情報保護學會論文誌
第16卷 第6號, 2006. 12

원격응용에 적합한 지문 정보 보호*

문 대 성,[1†] 정 승 환,[1] 김 태 해,[1] 이 한 성,[1] 정 용 화,[1‡] 양 종 원,[2] 최 은 화,[2] 서 창 호[2]

[1]고려대학교, [2]공주대학교

Protecting Fingerprint Data for Remote Applications

Daesung Moon,[1†] Seunghwan Jung,[1] Taehae Kim,[1] Hansung Lee,[1]
Yongwha Chung,[1‡] Jongwon Yang,[2] Eunwha Choi,[2] Changho Seo[2]

[1]Korea University, [2]Kongju University

요 약

본 논문에서는 지문 센서-클라이언트-서버 모델의 원격 지문 인식 시스템을 이용한 안전하고 효과적인 사용자 인증 방법을 제안한다. 특히, 실시간성, 확장성, 프라이버시 이슈 등을 고려하여 지문 인식 과정 중 가장 많은 계산시간을 필요로 하는 지문 특징 추출 과정을 클라이언트에 할당하는 일반적 구현과 달리, 클라이언트가 일반 사용자에 의해 관리되어 여러 공격에 취약할 수 있다는 가정하에서도 동작할 수 있는 방법을 제안한다. 즉, 지문 센서와 서버 사이에 위치한 클라이언트를 신뢰할 수 없는 경우라도 실시간성, 확장성, 프라이버시 이슈 등을 만족하기 위해서는 클라이언트를 활용할 수밖에 없으며, 지문 센서나 서버에서는 신뢰할 수 없는 클라이언트에게 위임하여 생성된 지문정보를 검증해야 한다. 또한, 자원 제약적인 지문센서가 클라이언트가 생성한 지문 정보를 실시간으로 검증하기 위해서는 검증 과정 자체가 간단해야 된다는 제약이 있다. 본 연구에서는 이러한 문제를 해결하기 위해 지문 특징 추출 과정을 이진화와 특징점 추출 과정으로 분리하여, 클라이언트에서 이진화 과정을 실행하고 지문 센서에서는 클라이언트로부터 받은 이진화 결과의 정당성을 확인하기 위한 경량화된 검증 방법을 수행한다. 검증 후 이상이 없으면 클라이언트로부터 수신한 이진 영상에서 특징점을 추출한 후 서버로 전송한다. 제안된 방법의 타당성을 확인하기 위해 지문 영상을 이용한 실험을 수행한 결과, 제안된 방법이 지문 센서-클라이언트-서버 모델에서 실시간으로 안전하게 수행될 수 있음을 확인하였다.

ABSTRACT

In this paper, we propose a secure solution for user authentication by using fingerprint verification on the sensor-client-server model, even with the client that is not necessarily trusted by the sensor holder or the server. To protect possible attacks launched at the untrusted client, our solution makes the fingerprint sensor validate the result computed by the client for the feature extraction. However, the validation should be simple so that the resource-constrained fingerprint sensor can validate it in real-time. To solve this problem, we separate the feature extraction into binarization and minutiae extraction, and assign the time-consuming binarization to the client. After receiving the result of binarization from the client, the sensor conducts a simple validation to check the result, performs the minutiae extraction with the received binary image from the client, and then sends the extracted minutiae to the server. Based on the experimental results, the proposed solution for fingerprint verification can be performed on the sensor-client-server model securely and in real-time with the aid of an untrusted client.

Keywords : *Fingerprint verification, sensor-client-server model, Real-Time Processing*

접수일: 2006년 8월 4일 : 채택일: 2006년 9월 29일
* 본 논문은 2004년 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2004-002-D00388).

† 주저자, daesung@korea.ac.kr
‡ 교신저자, ychungy@korea.ac.kr

Ⅰ. 서 론

정보시스템에 접근하기 위한 사용자 인증 방법으로 패스워드 또는 PIN(Personal Identification Number)을 이용한 사용자 인증 방법이 현재까지 널리 쓰이고 있으나 타인에게 노출되거나 잊어버리는 등의 문제가 있다. 최근에는 이러한 문제를 해결하기 위하여 개인의 생물학적 특징이나 행동학적 특징 등의 바이오 정보를 이용한 사용자 인증 방법이 대안으로 떠오르고 있다. 본 논문에서는 다양한 바이오 정보 중 가용성, 정확도, 경제성면에서 현재까지 가장 현실적인 대안으로 평가받고 있는 지문을 선택하였다[1].

현재의 지문 인식 시스템은 안전한 액세스 관리와 주거지 접근통제 등의 좁은 범위에서 사용되고 있지만, 향후 인터넷을 통한 원격 신원 확인 등의 다양하고 광범위한 범위에서 사용될 것으로 기대된다. 그러나 원격응용에서 지문을 포함한 바이오 인식 시스템을 적용하려면 공통적인 문제를 해결해야 한다. 예를 들어, 지문 센서가 클라이언트와 연결되고 클라이언트는 인터넷을 통해 서버에 연결된 모델에서, 통신 채널에서 발생하는 "Replay Attack"과 시스템 모듈에서 발생하는 "Trojan Horse Attack" 등에 대한 안전이 보장되어야 한다[2]. 그러나 Replay Attack으로부터 전송되는 지문정보를 보호하기 위한 연구들은 일부 보고되고 있으나[1-5], Trojan Horse Attack 등의 시스템 모듈에 대한 공격으로부터 지문 인식 시스템을 보호하기 위한 사전 연구는 아직 보고되지 않고 있는 실정이다.

