(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04N 1/32

(11) 공개번호 특2001-0043172
(43) 공개일자 2001년05월25일

(21) 출원번호 10-2000-7012092
(22) 출원일자 2000년10월30일
번역문제출일자 2000년10월30일
(86) 국제출원번호 PCT/EP1999/02928 (87) 국제공개번호 WO 1999/57885
(86) 국제출원출원일자 1999년04월29일 (87) 국제공개일자 1999년11월11일
(81) 지정국 EP 유럽특허 : 오스트리아 벨기에 스위스 독일 덴마크 스페인 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투칼 스웨덴 핀랜드 사이프러스

국내특허 : 일본 대한민국

(30) 우선권주장 09/070,524 1998년04월30일 미국(US)
(71) 출원인 메디아섹 테크놀로지즈 엘엘시

미합중국 02903 로드 아일랜드주 프라비던스 사우스 메인 스트리트 321 슈이트 2

프라운호퍼 센터 포 리서치 인 컴퓨터 그래픽스 인코포레이티드

미합중국 02903 로드 아일랜드주 프라비던스 사우스 메인 스트리트 321 슈이트 2

(72) 발명자 코흐엑카드

독일연방공화국데-45134에센준뎀홀츠71

차오지앙

미합중국02904로드아일랜드주프라비던스토마스올니커먼64

(74) 대리인 김성기, 송병옥

심사청구 : 없음

(54) 아날로그 문서의 디지털 인증

요약

본 발명은 디지털 표현 및 디지털 표현으로부터 생성된 아날로그 형태의 보안성을 보호하는 기술에 관한 것이다. 이 기술은 디지털 표현 및 디지털 표현으로부터 생성된 아날로그 형태 모두를 인증할 수 있는 인증 기술, 워터마크가 판독되면 실행될 수 있는 프로그램 코드를 포함하는 활성 워터마크, 및 워터마크를 판독하고 워터마크를 포함하는 디지털 표현에 관한 정보 메시지를 전송하는 워터마크 에이전트를 포함한다. 인증 기술은 의미 정보를 사용하여 인증 정보를 생성한다. 디지털 표현으로부터 아날로그 형태를 생성하는 경우, 의미 정보 및 인증 정보 모두가 존속한다. 하나의 실시예에서, 의미 정보는 문자-숫자 문자이며, 인증 정보는 디지털 표현에 내장된 워터마크에 포함되거나 바 코드로 표현된다. 활성 워터마크를 사용하는 경우, 워터마크는 프로그램 코드를 포함한다. 워터마크 판독기가 워터마크를 판독하는 경우, 프로그램 코드가 실행된다. 활성 워터마크를 사용하는 한가지 예가 활성 워터마크가 작동될 때 메시지를 전송하는 문서를 작성하는 것이다. 워터마크 에이전트는 네트워크의 노드 또는 복사기와 같은 장치에 영구적으로 상주하거나 하나의 네트워크 노드에서 다른 네트워크 노드로 이동할 수 있다. 이들 장치 또는 노드에서, 워터마크 에이전트는 워터마크 에이전트와 관련된 워터마크가 표시된 디지털 표현에 대하여 노드 또는 장치에 상주하는 디지털 표현을 검사하는 코드를 실행한다. 그 후 워터마크 에이전트는 디지털 표현의 검사 결과를 보고하는 메시지를 전송한다. 워터마크가 활성화되는 경우, 워터마크 에이전트 및 활성 워터마크는 함께 동작할 수 있으며, 워터마크 에이전트에 의해 활성 워터마크를 포함하는 일부 또는 모든 코드를 실행시킬 수 있다.

대표도

도2

색인어

의미 정보, 인증 정보, 디지털 표현, 아날로그 형태, 인증기, 결합기, 디지털 워터마크, 워터마크 에이전트, 활성 워터마크, 식별 정보, 광학 문자 인식기, 다이제스트, 의미 정보 인식기, 인증 정보 판독기.

명세서

기술분야

본 출원의 상세한 설명은 Jian Zhao에 의해 본 출원과 동일한 일자에 출원되어 Fraunhofer CRCG에게 양도된 Active Watermarks and Watermark Agents와 동일하다.

본 발명은 일반적으로 영상 및 기타 다른 정보의 디지털 표현에 관한 것이며, 더 구체적으로는 디지털 표현 및 이들로부터 생성된 아날로그 형태의 보안성(security)을 유지하기 위한 기술에 관한 것이다.

배경기술

오늘날 화상 또는 음성을 다루기 위한 가장 쉬운 방법은 화상 또는 음성의 디지털 표현을 만드는 것이다. 디지털 표현이 만들어지면, 컴퓨터를 사용하는 모든 사람은 디지털 표현의 상태에 나쁜 영향을 미치지 않으면서 이를 복제, 개작하고, 세계 어디든지 거의 순간적으로 전송할 수 있다. 마침내 인터넷을 통해 어떠한 디지털 표현도 세계 모든 곳으로 전달할 수 있게 되었다.

그러나 디지털 표현의 소유자의 입장에서 보면, 합법적인 소유권자 및 사용자가 그러하듯이, 침해자(pirates) 역시 컴퓨터를 사용하여 디지털 표현을 복제, 개작, 배포할 수 있다는 문제점이 있다. 원래의 디지털 표현을 소유하고 있는 소유권자가 디지털 표현의 창조와 공표에 대한 적합한 보상을 받도록 하기 위해서는, 침해자들로부터 디지털 표현을 보호해야 한다. 다음과 같은 다수의 서로 다른 방법을 사용할 수 있다.

· 예정된 수신인(intended recipient)을 제외하고는 디지털 표현을 판독할 수 없도록 할 수 있다. 이는 암호화(encryption) 기술을 통해 구현된다.

· 디지털 표현에 그 인증 여부를 표시할 수 있다. 이는 디지털 서명(digital signature)을 통해 구현된다.

· 디지털 표현이 전송 중에 개작되었는지를 판단할 수 있는 정보를 포함할 수 있다. 이 정보는 다이제스트(digest)라 불리며, 디지털 서명이 다이제스트를 포함하는 경우도 종종 있다.

· 디지털 표현은 소유권자에 대한 비가시적인 표현인 워터마크(watermark)를 포함할 수 있으며, 워터마크는 디지털 표현으로부터 제거될 수 없으며 디지털 표현으로부터 생성된 아날로그 복제물에서도 검출될 수 있다.

· 디지털 표현을 보호하고 디지털 표현의 사용을 측정하고/측정하거나 불법적인 사용을 검출할 수 있는 전술한 기술을 시스템에 사용할 수 있다.

암호화 기술을 사용하여 디지털 표현을 보호하는 시스템의 일례로 Saito의 "Data Copyright Management Method" (미합중국 특허번호 제 5,646,999호, 1997년 7월 8일 특허 받음)를 참조하고, 디지털 워터마크에 관한 일반적인 논의에 대해서는 Jian Zhao의 "Look, It's Not There"(Byte Magazine, 1997년 1월)를 참조하라. 디지털 워터마크에 관한 특정 기술에 대한 상세한 설명은 E. Koch 및 J. Zhao의 "Towards Robust and Hidden Image Copyrights Labeling" (1995 IEEE Workshop on Nonlinear Signal and Image Processing, 1995년 6월 20-22일) 및 Rhoads의 "Method and Apparatus Responsive to a Code Signal Conveyed through a Graphic Image"(미합중국 특허번호 제 5,710,834호, 1998년 1월 20일에 특허 받음)에 기재되어 있다. Rhoads 특허에 기재된 디지털 워터마크 기술을 사용하는 상업용 워터마크 시스템의 일례로, http://www.digimarc.com에서 1998년 3월에 발표한 Digimarc Watermarking Guide (Digimarc Corporation, 1997)를 참조하라.

도 1은 전술한 보호 기술을 사용하는 종래의 시스템(101)을 보여준다. 다수의 디지털 표현 클라이언트(digital representation clients)(105)[여기서는 하나의 디지털 표현 클라이언트[105(j)]만을 도시함]는 디지털 표현 서버(digital representation server, DR 서버)(129)와 연결되며, 서버(129)는 인터넷과 같은 네트워크(103)를 통해 클라이언트(105)로부터 디지털 표현을 수신하고 이를 클라이언트(105)에게 배포한다. 서버(129)는 배포할 복제 디지털 표현(copied digital representations, CDR)(137) 및 관리 데이터베이스(management data base, MGDB)(139)를 가지는 데이터 기억 장치(data storage device)(133)를 포함한다. 또한 서버(129)는 디지털 표현 관리 프로그램(digital representation management program, DRMG)(131), 워터마크 판독 및 기록 프로그램(program for reading and writing watermarks, WMR/W)(109), 디지털 표현을 인증하고 디지털 표현의 인증 여부를 확인하는 인증 및 확인 프로그램(program for authentication and confirmation)(111) 및 디지털 표현의 암호화 및 해독 프로그램(encrypting and decrypting digital representation)(113)을 추가로 포함한다. 프로그램(109, 111, 113)은 함께 보안 프로그램(security programs)(107)을 이룬다.

클라이언트(105)는 고유 버전의 보안 프로그램(107)을 포함하며, 네트워크(103)를 통해 수신하거나 기억 장치(117)에 저장되어 있는 디지털 표현을 편집하거나 볼 수 있는 편집기/뷰어 프로그램(editor/viewer program)(115)을 추가로 포함한다. 도시한 기억 장치(117)는 클라이언트(105)의 사용자가 작성한 원 디지털 표현(original digital representation, ODR)(119) 및 DR 서버(129)로부터 수신한 복제된 디지털 표현(copied digital representation, CDR)(121)을 포함한다. 물론 사용자는 복제 디지털 표현을 개작함으로써 새로운 원 디지털 표현(119)을 창작할 수 있다. 사용자는 편집기/뷰어 프로그램(115)을 사용하여 디지털 표현을 아날로그 출력 장치(123)에 출력할 수 있다. 이들 장치의 일례가 디지털 표현으로부터 생성된 아날로그 영상(124)이 표시되는 표시 장치(display device)(125) 및 디지털 표현으로부터 생성된 아날로그 영상(126)이 인쇄되는 프린터(127)이다. 확성기 또한 아날로그 출력 장치(123)에 포함될 수 있다. 본 명세서에서는 아날로그 출력 장치의 출력을 디지털 표현의 "아날로그 형태"라 한다. 예를 들어 출력 장치가 프린터인 경우에는 아날로그 형태가 인쇄 용지(126)에 인쇄되며, 출력 장치가 표시 장치인 경우에는 아날로그 형태가 표시 장치(124)에 표시된다.

클라이언트[105(j)]가 서버(129)로부터 디지털 표현을 수신하고자 하는 경우, 클라이언트는 디지털 표현

을 요구하는 메시지를 서버(129)에 전송한다. 메시지는 적어도 원하는 디지털 표현 ID(identification) 및 사용자 ID를 포함한다. 관리자(관리 프로그램)(131)는 디지털 표현을 CDR(137)에 위치시킴으로써 요구에 응답하며, 관리 데이터베이스(139)를 참조하여 디지털 표현이 배포될 수 있는 조건 및 고객인 클라이언트(105) 사용자의 상태를 결정한다. 데이터베이스(139)의 정보가 트랜잭션(transaction)이 진행되어야 함을 관리자(131)에게 나타내면, 관리자(131)는 선택된 디지털 표현의 복제물을 클라이언트[105(j)]에게 전송한다. 복제물이 전송되는 동안, 관리자(131)는 워터마크 판독 및 기록 프로그램(109)을 사용하여 워터마크를 디지털 표현에 추가하고, 인증 및 확인 프로그램(111)을 사용하여 인증 정보(authentication information)를 추가하고, 암호화 및 해독 프로그램(113)을 사용하여 DR 클라이언트[105(j)]에서만 해독될 수 있는 방법으로 디지털 표현을 암호화할 수 있다.

클라이언트[105(j)]가 디지털 표현을 수신하면, 암호화 및 해독 프로그램(113)을 사용하여 디지털 표현을 해독하고, 인증 및 확인 프로그램(111)을 사용하여 디지털 표현의 인증 여부를 확인하고, 워터마크 판독 및 기록 프로그램(109)을 사용하여 워터마크를 표시할 수 있다. 클라이언트[105(j)]의 사용자는 암호화 또는 해독된 디지털 표현을 기억 장치(119)에 저장한다. 클라이언트[105(j)]의 사용자는 편집기/뷰어(115)를 사용하여 디지털 표현을 해독하고, 해독 결과를 아날로그 출력 장치(123)에 출력한다. 아날로그 출력 장치(123)에는 표시 장치(125), 프린터(127) 등이 있으며, 오디오의 디지털 표현인 경우에는 확성기 등이 있다.

디지털 표현이 아날로그 형태로 표시되거나 인쇄되는 경우, 복제를 방지하기 위한 유일한 방법은 바로 워터마크(128)이다. 인간 관찰자는 이 아날로그 형태에서 워터마크(128)를 찾아낼 수 없지만 아날로그 형태를 스캐닝하거나 컴퓨터를 사용하면 이를 검출할 수 있다. 따라서 워터마크(128)는 암호화의 보완 수단이다. 즉, 누군가가 암호를 깨고 들어가거나 디지털 표현을 합법적으로 액세스한 누군가가 불법 복제물을 만드는 등 디지털 표현에 대한 침해 행위가 발생한 경우, 워터마크는 적어도 원 디지털 표현의 소유권자를 결정할 수 있게 하여 이를 침해 행위에 대한 증거로서 제공하여 저작권 침해 및/또는 비밀 계약 위반 등의 침해 행위를 추적할 수 있게 한다.

클라이언트[105(j)]의 사용자가 원 디지털 표현(119)을 DR 서버(129)에 전송하여 배포하고자 하는 경우, 편집기/뷰어(115)는 원 디지털 표현(119)을 서버(129)에 전송한다. 이 동안에 편집기/뷰어(115)는 보안 프로그램(107)을 사용하여 디지털 표현에 워터마크를 부가하고, 인증하고, DR 서버(129)에 의해서만 해독될 수 있도록 암호화한다. DR 서버(129)의 관리자(131)는 원 디지털 표현(119)을 수신하면, 보안 프로그램(107)을 사용하여 원 디지털 표현(119)을 해독하고, 인증 여부를 확인하고, 관리 데이터베이스(139)에 이에 대한 정보를 입력하고, 기억 장치(133)에 저장한다.

전술한 Digimarc 시스템의 경우, 관리자(131)는 체계적으로 HTTP 및 FTP 링크와 같은 월드 와이드 웹(world wide web) 링크를 따라가 링크가 가리키는 자료를 인출(fetch)하는 프로그램인 월드 와이드 웹 스파이더(world wide web spider)를 포함한다.

관리 프로그램(131)은 워터마크 판독 및 기록 프로그램을 사용하여 모든 워터마크를 판독하고, 워터마크가 관리 데이터베이스(139)에 알려져 있다면 예를 들어 그 디지털 표현을 가지고 있는 사이트가 그런 권한이 있는지의 여부를 결정하고 그렇지 않은 경우 디지털 표현의 저작권자에게 통지하는 등, 필요한 동작을 모두 실행한다.

디지털 표현의 소유권자가 암호화, 인증 및 워터마크 표시를 통해 그들의 자산을 훨씬 쉽게 보호할 수 있긴 하지만, 이 경우에도 여전히 문제점이 존재한다. 첫 번째 문제점은 현재의 디지털 문서 인증 기술을 아날로그 형태에는 적용할 수 없다는 점이다. 따라서 디지털 표현이 아날로그 형태로 출력되는 경우에는 인증 여부를 확인할 수 없다. 두 번째 문제점은 디지털 표현을 관리하는 현재의 시스템의 적용 범위가 충분히 넓지 않다는 점이다. 세 번째 문제점은 전술한 워터마크 스파이더에 의해 행해지는 워터마크 검사의 범위가 인터넷 상에서 사용할 수 있는 디지털 표현으로 제한된다는 점이다. 본 발명의 목적은 전술한 문제점을 극복하고 그 결과 디지털 표현을 배포하기 위한 개선된 기술을 제공하는 것이다.

