(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 17/00
G06F 15/00

(11) 공개번호 10-2005-0117552
(43) 공개일자 2005년12월14일

(21) 출원번호 10-2005-7016907
(22) 출원일자 2005년09월09일
번역문 제출일자 2005년09월09일
(86) 국제출원번호 PCT/IB2004/050170
국제출원일자 2004년03월01일
(87) 국제공개번호 WO 2004/081767
국제공개일자 2004년09월23일

(30) 우선권주장 03100606.7 2003년03월11일 유럽특허청(EPO)(EP)

(71) 출원인 코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1

(72) 발명자 투일스 핌 티.
네덜란드, 아아 아인드호펜 5656, 홀스트란 6
케베나르 토마스 아. 엠.
네덜란드, 아아 아인드호펜 5656, 홀스트란 6
슈리헨 기르트 제이.
네덜란드, 아아 아인드호펜 5656, 홀스트란 6

(74) 대리인 정상구
신현문
이범래

심사청구 : 없음

(54) 원격 메시지 합성을 인에이블링하는 방법 및 시스템

요약

원격 단말(101)에서 메시지의 합성을 인에이블링하는 방법 및 서버. 방법은 입력 수단을 나타내는 복수의 심볼들을 포함하는 이미지를 생성하는 단계로서, 상기 심볼들은 상기 심볼들 중 적어도 2개의 심볼들에 대하여 상이한 관련된 특정 시각적 특징을 갖는, 상기 이미지 생성 단계; 상기 원격 단말(101) 상에서의 디스플레이를 위하여 상기 이미지를 전송하는 단계; 상기 원격 단말(101)로부터 좌표들의 시퀀스를 수신하는 단계; 상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들에 의해 나타나는 입력 수단의 시퀀스로서 상기 메시지를 재구성하는 단계; 상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들과 관련된 시각적 특징들의 시퀀스로서 인증 코드를 구성하는 단계; 및 상기 인증 코드가 미리 결정된 시각적 특징들의 시퀀스와 일치하면 메시지를 진정한 것으로 하여 받아들이는 단계를 포함한다.

대표도

도 2c

색인어

인증 코드, 원격 단말, 입력 수단, 메시지, 이미지

명세서

기술분야

본 발명은 원격 단말에서 메시지의 합성을 인에이블링하는 방법에 관한 것으로, 입력 수단을 나타내는 복수의 심볼들을 포함하는 이미지를 생성하는 단계; 상기 원격 단말 상에서의 디스플레이를 위하여 상기 이미지를 전송하는 단계; 상기 원격 단말로부터 좌표들의 시퀀스를 수신하는 단계; 및 상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들에 의해 나타나는 입력 수단의 시퀀스로서 상기 메시지를 재구성하는 단계를 포함한다.

본 발명은 또한 서버와 컴퓨터 프로그램에 관한 것이다.

배경기술

제 US-B-6209102호는 원격 단말의 디스플레이 상에서 시각적으로 렌더링된 입력 수단을 통하여 메시지의 합성을 허용하는 방식을 공개한다. 서버는 이미지를 생성하여서, 그 이미지가 키보드 상의 키들과 같은 복수의 입력 수단을 나타낸다. 각각의 입력 수단은 사용자에 의해 포함될 메시지 내에서 사용될 수 있는 요소를 나타낸다.

원격 단말에서, 사용자는, 그 후, 디스플레이 상의 이미지로서 렌더링된 입력 수단을 선택함으로써 사용자가 복귀하기를 원하는 메시지를 포함한다. 입력 수단을 선택하는 것은 단말의 디스플레이 상에서 특정 좌표의 세트를 선택함으로써 이행된다.

좌표의 세트는 그 후, 서버로 다시 전송된다. 비밀리에 원격 단말에 설치된 엿듣기 소프트웨어 또는 단말로부터 서버로 복귀 채널 내에 도청은 이러한 방식으로 입력된 어떤 패스워드들 또는 민감한 정보를 알 수 없다. 무엇보다도, 그러한 소프트웨어는 이 특정 세션에서 입력된 특정 좌표의 세트를 알 수 없을 것이다. 이미지 수단의 배치를 매번 랜덤화함으로써, 따라서, 알게된 정보는 앞으로의 세션에서는 필요 없다.

