촉각을 이용한 보안키패드의 설계

서화정, 이연철, 김현진, 박태환,
나엔하반, 석선희, 김경훈, 김호원*

< 요 약 >

현재 스마트폰 상에서의 온라인 뱅킹 서비스는 안전한 접근제어를 위해 사용자에게 계좌에 대한 비밀번호를 요청하게 된다. 해당 비밀번호는 사용자를 인증함과 동시에 다른 사용자에 의한 무분별한 금융 서비스 접근을 통제하는 역할을 한다. 하지만 스마트폰 상에서의 비밀번호 입력 방식은 공격자가 어깨너머로 스마트폰의 입력창을 훔쳐볼 경우 비밀번호가 노출될 가능성이 있다. 그 이유는 가상 키보드는 물리적 키보드에 비해 오타율이 높아 피드백의 일한으로 마지막 글자가 입력창에 출력되기 때문이다. 해당 문제점을 해결하기 위해 2013년도 금융보안공모전 우수상 논문에서는 각각의 입력키에 대한 피드백을 주는 대신 무작위로 색정보가 입혀진 키패드의 색상정보를 입력창에 띄워 줌으로써 피드백과 글자에 대한 마스크 역할을 동시에 할 수 있는 기법이 제안되었다. 하지만 색상 정보 또한 공격자에게는 비밀번호를 알아내기 위한 하나의 힌트로 작용할 수 있다. 예를 들어 첫 번째 문자와 두 번째 문자의 색상이 다른 경우 두 글자는 상이한 글자이다. 만약 두 글자의 색상이 동일한 경우 매우 높은 확률로 해당 글자는 동일한 글자일 가능성이 있다. 또한 여러 번의 입력창 정보를 수집할 경우 비밀번호를 온전히 추론하는 것이 가능하다. 따라서 안전한 금융보안을 위해서는 공격자에게 어떠한 힌트도 제공하지 않는 보안 키패드에 대한 연구가 필요하다. 본 논문에서는 기존의 피드백에서 사용하던 시각적인 정보 대신 촉각적인 정보로 사용자에게 피드백을 주는 방식을 제안한다. 해당 방식은 가상 키패드의 오타가 발생하지 않도록 레이아웃을 설계함과 동시에 문자에 대한 피드백을 스마트폰의 진동으로 대체함으로써 시각으로 노출되는 정보의 양을 줄였다. 따라서 공격자는 어깨너머 공격을 통해 비밀번호를 유추하는 것이 어려워지며 사용자는 진동 피드백 정보를 통해 오탈자를 정확하게 구별하는 것이 가능해 진다. 해당 제안 기법은 실제로 안드로이드 폰 상에 구현 및 실험되었다. 보안성 분석결과 기존의 기법에 비해 전수조사 공격 및 유추에 의한 번호 크래킹에 강인한 특성을 가진다. 타자 성능인 정확도와 신속성은 기존의 보안 키보드와 유사하게 도출되었다. 이는 기존의 스마트폰 상에서의 보안 키보드를 안전하게 대체할 수 있는 기술로써 그 효용성이 매우 높다고 할 수 있다.

Ⅰ. 서론

급속한 ICT 기술 발전은 전 국민이 언제 어디서나 온라인 금융서비스에 접속하여 인터넷 뱅킹을 사용하는 것이 가능하게 하였다. 모바일 뱅킹 서비스는 스마트폰 내부의 공인 인증서와, 보안 카드의 보안 정보 그리고 사용자의 비밀번호를 통해 사용자 인증 절차를 거친 후 편리하고 안전하게 은행 업무를 처리하는 것이 가능하게 하였다. 현재 인터넷 뱅킹서비스 이용률은 지속적으로 증가하여 2013년 1/4분기 기준 모바일뱅킹 서비스의 하루 평균 이용률은 5,285 만 건으로써 전 분기 대비 10.8%의 성장률을 보여주고 있다. 또한 사용 연령대는 20~30대 비중이 75.2%에서 64.7%로 낮아짐에 따라 점차 전 연령대가 자유롭게 모바일 뱅킹을 사용하고 있음을 확인할 수 있다 [1].

현재 모바일 뱅킹 어플리케이션에서 사용되는 보안 솔루션은 크게 보안카드, 공인인증서 그리고 키보드 보안 솔루션으로 나누어 볼 수 있다. 보안카드는 은행에서 발급해주는 카드로써 불규칙적인 난수 규칙을 통해 비밀정보가 생성되기 때문에 공격자가 해당 정보를 유추하는 것이 불가능하다. 공인인증서는 사용자가 신분을 법적으로 증명하기 위해 공인된 기관으로부터 발급받은 인증서로써 온라인상에서 사용자의 신분을 증명한다. 키보드 보안 솔루션은 키보드 상에서 발생하는 취약점을 보완하며 크게 두 가지 기술이 사용되고 있다. 먼저 숫자 키패드의 경우에는 숫자 배열을 무작위로 배치하여 공격자가 누르는 위치를 유추하는 키 로깅 공격이 어렵게 하는 방식이 사용되고 있다. 쿼티 키패드에서는 각 버튼의 배열 간격을 달리하여 내부적으로는 키 로깅 공격에 대비하고, 외부적으로는 어깨 너머 공격에 대비할 수 있도록 비밀번호를 별표로 표시하고 있다. 또 다른 키보드보안은 스마트폰 내부의 정보를 공격자가 확인할 수 없도록 일련의 암호화 보안 기술을 적용하여 난독화하는 기법을 사용한다.

하지만 현재 널리 사용되고 있는 키패드의 입력은 화면상에 입력된 비밀번호의 마지막 글자를 보여주는 방법을 통해 입력 값에 대한 피드백을 줌으로써 어깨너머 공격에 취약하다. 기존 기법에서 피드백을 주는 이유는 터치 키패드의 입력 오타율이 기존의 물리적 키패드에 비해 높아 사용자에게 입력한 글자에 대한 적절한 피드백이 없다면 비밀번호 입력 시 사용자가 많은 오타를 입력하기 때문이다. 하지만 스마트폰 모바일 뱅킹은 언

1) 한국은행, “2013년 1/4분기 국내 인터넷뱅킹서비스 이용현황”, 2013.05.15.

제 어디서나 사용 가능하기 때문에 공공장소에서 주위의 사람이 우연히 사용자의 스마트폰을 어깨너머로 살펴보게 된다면 비밀번호가 유출 될 수 있고, 유출된 정보는 실제적인 금전적 피해로 이어질 수 있으므로 강인한 보안 기법이 필요하다. 특히 블랙햇 USA 2014에서는 최신 구글 글래스를 이용하여 3m 거리에서 목표물이 터치스크린에 암호를 입력하는 모습을 촬영한 다음 이를 분석하여 90%의 정확도로 암호를 훔치는 어깨너머 공격을 선보일 예정이다. 이는 구글 글래스를 사용하여 사용자의 행동 및 스크린을 분석하여 입력한 문자를 확인하는 방법이다 [2)3)]. 다양한 어깨너머 공격을 방지하기 위한 기법 중 2013년도 금융보안공모전 우수논문에서는 개선된 피드백 메커니즘을 설계 및 구현함으로써 기존의 어깨너머 공격을 방지하였다 [4)]. 해당 제안 기법은 피드백을 위해 마지막 글자를 보여주는 방법을 선택하는 대신 해당 키패드에 정의된 색상을 피드백으로 줌으로써 실제 입력 값에 색상으로 마스킹이 된 결과 값만을 공격자가 확인할 수 있도록 하였다. 하지만 해당 색상 정보를 통해 공격자는 실제 비밀번호를 전수 조사 및 유추를 통해 높은 확률로 비밀번호 도출 가능하다 따라서 해당 기법의 문제점을 해결할 수 있는 보안 키패드의 제안이 필요하다.

본 논문에서는 기존의 보안 키패드의 보안 취약점을 개선하는 촉각기반 보안 키패드를 제안한다. 해당 키패드는 기존의 시각적인 피드백 기법과는 달리 공격자에게 단 하나의 시각적 힌트도 제공하지 않는다. 기존의 보안 키패드들은 시각적인 피드백에 중점을 두었다면 본 논문에서는 촉각이라는 새로운 피드백 수단을 개척 및 개발하여 사용자에게 오탈자에 대한 적절한 피드백을 준다. 이는 시각적으로 확인이 불가능한 정보를 사용함으로 어깨너머 공격을 수행하는 공격자는 입력창을 통해서는 사용자의 비밀정보를 얻는 것이 불가능 혹은 매우 제한적이다.

본 논문의 구성은 다음과 같다. 2장에서는 보안 키패드에 대한 관련 연구에 대해 살펴본다. 3장에서는 제안하는 키패드에 대해 제시하며 4장에서는 이에 대한 성능 평가를 한다. 마지막으로 5장에서는 본 논문의 결론을 내린다.

---

2) 월간 정보보호21c 통권 제107호, 개인인증정보 보호를 위한 새로운 솔루션, http://www.boannews.com/know_how/view.asp?page=2&gpage=1&idx=2671&numm=2300&search=title&find=&kind=05&order=ref

3) “블랙햇 USA 2014에서 공개될 10가지 충격적인 공격 사례”, http://www.itworld.co.kr/slideshow/88304

4) 김현진, 서화정, 이연철, 박태환, 김호원, “어깨 넘어 훔쳐보기에 저항성을 가진 가상금융키패드의 구현,” 정보보호학회지, 제23권, 제6호, pp. 21-29, 2013. 12.

Ⅱ. 관련 연구

금융 보안 연구원에서 출판한 스마트폰 보안 가이드에 따르면 스마트폰의 보안을 위해서는 중요 입력 정보와 지점에 대한 보호기술이 제공되어야 한다 [5]. 이는 네트워크의 전송구간 상 메시지 탈취와 메모리 분석 그리고 키 로깅을 통한 물리적인 정보 획득 공격에 대해서 사용자의 온라인 뱅킹이 안전해야 함을 의미한다.

현재 대부분의 금융 어플리케이션에서는 안전한 인터넷 뱅킹을 위해 보안 키패드를 제공하고 있으며 이를 통해 안전한 서비스의 제공이 가능하도록 하고 있다. 본 장에서는 실제 온라인상에서 제공되는 금융 어플리케이션의 구현 현황에 대해 살펴보도록 한다.

1. 보안 요구 사항

가. 입력정보 보호 및 전달 구간 내 저장 및 노출 금지

입력정보 보호 및 전달 구간 내 정보의 노출 금지는 가상키보드를 통해 입력된 정보를 암호화하여 저장 및 전달함으로써 이용자의 중요 입력 정보가 공격자의 메모리 혹은 네트워크 패킷 분석을 통해 쉽게 유출되지 않도록 한다. 따라서 서버와 클라이언트 사이에서 암호화된 송수신 정보는 공격자에게 노출되더라도 서버와 클라이언트 간에 공유된 비밀 키가 유출되지 않는다면 공격으로부터 안전하다.

나. 입력지점에 대한 입력정보 보호

입력지점에 대한 입력정보 보호를 위해서는 정보 입력 시 키패드에 발생하는 물리적인 특징으로 키를 유추하는 키 로깅을 방지해야 한다. 키 로깅 공격기법이란 사용자의 PC 혹은 스마트폰 상에서 사용자가 모르는 사이 키보드의 키 입력을 추적하거나 기록하는 기법으로서, 소프트웨어 기반 방식과 하드웨어 기반 방식 그리고 원격 RF와 음향 분석기법등이 있다 [6][7].

첫 번째로, 소프트웨어 기반 코너 로거 방식은 키 로깅 공격기법 중 가장 기본적인 방식으로서, 스마트폰의 모션 센서를 기반으로 키보드의 중간과 좌우상하의 코너에 대한 입력을 인식하는 방법이다. 따라서 모션 센서

5) 금융보안연구원, “금융부문 스마트폰 보안 가이드”, 2010.12
6) Gold, Steve. “Electronic countersurveillance strategies.“ Network Security 2013.2 (2013): 15-18.
7) Darer, Alexander. “Mini Project 2: A key-logger which infers keystrokes on a touch-screen keyboard from smartphone motion.“ (2013).

를 통해 받은 데이터를 기반으로 필터를 생성하여 기계학습과 분류 알고리즘을 이용하여 비밀정보를 확인할 수 있다 [8]. 두 번째로는 코너 로거 방식을 확장한 키패드 로거 방식으로, 기존의 코너 로거 방식에 비해 0부터 9까지의 숫자 입력에 대한 키 로깅 공격기법이다. 코너 로거방식에 비해 좀 더 복잡한 모션 필터와 학습 알고리즘을 기반으로 취약성을 분석할 수 있다. 여기서 사용된 학습 알고리즘에는 베이시안 네트워크, 다층 퍼셉트론, J48 Tree, Random Forest알고리즘이 사용되었으며, 이 중에서 다층 퍼셉트론 알고리즘이 다른 학습 알고리즘에 비해 약 78%의 정확성을 가지고 있다. 그리고 안드로이드 상에서 스마트폰의 3축 센서 정보를 획득하여 공격하는 기법도 보고되고 있다 [9]. 이러한 공격기법은 키보드에 키 입력 시, 발생하는 스마트폰의 진동을 모션 센서를 통해 획득하여 공격하는 기법으로서, 모션 기반 키 입력 추론 공격기법이라고 한다 [10].

