(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년01월14일
(11) 등록번호 10-0794890
(24) 등록일자 2008년01월08일

(51) Int. Cl.
G06F 12/14 (2006.01)
(21) 출원번호 10-2006-0017098
(22) 출원일자 2006년02월22일
심사청구일자 2006년02월22일
(65) 공개번호 10-2006-0094042
(43) 공개일자 2006년08월28일
(30) 우선권주장
JP-P-2005-00047601 2005년02월23일 일본(JP)
(56) 선행기술조사문헌
JP11308564 A
JP2004040307 A
JP2004140622 A
KR1020010069575 A
전체 청구항 수 : 총 19 항

(73) 특허권자
캐논 가부시끼가이샤
일본 도꾜도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
이와무라 게이이찌
일본 도꾜도 오오따꾸 시모마루꼬 3-30-2 캐논 가부시끼가이샤 내
(74) 대리인
구영창, 이중희, 장수길

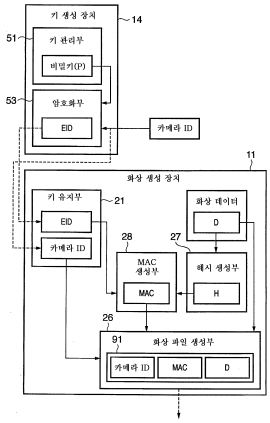
심사관 : 이종익

(54) 정보 처리 방법, 위변조 검증 방법 및 장치, 저장 매체

(57) 요 약

장치의 고유 정보와 비밀스럽게 관리되는 제1 정보와의 산술 연산에 의해 비밀 데이터를 외부에서 취득하여, 이것을 키 데이터로서 키 유지부에 비밀스럽게 유지한다. MAC 생성부는 보호 대상 데이터로부터 얻어진 해시값과 키 유지부(21)에 유지되는 키 데이터에 기초하여 인증 데이터를 생성한다. 화상 파일 생성부는 화상 파일을 생성하여, 고유 정보와 인증 데이터를 보호 대상 데이터와 함께 화상 파일로서 제공한다.

대표도 - 도9



특허청구의 범위

청구항 1

위변조 검출을 위한 정보를 포함하는 데이터를 제공하는 정보 처리 장치로서,

장치의 고유 정보와, 외부 장치에서 비밀스럽게 관리된 비밀키 혹은 시드 정보와의 산술 연산에 의해 얻어진 비밀 데이터를, 상기 외부 장치로부터 취득하는 취득 수단과,

상기 취득 수단에 의해 취득된 상기 비밀 데이터에 기초하여 키 데이터를 취득하여, 비밀스럽게 유지하는 유지 수단과,

보호 대상 데이터와 상기 유지 수단에 유지된 키 데이터에 기초하여 인증 데이터를 생성하는 생성 수단과,

상기 고유 정보와 상기 인증 데이터를 상기 보호 대상 데이터와 함께 제공하는 제공 수단

을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 2

제1항에 있어서,

상기 유지 수단은 상기 취득 수단에 의해 취득된 상기 비밀 데이터를 상기 키 데이터로서 유지하는 것을 특징으로 하는 정보 처리 장치.

청구항 3

제1항에 있어서,

상기 취득 수단에 의해 취득된 상기 비밀 데이터와, 사용자마다 상이한 비밀 정보로부터 키 데이터를 생성하는 키 생성 수단을 더 포함하며,

상기 유지 수단은, 상기 키 생성 수단에 의해 생성된 키 데이터를 유지하는 것을 특징으로 하는 정보 처리 장치.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

입력 화상 또는 사용자 설정에 따른 정보를 설정하는 설정 수단을 더 포함하고,

상기 생성 수단은, 상기 유지 수단에 유지된 키 데이터를 상기 설정 수단에 의해 설정된 설정 정보를 이용하여 변경하고, 변경 후의 키 데이터와 상기 보호 대상 데이터에 기초하여 인증 데이터를 생성하며,

상기 제공 수단은, 상기 고유 정보, 상기 인증 데이터 및 상기 생성 수단에 의해 사용된 설정 정보를 상기 보호 대상 데이터와 함께 제공하는 것을 특징으로 하는 정보 처리 장치.

청구항 5

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 인증 데이터는 MAC인 것을 특징으로 하는 정보 처리 장치.

청구항 6

제1항에 있어서,

상기 비밀 데이터는 공개키 암호의 공개키 또는 비밀키 중 어느 하나이며,

상기 유지 수단은 공개키 또는 비밀키 중 어느 하나를 키 데이터로서 유지하고,

상기 인증 데이터는 상기 보호 대상 데이터와 상기 유지 수단에 유지된 키 데이터에 기초하여 생성된 암호화 데이터인 것을 특징으로 하는 정보 처리 장치.

청구항 7

제6항에 있어서,

상기 유지 수단에 유지된 키 데이터는 비밀키이며, 상기 암호화 데이터는 서명 데이터인 것을 특징으로 하는 정보 처리 장치.

청구항 8

보호 대상 데이터의 위변조의 유무를 검출하는 위변조 검출 장치로서,

해당 장치 내에서 비밀키를 비밀스럽게 유지하는 유지 수단과,

상기 보호 대상 데이터를 제공한 제공 장치의 고유 정보와 상기 비밀키를 이용하여 키 데이터를 생성하는 제1 생성 수단과,

상기 키 데이터와, 상기 보호 대상 데이터에 대하여 해시 함수를 이용하여 얻어진 파생 데이터를 이용하여 인증 데이터를 생성하는 제2 생성 수단과,

상기 제2 생성 수단에 의해 생성된 인증 데이터와 상기 보호 대상 데이터에 부가된 인증 데이터와의 비교에 의해 상기 보호 대상 데이터의 위변조의 유무를 판정하는 판정 수단

을 포함하는 것을 특징으로 하는 위변조 검출 장치.

청구항 9

제8항에 있어서,

상기 유지 수단은 또한 상기 제공 장치가 소유하는 사용자마다 상이한 비밀 정보를 비밀스럽게 유지하며,

상기 제1 생성 수단은, 상기 고유 정보와 상기 비밀키와 상기 비밀 정보를 이용하여 키 데이터를 생성하는 것을 특징으로 하는 위변조 검출 장치.

청구항 10

제8항 또는 제9항에 있어서,

상기 제2 생성 수단은, 상기 보호 대상 데이터에 부가된 입력 화상 또는 사용자 설정에 따라 설정된 정보를 이용하여 상기 키 데이터를 변경하여 이용하는 것을 특징으로 하는 위변조 검출 장치.

청구항 11

보호 대상 데이터의 위변조의 유무를 검출하는 위변조 검출 장치로서,

시드 정보를 비밀스럽게 유지하는 유지 수단과,

상기 보호 대상 데이터를 제공한 제공 장치의 고유 정보와 상기 시드 정보를 이용하여 공개키 암호의 공개키 또는 비밀키를 키 데이터로서 생성하는 제1 생성 수단과,

상기 키 데이터를 이용하여 상기 보호 대상 데이터에 부가된 인증 데이터를 복호하는 복호 수단과,

상기 복호 수단에 의해 얻어진 데이터와 상기 보호 대상 데이터로부터 해시 함수를 이용하여 얻어진 파생 데이터와의 비교에 의해 상기 보호 대상 데이터의 위변조의 유무를 판정하는 판정 수단

을 포함하는 것을 특징으로 하는 위변조 검출 장치.

청구항 12

제11항에 있어서,

상기 키 데이터는 공개키이며, 상기 인증 데이터는 서명 데이터인 것을 특징으로 하는 위변조 검출 장치.

청구항 13

위변조 검출을 위한 정보를 포함하는 데이터를 제공하는 정보 처리 방법으로서,

장치의 고유 정보와, 외부 장치에서 비밀스럽게 관리된 비밀키 혹은 시드 정보와의 산술 연산에 의해 얻어진 비밀 데이터를, 상기 외부 장치로부터 취득하고, 상기 비밀 데이터에 기초한 키 데이터를 메모리에 비밀스럽게 유지하는 유지 단계와,

보호 대상 데이터와 상기 메모리에 유지된 키 데이터에 기초하여 인증 데이터를 생성하는 생성 단계와,

상기 고유 정보와 상기 인증 데이터를 상기 보호 대상 데이터와 함께 제공하는 제공 단계

를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 14

보호 대상 데이터의 위변조의 유무를 검출하는 위변조 검출 방법으로서,

비밀키를 비밀스럽게 메모리에 유지하는 유지 단계와,

상기 보호 대상 데이터를 제공한 제공 장치의 고유 정보와 상기 비밀키를 이용하여 키 데이터를 생성하는 제1 생성 단계와,

상기 키 데이터와, 상기 보호 대상 데이터에 대하여 해시 함수를 이용하여 얻어진 파생 데이터를 이용하여 인증 데이터를 생성하는 제2 생성 단계와,

상기 제2 생성 단계에서 생성된 인증 데이터와 상기 보호 대상 데이터에 부가된 인증 데이터와의 비교에 의해 상기 보호 대상 데이터의 위변조의 유무를 판정하는 판정 단계

를 포함하는 것을 특징으로 하는 위변조 검출 방법.

청구항 15

보호 대상 데이터의 위변조의 유무를 검출하는 위변조 검출 방법으로서,

시드 정보를 비밀스럽게 메모리에 유지하는 유지 단계와,

상기 보호 대상 데이터를 제공한 제공 장치의 고유 정보와 상기 시드 정보를 이용하여 공개키 암호의 공개키 또는 비밀키를 키 데이터로서 생성하는 제1 생성 단계와,

상기 키 데이터를 이용하여 상기 보호 대상 데이터에 부가된 인증 데이터를 복호하는 복호 단계와,

상기 복호 단계에서 얻어진 데이터와 상기 보호 대상 데이터에 대하여 해시 함수를 이용하여 얻어진 파생 데이터와의 비교에 의해 상기 보호 대상 데이터의 위변조의 유무를 판정하는 판정 단계

를 포함하는 것을 특징으로 하는 위변조 검출 방법.

청구항 16

위변조 검출 방법으로서,

데이터 제공 장치의 고유 정보에, 비밀스럽게 유지된 비밀키를 이용한 암호화 처리를 실시하여 생성된 비밀 데이터를 상기 데이터 제공 장치에 공급하는 공급 단계와,

상기 데이터 제공 장치에서,

상기 공급 단계에서 공급된 상기 비밀 데이터에 기초한 키 데이터를 메모리에 비밀스럽게 유지하는 제1 유지 단계와,

보호 대상 데이터와 상기 메모리에 유지된 키 데이터에 기초하여 인증 데이터를 생성하는 제1 생성 단계와,

상기 고유 정보와 상기 인증 데이터를 상기 보호 대상 데이터와 함께 제공하는 제공 단계와,

위변조 검출 장치에서,

상기 비밀키를 비밀스럽게 메모리에 유지하는 제2 유지 단계와,

상기 제공 단계에서 제공된 상기 고유 정보와 상기 비밀키를 이용하여 키 데이터를 생성하는 제2 생성 단계와,

상기 키 데이터와, 상기 보호 대상 데이터에 해시 함수를 이용하여 얻어진 파생 데이터를 이용하여 인증 데이터

를 생성하는 제3 생성 단계와,

상기 제3 생성 단계에서 생성된 인증 데이터와 상기 제공 단계에서 제공된 인증 데이터와의 비교에 의해 상기 보호 대상 데이터의 위변조의 유무를 판정하는 판정 단계

를 포함하는 것을 특징으로 하는 위변조 검출 방법.

청구항 17

위변조 검출 방법으로서,

데이터 제공 장치의 고유 정보와 비밀스럽게 유지된 시드 정보를 이용하여 생성된 공개키 암호를 위한 키 페어 중 한 쪽의 키 데이터를 상기 데이터 제공 장치에 공급하는 공급 단계와,

상기 데이터 제공 장치에서,

상기 공급 단계에서 공급된 상기 키 데이터를 메모리에 유지하는 제1 유지 단계와,

보호 대상 데이터에 대하여 해시 함수를 이용하여 얻어진 파생 데이터를 상기 키 데이터를 이용하여 암호화하여 암호화 데이터를 생성하는 제1 생성 단계와,

상기 고유 정보와 상기 암호화 데이터를 상기 보호 대상 데이터와 함께 제공하는 제공 단계와,

위변조 검출 장치에서,

상기 시드 정보를 메모리에 비밀스럽게 유지하는 제2 유지 단계와,

상기 시드 정보와 상기 제공 단계에서 제공된 상기 고유 정보를 이용하여 상기 공개키 암호를 위한 키 페어 중 다른 쪽의 키 데이터를 생성하는 제2 생성 단계와,

상기 제2 생성 단계에서 생성된 키 데이터를 이용하여 상기 암호화 데이터를 복호하는 복호 단계와,

상기 복호 단계에서 얻어진 데이터와 상기 보호 대상 데이터에 대하여 해시 함수를 이용하여 얻어진 파생 데이터와의 비교에 의해 상기 보호 대상 데이터의 위변조의 유무를 판정하는 판정 단계

를 포함하는 것을 특징으로 하는 위변조 검출 방법.

청구항 18

제13항에 따른 정보 처리 방법을 컴퓨터에 실행시키기 위한 제어 프로그램을 저장한 기억 매체.

청구항 19

제14항에 따른 위변조 검출 방법을 컴퓨터에 실행시키기 위한 제어 프로그램을 저장한 기억 매체.

명 세 서

발명의 상세한 설명

발명의 목적

종래기술의 문헌 정보

<40> [특허 문헌1] 미국 특허 제5,499,294호

발명이 속하는 기술 및 그 분야의 종래기술

<41> 본 발명은, 데이터의 위변조의 유무를 판정하기 위한 정보 처리 기술에 관한 것이다. 특히, 본 발명은 화상 파일의 완전성(또는 변경)을 보증하기 위한 기술에 적합한 것이다.

<42> 최근, 렌즈를 통해서 광학적 화상을 CCD 또는 CMOS 등의 센서로 전기 신호로 변환하여, 얻어진 데이터가 디지털 형식으로 보존되는 디지털 카메라가 광범위하게 보급되었다.

