한국항행학회 논문지 제15권 제1호 2011년 2월

바이오매트릭스 정보를 이용한 모바일 기반의 통합 OTP 프레임워크의 유효성 검증

Availability Verification of Integration OTP Framework using Biometrics Information

차병래*, 김남호**, 김종원***

Byung-Rae Cha*, Nam-Ho Kim** and Jong-Won Kim***

요 약

모바일 장치의 광범위한 응용과 더불어 통신 보안과 연구가 최근 중요한 관심사가 되고 있다. 본 논문에서는 바이오매트릭스의 지문과 음성의 특징을 이용한 모바일 통합 OTP의 일회용 암호 키 토큰을 생성하는 방법을 제안한다. 강력한 개인 인증에 사용되는 바이오매트릭스의 지문과 음성 정보를 이용하여 모바일 환경의 가변적이고 안전한 일회용 암호 키를 생성하는 OTP 프레임워크를 제안하였으며, 또한 제안 기법에 대한 dendrogram을 이용한 지문과 음성 특징 점에 의한 준동형적 가변성 그리고 지문과 음성 특징 점의 분포를 시뮬레이션 하여 유효성을 검증하였다.

Abstract

As the applications within Mobile devices becoming more extensive, the mobile communication security issues of these applications and researches are appearing to be the most important concern. In this paper, we propose new integration OTP framework technique which uses the fingerprint and voice features of biometrics in order to generate Mobile One Time Passwords (OTPs) Token. The fingerprint and voice are considered to be one of the powerful personal authentication factors of biometrics and it can be used for generating variable passwords based on mobile environments for one time use. However, we performed a simulation of homomorphic variability of fingerprint and voice feature points using dendrogram and distribution of fingerprint and voice feature points for proposed password generation method, and verified validation of availability.

Key words : fingerprint , voice, OTP, mobile

I. 서 론

생활환경의 변화에 따른 IT의 대응이라는 것은 간략하게 말해서 비즈니스 환경 및 실생활 환경의 '급격한' 변화에 따른 IT의 근본적인 변화라고 생각해도 무방할 것이다. 다양해진 수요자의 요구사항과 높아진 기대치를 충족시키기 위한 새로운 비즈니스 모델과 시스템이 필요해졌고, 이를 뒤에서 지원할 수 있

* 광주과학기술원(SCENT Center, GIST)
** 호남대학교 인터넷소프트웨어학과 (Dept. of Internet Software, Honam University)
*** 광주과학기술원 정보통신공학부 (School of Information and Communications, GIST)
· 제1저자 (First Author) : 차병래
· 투고일자 : 2010년 12월 8일
· 심사(수정)일자 : 2010년 12월 9일 (수정일자 : 2011년 2월 7일)
· 게재일자 : 2011년 2월 28일

는 보안 서비스 등이 필수적으로 필요한 상황이다.

일회용 패스워드(One-Time Password)는 매번 로그인 할 때마다 그 세션에서 사용 가능한 1회용 비밀번호를 생성하는 보안 매체로서, 현재 사용하는 비밀번호로부터 다음에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성을 가진다. 따라서 OTP를 이용한 인증방식은 기존의 ID/패스워드 인증방식에서 문제가 되었던 패스워드 재사용 공격, 키로거(Keylogger) 프로그램을 이용한 패스워드 탈취 공격 등의 여러 공격들로부터 안전성을 제공하기 때문에, 금융권 전자금융거래, 기업체 사내시스템 접근통제, 인터넷포털 사이트의 사용자 인증 등 민감한 자원을 다루는 분야에서 활발하게 사용되고 있다. 이와 관련하여 IETF 등에서는 OTP 알고리즘 및 보안 프로토콜을 중심으로 표준화를 진행하고 있는 상태이며, 많은 벤더들로부터 여러 제품들이 출시되어 다양한 산업 영역에 도입되어 서비스되고 있는 중이다.

OTP를 사용하기 위해서 사용자는 패스워드를 생성하는 디바이스를 소지해야 하며, 해당 디바이스가 등록된 인증시스템으로 해당 OTP에 대한 인증 확인을 받아야 한다. OTP 인증 방식이 사용자가 기억하고 있는 패스워드와 함께 OTP 디바이스를 소지해야만 한다는 측면에서 멀티 팩터 인증방식으로 잘 알려져 있다. 그러나, 최근 OTP 기반의 인증과 관련하여, 사용자 편의성을 고려하지 않을 경우 여러 응용서비스들을 사용하는 사용자는 하나 이상의 OTP 디바이스를 소지해야 하는 문제가 제기되고 있다. 따라서 좀더 단순화되거나 사용자 편의성을 고려하는 처리 모델이 요구되고, 이를 위해서 통합 프레임워크 내지 인증 시스템 간 연동 프레임워크의 개발 필요성이 제기되었다.

프레임워크란 한 번 만들어지면 쉽게 바꿀 수 없이 모든 사람들이 사용해야 하는 반쯤 완성된 애플리케이션 (Semi-complete application)이다. 흔히 우리가 사용하고 있는 라이브러리는 내부적인 컨트롤 플로우 (Control Flow)를 갖고 있지 않은 개발 소스들의 단순 집합체이지만 프레임워크는 컴포넌트간의 관계를 고려한 오버라이딩이 가능한 컨트롤 플로우를 제공한다. 요즘과 같은 IT 시장에서는 트랜드가 빠르게 변하면서 특화된 요구를 만족하고 생산성을 높이기 위해 프레임워크의 개발이 요구된다. 프레임워크를 구축할 때 조금이나마 시행착오를 줄이기 위해 기본적으로 5가지 속성인 조직 (Organization), 계획 (Planning), 아키텍처 (Architecture), 설계 (Design), 개발 (Development)를 고려해야 한다. 이러한 요구사항으로부터 ITU-T에서는 2008년 9월 회의에서 국내 금융보안연구원의 주도로 OTP 인증 프레임워크에 대한 신규 표준화 아이템 제안이 SG17의 Q7 (Secure Application Services)로 기고 및 채택 (x.sap-3) 되었으며, 2009년 6월 ITU-T 임시회의에서 2번째 개정된 표준 초안이 발표되었다. ITU-T 표준 초안에서는 OTP 인증 단일모델, 중앙 집중형 모델, 확장된 중앙 집중형 모델, 센터간 통합인증 모델의 4가지 모델을 기술하고 각 기능들을 기술하고 있다. 이를 기반으로 본 표준은 ITU-T 표준 초안의 내용들을 재구성하여 중앙 집중형 모델과 확장된 중앙 집중형 모델을 합쳐서 센터 모델로 기술하여 센터 간의 연동 방안을 추가하였다.

본 논문의 2장에서는 관련 연구로 바이오매트릭스를 이용한 OTP와 OTP 통합인증 서비스 프레임워크에 대해 기술하였다. 3장에서는 바이오매트릭스 정보를 이용한 OTP 프레임워크를 설계하였으며, 4장에서는 Mobile OTP를 이용한 사용자 인증과 화자 인증, 그리고 보안 서비스에 대해 기술한다. 마지막으로 5장에서 결론을 기술하였다.

Ⅱ. 관련 연구

지문과 음성을 이용한 바이오매트릭스 정보를 이용한 OTP의 토큰 생성을 위한 방법과 OTP 통합인증 서비스 프레임워크에 대하여 기술한다.

2-1 바이오매트릭스를 이용한 OTP

바이오매트릭스 정보는 절도나 누출에 의하여 도용되거나, 변경 분실될 위험성이 없는 신분검증 방법으로 평가받고 있다. 하지만 이 또한 모조에 의한 보안의 문제점을 안고 있어, 이러한 패스워드의 누출을 방지하기위하여 일회용 암호 키(OTP) 생성 방법을

생체인증 방법에 적용하여 암호화 인증키를 생성하는 방법을 연구하게 되었다. 이의 대표적인 생체인증 방법으로 지문인식과 음성인식 방법이 있다.

