情 報 保 護 學 會 誌
第 15 卷 第 6 號, 2005. 12

워터마킹 기법을 이용한 생체정보 보호

김 태 해*, 정 승 환*, 정 용 화*, 문 대 성**, 문 기 영**

요 약

21세기를 맞이하면서 정보통신기술의 발전과 인터넷 이용 확산 등으로 사용자 인증이 중요한 문제로 대두되고 있다. 패스워드 또는 PIN(Personal Identification Number)을 이용한 사용자 인증 방법이 현재까지 널리 쓰이고 있으나 타인에게 노출되거나 잊어버리는 등의 문제점이 있다. 이러한 문제를 해결하기 위하여 개인의 고유한 생체정보를 이용한 주요 정보 보호 및 사용자 인증 등의 연구가 활발히 진행되고 있다. 그러나 이러한 생체인식 기술을 대규모 응용에 적용하기 위해서는 생체정보의 안전한 저장/전송/처리 등 생체정보 보호에 대한 연구가 필수적이다. 본 고에서는 디지털 컨텐츠 보호에 사용되는 워터마킹 기법을 이용하여 이러한 생체정보를 보호하려는 경우 발생하는 이슈와 관련 연구 동향을 소개한다.

Ⅰ. 서 론

최근 21세기 정보의 시대는 인터넷 보급 등으로 인하여 원하는 정보를 수집, 분석, 가공 등이 편리하게 되었다. 그러나 인터넷을 이용하여 글로벌 네트워크가 형성되어 편리하게 수집, 분석 및 가공한 개인의 중요한 정보가 타인에 의해 도용되거나 파괴되는 심각한 문제가 제기되고 있다. 이는 개인의 정보만이 손실되는 것이 아니라 국가의 중요 정보와 전자상거래 등의 경제 활동에 필요한 정보도 손실되는 현상이 발생되고 있는 현실이다. 그러므로 현재까지 사용되고 있는 사용자 패스워드 또는 PIN(Personal Identification Number)만을 이용한 사용자 인증 방법으로는 개인, 산업, 국가의 중요 정보를 안전하게 보관할 수 없는 실정이다. 이러한 문제를 해결하기위해 최근 들어 개인의 고유한 생체정보인 신체적 또는 행동학적 특징에 따라 사람들의 신원을 확인하는 바이오메트릭 즉, 생체인식 기술이 대두되고 있다.

"자동화된 특정 개인의 소추된 특성을 인증하거나 신분을 인식하기 위해, 측정 가능한 특성 또는 개인의 특징을 연구하는 학문"으로 정의되는 생체인식의 예로는 지문, 음성, 얼굴 모양, 홍채 패턴, 손의 형태, 손등의 정맥 분포 등 아주 다양하며, 이들은 신체의 일부분이거나 개개인의 행동 특성을 반영하므로 잊어버리거나 타인에게 대여 혹은 도난 복사가 되지 않는다. 즉, 타인이 지문 혹은 홍채 패턴을 훔쳐갈 수 없고 개인은 지문이나 홍채 패턴 등을 망각할 수 없으며, 집에 두고 올 수도 없다는 것이다. 그러므로 안전한 정보보안을 위한 분야로 활발하게 연구가 진행되고 있다[1-2].

그러나 생체인식 기술이 이러한 장점이 있지만 사용자 인증을 위해 저장된 생체정보가 타인에게 도용된다면 패스워드나 PIN과 달리 변경이 불가능하므로 심각한 문제를 일으킨다. 생체정보의 안전한 보관을 위해 최근에는 보안토큰(스마트카드 또는 USB 토큰), PDA 등의 개인기기에 저장하는 연구도 활발하지만, 원격 인증 분야 등에서는 완벽한 보안을 제공하지 못한다. 생체인식 기술이 도어락, PC 보안 등 standalone형 소규모 응용에 성공적으로 적용됨에 따라, 다음 단계인 전자정부/전자거래 등 네트워크를 이용한 원격 응용에 적용되기 위해서는 생체정보 보호/관리에 대한 기술 연구가 필요한 실정이다. 또한 네트워크를 이용한 비대면 응용에 적용되기 위해서는 개인의 프라이버시 보호를 위한 생체정보의 안전한 저장/전송/처리 기술이 필요하다. 그리고 생체정보의 상호운용성 보장을 위한 표준화 작업이 급진전되고 있으므로, 생체정보 오남용에 의한 피해를 막기 위한 연구가

* 고려대학교 컴퓨터정보학과 ({taegar, sksghksl, ychungy}@korea.ac.kr)
** 한국전자통신연구원 ({daesung, kymoon}@etri.re.kr)

필요하다.

언급한 것과 같이 원격응용을 위한 기존의 비밀번호 보호/위변조 탐지/대응 기술에 상응하는 생체정보 보호/관리 기술 개발이 필요하므로, 본 고에서는 생체정보를 이용한 인증 시스템의 취약점을 분석하고 이를 해결하기 위하여 컨텐츠 보호에 사용되는 워터마킹 기법을 이용하는 경우 발생하는 이슈들과 관련 연구 동향을 설명한다.

Ⅱ. 생체 인식시스템의 취약점

그림 1은 전형적인 생체인식 시스템에서의 가능한 공격 포인트를 보여주고 있는데, 이를 간단히 살펴보면 다음과 같다.

① 사용자로부터 신호를 얻는 부분으로, 센서에 가짜 지문이나 복사한 서명, 얼굴 사진 등을 이용하는 경우이다.

② 미리 저장해둔 생체 신호를 다시 사용하는 경우로, 센서를 바이패스(bypass)하고 지문의 복사본이나 오디오 신호를 전송한다.

③ 침입자가 원하는 특징을 생성하도록 트로이 목마 등을 이용하여 특징 추출단을 공격한다.

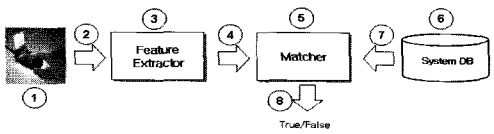
④ 생체인식 시스템의 특징 표현법을 알고 있을 때 이를 임의로 변경하는 경우로, 특징추출과 정합이 한 단계로 이루어지면 어느 정도 해결할 수 있으나, 인터넷으로 특징점이 전송되는 경우에는 TCP/IP에 대한 스누프(snoop)를 통하여 패킷을 변경할 수도 있다.

