ISSN 2288-4866 (Print)
ISSN 2288-4882 (Online)
http://www.jiisonline.org
J Intell Inform Syst 2013 September: 19(3): 45~55 http://dx.doi.org/10.13088/jiis.2013.19.3.045

다중 지문 시퀀스를 이용한 스마트폰 보안

배경율
상명대학교 소프트웨어대학 컴퓨터과학부
(jbae@smu.ac.kr)

최근 모바일 디바이스와 휴대기기의 발달로 원격접속이 늘어남에 따라 보안의 중요성도 점차 증가되었다. 그러나 기존 패스워드나 패턴과 같은 보안 프로그램은 지나치게 단순할 뿐 아니라 다른 사용자가 쉽게 취득하여 악용할 수 있다는 단점이 있다. 생체인식을 활용한 보안 시스템은 보안성이 강화 되었지만 위조 및 변조가 가능하기 때문에 완전한 해결책을 제시하지 못한다. 본 논문에서는 이러한 문제점을 해결하기 위해 지문인식과 패스워드를 결합하여 보안성을 향상시킬 수 있는 방안을 연구하였다. 제안한 시스템은 하나의 지문이 아니라 다수의 지문을 이용하는 방법으로, 사용자가 패스워드를 입력할 때 여러 지문 중에서 정확한 지문의 순서를 제공하도록 한다. 오늘날 스마트폰은 패스워드나 패턴, 지문을 이용할 수 있지만 패스워드의 강도가 낮거나 패턴이 쉽게 노출되는 등의 문제가 있다. 반면에 제안한 시스템은 다양한 지문의 이용과 패스워드의 연계, 또는 다른 생체인식 시스템과 연결함으로써 매우 강력한 보안장치가 될 수 있다.

논문접수일 : 2013년 09월 05일 논문수정일 : 2013년 09월 14일 게재확정일 : 2013년 09월 15일
투고유형 : 국문급행 교신저자 : 배경율

1. 서론

스마트폰과 같은 이동 단말의 보급이 점진적으로 증가하면서 교육이나 뉴스, 금융 등의 분야에서 이들 단말을 사용하는 사람들이 급속히 늘어가고 있다. 2007년 1월 애플사에서 아이폰을 출시하면서부터 스마트폰 사용자가 급속히 증가하였으며, 스마트폰은 새로운 시장을 창조하고 사용 영역을 넓혀나가고 있다. 스마트폰은 무선 인터넷 망인 Wi-Fi를 이용하거나 이동 네트워크인 3G 네트워크 또는 LTE(long term evolution) 네트워크를 이용함으로써 언제 어디서나 인터넷에 접속할 수 있는 특징이 있으며 사용자가 원하는 다양한 애플리케이션을 앱스토어나 마켓에서 다운받아 사용할 수 있다는 특징을 가지고 있다. 이러한 애플리케이션으로 인하여 현재 내가 있는 위치 주변에 어떠한 건물이 있는지 검색할 수 있게 되었고, 버스나 지하철 같은 대중교통의 도착시간을 실시간으로 확인하거나 인터넷 뱅킹 및 주식거래, 음악 감상, 게임 등을 장소와 시간에 제약받지 않고 이용할 수 있는 환경을 구축하였다(Korea Broadcasting and Communication Committee, 2011).

스마트폰에 의해서 컴퓨터의 기능이 대체되면서 스마트폰에는 금융거래정보나 개인적인 사진과 동

* 본 연구는 2012학년도 상명대학교 학술연구 지원비에 의해서 이루어졌음.

영상과 같은 중요한 사용자 정보가 포함되어 있다. 현재 스마트폰 보안 시스템은 너무 단순할 뿐 아니라 잠금해제를 위한 방법이 널리 알려져 있다. 아이폰은 숫자와 문자의 조합으로 스마트폰의 개인정보 접근을 보호하고 있으나 미국 IT 전문지인 Engadget은 이들 조합이 숫자 패드와 버튼의 몇 가지 조합으로 쉽사리 잠금해제 된다는 것을 보였다. 아이폰 iOS 4.1 미만의 버전은 4자리의 숫자를 비밀번호로 설정하는 것이 가능하며 4.1 이후부터 문자입력이 가능하다. 하지만 영국의 웹사이트 'Lockdown'에 소개된 'Password Recovery Speeds'라는 연구결과를 살펴보면 듀얼코어 PC(Dual Processor PC)의 경우 특수문자를 포함한 영문 대문자와 소문자 숫자를 결합한 4자리의 패스워드는 8초 이내의 해제할 수 있는 것으로 나타났으며, 워크스테이션(Workstation)을 이용할 경우 1초 이내로 패스워드를 해제 할 수 있는 것으로 나타났다. 안드로이드 운영체제 역시 보안에 취약하다. 안드로이드 운영체제는 9개의 점을 갖고 있는 패턴을 보여주고 사용자에 의해서 설정된 패턴으로 잠금장치를 사용하고 있으나 펜실베니아 주립대학의 Jonathan Smith 교수 연구팀에 의하면 이들 패턴도 스마트폰의 스크린 상에 남아있는 지문을 따라가는 것에 의해서 손쉽게 잠금해제가 된다(Digital Times, 2010).

