(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월21일
(11) 등록번호 10-1432936
(24) 등록일자 2014년08월14일

(51) 국제특허분류(Int. Cl.)
G06F 21/30 (2013.01)
(21) 출원번호 10-2013-0054514
(22) 출원일자 2013년05월14일
심사청구일자 2013년05월14일
(56) 선행기술조사문헌
KR1020070109775 A
KR1020080025773 A
KR1020090063903 A

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기 부천시 원미구 계남로 81, 2222동 702호 (상동, 진달래마을)
(74) 대리인
양성보

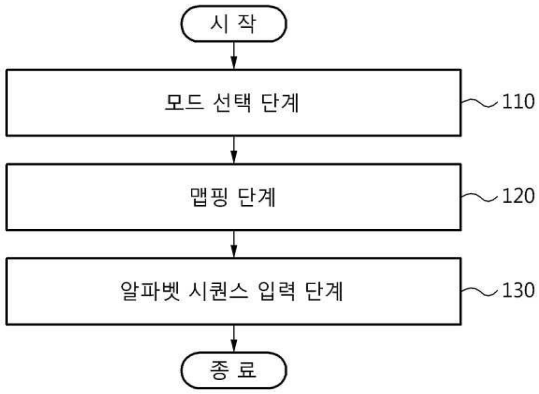
전체 청구항 수 : 총 5 항 심사관 : 문남두

(54) 발명의 명칭 **랜덤 매칭을 이용한 안전한 사용자 인증 방법 및 장치**

(57) 요 약

사용자 인증 시스템에 관한 것으로서, 특히 숄더 서핑 공격을 효과적으로 예방하는 새로운 핀-엔트리 방법을 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 방법 및 장치가 제시된다. 일 실시예에 따르면, 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 방법은 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하고, 핀 숫자에 랜덤으로 알파벳을 맵핑하고, 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력한다. 핀 패드의 형태에 따라 포트레이트 모드 또는 랜드스캐이프 모드를 선택하고, 핀 숫자에 맵핑되는 알파벳의 수에 따른 두 가지 모드를 선택한다. 포트레이트 모드는 핀 숫자에 대응하는 알파벳으로 이루어진 일반적인 핀 패드 4개로 핀 패드가 구성되고, 랜드스캐이프 모드는 핀 숫자에 대응하는 알파벳을 하나의 행으로 배열하고, 이러한 행 4개로 핀 패드가 구성된다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 10039180
부처명 산업통상자원부
연구사업명 산업융합원천기술개발사업
연구과제명 모바일 환경하에서 모바일 인증과 보안 강화를 위해 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI) 기반 Usable Security 원천기술 개발
기 여 율 1/2
주관기관 세종대학교 산학협력단
연구기간 2011.05.01 ~ 2015.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 NIPA-2013-H0301-13-1003 / 1415123340
부처명 미래창조과학부
연구사업명 대학 IT연구센터 지원사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및 연구인력양성
기 여 율 1/2
주관기관 숭실대학교 산학협력단
연구기간 2013.01.01 ~ 2013.12.31

특허청구의 범위

청구항 1

핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하는 단계;

상기 핀 숫자에 랜덤으로 알파벳을 맵핑하는 단계; 및

상기 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력하는 단계

를 포함하는 랜덤 매칭을 이용한 사용자 인증 방법.

청구항 2

제1항에 있어서,

상기 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하는 단계는

핀 패드의 형태에 따라 포트레이트 모드 또는 랜드스캐이프 모드를 선택하고, 상기 핀 숫자에 맵핑되는 알파벳의 수에 따른 두 가지 모드를 선택하는

랜덤 매칭을 이용한 사용자 인증 방법.

청구항 3

제2항에 있어서,

상기 포트레이트 모드는 핀 숫자에 대응하는 알파벳이 다수의 행과 다수의 열로 배열된 핀 패드가 4개로 구성되고,

상기 랜드스캐이프 모드는 핀 숫자에 대응하는 알파벳이 하나의 행으로 배열된 핀 패드가 4개로 구성되는

랜덤 매칭을 이용한 사용자 인증 방법.

청구항 4

핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하는 모드 선택부;

상기 모드 선택부에서 선택된 모드에 따라 상기 핀 숫자에 알파벳을 랜덤으로 맵핑하는 맵핑부;

상기 맵핑부에서 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력 받는 입력부; 및

상기 핀 패드를 나타내는 디스플레이부

를 포함하는 랜덤 매칭을 이용한 사용자 인증 장치.