발명의 상세한 설명

디지털 표현으로부터 생성되는 모든 아날로그 형태에 존재하는 정보인 의미 정보(semantic information)에 기초한 의미 정보 인증 기술을 사용함으로써 디지털 인증 기술의 사용 범위가 디지털 표현으로 제한되는 문제점을 해결한다. 의미 정보를 사용하여 다이제스트 등의 식별 정보를 생성하며, 다이제스트를 디지털 표현에 추가할 때는 의미 정보에 영향을 미치지 않도록 한다. 한 실시예에서는 식별 정보가 디지털 표현에 워터마크로 추가된다. 다른 실시예에서는 다이제스트가 바코드로 표현된다. 디지털 표현 또는 아날로그 형태가 의미 정보에 기초한 인증 정보를 포함하는 경우, 의미 정보를 다시 사용하여 인증 정보를 연산 처리하고 새로이 연산 처리된 인증 정보를 디지털 표현 또는 아날로그 형태의 인증 정보와 비교함으로써, 디지털 표현 또는 아날로그 형태를 인증한다. 이들 정보가 일치하면, 그 디지털 표현 또는 아날로그 형태는 인증된 것이다. 의미 정보 및 인증 목적에 따라 일치의 형태는 정확한 일치 또는 퍼지(fuzzy) 일치가 된다. 의미 정보에 기초한 인증에는 전자 문서의 디지털 형태의 인증, 종이 디지털 화폐(paper digital cash)의 인증, 종이 디지털 수표(paper digital checks)의 인증 및 은행 카드 따위의 식별 카드의 인증 등이 있다.

본 발명이 속하는 기술 분야의 당업자는 다음의 실시예 및 도면을 정독함으로써 본 발명의 다른 목적 및 이점을 명확하게 이해하게 될 것이다.

도면의 간단한 설명

도 1은 디지털 표현의 배포 시에 보안성을 유지하기 위한 종래의 시스템을 도시한 블록도이다.

도 2는 본 발명의 제1 실시예에 따른 인증 가능한 아날로그 형태를 도시한 도면이다.

도 3은 본 발명의 제2 실시예에 따른 인증 가능한 아날로그 형태를 도시한 도면이다.

도 4는 인증 정보를 아날로그 형태에 부가하는 시스템을 도시한 도면이다.

도 5는 아날로그 형태의 인증 시스템을 도시한 도면이다.

도 6은 활성(active) 워터마크 생성 시스템을 도시한 도면이다.

도 7은 활성 워터마크 코드의 일례를 도시한 도면이다.

도 8은 활성 워터마크의 코드를 실행하기 위한 시스템을 도시한 도면이다.

도 9는 워터마크 에이전트(watermark agent) 생성 시스템을 도시한 도면이다.

도 10은 워터마크 에이전트 수신 시스템을 도시한 도면이다.

도 11은 액세스 정보(access information)(603)를 상세하게 도시한 도면이다.

도 12는 워터마크 에이전트에 의해 실행되는 코드의 예를 도시한 도면이다.

도면 부호는 적어도 3자리 숫자로 이루어져 있다. 최우측 두 자리 숫자는 그 도면 내의 도면 부호이며, 최우측 두 자리 숫자의 좌측에 위치하는 숫자는 도면번호로 식별되는 항목이 처음으로 나타나는 도면의 번호이다. 예를 들어 도면번호 (203)로 표시되는 항목은 도 2에 처음으로 나타난다.

실시예

다음의 상세한 설명에서는 디지털 표현의 아날로그 형태의 출력에 적용될 수 있는 디지털 표현 인증 기술에 대하여 먼저 설명한 후에, 활성 워터마크 즉 프로그램을 포함하는 워터마크에 대하여 설명하고, 마지막으로 워터마크 에이전트 즉 시스템에 저장된 디지털 표현의 디지털 워터마크를 검사하여 불법적으로 사용되는 디지털 표현을 검색하는 프로그램에 대하여 설명한다.

아날로그 형태의 인증: 도 2 내지 도 5

디지털 표현이 전송 중에 변경되지 않았음을 보증하기 위해 디지털 표현을 인증한다. 이러한 변경은 디지털 표현의 소스로부터 목적지로 전송되는 도중에 발생하는 전송 오류, 디지털 표현을 전송하는 데 사용되는 기억 장치의 손상 때문에 발생하는 오류, 디지털 표현을 기억 장치에 기록하거나 기억 장치로부터 디지털 표현을 판독하는 과정에서 발생하는 오류로 인한 것이거나, 인간의 개입으로 인하여 발생할 수 있다. 표준 인증 기술은 디지털 표현의 다이제스트를 생성하고, 이 다이제스트를 디지털 표현과 함께 목적지로 전송한다. 목적지에서, 수신된 디지털 표현의 다른 다이제스트를 생성하고, 이를 전송 이전의 다이제스트와 비교한다. 이들 다이제스트가 동일한 경우, 디지털 표현은 변경되지 않은 것으로 판정된다. 다이제스트는 디지털 표현에 비해 훨씬 그 길이가 짧지만 디지털 표현이 조금이라도 변경되면 다이제스트도 변경될 가능성이 아주 높도록 하는 방식으로 디지털 표현과 연관된 단순한 값이다.

인간 개입이 심각한 문제가 되는 경우, 일방향 해시(one-way hash) 기능을 사용하여 다이제스트를 생성하는데, 일방향 해시 기능으로 생성된 다이제스트로는 다이제스트를 생성한 입력에 대하여 무언가를 알아내기가 어렵거나 불가능하다. 다이제스트는 디지털 표현의 수신인만이 이를 판독할 수 있도록 추가로 암호화된다. 통상적인 기술은 디지털 표현이 전송 중에 변경되지 않았으며 전송되어야 할 송신지로부터 디지털 표현이 전송되었음을 나타내는 디지털 표현의 암호화된 다이제스트를 디지털 서명으로 사용하는 것이다. 송신인 및 수신인이 공용 키(public key)를 교환한 경우, 송신인은 다이제스트를 전송자의 개인 키로 암호화함으로써 디지털 서명을 생성할 수 있다. 수신인은 송신인의 공용 키를 사용하여 다이제스트를 해독할 수 있으며, 수신인은 다이제스트를 해독한 후에 수신한 디지털 표현으로부터 생성된 다이제스트와 해독한 다이제스트를 비교한다. 디지털 표현이 변경되었거나 다이제스트를 해독하기 위해 사용되는 공용 키를 가지지 않은 사람으로부터 디지털 표현이 전송된 경우에는 이들 다이제스트가 동일하지 않다. 인증에 대한 상세한 설명은 Bruce Schneier의 Applied Cryptography(John Wiley and Sons, 1994)의 제 32장에 기재되어 있다.

인증과 관련된 유일한 문제점은 인증이 전적으로 디지털 표현에 기초한다는 것이다. 디지털 표현이 아날로그 형태로 출력되는 경우에는 다이제스트를 생성하는 데 사용되는 정보가 멸실된다. 예를 들어 디지털 표현이 문서인 경우에는, 디지털 표현으로부터 생성된 종이 복제물로부터, 종이 복제물을 생성한 디지털 표현의 인증 여부를 판정하거나 종이 복제물 자체가 디지털 표현의 진정한 복제물인지를 판정할 수 있는 방법이 없다.

디지털 표현이 아날로그 형태로 출력되는 경우, 디지털 워터마크가 살아남아 검출 가능하다고 하더라도, 다이제스트 또는 디지털 서명을 워터마크에 삽입함으로써 인증 문제를 간단하게 해결할 수는 없다. 여기에는 다음과 같은 두 가지 이유가 존재한다.

· 워터마크 표시는 디지털 표현을 변경한다. 따라서 원 다이제스트가 생성된 후에 디지털 표현에 워터마크를 표시하는 경우, 워터마크 표시가 원 다이제스트를 쓸모 없는 것으로 만들어 버리기 때문에, 수신자는 워터마크가 부가된 문서로부터 생성한 새로운 다이제스트와 원 다이제스트를 비교할 수 없다.

· 디지털 표현이 아날로그 형태로 출력되고 디지털 표현에 대한 정보가 많이 손상되어 아날로그 형태로부터 디지털 표현을 재구성할 수 없는 경우, 더 심각한 문제가 존재한다. 따라서 원 다이제스트가 여전히 유효한 경우에도, 아날로그 형태로부터 비교 가능한 새로운 다이제스트를 생성할 수 없다.

이러한 문제점을 해결하기 위해서는 디지털 표현의 특정 형태에 영향을 받지 않으며 아날로그 형태로 출력할 때 그 아날로그 형태에 포함될 인증 정보를 사용하는 인증 기술이 필요하다. 아래에서 더 상세하게 설명하고 있는 바와 같이, 디지털 표현으로부터 의미 정보를 선택하고 의미 정보만을 사용하여 다이제스트를 생성함으로써 제1 요건을 충족한다. 다이제스트를 생성하는 데 사용되는 의미 정보에 영향을 주지 않는 한편 아날로그 형태에서도 존속하도록 하는 방법으로 다이제스트를 디지털 표현과 결합함으로써 제2 요건을 충족한다. 문서의 경우, 이들 요건을 충족하는 인증 기술은 일차적으로 디지털 형태로 존재하는

문서의 아날로그 형태를 인증하는 데 사용될 수 있을 뿐만 아니라 종이 수표 및 식별 카드와 같이 아날로그 형태로만 존재하거나 일차적으로 아날로그 형태로 존재하는 문서를 인증하는 데 사용될 수 있다.

의미 정보

디지털 표현의 의미 정보는 그 디지털 표현으로부터 생성된 아날로그 형태를 접한 사람이 이를 디지털 표현을 생성한 원본의 복제물로 인정하기 위하여 아날로그 형태에 존재해야 하는 디지털 표현 정보의 일부이다. 예를 들어 문서 영상의 디지털 표현의 의미 정보는 문서의 문자-숫자(alphanumeric) 표현인데, 여기서 문자-숫자는 비라틴계 문자(non-Latin alphabet), 음절 문자 체계(syllabic writing system) 및 표의 문자 체계(ideographic writing systems)에 속하는 문자를 비롯하여 모든 종류의 문자 또는 문장 부호(또는 구두점) 표현을 포함하는 것으로 해석된다. 의미 정보가 문자-숫자 문자로 이루어져 있다고 가정하면, 아날로그 형태를 수신한 사람은 문자가 원 문서와는 다른 글꼴 및 포맷으로 형성되어 있는 경우에도 문서가 원 문서의 복제본인지를 알 수 있다. 화상 및 음성 정보의 디지털 표현에도 이와 유사한 의미 정보가 존재한다. 화상의 경우, 아날로그 형태를 접한 사람이 그 아날로그 형태가 원 화상의 복제본(화상 질이 나빠졌음에도 불구하고)임을 인정하기 위해서는 이러한 정보가 필요하며, 이는 음성 정보의 경우에도 마찬가지이다.

문서가 영어로 작성된 경우, 문서의 의미 정보는 문서의 글자와 문장 부호이다. 문서가 디지털 형태로 작성되어 있는 경우, 이 문서는 디지털 영상으로 표현되거나 워드 프로세싱(문서 처리) 또는 인쇄에 사용되는 것과 같은 문자 언어(text representation language)로 표현될 수 있다. 전자의 경우에는 광학 문자 인식(optical character recognition, OCR) 기술을 영상에 적용하여 글자와 구두점을 얻을 수 있으며, 후자의 경우에는 문자 언어로 문자와 문장 부호를 표현하는 데 사용되는 코드를 분석(parsing)하여 디지털 표현을 해석할 수 있다. 문서가 아날로그 형태로 작성된 경우, 아날로그 형태의 문서를 스캐닝하여 디지털 영상을 생성하거나 스캐닝에 의해 생성된 디지털 영상에 OCR 기술을 적용할 수 있다.

의미 정보를 사용한 아날로그 형태의 인증: 도 2 및 도 3

의미 정보가 아날로그 형태로 존재해야 하기 때문에, 의미 정보는 아날로그 형태로부터 판독될 수 있으며 의미 정보를 사용하여 새로운 다이제스트를 연산 처리할 수 있다. 이와 유사하게 디지털 표현의 의미 정보로부터 구(old) 다이제스트가 생성되면, 아날로그 형태로부터 구 다이제스트를 판독할 수 있으며, 전술한 인증 방법과 마찬가지로 새로운 다이제스트와 구 다이제스트를 비교하여 아날로그 형태의 인증 여부를 결정할 수 있다.

도 2는 구 다이제스트를 아날로그 형태(203)와 결합하기 위한 기술(201)을 도시한 도면이다. 아날로그 형태(203)는 의미 정보(205)를 포함하며, 여기서 아날로그 형태(203)는 인쇄되거나 팩스로 전송된 문서이며, 의미 정보(205)는 아날로그 형태(203)의 문자-숫자 문자의 일부 또는 전체이다. 아날로그 형태(203)가 생성되기 얼마 이전에, 아날로그 형태(203)를 생성하는 디지털 표현의 의미 정보(205)를 사용하여 의미 다이제스트(207)를 생성하는데, 의미 다이제스트(207)는 아날로그 형태(203)가 인쇄되면 의미 정보(205)가 없는 위치에서 아날로그 형태(203)와 결합된다. 일부 실시예에서는 의미 다이제스트(207)가 원 디지털 표현에 추가될 수 있으며, 다른 실시예에서는 아날로그 형태가 생성되기 직전에 추가될 수 있다. 아날로그 형태(203)로부터 검출할 수 있는 것이면 어느 것이나 의미 다이제스트(207)의 표현으로 사용할 수 있는데, 기술(201)에서는 의미 다이제스트(207)가 가시적 바 코드이다. 물론 의미 다이제스트(207)는 추가 정보를 포함할 수 있다. 예를 들어 전술한 바와 같이 암호화될 수 있으며, 의미 다이제스트(207)를 해독하는 데 필요한 공용 키를 소유하고 있는 사용자의 식별자(identifier)를 포함할 수 있다. 이 경우 의미 다이제스트(207)는 아날로그 형태에서도 살아남는 디지털 서명이다.

워터마크 방법을 사용하는 경우, 도 3에 도시되어 있는 바와 같이 의미 다이제스트를 아날로그 형태에 시각적으로 추가할 수 있다. 기술(301)에서, 아날로그 형태(303)는 의미 정보(305)를 포함한다. 전술한 바와 같이 아날로그 형태(303)를 생성하기 전에 아날로그 형태(303)를 생성하는 디지털 표현의 의미 정보를 사용하여 의미 다이제스트(207)를 생성한다. 그러나 이 때 디지털 표현으로부터 아날로그 형태가 생성되기 전에 디지털 표현에 추가되며 도 2의 바 코드와 마찬가지로 아날로그 형태의 생성에도 잔존하는 의미 다이제스트(207)가 워터마크(307)와 결합된다. 워터마크 판독기는 아날로그 형태(303)를 스캐닝함으로써 생성된 디지털 영상으로부터 워터마크(307)를 판독할 수 있으며, 그 결과 워터마크(307)로부터 의미 다이제스트(207)를 복구할 수 있다. 가시적 의미 다이제스트의 경우와 마찬가지로, 워터마크(307)의 의미 다이제스트는 암호화되어 디지털 서명의 기능을 할 수 있다.

의미 다이제스트를 아날로그 형태에 추가: 도 4

도 4는 의미 다이제스트를 아날로그 형태(203)에 추가하는 시스템(401)에 대해 도시하고 있다. 이 공정은 내용에 의미 정보(205)가 들어 있는 디지털 표현(403)에서 시작한다. 디지털 표현(403)은 의미 판독기(405)에 수신되며, 의미 판독기(405)는 디지털 표현(403)으로부터 의미 정보(205)를 판독한다. 의미 판독기(405)의 동작은 의미 정보의 형태에 따라 다르다. 예를 들어 디지털 표현(403)이 문서를 표현하는 경우, 의미 정보의 형태는 문서가 표현되는 방식에 따라 달라진다. 문서가 비트 맵 영상으로 표현되는 경우, 의미 정보는 문자-숫자 문자의 비트 맵 영상이 될 수 있다. 문자-숫자 문자를 코드로 표현하는 다수의 문서 표현 중에서 하나의 문서 표현을 사용하여 문서가 표현되는 경우, 의미 정보는 문자-숫자 문자의 코드가 될 수 있다. 전자의 경우에 의미 판독기(405)는 광학 문자 인식(OCR)이 될 수 있으며, 후자의 경우에 의미 판독기(405)는 문자 코드를 검색하여 문서 표현을 간단하게 분석할 수 있다.

