



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0129687
(43) 공개일자 2014년11월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/31 (2013.01) G06F 21/46 (2013.01)
(21) 출원번호 10-2013-0048287
(22) 출원일자 2013년04월30일
심사청구일자 2013년04월30일

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

전체 청구항 수 : 총 8 항

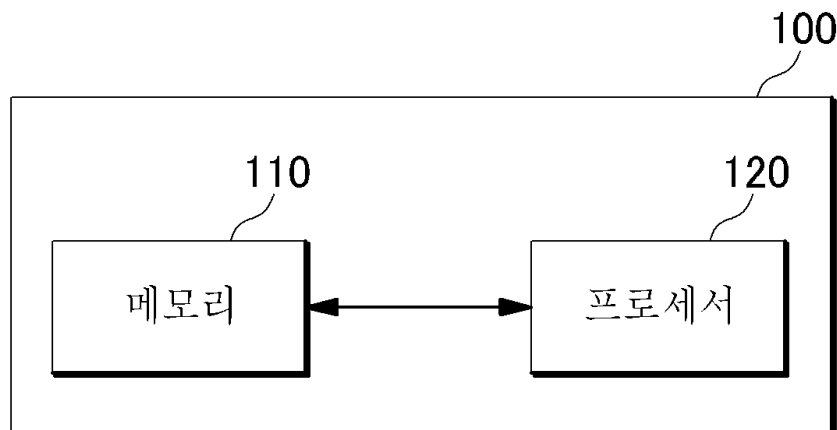
(54) 발명의 명칭 사용자 인증 처리 장치 및 방법

(57) 요약

본 발명에 따른 사용자 인증 처리 장치는 사용자 인증 애플리케이션이 저장된 메모리 및 상기 사용자 인증 애플리케이션을 실행하는 프로세서를 포함하되, 상기 메모리는 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 숫자 암호 테이블 및

(뒷면에 계속)

대표도 - 도1



사용자에 의하여 설정된, 상기 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 상기 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 암호 정보를 저장하고, 상기 프로세서는 상기 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시하고, 사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하고, 상기 해독 정보와 상기 메모리에 저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행한다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1415121995
부처명	지식경제부
연구관리전문기관	한국산업기술평가관리원
연구사업명	SW컴퓨팅산업원천기술개발
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	세종대학교산학협력단
연구기간	2011.05.01 ~ 2015.02.28이 발명을 지원한 국가연구개발사업
과제고유번호	1415123340
부처명	지식경제부
연구관리전문기관	정보통신산업진흥원
연구사업명	정보통신기술인력양성
연구과제명	클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성
기 여 율	1/2
주관기관	송실대학교산학협력단
연구기간	2012.06.01 ~ 2015.12.31

특허청구의 범위

청구항 1

사용자 인증 처리 장치에 있어서,

사용자 인증 애플리케이션이 저장된 메모리 및

상기 사용자 인증 애플리케이션을 실행하는 프로세서를 포함하되,

상기 메모리는 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 숫자 암호 테이블 및

사용자에 의하여 설정된, 상기 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 상기 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 암호 정보를 저장하고,

상기 프로세서는 상기 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시하고,

사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하고, 상기 해독 정보와 상기 메모리에 저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행하는 사용자 인증 처리 장치.

청구항 2

제 1 항에 있어서,

상기 프로세서는 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블의 표시 후에 제 2 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 순차적으로 표시하고,

상기 사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 해당하는 숫자 암호 테이블 및 제 2 설정에 해당하는 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하는 사용자 인증 처리 장치.

청구항 3

제 1 항에 있어서,

상기 숫자 암호 테이블은 $m \times n$ 행렬로 이루어진 테이블이고, 각 행의 하나의 열방향 및 각 열의 하나의 행방향에 상측 및 하측에 위치한 두 개의 숫자를 배치시키고, 상기 숫자를 배치시킨 하나의 행 및 열을 제외한 행과 열에 상기 문자를 배치시킨 사용자 인증 처리 장치.