청구항 5

제4항에 있어서,

상기 모드 선택부는 핀 패드의 형태에 따라 포트레이트 모드 또는 랜드스캐이프 모드를 선택하고, 상기 핀 숫자에 맵핑되는 알파벳의 수에 따른 두 가지 모드를 선택하는

랜덤 매칭을 이용한 사용자 인증 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 숄더 서핑 공격(shoulder surfing attacks, SSA)을 효과적으로 예방하는 새로운 핀-엔트리 방법을 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 방법 및 장치에 관한 것이다. 더욱 상세하게는 사용자가 핀 패드의 모드를 선택함으로써 주어진 핀 숫자와 알파벳을 랜덤 맵핑한다. 사용자는 이러한 핀 숫자와 알파벳의 맵핑을 인식하고 핀 숫자 대신에 맵핑된 알파벳 시퀀스로 암호를 입력하는 랜덤 매칭을 이용한 안전한 사용자 인

증 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 본 발명은 사용자 인증 시스템에 관한 것으로서, 특히 숄더 서핑 공격(shoulder surfing attacks, SSA)을 효과적으로 예방하는 새로운 핀-엔트리 방법을 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 방법 및 장치에 관한 것이다.

[0003] 한국공개특허 10-20040101950 호는 인증정보를 저장하고 있는 이동통신 단말기로 인증 및/또는 결제를 위한 SMS를 전송하여 간단한 절차로 인증이 이루어질 수 있도록 하기 위한 인증정보를 저장하고 있는 이동통신단말기와 SMS를 이용한 유무선 통합 인증 및 결제방법에 관한 기술을 제시한다.

[0004] 컴퓨터와 통신의 발전, 광범위한 전산망의 보급과 함께 메모리와 연산기능을 갖는 집적회로(Integrated Circuit, IC) 카드 기술의 발전으로 다양한 응용 분야가 발생하고 사람들에게는 많은 편리함이 제공되고 있다. IC 카드의 응용분야의 하나인 전자화폐는 전자지갑내의 잔액, 거래내역 등을 조회하는 기능이 필요하다. 또한 사용자는 은행에 직접 가지 않고서 자신의 계좌에 있는 돈을 관리할 수 있으며, 자신의 집에서 컴퓨터를 이용한 원거리 접속으로 자신이 원하는 많은 일을 쉽게 할 수 있다. 이때, 서비스 제공자(은행, 네트워크 서버 등)는 서비스를 원하는 사용자가 정당한 권한이 있는 사용자인지를 확인하는 것이 필수적이다.

[0005] 만일 사용자 인증 시스템의 취약으로 정당한 사용자를 가장한 공격이 성공하게 된다면 개인의 사생활 침해는 물론 정신적, 물질적으로 엄청난 피해를 가져오게 된다. 특히 사용자가 원거리에서 서비스를 원하는 경우에 서비스 제공자는 사용자를 직접 만나지 않는 상황에서 사용자의 신분을 확실하게 확인할 수 있는 방법이 필요하다. 사용자의 신분을 인증하기 위해서는 그 사용자만이 알고 있는 것이나 그 사용자만이 소유하고 있는 것 또는 그 사용자만의 신체적 특징이나 습관 등을 이용할 수 있다. 지금까지 사용자의 신분을 인증하기 위해서 사용되고 있는 가장 기본적이고 일반적인 방법은 패스워드(password)를 이용하는 것이다. 패스워드 방식은 그 사용자만이 알고 있는 것을 확인함으로써 사용자의 신분을 인증하는 것이다. 즉 서비스를 받기를 원하는 사용자는 처음에 자신만이 알고 있는 패스워드를 선택하여 서비스 제공자 서버에 등록을 한다. 사용자는 통상 몇 자리의 숫자나 문자를 패스워드로 사용한다. 신분 인증을 받기를 원하는 사용자는 자신이 기억하고 있는 패스워드를 서버에게 전달하고, 서버는 서비스 초기에 등록된 사용자의 패스워드와 비교해서 사용자를 인증하게 된다.

[0006] 그리고 보다 안전한 사용자 인증을 위해서는 사용자가 신분인증을 받고자 할 때마다 패스워드가 달라지는 일회용 패스워드를 사용하는 것이다. 이것은 사용자가 인증을 받고자 할 때마다 매번 패스워드가 달라지게 되므로 공격자가 한 번 패스워드를 알아냈다고 하더라도 이를 다음에는 다시 사용할 수 없다. 일회용 패스워드를 사용하여 신분 인증을 하기 위해서는 사용자가 일회용 패스워드를 생성할 수 있는 장치가 필요하다. 이때 각 사용자마다 가지고 있는 일회용 패스워드 생성용 단말기를 사용한다면 사용자 인증을 위해서 그 사용자만이 알고 있는 것과 그 사용자만이 소유하고 있는 것을 동시에 확인할 수 있기 때문에 보안 수준을 훨씬 높일 수 있다. 일회용 패스워드는 기존의 패스워드와 달리 매번 다른 패스워드를 생성하기 위하여 매번 달라지는 변수가 필요하며 이를 위해 시각(Real Time Clock, RTC)을 이용하는 방법과 난수를 이용하는 시도/응답 방법(Challenge/Response)이 있다.

[0007] 시각을 변수로 사용한 사용자 인증 방법은 사용자가 소유한 단말기와 서비스 제공자의 서버가 일치 시킨 시간을 사용한다. 즉 사용자가 인증을 받고자 하는 시간에 단말기내의 시간에 의한 일회용 패스워드가 발생되고, 서버도 같은 시간에 패스워드를 발생시켜서 이 값들을 비교하여 사용자 인증을 수행하게 된다.

