JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 11: 1471~1477, Nov. 2019

원형 스마트폰 잠금 패턴 방식 제안

임지우[1] · 이승재[1] · 장원준[1] · 권혁동[2] · 서화정[3*]

A proposal of Circular Lock Pattern Method on Smart phone

Ji-woo Im[1] · Seung-jay Lee[1] · Won-jun Jang[1] · Hyeok-dong Kwon[2] · Hwa-jeong Seo[3*]

[1]Undergraduate Student, Department of IT Engineering, Hansung University, Seoul 02876 Korea
[2]Graduate Student, Department of IT Engineering, Hansung University, Seoul 02876 Korea
[3*]Assistant Professor, Department of IT Engineering, Hansung University, Seoul 02876 Korea

요 약

스마트폰에는 현재 다양한 보안 방식이 사용되고 있다. 그중에서도 핀 번호와 패턴 잠금 방식은 초기 스마트폰부터 사용되었을 정도로 오래 사용되었다. 하지만 패턴 잠금 방식은 오래 사용된 만큼 보안이 취약하다. 핀 번호 방식의 보안 강도가 약간 높은 정도라면 패턴 잠금 방식은 중간 정도에 그친다. 그럼에도 많은 스마트폰 사용자들은 패턴 잠금 방식을 이용하고 있는데 아직 생체보안을 지원하지 않는 기종을 사용하는 사용자가 있기 때문이다. 생체보안을 지원하지 않는 기종에서 제일 편리한 보안 방식은 패턴 잠금 방식이다. 그러나 기존의 패턴 잠금 방식은 Shoulder surfing attack과 Smudge attack에 취약하다. 따라서 패턴 잠금 방식의 편리성을 유지하면서 동시에 기존 방식의 취약점을 해결하는 방식을 제안하고자 한다. 제안하는 방식은 화면에 배치되는 각각의 점을 원형으로 배치한 뒤 무작위로 숫자를 부여하는 잠금 방식이다. 본 방식을 도입하게 된다면 기존의 취약점을 상당히 해결할 수 있다. 즉, 기존의 패턴 잠금 방식에 비해 보안성을 높일 수 있다.

ABSTRACT

Currently, there are various security methods in smart phone. Among them, pin number and pattern lock were used long as they were used from early smart phone. However, security is weak that much. The security of pin number is slightly high, but the security of conventional pattern lock remains moderate. However, the conventional pattern lock is still used by several people because of convenience. This is because some users' smart phones don't support biometric security. The most convenient security method for devices that don't support biometric security is pattern lock. However, this method is vulnerable to shoulder surfing attack and smudge attack. Therefore, we introduce random pattern lock that solves the vulnerability of the conventional pattern lock while maintaining the convenience of the pattern lock. This is a lock method that places each point placed on the screen in a circular shape and assigns a random number to it. Therefore, If this is introduced, It's expected to solve vulnerability.

키워드 : 보안 키패드, 원형, 패턴 잠금, 휴대폰 잠금

Keywords : Cell phone Lock, Circle, Patten lock, Security keypad

Received 15 July 2019, **Revised** 26 July 2019, **Accepted** 14 August 2019

*** Corresponding Author** Hwajeong Seo(E-mail:hwajeong84@gmail.com, Tel:+82-2-760-8033)
Assistant Professor, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.11.1471 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

스마트폰의 등장 이전까지만 하더라도 대부분의 사람들은 휴대폰의 보안에 크게 신경 쓰지 않았다. 하지만 스마트폰이 등장하고 급속도로 보급되면서 사용자의 다양한 개인 정보가 스마트폰 속에 저장되기 시작했다. 기술 발전으로 인한 저장 공간 확장, 스마트폰을 이용한 모바일 뱅킹과 같은 간편 결제가 상용화됨에 따라서 휴대 기기에 민감한 정보가 다량으로 저장되고 있다. 이러한 정보를 지키기 위해 스마트폰의 보안 기술 필요성은 더욱 중요해지고 있다. 스마트폰의 보안 기술 중에서도 패턴 잠금 방식은 안드로이드 초기 OS에 탑재되어 현재까지 확고한 사용자층을 가지고 있다.

