情 報 保 護 學 會 誌
第 15 卷 第 6 號, 2005. 12

Biometric System에서의 Privacy 보호 기술

최 경 택*, 박 강 령**, 김 재 희***

요 약

본 논문은 현재 생체인식에서의 큰 문제로 대두되고 있는 개인 정보(Privacy) 보호문제를 해결하기 위한 방법들을 소개하고 있다. 이를 위해서는 여러 가지 기술이 사용되는데, 우선 생체정보가 도난되었을 경우 그 피해를 최소화하기 위해 원래의 생체정보를 저장하는 것이 아니라 변환된 생체정보를 저장하고 사용하는 생체정보 변환 기술을 소개한다. 또한 원래의 생체정보가 유출되어 이를 이용해 위조 생체 등을 만들어 공격할 경우를 대비할 수 있는 위조 생체 검출 기술을 소개하며, 생체정보의 유출된 출처를 찾기 위해 생체정보에 소유권 등을 표시하는 데이터 은닉 기법도 소개한다. 이 외에 생체정보를 이용하여 일반적인 암호화 알고리즘에 사용되는 키를 은닉하고 생체정보를 통해 인증된 사용자에 한하여 키를 사용하도록 하는 방법도 소개한다. 끝으로 이러한 개인 정보 보호 기술들을 이용하여 생체인식 시스템의 보안성을 향상시키는 방법에 대하여 논의한다.

Ⅰ. 서 론

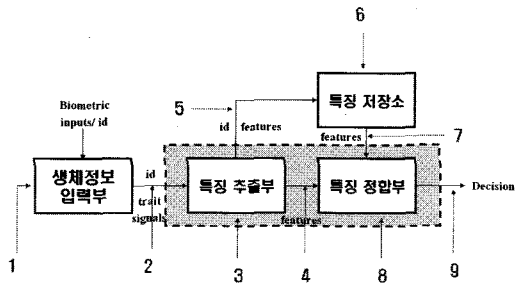
지난 수년간 전자상거래의 발달, 국제 테러 위협의 증가, 공공기관의 전자 행정화 등의 이유로 국내외적으로 개인 인증 기술이 크게 발달되어 왔다. 특히 종래의 패스워드 시스템의 취약점인 분실이나 타인의 남용 및 소지 또는 암기의 불편들을 극복하고자 생체인식 기술이 대두되었고 최근 비약적으로 발전하였다. 현재 가장 대표적인 생체인식 기술(Biometrics)인 지문, 홍채, 얼굴, 서명, 음성 인식 등의 기술은 이미 공항 및 항만의 출입국 관리소 같은 공공기관이나 기업의 사내 전산망 및 출입 통제 시스템 그리고 은행의 고객 인증 시스템과 같이 여러 분야에 널리 퍼져있다. 이렇게 생체인식 기술이 널리 퍼지면서 여러 문제점 또한 대두되었는데 그 중 가장 시급한 것은 '과연 생체인식 기술이 이상적이고 안전한 기술인가?' 하는 점이다. 생체인식 기술은 본인의 신체 일부나 행동패턴 등의 정보를 사용하기 때문에 본인이 직접 시스템을 이용해야 한다는 안전성과 분실하거나 암기할 필요가 없다는 점에서 확실히 본인 인증에 이상적인 기술로써 향후 패스워드 시스템을 대체할 기술로 받아들여지고 있다. 하지만 이러한 생체인식 기술에도 보안상의 여러 허점들이 있고 이를 극복하기 위해 많은 연구가 진행되고 있다.

일반적으로 생체 인식 시스템은 그림 1과 같이 크게 4개의 부분으로 구분될 수 있다. 우선 생체정보를 취득하는 입력부가 있고 취득된 생체정보에서 인식에 사용되는 특징을 추출하는 부분이 있으며, 특징 및 개인의 정보 등을 저장하는 저장소 그리고 인증 과정 시, 저장소의 특징과 새로 입력된 특징을 비교하는 특징 정합부로 구성된다. 이러한 생체 인식 시스템의 보안상의 허점은 9가지로 분류 될 수 있으며 각 허점의 공격 포인트는 그림 1에 나와 있고 그 내용은 다음과 같다[1].

1. 위조 생체를 입력하여 시스템을 기만하는 방법
2. 이 전에 불법 취득한 생체정보를 재생(Replay)하는 방법
3. 특징 추출부를 공격, 위조된 특징을 임의로 생성하는 방법

본 연구는 과학기술부 지정 한국과학재단 생체인식 연구센터(BERC)의 지원으로 수행 되었습니다.
* 연세대학교 전기전자공학부 (maninquestion@yonsei.ac.kr)
** 상명대학교 미디어학부 (parkgr@smu.ac.kr)
*** 연세대학교 전기전자공학부 (jhkim@yonsei.ac.kr)

4. 임의의 위조된 특징을 전송, 시스템의 정합 오류를 유도 하는 방법
5. 저장소로 전송되는 생체 특징 정보나 개인정보를 절취 또는 타인의 정보로 대체하는 방법
6. 저장소에 침투하여 기 저장된 생체 데이터를 조작, 삭제, 절취하는 방법
7. 저장소에서 정합부로 전송되는 생체 특징을 절취 또는 타인의 정보로 대체하는 방법
8. 특징 정합부에서 정합 값을 임의로 변경하는 방법
9. 8번과 유사하게 최종 인증 결과(Accept or Reject)를 바꾸는 방법



〔그림 1〕 생체인식 시스템의 개요도 및 보안상의 취약점

위의 허점들 중에 3, 4, 8, 9와 같이 악의적인 프로그램에 의해 시스템의 오판을 유도하는 방법들은 생체인식 기술이 아닌 다른 인증 기술에서도 문제가 되고 있고, 이를 막기 위한 연구가 해당 분야에서 현재 진행되고 있다. 또한 이러한 악의적인 프로그램에 의한 문제들은 생체인식 기술의 가장 큰 취약점인 개인정보(Privacy)의 유출이나 오용과는 직접적인 연관이 없기 때문에 본 논문에서는 다루지 않는다. 하지만 1, 2, 5, 6, 7번과 같은 공격방법들은 개인 정보를 절취하거나 남용하는 방법들로서 이를 막거나 사후처리에 필요한 기술들은 현재 생체인식 분야에서 중점적으로 연구되어야 할 과제이다. 개인 정보의 유출이나 남용이 큰 문제가 되는 이유는 개인의 생체정보는 영구 불변성을 띄고 있어 이러한 정보가 유출되고 타인에 의해 악용되었을 경우에는, 쉽게 변경할 수 있는 (Cancelable) 패스워드와는 달리 생체정보가 유출된 개인은 해당 생체정보를 다시는 이용할 수 없다는데 있다. 또한 생체인식 기술을 여러 기관에서 사용하면서 개인정보의 관리상에 문제가 발생할 수 있는데 이러한 요인들이 개인정보의 유출 문제를 키우고 있다.