별도의 하드웨어 없이 그래픽 인터페이스를 이용하여 안전하고 편리하게 패스워드를 생성 및 관리하는 기법도 본격적으로 연구되고 있다. 본 방식은 패스워드를 직접 입력하는 방식이 아닌 그림이나 아이콘 등의 그래픽 인터페이스의 경로를 사용하여 패스워드가 입력하는 방식이다. 이러한 방식을 통해 매번 다른 그림 경로를 이용한 경로 인증 방식과 의미 없는 정보과의 조합을 이용하여 어깨 너머 공격과 피싱 등의 해킹공격 기법에 강인하다는 장점이 있다. ㈜민인포에서는 개인정보 유출방지를 위한 차세대 그래픽 인증 솔루션으로, DEMENTOR를 개발하였으며, 본 솔루션 중, DEMENTOR-SGP의 경우, 그래픽 일회용 패스워드 인증 방식을 기반으로 하여 이미지간의 상대경로를 통해 인증하는 방식을 이용한다. <그림 1, 2>에서 UI상의 방향키를 이용하여 각 아이콘의 경로를 설정한 후, 인증 시, 사용자는 사용자의 경로를 생각하여 아이콘을 이동하여 카운터를 이용하여 이동횟수를 알아보도록 하여 인증 하는 기법을 이용한다. 또한 이러한 그래픽 일회용 패스워드 인증 방식을 통해, 기존의 텍스트 입력 기반의 한계를 극복할 수 있는 장점이 있다 [11]. 현재, DEMENTOR는 우리은행, STX 조선그룹, 어린이 재단, 프리챌 게임, 일본 히타치(일본 e-banking)등 내,

8) Cai, Liang, and Hao Chen. "TouchLogger: inferring keystrokes on touch screen from smartphone motion." Proceedings of the 6th USENIX conference on Hot topics in security. USENIX Association, 2011.

9) Cai, Liang, and Hao Chen. "On the practicality of motion based keystroke inference attack." Trust and Trustworthy Computing. Springer Berlin Heidelberg, 2012. 273-290.

10) Asonov, D., Agrawal, R.: Keyboard acoustic emanations. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 3-11 (May 2004)

11) 보안뉴스, 피싱・파밍 예방에 그래픽인증 방식 효과적, 2008.02.04., http://company.hauri.co.kr/news/security_news_view.html?intSeq=1159&no=

외부 인증 시스템 및 국내외 구축 및 진행을 하고 있으며, 현재 일본에서 인증에 대한 하드웨어 및 소프트웨어 보안군으로 나누어 활성화를 위한 준비 중이며, 소프트웨어 보안군으로서는 보안등급 최상급 받아 진행 중에 있다 12).

<그림 1>

DEMENTOR-SGP

실행화면

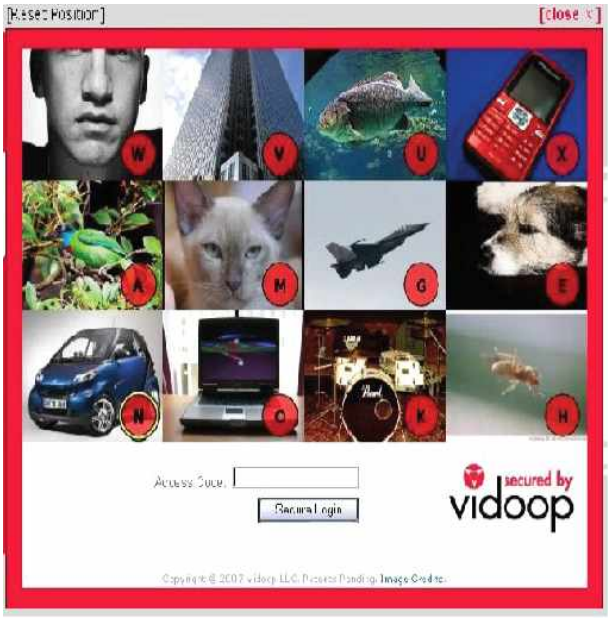
<그림 2> DEMENTOR-SGP의 장점 및 차이점

메모리장치 플랫폼 기업인 퍼닛에서 GOTP기반의 인증방식이 탑재된 USB 메모리 퍼닛(funit)을 출시하였다. 이는 설정한 아이콘을 마우스로 인

12) 월간 정보보호21c 통권 제107호, 개인인증정보 보호를 위한 새로운 솔루션, http://www.boannews.com/know_how/view.asp?page=2&gpage=1&idx=2671&numm=2300&search=title&find=&kind=05&order=ref

증하며 상대 경로시스템 및 가상좌표계를 이용한 OTK(One Time Key)를 생성하여 인증하는 방식이다. 각 아이콘의 경로 좌표 값으로 인증하기 때문에 어깨 너머 공격에 강인하다는 장점이 있다 [13]. 외국의 경우, <그림 3>과 같이 2007년 4월에 있었던 Web2.0 엑스포 세미나에서 Opend ID provider 기업인 VIDOOP사에서 해당 이미지의 알파벳 텍스트 화 기반의 GOTP를 선보였다 [14][15].

<그림 3> Vidoop에서의 GOTP 제공 모습



13) 전자신문, 퍼닛, 그래픽 인증 탑재한 보안 USB메모리 출시, 2010.08.15., http://www.etnews.com/news/computing/solution/2273363_1476.html

14) ㈜민인포, 통합보안관리 체계를 위한 차세대 인증시스템, 2007.09., http://www.ddaily.co.kr/DATA/whitepaper/%C6%AE%B7%A22-4%20%B9%CE%C0%CE%C6%F7%20Mind-Key_1_20070912323.pdf

15) Wikipedia, “Vidoop”, http://en.wikipedia.org/wiki/Vidoop

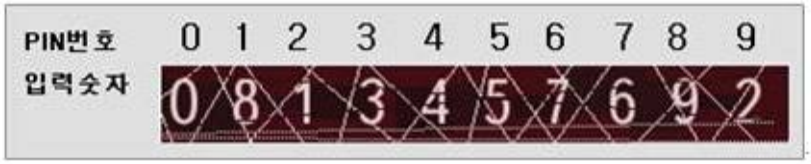
<그림 4> passfaces에서 GOTP를 제공하는 모습

<그림 4>와 같이 passfaces사에서는 135개의 얼굴 이미지를 포함한 이미지 라이브러리 기반으로 GOTP서비스를 제공하며, 매년 라이브러리에 포함된 이미지의 개수를 증가시키고 있다. 이러한 이미지를 기반으로 사용자가 초기에 설정한 이미지의 순서를 기반으로 이미지의 상대경로와 이미지 라이브러리상의 이미지(JPEG)파일 명을 기반으로 인증하는 기법을 제공하고 있다. pasafaces사는 기존의 알파벳 기반의 GOTP방식의 한계점을 극복하고자, 모든 인종의 얼굴사진을 이용함으로써 기존의 방식에 비해 보다 더 안전성을 높였고, 이와 관련된 특허를 가지고 있다 16)17).

16) ㈜민인포, 통합보안관리 체계를 위한 차세대 인증시스템, 2007.09., http://www.ddaily.co.kr/DATA/whitepaper/%C6%AE%B7%A22-4%20%B9%CE%C0%CE%C6%F7%20Mind-Key_1_20070912323.pdf

17) Passfaces Homepage about section, http://www.realuser.com/enterprise/about/about_passfaces.htm

<그림 5> 피망 GOTP의 동작원리



피망 GOTP서비스의 경우 사용자가 가입 시 휴대폰으로 발급받은 PIN번호를 이용하는 방식으로, 서비스 이용 시, 매번 새로운 숫자로 제공되는 PIN번호 이미지와 이미 발급받은 PIN번호를 매칭 하여 해당 숫자를 입력하는 방식. <그림 5>과 같이, PIN번호 입력 방법은 첫 번째, 휴대폰으로 전송된 PIN번호를 확인하고, 이미지 숫자에서 PIN번호에 해당하는 입력 숫자를 입력한다 [18].

하드웨어 기반 방식에는 PC용 키보드 케이블 커넥터 형식으로 키 로깅을 하는 방식이 있으며, PC용 키보드 상에서 키 입력 시, 각키 마다 발생하는 소리가 다르다는 점에 기반으로 한 키보드 음향 발산 기반 공격이 있다 [19]. 유선, 무선 키보드에 대한 전자기파 기반의 키 로깅 공격 기법도 제안되고 있다 [20]. 하지만 하드웨어 기반의 공격 방식은 소프트웨어 기반의 공격 방식에 비해 신호에 대한 잡음을 처리하기 어려워 공격하기 어렵다는 단점이 있다 [21].

현재 키패드에 표기되는 문자를 무작위로 배열함으로써 공격자가 해당 키패드의 정보를 유추하는 것이 불가능하게 하는 기술이 실용화되어 있다. 여기서 무작위 배열이란 <그림 6>와 같이 일반적인 숫자 키패드 배열에서 기존의 배치와는 달리 키패드를 생성하여 공격자가 시도하는 키 로깅을 통해서는 입력 위치를 파악하더라도 입력 정보를 유추하는 것이 어렵게 한다. 쿼티 키패드에서는 입력하는 키가 많은 특성상 무작위 배열 시에 사용자에게 혼란을 가중시킬 수 있기 때문에 키의 배열순서는 그대로 두고 키 사이의 간격을 <그림 7>와 같이 무작위로 늘리거나 줄임으로서 키 로

18) 피망 고객센터, 피망 GOTP서비스란 무엇인가요?, http://help.pmang.com/faq/searchFaq.do?pageIdx=&fsCategoryId=PF007006007&fsKeyword=&faqId=&orderType=ASC&orderCol=ranking

19) Vuagnoux, M., Pasini, S.: Compromising electromagnetic emanations of wired and wireless keyboards. In: Proceedings of the 18th Conference on USENIX Security

20) Kwon, Sunghyuk, Donghun Lee, and Min K. Chung. "Effect of key size and activiation area on the performance of a regional error correction method in a touch-screen QWERTY keyborad." International Journal of Industrial Ergonomics 39.5(2009):888-893

21) Roth, Volker, Kai Richter, and Rene Freidinger. "A PIN-entry method resilient against shoulder surfing." In Proceedings of the 11th ACM conference on Computer and communications security, pp. 236-245. ACM, 2004.

깅에 효율적으로 대처할 수 있도록 하였다.

<그림 6> **숫자 키패드** <그림 7> **쿼티 키패드**

다. 사회 공학적 기법

사회 공학적 기법이란 시스템이 아닌 사람의 심리상태나 습관에서 발생하는 취약점을 공략하여 원하는 정보를 얻어내는 공격기법이다 [22]. 이러한 사회 공학적 기법의 대표적인 예로서는 피싱, 파싱 그리고 어깨너머 공격이 있다 [23]. 그 중에서도 어깨너머 공격은 사용자의 주위에서 어깨너머로 육안이나, 카메라, 비디오카메라, 구글 글라스 등을 이용하여 사용자의 스크린을 훔쳐봄으로서 비밀정보를 얻어내는 공격 기법이다. 실제로 블랙햇 USA2014에서는 구글 글라스를 통해 90%의 확률로 비밀번호를 해킹하는 기술을 2014년 8월 라스베가스에서 발표할 예정이다 [24][25].

최근 발생한 ATM 상에서의 어깨너머 공격 역시 PIN(Personal Identification Number)을 통한 사용자 인증이 취약할 수 있음을 보여주었다 [26]. 현재 스마트폰 금융 어플리케이션은 기존의 ATM 보다 많은 단계의

22) 조한진. "개인정보 입력 감지를 이용한 사회공학적 공격 대응방안." 한국콘텐츠학회논문지 12, no. 5 (2012): 32-39.
23) 서동일. "사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석." 情報保護學會誌 16, no. 1 (2006): 40-48.
24) 월간 정보보호21c 통권 제107호, 개인인증정보 보호를 위한 새로운 솔루션, http://www.boannews.com/know_how/view.asp?page=2&gpage=1&idx=2671&numm=2300&search=title&find=&kind=05&order=ref
25) "블랙햇 USA 2014에서 공개될 10가지 충격적인 공격 사례", http://www.itworld.co.kr/slideshow/88304
26) 양형규. "스마트폰을 위한 보안 키패드의 안전성 분석." 정보보호학회지 21, no. 7 (2011): 30-37.