⑤ 정합단 자체를 공격하여 미리 선택된 정합 결과가 나오도록 하는 경우로, 아무리 정합알고리즘이 정확하더라도 원하지 않는 결과가 나오게 된다.

⑥ 템플릿이 저장된 데이터베이스를 공격하여 저장된 템플릿을 변경하는 경우로, 특히 템플릿이 분산 저장된 경우에는 그 중에 일부 혹은 전체를 변경함으로써 타인 수락율이나 본인 거부율이 높아지는 현상을 초래할 수 있다.

⑦ 저장된 템플릿이 전송 채널을 통해서 정합단으로 전송될 때 채널을 공격하는 경우로, 전송되는 데이터를 가로채어 다른 형태로 변경함으로써 상이한 정합 결과를 초래한다.

⑧ 최종 판결을 공격하는 경우로, 아무리 실제 시스템이 우수하고 정확하다고 하더라도 정합결과가 공격을 당하면 아무런 의미가 없게 된다.



〔그림 1〕 생체인식 시스템에서 가능한 공격 포인트

위와 같이 여러 공격 포인트가 존재하며, 아울러 이러한 공격을 피해갈 수 있는 방안 또한 강구되어야 한다. ①번 공격 포인트에 대한 부분은 현재 일본 등에서 다각적으로 검토 연구되고 있다[3]. 실제 손가락을 이용한 방법 뿐 아니라 잔상 지문을 이용해서도 유사한 방법으로 가짜 지문을 만들 수 있다. 따라서 "가짜 지문 여부를 어떻게 판단 할 것인가?"라는 문제에 봉착하게 된다. 이의 해결 방법으로는 소프트웨어적 접근법과 하드웨어적 접근법이 있다. 소프트웨어적인 방법으로는 지문의 경우 땀샘, 얼굴의 경우 머리의 움직임, 홍채의 경우 눈의 움직임 등을 이용한다. 하드웨어적인 방법으로는 지문의 경우 손가락의 온도와 맥박을 측정하거나 전기적 특성을 이용하는 방법도 가능하다. 이들 방법을 잘 이용하면 완전하지는 않지만 센서단에서의 공격은 어느 정도 막을 수 있다. 암호화된 채널을 이용하면 공격 포인트 ④번에서의 원격공격은 막을 수 있다. 그리고 공격 포인트 ⑤, ⑥, ⑦에 대한 간단한 방어책은 정합단이나 데이터베이스를 안전한 곳에 설치하는 것이다. 일반적으로 ⑧번의 경우는 암호화를 통해서 공격을 막을 수 있다. 지금부터는 이들에 대한 예를 통해서 가능한 공격을 이해하고 대응방법에 대해서 논하기로 한다.

Ⅲ. 디지털 컨텐츠 보호를 위한 워터마킹 기법

1. 디지털 워터마킹 기법

워터마크의 역사는 고대 이집트에서도 찾을 수 있다. 파피루스를 이용해서 만드는 과정에 섬유질을 물에 풀었다가 압착하기 위해 틀을 사용하였는데, 워터마크간 물을 빼는 과정에서 자연 발생한 고유의 무늬를 지칭하는 것으로, 이후에 직접적으로 보이지는 않지만 변화 및 파손 없이 빛을 통해 확인할 수 있는 모양을 의미한다.

현재 워터마킹을 주로 활용하는 분야는 화폐제조 분야이다. 화폐에서 워터마킹을 하는 방법은 젖어있는 상태에서 고유의 워터마크를 인쇄하는 고도의 인쇄 기술이다. 이런 방식으로 인쇄된 지폐는 불빛을 통해 희미한 고유 마크를 확인 할 수 있으며 위조지폐의 진위

를 가릴 때 참고로 사용되어 진다. 하지만 일반적으로 워터마크는 사용자의 육안에서는 좀처럼 찾아보기 힘들어 내용을 숨기고 있다고 볼 수 있다.

아날로그에서 디지털로 시대가 변화함에 따라 많은 인쇄물들이 디지털화되어 인터넷을 통해 널리 이용되게 되었다. 이런 과정에서 저작물의 사용자 정보 등을 은닉하는 기술로 발전하게 되었다(물론 눈으로 볼 수 있도록 하는 경우도 있다.).

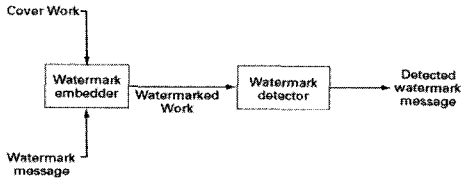
디지털정보는 손쉬운 접근과 활용이라는 특성 때문에 추가적인 문제가 발생하기도 한다. 대표적인 사례가 바로 저작권 문제이다. 디지털 컨텐츠는 복사할 경우 구분할 수 없는 또 하나의 원본이 쉽게 만들어지므로 원작자의 동의 없이 함부로 복제되거나 표절되기 쉽다. 더욱이 다른 사람의 아이디어가 담긴 각종 데이터를 복제하거나 변형해도 별다른 죄의식을 느끼지 않는다는 점이다. 나의 소중한 지적 재산에 내 것이라고 표시할 수 있는 방법은 없을까? 이런 고민에 대한 해답을 제시하기 위해 탄생한 것이 바로 디지털 워터마크이다.

2. 디지털 워터마킹의 요소

디지털 워터마킹은 디지털 컨텐츠에 워터마크 데이터를 삽입하는 것으로 삽입 시 필요로 하는 요소는 아래와 같다[4].

- Cover Work : 디지털 컨텐츠.
- Watermark Message : 삽입되는 워터마크 데이터.
- Watermarking Algorithm : 워터마크를 삽입과 탐지 및 복구에 사용되는 알고리즘.