[0008] 난수를 이용한 시도/응답 방법은 일회용 패스워드를 발생시키기 위하여 난수 발생기를 이용해서 만든 난수값을 이용하게 된다. 사용자 인증을 시작하면 먼저 서버가 난수값을 생성하여 사용자에게 전달한다. 단말기는 서버와 공유하고 있는 비밀값으로 이 난수값을 암호화해서 일회용 패스워드를 생성시켜서 서버에 전송한다. 서버는 단말기와 공유하고 있는 비밀값과 자신이 전송한 난수값을 사용해서 패스워드를 발생시키고 단말기가 발생한 패스워드와 비교해서 사용자를 인증하게 된다.

[0009] 한편, 현재 가장 널리 사용되고 있는 사용자 인증방법인, 패스워드를 이용한 사용자 인증방법은 많은 문제점을 가지고 있다. 패스워드는 대개 몇 자리의 숫자나 문자만을 사용하며 특히 개인의 정보(전화번호, 생일, 주민등록번호 등)를 사용하기 때문에 타인이 쉽게 유추하여 알아낼 수 있다. 사용자는 자신이 선택한 패스워드를 잊어버리지 않기 위해서 패스워드를 어디엔가 기록하게 되는데 이를 통해서 타인에게 노출이 된다. 또한 원거리에서 서비스를 받기를 원하는 사용자가 사용자 인증을 받기 위해서 자신의 패스워드를 전화선이나 전산망을 통

해서 전달하는 경우에는 도청을 통해서 쉽게 노출될 수 있다.

[0010] 핀은 스마트 폰, ATM, 전자 문 잠금 장치와 같은 많은 장치에서 사용하는 사용자 인증 방법으로 잘 알려져 있다. 그러나 종래의 핀-엔트리 방법은 레이아웃이 고정되어 있고, 사용자는 항상 핀에 기반하여 같은 정보를 입력하기 때문에 숄더 서핑 공격(shoulder surfing attacks, SSA)에 상당히 취약하다. 이러한 문제를 해결하기 위해 랜덤 챌린지(challenge)와 보안 핀 숫자로부터 계산된 사용자의 적절한 반응을 포함하는 대응책을 위한 다양한 방법이 제안되었다. 하지만 이러한 대응책은 복잡한 발달 과제를 수행하거나 촉각 정보와 오디오를 인식하기 위한 이차 채널을 필요로 한다. 따라서, 이러한 방법은 인증 시간을 증가시키고, 잘못된 입력의 비율을 놓여서 핀-엔트리 방법의 유용성을 상당히 떨어뜨린다. 그러므로 본 발명에서는 어떠한 이차 채널 없이도 사용할 수 있는 새로운 핀-엔트리 방법을 제안한다.

발명의 내용

해결하려는 과제

[0011] 본 발명이 이루고자 하는 기술적 과제는 사용자가 핀 패드의 모드를 선택함으로써 주어진 핀 숫자와 알파벳을 랜덤 맵핑하고, 사용자는 이러한 핀 숫자와 알파벳의 맵핑을 인식하고 핀 숫자 대신에 맵핑된 알파벳 시퀀스로 암호를 입력함으로써 사용자에게 용이한 인터페이스와 빠른 인증 시간 및 신뢰성을 보장한다. 또한, 실험적 결과를 통해 에러비율도 감소함을 확인 할 수 있다.

과제의 해결 수단

[0012] 일 측면에 있어서, 본 발명에서 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 방법은 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하는 단계와, 핀 숫자에 랜덤으로 알파벳을 맵핑하는 단계와, 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력하는 단계를 포함한다.

[0013] 매칭을 이용한 안전한 사용자 인증 방법에서 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하는 단계는 핀 패드의 형태에 따라 포트레이트 모드 또는 랜드스캐이프 모드를 선택하고, 핀 숫자에 맵핑되는 알파벳의 수에 따른 두 가지 모드를 선택한다.

[0014] 매칭을 이용한 안전한 사용자 인증 방법에서 포트레이트 모드는 핀 숫자에 대응하는 알파벳으로 이루어진 일반적인 핀 패드 4개로 핀 패드가 구성되고, 랜드스캐이프 모드는 핀 숫자에 대응하는 알파벳을 하나의 행으로 배열하고, 이러한 행 4개로 핀 패드가 구성된다.

[0015] 일 측면에 있어서, 본 발명에서 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 장치는 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택하는 모드 선택부와, 모드 선택부에서 선택된 모드에 따라 핀 숫자에 알파벳을 랜덤으로 맵핑하는 맵핑부와, 맵핑부에서 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력 받는 입력부와, 핀 패드를 나타내는 디스플레이부를 포함한다.

[0016] 랜덤 매칭을 이용한 안전한 사용자 인증 장치에서 모드 선택부는 핀 패드의 형태에 따라 포트레이트 모드 또는 랜드스캐이프 모드를 선택하고, 핀 숫자에 맵핑되는 알파벳의 수에 따른 두 가지 모드를 선택한다.

