# 터치스크린에서의 블라인드 인터랙션 기반의 상대적 위치 패턴 잠금 해제 솔루션

김주웅<sup>1</sup>, 반영환<sup>2\*</sup> <sup>1</sup>국민대학교 테크노디자인전문대학원 인터랙션디자인 전공 박사과정 <sup>2</sup>국민대학교 테크노디자인전문대학원 인터랙션디자인 전공 교수

# Relative Position Pattern Unlocking Solution based on Blind Interaction on Touch Screen

Zhou-Xiong Jin<sup>1</sup>, Young-Hwan Pan<sup>2\*</sup>

<sup>1</sup>Ph.D.Course, Dept. of Interaction Design, TED, Kookmin University

<sup>2</sup>Professor, Dept. of Interaction Design, TED, Kookmin University

요 약 본 연구에서는 현존하고 있는 잠금 해제 방식에서 보이는 문제점으로부터 출발해 보안성 및 사용성 측면에서 개선된 블라인드 인터랙션을 적용한 상대적 위치 기반 패턴 잠금 해제 방식을 제안하고 이론적 타당성을 고찰했다. 기존 숫자암호 잠금 해제 방식과 패턴 그리기 잠금 해제 방식과의 차이를 실험을 통해 확인하고 실용적 가치를 평가했다. 상대적 위치 패턴은 숫자 암호 보다 쉽게 기억되고 그리기 패턴과 비슷한 정도의 학습 용이성을 보여 주었고 타 방식에 비해 훔쳐보기 공격에 안전한 결과를 얻었다. 생체신호를 센싱 할 센싱 모듈을 사용할 필요 없이 터치스크린의 기본기능 만으로 실현 가능하기에 적은 원가로 제작할 수 있다. 시각적 요소가 필요 없는 방식이기에 시각 장애인과 같은 특수 사용자들도 불편함 없이 사용할 수 있기에 실용적 가치도 상대적으로 높다.

주제어: 인터랙션, 블라인드 인터랙션, 잠금 해제, 상대적 위치 패턴, 터치 스크린

**Abstract** In this study, we propose a new Relative position pattern unlocking solution based on blind interaction, which is a new unlocking method, and compared it with existing unlocking methods to verify usability and security improvement. And verified the practical value of the proposed new unlocking solution. The relative position pattern unlock method is easily remembered than the numeric code method and is worth practical enough to show a degree of learning ease similar to the drawing pattern method. The new method is safer to steal than other two methods. It can be manufactured at a low cost and can also be used by special users such as blind people. Therefore, the practical value is relatively high.

Key Words: Interaction, Blind Interaction, Unlock Interaction, Relative Position Pattern, Touch Screen

#### 1. 서론

오늘날 스마트 기기의 보급과 기술의 발전으로 인하여

터치스크린 기반 인터페이스의 적용 범위는 점점 광범위해지고 있다. 모바일 디바이스는 물론 터치스크린으로 된 Kiosk도 주변에서 쉽게 볼 수 있다. 테슬라의 전기 자동

