(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년07월15일
(11) 등록번호 10-2278236
(24) 등록일자 2021년07월12일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2021.01) *G06F 21/35* (2013.01)
H04M 1/725 (2021.01)
(52) CPC특허분류
H04W 12/06 (2021.01)
G06F 21/35 (2013.01)
(21) 출원번호 10-2016-7012883
(22) 출원일자(국제) 2014년10월29일
심사청구일자 2019년10월29일
(85) 번역문제출일자 2016년05월16일
(65) 공개번호 10-2016-0077096
(43) 공개일자 2016년07월01일
(86) 국제출원번호 PCT/GB2014/053209
(87) 국제공개번호 WO 2015/063474
국제공개일자 2015년05월07일
(30) 우선권주장
61/896,820 2013년10월29일 미국(US)
1407528.7 2014년04월29일 영국(GB)
(56) 선행기술조사문헌
US20080041933 A1*
US20130278552 A1*
WO2009096767 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
크립토매틱 엘티디
영국 씨비4 0더블유지 캠브리지샤이어, 캠브리지, 밀튼로드, 캠브리지사이언스 파크 327
(72) 발명자
랜드락, 피터
영국 CB3 0DX 캠브리지샤이어, 캠브리지, 스토리즈 웨이 52
본드, 마이크
영국 CB4 0WG 캠브리지샤이어, 캠브리지, 밀튼로드, 캠브리지사이언스 파크 329
(74) 대리인
특허법인 아이피에스

전체 청구항 수 : 총 44 항 심사관 : 이준석

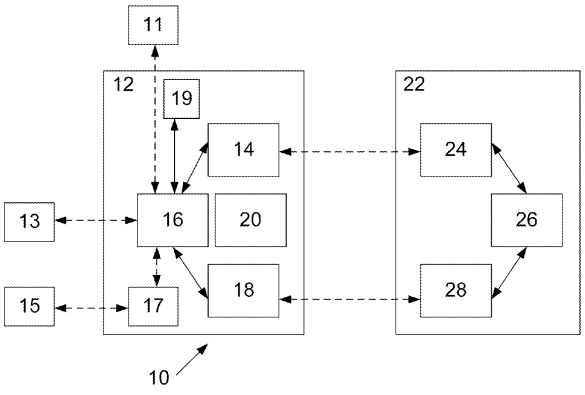
(54) 발명의 명칭 **보안 모바일 사용자 인터페이스**

(57) 요 약

본 발명은 모바일 디바이스에 사용자로부터 사용자 데이터를 안전하게 입력하고, 모바일 디바이스에 사용자에 의해 입력되는 사용자 데이터를 생성하기 위한 시스템 및 방법을 제공한다. 예를 들어, 상기 모바일 디바이스에 사용자로부터 사용자 데이터를 안전하게 입력하기 위한 모바일 디바이스 케이스를 제공하고, 상기 케이스는 마이크

(뒷면에 계속)

대 표 도 - 도2



로 컨트롤러, 모바일 디바이스와 통신하는 통신 모듈 및 사용자가 상기 사용자 데이터를 입력할 수 있는 사용자 인터페이스를 포함한다. 상기 마이크로 컨트롤러는 바람직하게는 상기 사용자 인터페이스를 통해 사용자에 의해 입력받은 사용자 데이터를 전달받고, 처리된 데이터를 생성하기 위해 상기 사용자 데이터를 처리하고, 상기 모바일 디바이스에 처리된 데이터를 전송하기 위해 구성된다. 대안적으로, 상기 마이크로 컨트롤러는 상기 사용자 데이터를 생성하기 위한 요청을 받고; 사용자 데이터를 생성하고; 상기 사용자 인터페이스에 상기 사용자 데이터를 표시한다.

(52) CPC특허분류
H04M 1/72409 (2021.01)
H04M 2250/22 (2013.01)

명 세 서

청구범위

청구항 1

사용자로부터 사용자 데이터를 안전하게 입력받기 위한 모바일 디바이스 케이스에 있어서, 상기 케이스는,

마이크로 컨트롤러;

통신 모듈; 및

사용자 인터페이스를 포함하고,

상기 모바일 디바이스 케이스의 상기 사용자 인터페이스는 상기 사용자가 상기 사용자 데이터를 입력하는 것을 가능하게 하고,상기 모바일 디바이스 케이스의 상기 마이크로 컨트롤러는,

상기 사용자 인터페이스를 통해 사용자로부터 입력된 상기 사용자 데이터를 받고,

문자가 입력될 때 상기 사용자 데이터의 각각의 문자 선택에 따라 모바일 디바이스가 시각적으로 표시하도록, 상기 모바일 디바이스 케이스의 내부에 수용되는 상기 모바일 디바이스와 통신하고,

처리된 데이터를 생성하기 위해 상기 사용자 데이터를 처리하며,

상기 사용자 데이터는 상기 모바일 디바이스 또는 서드 파티(third party)에 의하여 상기 처리된 데이터로부터 결정되지 않고,

상기 마이크로 컨트롤러는 상기 사용자 데이터를 확인하거나 - 상기 확인은 (i) 상기 사용자 데이터와 상기 마이크로 컨트롤러에 저장된 암호를 비교하는 것 또는 (ii) 상기 사용자 데이터에 일방향성 함수를 적용하고, 상기 처리된 데이터에 저장된 데이터를 매칭시키는 것으로 구성되며, 상기 저장된 데이터는 상기 일방향성 함수가 적용된 상기 사용자 데이터로부터 생성됨-, 또는 상기 사용자 데이터를 암호화함으로써 상기 사용자 데이터를 처리하도록 구성되고,

상기 처리된 데이터는 상기 사용자 데이터가 확인되었는지 여부를 나타내고,

상기 모바일 디바이스 또는 상기 서드 파티(third party)로 상기 처리된 데이터를 출력하되, 상기 사용자 데이터는, 상기 모바일 디바이스 또는 상기 서드 파티가 상기 사용자 인터페이스를 통해 입력된 상기 사용자 데이터를 해석하는 일 없이, 상기 모바일 디바이스 또는 상기 서드 파티로 안전하게 전송될 수 있도록 하는 모바일 디바이스 케이스.

청구항 2

제1항에 있어서,

상기 사용자 인터페이스는 상기 사용자 데이터의 어떤 문자가 입력되는지를 상기 사용자에게 표시하기 위한 적어도 하나의 시각적 인디케이터를 포함하는 모바일 디바이스 케이스.

청구항 3

제2항에 있어서,

상기 적어도 하나의 시각적 인디케이터는 다수의 광원을 포함하고, 상기 다수의 광원은 입력되고 있는 사용자 데이터의 문자를 표시하기 위해 한번에 하나씩 점등되는 모바일 디바이스 케이스.

청구항 4

제2항에 있어서,

상기 적어도 하나의 시각적 인디케이터는 다수의 점등 광원을 포함하고, 상기 다수의 점등 광원은 입력되고 있는 사용자 데이터의 문자를 나타내기 위해 한번에 하나씩 소등되는 모바일 디바이스 케이스.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 사용자 인터페이스는 사용자가 상기 사용자 데이터의 각각의 문자를 입력하도록 하는 터치 메커니즘을 포함하는 모바일 디바이스 케이스.

청구항 6

제5항에 있어서, 제3항 또는 제4항을 인용하는 경우,

상기 터치 메커니즘은 점등 광원 또는 소등 광원을 변경하는 터치센서를 포함하는 모바일 디바이스 케이스.

청구항 7

제5항에 있어서,

상기 터치 메커니즘은 다수의 터치센서를 포함하고,

하나의 터치센서는 상기 사용자 데이터를 위한 것이며,

이 때, 상기 사용자는 원하는 문자에 대응되는 터치 센서를 프레스하여 상기 사용자 데이터를 입력하는 모바일 디바이스 케이스.

청구항 8

제6항 또는 제7항에 있어서,

상기 터치센서 또는 각각의 터치센서는 용량성 터치 센서인 모바일 디바이스 케이스.

청구항 9

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 사용자 인터페이스는 상기 모바일 디바이스로부터 상기 통신 모듈을 통해 조정 데이터를 수신하도록 구성되고,

상기 모바일 디바이스는 상기 사용자 데이터를 입력 받는데 사용될 수 있는 모바일 디바이스 케이스.

청구항 10

제9항에 있어서, 제3항 또는 제4항을 인용하는 경우,

상기 마이크로 컨트롤러는 상기 조정 데이터에 기초하여 점등 광원 또는 소등 광원을 변경하도록 구성되는 모바일 디바이스 케이스.

청구항 11

제10항에 있어서,

상기 마이크로 컨트롤러는 상기 사용자 데이터의 적어도 첫 번째 문자가 입력되기 전에 다수의 광원 중 하나를 임의로 밝히도록 구성되는 모바일 디바이스 케이스.

청구항 12

제10항에 있어서,

상기 사용자 인터페이스는 상기 통신 모듈을 통해 상기 모바일 디바이스로부터 문자 데이터를 수신하도록 구성되고,

상기 문자 데이터는 상기 모바일 디바이스의 스크린에 표시되고 각각의 광원과 정렬되도록 문자를 표시하고,

상기 마이크로 컨트롤러는 상기 문자 데이터에서 선택된 문자를 판정하기 위해 구성되는 모바일 디바이스 케이스.

청구항 13

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 마이크로 컨트롤러는 토큰을 생성하기 위해 상기 사용자 데이터를 처리하도록 구성되고,

처리된 후 상기 토큰은 상기 모바일 디바이스로 전송되는 모바일 디바이스 케이스.

청구항 14

제13항에 있어서,

카운터를 더 포함하고,

상기 마이크로 컨트롤러는 상기 카운터로부터의 카운트를 이용하여 토큰을 생성하도록 구성되는 모바일 디바이스 케이스.

청구항 15

제13항에 있어서,

클럭(clock)을 더 포함하고,

상기 마이크로 컨트롤러는 상기 클럭으로부터 얻어진 현재의 시간을 이용하여 상기 토큰을 생성하도록 구성되는 모바일 디바이스 케이스.

청구항 16

제13항에 있어서,

상기 마이크로 컨트롤러는 인증 데이터를 이용하여 상기 토큰을 생성하도록 구성되고,

상기 인증데이터는 상기 모바일 디바이스에서 실행되는 어플리케이션 종류와 관련된 데이터, 모바일 디바이스의 종류과 관련된 데이터 및 사용자 특성 데이터 중 하나 이상으로 구성되는 모바일 디바이스 케이스.

청구항 17

제16항에 있어서,

상기 케이스에 통합된 스마트 카드 리더를 더 포함하고,

상기 사용자 특성 데이터는 상기 리더에 삽입된 스마트 카드로부터 얻어지는 모바일 디바이스 케이스.

청구항 18

제16항에 있어서,

상기 마이크로 컨트롤러를 포함하는 내장형 EMV칩을 더 포함하고,

상기 사용자 특성 데이터는 상기 EMV칩으로부터 얻어지는 모바일 디바이스 케이스.

청구항 19

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 사용자 인터페이스는 상기 케이스가 무결성이나 비밀 보호 모드인지를 표시하기 위한 시각적 인디케이터를 포함하는 모바일 디바이스 케이스.

청구항 20

모바일 디바이스에 안전하게 데이터를 입력하기 위한 시스템에 있어서,

상기 시스템은,

제1항 내지 제19항 중 어느 한 항에 따른 모바일 디바이스 케이스; 및

디스플레이 및 상기 모바일 디바이스 케이스와 통신하기 위한 통신모듈로 구성된 모바일 디바이스를 포함하는 시스템.

청구항 21

제20항에 있어서,

상기 모바일 디바이스는 상기 디스플레이에 문자들의 세트를 표시하기 위해 구성되는 시스템.

청구항 22

제21항에 있어서,

상기 모바일 디바이스 케이스는 다수의 광원 중 하나가 각각의 표시된 문자와 정렬된 다수의 광원을 포함하며,

하나의 광원은 선택되고 있는 문자를 표시하기 위해 한번씩 점등되는 시스템.

청구항 23

제21항에 있어서,

상기 모바일 디바이스 케이스는 다수의 광원 중 하나가 각각의 표시된 문자와 정렬된 다수의 광원을 포함하고,

하나의 광원은 선택되고 있는 문자를 표시하기 위해 소등되는 시스템.

청구항 24

제22항 또는 제23항에 있어서,

상기 모바일 디바이스는 적어도 하나 이상의 터치센서를 포함하고,

상기 모바일 디바이스는 조정 데이터를 상시 모바일 디바이스 케이스로 전송하되, 상기 광원은 점등과 소등이 제어 가능한 시스템.

청구항 25

제20항에 있어서,

상기 모바일 디바이스와 모바일 디바이스 케이스는 하나의 디바이스에 통합된 시스템.

청구항 26

제25항에 있어서,

상기 모바일 디바이스 케이스는 가상의 케이스인 시스템.

청구항 27

제20항에 있어서,

상기 모바일 디바이스는 스마트 폰 또는 태블릿 컴퓨터인 시스템.

청구항 28

사용자로부터 입력될 수 있는 사용자 데이터를 생성하고 모바일 디바이스를 수용하기 위한 모바일 디바이스 케이스에 있어서,

상기 사용자 데이터는 복수의 문자로 구성되고,

상기 모바일 디바이스 케이스는,

마이크로 컨트롤러; 및

상기 사용자 데이터의 상기 복수의 문자 각각을 상기 사용자에게 나타내는 다수의 광원을 포함하고,

상기 다수의 광원 각각은 상기 모바일 디바이스 케이스 내에 수용되는 상기 모바일 디바이스에 디스플레이되는

복수의 문자 중 하나의 문자에 정렬되도록 구성되고,

상기 마이크로 컨트롤러는,

상기 사용자 데이터를 생성하기 위한 요청을 수신하고,

상기 사용자 데이터를 생성하고,

상기 사용자 데이터의 상기 복수의 문자 각각을 나타내기 위하여 상기 모바일 디바이스 케이스의 상기 다수의 광원을 순차에 따라 발광하게 제어하도록

구성되는

모바일 디바이스 케이스.

청구항 29

제28항에 있어서,

상기 모바일 디바이스 케이스는 카운터를 더 포함하고,

상기 마이크로 컨트롤러는 상기 카운터로부터의 카운트를 이용하여 상기 사용자 데이터를 생성하기 위해 구성되는 모바일 디바이스 케이스.

청구항 30

제28항 또는 제29항에 있어서,

클럭(clock)을 더 포함하고,

상기 마이크로 컨트롤러는 상기 클럭으로부터 얻은 현재의 시간을 이용하여 사용자 데이터를 생성하기 위해 구성되는 모바일 디바이스 케이스.

청구항 31

제28항 또는 제29항에 있어서,

상기 마이크로 컨트롤러는 인증 데이터를 이용하여 상기 사용자 데이터를 생성하기 위해 구성되고,

상기 인증 데이터는 상기 모바일 디바이스에서 실행되는 어플리케이션 종류와 관련된 데이터, 모바일 디바이스의 종류과 관련된 데이터 및 사용자 특성 데이터 중 적어도 하나 이상으로 구성되는 모바일 디바이스 케이스.

청구항 32

제31항에 있어서,

상기 케이스에 통합된 스마트 카드 리더를 더 포함하고,

상기 사용자 특성 데이터는 상기 리더에 삽입된 스마트 카드로부터 얻어지는 모바일 디바이스 케이스.

청구항 33

제32항에 있어서,

상기 사용자 특성 데이터는 상기 케이스에 저장되어 있는 모바일 디바이스 케이스.

청구항 34

제33항에 있어서,

상기 마이크로 컨트롤러를 포함하는 내장형 EMV칩을 더 포함하고,

상기 사용자 특성 데이터는 EMV칩으로부터 얻어지는 모바일 디바이스 케이스.

청구항 35

제28항에 있어서,

상기 마이크로 컨트롤러는

상기 다수의 광원이 한번에 하나씩 상기 순차에 따라 점등되도록 제어하고,

각각의 점등 광원은 상기 사용자 데이터의 각각의 순차적인 문자를 나타내는 모바일 디바이스 케이스.

청구항 36

제28항에 있어서,

상기 마이크로 컨트롤러는

상기 다수의 광원이 한번에 하나씩 상기 순차에 따라 소등되도록 제어하고,

소등 광원은 상기 사용자 데이터의 각각의 순차적인 문자를 나타내는 모바일 디바이스 케이스.

청구항 37

모바일 디바이스에 데이터를 입력하기 위한 시스템에 있어서,

상기 시스템은,

제28항 내지 제36항 중 어느 한 항에 따라 사용자 데이터를 생성하기 위한 모바일 디바이스 케이스; 및

디스플레이를 포함하는 모바일 디바이스를 포함하는 시스템.

청구항 38

제37항에 있어서,

상기 모바일 디바이스는 상기 디스플레이에 문자들의 세트를 표시하도록 구성되는 시스템.

청구항 39

제38항에 있어서,

상기 다수의 광원 중 각각 하나의 광원은 생성되는 상기 사용자 데이터의 문자를 표시하기 위해 한번씩 점등되는 시스템.

청구항 40

제38항에 있어서,

상기 다수의 광원 중 각각 하나의 광원은 생성되는 상기 사용자 데이터의 문자를 표시하기 위해 한번씩 소등되는 시스템.

청구항 41

제37항 내지 제40항 중 어느 한 항에 있어서,

상기 모바일 디바이스는, 그것이 상기 모바일 디바이스에서 생성되었을 때, 상기 사용자가 상기 사용자 데이터를 입력할 수 있도록 가상의 키패드를 표시하는 시스템.

청구항 42

제37항 내지 제40항 중 어느 한 항에 있어서,

상기 모바일 디바이스 케이스는 상기 제1항 내지 제19항에 의해 생성된 사용자 데이터가 안전하게 입력되도록 구성된 시스템.

청구항 43

모바일 디바이스 케이스를 이용하여 사용자로부터 사용자 데이터를 안전하게 입력받는 방법에 있어서, 상기 모바일 디바이스 케이스는, 마이크로 컨트롤러, 통신모듈 및 사용자가 사용자 데이터를 입력하기 위한 사용자 인

터페이스를 포함하고,

상기 방법은,

상기 마이크로 컨트롤러에서 상기 사용자 인터페이스를 통해 입력한 사용자 데이터를 수신하는 단계; 상기 모바일 디바이스 케이스의 상기 사용자 인터페이스는 상기 사용자가 상기 사용자 데이터를 입력하는 것을 가능하게 하고,

상기 마이크로 컨트롤러는 문자가 입력될 때 상기 사용자 데이터의 각각의 문자 선택에 따라 모바일 디바이스가 시각적으로 표시하도록 상기 모바일 디바이스 케이스의 내부에 수용되는 모바일 디바이스와 통신하도록 구성되고,

상기 마이크로 컨트롤러에서, 처리된 데이터를 생성하기 위해 상기 사용자 데이터를 처리하는 단계; 및

상기 마이크로 컨트롤러는 상기 사용자 데이터를 확인하거나 - 상기 확인은 (i) 상기 사용자 데이터와 상기 마이크로 컨트롤러에 저장된 암호를 비교하는 것 또는 (ii) 상기 사용자 데이터에 일방향성 함수를 적용하고, 상기 처리된 데이터에 저장된 데이터를 매칭시키는 것으로 구성되며, 상기 저장된 데이터는 상기 일방향성 함수가 적용된 상기 사용자 데이터로부터 생성됨-, 또는 상기 사용자 데이터를 암호화함으로써 상기 사용자 데이터를 처리하도록 구성되고,

상기 처리된 데이터는 상기 사용자 데이터가 확인되었는지 여부를 나타내고,

모바일 디바이스 또는 서드 파티(third party)로 상기 처리된 데이터를 출력하는 단계를 포함하는 방법.