서버가 좌표의 세트를 수신할 때, 서버는 그 좌표의 세트를 이미지 상에 나타난 특정 입력 수단으로 변환한다. 사용자에 의해 포함된 메시지는 좌표의 세트들이 변환되었던 특정 입력 수단에 의해 나타난 요소들로서 구성된다.

위에 기술된 시스템의 문제점은 서버가 응답이 정말로 의도된 사용자로부터 유래한 것인지 확신할 수 없는 것이다. 적(adversary)은, 예를 들어, 어떤 랜덤 위치들을 랜덤하게 선택할 수 있고, 그들을 서버로 되돌려 보낼 수 있다. 서버는 의도된 정직한 사용자에 의한 유효하지 않은 응답으로부터 그러한 응답을 구별할 수 없다. 달리 말하면, 단말로부터 서버에의 어떠한 메시지 인증도 없다.

또한, '스왑(swap)' 공격이 가능하다. 적이 서버로 전송된 좌표의 세트를 인터셉팅함으로써 유효한 응답을 생성할 수 있고, 단순히 좌표의 일부의 순서를 스와핑할 수 있다. 서버는 이것을 검출하지 못한다. 이것은 메시지가 예를 들어, 은행 계좌번호 또는 은행 계좌로부터 전송되고 인출된 양과 같은 임의의 입력을 나타낼 때, 특히 문제가 된다.

발명의 상세한 설명

본 발명의 목적은 서론에 따른 '스왑' 공격에 대항하여 보호하는 방법을 제공한다.

이 목적은, 본 발명에 따라, 입력 수단을 나타내는 복수의 심볼들을 포함하는 이미지를 생성하는 단계로서, 심볼들은 심볼들 중 적어도 2개의 심볼들에 대하여 상이한 관련된 특정 시각적 특징을 갖는, 이미지 생성 단계; 원격 단말 상에서의 디스플레이를 위하여 이미지를 전송하는 단계; 원격 단말로부터 좌표들의 시퀀스를 수신하는 단계; 수신된 좌표에서 이미지 내에 포함된 심볼들에 의해 나타나는 입력 수단의 시퀀스로서 메시지를 재구성하는 단계; 수신된 좌표에서 이미지 내에 포함된 심볼들과 관련된 시각적 특징들의 시퀀스로서 인증 코드를 구성하는 단계; 및 인증 코드가 미리 결정된 시각적 특징들의 시퀀스와 일치하면 메시지를 진정한 것으로 하여 받아들이는 단계를 포함하는 방법에서 달성될 수 있다.

바람직하게, 시각적 특징은 입력 수단의 컬러 또는 시각적 형태를 포함한다. 단말에 전송된 이미지는 비로소 예를 들어, 2개의 세트의 문자 숫자식 문자들(alphanumeric characters)을 포함하고, 제 1 세트의 문자들은 제 1 컬러이고, 제 2 세트

의 문자들은 제 2 컬러이다. 사용자는 그 후, 제 1 세트로부터 문자를 먼저 선택하고, 그 후, 제 2 세트로부터 문자를 선택함으로써 사용자의 메시지를 포함할 수 있다. 적이 이어서, 좌표의 순서를 반대로 하면, 서버는, 문자들과 관련된 컬러들이 잘못된 순서로 되어있기 때문에, 이 템퍼링(tempering)을 검출할 수 있다.

바람직하게 미리 결정된 시퀀스는 원격 단말의 특정 사용자에 관련된다. 시각적 특징들의 미리 결정된 시퀀스는 그 후, 메시지가 사실 그 특정 사용자에 의해 포함되었다는 증거로서 사용된다. 대안으로, 상이한, 바람직하게, 랜덤하게, 선택된, 미리 결정된 시퀀스는 모든 이미지에 대하여 사용될 수 있고, 이 경우에는, 시퀀스는 이미지 내에 표시되어야 한다.

선택적으로, 인증 코드가 미리 결정된 시퀀스과 일치하면, 경고는 일어난다. 이 방식으로, 적으로부터의 위협하에서 사용자 동작은 비밀리에 경고를 일으킬 수 있다. 적이 경고가 일어났다는 것을 알아차리지 못하도록 메시지는 여전히 받아들여져야 한다. 사용자는 '보통(normal)' 동작용 과 위협용 2개의 미리 결정된 시퀀스들이 할당될 수 있다.

