



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2008년01월29일  
(11) 등록번호 10-0799090  
(24) 등록일자 2008년01월23일

(51) Int. Cl.

G06F 13/00 (2006.01)

(21) 출원번호 10-2002-7010746

(22) 출원일자 2002년08월17일

심사청구일자 2006년02월14일

번역문제출일자 2002년08월17일

(65) 공개번호 10-2003-0007432

(43) 공개일자 2003년01월23일

(86) 국제출원번호 PCT/US2001/004812

국제출원일자 2001년02월14일

(87) 국제공개번호 WO 2001/61508

국제공개일자 2001년08월23일

(30) 우선권주장

60/183,681 2000년02월19일 미국(US)

(뒷면에 계속)

(56) 선행기술조사문헌

US5841978 A

(뒷면에 계속)

전체 청구항 수 : 총 4 항

(73) 특허권자

디지털 코퍼레이션

미국, 오리곤97008, 비버튼, 에스더블유 제미니 드라이브 9405

(72) 발명자

라모스다니엘오.

미국, 오리곤97007,

비버튼, 에스더블유하기스로드16869

존스캐빈씨.

미국, 오리곤97229, 포트랜드, 엔더블유네스코원애비뉴4850

로아즈게프리비.

미국, 오리곤97068,

웨스트린, 에스더블유터너로드2961

(74) 대리인

이병호, 장훈

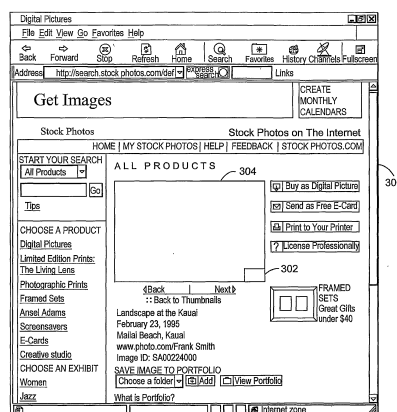
심사관 : 이재근

(54) 워터마크 인코더 및 디코더를 작동시키는 소프트웨어 및 장치들

(57) 요약

워터마크 인코더들 및 디코더들은 오퍼레이팅 시스템들, 인터넷 브라우저들(300), 매체 플레이어들 및 다른 애플리케이션들 및 장치들 내에 통합된다. 이러한 통합으로 워터마크-가능하게 된 애플리케이션(304) 또는 장치들이 워터마크를 통해 이용 가능한 부가 기능 및 정보(302)를 제공하게 한다. 워터마크는, 예를 들면, 매체 객체와 관련된 메타데이터 또는 작용들과 링크할 수 있다. 이러한 워터마크 가능하게 된 기능을 개발하기 위하여, 통합 애플리케이션은 워터마크 디코더를 사용하여, 관련된 메타데이터 및 작용들에 액세스한다. 통합 애플리케이션의 사용자 인터페이스는 워터마크를 통해 링크된 메타데이터 및 작용들을 제공하기 위해 개선된다. 마찬가지로, 워터마크 인코더들은 매체 객체들을 개선되어 워터마크된 객체들로 변환하기 위해 애플리케이션 내에 통합될 수 있다.

대표도 - 도3



(56) 선행기술조사문헌

W097/43735 A

W099/57623 A

US5838458 A

US5956716 A

US5862260 A

(81) 지정국

국내특허 : 아랍에미리트, 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 코스타리카, 독일, 덴마크, 도미니카, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르기즈스탄, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 모로코, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 폴란드, 포르투갈, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 슬로베니아, 슬로바키아, 타지키스탄, 투르크멘, 터키, 트리니다드토바고, 우크라이나, 우간다, 우즈베키스탄, 베트남, 남아프리카, 그라나다, 가나, 감비아, 크로아티아, 인도, 인도네시아, 세르비아 앤 몬테네그로, 짐바브웨, 시에라리온

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 시에라리온, 가나, 감비아, 짐바브웨, 탄자니아, 모잠비크

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르기즈스탄, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크멘

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀란드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투갈, 스웨덴

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디부아르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고, 기니 비사우

(30) 우선권주장

60/191,778 2000년03월24일 미국(US)

09/636,102 2000년08월10일 미국(US)

**특허청구의 범위**

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

### 청구항 33

통신 네트워크를 통해 상호 접속된 컴퓨터들 상에서 실행하는 프로그램들에서 분배되는 워터마크 콘텐츠 필터들을 포함하는 콘텐츠 필터링 시스템에 있어서,

상기 워터마크 콘텐츠 필터들은, 상기 네트워크의 한 위치에서 콘텐츠 내의 디지털 워터마크들을 검출하고, 워터마크 페이로드 정보를 판독하고, 상기 워터마크 페이로드 정보 내의 데이터 또는 상기 워터마크 페이로드에 의해 참조되는 데이터에 기초하여 상기 콘텐츠의 렌더링 또는 전송을 제어하는 작용을 취하도록 동작가능한, 콘텐츠 필터링 시스템.

### 청구항 34

제 33 항에 있어서,

상기 콘텐츠 필터들은, 사용자들로 하여금 콘텐츠를 탐색할 수 있도록 하는 탐색가능한 데이터베이스에 검출 이벤트들을 보고하고, 상기 콘텐츠가 상기 콘텐츠 필터들에 의해 검출된 곳을 표시하는 네트워크 어드레스를 찾아 내는, 콘텐츠 필터링 시스템.

### 청구항 35

제 33 항에 있어서,

상기 콘텐츠 필터들은, 사용자 ID 및 상기 디지털 워터마크들 내의 데이터 또는 상기 디지털 워터마크들에 의해 참조되는 데이터에 기초하여 콘텐츠의 렌더링 또는 전송을 제어하는 규칙들을 실행하는, 콘텐츠 필터링 시스템.

### 청구항 36

제 33 항에 있어서,

상기 워터마크 페이로드 정보 내의 데이터 또는 상기 워터마크 페이로드 정보에 의해 참조되는 데이터는 상기 콘텐츠의 렌더링과 함께 광고의 렌더링을 가능하게 하거나 또는 불가능하게 하기 위해 사용자의 액세스 권리들에 관련된 규칙들과 조합하여 사용되는, 콘텐츠 필터링 시스템.

### 청구항 37

삭제

### 청구항 38

삭제

### 청구항 39

삭제

### 청구항 40

삭제

### 청구항 41

삭제

### 청구항 42

삭제

### 청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

## 명세서

### 기술분야

#### <1> 관련된 출원 데이터

<2> 본 특허 출원은 본 명세서에 편입되며, 2000년 3월 24일 출원된 미국 가출원 제 60/191,778 호를 우선권을 주장한다. 본 출원은 또한 본 명세서에 편입되며, 1998년 10월 1일 출원된 출원 제 09/165,142 호, 2000년 2월 14일 출원된 제 09/503,881 호, 2000년 2월 17일 출원된 제 09/507,096 호, 2000년 3월 15일 출원된 제 09/526,982 호, 2000년 3월 20일 출원된 제 09/531,076 호, 및 2000년 7월 20일 출원된 제 09/620,019 호의 일부 계속출원이다.

<3> 본 특허출원은 또한 본 명세서에 편입되어 참조되는, "디지털 워터마크들의 멀티미디어 콘텐츠로의 통합(Integrating Digital Watermarks into Multimedia Content)"으로 명칭되어 2000년 3월 15일 출원된 미국특허출원 제 09/525,865호, "접속된 오디오 및 다른 매체 객체들(Connected Audio and Other Media Objects)"로 명칭되어 2000년 5월 2일 출원된 09/563,664호, "물리적 및 전자적 객체들로부터 인터넷 리소스들에 링크하거나 컴퓨터를 제어하는 방법들 및 시스템들(Methods and Systems for Controlling Computers or Linking to Internet Resources from Physical and Electronic Objects)"로 명칭되어 2000년 5월 15일 출원된 제 09/571,422호, 및 "디지털 워터마킹을 채용하는 방법들 및 시스템들(Methods and Systems Employing Digital Watermarking)"로 명칭되어 2000년 5월 18일 출원된 제 09/574,726호에 관한 것이다.

#### <4> 기술분야

<5> 본 발명은 디지털 워터마킹(digital watermarking), 특히 소프트웨어 및 장치들에서의 디지털 워터마크 인코더들 및 디코더들의 애플리케이션들에 관한 것이다.

### 배경 기술

<6> 디지털 워터마킹은 물리적 또는 전자적 매체들을 변화시켜 기기-판독 가능 코드(machine-readable code)를 매체에 삽입하기 위한 프로세스이다. 이러한 매체에서는 임베딩된 코드가 사용자에게 지각될 수 없거나 또는 거의 지각될 수 없도록 변경되지만, 자동화된 검출 프로세스를 통해서는 검출될 수 있다. 통상, 대부분의 디지털 워터마킹은 이미지들, 오디오 신호들, 및 비디오 신호들 등의 매체 신호들에 적용된다. 그러나, 또한 (예를

들면, 선, 워드 또는 캐릭터 시프팅(character shifting)을 통해) 문서들, 소프트웨어, 다차원 그래픽 모델들 및 객체의 면 텍스처들(surface textures)을 포함하는 다른 형태들의 매체 객체들에 적용될 수 있다.

<7> 디지털 워터마킹 시스템은, 일반적으로 호스트 매체 신호 내에 워터마크(watermark)를 삽입하는 인코더, 및 워터마크를 포함하는 의심되는 신호(suspect signal)로부터 임베딩된 워터마크를 검출하여 판독하는 디코더의 2가지 주요 구성요소를 갖고 있다. 인코더는 호스트 매체 신호를 변경함으로써 워터마크를 삽입한다. 판독 구성요소는 서스펙트 신호를 분석하여, 워터마크가 존재하는가의 여부를 검출한다. 워터마크가 정보를 인코딩하는 애플리케이션들의 경우, 판독기는 상기 검출된 워터마크로부터 상기 정보를 추출한다.

<8> 대부분의 특정 워터마킹 기술들은 공지되었다. 판독기는 본 분야의 문헌에 잘 알려져 있는 것으로 가정된다. 매체 신호들 내의 지각할 수 없는 워터마크들을 삽입하고 검출하기 위한 특수한 기술들은 본 양수인의 공동 계류중인 출원번호 제 09/503,881호에 상세히 개시되어 있다. 다른 워터마킹 기술들은 NEC(발명자 Cox 등), IBM(발명자 Morimoto와 Braudaway 등), Dice(발명자 Cooperman), Philips(발명자 Kalker, Linnartz, Talstra 등)에 의해 공개된 특허들에 개시되어 있다. 오디오 워터마킹 기술들은 Aris(발명자 Winograd, Metois, Wolosewicz 등), Solana(발명자 Lee, Warren 등), Dice, Audio Track, Philips에 의해 공개된 특허들에 개시되어 있다.

### 발명의 상세한 설명

<9> 본 발명은 소프트웨어 애플리케이션들, 장치들 및 시스템들에서의 워터마크 인코딩 및 디코딩 기능을 통합하는 것에 관한 것이다. 워터마크 인코더들 및 디코더들은 오퍼레이팅 시스템들, 인터넷 브라우저들, 미디어 플레이어들, 다른 애플리케이션들 및 장치들에 통합된다. 이러한 통합은 워터마크-가능하게 된 애플리케이션(watermark-enabled application) 또는 장치가 이 워터마크를 통해 이용될 수 있는 부가적인 기능성 및 정보를 제공할 수 있게 한다. 워터마크는, 예를 들면, 매체 객체와 관련된 메타데이터(metadata) 또는 작용들과 링크할 수 있다. 이와 같이 워터마크 가능하게 된 기능성을 활용하기 위하여, 통합된 애플리케이션은 워터마크 디코더(watermark decoder)를 사용하여 관련 메타데이터 및 작용들에 액세스한다. 통합 애플리케이션의 사용자 인터페이스(user interface)는 워터마크를 통해 링크된 메타데이터 및 작용들을 제공하기 위해 강화된다. 마찬가지로, 워터마크 인코더는 애플리케이션에 통합되어, 매체 객체를 강화된 워터마크 객체로 변화시킬 수 있다.

<10> 본 발명의 일 양태는 강화된 파일 브라우저 시스템(enhanced file browser system)에 관한 것이다. 파일 브라우저는 사용자가 매체 객체 파일(media object file)을 포함하는 파일에 브라우징하게 한다. 이것은 선택된 매체 객체 파일로부터 객체 식별자(object identifier)를 디코딩하기 위한 확장을 포함한다. 이 확장은 객체 식별자를 통해 매체 객체 파일과 연관된 메타데이터 또는 작용들을 검색하여 디스플레이한다.

<11> 본 발명의 다른 양태는 객체 식별자를 인코딩하기 위한 확장을 갖는 파일 브라우저에 관한 것이다. 이러한 확장은 사용자가 객체 식별자를 선택된 매체 객체 파일로 인코딩하게 한다. 파일 브라우저의 사용자 인터페이스에 대한 확장에서는, 객체 식별자의 인코딩을 제어하기 위한 옵션들을 디스플레이한다. 객체 식별자는 매체 객체 내에 임베딩된 워터마크 내에 인코딩될 수 있다.

<12> 본 발명의 또 다른 양태는 호스트 애플리케이션(host application)에 통합된 워터마크 디코더 시스템(watermark decoder system)에 관한 것이다. 호스트 애플리케이션은 매체 객체 파일들의 표현을 디스플레이하기 위한 사용자 인터페이스를 갖는다. 이것은 또한 선택된 매체 객체로부터 워터마크를 디코딩하고, 상기 워터마크를 통해 매체 객체 파일과 연관된 메타데이터를 디스플레이하기 위한 확장을 갖는다.