청구항 4

사용자 인증 처리 장치를 통한 사용자 인증 처리 방법에 있어서,

숫자 암호 테이블 상에서 사용될 암호 정보를 저장하는 단계;

상기 사용자 인증 처리 장치에 설치된 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시하는 단계;

사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하는 단계 및

상기 해독 정보와 기저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행하는 단계를 포함하되,

상기 숫자 암호 테이블은 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 것이고,

상기 암호 정보는 사용자에 의하여 설정된, 상기 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 상기 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 것인 사용자

인증 처리 방법.

청구항 5

제 4 항에 있어서,

상기 숫자 암호 테이블을 표시하는 단계는 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블의 표시 후에 제 2 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 순차적으로 표시하는 사용자 인증 처리 방법.

청구항 6

제 5 항에 있어서,

상기 해독 정보를 생성하는 단계는 상기 사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 따른 숫자 암호 테이블 및 제 2 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하는 사용자 인증 처리 방법.

청구항 7

제 4 항에 있어서,

상기 숫자 암호 테이블은 $m \times n$ 행렬로 이루어진 테이블이고, 각 행의 하나의 열방향 및 각 열의 하나의 행방향에 상측 및 하측에 위치한 두 개의 숫자를 배치시키고, 상기 숫자를 배치시킨 하나의 행 및 열을 제외한 행과 열에 상기 문자를 배치시킨 사용자 인증 처리 방법.

청구항 8

청구항 4 내지 청구항 7 중 어느 한 항에 기재된 방법을 컴퓨터 상에서 수행하기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

명세서

기술 분야

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

배경 기술

[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 환경은 고정형 기기의 기능을 장소 및 시간의 구애 없이 사용할 수 있는 장점이 있다. 그러나 개인적인 장소뿐만 아니라 공공 장소에서 사용이 가능함에 따라, 사용자 인증 처리를 위한 비밀번호 또는 암호의 유출 가능성이 높아지는 단점이 있다.

[0003] 특히, 숄더 서핑 공격에 대비한 기술 개발은 미비한 실정이다. 종래의 기술에서 비밀번호 또는 암호 설정은 모바일 기기의 화면에 바로 입력하거나 표시되어 유출의 가능성이 매우 높으며, 패턴 등을 이용한 암호 설정은 보안성이 높아질수록 암기가 어려워 사용자로 하여금 오류를 발생하게 한다.

[0004] 따라서, 숄더 서핑 공격에 대비하고, 보안성이 높은 사용자 인증 처리를 위한 기술 개발이 필요하다.

[0005] 이와 관련하여 한국 공개특허공보 제 10-2011-0003027호(발명의 명칭: 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법)에는 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 일정한 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하여 키로깅 공격과 숄더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공하고 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 OTP 암호를 생성할

수 있는 행렬로 구성된 사용자 인증 처리 장치 및 방법을 제공하고자 한다.

과제의 해결 수단

[0007] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 일 실시예에 따른 사용자 인증 처리 장치는 사용자 인증 애플리케이션이 저장된 메모리 및 상기 사용자 인증 애플리케이션을 실행하는 프로세서를 포함하되, 상기 메모리는 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 숫자 암호 테이블 및 사용자에게 의하여 설정된, 상기 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 상기 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 암호 정보를 저장하고, 상기 프로세서는 상기 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시하고, 사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하고, 상기 해독 정보와 상기 메모리에 저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행한다.

[0008] 또한, 본 발명의 다른 실시예에 따른 사용자 인증 처리 장치를 통한 사용자 인증 처리 방법은 숫자 암호 테이블 상에서 사용될 암호 정보를 저장하는 단계, 상기 사용자 인증 처리 장치에 설치된 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시하는 단계, 사용자의 암호 입력에 해당하는 숫자를 상기 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하는 단계 및 상기 해독 정보와 기저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행하는 단계를 포함하되, 상기 숫자 암호 테이블은 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 것이고, 상기 암호 정보는 사용자에게 의하여 설정된, 상기 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 상기 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 것이다.

