The Journal of the Convergence on Culture Technology (JCCT)
Vol. 10, No. 3, pp.885-890, May 31, 2024. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2024.10.3.885
JCCT 2024-5-101

스트레처블 디스플레이가 적용된 모바일 기기의 보안 키패드 연구

Research on Secure Keypads for Mobile Devices with Stretchable Displays

최동민*

Dongmin Choi*

요 약 본 연구는 스트레처블 디스플레이 기술이 적용된 모바일 기기의 화면 변화에 대응 가능한 보안 키패드 구조를 제안하였다. 이를 위해 우리는 현재의 리지드 폼 팩터 기반 스마트폰에 적용된 인증기법들을 스트레처블 디스플레이 기술의 전 단계에 해당하는 롤러블 및 벤더블 디스플레이 기술이 적용된 스마트폰에 적용된 인증기법들과 비교 분석하였다. 이 분석 결과를 바탕으로 우리는 스트레처블 디스플레이가 적용될 모바일 응용제품 규격인 스마트 월렛, 멀티태스킹, 스크린 확장 및 미디어 시청, 게임 및 엔터테인먼트용 폼팩터 구조에서 발생할 수 있는 사용자 편의성 문제와 보안 안전성 문제를 도출하였고 이에 대응하는 보안 키패드 구조를 제안하였다. 제안하는 보안 키패드 구조는 기존의 리지드 디스플레이 기반 폼 팩터 및 롤러블, 벤더블 디스플레이 기반 폼 팩터의 스마트폰 환경에 적용된 구조에 비해 더욱 향상된 사용자 편의성 및 보안 안전성을 제공한다.

주요어 : 리지드 디스플레이, 롤러블 디스플레이, 벤더블 디스플레이, 스트레처블 디스플레이, 보안위협, 사회공학 공격, 스마트폰, 보안 키패드

Abstract This study proposes a secure keypad structure that can adapt to screen changes in mobile devices equipped with stretchable display. For this purpose, we compared and analyzed the authentication methods applied to current rigid form factor smartphones with those applied to rollable and bendable display based smartphones, which are the previous stages of stretchable display. Based on the results of this analysis, we identified potential user convenience and security safety issues that may arise in the form factor structure for smart wallets, multitasking, screen expansion and media viewing, and gaming and entertainment applications where stretchable displays will be applied, then proposed a security keypad structure for these form factors. Our keypad structure provides enhanced user convenience and security compared to the structures applied in the smartphone environment based on the conventional rigid display form factor and rollable, bendable display form factor.

Key words : Rigid Display, Rollable Display, Bendable Display, Stretchable Display, Security Threat, Social Engineering Attack, Smartphone, Secure Keypad

*정회원, 조선대학교 자유전공학부 부교수 (제1저자)
접수일: 2024년 3월 4일, 수정완료일: 2024년 4월 10일
게재확정일: 2024년 4월 20일

Received: March 4, 2024 / Revised: April 10, 2024
Accepted: April 20, 2024
*Corresponding Author: jdmcc@chosun.ac.kr
Div. of General Studies, Chosun Univ, Korea

Ⅰ. 서 론

소형화된 폼팩터에 계산기, 주소록, 세계 시각, 메모장, 이메일, 전자우편, 팩스 송수신, 게임 등과 같이 간단한 기능을 내장한 최초의 스마트폰 출시[1,2]는 디지털 전환의 촉매가 되었으며[3] 사용자 편의성을 극대화하여 개발된 스마트폰은 점점 다양한 애플리케이션[4]을 포함하고 폼팩터 변형을 시도하고 있다. 이러한 시도는 스마트폰 폼팩터의 상당 부분을 구성하는 디스플레이 구조와 관련이 있으며, 유연한 디스플레이 구조는 곧 유연한 스마트폰 폼팩터를 가능하게 한다[5,6].

스마트폰의 출시와 함께, 스마트폰이 취급하는 개인정보에 대한 보호 및 다양한 정보의 보호를 위한 사용자 인증기법들이 제안 및 사용되었다. 이들 중 PIN 및 패턴 인증[7,8] 기법은 사용자가 무엇을 알고 있는지에 대한 비교를 통해 인증을 진행하는 지식기반 사용자 인증기법으로 다양한 스마트폰 폼팩터에서 기본적으로 사용되는 간단하고 직관적이며 사용하기 편리한 사용자 인증기법이다.