차와 같이 자동차 내에 적용된 터치스크린 컨트롤 패드 도 자동차 분야에서 하나의 추세를 이루고 있다. 터치스 크린의 적용 범위가 많이 광범위해진 데 비하여 스크린 의 잠금 해제 방식은 아직 많은 시도와 방법이 나와 있지 않는 상황이다. 최근 비교적 꾸준히 새로운 방식을 적용 하고 있는 영역은 스마트 모바일 디바이스 영역이다. 애 플의 IOS 슬라이드 잠금 해제로부터 시작해서 안드로이 드의 패턴 그리기 잠금 해제, 그리고 현재 주를 이루고 있는 지문인식과 3D 안면인식을 통한 잠금 해제 방식으 로 발전해 왔다. 하지만 지문인식이나 3D 안면인식과 같 은 방식은 특정 개체에 한해서만 사용 가능한 방식이다. 특정 개체가 아닌 다수의 접근을 허용하는 사용 콘텍스 트에서는 적용할 수 없다. 현재 이런 잠금 해제 방식을 적용한 디바이스에서도 단일 잠금 해제 방식만 제공하는 것이 아니라 기타 잠금 해제 방식을 병행하여 제공하고 있다. 주로 숫자조합 패스워드 잠금 해제 방식, 패턴 그리 기 방식 등을 병행하고 있다. 모바일 디바이스에서의 잠 금 해제 방식 병행 사용은 다수의 접근을 가능하게 하는 이유도 있지만 디바이스의 외적 내적 이슈로 인한 인식 오류가 발생해 잠금 해제가 제대로 이루어지지 않는 상 황에서 차선책을 제공해야 하는 이유도 있다. 현재 대부 분 모바일 디바이스는 장소의 제한이 없이 언제 어디서 나 사용할 수 있게 되었다. 편리성이 많이 강화된 동시에 공적인 장소에서의 사용이 일반화되면서 항상 보안 위협 에 노출되고 있다. 잠금 해제 과정이 쉽게 타인한테 공개 될 수 있기에 이는 사용하는 과정에서 비교적 심각한 보 안 이슈를 동반하고 있다고 볼 수 있다. 스마트폰과 같은 사용 대상이 제한된 사적인 모바일 디바이스도 보안 위 협에서 완전히 벗어나기 힘든 상황이다. 이에 비해 항시 공적인 장소에 배치된 디바이스들은 더욱 심각한 보안 위협에 노출되어 있다[16]. 때문에 터치스크린의 잠금 해 제 보안성을 개선하기 위해서는 잠금 해제 방식 자체에 관한 고민뿐만 아니라 외부 영향 요소에 관한 고민을 동 시에 해야 한다. 본 연구에서는 새로운 잠금 해제 방식인 블라인드 인터랙션이 적용된 상대적 위치 기반 패턴 잠 금 해제 솔루션을 제안하고 기존 잠금 해제 방식들과의 비교 실험을 통해 사용성 및 보안성의 개선 여부와 제안 한 새로운 잠금 해제 솔루션의 실용적 가치를 확인하는 것을 연구 목적으로 했다. IoT 환경 혹은 5G 환경에서의 통신과 관련된 보안 기술에도 보안 이슈[17,18]가 존재 하지만본 연구에서 다루는 보안성은 완전한 사용자 시점 에서의 잠금 해제 조작의 보안성에 주목하여 진행했다.

# 2. 연구방법

본 연구에서는 현존하고 있는 잠금 해제 방식에서 보여지는 문제점으로부터 출발하여 보안성 및 사용성 측면에서 개선된 블라인드 인터랙션을 적용한 상대적 위치기반 패턴 잠금 해제 방식을 제안했다. 이론적 타당성을 고찰하고 실제 기존 숫자암호 잠금 해제 방식과 패턴 그리기 잠금 해제 방식에 비해 사용성과 보안성 면에서의 차이를 확인하기 위하여 비교 실험을 설계했다. 도출한실험 결과를 통해 사용성 및 보안성에 관한 차이를 확인하고 제안한 새로운 잠금 해제 솔루션의 실용적 가치에대해 평가를 진행했다.

# 3. 잠금 해제 솔루션

# 3.1 현황 및 문제점

현재 가장 보편적으로 많이 사용하고 있는 암호 방식 은 텍스트 기반의 암호다. 텍스트 유형에 따른 조합이 많 을수록 암호의 해독 난이도는 높아지고 보안성도 높아진 다. 따라서 이런 멀티 텍스트 암호는 높은 보안성을 요하 는 곳에 많이 사용되고 있다. 하지만 이런 멀티 텍스트 기반의 비밀번호는 사용성 부분에서 일부 문제점을 가지 고 있다. 사용자들은 보통 일정 기간 동안 새로운 텍스트 형식의 비밀번호를 완전히 기억하지 못한다. 완전히 기억 하기 까지는 비교적 긴 시간과 노력이 필요하다. 다수의 텍스트 유형이 포함된 암호를 입력하는 과정도 조작에 있어서 효율적이라고 말하기 어렵다. 때문에 디바이스의 잠금 해제와 같은 일상생활에서 실행 빈도가 비교적 높 고 잠금 해제 조작도 효율적으로 이루어져야 하는 사용 콘텍스트 에서는 숫자 암호와 같은 단일 유형의 텍스트 로 이루어진 암호 방식을 주로 사용한다. 숫자로만 이루 어진 암호 방식을 사용함에도 불구하고 숫자를 기억하는 것에 대한 부담은 여전히 존재한다[1]. 때문에 사용자들 은 보통 간단하고 기억하기 쉬운 암호를 선택하여 사용 하게 되는데 이는 또 보안성 문제를 동반하게 된다[2]. 안 드로이드 패턴 그리기 잠금 해제 방식과 같은 그래픽컬 암호들은 기억하기 어려운 문제점을 어느 정도 해결해 준다. 기존의 연구로부터 그래픽컬 정보를 인간의 대뇌가 더 쉽게 기억한다는 것을 알 수 있다[3-5]. 이미 한 세기 넘게 심리학 연구에서는 인간의 대뇌는 텍스트 기반의 정보보다 시각적인 정보를 기억하고 식별하는데 더 우월

