

지문 특징을 이용한 모바일 일회용 암호키 및 시뮬레이션

An Mobile-OTP(One Time Password) Key and Simulation using Fingerprint Features

차병래*, 김용일**

Byung-Rae Cha*, Yong-Il Kim**

요 약

인터넷 및 유비쿼터스의 광범위한 응용과 더불어 인터넷 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 지문의 특징을 이용한 모바일 OTP의 일회용 암호 키를 생성하는 방법을 제안한다. 본 연구는 잘 알려진 강력한 개인 인증요소인 지문 정보를 이용하여 가변적이고 안전한 일회용 암호 키를 생성하였으며, 또한 제안 기법에 대한 dendrogram을 이용한 지문 특징점의 준동형 그래프간의 가변성 그리고 지문 특징점의 분포를 시뮬레이션을 통해 성능을 분석하였다.

Abstract

As the applications within Internet and Ubiquitous becoming more extensive, the 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 fingerprint features in order to generate Mobile One Time Passwords(OTPs). Fingerprint is considered to be one of the powerful personal authentication factors and it can be used for generating variable passwords for one time use. Also we performed a simulation of homomorphic graph variable of fingerprint feature point using dendrogram and distribution of fingerprint feature points for proposed password generation method.

Key words : Mobile-OTP, Fingerprint Features

I. 서 론

인터넷 및 유비쿼터스의 광범위한 응용과 더불어 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 확대되고 있어, 정보 시스템에 대한 악의적 공격 피해에 대한 방어 및 복구에 대한 중요성이 커지고 있다. 악의의 행위를 방지하기 위한 보안 시스템은 어느 한부분의 취약점으로 전체 정보 시스템의 완결성에 치명적

* 조선대학교 정보통신공학과

** 호남대학교 인터넷소프트웨어학과

· 제1저자 (First Author) : 차병래

· 투고일자 : 2009년 7월 7일

· 심사(수정)일자 : 2009년 7월 8일 (수정일자 : 2009년 8월 3일)

· 게재일자 : 2009년 8월 30일

인 결과를 발생하게 된다. 정보 시스템 각각의 보안 요소마다 다양한 기법 및 응용에 대한 연구와 시스템적 응용에 대한 연구가 필수적으로 융합되어 이루어져야 있다. OTP는 사용자 인증에서 출발하여 좀 더 강력한 인증을 제공하는 개방형 네트워크 환경의 1차적인 보안 방법이었으나, 모바일 환경에서 한 차원 더 발전시켜 강력한 사용자 인증을 제공하는 방법으로 모바일 OTP가 연구 및 실현 단계에 도달하고 있다. 대부분의 경우 사용자 인증은 사용자 ID와 비밀번호 기반으로 이루어지고 있다. 이것은 아이디와 비밀번호 방식이 시스템적으로 가장 간단하며, 사용자 측면에서도 외우기 쉬운 정보로 설정하거나 고정된 비밀번호를 사용하는 편리성 때문이다. 하지만 이러한 방식은 사회공학을 이용한 악의적 공격에 쉽게 노출될 수 있다는 문제점이 있다. 특히 도청에 의해서 쉽게 노출될 가능성이 높기 때문에 악의적인 공격자가 이를 이용하여 정당한 사용자로 위장할 수 있다[1, 2]. 일회용 패스워드 기술(OTP: One Time Password)은 이러한 단점을 극복할 수 있는 인증 기법이다[3, 4, 5]. OTP는 매번 새로운 패스워드를 생성함으로써 아이디와 비밀번호 기반 방식의 문제점을 보완하고 있다. 이러한 OTP는 주로 인터넷 뱅킹에서 사용되어 왔으나, 최근에는 온라인상의 다양한 형태의 상거래에서 활용 및 모바일 환경으로 전환되고 있다.

본 논문에서는 지문의 특징을 이용한 모바일 OTP의 일회용 암호 키를 생성하는 방법을 제안한다. 본 연구는 잘 알려진 강력한 개인 인증요소인 지문 정보를 이용하여 가변적이고 안전한 일회용 암호 키를 생성하였으며, 또한 제안 기법에 대한 시뮬레이션을 통해 성능을 분석하였다. Dendrogram을 이용한 지문 특징점의 준동형 그래프간의 가변성을 측정하였으며, 지문 특징점의 변화에 따른 고정 및 변화를 보인 특징점의 분포를 분석하였다.

II. 관련연구

2-1 지문 및 지문스캔 모바일 장치

생체인식(Biometrics)은 인간의 생리적, 행동 양식

적 특징을 기반으로 하여 인간을 인식하는 자동화된 방법이며, 특정 개인의 특성을 인증하거나 신분을 인식하기 위해, 측정 가능한 특성 또는 개인의 특징을 연구하는 분야이다[6,7]. 실제로 사람은 누구나 독특 하면서 변하지 않는 지문을 가지고 있으며, 지문은 손가락 표면의 융기 부분과 고랑 부분으로 이루어져 있다. 지문은 루프와 소용돌이 그리고 궁상문(arch)들을 포함하는 많은 수의 키 패턴에 의해 분류될 수 있다. 지문의 특징은 특징점(Minutiae Point) 및 요철의 형태에 의해 결정된다. 여기서 특징점이란 융기부분의 분기점이나 끝점에 생긴 국소적인 특징을 말한다 [8,9]. 지문을 비교하기 위한 가장 확실한 방법은 지문의 모든 영상 정보를 전부 비교하는 것이다. 그러나 현실적으로 이것은 불가능하다. 영상 정보를 전체적으로 비교하기 위해서는 그만큼 처리해야 할 자료의 양이 많아지게 되어 상용화된 시스템을 만들기에는 부적절하다. 실제로 상용화된 시스템을 보면, 지문의 영상을 그대로 저장하는 대신 영상의 특징점들의 위치와 관련된 코드를 저장한다. 특징점만을 저장하기 때문에 나중에 지문영상으로 복원할 수 없어 범시행 기관들에 의한 증명 방법으로는 사용될 수 없다 [6].

모바일 환경에서의 OTP를 지원하기 위해서는 하드웨어적인 측면도 고려해야만 하며, 대표적인 예로는 그림 1과 같은 LG전자와 레노보의 지문인식기가 장착된 핸드폰이 있다.



