情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

터치스크린을 이용한 터치 위치기반 사용자 인증*

김 진 복† , 이 문 규‡
인하대학교 컴퓨터정보공학부

User authentication using touch positions in a touch-screen interface*

Jin-Bok Kim† , Mun-Kyu Lee‡
School of Computer and Information Engineering, Inha University

요 약

최근 다양한 기능을 탑재한 모바일 장치가 보급되고 개인정보를 다루는 각종 응용들이 등장하면서 사용자에 대한 인증이 중요한 이슈가 되고 있다. 본 논문에서는 기존의 PIN 방식과 더불어 터치스크린 상에서 입력을 하였을 때 얻을 수 있는 터치 위치데이터를 인증에 이용하는 터치 위치기반 인증방법을 제안한다. 본 연구에서 제안하는 방식은 키패드를 이용하는 기존의 PIN 입력 방식과 동일한 인터페이스를 이용하므로 호환성을 제공하며, 기존 PIN 입력 방식의 안전성을 높이는 방법 중 하나인 행위 분석 방식에 비해 사용자 등록 단계가 간소화되어 편의성을 제공한다. 사용자 인증 실험 결과에 의하면 서로 다른 사용자가 같은 PIN 및 전화번호를 입력한다고 가정할 때 4자리, 6자리 PIN 및 11자리 전화번호에 대해 각각 8.1%, 6.2%, 8.1%의 EER을 나타내었으며, 이를 사용자마다 다른 PIN 및 전화번호를 사용하는 상황에 적용하면 매우 높은 사용자 인식 성능을 보장할 수 있다. 또한 기존 PIN 입력 방식과 동일한 크기의 패스워드(PIN) 탐색 공간을 갖도록 파라미터를 설정한 후 수행한 공격 실험에 의하면 같은 안전성을 가지는 기존의 PIN 입력 방식에 비해 제안한 방식이 매우 높은 안전성을 가짐을 확인할 수 있었다.

ABSTRACT

Recent advances in mobile devices and development of various mobile applications dealing with private information of users made user authentication in mobile devices a very important issue. This paper presents a new user authentication method based on touch screen interfaces. This method uses for authentication the PIN digits as well as the exact locations the user touches to input these digits. Our method is fully compatible with the regular PIN entry method which uses numeric keypads, and it provides better usability than the behavioral biometric schemes because its PIN registration process is much simpler. According to our experiments, our method guarantees EERs of 12.8%, 8.3%, and 9.3% for 4-digit PINs, 6-digit PINs, and 11-digit cell phone numbers, respectively, under the extremely conservative assumption that all users have the same PIN digits and cell phone numbers. Thus we can guarantee much higher performance in identification functionality by applying this result to a more practical situation where every user uses distinct PIN and cell phone number. Finally, our method is far more secure than the regular PIN entry method, which is verified by our experiments where attackers are required to recover a PIN after observing the PIN entry processes of the regular PIN and our method under the same level of security parameters.

Keywords: password, personal identification number, shoulder surfing, touch-screen, touch position

접수일(2010년 11월 26일), 수정일(2011년 1월 26일)
게재확정일(2011년 2월 23일)
* 이 논문은 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임
(과제번호 : 2010-0016787)
† 주저자, maljb@hanmail.net
‡ 교신저자, mklee@inha.ac.kr

I. 서 론

최근 모바일 장치, 특히 스마트폰의 사용이 증가하면서 모바일 장치를 이용한 다양한 응용 서비스들이 등장하고 있다. 따라서 모바일 단말기는 전화번호 및 주소록, 통화 목록 등 기존에 저장되던 기본적인 개인정보 이외에 실명인증, 신용조회, 인터넷뱅킹, 소셜 네트워크 등 각종 서비스에 필요한 추가 정보까지 다루게 됨으로써 분실 및 도난 등의 사고에 대비하여 모바일 장치를 보호하는 것이 점점 더 중요한 문제가 되고 있다.[1]

