

웨이블릿을 이용한 생체정보의 강인한 워터마킹 알고리즘

A Robust Watermarking Algorithm using Wavelet for Biometric Information

이욱재* · 이대종** · 문기영*** · +전명근*

Wook-Jae Lee*, Dae-Jong Lee**, Ki-Young Moon***, +Myung-Geun Chun*

* 충북대학교 전기전자컴퓨터공학부

** 충북대학교 BK21 충북정보기술사업단

*** 한국전자통신연구원 정보보호연구단 바이오인식기술 연구팀

요 약

본 논문에서는 얼굴, 지문 등의 생체특징을 안전하게 은닉하고 효과적으로 은닉정보를 추출할 수 있는 웨이블릿 기반 워터마킹 기법을 제안한다. 제안된 방법은 웨이블릿을 이용하여 워터마크 삽입위치를 결정하고 배경영상의 특성을 고려한 적응적 가중치설정방법에 의해 워터마크를 효과적으로 은닉하였다. 은닉된 워터마크 데이터는 워터마크가 삽입된 영상에 웨이블릿 역변환을 적용하여 효과적으로 생체특징을 추출한다. 제안된 방법의 타당성을 검증하기 위하여 워터마크 데이터인 생체특징의 은닉 전과 후의 특성분석과 워터마크 알고리즘이 생체 인식시스템에 미치는 영향을 평가하였다. 워터마킹 알고리즘을 적용하여 얼굴과 지문으로 구성된 다중생체 인식실험을 한 결과 인식이 98.67%로 나타났다. 이로부터 제안된 방법은 효과적으로 생체정보를 은닉하고 생체인식률의 저하 없이 효과적으로 생체정보를 보호할 수 있음을 확인할 수 있었다.

키워드 : 워터마킹, 생체정보, 웨이블릿

Abstract

This paper presents a wavelet-based watermarking algorithm to securely hide biometric features such as face and fingerprint and effectively extract them with less distortion of the concealed data. To hide the biometric features, we proposed a determination method of insert location based on wavelet transform and adaptive weight method according to the image characteristics. The hidden features are effectively extracted by applying the inverse wavelet transform to the watermarked image. To show the effectiveness, we analyze the various performance such as PSNR and correlation of watermark features before and after applying watermarking. Also, we evaluate the effect of watermarking algorithm with respect to biometric system such as recognition rate. Recognition rate shows 98.67% for multimodal biometric systems consisted of face and fingerprint. From these, we confirm that the proposed method makes it possible to effectively hide and extract the biometric features without lowering recognition rate.

Key Words : Watermarking, Biometric information, Wavelet

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[2][3].

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[4]. 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 분야의 선두주자인 Jain 등은 지문 영상에 얼굴정보를 삽입할 수 있는 지문 영상 워터

접수일자 : 2007년 7월 30일
완료일자 : 2007년 10월 10일
감사의 글 : 이 논문은 2007년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었음
+ : 교신저자

마킹기법을 제시하였다[5]. 이 기법은 얼굴의 특징인 고유 얼굴을 지문 영상에 워터마크로써 삽입한 후, 복원된 얼굴 영상은 얼굴 확인에 이용될 수 있음을 제안하였으나, 시스템 차원에서의 얼굴인증은 시도하지 않았다. 또한, 워터마킹에 따른 지문 영상과 지문 특징의 변형정도를 실험결과로 제시하였으나, 지문 및 복원된 얼굴 인식에 대한 실험은 제시되지 않았다. 이 외에도 Wu와 Kuo는 음성신호의 무결성을 보장하는 워터마킹 기법을 제안하였고, Soutar은 생체데이터를 이용하여 디지털 키를 연결하고 가져오는 생체암호화 기법을 제안하였다[6][7].

그러나 앞서 설명한 연구방법들은 일반적인 디지털 워터마킹에서 사용되는 방법과 동일하게 이진화된 생체정보의 은닉 및 추출방법에 주안점을 두고 있다. 일반적인 디지털 워터마킹 관점에서는 생체의 정보가 아닌 디지털 콘텐츠 보호를 위한 이진화된 영상만을 사용함으로써 은닉될 정보의 양이 생체 정보에 비해 극히 적으므로 다양한 방법들을 이용하여 우수한 성능을 보이는 기법들이 제안되어 적용되고 있다[4][8]. 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 이진화된 값이 아닌 실수의 형태의 값을 취하므로 어떠한 방법을 가지고 실수값을 이진화 할 것인가에 대한 문제와 이진화 하였을 경우 매우 많은 정보를 은닉성이 극대화 되도록 할 것인가에 대한 문제가 선행되어야 하며 이에 적합한 이진화과정과 워터마킹 알고리즘 개발이 중요하다[9].

본 논문에서는 웨이블릿 다해상도 기법을 이용한 생체정보의 안전한 은닉 및 복원기법을 제안한다. 제안된 방법은 생체정보가 아닌 이진화 영상에 대하여 Liu 등이 제안한 워터마킹 방법을 생체정보에 적용함과 동시에 생체정보의 은닉 및 복원에 효과적이도록 워터마킹 방법을 개선하였다. 또한 많은 양의 생체정보는 생체인식시스템의 성능 저하를 일으킴으로 본 논문에서 은닉할 생체정보의 양을 효과적으로 줄일 수 있는 가변 비트형 생체정보 이진화 과정 및 전송기법을 제안한다. 제안된 방법은 얼굴 인식 시스템과 지문 인식 시스템의 단일 생체 인식 시스템에 적용하여 유용성을 평가한다.

2. 웨이블릿을 이용한 생체정보의 은닉 및 복원 기술

웨이블릿을 이용하여 정보를 은닉하는 방법 중에서 본 논문에서는 이진영상의 은닉 및 복원을 위한 워터마킹 기법을 제안한 Liu 방법을 개선하여 생체정보의 은닉 및 복원을 위한 워터마킹 기법을 제안한다[10]-[12]. 그림 1에서는 Liu 등이 제안한 워터마킹 기법을 나타냈다. 그림 1에서 나타낸 Liu의 방법을 단계별로 살펴보면 다음과 같다.

[단계 1] 원영상(X)를 1-레벨 웨이블릿 변환한다.

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

[단계 3] 고주파부분을 제거한 값을 웨이블릿 역변환을 하여 기준영상(X')를 만든다.