어떠한 경우이든 공정의 마지막 단계에서 의미 판독기(405)는 예를 들어 문자-숫자 문자에 해당하는 ASCII 코드와 같은 디지털 표현(403)으로부터 추출된 일정한 형태의 의미 정보를 가지게 된다. 이러한 디지털 정보는 다이제스트 생성기(digest maker)(409)에 공급되며, 다이제스트 생성기(409)는 디지털 정보를 사용하여 알려진 여러 가지 방법 중 하나 이상의 방법으로 의미 다이제스트(411)를 생성한다. 의미 다이제스트가 생성되는 문서의 종류 및 사용 목적에 따라, 의미 다이제스트는 새로운 다이제스트와의 정확한 일치가 필요한 형태가 되거나 퍼지 일치가 필요한 형태가 될 수 있다. 디지털 표현(403) 및 의미 다이제스트(411)는 다이제스트 결합기(digest incorporator)(413)가 제공되는데, 다이제스트 결합기(413)는 의미 다이제스트(411)의 표현(207)을 디지털 표현과 결합하여 아날로그 형태(203)를 생성한다. 전

술한 바와 같이, 표현은 의미 정보(205)에 영향을 미치지 않는 방법으로 결합되어야 한다. 결합기(413)는 생성한 표현을 아날로그 형태 작성기(analog form producer; 415)에 출력하며, 아날로그 형태 작성기(analog form producer; 415)는 통상적인 방법으로 아날로그 형태(203)를 생성한다. 물론 아날로그 형태(203)는 의미 정보(205) 및 의미 다이제스트(411)의 표현(207)을 포함한다. 여기서는 바코드를 사용하지만, 이와 동등한 방법으로서 표현(207)이 아날로그 형태(303)에서처럼 워터마크의 일부가 될 수 있다. 부품(405, 409, 413)은 디지털 컴퓨터 시스템에서 실행되는 프로그램으로 구현될 수 있으며, 아날로그 형태 작성기(415)로는 아날로그 형태를 출력할 수 있으면 어느 장치나 될 수 있다.

의미 다이제스트를 가지는 아날로그 형태의 인증

도 5는 의미 다이제스트(207)를 가지는 아날로그 형태(503)를 인증하기 위한 시스템(501)을 예시한다. 아날로그 형태(503)는 의미 다이제스트 판독기(semantic digest reader)(505) 및 의미 판독기(507)에 제공된다. 의미 다이제스트 판독기(505)는 의미 다이제스트(207)를 판독한다. 의미 다이제스트(207)가 바코드인 경우, 의미 다이제스트 판독기(505)는 바 코드 판독기가 된다. 의미 다이제스트(207)가 디지털 워터마크에 포함되어 있는 경우, 의미 다이제스트 판독기(505)는 스캐너로부터 입력을 수신하는 디지털 워터마크 판독기이다. 의미 다이제스트(505)를 해독해야 하는 경우, 이는 의미 다이제스트 판독기(505)에 의해 수행된다. 일부 경우에, 암호화된 의미 다이제스트를 적당한 키를 가지는 원격 위치로 전송해야 할 때도 있다.

의미 판독기(507)는 의미 정보(305)를 판독한다. 아날로그 형태(503)가 문서인 경우, 의미 판독기(507)는 OCR 소프트웨어에 출력을 제공하는 스캐너이다. 다른 영상과 마찬가지로, 스캐너는 의미 정보(305)를 이루는 영상의 특징을 분석하기 위해 필요한 모든 영상 분석 소프트웨어에 출력을 제공한다. 아날로그 형태(503)가 음성인 경우, 음성은 음성 분석 소프트웨어로 입력된다. 의미 데이터(509)로 축소된 의미 정보는 의미 다이제스트 생성기(511)에 제공되며, 의미 다이제스트 생성기(511)는 이 정보로부터 새로운 의미 다이제스트(513)를 생성한다. 이를 위해, 구 의미 다이제스트(515)를 생성하기 위해 사용된 기술과 동일한 기술을 사용한다. 비교기(517)는 구 의미 다이제스트(515)를 새로운 의미 다이제스트(513)와 비교하고, 이들 다이제스트가 일치되는 경우에는 아날로그 형태(203)가 인증되었음을 가리키는 비교 결과(519)를 출력하고, 이들 다이제스트가 일치되지 않는 경우에는 이들이 인증되지 않았음을 가리키는 비교 결과(519)를 출력한다. 여기서 사용되는 "일치"의 의미에 대해서는 아래에서 상세하게 설명한다.

의미 다이제스트 "일치"

다이제스트를 사용하여 디지털 표현을 인증하는 경우에는, 구 다이제스트와 새로운 다이제스트가 정확하게 일치하여야 한다. 그 이유는 대부분의 디지털 상황(contexts)의 경우에 "대략적으로 정확한" 데이터는 쓸모가 없으며, 다이제스트에 일반적으로 사용되는 일방향 해시는 "암호법"에 의한 것이기 때문이다. 즉 다이제스트의 값이 해시 기능을 사용하여 생성한 값과는 아무 관련이 없거나, 더 실제적으로는 디지털 표현에서 한 비트만 변화하더라도 해시 기능이 생성한 값이 크게 변화하기 때문이다. 때문에 이들 다이제스트의 동일성(equality)을 비교해야 한다.

아날로그 형태의 인증 시에 다이제스트를 동일하게 하는 것은 어렵다. 그 이유는 아날로그 형태로부터 의미 정보를 판독할 때 오류가 발생하기 쉽기 때문이다. 예를 들어 수년간의 노력 끝에, OCR 기술은 포맷이 단순하며 적절한 형태의 글꼴을 사용하여 작성된 깨끗한 문서의 복제본인 경우, 대체로 98 %의 정확도로 문자를 인식할 수 있는 정도까지 발달하였다. 이러한 오류율은 대부분의 목적에는 완전히 부합하는데, 임의의 크기의 의미 정보에 대하여 구 의미 다이제스트를 생성하기 위해 사용된 의미 데이터와 98 % 동일한 의미 데이터로 새로운 다이제스트를 작성하는 경우에는 새로운 다이제스트와 구 다이제스트는 거의 동일하지 않다. 한편 아날로그 형태로부터 얻어진 의미 데이터가 디지털 표현으로부터 얻어진 의미 데이터와 98 % 동일한 경우, 아날로그 형태는 실제로 디지털 표현의 인증받은 복제본일 가능성이 아주 높다.

정확한 일치(precise matches)

물론 의미 정보의 크기가 제한되고 한정되는 경우, 정확하게 동일한 다이제스트를 요구할 수 있다. 예를 들어 수표 또는 식별 카드와 같은 것의 특정 필드를 판독하는 경우 다수의 오류가 제거될 수 있으며, OCR 장비는 필드의 내용 특성을 고려하도록 프로그래밍된다. 예를 들어 필드가 숫자만을 포함하는 경우, OCR 장비는 글자 o와 0를 숫자 0으로 처리하고, 글자 l, i 또는 I를 숫자 1로 처리하도록 프로그래밍된다. 더욱이 일치가 이루어지지 않으며 OCR 장비가 쉽게 혼동할 수 있는 문자를 의미 정보가 포함하는 경우, 그 문자를 그것과 혼동되는 문자들 중 하나로 바꾸어 다이제스트를 다시 연산 처리할 수 있으며, 재 연산 처리된 다이제스트를 사용하여 비교 작업을 다시 시작할 수 있다.

퍼지 일치(fuzzy matches)

의미 정보가 매우 제한되지 않은 경우, 아주 유사한 의미 정보가 아주 유사한 다이제스트를 생성하도록 다이제스트를 작성해야 한다. 따라서 이 때에는 두 다이제스트의 동일성 여부를 따지는 것이 아니라 이들 사이의 차이가 임계값 이내인지를 결정하기 위한 판단한다. Marc Schneier 및 Shin-Fu Chang의 논문 "A Robust Content Based Digital Signature for Image Authentication"(Proceedings of the 1996 International Conference on Image Processing)은 디지털 영상 부문과 관련된 어려움을 해결하는 기술에 대해 기재하고 있다. 디지털 표현을 사용하여 아날로그 형태를 생성하는 경우에 발생하는 정보 손실 및 아날로그 형태를 판독하는 경우에 발생하는 오류로 인해서는 문제가 발생하지 않으며, 영상의 "손실성(lossy)" 압축 즉 정보 손실을 야기하는 기술을 사용하는 압축으로 인하여 문제가 발생한다. 디지털 표현의 압축으로부터 정보가 손실되기 때문에, 압축 표현 및 비압축 표현이 동일한 의미 정보를 포함하더라도 암호법을 사용하여 압축된 디지털 표현으로부터 작성된 다이제스트는 압축 이전의 디지털 표현으로부터 작성된 다이제스트와 동일하지 않다. 일반적으로 Schneier 논문에 기재된 기술은 영상 특징(feature)의 공간적 위치와 같이 압축에 의해 영향을 받지 않는 영상의 문자로부터 다이제스트 값을 계산함으로써 이러한 문제들을 처리한다. 영상 시퀀스가 존재하는 경우, 영상 시퀀스의 순서를 사용하여 다이제스트 값을 계산한다.

아날로그식 접근방법을 사용하여 의미 다이제스트를 연산 처리하여 아날로그 형태를 인증할 수도 있다. 예를 들어 문서용 의미 다이제스트는 다음과 같이 연산 처리될 수 있다.

1. 의미 다이제스트를 "0"으로 유지하는 다이제스트 스트링(digest string)의 현재 길이를 설정함.

2. 문서의 제1 문자-숫자 문자에서부터 시작하여, 문서 내에 문자가 발견되지 않을 때까지 다음 단계를 수행한다.

a. 다음 문자 군을 선택한다.

b. 선택된 군에 대하여,

ⅰ. 다수의 OCR 오류를 야기하는 0, 0, o, l, l, l, 1 또는 c, e와 같은 군에 속하는 문자를 "무정의(don't care)문자"로 대체한다.

ⅱ. 문자 군으로부터 해시 값을 설정한다.

ⅲ. 해시 값을 의미 다이제스트 스트링에 첨부한다.

c. 단계 (a)로 돌아간다.

3. 문서 내에 문자가 더 이상 발견되지 않는 경우, 다이제스트 스트링으로부터 의미 다이제스트를 작성한다.

이러한 방법으로 연산 처리하는 경우, 의미 다이제스트 스트링의 시퀀스 값은 다이제스트를 연산 처리하는 데 사용되는 시퀀스 각각의 문자 순서에 영향을 미친다. 아날로그 형태로부터 연산 처리되는 새로운 의미 다이제스트의 시퀀스 값이 구 의미 다이제스트의 시퀀스 값과 매우 높은 비율로 일치하는 경우, 문서가 동일한 의미 정보를 포함하고 있을 확률이 높다.

아날로그 형태의 인증을 적용한 예

하나의 예는 통상적으로 기록 문서를 인증하는 것이다. 문서가 임의의 길이로 작성되고 다이제스트가 상당한 양의 내용으로부터 연산 처리된다는 점에서, 다이제스트는 퍼지 일치를 허용하는 방식으로 연산 처리되어야 한다. 다이제스트가 문서의 매우 한정된 필드로부터 연산 처리되는 경우, 정확한 일치를 사용할 수 있다.

다른 예는 전자 화폐, 전자 수표 및 은행 카드와 같은 금융 문서를 인증하는 것이다. 여기서 다이제스트가 연산 처리되는 필드는 매우 제한되며, 보안성을 위해 정확한 일치를 요구할 수 있다. 이들 모든 경우에, 전술한 바와 같이 다이제스트 또는 의미 정보 자체를 암호화하여 디지털 서명을 생성할 수 있다.

일반적인 종이 및 디지털 화폐

현재 디지털 화폐는 순전히 전자 지불 매체이다. 소정의 품목의 디지털 화폐는 고유 일련 번호 및 디지털 서명으로 이루어진다. 인증을 위해 의미 정보를 사용한다면, 디지털 화폐는 디지털 종이 화폐로 인쇄될 수 있다. 종이 화폐는 배경 그림, 일련 번호 및 금액이 표시된 전자 영상으로부터 인쇄된다. 일련 번호 및 금액은 의미 정보이다. 일련 번호 및 금액을 사용하여 디지털 서명을 작성할 수 있으며, 디지털 서명을 전자 워터마크로서 배경 그림에 삽입할 수 있다. 종이 화폐는 돈을 지급하는데 필요한 모든 기계에 의해 인쇄될 수 있다. 따라서 ATM은 종이 화폐 대신에 디지털 종이 화폐를 지급할 수 있다. 이와 유사하게 자동 판매기는 디지털 종이 화폐를 사용하도록 변경될 수 있으며, 상인 또한 디지털 종이 화폐를 사용할 수 있다. 디지털 종이 화폐는 종이 화폐와 동일한 방법으로 사용될 수 있다. 상인(또는 자동 판매기)이 계산 시에 디지털 종이 화폐를 받는 경우, 그는 특별한 스캐너(OCR 기술 및 워터마크 판독기)를 사용하여 인쇄된 영상으로부터 워터마크(즉 일련 번호 및 금액)를 검출하고, 확인(verification)을 위해 현재의 신용카드의 경우와 동일한 방법으로 이를 은행으로 전송한다.

디지털 수표

디지털 종이 화폐의 경우에 사용되는 기술과 동일한 기술을 사용하여 디지털 수표를 작성할 수 있다. 디지털 수표는 배경 그림, 은행 계좌 번호, 지불 금액 및 지불자의 성명을 포함한다. 지불자의 개인 키를 사용하여 적어도 은행 ID 및 지불 금액으로부터 디지털 서명을 생성하며, 디지털 서명은 배경 그림의 전자 워터마크로 삽입된다. 금액을 입력하고, 지불자의 개인 키를 사용하여 은행 계좌 번호 및 금액으로부터 디지털 서명을 생성하고, 디지털 서명을 배경 그림에 삽입하는 3단계의 과정을 통해 디지털 수표를 작성한다. 은행은 디지털 수표로부터 워터마크를 검출하고, 지불자의 공용 키를 사용하여 디지털 서명을 해독하고, 영상으로부터의 은행 계좌 번호와 금액을 수표 표면의 은행 계좌 번호와 금액과 비교함으로써 수표를 검사한다. 디지털 수표는 전자 형태 또는 종이 형태로 사용될 수 있다. 후자의 경우에는, 종이 수표로부터 워터마크를 판독하기 위해 스캐너(OCR 기술 및 워터마크 판독기)가 필요하다.

식별 카드의 인증

전술한 디지털 종이 화폐 또는 디지털 수표 인증 기술은 은행 카드를 포함하는 식별 카드를 사용하여 구현될 수 있다. 카드의 표면에 표시된 카드 번호 또는 기타 다른 식별 정보는 디지털 서명으로 암호화되어, 은행 카드의 배경 그림에 디지털 워터마크로 내장된다. 카드를 발행한 기관의 개인 키를 사용하여 암호화를 구현할 수 있다. 상인은 스캐너를 사용하여 카드로부터 디지털 서명(즉 카드 번호 또는 다른 ID)을 검출하고, 서명을 카드에 내장된 인증과 비교한다. 물론 이러한 기술은 종래의 홀로그래피 로고(holographic logo)와 같은 종래의 인증 기술과 결합될 수 있다.

