생체인식시스템 : 왜 필요하고 왜 두려워하고 있는가?

이 남 일[1)]

목 차

1. 서 론

생체인식 시스템은 다른 사용자 인증 시스템에 비해서 여러 가지 장점을 가지고 있기 때문에 요즈음 사용자 인증의 수단으로 많이 사용되고 있는 추세다. 보안이 중요시 되고 있는 응용분야에서 특히 m-Commerce 나 e-Commerce 등에서 사용될 때 다양한 공격으로부터의 방지 대책이 강구되어야 함은 아주 중요한 사실이다. 지금부터 이러한 관점에서 먼저 생체인식시스템의 강점과 약점을 살펴보고 이들 약점을 보강할 수 있는 방법에 대한 기술등을 언급을 하면서 일반 사용자들이 이들 제품을 사용함에 있어서 선택의 기준을 정하는데 조금이나마 보탬이 되었으면 하는 마음에서 글을 전개 하고자 한다.

웹을 사용하는 세계에서 믿을 만한 사용자 인증은 점점 더 그 중요도가 증가하고 있다. 기업내부에서 사용되는 일련의 위협요소가 존재하는 사용자 인증시스템은 비밀스러운 데이터의 손실, 서비스의 거부, 그리고 데이터의 불일치성 등, 기업에 치명적인 결과를 가져올 수도 있다. 그 외에도 인터넷 뱅킹, e-Commerce ,그리고 컴퓨터 자료의 접근 통제 등 우리의 일상 생활에서 사용되는 많은 응용분야에서도 사용자 인증이 필요할 뿐아니라 시큐리티를 강화함으로써 이익을 가져올 수도 있다. 사용자 인증방법은 암기를 통해서 가능한 사용자 ID, 비밀번호와 휴대가 가능한 카드, 뺏지, 키 등이 있으며 마지막으로 암기하거나 휴대할 필요가 없는 생체인식 분야다.

암호나 사용자 ID 혹은 인증 카드나 PIN 번호 등을 사용하는 사용자 인증 시스템의 기술은 여러 가지 한계를 가지고 있다. 패스워드나 PIN 번호는 도용될 가능성이 많고 일단 도용이 되기 시작하면 누가 진짜 사용자 ID나 패스워드를 사용하는지를 알 방법이 없다는 것이다. 물론 신용카드 번호가 포함된 데이터의 전송이 웹상에서 이루어질 때도 같은 현상이 발생하게 된다. 물론 데이터가 암호화되어서 전송은 되지만 시스템은 최초의 데이터가 옳은 사용자의 것인지는 알 수가 없다. 지금과 같은 분산된 환경에서는 단순한 ID나 패스워드의 조합에 의한 사용자인증은 불확실한 형태라고 할 수 있다. 다행히 일반적인 생체인식은 특별히 지문인식 기술은 훨씬 더 정확하고 ale을

1) (주)시큐아이티 상무

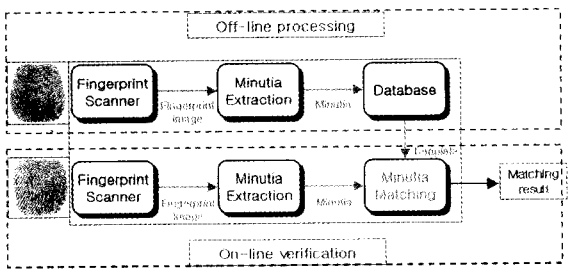
만한 사용자 인증 방법을 제공할 수 있다. 생체인식의 경우 아무것이나 사용할 수 있는 것은 아니고 다음과 같은 요구사항을 만족하는 정도는 되어야 생체인식의 한 분야로서 사용이 가능하다고 할 수 있다.

- 보편성 : 모든 사람이 가지고 있는 특성인가?
- 유일성 : 동일한 특성을 가진 타인이 없는가?
- 영구성 : 시간에 따른 변화가 없는 특성인가?
- 획득성 : 정량적으로 계측이 가능한 특성인가?
- 정확성 : 환경변화와 무관하게 높은 정확성을 얻을 수 있는가?
- 수용성 : 사용자의 거부감은 없는가?
- 기만성 : 작위적인 부정 사용으로부터 안전한 특성인가?

이 중에서 지문, 얼굴, 홍채나 음성인식 등 사람의 신체적 특성이나 행동적인 특성에 따라 개인을 확인하는 요즘 급격하게 발전하는 분야가 생체 인식이다. 생체인식은 개인 고유의 특성이기 때문에 복제가 어렵고 공유가 거의 불가능하다. 더구나 개인의 생체정보는 심각한 사고에 의하지 않고는 잃어버릴 수 없다. 생체정보는 그 길이가 수백 바이트에서 수메가 바이트에 이르므로 패스워드나 PIN 번호보다 일반적으로 더 안전하다. 또한 생체 인식이 기존의 패스워드나 PIN 번호와 같은 개인인증방법에 존재하는 여러 가지 공격포인트가 있지만 생체인식을 사용함으로써 이러한 공격에 대하여 훨씬 더 강화된 시스템이 될 수 있다. 그러나 아무리 생체 인식제품이라고 하더라도 아직은 해커들이 들어올 만한 약점이나 침투 가능성이 있는 부분이 존재한다. 생체인식 관련 데이터가 한번 도용되기 시작하면 생체인식 시스템은 심각한 지경에 이르게 된다[1]. 다른 개인인증 시스템(신용카드, 비밀번호 등)의 경우 잃어버리거나 도용되었다고 판단되는 경우에는 쉽게 버리고 새로운 것을 만들면 된다. 그러나 생체 정보를 이용하는 경우 한 개의 얼굴, 열 개의 손가락, 두 개의 눈,두 개의 손 등 사용할 수 있는 종류가 한정되어 있기 때문에 생체 정보가 도용되었을 경우 인증을 위해 사용할 대체 방안이 제한을 받을 수 밖에 없다. 그래서 일단 한번 도용이 되면 영원히 사용될 수 밖에 없다. 본 논고에서는 지문을 중심으로 생체인식 시스템에 대한 간단한 이해와 이들에 대한 공격 포인트, 그리고 그에 대한 대처 방안을 중심으로 기술하고자 한다.

2. 지문인증 시스템

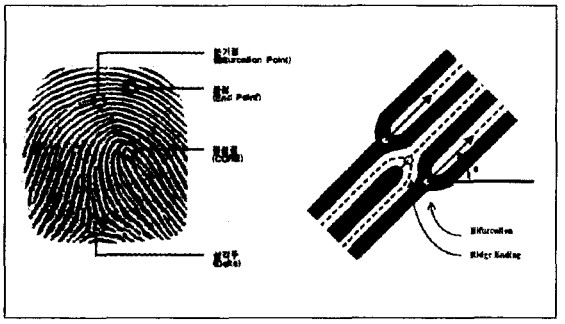
지문은 일반적으로 손가락이 잘리거나 손상을 입지 않으면 평생 불변의 특징을 가지고 있다고 한다. 인증 절차는 (그림 1)과 같이 몇단계를 통해서 이루어 지는데 첫 번째 단계는 지문영상을 얻는 과정이다.



