음성 특징 파라메터를 이용한 모바일 기반의 OTP 설계

Design of OTP based on Mobile Device using Voice Characteristic Parameter

차병래*, 김남호**, 김종원***

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

요 약

유비쿼터스와 모바일의 광범위한 응용과 더불어 통신 보안은 최근 중요한 관심사가 되고 있다. 따라서 각각의 보안 요소마다 다양한 기법 및 응용에 대한 연구와 시스템적 응용에 대한 연구가 활발히 이루어지고 있다. 본 논문에서는 음성의 특징을 이용한 모바일 OTP의 일회용 암호 키를 생성하는 방법을 제안한다. 본 연구는 강력한 개인 인증에 사용되는 바이오매트릭스의 음성 정보를 이용하여 가변적이고 안전한 일회용 암호 키를 생성하였으며, 또한 제안 기법에 대한 덴드로그램(dendrogram)을 이용한 음성 특징점에 의한 준동형적(homomorphic) 가변성 그리고 음성 특징점의 분포를 시뮬레이션 하였다.

Abstract

As the applications based on Mobile and Ubiquitous becoming more extensive, the communication security issues of those applications are appearing to be the most important concern. Therefore, every part of the system should be thoroughly designed and mutually coordinated in order to support overall security of the system. In this paper, we propose new technique which uses the voice features in order to generate Mobile One Time Passwords(OTPs). Voice is considered to be one of the powerful personal authentication factors of biometrics and it can be used for generating variable passwords for one time use. Also we performed a simulation of homomorphic variability of voice feature points using dendrogram and distribution of voice feature points for proposed password generation method.

Key words : Voice, OTP, Mobile Device

I. 서 론

컴퓨터는 메인 프레임과 워크스테이션을 거쳐 PC로 점점 소형화되어 왔으며 근래에는 노트북, 스마트폰 크기로 작아져 휴대가 간편해 졌다. 컴퓨팅 장치의 소형화와 대량 생산으로 유비쿼터스 컴퓨팅 패러다임의 서막이 시작되고 있다. 하지만 유비쿼터스 환경에서 컴퓨팅 장치의 특징은 최소형화된 컴퓨터이며, 기본적인 컴퓨팅 기능을 제외하고 PC 수준의 컴퓨팅 능력을 수행하기 힘든 실정이다. 앞으로 점차

* 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 6월 14일
· 심사(수정)일자 : 2010년 6월 14일 (수정일자 : 2010년 8월 20일)
· 게재일자 : 2010년 8월 30일

컴퓨팅 능력이 향상되겠지만 필요한 컴퓨팅 능력을 가지지 못한 유비쿼터스 컴퓨팅 장치들은 충분한 수준의 보안 애플리케이션을 수행하기 힘들다. 따라서 유비쿼터스 컴퓨팅 환경에서는 경량 암호화 알고리즘 및 프로토콜의 개발이 필요하며, 또한 충분한 컴퓨팅 능력을 가진 신뢰관계에 있는 다른 컴퓨팅 장치에 위임하는 등의 연구가 필요하다.

유비쿼터스 컴퓨팅 장치들 중에서 가장 주목받는 것은 모바일 장비인 스마트폰이며, 항상 사용자에게 가장 근접하여 개인 정보를 많이 갖고 있는 장치이다. 그러나 해킹이나 정보유출로 인하여 개인의 신상정보의 수집/분석/검색/복제/유통이 훨씬 용이해지면서 프라이버시 문제를 발생시키고 있다. 특히 스마트폰 장치들은 개인의 프라이버시에 민감한 데이터가 노출되기 쉽기 때문에 정보보안 분야에서 최근 가장 큰 이슈로 대두되고 있다. 스마트폰 마켓의 한 예로 Android Market[1]은 22개의 Category를 갖고 있으며, Security과 관련된 Category는 존재하지 않고 있다. Category:Communication에서는 또한 Featured, Top Free, 그리고 Top Paid로 구분되며, 등록된 보안 도구는 Featured 항목에서는 40 아이템 중에서 보안 관련 아이템은 존재하지 않았으며, Top Free 항목에서는 79 아이템 중에서 보안에 관련된 아이템은 2개, Top Paid 항목에서는 80 아이템 중에서 보안 관련 아이템은 1개로 나타났다. 현재 안드로이드 마켓은 애플리케이션 아이템들의 개발 및 등록의 활성화에 있으며, 향후에 애플리케이션 아이템들의 활성화로 보안 관련 아이템들도 활발히 개발될 것으로 기대한다.

