한국지능시스템학회 논문지 2009, Vol. 19, No. 1, pp. 75-82

워터마킹 기법을 이용한 생체정보와 취급자 정보의 은닉

Biometric Features and Responsible Person Information Hiding by Watermarking Technique

이욱재* · 이대종** · 박진일* · 조재훈* · 전명근*+
Wook-Jae Lee*, Dae-Jong Lee**, Jin-Il Park*, Jae-Hoon Cho*, Myung-Geun Chun*+

*충북대학교 전기전자컴퓨터공학부 컴퓨터정보통신연구소

요 약

본 논문에서는 인증되지 않은 불법 사용자로부터 얼굴, 지문 등의 생체정보의 유출을 막기 위한 은닉기법과 더불어 이러한 생체정보가 유출 되었더라도 이진 영상으로 표현되는 취급자 정보를 삽입하여 관리함으로서 책임소재를 파악할 수 있는 기법을 제안한다. 이를 위해, 생체인식 기법으로 널리 사용되고 있는 지문인식과 얼굴인식을 대상으로 각각이 워터마킹의 커버영상으로 사용되었을 경우의 인식률과 추출된 취급자 정보의 비트 에러율을 조사하여 생체인식 기법별로의 특성을 파악하는 실험을 수행하고 그 특성을 비교 분석하였다. 이러한 다양한 실험의 결과로부터 본 연구에서 제안된 방법이 생체정보의 보호를 위한 다양한 응용 분야에 적용될 수 있음을 확인 할 수 있었다.

키워드 : 워터마킹, 생체정보, 웨이블렛

Abstract

This paper propose a method to hide not only biometric features in the biometric image such as face and fingerprint for protecting them from unauthorized entity but also information of responsible person expressed as binary image which can be used to identify the responsibility of divulgence. For this, we investigate the recognition rates and bit error rates of extracted responsible person information watermark for the cases of using face and fingerprint images as cover images for fingerprint and face recognition which are the most popular biometric techniques. From these experiments, we confirm that the proposed method can be used for various application requiring to protect personal biometric information

Key Words : Biometric System, Watermarking, information hiding

1. 서 론

최근 정보통신 기술이 급속히 발달함에 따라 인간의 삶의 질은 향상되어 가고 있지만, 컴퓨터 간 정보의 불법 복제 및 삭제, 불법 정보유출 등에 의한 사회적 손실도 증가하고 있다. 이러한 문제점을 해결하기 위하여 해킹, 누출에 의해 정보가 도용될 수 없고, 또한 변경되거나 분실할 위험성이 없는 신분 검증 기법인 생체인식 기술이 각광을 받고 있다[1]. 이러한 생체인식기술은 인터넷 뱅킹, 금융서비스, 인터넷을 통한 중요한 자료에 대한 정보보호 등으로 이용되고 있으며, 테러 용의자, 범죄자 등의 접근을 차단하는 최첨단 감시시스템으로서도 주목받고 있다.

개인마다 타고난 신체적·행동적 특성을 이용한 생체정보의 불변성은 보안시스템의 성능을 극대화하는 반면에 생체정보가 분실되었을 경우 비밀번호나 ID처럼 변경이 어렵다는 치명적인 단점을 지니고 있다. 이런 이유로 생체인식시스템의 개발에도 불구하고 사용자로 하여금 생체정보의 유출에 따른 문제로 생체정보의 데이터베이스화 하거나 온라인상에서 생체정보의 사용을 꺼려하고 있는 추세다[2]. 이와 같이 생체정보의 유출 및 불법적 사용에 대한 문제점을 해결하기 위하여 생체정보를 은닉하여 불법 사용자가 은닉된 생체데이터에 접근하지 못하도록 하는 워터마킹에 대한 연구가 진행되고 있다. 생체정보의 은닉을 위한 연구 분야에서 Jain 등은 지문 영상에 얼굴정보를 삽입할 수 있는 지문 영상 워터마킹 기법을 제시하였다[3]. 이 기법은 얼굴의 특징인 고유 얼굴을 지문 영상에 워터마크로써 삽입한 후, 복원된 얼굴 영상은 얼굴 확인에 이용될 수 있음을 제안하였고, 워터마킹에 따른 지문 영상과 지문 특징의 변형정도를 실험결과로 제시하였으나, 지문 및 복원된 얼굴 인식에 대한 실험은 제시되지 않았다. 또한, Wu와 Kuo는 음성신호의 무결성을 보장하는 워터마킹 기법을 제안하였고, Soutar은 생체데이터를 이용하여 디지털 키를 연결하고 가져오는 생체암호화 기법을 제안하였다[4][5]. 이외에도 Vatsa 등은 RDWT 워터마킹 알고리즘을 이용하여 칼라 얼굴영상 내에 음성특징을 삽입하고 추출한 후 두 가지의 생체정보를 이용한 다중생체인식시스템을 제안하였고[6], Marcos[7] 등은 화자인식시스템 성능향상을 위한

접수일자 : 2008년 9월 11일
완료일자 : 2009년 1월 5일
본 연구는 보건복지가족부 보건의료기술진흥사업의 지원에 의하여 이루어진 것임. (과제고유번호 : A040032)
+ : 교신저자

음성워터마킹 알고리즘을 제안하는 등 최근까지 생체특징을 은닉하기 위한 연구가 활발히 진행되고 있다. 그러나 아직 생체정보 보호와 생체정보의 유출에 대비한 취급자 정보의 은닉을 동시에 다루는 연구는 이루어지고 있지 않고 있다.