<43> 디지털 카메라는, 종래의 은염 사진과 같이, 촬영된 화상을 현상 및 프린트하는 수고가 줄여 질 수 있다는 점

뿐만 아니라, 노후 열화(aged deterioration)가 없고, 화상이 쉽게 보관 또는 검색될 수 있으며, 통신 회선을 통해 원격지에 데이터가 전송될 수 있다는 다양한 장점들을 갖는다. 이 때문에, 디지털 카메라가 많은 업무 분야에서 이용되고 있다.

<44> 그러나, 몇몇 디지털화의 단점들도 지적된다. 그것은, 시판되고 있는 사진 수정 툴을 이용함으로써 쉽게 디지털 이미지가 가공 또는 수정된다는 특징에 기인한다.

<45> 따라서, 화상 변경이 쉽다는 디지털 화상의 단점을 극복하는 구조에 대한 요구가 있다.

<46> 현재, 암호 기술을 이용한 디지털 서명에 기초한 화상 데이터의 위변조 검출 시스템이 제안되어 있다. 예를 들면, 미국 특허 제5,499,294호에 제안된 바와 같은 시스템은 화상 데이터를 생성하는 화상 생성 장치(카메라)와, 화상 데이터의 완전성을 검증하는 화상 검증장치를 구비한다. 이 화상 생성 장치는, 그 화상 생성 장치 고유의 비밀 정보와 그 화상 생성 장치에서 촬영된 디지털 화상 데이터에 기초하여, 소정의 산술 연산을 수행하여 화상 데이터를 식별하는(위변조를 검출하는) 정보인 디지털 서명 데이터를 생성한다. 그리고, 생성된 디지털 서명 데이터와 상기 디지털 화상 데이터가 화상 생성 장치로부터 출력된다. 한편, 화상 검증 장치는, 소정의 산술 연산을 디지털 화상 데이터에 수행한 결과의 데이터와, 디지털 서명 데이터에 반대의 생성 연산을 수행한 결과의 데이터를 비교함으로써 검증을 행한다. 또한, 상기 미국 특허 제5,499,294호에서는, 디지털 서명 데이터 생성에 해시 함수(압축 함수)와 공개키 암호화가 이용된다.

<47> 또한, 상기의 디지털 서명 데이터 대신에 MAC(Message Authentication Code)이 이용될 수도 있다. MAC는 공유키(shared key) 암호화 및 해쉬 함수를 사용하여 생성되며, 처리 속도가 공개키(public key) 암호화 보다도 고속인 것이 특징이다. 그러나, MAC의 생성 또는 검증에 사용되는 공유키는 화상 검증 장치에서 엄중히 관리될 것이 요구된다.

<48> 카메라로 촬상한 화상 데이터는 주로 카메라에 접속되어 있는 소형의 메모리 카드(불휘발성 메모리)에 기억되며, 그 메모리 카드는 주로 플래시 EEPROM에 의해서 구성된다. 또한, 상기 플래시 EEPROM 외에 CPU, RAM, ROM으로 구성되는 산술 연산부를 갖는 보안 기능의 메모리 카드나 IC 카드가 실용화되고 있다. 이러한 산술 연산 기능으로, 화상 생성 장치의 외부(즉, 메모리 카드 또는 IC 카드의 내부)로 상기의 디지털 서명 데이터 위변조 검출을 위한 데이터가 생성될 수 있다.

발명이 이루고자 하는 기술적 과제

<49> 이하에서는, 카메라와 같은 화상 생성 장치에 대한 MAC 또는 디지털 서명을 이용하여 위변조를 검출하는 시스템이 고려된다. MAC는 전술한 바와 같이 공유키 암호화를 이용하여 검증 데이터를 작성하고 이를 검증하는 구조이다. 그러나, 그 공유키가 알려지면, 안전성은 보장될 수 없다. 또한, 디지털 서명에 있어서, 그 서명에 사용되는 사설키(private key)가 알려지면, 그 안전성은 보장될 수 없다. 따라서, 카메라가 검증 데이터의 생성측에, IC 카드가 검증 측에 있는 경우, 카메라와 같은 화상 생성 장치는 IC 카드에 비해 보안 성능이 취약하다.

<50> 본 발명은 상기의 과제에 감안하여 이루어진 것으로, 데이터의 위변조에 대한 보안 성능을 개선하는 것이 본 발명의 목적이다.

발명의 구성 및 작용

<51> 본 발명의 일 양태에 따르면, 위변조 검출을 위한 정보를 포함하는 데이터를 제공하는 정보 처리 장치로서, 장치의 고유 정보와 비밀스럽게 관리되는 제1 정보와의 산술 연산에 의해 얻어진 비밀 데이터를 취득하는 취득 수단; 상기 취득 수단에 의해 취득된 상기 비밀 데이터에 기초하여 키 데이터를 취득하여, 비밀스럽게 유지하는 유지 수단; 보호 대상 데이터와 상기 유지 수단에 유지되는 키 데이터에 기초하여 인증 데이터를 생성하는 생성 수단; 및 상기 고유 정보와 상기 인증 데이터를 상기 보호 대상 데이터와 함께 제공하는 제공 수단을 포함하는 정보 처리 장치가 제공된다.

<52> 본 발명의 또 다른 양태에 따르면, 위변조 검출을 위한 정보를 포함하는 데이터를 제공하는 정보 처리 방법으로서, 장치의 고유 정보와, 외부장치에서 비밀스럽게 관리되는 제1 정보와의 산술 연산을 행하여 외부 장치로부터 비밀 데이터를 취득하고, 상기 비밀 데이터에 기초한 키 데이터를 메모리에 비밀스럽게 유지하는 유지 단계; 보호 대상 데이터와 상기 메모리에 유지되는 키 데이터에 기초하여 인증 데이터를 생성하는 생성 단계; 및 상기 고유 정보와 상기 인증 데이터를 상기 보호 대상 데이터와 함께 제공하는 제공 단계를 포함하는 정보 처리 방법이 제공된다.

<53> 본 발명의 다른 특징 및 장점들은, 동일 참조 부호가 동일 또는 유사한 부분을 지칭하는 첨부 도면과 함께 제공되는 이하의 상세한 설명으로부터 분명하게 될 것이다.

<54> 발명의 상세한 설명의 일부를 구성하며 이에 포함되는 첨부 도면들은 본 발명의 실시예들을 도시하며, 상세한 설명과 함께 본 발명의 원리를 설명하는데 이바지 한다.

<55> 이하, 본 발명의 바람직한 실시예들을 첨부 도면들을 참조하여 상세하게 설명한다.

<56> [제1 실시예]

<57> 이하의 실시예에 있어서, 화상 데이터를 보호 대상의 데이터, 즉 위변조 검출 대상의 데이터로서 설명한다. 본 실시예의 시스템은 다른 형태의 데이터를 보호 대상의 데이터로 할 수도 있음은 당업자에게 자명하다.

<58> [시스템 구성]

<59> 본 실시예의 시스템은, 도 1에 도시한 바와 같이, 화상 생성 장치(11), 공격 저지 장치(12), 화상 검증 보조 장치(13), 및 키생성 장치(14)를 구비한다.

<60> 화상 생성 장치(11)는 보호 대상의 데이터(본 실시예에서 화상 데이터)를 위변조 검출을 위한 인증 데이터(본 실시예에서 MAC)와 함께 출력한다. 화상 생성 장치(11)는 MAC 작성용 키를 설정 및/또는 유지하는 기능과, 촬영된 화상으로부터 화상 데이터를 생성하는 기능과, 생성된 화상 데이터에 대한 MAC 데이터를 생성하는 기능과, 보조 파라미터들(예컨대, 카메라의 경우, 촬영 시간, 촛점 거리, f-값, ISO 감도, 측광 모드, 화상 파일 사이즈, 촬영자 정보)을 생성하는 기능과, MAC 데이터 첨부 화상 파일(화상 데이터, MAC 데이터, 보조 파라미터 등으로 구성됨)을 생성하는 기능과, 공격 저지 장치(12)와 통신하는 기능을 갖는다. 화상 생성 장치(11)는, 디지털 카메라 또는 디지털 비디오 카메라 등의 촬상 장치, 스캐너, 카메라 유닛을 갖는 전자 기기, 또는 디지털 화상을 생성하는 장치일 수 있다. 간단화를 위해서, 본 실시예에 있어서 화상 생성 장치(11)는 디지털 카메라로서 설명된다.

<61> 공격 저지 장치(12)는, 화상 생성 장치(11)에서 생성된 보호 대상의 데이터(화상 파일)를 저장하며, 그 데이터의 위변조 유무를 판정한다. 공격 저지 장치(12)는 화상 생성 장치(11)에서 생성된 화상 파일을 저장하는 기능과, 검증에 필요한 정보를 계산하는 기능과, 화상 생성 장치(11) 또는 화상 검증 보조 장치(13)와 데이터를 통신하는 기능을 갖는다. 공격 저지 장치(12)로서는 플래시 EEPROM 외에 CPU, RAM, 및 ROM으로 구성되는 산술 연산부를 갖는 보안 기능의 메모리 카드, 또는 IC 카드일 수 있다. 간단화를 위해, 본 실시예에서는 공격 저지 장치(12)가 IC 카드인 것으로 하여 설명한다.

<62> 화상 검증 보조 장치(13)는 공격 저지 장치(12)가 보호 대상 데이터의 위변조의 유무를 판정하는 경우, 보호 대상 데이터로부터 인증 정보 등을 추출하여 공격 저지 장치(12)에 이를 제공한다. 화상 검증 보조 장치(13)는 MAC 데이터 첨부 화상 파일을 화상 데이터와 MAC 데이터로 분리하는 기능과, 분리된 화상 데이터의 해시값을 계산하는 기능과, 공격 저지 장치(12)와 통신하는 기능과, 그 판정 결과를 표시하는 기능을 갖는다. 또한, 화상 검증 보조 장치(13)는 데이터를 축적 및 분배하는 웹 서버에서의 퍼스널 컴퓨터(PC), 또는 CPU와 메모리를 갖은 소형 기기일 수도 있다. 간단화를 위해, 본 실시예에서 화상 검증 보조 장치(13)는 PC로서 설명한다.

<63> 키생성 장치(14)는 비밀키를 안전하게 관리하는 기능과, 그 비밀키를 이용하여 입력된 카메라 ID를 암호화하는 기능과, 그 카메라 ID와 암호화 정보를 화상 생성 장치(11)에 설정하는 기능을 갖는다. 또한, 키생성 장치(14)는 플래시 EEPROM 외에 CPU, RAM, 및 ROM으로 구성되는 산술 연산부를 갖는 보안 기능을 갖는 메모리 카드일 수 있으며, 또는 패스워드나 액세스 제어 등에 따라서 비밀키 정보를 보호할 수 있는 PC일 수도 있다. 간단화를 위해, 본 실시예에서는 키생성 장치(14)는 PC로서 설명한다.

<64> 도 2는 화상 생성 장치(11)의 구성예를 나타내는 블록도이다. 각 부의 기능은 후술하는 위변조 검출 처리의 설명에 있어서 분명하게 되지만, 이하 간단하게 설명한다. 키 유지부(21)는 키생성 장치(14)로부터 송신된 암호화 정보나 카메라 ID를 유지하며, 이들에 기초하여 키를 생성한다. 조작부(22)는, 촬영지시 등, 화상 생성 장치(11)에 대한 여러가지의 사용자 조작을 구현한다. 산술 연산부(23)는 인증 정보의 생성에 있어서의 각종 산술 연산 조작을 수행한다. 통신부(24)는 공격 저지 장치(IC 카드)(12)와의 통신을 행한다. 촬영부(25)는 CCD(전하 결합 소자) 등의 광학 센서를 가지며, 조작부(22)로부터 입력된 지시에 따라 피사체의 화상 데이터 또는 보조 파라미터들을 생성한다. 화상 파일 생성부(26)는 촬상부(25)에 의해서 얻어진 화상 데이터에 인증 정보(본 실시예에서 MAC)를 첨부하여 화상 파일을 생성한다. 해시 생성부(27)는 화상 데이터로부터 해시값을 생성한다. MAC 생성부(28)는 해시 생성부(27)에 의해 생성된 해시값과 키 유지부(21)에 유지된 키를 이용하여 MAC

를 생성한다. 제어부(29)는 CPU, ROM, 및 RAM 등으로 구성되어, 전술한 각 부를 총괄적으로 제어한다. 또한, 전술한 각 부는 하드웨어로 구현될 수도 있으나, 부분적으로는 CPU의 기능에 의해 구현될 수도 있다.

<65> 도 3은 공격 저지 장치(IC 카드)(12)의 구성예를 도시하는 블록도이다. 키 유지부(31)는 암호화부(33)에서 사용하기 위한 키 데이터를 유지한다. 키 유지부(31)는 키 정보가 누설되지 않도록, 암호화부(33) 이외의 외부에의 키의 판독을 금지시킨다. 산술 연산부(32)는 인증에 관한 각종 산술 연산을 수행한다. 암호화부(33)는 키 유지부(31)에 유지되는 키 데이터를 이용하여 인증 처리를 위한 키 데이터를 생성한다. 통신부(34)는 화상 생성 장치(11) 및 화상 검증 보조 장치(13)와의 통신을 실현한다. MAC 생성부(35)는 암호화부(33)에 의해 생성된 키 데이터를 이용하여 MAC를 생성한다. 판정부(36)는 화상 파일에 첨부된 MAC과 MAC 생성부(35)에 의해 생성된 MAC과의 비교로부터 화상 데이터의 위변조의 유무를 판정한다. 제어부(37)는 CPU, ROM, 및 RAM 으로 구성되어, 전술한 각 부를 총괄적으로 제어한다. 또한, 전술한 각 부는 하드웨어로 구현될 수도 있으나, 부분적으로는 CPU의 기능에 의해 구현될 수도 있다.