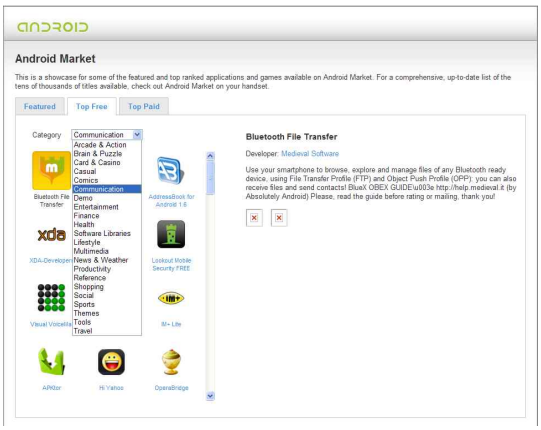

그림 1. 안드로이드 마켓
Fig. Android market

모바일 장치는 정보보안 측면의 개인의 프라이버시에 매우 민감한 부분이며, 모바일 장치에 간단한 기능을 추가함으로써 보안 기능을 제공할 수 있는 방법을 제안한다. 본 논문에서는 모바일 기반의 음성을 이용한 OTP를 생성하는 방법을 제안하였으며, 이를 임의의 사용자 5명으로부터 음성을 샘플링하여 제안된 방법으로 시뮬레이션을 수행하여 음성에서 잡음을 제거함으로써, OTP를 위한 키 생성에 우수하다는 것을 증명하였다.

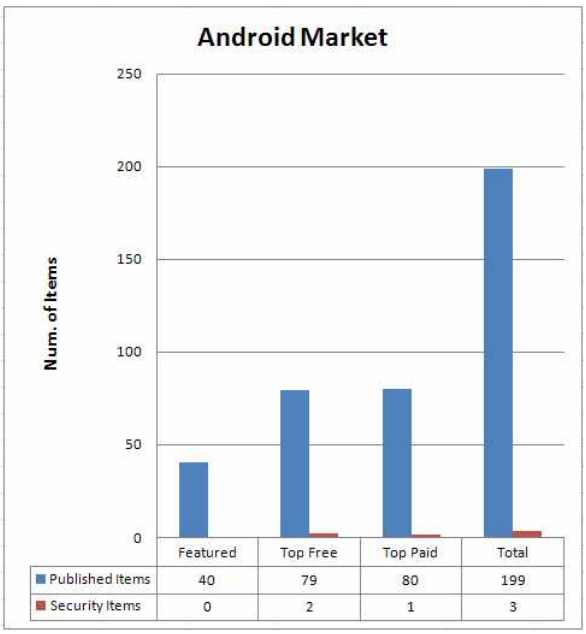

그림 2. 안드로이드 마켓의 보안 아이템의 비율
Fig. 2 Security items ratio in Android market

Ⅱ. 관련 연구

2-1 VoIP와 화자 인식

저렴한 요금의 특성으로 인터넷전화(VoIP) 사용이 급격히 늘어나고 있으며, 특히 이동통신과 인터넷전화가 결합된 유무선통합(FMC)서비스가 화두가 되는 등 인터넷전화 서비스가 차세대 통신 서비스의 주류로 자리매김할 것으로 예상되는 가운데 보안에 대한 관심도가 높아지고 있다. 가입자가 금년 상반기에 1000만명을 넘어설 것으로 예상되는 가운데 빠르게 PSTN을 대체하고 있다. 하지만 지난해 인터넷전화

게이트웨이 IP 해킹으로 약 1억원 이상의 요금이 사용자 측에 청구되는 보안사고가 발생하는 등 시장 성숙과 맞물려 그 어느 때 보다 VoIP 보안에 관한 관심이 높아진 상황이다. 이로 말미암아 기존의 저장형 암호기반의 인증 정보의 보안도 안심할 수 있는 여건이 아니라 판단된다. 결국 이러한 보안의 대안으로서 고정형 비밀번호를 대체할 수 있는 일회용암호 기술의 도입이 더욱 필요하게 되었으며, 쉽게 취득하여 처리할 수 있는 음성정보의 활용이 대안이라 보여진다. 음성은 허용성의 차원에서 인간에게 가장 자연스럽게 취득 될 수 있을 뿐만 아니라, 전화나 통신망 등을 통하여 원거리에서도 쉽게 보내어 질 수 있기 때문에 음성인식과 화자인식 분야에서 많이 연구되어 왔다. 특히, 음성을 이용한 생체인식 기법은 그 어떤 생체 특성보다도 향후의 네트워크 및 유무선 통신망의 발달에 발맞추어 그 활용분야가 넓어지리라 기대되고 있다. [2]