한국정보보호 진흥원에서는 생체인식 시스템을 개인식별에 이용하는 생체정보를 보호하기 위하여 준수하여야 할 사항을 정함으로써 생체정보의 안전한 이용환경을 조성함을 목적으로 생체정보보호 가이드라인을 제정하여 운영하고 있다[8]. 이의 제 4조의 기본원칙에 따르면, 생체인식 시스템의 운영자는 생체정보의 도난, 멸실, 훼손, 유출 등 각종 위험을 방지하기 위하여 적절한 보호 조치를 취하여야 한다고 규정하고 있다. 그러나 이러한 생체정보보호를 위한 생체인식 시스템의 관리적 기법과 더불어 기술적으로 이를 지원하기 위한 방법들에 관한 연구는 미비한 실정이다.

이에, 본 논문에서는 생체정보의 은닉 및 추출만을 고려한 논문 [9]의 연구결과를 토대로 생체정보와 더불어 취급자 정보를 효과적으로 은닉 및 추출할 수 있는 방법을 개발한다. 개발된 방법은 인증되지 않은 불법사용자로부터 생체정보의 유출을 방지하기 위한 기법뿐만 아니라 설령 생체정보가 유출되더라고 취급자정보에 의해 유출된 생체정보의 유출 정보를 파악할 수 있는 특징이 있다. 제안된 방법의 유용성을 보이기 위해, 생체인식 기법으로 널리 사용되고 있는 지문인식과 얼굴인식을 대상으로 각각이 워터마킹의 커버영상으로 사용되었을 경우의 인식률과 추출된 취급자 정보의 비트 에러율을 조사하여 생체인식 기법별로의 특성을 파악하는 실험을 수행하고 그 특성을 비교 분석하였다.

2. 워터마킹 기법을 이용한 생체정보와 취급자 정보의 은닉

그림 1에서는 워터마킹 알고리즘을 적용한 개인정보의 은닉기법 구성도를 나타냈다. 그림 1에서 보는 바와 같이 본 연구에서는 원본영상으로 얼굴, 지문 등의 생체정보를 고려하였고, 은닉하고자 하는 정보로서는 특징추출기법에 의해 계산된 얼굴, 지문 등의 생체특징과 취급자정보를 동시에 고려하였다. 이를 은닉하기 위한 정보의 형태는 통상의 워터마크로 널리 사용되고 있는 이진영상을 응용하여 그림 2와 같이 표현되는 영어 알파벳과 숫자의 이진 영상의 텍스트를 이용하였으며 지문이나 얼굴영상의 사이즈를 고려하여 여기에 은닉하기에 적합한 사이즈로 글자당 5×6의 픽셀 크기를 갖도록 구성 하였다.

본 연구에서는 기존의 지문, 얼굴 등의 생체 인식시스템의 성능저하를 초래하지 않으면서도 생체특징과 취급자정보를 안전하게 은닉할 수 본 저자들에 의해 제안된 웨이블릿기반 워터마킹 알고리즘을 적용하였다. 일반적으로 워터마킹 알고리즘은 정보를 안전하게 은닉하는 은닉과정과 은닉된 정보를 복원하는 추출단계로 구성되는데 본 논문에서는 워터마크 알고리즘을 적용하여 취급자 정보와 생체정보를 동시에 은닉할 경우 생체특징별로 추출된 특징정보의 인식률과 추출된 취급자 정보에 대한 비트 에러율에 대한 다양한 실험에 초점을 두었다. 사용되는 워터마킹 기법을 은닉과정과 추출과정으로 구분하여 설명하면 다음과 같다[9].

먼저, 생체정보 및 취급자 정보의 은닉과정은 다음과 같다.

[단계 1] 원본 영상 (X)를 1-레벨 웨이블릿 변환한다.

[단계 2] 고주파부분의 서브밴드(LH1, HL1, HH1)계수를 0으로 바꾼다.

[단계 3] 고주파부분을 제거한 값을 역 웨이블릿 변환을 하여 기준영상 (X′)을 만든다.

[단계 4] 원본 영상(X)과 기준 영상 (X′)간의 차를 계산한다.

[단계 5] 랜덤하게 결정된 삽입위치 (Key값) 에 아래와 같은 식 (1)을 이용해 워터마크를 삽입하게 되며, 가중치 α는 다음 식 (2)에 따라 적응적으로 결정된다. 여기서 은닉하고자 하는 생체정보와 취급자정보의 워터마크 값은 1(흰색) 또는 -1(검은색) 로 표현되는 이진값을 갖는다.

$$Xw(idx(i,j)) = \begin{cases} x(idx(i,j)) + \alpha & \text{if } w(k) = 1 \text{ and } s < x(idx(i,j)) - x'(idx(i,j)) < t \\ x(idx(i,j)) - \alpha & \text{if } w(k) = -1 \text{ and } s < x'(idx(i,j)) - x(idx(i,j)) < t \end{cases} \quad (1)$$

여기서,
$$\alpha = f(x, a, c) = \frac{1}{1+e^{-a(x-c)}} \quad (2)$$

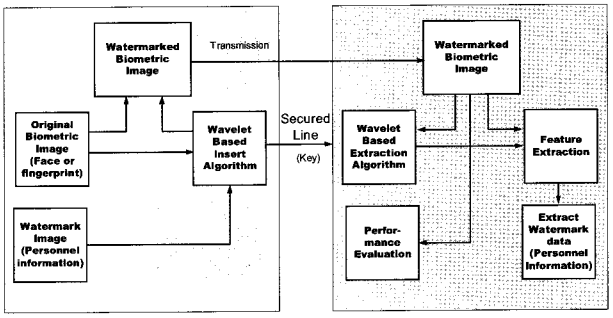


그림 1. 생체정보와 취급자정보의 은닉기법
Fig. 1 Hiding method of biometric and responsible person information

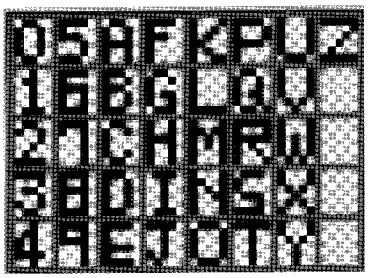


그림 2. 취급자정보를 표현하기 위해 사용된 텍스트 영상
Fig. 2 Text based image for responsible person information

워터마킹 삽입 후에 은닉된 워터마크 데이터 추출과정을 단계별로 살펴보면 다음과 같다.

