(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년10월12일
(11) 등록번호 10-0921512
(24) 등록일자 2009년10월06일

(51) Int. Cl.
G06T 1/00 (2006.01) *H04N 1/40* (2006.01)
(21) 출원번호 10-2007-7020652
(22) 출원일자 2006년01월25일
심사청구일자 2007년09월13일
(85) 번역문제출일자 2007년09월10일
(65) 공개번호 10-2007-0102747
(43) 공개일자 2007년10월19일
(86) 국제출원번호 PCT/JP2006/301603
(87) 국제공개번호 WO 2006/085453
국제공개일자 2006년08월17일
(30) 우선권주장
JP-P-2005-00033016 2005년02월09일 일본(JP)
(56) 선행기술조사문헌
KR1019980041902 A*
KR1020030012487 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
캐논 가부시끼가이샤
일본 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
하야시 주니치
일본국 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고 캐논가부시끼가이샤 나이
(74) 대리인
권태복, 이종근

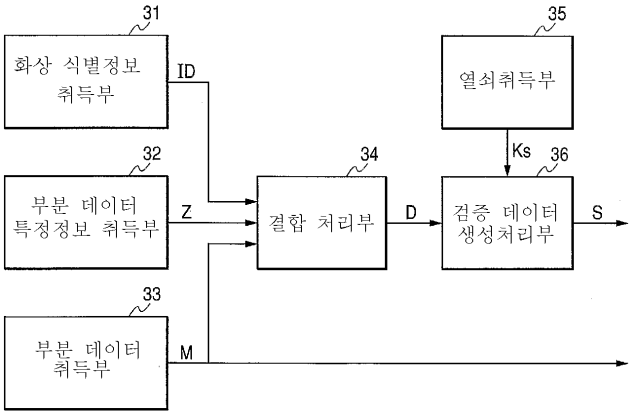
전체 청구항 수 : 총 14 항 심사관 : 김성우

(54) 정보처리방법 및 장치, 및 컴퓨터 판독가능한 기억매체

(57) 요 약

부분 데이터 취득부는 디지털 데이터에 포함되는 부분 데이터를 취득하고, 부분 데이터 특정 정보 취득부는 부분 데이터의 특정 정보를 취득하고, 결합부는 부분 데이터와 특정 정보를 결합하고, 검증 데이터 생성부는 검증 데이터를 생성한다. 이와 같이, 화상 데이터중의 영역 데이터가 변경된 것인가 아닌가를 검증하는 것이 가능하다. 아울러, 상기 영역 데이터가 원화상 데이터와는 다른 화상 데이터중의 영역 데이터인 것을 검증 가능, 및/또는 상기 영역 데이터가 원화상 데이터에 포함된 다른 영역 데이터인 것을 또 검증 가능하게 하는 것이다.

대 표 도 - 도4



특허청구의 범위

청구항 1

디지털 데이터의 부분적인 완전성을 검증하기 위한 검증 데이터를 생성하는 정보처리방법으로서,

상기 디지털 데이터를 특정하는 디지털 데이터 식별정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보를 취득하는 제1취득 공정과,

상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득 공정과,

상기 제1취득 공정에서 취득한 상기 디지털 데이터 식별 정보와 상기 부분 데이터 위치 정보와, 상기 제2취득 공정에서 취득한 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성 공정과,

열쇠정보를 취득하는 열쇠정보 취득 공정과,

상기 열쇠정보 취득 공정에 의해 취득한 열쇠정보를 이용해서, 상기 결합 데이터 생성 공정에서 생성된 결합 데이터의 검증 데이터를 생성하는 검증 데이터 생성공정을 포함한 것을 특징으로 하는 정보처리방법.

청구항 2

제 1 항에 있어서,

상기 디지털 데이터는 화상 데이터이며,

상기 부분 데이터 특정 정보는, 상기 화상 데이터에 포함되는 영역, 해상도, 화질, 성분 또는, 이것들의 조합을 특정하는 정보인 것을 특징으로 하는 정보처리방법.

청구항 3

제 1 항에 있어서,

상기 디지털 데이터는 복수의 요소 내용으로 구성된 문서 데이터이며,

상기 부분 데이터 특정 정보는, 상기 문서 데이터에 포함되는 요소 내용을 특정하는 정보이고,

상기 부분 데이터는, 상기 문서 데이터에 포함되는 요소 내용인 것을 특징으로 하는 정보처리방법.

청구항 4

제 1 항에 있어서,

상기 디지털 데이터는 데이타베이스 정보이며,

상기 부분 데이터 특정 정보는, 상기 데이타베이스 정보에 포함되는 레코드를 특정하는 정보이고,

상기 부분 데이터는, 상기 데이타베이스 정보에 포함되는 레코드인 것을 특징으로 하는 정보처리방법.

청구항 5

디지털 데이터를 특정하는 디지털 데이터 식별 정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터로부터 생성된 검증 데이터를 이용해서, 디지털 데이터의 부분적인 완전성을 검증하는 정보처리방법으로서,

상기 검증 데이터와 열쇠정보로부터 복호 데이터를 취득하는 제1취득 공정과,

상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득 공정과,

상기 제2취득 공정에 의해 취득된 상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성 공정과,

상기 제1취득 공정에서 취득한 복호 데이터와, 상기 결합 데이터 생성 공정에서 생성된 결합 데이터를

이용해서, 상기 부분 데이터가 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터인지를 검증하는 검증 공정을 포함한 것을 특징으로 하는 정보처리방법.

청구항 6

제 5 항에 있어서,

상기 디지털 데이터는 화상 데이터이며,

상기 부분 데이터 특정 정보는, 상기 화상 데이터에 포함되는 영역, 해상도, 화질, 성분 또는, 이것들의 조합을 특정하는 정보인 것을 특징으로 하는 정보처리방법.

청구항 7

디지털 데이터의 부분적인 완전성을 검증하기 위한 검증 데이터를 생성하는 정보처리장치로서,

상기 디지털 데이터를 특정하는 디지털 데이터 식별정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보를 취득하는 제1취득부와,

상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득부와,

상기 제1취득부에서 취득한 상기 디지털 데이터 식별 정보와 상기 부분 데이터 위치 정보와, 상기 제2취득부에서 취득한 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성부와,

열쇠정보를 취득하는 열쇠정보 취득부와,

상기 열쇠정보 취득부에 의해 취득한 열쇠정보를 이용해서, 상기 결합 데이터 생성부에서 생성된 결합 데이터의 검증 데이터를 생성하는 검증 데이터 생성부를 포함한 것을 특징으로 하는 정보처리장치.

청구항 8

제 7 항에 있어서,

상기 디지털 데이터는 화상 데이터이며,

상기 부분 데이터 특정 정보는, 상기 화상 데이터에 포함되는 영역, 해상도, 화질, 성분 또는, 이것들의 조합을 특정하는 정보인 것을 특징으로 하는 정보처리장치.

청구항 9

제 7 항에 있어서,

상기 디지털 데이터는 복수의 요소 내용으로 구성된 문서 데이터이며,

상기 부분 데이터 특정 정보는, 상기 문서 데이터에 포함되는 요소 내용을 특정하는 정보이고,

상기 부분 데이터는, 상기 문서 데이터에 포함되는 요소 내용인 것을 특징으로 하는 정보처리장치.

청구항 10

제 7 항에 있어서,

상기 디지털 데이터는 데이타베이스 정보이며,

상기 부분 데이터 특정 정보는, 상기 데이타베이스 정보에 포함되는 레코드를 특정하는 정보이고,

상기 부분 데이터는, 상기 데이타베이스 정보에 포함되는 레코드인 것을 특징으로 하는 정보처리장치.

청구항 11

디지털 데이터를 특정하는 디지털 데이터 식별 정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터로부터 생성된 검증 데이터를 이용해서, 디지털 데이터의 부분적인 완전성을 검증하는 정보처리장치로서,

상기 검증 데이터와 열쇠정보로부터 복호 데이터를 취득하는 제1취득부와,

상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득부와,

상기 제2취득부에 의해 취득된 상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성부와,

상기 제1취득부에서 취득한 복호 데이터와, 상기 결합 데이터 생성부에서 생성된 결합 데이터를 이용해서, 상기 부분 데이터가 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터인지를 검증하는 검증부를 포함한 것을 특징으로 하는 정보처리장치.

청구항 12

제 11 항에 있어서,

상기 디지털 데이터는 화상 데이터이며,

상기 부분 데이터 특정 정보는, 상기 화상 데이터에 포함되는 영역, 해상도, 화질, 성분 또는, 이것들의 조합을 특정하는 정보인 것을 특징으로 하는 정보처리장치.

청구항 13

삭제

청구항 14

디지털 데이터의 부분적인 완전성을 검증하기 위한 검증 데이터를 생성하는 정보처리방법으로서,

상기 디지털 데이터를 특정하는 디지털 데이터 식별정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보를 취득하는 제1취득 공정과,

상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득 공정과,

상기 제1취득 공정에서 취득한 상기 디지털 데이터 식별 정보와 상기 부분 데이터 위치 정보와, 상기 제2취득 공정에서 취득한 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성 공정과,

열쇠정보를 취득하는 열쇠정보 취득 공정과,

상기 열쇠정보 취득 공정에 의해 취득한 열쇠정보를 이용해서, 상기 결합 데이터 생성 공정에서 생성된 결합 데이터의 검증 데이터를 생성하는 검증 데이터 생성공정을 포함한 정보처리방법을 실행하기 위한 컴퓨터 프로그램을 기억한 것을 특징으로 하는 컴퓨터 판독 가능한 기억매체.

청구항 15

삭제

청구항 16

디지털 데이터를 특정하는 디지털 데이터 식별 정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터로부터 생성된 검증 데이터를 이용해서, 디지털 데이터의 부분적인 완전성을 검증하는 정보처리방법으로서,

상기 검증 데이터와 열쇠정보로부터 복호 데이터를 취득하는 제1취득 공정과,

상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득 공정과,

상기 제2취득 공정에 의해 취득된 상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성 공정과,

상기 제1취득 공정에서 취득한 복호 데이터와, 상기 결합 데이터 생성 공정에서 생성된 결합 데이터를

이용해서, 상기 부분 데이터가 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터인지를 검증하는 검증 공정을 포함한 정보처리방법을 실행하기 위한 컴퓨터 프로그램을 기억한 것을 특징으로 하는 컴퓨터 판독 가능한 기억매체.

명 세 서

기 술 분 야

<1> 본 발명은 디지털 데이터의 검증 또는 인증 또는 그 검증 데이터를 생성하기 위한 정보처리방법 및 장치와, 그 정보처리방법을 실행하기 위한 컴퓨터 프로그램과, 그 컴퓨터 프로그램을 기억하는 컴퓨터 판독 가능한 기억매체에 관한 것이다.

배 경 기 술

<2> 종래, (화상 데이터의 전체가 아닌) 부분적인 영역 데이터가 변경된 것인가 아닌가를 검증하는 것을 목적으로 하는 서명 방법이 미국특허번호 5,898,779에 제안되어 있었다. 보다 구체적으로, 미국특허번호 5,898,779에 제안되어 있는 디지털 화상에 대한 서명 방법은, 도17에 나타나 있는 바와 같이, 우선, 관련 화상의 ROI(region of interest)를 선택하고(스텝S131), 선택한 ROI의 해쉬값(즉, 메시지 다이제스트)을 산출하며(스텝S132), 산출한 해쉬값을 비밀열쇠로 암호화함으로써 디지털 서명을 생성하고(스텝S133), 그 생성된 디지털 서명을 관련 화상에 첨부하는(스텝S134) 방법이다.

<3> 이와 같이, 종래의 기술에 의하면, 원화상 데이터중의 영역 데이터가 변경된 것인가 아닌가를 검증하는 것은 가능했다. 그러나, 종래의 기술에서는, 영역 데이터와 원화상 데이터의 관계가 옳은지를 검증하는 것은 곤란했다. 예를 들면, 상기 영역 데이터가 원화상 데이터에 있는 부분 화상 데이터인지 검증하는 것이 곤란하고, 또한 부분 화상 데이터가 원화상 데이터중의 옳은 위치의 영역 데이터인 것인지 검증하는 것이 곤란하다. 즉, 본래의 원화상 데이터와는 다른 원화상 데이터에, 디지털 서명을 가지는 부분 화상 데이터를 부가하는 경우에도, 상기 변경을 검출할 수는 없었다. 또한, 부분 화상 데이터를 본래의 원화상 데이터중의 다른 영역 데이터로 잘못 교체한 경우에도, 관련된 다른 영역 데이터의 디지털 서명이 존재하면 그러한 변경을 검출할 수는 없었다.