한 능력을 보여 준다고 했다[6-11]. 하지만 안드로이드 의 패턴 그리기 암호 잠금 해제 방식도 자주 보안성 문제 가 지적됐다. Von Zezschwitz[12]는 패턴 그리기 잠금 해제 방식을 대상으로 훔쳐보기 평가를 진행하여 훔쳐보 기 공격에 영향을 주는 중요한 요소는 패턴 라인의 가시 성과 패턴의 길이라는 것을 발견했다. 그리고 Aviv et al[13]는 터치스크린 표면의 기름성분 잔유물로 인한 오 염 때문에 패턴 그리기를 진행 후 스크린 표면에 흔적이 남게 되는데 제3자가 이 흔적을 통해 잠금 해제 패턴을 해독하는 상황을 포착했다. 이런 정황들로부터 출발하여 본 연구에서는 새로운 잠금 해제 솔루션의 제작을 가시 성과 그래픽컬 요소를 핵심으로 하여 진행했다. 새로운 솔루션은 가시적인 부분을 약화하고 암호 방식은 그래픽 컬 적인 요소를 가지도록 했다.

# 3.2 블라인드 인터랙션

Jin Zhouxiong은 비인지 인터랙션의 분류체계를 제 기했다. 비인지 인터랙션의 분류는 인터랙션 관련 요소 중에 인지 불가한 요소가 포함된 인터랙션에 관한 분류 다. 비인지 인터랙션을 의미의 비인지, 정도의 비인지, 흔 적의 비 인지로 분류했다[14]. 본 연구에서는 인터랙션 관 련 요소 중에 비 가시적인 요소가 있는 인터랙션을 블라 인드 인터랙션이라고 정의했다. 블라인드 인터랙션은 비 인지 인터랙션에서 시각적으로 인지가 불가한 요소가 포 함된 인터랙션에 해당된다. LuoTao는 인터랙션의 핵심 구조를 Control item과 Widget item의 Mapping 관계 로 정의했다[15]. 이론적으로 인터랙션을 구성하는 모든 요소는 비가시적이 될 수 있다. Control item, Widget item에서 임의의 부분에 비가시적인 요소가 적용되면 해 당 인터랙션을 블라인드 인터랙션이라고 할 수 있다.

# 3.3 상대적 위치 패턴 잠금해제 솔루션

상대적 위치 기반 터치 패턴 잠금 해제 솔루션은 터치 기반의 디바이스, 소프트웨어 응용 프로그램의 스크린 좌 표 값을 활용한 기능이다. 각각의 터치의 센싱으로부터 얻은 좌표 값들의 상호 관계를 활용하여 로직을 구성하 고 이런 로직을 잠금 해제 패턴으로 추상화했다. 상대적 터치 포인트 로직은 현재 터치 포인트와 이전 터치 포인 트의 센싱된 좌표값(x,y)의 관계를 판단하는 방식이다. 아래 5개 터치 포인트로 이루어진 상대적 위치 가반 터 치 패턴 잠금 해제 사례를 예로 들어 설명한다. 잠금 해 제 패턴 로직은 아래와 같다. 5개의 터치 포인트를 순서

대로 1PT, 2PT, 3PT, 4PT, 5PT로 표시했다. 여기 서 상대적 위치란 바로 이전의 터치 위치와 현재 터치 위 치 사이의 상대적 관계를 의미한다. 각 터치 포인트의 로 직을 정리하면 아래와 같다.

1PT:최초 시작 포인트

2PT:1PT 기준 상대적 우(右)

3PT:2PT 기준 상대적 상(上)

4PT:3PT 기준 상대적 하(下)

5PT:4PT 기준 상대적 우(右)

상대적 상, 하, 좌, 우의 관계는 터치포인트의 좌표값 의 관계다. 때문에 좌표값이 존재하는 모든 터치스크린, 패드 상에 적용 가능하다. 상술한 5개 터치 포인트로 이 루어진 상대적 위치 가반 터치 패턴 잠금 해제 패턴을 좌 표값 관계 로직으로 표시하면 아래와 같다.

1PT(x1, y1):최초 시작 포인트

 $2PT(x2, y2):x2 \times 1$ 

3PT(x3, y3):y3(y2)

 $4PT(x4, y4):y4\rangle y3$ 

5PT(x5, y5):x5x4

사례로 사용한 스크린의 좌표 체계와 잠금 해제 로직 을 표시하면 Fig. 1과 같다.