활성 워터마크: 도 6 내지 도 8

지금까지 디지털 워터마크는 라벨 이상의 그 무엇도 아니었다. 디지털 워터마크는 디지털 표현의 소유권자 및 저작자의 식별자 및 예를 들어 디지털 표현이 복제 또는 변경될 수 있는지를 제어하는 액세스 제어 정보 등의 통상적으로 포함되는 정보를 가진다. 그러나 모든 종류의 정보를 디지털 워터마크에 위치시킬

수 있다. 워터마크 내의 정보가 실행될 동작을 기술하는 경우, 워터마크는 활성화되며, 활성 워터마크를 포함하는 디지털 표현 역시 활성화된다. 이는 예를 들어 Microsoft Active Documents와 마찬가지로, 프로그램 내의 디지털 표현을 밀폐(encapsulation)하는 일반적인 실행과는 반대이다. 디지털 워터마크가 디지털 시스템에 사용되기 때문에, 워터마크를 동작시키는 가장 간단한 방법은 디지털 표현이 현재 상주하는 컴퓨터 시스템에 의해 실행될 수 있는 프로그램 코드를 포함하는 것이다. 함수의 관점에서 보면, 컴퓨터 시스템이 코드를 실행할 수 있는 모든 언어로 코드를 작성할 수 있다. 그러나 실제로 코드는 최근의 컴퓨터 시스템에 의해 번역(interpretation)되는 Java™ 또는 Perl과 같은 언어로 기록되는 것이 가장 바람직하다.

도 6은 활성 워터마크(619)를 생성하는 시스템(601)의 개략도이다. 워터마크는 이전과 마찬가지로 소유권자 정보(605), 액세스 정보(607) 및 소유권자-지정 정보(owner-defined information; 609)를 포함하고 추가로 코드(611)를 포함하는 워터마크 정보(603)로 이루어진다. 코드(611)는 소정의 종류의 디지털 표현을 위한 표준 코드가 될 수 있으며 또는 소정의 디지털 표현을 위한 코드를 특별하게 지정할 수 있다. 물론 코드(611)는 워터마크 정보 내의 다른 정보를 데이터로 사용할 수 있다. 워터마크 정보(603) 및 디지털 표현(613)은 워터마크 생성기(615)에 입력되며, 워터마크 생성기(615)는 디지털 표현(613)이 워터마크 정보(603)로부터 워터마크(619)를 포함하도록 변경된 디지털 표현(617)을 출력한다. 워터마크 정보(603)가 코드(611)를 포함하기 때문에, 워터마크(619)는 활성 워터마크이다.

도 11은 바람직한 실시예의 액세스 정보(607)를 도시한 도면이다. 액세스 정보(607)는 다음과 같은 필드를 포함한다.

· 사용자가 액세스할 액세스의 종류를 표시하는 8 비트의 허용 필드(permission field; P). 액세스의 종류에는 표시를 허용하는 액세스, 국부 복제물의 저장을 허용하는 액세스 및 인쇄를 허용하는 액세스가 있다.

· 디지털 표현 콘텐츠의 감도 정도를 표시하는 값을 가지는 4 비트의 감도 필드(sensitivity field);

· 디지털 표현의 위치 결정을 허용하는 IP 어드레스를 포함하는 32 비트의 위치 허용 필드(allowed location field); 및

· 디지털 표현의 사용이 허용되는 구간의 시간을 포함하는 32 비트의 구간 허용 필드(allowed period field).

도 7은 코드(611)에서 발견될 수 있는 프로그램의 일례이다. 프로그램(701)은 Java 프로그래밍 언어로 작성된다. 그 후 프로그램(701)은 Java 번역기에 의해 번역되는 Java 바이트부호(bytecode)로 컴파일링된다. 이들 바이트부호는 디지털 워터마크에 포함된다. 프로그램(701)이 실행되는 경우, 활성 워터마크를 포함하는 디지털 표현(617)이 표시되었음을 표시하는 메시지는 인터넷을 통해 디지털 표현(617)의 표시를 감시하도록 설정된 시스템으로 전송되어, 라이센스 비용(license fee)을 연산 처리한다. 코드의 라인(703)은 데이터그램을 감시 시스템(monitoring system)으로 전송할 수 있는 소켓(socket) s를 설정한다. 코드의 라인(709)은 "syscop.crg.edu"(705)에서 지정한 감시 시스템의 현재 인터넷 어드레스 a를 찾는다. 라인(1715)은 메시지에 대한 새로운 데이터그램 패킷을 생성하며, "XYZ Displayed" 및 인터넷 어드레스 a.를 포함한다. 라인(1719)은 소켓 s와 연관된 send 연산을 사용하여 인터넷을 통해 a에 의해 지정된 목적지로 전달되는 메시지를 전송한다.

도 8은 활성 워터마크(619)의 코드를 실행하는 시스템(801)을 도시한 도면이다. 활성 워터마크(619)를 포함하는 디지털 표현(617)은 워터마크 판독기(803)에 입력되고, 워터마크 판독기(803)는 활성 워터마크(619)로부터 워터마크 정보(603)를 추출한다. 워터마크 정보(603)는 워터마크 판독기(803)가 코드 번역기(805)에 제공하는 코드(611)를 포함한다. 코드 번역기(805)는 코드(611)를 번역하여, 코드 번역기(805)를 구동하는 컴퓨터 시스템에 의해 실행 가능한 명령어를 제공한다. 일부 실시예에서는 코드 번역기가 컴퓨터 시스템에 의해 제공되는 Java와 같은 표준 언어용 번역기이며, 다른 실시예에서는 워터마크 판독기(803)의 구성요소로 제공될 수 있는 번역기(805)가 될 수 있다. 일부 실시예에서, 코드(611)는 활성 워터마크용으로 특별하게 설계된 언어로 작성될 수 있다.

활성 워터마크(619)는 활성 워터마크를 판독하는 컴퓨터 시스템이 활성 워터마크에 포함된 코드에 의해 기술될 수 있는 모든 동작을 실행할 수 있도록 한다. 이 때 코드가 워터마크의 일부라는 사실 때문에 한계가 발생한다. 이들 한계 중의 하나가 코드의 크기인데, 워터마크에 포함된 코드는 비교적 짧아야 한다. 정보 손실을 야기하지 않는 "비손실성(non-lossy)" 압축 기술을 사용하여 코드를 압축함으로써 이러한 한계를 완화시킬 수 있다. 다른 한계는 워터마크의 손상이 코드의 손상을 야기할 수 있으며, 따라서 디지털 표현(617)이 "손실성" 조작과 연관되어 있는 경우 즉 조작에 의해 디지털 표현(617)의 정보가 손실되는 경우, 활성 워터마크가 제대로 동작하지 않는다는 것이다. 이러한 손실성 조작의 예로는, 디지털 표현의 편집, 디지털 표현의 하나의 포맷으로부터 다른 포맷으로의 손실성 번역, 디지털 표현의 손실성 압축 및 구 디지털 표현으로부터 생성되는 아날로그 형태로부터 새로운 디지털 표현을 생성하는 것(예를 들어 종이 복제본의 문서로부터 워터마크를 판독함으로써 코드를 얻는 경우) 등이 있다.

물론 전술한 바와 같이 다이제스트의 정확한 일치와 연관된 기술을 사용하여 손상된 워터마크 또는 아날로그 형태로부터 코드를 복구할 수 있으며, 이 기술이 성공적인 경우에는 손실성 조작이 발생하는 경우에도 활성 워터마크를 사용할 수 있다. 예를 들어 아날로그 형태의 워터마크는 인증 정보 외에도 코드를 포함할 수 있다. 복사기가 워터마크 판독기 및 활성 워터마크에 사용되는 코드의 번역기를 포함하는 경우, 예를 들어 활성 워터마크는 복사기가 아날로그 형태를 복사하는 것을 방지할 수 있다.

활성 워터마크를 사용하여 다음과 같은 동작을 수행할 수 있다.

· 워터마크를 포함하는 디지털 표현의 처리 방식을 개별화(customization)한다. 코드(611)는 디지털 표현의 종류를 다르게 할 수 있으며, 단일 디지털 표현으로 특화될 수 있다.

· 디스플레이, 복제, 인쇄 또는 편집이 수행될 때마다 디지털 표현에 의해 메시지를 전송한다. 예를

들어 서버로부터 웹 서버 상에 저장된 활성 워터마크를 가지는 문서가 다운로드될 때마다, 활성 워터마크는 요금청구 정보(billing information)를 포함하는 메시지가 요금청구용 서버로 전송되도록 할 수 있다.

· 디지털 표현이 동작 및 디지털 표현의 사용을 제어하는 국부적으로 가능한 정보를 획득할 수 있다.

· 사용자가 액세스 정보(603)에 의해 허용되지 않는 무언가를 하려고 하는 경우, 디지털 표현이 보호 동작(protective action)을 한다. 보호 동작에는 메시지 전송을 통해 경고하거나, 워터마크를 포함하는 디지털 표현을 파괴하기 위한 의도된 동작을 차단하는 것 등이 있다.

워터마크 에이전트(watermark agents)

다른 모든 디지털 데이터와 마찬가지로 쉽게 디지털 표현을 복제하고 네트워크를 통해 배포할 수 있기 때문에, 디지털 표현은 소유권자에게 특별한 문제점을 안겨준다. 그러나 이들 디지털 데이터의 특성 때문에 디지털 표현의 배포를 자동으로 감시할 수 있으며 워터마크가 있는 디지털 표현을 사용할 수 있다. 그 방법 중의 하나가 워터마크 스파이더(watermark spider)이다. 종래 기술에 대한 설명에서 기술한 바와 같이, 워터마크 스파이더는 웹 페이지를 URL을 따라 워터마크를 검색하고 검사한다. 워터마크 스파이더가 관련된 워터마크를 발견하는 경우, 워터마크 스파이더는 이를 감시 프로그램(monitoring program)에 보고한다. 워터마크 스파이더와 관련된 두 가지 문제점이 있다. 첫 번째 문제점은 워터마크 스파이더의 사용이 일반 대중이 사용가능한 URL에 의해 액세스 가능한 디지털 표현으로 제한된다는 점이다. 따라서 워터마크 스파이더는 WWW 서버의 반대 측인 WWW 클라이언트 상에서는 디지털 표현의 복제물을 찾을 수 없다. 다른 문제점은 스파이더가 네트워크를 통해 검사될 디지털 표현 각각을 인출해야 한다는 것이다. 종종 디지털 표현의 크기가 크기 때문에, 각각의 디지털 표현을 인출해야 하는 필요성에 의해 네트워크 트래픽의 양이 대체로 증가한다.

이들 문제점은 네트워크 워터마크 에이전트(network watermark agent), 즉 네트워크를 통해 관련된 디지털 표현을 저장할 수 있는 시스템에서 시스템으로 순회하는 워터마크 감시 장치(watermark monitor)에 의해 해결될 수 있다. 각각의 시스템에서, 워터마크 에이전트는 시스템의 파일 시스템을 검사하여 관련된 워터마크를 가지는 디지털 표현을 찾는다. 워터마크 에이전트가 이러한 워터마크를 발견하는 경우, 워터마크 에이전트는 이를 통지하는 메시지를 네트워크를 통해 감시 프로그램에 전송할 수 있다. 따라서 워터마크 에이전트는 대중적인 URL을 통해 사용할 수 없으며 비교적 드물게 이용되는 네트워크 대역폭을 사용하는 디지털 표현을 감시할 수 있으며, 디지털 표현과 비교하여 작은 메시지만을 전송할 수 있다. 아래에서, 워터마크 에이전트의 생성 및 시스템 동작에 대해 상세하게 설명한다.

워터마크 에이전트의 생성: 도 9

도 9는 네트워크(103)를 통해 워터마크 에이전트(925)를 생성하고 배포(dispatch)하며 워터마크 에이전트로부터의 메시지에 응답하는 워터마크 감시 시스템(901)을 도시한다. 워터마크 에이전트(925)는 네트워크(103) 상에서 하나의 노드에서 다른 노드로 전송할 수 있는 프로그램이다. 워터마크 에이전트(925)는 노드 각각에서 워터마크가 있는 문서를 조사하고, 조사 결과를 포함하는 메시지(935)를 감시 시스템(901)으로 전송하며, 메시지 처리기(message handler; 920)는 종종 정보를 관리 데이터베이스(903)에 추가함으로써 메시지를 처리한다.

더 상세하게 설명하면, 에이전트(925)는 두 개의 주요 부분을 가지는데, 그 중 하나는 에이전트(925)가 노드에 도달하는 경우 실행되는 에이전트 코드(927)이며, 다른 하나는 에이전트(925)가 코드를 실행하고 다음 노드로 이동할 때 사용하는 정보를 포함하는 에이전트 데이터(929)이다. 적어도 에이전트 코드(927)는 워터마크를 포함할 수 있는 파일을 찾기 위해 노드를 검색하는 코드, 모든 필요한 메시지를 생성하고 이 메시지를 감시 시스템(901)으로 전송하는 코드, 에이전트(925)를 클론화(clone)하는 코드 및 이 클론을 다음 노드로 전송하는 코드를 포함한다. 활성화 워터마크에 코드를 사용하는 경우, 노드에서 실행될 수 있는 모든 언어로 코드(927)를 작성할 수 있으며, Java 같은 표준 언어 또는 특별 워터마크 에이전트 언어를 사용할 수 있다.

도 12는 워터마크 표시 에이전트(925)가 실행할 수 있는 Java 언어로 작성된 코드(1201)의 일례를 도시한다. 코드(1201)는 에이전트(925)가 현재 영상 파일을 찾는 네트워크 노드의 파일 시스템을 검색하고, 영상 파일 각각에 대하여 워터마크를 검사하고, 워터마크를 발견하는 경우 워터마크 및 노드가 요구하는 동작을 수행하고, 수행된 동작의 리스트를 포함하는 메시지를 작성한다.

더 상세하게 설명하면, 코드(1201)는 두 개의 주요 부분, 초기화 부분(1203) 및 검사 루프(checking loop; 1213)를 가진다. 초기화 부분(1203)의 제1 단계는 노드의 파일 시스템의 파일을 필터링하기 위해 파일 필터를 사례화(instantiate)하는 것이다(1205). 그 후 영상 파일을 찾는 필터 기능을 사용하여 파일 시스템의 영상 파일 이름 filenames 리스트를 생성한다(1207). 그 결과 에이전트가 워터마크를 검사하기 위해 필요로 하는 노드의 환경 정보를 검색하고, 가변 env 상태가 된다(1209). 마지막으로 results로 불리는 데이터 구조를 생성하여 워터마크 검사의 결과를 유지한다(1211).

루프(1213)에서는, filenames의 파일 각각에 대하여 워터마크를 검사하고(1215), 워터마크가 발견되는 경우 단계(1217)에서 지시하는 동작을 수행하고, 워터마크의 콘텐츠를 환경 정보와 비교하여 match라 불리는 결과를 얻는다(1219). 다음으로 match는 match 값에 의해 결정되는 동작을 수행하는 함수로 전달되어, 동작의 결과를 표시하는 값 result로 돌아간다(1221). 마지막으로 result가 데이터 구조 results에 추가된(1223) 후에, results로 돌아간다(1225). 워터마크 에이전트의 사용 방법에 따라 results는 메시지를 감시 시스템(901)으로 전송할 수 있다.

에이전트 데이터(929)에 대해 상세하게 설명하면, 에이전트 데이터(929)는 맵(map)(931), 디지털 표현 기술(digital representation description, DR DESC)(933), 키(key)(934) 및 파라미터(parameter)(921)를 포함한다. 맵(931)은 네트워크(103) 상의 어드레스 리스트이다. 어드레스 각각은 에이전트(925)가 작동할 수 있는 환경을 제공할 수 있는 네트워크(103)의 엔티티(entity)를 지정한다. 어드레스는 예를 들어 이-메일 어드레스 또는 IP 어드레스가 될 수 있다. 디지털 표현 기술(933)은 에이전트가 찾고 있는 디지털 표현을 기술하는 모든 정보가 될 수 있다. 파일 네임용 필터가 존재할 수 있으며, 또한 워터마크로부

터 식별 정보가 존재할 수 있다. 예를 들어 검사될 파일이 .bmp 파일인 경우, 필터는 *.bmp를 지정하고 .bmp 확장자를 가지는 모든 파일이 검사될 것임을 표시할 수 있다. 키(934)는 워터마크를 판독하기 위해 필요한 워터마크 키를 포함하며, 감시 시스템(901)에 전송되는 메시지를 암호화하는 데 사용되는 키를 포함한다. 모든 가능한 기술을 사용하여 키 보안성을 유지할 수 있다. 바람직한 실시예에서, 파라미터는

에이전트가 전송하는 메시지의 이메일 어드레스;

에이전트(925)가 액세스하지 않은 파일에 대하여 보고할 것인지;

최종 감시 일자 및 그 일자 이후에 갱신된 파일만을 검사할 것인지;

활성 워터마크(619)의 코드(611)를 실행할 것인지; 및

에이전트(925)의 종료 조건

을 포함한다.