<13> 본 발명의 또 다른 양태는 강화된 인터넷 브라우저(enhanced internet browser)에 관한 것이다. 이 브라우저는 HTML 문서 내의 매체 객체들을 식별하고, 객체 식별자가 마크된 객체를 발견하였을 때, 핸들러를 HTML 문서에 삽입하는 리스너 프로그램(listener program)으로 강화된다. 핸들러는 사용자 입력에 응답하여 객체 식별자를 통해 링크된 메타데이터를 디스플레이한다.

<14> 본 발명의 또 다른 양태는 브랜딩 정보(branding information)와 함께 메타데이터 객체를 렌더링하는 방법에 관한 것이다. 이 방법에서는, 매체 객체로부터 객체 식별자를 디코딩하고, 이 객체 식별자를 메타데이터 서버(metadata server)에 전송하고, 이 메타데이터 서버로부터 브랜드 식별자(brand identifier)를 수신하고, 이 브랜드 식별자의 표현을 디스플레이한다.

<15> 본 발명의 또 다른 양태는 매체 플레이어의 사용자 인터페이스를 확장하기 위한 방법이다. 매체 객체의 재생을 요구하는 입력에 응답하여, 상기 방법에서는, 객체 매체로부터 객체 식별자를 추출한다. 이 방법에서는, 객체

식별자를 이용하여 매체 객체와 연관된 메타데이터를 룩업(look-up)한다. 이 후, 매체 객체와 연관된 메타데이터의 표현을 포함하도록 매체 플레이어의 사용자 인터페이스를 확장한다.

<16> 본 발명의 다른 특징들은 이하의 상세한 설명과 첨부된 도면들을 참조하면 명확해질 것이다.

## 실시예

<30> 서두

<31> 워터마크는 이미지, 비디오 또는 오디오 파일과 같은 매체 객체를 부가 정보 및 작용들에 연관시키기 위하여 사용될 수 있다. 워터마크는 매체 객체를 이 매체 객체 내에 인코딩되거나 또는 외부에 저장되는 메타데이터 또는 프로세싱 작용들과 연관시킬 수 있다. 메타데이터는 매체 객체 파일 내에 저장되거나, 또는 매체 객체 파일 외부에 저장된 워터마크 메시지 내에서 인코딩될 수 있다. 메타데이터가 매체 객체 외부에 저장되면, 워터마크는 매체 객체 내의 객체 식별자(번호, 어드레스, 인덱스, 포인터 등) 등과 같은 메타데이터와의 지각할 수 없고 분석하기 어려운 링크를 인코딩할 수 있다. 매체 객체가 이동할 때는 항상, 워터마크 디코더-인에이블 소프트웨어 또는 장치들은 매체 신호로부터 워터마크를 추출하고, 이 워터마크 링크(watermark link)를 통해 객체와 연관된 메타데이터 또는 작용들에 액세스한다.

<32> 워터마크를 통해 매체 객체와 연관된 메타데이터 또는 작용들을 검색하기 위한 특정한 구조는 변경될 수 있다. 메타데이터 또는 프로세싱 작용들은 매체 객체와 동일한 장치 또는 시스템 내, 또는 유선 또는 무선 네트워크를 통해 액세스 가능한 원격 장치 또는 시스템 내의 메타데이터 데이터베이스 내에 잔류한다. 인터넷 같은 분산 컴퓨팅 환경(distributed computing environment)에서는, 워터마크 메시지에서 추출된 객체 식별자를 취하여, 메타데이터 또는 URL 링크를 컴퓨터 또는 장치("클라이언트")로 되돌리고, 식별자를 다른 서버에 라우팅하고, 소정의 프로그램 또는 프로그램 세트들을 실행하는 등의 식별자와 연관된 하나 이상의 작업들을 수행하는 방법이 있다. 워터마크 메시지는 워터마크를 통해 호스트 매체 객체에 인코딩된 보조 데이터(auxiliary data)라 한다.

<33> 이하의 섹션들은 오퍼레이팅 시스템, 인터넷 브라우저 및 다른 애플리케이션(하드웨어 장치, 소프트웨어 또는 하드웨어와 소프트웨어를 조합하여 실행되는 것)에서 상기 기능의 장점을 취하는 방법들을 요약한다.

<34> **오퍼레이팅 시스템들 및 다른 애플리케이션들에서의 워터마크 디코더 통합**

<35> **오퍼레이팅 시스템 내**

<36> 워터마크 디코더는 오퍼레이팅 시스템의 파일 브라우저 성분에 통합될 수 있다. 이 디코더는 파일 브라우저가 워터마크를 추출하고, 워터마크 가능하게 된 매체 객체들용의 메타데이터를 검색하게 한다. 사용자가 파일들을 브라우징할 때, 워터마크 디코더는 자동적으로 또는 사용자-개시의 포그라운드(foreground) 또는 백그라운드(background) 작업으로 워터마크를 검색하도록 동작할 수 있다. 워터마크를 발견하면, 브라우저는 워터마크와 연관된 애플리케이션(들)에 의해 지시된 바에 따라 매체 객체의 표현을 애노테이팅한다(annotate). 실행에 따라서, 브라우저는 워터마크를 통하여 객체와 연관된 추가 정보와 작용들의 검색을 진행하고, 이에 따라 매체 객체의 그것의 표현에 애노테이팅할 수 있다. 예를 들면, 브라우저는 매체 객체에 워터마크를 통해 링크된 정보 또는 작용들의 기술(예를 들면, 간단한 기술 및/또는 http 링크)을 애노테이팅할 수 있고, 객체에 실제적인 정보 또는 작용들을 애노테이팅할 수 있다.

<37> 워터마크 검출 및 이 워터마크를 통한 정보 또는 작용들의 참조의 프로세스는 사용자에게 알기 쉽게 실행될 수 있다. 예를 들면, 파일 브라우저는 사용자가 워터마크 검출 또는 정보 검색 프로세스를 간섭할 필요없이 워터마크 링크를 통해 얻어진 정보 또는 옵션들을 디스플레이한다.

<38> 대안으로, 파일 브라우저는 사용자에게 워터마크 페이로드(watermark payload)에 의해 트리거링되는 다양한 스테이지들의 워터마크 검출 및 프로세싱을 제어할 기회를 줄 수 있다. 예를 들면, 사용자는 워터마크 디코더가 매체 객체들 상에서 조작될 수 있게 하고, 워터마크 페이로드에 의해 트리거링된 작용이 어떤 것이고 어떻게 진행되어야 하는가를 결정하는 옵션을 제공할 수 있다. 워터마크의 검출시, 예를 들면, 매체 객체는 특유의 사운드 또는 로고와 같은 표시자로 애노테이트될 수 있는데, 즉 사용자는 워터마크에 임베딩된 링크를 통해 정보와 작용들이 액세스될 수 있음을 통지한다. 사용자는, 예를 들면, 사용자 인터페이스에서의 객체와 연관된 시각적 로고를 선택함으로써 매체 객체와 연관된 추가 정보에 액세스할 옵션을 갖는다. 오디오 "로고"는 사용자가 객체를 선택할 때(예를 들면, 사용자 인터페이스에서의 그것의 그래픽적 표현상에 커서를 통과시킴) 재생될 수 있다.



- <39> 애플리케이션의 사용자 인터페이스는 사용자에게 워터마크 링크의 존재 및 이와 연관된 정보와 작용들을 통지하는 다양한 그래픽 및/또는 오디오 효과를 애노테이팅한다. 사용자 인터페이스에서의 변화는 워터마크 검출 및 메타데이터 검색 프로세스에서 다른 스테이지들을 전달하기 위해 사용될 수 있다. 예를 들면, 우선 워터마크의 존재를 검출하면, 디코더(또는 호스트 애플리케이션(host application))가 간단한 로고 또는 오디오 클립 같은 범용 표시기를 재생한다. 이 후, 적절한 메타데이터 서버가 워터마크를 통해 링크된 명령들 및/또는 메타데이터를 리턴시킬 때, 사용자 인터페이스는 객체와 연관된 특수한 정보를 제시한다.
- <40> 서버는 자바 애플릿들, 비주얼 베이직 스크립트, XML 또는 소정의 다른 명령어들 세트 같은 프로그램 코드(예를 들면, 웹사이트들, 다른 콘텐츠 또는 프로그램 코드와의 핫 링크 또는 URL)를 리턴시킨다. 이러한 코드를 수신시, 클라이언트 컴퓨터 또는 장치는 이것을 실행시킨다. 클라이언트는 일반적으로 워터마크 링크를 디코딩하고, 이 링크에 기초한 요구를 서버에 발행하는 컴퓨터 또는 장치이다. 상기 코드는 워터마크된 매체 객체와 관련 매체 객체들의 렌더링 제어를 포함한 다양한 기능들을 수행할 수 있으며, 상기 객체들 중 일부는 링크된 메타데이터와 함께 리턴될 수 있다. 서버는 매체 객체 또는 워터마크된 매체 객체와 함께 재생될 다른 매체 신호의 디코딩 또는 디스크립팅을 제어하기 위해 코드를 리턴할 수 있다. 또한, 서버는 코드 및/또는 링크들을 리턴하여 사용자가 라이선스를 확립하고, 국지적으로 및/또는 원격으로 라이선싱 컴퓨터(예를 들면, 인터넷을 통한 라이선싱 서버(licensing server))를 실행시키는 라이선싱 프로그램의 전자적인 사용권들을 얻도록 한다.
- <41> 서버는 (URL들, 명령어들 등을 제공함으로써) 취해진 작용들을 정의하는 XML과 같은 데이터를 리턴할 수 있다. 작용들의 정의 등을 수신하는 장치 또는 클라이언트 컴퓨터는 작용을 실행시키거나, 또는 이들을 사용자에게 사용자 입력(예를 들면, 음성 인식 엔진 등을 통해 음성 명령들에 응답하여 컴퓨터의 사용자 인터페이스에서의 옵션의 그래픽적 표현을 클릭함)에 응답하여 실행되는 옵션들로서 제시한다.
- <42> 사용자는 사용자 인터페이스에서의 객체의 그래픽적 표현을 선택함으로써 링크된 정보 또는 작용들에 액세스할 수 있다. 예를 들면, 사용자는 객체를 나타내는 아이콘 또는 객체(예를 들면, 이미지)의 렌더링된 버전을 "클릭-온"하여, 메타데이터 또는 작용들이 객체와 링크되었는가의 여부를 결정하거나, 또는 메타데이터의 링크된 작용 또는 검색을 개시할 수 있다.
- <43> 워터마크 디코더는 소정의 간격들로 이벤트에 응답하거나, 또는 사용자 요구에 응답하여 특정한 위치(예를 들면, 디렉토리들, 하드 드라이브 등)의 매체 객체들 내에서의 워터마크들의 존재를 탐색하도록 설계될 수 있다. 예를 들면, 워터마크 디코더는 파일 탐색 유틸리티와 유사한 유틸리티 서비스로서 실행될 수 있어서, 사용자는 매체 객체 파일, 또는 파일들의 그룹으로부터 워터마크 링크를 추출을 야기할 수 있다. 다른 예로서, 오퍼레이팅 시스템은 선택된 저장 위치에 주어진 타입의 모든 파일 상에서(예를 들면, 하드 드라이브 상에서) 부트업시 디코더를 불러오도록 설계될 수 있다. 오퍼레이팅 시스템은 또한 백그라운드 유틸리티로서 디코딩을 실행하여 매체 객체의 워터마크 링크에 대하여 주기적으로 검사한다. 타이머 또는 클록 서비스는 시간이 경과할 때나 또는 미리 결정된 시간 간격들로 워터마크 검출을 트리거하기 위해 사용될 수 있다. 오퍼레이팅 시스템은, 예를 들면, 파일 다운로드, 파일 저장 등의 기술된 이벤트가 발생하였을 때, 디코더를 실행할 수 있다. 이러한 이벤트들에 응답하여 디코더를 트리거링함으로써, 오퍼레이팅 시스템은 상기 매체 객체들이 오퍼레이팅 시스템이 실행되는 시스템 또는 장치에 언제 입력하고, 이들이 언제 편집되는가가 검사될 수 있도록 한다.
- <44> 워터마크 디코더의 효율을 향상시키기 위하여, 파일 시스템은 매체 객체들이 워터마크들에 대하여 검색되는 때, 트래킹을 위한 구조를 구현할 수 있다. 일례의 구조에서는, 속성을 각 매체 객체에 할당하여, 검사되었는가의 여부, 워터마크되었는가의 여부, 그렇다면, 워터마크된 때를 표시한다. 이 후, 디코더는 상기 정보를 사용하여, 검사되지 않거나 또는 변화된 매체 객체만을 검사하거나, 또는 최종 검사까지 주어진 시간이 경과하는 동안 매체 객체들에 대해서 검사된다. 매체 객체가 변화된 때마다, 마크가 검사되었음을 나타내는 속성이 새롭고 변화된 객체만이 다시 검사될 수 있도록 리셋될 수 있다.
- <45> 이러한 개념을 예시하기 위하여, 윈도우 오퍼레이팅 시스템에서의 실행을 고려한다. 도 1은 매체 객체의 워터마크 임베딩 및 판독을 지원하기 위한 윈도우 익스플로러 사용자 인터페이스의 확장의 일례를 예시한다. 매체 객체 파일들은 일반적으로 윈도우 익스플로러 파일 브라우저의 사용자 인터페이스(102) 내의 아이콘들(100)로 표시된다. 이 파일 아이콘(100) 위에 커서를 위치하면서 마우스를 클릭함으로써, 사용자는 선택된 매체 객체와 연관된 옵션들의 콘텍스트 메뉴(104)에 액세스할 수 있다.
- <46> 상기 "워터마크 알림(watermark aware)" 파일 브라우저는 "판독 워터마크" 또는 "워터마크" 같은 옵션을 리스팅함으로써 콘텍스트 메뉴의 옵션들을 증대시킨다. 사용자가 "판독 워터마크" 옵션 위에 커서를 위치시키면, 오

퍼레이팅 시스템은 매체 객체 상의 워터마크 디코더를 불러온다. 워터마크 디코더는 네트워크 통신 소프트웨어와 관련된 워터마크 링크 및 작용들을 추출하여, 메타데이터에 액세스하고, 워터마크 링크와 연관된 데이터베이스로부터 아이템을 검색한다. 파일 브라우저는 이러한 아이템들을 윈도우(106)에 디스플레이한다.