패턴 잠금 방식은 점을 이어 화면에 그림을 그리는 특유의 편리성으로 고정 사용자층을 보유하고 있다. 최근 생체인식 기술의 개발로 인해 사용자들의 주요 잠금 방식은 생체인식 보안으로 넘어갔지만, 기존 잠금 방식은 여전히 중요한 요소이다. 먼저 기존 잠금 방식을 선호하는 사용자가 상당수를 이루며, 생체인식 보안 기술을 사용하더라도 특수한 상황에서 인식 오류가 일어날 가능성에 대비해 기존 방식을 필수로 설정해야하기 때문이다. 게다가 아직 생체보안을 지원하지 않는 기종의 스마트폰 사용자들은 기존 잠금 방식을 사용해야 하므로, 패턴 잠금 방식과 개인 식별 번호(PIN, Personal Identification Number)는 여전히 스마트폰 시장에서 중요한 잠금 방식이다. 현재 생체인식 기술을 제외한 주요 스마트폰 잠금 기술로는 개인 식별 번호 방식과 패턴 잠금 방식 총 2가지가 있다.

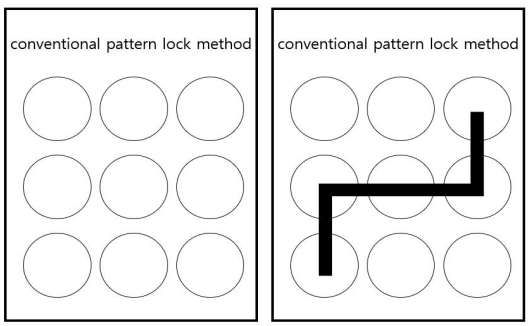

Fig. 1 Left) Before pattern input
Right) Recognized pattern[1]

그 중에서 패턴 잠금 방식은 다수의 사용자가 핀 번호 방식보다 외우기 쉽고 편리하다는 점에서 사용하고 있으며 그림 1을 보면 패턴의 편리함을 알 수 있다. 그러나 다수의 사용자가 단순한 패턴을 사용한다는 점[2], 패턴을 해제할 때 다른 사람이 훔쳐볼 수 있다는 점 및 화면에 패턴 모양의 자국이 남는다는 점 때문에 보안에 취약하다. 패턴 잠금 방식의 취약성 중 하나는 Shoulder surfing attack[3]이다. Shoulder surfing attack이란 사용자가 패턴을 해제하는 과정을 다른 사람이 어깨너머에서 움직임을 파악한 후 이를 유추하여 잠금을 해제하는 것이다. 두 번째는 Smudge attack[4]이다. 패턴 해제 시 이물질이나 먼지로 인해 화면에 보안 패턴 모양의 자국이 생긴다는 점을 악용하여 패턴을 유추하는 것이다. 패턴 잠금 방식의 문제점들을[5] 해결하기 위해 본 논문에서는 핀 번호와 패턴 잠금 방식을 합쳐 기존보다 뛰어난 보안성의 잠금 방식인 새로운 원형 랜덤 패턴 잠금을 제시하고자 한다.

본 논문의 구성으로는 2장에서 관련 연구 동향을 살펴보고 3장에서 원형 랜덤 패턴 잠금 기법과 네 가지의 추가 기법을 제안하고 4장에서 성능을 평가해본 후 마무리한다.

Ⅱ. 관련 연구 동향

본 논문의 2장에서는 패턴 잠금 외에도 다른 잠금 기법에 대해 알아보고자 한다. 또한, Smudge attack, Shoulder surfing attack에 대한 동향을 알아보고자 한다.

2.1. 스마트폰에 남은 자국을 통해 기계학습으로 패턴을 유추하는 Smudge attack[6]

Smudge attack에 기계학습을 적용한 방법이다. 패턴 잠금 해제 후 스마트폰에 생기는 자국으로 기계학습을 통해 패턴을 알아낸다. 일반 환경에서 패턴 잠금 해제 후 스마트폰을 사용하는 것을 고려해 스마트폰에 남는 자국을 세 단계로 구분해 기계학습을 진행했다. 또한, 패턴의 복잡도를 고려해 길이 6 이하의 단순한 패턴 100개와 7~9개의 포인트를 지나며 평균 길이 6 이상의 복잡한 패턴 100개로 총 200개의 랜덤 패턴을 선정하였다. 또한, TinyLock과 일반 안드로이드 패턴 잠금에 대한 공격을 비교하였다. 실험에서의 자국 이미지로 라벨을 생성하고, 훈련 데이터를 기계학습 알고리즘을 통