[단계 1] 워터마크된 이미지(Xw)를 1-레벨 웨이블릿 변환한다.

[단계 2] 고주파부분의 서브밴드(LH1, HL1, HH1)계수를 0으로 바꾼다.

[단계3] 고주파부분을 제거한 값을 역 웨이블릿 변환을 하여 기준영상(X′)를 만든다.

[단계 4] 원본영상 (X)과 기준영상 (X′) 간의 차를 계산한다.

[단계 5] 전달받은 Key와 아래 식 (3)을 이용해 취급자정보와 생체정보를 담고 있는 워터마크 데이터를 추출한다.

$$w'(k) = \begin{cases} 1 \text{ if } Xu(idx(i,j)) \geq Xw(idx(i,j)) \\ -1 \text{ if } Xu(idx(i,j)) \leq Xw(idx(i,j)) \end{cases} \quad (3)$$

3. 실험 및 결과분석

3.1 실험 방법

제안된 워터마크 알고리즘의 성능을 평가하기 위한 실험 방법은 다음과 같이 다양한 경우를 고려하였다. Case 1)의 실험을 살펴보면, 제안된 방법의 성능비교 기준인 워터마크 삽입전의 인식률을 분석하였다. 또한, 이진영상으로 표현된 취급자 정보를 포함하고 있는 얼굴영상에 퍼지 선형판별분석기법[10]을 적용하여 계산된 얼굴특징값을 이용한 인식률 분석과 은닉된 취급자 정보를 제안된 방법에 의해 추출한 후의 취급자정보의 왜곡상태를 분석하였다. 은닉하고자 하는 취급자 ID 정보는 그림 3에서 보는 바와 같이 주민등록 번호와 같은 13자리의 숫자와 이름을 표현하기 위한 11개의 스트링 길이를 갖는 영문 알파벳으로 구성하였다. 이 외에도 얼굴특징과 취급자정보가 동시에 은닉된 얼굴영상에 대한 인식률과 제안된 방법에 의해 추출된 얼굴특징과 취급자 정보에 대한 성능도 평가하였으며, 지문특징과 취급자정보가 동시에 은닉한 얼굴영상에 대한 분석도 수행하였다. Case 2)의 지문영상에 대한 실험은 Case 1)의 얼굴영상 대신에 지문영상이 대체된 것으로 Case 1)의 실험방법과 동일하다.

Case 1) 얼굴영상에 워터마크를 삽입한 경우
- ① 얼굴영상에 취급자정보를 은닉한 경우의 특성
- ② 얼굴영상에 얼굴특징과 취급자정보를 동시에 은닉한 경우의 특성
- ③ 얼굴영상에 지문특징과 취급자정보를 동시에 은닉한 경우의 특성

Case 2) 지문영상에 워터마크를 삽입한 경우
- ① 지문영상에 취급자정보를 은닉한 경우의 특성
- ② 지문영상에 얼굴특징과 취급자정보를 동시에 은닉한 경우의 특성
- ③ 지문영상에 지문특징과 취급자정보를 동시에 은닉한 경우의 특성

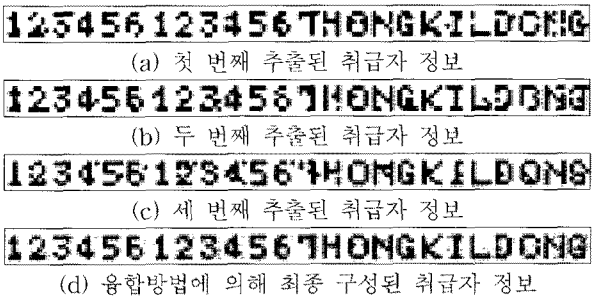
그림 3. 이진영상으로 구성된 취급자의 ID 정보
Fig. 3 ID information of responsible person consisted of binary image

실험에 사용된 얼굴영상과 지문영상은 포항공대에서 제작한 얼굴 DB와 충북대에서 제작한 지문 DB를 각각 사용하였다. 얼굴 DB는 서로 다른 환경에서 50명으로부터 한 사람당 6개의 얼굴을 취득하여 총 300개의 얼굴 영상으로 구성되어 있다 각각의 얼굴영상들은 0에서 255까지 그레이 값을 가진 256×256영상 크기에 의해 나타내어진다. 지문 DB인 경우에도 서로 다른 환경에서 50명으로부터 한 사람당 256×256의 크기를 갖는 6개의 지문을 취득하여 총 300개의 지문 영상으로 구성되어 있다. 인식률 분석을 위해 한 사람당 총 6개의 얼굴 또는 지문영상 중에서 3장은 학습용으로 나머지 3장은 검증용으로 사용하였다. 학습용으로 사용된 생체영상은 얼굴의 경우 퍼지 선형판별분석기법[10], 지문의 경우는 체인코드 컨투어 기법[11]을 적용하여 산출된 얼굴 및 지문 특징들이 생체 DB에 저장된다. 이후 검증용으로 사용된 나머지 영상들을 이용하여 동일한 방법으로 퍼지 선형판별분석기법 및 체인코드 컨투어기법에 의해 특징들을 추출한 후 생체 DB에 저장된 학습용 특징들과 비교를 통하여 최종 인식률을 산출한다. 이 때 검증용으로 사용된 생체영상에 위에서 설명한 여러 가지의 워터마크 데이터를 삽입하여 워터마크 삽입전과 후의 특성을 본 실험을 통하여 분석하고자 한다.