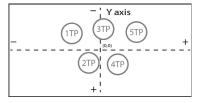


Fig. 1. Coordinate system of the case.

#### 3.4 상대 위치 기반 패턴 특성

상대적 위치 기반 터치 패턴 잠금 해제는 패턴의 형태 가 상대적 위치에 의해 결정되기에 한 가지 유일한 형태 로 정형화할 수 없다. 똑같은 로직을 갖고 있는 패턴도 여려 형태를 가질 수 있다. 상기 사례에서 제기한 잠금 해제 로직을 여러 형태로 완성한 모습을 표시하면 Fig. 2 와 같다.

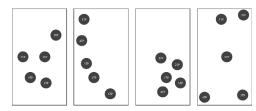


Fig. 2. The case of same logic with different forms

때문에 암호 패턴을 입력하는 과정에서 제3자가 옆에 서 패턴을 도취하는 위험에 노출되어 있을 시 단일 형태 를 갖고 있는 패턴에 비해 도취 난이도가 높아진다. 잠금 해제 패턴은 상대적 위치를 기반으로 하기에 숫자입력 자판과 같은 시각적인 명확한 입력 위치를 인터페이스에 서 설정할 필요가 없다. 시각적인 요소를 제거한 인터페 이스에서 잠금 해제 인터랙션이 가능하기에 동일한 맥락 으로 인터페이스를 보지 않는 상황에서도 잠금 해제를 진행할 수 있다. 시각적인 제한을 제거해 주었기에 기타 잠금 해제 인터랙션에 비해 실행 효율을 높임과 동시에 보안성을 강화하는 효과가 있다. 본 연구에서 제안하는 상대적 위치를 기반 잠금 해제 솔루션은 기존의 생체신 호를 활용한 잠금 해제 방식에 비해 추가적인 센싱 모듈 을 사용할 필요 없이 터치스크린의 기본 센싱 기능만으 로 실현 가능하기에 상대적으로 적은 원가로 제작할 수 있으면 특정 개체의 접근이 아닌 다수 개체의 접근을 가 능하게 한다. 이외 시각적 요소가 필요 없는 방식이기에 시각 장애인과 같은 특수 사용자들도 불편함 없이 사용 할 수 있다.

# 4. 실험

### 4.1 실험 계획

본 연구에서는 숫자암호 잠금 해제. 패턴 기반의 잠금 해제 와 상대적 위치 기반의 터치 잠금 해제 방식의 사용 성과 보안성 차이를 알아보고 상대적 위치 기반 패턴 잠 금 해제 방식의 실용적 가치를 확인하기 위하여 각각의 잠금 해제 방식을 적용한 잠금 해제 콘텍스트를 설계했 다. 숫자암호 잠금 해제, 상대적 위치 기반 터치 잠금 해 제 프로토타입은 Origami studio를 활용하여 제작했고 패턴 기반의 잠금 해제는 안드로이드 디바이스의 패턴 잠금 해제 기능을 사용했다. 실험에서 사용한 잠금 해제 암호는 전부 랜덤으로 생성했으며 Origami studio프로 그램 내에 탑재된 Random Patch를 통해 램덤수를 추 출하여 각각의 잠금 해제 방식에 적용했다. 4자리 암호와 6자리 암호는 비교적 범용으로 사용되고 있는 방식이다. PIN 암호와 아이폰 숫자암호 설정에서 4자리 숫자암호 를 최소 자리수로 하고 있는데 이는 4자리 암호로 구성 할 수 있는 암호의 경우의 수가 10,000개가 되기에 3자 리의 1000개의 경우의 수에 비해 해독 난이도가 어느 정 도 보장되고 동시에 기억 부담도 비교적 적기 때문이다. 본 연구에서는 가능한 동일한 상황에서 비교를 진행하기 위하여 숫자암호는 각 4자리 암호와 5자리, 6자리 암호를 사용하고 상대 위치 기반 터치포인트도 4포인트와 5 포인트, 6포인트를 사용하고 패턴의 경우 그리는 선의 꺾이는 회수를 기준으로 하여 각각 4회, 5회, 6회 꺾임 패턴을 사용했다. 랜덤으로 생성된 암호에서 반복되는 횟수가 많거나 기억 난도가 특별히 낮은 암호는 배제했다. 각실험 참여자는 한 가지 잠금 해제 방식을 사용하게 지정하고 한 방식에 10명의 실험 참가자를 배정했다(총 90명).