현재 모바일 장치에서의 사용자 인증을 위해서는 숫자를 패스워드로 갖는 개인식별번호(Personal Identification Number: 이하 PIN) 방식이 보편화되어 있다. 하지만 많은 사람들이 모바일 장치 이용의 편의를 위하여 네자리 정도의 짧은 PIN을 사용하기 때문에 PIN은 충분한 안전성을 보장한다고 보기 어렵다. 따라서 기존의 패스워드 및 PIN보다 더 큰 키 공간을 가지면서 적정 수준의 편의성을 보장하는 인증 방법을 개발하기 위한 연구가 널리 진행된 바 있는데, 그 예로 터치 화면상에 표시된 2차원 그리드 상에 셀들을 순서대로 연결 지어 미리 등록된 패턴을 입력하여 인증하는 DAS (Draw A Secret)[2], 텍스트나 숫자 대신 랜덤 이미지를 패스워드로 이용하는 Deja Vu[3], 사람의 얼굴을 패스워드로 이용하는 Passface[4] 등이 있다. 또한 미국 Rutgers 대학에서 대규모로 진행된 'Graphical password' 프로젝트에서는 Passpoint[5], CHC (Convex Hull Click)[6] 등 다양한 인증 방법을 시도한 바 있다.

그러나 이 방법들 중 대부분은 충분한 엔트로피를 제공하지 못해 안전성에 문제가 있거나, 지나치게 긴 인증 소요 시간과 정상 사용자의 입력 오류 등 편의성 측면에서 많은 문제점이 발견된 바 있다[7][8][9]. 또한 기존 방식과 완전히 다른 기법의 사용으로 인한 호환성 문제가 존재하며, 특히 복잡한 그래픽들을 사용함으로써 모바일 단말기의 제한적인 디스플레이에는 사용이 거의 불가능하다는 문제점도 있다.

따라서 기존의 PIN이나 텍스트 입력 방식을 유지하면서 추가적인 정보를 이용하여 패스워드의 복잡도를 높이는 방법들이 제안된 바 있는데, PC에서 사용되는 키스트로크 패턴이나 마우스 움직임을 이용한 인증 방식[10]의 모바일 기기 버전이라 볼 수 있는 모바일 단말기 상의 키스트로크 패턴 기반 사용자 인증[11]이 그 대표적인 예라 할 수 있겠다. 이 방식은 기존 인터페이스에 대한 변경없이 전화번호나 SMS, PIN 등을 입력하는 과정에서 사용자가 키패드를 누르는 패턴을 단말기가 학습하여 이 패턴을 인증을 위한 추가 정보로 활용하는 기법이며, 최근에는 사용자가 인위적인 리듬을 기억하고 이 리듬에 따라 키패드를 누르도록 함으로써 패턴의 질을 향상시키는 연구가 진행된 바 있다[12]. 그러나 이 방식들 또한 사용자의 PIN 등록 과정에서 특정한 패턴을 이용한 인증모델을 생성하기 위하여 복잡한 알고리즘과 상당히 많은 양의 데이터 입력이 요구된다는 문제점이 있다. 즉, 정상 사용자와 타인 간의 입력을 명확히 구분할 수 있는 정도의 인증 모델을 생성하기 위해서는 사용자가 수십 회에서 수백 회 가량의 PIN 입력을 반복해야 한다[12].

이에 본 논문에서는 기존의 숫자 기반 PIN과 호환이 가능한 동시에 입력 패턴 기반의 인증 방식에 비해 등록 단계에서 상대적으로 적은 양의 입력만을 필요로 하는 터치 위치 기반 인증 방법을 제시한다. 즉, 기존의 PIN방식은 사용자가 기억하는 숫자만을 이용하여 인증이 이루어지는 반면, 본 연구에서 제시하는 방식은 숫자 뿐 아니라 사용자가 해당 숫자를 입력하기 위해 터치 위치데이터를 추가로 이용하게 된다. 따라서 정상 사용자가 아닌 공격자가 인증에 성공하기 위해서는 PIN 숫자와 함께 각 숫자에 대한 터치 위치도 모두 정확히 맞추어야 하며, 만일 정상 사용자가 입력하는 과정을 엿봄으로써 PIN을 획득하는 엿보기 공격을 수행할 경우 단순히 숫자만을 기억하는 것이 아니라 사용자가 입력한 터치 위치를 추가로 기억해야 한다.

