지문 특징을 이용한 일회용 암호키 생성기법

An OTP(One Time Password) Generation Method Using the Features of Fingerprint

차병래(Byung Rae Cha)*, 고일석(Franz I.S. Ko)**

초 록

인터넷의 광범위한 응용과 더불어 인터넷 보안은 최근 중요한 관심사가 되고 있다. 악의의 행위를 방지하기 위한 보안 시스템은 구성 요소 및 동작의 완결성이 보장되어야만 시스템의 안전성을 보증할 수 있게 된다. 어느 한부분의 약점은 전체 시스템의 완결성에 치명적인 결과를 발생하게 된다. 따라서 각각의 보안 요소마다 다양한 기법 및 응용에 대한 연구와 시스템적 응용에 대한 연구가 활발히 이루어지고 있다.

본 논문에서는 지문의 특징을 이용한 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.

ABSTRACT

As the applications within Internet becoming more extensive, the security issues of those applications are appearing to be the most important concern. We have to be sure if all elements of the system are robust and perform well. Even if some small part of the system is vulnerable, it might cause the total system crash-down. 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 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 for proposed password generation method.

키워드 : 지문, 일회용 패스워드, 보안, 인증
Fingerprint, One Time Password, Security, Authentication

본 논문은 2007년 호남대학교의 교내연구비를 지원받은 연구결과의 논문입니다.

* 호남대학교 컴퓨터공학과
** 교신저자, 동국대 컴퓨터학과

1. 서 론

인터넷의 광범위한 응용과 더불어 인터넷 보안은 더욱 중요한 관심사가 되고 있다. 그러나 인터넷은 개방형 네트워크이기 때문에 악의의 공격자에 의한 시스템 침입, 크래킹, 도청 등과 같은 다양한 형태의 공격에 대해 취약하다. 근래에는 온라인 마켓의 개념이 전통적인 오프라인 산업의 마켓까지 확대되고 있어, 인터넷 시스템에 대한 악의적 공격 피해에 대한 방어 및 복구에 대한 중요성이 커지고 있다.

악의의 행위를 방지하기 위한 보안 시스템은 구성 요소 및 동작의 완결성이 보장되어야만 시스템의 안전성을 보증할 수 있게 된다. 어느 한부분의 약점은 전체 시스템의 완결성에 치명적인 결과를 발생하게 된다. 따라서 각각의 보안 요소마다 다양한 기법 및 응용에 대한 연구와 시스템적 응용에 대한 연구가 활발히 이루어지고 있다.

개방형 네트워크 환경의 1차적인 보안은 사용자 인증이라 할 수 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 사용하기 때문에 편리하기 때문이다. 하지만 이러한 방식은 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[4, 13].

일회용 패스워드 기술(OTP : One Time Password)은 이러한 단점을 극복할 수 있는 인증 기법이다[3, 9, 13]. OTP는 매번 새로운 패스워드를 생성함으로서 상기 아이디와 비밀번호 기반 방식의 문제점을 보완하고 있다. 이러한 OTP는 주로 인터넷 뱅킹에서 사용되어 왔으나, 최근에는 온라인상의 다양한 형태의 상거래에서 활용하고 있다.

본 논문에서는 지문의 특징을 이용한 OTP의 일회용 암호 키를 생성하는 방법을 제안한다. 본 연구는 잘 알려진 강력한 개인 인증 요소인 지문 정보를 이용하여 가변적이고 안전한 일회용 암호 키를 생성하였으며, 또한 제안 기법에 대한 시뮬레이션을 통해 성능을 분석하였다.

2. 관련 연구

2.1 지문

생체인식(Biometrics)은 인간의 생리적, 행동 양식적 특징을 기반으로 하여 인간을 인식하는 자동화된 방법이며, 특정 개인의 특성을 인증하거나 신분을 인식하기 위해, 측정 가능한 특성 또는 개인의 특징을 연구하는 분야이다[2, 12]. 실제로 사람은 누구나 독특하면서 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 특징 점(Minutiae Point) 및 요철의 형태에 의해 결정된다. 여기서 특징점이란 융기부분의 분기점이나 끝점에 생긴 국소적인 특징을 말한다[6, 8].