(그림 1) 지문인증 절차

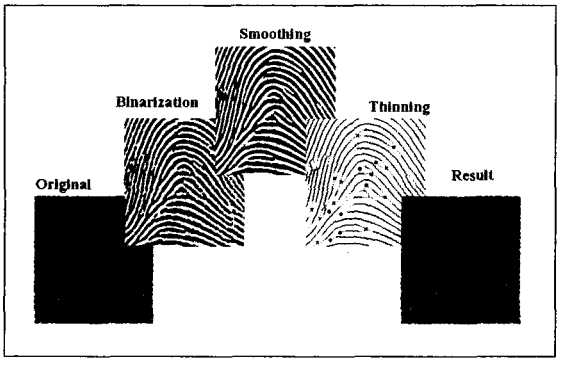
여러 가지 영상취득방법이 가능하지만 (그림 2)와 같이 크게 3가지 정도로 구분할 수 있다. 이에 대한 자세한 사항은 다음 기회로 돌리기로 하고 이렇게 얻어진 지문영상은 일반적으로 200 ~ 500 DPI(dots per inch) 정도의 질을 가지며 한 픽셀(Picture Element:pixel)은 8 비트로 나타내는데 0 ~ 255 까지의 값으로 밝기를 표현하여 지문의 융선과 골을 표현하고 있다.

일반적으로 지문에서의 정보는 그 첫째가 융선의 흐름에 의한 정보이고 다음으로는 (그림 2)와 같이 융선의 특징과 골과의 관계에 의해서 융선의 분기점(bifurcation point)이나 끝점(ending point) 그리고 중심점(Core), 삼각주(Delta) 등으로 명명되는 여러 개의 특징점(minutiae)과 단점(singular point)이 존재하게 되는데 이 특징은 개인별로 서로 상이하게 때문에 이를 이용해서 서로의 일치여부를 판단하게 된다.



(그림 2) 지문의 특징점과 단점

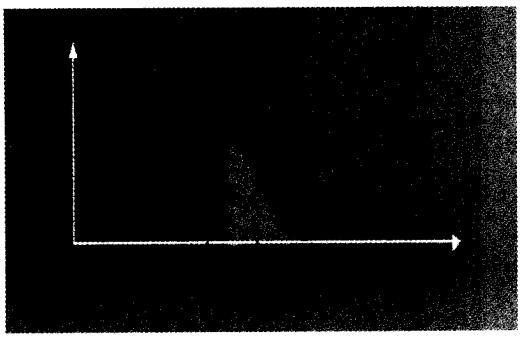
다음 단계는 여러 가지 복잡한 영상처리 기법을 이용하여 이러한 특징들의 위치를 파악하는 것이다. 각각의 특징은 그들의 위치정보(x,y)와 융선의 방향정보(theta)를 가지고 표현하는 것이 가장 일반적인 방법이다.



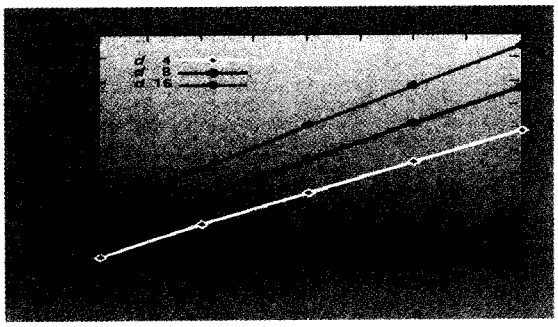
(그림 3) 지문특징을 추출하는 과정

그러나 센서의 잡음이나 (그림 3)과같이 영상처리과정에서의 복잡성 때문에 특징을 추출하는 과정에서 실제 특징이 누락되거나 가짜 특징이 만들어지는 경우가 발생한다. 더구나 사람 손가락의 전도율이나 누르는 압력의 차이, 습도나 온도 등의 환경 요인 등 때문에 첫 번째 지문과 다음에 취득한 지문 영상에서 항상 완벽한 일치성을 갖기는 참으로 어려운 문제이다.

마지막 단계에서는 회전, 변형 그리고 크기변화에 따른 보상을 한 후 두 영상간의 유사도를 측정하여 일치여부를 확인하는 단계이다. 유사도는 가끔 점수(match-score)로 환산하여 사용되는데 이 점수에 근거하여 최종적으로 일치 여부를 판단한다. 만약에 점수가 일정한 기준(threshold)보다 작을 경우에는 불일치로하고 클 경우에는 일치로 간주한다. 운영상에서도 일반 비밀번호 시스템보다는 훨씬 복잡하고 어려움이 있다. 시스템 성능면에서 보면 등록실패도 고려해야만 한다. 어떤 이는 지문이 아주 좋지않거나 전혀 손가락이 없는 경우도 존재하게 된다. 이럴 경우에는 그들에게는 본 시스템을 사용할 수 없게 되는데 지문의 영상의 질에 따라 등록이 거절되는 경우에 대한 대비가 필요한 것이다. 좋지 않는 지문의 원인으로는 사용자의 부주의, 가짜지문의 사용, 손가락에 존재하는 먼지나 물기, 그리고 입력 장비의 결함에서도 발생할 수 있다. 비밀번호 기반의 시스템의 경우에는 아날로그 데이터에 대한 처리가 필요하지 않다. 즉, 항상 바른 결정을 내릴 수 있다는 것이다. 비밀번호가 맞으면 반응을 하고 그렇지 않는 경우에는 거부하는 것이다. 그러나 생체 인증 시스템의 경우에는 일치여부를 결정함에 있어서 확실한 기준선이 없다는 것이다. 전체 시스템의 정확도가 입력데이타의 질과 특징을 추출하고 일치여부를 판단하는 알고리즘의 성능에 따라 달라진다. 생체인식에 있어서 본인거부율(FRR:false rejection rate)과 타인수락율(FAR:false



(그림 4) 생체인식시스템의 에러률



〔그림 5〕 특징점 수와 비밀번호 자리수의 비교.

accept rate) 등 두가지 형태의 인식 에러가 존재한다.

위 (그림 4)에서 보는 바와 같이 기준값(threshlod)을 변형하여 한 가지의 에러를 줄이고자 하면 다른 쪽의 에러는 증가하게 된다. 생체인증 시스템에서는 응용분야에 따라 기준점을 찾아서 사용하게 된다. 두 가지의 에러를 동시에 영(zero)에 가깝게 하는 것은 현실적으로 불가능하다. 기준값을 높게 셋팅하면 FAR은 영(zero)에 가깝게 되어 보안성은 뛰어나나 사용상에 불편함이 존재한다. 반면 기준값을 아주 낮게 하면 FRR은 영에 가까워지나 보안성이 떨어지게 된다. 제조업체에서 제공하는 에러율은 개인 데이터베이스를 기준으로 한 것이기 때문에 실제 값보다는 높게 된다. 일반적으로 사용되는 효율성을 강조하는시스템의 경우 FAR의 범위가 10-6 ~ 10-4 정도이다. 이러한 에러율은 실제 사용하는 사람의 행위가 수반되는 부분이므로 일반적인 다른 개인인증 방법에서의 에러율과 동일한 선상에서 평가하기는 어렵다. 이에 대한 일반적인 접근 방법〔2〕을 다음 (그림 5)에서는 특징점의 수에 따라 해당하는 비밀번호의 자리 수를 비교 해주고 있다.

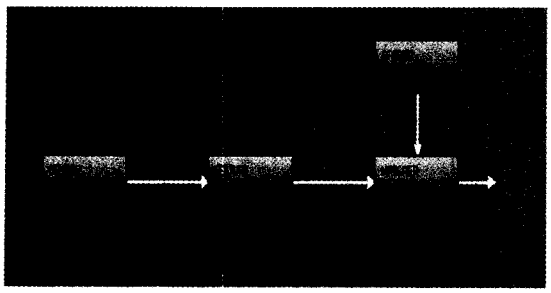
여기서 m은 특징점의 개수를 의미하고 d 는 특징점의 방향성을 각각 나타낸다. 세로축의 숫자는 그에 해당하는 비밀번호의 자리수를 나타낸다. 위 그림에서와 같이 m이 16이고 d가 8일 경우가 지문인식 시스템에서 가장 많이 나타나는 경우라고 할 수가 있다. 이 경우 약 140 비트 길이의 비밀번호와 같은 안정성을 가진다는 말이 된다. 물론 이는 실제 사용되는 시스템의 현실적인 면이 가미되지 않은 다분히 이론적이긴 하지만 그만큼 보안성이 뛰어나다는 말이 된다. 편의성과 보안성이 이렇게 뛰어나다면 과연 그 "생체 정보가 안전하게 보장될 수 있는가?" 가 또 다른 논쟁의 대상이 된다.

