(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0006980
(43) 공개일자 2015년01월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/31 (2013.01) *G06F 21/45* (2013.01)
(21) 출원번호 10-2013-0080674
(22) 출원일자 2013년07월10일
심사청구일자 2013년07월10일

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
권태경
서울 광진구 능동로 209, 율곡관 403B호 (군자동, 세종대학교)
박상호
서울 광진구 능동로 209, 율곡관 403B호 (군자동, 세종대학교)
(74) 대리인
특허법인엠에이피에스

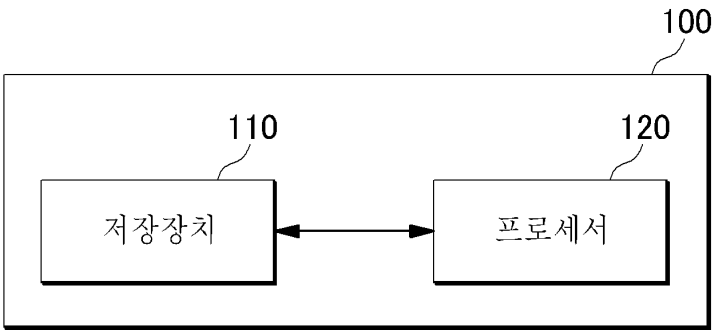
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 **랜덤 패턴을 이용한 사용자 인증 처리 장치 및 방법**

(57) 요 약

본 발명에 따른 사용자 인증 처리 장치는 사용자 인증 애플리케이션이 저장된 저장장치 및 사용자 인증 애플리케이션을 실행하는 프로세서를 포함하되, 상기 저장장치는 사용자에 의해 설정된 복수의 점을 연결한 암호 인증 패턴을 저장하고, 상기 프로세서는 상기 사용자 인증 애플리케이션의 실행 시에, 사용자의 인증 패턴 입력에 따른 인증 처리를 수행하고, 사용자의 인증 패턴 입력 이후에 상기 암호 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴을 생성하여, 사용자의 상기 랜덤 인증 패턴 입력을 유도한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 1415121995
부처명 산업통상자원부
연구관리전문기관 한국산업기술평가관리원
연구사업명 산업원천기술개발사업
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 2013.03.01 ~ 2014.02.28이 발명을 지원한 국가연구개발사업
과제고유번호 1415128814
부처명 미래창조과학부
연구관리전문기관 정보통신산업진흥원
연구사업명 정보통신기술인력양성
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성 연구
기 여 율 1/2
주관기관 숭실대학교산학협력단
연구기간 2013.01.01 ~ 2013.12.31

특허청구의 범위

청구항 1

사용자 인증 처리 장치에 있어서,

사용자 인증 애플리케이션이 저장된 저장장치 및

사용자 인증 애플리케이션을 실행하는 프로세서를 포함하되,

상기 저장장치는 사용자에 의해 설정된 복수의 점을 연결한 암호 인증 패턴을 저장하고,

상기 프로세서는 상기 사용자 인증 애플리케이션의 실행 시에, 사용자의 인증 패턴 입력에 따른 인증 처리를 수행하고, 사용자의 인증 패턴 입력 이후에 상기 암호 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴을 생성하여, 사용자의 상기 랜덤 인증 패턴 입력을 유도하는 사용자 인증 처리 장치.

청구항 2

제 1 항에 있어서,

상기 프로세서는 상기 암호 인증 패턴을 구성하는 복수의 점 중 적어도 절반 이상의 점을 포함하는 랜덤 인증 패턴을 생성하되, 상기 랜덤 인증 패턴을 구성하는 하나 이상의 점은 상기 암호 인증 패턴에 포함되지 않는 것인 사용자 인증 처리 장치.

청구항 3

제 1 항에 있어서,

상기 프로세서는 상기 암호 인증 패턴을 구성하는 점의 개수와 동일한 개수의 점으로 구성된 랜덤 인증 패턴을 생성하는 사용자 인증 처리 장치.

청구항 4

제 1 항에 있어서,

상기 프로세서는 상기 랜덤 인증 패턴을 구성하는 점의 연결 순서를 랜덤하게 설정하여 생성하되, 상기 암호 인증 패턴을 구성하는 점의 연결 순서와 상이하게 설정하는 사용자 인증 처리 장치.

청구항 5

제 1 항에 있어서,

상기 프로세서는 사용자에 의해 입력된 인증 패턴 및 상기 암호 인증 패턴이 일치하면 인증을 승인하는 사용자 인증 처리 장치.

청구항 6

제 5 항에 있어서,

상기 프로세서는 상기 랜덤 인증 패턴을 따라 사용자에 의해 입력된 인증 패턴이 상기 랜덤 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유할 경우 인증을 승인하는 사용자 인증 처리 장치.

청구항 7

제 5 항에 있어서,

상기 프로세서는 상기 랜덤 인증 패턴을 구성하는 점 및 상기 랜덤 인증 패턴을 따라 사용자에 의해 입력된 인증 패턴을 구성하는 점이 일치하면 인증을 승인하는 사용자 인증 처리 장치.