- <47> 메타데이터 데이터베이스에 액세스하기 위한 방법은 다양하다. 메타데이터는 국지적으로(매체 객체와 같은 기기에서), 근거리 네트워크(local area network) 또는 광대역 네트워크(wide area network)로 저장될 수 있다. 데이터베이스가 인터넷 같은 컴퓨터 네트워크 상의 원격 컴퓨터에 위치하면, 네트워크 통신 소프트웨어는 데이터베이스와의 접속 확립을 위해 사용될 수 있다.
- <48> 선택될 때, "워터마크" 옵션은 판독 및 임베딩 정보("Read Infomation..." 및 "Embed Infomation...")에 대한 다른 옵션들을 디스플레이한다. 윈도우 라벨링된 이미지 정보(106)는 이미지와 연관된 메타데이터 및 작용들을 이들에 임베딩된 워터마크 링크를 통해 디스플레이한다. 본 예에서, 윈도우(106)는 이미지의 썸네일(thumbnail), 이미지 속성들(예를 들면, 폭, 높이, 해상도, 픽셀당 비트), 및 HTML 링크들(108 내지 116)의 시리즈를 부가 정보 및 작용들(예를 들면, 링크들(114, 116)에 관련된 이미지들에 대한 탐색)에 디스플레이한다.
- <49> 워터마크를 통해 링크된 아이템들을 디스플레이하기 위한 다른 방법으로는, 이들을 도 2에 나타난 바와 같이 추가 속성 페이지(additional property page) 내에 삽입하는 것이 있다. 파일 브라우저를 실행하는 동안, 사용자는 매체 객체의 아이콘 위에 커서를 위치시키면서 마우스의 우측 클릭을 함으로써 속성들(도 1에서의 옵션(118))에 액세스한다. 선택 속성들에 응답하여, 오퍼레이팅 시스템은 도 2에 나타난 것과 같은 속성들 윈도우(properties window)를 디스플레이한다. 각각의 매체 객체와 연관된 속성 페이지들은 탭(예를 들면, 범용, 이미지, 워터마크, 보안)을 갖는다. 워터마크 페이지는 도 2에서 선택된다. 도 1의 윈도우(106)에 디스플레이된 옵션들과 같이, 워터마크 페이지(watermark page)는 HTML 링크들(202 내지 210)의 시리즈를 부가 정보 또는 작용들에 리스트한다. 선택될 때, 링크는 인터넷 브라우저를 불러와서, 하부 URL에서 정보를 검색한다. 탐색(208 내지 210)와 같은 동작들을 위해, 링크는 URL에서 서버에 매체 객체의 속성들과 같은 부가 파라미터들을 통과시킬 수 있고, 이어서 상기 파라미터를 사용하여 탐색을 실행하고, 그 결과들을 인터넷 브라우저에 리턴한다.
- <50> 파일이 워터마크된 데이터를 포함하였음을 반영하는 다른 방법으로는, 파일 내에 워터마크의 존재를 암시하기 위하여 그래픽적 "워터마크 표시자" 아이콘을 파일의 아이콘에 중첩한다.
- <51> 이러한 실행은 변화될 수 있고, 도 1 및 2에 도시된 예들은 윈도우 익스플로러 파일 브라우저의 셸 확장들(shell extensions)이다. 디코더는 윈도우 익스플로러의 COM 객체 클라이언트(COM object client)로서 실행된다. COM 객체 클라이언트는 셸 확장 핸들러(shell extension handler)로서 오퍼레이팅 시스템으로 등록된다. 도 1은 콘텍스트 메뉴 핸들러(context menu handler)를 도시하고, 도 2는 속성 페이지 핸들러(properties page handler)를 도시한다.
- <52> 다른 가능한 구현은 메타데이터 옵션을 취하여 디스플레이하는 메타데이터 검색 애플리케이션(metadata retrieval application)을 론칭하기 위해 셸 실행 명령(shell execute command)을 사용하는 셸 확장을 실행하는 것이 있다. 이 구현은 콘텍스트 메뉴 확장(context menu extension)과 같은 확장을 파일 브라우저 사용자 인터페이스에 부가한다. 사용자가 파일 브라우저 사용자 인터페이스 내의 매체 파일 객체를 선택할 때, 사용자는 옵션을 갖는 콘텍스트 메뉴를 디스플레이하여, 소정 타입의 매체 객체들과 연관된 메타데이터 검색 프로그램을 론칭한다. 복수의 작용들이 상기 옵션과 연결될 수 있다. 한 작용은 메타데이터 검색 애플리케이션 프로그램을 론칭하는 것이다. 다른 작용들은 선택된 옵션을 재생하기 위해 매체 플레이어를 론칭하는 것이다. 물론, 이 두 가지 작용들은 멀티태스킹 오퍼레이팅 시스템에서 동시에 개시될 수 있다.
- <53> 메타데이터 검색 애플리케이션의 일례는 워터마크 메시지를 추출하고, 이 메시지에서부터의 객체 식별자를 메타데이터 서버에 포워드시킨 후, 메타데이터를 리턴시키는 워터마크 디코더가 있다. 상술한 바와 같이, 검색 애플리케이션은 워터마크로부터의 객체 식별자가 이미 검출되어, 메타데이터를 검색하기 위해 최근에 사용되었다면, 객체 식별자를 검출할 필요가 없다. 대신에, 검색 애플리케이션은 사용자에게 메타데이터 및 작용들의 디스플레이를 행할 수 있다.
- <54> 검색 애플리케이션을 론칭하기 위하여, 셸 실행 명령은 매체 객체의 명칭 및 위치를 검색 애플리케이션에 전해진다. 검색 애플리케이션은 그 자신의 사용자 인터페이스를 제시하여, 링크된 메타데이터 및 작용들을 디스플레이하거나, 또는 이것들을 파일 브라우저에 전한 후, 이것들을 속성들 페이지 또는 콘텍스트 메뉴 확장 같은 확장 내에 디스플레이한다. 검색 애플리케이션은 워터마크 디코딩 전, 또는 메타데이터 서버로부터 메타데이터

의 갱신을 요구하기 전에, 허용을 요구하기 위해 사용자에게 촉구할 수 있다. 또한, 검색 애플리케이션은 인터넷 브라우저와 같은 하나 이상의 다른 애플리케이션을 론칭하여, 웹서버로부터 메타데이터에 대한 요구를 발행하고, 서버로부터 리턴된 HTML 문서 내의 메타데이터 및 작용들을 디스플레이할 수 있다.

<55> 상술된 방식은 이미지, 비디오 및 오디오 파일을 포함한 다양한 매체 객체 파일에 대하여 실행될 수 있다. 또한, 객체 식별자는 워터마크 내에 삽입될 필요가 없지만, 대신에 파일 헤더(file header)와 같은 매체 객체 파일 외의 어떤 곳에도 배치될 수 있다.

<56> 브라우저 내

<57> 워터마크 디코더는 또한 인터넷 브라우저 애플리케이션 내에 통합될 수 있다. 파일 브라우저와 같이, 인터넷 브라우저는 로컬 컴퓨터 내, 또는 네트워크간 파일들의 디렉토리들을 브라우징할 수 있다. 마이크로소프트사의 인터넷 익스플로러 및 네스케이프 네비게이터 같은 상용의 브라우저는, 일반적으로 HTTP 및 FTP 같은 전달 프로토콜들을 지원하고, HTML, 자바, 비주얼 베이직 및 스크립트(예를 들면, 자바 스크립트, 비주얼 베이직 스크립트 등)를 포함한 코드를 해석 또는 컴파일링하기 위한 부가적인 구성요소를 갖는다. 또한, 인터넷 브라우저들은 컴퓨터 또는 다른 장치의 사용자 인터페이스 내에 디스플레이하기 위해 HTML을 분석하여 렌더링할 수 있다.

<58> 인터넷 브라우저 내에 워터마크 디코더를 통합하는 것에 대해 예시하기 위하여 다음의 예들을 고려한다. 인터넷 브라우저가 인터넷 상에서 매체 객체들과 함께 웹페이지들을 다운로드하여 분석함에 따라, 상기 객체들의 리스팅을 유지하고, 워터마크의 존재에 대하여 검색한다. 리스팅 시에는, 워터마크의 존재를 반영하기 위하여 워터마크를 갖는 객체의 표현에 애노테이팅하고, 매체 객체가 설정된 경우에 URL과 같은 다른 데이터에 애노테이팅한다. 사용자는 매체 객체들의 비주얼 표현을 나타내는 애플리케이션 윈도우(예를 들면, 애플리케이션 바)를 봄으로써 상기 리스트에 액세스할 수 있다. 이미지들에 대하여, 매체 객체를 표시하는 한가지 방법으로는 이미지의 썸네일을 사용하는 것이 있다. 이미지들 및 다른 객체들은 그래픽적 아이콘, 텍스트 기술, 또는 이들 모두로서 나타낼 수 있다.

<59> 워터마크 객체들은 구별 사운드 또는 로고와 같은 비주얼 또는 오디오 표시자로 구별될 수 있다. 사용자는 워터마크-가능하게 된 객체의 표현을 소정의 형태로 선택함으로써 매체 객체와 연관된 메타데이터 또는 작용들을 본다. 예를 들면, 사용자는 썸네일, 아이콘, 로고 또는 텍스트 기술을 클릭함으로써, 워터마크를 통해 객체와 링크된 메타데이터 또는 작용들의 메뉴에 액세스할 수 있다.

<60> 워터마킹된 객체들을 표시하는 다른 방법은 사용자가 워터마킹된 객체 위에 커서를 보낼 때 소프트웨어 애플리케이션의 그래픽적 사용자 인터페이스 내의 커서의 모양, 또는 그래픽적 사용자 인터페이스 내에 디스플레이된 객체의 표현을 변경하는 것이 있다. 커서를 변경하는 하나의 방법은 이 커서를 종래의 포인터로부터 검출되어 워터마킹된 객체 타입과 연관된 구별 그래픽 아이콘으로 변경하는 것이 있다. 다른 방법으로는, 프레임들의 시퀀스를 통해 소정의 다른 형상 또는 그래픽적 설계로 모프(morph)한 커서를 애니메이션하는 것이다. 마찬가지로, 사용자 인터페이스는 사용자가 커서를 이동시킴에 따라 워터마킹된 객체의 외관을 변형시킬 수 있다. 또한, 사용자 인터페이스는 사용자가 워터마크를 포함하는 것을 나타내기 위해 객체 위에 커서를 보낼 때, 구별 사운드(distinctive sound)를 생성할 수 있다.

<61> 미국특허출원 제 09/165,142 호는 HTML 페이지 내의 이미지로부터 워터마크를 어떻게 디코딩하고, 워터마크가 존재함을 나타내는 로고로 이미지를 애노테이팅하는 예를 개시한다. 여기서는, 브라우저의 애플리케이션 윈도우에서 매체 객체(이미지의 썸네일)의 표현을 나타내는 방법을 설명한다. 그 한가지로, 상기 애플리케이션 윈도우는 이미지들의 썸네일들을 디스플레이하도록 사용되어, 인터넷 등 상에 웹페이지들을 브라우징하면서 나타나는 이미지들의 히스토리를 나타낸다. 사용자는 이미지를 클릭함으로써, 이것을 독립 "북마크" 또는 "선호(favorites)" 리스트에 추가할 수 있다. 다른 애플리케이션 윈도우는 상기 북마크 리스트 내에 이미지들의 썸네일들을 디스플레이하기 위해 사용될 수 있다. 이미지 또는 이미지의 표현을 선택함으로써, 브라우저는 선택된 이미지와 연관된 네트워크 리소스에 (예를 들면, 연관된 URL을 통해) 링크한다. 상기 네트워크 리소스는 이미지가 생성된 웹페이지일 수 있다. 대안으로, 리소스는 이미지에 임베딩된 워터마크 링크를 통해 참조된 웹페이지일 수 있다. 워터마크 메시지는 URL, 또는 웹페이지 같은 네트워크 리소스의 URL을 록업하기 위해 사용되는 객체 식별자일 수 있다. 예를 들면, URL은 소유자의 웹페이지 또는 라이선싱 서버와 링크할 수 있다.

