



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0133073

(43) 공개일자 2015년11월27일

(51) 국제특허분류(Int. Cl.)

G06F 21/33 (2013.01)

(21) 출원번호 10-2014-0059933

(22) 출원일자 2014년05월19일

심사청구일자 2014년05월19일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

한치근

경기도 성남시 분당구 정자일로 15, 103동 603호 (금곡동, 분당하우스토리)

강효관

경기도 수원시 영통구 봉영로 1517번길 73, 909동 1801호 (영통동 벽적골 9단지)

(74) 대리인

유미특허법인

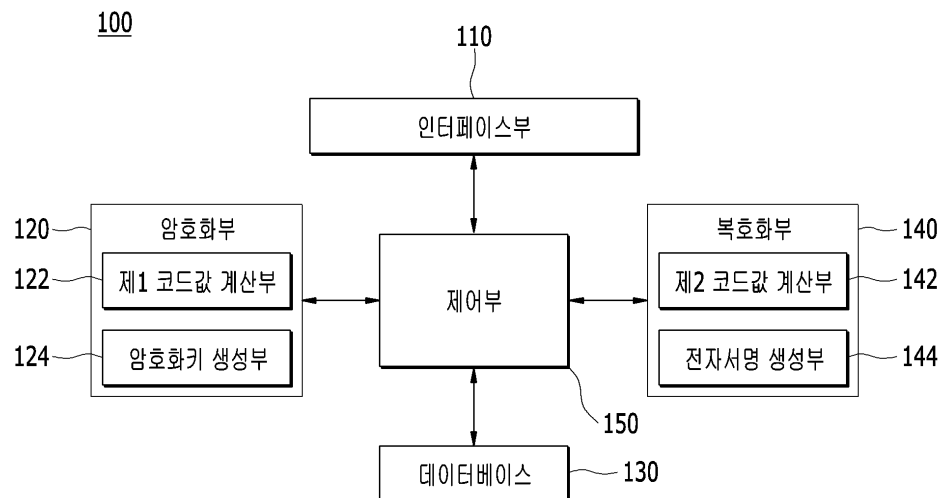
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 전자서명 생성 장치 및 이를 이용한 전자서명 생성 방법

(57) 요약

본 발명에 따른 전자서명 생성 방법은 전자서명 생성 장치가 전자서명을 생성하는 방법에서, 사용자 단말이 선택한 적어도 하나 이상의 이미지와 동작을 이용해 인증서의 개인키를 암호화하는 단계, 상기 사용자 단말로부터 상기 이미지와 상기 동작을 입력 받는 단계, 그리고 입력된 상기 이미지와 상기 동작을 이용해 상기 인증서의 개인키를 복호화하여 전자서명을 생성하는 단계를 포함한다.

대표도 - 도1



명세서

청구범위

청구항 1

전자서명 생성 장치가 전자서명을 생성하는 방법에서,
사용자 단말이 선택한 적어도 하나 이상의 이미지와 동작을 이용해 인증서의 개인키를 암호화하는 단계,
상기 사용자 단말로부터 상기 이미지와 상기 동작을 입력 받는 단계, 그리고
입력된 상기 이미지와 상기 동작을 이용해 상기 인증서의 개인키를 복호화하여 전자서명을 생성하는 단계를 포함하는 전자서명 생성 방법.

청구항 2

제1항에서,
상기 개인키를 암호화하는 단계는,
복수개의 이미지를 사용자 단말에 표시하는 단계,
상기 사용자 단말로부터 이미지를 선택 받는 단계, 그리고
상기 사용자 단말로부터 상기 선택된 이미지와 매칭시킬 동작을 입력받는 단계를 포함하는 전자서명 생성 방법.

청구항 3

제2항에서,
상기 개인키를 암호화하는 단계는,
상기 사용자 단말로부터 이미지를 추가적으로 선택 받고, 추가적으로 선택된 이미지와 매칭시킬 동작을 추가적으로 입력받는 단계를 더 포함하는 전자서명 생성 방법.

청구항 4

제1항에서,
상기 개인키를 암호화하는 단계는,
상기 이미지와 상기 동작에 따른 제1 코드값을 계산하고, 상기 제1 코드값의 단방향 암호화를 통해 제1 암호화키를 생성하는 단계, 그리고
생성된 상기 제1 암호화키를 사용하여 상기 개인키를 암호화하는 단계를 포함하는 전자서명 생성 방법.