<66> 도 4는 화상 검증 보조 장치(13)의 구성예를 도시하는 블록도이다. 통신부(41)는 공격 저지 장치(12)와의 통신을 행한다. 화상 파일 분리부(42)는 보호 대상 데이터룰 포함하는 화상 파일(예컨대, 공격 저지 장치(12)로부터 통신부(41)를 통하여 입력된 화상 파일)로부터 화상 데이터와 인증 데이터를 분리하여 추출한다. 해시 생성부(43)는 화상 파일 분리부(42)로부터 얻어진 화상 데이터로부터 해시값을 생성한다. 표시부(45)는 액정 디스플레이 상에 각종의 데이터를 표시한다. 제어부(46)는 전술한 각 부의 제어를 행한다. 또한, 전술한 각 부는 하드웨어에 의해 실현될 수도 있으나, 부분적으로는 CPU의 기능에 의해 실현될 수도 있다. 본 실시예에서 화상 검증 보조 장치(13)는 PC에서 구성되기 때문에, 전술한 각 부는 소정의 어플리케이션 프로그램을 실행하는(CPU가 소정의 제어 프로그램을 실행함)것에 의해 구현된다.

<67> 도 5는 키생성 장치(14)의 구성예를 나타내는 블록도이다. 키 관리부(51)는 암호화부(53)에서 이용하기 위한 키 데이터(비밀키 P)를 관리한다. ID 입력부(52)는 보호 대상 데이터를 제공하는 장치(본 실시예에서 화상 생성 장치(11))의 고유의 정보(예컨대, ID)를 입력한다. 암호화부(53)는, AES 등의 안전성이 확인된 공유키 암호를 탑재하고 있어, ID 입력부(52)로부터의 데이터를 비밀키(P)를 이용하여 암호화한다. 통신부(54)는 소정의 프로토콜에 따라 화상 생성 장치(11)와의 통신을 행한다. 제어부(55)는 전술한 각 부의 제어를 행한다. 각 부는 하드웨어로 구현될 수도 있으나, 부분적으로는 CPU의 기능에 의해 구현될 수도 있다. 본 실시예에 있어서, 키생성 장치(14)는 PC에서 구성되므로, 각 부는 소정의 어플리케이션 프로그램을 실행함(CPU가 소정의 제어 프로그램을 실행함)에 의해 구현된다.

<68> 키생성 장치(14) 내의 키 관리부(51)는 패스워드 또는 정당 사용자의 생체 정보를 사용하여 제한적으로 판독된다. 즉, 키 관리부(51)는 비밀키(P)가 누설되지 않도록 주로 암호화부(53) 이외의 외부로부터 판독될 수 없다. ID 입력부(52)는 키보드일 수 있으며, 또는 통신부(54)를 통하여 화상 생성 장치(11)로부터 ID가 취득될 수도 있다.

<69> [위변조 검출 처리의 설명]

<70> 이하, 도 6 내지 도 10을 참조하여, 본 실시예에 따른 이상의 구성을 갖춘 시스템에 있어서의 위변조 검출 처리에 대하여 상세히 설명한다. 도 6은 위변조 검출의 이전의 처리, 또는 키생성 장치(14)가 화상 생성 장치(11)에 위변조 검출을 위한 정보를 설정하는 처리를 설명하는 플로우차트이다. 도 7은 화상 생성 장치(11)에 있어서 위변조 검출을 위한 정보(인증 정보)를 포함한 화상 파일의 생성 처리를 설명하는 플로우차트이다. 도 8은 공격 저지 장치(12)와 화상 검증 보조 장치(13)에서의 위변조 검출 처리를 설명하는 플로우차트이다. 또한, 도 9는 도 6 및 도 7의 플로우차트에 도시된 처리에서 이용되어 생성되는 데이터 및 그 흐름을 설명하는 도면이다. 마찬가지로, 도 10은 도 8의 플로우차트에 도시된 처리에서 이용되어 생성되는 데이터 및 그 흐름을 설명하는 도면이다.

<71> 우선, 처리에 있어서, 키생성 장치(14)는 도 9에 도시한 바와 같이 미리 정해진 비밀키(P)를 키 관리부(51)에 갖는 것으로 한다. 이 비밀키(P), 카메라 ID, 및 키(K)는 수치를 나타내며, 소정의 비트 길이를 갖는 수치로서 설정된다.

<72> 이하, 도 6의 플로우차트를 참조하여, 키생성 장치(14)에 의한 화상 생성 장치(11)에의 키 설정의 수순을 설명한다. 이하의 처리는 제어부(55)의 제어하에서 수행된다.

<73> 우선, 고유의 ID(카메라 ID)가 화상 생성 장치(11)에 ID 입력부(52)를 통해서 입력되면, 카메라 ID가 암호화부(53)에 보내진다(단계 S61). 암호화부(53)는 키 관리부(51)에 의해서 관리 및 유지되는 비밀키(P)를 이용하여,

입력된 카메라 ID를 암호화하고 EID를 취득한다(단계 S62). 그리고, ID 입력부(52)를 통하여 입력된 카메라 ID와, 이를 암호화하여 얻은 EID는 통신부(54)를 통하여 화상 생성 장치(11)에 송신된다(단계 S63). 송신된 카메라 ID와 EID는 통신부(24)를 통하여 화상 생성 장치(11)에 의해 수신되어, 도 9에 도시한 바와 같이, 화상 생성 장치(11) 내의 키 유지부(21)에 설정된다. 즉, 통신부(24)는 공격 저지 장치(12) 및 키생성 장치(14)와 통신할 수 있다. 또한, 임의의 통신의 형태가 이용될 수도 있다.

<74> 이하, 도 7의 플로우차트를 참조하여, 화상 생성 장치(11)에 있어서 인증 정보(MAC)를 갖는 화상 파일의 생성 처리를 설명한다. 이하의 처리는 제어부(29)의 제어하에서 수행된다.

<75> 화상 생성 장치(11)는 촬상부(25)로부터 화상(D)을 입력한다(단계 S71). 해시 생성부(27)는 화상(D)에 대한 해시값(H)을 계산한다(단계 S72). MAC 생성부(28)는, 도 9에 도시한 바와 같이, 전술한 단계 S63의 처리를 통해 키 유지부(21)에 유지되는 EID를 키(K)로 사용하여, 해시 생성부(27)에서 생성된 해시값(H)에 대한 MAC을 계산한다(단계 S73). 그리고, 화상 파일 생성부(26)는 화상(D)의 화상 파일에 MAC와 카메라 ID를 첨부함으로써, 인증 정보를 갖는 화상 파일(도 9의 91)을 생성한다(단계 S74).

<76> 상기 처리에서, 촬상부(25)로부터 얻어진 화상(D)는, 화상 파일 생성부(26)에 의해서 JPEG 방식에 따라 압축되는 것으로 가정한다. 또한, 화상 파일 생성부(26)의 화상 파일의 파일 형식은, 예컨대, JFIF(JPEG File Interchange Format), TIFF(Tagged Image File Format) 및 GIF(Graphics Interchange Format)일 수 도 있다. 그러나, 파일 형식은 이들에 한정되는 것이 아니라, 이들을 확장한 형식일 수도 있거나, 또는 다른 임의의 화상 파일 형식일 수도 있다. 또한, 해시 생성부(27)에서 사용하기 위한 해시 함수는, 일반적으로 알려진 바와 같이, MD5, SHA1, 또는 RIPEMD 일 수 있으며, 이들 중 임의의 하나가 이용될 수도 있다. 또한, MAC 생성부(28)에 대한 MAC 데이터 생성 알고리즘은, DES나 AES 등의 공유키 암호화의 CBC(Cipher Block Chaining) 모드를 이용하여, 또는 HMAC이라고 불리는 키를 갖는 해시 함수를 이용하여, 구현될 수도 있으며, 모두 공지되어 있다. 이들 방법 중 어느 것이나, MAC 생성부(28)의 MAC 데이터 생성 알고리즘으로서 이용할 수 있다. 예컨대, DES의 CBC 모드에서는, 대상 데이터를 CBC 모드로 암호화하여 최종 블록의 전반의 32 비트가 MAC 데이터로 이루어진다.

<77> 이하, 도 8 및 도 10을 참조하여, 상기 방법에서 생성된 화상 파일(도 9의 91)에 대한 공격 저지 장치(12)와 화상 검증 보조 장치(13)에 의해 수행되는 위변조 검출 처리에 대하여 설명한다. 또한, 공격 저지 장치(IC 카드)(12)는, 도 10에 도시한 바와 같이, 키 유지부(31)에 비밀키(P)를 갖는다.

<78> 우선, 화상 검증 보조 장치(13)는 화상(D)와 MAC 및 카메라 ID를 포함하는 화상 파일을 통신부(41)로부터 판독한다(단계 S81). 화상 검증 보조 장치(13)의 화상 파일 분리부(42)는 판독된 화상 파일을 화상(D)와 MAC 및 카메라 ID로 분리한다(단계 S82). 다음, 화상 검증 보조 장치(13)는 해시 생성부(43)를 이용하여 단계 S82에서 취득된 화상에서 해시값(H)을 생성한다(단계 S83). 화상 검증 보조 장치(13)는 통신부(41)을 통하여 공격 저지 장치(12)에 해시 생성부(43)로부터 생성된 해시값(H)과, 화상 파일 분리부(42)로 얻어진 MAC 및 카메라 ID를 보낸다(단계 S84). 본 실시예에서는, 공격 저지 장치(12)가 IC 카드이므로, 통신부(41)는 IC 카드와의 I/O 인터페이스를 포함한다.

<79> 한편, 공격 저지 장치(12)는 통신부(34)를 통하여 카메라 ID, 해시값(H), 및 MAC를 수신한다. 그리고, 수신된 카메라 ID는 키 유지부(31)에 유지되는 비밀키(P)를 이용하여 암호화부(33)에 의해 암호화된다(단계 S91). 여기서, 암호화부(33)에 의해 사용되는 암호화 처리는 암호화부(53)에 의해 사용되는 암호화 처리와 동일하다. 따라서, 공격 저지 장치(12)의 카메라 ID를 암호화하여 얻어지는 EID는 키생성 장치(14)의 카메라 ID를 암호화하여 얻어지는 EID와 동일하다. 그리고, 이 EID는 상기 단계 S73의 처리와 마찬가지로 MAC 계산을 위한 키(K)로서 이용된다. 즉, MAC 생성부(35)는, 암호화부(33)에 의해 얻어진 EID를 키(K)로서 사용하여, 화상 검증 보조 장치(13)로부터 송신된 해시값(H)에 대한 MAC(이하, MAC2)를 생성한다(단계 S92). 여기서, MAC 생성부(35)는 화상 생성 장치(11)의 MAC 생성부(28)와 동일한 알고리즘을 사용하여 DES나 AES 등의 공유키 암호화로 MAC를 계산한다. 그리고, 판정부(36)는 MAC 생성부(35)에 의해 생성된 MAC2와 화상 검증 보조 장치(13)로부터 송신된 MAC가 일치하는지의 여부를 판정한다(단계 S93). 이 결과, MAC와 MAC2가 일치하면 위변조가 없는 것이며(단계 S94), 일치하지 않으면 위변조가 있는 것으로 판정한다(단계 S95).

<80> 상기 판정의 결과는 통신부(34)를 통해 화상 검증 보조 장치(13)에 보내진다(단계 S96). 화상 검증 보조 장치(13)는 송신된 판정 결과를 표시부(45) 상에 표시한다(단계 S85). 예컨대, 판정부(36)가 위변조가 없는 것으로 판정한다면, "위변조 없음"이 표시되고, 또는 위변조가 있는 것으로 판정한다면, "위변조 있을 수 있음"이 표시된다.

<81> 전술한 바와 같이, 제1 실시예에 따르면, 보안성이 취약한 화상 생성 장치(카메라)는 비밀키(P)를 유지하지 않으므로 보안성이 향상된다. 공격 저지 장치(12)는 비밀키(P)를 유지하기 때문에, 모든 화상 생성 장치에 대하여 동일한 공격 저지 장치(12)(IC 카드)를 사용하여 위변조 검출을 행할 수 있다. 또한, 각 화상 생성 장치(카메라)에 맞도록 키가 개별화되므로, 하나의 화상 생성 장치(카메라)가 알려진다해도, 다른 화상 생성 장치(카메라)의 키들은 안전하다.

<82> [제2 실시예]

<83> 제1 실시예에서는 키생성 장치(14)가 카메라(11)에 카메라 ID와 그 암호화 정보 또는 EID를 설정하지만, 키생성 장치(14)가 관리면에서 불량하다면, 그 카메라 ID와 EID와의 사이의 대응이 누설될 수도 있다. 제2 실시예에서는, 각 사용자 별로 별도의 비밀 정보(A)를 키 유지부(21)에 설정하여 안전성을 보다 향상시키는 구성을 설명한다. 또한, 제2 실시예에서는, 각 촬영 별로 생성된 난수가 MAC에 대한 키를 변경하는데 사용되어 MAC 용의 키를 변경하는 구성이 제공되어, 안전성을 더욱 증가시킨다. 그러나, 비밀 정보(A)는 사용자가 개별로 조작부(22)를 이용하여 키 유지부(21)에 설정하는 정보이다. 또한, 비밀 정보(A)는 공격 저지 장치(12)의 키 유지부(31)에도 설정되어 있고, 안전하게 관리되는 것으로 가정한다.

<84> 제2 실시예에 따른 화상 생성 장치(11), 공격 저지 장치(12), 화상 검증 보조 장치(13), 및 키생성 장치(14)의 구성은, 제1 실시예(도 1 ~ 도 5)와 마찬가지이다. 이하, 도 11 ~ 도 13의 플로우차트, 및 도 14 및 도 15의 데이터의 흐름도를 참조하여, 제2 실시예에 따른 위변조 검출 처리를 설명한다.

<85> 키생성 장치(14)의 동작은 제 l 실시예(도 6)에서 설명한 바와 같다. 화상 생성 장치(11)의 산술 연산부(23)는, 키생성 장치(14)로부터의 암호화 정보 EID와 비밀 정보(A)로부터 키(K)를 생성하여, 이것을 키 유지부(21)에 유지한다. 즉, 도 11 및 도 14에 도시된 바와 같이, 화상 생성 장치(11)는 키생성 장치(14)로부터 암호화 정보의 EID를 수신하면, 산술 연산부(23)에서 EID*A를 계산하고, 이를 키(K)로 한다(단계 S111). 그리고,이 키(K)를 새로운 키로서 키 유지부(21)에 보존한다(단계 S112).

