(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0122657
(43) 공개일자 2009년12월01일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 17/00* (2006.01)
H04L 9/00 (2006.01) *G06F 15/00* (2006.01)
(21) 출원번호 10-2008-0048581
(22) 출원일자 2008년05월26일
심사청구일자 2008년05월26일

(71) 출원인
동명대학교산학협력단
부산광역시 남구 용당동 535번지
(72) 발명자
이성운
대구광역시 달성군 가창면 상원리 60번지
김현성
대구광역시 북구 복현2동 서한타운 105동 301호
(74) 대리인
김도형

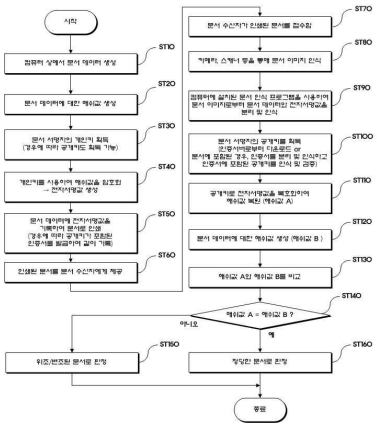
전체 청구항 수 : 총 10 항

(54) 문자 인식을 통한 공개키 기반의 문서위조 방지 방법

(57) 요 약

본 발명은 문서위조 방지 기술에 관한 것으로, 특히 휴대폰과 같은 모바일 장치에 장착된 카메라나 개인 컴퓨터에 연결된 스캐너 등과 문서인식 알고리즘을 사용하여 오프라인 문서의 내용을 인식함으로써 문서내용에 대한 전자서명을 생성하고 추가적으로 문서에 기록하여 문서 내용을 보증할 뿐만 아니라 문서 내용과 전자서명을 검증하여 문서의 위변조를 판단할 수 있는 문서위조 방지 기술에 관한 것이다. 본 발명에 따르면 카메라가 장착된 모바일 장치를 사용하여 시간, 장소에 구애받지 않고 인쇄된 문서나 직접 수기로 작성한 문서를 전자서명할 수 있으며, 전자서명된 문서를 지닌 경우에는 문서를 촬영하는 것만으로 문서의 위변조 여부를 즉석에서 간편하게 확인할 수 있는 효과가 있다. 또한, 전자서명된 문서 발급 시에 전자서명값이나 공개키 포함 인증서를 바코드로 출력하여 원본 문서에 부착할 경우에는 전자서명값을 보다 명확하게 인식할 수 있으며 수신자가 공개키를 쉽게 획득할 수 있는 효과가 있다.

대 표 도 - 도3



특허청구의 범위

청구항 1

(A) 문서 데이터를 입력받고, 상기 문서 데이터에 대한 해쉬값을 생성하고, 문서 서명자의 개인키를 획득하고, 상기 개인키로 상기 해쉬값을 암호화하여 상기 문서 데이터에 대한 전자서명값을 생성하고, 상기 전자서명값이 표시되도록 상기 문서 데이터를 인쇄하는 문서발급 단계; 및

(B) 촬상수단을 통해 문서의 이미지를 입력받고, 문서인식 알고리즘을 이용하여 상기 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식하고, 상기 문서 서명자의 공개키를 획득하고, 상기 공개키로 상기 전자서명값을 복호화하여 해쉬값(이하, '해쉬값 A'라 함)을 복원하고, 상기 인식된 문서 데이터에 대한 해쉬값(이하, '해쉬값 B'라 함)을 생성하고, 상기 해쉬값 A와 상기 해쉬값 B을 비교하여 두 값이 일치하면 상기 문서를 정당한 문서로 판단하는 문서검증 단계;

를 포함하여 구성되는 문서위조 방지 방법.

청구항 2

청구항 1에 있어서,

상기 (A) 문서발급 단계는,

상기 문서 서명자의 공개키를 획득하는 단계; 및

상기 문서 데이터에 상기 공개키가 포함된 인증서를 추가로 표시하여 인쇄하는 단계;

를 더 포함하여 구성되고,

상기 (B) 문서검증 단계에서 상기 공개키를 획득하는 단계는,

상기 이미지로부터 인증서를 분리 및 인식하는 단계; 및

상기 인증서에 포함된 공개키를 인식 및 검증하는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 3

청구항 1에 있어서,

상기 (B) 문서검증 단계에서 상기 공개키를 획득하는 단계는,

인증서버에 접속하는 단계; 및

상기 인증서버로부터 상기 문서 서명자의 공개키를 제공받는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 4

(C) 촬상수단을 통해 문서의 이미지를 입력받고, 문서인식 알고리즘을 이용하여 상기 이미지로부터 문서 데이터를 인식하는 문서인식 단계;

(D) 상기 문서 데이터에 대한 해쉬값을 생성하고, 문서 서명자의 개인키를 획득하고, 상기 개인키로 상기 해쉬값을 암호화하여 상기 문서 데이터에 대한 전자서명값을 생성하고, 상기 전자서명값을 출력하는 문서발급 단계; 및

(E) 촬상수단을 통해 문서의 이미지를 입력받고, 문서인식 알고리즘을 이용하여 상기 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식하고, 상기 문서 서명자에 대한 공개키를 획득하고, 상기 공개키로 상기 전자서명값을 복호화하여 해쉬값(이하, '해쉬값 A'라 함)을 복원하고, 상기 인식된 문서 데이터에 대한 해쉬값(이하, '해쉬값 B'라 함)을 생성하고, 상기 해쉬값 A와 상기 해쉬값 B을 비교하여 두 값이 일치하면 상기 문서를 정당한 문서로 판단하는 문서검증 단계;

를 포함하여 구성되는 문서위조 방지 방법.

청구항 5

청구항 4에 있어서,

상기 (C) 문서인식 단계는,

모바일 장치(이하, '단말기 A'라 함)에 장착된 카메라 수단을 사용하여 문서의 이미지를 입력받는 단계; 및

상기 단말기 A에 내장된 문서인식 알고리즘을 이용하여 상기 이미지로부터 문서 데이터를 인식하는 단계;

를 포함하여 구성된 것을 특징으로 하고,

상기 (D) 문서발급 단계는,

상기 단말기 A에 내장된 해쉬 알고리즘을 이용하여 상기 문서 데이터에 대한 해쉬값을 생성하는 단계;

상기 단말기 A가 상기 문서 서명자의 개인키를 획득하는 단계;

상기 개인키로 상기 해쉬값을 암호화하여 전자서명값을 생성하는 단계; 및

상기 전자서명값을 화면을 통해 표시하는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 6

청구항 5에 있어서,

상기 (E) 문서검증 단계는,

모바일 장치(이하, '단말기 B'라 함)에 장착된 카메라 수단을 사용하여 문서의 이미지를 입력받는 단계;

상기 단말기 B에 내장된 문서인식 알고리즘을 이용하여 상기 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식하는 단계;

상기 단말기 B가 상기 문서 서명자의 공개키를 획득하는 단계;

상기 공개키로 상기 전자서명값을 복호화하여 상기 해쉬값 A를 복원하는 단계;

상기 단말기 B에 내장된 해쉬 알고리즘을 이용하여 상기 인식된 문서 데이터에 대한 상기 해쉬값 B를 생성하는 단계;

상기 해쉬값 A와 상기 해쉬값 B을 비교하는 단계; 및

비교결과 상기 두 값이 일치하면 상기 문서가 정당한 문서임을 나타내는 메시지를 상기 단말기 B의 화면을 통해 표시하는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 7

청구항 6에 있어서,

상기 (D) 문서발급 단계는,

상기 전자서명값에 대응되는 바코드를 생성하는 단계; 및

바코드 출력수단을 통해 상기 바코드를 출력하는 단계;

를 더 포함하여 구성되고,

상기 (E) 문서검증 단계의 전자서명값 분리 및 인식단계는,

상기 이미지로부터 바코드를 분리 및 인식하는 단계; 및

상기 바코드로부터 전자서명값을 판독하는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 8

청구항 4 내지 청구항 7 중 어느 한 항에 있어서,

상기 (D) 문서발급 단계는,

상기 문서 서명자의 공개키를 획득하는 단계; 및

상기 공개키가 포함된 인증서를 출력하는 단계;

