모바일 OTP의 패스워드 Seed 확장을 위한 지문 중첩 기법

Fingerprint overlay technique of mobile OTP to extent seed of password

김남호*, 황부현**

Nam-Ho Kim*, Bu-Hyun Hwang**

요 약

지문은 바이오매트릭스를 이용한 대표적인 신분인증 방법이다. 패스워드 방법에 비하여 도용이나 분실의 위험성이 적은 특징이 있다. 이러한 특징으로 OTP 생성에 지문을 이용한 시도를 하게 되었다. 본 논문은 개발된 OTP 시스템의 프로토타입을 소개하며, 지문을 이용한 OTP 시스템은 와상형 지문의 특징점이 적게 추출된다는 단점을 극복하는 방법을 제안한다. 적은 특징점은 OTP 세션을 위한 많은 암호화 키를 생성하지 못한다. 제안된 방법은 간단하게 동일한 지문을 겹침으로써, 편의를 갖는 중첩된 지문의 많은 특징점이 추가된다. 이로 인하여, 지문을 이용한 OTP의 보안성과 패스워드 추측에 대한 임의성이 강화된다.

Abstract

The fingerprint is the identity authentication method which is representative uses biometrics. Compared with password methods there is a feature where the dangerousness of embezzling or lossing is few. With like these features using the fingerprint in OTP creations. In this paper, we introduce the developed prototype of OTP system using fingerprint. And the overcome method of OTP system's demerit using fingerprint which extracts few minutiae points into a whole fingerprint image is proposed. A few minutiae points wasn't generated many encryption key for OTP session. The proposed method is overlaid the same fingerprint simply and added many minutiae points as biased overlaid fingerprints. Hence the security of OTP using fingerprint and the randomness over password-guessing are strengthened.

Key words : Fingerprint, OTP, Overlay, Biometrics Information

I. 서 론

최근에는 스마트폰을 이용한 커뮤니티 활성화가 스마트워크(SmartWork)로 확대됨에 따라 정보의 대용량화라는 빅 데이터(Big Data) 문제가 발생되고 있으며, IT 분야의 주요 이슈로 부각되고 있다. 빅 데이터 문제를 해결하기 위한 저장 공간의 확대와 더불어 각 통신사가 제공하는 u-cloud 서비스를 이용해 개인

* 호남대학교 (Honam University)
** 전남대학교 (Chonnam National University)
· 제1저자 (First Author) : 김남호
· 투고일자 : 2012년 2월 27일
· 심사(수정)일자 : 2012년 2월 28일 (수정일자 : 2012년 4월 25일)
· 게재일자 : 2012년 4월 30일

이 소지한 기존의 물리적인 저장 공간인 외장형 HDD, USB메모리에서 스마트폰의 3G, LTE 통신을 이용하는 등의 다양한 기술에 의한 대안책을 강구하고 있다. 더불어 빅 데이터의 문제와 동반되는 개인의 저장 공간 접근을 단순한 텍스트를 입력하는 login 방식에서 진화된 새로운 인증방식에 대한 보안 기술의 필요성이 증가하고 있다. 특히 최근에 스마트폰과 인터넷 메신저 서비스 및 포털 사이트를 제공하는 몇몇 사이트에서 개인정보가 대규모로 유출되었고, 바이러스 및 해킹방지 보안 프로그램을 서비스하는 업체의 서버를 해킹하여 3500만 명의 회원의 개인정보가 유출되어 주민등록번호와 ID/Password를 통한 개인인증은 더 이상 개인정보를 보호할 수 없는 단계에 이르렀다.

이처럼 개인 확인 및 인증방법의 한계를 극복하기 위한 새로운 형태의 개인인증 방법에 대한 연구 분야로 생체인식의 한 종류인 지문인식이 보편화 되었다. 개인이 가지는 고유의 지문 특징점들을 체계화하여 바이오매트릭스를 만들어 서버에 저장하고 인증을 하는 방식으로 해킹, 누출에 의해 정보가 도용되거나 변경, 분실할 위험성이 없는 개인인증 기술로 각광받고 있다. 하지만 이러한 생체인식 같은 경우 인증업체의 서버관리에 대한 부실로 바이오매트릭스가 유출될 경우 2차 피해에 대한 대처방안을 찾을 수가 없다. 이를 보안하기 위해서 본 논문에서는 스마트폰을 이용하여 지문영상을 받아 지문인식의 특징점을 이용하여 OTP(One Time Password)를 생성하고, 이를 통해 인증을 구현함으로써 지문인식 바이오매트릭스의 유출로 인한 2차 피해를 차단할 수 있는 방법을 제시하고자 한다.

본 논문의 구성은 2장에서 관련 연구로 사용자 인증 기술과 OPT에 대한 관련 기술을 소개하고 3장에서는 바이오매트릭스 인증기반의 OTP에 대해서 기술한다. 4장에서는 프로토타입의 구현을, 5장에서 지문을 이용한 OTP의 단점을 극복하기위한 오버레이 기법의 시뮬레이션을 수행하였으며, 마지막으로 6장에서는 간략하게 결론으로 마무리한다.

Ⅱ. 관련 연구

2-1 사용자 인증기술

모바일 환경의 금융거래, 쇼핑몰, 개인정보 서비스 등의 활성화와 함께 거래 당사자를 확인하는 인증기술의 중요성이 증대되고 있다. 사용자 인증기술은 인증의 기반이 되는 요소에 따라 지식을 통한 인증, 소유한 물건을 이용한 인증, 신체적 특징을 이용한 인증으로 구분 할 수 있다. 일반적으로 이 중 두 가지 이상의 방법을 이용하여 인증을 함으로써 보안성을 한층 강화 시킬 수 있으며, 다중요소 인증시스템(Multi-Factor Authentication System)이라고 한다 [1].