해 예측 모델을 생성한다. 기계학습을 통한 Smudge attack 결과, 일반 패턴 잠금에 대해서는 92%의 공격 성공률을 보였다. 사람에 의한 Smudge attack은 68%의 성공률을 보인다는 점과 비교하면 매우 높은 수치이다. 추가로 사람들이 자주 사용하는 단순한 패턴에 대한 공격 성공률이 복잡한 패턴보다 높았고 스마트폰을 패턴 잠금 해제 후 오래 사용할수록 공격 성공률은 떨어졌다. 또한, TinyLock은 사람에 의한 공격 성공률은 0%로 매우 낮게 나타났다. 특히 TinyLock에 대한 공격 성공률은 2% 미만으로 일반 안드로이드 패턴 잠금보다 매우 떨어졌다.

2.2. 입력 시간을 측정하는 쓰레드를 활용한 패턴 잠금 보안 강화[1]

입력 시간을 측정하는 쓰레드를 활용하여 기존의 패턴 잠금 기법에 입력 시간을 추가로 측정해 이를 잠금을 해제하는 요소로 활용하는 방법이다. 입력 시간을 보안의 요소로 활용하기 위해 쓰레드를 이용하였다. 쓰레드를 활용해 패턴을 입력하는 기능, 각각의 포인트에 입력하는 시간을 측정하는 기능을 동시에 수행한다. 기존의 패턴 잠금에 각 포인트에 머무는 시간을 3단계로 나누어 이를 진동으로 사용자가 알 수 있게 한다. 각각의 포인트에서 3단계로 나누어진 입력 시간을 측정하므로 경우의 수가 기존의 패턴 잠금의 경우의 수보다 3의 n 제곱만큼의 증가하게 된다. 입력 시간 단계를 진동을 통해 알려주기 때문에 Shoulder surfing attack에 높은 내성을 띠고 있다. 또한, 기존의 패턴에 추가로 입력 시간을 보안의 요소로 사용하고 있으므로 Smudge attack에도 내성이 있다. 즉 기존의 패턴 잠금 기법보다 Smudge attack, Shoulder surfing attack에 내성을 띠고 있으며 높은 보안성을 가지고 있다.

2.3. 알고리즘을 활용한 Shoulder surfing attack[7]

알고리즘을 통해 일정한 순서에 따라 사용자의 잠금 패턴을 알아내어 쉽게 잠금을 해제하는 방법이다. 사용자가 패턴을 해제할 때, 근처에서 패턴을 푸는 모습을 포착한다. 이때, 거리가 가까울수록 더욱 성공률이 높아진다. 사용자가 패턴을 해제하는 것을 영상으로 촬영한 후, 알고리즘 프로그램을 통해 각각의 영상의 프레임에서 손가락의 움직임을 분석하여 그 자취를 그래프로 그린다. 그리고 그래프의 움직임을 통해 점과 점 사이의 거리를 예측하여 경우의 수를 줄인다. 이를 통해 경우의 수를 5개 이하로 줄이면 패턴 해제 시 5번의 기회를 준다는 점을 이용하여 쉽게 잠금 해제할 수 있다.

Table. 1 As the intersecting points increase, the probability of unlocking in the fifth trial increases.

No intersecting point	60% Success
Three intersecting points	87.5% Success

패턴의 모양이 복잡할수록 알고리즘이 쉽게 잠금을 해제할 수 있다. 표 1에서 볼 수 있듯이 패턴의 교차점이 늘어날수록 패턴을 푸는 성공률이 높아지는 것을 알 수 있다. 반대로 패턴이 간단할수록 각 포인트에 대입할 경우의 수가 늘어나므로 알고리즘을 통한 Shoulder surfing attack에 의해 패턴이 유출되는 것을 방지하려면 간단한 패턴을 설정해야 한다. 하지만 간단한 패턴일수록 화면에 남는 자국을 보고 패턴을 유추하기 쉬워져서 Smudge attack에 의해 패턴이 유출될 위험이 커진다.

