情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

한국어 획 기반 그래피컬 패스워드 기법에 관한 연구

고 태 형,[1†] 손 태 식[2], 홍 만 표[2‡]
[1]아주대학교 대학원 컴퓨터공학과, [2]아주대학교 정보컴퓨터공학부

A Study on the Korean-Stroke based Graphical Password Approach

Taehyoung Ko,[1†] Taeshik Shon[2], Manpyo Hong[2‡]
[1]Graduate School of Ajou University, [2]Division of Information Computer Engineering, Ajou University

요 약

테블릿 PC, 스마트폰, 넷북 등 다양한 형태를 가진 스마트 기기의 증가에 따라 그러한 스마트 기기를 기반으로 하는 모바일 환경에서의 정보보호가 큰 이슈로 떠오르고 있다. 이때 안전하게 패스워드를 입력하는 것은 매우 중요한 요소이며, 다양한 형태의 모바일 기기에서는 기기 자체의 하드웨어 제약 사항에 따라 키보드와 마우스 등의 보조 입력장치를 구비하기 힘든 어려움을 가진다. 또한 입력 정보들이 주로 터치스크린을 통해서 이뤄지기 때문에 정확도가 떨어질 수 있는 문제점도 가지게 된다. 앞서 언급한 문제들 때문에 현재 거의 보편적으로 사용되는 4자리 패스워드 기반의 인증 기법이 향후에는 점차 문자 기반에서 그래피컬 패스워드로 변화 할 것으로 예상되며, 이러한 그래피컬 패스워드는 문자기반의 패스워드에 비해서 사용하기 쉽고, 엿보기 공격에 강한 특성을 가지는 것으로 알려져 있다. 그러므로 본 논문에서는 엿보기 공격을 방어하기 위해서 한글의 자모를 분해하여 도출된 5개의 획 기반으로 이루어진 새로운 그래피컬 패스워드 기법을 제안하고 검증하였다.

ABSTRACT

With increasing the number of smart device such as Tablet PC, smart phone and netbook, information security which based on smart device in mobile environment have become the issue. It is important to enter a password safety. In various types of mobile devices, because of hardware limitation of device, it is difficult that to equip secondary input device such as keyboard and mouse. Also, a loss of accuracy becomes a problem because input information was entered by touch screen. Because of problem mentioned above it can be predicted to change password scheme text based password scheme to graphical password scheme, graphical password scheme is easy to use and is resistant to shoulder surfing attack. So this paper proposes new graphical password scheme based 5 strokes which are made by decomposed the Korean to defend against shoulder surfing attack.

Keywords: Graphical password, Shoulder surfing attack, stroke

I. 서 론

오늘날 컴퓨터가 점점 발전되어 오면서 컴퓨팅 패러다임을 많은 변화를 겪고 있다. 그것은 바로 기존의 데스크탑 환경에서 모바일 컴퓨팅 환경으로 변화되고 있는 것이다. 이러한 컴퓨팅 환경의 변화는 스마트폰의 보급과 발전으로 인해서 더욱 가속화 되었다.

모바일 컴퓨팅 환경은 뛰어난 휴대성과 무선 네트워크의 발전으로 어디서든지 정보에 쉽게 접근 가능한 장점을 가지고 있다. 이런 이유 때문에 많은 사람들이 자신의 모바일 기기를 이용하여 모바일 뱅킹, 주식 거래 등의 금융 거래를 하고, SNS(Social Network

접수일(2011년 5월 31일), 수정일(1차: 2011년 9월 19일, 2차: 2012년 1월 4일), 게재확정일(2012년 1월 21일)
† 주저자, shiichiro@ajou.ac.kr
‡ 교신저자, mphong@ajou.ac.kr

Service)와 같은 커뮤니티 활동에도 많이 사용하고 있다. 그렇기 때문에 모바일 기기에 많은 민감하고 사적인 정보들이 많이 존재하게 된다. 따라서 이러한 정보들을 안전하게 가지고 있는 것과 안전하게 사용자 인증하는 것이 매우 중요하다. 하지만 이러한 모바일 컴퓨팅에서 몇 가지 단점을 가지고 있는데, 첫 번째는 입력방식의 제한이다. 기존 데스크탑 환경에서는 키보드와 마우스의 입력장치가 존재했었는데, 모바일 컴퓨팅 환경에서는 휴대성을 위해서 이러한 장치들을 구비하기가 힘들다. 그렇기 때문에 대부분의 기기는 터치스크린을 이용한 입력을 주로 사용하고 있다. 이 기법은 입력할 수 있는 공간이 터치스크린 화면 크기에 종속되기 때문에 많은 제약을 가지고 있다. 때문에 입력기법에 있어서 정확한 입력을 하기에 취약성을 가지고 있다. 또한 패스워드 설정에 있어서 기존의 글자 기반의 패스워드는 모바일 디바이스에 적용하기에는 입력장치의 제한에 있어서 취약성을 가지고 있다. 두 번째에는 뛰어난 이동성으로 인해서 개인정보가 쉽게 노출 될 수 있다는 점이다. 이것은 바로 엿보기 공격과 귀결되는 사항이다. 엿보기 공격이란 사용자가 자신의 비밀 정보를 입력할 시에 그 장면을 공격자가 엿보는 기술로 개인정보를 노출시키게 된다. 뛰어난 휴대성으로 인해서 어디에서나 서비스를 제공받을 수 있는 반면에 자신의 정보 또한 노출되기 쉽기 때문에 이 부분에 있어서 조심해야 된다. 이 때문에 모바일 디바이스에 있어서 안전하게 개인정보를 입력하는 것은 중요한 사항이다.