Mobile-OTP는 OTP 전용단말기를 휴대해야 하는 기존 OTP 방식의 단점을 극복하기 위해 사람들이 사용하는 핸드폰에 OTP 모듈을 탑재하여 사용하는 개념이다. 자바 애플릿이 동작되는 휴대전화가 많이 보급되어 있으며, 이러한 자바언어가 가능한 휴대폰이나 PDA과 같은 모바일 장비는 Mobile-OTP를 가능하게 한다. 운영 방식은 클라이언트 컴포넌트(J2ME MIDlet)과 서버 컴포넌트(unix shell script)로 구성되며, 서버 컴포넌트는 라우터, 방화벽, 웹서버, 엑세스 포인트, linux 등에서 사용자를 인증하기 위해 XTRadius와 같은 공개용 RADIUS 서버에 쉽게 플러그인할 수 있다. 클라이언트 컴포넌트인 MIDlet는 MD5 [1]를 가지고 현재 시간, 사용자가 입력한 4자리 PIN 번호, 장치 초기화 시점에서 생성된 16개의 16진수 비밀코드 등의 데이터를 해쉬하여 OTP를 생성한다. 현재 운영되고 있는 모바일 OTP의 예로는 에이티솔루션의 U-OTP [2], 이니텍의 INISAFE MOBILE OTP [3], RSA의 SecureID [4], 블리자드 모바일 인증기 [5]가 있다. 먼저 지문의 특징 정보를 이용하여 OTP의 암호화키를 생성할 경우, 동일한 지문에 대해 매번 동일한 지문 특징 정보를 갖게 되며 이에 따라 암호화 키 또한 동일해 진다. 기존의 연구 방법들은 이와 같이 사용자 개인의 지문에 동일한 값으로 인식을 하게 된다. 따라서 기존의 연구방법에서는 지문을 OTP를 위한 기반 정보로 활용할 수 없게 된다. 하지만 엄밀히 말해 동일한 지문도 매번 스캔할 때마다 약간의 차이를 보이게 된다. 즉 지문 스캔 시에 동일한 지문에 대해서도 스캐닝 되는 위치와 각(Angle)의 변화에 의해서 특징 점 추출에 의한 특징 점 그래프의 변화를 보이게 되며, 준동형 그래프를 생성하게 된다. 이러한 특징을 이용하면 동일한 지문도 매번 스캔 시 특징 점 그래프의 변화에 의한 다른 암호화 키를 생성할 수 있게 되어 지문을 OTP에 사용할 수 있게 된다.

일반적으로 고정된 암호를 이용한 인증은 암호의 추측, 망각, 메모 분실, 도청이나 고의적 누설 등으로 보안상 단점을 가지고 있다. 이에 대한 보완책으로 모바일 OTP는 인터넷뱅킹이나 인터넷쇼핑에 적합한 원격인증 솔루션이라 할 수 있다. 대만의 OTP시스템사의 eCode Mobile 제품의 경우 모바일 OTP생성과 인증을 담당하는 중앙시스템과 SMS 전송시스템으로 구성되어있다. 이 시스템은 스마트카드 시스템과 유사하게 동작하며, 처리절차는 다음과 같다. 먼저 아이디와 고정된 비밀번호를 입력하면 OTP를 생성하여 SMS를 통해 모바일 폰에 전달되고 사용자는 OTP를 입력하여 인터넷뱅킹에 로그인 하게 된다. 원하는 처리 업무를 선택하게 되면 서명 처리데이터를 SMS를 통해 전송받아 확인하여 처리하는 과정으로 구성되어 있다[6]. 또 다른 예로 vidoopSecure사의 Voice OTP시스템의 경우는 인증을 요청한 사용자에게 청취 가능한 일회용 암호를 전화를 통하여 전달하여 사용자를 인증하는 서비스이다. 이를 이용하기 위해서는 사용자 이름과 패스워드를 전송하여 기본적인 사용자 인증을 받은 후 사용자 아이디와 전화번호를 가지고 음성 OTP서비스를 요청하고, 등록한 전화를 통하여 서비스를 제공받는 시스템 구조이다[7]. 한편 모바일 환경의 음성기반 일회용 암호시스템이 응용되어 상용화된 시스템은 스위스의 인증보안 업체인 BIOMETRY사의 MobiComBiom 제품의 경우, 생체정보인 얼굴인식과 음성인식, 입술움직임, 단어인식의 4가지 인증절차로 구성되어있다. 먼저 휴대폰의 두 개의 숫자 버튼을 누르게 되면 화면에 4개 숫자로 구성된 일회용 암호가 표시되고, 사용자는 휴대폰에 내장된 카메라와 마이크를 통해 이들 숫자를 말하게 되면 암호화되어 인증센터에 전송되어 미리 학습 저장된 사용자의 0,1, 2, ..., 9까지의 숫자발음 정보와 비교하여 화자가 일치할 경우 인증을 받게 된다[8].

지금까지 설명한 시스템들의 경우 공통으로 서비스 제공자가 OTP를 생성 제공하여 사용자를 인증하는 구조로 되어있으나, 본 연구에서 제안한 시스템은 사용자의 음성으로부터 자동으로 OTP를 생성하여 본인을 확인하는 근본적인 차이점이 있다. 한편 음성정보를 이용한 OTP 생성의 경우는 외부장치로부터 음성이 입력되고, 입력된 음성을 샘플링한다. 샘플링된 음성에서 잡음을 제거하고 잡음이 제거된 음성신호를 이용하여 OTP의 키를 생성한다. 그리고 생성된 OTP의 키를 이용하여 제안하는 프로토콜로 장치들

간의 OTP의 키를 교환 및 Secure Communication을 수행한다. 이때 지문을 이용한 OTP의 경우는 세션을 유지하기 위한 패스워드의 키의 개수가 적어 키들을 순열로 만들어 일시적으로 무한대의 키 열을 생성하는 방법을 사용해야 하지만, 음성의 경우는 일시적으로 많은 OTP 키를 생성할 수 있어 이러한 단점을 극복할 수 있다.

2-2 OTP 통합인증 서비스 프레임워크

OTP 통합인증 서비스 프레임워크는 OTP 서비스들의 통합된 운영을 제공하기 위한 프레임워크이다.[9] OTP 인증 서비스를 제공하기 위한 서비스 프로바이더는 해당 서비스 도메인의 요구사항과 응용 특성에 따라 기본 모델과 상호 운용 관리 모델을 구현할 수 있으며, 후자는 다시 중앙 집중형 모델, 확장된 중앙 집중형 모델 그리고 크로스 도메인 모델로 구분된다.

기본 관리 프레임워크는 사용자와 단일 서비스 제공자 간의 인증모델이며, OTP 인증 서비스를 제공하기 위한 필수 구성 요소만 갖는다. OTP 인증의 특정 서비스 제공자로부터 OTP 기기 발급받으며, 서비스 제공자는 OTP 인증 서버 구축하며, 사용자는 OTP 인증 요청 검증 기능을 제공하게 된다. 상호 운용관리 프레임워크의 중앙 집중형 모델은 다수개의 기본 프레임워크가 혼합된 형태이다. 개인 사용자가 다수의 서비스 제공자들을 이용하는 시나리오이며, 중앙에 단일화된 OTP 인증 시스템을 구축하며, 다수의 서비스 제공자들에게 OTP 인증을 대행하는 기능을 수행한다. 운영 절차는 최초 OTP 기기 발급하며, 다른 서비스 제공자에게도 OTP 인증을 사용하기 위해서, 새로운 OTP 기기 발급하지 않는다. 그리고 이미 발급된 OTP 기기를 이용/등록하여 사용한다. 서비스 제공자는 자체의 OTP 인증 서버를 구축하지 않고 강한 인증 서비스 제공한다. 상호 운용관리 프레임워크의 확장된 중앙 집중형 모델은 OTP 중앙 집중형 모델의 문제점인 OTP 인증 서비스 제공자의 인증시스템 장애 문제를 극복할 수 있다. 안정성 보장을 위하여 OTP 인증 서비스 제공자의 모든 시설을 이중화한다. 통신구간의 오류, 복구 불가능한 파손에는 서비스를 중단하며, 서비스 중단이 치명적 손실인 특정분야(전자금융, 전자결재)에서는 안정적인 운영을 위한 대체 방안으로 확장할 수 있다. 개별 서비스 제공자가 자체적으로 별도의 OTP 인증 시스템(대체 인증 서버)을 가짐을 제외한 OTP 통합인증 프레임워크와 동일한 구조를 갖는다. 그리고 타 OTP 기기의 등록/사용하는 경우에 OTP 인증 서비스 제공자의 인증 서버를 통해 인증 수행한다. 상호 운용관리 프레임워크의 크로스 도메일 모델은 다수 개의 중앙집중형 모델 간에 연동을 지원하며, 각 도메인은 금융 도메인, 전자정부 도메인, 타국가의 특정 도메인 등의 예를 들 수 있다. 사용자는 1개의 OTP 토큰을 가지고 모든 서비스 제공자에게 인증 서비스 받을 수 있다. 해당 도메인을 담당하는 OTP 인증서비스 제공자 간의 인증시스템 연동만으로 기존 시스템의 변경없이 도메인 간 확장 가능하다.