<4> (발명의 개시)

<5> 본 발명은, 이러한 종래의 문제점을 감안하여 이루어진 것으로서, 화상 데이터중의 영역 데이터가 변경되어 있는 것인가 아닌가를 검증하는 것에 더하여, 상기 영역 데이터가 본래의 원화상 데이터와는 다른 원화상 데이터중의 영역 데이터인 것을 검증 가능, 및/또는, 상기 영역 데이터가 본래의 원화상 데이터중의 다른 영역 데이터인 것을 검증 가능하게 하는 기술을 제공하는 것을 목적으로 한다.

<6> 상기 종래의 문제점을 해결하기 위해서, 본 발명에 따른 정보처리방법은, 디지털 데이터의 부분적인 완전성을 검증하기 위한 검증 데이터를 생성하는 정보처리방법으로서,

상기 디지털 데이터를 특정하는 디지털 데이터 식별정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보를 취득하는 제1취득 공정과,

상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득 공정과,

상기 제1취득 공정에서 취득한 상기 디지털 데이터 식별 정보와 상기 부분 데이터 위치 정보와, 상기 제2취득 공정에서 취득한 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성 공정과,

열쇠정보를 취득하는 열쇠정보 취득 공정과,

상기 열쇠정보 취득 공정에 의해 취득한 열쇠정보를 이용해서, 상기 결합 데이터 생성 공정에서 생성된 결합 데이터의 검증 데이터를 생성하는 검증 데이터 생성공정을 포함하는 것을 특징으로 한다.

<7> 삭제

<8> 삭제

<9> 삭제

<10> 또한, 상기 종래의 문제점을 해결하기 위해서, 본 발명에 따른 정보처리 방법은, 디지털 데이터를 특정하는 디지털 데이터 식별 정보와, 상기 디지털 데이터 중에 포함되는 부분 데이터의 디지털 데이터에서의 위치를 특정하는 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터로부터 생성된 검증 데이터를 이용해서, 디지털 데이터의 부분적인 완전성을 검증하는 정보처리방법으로서,

상기 검증 데이터와 열쇠정보로부터 복호 데이터를 취득하는 제1취득 공정과,

상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터를 취득하는 제2취득 공정과,

상기 제2취득 공정에 의해 취득된 상기 디지털 데이터 식별 정보와, 상기 부분 데이터 위치 정보와, 상기 부분 데이터를 포함하는 결합 데이터를 생성하는 결합 데이터 생성 공정과,

상기 제1취득 공정에서 취득한 복호 데이터와, 상기 결합 데이터 생성 공정에서 생성된 결합 데이터를 이용해서, 상기 부분 데이터가 상기 디지털 데이터 식별 정보에 대응하는 디지털 데이터 중, 상기 부분 데이터 위치 정보에 대응하는 부분 데이터인지를 검증하는 검증 공정을 포함한 것을 특징으로 한다.

<11> 삭제

<12> 삭제

<13> 삭제

<14> 삭제

<15> 삭제

<16> 본 발명의 다른 목적, 특징 및 이점은, 첨부도면을 참조한 다음의 상세한 설명으로부터 명백해질 것이다.

도면의 간단한 설명

<17> 도1은 본 발명의 실시예에 있어서의 시스템의 전체 구성을 나타내는 도면,

<18> 도2는 실시예에 있어서의 화상재생 클라이언트에 있어서 적용가능한 GUI(graphical user interface)의 예를 나타내는 도면,

<19> 도3은 실시예에 있어서의 호스트 컴퓨터를 나타내는 도면,

<20> 도4는 실시예에 있어서의 검증 데이터 생성 처리부의 구성을 나타내는 블록도,

<21> 도5는 실시예에 있어서의 부분 데이터 특정 정보를 설명하는 도면,

<22> 도6은 실시예에 있어서의 결합 데이터를 설명하는 도면,

<23> 도7은 실시예에 있어서의 검증 데이터 생성 처리의 흐름도,

<24> 도8은 실시예에 있어서의 검증 처리부의 구성을 설명하는 블록도,

<25> 도9는 실시예에 있어서의 검증 처리의 흐름도.

<26> 도10은 종래기술에 있어서의 디지털 서명 생성 처리를 설명하는 도면,

<27> 도11은 종래기술에 있어서의 검증 결과를 설명하는 도면,

<28> 도12는 실시예에 있어서의 검증 결과를 설명하는 도면,

<29> 도13은 실시예에 있어서의 부분 데이터 특정 정보 취득부의 구성을 나타내는 블록도,

<30> 도14는 실시예에 있어서의 결합 데이터를 설명하는 도면,

<31> 도15는 실시예에 있어서의 문서 데이터를 나타내는 도면,

<32> 도16은 실시예에 있어서의 데이타베이스 정보를 설명하는 도면,

<33> 도17은 종래기술에 있어서의 서명 처리의 흐름도다.

<34> [발명을 실시하기 위한 최선의 형태]

<35> 이후, 본 발명의 바람직한 실시예들을 첨부된 도면을 참조하여 설명하겠다.

<36> <전체 구성의 설명>

<37> 우선, 본 실시예에 있어서의 시스템 개요 예를 도1에 나타낸다. 여기서, 본 실시예에 있어서의 시스템은, 화상재생 클라이언트(11), 화상 전송 서버(12), 화상DB(database;13), 및 네트워크(14)로 구성된다.

<38> 도 1에서, 화상재생 클라이언트(11)는, 화상 전송 서버(12)에 대하여 원하는 화상 데이터의 취득 요구를 송신하고, 화상 전송 서버(12)로부터 네트워크(14)를 경유하여 전송된 화상 데이터를 재생한다. 또한, 본 실시예에 있어서는, 화상 데이터에 더하여, 해당 화상 데이터에 대응하는 검증 데이터를 수신하고, 그 수신된 화상 데이터가 변경되어 있는가 아닌가를 검증한다.

<39> 화상 전송 서버(12)는, 화상재생 클라이언트(11)로부터 수신한 화상 데이터의 취득 요구에 응답하여, 화상DB(13)에 기억된 화상 데이터를 송신한다. 본 실시예에 있어서는, 화상 전송 서버(12)는, 화상 데이터에 더하여, 해당 화상 데이터가 변경되어 있는 것인가 아닌가를 화상재생 클라이언트(11)에서 검증가능한 검증 데이터를 생성하여, 화상재생 클라이언트(11)에 송신한다.

<40> 화상재생 클라이언트(11) 및 화상 전송서버(12)는 인터넷 등의 네트워크(14)를 통해 서로에 상호 접속되어 있어서, 각종 데이터는 화상재생 클라이언트(11)와 화상 전송서버(12)간에 교환가능하다. 여기서, 주목해야 하는 것은, 화상재생 클라이언트(11) 및 화상 전송 서버(12)가 일반적인 퍼스널 컴퓨터 등의 범용 장치이어도 된다는 것이다. 여하튼, 상기 시스템에서 실행되는 처리의 흐름을 이후 간단하게 설명하면 다음과 같다.

<41> 상기 시스템에서 화상 열람 사용자는, 먼저 화상재생 클라이언트(11)를 이용하여, 원하는 화상 데이터를 화상 전송 서버(12)에 요구한다. 이 때에, 사용자는, 화상 데이터 전체가 아닌, 즉 부분적인 화상 데이터를 지정하고, 요구하는 것이 가능하다(도1에 있어서의 "부분 데이터 요구"(1)).

<42> 화상 전송 서버(12)는, 화상재생 클라이언트(11)로부터 요구된 부분 화상 데이터를 화상DB(13)로부터 취득해(도1에 있어서의 "부분 데이터 취득"(2)), 그 취득된 부분 화상 데이터에 대응하는 검증 데이터를 생성한다(도1에 있어서의 "검증 데이터 생성 처리"(3)). 그리고, 취득한 부분 화상 데이터, 및 생성한 검증 데이터를 화상 재생 클라이언트(11)에 전송한다(도1에 있어서의 "부분 데이터 및 검증 데이터 전송"(4)).

<43> 이어서, 화상재생 클라이언트(11)는, 부분 화상 데이터 및 검증 데이터를 수신하고, 해당 검증 데이터를 이용하여, 수신된 부분 화상 데이터가 옳은 부분 화상 데이터인가 아닌가를 검증하여, 그 검증 결과를 표시한다(도1에서 "부분 데이터의 재생 및 검증"(5)).

<44> 이상이, 본 실시예에 있어서의 시스템의 개요 예이다.

<45> 여기에서, 이상에서 설명한 것 같은 화상 전송 시스템에 있어서, 이후, 부분 화상 데이터 요구, 화상 데이터 검증 처리, 및 화상 데이터 재생 처리의 조작 화면 예(윈도우)에 대해서 도2를 참조하여 설명한다.

<46> 도2에 있어서, 윈도우(21)의 상부에는, 원하는 화상 데이터의 "화상ID"를 지정하는데 사용되는 섹션(22)을 갖는다. 섹션(22) 상에, 사용자는 도면에 나타내지 않은 키보드 등에 의해 화상ID를 직접 입력함에 의해 화상 ID를 지정한다. 섹션(22)의 오른쪽에는, 섹션(22)에 의해 지정된 화상ID의 섬네일을 취득하고, 표시하기

위한 버튼(23)을 가진다.

<47> 도면에 나타내지 않은 마우스 등에 의해 버튼(23)을 클릭함에 의해, 섹션(22)을 통해 지정된 화상ID에 대응하는 화상 데이터의 섬네일이 섬네일 뷰어(24)에 표시된다.

<48> 섬네일이 표시된 후, 사용자는 마우스 등을 이용해서 섬네일중의 원하는 영역(25)을 자유롭게 선택할 수 있다. 섬네일 뷰어(24)의 하부에는, 상기 지정된 원하는 영역(25)의 상세한 정보를 표시하는데 사용된 버튼(26)을 가진다. 원하는 영역(25)을 선택한 상태에서, 마우스 등에 의해 사용자가 버튼(26)을 클릭함에 의해, 영역(25)에서 지정한 부분 화상 데이터의 상세가 화상 뷰어(27)에 표시된다. 또한, 화상 뷰어(27)에 표시된 부분 화상 데이터가 옳은 데이터인가 아닌가를 나타내는 검증 처리 결과가, 섹션(28)에 표시된다.

<49> 즉, 버튼(26)을 클릭함에 의해, 도1에 있어서의 "부분 데이터 요구"(1), "부분 데이터 취득"(2), "검증 데이터 생성"(3), "부분 데이터 및 검증 데이터 전송"(4), 및 "부분 데이터 재생 및 검증"(5)의 일련의 처리가 자동적으로 실행된다고 생각하면 이해하기 쉽다.

<50> 이때, 도2에 나타낸 윈도우는 본 발명에 적용 가능한 일 예를 나타내는 것이며, 즉, 본 발명은 이것에 한정되지 않는 것이 명확하다.

<51> 다음에, 도3을 참조하여, 본 발명의 실시예에 적용 가능한 호스트 컴퓨터에 관하여 설명한다. 즉, 도3은 화상재생 클라이언트 또는 화상 전송서버로서 기능할 수 있는 호스트 컴퓨터의 기본구성을 나타냄과 동시에, 그 주변기기와의 관계를 나타낸다. 도3에 있어서, 호스트 컴퓨터(121)는, 예를 들면, 일반적으로 보급되고 있는 퍼스널 컴퓨터이다. 호스트 컴퓨터(121)는, HD(하드디스크)(126), CD(콤팩트디스크)(127), FD(플로피디스크)(128), 및 DVD(디지털 다기능 디스크)(129) 등에 화상 데이터를 축적하고, 또한, 그 HD(126), CD(127), FD(128), 및 DVD(129)에 축적되어 있는 화상 데이터를 모니터(122)에 표시하는 것이 가능하다. 또한, 호스트 컴퓨터(121)는, NIC(네트워크 인터페이스 카드)(1210)등을 사용하여, 이것들의 화상 데이터를 인터넷 등을 통해 전송할 수 있다. 한편, 유저로부터의 각종 지시 등은, 마우스(1213) 및 키보드(1214)를 통해 입력한다. 호스트 컴퓨터(121)의 내부에서는, 버스(1216)에 의해 후술하는 각 블록이 접속되어, 여러 가지의 데이터 교환이 가능하다.

