리즘*

문 대 성,[1†] 정 승 환,[2] 김 태 해,[2] 정 용 화,[2‡] 문 기 영[1]
[1]한국전자통신연구원, [2]고려대학교

An Watermarking Algorithm for Multimodal Biometric Systems*

DaeSung Moon,[1†] SeungHwan Jung,[2] TaeHae Kim,[2]
Yongwha Chung,[2‡] KiYoung Moon[1]
[1]ETRI, [2]Korea University

요 약

본 논문에서는 원격 생체인식 시스템에서 생체데이터의 안전한 전송을 위한 워터마킹 기법을 제안하며, 워터마크의 삽입으로 인한 인식 성능의 상관관계를 비교한다. 특히, 원격 생체인식 시스템은 사용자의 얼굴과 지문 정보를 동시에 사용하는 다중 생체인식 시스템으로 가정한다. 다중 생체인식 시스템에 워터마킹 기법을 적용하기 위하여 우선 두 가지 가능한 시나리오를 고려한다. 첫 번째 시나리오는 얼굴의 특징 정보를 지문 영상에 워터마크로 삽입하며, 반대로 두 번째 시나리오는 지문의 특징 정보를 얼굴 영상에 삽입한다. 실험에 의해 얼굴 영상에 지문 특징정보를 워터마크로 삽입하는 것이 얼굴 및 지문인식 성능의 저하가 거의 발생하지 않음을 확인하였다.

ABSTRACT

In this paper, we describe biometric watermarking techniques for secure user verification on the remote, multimodal biometric system employing both fingerprint and face information, and compare their effects on verification accuracy quantitatively. To hide biometric data with watermarking techniques, we first consider possible two scenarios. In the scenario 1, we use a fingerprint image as a cover work and hide facial features into it. On the contrary, we hide fingerprint features into a facial image in the Scenario 2. Based on the experimental results, we confirm that the Scenario 2 is superior to the Scenario 1 in terms of the verification accuracy of the watermarking image.

Keywords : *Watermarking, Multimodal, Fingerprint, Facial, Verification*

Ⅰ. 서 론

정보시스템에 접근하기 위한 사용자 인증 수단으로 패스워드, PIN(Personal Identification Number) 또는 스마트카드 등의 전통적인 방법들이 널리 이용하고 있으나, 이러한 인증수단은 분실, 도난, 망각으로 인한 위험이 존재한다. 이러한 위험을 해결하기 위하여 개인의 고유한 생체정보를 이용하는 생체인식에 관한 연구가 활발히 진행되고 있다.[1]

일반적으로 생체인식 시스템은 두 가지 모드로 분류 할 수 있다. 즉, 하나의 생체정보를 이용하는 **단일 생체인식 시스템**과 두 가지 이상의 생체정보를 동시에 이용하여 사용자를 인증하는 **다중 생체인식 시스템**으로 구분 할 수 있는데, 다중 생체인식 시스템은 대용량 응용에서 단일 생체인식 시스템의 성능 한계를 극복하기 위한 중요한 연구동향으로 부각되

접수일 : 2005년 7월 27일 ; 채택일 : 2005년 8월 11일
† 주저자, daesung@etri.re.kr
‡ 교신저자, ychungy@korea.ac.kr

고 있다. 본 논문에서는 생체 인식의 여러 분야 중 널리 사용되고 있는 지문과 얼굴정보를 다중 생체인식 시스템의 생체정보로 활용한다.

앞서 언급한 것처럼 생체인식 기술은 기존의 개인 인증 수단에 비해 많은 장점을 가지고 있지만, 개인의 고유한 생체정보가 악의적인 사용자에게 유출된다면 생체정보의 무결성과 기밀성에 대하여 심각한 문제가 발생한다. 예를 들어, 사용자의 아이디와 패스워드가 유출되었을 경우에는 쉽게 변경이 가능하지만, 사용자의 생체정보는 유한(하나의 얼굴, 열개의 지문)하기 때문에 유출되었을 경우에 변경이 불가능하거나 극히 제한적이다.