먼저, 지식을 통한 인증의 대표적인 방법으로 패스워드 인증방식이 있다. 패스워드 인증방식은 사용법이 간단하여 편리한 방식으로 인식되고 있지만, 패스워드 값이 고정적일 때 서버로 전송되는 패스워드를 공격자가 해킹하여 사용할 경우 사용자가 직접 패스워드를 변경할 때 까지는 취득한 패스워드를 사용할 수 있는 문제가 발생한다. 그리고 일반 사용자들은 자신이 기억하기 쉬운 문자나 숫자를 이용하여 패스워드를 구성하기 때문에 추측에 의한 사회 공학적 공격으로 인한 패스워드 노출이 가능하다. 이처럼 패스워드 방식은 누출, 도청, 유추에 의한 개인정보 인증의 단점이 있다. 이에 대해 일회용 암호 메커니즘은 사용자의 인증 요구 때마다 새로운 암호를 생성하여 사용함으로써 시스템 내에 암호 파일을 보관해 둘 필요가 없으며, 암호가 항상 바뀌므로 설사 한번 도청 또는 누출된다고 하더라도 문제가 되지 않으며 사전공격 등에도 안전한 대처 방안이 된다 [2].

두 번째 소유한 물건을 이용한 방법은 인증을 받기 위해 토큰(token)을 이용한다. 토큰은 그 내부 메커니즘이 쉽게 읽혀져서는 안 되며, 복조 불가능해야 한다. 또한 사용이 편리해야 하며 휴대가 간편할수록 좋다. 보통 스마트카드, PCMCIA카드, 일회용 암호 생성기, USB키, 보안카드 등의 형태로 만들어진다. 일반적으로 PIN(Personal Identification Number)을 입력함으로써 잠긴 상태가 풀리게 되어 사용이 가능해진다. 단점은 항상 휴대해야하기 때문에 분실의 위험성이 있으며, 사용을 위해서는 리더기 등의 특별한 장치가 필요하며, 해체에 대비해야 한다는 점이다. 장점으로는 특별히 외울 것이 거의 없다는 것이다.

세 번째, 자신의 몸, 생체를 이용한 인증방식은 미

리 입력해 놓은 사람의 생체 패턴을 검사 비교하는 방식으로 가장 고수준의 사용자 인증 방식으로 평가받고 있다. 보안적 성능이 약한 것에서 강한 것 순으로, 사인, 자판입력 패턴, 음성, 손도장, 지문, 홍채 등으로 나열할 수 있다. 하지만 이 또한 모조가 가능하며, 보통 고가의 장비와 기술이 필요하다는 단점이 있다 [3].

2-2 일회용 패스워드 방식 (OTP)

(1) OTP 기술의 필요성

해킹 기술의 다변화, 고도화 및 대중화로 ID/Password 인증방식의 안전성이 저하되고 있다. 이에 따라 기존의 패스워드 인증방식의 문제점을 개선하기 위하여 일회용 패스워드 방식이 제시되었다. 일회용 패스워드 방식은 클라이언트가 서버로 전송하는 패스워드의 값을 한 세션의 통신에서 일회용 패스워드를 사용 후 폐기한다. 따라서 일회용 패스워드가 노출된다고 하더라도 한번 사용 후 다른 값을 생성하기 때문에 공격자가 이전 패스워드를 이용하여 인증받을 수 없다. 안전한 OTP인증기법을 설계하기 위해서는 다음의 공격유형들이 고려되어야 한다 [4]. 먼저 추측공격 유형으로, 토큰정보를 찾아내기 위해 반복적인 검증시도를 통한 OTP 유도방식이다. 탈취 공격 유형은 인증 요청을 성공시키기 위해서 전송 토큰정보의 도청 및 탈취에 의해 불법인증을 시도하는 방식이다. 피싱공격 방식은 사용자가 실제 사이트로 오인하도록 유도하여 입력한 OTP를 탈취한다. 위장공격 방식은 토큰을 원소유자의 것처럼 위장 등록하여 향후 전송되는 인증정보를 가로채어 불법 인증한다. 중간자공격 방식은 인증시스템에게 사용자인 것처럼 위장하거나, 인증시스템으로 위장하여 토큰정보를 가로채 인증 정보를 교체하는 방식이다. 아울러 일회용 패스워드는 빠른 속도를 기반으로 강력한 안전성이 보장되어야한다.

이에 따라 OTP에서의 보안 요구사항은 다음과 같다. 첫 번째, 기밀성으로 통신에 사용되는 데이터들은 정당한 통신 객체들만 공유되어야 하고 통신 중간에 노출되더라도 데이터 값을 유추할 수 없어야 한다. 다음 무결성 조건으로 통신상에서 전송되는 데이터들은 통신 중 위조 및 변조되지 않아야 한다. 또한 빠른 속도로 인증과정을 수행해야 하기 때문에 연산 효율성이 높아야한다. 아울러 OTP를 생성하기 위하여 입력값으로 사용되는 시간 및 이벤트 값이 동기화되어 있어야하며 전송중 비동기화가 발생하지 않아야하는 요구사항들이 있다.

(2) OTP 인증 과정

OTP는 사용자가 인증을 받고자할 때 매번 새로운 패스워드를 생성해주는 방식이다. OTP는 One Time Password의 약자로서, OTP토큰과 인증 서버간 시간이나 씨드(seed)와 같은 비밀 정보를 공유하고 이러한 정보를 해쉬 함수와 같은 알고리즘을 통해 일회용 패스워드를 생성하는 방식을 말한다. OTP인증 과정은 다음과 같다. 그림 1에서와 같이 OTP토큰은 인증서버와 공유하고 있는 시간정보와 Seed 값을 해쉬와 같은 알고리즘을 통해 OTP값을 생성하고 이를 로그인 서버로 ID와 함께 전송한다.