에이전트(925)는 디지털 표현 관리자(digital representation manager)(131)의 구성성분으로 구현될 수 있는 에이전트 발생기(923)에 의해 생성된다. 에이전트 발생기(923)는 관리 데이터베이스(131)의 정보로부터 에이전트(925) 및 에이전트 파라미터(921)를 생성하는데, 여기에 도시된 것은 감시 시스템(901)의 사용자에 의해 반복적으로 제공되며 관리 데이터베이스(903)에 저장될 수 있는 에이전트 및 에이전트 파라미터이다. 관리 데이터베이스(903)의 정보는 파라미터(921) 및 관리 데이터베이스(903)의 다른 정보와 함께 사용되는 다수의 템플리트 중에서 하나인 에이전트 템플리트(905(i))를 포함하여, 서로 다른 종류의 에이전트(925)에 대한 에이전트 코드(927)를 생성한다. 서스피서스 사이트(suspicious site; 907)는 검사할 가치가 있는 네트워크 위치의 리스트이다. 물론 서스피서스 사이트(907) 리스트에 올라야 하는 사이트에 대한 하나의 정보 소스는 이전에 할당된 에이전트로부터 수신된 메시지이다. 서스피서스 사이트(907) 및 네트워크 정보(909)를 함께 사용하여 에이전트(925) 내에 맵(931)을 생성한다. 최종적으로 디지털 표현 정보(911)는 에이전트가 찾고 있을 디지털 표현에 대한 정보를 포함한다. 이 정보를 사용하여 DR 기술(933)을 작성한다. 소정의 디지털 표현 또는 디지털 표현 군에 대한 정보(911(i))는 디지털 표현의 워터마크용 워터마크 키(913), 및 소유권자 ID(915), 사용자 ID(917) 및 사용 허용 정보(919)를 포함하는 워터마크 정보를 포함할 수 있다. 사용자 ID(917)는 디지털 표현을 다운로드한 사용자를 식별한다. 따라서 감시 시스템(901)이 에이전트(905)를 생성한 후에, 에이전트(925)는 에이전트를 클론화하고, 클론을 맵(931)에서 지정한 제1 엔티티를 위해 요구되는 종류의 메시지로 설정한다. 그 결과 에이전트(925)는 스스로 종료된다.

네트워크 노드의 워터마크 에이전트: 도 10

도 10은 워터마크 에이전트(925)에 의한 노드의 감시와 연관된 네트워크 노드(1001)의 구성요소를 도시한 도면이다. 구성요소는

· 에이전트(925)가 코드를 실행하고 메시지를 포함하는 에이전트(925)가 어드레스하는 엔티티인 환경을 제공하는 에이전트 엔진(agent engine)(1003);

· 에이전트(925)와 관련된 디지털 표현(DRS)(1023)을 포함하는 파일 기억장치(1031);

· 디지털 표현(1023)이 파일을 액세스할 수 있도록 하는 파일 시스템(1029);

· 워터마크를 판독하는 워터마크 판독기(1019); 및

· 코드가 에이전트(925)에서 사용되는 코드와 동일한 언어로 작성되는 경우, 에이전트(925)의 코드 및 활성 워터마크의 코드를 번역할 수 있는 코드 번역기(1011)

를 포함한다.

SS(1035)는 선택적인 보안 코프로세서(security coprocessor)인데, 그 기능에 대해서는 아래의 보안성에 대한 설명에서 상세하게 설명한다.

구성요소(1001)의 동작은 다음과 같다. 메시지를 포함하는 에이전트(925)가 네트워크(103)로부터 에이전트 엔진(1003)에 도달하는 경우, 에이전트 엔진(1003)은 메시지로부터 에이전트(925)를 추출하고, 편리한 시간에 코드 번역기(1011)를 사용하여 코드를 실행하기 시작한다. 물론 코드는 임의적(arbitrary) 동작을 수행한다. 일반적으로 다음의 동작을 수행한다.

1. 에이전트가 노드에 도달했음을 통지하는 메시지를 시스템(901)에 전송한다.

2. DR DESC(933)로부터 파일 필터를 구하고, 이를 스파이더(1009)에 전달하여 필터와 일치하는 파일 리스트를 생성한다.

3. 리스트 상의 파일 각각에 대해 다음을 수행한다.

a. 스파이더(1009)를 사용하여 파일용 파일 ID를 구한다.

b. 워터마크가 존재하는 경우 키(934)로부터의 워터마크 키를 사용하여 워터마크를 판독하는 워터마크 판독기(1019)에 파일 ID(1021)를 전달한다.

c. 워터마크 콘텐츠(1017)를 수신한다.

d. 코드(927)에서 지정한 대로 워터마크 콘텐츠(1017)를 처리한다. 메시지를 시스템(901)에 전송하는 것 또는 데이터(1013)를 실행하고 수신하기 위해 코드 및 데이터(1015)를 활성 워터마크로부터 코드 번역기(1011)로 전달하는 등의 처리가 있다.

4. 모든 파일을 처리한 경우

a. 방문 결과 및 방문할 다음 노드에 대한 요약 정보를 가지는 메시지를 감시 시스템(901)으로 전송한다.

b. 에이전트(925)의 클론을 생성하고 맵(931)에서 지정한 다음 어드레스로 클론을 전송한다.

c. 에이전트(925)를 종료한다.

전술한 바와 같이 워터마크 에이전트는 기본적으로 임의적인 동작을 수행할 수 있다. 워터마크 에이전트가 처리하는 문서가 활성 워터마크를 가지는 경우, 관련된 문서를 워터마크 에이전트의 코드와 활성 워터마크 코드로 분할하여 처리하는 다수의 방법이 존재한다. 예를 들어 전술한 실시예에서, 단계 3(d)은 단순히 문서의 활성 워터마크의 코드를 실행하는 것을 포함할 수 있다.

일반적으로 워터마크의 정보가 에이전트(925)가 파일을 발견하는 시간 또는 공간과 일치되지 않는 경우, 또는 시간 및 공간이 파일 액세스 특권에 부적당한 경우에, 단계 3(d)에서 수행되는 동작이 수행된다. 동작은 파라미터(921)의 파라미터가 지정하는 소정의 세트 중에서 하나의 동작이 될 수 있으며, 에이전트(925)의 코드(927)에 의해 정의되는 하나의 동작이 될 수 있으며, 활성 워터마크에 의해 정의되는 하나의 동작이 될 수 있다. 소정의 동작은 다음과 같다.

1. 파일의 감도 레벨이 매우 높은 경우, 파일을 파괴한다.

2. 감도 레벨이 중간 정도인 경우 파일을 안전 위치로 이동한다.

3. 감도 레벨이 낮은 경우에는

a. 로컬 관리자 또는 웹마스터에게 위반(violation)을 경고한다.

b. 수신인에게 위반을 경고하거나 또는

c. 파일 소유권자에게 위반을 알리는 메시지를 전송한다.

4. 감도가 매우 낮은 경우, 로컬 호스트 및 로컬 관리자를 교란하지 않고 감시 장치(901)에게 메시지를 전송한다.

워터마크 에이전트(925)는 다음 목적지로 향하기 전에, 감시 장치(901)로부터 다음 목적지에 대한 정보를 포함하는 메시지를 기다린다. 이 정보는 다음과 같은 정보를 포함한다.

· 에이전트가 목적지를 최종적으로 방문한 시간.

· 예를 들어 검사될 디지털 표현에 대한 상세한 정보와 같은 목적지에 대한 정보.

순회하지 않는(nontravelling) 워터마크 에이전트

워터마크 에이전트와 워터마크 스파이더의 중요한 차이는 워터마크 에이전트가 문서가 저장되거나 처리되는 시스템의 문서와 상호작용하며, 따라서 워터마크 스파이더에 비해 훨씬 더 많은 기능을 수행할 수 있다는 것이다. 이러한 차이에 의해, 워터마크 에이전트는 순회할 필요가 없으며, 시스템의 영구 구성요소로 간단하게 결합될 수 있다. 예를 들어 복사기는 복사될 종이 문서의 워터마크를 판독하는 워터마크 에이전트를 포함할 수 있으며, 워터마크가 문서 복제 불가를 표시하는 경우 워터마크 에이전트는 복사기에 의해 문서가 복제되는 것을 방지할 수 있다. 순회하지 않는 워터마크를 적용함으로써, 종이 디지털 화폐의 복제를 방지하는 중요한 결과를 얻을 수 있다.

물론 복사기가 네트워크에 액세스하는 경우, "순회하지 않는" 워터마크 에이전트가 네트워크를 통해 복사기로 이동하는 경우에도, 네트워크는 복사기의 워터마크 에이전트를 편리하게 갱신할 수 있다. 물론 "순회하지 않는" 워터마크 에이전트는 이와 유사한 방법으로 네트워크를 통해 액세스 가능한 모든 시스템으로 분배될 수 있다.

보안성 고려(security considerations)

일부의 경우에, 예를 들어 비공개 군사 또는 산업 네트워크 또는 시스템의 경우, 에이전트(925)는 취약 환경(hostile environment)에서 동작하지 않을 수 있으며, 감시 장치(901) 및 에이전트 엔진(1003)을 운영 체제의 내부 구성요소로 구현할 수 있다. 그러나 대부분의 경우에 에이전트(925)는 적어도 다음과 같은 네 가지 점에서 취약한 환경에서 동작한다.

· 에이전트(925)가 자신을 전송하는 목적지인 노드가 노드 상에서 실행될 코드를 포함하는 외부로부터의 적당하게 의심스러운 메시지를 가지고 있다.

· 노드 상의 사용자가 디지털 표현 수신 조건을 위반한다고 가정한 상태에서, 이들 동작을 숨기거나 또는 에이전트(925)를 디스에이블하고자 한다.

· 노드 상의 사용자가 에이전트(925)에 의해 전송되는 다른 데이터 및 키를 액세스하고자 한다.

· 다른 네트워크(103) 사용자가 에이전트(925)와 감시 장치(901) 사이에서 교환될 메시지의 콘텐츠에 관심을 가지고 있다.

제1 문제점은 "고의적인 에이전트 문제(malicious agent problem)"이다. 이는 일반적으로 코드를 다운로드하고 실행하는 시스템의 경우에 발생하며, 이들 경우에 사용되는 해결방법을 에이전트 엔진(1003) 및 에이전트(925)에도 동일하게 적용할 수 있다. 예를 들어 워터마크 에이전트의 코드가 Java로 작성되는 경우, 에이전트 코드를 구동하는 시스템은 Java 번역기에 의해 제공되는 모든 보호 기능을 가지게 된다. 노드의 관리자가 에이전트 엔진(1003) 및 에이전트(925)가 노드에 어떠한 손상도 입히지 않는다는 사실을 확신하는 경우, 엔진(1003) 및 에이전트(925)를 단순히 디지털 표현 다운로드의 조건으로 수용하도록 할 수 있다. 예를 들어 디지털 표현 관리자가 디지털 표현을 노드로 다운로드하는 트랜잭션은, 에이전트 엔진(1003)으로 전송되며 에이전트 엔진(1003)의 존재 및 동작을 확인하는 메시지를 포함한다. 메시지에

대한 적합한 응답이 없는 경우, 디지털 표현 관리자는 노드에서 트랜잭션을 추가로 처리하기 전에 에이전트 엔진(1003)을 다운로드하고 설치할 것을 요구한다.

나머지 문제점은 "고의적인 노드 문제점(malicious node problems)"이다. 이는 전술한 Schneirer의 논문에 기술되어 있는 바와 같이 표준 암호법 기술에 의해 해결될 수 있다. 예를 들어 디지털 표현 관리자 및 에이전트 엔진(1003) 각각은 공용 키-개인 키 한 쌍을 가지고 있다. 이 경우에 네트워크 정보(909)는 소정의 노드에서의 에이전트 엔진(1003)용 공용 키를 포함하며, 방문될 노드의 에이전트 엔진(1003)용 공용 키가 맵(931)에 포함된다. 디지털 표현 관리자 또는 에이전트(925)에 의해 전송되는 모든 메시지는 에이전트 엔진(1003)의 공용 키를 사용하여 암호화될 수 있으며, 디지털 표현 관리자의 공용 키를 사용하여 에이전트 엔진(1003) 및 에이전트(925)에 의해 디지털 표현 관리자로 모든 메시지를 전송할 수 있다. 물론 디지털 표현 관리자의 공용 키는 에이전트(925)의 키(934)에 포함될 수 있다. 표준 디지털 서명 기술을 사용하여 메시지를 인증할 수 있으며, 예를 들어 에이전트 데이터(929)는 에이전트(925)용으로 디지털 표현 관리자로부터의 디지털 서명을 포함할 수 있으며, 디지털 표현 관리자로부터 에이전트 엔진(1003)으로 전송된 메시지는 디지털 표현 관리자의 디지털 서명을 포함할 수 있으며, 에이전트 엔진(1003)으로부터의 메시지는 에이전트 엔진(1003)의 디지털 서명을 포함할 수 있다.

전술한 E. Koch 및 J. Zhao의 "Towards Robust and Hidden Image Copyright Labeling"에 기재되어 있는 바와 같이 암호화 기술을 사용하여 워터마크를 작성하는 경우, 에이전트는 워터마크 해독 방법을 가지고 있어야 한다. 상황에 따라, 에이전트 엔진으로 전송되는 다른 메시지 또는 워터마크가 자신의 키(913)를 가지는 방법과 동일한 방법을 사용하여, 워터마크 에이전트의 공용 키로 워터마크를 암호화하고 디지털 서명을 인증할 수 있다. 전자의 경우에는 워터마크 에이전트의 개인 키를 보호해야 하며, 후자의 경우에는 워터마크 키(913)를 보호해야 하는데, 이는 키를 액세스함으로써 디지털 표현을 몰래 가져가 디지털 표현의 워터마크를 제거하거나 수정할 수 있기 때문이다. 에이전트(925)가 순회 중인 경우, 에이전트(925)의 나머지 정보와 동일한 방법으로 암호화함으로써 워터마크 키(913)를 보호할 수 있다. 에이전트(925)를 해독하는 경우, 에이전트(925)가 현재 방문하는 노드에서 워터마크 키(913) 및 에이전트 엔진(1003)의 개인 키를 보호해야 한다. 추가로 에이전트(925)가 현재 방문하는 노드의 사용자가 개인 키를 사용하여 에이전트 엔진(1003)으로 전송될 메시지를 해독하거나 또는 에이전트(1003)의 디지털 서명에 추가하는 것을 방지하기 위해 에이전트 엔진(1003)의 개인 키를 보호해야 한다.