[단계 4] 원영상(X)과 기준영상(X')간의 차를 계산한다.

[단계 5] 임의로 결정된 삽입위치에 아래와 같은 식 (1)을 이용해 워터마크를 삽입하게 되며, 가중치 α는 다음 식 (2)에 따라 결정된다.

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

$$\alpha = \text{round}[(s+t)/2] \quad (2)$$

식 (1)에서 은닉하고자 하는 워터마크값인 W는 다음과 같다.

$$W = \{w(k) \mid 1 \leq k \leq n, w(k) \in \{1, -1\}\} \quad (3)$$

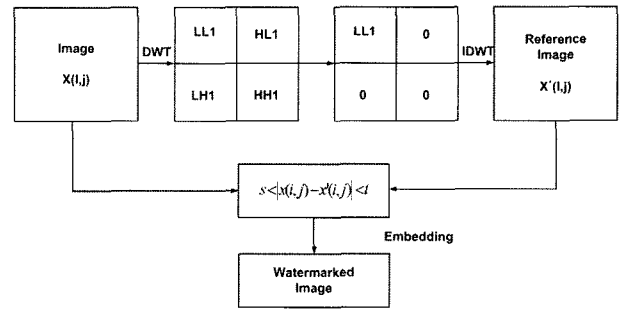


그림 1. Liu에 의해 제안된 워터마크 삽입과정
Fig. 1. Watermark embedding process by Liu et al.

그림 1에 나타낸 Liu의 방법을 생체정보의 은닉 및 복원에 적용하기 위해서는 몇 가지 고려사항이 존재한다. 우선적으로 생체정보는 이진영상이 아닌 실수형의 데이터 형태임으로 은닉을 위해서는 -1과 1의 값을 갖도록 하는 이진화과정이 수행된다. 이를 위해 본 논문에서는 실수형의 값을 갖는 생체정보를 T 비트로 양자화하여 이진화된 생체데이터를 산출하였다. 그러나 모든 생체정보의 값을 T 비트로 고정할 경우 은닉하여야 이진 생체 데이터의 양이 많아지고 이는 은닉해야 할 정보의 양이 많은 것과 동일함으로 복원율에도 악영향을 미친다. 따라서 본 논문에서는 생체정보의 크기에 맞는 가변 비트형 생체정보 이진화 과정을 제안한다. 제안된 이진화 과정을 그림 2에 나타냈다. 그림 2에서 보는 바와 같이 생체 정보를 7비트로 양자화한 경우 최상위비트가 0이 아닌 값을 최대 비트로 가정하여 생체정보의 크기에 따라서 양자화할 비트의 값을 가변시켰다. 이 때 이진화된 생체 데이터의 비트정보를 나타내는 최대 자리수는 나중에 생체 인증을 위해 이진화된 영상을 실수형으로 변환할 때 중요한 인증키로서 작용한다. 실수형의 생체 데이터에 대하여 필요한 비트 자리정보 N_{bit} 는 식 (4)에 의해 구해진다. 식 (4)에서 $f(k)$ 는 정규화된 생체 데이터의 값을 나타내고, N은 양의 정수를 나타낸다.

$$N_{bit} = \begin{cases} N+1 & \text{if } N+1 \geq \frac{\log(|f(k)|)}{\log(2)} > N \\ N & \text{if } \frac{\log(|f(k)|)}{\log(2)} = N \end{cases} \quad (4)$$

또한, 본 논문에서는 워터마크 삽입에 가중치값을 나타내는 α 값을 원영상과 기준영상과의 차이특성을 이용하여 적응적으로 설정하였다. 즉, Liu 등은 식 (1)에서 보는 바와 같이 주어진 조건을 만족하는 픽셀 정보에 대해 원영상과 기준영상과의 차이를 이용하여 고정된 α 값을 설정하였다. 그러나 일반적으로 원영상과 기준영상과의 차이가 큰 경우에는 가중치 값을 작게 설정해도 복원

율에는 영향을 미치지 않는다. 이와 반대로 원영상과 기준영상과의 차이가 작은 경우에는 상대적으로 큰 가중치값을 부여하는 것이 복원에는 효과적이다. 따라서 본 논문에서는 원영상과 기준영상과의 차이 특성을 이용하여 적응적으로 가중치를 부여하는 방법을 적용한다. 즉, 제안된 방법은 원영상과 기준영상과의 차이에 반비례하도록 식 (5)와 같이 적응적인 가중치값을 설정하였다.

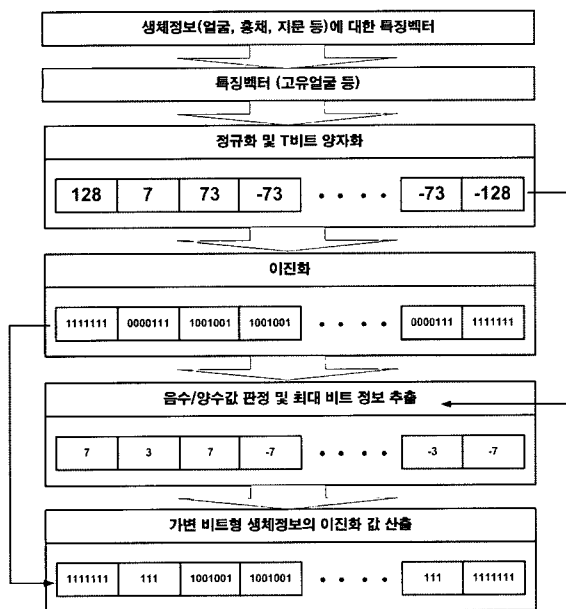


그림 2. 가변 비트형 생체정보의 이진화 값 산출 과정
Fig. 2. Binalization process for biometric information with variable length

또한, 본 논문에서는 워터마크 삽입에 가중치값을 나타내는 α 값을 원영상과 기준영상과의 차이특성을 이용하여 적응적으로 설정하였다. 즉, Liu 등은 식 (1)에서 보는 바와 같이 주어진 조건을 만족하는 픽셀 정보에 대해 원영상과 기준영상과의 차이를 이용하여 고정된 α 값을 설정하였다. 그러나 일반적으로 원영상과 기준영상과의 차이가 큰 경우에는 가중치 값을 작게 설정해도 복원율에는 영향을 미치지 않는다. 이와 반대로 원영상과 기준영상과의 차이가 작은 경우에는 상대적으로 큰 가중치 값을 부여하는 것이 복원에는 효과적이다. 따라서 본 논문에서는 원영상과 기준영상과의 차이 특성을 이용하여 적응적으로 가중치를 부여하는 방법을 적용한다. 즉, 제안된 방법은 원영상과 기준영상과의 차이에 반비례하도록 식 (5)와 같이 적응적인 가중치값 α_1 을 설정하였다.