3.2 실험 결과

(1) 얼굴영상에 워터마크를 삽입한 경우의 특성분석 (Case 1)

본 연구에서는 생체정보 뿐만 아니라 이진 영상으로 표현된 취급자 정보를 동시에 고려한 은닉방법을 제안하였다. 우선, 취급자 정보의 삽입 정도에 따른 생체 인식시스템의 영향을 분석하기 위하여 동일한 취급자 정보를 1회, 2회 및 3회 반복적으로 삽입하였다. 2회 또는 3회 취급자 정보를 삽입한 후 추출한 경우에는 1회 삽입 후 추출한 경우와 달리 최종 판단을 위한 융합과정이 필요하다. 본 논문에서는 가시성을 향상시키기 위하여 이진영상으로 표현된 취급자정보를 평균한 그레이 영상으로 표현하였다. 그림 4에서는 개인정보를 3회 삽입하고 추출한 후 제안된 융합방법에 의한 최종적인 개인정보를 나타냈다. 그림 4에서 보는 바와 같이 대응되는 3개의 모든 픽셀의 값이 0 또는 1이면 융합한 결과는 0 또는 255로 그레이 영상으로 변환된다. 또한, 대응되는 3개의 픽셀 값 중에서 0인 값이 1개이고 1인 값이 2개인 경우 170(255×2/3)인 그레이 영상으로 변환된다. 따라서 대응되는 모든 픽셀의 값이 동일하다면 시각적으로 뚜렷한 값을 나타내고, 이와 달리 픽셀의 값이 차이가 발생한다면 발생된 픽셀의 0 또는 1의 빈도값에 의해 최종 구성 영상의 명암이 결정된다. 그림 4에서도 알 수 있는 바와 같이 개인정보를 3회 삽입한 후 추출하고 제안된 융합방법에 의해 취급자 정보를 추출한 결과가 우수하게 나타났다. 그러나 개인정보의 추출 성능만을 고려하여 삽입횟수를 증가시킬 경우 원본 영상의 은닉성이 떨어짐으로 본 연구에서는 최대 3회까지 개인정보를 은닉하였다.



(a) 첫 번째 추출된 취급자 정보

(b) 두 번째 추출된 취급자 정보

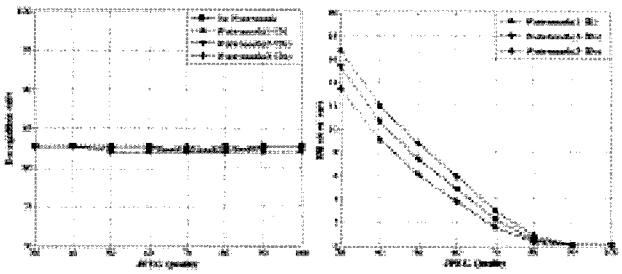
(c) 세 번째 추출된 취급자 정보

(d) 융합방법에 의해 최종 구성된 취급자 정보

그림 4. 얼굴영상에 동일한 취급자 정보를 3회 은닉 후 추출한 결과(JPEG 60)
Fig. 4 Result extracted of responsible person information (JPEG 60)

그림 5에서는 커버얼굴영상에 이진영상의 취급자정보를 삽입한 후의 특성을 나타냈다. 그림 5(a)에서는 JPEG 품질

을 변화시키면서 취급자정보가 커버 얼굴영상에 대한 인식률을 나타내었다. 그림 5(a)에서 보는 바와 같이 영상의 JPEG 품질(Quality)을 저하시키더라도 인식률의 저하는 초래하지 않았다. 그러나 그림 5(b)에 나타낸 바와 같이 추출된 취급자 정보는 영상의 JPEG 품질이 저하될 경우 비트에러율을 급격히 증가함을 알 수 있다. 그림 6에서는 비트에러율이 가장 크게 나타난 JPEG 품질이 30이고 취급자 정보를 3회 반복 삽입한 후 추출된 결과를 나타냈다. 그림 6에서 보는 바와 같이 비트에러율은 크게 증가했으나 추출된 영상으로 취급자 정보를 확인할 수 있음으로 영상의 JPEG 품질저하에 따른 문제점을 극복할 수 있는 것으로 판단된다.

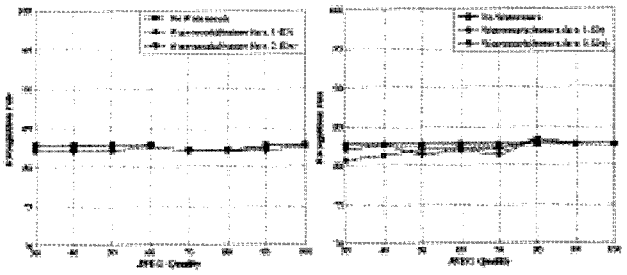


(a) 취급자정보 삽입에 따른 인식률 (b) 취급자정보 추출후의 비트 에러율

그림 5. 얼굴영상에 취급자정보를 은닉한 경우의 실험결과
Fig. 5. Experimental results in case of hiding responsible person information in face image

그림 6. 취급자정보 3회 반복 은닉 후 추출한 결과 (JPEC 30)
Fig. 6 Result extracted of responsible person information (JPEG 30)

