워터마킹 기법을 이용한 다중생체정보의 안전한 은닉

Secure Hiding of Multimodal Biometric Information Using Watermarking Method

이욱재, 이대종, 전명근

충북 청주시 충북대학교 전기전자컴퓨터 공학부
E-mail: mgchun@chungbuk.ac.kr

요 약

본 논문에서는 얼굴, 홍채 등의 생체정보를 안전하게 은닉하고 효과적으로 은닉정보를 추출할 수 있는 웨이블렛 기반 워터마킹 기법을 제안한다. 얼굴과 홍채의 특징데이터는 Fuzzy-LDA(Fuzzy-Based Linear Discriminant Analysis)를 이용하여 추출하였다. 워터마킹알고리즘은 Wavelet을 이용하여 생체이미지에 생체특징 삽입 이전의 생체 인식율과 워터마킹알고리즘을 거쳐 생체특징을 추출한 후의 인식률 비교를 통해 성능을 평가하였다. 또한 단일생체특징 삽입과 다중생체특징삽입을 통해 단일생체보안과 다중생체보안의 실험을 수행, 평가하였다.

Key Words : Watermarking, Biometrics, Information Hiding, 다중생체인식

1. 서 론

생체인식기술은 인터넷 뱅킹, 금융서비스, 인터넷을 통한 중요한 자료에 대한 정보보호 등으로 이용되고 있으며, 현재는 온라인 활동이 많아져 사용자의 신원확인 여부가 중요한 문제로 등장하게 되었다. 이러한 신원확인에 있어 생체인식은 사용자가 기억하거나 소지할 필요가 없으며, 분실이나 도난의 문제가 전혀 없는 장점을 갖고 있어 높은 보안 성능을 제공한다[1].

생체인식기술은 꾸준한 발전을 이루고 있으며 국내에서도 다양한 생체인식시스템이 개발되어 상용화되고 있다. 이런 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.

기존의 워터마킹 관점에서는 생체의 정보가 아닌 디지털 컨텐츠 보호를 위한 2진화된 영상만을 사용함으로써 은닉될 정보의 양이 생체정보에 비해 극히 적으므로 다양한 방법들을 이용하여 우수한 성능을 보이는 기법들이 제안되어 적용되고 있다. 그러나 얼굴, 지문, 홍채 등의 생체 정보는 기존의 워터마킹기법에서 다루어진 워터마킹 데이터와는 큰 차이점을 보이고 있다. 우선적인 큰 차이점으로는 생체 정보의 양이라 할 수 있다. 즉, 기존의 워터마킹에서는 2진화된 적은 양의 데이터만을 다루지만 생체정보는 2진화된 값이 아닌 실수의 형태의 값을 취하므로 어떠한 방법을 가지고 실수값을 2진화 할 것인가에 대한 문제와 2진화 하였을 경우 매우 많은 정보를 은닉성이 극대화 되도록 할 것인가에 대한 문제가 선행 되어야 하며 이에 적합한 2진화과정과 워터마킹 알고리즘 개발이 중요하다[3].

따라서 본 논문에서는 얼굴과 홍채 등의 생체정보를 안전하게 은닉하고 효과적으로 은닉정보를 추출할 수 있는 Public Watermarking 기법을 제안한다. Public Watermarking 기법은 워터마크 추출 시 Cover Image를 사용하지 않는 기법으로 1-레벨 웨이블릿 변환을 통한 Reference Image를 통해 워터마크를 삽입하고 추출하는 기법이다.

은닉될 생체정보는 Fuyzzy-LDA에 기법에 의해 추출한 후, 워터마킹 삽입을 위해 생체특징값에 대해 이진화 과정을 수행한다. 생체정보의 삽입 및 추출은 웨이블렛 다해상도 기법에 의해 수행한다. 제안된 방법은 얼굴과 홍채 등의 인식 시스템에 적용하여 유용성을 평가한다.