$$\alpha_1 = f(x, a, c) = \frac{\alpha}{1 + e^{-a(x-c)}} \quad (5)$$

Liu의 연구와 본 논문에서 제안한 방법의 마지막 차이점으로서 워터마크 데이터를 삽입하는 영상의 선택문제에 있

다. 일반적인 이진영상에 대한 워터마킹 기법을 제안한 Liu 등은 은닉하고자 하는 워터마크 데이터에 중점을 가질 뿐 원영상을 이용하지는 않는다. 그러나 본 논문에서는 워터마크가 삽입된 영상정보를 이용하여 생체 인증 시스템을 구축한다. 이런 경우 고주파가 제거된 저주파 정보만을 이용하여 생체 인식 시스템을 구축할 경우 인식률이 떨어지는 문제점이 있다. 따라서 본 논문에서는 기준영상에 워터마크를 삽입한 Liu의 방법과 달리 원영상에 워터마크 데이터를 삽입하였다.

워터마킹 삽입 후에 은닉된 워터마크 데이터 추출과정은 Liu의 방법을 적용하였으며, 복원과정을 단계별로 살펴보면 다음과 같다.

- [단계 1] 워터마크된 이미지(X_w)를 1-레벨 웨이블릿 변환한다.
- [단계 2] 고주파부분의 서브밴드(LH₁, HL₁, HH₁)계수를 0으로 바꾼다.
- [단계 3] 고주파부분을 제거한 값을 웨이블릿 역변환을 하여 기준영상(X')을 만든다.
- [단계 4] 원영상(X)과 기준영상(X')간의 차를 계산한다.
- [단계 5] 전달받은 Key와 아래 식 (6)을 이용해 워터마크 데이터를 추출한다.

$$w'(k) = \begin{cases} 1 & \text{if } X_w(idx(i,j)) \geq X_w'(idx(i,j)) \\ -1 & \text{if } X_w(idx(i,j)) < X_w'(idx(i,j)) \end{cases} \quad (6)$$

3. 워터마킹 기법을 이용한 다중 생체 인식 시스템 구현

그림 3에서는 워터마킹 기법을 이용한 다중 생체 인식 시스템을 구성도를 나타냈다. 그림 3에서 보는 바와 같이 본 논문에서는 원영상으로 얼굴, 지문의 생체정보를 고려하였다. 또한, 은닉하고자 하는 생체정보로서는 다른 생체정보에 비해 유출 가능성이 가장 높은 지문 영상을 고려하였다. 은닉하고자 하는 지문 영상은 특징 추출 기법에 의해 산출된 실수형의 특징값을 이용하여 이진화 과정을 수행한 후, 웨이블릿 기반 삽입 알고리즘을 통하여 지문 정보를 담고 있는 워터마크가 삽입된 생체 영상을 얻는다. 워터마크 추출과정에서는 웨이블릿 기반 삽입 알고리즘을 통하여 이진값을 갖는 워터마크 데이터를 추출한 후 생체 인증을 위하여 십진수의 값을 갖도록 십진화 과정을 수행한다.

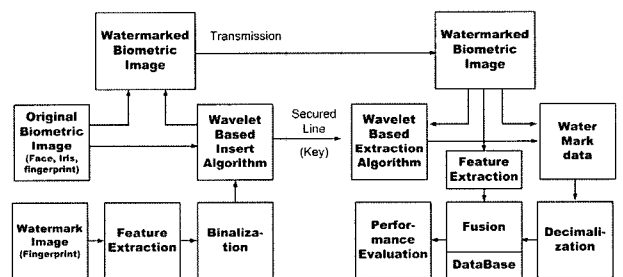


그림 3. 워터마킹 기법을 이용한 다중생체 인식시스템
Fig. 3. Multi-modal biometric system using watermarking algorithm

추출과정에서는 비밀전송망을 통하여 전송된 워터마크 삽입위치정보 및 최대정보 비트 정보를 이용한다. 다중생체 인식시스템은 워터마크가 삽입된 생체 영상과 워터마크가 삽입된 지문 영상을 이용한 융합기법 중 가중치합 방법을 적용하여 최종 인증을 수행한다.

본 논문에서는 은닉하고자 하는 생체특징을 추출하기 위해 알고리즘의 타당성이 검증된 방법을 사용하였다. 즉, 얼굴인 경우에는 Fuzzy LDA 기법을 이용하였고, 지문의 경우에는 체인코드 컨투어기법을 적용하였다. 적용된 방법을 간단히 설명하면 다음과 같다.

3.1 Fuzzy LDA를 이용한 얼굴의 특징 추출

얼굴의 특징을 추출하기 위해 본 논문에서 적용된 Fuzzy LDA 알고리즘은 주성분분석기법(PCA : Principal Component Analysis)에 의해 얼굴 영상의 입력차원을 축소 한 후, 축소된 특징벡터와 퍼지소속도 함수를 이용하여 산출한다[13]. Fuzzy LDA 알고리즘 설명을 해 하나의 얼굴 영상이 각각의 화소 값을 갖는 2차원 배열($n \times n$)이라고 가정하자. 영상 z_i 는 연속적인 행들의 연결로 $n^2 \times 1$ 의 벡터로서 고려된다. 그러면 N 개 얼굴 영상의 학습 집합은 $Z = (z_1, z_2, \dots, z_N)$ 로 표시된다. 우선, 주성분 분석기법에 의한 축소된 얼굴의 특징값을 구하기 위한 공분산 행렬을 정의하면 다음과 같다.

$$R = \frac{1}{N} \sum_{i=1}^N (z_i - \bar{z})(z_i - \bar{z})^T = \Phi\Phi^T \quad (7)$$

$$\bar{z} = \frac{1}{N} \sum_{i=1}^N z_i \quad (8)$$

그러면, 공분산 행렬의 고유치와 고유벡터가 계산된다. 여기서 r 개의 가장 큰 고유치에 대응하는 r 개의 고유벡터를 $E = (e_1, e_2, \dots, e_r)$ 라 하자. 얼굴 영상의 집합 Z 에 대해서, 그것들의 대응되는 특징벡터 $X = (x_1, x_2, \dots, x_N)$ 는 다음과 같이 Z 를 PCA-변환된 공간으로 투영함으로써 얻어진다.

$$x_i = E^T(z_i - \bar{z}) \quad (9)$$

여기서 x_i 는 i 번째 $r \times 1$ 벡터이다.

