생체 정보 보호 기술

박강령 | 김재희
상명대학교 · 연세대학교

요 약

최근 생체 인식 시스템의 보급과 함께, 생체 인식 시스템의 인증 정확도 외에 생체 데이터와 생체 인식 시스템 자체의 보안성, 그리고 개인의 프라이버시 보호에 대해 요구가 증가되고 있다.

생체 데이터와 생체 인식 시스템의 보안성 증대를 위해서는 다양한 기술이 연구되고 있는데, 본 논문에서는 (과기부 지정 ERC) 생체인식센터에서 중점적으로 연구하고 있는 생체 정보 보호 기술에 대하여 소개한다. 이러한 생체 정보 보호 기술에는 생체정보가 도난 되었을 경우 그 피해를 최소화하기 위해 원래의 생체정보를 그대로 저장하는 것이 아니라 이를 바꾸어 변환된 생체정보를 저장하고 사용하는 생체정보 변환 기술이 있다.

또한, 원래의 생체정보가 유출되고 이를 이용하여 위조 생체 등을 만들어 공격할 경우를 대비할 수 있는 위조 생체 검출 기술이 있으며, 생체정보의 유출된 출처를 찾기 위해 생체정보에 소유 책임기관 등을 표시하는 데이터 은닉 기법이 연구되고 있다.

이 외에 생체정보를 이용하여 일반적인 암호화 알고리즘에 사용되는 키를 은닉하고 생체정보를 통해 인증된 사용자에 한하여 키를 사용하도록 하는 방법도 본 논문에서 소개한다. 끝으로 이러한 생체 정보 보호 기술을 이용하여 생체 인식 시스템의 보안성을 향상시키는 방법에 대하여 논의한다.

I. 서 론

사람의 생물학적 또는 행동학적 특징을 이용하여 개인을 인증하는 생체인식은 최근 전자상거래의 발달, 국제 테러 위협의 증가, 공공기관의 전자 행정화 등의 이유로 국내외적으로 활발히 연구되고 있다. 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 우리의 생활 속에 널리 퍼지면서 '과연 생체인식이 이상적이고 안전한 기술인가? 하는 생체인식 시스템의 보안성 및 개인의 프라이버시 보호에 대해 문제가 대두 되고 있다. 개인의 생체특징은 개인마다 다르다는 고유성(Uniqueness)과, 시간의 흐름에도 크게 변하지 않는다는 불변성(Permanence)의 특성으로 기존의 개인인증 방법인 비밀번호나 ID카드에 비해 안전하고 그 정확성의 장점으로 개인인증의 수단으로써 계속 사용 될 것이다. 하지만 이러한 생체인식 기술에도 보안상의 여러 허점들이 있고 이를 극복하기 위해 많은 연구가 진행되고 있다.

일반적인 생체 인식 시스템은 (그림 1)과 같이 크게 4개의 부분으로 구분될 수 있다[40]. 우선 생체정보를 취득하는 입력부가 있고 취득된 생체정보에서 인식에 사용되는 특징을 추출하는 부분이 있으며, 특징 및 개인의 정보 등을 저장하

본 연구는 과학기술부 지정 한국과학재단 생체인식 연구센터(BERC)의 지원으로 수행 되었습니다.

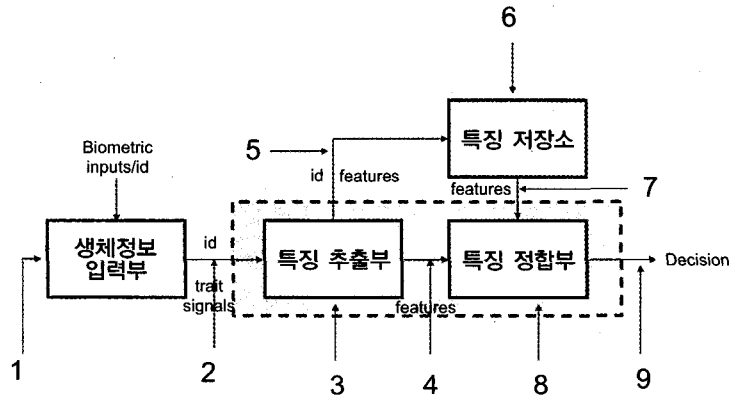
는 저장소 그리고 인증 과정 시, 저장소의 특징과 새로 입력된 특징을 비교하는 특징 정합부로 구성된다. 이러한 생체인식 시스템의 보안상의 허점은 9가지로 분류 될 수 있으며 각 허점의 공격 포인트는 그림 1에 나와 있고 그 내용은 다음과 같다[1][40].

1. 위조된 생체(Fake Biometric Data)를 입력하여 시스템을 기만하는 방법
2. 공격자에의해 불법 취득한 생체정보를 재생(Replay)하는 방법
3. 위조된 특징을 임의로 생성하여 특징 추출 부를 공격하는 방법
4. 임의의 위조된 특징을 전송, 시스템의 정합 오류를 유도하는 방법
5. 생체데이터의 저장소로 전송되는 생체 특징 정보나 개인정보를 절취 또는 타인의 정보로 대체하는 방법
6. 생체데이터의 저장소에 침투하여 기 저장된 생체 데이터를 조작, 삭제, 절취하는 방법
7. 생체데이터의 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

전술한 허점들 중에 3, 4, 8, 9와 같이 악의적인 프로그램에 의해 시스템의 오판을 유도하는 방법들은 생체인식 기술이 아닌 다른 일반적인 정보보호 기술에서도 문제가 되고 있고, 이를 막기 위한 연구가 해당 분야에서 현재 진행되고 있다. 또한 이러한 악의적인 프로그램에 의한 문제들은 생체인식 기술의 가장 큰 취약점인 개인 정보(Privacy)의 유출이나 오용과는 직접적인 관련이 없기 때문에 본 논문에서는 다루지 않는다[40].