Ⅲ. 제안 기법

2장에서 살펴보았듯이 기존의 패턴 잠금 방식은 Smudge attack과 Shoulder surfing attack에 취약하다. 잠금을 해제하기 위해서 입력해야 하는 패턴의 모양이 모두 같고, 패턴을 입력하는 포인트의 위치가 고정되어 있기 때문이다. 이 문제를 해결하기 위해 잠금을 해제할 때마다 그려야 하는 패턴이 달라지는 원형 랜덤 패턴을 제안한다. 9개의 포인트는 원형으로 배치되어있고, 원형으로 배열된 패드의 점에는 1~9까지의 숫자가 부여되어 있다. 포인트에 부여되는 숫자는 잠금 해제를 시도할 때마다 무작위로 바뀐다. 사용자는 잠금을 해제하기 위해서 고정된 패턴을 그리는 대신, 미리 정해둔 숫자가 부여된 포인트를 순서에 맞게 그려야 한다. 그림 2에서 작동원리를 알 수 있다.

하지만 원형 랜덤 패턴 잠금 기법을 그대로 적용할 경우, 편리성이 떨어지기 때문에 실용성이 떨어질 우려가 있다. 따라서 편리성을 보완하기 위한 3가지 방법을 3.1, 3.2, 3.3, 3.4, 3.5와 같이 제안한다.

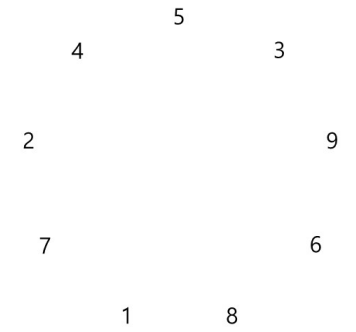

Fig. 2 Random Pattern lock

3.1. 숫자 그룹화

먼저 숫자를 묶어 3개의 리스트로 분류한 후 인접한 위치에 포인트를 배열하는 방법이 있다. 1부터 9까지의 숫자를 1~3, 4~6, 7~9로 묶어 포인트를 배열하는 방법이다. 사용자가 잠금 해제 시도를 할 때마다 숫자의 세 묶음이 다른 위치에 나오게 된다. 사용자가 숫자를 찾을 때 원형 패드 전체를 훑어보는 대신 그룹화 된 리스트 중 3개의 숫자에서만 찾으면 되므로 잠금 해제 시간을 단축할 수 있다. 그림 3의 상단을 보면 (2, 1, 3), (5, 6, 4), (8, 7, 9) 세 묶음으로 이루어져 있다는 것을 알 수 있다.

3.2. 색깔 입히기

사용자에게 숫자 대신 색깔을 선택하게 한다. 숫자를 읽기 위해 어느 정도의 시간이 걸리는 반면 색깔은 보고 포인트를 연결하면 되므로 보안성을 유지하고 편리성을 높이는 방안이다. 그림 3의 중간은 이를 도식화한 것이다. 예를 들어 사용자가 'Red', 'Blue', 'Orange', 'Purple'을 선택하면, 패턴 입력 시 여러 개의 색깔 중에서 사용자가 선택한 배열 순서대로 색깔이 입혀진 포인트를 이으면 잠금이 해제된다.

3.3. 포인트에 숫자 지정하기

사용자가 숫자를 일부 포인트에 1~2개를 미리 설정해 놓으면 편리성을 높일 수 있다. 잠금 해제 시도를 하면 각각의 포인트에 다른 숫자가 부여되는 데 일부 포인트에 숫자를 미리 지정해 놓으면 고정된 숫자가 나오게 된다. 가령 패턴 설정 번호를 1 - 2 - 3 - 4라고 했을 때, 2번 숫자를 어느 한 포인트에 고정하여 놓으면 사용자는 나머지 1, 3, 4가 부여된 포인트만 찾으면 잠금을 해제할 수 있으므로 소요 시간을 단축할 수 있다. 그림 3의 하단에서 숫자 6을 3번째 자리에 고정하고 나머지 숫자만 무작위로 배치되는 것을 확인할 수 있다.