청구항 5

제1항에서,
상기 이미지와 상기 동작을 입력 받는 단계는,
상기 사용자 단말이 선택한 이미지를 포함하는 이미지 팝업을 제공하는 단계, 그리고
상기 사용자 단말로부터 상기 암호화하는 단계에서 설정한 이미지를 선택받고, 선택된 이미지와 매칭시킨 동작을 수신하는 단계

를 포함하는 전자서명 생성 방법.

청구항 6

제5항에서,

상기 이미지와 상기 동작을 입력 받는 단계는,

상기 암호화하는 단계에서 설정된 이미지가 복수개인 경우, 설정된 복수개의 이미지를 순차적으로 선택 받으면서 각 이미지에 매칭되는 동작을 수신하는 단계

를 포함하는 전자서명 생성 방법.

청구항 7

제4항에서,

상기 전자서명을 생성하는 단계는,

상기 사용자 단말로부터 선택된 이미지와 동작을 기준으로 제2 코드값을 계산하는 단계, 그리고

상기 제2 코드값을 기반으로 제2 암호화키를 생성하는 단계

를 포함하는 전자서명 생성 방법.

청구항 8

제7항에서,

상기 전자서명을 생성하는 단계는,

상기 제1 코드값과 상기 제2 코드값이 일치하거나, 상기 제1 암호화키와 상기 제2 암호화키가 일치하는 경우, 상기 제2 암호화키를 이용해 상기 개인키를 복호화하여 전자서명을 생성하는 단계

를 더 포함하는 전자서명 생성 방법.

청구항 9

제1항에서,

상기 동작은,

우방향 또는 좌방향 사선, 원, 수평선, 점 또는 수직선 중 적어도 하나 이상을 포함하는 전자서명 생성 방법.

청구항 10

사용자 단말에 이미지 팝업을 제공하고, 상기 사용자 단말로부터 이미지를 선택받고, 선택된 이미지와 매칭시킬 동작을 수신하는 인터페이스부, 그리고

사용자 단말 별로 선택된 적어도 하나 이상의 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화하는 암호화부

를 포함하는 전자서명 생성 장치.

청구항 11

제10항에서,

상기 암호화부에서 설정된 이미지와 동작을 사용자 단말로부터 수신하고, 수신된 이미지와 동작을 이용해 상기 인증서의 개인키를 복호화하여 전자서명을 생성하는 복호화부

를 더 포함하는 전자서명 생성 장치.

청구항 12

제11항에서,

상기 암호화부는,

상기 이미지와 상기 동작에 따른 제1 코드값을 계산하는 제1 코드값 계산부, 그리고

상기 코드값으로 단방향 암호화를 통해 제1 암호화키를 생성해 상기 개인키를 암호화하는 암호화키 생성부를 포함하는 전자서명 생성 장치.

청구항 13

제12항에서,

상기 복호화부는,

수신된 이미지와 동작을 기준으로 제2 코드값을 계산하는 제2 코드값 계산부, 그리고

상기 제2 코드값을 기반으로 제2 암호화키를 생성하여 상기 개인키를 복호화해 전자서명을 생성하는 전자서명 생성부

를 포함하는 전자서명 생성 장치.

청구항 14

제13항에서,

상기 동작은,

점, 선, 또는 도형 중 적어도 하나 이상을 포함하는 전자서명 생성 장치.

발명의 설명

기술 분야

[0001] 본 발명은 전자서명 생성 장치 및 이를 이용한 전자서명 생성 방법에 관한 것이다.

배경 기술

[0002] 최근 상거래나 서비스 영역에 대한 대가를 지불하는 수단으로 신용카드를 많이 사용하고 있으며, 전자 상거래 및 금융관련 업무에서 공인인증서를 이용해 사용자의 신원을 확인하는 용도로 사용하고 있다.

[0003] 현재 국내에서 공인인증서를 이용할 때 기존의 공개키 기반 구조(Public Key Infrastructure, PKI) 기술이 이용하고 있다. 이러한, PKI 기술에서는 사용자가 키보드를 통해서 입력하는 문자를 패스워드로 사용한다. 따라서, 기존의 기술은 키보드 후킹 프로그램 등의 각종 악성 프로그램을 통해 유출될 수 있는 단점이 있다.