이러한 음성은 개인의 신원이나 구사된 언어의 종류, 화자의 심리적, 육체적, 감정상의 상태에 대한 정보를 포함하고 있다. 이러한 정보를 이용한 화자의 신원 파악, 즉 화자 인식이 많은 관심을 끌고 있다. 특히 음성의 특징은 화자간의 변이가 화자내의 변이에 비해 상대적으로 크다는 성질을 이용하여 어느 정도의 신뢰성을 가지고 화자를 구분할 수 있다. 이러한 화자간의 변이를 이용하여 발성한 사람을 알아내는 것을 화자인식시스템이라 한다. [3, 4] 이러한 화자인증 및 화자식별 기술은 개인의 음성 특징이 유일하다는 사실을 근거로 하고 있으며 최근의 인터넷과 모바일 기술의 발전과 더불어 보안을 위한 인증방법으로 각광을 받고 있다. 하지만 개인의 생체정보는 영원히 변하지 않는다는 것이 프라이버시 문제의 시작인데, 비인가된 불법 디바이스에 의해 사용자의 원본 생체정보가 아닌 조작된 생체정보가 입력된다던지, 획득되어지는 음성 생체정보가 라이브 정보가 아닌 녹음기를 통한 가짜 정보가 입력되는 경우 문제가 생겨날 수 있다. [5] 이와 같은 문제를 해결하고자 일회용 패스워드(OTP)와 같은 정보보호 기술의 도입이 필요하다.

2-2 Voice-OTP

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 처리데이타를 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.

2-3 지문을 이용한 Mobile-OTP

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 MD5를 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 [9], 이니텍의 INISAFE MOBILE OTP [10], RSA의 SecureID [11], 블리자드 모바일인증기 [12]가 있다.

Ⅲ. 음성을 이용한 OTP 설계

지문을 이용한 Mobile-OTP와의 제안한 Voice-OTP는 모든 절차와 특징은 거의 동일하지만, 단지 세션을 유지하기 위한 패스워드의 키의 개수에서 차이점을 갖고 있다. 이러한 상황은 지문을 이용한 Mobile-OTP의 단점으로 작용하고 있다. 이를 해결하는 방법으로 키들을 순열로 만들어 일시적으로 무한대의 키 열을 생성하는 방법을 사용하고 있다. Voice를 이용한 OTP를 생성할 경우에는 일시적으로 많은 키를 생성할 수 있으므로 이러한 단점을 극복할 수 있으며, 키들을 순환으로 만들 필요가 없다.

3-1 음성을 이용한 OTP의 절차

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.

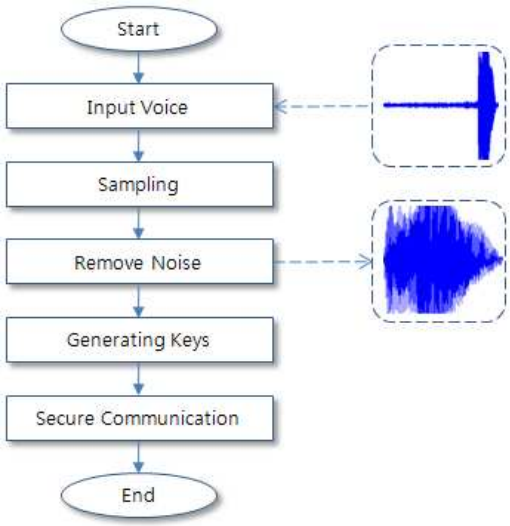

그림 3. 음성을 이용한 OTP의 절차
Fig. 3 OTP procedures using voice

그림 3에 나타낸 것과 같이, 제안된 음성을 이용한 OTP 방법의 절차는 4단계로 구성된다.

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

3-2 음성 신호에서의 백색 잡음 제거

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.

