# 보안성과 편리성이 향상된 노크코드 기반 인증 기법

이상화*, 박용수*
*한양대학교 컴퓨터 소프트웨어학과
e-mail : lsh11112@hanyang.ac.kr

# An Improved Knock Code-Based Authentication Scheme

Sanghwa Lee*, Yongsu Park*
*Dept. of Computer Science, Hanyang University

**요 약**

스마트폰에 저장되는 개인정보가 늘어나면서 이를 보호하기 위한 여러가지 인증기법이 제안되었다. 이중 안드로이드 OS 에 탑재된 패턴락은 가장 많이 사용되는 인증기법 중 하나이지만 Smudge 공격과 Shoulder surfing 공격에 취약하다고 알려져 있다. LG 전자는 패턴락에 비해 보안성, 편리성이 뛰어난 노크코드라는 기법을 고안하였다. 노크코드는 꺼진 화면에 사용자가 정한 영역을 순서대로 '터치'함으로써 인증을 완료한다. 본 논문에서는 '터치'만을 사용하는 기존 노크코드 기법에 '슬라이드'를 입력으로 추가할 수 있도록 변형시킨 기법 두 가지를 제안하였다. 분석 결과, 기존 기법에 비해 패스워드의 길이가 n(6~8)으로 같을 경우 패스워드의 개수가 $4^n$ 배까지 증가했음을 정량적으로 보였고 슬라이드 입력을 이용해 Smudge 를 직접적으로 제거함으로써 Smudge 공격에 대한 저항력을 높일 수 있음을 보였다.

## 1. 서론

최근 스마트폰에 저장되는 중요한 개인정보들이 점점 늘어나고 있으며 어디서든 소지해야 하는 필수기기가 되어가고 있다. 항상 소지해야 하므로 분실이나 도난의 위험에 노출되어 있고 그 결과, 현재 모든 스마트폰에는 다양한 기법의 잠금 시스템이 장착되어 있다.

그래픽 기반 인증 기법 중 하나인 패턴락 기법은 현재 스마트폰에서 가장 널리 사용되고 있는 안드로이드 OS 에서 사용되고 있다[1]. 패턴락 기법은 인증 시 공격자의 관찰을 통한 공격 방법인 Shoulder surfing 공격에 취약하며[3] 사용자의 패턴 인증 뒤에 손에 있던 기름에 의해 화면에 남은 자국을 이용한 공격 방법인 Smudge 공격에 취약하다[2].

LG 전자에서는 Shoulder surfing 공격, Smudge 공격에 의한 취약점을 보완함과 동시에 편리성을 제공하는 새로운 인증방식인 노크코드를 장착한 스마트폰을 최초로 선보였다. 노크코드의 인증은 기존의 그래픽 기반의 기법들과 다르게 꺼진 화면에서 진행된다. 꺼진 화면은 좌측상단, 좌측하단, 우측상단, 우측하단 4 영역으로 나눠지며 사용자가 설정해 놓은 순서대로 최소 6 번에서 최대 8 번 올바른 면을 순서대로 터치하면 인증이 완료된다. 화면에 패턴이 그려지는 패턴락에 비해 노크코드는 꺼진 화면에서 인증이 진행되기 때문에 Shoulder surfing 공격을 이용한 공격이 더 어렵고, 이어진 선이 아니라 점의 형태로 자국이 남게 되므로 Smudge 공격에 대한 저항력 역시 더 강하다. 또한 화면을 보지 않고도 인증이 가능하다는 편리성도 가지고 있다.

이 글에서는 기존 노크코드에서 보안성을 증가시킨 새로운 노크코드 기법을 두가지 제안할 것이다. 2 장에서는 기존에 연구되었던 그래픽 기반 인증 기법과 노크코드에 대한 분석을 다룰 것이며 3 장에서는 제안 기법의 상세한 사용법에 대해 다룰 것이다. 이후 4 장에서 제안 기법의 보안성 에 대해 다루고 5 장에서 한계점 및 결론으로 마무리 할 것이다.