<86> 이하, 도 12 및 도 14를 참조하여, 화상 생성 장치(11)에 의한 MAC 생성 처리를 설명한다. 우선, 화상 생성 장치(11)는 화상(D)을 촬상부(25)로부터 입력한다(단계 S121). 다음, 화상(D)에 대한 해시값(H)를 해시 생성부(27)를 이용하여 계산한다(단계 S122). 화상 생성 장치(11)는 매번 촬영시에 산술 연산부(23)에서 난수(r)를 생성한다. 그리고, 단계 S112에서 키 유지부(21)에 유지되는 키(K)와 난수(r)를 이용하여, 촬영에 대한 키(K=K*r)를 연산부(23)에서 계산한다(단계 S123). 이렇게 해서 계산된 키(K= EID*A*r)를 이용하여, 상기 단계 S54에서와 마찬가지의 처리를 통해 해시값(H)에 대한 MAC이 생성된다(단계 S124). 그리고, 화상 생성 장치(11)의 화상 파일 생성부(26)는, 화상(D)의 화상 파일에 MAC와 카메라 ID와 단계 S123에서 생성된 난수(r)를 첨부함으로써 화상 파일(1401)을 생성한다(단계 S125).

<87> 이하, 도 13을 참조하여, 제2 실시예에 따른 위변조 검출 처리(MAC 검증 처리)를 설명한다.

<88> 화상 검증 보조 장치(13)는 화상(D), MAC, 카메라 ID, 및 난수(r)를 포함하는 화상 파일을 통신부(41)로부터 판독한다(단계 S131). 화상 검증 보조 장치(13)의 화상 파일 분리부(42)는 판독한 화상 파일을, 도 15에 도시한 바와 같이, 화상(D), MAC, 카메라 ID, 및 난수(r)로 분리한다(단계 S132). 다음, 화상 검증 보조 장치(13)는 해시 생성부(43)를 이용하여 화상(D)에서 해시값(H)를 생성한다(단계 S133). 그리고, 화상 검증 보조 장치(13)는 생성한 해시값(H)과 분리한 MAC, 카메라 ID 및 난수(r)를, 통신부(41)를 통해 공격 저지 장치(12)에 보낸다(단계 S134).

<89> 공격 저지 장치(12)는 통신부(34)를 통하여 보내여져 온 카메라 ID를 키 유지부(31)에 유지되어 있는 비밀키(P)를 이용하여 암호화부(33)로 암호화하여 EID를 얻는다(단계 S141). 여기서, 암호화부(33)에서 사용되는 암호화 처리는 키생성 장치(14)의 암호화부(53)에서 사용되는 암호화 처리와 동일하다. 다음, 상기 단계 S111과 단계 S123의 처리를 통해 얻어진 화상(D)에 대한 키(K= EID*A*r)를 산술 연산부(32)에서 계산한다(단계 S142). 이렇게 해서 얻어진 키(K)는 MAC 계산을 위해이용된다. 즉, MAC 생성부(35)는, 단계 S142에서 얻어진 키(K)를 이용하여, 화상 검증 보조 장치(13)로부터 보내온 해시값(H)에 대한 MAC(이하, MAC2)를 생성한다(단계 S143). 판정부(36)는 MAC 생성부(35)에 의해 생성된 MAC2와 화상 검증 보조 장치(13)로부터 보내온 MAC가 일치하는지 여부를 판정한다(단계 S144). 그리고, MAC와 MAC2가 일치하면 위변조가 없는 것으로 판정하며(단계 S145), 또는 일치하지 않으면 위변조가 있는 것으로 판정한다(단계 S146).

<90> 상기 판정의 결과는 통신부(34)를 통해 화상 검증 보조 장치(13)에 보내진다(단계 S147). 화상 검증 보조 장치(13)는 보내여져 온 판정 결과를 표시부(45) 상에 표시한다(단계 S135). 예컨대, 판정부(36)가 위변조가 없는

것으로 판정하면, "위변조 없음"이 표시되고, 위변조가 있다면, "위변조 있을 수 있음"이 표시된다.

<91> 또한, 비밀 정보(A)와 난수(r)는 반드시 양측 모두가 설정되지 않아도 되며, 비밀 정보(A) 또는 난수(r) 어느 것만이라도 설정되어도 된다. 예컨대, 비밀 정보(A)만 사용된다면, 도 12의 단계 S123는 불필요하며, 단계 S124에 있어서 키(K= EID*A)를 이용하여 MAC가 생성된다. 또한, 난수(r)가 존재하지 않기 때문에, 도 13의 단계 S132 및 S134에서의 처리는 제1 실시예(도 8)의 단계 S82 및 S84에서의 처리와 동일하다. 또한, 단계 S142에서 키(K= EID*A)가 이용된다. 한편, 난수(r)만이 설정되면, 도 11의 단계 S111에서의 처리는 불필요하며, 키 유지부(21)에 EID가 키(K)로서 유지된다. 또한, 도 13의 단계 S142에서의 처리를 통해 키(K= EID* r)가 계산된다.

<92> 또한, 비밀 정보(A)만이 사용되는 모드, 난수(r)만이 사용되는 모드, 및 비밀 정보(A) 및 난수(r)의 양측 모두가 사용되는 모드가 의지대로 절환될 수도 있다.

<93> 상기 실시예에 있어서, 화상 생성 장치(11)에서 생성된 키(K)는 키 유지부(21)에 유지되지만, 본 발명은 이러한 형태에 한하지 않는다. 예컨대, MAC이 생성될 때마다, EID*A 또는 EID*A*r이 계산될 수도 있다.

<94> 전술한 바와 같이, 제2 실시예에 따르면, 제1 실시예의 효과에 더하여, 비밀 정보(A)를 이용하여 EID를 처리함으로써 키(K)가 생성되므로, 보안이 더욱 향상된다는 효과가 있다. 또한, 보호 대상의 데이터(화상 데이터)에 대한 인증 정보(MAC)를 생성할 때마다 난수(r)를 이용하여 키(K)가 변경되어, 보안이 향상될 수 있다. 또한, 난수(r)는 각 화상 또는 각 사용자 별로 설정될 수도 있다. 또한, 여기서 r는 난수이지만, r는 난수가 아니라, 촬영마다, 또는 화상 또는 사용자 마다 설정될 수도 있다.

<95> [제3 실시예]

<96> 제1 및 제2 실시예에서는 MAC이 사용되지만, 제3 실시예에서는 공개키 암호화에 의한 디지털 서명이 사용된다. 시스템의 구성은 제1 실시예(도 1)와 마찬가지이다. 또한, 화상 검증 보조 장치(13)의 구성은 제1 실시예(도 4)와 마찬가지이므로, 그 도시 및 설명은 생략된다. 그러나, 공개키 암호화가 사용되면, 검증용의 키는 공개할 수 있기 때문에, 공격 저지 장치(12)는 불필요할 수 있다. 이 경우, 카메라 ID에 대응하는 공개키를 관리하는 서버에 조회하여, 화상 검증 보조 장치(13)에 의해 직접 검증을 행할 수도 있다. 이하에서는, 공격 저지 장치가 공개 키를 생성 및 관리하는 장치로서 또한 검증 장치로서 사용되는 경우를 설명한다.

<97> 도 16은 제3 실시예에 따른 화상 생성 장치(11)의 구성을 나타내는 도면이다. 제1 실시예(도 2)와 마찬가지의 부분에는 동일한 참조 번호가 지정되어 있다. 서명 생성부(161)는 해시 생성부(27)에 의해 생성된 해시값(H)과 키 유지부(21)에 유지되는 키 데이터에 기초하여 서명 데이터를 생성한다.

<98> 도 17은 제3 실시예에 따른 공격 저지 장치(12)의 구성을 나타내는 도면이다. 제1 실시예(도 3)와 마찬가지의 부분에는 동일한 참조 번호가 지정되어 있다. 시드 유지부(171)는 시드 값을 유지한다. 키페어 생성부(172)는 시드 유지부(171)에 유지된 시드 값과 카메라 ID를 이용하여 키의 페어(공개키, 비밀키)를 생성한다. 서명 검증부(173)는 키페어 생성부(172)에 의해 생성된 공개키를 이용하여 서명 데이터를 검증한다.

<99> 도 18은 제3 실시예에 따른 키생성 장치(14)의 구성을 나타내는 블록도이다. 제1 실시예(도 5)와 마찬가지의 부분에는 동일한 참조 번호가 지정되어 있다. 키페어 생성부(181)는 시드 관리부(182)에서 관리 및 유지되는 시드 값과 ID 입력부(52)를 통하여 입력되는 카메라 ID에 기초하여 키페어(공개키, 비밀키)를 생성한다. 시드 관리부(182)는 제1 실시예에서 키 관리부(51)가 비밀 키(P)를 관리하는 것과 마찬가지로, 시드 값(소정의 비트 수의 수치)을 안전하게 관리한다. 즉, 시드 관리부(182)는 패스워드 또는 정당 사용자의 생체 정보를 사용하여 제한적으로 판독된다. 그리고, 시드 관리부(182)는 시드 값이 누설되지 않도록 키페어 생성부(181) 이외의 외부에 키의 판독을 금지시킨다. 키페어 생성부(123)는 공지된 공개키에 대한 키페어 계산 알고리즘을 이용하여 키페어를 계산한다. 이하, 시드 값은 시드(S)라 한다.

<100> 이하, 제3 실시예에 따른 이상의 구성을 갖는 시스템의 위변조 검출 처리에 대하여 도 19 내지 도 21의 플로우차트 및 도 22 및 도 23의 데이터 흐름도를 참조하여 설명한다.

<101> 도 19는 제3 실시예에 따른 키생성 장치(14)에서의 키생성 처리의 수순을 나타낸 플로우차트이다. 우선, 카메라마다 다른 카메라 ID가 ID 입력부(52)에 의해 입력되면, 입력된 카메라 ID는 키페어 생성부(181)에 보내진다(단계 S191). 키페어 생성부(181)는 시드 관리부(182)에 유지되는 시드(S)를 이용하여 카메라 ID의 곱인 S*ID를 계산한다(단계 S192). 그리고, 키페어 생성부(181)는 산출된 S*ID로부터 공개키 암호의 공개키와 비밀키의 키페어(key pair)를 계산한다(단계 S193). 단계 S193에서 계산된 키페어 중의 비밀키를 화상 생성 장치(11)에

통신부(54)를 통하여 송신한다(단계 S194). 송신된 비밀키는 도 22에 도시된 바와 같이, 화상 생성 장치(11)의 키 유지부(21)에 설정된다.

<102> 도 20은 화상 생성 장치(11)의 위변조 검출을 위한 정보(서명 정보)를 포함하는 화상 파일을 생성하는 처리를 설명하는 플로우차트이다.

<103> 화상 생성 장치(11)는 화상(D)을 촬상부(25)로부터 입력한다(단계 S201). 다음, 해시 생성부(27)는 화상(D)에 대한 해시값(H)를 계산한다(단계 S202). 다음, 서명 생성부(161)는 키 유지부(21)에 유지되는 비밀키를 이용하여, 해시 생성부(27)에서 얻어진 해시값(H)에 대한 디지털 서명(G)을 계산한다(단계 S153). 화상 파일 생성부(26)는 화상(D)의 화상 파일에 서명 생성부(161)에 의해 생성된 서명(G)과 카메라 ID를 첨부함으로써 화상 파일(221)을 생성한다(단계 S154). 서명 생성부(161)의 디지털 서명 생성 알고리즘은 RSA 암호 등의 공개키 암호화를 이용할 수도 있다.

<104> 이하, 도 21 및 도 23을 참조하여, 상기와 같이 생성된 화상 파일(도 22의 221)에 대한 공격 저지 장치(12) 및 화상 검증 보조 장치(13)에 의해 수행되는 위변조 검출 처리를 설명한다. 또한, 공격 저지 장치(IC 카드)(12)는, 도 23에 도시한 바와 같이, 시드 유지부(171)에 시드(S)를 안전하게 유지한다. 이 시드(S)는 키생성 장치(14)의 시드 관리부(182)에 의해 관리되는 시드(S)와 동일하다. 또한, 시드 유지부(171)는 시드 관리부(182)와 마찬가지의 구성를 가질 수도 있다. 또한, 키페어 생성부(172)는 키생성 장치(14)의 키페어 생성부(181)와 마찬가지의 구성을 가질 수도 있다. 또한, 서명 검증부(173)는 화상 생성 장치(11)의 서명 생성부(161)에 대응하는 서명 검증 알고리즘을 갖는다.

<105> 이하, 도 21의 플로우차트를 참조하여, 제3 실시예에 따른 공격 저지 장치(12) 및 화상 검증 보조 장치(13)에 의한 서명 검증의 수순을 설명한다.

<106> 우선, 화상 검증 보조 장치(13)는 화상(D)와 서명(G) 및 카메라 ID를 포함하는 화상 파일을 통신부(41)로부터 판독한다(단계 S211). 화상 검증 보조 장치(13)의 화상 파일 분리부(42)는 판독된 화상 파일을 화상(D)와 서명 데이터 G 및 카메라 ID로 분리한다(단계 S212). 화상 검증 보조 장치(13)는 화상(D)에서 해시 생성부(43)를 이용하여 해시값(H)을 생성한다(단계 S213). 화상 검증 보조 장치(13)는 해시값(H), 분리된 G, 및 카메라 ID를 통신부(41)를 통하여 공격 저지 장치(12)에 보낸다(단계 S214).

<107> 공격 저지 장치(12)에서는, 키페어 생성부(172)가 통신부(44)를 통해 보내여져 온 카메라 ID와, 시드 유지부(171)에 유지되어 있는 시드(S)를 이용하여 S*ID를 계산한다(단계 S221). 그리고, 키페어 생성부(172)는 계산된 S*ID로부터 공개키 암호화에 대한 키 페어를 생성한다(단계 S222). 여기서 이용되는 키페어 생성 알고리즘은 키생성 장치(14)의 키페어 생성부(181)에서 이용된 것과 동일하다. 따라서, 키페어 생성 소오스의 S*ID가 동일하다면, 키페어 생성 장치(14)의 키페어 생성부(181)로 얻어지는 키페어와, 공격 저지 장치(12)의 키페어 생성부(172)에 의해 얻어지는 키페어는 동일하다. 즉, 공격 저지 장치(12)에 의해 계산된 공개키는 키생성 장치(14)에 의해 계산된 비밀키와 쌍을 이루는 키로서 생성된다.