그림 1. OTP 인증 과정
Figure 1. Process of OTP authentication

ID와 OTP를 전송받은 로그인 서버는 해당 정보를 인증센터에 전송하고 OTP를 검증한다. 인증 센터는 수신한 ID를 확인하고 해당되는 시간정보와 seed 정보를 OTP 토큰이 가지고 있는 알고리즘과 동일한 알고리즘을 이용해서 패스워드를 생성하고 이 값과 수신한 OTP 값이 동일한지 여부를 확인하여 로그인 서버에 검증 결과를 알려준다. OTP의 생성방식은 비동기화 방식인 질의응답(Challenge-Response) 방식과 동기화 방식인 시간 동기화(Time-Synchronous) 방식, 이벤트 동기화(Event-Synchronous)방식 그리고 조합 방식 등의 네 가지 방식이 있다.

Ⅲ. 바이오매트릭스 인증기반의 OTP

바이오매트릭스 정보는 절도나 누출에 의하여 도용되거나, 변경 분실될 위험성이 적은 신분 검증 방법으로 평가받고 있지만, 이 또한 모조에 의한 보안의 문제점을 안고 있다. 이러한 패스워드의 누출을 방지하기위하여 일회용 암호키(OTP) 생성에 바이오매트릭스 정보를 이용하여 암호화 인증 키를 생성하는 연구가 필요하게 되었으며, 대표적인 생체인증 방법으로 지문인식 방법이 있다. 지문을 이용하여 추출된 바이오매트릭스 정보로 패턴 매칭과 변위 추적으로 사용자 인증과 보안 토큰의 Seed를 생성할 수 있다. 추출된 사용자의 바이오매트릭스 정보와 기존에 등록된 사용자의 바이오매트릭스 정보를 패턴 매칭에 의한 사용자 인증을 통한 접근제어를 제공한다. 추출된 바이오매트릭스 정보를 이용하여 OTP의 토큰 생성에 사용될 Seed를 생성한다 [5].

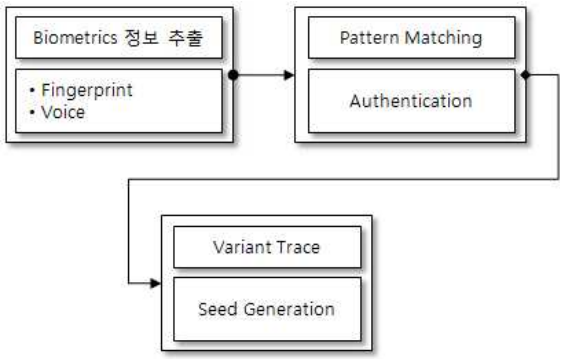


그림 2. 패턴 매칭과 변위 추적에 의한 인증과 Seed 생성
Figure 2. Authentication and Seed generation using pattern matching and variance trace

3-1 바이오매트릭스 정보에 의한 인증

바이오매트릭스 정보에 의한 생체 인식 시스템의 수행 절차는 그림3과 같이 나타낸다. 본 논문에서는 생체 정보의 대표적인 예로 지문을 이용하였다 [5].

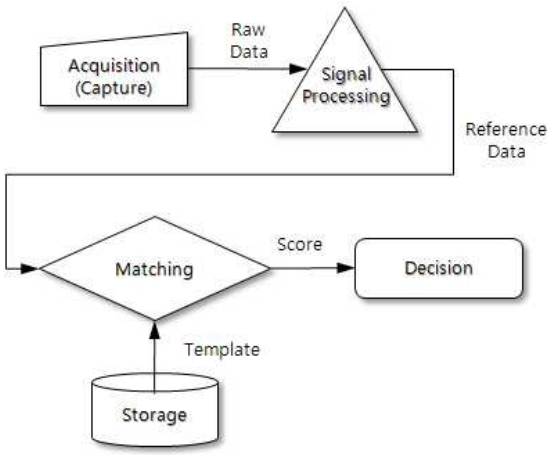


그림 3. 생체인식 시스템의 수행 절차
Figure 3. Procedure of biometrics system

1) 지문인식 및 인증 과정

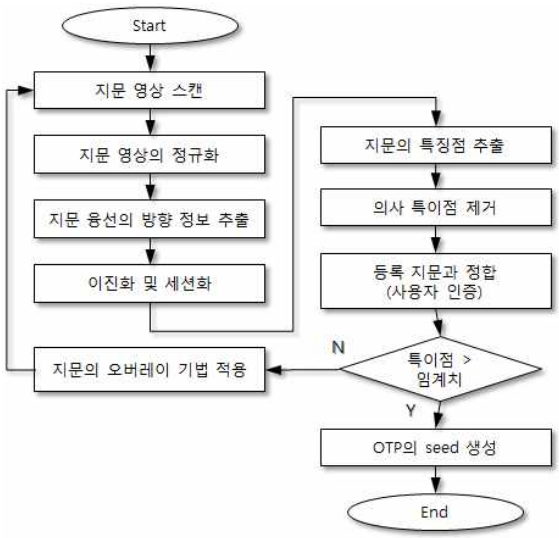


그림 4. 지문 인식 과정의 플로우챠트
Figure 4. Flowchart of fingerprint recognition process

지문 영상의 품질향상을 위한 정규화 단계는 Pixel-wise 연산으로 융선과 골의 구조는 바뀌지 않고, 융선과 골 각각을 따라 변화의 폭을 줄이고 골과 융선의 대조를 분명하게 하는데 목적이 있다. 입력영상의 밝기 정보를 기준으로 mean과 variance로 정규화 한다