OTP 인증 모델은 서비스 프로바이더의 응용 특성, 서비스 모델, 사용자 요구사항에 따라 다양한 서비스 시나리오를 구현할 수 있다. 2009년 9월, Q7/SG17로 OTP 인증 서비스 관리 프레임워크(X.Sap-3)로 최종 초안이 제출되었다. 진행 중인 표준화 아이템은 엄격한 사용자 인증 제공 및 관리하는 OTP 기반의 멀티 팩터 인증관리 프레임워크이다. 일반 인증 프레임워크와의 연동 관리 방안이 고려되어야 하며, 관련 분야는 아이덴티티 관리 프레임워크 및 생체인증 등의 멀티 팩터 인증 프레임워크들의 표준 추진 현황으로 강한 인증 서비스(Strong authentication)를 제공하기 위한 신뢰성 있는 인증 서비스의 체계적인 관리 프레임워크 정의 측면의 상관성 분석이 요구된다. 또한 OTP, 바이오인증 및 PKI 인증 프레임워크와 아이덴티티 프레임워크 간의 상호연동 및 관리 프레임워크 정의가 필요하다.

Ⅲ. Biometrics 정보를 이용한 OTP 프레임워크

다양한 바이오매트릭스 정보를 이용한 다양한 보안 시스템들의 구축을 Application Security Framework 도입을 통해 개발 생산성과 안정성을 확보하고 다양

한 비즈니스에 적합하도록 구축하는 것이 주요한 목적이다. Framework 도입 방식은 SI 또는 Package 방식에 비해 최적화된 효과적인 기능 구현이 가능할 뿐만 아니라 고성능의 안정적이고 유연한 베이스 플랫폼을 제공할 수 있다는 장점을 갖는다.

Framework 이란 간단히 요약하면 애플리케이션 구축 시 이를 검증된 아키텍처의 위에서 모든 개발자가 표준화된 방법으로 개발할 수 있게 해주는 컴포넌트와 툴을 포함한 하나의 틀이라고 정의되어 질 수 있다. 프레임워크를 도입하는 첫 번째 목적은 전체 로직 중에서 시스템 의존적인 로직을 분리하는 데 있으며, 두 번째는 프레임워크가 지원할 개념을 위주로 코어 애플리케이션 모듈을 설계해야 하며, 마지막으로는 개발 리소스의 통합 관리를 통한 유지 보수 용이성 등의 제공이다. 프레임워크는 단순히 개발 생산성 향상이라는 개발 측면에 국한된 기능을 제공하지 않으며, 보안 서비스와 운영 단계에서도 전반적인 서비스를 제공한다.

3-1 바이오매트릭스 정보를 이용한 OTP 프레임워크의 기본 구성

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 지문과 음성이 가장 적합할 것이다. 본 연구에서는 모바일 OTP의 바이오매트릭스 정보를 지문과 음성을 기반으로 진행하였다.

모바일 OTP의 절차는 그림 1과 같이 나타낼 수 있으며, 지문 또는 음성을 이용한 사용자 인증 절차, 그리고 지문 또는 음성을 이용한 Mobile OTP와 통신 모듈로 구성된다.

그림 1의 Mobile OTP는 세부적으로 나타내면 그림 2와 같이 나타낼 수 있으며, 바이오매트릭스 정보를 이용한 OTP 프레임워크는 지문과 음성을 이용한 바이오매트릭스 정보 추출, 패턴 매칭에 의한 인증과 변위 추적에 의한 보안 토큰 생성, 기업 또는 모바일 기반의 보안 서비스 제공 등의 절차로 구성된다.

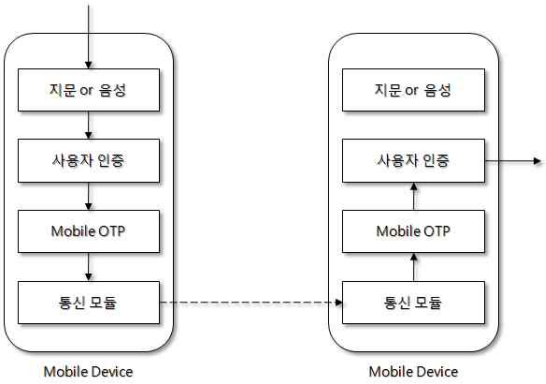

그림 1. 지문 및 음성 정보를 이용한 모바일의 개인 인증 및 모바일 OTP의 절차
Fig. 1. Procedures of Personal Identification and Mobile-OTP of Mobile using Fingerprint and voice information

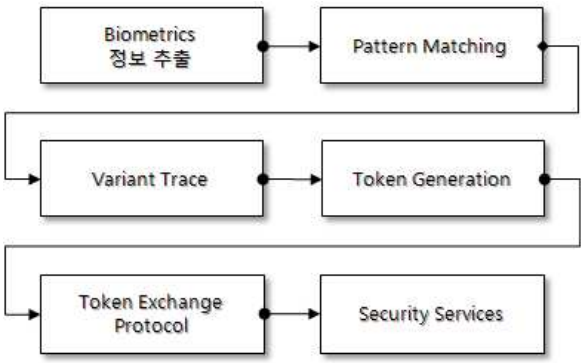

그림 2. 바이오매트릭스 정보를 이용한 OTP 프레임워크
Fig. 2. OTP Framework using biometrics information

3-2 바이오매트릭스 정보 추출

바이오매트릭스 정보를 생성하기 위하여 지문과 음성을 이용한다. 모바일 장치는 주로 핸드폰, PDA, 이며, 대부분이 손 또는 음성을 이용하여 모바일 장치를 사용한다. 그러한 이유로 바이오매트릭스 정보의 대상을 손의 지문과 음성을 이용한 바이오매트릭스 정보를 생성한다.

3-2-1 지문의 바이오매트릭스 정보 추출

지문 인식 시스템은 지문 센서로부터 지문 영상을 획득하는 과정으로부터 시작된다. 지문 영상을 획득하면, 영상을 입력하고 저장하여 지문의 인식 검증

과정에 사용한다. 이 과정에서 전처리 → 방향영상 → 전경 분리 → 이진화 → 세션화의 방법을 거치게 된다. 세션화까지 거치고 나면 후보 특징 점을 추출해서 특징 점을 저장 될 수 있는 점을 추출하여 저장하며, 그 특징 점의 방향을 결정하고, 지문 오인식의 원인이 될 수 있는 잔가지구조, 원형구조, 끊긴 구조 등의 의사 특징 점을 제거한다. 지문을 이용한 OTP 토큰을 생성하는 절차는 그림 3과 같이 나타낸다[18, 19].

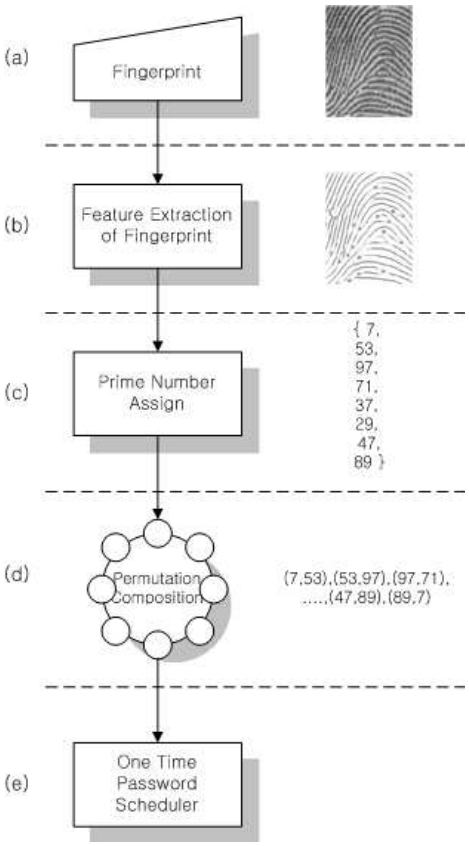

그림 3. 지문 특징점을 이용한 OTP의 토큰 생성 과정
Fig. 3. Token Generation of OTP using Fingerprint Feature Points

3-2-2 음성의 바이오매트릭스 정보 추출

제안된 음성을 이용한 OTP 방법의 절차는 모바일 장치에 음성이 입력되고, 입력된 음성을 샘플링한다. 샘플링된 음성에서 잡음을 제거하고 잡음이 제거된 음성 신호를 이용하여 OTP의 키를 생성한다. 그리고 생성된 OTP의 키를 이용하여 모바일 장치의 보안 적용으로 Secure Communication 및 다양한 보안을 지원할 수 있다. 그림 4에 나타낸 것과 같이, 제안된 음성을 이용한 OTP 방법의 절차는 4단계로 구성되며, 각 단계는 다음과 같다[14].