이러한 요인들에 인해서 모바일 컴퓨팅 환경에 있어서 기존의 문자 기반 패스워드는 제한된 입력 장치로 인해서 정확한 패스워드를 입력하기 힘들고, 엿보기 공격에 쉽게 노출 되어있기 때문에 안전한 인증 방법으로 사용하기에 힘들다. 따라서 이를 보완할 새로운 패스워드 기법이 필요하게 된다. 새로운 패스워드 기법은 제한된 입력장치로 인해서 입력하기에 쉬워야 하며, 또한 패스워드가 기억하기 쉬운 방법이어야 한다. 그리고 뛰어난 이동성으로 개인정보가 쉽게 노출 될 수 있기 때문에 엿보기 공격에 강해야한다. 때문에 이러한 요건들을 충족시키기 위해서 문자기반의 패스워드에 비해서 사용하기 쉽고 엿보기 공격에 강한 특성을 지닌 그래피컬 패스워드(graphical password)를 사용해야 된다. 하지만 기존 그래피컬 패스워드를 입력하기 쉬운 방법은 상대적으로 엿보기 공격에 약하고, 엿보기 공격에 강한 방법은 입력하기에 어려운 단점들이 보인다. 그렇기 때문에 본 논문에서는 이러한 단점들을 보완하는 그래피컬 패스워드 기법을 제안한다.

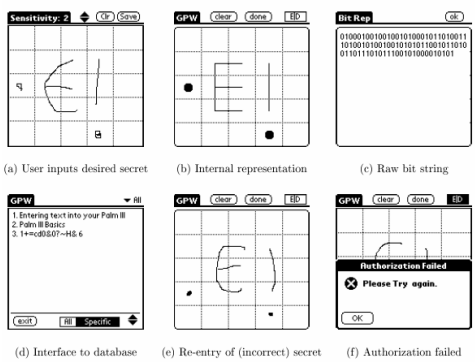
본 논문의 구성은 다음과 같다. 2장에서는 그동안 연구되었던 그래피컬 패스워드 기법을 살펴본다. 3장에서는 제안하는 방법에 대해서 설명한다. 4장에서는 제안하는 방법을 실제 안드로이드 어플리케이션으로 제작하여 사용한 결과를 나타낸다. 5장에서는 실험을 통해서 제안하는 방법의 우수성을 검증하고 마지막 장에서는 결론과 함께 추후 연구 방향에 대해서 설명한다.

II. 관련연구

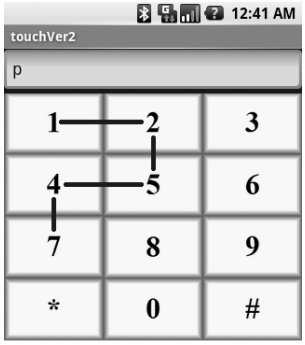
현재까지 발전되어온 그래피컬 패스워드 기법을 살펴보면 크게 두 가지의 기법으로 나눌 수 있다. 첫 번째 기법은 상기기반 그래피컬 패스워드 기법이다. 이 기법은 사용자가 미리 설정해둔 패스워드를 인증 시에 그대로 입력하여서 인증을 수행하는 기법이다. 이 기법을 사용하면 사용자 입력의 자유도가 높아진다. 두 번째 기법은 인지기반 그래피컬 패스워드 기법이다. 사용자는 하나 또는 여러 개의 그림을 패스워드로 등록한 후, 인증 시에 해당하는 그림들을 선택하거나 이 그림들을 이용하여서 인증하는 기법이다.

2.1 상기기반 그래피컬 패스워드 기법

그래피컬 패스워드가 가져야 하는 특징 중 하나는 사용자가 입력하기 쉬운 방법이어야 한다. 그렇기 때문에 사용자가 패스워드 설정 시에 했던 행동을 그대로 하는 기법인 상기기반 그래피컬 패스워드 기법을 사용하면 이 조건에 부합하게 된다. 그러면 상기기반



〔그림 1〕 Draw-a-Secret(DAS)〔1〕



〔그림 2〕 I-Horng Jeng가 발표한 기법〔2〕

〔그림 3〕 Pass-Objects〔4〕

그래피컬 패스워드 기법들을 살펴보겠다.

DAS(Drow-a-Secret)〔1〕는 1999년에 제안된 그래피컬 패스워드 기법이다. 이 기법에서는 사용자가 자신의 패스워드를 입력을 위한 일정한 공간위에 그리도록 하는 기법이다. 이 기법에서 사용자의 패스워드를 입력받기 위해서 입력 공간을 N * N크기의 그리드로 나누어서 사용자가 그리는 패스워드를 각 그리드 좌표에 할당하는 기법을 사용한다. 〔그림 1〕을 살펴보면 이 기법을 사용하는 화면을 볼 수 있다. 이 기법은 입력하기에는 쉽지만 엿보기 공격에 있어서는 취약성을 보이게 된다.

2009년에 I-Horng Jeng 등에 의해서 발표된 그래피컬 패스워드 기법이다〔2〕. 이 기법은 앞서 살펴본 DAS와 다르게 PIN 기법의 패스워드를 입력하기 위한 전화기 숫자버튼을 그대로 이용한다. 그리고 패스워드의 한 글자를 입력하기 위한 터치는 단 한 번의 터치를 한붓그리기를 이용해서 입력한다. a부터 z까지 각 알파벳은 각각의 한붓그리기로 할당되어져 있다. 〔그림 2〕는 'p'를 입력하는 화면을 보여 준다. 이 기법을 이용하게 되면 패스워드 입력하는 환경은 기존의 기법과 동일하여서 사용자에게 친밀감을 주는 장점을 가지고 있다.

2.2 인지기반 그래피컬 패스워드

사람의 기억에 대한 연구결과에 따르면 사람은 글자보다 그림을 더 잘 기억한다고 한다〔3〕. 따라서 그림의 조합을 인지기반 그래피컬 패스워드 기법을 사용하면 외우기 쉬운 패스워드를 만들 수 있다.