PIN정보를 입력함으로서 보안성을 강화되었지만 여전히 PIN 기반 인증을 해야 하는 한계를 가진다. 또한 어깨 너머 공격은 전문적인 지식 없이도 누구나 쉽게 할 수 있고, 만약 공격에 성공한다면 사용자의 비밀번호를 손쉽게 파악할 수 있다. 현재 스마트폰 금융 어플리케이션은 공공장소에서도 널리 사용되고 있으며 이는 사회 공학적 기법에 취약한 문제를 가진다. 현재 보안 키패드 상에서는 사용자의 비밀 정보 입력 시 마지막 정보를 사용자에게 피드백 정보로 알려주게 된다. 이는 사용자의 오타율을 낮출 수 있는 장점을 가지지만 공격자에게는 비밀정보를 쉽게 엿볼 수 있는 기회를 제공 할 수 있다. 최근에는 어깨 너머 공격에 대처하기 위해 입력 숫자를 다른 이미지로 대치하여 방어하는 기법이 제시 되었다. 하지만 사용자가 일일이 모든 이미지를 기억해야하는 불편함이 있어 실질적인 실용성은 매우 떨어진다. 이를 해결하기 위해 2013년도 금융보안공모전 우수논문에서는 색상을 통해 키를 마스킹하는 기법이 제안되었다. 하지만 해당 기법은 노출되는 색상정보를 통해 공격자가 비밀번호를 유추하는 것이 가능하게 되는 문제점을 가진다. 따라서 본 논문에서는 촉각을 통해 사용자에게는 적절한 피드백을 주지만 공격자의 어깨 너머 공격에는 보다 강인한 보안 키패드를 설계 및 구현하여 안전하고 편리한 온라인 뱅킹환경을 도모한다.

2. 어깨너머 공격에 대한 연구

어깨너머 공격에 대한 기존의 연구로는 애플리케이션에서 제공하는 가상 키보드의 랜덤성과 그 구조의 문제점을 해결한 키보드에 대한 제안이 있었으며, 공항 라운지, 벤치, 커피숍등과 같은 공공장소에서 어깨너머 공격을 통해 얻은 정보를 바탕으로 피해자가 어떤 사람이며, 어떠한 프로그램을 사용하는지 추론을 통한 개인 정보 획득과 카메라를 이용하여 현금인출기에서의 비밀번호 획득과 같은 사례 또한 발생하고 있다.

이러한 어깨너머 공격을 대응하기 위해 어깨너머 공격자 모델링에 대한 연구가 있었다 [27]. 이 연구에 있어서 어깨너머 공격자의 조건으로 인간의 인지력, 공격자가 피해자의 스크린과의 각도, 공간과 거리 그리고 시야각을 중심 조건으로 하여 연구하였으며, 인간의 인지력과 관련하여서는 얼마만큼의 시간이 주어졌을 때, 인지력이 높은지, 단기기억력과 시간경과에 따른 망각에 대해서 언급하고 있다. 스크린의 각도의 경우, 스크린 평면을

27) 김성환, 이진혁, 김승주, “어깨너머공격자 모델링 및 보안 키패드 취약점 분석”, 한국정보보호학회 하계 학술대회, 2014

기준으로 하여 45도에서 315도 범위인 약 270도의 범위에서 공격자가 어깨너머 공격이 가능하다고 언급하고 있다. 피해자와의 공간과 거리에 있어서 피해자의 퍼스널 스페이스(personal space)를 침범하지 않으며, 공격자에게 피해자의 정보를 파악할 수 있는 가독성을 제공할 수 있는 거리에서 어깨너머 공격이 가능하다고 언급하고 있다. 앞서 설명한 스크린 각도와 공격자의 시야각(FOV, Field Of View)사이에 교차점이 형성되면 공격자는 쉽게 피해자의 정보를 획득할 수 있다. 또한 기존 보안 키패드의 취약점으로는 Random 배열과 사용자 입력에 따른 피드백과 피드백 시간 등이 있으며, Random 배열의 경우, 쿼티 키패드(Qwerty keypad)의 특징으로 인해 각 행의 공백이 작고 제한적인 환경에서의 Random화로 공격자가 쉽게 사용자의 키패드 위치를 통해 어떤 키인지 유추 혹은 파악할 수 있다. 기존의 보안 키패드에서 사용자의 입력에 따른 피드백을 위해, '*' 모양의 피드백을 주었지만, 이러한 피드백으로 인해, 사용자의 오타율이 높아지자, 현재는 많은 보안 키패드에서 사용자가 가장 최근에 입력한 키를 보여주는 형태의 피드백을 제공하고 있으며, 이러한 피드백은 어깨너머 공격에 매우 취약하다. 또한 이러한 피드백과 더불어 사용자의 충분한 피드백 인지를 위한 피드백 시간으로 인해 공격자 또한 사용자의 입력에 대한 피드백을 통한 정보 획득이 쉬워진다는 단점이 있다.

스마트폰에서의 PIN값에 대한 입력은 어깨 너머 공격에 취약점을 가지며 이를 해결하기 위해 많은 연구가 진행되어 왔다. 본 절에서는 현재까지 진행된 어깨너머 공격에 관련 연구를 소개한다. cognitive trapdoor games 라 불리는 방식을 통해 기존 PIN을 대체하는 기술이 제안되었다 [28]. 초기 입력 화면이 공격자에 노출된다고 하더라도 실제 입력하는 숫자가 노출되지 않는 방식을 취하기 때문에 어깨 너머 공격으로부터 안전하다. 하지만 확률을 기반으로 동작하여 실용적인 구현은 어렵다. 그래픽 기반 패스워드도 어깨 너머 공격을 방지하기 위해 제안되었다 [29]. 특히 보다 개선된 그래픽 기반 패스워드인 CHC(Convex Hull Click) 스키마는 이미지 기반 입력 화면에 초기 설정된 이미지들을 사용하여 Convex Hull을 만들고 이미지들이 연결된 내부 도형을 선택함으로써 challenge를 발생시킨다. 이를 통해 안전하

28) Roth, Volker, Kai Richter, and Rene Freidinger. "A PIN-entry method resilient against shoulder surfing." In Proceedings of the 11th ACM conference on Computer and communications security, pp. 236-245. ACM, 2004.

29) Wiedenbeck, Susan, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. "Design and evaluation of a shoulder-surfing resistant graphical password scheme." In Proceedings of the working conference on Advanced visual interfaces, pp. 177-184. ACM, 2006.

게 키를 선택하는 것이 필요하지만 초기에 3개의 이미지를 설정하여야 하는 불편함을 가진다. EyePassword라는 기술은 직접 키를 터치하여 입력하는 방식이 아니라 시선 추적을 통하여 버튼을 입력하도록 하였다 30). 빨간 점을 키패드 각각에 추가하여 시선이 키패드 버튼 중심에 고정될 수 있도록 하여 정확성을 증가시켰다. 하지만 입력에 비해 이를 처리하는 비용이 많이 드는 기법으로 실제 활용에는 적합하지 않다. 현재까지 진행된 연구에서는 공격자로부터 입력을 보이지 않도록 하는데 집중하여 이를 처리하는 비용이 증가했으며 따라서 실제 응용에는 매우 적합하지 않다. 또한 시각적인 피드백을 사용함으로써 공격자에게 비밀번호가 노출되는 문제점을 가진다. 따라서 본 논문에서는 기존의 PIN 방식에서의 보안성을 증가시키면서 실제 바로 적용이 가능한 촉각 기반 보안 키패드 방식을 제안한다.

3. 가상 키패드

스마트폰의 사이즈와 무게를 줄이기 위해 초기의 물리 키보드가 있던 모델은 소프트웨어를 이용한 터치 키패드를 스마트폰에 적용하고 있다. 하지만 사용자가 터치를 하는데 주로 사용하는 엄지손가락은 가상키패드의 키에 비해 상대적으로 크기 때문에 입력 속도가 느리고, 오타율이 높은 단점을 가진다 31). 기존의 물리 키보드는 각 키가 오목한 면으로 구분되어 있어서 촉각적인 피드백을 통해 오타를 감지 할 수 있기에 사용자는 정확한 키 입력이 가능했다. 하지만 터치 키보드는 촉각적인 피드백을 주지 못하기 때문에 보다 높은 오타율이 발생하게 된다 32). 이러한 터치 키패드의 오류율을 줄이기 위해서 누르고자 하는 키의 버튼에 대한 접촉 면적이 다른 버튼에 비해 높다는 예측적 접근이 도입되면서 오류율이 줄어들었지만 원천적으로 타자 오류를 차단하는 것은 불가능하다. 터치 키패드에서는 키의 크기 또한 입력속도와 오류율에 큰 영향을 미친다 33). <그림 8>의 결과는 일반적인 정사각형 형태의 숫자 키패드에서의 오류율을 나타내고 있다. 그래프의 결과에서 알 수 있듯이 키패드의 크기가 커질수록 입력 오류율이 줄어들게 된다. 또한 입력오류율은 비밀번호에 큰 영향을 받아 입력 자

30) Kumar, Manu, Tal Garfinkel, Dan Boneh, and Terry Winograd. “Reducing shoulder-surfing by using gaze-based password entry.“ In Proceedings of the 3rd symposium on Usable privacy and security, pp. 13-19. ACM, 2007.

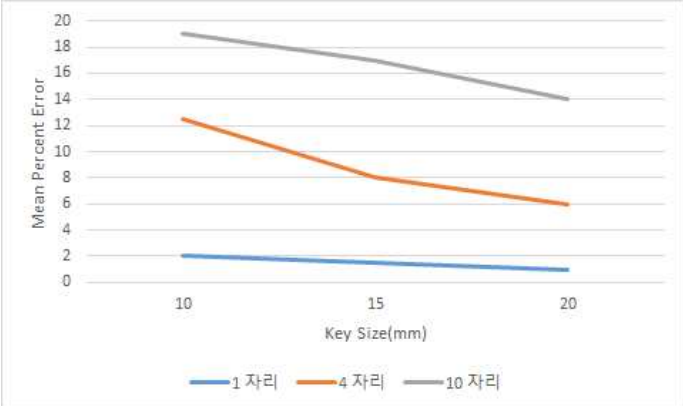
31) 양형규. “스마트폰을 위한 보안 키패드의 안전성 분석.“ 정보보호학회지 21, no. 7 (2011): 30-37.

32) 박건혁; 황경훈; 김선욱; 사재천; 정문채; 최승문. 터치스크린 모바일 폰에서 진동 피드백을 이용한 버튼 클릭감 모사, 한국HCI학회 학술대회, 2011, 254-256.

33) 임수민; 김형중; 김성기. Shoulder Surfing 공격을 고려한 패스워드 입력 시스템 구현 및 통계적 검증. 전자공학회논문지, 2012, 49.9: 215-224.

릿수의 길이가 커질수록 오차율이 높음을 확인할 수 있다. 예를들어 가로, 세로 10mm의 자판 기준으로 10자리 비밀번호 입력 시 오타율이 19%를 나타냄을 확인할 수 있다.