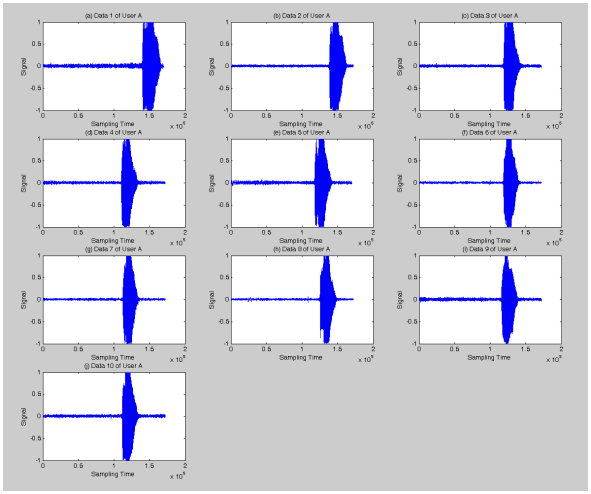

그림 4. User A의 Voice와 Noise를 포함한 10개의 샘플링 DataSets
Fig. 4 10 sampling datasets include user A's voice and noise

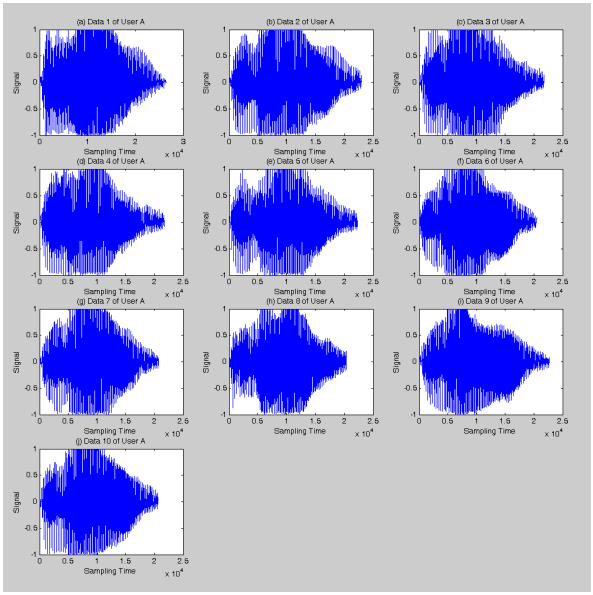

그림 5. User A의 Voice만 포함한 10개의 샘플링 DataSets
Fig. 5 10 Sampling datasets include user A's voice

이러한 취약점을 제거하기 위해서는 잡음을 제거하므로써 확산의 취약성을 일부 제거할 수 있다. 음성 신호를 샘플링하면 백색잡음 영역과 음성 영역이 확연히 구분된다. 그림 4에서 User A의 “Hello"라는 음성을 10번 샘플링한 결과를 나타낸 것이다. 그림 5는 그림 4에서 잡음을 제거한 후의 음성 샘플링을 나타낸 것이다. 그림 5은 그림 4보다는 고유의 패턴에 대한 특성이 매우 잘 나타나 있으나, 잡음을 제거하므로써 OTP의 키를 숫자가 줄어드는 영향을 받게 된다. 그러나 그 영향력은 매우 미비하며, 지문을 이용한 OTP와는 생성된 키 숫자 측면에서 매우 우수한 특성을 갖는다. 더불어 음성처리와 비교하여 이미지 처리를 위한 컴퓨팅 파워가 절약되며, 키 순열을 만드는 절차가 줄어들게 된다. 그림 6은 Voice만을 포함한 DataSet과 Voice와 Noise를 포함한 DataSet의 3D Plot을 나타낸다. 그림 6에서는 잡음을 포함하는 경우 Signal Length와 평균의 위치가 훨씬 크지만, 패턴들의 분포들은 협소하게 위치하여 있다. 특징 패턴의 왜곡 현상을 갖고 있는 것으로 파악할 수 있다.