최근의 스마트폰 폼팩터는 폴더블, 벤더블, 롤러블을 거쳐 스트레처블 디스플레이를 적용한 유연한 형태의 폼-프리 스마트폰 개발을 진행 중이다. 그러나 shoulder surfing[9], Recording[10], Smudge[11], thermal[12], Touchlogger[13] 와 같이 다양한 공격 기법을 고려하면 이와 같은 폼팩터는 디스플레이 구조에 의존적인 사용자 인증기법의 안전성에 영향을 미칠 수 있다. 이에 본 연구는 앞으로 예상되는 스트레처블 디스플레이 규격과 응용에 적용이 가능한 보안 키패드 구조를 제안하였다.

본 연구는 다음과 같이 구성된다. 2장에서 우리는 디스플레이 특성별 폼팩터와 이에 대응하는 기존의 PIN 및 패턴 인증기법의 특징 및 문제점을 몇 가지 주요 보안 위협을 가정하여 취약점을 분석한다. 3장에서는 스트레처블 디스플레이 특성에 따라 발생이 가능한 보안 취약점을 앞 장의 보안 위협을 통해 분석한다. 4장에서는 스트레처블 디스플레이가 적용될 모바일 응용제품 규격을 고려한 보안 키패드 인증기법을 제안하며 5장에서 결론을 맺는다.

Ⅱ. 관련연구

디스플레이 형태는 해당 디스플레이가 적용된 스마트폰의 외관을 결정하는 요인이 되기 때문에 스마트폰의 폼팩터는 디스플레이 특성에 영향을 받는다고 할 수 있다. 디스플레이는 그 물리적 특성에 따라 고정형 디스플레이와 변형 디스플레이로 구분할 수 있다.

1. 디스플레이 특성별 폼팩터 분류[14]

1) 고정형 디스플레이

일반적인 평면 디스플레이가 적용된 방식으로, 브릭, 바, 슬레이트 타입의 기기 변형이 없는 스마트폰 폼팩터이다.

2) 변형 디스플레이

구부리거나, 접히거나, 말거나, 신축성을 지닌 유연한 디스플레이가 적용된 방식으로, 최근 상용화된 벤더블, 폴더블, 롤러블 스마트폰 폼팩터와 3축 방향으로 연신 가능한 소재로 이루어진 스트레처블 디스플레이가 적용된 폼팩터이다.

이처럼 크게 두 가지로 분류된 디스플레이 특성에 따른 다양한 스마트폰 폼팩터에서 기기에 특화된 사용자 인증기법을 제외한 범용 인증기법들이 있다. 이들은 인증을 위한 별도의 장비가 필요하지 않으며 디스플레이와 터치 인식 기능만으로 동작하는 단순한 구조의 지식기반 사용자 인증기법으로 PIN과 Pattern 인증이 있다.

2. 인증기법

1) PIN

PIN은 패스워드 인증과 같이 사용자가 기억하는 여러 자릿값을 갖는 문자 집합 또는 숫자 집합을 사용자 인증을 위한 패스 코드로 사용하는 방식으로 기억 및 입력이 편리하며 집합의 길이가 길어질수록 보안성이 높다.

2) Pattern

Pattern은 3x3 격자 위의 9개의 점을 끊임없이 연결하는 선분의 조합을 사용자 인증을 위한 하나의 패턴으로 사용하는 방식으로 PIN과 같이 패턴의 길이가 길어질수록 보안성이 높으며 각 숫자에 매번 키를 입력하는 PIN에 비해 한붓그리기 형식의 입력으로 간편하다.

스마트폰 사용자 환경에서 공격자는 사용자의 비밀

정보를 획득하기 위해 다음과 같은 시도를 할 수 있다. 이는 인적오류에 대한 사회공학 공격과 스마트폰의 센서 정보를 이용한 비밀정보 추정 공격이며 다음과 같이 분류할 수 있다.

3. 보안 위협

1) Shoulder surfing

Shoulder surfing attack은 사용자가 패스워드를 입력하는 과정에서 공격자가 물리적으로 사용자 장치의 화면이나 비밀번호 입력 키패드를 보며 개인정보를 획득하는 사회공학 공격이다.