퍼지 LDA는 축소된 특징벡터와 퍼지 소속도각각의 클래스의 평균값을 식 (10)과 같이 특징벡터와 퍼지소속도를 이용하여 산출한다.

$$\hat{m}_i = \frac{\sum_{j=1}^N \mu_{ij} x_j}{\sum_{j=1}^N \mu_{ij}} \quad (10)$$

여기서 μ_{ij} 는 j 번째 레벨된 샘플 집합의 i 번째 클래스의 소속도이다. 위의 결과를 이용하여 퍼지 클래스간 분산행렬 S_{FB} 와 퍼지 클래스내 분산 행렬 S_{FW} 는 각각 다음과 같이 정의한다.

$$S_{FB} = \sum_{i=1}^c N_i (\hat{m}_i - \bar{m})(\hat{m}_i - \bar{m})^T \quad (11)$$

$$S_{FW} = \sum_{i=1}^c \sum_{x_k \in C_i} (x_k - \hat{m}_i)(x_k - \hat{m}_i)^T = \sum_{i=1}^c S_{FW_i} \quad (12)$$

위 식에서, 여기서, N_i 는 i 번째 클래스 C_i 에서의 벡터의 수이고, \bar{m} 은 모든 특징벡터들의 평균값을 나타낸다. 최종적으로 최적의 퍼지 투영행렬 W_{F-FLD} 와 퍼지 LDA 방법에 의해 투영된 특징벡터는 각각 다음과 같이 계산된다.

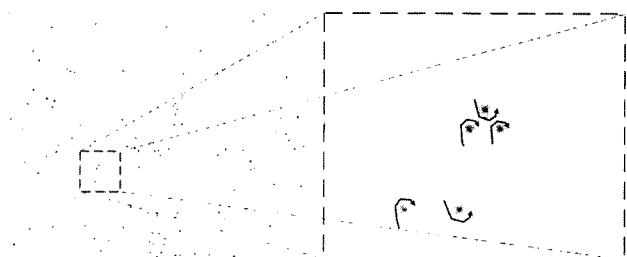
$$W_{F-FLD} = \arg \max_w \frac{|W^T S_{FB} W|}{|W^T S_{FW} W|} \quad (13)$$

$$\hat{v}_i = W_{F-FLD}^T x_i = W_{F-FLD}^T E^T (z_i - \bar{z}) \quad (14)$$

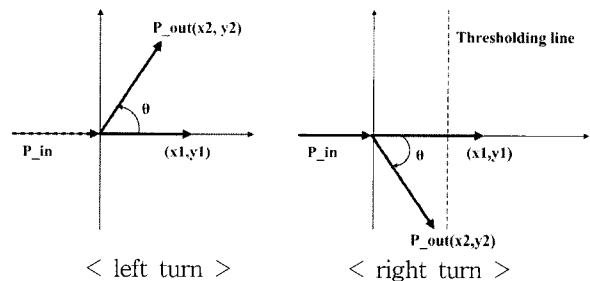
훈련영상과 검증영상에 대하여 퍼지 LDA를 이용하여 얼굴 영상의 특징을 추출한 후, 최종 인식단계에서는 훈련영상과 검증영상간의 유클리디안 거리를 측정하여 분류한다.

3.2 체인코드 컨투어기법을 이용한 지문의 특징추출

본 논문에서는 지문의 특징을 추출하기 위하여 지문의 변화와 회전에 강인한 것으로 나타난 체인코드 컨투어 기법을 적용하였다. 체인코드는 물체의 윤곽선에 대한 표현 방법으로서 Shi 등은 지문의 윤곽선을 이용하여 지문의 특징을 추출하였다[14]. 즉, 그림 4(a)에서 보는 바와 같이 지문의 경우 단점(ridge ending) 분기점(ridge bifurcation)에서는 급격한 지문의 변화(회전)이 발생한다. 이러한 지문 윤곽성의 특성을 이용하여 그림 4(b)에서 보는 좌회전(left turn)과 우회전(right turn)으로 정의되는 특징정보를 취득한다. 이러한 좌회전 또는 우회전 모양을 검출하기 위해 방향변화의 중요적도를 나타내는 θ 를 식 (15)와 같이 정의한다.



(a) Minutia location in chaincode contours



(b) To calculate the significant turns

그림 4. 체인코드를 이용한 지문특징 추출

Fig. 4. Fingerprint feature extraction based on chaincode contours

$$\theta = \arccos \frac{P_{\in} \cdot P_{out}}{|P_{\in}| |P_{out}|} \quad (15)$$

식 (15)에서 $P_{\in} = (x_1, y_1)$ 이고 $P_{out} = (x_2, y_2)$ 임으로 식 (15)는 식 (16)과 같이 표현된다.

$$\theta = \arccos(x_1y_1 + x_2y_2) \quad (16)$$

다음 단계로 $(x_1y_1 + x_2y_2) < T$ 를 만족하는 임계값 T 를 선택한 후, 방향 결정은 $\sin\theta (= x_1y_2 - x_2y_1)$ 의 부호에 의해 양의 값을 갖는다면 좌회전 모양으로 결정하고 음의 값을 갖는다면 우회전 모양으로 결정하게 된다. 최종적으로는 좌회전 모양 또는 우회전 모양으로 결정된 영역에 대한 (x축, y축 및 각도(θ))로 표현되는 지문의 특징을 추출하게 된다.