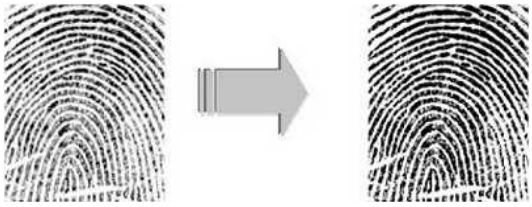


그림 5. 영상의 정규화
Figure 5. Normalization of image

융선의 방향 정보 추출은 일정 블럭 단위로 융선의 방향정보를 추출하는 단계로, 계산 복잡도가 낮은 Sobel 연산자를 이용하여 구한다. 그렇게 구한 융선의 방향은 아래 그림 6의 왼쪽과 같이 잡음이나 상처 등의 여러 가지 원인으로 지문영상의 손실이 생겨 융선의 방향이 급격하게 변하는 잘못된 방향성 정보를 갖게 된다. 따라서 이웃하는 방향성 정보를 이용하여 smoothing 연산을 통해 오른쪽 그림과 같이 융선의 흐름대로 방향성을 갖도록 보정한다.

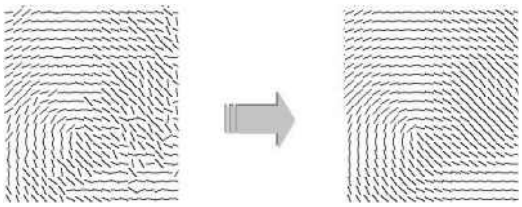


그림 6. 방향 정보 추출
Figure 6. Extraction of direction information

융선 주파수 정보 추출은 방향정보 추출 단계와 같이 블록 단위로 주파수를 구하는 단계이다. 지문의 융선과 골이 주기성을 갖고 있다. 각 블록을 중심으로 윈도우를 씌우고 앞서 구한 방향정보를 이용하여 윈도우를 회전하고 융선의 방향으로 투영하여 그림 6과 같이 1차원 웨이브를 얻는다. 그 웨이브의 봉우리를 구하여 봉우리간의 평균거리를 구한다. 블록 중 지문으로 판별 할 수 없는 경우는 -1로 설정하고, 그런 블럭들은 이웃 블록의 주파수 정보와 Gaussian kernel을 이용하여 보정하고, 마지막으로 블록단위로 low-pass filtering을 하여 최종적인 주파수 정보를 얻는다.

그림 7. 이진화
Figure 7. binarization

그림 7의 이진화 과정에서 가버 필터(Gabor filter)는 빈도 선택적(frequency-selective) 성질과 방향 선택적(orientation-selective) 성질을 갖는다. 앞의 절차의 지문에서 추출한 방향 정보와 주파수 정보를 이용하여 가버 필터 계수를 구하여 필터링(filtering)을 수행한다. 그 결과가 양수이면 골, 음수이면 융선으로 결정하여 이진 영상을 얻는다. 가버 필터는 Bandpass필터로, 융선(ridge)과 골(valley)을 보호하면서 노이즈를 제거하는 융선 추출방법으로, 단순히 영상 밝기 값을 임계(threshold) 값으로 이진화하는 방법에 비해 그 결과가 우수하다. 그림7에서와 같이 주름, 땀샘, 상처로 떨어져 있는 융선을 연결시켜 주고 있는 것을 볼 수 있다. 세선화 과정은 이진화된 영상을 한 픽셀 두께를 갖도록 융선을 세선화 한다.

특징점 추출은 그림 8과 같이 3×3 윈도우를 씌워서 특이점 추출하기 위한 값 CN을 구한다. 그 값이 6이면 분기점이고, 2이면 끝점으로 본다. 그 점의 좌표와 특징점의 방향, 그리고 특징점의 종류를 저장한다.

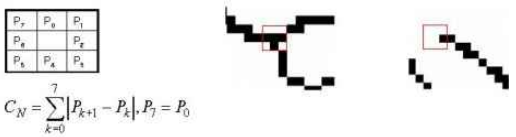


그림 8. 지문의 특이점 추출
Figure 8. Minutiae extraction of fingerprint

의사 특징점 제거 과정은 건조하거나 습한 지문의 상태, 압력의 차이, 먼지, 흉터 등 여러 가지 원인에 의한 영상의 왜곡으로 가짜 특징점이 발생하게 되는데, 이런 가짜 특징점은 인식률의 저하와 특징점의 수 증가로 처리시간과 기억공간의 증가 등 바람직하

지 않은 문제점을 발생시킨다. 다음 그림 9에서 정의한 의사 특징점은 추출된 특징점의 방향정보, 특징점들 간의 거리정보와 각도정보를 이용하여 제거한다.

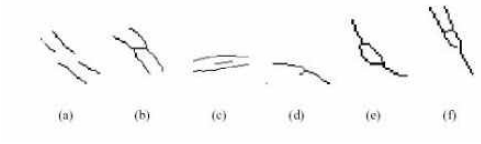


그림 9. 의사 특징점 제거
Figure 9. Elimination of pseudo minutiae

등록 지문과 정합 과정은 동일한 지문이라 하더라도 획득되는 단계에서 shifted, rotated, stretched 된다. 입력 지문 영상과 데이터베이스에 있는 지문 영상 간의 translation, rotation 같은 변형을 추정하여 맞추는 단계로써, 다음 그림 10에서와 같이 등록 지문과 입력지문의 reference 쌍이 붉은 원으로 표시한 특징점이라고 했을 때, 등록된 지문의 reference 특징점을 중심으로 입력된 지문을 translation하고 rotation하여 매칭되는 특징점들을 구한다.