바람직하게, XOR 연산은 사용자와 연산이 원격 단말 상의 디스플레이를 위하여 전송되는 것의 결과에 관련된 키 시퀀스를 사용하여 이미지에 적용된다. 이는 믿을 수 없는 네트워크 상에서 서버로부터 단말로 이미지를 비밀리에 전송하기 위하여 시각적 암호화 기법의 사용을 인에이블링한다. XOR 연산의 결과는 믿을 수 없는 단말 상에 디스플레이될 수 있다. 사용자는 단말 상에 해독 장치를 첨가하여, 이미지를 시각적으로 재구성한다. 메시지의 안전한 합성을 인에이블링하는 시각적 암호화 기법 및 애플리케이션은 유럽 특허 출원 제 02075527.8호(PHNL020121) 및 유럽 특허 출원 제 02078660.4호(PHNL020804)에서 논의된다. 이 설정에서, 모든 이미지에서 새로운 랜덤하게 선택된 미리 결정된 시퀀스를 사용하는 것이 바람직하다. 그 후, 이 시퀀스는 어떠한 방식으로 전송된 이미지 내에 (예를 들어, 입력 수단의 컬러들에 대응하는 컬러들의 시퀀스를 표시함으로써) 표시되어야 한다.

바람직하게, 복수의 좌표들의 시퀀스들은 수신되고, 복수의 개별 메시지들 및 인증 코드들은 재구성되며, 메시지는 모든 개별 메시지들이 동일하고, 모든 인증 코드들이 각각의 미리 결정된 시각적 특징들의 시퀀스들과 일치하면 진정한 것으로 하여 받아들여진다. 이는 적이 유효한 메시지를 여전히 초래하는 방식으로 조정할 수 있는 확률을 상당히 감소시킨다. 단일 메시지가 사용자에 의하여 입력될 때, 예를 들어, 단지 총 4개인 상이한 특징들이 이미지에서 사용되기 때문에 동일한 시각적 특징을 갖는 입력 수단에 대응하는 2개의 좌표의 세트들을 식별하는 것이 가능할 수 있다.

본 발명의 이들 및 다른 특징들은 도면에 도시된 실시예들를 참조하여 명백하고 명확할 수 있다.

도면의 간단한 설명

도 1은 서버 및 여러 단말들을 포함하는 시스템을 개략적으로 도시한 도면.

도 2A, 2B, 2C는 서버에 의해 생성될 수 있는 예 이미지들을 도시한 도면.

도 3A, 3B, 3C는 시각적 암호화 기법을 사용하는 시스템의 실시예를 개략적으로 도시한 도면.

실시예

도면들을 통하여, 동일한 참조 번호들은 유사하거나 대응하는 특징들을 지시한다. 도면들에 지시된 일부 특징들은 일반적으로, 소프트웨어 모듈들 또는 객체들과 같은 소프트웨어 엔티티를 나타내는 소프트웨어 내에 구현된다.

도 1은 서버(100) 및 여러 단말들(101, 102, 103)을 포함하는 본 발명에 따른 시스템을 개략적으로 도시한다. 단말들(101-103)은 여기서, 랩탑 컴퓨터(101), 팜탑 컴퓨터(102) 및 이동 전화(103)로서 실현되나, 그들은 실은, 상호 작용적으로 서버(100)와 통신할 수 있고, 디스플레이 상에 그래픽 이미지를 렌더링할 수 있는 한, 어떤 종류의 디바이스로서도 실현될 수 있다. 통신은 랩탑(101)의 경우와 같이 유선을 통하여 일어날 수 있거나, 팜탑(102) 및 이동 전화(103)와 같은 무선으로 일어날 수 있다. 인터넷 또는 전화 네트워크와 같은 네트워크는 서버(100) 및 임의의 단말들(101-103)과 상호 연결할 수 있다.

서버(100)는 단말(101)의 사용자에게 통신될 필요가 있는 메시지를 나타내는 이미지를 생성한다. 이미지는 키보드 상의 키들과 같은 복수의 입력 수단을 나타낸다. 그러한 키들은 상이한 문자 숫자식 문자들을 나타내는 키들, '예(Yes)', '아니오(No)', '더 많은 정보(more information)'과 같은 선택을 나타내는 버튼들로서 시각적으로 렌더링될 수 있다. 각각의 입력

수단은 사용자에 의해 포함될 메시지에서 사용될 수 있는 요소들을 나타낸다. 키들 다음으로, 입력 수단은 또한 체크박스들, 선택 리스트들, 슬라이더들 또는 사용자 입력을 용이하게 하기 위하여 사용자 인터페이스에 사용되는 다른 요소들일 수 있다. 입력 수단을 시각적으로 나타내는 다른 방식들이 기술에 잘 알려져 있다.