<52> 도3에서, 도면부호 122는, 호스트 컴퓨터(121)에서 다양한 정보를 표시할 수 있는 모니터이다.

<53> 도면부호 123은, 호스트 컴퓨터(121)안의 각 부의 동작을 제어하고, 또한 RAM(랜덤 액세스 메모리)(125)에 로드된 프로그램을 실행할 수 있는 CPU(중앙처리장치)이다. 도면부호 124는, BIOS(Basic Input/Output System) 및 부트 프로그램을 기억하고 있는 ROM(판독전용 메모리)이다. 도면부호 125는 CPU(123)에서 처리를 행하기 위해서 일시적으로 프로그램이나 처리 대상의 화상 데이터를 받아들여 두는 RAM이다. 게다가, 이 RAM(125)에 OS나 CPU(123)가 후술하는 각종 처리를 행하기 위한 프로그램이 로드되게 된다.

<54> 도면부호 126은, RAM등에 전송되는 OS 및 프로그램을 기억한 HD이다. 또한, HD(126)는, 장치가 동작중에 화상 데이터를 격납하고 판독하는데 사용된다. CD(127)는 외부 기억매체의 하나인 CD-ROM(CD-R)에 대해 각종 데이터를 판독하고 기록할 수 있는 CD-ROM드라이브다. 이와 관련하여, 주목해야 하는 것은, 이후 CD(127)를 CD-ROM 드라이브(127)라고도 한다는 것이다.

<55> FD(128)은, CD-ROM드라이브(127)와 마찬가지로, FD드라이브(128)인 FD(128)는, 플로피™디스크에 대해 판독 및 기록을 할 수 있다. 이와 관련하여, 주목해야 하는 것은, 이후, FD(128)도 FD드라이브(128)라고 한다는 것이다. DVD(129)는, CD-ROM드라이브(127)와 마찬가지로, DVD-ROM으로부터 데이터를 판독할 수 있고, DVD-RAM에 데이터를 기록할 수 있는 DVD-ROM(DVD-RAM)드라이브(128)이다. 이와 관련하여, 주목해야 하는 것은, 이후, DVD(129)가 DVD-ROM 드라이브 또는 DVD-RAM 드라이브라고도 한다는 것이다. 한편, CD-ROM, FD, DVD-ROM 등에 화상처리용의 프로그램이 기억되어 있는 경우에는, 이것들 프로그램을 HD(126)에 인스톨하고, 필요에 따라 RAM(125)에 전송되게 되어 있다.

<56> 도면부호 1211은, RAM(125), HD(126), CD-ROM(127), FD(128), DVD(129) 등에 기억되어 있는 화상 데이터를, 인터넷 등의 네트워크에 접속하는 NIC(1210)에 호스트 컴퓨터(121)를 접속하는 I/F(인터페이스)이다. 그래서, I/F(1211)를 거쳐서 호스트 컴퓨터(121)는, 인터넷에 및 인터넷으로부터 데이터를 전송하거나 인터넷으로 데이터를 수신할 수 있다.

<57> 도면부호 1215는, 호스트 컴퓨터(121)에 마우스(1213)와 키보드(1214)를 접속하기 위한 I/F이다. 이와 같이, I/F(1215)를 거쳐서 마우스(1213)와 키보드(1214)로부터 입력된 각종의 지시와 데이터는 CPU(123)에 전송

된다.

<58> <검증 데이터 생성 처리>

<59> 다음에, 본 발명의 실시예에 적용 가능한 검증 데이터 생성 처리부, 및 그 검증 데이터 생성방법에 대해서 도4를 참조하여 설명한다.

<60> 즉, 도4는, 본 실시예에 있어서의 검증 데이터 생성 처리 기능, 및 검증 데이터 생성방법을 설명하는 도면이다. 도4에 있어서, 도면부호 31은 화상 식별정보 취득부, 도면부호 32는 부분 데이터 특정 정보취득부, 도면부호 33은 부분 데이터 취득부, 도면부호 34는 결합 처리부, 도면부호 35는 열쇠 취득부, 도면부호 36은 검증 데이터 생성 처리부다.

<61> 여기서, 주목해야 하는 것은, 도4에 나타내는 검증 데이터 생성 처리 기능이, 도 1에 도시된 화상 전송 서버(12)에 탑재되는 일 기능이라는 것이다.

<62> 여하튼, 우선, 화상 식별정보 취득부(31) 및 부분 데이터 특정 정보 취득부(32)에 관하여 설명한다. 즉, 화상식별 정보 취득부(31)는, 화상재생 클라이언트(11)로부터 요구된 화상식별 정보ID를 취득하여 출력하고, 또한 부분 데이터 특정 정보 취득부(32)는, 부분 데이터 특정 정보Z를 그 화상재생 클라이언트(11)로부터 취득하여 출력한다.

<63> 여기에서, 화상식별 정보ID란 화상 데이터를 특정하기 위한 정보이고, 부분 데이터 특정 정보Z란 상기 화상 데이터중의 부분적인 데이터를 특정하기 위한 정보다.

<64> 본 실시예에서는 화상식별 정보ID로서, 예로서, 화상 데이터의 파일명을 사용한다. 그러나, 본 발명은 이것에 한정되지 않는다. 즉, 화상 데이터의 위치를 나타내는 URL(Uniform Resource Locator), 화상 데이터를 유일하게 식별하는 URI, 화상 데이터의 해쉬 값 등을 화상식별 정보ID로서 적응 가능한 것은 명확하다.

<65> 또한, 본 실시예에서는 부분 데이터로서, 도2에 있어서의 영역(25)에서 나타낸 바와 같은 화상 데이터중의 부분적인 사각형 영역을 사용한다. 부분 데이터로서 사각형 영역을 사용하는 경우, 부분 데이터 특정 정보Z로서, 사각형 영역의 좌측위의 좌표정보(x1, y1), 및 우측하의 좌표정보(x2, y2)을 이용할 수 있다.

<66> 아울러, 본 발명은 이것에 한정되지 않는다. 즉, 사각형 영역의 이외에도, 영역을 특정 가능한 여러 가지의 부분 데이터 특정 정보가 적용 가능한 것은 명확하다.

<67> 보다 구체적으로는, 임의 형상 영역을 부분 데이터로서 지정할 경우, 부분 데이터 특정 정보Z로서는, 부분 데이터로서 지정된 위치에 대응하는 화소를 "0", 및 부분 데이터로서 지정되지 않는 위치에 대응하는 화소를 "1"이라고 한 2진 화상 데이터를 이용할 수 있다. 예를 들면, 도5에 나타나 있는 바와 같이, 하트의 외부(171)가 "0", 하트의 내부(172)가 "1"인 2진 화상을 부분 데이터 특정 정보Z로서 적용 가능하다.

<68> 또한, 화상 데이터가 각각 겹치지 않는 복수의 타일로 분할되어 있는 경우, 부분 데이터 특정 정보Z로서, 타일을 식별하는 타일 인덱스를 이용할 수 있다.

<69> 어쨋튼, 부분 데이터를 유일하게 특정가능한 여러 가지의 정보를 부분 데이터 특정 정보로서 적용 가능하다.

<70> 다음에, 부분 데이터 취득부(33)에 관하여 설명한다. 부분 데이터 취득부(33)는, 전술한 화상식별 정보 취득부(31) 및 부분 데이터 특정 정보 취득부(32)에 의해 취득된 화상식별 정보ID, 및 부분 데이터 특정 정보Z를 사용하여, ID 및 Z에 대응하는 부분 데이터M을 화상DB(13)로부터 취득하여, 출력한다.

<71> 전술한 바와 같이, 본 실시예에 있어서는, 부분 데이터M으로서는, 화상 데이터중의 부분적인 사각형 영역의 데이터가 출력된다.

<72> 다음에, 결합 처리부(34)에 관하여 설명한다. 결합 처리부(34)에서는, 전단의 화상식별 정보 취득부(31), 부분 데이터 특정 정보 취득부(32), 및 부분 데이터 취득부(33)로부터 출력된, 화상식별 정보ID, 부분 데이터 특정 정보Z, 및 부분 데이터M이 입력되어, 이것들을 결합하고, 결합 데이터D가 출력된다.

<73> 여기에서, 본 실시예에 있어서의 결합 데이터D에 대해서 도6을 사용하여 설명한다. 도6에 나타나 있는 바와 같이, 본 실시예에서는, 화상식별 정보ID, 부분 데이터 특정 정보Z 및 부분 데이터M을 소정의 순서로 연결한 정보를 결합 데이터D라고 한다. 여기서, 그 데이터를 연결하는 순서는, 도6의 순서가 아니어도 좋은 것은 말할 필요도 없다.

<74> 다음에, 열쇠취득부(35)에 관하여 설명한다. 즉, 열쇠취득부(35)에서는, 검증 데이터 생성 처리부(36)에 의해 수행되는 검증 데이터 생성 처리 때문에 필요한 열쇠정보Ks가 취득되어, 출력된다.

<75> 부수적으로, 본 실시예에 있어서의 열쇠정보Ks의 상세에 대해서는, 후술한다.

<76> 다음에, 검증 데이터 생성 처리부(36)에 관하여 설명한다. 즉, 검증 데이터 생성 처리부(36)에서는, 전단의 결합 처리부(34)로부터 출력된 결합 데이터D, 및 열쇠취득부(35)로부터 출력된 열쇠정보Ks가 입력되어, 열쇠정보Ks를 이용해서 결합 데이터D에 대응하는 검증 데이터S가 생성되어, 생성된 검증 데이터S가 출력된다.

<77> 본 실시예에서, 검증 데이터 생성 처리는 특별하게 언급하지 않는다. 즉, RSA(Rivest Shamir Adleman) 알고리즘, DSA(digital signature algorithm) 등의 디지털 서명 생성 알고리즘이나, HMAC(hash-based MAC) 생성 알고리즘이나 CMAC(cipher-based MAC) 생성 알고리즘 등의 MAC(message authentication) 생성 알고리즘등 여러 가지의 검증 데이터 생성 처리를 적용가능하다. 또한, 검증 데이터 생성 처리로서, 디지털 서명 생성 알고리즘을 사용할 경우, 상기 열쇠취득부(35)에서 취득되는 열쇠정보Ks는 화상 전송 서버(12)의 비밀열쇠로서 사용된다. 또한, MAC생성 알고리즘을 사용한 경우에는, 열쇠정보Ks는 화상 재생 클라이언트(11) 및 화상 전송 서버(12)로 안전하게 공유하는 공유 열쇠이다.

<78> 또한, 결합 데이터D에 대하여 검증 데이터 생성 처리를 실시하기 전에, MD(Message Digest) 5, SHA(Secure Hash Algorithm)1 등의 해쉬 함수를 결합 데이터D에 적용하여서, 해쉬 함수의 출력값에 대하여 검증 데이터 생성 처리를 적용할 수 있다.

<79> 본 실시예에 있어서의 검증 데이터 생성 처리 및 방법에 관하여 설명했다.

<80> 다음에, 이상에서 설명한 검증 데이터 생성 처리의 흐름을 도7에 도시된 흐름도를 사용하여 설명한다. 즉, 도7은 본 실시예에 적용 가능한 검증 데이터 생성 처리를 설명하는 흐름도이다.

<81> 우선, 스텝S51에서는, 화상식별 정보ID 및 부분 데이터 특정 정보Z를 각각 도4의 화상 식별정보 취득부(31) 및 부분 데이터 특정 정보 취득부(32)에 의해 취득한다. 그리고, 스텝S52에서는, 상기 화상식별 정보ID 및 부분 데이터 특정 정보Z에 대응한 부분 데이터M을 도4의 부분 데이터 취득부(33)에 의해 취득한다. 그 후에 스텝S53에서는, 그 화상식별 정보ID, 부분 데이터 특정 정보Z 및 부분 데이터M을 도4의 결합 처리부(34)에 의해 결합하여, 결합 데이터D를 생성한다. 그 후, 스텝S54에서는, 검증 데이터를 생성하기 위한 열쇠정보Ks를 취득하고, 스텝S55에서는 결합 데이터D의 검증 데이터S를 열쇠정보Ks를 사용해서 생성하고, 검증 데이터 생성 처리를 종료한다.