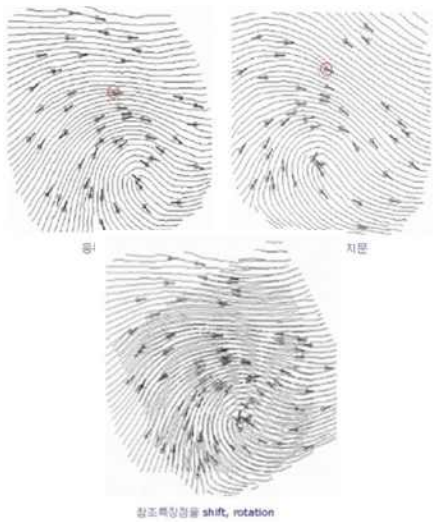


그림 10. 지문의 정합 과정
Figure 10. Matching process of fingerprint

2) 개발한 프로토타입의 인식 과정

특징 점을 제거한 지문에서 위치이동 변화가 큰 점들 저장 한 후 저장한 지문과 입력한 지문의 거리를 특징 점을 이용하여 계산하며, 두 지문의 겹치는 영역 밖의 특징 점은 제거한다. 최종적으로 제거되지 않은 특징 점들을 이용하여 등록된 지문 영상과 입력된 지문 영상의 유사도를 결정하여 지문 인식을 검증한다.

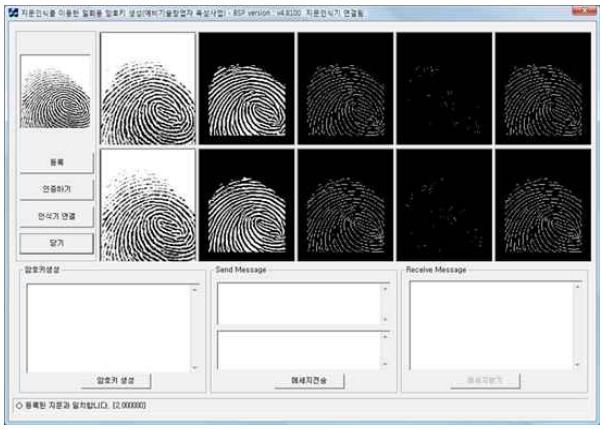


그림 11. 스캔한 지문의 인식 과정
Figure 11. Recognition process of scanned fingerprint

그림 11은 위와 같은 일련의 과정을 거쳐 등록된 지문과 스캔하여 인증한 후의 화면을 보여주고 있다. 패턴 매칭에 의한 사용자 인증의 일반적인 생체인식 시스템의 처리 단계는 그림 4와 같은 과정을 통하여 이루어진다. 지문의 생체정보를 획득한 후 신호처리를 통하여 특징을 추출하는 단계가 공통적으로 포함된다. 이를 기반으로 그림 3과 같이 사전에 동일한 단계를 통하여 변환되어 저장된 데이터베이스 내의 지문의 생체정보와 비교하여 결과를 결정하는 단계로 구성된다.

3-2 바이오매트릭스 OTP 프레임워크

바이오매트릭스 정보는 지문, 음성, 홍채, 망막, 정맥, 서명, 얼굴, 손바닥 등을 이용한다. 그러나 이러한 바이오매트릭스 정보 중에서 모바일 장비와의 인터페이스 측면과 편리성 측면에서 다른 바이오매트릭스 정보보다도 지문이 가장 적합할 것이다. 본 연구에서는 모바일 OTP의 바이오매트릭스 정보를 지문을 기반으로 진행하였다.

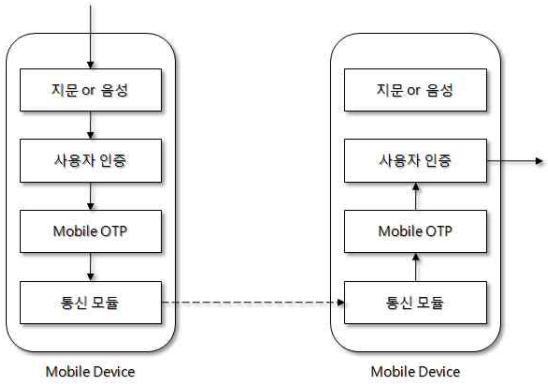


그림 12. 지문 정보를 이용한 모바일의 개인 인증 및 모바일 OTP의 절차
Figure 12. Procedures of Personal Identification and Mobile-OTP of Mobile using Fingerprint and voice information

모바일 OTP의 절차는 그림 12와 같이 나타낼 수 있으며, 지문을 이용한 사용자 인증 절차, 그리고 지문을 이용한 모바일 OTP와 통신 모듈로 구성된다 [6]. 그림 12의 모바일 OTP는 세부적으로 나타내면 그림 13과 같이 나타낼 수 있으며, 바이오매트릭스 정보를 이용한 OTP 프레임워크는 지문을 이용한 바이오매트릭스 정보 추출, 패턴 매칭에 의한 인증과 변위 추적에 의한 보안 토큰 생성, 기업 또는 모바일 기반의 보안 서비스 제공 등의 절차로 구성된다 [9].