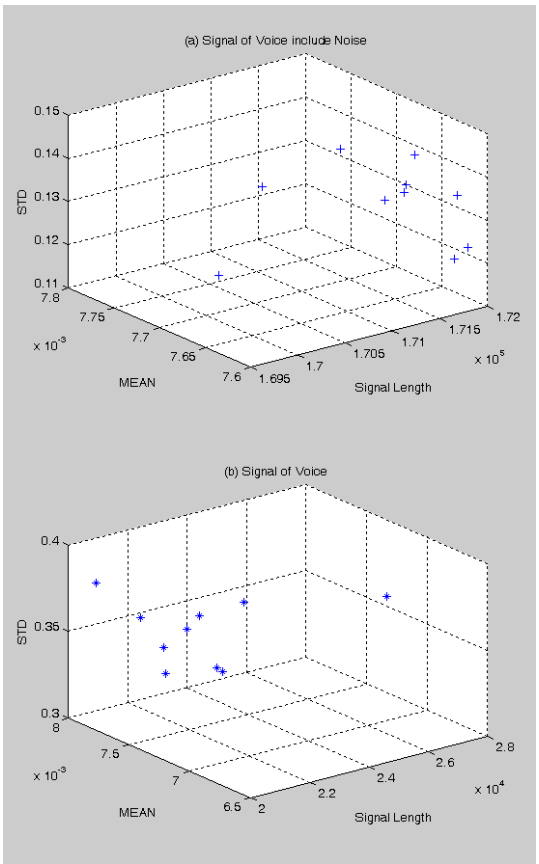

그림 6. Voice만을 포함한 DataSets과 Voice와 Noise를 포함한 DataSets의 3D Plot
Fig. 6 3D plot among signaal length, MEAN, and STD about 2 DataSets

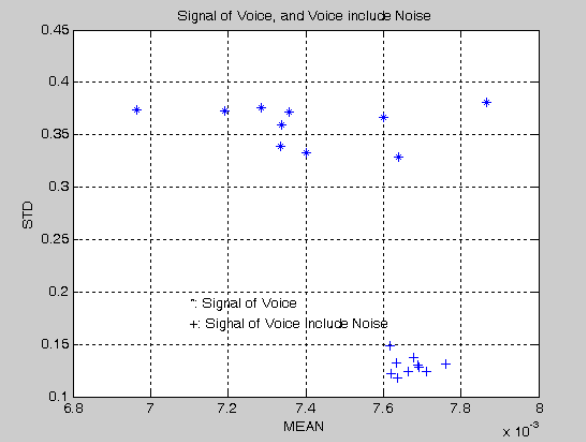

그림 7. 2 개의 DataSets의 MEAN과 STD 측면의 2D Plot
Fig. 7 2D plot between MEAN and STD about 2 DataSets

그림 7은 Voice만을 포함한 DataSet과 Voice와 Noise를 포함한 DataSet의 MEAN과 STD 측면의 2D Plot을 나타냈으며, 좀더 세밀하게 분석 및 파악할 수 있다. 그림 8과 그림 9는 User A, B, C, D, 그리고 E의 Voice와 Noise를 포함한 DataSet 분포와 User A, B, C, D, 그리고 E의 Voice만 포함한 DataSet 분포를 나타낸 것이다. 그림 8과 그림 9를 비교하면 그림 9의 User A, B, C, D 그리고 E의 5명의 DatSet 분포가 그림 8의 분포보다 패턴들의 평균값은 감소하였지만, MEAN과 STD 측면에서 훨씬 더 넓게 분포되어 있음을 확인할 수 있다.

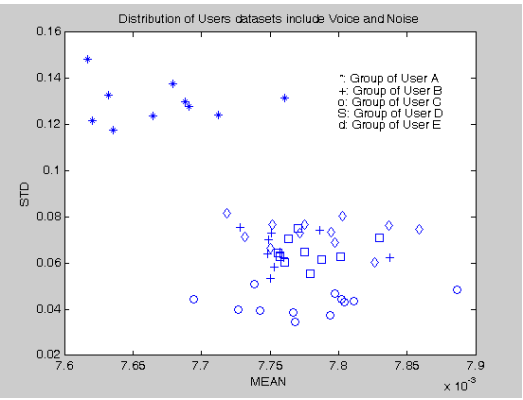

그림 8. User A ~ D, 그리고 E의 Voice와 Noise를 포함한 DataSets 분포
Fig. 8 DataSets distribution of user A ~ D, and E's voice and noise