2. 웨이블렛 이용한 생체정보의 은닉 및 추출 기법

본 논문에서 웨이블렛 다해상도 기법을 이용하여 생체정보를 안전하게 은닉하고 추출할 수 있는 기법을 제안한다. 제안된 방법은 그림 1과 같이 얼굴과 홍채로 구성된 다중생체인식시스템에 적용한다. 기존의 이진화된 워터마크 데이터 대신에 생체특징 데이터가 워터마크 데이터로서 은닉된다. 여기서, 얼굴 및 홍채에 대한 생체특징 데이터는 퍼지 선형판별분석기법에 의해 추출된다[4,5]. 그러나 선형 판별분석기법에 의해 산출된 데이터는 실수값으로 표현됨으로 워터마크 삽입을 위해 7비트로 이진화 과정을 수행한다. 이 때 이진화된 생체특징 데이터를 모두 사용할 경우 필요 이상의 비트수가 소요됨으로 식 (1)를 이용하여 소요 비트수를 감소시켰다. 식 (1)에서 N은 양의 정수를 의미한다. 그림 1은 bit를 줄이는 방법의 예이며 특징데이터 값을 변환하기 위한 bit 자리 정보 N은 워터마크 추출 후 Decimalization에서 사용된다.

$$N_{bit}=\begin{cases} N+1 \text{ if } N+1 \geq \dfrac{\log(|f(k)|)}{\log(2)} > N \\ N \quad \text{if } \dfrac{\log(|f(k)|)}{\log(2)} = N \end{cases} \tag{1}$$

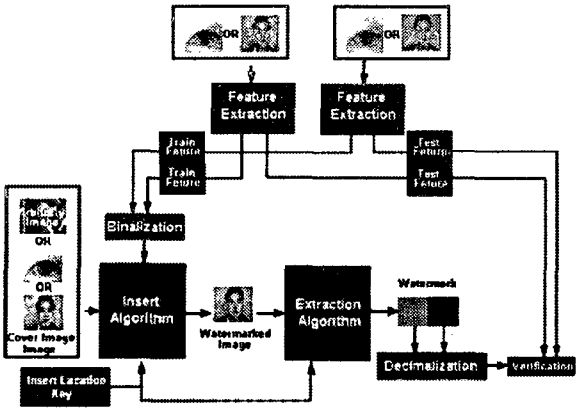

그림 1. 다중 생체정보보호를 위한 워터마킹 흐름도

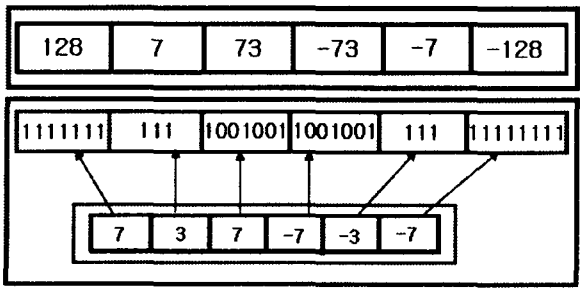

그림 2. 생체특징 데이터의 이진화 과정

그림 2에서 보는 바와 같이 이진화된 생체특징데이터를 웨이블렛 다해상도 기법을 이용하여 은닉 및 추출한다. 우선적으로 이진화된 생체데이터의 은닉방법을 단계별로 살펴보면 다음과 같다.

[단계 1] 그림 3에서 보는 바와 같이 1-레벨 웨이블렛을 이용하여 원본 영상에 대하여 대역별 웨이블렛 계수를 산출한 후, 저주파를 제외한 고주파에 해당하는 서브밴드영역인 HL1, LH1, HH1 영역의 계수를 0으로 대치한다.

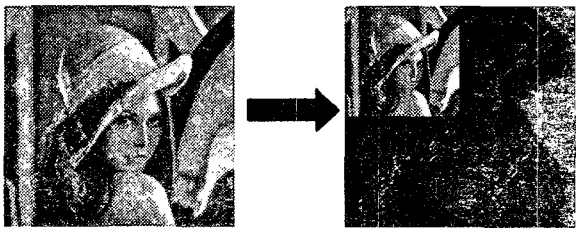

그림 3. Lena 영상의 1-레벨 웨이블릿 변환

[단계 2] 서브밴드 영역이 0으로 바뀐 웨이블릿 계수를 IDWT를 통해 기준영상 X_R을 얻는다. 그림 4에서는 원본영상과 기준영상을 나타냈다. 그림 4에서 보는 바와 같이 기준영상은 원본 영상에 비해 고주파성분이 사라져 약간의 스무딩 현상을 볼 수 있다.