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 갖고 있어서 이러한 정보가 유출되고 타인에 의해 악용되었을 경우에는, 쉽게 변경할 수 있는(Changeable) 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 1)의 6 공격에 대한 대비책으로 생체정보를 저장 시 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 사용



(그림 1) 생체인식 시스템의 개요도 및 보안상의 취약점[40]

자는 변환된 생체정보를 폐기하고 다시 새로운 변환된 생체정보를 생성하여 사용함으로써 생체정보 유출에 의한 피해를 최소화 할 수 있다. 다음은 (그림 1)의 1공격에 대한 대비책으로 위조 생체를 막는 방법(Fake Biometric/Liveness Detection)이 있을 수 있다[40].

이와 같은 생체정보의 유출은 실제 동작중인 생체인식 시스템에서 일어날 수도 있지만 일반 생활에서도 발생할 수 있다. 가령 지문 같은 경우는 컵이나 유리등의 물건에 잔여지문(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 검출 기술이 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[40].

본 논문에서는 생체인신센터에서 중점적으로 연구하고 있는 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 개인정보를 보호할 수 있는 지침을 제시하고자 한다.

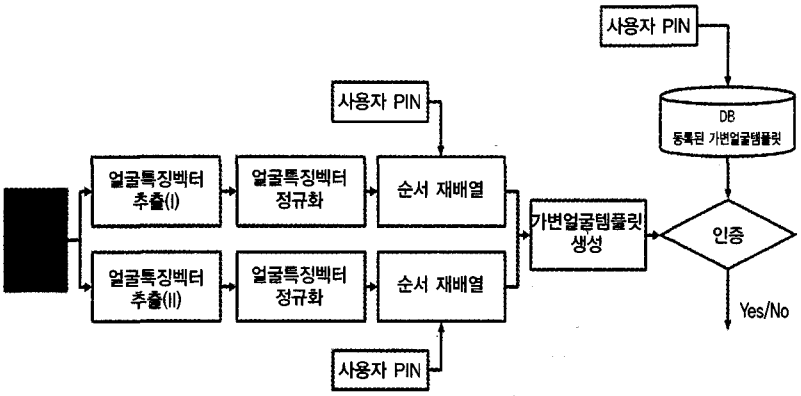
본 논문의 구성은 다음과 같다. 2장에서는 생체정보 변환기술, 3장에서는 위조생체 검출기술, 4장에서는 데이터 은닉기법, 5장에서는 생체 코드 추출방법 등에 대해 기술하고 끝으로 마지막 장에 개인정보 보호를 위해 취할 수 있는 종합적 대책에 설명한다.

II. 생체정보 변환기술 (Changeable Biometrics)

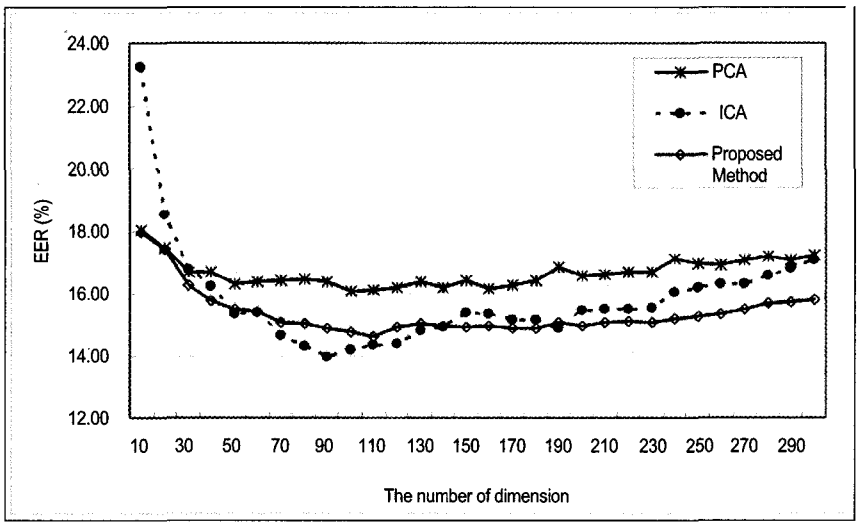
생체정보가 개인 인증의 수단으로써 사용될 수 있는 가장 큰 이유는, 생체정보는 개인마다 다르다는 고유성(Uniqueness)과, 시간의 흐름에도 크게 변하지 않는다는 불변성(Permanence) 때문이다. 하지만 이러한 생체정보의 고유성과 불변성은 개인 생체정보의 도난이나 도용 시 심각한 프라이버시 침해의 문제를 야기할 수 있다. 전통적인 개인 인증 방법인 신분증이나 패스워드의 경우 도난이나 도용 시 새로운 신분증이나 패스워드를 재발급하면 문제를 해결 할 수 있으나, 생체정보의 경우 새로운 생체정보를 재 생성하는 것은 불가능하다. 또한 생체인식을 이용한 개인 인증방법이 활성화되면서 개인의 생체정보가 범죄수사와 같은 수사기관이나 은행 또는 기타 인터넷을 이용하는 다른 상업적인 기업체와 공유될 수 있고 이로 인해 개인의 생체정보가 도용될 수 있는 문제점이 있다. 이러한 문제점을 해결하기 위해 최근에 생체정보를 변환 후 변환된 생체정보를 이용해 개인을 인증 하는 변환생체인식(Changeable Biometrics)의 개념이 소개 되었다[1,3]. 이러한 가변생체인식이 만족해야 될 조건은 다음과 같다. i) 변환된 생체정보는 원 생체정보와 달라야한다(변환성). ii) 변환된 생체정보와 변환 방법을 알더라도 원 생체정보의 복원이 쉽지 않아야 한다(비가역성). iii) 다수의 변환된 생체정보의 생성이 가능해야 한다(재생산성). iv) 변환된 생체정보를 사용하더라도 인식성능의 저하가 적어야 한다. 이번 장에서는 얼굴특징 정보를 이용하는 가변 얼굴템플릿 방법[50]과, 정렬을 요구하지 않는 가변 지문템플릿 방법[51]에 대해 소개한다.