청구항 8

제 7 항에 있어서,

상기 프로세서는 상기 랜덤 인증 패턴을 구성하는 점의 연결 순서 및 상기 인증 패턴을 구성하는 점의 연결 순서가 일치하면 인증을 승인하는 사용자 인증 처리 장치.

청구항 9

사용자 인증 처리 장치를 통한 사용자 인증 처리 방법에 있어서,

사용자의 인증 패턴 입력에 따른 인증 처리를 수행하는 단계 및

사용자의 인증 패턴 입력 이후에, 사용자에 의해 기설정된 암호 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴을 생성하여, 사용자의 상기 랜덤 인증 패턴 입력을 유도하는 단계를 포함하는 사용자 인증 처리 방법.

청구항 10

제 9 항에 있어서,

상기 랜덤 인증 패턴 입력을 유도하는 단계는 상기 암호 인증 패턴을 구성하는 복수의 점 중 적어도 절반 이상의 점을 포함하는 랜덤 인증 패턴을 생성하되, 상기 랜덤 인증 패턴을 구성하는 하나 이상의 점은 상기 암호 인증 패턴에 포함되지 않는 것인 사용자 인증 처리 방법.

청구항 11

제 9 항에 있어서,

상기 랜덤 인증 패턴 입력을 유도하는 단계는 상기 암호 인증 패턴을 구성하는 점의 개수와 동일한 개수의 점으로 구성된 랜덤 인증 패턴을 생성하는 사용자 인증 처리 방법.

청구항 12

제 9 항에 있어서,

상기 랜덤 인증 패턴 입력을 유도하는 단계는 상기 랜덤 인증 패턴을 구성하는 점의 연결 순서를 랜덤하게 설정하여 생성하되, 상기 암호 인증 패턴을 구성하는 점의 연결 순서와 상이하게 설정하는 사용자 인증 처리 방법.

청구항 13

제 9 항에 있어서,

상기 인증 처리를 수행하는 단계는 사용자에 의해 입력된 인증 패턴 및 상기 암호 인증 패턴이 일치하면 인증을 승인하는 사용자 인증 처리 방법.

청구항 14

제 9 항에 있어서,

상기 랜덤 인증 패턴을 따라 사용자에 의해 입력된 인증 패턴에 따른 보조 인증 처리를 수행하는 단계를 더 포함하는 사용자 인증 처리 방법.

청구항 15

제 14 항에 있어서,

상기 보조 인증 처리를 수행하는 단계는 상기 랜덤 인증 패턴을 구성하는 점 중 일정 개수의 점을 경유하는 인증 패턴이 입력되면 인증을 승인하는 사용자 인증 처리 방법.

청구항 16

제 14 항에 있어서,

상기 보조 인증 처리를 수행하는 단계는 상기 랜덤 인증 패턴을 구성하는 점 및 상기 인증 패턴을 구성하는 점

이 일치하면 인증을 승인하는 사용자 인증 처리 방법.

청구항 17

제 16 항에 있어서,

상기 보조 인증 처리를 수행하는 단계는 상기 랜덤 인증 패턴을 구성하는 점의 연결 순서 및 상기 인증 패턴을 구성하는 점의 연결 순서가 일치하면 인증을 승인하는 사용자 인증 처리 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 랜덤 패턴을 이용한 사용자 인증 처리 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 모바일 환경이 급속도로 고도화 및 보편화되고 있다. 모바일 환경이란 노트북, 휴대폰, 스마트폰, 태블릿 PC 등의 모바일 기기가 관련된 하드웨어나 소프트웨어, 네트워크 및 서비스 환경을 의미한다. 모바일 환경에서는 고정형 기기의 기능을 장소 및 시간의 구애 없이 사용할 수 있는 장점이 있다.

[0003] 그러나 개인적인 장소뿐만 아니라 공공장소에서 사용이 가능함에 따라, 사용자 인증을 처리하는 과정에서 숄더 서핑 공격(Shoulder Surfing Attack) 및 스머지 공격(Smudge Attack)에 의한 비밀번호 및 입력 패턴 등이 유출될 가능성이 매우 높은 단점이 있다. 특히, 스머지 공격의 경우, 사용자만이 알고 있어야 할 패턴이 디스플레이에 남은 지문 자국을 통해 타인에게 노출될 수 있어 이에 대비할 수 있는 연구의 개발이 필요한 실정이다.

[0004] 한편, 이와 관련하여 한국 공개특허공보 제2013-0006986호(발명의 명칭: 휴대 단말기 및 그 제어 방법)은 실제 터치스크린의 화면 잠금 해제를 위한 터치제스처 패턴과 상기 화면 잠금 해제와는 무관한 터치제스처 패턴이 조합된 형태의 터치제스처 패턴을 이용하여 상기 화면 잠금을 해제할 수 있는 휴대 단말기 및 그 제어 방법을 제안하고 있다.