원격응용에서 네트워크를 통해 생체정보를 전송할 때, 생체정보를 보호하기 위한 방법으로 암호 기술이나 디지털 워터마킹과 같은 몇몇 방법들이 사용가능하다. 생체정보의 무결성과 기밀성을 보장하기 위하여 일반적인 암호 기술[2]을 사용하는 경우, 클라이언트에서 획득된 생체정보는 서버로 전송되기 전에 암호화 되며, 서버에서는 전송된 생체정보를 복호화한 후, 인증 과정을 실행한다. 암호화된 생체정보는 공유된 키를 소유해야 복호화가 가능하므로 기밀성과 무결성을 보장하지만, 암호화된 생체정보가 한번 복호화 된 후에는 생체정보의 보호가 불가능하다.

디지털 워터마킹은 이러한 암호 기술의 문제점을 보완 또는 암호기술과 혼용할 수 있는 방법으로써, 삽입되어지는 정보를 **워터마크**라 하며, 워터마크가 삽입되는 원 영상 또는 컨텐츠를 **원본 영상**이라고 한다. 디지털 워터마킹은 추출과정 후에도 원본 영상에 삽입된 워터마크가 제거되지 않으며, 암호화, 압축, 파일형식 변환 등의 다양한 공격에도 강인하도록 설계될 수 있다. 이처럼 워터마킹 기술은 한번 삽입된 워터마크는 외부 공격이 가해지더라도 원본 영상에 존재하기 때문에 원본 영상의 무결성을 보장해 준다. 또한, 생체 특징을 워터마크로 사용할 경우에 기밀성 보장이 가능하다. 더욱이, 워터마크가 삽입된 생체정보를 암호화함으로써 더욱 향상된 생체정보 보호를 가능하게 할 수 있다. [3]에서와 같이, 본 논문에서는 디지털 워터마킹 기술을 이용하여 생체정보를 보호하는 방법을 제안한다.

일반적으로 불법복제 방지와 저작권 보호를 위해 사용되어지는 디지털 워터마킹 기술은 원본 영상에 워터마크를 삽입하게 되며, 이러한 삽입과정으로 인하여 원본 영상의 품질이 떨어지게 된다. 일반적인 워터마킹 기술에서는 이러한 품질의 저하를 멀티미디어 서비스 사용자가 인지하지 못할 수준으로 제공하면 충분하지만, 생체 워터마킹 기술은 이러한 생체정보의 품질 저하로 인하여 생체인식 성능에 영향을 주게 되므로, 생체 워터마킹과 인식 성능과의 관계를 충분히 고려한 후에 워터마킹 알고리즘을 설계하여야 한다.

본 논문에서는 두 가지 가능한 시나리오를 제안하고, 각 생체 워터마킹 시나리오에서 워터마크의 삽입으로 인한 생체인식 성능과의 관계를 분석한다. 첫 번째 시나리오에서, 지문영상을 원본 영상으로 사용하며 얼굴 특징정보를 워터마크로 사용하여 지문영상에 삽입한다. 반대로, 두 번째 시나리오에서는 얼굴영상을 원본 영상으로 사용하며 지문 특징정보를 얼굴영상에 삽입한다.

본 논문의 구성은, 2장에서 다중 생체인식 시스템에 대하여 설명하며, 생체 워터마킹에 관한 관련 연구를 기술한다. 3장에서는 다중 생체인식 시스템에 적용 가능한 두 가지 워터마킹 시나리오에 관하여 설명하고, 실험결과를 4장에서 기술한다. 마지막으로, 결론을 5장에서 맺는다.

Ⅱ. 연구 배경

2.1 생체 워터마킹

Yeung과 Pankanti[4]는 원본 영상으로 사용한 지문영상에 약한(fragile) 워터마킹 기법을 적용하여 지문영상의 무결성을 보장하였다. 워터마크 정보가 삽입 되는 위치는 삽입/검출 모듈사이에 서로 공유한 키를 통해 결정된다. 또한, Uludag과 Tekalp[5]는 강인한(robust) 워터마킹 기법을 사용하여 워터마크가 삽입된 지문영상에 강한 왜곡이 발생하여도 삽입된 워터마크 정보를 검출할 수 있다. 이처럼, 생체정보에 워터마킹 기술을 적용한 연구들은 지문영상의 무결성을 보장하기 위해 지문영상을 원본 영상으로 사용하거나 지문 특징정보의 기밀성을 보장하기 위해 지문 특징정보를 워터마크로 사용하여 연관성 없는 원본 영상에 삽입하였다.