[0004] 그리고, 스마트폰을 비롯한 각종 터치기반의 각종 장비가 활성화될수록 기존 키보드 기반의 입력보다는 터치 기반의 입력을 고려한 시스템이 필요하며, 또한, 키보드 후킹을 통한 보안 취약점을 대응할 수 있는 방안이 요구된다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 인증서의 보안을 강화할 수 있는 전자서명 생성 장치 및 이를 이용한 전자서명 생성 방법을 제안하고자 한다.

과제의 해결 수단

[0006] 본 발명의 전자서명 생성 방법은 전자서명 생성 장치가 전자서명을 생성하는 방법에서, 사용자 단말이 선택한 적어도 하나 이상의 이미지와 동작을 이용해 인증서의 개인키를 암호화하는 단계, 상기 사용자 단말로부터 상기 이미지와 상기 동작을 입력 받는 단계, 그리고 입력된 상기 이미지와 상기 동작을 이용해 상기 인증서의 개인키를 복호화하여 전자서명을 생성하는 단계를 포함한다.

- [0007] 상기 개인키를 암호화하는 단계는, 복수개의 이미지를 사용자 단말에 표시하는 단계, 상기 사용자 단말로부터 이미지를 선택 받는 단계, 그리고 상기 사용자 단말로부터 상기 선택된 이미지와 매칭시킬 동작을 입력받는 단계를 포함할 수 있다.
- [0008] 상기 개인키를 암호화하는 단계는, 상기 사용자 단말로부터 이미지를 추가적으로 선택 받고, 추가적으로 선택된 이미지와 매칭시킬 동작을 추가적으로 입력받는 단계를 더 포함할 수 있다.
- [0009] 상기 개인키를 암호화하는 단계는, 상기 이미지와 상기 동작에 따른 제1 코드값을 계산하고, 상기 제1 코드값의 단방향 암호화를 통해 제1 암호화키를 생성하는 단계, 그리고 생성된 상기 제1 암호화키를 사용하여 상기 개인키를 암호화하는 단계를 포함할 수 있다.
- [0010] 상기 이미지와 상기 동작을 입력 받는 단계는, 상기 사용자 단말이 선택한 이미지를 포함하는 이미지 팝업을 제공하는 단계, 그리고 상기 사용자 단말로부터 상기 암호화하는 단계에서 설정한 이미지를 선택받고, 선택된 이미지와 매칭시킨 동작을 수신하는 단계를 포함할 수 있다.
- [0011] 상기 이미지와 상기 동작을 입력 받는 단계는, 상기 암호화하는 단계에서 설정된 이미지가 복수개인 경우, 설정된 복수개의 이미지를 순차적으로 선택 받으면서 각 이미지에 매칭되는 동작을 수신하는 단계를 포함할 수 있다.
- [0012] 상기 전자서명을 생성하는 단계는, 상기 사용자 단말로부터 선택된 이미지와 동작을 기준으로 제2 코드값을 계산하는 단계, 그리고 상기 제2 코드값을 기반으로 제2 암호화키를 생성하는 단계를 포함할 수 있다.
- [0013] 상기 전자서명을 생성하는 단계는, 상기 제1 코드값과 상기 제2 코드값이 일치하거나, 상기 제1 암호화키와 상기 제2 암호화키가 일치하는 경우, 상기 제2 암호화키를 이용해 상기 개인키를 복호화하여 전자서명을 생성하는 단계를 더 포함할 수 있다.
- [0014] 상기 동작은, 우방향 또는 좌방향 사선, 원, 수평선, 점 또는 수직선 중 적어도 하나 이상을 포함할 수 있다.
- [0015] 본 발명의 전자서명 생성 장치는 사용자 단말에 이미지 팝업을 제공하고, 상기 사용자 단말로부터 이미지를 선택받고, 선택된 이미지와 매칭시킬 동작을 수신하는 인터페이스부, 그리고 사용자 단말 별로 선택된 적어도 하나 이상의 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화하는 암호화부를 포함한다.
- [0016] 상기 암호화부에서 설정된 이미지와 동작을 사용자 단말로부터 수신하고, 수신된 이미지와 동작을 이용해 상기 인증서의 개인키를 복호화하여 전자서명을 생성하는 복호화부를 더 포함할 수 있다.
- [0017] 상기 암호화부는, 상기 이미지와 상기 동작에 따른 제1 코드값을 계산하는 제1 코드값 계산부, 그리고 상기 코드값으로 단방향 암호화를 통해 제1 암호화키를 생성해 상기 개인키를 암호화하는 암호화키 생성부를 포함할 수 있다.
- [0018] 상기 복호화부는, 수신된 이미지와 동작을 기준으로 제2 코드값을 계산하는 제2 코드값 계산부, 그리고 상기 제2 코드값을 기반으로 제2 암호화키를 생성하여 상기 개인키를 복호화해 전자서명을 생성하는 전자서명 생성부를 포함할 수 있다.
- [0019] 상기 동작은, 점, 선, 또는 도형 중 적어도 하나 이상을 포함할 수 있다.