#### 4.2 실험

#### 4.2.1 사용성 실험

사용성 부분에서는 잠금 해제 암호의 특성상 쉽게 기억하여 사용해야 하는 부분을 고려하여 학습 용이성(기억 용이성)을 중심으로 실험 콘텍스트를 설정하고 새로운 방식의 암호를 기억하여 사용함에 있어서 기존의 암호 방식과의 차이를 알아봤다. 숫자암호를 기억하는데 걸리는 시간과 상대 위치 기반 암호를 기억하는데 걸리는 시간에는 차이가 있을 것이라는 가설을 세워 양자 간의차이 존재 여부를 독립표본 t-검증을 통해 검정했다. 그리기 패턴 암호를 기억하는데 걸리는 시간과 상대 위치기반 암호를 기억하는데 걸리는 시간과 상대위치기반 암호를 기억하는데 걸리는 시간의 차이 존재 여부도 같은 방식으로 검정하여 현재 주로 사용되는 잠금 해제 방식에 비해 상대위치 암호의 학습 용이성에 차이가있는지를 확인해 봤다.

각 실험 참여자한테 배정받은 암호 해제 방식을 기억하게 하고 1일 1회 잠금 해제를 실행하게 했다. 실행 결과는 체크리스트를 제공하여 매일 잠금 해제 실행 성공여부를 체크하게 한다. 총 2주(14일) 동안 임무를 수행후 각각의 잠금 해제 방식을 완전히 기억하는데 수요되는 시간을 기록했다.

#### 4.2.2 보안성 실험

보안성 부분은 일상생활 속에서 일어날 수 있는 위험 요소에 주목하여 사용자가 가장 우려하는 암호 해제 과정 중 제3자에 의한 암호 도취 상황을 핵심 실험 콘텍스트로 지정하고 잠금 해제 실행자에 대한 훔쳐보기 공격을 가하는 방식으로 진행했다. 동일한 조건에서 실험을 진행하기 위하여 잠금 해제 실행자에 대해서는 잠금 해제 시 인위적으로 공격자의 시야를 가리는 행동을 금지하고 공격자한테 잠금 해제 과정 자체를 제외한 기타 방해요소가 없는 환경을 마련했다.

각 잠금 해제 실행 과정에서 회당 1명의 공격자를 배정하고 총 10회 잠금 해제를 실행했다. 즉 한 잠금 해제 방안은 총 10명의 공격자가 각각 1회씩 공격을 진행했다. 공격 실행 후 공격자는 공격한 잠금 해제에 대한 잠금 해제 시도를 통해 공격의 성공 여부를 판단했다. 실험을 통해 얻은 공격 성공 확률 데이터를 기반으로 각 잠금 해제 방식의 보안성 차이를 비교했다. 실험 종료 후 각참여자들의 실험에 관한 피드백을 추가로 수집했다.

# 4.3.1 학습 용이성 실험 결과 및 분석

학습의 용이성을 비교하기 위하여 진행한 2주(14일) 간 실험 결과는 아래와 같다. (Table 1-3 참고)

Table 1. Number password memory results

	Type count	Total participants	Memorization day Average
Four-digit number	10	10	1.1
Five-digit number	10	10	1.8
Six-digit number	10	10	3.9

Table 2. Line drawing pattern memory results

	Type count	Total participants	Memorization day Average
Four times folded	10	10	1
Five times folded.	10	10	1.3
Six times folded.	10	10	2.5

Table 3. Relative position pattern memory results

			1
	Type count	Total participants	Memorization day Average
Four-point 10		10	1
Five-point 10		10	1.7
Six-point	10	10	2

우선 첫 번째로 숫자 암호와 상대 위치 패턴 암호는 기억하는데 걸리는 시간에 차이가 있을 것이라는 가설을 설정했다. 독립변인은 숫자암호 방식(1)과 상대 위치 패턴 방식(2)로 구분하고 종속변인인 완전히 기억하는데 걸린 시간은 실험 일 수에 근거하여 1~15로 척도를 지정하여 측정했다. 독립표본 t-검정 결과는 Table 4와 같다.

Table 4. T-test result (Independent variable: number code & relative position pattern)

	Number code	Relative position pattern	
Average	2.2667	1.5667	
Standard deviation	1.65952	0.77385	
Cases	30 30		
t value -2.094		-2.094	
p-value	0.041		

Table 4 와 같이 독립표본 t-검정 결과를 살펴보면 잠금 해제 방식에 따른 암호를 기억하는데 걸리는 시간에는 통계적으로 유의미한 차이가 있는 것으로 나타났다. t값 -2.094, 자유도58, 유의확률 0.041. 평균값을 보면 숫자암호 방식을 기억하는데 걸리는 평균 시간은 2.26일이고 상대 위치 패턴 방식을 기억하는데 걸리는 평균 시간은 1.56일로 나타나 상대적 위치 패턴 방식을 기억하는데 걸리는 시간 보다 조금 빠르다고 할 수 있다. 이로써 숫자 암호 잠금해제 방식과 상대적 위치 패턴 암호를 기억하는데 걸리는 시간에 차이가 있으므로 가설은 채택되었다.

