Journal of Korea Multimedia Society Vol. 9, No. 10, October 2006(pp. 1304-1313)

임베디드 프로세서에 적합한 LSB 기반 지문영상의 효율적인 부분 암호화 방법

문대성[†], 정용화[††], 반성범[†††], 문기영[††††], 김주만[†††††]

요 약

21세기를 맞이하면서 정보통신기술의 발전과 인터넷 이용 확산 등으로 사용자 인증이 중요한 문제로 대두되고 있으며, 보다 강력한 사용자 인증을 위하여 생체인식 기술의 연구가 활발히 진행되고 있다. 그러나 사용자 인증을 위한 생체정보가 타인에게 도용된다면 패스워드나 PIN과 달리 변경이 불가능하므로 심각한 문제를 일으킨다. 본 논문에서는 센서에서 획득된 지문영상을 클라이언트로 안전하게 전송하는 프로토콜을 제안한다. 특히, 계산능력이 부족한 임베디드 프로세스를 내장한 지문센서에서 지문영상을 실시간으로 암호화하기 위하여 지문영상 전체를 암호화하는 대신, 지문영상의 특정 비트 평면만을 암호화하는 부분암호화 알고리즘을 제안한다. 일반적인 부분암호화 방법에서 사용되어지는 최상위 비트 평면으로 부분암호화를 할 경우 간단한 공격으로 지문의 융선정보를 알 수 있기 때문에 지문인식 시스템에 공격이 가능한 문제점이 있다. 본 논문에서는 이러한 문제를 해결하기 위하여, 최상위 비트정보 대신 최하위 비트정보를 이용하는 개선된 선택적 비트 평면 암호화 방법을 사용하였다. 제안된 알고리즘의 성능을 분석하기 위해 16비트 임베디드 프로세서를 가진 지문센서를 개발하고 부분암호화 방법을 구현한 결과, 기밀성 보장 및 실시간 처리가 가능함을 확인하였다.

A LSB-based Efficient Selective Encryption of Fingerprint Images for Embedded Processors

Daesung Moon[†], Yongwha Chung[††], Sung-Bum Pan[†††], Kiyoung Moon[††††], Juman Kim[†††††]

ABSTRACT

Biometric-based authentication can provide strong security guarantee about the identity of users. However, security of biometric data is particularly important as the compromise of the data will be permanent. In this paper, we propose a secure and efficient protocol to transmit fingerprint images from a fingerprint sensor to a client by exploiting characteristics of fingerprint images. Because the fingerprint sensor is computationally limited, however, such encryption algorithm may not be applied to the full fingerprint images in real-time. To reduce the computational workload on the resource-constrained sensor, we apply the encryption algorithm to a specific bitplane of each pixel of the fingerprint image. We use the LSB as specific bitplane instead of MSB used to encrypt general multimedia contents because simple attacks can reveal the fingerprint ridge information even from the MSB-based encryption. Based on the experimental results, our proposed algorithm can reduce the execution time of the full encryption by a factor of six and guarantee both the integrity and the confidentiality without any leakage of the ridge information.

Key words: Fingerprint Recognition(지문인식), Fingerprint Protection(지문정보보호), Selective Encryption(부분암호화)

※ 교신저자(Corresponding Author) : 문대성, 주소 : 대전광역시 유성구 가정동 161(305-350), 전화 : 042)860-1083, FAX : 042)860-5611, E-mail : daesung@etri.re.kr
접수일 : 2006년 4월 11일, 완료일 : 2006년 8월 10일
[†] 한국전자통신연구원 정보보호연구단 바이오인식기술연구팀 선임연구원
[††] 고려대학교 컴퓨터정보학과 부교수
(E-mail: ychungy@korea.ac.kr)
[†††] 조선대학교 정보통신공학부 전임강사
(E-mail: sbpan@chosun.ac.kr)
[††††] 한국전자통신연구원 정보보호연구단 바이오인식기술연구팀 팀장
(E-mail: kymoon@etri.re.kr)
[†††††] 부산대학교 바이오시스템공학부 조교수
(E-mail : joomkim@pusan.ac.kr)

1. 서 론

정당한 사용자가 정보시스템에 접근하기 위하여 패스워드 또는 PIN(Personal Identification Number)을 이용한 사용자 인증 방법이 널리 쓰이고 있으나, 타인에게 노출되거나 잊어버리는 등의 문제가 있다. 이러한 문제를 해결하기 위하여 개인의 고유한 생체정보를 이용한 정보보호 및 사용자인증 등의 연구가 활발히 진행되고 있다[1,2].

그러나 사람마다 하나의 얼굴, 열개의 손가락 등 한정된 개수를 가진 생체정보는 패스워드와 다르게 유출시 마다 변경할 수 없으며, 일반적으로 사용자는 동일한 생체정보를 다양한 응용에 사용하기 때문에 유출된 생체정보가 모든 응용에서 재사용될 수 있기 때문에 많은 장점을 가진 생체정보가 악의적인 목적을 가진 공격자에게 유출된다면 심각한 문제를 야기할 수 있다. 따라서 생체정보를 불법적인 취득이나 위변조 시도로부터 안전하게 보호하기 위한 연구가 필요하다[2-4].

지문은 가용성, 정확도, 경제성 면에서 현재까지 가장 현실적인 대안으로 평가받고 있으므로 본 논문에서는 생체정보 중 지문을 선택하였다[2]. 또한, 센서-클라이언트-서버 모델[3]을 사용한 원격 사용자 인증을 가정하였다. 본 모델에서는 센서에서 획득된 지문영상을 클라이언트로 전송하면, 클라이언트는 지문영상으로부터 특징정보를 추출하고 서버로 특징정보를 전송한다. 서버는 클라이언트로부터 전송된 특징정보를 서버에 기 저장된 정보와 비교하여 본인여부를 확인할 수 있다.