터치 위치를 인증에 이용하는 아이디어는 본 논문에서 처음 제시 한 것이 아니라 'Pass Point'[5], 'Passlogix'[13]과 'sfr'[14]에 의해 개발된 방식, 'Jansen'[15]이 제안한 방식 등에서 이미 이용된 바 있다. 하지만 앞서 제안된 방식은 기존의 PIN방식보다 인증에 소요되는 시간이 많으며[16] 기존의 PIN 입력 방식과 전혀 다른 인터페이스를 가지고 있기 때문에 호환성에도 많은 문제를 가지고 있다. 반면에, 본 논문에서 제안한 방식은 기존 PIN 입력 방식과 유사한 인터페이스를 가지고 있으며 터치 위치를 사용할 수 없는 단말기의 경우 기존 PIN 입력 방식과 동일하게 숫자 정보만을 이용하여 인증을 수행 할 수 있다.

본 논문에서는 제안된 방식의 유효성을 확인하기 위해 편의성 및 안전성에 대한 다양한 실험을 수행하였다. 먼저 편의성 측면에서는 4자리, 6자리 PIN과 11자리 전화번호 입력 시 PIN 및 전화번호가 모든

사용자에 대해 동일하다고 가정한 경우에도 터치 위치 데이터만으로 각각 8.1%, 6.2%, 8.1%의 EER (Equal Error Rate)을 얻을 수 있었으며, 여기에 사용자마다 각각 다른 PIN과 전화번호를 적용할 경우 정상 사용자와 타인을 매우 높은 확률로 구분할 수 있다. 또한 PIN 등록 후 일정 시간이 지난 후에도 PIN 숫자와 함께 터치 위치를 기억하는 데 큰 어려움을 겪지 않는다는 사실도 확인할 수 있었다. 안전성 측면에서는, 제안 방식이 사용자로 하여금 PIN 숫자 이외에 추가적인 정보를 기억하게 하여 패스워드 공간의 크기를 늘리는 방식이므로, 단순히 PIN의 구성 자리수를 늘려 패스워드 공간의 크기를 늘리는 방법과 안전성을 비교하였다. 좀 더 구체적으로, 기존방식과 제안 방식에 대해 각각 PIN 입력 과정을 공격자들에게 관찰하게 한 후 인증을 수행하게 함으로써 인증에 성공하는 비율을 비교하였다. 실험 결과에 따르면 같은 정도의 패스워드 공간을 갖도록 파라미터를 설정할 때 제안 방식이 기존에 비해 공격 성공률이 월등히 낮음을 확인할 수 있었다.

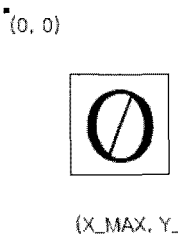
본 논문의 구성은 다음과 같다. 2장에서는 제안한 터치 위치기반의 사용자 인증 방법에 대하여 설명한다. 3장에서는 제안한 방법에 대해 인증 실험을 수행한 환경 및 결과를 분석한다. 4장 안전성 분석에서는 기존의 PIN입력 방식과 안전성을 비교하고 분석한다. 5장 공격 실험에서는 4장에서의 내용을 검증하기 위해 공격 실험을 수행한 환경 및 결과를 분석한다. 6장 결론에서는 이 논문의 결론과 향후 연구 방향에 대해 기술한다.