발명의 효과

[0009] 전술한 본 발명의 과제 해결 수단에 의하면, 사용자에게 의해 설정된 문자 및 위치 정보에 매칭되는 숫자 암호를 생성할 수 있도록 행렬로 구성된 숫자 암호 테이블에 문자 및 숫자를 랜덤하게 표시하여 OTP를 생성할 수 있다.

[0010] 또한, 전술한 본 발명의 과제 해결 수단에 의하면, 사용자는 기설정된 문자 및 위치 정보에 매칭되는 숫자 암호를 행렬로 구성된 숫자 암호 테이블을 통해 추출한 간접적인 숫자 암호를 입력함으로써, 솔더 서핑 공격으로부터 암호의 유출을 방지할 수 있다.

도면의 간단한 설명

[0011] 도 1은 본 발명의 일 실시예에 따른 사용자 인증 처리 장치의 구성도이다.

도 2는 암호 정보 설정의 일례를 설명하기 위한 도면이다.

도 3은 숫자 암호 테이블을 통한 숫자 암호 입력의 일례를 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 사용자 인증 처리 장치를 통한 사용자 인증 처리 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 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.

[0013] 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.

- [0014] 도 1은 본 발명의 일 실시예에 따른 사용자 인증 처리 장치의 구성도이다.
- [0015] 이때, 본 발명의 일 실시예에서는, 사용자 인증 처리 장치(100)가 모바일 기기(예를 들어, 스마트폰)인 것을 예로서 설명하도록 한다.
- [0016] 참고로, 도 1에서는 본 발명의 일 실시예에 따른 행렬 테이블을 이용한 사용자 인증 처리를 위한 구성들을 도시하였으나, 장치의 종류에 따라 이 외에도 다른 처리부(미도시)들이 더 포함될 수 있다.
- [0017] 또한, 사용자 인증 처리 장치(100)는 휴대용 단말기 또는 컴퓨터로 구현될 수 있다. 여기서, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, 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, 스마트폰(Smart Phone), 스마트 패드(Smart Pad) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다. 또한, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop), 태블릿 PC 등을 포함할 수 있다.
- [0018] 본 발명의 일 실시예에 따른 사용자 인증 처리 장치(100)는 메모리(110) 및 프로세서(120)를 포함한다.
- [0019] 메모리(110)는 사용자 인증 애플리케이션이 저장된다. 또한, 메모리(110)는 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 숫자 암호 테이블 및 사용자에게 의하여 설정된, 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 암호 정보를 저장한다.
- [0020] 이때, 숫자 암호 테이블은 $m \times n$ 행렬로 이루어진 테이블이고, 각 행의 하나의 열방향 및 각 열의 하나의 행방향에 상측 및 하측에 위치한 두 개의 숫자를 배치시키고, 숫자를 배치시킨 하나의 행 및 열을 제외한 행과 열에 문자를 배치시킬 수 있다.
- [0021] 예를 들면, 6×6 행렬로 이루어진 행렬 테이블의 경우, 각 행의 하나의 열방향으로서 각 행의 1열 및 각 열의 하나의 행방향으로서 각 열의 1행에 숫자를 배치시킬 수 있다. 이때, 숫자는 좌상측 및 우하측에 각각 위치한 두 개의 숫자쌍이 될 수 있다. 한편, 숫자를 배치시킨 1행 1열을 제외한 행과 열에 문자를 배치시킬 수 있다. 여기서, 문자는 알파벳, 한글, 한자, 기호 등이 포함될 수 있으며, 문자를 배치시킬 때 사용자에게 의해 지정된 문자를 포함한 복수의 문자가 임의로 배치될 수 있다. 즉, 숫자 암호 테이블은 6×6 행렬 테이블의 1행 1열에는 숫자가, 나머지 행과 열에는 문자가 배치된 형태일 수 있다.
- [0022] 숫자 암호 테이블은 사용자가 지정한 둘 이상의 문자와 숫자 암호로 지정될 숫자의 위치 정보를 통해 OTP(One Time Password)용 숫자 암호를 생성하기 위한 것이다. 즉, 메모리(110)는 사용자에게 의하여 설정된 둘 이상의 문자와 숫자의 위치 정보를 암호 정보로 저장하고, 암호 정보와 매칭되는 숫자 암호를 생성하기 위한 숫자 암호 테이블을 저장할 수 있다. 암호 정보는 고정된 숫자를 입력하는 것이 아닌 OTP용 숫자를 입력할 수 있는 간접적인 암호로써, 암기가 용이하고 솔더 서핑 공격을 방어할 수 있다. 이에 대한 보다 상세한 설명은 하기 도 2를 참조하여 후술하기로 한다.
- [0023] 프로세서(120)는 사용자 인증 애플리케이션을 실행한다. 또한, 프로세서(120)는 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시하고, 사용자의 암호 입력에 해당하는 숫자를 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성하고, 해독 정보와 메모리(110)에 저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행한다.
- [0024] 예를 들면, 프로세서(120)는 사용자 인증 애플리케이션을 실행한 후 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시할 수 있다. 또한, 사용자가 입력한 숫자를 통해서 표시된 숫자 암호 테이블상의 문자 및 숫자의 위치 정보를 파악할 수 있고, 파악된 문자 및 숫자의 위치 정보가 메모리(110)에 저장된 암호 정보 즉, 사용자에게 의하여 기설정된 문자 및 숫자의 위치 정보와 일치하는지 판단할 수 있다. 만약, 일치한다면 사용자 인증 승인에 따른 보안을 해제할 수 있고, 일치하지 않다면 사용자 불인증에 따른 보안 상태를 유지할 수 있다. 이에 대한 보다 상세한 설명은 하기 도 3을 참조하여 후술하기로 한다.
- [0025] 또한, 프로세서(120)는 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블의 표시 후에 제 2 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 순차적으로 표시하고, 사용자의 암호 입력에