- Step 1: 모바일 장치(특히 핸드폰 또는 인터넷 폰)에 음성이 입력되면, 입력된 음성으로 샘플링을 수행한다.
- Step 2: 샘플링된 음성에서 잡음을 제거한다.
- Step 3: 잡음이 제거된 음성 샘플링으로 OTP의 키를 생성한다.
- Step 4: 제안하는 프로토콜로 모바일 장치 또는 장치들 간의 OTP의 키를 교환 및 모바일 장치들 간의 Secure Communication을 수행한다.

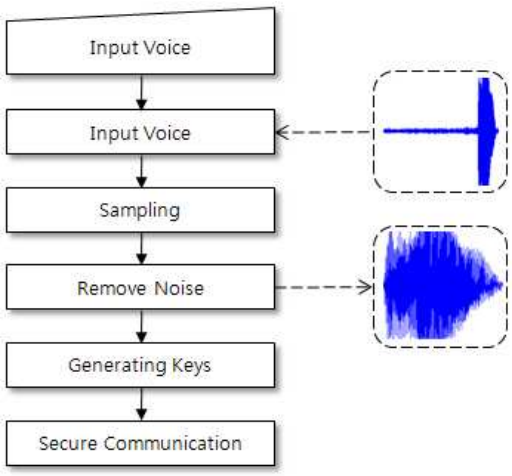

그림 4. 음성을 이용한 OTP의 절차
Fig. 4 OTP Procedure using voice

3-3 패턴 매칭 및 변위 추적

지문과 음성을 이용하여 추출된 바이오매트릭스 정보로 패턴 매칭과 변위 추적으로 사용자 인증과 보안 토큰의 Seed를 생성할 수 있으며, 그림 5와 같이 나타낸다. 그림 5는 그림 2의 바이오매트릭스 정보 추출, 패턴 매칭, 그리고 변이 추적의 단계를 세부적으로 나타낸 것이다. 그림 5의 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.

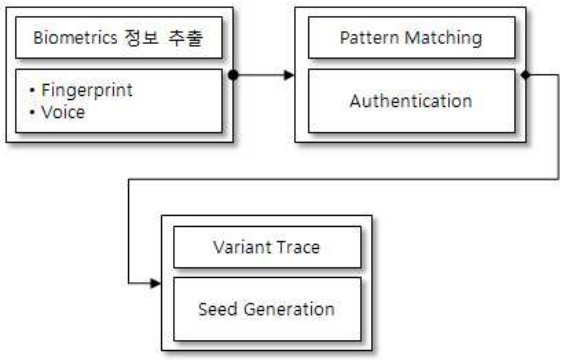

그림 5. 패턴 매칭과 변위 추적에 의한 인증과 Seed 생성
Fig. 5. Authentication and Seed generation using pattern matching and variance trace

3-3-1 패턴 매칭에 의한 사용자 인증

일반적인 생체인식 시스템의 처리 단계는 다음의 그림 6과 같은 과정을 통하여 이루어진다. 센서 등의 생체 디바이스에서 생체정보를 획득한 후 신호처리를 통하여 특징을 추출하는 단계가 공통적으로 포함된다. 이를 기반으로 사전에 동일한 단계를 통하여 변환되어 저장된 데이터베이스 내의 생체정보와 비교하여 결과를 결정하는 단계로 구성된다[10].

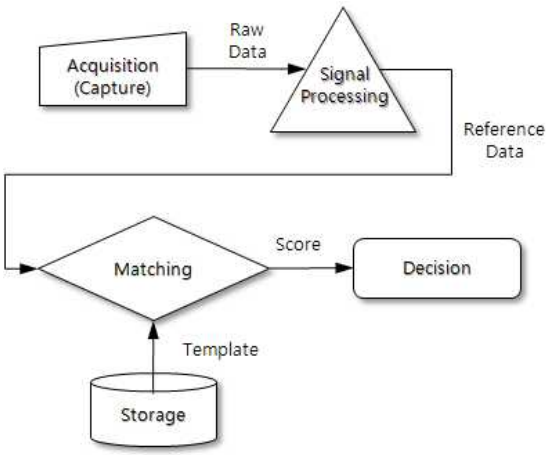

그림 6. 생체인식 시스템의 수행 절차
Fig. 6. Procedure of biometrics system

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

3-3-2 바이오매트릭스 정보의 변위에 의한 보안 토큰 생성

지문과 음성의 바이오매트릭스 정보를 이용한 Mobile OTP의 토큰을 생성하는 절차에 대해서 언급한다.

(1) 지문 정보의 경우

먼저, 지문의 경우에는 임의의 한 지문을 매번 스캔하면 지문의 형태는 불변하지만, 매번 스캔할때마다 동일한 지문에 대해서 위치와 각의 변화를 감지할 수 있으며, 이러한 변의 예로 그림 7에 나타낸다.

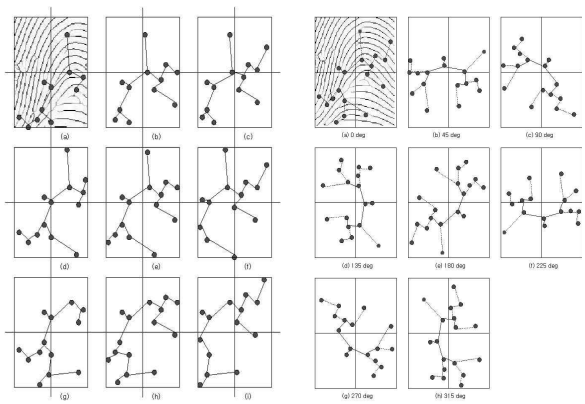

그림 7. 동일한 지문의 위치와 위치 변화에 의한 특징점의 변화
Fig. 7. Variant of Fingerprint Feature Point by Changed Location and Angle using Same Fingerprint

그림 7의 왼쪽은 동일한 지문을 이용하여 우측과 아래쪽으로 3mm씩 이동하여 지문의 특징 점 추출과 추출된 특징 점을 이용한 준동형 그래프의 변화를 나타낸 것이며, 그림7의 오른쪽은 동일한 지문의 각의 변화에 따른 준동형 그래프의 변화를 나타내었다. 지문의 특징점 그래프 생성 과정은 스캔화면의 정중앙에서 가장 가까운 노드에서 시작하여 프림 알고리즘으로 MST(Minimum spanning tree) 그래프 [11]를 생성하여 나타낸다. 그림 7을 통해서 동일한 지문도 매번 스캔할 때마다 약간의 차이를 갖게 된다는 것을 알 수 있다. 즉 지문 스캔 시에 동일한 지문에 대해서도 스캐닝되는 위치

와 각(Angle)의 변화에 의해서 특징 점 추출에 의한 특징 점 그래프의 변화를 보이게 되며, 준동형 그래프를 생성하게 된다. 이러한 특징을 이용하면 동일한 지문도 매번 스캔 시 특징 점 그래프의 변화에 의한 다른 토큰을 생성할 수 있는 Seed를 생성할 수 있게 되어 지문을 OTP에 사용할 수 있게 된다. 이러한 상황은 다른 바이오매트릭스도 동일한 상황일 것으로 예측한다.

(2) 음성 정보의 경우

먼저, 음성 신호에서 OTP의 키를 생성하기 위해서는 음성 신호와 잡음 신호를 구분하여 제거하여야 한다. 음성 신호의 샘플링에서 잡음 신호를 제거하지 않으면 OTP의 키가 생성된 공간에서 일부 영역에 응집된 형태를 보이게 되므로 패스워드 키 공간의 확산 측면에서 취약점을 갖게 된다. 이러한 취약점을 제거하기 위해서는 잡음을 제거하므로 써 확산의 취약성을 일부 제거할 수 있다. 음성 신호를 샘플링하면 백색잡음 영역과 음성 영역이 확연히 구분된다.