II. 터치 위치기반 사용자 인증

본 연구는 합법적인 사용자가 인증을 수행할 때 PIN 뿐만 아니라 PIN을 입력할 때의 터치 위치데이터를 함께 사용함으로써 안전성을 높이고 있다. 제안하는 방법은 크게 합법적인 사용자가 자신의 PIN과 PIN의 터치 위치데이터를 통하여 인증모델을 생성하는 사용자 등록단계와, 인증을 요청한 사용자가 입력한 PIN 정보를 확인하고 해당 위치데이터와 합법적인 사용자가 사전에 생성한 인증모델의 위치데이터간의 거리 차이를 이용하여 인증을 수행하는 인증단계로 나뉜다.

2.1. 터치 위치데이터

본 연구에서 사용자 인증에 사용하는 데이터는



〔그림 1〕 버튼상의 좌표

PIN 숫자정보와 해당 숫자를 입력하기 위해 터치한 좌표(X, Y)이다. 좌표는 각 버튼에 대해 〔그림 1〕과 같이 좌측 상단의 (0, 0)부터 오른쪽 하단인 (X_MAX, Y_MAX)로 표현된다. 사용자가 터치스크린에 입력을 하였을 시 발생하는 Mouse Up 이벤트의 좌표를 해당 PIN 정보에 대한 터치 위치데이터로 사용한다.

2.2. 인증모델

인증모델은 정상사용자가 반복하여 입력한 PIN으로부터 생성하는 일종의 기준 값으로, 인증 시 사용자가 입력한 값과 비교대상이 된다. 인증모델을 생성하기 위하여 합법적인 사용자가 K자리의 PIN을 N회 반복 입력하는 경우 j번째 자리 각각에 대해 PIN 숫자정보는 $P_j(j=1,\cdots,K)$로 표시하며, 입력된 위치데이터는 다음 식 (1), (2)와 같이 표시한다.

$$X_j=\{x_{ij}|i=1,\cdots,N\}, j=1,\cdots,K \quad (1)$$

$$Y_j=\{y_{ij}|i=1,\cdots,N\}, j=1,\cdots,K \quad (2)$$

위의 터치 위치데이터를 이용하여 생성하는 PIN의 j번째 자리에 대한 기준좌표 $L_j(j=1,\cdots,K)$는 다음 식 (3)과 같이 N회 입력된 좌표 값들의 평균으로 정의한다. 또한, 인증모델은 $((P_1,L_1),\cdots,(P_K,L_K))$ 로 정의한다.

$$L_j=(\frac{1}{N}\sum_{i=1}^{N}(x_{ij}),\frac{1}{N}\sum_{i=1}^{N}(y_{ij})), j=1,\cdots,K \quad (3)$$

2.3. 인증단계

인증 단계의 전체적인 절차는 〔그림 2〕와 같이 표현 할 수 있다. 먼저, 〔그림 2〕의 Step 1과 같이 인증을 요청한 사용자가 입력한 PIN $P_j'(j=1,\cdots,K)$와 합법적인 사용자가 사전에 등록한 PIN $P_j(j=1,\cdots,K)$

```
Input : K, P_j (j= 1,···,K), L_j (j=1,···,K),
        P_j' (j= 1,···,K), L_j' (j=1,···,K), t, θ
Output : ACCEPT, REJECT

Step 1 : 입력한 PIN과 인증모델의 PIN과 비교
        For j = 1 to K
          If P_j ≠ P_j' then REJECT
        End For

Step 2 : 입력한 PIN의 위치데이터와  인증모델과의
          거리 차이 비교
        counter = 0
        For j = 1 to K
          If | L_j − L_j' | ≤ t then counter = counter + 1
        End For

Step 3 : counter와 파라미터 θ를 비교
        If counter ≥ θ then
          ACCEPT
        Else
          REJECT
        End If
```

〔그림 2〕 사용자 인증 절차

가 일치하는 지 비교하고 하나라도 일치하지 않는다면 요청한 인증은 실패하게 된다.