[0005] 하지만 화면 잠금 해제와 무관한 터치제스처 패턴은 오히려 화면 잠금 해제를 위한 터치제스처 패턴과 구분될 수 있기 때문에 본래의 화면 잠금 해제용 터치제스처 패턴이 유출될 수 있는 문제점이 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 사용자 인증을 위한 패턴 입력 시에 스머지 공격으로부터 안전한 패턴을 생성하는 사용자 인증 장치 및 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0007] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 사용자 인증 처리 장치는 사용자 인증 애플리케이션이 저장된 저장장치 및 사용자 인증 애플리케이션을 실행하는 프로세서를 포함하되, 상기 저장장치는 사용자에 의해 설정된 복수의 점을 연결한 암호 인증 패턴을 저장하고, 상기 프로세서는 상기 사용자 인증 애플리케이션의 실행 시에, 사용자의 인증 패턴 입력에 따른 인증 처리를 수행하고, 사용자의 인증 패턴 입력 이후에 상기 암호 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴을 생성하여, 사용자의 상기 랜덤 인증 패턴 입력을 유도한다.

[0008] 또한, 본 발명의 제 2 측면에 따른 사용자 인증 처리 장치를 통한 사용자 인증 처리 방법은 사용자의 인증 패턴 입력에 따른 인증 처리를 수행하는 단계 및 사용자의 인증 패턴 입력 이후에, 사용자에 의해 기설정된 암호 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴을 생성하여, 사용자의 상기 랜덤 인증 패턴 입력을 유도하는 단계를 포함한다.

발명의 효과

[0009] 전술한 본 발명의 과제 해결 수단에 의하면, 사용자는 암호 인증 패턴 입력시 발생된 지문 자국과 랜덤 인증 패

턴 입력시 발생된 지문 자국이 일부 중복되도록 함으로써, 지문 자국에 의해 암호 인증 패턴이 노출되는 것을 방지할 수 있다.

도면의 간단한 설명

[0010] 도 1은 본 발명의 일 실시예에 따른 사용자 인증 처리 장치의 구성을 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 암호 인증 패턴 및 랜덤 인증 패턴의 일례를 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 랜덤 인증 패턴 입력을 위한 가이드의 일례이다.

도 4는 본 발명의 일 실시예에 따른 암호 인증 패턴 및 랜덤 인증 패턴이 입력된 화면의 일례를 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 사용자 인증 처리 장치를 통한 사용자 인증 방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0012] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0013] 도 1은 본 발명의 일 실시예에 따른 사용자 인증 처리 장치의 구성을 설명하기 위한 도면이다.

[0014] 이때, 본 발명의 일 실시예에서는, 사용자 인증 처리 장치(100)가 모바일 기기(예를 들어, 스마트폰)인 것을 예로서 설명하도록 한다.

[0015] 참고로, 도 1에서는 본 발명의 일 실시예에 따른 사용자 인증 처리 장치(100)의 구성들을 도시하였으나, 장치의 종류에 따라 이외에도 다른 처리부(미도시)들이 더 포함될 수 있다.

[0016] 또한, 본 발명의 일 실시예에 따른 사용자 인증 처리 장치(100)는 모바일 기기에 한정되는 것이 아닌 다양한 종류의 기기일 수 있으며, 각 기기의 종류 및 목적에 따라 상이한 처리부들을 더 포함할 수 있다.

[0017] 또한, 사용자 인증 처리 장치(100)는 컴퓨터나 휴대용 단말기로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, 스마트폰(Smart phone), 태블릿 PC(Tablet PC), PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.

[0018] 본 발명의 일 실시예에 따른 사용자 인증 처리 장치(100)는 저장장치(110) 및 프로세서(120)를 포함한다.

[0019] 저장장치(110)는 사용자 인증 애플리케이션이 저장된다. 또한, 저장장치(110)는 사용자에 의해 설정된 복수의 점을 연결한 암호 인증 패턴을 저장한다. 암호 인증 패턴은 사용자 인증을 위한 비밀 암호로서, 복수의 점을 연결하여 생성될 수 있는데, 도 2를 참고하여 구체적으로 설명한다. 도 2는 본 발명의 일 실시예에 따른 암호 인증 패턴 및 랜덤 인증 패턴의 일례를 설명하기 위한 도면이다. 이때, 저장장치(110)는 DRAM, SRAM과 같은 휘발성 메모리 또는 플래쉬 메모리, SSD, HDD와 같은 비휘발성 메모리 등 다양한 형태일 수 있다.

[0020] 도 2의 (a)에 도시된 바와 같이, 암호 인증 패턴(200)은 9개의 점 중 5개의 점(P1, P2, P4, P5, P6)이 연결된 형태일 수 있다. 이때, 점의 연결 순서는 2번 점(P2)에서 출발하여 6번 점(P6)까지 차례로 연결되는 구성인 'P2→P1→P4→P5→P6'의 순서가 될 수 있다. 이와 같이, 사용자에 의해 생성된 5개의 점(P1, P2, P4, P5, P

6)이 연결된 암호 인증 패턴(200)은 저장장치(110)에 저장되고, 차후 사용자 인증을 위한 용도로 사용될 수 있다.