일반적으로 센서-클라이언트-서버 모델의 지문인증 시스템에서 가능한 공격포인트는 지문획득, 특징추출, 지문매칭 등의 지문인증 모듈 및 센서-클라이언트-서버 사이의 통신채널에서 발생할 수 있지만, 본 논문에서는 통신채널에서의 공격만을 고려하였다. 특히, 지문센서로부터 획득된 지문영상을 안전하게 클라이언트로 전송하는 방법을 제안한다.

지문정보(지문영상 및 지문특징) 전송 시 지문정보의 기밀성과 무결성을 보장하는 가장 간단한 방법은 암호 기법[5]을 사용하는 것이다. 클라이언트와 서버 간의 통신채널에서는 지문정보를 암호화 시킨 후 전송함으로써 지문정보의 기밀성과 무결성을 보장할 수 있다. 그러나 센서와 클라이언트 사이의 통신채널에는 적용하기 어렵다. 왜냐하면 일반적으로 지문 센서에는 프로세서가 내장되지 않거나, 내장되더라도 클라이언트보다 계산능력이 현저히 떨어지는 임베디드 프로세서를 사용하기 때문에 지문영상 전체를 실시간으로 암호화할 수 없다. 이러한 문제를 해결하기 위하여, 제한된 하드웨어 자원을 가진 지문센서의 작업부하를 줄이면서 전송되는 지문영상의 기밀성과 무결성을 동시에 보장하는 방법의 개발이 필요하다.

본 논문에서는 지문영상을 해싱(hashing)한 후 서명하는 대신 난스(nonce)를 암호화한 질의-응답 프로토콜을 이용하여 무결성을 보장하고, 되풀이공격(replay attack)을 막는다. 또한, 기밀성을 보장하기 위하여 지문영상 전체를 대칭키로 암호화하는 대신 일부분만을 암호화하는 부분암호화 알고리즘을 사용하여 실시간 처리를 가능하게 하였다. 즉, 지문영상의 각 화소에서 특정 비트 평면(bit plane)을 선택하여 생성된 비트열(bit string)만 암호화하며, 특정 비트는 최하위 비트(LSB : Least Significant Bit)를 사용하였다. 암호화 되지 않은 원 지문영상은 최하위 비트열과 배타적논리합(XOR) 연산을 수행함으로써 기밀성을 유지할 수 있도록 하였다. 지문센서에 의하여 획득된 지문영상의 최하위 비트열은 랜덤노이즈(random noise)와 유사한 성격을 가지기 때문에 일회용암호(one-time pad)와 유사하게 동작한다.

또한, 본 논문에서 제안한 방법을 임베디드 프로세서가 내장된 지문센서에서 실험하였다. 실험결과에 의해서, 최하위 비트열을 이용한 부분암호화 방법은 다양한 공격으로부터 지문영상을 보호할 수 있었다. 또한, 지문영상의 기밀성을 보장하기 위하여 배타적 논리합 연산을 추가적으로 수행했음에도 불구하고 제안한 부분암호화 방법은 실시간에 처리할 수 있음을 확인하였다.

본 논문의 구성은, 2장에서 일반적인 원격응용 지문인식에서의 공격 포인트에 대하여 설명하고, 안전한 지문영상 전송 프로토콜과 최하위 비트열을 이용한 부분암호화 방법을 3장에서 설명한다. 구현의 세부적인 내용과 성능 평가를 4장에서 언급하며, 마지막으로 5장에서 결론을 맺는다.

2. 지문인식 시스템

2.1 지문인식

본 논문에서는 다양한 생체 정보 중에서 지문 정

보를 이용하여 사용자 인증을 한다. 지문이란 인간의 손바닥에 존재하는 땀구멍이 융기한 선으로 형성된 문형을 말하는 것으로, 융기되어 나타나는 융선(ridges)과 두 융선 사이의 패인 골(valleys)로 나타내어진다. 지문 인식의 방법으로는 영상을 기반으로 하는 방법[6]과 영상 내에 존재하는 특징점(minutiae)을 이용하는 방법[7]으로 나눌 수 있다.

특징점 기반 지문 인증 시스템은 그림 1과 같이 사용자 등록(enrollment) 과정과 사용자 인증(verification) 과정으로 수행된다. 주로 오프라인에서 수행되는 사용자 등록 과정은 획득된 지문 영상의 품질을 향상시키기 위한 전처리단계를 거친 후 특징추출 단계에서 특징점 정보들을 추출하여 서버에 저장하는 과정이며, 사용자 인증 과정은 등록과정과 동일하게 전처리, 특징추출 단계를 거쳐 추출된 특징점 정보와 등록과정에서 미리 저장된 특징점 사이에 정합(matching)을 수행함으로써 입력된 지문이 저장된 지문과 동일한 지문인지를 판단하는 과정이다.

이러한 지문인식 시스템에서 전처리 과정과 특징점 추출 과정은 많은 메모리 사용과 명령어(instruction) 수를 요구하며 전체 시스템 작업부하의 96%를 차지한다[8]. 따라서 센서-클라이언트-서버 모델에서 실시간 지문인식을 가능하게 하기위해서 작업부하가 큰 두 단계를 자원제약적인 센서보다는 계산능력이 월등한 클라이언트에 할당하는 것이 타당하다. 물론 전처리나 특징 추출 단계를 서버에 할당할 수 도 있으나, 현재의 PC급 클라이언트로도 두 단계를 실시간에 처리할 수 있다. 따라서 서버에는 여러 대의 클라이언트가 접속되고 클라이언트-서버간의 통신부하를 고려한다면, 두 단계를 클라이언트에서 처리하고 추출된 특징만을 서버로 전송하는 시나리오가 타당한 것으로 판단된다.