<108> 다음, 서명 검증부(173)는 단계 S222에서 생성된 공개키를 이용하여 서명(G)을 복호함으로써 H2를 생성한다(단계 S223). 그리고, 판정부(36)는, 단계 S223에서 생성된 H2와 화상 검증 보조 장치(13)로부터 송신된 H가 일치하는지 여부를 판정한다(단계 S224). 그리고, H와 H2가 일치하면, 위변조가 없는 것으로(단계 S225), 일치하지 않으면 위변조가 있는 것으로 판정한다(단계 S226).

<109> 상기 판정의 결과는 통신부(34)를 통해 화상 검증 보조 장치(13)에 보내진다(단계 S227). 화상 검증 보조 장치(13)는 송신된 판정 결과를 표시부(45)상에 표시한다(단계 S215). 예컨대, 판정부(36)가 위변조가 없는 것으로 판정하면, "위변조 없음"이 표시되고, 또는 위변조가 있는 것으로 판정하면, "위변조 있을 수 있음"이 표시된다.

<110> 전술한 바와 같이, 상기의 각 실시예에 따르면, 화상 생성 장치의 보안 취약성이 제거되고, 보안 성능이 향상된다. 또한, 1 개의 IC 카드로 전 카메라의 검증 데이터를 조작할 수 있는 시스템을 제공할 수 있다.

<111> 제3 실시예에서는, 서명(G)을 생성하기 위하여 비밀키가, 서명(G)을 검증하기 위하여 공개키가 이용되지만, 암호화의 경우, 암호문(G)을 생성하기 위하여 공개키가, 암호문(G)을 해독하기 위하여 비밀키가 이용될 수도 있다.

<112> 전술한 바와 같이, 제3 실시예에 따르면, 제1 실시예의 효과에 더하여, 보호 대상 데이터의 위변조 검출에 공개키 암호화를 이용한 디지털 서명이 이용될 수도 있다는 효과가 있다.

<113> [각종 변형예]

<114> 이하, 제1 내지 제3 실시예에 관한 각종 변형예를 설명한다.

<115> 제1 및 제2 실시예에 있어서, MAC 데이터 생성 처리는 피사체의 화상 데이터만을 이용하여 수행되지만, 본 발명은 이러한 형태에 한하지 않는다. 예컨대, 보조 파라미터(예컨대, 촬영 시각, 촛점거리, f-값, ISO 속도, 측광 모드, 화상 파일 사이즈, 촬영자 정보, 등)과 같은 화상 데이터의 메타 데이터에 해당하는 정보에 대하여, 화상 데이터와 같은 방식으로 MAC 데이터가 생성된다. 따라서, 화상 데이터와 마찬가지의 MAC 검증 처리가 보조 파라미터에 대하여 구현될 수 있다. 화상 데이터 및 메타 데이터는 이진 데이터(디지털 데이터)이다. 따라서, 화상 데이터를 메타 데이터로 치환하여, 즉 화상 데이터로부터 메터 데이터로 절환하여 해시 생성부(27)에 입력되되록 함으로써, 상기 처리가 구현될 수 있음은 분명하다. 또한, 데이터의 절환이 사용자로부터의 지시에 의해 이루어질 수도 있다.

<116> 전술된 바와 같이, 보조 파라미터에 MAC를 첨부함으로써 검증함에 있어서, 도 7 및 도 8에 도시된 처리에서 화상(D)가 보조 파라미터들로 치환될 수도 있다. 또한, MAC이 디지털 서명으로 변경되면, 공개키 암호화에 의해서 보조 파라미터들이 검증될 수 있음은 분명하다.

<117> 또한, 제1 실시예에서는, MAC 검증 처리가 화상 검증 보조 장치(13)(PC) 및 격 저지 장치(12)(IC 카드)로 분리되지만, 화상 검증 보조 장치(13)와 공격 저지 장치(12)는 검증 장치로서 일체화될 수도 있다. 이러한 경우, 화상 파일 생성부(26)에서 생성된 화상 파일만을 화상 생성 장치(11)로부터 검증 장치에 입력함으로써 해당 화상의 위변조가 검증될 수 있다. 또한, 이러한 경우, 도 8에 도시된 처리는 하나의 장치 내에서 수행되며, 화상 검증 보조 장치(13)와 공격 저지 장치(12)와의 구별은 필요없다.

<118> 또한, 제2 실시예(도 11 내지 도 13)에서는, 새로운 키를 생성하는 산술 연산으로서 K= K*X가 이용되지만, 다른 함수가 이용될 수도 있다. 즉, K= f(K, X)으로서 키가 산출될 수도 있다. 예컨대, K= K+X 이어도 된다.

<119> 이상의 변형예는 공개키 암호화에 의한 제3 실시예에 대하여 마찬가지로 구현될 수도 있다.

<120> 또한, 본 발명의 목적은 전술한 실시예의 기능을 실현하는 소프트웨어의 프로그램 코드를 기록한 기록 매체(또는 기억 매체)를 시스템 또는 장치에 공급하여, 그 시스템 혹은 장치의 컴퓨터(또는 CPU, 또는 MPU)가 기록 매체에 저장된 프로그램 코드를 판독하여 실행함으로써 달성될 수도 있다. 이러한 경우, 기록 매체로부터 판독된 프로그램 코드 자체는 전술한 실시예의 각 기능을 구현할 수 있으며, 그 프로그램 코드를 기록한 기록 매체는 본 발명을 구성할 수 있다.

<121> 상기 실시예들에 있어서, 컴퓨터가 프로그램 코드를 판독하여 실행하거나, 컴퓨터 상에서 동작하는 운영 체제(OS)가 그 프로그램 코드의 지시에 기초하여, 실제의 처리의 일부 또는 전부를 행하는 방식으로, 각 기능이 구현될 수도 있다.

<122> 또한, 상기 실시예들에 있어서, 기록 매체로부터 판독된 프로그램 코드를 컴퓨터에 삽입된 기능 확장 카드 또는 컴퓨터에 접속된 기능 확장 유닛에 구비된 메모리에 기입하여, 그 프로그램 코드의 지시에 기초하여, 기능 확장 카드 또는 기능 확장 유닛에 구비된 CPU 등이 실제의 처리의 일부 또는 전부를 수행함으로써, 각 기능이 구현될 수도 있다.

<123> 본 발명이 기록 매체에 적용되는 경우, 그 기록 매체는 전술한 바와 같이 플로우차트에 해당하는 프로그램 코드를 저장할 수도 있다.

발명의 효과

<124> 본 발명에 따르면, 데이터의 위변조에 대한 보안 성능을 향상시킬 수 있다.

<125> 본 발명의 많은 다양하고 광범위한 실시예들이 그 개념 및 범주를 일탈하지 않고서 이루어질 수 있으므로, 본 발명은 첨부된 청구범위에 정의된 바 외에 지정된 실시예들에 제한되는 것은 아니다.

도면의 간단한 설명

<1> 도 1은 본 발명의 일 실시예에 따른 화상 검증 시스템의 일 구성예를 설명하는 블록도.

<2> 도 2는 제1 실시예에 따른 화상 생성 장치(11)의 주요 기능 구성을 설명하는 블록도.

<3> 도 3은 제1 실시예따른 공격 저지 장치(12)의 주요 기능 구성을 설명하는 블록도.

<4> 도 4는 제1 실시예에 따른 화상 검증 보조 장치(13)의 주요 기능 구성을 설명하는 블록도.

<5> 도 5는 제1 실시예에 따른 키 생성 장치(14)의 주요 기능 구성을 설명하는 블록도.

<6> 도 6은 제1 실시예에 따른 키설정 처리를 설명하는 플로우차트.

<7> 도 7은 제 1 실시예에 따른 MAC 생성 처리를 설명하는 플로우차트.

<8> 도 8은 제1 실시예에 따른 MAC 검증 처리를 설명하는 플로우차트.

<9> 도 9는 도 6 및 도 7의 플로우차트에 도시된 처리에서 이용 및 생성되는 데이터 및 그 흐름을 설명하는 도면.

<10> 도 10은 도 8의 플로우차트에 도시된 처리에서 이용 및 생성되는 데이터 및 그 흐름을 설명하는 도면.

<11> 도 11은 제2 실시예에 따른 키 설정 처리를 설명하는 플로우차트.

<12> 도 12는 제2 실시에 따른 MAC 생성 처리를 설명하는 플로우차트.

<13> 도 13은 제2 실시예에 따른 MAC 검증 처리를 설명하는 플로우차트.

<14> 도 14는 도 11 및 도 12의 플로우차트에 도시된 처리에서 이용 및 생성되는 데이터 및 그 흐름을 설명하는 도면.

<15> 도 15는 도 13의 플로우차트에 도시된 처리엣 이용 및 생성되는 데이터 및 그 흐름을 설명하는 도면.

<16> 도 16은 제3 실시예에 따른 화상 생성 장치(11)의 주요 기능 구성을 설명하는 블록도.

<17> 도 17은 제3 실시예에 따른 공격 저지 장치(12)의 주요 기능 구성을 설명하는 블록도.

<18> 도 18은 제3 실시예에 따른 키 생성 장치(14)의 주요 기능 구성을 설명하는 블록도.

<19> 도 19는 제3 실시예에 따른 키 설정 처리를 설명하는 플로우차트.

<20> 도 20은 제3 실시예에 따른 서명 생성 처리를 설명하는 플로우차트.

<21> 도 21은 제3 실시예에 따른 서명 검증 처리를 설명하는 플로우차트.

<22> 도 22는 도 19 및 도 20의 플로우차트에 도시된 처리에서 이용 및 생성되는 데이터 및 그 흐름을 설명하는 도면.

<23> 도 23은 도 21의 플로우차트에 도시된 처리에서 이용 및 생성되는 데이터 및 그 흐름을 설명하는 도면.