지문 추출 기술은 지문을 비교하기 위한 가장 확실한 방법은 지문의 모든 영상 정보를 전부 비교하는 것이다. 그러나 현실적으로 이것은 불가능하다. 영상 정보를 전체적으로 비교하기 위해서는 그만큼 처리해야할 Data의 양이 많아지게 되어 상용화된 시스템을 만들기에는 부적절하다. 실제로 상용화된 시스템을 보면, 지문의 영상을 그대로 저장하는 대신 영상의 특징 점을 저장하여 그 특징 점들의 위치와 관련된 코드를 저장한다. 특징 점만을 저장하기 때문에 나중에 지문영상으로 복원할 수 없어 법 시행 기관들에 의한 증명 방법으로는 사용될 수 없다[2].

2.2 일회용 암호 시스템

OTP는 일회에 한해 사용할 수 있는 인증 기법으로 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[9, 10]. OTP는 IETF에 의해서 표준화 되었으며, 그 후에는 인증관련 업체에서 표준화를 주도하고 있으며 대표적으로 RSA[14] 진영과 OATH[11] 진영이 경쟁적으로 표준화를 진행하고 있다.

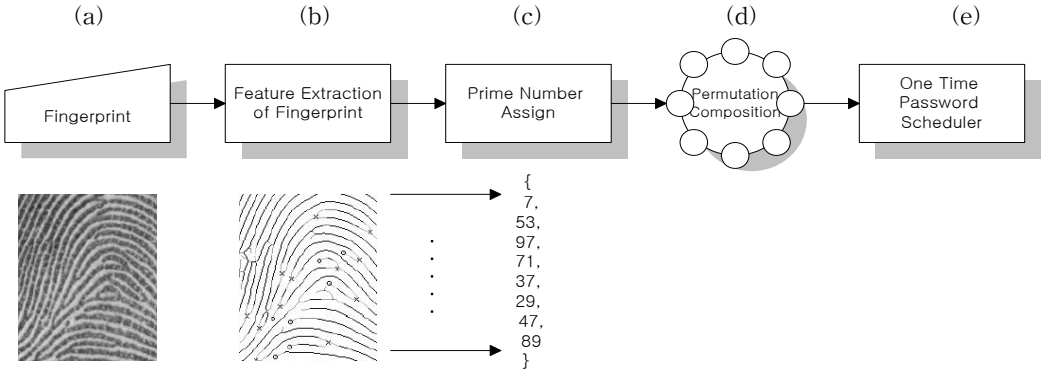
3. 지문 특징 정보를 이용한 암호화 키 생성

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 1>은 OTP의 암호화 키 생성 과정을 나타낸 것이다.

암호화 키 생성 과정을 위해 사용자는 먼저 <그림 1>의 (a)와 같이 지문을 스캐닝한다. 스캔된 지문은 <그림 1>의 (b)와 같이 클라이언트 측의 사용자 지문을 이용하여 특징 정보를 추출하며, <그림 1>의 (c)와 같이 추출된 지문의 특징 정보에 의해서 특징 점에 임의의 소수를 무작위로 할당하게 된다. <그림 1>의 (d)는 할당된 소수를 순서 관계에 의해



〈그림 1〉 지문 특징 점을 이용한 OTP의 암호화 키 생성 과정

서 순열 조합을 생성하는 과정이며, <그림 1>의 (e)는 순열을 이용하여 OTP의 패스워드를 생성한다. OTP의 암호화 키 생성 모듈은 OTP의 클라이언트 측에 위치하고 있다. <그림 1>의 (d)는 순열을 이용하여 한 세션에 대한 일시적으로 사용 가능한 무한대의 OTP의 패스워드를 생성하게 된다. 생성할 수 있게 되는 것은 순열의 특징을 이용하기 때문이며, <그림 5>에서 자세히 다루고 있다.