또한, 지문인식 시스템에서 사용자의 중요한 지문정보(원 지문영상, 지문 특징점)를 안전하게 보호하기 위한 사전연구들은 대부분 Replay Attack에 관한 것으로써, 서버에 저장되어 있는 지문의 특징점을 안전하게 보호하기 위한 방법[6-7]에 관한 내용과 지문센서에서 획득된 지문영상 자체를 실시간 암호알고리즘을 이용하여 안전하게 전송하는 방법[8]에 관한 것이 대부분이다. 하지만, 센서에서 획득된 지문영상이 다양한 전송채널을 통해서 전송하는 도중 공격자에게 가로채일 경우 개인의 프라이버시 문제가 심각하게 대두되기 때문에 지문의 특징점 정보만을 전송하는 것이 타당하다.

일반적으로 지문 인식 시스템은 지문 획득, 특징 추출, 특징 정합 모듈로 구성되어 있다. 실시간성, 확장성, 프라이버시 이슈 등을 고려할 때 일반적인 지문 센서-클라이언트-서버 모델에서의 지문 인식은, 센서에서 지문 영상을 획득하고, 클라이언트는 지문 영상으로부터 특징 정보를 추출하며, 마지막으로 서버는 DB안에 저장된 특징 정보와 추출된 특징 정보를 비교한다[1]. 여기서 서버는 안전한 장소에서 보안전문가에 의해 보호되고, 지문 센서는 하드웨어적으로 공격에 안전한 장치인 보안토큰에 통합[9]될 수 있으나, 클라이언트는 보안전문가가 아닌 일반 사용자에 의해 관리된다고 가정할 수 있다. 즉, 클라이언트의 특징 추출 모듈은 여러 공격에 매우 취약할 수 있으나, 실시간성, 확장성, 프라이버시 이슈 등을 고려할 때 가장 많은 계산시간을 요구하는 지문 특징 추출 단계를 지문 센서나 서버에 할당하지 못하고 신뢰할 수 없는 클라이언트를 활용할 수밖에 없는 경우가 발생한다.

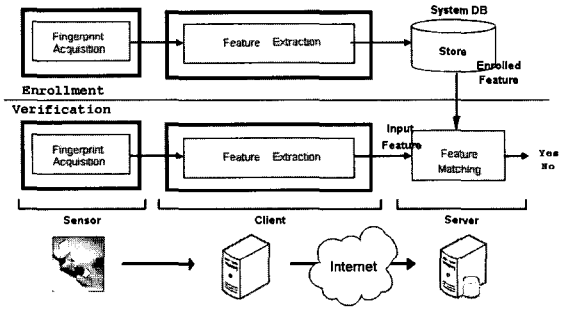
이러한 환경에서 지문 인식을 안전하게 수행하기 위해서는 신뢰할 수 없는 클라이언트에게 지문 특징 추출의 상당 부분을 위임하되 이렇게 클라이언트에 의해 생성된 특징 정보 추출 결과에 대한 지문 센서의 검증이 필요하다. 본 논문에서는 지문 센서-클라이언트-서버 모델에서 클라이언트를 신뢰할 수 없는 경우에 실시간성, 확장성, 프라이버시 이슈 등을 만족하는 지문 인식 및 지문 정보 보호 방법을 제안한다.

본 논문의 구성은, 2장에서 일반적인 지문 인식 시스템에서 발생할 수 있는 공격들을 설명하며, 3장에서는 제안하는 지문 인식 및 지문 정보 보호 방법을 설명한다. 제안된 방법의 성능 평가를 4장에서 기술하며, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 지문 인식 시스템

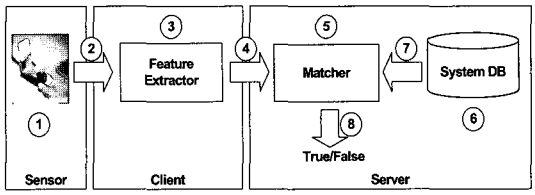
지문 인식 시스템은 [그림 1]과 같이 등록과 인식 과정으로 구성된다. 오프라인에서의 지문 등록은 지문 영상 전처리, 특징 추출, 그리고 서버에 저장하는 순으로 진행된다. 그리고 인식 단계는 지문 획득, 특징 추출, 그리고 특징 정합 3가지 모듈로 구성된다[1]. 지문 획득은 각 사용자들이 센서에 지문을 접촉함으로서 획득되고, 특징 추출 모듈은 획득한 지문 영상으로부터 특징 정보를 추출한다. 마지막으로, 특징 정합 모듈은 입력된 지문의 특징 정보와 서버의 DB안에 저장되어 있는 특징 정보를 비교한다. 이때, 전체 지문 인식 시스템 중 지문 영상 전처리와 특징 추출 단계에서 많은 산술 연산이 필요하며, 전체 시스템 작업부하의 96%를 차지한다[10]. 특히,