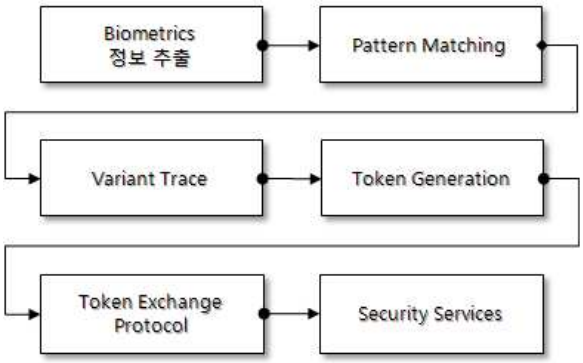


그림 13. 바이오매트릭스 정보를 이용한 OTP 프레임워크
Figure 13. OTP Framework using biometrics information

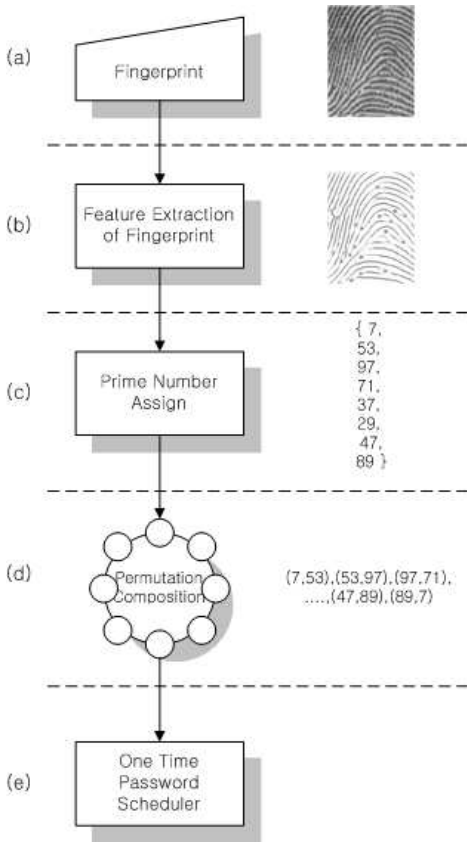


그림 14. 지문 특징점을 이용한 OTP의 토큰 생성 과정
Figure 14. Token Generation of OTP using Fingerprint Feature Points

바이오매트릭스 정보를 생성하기 위하여 지문을 이용한다. 모바일 장치는 주로 스마트폰, 탭, PDA 등이며 대부분이 손을 이용하여 모바일 장치를 사용하기 때문에 지문을 이용한 바이오매트릭스 정보를 생성한다. 지문 인식 시스템은 지문 센서로부터 지문 영상을 획득하는 과정으로부터 시작된다. 지문을 이용한 OTP 토큰을 생성하는 절차는 그림 14와 같다 [7, 8, 9].

Ⅳ. 프로토타입 설계 및 구현

4-1 프로토타입 시스템 인터페이스 구성

프로토타입 시스템의 인터페이스는 그림 15와 그림 16과 같이 구성되었으며, 등록된 지문과 스캔한 지문의 각 처리 과정들의 데이터를 비교할 수 있는

인터페이스를 각 항목들을 나타낸다. 또한 생성된 OTP의 Seed에 의한 암호화 키를 생성해고, 입력한 메시지를 암호 및 복호화하는 과정 및 결과를 나타내어 준다. 각 과정에 대한 명령버튼은 지문등록, 지문인증, 암호키 생성, 메시지 암호화 후 전송, 메시지 복호화를 수행하기 위한 버튼들로 구성하였다.

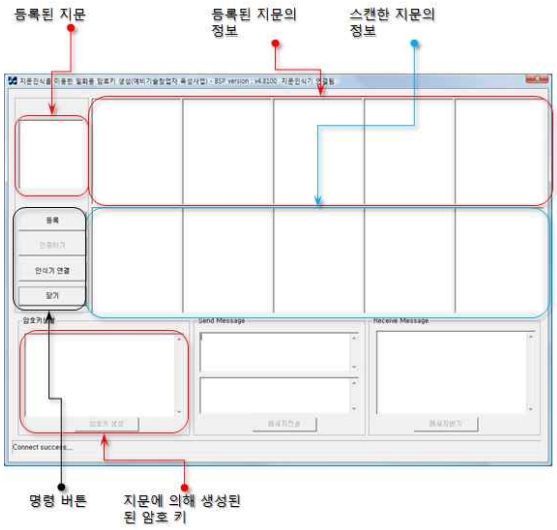


그림 15. 프로토타입 인터페이스 1
Figure 15. Prototype interface 1

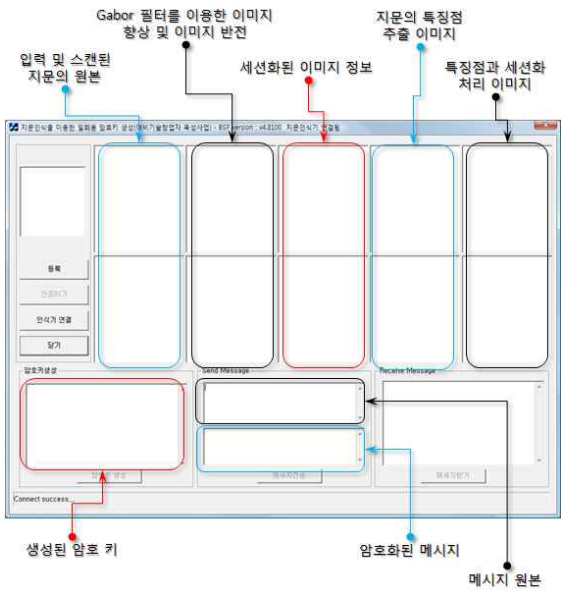


그림 16. 프로토타입 인터페이스 2
Figure 16. Prototype interface 2

4-2 지문을 이용한 OPT생성

구현된 프로토타입에 의한 결과를 그림 17에서 보여주고 있으며, 등록된 지문 정보와 스캔한 지문 정보의 각 처리 과정의 결과를 보여주고 있다. 또한 암호키의 생성과 이를 이용한 보내고자하는 메시지의 암호화와 이를 다시 복호화 한 결과를 보여주고 있다.