그림 1. LG전자와 레노보의 지문인식기가 장착된 핸드폰들

Fig. 1. Mobile Devices include Fingerprint Scanner of LG and Lenovo

2-2 OTP와 Mobile-OTP

OTP는 일회에 한해 사용할 수 있는 인증기법으로 매번 다른 비밀번호를 이용하여 사용자를 인증하는 방식이다. 현재의 비밀번호에서 다음의 비밀번호를 유추하는 것을 어렵게 하여 보안성을 높이는 방법이다. OTP는 일정 시간마다 전용 단말기 등에 새로운 비밀번호가 생성되어 시스템에 접근할 때마다 새로운 비밀번호를 입력해야 하기 때문에 해킹이나 사용자의 관리소홀 등으로 비밀번호가 노출되는 것을 방지할 수 있다. 정해진 범위에서 비밀번호를 입력하는 기존의 인쇄된 보안카드에 비해 OTP는 사용자 비밀번호가 노출되더라도 새로 생성된 비밀번호를 입력해야 하기 때문에 훨씬 강력한 보안성을 제공할 수 있다. 대부분의 모든 OTP 생성 알고리즘은 일방향 함수(출력 값을 통해 입력 값을 유추할 수 없는 함수)에 기반을 두고 있다. 유닉스(UNIX) 운영체제(OS)에 구현되어 있는 S/Key 시스템(RFC1760)이 그 예이다 [3,5]. OTP는 IETF에 의해서 표준화 되었으며, 그 후에는 인증관련 업체에서 표준화를 주도하고 있으며 대표적으로 RSA[10] 진영과 OATH[11] 진영이 경쟁적으로 표준화를 진행하고 있다.

Mobile-OTP는 OTP 전용단말기를 휴대해야 하는 기존 OTP 방식의 단점을 극복하기 위해 사람들이 사용하는 핸드폰에 OTP 모듈을 탑재하여 사용하는 개념이다. 자바 애플릿이 동작되는 휴대전화기 많이 보급되어 있으며, 이러한 자바언어가 가능한 휴대폰이나 PDA와 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, 액세스 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[12], 이니텍의 INISAFE MOBILE OTP[13], RSA의 SecureID[14], 블리자드 모바일인증기[15]가 있다.

III. 지문 특징 정보를 이용한 암호화 키 생성

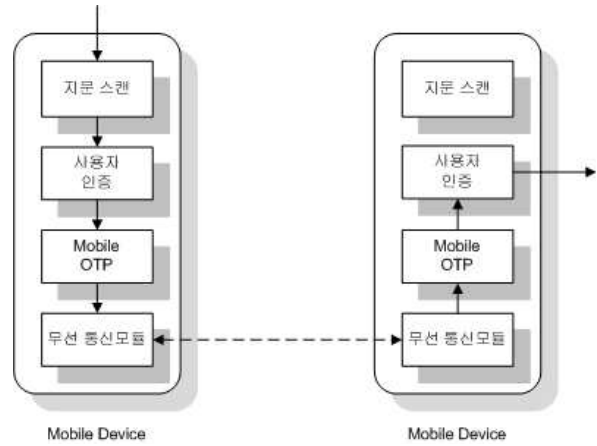


그림 2. 지문 정보를 이용한 모바일의 개인 인증 및 모바일 OTP의 절차

Fig. 2. Procedures of Personal Identification and Mobile-OTP of Mobile using Fingerprint Information

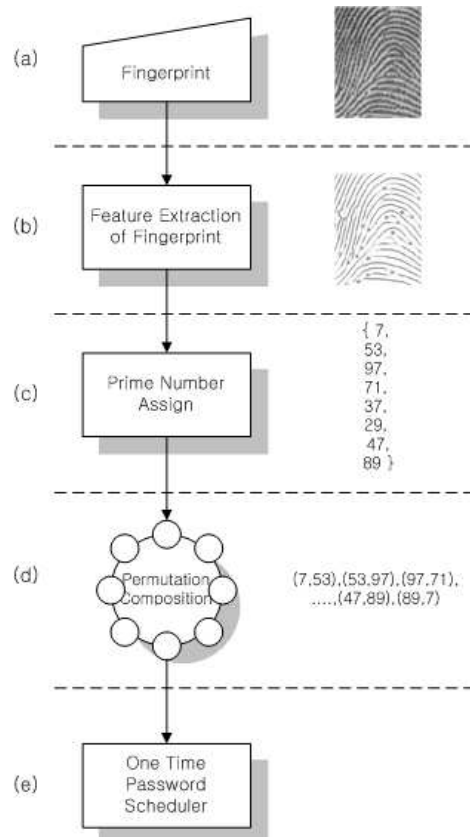


그림 3. 지문 특징점을 이용한 OTP의 암호화 키 생성 과정

Fig. 3. Password Key Generation of OTP using Fingerprint Feature Points

일회용 암호 메커니즘을 구성하는 요소들은 보안/ 암호 알고리즘이 내장된 토큰 혹은 일회용 암호생성기와 인증 서버와 인증 클라이언트로 구성되어 있다. 일회용 암호 메커니즘 역시 프로그램이므로 임의적으로 무작위성을 갖게 프로그램이 되었지만 임의의 시간이 경과됨에 따라 무작위성이 깨지고 예측이 가능하게 되므로, 일회용 암호 메커니즘도 일정기간 단위로 암호화 모듈을 교체해야 하는 단점을 갖게 된다. 이러한 단점을 극복하기 위해서 본 논문에서는 OTP 서버의 암호화 키 모듈을 지문 특징 정보를 이용하여 생성하는 방법을 제안하며, 그림 2는 바이오 매트릭스 정보를 이용한 모바일의 개인 인증 과정에서 모바일 OTP의 절차를 개략적으로 나타내며, 그림 3은 모바일 OTP의 암호화 키 생성 과정을 세부적으로 나타낸 것이다.

그림 3에서 암호화 키 생성 과정을 위해 사용자는 먼저 지문을 스캐닝한다(a). 스캔된 지문은 클라이언트 측의 사용자 지문을 이용하여 특징 정보를 추출한다(b). 추출된 지문의 특징 정보에 의해서 특징점에 임의의 소수를 무작위로 할당하게 된다(c). 할당된 소수를 순서 관계에 의해서 순열 조합을 생성하며(d), 순열을 이용하여 OTP의 패스워드를 생성한다(e). OTP의 암호화 키 생성 모듈은 OTP의 클라이언트 측에 위치하고 있으며, 과정 (d)에서처럼 순열을 이용하여 한 세션에 대해 일시적으로 사용 가능한 무한대의 OTP 패스워드를 생성하게 된다.