2.2 지문인식 시스템의 공격 포인트

2.1절에서 설명한 것처럼 지문센서는 사용자의 지문영상을 획득하고, 클라이언트에서 획득된 지문영상으로부터 특징점을 추출한 후 서버에서 정합단계를 수행하는 센서-클라이언트-서버 모델에서 다양한 공격 포인트를 가정할 수 있다[2]. 예를 들어, 그림 2에서처럼 ①센서, ②센서와 특징추출 모듈 사이의 통신채널, ③특징추출 모듈, ④특징추출 모듈과 정합

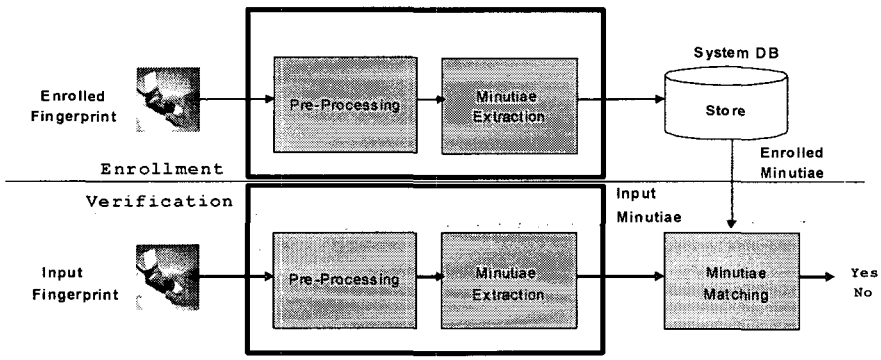


그림 1. 지문인증 과정

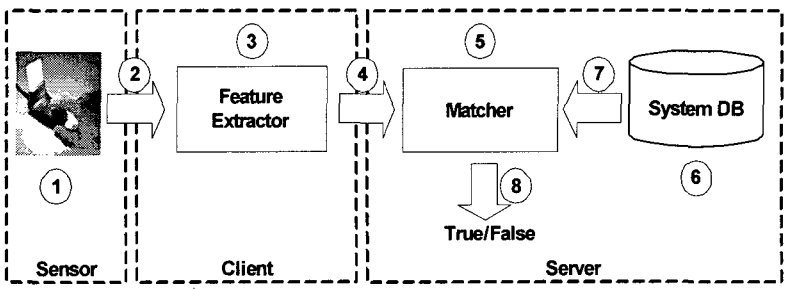


그림 2. 가능한 공격포인트

모듈 사이의 통신채널, ⑤정합 모듈, ⑥데이터베이스, ⑦데이터베이스와 정합 모듈 사이의 통신채널, ⑧정합 모듈과 응용 프로그램 사이의 통신채널 등에서 공격이 가능하다. 이러한 공격 포인트는 센서-클라이언트-서버 모델 뿐 만아니라, 지문획득부터 특징추출, 정합 등의 모든 지문인증 모듈이 하나의 시스템에서 수행되는 자립형(stand-alone) 시스템에서도 유사하게 존재한다.

특히, ②,④,⑦의 공격은 모두 통신 채널에서 발생하기 때문에 매우 유사한 특성을 가지며, 일반적으로 되풀이(replay) 공격이라고 한다[2]. 본 논문에서는 ②번 공격, 특히 자원제약적인 센서와 관련된 되풀이 공격에 대비한 방법에 국한하여 언급한다.

3. 안전한 지문영상 전송 프로토콜

본 장에서는 지문영상을 안전하게 전송하기 위해 암호화할 때 자원제약적인 센서의 부하를 감소시킬 수 있는 프로토콜을 제안한다. 또한, 센서가 특정 클라이언트에 고정되어 연결되어있기 때문에, 클라이언트와 센서는 마스터키를 공유하고 있다고 가정한다.

3.1 기밀성과 무결성 보장을 위한 프로토콜

센서와 클라이언트 간에 지문영상의 안전한 전송을 위해서는 지문영상의 기밀성과 무결성이 보장되어야 한다. 먼저 지문영상의 기밀성 보장을 위하여 비대칭키 암호방식 대신 연산량이 적은 대칭키 암호 알고리즘을 사용한다. 자원제약적인 지문센서에서 원본 지문영상 전체를 실시간으로 암호화할 수 없기 때문에 지문영상 전체를 암호화하는 대신 지문영상의 일부분을 암호화하면서 지문영상의 기밀성을 보장하는 부분암호화 방법이 필요하며 지문영상에 적합한 부분암호화 방법은 3.2절에서 자세히 언급하기로 한다.

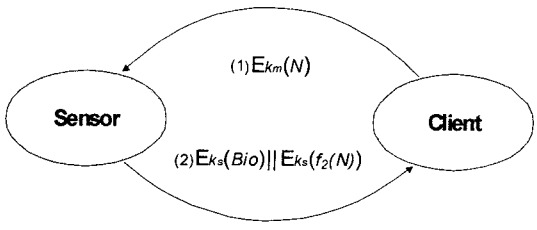


그림 3. 지문영상을 위한 전송 프로토콜

또한, 센서에서 획득된 지문영상을 클라이언트로 전송할 때 전송된 지문영상의 무결성을 보장하기 위하여 그림 3과 같이 난스(nonce)를 이용한 단순한 질의-응답 프로토콜을 사용한다. 무결성 보장을 위하여 일반적으로 사용되어지는 해쉬, MAC, 서명 등의 기법을 적용할 경우 자원제약적인 지문센서에서 실시간 수행이 어려우므로 제안된 프로토콜은 난스정보에 간단한 함수를 적용하는 질의-응답 프로토콜을 사용함으로써 연산량을 최소화할 수 있으며, 클라이언트에서 질의를 위한 난스정보를 생성하기 때문에 센서에서 난수발생기의 요구도 배제하였다.