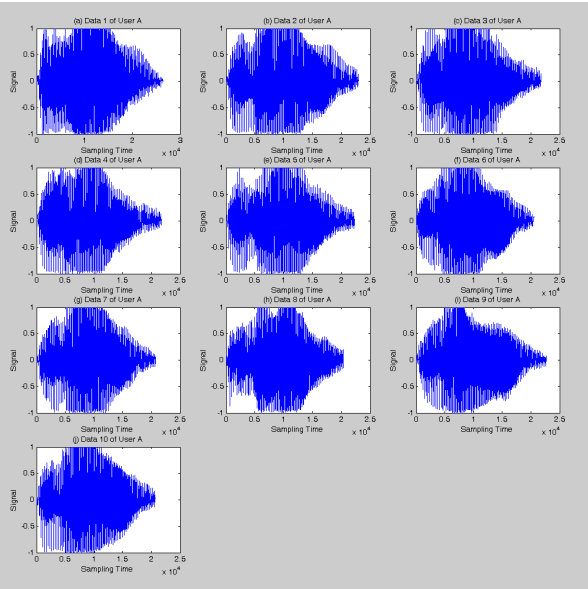

그림 8. User A의 10개 Voice Sampling DataSets
Fig. 8. User A's 10 Voice Sampling DataSets

그림 8은 음성에서 잡음을 제거한 후의 음성 샘플링을 나타낸 것이며, 잡을 제거하지 않은 음성보다 사용자 음성의 고유 패턴에 대한 특성이 매우 잘 나타난다. 그림 9는 User A, B, C, D, 그리고 E의 Voice의 DataSet 분포를 나타낸 것이며, 잡음을 포함하는 음성의 분포보다 패턴들의 평균값은 감소하였지만, MEAN과 STD 측면에서 훨씬 더 넓게 분포되어 있음을 확인할 수 있다.

음성을 이용한 OTP는 지문을 이용한 OTP와 생성된 키 숫자 측면에서 매우 우수한 특성을 갖으며, 이미지 처리와 비교하여 음성처리를 위한 컴퓨팅 파워가 절약되며, 또한 키 순열을 만드는 절차가 줄어들게 되는 장점을 갖게 된다.

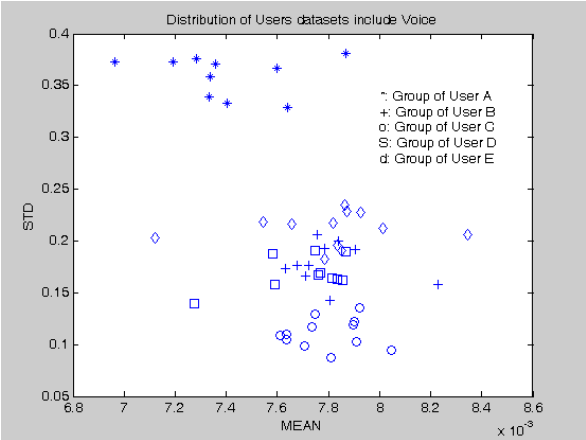

그림 9. User A ~ D, 그리고 E의 Voice DataSets의 분포
Fig. 9 Dist. of User A ~ D, and E's Voice DataSets

Ⅳ. Mobile-OTP의 보안 서비스

4-1 Biometrics 정보를 이용한 사용자 인증

기존의 단순한 형태의 개인 확인 및 검증방법의 한계를 극복하여, 절도나 누출에 의하여 도용 될 수 없으며 변경되거나 분실할 위험성도 없는 새로운 형태의 신분 검증 방법에 대한 연구 분야가 바로 생체인식기법이라고 말하는 바이오매트릭스 분야이다. 이 분야에서 대상으로 하는 인간의 생체학적 특성은 크게 지문이나 얼굴, 홍체, 화자인식, 서명인식 등이 있다.

4-1-1 지문을 이용한 사용자 인증

개개인의 인증을 위한 방법으로 바이오매트릭스 정보 중의 하나인 지문을 많이 이용하고 있다. 각 개인의 지문은 땀샘이 융기되어 일정한 흐름을 형성한 것으로, 그 모양이 개인마다 서로 다를 뿐만 아니라 태어날 때

의 모습 그대로 평생 동안 변하지 않음이 증명되어 실생활에 사용되어져 왔다. 인식에 필요한 개인별 특징추출에 사용되는 방법으로는 주파수 공간에서의 Fourier, Wavelet 변환 또는 신경회로망이나 퍼지논리에 의한 것 등을 들 수 있다. 하지만 지문에는 기준 좌표축이 존재하지 않으므로 임의로 회전되어 채취된 지문에 대한 처리가 어려우며, 또한 지문은 진체의 일부로서 유연성을 가지고 있어 채취할 때마다 그 모양이 달라 보이는 문제점이 있기는 하지만, 오히려 이는 지문정보가 OTP 생성에 유용한 장점을 제공한다고 볼 수 있다.

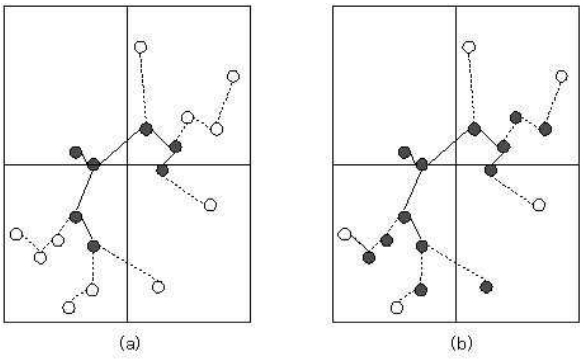

그림 10. 위치와 각변화에 따른 특징점 그래프의 고정된 노드와 변화된 노드
Fig. 10. Fixed and Variant Node of Feature Point Graph by Changed Location and Angle

4-1-2 음성을 이용한 화자 인증

화자 인식은 화자의 음성에 의한 화자를 인식하는 것이다. 응용에 따라 화자 확인 (Speaker verification)과 화자 식별 (Speaker Identification)으로 구분된다. 화자 확인은 사용자의 발성된 음성이 원하는 화자 인지 아닌지를 구분하기 위하여 기준 패턴과 입력 패턴을 비교하여 임계치를 넘어서면 승인한다. 이를 위하여 의뢰인에 대한 초기 등록이 요구된다.

음성에 의한 개개인 고유의 음성특징을 이용하여 본인 여부를 화자 확인에 의한 인증해주는 화자 인증은 모바일 디바이스의 분실이나 불법 도용의 위험이 없는 첨단 보안 기술이며 그림 11과 같이 나타낸다. 또한 다른 생체인식에 비해 기술적, 경제적인 면에서 효용성이 크고, 모바일 디바이스 등의 다양한 하드웨어는 물론 홈뱅킹과 홈트레이딩, 전자상거래, 등의 기타 각종 유료사이트 등 인터넷과 전화를 통한 원거리에서의 인증도 가능하다는 장점이 있다. 단 3회의 음성암호 등록만으로 사용자의 고유 음성에 대한 완벽한 학습이 가능함과 복잡한 등록절차를 간소화 하여 비숙련된 사용자가 쉽게 사용할 수 있다.

기존의 단순한 음성신호의 비교 방식이 아닌 문맥 독립적인 음소모델과 이중으로 비교하는 다원적인 음성비교로 인증률의 향상 및 주기적으로 변화하는 사용자의 목소리의 변화를 매 인증 시 마다 음성암호 DB에 자동적으로 반영하도록 구성되어 화자인증의 인증률이 시간이 지나감에 따라 저하되는 치명적인 단점을 해결할 수 있다. 다수의 단어 DB의 비교가 아니므로 인증 속도가 획기적으로 향상될 수 있다.