필수적으로 필요하지는 않지만, 상이한 입력 수단은 상이한 심볼들을 나타낼 수 있다는 것이 관찰된다. 동일한 심볼을 나타내는 다수의 입력 수단을 제공하는 것은 시퀀스가 반복들을 포함할 때조차도, 사용자에 의해 만들어진 입력들의 시퀀스가 랜덤처럼 나타날 수 있다는 잇점을 갖는다. 여기서 사용되는 바와 같이, 용어 "심볼(symbol)"은 단일 문자 숫자식 문자들을 의미할 수 있지만, 또한 다른 언어적 또는 심볼의 요소들뿐만 아니라, '예', '아니오' 등과 같은 텍스트를 의미할 수 있다.

어떤 예시의 이미지들은 도 2A, 2B 및 2C에서 도시된다. 모든 심볼들은 심볼들 중 적어도 2개에 대하여 서로 상이한 관련된 특정 시각적 특징을 갖는다. 바람직하게, 시각적 특징은 입력 수단의 컬러 또는 시각적 형태를 포함한다. 도 2A, 2B 및 2C에서, 심볼들은 3개의 그룹들로 그룹화되고, 하나의 그룹의 심볼들은 시각적 특징을 공유하고, 상이한 그룹들의 시각적 특징들은 상이하다. 도 2에서, 그룹들은 상이한 배경 패턴들을 갖는다. 도 2B에서, 그룹들은 서로 상이한 형태들을 갖는다.

도 2C에서, 그룹들은 상이한 컬러들(그레이스케일 값들)을 갖는다. 입력 수단을 나타내는 심볼들은 지금 또한 이미지 상에 (유사-)랜덤 방식으로 분포된다. 이 방식으로, 그들의 위치는 응답을 조정하기를 바라는 적에 의해 추측될 수 없다. 또한, 도 2C에서 입력 수단이 선택되는 순서의 표시(201)가 있다.

도 1을 참조하면, 서버(100)는 생성된 이미지를 디스플레이를 위하여 단말(101)에 전송한다. 사용자는 그 후, 키 또는 디스플레이 상에 이미지로서 렌더링될 수 있는 다른 입력 수단을 선택함으로써, 사용자가 서버(100)에 전송하기를 원하는 메시지를 포함한다.

입력 수단을 선택하는 것은 단말(101)의 디스플레이 상에 특정 좌표의 세트를 선택함으로써 이행된다. 바람직하게 사용자는 디스플레이의 특정 스팟에 압력을 적용함으로써 좌표의 세트를 입력하고, 좌표의 세트는 특정 스팟에 대응한다. 터치 감지 스크린이 장착된 디스플레이는 그 후, 압력이 적용된 스팟에 등록하고, 이를 좌표의 세트로 변환한다. 물론, 마우스, 그래픽 타블렛 또는 키보드와 같은 다른 입력 장치들이 또한 사용될 수 있다.

그 후, 좌표의 세트는 서버(100)로 다시 전송된다. 서버(100)가 죄표들의 세트를 수신할 때, 서버는 좌표의 세트를 이미지 상에 나타난 특정 입력 수단으로 변환한다. 사용자에 의해 포함된 메시지는 죄표의 세트가 변환되는 특정 입력 수단에 의해 나타나는 요소들로서 구성된다. 예를 들어, 도 2C의 이미지를 사용하면, 결과는 7-3-1 또는 4-9-1일 수 있다. 적에 의해 생성된 랜덤 좌표는 일반적으로 입력 수단에 대응하지 않을 것이고, 그래서, 메시지는 유효한 메시지와 쉽게 구별될 수 있다.

구성된 메시지가 인증된 것인지를 확인하기 위하여, 서버(100)는 다음으로 인증 코드를 구성한다. 서버(100)는 비로소 수신된 좌표에서 원래의 이미지 내에 포함된 심볼들과 관련된 시각적 특징들의 시퀀스를 구성한다. 예를 들어, 도 2C의 이미지를 사용하면, 결과는 블랙-그레이-화이트 또는 그레이-그레이-화이트일 수 있다. 도 2B의 경우에 결과는 정사각형-원-부등변 4각형일 수 있다. 서버(100)는 인증 코드가 미리 결정된 시각적 특징들의 시퀀스와 일치하면 진정한 것으로 하여 메시지를 받아들인다.