따라서, 안드로이드와 아이폰 운영체제는 보안위협에 대해서 매우 취약하다는 것을 알 수 있다. 패스워드와 패턴을 이용한 보안방식의 문제점과 비교하면, 지문 인식을 이용한 보안방식은 안전성과 분실가능성에 대한 장점을 갖는다. 이러한 안전성에도 불구하고 스마트폰에서 지문인식 시스템이 널리 사용되지 않는 이유는 적절한 가격을 제시하지 못하고 있으며, 개인 생체정보에 대한 우려 때문이다. 지문인식 센서의 가격이 현재는 적정하지 못한 수준이고, 스마트폰과 같은 소형단말에 적절한 크기로 제공되지 못하고 있으나 기술의 발전에 따라서 가격이 하락할 것이며, 소형화에 의해서 스마트폰으로의 탑재가 가능해질 것이다(Bae et al., 2012).

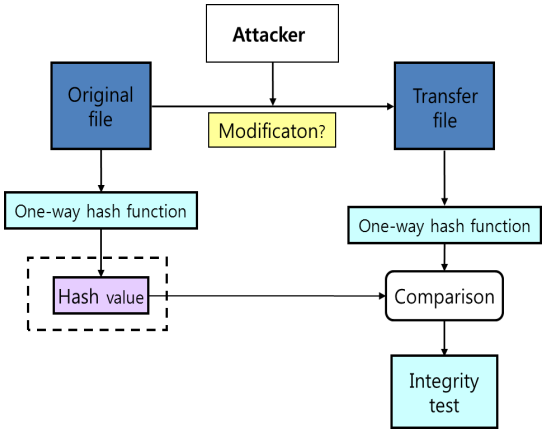
일단 지문인식 시스템이 스마트폰에서의 사용이 활성화되고 금융기관과 공공기관의 지문인식 센서를 이용한 공인인증이 시작된다면 스마트폰의 생체정보 활용의 폭은 더 넓어질 것이다. 따라서 본 논문에서는 기존 지문인식 잠금장치의 보안성을 강화하고 지문과 패스워드 시스템을 결합한 스마트폰에 적용될 수 있는 지문 시퀀스 보안 시스템을 제안하고자 한다.

2. 패스워드 시스템

패스워드 시스템에서는 사용자가 자신의 식별자(identifier, ID)와 패스워드를 입력하여 자신을 인증한다. 모든 사용자들의 식별자와 패스워드는 시스템 내에 저장되어 있고 시스템은 입력된 식별자와 패스워드를 저장되어 있는 것과 비교한다. 비교결과 올바른 식별자와 패스워드가 입력되었을 경우에만 사용자에게 시스템이나 파일에 접근할 수 있는 권한을 준다(Lee et al., 1991).

최초의 패스워드는 식별자와 패스워드를 패스워드 파일에 저장하고 시스템 관리자를 제외한 모든 이에게 파일에 대한 접근을 제한하는 방식이었지만 시스템 관리자의 패스워드 노출이나 관리자에 의한 패스워드 유출에 대한 위험 때문에 이에 대한 해결책으로 해시함수(Hash function)를 이용한 새 방법이 고안되었다. 이 방법은 패스워드를 입력하여 일방향 함수를 계산한 결과를 식별자와 함께 패스워드 파일에 저장하는 것이다. 일방향 함수란 한 방향으로의 계산은 쉬운 반면 반대방향의 계산은 불가능한 함수를 말한다. 사용자가 식별자와 패스워드를 입력하면 시스템은 그 패스워드를