3.1 지문을 이용한 특징점 추출

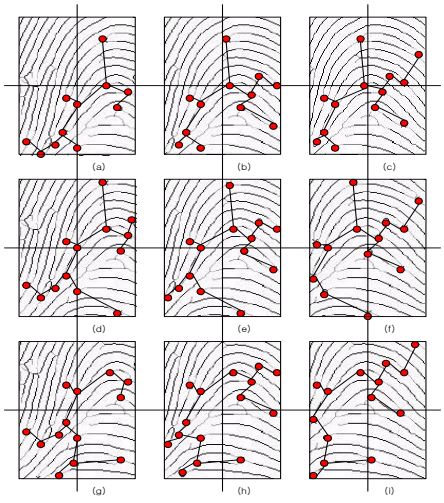
일반적으로 지문의 특징 정보를 이용하여 OTP의 암호화키를 생성할 경우, 동일한 지문에 대해 매번 동일한 지문 특징 정보를 갖게 되며 이에 따라 암호화 키 또한 동일해진다. 기존의 연구 방법들은 이와 같이 사용자 개인의 지문에 동일한 값으로 인식을 하게 된다. 따라서 기존의 연구방법에서는 지문을 OTP를 위한 기반정보로 활용할 수 없게 된다.

자필에 의한 인증시스템이 발달하지 못한 과거의 동양에서는 문서에 서명이 필요한 부분에 도장으로 서명을 대신하였다. 그러나 서명을 대신하는 문장으로 각인된 도장을 찍다 보면 매번 동일한 문장이 약간씩 다르다는 것을 발견할 수 있다. 찍힌 문장의 위치(Location)의 변화를 관찰하게 된다.

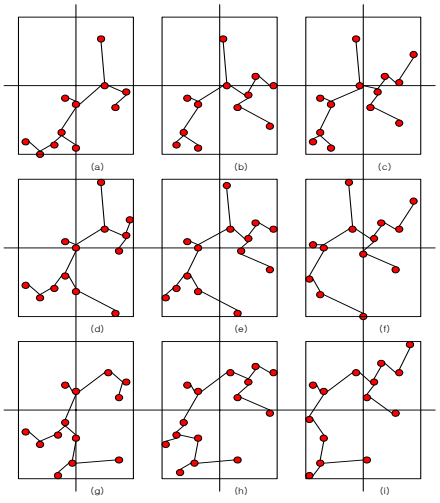
<그림 2>와 <그림 3>은 동일한 지문을 이용하여 우측과 아래쪽으로 3mm씩 이동하여 지문의 특징 점 추출과 추출된 특징 점을 이용한 준동형 그래프의 변화를 나타낸 것이다. <그림 3>은 그래프의 변화를 관찰하기 쉽게 하기 위하여 <그림 2>에서 지문을 제거하여 나타낸 것이다. 특징 점 그래프의 생성 과정은 스캔화면의 정중앙에서 가장 가까운 노드에서 시작하여 프림 알고리즘으로 MST(Minimum spanning tree) 그래프[1]를 생성하여 나타낸다.

<그림 2>와 <그림 3>을 통해서 동일한 지문도 매번 스캔할 때마다 약간의 차이를 갖게 된다는 것을 알 수 있다. 즉 지문 스캔 시에 동일한 지문에 대해서도 스캐닝되는 위치와 각(Angle)의 변화에 의해서 특징 점 추출에 의한 특징점 그래프의 변화를 보이게 되며, 준동형 그래프를 생성하게 된다.

이러한 특징을 이용하면 동일한 지문도 매



〈그림 2〉 동일한 지문의 위치에 의한 특징 점 노드의 변화



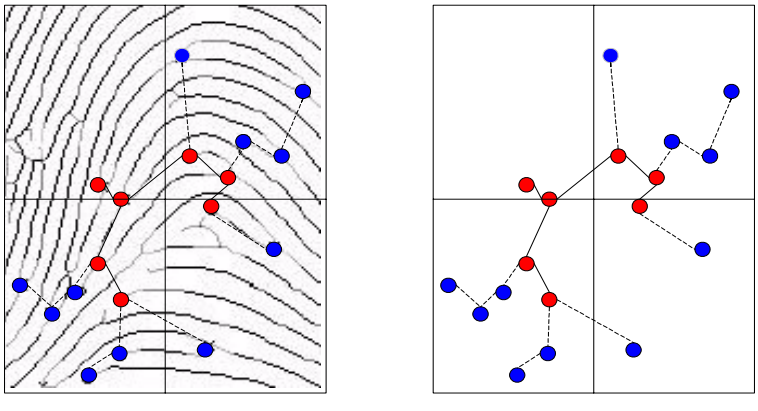
〈그림 3〉 특징 점 그래프의 위치에 따한 노드의 변화

번 스캔 시 특징점 그래프의 변화에 의한 다른 암호화 키를 생성할 수 있게 되어 지문을 OTP에 사용할 수 있게 된다.