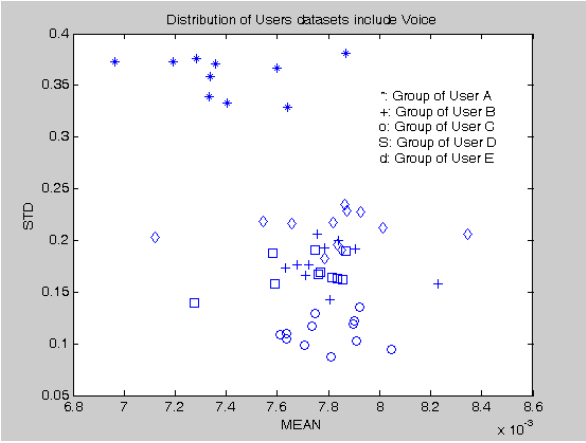

그림 9. User A ~ D, 그리고 E의 Voice만 포함한 DataSets 분포
Fig. 9 DataSets distribution of user A ~ D, and E's voice

Ⅳ. 시뮬레이션

4-1 카오스 신호 vs. Voice 신호

카오스의 구성요소는 초기치와 그의 전개 양상을 결정짓는 전개함수의 모양이다. 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 10는 카오스 방정식에 의해서 임의적으로 무작성을 갖는 패턴을 생성할 수 있으나, Mu와 초기치를 알면 반복적인 계산에 의해서 패턴을 추적가능하게 된다. 특히 그림 10의 (a), (c) 그리고 (e)는 Mu 값의 변화에 따른 진폭과 반복된 계산 결과를 나타낸 것이며, 그림 10의 (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 11은 User A의 Voice의 Signal과 히스토그램을 나타냈으며, 분포가 정규분포적인 형태를 보였다. 그림 11에 나타낸 잡음을 제거

한 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.

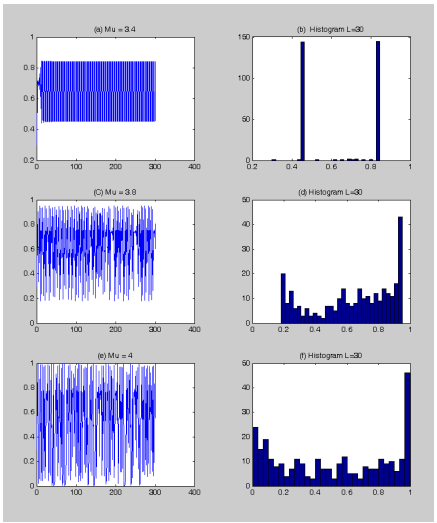

그림 10. 카오스 방정식에 의한 Mu 값의 변화에 따른 생성된 Signal과 히스토그램
Fig. 10 Signal and histogram according to variance Mu value by chaos equation

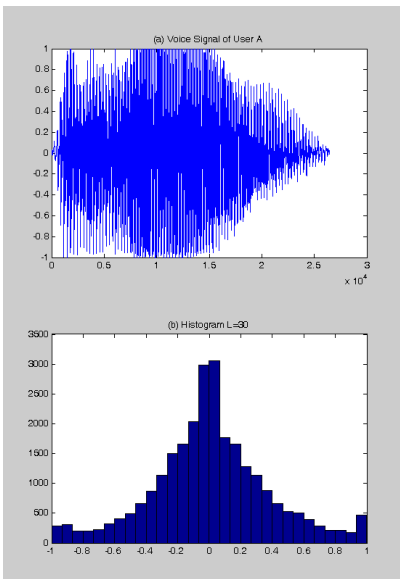

그림 11. User A의 Voice의 Signal과 히스토그램
Fig. 11 Signal and histogram of user A's voice

4-2 무작위성

덴드로그램(Dendogram)은 Bio-Information의 게놈 프로젝트에서 유전자들 간의 거리를 측정하는 도구로 많이 사용된다. User A의 "Hello"라는 음성을 10번 샘플링한 DataSet을 음성만 포함한 DataSet과 음성과 백색 잡음을 포함한 DatSet으로 구분하여 덴드로그램으로 나타냈다.