1. 가변 얼굴템플릿 생성방법

(그림 2)는 제안하는 방법의 전체과정을 보여준다. 제안하는 가변 얼굴템플릿은 두개의 얼굴특징벡터의 합으로 생성되는데, 두개의 얼굴특징벡터는 한 장의 입력 얼굴영상에서 서로 다른 통계적 형상기반의 얼굴특징추출 방법(PCA, ICA, NMF 등)에 의해 구해진다. 구해진 두 특징벡터는 우선 정규화(Normalization)되고 두 특징벡터 요소의 순서를 재배열시킨 후 합으로 가변 얼굴템플릿을 생성한다. 얼굴특징벡터의 정규화는 각 특징벡터를 각 벡터의 놈으로 나누어 주는 과정으로 두 얼굴특징벡터들의 요소 값의 범위를 비슷하게 만들어 합으로 생성된 가변 얼굴템플릿에서 원 얼굴특징벡터의 정보를 추출하기 어렵게 만들기 위해 실시하는 것이다. 얼굴특징벡터의 재배열은 다 수의 가변 얼굴템플릿의 생성을 위해 실시한다. 단순히 두 얼굴특징벡터들의 합으로



(그림 2) 가변 얼굴템플릿 생성방법[50]



(그림 3) 가변 얼굴템플릿 성능비교[50]

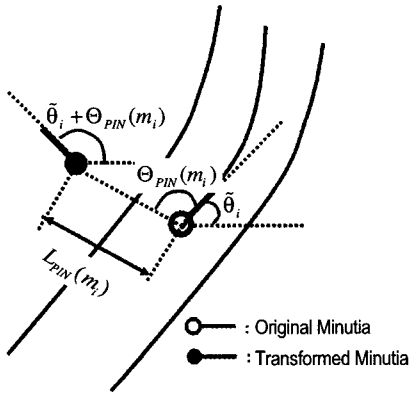
가변 얼굴템플릿을 생성할 경우 하나의 가변 얼굴템플릿만이 생성될 수 있다[50]. 이 경우 가변 얼굴템플릿의 도난 시 새로운 가변 얼굴템플릿으로 대치 될 수 없다. 이를 해결하기 위해 두개의 얼굴특징벡터를 합하기 전에 각 얼굴특징벡터의 요소를 서로 다르게 재배열시킨다. 재배열규칙은 사용자의 PIN(Personal Identification Number)에 의해 결정된다[50]. 그러므로 가변 얼굴템플릿의 도난 시 새로운 가변 얼굴템플릿은 사용자의 PIN을 변경시킴으로써 재 생성될 수 있고, 동일 사용자의 경우 같은 재배열 순서가 적용되고 타인 사용자와는 다른 재배열순서가 적용된다. (그림 3)은 제안한 가변 얼굴특징 벡터를 사용하는 경우와 원 원굴 특징벡터를 사용하는 경우의 EER(Equal Error Rate)를 보여준다. 실험결과는 변형 후에도 성능의 저하가 거의 없음을 보여준다[50].

2. 가변 지문템플릿 생성방법

기존의 가변 지문템플릿 생성 방법[1,3,49]은 특징점의 절대 적인 위치를 기준으로 새로운 위치의 지문 특징점을 갖는 템플릿을 생성하므로 동일 지문에 대해 동일한 가변 지문템플릿을 생성하기 위해 변환 전에 입력 지문영상의 정렬

이 반드시 요구되는 문제점이 있다. 제안 방법은 입력지문 영상의 정렬 없이 가변 지문템플릿을 생성하기 위해 각 특징점에서 입력지문의 이동 및 회전에 불변한 값 (Invariant Value)을 추출하고, 그 값을 기준으로 각 특징점의 이동 량을 결정한다. (그림 4)는 제안한 방법의 특징점 변경 방법을 보여준다.

원 특징점은 원 특징점의 방향 θ 을 기준으로 $\Theta_{PIN}(m_i)$ 의 방향으로 $L_{PIN}(m_i)$ 거리만큼 이동한다. 그리고 이동된 특징점의 방향은 원 특징점의 방향에 $\Theta_{PIN}(m_i)$ 더한 방향으로 설정한다. 이를 수식으로 표현 하면 수식 (1)과 같다[51].

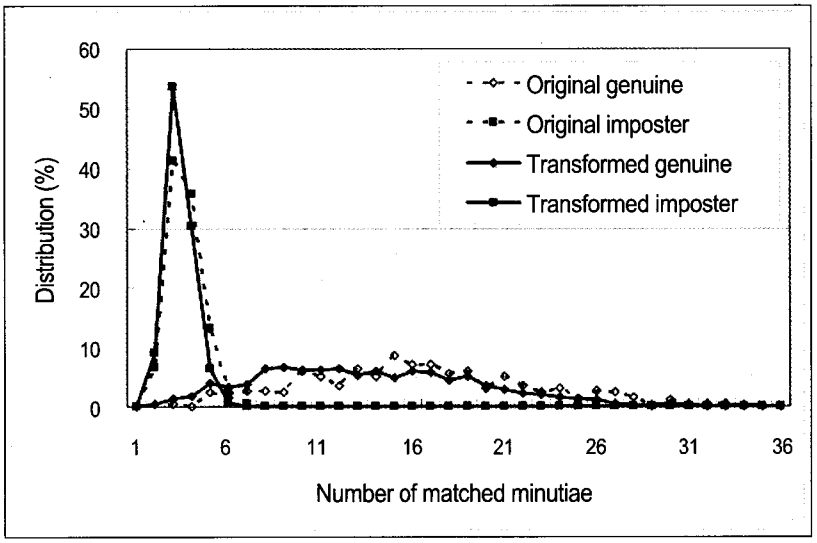


(그림 4) 지문 특징점 변환 방법[51]

$$\begin{aligned} x_i^c &= x_i + L_{PIN}(m_i)\cos(\tilde{\theta}_i + \Theta_{PIN}(m_i)) \\ y_i^c &= y_i + L_{PIN}(m_i)\sin(\tilde{\theta}_i + \Theta_{PIN}(m_i)) \\ \theta_i^c &= \theta_i + \Theta_{PIN}(m_i) \end{aligned} \quad (1)$$

여기서 x_i, y_i, θ_i 는 원 특징점의 x, y 좌표와 방향이고 x_i^c, y_i^c, θ_i^c 는 변형된 특징점의 x, y 좌표와 방향을 나타낸다. $L_{PIN}(m_i)$ 와 $\Theta_{PIN}(m_i)$ 는 거리 이동 량과 방향 이동 량을 나타내는데, 각 이동 량은 입력지문의 이동 및 회전에 불변한 값 m_i 을 두 변경함수 $(L_{PIN}(), \Theta_{PIN}())$ 의 입력으로 해서 그에 해당하는 출력으로 설정한다. 그러므로 지문템플릿의 도난 시 새로운 지문 템플릿은 두 변경함수를 교체함으로써 가능해진다. 각 특징점에서 입력지문의 이동 및 회전에 불변한 값은 특징점의 방향 정보와 특징점 주변의 방향정보를 이용하여 구하였고, 두 변경함수는 두 랜덤수생성기를 이용하여 생성하였다[51].