발명의 효과

- [0020] 본 발명에 따르면, 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화함으로써, 인증서에 대한 보안을 강화하고, 키 입력에 대한 후킹 등을 통한 인증서 및 개인키의 비밀번호 유출을 방지할 수 있는 환경을 제공한다.

도면의 간단한 설명

- [0021] 도 1은 본 발명의 한 실시예에 따른 전자서명 생성 장치를 간략히 도시한 도면이다.
- 도 2는 본 발명의 한 실시예에 따른 전자서명 생성 장치가 전자서명을 생성하는 과정을 간략히 도시한 흐름도이다.
- 도 3은 본 발명의 한 실시예에 따라 이미지와 동작을 조합하는 예를 도시한 도면이다.
- 도 4는 기존 방법에 따라 인증서 발급시에 문자로 비밀번호를 입력하는 예를 도시한 도면이다.

도 5는 본 발명의 한 실시예에 따라 인증서 발급시에 이미지와 동작으로 개인키를 암호화하는 예를 도시한 도면이다.

도 6은 본 발명의 한 실시예에 따라 인증서 사용시에 이미지와 동작을 입력해 전자서명을 생성하는 예를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 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.
- [0023] 명세서 전체에서, 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.
- [0024] 또한, 명세서에 기재된 "...부", "...모듈" 의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.
- [0025] 이제 도 1 내지 도 6을 참고하여 본 발명의 한 실시예에 따른 전자서명 생성 장치 및 이를 이용한 전자서명 생성 방법에 대하여 상세하게 설명한다.
- [0026] 도 1은 본 발명의 한 실시예에 따른 전자서명 생성 장치를 간략히 도시한 도면이다. 이때, 전자서명 생성 장치는 본 발명의 실시예에 따른 설명을 위해 필요한 개략적인 구성만을 도시할 뿐 이러한 구성에 국한되는 것은 아니다.
- [0027] 도 1을 참조하면, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 전자서명 생성에 필요한 개인키를 안전하게 보관하기 위해 사용자가 입력한 이미지와 동작을 기반으로 개인키 암호화키를 생성하고 이를 암호화하는 기능과 전자서명 생성을 위해 개인키를 복호화하고 이를 통해 전자서명문을 생성하는 기능을 가진다. 또한, 여기서, 전자서명 생성 장치(100)는 인증서의 신규 발급, 및 갱신 시 또는 기 발급된 인증서 개인키의 비밀번호 변경 시에 개인키를 다시 암호화할 수 있다.
- [0028] 그리고, 전자서명 생성 장치(100)는 본 발명의 한 실시예에 따라 인터페이스부(110), 암호화부(120), 데이터베이스(130), 복호화부(140) 및 제어부(150)를 포함한다.
- [0029] 인터페이스부(110)는 사용자 단말에 다수의 이미지가 표시된 이미지 팝업을 제공한다. 그리고, 인터페이스부(110)는 인증서의 개인키를 암호화하기 위해서 사용자 단말로부터 이미지를 선택 받고, 선택된 이미지와 매칭시킬 동작을 수신한다. 여기서, 동작은 점, 선, 또는 원 중 적어도 하나 이상을 포함하며, 본 발명의 한 실시예에 따라 우방향 또는 좌방향 사선, 원, 점, 수평선 또는 수직선 중 적어도 하나 이상을 포함할 수 있다.
- [0030] 그리고, 전자서명 생성 장치(100)는 인터페이스부(110)를 통해 사용자 단말이 원하는 만큼 복수개의 이미지와 동작을 반복적으로 수신하고, 수신된 복수개의 이미지와 동작을 이용해 개인키의 암호화를 수행할 수 있다.
- [0031] 또한, 전자서명 생성 장치(100)는 인터페이스부(110)를 통해 사용자 단말이 기설정된 이미지 및 동작을 수신함으로써, 암호화된 인증서의 개인키를 복호화할 수 있다.
- [0032] 암호화부(120)는 사용자 단말 별로 선택된 적어도 하나 이상의 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화한다. 그리고, 암호화부(120)는 사용자 단말이 입력한 이미지를 통해서 개인키를 암호화할 대칭키를 생성한다. 여기서, 암호화부(120)는 사용자 단말로부터 수신한 이미지와 동작을 이용해 코드값을 계산하고, 계산된 코드값을 이용해 암호화키를 생성할 수 있다.
- [0033] 그리고, 암호화부(120)는 본 발명의 한 실시예에 따라 제1 코드값 계산부(110) 및 암호화키 생성부(120)를 포함한다.
- [0034] 제1 코드값 계산부(110)는 이미지와 동작에 따른 제1 코드값을 계산하고, 계산된 제1 코드값을 암호화키 생성부(120)에 제공한다.
- [0035] 그리고, 암호화키 생성부(120)는 제1 코드값으로 단방향 암호화를 통해 제1 암호화키를 생성해 인증서의 개인키