해당하는 숫자를 제 1 설정에 해당하는 숫자 암호 테이블 및 제 2 설정에 해당하는 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성할 수 있다.

- [0026] 예를 들면, 암호 정보로서 저장된 둘 이상의 문자가 설정되었을 경우, 문자 하나당 하나의 설정 즉, 문자 n 개당 제 n 설정을 할 수 있다. 즉, 하나의 문자에 따른 숫자 암호 테이블을 표시하여 입력된 숫자를 디코딩하고, 또 다른 문자에 따른 또 다른 숫자 암호 테이블을 표시하여 입력된 숫자를 디코딩한 후 해독 정보를 종합하여 인증 처리를 수행할 수 있다. 이에 대한 보다 상세한 설명은 하기 도 3을 참조하여 후술하기로 한다.
- [0027] 도 2는 암호 정보 설정의 일례를 설명하기 위한 도면이다.
- [0028] 이때, 본 발명의 일 실시예에서는, 사용자 인증 처리 장치(100)가 모바일 기기(예를 들어, 스마트폰)인 것을 예로서 설명하도록 한다.
- [0029] 먼저, 암호 정보는 적어도 둘 이상의 문자 및 숫자의 위치 정보를 포함한다. 즉, 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함할 수 있다. 그러므로, 문자를 설정하는 문자 설정 영역(201) 및 숫자의 위치 정보를 입력하는 위치 설정 영역(202)을 표시하여 사용자로 하여금 문자 및 위치 정보를 입력할 수 있도록 할 수 있다.
- [0030] 문자 설정 영역(201)은 두 개의 문자를 설정할 수 있다. 도 2에 도시된 바와 같이, 알파벳 'D'와 알파벳 'H'가 문자로 설정될 수 있다. 본 일례에서는 두 개의 문자를 설정하는 문자 설정 영역(201)을 도시하였으나, 문자 설정의 개수는 한정된 것이 아니다.
- [0031] 위치 설정 영역(202)은 하나의 문자당 두 개의 위치 정보를 설정할 수 있다. 이는, 문자의 행방향 및 열방향에 위치한 숫자를 지목하는 위치 정보이다. 예를 들어, 문자 'D'의 위치 정보를 좌상측 및 좌상측으로 설정할 경우, 첫 번째 좌상측은 문자 'D'의 행방향에 위치한 숫자 중 좌상측에 위치한 숫자를 지목하는 것이며, 두 번째 좌상측은 문자 'D'의 열방향에 위치한 숫자 중 좌상측에 위치한 숫자를 지목하는 것일 수 있다. 또한, 문자 'H'의 위치 정보를 좌상측 및 우하측으로 설정할 경우, 좌상측은 문자 'H'의 행방향에 위치한 숫자 중 좌상측에 위치한 숫자를 지목하는 것이며, 두 번째 우하측은 문자 'H'의 열방향에 위치한 숫자 중 우하측에 위치한 숫자를 지목하는 것일 수 있다. 결론적으로, 암호 정보는 "D의 행 - 좌상측, D의 열 - 좌상측, H의 행 - 좌상측, H의 열 - 우하단"이 될 수 있다.