지문 인식의 정확도가 지문 특징 추출 과정의 정확도에 크게 의존하기 때문에 많은 지문 인식 알고리즘들이 복잡한 특징 추출 과정을 수행하여 일반 PC에서 수행하더라도 수초가 소요되며[11], 이러한 계산 시간을 줄이기 위한 임베디드 시스템용 하드웨어 구현 결과[12]가 발표되고 있는 실정이다. 따라서 실시간적 요구사항을 만족하려면 작업부하가 큰 두 단계를 자원 제약적인 센서보다는 계산능력이 월등한 클라이언트 또는 서버에 할당하는 것이 적합하다. 그러나 서버에 특징 추출 단계를 할당하면 지문 원영상이 서버로 전송되어 최근 이슈가 되고 있는 프라이버시 문제[13]를 해결할 수 없고, 대규모 응용의 경우 확장성 문제가 발생한다. 즉, 실시간성, 확장성, 프라이버시 이슈 등을 고려할 때 일반적인 지문 센서-클라이언트-서버 모델에서의 지문 인식은, 센서에서 지문 영상을 획득하고, 클라이언트는 지문 영상으로부터 특징 정보를 추출하며, 마지막으로 서버는 DB안에 저장된 특징 정보와 추출된 특징 정보를 비교하는 방식을 따른다[1].



〔그림 1〕 일반적인 지문 등록 및 인식 과정[1]

앞서 언급한대로 센서가 특정 클라이언트에 고정되어 연결되고 클라이언트와 서버는 오픈 네트워크로 연결된 센서-클라이언트-서버 모델에서는 많은 공격 포인트가 발생된다[2]. 예를 들어, 〔그림 2〕처럼 ①센서, ②센서와 특징 추출기간의 채널, ③특징 추출기, ④특징 추출기와 정합기간의 채널, ⑤정합기, ⑥데이터베이스시스템, ⑦데이터베이스와 정합기간의 채널, ⑧정합기와 응용간의 채널 등의 공격 포인트를 생각할 수 있다. 특히, ①, ③, ⑤, ⑥의 공격은 시스템 모듈에서 발생하기 때문에 매우 유사한 특성을 가지며, 일반적으로 Trojan Horse Attack으로 통칭된다[1]. 본 논문에서는 원격 지문인식 시스템의 ③에서 발생할 수 있는 Trojan Horse Attack과 ②와 ④에서 발생할 수 있는 Replay Attack을 고려한다.



〔그림 2〕 가능한 공격포인트[2]

현재까지 이러한 원격 지문 인식 시스템에서 발생할 수 있는 공격들을 막는 많은 방법이 연구되어왔다. 그러나 대부분 통신 채널[4,5]이나 특징 정합 모듈상에서 가능한 공격만을 고려하였다[14]. 그러나 실시간성, 확장성, 프라이버시 이슈 등을 고려할 때 지문 인식 과정 중 가장 많은 계산을 요하는 지문 특징 추출 과정을 클라이언트에 할당해야 하는 상황에서 클라이언트가 공격취약성으로 인해 신뢰할 수 없는 경우에도 동작할 수 있는 원격 지문 인식 시스템에 대한 사전 연구는 발표되지 않고 있는 실정이다.

Ⅲ. 원격 지문 인식 시스템 구현

본 논문에서는 센서가 특정 클라이언트와 연결되어 있고, 클라이언트는 인터넷을 통하여 서버와 연결되어 있다고 가정한다. 또한, 센서, 클라이언트, 서버는 암호화와 복호화를 위하여 공개키와 개인키가 필요하다고 가정한다. 키 분배 문제는 본 연구의 범위가 아니며, 이 문제를 해결하기 위한 많은 방법이 발표되어 있다[12].

3.1 신뢰할 수 없는 클라이언트를 활용한 안전한 지문 인식

본 논문에서는 자원 제약적인 센서의 작업부하를 줄이기 위해 특징 추출 모듈을 이진화와 특징점 추출 과정으로 구분한다. 이진화 과정은 특징 추출 모듈에서 이진화 지문 영상을 생성하고, 특징점 추출 과정은 이진화 지문 영상으로부터 특징점을 추출한다. 앞서 언급했듯이 지문 영상의 이진화는 많은 계산량을 요구하고, 특징점은 지문 영상의 이진화 결과로부터 쉽게 추출될 수 있다. 따라서 클라이언트와

센서에 각각 이진화와 특징점 추출 과정을 할당하는 것이 합리적이다. 본 논문에서는 신뢰할 수 없는 클라이언트에서 이진화 과정을 통해 생성된 정보를 센서가 수신하여 특징점을 추출하는 방식을 이용하여 원격응용에 적합한 지문 정보 보호 방법을 제안한다. 시스템의 구성요소 및 역할은 다음과 같다.