<그림 4>의 (a)는 <그림 2>의 9장의 이미지를 하나로 만들어 추출한 특징점 그래프를 나타낸 것이며, <그림 4>의 (b)는 <그림 4>의 (a)에서 지문 이미지를 삭제한 것이다. 특징점 그래프의 빨강색의 노드는 특징 점 그래프에서 변화를 보이지 않는 부분이며, 파랑색의 노드는 위치 변화에 따른 노드의 제거 또는 추가의 변화를 보인 노드를 나타낸 것이다.

3.2 암호화 키 및 순열 생성

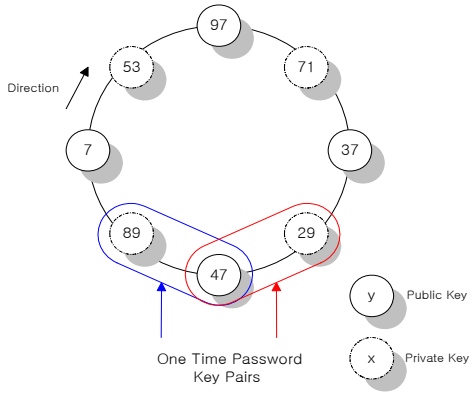
먼저 지문 특징 점을 이용한 그래프 각각의



(a) (b)

〈그림 4〉 특징 점 그래프의 고정된 노드와 변화된 노드

노드에 임의의 소수를 할당하고 MST 그래프의 탐색 순서에 의해서 순서 관계를 순열로 구성한다. 순열의 암호화 키 생성은 <그림 5>와 같이 MST 그래프의 시작 노드를 원점으로 그래프의 탐색 순서로 임의적으로 할당된 소수를 이용하여 암호화 키를 생성한다.



〈그림 5〉 OTP의 키 생성을 위한 순열 구성

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.

순열은 순열의 서로소에 의해서 순회순열의 곱으로 표시할 수 있으며, 이러한 순회순열의 특징으로 순회순열의 곱의 수만큼의 일회용 패스워드 쌍의 생성이 가능하게 된다.

{7, 53, 97, 71, 37, 29, 47, 89} =>
{(7, 53), (53, 97), (97, 71), (71, 37),
(37, 29), (29, 47), (47, 89), (89, 7)}

또한 순열을 이루는 암호화 키 리스트의 수가 짝수 또는 홀수에 관계가 없으므로, 순열에 의한 암호화 키 쌍을 공개키와 개인키로 할당함으로서 공개키 암호화 시스템에 적용 가능하게 된다.