(그림 5)는 원 지문템플릿을 사용하는 경우의 본인 매칭 분포와 본인과 타인 매칭 분포, 변환된 지문템플릿을 사용하는 경우의 본인 매칭 분포와 본인과 타인 매칭 분포를 나타낸다. 변환된 지문템플릿을 사용하는 경우 성능이 약간 저하됨을 알 수 있다[51].



(그림 5) 본인 및 타인의 매칭 값 분포 비교[51]

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[40].

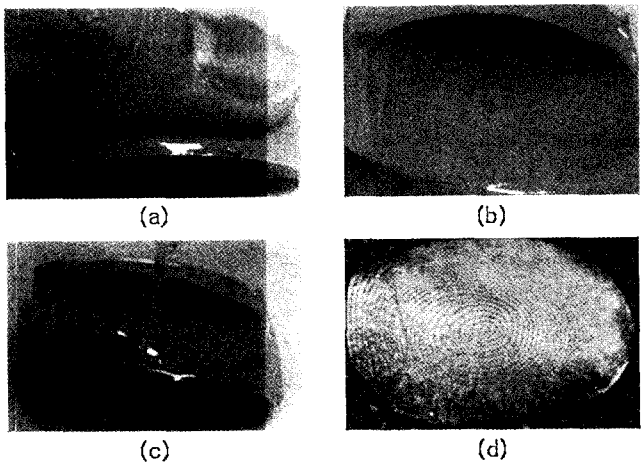
위조 생체를 생성하는 방법은 크게 2가지로 나누어질 수 있다. 첫째는 실제 소유자의 도움을 받아 생성하는 것이고 다른 하나는 유출된 생체정보(잔여지문, 홍채사진 등)를 통해서 생성하는 것이다. 이외에도 영화에서 나왔듯이 사람의 손가락을 자르거나 안구를 뽑아서 시스템을 기만할 수 있다[5,6].

세부적으로, 위조 지문을 생성하기 위해서는 시스템 사용자의 협조를 통하여 (그림 6(a))와 같이 사용자가 플라스틱, 찰흙 및 치과 인상 재료 등 지문의 융선과 골의 세밀한 형태를 나타낼 수 있는 틀을 만들고 그 틀에 젤라틴, 실리콘 및 찰흙 등을 주입하여 (그림 6(d))와 같은 위조 지문을 만드는 방법이 있다[40]. 그리고 또 다른 방법으로는 범죄 수사 시 사용하는 흑색의 고운 분말과 접착테이프 등을 이용하여 사용자의 잔여지문을 취득하고 그 잔여지문을 디지털 현미경 및 카메라로 취득하는 방법이 있다. 위 방법을 통하여 영상을 획득한 후 여러 가지의 영상 처리(노이즈 제거 및 영상 개선) 방법을 통하여 이를 필름에 인화하고 감광성의 PCB(Photosensitive Printed Circuit Board)에 부착 후 자외선을 조사하여 주형을 생성하게 된다. 이 주형에 젤라틴 및 실리콘과 같은 용액을 부어 위조 지문이 생성된다[7,8,9].

이러한 공격을 차단하는 위조 지문 검출방법(Liveness Detection)은 크게 2가지로 나눌 수 있다[40]. 첫 번째 방법은 추가적인 하드웨어를 사용하여 맥박이나 온도 및 피부의 전기적 저항과 같은 생체 고유의 특성을 측정하거나 위조 지문의 빛의 투과성 및 다양한 빛의 파장에 의해 반사된 영상을 분석하는 방법 등이 있다[6,7]. 좀더 자세히 살펴보면 부수적인 하드웨어를 이용하여 손가락에서 얻을 수 있는 생체정보로는 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[6,7]. 이 방법은 기존의 시스템을 교체해야 하므로 비용이 많이 들고 시스템의 크기가 커지는 단점이 있다. 두 번째 방법은 지문 인식 센서로부터 얻은 영상으로부터 실제 지문과 위조 지문의 차이를 탐지하는 방법이다. 이는 첫 번째 방법에 비하여 비용을 절감할 수 있고 또한 시스템의 크기를 줄일 수 있지만 인식 시스템의 알고리즘이 복잡해지는 문제점이 있다.

지문 센서에서 취득된 영상 정보만을 이용해 위조 지문을 검출하는 방법으로는 첫 번째로 센서에 지문을 접촉할 시 발생하는 변형이 실제 지문의 경우에는 사람 피부의 탄성에 의하여 지문의 각 부분마다 비선형적인 변형이 일어나지만 위조지문의 경우, 물질의 특성이 실제 피부와는 다르기 때문에 다른 형태의 선형적인 변형을 보인다는 점에 착안하여 이를 검출하는 방법이 존재한다[16]. 또한 실제지문의 경우에는 땀샘이 존재하지만 위조 지문 생성 과정에서는 이를 완벽히 복원할 수 없으므로 이를 검출하는 방법과 땀샘의 발한작용에 의해 시간의 변화에 따른 지문의 변화를 측정하는 방법들이 있다[11,12,13]. 마지막으로는 카메라를 이용하여 실제 지문의 피부 및 위조 지문의 재질의 차이를 고려한 위조 지문 검출 방법이 존재한다[17]. 하지만 땀샘의 발한작용은 수초의 측정시간을 요구하므로 사용자에게 불편함을 야기할 수 있으며, 지문의 변형 정보를 이용하기 위해서는 사용자의 상당한 협조를 필요로 하므로 이는 현실적으로 사용하기에는 어려움이 존재한다. 따라서 본 생체 인식 연구센터에서는 사용자의 편의를 고려하여 입력받은 한 장의 영상을 통하여 실제 지문을 판단 할 수 있는 지문 땀샘의 주기성 및 노이즈, 위조 지문의 형태 등 실제 지문과 구별되는 다양한 영상의 특성을 이용하여 위조 지문을 판별하는 연구를 수행하고 있다.