Step 2와 Step 3은 터치 위치를 확인하는 과정이다. 단, 사용자가 인증을 시도 할 때 마다 인증 모델에 정의된 위치데이터와 완전히 동일하게 입력하는 것은 현실적으로 불가능하다. 따라서 어느 정도 위치를 벗어나도 인증이 성공적으로 수행될 수 있도록 허용범위를 설정해 주어야한다. 파라미터 t는 인증모델과 입력한 위치데이터 간의 거리차이의 허용범위(단위: 픽셀)이고 파라미터 θ는 K자리 PIN 중 거리차이가 t이하인 것이 몇 개 이상이어야 성공으로 인정할 것인지를 나타내는 값이다.

Step 2에서는 인증을 요청한 사용자가 입력한 PIN에 대한 터치 위치데이터 $L_j'(j=1,\cdots,K)$와 합법적인 사용자가 등록단계에서 생성하였던 기준좌표 $L_j(j=1,\cdots,K)$의 거리차이가 t내에 있는지 비교하여 성공한 PIN의 자릿수를 계산한다. Step 3과 같이 성공한 자리의 수가 θ이상이면 인증에 성공한다.

III. 인증 실험

이 장은 제안한 방식에 대한 인증 성공률 실험이다. 실험에 사용한 단말기의 모델은 Sony Ericsson사의 Xperia X1이며 운영체제는 Windows Mobile 6.1이 탑재되어 있다. X1모델은 480×800의 해상도를 갖는 3인치 크기의 터치스크린을 사용하고 있다. PIN 입력을 위한 인터페이스는 〔그림 3〕과 같이 기존 PIN 입력방식과 유사하게 설계하였다. 입력 버튼은 총 10개 이며 각 버튼은 1번 버튼에 표시한 점선만큼 영역을 가진다. 사용자가 보는 버튼의 영역보다 실제 인식영역을 더 확대함으로써 사용자가 손가락으로 버튼의 가장자리에 입력하더라도 공간의 여유를 두어 다른 버튼을 누르는 오류를 줄일 수 있다.

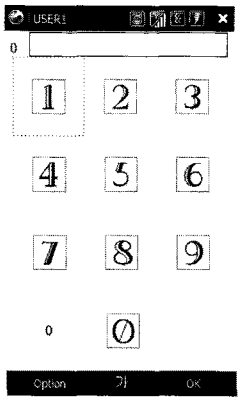
〔표 1〕 실험에 사용한 PIN 및 전화번호

자릿수(K)	PIN(P)
4자리	1234
6자리	654321
11자리(전화번호)	01023459876

터치스크린 사용에 익숙한 피실험자 10명을 대상으로 데이터를 수집하였으며 실험에 앞서 피실험자들에게 실험의 목표와 내용에 대해 자세히 설명하였다. 실험에 사용한 PIN은 〔표 1〕과 같이 고정하였으며 이는 같은 PIN을 사용하는 상황에서 위치데이터에 의한 인증 효과만을 측정하기 위함이다. 즉, 그림 2의 알고리즘에서 Step 1의 비교 과정을 100% 통과한다고 가정하였다. 실험은 각 자릿수에 대해 손을 사용하여 입력하였으며 10회의 반복입력을 통해 PIN을 입력함으로써 각 자릿수에 대한 자신의 인증 모델을 생성하고 5회에 걸쳐 인증을 시도하였다.

사용자가 인증을 시도할 때 발생할 수 있는 오류는 두 종류로, FAR(False Acceptance Rate)과 FRR(False Rejection Rate)에 의해 그 확률이 예측될 수 있다. FRR은 정상 사용자임에도 인증에 실패하는 비율이며 FAR은 정상 사용자가 아님에도 인증에 성공하는 비율이다. 이 두 비율이 같아지는 지점을 EER (Equal Error Rate)이라 한다. EER이 낮을수록 해당 사용자들을 정확하게 식별해 낼 수 있다는 것을 보장한다. 가장 낮은 EER을 찾기 위하여 인증모델과 사용자가 입력한 PIN의 터치 위치데이터 간의 거리차이 허용범위인 파라미터 t의 값은 1~100까지 1픽셀단위로 증가시켜 가면서 실험을 하였으며 인증에 성공하기 위해 최소한으로 성공해야하는 자리수인 파라미터 θ는 K와 $K-1$에 대해서만 실험을 수행하였다.