미리 결정된 시퀀스는 도 2의 경우에서처럼 이미지에 대하여 고유하고, 표시(201)은 우선 블랙 입력 심볼을 사용하고, 그 후 그레이스케일 심볼, 그리고 마지막으로 화이트 심볼을 사용함으로써 사용자가 그의 메시지를 포함해야 한다는 것을 사용자에게 알려주도록 사용된다. 결과 7-3-1은 블랙 '7' 심볼, 그레이 '3' 심볼 및 화이트 '1' 심볼이 그 순서로 사용자에 의해 선택되었다면, 진정한 것으로 하여 받아들여질 것이다.

대안으로, 미리 결정된 시퀀스는 사용자와 관련될 수 있다. 예를 들어, 서버(100)는 사용자의 리스트와 그 사용자들이 사용할 시퀀스들의 리스트를 유지할 수 있다. 한 사용자는 "정사각형-원-부등변 4각형(square-circle-trapezoid)"가 할당될 수 있고, 다른 사용자는 "원-부등변 4각형-정사각형(circle-trapezoid-square)"이 할당될 수 있다. 두 사용자 모두는 도 2b의 이미지를 사용할 수 있다.

한 사용자는 2개의 미리 결정된 시퀀스들이 또한 할당될 수 있고, 그들 중 하나는 사용자가 위협 하에 단말(101)을 동작할 때만, 사용되기로 되어있다. 이 경우에, 서버(100)는 경고(미도시)를 촉발한다. 두 시퀀스들 모두 적이 경고가 일어난 것을 모르게 하기 위해 진정한 것으로 하여 받아들인다.

c를 입력되어야 하는 다음 숫자의 적당한 컬러의 영역으로서 정의하고, A를 총 디스플레이 영역으로서 정의한다. 성공적인 대체 공격을 수행할 확률 P_s는 비로소 (1보다 작은 비례 인수를 갖는) 심볼 당

$$\frac{c}{A}$$

에 비례하게 된다. 이 확률을 더 감소시키기 위해서, 사용자는 매번 사용되는 상이한 미리 결정된 시퀀스들과 함께 사용자의 메시지를 k번 (k>1) 타이핑하도록 요청될 수 있다. 이 경우, 확률은,

$$\left(\frac{c}{A}\right)^{k}$$

에 비례한다.

시스템의 안정성을 더 증가시키기 위하여, 바람직한 실시예에서, 서버(100)는 시각적 암호화 기법에 기초하여 정보 유닛들의 시퀀스로서 이미지를 인코딩한다. 이는 바람직하게 단말(101)의 사용자에 관련된 키 시퀀스를 사용하여 이미지 내에 모든 픽셀에 XOR 연산을 적용함으로써 이행된다. 결과는 이미지 자체 대신에 단말(101)에 전송된다. 메시지들의 안전한 합성을 인에이블하는 시각적 암호화 기법 및 애플리케이션은 유럽 특허 출원 제 02075527.8호(PHNL020121) 및 유럽 특허 출원 제 02078660.4호(PHNL020804)에서 논의된다. 이들 애플리케이션들은 인코딩된 이미지와 키 시퀀스를 디스플레이하기 위하여 액정 디스플레이들(LDCs)을 사용하여, 시각적 암호화 기법을 논한다. '고전(Classical)' 시각적 암호화 기법은 투명한 시트들을 사용하고, 인코딩할 때, 모든 픽셀을 픽셀들의 블럭으로 바람직하게, 2x2 또는 2x1 픽셀들로 매핑하는 것을 필요로 한다. 이는 또한 위에 언급한 유럽 특허 출원에서 논의된다.

시각적 암호화 기법을 사용하는 것은, 예를 들어, 전송 전에, 인코딩된 시퀀스를 암호화하거나, 안전한 인증된 채널을 설정함으로써 더 이상 전송을 보호할 필요가 없는 것을 의미한다. 키 시퀀스가 사용 가능하지 않고 조심스럽게 선택되지 않는다고 가정하면, 엿듣는 사람이 단지 인코딩된 시퀀스를 사용함으로써 이미지를 복구하는 것은 불가능하다. 시각적으로 인코딩된 이미지의 해독은 지금 더 자세히 기술될 것이다.