- 센서 : 센서는 지문 정보를 읽을 수 있는 기능뿐만 아니라 지문 정보를 암복호화 할 수 있는 스마트 센서를 사용한다. 또한, 신뢰할 수 없는 클라이언트에서 계산된 이진화 결과를 검증하기 위해 경량화된 이진화 검증 알고리즘을 실행 할 수 있으며 검증이 확인되면 클라이언트에서 수신한 이진화 결과로부터 실시간으로 특징점을 추출할 수 있다.
- 클라이언트 : 클라이언트는 지문 정보에서 특징정보를 추출하기 위하여 이진화 과정을 실행한다. 그리고, 센서와 서버간 지문 정보 전송을 실행할 수 있다.
- 서버 : 서버는 저장되어진 지문 정보와 입력되어진 지문의 특징점 정보를 이용하여 정합을 실행한다. 인증과정에서 발생하는 정보 중에 서버와 클라이언트, 클라이언트와 서버 간에 발생되는 정보는 세션키로 보호되며 서버와 센서 간에는 센서의 개인키 및 공개키로 보호된다.

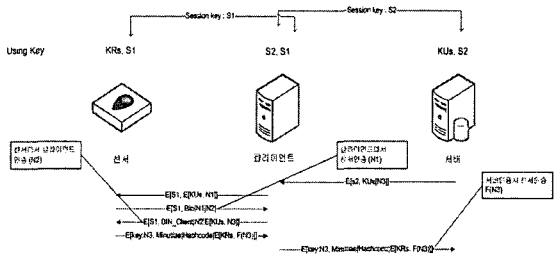
3.1.1. 기호 설명

- KUs, KRs : 센서의 공개키, 개인키
- S1, S2 : 서버와 클라이언트, 클라이언트와 서버 간 세션키
- Bio : 지문 정보
- BIN_Client : 클라이언트에서 생성된 이진화 영상
- Minutiae : 지문 특징점
- Hashcode : 지문 특징점의 해쉬값
- E(K, M) : 키를 K로 하여, 메시지 M을 암호화
- N1, N2, N3 : 센서, 클라이언트, 서버의 메시지 인증에 사용되는 난수
- Key:N3 : N3을 이용하여 생성된 키
- F(N3) : N3을 이용한 임의 함수3

3.1.2. 지문 인식 프로토콜

〔그림 3〕은 신뢰할 수 없는 클라이언트를 포함한 센서-클라이언트-서버 모델에서 지문 인식을 안전하게 수행하기 위해 제안한 프로토콜을 보여준다. 클라이언트 모듈이 신뢰할 수 없는 경우라도 서버는 센서의 공개키와 서버에서 생성한 난수(N3)를 이용하여 센서를 인증하고, 클라이언트와 센서 모듈 간 인증은 난수(N1, N2)를 이용하여 채널상의 Replay Attack을 막을 수 있다.

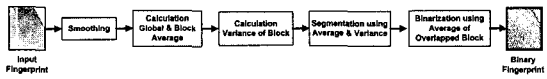
우선, 센서는 지문 영상(Bio)을 획득하고, 암호화된 형태의 지문 영상을 클라이언트에 전송한다. 클라이언트는 전송받은 암호화된 지문 영상을 복호화하고, 특징 추출의 중간 단계 결과물인 이진화 지문 영상(BIN_Client)을 생성한다. 클라이언트는 서버에 이진화 지문 영상을 보내는 대신, 센서로 보내 이진화 지문 영상을 검증받는다.(서버에서 이진화 결과에 대한 검증을 하려면 지문 원영상이 서버로 전송되어야 하는데, 이 경우 프라이버시 문제가 발생한다.) 신뢰할 수 없는 클라이언트로부터 이진화 지문 영상을 받은 센서는 다음에 설명될 이진화 검증 알고리즘을 통하여 이진화 결과의 정당성을 확인한다. 만약 검증 결과가 만족스러우면, 센서는 클라이언트에서 받은 이진화 지문 영상으로부터 특징점(Minutiae)을 추출하고 서버로 보낸다. 그러나 이 경우에도 신뢰할 수 없는 클라이언트를 통해서만 이 서버로 보낼 수 있으므로, 특징점을 안전하게 전달하기 위하여 특징점의 해쉬값(Hashcode)을 계산하고, 센서의 개인키(KRs)와 함께 디지털 서명을 한 후, 센서와 서버 사이에 전달된 난수정보를 이용한 세션키(key:N3)로 모든 정보를 암호화한다. 센서는 서버로 암호화된 특징점을 전송함으로써 클라이언트가 암호화된 특징점을 수정하거나 읽을 수 없다. 서버는 특징점을 복호화하고 첨부된 디지털 서명을 검증하며, 사용자를 인증하기 위해 서버에 저장된 특징점과 정합을 실행한다.