3. 공격 취약포인트

"왜 필요하고 왜 사용을 두려워하고 있는가?" 라는 명제를 가지고 이제는 위와 같은 간단한 이해를 바탕으로 생체인식 시스템에서의 취약포인트〔2〕를 점검해보고 이에 대한 대체 방안은 무엇인지를 살펴봄으로써 생체인식 제품을 개발 또는 사용하고자 하는 시점에서 관찰해야 할 항목을 기술하고자 한다.

(그림 6)은 전형적인 생체인식 시스템에서의 가능한 공격포인트〔1〕를 보여주고 있는데 이를 간단히 살펴 보면 다음과 같다.

1) 사용자로부터 신호를 얻는 부분으로 센서단에 가짜 지문이나 복사한 사인, 얼굴 마스크 등을 이용하는 경우다.
2) 미리 저장해둔 생체 신호를 다시 사용하는 경



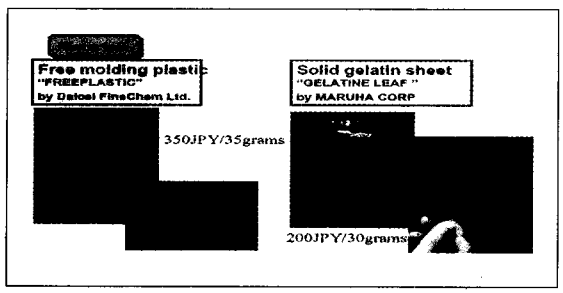
(그림 6) 생체인식 시스템에서의 가능한 공격포인트

우로 센서를 바이패스(bypassing)하고 지문의 복사본이나 오디오 신호를 단자를 통해서 전송한다.

3) 침입자가 선정한 특징을 만들도록 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 해결을 할 수 있으나 인터넷으로 특징점이 전송되는 경우에는 TCP/IP에 대한 스누프(snoop)를 통해서 패킷을 변경할 수도 있다.
5) 정합하는 자체를 공격하여 미리 선택된 정합 결과를 나타내도록 하는 경우로 아무리 정합알고리즘이 좋을 지라도 원하지 않는 결과가 나오게 된다.
6) 템플릿이 저장된 데이터 베이스를 공격하여 저장된 템플릿을 변경하는 경우로 특히 템플릿이 분산 저장된 경우에는 그 중에 일부 혹은 전체를 변경하여 타인 수락율이 높아 진다거나 혹은 본인 거부율이 높아지게 되는 현상을 초래할 수도 있다.
7) 저장된 템플릿이 전송 채널을 통해서 정합부분으로 전송될 때 채널을 공격하는 경우해서 전송되는 데이타를 가로채어 다른 형태로 바꾸어 버리게되어 정합의 결과를 틀리게 한다.
8) 마지막 판결을 공격하는 경우로 아무리 실제 시스템이 우수하고 정확하다고 하더라도 정합결과가 공격을 당하면 아무런 의미가 없게 된다.

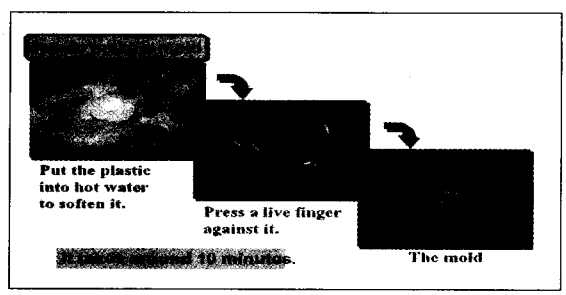
위와 같이 여러가지 공격포인트가 존재하고 있으며 아울러 이러한 공격을 피해갈 수 있는 방안 또한 강구되어야 한다. 1번 공격포인트에 대한 부분은 현재 일본[3] 등에서 다각적으로 검토 연구되고 있다. 먼저 paper, silicone rubber, 그리고 gelatin을 이용하여 인위적으로 지문을 만드는 경우가 존재하는데 이를 간단히 살펴보기로 한다.

1) 가짜지문을 위한 재료(몰딩 플라스틱, 젤라틴)를 준비한다.



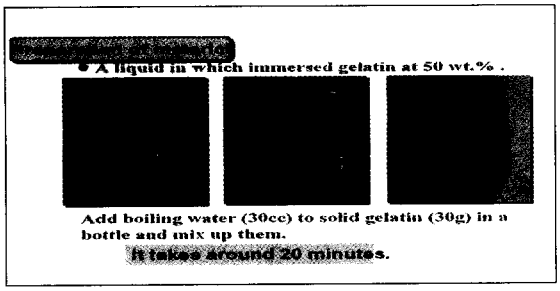
(그림 7) 거미핑거를 위한 재료(플라스틱,젤라틴)

2) 플라스틱을 뜨거운 물에 넣고 부드럽게 한 후 실제 손가락을 눌러서 몰딩을 만든다. 이것은 약 10분 정도의 시간이 소요된다.



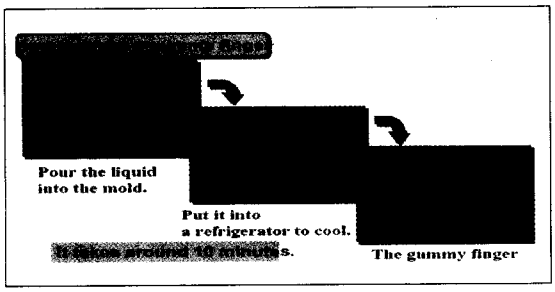
(그림 8) 몰딩을 만드는 벙법

3) 필요한 재료(젤라틴, 뜨거운 물)를 병에 넣고 섞는다. 그리고 20 분 정도를 기다린다.



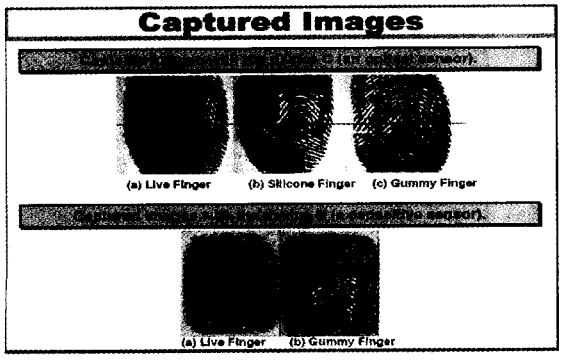
(그림 9) 재료를 만드는 과정

4) 녹은 젤라틴을 몰딩에 붓는다. 그리고 냉장고에 넣고 10분 정도 지난 후 거미핑거를 뺀다.



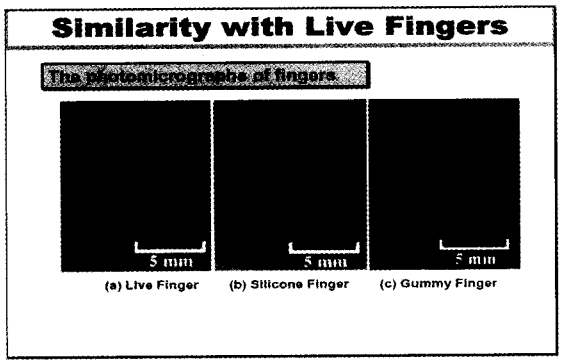
(그림 10) 거미 핑거를 만드는 과정

이렇게 하여 얻은 거미핑거를 광학식 센서와 반도체 방식 센서를 통해서 채취한 지문을 실제 지문과 비교한 것이 아래 (그림 11)이다.