첫 번째 살펴볼 기법은 Pass-Objects〔4〕이다. Pass-Objects는 Sobrado and Birget에 의해서 2002년에 발표된 기법이다. 이 기법은 엿보기 공격을 방지하기 위해서 만들어졌다. 사용자는 인증에 앞서 패스이미지를 미리 설정한다. 그 후 인증 단계에서 패스이미지를 포함하여 많은 다른 이미지를 보여준다. Pass-Objects의 첫 번째 방법은 그 후 사용자가 패스이미지를 포함하는 다각형을 그려서 인증을 시도한다. 〔그림 3〕을 보면 패스이미지는 빨간 동그라미가 쳐져있는 이미지이다. 사용자는 이 이미지들로 이루어진 보라색영역 모양의 다각형을 그리면 된다. 두 번째 방법은 일정 모양의 프레임을 이동시켜 해당 프레임 안에 모든 패스이미지가 위치하게 되면 인증이 되는 기법이다. 이 기법을 사용하게 되면 사용자는 패스이미지만 기억하면 된다. 하지만 패스이미지 외에 다른 이미지가 너무 많은 경우에는 인증 시에 오랜 시간이 걸릴 것으로 예상된다.

다음에 살펴볼 기법은 2010년에 Haichang Gao 등에 의해서 발표된 기법〔5〕이다. 이 기법은 엿보기 공격을 방지하기 위해서 개발된 이미지 기반 패스워드이다. 이 기법에서는 n * k크기의 그리드에 이미지를 그려 놓고 미리 사용자가 지정한 패스이미지의 순서대로 드래그(drag)를 통해서 인증절차를 가지게 된다. 이 기법에서는 인증시도시마다 모든 이미지들이 랜덤하게 재배치된다. 이 기법에서 특이점은 패스이미지를 선택하는 부분이다. 패스이미지를 선택할 때 무작정 선택하는 것이 아니라 일련의 이야기를 가지고 이미지를 선택하도록 한다. 예를 들어서 남자, 여자, 아기, 집 그리고 케이크를 패스이미지로 선택한다면 '한 부부가 아기와 함께 집에서 케이크를 먹으려한다'라는 이야기로 패스이미지를 선택하도록 한다. 이러한 기법을 사용하면 사용자는 패스이미지를 외우기에 좀 더 쉬워질 것이다. 〔그림 4〕를 살펴보면 위에서 예로 들었던 패스이미지들을 입력하는 예를 보여준다.

〔그림 4〕 Haichang Gao등에 의해서 발표된 기법〔5〕

2.3 기존 기법들의 비교

앞에서 살펴본 기존기법들의 장단점을 표로 정리해 보았다.

〔표 1〕을 살펴보면 몇 가지 특징을 알 수 있다. 일단 패스워드 기법의 사용성을 살펴보면 상기기반 그래피컬 패스워드 기법들은 사용하기 편한 장점이 있다. 반면에 인지기반 그래피컬 패스워드 기법들들은 여러 그림들을 이용해서 인증 절차를 수행하기 때문에 사용자가 사용하기에는 혼동을 가져온다는 단점이 있었다. 그리고 엿보기 공격측면에서 사용자와 그 외에 스크린을 볼 수 있는 사람에게 드러난 정보를 살펴보면 상기기반 그래피컬 패스워드 기법들은 직접 그리기 때문에 사용자가 입력하는 정보가 모두 외부에 드러나는 것을 볼 수 있다. 하지만 인지기반 그래피컬 패스워드 기법들을 살펴보면 많은 이미지들을 이용하기 때문에 이 중에서 어느 것이 인증에 필요한 이미지인지 쉽게 드러나지 않는다. 이를 종합하면 상기기반 그래피컬 패스워드 기법들은 사용하기는 쉬운 반면에 외부에 드러나는 정보가 많고, 인지기반 그래피컬 패스워드 기법들은 사용하기 번거로운 반면에 외부에 드러나는 정보가 적다.

이를 토대로 볼 때 새로운 그래피컬 패스워드 기법은 엿보기 공격에 강하고 입력하기 쉬운 방법이어야 한다.

III. 제안 기법

3.1 한글의 획 분해

이 방법은 한글을 대상으로 하고 있다. 여기서 말하는 획도 한글을 구성하는 자음과 모음의 획을 말하는 것이다. 한글을 사용한 이유는 패스워드를 기억하기 쉽게 만들기 위해서이다. 패스워드를 자신이 알고 있는 단어나 단어의 자음만으로 만들게 된다면 사용자는 패스워드를 외우기 쉬울 것이다.

그리고 엿보기 공격을 방어하기 위해서 획 기반 입력시스템을 이용한다. 획 기반 입력시스템이란 한글의 자음과 모음의 획을 모두 분해해서 단순화 한 후에 입력하는 것이다. 예를 들면 'ㄱ'을 입력할 경우에는 왼쪽으로 가로획과 아래로 내리는 세로획으로 이루어져 있다. 이런 식으로 모든 한글을 획으로 분해해서 입력

〔표 1〕 각 그래피컬 패스워드들의 장점, 단점

패스워드기법		인증절차	사용자에게 드러난 정보	장점	단점
상기기반 그래피컬 패스워드 기법	DAS〔1〕	일정 공간에 그려서 인증	그리드에 쓰이는 모양이 드러남	입력이 빠르다 입력이 쉽다.	엿보기 공격에 약함 그린 것의 오차를 어디까지 허용해야 하는 문제
	I-Horng Jeng〔2〕	숫자패드에 매 글자마다 한붓그리기로 글자 입력하여 인증	쓰이는 모양이 드러남 시작점이 다를 수 있음	패스워드를 외우기 쉬움	엿보기 공격에 약함
인지기반 그래피컬 패스워드 기법	Pass-Objects〔4〕	패스이미지를 포함하는 다각형을 그려서 인증	많은 이미지들이 드러남 패스이미지가 드러나는 확률이 적어짐	엿보기 공격에 강함	패스이미지 외에 이미지가 많을 경우에 사용하기 불편함
	Haichang Gao〔5〕	시작점부터 끝점까지 패스이미지들을 드래그하여 인증	많은 이미지가 드러남 패스이미지가 드러나는 확률이 적어짐	패스워드를 기억하기 쉬움	길을 찾는데 시간이 걸림

하는 것이다. 한글에서 사용하는 획을 살펴보면 세로획, 가로획, 오른쪽에서 대각선획, 왼쪽에서 대각선획, 원이 있다.