〔그림 3〕 신뢰할 수 없는 클라이언트를 포함한 안전한 지문 인식 프로토콜

3.2 센서에서의 실시간 이진화 검증

설명의 편의를 위해 클라이언트로부터 받은 특징 추출을 위한 이진화 지문 영상을 BIN_Client라고 하고, 센서에 의해 생성된 검증용 이진화 지문 영상을 BIN_Sensor라고 표시한다. BIN_Client는 특징 추출 모듈에서 스무딩, 영상 강화, 영상 품질 평가, 방향 표시, 세그먼테이션과 같이 시간이 많이 소요되는 전처리 단계를 거친 후 생성된다. 그러나 실시간으로 생성되는 BIN_Client가 클라이언트에서 정당하게 생성된 것인지를 구분하기 위해 BIN_Sensor 영상을 자원 제약적인 센서에서 실시간으로 검증하는 경량화 알고리즘의 개발이 필요하다.

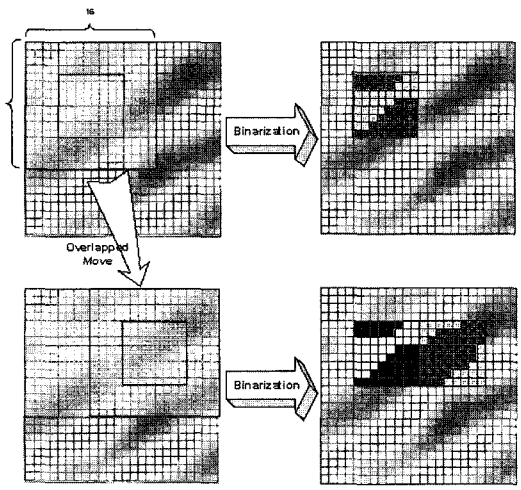


〔그림 4〕 이진화 검증 알고리즘

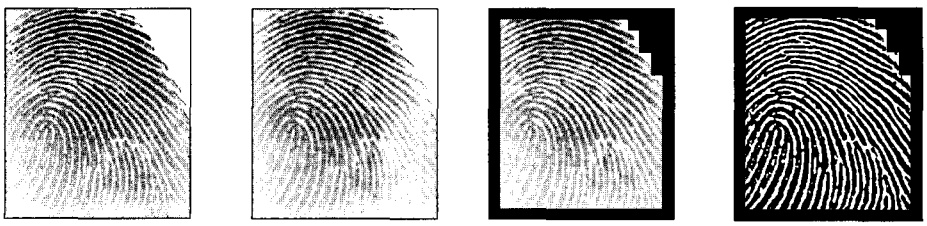
본 논문에서는 자원 제약적인 센서에서 BIN_Sensor 검증 영상을 생성하기 위한 경량화된 알고리즘을 제안한다(〔그림 4〕 참조). 먼저, 센서에 의해 얻어진 지문 영상의 노이즈를 제거하기 위하여 메디언 필터링과 중간 필터링 같은 스무딩 처리를 한다. 이때 지문 영역의 지역성을 분석하기 위해 지문 영상을 블록으로 나누고, 블록 안에 모든 픽셀을 같은 결과 값으로 할당한다. 그리고 영상으로부터 지문 영역을 분리하는 세그먼테이션 단계를 위하여 블록 평균, 전체 평균, 블록 표준편차를 계산한다. 블록 평균과 블록 표준편차는 각각 16×16 블록으로 계산하고, 세그먼테이션 단계에서는 지문 영역과 배경 영역을 구분 한다. 여기서 $Block_i$는 i번째 블록을 의미한다. 또한, F_Block과 B_Block은 지문 영역과 배경 영역을 나타내고, 픽셀 값은 각각 0과 255로 나타낸다. 마지막으로 AVG_G, AVG_B, VAR_B, α는 각각 전체 평균, 블록 평균, 블록 표준편차, 강도를 나타낸다.

$$Block_i = \begin{cases} F\_Block & \text{if}(AVG_G > \alpha AVG_B)\,\text{and}\,(VAR_B > Threshold) \\ B\_Block & otherwise \end{cases} \quad (1)$$

이진화 단계에서는 융선을 나타내는 지문 영상 영역 안에 픽셀들을 결정한다. 이진화 단계에서 생성된 검증 영상에서 융선(ridge)과 골(valley)들은 각각 검정 및 흰 픽셀로 나타난다. 본 논문에서 지문 영역은 16×16 픽셀 블록 영역으로부터 내부 8×8 픽셀 블록으로 구분하고, 〔그림 5〕에서와 같이 이웃한 블록 영역들을 1/2만큼 중첩시킨다. 이진화 단계가 각각의 블록을 모두 처리하면, 지역 평균값이 지문 영역들에 대해 계산된다. 만약 블록안의 픽셀 값이 지역 평균값보다 작으면, 그 픽셀 값은 융선을 나타내는 검은색으로 표시된다.