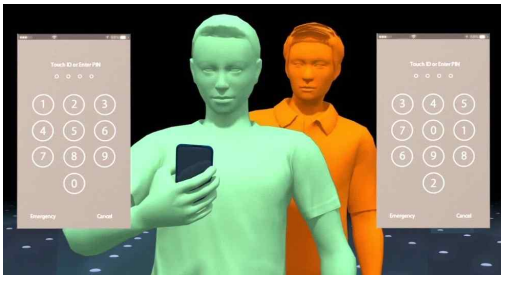

그림 1. 엿보기 공격 예시[15]
Figure 1. Example of shoulder surfing attack.

고정형 디스플레이 환경인 브릭, 바, 슬레이트 타입의 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 크기에 따라 인증UI 영역도 조절된다. 따라서 기기 화면의 크기가 클수록 shoulder surfing attack에 대해 취약하다.

변형 디스플레이 환경인 벤더블, 폴더블, 롤러블 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 크기에 따라 인증 UI 영역도 조절된다. 그러나 벤더블, 폴더블, 롤러블 디스플레이는 크기의 변형이 있는 특성으로 인해 동일 기기라 할지라도 shoulder surfing attack에 대한 취약성은 화면 크기에 따라 바뀐다.

2) Recording

Recording attack은 shoulder surfing과 같이 사용자가 비밀번호, PIN 번호, 개인 식별 정보 등을 입력하는 과정에서 공격자가 스마트폰의 화면을 물리적으로 또는 원격으로 녹화하거나 사진을 찍어 사용자의 개인정보를 획득하는 사회공학 공격이다.

고정형 디스플레이 환경인 브릭, 바, 슬레이트 타입의 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 크기에 따라 인증UI 영역도 조절된다. 따라서 기기 화면의 크기가 클수록 광학 장비를 이용한 기록, 재생, 확대가 가능한 Recording attack에 매우 취약하다.

변형 디스플레이 환경인 벤더블, 폴더블, 롤러블 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 크기에 따라 인증 UI 영역의 크기도 조정된다. 벤더블, 폴더블, 롤러블 디스플레이는 크기의 변형이 있는 특성이 있으나 광학 장비를 이용한 기록, 재생, 확대가 가능한 Recording attack에 매우 취약하다.

3) Smudge

Smudge Attack은 스마트폰 터치스크린을 통해 사용자가 비밀번호를 입력할 때 사용자의 손가락이 남긴 유분 즉, 생성된 지문 흔적으로부터 비밀정보를 추론하는 정보 추출 공격이다.

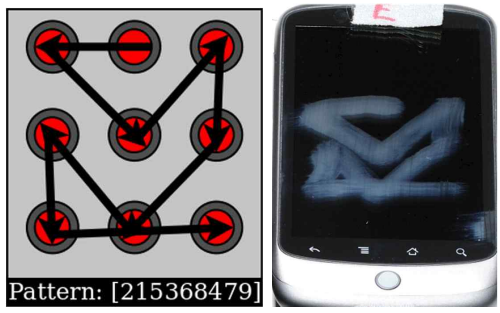

그림 2. 스머지 공격 예시[11]
Figure 2. Exmaple of smudge attack.

고정형 디스플레이 환경인 브릭, 바, 슬레이트 타입의 스마트폰 폼 팩터에서 PIN과 Pattern 인증은 모두 화면의 터치스크린을 이용한 입력을 하므로 화면의 유분 흔적을 이용해 비밀정보를 추론하는 Smudge attack에 취약하다.

변형 디스플레이 환경인 벤더블, 폴더블, 롤러블 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 터치스크린을 이용한 입력을 한다. 여기에 벤더블, 폴더블, 롤러블 디스플레이의 재질은 기존의 고정형 디스플레이 재질보다 유분 흔적이 더 잘 남게 되는 재질을 주로 사용하므로 화면의 유분 흔적을 이용해 비밀정보를 추론하는 Smudge attack에 고정형 디스플레이 대비 더욱 취약하다.

4) Thermal

Thermal Attack은 스마트폰 터치스크린을 통해 사용자가 비밀번호를 입력할 때 사용자의 손가락이 남긴 열 흔적을 이용하는 공격이다. 열 흔적은 열 감지 카메라를 이용하여 추출할 수 있으므로 이를 통해 키 입력

또는 시간에 따른 열 흔적의 구분을 세분화하면 키 입력 순서까지도 재구성하여 비밀정보를 추론하는 공격이 가능하다.