## 2. 관련 연구

그래픽 기반 기법들을 분석한 연구에서, 그래픽 기반 기법을 RECALL-BASED, RECOGNITION-BASED,CUED-RECALL 기법으로 구분했다[1].

RECALL-BASED 기법은 점 또는 선으로 이루어진 패스워드를 화면에 그려서 인증하는 기법이며 노크코드 역시 RECALL-BASED 기법에 해당한다. 본 장에서는 그동안 연구되었던 노크코드를 포함한 각종 RECALL-BASED 기법들에 대해 소개할 것이다.

· **DAS** : 그래픽 패스워드 기법 중 가장 오래되었으며, 이후의 그래픽 패스워드 연구에 가장 많은 영향을 준 기법은 1999 년에 고안된 DAS(Draw A Secret)이다[4].
DAS 의 인증은 2 차원 격자에서 이루어진다. 사용자는 비밀번호 설정 시에 격자에 점 또는 방향이 있는 선을 그릴 수 있다. 인증시에 설정 시 그렸던 순서 그대로 그리면 인증이 완료된다. DAS 로 만들 수 있는 패턴의 개수는 $2^{48}$ 개임을 재귀를 이용한 계산법으로 알 수 있다.

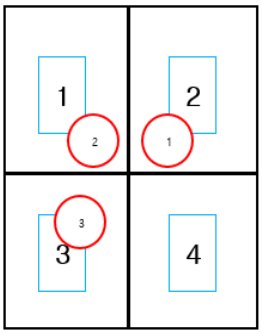
· **TMD** : 2013 년, Hsin-Yi Chiang 은 안드로이드 패턴락보다 가능한 패스워드의 개수가 많고 Shoulder surfing 공격에 강한 새로운 패턴락 기법인 TMD(Touchscreen Multi-layered Drawing)를 선보였다[5]. TMD 는 기존 안드로이드 패턴락과 다르게 5X7 격자를 사용하며 다층 인증방식을 이용한다.
TMD 의 5X7 격자는 Selected cell, Unselected cell, Warp cell 로 이루어져 있다. 좌측 상단,우측 상단, 좌측 하단,우측 하단은 항상 Warp cell 이며 처음 입력시에 Warp cell 을 제외한 31 개의 cell 은 Unselected cell 로 설정되어 있다. 인접한 Unselected cell 을 한 개씩 선택해 가면서 패턴을 그리게 되며 선택된 cell 은 Selected cell 로 변하게 된다. 패턴을 그려 나가다 Warp cell 에 도착하게 되면 모든 Selected cell 이 Unselected cell 로 변하면서 다음 층으로 넘어가게 된다. 현재 Warp cell 에서 시작해서 다시 패턴을 그리게 된다. 즉, Warp cell 에 도착할 때마다 다음 층으로 넘어가서 새로운 패턴을 그리는 식으로 진행되며, 각 층마다 정확한 패턴을 그렸을 시에 인증이 완료된다.
층의 개수가 D 일 때 TMD 가 만들 수 있는 패스워드 개수의 lower bound 는 $2^{62}$ X D 로 기존의 안드로이드 패턴락보다 더 많으며 특정 순간에 사용자는 한 층에 대한 패턴 정보만 노출하므로 Shoulder surfing 공격에 더 강하다는 것을 보였다.

· **TinyLock** : 2014 년, Kwon 등은 안드로이드 패턴락의 격자 사이즈를 엄지손가락만으로 가려질 만큼 작게 만든 TinyLock 을 제안했다[7].
TinyLock 은 두개의 격자를 화면의 위 아래에 둔다. 아래쪽의 격자는 기존의 방식과 같이 직접 패턴을 그리는 격자이고 위쪽의 격자는 첫 입력시에만 아래쪽 격자에서 누른 똑같은 cell 을 표시해줌으로써 사용자의 편의를 돕는다. TinyLock 은 새로운 cell 을 누를 때마다 진동효과를 주어서 엄지손가락으로 인해 인증화면이 가려지는 단점을 완화하였고, 패턴을 그린 뒤에 시계 방향이나 반 시계 방향으로 원형의 가상휠을 그려야 인증이 완료되도록 해서 Smudge 를 제거하도록 강제한다.
사용자 실험에서 속도와 정확도가 기존의 패턴락에 약간 못 미친다는 결과가 나왔지만 Smudge 를 아예 제거해 버림으로써 Smudge 공격을 완벽하게 예방할 수 있다.