J. D. Tyger 및 Bennet Lee의 "Secure Coprocessors in Electronic Commerce Applications, FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE (1995년 7월)에 개시되어 있는 바와 같이, 이들 키 보호 문제를 해결하기 위한 하나의 방법이 보안 코프로세서이다. 1033에 도시되어 있는 바와 같이, 보안 코프로세서는 보안 기억 장치(1035) 및 보안 프로세서(PROC)(1045)를 포함한다. 보안 기억 장치(1035)는 보안 프로세서(1045)를 통해서만 액세스가능하며, 보안 프로세서(1045)를 통하지 않고 보안 코프로세서(1033)의 정보를 액세스하려는 시도가 있는 경우 반드시 정보가 파괴되도록 하는 방법으로 보안 코프로세서(1033)가 구축된다. 보안 코프로세서(1033)는 보안 기억 장치(1035)에 정보를 기록하고 보안 기억 장치(1035)로부터 정보를 판독할 수 있으며, 암호화 및 해독이 가능하며, 디지털 서명을 생성하고 검사할 수 있다. (1047) 및 (1049)에 예시되어 있는 바와 같이 보안 기억 장치(1035)에 저장된 코드를 실행함으로써 또는 코드화 및 특수화 하드웨어 장치를 결합함으로써 전적으로 이들 동작이 구현될 수 있다. 암호화, 해독 및 디지털 서명을 생성하고 검사하는데 필요한 키가 보안 기억 장치(1035)에 저장되어 있다. 워터마크 키(WM KEY)(913), 감시 장치 공용 키(monitor public key, MON KEY)(1039), 에이전트 엔진 공용 키(agent engine public key, AEKU)(1041) 및 에이전트 엔진 개인 키(agent engine private key, AEKR)(1043)가 도 10에 도시되어 있다. 공용 키의 경우, 보안 기억 장치(1035)에 저장하는 것은 단순히 편리하기 때문이며, 보안 프로세서(1045)는 노드(1001)의 구성성분으로부터의 요구에 응답하여 공용 키에 액세스할 수 있다. 워터마크 키(913) 및 에이전트 엔진(1003)의 개인 키(1043)의 경우, 해독된 키(913 및 1043)는 단지 보안 코프로세서(1033) 내에서만 사용된다.

이러한 시스템(1001)에서, 에이전트 엔진(1003)의 공용 키(1041)로 암호화된 메시지가 에이전트 엔진(1003)에 도달하는 경우, 에이전트 엔진(1003)은 보안 코프로세서(1033)를 사용하여 이 메시지를 해독한다. 메시지가 에이전트(925)를 포함하는 경우, 에이전트 엔진(1003)은 보안 코프로세서(1033)를 사용하여 에이전트(925)의 디지털 서명이 디지털 표현 관리자로부터의 디지털 서명인 지를 검사하고, 워터마크 키(913)를 해독한다. 해독된 키는 에이전트 엔진(1033)으로 돌아가지 않고 보안 기억 장치(1035)에 저장된다. 그러고 나서 워터마크 판독기(1019)는 보안 코프로세서(1033)를 사용하여 에이전트(925)에 의해 현재 검사되는 디지털 표현의 워터마크를 해독한다.

워터마크 에이전트를 사용한 예

워터마크 에이전트를 프로그래밍하여 사실상 무엇이든 할 수 있다. 워터마크 에이전트가 활성 워터마크와 결합하여 사용되는 경우, 워터마크 에이전트의 사용 범위(flexibility)가 증가한다. 워터마크 에이전트의 적용 예가 저작권 소유권자 또는 라이센스 대리인을 위해 저작권 등록된 디지털 표현의 사용을 감시하는 것이다. 예를 들어 저작권 소유권자 또는 라이센스 대리인은 워터마크 에이전트를 사용하여 허용되지 않은(unlicensed) 디지털 표현의 복제물을 찾거나 라이센스된 복제물의 사용을 주기적으로 감시한다. 활성 워터마크를 가지는 문서는 인쇄될 때마다 에이전트 엔진(1003) 내의 노드 사용 횟수(usage count)를 증가시킬 수 있으며, 에이전트(925)는 노드를 방문하는 즉시 그 횟수를 판독하고, 현재 횟수 값을 다시 관리 데이터베이스(903)에 보고하고, 카운터를 리셋한다.

다른 적용 예는 침해 가능성을 배제하기 위해 디지털 표현의 사용을 감시하는 것이다. 예를 들어 기업에서 네트워크 상에 인가되지 않은 디지털 표현이 있는 지 또는 인가된 디지털 표현이 라이센스 계약에 따라 사용되고 있는 지를 확인하려고 하는 경우도 있다. 라이센스 대리인이 감시하는 것과 동일한 방식으로, 에이전트가 기업 네트워크 상의 디지털 표현의 사용을 감시할 수 있다. 이 경우에 감시는 불법 복제본을 파괴하는 것까지도 포함할 수도 있다.

다른 적용 예는 인증되지 않은 복제, 스캐닝, 또는 인쇄를 방지하는 것이다. 이는 네트워크의 서버 및 클라이언트 상의 "순회하지 않는" 워터마크 에이전트에 의해 가능하며, 복사기, 스캐너, 프린터와 같은 장치에 구축된 "순회하지 않는" 워터마크 에이전트에 의해서도 가능하다. 예를 들어 "복제 불가" 워터마

크가 화폐에 삽입되어 있으며 사진복사기(photocopier)가 이와 같은 워터마크를 조사하고 워터마크를 발견하면 복제를 금지하는 에이전트를 가지고 있는 경우, 사진복사기를 사용하여 화폐를 복사할 수 없다.

워터마크 에이전트를 사용하여 군사 또는 기업 문서에 보안 규칙을 적용할 수 있다. 이러한 경우에, 문서의 보안 등급이 워터마크로 내장되며, 워터마크 에이전트는 군사 또는 기업 파일 시스템 및 네트워크를 조사하여 보안 등급이 요구하는 대로 처리되지 않은 문서를 찾는다. 이러한 문서의 예로는 잘못된 위치에 있는 문서 또는 미리 정해진 기간보다 긴 시간동안 보관되어 있는 문서 등이 있다. 에이전트에 의해 수행되는 동작의 범위는 보고나 경고에서부터 문서의 액세스 권한을 변경하거나 문서를 안전 위치로 이동하는 등과 제 위치를 벗어난 문서를 즉각적으로 파괴하는 것에 이른다. 즉 이러한 에이전트는 순회할 필요가 없으며, 간단히 파일 시스템의 영구 구성요소가 될 수 있다.

마지막으로 워터마크 에이전트를 사용하여 군사 또는 기업 파일 시스템 또는 네트워크에서 분실된 문서를 찾을 수 있다. 문서 각각이 관련된 고유의 식별자를 가지며, 식별자가 한편으로는 데이터베이스에 보관되며 다른 한편으로는 문서의 워터마크와 결합되는 경우, 간단하게 워터마크 에이전트에 소정의 범용 식별자를 부여할 수 있으며, 워터마크 에이전트를 전송하여 파일 시스템, 또는 네트워크를 조사하여 문서를 찾을 수 있다. 에이전트가 문서를 찾은 경우, 에이전트는 그 위치를 에이전트가 전송된 위치에 보고한다.

결론

전술한 상세한 설명은 아날로그 형태의 문서와 디지털 표현의 문서 사이에서 변환되는 인증된 문서를 생성하고 사용하는 방법, 활성 워터마크를 가지는 디지털 표현을 생성하고 사용하는 방법 및 이동식 워터마크 에이전트를 포함하여 워터마크 에이전트를 생성하고 사용하는 방법을 기술하며, 추가로 이러한 인증을 생성하고 활성 워터마크를 생성하고 워터마크 에이전트를 생성하는 현재에 알려진 최적의 모드를 기술한다. 기재된 기술은 아주 일반적이며, 다수의 서로 다른 목적을 위해 다수의 서로 다른 방법으로 구현될 수 있다. 예를 들어 인증 기술은 모든 종류의 의미 정보에 기초할 수 있으며, 여러 가지 방법을 사용하여 의미 정보로부터 인증 정보를 파생시키고 인증 정보를 디지털 표현 또는 아날로그 형태로 하고 인증 정보를 비교한다. 이와 유사하게 활성 워터마크의 프로그램 코드는 모든 프로그래밍 언어로 작성될 수 있으며, 소스 또는 객체 형태로 작성될 수 있으며, 실행될 때 임의의 동작을 수행할 수 있다. 워터마크 에이전트는 임의의 동작을 수행할 수 있으며, 네트워크 상에서 메시지를 전송하고 노드에서 노드로 이동하기 위한 여러 가지 기술을 사용할 수 있다. 물론 워터마크 에이전트는 인증 정보를 수행하고 활성 워터마크로부터 코드를 실행할 수 있다.

본 발명에 의한 기술이 일반적이며 여러 가지 방법으로 구현될 수 있기 때문에, 상세한 설명은 모든 점에서 일례를 들기 위한 것이지 본 발명을 제한하기 위한 것은 아니다. 본 명세서의 범위는 상세한 설명에 의해 결정되는 것이 아니라 특허법에 의해 허용되는 전체 범위로 해석되는 청구의 범위로부터 결정된다.

(57) 청구의 범위

청구항 1

디지털 표현의 의미 정보를 사용하여 인증 정보를 생성하는 인증기(authenticator), 그리고

상기 의미 정보의 의미가 변경되지 않도록 상기 인증 정보를 디지털 표현에 결합하는 결합기(incorporator)

를 포함하며,

상기 인증 정보는 상기 디지털 표현으로부터 생성된 아날로그 형태에 남아있는

디지털 표현에 인증 정보를 추가하는 장치.

청구항 2

제1항에 있어서,

상기 결합기가 특별한 도움 없이는 상기 아날로그 형태에서 찾아낼 수 없는 형태로 상기 인증 정보를 결합하는 인증 정보 추가 장치.

청구항 3

제2항에 있어서,

상기 찾아낼 수 없는 형태가 디지털 워터마크인 인증 정보 추가 장치.

청구항 4

제1항에 있어서,

상기 결합기가 특별한 도움 없이도 상기 아날로그 형태에서 찾아낼 수 있는 형태로 상기 인증 정보를 디지털 표현에 결합하는 인증 정보 추가 장치.

청구항 5

제4항에 있어서,

상기 찾아낼 수 있는 형태가 바 코드인 인증 정보 추가 장치.

청구항 6

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 인증 정보가 상기 의미 정보로부터 생성된 다이제스트인 인증 정보 추가 장치.

청구항 7

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 인증 정보는 상기 아날로그 형태로부터 상기 의미 정보를 판독할 때 발생하는 비실질적인 오류(insubstantial error)의 영향을 받지 않는 인증 정보 추가 장치.

청구항 8

제7항에 있어서,

상기 인증 정보가 적어도 부분적으로 상기 의미 정보의 순서를 반영하는 인증 정보 추가 장치.

청구항 9

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 디지털 표현은 문서의 디지털 표현이며,

상기 의미 정보는 상기 문서의 문자-숫자 문자(alphanumeric characters)를 포함하는

인증 정보 추가 장치.

청구항 10

제9항에 있어서,

상기 디지털 표현은 문서의 디지털 영상이며,

상기 장치는 문자-숫자 문자를 인식하는 광학 문자 인식기를 포함하는

인증 정보 추가 장치.

청구항 11

제10항에 있어서,

상기 디지털 영상은 상기 문서의 아날로그 형태를 스캐닝함으로써 생성되며,

상기 인증 정보는 상기 스캐닝된 아날로그 형태로부터 생성된 복제본에 추가될 수 있는

인증 정보 추가 장치.

청구항 12

제9항에 있어서,

상기 디지털 표현은 상기 문자-숫자 문자를 나타내는 디지털 코드를 포함하며,

상기 장치는 문자-숫자 문자를 나타내는 상기 디지털 코드를 인식하는 구문분석기(parser)를 포함하는

인증 정보 추가 장치.

청구항 13

제9항에 있어서,

상기 디지털 표현으로부터 생성된 상기 아날로그 형태가 종이 디지털 화폐인 인증 정보 추가 장치.

청구항 14

제9항에 있어서,

상기 디지털 표현으로부터 생성된 상기 아날로그 형태가 종이 디지털 수표인 인증 정보 추가 장치.

청구항 15

제9항에 있어서,

상기 디지털 표현으로부터 생성된 상기 아날로그 형태가 식별 카드인 인증 정보 추가 장치.

청구항 16

제9항에 기재된 장치를 사용하는 프린터로서, 아날로그 형태를 인쇄할 때 상기 인증 정보를 상기 아날로그 형태에 추가하는 프린터.

청구항 17

아날로그 형태의 의미 정보를 사용하여 생성되며 상기 의미 정보의 의미가 변경되지 않도록 상기 아날로그 형태에 결합되는 제1 인증 정보를 포함하는 상기 아날로그 형태의 인증 여부(authenticity)를 판단하는 장치로서,

상기 아날로그 형태의 상기 의미 정보를 인식하는 의미 정보 인식기(semantic information recognizer),

상기 아날로그 형태로부터 상기 제1 인증 정보를 판독하는 인증 정보 판독기(authentication information reader), 그리고

상기 인식된 의미 정보로부터 제2 인증 정보를 연산 처리하고 상기 제1 인증 정보를 상기 제2 인증 정보와 비교함으로써 상기 아날로그 형태의 인증 여부를 판단하는 인증기

를 포함하는 인증 여부 판단 장치.

청구항 18

제17항에 있어서,

상기 인증 정보가 특별한 도움 없이는 상기 아날로그 형태에서 찾아낼 수 없는 형태로 결합되는 인증 여부 판단 장치.

청구항 19

제18항에 있어서,

상기 찾아낼 수 없는 형태는 디지털 워터마크이고,

상기 인증 정보 판독기는 디지털 워터마크 판독기인

인증 여부 판단 장치.

청구항 20

제17항에 있어서,

상기 인증 정보가 특별한 도움 없이도 상기 아날로그 형태에서 찾아낼 수 있는 형태로 결합되는 인증 여부 판단 장치.

청구항 21

제20항에 있어서,

상기 찾아낼 수 있는 형태는 바 코드이며,

상기 인증 정보 판독기는 바 코드 판독기인

인증 여부 판단 장치.

청구항 22

제17항 내지 제21항 중 어느 한 항에 있어서,

상기 인증 정보가 상기 의미 정보로부터 생성된 다이제스트인 인증 여부 판단 장치.

청구항 23

제17항 내지 제21항 중 어느 한 항에 있어서,

상기 인증기가 상기 의미 정보 인식기에 의해 발생하는 비실질적인 오류의 영향을 받지 않도록 하는 방식으로 상기 제2 인증 정보를 연산 처리하는 인증 여부 판단 장치.

청구항 24

제23항에 있어서,

임계값 이내의 부분적 일치가 상기 아날로그 형태의 인증 여부를 가리키도록 하는 방법으로, 상기 인증기가 상기 제1 인증 정보를 제2 인증 정보와 비교하는 인증 여부 판단 장치.

청구항 25

제23항에 있어서,

상기 인증 정보가 적어도 부분적이나마 상기 의미 정보의 순서를 반영하는 인증 여부 판단 장치.

청구항 26

제17항 내지 제21항 중 어느 한 항에 있어서,

상기 인증기가 상기 의미 정보 인식기에 의해 발생하는 비실질적인 오류의 영향을 받지 않도록 하는 방식으로 상기 제1 인증 정보를 상기 제2 인증 정보와 비교하는 인증 여부 판단 장치.

청구항 27

제26항에 있어서,

상기 의미 정보는 제한되어 있으며,

상기 인증기는 상기 인식된 의미 정보의 오류를 보정하기 위한 제한을 사용하는 오류 보정기(error corrector)를 포함하고, 상기 제1 인증 정보와 상기 제2 인증 정보가 정확하게 일치하지 않는 경우 상기

인식되고 보정된 의미 정보를 사용하여 제2 인증 정보를 재연산 처리하는 인증 여부 판단 장치.

청구항 28

제17항 내지 제21항 중 어느 한 항에 있어서,

상기 아날로그 형태는 상기 제1 인증 정보를 포함하는 상기 디지털 표현으로부터 생성된 인증 여부 판단 장치.

청구항 29

제17항 내지 제21항 중 어느 한 항에 있어서,

상기 아날로그 형태는 문서이며,

상기 의미 정보는 문서의 문자-숫자 문자를 포함하고,

상기 의미 정보 인식기는 광학 문자 인식기인

인증 여부 판단 장치.

청구항 30

제29항에 있어서,

상기 문서가 종이 디지털 화폐인 인증 여부 판단 장치.

청구항 31

제29항에 있어서,

상기 문서가 종이 디지털 수표인 인증 여부 판단 장치.

청구항 32

제29항에 있어서,

상기 문서가 식별 카드인 인증 여부 판단 장치.

청구항 33

제29항에 기재된 장치를 사용하는 스캐너로서, 아날로그 형태를 스캐닝하여 스캐닝된 아날로그 형태의 인증 여부를 판단하는 스캐너.