지문의 특징점이 추출된 후에 K-plet 방법을 이용하여 특징점을 재 표현한다. 여기서, K-plet 방법은 절대 좌표계가 아닌 지역좌표계로 표현함으로 지문의 변형과 회전에 강인한 장점을 나타낸다. 최종 단계에서는 Coupled -BFS(Breadth First Algorithm)알고리즘을 이용하여 훈련지문과 검증 지문간의 유사성 s 를 식 (17)에 의해 산출한 후 지문 인식을 한다[15][16]. 식 (17)에서 m 은 일치된 특징점의 수, M_R 은 훈련 지문에 대한 특징점의 수, M_T 은 검증 지문의 특징점의 수를 각각 의미한다.

$$s = \frac{m^2}{M_R M_T} \quad (17)$$

4. 실험 및 결과

4.1 제안된 워터마크 알고리즘의 성능평가

제안된 워터마크 알고리즘의 성능을 평가하기 위하여 포항공대에서 제작한 얼굴 DB와 충북대에서 제작한 지문 DB를 사용하였다. 얼굴 DB는 서로 다른 환경에서 50명으로부터 한 사람당 6개의 얼굴을 취득하여 총 300개의 얼굴 영상으로 구성되어 있다. 각각의 얼굴 영상들은 0에서 255까지 그레이 값을 가진 256×256 영상 크기에 의해 나타내어진다. 지문 DB인 경우에도 서로 다른 환경에서 50명으로부터 한 사람당 300×300 의 크기를 갖는 6개의 지문을 취득하여 총 300개의 지문 영상으로 구성되어 있다. 그림 5에서는 지문 영상의 일부를 나타냈다.

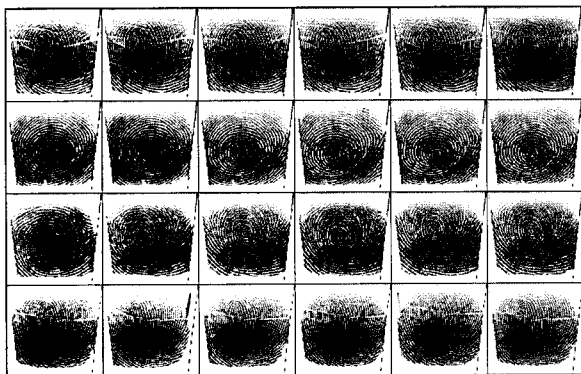


그림 5. 지문이미지

Fig. 5. Sample fingerprint images

제안된 워터마크 알고리즘의 성능을 평가하기 위한 실험 방법은 다음과 같이 네 경우를 고려한다.

- Case 1) 얼굴영상에 얼굴 특징값을 은닉한 경우
- Case 2) 얼굴영상에 지문 특징값을 은닉한 경우
- Case 3) 지문영상에 얼굴 특징값을 은닉한 경우
- Case 4) 지문영상에 지문 특징값을 은닉한 경우

워터마크 데이터를 은닉하는데 사용한 원영상은, 얼굴 영상과 지문 영상 모두 한 사람당 취득한 6장의 영상 중에서 3장은 워터마크 은닉하는데 사용한 원영상으로 사용하였고, 나머지 3장은 은닉 데이터인 워터마크 데이터로서 사용하였다. 따라서 워터마크 삽입 및 추출후의 평가를 위해 사용된 데이터는 네 경우 모두 총 150장 (3장×50명)이 사용된다. 은닉할 워터마크 데이터를 산출하기 위하여 PCA와 퍼지 LDA를 이용하여 41개의 실수값을 갖는 얼굴특징을 추출하였고, 지문은 체인코드 쿼터어 기법을 이용하여 실수값을 갖는 지문 특징을 추출하였다. 추출된 특징값들은 각각 본 논문에서 제안된 가변 비트형 생체정보 이진화과정을 수행한 후, 워터마크 알고리즘을 적용하여 은닉한다.

본 논문에서 제안된 워터마크 알고리즘은 2장에서 살펴본 바와 같이 원영상과 기준영상간의 차를 이용하여 워터마크 삽입위치를 탐색한 후, 1과 -1로 구성된 워터마크 데이터에 복원 성능을 향상시키기 위하여 가중치값을 더하여 은닉한다. 그림 6에서는 지문 영상에 지문 특징값을 은닉한 경우 원영상과 기준영상간의 절대값 차이와 가중치값에 의해서 에러가 발생된 비트의 평균값을 나타냈다.

그림 6에서 보는 바와 같이 원영상과 기준영상간의 절대값 차이가 크고, 가중치값이 크게 발생 할수록 에러가 발생된 비트의 수는 감소함을 알 수 있다. 그러나 에러를 감소시키기 위하여 가중치를 크게 설정할 경우 워터마크의 중요 성능지표인 비가시성이 저하되는 문제점이 발생한다. 따라서 본 논문에서는 본 논문에서는 기존 연구에서 제안된 일정한 값을 부여하는 가중치 방법 대신에 영상의 특성을 고려한 적응적 가중치 부여 방법을 제안한다. 제안된 방법은 원영상과 기준영상과의 차이가 크게 발생하는 삽입 영역은 가중치값을 적게 부여하고, 차이가 작게 발생하는 삽입 영역은 가중치값을 크게 부여하는 방법으로 설명할 수 있다.

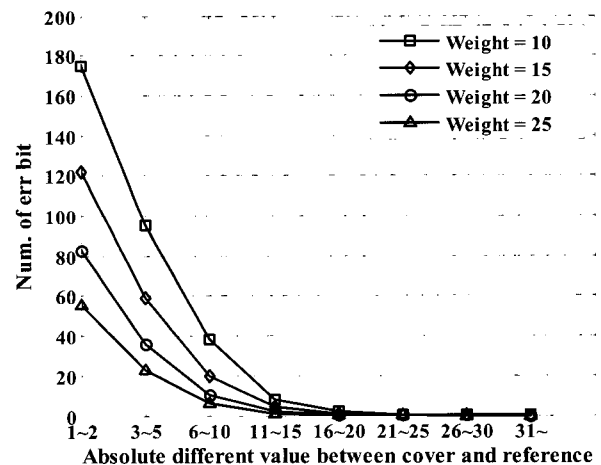


그림 6. 절대값 차이와 가중치 값에 따른 에러비트의 평균값
Fig. 6. The number of error bit according to difference and weight

그림 7에서는 가중치 부여 방법에 따른 평균 PSNR과 오차 비트의 평균수를 나타냈다. 그림 7의 (a)에서는 얼굴 특징값이 삽입된 얼굴 영상에 대한 PSNR과 얼굴 특징값 삽입 전과 삽입후의 값이 상이한 비트의 수를 나타냈다. 그림 7(a)에서 보는 바와 같이 얼굴 특징값이 삽입된 얼굴 영상의 경우 PSNR과 오차비트의 수는 큰 차이를 나타내지는 않았다. 그러나 그림 7(b)에서 보는 바와 같이 지문 특징값이 삽입된 얼굴 영상의 경우에는 적응적 가중치 방법을 적용한 방법이 기존 방법에 비하여 우수한 것으로 나타났다.