그림 3의 지문영상을 위한 전송 프로토콜을 보다 상세히 설명하면, 먼저 클라이언트에서 난스 N을 생성하여 공유된 마스터키로 암호화한 후 센서로 전송(질의)한다. 센서에서는 먼저 동일한 마스터키로 복호화한 후, 마스터키와 전송된 N을 이용하여 세션키를 생성한다. 그리고, N에 간단한 함수를 적용하여(예를 들어, 더하기 1) 암호화한 후, 클라이언트로 전송(응답)한다.

그림 3의 프로토콜은 자원제약적인 센서와 클라이언트 사이에서 고려할 수 있는 간단한 프로토콜로써 제안된 프로토콜의 안전성을 살펴보면 다음과 같다. 먼저, 센서와 클라이언트만이 마스터키 및 세션키를 공유하기 때문에 전송되는 질의 및 응답 정보는 센서와 클라이언트만이 송·수신 할 수 있으며 단지 두 번의 통신만으로 지문영상의 획득이 가능하다. 또한 클라이언트는 자신이 전송한 질의(nonce)에 함수 f를 적용한 결과를 응답된 f(N)과 비교함으로써 센서가 응답하였음을 확인한다. 따라서 f(N)과 함께 전송된 지문영상에 replay 공격이 가해졌는지 확인할 수 있다. 그러나, 상기 질의-응답 프로토콜은 전송되는 지문영상의 무결성을 보장하기 위한 방법이며, 그림 3에서는 기밀성을 보장하기 위하여 지문영상(Bio)을 센서에서 생성된 세션키를 이용하여 암호화 한 후 클라이언트로 전송한다. 하지만, 연산능력이 부족한 센서는 지문영상 전체에 대하여 실시간으로 대칭키 암호화 알고리즘을 적용하는 것이 불가능하다. 따라서 지문영상을 위한 전송 프로토콜이 안전하면서 실시간으로 동작하기 위해서는 그림 3의 프로토콜을 기반으로 전체 지문영상이 아닌 일부분만을 암호화하면서 기밀성을 보장할 수 있는 방법이 필요하다.

3.2 영상기반 부분 암호화

앞서 설명한 것처럼, 자원제약적인 지문 센서에서 지문영상 전체를 암호화 할 경우 실시간 처리가 불가능하다. 따라서 지문영상 암호화에 요구되는 연산량을 줄이기 위하여 지문영상 전체를 암호화하는 대신 일부분만을 암호화해야 한다. 일반적인 멀티미디어 데이터를 대상으로 하는 부분암호화(Selective Encryption) 방법은 선택적 영역 암호화(selective spatial encryption)와 선택적 비트평면 암호화(selective bit-plane encryption)로 나눌 수 있다.

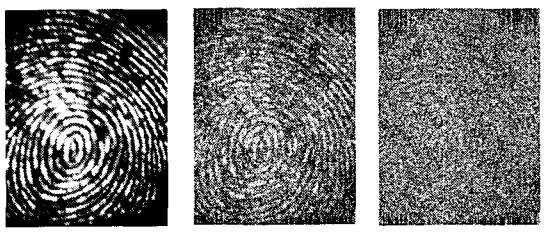
영상을 주파수 공간(frequency domain)으로 변환시킨 후 특정 주파수만을 선택적으로 암호화하는 다양한 기법들이 보고되고 있으나, 주파수 공간으로 변환하기 위한 영상변환 방법들 자체가 많은 연산을 필요로 하기 때문에, 본 논문에서의 부분암호화는 영상공간(spatial domain)에서의 암호화만을 고려한다.

선택적 영역 암호화 방법은 지문영상의 일부분만을 암호화하는 것으로 일반적으로 중앙부분에 중요한 정보가 많기 때문에 중앙 부분만을 암호화하는 것이다. 특히, 사용자 인식에 사용되는 지문영상의 경우에 중앙부분에 대부분의 특징정보가 존재한다. 전체 지문영상을 9개의 부분영상으로 분할하고 중앙의 부분영상에만 암호화 과정을 적용한다. 따라서 공격자가 암호화된 중앙부분을 복호화할 수 없기 때문에 기밀성이 유지된다고 주장할 수 있다. 그러나, 실제로는 사용자가 지문센서에 자신의 손가락을 위치시킬 때 항상 동일하게 위치시킬 수 없다. 따라서, 그림 4와 같이 전송되는 여러 개의 부분암호화 영상을 공격자가 가로챈 후 중첩시킴으로써 원영상에 근접한 영상을 복원(mosaic)[2]할 수 있다는 문제가 있다. 그림 4에서 지문영상의 중앙을 기준으로 정해진 크기만큼의 영역을 암호화하였음을 보여주기 위하여 화이트박스로 표시하였다. 지문영상은 동일인으로부터 획득된 영상이라도, 획득될 때마다 천이(translation) 및 회전(rotation)의 영향으로 동일한 영상이 획득되지 않는다. 그림 4에서처럼 단지 2개의 지문 영상만을 합성하더라도, 암호화되어 공격자가 인식하지 못하는 부분(화이트박스)이 상당히 줄어드는 것을 확인할 수 있다. 따라서, 공격자가 여러 장의 지문영상을 확보한다면, 원지문 영상과 매우 유사한 지문 영상을 복원할 수 있다.