청구항 34

디지털 표현으로부터 생성된 아날로그 형태로 보존되는 특성을 가지는 인증 정보를 상기 디지털 표현의 의미 정보로부터 생성하는 단계, 그리고

상기 의미 정보의 의미가 변경되지 않도록 상기 인증 정보를 상기 디지털 표현에 결합하는 단계

를 포함하는 인증 정보를 디지털 표현에 추가하는 방법.

청구항 35

아날로그 형태의 의미 정보를 사용하여 생성되며 상기 의미 정보의 의미가 변경되지 않도록 상기 아날로그 형태에 결합되는 제1 인증 정보를 포함하는 상기 아날로그 형태의 인증 여부를 판단하는 방법에 있어서,

상기 아날로그 형태의 상기 의미 정보를 인식하는 단계,

상기 제1 인증 정보를 판독하는 단계,

상기 인식된 의미 정보로부터 제2 인증 정보를 연산 처리하는 단계, 그리고

상기 제1 인증 정보를 상기 제2 인증 정보와 비교함으로써 상기 아날로그 형태의 인증 여부를 판단하는 단계

를 포함하는 아날로그 형태의 인증 여부 판단 방법.

청구항 36

의미 정보, 그리고

상기 의미 정보를 사용하여 생성되며 상기 의미 정보의 의미에 실질적으로 영향을 미치지 않는 인증 정보

를 포함하며,

상기 인증 정보는 상기 아날로그 형태의 일부인

인증된 아날로그 형태.

청구항 37

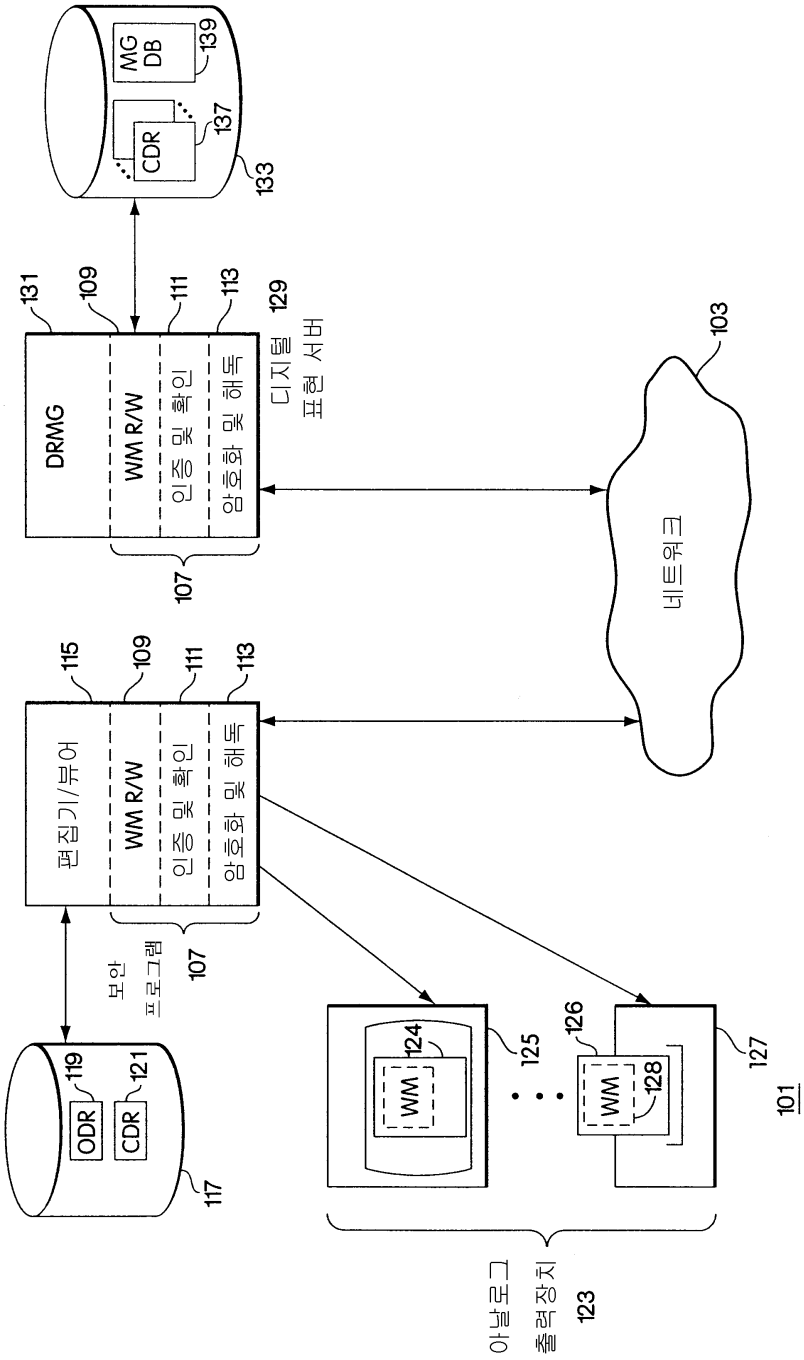
의미 정보의 디지털 표현, 그리고

상기 디지털 표현의 일부이지만 상기 의미 정보의 의미를 변경하지 않으며, 상기 의미 정보의 디지털 표현을 사용하여 생성되며, 상기 디지털 표현으로부터 생성된 아날로그 형태에도 존속하는 인증 정보

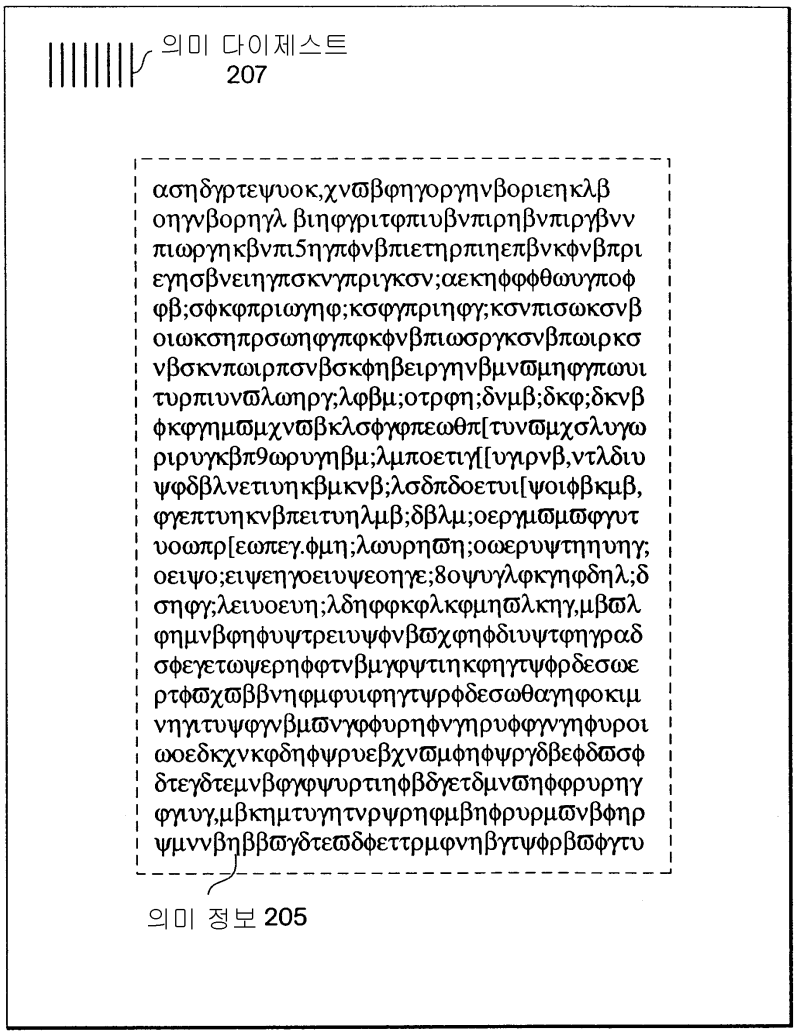
를 포함하는 인증된 디지털 표현.

도면

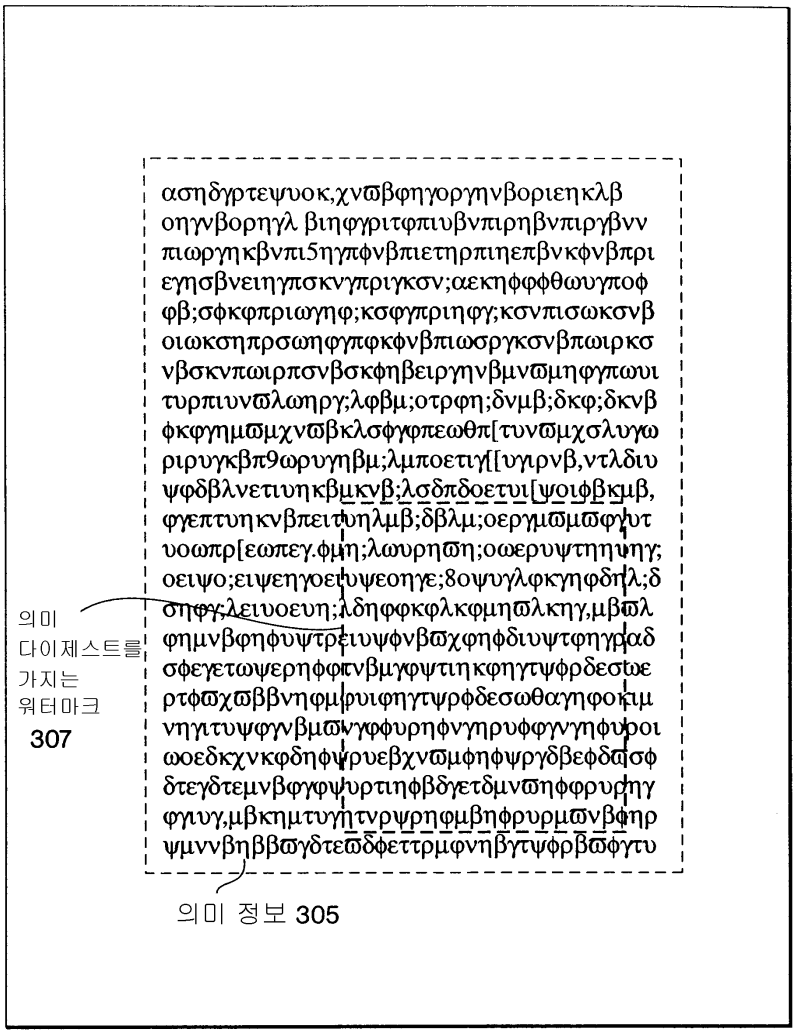
도면1



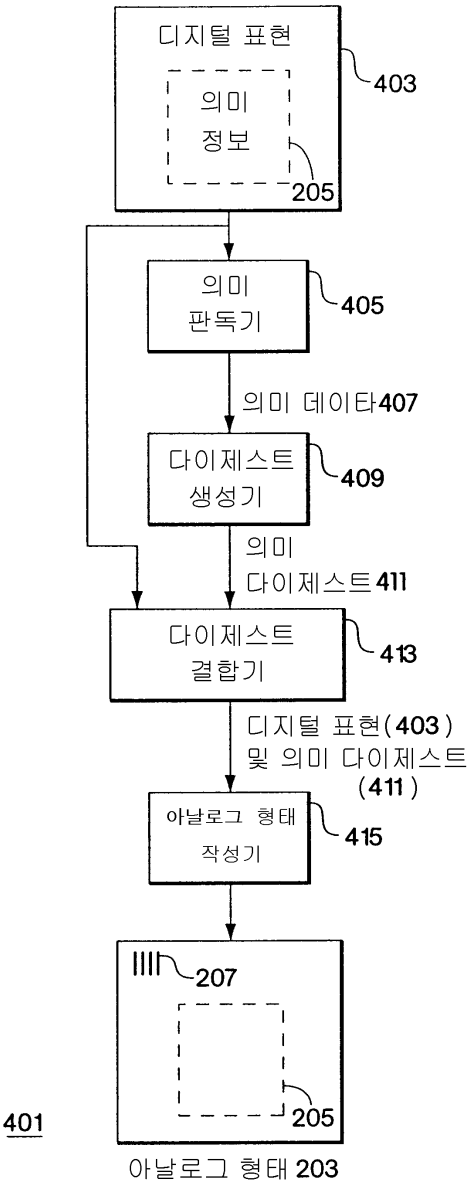
도면2


의미 다이제스트
207
αση δγρτεψυοκ,χνϖβφηγοργηνβοριεηκλβ
οηγνβορηγλ βιηφγριτφπιυβνπιρηβνπιργβνν
πιωργηκβνπι5ηγπφνβπιετηρπιηεπβνκφνβπρι
εγησβνειηγπσκνγπριγκσν;αεκηφφφθωυγποφ
φβ;σφκφπριωγηφ;κσφγπριηφγ;κσνπισωκσνβ
οιωκσηπρσωηφγπφκφνβπιωσργκσνβπωιρκσ
νβσκνπωιρπσνβσκφηβειργηνβμνϖμηφγπωυι
τυρπιυνϖλωηργ;λφβμ;οτρφη;δνμβ;δκφ;δκνβ
φκφγημϖμχνϖβκλσφχφπεωθπ[τυνϖμχσλυγω
ριρυγκβπ9ωρυγηβμ;λμποετιγ[[υγιρνβ,ντλδιυ
ψφδβλνετιυηκβμκνβ;λσδπδοετυι[ψοιφβκμβ,
φγεπτυηκνβπειτυηλμβ;δβλμ;οεργμϖμϖφγυτ
υοωπρ[εωπεγ.φμη;λωυρηϖη;οωερυψτηηυηγ;
οειψο;ειψεηγοειυψεοηγε;8οψυγλφκγηφδηλ;δ
σηφγ;λειυοευη;λδηφφκφλκφμηϖλκηγ,μβϖλ
φημνβφηφυψτρειυψφνβϖχφηφδιυψτφηγραδ
σφεγετωψερηφφτνβμγφψτιηκφηγτψφρδεσωε
ρτφϖχϖββνηφμφυιφηγτψρφδεσωθαγηφοκιμ
νηγιτυψφγνβμϖνγφφυρηφνγηρυφφγνγηφυροι
ωοεδκχνκφδηφψρυεβχνϖμφηφψργδβεφδϖσφ
δτεγδτεμνβφγφψυρτιηφβδγετδμνϖηφφρυρηγ
φγιυγ,μβκημτυγητνρψρηφμβηφρυρμϖνβφηρ
ψμννβηββϖγδτεϖδφεττρμφνηβγτψφρβϖφγτυ
의미 정보 205
아날로그 형태 203
201