세로획 : ↓

가로획 : →

오른쪽에서 대각선획 : ↙

왼쪽에서 대각선획 : ↘

원 : O

각 한글의 자음과 모음에서 사용하는 획은 〔표 2〕를 살펴보면 알 수 있다.

〔표 2〕 한글 자모에서 사용하는 획

자모	사용하는 획
ㄱ	→ ↓
ㄴ	↓ →
ㄷ	→ ↓ →
ㄹ	→ ↓ → ↓ →
ㅁ	↓ → ↓ →
ㅂ	↓ ↓ → →
ㅅ	↙ ↘
ㅇ	O
ㅈ	→ ↙ ↘
ㅊ	↓ → ↙ ↘
ㅋ	→ ↓ →
ㅌ	→ ↓ → →
ㅍ	→ ↓ ↓ →
ㅎ	↓ → O
ㅏ	↓ →
ㅑ	↓ → →
ㅓ	→ ↓
ㅕ	→ → ↓
ㅗ	↓ →
ㅛ	↓ ↓ →
ㅜ	→ ↓
ㅠ	→ ↓ ↓
ㅡ	→
ㅣ	↓

3.2 엿보기 공격에 강한 입력방법

엿보기 공격은 사용자의 입력을 훔쳐보고 그것을 이용해서 인증을 시도하는 방법이다. 그렇기 때문에 많은 방법에서 엿보기 공격을 막기 위한 조취를 취하고 있다. 엿보기 공격을 막기 위해서 3.1에서 단순화한 획들의 중심점을 원점으로 하여서 입력을 시도한다. 5가지 획들의 중심점을 원점으로 하여서 살펴보면 〔그림 5〕과 같다.

〔그림 5〕에서 최종적으로 나온 모양을 살펴보면 매우 단순화된 모습을 확인할 수 있다. 사용자는 〔그림 5〕과 같은 획이 그려진 곳에 드래그를 통해서 자신이 원하는 획을 입력하여서 인증을 진행하게 된다.

〔그림 5〕 획들의 병합

3.3 제안방법의 적용

본 논문에서 제안하는 그래피컬 패스워드 기법은 모바일 디바이스의 여러 가지 어플리케이션에 적용 가능하다. 첫 번째로 적용 가능한 영역은 모바일 디바이스의 잠금 기능이다. 현재 모바일 디바이스에서 사용하는 잠금 해제 방법은 PIN번호 입력, 패턴 입력, 단순한 슬라이드 등이 있다. 기존 방법들은 엿보기 공격에 약한 특성을 가지고 있기 때문에 제시하는 방법을 사용하면 안전하게 잠금 해제를 할 수 있다. 또한 사용자들은 잠금 해제를 번거롭지 않게 하려는 경향이 있기 때문에 간단하게 사용하는 이 기법이 좋을 것이다. 두 번째로 적용 가능한 영역은 모바일 공인인증서이다. 모바일 공인인증서는 주로 모바일 뱅킹할 때 사용된다. 그렇기 때문에 모바일 공인인증서를 사용 할 때 안전하게 패스워드를 입력하는 것이 중요하다. 제안하는 방법은 엿보기 공격에 강한 입력방법이기 때문에 해당 영역에서 사용하면 안전하게 사용 할 수 있다.

사용 예를 살펴보면 사용자가 패스워드로 '한'이라는 글자를 설정한다고 가정한다. 그렇게 되면 패스워드 설정 시에 '↓ → O ↓ → ↓ →'를 입력하면 설정이 완료된다. 그 다음에 로그인 할 시에 동일한 입력을 하게 되면 로그인이 완료된다.

IV. 구현결과 및 검증

4.1 구현

3장에서 제안한 획 기반 그래피컬 패스워드 기법의 구현에 앞서 대략적인 프로그램의 흐름도(flow chart)를 아래 〔그림 6〕에서 확인 할 수 있다. 4자리 PIN은 10^4의 패스워드의 개수를 가지고 제안하는 방법은 6개의 획으로 이루어 졌을 때 5^6의 패스워드의 개수를 가진다. 따라서 최소 6개의 획으로 이루어져 있어야 4자리 PIN보다 많은 패스워드의 개수를 가진다.

〔표 3〕 패스워드 입력 알고리즘

패스워드 입력 알고리즘 1 단계 : 획의 입력을 기다림 2 단계 : 획의 종류 검정 3 단계 : 획이 끝점까지 도달하는지 검정 4 단계 : 입력되는 획 수(N_0) 계산 if $N_0 \neq N$ then 1 단계로 or 계속 (N = 저장된 패스워드의 획 수)

($10^4 < 5^6$) 그렇기 때문에 패스워드의 최소 길이는 6개여야 한다.

패스워드 입력 알고리즘을 살펴보면 〔표 3〕과 같다. 각 획마다 빨간 점을 시작점으로 하여 각 획을 인식하게 된다. 획의 종류를 알아낸 후 그 입력이 획의 끝까지 이루어지면 하나의 획으로 인식하게 된다. 그 후 입력되는 획수와 저장된 패스워드의 획수가 일치되었을 때 입력된 획과 저장된 패스워드를 비교하게 된다.