그림 7에서는 얼굴영상에 얼굴특징과 취급자정보를 동시에 은닉한 경우의 특성결과를 나타냈다. 취급자 정보만을 은닉하였을 경우에는 최대 3회 반복 삽입하였으나 얼굴특징과 취급자 정보를 동시에 고려할 경우에는 원본영상의 비가시성을 고려하여 취급자 정보는 최대 2회 반복 삽입하였다. 따라서 은닉하고자 하는 정보인 얼굴의 특징은 1회 삽입하고, 취급자 정보는 1회와 2회 각각 삽입한 후 특성을 분석하였다. 그림 7(a)에서는 두 가지 정보를 은닉한 얼굴영상에 대한 JPEG 품질 대비 인식률을 나타냈으며, 그림 7(b)는 은닉 후 추출된 얼굴의 특징값을 이용한 인식률을 나타냈다. 그림 7에 나타낸 두 가지의 은닉정보가 삽입된 얼굴영상에 대한 인식률과 은닉한 후 추출된 얼굴의 특징값을 이용하여 구한 인식률을 살펴보면, 영상의 JPEG 품질이 저하되더라도 약간의 인식률 저하는 발생하였지만 전반적으로 인식률의 변화는 적은 것으로 나타났다. 특히 JPEG 품질이 100인 경우 은닉정보가 포함된 커버 얼굴영상에 대한 인식률과 삽입후 추출된 얼굴특징에 대한 인식률은 은닉정보가 있지 않은 커버 얼굴영상에 대한 인식률과 동일하게 나타났다. 이는 인위적으로 JPEG 품질을 저하시키지 않을 경우 중요한 정보를 얼굴에 은닉하더라도 인식률의 관점에서의 손실은 발생하지 않음을 의미한다. 이진영상의 취급자 정보는 은닉 후 추출알고리즘에 의해 추출된 경우 본래의 취급자 정보와 비교해 볼 때 비트에러율을 급격히 증가하였다. 그러나 그림 8에서 보인 바와 같이 비트에러율이 증가하나, 시각적으로 충분히 취급자 정보를 확인할 수 있는 정도이다.



(a) 워터마크 삽입에 따른 인식률 (b) 얼굴특징 추출 후의 인식률

그림 7. 얼굴영상에 얼굴특징 및 취급자정보를 은닉한 경우
Fig. 7. Experimental results in case of hiding face feature and responsible person information in face image

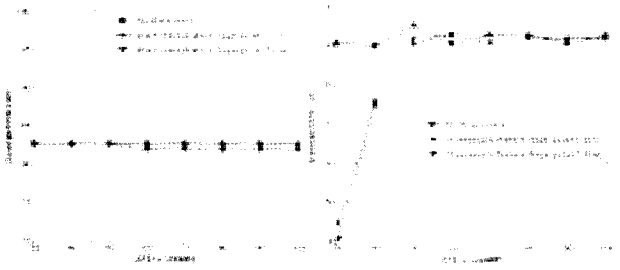
그림 8. 취급자정보 2회 반복 은닉 후 추출한 결과(JPEC 30)
Fig. 8 Result extracted of responsible person information (JPEG 30)

그림 9에서는 얼굴영상에 지문특징과 취급자정보를 동시에 은닉한 경우의 특성결과를 나타냈다. 이 때 은닉하고자 하는 정보인 지문의 특징은 1회 삽입하고, 취급자 정보는 1회와 2회 각각 삽입한 후 결과를 구하였다. 그림 9(a)에서는 두 가지 정보를 은닉한 얼굴영상에 대한 JPEG 품질 대비 인식률을 나타냈으며, 그림 9(b)는 은닉 후 추출된 지문의 특징값을 이용한 인식률을 나타냈다. 그림 9에 나타낸 두 가지의 은닉정보가 삽입된 얼굴영상에 대한 인식률을 살펴보면, 영상의 JPEG 품질이 저하되더라도 약간의 인식률 저하는 발생하였지만 전반적으로 인식률의 변화는 적은 것으로 나타났다. 지문특징을 얼굴영상에 은닉한 후 추출한 후 지문 인식률을 살펴본 결과 JPEG 품질이 50 미만으로 저하된 경우 인식률은 급격히 감소한 것으로 나타났다. 그러나 JPEG 품질을 저하시키지 않을 경우 지문정보를 얼굴에 은닉하더라도 기존 생체인식시스템의 성능과 거의 동일함을 확인할 수 있다. 이진영상의 취급자 정보는 은닉 후 추출알고리즘에 의해 추출된 경우 본래의 취급자 정보와 비교해 볼 때 비트에러율이 급격히 증가하였으나, 그림 10에서 보인 바와 같이 비트에러율이 증가하였다 하더라도 시각적으로 충분히 취급자 정보를 해석할 수 있는 것으로 나타났다.

(2) 지문영상에 워터마크를 삽입한 경우의 특성분석 (Case 2)

그림 11에서는 커버 지문영상에 이진영상의 취급자정보를 워터마킹 알고리즘에 의해 삽입한 후의 특성을 나타냈다. 그림 11(a)에서는 JPEG 품질을 변화시키면서 취급자정보가 은닉된 지문영상에 대한 인식률을 나타냈다. 취급자정보는 1회, 2회 및 3회 반복적으로 삽입하였다. 그림 11(a)에서 보는 바와 같이 영상의 JPEG 품질(Quality)을 저하시키더라도 인식률의 저하는 초래하지 않았다. 또한, 그림 11(b)에 나타낸 추

출된 취급자 정보도 지문영상의 JPEG 품질이 저하되더라도 비트에러율의 감소는 크게 나타나지 않았다. 이는 얼굴영상에 취급자 정보를 삽입한 후 추출한 경우에 그림 5(b)에서 보는 바와 같이 JPEG 품질 저하에 따라 비트에러율이 급격히 증가한 결과와 비교되는 결과로서 지문영상에 취급자 정보를 삽입한 경우가 비트에러 측면에서는 우수한 것으로 분석된다.