<그림 8> **일반적인 키패드 상에서의 오류율**



<그림 9> **오타 발생 시나리오**

<그림 8>의 오차율을 실제 금융어플리케이션에 적용하여, 숫자 키패드로 계좌 비밀번호와 보안카드 비밀번호를 입력한다면 입력 값의 길이가 4자리를 넘지 않고, 각 키 사이즈가 갤럭시 S2기준 가로 30mm * 세로 20mm라고 할 때 오타 입력 확률은 2~4% 대로 수렴함을 확인할 수 있다. 그에 반해 쿼티 키패드에서는 키패드의 크기가 20mm*10mm의 크기이므로 입력

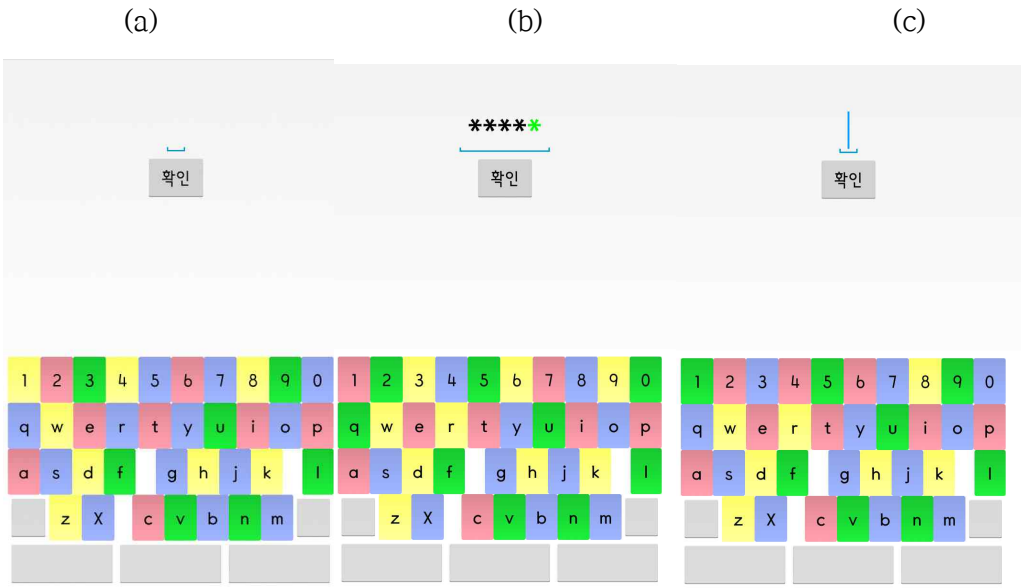
하는 비밀번호가 10자리 비밀번호라고 생각해볼 때 오타율은 14~16% 임을 확인할 수 있다. 따라서 사용자가 자신의 오타를 인식하고 이를 알맞게 수정하는 피드백 작업을 효율적으로 수행하기 위한 방법이 사용되고 있다. 기존의 물리 키보드를 사용하는 PC 환경에서는 오타율이 비교적 낮았기 때문에 피드백 없이 화면에 비밀번호를 '*' 기호를 이용하여 나타내었다. 하지만 터치 키패드에서는 높은 오타율에 대한 피드백을 주기 위해 입력한 마지막 키 값을 화면에 그대로 표시하고 이전 입력 값은 '*' 를 통해서 은닉 하는 방법을 사용하고 있다. 오타율과 그에 대한 피드백에 대한 시나리오를 <그림 9>를 통해 쉽게 생각해 볼 수 있다. 만약 사용자가 키 'j' 를 눌렀을 경우에 오타를 누를 가능성이 있는 주변의 키들은 i, h, k, n, m이다. 따라서 사용자가 누르고자 했던 j와 주변키들 간에 차별화된 피드백을 사용자에게 비밀리에 전달할 수 있다면 사용자는 오타를 인식할 수 있을 뿐 아니라 비밀번호를 주위의 공격자에게 노출하지 않게 된다. 이러한 입력방식은 터치 키패드의 높은 입력 오류율의 해결에는 효과적이지만 공공장소에서 악의적인 공격자의 어깨너머 공격에 매우 취약한 단점을 가진다. 따라서 비밀번호를 주위의 악의적인 공격자에게 숨기면서 사용자에게는 적절한 피드백을 줄 수 있는 방안에 대한 연구가 필요하다. 이를 위해 2013년도 금융보안공모전에서는 색상을 통한 키패드 마스킹 기법이 제안되었다. 사용자는 문자를 통한 피드백 대신 색상정보를 대신 얻게 됨으로써 공격자에게는 정보를 노출시키지 않으며 자신에게 필요한 적절한 피드백을 받을 수 있도록 하였다. 하지만 해당 보안키패드는 악의적인 공격자의 공격에 취약성을 가진다. 자세한 분석은 다음 장에서 확인해 보도록 한다.

4. 2013년도 금융보안공모전 우수상 논문에서 제안된 보안 키패드의 취약성 분석

2013년도 금융보안공모전에 소개된 색상 마스크 보안 키패드의 동작방식은 기존에 숫자 혹은 글자를 그대로 보여주던 피드백 방식에서 벗어나 각각의 키에 매칭되는 색상을 표기함으로써 공격자가 입력 문자를 분석하는 것이 불가능하게 하였다. 또한 매번 자판의 색상을 무작위로 배치하여 색상을 통해 1대1로 매칭되는 경우의 수를 줄임으로써 보안 강도를 높였다. 색상을 이용하여 마스킹을 한 보안 키패드는 무작위로 키패드가 배열되기 때문에 공격자는 비밀번호를 알 수 없다. 만약에 키패드의 배열을 확인한

경우에도 전체 키의 수 (N), 색상 수 (C), 전체 비밀번호의 수(L)를 통해 도출된 비밀번호가 노출될 확률은 (N/C)^L과 같이 계산된다. 이는 전수조사의 경우 N^L의 경우의 수에 비해 개선된 보안성을 제시한다. 하지만 이는 실제 환경 상에서는 매우 심각한 보안 문제를 안고 있다.

<그림 10> **색상 마스킹 보안키패드**



두 가지의 환경을 가정하여 공격 성공 확률을 확인해 보도록 한다. 먼저 비밀번호는 간단하게 “12341” 이라고 가정하며 키패드는 무작위로 생성되었다고 가정한다. 이는 36^5의 복잡도로 계산되는 60466176의 경우의 수를 가진다. 첫 번째 가정부터 확인해보도록 한다. 공격자가 <그림 10>에서 입력창 즉 확인 버튼 위의 글을 어깨너머 공격을 시도한 경우이다. 공격자가 알 수 있는 정보는 비밀번호의 길이 그리고 각각의 색상이다. 각각의 무작위 키패드에서 생성된 색상을 살펴보면 (a) 노빨녹노노, (b) 빨녹노파빨, (c) 녹빨파빨녹 이 된다. 먼저 모든 경우의 수(a, b, c)에 동일한 색상이 나온 첫 번째 그리고 다섯 번째 ‘1’ 이라는 비밀번호는 동일한 수라는 것을 확인할 수 있다. 그리고 경우에 따라 동일한 색상이 나왔지만 나머지 키들은 모두 다른 비밀번호라는 것을 확인할 수 있다. 따라서 키패드를 확인하지 않은 경우에도 복잡도는 (36/4-1)*(36/4)^4 로써 경우의 수는 52488로 줄어들게 된다.

두 번째 가정은 키패드의 배열과 문자입력창을 확인하였다고 가정해보

자. 해당 경우의 수는 이전 연구에 의하면 색상은 4가지인 경우 (36/4)^5를 통해 59049이 도출된다. 하지만 실제로는 경우의 수가 1로써 100%의 확률로 비밀번호 검출이 가능하다. 예를들어 첫 번째 비밀번호 1은 (a) 노, (b) 빨, (c) 녹으로 표기된다. (a)에서 노란색인 키패드는 "1, 4, 8, w, d, h, k, z" 이며 (b)에서 빨간색인 키패드는 1, 7, e, t, u, p, a, c 이며 (c)에서 녹색인 키패드는 "1, 5, 9, u, f, l, v, n" 이다. 세 개의 집합의 교집합을 계산해보면 결과값은 "1" 이 되며 이는 비밀번호와 일치하는 값이 된다. 따라서 무작위 키패드는 오히려 보안강도를 낮추게 되며 색상 마스킹은 온전한 방어 기법이 될 수 없음을 확인할 수 있다.

5. 진동을 이용한 피드백 관련 연구

휴대폰 보급과 활발한 사용에 의해 휴대폰 기술 연구가 활발하게 진행되었으며 특히 터치스크린에 대한 피드백 관련 연구도 많이 진행되고 있는 실정이다. 본 절에서는 진동을 이용한 피드백 관련 연구에 대해 요약한다.

진동 모터는 햅틱, 가상현실, 휴먼 컴퓨팅 등에서 많이 사용되는 Actuator이며, 가격이나 사이즈 측면에서 장점이 있기 때문에 많이 사용된다. 진동 모터의 출력은 진폭과 주파주에 대해 상관관계를 가지며 사용자가 인지할 정도의 진동을 위한 입출력 전압을 연구되기도 하였고, 또한 진동 랜더링 방식이 제안되기도 하였다 [34)35)]. 진동 랜더링 방식은 사용자가 인지할 수 있는 진동 효과를 판단하기 위한 방법을 말하며 햅틱에서의 진동 디자인을 고려하였다.

모바일 기기에서 정보 전달 과정은 촉각을 통해서 이루어지며 이때 진동 강도 인지의 비선형성으로 인한 정보 왜곡을 파악하고, 이를 해결하기 위한 진동 랜더링 방법에 대한 연구가 진행되었다 [36)]. 두 개의 서로 다른 인가전압이 PTR을 사용하여 결정되었을 때, 사용자가 느끼는 진동의 비선형성을 보정할 수 있고 이들의 구분정확도를 크게 향상시킬 수 있다. 또한, PTR을 사용하면, 진동 강도의 레벨을 많이 나누어도 구분 정확도가 크게 감소하지 않기 때문에 진동 강도의 수를 많이 누눌 수 있어 진동의 다양성을 향상시킬 수 있다.

34) J. Ryu, J. Jung, S. Kim, S. Choi, "Perceptually Transparent Vibration Rendering Using a Vibration Motor for Haptic Interaction", in Proceedings of IEEE ROMAN 2007, pp.310-315

35) J. Ryu, S. Choi, "Benefits of Perceptually Transparent Vibration Rendering in Mobile Device", Lecture Notes on Computer Science (EuroHaptics 2008), vol. 5024, pp.706-711

36) 류종현; 최승문. 모바일 기기에서 인지적으로 명료한 진동 렌터링을 통해 단진동의 인지 정확도 향상, 한국HCI학회 학술대회, 2010, 203-205.

진동, 소리에 대한 사용자 경험 및 느낌을 정성 조사하고 이에 따른 사용자 만족도를 분석하였으며 어느 쪽이든 제공되는 것이 만족도를 증가시키며, 이러한 피드백을 방해하는 자극에 따라 작업 부하량을 나타내는 실험 또한 진행하였으며 진동과 소리 피드백이 제공될 경우 작업 부하를 낮추고 사용자가 덜 귀찮다고 느낀다 [37]. 이를 통해 휴대폰에서의 피드백의 질적 측면 및 작업 수행과의 관계 및 실사용 환경에서 피드백을 선택하게 하는 요인 등을 확인 할 수 있다.

또한 LRA(Linear Resonance Actuator)와 DMA(Dual Mode Actuator)를 사용하여 실제 버튼 클릭 시 발생하는 진동을 모사하고 실제 버튼과 비교하는 실험도 진행되었다 [38]. 버튼 클릭 시 발생하는 진동 파형, 신호 변조 조건, 진동자, 파형 등을 분석하여 실제 진동을 모사할 수 있는 모델을 세웠다. 최근에는 3개의 서로 다른 진동 패턴을 가지는 키보드를 통해 사용자가 값 입력 시 적합한 피드백을 받는 것이 가능한 기법이 제시되었다 [39]. 이는 진동의 주기가 서로 다름을 손가락의 끝으로 인지하는 것이 가능하도록 설계되었다. 제안하는 기법에서는 해당 기법을 확장하여 사용한다. 이전의 기법은 키보드의 배치를 고려한 입력이 아닌 3개의 다른 패턴을 배치한다. 하지만 제안하는 기법은 키보드의 배치를 같이 고려함으로써 사용자의 입력 오류를 줄이고 타자 속도를 높이는 기법을 제안한다.

Ⅲ. 제안하는 보안 키패드

본 논문에서는 어깨너머 공격에 강인한 보안 키패드를 제안한다. 위에서 제시한 기법들을 사용하여 기존의 실제 문자를 화면에 띄워주는 방식과는 진동을 발생시켜 피드백을 줌으로써 공격자의 어깨너머 공격을 효과적으로 방어한다. 이는 키패드의 각 글자마다 독특한 특성을 가지는 진동을 발생시켜 사용자가 확인이 가능하도록 하는 기법이다. 사용자는 손으로 느껴지는 진동을 통해 입력된 문자 정보를 확인하는 것이 가능하지만 공격자는 입력된 키보드의 정보를 얻는 것이 매우 제한적이다. 따라서 이와 같은 특징은 기존의 보안키패드에 비해 제안하는 키보드의 보안성이 한층 높아

37) 김영일; 김세미; 민영삼. 터치스크린 휴대폰 사용 환경을 고려한 소리, 진동 피드백 연구. 한국HCI학회 학술대회, 2008, 130-134.

38) 박건혁; 황경훈; 김선욱; 사재천; 정문채; 최승문. 터치스크린 모바일 폰에서 진ㄴ동 피드백을 이용한 버튼 클릭감 모사, 한국HCI학회 학술대회, 2011, 254-256.

39) BIANCHI, Andrea; OAKLEY, Ian; KWON, Dong Soo. The secure haptic keypad: a tactile password system. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010. p. 1089-1092.

졌다고 할 수 있다.

1. 진동을 이용한 피드백 기법

키패드를 입력하게 될 때 사용자가 기대하게 되는 것은 자신이 적합한 키를 입력했는지에 대한 피드백을 시각적으로 제공하는 것이다. 하지만 본 논문에서는 시각이 아닌 진동을 통해 사용자에게 피드백이 전달됨으로써 안전한 보안 키패드를 제안한다. 먼저 가장 쉽게 생각해 볼 수 있는 부분은 진동이 있고 없음으로 생각해 볼 수 있다. 2진법으로 생각해보면 진동이 있는 경우에는 정보가 1이며, 없는 경우는 0으로 생각해 볼 수 있다. 더 나아가 진동의 패턴 혹은 세기 그리고 주기를 생각해보면 정보의 양은 무한히 늘어날 수 있다.