(a) 원본 영상 (b) 기준 영상

그림 4. Lena 영상를 통한 원본영상과 기준영상

[단계 3] 원본영상 X와 기준 영상 X_R의 차이가 0인 경우, 양수인 경우, 음수인 경우의 3가지로 나누어 해당 픽셀 부분의 인덱스$idx(i,j)$를 얻는다.

네 번째 번째 단계로 식 (2)와 같이 워터마크 이미지를 Watermark 값에 따라 기준영상 X_R에 가중치 α를 더해 구한다. 식 (2)에서 가중치 α는 강인한 워터마킹과 시각적 무감지성과의 트레이드오프에 놓이게 된다.

$$x_w(idx(i,j))=\begin{cases} x_r(idx(i,j))+\alpha & \text{if } w(k)=1 \\ x_r(idx(i,j))-\alpha & \text{if } w(k)=-1 \end{cases} \tag{2}$$

생체데이터을 은닉하기 위한 워터마크 삽입 후, 복원을 위한 추출과정은 다음 단계를 통해 이루어진다.

[단계 1] 워터마크 삽입된 이미지 X_w를 워터마크 삽입과 같은 과정으로 웨이블렛 변환을 한 후, 고주파영역의 서브밴드인 HL1, LH1, HH1 영역의 계수를 0으로 모두 바꾼다.

[단계 2]두 번째 단계에서도 역시 삽입과정과 동일하게 변환된 웨이블릿계수를 IDWT를 통해 워터마크 삽입된 이미지의 기준 영상 $X'w$를 구한다.

[단계 3] 워터마크 삽입위치를 임의의 보안키 데이터로 사용한다는 가정에 따라 삽입 위치를 알고 있을 때 검출 된 워터마크 w'는 다음 식 (3)과 같이 구할 수 있다.

$$w'(k)=\begin{cases}1 & \text{if } x_w(idx(i,j)) \geq x'_w(idx(i,j)) \\ -1 & \text{if } x_w(idx(i,j)) < x'_w(idx(i,j))\end{cases} \quad (3)$$

앞서 설명된 얼굴과 홍채의 생체정보에 대해서 워터마크 삽입과 추출 알고리즘을 거쳐 워터마크 데이터로 얻어지며, 추출된 이진화된 워터마크 데이터는 십진수로 변환한 후, 개인정보가 저장된 학습데이터와 유사도 비교를 통해 스코어 값을 얻게 된다. 단일 생체인식데이터의 경우는 이렇게 계산된 매칭 스코어 값에 따른 인증을 거치며 다중생체인식의 경우는 두 생체데이터의 스코어 값의 가중치 합을 통하여 인증을 한다[6]. 가중치 합은 그림 5와 같이 설명 할 수 있으며, 워터마킹 추출에 의해 얻은 각각의 생체 특징데이터의 매칭값을 이용하여 Z-score에 의한 균등화 과정을 거쳐 매칭값이 높은 데이터에 약간의 가중치를 더 높게 주는 가중치 합을 통해 인식 성능을 구할 수 있다. 또한, 본 논문에서는 워터마크 삽입이전의 생체데이터의 인식률과 워터마크 추출후의 생체데이터의 인식률을 통하여 생체정보보호를 위한 워터마킹 기법의 성능을 평가한다.