일방향 함수를 거쳐 저장되어 있는 것과 비교하여 사용자를 인증한다. 역함수의 계산이 불가능해짐으로써 패스워드 파일 자체에 대한 보안이 불필요해 졌다는 것이 큰 특징이다. 해시함수로는 대표적으로 MD5, SHA1, RMD160, TIGER 등이 많이 쓰이며, 현재 가장 많이 사용되고 있는 방식으로는 SHA (Secure Hash Algorithm)이 있다. SHA는 1993년에 미국 NIST에 의해 개발되었고 가장 많이 사용되고 있는 방식이다. SHA1은 DSA(Digital signature algorithm)에서 사용하도록 되어 있으며 많은 인터넷 응용에서 기본적인 해시 알고리즘으로 사용된다. SHA256, SHA384, SHA512는 AES(Advanced Encryption Standard)의 키 길이인 128, 192, 256 비트에 대응하도록 출력 길이를 늘인 해시알고리즘이다.



<Figure 1> Hash Function Block Diagram

패스워드 시스템의 보안적 위협이란 사용자의 패스워드가 불법적으로 노출되는 것을 말한다. 시스템에 침입하려는 공격자는 아래의 세 가지 방법으로 사용자의 패스워드를 알아 낼 수 있다(Morris et al., 1979).

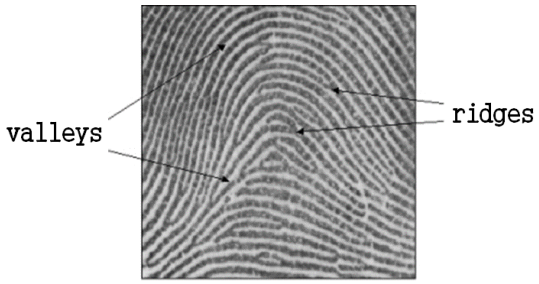
첫째, 시스템의 패스워드 파일을 읽어내는 방법이 있다. 패스워드 파일은 사용자들의 패스워드와 식별자를 저장한 파일이며 만약 노출되면 시스템과 모든 사용자들의 자료는 위험에 빠지게 된다. 따라서 패스워드 파일은 일반 사용자에게 접근을 제한하며 오직 보안 관리자만이 권리를 갖게 한다. 그러나 시스템의 고장이나 보안 관리자가 악의적으로 패스워드 파일을 노출시킨 경우에 이러한 패스워드 시스템은 전혀 안전하지 못하다. 보다 확실한 방법은 패스워드를 일방향 함수를 통해 그 결과를 식별자와 함께 파일을 저장하여 패스워드 파일이 노출되더라도 사용자 패스워드를 안전하게 유지하는 것이다. 이 방법은 입력된 패스워드에 일방향 함수를 적용하여 그 결과를 저장된 것과 비교함으로써 사용자 인증을 한다.

둘째, 사용자와 시스템 간에 패스워드를 주고받는 통신을 도청 할 수 있다. 만약 보안 관리자가 패스워드 시스템의 도청 위험이 크다고 판정하면 통신되는 패스워드는 입력 장소에서 암호화되어 비교 장소까지 전달되는 방법을 취해야 한다.

셋째, 패스워드가 부주의하게 만들어져 쉽게 추측할 수 있는 경우이다. 실제로 사용자들은 자신들과 연관되거나 흔히 사용하는 단어를 패스워드로 선택하는 경우가 많으므로 패스워드의 추측이 용이한 경우가 많다. 패스워드의 추측을 어렵게 하려면 사용자가 보다 무작위로 선택하거나 자동으로 시스템에서 패스워드를 무작위로 만들어주는 방법이 있다.

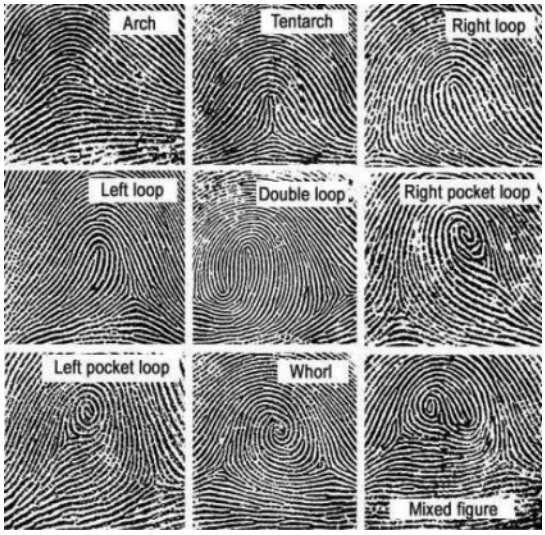
3. 지문인식 시스템

지문이란 인간의 손바닥에 존재하는 땀구멍이 융기한 선으로 형성된 문형을 말하는 것으로 융기되어 나타나는 선을 융선(ridges), 두 융선 사이에 패인 곳을 골(valleys)이라고 한다.