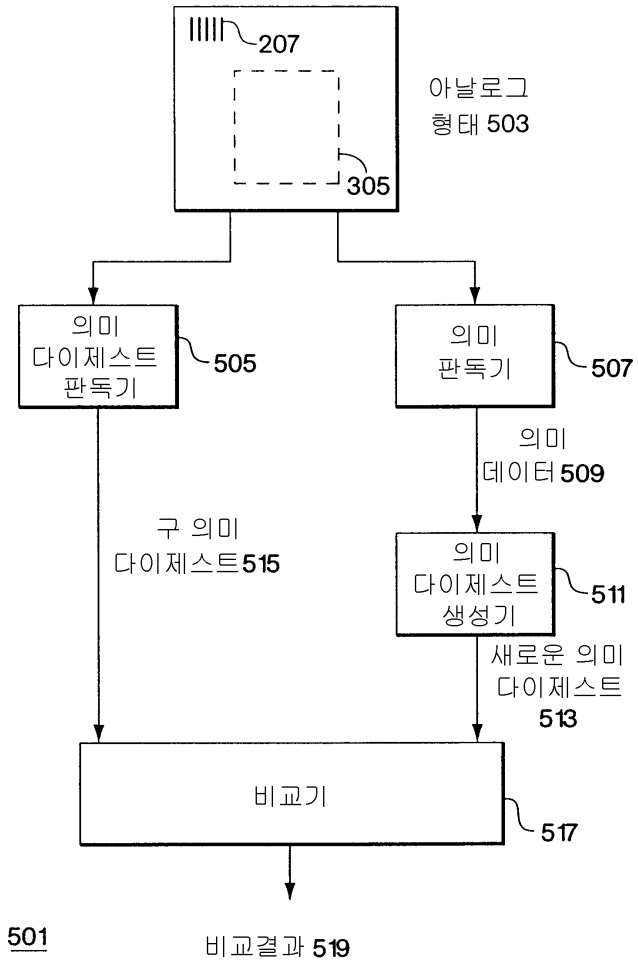
도면3



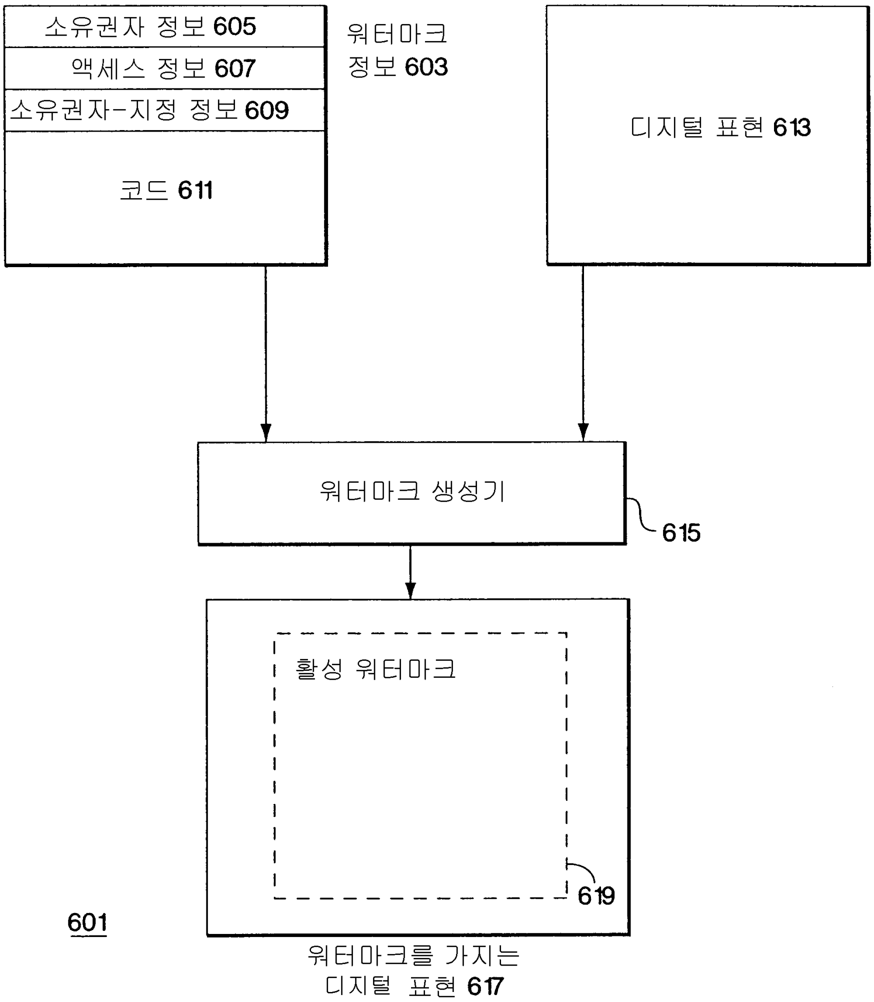
도면4


디지털 표현
의미 정보
205
403
의미 판독기
405
의미 데이타407
다이제스트 생성기
409
의미 다이제스트411
다이제스트 결합기
413
디지털 표현(403) 및 의미 다이제스트 (411)
아날로그 형태 작성기
415
207
205
401
아날로그 형태 203

도면5


207
305
아날로그
형태 503
의미
다이제스트
판독기
505
의미
판독기
507
의미
데이터 509
구 의미
다이제스트 515
의미
다이제스트
생성기
511
새로운 의미
다이제스트
513
비교기
517
501
비교결과 519

도면6



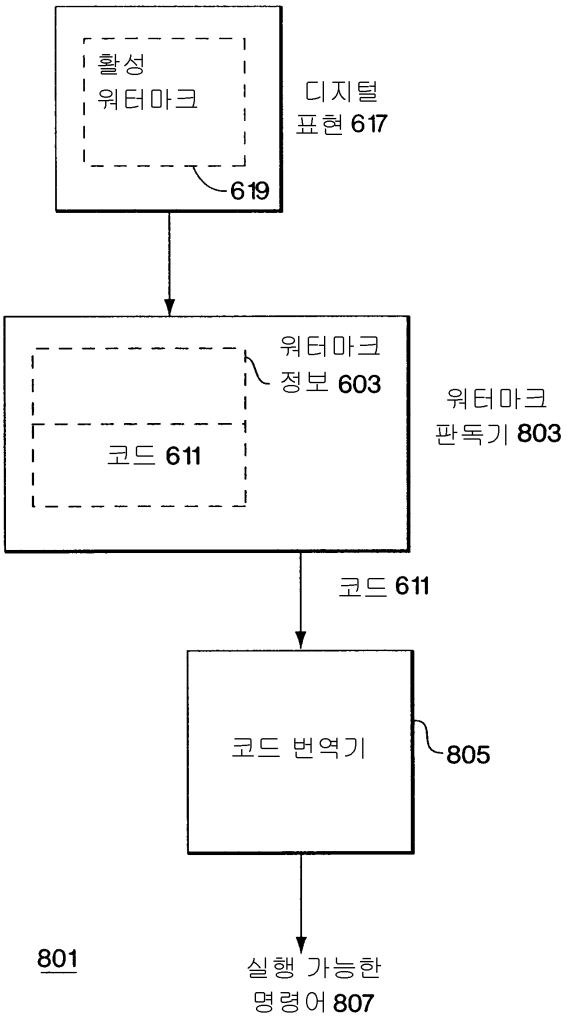
도면7

```
DatagramSocket s = new DatagramSocket (0);

InetAddress a =
    netAddress.getByName ("syscop. crcg.edu");

DatagramPacket p = new DatagramPacket ('XYZ
    Displayed", 13, a, 14);

s.send(p);
```

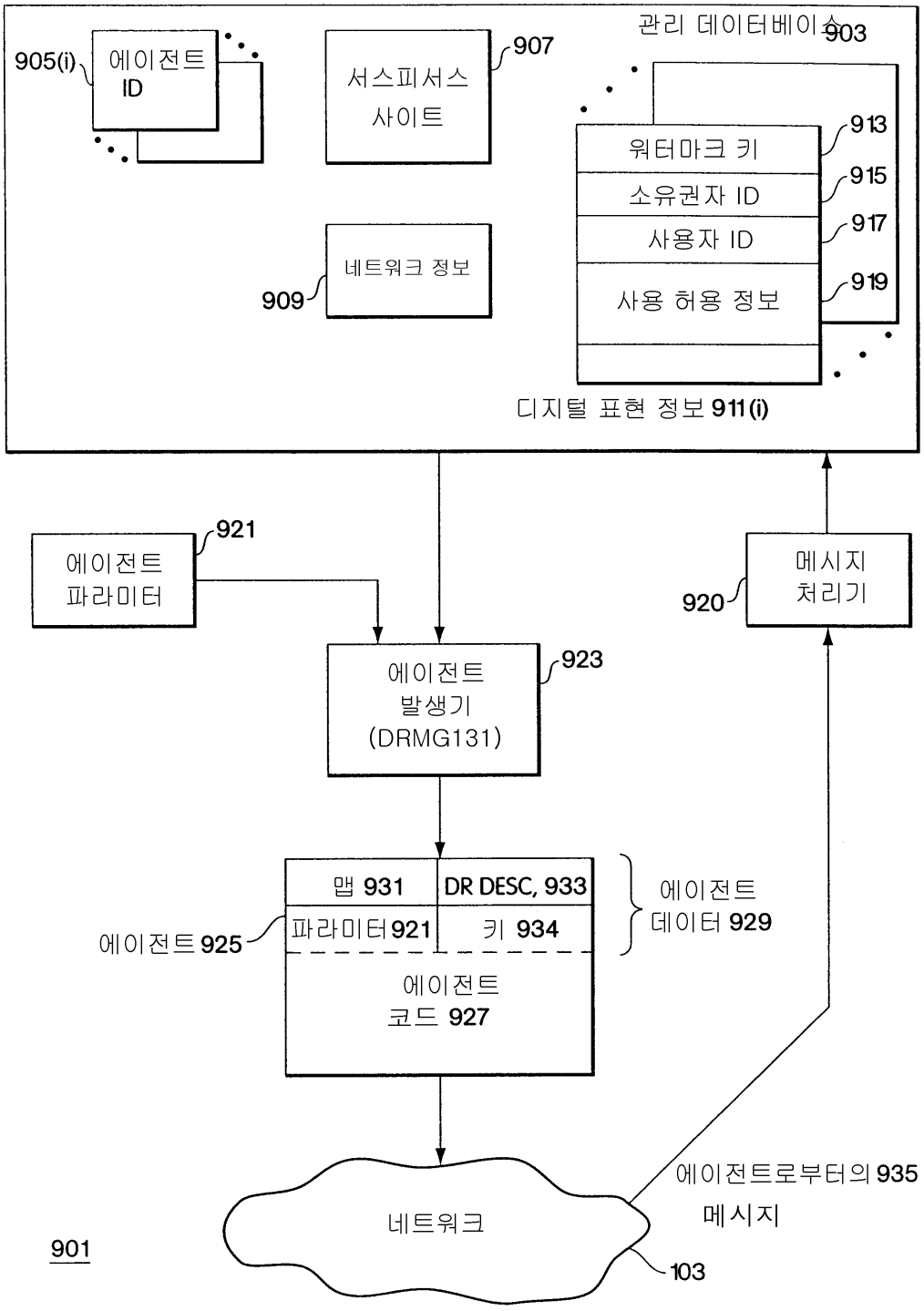
703 705 709 1715 1711 1713 1719

701

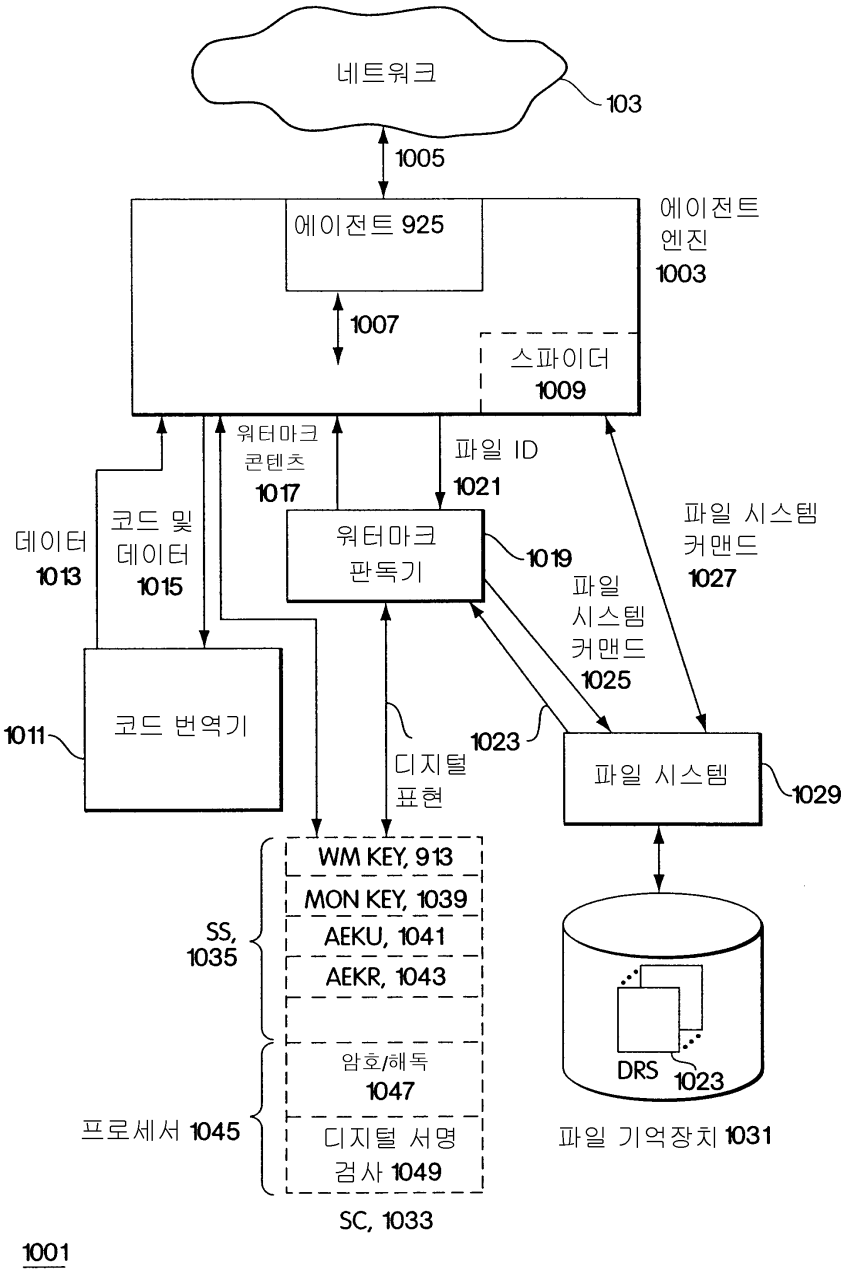
도면8


활성
워터마크
619
디지털
표현 617
워터마크
정보 603
코드 611
워터마크
판독기 803
코드 611
코드 번역기
805
801
실행 가능한
명령어 807

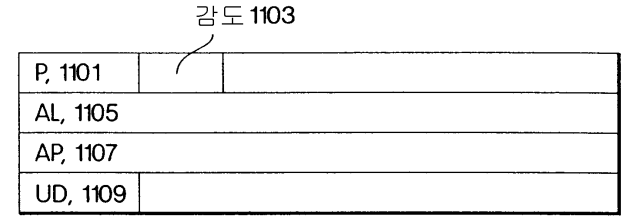
도면9


관리 데이터베이스 903
905(i)
에이전트 ID
서스피서스 사이트
907
워터마크 키
913
소유권자 ID
915
사용자 ID
917
사용 허용 정보
919
네트워크 정보
909
디지털 표현 정보 911(i)
에이전트 파라미터
921
메시지 처리기
920
에이전트 발생기 (DRMG131)
923
맵 931
DR DESC, 933
에이전트 데이터 929
에이전트 925
파라미터 921
키 934
에이전트 코드 927
에이전트로부터의 935 메시지
네트워크
103
901

도면10


네트워크
103
1005
에이전트 925
에이전트
엔진
1003
1007
스파이더
1009
워터마크
콘텐츠
1017
파일 ID
1021
데이터
1013
코드 및
데이터
1015
워터마크
판독기
1019
파일 시스템
커맨드
1027
파일
시스템
커맨드
1025
1011
코드 번역기
1023
디지털
표현
파일 시스템
1029
WM KEY, 913
MON KEY, 1039
AEKU, 1041
AEKR, 1043
SS,
1035
암호/해독
1047
프로세서 1045
디지털 서명
검사 1049
SC, 1033
DRS
1023
파일 기억장치 1031
1001

도면11


감도 1103
P, 1101
AL, 1105
AP, 1107
UD, 1109
607

도면12

```
// Instantiate a file filter.
FileFilter fileFilter =new FileFilter();
// filter out all image files from the file system.
String {} filenames = fileFilter.filterImages();
// get host environment information.
EnvInfo env = getEnvInfo();
// construct a new vector used to store action results.
Vector results = new Vector();

for(int i=0; i<filenames.length; i++) {
  // check each image file for watermark.
  String watermark = checkWatermark (filenames[i]);
  if (watermark != null) { // if a watermark is found

     // match the watermark with the host environment.
     String match  = matchEnv(watermark, env);
     // take action according to the matching result.
     String result = takeAction (match);
     // add the result to the vector.
     results.addElement (result);
  }
}
return results;
```

1205 1207 1209 1211 1203 1215 1213 1217 1219 1221 1223 1225

1201