다음으로 패턴 그리기 방식과 상대적 위치 패턴 방식을 기억하는데 걸리는 시간의 차이를 동일한 방식으로 검정했다. 독립변인은 패턴 그리기 방식(1)과 상대적 위치 패턴 방식(2)로 구분하고 종속변인인 완전히 기억하는데 걸린 시간은 실험 일 수에 근거하여 1~15로 척도를 지정하여 측정했다. 독립표본 t-검정 결과는 Table 5와 같다.

Table 5. T-test result (Independent variable: line drawing pattern & relative position pattern)

	Line drawing pattern	Relative position pattern	
Average	1.6000	1.5667	
Standard deviation	0.77013	0.77385	
Cases	30 30		
t value	-0.167		
p-value	0.868		

Table 5와 같이 독립표본 t-검정 결과를 살펴보면 잠금 해제 방식에 따른 암호를 기억하는데 걸리는 시간에는 통계적으로 유의미한 차이가 없는 것으로 나타났다. t값 -0.167, 자유도58, 유의확률 0.868. 패턴 그리기 방식을 기억하는데 걸리는 평균 시간은 1.6일이고 상대위치 패턴 방식을 기억하는데 걸리는 평균 시간은 1.56일

이다. 이로써 패턴 그리기 암호 잠금 해제 방식과 상대적 위치 패턴 암호를 기억하는데 걸리는 시간에 유의미한 차이가 없으므로 가설은 기각되었다. 숫자 잠금 해제 암 호를 기억하는데 걸리는 시간과 상대적 위치 패턴 암호 를 기억하는데 걸리는 시간에는 통계적으로 유의미한 차 이가 있고 패턴 그리기 암호를 기억하는데 걸리는 시간 과 상대적 위치 패턴 암호를 기억하는데 걸리는 시간에 는 통계적으로 유의미한 차이가 없었다. 숫자 암호는 텍 스트 기억 방식으로 각 숫자의 배열 순서를 기억해야 한 다. 패턴 그리기 암호는 주로 도형 기억 방식으로 기억하 게 된다. 상대적 위치 기반 패턴 잠금 해제 같은 경우 참 여한 실험 참가자들 일부는 상하좌우 방식으로 상대적인 위치 배열로 기억했고 그리고 나머지 일부 사용자는 상 대적 위치를 서로 연결해 형성된 패턴 형태를 기억했다. 상대적 위치 기반 패턴 암호는 텍스트 방식의 암호와 도 형 형식의 암호가 가지는 특징을 동시에 갖고 있다. 결론 적으로 상대적 위치 패턴 잠금 해제 방식은 숫자 암호 방 식보다 쉽게 기억되고 그리기 패턴 방식과 비슷한 정도 의 학습 용이성을 보여주기에 충분히 실용적 가치가 있 다고 볼 수 있다.

#### 4.3.2 보안성 실험 결과 및 분석

보안성을 확인하기 위한 훔쳐보기 공격 실험 결과는 아래와 같다. (Table 6-8 참고)

Table 6. The result of number password decoding record

	Type count	Total participants	Attack success rate	Average
Four-digit number	5	50	100%	
Five-digit number	5	50	100%	99.3%
Six-digit number	5	50	98%	

Table 7. The result of line drawing pattern decoding record

	Type count	Total participants	Attack success rate	Average
Four times folded	5	50	88%	
Five times folded	5	50	84%	78%
Six times folded	5	50	62%	

Table 8. The result of relative position pattern decoding record

	Type count	Total participants	Attack success rate	Average
Four-point	5	50	6%	
Five-point	5	50	0%	2%
Six-point	5	50	0%	