를 암호화한다.

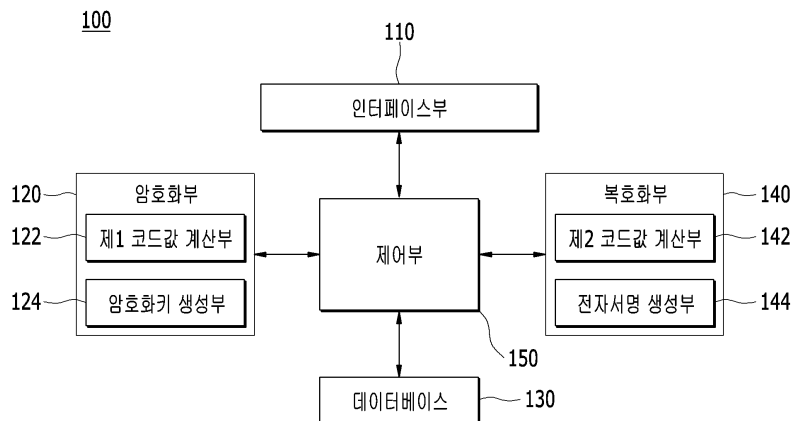
- [0036] 데이터베이스(130)는 암호화부(120)에서 암호화된 개인키를 저장한다. 그리고, 데이터베이스(130)는 인터페이스부(110)에 수신된 이미지와 동작을 저장하거나, 암호화부(120)에서 계산된 제1 코드값 및 제1 암호화키 등 저장하고, 저장된 데이터를 제어부(150)의 요청을 받아 제공할 수 있다.
- [0037] 복호화부(140)는 암호화부(120)에서 설정된 이미지와 동작을 사용자 단말로부터 수신하고, 수신된 이미지와 동작을 이용해 인증서의 개인키를 복호화하여 전자서명을 생성한다.
- [0038] 그리고, 복호화부(140)는 본 발명의 한 실시예에 따라 제2 코드값 계산부(142) 및 전자서명 생성부(144)를 포함한다.
- [0039] 제2 코드값 계산부(142)는 수신된 이미지와 동작을 기준으로 제2 코드값을 계산하고, 계산된 제2 코드값을 전자서명 생성부(144)에 제공한다.
- [0040] 전자서명 생성부(144)는 제2 코드값을 기반으로 제2 암호화키를 생성하여 암호화된 개인키를 복호화해 전자서명을 생성한다. 이때, 전자서명 생성부(144)는 제1 코드값과 제2 코드값을 비교해서 일치하거나, 제1 암호화키와 제2 암호화키를 비교해서 일치하는 경우, 제2 암호화키를 이용해 전자서명을 생성할 수 있다.
- [0041] 제어부(150)는 인터페이스부(110), 암호화부(120), 데이터베이스(130) 및 복호화부(140) 각 부가 원활히 수행하도록 제어한다. 그리고, 제어부(150)는 인터페이스부(110)에 수신된 이미지 및 동작을 데이터베이스(130)에 저장하도록 제어하거나, 암호화부(120) 및 복호화부(140)에 전달하도록 제어한다. 또한, 제어부(150)는 암호화부(120)가 이미지 및 동작을 통해 인증서의 개인키를 암호화하도록 제어하며, 복호화부(140)가 암호화된 인증서의 개인키를 복호화해 전자서명을 생성하도록 제어한다.
- [0042] 따라서, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화함으로써, 인증서에 대한 보안을 강화하고, 키 입력에 대한 후킹 등을 통한 인증서 및 개인키의 비밀번호 유출을 방지할 수 있는 환경을 제공한다.
- [0043] 도 2는 본 발명의 한 실시예에 따른 전자서명 생성 장치가 전자서명을 생성하는 과정을 간략히 도시한 흐름도이다. 이때, 이하의 흐름도는 도 1의 구성과 연계하여 동일한 도면부호를 사용하여 설명한다.