이러한 생체 정보의 유출 및 그에 따른 남용을 막기 위한 방법에는 크게 세 가지를 들 수 있다. 우선, 그림 1의 6 공격에 대한 대비책으로 생체정보를 저장시 생체정보를 변환하여 저장함으로써 변환된 생체정보가 유출되더라도 원래의 생체정보를 알 수 없게 하는 생체정보 변환(Changeable Biometric)기술이 있다. 이 기술은 변환된 생체정보가 유출되더라도 공격자가 원래의 생체정보를 알 수 없으므로 사용자는 변환된 생체정보를 폐기하고 다시 새로운 변환된 생체정보를 생성하여 사용함으로써 생체정보 유출에 의한 피해를 최소화 할 수 있다. 다음은 그림 1의 1공격에 대한 대비책으로 위조 생체를 막는 방법(Fake Biometric/Liveness Detection)이 있을 수 있다.

이와 같은 생체정보의 유출은 실제 동작중인 생체인식 시스템에서 일어날 수도 있지만 일반 생활에서도 발생할 수 있다. 가령 지문 같은 경우는 컵이나 유리 등의 물건에 잔여 지문(Latent Fingerprint)이 존재할 수 있는데 이는 원래의 생체정보가 유출되는 경우이므로 생체정보 변환 기술로도 막을 수 없다. 따라서 유출된 정보를 이용하여 위조 지문을 만들어 공격자가 침투할 경우 이를 막기 위한 위조 생체 검출기술이 필요하다. 마지막으로 생체정보가 유출되었을 경우 어디에서 유출되었는지 파악을 해야 유출된 곳의 안정성을 보완할 수 있다. 따라서 생체정보에 출처를 암시할 수 있는 표식을 은닉하는 기법(Watermarking)들이 필요하며, 이를 이용하여 그림 1의 2, 5, 7 공격을 막을 수 있다. 그 외에도 생체정보를 암호화하거나 생체정보로부터 암호화에 사용 가능한 코드를 추출하는 기술(Biometric Key Generation)들도 필요하다.

본 논문에서는 개인 정보 보호를 위한 생체정보 변환기술, 위조 생체 검출 기술, 데이터 은닉기법, 생체 코드 추출 방법 등에 대해 현재까지 연구된 기술들에 대해 소개하고 이를 토대로 개인 정보를 보호할 수 있는 지침을 제시하고자 한다.

본 논문은 이 장을 포함하여 총 6장으로 구성되어 있으며 2장에서는 생체정보 변환기술, 3장에서는 위조생체 검출기술, 4장에서는 데이터 은닉기법, 5장에서는 생체 코드 추출방법 등에 대해 기술하고 끝으로 마지막 장에 개인정보를 보호를 위해 취할 수 있는 종합적 대책에 대해 논의 하겠다.

II. 생체정보 변환기술 (Changeable Biometrics)

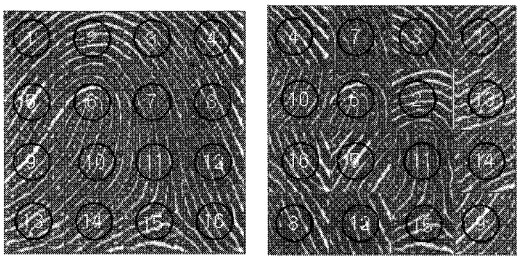
이전 장에서도 언급했듯이 대부분의 생체정보는 영구불변의 특성이 있다. 이는 생체인식 기술이 널리 활

용되도록 하는 장점이지만 보안적인 측면에서 보면 큰 단점이 될 수 있다. 왜냐하면 한번 생체정보가 유출될 경우 그 생체정보의 소유주는 다시는 해당 생체를 본인 인증에 사용할 수 없기 때문이다. 이러한 문제를 해결하기 위해 많은 연구기관에서는 일반적인 패스워드 시스템처럼 분실되거나 기억이 나지 않을 경우 다시 재발급할 수 있는 생체인식 시스템을 연구하고 있으며 이것이 생체정보 변환 기술이다[1,3]. 생체정보 변환 기술의 핵심은 원래의 생체정보가 들어왔을 때 이를 역 변환이 불가능한 함수(Non-invertible Function)를 통해 변환하여 변환된 생체정보를 통해 원 정보를 유추하지 못하도록 하는 것이며 또한 변환된 생체정보를 이용하여 개인을 인증하더라도 인증 성능이 원래의 정보를 이용하는 것에 비해 크게 저하되지 않아야 한다는 것이다. 이러한 생체정보의 변환 단계는 다음과 같이 크게 2가지로 구분될 수 있다. 생체정보 입력부 단계에서 취득된 정보를 변환하는 방법과 특징 추출부 단계에서 추출된 특징을 변환하는 방법이다. 입력부 단계에서 변환하는 방법의 예로 그림 2와 같이 얼굴인식에서 취득된 얼굴영상에서 눈의 위치를 찾고 그것을 기준으로 하여 그림 2-a와 같이 격자를 씌운 다음 각 격자점을 임의로 이동하여 와핑(Warping)기법[2]에 의해 변형된 영상으로 바꾸어 사용할 수 있다[1]. 특징 추출부 단계에서 특징을 변환하는 예로는 지문의 경우 영상에서 추출된 융선을 그림 3-a와 같이 여러 섹터로 나눈 후 그림 3-b와 같이 각 섹터의 위치를 무작위로 배치하는 방법이 있을 수 있고 융선이 아니라 그림 4와 같이 특징점의 좌표를 변환하여 새로운 좌표로 이동시킨 후 이를 정합하는 방법이 있다[1].

다른 생체 정보 변환의 예로 장문 인식(Palmprint Recognition)의 경우 Tee Connie등은 그림 5와 같이 랜덤한 $n \times m$ 행렬을 생성하고 Gram-Schmidt의 직교화 방법을 이용 m개의 직교정규 벡터로 만들었다.