- [0032] 설정된 둘 이상의 문자 및 숫자의 위치 정보는 암호 정보로 저장되어, 차후 사용자가 암호 입력에 해당하는 숫자를 입력하였을 때, 입력된 숫자를 디코딩한 해독 정보와 비교될 수 있다. 암호 정보와 해독 정보가 일치할 경우, 사용자 인증이 처리되어 보안이 해제될 수 있다. 설정된 암호 정보를 바탕으로 숫자 암호를 입력하는 일례는 도 3을 참조하여 후술하기로 한다.
- [0033] 도 3은 숫자 암호 테이블을 통한 숫자 암호 입력의 일례를 설명하기 위한 도면이다.
- [0034] 도 3의 (a) 및 도 3의 (b)에 도시된 바와 같이, 숫자 암호 테이블(301)은 6 x 6 행렬 테이블에 의해 생성될 수 있다. 이때, 1행 1열에 숫자를 랜덤하게 배치하고, 나머지 행과 열에 문자를 랜덤하게 배치할 수 있다. 숫자를 배치할 때는 좌상측 및 좌하측에 두 개의 숫자를 배치할 수 있다.
- [0035] 사용자는 암호 정보로 설정된 "D의 행 - 좌상측, D의 열 - 좌상측, H의 행 - 좌상측, H의 열 - 우하단"를 숫자 암호 테이블(301)에 순차적으로 적용하여 숫자 암호를 입력할 수 있다. 이때, 숫자 암호 테이블(301)은 하나의 문자당 하나의 숫자 암호 테이블(301)이 갱신될 수 있다. 사용자는 하나의 문자에 해당하는 숫자 암호 테이블(301)을 확인한 후, 화면을 넘겨 새로운 숫자 암호 테이블(301)을 표시할 수 있다.
- [0036] 먼저, 도 3의 (a)에 도시된 숫자 암호 테이블(301)을 이용하여 문자 'D'의 숫자 암호를 찾을 수 있다. 문자 'D'에 대한 암호 정보는 "D의 행 - 좌상측, D의 열 - 좌상측"이므로 먼저, 문자 'D'의 행에 배치된 숫자 중 좌상측에 위치한 숫자가 '7'임을 확인할 수 있다. 다음으로, 문자 'D'의 열에 배치된 숫자 중 좌상측에 위치한 숫자는 '9'임을 확인할 수 있다. 즉, "D의 행 - 좌상측: 7, D의 열 - 좌상측: 9"이므로 숫자 '7', '9'가 순차적으로 입력될 수 있다.
- [0037] 다음으로, 먼저, 도 3의 (b)에 도시된 숫자 암호 테이블(301)을 이용하여 문자 'H'의 숫자 암호를 찾을 수 있다. 문자 'H'에 대한 암호 정보는 "H의 행 - 좌상측, H의 열 - 우하단"이므로 먼저, 문자 'H'의 행에 배치된 숫자 중 좌상측에 위치한 숫자가 '9'임을 확인할 수 있다. 다음으로, 문자 'H'의 열에 배치된 숫자 중 우하측에 위치한 숫자는 '5'임을 확인할 수 있다. 즉, "H의 행 - 좌상측: 9, H의 열 - 우하단: 5"이므로

로 숫자 '9' , '5' 가 순차적으로 입력될 수 있다.