그림 2는 워터마킹 기법을 흐름도로 표시 하였다. 보호해야 할 디지털 컨텐츠와 그 저작권 등을 명시한 워터마크 데이터는 워터마크 삽입 모듈에서 워터마킹된 디지털 컨텐츠를 생성을 한다. 탐지 시에는 워터마크 탐지 모듈에서 워터마크의 유무를 검사하게 되며 탐지 시 적합한 사용자만이 워터마크를 탐지, 복구 및 수정을 할 수 있다. 이를 위하여 일반적으로 공유된 워터마크 키가 사용된다.



〔그림 2〕 워터마킹 흐름도

워터마크 알고리즘은 아래와 같은 조건을 측정하여 해당 응용에 적합한 알고리즘을 사용하거나, 기존 알고리즘을 향상시켜 요구하는 조건을 충분히 만족시켜야 한다.

- Robustness: 수정이나 혹은 전송중의 오류 등 데이터가 변하지 않는 정도.
- Fragileness: 악의적인 공격에 의해 워터마크 데이터가 변하는 정도.
- Fidelity: 워터마크의 삽입으로 원본 영상의 가시적 변형 상태 정도.
- Data Payload: 워터마크의 삽입으로 인한 전체 적인 데이터 손실 비용.
- Blind or Informed Detection: 워터마크 복원 시 원본이미지의 필요 유무.
- Security: 삽입된 워터마크는 해당 사용자만이 추출을 할 수 있음.
- Modification Watermarks: 워터마크 데이터의 수 정 여부.
- Multiple Watermarks: 워터마크를 여러 개 삽입 가능 여부.
- Localization: 특정 위치 워터마킹 여부.
- Nonenviable: 워터마크를 가시적으로 확인 가능한지 여부.

위의 요소들은 해당 응용에 대해 최고의 성능을 가져야 한다. 하지만 리소스가 제한된 디지털 컨텐츠 안에서 모든 요소들을 최고의 성능을 발휘할 수가 없기 때문에, 각각의 요소들은 서로 어느 정도 trade-off를 통하여 최적의 성능을 유도해야 한다.

인터넷의 보급 확산으로 인한 DRM 기법의 수요가 증가되고 있다. 일반적으로 암호학 기법은 정보보호의 필수적인 요소이나, 암호학 기법을 이용하면 암호화된 데이터는 보호될 수 있지만 한번 복호화 된 데이터는 보호될 수가 없다. 따라서 암호학 기법만으로 DRM을 구성하기에 큰 취약점을 가지고 있다. 따라서 워터마킹 기법은 암호학의 단점인 복호화 된 데이터의 보호에 사용되어 정보보호를 더욱 완벽히 할 수 있다.

Ⅳ. 워터마킹 기법을 이용한 생체정보 보호

1. 생체정보 상의 데이터 은닉

생체정보의 위변조 방지를 위해 생체정보에 추가

정보를 삽입하는 워터마킹 기법을 이용하는 것을 고려할 수 있다. 만약, embedding algorithm이 알려지지 않는다면, 서비스 공급자는 표준 워터마킹 기술을 사용해 전송될 지문 영상의 안전성을 보장할 수 있을 것이다. 즉, 공격 포인트 ④, ⑥, ⑦에 대한 대비책으로, DB에 저장된 지문 영상의 위변조를 막거나 전송 전에 워터마크를 삽입하고 수신단에서 워터마크를 확인함으로써 지문 영상을 안전하게 전송할 수 있다.

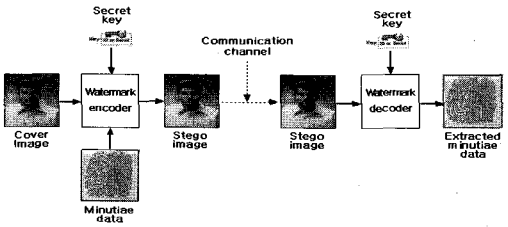
영상에 대한 워터마크를 삽입하여 데이터를 은닉하는 기술은 많이 알려져 있다. 그러나 대부분의 워터마크 기술들은 저작권 보호 등을 위한 연구였으며, 인증에 대한 연구는 거의 없었다. 최근 발표된 지문 영상을 위한 fragile watermarking 기법[5]에서는 영상 도메인에서 워터마크를 삽입할 때 정확성을 조사하였고, 국부적인 블록 평균에 근거한 semi-unique key를 이용하여 지문이나 얼굴 영상의 위변조를 검출하는 연구[6]도 발표되었다. 또한, 지문 특징추출 전과 후에 워터마크를 삽입하는 방법에 대한 연구[7]에서는 지문특징이 신원 확인을 위해 사용되기 때문에 삽입된 워터마크가 지문 영상의 특징을 변경하지 않도록 제안되었다.

최근에는 얼굴 영상에 지문 특징 또는 지문 영상에 얼굴 특징[8]을 은닉하여 지문/얼굴 호스트 영상의 위변조 여부를 확인함과 동시에 은닉된 얼굴/지문 특징을 추가로 이용하여 멀티 모달 생체인식 시스템에 대한 연구도 발표되었다. 예를 들어, 그림 3은 얼굴 호스트 영상에 지문 특징을 워터마크로 사용한 워터마킹 시스템을, 그림 4는 지문 호스트 영상에 Eigen Face Coefficient를 워터마크로 사용한 워터마킹 시스템을 보여준다.

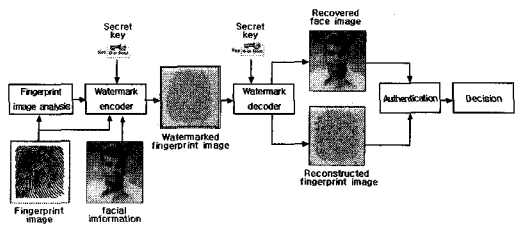
2. WSQ(Wavelet Scalar Quantization) 기반의 데이터 은닉

다음은 앞서 언급한 워터마킹의 특별한 경우로, 압축된 지문영상에 대한 데이터 은닉 기법에 대하여 설명한다. 일반적으로 웹 기반이나 온라인 전송 시스템에서는 전송 대역폭의 제한 때문에 압축하지 않는 상태로 영상을 서버로 보내는 것이 바람직하지 않다. 예를 들어, 512×512 픽셀의 256 그레이 영상(256 Kbyte)을 53 Kbaud 의 전송 속도로 전송하면 약 40초가 소요된다. 불행히도, 대부분의 표준 영상 압축 방식(JPEG 등)들은 고주파 성분이 왜곡되어 지문의 융선 구조가 왜곡된다는 문제가 있다. 따라서 영상 왜곡을 최소화한 WSQ 영상 압축을 FBI에서 제안하였으며, 지문 영상 압축 방식으로 사실상 표준화되어 사용되고 있다.