(a) 원영상 (b) 변형된 영상

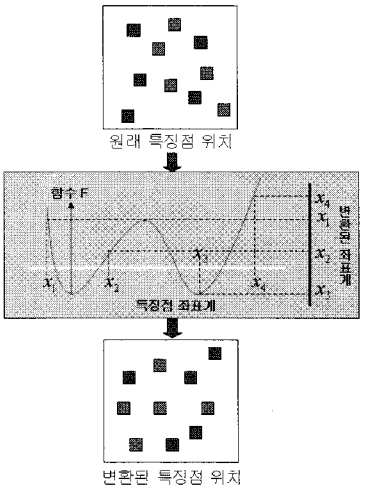
〔그림 2〕 입력 단계에서 변환된 얼굴정보의 예



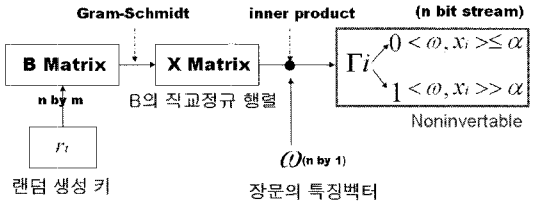
a) 세선화된 지문 원영상 b) 변환된 지문 영상

〔그림 3〕 세선화된 지문 영상을 이용 변환한 예

그리고 장문이미지를 n개의 FDA (Fisher Discriminant Analysis) 기저벡터에 투영하여 n차원의 벡터 w를 얻은 후 이전에 구했던 n차원의 m개의 직교정규 벡터와 내적하여 m개의 계수값 T_i을 얻고 각 계수값이 임계값 α보다 작거나 같으면 0 아니면 1로 하는 m bit의 코드를 얻었다. 이렇게 생성된 코드가 변환된 생체정보로써 본인 인증과정에 사용된다[4].



〔그림 4〕 특징점 위치를 변환한 예



〔그림 5〕 장문 인식에서의 생체정보 변환의 예

이외에도 생체인식연구센터에서는 지문인식에서 추출된 특징점(Minutiae) 및 지문 영상 자체를 변형하

고, 얼굴인식에서 얼굴 특징값들을 변형함으로써 생체 정보를 변환할 수 있는 연구를 활발히 진행하고 있다[32].

앞에서 언급했듯이 생체정보 변환을 위해서는 변환함수에 역함수가 존재하지 않고 변환된 생체정보의 인식 성능이 저하되지 않아야 한다. 그 외에도 대부분의 생체정보에는 잡음이나 위치의 변이 및 회전 또는 지문의 경우 압력에 의한 비선형 변형(Non-linear Distortion) 등이 발생하여 등록 시 얻은 생체정보와 똑같은 생체정보를 인식 과정에서 얻기는 불가능하다. 따라서 이러한 생체정보 변환기술은 각 생체정보에 맞게 환경영향에 강인하도록 설계되어야 하며, 변환된 생체정보가 유출되는 경우 또다시 변환된 생체정보를 새롭게 생성할 수 있는 능력이 있어야 한다. 본 논문에서 언급한 얼굴, 지문, 장문의 예 외에도 홍채, 음성 등에 관한 방법 또한 특허에 언급되어 있다[3].

Ⅲ. 위조생체 검출기술 (Fake Biometric/Liveness Detection)

전술한 바와 같이 생체정보 변환기술은 원래의 생체정보의 유출을 막아 생체정보 유출에 의한 피해를 최소화 할 수 있는 기술이다. 하지만 원래의 생체정보는 생체인식 시스템이 아닌 다른 경로로 유출이 가능하다. I장에서 언급했듯이 지문의 경우에는 잔여지문(Latent Fingerprint)을 통해 유출될 수 있고, 얼굴이나 홍채의 경우 사진이나 안과에서의 진단과정에서 유출될 수 있다. 이렇게 원래의 생체정보가 유출되었을 경우 공격자는 이 정보를 이용해 위조 생체를 생성하여 공격할 수 있다.

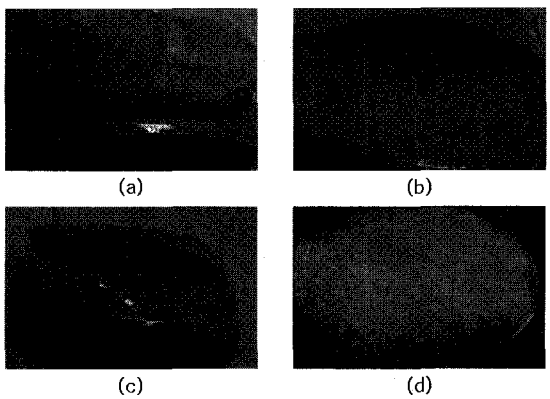
현재까지는 주로 지문과 홍채에 대한 위조 생체 생성방법과 이를 막는 기술들이 연구 되고 있다. 위조 생체를 생성하는 방법은 크게 2가지로 나누어질 수 있다. 첫째는 실제 소유자의 도움을 받아 생성하는 것이고 다른 하나는 유출된 생체정보(잔여지문, 사진 등)를 통해서 생성하는 것이다. 이외에도 영화에서 나왔듯이 사람의 손가락을 자르거나 안구를 뽑아서 시스템을 기만할 수 있다[5,6].

지문의 경우 소유자의 도움을 받아 위조 지문을 만드는 방법은 그림 6-a와 같이 사용자가 플라스틱 찰흙 등에 지문을 찍어 틀을 만들고 그 틀에 젤라틴이나 실리콘을 부어 그림 6-d와 같은 위조 지문을 만드는 것이다. 잔여지문을 통해서 위조 지문을 만드는 방법은 범죄 수사 시 사용하는 고운 분말과 접착테이프 등을 이용하여 잔여지문을 취득하고 그 잔여지문을 디지털 현미경으로 찍어 영상을 얻은 후 영상 처리를 하여 잡음을 없애고 이를 필름에 인화하여 감광성의 PCB (Photosensitive Printed Circuit Board)에 부착한 후 자외선을 조사하여 주형을 생성한다. 이 주형에 젤라틴과 같은 용액을 부으면 그림 7과 같은 위조 지문이 생성된다[7,8,9].

Matsumoto는 위에서 언급한 방법으로 젤라틴 위조지문을 만들어 7개의 광학 센서(Optical Sensor)와 4개의 전기 용량 방식(Capacitive Sensor)의 센서에 대해서 5명의 사용자를 대상으로 실험 하였다. 총 11개의 센서에 대해서 각 사용자 별로 100회 공격한 결과 11개 센서 모두에서 최소 60번 이상 위조 지문에 의한 공격이 성공하였다[7].

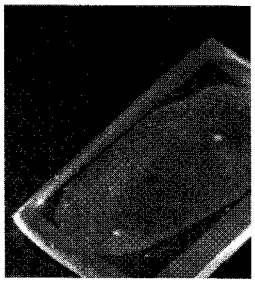
이러한 공격을 차단하는 위조 지문 검출방법(Liveness Detection)은 크게 2가지로 나눌 수 있다. 첫 번째 방법은 추가적인 하드웨어를 사용하여 맥박이나 온도와 같은 생체 고유의 신호를 측정하는 것이다. 이 방법은 비용이 많이 들고 시스템이 커지는 단점이 있다. 두 번째 방법은 지문 인식 센서로부터 얻은 영상에서 실제 지문과 위조 지문의 차이를 탐지하는 방법이다. 이는 첫 번째 방법에 비해 비용을 절감할 수 있고 또한 시스템의 크기를 줄일 수 있지만 인식 시스템의 알고리즘이 복잡해진다. 부수적인 하드웨어를 이용하여 손가락에서 얻을 수 있는 생체 정보로는 표피 온도, 표피의 광학적 특성, 맥박, 헤모글로빈(hemoglobin)의 산소 포화도, 혈압, 전기적 저항, 상대적 유전체 유전율 (Relative dielectric permittivity), 내피 탐지 (Detection under epidermis) 등이 있다[6,10].