전통적인 워터마킹 알고리즘을 설계할 때 다양한 공격에 대한 강인성, 워터마크를 삽입할 위치의 선택 등 여러 가지를 고려해야 한다. 추가적으로, 생체인식 시스템에서 생체정보를 보호하기 위하여 워터마킹 기술을 적용할 때는 생체인식 시스템의 인식

성능 변화에 관한 고려가 필요하다. 예를 들어, 지문영상에 워터마크를 삽입하면 정도의 차이는 있겠지만 원 지문영상의 품질에 왜곡이 발생하여 워터마크를 삽입하지 않았을 때의 성능을 보장할 수 없다. 따라서 생체인식 시스템에 워터마킹 기술을 적용할 때에는 인식 성능의 저하가 최소화되는 생체 워터마킹 알고리즘의 개발이 필요하다.

다양한 디지털 워터마킹 알고리즘들이 연구되고 여러 분야에서 적용이 되고 있지만, 워터마크 삽입 알고리즘의 일반식은 수식 1과 같다.

$$I_{WM}(x,y) = I(x,y) + k^* W, \quad (1)$$

$I(x,y)$는 원 영상의 화소 값이고, W는 삽입될 워터마크이다. $I_{WM}(x,y)$는 원 영상에 워터마크가 삽입된 결과 영상이며, k는 가중치로 k의 값에 의하여 워터마크의 삽입강도가 결정된다.

2.2 다중 생체 인식 시스템

앞서 언급한바와 같이 생체인식 시스템은 하나의 생체정보를 이용하는 단일 생체인식 시스템과 두 가지 이상의 생체정보를 동시에 이용하여 사용자를 인증하는 다중 생체인식 시스템의 두 가지 모드로 구분할 수 있다. 단일 생체인식 시스템의 인식 성능은 대용량 생체인식 서비스를 제공하기에는 한계가 있으며, 운용상의 어려움, 예를 들어 심하게 훼손된 지문을 가진 사용자에게는 지문인식 시스템이 적당하지 않은 문제점으로 인하여 다중 생체인식 시스템이 중요한 연구동향으로 부각되고 있다.[6] 본 논문에서는 다양한 생체정보 중에서 얼굴과 지문정보를 통합하여 다중 생체인식 시스템을 구현하는 경우 워터마크 삽입으로 인한 인식 성능 저하를 최소화하는 방안을 제시한다.

Ⅲ. 다중 생체인식 시스템에 적합한 워터마킹 알고리즘

본 논문에서 구현하는 지문과 얼굴정보를 통합한 다중 생체인식 시스템에 워터마킹 기술을 적용하기 위하여 두 가지 가능한 시나리오를 제안한다. 시나리오 1은 지문영상을 원본 영상으로 사용하며 워터마크로 사용된 얼굴의 특징정보를 지문영상에 삽입한다. 시나리오 2는 얼굴영상을 원본 영상으로 사용하고 지문의 특징정보를 삽입한다. 즉, 시나리오 1과 시나리오 2에서 얼굴 특징정보와 지문 특징정보는 식 (1)의 W에 해당한다.

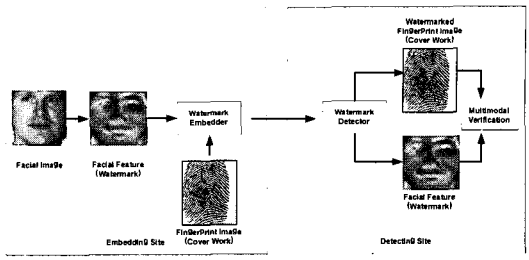


그림 1. 시나리오 1의 흐름도

3.1 지문 정보에 얼굴 특징 정보 은닉

시나리오 1은 그림 1과 같이 삽입부에서 두 가지 생체정보 즉, 얼굴과 지문영상을 각각 센서로부터 획득한 후, 워터마크로 사용될 얼굴 특징정보를 추출한다. 원본 영상으로 사용되는 지문영상의 특정 위치에 추출된 얼굴 특징정보가 삽입된 후 전송된다. 워터마크가 삽입된 지문영상을 수신한 검출부에서는 검출 알고리즘에 의하여 삽입된 얼굴 특징정보를 검출한다. 마지막으로 전송받은 지문영상과 얼굴 특징정보를 이용하여 사용자 인증과정을 수행한다. 지문과 얼굴의 두 가지 생체정보를 이용하여 사용자 인증을 수행하기 때문에 인식 성능을 향상시킬 수 있다.