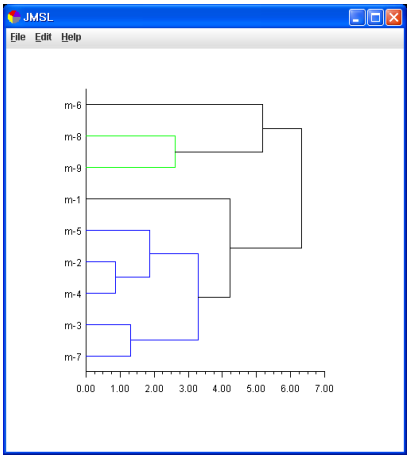
4. 시뮬레이션

4.1 한 지문의 위치 변화에 의한 거리 비교

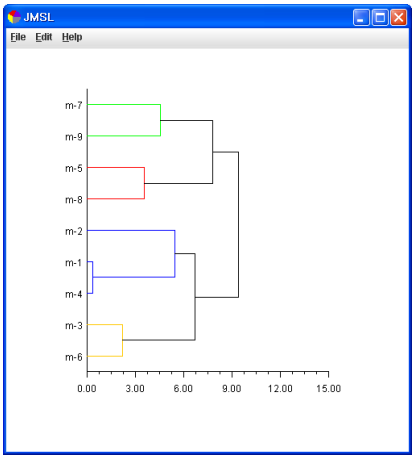
지문 특징 점에 의해 생성된 <그림 4>의 9개의 준동형 그래프를 이용하여 dendrogram [5]과 각각의 노드에 임의의 3자리 난수를 할당하여 dendrogram으로 나타내었다. 이때 dendrogram은 JMSL[7] 라이브러리를 이용하였다. <그림 6>과 <그림 7>에서 dendrogram에 의해서 동일한 지문이지만 유한개의 준동형 그래프 생성으로 무작위성을 갖을 수 있음을 알 수 있고 난수 할당에 의해 무작위성과 확산이 확대되었음을 알 수 있다. 이 경우 순열 구성을 이용함으로서 한 세션에 대해 일시적으로 무한개의 암호화 키를 생성할 수 있게 된다.

4.2 샘플 지문 이미지의 위치변화에 따른 특징 변화 측정

지문 샘플 데이터 30개를 이용하여 위치 변



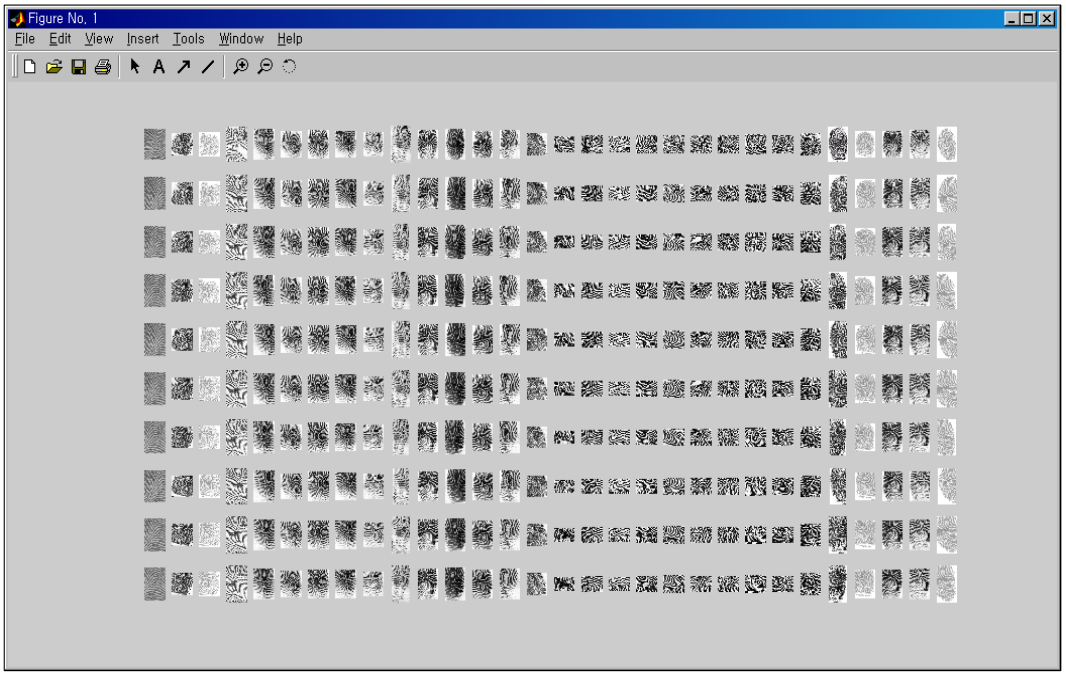
〈그림 6〉 9개의 지문 그래프에 의한 Dendrogram



〈그림 7〉 난수 할당에 의한 무작위성과 확산의 확대

화에 따른 지문 특징 점의 준동형 그래프를 분석하였다. <그림 8>은 샘플 지문 이미지의 위치 변화에 따른 지문 이미지의 스캔 영역을 나타낸 그림이다. 가로 축은 지문 샘플 데이터 30개를 나타내며, 세로 축은 원본 지문과 위치변화에 의한 9개의 스캔닝된 샘플 지문 이미지를 나타낸 것이다.