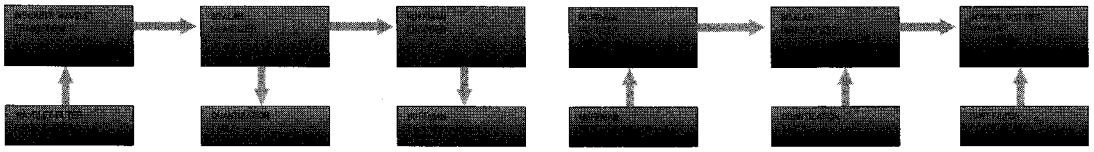
일반적으로 압축된 영상은 사용자의 PIN을 대신해서 표준 암호화 채널을 통해서 전송된다. 그러나 개방된 압축표준 때문에 인터넷을 통해서 WSQ로 압축된 영상을 전송하는 것은 그렇게 안전하다고 할 수 없다. 만약에, 압축된 지문 영상이 전송 단에서 자유롭게 가로챌 수 있다면, 복원 소프트웨어를 사용해 지문 영상을 자유로이 읽을 수 있으며, 결과적으로 신호를 저장하여 재사용이 가능해 진다(공격 포인트 ②). 상업용으로 사용되는 온라인 지문인식 시스템에서는 replay attacks으로부터 전송정보를 보호할 수 있어야 한다. 이러한 목적으로, 서비스 공급자는 전송될 지문 영상들에 대해 매번 서로 다른 인증 스트링(verification string)을 부여한다. 즉, 전송하기 전에 전송될 지문 영상에 스트링을 첨부한다. 그리고 서비스 공급자가 받은 영상은 복원되며 one-time verification string을 검사하여 올바른 지문 영상인지 확인한다. 여기서 인증 스트링은 복원 영상에 영향을 최소화하는 방향으로 설정되어야 한다. 또한, 이 스트링은 고정된 장소에 숨겨져서는 안 된다. 고정된 위치에 둘 경우 해킹을 당할 염려가 있기 때문이다. 따라서 이미지 자체의 구조를 이용해서 다른 장소에 위치시켜야 한다. 다음 예에서 지문 영상 압축 과정에서 워터마크를 첨부하는 방법을 중심으로 기술하고자 하는데, 웨이블릿 얼굴 압축 이미지와 같은 다른 생체 기술에도 쉽게 적용 될 수 있다. 이 정보 은닉(Information Hiding)기술은



〔그림 3〕 지문 은닉

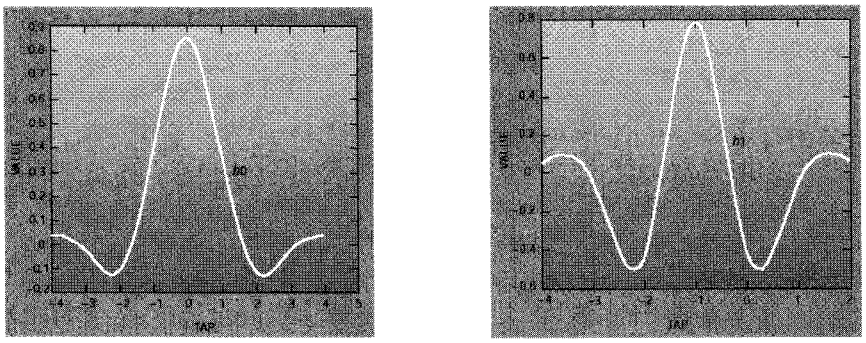


〔그림 4〕 얼굴 은닉



(a) 압축과정 (b) 복원과정

〔그림 5〕 WSQ 알고리즘[9]



〔그림 6〕 FBI WSQ 표준필터[9]

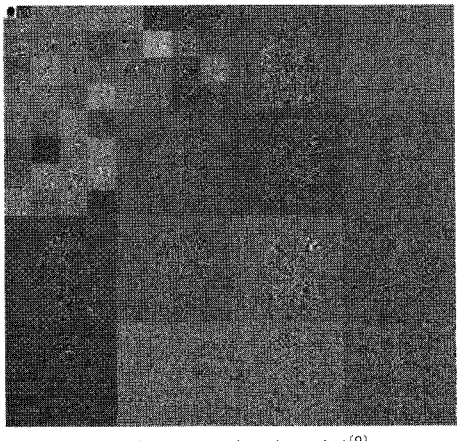
WSQ 지문 이미지 송신단과 수신단의 결합으로 동작한다. 지문 영상의 WSQ 송신단과 수신단에서 정보 은닉하는 과정을 그림 5에 나타내었다.

WSQ 압축은 크게 두 가지 과정으로 구성되어 있다[9]. 첫 번째 과정은, 입력 영상을 DWT(Discrete Wavelet Transformation) 필터에 근거하여 완전 복원(perfect reconstruction)이 가능한 64 spatial frequency filter bank로 분해하는 것이다. FBI에서 표준으로 사용되고 있는 두 필터를 그림 6에 나타내었다. 이들 필터를 적용한 지문 영상 그림 7에 대한 64 서브밴드 영상은 그림 8과 같다.

WSQ 압축의 두 번째 과정은 양자화 처리(quantization process)이다. 각각의 서브밴드를 일정한 스칼라 양자화(scalar quantization)를 이용하여 작은 정수 값인 DWT 계수들로 정한다. 각 주파수 밴드에는 두 가지 특징(The zero of the band(Z_k)와 The width of the bins (Q_k))이 있는데, 이를 정보 손실 없이 압축하기 위해서는 두 가지 파라미터들의 값을 적절히 선택해야 한다. 각 주파수 밴드의 Z_k, Q_k는 수신 단에 전달된다. 그리고 각각의 밴드들은 3개로 군집화하고, 각각의 군집 블록에 있어서 정수 계수들은 테이블에 의해 0~255 사이의 값으로 재 할당된다.