그림 7(c)와 (d)는 얼굴특징값을 지문 영상에 삽입한 경우와 지문 특징값을 지문 영상에 삽입한 경우 가중치 부여방법에 따른 PSNR과 오차비트의 수를 각각 나타냈다. 그림 7(c)와 (d)에서 알 수 있는 바와 같이 특징값의 삽입 전후 발생한 오차 비트의 수는 가중치 부여 방법에 의해 큰 차이를 보이지 않았지만, 비가시성 측면에서는 적응적 가중치 부여방법이 기존 방법에 비하여 효과적인 것으로 나타났다. 또한, 그림 7로부터 비가시성 측면에서 제안된 가중치 부여방법은 특징값을 얼굴 영상에 삽입한 경우보다 지문 영상에 삽입하는 경우 보다 더 효과적인 것으로 나타났다.

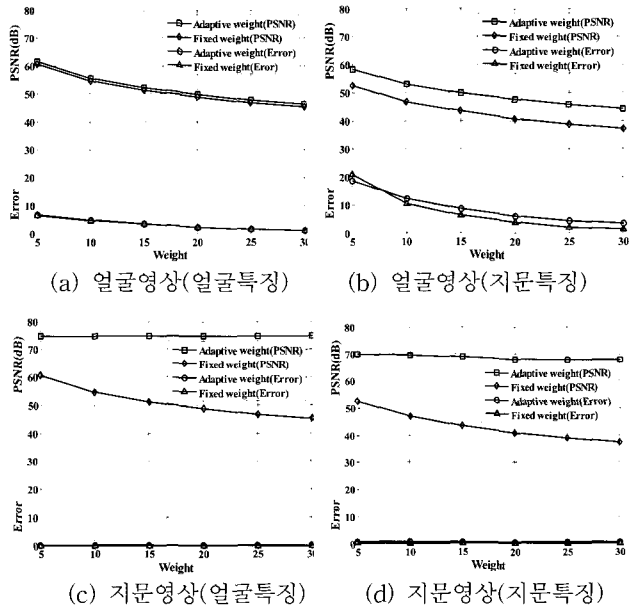


그림 7. 가중치 설정방법에 따른 성능평가
 Fig. 7 Performance evaluation according to weight

그림 8에서는 가변 비트형 이진화 방법 및 가중치 부여방법에 따른 워터마크(생체정보)가 삽입된 영상의 PSNR과 워터마크 삽입 전과 후의 오차비트의 수를 나타냈다. 그림 8(a)에서 보는 바와 같이 본 논문에서 제안된 가변 비트형 이진화방법과 적응적 가중치 부여 방법을 적용한 경우 다른 방법에 비하여 우수한 결과를 나타냈다. 또한, 워터마크 삽입 전과 후의 오차측면에서는 제안된 방법이 가변 비트형 이진화방법과 고정된 가중치를 부여한 방법보다 오차가 높게 나타났으나, 오차가 발생한 비트의 차이는 2비트로서 전체 비트의 수 150에 비하여 1.3%로 이러한 비트의 차이가 생체인식 단계에서는 큰 영향을 미치지 않는다는. 따라서 제안된 가변 비트형 이진화방법과 적응적 가중치 부여방법이 생체정보 보호를 위한 워터마킹 알고리즘에 효과적인 것으로 분석된다.

4.2 워터마크 기법을 이용한 다중 생체인식 결과

표 1에서는 원영상에 워터마크를 삽입한 방법과 기준영상에 워터마크를 삽입하는 방법 등에 따른 인식률 결과를 나타냈다. 삽입위치에 따른 성능을 평가하기 위한 방법 중에서 워터마크가 삽입되지 않은 얼굴 영상의 경우에 있어서 원영상은 고려하는 얼굴 영상과 동일하지만, 기준영상은 고려하는 얼굴 영상 중에서 고조파 성분이 제거된 저주파 성분만을 이용한 영상이라 할 수 있다. 워터마크가 삽입되지 않은 지문 영상의 경우에도 동일한 의미를 갖는다.

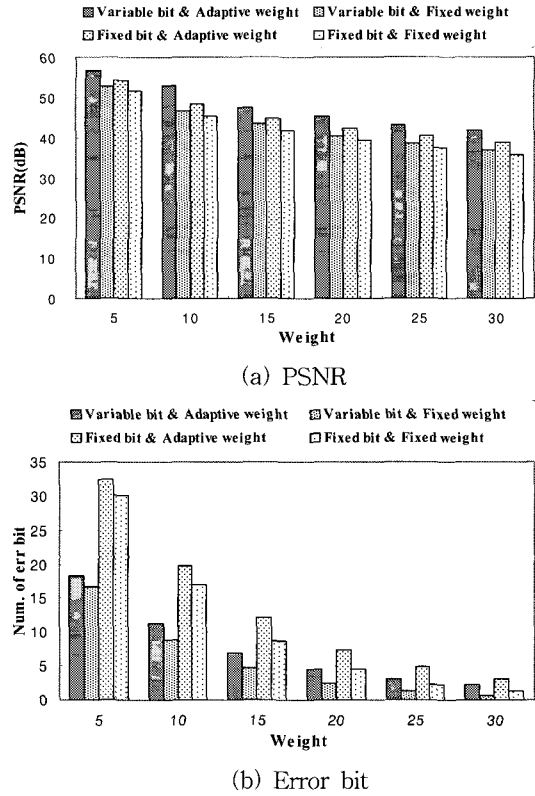


그림 8. 적용방법에 따른 성능평가

Fig. 8. Performance evaluation by each applied method

표 1. 워터마크 삽입위치에 따른 인식률

Table 1. Recognition result according to original and reference images

Cover image (watermark)	original image		reference image	
	recognition	PSNR	recognition	PSNR
Face (no watermark)	82.67%	-	82.67%	-
Fingerprint (no watermark)	93.33%	-	83.33%	-
Face(Fingerprint)	82.67%	47.61dB	82.67%	37.40dB
Fingerprint(Face)	86.67%	68.81dB	83.33%	23.93dB