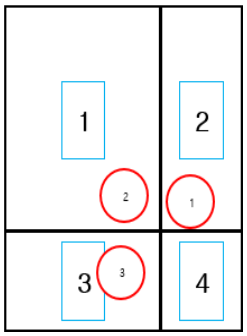
· **Duplicated and Temporal Codes** : 2016년, Ashley Colley 등은 안드로이드 패턴락과 동일한 인터페이스를 가지지만 두가지 요소를 추가한 패턴락 기법을 제안했다[8].
이 기법에서는 안드로이드 패턴락과 다르게 한번 선택된 cell을 다시 선택 가능 할 수 있게 했고 cell을 누르고 있는 시간이 한계시간을 넘게 되면 다른 입력으로 취급함으로써 가능한 패스워드의 개수를 늘렸다.
결국 같은 Smudge에 다른 패스워드가 나오는 경우가 안드로이드 패턴락보다 많아지게 되고 Smudge 공격에 강한 저항력을 보여준다. Smudge 공격에 강한 모습을 보여주면서도 실험자들을 대상으로 한 실험에서 인증 속도는 기존의 방법과 비슷하다는 것을 보였다.

· **Pass-O** : 2017 년, Harshal Tupsamudre 등은 안드로이드 패턴락의 3X3 격자를 원형으로 배치한 새로운 패턴락 기법 Pass-O 를 제안했다[6].
Pass-O 가 만들 수 있는 패스워드의 수는 985,824 개로 기존의 안드로이드 패턴락에 비해 대략 2.5 배 많은 수이다.
또한 위 연구에서는 Pattern length, Stroke length, Intersection 등의 Shoulder surfing 공격에 대한 보안성 비교를 정량적으로 가능하게 해주는 지표를 도입함으로써 기존의 패턴락보다 Shoulder surfing 공격에 강하다는 것을 보였다.

· **Knock code** : LG 전자 노크코드의 인증은 기존의 그래픽 기반의 기법들과 다르게 꺼진 화면에서 진행된다. 꺼진 화면은 (그림 1)과 같이 좌측상단, 우측상단, 좌측하단, 우측하단 4 영역으로 나눠지며 사용자가 설정해 놓은 순서대로 최소 6 번에서 최대 8 번 올바른 면을 순서대로 터치하면 인증이 완료된다. (그림 1)의 파란색 박스 안 숫자는 영역의 번호를 나타내며, 이 경우 패스워드는 2->1->3 이 된다.
(그림 2)를 보면 중점의 위치가 다른 것을 볼 수 있다. 노크코드는 첫 입력에 따라 영역의 중점을 결정한다. (그림 2)에서의 2 영역의 첫 번째 터치를 (그림 1)에 비해 오른쪽 아래쪽에 했으므로 중점 또한 오른쪽 아래 있다. 이처럼 노크코드는 첫 터치를 어느 곳에 하는지에 상관 없이 사용자가 미리 정한 순서인 2 영역 -> 1 영역 -> 3 영역으로 누르기만 하면 인증이 완료된다.
노크코드의 경우 매 입력마다 4 영역 중 한가지를 순대로 중복 가능하게 선택하면 되므로 가능한 패스워드의 개수는 패스워드 길이가 6 인 경우 $4^6$개, 7 인 경우 $4^7$ 개, 8 인 경우 $4^8$ 로 총 $4^6$+ $4^7$+ $4^8$= 4096 + 16384 + 65536= 86016 개가 된다.
꺼진 화면에 패턴이 그려지는 패턴락에 비해 노크코드는 꺼진 화면에서 인증이 진행되기 때문에 Shoulder surfing 공격을 이용한 공격이 더 어렵고, 이어진 선이 점의 형태로 자국이 남게 되므로 Smudge 공격에 대한 내성 역시 더 강하다. 또한 화면을 보지 않고도 인증이 가능하다는 편리성도 가지고 있다.