청구항 44

모바일 디바이스 케이스를 이용하여 사용자로부터 입력받을 수 있는 사용자 데이터를 생성하고 모바일 디바이스를 수용하기 위한 방법에 있어서,

상기 사용자 데이터는 복수의 문자로 구성되고,

상기 모바일 디바이스 케이스는

마이크로 컨트롤러 및

상기 사용자 데이터의 상기 복수의 문자 각각을 상기 사용자에게 나타내는 다수의 광원을 포함하고,

상기 다수의 광원 각각은 상기 모바일 디바이스 케이스 내에 수용

되는 상기 모바일 디바이스에 디스플레이되는 복수의 문자 중 하나의 문자에 정렬되도록 구성되고,

상기 방법은,

상기 마이크로 컨트롤러에서 상기 사용자 데이터를 생성하기 위한 요청을 수신하는 단계;

상기 마이크로 컨트롤러에서 상기 사용자 데이터를 생성하는 단계; 및

상기 마이크로 컨트롤러에서 상기 사용자 데이터의 상기 복수의 문자 각각을 나타내기 위하여 상기 모바일 디바이스 케이스의 상기 다수의 광원을 순차에 따라 발광하게 제어하는 단계

를 포함하는 방법.

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 모바일 디바이스를 위한 하드웨어 기반의 사용자 인터페이스에 관한 것이다. 특히 보안 사용자 인터페이스 시스템들의 유용성과 모바일 디바이스에 안전하게 데이터를 입력하는 방법에 관한 것이다.

배 경 기 술

[0002] 스마폰, 태블릿, e-리더와 같은 모바일 디바이스들은 종종 인터넷으로 컨텐츠를 보고, 온라인으로 상품을 구입하고, 온라인 은행거래를 수행하고, 은행잔고를 확인하는데 사용된다.

[0003] 모바일 디바이스 사용자는 정기적으로 데이터를 보거나 거래를 수행하고, 데이터를 보거나 거래를 수행하는 것은 거래를 완료하기 전에 권한을 부여받기 위해 사용자에게 패스워드를 입력받는 것을 요구한다.

[0004] 그러나, 모바일 디바이스들은 종래의 PC등과 같은- 악성 소프트웨어에 감염되는 것에 취약하며, 비밀 데이터를 안전하게 입력하는 것이 어렵거나, 훼손 위험 없이 중요한 거래 데이터를 입력하는 것이 어렵다.

[0005] 모바일 디바이스가 손상된다면, 악성 소프트웨어는 상기 디바이스의 사용자에 의해 입력되는 어떠한 기밀 데이터로 기록될 수 있고, 기밀 데이터를 서드 파티(third party)로 전송할 수 있다. 또는, 사용자가 의도하지 않은 동작을 실행하기 위해 입력된 데이터를 변경하거나, 사용자를 기만하기 위해 디바이스에 표시된 데이터를 변경시킬 수 있다. (예를 들어, 사용자에게 기밀 정보를 더 입력하도록 함)

[0006] 악성 소프트웨어 공격은 자금, 개인정보 및 보안의 손실을 유발할 수 있다. 따라서, 디바이스 상의 어떠한 악성 소프트웨어도 방해할 수 없도록 디바이스에 안전하게 데이터를 입력할 수 있게 할 필요가 있다. (예를 들어, 비밀스럽게 또는 데이터의 훼손 없이)

[0007] 다수의 고객들은 모바일 디바이스들을 이용하여 자신의 온라인 은행 계좌에 접근한다. 금융기관은 고객들의 계좌가 허가 없이 접근되는 리스크를 감소시키기 위해 다수의 프로세스를 설정한다.

[0008] 예를 들어, 대부분의 기관들은 온라인 뱅킹을 위한 보안 웹사이트들(예를 들어, HTTPS 통신 프로토콜)을 사용하고, 대부분은 접근을 승인하기 위해 적어도 하나의 패스워드가 입력되는 것을 요구한다.

[0009] 다수의 은행은 계좌에 대한 접근을 제어하고, 온라인 은행 거래를 인증하기 위해 OTP 시스템을 사용한다.

[0010] 전형적으로, 고객은 패스워드를 입력해야 하고, 웹사이트에 로그인 하며, OTP(one-time password)를 입력한다. 상기 OTP는 특정한 거래에 인증하기 위해 오직 한번의 로그인 세션과 거래에 유효한 패스워드를 의미한다. OTP는 몇몇의 다른 방식으로 이용될 수 있다.

[0011] OTP는 SMS 메시지를 통해 은행으로부터 고객의 모바일 폰으로 전송될 수 있다. 만약 OTP가 SMS를 통해 고객에게 전송되는 경우, 상기 고객은 SMS를 읽기 위해 그들의 모바일 디바이스 상의 웹사이트와 SMS 어플리케이션 사이를 앞뒤로 전환해야하고, OTP를 기억하고, 이를 웹사이트에 입력해야 한다. 사용자는 이러한 방식이 불편하거나 어려운 수행방법임을 알 수 있다.

[0012] 상기 고객은 보안 토큰을 이용하여 필요할 때 OTP를 생성할 수 있다. 상기 보안 토큰은 일반적으로 클럭이나 카운터를 포함하는 하드웨어의 일부이다. 따라서, 시간 및 이벤트 순서는 OTP 생성 알고리즘의 중요한 부분이다. 대안적으로, 상기 OTP는 이하에서 보다 자세히 설명될 칩 인증 프로그램(CAP) 장치를 이용하여 고객에 의해 생성될 수 있다. 상기 OTP를 생성하는 방법에 관계없이 사용자는 온라인 거래를 완료하기 위해 OTP를 은행의 웹사이트에 입력한다.

[0013] 다수의 은행들은 온라인 은행 거래를 인증하기 위해 칩 인증 프로그램(CAP)를 사용한다. CAP는 "칩과 PIN" 은행 카드(또는 칩 카드) 및 OTP를 생성하기 위한 유효한 PIN를 모두 요구하는 두 단계의 인증 시스템이다. 그들의 온라인 은행 계좌에 로그인하는 사용자와 거래를 수행하고자 하는 사용자는(예를 들어, 계정사이에 돈을 송부하거나, 결제를 하는) 그들의 거래를 성공시키기 위해 반드시 CAP를 이용해서 생성된 OTP를 온라인 은행 시스템에 입력해야 한다. CAP는 일반적으로 카드 슬롯, 숫자 키패드 및 다수의 문자/숫자를 표시할 수 있는 디스플레이를

포함하는 핸드 헬드 디바이스 또는 CAP 리더를 필요로한다. 온라인 은행 거래를 희망하는 사용자는 그들의 "칩과 PIN" 은행 카드를 카드 슬롯에 삽입하고, 키패드를 통해 CAP리더에 그들의 PIN을 입력해야한다. 또한, 사용자는 그들이 하고자 하는 거래의 종류뿐만 아니라 세부사항을 선택할 수 있다. CAP 리더는 PIN, 은행 카드 고유 데이터 및 현재의 시간을 이용하여 숫자 패스워드(예를 들어, OTP)를 출력한다. 상기 사용자는 은행 거래를 완료하기 위해 OTP를 온라인으로 입력할 필요가 있다.

[0014] CAP는 모바일 디바이스를 통해 온라인 거래를 수행하고자하는 사용자가 CAP리더를 함께 휴대하는 것이 요구된다. 도 1은 스마트 폰(22), 스마트 폰 케이스(30), 칩과 PIN 은행 카드(또는 EMV 카드)(32) 및 CAP 리더(34)의 상대적인 크기를 나타내는 도면이다.

[0015] 도 1에 도시한 바와 같이 일반적인 CAP 리더(34)는 다수의 스마트폰(22)과 유사한 크기일 수 있다. 따라서, 사용자는 스마트 폰과 추가적인 장치를 휴대하는 것이 번거러운 것을 알 수 있다. 상기 CAP 방법은 보안 거래를 완료하기 위해 두 가지 다른 디바이스와 함께 두 가지 다른 사용자 인터페이스가 필요하므로, 사용자에게 매력적이지 못하다. 또한, CAP 리더는 특정한 은행에 관계된 거래에만 사용될 수 있고, 안전하게 패스워드를 입력하거나 비밀의 사용자 데이터의 입력을 요구하는 다른 작업을 수행하는데 이용될 수 없다.

[0016] 스마트폰들은 일반적으로 소프트웨어에 의해 보호되고, 결과적으로 스마트 폰 및 유사한 모바일 디바이스들은 아직 저장하는데 널리 사용되거나, 매우 민감한 정보를 안심하고 저장하는 것을 보장하지 못한다. 예를 들어, 스마트 폰은 직불 카드 또는 신용카드의 칩에 저장된 비밀 정보를 저장하기 위해 신뢰되지 않을 수 있다. 반면에, 직불 카드 또는 신용 카드 내의 칩은 일반적으로 충분히 안전하다고 생각된다. 스마트 폰에서 보안이 부족한 하나의 이유는 스마트 폰의 칩 또는 마이크로 프로세서가 소위 보안 요소(이론적으로 안전한 저장 및 적절한 보호를 제공할 수 있음)가 포함되어 있다는 사실에도 불구하고, 이러한 '보안요소'는 모두 전화 네트워크의 오퍼레이터에 의해 제어된다. 즉, 이러한 스마트폰 칩은 예를 들어 은행에서 실행되는 보안 거래(예를 들어, 스마트 폰을 통한 온라인 은행 거래)를 수행하기 위해 일반적으로 제공되는 소프트웨어 어플리케이션에 접근할 수 없다. 따라서, 스마트 폰의 '보안요소'는 스마트 폰이 거래를 수행하는 데 사용될 때 사용되지 않으며, 그 결과로 스마트 폰은 거래 중에 안전하고 특별하게 민감한 정보를 저장할 수 없다.

[0017] 종래기술의 정보는 EP1467275A2, US2013/0120913, US2013/0077235, US2003/0073415, US2002/0089410 및 EP1971111A2에서 찾을 수 있다.

[0018] 본 출원인은 보안 모바일 컴퓨팅의 사용자 경험을 향상시킬 필요성을 인식하고 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0019] 본 발명의 첫 번째 측면에 따르면, 사용자가 사용자 데이터를 안전하게 입력하기 위한 모바일 디바이스 케이스가 제공되며, 상기 케이스는 마이크로 컨트롤러, 모바일 디바이스 또는 서드 파티(third party)와 통신하는 통신 모듈 및 상기 사용자 데이터를 사용자가 입력할 수 있는 사용자 인터페이스를 포함한다. 바람직하게는 상기 마이크로 컨트롤러는 상기 사용자 인터페이스를 통해 사용자로부터 입력된 사용자 데이터를 받고, 처리된 데이터를 생성하기 위해 상기 사용자 데이터를 처리하며, 상기 처리된 데이터를 상기 모바일 디바이스 또는 상기 서드 파티로 전송하도록 구성된다.

[0020] 본 발명의 두 번째 측면에 따르면, 모바일 디바이스 케이스에 사용자로부터 사용자 데이터를 입력하는 방법을 제공하며, 상기 모바일 디바이스 케이스는 마이크로 컨트롤러, 통신 모듈 및 상기 사용자가 사용자 데이터를 입력할 수 있는 사용자 인터페이스를 포함한다.

[0021] 상기 두 가지 측면에 따르면, 상기 사용자 데이터는 상기 사용자 인터페이스를 통해 입력되는 상기 사용자 데이터가 상기 모바일 디바이스 또는 서드 파티에 의해 해석되는 일 없이 상기 모바일 디바이스 또는 서드파티에 안전하게 전송된다. 예를 들어, 상기 모바일 디바이스와 서드파티는 무작위 데이터로부터 입력된 사용자 데이터를 구별할 수 없다. 하기의 특징은 본 발명의 두 가지 측면에 적용된다.

[0022] 상기 사용자 데이터는 패스워드(PIN들과 패스코드를 포함), 또는 수취인 세부사항과 같은 민감한 거래 데이터를

포함한다. 상기 사용자 데이터는 숫자 또는 예를 들어 알파벳 문자와 같은 다른 문자를 포함할 수 있다. 상기 사용자 데이터는 상기 모바일 디바이스에 실행되는 어플리케이션에 안전하게 입력될 수 있다. (예를 들어, 게임, 웹 브라우저, 오피스 제품군 등) 대안적으로, 상기 사용자 데이터는 서드 파티로 안전하게 전송될 수 있다. 상기 서드 파티는 예를 들어, 은행 또는 상점과 같은 사용자 데이터가 필요한 어떠한 당사자일 수 있고, 또는 이러한 서드 파티들로부터 분리된 인증 서비스 일수 있다.

[0023] 상기 케이스는 사용자가 사용자 데이터를 케이스에 직접 또는 모바일 디바이스를 통해 비직접적으로 입력하는 사용자 인터페이스를 포함한다. 이러한 방식은 아래에서 보다 자세히 설명하겠지만 상기 모바일 디바이스를 키보드로 사용하는 것은 피한다. 상기 모바일 디바이스에 존재하는 악성 소프트웨어는 상기 모바일 디바이스가 문자를 직접적으로 받는 것이 아니라 상기 문자들이 상기 케이스에 통합된 하드웨어를 이용하여 시스템에 입력되고, 상기 모바일 디바이스에 입력된 어느 데이터도 알려지지 않은 초기 데이터와 연관되어 있기 때문에 사용자에 의해 입력되는 문자를 알지 못한다. 또한, 상기 사용자 데이터는 상기 모바일 디바이스 또는 서드파티로 전송되기 전에 상기 케이스의 상기 마이크로 컨트롤러에 의해 처리되며, 상기 사용자 데이터는 상기 케이스로부터 깨끗하게 수신되지 않는다. 즉, 상기 사용자 데이터는 처리된 데이터로부터 결정되지 않는다.

[0024] 이러한 작업을 위해서, 상기 케이스는 신호들이 상기 모바일 디바이스에 알려지지 않도록 신호들을 사용자에게 보내야만 한다. 첫 번째 옵션은 상기 케이스의 상기 사용자 인터페이스가 어떠한 문자가 현재 선택되었는지 표시하는 적어도 하나의 시각적 인디케이터를 가지도록 하는 것이다. 상기 시각적 인디케이터는 예를 들어 LED와 같은 적어도 하나의 광원을 포함한다. 이러한 광원들은 케이스의 무게 또는 크기를 크게 증가시키지 않도록 작은 크기로 상기 케이스에 통합된다. 예를 들어, 0에서 9까지의 각각의 번호에 대한 하나에 대한 다수의 광원을 포함한다. 상기 다수의 광원은 점등에 의해 상기 사용자 데이터의 어떤 문자가 선택되었는지 나타내기 위해 한 번에 하나씩 점등할 수 있다. 대안적으로 다수의 광원은 입력을 위해 선택된 상기 사용자 데이터의 어떠한 문자가 선택되었는지를 소등에 의해 나타내기 위해 하나를 제외하고는 모두 발광할 수 있다. 대안적으로 다른 색상의 광원들은 입력을 위해 어떠한 문자가 선택되었는지를 보여주는데 사용될 수 있다. 예를 들어, 녹색은 선택된 문자를 위한 것이고, 빨간색은 다른 문자들을 위한 것일 수 있다. 다시 말해, 하나의 광원은 어떠한 문자가 선택되었는지를 나타내기 위해 다른 것들과 다를 수 있다. 상기 광원은 상기 케이스의 하나 이상의 측을 따라 배치될 수 있다. 바람직하게는 각각의 광원은 케이스 상에 보이거나 모바일 디바이스 스크린에 표시된 문자와 정렬될 수 있다.

[0025] 상기 사용자 인터페이스는 사용자가 상기 사용자 데이터의 각각의 문자를 입력하기 위한 터치 메커니즘을 포함한다. 예를 들어, 다수의 광원이 있고, 상기 터치 메커니즘은 상기 사용자가 광원이 발광함에 따라 변경할 수 있도록 하는 터치센서를 포함할 수 있다. 상기 사용자의 손가락의 움직임은 상기 터치센서에 의해 감지되고, 발광 광원의 순환을 유발한다. 예를 들어, 한 방향으로 스와이프하거나 터치센서를 누르는 등의 움직임에 의한다. 상기 사용자는 순환을 시작하기 위해 상기 센서를 터치 하고, 이후 원하는 광원이 주기적으로 발광하면 그들의 손가락을 이탈시킴으로써 상기 사용자 데이터의 문자를 선택할 수 있다. 그리고/또는 원하는 광원이 켜지면 센서를 탭함으로써 사용자 데이터의 문자를 선택할 수 있다.

[0026] 부가적으로 또는 대안적으로 상기 터치 메커니즘은 상기 사용자 데이터의 문자와 각각 대응되는 다수의 터치센서를 포함할 수 있다. 이러한 방식에서, 상기 시각적 인디케이터는 사용자가 단순히 문자를 입력하기 위해 정확한 터치센서를 누를 수 있는 단순히 각각의 터치센서에 인접하거나 터치센서 상의 문자일 수 있다. 만약 사용자 인터페이스가 다수의 광원을 포함하는 경우 각각의 광원은 터치 센서에 인접할 수 있다. 복수의 센서는 각각의 광원이 센서나 센서 버튼에 대응될 수 있도록 케이스 상에 배열되어 제공될 수 있다. 상기 사용자는 문자선택을 위해 원하는 광원과 연관된 센서를 탭할 수 있다.

[0027] 이러한 방법에서, 상기 케이스 상의 터치 메커니즘은 사용자 데이터를 입력하는데 사용되고, 상기 모바일 디바이스는 어떠한 문자가 선택되었는지 알 수 없고, 상기 보안 마이크로 프로세서에서 처리된 데이터 또한 알 수 없다. 따라서, 상기 사용자 데이터의 입력 프로세스는 상기 모바일 디바이스로부터 숨겨진다. 상기 센서는 용량성 센서일 수 있다. 즉, 다수의 랩탑 터치패드에 사용되는 기술과 유사할 수 있다.

[0028] 상기 사용자 인터페이스의 대안으로 터치 메커니즘으로 구성될 수 있고, 상기 사용자 인터페이스는 통신모듈을 통해 모바일 디바이스로부터 조정 데이터를 수신하도록 구성될 수 있다. 상기 조정 데이터는 보안 케이스에 의해 표시되는 선택된 값의 원하는 변경을 나타낼 수 있다. 예를 들어, 다수의 광원이 있는 방법에서, 상기 모바일 디바이스의 스크린 상의 수직적인 터치 제스처는 광원이 발광하는 순환에 이용될 수 있다. 이러한 방법에서, 사용자는 상기 모바일 디바이스 자체의 터치스크린을 이용함으로써 입력되는 데이터가 표시되는 절대값 없이 발

광 광원을 바꿀 수 있다.