<24> <도면의 주요 부분에 대한 부호의 설명>

<25> 11 화상 생성 장치 12 공격 저지 장치

<26> 13 화상 검증 보조 장치 14 키 생성 장치

<27> 21 키 유지부 22 조작부

<28> 23 산술 연산부 24 통신부

<29> 25 촬상부 26 화상 파일 생성부

<30> 27 해시 생성부 28 MAC 생성부

<31> 29 제어부 34 통신부

<32> 31 키 유지부 33 암호화부

<33> 32 산술 연산부 35 MAC 생성부

<34> 36 판정부 37 제어부

<35> 42 화상 파일 분리부 46 제어부

<36> 45 표시부 41 통신부

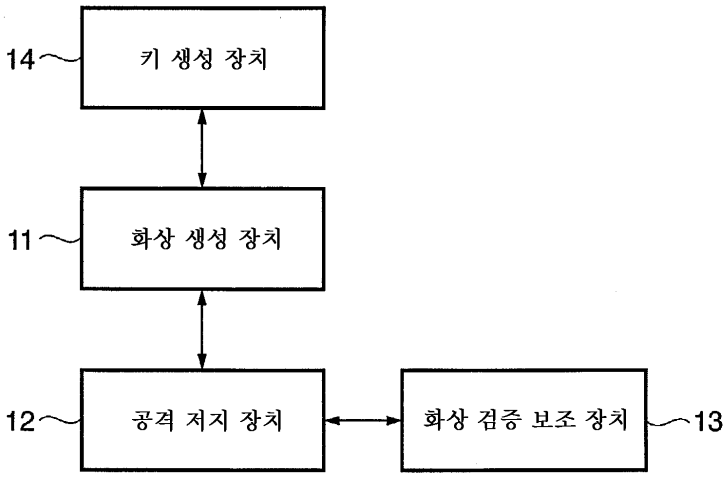
<37> 43 해시 생성부 52 ID 입력부

<38> 53 암호화부 51 키 관리부

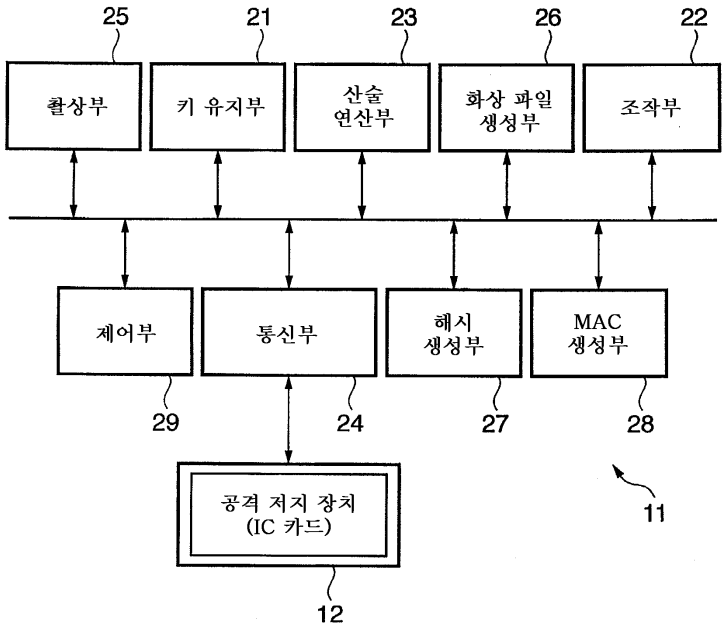
<39> 54 통신부 55 제어부

도면

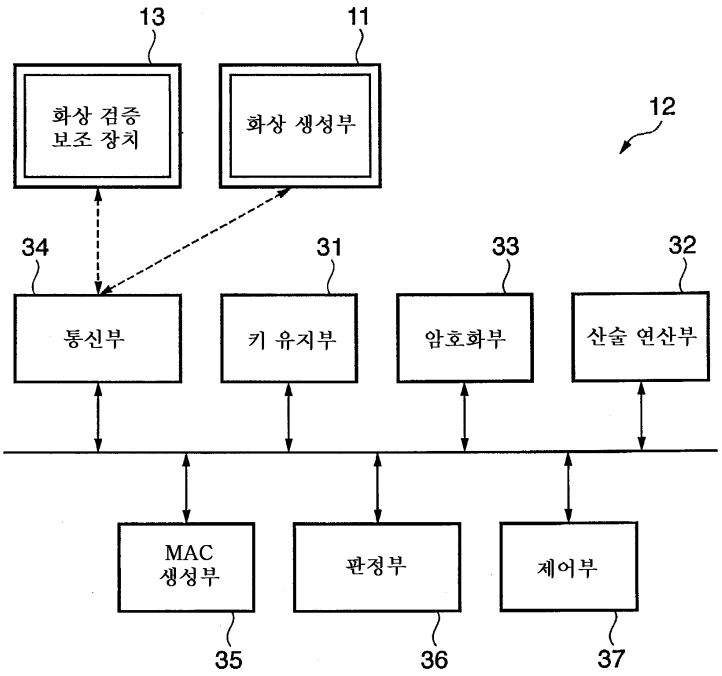
도면1



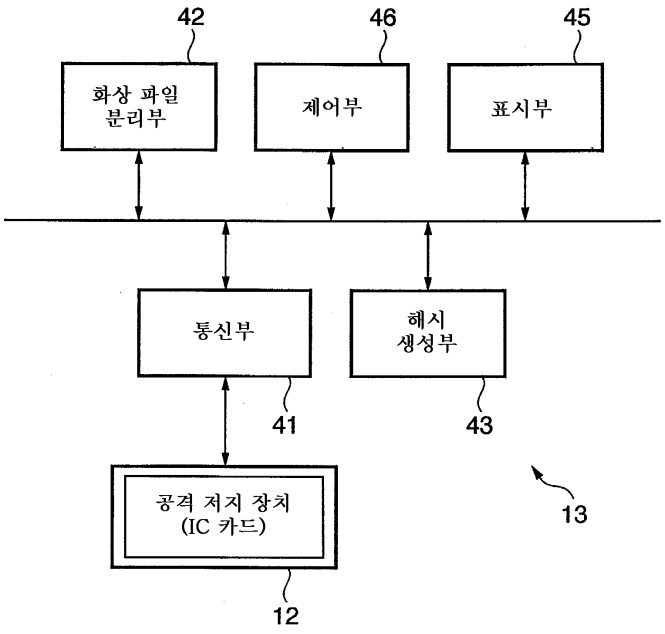
도면2



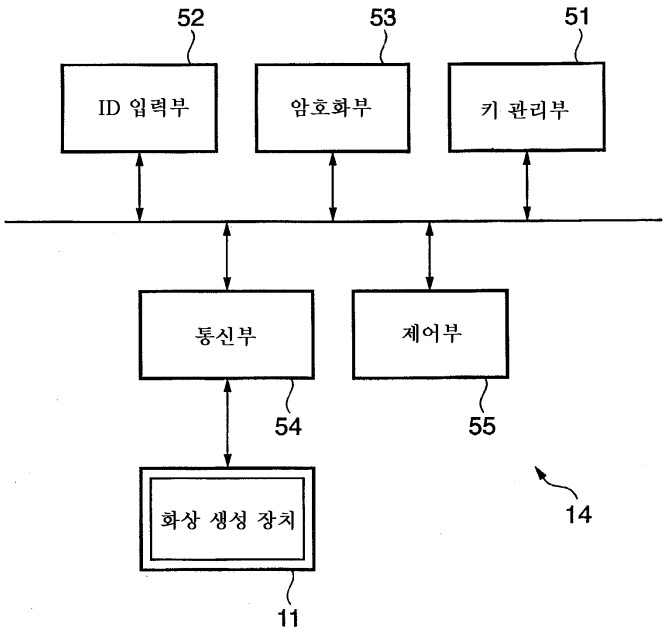
도면3


13
11
화상 검증
보조 장치
화상 생성부
12
34
31
33
32
통신부
키 유지부
암호화부
산술 연산부
MAC
생성부
판정부
제어부
35
36
37

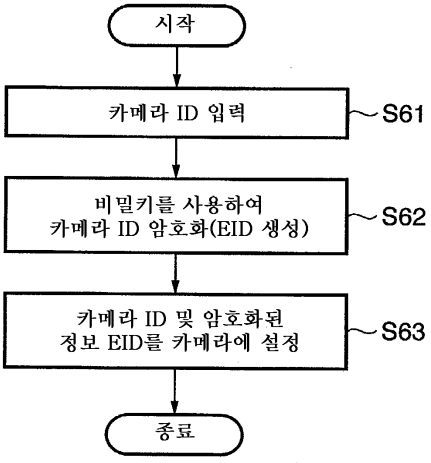
도면4


42
46
45
화상 파일
분리부
제어부
표시부
통신부
해시
생성부
41
43
공격 저지 장치
(IC 카드)
13
12

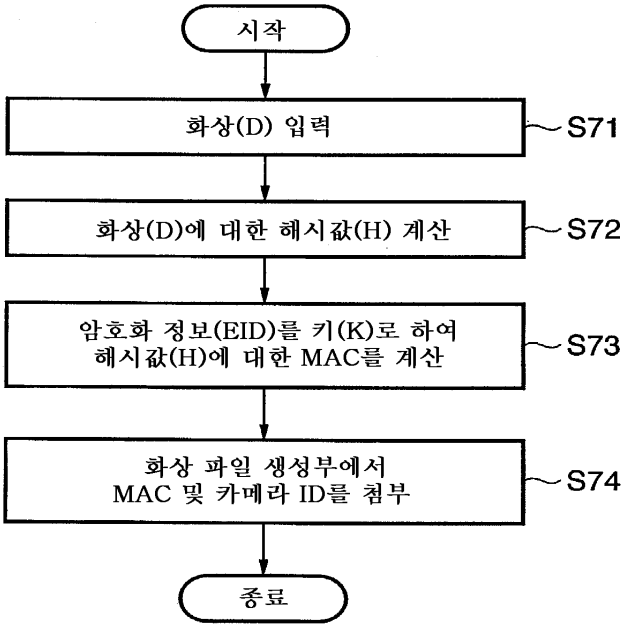
도면5


52
53
51
ID 입력부
암호화부
키 관리부
통신부
제어부
54
55
화상 생성 장치
14
11

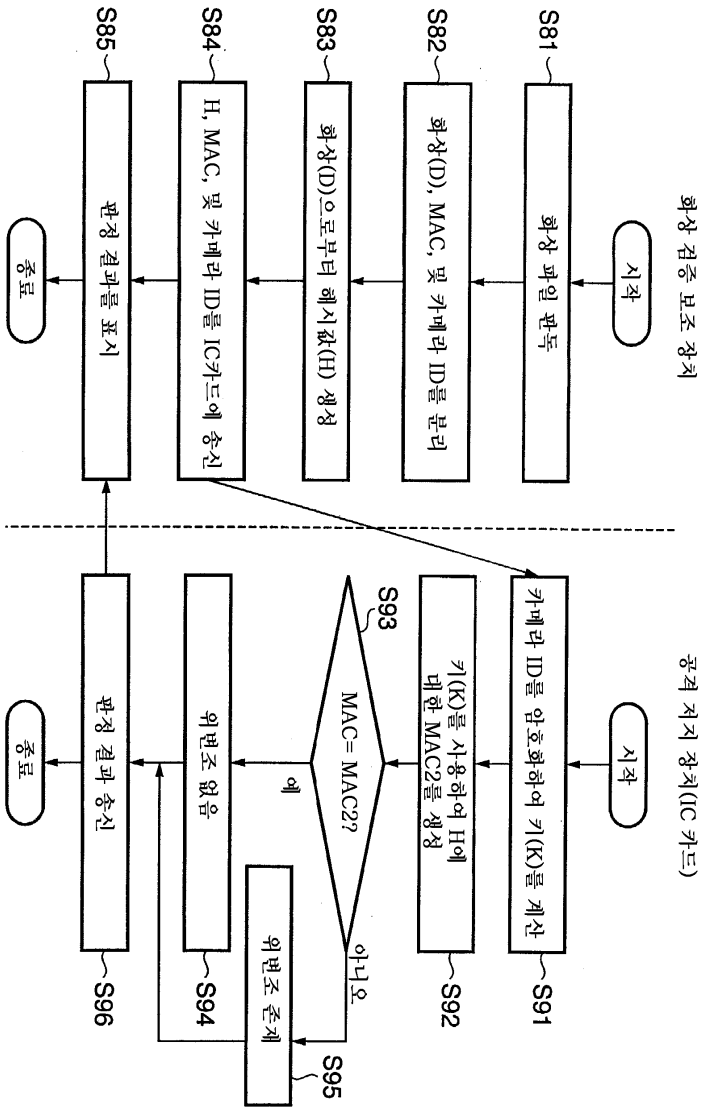
도면6


시작
카메라 ID 입력
S61
비밀키를 사용하여
카메라 ID 암호화(EID 생성)
S62
카메라 ID 및 암호화된
정보 EID를 카메라에 설정
S63
종료

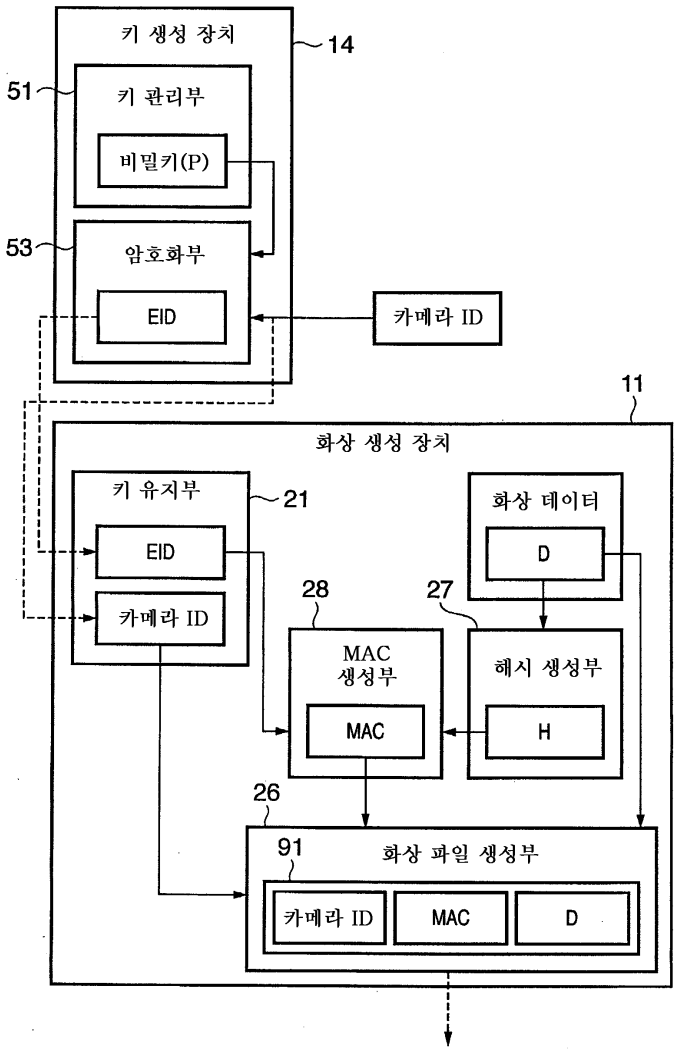
도면7


시작
화상(D) 입력
S71
화상(D)에 대한 해시값(H) 계산
S72
암호화 정보(EID)를 키(K)로 하여
해시값(H)에 대한 MAC를 계산
S73
화상 파일 생성부에서
MAC 및 카메라 ID를 첨부
S74
종료

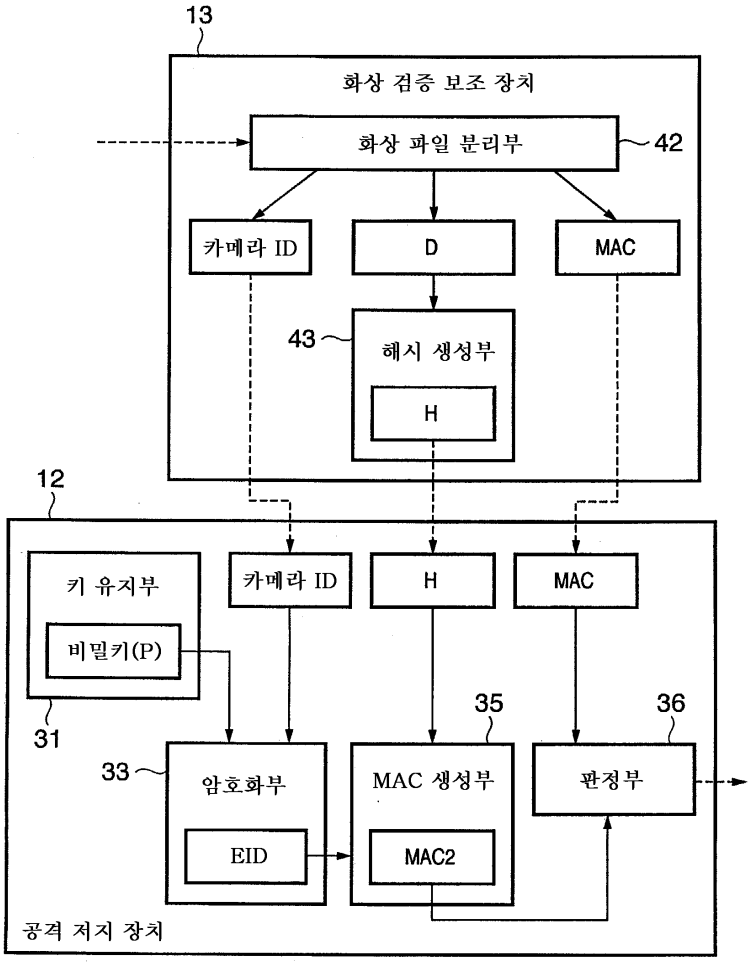
도면8


화상 검증 보조 장치
시작
S81
화상 파일 판독
S82
화상(D), MAC, 및 카메라 ID를 분리
S83
화상(D)으로부터 해시값(H) 생성
S84
H, MAC, 및 카메라 ID를 IC카드에 송신
S85
판정 결과를 표시
종료
공격 저지 장치(IC 카드)
시작
S91
카메라 ID를 암호화하여 키(K)를 계산
S92
키(K)를 사용하여 H에 대한 MAC2를 생성
S93
MAC= MAC2?
예
아니오
위변조 없음
S94
위변조 존재
S95
판정 결과 송신
S96
종료