(a) 워터마크 삽입에 따른 인식률 (b) 지문특징 추출 후의 인식률

그림 9. 얼굴영상에 지문특징 및 취급자정보를 은닉한 경우의 실험결과

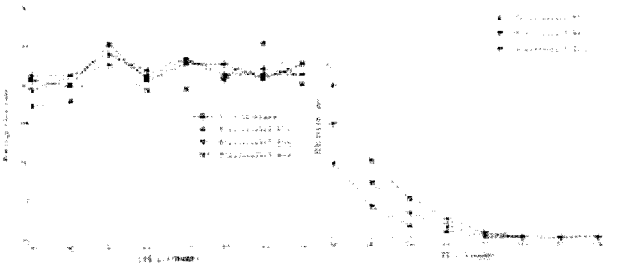
Fig. 9. Experimental results in case of hiding fingerprint feature and responsible person information in face image

그림 10. 취급자정보 2회 반복 은닉 후 추출한 결과 (JPEC 30)

Fig. 10 Result extracted of responsible person information (JPEG 30)

그림 13에서는 지문영상에 얼굴특징과 취급자정보를 동시에 은닉한 경우의 결과를 나타냈다. 이 때 은닉하고자 하는 정보인 얼굴의 특징은 1회 삽입하고, 취급자 정보는 1회와 2회 각각 삽입한 후 결과를 구하였다. 그림 13(a)에서는 두 가지 정보를 은닉한 지문영상에 대한 JPEG 품질 대비 인식률을 나타냈으며 그림 13(b)는 은닉 후 추출된 얼굴의 특징값을 이용한 인식률을 나타냈다. 그림 13의 결과를 보면, 앞의 그림 7에 결과와 같이 사용된 영상과 삽입된 얼굴특징 모두 JPEG 품질이 저하되더라도 약간의 인식률 저하는 발생하였지만, 전반적인 인식률의 변화는 적은 것으로 나타났다. 하지만 그림 14에서와 같이 추출된 이진영상의 취급자정보에 경우 앞의 Case 1에서의 그림 8보다 가시적으로 우수한 성능을 보이는 것을 확인할 수 있었다. 이는 이진영상의 취급자 정보의 경우 Case 1의 얼굴영상보다 Case 2의 지문영상에서 더 우수한 성능을 보이는 것을 나타낸다.

그림 15에서는 지문영상에 지문특징과 취급자정보를 동시에 은닉한 경우의 특성결과를 나타냈다. 이 때 은닉하고자 하는 정보인 지문의 특징은 1회 삽입하고, 취급자 정보는 1회와 2회 각각 삽입한 후 결과를 구하였다. 그림 15(a)에서는 두 가지 정보를 은닉한 얼굴영상에 대한 JPEG 품질 대비 인식률을 나타냈으며, 그림 15(b)는 은닉 후 추출된 지문의 특징값을 이용한 인식률을 나타냈다. 그림 15에 나타낸 두 가지의 은닉정보가 삽입된 얼굴영상에 대한 인식률을 살펴보면, 영상의 JPEG 품질이 저하되더라도 약간의 인식률 저하는 발생하였지만 전반적으로 인식률의 변화는 적은 것으로 나타났다. 지문특징을 얼굴영상에 은닉한 후 추출한 후 지문 인식률을 살펴본 결과 JPEG 품질이 저하되더라도 지문 인식률이 크게 감소하지는 않았다. 또한 그림 16에서와 같이 이진영상의 취급자 정보도 마찬가지로 JPEG 품질이 저하되더라도 비트에러율이 최대 4% 이내로 우수한 결과를 나타내었다.



(a) 취급자정보 삽입에 따른 인식률 (b) 취급자 정보 추출후의 비트 에러율

그림 11. 지문영상에 취급자정보를 은닉한 경우의 실험결과

Fig. 11. Experimental results in case of hiding responsible person information in fingerprint image

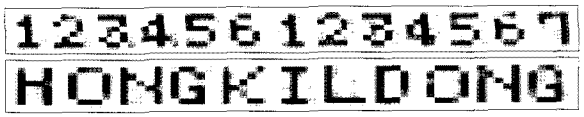
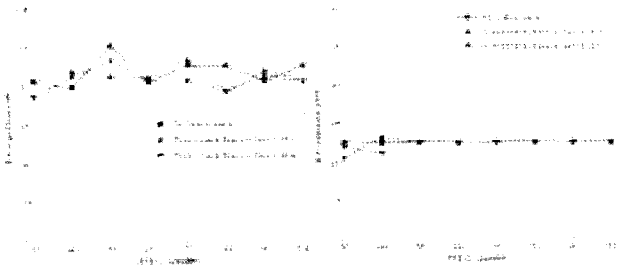


그림 12. 취급자정보 3회 반복 은닉 후 추출한 결과(JPEG 30)

Fig. 12 Result extracted of responsible person information (JPEG 30)



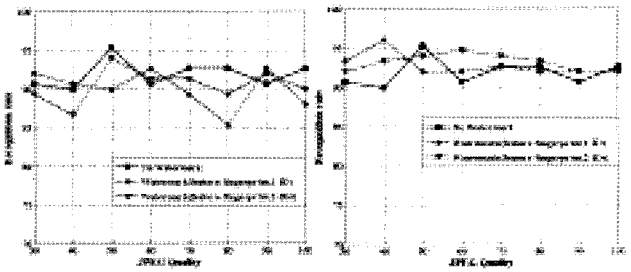
(a) 워터마크 삽입에 따른 인식률 (b) 얼굴특징 추출후의 인식률

그림 13. 지문영상에 얼굴특징 및 취급자정보를 은닉한 경우의 실험결과

Fig. 13. Experimental results in case of hiding face features and responsible person information in fingerprint image

그림 14. 취급자정보 2회 반복 은닉 후 추출한 결과(JPEG 30)

Fig. 14 Result extracted of responsible person information (JPEG 30)



(a) 워터마크 삽입에 따른 인식률 (b) 지문 특징 추출후의 인식률

그림 15. 지문영상에 지문특징 및 취급자정보를 은닉한 경우의 실험결과

Fig. 15. Experimental results in case of hiding fingerprint features and responsible person information in fingerprint image

그림 16. 취급자정보 2회 반복 은닉 후 추출한 결과(JPEG 30)

Fig. 16 Result extracted of responsible person information (JPEG 30)