[0029] 이러한 사용자 데이터 입력방법은 상기 모바일 디바이스의 키보드를 이용하여 문자를 입력하는 방법보다 안전할 수 있다. 상기 모바일 디바이스의 악성 소프트웨어는 상기 스크린 상에 표시되는 문자들을 볼 수는 있으나 상기 광원은 케이스의 일부이지 상기 모바일 디바이스의 일부가 아니므로 어떠한 광원이 발광하는지를 볼 수 없다. 다만, 상기 모바일 디바이스 및 디바이스에 실행되는 어떤 악성 소프트웨어는 사용자의 손가락의 움직임에 의해 상기 사용자 데이터에 대한 정보(제한적이긴 하지만)를 얻을 수 있다. 따라서, 향상된 보안은 마이크로 컨트롤러가 단일 무작위적으로 선택된 광원의 발광을 유도하는 것에 의해 제공될 수 있고, 단일 무작위적으로 선택된 광원을 스위치 오프 시키는 것을 유도하는 것에 의해 제공될 수 있다. 무작위적인 광원은 최대의 안전을 위해 상기 사용자 데이터의 각각의 문자가 입력되기 전에 선택될 수 있고, 또는 최소한 첫 번째 문자가 입력되기 전에 선택될 수 있다. 상기 무작위적으로 선택된 광원은 임의의 '초기위치'를 나타낸다. 상기 사용자는 단순히 원하는 문자 옆의 스크린을 터치할 수 없다. - 그들은 원하는 숫자에 도달할 때까지 초기위치로부터 문자들을 통해 순환되어야 한다. 상기 스크린 상의 상기 사용자 손가락의 초기위치 및 상기 스크린을 따라 움직이는 거리는 상기 모바일 디바이스에 알려질 수 있다. 또는, 상기 디스플레이 스크린은 문자들의 세트를 표시하도록 구성될 수 있고, 각각의 문자는 다수의 광원 중 하나와 정렬될 수 있다. 상기 사용자 인터페이스는 추가적으로 각각의 광원과 정렬된 문자의 특성을 포함하는 문자 데이터를 수신할 수 있다. 표시된 문자들의 세트는 사용자 인터페이스가 각각의 광원과 정렬된 문자를 나타내는 문자 데이터를 오직 한번 수신하는 경우 고정될 수 있다. 대안적으로, 표시된 문자들의 세트는 변경될 수 있다. 예를 들어, 입력될 수 있는 데이터의 다양성을 허가하기 위해 표시된 문자들의 세트는 변경될 수 있다. 이러한 방법에서, 문자들의 세트에 대한 업데이트는 상기 사용자 인터페이스에 전송되는 것이 필요하다. 다시 이러한 문자데이터는 바람직하게는 마이크로 컨트롤러에 전송되고, 상기 마이크로 컨트롤러는 데이터를 처리한다. 상기 마이크로 컨트롤러는 상기 문자 데이터에서 어떤 문자가 선택되었는지 판정하도록 구성될 수 있다. 다만, 상기 모바일 디바이스와 케이스는 모두 상기 사용자 데이터를 입력하기 위해 사용되고, 상기 케이스와 상기 모바일 디바이스에서 일어나는 과정은 상기 디스플레이 상의 세트로부터 사용자가 선택된 것이 어떠한 문자인지 알지 못한다.

[0030] 예를 들어, 전체의 PIN과 같은 사용자 데이터가 입력되면, 상기 케이스의 마이크로 컨트롤러는 상기 사용자 데이터를 처리한다. 예를 들어, 상기 마이크로 컨트롤러는 수신한 숫자들에 수학적인 함수를 적용한다. 상기 과정은 사용자에 의해 입력된 사용자 데이터의 문자와 처리된 데이터를 확인하는 것을 포함할 수 있다. 상기 처리된 데이터는 확인의 결과로 출력된 것일 수 있다. 상기 확인과정은 상기 사용자 데이터의 전달받은 문자와 상기 마이크로 컨트롤러에 저장된 패스워드를 비교하고, 전달받은 문자와 저장된 패스워드의 일치를 판정하는 과정을 포함할 수 있다. 따라서, 이러한 방법에서는 적용되는 수학적 함수가 간단한 매칭 과정일 수 있다. 대안적으로, 상기 마이크로 컨트롤러는 암호화된 해시 함수 또는 유사한 일방향성 함수를 전달받은 문자들에 적용하도록 구성될 수 있다. 해시함수의 출력은 출력된 값이 저장된 값에 매칭되는지를 판정하기 위해 상기 마이크로 컨트롤러에 저장된 해시 값(또는 동일하게 입력된 사용자 데이터에 동일한 일방향성 함수를 이용하여 계산된 값)을 비교할 수 있다. 일방향성 함수를 이용하는 장점은 상기 케이스가 접근가능한 형태로 상기 사용자 데이터를 저장하지 않고 동일한 사용자 데이터가 입력되며 저장된 값과 동일한 값을 항상 재생산하는 것에 있다. 만약 상기 사용자 데이터(해시되거나 해시되지 않거나)가 일치하지 않으면, 상기 사용자는 사용자 데이터를 수정하여 입력하기 위한 정해진 횟수의 기회를 허가 받고, 정확한 데이터가 정확히 입력되지 않는 경우 상기 사용자는 거래를 완료하는 것에 대해 배제 및/또는 차단될 수 있다.

[0031] 추가적으로 또는 대안적으로, 상기 마이크로 컨트롤러는 상기 마이크로 컨트롤러에 저장된 암호화키를 이용하여 전달받은 수치적 문자를 암호화하도록 구성될 수 있다. 상기 암호화된 데이터는 서드 파티에 의해 해석 및 확인될 수 있다. 이러한 방법에서, 상기 모바일 디바이스 케이스는 그 자체로 전달받은 수치적 문자를 확인하지 않고, 인증을 위해 상기 전달받은 수치적 문자를 서드 파티에 전송할 수 있다. (예를 들어, 모바일 디바이스의 통신모듈을 통해) 상기 암호화 키는 공개 키일 수 있고, 상기 서드 파티는 암호화된 데이터를 해독하는데 개인키를 사용할 수 있고, 상기 사용자 데이터가 서드 파티에 알려진 정확한 사용자 데이터와 일치하는지를 판정한다. 이러한 시나리오에서, 시스템에는 사용자 특성 데이터가 저장될 필요가 없으므로, 보안은 향상된다.

[0032] 상기 시스템은 적어도 전달받은 사용자 데이터를 일회용 패스워드(OTP) 또는 거래 인증 번호(TAN)과 같은 보안 토큰을 생성하는데 사용되도록 구성될 수 있다. 보안 토큰의 생성은 수신된 데이터에 카운트, 현재시간, 상기 모바일 디바이스에 실행되는 어플리케이션의 종류와 관련된 데이터, 모바일 디바이스의 종류와 관련된 데이터 및/또는 사용자 특성 데이터와 같은 추가되는 인증 데이터를 더 필요할 수 있다.

[0033] 상기 보안 토큰 생성에 카운트가 필요한 경우, 상기 케이스는 카운트를 제공하기 위한 카운터를 더 포함할 수

있다. 유사하게, 상기 보안 토큰 생성에 현재 시간이 필요한 경우, 상기 케이스는 클럭(clock)을 더 포함할 수 있다. 상기 클럭은 패스워드를 요청하는 어플리케이션과 연결된 인증 서버의 클럭과 동기화될 수 있다.

[0034] 상기 토큰 생성이 사용자 특성 데이터를 포함하는 경우 상기 인증 데이터는 스마트 카드로부터 판독한 데이터로부터 얻을 수 있다. (예를 들어, "칩 및 핀" 카드 또는 EMV 카드) 따라서, 상기 케이스는 이전에 설명한 CAP리더와 유사한 기능을 수행하도록 구성될 수 있다. 따라서, 상기 케이스는 상기 케이스에 통합된 스마트 카드 리더를 더 포함할 수 있고, 또는 상기 케이스에 통합된 비접촉식 스마트 카드리더를 더 포함할 수 있다. 대안적으로, 상기 케이스의 마이크로 컨트롤러는 실제로 본 발명의 추가적인 기능이 있는 내장된 EMV 칩일 수 있다.

[0035] 상기 시각적 인디케이터는 시스템의 보안 모드를 나타내도록 사용될 수 있다. 예를 들어, 상기 시각적 인디케이터는 상기 케이스가 무결점 또는 비밀 보호 모드인지를 나타낼 수 있다. 예를 들어, 다수의 LED가 있고, 다수의 LED는 다색광 LED일 수 있다. 광원의 하나의 색상(예를 들어, 녹색)은 상기 사용자 데이터가 패스워드 입력에 적절하도록 모바일 디바이스에 보통문자로 절대 나타나지 않는 비밀 보호모드를 나타낼 수 있다. 다른 색상은 거래 수취 또는 입금에 적절하도록 상기 모바일 디바이스가 보통문자로 데이터 값을 알 수 있지만 탐지없이 변경할 수 없는 무결성 보호 모드를 나타낼 수 있다. 상기 마이크로 컨트롤러는 적절하게 상기 LED의 색상을 변경하도록 구성될 수 있다.

[0036] 상기 모바일 디바이스의 케이스는 모바일 디바이스와 함께 사용되도록 디자인될 수 있고, 바람직하게는 부착과 이탈이 가능하도록 디자인 될 수 있다. 일반적으로, 상기 모바일 디바이스는 상기 모바일 디바이스 케이스에 수용되거나 상기 모바일 디바이스의 적어도 일부가 커버될 수 있다. 따라서, 본 발명의 다른 측면에서, 설명된 시스템은 상술한 모바일 디바이스 케이스와 디스플레이 및 모바일 디바이스 케이스와 통신하는 통신모듈로 구성된 모바일 디바이스를 포함할 수 있다. 바람직하게는 상기 사용자 데이터가 입력 가능하도록 상기 모바일 디바이스와 상기 모바일 디바이스 케이스는 서로 상호작용하고, 통신할 수 있다. 다만, 상술한 바와 같이 상호작용은 상기 모바일 디바이스에 사용자 데이터가 보통문자로 입력되는 것을 방지하도록 설계될 수 있다.- 또는 상기 모바일 디바이스에 의해 어떠한 방식으로든 해석되는 것을 방지할 수 있다.

[0037] 대안적으로, 상기 모바일 케이스의 기능은 실제로 상기 모바일 디바이스에 내장된 추가적인 특징으로 제공될 수 있다. 상기 모바일 디바이스 케이스와 모바일 디바이스는 완전히 통합될 수 있다. 상기 모바일 디바이스 케이스는 표준적인 모바일 폰의 케이스의 전체 또는 일부로 물리적으로 대체될 수 있다. 대안적으로, 상기 시스템은 상술한 물리적인 모바일 케이스의 기능이 상기 모바일 디바이스에 추가되어 가상의 모바일 디바이스 케이스로 구성될 수 있다. 상기 케이스와 모바일 디바이스가 통합되면, 두개의 분리된 프로세서가 필요하다. 즉, 표준화된 프로세서는 모바일 디바이스의 기능을 제어하고, 독립적이고 분리된 마이크로 컨트롤러는 상술한 상기 모바일 디바이스 케이스의 기능을 제공한다.

[0038] 상기의 또는 각각의 프로세서는 마이크로 프로세서, 디지털 신호처리 칩(Digital Signal Processing, DSP), 주문형 반도체(Application Specific Integrated Circuit, ASIC), 필드 프로그래머블 게이트 어레이(Field Programmable Gate Arrays, FPGAs) 등과 같이 알려진 적절한 하드웨어로 실행될 수 있다. 상기의 또는 각각의 프로세서는 각각의 코어가 독립적으로 동작하도록 하나 이상의 처리코어를 포함할 수 있다. 상기의 또는 각각의 프로세서는 실행명령과 버스로 연결될 수 있고, 예를 들어 메모리와 같은 곳에 저장된 정보를 처리할 수 있다.

[0039] 상기 모바일 디바이스는 상기 디스플레이에 문자들의 세트를 표시하도록 구성될 수 있다. 상기 케이스는 다수의 광원을 포함하고, 문자는 각각의 광원과 정렬되어 표시될 수 있다. 상술한 바와 같이 상기 모바일 디바이스는 상기 모바일 디바이스의 터치센서를 이용하여 어떠한 광원이 발광할지를 제어하는 것을 사용자에게 허가할 수 있다. 예를 들어, 상기 시스템의 사용자는 발광되는 LED와 인접한 상기 스크린의 한 점에서 시작하여 상기 터치스크린을 스와이프 함으로써 상기 표시된 문자들로부터 상기 사용자 데이터의 각각의 문자를 선택할 수 있다. 상기 케이스는 상기 모바일 디바이스의 배면을 보호할 수 있고, 상기 모바일 디바이스의 측면을 따라 상기 모바일 디바이스가 해제가능하도록 고정될 수 있다.

[0040] 상기 모바일 디바이스와 모바일 디바이스 케이스가 상호작용하는 다른 방법이 있다. 예를 들어, 본 발명의 또 다른 측면에서, 상기 사용자에 의해 모바일 디바이스로 입력되는 사용자 데이터가 생성되도록 모바일 디바이스 케이스가 제공되고, 상기 케이스는 마이크로 컨트롤러와 사용자에게 생성된 사용자 데이터를 표시하기 위한 사용자 인터페이스를 포함한다. 상기 마이크로 컨트롤러는 상기 사용자 데이터를 생성하기 위한 요청을 수신하기 위해 구성되고, 상기 사용자 데이터를 생성하고, 상기 사용자 인터페이스에 상기 사용자 데이터를 표시한다. 이러한 방법에서, 상기 케이스는 TAN 및/또는 OTP를 생성한다. 상기 사용자 데이터의 생성은 사용자에 의해 요청되고, 서드 파티(예를 들어, 모바일 폰을 통해)에 의해 요청될 수 있다.

[0041] 상기 사용자 데이터의 생성은 카운트, 현재시간, 모바일 디바이스에 실행되는 어플리케이션의 종류, 모바일 디바이스의 종류 및/또는 사용자 특성 데이터와 같은 인증데이터를 이용하는 것이 요구될 수 있다.

[0042] 만약, 사용자 데이터의 생성이 카운트를 필요로 하는 경우, 상기 케이스는 카운트를 제공하는 카운터를 더 포함할 수 있다. 유사하게, 상기 사용자 데이터의 생성이 현재시간을 필요로 하는 경우, 상기 케이스는 클럭을 더 포함할 수 있다. 상기 클럭은 상기 사용자 데이터를 요청한 어플리케이션과 연결된 인증서버의 클럭과 동기화될 수 있다.

[0043] 상기 사용자 데이터의 생성이 사용자 특성 데이터를 포함하는 경우 상기 인증 데이터는 스마트 카드로부터 판독한 데이터로부터 얻을 수 있다. (예를 들어, "칩 및 핀" 카드 또는 EMV 카드) 따라서, 상기 케이스는 이전에 설명한 CAP리더와 유사한 기능을 수행하도록 구성될 수 있다. 따라서, 상기 케이스는 상기 케이스에 통합된 스마트 카드 리더를 더 포함할 수 있고, 또는 상기 케이스에 통합된 비접촉식 스마트 카드리더를 더 포함할 수 있다. 대안적으로, 상기 사용자 특성 데이터는 케이스에 저장될 수 있다. (아마도 영구적으로) 예를 들어, 보안 메모리에 저장될 수 있다.

[0044] 상기 사용자 인터페이스는 사용자에게 생성된 사용자 데이터를 위한 문자를 표시하기 위한 하나 이상의 시각적 인디케이터를 포함할 수 있다. 상기 시각적 인디케이터는 예를 들어, 상술한 LED들과 같이 하나 이상의 광원을 포함할 수 있다. 상기 다수의 광원은 각각의 발광광원이 상기 사용자 데이터의 각각의 순차적인 문자를 나타냄에 따라 순차적으로 한번씩 발광될 수 있다. 상기 광원은 상기 케이스의 하나 이상의 측을 따라 배치될 수 있다. 각각의 광원은 상기 모바일 디바이스 자체에 표시되는 문자에 정렬될 수 있다. 대안적으로, 상기 케이스는 문자와 대응되는 광원이 나타내는 정보를 포함할 수 있다. (예를 들어, 광원들과 인접한 문자들)

[0045] 상기 생성된 사용자 데이터는 상기 사용자 데이터가 생성된 상기 모바일 디바이스에 입력될 수 있다. 따라서, 본 발명의 다른 측면에 따르면, 모바일 디바이스 케이스는 상술한 사용자 데이터를 생성하도록 제공되고, 모바일 디바이스는 디스플레이를 포함한다.

[0046] 상기 모바일 디바이스는 디스플레이에 문자들의 세트를 표시하도록 구성될 수 있다. 또한, 이전 실시 예와의 연관성에서 상세히 설명한 바와 같이 상기 모바일 디바이스 케이스는 다수의 광원 중 하나와 정렬되는 각각의 표시되는 문자와 다수의 광원을 포함한다. 이전의 실시 예와 다른 점은 상기 광원들이 상기 사용자 데이터의 어떤 문자들이 생성되었는지를 표시하는데 이용되는 것이다. 예를 들어, 상기 케이스에 통합된 상기 LED들은 상기 마이크로 컨트롤러에 의해 생성된 패스워드를 보여주기 위해 순차적으로 반짝일 수 있다.

[0047] 상기 모바일 디바이스는 상기 모바일 디바이스에서 생성된 상기 사용자 데이터를 상기 사용자가 입력하기 위한 가상의 키패드를 표시할 수 있다. 상기 가상의 키패드는 광원들과 인접하도록 표시된 문자들과 동일할 수 있고, 또는 별도의 키패드일 수 있다. 예를 들어, 상기 사용자는 상기 모바일 디바이스의 터치패널에 표시된 가상의 키패드 상의 버튼을 탭할 수 있고, 상기 키패드 버튼은 상기 광원들과 정렬될 수 있다. 상기 사용자가 각각의 반짝이는 광원과 대응되는 적절한 키패드 버튼을 터치함으로써 상기 사용자는 사용자 데이터를 입력할 수 있다. 예를 들어, 상기 사용자는 복수 자리수의 숫자 코드를 반짝거리는 광원을 따라함으로써 입력할 수 있다. 상기 사용자는 패스워드의 생성과 입력을 위해 디바이스들 간에 전환할 필요가 없고, 상기 코드의 어떠한 숫자도 기억하지 않아도 되는 장점이 있다. 또한, 상기 케이스와 상기 모바일 디바이스 간의 어떠한 통신(무선이든 다른 방법이든)도 필요하지 않다. 또한, 상기 모바일 디바이스의 디스플레이 스크린 상의 가상의 키보드 옆에 광원이 배열되면, 상기 사용자에게 사용자 데이터를 입력하는 과정은 간단해진다.