시나리오 1에서 얼굴을 이용한 생체인식은 얼굴 특징정보가 워터마크로 사용되기 때문에 워터마킹 알고리즘의 강인성이 보장된다면 얼굴인식 성능에는 변화가 없다. 하지만 워터마크의 삽입으로 인한 지문영상의 왜곡이 발생하여 지문인식 성능에 영향을 줄 수 있다. 워터마크의 삽입 시 지문인식 성능의 저하를 최소화하기 위해 Jain과 Uludag[3]이 제안한 삽입 알고리즘을 사용한다. [3]의 알고리즘은 워터마크가 삽입될 위치를 결정할 때 지문인식 성능에 영향을 주는 특징점 영역(Minutiae Mask)과 융선 영역(Ridge Mask)을 고려한다.

원 지문영상과 워터마크가 삽입된 지문영상의 인식 성능 측정을 위하여 스마트카드용 지문인식 알고리즘[7]을 사용하였으며, 실험 결과는 4장에 기술한다.

3.2 얼굴 정보에 지문 정보 은닉

시나리오 2는 그림 2와 같이 워터마크로 사용될

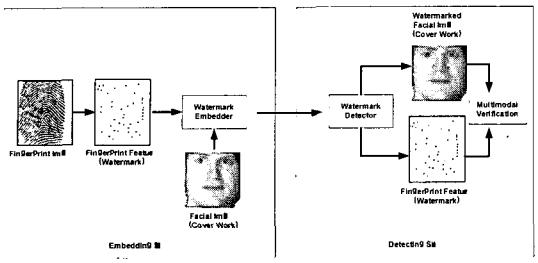


그림 2. 시나리오 2의 흐름도

지문 특징 정보를 삽입 측에서 추출한 후 원본 영상으로 사용되는 얼굴영상에 삽입한다. 워터마크가 삽입된 얼굴영상을 수신한 검출부에서는 삽입된 지문 특징정보를 검출한 후 얼굴영상과 지문 특징 정보를 이용하여 사용자 인증과정을 수행한다.

원 얼굴영상과 워터마크가 삽입된 얼굴영상의 인식 성능을 비교하기 위하여 Eigenface 방법[8]과 LFA(Local Feature Analysis) 방법[9]을 사용하였다. 전역적인 특징을 추출하는 대표적인 방법으로 PCA(Principal Component Analysis)를 이용하는 Eigenface 방법의 기저 벡터는 얼굴 형태를 기술하는 모델로서, 얼굴을 이루는 눈, 코, 턱, 그리고 볼 같은 지역적 구조의 형태보다 얼굴의 전체적인 모양을 기술한다. 기저벡터에 얼굴 영상 데이터를 선형 투영하여 얻은 계수 값들을 특징 벡터로 하여 인식에 사용한다. Eigenface는 간단하면서 빠른 인식 속도를 보여 주지만, 조명과 얼굴 방향 같은 외부 변화에 인식률이 많은 영향을 받는다.

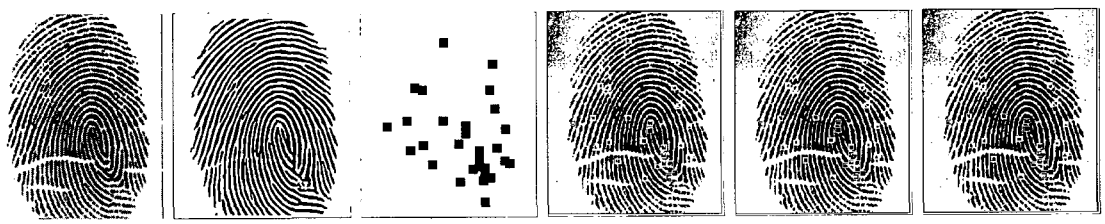
반면 Composite Template 얼굴인식 알고리즘[9]은 대표적인 지역적 얼굴 특징 추출 방법으로 알려진 LFA를 이용한 것으로, 지역적 특징을 이용하기 때문에 환경 변화에 비교적 영향을 받지 않는다. LFA는 눈, 코, 턱, 그리고 볼 같은 얼굴을 이루는 세부적인 구조를 잘 기술하는 kernel이라는 기저벡터를 생성한다. 하지만 입력영상의 차원과 동일한 개수의 kernel이 생성되기 때문에 차원 축소를 위해 인식에 적합한 kernel의 부분집합을 선택해야 하는 문제점이 있다. Composite Template 방법은 이러한 차원 축소의 문제점을 해결하면서 얼굴인식 성능 향상에 효과적인 부분 집합을 선택하는 방법을 제안하였으며, 실험 결과는 4장에서 기술한다.