<Figure 2> Ridges and Valleys on a Fingerprint Image

즉 지문은 손가락 끝에 나타나는 융선과 골의 연속이라 할 수 있으며 지문 인식이란 이러한 융선의 흐름을 분석하여 같은 흐름을 보이는 지문을 찾는 과정이라고 할 수 있다(Pan et al., 2001). 지문 패턴은 하나 이상의 융선과 골을 갖고 있는 영역을 보유하며, 이들 영역은 루프, 델타, 소용돌이와 같은 세 가지 클래스로 구분될 수 있다. 대다수 지문 인식 알고리즘은 랜드마크 또는 코어라 불리는 중심점을 기준으로 지문영상을 사전에 재배열하고 표준 지문 모델을 이용하여 지문을 인식한다.



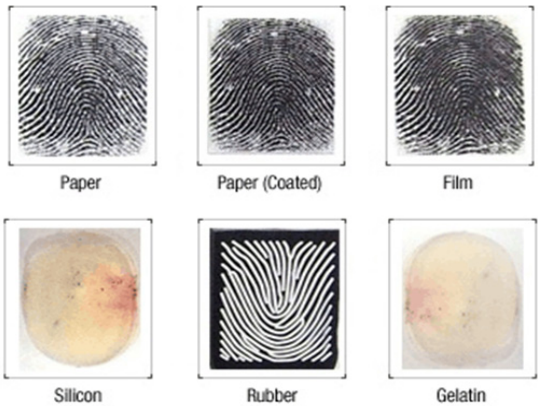
<Figure 3> Specific Regions and Core Points in Fingerprint Images

하지만 지문인식 기술도 위・변조가 가능하며 이에 따른 보안적 위협이 존재한다. 위・변조 생체정보는 인간의 생체정보를 모방하여 동일한 생체특징을 가진 것을 의미하며 최근 생체 생성 기술이 급속도로 발전하면서 위조 생체를 어렵지 않게 제조할 수 있게 되었다. 특히 실리콘 또는 젤라틴과 같은 물질을 이용하여 실제 지문과 구분하지 못할 정도로 유사한 위조 지문을 생성할 수 있으며 투명 렌즈를 이용한 위조 홍채 기술도 급격하게 발전하고 있다. 위조 지문을 생성하는 방법은 사용자의 도움을 받는 경우와 그렇지 않은 경우로 나누어 볼 수 있다.

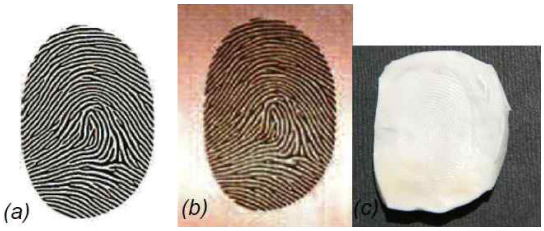
사용자의 도움을 받는 경우는 플라스틱 또는 고무 찰흙과 같은 세밀한 묘사가 가능한 재료를 이용하여 주형을 만들고 이렇게 제작된 주형 위에 젤라틴 용액이나 실리콘을 주입하여 위조 지문을 생성하게 된다.

위・변조 지문을 생성하는 두 번째 방법으로 지문의 흔적을 이용하는 방법이 있다 지문의 흔적을 이용하는 방법은 사용자가 유리잔과 같은 물체에 남겨놓은 잔여 지문을 이용하는 것으로 현재 가장 많이 사용되고 있으며, 보안 취약성에 가장 심각한 문제를 제공하고 있다. 지문의 흔적을 통해 위조 지문을 생성하는 방법은 먼저 고운 분말이나 지문 채취용 분말 또는 접착테이프를 이용하여 사용자의 지문의 흔적을 채취한다. 채취한 지문의 형상을 고성능 카메라를 이용하여 영상으로 변환한 뒤 영상처리 기법을 통하여 영상의 잡음을 제거 한 후 이렇게 제조된 영상을 필름에 인화하여 감광성의 PCB (Printed Circuit Board)에 부착한 후 자외선을 조사하여 주형을 생성한다.