<82> <검증 처리 및 방법>

<83> 다음에, 본 실시예에 적용 가능한 검증 처리 및 방법에 대해서 도8을 사용하여 설명한다. 도8에 있어서, 도면부호 61은 검증 데이터 취득부, 도면부호 62는 열쇠취득부, 도면부호 63은 검증 데이터 복호부, 도면부호 64는 화상식별 정보 취득부, 도면부호 65는 부분 데이터 특정 정보 취득부, 도면부호 66은 부분 데이터 취득부, 도면부호 67은 결합 처리부, 및 도면부호 68은 비교부다.

<84> 여기서, 도8에 나타낸 검증 처리 기능은, 도1에 도시된 전술한 화상재생 클라이언트(11)에 탑재되는 일 기능이다.

<85> 우선, 검증 데이터 취득부(61)에 관하여 설명한다. 즉, 검증 데이터 취득부(61)에서는, 화상 전송 서버(12)로부터 전송된 검증 데이터S를 취득하여, 출력한다. 부수적으로, 여기에서 취득되는 검증 데이터S는, 도4에 있어서의 검증 데이터 생성 처리부(36)에서 출력된 데이터라고 생각하면 이해하기 쉽다.

<86> 다음에, 열쇠취득부(62)에 관하여 설명한다. 즉, 열쇠취득부(62)는, 검증 데이터 복호부(63)에서 검증 데이터 복호처리를 위해 필요한 열쇠정보Kp를 취득하여 출력한다.

<87> 여기서, 열쇠취득부(62)에 있어서 취득된 열쇠정보Kp는, 실질적으로 도4에 있어서의 열쇠취득부(35)에서 취득된 열쇠정보Ks에 대응하는 정보다. 다시 말해, 열쇠취득부(35)에 있어서 화상 전송 서버(12)의 비밀열쇠가 열쇠정보Ks로서 취득되었을 경우, 열쇠취득부(62)에서는, 열쇠정보Ks로 한 쌍을 이루는 화상 전송 서버(12)의 공개 열쇠를 열쇠정보Kp로서 취득하도록 한다. 한편, 열쇠취득부(35)에 있어서 공유 열쇠가 열쇠정보Ks로서 취득되었을 경우, 열쇠취득부(62)에서는, 열쇠정보Ks와 마찬가지의 값을 열쇠정보Kp로서 취득한다.

<88> 다음에, 검증 데이터 복호부(63)에 관하여 설명한다. 즉, 검증 데이터 복호부(63)에는, 검증 데이터 취득부(61)에서 취득된 검증 데이터S, 및 열쇠취득부(62)에서 취득된 열쇠정보Kp가 입력되고, 열쇠정보Kp을 사용

해서 입력된 검증 데이터S가 복호되어, 검증 데이터 복호부(63)로부터 그 복호된 값D가 출력된다.

<89> 여기서, 검증 데이터 복호부(63)에서 실행되는 검증 데이터 복호처리는, 도4에 있어서의 검증 데이터 생성 처리부(36)에서 실행된 검증 데이터 생성 처리에 대응하는 처리를 적용하도록 한다.

<90> 특히, 검증 데이터로서 MAC 데이터를 이용하고 있는 경우에는, 검증 데이터 복호처리를 실행하는 것이 가능하지 않다. 이 경우, 입력된 검증 데이터S와 같은 값이 복호된 D로서 출력된다.

<91> 다음에, 화상식별 정보 취득부(64) 및 부분 데이터 특정 정보 취득부(65)에 관하여 설명한다. 즉, 화상식별 정보 취득부(64) 및 부분 데이터 특정 정보 취득부(65)는, 각각, 후술하는 부분 데이터 취득부(66)에서 취득되는 부분 데이터에 대응하는 화상 데이터, 및 부분 데이터를 특정하기 위한 정보를 취득하여, 출력한다.

<92> 또한, 도8에서, 화상식별 정보ID 및 부분 데이터 특정 정보Z는, 각각 도4에 있어서의 화상식별 정보 취득부(31), 및 부분 데이터 특정 정보 취득부(32)에 있어서 취득된 화상식별 정보ID, 및 부분 데이터 특정 정보Z와 마찬가지의 정보를 취득하도록 한다. 본 실시예에서는 부분 데이터 요구 처리전에, 미리 도2에 있어서의 섹션(22) 및 영역(25)에 의해 각각 지정된 화상식별 정보와 부분 데이터 특정 정보를 RAM(125)(도3)에 기억해두고, 검증 처리 단계에 있어서, RAM(125)에 기억된 화상식별 정보ID 및 부분 데이터 특정 정보Z를 취득한다.

<93> 이때, 본 발명은 이것에 한정되지 않는다. 즉, 화상 전송 서버(12)로부터 화상재생 클라이언트(11)에, 결합 데이터D(도6)가 전송할 수 있고, 또한, 수신한 결합 데이터D중의 화상식별 정보ID와 부분 데이터 특정 정보Z를, 화상식별 정보 취득부(64) 및 부분 데이터 특정 정보 취득부(65)에서 각각 취득할 수 있다. 이 경우, 부분 데이터를 요구할 때 각각 지정한 화상식별 정보ID 및 부분 데이터 특정 정보Z와, 취득한 화상식별 정보ID 및 부분 데이터 특정 정보Z를 각각 비교하여, 일치하지 않은 경우에는, 수신한 부분 데이터M'은 옳지 않다고 판정하여, 그 처리를 중지하는 것이 가능하다.

<94> 다음에, 부분 데이터 취득부(66)에 관하여 설명한다. 부분 데이터 취득부(66)에서는, 화상 전송 서버(12)로부터 전송된 부분 데이터M'을 취득하여, 출력한다. 또한, 여기에서 취득된 부분 데이터M'은, 도4에 있어서의 부분 데이터 취득부(33)로부터 출력된 데이터라고 생각하면 이해하기 쉽다.

<95> 다음에, 결합 처리부(67)에 관하여 설명한다. 즉, 결합 처리부(67)에서는, 화상식별 정보취득부(64)에서 취득된 화상식별 정보ID, 부분 데이터 특정 정보 취득부(65)에서 취득된 부분 데이터 특정 정보Z 및 부분 데이터 취득부(66)에서 취득된 부분 데이터M'이 입력되어, 이것들을 결합하고, 결합 데이터D'가 출력된다.

<96> 여기에서, 결합 데이터D'는, 전단의 화상식별 정보 취득부(64), 부분 데이터 특정 정보 취득부(65), 및 부분 데이터 취득부(66)로부터 각각 취득된 화상식별 정보ID, 부분 데이터 특정 정보Z, 및 부분 데이터M'을 도4에 있어서의 결합 처리부(34)로 같은 방법으로 결합해서 생성된다.

<97> 부수적으로, 전술한 바와 같이, 검증 데이터 생성 처리부(36)(도4)에 있어서, 해쉬함수가 적용되는 경우에는, 결합 처리부(67)에서 D'를 생성한 후, 검증 데이터 생성 처리부(36)에서 적용한 해쉬함수와 같은 해쉬함수를 D'에 대하여 적용하여, 해쉬 값을 출력하도록 한다. 물론, 그 후에 해쉬 값을 비밀열쇠로 암호화하여, 디지털 서명을 생성하는 것도 가능하다.

<98> 또한, 검증 데이터로서 MAC 데이터를 이용하는 경우에는, 열쇠취득부(62)에서 취득한 Kp을 사용하여, 결합 데이터D(또는, 그 해쉬 값)의 MAC 데이터를 생성하고, 그 생성한 MAC 데이터를 출력한다.

<99> 다음에, 비교부(68)에 관하여 설명한다. 비교부(68)에서는, 전단의 검증 데이터 복호부(63)로부터 출력된 결합 데이터D와 결합처리부(67)로부터 출력된 결합 데이터D'를 비교하여, 검증 결과를 출력한다.

<100> 본 실시예에 있어서는, 결합 데이터 D의 값과 결합 데이터 D'의 값이 일치하는 경우, 부분 데이터M'은 옳은 데이터(검증 성공)라고 판정한다. 한편, 결합 데이터 D의 값과 결합 데이터 D'의 값이 서로 다른 경우, 부분 데이터M'은 옳은 데이터가 아니다(검증 실패)라고 판정한다.

<101> 이상, 본 실시예에 있어서의 검증 처리 및 방법에 관하여 설명했다.

<102> 다음에, 이상에서 설명한 검증 데이터 생성 처리(방법)의 흐름을 도9를 사용하여 설명한다. 즉, 도9는 본 실시예에 적용 가능한 검증 데이터 생성 처리를 설명하는 흐름도다.

<103> 우선, 스텝S71에서는, 도8의 검증 데이터 취득부(61) 및 열쇠취득부(62)에 의해 각각 검증 데이터S 및

열쇠정보Kp를 취득한다. 그리고, 스텝S72에서는, 도8의 검증 데이터 복호부(63)에 의해 상기 검증 데이터S를 상기 열쇠정보Kp을 사용해서 복호하고, 결합 데이터D를 산출한다. 또한, 스텝S73에서는, 도8의 화상 식별정보 취득부(64), 부분 데이터 특정 정보 취득부(65) 및 부분 데이터 취득부(66)에 의해 각각 화상식별 정보ID, 부분 데이터 특정 정보Z 및 부분 데이터M'을 취득한다. 다음에, 스텝S74에서는, 도8의 결합처리부(67)에 의해 화상식별 정보ID, 부분 데이터 특정 정보Z 및 부분 데이터M'을 결합하여, 결합 데이터D'를 생성한다. 그 후에 스텝S75에서는, 결합 데이터D와 D'가 마찬가지의 것인가 아닌가를 판정한다. 마찬가질 경우에는 스텝S76에서는 "부분 데이터M'이 옳은 데이터(검증 성공)"의 메시지를 표시한다. 한편, 마찬가지가 아닐 경우에는 스텝S77에서는 "부분 데이터M'이 옳은 데이터가 아니다(검증 실패)"라고 표시한다.

<104> 이상, 본 실시예에 적용 가능한 검증 데이터 생성 처리(방법), 및 검증 처리(방법)에 관하여 설명했다.

<105> <검증 결과예>

<106> 이후, 이상에서 설명한 검증 데이터 생성 처리 및 검증 처리를 적응했을 경우의 여러 가지의 검증 결과에 대해서, 종래기술과 본 실시예를 비교하면서, 구체적인 예를 사용하여 설명한다.

<107> 우선, 전술한 본 실시예에 있어서의 시스템(도1)에 대하여, 종래의 기술(USP 5, 898, 779)을 적용했을 경우의 예를 설명한다. 이 경우, 서버에 있어서 영역 데이터를 전송할 때에, 전송해야 할 영역 데이터(ROI)에 대하여 디지털 서명을 생성하고, 영역 데이터와 함께 영역 데이터에 대한 디지털 서명을 클라이언트에 전송한다. 그 후에, 클라이언트에서 상기 수신한 영역 데이터를 검증 또는 인증하여서, 그 수신한 영역 데이터가 네트워크의 트랙에서 변경된 것인가 아닌가를 검증하는 것이 가능하다.

<108> 이 구체적인 예를, 도10을 사용하여 설명한다. 도10에 있어서, 도면부호 161은 서버에 기억되어 있는 화상 데이터, 도면부호 162는 클라이언트에 의해 요구된 영역, 도면부호 163은 영역 162을 잘라서 취득한 영역 데이터, 도면부호 164는 그 영역 데이터(163)의 디지털 서명이다.

<109> 클라이언트로부터 서버에 대하여, 화상 데이터(161)에 포함되는 영역(162)의 전송요구가 발생하는 경우에, 서버는, 영역 162을 화상 데이터(161)로부터 잘라서 영역 데이터(163)를 생성함과 동시에, 영역 데이터(163)의 디지털 서명(164)을 생성한다. 그리고, 생성한 영역 데이터(163) 및 그 디지털 서명(164)을 클라이언트에 전송한다. 그래서, 클라이언트는, 수신한 영역 데이터(163)가 네트워크의 트랙에서 변경된 것인가 아닌가를 디지털 서명(164)를 사용하여 검증하는 것이 가능하다.