실험 결과, 워터마크를 삽입하지 않은 얼굴 영상의 경우에는 원영상과 기준영상에 의해 인식률에는 큰 차이를 보이지는 않았다. 그러나 지문 영상의 경우에는 기준영상에 적용한 경우 원영상을 이용하는 경우보다 인식률이 저조하게 나타났다. 지문 특징값이 삽입된 얼굴 영상을 이용하여 인식하는

경우 삽입 위치(원영상/기준영상)에 의해 인식률에는 차이가 나타나지 않았으나 PSNR 측면에서는 원영상에 지문 특징을 삽입하는 경우 효과적인 것으로 나타났다. 마지막 실험으로서, 얼굴 특징값이 삽입된 지문 영상을 이용하여 인식하는 경우 원영상에 지문특징을 삽입하는 경우가 인식률 및 PSNR 측면에서도 효과적인 것으로 나타났다. 이러한 결과로부터 얼굴 영상보다 지문 영상이 삽입 위치에 의해 인식률에 차이가 나타났다. 그림 9에서는 원영상(지문), 얼굴 특징값이 원영상에 삽입된 지문 영상과 기준영상에 삽입된 지문 영상에 대한 특징 추출 결과를 나타냈다. 그림 9에서 보는 바와 같이 얼굴 특징값이 삽입된 지문 영상의 경우에는 추출된 특징값이 원영상(지문)에서 추출된 특징값과 동일하게 나타났다, 기준영상에 얼굴 특징값을 삽입한 지문 영상에 대해 추출된 특징값은 새로운 특징영역이 결정되거나 원영상(지문)에 존재하는 특징값들이 선택되지 않는 경우가 발생한 것으로 나타났다. 이는 얼굴의 경우 고조파 성분보다는 저주파 성분에 의해 표현되지만, 지문의 경우에는 고조파 성분들이 지문 특징값을 산출하는데 중요한 영향을 주기 때문에 지문의 경우에 고조파를 제거할 경우 인식률이 저조한 것으로 분석된다. 따라서 이러한 결과로부터 생체인식시스템 관점에서는 은닉할 생체 데이터를 기준영상이 아닌 원영상에 삽입하는 것이 효과적임을 확인 할 수 있다.

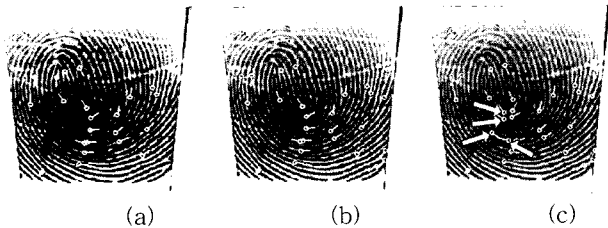


그림 9. 각각의 지문영상에 특징점

Fig. 9. Minutiae point in each image

- (a) Original image (b) Watermarked original image
- (c) Watermarked reference image

표 2에서는 워터마크 데이터와 워터마크가 삽입된 영상을 이용한 실험결과를 나타냈다. 실험방법은 ①워터마크를 적용하지 않은 경우, ②얼굴 영상에 지문 특징값을 은닉한 경우, ③지문영상에 얼굴 특징값을 은닉한 경우 등 세 가지 실험방법을 고려하였다. 표 1에서 보는 바와 같이 워터마크가 삽입되지 않은 얼굴 영상의 경우 인식률은 82.67%, 지문 특징값이 삽입된 얼굴 영상의 경우 82.67%, 지문에 삽입 및 추출된 얼굴 특징값을 이용한 경우에도 82.67%로 나타나 얼굴 영상의 경우 삽입 여부에 의해, 차이가 발생하지 않았다. 지문인식의 경우에는 워터마크를 삽입하지 않은 경우 인식률이 93.33%, 얼굴에 삽입 및 추출된 지문 특징값을 적용한 경우 90.00%, 얼굴 특징값이 삽입된 지문 영상의 경우 86.67%로 나타나 지문 영상의 경우에는 워터마크 삽입에 따라 인식률이 저하된 것으로 나타났다. 특히, 얼굴 특징값이 삽입된 지문 영상인 경우에는 워터마크를 삽입하지 않은 경우에 비하여 인식률이 7%로 저하된 것으로 나타났다. 그러나 생체정보가 은닉된 생체영상과 은닉된 생체 특징값을 융합한 방법에서는 워터마크를 적용하지 않은 방법과 비교하여 인식률이 저조하게 나타나지는 않았다. 이 결과로부터 본 논문에서 제안된 워터마크 알고리즘과 다중 생체인식시스템 구현 방법의 타당성을 확인 할 수 있다. 또한 표 3에서는 생체 영상이 아닌 일반 영상을 배경영상으로 사용하여 실험한 결과로 일반

영상에 얼굴과 지문 특징값을 모두 은닉후 추출한 특징값을 이용하여 다중 생체 인식률을 구하였다. 일반 영상을 대상으로 한 다중 생체인식시스템의 구현 역시 타당성을 확인 할 수 있다.

표 2. 다중 생체 워터마킹의 인식률

Table 2. Recognition rates for the multimodal biometrics

Cover image (watermark)	Face	Fingerprint	Fusion	PSNR
No watermark	82.67%	93.33%	98.67%	-
Face(Fingerprint)	82.67%	90.00%	99.33%	47.61
Fingerprint(Face)	82.67%	86.67%	98.67%	68.81

표 3. 일반 영상을 이용한 다중 생체 워터마킹의 인식률

Table 3. Recognition rates for the multimodal biometrics using natural images

Cover image (watermark)	Face	Fingerprint	Fusion	PSNR
LENNA	82.67%	92.66%	98.67%	62.18dB
Mandrill	82.67%	93.33%	98.67%	64.39dB
Sailboat	82.67%	93.33%	98.67%	65.77dB



그림 10. 배경영상

Fig. 10. Sample natural images

4. 실험 및 결과

논문에서는 생체인식에 있어서 가장 취약점으로 나타날 수 있는 생체데이터의 유출에 대한 대책의 한 방법으로 워터마킹기법을 이용한 생체정보 보호를 제안 하였다. 일반적인 디지털워터마킹기법과 달리 원영상을 생체 데이터의 이미지를 사용하여 실험하였다. 삽입 이전의 생체특징 인식률과 추출후의 인식률 비교와 생체정보 삽입이전의 생체이미지와 생체정보가 은닉된 생체이미지간의 인식률 비교를 통해 성능을 평가하였다.