(그림 1) 노크코드




(그림 2) 노크코드(다른중점)

* □ : 안의 숫자는 영역번호
* ○ : 터치한 곳을 의미하며 안의 숫자는 터치순서

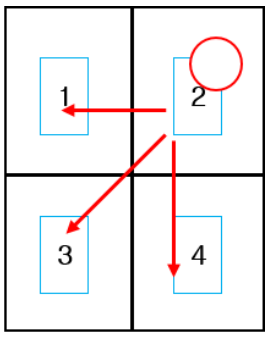
## 3. 새로운 기법 제안

본 장에서는 '터치' 만을 입력으로 지원했던 노크코드에 '슬라이드' 또한 입력으로 지원하는 노크코드를 제안할 것이다. 영역의 개수를 기존의 노크코드와 같이 4 개로 유지하면서 슬라이드를 입력으로 지원하는 기법과 영역의 개수를 2 개로 줄이고 슬라이드를 입력으로 지원하는 기법 두가지가 있으며 각각을 편의상 2X2 노크코드, 1X2 노크코드로 표기할 것이다.

**· 슬라이드를 지원하는 2X2 노크코드 :** 슬라이드를 입력으로 지원하는 2X2 노크코드는 기존의 노크코드에서 각 영역 당 3 가지의 '슬라이드' 입력을 추가함으로써 총 12 가지의 입력을 추가시킨 것이다.

(그림 3)을 보면 2 영역을 이용해 만드는 입력으로 2 영역에서 1 영역으로 슬라이드, 2 영역에서 3 영역으로 슬라이드, 2 영역에서 4 영역으로 슬라이드 총 3 가지 입력을 기존의 2 영역 터치 입력에 추가시킨 것을 알 수 있다. 결국 한번 입력 시 선택 할 수 있는 경우의 수는 1,2,3,4 영역에 각각 4 가지(슬라이드 3,터치 1)로 총 16 가지가 된다.

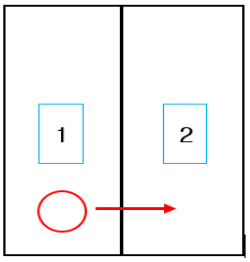
2X2 노크코드가 만들 수 있는 총 패스워드의 개수는 $16^6+16^7+16^8$=16,777,216+268,435,456+4,294,967,296= 4,580,179,968(약 45 억)개가 된다.




(그림 3) 슬라이드를 지원하는 2X2 노크코드

**· 슬라이드를 지원하는 1X2 노크코드 :** 슬라이드를 지원하는 1X2 노크코드는 기존의 노크코드에서 영역을 2 개 영역(1X2)으로 줄이고 1 영역에서 2 영역으로 슬라이드, 2 영역에서 1 영역으로 슬라이드 입력을 추가시킨 기법이다.

(그림 4)와 같이 영역은 1 영역, 2 영역으로만 나눠지며 1 영역에서의 입력은 1 영역 터치와 1 영역에서 2 영역으로 슬라이드, 총 2 가지가 된다. 결국 한번 입력 시 선택 할 수 있는 경우의 수는 1,2 영역 2 가지씩 총 4 가지가 된다. 결국 기존의 노크코드와 같은 86,016 개의 패스워드를 만들 수 있다.




(그림 4) 슬라이드를 지원하는 1X2 노크코드

## 4. 보안성 비교 분석

본 장에서는 기존의 노크코드에 비해서 슬라이드를 입력으로 지원하는 1x2,2x2 노크코드가 보안성 면에서 가지는 이점에 대해서 다룰 것이다.