<110> 어쨋튼, 우선, 종래기술에 의한 검증 결과 예에 대해서, 도11을 사용하여 설명한다. 도11에 있어서, 도면부호 141은 클라이언트에 의해 요구된 화상 데이터 I0001, 도면부호 142는 클라이언트에 의해 요구된 화상 데이터I0001중의 일부의 영역, 도면부호 143은 화상 데이터 I0001과는 다른 화상 데이터I0002, 도면부호 144는 화상 데이터I0001에 있어서 부분영역142와 같은 위치의 영역, 도면부호 149은 화상 데이터I0001중에서 부분영역142와 다른 위치의 영역이다. 여기에서, 화상 데이터I0001 및 화상 데이터I0002는 서버 상에 축적되어 있는 것으로 한다.

<111> 우선, 표 1410에서, 영역142와 그 영역142에 대응하는 디지털 서명을 수신한 경우에(데이터 145), 데이터가 변경되지 않았다(검증 성공)고 판정가능하다. 또한, 영역142가 변경된 데이터와 그 영역142에 대응하는 디지털 서명을 수신한 경우에(데이터 146), 데이터가 변경되었다(검증 실패)고 판정가능하다.

<112> 한편, 비록 영역142가 요구되었지만 상기 영역149와 그 영역149에 대응하는 디지털 서명을 수신했을 경우(데이터 147), 데이터가 변경되지 않았다(검증 성공)고 판정되어버린다. 왜냐하면, 검증처리에서, 수신한 영역149와 그 영역149의 그 디지털 서명이 전혀 변경되지 않기 때문이다. 다시 말해, 이 경우, 영역142 대신에, 영역149가 수신된 것을 검출할 수 없다.

<113> 또한, 비록 화상 데이터(141)중의 영역142가 요구되었지만 영역144와 그 영역144에 대응하는 디지털 서명을 수신하는 경우(데이터 148), 데이터가 변경되지 않았다(검증 성공)고 판정되어버린다. 왜냐하면, 검증처리에서, 수신한 영역 144와 그 영역144의 그 디지털 서명이 전혀 변경되지 않기 때문이다. 다시 말해, 영역142 대신에, 영역144가 수신된 것을 검출할 수 없다.

<114> 이상, 종래기술에 의한, 검증 결과 예의 구체적인 예를 설명한다.

<115> 다음에, 본 실시예에 의한 검증 결과 예에 대해서, 도12를 사용하여 설명한다. 도12에 있어서, 도면부호 81은 화상재생 클라이언트(11)(도1)에 있어서, 섹션(22)(도2)을 사용해서 지정된 화상 데이터 전체(화상식별

정보는 I0001이다), 또한 도면부호 82는 영역25(도2)를 사용해서 지정된 부분 데이터를 나타낸다.

<116> 또한, 도면부호 89는, 화상 데이터I0001에 있어서, 섹션(22)에서 지정된 영역(82)과는 다른 영역을 나타내는 부분 데이터이다. 다시 말해, 도면부호 89는 부분 데이터(82)와 같은 화상식별 정보ID를 갖지만, 그 부분 데이터(82)와 다른 부분 데이터 특정 정보Z'를 갖는다.

<117> 또한 도면부호 84는, 화상 데이터I0001과는 다른 화상 데이터(83)(화상식별 정보는 I0002)중에서, 섹션(22)에서 지정된 영역(82)과 같은 영역(즉, 좌측위의 좌표, 및 우하의 좌표가 영역(82)의 것과 마찬가지다)을 나타내는 부분 데이터다. 다시 말해, 도면부호 84는 부분 데이터 82와 다른 화상식별 정보ID를 갖지만, 그 부분 데이터 82와 마찬가지의 부분 데이터 특정 정보Z를 갖는다.

<118> 표 810은, 화상재생 클라이언트(11)가, 화상 데이터(81)(화상식별 정보ID는 I0001이다.)중의 부분 데이터(부분 데이터 특정 정보는 Z)를 요구한 경우에, 실제로 수신한 부분 데이터와, 각각의 검증 결과를 나타낸다.

<119> 우선, 영역82와 그 영역82에 대응하는 검증 데이터를 수신한 경우에는(데이터 85), 도8에 있어서, 화상식별 정보ID, 부분 데이터 특정 정보Z 및 부분 데이터M'은, 각각, 검증 데이터D(도6)의 화상식별 정보ID, 부분 데이터 특정 정보Z 및 부분 데이터와 마찬가지가 되어서, 결과적으로 D와 D'는 마찬가지가 된다. 결과적으로, 수신한 부분 데이터M'은 옳다(검증 성공)고 판정가능하다.

<120> 다음에, 상기 변경된 화상 데이터인 영역82와 그 영역(82)에 대응하는 검증 데이터를 수신한 경우에(데이터 86), 도8에 있어서, 화상식별 정보ID 및 부분 데이터 특정 정보Z는, 각각, 검증 데이터D(도6)의 화상식별 정보ID 및 부분 데이터 특정 정보Z와 마찬가지이다. 한편, 부분 데이터M'은, 검증 데이터D(도6)의 부분 데이터M과 다른 데이터가 되고, 결과적으로 D와 D'는 다른 값이 된다. 결과적으로, 수신한 부분 데이터M'은 옳지 않다(검증 실패)고 판정된다.

<121> 또한, 비록 영역82를 요구하였지만 영역89와 그 영역89에 대응하는 검증 데이터를 수신하는 경우(데이터 87), 도8에 있어서, 화상식별 정보ID 및 부분 데이터M'은, 검증 데이터D의 화상식별 정보ID 및 부분 데이터M과 각각 마찬가지이다. 한편, 부분 데이터 특정 정보Z는, 검증 데이터D의 부분 데이터 특정 정보Z와는 다르다. 왜냐하면, 이 경우, 검증 데이터D의 부분 데이터 특정 정보는, 영역82를 특정하는 정보가 아니고, 영역89를 특정하는 정보이기 때문이다. 따라서, D와 D'는 다른 값이 된다. 결과적으로, 수신한 부분 데이터M'은 옳지 않다(검증 실패)고 판정된다.

<122> 또한, 비록 영역82을 요구하였지만, 영역84와 그 영역84에 대응하는 검증 데이터를 수신했을 경우(데이터 88), 도8에 있어서, 부분 데이터 특정 정보Z 및 부분 데이터M'은, 각각 검증 데이터D의 부분 데이터 특정 정보Z 및 부분 데이터M과 마찬가지이다. 한편, 화상식별 정보ID는, 검증 데이터중의 화상식별 정보ID와는 다르다. 왜냐하면, 이 경우, 검증 데이터D의 화상식별 정보ID는, 화상 데이터I0001이 아니고, 화상 데이터I0002이기 때문이다. 따라서, D와 D'는 다른 값이 된다. 결과적으로, 수신한 부분 데이터M'은 옳지 않다(검증 실패)고 판정된다.

<123> 이상, 본 실시예에 있어서의 검증 데이터 생성 처리 및 검증 처리에 의한 검증 결과에 관하여 설명했다.

<124> 부수적으로, 실제로 네트워크상에서 어떤 공격이 이루어진 경우에, 이상에서 설명한 데이터(86-88)와 같은 부분 데이터를 수신할 수 있는지를 설명한다.

<125> 데이터 86과 같은 부분 데이터는, 부분 데이터M'이 화상 전송 서버(12)로부터 화상재생 클라이언트(11)에 전송되는 경우에, 네트워크(14)의 트랙에서, 악의가 있는 공격자에 의해 부분 데이터M'이 변경된 경우에 수신될 수 있다.

<126> 한편, 데이터 87 및 88과 같은 부분 데이터는, 어떤 시간에 부분 데이터가 전송되는 경우에, 부분 데이터M'가 악의가 있는 공격자에 의해 잘못 감시된 후, 그 감시된 부분 데이터M'이 화상재생 클라이언트(11)에 전송되었을 경우(소위, 재송 공격)에 수신될 수 있다.

<127> 부수적으로, 본 실시예에서는, 설명을 위해 네트워크 상에 서버 및 클라이언트를 배치한 온라인의 예를 설명했다. 그렇지만, 본 발명은 이것에 한정되지 않는다. 즉, 서버 및 클라이언트를 사용하지 않는 오프라인의 경우에 본 발명을 적용 가능한 것은 명확하다. 오프라인의 경우에는, 도8에 나타낸 검증 방법을 사용해서 검증 가능하게 하기 위해서, 부분 데이터M'을 취득했을 때에, 그 부분 데이터M'에 대응한 화상식별 정보ID, 부분 데이터 식별 정보Z 및 검증 데이터S도 동시에 취득하고, 이들 데이터를 다른 것들과 관련시켜 기억해둔다.

그리고, 검증이 필요한 경우, 도8에 나타낸 방법을 사용해서 검증 처리를 실행해야만 한다.

<128> <변형 예1>

<129> 본 실시예에서는, 부분 데이터 특정 정보 취득부(32)(도4) 및 부분 데이터 특정 정보 취득부(65)(도8)에 있어서 취득된 부분 데이터 특정 정보Z는, 화상 데이터중의 공간적인 일부의 영역을 특정하는 정보이었다. 그렇지만, 본 발명은 이것에 한정되지 않는다. 즉, 화상 데이터중의 부분 데이터를 특정하는 정보이면, 해상도, 화질 및 성분 등을 특정하는 여러 가지의 정보를 본 발명에 적용 가능한 것은 명확하다. 또한, 상기 정보 데이터 중에서 적어도 2개 이상의 정보 데이터를 적절하게 조합해서 취득된 데이터도 본 발명에 적용 가능한 것은 명확하다.

<130> 이후, 그 영역에 더하여, 해상도, 화질 및 성분을 조합해서 부분 데이터 특정 정보Z로서 상기 취득한 조합을 지정한다고 가정한다. 이러한 경우에, 부분 데이터 특정 정보Z의 실제 취득 방법에 대해서, 도13을 사용하여 설명한다.

<131> 도13은, 전술한 부분 데이터 특정 정보 취득부(32)(도4), 및 부분 데이터 특정 정보 취득부(65)(도8) 대신에 적용된 부분 데이터 특정 정보 취득부를 설명하는 블록도이다.

<132> 도13에서, 부분 데이터 특정 정보 취득부(91)는, 영역특정 정보 취득부(92), 해상도 특정 정보 취득부(93), 화질 특정 정보 취득부(94), 성분 특정 정보 취득부(95), 및 결합 처리부(96)로 구성된다.

<133> 우선, 영역특정 정보 취득부(92)에서는, 전술한 부분 데이터 특정 정보 취득부(32)(도4) 및 부분 데이터 특정 정보 취득부(65)(도8)와 마찬가지로, 화상중의 공간적인 영역을 지정하는 정보가 취득되고, 해상도 특정 정보 취득부(93)에서는, 화상의 해상도를 지정하는 정보가 취득된다. 예를 들면, JPEG(Joint Photographic Experts Group) 2000에 있어서, 해상도 특정 정보 취득부(93)는 소정의 해상도 레벨의 식별자를 취득한다. 또한, 화질특정 정보 취득부(94)에서는, 화상의 화질을 지정하는 정보가 취득된다. 예를 들면, JPEG 2000에서, 화질특정 정보 취득부(94)는 소정의 레이어를 취득한다. 또한, 성분 특정 정보 취득부(95)에서는, 화상중의 성분을 지정하는 정보가 취득된다. 예를 들면, JPEG 2000에 있어서, 성분 특정 정보 취득부(95)는, 휘도성분과 소정의 색성분을 취득한다.

<134> 다음에, 결합 처리부(96)를 설명한다. 즉, 결합 처리부(96)에서는, 영역 특정 정보 취득부(92), 해상도 특정 정보 취득부(93), 화질특정 정보 취득부(94) 및 성분 특정 정보 취득부(95)에서 각각 취득된 영역 특정 정보P, 해상도 특정 정보R, 화질 특정 정보L, 및 성분특정 정보C를 결합한다. 그리고, 결합 처리부(96)는, 결합된 데이터를 특정 정보Z로서 출력한다.