데이터 은닉 알고리즘은 마지막 변형 전에 양자화 된 인덱스에 의해서 동작되며 메시지 크기는 영상에 비해 매우 작다. 그러나 허프만 코딩 특징과 테이블은 변하지 않는다. 실제 영상 송신 과정에서 메시지를 숨기기 위해서는 다음과 같은 4 단계를 거쳐서 처리된다.

〔그림 7〕 WSQ 데이터 은닉 결과[9]



〔그림 8〕 64 서브밴드 영상[9]

i) 위치 후보자 집합 S의 선택

부분적으로 양자화 된 정수 인덱스가 주어지면 이 단계에서는 모든 가능한 계수의 인덱스를 모은다. 작은 변화에도 영상의 많은 부분에 영향을 주기 때문에, 일반적으로 저주파 대역에서의 모든 부분은 제외한다. 고주파 대역에서는 큰 계수를 가졌을 경우에 후보자로 선정한다. 여기서는 일반적인 경우를 생각해서 0~255 사이의 정수 계수가 주어지면, 실제 중요한 정보가 있는 계수 범위(예, 107~254)를 정하여 후보 집합 S를 정한다.

ii) RNGS(Random Number Generation Seed)의 생성과 위치 선택

후보 집합 S 의 모든 계수를 입력 변수로 사용하여, 이것의 조합으로 후보 집합 S 중 하나의 밴드를 선택하는 함수를 정의한다(seed selecting algorithm). 그리고 seed selecting algorithm에 의해 선택된 하나의 주파수 밴드를 메시지 은닉 밴드로 설정한다.

iii) 선택된 위치에 메시지 숨김

먼저 숨겨져야 할 메시지를 일련의 비트로 변환한다. 각각의 비트는 seed가 되는 RNG(Random Number Generator)에 의해서 선택된 부분과 일치되게 선택한다. 만약에 선택된 위치가 이미 사용 중이라면 다음 생성된 위치가 선택된다. 앞에서 RNG에 의해 선택된 주파수 밴드에 지문영상의 authentication을 위한 메시지를 첨부한다.

iv) 이미지에 비트 첨가

선택사양으로 모든 하위 비트는 사용자 명령어 항목으로 압축된 비트 스트링에 첨가된다. 그러므로 이 하위 비트는 숨겨진 메시지와는 아무런 관계를 갖지 않는다. 복구과정이 포함되어있다면 수신단은 메시지를 재구성하는 동안 하위 비트를 선택적으로 복원할 수 있다. 이렇게 함으로써 메시지가 첨부되어있음에도 불구하고 원래의 압축과 거의 유사한 이미지를 만들어 내게 된다. 실제 메시지가 첨가됨으로 인한 차이는 인식할 수 있을 정도가 되지 않으며, 후속적인 처리 과정이나 개인인증의 기능에 전혀 영향을 주지 않는다. 그림 7에 위와 같은 결과로 만들어진 이미지를 원 이미지와 비교해주고 있다.

이와 같은 처리 과정을 이용함으로써 아주 특별한 수신 단만이 압축된 영상으로부터 위치를 알고 해당하는 메시지를 추출 할 수 있다. 즉, 수신단에서 RNG를 가지고 있다면, 메시지가 은닉되어 있는 주파수 밴드로부터 은닉 메시지를 확인할 수 있다. 이 메시지는 인증서나 개인 ID와 같이 혼용하여 사용할 수 있다. 만약, 비트열이 메시지를 갖고 있지 않다거나 다른 형태를 가질 경우에는 이 특수한 수신단은 특별한 메시지 추출에 실패하여 이 영상을 거절하게 된다. 동일한 많은 알고리즘이 실제 구현됨에 있어서는 서로 다른 RNG를 사용하기 때문에 큰 노력이 없이도 모든 구현을 유일하게 만들 수 있다. 또한, 하나의 결과가 다른 수신단의 결과와는 부분적으로도 같을 수 없다. 따라서 한 버전을 크래킹 하더라도 다른 버전에서는 사용이 불가능하다. 이와 같은 방법을 사용하면, 해커가 센서로부터 전송되는 압축 지문영상을 가로채더라도, 데이터 은닉 알고리즘을 가지고 있지 않다면 압축 지문영상의 재사용이 불가능하게 된다.

3. 삽입된 워터마크에 의한 인식률 변화

생체정보에 앞서 언급한 방식으로 워터마크가 삽입되면 인식율의 감소가 불가피하고 이를 해결하기 위한 연구가 필요하다. 이런 워터마크 기법은 워터마크의 목적과 데이터의 특성에 따라 인식률이 최적인 상태의 워터마크 알고리즘을 필요하게 된다.

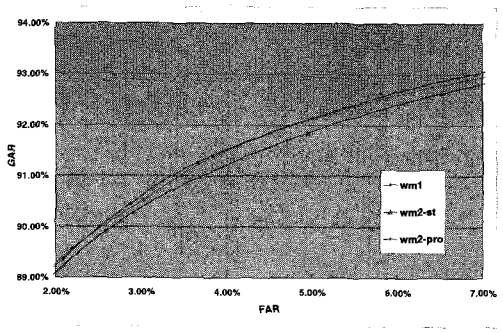
3.1 생체정보 데이터 은닉기법

여기에서는 지문을 원본 영상으로 사용하며 워터마크 데이터로 얼굴 특징정보를 사용하였고, 생체정보 보호를 위한 워터마킹 기법은 아래의 두 가지 목적을 가진다[6].

- 지문 이미지에 얼굴 특징을 워터마킹함으로써 두 번의 인증 과정을 통해 인식 성능 향상을 기대할 수 있다.
- 지문의 특성을 고려한 따라 특징점과 융선 기반의 워터마킹 중 인식 성능에 영향을 주는 정도를 평가한다.

워터마킹 삽입 알고리즘은 두 가지 방법을 통하여 지문인식 성능을 테스트 하였다. 지문 내의 특징점을 이용한 방법과 지문 내의 융선 혹은 굴곡을 이용한 방법을 사용하였고, 지문이미지에 얼굴 특징을 삽입시킨 후 공유하는 암호키와 함께 워터마킹을 하여 워터마크된 지문 이미지를 생성하였다.