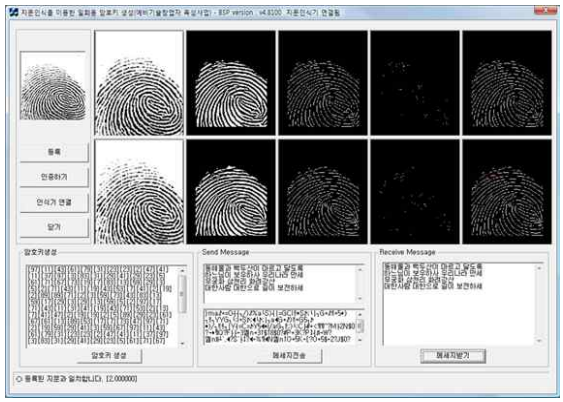


그림 17. 지문을 이용한 암호키 생성 및 메시지 송신/수신 후의 암복화 과정
Figure 17. Encryption key generation and encryption/decryption after transfer/receive of message using fingerprint

Ⅴ. 지문의 중첩 기법 적용

5-1 지문 특징점에 의한 OTP의 취약점 극복을 위한 중첩 기법

지문을 이용한 OTP 시스템은 특히 와상형 지문 영상에서 추출되는 특징점이 매우 적다는 단점을 극복하기 위한 방법으로 지문의 오버레이 기법을 제안한다. 그림 18과 같은 와상형 지문의 적은 특징점은 OTP 세션을 유지하는 많은 암호화 키를 생성할 수 없게 된다. 제안된 방법은 동일한 지문을 오버레이하며 중첩된 지문은 더 많은 특징점을 추가할 수 있으며, 그림 19와 같이 간략하게 나타낸다.

그림 18. 와상형 지문
Figure 18. Fingerprint of type

그림 19. 중첩된 와상형 지문
Figure 19. Overlayed fingerprint

5-2 와상형 지문의 오버레이 기법에 의한 특징점의 변화

와상형 지문과 오버레이 기법을 적용한 와상형 지문의 특징점 수를 시뮬레이션을 통해 비교한다. 그림 20은 와상형 지문의 샘플들을 나타나며, 그림 21은 와상형 지문 샘플의 특징점 수를 나타낸다. 와상형 지문의 오버레이 기법에 의한 중첩된 지문의 간섭에 의해서 임의적으로 특징점 추출에 의한 패스워드의 Seed가 급격히 증가함을 그림 22와 같이 시뮬레이션 결과에서 볼 수 있다. 그림 23은 와상형 지문의 특징점 수와 오버레이 기법을 적용한 와상형 지문의 특징점 수를 비교한 것이며, 최저 3배에서 최대 8배의 비율로 이미지의 간섭에 의한 더 많은 지문의 특징점을 생성하였다. 지문 중첩에 의한 이러한 현상은 지문을 이용한 OTP의 단점으로 부각되는 한정된 패스워드의 씨드를 기하급수적으로 증가시키게 된다. 그러므로 지문의 한정된 패스워드 씨드를 이용하는 순환기법으로 일시적인 패스워드 씨드를 생성하는 것보다 더 신뢰적이며, 임의성을 강화시키는 효과를 제공하게 된다.