3-1 지문을 이용한 특징점 추출

OTP 클라이언트와 서버 개체는 서로 신뢰 관계를 기본으로 한다. 신뢰관계에서 지문 특징 점을 이용하여 예측되거나 편의를 갖지 않는 OTP 패스워드 키를 지원하기 위해서 생체 지문 정보의 공개는 단지 클라이언트 쪽에서 패스워드 키를 생성하는데만 이용될 뿐 지문 정보를 서버 쪽으로 공개되거나 전송되지는 않는다. 클라이언트 쪽으로부터 받은 순열 자료구조의 패스워드 키를 이용하여 지문 정보를 생성할 수 없는 일방향 함수의 성질을 갖는다. 또한 지문의 특징 점만을 저장하기 때문에 나중에 지문영상으로 복원할 수 없다. 본 논문에서는 지문 정보를 완벽하게 지원 하는 것이 아니라, 동일한 지문 정보를 이용해서

편의와 예측 불가능한 많은 패스워드 키를 생성하기 때문에 이론을 떠나서 실제 구현에서도 클라이언트 쪽의 지문 스캐너의 해상도와 지문 이미지의 처리에 의해서 무한한 가변성을 가질 수 있다. 지문의 RGB 이미지를 그레이 그리고 흑백 이미지로 변환 후에 thin 과 skel 세션화 과정 및 세션화 과정의 조합 결과를 통한 지문 이미지 처리에 가변성을 증가시킬 수 있다.

일반적으로 지문의 특징 정보를 이용하여 OTP 암호화키를 생성할 경우, 동일한 지문에 대해 매번 동일한 지문 특징 정보를 갖게 되며 이에 따라 암호화키 또한 동일해진다. 기존의 연구 방법들은 이와 같이 사용자 개인의 지문을 동일한 값으로 인식함에 따라 지문을 OTP를 위한 기반정보로 활용할 수 없게 된다.

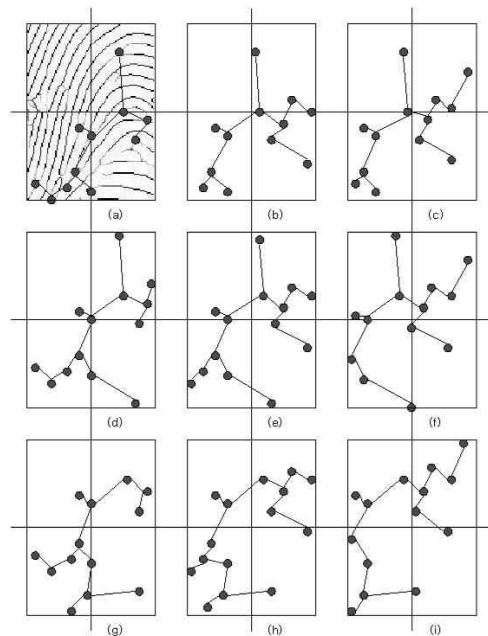


그림 4. 동일한 지문의 위치 변화에 의한 특징점의 변화

Fig. 4. Variant of Fingerprint Feature Point by Changed Location using Same Fingerprint

그림 4와 5는 동일한 지문을 이용하여 우측과 아래쪽으로 3mm씩 이동하여 지문의 특징점 추출과 추출된 특징점을 이용한 준동형 그래프의 변화를 나타낸 것이다. 그림 4의 (b)~(i)까지는 그림 4의 (a)와는 달리 지문 이미지를 제거하여 지문의 준동형 그래프

의 변화를 관찰하기 쉽게 나타낸 것이다. 특징점 그래프의 생성 과정은 스캔화면의 정중앙에서 가장 가까운 노드에서 시작하여 프림 알고리즘으로 MST(Minimum spanning tree) 그래프[16]를 생성하여 나타낸다.

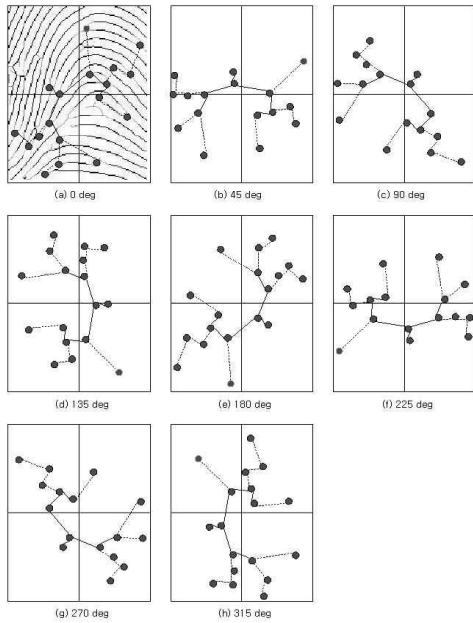


그림 5. 동일한 지문의 각 변화에 의한 특징점의 변화

Fig. 5. Variant of Fingerprint Feature Point by Changed Angle using Same Fingerprint

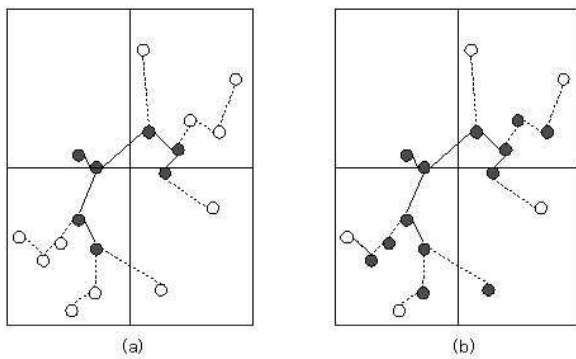


그림 6. 위치와 각변화에 따른 특징점 그래프의 고정된 노드와 변화된 노드

Fig. 6. Fixed and Variant Node of Feature Point Graph by Changed Location and Angle

그림 4와 5를 통해서 동일한 지문도 매번 스캔할 때마다 약간의 차이를 갖게 된다는 것을 알 수 있다. 즉 지문 스캔 시에 동일한 지문에 대해서도 스캐닝되

는 위치(location)와 각(angle)의 변화에 의해서 특징점 추출에 의한 특징점 그래프의 변화를 보이게 되며, 준동형 그래프(Homomorphic Graph)를 생성하게 된다. 이러한 특징을 이용하면 동일한 지문도 매번 스캔 시 특징점 그래프의 변화에 의한 다른 암호화 키를 생성할 수 있게 되어 지문을 OTP에 사용할 수 있게 된다.