를 더 포함하여 구성되고,

상기 (E) 문서검증 단계에서 상기 공개키를 획득하는 단계는,

상기 이미지로부터 인증서를 분리 및 인식하는 단계; 및

상기 인증서에 포함된 공개키를 인식 및 검증하는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 9

청구항 8에 있어서,

상기 (D) 문서발급 단계는,

상기 인증서에 대응되는 바코드를 생성하는 단계; 및

바코드 출력수단을 통해 상기 바코드를 출력하는 단계;

를 더 포함하여 구성되고,

상기 (E) 문서검증 단계에서 상기 공개키를 획득하는 단계는,

상기 이미지로부터 바코드를 분리 및 인식하는 단계;

상기 바코드로부터 인증서를 판독하는 단계; 및

상기 인증서에 포함된 공개키를 인식 및 검증하는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

청구항 10

청구항 4 내지 청구항 7 중 어느 한 항에 있어서,

상기 (E) 문서검증 단계에서 상기 공개키를 획득하는 단계는,

상기 단말기 B가 이동통신망을 통해 인증서버에 접속하는 단계; 및

상기 인증서버로부터 상기 문서 서명자에 대한 공개키를 제공받는 단계;

를 포함하여 구성된 것을 특징으로 하는 문서위조 방지 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 문서위조 방지 기술에 관한 것으로, 특히 휴대폰과 같은 모바일 장치에 장착된 카메라나 개인 컴퓨터에 연결된 스캐너 등과 문서인식 알고리즘을 사용하여 오프라인 문서의 내용을 인식함으로써 문서내용에 대한 전자서명을 생성하고 추가적으로 문서에 기록하여 문서 내용을 보증할 뿐만 아니라 문서 내용과 전자서명을 검증하여 문서의 위변조를 판단할 수 있는 문서위조 방지 기술에 관한 것이다.

배 경 기 술

<2> 지금까지 널리 일반적으로 사용된 종이문서의 수기 서명이나 도장 날인은 문서의 내용이 서명 또는 도장이 대표하는 특정인에 의해 서명되었음을 보증하며 문서의 내용 또한 특정인의 이름을 걸고 보증하는데 사용되고 있다.

<3> 이러한 수기 서명이나 도장 날인의 방식은 사람마다 필적이 다르고 도장의 형태가 다름을 이용하여 타인이 쉽게 모방할 수 없는 효과를 가져온다. 하지만 정밀 검사를 거치지 않는 한 육안으로 판단하는 서명 또는 도장 날인은 타인에 의해 어느 정도 똑같이 흉내 낼 수 있으며, 문서 내용의 경우 외부에 그대로 노출되어 있으므로 문서 내용에 누군가가 일부 내용을 첨가하더라도 수기 서명이나 도장 날인이 처음 그대로의 문서 내용이 유지되었음을 입증할 수 없다는 문제점이 있다.

<4> 이러한 문제점을 극복하기 위해 전자 매체를 통해 전송되는 전자문서에 부여하는 전자서명 방식이 등장하여 사용되고 있다. 전자서명은 암호 기법을 이용한 정보 보호 기능과 인증기능을 활용함으로써 서명에 참여한 서명자 인증과 서명 대상인 전자문서의 인증을 동시에 수행할 수 있다. 따라서, 전자문서를 전송받은 수신자는 타인에 의한 서명 위조 여부를 판별할 수 있으며, 전자문서의 내용이 문서서명자가 서명할 때의 원본 내용 그대로 유지되었는지를 판별할 수 있다.

<5> 그러나, 전자서명을 사용하는 방식은 지금까지 주로 전자 매체를 통해 전송되는 전자문서에 적용되어 사용되고 있으며, 오프라인상에서는 여전히 수기 서명이나 도장 날인의 방식을 통해 문서의 정당성을 보증하는 방식이 사용되고 있다. 전자서명 방식은 전자적인 처리 수단을 통해 문서가 생성된 후 전송매체를 통해 상대방에게 전송되어 검증되는 일련의 과정이 자동적으로 이루어지므로 오프라인상에서 종이문서를 주로 취급하는 개인이나 기관이 손쉽게 사용할 수 없다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<6> 본 발명의 목적은 카메라가 장착된 모바일 장치나 스캐너가 연결된 컴퓨터를 사용하여 손쉽게 전자서명값이 기재된 문서의 위변조 여부를 파악할 수 있는 문서위조 방지 기술을 제공하는 것이다.

과제 해결수단

<7> 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법은 (A) 문서 데이터를 입력받고, 문서 데이터에 대한 해쉬값을 생성하고, 문서 서명자의 개인키를 획득하고, 개인키로 해쉬값을 암호화하여 문서 데이터에 대한 전자서명값을 생성하고, 전자서명값이 표시되도록 문서 데이터를 인쇄하는 문서발급 단계; 및 (B) 촬상수단을 통해 문서의 이미지를 입력받고, 문서인식 알고리즘을 이용하여 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식하고, 문서 서명자의 공개키를 획득하고, 공개키로 전자서명값을 복호화하여 해쉬값(이하, '해쉬값 A'라 함)을 복원하고, 인식된 문서 데이터에 대한 해쉬값(이하, '해쉬값 B'라 함)을 생성하고, 해쉬값 A와 해쉬값 B을 비교하여 두 값이 일치하면 문서를 정당한 문서로 판단하는 문서검증 단계;를 포함하여 구성된다.

<8> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (A) 문서발급 단계는, 문서 서명자의 공개키를 획득하는 단계; 및 문서 데이터에 공개키가 포함된 인증서를 추가로 표시하여 인쇄하는 단계;를 더 포함하여 구성되고, (B) 문서검증 단계에서 공개키를 획득하는 단계는, 이미지로부터 인증서를 분리 및 인식하는 단계; 및 인증서에 포함된 공개키를 인식 및 검증하는 단계;를 포함하여 구성되는 것이 바람직하다.

<9> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (B) 문서검증 단계에서 공개키를 획득하는 단계는, 인증서버에 접속하는 단계; 및 인증서버로부터 문서 서명자의 공개키를 제공받는 단계;를 포함하여 구성되는 것이 바람직하다.

<10> 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법은 (C) 촬상수단을 통해 문서의 이미지를 입력받고, 문서인식 알고리즘을 이용하여 이미지로부터 문서 데이터를 인식하는 문서인식 단계; (D) 문서 데이터에 대한 해쉬값을 생성하고, 문서 서명자의 개인키를 획득하고, 개인키로 해쉬값을 암호화하여 문서 데이터에 대한 전자서명값을 생성하고, 전자서명값을 출력하는 문서발급 단계; 및 (E) 촬상수단을 통해 문서의 이미지를 입력받고, 문서인식 알고리즘을 이용하여 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식하고, 문서 서명자에 대한 공개키를 획득하고, 공개키로 전자서명값을 복호화하여 해쉬값(이하, '해쉬값 A'라 함)을 복원하고, 인식된 문서 데이터에 대한 해쉬값(이하, '해쉬값 B'라 함)을 생성하고, 해쉬값 A와 해쉬값 B을 비교

하여 두 값이 일치하면 문서를 정당한 문서로 판단하는 문서검증 단계;를 포함하여 구성된다.

<11> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (C) 문서인식 단계는, 모바일 장치(이하, '단말기 A'라 함)에 장착된 카메라 수단을 사용하여 문서의 이미지를 입력받는 단계; 및 단말기 A에 내장된 문서인식 알고리즘을 이용하여 이미지로부터 문서 데이터를 인식하는 단계;를 포함하여 구성되고, (D) 문서발급 단계는, 단말기 A에 내장된 해쉬 알고리즘을 이용하여 문서 데이터에 대한 해쉬값을 생성하는 단계; 단말기 A가 문서 서명자의 개인키를 획득하는 단계; 개인키로 해쉬값을 암호화하여 전자서명값을 생성하는 단계; 및 전자서명값을 화면을 통해 표시하는 단계;를 포함하여 구성되는 것이 바람직하다.