(3) 인식률 실험 결과 분석

표 1에서는 커버영상의 선택에 따른 특성을 인식률의 관점에서 비교 및 분석한 결과를 나타내었다. 표 1에서 얼굴 특징값과 지문특징값은 1회, 그리고 취급자 정보인 ID는 2회 삽입하였을 경우를 기준으로 하였다. 워터마크 정도의 삽입 유무 및 JPEG 품질에 따른 원본영상의 특성을 살펴보면, 얼굴영상의 경우 취급자 정보인 ID, 얼굴특징과 지문특징 등의 워터마크 정보의 삽입에 상관없이 원본영상의 얼굴을 대상으로 한 인식률의 변화는 크게 나타나지 않았다. 또한 JPEG의 품질이 저하되더라도 원본영상의 인식률은 크게 낮아지지 않았다. 반면에, 워터마크정보가 삽입된 지문영상의 경우에는 JPEG 품질 저하가 발생하지 않은 경우 삽입 유무에 따라 지문 인식률의 저하는 크게 나타나지 않았다. 그러나 JPEG 품질저하가 발생한 경우 워터마크를 삽입하지 않더라도 지문인식률이 3% 저하되었으며, 워터마크가 삽입된 상태에서 지문영상의 JPEG 품질저하가 발생할 경우에는 지문 인식률이 5% 정도 저하되었다.

위 결과로부터 얼굴영상의 경우에는 JPEG 품질저하에 상대적으로 강인한 특성을 보이나 지문의 경우에는 JPEG 품질저하에 민감한 특성을 보임을 확인할 수 있다. 이는 얼굴영상의 경우 전체적인 얼굴영상의 정보를 이용하여 특징값을 계산하기 때문에 고조파 성분이 일부 제거되는 JPEG 품질저하가 발생되더라도 얼굴영상의 왜곡이 작고, 이는 퍼지 선형 판별분석기법에 의해 구해진 얼굴특징값에도 크게 영향을 미치지 못하는 것으로 해석할 수 있다. 그러나 지문의 경우 얼굴과 달리 국부적인 단점과 분기점의 위치와 각도를 특징으로 이용하기 때문에 JPEG 품질저하에 의해 국소적인 변화가 발생할 경우 지문의 특징값들이 민감하게 반응하게 때문에 지문영상이 얼굴영상에 비하여 JPEG에 의해 인식률이 저하된 것으로 해석할 수 있다.

다음으로, 취급자 정보인 ID와 얼굴특징값을 워터마크 정보로 삽입하고 추출한 결과를 살펴보고자 한다. 표 1에서 보는 바와 같이 얼굴영상 또는 지문영상 등의 원본영상의 종류에 상관없이 제안된 알고리즘에 의해 얼굴 특징값을 은닉하고 추출하였다 하더라도 얼굴인식률이 82[%]로 나타나 JPEG 품질저하와 커버영상의 종류에 상관없이 동일한 결과를 보였다. 그러나 ID와 지문특징값을 워터마크 정보로 은닉하고 추출한 결과는 얼굴특징의 결과와 상이하게 나타났다. 즉, JPEG 품질이 30일 경우 취급자정보를 포함하여 얼굴영상에 지문 특징값을 은닉 후에 추출하여 지문인식률을 구한 결과 40.67[%]로 나타났으며, 동일한 정보를 지문영상에 은닉한 후에 추출하여 지문인식률을 구한 결과 92.0[%]로 나타났다. 이러한 결과로부터 얼굴특징값을 어떤 종류의 생체정보에 삽입하든 큰 문제는 발생하지 않는 것으로 해석할 수 있다. 그러나 지문특징값인 경우에는 얼굴영상 보다는 지문영상에 삽입하는 것이 효과적인 것으로 해석된다. 이는 적용

표 1. 커버영상과 워터마크 정보의 삽입전과 후의 특성 분석

Table 1. Experimental results by proposed method

JPEG Quality	Watermark information	Cover image		Cover image					
				Face			Fingerprint		
				Extracted features			Extracted features		
		Face	Finger	face	fingerprint	ID	face	fingerprint	ID
100	No watermak	82.67	93.33	N/A	N/A	N/A	N/A	N/A	N/A
	ID	82.00	90.00	N/A	N/A	**0**	n/a	N/A	**0**
	ID+features(face)	82.67	90.67	**82.67**	N/A	**0**	**82.67**	N/A	**0**
	ID+features(finger)	82.00	91.00	N/A	**92.00**	**0**	N/A	**92.00**	**0**
30	No watermak	82.67	90.67	N/A	N/A	N/A	N/A	N/A	N/A
	ID	82.67	87.33	N/A	N/A	43.47	N/A	N/A	1.99
	ID+features(face)	82.00	88.67	82.00	N/A	14.16	82.00	N/A	3.64
	ID+features(finger)	82.67	89.33	N/A	40.67	16.74	N/A	92.00	4.08

된 워터마킹 알고리즘이 고조파 영역에 삽입하는 것이 강인한 특성을 보이기 때문에 저주파 영역이 대부분 존재하는 얼굴영상보다는 고조파 영역이 다수 존재하는 지문영상에 효과적인 것으로 해석할 수 있다.

마지막 분석으로, 취급자 정보의 은닉 전과 은닉후의 특성을 살펴보면 JPEG 품질저하가 발생하지 않을 경우 삽입전과 후의 비트에러율은 발생하지 않는다. 그러나 JPEG 30의 품질저하가 발생할 경우 얼굴영상에 취급자 정보를 삽입하고 추출할 경우 비트에러율을 약 13%이상으로 나타난 반면에 지문영상에 취급자 정보를 삽입하고 추출할 경우 비트에러율이 약 4% 이내로 이진 영상의 취급자 정보는 얼굴보다는 지문에 삽입하는 것이 효과적인 것으로 나타났다. 이는 사용된 워터마크 알고리즘이 고조파 성분에 우수한 효과를 나타내기 때문에 고조파 성분이 많은 지문영상이 고조파 영역이 적은 얼굴영상에 비해 취급자 정보의 비트에러율이 낮게 나타난 것으로 해석할 수 있다.