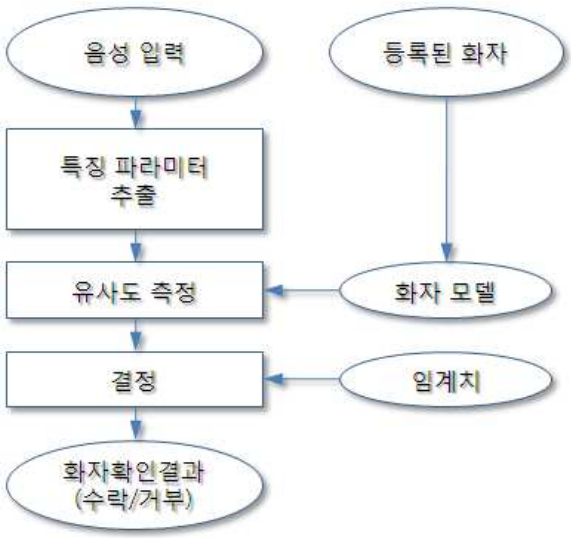

그림 11. 음성에 의한 화자 확인 절차
Fig. 11. Speaker verification procedure using voice

4-2 Mobile-OTP의 보안 서비스

Mobile OTP의 보안 서비스는 크게 두 개의 그룹으로 일반적인 모바일 서비스와 보안 서비스로 나눌 수 있다. [20] 사용자 B와 사용자 C 간의 일반적인 모바일 서비스와 사용자 A와 B, 그리고 사용자 A와 사용자 C 간의 신뢰를 제공할 수 있는 보안 서비스로 구분된다. 그림 12에 나타난 것과 같이 사용자 A는 모든 사용자들의 연락처와 바이오매트릭스 정보에 의한 OTP 토큰을 갖고 있으며, 사용자 B와 사용자 C는 각각의 사용자들 연락처만을 갖고 있다. 사용자 A의 경우에는 사용자 B 또는 사용자 C와의 통신 서비스에 바이오매트릭스의 OTP 토

큰을 이용하여 음성 통신과 SMS의 암호화 기능을 지원할 수 있으며, 비신뢰 관계에 의한 SMS 필터링 및 거부 등의 부가적인 기능을 제공할 수 있다.

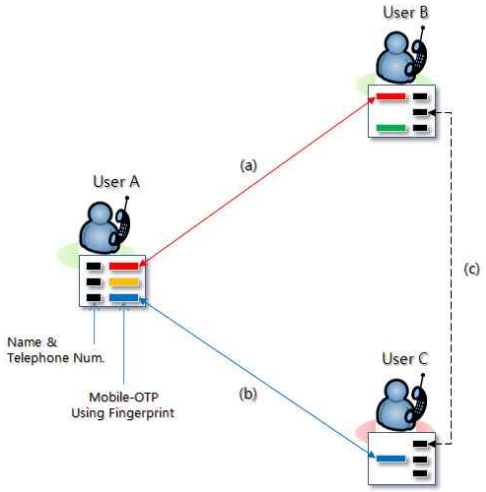

그림 12. Mobile OTP 기반의 보안 서비스
Fig. 12. Secure Services of Mobile OTP based

V. 시뮬레이션

5-1 지문을 이용한 OTP

지문을 이용한 OTP의 시뮬레이션은 지문의 변화에 따른 dendrogram에 의한 거리 비교와 지문의 특징 점 변화를 측정 및 분석한다.

5-1-1 지문의 위치와 각 변화에 의한 거리 비교

Dendogram은 Bio-Information의 게놈 프로젝트에서 유전자들 간의 거리를 측정하는 도구로 많이 사용된다. 지문 특징 점에 의해 생성된 9개의 준동형 그래프를 이용하여 dendrogram [12]과 각각의 노드에 임의의 3자리 난수를 할당하여 dendrogram으로 나타내었다. 이때 dendrogram은 JMSL [13] 라이브러리를 이용하였다.

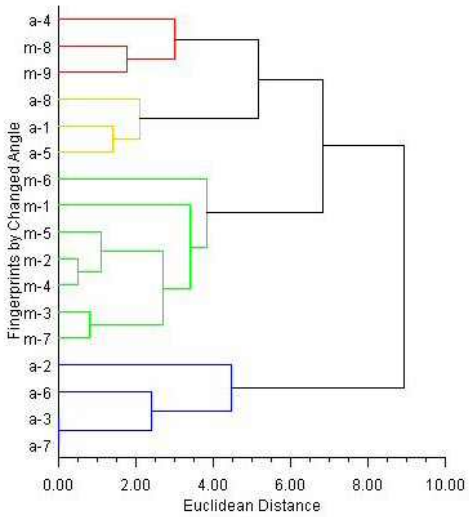

그림 13. 위치와 각의 변화를 혼합한 지문 그래프의 Dendrogram
Fig. 13. Dendrogram of Fingerprint by Changed Location and Angle

그림 13에서 dendrogram에 의해서 동일한 지문이지만 위치와 각의 변화에 의해서 17개의 준동형 그래프 생성으로 무작위성을 갖을 수 있음을 알 수 있고, 난수 할당에 의해 무작위성과 확산이 확대되었음을 보여준다. 지문은 음성에 비교해서 특징점이 많지 않다는 단점을 지문 특징 점의 순열 구성을 이용함으로서 한 세션에 대해 일시적으로 무한개의 암호화키를 생성할 수 있게 된다.

5-1-2 지문의 위치 변화에 따른 특징 점 변화 측정

샘플 지문 데이터 30개의 위치변화에 따른 지문 특징 점의 준동형 그래프의 변화를 측정하였다. 그림 14는 30개 샘플 지문의 위치와 각 변화에 대한 고정 및 변화된 특징 점과 특징 패턴들 간의 관계를 나타내었다. 지문 데이터의 위치 변화에 따른 특징 점의 준동형 그래프에서 고정된 특징 점의 비율에 대한 최소와 최대는 각각 12%와 83%이었다. 또한, 변화된 특징 점의 비율은 최소와 최대는 각각 17%와 88%이었다. 고정 및 변화된 특징 점의 평균은 52.1%와 47.9%이며, 표준편차는 2.8328%이었다. 위 시뮬레이션의 결과는 하나의 지문을 스캔한 지

문 이미지에 대해서 위치 변화에 따른 준동형 그래프를 생성하였으며, 그 결과를 순열을 이용하여 일시적으로 무한대의 암호화키를 생성할 수 있음으로 보였다. 이러한 특징 때문에 사전 연구로써 OTP 시스템에 사용될 수 있는 유효성을 검증하였다.

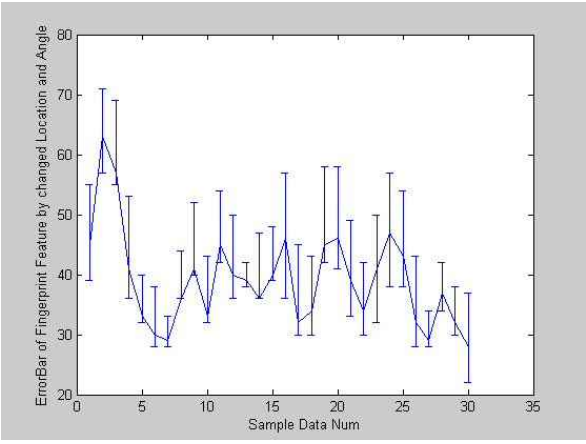

그림 14. 30개 샘플 지문 데이터의 위치(Location)과 각(Angle) 변화에 대한 고정된 특징 점과 변화된 특징 점 그리고 특징 패턴 간의 관계
Fig. 14. Relation of Fixed and Variant Feature Pattern of 30 Sample Fingerprint by Changed Location and Angle

5-2 음성을 이용한 OTP

5-2-1 카오스 신호 vs. Voice 신호

카오스의 구성요소는 초기 치와 그의 전개 양상을 결정짓는 전개함수의 모양을 갖는다. 초기치란 그 출발점(x0)을 말하며, 전개함수의 모양이란 일단 주어진 출발점의 값이 전개되어 가는 양상을 말한다. 반복되는 함수(Iterative function) 연산의 피드백에 의한 0에 수렴하거나, 무한대로 발산하거나, 또는 초기 값이 극히 조금만 달라져도 그 안정은 깨져버리는 매우 불안정한 수렴상태(unstable convergence)로 (-∞와 +∞)사이의 모든 실수 집합을 세 부류(three subsets)로 나누어주는 프랙탈 기하(trichotomy fractal geometry)를 구성한다.