(그림 11) 채취한 영상의 비교

위 (그림 11)(a),(b),(c)에서 빨간 마크가 된 부분을 확대하여 자세히 비교해 보면 다음 (그림 12)와 같다. 동일한 사람의 동일한 손가락을 실제 5 mm 내에서의 비교 분석을 해보면 크게 차이가 없음을 알 수가 있다.



(그림 12) 각 지문의 유사도 비교

이를 다음과 같이 4가지 타입에 따라 20 ~ 40 대에 있는 5명을 대상으로 100번의 1 대 1 매칭을 한 결과 대부분의 제품에서 90% 정도가 통과되었다.

Experiment	Enrollment	Verification
Type 1	Live Finger	Live Finger
Type 2	Live Finger	Gummy Finger
Type 3	Gummy Finger	Live Finger
Type 4	Gummy Finger	Gummy Finger

위에서 살펴 본 바와같이 아주 많은 돈을 들이지 않고 짧은 시간에, 그리고 그리 어렵지 않게 거미핑거를 만들 수 있다는 것을 알 수 있다. 실제 손가락을 이용한 방법뿐 아니라 잔상 지문을 이용해서도 유사한 방법으로 가짜 지문을 만들 수 있다. 그러면 우리는 어떻게 생체인식시스템을 안전하게 만들 수는 없을까하는 문제에 봉착하게 된다.

즉, 가짜지문인지 아니지를 어떻게 판단할 것인가. 이를 위한 방법에는 소프트웨어적 접근법과 하드웨어적 접근법으로 생각할 수 있다. 소프트웨어적인 방법으로 지문은 땀샘, 얼굴은 머리의 움직임, 홍채는 눈의 움직임 등을 이용한다. 하드웨어적인 경우 지문은 손가락의 온도와 맥박을 측정하거나 전기적 특성을 이용하는 방법도 가능하다. 이들 방법을 잘 이용하면 완전하지는 않겠지만 센서 단에서의 공격은 어느 정도 막을 수 있다. 암호화된 채널을 이용하면 공격포인트 4번에서의 원격공격은 막을 수 있다. 그리고 공격 포인트 5,6,7에 대한 간단한 방어책은 매처나 데이타베이스를 안전한 곳에 설치하는 것이다. 물론 충격이나 파괴에 의한 공격은 어쩔 수 없다. 일반적으로 8번의 경우는 암호화를 통해서 공격을 막을 수 있다. 지금부터 이들에 대한 예를 통해서 공격을 이해하고 방어책에 대해서 논하기로 한다.

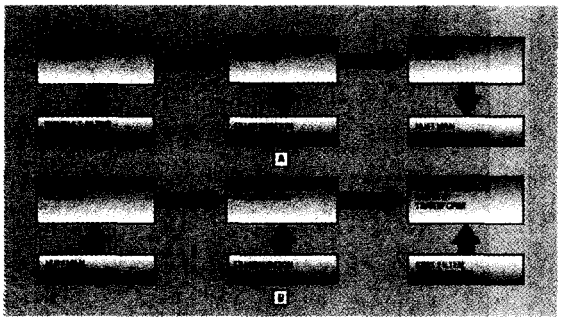
3.1 WSQ based data hiding

웹 기반이나 On-line 전송 시스템에서는 전송 bandwidth의 제한 때문에 압축하지 않는 상태로 영상을 서버로 보낸다는 것은 바람직하지 않다. 일반적으로 512*512 pixels 의 256 gray levels 영상이면 256Kbyte가 소요된다. 이 경우 53 Kbaud의 전송 속도로 전송하는 경우에 약 40 sec의 시간이 소요된다. 불행히도, 대부분의 표준 영상 압축 방식(JPEG)들은 고주파 성분이 왜곡되는 단점이 있다. 그래서 Ridge 구조가 왜곡된다. 따라서, 영상 왜곡을 최소화한 WSQ 영상 압축을 FBI에서 제안하였으며, 지문 영상 압축 방식으로 상당히 많이 사용된다. 전형적으로 압축된 영상은 사용자의 PIN을 대신해서 표준 암호화 채널을 통해서 전송된다. 그러나 개방 압축표준 때문에 인터넷을 통해서 WSQ 로 압축된 영상을 전송하는 것은 그렇게 안전하다고 할 수는 없다. 만약에, 압축된 지문 영상이 전송단(Internet)에서 자유롭게 가로채갈 수 있다면, Decompressing Software를 사용해 지문 영상을 자유로이 읽을 수 있으며, 결과적으로 신호를 저장하여 재사용이 가능해 진다.(공격포인트 2)

이런 문제점을 해결하기 위한 방법으로, 압축지문 영상에 추가 정보를 끼워넣는 data hiding techniques의 사용이다. 만약, Embedding Algorithm이 알려지지 않는다면, 서비스 공급자는 표준 watermarking 기술을 사용해 전송될 지문 영상의 안전성을 보장할 수 있을 것이다. 영상에 대한 watermark를 통해 data를 은닉하는 기술은 많이 알려져 있다. 한가지 예로, Hsu와 Wu는 JPEG 압축 영상에 대한 watermark를 이용한 data 은닉 기술을 발표했다. 그러나, 대부분의 watermark 기술들은 저자권, 개인 신상등을 위한 연구였으며, Authentication에 대한 연구는 없었다. 최근들어, Yeung and Pankanti는 지문 영상을 위한 watermarking 기법을 연구하였다. 그러나, 그들의 연구는 Image domain에서 watermark를 첨부하였을때 정확성을 조사하는 것이었을 뿐, 지문 영상의 보호 목적은 아니다.

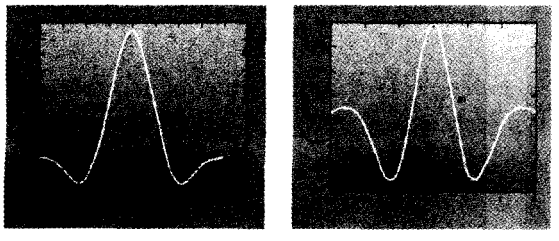
상업용으로 사용되는 On-line 지문 인식 시스템에서 Replay attacks으로부터 전송정보를 보호할 수 있어야한다. 이런 목적으로 서비스 공급자는 전송될 지문 영상들에 대해 매번 서로 다른 verification string을 부여한다. 즉, 전송하기 전에 전송될 지문 영상에 String을 첨부한다. 그리고 서비스 공급자가 받는 영상은 decompressed 되며 one-time verification string을 검사하여 올바른 지문 영상인지 확인한다. 여기서 verification string은 decompressed image에 영향을 최소화하는 방향으로 설정되어야 한다. 더구나 이 스트링은 고정된 장소에 숨겨져서는 안된다. 고정된 위치에 둘 경우 해킹을 당할 염려가 있기 때문이다. 따라서 이미지 자체의 구조를 이용해서 다른 장소에 위치 시켜야한다. 다음 예에서

지문 영상 압축 과정에서 watermark를 첨부하는 방법을 중심으로 기술하고자 하는데 웨이블릿 얼굴입축 이미지와 같은 기타 다른 생체 기술에도 쉽게 적용 될 수 있다. 이 information hiding 기술은 WSQ 지문 이미지 encoder와 decoderdml 결합으로 동작을 한다. 지문 영상의 WSQ Encoder, Decoder 과정에서 정보 은닉하는 과정은(그림 13A, 13B)와 같다.