발명의 효과

[0017] 본 발명의 실시예들에 따르면 종래의 숄더 서핑 공격-저항(shoulder surfing attack-resistant) 방법 보다 인증 시간이 감소되고, 에러 비율도 감소시킬 수 있다. 사용자가 핀 패드의 모드를 선택함으로써 주어진 핀 숫자와 알파벳을 랜덤 맵핑하고, 사용자는 이러한 핀 숫자와 알파벳의 맵핑을 인식하고 핀 숫자 대신에 맵핑된 알파벳 시퀀스로 암호를 입력함으로써 사용자에게 용이한 인터페이스와 빠른 인증 시간 및 신뢰성을 보장한다. 또한, 실험적 결과를 통해 에러비율도 감소함을 확인 할 수 있다.

도면의 간단한 설명

[0018] 도 1은 랜덤 매칭을 이용한 안전한 사용자 인증 방법을 설명하기 위한 순서도이다.

도 2는 본 발명의 일 실시예에 따른 핀 패드의 모드를 나타내는 도면이다.

도 3은 본 발명의 일 실시예에 따른 핀 숫자에 맵핑된 알파벳의 모드에 따라 암호에 대응하는 알파벳의 시퀀스를 입력하기 위한 키패드를 나타내는 도면이다.

도 4는 랜덤 매칭을 이용한 안전한 사용자 인증 장치의 구성을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0020] 도 1은 랜덤 매칭을 이용한 안전한 사용자 인증 방법을 설명하기 위한 순서도이다.

[0021] 핀은 스마트 폰, ATM, 전자 문 잠금 장치와 같은 많은 장치에서 사용하는 사용자 인증 방법으로 잘 알려져 있다. 그러나 종래의 핀-엔트리 방법은 레이아웃이 고정되어 있고, 사용자는 항상 핀에 기반하여 같은 정보를 입력하기 때문에 숄더 서핑 공격(shoulder surfing attacks, SSA)에 상당히 취약하다. 이러한 문제를 해결하기 위해 랜덤 챌린지(challenge)와 보안 핀 숫자로부터 계산된 사용자의 적절한 반응을 포함하는 대응책을 위한 다양한 방법이 제안되었다. 이러한 대응책은 복잡한 발달 과제를 수행하거나 촉각 정보와 오디오를 인식하기 위한 이차 채널을 필요로 한다. 따라서, 이러한 방법은 인증 시간을 증가시키고, 잘못된 입력의 비율을 놓여서 핀-엔트리 방법의 유용성을 상당히 떨어뜨린다. 그러므로 본 발명에서는 어떠한 이차 채널 없이도 사용할 수 있는 새로운 핀-엔트리 방법을 제안한다.

[0022] 도 1을 참고하면, 랜덤 매칭을 이용한 안전한 사용자 인증 방법은 모드 선택단계(110), 맵핑단계(120), 알파벳 시퀀스 입력단계(130)를 포함한다.

[0023] 먼저, 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택한다(110). 일 실시예에 따르면, 핀 패드의 모드는 포트레이트 모드(portrait mode)와 랜드스캐이프 모드(landscape mode)의 두 종류가 있으며, 핀 숫자에 맵핑되는 알파벳의 모드는 26개의 알파벳 모드와 10개의 알파벳 모드 두 종류가 있다. 따라서, 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드의 조합으로 4가지의 모드를 구현할 수 있다.

[0024] 포트레이트 모드(portrait mode)는 핀 숫자에 부합하는 알파벳으로 이루어진 4개의 일반적인 핀 패드로 구성된다. 이때, 4개의 일반적인 핀 패드는 암호의 각 핀 숫자를 위한 것이다. 상세히 설명하면, 왼쪽 위 핀 패드는 첫 번째 핀 숫자를 위한 것이고, 오른쪽 위 핀 패드는 두 번째 핀 숫자를 위한 것이다. 그리고 왼쪽 아래 핀 패드는 세 번째 핀 숫자를 위한 것이고, 오른쪽 아래 핀 패드는 마지막 핀 숫자를 위한 것이다.

[0025] 랜드스캐이프 모드(landscape mode)는 핀 패드는 포트레이트 모드(portrait mode)와 다르게 하나의 행으로 배열된다. 그리고, 4개의 핀 숫자를 입력 받기 위해 챌린지 스크린(challenge screen)은 4개의 행으로 구성된다.

[0026] 포트레이트 모드(portrait mode)와 랜드스캐이프 모드(landscape mode)에 대한 설명은 도 2를 참조하여 상세히 설명한다.

[0027] 핀 숫자에 맵핑되는 알파벳의 모드로 26개의 알파벳 모드 사용할 경우, 알파벳 26개 중에서 랜덤으로 10개를 추출하여 사용한다.

[0028] 핀 숫자에 맵핑되는 알파벳의 모드로 10개의 알파벳 모드 사용할 경우, A, B, C, D, E, F, G, H, J, 그리고 K의 10개의 알파벳을 사용한다. 이때, 알파벳 'I' 는 사용자에게 숫자 '1'과 혼동을 가져올 수 있으므로 'I'를 제외한 A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳을 사용한다.