[0021] 한편, 프로세서(120)는 사용자 인증 처리 장치(100)의 구동을 위한 각종 제어 동작을 수행할 수 있다.

[0022] 다시 도 1을 참조하면, 프로세서(120)는 사용자 인증 애플리케이션을 실행한다. 또한, 프로세서(120)는 사용자 인증 애플리케이션의 실행 시에, 사용자의 인증 패턴 입력에 따른 인증 처리를 수행하고, 사용자의 인증 패턴 입력 이후에 암호 인증 패턴(200)을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴(300)을 생성하여, 사용자의 랜덤 인증 패턴(300) 입력을 유도한다.

[0023] 먼저, 프로세서(120)는 사용자 인증을 위하여 입력받은 인증 패턴과 사용자에 의해 기설정된 암호 인증 패턴(200)의 일치 여부에 따라 인증 처리를 수행한 후에, 임의의 패턴(즉, 랜덤 인증 패턴(300))을 생성하고 입력을 유도하여, 사용자로 하여금 암호 인증 패턴(200)의 자국과 혼동될 수 있는 임의의 자국을 남길 수 있도록 할 수 있다. 여기서, 자국은 스머지 공격(Smudge Attack)에 이용되는 디스플레이 표면에 남은 지문의 흔적을 지칭한다. 이를 통해, 사용자는 암호 인증 패턴(200)에 따른 자국과 랜덤 인증 패턴(300)에 따른 고의적인 자국을 혼합시킨 자국을 사용자 인증 처리 장치(100)에 남김으로써 암호 인증 패턴(200)이 노출되는 것을 방지할 수 있다. 이때, 랜덤 인증 패턴(300)은 프로세서(120)에 의해 임의의 점으로 구성된 패턴일 수 있다. 랜덤 인증 패턴(300)의 일례는 다음의 프로세서(120)의 설명과 함께 도 2를 참고하여 구체적으로 설명한다.

[0024] 프로세서(120)는 암호 인증 패턴(200)을 구성하는 복수의 점 중 적어도 절반 이상의 점을 포함하는 랜덤 인증 패턴(300)을 생성할 수 있다. 이때, 랜덤 인증 패턴(300)을 구성하는 하나 이상의 점은 암호 인증 패턴(200)에 포함되지 않는 것일 수 있다. 예를 들면, 암호 인증 패턴(200)이 6개의 점으로 구성되었을 경우, 프로세서(120)는 6개의 절반인 3개 이상의 점을 포함하여 랜덤 인증 패턴(300)을 생성할 수 있다. 만일, 암호 인증 패턴(200)이 7개인 경우에는, 프로세서(120)는 7개의 절반인 3.5개 이상(즉, 4개 이상)의 점을 포함하여 랜덤 인증 패턴(300)을 생성할 수 있다. 도 2를 참고하면, 도 2의 (a)와 같이 암호 인증 패턴(200)이 5개의 점(P1, P2, P4, P5, P6)으로 구성되었을 경우, 랜덤 인증 패턴(300)은 5개의 절반인 2.5개 이상(즉, 3개 이상)의 점을 경유하도록 생성될 수 있다. 즉, 도 2의 (b)에 도시된 바와 같이, 랜덤 인증 패턴(300)은 암호 인증 패턴(200)에 포함된 3개의 점(P2, P4, P5)을 경유하도록 생성될 수 있다.

[0025] 또한, 프로세서(120)는 암호 인증 패턴(200)을 구성하는 점의 개수와 동일한 개수의 점으로 구성된 랜덤 인증 패턴(300)을 생성할 수 있다. 예를 들면, 암호 인증 패턴(200)이 5개의 점으로 구성되었을 경우, 랜덤 인증 패턴(300) 또한 5개의 점으로 구성될 수 있다. 도 2를 참고하면, 도 2의 (a)와 같이 암호 인증 패턴(200)이 5개의 점(P1, P2, P4, P5, P6)으로 구성되었을 경우, 랜덤 인증 패턴(300) 또한 5개의 점(P2, P3, P4, P5, P8)으로 구성되어 생성될 수 있다.