<12> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (E) 문서검증 단계는, 모바일 장치(이하, '단말기 B'라 함)에 장착된 카메라 수단을 사용하여 문서의 이미지를 입력받는 단계; 단말기 B에 내장된 문서인식 알고리즘을 이용하여 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식하는 단계; 단말기 B가 문서 서명자의 공개키를 획득하는 단계; 공개키로 전자서명값을 복호화하여 해쉬값 A를 복원하는 단계; 단말기 B에 내장된 해쉬 알고리즘을 이용하여 인식된 문서 데이터에 대한 해쉬값 B를 생성하는 단계; 해쉬값 A와 해쉬값 B을 비교하는 단계; 및 비교결과 두 값이 일치하면 문서가 정당한 문서임을 나타내는 메시지를 단말기 B의 화면을 통해 표시하는 단계;를 포함하여 구성되는 것이 바람직하다.

<13> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (D) 문서발급 단계는, 전자서명값에 대응되는 바코드를 생성하는 단계; 및 바코드 출력수단을 통해 바코드를 출력하는 단계;를 더 포함하여 구성되고, (E) 문서검증 단계의 전자서명값 분리 및 인식단계는, 이미지로부터 바코드를 분리 및 인식하는 단계; 및 바코드로부터 전자서명값을 판독하는 단계;를 포함하여 구성되는 것이 바람직하다.

<14> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (D) 문서발급 단계는, 문서 서명자의 공개키를 획득하는 단계; 및 공개키가 포함된 인증서를 출력하는 단계;를 더 포함하여 구성되고, (E) 문서검증 단계에서 공개키를 획득하는 단계는, 이미지로부터 인증서를 분리 및 인식하는 단계; 및 인증서에 포함된 공개키를 인식 및 검증하는 단계;를 포함하여 구성되는 것이 바람직하다.

<15> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (D) 문서발급 단계는, 인증서에 대응되는 바코드를 생성하는 단계; 및 바코드 출력수단을 통해 바코드를 출력하는 단계;를 더 포함하여 구성되고, (E) 문서검증 단계에서 공개키를 획득하는 단계는, 이미지로부터 바코드를 분리 및 인식하는 단계; 바코드로부터 인증서를 판독하는 단계; 및 인증서에 포함된 공개키를 인식 및 검증하는 단계;를 포함하여 구성되는 것이 바람직하다.

<16> 또한, 본 발명에 따른 문자 인식을 통한 공개키 기반의 문서위조 방지 방법에서 (E) 문서검증 단계에서 공개키를 획득하는 단계는, 단말기 B가 이동통신망을 통해 인증서버에 접속하는 단계; 및 인증서버로부터 문서 서명자에 대한 공개키를 제공받는 단계;를 포함하여 구성되는 것이 바람직하다.

효 과

<17> 본 발명에 따르면 카메라가 장착된 모바일 장치를 사용하여 시간, 장소에 구애받지 않고 인쇄된 문서나 직접 수기로 작성한 문서를 전자서명할 수 있으며, 전자서명된 문서를 지닌 경우에는 문서를 촬영하는 것만으로 문서의 위변조 여부를 즉석에서 간편하게 확인할 수 있는 효과가 있다.

<18> 또한, 전자서명된 문서 발급 시에 전자서명값이나 공개키 포함 인증서를 바코드로 출력하여 원본 문서에 부착할 경우에는 전자서명값을 보다 명확하게 인식할 수 있으며 수신자가 공개키를 쉽게 획득할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<19> 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

<20> 도 1은 본 발명의 제 1 실시예에 따른 문서위조 방지 기술을 구현하기 위한 전체 시스템 구성도이다.

<21> 문서발급 영역(10)에서는 문서 데이터 원본 내용과 문서 서명자의 정당성을 인증하는 전자서명값을 생성하여 이를 문서 데이터와 함께 문서(20)로 인쇄하며, 문서검증 영역(30)에서는 문서(20)에 인쇄된 전자서명값(21)의 유효성을 인증하고 문서(20)에 인쇄된 문서 데이터의 위조 및 변조 여부를 판단한다.

<22> 문서발급 영역(10)에서 문서 서명자(11)는 개인 컴퓨터(12)에 설치된 문서작성 프로그램을 이용하여 문서 데이터를 작성하거나 이미 작성된 문서 데이터를 준비한다. 그리고, 사전에 인증기관(CA : certificate authority)

을 통해 개인키와 공개키를 준비한 후 개인키는 USB 메모리나 모바일 장치 내의 USIM 등과 같은 안전한 개인 저장소에 보관하고 인증기관에 의해 전자서명된 공개키를 포함한 인증서는 인증기관이 운영하는 안전한 공개 저장소에 보관시킨다. 필요에 따라 문서 서명자(11)는 개인키와 함께 자신의 인증서값도 보관할 수 있다.

<23> 개인 컴퓨터(12)에서는 문서 데이터를 해쉬값으로 변환한 후에 개인키를 사용하여 암호화함으로써 전자서명값을 생성하며, 문서 데이터와 전자서명값이 함께 기록된 문서를 생성해낸다. 일반적으로는, 문서 데이터에 서명자 ID 및 서명날짜 등을 포함시키고 여기에 해쉬 알고리즘을 적용하여 해쉬값으로 변환한다.

<24> 문서 서명자(11)의 선택에 따라 문서에 공개키를 추가로 기록할 수도 있다. 일반적으로, 공개키는 인증서에 포함된 형태로 기록된다. 해쉬값과 전자서명값을 생성하는 과정에 대해서는 이후 도 5를 통해 보다 상세히 설명하기로 한다.

<25> 프린터(13)는 개인 컴퓨터(12)에서 생성된 문서(20)를 인쇄한다.

<26> 따라서, 문서(20)에는 문서 데이터의 내용뿐만 아니라 문서 데이터의 정당한 서명을 보증하는 전자서명값이 함께 기재된다. 서명자 ID와 서명날짜를 포함시켜 해쉬값을 산출한 경우에는 서명자 ID와 서명날짜도 함께 기재된다.

<27> 이처럼 종이 문서의 형태로 문서 데이터(서명자 ID 및 서명날짜 포함)와 전자서명값(21)이 함께 기재된 문서(20)는 문서발급 영역(10)을 벗어나 문서검증 영역(30)의 수신자에게 전달된다.

<28> 문서검증 영역(30)에서 촬상수단(32)은 문서(20)의 이미지를 인식하여 디지털 이미지로 변환한다. 촬상수단(32)으로는 카메라(321) 및 스캐너(322) 등이 사용된다.

<29> 수신자 개인 컴퓨터(31)는 촬상수단(32)과 연결되어 촬상수단(32)을 통해 인식된 문서 이미지를 제공받는다.

<30> 또한, 수신자 개인 컴퓨터(31)에는 문서인식 프로그램이 설치되어 있어서 촬상수단(32)을 통해 제공받은 문서 이미지로부터 문서 데이터(서명자 ID 및 서명날짜 포함)와 전자서명값을 분리 및 인식해낸다.

<31> 그리고, 수신자 개인 컴퓨터(31)는 전자서명값으로부터 해쉬값을 복원하고, 또한 문서 데이터(서명자 ID 및 서명날짜 포함)로부터 해쉬값을 산출하여 이 두 종류의 해쉬값의 일치여부를 통해 문서의 정당성을 검증해낸다.

<32> 이때, 전자서명값으로부터 해쉬값을 복원하기 위해서는 문서 서명자(11)에 대한 공개키가 필요한데, 공개키는 네트워크(40)를 통해 인증서버(50)에 접속하여 제공받을 수도 있으며 또는 문서 서명자(11)가 문서(20)에 공개키가 포함된 인증서를 함께 기록해놓은 후에 수신자 개인 컴퓨터(31)의 문서인식 프로그램을 통해 인증서를 추출해내어 공개키를 얻을 수도 있다.

<33> 공개키와 전자서명값을 사용하여 문서의 정당성을 검증하는 과정에 대해서는 이후 도 6을 통해 보다 상세히 설명하기로 한다.

<34> 도 2는 본 발명의 제 2 실시예에 따른 문서위조 방지 기술을 구현하기 위한 전체 시스템 구성도이다.

<35> 제 1 실시예와의 차이점은 사람이 손으로 작성했거나 이미 인쇄된 문서에 대하여 전자서명값을 생성할 수 있다는 점이다. 따라서, 문서검증자뿐만 아니라 문서발급자도 촬상수단과 문서인식 프로그램을 구비해야 한다.