<62> 미국특허출원 제 09/165,142 호에 기술된 방법들은 비디오 및 오디오 신호와 같은 다른 매체 객체에 적용될 수도 있다.

- <63> 사용자를 워터마크를 통해 매체 객체와 링크된 메타데이터 및 작용들에 액세스시키는 한가지 방법으로는, 이들을 인터넷 브라우저의 사용자 인터페이스 내의 메뉴에 디스플레이하는 것이 있다. 도 3은 인터넷 브라우저의 사용자 인터페이스(300) 내의 매체 객체와 연관된 메타데이터 및 작용들을 디스플레이하는 방법의 일례를 나타낸다. 브라우저 리스너 프로그램(browser listener program)은 인터넷 브라우저로부터 이벤트를 수신하여, 웹 페이지가 다운로드된 때를 표시한다. 이 리스너는 웹페이지 내의 매체 객체들의 어드레스 또는 어드레스들을 브라우저로부터 요청한다. 이 어드레스는 매체 객체가 메모리(메인 메모리, 비주얼 메모리, 캐시 등) 내에 잔류함을 표시한다. 리스너는 매체 객체 또는 객체들 상의 워터마크 디코더를 불러내서, 이것을 메모리 내의 객체의 어드레스에 보낸다.
- <64> 워터마크를 발견하면, 리스너는 핸들러 프로그램을 메모리 내의 웹페이지 내에 삽입한다. 상기 핸들러 프로그램은 로고 또는 다른 표시자를 사용자에게 제시하여, 워터마크의 존재를 표시하고, 핫 링크를 정보 및 작용들에 제공한다. 예를 들면, 도 3의 표시자는 브라우저의 사용자 인터페이스 내의 워터마킹된 이미지 객체의 렌더링된 버전(304) 위에 추가된 로고(302)이다.
- <65> 사용자가 로고 위에 커서를 보내고, 이것을 선택하면, 이와 연관된 핸들러 프로그램은 도 4에 나타낸 바와 같이 옵션들의 메뉴(400)를 디스플레이한다. 리스너 프로그램은 메타데이터 서버(예를 들면, 로컬 또는 원격 데이터 베이스)와의 접속을 확립하고, 워터마크로부터 추출된 객체 식별자를 서버에 전달하고, 서버로부터 연관된 아이템들을 수신함으로써 상기 옵션들을 검색한다. 상기 아이템들은 매체 객체와 관련된 웹페이지들, 매체 객체에 관한 정보와의 URL 링크들, 또는 라이선싱 서버(licensing server)와 같은 작용과의 링크들을 포함할 수 있다.
- <66> 특정한 실행들은 변화될 수 있는데, 도 3 및 도 4에 도시된 예는 문서 뷰 확장들(document view extensions)을 사용하여 마이크로소프트사의 인터넷 익스플로러 브라우저에 실행된다. 마이크로소프트사의 동적 HTML은 인터넷 익스플로러 리스너 프로그램이 코드를 삽입하여 HTML 문서를 변화시키도록 인터페이스를 제공한다. 상기 인터페이스를 사용함으로써, 리스너 프로그램은 디스플레이를 제어하는 자바 스크립트를 삽입하여, 도 3에 나타낸 이미지에 중첩된 로그로의 입력에 응답한다.
- <67> 소정의 애플리케이션에서, 매체 콘텐츠 및 웹사이트 개발자는 워터마크 링크와 연관된 기능을 선택적으로 가능하게 또는 불가능하게 하고자 한다. 이러한 특징들을 구현하기 위한 한가지 방법으로는, 제어 파라미터(헤더 파일 내의 플래그 등)를 포함하도록 매체 객체의 컨테이너(예를 들면, HTML)로서 작용하는 매체 객체 파일 또는 다른 파일을 변경하는 것이 있다. 이러한 제어 파라미터는 워터마크 가능하게 된 매체 객체의 존재, 및 워터마크 링크가 가능 또는 불가능하게 되었는가의 여부를 표시한다. 제어 파라미터는 명확히 턴 오프되거나 또는 그 반대가 아니라면, 액티브로 디폴트로 되도록 설계될 수 있다. 콘텐츠 개발자들이 웹사이트와 같은 소정의 멀티미디어 작업시에 객체를 포함할 때, 이들은 제어 파라미터를 통해 워터마크 링크를 불가능하게 할 수 있다. 편집 툴들, 다른 애플리케이션 프로그램들, 및 장치들은 워터마크 링크를 불가능하게 하기 위해 명확하게 지시되지 않을시, 플래그를 되돌리도록 설계될 수 있다.
- <68> 다른 애플리케이션들에서, 워터마크가 연관된 메타데이터와의 영속적인 링크로서 작용하는 것이 중요하다. 매체 객체가 다른 시스템들을 통해 이동함으로써, 코딩/디코딩되고, 변경 등이 되기 때문에, 매체 객체 파일에 저장된 종래의 메타데이터를 잃을 수 있다. 이 경우들에서, 워터마크 링크는 워터마크가 여러 가지 변형들의 형태들(예를 들면, 디지털 대 아날로그 변환, 아날로그 대 디지털 변환, 압축 등)에 내성이 있기 때문에 메타데이터를 복원하기 위해 사용될 수 있다.
- <69> 워터마크를 통해 이용될 수 있도록 이루어진 기능을 선택적으로 제어하는 다른 방법으로는, 사용자가 매체 객체들 상으로의 워터마크 디코딩을 가능 또는 불가능하게 하는 것이다.
- <70> 워터마크는 또한 브라우저의 파일 캐시 시스템(file cache system)에 대한 속성으로 사용될 수 있다. 이는 캐시 브라우저 애플리케이션들이 캐시된 파일들이 워터마킹되었는가를 식별하도록 하고, 본 문헌 전반에 설명된 바와 같이 워터마크 내에 임베딩된 정보와 연관된 기능들을 수행하게 한다.
- <71> **다른 애플리케이션들 내**
- <72> 상기 요약한 특징들은 매체 객체들을 프로세싱하는 장치들 또는 소정의 소프트웨어 애플리케이션들 내에서 구현될 수 있다. 예를 들면, 매체 객체 데이터베이스 관리 시스템은 유사한 기능을 구현할 수 있다. 디지털 자산 관리(digital asset management) 및 디지털 권리 관리 시스템(digital rights management)은 워터마크 가능하게 된 링크들을 사용하여 매체 객체들의 사용을 추적하고 제어할 수 있다.



- <73> 워드 프로세싱, 스프레드시트, 프리젠테이션 프로그램들, 매체 객체 편집 툴들 등의 매체 객체에 필요한 다른 애플리케이션들은 매체 객체들을 부가 정보 및 작용들과 링크시키기 위해 상기 요약한 특징들의 소정의 버전을 모두 사용할 수 있다.
- <74> 많은 애플리케이션 프로그램들은 본 문헌에서 설명된 기술을 사용하여 향상될 수 있는 파일 브라우저 능력을 갖는다. 예를 들면, 파일 개방 명령(File Open command)은 종종 파일 객체들을 브라우징하기 위해 사용된다. 상술된 콘텍스트 메뉴 및 속성 페이지 확장들은 파일 브라우징 서비스들을 제공하는 애플리케이션들에 대해 구현될 수 있다.
- <75> 워터마크 인코딩 및 디코딩 기능은 또한 넵스터(Napster), 구텔라(Gnutella), 프리넷(Freenet), 스코어(Scour) 등의 피어 투 피어 파일 공유 시스템(peer to peer file sharing systems)과 같은 파일 공유 시스템으로 통합될 수 있다. 파일 공유 시스템에서, 파일 공유 소프트웨어는 컴퓨터 네트워크와 상호접속된 복수의 클라이언트 컴퓨터들 상에서 실행된다. 이러한 소프트웨어는 이것을 실행시키는 컴퓨터와 함께 네트워크와 상호접속된 다른 컴퓨터 내에 공유하기 위해 사용될 수 있는 파일들을 추적한다. 파일 공유 소프트웨어는 워터마크 또는 다른 형태로 파일에 임베딩된 데이터를 사용하여, 파일 전송(컴퓨터에 파일들을 업로딩 또는 다운로드함)을 제어해서, 파일이 완전하고 바이러스가 없음을 확인하고, 파일 공유 시스템 내의 파일들을 탐색하기 위해 사용될 수 있는 메타데이터를 전달하고, 사용 권리를 얻거나, 또는 파일에 대한 지적소유권 또는 관련 제품들 또는 서비스들을 구입하기 위한 기회들 및 부가 정보와의 링크들을 전달할 수 있다. 이러한 기능들에 액세스하기 위하여, 파일 공유 소프트웨어는 워터마크 또는 다른 임베딩된 데이터 디코딩 소프트웨어를 포함한다. 상기 기능을 삽입하거나 또는 변경하기 위하여, 파일 공유 소프트웨어는 워터마크 또는 다른 임베딩된 데이터 인코딩 소프트웨어를 포함한다. 본 출원에 관한 더 많은 정보를 위하여, "Using Embedded Data with File Sharing"로 명칭되어 2000년 7월 20일 출원된 미국특허출원 제 09/620,019 호를 참조한다.

#### **콘텍스트 민감형 워터마크 링크들**

- <76> 삭제
- <77> 워터마크를 통해 매체 객체와 링크된 작용들 또는 정보는 콘텍스트 민감형이다. "콘텍스트"의 소정 예들은 애플리케이션 콘텍스트(예를 들면, 객체에서 오퍼레이팅하는 애플리케이션 프로그램이라 함), 객체 위치 콘텍스트(여기서, 객체는 사용자와 관련하여 잔류함)를 포함한다. 예를 들면, 링크의 상태는 워드 프로세싱 문서, 스프레드시트 또는 프리젠테이션 같은 문서 내에 객체를 삽입하는 것에 반하여, 편집 툴에서의 객체를 사용자가 조작할 때는 다를 수 있다. 또한, 워터마크 링크의 상태는 객체가 로컬인가, 사용자와 관련된 인터넷 또는 인터넷 상에 있는가의 여부에 기초하여 변화될 수 있다.
- <78> 디코더 애플리케이션은 매체 객체의 콘텍스트에 따라 다른 메타데이터 또는 프로세싱 작용들과 링크할 수 있다. 이러한 기능을 실행하기 위하여, 워터마크 디코더는 콘텍스트 정보를 메타데이터 데이터베이스에 제공하고, 이어서 콘텍스트 특정 메타데이터를 제공하거나, 또는 콘텍스트 특정 작용들을 개시한다. 예를 들면, 객체가 편집 툴로 편집되면, 디코더는 편집 툴에 관한 정보를 워터마크로부터 추출된 링크와 함께 데이터베이스에 공급한다. 마찬가지로, 디코더는 객체가 사용자의 컴퓨터에 대해 잔류함을 표시하는 콘텍스트 정보를 공급할 수 있다. 키로서 콘텍스트 정보를 사용하여, 메타데이터 데이터베이스는 메타데이터를 리턴시키거나, 또는 콘텍스트와 연관된 프로세싱 작용들을 개시한다.
- <79> 콘텍스트 민감형 상태를 구현하기 위한 다른 방법은 디코더가 매체 객체의 콘텍스트에 기초하여 워터마크 링크된 작용 또는 정보의 프리젠테이션을 제어하도록 하는 것이 있다. 콘텍스트가 애플리케이션에 의해 정의된 경우, 상기 방식은 링크된 메타데이터 또는 작용들 모두에 애플리케이션 액세스를 제공한 후, 링크된 작용들 또는 정보의 애플리케이션 제어 프리젠테이션을 사용자에게 제공하는 것과 유사하다. 이러한 시나리오에서, 메타데이터 데이터베이스는 적어도 링크된 정보 및 작용들의 디스크립터(descriptor)를 리턴시키고, 애플리케이션은 콘텍스트에 기초하여 적용하기 위한 정보 및 작용들의 서브 세트를 선택한다. 콘텍스트가 객체의 위치에 의해 정의되는 경우, 디코더는 마찬가지로 형태로 동작한다. 예를 들면, 오브젝트의 위치에 기초하여 정보의 링크된 작용들의 서브-세트를 선택할 수 있다.
- <80> 콘텍스트 정보의 특정 예는 "쿠키(cookie)" 기술을 사용한 인터넷상에서 웹 서버에 사용자의 컴퓨터에 의해 공급된 사용자 정보이다. 우선, 사용자의 컴퓨터는 이미지, 오디오 또는 비디오 신호 같은 매체 객체로부터의 워터마크를 디코딩한다. 이 후, 사용자 정보를 포함한 쿠키와 함께 워터마크로부터 추출된 정보를 메타데이터 서

버 또는 라우터(일반적으로는 서버라 함)에 전송한다. 서버는 매체 객체 내의 워터마크로부터 추출된 정보와 함께 쿠키로부터의 사용자 정보를 조작하여, 사용자에게 개인화된 정보 또는 작용들을 록업한다. 메타데이터 서버는, 예를 들면, 쿠키를 분석하고, 이것을 사용하여 쿠키 내의 정보에 관한 데이터베이스 내의 네트워크 리소스(웹페이지의 URL)로의 정보 또는 어드레스들을 참조한다. 서버는 또한 워터마크 정보를 사용함으로써 영속적인 정보 또는 링크들을 좁혀서, 워터마킹된 객체에 영속하는 정보 또는 링크들의 서브세트를 록업한다. 데이터베이스 동작들에 의해 참조된 서버, 또는 다른 네트워크 리소스는 연관된 정보를 디스플레이 또는 오디오 출력 장치 상에 렌더링하기 위한 사용자 컴퓨터에 리턴한다. 이러한 방식은 사용자에게 관심있을 만한 특종 뉴스, 광고, 콘텐츠 등에 리턴된 정보를 제한하기 위해 사용될 수 있다. 유사한 결과가 쿠키 정보와 마찬가지로 사용되는 사용자의 선호들을 공급하기 위해 사용자의 컴퓨터를 프로그래밍함으로써 달성될 수 있다.