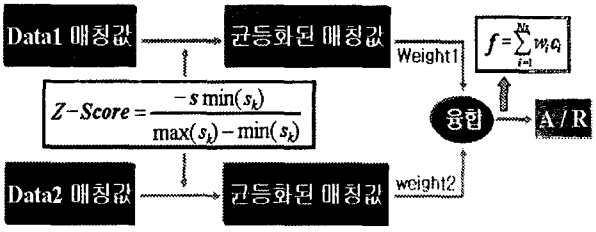

그림 5. 가중치 합에 의한 융합과정

3. 실험 및 결과

본 논문에서는 웨이블렛 다행상도 기법을 이용한 생체정보의 워터마킹 기법을 제안하였다. 제안된 방법의 유용성을 보이기 위해 얼굴과 홍채의 생체특징을 이용하였다. 실험은 개별 단일 생체인식시스템과 다중 생체인식시스템에 적용한다. 우선, 단일생체인식을 위한 워터마킹은 생체데이터의 특징 추출 및 추출된 생체데이터의 이진화, 워터마킹 삽입과 추출, 추출된 워터마킹의 실수화로 나눌 수 있으며, 실수화 된 워터마킹과 검증데이터 비교로 최종 인식률을 얻는 4단계로 구성되어 있다. 다중 생체인식을 위한 워터마킹에서는 단일 생체인식에서의 실험방법 외에 가중치합에 의한 융합부분이 추가되어 수행된다. 전체적인 실험은 다음 그림 6과 같이 설명할 수 있다. 그림 6에서 보는 바와 같이 단일 생체인식시스템의 경우 얼굴 영상에 홍채와 얼굴의 워터마크 데이터를 삽입 및 추출한 경우와 홍채영상에 홍채와 얼굴의 워터마크 데이터를 삽입 및 추출한 경우에 대하여 실험한다. 또한 다중생체 인식시스템의 경우에는 얼굴영상에 얼굴과 홍채 워터마크 데이터를 삽입 및 추출할 경우와 홍채 영상에 얼굴과 홍채의 워터마크 데이터를 삽입한 경우로 실험을 한다.

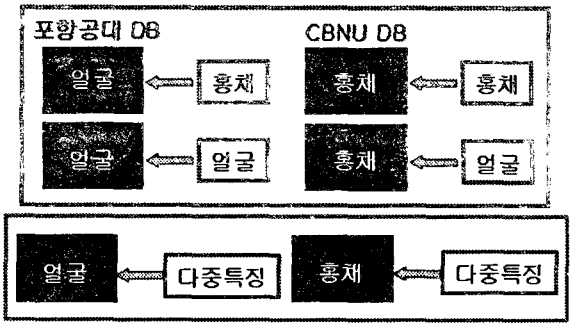

그림 6. 배경영상과 워터마크 데이터에 따른 실험

실험을 위해 사용된 생체 데이터로는 포항공대 얼굴DB와 CBNU 홍채 DB를 사용하였다. 이러한 얼굴과 홍채 데이터는 50명의 사람으로부터 취득하였으며, 동일한 사람에 대한 3장의 영상은 학습데이터로 사용하였고 나머지 3장은 검증데이터로 사용하였다.

표 1에서는 단일 및 다중생체인식의 결과를 나타냈다. 우선, 단일생체인식시스템의 실험결과를 살펴보면, 생체정보의 은닉기법을 사용하지 않은 홍채인식시스템은 인식률이 90%로 나타났다. 생체정보의 불법 유출을 방지하기 위해 제안된 워터마크 기법을 적용한 경우 얼굴영상에 홍채특징을 워터마크 삽입 및 추출한 경우 인식률이 90%, 홍채영상에 홍채특징을 삽입 및 추출한 경우 인식률이 90.67%로 나타나 워터마크를 적용하지 않은 경우와 인식률이 동일 또는 향상되어 나타났다. 얼굴인식시스템

의 경우에 은닉기법을 사용하지 않은 경우 인식률이 90%로 나타났다. 생체정보의 은닉을 적용한 얼굴인식 시스템은 얼굴영상에 얼굴특징을 삽입 및 추출한 경우 82.67%의 인식률은 나타냈으며, 홍채영상에 얼굴특징을 삽입한 경우에도 82.67%의 인식률을 나타냈다.

다중생체 인식시스템의 실험결과를 살펴보면, 얼굴영상을 사용한 경우와 홍채영상을 배경 영상으로 사용한 경우 모두 95.3%의 인식률을 나타내었고 워터마킹을 적용하지 않은 경우와 실험결과가 동일하게 나타났다. 이러한 결과로부터 제안된 방법은 단일 생체정보를 안전하게 은닉하면서도 동일한 인식률을 나타냄으로 생체정보의 은닉을 위한 효과적인 방법으로 제안된 방법을 적용할 수 있음을 알 수 있다.