위조 홍채는 실제 사람의 홍채와 유사하게 인공적으로 제작된 홍채이다. 위조 홍채를 제작하는 방법은 (그림7(a))와 같이 고해상도 프린터로 홍채 영상을 프린트하는 방법, (그림 7(b))의 프린트된 영상과 투명한 콘택트렌즈를 결합하는

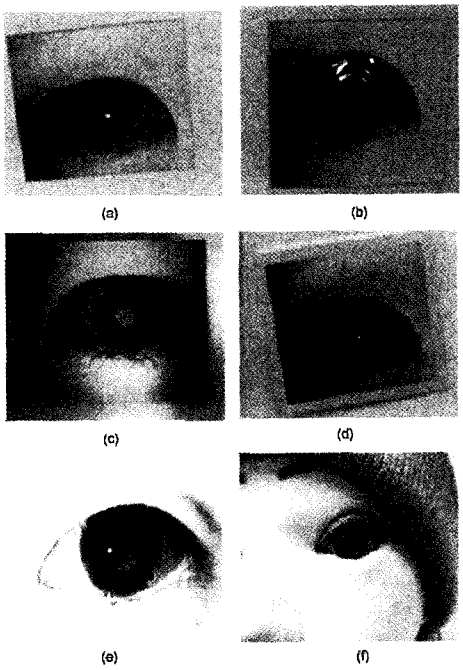


(그림 6) 사용자의 협조로 생성된 젤라틴 위조 지문[40]

방법, (그림 7(c))의 프린트된 영상의 동공을 뚫는 방법, (그림 7(d))의 사진으로 인화하는 방법, (그림 7(e))의 위조 홍채 패턴이 있는 콘택트렌즈를 착용하는 방법, 그리고 (그림 7(f))의 인공안구를 제작하는 방법 등이 있다[40].

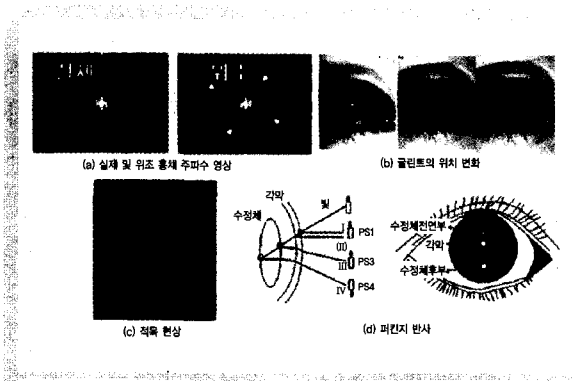
기존의 연구결과에 따르면 이러한 위조 홍채를 이용하여 상용화된 홍채 인식 시스템이 기만당할 수 있다는 사실이 밝혀졌다. L. Thalheim[38]과과 Matsumoto[39]는 프린트된 홍채 영상의 동공을 뚫어 상용화된 홍채 인식 시스템을 기만하였다. 즉, 기존의 홍채 인식 알고리즘은 본인과 타인을 구분하는 정확성은 높지만 실제 홍채와 위조 홍채를 정확하게 구분하지 못하는 문제점이 있다.

이러한 문제를 해결하지 위해 실제 홍채와 위조 홍채를 구분하는 연구의 필요성이 대두되었고, 많은 위조 홍채 검출 방법들이 제안되었다. (그림 8(a))와 같이 프린트한 영상에는 도트(dot)의 주기성이 존재함에 착안하여 이차원 푸리에 스펙트럼(Fourier spectrum)분석을 이용한 위조 홍채를 검출하는 방법, (그림 8(b))의 여러 개의 LED를 임의로 번갈아 키면서 글린트의 위치 변화로 검출하는 방법, (그림 8(c))에서와 같이 눈의 적목 현상(Red Eye Effect)을 이용하는 방법, (그림 8(d))의 각막의 외막과 내막 및 수정체의 외막과 내막의 굴절률 차이에 의한 퍼킨즈(Purkinje) 반사현상을 검출하는 방법, 빛의 세기에 따른 동공의 확대 축소를 검출하는 방법 그리고 눈꺼풀의 깜박임을 검출하는 방법 등이 있다[40, 41,42]. 생체인식연구센터에서는 홍채 및 공막에서 적외선



(그림 7) 다양한 위조 홍채 영상[40]

조명의 반사차이 및 퍼킨즈 반사를 이용하여 위조 홍채를 판별하는 연구를 진행하고 있으며, 특히 홍채 및 공막에서 적외선 조명의 반사차이를 이용하는 방법에 의해 프린트 홍채, 인공안구 및 위조 컨텍트 렌즈 등 다양한 종류의 위조 홍채를 오류 없이 검출해 낼 수 있었다[34][35][43].



(그림 8) 다양한 위조 검출 방법[40]

위조 지문이나 위조 홍채 이외에도 변장이나 성형에 의한 위조 얼굴, 혹은 성대모사와 같은 위조 음성 등의 위조 생체가 있을 수 있지만 지문이나 홍채에 비해 활발히 연구되지는 않았다. 이중 위조 얼굴에 대한 검출 연구는 3D 얼굴 정보 및 얼굴에서의 조명 투과율을 이용한 방법에 의해 생체인식 연구센터에서 활발히 연구 진행 중이다.