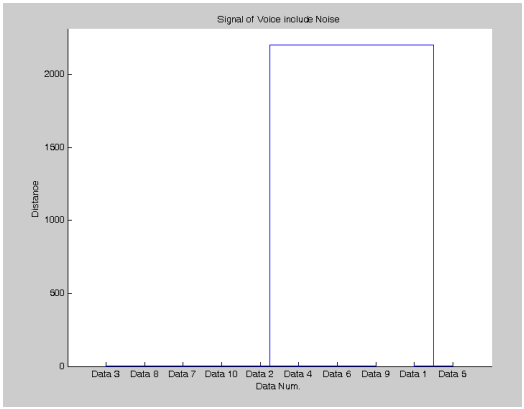

그림 12. User A의 Voice와 Noise를 포함한 Dataset의 덴드로그램
Fig. 12 Dendrogram of Dataset include user A's voice and noise

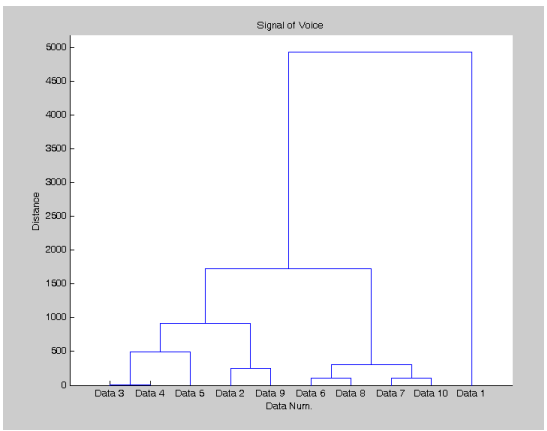

그림 13. User A의 Voice만 포함한 Dataset의 덴드로그램
Fig. 13 Dendrogram of Dataset include user A's voice

그림 12는 User A의 음성과 잡음을 포함한 DataSet의 10개 샘플링들 간의 덴드로그램을 나타냈으나, Distance가 500 이상을 기준으로 2개의 그룹으로 나눌 수 있으며, 그룹은 1은 8개의 샘플링이 그룹 2는

2개의 샘플링으로 구성되었다. 각각의 그룹에서의 Distance는 100이 넘지 않아서 각 샘플들이 근소한 차이에 의해서 밀집되어 있다고 할 수 있다. 그림 13은 User A의 음성에서 잡음을 제거하여 10개의 샘플링을 비교하였다. Distance 500을 기준으로 5개의 그룹으로 나눌 수 있으며, Distance 1000을 기준으로 3개의 그룹으로 나누어진다. 그림 12와 그림 13을 비교하면 잡음은 샘플링된 음성 신호의 특성을 제거하는 단점을 갖음을 알 수 있다. 그림 12는 DataSet에서 샘플링된 음성들 간의 가장 큰 Distance은 2000을 기준으로 하고 있으나, 그림 13은 가장 큰 Distance를 5000을 기준으로 하고 있다. 결과적으로 음성 샘플링에서 잡음을 제거하면 샘플링된 음성들간의 정밀한 특징 패턴을 갖고, 더불어 Distance 측정으로 무작위성이 커짐을 확인할 수 있다.

4-3 카오스와 음성에 의한 키 생성

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

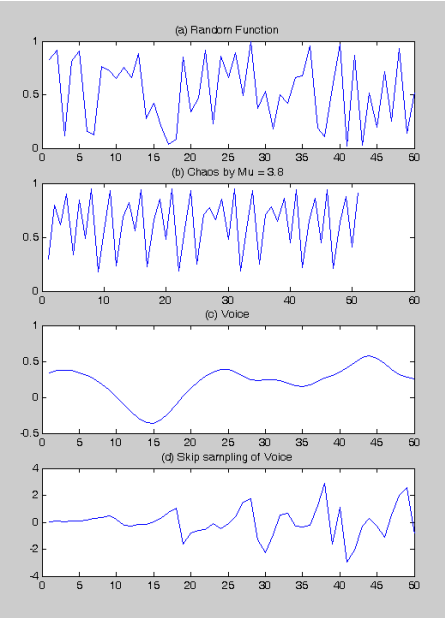

그림 14. Random 함수, 카오스 신호, 음성 신호, 그리고 일정한 간격의 음성 신호 샘플링 결과
Fig. 14 Sampling results of random function, chaos signal, voice signal, and skipped voice signal

그림 14는 무작위(Random) 함수와 카오스 신호, 음성 신호, 그리고 일정한 간격의 음성 신호를 샘플링한 것을 나타낸 것이다. 그림 14의 신호들을 이용한 키를 만들기 위해서는 키 공간에서의 키들의 확산 정도를 측정하여야 한다. 이를 위한 여러 방법 중에서 간단하게 생성된 키들의 분포를 검사하여 비교 분석한다. 그림 15는 무작위 함수와 카오스 신호, 음성 신호, 그리고 일정한 간격의 샘플링한 음성 신호들의 분산과 평균을 나타내고 있다. 1차 평가로 네 가지 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 확산 정도를 비교할 수 있다. 그림 15의 평균에서 일정한 간격의 샘플링한 음성 신호가 또한 평균값도 상대적으로 작아서 확산 정도가 다른 신호들에 비해서 큼을 나타내었다.