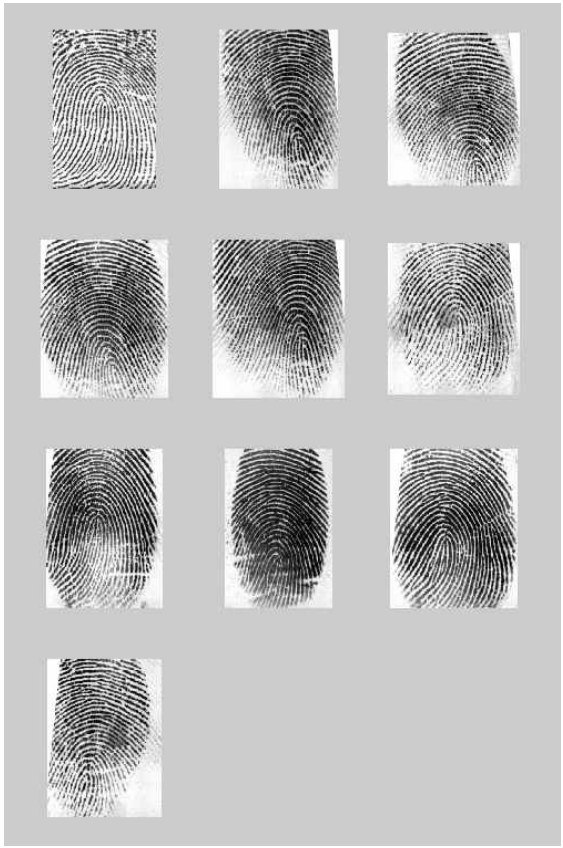


그림 20. 와상형 지문의 샘플
Figure 20. Sample of whorl type fingerprint

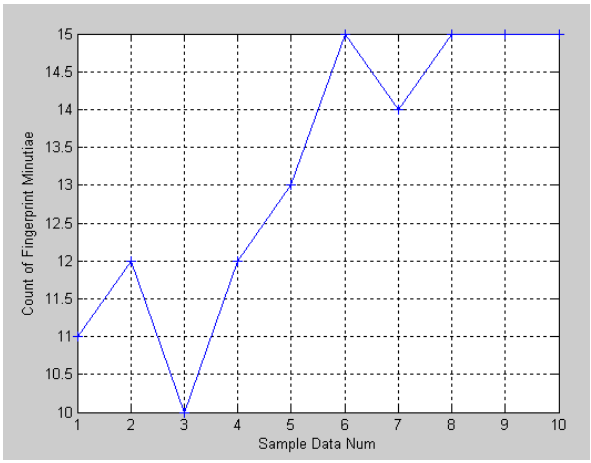


그림 21. 와상형 지문의 특징점 수
Figure 21. Minutiae number of whorl type fingerprint

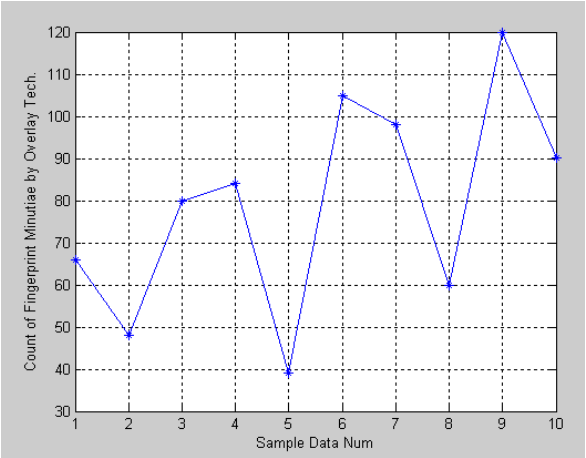


그림 22. 와상형 지문의 오버레이 기법에 의한 특징점 수
Figure 22. Minutiae number of whorl type fingerprint by overlay technique

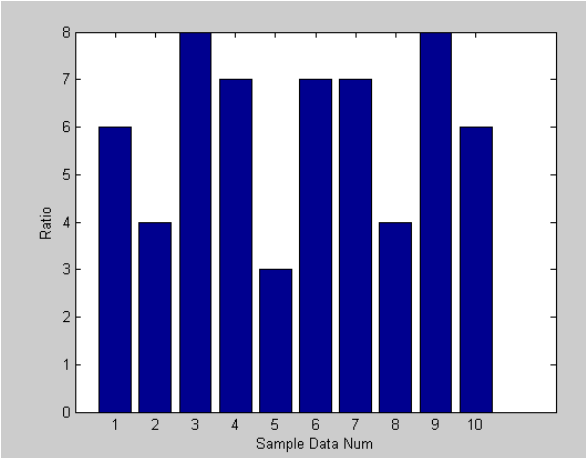


그림 23. 와상형 지문과 오버레이 기법에 의한 특징점 수의 비율
Figure 23. Ratio of whorl type fingerprint vs. whorl type fingerprint by overlay technique

VI. 결 론

지금까지 생체인증 정보 중에 하나인 지문인식을 이용한 OTP를 생성하는 과정과 이의 활용을 보여주는 시스템을 개발하였다. 지문 특징을 이용한 OTP의 Seed를 생성하는 기법의 단점은 지문의 특징점의 적은 경우 보안을 위한 패스워드 생성 측면에서 매우 취약하였다. 이러한 단점의 대표적인 와상형 지문의 경우에는 동일한 지문의 오버레이 기법에 의한 지문의 간섭에 의한 임시적인 특징점을 추가할 수 있으며, 그로 인하여 패스워드의 Seed를 일시적으로 증가시킬 수 있음을 보였다. 지문 중첩에 의한 패스워드의 씨드를 기하급수적으로 증가시키므로 지문의 한정된 패스워드 씨드를 이용하는 순환기법보다 더 신뢰적이며, 임의성을 강화시키는 효과를 제공하게 된다.

참 고 문 헌

[1] Jalal Feghhi & P. Williams, Digital Certificates: Applies Internet Security, *Addison Wesley,* 1999.

[2] A. J. Menezes, P. C. Oorschot & S. A. Vanstone, Handbook of Applied Cryptography, *CRC Press LLC,* 1997.

[3] 김홍기, 이임영, “모바일 환경에서 안전한 One-Time Password 인증 기법에 관한 연구”, *멀티미디어학회 논문지,* 2011년 6월.

[4] J. Archer Harris, "OPA : A One-Time Password System, " 10.1109/ICPPW. 2002, 1039708, 2002.

[5] 김남호, 차병래, 황부현, “Testing of OTP token based on mobile using fingerprint and voice of biometrics”, *JCICT & YES-ICUS 2011,* 2011년 8월.

[6] 차병래, 김남호, 김종원, “바이오매트릭스 정보를 이용한 모바일 기반의 통합 OTP 프레임워크의 유효성 검증”, *한국항행학회 논문지,* 2011년 2월.

[7] 차병래, 고일석, “지문 특징을 이용한 일회용 암호키 생성기법”, *한국전자거래학회 논문지,* 2008년 2월.

[8] 차병래, “지문 특징의 준동형 그래프를 이용한 일회용 암호키 생성기법 및 시뮬레이션”, *한국정보처리학회 논문지,* 2008년 12월.

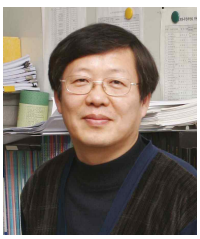
[9] 차병래, 고일석, “Novel OTP System Design using homomorphic graph of Fingerprints”, *IETE Technical Review*, 2009년 7월.

김 남 호 (金男澔)

1997년 8월 : 포항공과대학교 정보통신 학과(공학석사)
2000년 8월 : 전남대학교 전산통계학과 (박사수료)
1991년 4월~1998년 2월 : 포스데이타(주)
1998년 3월~현재 : 호남대학교 인터넷콘텐츠학과 부교수

관심분야 : 데이타마이닝, 유비쿼터스 컴퓨팅, 가상현실 응용, 생체인증 등

황 부 현 (黃富顯)



1978년 숭실대학교 전산학과(학사)
1980년 한국과학기술원 전산학과 (공학석사)
1994년 한국과학기술원 전산학과 (공학박사)
1980년~현 재 전남대학교 전자컴퓨터 공학부 교수

관심분야: 스트림 데이터 마이닝, 이동컴퓨팅, 분산 시스템, 분산 데이터베이스, 전자상거래