<36> 또한, 이에 덧붙여서 개인 컴퓨터를 갖출 필요없이 카메라가 장착된 휴대폰 등의 모바일 장치를 통해 전자서명값을 생성하거나 문서를 검증할 수 있다. 이를 위해서는 모바일 장치에 카메라가 장착되어 있어야 하고, 문서인식 프로그램, 해쉬 알고리즘, 개인키/공개키를 통한 암호화/복호화 기능이 구비되어 있어야 한다. 그러나, 구현 방식에 따라 모바일 장치에서는 문서 이미지만 인식하고 나머지 연산과정은 별도의 연산처리 서버를 두어 처리하도록 시스템을 구성하는 것도 가능하다.

<37> 문서발급 영역(60)에서는 문서 데이터의 원본 내용과 서명의 정당성을 인증하는 전자서명값을 생성하여 화면을 통해 보여주며, 문서검증 모바일 장치(80)에서는 문서(70)에 기재된 전자서명값(71)의 유효성을 인증하고 문서(70)에 기재된 문서 데이터의 위조 및 변조 여부를 판단한다.

<38> 문서발급 영역(60)에서 문서 서명자(61)는 직접 손으로 써서 문서(62)를 작성하거나 또는 다른 곳에서 수집한 문서 내용들을 스크랩하여 오프라인상의 인쇄된 문서(62)를 마련한다. 즉, 문서 서명자(61)에 의해 마련된 문서(62)는 디지털화되지 않은 아날로그 데이터이다.

<39> 문서발급 모바일 장치(63)는 카메라가 장착되어 있는 휴대폰 등의 모바일 장치로서, 문서 서명자(61)의 조작에 의해 문서(62)의 이미지를 인식한다. 그리고, 내장된 문서인식 프로그램을 통해 문서 이미지로부터 문서 데이터

를 생성해낸다.

<40> 그리고, 문서발급 모바일 장치(63)는 문서 데이터를 해쉬값으로 변환한 후에 개인키를 사용하여 암호화함으로써 전자서명값을 생성한다. 일반적으로는, 문서 데이터에 서명자 ID 및 서명날짜 등을 포함시키고 여기에 해쉬 알고리즘을 적용하여 해쉬값으로 변환한다. 해쉬값과 전자서명값을 생성하는 과정은 이후 도 5를 통해 보다 자세히 설명한다.

<41> 이때, 개인키는 앞서 도 1에서 설명한 바와 같이 사전에 인증기관을 통해 미리 준비해둔 후 USB 메모리나 모바일 장치 내의 USIM 등과 같은 안전한 개인 저장소에 보관한다. 또한, 공개키의 경우에도 인증기관에 의해 전자서명된 공개키를 포함한 인증서를 인증기관이 운영하는 안전한 공개 저장소에 보관시키거나, 필요에 따라 인증서값을 개인키와 함께 보관할 수도 있다.

<42> 문서발급 모바일 장치(63)는 전자서명값이 생성되면 이를 모바일 장치 화면을 통해 보여준다. 따라서, 문서 서명자(61)는 모바일 장치 화면에 나타난 전자서명값을 문서(62)의 여백에 기재함으로써 문서내용과 문서내용의 정당성을 보증하는 전자서명값(71)이 함께 기재된 문서(70)를 마련하게 된다. 서명자 ID와 서명날짜를 포함시켜 해쉬값을 산출한 경우에는 서명자 ID와 서명날짜도 문서(62)의 여백에 함께 기재되어야 한다.

<43> 문서 서명자(11)의 선택에 따라 문서검증자의 수고를 덜 수 있게 문서에 공개키를 추가로 기록할 수도 있다. 일반적으로, 공개키는 인증서에 포함된 형태로 기록된다.

<44> 이처럼 종이 문서의 형태로 문서 데이터(서명자 ID 및 서명날짜 포함)와 전자서명값(71)이 기재된 문서(70)는 문서발급 영역(60)을 벗어나 문서검증 모바일 장치(80)를 지닌 사람에게 전달된다.

<45> 문서검증 모바일 장치(80)는 문서발급 모바일 장치(63)와 마찬가지로 카메라가 장착되어 있으며 문서인식 프로그램, 해쉬 알고리즘, 개인키/공개키를 통한 암호화/복호화 기능이 구비되어 있는 휴대폰 등의 모바일 장치를 의미한다. 따라서, 문서검증 모바일 장치(80)와 문서발급 모바일 장치(62)는 사용자의 입장에 따라 특정 문서에 대한 전자서명값을 생성하는데에 사용될 수도 있으며 특정 문서의 정당성을 검증하는데 사용될 수도 있다.

<46> 문서검증 모바일 장치(80)는 장착된 카메라를 통해 문서(70)의 이미지를 인식한다. 그리고, 문서검증 모바일 장치(80)에 내장된 문서인식 프로그램을 통해 문서 이미지로부터 문서 데이터(서명자 ID 및 서명날짜 포함)와 전자서명값을 분리 및 인식해낸다.

<47> 그리고, 문서검증 모바일 장치(80)은 전자서명값으로부터 해쉬값을 복원하고, 또한 문서 데이터(서명자 ID 및 서명날짜 포함)로부터 해쉬값을 산출하여 이 두 종류의 해쉬값의 일치여부를 통해 문서의 정당성을 검증해낸다. 문서의 정당성을 검증하는 과정은 이후 도 6에서 보다 자세하게 설명한다.

<48> 이때, 전자서명값으로부터 해쉬값을 복원하기 위해서는 문서 서명자(61)에 대한 공개키가 필요한데, 공개키는 이동통신망(90)를 통해 인증서버(50)에 접속하여 제공받을 수도 있으며 또는 문서 서명자(61)가 문서(70)에 공개키가 포함된 인증서를 함께 기록해놓은 후에 문서검증 모바일 장치(80)의 문서인식 프로그램을 통해 인증서를 추출해내어 공개키를 얻을 수도 있다.

<49> 이상 설명한 본 발명의 구성은 제 1 실시예와 제 2 실시예에 의해 개인 컴퓨터를 사용하는 경우와 휴대폰 등의 모바일 장치를 사용하는 경우가 명확히 구분되는 것은 아니며, 문서의 발급은 개인 컴퓨터를 통해 이루어지더라도 문서의 검증은 모바일 장치를 통해 이루어질 수도 있으며 또는 그 반대의 경우도 성립이 가능하다.

<50> 여기서, 문서 서명자는 개인에 한정되지 않으며 개인이 소속된 기관이나 단체를 포함한 넓은 의미로 확장하여 이해할 수 있다.

<51> 또한, 도 1과 도 2에서는 문서 서명자(11, 61)가 직접 문서를 작성하는 경우를 기준으로 설명하였지만, 경우에 따라서는 문서 작성자와 문서 서명자를 구분하여 별도의 문서 작성자가 문서를 작성하고 문서 서명자는 문서를 서명하여 발급하는 역할만을 수행할 수도 있다.

<52> 도 3은 본 발명의 제 1 실시예에 따른 문서위조 방지 기술의 전체 동작과정을 나타낸 순서도이다.

<53> 전체 동작과정은 문서발급 단계(ST10 ~ ST60)와 문서검증 단계(ST70 ~ ST160)으로 구분될 수 있다.

<54> ■ 문서발급 단계

<55> 먼저, 문서 서명자가 개인 컴퓨터를 사용하여 문서를 타이핑하거나 수집하는 등의 과정을 거쳐 문서 데이터를 생성한다(ST10).

<56> 그리고, 생성된 문서 데이터에 대한 전자서명값을 생성하도록 명령을 내리면, 개인 컴퓨터는 해쉬 알고리즘을 사용하여 문서 데이터에 대한 해쉬값을 생성한다(ST20).

<57> 일반적으로, 해쉬값을 생성하기 전에 문서 데이터에 서명자 ID와 서명날짜를 포함시켜 해쉬값을 생성하며, 이하의 내용(도 3 ~ 도 6)에서도 별도의 언급이 없어도 문서 데이터에 단독으로 해쉬 알고리즘을 적용하는 경우뿐만 아니라 문서 데이터에 서명자 ID와 서명날짜를 포함시켜 해쉬 알고리즘을 적용하는 경우를 포함하는 것으로 해석되어야 한다. 문서 검증의 경우에도 마찬가지로 서명자 ID와 서명날짜가 포함된 경우를 추가하여 해석되어야 한다.