#### <81> 다중 워터마크 타입들 지원

<82> 워터마크 기술이 발전함에 따라, 매체 객체들은 워터마크 인코더들 및 디코더들과 각각 연관된 다른 타입들의 워터마크들을 가질 수 있다. 다른 워터마크 타입들에 적응시키기 위하여, 디코더는 다른 워터마크 프로토콜들을 지원하도록 설계될 수 있다. 워터마크 프로토콜들은 키들 및 소정 타입의 워터마크를 디코딩할 방법을 지정하는 다른 파라미터들을 제공한다. 대안으로, 공통 애플리케이션 프로그래밍 인터페이스(Application Programming Interface; API)는 다른 코어 워터마크 인코더(core watermark encoder) 및 디코더 소프트웨어 모듈들 또는 장치들에 대하여 지정될 수 있다. 이러한 구조들은 워터마크 인코더 및 디코더 기능들을 불러내는 많은 다른 타입들의 애플리케이션들 및 장치들의 개발을 촉진시키지만, 워터마크 프로토콜 및/또는 코어 워터마크 방법들과는 무관하다.

<83> 다른 코어 워터마크 방법을 지원하기 위하여, 사용자는 2개 이상의 다른 코어 워터마크 인코더/디코더 모듈들을 설치할 수 있다. 예를 들면, 코어 모듈들은 플러그-인들(plug-ins) 또는 동적 링크 라이브러리들로서 실행될 수 있다. 모듈을 인스톨할 때, 인스톨 프로세스가 윈도우 오퍼레이팅 시스템 내의 레지스트리 같은 레지스트리(registry)를 갱신하여, 워터마크 타입이 지원됨을 반영한다. 이러한 방식에서는, 다른 매체 타입들에 대한 워터마크 디코더들, 및 단일 매체 타입에 대한 다른 디코더들의 타입들이 지원될 수 있다.

<84> 매체 객체가 미지의 타입의 워터마크를 포함하는 경우들에서, 매체 객체 파일은, 예를 들면, 파일 헤드 내의 파라미터를 통해 워터마크 타입을 지정할 수 있다. 파일 브라우저, 또는 코어 워터마크 모듈의 다른 클라이언트는 매체 객체로부터 타입 파라미터를 추출하고, 이것과 매체 객체로의 참조를 API를 통해 코어 모듈에 전달한다. API는 적절한 코어 모듈(appropriate core module)로의 요구를 라우팅한 후, 워터마크 메시지를 추출하고, 이것을 API에 리턴시킨다. API는 이 메시지를 요구 애플리케이션에 전달한다.

<85> 타입 파라미터가 이용되지 않는 경우, 애플리케이션 또는 장치 프로세싱 객체는 소정의 프로토콜이 존재하는가를 검색하기 위하여 모든 지원된 워터마킹 프로토콜 전반을 번호화할 수 있다. 소정의 매체 또는 파일 타입에 대한 워터마크 프로토콜들은 장치 또는 애플리케이션 내에(예를 들면, 오퍼레이팅 시스템의 레지스트리 내에) 등록될 수 있다. 각각에 대한 검사를 위하여, 애플리케이션은 이들 프로토콜들에 대한 워터마크 스크리닝 프로세스(watermark screening process)를 불러와서, 프로토콜들과 연관된 워터마크가 존재하는가의 여부를 결정한다.

#### <86> 매체 객체 브랜딩

<87> 워터마크는 다른 서비스들과의 전자 액세스(electronic access)를 촉진함과 더불어 "브랜딩(branding)"을 확립하기 위하여 사용될 수 있다. 이러한 브랜딩 애플리케이션에서, 클라이언트측의 워터마크 디코더 임베딩된 애플리케이션 또는 장치는 객체로부터의 임베딩된 워터마크 메시지를 판독하고, 이것을 사용하여 썸네일 이미지(예를 들면, 브랜드 "브랜드 이미지")와 같은 디지털 로고에 액세스한다. 디코더-인에이블 애플리케이션(decoder-enable application)은 워터마크 메시지에서부터 취해진 객체 식별자를 로그 리턴에 응답하여 서버(예를 들면, 인터넷상의 메타데이터 서버)에 전송한다. 이 후, 애플리케이션은 바람직하게는 매체 객체의 렌더링된 버전 또는 그 그래픽적 표현을 클라이언트 컴퓨터 또는 장치의 사용자 인터페이스에 중첩된 로고를 렌더링한다.

<88> 일부 시나리오들에서, 서버는 또한 범용 "사용권" 서버 또는 매체 소유자에 의해 유지되는 고객 "사용권"으로 어드레스(예를 들면, URL) 포인팅을 리턴시킨다. 인터넷 콘텍스트에서, 서버는 관련 웹사이트에 하나 이상의 링크를 리턴시킬 수 있다. 접속권 및 통합 브랜딩 서비스들은 인터넷상의 중앙 서버를 통해 제공될 수 있다.

<89> 작용 및 메타데이터와의 링크를 위해 객체 식별자를 이용함으로써, 워터마크 인에이블 애플리케이션(watermark enabled applications)은 브랜딩 및 사용권 서비스들을 확인하기 위한 많은 옵션들을 갖는다. 애플리케이션은

객체 식별자와 연관된 "갱신 가능한" 사용권을 디스플레이할 수 있다. 가상 매체 객체들(virtual media objects)에서, 애플리케이션은 렌더링된 객체부 위에 (소정 주기 동안 주기적으로 비디오 프레임의 코너에) 중첩된 브랜딩 로고를 시각적으로 디스플레이하거나, 또는 매체 객체의 재생이 제시되기 전에 스플래시 스트린 개시로서 디스플레이될 수 있다. 브랜딩 정보를 보다 약화시키기 위하여, 메뉴를 통한 요구시에(예를 들면, 사용자가 "도움말" 메뉴 또는 객체의 표현을 클릭할 때) 액세스할 수 있다.

<90> 브랜딩 서비스는 콘텐츠 소유자의 홈페이지 또는 라이선싱 서버로의 핫 링크와 같은 부가적인 기능을 갖는 실질적인 항상 존재하는 브랜딩 기회로 저작권 통지의 의사를 변형시킨다. 브랜딩 서비스는 워터마크 페이로드시, 카피 관리 명령어(copy managemament instruction) 같은 다른 워터마크 가능하게 된 기능과 연관될 수 있으며, 예를 들면, 제어 파라미터는 객체가 재생되고, 카피되고, 기록되고, 다른 장치 또는 시스템에 변형될 수 있는가의 여부를 표시한다. 사용을 제어하기 위해 이러한 명령어를 제공함과 더불어, 워터마크 페이로드는 추가적인 값을 고객에게 제공하여(매체 객체와 연관된 서비스들 및 부가 정보와 링크시킴), 매체 객체가 재생 중 라벨링되고 브랜딩되도록 보증한다.

<91> 핫 브랜딩 링크들(hot branding links)를 더 정교히 하기 위하여, 사용권 서비스(usage rights services) 및 콘텍스트 민감형 링킹(context-sensitive linking)은 워터마크 링크를 소프트웨어 프로그램들, 메타데이터, 및 포인터들에 연관시킴으로써 상기 특징들을 지원하는 프로그램들 및 메타데이터에 부가될 수 있다. 이러한 특징들은 이들을 매체 객체 식별자 수신에 응답하여 실행되거나 또는 리턴될 작용 및/또는 메타데이터의 리스트에 부가함으로써 메타데이터 서버 내에 부가될 수 있다. 또한, 디코더 인에이블 애플리케이션은 객체 식별자에 대한 다른 서비스들의 세트들 또는 메타데이터를 제공하는 2개 이상의 서버들에 매체 객체 식별자를 전송하도록 프로그래밍될 수 있다.

#### <92> 메타데이터 통합

<93> 일부 애플리케이션에서, 매체 객체는 2개 이상의 다른 소스들로부터의 메타데이터와 연관될 수 있다. 메타데이터는 매체 객체를 저장하는 파일 내에 저장될 수 있다. 예를 들면, JPEG2000, TIFF, JPEG, PSG, PSD 같은 파일 포맷들은 메타데이터가 매체 신호(예를 들면, 이미지)와 함께 저장되게 할 수 있다. 매체 객체와 연관된 명령어들과 메타데이터는 매체 객체와 동일한 장치, 또는 원격 장치(예를 들면, 원격 데이터베이스)에 저장될 수 있다. 이러한 타입들의 애플리케이션들에서, 디코더들은 각 다른 소스들로부터 메타데이터를 추출하도록 프로그래밍될 수 있다. 파일 타입의 매체 타입은 상기 다른 소스들로부터의 메타데이터를 추출하기 위하여 디코더에 신호를 보낼 수 있다. 대안적으로는, 워터마크 메시지 또는 파일 메타데이터는 메타데이터의 다른 소스들을 변조할 수 있다.

<94> 상기 애플리케이션에서, 디코더는 하나 이상의 소스들로부터 메타데이터를 취하도록 설계된 후, 모든 정보의 통합하여 나타낸다. 디코더는 자동적으로 통합 기능을 수행하거나, 또는 사용자가 디스플레이를 위해 소망하는 메타데이터의 소스를 선택할 수 있다.

#### <95> 부가 기능

<96> 다수의 특징들이 워터마크 메시지 페이로드 및 다른 데이터와 작용들에 대한 워터마크 링크들을 사용하여 구현될 수 있다. 수 개의 예들이 이하에 강조된다:

#### <97> 메타데이터

<98> 메타데이터는 많은 형태들로 표현될 수 있고 부가적인 기능을 제공할 수 있다. 일반적으로, 메타데이터는 매체 객체에 관한 정보이다. 메타데이터는 또한 실행될 기기 명령, 또는 정보나 명령에 관한 참조(데이터베이스에 대한 객체, 사용자, 프로그램 또는 기기 식별자들, URL들, 포인터들, 어드레스들, 지표들 또는 키들 등)를 포함할 수 있다. 기기 명령어들은, 예를 들면, 객체의 렌더링, 디코딩, 암호화 또는 다른 프로세싱을 제어할 수 있다. 대안으로, 명령어들은 소정의 보조 기능을 제공할 수 있다.

<99> 메타데이터의 하나의 중요한 애플리케이션은 소유권 정보(ownership information)를 제공하는 것이다. 다른 것으로는 라이선싱 아이템 및 사용권을 제공하는 것이다.

<100> 메타데이터는 사용자 또는 다른 애플리케이션이 사용할 수 있는 매체 객체의 속성을 설명하기 위해 사용될 수 있다. 예를 들면, 하나의 속성으로는 애플리케이션이 비인증된 사용자에게 대하여 렌더링하는 것을 방지하는 제한을 하여 콘텐츠를 설계할 수 있다. 다른 속성으로는 객체가 렌더링되기 전에 지불 또는 라이선스를 추구하는 애플리케이션을 필요로 하는 상업용으로 객체를 설계할 수 있다.