[0029] 다음으로, 핀 숫자에 랜덤으로 알파벳을 맵핑한다(120).

[0030] 사용자는 사용자의 핀 숫자와 알파벳 문자의 랜덤 맵핑을 제공하는 스크린이 주어진다. 모드 선택단계(110)에서 선택된 모드에 따라 핀 숫자에 랜덤으로 알파벳을 맵핑하여 챌린지 스크린(challenge screen)을 구성한다.

[0031] 포트레이트 모드(portrait mode)일 경우, 핀 숫자에 부합하는 알파벳으로 이루어진 4개의 일반적인 핀 패드를 구성하고, 랜드스캐이프 모드(landscape mode)일 경우, 핀 패드는 하나의 행으로 배열된 핀 패드 4개가 챌린지 스크린(challenge screen)을 구성한다.

[0032] 그리고, 26개의 알파벳 모드 사용할 경우, 알파벳 26개 중에서 랜덤으로 10개를 추출하여 맵핑에 사용하고, 10개의 알파벳 모드 사용할 경우, A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳을 사용하여 맵핑한다.

[0033] 그리고, 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력한다(130).

[0034] 맵핑단계(120)에서 맵핑된 핀 숫자와 알파벳을 사용자가 인식한 후, 어떤 스크린 영역을 선택하면, 응답 단계로 넘어가게 된다. 따라서, 사용자는 인식한 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력한다. 이때, 알파벳의 시퀀스를 입력하는 키패드는 모드 선택단계에서 선택한 핀 숫자에 맵핑되는 알파벳의 모드에 따라 두 종류로 이루어질 수 있다.

[0035] 26개의 알파벳 모드를 선택했을 경우, 키패드는 26개의 알파벳으로 이루어진 키패드를 스크린에 나타낸다. 또한, 10개의 알파벳 모드를 선택했을 경우, A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳으로 이루어진 키패드를 스크린에 나타낸다.

[0036]

[0037] 도 2는 본 발명의 일 실시예에 따른 핀 패드의 모드를 나타내는 도면이다.

[0038] 핀 패드의 모드는 포트레이트 모드(portrait mode)와 랜드스캐이프 모드(landscape mode)의 두종류가 있으며, 도 2a는 포트레이트 모드(portrait mode)를 나타내고, 도 2b는 랜드스캐이프 모드(landscape mode)를 나타낸다. 또한, 핀 숫자에 맵핑되는 알파벳의 모드는 26개의 알파벳 모드와 10개의 알파벳 모드 두 종류가 있다. 따라서, 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드의 조합으로 4가지의 모드를 구현할 수 있다.

[0039] 포트레이트 모드(portrait mode)는 핀 숫자에 부합하는 알파벳으로 이루어진 4개의 일반적인 핀 패드(210a, 220a, 230a, 240a)로 구성된다. 이때, 4개의 일반적인 핀 패드(210a, 220a, 230a, 240a)는 암호의 각 핀 숫자를 위한 것이다. 상세히 설명하면, 왼쪽 위 핀 패드는 첫 번째 핀 숫자를 위한 것이고, 오른쪽 위 핀 패드는 두 번째 핀 숫자를 위한 것이다. 그리고 왼쪽 아래 핀 패드는 세 번째 핀 숫자를 위한 것이고, 오른쪽 아래 핀 패드는 마지막 핀 숫자를 위한 것이다.

[0040] 이 때, 사용자는 핀 숫자에 맵핑된 알파벳을 인식하고, 암호를 입력할 때 핀 숫자에 대응하는 알파벳 문자를 기억하였다가 이에 해당하는 알파벳 문자를 입력한다. 도 2a를 참조하여 예를 들면, 암호의 핀 숫자가 3146이라고 가정하자. 그러면, 매칭된 알파벳 시퀀스는 KJBA 이다. 따라서, 암호의 핀 숫자 대신 KJBA를 입력하면 된다. 이때, 핀 숫자와 문자 사이의 연관은 각 인증 세션에 대해 랜덤이다.

[0041] 랜드스캐이프 모드(landscape mode)는 핀 패드는 포트레이트 모드(portrait mode)와 다르게 하나의 행으로 배열된다. 그리고, 4개의 핀 숫자를 입력 받기 위해 챌린지 스크린(challenge screen)은 이러한 하나의 생들이 모여 4개의 행(210b, 220b, 230b, 240b)으로 구성된다.

[0042] 이때, 포트레이트 모드(portrait mode)와 같이 사용자는 핀 숫자에 맵핑된 알파벳을 인식하고, 암호를 입력할 때 핀 숫자에 대응하는 알파벳 문자를 기억하였다가 이에 해당하는 알파벳 문자를 입력한다. 도 2b를 참조하여 예를 들면, 암호의 핀 숫자가 3146이라고 가정하자. 그러면, 매칭된 알파벳 시퀀스는 UJKE 이다. 따라서, 암호의 핀 숫자 대신 UJKE 를 입력하면 된다.