<58> 이때, 전자서명값을 생성하기 위해서는 문서 서명자의 개인키가 필요한데, 사전에 미리 인증기관(CA)을 통해 준비되어 안전한 개인 저장소에 보관되어 있는 문서 서명자의 개인키를 획득한다(ST30). 경우에 따라서는 개인키와 함께 대응되어 생성되는 공개키도 미리 획득해둘 수 있다. 공개키는 개인키와는 달리 개인 저장소뿐만 아니라 원격지의 안전한 공개 저장소에 보관되기도 하며, 일반적으로 인증서에 포함된 형태로 보관된다.

<59> 그 다음으로, 개인 컴퓨터는 문서 서명자의 개인키로 해쉬값을 암호화함으로써 문서 데이터에 대한 전자서명값을 생성한다(ST40).

<60> 마지막으로, 전자서명값이 표시되도록 문서 데이터를 인쇄하고(ST50), 인쇄된 문서는 문서 수신자에게 제공된다(ST60). 만약 공개키를 미리 구비한 상태라면 문서 서명자의 선택에 따라 문서 데이터에 공개키를 인증서에 포함된 형태로 추가로 표시할 수도 있다.

<61> ■ 문서검증 단계

<62> 문서 수신자가 문서발급 단계를 통해 인쇄된 문서를 접수한다(ST70).

<63> 그리고, 카메라 및 스캐너 등의 촬상수단을 통해 문서 이미지를 인식하고, 촬상수단에 연결된 개인 컴퓨터가 문서의 이미지를 입력받는다(ST80).

<64> 개인 컴퓨터에는 이미지로부터 문자를 인식할 수 있는 문서인식 프로그램에 내장되어 있으며, 문서인식 프로그램의 문서인식 알고리즘을 이용하여 입력받은 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식한다(ST90).

<65> 전자서명값을 복호화하기 위해서는 공개키가 필요하다. 따라서, 인증서버로부터 다운로드하는 등의 방식을 통해 문서 서명자의 공개키를 획득한다(ST100). 또는, 문서에 공개키가 포함된 인증서가 표시되어 있다면 문서인식 알고리즘을 통해 인증서를 분리 및 인식하고 이로부터 공개키를 인식 및 검증하여 획득할 수도 있다.

<66> 그 다음으로, 공개키를 사용하여 전자서명값을 복호화하여 해쉬값을 복원한다(ST110). 이를 다른 해쉬값과 구별하기 위해서 해쉬값 A라 부르기로 한다.

<67> 또한, 해쉬 알고리즘을 사용하여 문서 데이터에 대한 해쉬값을 생성한다(ST120). 이를 해쉬값 B로 부르기로 한다.

<68> 그리고, 해쉬값 A와 해쉬값 B을 비교하여(ST130) 두 값이 일치하면(ST140) 해당 문서를 정당한 문서로 판단한다(ST160). 그러나, 두 해쉬값이 동일하지 않으면 위조 및 변조된 문서로 판정한다(ST150).

<69> 이를 통해, 문서 수신자가 접수한 문서가 문서 서명자가 생성한 문서와 동일한 내용의 문서인지 여부와 문서 서명자에 의해 서명되었는지 여부를 확인할 수 있다.

<70> 도 4는 본 발명의 제 2 실시예에 따른 문서위조 방지 기술의 전체 동작과정을 나타낸 순서도이다.

<71> 전체 동작과정은 문서인식 단계(ST210 ~ ST230), 문서발급 단계(ST240 ~ ST280), 문서검증 단계(ST290 ~ ST380)으로 구분될 수 있다.

<72> ■ 문서인식 단계

<73> 먼저, 문서 서명자가 직접 손으로 써서 문서를 작성하거나 오프라인상에서 수집하여 인쇄된 문서를 준비한다(ST210).

<74> 그런 후에, 문서 서명자가 카메라가 장착된 휴대폰 등의 모바일 장치를 사용하여 문서의 이미지를 촬영하여 입력한다(ST220).

<75> 모바일 장치에는 문서인식 알고리즘이 적용된 문서인식 프로그램이 내장되어 있으며, 문서인식 프로그램을 사용

하여 이미지로부터 문서 데이터를 인식한다(ST230).

<76> ■ 문서발급 단계

<77> 문서인식 단계를 통해 문서 데이터가 마련되면, 문서 데이터에 대한 해쉬값을 생성한다(ST240). 해쉬값은 모바일 장치에 내장된 해쉬 알고리즘을 통해 생성될 수 있으며, 경우에 따라 외부 서버나 장치의 도움을 받을 수도 있다. 그 다음으로, 문서 서명자의 개인키를 획득한다(ST250).

<78> 개인키는 사전에 미리 인증기관(CA)을 통해 준비되어 안전한 개인 저장소에 보관되어 있으므로 이를 통해 획득하면 된다. 경우에 따라 공개키가 포함된 인증서를 함께 획득해둘 수도 있다. 공개키는 개인키와는 달리 개인 저장소뿐만 아니라 원격지의 안전한 공개 저장소에 보관되는 경우가 있다.

<79> 개인키가 마련되면, 개인키를 사용하여 해쉬값을 암호화함으로써 문서 데이터에 대한 전자서명값을 생성한다(ST260).

<80> 마지막으로, 모바일 장치에서는 생성된 전자서명값을 화면을 통해 표시하여 출력한다(ST270). 그러면, 문서 서명자는 오프라인상의 종이문서에 전자서명값을 수기로 기재하여 문서 수신자에게 제공함으로써(ST280) 전자서명값이 표시된 문서를 배포할 수 있다.

<81> 만약 공개키를 미리 구비한 상태라면 모바일 장치 화면을 통해 공개키를 확인할 수 있으며, 문서 서명자가 문서에 공개키를 인증서에 포함된 형태로 추가로 기입하여 배포할 수도 있다.

<82> 선택에 따라 모바일 장치에 바코드 출력수단을 연결하여 전자서명값, 공개키가 포함된 인증서, 서명자 ID, 서명날짜에 대응되는 바코드를 생성하여 출력하는 것도 가능하다. 바코드가 사용되는 문서 서명자는 바코드를 문서에 붙임으로써 공개키가 포함된 인증서 또는 전자서명값이 기재된 문서가 만들어진다.

<83> 또한, 바코드 출력수단 이외에도 전자서명값, 공개키가 포함된 인증서, 서명자 ID, 서명날짜를 문서에 도장처럼 기록할 수 있는 별도의 전자적인 전용출력장치를 사용하여 문서에 해당 값들을 기록할 수도 있다.

<84> ■ 문서검증 단계

<85> 먼저, 문서 수신자가 문서발급 단계를 통해 배포된 문서를 접수한다(ST290).

<86> 그리고, 카메라가 장착된 휴대폰 등의 모바일 장치를 사용하여 문서의 이미지를 촬영하여 입력한다(ST300).

<87> 모바일 장치에는 문서인식 프로그램이 내장되어 있으며, 문서인식 프로그램을 사용하여 이미지로부터 문서 데이터와 전자서명값을 분리 및 인식한다(ST310).

<88> 또한, 문서 서명자에 대한 공개키를 획득한다(ST320). 이는 이동통신망을 통해 무선 인터넷에 연결된 인증서버에 접속하여 다운로드 받거나, 만약 문서에 공개키가 포함된 인증서가 함께 기재되어 있다면 문서인식 프로그램을 통해 인증서를 분리 및 인식하고 이로부터 공개키를 인식 및 검증하여 획득할 수도 있다.

<89> 만약, 전자서명값이나 공개키가 바코드로 생성되어 문서에 붙어 있는 경우라면 모바일 장치에 내장된 바코드 인식 프로그램을 통해 바코드로부터 전자서명값 및 공개키를 획득한다.

<90> 그 다음으로, 공개키를 사용하여 전자서명값을 복호화하여 해쉬값을 복원한다(ST330). 이를 다른 해쉬값과 구별하기 위해서 해쉬값 A라 부르기로 한다.

<91> 또한, 해쉬 알고리즘을 사용하여 문서 데이터에 대한 해쉬값을 생성한다(ST340). 이를 해쉬값 B로 부르기로 한다.

<92> 그리고, 해쉬값 A와 해쉬값 B을 비교하여(ST350) 두 값이 일치하면(ST360) 해당 문서를 정당한 문서로 판단한다(ST380). 그러나, 두 해쉬값이 동일하지 않으면 위조 및 변조된 문서로 판정한다(ST370). 이러한 판단 결과는 모바일 장치의 화면을 통해 정당한 문서임을 나타내는 메시지를 표시하거나 정당하지 않은 문서임을 나타내는 메시지를 표시한다.