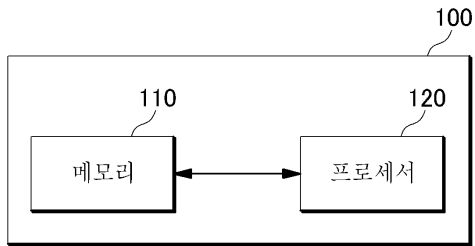
- [0038] 도 3의 (a) 및 도 3의 (b)에서 확인된 숫자는 도 3의 (c)에 도시된, 숫자 입력 영역(303)을 통해 입력될 수 있다. 하나의 문자당 두 개의 숫자가 생성되므로, 네 자리 숫자가 입력될 수 있으며 입력 여부는 입력 확인 영역(305)을 통해 확인할 수 있다. 그러므로 사용자는 도 3의 (c)에 도시된 바와 같이, 입력 확인 영역(305)을 통해 숫자 '7995'가 입력되었음을 확인할 수 있다. 이때, 입력 확인 영역(305)은 숫자가 아닌 통일된 기호로 암호 입력을 표시하여 보안을 강화할 수 있으나, 본 발명에서의 숫자 암호는 OTP용 암호로써 매회 다른 숫자 암호가 설정되므로 숫자가 노출되어도 본래의 암호가 유출되는 것을 방지할 수 있다.
- [0039] 도 4는 본 발명의 일 실시예에 따른 사용자 인증 처리 장치를 통한 사용자 인증 처리 방법을 설명하기 위한 흐름도이다.
- [0040] 단계 (S110)에서는, 숫자 암호 테이블 상에서 사용될 암호 정보를 저장한다. 이때, 숫자 암호 테이블은 복수의 문자를 행렬 테이블상에 배치시키고, 각 문자에 대하여 행방향 및 열방향으로 각각 서로 다른 두 개의 숫자를 상이한 위치에 배치시킨 것이다. 또한, 숫자 암호 테이블은 $m \times n$ 행렬로 이루어진 테이블이고, 각 행의 하나의 열방향 및 각 열의 하나의 행방향에 상측 및 하측에 위치한 두 개의 숫자를 배치시키고, 숫자를 배치시킨 하나의 행 및 열을 제외한 행과 열에 문자를 배치시킨 것이다. 또한, 암호 정보는 사용자에게 의하여 설정된, 숫자 암호 테이블 상에서 사용될 적어도 둘 이상의 문자 및 문자의 행방향 및 열방향에 위치한 숫자 중 숫자 암호로 지정될 숫자의 위치 정보를 포함하는 것이다.
- [0041] 단계 (S120)에서는, 사용자 인증 처리 장치에 설치된 사용자 인증 애플리케이션의 실행시에, 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 표시한다. 또한, 단계 (S120)는 제 1 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블의 표시 후에 제 2 설정에 따라 문자 및 숫자가 랜덤하게 배치된 숫자 암호 테이블을 순차적으로 표시할 수 있다.
- [0042] 단계 (S130)에서는, 사용자의 암호 입력에 해당하는 숫자를 제 1 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성한다. 또한, 단계 (S130)에서는 사용자의 암호 입력에 해당하는 숫자를 제 1 설정에 따른 숫자 암호 테이블 및 제 2 설정에 따른 숫자 암호 테이블에 적용하여, 해당 숫자에 매칭되는 문자 및 해당 문자에 매칭될 숫자 암호의 위치 정보를 디코딩하여 해독 정보를 생성할 수 있다.
- [0043] 단계 (S140)에서는, 해독 정보와 기저장된 암호 정보를 비교한 결과에 기초하여 인증 처리를 수행한다. 즉, 해독 정보에 따른 문자 및 위치 정보가 기저장된 암호 정보의 문자 및 위치 정보와 일치하는지 판단하고, 일치할 경우 사용자 인증을 승인하여 보안을 해제할 수 있다. 만약, 불일치할 경우 사용자 인증을 미승인하여 보안을 유지할 수 있다.
- [0044] 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.
- [0045] 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.
- [0046] 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