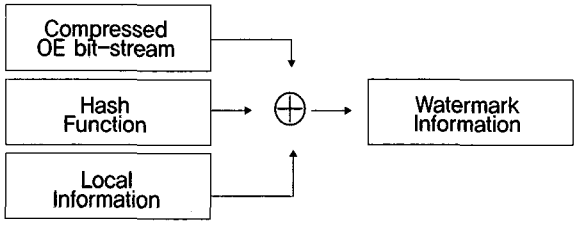
IV. 데이터 은닉기법(Watermarking)

생체인식 기술의 폭넓은 활용을 위해서는 생체 영상의 보안성을 높일 필요가 있다. 그 방법으로 암호화와 디지털 워터마킹 기술 두 가지가 있다. 암호화는 정보를 기호화하여 권한이 없는 자에게는 의미 없는 정보로 만드는 방법이며, 디지털 워터마킹 기술은 소유정보를 생체 영상에 삽입하여 정당한 지적 소유권을 보호하거나 또는 그 영상을 무결성을 인증한다. 암호화의 경우는 복호키를 이용하여 복호화 된 이후의 데이터에 대해서는 어떠한 보안성도 가지지 않는다. 따라서 복호화 된 데이터 또는 복호화에 필요한 복호화 키가 유출될 수 있기 때문에 복호화 이후에도 보안성을 유지하려 한다는 측면에서 암호화는 생체영상의 보안성을 끝까지 보장할 수 없다. 암호화-복호화 과정이 없는 워터마킹은 생체영상의 불법적인 사용에서 또 다른 방어가 가능하다.

본 알고리즘은 생체영상의 보안성을 높이기 위하여 워터마킹을 사용하였으며, 워터마킹을 이용하여 원본영상의 인증을 하였다. 그리고 인증이 되었을 경우 원본영상으로 완벽한 복원이 가능하며 기존의 워터마킹과는 달리 더 나아가 인증이 되지 않았을 경우, 즉 원본 생체영상이 조작되었음을 확인하면 그 위치까지 찾을 수 있도록 구현되었다.

1 데이터 삽입 방법

알고리즘은 (그림 9)에서와 같은 방법으로 삽입될 워터마크를 생성한다. 영상을 블록 단위로 나누어 각 블록에 심볼 결정 함수를 적용 O(odd), E(Even)의 블록으로 이름 짓는다. 모든 블록에 이처럼 적용하면 O, E로 이름 지어진 0과 1의 비트 스트림을 얻을 수 있다. 이 비트 스트림을 이용하여 무손실 영상압축을 하게 되면, 원본영상의 정보를 그대로 가지고 있으며 부가적인 정보, 즉 워터마크를 삽입할 수 있는 공간을 만들 수 있다.



(그림 9) 워터마크 정보 생성 개념도[44]

영상의 인증 여부를 결정짓기 위해 원본 영상에 해쉬(Hash) 함수를 적용하여 128 비트의 고유 정보를 생성한다. 해쉬 함수의 특성상 모든 영상은 다른 해쉬 값을 가지게 되면 이 경우 다른 두 영상이 같은 해쉬를 가질 확률은 $1/2^{128}$이 된다.

인증 이후 영상에 조작이 가해졌다고 판단이 되면 그 위치를 찾을 수 있도록 하기 위해 원본영상의 지역정보를 삽입한다. 즉, 8x8 블록 단위로 블록 내부의 비트화 된 심볼의 개수를 이용하여 패리티 비트를 생성한다. 생성된 패리티 비트를 이용하여 패리티 비트의 사용 개수에 따라 1비트를 사용했을 경우 (그림 2)에서와 같이 1/2의 확률로 조작위치 여부를 판단할 수 있다[44].

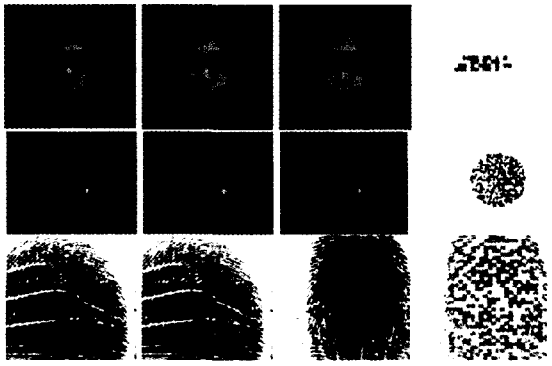
2. 데이터 추출 방법

워터마크를 추출하는 과정은 삽입하는 과정과 거의 동일하다. 블록단위로 OE - 비트 스트림을 뽑아낸 후 무손실 영

상압축 기술로 복원한다. 복원된 원본 영상과 입력된 영상의 해쉬 값 비교를 통하여 영상의 인증여부를 판단한다. 물론 인증이 되지 않는다면 영상에서 지역정보를 추출하여 조작된 위치를 파악할 수 있다[44].

3. 실험결과

(그림 11)은 제안된 알고리즘을 얼굴, 홍채, 지문 등의 생체 영상에 적용하여 실험한 결과이다. 원본영상과 워터마크가 삽입된 영상을 비교해 보면 두 영상의 차이를 알 수 있다. 즉, 워터마크는 LSB(Least Significant Bit)를 이용하여 삽입하기 때문에 영상에서 차이를 느낄 수가 없다. 이것은 워터마크의 비가시성을 잘 가지고 있음을 확인할 수 있다. (그림 10(c))의 경우 얼굴은 눈 부분을, 홍채는 홍채의 패턴영역을, 지문은 전체적인 바꿔치기를 가해보았다. 그 결과 모두 인증이 되지 않았으며, (그림10(d))에서와 같이 조작된 위치를 찾을 수 있었다[26][44].

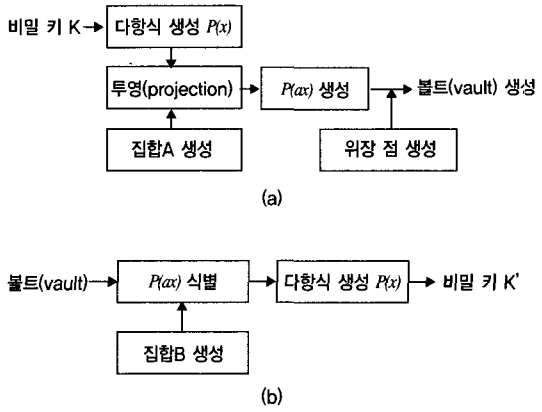


좌측에서부터 (a)원본영상 (b)워터마크된 영상
(c)공격 받은 영상 (d)공격 위치 검출
(그림 10) 실험 결과 영상[40]

V. 생체 키 생성방법 (Biometric key Generation)

생체 키 생성은 생체정보를 이용하여 암호화 알고리즘에 사용하는 비밀 키를 안전하게 관리하고 생성하는 방법이다. 생체 키 생성의 대표적인 방법으로 퍼지 볼트(fuzzy vault)방법이 있다.