[0026] 또한, 프로세서(120)는 랜덤 인증 패턴(300)을 구성하는 점의 연결 순서를 랜덤하게 설정하여 생성하되, 암호 인증 패턴(200)을 구성하는 점의 연결 순서와 상이하게 설정할 수 있다. 즉, 랜덤 인증 패턴(300) 생성시, 랜덤 인증 패턴(300)의 점의 연결 순서를 암호 인증 패턴(200)의 점의 연결 순서와 다르게 설정하여, 디스플레이에 남은 흔적이 최대한 다양한 방향으로 교차하도록 패턴을 생성할 수 있다. 예를 들면, 도 2의 랜덤 인증 패턴(300)은 암호 인증 패턴(200)의 2번 점(P2), 4번 점(P4) 및 5번 점(P5)이 중복되도록 생성되었다. 그러나 도 2의 (a)에 도시된 암호 인증 패턴(200)의 2번 점(P2), 4번 점(P4) 및 5번 점(P5)의 연결 순서는 'P2→(P1→)P4→P5' 인 반면, 도 2의 (b)에 도시된 랜덤 인증 패턴(300)의 2번 점(P2), 4번 점(P4) 및 5번 점(P5)의 연결 순서는 'P5→P4→P2' 임을 확인할 수 있다. 이는, 암호 인증 패턴(200) 입력시 남은 자국을 통해 입력된 점이 유추될 경우, 랜덤 인증 패턴(300)이 다른 방향으로 남긴 자국으로 인해 입력 순서를 유추할 수 없도록 하기 위한 것이다.

[0027] 프로세서(120)는 사용자 인증 처리를 수행할 수 있다. 먼저, 프로세서(120)는 사용자에 의해 입력된 인증 패턴 및 암호 인증 패턴(200)이 일치하면 인증을 승인할 수 있다. 프로세서(120)는 인증이 승인되면 랜덤 인증 패턴(300)을 생성하여 입력을 유도할 수 있다.

[0028] 이때, 프로세서(120)는 랜덤 인증 패턴(300)을 따라 사용자에 의해 입력된 인증 패턴이 랜덤 인증 패턴(300)을 구성하는 복수의 점 중 일정 개수의 점을 경유할 경우 인증을 승인할 수 있다. 예를 들면, 랜덤 인증 패턴(300)으로 6개의 점(P1, P2, P3, P4, P5, P6)이 설정되었고, 이 중 사용자에 의해 3개의 점(P1, P5, P6)만이 경유되더라도 인증을 승인할 수 있다. 또는, 암호 인증 패턴(200)의 점을 필수로 포함하는 조건일 경우, 해당 필수 점을 포함하여 일부만을 경유할 수 있다. 이때, 경유해야 할 최소한의 점 개수 또는 필수 점 등의 설정은

사용자에 의해 변경될 수 있다.

[0029] 또한, 프로세서(120)는 랜덤 인증 패턴(300)을 구성하는 점 및 랜덤 인증 패턴(300)을 따라 사용자에 의해 입력된 인증 패턴을 구성하는 점이 일치하면 인증을 승인할 수 있다. 즉, 프로세서(120)에서 생성한 랜덤 인증 패턴(300)의 점과 사용자가 입력한 인증 패턴의 점이 일치할 경우 인증을 승인할 수 있다. 예를 들면, 랜덤 인증 패턴(300)이 1번 점, 2번 점, 3번 점, 4번 점, 5번 점, 6번 점(P1, P2, P3, P4, P5, P6)으로 구성된 경우, 프로세서(120)는 사용자에 의해 입력된 인증 패턴이 'P1→P2→P3→P4→P5→P6', 'P2→P1→P4→P5→P3→P6' 또는 'P6→P3→P5→P2→P4→P1' 등의 입력 순서로 입력되면 사용자 인증을 승인할 수 있다. 즉, 프로세서(120)는 사용자에 의해 입력된 인증 패턴이 입력 순서와 상관없이 1번 점, 2번 점, 3번 점, 4번 점, 5번 점, 6번 점(P1, P2, P3, P4, P5, P6)을 경유할 경우 사용자 승인을 허가할 수 있다.

[0030] 또한, 프로세서(120)는 랜덤 인증 패턴(300)을 구성하는 점의 연결 순서 및 인증 패턴을 구성하는 점의 연결 순서가 일치하면 인증을 승인할 수 있다. 즉, 사용자에 의해 입력된 인증 패턴의 점과 랜덤 인증 패턴의 점이 같고, 입력 순서 또한 일치할 경우 인증을 승인할 수 있다. 이때, 랜덤 인증 패턴(300)은 점의 시작점 표시, 끝점 표시 또는 화살표 등의 표시를 통해 랜덤 인증 패턴(300)의 입력 순서를 가이드할 수 있다. 이에 대한 보다 상세한 설명은 하기 도 3을 참고하여 설명한다.

[0031] 도 3는 본 발명의 일 실시예에 따른 랜덤 인증 패턴 입력을 위한 가이드의 일례이다.