- [0044] 도 2를 참조하면, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 사용자 단말이 설정한 이미지와 동작을 이용해 인증서의 개인키를 암호화한다(S100). 이때, 전자서명 생성 장치(100)는 인증서를 신규 발급 받을 때 개인키를 암호화할 수 있으며, 인증서의 비밀번호를 변경할 때에 개인키를 암호화할 수도 있다.
- [0045] 그리고, 전자서명 생성 장치(100)는 사용자 단말이 개인키를 암호화한 인증서를 사용할 때 인증서 암호 선택창에서 이미지 암호를 입력할 수 있는 이미지 암호 버튼을 제공한다(S110).
- [0046] 그리고, 전자서명 생성 장치(100)는 사용자 단말로부터 인증서의 개인키를 암호화할 때 설정한 이미지와 동작을 수신한다(S120).
- [0047] 그리고, 전자서명 생성 장치(100)는 암호화된 인증서를 사용하기 위해서 사용자 단말로부터 수신된 이미지와 동작을 이용해 인증서의 개인키를 복호화하여 전자서명을 생성한다(S130).
- [0048] 도 3은 본 발명의 한 실시예에 따라 이미지와 동작을 조합하는 예를 도시한 도면이다.
- [0049] 도 3에 도시된 바와 같이, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 각각의 이미지에 서로 다른 패턴을 갖는 동작을 매칭시킬 수 있다. 그리고, 전자서명 생성 장치(100)는 매칭된 이미지와 동작을 이용해 인증서의 개인키를 암호화할 수 있다. 이때, 이미지와 동작의 조합은 사용자 단말이 자유롭게 선택이 가능하다. 그리고, 이미지는 다양하게 변형 또는 변경이 가능하며, 사용자 단말이 원하는 직접 이미지를 입력해 사용할 수도 있다.
- [0050] 도 4는 기존 방법에 따라 인증서 발급시에 문자로 비밀번호를 입력하는 예를 도시한 도면이다. 도 5는 본 발명의 한 실시예에 따라 인증서 발급시에 이미지와 동작으로 개인키를 암호화하는 예를 도시한 도면이다.
- [0051] 도 4에서와 같이, 기존에는 공인인증서 발급시에 영문이나 숫자를 포함한 문자로 인증서의 비밀번호를 입력했다. 따라서, 기존과 같이 문자로 입력하는 경우에는 해킹에 의해 비밀번호가 유출될 수 있어 보안에 취약한 문제가 있었다. 여기서, 공인인증서를 발급받는 과정은 기존 시스템과 동일하므로 생략한다.
- [0052] 그러나, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 도 5에서와 같이, 문자로 된 비밀번호를 입력

받을 때, 사용자 단말로부터 이미지와 동작을 수신 받아 개인키를 암호화할 수 있다.