실제 인증을 위해서는 워터마크 삽입 모듈에서 사용되었던 동일한 암호키를 가지고 워터마크 추출 모듈을 이용하여 지문 이미지에서 얼굴 이미지를 추출하였다. 인증은 위의 워터마크된 지문 이미지와 워터마크 데이터인 얼굴 특징정보를 이용하여 멀티 모달 생체인



〔그림 9〕 이중 워터마킹 ROC 곡선

식을 할 수 있다. 이렇게 생성된 워터마크된 지문이미지는 스마트카드 등의 매체에 저장되어 활용될 수 있다.

〔6〕에서는 세 가지의 ROC 곡선, 즉 인증시 워터마크 없이 정합을 테스트한 것(Original)과, 특징점 기반으로 워터마킹된 것(Minutiae-based data hiding)과, 융선 기반으로 워터마킹된 것(Ridged-based data hiding)의 실험 결과를 나타내었다. 실험 결과 인증 성능에 최소한의 변화를 주는 방법은 융선 기반의 워터마크 기법이며, 원본 인증과 거의 유사함을 확인할 수 있었다.

여기서 사용된 워터마킹 방법은 공간영역에서 워터마킹하는 방법으로 이미지의 변환과정이 필요 없어서 빠르게 삽입을 할 수 있는 장점이 있다. 하지만 일반적으로 주파수 영역의 워터마킹보다 잡음과 JPEG 압축 등에 강인성(Robustness)이 낮아지는 단점이 있다.

3.2 이중 워터마킹 기술을 이용한 지문정보 보호

다음은 지문정보의 전송 경로에서 발생할 수 있는 replay attack과 지문 데이터베이스의 유출로 인한 사후 처리 방안으로 강인성(Robustness)과 약한 성질(Fragileness)을 동시에 만족시킬 수 있는 이중 워터마킹(Dual Watermarking)알고리즘을 설명한다. 특히, 두 가지의 워터마킹 알고리즘을 동시에 사용할 때 발생할 수 있는 워터마크 삽입 위치에 의한 간섭을 최소화하기 위하여 두 번째로 삽입되는 약한 워터마크를 삽입할 때 융선의 윤곽선 정보를 이용하였다.

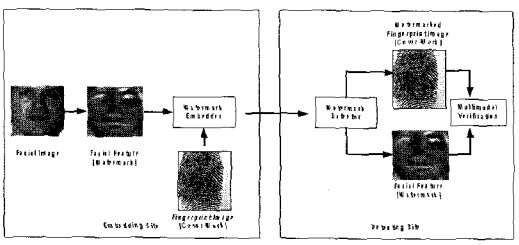
이중 워터마킹은 지문영상의 무결성을 검증하고 중요정보를 동시에 삽입하기 위해 다음 조건을 만족 시켜야 한다.

- 강인한 정보, 약한 정보 순서로 삽입한다.
- 삽입 정보 간에 간섭이 없어야 한다.
- 인식률에 미치는 영향을 최소화 한다.

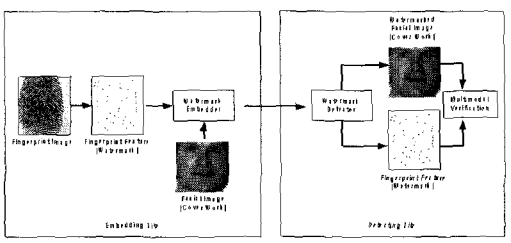
강인한 워터마킹 알고리즘으로 Dugad 방법[10]을 사용하며, 약한 워터마킹 알고리즘으로 Jain 방법[6]을 사용하였다. 그러나 Jain의 워터마킹 기법이 Dugad의 알고리즘에 영향을 주기 때문에 두 알고리즘을 단순 결합하여 이중 워터마킹 기술을 구현할 경우 Dugad의 워터마크 추출률이 떨어진다는 문제점이 있다. 따라서 Jain의 워터마킹 알고리즘을 개선하여 Dugad의 워터마킹 알고리즘에 영향을 주지 않게 하였다. 그리고 지문의 융선 정보를 보호하기 위하여 융선의 경계부분에 워터마크가 삽입이 되지 않게 하였고, 따라서 단순 결합한 이중 워터마킹에 비하여 개선한 이중 워터마킹 알고리즘은 인식률이 크게 떨어지지 않음을 알 수 있다. 그림 9는 단순 결합한 이중 워터마킹(wm2-st)의 ROC와 개선한 이중 워터마킹(wm2-pro)의 ROC를 보여주고 있다. 단순 결합된 이중 워터마크보다 개선한 이중 워터마킹(wm2-pro)의 ROC 곡선이 단일 워터마킹(wm1)된 ROC와 거의 유사하여 인식률에 영향을 적게 주는 것을 보여준다.

3.3 생체 워터마킹 기술의 성능 분석 및 고려사항

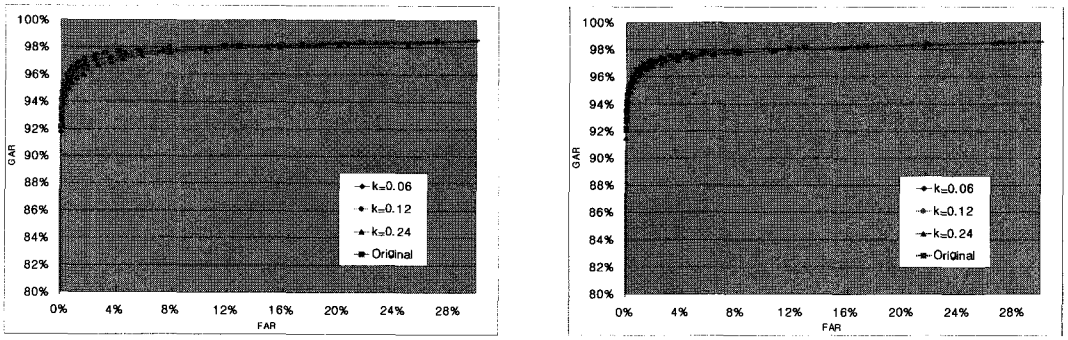
마지막으로 원격 생체인식 시스템에서 생체데이터의 안전한 전송을 위한 워터마킹 기법을 설명하며 워터마크의 삽입으로 인한 인식 성능의 상관관계를 비교한다. 특히, 원격 생체인식 시스템은 사용자의 얼굴과 지문 정보를 동시에 사용하는 다중 생체인식 시스템으