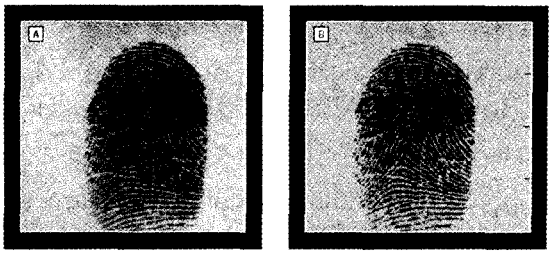


(그림 13) A,B WSQ 알고리즘;
(A) Compression (B)Decompression

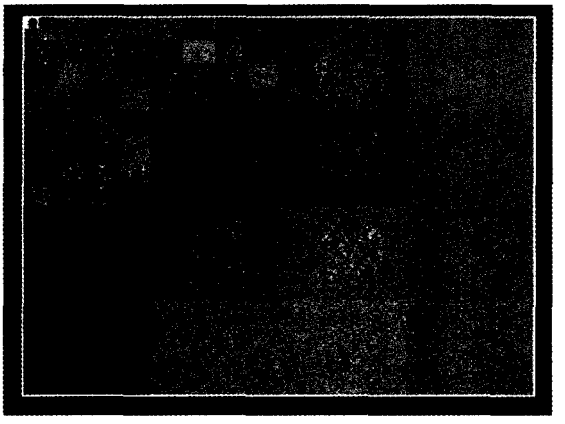
WSQ 압축은 크게 두가지 과정으로 구성되어 있다. 첫번째 과정은, 입력 영상을 DST (descrete wavelet Transformation) filter에 근거하여 perfect reconstruction이 가능한 64 spatial frequency filter bank로 decomposition하는 것이다. FBI에서 표준으로 사용되고 있는 두 필터가 (그림 14)이다. 이들 필터를 적용한 (그림 15A)의 지문 영상에 대한 64 subband 영상은 (그림 16)과 같다.



(그림14) FBI WSQ 표준 필터



(그림 15) WSQ data-hiding 결과 ;
(A)Original image (B)Reconstructed Image



(그림 16) 그림15 영상에 대한 64 subbands

WSQ 압축의 두번째 과정은 양자화 처리 (Quantization process)다. 각각의 subband를 일정한 스칼라 양자화(Scalar quantization)를 이용하여 작은 값의 정수값인 DWT(Discrete Wavelet Tranform) 계수들을(coefficients)' 정한다. 각 주파수 밴드에는 두가지 특징(The zero of the band(Zk)와 the width of the bins (Qk))이 있다. 정보 손실없이 압축하기 위해서는 두가지 파라미터들의 값을 적절히 선택해야한다. 각 주파수 밴드의 Zk, Qk는 decoder에 전달된다. 그리고 비슷한 특성을 갖는 3개의 밴드들끼리 군집화(grouping)를 해서 DWT 계수들의 정수값들은 Huffman coding을 하게 된다. 마지막으로, 각각의 군집 블록에 있어서 정수 계수들은 Translation table에 의해 0~255 사이의 값으

로 재할당된다.

data-hiding algorithm은 마지막 변형전에 양자화된 인덱스에 의해서 동작된다. Data-hiding algorithm의 메시지 크기는 영상에 비해 매우 작다. 그러나, Huffman coding 특징(characteristics)와 표(tables)은 변하지 않는다. 즉, 표는 Original Coefficients에 의해서만 계산된다. 실제 Image encoding process에서 메시지를 숨기기 위해서는 다음과 같은 4 단계를 거쳐서 처리된다.

3.1.1 위치 후보자 set S의 선택

부분적으로 양자화된 정수 인덱스가 주어지면 이 단계에서는 모든 가능한 계수의 인덱스를 모은다. 조그만한 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 candidate set S를 정한다.

3.1.2 Random number generation seed의 생성과 위치 선택

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

3.1.3 선택된 위치에 메세지를 숨기기

먼저 숨겨져야 할 메세지를 일련의 bit 로 변환한다. 각각의 bit는 seed가 되는Random number generator에 의해서 선택된 부분과 일치되게 선택한다. 만약에 선택된 위치가 이미 사용중이라면 다음 생성된 위치가 선택된다. 앞에서 Random number generator에 의해 선택된 주파수 밴드에 지문영상의 Authenti- cation을 위한 메시지를 첨부한다.

3.1.4 이미지에 bit를 첨가하기

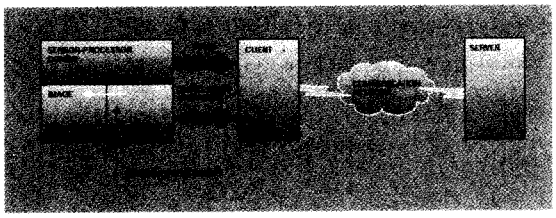
선택사양으로 모든 하위 bit는 사용자 명령어 항목으로 압축된 bit string에 첨가된다. 그러므로 이 하위 비트는 숨겨진 메세지와는 아무런 관계를 갖지 않는다. restoration 과정이 포함되어 있다면 decoder는 메세지를 재구성하는 동안에 하위 bit를 선택적으로 resotre할 수 있다. 이렇게 함으로써 메세지가 첨부되어있음에도 불구하고 원래의 압축과 거의 유사한 이미지를 만들어내게 된다. 실제 메세지가 첨가됨으로 인한 차이는 인식할 수 있을 정도가 되지 않으며 후속적인 처리 과정이나 개인인증의 기능에 전혀 영향을 주지 않는다. (그림 4)는 위와같은 결과로 만들어진 이미지를 원 이미지와 비교를 해주고 있다.

이와같은 처리 과정을 이용함으로 인해 아주 특별한 DECODER만이 decoding 동안에 압축된 영상으로부터 위치를 알고 해당하는 메세지를 추출할 수 있다. 즉, Decoder에서 Random number generator를 가지고 있다면, 메시지가 은닉되어 있는 주파수 밴드로부터 은닉 메시지를 확인할 수 있다. 이 메세지는 인증서나 개인 ID와 같이 섞어서 사용할 수가 있다. 따라서 만약에 bit stream이 메세지를 갖고 있지 않다거나 다른 형태를 가질 경우에는 이 특수한 decoder는 특별한 메세지의 추출이 실패하여 이 영상을 거절하게 된다. 같은 많은 알고리즘이 실제 구현됨에 있어서는 서로 다른 rendom number generator를 사용하기 때문에 큰 노력이 없이도 모든 구현을 유일한 것이 될 수 있도록 할 수 있다. 또한 하나의 결과가 다른 decoder의 결과와는 부분적으로도 같을 수 없다. 따라서 한 version을 크랙킹했

더라도 다름 버전에서는 사용이 불가능하다. 이와 같은 방법을 사용하게 되면, 해커가 센서로부터 전송되는 압축 지문영상을 가로챘더라도, Data Hiding Algorithm을 갖지고 있지 못한다면 압축 지문영상의 재사용이 불가능 하게 된다.