<93> 이를 통해, 문서 수신자가 접수한 문서가 문서 서명자가 생성한 문서와 동일한 내용의 문서인지 여부와 문서 서명자에 의해 서명되었는지 여부를 확인할 수 있다.

<94> 지금까지 도 1부터 도 4를 통해 설명한 전자서명 과정은 여러 문서 서명자들이 순차적으로 서명하고 그에 따라 검증이 이루어질 수 있다.

<95> 또한, 여러 장의 문서를 전자서명할 때에는 각 페이지의 문서마다 전자서명을 하고, 문서의 첫 장이나 마지막 장에 각 페이지의 전자서명값들을 종합하여 전체적으로 서명하도록 구현하는 것도 가능하다.

<96> 도 5는 해쉬 알고리즘과 개인키를 통해 문서에 대한 전자서명값이 생성되는 과정을 나타낸 흐름도이다.

<97> 문서를 발급하고자 하는 개인이나 기관은 다음과 같은 과정을 통하여 문서를 발급한다. 전자서명값이 기재된 문서를 발급하는 과정은 다음과 같다.

<98> (1) 발급하고자 하는 문서내용(c_A)을 입력한다.

<99> (2) 발급하고자 하는 문서내용(c_A)을 입력받아 해쉬 알고리즘(h)을 사용하여 해쉬값(g_A)을 계산한다. 해쉬 알고리즘(h)은 임의의 길이를 갖는 입력값을 일정한 길이를 갖는 값으로 변환하여 주므로 길이가 긴 문서내용(c_A)을 다루기 쉬운 값으로 변환할 수 있다. 또한, 해쉬 알고리즘(h)은 해쉬값의 동일 여부에 따라 입력값의 동일 여부를 판단할 수 있도록 고안되어 있다. 해쉬 알고리즘(h)에 의한 해쉬값 계산 과정은 아래와 같은 수학식 1로 표현할 수 있다.

<100> [수학식 1]

<101> $g_A = h(c_A)$

<102> (3) 발급문서의 해쉬값을 자신의 개인키(sk)로 암호화(E)하여 발급할 문서에 대한 전자서명값(s_A)를 계산한다. 개인키(sk)는 공개키(pk)와 쌍으로 생성되며 문서발급자가 임의로 생성할 수 없으므로 인증기관의 인증을 받아 제공받아야 하며, 타인에게 공개하지 않고 인증자가 잘 보관해야하는 키이다. 개인키에 의한 전자서명값 계산 과정은 아래의 수학식 2로 표현할 수 있다.

<103> [수학식 2]

<104> $s_A = E_{sk}(g_A)$

<105> (4) 발급 문서의 적절한 위치에 전자서명값(s_A)를 기록한 후 문서를 발급한다. 이후, 문서는 문서 수신자에게 전달된다.

<106> 도 6은 문서인식 프로그램과 공개키 및 해쉬 알고리즘을 통해 정당한 문서 여부를 검증하는 과정을 나타낸 흐름도이다.

<107> 문서를 수신한 개인이나 기관은 다음과 같은 과정을 통해 문서를 검증할 수 있다.

<108> (5) 카메라 및 스캐너 등의 촬상수단을 통해 문서 이미지를 캡쳐하여 개인 컴퓨터로 제공하거나, 휴대폰 등의 모바일 장치에 장착된 카메라를 통해 문서 이미지를 캡쳐한다. 그리고, 캡쳐된 문서 이미지를 문서인식 프로그램을 사용하여 문서 내의 모든 내용을 인식하고 문서내용(c_B)과 전자서명값(s_A)을 분리한다

<109> (6) 문서 발급자의 공개키(pk)를 이용하여 전자서명값(s_A)을 복호화(D)함으로써 해쉬값(g_A)을 구한다. 문서 발급자의 공개키(pk)는 개인키와는 달리 일반에게 공개될 수 있는 키이며, 공개키를 통해 문서를 검증할 수는 있으나 문서를 수정할 수는 없다. 공개키에 의한 해쉬값 복원 과정은 아래의 수학식 3으로 표현할 수 있다.

<110> [수학식 3]

<111> $g_A = D_{pk}(s_A)$

<112> (7) 해쉬 알고리즘(h)을 사용하여 문서내용의 해쉬값(g_B)을 계산한다. 만약, 문서내용이 변경되지 않았다면 (3) 과정을 통해 문서발급자에 의해 생성된 해쉬값과 동일한 값이 생성되어야 한다. 문서인식된 문서내용에 대한 해쉬값 계산과정은 아래의 수학식 4로 표현할 수 있다.

<113> [수학식 4]

<114> $g_B = h(c_B)$

<115> (8) 복호화된 해쉬값(g_A)과 문서수신자가 계산한 해쉬값(g_B)를 비교하여 일치하면 위변조되지 않은 정당한 문서

로 판정할 수 있다. 그러나, 일치하지 않는 경우에는 위변조된 문서로 판정한다.

<116> 이상에서 실시예를 들어 본 발명을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것은 아니고, 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형실시될 수 있다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면의 간단한 설명

<117> 도 1은 본 발명의 제 1 실시예에 따른 문서위조 방지 기술을 구현하기 위한 전체 시스템 구성도,

<118> 도 2는 본 발명의 제 2 실시예에 따른 문서위조 방지 기술을 구현하기 위한 전체 시스템 구성도,

<119> 도 3은 본 발명의 제 1 실시예에 따른 문서위조 방지 기술의 전체 동작과정을 나타낸 순서도,

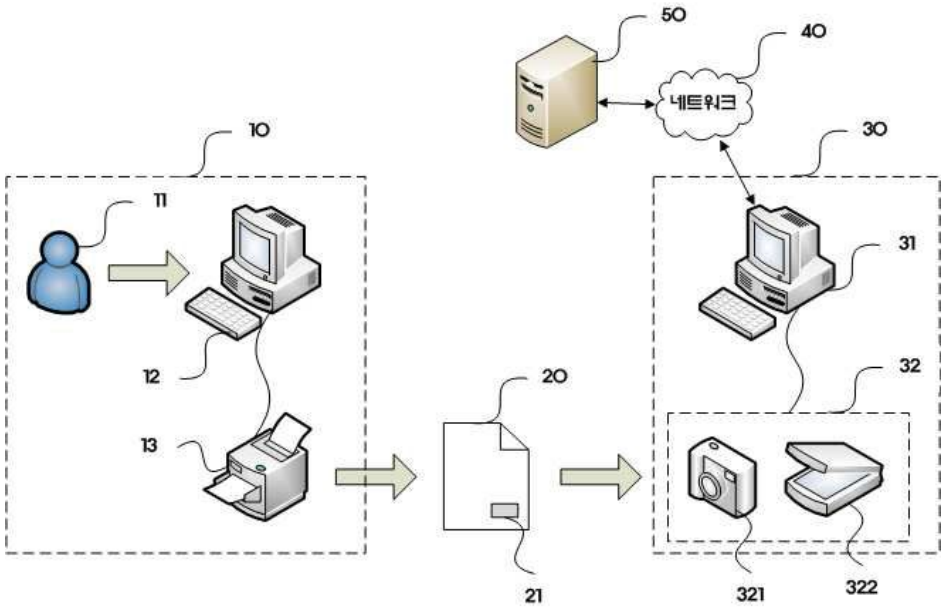
<120> 도 4는 본 발명의 제 2 실시예에 따른 문서위조 방지 기술의 전체 동작과정을 나타낸 순서도,