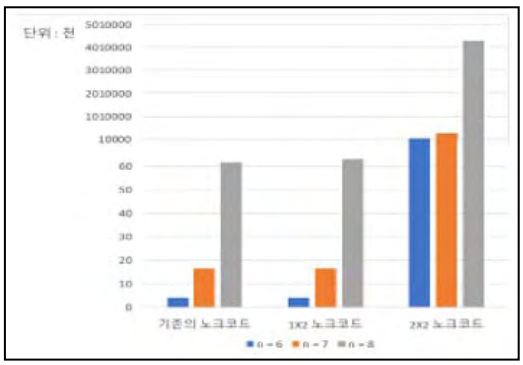
### 4.1 패스워드 경우의 수 분석

인증기법의 보안성은 만들 수 있는 패스워드의 총 개수로 정량화 시킬 수 있다. 2,3 장에서의 설명에 따르면 기존의 노크코드는 패스워드의 길이 n 일 때 만들 수 있는 총 패스워드의 개수는 $4^n$ 이 되며 밀기를 추가한 1x2 노크코드 역시 $4^n$개이다.

슬라이드를 추가한 2x2 노크코드의 경우는 $16^n$ 개가 된다. <표 1>과 (그림 5)에서 노크코드가 가질 수 있는 패스워드 길이 6~8 에 대한 각각의 가능한 패스워드 개수를 시각화 하였다. 기존의 노크코드와 1x2 노크코드는 $4^n$ 으로 동일한 개수의 패스워드를 만들 수 있다. 영역의 개수를 절반으로 줄였음에도 같은 수준의 보안성을 가진다는 것을 알 수 있다. 2x2 노크코드는 기존의 노크코드보다 $16^n$ / $4^n$ = $4^n$ 배의 패스워드를 더 만들 수 있다. 똑같이 4 개의 영역을 사용하지만 패스워드 길이가 8 일 시에 기존의 노크코드가 65,536 개의 패스워드를 만들 수 있는 반면에 슬라이드를 지원하는 2x2 노크코드는 42 억개 이상의 패스워드를 만들 수 있으므로 보안성이 더 뛰어남을 알 수 있다.

| 패스워드 길이 | 기존 노크코드 | 1X2 | 2X2 |
|---|---|---|---|
| 6 | 4,096 | 4,096 | 16,777,216 |
| 7 | 16,834 | 16,834 | 268,435,456 |
| 8 | 65,536 | 65,536 | 4,294,967,296 |

<표 1> 패스워드 길이(n)에 따른 인증기법별 가능한 패스워드 개수




(그림 5) 패스워드 길이(n)에 따른 인증기법 각각의 가능한 패스워드 개수

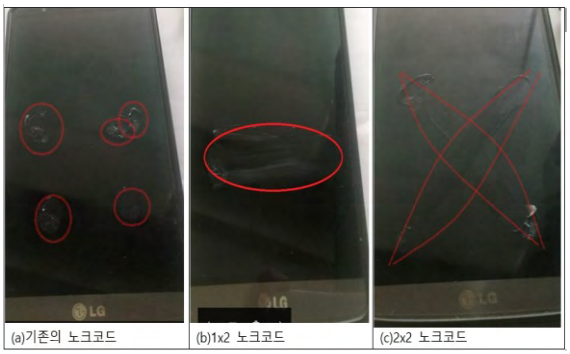
### 4.2 Smudge 공격에 대한 저항성 분석

본 절에서는 제안 기법이 기존 노크코드에 비해 슬라이드를 입력으로 지원함으로써 Smudge 공격에 대한 저항력을 증가시킬 수 있음을 보인다. 저항력을 증가시키는 방법은 TinyLock[7]에서 사용되는 패턴을 그린 후 마지막에 가상휠을 그릴 것을 강제해서 Smudge 를 제거하는 방법과 유사하다.