4. 결 론

본 논문에서는 워터마킹 기법을 적용한 생체정보 및 취급자 정보의 은닉 방법을 제시하였으며 다양한 실험을 통하여 제시된 방법의 유용성을 검증하였다. 분석결과를 요약하면, 워터마크가 삽입된 커버 영상의 인식률 측면에서는 지문영상보다는 얼굴영상이 효과적인 것으로 나타났다. 얼굴특징값을 은닉하는 경우, 얼굴영상 또는 지문영상 등의 커버영상에 상관없이 얼굴특징값을 이용한 얼굴 인식률의 저하는 발생하지 않았다. 그러나 지문특징값을 은닉하여 이용하는 경우에는 얼굴영상에 삽입하는 것보다 지문영상에 삽입하고 추출한 경우가 효과적인 것으로 나타났다. 마지막, 취급자정보 측면에서는 얼굴영상에 삽입하는 것보다 지문영상에 삽입하고 추출한 것이 효과적인 것으로 분석되었다. 생체인식에서의 개인정보 보호에 대한 사회적 수요가 늘어나고 있는 것을 감안하면 본 논문에서 제안된 방법이 다양한 응용분야에서 개인의 생체정보와 이를 적용한 취급자 정보를 효과적으로 은닉하고 추출할 수 있는 특성이 유용하게 적용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] 전명근, *생체인식(Biometrics)* 총론, 한국정보통신교육원, 2004.

[2] 전명근, "생체정보 이용과 프라이버시 보호," *정보보호학회논문지*, 15(6) 6, pp. 11-18, 2005.

[3] Anil K. Jain, Umut Uludag, "Hiding Biometric Data", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 25(11), pp. 1494-1498, 2003.

[4] C. P. Wu and C. C. J. Kuo, "Fragile Speech Watermarking for Content Integrity Verification", *IEEE International Symposium on Circuits and Systems(ISCAS)*, 2, pp. 436-439, 2002.

[5] C. Soutar, A. D. Roberge, A. Stoianov, R. Gilroy and B. V. K. Vijaya Kumar, *"Biometric Encryption"*, ICSA Guide to Cryptography, McGrow-Hill, 1999, (Available at http://www.bioscrypt.com/assets/ Biometric_Encryption.pdf).

[6] M. Vatsa, R. Singh, A. Noore, "Feature based RDWT watermarking for multimodal biometric system", *Image Vis. Comput.* Aceepted paper 2007. (Available online at www.sciencedirect.com)

[7] M. Faundez-Zanuy, M. Hagmuller, G. Kubin, "Speaker identification security improvement by means of speech watermarking", *Pattern Recognition*, 40, pp. 3027-3034, 2007.

[8] 한국정보보호진흥원, "생체 정보보호 가이드라인", 2006.

[9] 이욱재, 이대종, 문기영, 전명근, "웨이블렛을 이용한 생체정보의 강인한 워터마킹 알고리즘", *퍼지및지능시스템학회논문지*, 17(5), pp. 632-639, 2007.

[10] Keun-Chang Kwak, Witold Pedrycz "Face recognition using a fuzzy fisherface classifier", *Pattern recognition*, 38, pp. 1717-1732, 2005.

[11] Zhixin Shi, Venu Govindaraju, "A chaincode based scheme for fingerprint feature extraction", *Pattern Recognition Letters*, 27(5), pp. 462-468, 2006.

저 자 소 개

이욱재(Wook-Jae Lee)

2007년 : 충북대학교 전자공학과(학사)

2007년~현재 : 충북대학교 제어계측공학과 석사과정

관심분야 : 워터마킹, 생체정보보호, 임베디드 프로그래밍, 패턴인식

이대종(Dae Jong Lee)

1995년 : 충북대학교 전기공학과(학사)

1997년 : 충북대학교 전기공학과(공학석사)

2002년 : 충북대학교 전기공학과(공학박사)

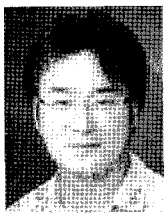
2004년~2005 : University of Alberta, Postdoc

2006년~현재 : 충북대학교 BK21 충북정보기술단 초빙조교수

관심분야 : 음성신호처리, 얼굴인식, 다중생체인식

박진일(Jin Il Park)
2001년 : 한밭대학교 제어계측공학과(학사)
2003년 : 한밭대학교 제어계측공학과 (공학석사)
2005년~현재 : 충북대학교 제어계측공학과 박사과정

관심분야 : 지능시스템, 다중생체인식, 퍼지이론
E-mail : moralskr@yahoo.co.kr



조재훈(Jae Hoon Cho)
2002년 : 한밭대학교 제어계측공학과(학사)
2004년 : 한밭대학교 제어계측공학과 (공학석사)
2005년~현재 : 충북대학교 제어계측공학과 박사과정

관심분야 : 지능시스템, 다중생체인식, 퍼지이론
E-mail : mmi8988@lycos.co.kr

전명근(Myung Geun Chun)
1987년 : 부산대학교 전자공학과(학사)
1989년 : KAIST 전기 및 전자공학과 (공학석사)
1993년 : KAIST 전기 및 전자공학과 (공학박사)
1993년~1996년 : 삼성전자 자동화연구소 선임연구원
2000년~2001년 : University of Alberta 방문교수
1996년~현재 : 충북대학교 전기전자컴퓨터공학부 교수
2008년~현재 : TTA PG505 부의장
2007년~현재 : ISO/IEC SC27 정보보호 표준화 전문위원

관심분야 : 바이오인식, 개인정보보호, 데이터마이닝, 지능시스템
이메일 : mgchun@chungbuk.ac.kr