지문 센서에서 취득된 영상 정보만을 이용해 위조



〔그림 6〕 사용자의 협조로 생성된 젤라틴 위조 지문

지문을 검출하는 방법에는 센서에 지문을 접촉 시 발생하는 변형이 실제 지문의 경우에는 비선형 특성을 갖는다는 점에 착안에 이를 검출하는 방법과 지문의 땀샘 정보까지 위조하기는 어렵다는 점에 착안한 방법 그리고 지문의 발한작용을 이용한 방법들이 있다[11,12,13]. 생체 인식 연구센터에서는 이중 지문 땀샘의 정적, 동적 특성을 이용하여 위조 지문을 판별하는 연구를 수행하고 있다[32].

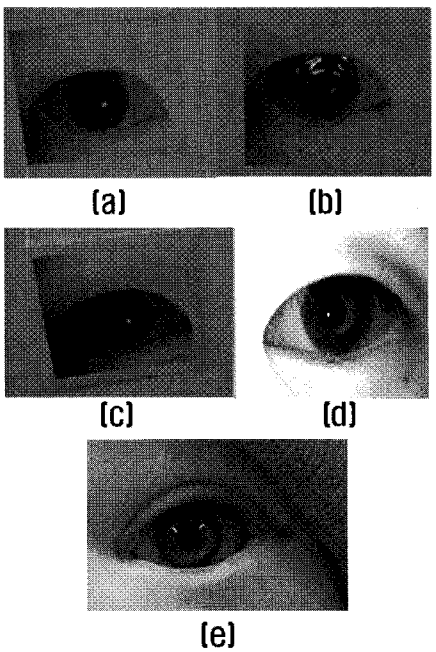


〔그림 7〕 잔여 지문을 통해 생성된 위조지문[7]

위조 홍채를 생성하는 방법에는 그림 8-a와 같이 고해상도 프린터로 홍채 영상을 프린트하는 방법, 그림 8-b의 프린트된 영상과 콘택트렌즈를 결합하는 방법, 그림 8-c의 사진으로 인화하는 방법, 그림 8-d의 공격자가 위조 홍채 패턴이 있는 콘택트렌즈를 착용하는 방법, 그리고 그림 8-e처럼 인공안구를 만드는 방법들이 있다[14,15]. 이러한 위조 홍채를 사용하여 본 논문에서는 각 위조 홍채마다 40회씩, 기존의 한 홍채인식 시스템을 공격해 보았고 결과는 표 1과 같다.

본 논문에서 실험했던 홍채인식 시스템에는 위조 홍채를 검출하는 기능이 있는데 그 기능을 끄고 실험을 하면 프린트와 콘택트렌즈를 함께 이용한 것이 100% 에러(위조를 검출하지 못하는 에러)를 보였고 위조 홍채 검출 기능을 켰을 때는 인공안구로 공격했을 때의 에러가 가장 컸다. 현재 기술로는 실제 사람의 홍채 패턴을 그대로 위조하는 인공안구를 만들기 어렵기 때문에 본 실험에서는 인공안구의 경우만 등록 시 위조 검출 기능을 끄고 인공안구로 등록 하였고 인식 시에는 위조 검출 기능을 끄거나 키고 인공안구를 입력하였다.

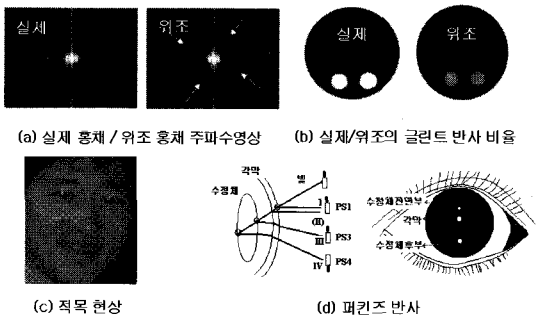
기존에 위조 홍채를 검출하는 방법은 한 장의 영상을 사용하는 정적 접근 방법과 여러 영상을 사용하는 동적 접근 방법으로 나뉠 수 있다. 정적 접근 방법에는 그림 9-a와 같이 프린트한 영상에는 도트(dot)의 주기성이 존재함에 착안하여 주파수 분석을 통해 위조 홍채를 검출하는 방법, 그림 9-b와 같이 동공과 글린트(Glint)에서 밝기 값의 비율의 차이를 비교하는 방법, 그림 9-c에서와 같이 눈의 적목 현상(Red Eye Effect)을 이용하는 방법 그리고 그림 9-d의 퍼킨즈(Purkinje) 반사현상을 검출하는 방법 등이 있다[16,17]. 동적접근 방법에는 여러 개의 LED를 임의로 번갈아 키면서 글린트의 위치 변화로 검출하는 방법, 빛의 세기에 따른 동공의 확대 축소를 검출하는 방법 그리고 눈꺼풀의 깜박임을 검출하는 방법 등이 있다[16-18]. 생체인식연구센터에서는 홍채 및 흰자위에서 적외선 조명의 반사차이 및 퍼킨즈 반사를 이용하여 위조 홍채를 판별하는 연구를 진행하고 있다[34,35].



〔그림 8〕 위조 홍채의 예

〔표 1〕 위조 홍채 공격 실험 결과

인식성능 / 위조방법	FAR(%) (위조 검출 기능 OFF 시)	FAR(%) (위조 검출 기능 ON 시)
프린트(그림 8-a)	90	0
프린트+콘택트렌즈 (그림 8-b)	100	27.5
사진 (그림 8-c)	0	0
인공안구 (그림 8-e)	92.5	47.5



(a) 실제 홍채 / 위조 홍채 주파수영상 (b) 실제/위조의 글린트 반사 비율

(c) 직목 현상 (d) 퍼킨즈 반사

〔그림 9〕 정적 접근 방법에 의한 위조 홍채 검출

표 2는 각 검출방법과 위조 방법에 따라 위조 홍채가 검출 가능한지 여부를 O(검출 가능)와 X(검출 불가능)로 표시하였다.