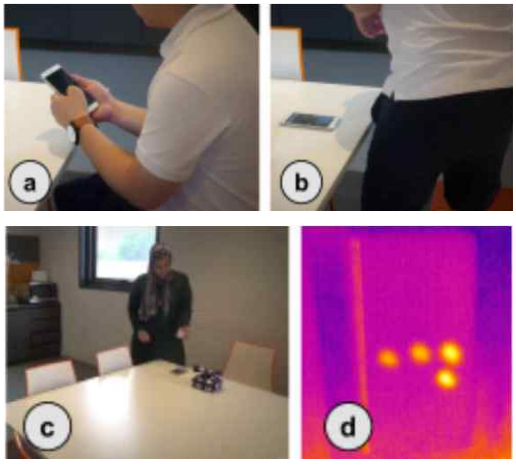

그림 3. 열감지 공격 예시[16]
Figure 3. Example of thermal attack.

고정형 디스플레이 환경인 브릭, 바, 슬레이트 타입의 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 터치스크린을 이용한 입력을 하므로 일정 시간 화면에 남게 되는 열 흔적을 이용해 비밀정보를 추론하는 Thermal attack에 취약하다.

변형 디스플레이 환경인 벤더블, 폴더블, 롤러블 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 터치스크린을 이용한 입력을 하므로 일정 시간 화면에 남게 되는 열 흔적을 이용해 비밀정보를 추론하는 Thermal attack에 취약하다.

5) Touchlogger

Touchlogger는 일반적인 물리 키보드에서 발생하는 소리나 전자기 방출을 이용한 키로깅 기법과는 다르게 물리 키보드가 없는 스마트폰에서 사용자가 가상키보드와 같은 입력 수단을 이용할 때 스마트폰에 내장된 모션 센서 값의 변화량을 감지하여 이를 통해 입력된 킷값을 추론하는 공격이다.

고정형 디스플레이 환경인 브릭, 바, 슬레이트 타입의 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 터치스크린을 이용한 입력을 하며 이때 발생하는 모션 센서 값의 변화량 감지를 통해 비밀정보를 추론하는 Thouchlogger에 취약하다.

변형 디스플레이 환경인 벤더블, 폴더블, 롤러블 스마트폰 폼팩터에서 PIN과 Pattern 인증은 모두 화면의 크기에 터치스크린을 이용한 입력을 하며 이때 발생하는 모션 센서 값의 변화량 감지를 통해 비밀정보를 추론하는 Touchlogger에 취약하다. 그러나 벤더블, 폴더블, 롤러블 스마트폰 폼팩터에서 스크린의 형태가 변형된 상태일 경우 모션 센서를 통해 얻게 되는 값에 오차가 있어 이 경우에는 공격 성공률이 낮다.

III. 취약점 분석

고정형 디스플레이 환경과 변형 디스플레이 환경에서 보편적으로 사용되는 인증기법인 PIN과 Pattern 인증은 모두 Shoulder surfing, Recording, Smudge, Thermal, Touchlogger에 취약하며 Touchlogger의 경우 변형 디스플레이 환경은 구조 변경에 따라 안전할 수 있다. 우리는 앞의 분석 결과를 바탕으로 차세대 디스플레이 환경인 스트레처블 디스플레이 구조를 응용제품 규격[17]이 예상되는 스마트 월렛, 멀티태스킹, 스크린 확장 및 미디어 시청, 게임 및 엔터테인먼트용 폼팩터 구조를 기준으로 각각에 대해 보안 취약점을 분석하였다.

1. 스트레처블 디스플레이 특성 및 응용 규격

스트레처블 디스플레이는 xyz 축에 대해 xy 양축에 대한 신축성과 z축 상하 방향으로 오목하게 말려 들어가거나 올라오는 특성, 그리고 서로 다른 축 방향과 위치로 신축하는 특성으로 분류된다. 이와 같은 특성을 바탕으로 다음과 같은 응용이 제안되었다.

1) 스마트 월렛

13.1인치의 320x137mm에서 3회의 폴딩으로 106x137mm까지 콤팩트한 크기이며 z축 상하 방향으로 변화한다.

2) 멀티 태스킹

2회 이상의 폴딩, 특정 각으로 디스플레이를 거치한 형태이며 z축 상하 방향으로 변화한다.

3) 스크린 확장 및 미디어 시청

디스플레이 전면을 늘리고 커브드로 세팅한 형태이며 xy 양축에 대한 신축성을 갖는다.