<121> 도 5는 해쉬 알고리즘과 개인키를 통해 문서에 대한 전자서명값이 생성되는 과정을 나타낸 흐름도,

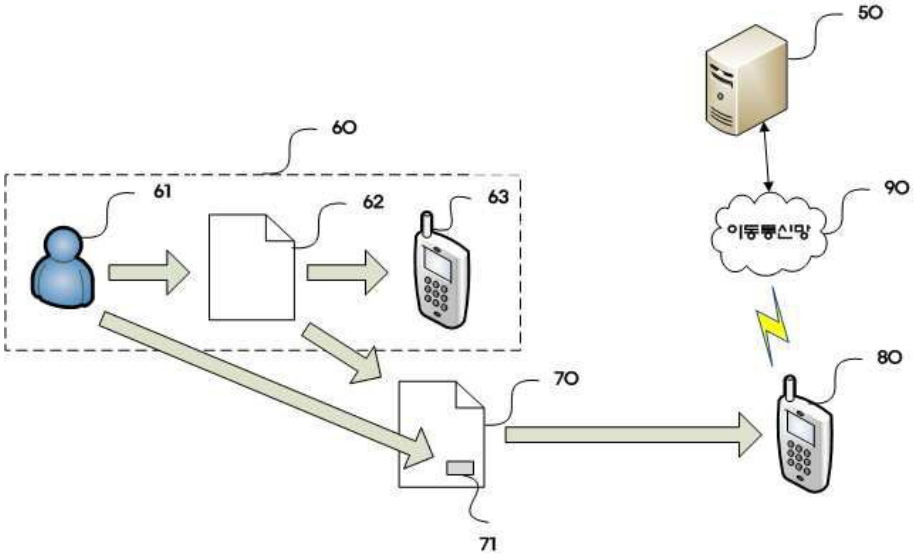
<122> 도 6은 문서인식 프로그램과 공개키 및 해쉬 알고리즘을 통해 정당한 문서 여부를 검증하는 과정을 나타낸 흐름도이다.