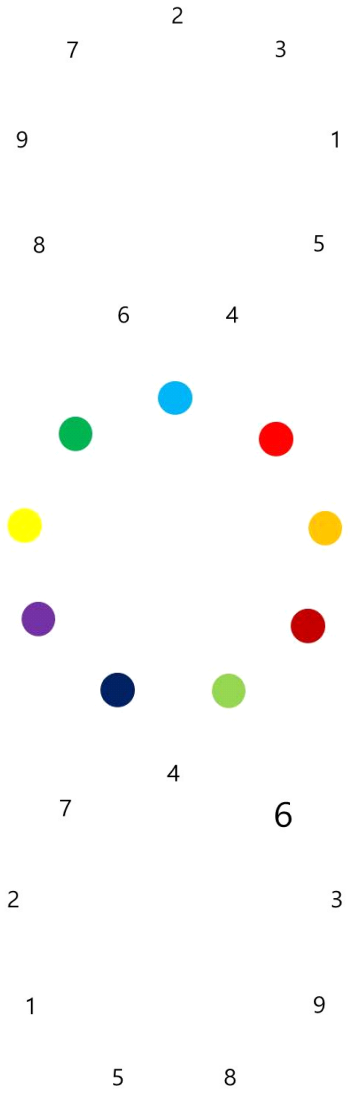

Fig. 3 Top) Number Grouping
Middle) Coloring
Bottom) Assigning a Number to a point

하지만 원형 랜덤 패턴 잠금도 지능형 지속 위협(APT, Advanced Persistent Threat)에는 안전하지 않다. 따라서 APT에 대해 어느 정도의 내구성을 갖게 하도록 보안성을 높이는 방안을 제시한다.

3.4. 보안 요소 추가

보안을 해제하는 요소를 추가하는 것이다. 숫자와 색깔을 동시에 배치한다면 공격자는 어떠한 요소로 보안을 해제하는지 알지 못하므로 더 많은, 더 세심한 관찰을 해야 한다. 사용자가 미리 숫자, 색깔 둘 중 어느 요소로 보안을 해제할지 정하고, 보안을 해제할 때 숫자와 색깔을 무작위로 각각 섞어 포인트에 부여한다. 위의 방식들은 Shoulder surfing attack이 매우 가까운 거리에서 시도되었을 때 취약하다. 따라서 그림 4와 같이 숫자의 순서, 각각 숫자 색깔의 위치를 모두 무작위로 배치하고 사용자는 색깔이나 숫자 둘 중 하나를 골라 순서를 정한다. 그러면 Shoulder surfing attack을 가까운 거리에서 시도하더라도 한 번의 관찰로는 잠금을 해제할 수 없다. Shoulder surfing attack을 성공시키려면 공격자는 숫자 순서, 색깔 순서를 동시에 관찰해야 한다. 공격자는 사용자의 패턴이 어떠한 보안 요소로 보안이 해제되는지 알지 못하므로 공격 시 색깔로 패턴을 해제, 숫자로 패턴을 해제하여 최소 2회 이상 시도하여야 한다.

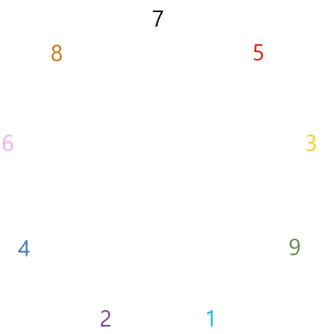

Fig. 4 The positions of the numbers and the sequence of colors are randomly arranged.

3.5. 흐리게 하기

3.1~3.4의 패턴 잠금 방식은 모두 잠금 해제가 완료될 때까지 숫자가 화면에 나타나 있다. 이때 Shoulder surfing attack이 가까운 거리에서 시도된다면 공격자가 숫자의 순서를 알아차릴 수 있다. 따라서 패턴을 그리기 전에만 화면에 숫자를 보여주고 패턴을 그리기 시작할 때 숫자를 흐리게 하거나 숨기는 방식이다. 그림 5와 같이 사용자는 잠금 해제 전 숫자들의 위치를 미리 확인한 후 잠금을 해제하면 되므로 그리는 데 큰 지장이 없지만, 공격자는 패턴을 인식하기 더욱 어려워진다.

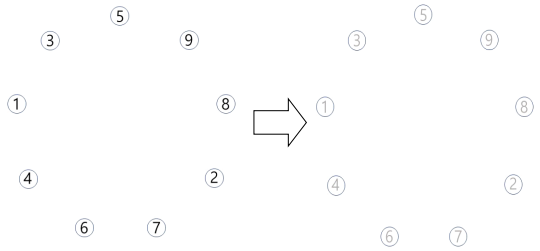

Fig. 5 Blurring color, when pattern is recognized.