실험 결과로 각 자릿수에 대해 단 10회 반복 입력을 통해 생성한 인증모델을 가지고도 〔표 2〕와 같이



〔그림 3〕 인터페이스

〔표 2〕 최적의 파라미터 및 EER

자릿수 K	최적 θ	최적 t	EER(%)
4자리	$K-1$	26	8.1
6자리	K	36	6.2
11자리 (전화번호)	$K-1$	32	8.1

낮은 수치의 EER을 얻을 수 있었다. 또한 위의 실험은 동일한 PIN을 가정하고 EER을 측정한 것이므로, 실제 PIN의 사용 예에서와 같이 사용자들의 PIN이 다르다면 더 높은 확률로 사용자들을 구분해낼 수 있을 것이다.

또한, PIN을 등록하고 일정시간이 지난 후에도 같은 인증 성공률을 보이는지 실험하였다. 앞선 실험과 같은 PIN을 사용하였으며 피실험자 5명을 대상으로 일정시간 간격을 두고 총 3회 실시하였다. 피실험자는 앞선 실험과 같이 10회 반복 입력을 통해 자신의 인증 모델을 생성한 후 5회에 걸쳐 인증을 시도한다. 2차, 3차 실험은 1차 실험이 끝나고 각각 1일과 5일이 지난 후 1차 실험에서 생성한 인증 모델에 대해 10회 인증을 시도 하였다.

실험 결과로 〔표 3〕과 같이 1차 실험과 1, 2, 3차 실험을 통합한 EER의 차이는 평균 5.8%로 나타나 사용자가 숫자 정보와 터치 위치정보를 함께 기억하는 데 큰 어려움이 없음을 알 수 있다.

IV. 안정성 분석

제안 방식은 사용자로 하여금 PIN숫자 이외에 추가적인 정보를 기억하게 하여 패스워드 공간의 크기를 늘리는 방법이므로, 단순히 PIN의 구성 자릿수를 늘려 패스워드 공간의 크기를 크게 하는 방법과 비교해 보는 것이 의미가 있다. 이 장에서는 터치 위치데이터 없이 PIN의 길이만을 늘려 제안 방식과 같은 정도의 패스워드 공간을 갖기 위해서는 몇 자리 PIN을 사용해야 하는지를 계산해 보기로 한다.

4.1. 동일한 Keypad를 사용할 때 기존의 PIN 방식과 비교

인증에 사용하는 자릿수를 N이라 하고, 제안한 방식에서 인증모델과 사용자가 입력한 PIN의 위치데이터간의 거리차이 허용범위인 파라미터 t의 평균값 T와 버튼의 면적 S를 다음 식 (4)라고 볼 때 동일한 안전성을 가지는 기존의 PIN방식의 입력횟수 X는 다음 식 (5)를 만족하면 된다. 여기서 $\frac{S}{T^2\pi}$는 본 제안 방법에서 한 버튼 내에서 구분 가능한 터치 위치의 수를 의미한다.

$$S = 150 \times 155,\ T = 31.17 \tag{4}$$

$$10^N \times (\frac{S}{T^2\pi})^N = 10^X \tag{5}$$

〔표 4〕는 $N \in \{4,6,11\}$에 대해 식 (5)를 만족하는 X를 계산한 것이다. 표 4의 결과를 통해 볼 때 동일한 수의 키패드를 가지고 PIN을 입력할 때 약 2배의 입력을 하여야만 기존의 PIN방식이 위치기반 인증방식과 같은 안전성을 가질 수 있음을 확인할 수 있다. 또