또한 개인용 해독 장치(110)가 도 1에 도시된다. 이 장치(110)는, 서버(100)에 의해 임의의 단말들(101-103)로 보내진 시각적으로 인코딩된 메시지들을 해독하기 위하여 사용되어야 하기 때문에, 사용자에게 개인적이며, 잘 보호되어야 한다. 해독 장치(110)에 대해 물리적 제어를 얻은 누구도 사용자를 위해 의도된 모든 시각적으로 암호화된 메시지들을 판독할 수 있다. 어떤 여분의 안정성을 부가하기 위하여, 패스워드 또는 개인 식별 번호(PIN: Personal Identification Number)를 입력하는 것은 해독 장치(110)의 활성 시 요구될 수 있다. 장치(110)는 또한 지문 판독기가 제공될 수 있거나, 적법한 소유자에 의한 음성 명령을 인지하기 위하여 장착될 수 있다.

해독 장치(110)는 디스플레이(111) 및 저장 영역(112)을 포함한다. 디스플레이(111)는 바람직하게 LCD 스크린으로서 실현된다. 일반적으로 그러한 디스플레이(111)가 액정층의 양면들 상에 편광 필터를 가질 수 있지만, 이 실시예에서는, 디스플레이(111)는 단지 하나의 편광 필터를 갖는다. 시각적으로 암호화된 메시지를 수신하는 단말(101)의 LCD 스크린은 그 후, 최상부의 편광 필터의 부분을 제거해야 한다. 이 부분은 디스플레이(111)가 위에 포개지는 것을 허용할 만큼 커야한다. 대안으로, 단말(101)의 LCD 스크린은 디스플레이(111)가 포개질 수 있는 (바람직하게 작은) 분리된 디스플레이가 제공될 수 있다. 다른 실시예에서, 디스플레이(111)는 어떤 편광 필터도 갖지 않는다.

저장 영역(112)은 시각적으로 암호화된 이미지들을 해독하는 데 있어서 사용되기 위하여 키 시퀀스를 포함한다. 키 시퀀스의 요소들은 디스플레이(111) 내의 셀들의 편광의 임의의 회전을 나타낸다.

단말(101)이 인코딩된 시퀀스를 수신할 때, 단말은 도 3A에 도시된 바와 같이, LCD 스크린(301)의 부분 상에서 각각의 픽셀들로서 시퀀스의 요소들을 디스플레이한다. 인코딩된 시퀀스는 인코딩된 시퀀스의 개별 요소들에 의해 표시된 양만큼 디스플레이(301) 내의 액정층에서 각각의 셀들의 편광을 회전함으로써 디스플레이된다.

그 후, 사용자는 도 3B에서 해독 장치(110)를 활성화한다. 이는 해독 장치(110)이 저장 영역(112)에 저장된 키 시퀀스에 상관없이 디스플레이(111) 상에 그래픽 표현을 출력하게 한다. 도 3C에서, 사용자는 디스플레이(301) 상에 디스플레이되는 픽셀 상에 개인용 해독 장치(110)를 포갠다. 해독 장치(110) 및 단말(101) 모두 각각 시각적으로 암호화된 이미지의 하나의 셰어(share)를 효과적으로 디스플레이하기 때문에, 사용자는 비로소 재구성된 이미지를 관찰할 수 있다. 도 3C의 예에서, 재구성된 메시지는 그레이스케일 바를 밑에 갖는 블랙 레터링(lettering)으로된 텍스트 메시지 "A!"이다.

단말(101) 또는 개인용 해독 장치(110) 모두 언제나 이미지를 재구성하기 위하여 충분한 정보를 가지고 있지 않기 때문에, 이미지의 컨텐트들은 각 장치 상에서 구동되는 악성 코드 애플리케이션에 의해 복구될 수 없다. 또한 개인용 해독 장치(110)가 어떤 통신 수단도 가지고 있지 않기 때문에, 해독 장치(110)의의 물리적 액세스를 얻지않고 저장 영역(112)으로부터 키 시퀀스를 얻는 것은 불가능하다.