4.2 구현 결과

모바일 컴퓨팅 환경을 대상으로 했기 때문에 널리 사용하고 있는 Android OS에 구현하였다. 표4는 구현된 어플리케이션을 실행하는 하드웨어의 상세사양

〔표 4〕 HTC desire hardware spec

명칭	상세사양
디스플레이	4.3 인치 480 x 800 WVGA 터치 스크린
CPU	1GHz (snapdragon)
휴대폰 내부 저장소	1.5 GB
RAM	768 MB
Wi-Fi®	IEEE 802.11 b/g/n
3G 다운로드 속도	14.4 Mbps
3G 업로드 속도	5.76 Mbps
Bluetooth®	Bluetooth® 2.1

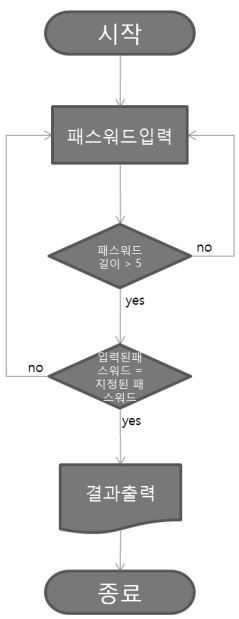
이다. 구현에 사용한 언어는 자바를 사용하고, 이클립스(eclipse)를 이용하여서 구현하였다.

대상 OS : 안드로이드 2.2 프로요(android 2.2 froyo)

대상 기기 : HTC desire

아래 〔그림 7〕에서는 안드로이드 어플리케이션으로 구현된 모습을 볼 수 있다.

좀 더 사용자에게 자신이 입력하는 것을 알려주기 위해서 각 획의 시작점에는 빨간 동그라미 아이콘을



〔그림 6〕 제안한 그래피컬 패스워드 기법의 흐름도

〔그림 7〕 구현된 어플리케이션

넣었다. 이 아이콘은 사용자의 입력에 따라 같이 움직여서 좀 더 명확한 입력을 제공한다. 또한 원은 원을 따라서 드래그 하기에는 시간이 많이 걸리고 정확도도 떨어지기 때문에 가운데 원점 부분을 터치하도록 하였다.

각 획들은 빨간 점을 시작점으로 반대편 끝까지 드래그 하여 이동 시킬 때 하나의 획으로 인식 된다. 현재 화면에서는 디버그 버전이기 때문에 입력되는 획들을 확인 할 수 있는 글상자가 존재한다. 가로획은 1, 세로획은 2 등 각 획들이 숫자에 매핑(mapping)되어서 입력되는 것을 볼 수 있다.

4.3 구현 결과 검증

기존의 그래피컬 패스워드를 살펴보면 패스워드의 기억성을 증가시키기 위해서 여러 가지 방법을 사용하였다. 직접 자신이 해당하는 그림을 그리는 방법, 기억하기 쉬운 이미지를 사용하는 방법과 이미지들의 조합을 이야기로 만드는 방법 등이 있었다. 하지만 제안한 기법에서는 단순하게 패스워드에 해당하는 문자만 기억하면 된다. 다른 복잡한 그래피컬 패스워드 기법에 비해서 기억해야 될 패스워드의 길이가 짧고 단순하기 때문에 패스워드를 기억하기가 쉽다. 또한 한글의 자모에서 5개의 획을 도출하여 사용하였기 때문에 더욱 기억성이 좋다. 다른 패스워드와 비교하여 본다면 일반적인 숫자의 경우에는 0~9까지 10개의 숫자를 사용하게 되고, 문자 기반의 패스워드의 경우에는 a-z까지 26개의 문자를 사용하게 된다. 이것들과 비교하여도 사용자가 외워야 되는 요소가 작아지기 때문에 기억성 측면에서 더욱 뛰어나다고 볼 수 있다.

모바일 디바이스의 제한된 입력 방법 때문에 사용자들은 텍스트 기반의 패스워드를 빠르고 정확하게 입력하기가 힘들었다. 하지만 제안한 기법을 사용하면 자신이 설정한 패스워드 문자를 입력하기에 쉽다. 그 이유는 한글의 획을 단순화하여서 입력부에 나타냈기 때문이다. 사용자는 자신이 생각하는 글자를 직접 쓴다는 생각으로 입력부에 있는 각 획들을 드래그하면 쉽게 입력할 수 있다.

4.4 구현결과의 보안적 검증

본 논문에서 제안한 그래피컬 패스워드 기법을 사용 했을 때 예상되는 위협들은 엿보기 공격, 무작위 대입 공격 (Brute force attack) 등이 있다.

〔표 5〕 자모의 여러 가지 표현

자모	사용하는 획
ㅁ	↓ → ↓ →
	↓ ↓ → →
ㅂ	↓ ↓ → →
	↓ → → ↓
ㅋ	→ ↓ →
	→ → ↓
ㅌ	→ ↓ → →
	→ → → ↓
	↓ → → →

4.4.1 엿보기 공격

본 논문에서 그래피컬 패스워드가 가장 고려한 보안성 측면은 엿보기 공격이다. 모바일 디바이스의 이동성 때문에 그만큼이나 패스워드가 외부에 노출되게 된다. 이를 해결하기 위해서 제안한 기법에서는 한글의 획을 분해하여서 사용하였다. 한글의 획을 분해하여서 단순화하였기 때문에 공격자가 엿보기 공격을 한다고 하여도 실제로 무엇을 입력하는지 알아내기가 어렵다. 또한 한글의 획을 쓰는 순서가 사람에 따라서 다를 수도 있다. 이 때문에 각 사용자의 개성에 맞게 입력을 하게 된다면 엿보기 공격에 더욱 강한 패스워드가 된다. 예를 들어 'ㅂ'을 입력한다고 할 때 사용하는 획은 ↓ ↓ → → 이다. 하지만 사람에 따라서 ↓ → → ↓ 가 될 수도 있다. 이러한 다양성이 오히려 엿보기 공격을 하는 공격자에게는 혼란을 가져올 수 있다. 'ㅂ'과 비슷하게 같은 자모인데 다른 형식으로 쓸 수 있는 경우는 살펴보면 〔표 5〕에 나타나 있다.