위와 같은 위험성에도 불구하고 기존의 지문인식은 한 개의 지문 혹은 손가락 전체를 동시에 인식기에 입력하여 인증하는 방법으로 지문의 위조에 의한 위험에 노출되어 있다.



<Figure 4> Examples of Fake Fingerprint

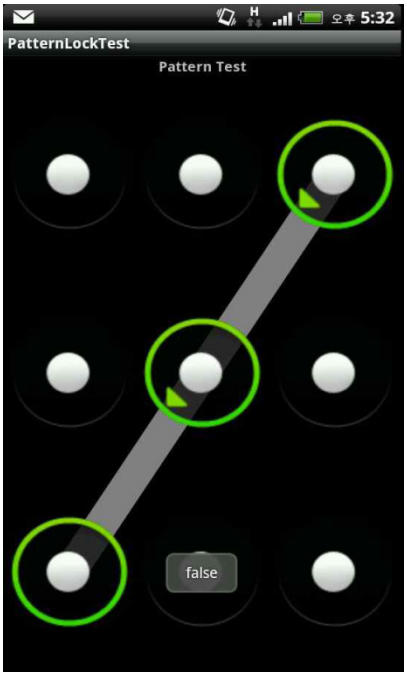


<Figure 5> Fabrication Example of the Fake Fingerprint (a) Reconstructed Fingerprint Image (b) Fingerprinted on the PCB (c) Fake Silicon Fingertip

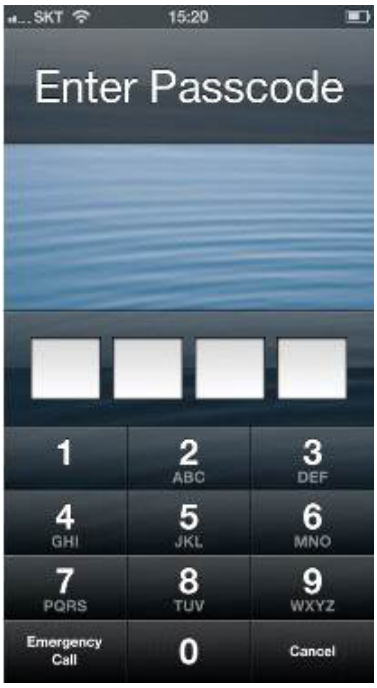
4. 스마트폰 보안 시스템

구글사의 안드로이드는 패턴 인식을 통해 기존의 암호 대신 일련의 동작을 입력하여 모바일 기기에 비인가된 사용자의 접근을 방지하고 있다. 안드로이드의 패턴인식 방식은 기존의 패스워드 입력 방식과 거의 같은 방식이며, 오히려 기존의 패스워드 입력 방식의 보안 메커니즘보다 보안성이 떨어진다. <Figure 6>에 보여진 것과 같이 기존 패스워드 입력 방식의 [1, 2, 4, 6, 9]라는 패스워드를 손가락의 패턴으로 입력하도록 하였다. 또한 안드로이드 패턴인식 보안 메커니즘은 [1, 9, 5]와 같이 멀리 떨어져 있는 번호를 입력할 수 없고 근접한 번호를 거쳐 가야한다는 점에서 안드로이드 패턴인식 보안 메커니즘은 기존의 패스워드 방식보다 보안성이 더 떨어진다는 것을 알 수 있다(Thai et al., 2010).

애플 아이폰의 경우 기본 숫자 4자리 패스워드를 요구하지만 사용자의 설정에 따라 영문 대소문자, 숫자 조합으로 패스워드를 입력할 수 있도록 하여 보안 강도를 높이고자 하였다. 하지만 안드로이드와 아이폰의 이러한 보안 메커니즘은 1차원적인 패스워드로써 기본 4자리 패스워드보다는 보안성이 강화되었더라도 여전히 패스워드의 문제점을 갖고 있다. 아이폰의 사용자 인증 패스워드는 최소 1자리와 최대 9자리라는 범위가 있기 때문이다. 공격자는 이 패스워드 범위를 통해 전사 공격을 시도 할 수 있고, 혹 공격자가 패스워드의 정확한 길이를 알면 더욱 쉽게 패스워드를 유추할 수 있게 된다.