그림 6의 (a)는 그림 4의 9장의 이미지를 하나로 만들어 추출한 특징점 그래프를 나타낸 것이며, 그림 6의 (b)는 그림 5의 8장의 이미지를 하나로 만들어 추출한 특징점 그래프를 나타낸 것이다. 특징점 그래프의 검정색의 노드는 특징점 그래프에서 변화를 보이지 않는 부분이며, 흰색의 노드는 위치 변화에 따른 노드의 제거 또는 추가의 변화를 보인 노드를 나타낸 것이다.

3-2 암호화 키 및 순열 생성

지문 특징점을 이용한 그래프 각각의 노드에 임의의 소수를 할당하고 MST 그래프의 탐색 순서에 의해서 순서 관계를 순열로 구성한다. 순열의 암호화 키 생성은 그림 7과 같이 MST 그래프의 시작 노드를 원점으로 그래프의 탐색 순서로 임의적으로 할당된 소수를 이용하여 암호화 키를 생성한다.

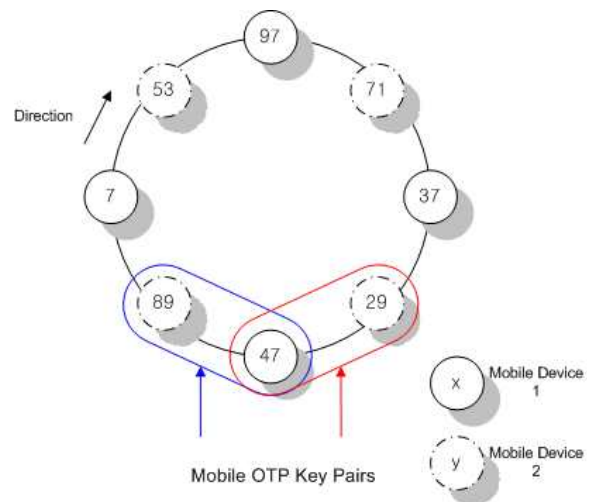


그림 7. 키 순열을 이용한 Mobile-OTP 구성
Fig. 7. Mobile-OTP Composition using Key Permutation

임의로 할당된 한정된 소수의 리스트를 사용하면

한 세션을 이루는 클라이언트와 서버 간의 왕복하는 여러 패킷에 대한 암호화 키가 부족하게 된다. 이러한 단점을 해결하기 위해서는 순열의 특징을 이용하여 하나의 암호화 키 리스트를 순열로 전환시켜서 계속적으로 순환시키면 일시적인 무한대의 암호화 키를 생성할 수 있게 된다. 한 세션이 끝나면 암호화 키를 생성하는 순열을 파기함으로서 다음 세션에는 새로운 순열을 생성하여 사용하므로 보안을 강화시킬 수 있다.

IV. 시뮬레이션

4-1 한 지문의 위치와 각의 변화에 의한 거리 비교

(1) 지문의 위치와 각의 변화

지문 특징점에 의해 생성된 그림 4의 9개의 준동형 그래프를 이용하여 dendrogram[17]과 각각의 노드에 임의의 3자리 난수를 할당하여 dendrogram으로 나타내었다. 이때 dendrogram은 JMSL[18] 라이브러리를 이용하였다.

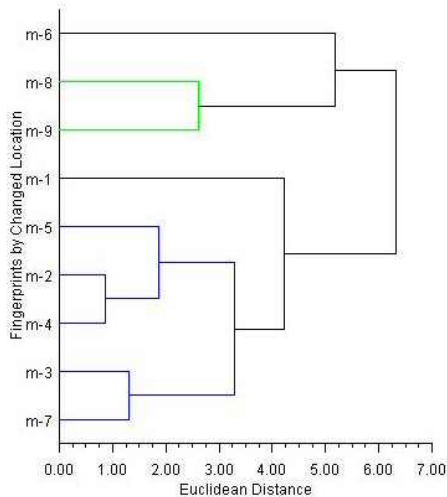


그림 8. 위치(Location) 변화에 대한 지문 그래프의 Dendrogram
Fig. 8. Dendrogram of Fingerprint by Changed Location

그림 8은 위치의 변화에 따른 지문 특징점에 의해

생성된 그림 4의 9개의 준동형 그래프를 이용하여 dendrogram으로 나타내었고, 그림 9는 각의 변화에 따른 지문 특징점에 의해 생성된 그림 5의 8개의 준동형 그래프를 이용하여 dendrogram으로 나타내었다.

그림 8과 9의 dendrogram에 의해서 동일한 지문이지만 유한개의 준동형 그래프 생성으로 무작위성을 가질 수 있음을 알 수 있고 난수 할당에 의해 무작위성과 확산이 확대되었음을 알 수 있다. 이 경우 순열 구성을 이용함으로써 한 세션에 대해 일시적으로 무한개의 암호화 키를 생성할 수 있게 된다.

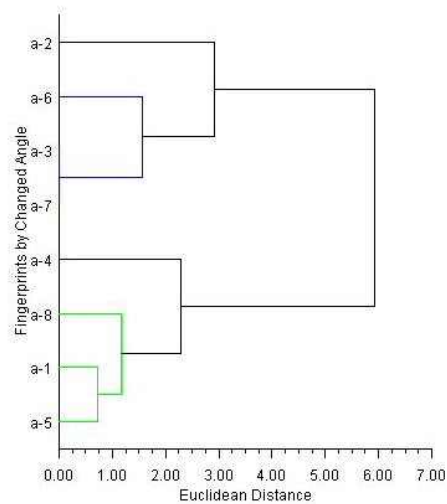


그림 9. 각(Angle) 변화에 대한 지문의 Dendrogram
Fig. 9. Dendrogram of Fingerprint by Changed Angle

(2) 위치와 각을 결합한 변화

그림 6의 (a)와 (b)를 비교하면 위치 변화에 의한 변화된 노드의 수가 11개이며, 각 변화에 의한 변화된 노드는 5개로서 위치 변화가 각 변화보다 더 많은 변화된 노드를 갖는다. 그러나 스캔된 지문을 사사분면으로 나누어서 준동형 그래프의 노드를 분석하면 각의 변화는 변화된 노드의 수는 적지만, 고정된 노드와 변화된 노드의 변화 폭이 큰 것을 인지할 수 있다. 즉 원점으로부터 멀어지면 동일한 각을 움직이더라도 변화된 거리는 더 크기 때문이며, 그 변화를 그림 10에 나타냈다. 그림 10은 위치와 각의 변화를 혼합한 지문 그래프의 Dendrogram으로 나타낸 것이다.