[0048] 상기 사용자 데이터는 상술한 보안 방법을 이용하여 입력될 수 있고, 상기 발명의 두 가지 관점이 결합될 수 있는 것은 이해할 수 있을 것이다.

[0049] 상술한 모든 실시 예에서, 상기 모바일 디바이스는 사용자에게 보안 데이터 입력을 요청하도록 구성된 어플리케이션이 실행될 수 있는 모바일 폰, 스마트 폰, 태블릿 컴퓨터 또는 다른 어떤 전자기기 일 수 있다. 상기 케이스는 상기 모바일 디바이스에 부착될 수 있는 어떠한 구성요소일 수 있다. 예를 들어, 상기 케이스는 상기 모바일 디바이스의 배면의 전체 또는 일부를 덮는 커버일 수 있다. 대안적으로, 상기 케이스는 상기 모바일 디바이스의 하나 이상의 측면에 단지 부착될 수 있다.

[0050] 상기 통신 모듈은 상기 케이스가 상기 모바일 디바이스와 무선으로 통신할 수 있는 무선 통신 모듈일 수 있다. 상기 무선 통신 모듈은 블루투스 칩 또는 저전력 블루투스 칩일 수 있다.

[0051] 본 발명은 상술한 시스템과 방법을 구현하기 위한 프로세서 제어 코드를 제공하고, 예를 들어, 일반적인 목적의

컴퓨터 시스템 또는 디지털 신호처리장치(digital signal processor, DSP)일 수 있다. 본 발명은 실행시 전술한 모든 방법을 구현하는 프로세서 제어 코드를 전달하는 매체를 제공할 수 있다. 특히 상기 매체는 디스크, 마이크로 프로세서, CD와 같은 비일시적 데이터 매체, DVD-ROM, 판독전용 메모리(ROM, Firmware)와 같은 프로그램된 메모리 또는 광학적 또는 전기적으로 신호를 전달하는 데이터 매체 일 수 있다. 상기 코드는 디스크, 마이크로 컨트롤러, CD- , DVD-ROM, 비휘발성 메모리(예를 들어, Flash)와 같은 프로그램된 메모리 또는 판독전용 메모리(ROM, Firmware)에 의해 제공될 수 있다. 본 발명의 실시 예를 구현하기 위한 코드(및/또는 데이터)는 소스를 포함할 수 있고, 상기 코드는 C, 어셈블리 코드, 주문형 반도체((Application Specific Integrated Circuit, ASIC)를 설정하거나 제어하기 위한 코드, 필드 프로그래머블 게이트 어레이(Field Programmable Gate Arra, FPGA), 베릴로그(Verilog™)와 같은 하드웨어 기술언어 또는 VHDL (Very high speed integrated circuit Hardware Description Language)와 같은 종래의 프로그램 언어로 프로그램된(해석되거나 컴파일된) 목적코드 또는 실행코드를 포함할 수 있다. 통상의 기술자는 이러한 코드 및/또는 데이터를 이해할 수 있고, 상기 데이터는 다른 구성들과 통신하는 다수의 연결된 구성요소로 분산될 수 있다. 본 발명은 상기 시스템의 구성요소의 하나 이상과 연결되는 마이크로 프로세서, 작업 메모리 및 프로그램 메모리를 포함하는 컨트롤러로 구성될 수 있다.

[0052] 물리적 또는 가상의 모바일 디바이스에서 동작하는 상기 소프트웨어는 바람직하게는 상기 모바일 디바이스 또는 서드 파티와 같은 동일한 구성에 의해 다시 프로그래밍되거나 개발되지 않는다. 이것은 상기 케이스를 위한 소프트웨어는 간단하지만 모바일 디바이스 자체에서 실행되는 다른 소프트웨어보다 높은 보안 표준으로 개발된다는 것을 의미한다.

발명의 효과

[0053] 본원 발명은 모바일 디바이스의 케이스를 제공한다. 상기 케이스는 상기 모바일 디바이스와 통신하도록 구성될 수 있고, 형성되는 PIN이나 패스워드를 모바일 디바이스에 실행중인 어플리케이션에 안전하게 입력할 수 있다.

도면의 간단한 설명

[0054] 본 발명은 예시적인 방법으로 개략적으로 도시되고, 첨부된 도면은 하기와 같다.

도 1은 스마트 폰, 스마트 폰 케이스, 은행 카드 및 CAP 리더의 연관되는 크기를 도시한다.

도 2는 모바일 디바이스 및 모바일 디바이스 케이스를 포함하는 보안 사용자 인터페이스 시스템의 개략도를 도시한다.

도 3a는 도 2의 보안 거래가 수행되는 시스템의 하나의 측면을 도시한다.

도 3b는 도 3a의 시스템에서 패스워드를 입력하는 단계를 나타내는 순서도이다.

도 4a는 터치패드를 포함하는 모바일 디바이스 케이스를 포함하는 대안적인 보안 사용자 인터페이스 시스템을 도시한다.

도 4b는 별개의 터치패드 버튼들을 포함하는 모바일 디바이스 케이스를 포함하는 대안적인 보안 사용자 인터페이스 시스템을 도시한다.

도 4c 및 도 4d는 도 4a 및 도 4b 각각의 시스템에서 패스워드를 입력하는 단계를 나타내는 순서도이다.

도 5는 본 발명의 보안 사용자 인터페이스 시스템을 이용한 일반적인 패스워드를 입력하는 일반적인 단계를 나타내는 순서도이다.

도 6은 보안 사용자 인터페이스 시스템을 이용한 안전하게 PIN을 입력하는 것이 필요한 특정의 온라인 은행 거래를 수행하는 단계를 나타내는 순서도이다.

도 7은 사용자를 위한 PIN을 생성하는 단계를 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0055] 대체로, 본원 발명은 모바일 디바이스의 케이스를 제공한다. -분리되거나 실제로 스마트폰에 부착물로 만들어질 수 있고, 하나의 향상된 유닛에 모두 통합될 수 있음- 상기 케이스는 상기 모바일 디바이스와 통신하도록 구성될 수 있고, 형성되는 PIN이나 패스워드를 모바일 디바이스에 실행중인 어플리케이션에 안전하게 입력할 수 있다. 상기 어플리케이션은 상기 디바이스에 실행중인 어떠한 어플리케이션일 수 있다. 예를 들어, 게임, 웹 브라

우저, 오피스 제품군 등일 수 있다. 본 발명은 아래에서, 주로 사용자의 모바일 디바이스에 실행되는 웹 브라우저를 통한 온라인 은행 거래를 수행하는 사용자의 예를 들어 설명한다. 그러나, 온라인 뱅킹은 단지 하나의 예가 될 뿐이고, 상기 시스템은 다른 어떤 서드 파티와의 보안통신에 적용될 수 있다 예를 들어, 보안 인터넷 쇼핑 또는 실제 상점의 판매시점관리(POS) 단말기에 적용될 수 있다.

[0056] 설명한 바와 같이 사용자가 그들의 모바일 디바이스를 이용하여 온라인 은행 거래를 수행하고 싶어하는 경우 상기 사용자는 일반적으로 웹 브라우저를 이용하여 그들의 계좌에 접근한다. 상기 사용자는 은행의 온라인 은행 서비스의 보안 영역으로 접근하기 위해 상기 모바일 디바이스의 키보드를 이용하여 PIN 또는 패스워드를 입력하고, 온라인 은행 거래를 완료하기 위해 두 번째 패스워드나 OTP를 입력한다. 그러나, 악성 소프트웨어가 모바일 디바이스에 실행된다면 상기 악성 소프트웨어는 키보드 입력(가상 또는 실제)을 검출하거나 가로챌 수 있다. 그리고/또는 상기 악성 소프트웨어는 모바일 디바이스의 디스플레이에 어떤 것이 입력되는지 볼 수 있다. 따라서, 상기 악성 소프트웨어는 권한 없이 접근할 수 있는 사용자 계좌 및/또는 비인가 거래를 수행할 수 있는 상기 사용자의 개인정보에 이용되는 상기 사용자의 비밀 PIN 또는 패스워드를 감지할 수 있다. (하기에서는 패스워드, 패스코드, 암호, PIN 및 OTP는 교환적으로 사용될 수 있다.)

[0057] 본 발명은 상기 모바일 디바이스의 키보드를 사용하지 않고 사용자에게 패스워드 입력을 요구함으로써 이러한 문제의 해결책을 제공한다. 또한, 일부의 접근에서는, 패스워드 숫자가 상기 모바일 디바이스 디스플레이에 표시되지 않는다.(심지어 간단하게라도) 이러한 것은 상기 케이스에 통합된 하드웨어를 이용하여 상기 사용자에게 상기 사용자의 패스워드에 대응되는 숫자들을 입력하게 함으로써 달성될 수 있고, 상기 모바일 디바이스의 키보드 사용을 피할 수 있다. 따라서, 상기 모바일 디바이스에서 실행되는 악성 소프트웨어는 상기 사용자가 입력하는 숫자를 알 수 없다.

[0058] 최근의 모바일 디바이스 상점에는 다수의 커버들이나 케이스들이 있다. 이러한 것들은 일반적으로 상기 모바일 디바이스의 전체나 주변영역에 대한 보호를 제공한다. (예를 들어, 스크래치로부터 모바일 디바이스를 보호함) 도 1은 예시적인 모바일 디바이스(22) 및 종래의 상기 디바이스에 부합되는 케이스(30)를 도시한다. 부합되는 케이스들은 특정한 모바일 디바이스들에 맞도록 디자인된다. 상기 케이스들은 일반적으로 슬롯들 또는 상기 모바일 디바이스의 버튼들에 접근이 가능하게 하는 구멍들, 카메라 렌즈들, 헤드 폰 및 충전용 소켓들 등을 포함한다. 통상적으로 상기 모바일 디바이스는 부합되는 케이스에 삽입되어, 상기 케이스가 충격으로부터 상기 폰의 배면과 측면을 보호하고; 폰의 전면을 사용자가 시인 가능하고, 접근 가능하도록 한다. 상기 케이스는 예를 들어, 경질 폴리머 재료, 고무 또는 비닐과 같은 충격 흡수 물질로 형성될 수 있다. 상기 보호 케이스들은 일반적으로 어떠한 추가적인 기술적 기능을 수행하지 않는다.

[0059] 도 2는 모바일 디바이스를 위한 보안 사용자 인터페이스 시스템(10)의 개략도이다. 상기 보안 사용자 인터페이스 시스템(10)은 종래의 케이스들과 일반적으로 유사한 사이즈, 물질 및 모양을 가지는 모바일 디바이스(22)에 대한 케이스(12)를 포함한다. 도 1에 도시된 알려진 케이스들과 달리, 본 발명은 하드웨어적 구성요소를 포함하고, 예를 들어, 인터넷 은행 거래와 같은 동작을 수행할 때 상기 케이스 내부에 유지되는 상기 모바일 디바이스(22)에 보안 패스워드 입력이 가능하도록 통신할 수 있는 케이스(12)를 제공한다. 상기 케이스(12)는 또한 표준 커버와 같은 보호를 제공할 수 있다. 상기 케이스(12)는 상기 사용자가 시인 가능하고 접근 가능하도록 상기 모바일 디바이스의 스크린과 상기 모바일 디바이스의 배면에 존재할 수 있는 카메라를 제외하고, 상기 모바일 디바이스의 배면과 측면의 전체 또는 일부를 덮을 수 있다.

[0060] 상기 모바일 디바이스(22)는 예를 들어, 디스플레이 스크린(28), 중앙 처리 유닛(CPU, 26) 및 통신 모듈(24)과 같은 다수의 표준 구성요소를 포함할 수 있다. 상기 디스플레이 스크린(28)은 예를 들어 용량성 터치스크린과 같은 터치스크린을 포함할 수 있다. 상기 통신 모듈은 블루투스(RTM) 칩 또는 근거리 무선통신을 위한 다른 수단을 포함할 수 있다.

[0061] 상기 케이스(12)는 예를 들어, 통신모듈(14), 마이크로 컨트롤러(16) 및 사용자 인터페이스(18)와 같은 상기 케이스에 통합된 다수의 구성요소를 포함할 수 있다. 상기 사용자 인터페이스(18)는 이후에 보다 상세하게 설명될 다수의 발광 다이오드(LEDs) 형태의 시각적 인디케이터를 포함할 수 있다. 상기 사용자 인터페이스(18)는 사용자가 패스워드를 입력가능하도록 상기 사용자에게 시각적인 표시를 제공하기 위해 상기 케이스(12) 내의 마이크로 컨트롤러(16)에 의해 제어될 수 있다. 상기 마이크로 컨트롤러(16)는 바람직하게는 예를 들어, 8비트 내지 32비트의 적어도 하나의 중앙 처리 유닛(CPU), 적어도 하나의 전용 암호화 엔진, 적어도 하나의 난수 발생기 및/또는 통신채널을 보안하고 데이터를 보호하는 다른 구성을 포함하는 보안 마이크로 컨트롤러를 포함할 수 있다. 상기 마이크로 컨트롤러는 마이크로 프로세서를 포함할 수 있다. 상기 케이스(12) 내부의 마이크로 컨트

롤러(16)는 상기 케이스(12)가 상기 케이스(12) 내부에 수용되는 모바일 디바이스(22)와 블루투스 또는 저전력 블루투스(BLE) 프로토콜을 통해 통신할 수 있는 블루투스(RTM)칩(14)을 포함하는 통신 모듈(14)을 제어할 수 있다. 대안적으로, 케이스(12)는 바람직하게 저전력 근거리 무선통신을 제공하는 다른 무선 통신 프로토콜을 이용하여 상기 모바일 디바이스(22)와 통신할 수 있다. 예를 들어, 상기 케이스(12)는 인접한 디바이스들 사이에 무선통신 채널을 수립하는 NFC(near-field communication)안테나를 포함할 수 있다. 즉, 상기 NFC안테나는 상기 케이스(12)와 상기 모바일 디바이스(22) 사이에 무선통신 채널을 수립할 수 있다. 상기 케이스(12)는 케이스의 외곽을 따라 배치된 용량성 슬라이더 및/또는 용량성 버튼과 같은 터치 메커니즘을 더 포함할 수 있다. 상기 터치메커니즘에 대해서는 도 4a 및 도 4b에 의해 후술하기로 한다.

[0062] 상기 케이스(12) 내부의 하드웨어는 배터리(20)에 의해 충전된다. 상기 배터리(20)는 충전식 배터리일 수 있다. 상기 충전식 배터리는 AC전원에 연결된 배터리 충전기를 통해 재충전되거나, 유도성 또는 무선 충전에 의해 재충전될 수 있다. 상기 AC전원은 상기 모바일 디바이스(22)를 충전하는 충전기와 동일한 충전기 또는 별개의 충전기일 수 있다. 대안적으로, 상기 배터리(20)는 낮은 전류 드레인을 가지는 포터블 디바이스들에 일반적으로 사용되는 비충전 배터리일 수 있다. 상기 케이스(12)는 일반적으로 모바일 디바이스(22)에 패스워드를 입력할 때만 사용되고, 상기 케이스(12) 내부의 하드웨어 구성요소는 간헐적으로 사용되므로, 상기 케이스(12) 내부의 비충전 배터리를 사용해도 일반적인 모바일 디바이스의 수명(2년 이상)을 충당하기에는 충분하다.

[0063] 본 발명의 특정 실시 예에서, 고객들이 온라인으로 그들의 계좌에 접근하는 것을 제공하는 기구들(예를 들어, 온라인 은행 기관과 금융기관)과 보안 사용자 인터페이스 시스템의 제공자들 사이에는 관계가 필요하다. 예를 들어, 은행들 또는 온라인 상점들은 사용자가 온라인 거래를 수행하는 것을 시도하는 때에 상기 사용자의 모바일 디바이스의 키패드(가상의 또는 현실의)를 이용하는 것 보다 웹사이트가 사용자에게 상기 보안 사용자 인터페이스(10)를 이용하여 사용자의 패스워드(그리고, 다른 추가적인 수치 보안 정보)를 입력하도록 하는 것으로 웹사이트를 설정하는 것이 필요할 수 있다.

[0064] 도 2에 도시한 바와 같이 상기 모바일 디바이스 케이스(12)는 메모리(19)를 더 포함할 수 있다. 상기 메모리(19)는 상기 마이크로 컨트롤러(16)의 일부일 수 있고, 상기 케이스(12) 내부의 분리된 저장/메모리 모듈로 제공될 수 있다. 상기 메모리(19)는 사용자에 의해 상기 케이스로 입력된 일시적인 데이터를 저장하는데 이용될 수 있고, 사용자 특성 데이터를 저장할 수도 있고, 생성된 보안 토큰 또는 전송을 위해 암호화된 데이터 등을 저장할 수 있다. 예를 들어, 상기 사용자 특성 데이터는 사용자의 패스워드 또는 사용자가 입력한 데이터를 확인하는데 사용될 수 있는 패스워드의 해시버전, 및/또는 데이터를 확인하는데 사용되는 다른 데이터일 수 있다. 상기 메모리(19)는 본 발명을 실시하기 위한 다수의 단계에 대한 프로세서 제어 코드를 저장할 수 있다.

[0065] 전술한 바와 같이, 상기 케이스(12)는 상기 케이스(12)와 상기 모바일 디바이스(22)가 통신하기 위한 통신 모듈(14)을 포함할 수 있다. 부가적으로 또는 대안적으로, 상기 케이스(12)는 상기 케이스가 직접 서드 파티(15)와 통신하는 것을 가능하게 하는 추가적인 통신 모듈(17)을 더 포함함으로써 상기 모바일 디바이스(22)를 우회할 수 있다. 이로써 상기 모바일 디바이스에 데이터가 전송되지 않아 보다 더 안전할 수 있다. 상기 추가적인 통신 모듈(17)은 상기 케이스(12)와 상기 서드 파티(15) 사이에 통신 연결을 수립하는 무선통신 프로토콜을 이용할 수 있다.

[0066] 상기 케이스(12)는 상기 케이스(12)에 통합된 스마트카드 리더(11) 및/또는 상기 케이스(12)에 통합된 비접촉식 스마트카드 리더를 포함할 수 있다. 대안적으로, 상기 케이스(12)는 상기 마이크로 컨트롤러의 일부이거나 상기 케이스 내부의 분리된 구성인 내장형 EMV 칩(13)을 포함할 수 있다. 따라서, 상기 케이스는 CAP리더의 기능을 수행할 수 있고, 마이크로 컨트롤러(16)가 사용자에 의해 입력된 PIN과 스마트 카드리더(11)를 이용하여 읽은 데이터나 내장형 EMV칩(13)에 저장된 데이터를 이용하여 OTP를 생성하여 상기 사용자는 유효한 PIN 또는 패스워드를 모바일 디바이스(상세한 설명은 후술함)에 안전하게 입력할 수 있다.