<Figure 6> Example of Pattern Recognition



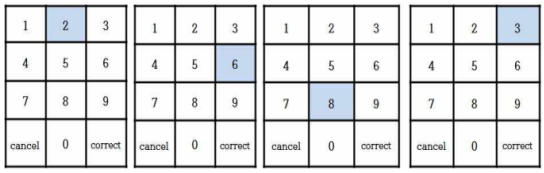
<Figure 7> Example of iPhone user Authorization

5. 지문번호 보안시스템

현재 많이 사용되고 있는 숫자 4자리 패스워드 입력은 <Figure 8>의 숫자 패스워드 입력 예와 같다. <Figure 8>에 [2. 6, 8, 3]으로 설정된 이러한 패스워드는 0000부터 9,999까지의 10,000개의 패스워드 범위를 가지기 때문에 공격자가 모든 경우의 수를 대입하는 전사 공격을 통해 패스워드를 크래킹 할 수 있으며, 4자리 숫자임을 고려해 사용자 정보로부터 공격자가 쉽게 유추하고 공격할 수 있다.

요즘 터치스크린 패스워드와 관련된 보안 문제점에 대해 발표되고 있는데, 입력한 패스워드가 전송되는 네트워크상의 프로토콜이나 기기 자체의 애플리케이션 취약점이 아닌 물리적인 취약점도 발표되고 있다. 패스워드 입력 시 터치스크린에 지문 자국이 남아 공격자가 쉽게 유추할 수 있다고 경고하고 있는 상황이다. 다시 말하면 공격자가 터치스크린에 남은 지문 자국을 이용해 패스워드에 사용된 숫자 4개가 어떤 것인지 알게 된다면 그 4가지 숫자 배열순서만 바꿔 시도함으로써 최대 4! = 24번 안에 매우 쉽게 공격할 수 있다. 또한 일반적인 경우에도 정상 사용자가 패스워드를 입력하는 것을 공격자가 엿볼 수 있다면 입력이 단순한 일반 패스워드는 쉽게 유추될 수 있다.

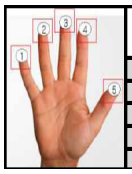
이와 같이 숫자로 이루어진 4자리 패스워드는 프로토콜과 애플리케이션의 보안성 외에도 많은 문제점이 지적되고 있다(Ju et al., 2011).



<Figure 8> Example of Sequence Password

이와 같이 보안 강도가 약한 기존의 숫자 4자리 패스워드를 대신하고 지문인식과 패스워드를 결합하여 보안강도를 높이고자 한다. 기존 지문인식 방식은 한 개의 지문을 지문인식장치에 입력하여 본인인증을 하는 방식으로 이는 단순 경우의 수로만 따져 보았을 때 10가지이며 보통 사용자는 지문인증 시 검지손가락을 사용한다는 점에 비추어볼 때 모조지문이 확보되었을 시 지문의 유추는 매우 쉽게 이루어 질 수 있다. 따라서 본 논문에서는 지문인증을 <Figure 9>와 같이 지문에 시퀀스를 부여하여 복잡도를 증가시킴으로서 보안성을 강화한 새로운 방식의 패스워드를 구성하려 한다. 조합가능 숫자는 기준이 되는 1개의 숫자 당 중복을 포함하여 10개의 숫자를 사용자는 지문에 부여된 시퀀스에 따라 다양한 조합으로 지문을 입력함으로써 보안성을 강화 할 수 있으며 무단사용자는 여러 개의 지문

을 채취해야 하는 동시에 조합되는 숫자 또한 유추해야 하는 어려움을 가진다.



standard number	Combination avaiable number									
1	1	2	3	4	5	6	7	8	9	10
2	1	2	3	4	5	6	7	8	9	10
3	1	2	3	4	5	6	7	8	9	10
4	1	2	3	4	5	6	7	8	9	10
5	1	2	3	4	5	6	7	8	9	10

<Figure 9> Example of Fingerprint Sequence Password

지문의 시퀀스 후에 이루어 질 수 있는 사용자 인증 방법에는 시퀀스가 부여된 지문을 동시에 인식하는 방법, 시퀀스가 부여된 지문을 순서대로 입력하는 방법, 다섯 손가락을 모두 이용하여 동시입력 하는 방법 등 여러 가지 방법이 있을 수 있다. 하지만 사용자 편의성을 고려하여 본 논문에서는 시퀀스가 부여된 지문을 순서대로 2개를 입력하는 방법을 채택하였다.