Ⅳ. 성능 평가

본 장에서는 원형 랜덤 패턴 잠금이 기존 패턴 잠금에 비해 얼마나 보안성이 있는지 알아보기 위해 대표적인 공격인 Shoulder surfing attack, Smudge attack에 대하여 어느 정도의 보안성을 가졌는지 평가해보려고 한다. 또한, 원형 랜덤 잠금은 기존에 존재하지 않는 새로운 방식이기 때문에 사용자가 익숙하지 않다는 점이 있다. 그러므로 실험을 통해 편의성이 얼마나 떨어지는지, 사용자의 시도에 따라 편의성이 얼마나 증가하는지 알아보려고 한다.

보안성 면에서는 본 논문에서 제안하는 원형 랜덤 패턴은 패턴 잠금보다 그릴 수 있는 패턴의 가짓수가 많다. 일단 원형 랜덤 패턴과 패턴 잠금 둘 다 4개 이상의 점을 이어야 한다. 기존 패턴 잠금은 양 끝점을 지나가는 선을 이을 때 중간에 있는 점이 입력되어 다시 입력될 수 없지만, 본 논문에서 제안한 원형 랜덤 패턴은 교차점이 만들어지지 않으므로 더 많은 패턴의 가짓수를 만들 수 있다. 이는 3장에서 제시한 원형 랜덤 패턴에서 그릴 수 있는 패턴의 가짓수는 대략 397억 가지에 이르며 계산은 수식 1에서 확인할 수 있다. 이에 반해 기존 패턴 잠금에서 그릴 수 있는 패턴의 가짓수는 389,112가지에 불과하다.

$$8! \times (PLSUB9_4 + PLSUB9_5 + PLSUB9_6 + PLSUB9_7 + PLSUB9_8 + PLSUB9_9) \quad (1)$$

4.1. Shoulder surfing attack

기존 패턴 잠금 방식은 점의 위치가 고정되어 있어,

Shoulder surfing attack에 취약했다. 하지만 본 제안 방식을 사용한다면 해당 위험성을 줄일 수 있다. 공격자가 숫자의 배열순서나 색깔 순서 등을 매우 자세히 보지 않는다면 패턴을 유추하기 어렵기 때문이다. 패턴에서 점의 위치가 계속 바뀌므로 손의 움직임을 분석하여 패턴을 알아내는 알고리즘 프로그램을 이용한 Shoulder surfing attack도 불가능하다.

4.2. Smudge attack

기존 패턴 잠금 방식은 잠금 해제에 5번의 기회를 준다. 공격자는 이 점을 악용하여 Smudge attack으로 5번의 기회 중 최소 2번 만에 패턴을 해제할 수 있었다. 제안 방식은 Smudge attack을 100% 방어할 수 있다. 액정 필름에 자국을 그대로 따라 그리더라도 포인트들의 위치가 계속 바뀌게 되므로 잠금을 해제할 수 없고 사용자는 스마트폰의 보안을 유지할 수 있다.

4.3. 편의성

본 논문에서 제안하는 원형 랜덤 패턴은 기존 패턴 잠금보다 편의성이 떨어지는 것이 사실이다. 실제로 패턴 잠금을 사용해본 사람들은 기존 사각형 배치에 익숙해져 있기 때문이다. 이 장에서는 여러 번의 잠금 해제 시도에 따라 편의성이 얼마나 증가하는지 알아보려고 한다. 안드로이드 스튜디오로 간단하게 구현물을 만든 뒤 피실험자가 사용하게 했다. 표 2는 평균나이 20.4세인 5명으로 구성된 피험자들의 10번 시도에 따른 시간을 나타냈다. 단위는 초이다.

Table. 2 Time spent table [SI unit:sec]

	1	2	3	4	5	6	7	8	9	10
A	3.6	3.78	3.67	3.78	3.55	3.47	3.96	9.87	3.37	1.42
B	3.24	3.42	3.53	2.83	2.57	3.06	3.08	2.74	3.30	3.34
C	4.34	3.44	2.68	3.36	3.80	3.13	3.47	2.89	3.2	2.05
D	2.63	2.89	2.89	3.21	2.55	2.47	3.02	2.62	3.31	2.8
E	3.19	3.28	3.1	2.93	3.87	4.01	3.42	3.21	3.05	2.87

위의 실험 결과를 보면 패턴 잠금 해제에 대체로 3초대의 시간이 걸렸다. 이는 기존 패턴 잠금 방식과 시간 차이가 크게 나지 않는다는 점을 알 수 있다. 그리고 C의 경우는 처음에는 4.3초가 걸렸으나 패턴을 사용할수록 익숙해져 마지막 시도에는 시간을 절반이나 단축시켰다.