그림 4. 모자이킹에 의한 지문영상 복원

선택적 비트평면 암호화 방법[9]은 영상의 부분암호화에 사용되어지는 일반적인 방법 중 하나로써 그레이영상일 경우에 8개의 비트로 구성된 각 화소에서 특정 비트평면을 암호화하는 방법이다. 즉, 일반적인 멀티미디어 데이터인 경우에는 8개의 비트들 중에서 가장 많은 정보를 포함하고 있는 최상위비트(MSB : Most Significant Bit)만을 암호화하거나 최상위비트와 다른 비트를 암호화하면 적은 연산만으로도 다양한 공격으로부터 안전하게 데이터를 보호할 수 있다고 보고되고 있다. 그러나 원본 데이터와 동일하게 복원하는 것이 공격의 목적인 멀티미디어 데이터와 달리 지문영상의 경우에는 공격자가 암호화된 지문영상을 공격하여 원본 지문영상의 대략적인 융선정보만 획득해도 지문인식 시스템을 공격할 수 있다. 즉, 대략적인 융선정보로부터 지문인식 시스템에서 사용되는 지문의 특징정보를 추출이 가능하다.

그림 5는 일반적인 선택적 비트평면 암호화 방법을 보여준다. 그림 5(a)는 원본 지문영상이며, 그림 5(b)와 그림 5(c)는 각각 그림 5(a)에 대하여 모든 화소의 최상위비트 정보를 암호화한 결과와 최상위비트 정보에 추가적으로 7번째 화소들을 암호화한 결과를 보여준다. 그림 5(c)에서 보는 것처럼 두 개의 비트열을 암호화 할 경우 지문영상에서 융선 정보를 알 수 없으며 모자이킹 공격에도 안전하다. 그림 6은 그림 5(c) 영상의 모든 화소에서 최상위비트와 7



(a) (b) (c)

그림 5. 선택적 비트평면 암호화의 결과: (a) 원본 지문영상 (b) 각 화소의 MSB를 암호화한 결과 (c) 각 화소의 MSB와 7번째 bit를 암호화 한 결과

그림 6. 그림 5(c)의 Replacement 공격 결과

번째 비트의 값을 0으로 변경하는 Replacement 공격 [4] 결과를 보여준다. 그림 6에서처럼 원 지문영상과 동일한 영상을 복원할 수는 없지만 간단한 공격으로 지문의 융선정보를 알 수 있기 때문에 지문인식 시스템에 공격이 가능한 문제점이 있다.

본 논문에서는 이러한 문제를 해결하기 위하여, 최상위 비트정보 대신 최하위 비트정보를 이용하는 개선된 선택적 비트평면 암호화 방법을 제안한다. 센서를 통해 획득된 영상의 최하위 비트정보는 그레이 영상에서 8개의 비트 중 가장 적은 정보를 가지고 있기 때문에 랜덤노이즈와 유사한 특성[5]을 가질 뿐만 아니라 동일인의 지문일지라도 획득될 때마다 항상 다르기 때문에 최상위비트 보다 제안한 방법에 더욱 적당하다.

제안한 방법은 1) 영상 왜곡(image distortion)과 2) 최하위비트 암호(LSB encryption) 과정으로 구성된다. 영상 왜곡 단계에서는 먼저 그림 7과 같이 지문영상에서 각 화소의 최하위 비트 정보로부터 생성된