<135> 부분 데이터 특정 정보 취득부(91)로부터 취득된 부분 데이터 특정 정보Z는, 결합 처리부(34)(도4), 또는 결합 처리부(67)(도8)에 입력되고, 또한 화상식별 정보ID 및 부분 데이터M(또는, M')과 결합되어, 결합 데이터D(또는, D')가 된다. 결과적으로, 도14에 나타나 있는 바와 같은 결합 데이터D(또는, D')가 취득된다.

<136> 도14에 나타나 있는 바와 같이, 복수의 부분 데이터를 특정하는 정보데이터(P, R, L 및 C)가 지정되었을 경우, 이들 데이터 모두를 결합한다. 그래서, 상기 취득한 결합 데이터를 부분 데이터 특정 정보Z로서 설정해야만 한다.

<137> 이상, 본 변형 예1에서는, 적어도 2개 이상의 정보 데이터를 조합해서 부분 데이터 특정 정보를 나타낼 수 있다. 부수적으로, 적어도 2개 이상의 정보를 조합해서 부분 데이터 특정 정보를 나타낼 수 있는 예는, 이것에 한정되지 않는다는 것은 말할 필요가 없다.

<138> <변형 예2>

<139> 본 실시예에 있어서는, 화상 데이터, 및 그 부분 데이터(영역, 해상도, 화질, 성분, 및 이것들의 조합)을 처리되는 대상으로서 설명한다. 그렇지만, 본 발명은 이것에 한정되지 않는다. 즉, 복수의 부분 데이터로 구성되는 여러 가지의 데이터에 대하여 본 발명을 적용 가능한 것은 명확하다.

<140> 여기에서, 예로서, XML(eXtensible Markup Language) 데이터, PDF(Portable Document Format) 데이터 등의 계층구조를 갖는 문서 데이터에 본 발명을 적용하는 경우의 예를, 도15를 사용하여 설명한다. 도15에 나타나 있는 바와 같이, 본 실시예에 있어서의 문서 데이터는, 하나의 "회사정보"요소로 이루어진다. 또한, 그 "회사 정보"요소는, 하나의 "회사명"요소와 복수의 "사원 정보"요소로 구성된다. 또한, 각 "사원 정보"요소는, 각각 하나의 "사원번호"요소, "이름"요소, 하나의 "성별"요소, 및 하나의 "담당"요소로 구성된다.

<141> 도15에 나타나 있는 바와 같은 문서정보의 경우, 화상 데이터 식별 정보 대신에, 각 문서를 식별하는 문서명(즉, "회사명"요소의 내용)을, 문서 데이터 식별 정보ID로서 이용한다. 또한, 부분 데이터 특정 정보Z로서 "사원번호"요소의 내용을, 그리고 부분 데이터M으로서 "사원정보"요소의 내용을 사용한다.

<142> 본 실시예에 의하면, 서버 상에 유지되어 있는 문서 데이터로부터, "사원번호"요소의 내용을 사용하여, 원하는 "사원정보"요소의 내용을 취득하고서, 그 취득한 "사원정보"요소의 내용이 옳은 정보인가 아닌가를 검증하는 것이 가능해진다.

<143> 게다가, 다른 예로서, 데이타베이스 정보에 대하여 본 발명을 적용하는 경우를, 도16a 및 도16b를 사용하여 설명한다. 도16a 및 도16b에 나타나 있는 바와 같이, 본 실시예에 있어서의 데이타베이스 정보는, "사원번호", "이름", "성별" 및 "담당"으로 구성된 사원정보(레코드)의 집합이다.

<144> 도16에 나타나 있는 바와 같은 데이타베이스 정보의 경우, 화상 데이터 식별 정보 대신에, 각 데이타베이스 정보를 식별하는 데이타베이스 이름을, 데이타베이스 식별 정보ID로서 사용한다. 또한, 부분 데이터 특정 정보Z로서 각 "사원번호"를 사용하고, 부분 데이터M으로서 각 "사원 정보"를 사용한다.

<145> 본 실시예에 의하면, 회사A(즉, 회사식별 정보ID)의 데이타베이스 정보로부터, 사원번호(즉, 부분 데이터 특정 정보Z)를 사용해서 원하는 사원정보(즉, 부분 데이터M)를 취득한 경우, 그 취득한 사원정보가 옳은 사원정보인가 아닌가를 검증하는 것이 가능해진다.

<146> 부수적으로, 본 실시예에서는, 부분 데이터M의 내부에 부분 데이터 특정 정보Z가 포함된다. 그러나, 본 발명은 이것에 한정되지 않는다. 부분 데이터M의 내부에 부분 데이터 특정 정보Z를 포함하지 않도록 하는 것도 가능하다. 이 경우, 원하는 부분 데이터로부터, 부분 데이터 특정 정보Z를 제거하여 취득한 데이터를 부분 데이터M으로서 설정해야 한다.

<147> 이어서, 같은 데이타베이스 정보를 사용한 경우에도, 데이타베이스 식별 정보ID와 부분 데이터 특정 정보Z를 적당하게 설정가능한 예를 설명한다.

<148> 도16a 및 도16b의 회사YYY의 데이타베이스에서는, 데이타베이스 정보식별 정보ID는, URL을 사용하여, 부분 데이터 특정 정보Z로서, "사원번호가 000002 및 성명"으로 설정하고, 부분 데이터 특정 정보Z의 부분 데이터M을 "DDD"로 설정할 수 있다. 상기와 같이, 데이터 생성측이 검증하길 원하는 대상에 따라, 검증 데이터를 생성하는 것이 가능하다. 또한, 데이타베이스 식별 정보ID와 부분 데이터 특정 정보Z를 어떻게 설정할지에 관한 규칙을 데이터 생성측과 데이터 검증측으로 비밀리에 공유하는 경우, 한층 더 그 데이터를 변경하기 어려워진다.

<149> <변형 예3>

<150> 상술한 것처럼, 본 발명에서, 화상 데이터를 암호화(인코딩) 및 암호복호하는(디코딩) 장치는, 일반적인 퍼스널 컴퓨터 등의 범용 정보처리장치이며, 본 발명은 일반적인 퍼스널 컴퓨터 상에서 동작하는 컴퓨터 프로그램으로 실현될 수 있다. 이 때문에, 본 발명의 범주는 컴퓨터 프로그램을 포함하는 것이 명확하다. 또한, 통상, 컴퓨터 프로그램은 CD-ROM등의 컴퓨터 판독 가능한 기억매체에 기억되어 있고, 본 발명은 그 기억매체의 관련 프로그램을 일반적인 퍼스널 컴퓨터의 시스템에 복사 또는 인스톨하여서 이루어질 수 있다. 이 때문에, 본 발명의 범주는 당연히 그 관련 컴퓨터 판독 가능한 기억매체를 포함하는 것도 명확하다.

<151> 이상에서 설명한 바와 같이 본 발명에 의하면, 화상 데이터에 포함된 영역 데이터가 변경되었는가 아닌가를 검증하는 것이 가능하다. 아울러, 상기 영역 데이터가 본래의 원화상 데이터와는 다른 원화상 데이터중의 영역 데이터인 것, 및/또는, 상기 영역 데이터가 본래의 원화상 데이터중의 다른 영역 데이터인 것이 검증 가능해진다.

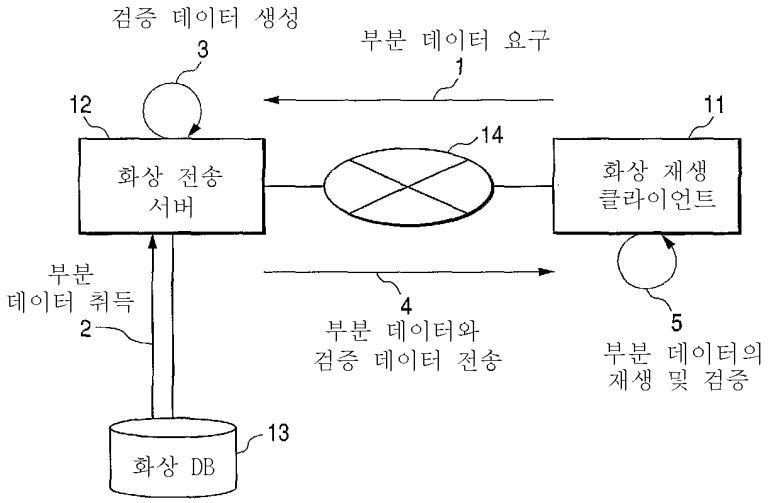
<152> 달리 말하면, 상술한 실시예들을 예시적 목적만을 위해 설명하고 모든 점에서 어떠한 제한을 부여하는 것으로서 파악되어서는 안 된다.

<153> 따라서, 본 발명의 범위는, 이하의 청구항에 의해서만 판단되고 명세서의 문맥에 의해 한정되지 않고, 청구범위와 동등한 범위 내에서 이루어진 변경은 본 발명의 진정한 사상과 범위 내에 속한다.

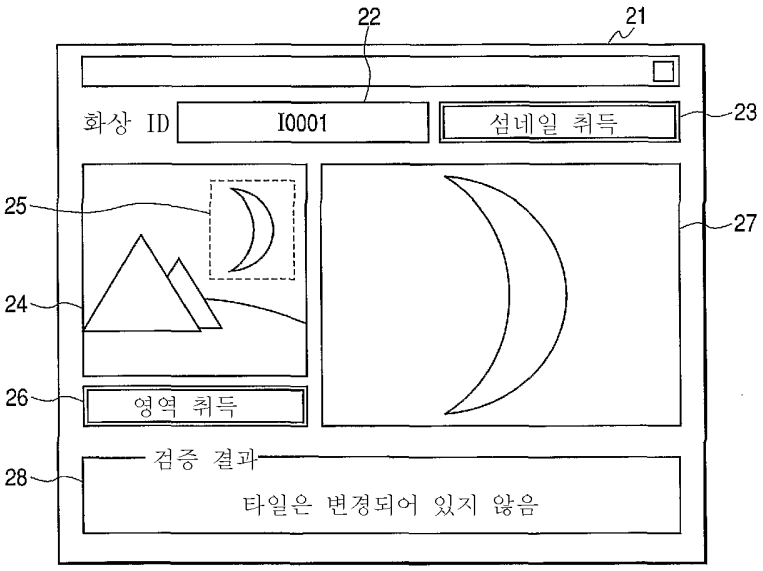
<154> 본 출원은 2005년 2월 9일자로 출원하는 여기서 참고로 포함되는 일본특허출원 번호 2005-033016을 우선권으로 주장한다.