[0043] 또한, 핀 숫자에 맵핑되는 알파벳의 모드는 26개의 알파벳 모드와 10개의 알파벳 모드 두 종류가 있다. 26개의 알파벳 모드 사용할 경우, 알파벳 26개 중에서 랜덤으로 10개를 추출하여 맵핑에 사용하고, 10개의 알파벳 모드 사용할 경우, A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳을 사용하여 맵핑한다.

[0044] 도 3은 본 발명의 일 실시예에 따른 핀 숫자에 맵핑된 알파벳의 모드에 따라 암호에 대응하는 알파벳의 시퀀스를 입력하기 위한 키패드를 나타내는 도면이다.

[0045] 맵핑된 핀 숫자와 알파벳을 사용자가 인식한 후, 어떤 스크린 영역을 선택하면, 응답 단계로 넘어가게 된다. 따라서, 사용자는 인식한 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력한다. 이때, 알파벳의 시퀀스를 입력하는 키패드는 모드 선택 시, 선택된 핀 숫자에 맵핑되는 알파벳의 모드에 따라 두 종류로 이루어질 수 있다.

[0046] 도 3a를 참조하면, 10개의 알파벳 모드를 선택했을 경우, A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳으로 이루어진 키패드를 스크린에 나타낸다. 이때, 알파벳 'I' 는 사용자에게 숫자 '1'과 혼동을 가져올 수 있으므로 'I'를 제외한 A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳을 사용한다.

[0047] 도 3b를 참조하면, 핀 숫자에 맵핑되는 알파벳의 모드로 26개의 알파벳 모드를 선택했을 경우, 키패드는 26개의 알파벳으로 이루어진 키패드를 스크린에 나타낸다. 이때, 핀 숫자에 맵핑되는 알파벳은 알파벳 26개 중에서 랜

덤으로 10개를 추출하여 맵핑하고, 사용자는 26개의 알파벳으로 이루어진 키패드에서 암호에 대응하는 알파벳의 시퀀스를 입력한다.

[0048] 도 4는 랜덤 매칭을 이용한 안전한 사용자 인증 장치(400)의 구성을 나타내는 도면이다.

[0049] 랜덤 매칭을 이용한 안전한 사용자 인증 장치(400)는 모드 선택부(410), 맵핑부(420), 입력부(430), 디스플레이부(440)로 구성된다.

[0050] 모드 선택부(410)는 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드를 선택한다.

[0051] 일 실시예에 따르면, 핀 패드의 모드는 포트레이트 모드(portrait mode)와 랜드스캐이프 모드(landscape mode)의 두 종류가 있으며, 핀 숫자에 맵핑되는 알파벳의 모드는 26개의 알파벳 모드와 10개의 알파벳 모드 두 종류가 있다. 따라서, 핀 패드의 모드 및 핀 숫자에 맵핑되는 알파벳의 모드의 조합으로 4가지의 모드를 구현할 수 있다.

[0052] 포트레이트 모드(portrait mode)는 핀 숫자에 부합하는 알파벳으로 이루어진 4개의 일반적인 핀 패드로 구성된다. 이때, 4개의 일반적인 핀 패드는 암호의 각 핀 숫자를 위한 것이다. 상세히 설명하면, 왼쪽 위 핀 패드는 첫 번째 핀 숫자를 위한 것이고, 오른쪽 위 핀 패드는 두 번째 핀 숫자를 위한 것이다. 그리고 왼쪽 아래 핀 패드는 세 번째 핀 숫자를 위한 것이고, 오른쪽 아래 핀 패드는 마지막 핀 숫자를 위한 것이다.

[0053] 랜드스캐이프 모드(landscape mode)는 핀 패드는 포트레이트 모드(portrait mode)와 다르게 하나의 행으로 배열된다. 그리고, 4개의 핀 숫자를 입력 받기 위해 챌린지 스크린(challenge screen)은 4개의 행으로 구성된다.

[0054] 핀 숫자에 맵핑되는 알파벳의 모드로 26개의 알파벳 모드 사용할 경우, 알파벳 26개 중에서 랜덤으로 10개를 추출하여 사용한다.

[0055] 핀 숫자에 맵핑되는 알파벳의 모드로 10개의 알파벳 모드 사용할 경우, A, B, C, D, E, F, G, H, J, 그리고 K의 10개의 알파벳을 사용한다.

[0056] 맵핑부(420)는 모드 선택부(410)에서 선택된 모드에 따라 핀 숫자에 알파벳을 랜덤으로 맵핑한다.

[0057] 포트레이트 모드(portrait mode)와 랜드스캐이프 모드(landscape mode)의 두 가지 핀 패드의 모드 중 하나를 선택하고, 이에 핀 숫자에 맵핑되는 알파벳의 모드로 26개의 알파벳 모드 또는 10개의 알파벳 모드 중 하나를 선택하여 랜덤으로 맵핑한다.

[0058] 입력부(430)는 맵핑부(420)에서 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력 받는다.