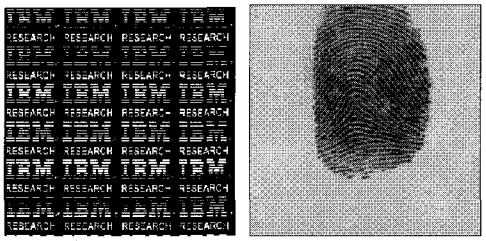
〔표 2〕 위조 홍채의 검출 방법에 따른 검출 성공표

검출방법 \ 위조홍채		프린트	사진	동공을 잘라낸 프린트	콘택트 렌즈	인공안구	단 점
정적접근방법	주파수 분석	○	X	○	○	X	Blur된 영상에 취약
	적목현상	○	○	X	X	○	
	퍼킨즈반사	○	○	X	X	○	조명 및 카메라 각도등 조건의 제약
동적접근방법	LED조명을 임의의 위치에 번갈아 킴	○	○	X	X	X	추가 LED가 요구됨
	동공확대축소	○	○	○	X	○	장시간 소요 추가조명
	눈꺼풀 깜박임	○	○	○	X	X	장시간 소요 사용자 불편

위조 지문이나 위조 홍채 이외에도 변장이나 성형에 의한 위조 얼굴, 혹은 성대 모사와 같은 위조 음성 등의 위조 생체가 있을 수 있지만 지문이나 홍채에 비해 활발히 연구되지는 않았다. 이중 위조 얼굴에 대한 검출 연구는 생체 인식 연구센터에서 활발히 연구 진행 중이다.

Ⅳ. 데이터 은닉기법(Watermarking)

생체 정보에 추가 데이터를 은닉하는 이유는 전술한 바와 같이 생체정보의 출처를 표시하여 정보가 유출될 경우 출처를 알아내는 용도로 사용가능하고, 입력단에서 비밀코드를 은닉함으로써 비밀코드가 없는



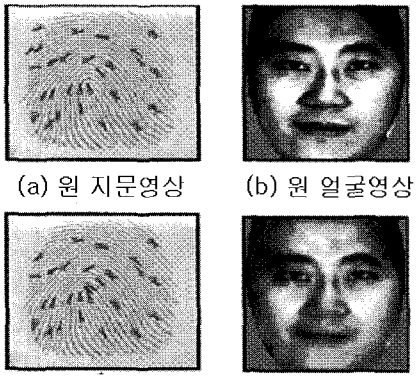
(a) 부가정보 (b) 워터마크 된 지문영상

〔그림 10〕 지문의 워터마킹 예[23]

생체 정보는 정상적인 입력 단을 거치지 않고 입력 된 것으로 간주 인증과정을 거부할 수 있기 때문이다. 또한 생체정보에 다른 부수적인 정보를 추가하여 저장할 수도 있다. 데이터에 추가 데이터를 은닉하는 기법을 워터마킹 (Watermarking)이라고 하는데 워터마킹에는 데이터에 워터마크가 삽입되어 있는지를 알 수 있는 워크마크(Visible Watermark)와 알 수 없는 워터마크(Invisible Watermark)가 두 종류가 있다[20,21].

워터마킹에서 가장 중요한 것은 워터마크를 삽입하였을 때 원래의 데이터의 손상이 적고 워터마크를 훼손하려는 여러 공격에 대해 강인해야 한다. 가령 입력부에서 생체정보에 워터마크를 삽입하여 특징 추출부에 전송하고 이를 이용해 특징 추출하여 인식을 시도해도 그 성능이 워터마크가 삽입되지 않은 원래의 생체정보를 이용하는 것과 큰 차이가 없어야 하며 워터마킹 된 영상에 잡음을 추가하거나 블러링(blurring)을 하거나 회전을 시키는 등의 공격에 강인해야 한다. 생체정보에 워터마크를 삽입한 예로는 지문의 경우에는 그림 10과 같이 Yeung 등이 지문영상의 소유권을 표시하기 위해 미국연방수사국에서 채택한 지문 압축 기법인 WSQ(Wavelet Scale Quantization) 방법[22]에 IBM 로고를 삽입하는 워터마킹 알고리즘을 추가하였다. 일반적으로 영상의 중요 정보는 저주파대역에 있으므로 고주파대역에서 임의로 주파수 대역을 선택하고 각 주파수의 계수 값을 양자화(Quantization)하는 과정에서 최하위 bit(Least Significant Bit)을 바꿔서 워터마크를 삽입하여 데이터를 전송한다. 수신단에서는 영상정보와 선택된 주파수 정보를 받아 압축된 정보를 푸는 과정에서 고주파 영역에 계수 값의 최하위 bit에서 워터마크를 추출하게 된다[23]. Jain등은 그림 11과 같이 보안성을 높이기 위해 지문 영상에 본인의 얼굴영상을 주성분 분석(PCA)방법을 통해 계수 값을 추출 이를 워터마크로 하여 삽입 후 지문과 얼굴이 동시에 인증되어야 본

인임을 인증하는 방법을 제안하였다[24,25]. 그림 11을 보면 워터마킹 된 영상에서 추출된 특징점의 위치 및 개수가 원 지문영상과 다소 차이가 있는 것을 알 수 있지만 그 영향이 적어 성능에는 큰 차이를 보이지 않았다.



(a) 원 지문영상 (b) 원 얼굴영상

(c) 워터 마킹된 영상 (d) 워터마크

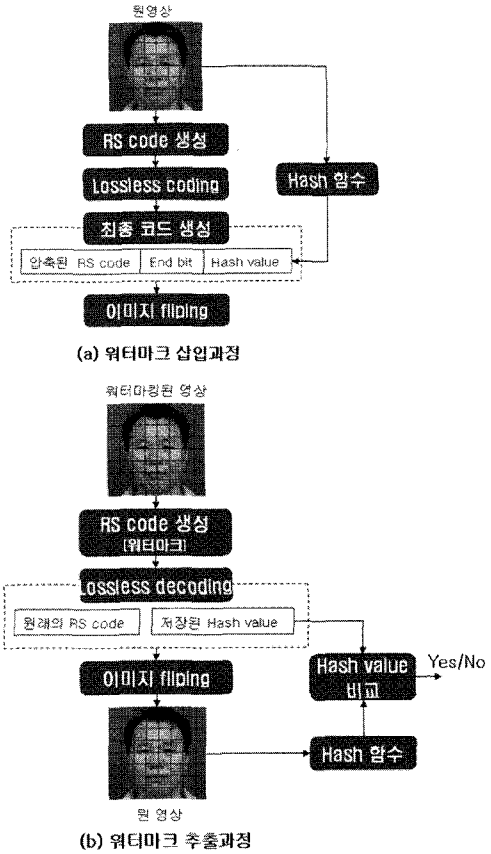
〔그림 11〕 지문영상에 얼굴정보를 워터마크로 삽입한 예[25]