[0032] 랜덤 인증 패턴(300)의 입력 순서를 가이드하기 위하여, 랜덤 인증 패턴(300)을 구성하는 점의 시작점(401), 끝점(402) 및 화살표(403)를 표시하여 입력 순서를 가이드하여 사용자의 인증 패턴 입력을 유도할 수 있다. 도 4를 보면, 3번 점(P3)은 시작점(401)이고 8번 점(P8)은 끝점(402)이며, 점과 점 사이에 표시된 화살표(403)는 점의 입력 방향 나타낸 것을 확인할 수 있다. 이를 통해, 도 4에 제시된 랜덤 인증 패턴(300)으로 구성된 점 및 입력 순서는 'P3→P5→P4→P2→P8' 임을 알 수 있다. 랜덤 인증 패턴(300)의 입력을 위한 가이드 표시는 이외 다양한 그래픽 및 인터페이스로 나타낼 수 있다.

[0033] 도 4는 본 발명의 일 실시예에 따른 암호 인증 패턴 및 랜덤 인증 패턴이 입력된 화면의 일례를 설명하기 위한 도면이다.

[0034] 도 4에 도시된 바와 같이, 사용자에 의해 인증 패턴이 입력되면 결과적으로 암호 인증 패턴(200) 및 랜덤 인증 패턴(300)의 자국이 중첩되어 사용자 인증 처리 장치(100)의 디스플레이에 남을 수 있다. 이때, 랜덤 인증 패턴(300)의 점(P2, P3, P4, P5, P8)은 암호 인증 패턴(200)의 점(P1, P2, P4, P5, P6)의 일부인 2번 점(P2), 4번 점(P4) 및 5번 점(P5)을 경유하도록 생성되었기 때문에 암호 인증 패턴(200)만을 유추하기 어려운 형태가 될 수 있다. 결론적으로, 디스플레이에 남은 자국은 점은 7개의 점(P1, P2, P3, P4, P5, P6, P8)이나, 암호 인증 패턴(200)의 5개의 점 및 랜덤 인증 패턴(300)의 5개의 점을 완전히 구분 지을 수 없으므로 암호 인증 패턴(200)이 유출되는 것을 방지할 수 있다.

[0035] 도 5는 본 발명의 일 실시예에 따른 사용자 인증 처리 장치를 통한 사용자 인증 방법을 설명하기 위한 순서도이다.

[0036] 단계 (S110)에서는, 사용자의 인증 패턴 입력에 따른 인증 처리를 수행할 수 있다. 이때, 사용자에 의해 입력된 인증 패턴 및 암호 인증 패턴이 일치하면 인증을 승인할 수 있다. 여기서, 암호 인증 패턴은 사용자 인증을 위한 비밀 암호로서, 복수의 점을 연결하여 생성될 수 있다.

[0037] 단계 (S120)에서는, 사용자의 인증 패턴 입력 이후에, 사용자에 의해 기설정된 암호 인증 패턴을 구성하는 복수의 점 중 일정 개수의 점을 경유하는 랜덤 인증 패턴을 생성하여, 사용자의 랜덤 인증 패턴 입력을 유도할 수 있다. 이때, 암호 인증 패턴을 구성하는 복수의 점 중 적어도 절반 이상의 점을 포함하는 랜덤 인증 패턴(300)을 생성할 수 있다. 이때, 랜덤 인증 패턴(300)을 구성하는 하나 이상의 점은 암호 인증 패턴(200)에 포함되지 않는 것일 수 있다. 또한, 암호 인증 패턴을 구성하는 점의 개수와 동일한 개수의 점으로 구성된 랜덤 인증 패턴을 생성할 수 있다. 예를 들면, 암호 인증 패턴이 5개의 점으로 구성되었을 경우, 랜덤 인증 패턴은 5개의 절반인 2.5개 이상(즉, 3개 이상)의 암호 인증 패턴의 점을 포함할 수 있으며, 이때, 총 5개의 점으로 구성된 랜덤 인증 패턴이 될 수 있다.

[0038] 또한, 단계 (S120)에서는, 랜덤 인증 패턴을 구성하는 점의 연결 순서를 랜덤하게 설정하여 생성하되, 암호 인증 패턴을 구성하는 점의 연결 순서와 상이하게 설정할 수 있다. 즉, 랜덤 인증 패턴을 구성하는 점의 연결 순서와 암호 인증 패턴을 구성하는 점의 연결 순서를 다르게 설정하여, 암호 인증 패턴 입력시 남긴 자국이 최대

한 노출되지 않도록 할 수 있다.

[0039] 단계 (S130)에서는, 랜덤 인증 패턴을 따라 사용자에 의해 입력된 인증 패턴에 따른 보조 인증 처리를 수행할 수 있다. 이때, 랜덤 인증 패턴을 구성하는 점 중 일정 개수의 점을 경유하는 인증 패턴이 입력되면 인증을 승인할 수 있다. 예를 들면, 5개의 점으로 구성된 랜덤 인증 패턴이 생성되었을 경우, 최소 3개 이상 경유시 인증이 승인되도록 설정하여 생성할 수 있다.