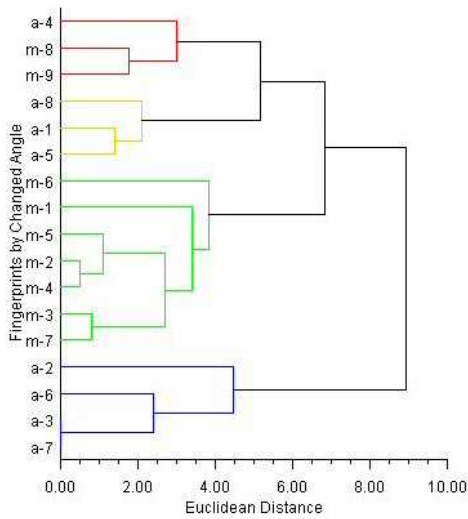


그림 10. 위치와 각의 변화를 혼합한 지문 그래프의 Dendrogram
 Fig. 10. Dendrogram of Fingerprint by Changed Location and Angle

그림 10에 의해서 위치와 각의 변화에 따른 무작

위한 변화를 가질 수 있음을 보여주고 있다. 이에 따라 동일한 지문이라도 매번 스캔하면 위치와 각에 의해서 임의의 무작위를 가질 수 있으며, 이러한 특징에 의해서 OTP의 암호화 키 생성에 사용할 수 있다. 지문 특징점의 거리 및 변화를 측정함으로써 지문 특징점을 이용한 OTP 시스템의 불편의성을 측정할 수 있다. 지문 특징점이 불편의성을 가지고 있어 매번 동일한 지문을 이용한 패스워드 생성시 동일한 패스워드가 생성되지 않음을 보여주게 된다. 이러한 점은 OTP의 패스워드 생성 측면의 비용이 매우 절감되는 장점이 된다.

4-2 지문 샘플이미지의 위치변화에 따른 특징 변화 측정

지문 샘플 데이터 30개를 이용하여 위치 변화에 따른 지문 특징점의 준동형 그래프를 분석하였다. 그림 11은 샘플 지문 이미지의 위치 변화에 따른 지문 이미지의 스캔 영역을 나타낸 그림이다. 가로 축은 지문 샘플 데이터 30개를 나타내며, 세로축은 원본

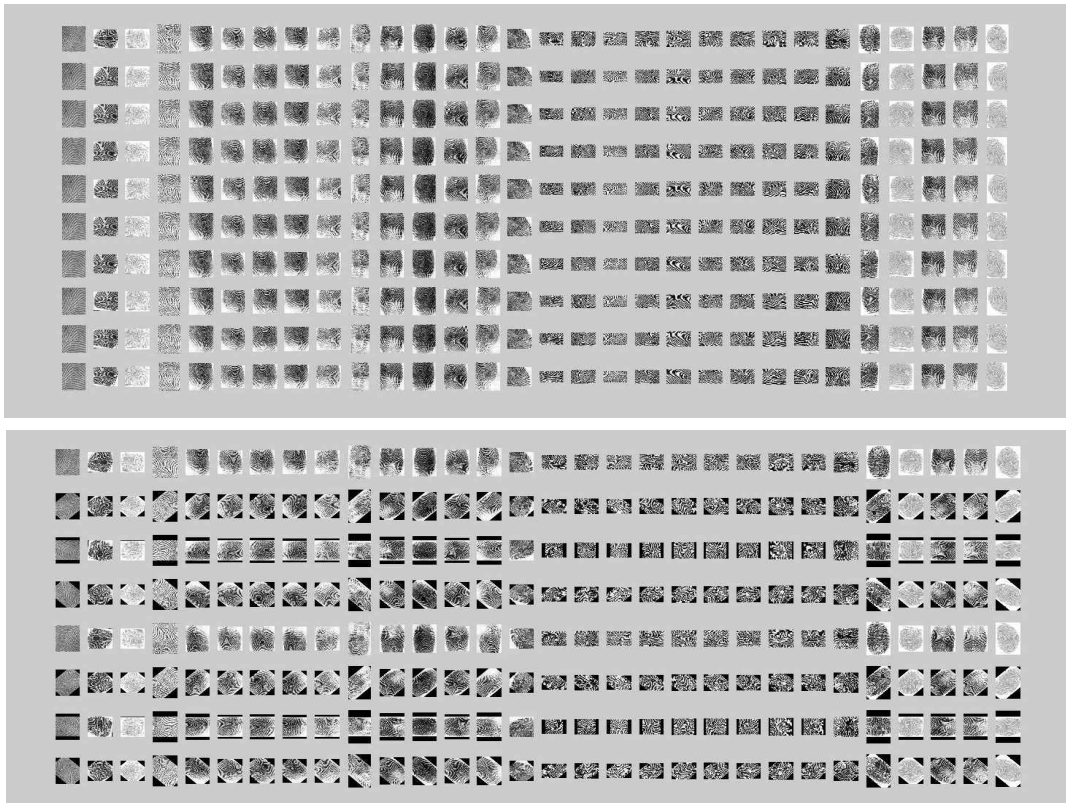


그림 12.] 30개의 샘플 지문 이미지와 각 변화에 따른 각각 8개의 지문 이미지
 Fig. 12. 30 Sample Fingerprint Image and 8 Fingerprint Images by changed Angle

지문과 위치변화에 의한 9개의 스캔된 샘플 지문 이미지를 나타낸 것이다.

그리고 그림 12는 샘플 지문 이미지의 각 변화에 따른 지문 이미지의 스캔 영역을 나타낸 그림이다. 가로 축은 지문 샘플 데이터 30개를 나타내며, 세로 축은 원본 지문과 각 변화에 의한 8개의 스캔된 샘플 지문 이미지를 나타낸 것이다. 30개의 샘플 지문 이미지의 위치 변화에서 추출된 특징 수는 최소 15개와 최대 34개가 추출되었으며, 표 1과 같은 분포를 보였다. 그리고 30개의 샘플 지문 이미지의 각 변화에서 추출된 특징 수는 최소 15개와 최대 35개가 추출되었으며, 표 2와 같은 분포를 보였다.