도면

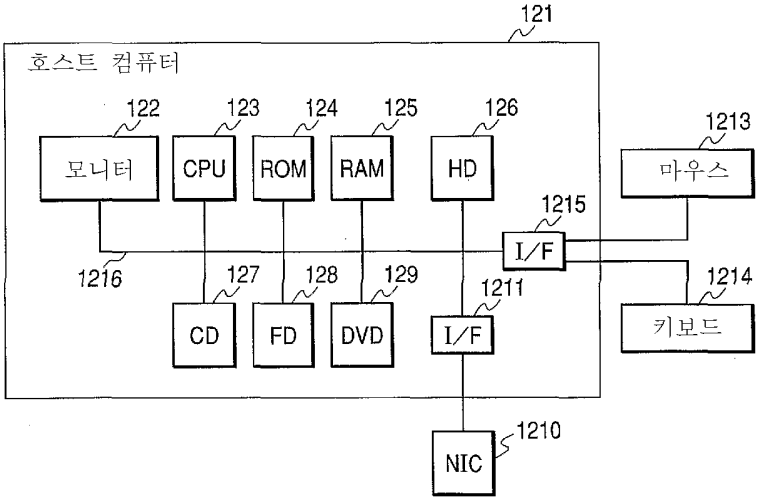
도면1


검증 데이터 생성
3
부분 데이터 요구
1
12
11
14
화상 전송 서버
화상 재생 클라이언트
부분 데이터 취득
2
4
부분 데이터와 검증 데이터 전송
5
부분 데이터의 재생 및 검증
13
화상 DB

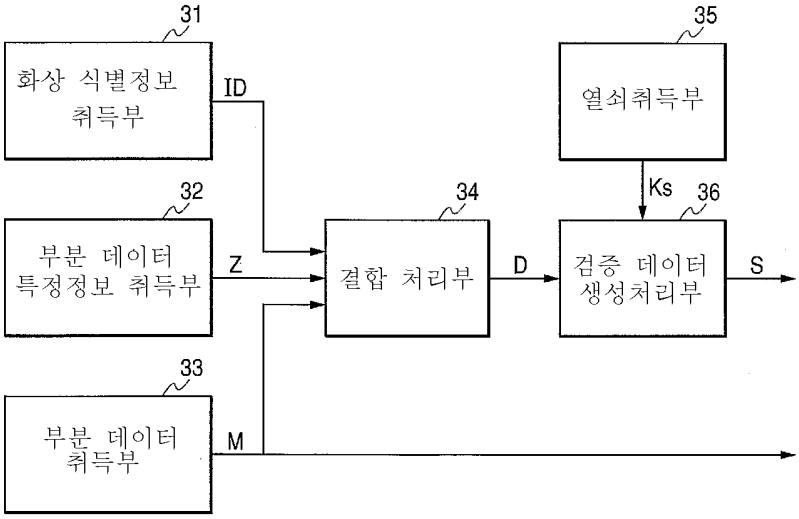
도면2


22
21
화상 ID
I0001
섬네일 취득
23
25
27
24
26
영역 취득
검증 결과
28
타일은 변경되어 있지 않음

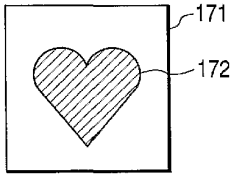
도면3


121
호스트 컴퓨터
122
123
124
125
126
모니터
CPU
ROM
RAM
HD
1213
마우스
1215
I/F
1216
127
128
129
1211
1214
CD
FD
DVD
I/F
키보드
1210
NIC

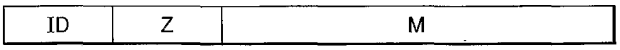
도면4


31
화상 식별정보 취득부
ID
35
열쇠취득부
Ks
32
34
36
부분 데이터 특정정보 취득부
Z
결합 처리부
D
검증 데이터 생성처리부
S
33
부분 데이터 취득부
M

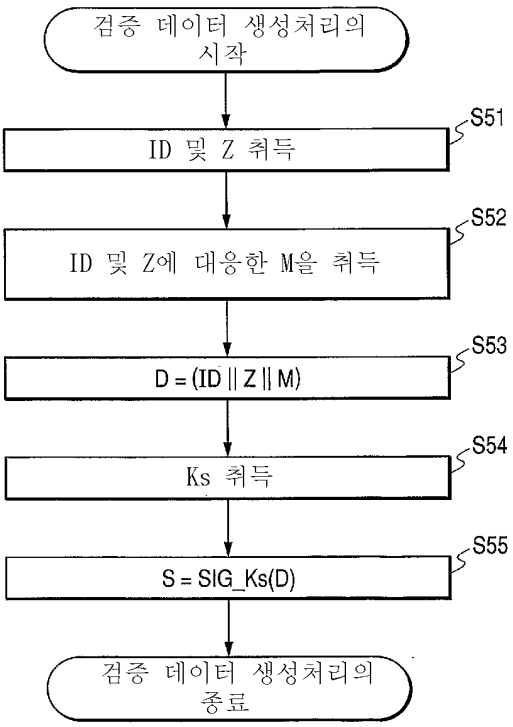
도면5


171
172

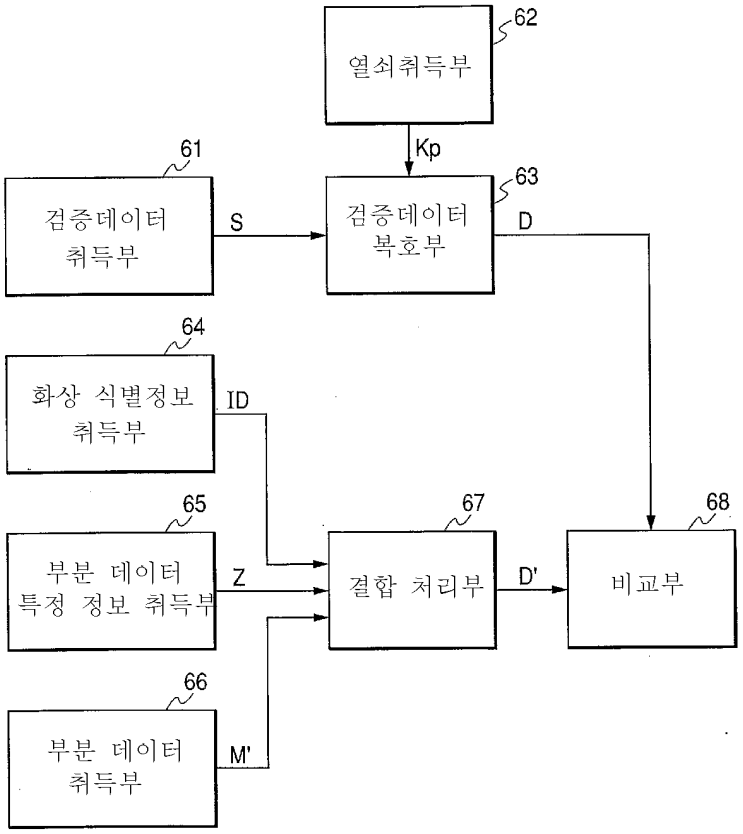
도면6


ID
Z
M

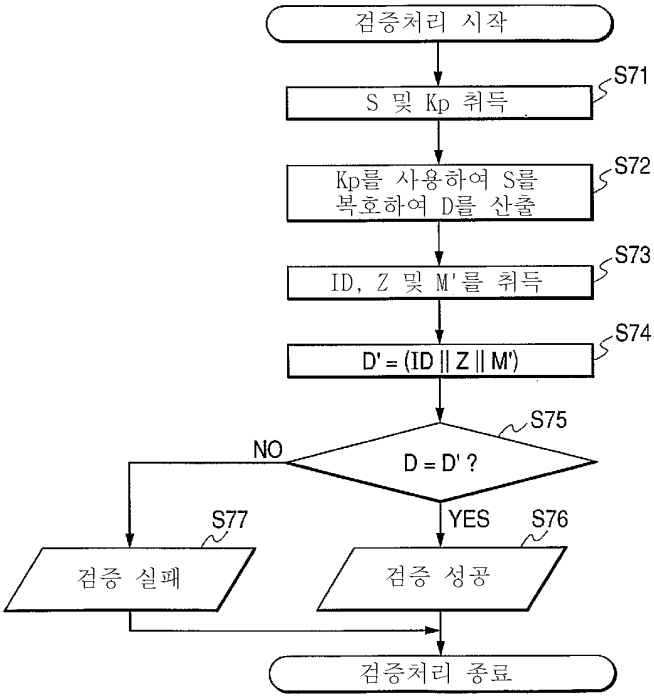
도면7


검증 데이터 생성처리의 시작
S51
ID 및 Z 취득
S52
ID 및 Z에 대응한 M을 취득
S53
D = (ID || Z || M)
S54
Ks 취득
S55
S = SIG_Ks(D)
검증 데이터 생성처리의 종료

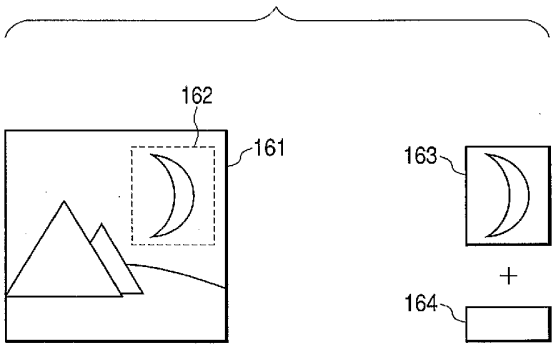
도면8


열쇠취득부
62
Kp
61
검증데이터 취득부
S
검증데이터 복호부
63
D
64
화상 식별정보 취득부
ID
65
부분 데이터 특정 정보 취득부
Z
67
결합 처리부
D'
68
비교부
66
부분 데이터 취득부
M'

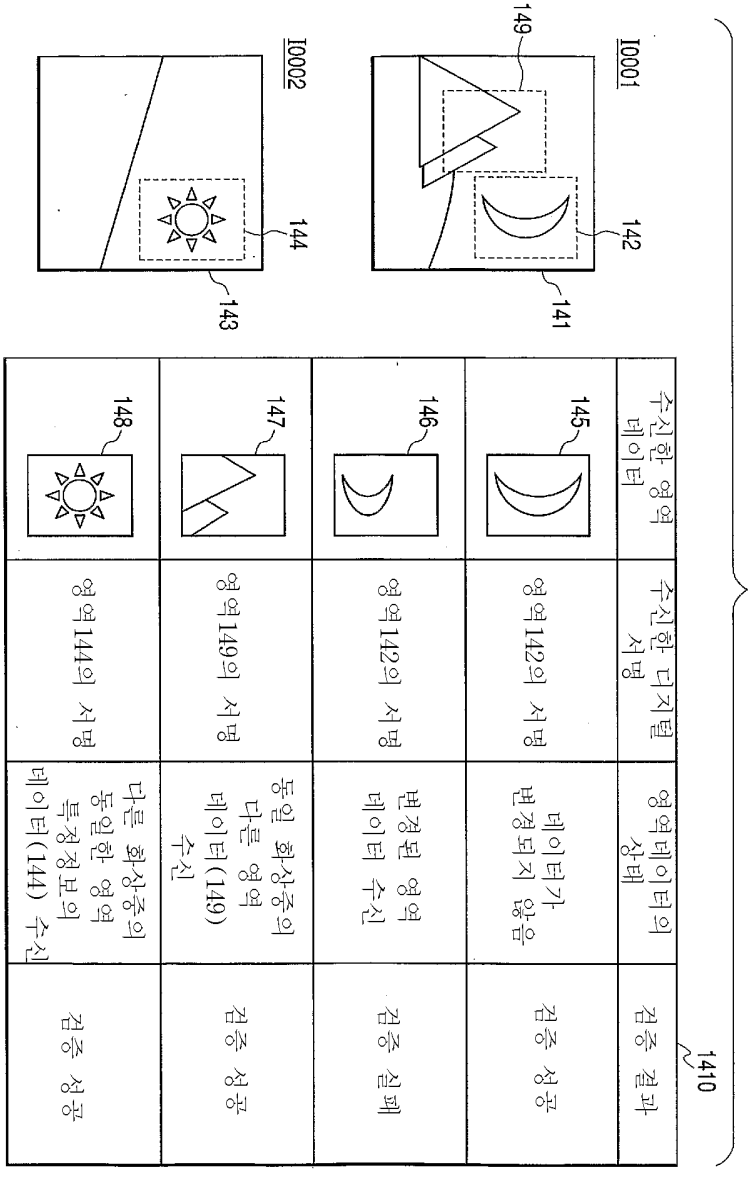
도면9


검증처리 시작
S71
S 및 Kp 취득
S72
Kp를 사용하여 S를 복호하여 D를 산출
S73
ID, Z 및 M'를 취득
S74
D' = (ID || Z || M')
S75
D = D' ?
NO
YES
S77
검증 실패
S76
검증 성공
검증처리 종료