영상에 출처를 표시하거나 인증 시 보안성을 높이기 위한 목적 외에도 데이터베이스에 저장된 생체정보가 훼손되거나 다른 것으로 교체 되었는지를 검출하기 위한 연구도 수행되고 있다. 생체 인식 연구센터에서는 그림 12와 같이 얼굴에 영상의 훼손여부와 위치를 검출할 수 있고 원래의 영상을 복원할 수 있는 워터마크를 삽입하는 연구를 수행하였다[26]. 우선 워터마크 삽입과정에는 영상 I를 $N\times N$ 사이즈의 블록으로 나눈 후 한 블록에 속한 밝기 값이 $(I_1,I_2,...,I_{NN})$ 이라고 할 때 식 1을 통해 F를 계산하고 $G(G(I))=I$가 되는 성질을 갖는 순람표(Lookup Table) G를 이용해 $(I_1,I_2,...,I_{NN})$을 $(I_1',I_2',...,I_{NN}')$로 변환한다.

$$F(I_1,I_2,...,I_{NN})=\sum_{k=1}^{NN-1}|I_k-I_{k+1}| \quad (1)$$

예를 들어 밝기 값 0은 1로 1은 0으로 변환한다. 그 후 $(I_1',I_2',...,I_{NN}')$를 가지고 식 1을 통해 F' 을 구하고 이 과정을 모든 블록에 대해서 수행한다. 각 블록에서 $F'>F$이면 1 (Regular Group), $F'<F$이면 0 (Singular Group), $F'=F$이면 사용하지 않는 블록 (Unusable Group)으로 정의하고 1과 0 값만을 붙여 RS 코드를 생성한다.

이 코드에 대해서 무손실 압축기법을 적용하고 원래의 영상을 해쉬 함수에 넣어 얻은 128bit의 해쉬



〔그림 12〕 영상 훼손 검출 위한 워터마킹

값을 압축된 코드에 붙이고 0 삽입(Zero padding) 등을 통해 원래 RS 코드와 같은 길이로 맞춘다. 그 후 최종 코드와 원래의 RS code의 각 bit를 비교하여 다르면 영상의 해당 블록에 G를 이용해 밝기 값을 변환함으로써 최종 코드 즉 워터마크가 영상에 삽입되도록 한다. 이렇게 하면 워터마크가 삽입된 영상에서 구한 RS 코드는 최종코드 즉 삽입된 워터마크와 동일하게 된다. 워터마크에서 압축을 풀면 원 영상에서 구한 RS 코드와 해쉬 값이 얻어지고 원 영상에서 구한 RS 코드와 워터마크와 비교하여 다르면 워터마킹된 영상을 G를 통해 밝기 값을 변환함으로써 원영상을 복원할 수 있다. 이 원영상을 해쉬함수를 통과 시켜 해쉬 값을 얻고 워터마크에 삽입된 해쉬 값과 비교하여 일치하면 워터마킹된 영상은 외부로부터 훼손이 일어나지 않은 것이고 만일 다르면 훼손이 일어난 것으로 판명할 수 있다. 그림 13은 훼손된 위치까지 검출하는 예를 보여주는 것으로 이 방법은 앞에 설명했던 과정에 오류 정정 부호를 삽입함으로써 가능하다.

원 워터마킹 영상 훼손된 워터마킹 영상 훼손위치 검출

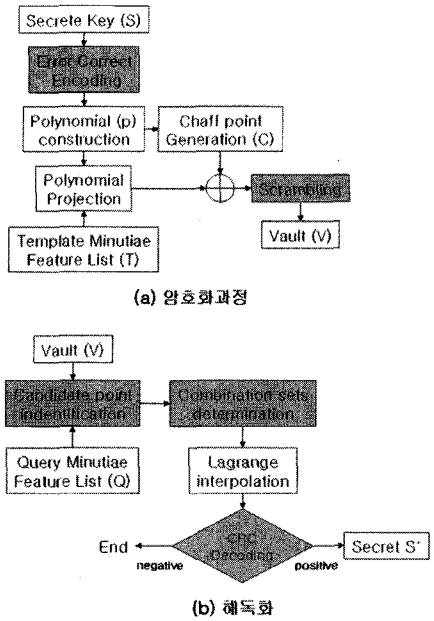
〔그림 13〕 훼손된 워터마킹 영상에서 훼손위치 검출

그림 13에서 보면 원래의 워터마킹 영상에서 공격자가 눈 부위를 다른 사람의 눈 부위와 바꾼 것을 알 수 있다. 그 결과 훼손 위치 검출 영상에서 눈 부위에만 255가 아닌 밝기 값을 가짐을 볼 수 있다.

V. 생체코드 추출방법 (Biometric Code Generation)

생체코드 추출은 개인 정보 보호와는 직접적인 연관은 없지만 생체정보를 이용하여 암호화 알고리즘에 사용하는 키를 생성하거나 은닉할 수 있다. 또한, 대부분의 생체 키 생성을 위한 알고리즘 자체를 생체 정보 변형 연구(Changeable Biometrics)에 적용 가능한 것으로 알려져 있다. 이러한 생체정보를 이용하여 비밀 키 코드를 은닉하는 대표적인 방법에는 퍼지 볼트(Fuzzy Vault)방법이 있다[27].

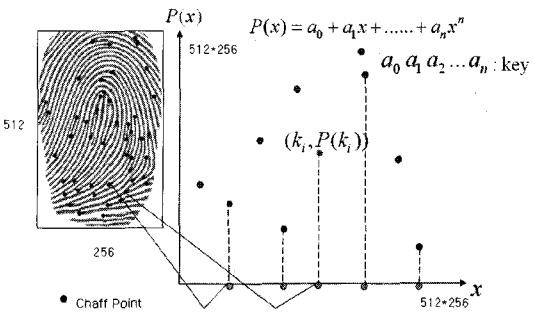
Jain교수 등은 지문에서의 퍼지볼트(Fuzzy Vault)를 이용하여 비밀 키를 암호화하는 방법에 대해 발표하였는데 그 개요도는 그림 14와 같다. 암호화 과정에서는 우선 128bit 비밀 키 S에 16bit CRC[28](Cyclic Redundancy Check) 코드를 추가하여 144 bit코드를 만들고 코드를 16 bit씩 잘라서 16 bit값이 다항식의 계수가 되는 8차 다항식 $P(x)$를 생성한다. 그림 15와 같이 지문에서 특징점을 뽑아 특징점의 좌표를 x값으로 하여 다항식에 넣어 $(x,P(x))$쌍을 구한다. 지문의 특징점 정보를 감추기 위해 위장 점(Chaff Points)들의 쌍$(x',P'(x'))$도 구해서 두 집합을 랜덤하게 섞어 볼트를 생성한다. 해독화(Decrypt) 과정에서는 사용자의 지문이 입력되면 특징점을 추출하고 다항식이 n차인 경우 n+1개의 특징점을 뽑아서 그것과 가장 유사한 x값을 갖는 쌍을 볼트에서 얻어내고 이를 이용해 라그랑쥐 보간법(Lagrange Interpolation)방법으로 다항식을 복원한다. 복원된 다항식의 계수를 이용해 다시 144 bit의 코드로 만들고 이를 CRC 복호화 과정을 거쳐 복호화하여 비밀키 S'을 얻는다. 암호화 과정과 해독화



〔그림 14〕 지문에서의 Fuzzy Vault 개요도

과정에서 사용된 두 지문이 동일인의 지문이고 정확히 정렬(align)이 되었다면 S'은 암호화한 비밀키와 일치할 것이다. 다른 지문의 경우에는 위장 점들의 영향으로 정확한 비밀 키를 얻을 수 없다.