〔그림 10〕 시나리오 1의 흐름도



〔그림 11〕 시나리오 2의 흐름도



(a) No Mask (b) Ridge Mask

〔그림 12〕 지문인식 ROC 곡선

로 가정한다. 다중 생체인식 시스템에 워터마킹 기법을 적용하기 위하여 우선 두 가지 가능한 시나리오를 고려한다. 시나리오 1은 지문영상을 원본 영상으로 사용하며 워터마크로 사용된 얼굴의 특징정보를 지문영상에 삽입하며, 시나리오 2는 얼굴영상을 원본 영상으로 사용하고 지문의 특징정보를 삽입한다.

첫 번째 시나리오에서 워터마크의 삽입 시 지문인식 성능의 저하를 최소화하기 위해 Jain[6]이 제안한 삽입 알고리즘을 사용한다. Jain[6]의 알고리즘은 워터마크가 삽입될 위치를 결정할 때 지문인식 성능에 영향을 주는 특징점(minutiae) 영역과 융선(ridge) 영역을 고려한다. 또한 원 지문영상과 워터마크가 삽입된 지문영상의 인식 성능 측정을 위하여 스마트카드용 지문인식 알고리즘[11]을 사용하였다.

두 번째 시나리오에서는 원 얼굴영상과 워터마크가 삽입된 얼굴영상의 인식 성능을 비교하기 위하여 Eigenface 방법[12]과 Composite Template 방법[13]을 사용하였다.

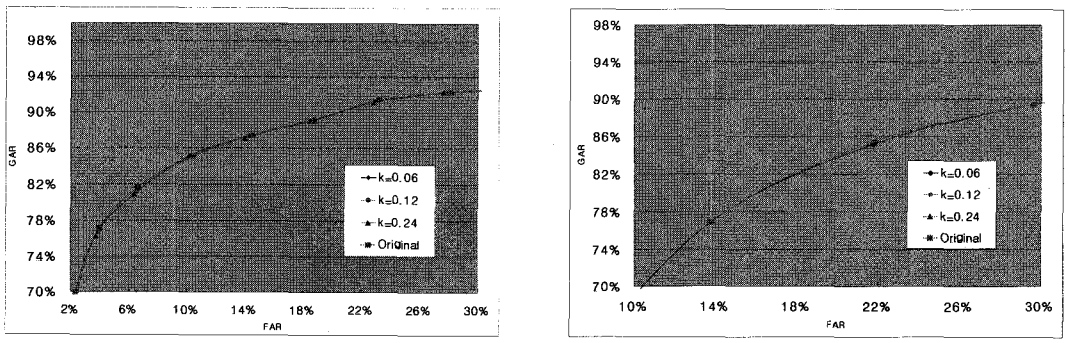
다양한 워터마크 삽입 알고리즘의 일반식은 수식 1과 같이 표현될 수 있다.

$$I_{WM}(x,y) = I(x,y) + k^* W \quad (1)$$

여기서 $I(x,y)$는 원 영상의 화소 값이고, W는 삽입될 워터마크이다. $I_{WM}(x,y)$는 원 영상에 워터마크가 삽입된 결과 영상이며, k는 가중치로 k의 값에 의하여 워터마크의 삽입강도가 결정된다.

그림 12는 k값의 변화에 따른 지문인식 성능에 관한 ROC곡선이다. 그림 12(a)는 워터마크의 삽입 위치를 선정할 때 지문 정보를 고려하지 않은 k값만 변화시킨 워터마킹 방법에 대한 지문인식 결과이고, 그림 12(b)는 융선 정보를 고려한 워터마킹 방법의 지문인식 결과이다. 지문 정보를 고려하지 않은 워터마킹 방법은 삽입 강도가 강해지면서 인식 성능이 저하되는 것을 볼 수 있다. 반면, 그림 12(b)의 융선 정보를 고려한 방법도 강도를 다르게 했을 때 인식성능에 약간의 차이는 있지만, 그림 12(a)의 지문정보를 고려하지 않은 방법보다는 성능의 저하가 덜 발생하는 것을 알 수 있다.

그림 13은 얼굴인식에 대한 ROC 곡선을 보여주며, 그림 13(a)는 Composite Template 방법을



(a) Composite Template (b) PCA

〔그림 13〕 얼굴인식 ROC 곡선

이용한 얼굴인식 결과이고, 그림 13(b)는 PCA 방법을 이용한 얼굴인식 결과이다. 그림 13(b)에서와 같이 얼굴영상이 워터마크의 삽입에 의하여 훼손되었을 경우에도 성능의 저하가 거의 없음을 알 수 있다. 이는 지문인식과는 달리 얼굴인식은 얼굴의 전역적인 정보를 이용하여 인식을 하기 때문이다. 또한, 그림 13(a)의 경우 전체적인 정보와 지역적인 정보를 같이 사용함으로써 얼굴인식 성능이 워터마크 삽입으로 인하여 약간 저하되었지만 시나리오 1의 지문인식 성능과 비교하면 그 차이는 무시할 수 있다. 또한, 일반적으로 생체인식관련 연구에서 보고된 것처럼 지문인식 시스템의 인식 성능이 얼굴인식 시스템의 인식 성능보다 우수하다는 것을 그림 12와 그림 13의 비교를 통하여 확인할 수 있다.

실험에 의해 얼굴 영상에 지문 특징정보를 워터마크로 삽입하는 것이 얼굴 및 지문인식 성능의 저하가 거의 발생하지 않음을 확인할 수 있다. 즉, 다음 3가지 이유로 인하여 얼굴영상에 지문의 특징정보를 삽입하는 것이 타당하다고 판단할 수 있다. 1) 얼굴영상은 이미 온라인상에서 쉽게 획득할 수 있기 때문에 얼굴정보를 숨기기 위한 워터마크로 사용하는 것보다 원본영상으로 사용하는 것이 타당하다. 2) 얼굴인식 성능은 워터마크의 삽입으로 발생하는 얼굴영상의 훼손에 덜 민감하다. 3) 일반적으로 지문인식 성능이 얼굴인식 성능 보다 우수하기 때문에 전체적인 시스템의 성능향상을 위하여 지문특징정보를 워터마크로 사용하여 보호하는 것이 타당하다.