- <101> **다중 워터마크들**
- <102> 매체 객체는 2개 이상의 워터마크들 또는 각각이 정보나 작용의 구별 세트와 연관된 워터마크 메시지들을 포함할 수 있다. 예를 들면, 매체 객체는 생성자 ID, 분배자 ID 등을 포함할 수 있으며, 이들은 각각 생성자 및 분배자에 관한 정보와 링크시킨다.
- <103> 객체가 전송, 카피 또는 편집됨에 따라 객체 생성 시간 또는 그 후에 매체 객체에 워터마크를 추가하는 다수의 방법들이 있다. 하나의 방법은 매체 객체의 다른 부분에 독립적인 워터마크들을 인터리브(interleave)하는 것이 있다. 이것은 매체 객체의 독립적인 속성들을 변경함으로써 달성될 수 있다. 상기 내용에서, "독립적인"이라 함은 각 워터마크들이 다른 워터마크들의 검출과 간섭하지 않는다는 것을 의미한다. 2개의 독립적인 워터마크가 매체 객체의 동일한 분리 샘플을 변경할 수 있지만, 이들은 워터마크 중 어떠한 것의 무효한 판독도 일으키지 않는 방식으로 행한다.
- <104> 독립적 워터마크들은 호스트 매체 신호(예를 들면, 이미지, 비디오, 오디오, 그래픽적 모델 등)의 다른 공간적 및 시간적 위치들에 배치될 수 있다. 또한, 이들은 신호의 다른 부분들의 위상, 에너지, 전력 등과 같은 신호의 독립적 특징들을 변경시킴으로써 독립적으로 이루어질 수 있다.
- <105> 상기 개념을 설명하기 위하여, 정지 이미지 객체(still image object)의 일례를 고려한다. 각 독립적 워터마크는 다른 워터마크 메시지(예를 들면, 매체 객체의 생성자, 분배자, 사용자 등에 대해 다른 워터마크 링크들)를 인코딩하기 위하여 사용되는 다른 프로토콜을 통해 정의될 수 있다. 독립적인 공간의 워터마크들은 각 워터마크들을 이미지에서 공간적 위치들의 고유 세트에 맵핑함으로써 인터리브될 수 있다.
- <106> 유사한 방식으로, 독립적 워터마크들은 각 워터마크를 고유의 시간적 위치들에 맵핑함으로써 오디오 또는 비디오와 같은 시간적인 데이터 시퀀스로 인코딩될 수 있다.
- <107> **디지털 권한 관리**
- <108> 워터마크는 매체 객체의 사용을 제어하는 정보 및 프로세싱 작용들에 링크될 수 있다. 예를 들면, 메타데이터는 라이선싱 기간과 조건들뿐만 아니라 객체에서의 지적재산권의 소유자를 표시할 수 있다. 또한, 워터마크 링크 또는 메타데이터는, 예를 들면, 사용자가 지불을 필요로 하고, 디코딩 키(decoding key)들을 교환하는(예를 들면, 암호화, 압축 등) 오브젝트의 사용을 제어하는 프로세싱 작용들을 트리거링한다. 소정량의 객체 디코딩이 워터마크를 추출하기 위해 필요하지만, 나머지 콘텐츠는 사용자가 적절한 사용권을 얻을 때까지 인코딩 및/또는 암호화될 수 있다.
- <109> 디지털 권한 관리 기능은 메타데이터 서버 같은 라이선싱 또는 사용권 서버에서 실행될 수 있다. 이 서버는 워터마크 메시지에 기초하여 소유자 및 라이선싱 기간들을 결정하고, 예를 들면, 사용자로부터의 지불 정보를 전자적으로 수신하고, 라이선스에 대한 사용자의 동의를 구하고 기록하며, 소유자와의 트랜잭션 상세를 포워딩하고, 사용권을 사용자에게 리터닝하는 객체 사용을 인증하기 위해 필요한 작용들을 실행한다. 사용자가 매체 객체를 재생하거나 렌더링함에 따라, 워터마크 디코더는 메시지를 서버에 전송하여, 사용예, 플레이어의 기기 ID, 사용 시간 등의 사용법에 관한 정보에 로그할 수 있다.
- <110> **사용권 제어를 위한 워터마크 및 컨텍스트 정보**
- <111> 워터마크 디코더는 또한 상기 객체의 사용을 제어하기 위해 매체 객체 내에 임베딩된 워터마크로부터 추출된 정보와 함께 컨텍스트 정보를 사용할 수 있다. 예를 들면, 워터마크 디코더는 객체가 잔류하는 장치 또는 시스템으로부터 유도된 워터마크 및 컨텍스트 정보에서 제어 데이터에 따라 매체 객체의 렌더링, 편집, 카핑 또는 전송을 제어하기 위해 프로그래밍될 수 있다. 예를 들면, 워터마크는 디코더에 명령하여, 소정 파일(예를 들면, 지정된 웹 페이지, 컴퓨터 시스템, 컴퓨터 네트워크 등) 이외라면 매체 객체의 렌더링을 금지시킨다. 상기 제어 데이터를 포함한 워터마크를 디코딩한 후, 디코더는 특정한 동작을 가능하게 하기 위해 존재해야 하는 영구 컨텍스트 정보(pertinent context information)를 결정한다. 이는 상기 동작들을 가능하게 하기 전에 사용자 식별자, 컴퓨터 식별자, 파일 식별자, 저장 매체 식별자, 컴퓨터 식별자, 네트워크 식별자 등의 존재를 검증함으로써 상기 작용을 포함할 수 있다. 이러한 식별자들은 이들이 식별하거나, 또는 상기 엔티티로부터 동적으로 유도된 엔티티와 연관하여 저장된다. 예를 들면, 파일 식별자는 파일 헤더 또는 푸터(header/footer) 내에 저장되거나, 또는 파일 내의 콘텐츠로부터 유도될 수 있다. 저장 장치 식별자는 저장 장치 상에 저장되거나, 또는 저장 장치나 이와 동일한 속성을 갖는 콘텐츠로부터 유도될 수 있다.
- <112> 상기 매체 객체들의 컨텍스트 민감형 제어는 특히 음악이나 영화 같은 매체 파일들의 사용을 제어시



유용하지만, 워터마크가 인코딩될 수 있는 다른 타입들의 매체 신호들에 적용된다. 예를 들면, 이 콘텍스트 민감형 제어는 매체 객체가 웹사이트의 콘텍스트, 컴퓨터, 저장 장치(예를 들면, CD 또는 DVD), 파일 공유 네트워크, 가입 서비스의 유료 가입자의 컴퓨터들, 관련 매체 객체들의 수집 등으로부터 제거될 때, 매체 객체의 렌더링, 카피 또는 전송을 금지하는데 사용될 수 있다.

#### <113> 자산 관리(Asset Management)

<114> 매체 객체 내에 임베딩된 워터마크는 자산 관리시 작용할 수 있다. 객체가 프로세스(개방, 편집, 카피 등)될 때마다, 디코더를 구비한 애플리케이션은 프로세싱 이벤트에 관한 정보를 로그할 수 있다. 대안으로, 인터넷을 통해 모니터링 서버에 트랜잭션 이벤트를 전송할 수 있다. 트랜잭션 이벤트는 그 ID, 사용자의 ID, 사용 시간 및 장소, 사용 특성(재생들의 횟수) 같은 객체에 관한 정보를 지정할 수 있다. 모니터링 서버 또는 애플리케이션은 상기 트랜잭션 이벤트를 데이터베이스에 기록하고, 요구시에, 주어진 객체의 사용에 관한 보고를 주어진 엔티티에 의해 발생한다. 트랜잭션 기록의 필드들 중 소정의 것은 데이터베이스에 질의하고, 고객 보고들을 생성하기 위하여 사용될 수 있다.

#### <115> 디렉토리 서비스들 통합

<116> LDAP(Lightweight Directory Access Protocol) 같은 디렉토리 서비스는 워터마크를 사용하거나, 또는 부가 기능을 제공하기 위하여 워터마크 디코더와 관련하여 동작할 수 있다. LDAP는 판독, 탐색, 부가 또는 제거 같은 디렉토리 동작을 수행하기 위하여 사용되는 온-더-와이어 프로토콜(on-the-wire protocol)이다.

<117> 예를 들면, LDAP 서비스는 워터마크 링크 및 매체 객체의 갱신 속성들을 추출할 때를 결정하기 위해 사용될 수 있다. 예를 들면, LDAP 서비스는 워터마크 디코더를 불러내고, 소정 시간에 메타데이터 서버로부터 그 속성들의 갱신을 검색함으로써 매체 객체의 속성들의 주기적인 갱신들을 제어할 수 있다. 워터마크 디코더를 유도하거나 또는 액세스하는 LDAP 탐색 필터(LDAP search filter)는 또한 컴퓨터상의 파일 디렉토리에 저장된 파일들 내의 워터마킹된 매체 신호들을 발견하기 위해 제공될 수 있다.

#### <118> 매체 객체 플레이어 및 딜리버리 통합

<119> 워터마크 디코더는 매체 객체들을 재생 또는 편집하기 위한 소프트웨어 및 장치들과 통합될 수 있다. 리쿼드 오디오, 마이크로소프트 및 리얼네트웍스의 다양한 상용 플레이어가 있다. 이러한 통합은 매체 객체에 링크된 메타데이터 및 작용들이 플레이어의 사용자 인터페이스를 통해 심리스(seamless) 형태로 사용자에게 액세스되도록 한다. 예를 들면, 사용자가 비디오 또는 오디오 파일을 재생할 때, 워터마크 인에이블 플레이어(watermark enable player)는 링크된 메타데이터 또는 작용들에 자동적으로 또는 사용자의 선택으로 액세스하여 디스플레이할 수 있다. 어떤 경우라도, 사용자는 메타데이터 또는 작용들이 객체 식별자를 통해 원격 서버로부터 얻어졌음을 알릴 필요는 없다. 또한, 이러한 통합은 콘텐츠 소유자가 객체에 링크하도록 하여, 객체가 언제 어디서 재생되더라도 재생 시에 사용 제어 정보 또는 작용들을 라이선싱 또는 주장할 수 있다. 이러한 정보 및 작용들은 객체 내의 워터마크에 데이터 또는 명령을 배치하거나, 또는 본 문헌 전반에 걸쳐 상세히 설명한 바와 같이 객체 외부에 메타데이터 또는 작용들과 링크한 워터마크 내에 객체 식별자를 놓음으로써 실행될 수 있다.

<120> 대부분의 경우에는, 사용자가 알 수 있는 워터마크를 통해 제공된 기능에 액세스하는 것이 바람직하다. 예컨대, 매체 플레이어는 사용자 인터페이스의 자연 확장에 나타나는 방식으로 워터마크를 통해 링크된 아이템들을 디스플레이할 수 있도록 개선될 수 있다. 사용자 또는 다른 프로그램이 객체를 재생하기 위하여 매체 플레이어를 불러올 때, 매체 플레이어의 사용자 인터페이스의 확장에서 워터마크를 통해 링크되거나 또는 내부에 제공된 메타데이터 또는 작용들을 디스플레이한다.

<121> 상기 메타데이터 또는 작용들은 매체 플레이어가 론칭될 때, 또는 소정의 다른 시각에(예를 들면, 백그라운드 작업으로서, 매체 플레이어가 잔류하는 컴퓨터 또는 장치에 객체가 로드될 때 사용자 요구에 응답시), 검색될 수 있다. 하나의 시나리오에서, 매체 플레이어는 객체 재생을 위해 사용자의 요구에 응답하여 객체 상의 워터마크 디코더를 불러낸다. 이 시나리오에서, 매체 플레이어는 객체의 어드레스를 워터마크 디코더에 전달하며, 이어서 이것에 임베딩된 워터마크의 디코딩을 시도한다. 워터마크를 위치시, 디코더는 이로부터 추출된 객체 식별자를 메타데이터 서버에 포워딩하여, 객체 식별자와 연관된 메타데이터 또는 작용들에 리턴시킨다. 메타데이터 검색 중, 매체 플레이어는 매체 객체의 재생을 진행한다. 링크된 메타데이터가 도달하면, 매체 플레이어의 확장이 리턴된 메타데이터 또는 작용들을 디스플레이한다.

<122> 도 5는 메타데이터 및 작용들을 나타내는 마이크로소프트사의 윈도우즈 매체 플레이어의 개선된 버전의 일례를 예시한다. 본 예에서, 플레이어의 사용자 인터페이스 윈도우는 바닥부(502)에 확장되어, 매체 객체와 연관된

메타데이터 및 링크들을 나타낸다. 사용자가 아이템들인 "Clip", "Author" 또는 "Copyright" 위에 커서를 위치시키면, 바텀 탭(bottom tab; 504)은 상기 아이템과 연관된 URL을 디스플레이한다. 상기 아이템들 중 하나를 클릭함으로써, 플레이어는 선택된 URL의 리소스에 질의(예를 들면, HTML을 다운로드하기 위해 HTTP 요구를 함)를 전송하는 인터넷 브라우저를 불러낸다.

<123> 워터마크 디코더는 매체 플레이어가 론칭하는 다른 애플리케이션에 의해 불러올 수 있다. 사용자가 파일 브라우저 또는 인터넷 브라우저로 오디오 또는 비디오 파일을 브라우징하는 경우에 대해서 고려하자. 재생을 위한 소망하는 매체 객체를 발견한 후, 사용자는 재생을 위한 객체를 선택한다. 예를 들면, 사용자는 윈도우 익스플로러의 콘텍스트 메뉴, 또는 상술한 바와 같은 HTML 문서 내에 삽입을 통해서 "재생(Play)" 옵션을 선택할 수 있다. 첫 번째 경우, 셀 확장은 연관된 메타데이터를 가질 수 있도록 워터마크 디코더를 불러내서, 매체 플레이어의 운영하는 프로그램(예를 들면, COM 객체, 스크립트 등)을 실행하고, 워터마크를 통해 링크된 부가 메타데이터를 디스플레이한다. 두 번째 경우에는, 자바 스크립트 또는 HTML 문서 내의 다른 삽입은 디코더를 불러내서, 유사한 형태로 매체 플레이어를 운영하는 프로그램을 개시한다.

<124> 윈도우 매체 플레이어를 제어하기 위한 프로그램을 실행하는 하나의 방법은 어드밴스드 스트리밍 리디렉터(Advanced Streaming Redirector; ASX) 파일의 사용을 통하는 것이다. 이 파일은 플레이어를 론칭하는 스크립트를 포함하고, 워터마크를 통해 링크된 메타데이터(예를 들면, URL 링크들 및 객체에 관한 정보)를 디스플레이한다. 윈도우 매체 플레이어를 제어하기 위한 ASX 파일들 및 상기 파일의 사용에 관한 정보는 마이크로소프트사의 개발자의 네트워크(Microsoft's Developer's Network)를 참조한다.

#### <125> 콘텐츠 인증 툴들

<126> 웹 페이지 설계 툴들을 포함하는 매체 콘텐츠 인증 툴들은 웹페이지 콘텐츠 같은 콘텐츠에 워터마크를 삽입하기 위한 워터마크 임베딩 기능(watermark embedding functionality)을 포함할 수 있다. 이때, 상기 임베딩된 데이터는 워터마크 디코더 인에이블 장치 및 소프트웨어에 신호를 보내, 임베딩된 워터마크 데이터와 연관된 기능들을 수행한다.