위에 언급된 실시예들은 본 발명을 제한하기보다 도시하는 것이 주지되어야 하고, 당업자들은 첨부된 청구범위의 범위에 벗어나지 않고 많은 대안의 실시예들을 설계할 수 있을 것이라는 것이 주지되어야 한다. 예를 들어, 시각적 암호화 기법을 사용하는 것은 필수적이 아니다. 이미지는 또한 종래의 비밀 키 및/또는 공개 키 암호화 알고리즘들을 사용하여 암호화될 수 있다. 이미지는 암호화되지 않고 안전한 채널 즉, 공격자가 도청할 수 없는 채널 상으로 보내질 수 있다.

본 발명은 서버로부터 단말로 및/또는 그 반대로의 안전한 통신이 필요한 어떤 종류의 시스템에서 사용될 수 있다. 원격 단말들(101-105)은 개인용 컴퓨터들, 랩탑들, 이동 전화들, 팜탑 컴퓨터들, 현금 자동 입출금기들, 공공 인터넷 액세스 단말들 등으로서 실현될 수 있다.

청구범위에서, 괄호 안에 위치된 어떤 참조 부호들은 청구항을 제한하는 것으로서 여겨지지 않아야 한다. 단어 "포함하다(comprising)"는 청구항에 나열된 요소들 및 단계들 외의 요소들 및 단계들의 존재를 배제하지 않는다. 요소 앞의 단수표현은 복수의 그러한 요소들의 존재를 배제하지 않는다.

본 발명은 여러 별개의 요소들을 포함하는 하드웨어에 의해, 그리고 적절히 프로그래밍된 컴퓨터에 의해 구현될 수 있다. 여러 수단을 열거하는 장치 청구항에서, 여러 이들 수단은 하나의 그리고 동일한 하드웨어의 아이템에 의해서 실현될 수 있다. 어떤 수단들이 상호 독립적인 청구범위에서 열거되는 단순한 사실은 이들 수단들의 조합이 이롭게하기 위해 사용될 수 없다는 것을 나타내지 않는다.

(57) 청구의 범위

청구항 1.

원격 단말(101)에서 메시지의 합성을 인에이블링하는 방법에 있어서,

입력 수단을 나타내는 복수의 심볼들을 포함하는 이미지를 생성하는 단계로서, 상기 심볼들은, 상기 심볼들 중 적어도 2개의 심볼들에 대하여 상이한, 관련된 특정 시각적 특징을 갖는, 상기 이미지 생성 단계;

상기 원격 단말(101) 상에서의 디스플레이를 위하여 상기 이미지를 전송하는 단계;

상기 원격 단말(101)로부터 좌표들의 시퀀스를 수신하는 단계;

상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들에 의해 나타낸 입력 수단의 시퀀스로서 상기 메시지를 재구성하는 단계;

상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들과 관련된 시각적 특징들의 시퀀스로서 인증 코드를 구성하는 단계; 및

상기 인증 코드가 미리 결정된 시각적 특징들의 시퀀스와 일치하면 메시지를 진정한 것으로 하여 받아들이는 단계를 포함하는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 2.

제 1 항에 있어서, 상기 시각적 특징은 상기 심볼의 컬러를 포함하는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 3.

제 1 항에 있어서, 상기 시각적 특징은 상기 심볼의 형태를 포함하는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 4.

제 1 항에 있어서, 상기 미리 결정된 시퀀스에서 상기 시각적 특징들의 순서는 (유사(pseudo)) 랜덤하게 선택되고, 상기 순서의 표시는 상기 이미지 내에 포함되는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 5.

제 1 항에 있어서, 상기 미리 결정된 시퀀스는 상기 원격 단말(101)의 특정 사용자와 관련되는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 6.

제 5 항에 있어서, 상기 인증 코드가 상기 미리 결정된 시퀀스과 일치하면,경고가 발생하는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 7.

제 4 항 또는 제 5 항에 있어서, XOR 연산은 상기 사용자와 관련된 키 시퀀스를 사용하여 상기 이미지에 적용되고, 상기 연산의 결과는 상기 원격 단말(101) 상에서의 디스플레이를 위해 전송되는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 8.

제 1 항에 있어서, 상기 이미지 내의 상기 심볼들은 (유사-) 랜덤 방식으로 분포되는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 9.

제 1 항에 있어서, 복수의 좌표들의 시퀀스들이 수신되고, 복수의 개별 메시지들과 인증 코드들은 재구성되며, 상기 메시지는 모든 개별 메시지들이 동일하고 모든 인증 코드들이 각각의 미리 결정된 시각적 특징들의 시퀀스들과 일치하면, 진정한 것으로 하여 받아들여 지는, 원격 단말에서 메시지의 합성을 인에이블링하는 방법.