Ⅳ. 실험 결과 및 성능 분석

시나리오별 타당성을 확인하기 위해 워터마크의 삽입으로 인한 인식 성능의 변화를 측정하였다. 먼저, 지문인식 성능의 측정을 위해 광학 센서[10]를 통해 입력된 248×292 크기의 gray scale 지문영상 2,412개를 사용하였다.

시나리오 1은 3장에서 설명한 것처럼 워터마크 삽입영역 결정시 지문영상의 특징점과 융선 정보를 고려한다. 그림 3(a)는 취득된 원 지문 영상이며, 그림 3(d)는 그림 3(a)에서 추출한 특징점 영역을 네모박스로 표시하였다. 그림 3(b)와 그림 3(c)는 각각 융선 영상(Ridge Mask)과 특징점의 위치를 표현한 영상(Minutiae Mask)이며 검은색 영역은 삽입 영역에서 배제된다. 그림 3(e)와 그림 3(f)는 각각 융선과 특징점 정보를 반영하여 워터마킹 알고리즘을 수행한 후에 추출한 특징점 영역을 나타낸다. 실험에 의하여 식 1의 가중치 k를 0.06으로 했을 때 사람의 눈으로 워터마크의 삽입여부를 구분할 수 없었다.

그림 4는 지문인식에 대한 4가지 ROC 곡선을 보여준다. 그림 4에서 특징점 정보(Minutiae Mask)를 이용한 워터마크 방법과 융선 정보(Ridge Mask)를 이용한 워터마크 방법이 원 지문영상(Original)의 인식 성능과 비교했을 때 약간의 저하가 나타난 것을 볼 수 있다. 그러나, 융선과 특징점 정보를 고려한 워터마킹 방법이 고려하지 않은 워터마킹 방법(No Mask)에 비해 인식 성능이 향상된 것을 알 수 있다.



(a) Original (b) BinaryMask (c) MinutiaeMask (d) Based NoMask (e) Based BinaryMask (f) Based MinutiaeMask

그림 3. 워터마크 삽입 후 특징점 추출 결과

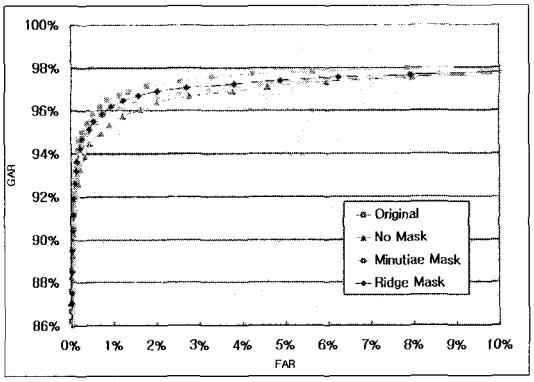
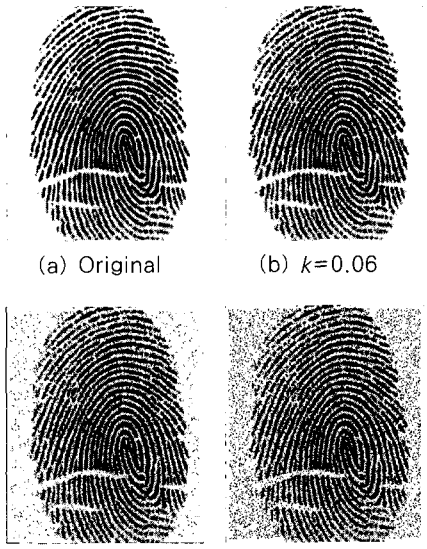


그림 4. 지문 인식 ROC 곡선

워터마크 삽입에 따른 지문인식 성능의 변화를 분석하기 위하여 식 1의 가중치 k를 다양하게 조절하여 얼굴의 특징정보를 삽입하였다. 그림 5(a)는 취득된 원 지문영상이며 5(b), 5(c)와 5(d)는 각각 가중치 k가 0.06, 0.12, 0.24일 때 워터마크가 삽입된 지문영상이다. k값이 큰 영상(그림 5(d))에서 영상의 훼손이 심한 것을 확인할 수 있다.