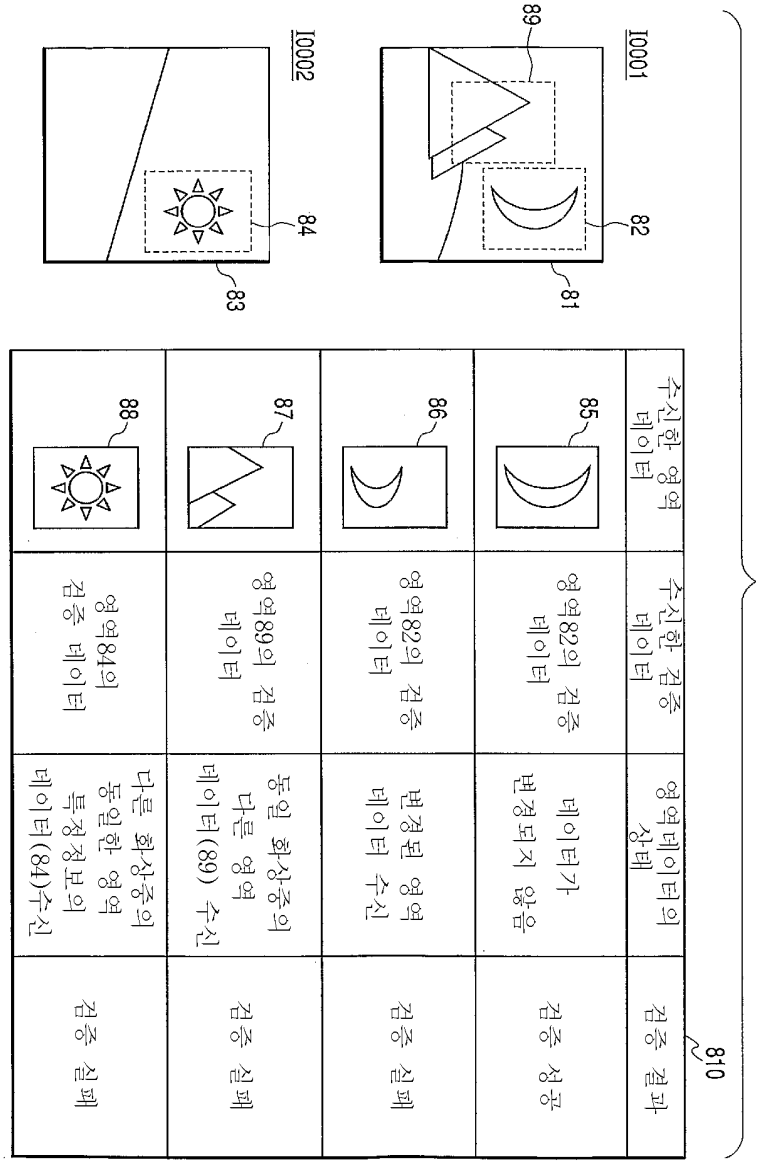
도면10


162
161
163
+
164

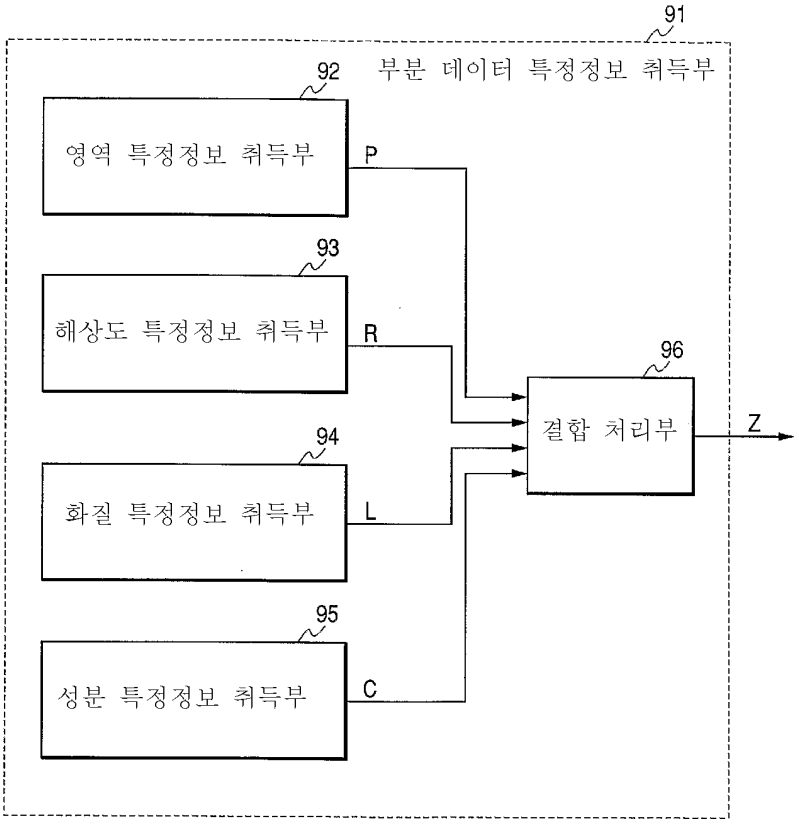
도면11


I0001
149
142
141
I0002
144
143
1410
수신한 영역 데이터
수신한 디지털 서명
영역데이터의 상태
검증 결과
145
영역142의 서명
데이터가 변경되지 않음
검증 성공
146
영역142의 서명
변경된 영역 데이터 수신
검증 실패
147
영역149의 서명
동일 화상중의 다른 영역 데이터(149) 수신
검증 성공
148
영역144의 서명
다른 화상중의 동일한 영역 특정정보의 데이터(144) 수신
검증 성공

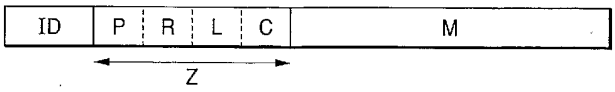
도면12


I0001
89
82
81
I0002
84
83
810
검증 결과
영역데이터의 상태
수신한 검증 데이터
수신한 영역 데이터
검증 성공
데이터가 변경되지 않음
영역82의 검증 데이터
85
검증 실패
변경된 영역 데이터 수신
영역82의 검증 데이터
86
검증 실패
동일 화상중의 다른 영역 데이터(89) 수신
영역89의 검증 데이터
87
검증 실패
다른 화상중의 동일한 영역 특정정보의 데이터(84)수신
영역84의 검증 데이터
88

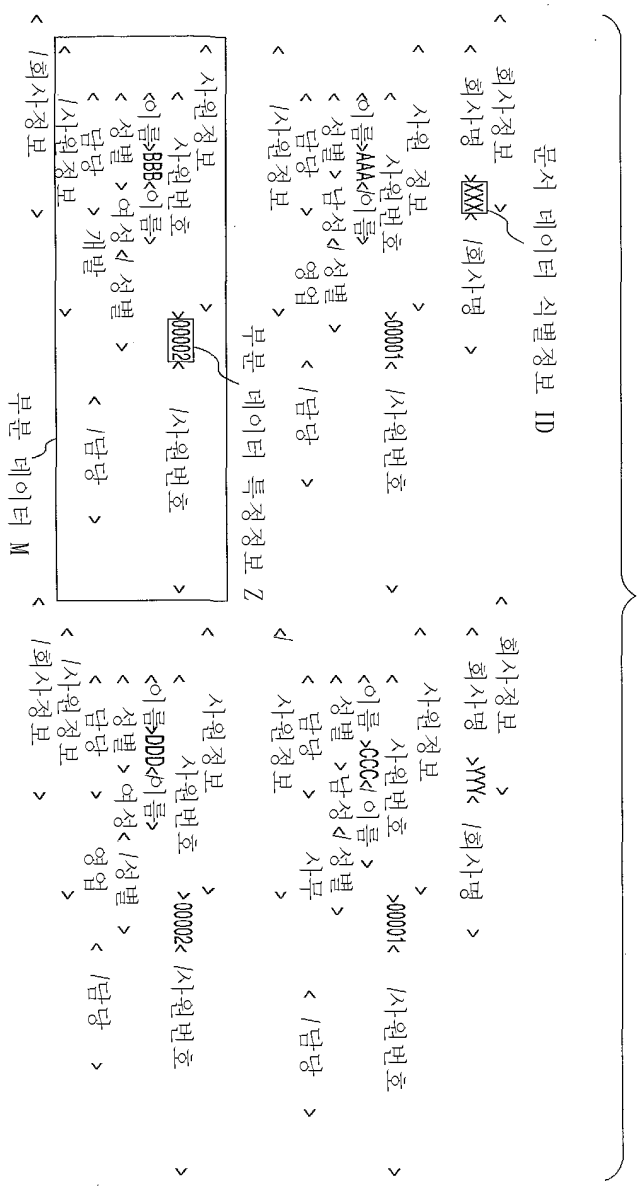
도면13


91
부분 데이터 특정정보 취득부
92
영역 특정정보 취득부
P
93
해상도 특정정보 취득부
R
96
결합 처리부
Z
94
화질 특정정보 취득부
L
95
성분 특정정보 취득부
C

도면14

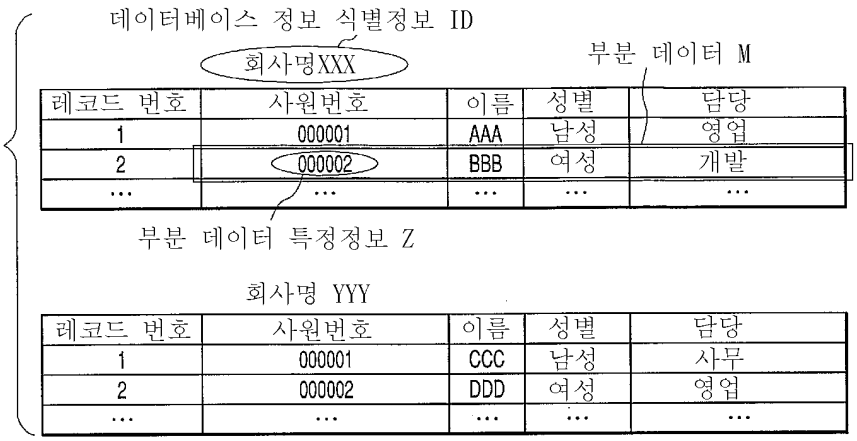

ID
P
R
L
C
M
Z

도면15


문서 데이터 식별정보 ID
<회사정보>
<회사명 >XXX< /회사명 >
<사원 정보 >
<사원번호 >00001< /사원번호 >
<이름>AAA</이름>
<성별 > 남성</성별 >
<담당 > 영업 < /담당 >
</사원정보 >
부분 데이터 특정정보 Z
<사원정보 >
<사원번호 >00002< /사원번호 >
<이름>BBB</이름>
<성별 > 여성</성별 >
<담당 > 개발 < /담당 >
</사원정보 >
부분 데이터 M
</회사정보 >
<회사정보 >
<회사명 >YYY< /회사명 >
<사원정보 >
<사원번호 >00001< /사원번호 >
<이름 >CCC</이름 >
<성별 >남성</성별 >
<담당 > 사무 < /담당 >
</사원정보 >
<사원정보 >
<사원번호 >00002< /사원번호 >
<이름>DDD</이름>
<성별 > 여성< /성별 >
<담당 > 영업 < /담당 >
</사원정보 >
</회사정보 >

도면16

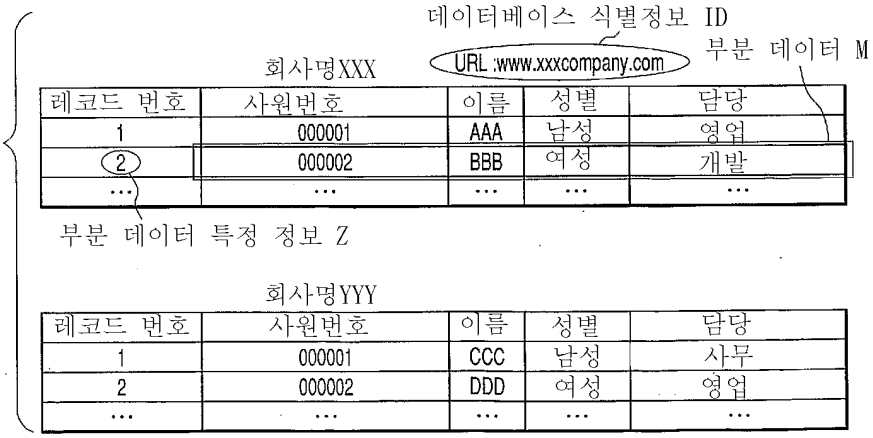
(a)



레코드 번호	사원번호	이름	성별	담당
1	000001	AAA	남성	영업
2	000002	BBB	여성	개발
…	…	…	…	…

레코드 번호	사원번호	이름	성별	담당
1	000001	CCC	남성	사무
2	000002	DDD	여성	영업
…	…	…	…	…

(b)



레코드 번호	사원번호	이름	성별	담당
1	000001	AAA	남성	영업
2	000002	BBB	여성	개발
…	…	…	…	…

레코드 번호	사원번호	이름	성별	담당
1	000001	CCC	남성	사무
2	000002	DDD	여성	영업
…	…	…	…	…

도면17