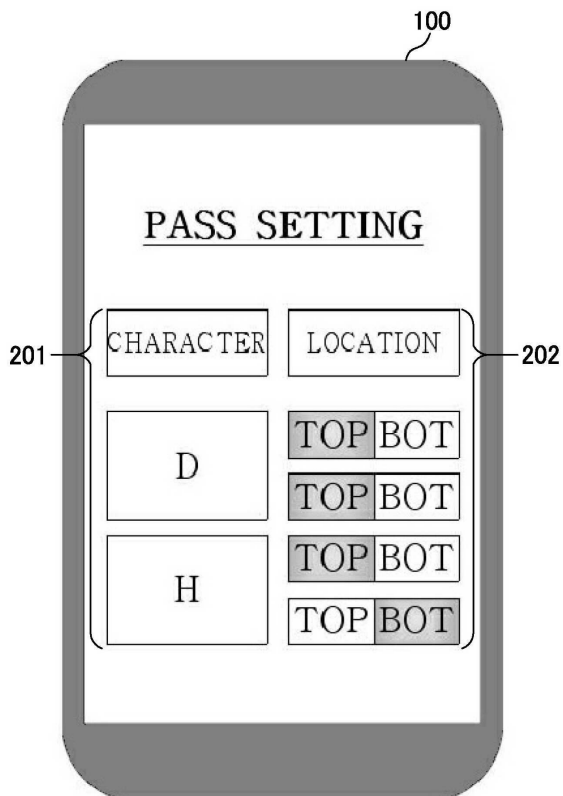
- [0047]
- | | |
|-------------------|----------------|
| 100: 사용자 인증 처리 장치 | 110: 메모리 |
| 120: 프로세서 | 201: 문자 설정 영역 |
| 202: 위치 설정 영역 | 301: 숫자 암호 테이블 |
| 303: 숫자 입력 영역 | 305: 입력 확인 영역 |

도면

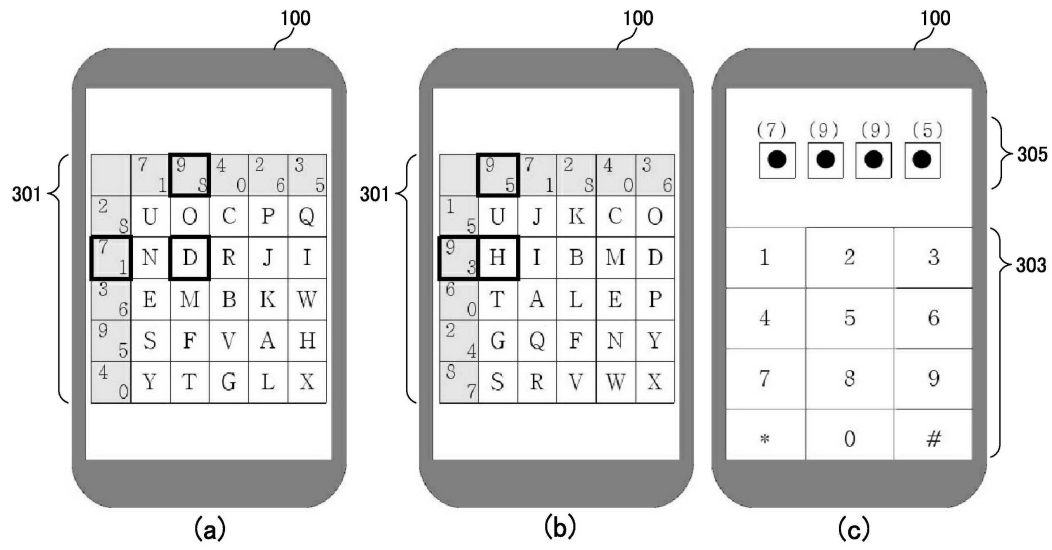
도면1



도면2



도면3



도면4