[0059] 맵핑부(420)에서 맵핑된 핀 숫자와 알파벳을 사용자가 인식한 후, 어떤 스크린 영역을 선택하면, 응답 단계로 넘어가게 된다. 따라서, 사용자는 인식한 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력한다. 이때, 알파벳의 시퀀스를 입력하는 키패드는 모드 선택 시, 선택된 핀 숫자에 맵핑되는 알파벳의 모드에 따라 두 종류로 이루어질 수 있다.

[0060] 10개의 알파벳 모드를 선택했을 경우, A, B, C, D, E, F, G, H, J, 그리고 K 의 10개의 알파벳으로 이루어진 키패드를 스크린에 나타내고, 26개의 알파벳 모드를 선택했을 경우, 키패드는 26개의 알파벳으로 이루어진 키패드를 스크린에 나타낸다.

[0061] 디스플레이부(440)는 핀 패드 및 알파벳의 시퀀스를 입력 받는 키보드를 표시한다.

[0062] 디스플레이부(440)에는 핀 숫자와 알파벳 문자의 랜덤 맵핑을 제공하는 스크린이 주어진다. 모드 선택단계에서 선택된 모드에 따라 핀 숫자에 랜덤으로 알파벳을 맵핑하여 챌린지 스크린(challenge screen)을 구성하고, 이러한 스크린을 디스플레이에 표시한다.

[0063] 또한, 핀 숫자에 랜덤으로 맵핑된 알파벳 중 암호에 대응하는 알파벳의 시퀀스를 입력하기 위한 키패드를 표시한다.

[0064] 본 발명에서는 숄더 서핑 공격(shoulder surfing attacks, SSA)을 효과적으로 예방하는 새로운 핀-엔트리(PIN-entry) 방법을 제안하였다. 제안된 랜덤 매칭을 이용한 안전한 사용자 인증 방법은 사용자가 모드를 선택함으

로써 주어진 핀 숫자와 알파벳 사이에 랜덤 맵핑을 수행할 수 있다. 사용자는 이렇게 맵핑된 핀 숫자와 알파벳을 인식하고, 핀 숫자 대신 맵핑된 알파벳 시퀀스로 암호를 입력할 수 있다. 따라서, 제안하는 랜덤 매칭을 이용한 안전한 사용자 인증 방법은 사용자에게 용이한 인터페이스를 제공하고 쉽게 사용할 수 있는 장점이 있다. 또한, 인증 시간의 단축과 신뢰성을 보장하는 새로운 방법으로써 파일롯 테스트(pilot test)를 통해 확인할 수 있다. 실험 결과에 따르면, 표1과 같이 평균 인증 시간은 5.8~6.8초이고, 평균 에러비율은 3.3%~6.7% 로 보여진다.

[0065] <표 1>

Method		Stage 1 (sec)	Stage 2 (sec)	Total time (sec)	Error rate (%)
Existing	Regular	-	-	approx. 3	approx. 0
	Binary [1]	-	-	23.2	9.0
	Undercover [2]	-	-	32-45	>31.5
	VibraPass [3]	-	-	8.2	>14.8
	Haptic Wheel [4]	-	-	23.0	16.4
	ColorPIN [5]	-	-	13.3-13.9	N.A.
	Phone Lock [6]*	-	-	12.2	4.8(+6.9)
	SpinLock [7]*	-	-	10.8-16.9	3.3(+64.0)
Pro-posed**	L/26	3.8	3.0	6.8	6.7
	L/10	3.2	3.2	6.4	3.3
	P/26	3.6	3.1	6.7	3.3
	P/10	2.9	2.9	5.8	6.7

[0066]

[0067] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0068] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0069] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판

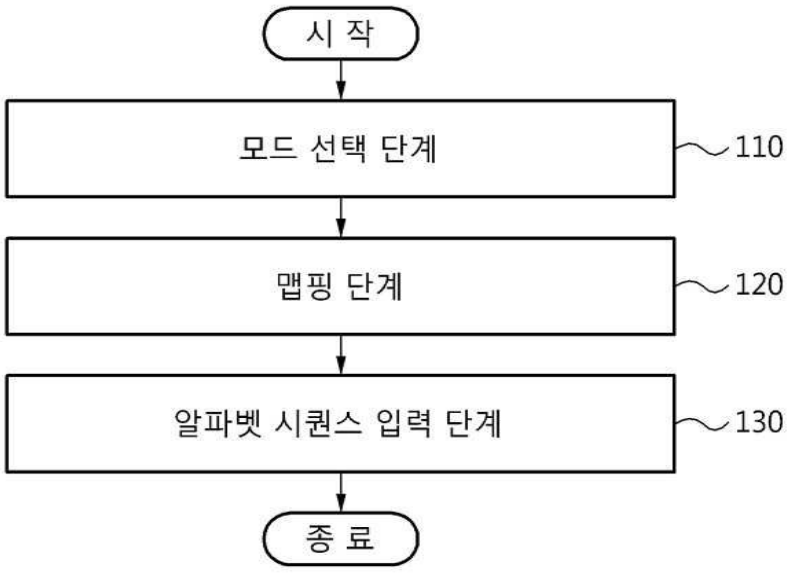
독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0070] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