4) 게임 및 엔터테인먼트

여러 각도로 당기고 비틀어 게임 및 엔터테인먼트를 즐기는 형태이며 서로 다른 축 방향과 위치로 신축성을 갖는다.

스트레처블 디스플레이 특성과 응용 각각에 대해 예상되는 보안 위협은 다음과 같다.

2. 보안 위협

1) Shoulder surfing

스트레처블 디스플레이는 변형 디스플레이 환경에 해당한다. 따라서 PIN과 Pattern 인증 모두 화면의 크기에 따라 인증UI 영역도 조절되는 환경이 될 것이며, 스트레처블 디스플레이의 제안된 4가지 응용 규격을 고려하면, 스마트 월렛, 멀티 태스킹, 스크린 확장 및 미디어 시청, 게임 및 엔터테인먼트 응용 규격 모두 취약하다.

2) Recording

Recording attack은 광학 장비가 적용된 강화된 shoulder surfing에 해당하므로 스트레처블 디스플레이의 제안된 4가지 응용 규격 모두 매우 취약하다.

3) Smudge

스트레처블 디스플레이는 변형 디스플레이 환경에 해당한다. 따라서 벤더블, 폴더블, 롤러블 디스플레이의 재질과 유사한 재질이 사용될 것이며 이는 기존의 고정형 디스플레이 재질보다 유분 흔적이 더 잘 남게 될 것이므로 스트레처블 디스플레이의 제안된 4가지 응용 규격 모두 매우 취약하다.

4) Thermal

사용자가 손가락으로 터치스크린을 사용한다는 가정하에 모든 디스플레이 규격은 열 감지 공격에 취약하다. 따라서 스트레처블 디스플레이의 제안된 4가지 응용 규격 모두 매우 취약하다.

5) Touchlogger

모션 센서 값의 변화량 감지는 변형 디스플레이 환경일 경우 모션 센서를 통해 얻게 되는 값에 오차가 있다. 따라서 스트레처블 디스플레이의 제안된 4가지 응용 규격 모두 모든 형태 변형에 대한 정보가 없는 경우 공격 성공률이 낮다.

Ⅳ. 제안

보안 취약점을 고려할 때, 스트레처블 디스플레이의 특성을 고려한 보안 키패드 인증기법은 다음의 요소를 포함해야 한다.

1. 화면에 표시되는 정보의 안전성 확보

앞의 보안 취약점 분석에 의하면 PIN과 Pattern 인증기법 모두 화면상에 표시된 정보를 통한 사용자의 정보 입출력이 이루어지는 구조이다. 따라서 동일한 구조를 사용하는 보안 키패드 인증기법은 스트레처블 디스플레이를 위한 응용으로 제안되었던 4가지 응용 규격 모두에 대해 화면에 표시되는 정보의 직접적인 표시를 지양해야 보안 위협에 대한 효과적인 대응이 가능하며, 화면 크기에 따라 자동 조절되는 UI의 비율을 제한하는 방향으로 설계해야 한다. 그러나 단순 제한만으로는 스트레처블 디스플레이의 유연한 변화에 대응할 수 없으므로 보안 키패드 UI의 크기, 위치, 형태가 사용자의 입력 편의 및 보안성 향상을 위해 사용자에 의해 비밀번호 셋업 단계 또는 보안 키패드 인터페이스를 사용할 때 동적 조절이 가능하도록 설계한다.

2. 터치스크린으로 입력하는 정보의 안전성 확보

PIN과 Pattern 인증기법 모두 정보 입력에 터치스크린을 사용한다. 따라서 동일한 구조를 사용하는 보안 키패드 인증기법은 터치스크린을 통한 입력으로 비밀정보 입력을 추정할 수 없도록 정보 입력에 터치스크린 이외의 방법을 사용하거나 터치스크린의 사용을 정보의 직접입력이 아닌 간접입력을 위한 수단으로 사용해야 한다.

이를 정리하면 곧 화면에 표시되는 입출력 UI의 동적 변경이 가능하게 하며 표시되는 정보의 제한이 가능하도록 하는 설계 반영, 그리고 사용자 맞춤형 인터페이스 적용으로 정보 입력이 관찰되지 않도록 하는 설계 반영이다. 이렇게 함으로써 스트레처블 디스플레이의 연신 특성을 고려한 PIN 및 Pattern 인증이 가능하며 자유로운 UI 구성이 가능하므로 입력 위치나 화면 출력 위치가 정형화된 기존 기법에 비해 자유로운 화면 배치 및 구성, 그리고 다양한 입력이 가능하므로 사용자 편의성 향상 면에서도 장점이 될 수 있다.