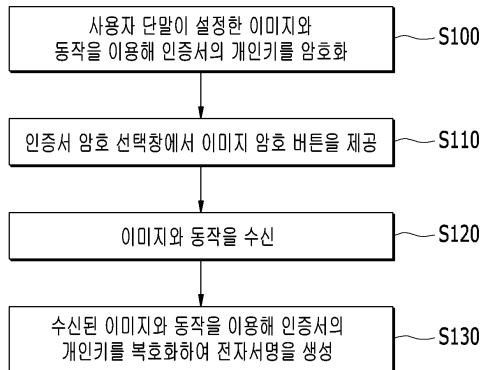
- [0053] 따라서, 전자서명 생성 장치(100)는 사용자 단말로부터 이미지를 선택받고, 선택된 이미지에 지정하는 동작을 입력받는다. 그리고, 전자서명 생성 장치(100)는 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화한다. 이때, 전자서명 생성 장치(100)는 본 발명의 한 실시예에 따라 이미지와 동작 자체를 비밀번호로 대체하여 사용할 수도 있다.
- [0054] 도 6은 본 발명의 한 실시예에 따라 인증서 사용시에 이미지와 동작을 입력해 전자서명을 생성하는 예를 도시한 도면이다.
- [0055] 도 6을 참조하면, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 사용자가 인증서를 사용할 때, 인증서 암호에 이미지 암호 버튼을 제공하고, 이미지 암호 버튼을 클릭하면, 이미지들이 표시된 팝업창을 제공한다.
- [0056] 따라서, 본 발명의 한 실시예에 따른 전자서명 생성 장치(100)는 사용자 단말이 기존에 설정한 이미지를 선택하고, 선택한 이미지와 매칭된 동작을 수행하면, 이를 바탕으로 인증서의 개인키를 복호화해 전자서명을 생성한다.
- [0057] 본 발명에 따르면, 본 발명의 한 실시예에 따른 전자서명 생성 장치 및 전자서명 생성 방법은 이미지와 동작을 매칭시켜 인증서의 개인키를 암호화함으로써, 인증서에 대한 보안을 강화하고, 키 입력에 대한 후킹 등을 통한 인증서 및 개인키의 비밀번호 유출을 방지할 수 있는 환경을 제공한다.
- [0058] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다. 이러한 기록 매체는 서버뿐만 아니라 사용자 단말에서도 실행될 수 있다.
- [0059] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

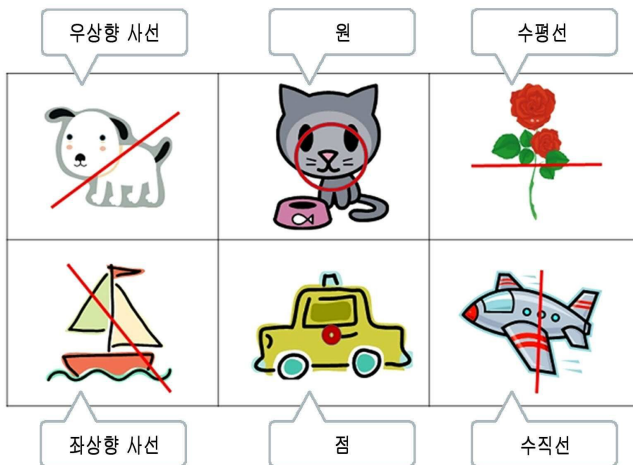
도면1



도면2



도면3



도면4

도면4는 '인증서(전자서명) 비밀번호 입력 [N]' 대화상자의 스크린샷입니다. 대화상자에는 인증서 비밀번호에 대한 안내문과 주의사항이 표시되어 있습니다.

인증서의 비밀 번호는 프로그램에 의하여 별도로 관리되지 않습니다.
인증서 비밀번호를 분실하지 않도록 주의하십시오.
* 영문, 숫자 포함 8자 이상 - 30자 이하(대/소문자 구분)
* 특수문자 이용 권장

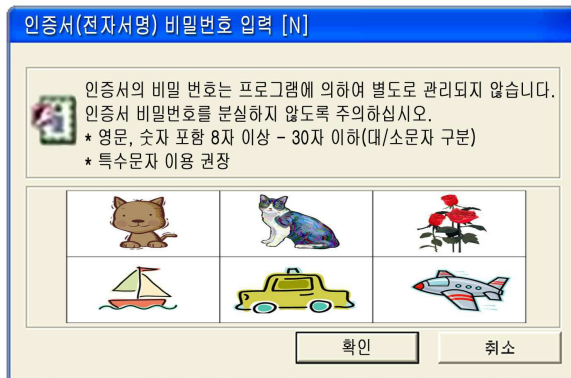
이전 인증서 비밀번호 :

신규 인증서 비밀번호 :

인증서 비밀번호(확인) :

확인 취소

도면5



도면6