본 논문에서 제안하는 진동을 이용한 피드백 기법은 사용자의 진동 민감도를 판단하는 것이 중요하다. 그 이유는 사용자가 진동의 차이를 느끼지 못한다면 정확한 피드백을 사용자가 받는 것이 어렵기 때문이다. 따라서 <그림 11>에서와 같이 사용자들에게 서로 상이한 진동 주기를 설정하고 사용자의 진동 민감도를 확인하였다. 총 3개의 진동인터벌 (0.1초, 2.1초), (0.7초, 2.1초), (1.3초, 2.1초)와 같이 사용자가 짧은 진동과 긴 진동을 구분하는 것이 가능한지에 대해서도 확인해 보았으며 결과적으로는 (0.7초, 2.1초)의 경우가 적합함을 확인할 수 있었다 (4장의 <그림 17> 참고). 그 이유는 진동간의 격차가 너무 짧은 (1.3초, 2.1초)의 경우 사람이 판단하기 힘들었으며 너무 하나의 진동이 짧은 경우 해당 진동을 느끼는 신경이 무뎌짐을 확인할 수 있었다. 따라서 본 논문에서는 진동의 유무, 진동의 주기(long, short)로 나누어 총 3가지의 정보(무진동, 짧은 진동, 긴 진동)를 사용한다. 자세한 실험치는 4장 평가에서 확인해 보도록 한다.

<그림 11> 진동 민감도 확인 실험

2. 키패드와 피드백의 관계

키패드에 타자를 입력 시 오타가 발생할 확률은 <그림 12>와 같이 크게 두 가지 경우이다. 첫 번째는 q, w와 같이 옆으로 근접해 있는 키를 잘못 누르는 경우이며 두 번째는 e, s와 같이 위, 아래로 배치된 키를 잘못 누르는 경우이다. 손가락은 대체로 옆으로의 길이가 길기 때문에 같은 행에 위치하는 키 간에 오타가 발생할 확률이 높다. 따라서 이러한 특징을 고려하면 같은 행에 대한 오차는 줄이며 위, 아래로는 어느 정도 오타율을 감안하는 보안 키패드의 디자인이 가능하다. 본 논문에서는 이러한 특징을 반영한 총 세 가지의 진동 기반 보안 키패드를 설계 및 구현하였다.

<그림 12> **키패드 상에서의 오차 발생 경우의 수**

3. 색상과 진동 마스킹 기법

첫 번째 기법은 색상과 진동 정보를 혼합하여 사용자에게 피드백을 주는 키보드이다. <그림 13>에는 설계된 키패드가 소개되어 있다. 먼저 해당 키보드는 열과 행에 대한 피드백을 색상과 진동으로 나누어 주는 기법을 적용하였다. 그림에서와 같이 현재 총 4개의 행으로 나뉘게 된다. 여기서 다시, 빨간 네모로 하이라이트가 된 부분과 그렇지 않은 부분으로 나뉜다. 먼저 같은 행에 위치한 문자열에 대한 피드백 정보는 색상이다. 만약 q, w를 누르게 된다면 화면상에는 빨간색 그리고 파란색이 나타나게 된다. 서로 다른 행간의 입력 오타를 확인하기 위해서는 진동이 사용된다. 만약 2번째 줄의 u와 3번째 줄의 h를 입력한 경우 동일하게 화면상에는 빨간색이 표시되게 된다. 하지만 다른 행간의 구별을 위해 우리는 진동을 피드백 정보로 사용하여 빨간 네모가 들어간 부분에서는 진동이 발생하도록 하였다. 따라서 u에서는 진동이 발생하지 않지만 h에서는 진동이 발생하여 동일한 색상을 피드백으로 받게 되는 경우에도 사용자는 진동을 통해 위, 아래의 글자를 비교하는 것이 가능해 진다. 키패드의 생성은 가능한 키패드 유추 공격을 방지하기 위해 키패드는 매번 고정된 형식으로 제시된다. 자세한 보안 키보드 동작 메커니즘은 알고리즘 1에 상세히 설계되어 있다.

알고리즘 1. 보안 색상, 진동 키패드	
입력: 버튼입력 출력: 입력창 출력, 색상 출력, 진동발생	
1.	if (진동 발생 행)
2.	if(빨간색 버튼)
3.	입력창에 빨간색 * 표기 및 진동 발생
4.	else
5.	입력창에 파란색 * 표기 및 진동 발생
6.	endif
7.	else
8.	if(빨간색 버튼)
9.	입력창에 빨간색 * 표기
10.	else
11.	입력창에 파란색 * 표기
12.	endif
13.	endif

〈그림 13〉 **진동/색상 융합 마스킹보안 키패드**

4. 진동기반 마스킹 기법

본 장에서 살펴볼 제안 기법은 색상을 통한 피드백을 완전히 제거한 구현기법이다. 그 이유는 공격자가 색상을 통한 피드백 정보는 악용이 가능하다는 문제점이 있기 때문이다. 따라서 진동만을 통해 사용자에게는 적절한 피드백을 제공하지만 공격자는 어깨너머 공격을 통해 사용자의 입력 정보를 얻는 것이 불가능하다.

알고리즘 2. 보안 진동 키패드	
입력: 버튼입력 출력: 입력창 출력, 진동발생	
1.	if (진동 버튼)
2.	입력창에 * 표기 및 진동 발생
3.	else
4.	입력창에 * 표기
5.	endif

가. 진동 마스킹 기법

진동만을 이용한 보안 키패드의 설계는 <그림 14>와 같다. 각각의 키패드에는 색상이 입혀졌지만 이는 색상정보를 나타내기 보다는 사용자에게 해당 버튼의 진동 유무를 표기하는 것이다. 예를 들어 파란색의 경우 진동이 없지만 빨간색의 경우 진동이 발생한다. 이때 입력창에는 파란색과 빨간색 버튼 모두 동일한 검은색 글자 형식으로 피드백이 나타나게 된다. 해당 기법은 위, 아래에 대한 오탈자의 확률을 키 간의 여백을 줌으로써 제거하고 행간의 피드백을 생략한 기법이다. 이는 사용자의 오탈자가 주로 양 옆의 키에서 발생하는 사실과 위, 아래의 키 간의 오탈자의 확률이 낮음에 착안하여 제시된 기법이다. 해당 기법은 공격자가 사용자의 키가 무엇이 입력되는지 확인할 수 없지만 사용자는 적합한 피드백을 받는 것이 가능하다는 장점을 가진다.

<그림 14> **진동 보안 키패드**

나. 문자수 마스킹 기법

이전 장에서 제안한 보안 키패드의 경우 지금까지 제안된 키패드 중 가장 안전한 키패드이다. 그 이유는 공격자가 확인 가능한 *라는 정보는 문자수를 제외한 그 어떤 정보도 공격자에게 제공하지 않았기 때문이다. 하지만 *라는 정보 역시 공격자에게는 유익한 정보가 될 수 있다. 예를 들어 사용자의 비밀번호의 개수가 6자리라는 것을 *의 수를 세어 확인한 경우 굳이 긴 비밀번호에 대한 전수조사를 수행할 필요 없이 6자리에 대한 전체 경우의 수를 살펴보면 정확한 키를 확인하는 것이 가능하다. 따라서 본

장에서는 비밀번호의 수까지 진동 피드백을 통해 완벽히 마스킹하는 기법을 제안하고자 한다. <그림 15> (a)에서는 진동을 이용한 문자수 마스킹 보안 키패드가 제시되어 있다. 여기서는 총 3가지 정보를 이용한다. 첫 번째는 파란색 버튼으로써 화면상에 *문자만 표기되고 진동은 발생하지 않는다. 두 번째는 빨간색 버튼으로써 화면상에 *문자가 표기됨과 동시에 짧은 진동이 발생하도록 한다. 세 번째는 노란색 버튼으로써 화면상에는 아무런 문자가 표기 되지 않고 긴 진동만이 발생하게 된다. 해당 기법을 사용하면 사용자가 노란색 버튼을 누르는 경우, *문자가 입력창에 표기되지 않으므로 공격자는 사용자의 비밀번호의 수를 정확히 파악하는 것이 힘들다. 해당 기법은 보다 안전성을 높여 설계하면 아예 문자를 보여주지 않는 기법으로 발전가능하다. <그림 15> (b)에서와 같이 두개의 키를 하나는 짧은 진동 그리고 다른 하나는 긴 진동을 주는 경우로 나누어 피드백을 주고 화면상으로는 아무런 글자가 표기하지 않는 기법을 통해 공격자가 화면을 훔쳐볼 때 얻을 수 있는 정보가 전혀 생성되지 않도록 하는 안전한 보안 키패드의 설계가 가능하다.

알고리즘 3. 보안 진동 마스킹 ver.1	
입력: 버튼입력 출력: 입력창 출력, 진동발생	
1.	if (무진동 버튼)
2.	입력창에 * 표기
3.	else if (짧은 진동 버튼)
4.	입력창에 * 표기 및 짧은 진동 발생
5.	else if (긴 진동 버튼)
6.	긴 진동 발생
7.	endif

알고리즘 4. 보안 진동 마스킹 ver.2	
입력: 버튼입력 출력: 진동발생	
1.	if (긴 진동 버튼)
2.	긴 진동 발생
3.	else if (짧은 진동 버튼)
4.	짧은 진동 발생
5.	endif

<그림 15> **진동을 이용한 문자수 마스킹 보안 키패드**

(a) ver1 (b) ver2

Ⅳ. 구현 및 성능 평가

본 장에서는 논문에서 제안하는 보안 키패드 기법을 실제 안드로이드 휴대폰에 구현 및 테스트하여 그 효용성에 대해 살펴본다. 안드로이드 스마트폰 어플리케이션에서의 기본적인 구현 방식은 다음과 같다. 각 키보드의 글자판은 버튼을 이용해서 구현한다. 버튼에는 각각의 구현 아이디어에 따라 다른 진동 패턴이 들어가게 된다.

1. 성능 평가

본 장에서는 보안성에 대해 확인해 보기 위해 현재 기법에서의 공격 가능성에 대해서 확률적 관점에서 확인해 보도록 한다. 또한 보안 키패드의

성능 분석을 위해서 키패드 상에서의 타자의 신속성 그리고 정확성을 비교 분석 한다.

2. 보안성

어깨너머 공격에 대한 보안성은 최근 출시되고 있는 스마트 디바이스인 구글 글라스에 의해 보다 그 중요성이 높아지고 있다. 공격자는 구글 글라스를 사용하여 아무런 제재 없이 사용자의 비밀번호 입력과정을 녹화하는 것이 가능하다. 만약 기존의 기법을 사용하여 비밀번호를 입력한다면 입력창 정보를 통해서도 공격이 가능한 취약점을 가진다. 하지만 제안된 보안키패드는 어깨너머 공격에 노출되더라도 공격자가 비밀번호를 확인하는 것이 어렵다. 그 이유는 모든 값이 별표로 표기되거나 아무런 글자도 표기되지 않으므로 키패드에서 어떤 값이 입력되었는지 유추하는 것이 불가능하다.

가. 진동, 색상 보안 키패드

해당 보안 키보드의 경우 전체 키의 개수가 N이라고 할 때 두 개의 색상 정보를 통해 구분되어 저장되면 N/2의 확률로 하나의 키에 대한 색상이 결정된다. 작년 금융보안 공모전 디자인의 경우 최소 3개 이상의 색상을 이용하였다. 그 이유는 그래프 이론에 따라 인접한 국가를 나타낼 때 최소 3개의 색이 필요하다는 특징 때문이다. 만약 3개의 색상을 이용하는 경우 N/3의 확률, 그리고 4개의 경우 N/4 확률로 색상이 결정되게 된다. 따라서 하나의 색상에 매칭되는 단어의 경우의 수가 제안하는 기법의 경우 높기 때문에 전수조사를 통한 공격에 보다 작년 보안금융보안 공모전에 비해 안전하다고 할 수 있다.

나. 진동 보안 키패드

해당 키보드에서 제공하는 정보는 사용자가 타자를 입력 시 *문자를 출력하는 것으로써 비밀번호의 길이를 제외한 모든 비밀정보가 마스킹이 되어 나타나게 된다. 따라서 해당 구현 기법을 통해 P개의 비밀번호를 입력할 경우 전체 키의 개수가 N일 때 약 N^P의 복잡도를 가지게 된다.