[0067] 도 3a는 모바일 디바이스(22) 및 케이스(12)를 포함하는 보안 사용자 인터페이스 시스템(10)의 프로토 타입을 도시한다. 이러한 접근에 있어서, 상기 케이스 상의 시각적 인디케이터는 상기 케이스에 통합되고, 케이스의 일측을 따라 제공되는 다수의 LED를 포함한다. 상기 LED 외에 다른 대안적인 광원이 사용될 수도 있다. 상기 보안 사용자 인터페이스 시스템(10)의 사용자가 그들의 모바일 디바이스(22)에 실행되는 웹 브라우저 어플리케이션을 통해 온라인 은행 거래(또는 다른 유사한 보안 거래)를 실행하기를 희망하면, 상기 은행(또는 다른 서드 파티)은 상기 케이스(12)를 통해 PIN입력을 시작하기 위해 상기 케이스(12)의 보안 마이크로 컨트롤러(16)와 통신한다.(상기 모바일 디바이스(22)의 CPU(26)을 통해) 추가적인 숫자들, 예를 들어 알파벳 또는 다른 문자들이 표시될 수 있다. 다만, 표시되는 각각의 문자는 다수의 LED(18) 중 하나와 정렬되는 것이 중요하다. 즉, 도시된 예

에서, 10개의 LED가 있고, 각각은 숫자 0 내지 9 중 어느 하나를 대표한다. 다만, 이러한 LED의 배열과 문자의 표시는 단지 예시에 불과하고, 어떠한 개수의 LED 및/또는 문자들도 이용될 수 있다. 또는 상기 다수의 LED(18)는 상기 케이스의 다른 측면을 따라 배치되거나(예를 들어, 왼손잡이 사용자를 위함) 상기 케이스의 두 측 또는 그 이상의 측에 배열될 수 있다.

[0068] 상기 보안 사용자 인터페이스 시스템(10)을 사용하고자 하는 상기 은행 고객은 그들의 계좌를 설정하기 위한 특정한 정보를 은행에 제공할 필요가 있다. 예를 들어, 상기 은행 고객은 어떠한 종류의 모바일 디바이스(22)를 그들이 계좌에 접근하기 위해 사용할지를 은행에 알릴 필요가 있다. (예를 들어, 모바일 디바이스 제조사, 디바이스 모델 번호 등) 모바일 디바이스 스크린 크기들은 제조사 및 모델에 따라 다양하며, 따라서, 이러한 정보는 고정된 문자들(38)이 상기 LED들(18)과 정렬되며 상기 디스플레이 스크린(26)에 정확히 표시되도록 하는데 필요하다. 상기 사용자는 온라인 은행 거래를 수행할 때 상기 보안 사용자 인터페이스 시스템을 사용하기 위해 입력되는 특별한 PIN 또는 수치적인 패스워드를 생성하는 것이 필요할 수 있다. 추가적으로 또는 대안적으로, 상기 PIN은 은행에 의해 사용자에게 제공될 수도 있다. 사용자가 PIN을 입력할 때 상기 보안 마이크로 컨트롤러가 PIN이 정확한지 여부를 확인할 수 있도록 상기 PIN은 상기 케이스(12)의 보안 마이크로 컨트롤러가 알고 있을 수 있다. 대안적으로, 서드 파티가 PIN의 일치여부를 확인할 수 있도록 상기 PIN은 상기 보안 마이크로 컨트롤러가 알지 못할 수도 있다. 이러한 설명은 도 5와 함께 이후에 보다 상세하게 설명한다.

[0069] 상술한 바와 같이 상기 보안 사용자 인터페이스 시스템은 사용자가 상기 모바일 디바이스의 키보드를 사용하지 않고 PIN 숫자를 입력하는 것을 가능하게 한다. 따라서, 악성 소프트웨어는 상기 사용자가 입력한 키를 확인할 수 없다. 도 3a는 본 발명의 일 실시 예를 도시한다. 본 발명의 일 실시 예는 사용자가 키보드를 사용하여 어떤 숫자를 입력하는 것 대신에 사용자는 숫자를 선택하기 위해 상기 모바일 디바이스(22)의 터치 스크린(28)을 이용한다. 이러한 예시적 구성에서 고정된 숫자들(38)은 상기 디스플레이 스크린(28)에 표시되고, 각각의 숫자는 스크린의 가장자리를 따라 배치된 다수의 LED(18) 중 하나와 나란히 배열된다. 상기 케이스(12)에 통합된 보안 마이크로 컨트롤러는 단일로, 랜덤 선택하여 LED를 발광하도록 유발한다. 도 3에서 상기 디스플레이 스크린 상의 숫자 '2' 옆의 LED가 발광된다. 상기 모바일 디바이스의 악성 소프트웨어는 스크린 상에 표시된 고정된 숫자들(38)을 볼 수 있지만, 상기 LED들(그리고, LED들을 제어하는 회로)은 상기 케이스(12)의 일부분이지 상기 모바일 디바이스(22)의 일부가 아니므로 어떠한 LED가 발광했는지는 볼 수 없다.

[0070] 도 3b는 안전하게 PIN을 입력하기 위한 상기 사용자, 모바일 디바이스 및 모바일 케이스 간의 상호작용을 나타낸다. S300 단계에서, 상기 사용자는 스크린 상의 메시지를 통해 그들의 PIN을 하나씩 입력하라는 것을 전달 받는다. 상기 스크린 상의 메시지는 상기 PIN을 입력하기 위해 필요한 문자들을 포함할 수 있다. 예를 들어, 상기 문자들을 포함하는 메시지는 상기 모바일 디바이스 스크린의 일 측에 있는 리스트로써 제공될 수 있다. 또한, 도 3a에 도시한 바와 같이 상기 스크린 상의 메시지(36)는 사용자의 PIN에는 다수의 숫자가 있기 때문에 적어도 다수의 박스가 있는 박스들의 열을 포함할 수 있다. 도 3a의 상기 사용자는 그들의 PIN의 세 번째 숫자를 입력하는 과정에 있다. 상기 과정은 숫자 '3'이 가르키는 열의 세 번째 박스에 의해 나타낼 수 있다. 다만, 도시한 바와 같이 사용자에 의해 입력된 첫 번째와 두 번째 숫자는 스크린의 첫 번째 박스와 두 번째 박스에 표시되지 않는다. (상기 박스들은 회색처리되거나 숫자가 입력될 때 별표를 포함하여 상기 사용자에게 그들이 어떠한 숫자를 입력하였는지를 시각적 표시와 함께 제한적으로 제공한다.) 이러한 방법으로 상기 모바일 디바이스에 PIN의 어떠한 문자도 표시되지 않는다.

[0071] 상기 스크린 상의 메시지가 나타남과 동시에(또는 잠시후에), LED들 중 하나가 무작위로 선택되고, 상기 케이스의 마이크로 컨트롤러에 의해 점등된다. 상기 스크린 상의 메시지는 스크린 상의 무작위로 선택된 LED의 옆에 나타날 수 있는 인디케이터(46)를 선택적으로 포함할 수 있다. 따라서, 도 3a에 예시적으로 도시한 바와 같이 상기 인디케이터(46)는 발광되는 LED에 대응되는 숫자 '2' 옆에 나타난다. 다만, 보안을 향상시키기 위해 이러한 인디케이터가 사용되지 않고 LED가 첫 번째로 발광할 때 스크린 상에는 어떠한 것도 나타나지 않을 수 있다.

[0072] 다음 단계(S304)는 특정한 숫자를 선택하기 위해 상기 사용자가 스크린(28)을 손가락으로 터치하고, 상기 스크린상의 상기 인디케이터(46)를 최초 위치에서 위로 또는 아래로 이동시킨다. (만약 인디케이터가 제공되지 않는다면, 상기 사용자는 간단히 그들의 손가락을 무작위로 선택되어 발광하는 LED 옆에 위치시키고, 상하로 움직여 숫자를 선택한다.) 상기 터치와 상기 스크린(28) 상의 이후의 움직임은 모바일 디바이스에 의해 감지되고, 상기 케이스로 전송한다. (S306) 상기 발광하는 LED는 상기 스크린 상의 상기 사용자의 손가락 위치에 따라 변경된다. (S308) 상기 사용자는 원하는 숫자에 대응되는 LED가 점등되면, 사용자의 손가락을 상기 스크린으로부터 릴리즈 시킨다. (S310) 이러한 움직임은 상기 모바일 디바이스에 의해 감지되고, 상기 케이스로 전송한다. (S312) 상기 사용자가 실수로 상기 스크린에서 손가락을 떼는 경우 상기 선택이 완료되기 전에 상기 LED는 '확

인 기간'을 위해 짧게 깜빡일 수 있다. 만약 사용자가 확인 기간 동안 스크린을 터치한다면, 상기 사용자는 그들의 숫자 선택을 변경할 수 있다. (만약 사용자가 실수로 틀린 숫자를 선택하고, 확인 기간 동안 선택을 변경하지 않는다면, 상기 사용자는 취소가 필요하고, 모든 단계를 다시 시작할 필요가 있다.)

[0073] 비록 상기 모바일 디바이스가 스크린을 가로지르는 움직임을 감지했다고 하더라도, 어떠한 LED가 발광하는지에 대한 정보(또한, 어떠한 숫자가 선택되었는지에 대한 정보)는 상기 케이스(12)의 보안 마이크로 프로세서에만 전달되고, 상기 모바일 디바이스(22)에는 전달되지 않는다. 상기 사용자에게 선택된 문자들은 오직 상기 케이스(1)의 보안 마이크로 컨트롤러에 알려지고, 상기 케이스(12)의 메모리에 저장될 수 있다. (S316) 상기 모바일 디바이스의 악성 소프트웨어는 상기 스크린 상의 알려지지 않은 시작점으로부터 단지 스크린(28) 상의 상기 사용자의 스크롤 동작을 관찰하여 어떠한 PIN의 자리수가 입력되었는지를 추론하기가 어려운 것을 발견할 것이다.

[0074] 문자가 입력된 이후 상기 시스템(예를 들어, 발광한 케이스의 컨트롤러)은 PIN을 위해 문자가 더 필요할지 여부를 판단한다. 상기 모바일 디바이스는 PIN이 완전히 입력되었는지 또는 상기 사용자가 PIN이 완전히 입력되도록 입력을 할 수 있는지 여부를 판단할 수 있는 것으로 이해할 수 있다.

[0075] 만약, 문자가 더 입력되어야 하는 경우 강화된 보안을 위해, 문자가 입력된 이후, 상기 케이스의 상기 마이크로 컨트롤러는 다음 문자가 입력되도록 하기 위해 초기위치의 LED를 발광시키기 위해 무작위로 선택한다. 다시 말해, 상기 과정은 S302 단계로 돌아가고, 다음 문자를 입력하는 단계를 시작한다. 이와 같이, 상기 사용자의 상기 스크린 상의 초기 위치는 각각의 새로운 숫자가 선택되는 때마다 달라진다. 대안적으로, 이전의 문자에 선택된 상기 LED가 발광한 상태를 유지하고, 사용자는 상기 LED에 대응되는 위치로부터 스크롤 할 수 있다. 다시 말해, 상기 과정은 S304 단계로 돌아갈 수 있다. (도면에서 대안적으로 도트 라인으로 도시되어 있음) 상기 사용자는 선택을 위해 키보드를 이용한 숫자 선택과 유사하게 원하는 숫자 옆의 스크린(28)을 탭할 수 없는 것은 중요한 접근이다. 상기 사용자는 그들이 원하는 숫자에 도달하기 까지 반드시 초기 위치로부터 스크롤 하여야 한다.(윗쪽 및/또는 아래쪽 방향으로) 상기 스크롤은 주기적일 수 있다. 상기 사용자에게 하나의 방향(예를 들어, 위쪽 또는 아래쪽)으로 스크롤 하는 것만 허용함으로써 진행방향(스크린 상의 상기 사용자의 손가락의 진행방향)에 따라 PIN이 알려지는 위험을 줄일 수 있어 보안은 향상될 수 있다.

[0076] 모든 PIN이 이러한 과정을 이용하여 입력되면, 상기 케이스(12)의 상기 보안 마이크로 컨트롤러는 수신된 숫자들에 수학적 함수를 실행할 수 있다. 상기 보안 마이크로 컨트롤러가 상기 사용자의 정확한 PIN을 알고 있다면(셋업 과정이나 다른방법을 통해), 수학적 함수는 마이크로 컨트롤러에서 상기 사용자가 은행 거래를 계속하는 것이 허용되는지를 결정하기 위해 정확한(저장된) PIN과 상기 사용자가 입력한 숫자를 비교한다. 상기 사용자가 정확하지 않은 PIN을 입력한다면, 상기 사용자는 정확한 PIN을 입력할 수 있도록 다른 숫자를 입력할 수 있는 기회를 받고, 이후에 PIN이 정확하게 입력되지 않는다면, 상기 사용자는 그들의 온라인 은행 계좌를 폐쇄당하고, 상기 거래를 완료할 수 없다. 상기 수학적 함수의 예는 이하에서 상세히 설명될 도 5의 상기 보안 마이크로 컨트롤러에서 수행된다.

[0077] 도 3a에서 사용자는 숫자의 고정 세트(38)로부터 숫자를 선택하기 위해 상기 모바일 디바이스(22)의 터치스크린(28)을 사용한다. 도 4a 및 도 4b는 숫자 선택을 위한 대안적인 접근을 도시한다. 도 4a에서 상기 모바일 디바이스 케이스(12)는 터치패드(40)를 포함한다. 숫자 선택을 위해 터치스크린(28)을 사용하는 것을 대신해, 상기 사용자는 상기 케이스(12)의 일 측에 통합된 센서 또는 터치패드(40)를 사용할 수 있다. 상기 센서(40)는 예를 들어, 다수의 랩탑 터치패드들에 사용되는 기술과 유사한 용량성 센서일 수 있다.

[0078] 도 4c는 도 4a의 방식으로 PIN을 안전하게 입력하기 위한 상기 사용자, 모바일 디바이스 및 모바일 디바이스 케이스 간의 상호작용을 나타낸다. 이전의 실시 예와 같이, 상기 모바일 디바이스는 LED들과 정렬된 PIN을 입력하기 위한 문자들로 구성된 "input PIN" 메시지를 출력할 수 있다. (S400) 상기 케이스는 하나의 LED를 발광시키고(S402) 상기 사용자는 원하는 문자에 부합하도록 발광 LED를 변경한다. (S404) 다만, 이전의 접근과는 달리 상기 사용자의 손가락 움직임은 상기 케이스의 센서에 의해 감지되고 무작위로 발광하는 첫 번째 LED는 필요하지 않다. 상기 모바일 디바이스가 터치패드 상의 움직임을 검출할 수 있는 방법은 없다. 상기 사용자는 주기적인 발광 프로세스가 원하는 LED를 발광시킬 때 상기 센서(40)로부터 그들의 손가락을 떠나게 함으로써 숫자를 선택할 수 있다. 그리고/또는 원하는 LED가 켜진 경우 상기 센서를(40) 탭 함으로써 숫자를 선택할 수 있다. (S408) 이전의 실시 예와 같이 사용자가 그들의 생각을 바꾸는 것을 허용하기 위해 선택적인 "깜빡거림" 단계가 있을 수 있다. 다음에, 상기 케이스의 마이크로 컨트롤러는 LED와 대응되는 문자를 판정하고 저장하고, (S412) 다른 문자가 필요한지 여부를 판단한다. (S414) PIN이 완전한지 여부에 대한 이러한 판정은 다른 방법으로 구성될 수 있다. 만약, 다른 문자가 더 필요한 경우 프로세스 사이클은 입력된 것과 동일한 또는 다른 것을 입력받

을 수 있도록LED를 발광하기 위해 돌아간다.

[0079] 도 4b에서, 상기 모바일 디바이스 케이스(12)는 다수의 별개의 터치패드 버튼들(42)을 포함할 수 있다. 열 개의 터치패드 버튼들(42)은 0 내지 9의 번호가 붙은 상기 케이스의 일측을 따라 제공될 수 있다. 상기 버튼들에 번호가 부여되면, 사용자는 정확한 순서대로 버튼을 누름으로써 그들의 PIN을 간단히 입력할 수 있고, 상기 케이스와 모바일 디바이스는 PIN을 생성하기 위한 상호작용을 하지 않는다. 상기 별개의 버튼들(42)은 키패드와 유사하다. 다만, 이 경우 버튼들은 PIN입력 기간동안 보안을 유지하는 상기 모바일 디바이스(22)에 제공되기 보다는 상기 케이스(12)에 통합된다. 버튼들을 상기 케이스의 일측을 따라 제공하는 것의 장점은 상기 보안 사용자 인터페이스 시스템(10)의 사용자가 어플리케이션들과 그들의 모바일 디바이스 간을 전환시키는 것을 필요로 하지 않는다는 것 또는 버튼에 접근하기 위해 상기 디바이스를 젖히는 것을 필요로 하지 않는 다는 것이다. 이러한 것은 사용자 경험(UX)을 향상시킬 수 있다.

[0080] 상기 버튼들에 번호가 붙여지는 경우 LED들은 생략될 수 있다. 대안적으로, 상기 케이스는 버튼들에 번호가 붙여지더라도 이전에 기술한 바와 같이 상기 모바일 디바이스와 상호작용할 수 있다. 이러한 구성에서 하나의 버튼이 하나의 LED와 대응되도록 상기 버튼들은 LED들(18)과 배열될 수 있다. 도 4d는 상기 디바이스와 케이스 간의 약간의 상호작용 방법을 나타낸다. 이전의 실시 예와 같이 상기 모바일 디바이스는 LED들과 정렬된 PIN을 입력하기 위한 문자들로 구성된 "input PIN" 메시지를 출력할 수 있다. (S450) 표시된 문자를 선택하기 위해, 상기 사용자는 원하는 문자 옆에 있는 버튼을 간단히 누를 수 있다. (S452) 이것은 버튼 옆의 LED를 점등시킨다. (S454) 상기 LED가 점등되면, 상기 사용자는 버튼을 릴리즈 하고(S456) 상기 프로세스는 확인 기간을 위해 선택적으로 LED의 깜빡거림을 유발한다. (S458) 이후 상기 케이스의 상기 마이크로 컨트롤러는 상기 LED와 대응되는 문자를 판정하고 저장하고, (S460) 다른 문자가 필요한지 여부를 판단한다. (S462) PIN이 완전한지 여부에 대한 이러한 판정은 다른 방법으로 구성될 수 있다. 만약 다른 문자가 더 필요한 경우 프로세스 사이클은 사용자가 다음 문자를 입력할 수 있도록 기다리는 것으로 돌아간다. (S452)

[0081] 상기 보안 사용자 인터페이스 시스템을 이용한 PIN을 입력하는 방법에는 다른 많은 방법이 있다. 예를 들어, 상기 모바일 디바이스 케이스(12)가 상기 터치패드(40) 또는 버튼(42) 대신에 회전하는 휠로 제공될 수도 있다. 상기 휠은 발광되는 LED를 변경하기 위해 사용자에 의해 회전될 수 있다. 상기 사용자는 원하는 숫자와 대응되는 LED가 발광되면 휠의 회전을 멈출 수 있다. 그리고/또는 상기 휠을 탭 하거나 눌러 선택할 수 있다.