퍼지 볼트방법의 암호화(encoding) 과정과 복호화(decoding) 과정은 (그림 11)과 같다. 먼저 암호화 과정에서는 생체정보를 이용하여 비밀 키를 은닉한다. (그림 11(a))와 같이 비밀 키로부터 다항식 P(x)를 생성하고 생체의 특징 정보로 이루어진 집합 A (A={a1, a2, ..., an})를 다항식에 투영하여 P(ai)를 얻는다. 비밀 키와 홍채특징정보가 결합된 P(ai)를 위장 점들(chaff points)을 이용하여 은닉시키고 마지막으로 볼트(vault)를 생성한다. 비밀 키를 생성하기 위해서는 암호화 과정에서 얻어진 볼트와 재입력된 사용자의 생체정보인 집합 B가 사용된다. 이 때 집합 B가 집합 A와 매우 비슷하면 집합 B로 볼트에 있는 P(ai)를 위장 점들로부터 식별하고 이 점들로부터 다항식을 재생성하여 최종적으로 비밀 키를 얻는다. 그러나 집합 B와 집합 A가 크게 다르면 위장 점에 의해 다른 다항식을 재생성함으로써 비밀 키를 얻어내지 못한다[45].

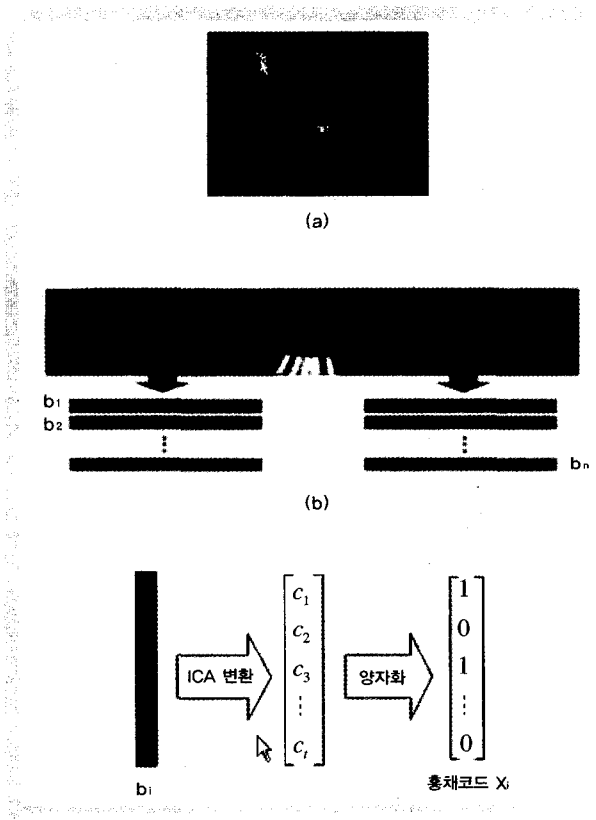


(그림 11) 퍼지 볼트 시스템 블록도: (a) 암호화 과정
(b) 복호화 과정[36][47][48].

이 방법은 생체의 특징 정보와 비밀 키가 함께 은닉되어 두 정보를 동시에 보호할 수 있는 장점을 갖는다. 또한 오류정정부호를 통해 생체정보의 잡음문제를 어느 정도 해결할 수 있다. 하지만 실제로 생체정보의 잡음이 미치는 영향은 비교적 크다. 따라서 생체정보와 퍼지 볼트를 결합하기 위해서는 생체 특징정보들이 정확히 정렬되도록 하는 방법이 요구된다[36][47][48]. 기존에 지문에 대한 연구를 시작으로 그 밖에 얼굴, 홍채, 타자 습관과 같은 생체 정보의 정합문제

를 해결하여 퍼지 볼트와 결합하기 위해 많은 노력을 기울이고 있다. 특히, 홍채는 다른 생체 정보들보다 타인과의 구분력이 뛰어난 것으로 인정받고 있어 퍼지 볼트에 적용할 경우 시스템의 성능 향상이 기대되어 홍채에 대한 연구가 주목을 받고 있다.

홍채를 이용한 연구에서는 집합 A 또는 집합 B를 얻기 위해 홍채의 특징정보를 추출하는 여러 알고리즘들 중 독립성분분석(ICA) 방법을 이용한 홍채특징 추출 알고리즘을 사용하였다[46]. 그 이유는 ICA 변환 방법은 홍채 패턴의 지역적 특성을 고려하여 여러 개의 홍채코드를 생성하므로 집합 A 또는 B가 여러 개의 서로 다른 성분들로 이루어져야 한다는 조건에 만족하기 때문이다[4]. 또한 ICA 변환 방법에 의한 인식성능이 홍채인식 알고리즘의 대표적 방법인 Daugman이 제안한 알고리즘의 성능과 비슷하기 때문이다[46][47].



(그림 12) 입력된 홍채 영상으로부터 홍채코드를 생성하는 과정: (a) 입력된 눈 영상에서 홍채영역 검출 (b) 정규화 된 홍채영상의 선택된 두 영역에서 여러 개의 하위 홍채영상 블록을 얻어냄 (c) 각 하위블록 bi는 ICA 변환을 통해 홍채코드 xi가 됨[48][52].

홍채코드 집합을 생성하는 방법은 다음과 같다. 우선 사용자의 눈 영상을 획득하고 눈 영상에서 (그림 12(a))와 같이 홍채 영역만을 검출한다. 검출된 홍채 영역은 극 좌표계로 변환되어 정규화된 직사각형 모양의 영상이 된다. (그림 12(b))와 같이 정규화된 홍채 영상에서 눈꺼풀과 조명반사에 의한 영향이 적은 두 영역을 선택하고, 각 영역을 여러 개의 블록으로 분할한다. 각 하위 블록들은 ICA 변환을 통해 홍채코드들을 생성한다[2]. 이러한 홍채코드들은 환경 변화에 의한 잡음을 갖고 있기 때문에 클러스터링(clustering) 방법[48][52]을 사용하여 잡음을 줄여준다. 최종적으로 얻어진 n개의 홍채코드들은 집합 A 또는 집합 B의 성분이 된다[47][48].