다. 진동 마스킹 보안 키패드

해당 기법에서는 공격자가 확인 가능한 정보는 비밀번호의 최소 길이 혹

은 아무런 정보가 없다. 부분적인 문자수 마스킹의 경우 나타난 *의 숫자가 비밀번호의 부분적인 개수를 나타낸다. 따라서 나타난 *수는 최소의 비밀번호 길이 임을 유추할 수 있다. 부분 문자수 마스킹 기법을 개선한 전체 문자 마스킹 기법의 경우에는 공격자가 어깨너머 공격을 통해 확인가능한 정보가 존재하지 않는다. 따라서 해당 기법은 지금까지 제안된 기법 중에 가장 안전하다고 할 수 있다.

3. 타겟 보드

사용된 타겟 보드는 <그림 16>와 같이 2가지 갤럭시 스마트폰으로 선정하였다. 이는 다양한 해상도와 화면 크기 그리고 CPU 환경을 고려하여 보다 객관적인 지표를 제공하기 위한 환경설정이다. 이전 스마트폰인 갤럭시 S1와 갤럭시S2의 경우 테스트를 진행해본 결과 속도가 느리며 스크린의 크기가 작고 해상도가 낮아 타자입력이 원활히 되지 않아 해당 성능 평가에서 제외되었다.

<그림 16> **타겟보드(갤럭시 S3, 갤럭시 S4)**

[표 1]에서는 갤럭시 시리즈에 대한 상세한 성능을 제시한다. 최신 스마트폰의 경우 가장 큰 화면과 해상도를 제공한다. 따라서 화면상의 버튼의 크기가 가장 커지게 되고 이는 추후에 실험에서 나타나는 바와 같이 높은 정확도와 빠른 타자 속도를 제공하게 된다.

[표 1] **타겟 장비에 대한 상세 설명**

특성	갤럭시1	갤럭시2	갤럭시3	갤럭시4
해상도	480X800	480X800	720X1280	1920X1080
디스플레이	4인치 슈퍼아몰레드	4.3인치 슈퍼아몰레드플러스	4.8인치 HD슈퍼아몰레드	5인치 풀HD 슈퍼아몰레드
버튼크기(cm) (가로x세로)	0.4x0.3	0.5x0.8	0.6x0.75	0.6x0.85
CPU	1GHz 싱글	1.2GHz 듀얼	1.4GHz쿼드	1.6GHz옥타

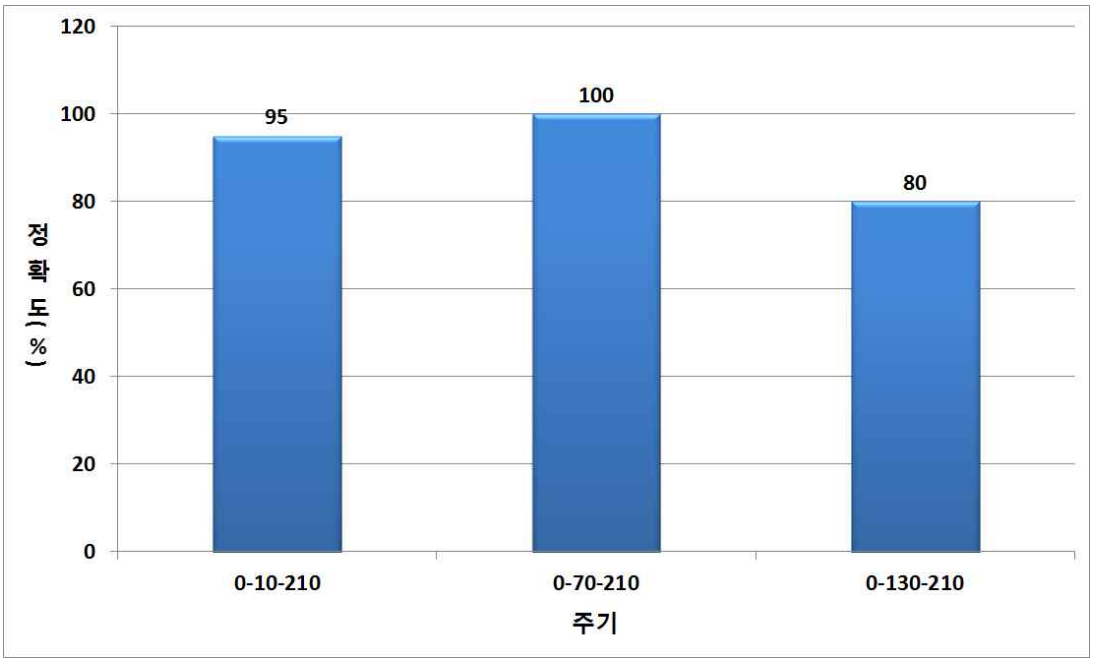
[표 2]에서는 실험에 참가한 4명의 실험자에 대한 상세 설명이다. 본 실험에 참가한 실험자들은 건장한 체격에 시력에 문제가 없으며 기존에 스마트폰을 사용하여 소프트 버튼을 능숙히 사용할 수 있다.

[표 2] **실험자에 대한 상세 설명**

특징	실험자1	실험자2	실험자3	실험자4
시력	0.8	0.7	0.8	1.0
어깨너비	105	100	100	105
체중(kg)	74	65	66	83
키(cm)	180	175	176	177

가장 먼저 진동에 대한 사용자들의 민감도에 대해서 확인해 보았다. <그림 17>에서는 4명의 실험자가 각기 다른 주기를 비교 테스트했을 때 구별에 대한 정확도를 나타내고 있다. 결과에서 알 수 있듯이 0-70-210(0초, 0.7초, 2.1초)을 통해 주기 테스트를 한 경우에 가장 높은 정확도를 나타내었다. 0-130-210(0초, 1.3초, 2.1초)의 경우에는 130과 210을 구별하는 것이 힘들었기 때문에 이를 피드백 정보로 사용하는 것은 좋지 않다. 또한 0-10-210(0초, 0.1초, 2.1초)의 경우 0과 10 즉 진동과 무진동에 대한 차이점을 구별하는 것이 힘들어서 올바른 측정이 되지 않았다. 자세한 실험 결과는 [표 3~6]에 상세히 기록되어 있다. 하나의 주기에 따라 5번의 시도가 수행되었으며 이를 통해 민감도를 확인하였다. ○표는 사용자가 정확히 진동을 파악한 경우이고 ×는 진동을 제대로 판단하지 못한 경우를 나타낸다.

<그림 17> **진동 주기에 따른 정확도 분석**



[표 3] **실험자1의 진동 민감도 테스트**

주기	실험자 1				
	시도1	시도2	시도3	시도4	시도5
0-10-210	○	○	○	○	○
0-70-210	○	○	○	○	○
0-130-210	○	○	○	○	○

[표 4] **실험자2의 진동 민감도 테스트**

주기	실험자 2				
	시도1	시도2	시도3	시도4	시도5
0-10-210	○	○	○	○	×
0-70-210	×	○	○	○	○
0-130-210	○	○	○	×	○

[표 5] **실험자3의 진동 민감도 테스트**

주기	실험자 3				
	시도1	시도2	시도3	시도4	시도5
0-10-210	○	○	○	○	○
0-70-210	○	○	○	○	○
0-130-210	○	○	×	○	×

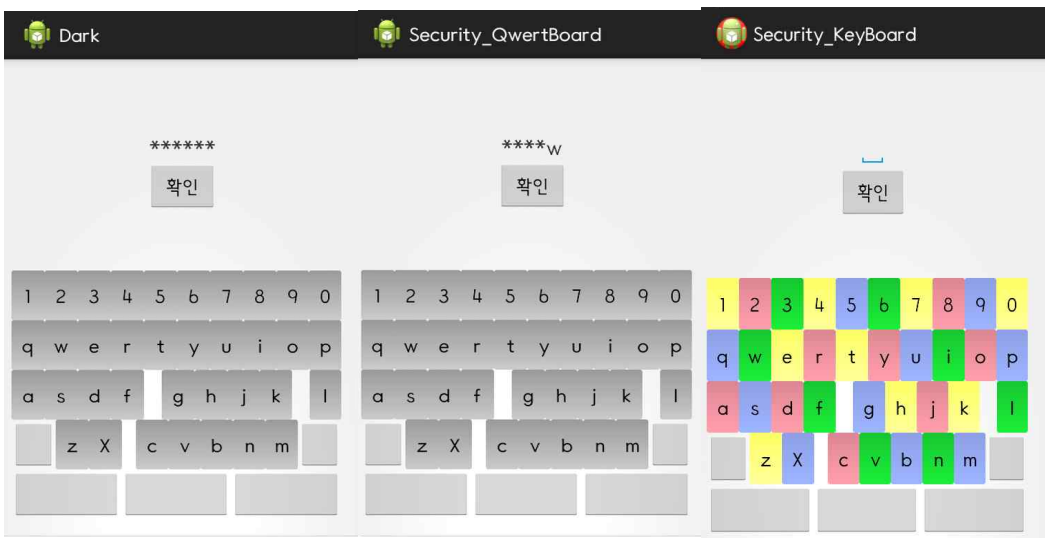
[표 6] **실험자4의 진동 민감도 테스트**

주기	실험자 4				
	시도1	시도2	시도3	시도4	시도5
0-10-210	○	○	○	○	○
0-70-210	○	○	○	○	○
0-130-210	×	○	○	○	○

키패드의 정확성, 신속성에 대한 실험은 현재 사용 중인 끝 글자가 보이는 키패드, 일반적으로 PC환경에서 사용되는 모든 글자가 '*' 로 은닉되는 키패드, 작년 보안공모전의 색상 키패드, 그리고 제안하는 진동 키패드 3종을 비교한다. 실험을 위해서 구현한 두 가지 기존 키패드 모델은 <그림 18> (a), (b)과 같은 화면 구성을 가진다. <그림 18> (c)에서는 색상 보안 키패드를 나타낸다. <그림 19>에서는 제안하는 진동 보안 키패드 3종을 나타낸다. 실험에서는 총 6가지 키패드를 이용하여 정확도와 신속도 그리고 보안에 대한 실제적인 데이터를 수집 및 분석하였다.

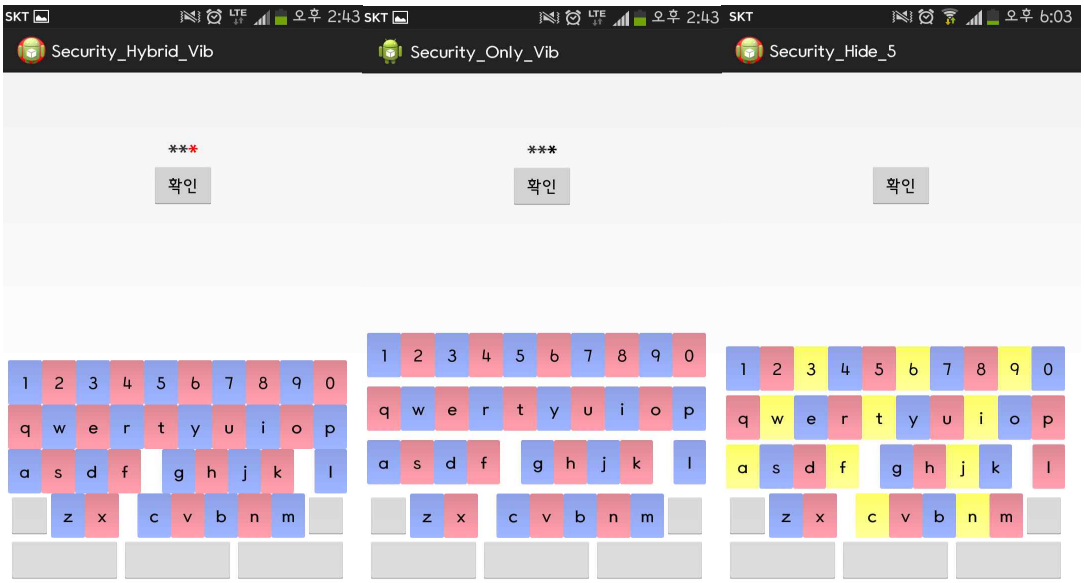
<그림 18> **기존 보안 키패드**

(a) 마지막 글자 마스킹 (b) 마지막 글자 표기 (c) 색상 표기



<그림 19> **제안하는 진동 보안 키패드**

(a) 색상+진동 (b) 진동+문자 (c) 진동



비밀번호의 안전성을 보장하기 위해서는 비밀번호에 대한 정보 노출을 줄이는 것이 중요하다. 하지만 높은 오타율을 해결하기 위해 입력 값에 대한 피드백을 제공하는 기존하는 보안 키패드는 어깨너머 공격에 매우 취약하다. 또한 2.4장에서 살펴보았듯이 색상 보안 키패드도 보안에 취약하다. 하지만 본 논문에서 제안한 기법은 높은 보안성과 함께 사용자에게 진동을 통한 피드백 정보를 제공하여 타자의 정확성를 유지할 수 있도록 설계되었다. 정확성과 신속성 실험은 동시에 이루어 졌으며 <그림 20>는 해당 실험의 동작화면이다. 실험은 키패드의 좌측 최 하단 버튼을 누르면 무작위의 12글자의 단어가 중간에 생성 되고, 해당 글자를 입력한 후에 확인 버튼을 누르면 오타율과 소요시간이 측정되도록 하였다. 이때 표시된 오타율과 소요시간은 실험자가 각자 자신의 답안지에 작성하였다. 작성된 답안지는 정리된 후 본 논문에 추가되었다.