샘플 지문 데이터의 위치와 각 변화에 따른 지문 특징점의 준동형 그래프의 고정된 특징점의 비율에 대한 최소/최대값은 각각 12%/83%와 50%/88%이었다. 또한, 변화된 특징점의 비율에 대한 최소/최대값은 각각 17%/88%와 12%/50%이었다. 위치 변화에 따른 고정 및 변화된 특징점의 평균은 52.1%와 47.9%이며, 표준편차는 22.8328%와 22.8328%이었으며, 각 변화에 따른 고정 및 변화된 특징점의 평균은 69.57%와 30.43%이며, 표준편차는 9.3833%와 9.3833%이었다. 위 시뮬레이션의 결과는 하나의 지문을 스캔한 지문 이미지에 대해서 위치 및 각 변화에 따른 준동형 그래프를 생성하였으며, 그 결과를 순열을 이용하여 일시적으로 무한대의 암호화 키를 생성할 수 있음으로 보였다. 이러한 특징 때문에 OTP 시스템에 사용될 수 있는 유효성을 시뮬레이션 하였다.

4-3 지문 샘플이미지의 최소 특징점과 최대 특징점 간의 비교

지문 샘플이미지의 특징점들은 크게 고정된 특징점과 변화를 갖는 특징점으로 구분된다. 표 1과 표 2에서 30개의 샘플중 지문 이미지 2번은 가장 많은 34(31, 4)개의 지문 특징점을 갖으며, 지문 이미지 7번은 가장 적은 15(12, 3)개의 지문 특징점을 갖고 있다. 그림 13은 위치 변화에 따른 지문 특징 점의 고정 패턴과 변화된 패턴을 나타낸 것이다. 특징 패턴으로 표현하기 위한 최소 값은 고정된 특징점으로 사

용하고 최대 값은 고정된 특징점과 변화된 특징점의 합의 값으로 표현할 수 있다. 그러나 지문 특징점을 패턴으로 변환하면 고정된 특징 점과 변화된 특징 점의 합보다는 분명히 같거나 작을 것이다. 그러므로 지문 샘플 이미지들의 최소 값과 최대 값 그리고 최적 값을 그림 14에 Errorbar 형태로 나타냈다.

표 1. 위치 변화에 따른 고정 및 변화를 갖는 지문 특징의 분포

Table 1, Distribution of fixed and variant Fingerprint features by changed Location

지문 번호	특징점 수	고정된 특징점 수	변화된 특징점 수	비율 (%)	비고
1	25	9	16	36:64	
2	34	18	16	53:47	*
3	29	20	9	69:31	
4	23	11	12	48:52	
5	17	12	5	71:29	
6	16	10	6	63:37	
7	15	12	3	80:20	*
8	18	13	5	72:28	
9	21	15	6	71:29	
10	17	12	5	71:29	
11	24	14	10	58:42	
12	22	15	7	68:32	
13	20	15	5	75:25	
14	18	15	3	83:17	*
15	21	15	6	71:29	
16	28	5	23	18:82	
17	17	4	13	24:76	
18	19	6	13	32:68	
19	24	7	17	29:71	
20	26	21	5	81:19	
21	22	7	15	32:68	
22	19	8	11	42:58	
23	25	3	22	12:88	*
24	28	5	23	18:82	
25	24	6	18	25:75	
26	18	5	13	28:72	
27	15	11	4	73:27	
28	20	13	7	65:35	
29	17	12	5	71:29	
30	17	4	13	24:76	

표 2. 각 변화에 따른 고정 및 변화를 갖는 지문 특징의 분포

Table 2. Distribution of fixed and variant Fingerprint features by changed Angle

지문 번호	특징점 수	고정된 특징점 수	변화된 특징점 수	비율 (%)	비고
1	26	17	9	65:35	
2	35	31	4	88:12	*
3	30	21	9	70:30	
4	23	14	9	61:39	
5	17	13	4	76:24	
6	16	10	6	63:37	
7	15	12	3	80:20	*
8	18	14	4	78:22	
9	21	14	7	67:33	
10	17	9	8	53:47	
11	24	16	8	67:33	
12	22	14	8	64:36	
13	20	16	4	80:20	
14	18	9	9	50:50	*
15	20	14	6	70:30	
16	28	19	9	68:32	
17	17	10	7	59:41	
18	19	14	5	74:26	
19	24	17	7	71:29	
20	25	15	10	60:40	
21	23	14	9	61:39	
22	19	16	3	84:16	
23	25	19	6	76:24	
24	28	20	8	71:29	
25	24	18	6	75:25	
26	18	11	7	61:39	
27	15	12	3	80:20	
28	20	17	3	85:15	
29	17	11	6	65:35	
30	17	11	6	65:35	

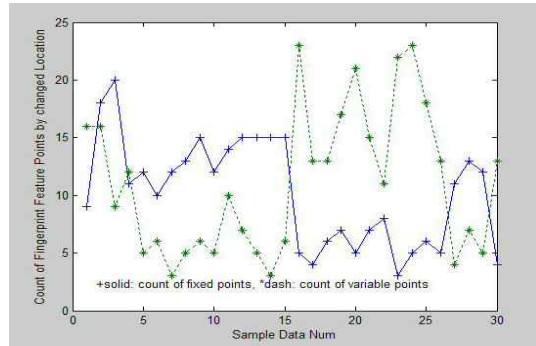


그림 13. 30개 샘플 지문 데이터의 위치(Location) 변화에 대한 고정 패턴(파랑)의 수와 변화를 가는 특징 패턴(초록)의 수

Fig. 13. Counts of Fixed(Blue) and Variant(Green) Pattern of Fingerprint by Changed Location

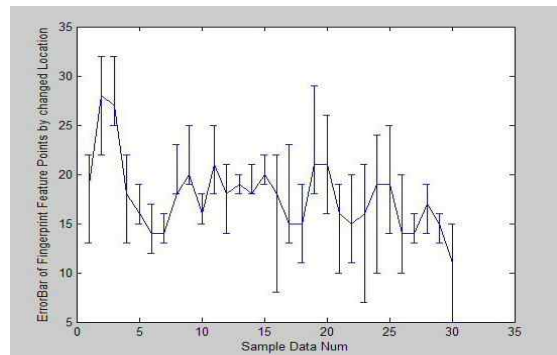


그림 14 30개 샘플 지문 데이터의 위치(Location) 변화에 대한 고정된 특징 패턴과 변화된 특징 패턴 간의 관계

Fig. 14. Relation of Fixed and Variant Feature Pattern of 30 Sample Fingerprint by Changed Location