또한, 3장에서 거론한 그룹화, 색깔 등의 방법을 적용한다면 사용자의 편의성이 더욱 증가할 것이다.

Ⅴ. 결 론

본 논문에서는 기존 패턴 잠금 방식의 보안 취약성을 파악하고 이와 관련된 연구 동향을 살펴보았고, 이러한 취약성을 해결하기 위해 원형 방식의 새로운 패턴 잠금 기법을 제안하게 되었다.

1, 2장에서 다루었듯이, 기존 패턴 잠금 방식은 Shoulder surfing attack과 Smudge attack에 취약하여 생체보안 기술의 오류 대비책 역할밖에 하지 못하고 있다. 그러나 3장에서 제안한 새로운 방식들은 보안성을 상당 부분 증대시킬 수 있다. 초기 스마트폰은 화면 크기가 작고 터치 정확도가 떨어졌지만, 최근 스마트폰은 큰 화면으로 출시되고 있고, PPI(Pixel Per Inch) 또한 높다. 이러한 장점을 활용하면 위의 제안 기법을 구현하기 훨씬 쉽고 사용하기 또한 편하다. 기존 패턴 잠금과는 다른 방식이므로 처음에는 사용자의 적응 시간이 좀 걸릴 수 있지만, 가독성이 높고 편리할뿐더러 보안성이 높다는 장점 때문에 사용자의 호응을 얻기 쉬울 것이다.

ACKNOWLEDGEMENT

This research was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation) and this research was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742).

References

[1] K. H. An, H. D. Kwon, K. H. Kim, and H. J. Seo, "Implement pattern lock security enhancement using thread to measure input time," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 4, pp. 470-476, Apr. 2019.

[2] M. D. Løge, "Tell Me Who You Are and I Will Tell You Your Unlock Pattern," M. S. theses, Norwegian University of Science and Technology, Trondheim, Sør-Trøndelag, 2015.

[3] A. H. Lashkari, S. Farmand, O. B. Zakaria, and R. Saleh, "Shoulder Surfing attack in graphical password authentication," *International Journal of Computer Science and Information Security*, vol. 6, no. 2, pp. 145-154, Nov. 2009.

[4] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Workshop on Offensive Technologies'10 Proceedings of the 4th USENIX conference on Offensive technologies*, Washington: DC, pp. 1-7, 2010.

[5] P. Andriotis, G. Oikonomou, A. Mylonas, and T. Tryfonas, "A Study on Usability and Security Features of the Android Pattern Lock Screen," *Information and Computer Security,* vol. 24, no. 1, pp. 53-72, March. 2016.

[6] S. M. Jung, and T. K. Kwon, "Automated Smudge Attacks Based on Machine Learning and Security Analysis of Pattern Lock Systems," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 26, no. 4, pp. 903-910, Aug. 2016.

[7] G. Ye, Z. Tang, D. Fang, X. Chen, K. I. Kim, B. Taylor, and Z. Wang, "Cracking Android Pattern Lock in Five Attempts," in *Proceedings 2017 Proceedings of the Network and Distributed System Security Symposium*, San Diego: CA, pp. 1-1, 2017.

임지우(Ji-woo Im)

2019년 2월: 심원고등학교 졸업
2019년 3월~현재: 한성대학교 IT공과대학 재학 중
※관심분야 : 컴퓨터시스템 및 정보보안, 게임 및 모바일 앱

이승재(Seung-jay Lee)

2018년 2월: 숭문고등학교 졸업
2019년 3월~현재: 한성대학교 IT공과대학 재학 중
※관심분야 : 네트워크 보안, 암호구현

장원준(Won-jun Jang)

2019년 2월: 영등포고등학교 졸업
2019년 3월~현재: 한성대학교 IT공과대학 재학중
※관심분야 : 컴퓨터 프로그래밍, 모바일 소프트웨어

권혁동(Hyeok-dong Kwon)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, 암호구현

서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT