산업융합연구 제22권 제2호 pp. 63-71, 2024
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2024.22.2.063

롤러블 및 벤더블 디스플레이 환경에 적합한 가변행렬 기반 보안 키패드

최동민*
조선대학교 자유전공학부 교수

An Adaptive matrix-based Secure Keypad designed for Rollable and Bendable Display Environments

Dong-Min Choi*
Professor, Div. of General Studies, Chosun University

요 약 기존 스마트폰에서 사용된 PIN과 같은 인증기법은 디스플레이 구조의 변형 또는 화면 크기의 가변성에 대한 고려가 이루어지지 않아 최근의 가변 디스플레이 기반 스마트폰에 적용될 경우 비밀정보 입력부의 축소나 확대로 발생 가능한 취약점과 같은 디스플레이 면적의 변형에 따른 사회공학 공격에 대한 취약점이 있다. 본 연구는 롤러블 및 벤더블 스마트폰과 같이 디스플레이 크기 변화에 대응하는 보안 키패드를 제안한다. 이를 위해 우선 각 기존 인증기법에서 새로운 폼팩터에 적용될 경우 발생할 수 있는 보안 문제를 분석하였으며 이에 대응하는 보안 요구사항을 도출하였다. 제안하는 보안 키패드는 롤러블 및 벤더블 스마트폰의 디스플레이 크기에 따라 입력에 적합한 간격과 크기로 키의 배열 및 배치가 변형 가능하므로 화면 크기가 작을 때 발생할 수 있는 키 입력 오류 문제를 고려하였다. 또한, 키 입력 좌표를 불규칙적으로 분산하여 사회공학 공격에 대한 입력 정보 유출 문제도 고려하였다. 제안 기법은 다양한 크기와 형태의 스마트폰에서 사용할 수 있어 기존 기법보다 더 나은 사용자 경험과 보안성을 제공한다.

키워드 : 롤러블, 벤더블 스마트폰, 사회공학 공격, 보안 키패드, 스와이프, 키 배열

Abstract Conventional methods like PIN used in conventional smartphone form factor have not considered the variation in display structure or screen size. As a result, when applied to recent variable display-based smartphones, the secret information input unit may get reduced or enlarged, leading to vulnerabilities for social engineering attacks due to deformation of the display area. This study proposes a secure keypad that responds to changes in display size in rollable and bendable smart phones. Firstly, the security problems that may arise when applying classical authentication methods to new form factors were analyzed, and corresponding security requirements were derived. The proposed security keypad addresses the key input error problem that can occur when the screen size is small. The arrangement and size of keys can be deformed with the spacing suitable for input depending on the display size of rollable and bendable smartphones. The study also considered the problem of leaking input information for social engineering attacks by irregularly distributing key input coordinates. The proposed method provides better user experience and security than existing methods and can be used in smartphones of various sizes and shapes.

Key Words : Rollable, Bendable smartphone, Social engineering, Secure keypad, Swipe, Key array

This study was supported by research fund from Chosun University, 2021.
*Corresponding Author : Dong-Min Choi(jdmcc@chosun.ac.kr)
Received January 18, 2024 Revised February 8, 2024
Accepted February 20, 2024 Published February 28, 2024

1. 서론

스마트폰의 폼팩터란 스마트폰의 물리적 배열이나 구성을 의미하는 말로, 스마트폰의 크기나 디자인 등 외형을 결정하는 요소이다[1].

이러한 스마트폰 폼팩터는 2007년 애플 아이폰 등장 이후 10여년 동안 크게 변화하지 않았으나, 2019년부터 5G와 폴더블 스마트폰의 출시로 인해 다양한 형태로 변하고 있다[2]. 폴더블, 벤더블, 롤러블 스마트폰은 디스플레이를 접거나 구부리거나 말 수 있는 유연한 형태의 스마트폰이다. 이러한 스마트폰은 기존의 고정된 크기와 비율을 극복하고 다양한 환경과 용도에 맞게 활용할 수 있다. 폴더블 스마트폰은 접을 수 있는 디스플레이를 사용하여 화면 크기를 유연하게 조절할 수 있는 장점이 있으며, 삼성전자는 갤럭시 Z 플립과 갤럭시 Z 폴드 시리즈로 이 분야에서 선도적인 역할을 하고 있다[3]. 중국 업체 중 오포(Oppo), TCL 등이 롤러블 스마트폰 시제품을 공개하였으며, 화웨이(Huawei), 샤오미(Xiaomi) 등도 벤더블 또는 폴더블 스마트폰 개발에 참여하고 있다[4].

스마트폰 보안기법은 스마트폰 사용자의 개인정보와 데이터를 보호하기 위한 기술로, 다양한 방식으로 발전해 왔다. 초기에는 비밀번호나 화면 패턴 등으로 잠급 설정하는 방식이 주류였으나, 지문 인식, 안면 인식, 홍채 인식 등 생체 인증 기술의 도입으로 이전보다 편리하고 안전한 방법으로 인증할 수 있게 되었다[5]. 그러나 최근의 사회공학 기법[6-9]을 고려하면 스마트폰의 폼팩터 변화는 사용자 인증기법의 안전성에 영향을 미칠 수 있다. 폴더블 스마트폰은 접혀 있을 때와 펴져 있을 때 화면 비율과 크기가 달라지므로, 생체 인증 기능의 위치와 작동 방식도 이를 고려하여 구현되어야 한다. 롤러블 및 벤더블 스마트폰은 일부 화면 영역을 사용할 수 있는 경우와 화면비의 변화와 같은 요소도 고려해야 하므로 다양한 구조와 상황에 적합한 유연하고 안전한 사용자 인증기법이 필요하다. 본 연구는 롤러블, 벤더블 규격의 스마트폰에 적용 가능한 보안 키패드 구조를 제안한다.

2. 관련연구

2.1 롤러블 및 벤더블 스마트폰 보안 문제

롤러블 및 벤더블 스마트폰의 경우 기존의 리지드 스마트폰 구조를 바탕으로 한 보안기법 설계가 적용된 보안 인증기법이 적용될 경우 다음과 같은 사회공학 기법에 취약할 수 있다.

2.1.1 엿보기 공격

엿보기 공격[6]은 글자 그대로 스마트폰을 사용하는 사용자 근처에서 비밀정보 입력을 엿보는 것이다. 이 기법은 스마트폰 화면에 나타난 모든 정보를 공격자 역시 열람 가능하므로 사용자가 입력하는 모든 정보와 화면에 나타나는 모든 정보는 유출된다.

2.1.2 레코딩 공격

레코딩 공격[7]은 엿보기 공격에 광학 영상 저장장치를 포함하는 것이다. 이 기법은 광학장비의 해상력에 따라 습득정보의 정확성이 높아지며 원거리에서도 비밀정보 취득이 가능하다. 또한, 취득 영상을 저장할 수 있어 반복재생이 가능하므로 취득정보의 정확도가 높아 공격 성공률도 높다.

2.1.3 스머지 공격

스머지 공격[8]은 스마트폰 사용자가 손가락으로 화면을 터치함에 따라 화면에 남게 되는 유분 흔적을 추적하여 비밀정보를 유추하는 공격으로 앞의 엿보기, 레코딩 공격과 다르게 스마트폰 사용자의 비밀정보 입력화면을 직접 관찰할 필요가 없고 유분 흔적을 통해 비밀정보를 추정한다.

2.1.4 열감지 공격

열감지 공격[9]은 스머지공격과 같은 비밀정보 추정 공격이며, 스마트폰 사용자가 손가락으로 화면을 터치함에 따라 화면에 남게 되는 잔열 흔적을 추적하여 비밀정보를 유추하는 공격이다.

2.2 보안기법

2.2.1 PIN과 패턴 인증기법

Personal Identification Number(PIN) 인증[10]은 4자리에서 8자리의 길이를 갖는 숫자 코드를 사용자의 인증 암호로 사용하는 지식 기반 인증기법으로 암호 입력이 편리하다. 패턴 인증기법[11]은 9개의 점을 연결하는 끊김 없는 선분의 조합을 인증방식으로 적용한 지식기반 인증기법이며, 같은 지식기반 인증기법이면서 다양한 키 입력을 사용하는 PIN에 비해 입력이 간편하다. 그러나 롤러블 및 벤더블 환경에서 해당 기법은 화면 UI의 구조 변경

이 없이 단순 확대 및 축소만 가능하므로 축소 시 발생하는 입력 편의성에 대한 문제가 있고, 확대 시에는 엿보기, 레코딩 공격과 같은 광학 기반 공격과 스머지, 열감지 공격과 같은 추정 공격에 비밀정보가 유출될 수 있다.

2.2.2 BendyPass

이 연구는 사용자가 비밀번호를 생성하고 기억하는 데 사용할 수 있는 방법인 "Bend Passwords"를 제안하고 있으며[12] 이전 연구에서 밝혀진 사용자 선호도를 바탕으로 간단한 구부리거나 접는 동작을 이용해 비밀번호를 조합, 입력하는 방법을 사용한다(Fig. 1 참고).

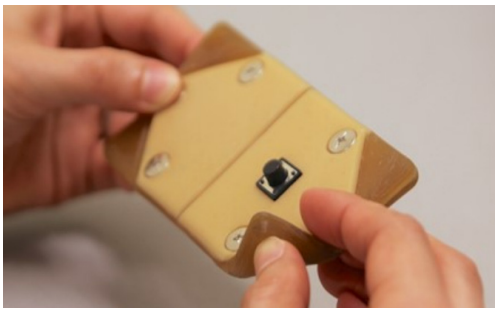

Fig. 1. BendyPass prototype

이 기법은 10개의 구분된 구부리거나 접는 동작을 이용해 PIN과 같은 수준의 입력 다양성을 확보할 수 있다. 또한, 이 방식은 시각 장애인들을 대상으로 한 실험에서 기존의 비밀번호 방식보다 쉽게 기억할 수 있으며, 사용자들이 편안하게 사용할 수 있음이 확인되었다. 그러나 학습에 필요한 시간 및 일반적인 기법과는 다른 조작으로 인한 불편감이 있으며 롤러블 및 벤더블 환경에서 기기 자체의 폼팩터가 구조적으로 해당 인증기법의 사용을 고려해야 하거나 별도의 하드웨어 인터페이스 추가와 같은 문제가 있고, 엿보기, 레코딩 공격과 같은 사회공학 공격으로 비밀정보가 유출될 수 있다.

2.2.3 Indirect Pattern Keypad

이 연구[13]에서 제안하는 키패드는 사용자는 PIN과 같이 숫자를 기억한다는 점에서는 같으나, 비밀번호의 입력은 암호를 알고 있다는 증명이 될 수 있는 암호와 연관된 간접 패턴을 입력하는 방법을 사용한다. 이 기법은 기존의 PIN 키패드 배열과 달리 무작위로 키 입력 위치가 바뀌며 비밀번호의 입력은 패턴 입력을 사용한다. Fig. 2는 비밀번호가 '1234'이며, 비밀번호 입력의 기준이 되는 시작점이 '3'일 때 비밀번호를 입력하는 방법이다.

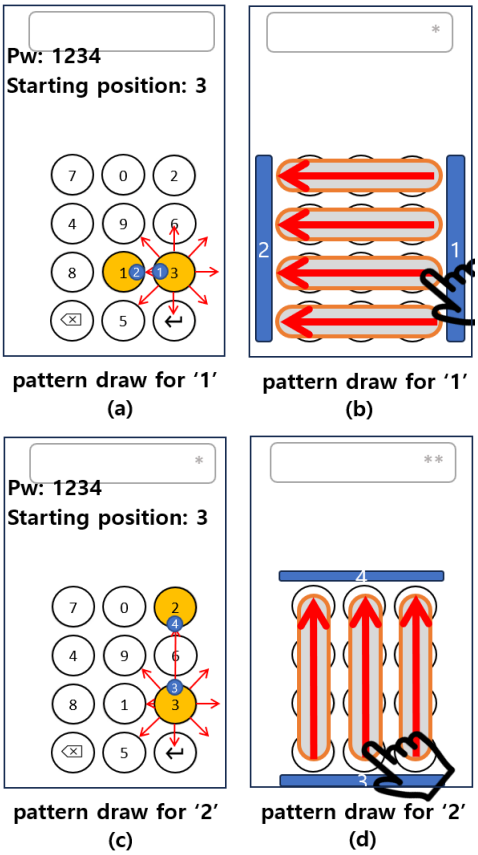

Fig. 2. Indirect pattern draw process

Fig. 2(a)에서 정해진 시작점 '3'의 위치에서 보았을 때 비밀번호 '1'의 위치와 연관된 8방향의 패턴 중 1->2 패턴을 그릴 수 있으며, 이 패턴은 Fig. 2(b)와 같이 4개의 패턴 '207', '694', '318', '↵ 5x'이 해당하며, 이 4가지 중 하나를 선택하여 패턴을 그린다. 여기서는 세 번째인 '318' 패턴을 그려 '1'을 입력했다. '2'를 입력하기 위해서는 'x'847', '5190', '↵ 362'의 3가지 패턴이 있으며 여기서는 두 번째인 '5190' 패턴을 그려 '2'를 입력했다. '3'은 시작점 '3'이 곧 입력값으로 사용될 수 있으므로 화면을 터치하면 바로 입력된다. '4'의 경우, '3'에서 출발하여 '1'을 거쳐 '4'로 가는 '직선+대각'의 조합과, '3'에서 출발하여 '9'를 거쳐 '4'로 가는 '대각+직선'의 조합이 있다. 직선 패턴은 '207', '694', '318', '↵ 5x'이 있으며, 대각 패턴은 '06', '397', '↵ 14', '58'이 있으므로 이들의 조합

으로 패턴을 그린다.

이 방식은 입력키의 위치가 무작위로 변하므로 같은 패턴이 발생하지 않으며 시작점에 의해서도 패턴이 바뀐다. 그러나 이 기법도 롤러블 및 벤더블 환경에서 화면UI의 구조 변경이 없이 단순 확대 및 축소만 가능하므로 축소 시 발생하는 입력 편의성에 대한 문제가 있고, 확대 시에는 엿보기, 레코딩 공격과 같은 사회공학 공격으로 비밀정보가 유출될 수 있다.

2.2.4 폴더블 스크린 보안 입력 기법

폴더블 스크린용 인증 기법[14]은 기존의 PIN 입력과 달리 화면상의 watch window에 표시된 정보만을 이용하여 스와이프 및 터치의 두 가지 동작만으로 입력하고자 하는 비밀정보를 선택하거나 입력하는 동작을 구현하였으며 이를 통해 비밀번호를 입력할 수 있도록 하였다(Fig. 3 참고).

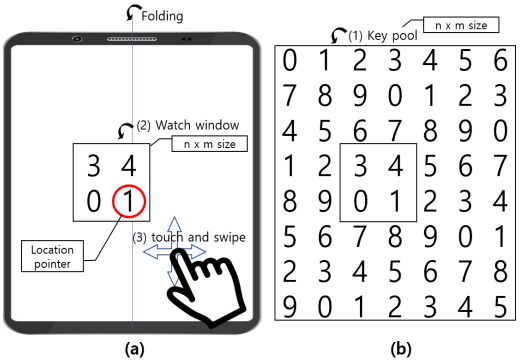

Fig. 3. Secure keypad for foldable screen devices

Fig. 3(b)는 화면 영역에 구성된 키 풀의 집합이며 최대 nxm(여기서는 7x8)으로 임의 구성된다. 이 구조는 상하단과 좌우 끝단이 맞닿아있는 순환식 테이블 구조이며 실제 사용자 화면에 보이지는 않고 Fig. 3(a)의 watch window를 통해서만 육안으로 확인할 수 있다. 이 watch window의 크기는 조정 가능하다(여기서는 2x2). 사용자는 watch window의 특정 영역을 키 입력을 위한 location pointer로 지정하여 이 영역에 있는 문자를 입력한다. Fig. 3의 (3) touch and swipe 영역은 watch window 영역을 제외한 모든 영역이다. 비밀정보가 '1234'일 경우, watch window의 (2, 2) 자리에 '1' 이 있으므로 그대로 스크린을 터치하여 '1'을 입력하며, '2' 입력을 위해 화면을 상하좌우로 스와이프하다가 watch window에 '2'가 보이면 '2'를 watch window의 (2, 2) 자리로 맞추어 놓고 터치하여 '2'를 입력한다.

이 기법은 watch window의 사용으로 엿보기, 레코딩 공격에 대해 외부로 유출되는 정보가 적으며 스머지 및 열감지 공격에 대해서도 위치 추정이 어려워 사회공학 공격에 대한 안전성을 갖추고 있고, 스와이프와 터치 두 가지 동작으로 비밀번호를 입력할 수 있어 사용자 편의성이 좋다. 그러나 롤러블 및 벤더블 환경에서 해당 기법은 화면UI의 구조 변경이 없이 단순 확대 및 축소만 가능하므로 축소 시 발생하는 입력 편의성에 대한 문제, 그리고 확대 시 발생할 수 있는 엿보기, 레코딩 공격과 같은 사회공학 공격에 대한 안전성의 문제는 watch window의 크기에 비례하고 행렬의 크기에 반비례하여 커질 수 있다.

2.2.5 이중 터치 기반 보안 키패드

이중 터치 기반 보안 키패드 기법[15]은 비밀번호 입력에 그룹화된 키패드를 사용한다(Fig. 4 참고).

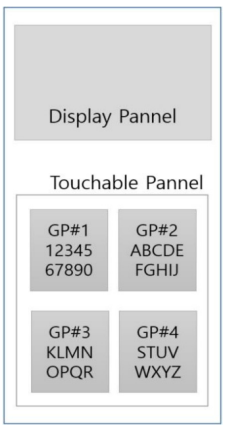

Fig. 4. Double-touch based secure keypad

그룹 키패드는 여러 개의 숫자나 문자가 하나의 버튼으로 묶여 있는 것으로 모든 숫자와 문자는 여러 개의 그룹으로 나누어져 구분되어 있다. 사용자는 비밀번호 입력에 해당하는 문자나 숫자가 포함된 그룹을 선택한 후 내부에 있는 숫자나 문자를 선택하여 입력한다. 이 기법은 기존 보안 키패드 대비 입력 오류율이 낮다. 그러나 롤러블 및 벤더블 환경에서 해당 기법은 화면UI의 구조 변경이 없이 단순 확대 및 축소만 가능하므로 UI 축소 시 발생하는 입력 편의성에 대한 문제는 여전하며 확대 시 발생하는 엿보기, 레코딩 공격과 같은 사회공학 공격에 대한

안전성 문제는 그룹화된 키패드의 그룹 크기에 비례하여 커질 수 있다.

3. 가변행렬 기반 보안 키패드

본 연구는 벤더블 및 롤러블 스마트폰과 같이 변형된 디스플레이 구조를 고려한 사용자 보안 입력 기법을 제안한다. 기존에 제안되었던 기법들은 고정형 또는 가변형 디스플레이가 적용된 환경에서 고정된 형태의 입출력 UI를 사용하는 인증기법으로, Fig. 5와 같은 폼팩터에 적용된 벤더블 및 롤러블 디스플레이 구조는 고려하지 않고 있다. 제안하는 기법은 단순히 확대 및 축소만 가능한 기존 인증 UI와 달리 기기 디스플레이 구조에 적합하게 배열된 UI를 사용할 수 있어 구조적인 문제로 인해 발생 가능한 편의성 문제와 보안 취약점을 고려한 기법이다.

Fig. 5. Example of rollable and bendable display product

3.1 구조

제안하는 기법은 롤러블 및 벤더블 디스플레이가 적용된 스마트폰 디스플레이를 고려하였으며 입력은 PIN 또는 패스워드 인증의 지식기반 인증을 기초로 한다. 이 기법의 키패드 구조는 다음의 Fig. 6와 같다.

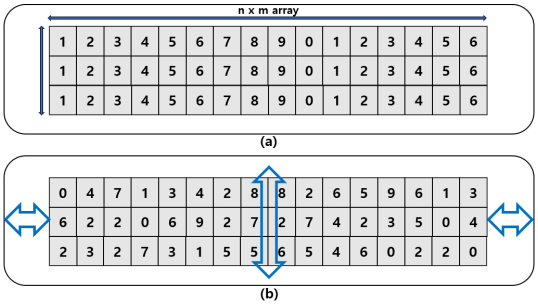

Fig. 6. N-array PIN with (a) default and (b) random array

3.2 Setup 단계

셋업 단계에서는 기기의 특성에 맞는 배열의 크기, 입력영역, 가시/비 가시 영역, 기준 포인터 그리드, 기준 포인터 그리드에 상대적인 실제 입력값의 위치, 그리고 비밀번호를 결정하는 단계이다.

Fig. 5와 같은 팔찌 형태의 일반적인 벤더블 스마트폰 구조를 고려할 경우, 제안기법은 Fig. 6의 구조로 디스플레이 비율에 맞추어 정렬된 nxm 배열의 숫자 또는 숫자와 문자가 혼합된 배열로 표시할 수 있다. 이 구조는 확대 및 축소 가능하며 이에 대한 기준은 각 기기의 디스플레이 규격과 기준 크기를 고려하여 표시할 수 있고 행과 열의 개수는 각각 1~n, 1~m으로 변경할 수 있다. 여기서는 팔찌 구조를 고려한 3행을 기준으로 하였다. 배열은 상하좌우 방향으로 스와이프 가능하며 각 끝단은 상호 연결된 환형 순환식 구조이다. 각 배열의 요소들은 임의배치 되어 비밀번호 추정 공격에 대응한다.

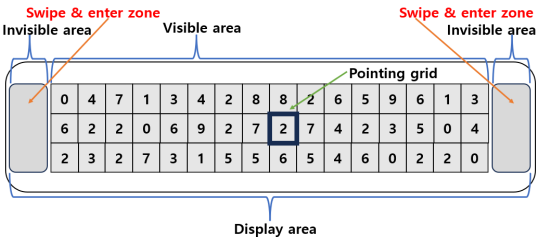

Fig. 7. Screen of proposed method

Fig. 7과 같이 제안기법은 크게 3가지 영역으로 구분된다. Display area는 디스플레이에서 물리적으로 정보가 표시 가능한 전체 영역을 뜻한다. 이 영역 안에 존재하는 Visible area는 실제 육안으로 확인할 수 있는 정보가 표시되는 영역이며 여기에 표시되는 nxm 크기의 문자 배열(여기서는 16x3 크기로 표현)은 크기가 커질수록 표시되는 정보의 양은 많아 각각의 크기가 작아지게 되므로 사용자가 자신의 기기에 맞게 적절한 수준으로 조절하여 크기를 변경할 수 있다. Visible area에 표시된 배열 가운데 굵은 사각형은 입력을 위한 기준점인 pointing grid이며 사용자가 임의로 위치를 변경할 수 있다. pointing grid는 실제 값이 입력되는 위치가 아니며 이 위치를 기준으로 실제 비밀정보가 입력되는 위치를 사용자가 결정할 수 있다. 마지막으로 Invisible area는 육안으로 확인할 수 있는 정보는 없는 영역으로써 이 영역 안의 Swipe

& enter zone에서만 터치, 스와이프 및 확대 축소와 같은 기능을 사용할 수 있도록 구별된 영역이다. 이 영역 또한 Visible area처럼 크기를 변경할 수 있다(Fig. 8 참고).

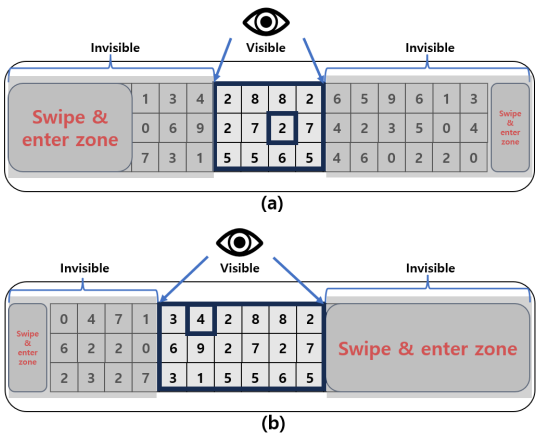

Fig. 8. Examples about changeable area setting of proposed method

Fig. 8과 같이 제안기법은 Display area 안에 크기가 조절 가능한 Visible, Invisible area, 그리고 Swipe & enter zone이 존재한다. Fig. 8(a)는 가운데의 4x3 배열만 육안으로 확인 가능한 영역이며 이 영역 안의 굵은 사각형은 입력을 위한 기준점인 pointing grid이다. 나머지 회색 톤으로 표시된 부분은 볼 수 있는 정보는 없는 영역이다. 본 연구의 Fig. 5에서 언급한 롤러블, 벤더블 디스플레이가 적용된 스마트폰의 팔찌 형태를 고려하면 보안 관점에서 볼 때 불필요하게 정보가 표시되는 영역이 있을 수 있고 이로 인해 외부 공격자에 의한 정보유출이 발생할 수도 있다. 또한 사용자 편의성 관점에서 볼 때 사용자가 보기 불편한 위치에 정보가 표시될 수 있어 사용에 불편감을 가질 수 있다. 따라서 Invisible area를 적절히 조절하도록 하여 보안 및 사용자 편의성을 고려하였다. Swipe & enter zone의 경우, 보안 관점에서 볼 때 외부 공격자에 의한 기기 조작 행동 관찰을 어렵게 하기 위한 목적과 사용자 편의성 관점에서 볼 때 사용자가 조작하기 편리한 위치에 Swipe & enter zone을 위치시켜 조작 편의성을 증대시키려는 목적을 갖는다. Fig. 8(b)는 Fig. 8(a)에 비해 영역과 위치가 변경된 Visible, Invisible area, Swipe & enter zone, 그리고 pointing grid를 나타내고 있다.

다음의 Fig. 9는 비밀번호 입력을 위한 입력 기준점이 되는 pointing grid와 이와 연관되어 실제 값이 입력되는 상대적인 위치에 대한 예시이다.

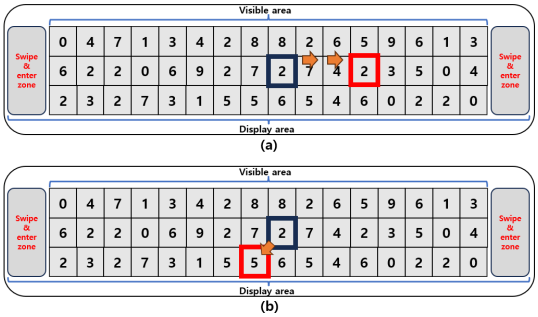

Fig. 9. Examples of actual input determined by pointing grid

Fig. 9(a)와 같이 사용자에 의해 결정된 실제로 값이 입력되는 위치가 흑색 사각형으로 표시된 pointing grid의 우측 3번째 자리였다면, 이 상태에서 Swipe & enter zone를 터치할 경우 붉은 격자로 표기된 부분이 실제 값이 입력되는 위치이므로 '2'가 선택된다. 또한, Fig. 9(b)와 같이 실제 입력값의 위치가 pointing grid의 좌측 하단자리였다면 현재 상태에서 Swipe & enter zone를 터치할 경우 붉은 격자로 표기된 '5'가 선택된다.

3.3 비밀번호 입력 절차

다음의 Fig. 10은 비밀번호가 '1234'이며 pointing grid의 우측 3번째 자리 실제 값이 입력되는 자리인 Fig. 9(a)와 같을 때 제안기법의 비밀번호 입력 순서이다.

비밀번호가 '1234'일 경우 '1'을 입력하기 위해 전체 Visible area에서 '1'의 위치를 찾는다. Fig. 10(a)와 같이 '1'은 총 3곳에 있으므로 이들 중 아무것이나 Swipe & enter zone을 이용해 상하좌우로 스와이프한다. 실제 값이 입력되는 위치인 pointing grid의 우측 3번째 자리로 스와이프하여 이동시킨 후 Swipe & enter zone을 터치하여 해당 값을 입력한다. '2'의 경우는 총 11곳에 있으며 이들 중 1곳은 실 입력 위치에 있으므로 바로 Swipe & enter zone을 터치해도 '2'가 입력된다. '3'의 경우는 총 4곳, '4'의 경우는 총 5곳에 있으므로 각각 차례대로 실 입력 위치에 Swipe & enter zone을 이용해 스와이프한 후 터치하면 비밀번호 입력을 할 수 있으며 모든 입력을 마치면 비밀번호 입력절차가 종료된다.

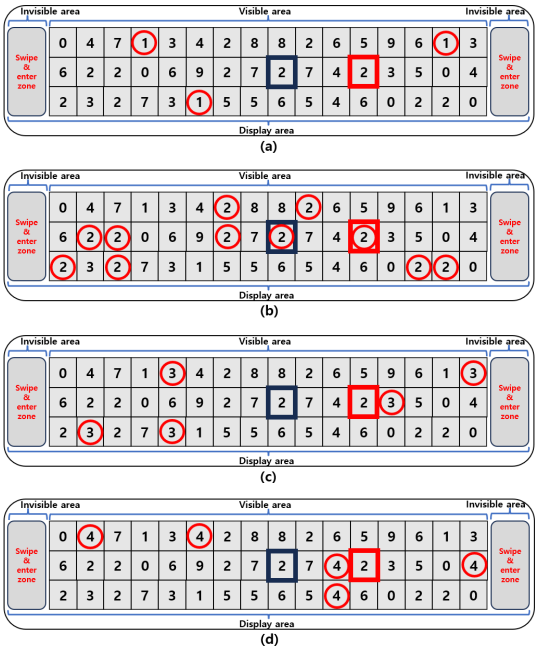

Fig. 10. Password input process

4. 안전성 및 편의성 분석

스마트폰의 보안 인증기법은 보안 안전성과 함께 사용자 편의성을 고려해야 한다. 보안 안전성은 고전 공격을 포함한 사회공학 공격에 대한 안전성을 의미하며, 사용자 편의성은 기법별로 적용된 비밀정보의 입출력 관련 전반적인 절차에 대해 사용자가 체감할 수 있는 입력과 출력에 대한 사용성이다. 이 장에서 우리는 제안기법의 안전성 및 편의성을 기존 기법 2가지와 함께 비교하였다.

4.1 보안 안전성

다음의 Table 1은 기존의 PIN, 이중 터지 기반 기법과 제안기법에 대해 롤러블, 벤더블 환경에서 사회공학 공격에 대한 보안 대책이 고려되어 있는지를 비교한 비교표이다.

Table 1. Security countermeasure comparison (c: considered, n: not considered)

Type of attack	Authentication method		
	PIN[10]	Double[15]	Proposed
Shoulder surfing	n	c	c
Recording	n	n	c
Smudge	n	c	c
Thermal	n	c	c

PIN의 보안 키패드는 비밀번호 입력 시 화면에 해당 정보가 바로 표시되므로 엿보기, 레코딩 공격에 의해 비밀정보가 바로 유출될 수 있다. 또한, 키패드 입력화면은 고정되어 변경되지 않으므로 유분 및 잔열에 의한 비밀번호 추정이 가능한 스머지, 열감지 공격에 취약하다.

이중 터치 기반 기법은 엿보기 공격을 고려한 기법으로 입력화면 그룹의 영역이 축소 표시되며 그룹의 문자로 임의 배정되므로 엿보기 공격을 통한 패스워드 추정 및 스머지와 열감지를 통한 패스워드 추정 공격에 확률적인 안전성을 기대할 수 있다. 그러나 확대 축소가 자유로운 광학 녹화 장비를 사용한 레코딩 공격의 경우 그룹의 비밀번호 입력과정이 그대로 누출, 녹화되므로 취약하다.

제안기법의 경우 터치 영역이 분리되어 제한된 구역에 있으므로 엿보기, 스머지, 열 감지 공격에 의한 비밀번호 추정이 어렵고, 비밀번호 입력과정을 직접 관찰 또는 녹화 재생하더라도 포인팅 그리드와 실 입력 위치에 대한 정보가 없다면 레코딩 공격에 의한 비밀번호 획득이 어렵다.

4.2 입력 편의성

다음의 Table 2는 기존의 PIN, 이중 터치 기반 기법과 제안기법을 4자리의 비밀정보를 입력한다고 가정했을 때, 이를 입력 편의성 측면에서 비교한 비교표이다.

Table 2. Input convenience comparison

Methods / Input	PIN[10]	Double[15]	Proposed
Input type	touch	touch	swipe + touch
number of inputs	5	5~11	4(swipe) +4(touch)

PIN의 보안 키패드는 각 키의 값이 고정되어 있거나 임의배치된 경우 모두 4자리의 입력값과 같은 횟수의 터치와 함께 입력종료를 의미한 엔터 키 터치를 포함하여 총 5회의 입력이 필요하다.

이중 터치 기반 기법은 모든 값이 하나의 그룹에 포함된 경우, 그룹 선택을 위한 터치 1회를 포함하여 4자리의 입력값과 같은 횟수의 터치가 필요하므로 적어도 5회의 터치가 필요하다. 최댓값은 모든 입력값이 별개의 그룹으로 분리되어있을 경우이며 이때는 처음 입력값이 포함된 그룹 선택을 위한 터치 1회와 입력값 선택을 위한 터치 1회, 그리고 해당 그룹에서 나오기 위한 'out' 키 터치 1회,

총 3회의 터치가 1자리의 입력에 포함된다. 이렇게 3회 반복하고 마지막 자리의 값은 'out' 키 입력은 제외하므로 모두 11회의 터치가 필요하다.

제안기법의 경우 최소값은 실 입력값의 위치가 4회 모두 일치하는 경우이며 이때는 터치 4회가 필요하다. 최댓값은 1회의 스와이프와 1회의 터치가 각 자리의 값 입력에 필요하므로 모두 8회의 스와이프와 터치가 필요하다.

5. 결론

본 연구에서 제안하는 기법은 롤러블 및 벤더블 디스플레이가 적용된 팔찌 구조의 스마트기기에서 기기의 구조를 고려한 보안 키패드이며 기존의 고전 인증기법에서 고려하지 못했던 변형 폼팩터 환경에서 발생할 수 있는 구조적, 외부적 요인에 의한 비밀정보 유출에 대응하는 기법이다.

플렉서블 디스플레이가 적용된 스마트폰 환경을 고려한다면 기존의 PIN, 패턴 인증 이외에도 현재 사용 중이거나 연구 중인 다양한 인증기법들에 대해서도 새로운 환경에 대한 보안성 검토가 필요하다.

제안기법은 이에 대해 가변 디스플레이 규격에 적응할 수 있는 유연한 크기의 입력 UI 문자 배열로 사용자 편의성을 고려하였으며, 이과 함께 가시, 비 가시 영역의 구분을 이용해 정보유출의 제한, 포인팅 그리드와 실 입력값 위치를 이용한 비밀정보 숨김, 그리고 스와이프 엔터존을 이용하여 비밀정보 추정 공격을 대비하였다.

향후 연구로써 우리는 플렉서블 이후의 환경인 디스플레이 크기를 물리적으로 키우거나 줄일 수 있는 구조인 스트레처블 디스플레이가 적용되는 미래의 폼리스 스마트폰 환경을 고려한 새로운 구조를 갖는 사용자 인증기법 연구를 진행하고자 한다.

REFERENCES

[1] J. Kim. (2020). *Tech trend, Endlessly evolving mobile device form factor evolution!* Samsung Display News room Tech Trend(Online). https://news.samsungdisplay.com

[2] J. E. Park. (2019). *First release of 5G foldable smartphone... Signal of change in form factor.* etnews(Online). https://www.etnews.com

[3] M. S. Kim. (2022). *What will the 'Rollable Phone', which will follow Samsung Electronics' foldable, look like.* Bizwatch(Online). https://news.bizwatch.co.kr/

[4] I. J. Choi. (2020). *Now, a 'rollable phone' that rolls and unfolds is coming.* Chosun Media (Online). https://www.chosun.com

[5] C. Wang, Y. Wang, Y. Chen, H. Liu & J. Liu. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks, 120(7),* 107118. DOI : 10.1016/j.comnet.2020.107118

[6] E. Miluzzo, A. Varshavsky, S. Balakrishnan & R.R. Choudhury. (2012, June). TapPrints: Your Finger Taps Have Fingerprints. *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services.* (pp. 323-336). Low Wood Bay : ACM. DOI : 10.1145/2307636.2307666

[7] T. Takada.(2008, October). Fake Pointer: An Authentication Scheme for Improving Security against Peeping Attacks using Video Cameras. *Proceeding of International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies.* (pp. 395-400). Valencia : IARIA. DOI : 10.1109/UBICOMM.2008.76

[8] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze & J.M. Smith. (2010, August). Smudge Attacks on Smartphone Touch Screens. *Proceeding of the 4th USENIX Conference on Offensive Technologies.* (pp. 1-7). Washington : ACM.

[9] Y. Abdelrahman, M. Khamis, S. Schneegass & F. Alt. (2017, May). Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* (pp. 3751-3763). Denver : ACM. DOI : 10.1145/3025453.3025461

[10] J. Kagan. (2023). Personal Identification Number (PIN): What It Is, How It's Used. Investopedia (Online). https://www.investopedia.com

[11] M. Shahzad, A.X. Liu & A. Samuel. (2013, September). Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You Can See It But You Can Not Do It. Proceeding of the 19th Annual International Conference on Mobile Computing & Networking. (pp. 39-50).

Miami : ACM. DOI : 10.1145/2500423.2500434

[12] D. B. Faustino, S. Nabil & Audrey Girouard. (2020, May). Bend or PIN: Studying Bend Password Authentication with People with Vision Impairment. Proceedings of Graphics Interface 2020. (pp. 183-191). Toronto : ACM. DOI : 10.20380/GI2020.19

[13] D. Choi. (2022). Design of Smartphone Secure Keypad Using Indirect Pattern. *Journal of Korea Multimedia Society, 25(7),* 932-944. DOI : 10.9717/kmms.2022.25.7.932

[14] D. Choi. (2021). A Study on User Authentication Method for Foldable Screen-Based Devices. *Journal of Korea Multimedia Society, 24(3),* 440-447. DOI : 10.9717/kmms.2020.24.3.44

[15] H. Mun. (2022). Design for Position Protection Secure Keypads based on Double-Touch using Grouping in the Fintech. *Journal of Convergence for Information Technology, 12(3),* 38-45. DOI : 10.22156/CS4SMB.2022.12.03.038

최 동 민(Dong-Min Choi) [정회원]

- 2003년 2월 : 경희대학교 공과대학 (공학사)
- 2007년 7월 : 조선대학교 교육대학 (교육학석사)
- 2011년 2월 : 조선대학교 컴퓨터공학과(공학박사)
- 2001년~2013년 : 조선대학교 BK사업팀 연구교수
- 2014년~현재 : 조선대학교 자유전공학부 부교수
- 관심분야 : 정보보안, 모바일 보안, 센서 네트워크 보안
- E-Mail : jdmcc@chosun.ac.kr