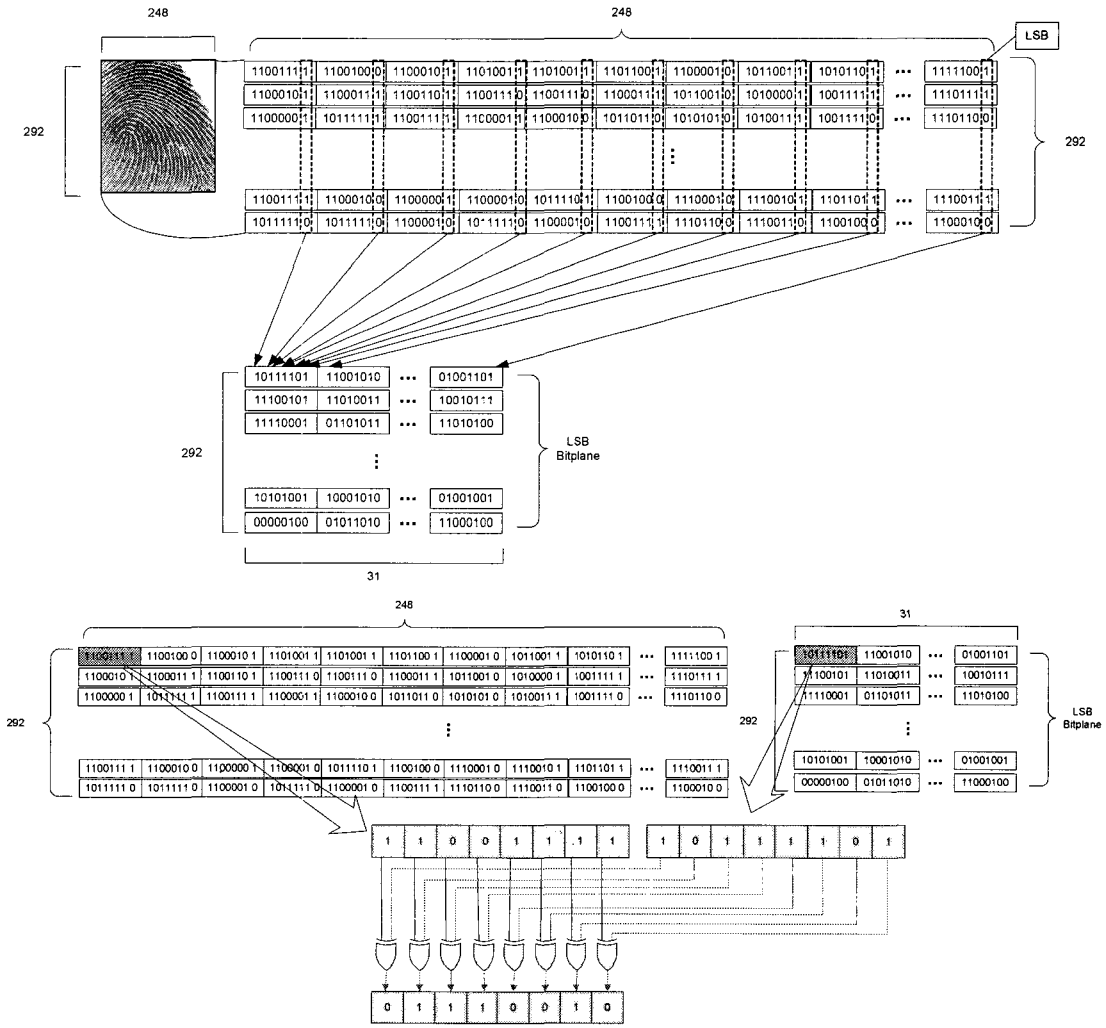


그림 7. 제안된 부분암호화과정

최하위 비트열을 생성한다. 다음으로 최하위 비트열과 지문영상에 대해 간단한 배타적논리합(XOR) 연산을 수행하여 전체 지문영상을 왜곡함으로써 공격자로부터 원본 지문영상을 은닉한다. 이 방법은 최하위 비트열이 랜덤노이즈와 유사한 특성을 가지기 때문에 일회용암호(one-time pad)처럼 동작한다고 볼 수 있다[10]. 영상 왜곡 단계를 수행한 후에 최하위비트 암호 단계에서 배타적 논리합 연산에 사용되었던 최하위 비트열 정보를 센서와 클라이언트 간에 공유된 세션키로 암호화한다. 동일한 세션키를 보유한 클라이언트에서는 지문센서로부터 전송된 정보에서

암호화된 최하위 비트열 정보를 복호화 한 후, 센서에서와 동일한 방법으로 배타적 논리합 연산을 수행함으로써 원영상을 복원할 수 있다. 이때, 공격자가 최하위 비트 정보를 알지 못한다면 원영상을 복원할 수 없으며 최하위 비트 정보는 표준암호방법으로 암호화되었기 때문에 안전하다. 결론적으로 센서로부터 클라이언트로 전송되는 정보는 그림 3에서 (2)에 해당하는 내용이 Bio ⊕ LSB || EKs (LSB) || EKs (f2(N)) 으로 변경된다.

본 논문에서 제안한 개선된 선택적 비트평면 암호화 방법은 앞서 언급한 모자이킹 공격을 피할 수 있을 뿐만 아니라, 원 지문영상과 최하위 비트열에 배타적 논리합 연산을 수행함으로써 센서에서 클라이언트로 전송되는 지문영상을 공격자가 취득하더라도 육안으로는 원영상을 인식하지 못할 뿐만 아니라 다양한 영상처리 공격 및 replacement 공격에도 안전하다.

4. 실험결과

본 논문에서 제안한 개선된 선택적 비트평면 암호화 방법의 실험을 위한 대칭키 암호 알고리즘으로 AES(Advanced Encryption Standard)를 사용하였으며, 두 가지 종류의 지문센서에 의하여 획득된 지문영상에 적용하였다. 실험에 사용된 지문센서의 특성은 표 1에서 보여준다. 특히, CY77C101B센서[11]에 의하여 획득된 지문영상은 영상복원 파라미터에 따라서 영상 크기가 변하며 본 논문에서는 288×432로 고정하고 사용하였다.

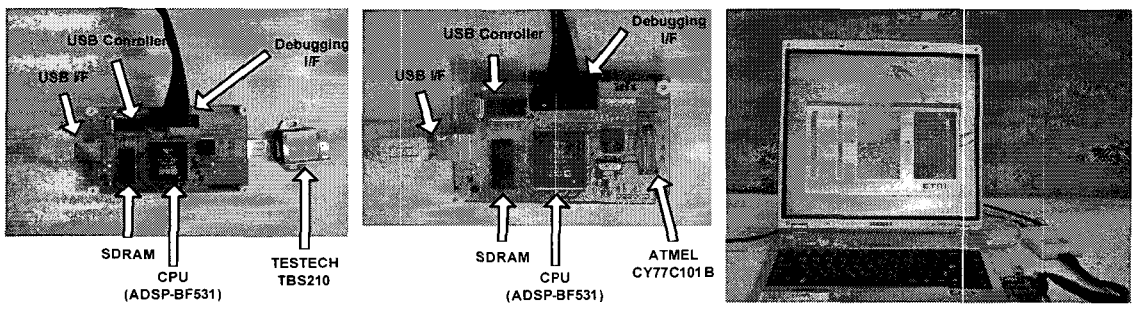
또한, 표 2는 지문센서와 클라이언트 사이의 안전한 지문전송을 위하여 본 논문에서 구현한 임베디드 프로세서가 내장된 지문센서의 시스템 규격을 보여준다. 표 2에서처럼 400MHz CPU[12], 2MBytes ROM, 그리고 16MBytes의 RAM을 사용하였으며, 표 1에서 설명한 2가지 지문센서를 시스템에 장착하였다. 그림 8(a)와 그림 8(b)는 각각 TBS210[13]과