〔그림 5〕 영역오버랩을 이용한 경량화된 이진화 검증 알고리즘의 동작 예



(a) (b) (c) (d)

〔그림 6〕 이진화 검증 영상

(a) 센서에 의해 획득한 지문 영상; (b) 스무딩 단계; (c) 세그먼테이션 단계; (d) 이진화 단계

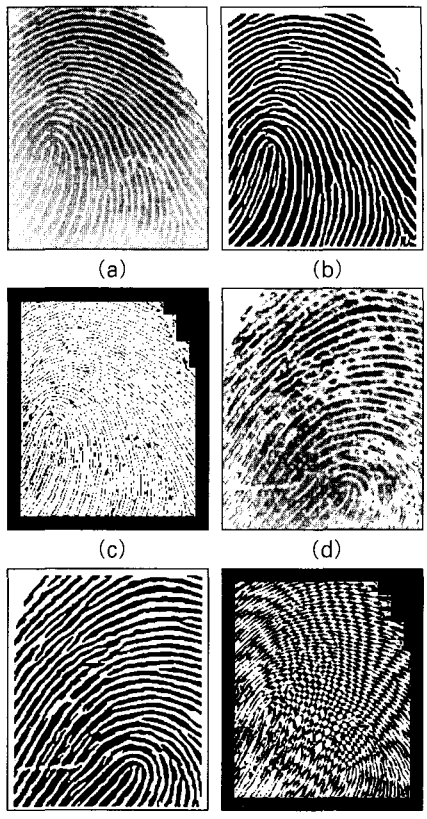
〔그림 6〕은 이진화 검증 영상들을 보여준다. 〔그림 6〕(d)는 경량화 이진화 검증 알고리즘에 의해 생성된 검증 영상이고, 〔그림 6〕(c)와 (d)의 융선 근처에 검은색 픽셀들은 세그먼테이션 단계에 의해 생성된 주변 영역을 나타낸다. 클라이언트로부터 받은 이진화 지문 영상은 경량화 이진화 검증 알고리즘에 의해 생성된 검증 영상(〔그림 6〕(d))과 함께 비교된다.

Ⅳ. 실험 및 성능 평가

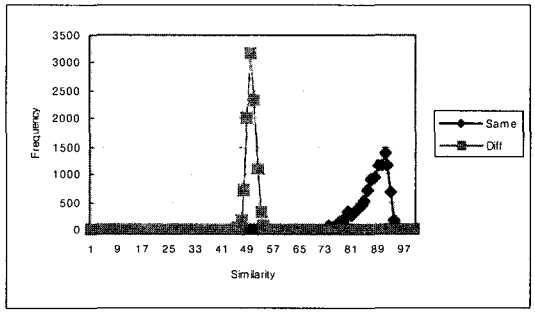
먼저, 제안한 경량화 검증 알고리즘의 타당성을 평가하기 위해 광학식 지문센서를 이용하여 한 개의 지문 당 4개의 지문 영상으로 각각 1,068명으로부터 수집된 4,272개의 지문 영상을 사용하였다[16]. 센서의 해상도는 500dpi이고, 획득된 지문 영상의 크기는 248×292 픽셀이다.

〔그림 7〕은 제안된 검증 알고리즘의 결과들을 보여준다. 〔그림 7〕(a)은 센서에 입력된 지문 원영상이고, 〔그림 7〕(b)은 클라이언트에 의해 생성된 이진화 지문 영상이다. 〔그림 7〕(b)가 〔그림 7〕(a)로부터 생성된 것인지 검증하기 위해서 〔그림 7〕(b)의 이진화 영상과 〔그림 6〕(d)의 검증 영상 사이의 유사도를 계산한다. 그 결과가 〔그림 7〕(c)인데, 지문 영역안의 흰 픽셀은 이중 영상 안에 같은 값을 나타낸다. 〔그림 7〕(b)와 〔그림 6〕(d)사이의 유사 스코어는 91%이다. 그러나 다른 지문(〔그림 7〕(d))로부터 생성된 〔그림 7〕(e)의 이진화 영상은 그림 6(d)의 검증 영상과 비교했을 때 많은 차이를 보이고(〔그림 7〕(f)의 경우, 〔그림 7〕(e)의 이진화 영상과 〔그림 6〕(d)의 검증 영상 사이의 유사 스코어는 51%이다.), 센서는 클라이언트가 이진화 영상을 정확하게 생성하지 않았음을 쉽게 확인할 수 있다.

〔그림 8〕은 같은 지문 영상들의 유사 스코어와 다른 지문 영상들의 유사 스코어의 분포를 보여준다. 실험을 위하여 상기 사용한 지문 영상을 사용하였으며 같은 지문 영상의 유사 스코어 분포를 추출하기 위해 10,000번의 정합을 실행하였으며, 다른 지문 영상의 유사 스코어 분포를 추출하기 위해 10,000번의 정합을 실행하였다. Y축은 실험 결과에 의한 유사 스코어의 획득 분포를 나타내고, X축은 0부터 100까지의 스코어 범위를 나타낸다. 〔그림 8〕에서의 다른 지문 영상들 사이에 유사 스코어는 같은 지문 영상들 사이의 유사 스코어와는 분포가 확실히 구분된다. 따라서 두 개의 영상이 같은 지문인지 아닌지를 정확하게 구분 할 수 있다.