실험결과, 128비트의 생체키를 생성하는데 평균 0.356%의 TER(Total Error Rate)이 발생함을 알 수 있었다.

여기서 TER이란 FAR(False Acceptance Rate : 타인의 홍채데이터로부터 본인의 생체 키가 나올 오류률)과 FRR(False Rejection Rate : 본인의 홍채데이터로부터 본인의 생체 키가 나오지 않을 오류률)의 합으로써, 이러한 TER이 최소가 되는 순간의 에러률을 측정한 것이다[52].

VI. 결 론

본 논문에서는 생체인식센터에서 중점적으로 추진하고 있는 생체인식 시스템에서의 개인 정보보호를 위한 여러 가지 기술들을 살펴보았다.

개인 정보를 보호하기 위해서는 본 논문에서 언급한 방법이 종합적으로 사용되어야 한다. 생체정보를 획득 후 저장 시에는 변환된 생체정보를 저장하고 이것이 유출되거나 조작될 수 있으므로 워터마크를 삽입하여야 한다. 또한 잔여 지문과 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 입력단에 생체정보 변환알고리즘과 더불어 워터마크를 심거나 질의응답 방법에 의해 정상적인 경로로 생체정보가 들어왔

는지를 점검해야 한다[40].

본 논문에서 소개한 생체 정보 보호 기술을 통해 향후 생체 인식 시스템의 안정성 문제를 해결할 수 있으며, 이를 통해 생체 인식 시스템의 대중화에 크게 기여할 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 2007.04.10)

[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] Athos Antonelli, Raffaele Cappelli, Dario Mario, and Davide Maltoni, "Fake Finger Detection by Skin Distortion Analysis", IEEE Trans. Information forensics And Security, VOL.1, NO.3, Sep 2006

[17] Y. S. Moon, J. S. Chen, K. C. Chan, K. So, K. C. Woo, "Wavelet Based Fingerprint Liveness Detection", IEE Electronics Letters, Vol. 41, No. 20, pp.1111-1112, Sept. 2005

[18] http://www.cl.cam.ac.uk/users /jgd1000/countermeasures.pdf, (accessed on 2007.04.10)

[19] http://ppw,kuleuven.be/labexppsy/purkinje.htm, (accessed on 2007.04.10)

[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-0110v2, 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 (AutoID), 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 2007.04.10)

[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 추계 학술대회, 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

[38] L. Thalheim, J. Krissler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", c' t magazine, November 2002

[39] T. Matsumoto, "Artificial Fingers and Irises: Importance of Vulnerability Analysis", 7th International

[40] 최경택, 박강령, 김재희, "Biometric system에서의 Privacy보호기술", 정보보호학회지, 2005년 12월호

[41] J. Daugman, "Recognizing Persons by their Iris Patterns: Countermeasures against Subterfuge", Biometrics: Personal Identification in Networked Society, pp. 103-121.

[42] J. Daugman, "Iris Recognition and Anti-Spoofing Countermeasures", 7th International Biometrics Conference, 2004, London.

[43] S. Lee et al., "Robust Fake Iris Detection Based on Variation of the Reflectance Ratio between the Iris and the Sclera," Proc. of Biometrics Symposium 2006, Sept.

19 ~ 21, 2006.

[44] 임재혁, 이효빈, 이상윤, "생체정보 저작권 보호 및 유출 방지 알고리즘", 제 5 회 BERC 생체인식워크샵 2007년 2월 1일-2일

[45] A. Juels and M. Sudan, "A fuzzy vault scheme," ACM Conference on Computer and Communications Security, CCS 2002.

[46] K. H. Bae, S. I. Noh and J. H. Kim, "Iris Feature Extraction Using Independent Component Analysis," LNCS on Audio-and Video-Based Biometric Person Authentication, Vol. 2688, pp. 838-844, 2003.

[47] 이연주, 이형구, 박강령, 김재희, "홍채 코드 기반 생체 고유키 추출에 관한 연구", 2005년 대한전자공학회 추계 학술대회, 서울대학교, 2005. 11. 26

[48] 이연주, 박강령, 김재희, "퍼지볼트 기반의 암호 키 생성을 위한 불변 홍채코드 추출," 2006년 대한전자공학회 하계학술대회, 29권 1호, 2006.

[49] R. Reiand LukeMcAven, "Cancelable Key-Based Fingerprint Templates," Information Security and Privacy: 10th Australasian Conference, ACISP, pp. 242-252, 2005.

[50] M. Jung, C. Lee, J. Kim, J. Choi, J. Kim, "A Changeable Biometric System for Appearance-based Face Recognition," Biometric Consortium Conference (BCC 2006), Baltimore, USA, Sept. 19-21, 2006.

[51] Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh, Sangyoun Lee, and Jaihie Kim, "Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information," IEEE Transactions on Systems, Man and Cybernetics -Part B, Special Issue on Recent Advances in Biometrics Systems, October, 2007.

[52] Youn Joo Lee, Kwanghyuk Bae, Sung Joo Lee, Kang Ryoung Park, Jaihie Kim, "A New Method for Generating Invariant Iris Cryptographic Key Based on Fuzzy Vault Scheme", IEEE Transactions on Systems, Man and Cybernetics -Part B, submitted.

약 력

박 강 령

1994년 연세대학교 전자공학과 졸업
1996년 연세대학교 전자공학과 석사
2000년 연세대학교 전기 · 컴퓨터공학과 박사
2000년 ~ 2003년 LG전자기술원 Digital Vision 그룹 선임연구원
현재 상명대학교 디지털미디어학부 조교수 및 생체인식연구센터 2총괄 책임자

김 재 희

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
한국생체인식포럼 의장
대한전자공학회 수석부회장
(과학기술부 지정) 생체인식 연구센터 소장