<127> 이러한 툴들은 또한 콘텐츠 개발자가 콘텐츠 인증 환경에서 워터마크들에 대한 매체 객체를 스크리닝하기 위한 워터마크 디코딩 특성을 사용할 수 있게 하는 워터마크 디코딩 기능을 포함할 수 있다. 편집될 매체 객체 내의 워터마크가 정보(예를 들면, 저작권 소유 정보, 라이선싱 기간들 등)를 전달하면, 이후 인증 툴(authoring tool)은 상기 정보 사용자에게 전달할 수 있다. 워터마크가 사용 제어 정보를 포함하면, 인증 툴은 상기 정보에 기초하여 매체 객체의 사용을 제어할 수 있다. 예를 들면, 매체 객체 내의 워터마크는 사용자가 라이선싱 서버로부터 인증을 확보하지 않는다면, 인증 툴이 매체 객체를 편집하는 것을 금지하는 명령을 전달할 수 있다.

#### <128> 웹 서버 통합 및 관련 애플리케이션들

<129> 워터마크 인코딩 및 디코딩 기능들은 또한 부가 기능과 마찬가지로 본 문헌에서 설명된 기능을 지원하기 위해 네트워크 서버 애플리케이션 소프트웨어 내에 통합될 수 있다. 특히, 워터마크 인코딩 및 디코딩은 웹 서버들 내에 통합될 수 있다.

<130> 워터마크 인코더들은 서버로부터 또는 서버를 통해 전달된 매체 콘텐츠 내에 워터마크를 임베딩하기 위해 웹 서버들에 통합될 수 있다. 서버에서 워터마크들을 삽입하는 하나의 이유는, 정보의 전송시에 서버로부터 또는 서버를 통해 매체 객체 내에 트랜잭션 전용 정보를 인코딩하는 것이다. 트랜잭션 특정 정보는 서버와 소정의 다른 컴퓨터 사이의 전자 트랜잭션에 관한 것이다. 예를 들면, 매체 객체를 다운로드 또는 업로딩하기 전에, 서버는 파일 내의 매체 신호에 파일의 수신/송신자에 관한 정보가 임베딩될 수 있다. 워터마크는 신호 내에 잔류하기 때문에, 워터마크 내의 송신/수신자에 관한 정보는 디지털 대 아날로그, 아날로그 대 디지털 변환, 파일 포맷 변화들 등을 통해 파일 내에 매체 신호와 함께 남는다.

<131> 서버는 송신/수신자의 선호들에 고유하게 테일러된 파일 내의 정보 또는 작용들과의 링크(관련 웹사이트와의 링크)를 삽입할 수 있다. 상기 선호들은, 예를 들면 인터넷 브라우저들 내에서 통상적으로 사용되는 대중적인 "쿠키" 기술을 통해서와 같이 사용자의 컴퓨터로부터 얻어지거나, 또는 사용자(사용자 식별자 또는 사용자의 컴퓨터의 식별자)를 사용자의 선호들(예를 들면, 뉴스, 금융 정보, 스포츠, 전자상거래 기회 등의 콘텐츠 선호들의 타입)와 연관시킨 소정의 다른 데이터베이스에 잔류할 수 있다. 이 경우, 서버는 사용자 식별자를 얻은 후, 연관된 선호들에 대한 데이터베이스에 질의한다.

<132> 서버는 또한 광고의 형태가 리턴되거나 또는 파일과 링크되는 것을 제어하는 방식으로 얻어진 선호들을 사용할 수 있다. 예를 들면, 사용자는 서버에 요구하여 소망하는 오디오, 비디오 또는 이미지 파일을 다운로드할 수

있다. 이에 응답하여, 서버는 사용자의 선호들을 얻고, 사용자의 선호들과 매치하는 웹사이트 링크들과 광고 정보와 함께 요구된 파일을 다운로드한다. 광고 정보 및 링크들은 정보의 어드레스를 포함하거나, 또는 정보를 저장 및/또는 다른 정보, 웹사이트 등과 링크하는 데이터베이스 엔트리에 대한 인덱스를 포함하는 워터마크를 임베딩함으로써 참조될 수 있다. 이후, 서버로부터 다운로드된 파일을 수신하는 사용자의 컴퓨터는 파일 내의 워터마크를 통해 서버 또는 파일과 링크된 소정의 다른 서버로부터 파일 및 다른 관련 광고 정보(예를 들면, HTML, XML 또는 소정의 다른 종래의 데이터 포맷에 제공됨)를 렌더링한다.

<133> 서버는 또한 서버와 사용자의 컴퓨터 사이의 전자 트랜잭션시 사용자에게 의해 요구되고 지불된 사용 제어권에 기초하여 매체 파일 내의 워터마크에 사용 제어 정보가 임베딩될 수 있다. 이러한 사용 제어권은 다른 애플리케이션들에 의해 디코딩될 수 있고, 파일, 카피, 레코딩, 전송 등의 렌더링을 제어하기 위해 사용될 수 있다.

<134> 네트워크 서버들은 또한 서버로부터 또는 서버를 통해 전송되는 파일 내의 매체 신호로부터 워터마크를 디코딩하기 위한 소프트웨어 같은 워터마크 디코딩 기능을 포함할 수 있다. 이는 서버가 향상된 기능성을 제공할 뿐만 아니라 상기 문서에 기술되거나 통합된 많은 워터마크 가능하게 된 기능을 수행하도록 한다. 예를 들면, 워터마크는 서버가 추출해서 작동하는 사용 제어 데이터를 포함할 수 있다. 사용 제어 데이터의 예들은 콘텐츠 레이팅 정보(성인 콘텐츠 표시자들), 카피 또는 전송 제어 정보, 렌더링 제어 정보, 압축/압축해제 제어 정보, 암호화/해독화 제어 정보, 외부 정보 또는 작용들과의 링크들 등을 포함한다.

<135> 상기 데이터를 워터마크로부터 추출한 후, 서버는 추출된 데이터에 기초하여 파일을 변경할 수 있다. 예를 들면, 서버는 파일을 전송하기 전에 워터마크 내에 지정된 방식으로 파일을 압축 또는 암호화할 수 있다. 파일을 수신하는 컴퓨터에서의 사용자는 파일 내의 매체 객체를 렌더링하기 위한 호환성 압축해제 또는 암호화 프로그램 또는 장치를 가질 필요가 있다.

<136> 추출된 워터마크 데이터에 기초하여 파일을 변경하기 위해 이와 더불어 또는 추가하여, 서버는 파일 사용을 제어하는 수신 컴퓨터에 관련 정보 또는 명령어들을 전송할 수 있다. 예를 들면, 서버가 "성인 콘텐츠"로 콘텐츠를 마크한 워터마크로부터 결정되면, 브라우저 같은 렌더링 소프트웨어에 어떻게 워터마크된 콘텐츠를 렌더링하는가를 명령하기 위해 파일과 함께 부가 정보(예를 들면, 워터마크된 콘텐츠를 포함하는 웹페이지와 함께 HTTP 헤더 정보)를 전송할 수 있다. 수신 컴퓨터상의 렌더링 소프트웨어는 어떻게 콘텐츠를 렌더링하는가를 결정할 수 있다. 예를 들면, 어린이가 파일을 수신하는 컴퓨터상에 로그인되면, 렌더링 소프트웨어는 "성인 콘텐츠"로서 마크된 파일 내의 콘텐츠의 렌더링을 선택할 수 없다. 다른 예로서, 서버는 워터마크를 디코딩할 수 있고, 이것에 지시하여 디스크립트 또는 압축해제 키를 렌더링 소프트웨어에 전송하여, 수신 컴퓨터가 콘텐츠를 디스크립트 또는 압축해제하도록 할 수 있다. 공개 키 암호화 구조들(public key encryption schemes)은 전송과 수신 컴퓨터들 사이의 키 교환을 수행하기 위해 사용될 수 있다. 다른 예로서, 서버는 워터마크를 디코딩하고, 이것에 지시하여, 링크를 포함한 워터마크된 파일과 함께 부가 데이터를 서버가 워터마크로부터 디코딩된 정보에 기초하여 웹사이트들에 전송한다.

#### <137> **콘텐츠 필터링 및 카운팅**

<138> 워터마크 디코더들은 워터마크된 매체 객체들을 필터링하고 워터마크된 매체 객체들의 경우들을 카운팅하기 위해 컴퓨터들 및 컴퓨터 네트워크들 내에 사용될 수 있다. 필터링은 워터마크 디코더의 사용을 참조하여 특정한 위치에 있는 객체들로부터의 워터마크를 디코딩하고, 그 사용을 제어하여, 워터마크 내의 데이터 제어에 응답하고, 임의로 워터마크 밖의 부가 콘텍스트 데이터에 응답하여 전송 또는 렌더링한다. 상기 매체 객체들은, 매체 객체를 전송할 책임이 있는 장치 또는 컴퓨터의 경우에서와 같이 상기 위치에 일시적으로 저장될 수 있다. 이러한 시스템의 예들은, 객체 내에서 발견된 워터마크의 적어도 일부에 기초하여 다른 장치 또는 컴퓨터로의 소정의 매체 객체의 전송 제어를 위해 워터마크 디코딩을 사용하는 컴퓨터 네트워크 내의 이메일 서버(e-mail server), 방화벽, 라우터 또는 게이트웨이 등이 있다. 매체 객체들은 또한 더 영구적인 기준에 따라 필터의 위치에 저장될 수 있다. 예를 들면, 필터는 하드 드라이브 또는 인터넷을 통해 액세스 가능한 대규모 저장 장치 상의 음악, 이미지, 영화 파일들의 원격 개인 라이브러리 또는 하드 드라이브와 같은 대규모 저장 장치로부터 사용자가 다운로드 또는 업로드하는 매체 객체들을 스크린하기 위하여 사용될 수 있다. 필터는 전송될 파일 내의 워터마크에 응답하여 대규모 저장 장치로부터 다운로드 또는 업로드하는 것을 금지하기 위해 사용되거나, 또는 대안적으로 파일의 렌더링을 제어하기 위해 사용될 수 있다.

<139> 객체 카운팅은 방화벽 또는 이메일 게이트웨이 같은 특정한 장치 또는 시스템을 통과하는 매체 객체를 필터링하거나, 또는 인터넷 같은 시스템의 네트워크를 활성으로 탐색하고 이 탐색 결과로서 발견되어 다운로드된 워터마크된 매체 객체에 대하여 스크리닝함으로써, 워터마크 객체가 나타나는 횟수만큼 로그인하는 방법을 참조한다.

워터마크 디코딩 시스템에 의해 유지된 로그들은, 소유자, 사용자 또는 트랜잭션 식별자, 트레이서 데이터(tracer data), 및 발견 장소, 사용 방법, 사용하고 있는 사람 등의 객체에 관한 정보 등의 워터마크로부터의 정보를 포함한 객체에 관한 부가 정보를 포함하도록 채택될 수 있다. 트레이서 데이터는, 예를 들면 비인증된 사용, 카피 또는 파일 전송 같은 소정의 이벤트에 응답하여 파일 내에 임베딩된 데이터를 포함한다.

<140> 워터마크 디코더는 특정한 요구에 응답하거나 또는 이벤트들에 응답하여 다른 장치 또는 컴퓨터에 전자적으로 로그를 전송하기 위해 더 증대될 수 있다. 예를 들면, 디코더는 워터마킹된 객체의 수가 임계치를 초과할 때, 및/또는 소정의 정보가 비인증된 사용 또는 그 카피의 검출에 응답하여 매체 객체에 임베딩된 특별한 식별자 또는 트레이서 데이터 같은 워터마크 내에 발견될 때, 다른 컴퓨터 상의 중앙 데이터베이스에 보고를 전송하도록 프로그래밍될 수 있다. 프로그램의 규칙들은 워터마킹된 매체 객체가 필터링되어 카운트되는 조건을 지정하고, 로그되는 정보를 지정하고, 로그된 정보가 다른 컴퓨터에 전송되는 때를 지정하기 위해, 디코더 내에 확립될 수 있다.

<141> 필터링 및 카운팅 기능에 기초한 워터마크는 다양한 소프트웨어 애플리케이션들 및 장치들에서 구현될 수 있다. 일부 예들은 매체 객체에 나타나는 네트워크 방화벽(network firewall), 다른 클라이언트, 서버 또는 피어-투-피어 소프트웨어 애플리케이션들(예를 들면, 오퍼레이팅 시스템들, 매체 플레이어들, 이메일 관독기들 및 서버들, 인터넷 브라우저들, 파일 공유 소프트웨어, 파일 관리 소프트웨어 등)을 포함한다. 필터링, 스크리닝 및 카운팅에 기초한 워터마크의 특정한 사용예는, 컴퓨터들간에 전송된 이메일들에 첨부되어 전송되는 워터마킹된 콘텐츠를 모니터링하는 것이 있다.

#### <142> 워터마크 기반 스파이더들(Watermark Based Spiders)

<143> 본 특허출원의 양수인에 의한 우선 특허문서는, 인터넷 등의 컴퓨터 네트워크 상의 매체 객체 파일의 자동화된 서칭 및 워터마크 스크리닝 방법 및 시스템을 개시한다. 본 명세서에 편입되어 참조되는 미국특허 제 5,862,260 호를 참조한다. 링크들 또는 인터넷 콘텐츠 컴파일링 및 자동화된 서칭을 수행하기 위해 사용되는 소프트웨어는 종종 웹 크롤러(web crawler) 또는 스파이더로 불리운다.