4.4.2 무작위 대입 공격

무작위 대입 공격을 살펴보면 입력 가능한 획을 모두 입력해보는 방법이다. 제안하는 그래픽 패스워드 기법에서 사용하는 획의 종류는 모두 5가지이다. 그러므로 N개의 획으로 이루어 졌다고 가정했을 때 가능한 입력방법의 수는 5^N번이다. 이에 비교하여서 숫자 기반 패스워드인 PIN을 살펴보면, PIN은 0부터 9까지의 숫자를 가지고 있다. 그렇기 때문에 PIN은 N개의 숫자를 입력할 때 10^N개의 가능한 입력방법을 가지고 있다. 보통 만일 획수를 6개 이상으로 하게 된다면 보통 스마트폰에서 사용하는 4자리의 PIN 보다 강력한 보안성을 가진다고 볼 수 있다.

4.4.3 각 공격에 대한 그래피컬 패스워드의 비교

엿보기 공격과 무작위 대입 공격에 대해 각 그래피컬 패스워드들을 살펴보면 표 6과 같다.

이 표를 살펴보면, 상기기반 그래피컬 패스워드 기법들은 사용자가 그리는 당시에는 많은 정보가 노출되게 된다. 하지만 무작위 대입 공격을 시도하기 위해서는 많은 어려움을 가진다. 인지기반 그래피컬 패스워드 기법들은 엿보기 공격을 시도 할 때 많은 이미지들을 사용하기 때문에 공격자는 혼동을 가지게 된다. 그리고 무작위 공격을 할 때에는 패스 이미지의 숫자에 따라서 공격의 가능성이 달라진다. 패스 이미지가 많을수록 공격 가능성이 낮아지는데, 그만큼 사용자가 패스워드를 입력하기에 힘들어 진다. 제시하는 기법은 엿보기 공격 시에 실제 사용하는 획은 드러나지만 사용하는 획도 5개이기 때문에 빠르게 입력하는 획의 조합을 다 기억하지 못하면 공격을 할 수 없다. 그리고 무작위 공격 측면에서는 획의 수에 따라서 공격 가능성이 변화한다. 4.3.2장에서 보았듯이 패스워드가 N개의 획으로 이루어 졌다고 할 때, 가능한 입력방법의 수는 5^N 번이다. 따라서 무작위 공격의 성공 가능성 $(\frac{1}{5})^N$은 이다.

V. 실험

3장과 4장에서는 다른 기법들과의 비교, 분석을 통해서 본 기법의 우수성을 알아보았다. 이번 5장에서는 직접적인 실험을 통해서 본 기법의 우수성을 알아보겠다. 첫 번째 알아 볼 것은 사용 시간의 비교이고, 두 번째는 패스워드 입력의 정확도이다. 세 번째로 알아 볼 것은 엿보기 공격에 대한 견고성을 측정하고자 한다.

5.1 실험 계획

제안하는 기법의 우수성을 검증하기 위해서 크게 2가지로 나누어서 실험을 진행하였다. 첫 번째 실험은 본 기법을 사용하였을 때 걸리는 입력시간을 체크하고 패스워드의 정확도를 비교하는 실험이다. 이를 위해서 20명의 참가자(대학생과 대학원생)를 모집하여서 실험을 진행하였다. 이 실험은 일반적인 영숫자 패스워드와 본 기법을 비교하여 우수성을 검증한다. 두 번째 실험은 엿보기 공격에 어느 정도 강한지 알아보는 실험이다. 이 실험에서는 3명씩 8조를 이뤄서 총 24명의 참가자를 모집하여서 수행하였다. 이 실험은 영숫자 패스워드와 본 기법을 사용하였을 때 엿보기 공격 수행 시 공격이 얼마나 성공하는지 검증하는 실험이다.

5.2 실험

첫 번째 실험은 다음과 같은 순서에 따라서 진행하였다.

1. 실험의 참가자들은 제안하는 기법의 기본적인 원리와 실제로 구현된 어플리케이션을 이용해서 몇 번의 로그인 시도를 통해 제안하는 기법을 숙지한다.
2. 참가자들이 제안하는 기법을 이용하여서 최소 6번의 획으로 구성된 패스워드를 생성하는데 걸린 시간을 측정한다.

〔표 6〕 각 공격에 대한 그래피컬 패스워드 기법 비교

패스워드 기법		엿보기 공격	무작위 대입 공격
상기기반 그래피컬 패스워드 기법들	DAS〔1〕	패스워드의 모양이 공격자에게 확연히 드러남	입력 가능한 모양이 많기 때문에 무작위 대입 공격이 어려움
	I-Horng Jeng〔2〕	입력하려는 문자의 모양이 드러남	알파벳 총 개수*2개만큼의 시도로 공격 가능
인지기반 그래피컬 패스워드 기법들	Pass-Objects〔4〕	패스이미지들의 영역이 보이지만 정확한 이미지를 알아 낼 수 없음	입력 가능한 모양이 많기 때문에 무작위 대입 공격이 어려움
	Haichang Gao〔5〕	패스이미지로 설정 가능할 만한 후보 이미지가 드러남	중복을 허용 하는 입력이기 때문에 무작위 대입 공격이 어려움
획기반기법	제안하는 기법	사용하는 획이 드러나지만 같은 문자에도 여러 입력 방법이 존재하기 때문에 입력하는 문자를 알아내기 힘듬	획의 수가 N개일 때, $(\frac{1}{5})^N$의 확률로 무작위 공격 성공

3. 패스워드를 생성한 후 총 10번의 성공적인 인증 시도를 통해서 인증실패 횟수와 인증하는데 걸리는 모든 시간을 측정한다.
4. 일반적인 영숫자 패스워드를 이용하여서 최소 6자리의 패스워드를 생성하는데 걸린 시간을 측정한다.
5. 패스워드를 생성한 후 총 10번의 성공적인 인증 시도를 통해서 인증실패 횟수와 인증하는데 걸리는 모든 시간을 측정한다.