〔그림 7〕 검증 알고리즘의 결과 (a) 및 (d) 입력 영상; (b) 및 (e) 클라이언트로부터 생성된 이진화 영상; (c)는 (b)와 그림 6(d) 사이의 상관관계 결과; (f)는 (e) 와 그림 6(d)사이의 상관관계 결과



〔그림 8〕 유사 스코어의 분포

마지막으로, 일반적인 특징추출 모듈과 제안된 경량화 검증 알고리즘의 수행 시간을 비교한다. 비교를 위하여 다음 세 가지 시나리오를 가정할 수 있다. 시나리오 1은 전형적인 지문 인식 구현의 예로 이진화 과정을 신뢰할 수 없는 클라이언트에서 수행하는 것이며, 시나리오 2는 시나리오 1의 이진화 과정을 신

뢰할 수 있지만 자원 제약적인 지문 센서에 할당하는 것이다. 마지막으로, 시나리오 3은 시나리오 1과 같이 이진화 과정을 클라이언트에서 수행하지만 그 결과를 경량화 검증 알고리즘으로 확인하는 것이다.

〔표 1〕 시나리오별 수행시간 및 안전성 분석

	수행시간			안전성
	센서 (ARM7, 28MHz)	클라이언트 (Pentium 4, 2GHz)	전체시간	
시나리오 1	-	0.183 sec	0.183 sec	나쁨
시나리오 2	6.1 sec	-	6.1 sec	좋음
시나리오 3	0.265 sec	0.183 sec	0.448 sec	좋음

〔표 1〕은 앞서 가정한 세 가지 시나리오에 대하여 이진화 지문 영상을 생성하기 위해 소요되는 시간을 측정한 결과와 시나리오별 안전성 정도를 나타내고 있다. 〔표 1〕에서 보는 바와 같이 시나리오 1은 처리 속도면에서 문제가 없으나 서버나 센서에 비하여 상대적으로 신뢰할 수 없는 클라이언트에서 모든 연산이 수행되기 때문에 수행시간 면에서는 가장 빠르지만 안전성에 문제가 있다. 시나리오 2는 시나리오 1의 안전성 문제를 해결하기 위하여 지문 센서에서 시나리오 1과 동일한 이진화 지문 영상 생성 과정을 수행한다. 표 1에서처럼 임베디드 프로세서를 가진 지문 센서에서 약 6초의 시간이 소요되어 실시간 수행이 불가능하다.

반면, 본 논문에서 제안한 방법인 시나리오 3에서는 클라이언트에서 시나리오 1의 이진화 지문영상 생성 방법으로 이진화를 수행한 후 지문 센서에서는 클라이언트에서 생성된 이진화 지문 영상의 유효성을 검증하기 위해 경량화된 이진화 검증 과정만을 수행한다. 〔표 1〕에서 보는 바와 같이 시나리오 3은 많은 연산이 필요한 이진화 과정을 클라이언트에 할당하고 확인을 위한 경량화된 이진화 검증 과정은 임베디드 프로세서를 내장한 지문 센서에서 수행하여 전체적으로 실시간 수행이 가능하다는 것을 확인 할 수 있다.

참고로 〔표 1〕에서 적용한 이진화 과정은 연구용으로 개발된 것[17]으로, 상용 시스템에서는 보다 정교한 이진화 결과를 얻기 위해 더 많은 계산을 필요로 한다. 따라서, 상용 시스템의 이진화 과정을 센서-클라이언트-서버 모델에 적용한다고 가정하면, 시나리오 1과 3에서는 계속 실시간 처리가 가능하지만 시나리오 2는 수십초 또는 수분의 수행시간이 필요할 것으로 예상된다.

V. 결 론

실시간성, 확장성, 프라이버시 이슈 등을 고려하여 지문 인식 과정 중 가장 많은 계산시간을 필요로 하는 지문 특징 추출 과정을 클라이언트에 할당하는 일반적 원격응용을 위한 지문 인식 구현과 달리, 본 논문에서는 클라이언트가 일반 사용자에 의해 관리되어 여러 공격에 취약할 수 있다는 가정하에서도 동작할 수 있는 지문 인식 및 지문 정보 보호 방법을 제안하였다. 즉, 지문 특징 추출 과정을 이진화와 특징점 추출 과정으로 분리하였고, 클라이언트에서 실행된 이진화 과정의 정당성을 자원 제약적인 지문 센서에서 실시간으로 검증하기 위한 경량화 검증 방법을 제안하였다. 제안된 방법의 타당성을 확인하기 위해 지문 영상을 이용한 실험을 수행한 결과, 제안된 방법이 지문 센서-클라이언트-서버모델에서 실시간으로 안전하게 수행될 수 있음을 확인하였다.

참 고 문 헌

〔1〕 A. Jain, R. Bole, and S. Panakanti, Biometrics: *Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

〔2〕 R. Bolle, J. Connell, and N. Ratha, "Biometric Perils and Patches," *Pattern Recognition*, Vol. 35, pp. 2727-2738, 2002.

〔3〕 G. Davida, et al., "On Enabling Secure Applications through Off-Line Biometric Identification," *Proc. of Symp. on Privacy and Security*, pp. 148-157, 1998.

〔4〕 D. Maio and D. Maltoni, "A Secure Protocol for Electronic Commerce based on Fingerprints and Encryption," *Proc. of SCI*, pp. 519-525, 1999.

〔5〕 A. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images," *Proc. of AutoID*, pp.