[0082] 도 5는 앞서 설명한 상기 보안 사용자 인터페이스 시스템을 이용한 패스워드 입력하는 일반적인 단계를 나타내는 순서도이다. 상기 보안 사용자 인터페이스 시스템의 사용자는 상기 모바일 디바이스에서 실행되는 어플리케이션을 시작한다. 상기 어플리케이션은 게임, 워드프로세싱 소프트웨어, 웹 브라우저 등일 수 있다. 상기 사용자는 예를 들어 온라인 은행 계좌와 같은 보안 웹사이트에 웹 브라우저를 통해 접근을 원할 수 있다. 또한 예를 들어, 사용자는 게임의 추가적인 기능에 접근을 원할 수 있다. 접근을 허가하기 위해 상기 어플리케이션은 패스워드나 PIN을 사용자로부터 입력하는 것을 요청할 수 있다. (S500) 상기 사용자는 앞서 설명한 보안 사용자 인터페이스 시스템을 통해 패스워드를 입력하는 것을 진행할 수 있다. (S502) 상기 패스워드의 입력은 앞서 설명한 대로, 상기 사용자에게 상기 모바일 디바이스의 터치 스크린을 스크롤/스와이프하는 것을 요구할 수 있다. 또는, 상기 패스워드의 입력은 상기 사용자에게 상기 케이스의 센서들/버튼들을 사용하는 것을 요구할 수 있다. 만약 상기 패스워드가 터치스크린을 터치함으로써 입력된다면, 상기 스크린 상의 상기 사용자의 최초 위치 및 스크린 상에서 이동한 거리는 상기 모바일 디바이스에 알려진다. 상기 데이터는 블루투스(RTM)를 통해 상기 보안 마이크로 컨트롤러에 전달되고, 상기 보안 마이크로 프로세서는 상기 스크린에서 상기 사용자가 선택한 숫자를 결정하기 위해 상기 데이터를 처리하고, 상기 케이스의 어떠한 LED를 발광시킬지 결정한다. 따라서, 상기 모바일 디바이스 및 케이스가 숫자를 입력하는데 사용될 때 상기 케이스와 모바일 디바이스에 일어나는 처리과정은 상기 디스플레이의 고정된 세트에서 사용자가 어떠한 숫자를 선택하였는지를 알지 못한다. 상기 패스워드가 케이스의 일측에 있는 센서들/버튼들을 이용하여 입력되는 경우, 상기 모바일 디바이스는 사용자가 선택한 어떠한 숫자나 상기 보안 마이크로 프로세서에서 수행되는 과정에 대한 인식을 알지 못한다.

[0083] 상기 케이스로부터 PIN의 모든 숫자가 수신되면(그리고, 모바일 디바이스에 대한 수신을 제외하고)(S504), 상기 케이스의 상기 보안 마이크로 컨트롤러는 수신된 숫자들에 수학적 함수를 수행한다. (S506) 상기 보안 마이크로 컨트롤러는 예를 들어, 하기와 같이 동작한다.

[0084] ● 상기 케이스에 저장되어 있던 정확한 PIN과 수신한 숫자를 비교한다. 만약, 상기 사용자가 정확한 PIN을 입력한 것으로 확인된다면, 상기 보안 마이크로 프로세서는 S508 단계를 실행한다. 상기 PIN이 정확하지 않다면, 상기 사용자는 앞서 설명한 대로 다수의 추가적인 시도를 허가 받을 수 있다.

[0085] ● 암호화 해시 함수를 이용하여 수신된 숫자들을 해시하고, 그 결과로 생긴 해시값과 상기 마이크로 컨트롤러에 저장된 해시 값을 비교한다. 이러한 방법은 상기 마이크로 컨트롤러가 정확한 PIN을 저장하지 않고 있어도 되며 상기 마이크로 컨트롤러에 저장되는 것은 단지 PIN의 해시이므로 앞서 설명한 것보다 안전한 옵션이 될 수 있다. 만약 상기 해시 값이 일치한다면, 상기 보안 마이크로 컨트롤러는 S508 단계를 수행한다.

[0086] ● 암호화 키를 이용하여 입력된 숫자들을 암호화 한다. 이러한 예에서, 상기 마이크로 컨트롤러는 스스로 확인 과정을 수행하지 못하고, 확인을 위해 서드 파티로 전송되는 암호화된 데이터를 생성한다. (S508) 이러한 방법은 상기 케이스에 데이터(정확한 PIN 또는 해시된 정확한 PIN)가 저장되지 않으므로, 이전의 2가지 예보다 더 안전할 수 있다.

[0087] 상기 수학적 함수의 출력은 각각의 경우에 따라 다른 데이터에 기초하여 수행된다. 예를 들어, 상기 보안 마이크로 컨트롤러가 스스로 PIN의 일치 여부를 확인하는 경우에 상기 출력은 보안토큰, 일회용 패스워드(one-time password, OTP), 거래 인증 번호(transaction authentication number, TAN) 등일 수 있다. 상기 입력되는 숫자들이 암호화된 경우에는 상기 출력은 암호화된 데이터일 수 있다. 각각의 경우에 상기 출력은 블루투스(RTM)과 같은 특정한 무선 통신 프로토콜을 이용하여 상기 모바일 디바이스에 전송될 수 있다. (S510) 상기 모바일 디바이스에 수신된 데이터는 상기 디바이스에 실행되고 있는 악성 소프트웨어에 의해 빼앗기거나 읽어질 수 있다. 다만, 상기 악성 소프트웨어가 데이터를 생성하기 위해 사용된 사용자의 PIN을 알아 내기는 어렵다. 이후 상기 모바일 디바이스는 패스워드를 요청한 상기 어플리케이션에 수신된 데이터를 입력한다. (S512) 상기 데이터는 암호화된 PIN이며, 상기 어플리케이션은 상기 PIN이 정확한지를 확인하기 위해 상기 데이터를 해독한다. (PIN이 정확하지 않으면, 상기 사용자는 상기 프로세스를 다시 시작하도록 안내받는다)

[0088] 상기 프로세스는 이상의 설명과 도 5에 도시되어 있다. 본 발명의 추가적인 설명을 위해, 도 6은 특정한 온라인 은행 거래의 수행 단계를 예시적으로 나타낸 순서도이다. 여기서, 상기 보안 마이크로 컨트롤러는 정확한 PIN과 사용자에 의해 입력된 PIN 숫자를 비교하도록 수행되도록 구성된 수학적 함수에 적용되는 정확한 PIN을 알고 있다.

[0089] S600 단계에서, 상기 보안 사용자 인터페이스 시스템의 사용자는 그들의 모바일 디바이스를 통해 온라인 은행 계좌에 로그인한다. 일반적으로, 상기 사용자는 웹 브라우저를 통해 그들의 계좌에 접근한다. 상기 사용자는 계좌들 간에 이체를 하거나 지불을 하는 것과 같은 온라인 은행 거래를 시작한다. (S602) 온라인 계좌에 접근하는 것이 보장된 사람은 은행계좌에 관계된 고객이다. 그리고, 상기 거래를 인가하기 위해서 상기 은행 웹사이트는 거래를 계속하기 위해 사용자에게 일회용 패스워드(OTP)를 입력하도록 할 수 있다. 상기 OTP는 이전에 설명된 어떠한 방법을 이용하여 입력될 수 있다. 예를 들어, 상기 웹사이트는 상기 모바일 디바이스가 상기 모바일 디바이스의 스크린에 상기 모바일 디바이스 케이스의 LED들과 정렬된 고정된 숫자 세트를 출력하도록 야기할 수 있다. 상기 사용자가 숫자를 선택한 때 상기 케이스의 마이크로 컨트롤러는 발광된 특정의 LED와 관련된 숫자를 저장한다. 따라서, 상기 스크린에 표시된 문자와 각각의 LED 위치의 연결 지식은 또한 상기 웹사이트로부터 케이스로 전송된다.

[0090] 상기 사용자가 PIN의 모든 숫자를 입력하면, 상기 보안 마이크로 컨트롤러는 사용자에 의해 입력된 숫자와 상기 사용자에 의해 입력된 PIN이 정확한지 여부를 확인하기 위해 상기 마이크로 컨트롤러가 알고 있는 정확한 PIN 값을 비교한다. (S608) (상기 정확한 PIN은 마이크로 컨트롤러에 저장되어 있을 수 있고, 또는 상기 케이스의 다른 하드웨어 구성요소로부터 상기 마이크로 컨트롤러에 접근가능할 수 있다.) 만약 상기 사용자에 의해 입력된 PIN이 정확하지 않은 것으로 판단되는 경우 상기 사용자는 동일한 숫자 선택 과정을 이용하여 그들의 PIN을 재입력하도록 유도 받는다. 상기 사용자는 PIN을 입력하기 위해 숫자를 수정할 수 있는 기회를 제공받고(예를 들어, 3회) 이후 사용자는 온라인 거래 계속에 대해 차단될 수 있다.

[0091] 상기 PIN이 정확한 것으로 확인 된 경우 상기 보안 마이크로 컨트롤러는 일회용 패스워드(OTP)를 발행할 수 있다. (S610) 이후 상기 OTP가 상기 모바일 디바이스로 (블루투스(RTM)와 같은 무선 통신 수단을 통해) 송신된다. (S612) 추가적으로 상기 OTP는 상기 모바일 디바이스에 의해 상기 웹사이트로 전송된다. (S614) 상기 OTP가 상기 모바일 디바이스에 알려진다 하더라도, 상기 모바일 디바이스의 악성 소프트웨어는 PIN과 OTP를 생성하는데 이용되는 어떠한 데이터에 접근할 수 없다. 이러한 것들은 오직 상기 모바일 디바이스 케이스에 제공될 뿐이기 때문이다. 또한, OTP는 한정된 유효 시간을 가지고 있고, 한 번의 거래에만 유효하다. 따라서, 악성 소프트웨어가 상기 OTP를 가로챈다고 하더라도, OTP는 한번의 사용으로 만료되므로, 상기 목적으로 사용될 수 없다. 부가적으로 또는 대안적으로, S610 단계에서 OTP를 발행하지 않고 상기 보안 마이크로 컨트롤러는 내부 자원들에 대한 접근을 해제 또는 원격으로 접근하는 자원들을 해제하기 위한 인증 토큰을 발행하거나, 안전한 전송 및 서드

파티(예를 들어 은행)에 의한 확인을 위해 암호화 키를 이용하여 사용자에 의해 입력된 PIN을 암호화 할 수 있다.

[0092] 상기 은행은 수신한 OTP를 확인한다. (S616) 예를 들어, 상기 은행은 상기 OTP 발행된 이후 적정한 시간에 수신되었는지를 확인할 수 있다. 상기 사용자가 거래를 시작하고, OTP를 발행해 달라는 요청과 OTP를 수신한 시간 사이에 만약 많은 시간이 경과하였다면(예를 들어 몇 분 이상) 상기 OTP는 만료될 수 있고, 상기 은행은 상기 사용자에게 새로운 OTP를 입력하도록 할 수 있다. 만약, 상기 OTP가 확인되는 경우 상기 은행은 온라인 거래를 완료한다. (S618)

[0093] 상기 보안 사용자 인터페이스 시스템은 지금까지 온라인 거래를 완료하기 위해 생성되는 OTP에 대해 설명하였으나, 이러한 특정한 용도는 단지 예시적인 목적으로 사용된 것이며, 제한되지 않는다. 상기 보안 사용자 인터페이스 시스템은 하기와 같은 다양한 목적으로 사용될 수 있으며, 이에 한정되지는 않는다.

[0094] ● 인증 코드를 생산하는 마스터 카드 CAP/ 비자 DPA(dynamic passcode authentication) 계산기. 상기 케이스에 통합된 상기 보안 마이크로 컨트롤러는 사용자의 "칩과 PIN" 또는 EMV은행카드와 같은 동일한 데이터를 저장할 수 있다. 대안적으로, 상기 케이스는 상기 은행 카드의 칩으로부터 데이터를 읽어 인증코드를 생성할 수 있는 통합된 EMV은행카드 리더를 포함할 수 있다. 상기 통합된 은행카드 리더는 물리적인 접촉(이전에 설명한 종래의 CAP 리더와 같이)또는 비접촉식일 수 있다;

[0095] ● 전술한OATH 호환 OTP 또는 TAN(transaction authentication number) 생성기;

[0096] ● 전술한 모바일 디바이스의 지역 어플리케이션을 해제하기 위한 보안 입력 디바이스;

[0097] ● 전술한 암호화/해시된 크리덴셜을 웹사이트/은행 시스템에 업로드 하기 위한 보안 입력 디바이스;

[0098] ● 지불/거래를 승인하기 위한 위한 디바이스;

[0099] ● 안전하게 통화를 유지하고, 비트코인(RTM)과 같은 가상의 통화들을 거래하지 위한 디바이스.

[0100] **<u>완전히 보호된 항목</u>**

[0101] 상기 보안 사용자 인터페이스 시스템은 입력된 데이터를 인증하는데 사용될 수 있다. 상기 사용자는 본 실시 예를 제외하고는 이전에 설명한 것과 동일한 방법으로 그들의 PIN의 각각의 숫자를 선택할 수 있고, 시작되는 숫자는 각각의 시간에 무작위적이지 않을 수 있고, 선택된 숫자들은 상기 디스플레이 스크린상에 숨겨지지 않을 수도 있다. 본 실시 예에서, 상기 보안 마이크로 컨트롤러는 사용자에 의해 입력된 PIN으로 메시지 인증 코드(message authentication code, MAC)를 구성할 수도 있고, 디지털 방식으로 상기 PIN을 보낼 수 있다. 상기 보안 사용자 인터페이스 시스템의 사용자들은 이전에 설명된 방법보다 간단한 방법으로 이러한 PIN 입력방법을 찾을 수 있다. 다만, 상기 비보안 입력 메커니즘이 남용되면 대응되는 위험이 발생한다. 본 실시 예에서 악성 소프트웨어의 공격을 줄이기 위해 상기 사용자는 상기 보안 사용자 시스템이 "보안 입력 모드" 인 경우(상기 시스템이 "비보안 입력 모드"인 경우가 아닌)에 오직 그들의 PIN을 입력하도록 권장받을 수 있다. 상기 시스템의 두 가지 다른 모드는 두 가지 색상의 LED들에 의해 사용자에게 알려질 수 있다. 예를 들어, 상기 시스템이 "보안 입력 모드"인 경우 상기 LED는 녹색으로 변경될 수 있고, 상기 시스템이 비보안 모드인 경우, 상기 LED는 적색으로 변경될 수 있다. 사용자들은 상기 광원들이 녹색이 될 때까지 그들의 PIN을 입력하지 않도록 교육받을 수 있다.

[0102] **<u>인간에 의해 확인되는 비밀 루트</u>**

[0103] 본 발명의 대안적인 접근에 있어서, 상기 모바일 디바이스 케이스는 상기 모바일 디바이스와 통신할 수 있다. 다만, 상기 케이스는 여전히 시간/카운터 기반(케이스 또는 보안 마이크로 컨트롤러의 클럭이나 카운터를 이용하여)이나 도 7에 도시된 안전하게 입력된 거래 데이터를 바탕으로 TAN/OTP를 생성하는 것과 같은 유용한 기능을 수행할 수 있다. 첫 번째 단계로써, 상기 케이스의 마이크로 컨트롤러는 TAN 또는 OTP를 생성한다. (S700) 상기 TAN 또는 OTP의 생성은 사용자의 요청이나 케이스에 맞는 카드가 상기 케이스에 삽입되는 것과 같은 사용자의 다른 행동에 의해 응하여 행해 질 수 있다. 이전의 실시 예와 같이 상기 모바일 디바이스는 다수의 LED 중 하나와 각각 정렬된 문자들의 세트를 표시한다. (S702) 상기 첫 번째 단계들은 동시로 또는 다른 순서로 진행될 수 있음을 이해할 수 있다. 상기 케이스에 통합된 상기 LED들은 생성된 TAN을 보여주기 위해 순차적으로 깜빡일 수 있다. (S704) 동시에, 상기 모바일 디바이스는 키보드나 사용자가 TAN을 입력할 수 있는 유사한 인터페이스를 표시한다. (S706) 상기 키패드 버튼은 사용자에게 코드의 입력을 간소화할 수 있도록LED와 함께 선택적으로 배열될 수 있다. 이후 상기 사용자는 상기 모바일 디바이스의 터치스크린 상의 출력된 가상의 키패드의 버튼들

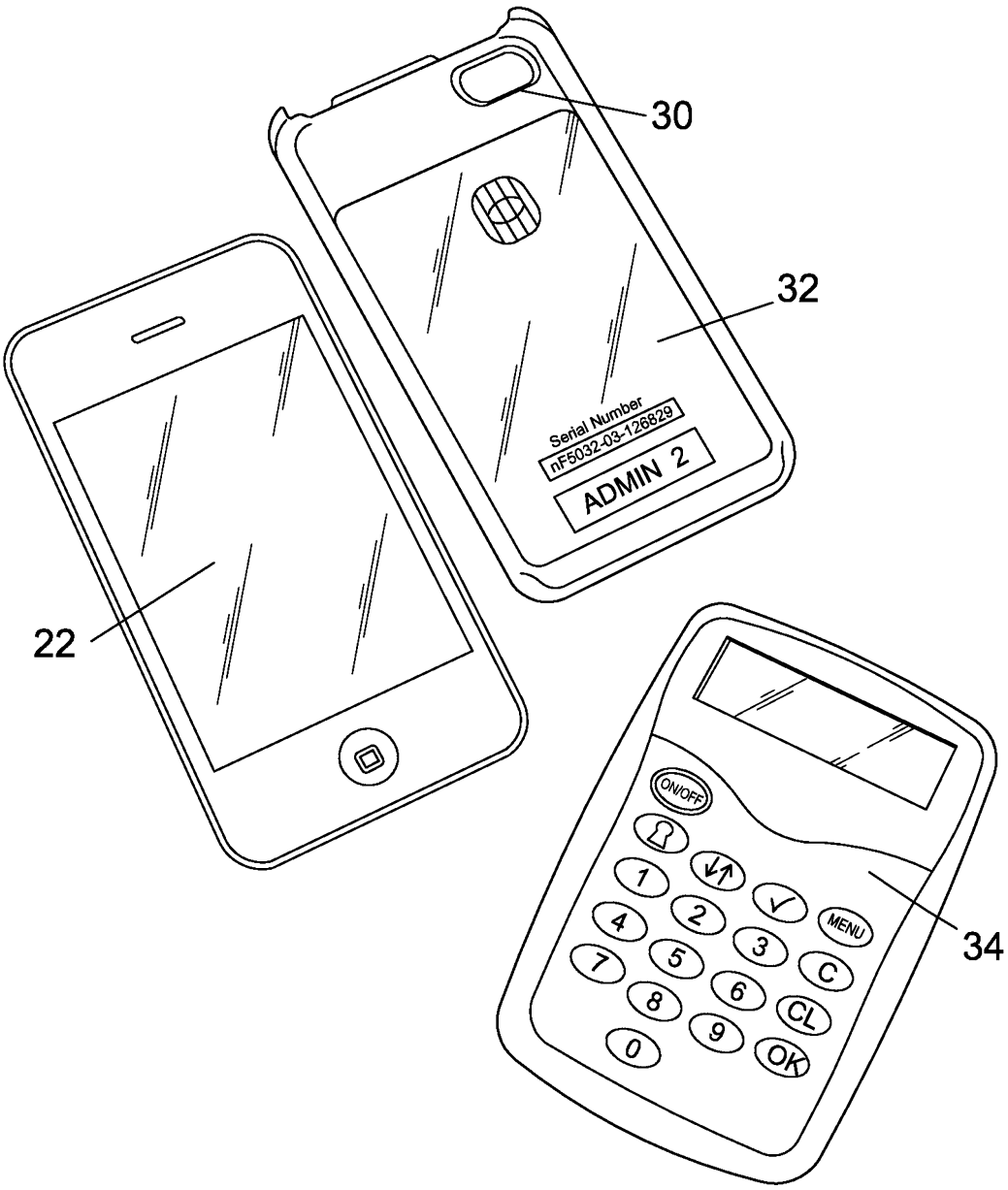
을 탭 할 수 있다. (S708) 상기 LED들은 상기 사용자 들이 각각의 깜빡이는 LED와 정렬된 적절한 키패드 버튼을 터치할 수 있도록 버튼들에 정렬되고, 상기 사용자는 코드의 어떠한 숫자도 기억하지 않고 LED의 깜빡거림을 따라 많은 자리수의 숫자 코드를 입력한다. 이러한 비밀 루트는 상기 보안 사용자 인터페이스 시스템이 상기 모바일 디바이스와 전기적인 통신을 할 필요없이 사용될 수 있도록 보장한다. 또한, 마지막 단계에서 도시한 바와 같이 상기 모바일 디바이스는 상기 모바일 디바이스로부터 비밀 데이터를 감추는 것 없이 직접 TAN을 수신한다.