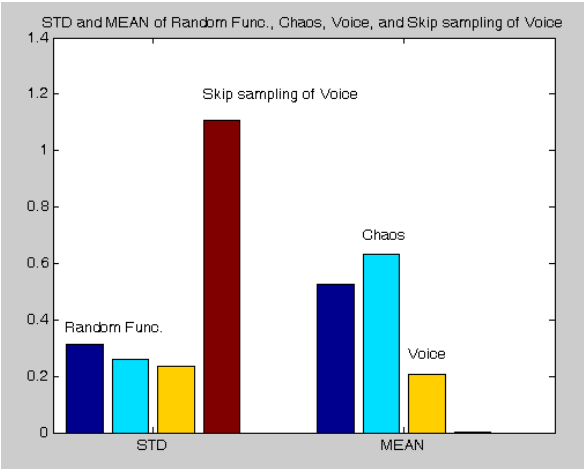

그림 15. 각 신호들의 분산과 평균
Fig. 15 Variance and Mean of each signals

V. 결 론

모바일 및 유비쿼터스의 광범위한 응용과 더불어 통신 보안 분야는 더욱 중요한 관심사가 되고 있으며, 정보 시스템의 대부분이 개방형 유무선 네트워크이기 때문에 악의의 공격자에 의한 다양한 형태의 공격에 대해 취약하다. 근래에는 온라인 및 모바일 마켓의 개념이 전통적인 오프라인 산업의 마켓까지 확

대되고 있어, 유무선 통신 시스템에 대한 악의적 공격 피해에 대한 방어 및 복구에 대한 중요성이 커지고 있다. 따라서 정보통신 시스템의 보안 측면에 대한 다양한 분야에서 연구가 진행되고 있으며, 인증과 암호화 기법은 보안에 가장 많이 사용되는 방법이다. 본 논문에서는 모바일 기반의 음성을 이용한 OTP를 생성하는 방법을 제안하였으며, 이를 임의의 사용자 5명으로부터 음성을 샘플링하여 제안된 방법으로 시뮬레이션을 수행하였으며 녹취된 음성 정보로부터 잡음을 제거함으로써, OTP를 위한 키 생성에 우수하다는 것을 증명하였다.

감사의 글

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

2. 본 논문은 “미래인터넷 인프라를 위한 가상화 지원 프로그래머블 플랫폼 및 핵심원천 기술개발” 과제 (2009-F-050-01)에 대한 결과물중 일부분입니다.

3. 본 연구는 호남대학교 교내학술연구지원사업에 의하여 수행된 연구결과입니다.

참 고 문 헌

[1] Android Market, http://www.android.com/market/

[2] 이대종외, “홍채와 음성을 이용한 고도의 개인 확인시스템‘, *퍼지및지능시스템학회논문지 2003,* Vol 13. No.3. pp348-354

[3] Gish. H. and Schmidt. M., "Text-independent speaker identification", *IEEE Signal Processing Magazine*, pp. 18-32, Oct. 1994.

[4] Douglas A. Reynolds, "An overview of automatic speaker recognition technology", pp.4072-4075, Vol. Ⅳ., ICASSP 2002.

[5] 한국정보통신기술협회, “생체정보보호를 위한 가이드라인”, *정보통신단체표준*, 2005.12. pp2-4

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

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

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

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

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

[11] SecureID, http://www.rsa.com/

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

차 병 래 (車炳來)

2004년 2월 : 국립 목포대학교 컴퓨터공학과(공학박사)
2005년 3월 ~ 2009년 2월 : 호남대학교 컴퓨터공학과 전임강사
2009년 9월~현재 : 광주과학기술원(GIST), 고성능컴퓨팅협업환경 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 (김종원)

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“