표 1. 지문센서의 특성

	TBS210[13]	CY77C101B[11]
제조사	Testech	ATMEL
획득방식	Light Emitting Touch	Thermal Array
해상도	500 dpi	500 dpi
영상크기	320× 440	Variable

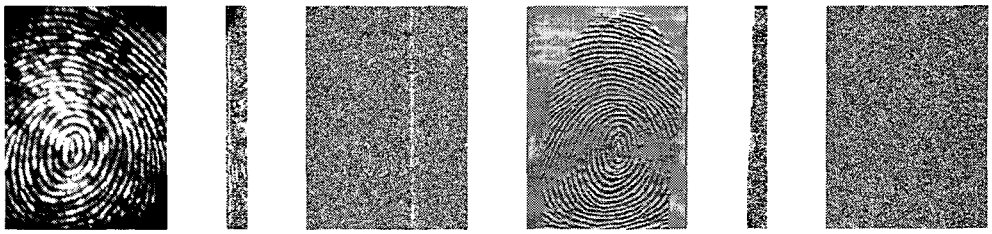
표 2. 안전한 지문센서의 시스템 명세

CPU	16-bit RISC Processor (ADSP-BF531[12], 400MHz)
ROM	FLASH ROM 2 MBytes
RAM	SDRAM 16 MBytes
Sensors	CY77C101B (ATMEL), TBS210 (Testech)



(a) (b) (c)

그림 8. 안전한 지문센서 시스템 구성: (a) 안전한 지문센서(TBS210), (b) 안전한 지문센서(CY77C101B), (c) 실험 환경



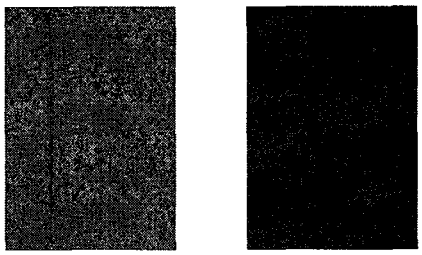
(a) (b) (c) (d) (e) (f)

그림 9. 제안한 부분암호화 결과; (a) 입력지문영상(TBS210), (b) (a)의 최하위 비트열, (c) (a)의 왜곡 결과, (d) 입력지문영상(CY77C101B), (e) (d)의 최하위 비트열, (f) (d)의 왜곡 결과

CY77C101B[11]가 장착된 안전한 지문센서의 하드웨어 보드를 보여주며, 그림 8(c)는 클라이언트 모듈과 디버깅 툴, 그리고 안전한 지문센서를 포함한 실험환경을 보여준다.

그림 9는 각각 입력 지문영상, 최하위 비트열, 그리고 본 논문에서 제안한 부분암호 알고리즘의 결과를 보여준다. 그림 9(a)와 그림 9(d)는 각각 TBS210과 CY77C101B에 의해서 획득된 입력 지문영상이다. 그림 9(b)와 그림 9(e)에서 보여주는 것처럼 최하위 비트열은 원본 지문영상 크기의 1/8이며, 랜덤노이즈와 유사하다는 것을 알 수 있다. 또한, 그림 9(c)와 그림 9(f)는 3.2절에서 설명된 부분암호 알고리즘에서 영상 왜곡의 결과를 보여준다. 선택적 영역 암호화 방법과 다르게, 공격자가 그림 9(c)와 그림 9(f)처럼 최하위 비트열에 의하여 왜곡된 지문영상을 여러 개를 가로챈다고 하더라도 합성 등의 공격에 의하여 지문 융선 정보를 알아내기는 어렵다. 왜냐하면, 모자이킹 기법을 이용하여 여러 장의 지문영상으로부터 원 지문영상을 복원하기 위해서는 지문영상들을 동일한 기준으로 정렬(alignment)한 후 중첩시켜야 하지만 배타적 논리합에 의하여 왜곡되어져 있어 정렬이 불가능하기 때문이다.

그림 10(a)는 그림 9(c)의 영상에 대하여 모든 화소의 최상위비트 정보를 상수 0으로 대체한 replacement 공격의 결과를 보여준다. 마찬가지로, 그림 10(b)는 그림 9(c)의 영상에 대하여 모든 화소의 최상위비트 정보와 7번째 비트정보를 상수 0으로 대체한 replacement 공격의 결과이다. 그림 6과 비교했을 때 그림 10의 Replacement 공격에 대한 결과는 지문의 융선 정보를 드러내지 않는다는 것을 알 수 있다.



(a) (b)

그림 10. Replacement 공격 결과; (a) 그림 10(c)의 MSB Replacement 공격, (b) 그림 10(c)의 MSB 와 7번째 비트열의 Replacement 공격

표 3에서는 본 논문에서 구현된 임베디드 프로세서를 내장한 안전한 지문센서 환경에서 제안된 부분암호화 방법의 수행시간과 전체 지문영상을 암호화하는 전형적인 방법의 수행시간을 비교한다. 최하위 비트열의 암호화 시간은 전체 지문영상을 암호화하는 시

표 3. ADSP-BF531[12] 프로세서에서 지문영상의 암호 수행시간 (400MHz)

			Testech TBS210[13] (Light Emitting Touch Type)	ATMEL CY77C101B[11] (Sweep Type)
부분암호화 (Proposed)	영상 왜곡 (Image distortion)	LSB 추출	0.06 sec	0.05 sec
		배타적 논리합 연산	0.09 sec	0.08 sec
	LSB 암호화(AES)		0.58 sec	0.51 sec
	전체수행시간		**0.73 sec**	**0.64 sec**
전체암호화(Typical)			4.69 sec	4.15 sec

간에 비하여 1/8만큼 단축된 것을 알 수 있으며, 전체 지문영상을 암호화하는 방법에는 없는 영상 왜곡의 추가적인 연산을 수행함에도 불구하고 전체 수행시간이 1/6만큼 감소하였다. 또한, 표 3에서 보는 바와 같이 실시간 처리가 가능하다는 것을 알 수 있다.