[0104] 대안적으로, 상기 사용자는 생성된TAN을 기록하거나 기억할 수 있다. 전체 TAN이 생성되면, 사용자는 이후 설명된 것들 중 보다 더 안전한 방법 중 하나로 TAN을 입력할 수 있다.

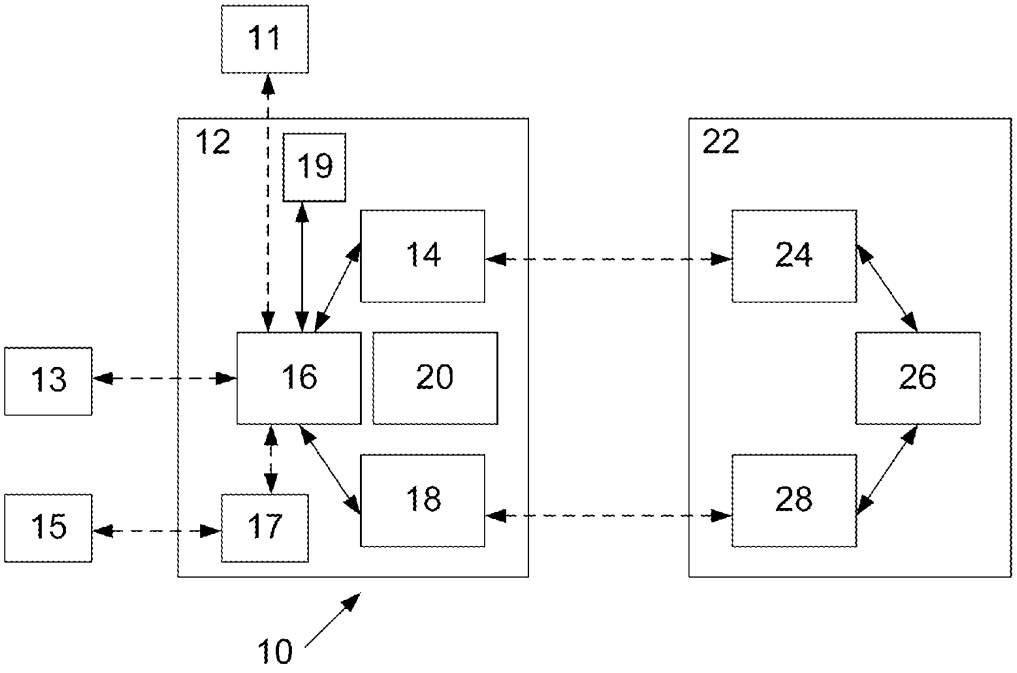
[0105] 다른 많은 효과적인 대안이 통상의 기술자들에 의해 발생하는 것은 의심의 여지가 없다. 본 발명은 상술한 실시예에 의해 한정되지 않으며, 통상의 기술자에 의한 명백한 변경은 첨부된 청구항의 범위와 사상에 포함된다.

도면

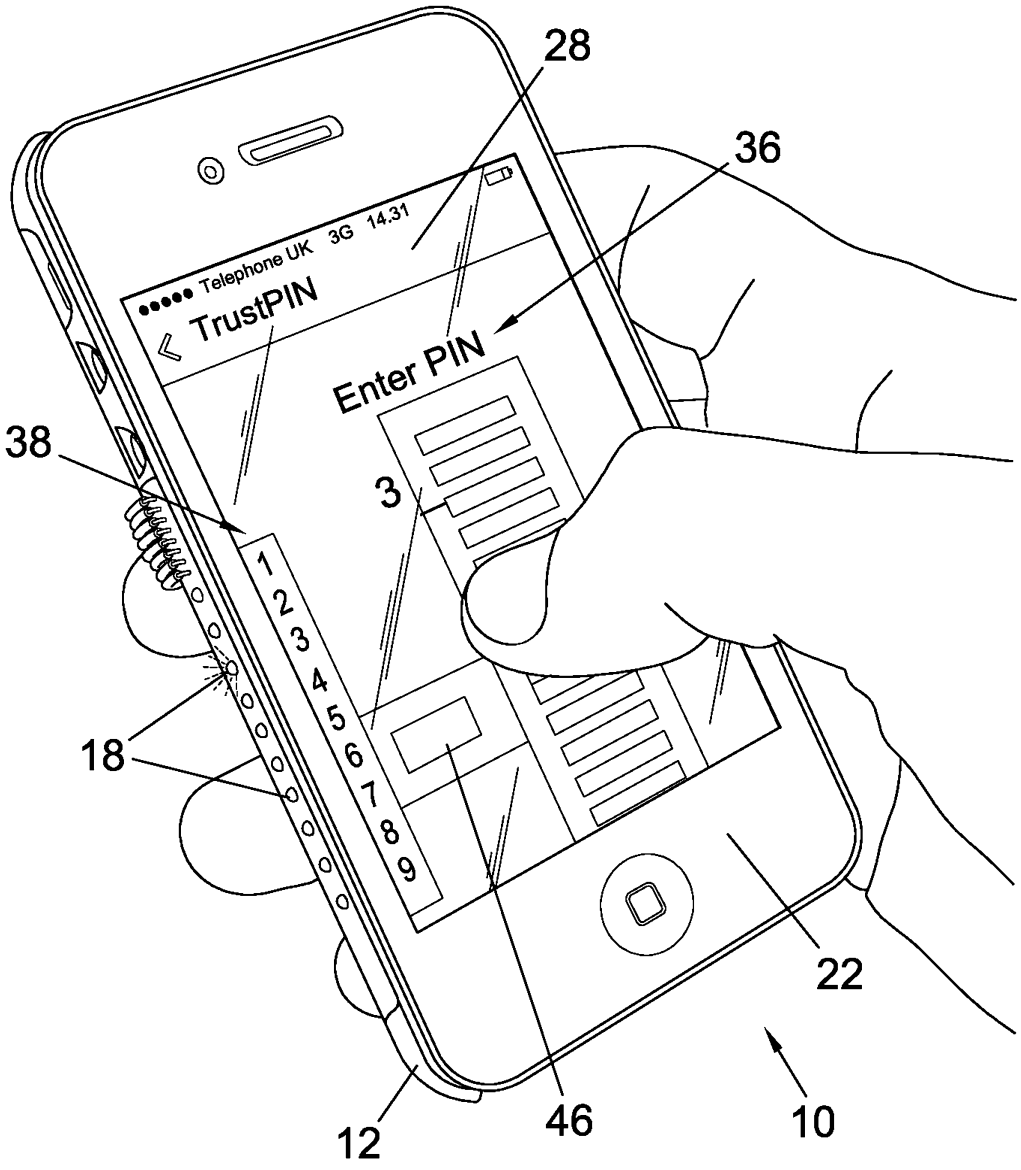
도면1



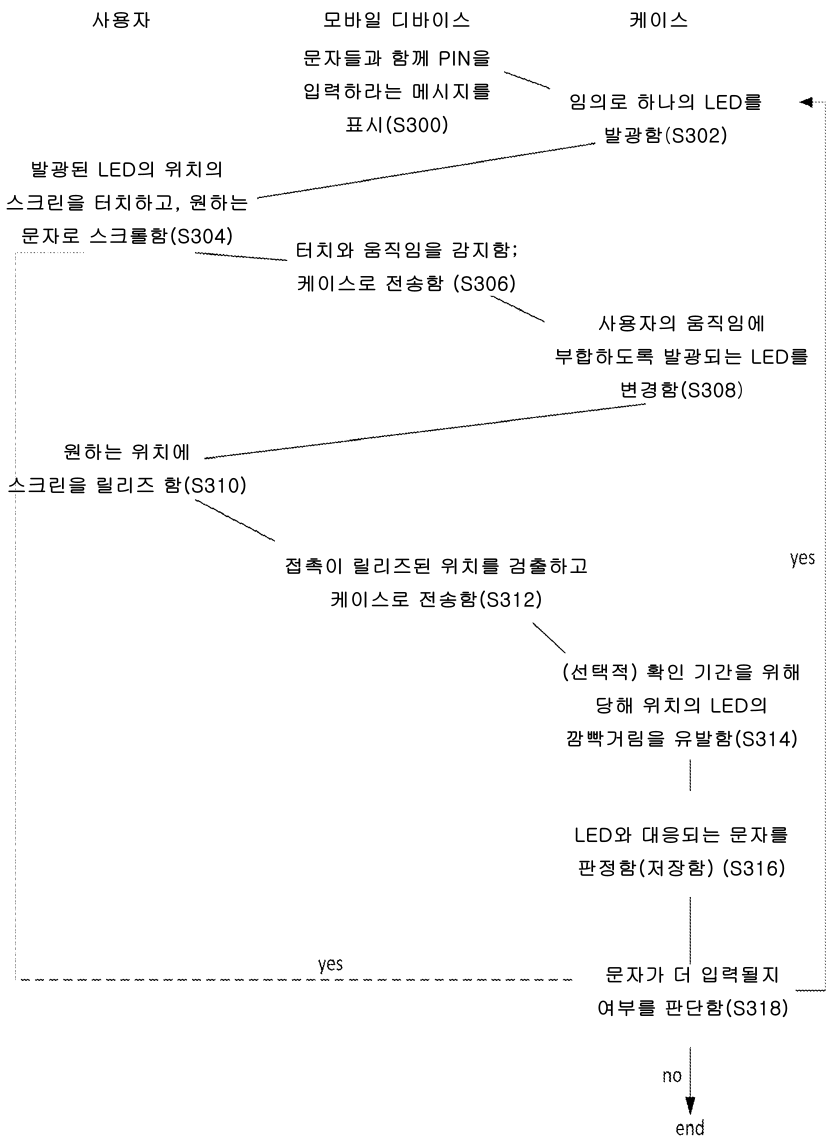
도면2



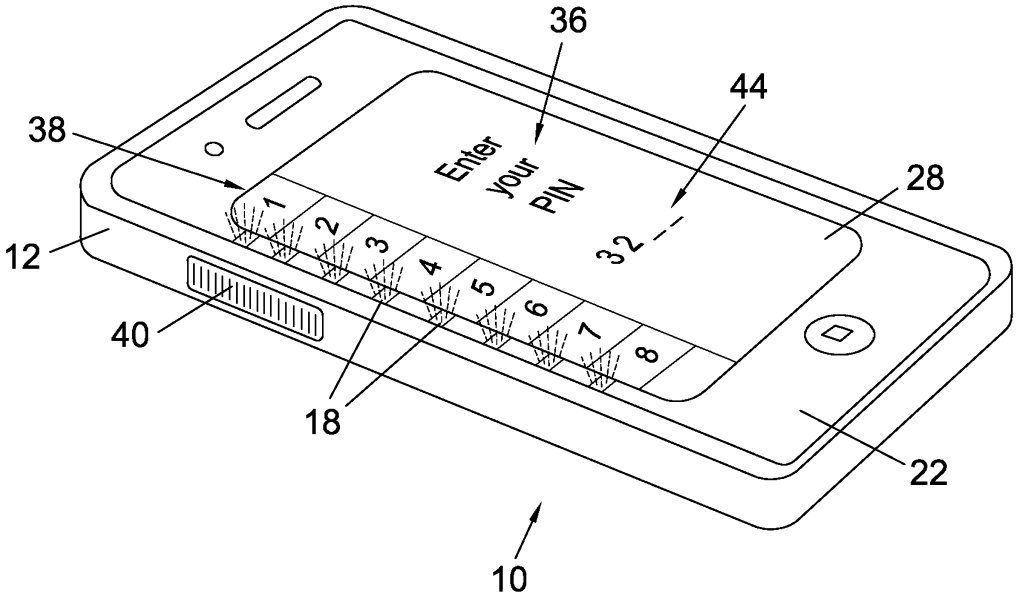
도면3a


28
36
Telephone UK 3G 14:31
TrustPIN
Enter PIN
38
3
1 2 3 4 5 6 7 8 9
18
22
12
46
10

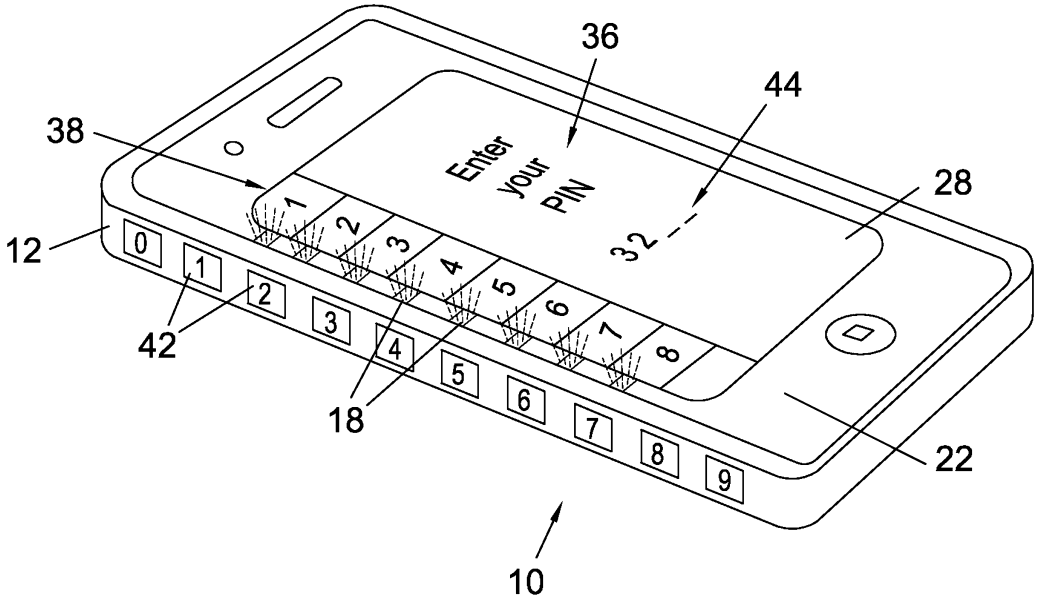
도면3b


사용자
모바일 디바이스
케이스
문자들과 함께 PIN을 입력하라는 메시지를 표시(S300)
임의로 하나의 LED를 발광함(S302)
발광된 LED의 위치의 스크린을 터치하고, 원하는 문자로 스크롤함(S304)
터치와 움직임을 감지함; 케이스로 전송함 (S306)
사용자의 움직임에 부합하도록 발광되는 LED를 변경함(S308)
원하는 위치에 스크린을 릴리즈 함(S310)
접촉이 릴리즈된 위치를 검출하고 케이스로 전송함(S312)
yes
(선택적) 확인 기간을 위해 당해 위치의 LED의 깜빡거림을 유발함(S314)
LED와 대응되는 문자를 판정함(저장함) (S316)
yes
문자가 더 입력될지 여부를 판단함(S318)
no
end