〔표 3〕 시간에 따른 최적의 파라미터 및 EER

자릿수 K	1차 실험			1, 2차 실험 통합			1, 2, 3차 실험 통합		
	최적 θ	최적 t	EER(%)	최적 θ	최적 t	EER(%)	최적 θ	최적 t	EER(%)
4자리	$K-1$	20	5.0	K	26	9.8	K	37	11.5
6자리	$K-1$	31	0.0	$K-1$	37	0.0	$K-1$	62	7.5
11자리 (전화번호)	$K-1$	31	1.0	$K-1$	33	4.0	$K-1$	33	4.6

〔표 4〕 동일한 안전성일 때 기존 PIN방식과 자릿수 비교

위치기반 인증(N)	기존 PIN방식(X)
4	7.53
6	11.29
11	20.69

한 태블릿 PC와 같이 스마트폰보다 더 큰 화면을 가지는 모바일 장치에 제안 방법을 적용한다면 버튼 당 터치 위치의 개수 $\frac{S}{T^2\pi}$는 더 커지게 되므로 더 높은 안전성을 기대할 수 있다.

4.2. 터치 위치데이터의 분포를 고려한 안전성 분석

인증모델 생성에 사용하는 터치 위치데이터는 사용자의 입력에 의존하는 만큼 그 분포가 일정 위치에 집중되는 경우가 발생할 수 있는데 3장에서 생성한 인증모델의 210개 터치 위치데이터에 대해 분포를 분석해 본 결과, 특정위치에 편중되는 현상을 발견할 수 있었다. 최악의 경우를 가려내기 위해 파라미터 t의 평균값인 31.17의 반지름을 가지는 원을 버튼 내에서 이동시키면서 가장 많은 점들이 포함되는 경우를 조사한 결과, 210개중 최대 100개가 포함되는 원이 존재함을 확인 하였다. 즉, 공격자가 이 분포를 파악하고 있다면 버튼에서 이 원의 중심점을 터치함으로써 위치를 $\frac{100}{210}$의 확률로 맞출 수 있다는 의미이다. 따라서 인증모델의 터치 위치데이터 분포가 랜덤한 경우를 가정하였던 식 (5)는 사용자의 터치 위치데이터의 분포를 적용할 때 최악의 경우 식 (6)과 같이 나타낼 수 있다. 이를 바탕으로 〔표 4〕를 재구성하면 〔표 5〕를 얻을 수 있다. 이 결과를 통해 볼 때, 터치 위치데이터의 분포를 고려한다면 기존의 PIN방식에서 약 1.32배의 입력을 통해 제안 방식과 동일한 안전성을 얻을 수 있음을 확인할 수 있다.

$$10^N \times (\frac{210}{100})^N = X^N \quad (6)$$

〔표 5〕 위치데이터의 분포를 고려한 안전성 비교

위치기반 인증(N)	기존 PIN방식(X)
4	5.28
6	7.93
11	14.54

V. 결 론

본 논문에서는 기존의 PIN 인증 방식에 위치데이터를 추가한 새로운 인증방법을 제안하였다. 이 방식은 행위기반의 인증방식에 비하여 등록단계에서 상대적으로 적은 양의 입력을 요구함으로써 불편함을 최소화 하였다. 또한 이러한 조건에도 기존 PIN방식보다 높은 안전성을 제공함과 동시에 낮은 EER을 나타냄으로써 효율적으로 사용될 수 있음을 보여주었다. 향후 연구로서, 본 제안 방식의 실용성을 확인하기 위해서는 모바일 장치뿐만 아니라 ATM (Automatic Teller Machine) 등과 같은 다양한 터치스크린 환경에서의 실험이 필요할 것으로 보인다. 특히 같은 PIN에 대해 버튼크기가 다른 ATM과 모바일 장치 간에 호환성을 제공하는 문제 등 다양한 편의성 실험을 수행 할 계획이다. 또한, 기존에 숫자패드 방식의 PIN 입력 방식에 익숙한 사용자들을 효과적으로 교육 시킬 수 있는 방안을 강구하고, 인증시의 불편함을 최소화하기 위해 사용자 평가를 반영하여 인증 방식을 지속적으로 개선하는 방안에 대해서도 연구할 계획이다.