숫자 암호 방식에 대한 공격은 4자리수 100%성공, 5 자리수 100%성공, 6자리수98%성공으로 전부 훔쳐보기 공격에 취약한 결과를 나타냈다. 패턴 그리기 암호 방식 에 대한 공격은 4회 꺾임88%성공, 5회 꺾임 84%성공, 6회 꺾임 62%성공으로서 숫자 암호 방식에 비해 공격의 성공률은 조금 낮은 것으로 보이나 평균 성공률 78%로 서 패턴 그리기 잠금 해제 방식도 역시 훔쳐보기 공격에 취약하다고 볼 수 있다. 마지막으로 상대적 위치 패턴 방 식에 대한 공격 결과는 4포인트 6%성공, 5포인트 0%성 공, 6포인트 0%성공으로 나타났다. 평균 공격 성공률2% 로 다른 두 잠금 해제 방식에 비해 훔쳐보기 공격에 확연 히 강한 모습을 보여줬다. 이로써 상대적 위치 패턴 암호 잠금 해제 방식은 암호 해제 과정 중 제3자에 의한 암호 도취 상황에서 숫자 암호 잠금 해제 방식과 패턴 그리기 암호 잠금 해제 방식보다 보안성이 강하다고 볼 수 있기 에 실용적 가치도 상대적으로 높다고 할 수 있다.

상대적 위치 기반 패턴 암호는 전반적으로 훔쳐보기 공격에서 안전한 결과가 나왔다. 그중 공격에 성공한 공격자들의 해독 방법에 대해 알아봤다. 상대 위치 패턴에서 각 터치 포인트 사이 거리를 크게 잡을 경우 이를 선명한 도형으로 인식하고 해독했다는 것을 알았다. 그리고 패턴의 실제 로직은 해독 실패했으나 임의로 스크린을 터치하여 잠금 해제되는 현상이 있었다. 4자리 상대 위치같은 경우 첫 포인트는 기준 포인트이고 패턴의 해독 확률은 나머지 3개 터치 포인트 위치에 의해 결정된다. 즉경우의 수가 4x4x4=64이고 해독 확률은 1/64이 된다. 타 방식에 비해 다소 높은 확률로 해독이 가능하기에 4자리 상대 위치 패턴에서는 동일한 방식으로 대량의 시도를 해 보았으나무작위 클릭 시 해독되는 상황은 나타나지 않았다.

#### 5. 결론

블라인드 인터랙션 기반의 상대적 위치 패턴 잠금 해 제 솔루션은 개인 혹은 다수의 대상이 사용하는 디바이 스에 적용 가능한 솔루션이다. 상대적 위치 기반 패턴 잠 금 해제는 패턴의 형태가 상대적 위치에 의해서 결정되 기에 이론적으로 무한한 형태를 가질 수 있어 단일 형태 만 갖고 있는 암호에 비해 도취 난도가 높다. 시각적인 제한을 제거해 주었기에 화면을 보지 않는 상황에서도 잠금 해제를 쉽게 실행할 수 있어 효율적인 면에서도 경 쟁력을 갖고 있다. 숫자 잠금 해제 암호를 기억하는데 걸 리는 시간과 상대적 위치 패턴 암호를 기억하는데 걸리 는 시간에는 통계적으로 차이가 있고 패턴 그리기 암호 를 기억하는데 걸리는 시간과 상대적 위치 패턴 암호를 기억하는데 걸리는 시간에는 통계적으로 차이가 없다. 상 대적 위치 패턴 잠금 해제 방식은 숫자 암호 방식보다 쉽 게 기억되고 그리기 패턴 방식과 비슷한 정도의 학습 용 이성을 보여주기에 충분한 실용적 가치가 있다고 할 수 있다. 상대적 위치 패턴 암호 잠금 해제 방식은 숫자 암 호 방식과 패턴 그리기 방식에 비해 훔쳐보기 공격에 안 전하다. 때문에 실용적 가치도 상대적으로 높다고 볼 수 있다. 상대적 위치 패턴을 실제 제품에 적용 시 5~6자리 혹은 그 이상의 자릿수를 사용하는 것이 더 안전하다. 그 리고 상대적 위치 패턴에서 각 터치 포인트 사이의 공간 을 크게 잡는 것보다 작게 잡는 것이 보안성의 제고에 더 도움이 된다. 블라인드 인터랙션이 적용된 상대적 위치 기반 패턴 잠금 해제 솔루션은 하나의 새로운 잠금 해제 방식으로서 다양한 디바이스에 적용할 수 있다. 추가적인 센싱 모듈을 사용할 필요 없이 터치스크린의 기본 센싱 기능만으로 실현 가능하기에 적은 원가로 제작할 수 있 으면 시각 장애인과 같은 특수 사용자들도 불편함 없이 사용할 수 있다. 아직은 경우의 수가 비교적 낮은 부분을 비롯한 일부 한계점이 존재 하지만 내부적인 로직을 개 선하거나 타 블라인드 요소를 접목시켜 보다 높은 경우 의 수를 확보할 수 있는 방안을 고안해 볼 수 있다. 추후 적합한 사용 환경이나 사용 콘텍스트에 관한 연구를 지 속적으로 진행하여 비교적 적절한 적용 방향을 고안해 볼 수 있다. 새로운 잠금 해제 솔루션으로서 다양한 제품 에 적용될 수 있는 것에 대해 긍정적인 결과가 있을 것으 로 예상한다.