[0040] 또한, 단계 (S130)에서는, 랜덤 인증 패턴을 구성하는 점 및 인증 패턴을 구성하는 점이 일치하면 인증을 승인할 수 있다. 즉, 사용자에 의해 입력된 인증 패턴의 점과 랜덤 인증 패턴의 점이 같을 경우 입력 순서와 관계없이 인증을 승인할 수 있다. 예를 들면, 랜덤 인증 패턴이 'P1, P2, P3, P4, P5, P6'으로 구성된 경우, 사용자에 의해 입력된 인증 패턴이 'P1→P2→P3→P4→P5→P6' 또는 'P2→P1→P4→P5→P3→P6' 또는 'P6→P3→P5→P2→P4→P1' 등과 같이, 입력 순서와 상관없이 'P1, P2, P3, P4, P5, P6'이 포함되도록 점이 입력된다면 사용자 승인을 허가할 수 있다.

[0041] 또한, 단계 (S130)에서는, 랜덤 인증 패턴을 구성하는 점의 연결 순서 및 인증 패턴을 구성하는 점의 연결 순서가 일치하면 인증을 승인할 수 있다. 즉, 사용자에 의해 입력된 인증 패턴의 점과 랜덤 인증 패턴의 점이 같고, 입력 순서 또한 일치할 경우 인증을 승인할 수 있다. 예를 들면, 랜덤 인증 패턴이 'P2→P1→P4→P5→P3→P6'일 경우, 사용자에 의해 입력된 인증 패턴 또한 'P2→P1→P4→P5→P3→P6'일 경우에만 인증을 승인할 수 있다.

[0042] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0043] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0044] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