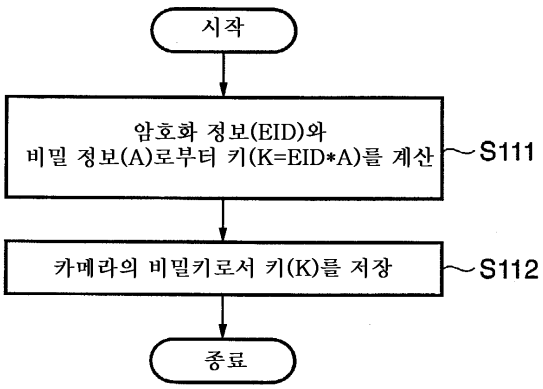
도면9


키 생성 장치
14
51
키 관리부
비밀키(P)
53
암호화부
EID
카메라 ID
11
화상 생성 장치
키 유지부
21
EID
카메라 ID
화상 데이터
D
28
27
MAC
생성부
MAC
해시 생성부
H
26
91
화상 파일 생성부
카메라 ID
MAC
D

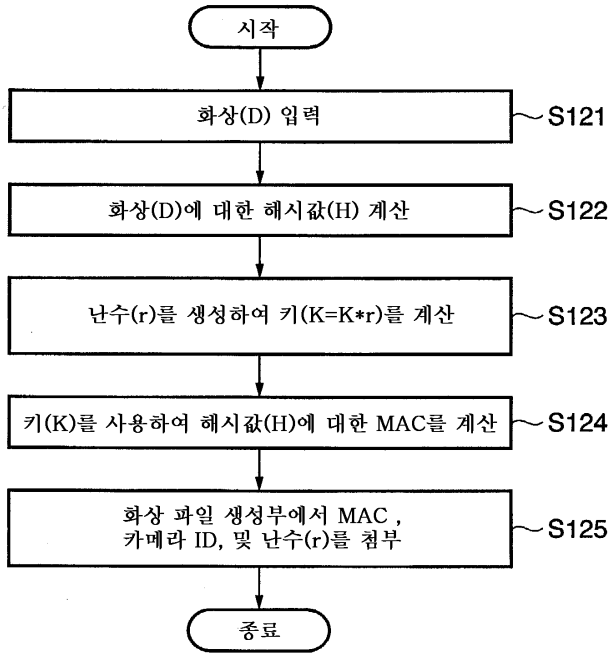
도면10


13
화상 검증 보조 장치
화상 파일 분리부
42
카메라 ID
D
MAC
43
해시 생성부
H
12
키 유지부
비밀키(P)
31
카메라 ID
H
MAC
35
36
33
암호화부
EID
MAC 생성부
MAC2
판정부
공격 저지 장치

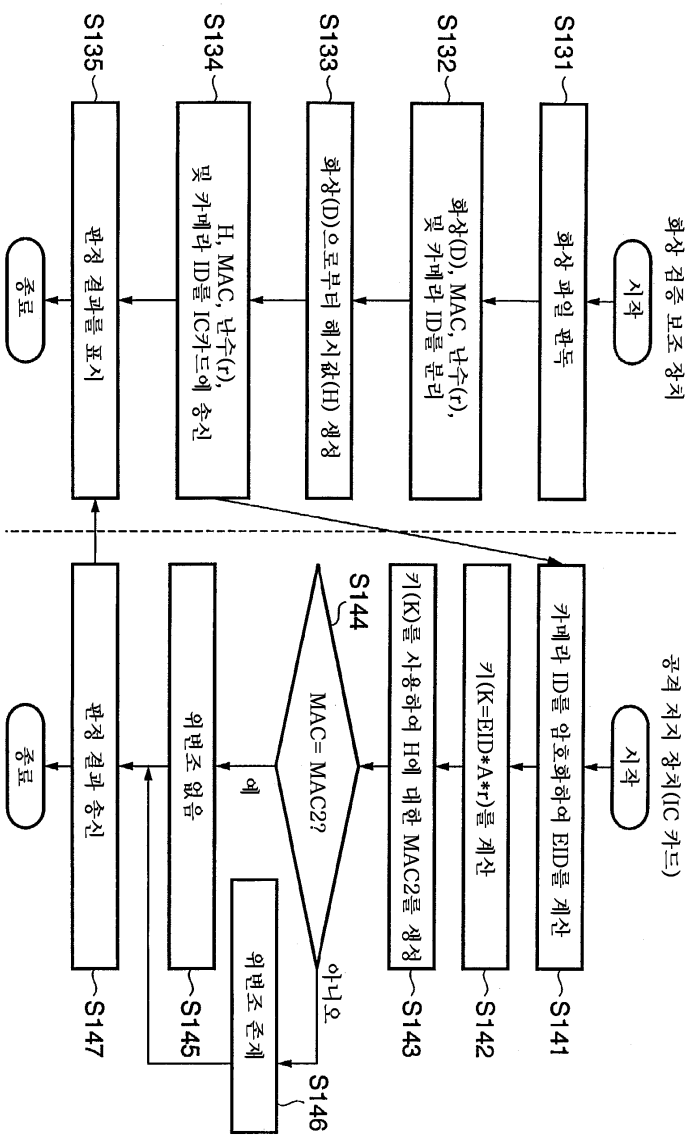
도면11


시작
암호화 정보(EID)와
비밀 정보(A)로부터 키(K=EID*A)를 계산
S111
카메라의 비밀키로서 키(K)를 저장
S112
종료

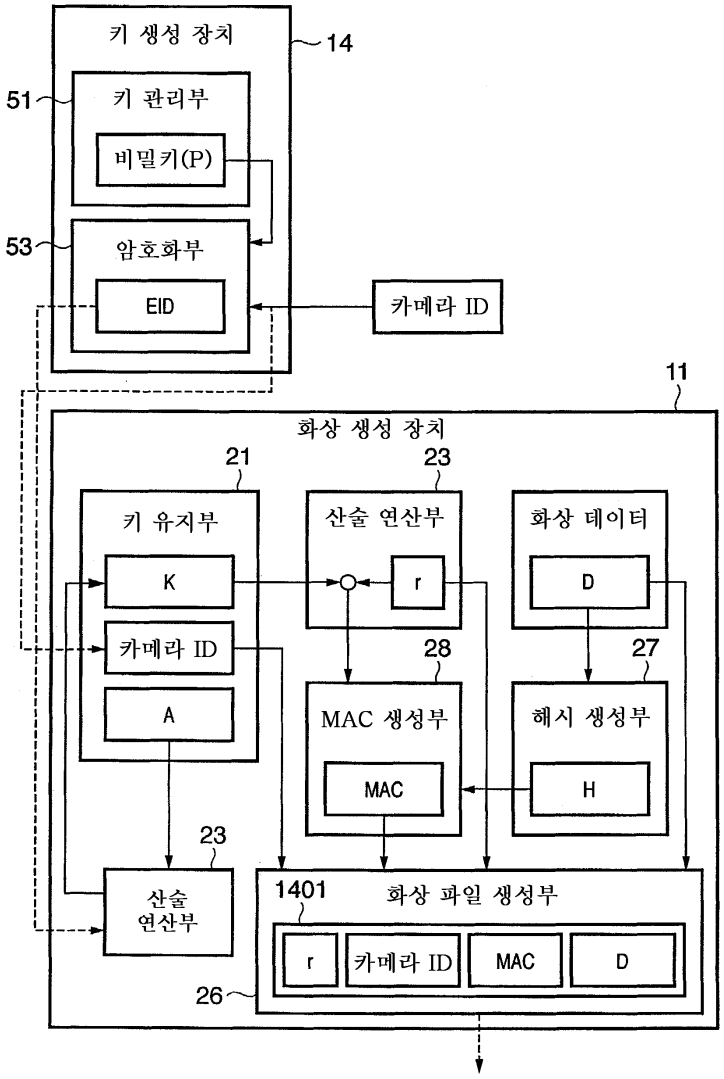
도면12


시작
화상(D) 입력
S121
화상(D)에 대한 해시값(H) 계산
S122
난수(r)를 생성하여 키(K=K*r)를 계산
S123
키(K)를 사용하여 해시값(H)에 대한 MAC를 계산
S124
화상 파일 생성부에서 MAC ,
카메라 ID, 및 난수(r)를 첨부
S125
종료

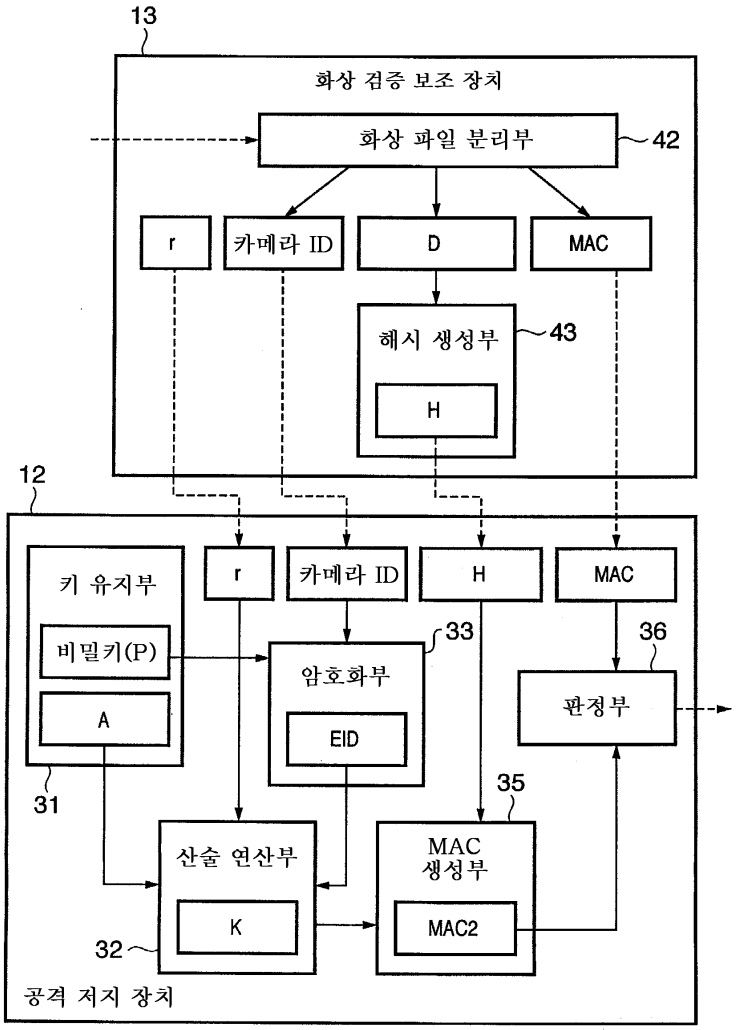
도면13


화상 검증 보조 장치
시작
화상 파일 판독
화상(D), MAC, 난수(r), 및 카메라 ID를 분리
화상(D)으로부터 해시값(H) 생성
H, MAC, 난수(r), 및 카메라 ID를 IC카드에 송신
판정 결과를 표시
종료
S131
S132
S133
S134
S135
공격 저지 장치(IC 카드)
시작
카메라 ID를 암호화하여 EID를 계산
키(K=EID*A*r)를 계산
키(K)를 사용하여 H에 대한 MAC2를 생성
MAC= MAC2?
예
아니오
위변조 없음
위변조 존재
판정 결과 송신
종료
S141
S142
S143
S144
S145
S146
S147

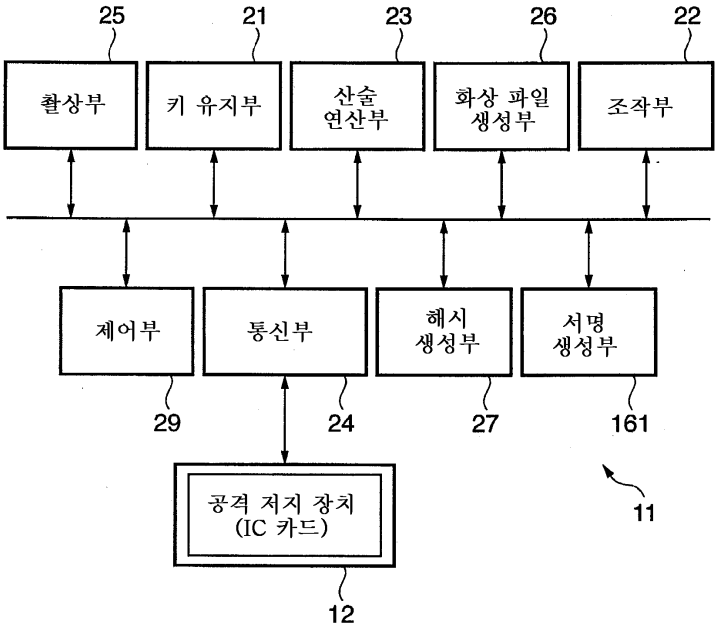
도면14


키 생성 장치
14
51
키 관리부
비밀키(P)
53
암호화부
EID
카메라 ID
11
화상 생성 장치
21
23
키 유지부
산술 연산부
화상 데이터
K
r
D
카메라 ID
28
27
A
MAC 생성부
해시 생성부
MAC
H
23
산술
연산부
1401
화상 파일 생성부
r
카메라 ID
MAC
D
26