97-102, 2002.
[6] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy Vault for Fingerprints," *LNCS 3546 - Proc. of AVBPA*, pp. 310-319, 2005.
[7] Y. Chung, et al., "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," *LNCS 3822 - Proc. of CISC*, pp. 358-369, 2005.
[8] D. Moon, et al., "An Efficient Selective Encryption of Fingerprint Images for Embedded Processors," *ETRI Journal*, Vol.28, No.4, pp. 444-452, 2006.
[9] Sony, *http://www.sony.com*.
[10] Y. Gil, D. Ahn, and Y. Chung, "Access Control System with High Level Security Using Fingerprints," *Proc. of Applied Imagery Pattern Recognition Workshop*, 2003.
[11] D. Maio, et al., "FVC 2004: Third Fingerprint Verification Competition," *LNCS 3072 - Proc. of ICBA*, pp. 1-7, 2004.
[12] 김기철 외, "융선 추적을 이용한 지문 특징점 추출기의 SoC 구현," 정보보호학회 논문지, 14권, 5호, pp. 97-107, 2004. 10.
[13] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric Recognition: Security and Privacy Concerns," *IEEE Security and Privacy*, pp. 33-42, 2003.
[14] 문대성 외, "지문 인증을 이용한 보안 토큰 시스템 구현," 정보보호학회 논문지, 13권, 4호, pp. 63-70, 2003. 8.
[15] W. Stallings, Cryptography and Network Security, *Person Ed.* Inc.,. 2003.
[16] 안도성 외, "ETRI 지문 DB 규격," ETRI 기술문서, 2002.
[17] M. Garris, et al., "User's Guide to NIST Fingerprint Image Software," *NIST*.

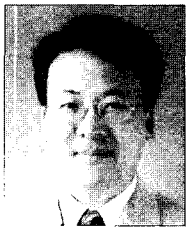
〈著者紹介〉

문 대 성 (Dae-sung Moon) 정회원
1999년 2월 : 인제대학교 전산학과 학사
2002년 2월 : 부산대학교 컴퓨터공학과 석사
2004년 3월~현재: 고려대학교 전산학과 박사과정
<관심분야> 생체인식, 정보보호, 영상처리

정 승 환 (Seung-hwan Jung) 학생회원
2005년 2월 : 고려대학교 전산학과 학사
2005년 3월~현재: 고려대학교 전산학과 석사과정
<관심분야> 생체인식, 정보보호, 병렬 알고리즘

김 태 해 (Tae-hae Kim) 학생회원
2002년 2월 : 인제대학교 전산학과 학사
2006년 2월 : 고려대학교 전산학과 석사
2005년 12월~현재: 인제대학교 디지털정보원
<관심분야> 생체인식, 정보보호, 병렬 알고리즘

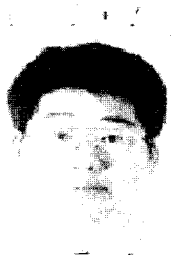
이 한 성 (Han-sung Lee) 학생회원
1996년 : 고려대학교 전산학과(학사)
1999년~2003년 : (주)대우엔지니어링 근무
2002년 : 고려대학교 전산학과(석사)
2002년~현재: 고려대학교 전산학과 박사과정
<관심분야> 기계학습, 데이터마이닝, 인공지능, 인공신경망, SVM, 침입탐지, 퍼지 이론



정 용 화 (Yong-wha Chung) 종신회원
1984년 : 한양대학교 전자통신공학과 학사
1986년 : 한양대학교 전자통신공학과 석사
1997년 : 미국 Univ. of Southern California 전기공학과(컴퓨터공학 전공) 박사
1986년~2003년 : 한국전자통신연구원 생체인식기술연구팀장
2003년~현재: 고려대학교 컴퓨터정보학과 부교수
<관심분야> 생체인식, 정보보호, 생체정보 보호

양 종 원 (Jong-won Yang) 학생회원
2003년 : 공주대학교 전자계산학과(학사)
2005년 : 공주대학교 일반대학원 컴퓨터공학과 (공학석사)
2005년 : 공주대학교 일반대학원 바이오정보학과 박사과정
2006년 ~ 현재 : 한국전자통신연구원 위촉연구원
<관심분야> 시스템 보안, 생체인식, 암호 알고리즘 등

이 은 화 (Eunw-ha Choi) 학생회원
2002년 : 공주대학교 응용수학과 졸업
2004년 : 공주대학교 일반대학원 수학과 (석사)
<관심분야> PKI, 네트워크 보안, 암호 알고리즘 등



서 창 호 (Chang-ho Seo) 종신회원
1990년 : 고려대학교 수학과(학사)
1992년 : 고려대학교 일반대학원 수학과 (이학석사)
1996년 : 고려대학교 일반대학원 수학과 (이학박사)
1996년~1996년 : 국방과학연구소 선임연구원
1996년~2000년 : 한국전자통신연구원 선임연구원, 팀장
2000년~현재 : 공주대학교 응용수학과(정보보호전공) 부교수
2001년~현재 : 공주대학교 바이오정보학과 부교수
<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보안, 시스템 보안 등