그림 6은 k값의 변화에 따른 지문인식 성능에 관한 ROC곡선이다. 그림 6(a)는 워터마크의 삽입 위치를 선정할 때 지문 정보를 고려하지 않은 k값만 변화시킨 워터마킹 방법에 대한 지문인식 결과이고, 그림 6(b)는 융선 정보를 고려한 워터마킹 방법의 지문인식 결과이다. 지문 정보를 고려하지 않은 워터마킹 방법은 삽입 강도가 강해지면서 인식 성능이 저하되는 것을 볼 수 있다. 반면, 그림 6(b)의 융선 정보를 고려한 방법도 강도를 다르게 했을 때 인식 성능에 약간의 차이는 있지만 그림 6(a)의 지문 정보를 고려하지 않은 방법보다는 성능의 저하가 덜 발생하는 것을 알 수 있다.



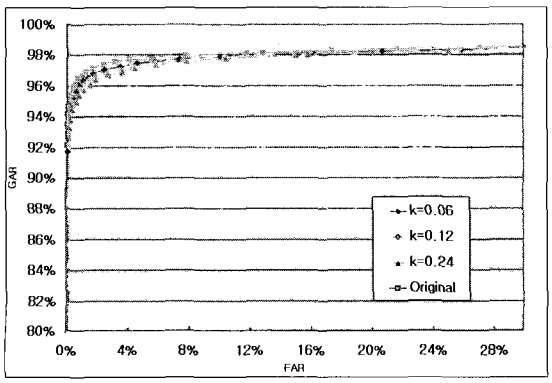
(a) Original (b) k=0.06

(c) k=0.12 (d) k=0.24

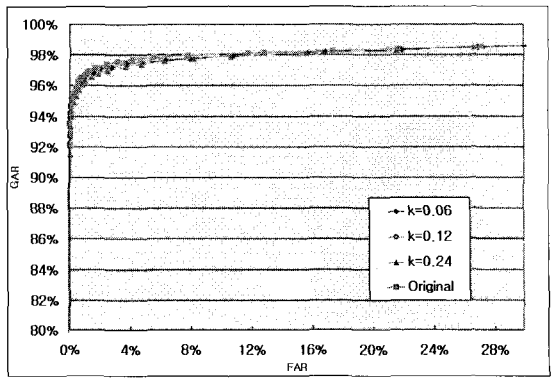
그림 5. 얼굴 정보가 삽입된 지문 영상

얼굴 인식 실험에 사용한 얼굴 영상 데이터베이스는 총 55명에 대해 1인 당 20장의 얼굴 정면 사진으로 구성되어 있으며, 영상 크기는 64×64이다. 55명의 영상 중 20명의 얼굴 영상은 특징 추출을 위한 기저 벡터 생성에 사용하였고, 나머지 35명의 얼굴 영상을 등록과 테스트에 사용하였다. 등록과 테스트에 1인당 각각 10장의 영상을 사용하고, Euclidean 거리를 이용하여 등록된 데이터와 테스트 데이터를 비교하였다.

시나리오 2의 워터마크 삽입에 따른 얼굴인식 성능의 변화를 분석하기 위하여 식 1의 가중치 k를 다양하게 조절하여 지문의 특징정보를 삽입하였다. 그림 7(a)는 취득된 원 얼굴영상이며 7(b), 7(c)와

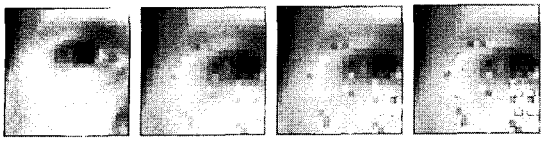


(a) No Mask



(b) Ridge Mask

그림 6. 지문인식 ROC 곡선



(a) Original (b) k=0.06 (c) k=0.12 (d) k=0.24

그림 7. 지문 정보가 삽입된 얼굴 영상

7(d)는 각각 가중치 k가 0.06, 0.12, 0.24일 때 워터마크가 삽입된 얼굴영상이다. 시나리오 1의 지문 영상과 마찬가지로 k값이 큰 영상(그림 7(d))에서 영상의 훼손이 심한 것을 확인할 수 있다.