(그림 6-a)는 길이가 6 인 패스워드를 설정 했을 시에 인증 후에 남은 Smudge 의 모습이다. 점의 형태로 자국이 남기 때문 4 영역을 모두 이용 했을 시에 그림과 같이 최소 4 개에서 6 개의 자국이 남게 되며 그림에서는 5 개의 자국을 확인 할 수 있다. 이 경우에 쉽게 분석 될 가능성이 있다.

(그림 6-b)과 (그림 6-c)는 각각 슬라이드를 지원하는 1x2,2x2 노크코드의 길이가 6 인 패스워드 Smudge 이다. (그림 6-b)의 경우 좌, 우로 슬라이드 입력을 입력의 후반부에 추가함으로써 (그림 6-a)의 점의 형태로 남은 Smudge 를 모두 제거해 주었다. (그림 6-c)는 입력의 후반부에 대각선 방향으로 슬라이드 입력을 추가해서 점의 형태로 남은 Smudge 를 모두 제거하였다.

위와 같이 입력의 후반부에 사용자가 슬라이드를 패스워드에 추가하면 Smudge 를 지워주는 효과가 있으므로 Smudge 공격에 대한 저항력을 높일 수 있다.




(그림 6) 기존의 노크코드(a)와 슬라이드를 지원하는 1x2 노크코드(b)와 2x2 노크코드(c) Smudge 비교

## 5. 결론 및 한계점

본 논문에서는 기존의 노크코드 기법에서 슬라이드를 입력으로 지원하는 1X2, 2X2 노크코드를 제안하고 새로운 기법이 패스워드의 개수, Smudge 공격 저항력 부분에서 더 우수하다는 것을 보였다.

슬라이드를 지원하는 1X2 노크코드는 영역의 개수를 절반으로 줄였지만 만들 수 있는 총 패스워드의 개수는 기존의 노크코드와 같으며 슬라이드를 추가한 2X2 노크코드는 영역의 개수를 2X2 그대로 유지하면서 만들 수 있는 총 패스워드의 개수는 45 억개 이상으로 기존의 노크코드보다 압도적으로 많음을 보였다.

Smudge 공격에 대한 저항력은 슬라이드 입력을 마지막에 추가해서 Smudge 를 지우는 방식으로 Smudge 공격에 대한 저항력을 향상시킬 수 있다.

하지만 본 연구에서는 시간적인 제약으로 인해 사용자 설문을 통한 편리성에 대한 부분을 다루지는 못하였다. 향후 연구에서는 프로토타입을 제작해 실제 실험집단에게 사용하도록 해봄으로써 인증속도, 정확성 등을 실제로 체크해보고 기존의 기법과 비교한 편리성에 대한 설문을 통해 더욱 정확한 분석을 보일 것이다.

## 참고문헌

[1] Robert Biddle, Sonia Chiasson, P.C. van Oorschot “Graphical Passwords: Learning from the First Twelve Years,” August. 2012.

[2] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith “Smudge attacks on Smartphone Touch Screens,” August. 2010.

[3] Arash Habibi Lashkari, Samaneh Farmand, Dr. Omar Bin Zakaria, Dr. Rosli Saleh “Shoulder Surfing attack in graphical password authentication,” December. 2009.

[4] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin “The design and analysis of graphical password,” August. 1999.

[5] Hsin-Yi Chiang “A GRAPHICAL PASSWORD SCHEME FOR MOBILE DEVICES,” January. 2013.

[6] Harshal Tupsamudre, Vijayanand Banahatti, Sachin Lodha “Pass-O: A Proposal to Improve the Security of Pattern Unlock Scheme,” April. 2017.

[7] Taekyoung Kwon, Sarang Na “TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems,” May. 2014.

[8] Ashley Colley, Tobias Seitz, Tuomas Lappalainen, Matthias Kranz, and Jonna Häkkilä1 “Extending the Touchscreen Pattern Lock Mechanism with Duplicated and Temporal Codes,” November. 2016.