그림 7에서는 얼굴영상에 홍채특징을 워터마크 삽입후의 PSNR을 나타냈다. 이 그림으로부터 얼굴영상에 워터마크 데이터를 삽입하더라도 PSNR이 작은 값을 나타냄으로 워터마크의 중요한 지표 중의 하나인 비가시성 측면에서도 효과적임을 확인할 수 있다.

표 2. 단일생체 워터마킹의 인식률

[%]

배경영상 / 은닉특징	얼굴영상	홍채영상	워터마크 적용 전
홍채인식	90.00%	90.67%	90.00%
얼굴인식	82.67%	82.67%	82.67%
다중생체인식	95.33%	95.33%	95.33%

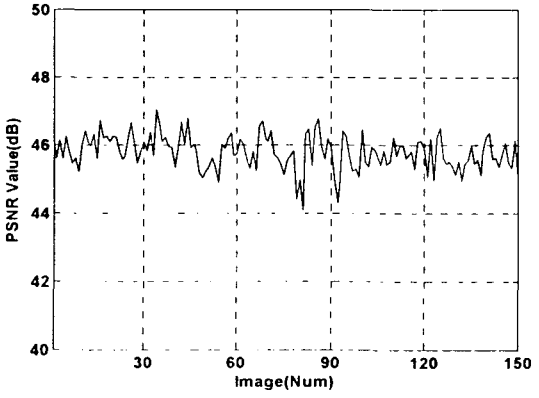

그림 7. 얼굴영상에 홍채 특징을 은닉한 경우 PSNR

5. 결 론

본 논문에서는 생체인식에 있어서 가장 취약점으로 나타날 수 있는 생체데이터의 유출에 대한 대책의 한 방법으로 워터마킹 기법을 이용한 생체정보 보호를 제안 하였다. 일반적인 디지털워터마킹기법과 달리 배경영상을 생체 데이터의 이미지를 사용하여 실험하였다. 제안된 방법을 얼굴과 홍채의 단일 생체인식시스템과 다중생체인식시스템에 적용하여 실험한 결과, 정보의 유출 가능성이 있는 은닉기법을 적용하지 않은 경우와 동일한 인식률을 나타내어 제안된 방법은 생체정보의 은닉을 위한 효과적인 방법인 것으로 나타났다. 또한, 배경영상에 생체정보를 은닉하더라도 워터마크의 중요한 지표 중의 하나인 비가시성 측면에서도 효과적임을 확인할 수 있다.

향후 연구과제로는 좀 더 강인한 워터마킹 알고리즘 개발과 디지털워터마킹에서 사용되는 워터마크와 달리 생체데이터는 데이터의 사이즈가 크므로 생체데이터의 특성이 변하지 않는 범위 내에서의 균등화와 압축을 위한 기법들이 연구 되어져야 하며, PDA와 같은 mobile 시스템에서의 생체데이터의 워터마킹 기법을 적용하여 생체데이터의 정보보호기법들이 이용되어지길 기대한다.

참 고 문 헌

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

[2] 전명근, "생체정보 이용과 프라이버시 보호," 정보보호학회, Vol. 15, No. 6, pp. 11-18, 2005.

[3] 김태해, 생체인식 시스템에 적합한 워터마킹 알고리즘에 관한 연구, 고려대학교, 전산학과 석사학위 논문, 2006.

[4] Keun-Chang Kwak, Witold Pedrycz, Hyoun-Joo Go, Myung-Geun Chun, "Fuzzy Aggregation Method Using Fisherface and Wavelet Decomposition for Face Recognition," Journal of Advanced computatinal Intelligence and Intelligent Informatics, Vol. 8, No.4, 2004.

[5] J. M. Keller, M. R. Gray, J. A. Givens, "A fuzzy k-nearest neighbor algorithm," IEEE Trans. on Systems, Man, and Cybernetics, Vol. 15, No. 4, 580-585, 1985.

[6] 유병진, 고현주, 이대종, 전명근, "다중생체 시스템에 기반한 스테가노그래피," Proc. of KFIS Spring Conf., Vol. 16, No. 1, 2006.