제안된 방법을 얼굴과 지문특징을 이용한 단일 생체인식 시스템과 원영상으로 사용된 생체데이터를 이용한 다중생체 인식시스템에 적용하여 실험한 결과, 워터마크 데이터로 사용된 특징의 단일 생체인식 시스템의 경우 인식률이 저하되는 것으로 나타났지만, 원영상으로 사용된 생체이미지와 추출된 생체특징을 이용한 다중 생체인식 시스템의 경우, 정보의 유출 가능성이 있는 은닉기법을 적용하지 않은 경우와 동일한 인식률을 나타내어 제안된 방법은 생체정보의 은닉을 위한 효과적인 방법인 것으로 나타났다. 또한, 자연 영상에 생체정보를 은닉하더라도 워터마크의 중요한 지표 중의 하나인 비가시성 측면에서도 효과적임을 확인할 수 있었다. 본

논문에서는 워터마킹 알고리즘을 이용하여 다중생체 인식시스템을 연구한 것으로서, 향후 다양한 공격에 대한 제안 방법의 강인성에 대한 연구를 진행하고자 한다.

참 고 문 헌

- [1] 전명근, 생체인식(Biometrics) 총론, 한국정보통신교육원, 2004.
- [2] 송장규, 권석영, 전명근, "Contourlet 변환 및 PCA에 의한 얼굴인식," 한국퍼지및지능시스템학회논문지, Vol. 17, No. 3, pp. 403-409, 2007.
- [3] 권만준, 양동화, 김용삼, 이대중, 전명근, "유비쿼터스 환경에서 PDA를 이용한 다중생체인식 시스템 구현", 한국퍼지및지능시스템학회논문지, Vol. 16, No. 4, pp. 430-435, 2006.
- [4] 전명근, "생체정보 이용과 프라이버시 보호", 정보보호학회, Vol. 15, No. 6, pp. 11-18, 2005.
- [5] Anil K. Jain, Umut Uludag, "Hiding biometric data," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 25, No. 11, pp. 1494-1498, 2003.
- [6] C. P. Wu and C. C. J. Kuo, "Fragile Speech Watermarking for content integrity verification", *IEEE International Symposium on Circuits and Systems (ISCAS)*, Vol. 2, pp. 436-439, 2002.
- [7] C. Soutar, A. Stoianov, R. Gilroy and B.V.K.V. Kumar, "Biometric encryption", http://www.bioscrypt.com/company/technology/white_papers.html.
- [8] 김태해, 정승환, 정용화, 문대성, 문기영, "워터마킹 기법을 이용한 생체정보 보호", 정보보호학회지, Vol. 15, No. 6, pp. 31-40, 2005.
- [9] 김태해, 생체인식 시스템에 적합한 워터마킹 알고리즘에 관한 연구, 고려대학교, 전산학과 석사학위 논문, 2006.
- [10] Mayank Vatsa, Richa Singh, Afzel Noore, "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking," *EIECE Electron. Express*, Vol. 2, No. 12, pp. 362-367, 2005.
- [11] Jiang-Lung Liu, Der-Chyuan Lou, Ming-Chang Chang and Hao-Kuan Tso, "A robust watermarking scheme using self-reference image", *Computer Standards & Interfaces*, Vol 28, No. 3, pp. 356-367, 2006.
- [12] Sanghyun Joo, Youngho Suh, Jaeho Shin, Hisakazu Kikuchi, and Sung-Joon Cho, "A new robust watermark embedding into wavelet DC components", *ETRI Journal*, Vol. 24, No. 5, pp. 401-404, 2002.
- [13] Keun-Chang Kwak, Witold Pedrycz, "Face recognition using a fuzzy fisherface classifier", *Pattern recognition*, Vol. 38, No. 10, pp. 1717-1732, 2005.
- [14] Zhixin Shi, Venu Govindaraju, "A chaincode based scheme for fingerprint feature extraction", *Pattern Recognition Letters*, Vol. 27, No. 5, pp. 462-468, 2006.
- [15] Chikkerur S., Govindaraju V. and Alexander N.

Cartwright, "K-plet and coupled BFS : A graph based fingerprint representation and matching algorithm", *Lecture Notes in Computer Science*, Vol. 3832, pp. 309-315, 2006.

- [16] Asker M. Bazen and Sabih H. Gerez, "Fingerprint matching by thin-plate spline modeling of elastic deformations", *Pattern Recognition*, Vol. 36, No. 8, pp. 1859-1867, 2003.

저 자 소개



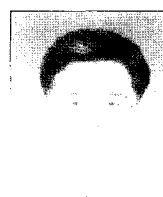
이욱재(Wook-Jae Lee)
2007년 : 충북대학교 전자공학과(학사)
2007년~현재 : 충북대학교 제어계측공학과 석사과정

관심분야 : 워터마킹, 생체정보보호, 임베디드 프로그래밍, 패턴인식



이대중(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



문기영(Ki-Young Moon)
1996년 : 경북대학교 전자공학과(학사)
1999년 : 경북대학교 전산학(공학석사)
2006년 : 충남대학교 전산학(공학박사)
1994년~현재 : 한국전자통신연구원 바이오인식기술연구팀, 팀장

관심분야 : 바이오인식, 정보보호, 웹서비스 보안



전명근(Myung Geun Chun)
1987년 : 부산대학교 전자공학과(학사)
1989년 : 한국과학기술원 전기 및 전자공학과(공학석사)
1993년 : 한국과학기술원 전기 및 전자공학과(공학박사)
1993년~1996년 : 삼성전자 자동화연구소 선임연구원

2000년~2001년 : University of Alberta 방문교수
1996년~현재 : 충북대학교 전기전자 및 컴퓨터공학부 교수

관심분야 : Biometrics, 감정인식, 음성신호처리, 얼굴인식