<그림 20> **정확도 및 신속도 실험 환경**

4. 정확성

비밀번호의 안전성을 보장하기 위해서는 비밀번호에 대한 정보 노출을 줄이는 것이 중요하다. 하지만 높은 오타율을 해결하기 위해 입력 값에 대한 피드백을 제공하는 기존하는 보안 키패드는 어깨너머 공격에 매우 취약하다. 하지만 본 논문에서 제안한 기법은 높은 보안성과 함께 사용자에게 피드백 정보를 제공하여 타자의 정확성도 유지할 수 있도록 설계되었다. [표 12~13]에서는 보안 키패드에 대한 정확도를 나타내며 각각의 플랫폼의 평균 정확도는 <그림 21>에 그래프로 도식하여 나타내었다. 정확도를 플랫폼에 따라 확인해 보면 화면의 크기가 작을수록 버튼의 크기가 작아지므로 오타율이 높아짐을 확인할 수 있다. 기법에 대해 확인해 보면 정확도가 기존기법1에서 97.5%, 기존기법2에서 97.94% 그리고 색상 보안 키패드기법에서 100%로 나타남을 확인할 수 있다. 제안하는 기법의 경우에도 99.54%, 98.94% 그리고 99.58%의 정확도를 나타낸다. 이처럼 정확도를 통해 확인해 볼 때 제안기법이 기존기법과 비교해 볼 때 결코 정확도가 떨어지지 않음을 확인할 수 있다.

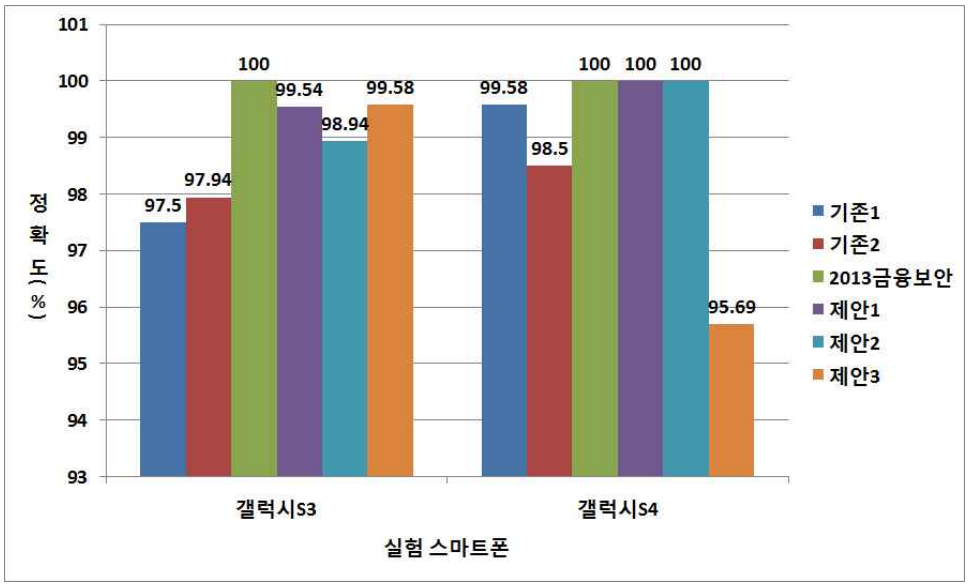
[표 11] **갤럭시 S3상에서의 정확도 실험결과**

기법	갤럭시S3 정확도 실험 결과(%)			
	실험자1	실험자2	실험자3	실험자4
기존 기법(1)	100	92	98	100
기존 기법(2)	100	95.778	100	96
2013년도 색상 키패드	100	100	100	100
(제안)진동, 색상 키패드	100	100	100	98.18
(제안)진동 키패드	100	97.78	100	98
(제안)진동 문자 마스킹 키패드	100	100	98.32	100

[표 12] **갤럭시 S4상에서의 정확도 실험결과**

기법	갤럭시S4 정확도 실험 결과(%)			
	실험자1	실험자2	실험자3	실험자4
기존 기법(1)	100	98.338	100	100
기존 기법(2)	100	96	100	98
2013년도 색상 키패드	100	100	100	100
(제안)진동, 색상 키패드	100	100	100	100
(제안)진동 키패드	100	100	100	100
(제안)진동 문자 마스킹 키패드	85	97.78	100	100

<그림 21> **보안 키패드 간 타자 정확도 비교**



5. 신속성

신속성이란 키패드를 통해 문자를 입력 시 얼마나 빠른 속도로 원하는 목표를 작성하는 지에 대한 척도이다. [표 14~15]에서는 12글자를 타이핑하는데 걸리는 시간을 나타낸다. 실험 결과 기존기법1에서는 7.3초, 기존기법2에서는 7.7초 색상 보안 키패드에서는 7.22초가 소모되었음을 확인할 수 있다. 제안하는 기법에서는 8.75초, 9.4초 그리고 8.06초가 소모됨을 확인할 수 있었다. 기존의 기법들에 비해 피드백을 진동이라는 새로운 방법을 통해 전달함으로써 익숙함이 떨어져서 해당 기법의 속도는 약간씩 느림을 확인할 수 있다. 하지만 큰 차이는 아니며 진동을 통한 피드백이 널리 사용되게 된다면 해당 기법에 대한 신속도도 향상 될 수 있을 것으로 생각된다. <그림 22>에서는 타겟 장비에 따른 신속도의 비교가 그래프를 통해 확인할 수 있도록 나타나 있다. 신속도의 차이는 각각의 디바이스마다 약간은 존재하지만 대체적인 신속도는 유사함을 확인할 수 있다.

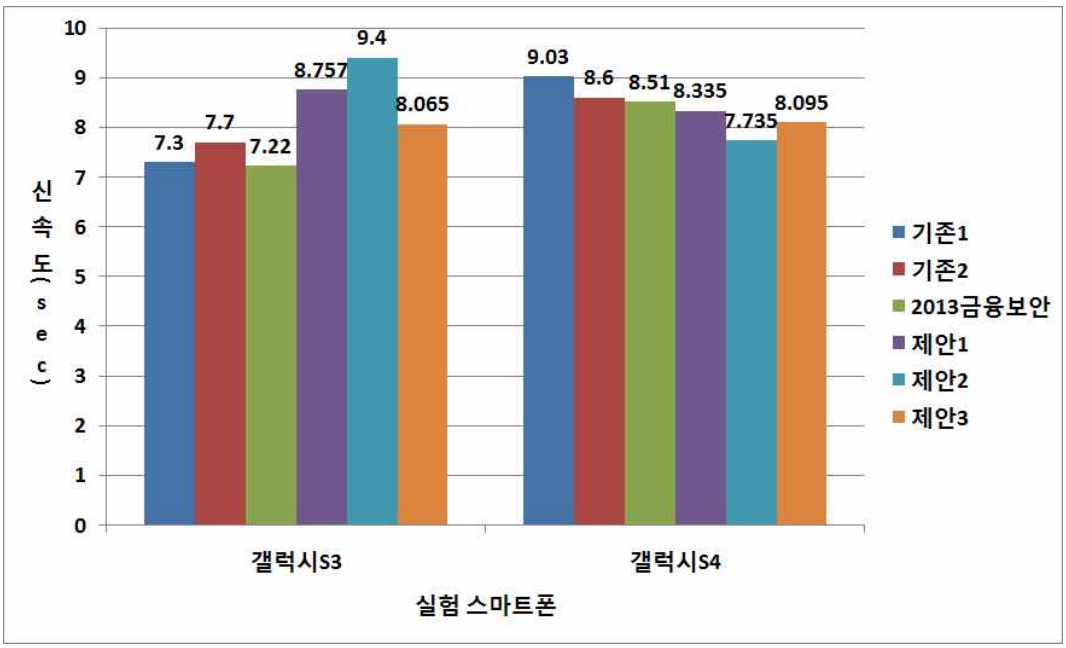
[표 13] **갤럭시 S3상에서의 신속도 실험결과**

기법	갤럭시S3 신속도 실험 결과(sec)			
	실험자1	실험자2	실험자3	실험자4
기존 기법(1)	5.699	6.46	8.7	8.3498
기존 기법(2)	6.3728	6.862	9.22	8.3306
2013년도 색상 키패드	7.52402	6.47	7.78	7.1258
(제안)진동, 색상 키패드	12.38	7.168	7.04	8.44
(제안)진동 키패드	14.02	8.42	6.92	8.24
(제안)진동 문자 마스킹 키패드	6.16	9.56	8.66	7.88

[표 14] **갤럭시 S4상에서의 신속도 실험결과**

기법	갤럭시S4 신속도 실험 결과(sec)			
	실험자1	실험자2	실험자3	실험자4
기존 기법(1)	6.8924	8.276	10.16	10.8046
기존 기법(2)	6.494	7.882	11.26	8.5708
2013년도 색상 키패드	8.5038	7.76	9.24	8.5306
(제안)진동, 색상 키패드	8.38	7.76	8.62	8.58
(제안)진동 키패드	8.62	7.08	7.76	7.48
(제안)진동 문자 마스킹 키패드	6.8	8.9	8.56	8.12

<그림 22> **보안 키패드 간 타자 신속도 비교**



[표 16~23]에서는 색, 진동 혹은 진동 보안 키패드에 대한 정확도 및 신속도 테스트 결과를 4명의 실험자를 토대로 실시한 결과이다. 각각의 실험

은 갤럭시 S3와 S4 상에서 5번씩 테스트되었으며 이를 토대로 이전에 살펴본 평균 정확도와 신속도가 계산되었다.

[표 16] **실험자1의 색, 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 1 (색+진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	13.6	9.4	12.5	11.9	14.5
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	8.5	11.0	8.7	6.8	6.9

[표 17] **실험자2의 색, 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 2 (색+진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	6.94	6.0	5.3	10.0	7.6
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	6.4	9.1	8.2	8.0	7.1

[표 18] **실험자3의 색, 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 3 (색+진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	8.4	6.4	8.1	5.8	6.5
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	9.9	9.9	6.6	9.1	7.6

[표 19] **실험자4의 색, 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 4 (색+진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	90.9	100	100	100
	속도(sec)	8.0	10.1	9.4	8.2	6.5
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	6.8	10.3	8.7	9.8	7.3

[표 20] **실험자1의 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 1 (진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	15.8	15.5	20.1	11.0	7.7
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	9.3	7.9	8.5	8.7	8.7

[표 21] **실험자2의 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 2 (진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	88.9	100	100	100	100
	속도(sec)	9.8	9.2	6.6	6.7	9.8
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	9.6	5.6	8.4	5.8	6.0

[표 22] **실험자3의 진동 보안 키패드 정확도/신속도 테스트**

타겟보드	구분	실험자 3 (진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	6.9	7.1	7.3	5.4	7.9
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	7.2	9.1	8.1	7.8	6.6

[표 23] **실험자4의 진동 보안 키패드 정확도/신속도 테스트**

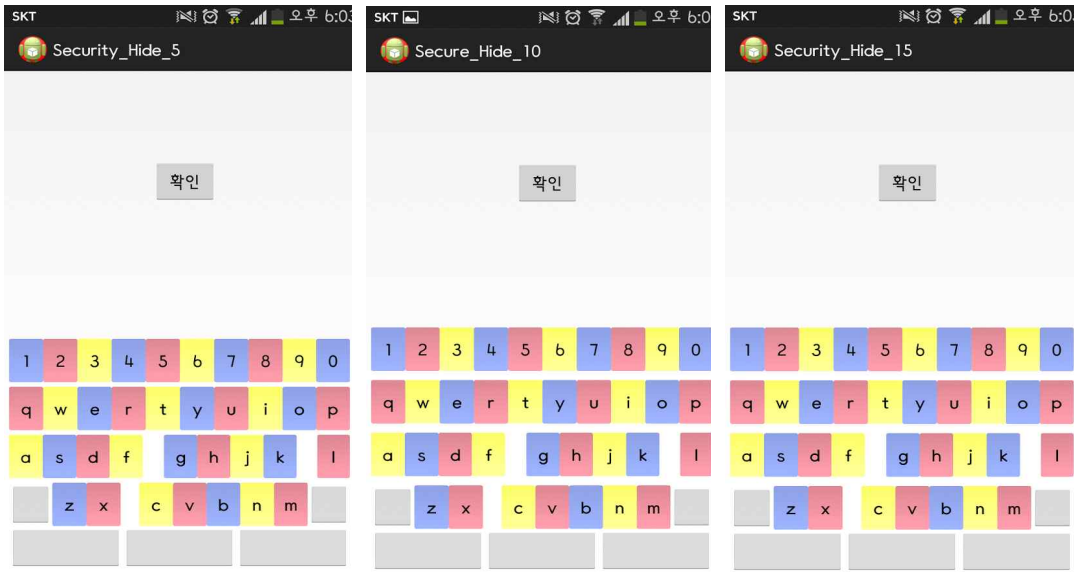
타겟보드	구분	실험자 4 (진동)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	90	100
	속도(sec)	7.5	5.9	8.0	11.2	8.6
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	8.2	5.8	8.8	6.2	8.4

6. 행간의 거리 차에 따른 정확도 고려

본 논문에서 제안하는 알고리즘에서 가장 중점을 둔 사항은 행간의 오차를 어떻게 하면 피드백없이 효율적으로 조정할 수 있는 지이다. 이를 위해 행간 간에 여백을 두는 기법을 사용하였다. 본 장에서는 행간의 거리를 조절하여 오차가 발생하는 비율을 조사해 봄으로써 적합한 행간의 여백을 확인해 보도록 한다. <그림 23>에서와 같이 실험에 사용한 자료는 2mm, 3mm, 그리고 4mm 진동 문자 마스킹 보안 키패드이다.