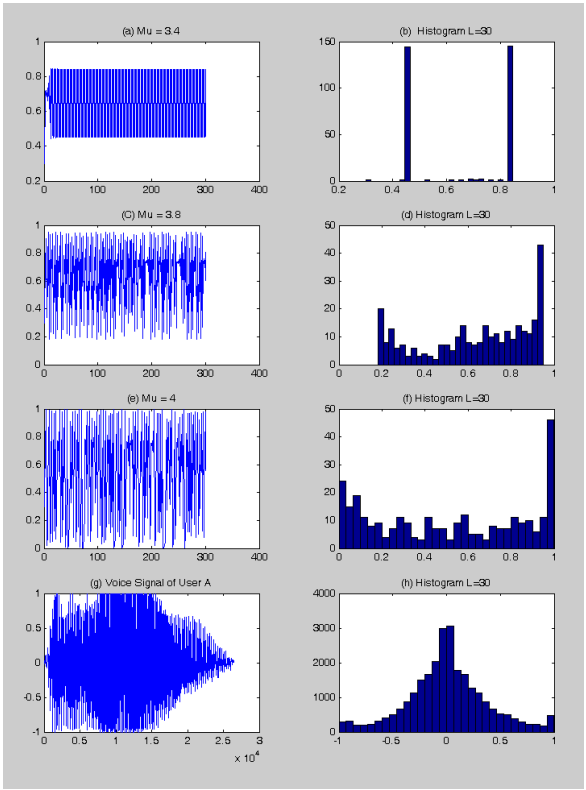

그림 15. 카오스 방정식에 의한 Mu 값의 변화에 따른 생성된 Signal과 히스토그램, 그리고 사용자 A의 Signal과 히스토그램
Fig. 15. Signal and Histogram of Chaos equation by Mu, and User A's Signal and Histogram

그림 15는 카오스 방정식에 의해서 임의적으로 무작성을 갖는 패턴을 생성할 수 있으나, Mu와 초기치를 알면 반복적인 계산에 의해서 패턴을 추적가능하게 된다. 특히 그림 15의 (a), (c) 그리고 (e)는 Mu 값의 변화에 따른 진폭과 반복된 계산 결과를 나타낸 것이며, 그림 15의 (b), (d) 그리고 (f)는 히스토그램으로 임의의 10개 영역의 분포를 나타냈다. Mu 값이 3.4에서 3.8, 4.0으로 커짐에 따라 패턴의 분포가 임의의 부분 영역에 집중되는 경향에서 점점 넓게 분포되는 경향을 보였다. 그림 15의 (g)와 (h)는 User A의 Voice의 Signal과 히스토그램을 나타냈으며, 분포가 정규분포적인 형태를 보였다. 잡음을 제거한 음성의 왜도(Skewness)와 첨도(Kurtosis)를 분석하면, 왜도가 0이고, 첨도가 3이면 좌우대칭이며 중첨이 형태이지만, 왜도 $\mu_3 = 0.0038$으로 약간 우비대칭이며, 첨도 $\alpha_4 = 3.5893$이므로 분포 형태가 급첨으로 나타났다[14]. 그림 16은 Mu 값의 카오스 신호와 음성의 신호에 대한 평균과 표준 편차를 나타낸다. 카오스 신호는 Mu값이 증가함에 따라 평균은 감소하는 경향을 보

였고, 표준 편차는 단조 증가하는 경향을 보였다. 그러나 음성 신호는 평균은 거의 0에 근접하였으나, 표준 편차는 다른 카오스 신호보다도 컸다.

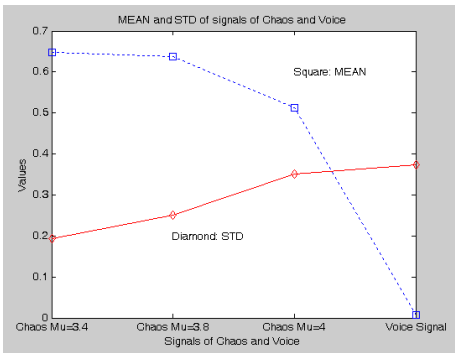

그림 16. Mu 값의 카오스 signal과 음성 signal의 MEAN과 STD
Fig. 16. MEAN and STD of chaos' signals according to Mu and voice signal

5-2-2 무작위성(Randomness)

User A의 “Hello"라는 음성을 10번 샘플링한 후에 잡음을 제거하여 DataSet을 구성하였다.

그림 17은 User A의 음성에서 잡음을 제거하여 10개의 샘플링을 비교하였다. Distance 500을 기준으로 5개의 그룹으로 나눌 수 있으며, Distance 1000을 기준으로 3개의 그룹으로 나누어진다. 잡음은 샘플링된 음성 신호의 특성을 제거하는 단점을 갖음을 알 수 있다[14]. 그림 17은 가장 큰 Distance를 5000을 기준으로 하고 있다. 결과적으로 음성 샘플링에서 잡음을 제거하면 샘플링된 음성들 간의 정밀한 특징 패턴을 갖고, 더불어 Distance 측정으로 무작위성이 커짐을 확인할 수 있다.

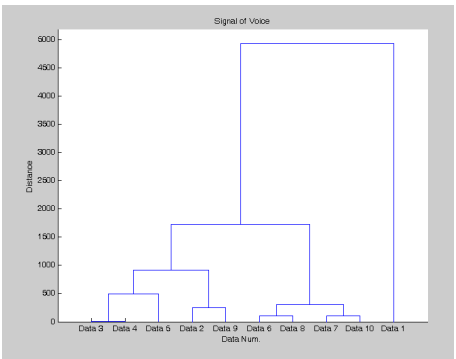

그림 17. User A의 Voice Dataset의 Dendrogram
Fig. 17. Dendrogram of User A's Voice Dataset

5-2-3 카오스와 Voice에 의한 키 생성

카오스와 Voice에 의한 키를 생성하여 키들 간의 분산을 비교 및 분석한다.

그림 18은 Random 함수와 카오스 신호, 음성 신호, 그리고 일정한 간격의 음성 신호를 샘플링한 것을 나타낸 것이다. 그림 18의 신호들을 이용한 토큰를 만들기 위해서는 키 공간에서의 키들의 확산 정도를 측정하여야 한다. 이를 위한 여러 방법 중에서 간단하게 생성된 토큰들의 분포를 검사하여 비교 분석한다.

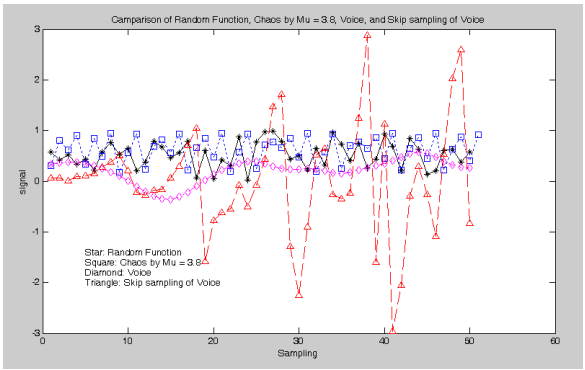

그림 18. Random 함수, 카오스, 음성, 그리고 음성 Skip 샘플링의 결과
Fig. 18. Results of Random Func., Chaos, Voice, and Voice Skip Sampling

그림 19는 Random 함수와 카오스 신호, 음성 신호, 그리고 일정한 간격의 샘플링한 음성 신호들의 분산과 평균을 나타내고 있다. 1차 평가로 4가지 신호들의 분산을 나타냈을 때, 일정한 간격의 샘플링한 음성 신호의 분산이 매우 컸다. 1차 평가로 신호들이 동등한 분산을 갖는다면 2차 평가로는 평균에 의한 평가로 신호들 간의 상대적 평가로 키들의 확산정도를 비교할 수 있다. 그림 19의 평균에서 일정한 간격의 샘플링한 음성 신호가 또한 평균값도 상대적으로 작아서 확산 정도가 다른 신호들에 비해서 크다는 것을 나타내었다.

5-2-4 Voice의 Skip sampling에 의한 키 생성

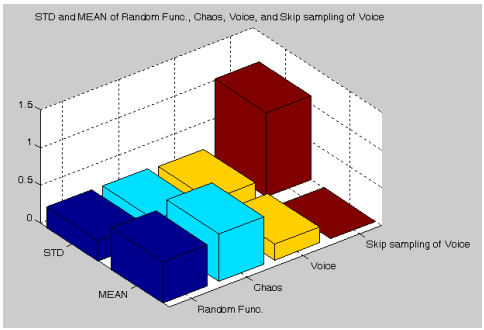

그림 19. 각 신호들의 분산과 평균
Fig. 19. STD and MEAN of each signals

음성을 이용한 키 생성에서의 단점은 음성 그래프가 Smooth 하다는 것이다. 이러한 단점을 일정한 간격으로 skip sampling에 의해서 키 생성에 확산성을 임의적으로 증가시킬 수 있다. 사용자 A의 음성의 일부를 샘플링한 것과 사용자 A의 음성을 skip sampling 하여 비교 분석한다.

그림 20은 사용자 A의 음성 샘플링으로 생성된 토큰을 dendrogram으로 나타냈으며, 그림 21은 음성을 Skip 샘플링으로 생성된 토큰을 dendrogram으로 나타낸 것이다. 그림 20과 21을 비교하면, 일반적으로 음성을 사용하는 것보다는 음성을 skip sampling하면 키 공간의 확산성이 커짐을 보였다.