30개의 샘플 지문 이미지에서 추출된 특징



〈그림 8〉 30개의 샘플 지문 이미지 데이터와 위치변화에 따른 각각 9개의 지문 이미지

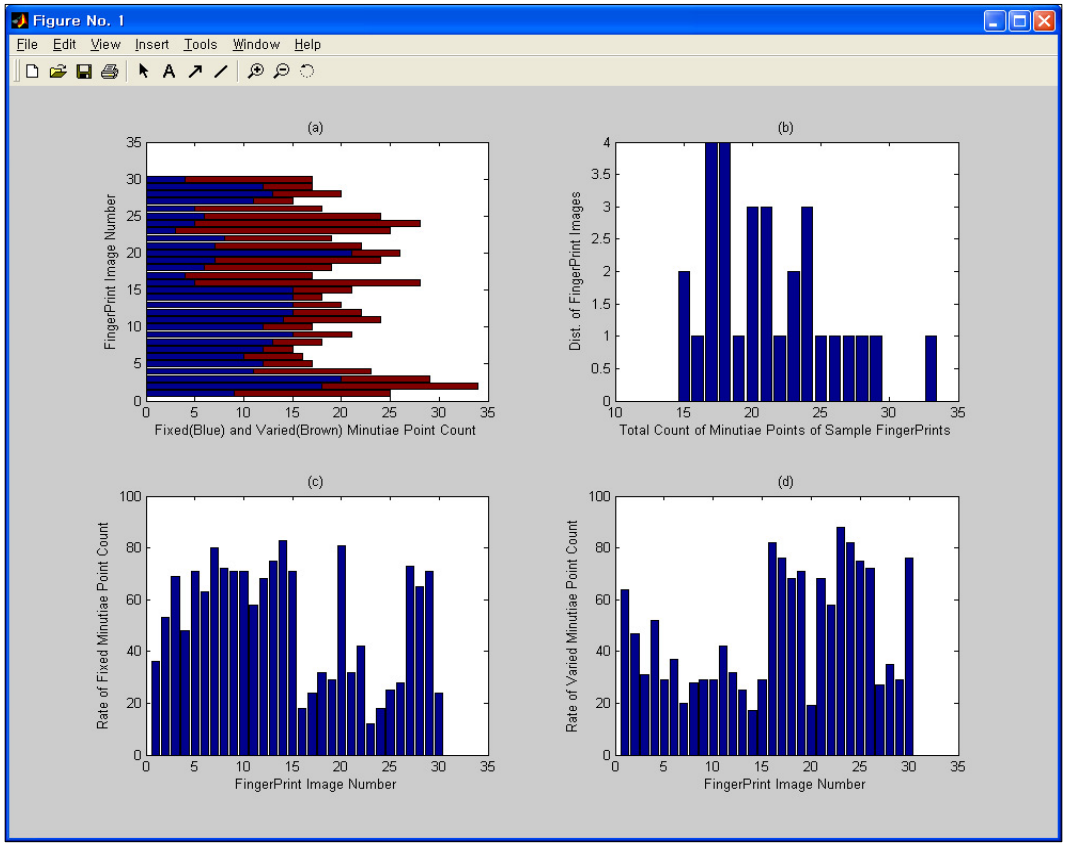
수는 최소 15개와 최대 34개가 추출되었으며, <그림 9>와 같은 분포를 보였다. 특징 점의 고정된 특징 점 수와 변화된 특징 점 수의 평균은 각각 10.7667와 10.5333이었으며, 표준 편차는 4.8968와 6.0898이었다.

<그림 9>의 (a)는 30개의 샘플 지문 이미지의 위치변화에 따른 고정된 특징 점 수와 변화된 특징 점 수를 나타낸 것이다. <그림 9>의 (b)는 샘플 지문 이미지를 특이 점 수에 따른 분포를 나타낸 것이다. <그림 9>의 (c)와 <그림 9>(d)는 샘플 지문 이미지에 대한 고정된 특이 점 비율과 변화된 특이점 비율을 나타낸 것이다.