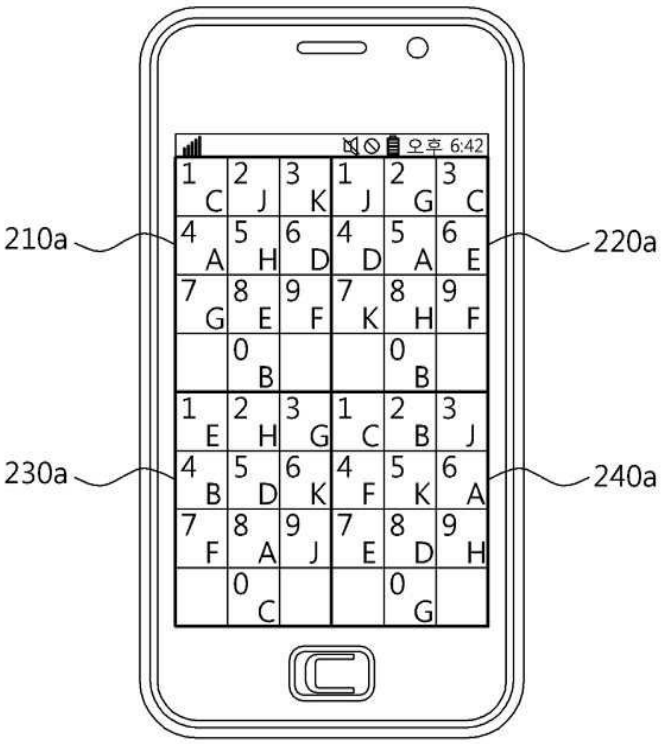
[0071] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

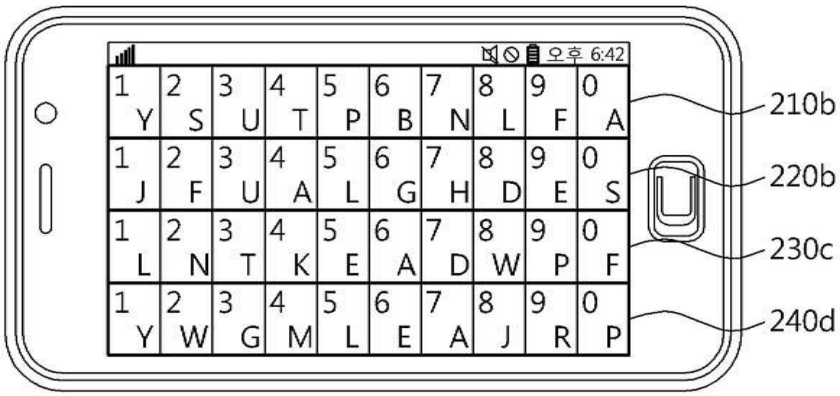
도면1



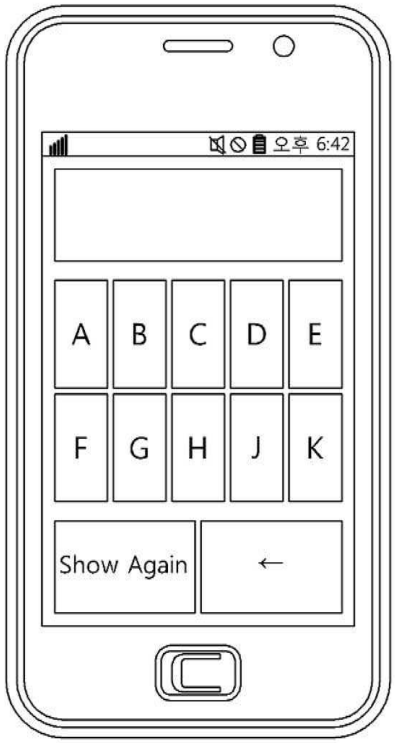
도면2a



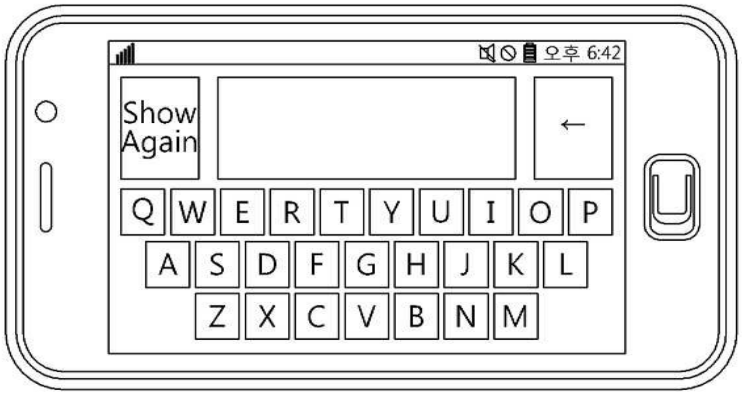
도면2b



도면3a


오후 6:42
A
B
C
D
E
F
G
H
J
K
Show Again
←

도면3b


오후 6:42
Show Again
←
Q
W
E
R
T
Y
U
I
O
P
A
S
D
F
G
H
J
K
L
Z
X
C
V
B
N
M

도면4