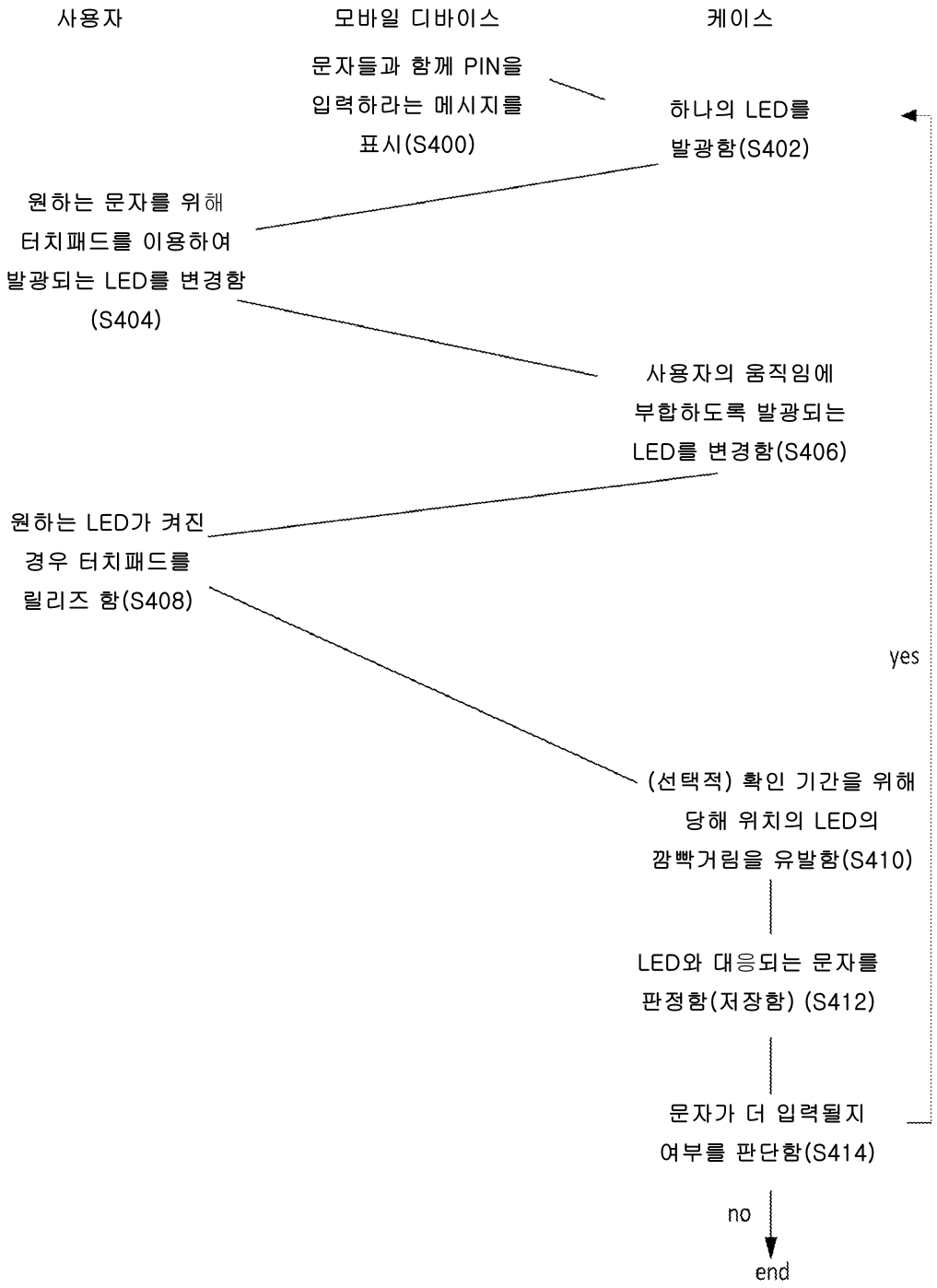
도면4a


36
44
38
Enter your PIN
28
12
32
40
18
22
10

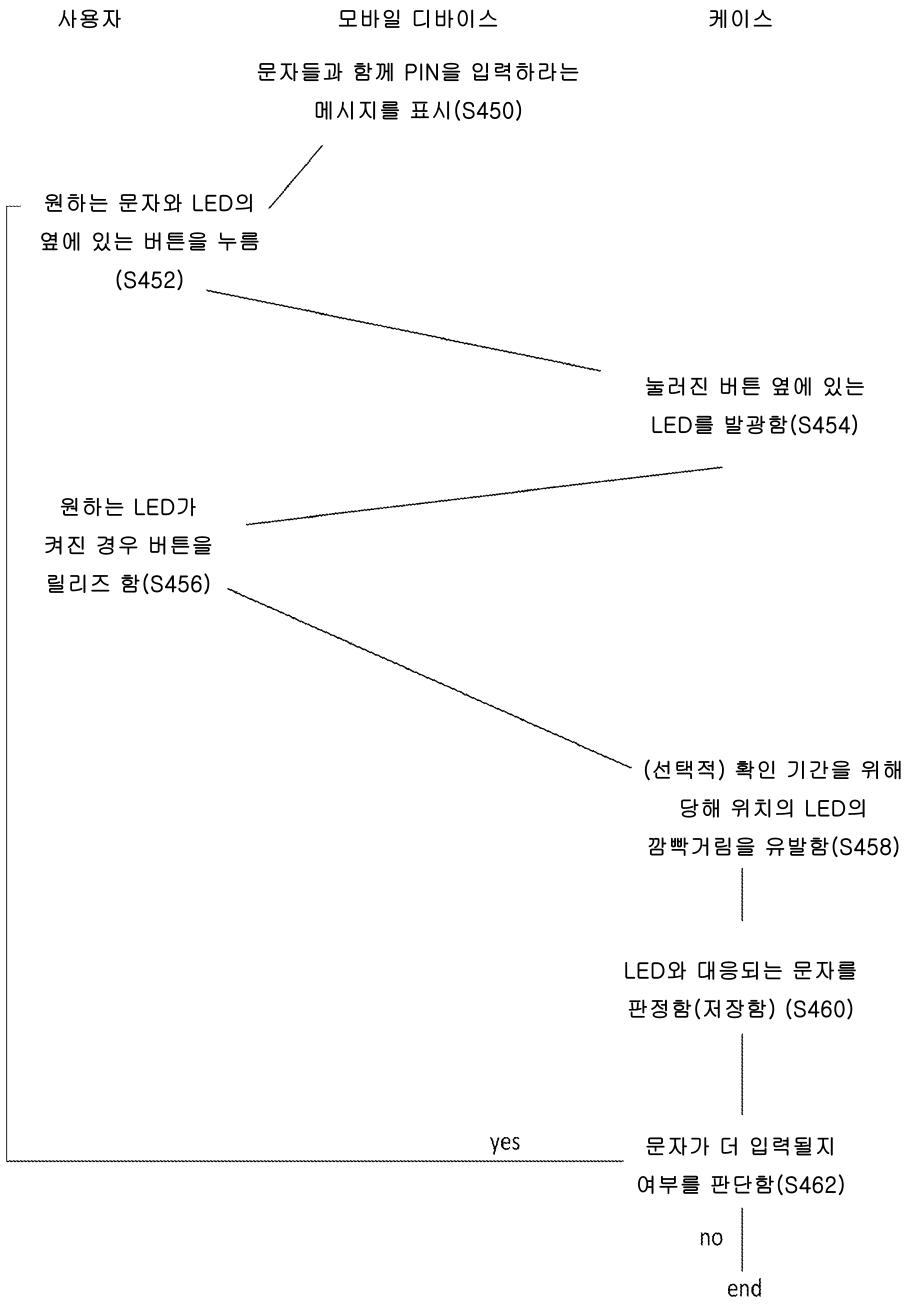
도면4b


36
44
38
Enter your PIN
28
12
32
42
18
22
10

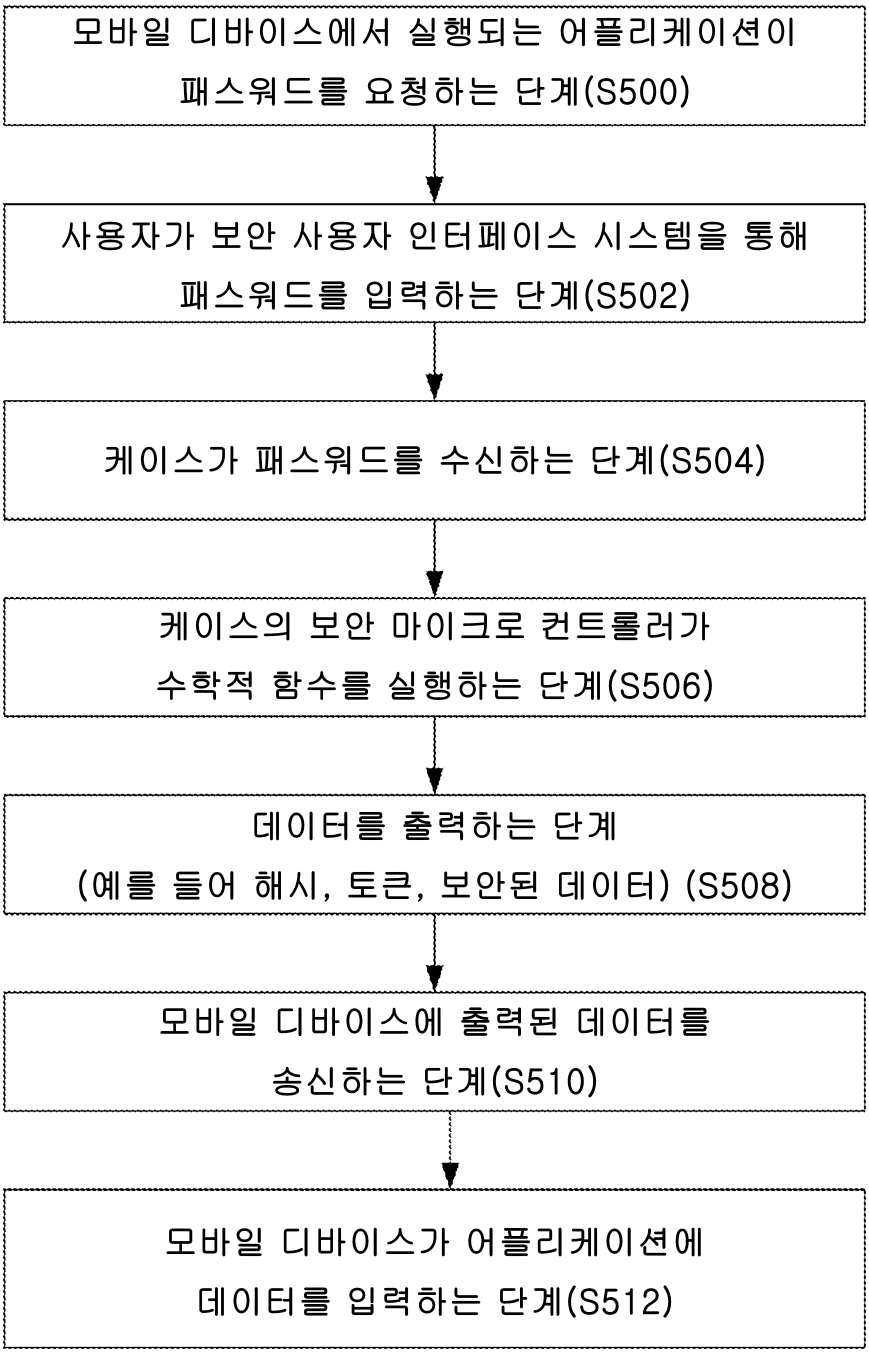
도면4c


사용자
모바일 디바이스
케이스
문자들과 함께 PIN을 입력하라는 메시지를 표시(S400)
하나의 LED를 발광함(S402)
원하는 문자를 위해 터치패드를 이용하여 발광되는 LED를 변경함 (S404)
사용자의 움직임에 부합하도록 발광되는 LED를 변경함(S406)
원하는 LED가 켜진 경우 터치패드를 릴리즈 함(S408)
(선택적) 확인 기간을 위해 당해 위치의 LED의 깜빡거림을 유발함(S410)
LED와 대응되는 문자를 판정함(저장함) (S412)
문자가 더 입력될지 여부를 판단함(S414)
yes
no
end

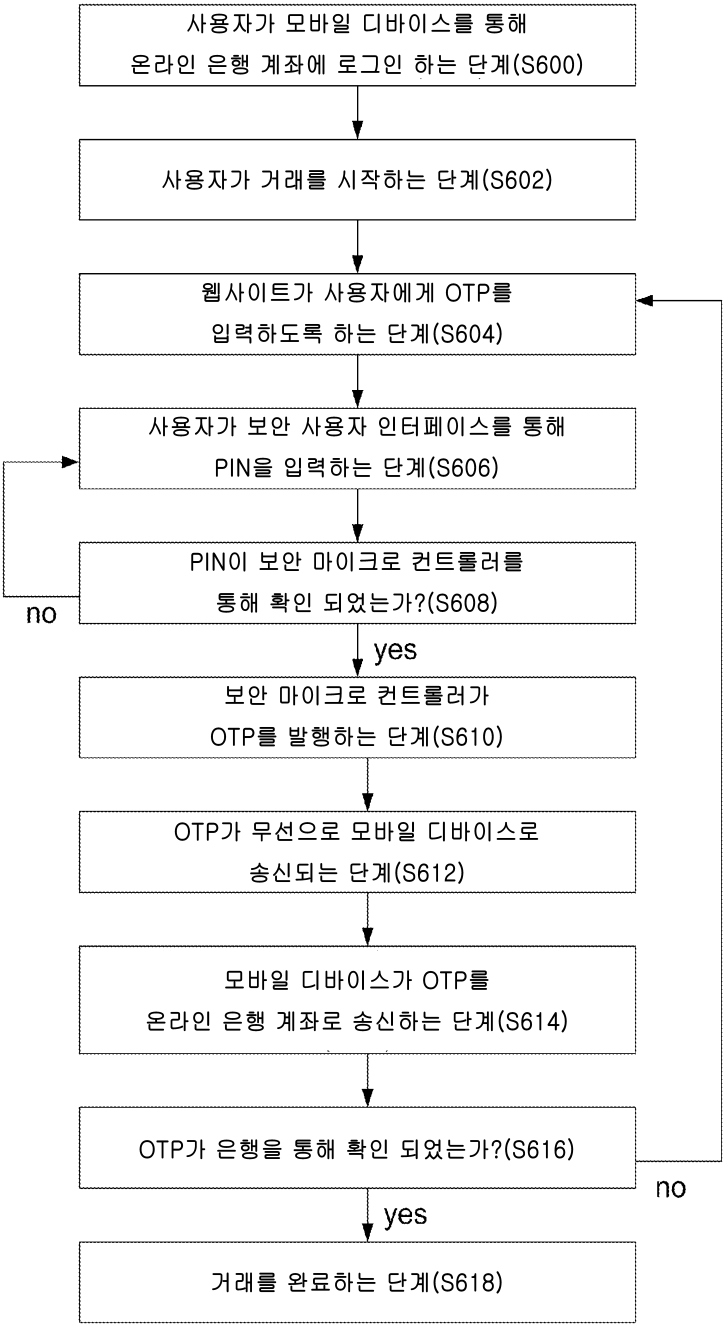
도면4d


사용자
모바일 디바이스
케이스
문자들과 함께 PIN을 입력하라는
메시지를 표시(S450)
원하는 문자와 LED의
옆에 있는 버튼을 누름
(S452)
눌러진 버튼 옆에 있는
LED를 발광함(S454)
원하는 LED가
켜진 경우 버튼을
릴리즈 함(S456)
(선택적) 확인 기간을 위해
당해 위치의 LED의
깜빡거림을 유발함(S458)
LED와 대응되는 문자를
판정함(저장함) (S460)
문자가 더 입력될지
여부를 판단함(S462)
yes
no
end

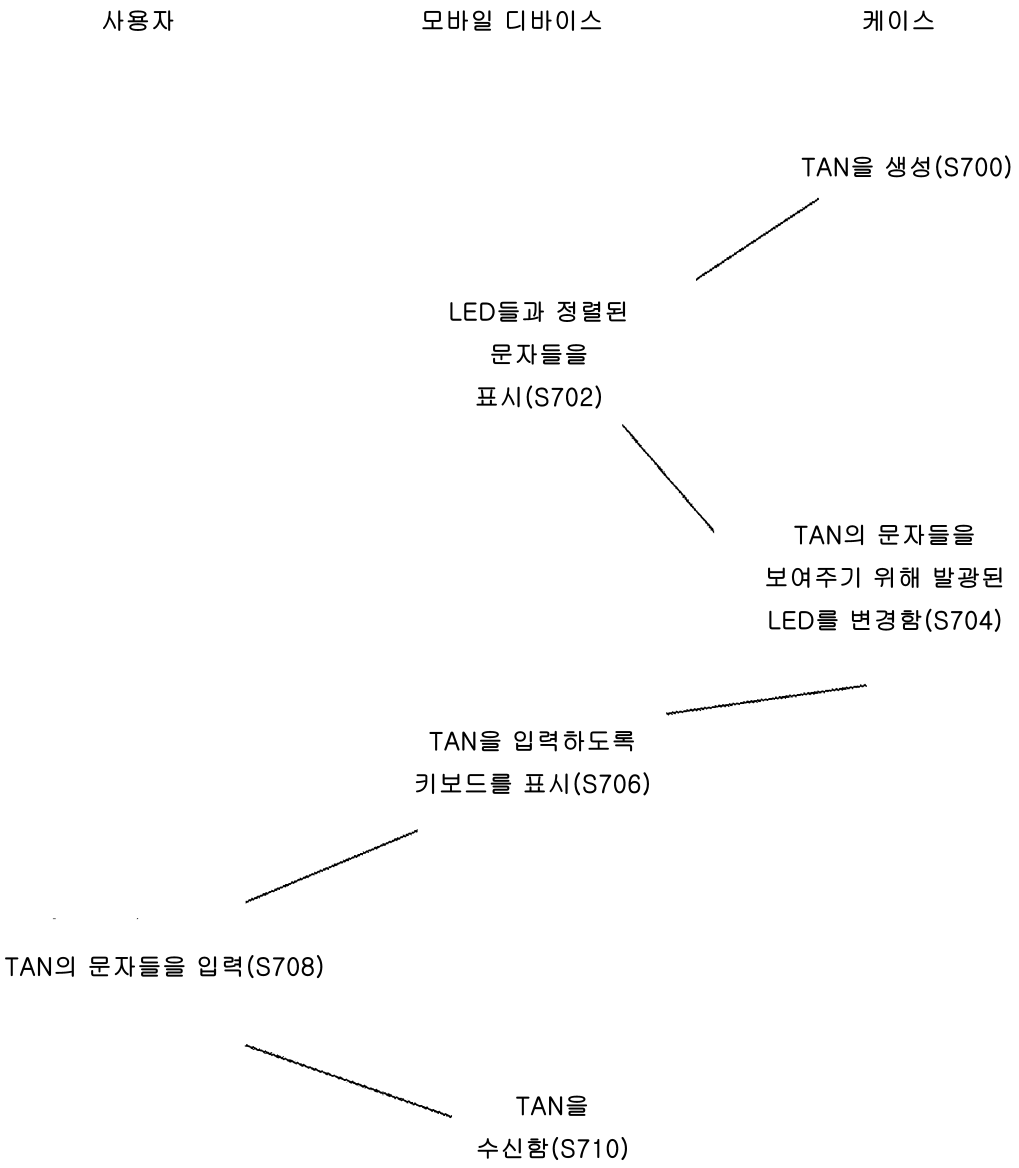
도면5


모바일 디바이스에서 실행되는 어플리케이션이
패스워드를 요청하는 단계(S500)
사용자가 보안 사용자 인터페이스 시스템을 통해
패스워드를 입력하는 단계(S502)
케이스가 패스워드를 수신하는 단계(S504)
케이스의 보안 마이크로 컨트롤러가
수학적 함수를 실행하는 단계(S506)
데이터를 출력하는 단계
(예를 들어 해시, 토큰, 보안된 데이터) (S508)
모바일 디바이스에 출력된 데이터를
송신하는 단계(S510)
모바일 디바이스가 어플리케이션에
데이터를 입력하는 단계(S512)

도면6


사용자가 모바일 디바이스를 통해
온라인 은행 계좌에 로그인 하는 단계(S600)
사용자가 거래를 시작하는 단계(S602)
웹사이트가 사용자에게 OTP를
입력하도록 하는 단계(S604)
사용자가 보안 사용자 인터페이스를 통해
PIN을 입력하는 단계(S606)
PIN이 보안 마이크로 컨트롤러를
통해 확인 되었는가?(S608)
no
yes
보안 마이크로 컨트롤러가
OTP를 발행하는 단계(S610)
OTP가 무선으로 모바일 디바이스로
송신되는 단계(S612)
모바일 디바이스가 OTP를
온라인 은행 계좌로 송신하는 단계(S614)
OTP가 은행을 통해 확인 되었는가?(S616)
no
yes
거래를 완료하는 단계(S618)

도면7


사용자
모바일 디바이스
케이스
TAN을 생성(S700)
LED들과 정렬된
문자들을
표시(S702)
TAN의 문자들을
보여주기 위해 발광된
LED를 변경함(S704)
TAN을 입력하도록
키보드를 표시(S706)
TAN의 문자들을 입력(S708)
TAN을
수신함(S710)