참고문헌

〔1〕 N.L. Clarke and S.M. Furnell, "Advanced user authentication for mobile devices," COMPUTER & SECURITY, vol. 26, pp. 109-119, Aug. 2006.

〔2〕 I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A.D. Rubin, "The design and analysis of graphical passwords," In Proc. of the 8th USENIX Security Symposium, 1999.

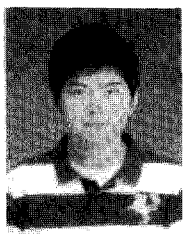
〔3〕 R. Dhamija and A. Perrig, "Deja vu: a user study using images for authentication," In Proc. of the 9th USENIX Security Symposium, 2000.

〔4〕 RealUser, http://www.realuser.com/enterprise/ products/for_windows.htm

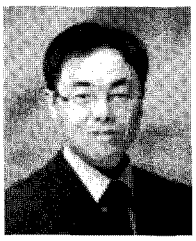
〔5〕 S. Wiedenbeck, J. Waters, L. Sobrado and J.-C. Birget and A. Brodskiy and N. Memon, "Passpoints: design and longitudinal evaluation of a graphical password system," In Proc. of AVI'06, May 2006.

[6] S. Wiedenbeck, J. Waters and J.C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," International J. of Human-Computer, Studies 63, pp. 102-127, Sep. 2005.
[7] Philippe Golle and David Wagner, "Cryptanalysis of a congnitive authentication scheme," SP'07, pp. 66-70, May 2007.
[8] 신동오, 강전일, 맹영재, 양대헌, "S3PAS의 교차 공격에 대한 취약성 분석," 한국정보보호학회 동계학술대회 논문집, 19(2), pp. 409, 2009년 12월.
[9] Chang Soon Kim and Mun-Kyu Lee, "Secure and user friendly PIN entry method," ICCE 2010, pp. 203-204, 2010.
[10] Maja Pusara and Carla E. Brodley, "User re-authentication via mouse movements," CizSEC/DMSEC'04, Oct. 2004.
[11] N.L. Clarke, S.M. Furnell, B.M. Lines and P.L. Reynolds, "Keystroke dynamics on a mobile handset: a feasibility study," Information Management & Computer Security, pp. 161-166, Nov. 2003.
[12] Pilsung Kang, Sunghoon Park, Seong-seob Hwang, Hyoung-joo Lee and Sungzoon Cho, "Improvement of keystroke data quality through artificial rhythms and cues," COMPUTER & SECURITY, vol. 27, pp. 3-11, Feb. 2008.
[13] L.D. Paulson, "Taking a graphical approach to the password," COMPUTER, vol. 35, pp. 19, 2002.
[14] sfr, "http://www.viskey.com/tech.html"
[15] W. Jansen, "Authenticating mobile device users through image selection," Data Security, May 2004.
[16] Xiaoyuan Suo, Ying Zhu and G.Scott. Owen, "Graphical passwords: a survey," ACSAC, 2005.

〈著者紹介〉



김 진 복 (Jin-Bok Kim) 학생회원
2010년 8월: 인하대학교 정보공학계열 학사
2010년 9월~현재: 인하대학교 컴퓨터정보공학 석사과정
관심분야: 정보보호, 유비쿼터스보안 등.



이 문 규 (Mun-Kyu Lee) 종신회원
1996년 2월: 서울대학교 컴퓨터공학과 학사
1998년 2월: 서울대학교 컴퓨터공학과 석사
2003년 8월: 서울대학교 전기컴퓨터공학부 박사
2003년 8월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 인하대학교 컴퓨터정보공학부 조교수
관심분야: 정보보호, 암호학, 컴퓨터이론 등.