두 번째 실험은 다음과 같은 순서로 진행하였다.

1. 실험의 참가자들은 3인이 1조로 이루어서 기본적인 제안하는 기법에 대한 설명과 사용법을 숙지한다.
2. 세 명중에서 한명을 피공격자로 선정한다. 나머지 두 명은 공격자로 선정한다.
3. 피공격자로 선택된 실험자는 본 기법을 이용하여서 자신의 패스워드를 생성한다.
4. 피공격자는 자신의 패스워드를 3회 인증 시도한다. 이 사이에 공격자들은 피공격자가 설정한 패스워드를 추측한다.
5. 3번의 인증이 종료된 후 공격자들은 자신이 추측한 패스워드를 이용하여 인증을 시도한다.
6. 피공격자들에게 3번의 인증 기회를 주어 몇 번 성공하였는지 횟수를 측정한다.
7. 1번에서 6번까지의 과정을 일반적인 영숫자 패스워드를 이용하여서 수행한다.

5.3 실험 결과

5.3.1 패스워드 생성 및 사용 시간 실험

패스워드를 생성하는데 걸린 평균 시간은 아래 〔표 7〕과 같다. 제안하는 기법을 사용하여 패스워드를 생성하는데 걸린 평균 시간은 13.86초였다. 영숫자를 사용하여 패스워드를 생성하는 경우에는 15.252초가 소요되었다. 이는 패스워드를 설정 시에 기존 키보드 자판을 이용해서 입력하는데 오랜 시간이 걸린다는 것을 볼 수 있다. 제한된 스크린의 크기 때문에 기존의 키보드 배열이 스마트폰에서는 입력하기 어렵다는 것을 알 수 있었다.

실험을 통해서 알아낸 패스워드를 생성하는데 걸린 시간의 유의미성을 검증하기 위해서 t-test를 이용하여서 검증하였다. 제안하는 기법에 대해서 t-test를 한 결과 $t(18)=2.68$, $p<0.020$로 이 값은 유의미하다는 것을 알 수 있었다. 영숫자의 경우에도 $t(18)=2.945$, $p<0.012$로 유의미한 평균값이라는 결과를 얻었다. 이를 통해서 두 평균값이 모두 유의미하고 같은 표본에서 나왔음을 알 수 있다.

〔표 7〕 패스워드 생성시간

	사용 기법	평균 시간(초)
패스워드 생성시간	제안하는 기법	13.836
	영숫자	15.252

패스워드 이용에서는 위에서 생성된 패스워드를 이용해서 10번 로그인 하였을 때의 시간을 측정하고 패스워드를 이용하여서 로그인할 때 몇 번 잘못 입력하였는지 측정하였다. 표8을 보면 제안하는 기법을 이용하여서 로그인 하는데 걸린 평균 시간은 104.17초이다. 영숫자를 이용하여서 로그인 하는데 걸린 평균 시간은 81.765초이다. 로그인하는데 걸린 시간을 t-test를 이용해서 검증을 해보면, 제안하는 기법에 대해서 t-test를 한 결과 $t(18)=6.70$, $p<2.1970E-5$로 이 값은 유의미하다는 것을 알 수 있었다. 영숫자의 경우에도 $t(18)=10.284$, $p<2.6427E-7$로 유의미한 평균값이라는 결과를 얻었다. 앞서 패스워드를 생성하는데 걸린 시간은 제안하는 기법이 더 적게 걸렸었는데 10번 로그인하는데 걸린 시간이 걸린 이유를 살펴보면 아래에 있는 로그인 시 틀린 횟수를 보면 알 수 있다.

로그인시 틀린 횟수를 살펴보면, 제안하는 기법은 1.46번 잘 못 입력하였고 영숫자 패스워드는 1.07번 잘 못 입력한 것을 볼 수 있다. 이는 제안하는 기법이 영숫자에 비해서 실험의 참가자들에게는 생소한 기법이기 때문에 로그인 시 틀린 횟수가 더 많다. 그렇기 때문에 생성하는데 걸린 시간이 짧았음에도 불구하고 10번 로그인 하는데 걸리는 시간 평균값이 약 20초 더 걸렸다. 이를 각 횟수로 나눠보면 약 2초의 시간이 더 걸렸다. 만일 제안하는 기법을 참가자들에게 좀 더 익숙하게 한다면 더 좋은 결과가 있을 것이다.

〔표 8〕 로그인 시간, 로그인 시 틀린 횟수

	사용 기법	평균 값
10번 로그인 시간	제안하는 기법	104.17 (초)
	영숫자	81.765 (초)
로그인 시 틀린 횟수	제안하는 기법	1.46 (번)
	영숫자	1.07 (번)

5.3.2 엿보기 공격 실험

엿보기 공격 실험에서는 3명씩 조를 이루어서 총 8조가 실험을 진행하였다. 각 조마다 공격자와 피공격자를 나누어서 실험을 진행하였는데 각 조안에서 공격자와 피공격자를 돌아가며 수행하였다. 한 조당 3번씩 총 24회의 실험이 실시되었다. 한 번의 실험마다 공격자는 2명이기 때문에 총 48번의 공격이 이루어졌다. 각 공격은 총 3차 시도로 이루어져있어서 공격이 성공하면 더 이상 공격을 시도하지 않았다. 각 기법에 대해서 공격 성공률을 살펴보면 〔표 9〕에 나와 있다.