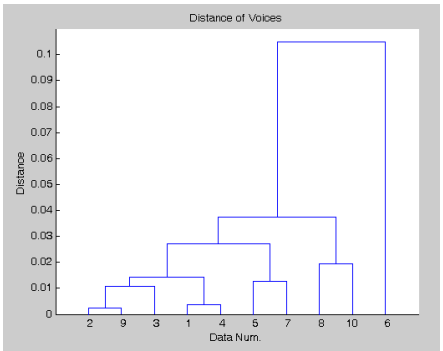

그림 20. 사용자 A의 음성 샘플링 DataSet의 Dendrogram
Fig. 20. Dendrogram of User A's Voice Sampling DataSet

5-3 mOTP Token Generator와의 비교

지문과 음성의 바이오매트릭스를 이용한 OTP에서 생성한 Token들과 mOTP Token Generator에서 생성한 Token들을 비교한다.

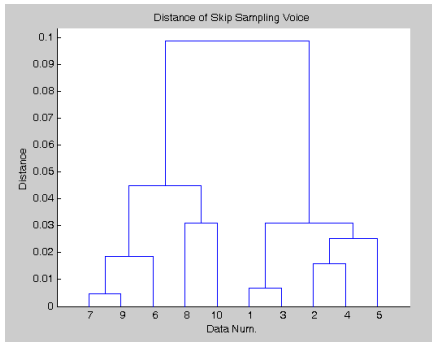

그림 21. 사용자 A의 Skip Sampling에 의한 음성 샘플링 DataSet의 Dendrogram
Fig. 21. Dendrogram of User A's Voice Skip Sampling DataSet

mOTP Token Generator [15] 는 SourceForge [16] 웹사이트에서 다운로드 및 설치가 가능한 오픈소스 코드이다. mOTP Token Generator는 파이썬 [17] 기반의 24비트의 토큰을 생성하며, 그림 21의 (a)와 같이 생성하였다. 그림 21의 (b)는 제안된 시스템으로 생성한 토큰을 나타낸 것이다.

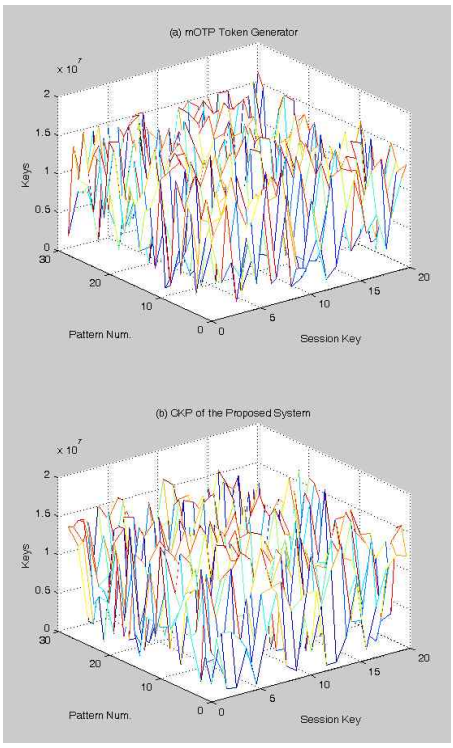

그림 21. mOTP Generator와 제안된 시스템의 키들
Fig. 21 Keys in mOTP token generator and the proposed system

Ⅵ. 결 론

모바일 장치의 광범위한 응용과 더불어 통신 보안과 연구가 최근 중요한 관심사가 되고 있다. 또한 정보 시스템의 대부분이 개방형 유무선 네트워크이기 때문에 악의의 공격자에 의한 다양한 형태의 공격에 대해 취약하다는 다양한 단점들을 갖고 있으며, 이러한 단점들을 극복하고자 많은 노력과 연구가 이루어지고 있다. 본 연구에서는 모바일 사용자의 지문과 음성의 바이오매트릭스 정보를 이용한 OTP 키를 생성하는 방법을 제안 및 시뮬레이션을 수행 및 유효성을 검증하였다. 특히 동일한 지문의 다수의 스캔에 의한 준동형의 특징 점에 의한 OTP의 토큰 생성에 의한 가변성을 보였으며, 음성의 경우에는 카오스와 랜덤함수, 사용자의 음성 샘플링, 그리고 음성의 skip sampling에 의한 토큰 생성에 의한 무작위성과 확산성을 보였으며, mOTP Generator와의 OTP 토큰의 비교하여 유효성을 검증하였다. 이를 기반으로 지문과 음성을 이용한 OTP 키의 생성을 통합하기 위한 프레임워크를 설계하였으며, 보안을 강화하기위한 지문과 음성을 통한 인증도 제공할 수 있음을 보였다. 또한 지문을 이용한 OTP의 단점을 음성에 의한 OTP로 해결할 수 있음을 보여준다.

감사의 글

이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. [NRF-2009-353-D00048]

참 고 문 헌

[1] MD5, http://en.wikipedia.org/wiki/MD5

[2] U-OTP, http://www.u-otp.co.kr/

[3] INISAFE MOBILE OTP, http://www.initech.com /www/html/inisafe/ goMenu3_5_1.html

[4] SecureID, http://www.rsa.com/node.aspx?id=1156

[5] 블리자드 모바일인증기, http://www.blizzard.co.kr/

[6] OTP Systems, "Mobile One-Time Password", http://www.otp.com.tw/Index/Section/23

[7] vidoopSecure, "Voice OTP", https://www.vidoop.com /docs/voice-otp

[8] BIOMETRY.com AG, "MobiComBiom, Mobile Communication Biometrics", http://www.biometry.com /perma-voice.html

[9] OTP 인증 프레임워크의 표준화 동향, *한국정보통신기술협회*, http://www.tta.or.kr/data /weekly_view.jsp?news_id=2748

[10] 생체정보보호를 위한 가이드라인, 정보통신단체 표준 TTAS.KO-12.0034, *한국정보통신기술협회*, Dec. 2005.

[11] MST, http://en.wikipedia.org/wiki /Minimum_spanning_tree

[12] Dendrogram, http://en.wikipedia.org /wiki/Dendrogram

[13] JMSL, http://www.vni.com/products/imsl/jmsl/

[14] 차병래, 김남호, 김종원, “음성을 이용한 모바일 기반의 OTP 설계”, *한국항항학회 논문지 8월호*, 2010.

[15] mOTP Token Generator, http://wiki.birth-online.de /software/python/motp-token-generator

[16] http://motp.sourceforge.net/

[17] Python, http://www.python.org/

[18] ByungRae Cha, Franz I. S. Ko, "Novel OTP System Design using homomorphic graph of Fingerprints", *IETE Technical Review,* vol. 26, July 2009.

[19] 차병래, 김남호, 김종원, “지문 특징을 이용한 모바일 일회용 암호키 및 시뮬레이션”, *한국항행학회 논문지 8월호*, 2009.

[20] 차병래, 김종원, “지문을 이용한 Mobile-OTP의 보안 응용에 관한 연구”, *한국통신학회 하계학술대회*, 2010. 6. 24.

차 병 래 (車炳來)

2004년 2월 : 국립 목포대학교 컴퓨터공학과(공학박사)
2005년 3월 ~ 2009년 2월 : 호남대학교 컴퓨터공학과 전임강사
2009년 9월~현재 : 광주과학기술원 (GIST), 고성능컴퓨팅·협업환경 연구센터 연구교수
관심분야 : 정보보안, Intrusion Detection System, 신경망, Future Internet 등

김 남 호 (金男澔)

1997년 8월 : 포항공과대학교 정보통신학과(공학석사)
2000년 8월 : 전남대학교 전산통계학과 (박사수료)
1991년 4월~1998년 2월 : 포스데이타(주)
1998년 3월~현재 : 호남대학교 인터넷소프트웨어학과 부교수
관심분야 : 데이타마이닝, 유비쿼터스 컴퓨팅, 가상현실 응용, 생체인증 등

김 종 원 (金宗源)

1997년 8월 ~ 2001년 7월 : University of Southern California 연구 조교수
1999년 12월 ~ 2000년 7월 Technology Consultant for VProtect Systems Inc.
2000년 7월 ~ 2001년 6월 Technology Consultant for Southern California Division of InterVideo Inc.
2001년 9월 ~ 2008년 3월 광주과학기술원 정보기전공학부 부교수
2008년 4월 ~ 현재 광주과학기술원 정보기전공학부 교수
관심분야 : Networked Media Systems and Protocols focusing "Reliable and Flexible Delivery for Integrated Media over Wired/Wireless Networks“