5. 결 론

본 논문에서는 지문정보를 안전하게 보호하기 위한 방법을 제안하였다. 특히, 지문센서에서 획득된 영상을 안전하고 효과적으로 클라이언트에 전송하는 프로토콜 및 부분암호화 방법을 제안하였다. 일반적인 멀티미디어 데이터에 관한 부분암호화 방법은 다양한 연구결과가 있으나, 지문인식 시스템에 사용되는 지문영상의 특성을 고려할 때 기존 부분암호화 방법은 적합하지 않다. 특히, 지문센서로부터 지문영상을 안전하게 전송하기 위한 부분암호화 방법에 관한 연구는 보고된 바 없다.

본 논문에서는 지문센서의 작업부하를 최소화하기 위하여 난스(nonce) 기반의 단순한 질의-응답 프로토콜을 사용하여 무결성을 보장하였다. 또한 기밀성 보장을 위하여 지문영상의 각 화소에서 최하위 비트 정보만을 암호화하고 원 지문영상과 최하위 비트열에 대하여 간단한 비트연산(XOR)을 수행하였다. 본 논문에서 제안한 안전한 지문영상 전송 프로토콜을 검증하기 위하여 16비트 임베디드 프로세서를 내장한 안전한 지문센서를 개발하였다. 실험을 통하여 제안된 부분암호화 알고리즘은 모자이킹 기법에 의한 영상복원 공격 및 Replacement 공격에 안전하다는 것을 확인하였고, 제한된 하드웨어 자원을 가지는 지문센서에서 실시간에 처리될 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] D. Maltoni, et al., *Handbook of Fingerprint Recognition*, Springer, 2003.

[3] R. Bolle, J. Connell, and N. Ratha, "Biometric Perils and Patches," *Pattern Recognition*, Vol. 35, pp. 2727-2738, 2002.

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

[5] W. Stallings, *Cryptography and Network Security*, Pearson Ed. Inc., 2003.

[6] A. K. Jain and L. Hong, "Filterbank-Based Fingerprint Matching", *IEEE Trans. on Image Processing*, Vol.9, No.5, 2000.

[7] N. Ratha, K. Karu, and A. Jain, "A Real-Time Matching System for Large Fingerprint Databases," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 18, No. 8, Aug. 1996.

[8] Y. Gil, Y. Chung, D. Ahn, D. Moon, and H. Kim, "Performance Analysis of Smart Card-based Fingerprint Recognition for Secure User Authentication," *Proc. of IFIP on E-commerce, E-business, E-government*, pp. 87~96, 2001.

[9] M. Podesser, H. Schmidt, and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments," *Proc. of the 5th IEEE Nordic Signal Processing Symposium*, 2002.

[10] R. Gonzalez, *Digital Image Processing*, Addison Wesley, 1992.

[11] ATMEL, http://www.atmel.com

[12] Analog Device, http://www.analog.com.

[13] Testech, http://www.testech.co.kr.

문 대 성

1999년 2월 인제대학교 전산학과(이학사)

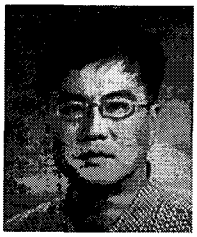
2001년 2월 부산대학교 대학원 컴퓨터공학과(공학석사)

2000년 12월~현재 한국전자통신연구원 정보보호연구단 바이오인식기술연구팀 선임연구원

관심분야 : 생체인식, 영상처리, 정보보호

정 용 화

1984년 2월 한양대학교 전자통신공학과(공학사)
1986년 2월 한양대학교 전자통신공학과(공학석사)
1997년 2월 미국 Univ. of Southern California 전기공학과(컴퓨터공학 전공) (공학박사)
1986년~2003년 한국전자통신연구원 생체인식기술연구팀장
2003년 9월~현재 고려대학교 컴퓨터정보학과 부교수
관심분야 : 생체인식, 정보보호, 생체정보보호



반 성 범

1991년 서강대학교 전자공학과(공학사)
1995년 서강대학교 전자공학과(공학석사)
1999년 서강대학교 전자공학과(공학박사)
1999년~2005년 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 팀장
2005년~현재 조선대학교 정보통신공학부(제어계측공학) 전임강사
관심분야 : 생체인식, 영상처리, VLSI 신호처리

문 기 영

1986년 2월 경북대학교 전자공학과(공학사)
1989년 2월 경북대학교 대학원 전자공학과(공학석사)
2006년 2월 충남대학교 대학원 컴퓨터과학과(이학박사)
1992년~1994년 (주)대우정보시스템 기술연구소 전임연구원
1994년 3월~현재 한국전자통신연구원 정보보호연구단 바이오인식기술연구팀 팀장
관심분야 : 생체인식, 웹서비스 보안, 분산 시스템

김 주 만

1984년 2월 숭실대학교 전산학과(공학사)
1998년 8월 충남대학교 대학원 컴퓨터공학과(공학석사)
2003년 8월 충남대학교 대학원 컴퓨터공학과(공학박사)
1985년~2000년 한국전자통신연구원 운영체제연구팀장(책임연구원)
1995년~1996년 Novell Inc. Research Center 방문연구원
2000년~2005년 밀양대학교 정보통신공학부 조교수
2006년~현재 부산대학교 바이오시스템공학부 조교수
관심분야 : 바이오 센서 제어, 유비쿼터스 컴퓨팅, 임베디드 소프트웨어