3.2 Image-based challenge/response method

앞에서 언급한 네트워크 트래픽 인터셉션(interception)이 외에도 여러 가지가 있을 수 있는데 자동 지문인식 시스템에 대한 교활한 방법 중의 하나로, 지문 센서로부터 나오는 신호를 공격하는 것이다(공격포인트 2). 이러한 공격을 방지하기 위한 새로운 방법이 변형된 challenge/response 방법이다. 기존의 일반적인 challenge/response 방법에서는 사용자에게 어머니의 처녀시절의 이름을 요구하는 등의 challenge나 특수목적의 계산기와 같은 물리적인 장치에 대한 challenge를 요구하는데 근거를 두고 있었다. 여기서는 사용자의 ID만 확인하는 것이 아니라, Sensor Device의 정보를 확인하는 시스템을 제안한다. 센서는 challenge에 반응을 할 수 있는 충분한 기능을 가지고 있기 때문이다. 물론 기존의 암호화 기술이 있기는 하지만 이는 확실한 답이 될 수가 없다. 수학적으로는 충분히 강력한 기능을 가졌다고 할 수는 있지만 수많은 센서에 대한 비밀 키를 관리 운영해야 한다. 더구나 암호화 방법은 시그널에 대한 liveness 체크는 불가능하다. 전호에서 논의 했던 다양한 가짜지문에 대한 대비가 전혀 불가능하다. 즉, 디지털화 되었을 경우에는 그것의 정확성은 체크할 수 있으나 liveness는 구분이 불가능하다. 여기서는 response string을 계산하는 것이다. 이것은 challenge string과 되돌아온 영상에도 관계를 한다. 그러면 challenge string을 바꾸기만 하면 획득한 영상이 challenge가 발생한 이후에 만들어진 것인지를 알 수가 있다. 영상 자체의 픽셀 값에 의해서 만들어지기 때문에 반응이 일어난 후의 다른 가짜 영상에 대해서는 구별이 가능하다.



challenge/response

(그림 17)은 위와 같은 시스템의 흐름을 보여주고 있다. 트랜잭션이 처음에 사용자 단말기나 서버에서 발생한다. 처음에 서버는 트랜잭션이나 서버를 위한 랜덤 challenge code를 만든다. 물론 지문 센서는 사람의 Liveness를 검사할 수 있으며, Transaction Server는 보안성을 유지한다는 가정이 있어야 한다. 그러면 클라이언트 시스템은 이 challenge를 센서에 보낸다. 그러면 센서는 새로운 영상을 얻고 이 영상과 challenge code를 이용, 새로운 response를 만든다. 물론 response processor와 sensor는 tightly coupled 되어 있어야한다. 예를 통해서 위의 시스템의 흐름을 살펴보기로 하자.

지문 센서에 대한 외부의 공격을 막기 위해, 지문 센서의 동작을 서버에서 제어하게 되는데, 센서의 제어를 위해 서버에선 Pseudorandom 함수를 클라이언트에 전송해주며, 센서-프로세서는 이 함수를 이용해 서버에 Challenge String을 전송하게 된다. Pseudorandom 함수로 사용할 수 있는 함수는 매우 많으며, 예로 서버에서 "3,10,50" 이란 명령을 클라이언트에게 하게 되면, 센서는 현재 입력하려는 사용자의 지문 영상으로부터 3, 10, 50 번째 gray pixel 값을 취득하여 일정한 규칙에 따라 새로운 string "133,

92, 176" 을 만든다. 이런 값을 Response string이라 정의하며, 이것은 서버로 전송된다. 반응 프로세서는 여러 가지 복잡한 response 함수를 사용할 수도 있다. 픽셀 수가 많은 간단한 함수가 적용될 수 있기 때문에 많은 그리고 다양한 response string을 만들 수가 있다. 만약, 해커가 관리자의 감독을 피해 센서로부터 지문 영상을 취득하려 하여도, 센서와 센서-프로세서가 One Chip으로 되어있어, 서버로부터 명령받는 Pseudorandom 함수 없이는 센서의 사용이 불가능해진다. 또한 Response string은 입력 영상에 종속적이어서 그 값은 항상 변하게 된다. 결국 센서-프로세서의 해킹 없이는 해킹이 불가능하다.

4. Cancelable Biometrics

신용카드 인증, 은행 ATM 접근 등과 같은 큰 시장에 생체 인식 제품을 적용하려면 트랜잭션에 대한 보안뿐만 아니라 그 이상의 부가적인 상황이 발생하게 된다. 이것은 가능성이 있는 개인 프라이버시의 침해에 대한 부분이다. 이름이나 생년월일 등과 같은 개인 신상에 대한 정보뿐 아니라 사용자는 지문, 얼굴, 홍채 등의 개인 신체의 일부에 대한 정보가 도난당할 수 있다는 것이다. 이들 영상이나 다른 생체 정보는 다양한 데이터베이스에 디지털 형태로 저장된다. 이렇게 디지털로 저장된 데이터가 범죄 수사와 같은 수사기관이나 은행이나 기타 인터넷을 이용하는 다른 상업적인 사업체에서 공유될 수 있다는 사실이다.

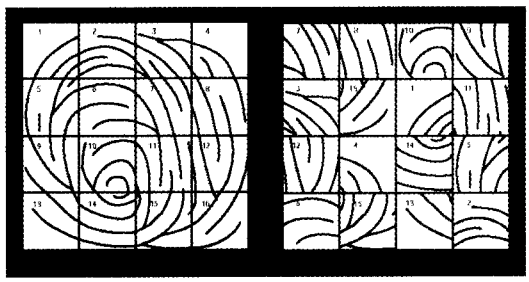
대중들은 우리 사회에서 개인에 관한 신상 및 신체의 일부에 대한 디지털화된 정보가 점차 상당한 속도로 증가하고 있다는 사실에 귀를 기울이게 된다. 이렇게 모아진 데이터가 많은 응용분야에서 사용되고 있으며 이들에는 의료기록이나 신체정보도 포함되고 있다. 그럼으로 인하여 다양한 데이터베이스로부터의 데이터를 공유하고 상호 협력할 수 있다는 것이 또한 큰 관심사가 되지 않을 수 없다. 생체 정보와 관련해서는 대중은 개인 회사에서 모아진 데이터가 범죄 수사용으로 사용되어질 수도 있다는 사실이다. 예를 들어서 지문의 경우 좋지 않은 결과를 위해서 FBI나 INS (Immigration and Naturalization Service)와 일치여부를 확인하는데 사용될 수 있다는 것이다. 한 사람의 생체인식 정보가 주어지면 이것은 다시는 바꿀 수 없다는 사실 때문에 더욱 더 큰 관심을 불러일으키고 있다. 생체 정보가 개인인증용으로 사용되어질 수 있는 가장 큰 이유 중의 하나는 시간의 흐름에도 크게 변하지 않는다는 것이다. 만약에 신용카드 번호가 피해를 입었을 경우 발행은행에서는 사용자에게 새로운 신용카드 번호를 부여함으로써 문제를 최소화할 수가 있다. 그러나 생체정보의 경우에는 데이터가 도용되고 있음에도 불구하고 바꿀 수 없다는 것이다. 위와 같은 문제를 줄이기 위해서는 생체정보를 취소할 수 있는 시스템이 되어야 하다. 일반적으로 이를 "Cancelable Biometrics[1]" 라고 부른다. 이것은 선택한 함수를 이용해서 의도적이면서도 반복 사용가능한 생체정보의 변형을 할 수 있는 것이다. 매번 등록이나 인증 시에 생체정보가 나타나면 같은 방법으로 정보를 변형하는 것이다. 이와 같은 방식으로 매번등록 시 마다 서로 다른 변형함수를 사용함으로써 크로스 매칭이 불가능하도록 하는 것이다. 더구나 변형된 생체정보가 도용되었을 경우에는 재등록을 위해서 다른 변수를 사용함으로써 변형함수를 간단하게 바꿀 수 있다. 즉 새로운 사람으로 인식되는 것이다. 일반적으로 변형함수는 noninvertible하게 만들어서 사용한다. 그래서 설사 변형함수가 알려지거나 심지어는 변형된 생체정보가 알려지더라도 원래 변형되기 전의 생체정보는 복구가 불가능하다.