두 손을 모두 시퀀스를 부여한다고 가정하며 중복된 숫자가 가능하다고 할 때 조합의 개수는 $_{10}P_2$ 이며 총 가능한 경우의 수는 90번이 된다. 10개의 손가락으로 처리할 수 있는 모든 시퀀스의 경우의 수는 $\Sigma_{I=1}^{10}{}_{10}P_i$ 이며, 총 9,864,100개의 경우의 수가 발생한다. 따라서 지문 시퀀스 보안 시스템은 모든 경우의 수를 알아야 하는 것 이외에도 사용자의 모든 지문을 취득해야만 해킹이 가능하기 때문에 매우 안전한 보안 시스템이 될 수 있다.

6. 결론

지문인식과 패스워드를 결합한 지문인식 시퀀스 보안 시스템은 하나의 지문만 입력 받는 것이 아닌 다수의 지문을 순서대로 입력 받아 입력하는 방식이다. 본 연구에서는 스마트폰 환경에서의 다중 입력을 통한 사용자 인증 방식에 대한 아이디어를 소

<Table 1> Fingerprint Sequence Number of Cases

1 sequence	$\frac{10!}{(10-1)!} = {}_{10}P_1$	10
2 sequence	$\frac{10!}{(10-2)!} = {}_{10}P_2$	90
3 sequence	$\frac{10!}{(10-3)!} = {}_{10}P_3$	720
4 sequence	$\frac{10!}{(10-4)!} = {}_{10}P_4$	5,040
5 sequence	$\frac{10!}{(10-5)!} = {}_{10}P_5$	30,240
6 sequence	$\frac{10!}{(10-6)!} = {}_{10}P_6$	151,200
7 sequence	$\frac{10!}{(10-7)!} = {}_{10}P_7$	604,800
8 sequence	$\frac{10!}{(10-8)!} = {}_{10}P_8$	1,814,400
9 sequence	$\frac{10!}{(10-9)!} = {}_{10}P_9$	3,628,800
10 sequence	$\frac{10!}{(10-10)!} = {}_{10}P_{10}$	3,628,800
total	$\sum_{I=1}^{10} {}_{10}P_i$	9,864,100

개하였다. 현재 스마트폰에서의 패턴과 비밀번호를 이용한 사용자 인증방식은 기존 피처폰을 넘어선 스마트폰 활용의 중요성에 비추어 보았을 때 패스워드 노출 위험이 크다.

따라서 제안하고자 하는 지문인식 시퀀스 방식은 기존 지문인식 방식의 지문의 복제라는 위험성을 보완하고 다른 생체인식 방식과 연계한다면 더욱 강력한 보안성을 가질 수 있을 것이다

본 연구에서 제시된 방식에서 해결돼야 할 문제점은 지문 시퀀스에 의한 입력시간의 증가와 하드웨어적 기술 개발이 선행 되어야 한다는 점이 있다. 앞으로 지문인식을 이용한 공인인증 방식이 공용화 되면 스마트폰에서의 지문인식은 중요한 보안이슈로 부각될 가능성이 높으며 본 연구는 지문인식의 보안성 강화 연구의 초석으로 활용될 수 있을 것이다.

참고문헌

Bae, K. Y. and H. Byun, "Utilization of Fingerprint System in the Mobile E-Government," *WORLD-COMP'12*, (2012), 557~583.

Galbally, J., R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez, "Fake Fingertip Generation from a Minutiae Template," *Pattern Recognition*, ICPR2008(2008), 1~4.

Ju, S. H. and H. S. Seo, "Password Based User Authentication Methodology using Multi-Input on Multi-Touch Environment," *Transaction on The Korea Society for Simulation*, Vol.20, No.1(2011), 39~49.

Korea Broadcasting and Communication Committee, *'12 3rd Survey for Status of the Smart phone usage*, Korea, 2011.

Lee, P. J. and H. C. Moon, "Study on the Security of the Password System," *Journal of Korea Communication and Information Security*, Vol.1, No.1(1991), 109~118.

Morris, R. and K. Thompson, "Password security : a case history," *Communications of the ACM*, Vol.22, No.11(1979), 594~597.

Park, J. S., *How easy to trespass the lock of smart phone, Digital times*, 2010. Available at http://www.dt.co.kr/contents.html?article_no=2010102802010351747002(Accessed 06 July, 2013).

Pan, S. B., J. H. Moon, Y. W. Chung, and H. I. Kim, "Technology Trends of the Fingerprint Recognition," *Electronics Telecommunication Trends*, Vol.16, No.5(2011), 46~54.