V. 결 론

본 고에서는 생체인식 기술을 대규모 응용에 적용하기 위하여 필요한 생체정보의 안전한 저장/전송/처리 등 생체정보 보호에 대한 연구 동향을 살펴보았다. 특히, 디지털 컨텐츠 보호에 사용되는 워터마킹 기법을 이용하는 경우 발생하는 인식률 저하의 정도 및 이를 보완할 수 있는 관련 연구 결과들을 소개하였다. 생체정보를 이용한 본인 인증은 기존의 패스워드에 비해 많은 사용상의 장점을 가지고 있다. 그러나 생체정보를 사용하는 시스템을 포함하여 어떠한 시스템이라도 미리 준비한 해커에 의한 공격에 대해서는 취약할 수 있으며, 생체정보의 가장 강력한 특징인 "시간의 흐름에도 변하지 않는다."는 점이 오히려 가장 큰 문제가 될 수 있다는 사실은 참으로 역설적인 사실이 아닐 수 없다. 개인이 가지고 있는 사용가능한 생체정보에는 한계가 있으며, 일단 생체정보가 도용되면 이는 더 이상 바꿀 수 없다는 문제가 있다. 이와 같은 문제를 해결하기 위해서는 워터마킹 기법 등을 이용한 생체정보 보호와 관련된 연구 개발이 보다 활발히 진행되어야 할 것으로 판단된다.

참 고 문 헌

[1] B. Schneier, "The Uses and Abuses of Biometrics", *Communications of the ACM*, Vol. 42, No. 8, pp. 136, 1999.

[2] N. Ratha, J. Connell, and R. Bolle, "An Analysis of Minutiae Matching Strength", *Proc. of AVBPA 2001(LNCS 2091)*, pp. 223-228, 2001.

[3] T. Matsumoto, et. al., "Impact of Artificial Gummy Fingers on Fingerprint Systems", *Optical Security and Counterfeit Deterrence Technique*, Vol. 4673, pp. 275-289, 2002.

[4] J. Cox. et. al., *Digital Watermarking*, Morgan Kaufmann, 2001.

[5] M. Yeung and S. Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval", *Journal of Electronic Imaging*, Vol. 9, No. 4, pp. 468-476, 2002.

[6] A. Jain, U. Uludag, and R. Hsu, "Hiding a Face in a Fingerprint Image", *Proc. of ICPR*, pp. 756-759, 2002.

[7] B. Gunsel, U. Uludag, and A. Tekalp, "Robust Watermarking of Fingerprint Images", *Pattern Recognition*, Vol. 35, pp. 2739-2747, 2002.

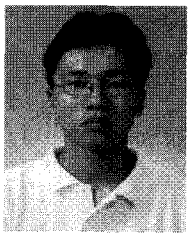
[8] A. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images", *Proc. of AutoID*, pp. 97-102, 2002.

[9] N. Ratha, J. Connell, and R. Bolle, "Secure Data Hiding in Wavelet Compressed Fingerprint Images", *Proc. of Multimedia*, pp. 127-130, 2000.

[10] R. Dugad, K. Ratakonda, and N. Ahuja, "A New Wavelet-based Scheme for Watermarking Images", *Proc. of the*

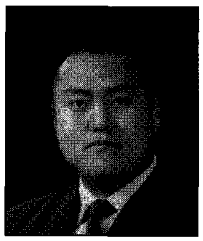
ICIP, 1998.
[11] S. Pan, et al., "A Memory-Efficient Fingerprint Verification Algorithm using A Multi-Resolution Accumulator Array for Match-on-Card", *ETRI Journal*, Vol. 25, No. 3, pp. 179-186, 2003.
[12] M. Turk and A. Pentland, "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, Vol. 3, pp. 71-86, 1991.
[13] Y. Lee, et al., "Local and Global Feature Extraction for Face Recognition", *LNCS 3546-AVBPA*, pp. 219-228, 2005.

〈著 者 紹 介〉



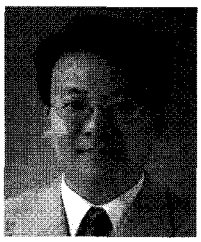
김 태 해 (TaeHae Kim)

2002년 2월: 인제대학교 전산학과 학사
2004년 3월~현재: 고려대학교 전산학과 석사과정
〈관심분야〉 생체인식, 정보보호, 병렬 알고리즘



정 승 환 (SeungHwan Jung)

2005년 2월: 고려대학교 전산학과 학사
2005년 3월~현재: 고려대학교 전산학과 석사과정
〈관심분야〉 생체인식, 정보보호, 병렬 알고리즘



정 용 화 (Yongwha Chung)
종신회원
1984년 2월: 한양대학교 전자통신공학과 학사
1986년 2월: 한양대학교 전자통신공학과 석사
1997년 2월: 미국 Univ. of Southern California 전기공학과(컴퓨터공학 전공) 박사
1986년~2003년: 한국전자통신연구원 생체인식기술연구팀장
2003년 9월~현재: 고려대학교 컴퓨터정보학과 부교수
〈관심분야〉 생체인식, 정보보호, 생체정보보호

문 대 성 (Daesung Moon)
정회원
1999년 2월: 인제대학교 전산학과 학사
2002년 2월: 부산대학교 컴퓨터공학과 석사
2002년 3월~현재: 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 연구원
〈관심분야〉 생체인식, 정보보호, 영상처리

문 기 영 (Kiyoung Moon)
1986년 2월: 경북대학교 전자공학과 학사
1989년 2월: 경북대학교 대학원 전자공학과 석사
1992년~1994년: (주)대우정보시스템 기술연구소 전임연구원
1994년 3월~현재: 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 팀장
〈관심분야〉 생체인식, 웹서비스 보안, 분산 시스템