청구항 10.

원격 단말(101)에서 메시지의 합성을 인에이블링하는 서버(100)에 있어서,

입력 수단을 나타내는 복수의 심볼을 포함하는 이미지를 생성하는 이미지 생성 수단으로서, 상기 심볼들은 상기 심볼들 중 적어도 2개의 심볼들에 대하여 상이한 관련된 특정 시각적 특징을 갖는, 상기 이미지 생성 수단;

상기 원격 단말(101) 상에서의 디스플레이를 위하여 상기 이미지를 전송하는 전송 수단;

상기 원격 단말(101)로부터 좌표들의 시퀀스를 수신하는 수신 수단;

상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들에 의해 나타나는 입력 수단의 시퀀스로서 상기 메시지를 재구성하는 메시지 재구성 수단; 및

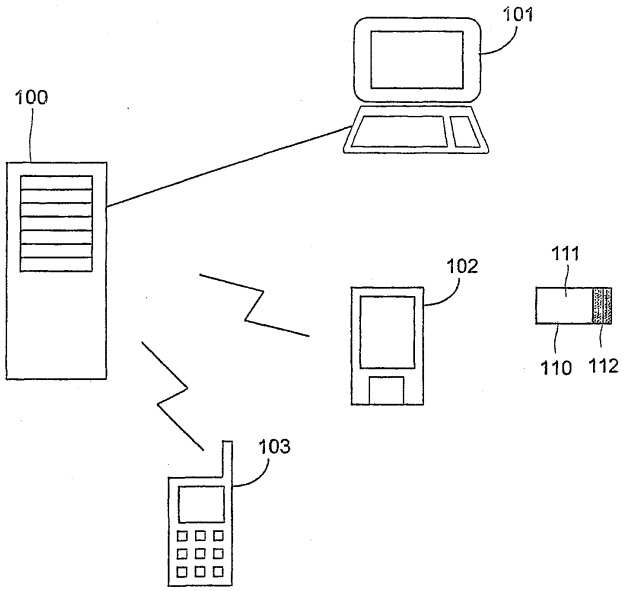
상기 수신된 좌표에서 상기 이미지 내에 포함된 상기 심볼들과 관련된 시각적 특징들의 시퀀스로서 인증 코드를 구성하고, 상기 인증 코드가 미리 결정된 시각적 특징들의 시퀀스와 일치하면 상기 메시지를 진정한 것으로 하여 받아들이는 인증 수단을 포함하는, 원격 단말에서 메시지의 합성을 인에이블링하는 서버.

청구항 11.

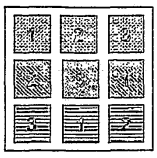
프로세서가 상기 제 1 항의 방법을 실행하게 하도록 배열된 컴퓨터 프로그램 제품.

도면

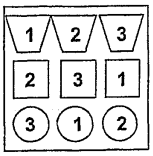
도면1



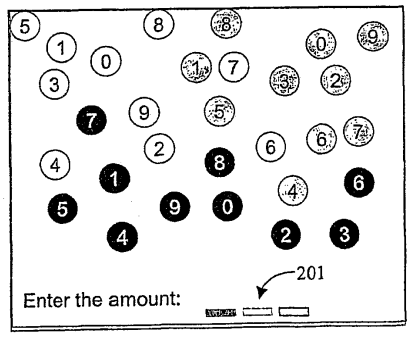
도면2a



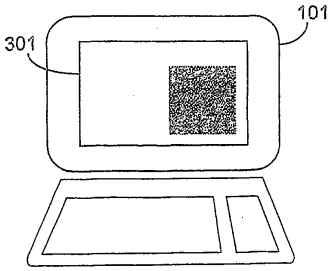
도면2b



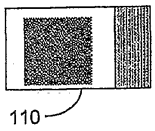
도면2c



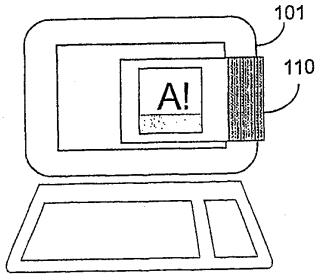
도면3



도. 3a



도. 3b



도. 3c