영숫자 패스워드의 경우에는 대부분 1차 시도에서 성공되는 것을 볼 수 있었다. 특히 전체 시도의 총합을 살펴보면 매우 높은 공격 성공도를 보였다. 이는 기존의 영숫자 패스워드가 엿보기 공격에 약하다는 것을 증명하는 부분이다. 제안하는 기법을 살펴보면 3차 시도의 경우에서 가장 많은 성공이 이루어지는 것을 볼 수 있었다. 전체 시도의 총합을 살펴보면 35.41%로 영숫자 패스워드에 비해서 낮은 수치를 볼 수 있었다. 이는 제안하는 기법이 영숫자 패스워드에 비해서 엿보기 공격에 더욱 강한 패스워드 기법이라는 것을 알 수 있다.

〔표 9〕 각 기법에 관한 엿보기 공격 실험 결과

(성공횟수:번,비율:%)

기법		1차	2차	3차	총 합
영숫자 패스워드	성공 횟수	22	7	4	33
	비율	45.8	14.6	8.3	68.8
제안하는 기법	성공 횟수	4	6	7	17
	비율	8.3	12.5	14.6	35.41

VI. 결론

본 논문에서는 모바일 컴퓨팅 환경에 적합한 그래피컬 패스워드 기법에 대해서 살펴보았다. 지금까지 발달되어온 그래피컬 패스워드 기법들을 살펴보면 몇 가지 특징을 알 수 있었다. 그 특징들은 일단 사용자들이 사용하기에 편해야 하며, 패스워드가 외우기 쉬어야 하고 엿보기 공격에 강해야 한다는 특징이 있었다. 이러한 특징에 따라서 한글의 자모를 분해하여 도출된 5가지 획으로 구성된 그래피컬 패스워드를 제안하였다. 이 기법은 실제 한글을 쓰는 획을 그대로 쓰되 획들의 기준점이 가운데에 모여 있는 기법이다. 이 기법을 사용하면 실제 한글을 쓰는 것처럼 쓰기 때문에 사용자들이 사용하기에 편한 장점이 있고 패스워드 자체도 한글 단어로 되어있고, 사용하는 획의 종류도 5가지이기 때문에 패스워드의 기억성도 높다. 그리고 획의 중심점을 모두 가운데로 모아놨기 때문에 엿보기 공격에도 매우 강한 그래피컬 패스워드 기법이라고 할 수 있다. 이러한 기법을 이용해서 모바일 컴퓨팅 환경에서 사용자들이 안전하게 개인정보를 보관할 수 있고 그에 따른 유용한 서비스들을 사용 할 수 있을 것이다.

참고문헌

〔1〕 I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin, "The design and analysis of graphical passwords," Proceedings of the 8th USENIX Security Symposium, pp.1-14, Aug. 1999.

〔2〕 I.H. Jeng, D.R. Tsai, H.A. Chen, Y.C. Yen, and C.K. Cheng, "Touch -sensitive alphanumeric encrypting PIN pad design based on hamilton -connected subgraph recognition," Processing of International Conference on Intelligent Information Hiding and Multimedia Signal, pp.258-261, Sept. 2009.

〔3〕 R.N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, no. 1, pp. 156-163, Feb. 1967.

〔4〕 L. Sobrado and J.C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Rutgers University, Camden New Jersey, vol. 4, Sept. 2002.

〔5〕 http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm

〔6〕 H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," Proceedings of International Conference on Cyberworlds, pp.194-199, Oct. 2010

〔7〕 W. Hu, X. Wu and G. Wei, "The security

analysis of graphical passwords," Proceedings of 2010 International Conference on Communications and Intelligence Information Security, pp.200-203, Oct. 2010.

〔8〕 X .Suo, Y. Zhu and G.S. Owen, "Graphical passwords: a survey," Proceedings of the 21st Annual Conference on Computer Security Applications, pp. 463-472, Dec. 2005.

〔9〕 R. Biddle, S. Chiasson, and P.v. Oorschot, "Graphical passwords: learning from the first twelve years," TR-11-01, Carleton University - School of Computer Science, Jan. 2011.

〔10〕 S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy and N. Memon, "Passpoints: design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies - Special isssue: HCI research in privacy and security is critical now archive, vol. 63, no. 1-2, pp. 102-127, July 2005.

〈著者紹介〉

고 태 형 (Taehyoung Ko) 학생회원
2010년 6월: 아주대학교 정보 및 컴퓨터공학부 졸업
2010년 9월~현재: 아주대학교 대학원 컴퓨터공학전공 석사과정
〈관심분야〉 정보보호, 그래피컬 패스워드, 사용자 인증

손 태 식(Taeshik Shon) 정회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 컴퓨터공학 석사
2005년 8월: 고려대학교 정보보호대학원 박사
2004년 2월~2005년 2월: University of Minnesota, Research Scholar
2005년 8월~2011년 2월: 삼성전자 DMC 연구소 책임연구원
2011년 2월~현재: 아주대학교정보통신공학부 조교수
〈관심분야〉 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

홍 만 표(Manpyo Hong) 정회원
1981년: 서울대학교 계산통계학 전공(학사)
1983년: 서울대학교 계산통계학 전공(석사)
1991년: 서울대학교 병렬처리 전공(박사)
1983년~1985년: 울산공과대학 전임강사
1993년~1994년: 미네소타 대학 교환 교수
2000년~2001년: 조지워싱턴 대학 교환 교수
1985년~현재: 아주대학교 교수