샘플 지문 데이터의 위치변화에 따른 지문 특징 점의 준동형 그래프의 변화를 측정하여 <표 1>에 나타냈다.

지문 특징 점의 준동형 그래프의 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 22.8328%와 22.8328%이었다.

위 시뮬레이션의 결과는 하나의 지문을 스캔한 지문 이미지에 대해서 위치 변화에 따른 준동형 그래프를 생성하였으며, 그 결과를 순열을 이용하여 일시적으로 무한대의 암호



〈그림 9〉 특징 점 개수에 따른 샘플 지문 이미지의 분포

〈표 1〉 준동형 그래프의 고정 및 변화를 갖는 특징 점의 분포

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

화 키를 생성할 수 있음으로 보였다. 이러한 특징 때문에 OTP 시스템에 사용될 수 있는 유효성을 시뮬레이션 하였다.

5. 결 론

인터넷의 광범위한 응용과 더불어 인터넷 보안은 더욱 중요한 관심사가 되고 있다. 그러나 인터넷은 개방형 네트워크이기 때문에 악의의 공격자에 의한 시스템 침입, 크래킹, 도청 등과 같은 다양한 형태의 공격에 대해 취약하다. 근래에는 온라인 마켓의 개념이 전통적인 오프라인 산업의 마켓까지 확대되고 있어, 인터넷 시스템에 대한 악의적 공격 피해에 대한 방어 및 복구에 대한 중요성이 커지고 있다. 따라서 보안에 대한 다양한 분야에 대해 연구가 이루어지고 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 OTP의 암호화 키 생성 기법을 제안하고 시뮬레이션 하

였다. 또한 시뮬레이션 결과 제안 기법을 통해 지문을 OTP에 활용할 수 있음을 입증하였다.

참 고 문 헌

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

[2] 바이오메트릭스(Biometrics)의 이해, http://ics1.mk.co.kr/file/cd104/biometrics1.pdf.

[3] Rubin, A. D., Independent One-Time Passwords, Proc. 5th UNIX Security Symposium, USENIX Association, 1995.

[4] Ed Tittel, Mike Chapple, James Michael Stewart, “CISSP : Certified Information Systems Security Professional,” Sybex, 2003.

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

[6] Jain, A., and Pankanti, S., “Fingerprint Classification and Matching,” Handbook for Image and Video Processing, A. Bovik (ed.), Academic Press, April 2000.

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

[8] Hong, L. and Jain, A. K., “Classification of Fingerprint Images,” MSU Technical Report, MSU Technical Report MSUCPS : TR98-18, 1998.

[9] Haller, N., Matz, C., Nesser, P., and Straw, M., “A One-Time Password System,” RFC 2289, IETF, 1998.

[10] Neil Haller, “The S/KEY One-Time Password System,” Proceedings of the Symposium on Network and Distributed System Security, 1994.

[11] OATH, http://www.openauthentication.org.

[12] Pankanti, S., Bolle, R. M., and Jain, A., “Biometrics : The Future of Identification,” IEEE Computer magazine, February, 2000.

[13] Rolf Oppliger, “Security Technologies for the World Wide Web,” Artech House, 2000.

[14] RSA, http://www.rsa.com.

저 자 소 개

차병래 (E-mail : chabr@honam.ac.kr)
1997년 호남대학교 컴퓨터공학과 (공학석사)
2004년 목포대학교 컴퓨터공학과 (공학박사)
2005년~현재 호남대학교 컴퓨터공학과 전임 교수
관심분야 컴퓨터 시스템 보안, 디지털 컨텐츠 보호, 신경망 등

고일석 (E-mail : isko@dongguk.edu)
1996년 경북대학교 컴퓨터공학 (공학석사)
2001년 미국 USIU MBA
2006년 연세대학교 컴퓨터산업시스템공학과 (공학박사)
2006년~현재 동국대학교 경주캠퍼스의 컴퓨터학과 교수 및 AICIT의 소장, IBC(Cambridge, UK)이 명예의장, The World Congress of Arts, Sciences and Communications (Cambridge, UK)의 부의장
관심분야 융합정보기술, 네트워크 기반의 미디어솔루션 및 서비스기술