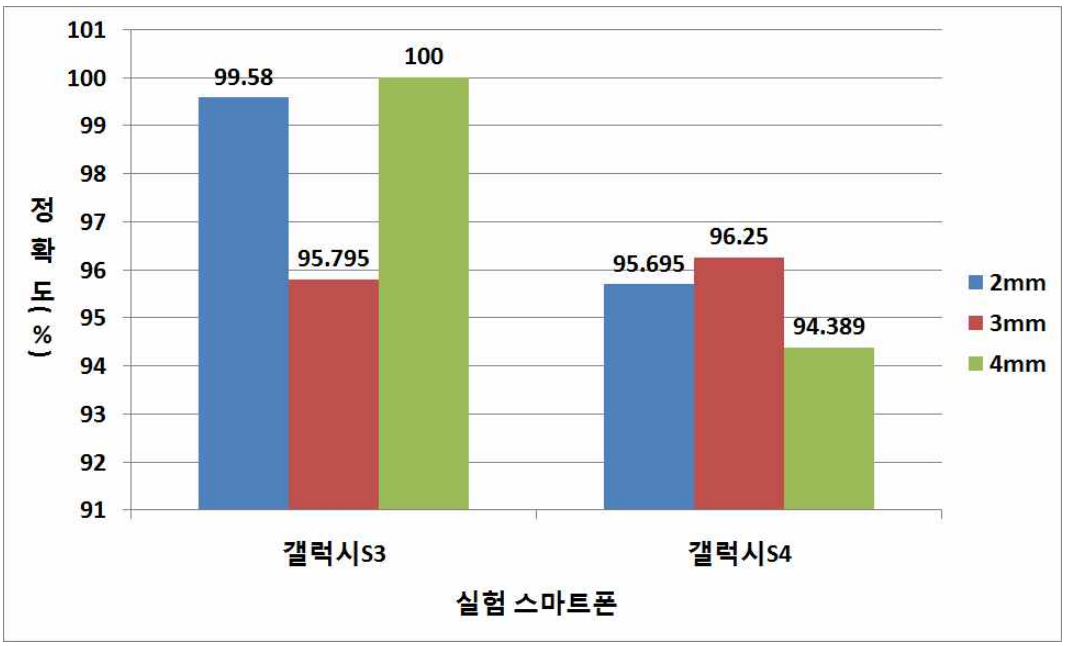
<그림 23> **각기 다른 행간의 거리 차를 이용한 정확도 확인**

(a) 2mm (b) 3mm (c) 4mm



<그림 24>에서는 진동 문자 마스킹 보안 키패드의 정확도가 행간의 폭을 기준으로 나타나 있다. 정확도 면에서는 3가지 보안키패드에서 비슷한 특성이 나타남을 확인할 수 있다. [표 24, 25]에서는 실험자 4명에 대한 정확도 상세 실험 결과가 나타나 있다.

<그림 24> **진동 문자 마스킹 보안 키패드 정확도**



[표 24] **갤럭시 S3상에서의 정확도 실험결과**

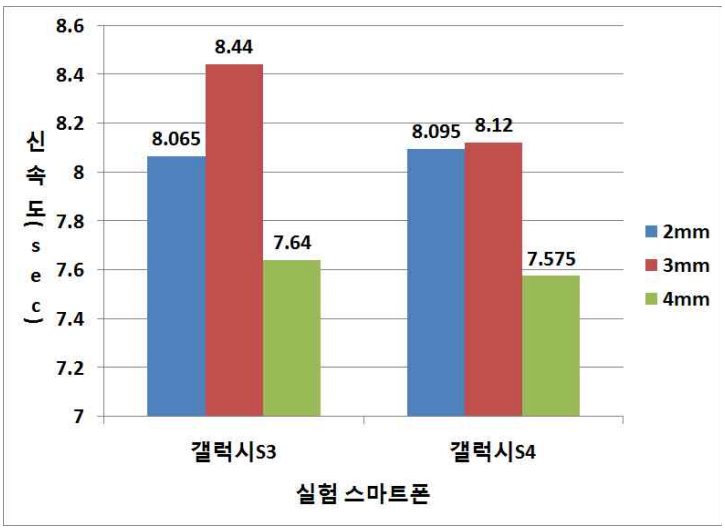
기법	갤럭시S3 정확도 실험 결과(%)			
	실험자1	실험자2	실험자3	실험자4
진동 문자 마스킹 2mm	100	100	98.32	100
진동 문자 마스킹 3mm	85	100	98.18	100
진동 문자 마스킹 4mm	100	100	100	100

[표 25] **갤럭시 S4상에서의 정확도 실험결과**

기법	갤럭시S4 정확도 실험 결과(%)			
	실험자1	실험자2	실험자3	실험자4
진동 문자 마스킹 2mm	85	97.78	100	100
진동 문자 마스킹 3mm	85	100	100	100
진동 문자 마스킹 4mm	100	77.556	100	100

<그림 25>에서는 진동 문자 마스킹 보안 키패드의 신속도가 나타나 있다. 여기서는 확실히 행간의 폭이 넓은 4mm의 경우에 가장 높은 신속도가 나타남을 확인할 수 있다. 그 이유는 오타가 날 확률이 비교적 낮은 심리적 안정 때문에 사용자들이 편하게 키보드 타이핑이 가능한 이유이다. 따라서 4mm 이상의 여백을 두고 행간을 디자인하는 것이 보안과 사용 편의성을 위해 적절하다고 할 수 있다. 자세한 실험 평균값은 [표 26, 27]에 상세히 표기되어 있다.

<그림 25> **진동 문자 마스킹 보안 키패드 신속도**



[표 26] **갤럭시 S3상에서의 신속도 실험결과**

기법	갤럭시S3 신속도 실험 결과(sec)			
	실험자1	실험자2	실험자3	실험자4
진동 문자 마스킹 2mm	6.16	9.56	8.66	7.88
진동 문자 마스킹 3mm	7.34	9.56	8.62	8.24
진동 문자 마스킹 4mm	6.38	8.28	8.22	7.68

[표 27] **갤럭시 S4상에서의 신속도 실험결과**

기법	갤럭시S4 신속도 실험 결과(sec)			
	실험자1	실험자2	실험자3	실험자4
진동 문자 마스킹 2mm	6.8	8.9	8.56	8.12
진동 문자 마스킹 3mm	8.3	7.14	8.5	8.54
진동 문자 마스킹 4mm	7.16	7.5	7.8	7.84

[표 28~38]에서는 진동 문자 마스킹 보안 키패드를 2mm, 3mm 그리고 4mm로 테스트한 결과 정확도와 신속도가 나타나 있다.

[표 28] **실험자1의 진동 문자 마스킹 보안 키패드(2mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 1 (진동마스크 2mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	6.7	6.1	5.8	5.9	6.3
갤럭시 S4	정확도(%)	100	100	25	100	100
	속도(sec)	5.6	8.1	7.7	6.6	6.0

[표 29] **실험자2의 진동 문자 마스킹 보안 키패드(2mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 2 (진동마스크 2mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	8.7	9.2	11.7	10.1	8.1
갤럭시 S4	정확도(%)	100	88.9	100	100	100
	속도(sec)	11.8	6.2	8.5	9.1	8.9

[표 30] **실험자3의 진동 문자 마스킹 보안 키패드(2mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 3 (진동마스크 2mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	91.6	100	100	100
	속도(sec)	9.5	10.2	6.9	9.2	7.5
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	6.5	9.3	8.9	8.4	9.7

[표 31] **실험자4의 진동 문자 마스킹 보안 키패드(2mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 4 (진동마스크 2mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	8.8	9.5	6.7	8.3	6.1
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	7.5	7.4	8.3	8.9	8.5

[표 32] **실험자1의 진동 문자 마스킹 보안 키패드(3mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 1 (진동마스크 3mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	25	100	100	100
	속도(sec)	8.7	7.0	6.3	6.2	8.5
갤럭시 S4	정확도(%)	100	25	100	100	100
	속도(sec)	8.5	6.9	9.1	8.3	8.7

[표 33] **실험자2의 진동 문자 마스킹 보안 키패드(3mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 2 (진동마스크 3mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	8.7	9.2	11.7	10.1	8.1
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	6.9	7.3	6.5	6.6	8.4

[표 34] **실험자3의 진동 문자 마스킹 보안 키패드(3mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 3 (진동마스크 3mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	90.9	100	100	100
	속도(sec)	8.4	7.5	8.2	10.7	8.3
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	8.4	12.9	6.4	8.2	6.6

[표 35] **실험자4의 진동 문자 마스킹 보안 키패드(3mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 4 (진동마스크 3mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	7.0	8.6	10.2	6.9	8.5
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	10.5	8.9	9.8	7.6	5.9

[표 36] **실험자1의 진동 문자 마스킹 보안 키패드(4mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 1 (진동마스크 4mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	7.1	5.9	5.3	8.3	5.3
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	7.3	6.8	6.2	8.4	7.1

[표 37] **실험자2의 진동 문자 마스킹 보안 키패드(4mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 2 (진동마스크 4mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	9.2	10.0	7.1	6.9	8.2
갤럭시 S4	정확도(%)	100	60	77.78	100	50
	속도(sec)	8.3	7.1	5.8	10.2	6.1

[표 38] **실험자3의 진동 문자 마스킹 보안 키패드(4mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 3 (진동마스크 4mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	9.5	9.4	7.3	6.6	8.3
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	6.9	10.7	6.2	8.5	6.7

[표 39] **실험자1의 진동 문자 마스킹 보안 키패드(4mm) 정확도/신속도 테스트**

타겟보드	구분	실험자 4 (진동마스크 4mm)				
		시도1	시도2	시도3	시도4	시도5
갤럭시 S3	정확도(%)	100	100	100	100	100
	속도(sec)	8.3	8.3	7.5	6.7	7.6
갤럭시 S4	정확도(%)	100	100	100	100	100
	속도(sec)	6.2	6.5	11.4	8.1	7.0

V. 결론

기존 스마트폰에서 안전한 금융 서비스를 위해 사용되는 보안 키패드는 오탈자를 확인하기 위한 용도로 사용자에게 입력된 문자의 마지막 정보를 제공한다. 하지만 이러한 피드백은 악의적인 공격자의 어깨너머 공격에 쉽게 노출되는 문제점을 가진다. 이를 보완하기 위해 작년 금융보안공모전에서는 색상을 이용한 보안 키패드가 제안되었다. 하지만 이 또한 공격자의 확률적인 공격에 비밀번호가 노출되는 문제를 가진다. 본 논문에서는 기존의 보안 키패드가 가지는 보안 취약성을 해결하기 위해 진동 정보를 통해 기존의 정보 제공 방식을 효과적으로 대체하는 새로운 개념의 보안 키패드를 제안한다. 기존의 오탈자 확인 정보가 문자 본연의 정보가 화면에 노출되는 방식이었다면 제안하는 방식은 사용자만 알 수 있는 촉감정보를 진동을 통해 전달함으로써 보안성을 제공함과 동시에 입력정확성도 확보할 수 있는 장점을 가진다. 해당 제안은 실제 구현 및 테스트를 통해 성능이 평가되었다. 보안성 측면에서는 어깨너머 공격이 100% 방지되는 안전성을 제공하며 신속성과 정확도 측면에서는 기존의 기법과 유사한 성능을 제시한다.