4.1 변형 함수

이와 같은 방법에서는 변형함수가 signal domain 이나 feature domain에서도 적용될 수 있다. 즉, 생체정보를 획득한 바로 후에 직접 변형을 할 수도 있고 아니면 평상시처럼 시그널을 처리한 후 추출한 특징을 변형하는 방법도 가능하다. 더우기 하나의 템플릿을 좀 더 넓게 확장하여 시스템의 blt strength를 더욱 강하게 할 수도 있다. 가장 이성적으로는 변형함수가 반드시 noninvertible해서 다양한 기관이나 회사 등에서 저장된 변형된 데이터를 이용해서는 원 영상을 복구할 수가 없어야 한다. signal 차원에서의 변형함수로는 grid morphing이나 block permutation 등을 들 수가 있다. 이렇게 변형된 영상은 원 영상과 성공적으로 매칭이 될 수가 없으며 같은 영상의 다른 인수에 의해 변형된 영상과도 매칭이 될 수가 없다. 변형 가능한 템플릿 방법을 사용하게 되면 이와 같은 매칭이 이루어 질 수도 있으며 잔상이 관계없는 영상과의 매칭에 많은 영향을 줄 수가 있다.

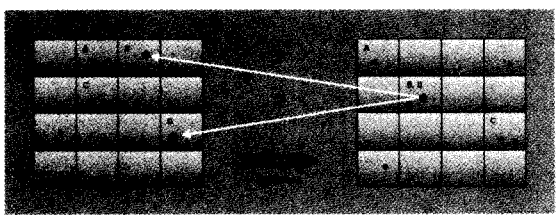
(그림18) Distortion transform based on image morphing

(그림 18)은 Image Morphing[5]에 의한 변형을 보여주고 있는데 왼쪽의 원 영상은 얼굴위에 그리드를 올려놓은 것처럼 보인다. 오른쪽의 경우에는 동일한 얼굴에 대한 morphing된 결과를 보여 주고 있다. (그림 19)는 블록 구조를 특징점이 원 영상에 위치된 형태로 조합된 것이다.



(그림19) Distortion transform based on block scrambling

Feature Domain 상에서 변형된 예로는 특징점의 Random, Repeatable perturbation set을 들 수가 있다. 이것은 원영상과 동일한 물리적인 공간에서 이루어질 수 있다. (그림 20)은 feature perturbation에 근거한 변환을 보여주고 있다. 여기서 왼쪽에 있는 block은 랜덤하게 오른쪽에 있는 block에 사상되고 있다. 물론 여러 개의 block이 같은 오른쪽 block에 사상될 수도 있다. 이와 같은 변형은 noninvertible하기 때문에 변형된 것을 이용해서는 원래의 특징을 찾을 수가 없다.



(그림 20) Distortion transform based on feature perturbation

예를 들어서 위 그림에서 오른쪽의 포인트 B, D가 어느 블록에서 왔는지는 알 수가 없다. 결과적으로 등록 시에 있었던 특별한 정가 없이는 생체정보의 주인이 누구인지를 확인할 수가 없다는 것이다. 그러나 변형이 repeatable하게 되기 위해서는 생체 시그널을 변형 전에 어디엔가 저장을

해두어야 한다.

4.2 Feature Domain Transforms

이제 point pattern 에 대한 noninvertible 한 예를 들어서 살펴보기로 하자. 이와 같은 point pattern은 다음과 같이 지문의 특징점의 집합으로 표현될 수 있다.

$$S = \{ (xi, yi, \theta i),\ i = 1, \ldots, M \}$$

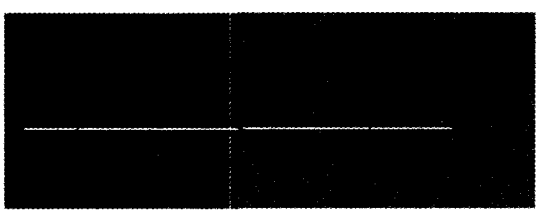
물론 이 집합은 다른 생체정보(음성의 주파수나 크기)를 나타낼 수도 있다. Noninvertible 함수는 이 집합 S를 새로운 집합 S' 로 변형을 할 수 있으나 원래 S는 S' 를 이용해서 복구가 불가능하다.

$$S = \{ (xi, yi, \theta i),\ i = 1, \ldots, M \} \rightarrow S' = \{ (Xi, Yi, \theta i),\ i = 1, \ldots, M \}$$

(그림 21)은 point set S의 x 좌표가 어떻게 mapping 함수 F(x)를 통해서 변형되는지를 보여 주고 있다. 여기서 F(x)는 고차원 polynomial

$$X = F(x) = \alpha nxn = \pi (x - \beta n)$$

으로 표현할 수 있다.



(그림 21) Example of Noninvertible Feature transform

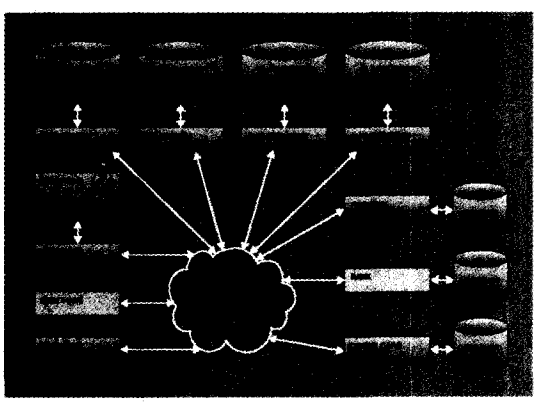
위 그림에서 보는바와 같이 x → X 은 1 대 1 사상이다. 그러나 X → x 방향은 1 대 다 사상이다. 예를 들어서 출력값 중의 하나인 X1 은 서로 다른 세 개의 입력값 x 로부터 만들어진 것이다. 그러므로 이 함수는 noninvertible 함수라고 할 수 있으며 원래의 특징인 x 는 X 로부터 복구가 불가능하다. 유사한 polynomial noninvertible 함수로는

$$Y = G(y) \quad \text{and} \quad \theta = H(\theta)$$

가 point set의 다른 좌표 등을 위해 사용될 수도 있다.

5. 결 론

생체정보의 변형을 위해서 여기서 사용되고 있는 기술은 시그널이나 영상처리기술을 이용한 단순한 압축과는 엄연히 차이를 두고 있다. 영상압축에 의한 것은 공간 도메인의 특징을 어느 정도의 손실을 감수해야만 하지만 이 기술은 모든 정보를 보전할 수 있다. 즉, 두 개의 포인트를 사용할 경우 압축전의 거리를 압축 후 다시 압축을 풀었을 때와는 어느 정도의 차이를 가지고 있다는 것이다. 이와 같은 현상이 distortion transform 에서는 발생하지 않는다. 또한 이 기술은 압축과는 또 다른 점이 있다. 암호화의 목적은 원래의 신



(그림 22) Authentication Process based on Cancelable Biometrics.

호를 합법적인 부분을 재생산하는 것이다. 반면에 distortion transform은 noninvertible 한 방법으로 신호를 영원히 감지할 수 없도록 만드는 것이다.

Cancelable Biometrics를 적용하려면 transform 함수나 그의 매개변수, 그리고 인식 템플릿을 저장할 수 있는 장소가 여러 군데 있어야 한다. 이를 생각하면 (그림 22)처럼 가능한 분산처리 모델로 정립함이 필요하다.