이 방법의 장점은 생체의 특징정보가 위장 점들에 의해 은닉되어 있고 비밀키 또한 생체정보를 통해 은닉되어 있어, 볼트를 안다고 해도 두 정보를 얻어내기 힘들다는 점이다. 하지만 생체정보에는 잡음이 클 수 있고 사전에 두 생체정보가 정확히 정렬되어야 한다는 제약이 있다. 잡음의 영향이 크지 않다면 오류 정정 부호법을 통해 어느 정도 해결 가능하다. 지문이외에도 홍채, 얼굴, 타자 습관 등의 생체 정보를 이용한 예도 있다[29]. 생체 인식 연구 센터에서는 퍼지볼트가 가



〔그림 15〕 특징점 위치를 이용한 비밀 키 암호화 과정

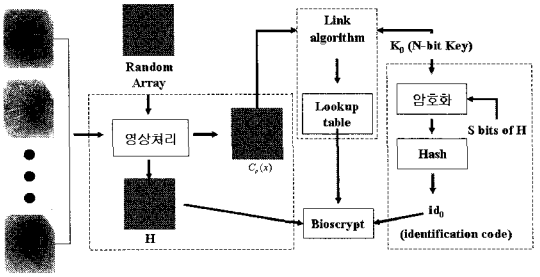
지는 생체 정보 정렬의 문제점을 해결하기 위하여 생체 정보 클러스터링 방법을 결합하여 홍채 영상으로부터 고유한 생체 키를 추출하는 연구를 진행 중이다[36]. 퍼지 볼트와 다른 방법으로 Bioscript에서 제안한 방법은 그림 16, 17과 같다[30]. 우선 암호화 과정에서는 다수의 생체영상($I_1, I_2, ..., I_N$)을 입력 받고 임의로 영상 R을 생성한다. 그리고 생체영상에 필터를 통과시켜 필터를 통과 시킨 영상 $C_o(x)$와 R이 유사하도록 필터 H를 설계한다. 그 후 해독화 과정에서는 암호화 과정과 마찬가지로 다수의 영상을 입력 받아 저장된 필터를 통과시켜 $C_1(x)$를 얻은 후 저장된 순람표를 이용해 비밀 키 K_1을 얻는다. 그러나 이러한 방법 역시 입력된 생체 정보의 정렬(alignment)이 키 코드 추출 성능에 상당히 중요하며, 이러한 문제점을 해결하기 위하여 생체 인식 연구센터에서는 격자 패턴(Lattice Pattern)을 이용한 생체 키 추출 연구를 진행하여 홍채 영상을 대상으로 16비트 코드 추출 시 약 4%의 에러 성능을 얻었다[37].

앞에서 언급한 퍼지볼트나 Bioscript가 제안한 방법 이외에도 에러 보정 코드만을 사용하여 암호화 하는 방법 등 다양한 방법들이 존재한다[31,32].

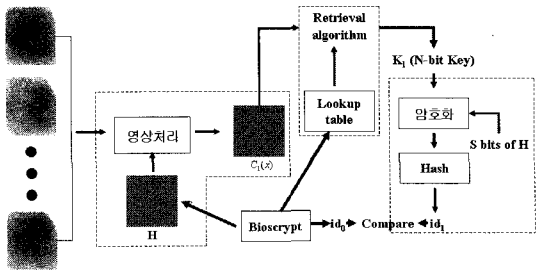
Ⅵ. 결 론

지금까지 생체인식 시스템에서 개인 정보보호를 위한 여러 가지 기술들을 살펴보았다. 우선 원래의 생체 정보의 유출을 막기 위해 생체정보 변환기술에 대해 소개하였고 원래의 생체정보가 유출되어 위조 생체가 만들어졌을 때 위조 생체를 검출하는 방법에 대해서 알아보았다. 또한 생체정보가 유출되거나 조작되었을 때 그 출처가 어디인지 혹은 조작여부를 알기 위한 워터마킹 방법 그리고 끝으로 생체정보를 이용하여 일반적인 암호화 알고리즘에 사용되는 키를 보호하는 방법에 대해서도 조사하였다.

개인 정보를 보호하기 위해서는 위에서 언급한 방법이 종합적으로 사용되어야 한다. 생체정보를 획득 후 저장 시에는 변환된 생체정보를 저장하고 이것이 유출되거나 조작될 수 있으므로 워터마크를 삽입하여야 한다. 또한 잔여지문과 같이 시스템으로부터 생체정보가 유출되는 것이 아니라 다른 경로로도 원래의 생체정보가 유출되어 위조생체와 같은 형태로 공격할 수 있으므로 입력 단에서는 위조생체를 검출하는 기능이 구현되어야한다. 그리고 정상적인 입력 단을 거치지 않고 우회적으로 공격할 수 있으므로 입력 단에 생체정보 변환알고리즘과 더불어 워터마크를 심거나 질의응답 방법에 의해 정상적인 경로로 생체정보가 들어왔는지를 점검해야 한다.



〔그림 16〕 Bioscript사의 생체 정보를 이용한 Key암호화 과정



〔그림 17〕 Bioscript사의 생체 정보를 이용한 Key해독화 과정

현재 국내외적으로 생체인식 시스템의 보급을 막는 가장 큰 요소 중의 하나는 개인 정보 보호 문제인데 본 논문에서 소개한 기술들의 개발을 통해 향후 생체인식 시스템의 안정성 문제를 해결할 수 있을 것으로 예상된다.