그림 8은 얼굴인식에 대한 ROC 곡선을 보여주며, 그림 8(a)는 Composite Template 방법을 이용한 얼굴인식 결과이고, 그림 8(b)는 PCA 방법을 이용한 얼굴인식 결과이다. 그림 8(b)에서와 같이 얼굴영상이 워터마크의 삽입에 의하여 훼손되었을 경우에도 성능의 저하가 거의 없음을 알 수 있다. 이는 지문인식과는 달리 얼굴인식은 얼굴의 전역적인 정보를 이용하여 인식을 하기 때문이다. 또한, 그림 8(a)의 경우 전체적인 정보와 지역적인 정보를 같이 사용함으로써 얼굴인식 성능이 워터마크 삽입으로 인하여 약간 저하되었지만 시나리오 1의 지문인식 성능과 비교하면 그 차이는 무시할 수 있다. 또한, 일반적으로 생체인식관련 연구에서 보고된 것처럼 지문인식 시스템의 인식 성능이 얼굴인식 시스템의 인식 성능 보다 우수하다는 것을 그림 6과 그림 8의 그래프 비교를 통하여 확인 할 수 있다.

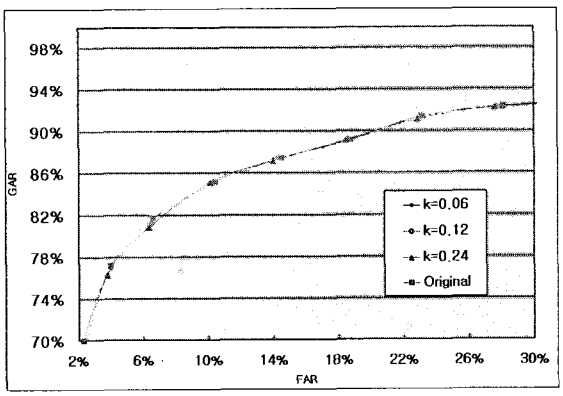
V. 결 론

원격 생체인식 시스템에 암호 기술 또는 디지털 워터마킹 기술을 적용함으로써 보다 향상된 안전성을 제공할 수 있다. 본 논문에서는 안전하지 않은 전송채널을 통해서 전송되는 생체정보의 보호를 위한 워터마킹 방법을 고려하였다. 특히, 지문과 얼굴을 이용하는 다중 생체인식 시스템에서 생체정보의 무결성과 기밀성을 보장하기 위한 방법을 제안하였다. 다중 생체 인식 시스템에서 가능한 두 가지 시나리오를 고려하였으며, 실험에 의하여 지문영상에 얼굴의 특징정보를 삽입하는 것보다 얼굴영상에 지문의 특징정보를 삽입하여 전송하는 것이 인식성능면에서 타당함을 확인하였다.

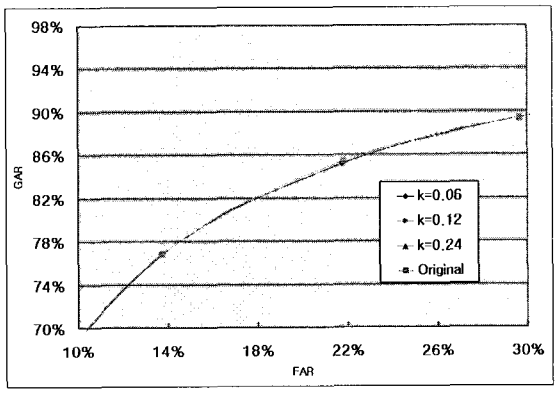
결론적으로, 다음 3가지 이유로 인하여 얼굴영상에 지문의 특징정보를 삽입하는 것이 타당하다. 1) 얼굴영상은 이미 온라인상에서 쉽게 획득할 수 있기 때문에 얼굴정보를 숨기기 위한 워터마크로 사용하는 것보다 원본 영상으로 사용하는 것이 타당하다. 2) 얼굴인식 성능은 워터마크의 삽입으로 발생하는 얼굴영상의 훼손에 덜 민감하다. 3) 일반적으로 지문인식 성능이 얼굴인식 성능 보다 우수하기 때문에 전체적인 시스템의 성능향상을 위하여 지문특징정보를 워터마크로 사용하여 보호하는 것이 타당하다. 따라서, 대용량 생체 인식 시스템에서 요구하는 멀티 모달 인식 시스템에서 보안을 더욱 강화 할 수 있다.