위 그림에서 보는 바와 같이 "merchant" 가 이 모델에서의 모든 내부 활동이 시작되는 시발점이 된다. customer ID에 근거를 해서 해당하는 변형함수를 변형함수 데이터베이스에서 가지고 온다. 그 후에 이를 해당 biometrics에 적용하는 것이다. 그러면 그 결과 변형된 biometrics는 인증을 위해 "Authorization" 서버에 보내지게 된다. 일단 사용자의 Identity가 확인되면 transaction이 처리를 필요로 하는 마지막 국가관이나 은행, 신용카드 회사 등으로 보내지게 된다. 한 사람이 여러 가지 기관이나 여러 가지 서비스를 위해 다양한 서비스를 등록할 수 있다는 것을 고려한다면 각각의 transaction 단위로 서비스 제공자에 의해서 각각이 독립적으로 인증이 이루어져야 함을 알 수가 있다. 마찬가지로 변형함수 역시 인증기관이나 기타 다른 독립적인 기관에서 관리함이 전체 시스템의 보안을 위해서는 필요하다고 본다. 아니면 개인의 프라이버시를 위해 개인 자신이 자기 자신의 변형함수를 스마트카드 등에 보관함도 또한 한 방법이 될 수도 있다. 만약에 카드를 분실하거나 도난당했을 경우에도 이 변형함수를 다른 사람의 생체 정보에 적용한다고 하더라도 큰 충격을 주지는 못할 것이다. 그러나 변형된 함수가 진짜 사용자 자신의 저장된 생체 정보에 적용될 경우에는 그 사람의 저장된 템플릿과의 매칭이 이루어 질 것이다. 그래서 이런 잘못된 사용을 방지하기 위해서는 "Liveness" 여부를 체크하는 시스템의 적용이 필요하다.

생체정보를 이용한 본인 인증은 기존의 패스워드에 비해 많은 사용상의 장점을 가지고 있다. 특별히 사용자는 자신의 정보를 아무리 나이가 어린 아이일지라도 결코 분실하지는 않는다. 앞에서 언급되어 있듯이 생체 정보는 기존의 패스워드보다는 비트 강도가 강함을 살펴보았다. 그러나 생체정보를 사용하는 시스템을 포함해서 어떠한 시스템이던지 미리 준비한 해커에 의한 공격에 대해서는 거의 무방비 상태일 수가 있다. 전형적인 생체인증 시스템에서의 가능한 공격 포인트를 8가지 정도로 분류해서 살펴보았다. 그리고 이를 방지하기 위한 몇 가지 정도의 방법에 대해서 살펴보았으며, 아울러 지속되는 공격에 대해서는 압축된 지문신호에 직접적으로 일정한 양의 mark를 첨부해서 사용하는 data-hiding 기술이나 센서로부터 얻어진 신호에 대한 생체의 확인은 challenge/response 기법으로 해결할 수 있음을 살펴보았다. 마지막으로 가끔 간과할 수 있는 개인 프라이버시 문제와 생체정보의 철회문제를 살펴보았다. 생체인식의 가장 강력한 힘인 시간의 흐름에도 변하지 않는다는 것이 오히려 동시에 가장 큰 문제가 될 수 있다는 사실은 참으로 역설적인 사실이 아닐 수 없다. 먼저 다른 생체 정보를 사용하고자 하더라도 개인이 가지고 있는 사용가능한 생체정보에는 한계가 있다. 일반적으로 10개의 손가락, 2개의 눈, 한 개의 얼굴, 2개의 손 등이 우리가 쉽게 생각할 수 있는 한계이다. 일단 생체정보가 도용되면 이는 더 이상 바꿀 수 없다는 것이다(Once compromised, compromised forever). 이와 같은 문제를 해결하기위한 일환으로 생체정보에 반복사용이 가능하고 복구가 불가능한 변형법을 적용하는 것이다. 취소는 단순히 새로운 distortion 함수를 사용하면 가능하다. 아울러 개인의 프라이버시 문제도 한층 더 강화 될 수 있다. 왜냐하면 서로 다른 서비스나 응용분야

에 대해서 서로 다른 변형 함수를 사용하기 때문이며(Different distortions for different accounts) 실제 생체정보는 저장되지 않을 뿐 아니라 나타나지도 않기 때문이다.

그러나 이러한 시스템을 구축하는데에는 아직도 생각해야 할 여지가 많이 남아있다. 그중에 하나는 변형함수를 어디에 안전하게 저장하느냐 하는 것이다. 앞에서 언급을 했지만 (그림 22)처럼 서버에 저장하는 경우 서버에 대한 보안이 기본적으로 전제되어야 한다. 아니면 개인이 소요하는 스마트카드 등에 저장 보관하게 되면 보안성 및 프라이버시 문제도 좀 더 확실하게 해주는 역할을 할 것이다. signal 이나 feature 기반의 distortion transform model 중 어느 것이 더 효과적인지는 뚜렷한 통계적 근거가 아직은 없는 상태다. 때에 따라서는 두 가지를 섞어서 사용하는 방법도 가능할 것이다. 앞에서 언급되었던 가짜 지문이나 위장 얼굴 등에 대해서 어떻게 처리할 것인가. 즉, 이들을 가지고 변형함수가 있는 database에 접근을 하게 되면 해결책을 찾을 수 없다. 또한 한 개의 지문이나 얼굴에 대해서 몇 가지 정도의 함수를 사용할 수 있을지? 마지막으로 이러한 시스템의 경우 에러율은 어떻게 변하는가에 대한 연구가 이루어져야한다. 또한 Cancelable biometrics 기술은 raw biometric data에 noninvertible 변형함수를 적용함으로써 항상 재사용이 가능하게는 할 수 있으나 모든 응용분야별로 따로 템플릿이나 데이터를 저장해야 하는 번거로움은 여전히 존재하게 된다. 즉, 한번 등록된 데이터를 공유할 수 있는 방법은 제공하고 있지 않다는 것이다[6]. 각각의 응용분야별로 유일한 포맷을 만들 수 있도록 하고 한 포맷에서 다른 포맷으로의 변환을 가능하도록 해준다면 매 응용마다 재등록을 할 필요도 없이 사용자의 인정하에 응용분야간 템플릿을 공유할 수가 있다. 그리고 매칭은 변형된 템플릿에서 이루어지도록 시스템을 디자인하면 단순한 Cancelable Biometrics 보다 더 효과적인 템플릿 관리가 될 수 있을 것이다.

참고문헌

[1] Ratha,N. and Connell,J., "Cancelable Biometrics," presented at Biometric Consortium 2000 Conference Sept. 13-14, 2000

[2] Nalini K. Ratha, Janathan H. Connell, and Ruud M. Bolle, "An Analysis of Minutiae Strength," IBM System Journal, Vol.39, No.3, 2000

[3] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino, " Impact of Artificial Gummy Fingers on Fingerprint System," Optical Security and Counterfeit Deterrence Technique 4, Vol. 4673, pp 275-289. 2002

[4] N.K. Ratha, J.H. Connell and R.M. Bolle, " Secure Data hiding in wavelet compressed fingerprint images," Proc. of the ACM Multimedia workshop on Multimedia and Security, Nov. 2000, pp.127-130

[5] G. Wolberg, "Image Morphing : A Survey," The Visual Computer 14, pp 360-372,1998

[6] Michael Braithwaite, UIF Cahn von Seelen, James Cambier, and John Daugman, " , Application - Dependent Biometriv Templates," Presented at Biometric Comsortium 2001 conference, Feb. 13-15, 2002

저자약력

이 남 일

1977년~1988년 경북대학교 전자공학과 학사
1981년~1986년 경북대학교 전자공학과 석사
1989년~1993년 경북대학교 전자공학과 박사
1995년~1996년 University of Washington 교환 교수
1986년~1989년 부산 동의공업대학 전임강사
1989년~1999년 안동대학교 부교수
2000년~현재 (주)시큐아이티 상무