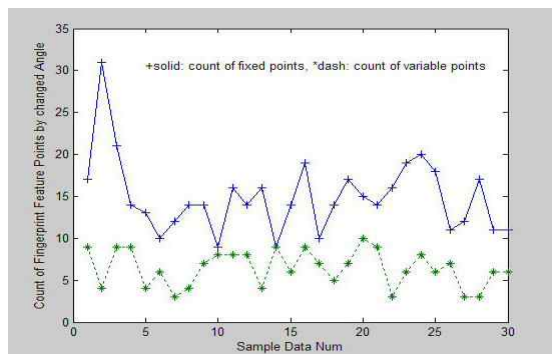


그림 15. 30개 샘플 지문 데이터의 각(Angle) 변화에 대한 고정 패턴(파랑)의 수와 변화를 가는 특징 패턴(초록)의 수

Fig. 15. Counts of Fixed(Blue) and Variant(Green) Pattern of Fingerprint by Changed Angle

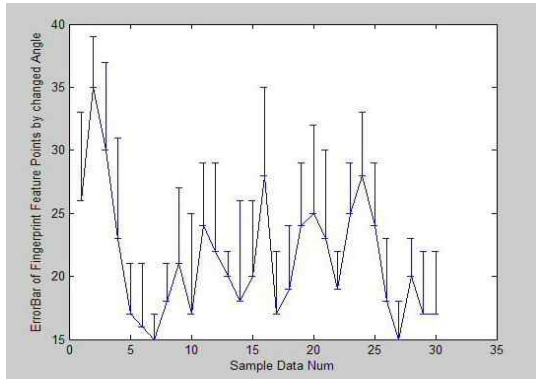


그림 16. 30개 샘플 지문 데이터의 각(Angle) 변화에 대한 고정된 특징 패턴과 변화된 특징 패턴 간의 관계

Fig. 16. Relation of Fixed and Variant Feature Pattern of 30 Sample Fingerprint by Changed Angle

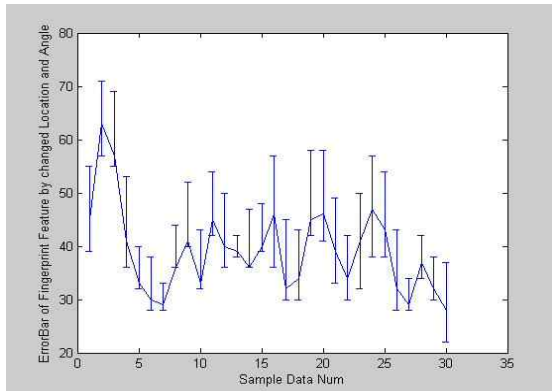


그림 17. 30개 샘플 지문 데이터의 위치(Location)과 각(Angle) 변화에 대한 고정된 특징점과 변화된 특징점 그리고 특징 패턴 간의 관계

Fig. 17. Relation of Fixed and Variant Feature Pattern of 30 Sample Fingerprint by Changed Location and Angle

그림 15는 각 변화에 따른 지문 특징 점의 고정 패턴과 변화된 패턴을 나타낸 것이며, 지문 샘플 이미지들의 최소 값과 최대 값 그리고 최적 값을 그림 16에 Errorbar 형태로 나타냈다.

그림 17은 위치와 각 변화를 Errorbar로 나타내었으며, 그림 14와 그림 16 보다 더 많은 변화의 범위를 포함하고 있다. 그림 18의 (a)는 위치 변화와 각 변화에 의한 극좌표를 나타내며, 그림 18의 (b)는 위치와 각 변화를 결합한 극좌표를 나타낸다.

V. 공개키 암호화를 이용한 Mobile-OTP의 키 순환 순열 전송

공개키(public key) 암호화는 두 개의 공개키와 개인키를 사용한다. 한 개는 암호화에 쓰이는 공개키이고, 또 하나는 복호화에 쓰이는 개인키이다. 모바일 디바이스 1은 모바일 디바이스 2의 공개키로 Mobile-OTP의 패스워드 순환순열을 암호화하여 서버로 전송한다. 서버는 전송받은 암호화된 Mobile-OTP의 키 순환 순열(Key Permutation Cyclic)을 개인키로 복호화를 수행한다. 공개키 암호화의 특성에 의해서 공개키를 안다고 해서 비밀 키를 알아낼 수 있는 것은 아니므로, 공개키는 아무한테나 알려져도 상관이 없다. 서버만이 개인키를 이용해서 복호화할 수 있으므로 전자서명의 기능도 갖을 수 있으며, 그림 19에 나타낸다.

VI. 결 론

인터넷 및 유비쿼터스의 광범위한 응용과 더불어 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 확대되고 있어, 인터넷 시스템에 대한 악의적 공격 피해에 대한 방어 및 복구에 대한 중요성이 커지고 있다. 따라서 정보 시스템의 보안 측면에 대한 다양한 분야에서 연구가 진행되고 있다. 인증은 보안에 가장 많이 사용되는 방법이다. 그 중에서 지문은 인증을 위한 안전한 정보라 할 수 있으며 OTP는 인증에서 활용할 수 있는 안전하고 효율적인 기법이다. 하지만 기존의 연구 방법에서는 지문이 가진 특징으로 인해 이를 OTP에 활용할 수 없었다.

본 연구에서는 지문을 이용한 Mobile-OTP의 암호화 키 생성 기법을 제안하고 시뮬레이션 하였다. 본 연구의 시뮬레이션에서는 하나의 지문에 대한 9개의 위치 변화와 8개의 각 변화를 갖는 30개의 샘플 지문의 준동형 그래프를 이용하여 고정 및 변화된 지문 특징점에 따른 변화를 측정했다.