도면

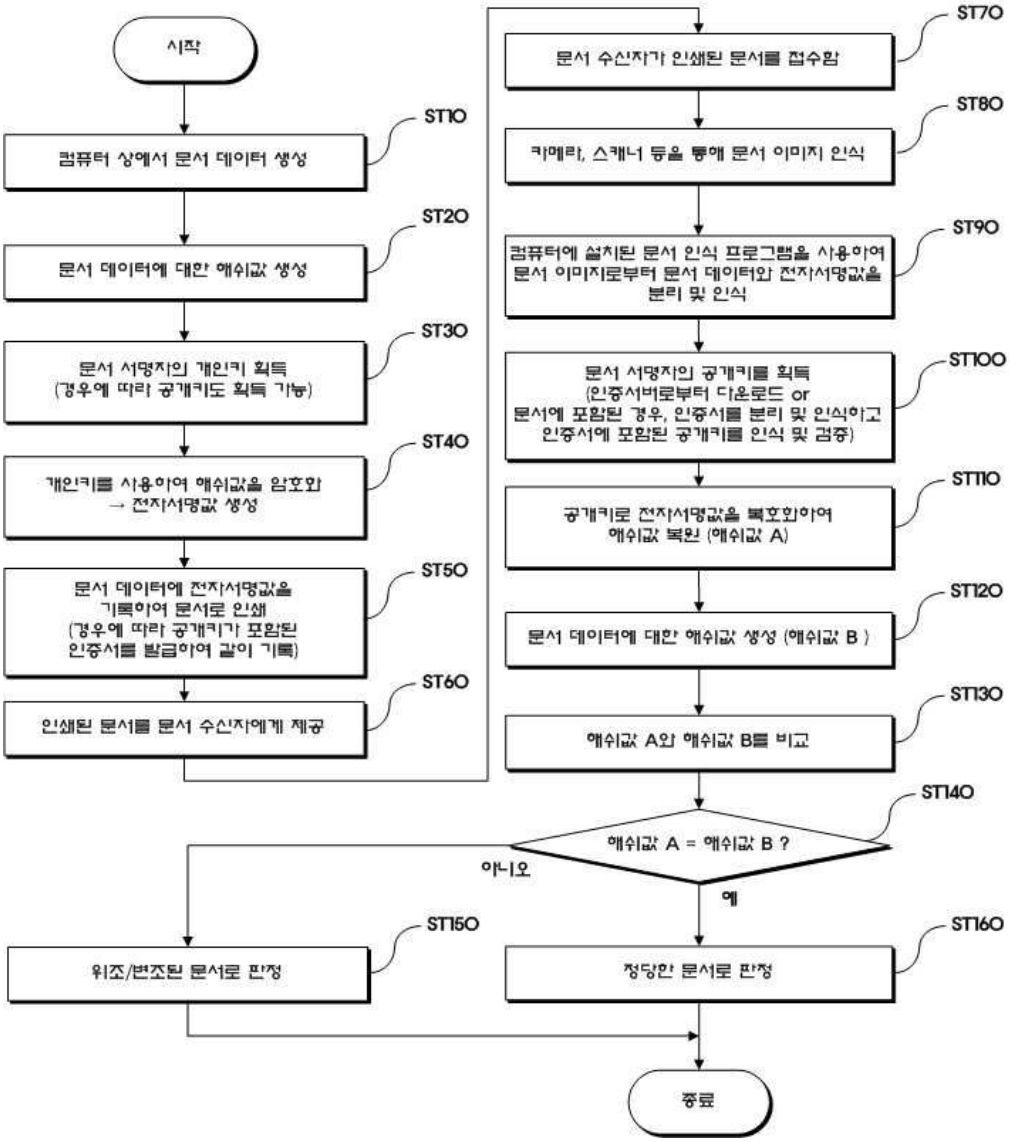
도면1



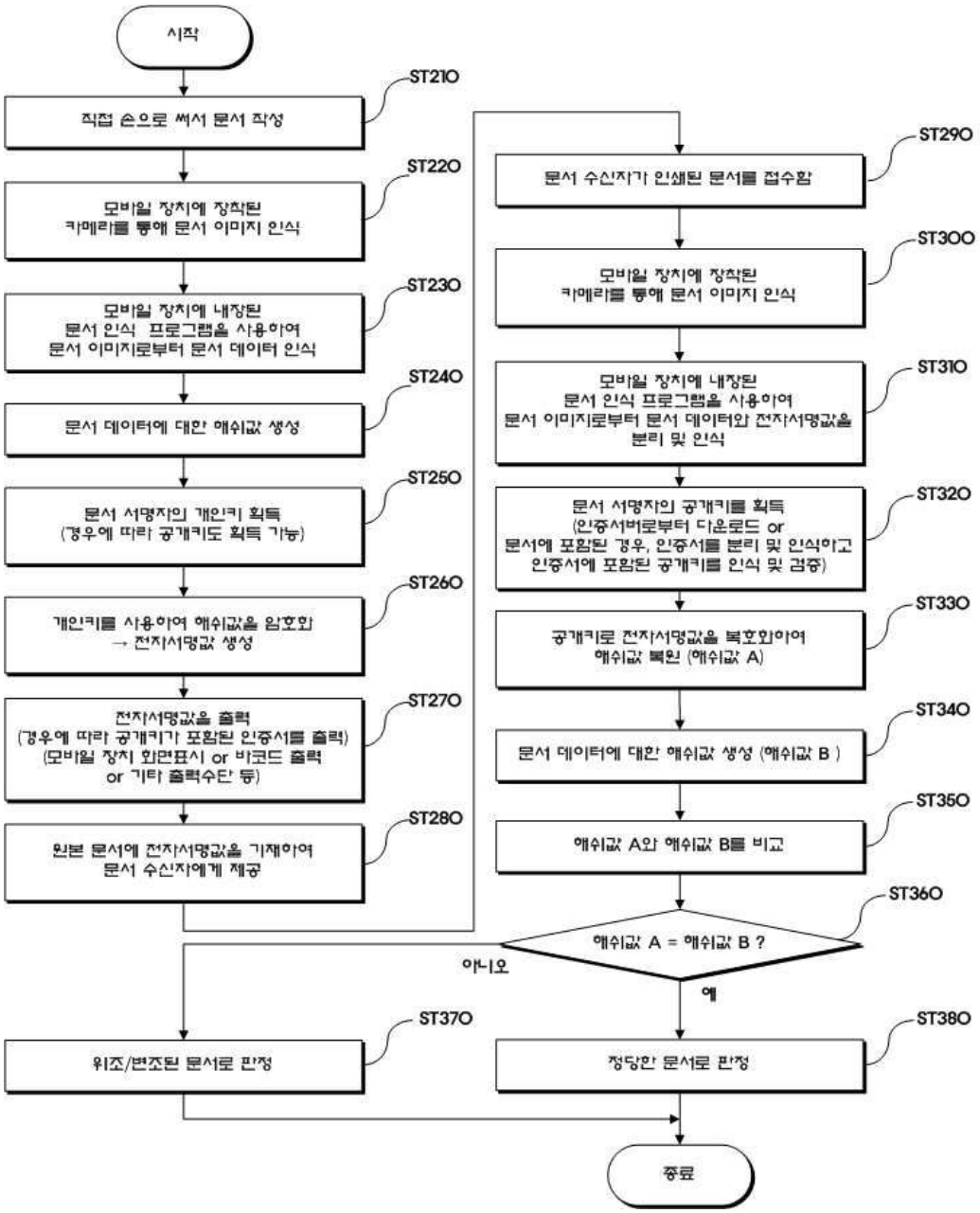
도면2



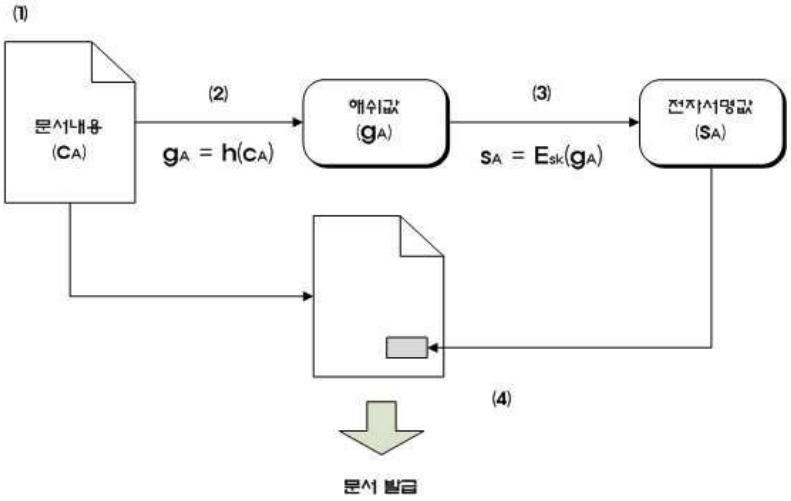
도면3


시작
ST10
컴퓨터 상에서 문서 데이터 생성
ST20
문서 데이터에 대한 해쉬값 생성
ST30
문서 서명자의 개인키 획득
(경우에 따라 공개키도 획득 가능)
ST40
개인키를 사용하여 해쉬값을 암호화
→ 전자서명값 생성
ST50
문서 데이터에 전자서명값을
기록하여 문서로 인쇄
(경우에 따라 공개키가 포함된
인증서를 발급하여 같이 기록)
ST60
인쇄된 문서를 문서 수신자에게 제공
ST70
문서 수신자가 인쇄된 문서를 접수함
ST80
카메라, 스캐너 등을 통해 문서 이미지 인식
ST90
컴퓨터에 설치된 문서 인식 프로그램을 사용하여
문서 이미지로부터 문서 데이터와 전자서명값을
분리 및 인식
ST100
문서 서명자의 공개키를 획득
(인증서버로부터 다운로드 or
문서에 포함된 경우, 인증서를 분리 및 인식하고
인증서에 포함된 공개키를 인식 및 검증)
ST110
공개키로 전자서명값을 복호화하여
해쉬값 복원 (해쉬값 A)
ST120
문서 데이터에 대한 해쉬값 생성 (해쉬값 B)
ST130
해쉬값 A와 해쉬값 B를 비교
ST140
해쉬값 A = 해쉬값 B ?
아니오
예
ST150
위조/변조된 문서로 판정
ST160
정당한 문서로 판정
종료

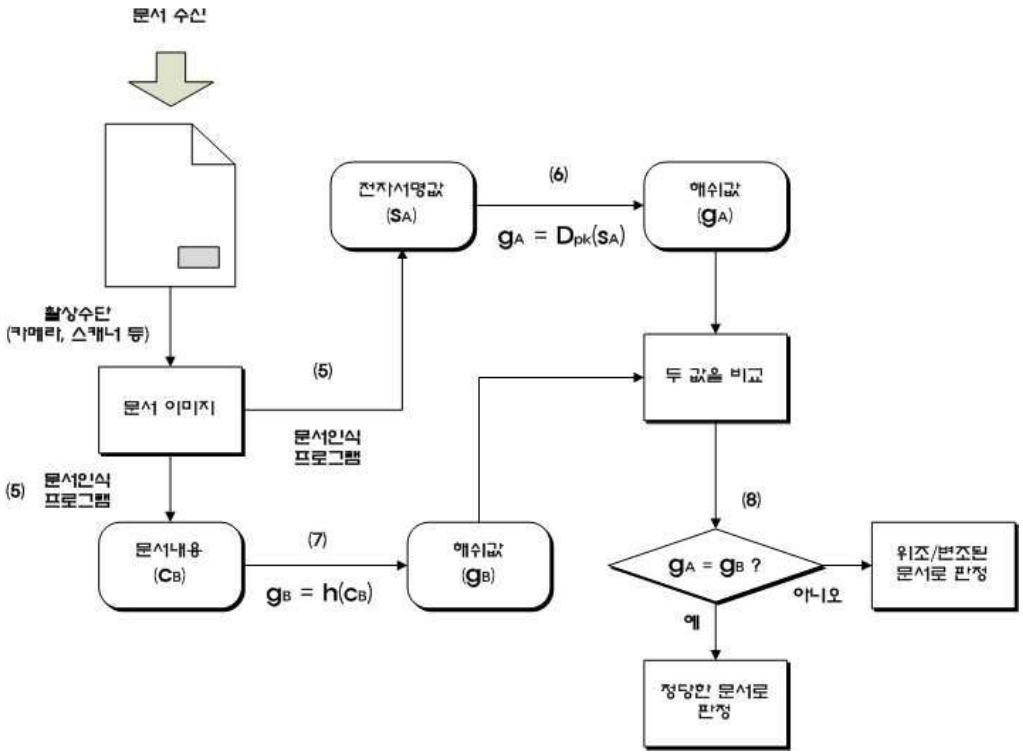
도면4


시작
ST210
직접 손으로 써서 문서 작성
ST220
모바일 장치에 장착된
카메라를 통해 문서 이미지 인식
ST230
모바일 장치에 내장된
문서 인식 프로그램을 사용하여
문서 이미지로부터 문서 데이터 인식
ST240
문서 데이터에 대한 해쉬값 생성
ST250
문서 서명자의 개인키 획득
(경우에 따라 공개키도 획득 가능)
ST260
개인키를 사용하여 해쉬값을 암호화
→ 전자서명값 생성
ST270
전자서명값을 출력
(경우에 따라 공개키가 포함된 인증서를 출력)
(모바일 장치 화면표시 or 바코드 출력
or 기타 출력수단 등)
ST280
원본 문서에 전자서명값을 기재하여
문서 수신자에게 제공
ST290
문서 수신자가 인쇄된 문서를 접수함
ST300
모바일 장치에 장착된
카메라를 통해 문서 이미지 인식
ST310
모바일 장치에 내장된
문서 인식 프로그램을 사용하여
문서 이미지로부터 문서 데이터와 전자서명값을
분리 및 인식
ST320
문서 서명자의 공개키를 획득
(인증서버로부터 다운로드 or
문서에 포함된 경우, 인증서를 분리 및 인식하고
인증서에 포함된 공개키를 인식 및 검증)
ST330
공개키로 전자서명값을 복호화하여
해쉬값 복원 (해쉬값 A)
ST340
문서 데이터에 대한 해쉬값 생성 (해쉬값 B)
ST350
해쉬값 A와 해쉬값 B를 비교
ST360
해쉬값 A = 해쉬값 B ?
아니오
예
ST370
위조/변조된 문서로 판정
ST380
정당한 문서로 판정
종료

도면5


(1)
문서내용
(CA)
(2)
gA = h(cA)
해쉬값
(gA)
(3)
sA = Esk(gA)
전자서명값
(SA)
(4)
문서 발급

도면6


문서 수신
촬상수단
(카메라, 스캐너 등)
문서 이미지
(5)
문서인식
프로그램
(5)
문서인식
프로그램
문서내용
(cB)
(7)
gB = h(cB)
해쉬값
(gB)
전자서명값
(SA)
(6)
gA = Dpk(sA)
해쉬값
(gA)
두 값을 비교
(8)
gA = gB ?
아니오
위조/변조된
문서로 판정
예
정당한 문서로
판정