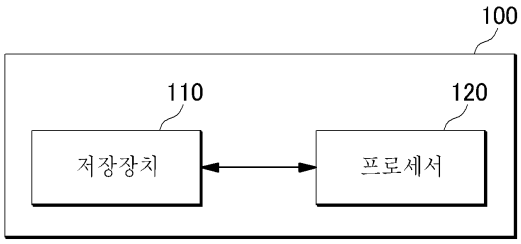
[0045] 100: 사용자 인증 처리 장치 110: 저장장치

120: 프로세서 200: 암호 인증 패턴

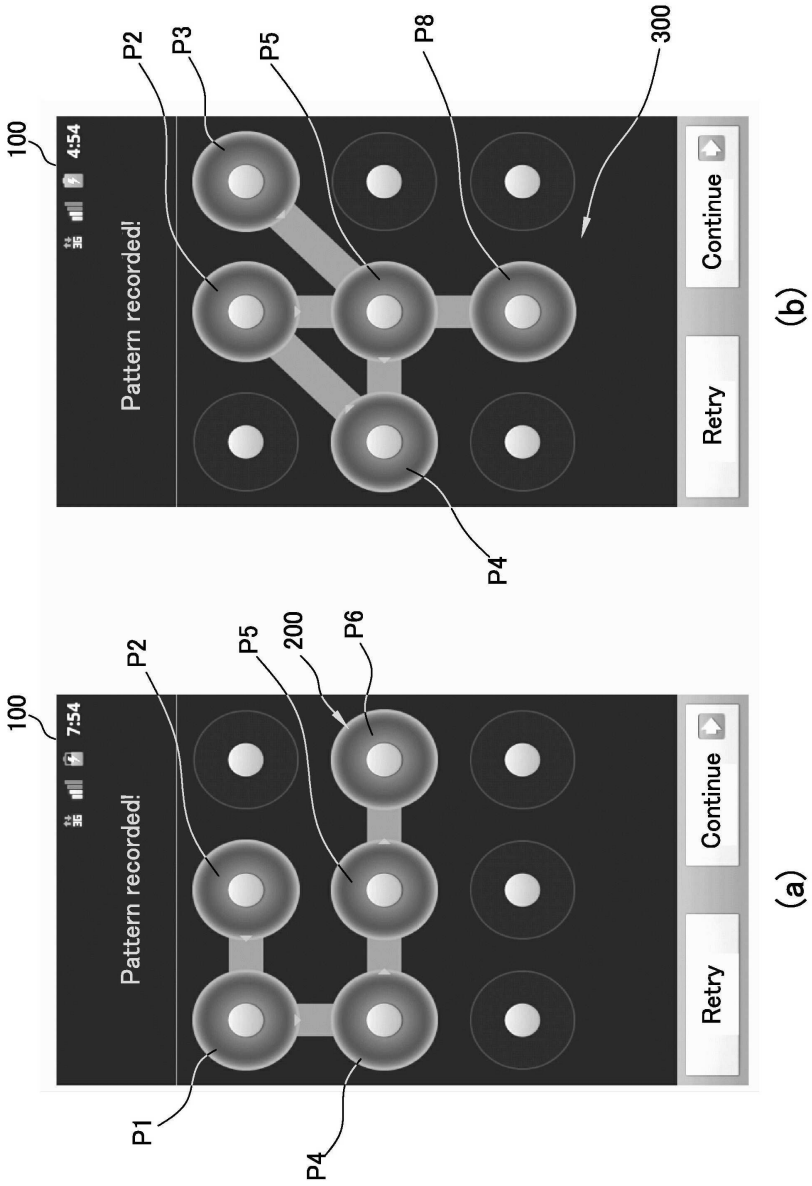
300: 랜덤 인증 패턴

도면

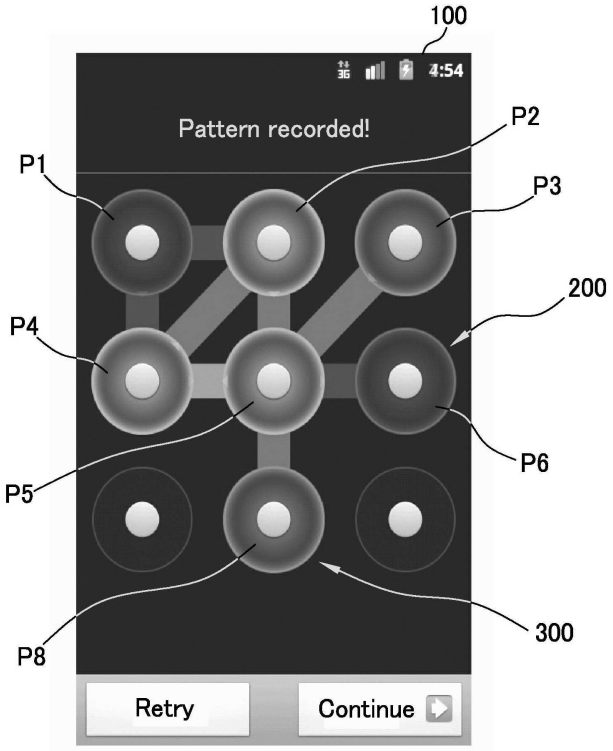
도면1



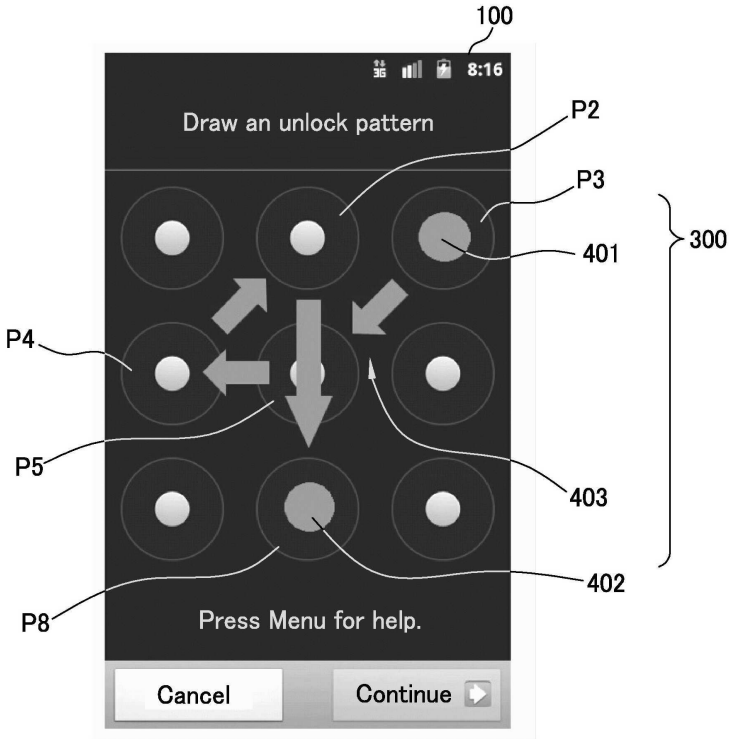
도면2


100
4:54
Pattern recorded!
P2
P3
P5
P8
300
Continue
Retry
P4
(b)
100
7:54
Pattern recorded!
P2
P5
200
P6
Continue
Retry
P1
P4
(a)

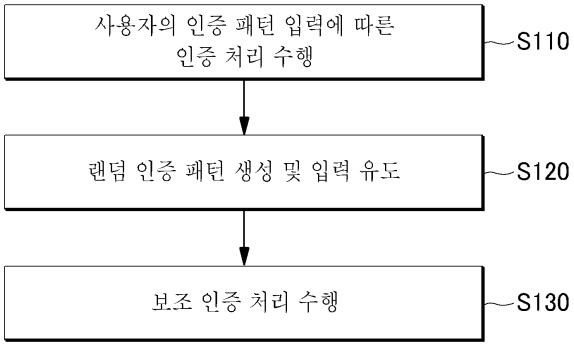
도면3


100
4:54
Pattern recorded!
P1
P2
P3
200
P4
P5
P6
P8
300
Retry
Continue

도면4


100
8:16
Draw an unlock pattern
P2
P3
401
300
P4
P5
403
402
P8
Press Menu for help.
Cancel
Continue

도면5


사용자의 인증 패턴 입력에 따른
인증 처리 수행
S110
랜덤 인증 패턴 생성 및 입력 유도
S120
보조 인증 처리 수행
S130