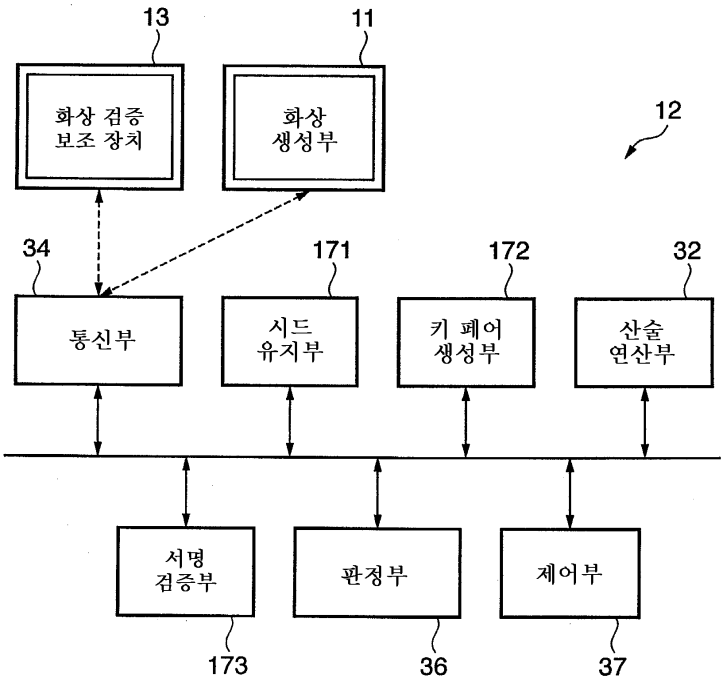
도면15


13
화상 검증 보조 장치
화상 파일 분리부
42
r
카메라 ID
D
MAC
해시 생성부
43
H
12
키 유지부
비밀키(P)
A
31
r
카메라 ID
H
MAC
33
암호화부
EID
36
판정부
35
산술 연산부
K
32
MAC
생성부
MAC2
공격 저지 장치

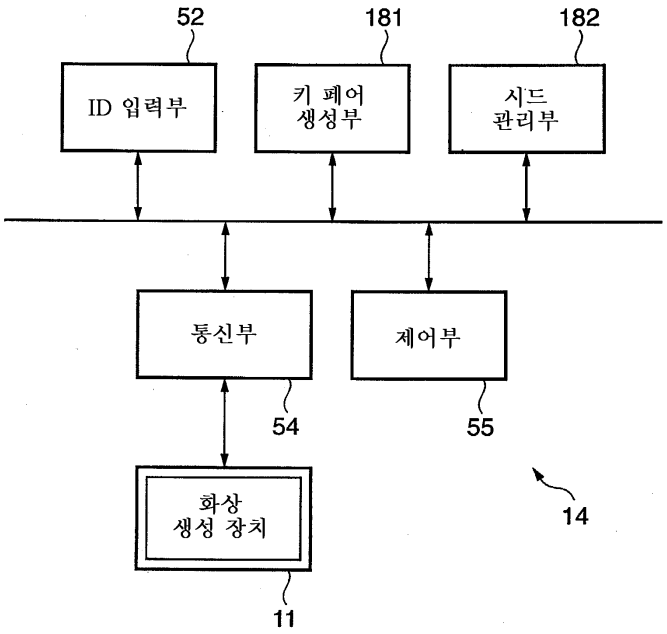
도면16


25
21
23
26
22
촬상부
키 유지부
산술 연산부
화상 파일 생성부
조작부
제어부
통신부
해시 생성부
서명 생성부
29
24
27
161
공격 저지 장치 (IC 카드)
11
12

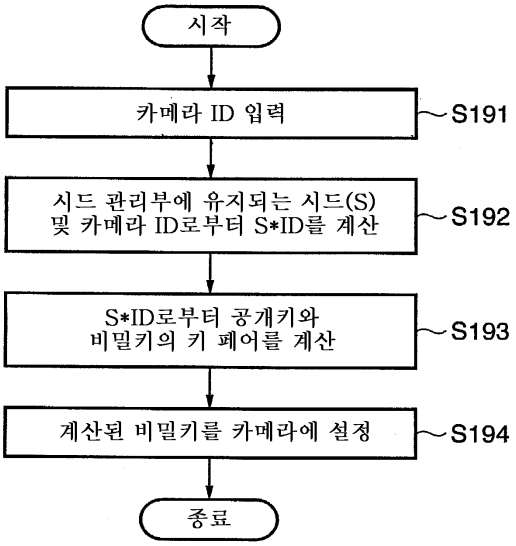
도면17


13
11
화상 검증 보조 장치
화상 생성부
12
34
171
172
32
통신부
시드 유지부
키 페어 생성부
산술 연산부
서명 검증부
판정부
제어부
173
36
37

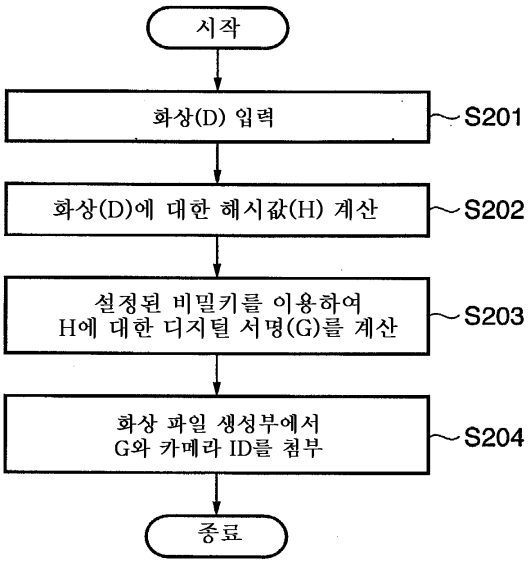
도면18


52
181
182
ID 입력부
키 페어 생성부
시드 관리부
통신부
제어부
54
55
화상 생성 장치
11
14

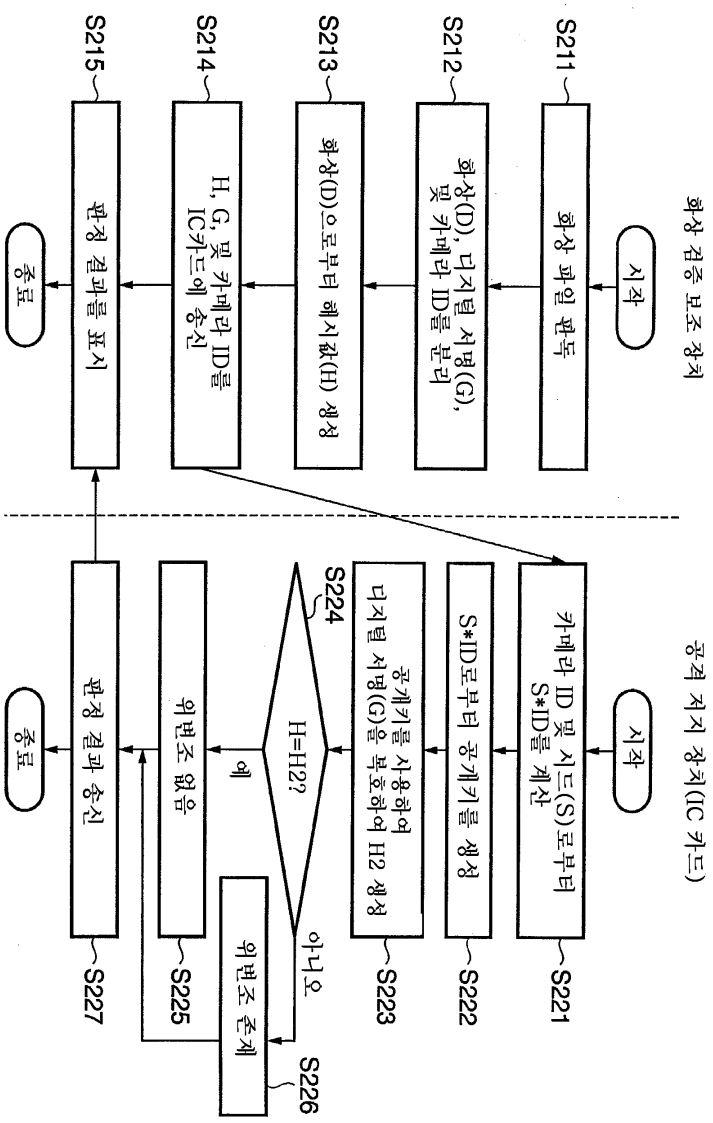
도면19


시작
카메라 ID 입력
S191
시드 관리부에 유지되는 시드(S) 및 카메라 ID로부터 S*ID를 계산
S192
S*ID로부터 공개키와 비밀키의 키 페어를 계산
S193
계산된 비밀키를 카메라에 설정
S194
종료

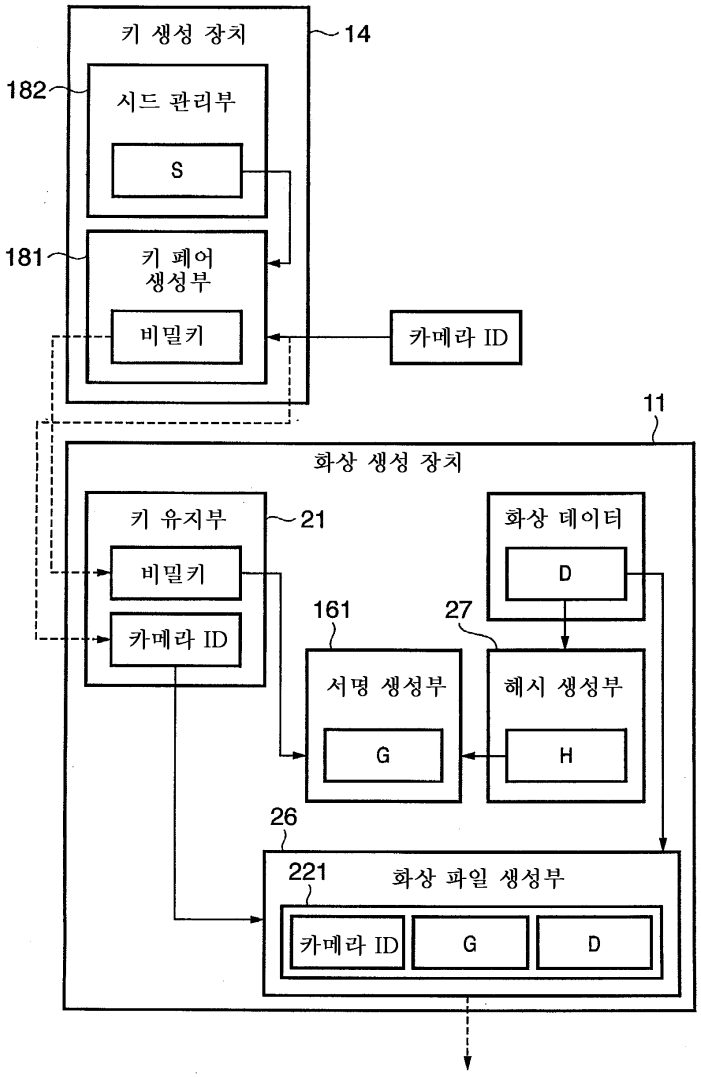
도면20


시작
화상(D) 입력
S201
화상(D)에 대한 해시값(H) 계산
S202
설정된 비밀키를 이용하여
H에 대한 디지털 서명(G)를 계산
S203
화상 파일 생성부에서
G와 카메라 ID를 첨부
S204
종료

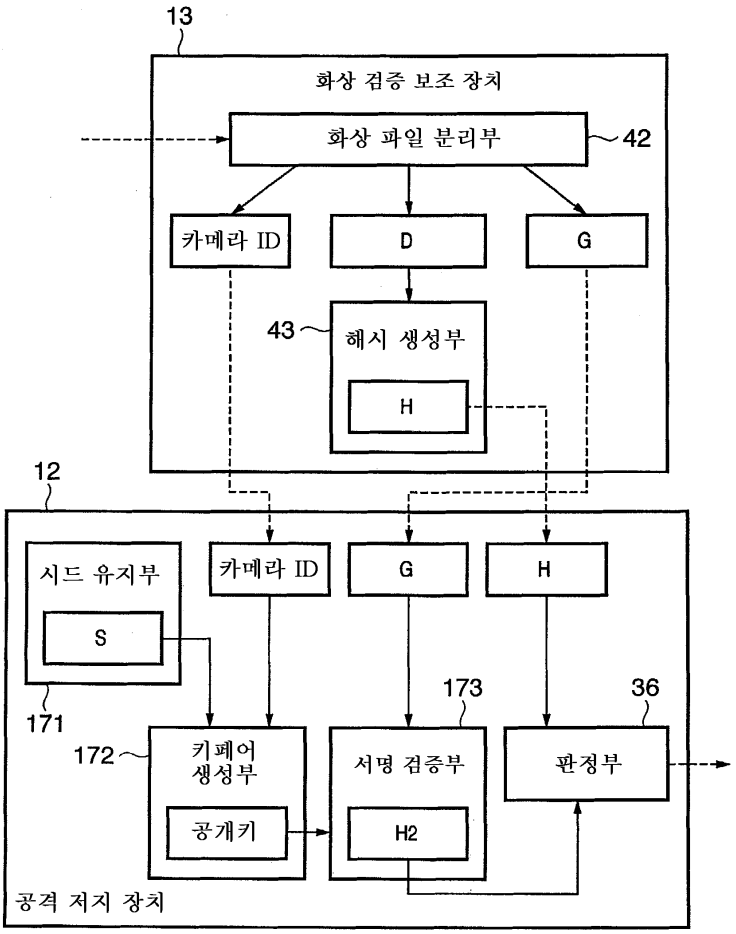
도면21


화상 검증 보조 장치
시작
화상 파일 판독
S211
화상(D), 디지털 서명(G), 및 카메라 ID를 분리
S212
화상(D)으로부터 해시값(H) 생성
S213
H, G, 및 카메라 ID를 IC카드에 송신
S214
판정 결과를 표시
S215
종료
공격 저지 장치(IC 카드)
시작
카메라 ID 및 시드(S)로부터 S*ID를 계산
S221
S*ID로부터 공개키를 생성
S222
공개키를 사용하여 디지털 서명(G)을 복호하여 H2 생성
S223
H=H2?
S224
아니오
예
위변조 존재
S226
위변조 없음
S225
판정 결과 송신
S227
종료

도면22


키 생성 장치
14
182
시드 관리부
S
181
키 페어 생성부
비밀키
카메라 ID
11
화상 생성 장치
키 유지부
21
비밀키
카메라 ID
화상 데이터
D
161
27
서명 생성부
G
해시 생성부
H
26
221
화상 파일 생성부
카메라 ID
G
D

도면23


13
화상 검증 보조 장치
화상 파일 분리부
42
카메라 ID
D
G
43
해시 생성부
H
12
시드 유지부
S
171
카메라 ID
G
H
173
36
172
키페어 생성부
공개키
서명 검증부
H2
판정부
공격 저지 장치