참 고 문 헌

〔1〕 N.K. Ratha, J.H. Cornell and R.M. Bole, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, Vol 40, No 3, pp. 614-634, 2001

〔2〕 G. Wolberg, "Image Morphing: A Survey," The Visual Computer 14, pp. 360 - 372, 1998

〔3〕 US Patent 6,836,554

〔4〕 Tee Connie, Andrew Teoh, Michael Goh, and David Ngo,"PalmHashing : A novel approach for cancelable biometrics", Information processing letters, Vol. 93, pp 1-5, 2005

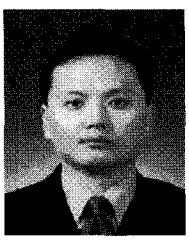
[5] S. Schuckers, "Spoofing and anti-spoofing measures", In Information Security Technical Report, volume 7, pages 56-62, 2002.
[6] T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned", In Smart Card Research and advanced Applications, pages 289-303, Kluwer Academic Publisher, 2000.
[7] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems", Proc. of SPIE, Optical Security and Counterfeit Deterrence techniques IV, Vol.4677, pp. 275-289, 2002
[8] M. Sandstrom, "Liveness Detection in Fingerprint Recognition Systems," Master's Thesis, Linkoping University, Linkoping, Sweden, June 2004
[9] ELFA. Factsheet - PCB production, 2004. Available at http://www.elfa.se/en/fakta.pdf(accessed on Dec. 5, 2004)
[10] US Patent 5,719,950
[11] R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners", Pattern Recognition, Vol. 36, pp. 383-396, 2003.
[12] S.A.C. Schuckers, S.T.V. Parthasaradhi, R. Derakshani, and L. A. Hornak, "Comparison of Classification Methods for Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices", Lecture Notes in Computer Science, Vol. 3072, pp. 256-263, 2004.
[13] S.A.C. Schuckers, and A. Abhyankar, "Detecting Liveness in Fingerprint Scanners Using Wavelets: Results of the Test Dataset", Lecture Notes in Computer Science, Vol. 3087pp. 100-110, 2004.
[14] L. Thalheim, J. Krissler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", c't magazine, November 2002
[15] T. Matsumoto, "Artificial Fingers and Irises: Importance of Vulnerability Analysis", 7th International
[16] J. Daugman, "Recognizing Persons by their Iris Patterns: Countermeasures against Subterfuge", Biometrics: Personal Identification in Networked Society, pp. 103-121.
[17] J. Daugman, "Iris Recognition and Anti-Spoofing Countermeasures", 7th International Biometrics Conference, 2004, London.
[18] http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf, (accessed on June 9, 2005)
[19] http://ppw.kuleuven.be/labexppsy/purkinje.htm, (accessed on November 3, 2005)
[20] Michael Arnold, Martin Schmucker and Stephen D. Wolthusen,"Techniques and Applications of Digital Watermarking and Content Protection", Artech House, 2003
[21] F. Hartung and M. Kutter, ""Multimedia watermarking techniques"", Proc. IEEE, vol. 87, no. 7, July 1999, pp.1079-1107.
[22] WSQGray-Scale Fingerprint Image Compression Specification, IAFIS-IC-0110 v2, Federal Bureau of Investigation, Criminal Justice Information Services Division (1993).
[23] M. Yeung and S. Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval", Journal of Electronic Imaging 9, No. 4, 468--476 (2000).
[24] A.K. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images", Proc. of Third Workshop on Automatic Identification Advanced Technologies (Auto-ID), pp. 97-102, Tarrytown, New York,

March 14-15, 2002.
[25] A. K. Jain, U. Uludag and R.-L. Hsu, "Hiding a Face in a Fingerprint Image", Proc. of ICPR, Quebec City, Canada, Aug., 2002.
[26] Jaehyuck Lim, Hyobin Lee, Sangyoun Lee, Jaihie Kim, "Invertible Watermarking Algorithmwith Detecting Locations of Malicious Manipulation for Biometric Image Authentication", LNCS on International Conference on Biometrics, Jan, 2006
[27] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", Proc. IEEE int'l. Symp. Information Theory, A. Lapidoth and E. Teletar, Eds., pp. 408, 2002.
[28] Umut Uludag, Shrath Pankanti, and Anil K. Jain, "Fuzzy Vault for Fingerprints", AVBPA 2005, LNCS 3546, pp. 310-319, 2005.
[29] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proc. IEEE, vol. 92, no. 6, pp. 948-960, 2004.
[30] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Vijaya, B., "Biometric Encryption: enrollment and verication procedures", Proc. SPIE Int. Soc. Opt. Eng., 3386 24-35 (1998)
[31] G. Davida, B. Matt, Y. Frankel, R. Peralta,"On the relation of error correction and cryptography to an offline biometric based identification scheme", Workshop on Coding and Cryptography, January, 1999, Paris, France.
[32] G. Davida, B. Matt and Y. Frankel, "On enabling secure application through off-line biometric identification", IEEE 1998 Symposium on Research in Security and Privacy, April 1998, Oakland, Ca.
[33] http://berc.yonsei.ac.kr (accessed on Nov. 14, 2005)
[34] Sungjoo Lee, Kang Ryoung Park, Jaihie Kim, "A Study on Fake Iris Detection based on the Reflectance of the Iris to the Sclera for Iris Recognition", ITC-CSCC 2005, pp. 1555-1556, Jeju, Korea, July 4-7, 2005
[35] Eui Chul Lee, Kang Ryoung Park, Jaihie Kim, "Fake Iris Detection By Using the Purkinje Image", Lecture Notes in Computer Science (ICBA'06), January 5-7, 2006
[36] 이연주, 이형구, 박강령, 김재희, "홍채 코드 기반 생체 고유키 추출에 관한 연구", 2005년 대한전자공학회 추계학술대회, 서울대학교, 2005. 11. 26
[37] Hyung Gu Lee, Seungin Noh, Kwanghyuk Bae, Kang Ryoung Park, Jaihie Kim"Invariant Biometric Code Extraction", 2004 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS'04), November 18-19, 2004, Seoul, Korea

〈著 者 紹 介〉

최 경 택 (Kyoungtaek Choi)
정회원

2001년 2월: 중앙대학교 전기전자공학부 졸업
2003년 3월: 연세대학교 전기전자공학부 석사
현재: 연세대학교 전기전자공학부 박사과정
〈관심 분야〉 인공지능, 영상처리, 생체인식(지문인식)



박 강 령 (Kang Ryoung Park)
정회원

1994년: 연세대학교 전자공학과 졸업
1996년: 연세대학교 전자공학과 석사
2000년: 연세대학교 전기·컴퓨터공학과 박사
2000년~2003년: LG전자기술원 홍채인식팀 선임연구원

현재: 상명대학교 미디어학부 조교수 및 생체인식연구센터 2총괄 책임자

김 재 희 (Jaihie Kim)
정회원

1979년: 연세대학교 전자공학과 졸업
1982년: 미국 Case Western Reserve University 전기 공학 석사
1984년: 미국 Case Western Reserve University 전기 공학 박사
현재: 연세대학교 전기전자공학부 교수
현재: 한국생체인식포럼 기술분과 위원장
현재: (과학기술부 지정) 생체인식 연구센터 소장