Ⅴ. 결론

디스플레이 특성에 따른 보안 취약점 분석 결과에 의하면 스트레처블 디스플레이가 적용된 4가지의 응용

에서 보안성과 사용자 편의성을 충족시킬 수 있는 보안 키패드는 비밀정보의 입출력 안전성 및 편의성 확보를 위해 기존 입출력 UI를 완전히 새로운 방향에서 접근해야 함을 보였다. 4장에서 언급한 우리의 제안은 차세대 모바일 기기의 보안을 강화하는 새로운 방향을 제시한다. 향후 연구에서 우리는 스트레처블 디스플레이를 활용한 보안 키패드의 사용성과 효율성이 더욱 향상된 사용자 인증기법을 제안하고자 한다.

References

[1] https://blog.uplus.co.kr/2149

[2] https://cjh38.tistory.com/entry/%EC%B5%9C%EC%B4%88%EC%9D%98-%EC%8A%A4%EB%A7%88%ED%8A%B8%ED%8F%B0-%EC%8A%A4%EB%A7%88%ED%8A%B8%ED%8F%B0%EC%9D%98-%EC%97%AD%EC%82%AC-%EB%B3%80%EC%B2%9C%EC%82%AC

[3] Seung Hyeog Moon, "A Study on ICT Conversion and Change of Industrial Society", *The Journal of the Convergence on Culture Technology (JCCT)*, Vol 7, No. 4, pp. 653-658, November, 2021. https://doi.org/10.17703/JCCT.2021.7.4.653

[4] Tae-Seung Ko, Byeong-Joo Kim, Jeong-Woo Jwa,"Development of wearable devices and mobile apps for fall detection and health management" *International Journal of Advanced Culture Technology,* Vol. 11, No. 1, pp. 370-375, 2023. https://doi.org/10.17703/IJACT.2023.11.1.370

[5] https://infogalactic.com/info/Form_factor_(mobile_phones)

[6] https://spectrum.ieee.org/consumerelectronics/portable-devices/from-foldablephones-to-stretchy-screens

[7] https://www.infopulse.com/blog/how-to-enable-secure-authentication-in-mobile-applications/

[8] C. Wang, Y. Wang, Y. Chen, H. Liu & J. Liu., "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, Vol. 120, No. 7, pp. 107118, DOI : 10.1016/j.comnet.2020.107118

[9] E. Miluzzo, A. Varshavsky, S. Balakrishnan & R.R. Choudhury, "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

[10] T. Takada, "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

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

[12] Y. Abdelrahman, M. Khamis, S. Schneegass & F. Alt, "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

[13] Cai,L.and Chen H., "TouchLogger:inferring keystrokes on touch screen from smartphone motion," *Proceedings ofthe 6th USENIX WorkshoponHotTopicsinSecurity,* pp. 9-9, 2011.

[14] Dongmin Choi, " A Study on the Correlation between Atypical Form Factor-based Smartphones and Display-dependent Authentication Methods," *Journal of Korea Multimedia Society,* Vol. 24, No. 8, pp. 1076-1089 August 2021. https://doi.org/10.9717/kmms.2021.24.8.1076

[15] https://pc-solucion.es/terminos/shoulder-surfing/

[16] Paul Bekaert, Norah Alotaibi, Florian Mathis, Nina Gerber, Aidan Christopher Rafferty, Mohamed Khamis, and Karola Marky."Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives," *In Nordic Human-Computer Interaction Conference (NordiCHI '22),* October 8 - 12, 2022, Aarhus, Denmark. ACM, New York, NY, USA pp. 1-9. https://doi.org/10.1145/3546155.3546706

[17] Do Kyung Kim, Chang Kuk You, "Analysis of Mobile Product Design Applying Stretchable Display(SD) -focused on the expansionary application design structure for 2030 new-media-generation in mobile environment-," vol. 24, no. 2, pp. 33-45, April 2023. DOI : 10.47294/KSBDA.24.2.3

※ This study was supported by research fund from Chosun University, 2022.