# **REFERENCES**

- [1] K. P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook & E. E. Schultz. (2007). Password Security and Memorability to Protect Personal and Organizational Information. *International Journal of Human-Computer Studies*, 65(8), 744-757.
- [2] A. S. Brown, E. Bracken, S. Zoccoli & K. Douglas. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641-651.
- [3] R. Biddle. S. Chiasson & P. C. Van Oorschot. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), 1-41.
- [4] L. Standing, J. Conezio & R. N. Haber. (1970). Perception and Memory for Pictures: Single-trial Learning of 2500 Visual Stimuli. *Psychonomic Science*, 19(2), 73-74.
- [5] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot & R. Biddle. (2009). Multiple Password Interference in Text Passwords and Click-based Graphical Passwords. CCS'09, (pp. 500-511). New York: ACM.
- [6] B. Kirkpatrick. (1894). An experimental study of memory. Psychological Review, 1, 602-609.
- [7] S. Madigan. (1983). Picture memory. Essays in Honor of Allan Paivio, chapter3, (pp. 65-89). Hillsdale: Lawrence Erlbaum Associates.
- [8] A. Paivio, T. Rogers & P. C. Smythe. (1968). Why are pictures easier to recall than words?. *Psychonomic Science*, 11, 137-138.
- [9] R. Shepard. (1967). Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning* and Verbal Behavior, 6, 156-163.
- [10] G. H. Bower, M. B. Karlin & A. Dueck (1975). Comprehension and memory for pictures. *Memory and Cognition*, 3, 216-220.
- [11] L. Standing. (1973). Learning 10,000 pictures. Quarterly Journal of Experimental Psychology, 25, 207-222.
- [12] E. Von Zezschwitz, A. De Luca, P. Janssen & H. Hussmann. (2015). Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)lock Patterns. CHI '15, (pp. 2339-2342). New York: ACM.
- [13] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze & J.M. Smith. (2010). Smudge attacks on smartphone touch screens. WOOT'10, USENIX, (pp. 2339-2342). CA: Association Berkeley.
- [14] Z. X. Jin & Y. H. Pan. (2016). A Taxonomy of Uninterpretable Interactions from Interaction Design Perspective. *Journal of the Ergonomic Society of Korea*, 52(1), 53-65. DOI: 10.5143/JESK.2016.35.1.53
- [15] L. Tao. (2018). Interaction Design Language. Beijing: Tsinghua University Press.

- [16] K. Kim & J. H. Kim. (2018). A Development of an Low Cost Smart Parcel Service System with Enhanced Security. *Journal of Convergence for Information Technology*, 8(6), 193-199.
  - DOI: 10.22156/CS4SMB.2018.8.6.193
- [17] S. Hong. (2019). Security Vulnerability and Countermeasure on 5G Networks: Survey. *Journal of Digital Convergence*, 17(12), 197–202.
- [18] S. Hong. (2018). Research on Security Model and Requirements for Fog Computing: Survey. *Journal of the Korea Convergence Society*, 9(5), 27-32.

# 김 주 웅(Zhou-Xiong Jin) [정회원]



- · 2009년 6월 : Yanbian University of Science & Technology 건축학 과(공학학사)
- · 2016년 2월 : 국민대학교 테크노디자 인전문대학원 인터랙션디자인전공(디 자인학석사)
- · 2016년 3월 ~ 현재 : 국민대학교 테

크노디자인전문대학원 인터랙션디자인전공 박사과정 · 관심분야 : 인터랙션 디자인, 블라인드 인터랙션

· E-Mail: jodesign19@gmail.com

# 반 영 환(Young-Hwan, Pin) [정회원]



- · 1991년 2월 : 한국과학기술원 산업공 학과(공학학사)
- · 1993년 2월 : 한국과학기술원 인간공
- 학(공학석사)
- · 1999년 8월 : 한국과학기술원 인간공
  - 학(공학박사)
- · 2006년 9월 ~ 현재 : 국민대학교 테크

노디자인전문대학원 교수

· 관심분야 : 인터랙션 디자인, 사용자 경험(UX)

· E-Mail: peterpan@kookmin.ac.kr