참 고 문 헌

[1] A. Jain, R. Bole, and S. Panakanti, *Biometrics:Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.



(a) Composite Template



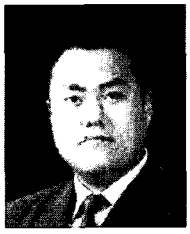
(b) PCA

그림 8. 얼굴인식 ROC 곡선

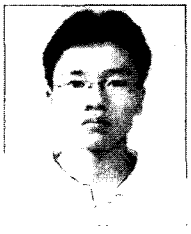
[2] W. Stallings, *Cryptography and Network Security*, Pearson Ed. Inc., 2003.
[3] A. Jain, U. Uludag, and R. Hsu, "Hiding a Face in a Fingerprint Image", *Proc. of Int. Conf. on Pattern Recognition*, Vol. 3, pp. 756-759, 2002.
[4] M. Yeung and S. Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval", *Journal of Electronic Imaging*, Vol. 9, No. 4, pp. 468-476, 2000.
[5] B. Gunsel, U. Uludag, and A. Tekalp, "Robust Watermarking of Fingerprint Image", *Pattern Recognition*, Vol. 35, No. 12, pp. 2739-2748, 2002.
[6] A. Ross and A. Jain, "Multimodal Biometrics: An Overview", *Proc. of European Signal Processing Conference*, pp. 1221-1224, 2004.
[7] S. Pan, et al., "A Memory-Efficient Fingerprint Verification Algorithm using A Multi-Resolution Accumulator Array for Match-on-Card", *ETRI Journal*, Vol. 25, No. 3, pp. 179-186, 2003.
[8] M. Turk and A. Pentland, "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, Vol. 3, pp. 71-86, 1991.
[9] Y. Lee, et al., "Local and Global Feature Extraction for Face Recognition", *LNCS 3546-AVBPA*, pp. 219-228, 2005.
[10] NitGen, http://www.nitgen.co.kr.

〈著者紹介〉

문 대 성 (DaeSung Moon) 정회원
1999년 2월: 인제대학교 전산학과 학사
2002년 2월: 부산대학교 컴퓨터공학과 석사
2002년 3월~현재: 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 연구원
〈관심분야〉 생체인식, 정보보호, 영상처리



정 승 환 (SeungHwan Jung)
2005년 2월: 고려대학교 전산학과 학사
2005년 3월~현재: 고려대학교 전산학과 석사과정
〈관심분야〉 생체인식, 정보보호, 병렬 알고리즘



김 태 해 (TaeHae Kim)
1992년 2월: 인제대학교 전산학과 학사
2004년 3월~현재: 고려대학교 전산학과 석사과정
〈관심분야〉 생체인식, 정보보호, 병렬 알고리즘

정 용 화 (Yongwha Chung) 종신회원
1984년 2월: 한양대학교 전자통신공학과 학사
1986년 2월: 한양대학교 전자통신공학과 석사
1997년 2월: 미국 Univ. of Southern California 전기공학과(컴퓨터공학 전공) 박사
1986년~2003년: 한국전자통신연구원 생체인식기술연구팀장
2003년 9월~현재: 고려대학교 컴퓨터정보학과 부교수
〈관심분야〉 생체인식, 정보보호, 생체정보보호

문 기 영 (KiYoung Moon)
1986년 2월: 경북대학교 전자공학과 학사
1989년 2월: 경북대학교 대학원 전자공학과 석사
1992년~1994년: (주)대우정보시스템 기술연구소 전임연구원
1994년 3월~현재: 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 팀장
〈관심분야〉 생체인식, 웹서비스 보안, 분산 시스템