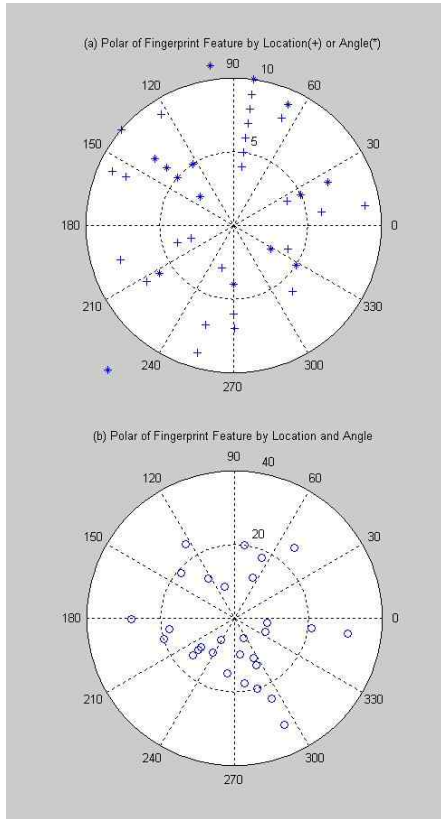


그림 18. 위치, 각, 그리고 위치와 각의 변화를 나타낸 지문 특징의 극좌표
 Fig. 18. Polar Coordinates of Fingerprint Feature Variant by Changed Location, Angle, and Location & Angle

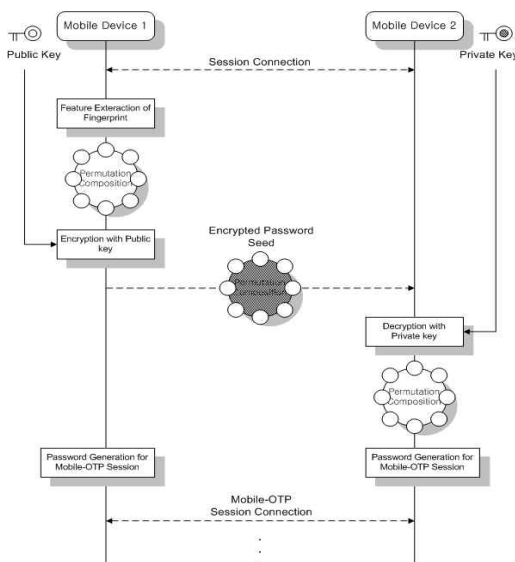


그림 19. 공개키 암호화를 이용한 Mobile-OTP의 키 순환 순열의 전송
 Fig. 19. Transmission of Key Permutation Cycle of Mobile-OTP using Public Crypto-System

측정된 자료가 얼마나 무작위성을 갖는지를 분석하였으며 평균 52.1%와 47.9%의 변화를 가짐을 보였다. 또한 시뮬레이션 결과에 의해서 제안 기법을 통해 지문을 Mobile-OTP에 활용할 수 있음을 입증하였다.

참 고 문 헌

[1] Ed Tittel, Mike Chapple, James Michael Stewart, "CISSP : Certified Information Systems Security Professional", Sybex, 2003.
 [2] Rolf Oppliger, "Security Technologies for the World Wide Web", Artech House, 2000.
 [3] Neil Haller, "The S/KEY One-Time Password System", *Proceedings of the Symposium on Network and Distributed System Security*, 1994.
 [4] A.D. Rubin, Independent One-Time Passwords, Proc. 5th UNIX Security Symposium, USENIX Association, June 1995.
 [5] N. Haller, C. Matz, P. Nesser, M. Straw, "A One-Time Password System", *RFC 2289*, IETF, 1998.
 [6] 바이오메트릭스(Biometrics)의 이해, <http://ics1.mk.co.kr/file/cd104/biometrics1.pdf>
 [7] Pankanti, S., Bolle, R. M., and Jain, A., "Biometrics: The Future of Identification". *IEEE Computer magazine*, February, 2000.
 [8] L. Hong, A. K. Jain, "Classification of Fingerprint Images", *MSU Technical Report, MSU Technical Report MSUCPS:TR98-18*, June 1998.
 [9] Jain, A., and Pankanti, S., "Fingerprint Classification and Matching". *Handbook for Image and Video Processing*, A. Bovik (ed.), Academic Press, April 2000.
 [10] RSA, <http://www.rsa.com>
 [11] OATH, <http://www.openauthentication.org>
 [12] U-OTP, <http://www.u-otp.co.kr/>
 [13] INISAFE MOBILE OTP, http://www.initech.com/www/html/inisafe/goMenu3_5_1.html

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

[15] 블리자드 모바일인증기, <http://www.blizzard.co.kr/>

[16] 박봉구, 한상언, 차병래, “컴퓨터를 활용한 이산수학”, 경문사, 2003.

[17] <http://en.wikipedia.org/wiki/Dendrogram>

[18] JMSL, <http://www.vni.com/products/imsl/jmsl.html>

[19] 차병래, 특허등록: 10-0806365, “지문의 구조적 정보를 이용한 암호화 시드 생성 시스템 및 방법”, Feb. 15. 2008.

[20] 차병래, 고일석, “지문 특징을 이용한 일회용 암호키 생성기법”, *한국전자거래학회지* 제13권 제1호, Feb. 2008.

[21] ByungRae Cha "Password Generation of OTP System using Fingerprint Features", *ISA2008*, April 2008.

[22] ByungRae Cha, KyungJun Kim, HyunShik Na, "Random Password Generation of OTP System using Changed Location and Angle of Fingerprint Features", *CIT2008*, July 2008.

[23] ByungRae Cha, Sun Park, "Design and Efficiency Analysis of New OTP System using homomorphic graph of Fingerprint Features", *ICCIT2008*, November 2008.

[24] 차병래, “지문 특징의 준동형 그래프를 이용한 일회용 암호키 생성기법 및 시물레이션”, *한국정보처리학회논문지* 제15-C권 제6호, 2008년 12월.

[25] Byungrae Cha and Franz I. S. Ko, "Novel OTP System Design using Homomorphic Graph of Fingerprints", *IETE Technical Review*, Vol. 26, Issue 4, Jul-Aug 2009.

차 병 래 (車炳來)



1995년 2월 : 호남대학교 수학과(이학사)

1997년 2월 : 호남대학교 컴퓨터공학과(공학석사)

2004년 2월 : 목포대학교 컴퓨터공학과(공학박사)

2005년 2월 ~ 2009년 2월 : 호남대학교 컴퓨터공학과 전임강사

2009년 3월 ~ 현재 : 조선대학교 정보통신공학과 연구교수

관심분야 : 정보보호, 디지털 저작권 관리, 신경망 학습 등