Thai, L. H. and H. N. Tam, "Fingerprint recognition using standardized fingerprint model," *IJCSI International Journal of Computer Science Issues*, Vol.7, Issue 3, No.7(2010), 11~17.

Yoon, B. N. and H. S. Ban, "Information Security in the Public Field-Certificate Service in the Public Field," *Journal The Korean Institute of Communications and Information Science*, Vol.19, No.8(2002), 20~29.

Abstract

Smartphone Security Using Fingerprint Password

Kyoung-Yul Bae*

Thereby using smartphone and mobile device be more popular the more people utilize mobile device in many area such as education, news, financial. In January, 2007 Apple release i-phone it touch off rapid increasing in user of smartphone and it create new market and these broaden its utilization area. Smartphone use WiFi or 3G mobile radio communication network and it has a feature that can access to internet whenever and anywhere. Also using smartphone application people can search arrival time of public transportation in real time and application is used in mobile banking and stock trading.

Computer's function is replaced by smartphone so it involves important user's information such as financial and personal pictures, videos. Present smartphone security systems are not only too simple but the unlocking methods are spreading out covertly. I-phone is secured by using combination of number and character but USA's IT magazine Engadget reveal that it is easily unlocked by using combination with some part of number pad and buttons Android operation system is using pattern system and it is known as using 9 point dot so user can utilize various variable but according to Jonathan smith professor of University of Pennsylvania Android security system is easily unlocked by tracing fingerprint which remains on the smartphone screen.

So both of Android and I-phone OS are vulnerable at security threat. Compared with problem of password and pattern finger recognition has advantage in security and possibility of loss. The reason why current using finger recognition smart phone, and device are not so popular is that there are many problem: not providing reasonable price, breaching human rights. In addition, finger recognition sensor is not providing reasonable price to customers but through continuous development of the smartphone and device, it will be more miniaturized and its price will fall. So once utilization of finger recognition is actively used in smartphone and if its utilization area broaden to financial transaction. Utilization of biometrics in smart device will be debated briskly. So in this thesis we will propose fingerprint numbering system which is combined fingerprint and password to fortify existing fingerprint recognition.

* Corresponding Author: Kyoung-yul Bae
College of Software, Sangmyung University
20, Hongjimun 2-gil, Jongno-gu, Seoul 110-743, Korea
Tel: +82-2-2287-5211, Fax: +82-2-2287-0072, E-mail: jbae@smu.ac.kr

Consisted by 4 number of password has this kind of problem so we will replace existing 4number password and pattern system and consolidate with fingerprint recognition and password reinforce security. In original fingerprint recognition system there is only 10 numbers of cases but if numbering to fingerprint we can consist of a password as a new method. Using proposed method user enter fingerprint as invested number to the finger. So attacker will have difficulty to collect all kind of fingerprint to forge and infer user's password.

After fingerprint numbering, system can use the method of recognization of entering several fingerprint at the same time or enter fingerprint in regular sequence. In this thesis we adapt entering fingerprint in regular sequence and if in this system allow duplication when entering fingerprint. In case of allowing duplication a number of possible combinations is $\sum_{I=1}^{10} {}_{10}P_i$ and its total cases of number is 9,864,100. So by this method user retain security the other hand attacker will have a number of difficulties to conjecture and it is needed to obtain user's fingerprint thus this system will enhance user's security.

This system is method not accept only one fingerprint but accept multiple finger in regular sequence. In this thesis we introduce the method in the environment of smartphone by using multiple numbered fingerprint enter to authorize user. Present smartphone authorization using pattern and password and fingerprint are exposed to high risk so if proposed system overcome delay time when user enter their finger to recognition device and relate to other biometric method it will have more concrete security. The problem should be solved after this research is reducing fingerprint's numbering time and hardware development should be preceded. If in the future using fingerprint public certification becomes popular. The fingerprint recognition in the smartphone will become important security issue so this thesis will utilize to fortify fingerprint recognition research.

Key Words : Smartphone, Fingerprint, Password, Security

저 자 소 개

배경율

미 Old Dominion University 정보과학 학사, Alabama University 정보과학 석・박사, Stillman College 전산과 교수, Alabama University 산업공학과 교수, 한라중공업 CIO역임, 서울시 정보화기획단장(CIO 1급) 역임, 현재 상명대학교 컴퓨터과학과 교수로 재직 중이다. 주요 관심분야는 전자상거래, 생산관리, 생체 인식 및 지능형 시스템이다.