<144> 미국특허 제 5,862,260 호에 기재되고 디지맥 코퍼레이션에 의해 마케팅된 정보 검색에 기초한 워터마크의 확장으로서, 워터마크 디코더는 인터넷을 포함한 네트워크 들상의 워터마킹된 매체 객체들의 워터마크 스크리닝 및 카운팅을 수행하도록 분배식으로 채용될 수 있다. 특히, 워터마크 디코더들은 인터넷 같은 컴퓨터 네트워크상에 다양한 위치들에서 배치될 수 있으며, 이것은 각 탐색 엔진에 의해 수집된 매체 객체를 스크리닝하는 인터넷 탐색 엔진들, 방화벽에서 나타나는 매체 객체를 스크리닝하는 네트워크 방화벽들, 통상 스파이더들이 도달하지 않는 데이터베이스들 및 로컬 에어리어 네트워크들, 콘텐츠 필터들 내에 포함된다. 이렇게 분배된 디코더들은 각각 본 문헌에서 설명되고, 참조되는 워터마크 정보를 로그하는 스파이더 스레드(spider thread)로서 작용한다. 정보 타입들의 예들로는 워터마킹된 매체 객체들, 매체 객체 카운트들, 매체 객체들의 위치(이들이 발견된 곳)의 어드레스들 및 다른 콘텍스트 정보(예를 들면, 객체가 사용되는 방법, 이것을 사용하는 사람) 내의 워터마크들로부터 디코딩된 식별자들을 포함한다. 이어서, 스파이더 스레드는 그 로그들 또는 보고들을 이들을 컴파일하는 중앙 스파이더 프로그램에 전송하고, 그 정보를 탐색가능한 데이터베이스의 필드들 내에 통합시킨다.

#### <145> 임베딩된 데이터에 기초한 이벤트 스케줄링

<146> 워터마크 디코딩은 소정 타입의 워터마크 메시지의 디코딩에 응답하여 발생된 프로그램적 이벤트를 스케줄링하기 위해 이벤트 스케줄러와 관련하여 사용될 수 있다. 본 문헌 전반에 걸쳐, 워터마크 메시지로부터의 정보, 명령어들 또는 링크들의 디코딩에 응답하여 작용들을 트리거링하는 많은 예들이 있다. 대부분의 경우들에서, 상기 작용들은 워터마크에 응답하여 소프트웨어에 의해 이루어진 프로그램적 작용들이지만, 다른 경우에, 상기 작용들은 오디오 및 비디오 플레이어들, 레코더들 등의 하드웨어 실행들에 있어 매체 신호들의 사용 제어의 경우와 같이 하드웨어 회로(hardware circuitry)로 이루어진 장치 작용들이다.

<147> 워터마크 메시지를 디코딩한 직후 작용을 취하는 것보다, 이벤트 스케줄러(event scheduler)는 클럭 또는 타이머에 따라 지정된 시간에, 또는 이후의 입력, 작용 등에 응답하여 이후의 이벤트에서 발생하는 프로그램적 또는 장치 작용을 스케줄링하기 위해 사용될 수 있다.

<148> 이러한 일례로는, 이후에 아마도 주기적인 이벤트로 활성화될 웹사이트와의 링크를 스케줄링하는 것이 있다. 예를 들면, 브라우저, 오퍼레이팅 시스템, 매체 플레이어 또는 다른 소프트웨어 애플리케이션에서 실행되는 워터마크 디코더는 객체를 하나 이상의 웹사이트에 링크시키는 매체 객체로부터 워터마크를 디코딩한다. 이 워터마크 디코딩에 응답하여, 디코더는 이후의 시각에 발생할 프로그램적 작용들을 스케줄링한다. 이러한 작용들의



소정 예들은, 주기적인 간격들로 또는 브라우저, 매체 플레이어 또는 다른 애플리케이션의 론칭 같은 프로그램 적 작용에 응답하여 지정된 웹사이트와의 링크와 함께 윈도우를 디스플레이하는 것이 있다. 이러한 방식은 매체 객체(음악 또는 비디오 트랙) 같은 제품 또는 매체 객체 내에 도식된 소정의 제품을 사용자가 구입하도록 촉구하기 위해 사용될 수 있다. 이러한 방식을 사용하여, 많은 작용들이 워터마크의 단일 디코딩에 응답하여 발생하도록 스케줄링될 수 있다.

<149> **오버레이팅 시스템들 및 다른 애플리케이션들에서의 워터마크 인코더 통합**

<150> 일부 애플리케이션들에서는, 워터마크를 인코딩하거나, 또는 상술한 기능(예를 들면, 트랙 사용들, 사용권 리프 레시, 부가 정보 및 작용들에 링크를 부가 등의 기능) 중 일부를 수행하기 위하여 하나 이상의 부가적 워터마크들을 오버레이(overlay)하는데 유용할 것이다. 워터마크 인코딩 기능은 오버레이팅 시스템, 인터넷 브라우저들, 또는 다른 애플리케이션들에 부가될 수 있다. 예를 들면, 드래그 및 드롭 절차를 통해, 사용자는 상기 요약한 다양한 기능들을 가능하게 하는 수단으로서 매체 객체 내에 워터마크를 임베딩될 수 있다.

<151> 다른 예로서, 워터마크 인코더는 디코더에 대해서 상기 요약한 것과 같은 통합 기술을 사용하여 파일 브라우저, 인터넷 브라우저, 매체 플레이어 또는 다른 애플리케이션 내에 통합될 수 있다. 도 1은, 예를 들면, 셀 확장을 통해 윈도우 익스플로러 파일 브라우저 내에 통합된 워터마크 인코더 기능을 나타낸다. 특히, 워터마크 인코더는 셀 확장 핸들러와 같이 실행된다. 이 핸들러는 윈도우즈 오버레이팅 시스템의 등록부 내에 콘텍스트 메뉴 확장으로서 등록된다. 대안으로, 속성들 페이지 확장 핸들러로서 실행될 수 있다.

<152> 도 1에서의 워터마크 인코더에 액세스하기 위하여, 예를 들면, 사용자는 매체 객체상의 우측 클릭을 하여, "임베딩된 정보"로 불리는 콘텍스트 메뉴 옵션을 선택한다. 이에 응답하여, 핸들러는 도 6에 나타난 윈도우(600)를 디스플레이한다. 이 윈도우는 사용자가 워터마크를 통해 이미지에 인코딩된 다양한 ID(예를 들면, 생성자 ID, 이미지 ID)를 입력하게 한다. 사용자는 또한 이미지 객체의 속성들을 설정 또는 선택할 수 있다. 최종적으로, 사용자는 스크롤 바 제어(scroll bar control)를 통해 워터마크의 내구성(durability)을 조정함으로써 임베딩 프로세스를 제어할 수 있다. 사용자는 "원래의(Original)"와 "워터마킹된(Watermarked)" 탭들을 선택함으로써 객체의 원형과 워터마킹된 버전을 비교할 수 있다. 만족되면, 사용자는 워터마킹된 이미지를 저장하고, (예를 들면, 클로즈를 선택함으로써) 윈도우를 빠져나올 수 있다. 메타데이터 및 작용들은 객체 ID와 연관된 메타데이터 서버에 이미지 객체를 포워딩함으로써 이미지 객체와 연관될 수 있다.

<153> 도 6의 예는 정지 이미지 객체(still image object)를 도시하였지만, 유사한 방식이 비디오, 오디오 객체 등의 다른 매체 객체 내에 워터마크가 임베딩되기 위해 사용될 수 있다. 마크된 것과 마크되지 않은 오디오 또는 비디오 객체를 비교하기 위하여, 셀 확장은 필요하다면 마크된 객체와 비마크된 객체들을 재생하기 위해 매체 플레이어를 론칭하도록 설계될 수 있다.

<154> **게이트웨이 및 제어 메커니즘으로서의 디지털 워터마크들**

<155> 인터넷은 인터넷 또는 다른 타입의 컴퓨터 네트워크와의 접속들 및 기밀 정보를 갖는 사람들과 기업들에 보안에 대한 필요성을 제시한다. 전통적으로, 기밀 정보를 포함한 문서들은 기호 또는 "CONFIDENTIAL", "PROPRIETARY" 같은 용어의 다른 시각적 표시로 마크된다. 상기 마크가 존재하게 되면 특별한 주의들 하에서 회사의 제어 밖으로 전송되어야 하는 문서를 취급하는 사람은 모두 주의를 하여야 한다. 누군가가 상기 문서들을 부주의로 비인증된 수신기에 수동 전송하는 것은 상대적으로 어렵고 비밀상적인 일이다. 그러나, 인터넷을 통해 이메일과 파일 전송들과 같은 전자 통신 서비스들을 사용은 고의나 부주의로 전송을 시도할 수 있다.

<156> 인터넷, 전자 메일, 및 다른 네트워크 파일 전송 프로토콜(FTP, HTTP 등)은 간단하고 고속으로 통신 프로세스를 한다. 이러한 프로토콜들은 또한 누군가가 부주의로 또는 우연히 기밀 문서를 비인증된 수신기에 훨씬 쉽게 전송할 수 있다.

<157> 본 섹션은 인터넷과 같은 컴퓨터 네트워크들을 통해 전송된 문서들의 수신 및/또는 전송을 제어하도록 디지털 워터마크들을 사용하기 위한 시스템 및 관련 방법들을 설명한다. 이러한 시스템 및 방법들은 비인증된 수신기들에 부주의하게 정보를 배포하는 것을 방지하기 위해 사용될 수 있다. 또한, 어떠한 보안 시스템도 완전한 신뢰를 줄 수 없어서, 상기 시스템 및 방법들은 의도적이지만 비인증된 비인증된 수신기들에 대한 정보의 배포로부터 보호하는데 도움을 준다.

<158> 대부분의 전자적으로 전송된 메시지들은 텍스트를 포함한다. 그러나, 전자 메일 시스템들은 일반적으로 이미지(즉, 사진) 또는 사운드 바이트가 메시지의 일부에 임베딩되어 형성되도록 한다. 예를 들면, 메시지는 용어 "기밀"을 갖는 "스탬프"를 포함할 수 있거나, 또는 메시지는 용어 "기밀"을 갖는 사운드 클립을 포함할 수 있다.



전자 메시지의 일부를 형성하는 이미지 또는 사운드 클립은 디지털 워터마크 판독 프로그램에 의해 검출되어 판독될 수 있는 디지털 워터마크를 전달할 수 있다. 또한, 텍스트는, 예를 들면, 바이너리 메시지를 PN 시퀀스로 확산 스펙트럼 변조함으로써 생성된 의사랜덤 패턴(pseudorandom pattern)과 같은 테스트의 의미를 변경하지 않는 숨김 패턴에 따라 캐릭터들이나 라인들을 부가 또는 제거함으로써, 스테거노그래픽 정보를 전달할 수 있다. 이러한 패턴은 소망하는 패턴으로 라인들과 단락들의 말단들에 공간을 부가 또는 제거하기 위해 사용될 수 있다. 대안으로, 테스트 문서의 이미지는 워터마크 패턴에 따라 하프톤 도트들을 온 또는 오프로 토글링(toggling)함으로써 워터마크를 전달할 수 있다.

<159> 디지털 워터마크 또는 스테거노그래픽 메시지 내의 "페이로드" 또는 디지털 데이터는 일반적으로 복수의 다른 필드들을 갖는다. 하나 이상의 상기 필드들은 메시지를 포함한 문서 또는 이미지가 기밀이나 다른 분류로 되어, 특수한 방식으로 배포되어야 하는 것으로 표시하는 플래그로 지정될 수 있다.

<160> 일반적으로, 이메일은 이메일 서버를 통해 전송 네트워크를 입력한다. 워터마크를 검출하고 판독할 수 있는 프로그램들은 공지되어 있고, 상업적으로 이용될 수 있다. 이러한 시스템의 일례에서, 이메일 서버는 워터마크 검출을 통해 각 이메일 메시지를 통과시키고, 네트워크를 통해 메시지를 전송하기 전에 프로그램을 판독한다. 워터마크 프로그램이 워터마크를 검출하면, 메시지가 어떻게 취급되어야 하는가를 결정하기 위해 소정의 플래그 비트에 질문을 한다. 워터마크 판독 프로그램이 특정 플래그가 설정되었음을 발견하면, 전송자와 네트워크 관리자 모두에게 주의하라는 작용을 취할 수 있다. 워터마크 프로그램이 워터마크가 없다는 것을 발견하거나, 특정한 플래그가 설정되지 않았음을 발견하면, 메시지는 종래의 방법으로 네트워크를 통해 전송된다.

<161> 이 시스템은 전자 메시지들의 배포 및 수신을 제어하는 제어 메커니즘으로서 작용할 수 있다.

<162> 메시지와 문서는 또한 웹 서버들과 FTP 서버들과 같은 서버들로부터 수신된 인터넷 및 다른 전자 네트워크들을 입력한다. 마찬가지로, 워터마크 검출 프로그램은 웹 및 FTP 서버들과 같은 서버들 상의 문서들을 통합하고, 특정한 상태에서 특정한 플래그를 갖는 워터마크가 검출되는 경우 알람을 울리는 것과 같은 작용을 취할 수 있다. 이러한 시스템은 비의도적으로 또는 부주의로 웹사이트에 부가된 웹 서버상의 파일들을 스크리닝하기 위해 사용될 수 있다. 파일 디렉토리들의 프로그램적 스크린에 의해 검출된 비인증된 파일들은 삭제되거나, 또는 FTP 또는 HTTP 요구들을 통해 파일들에 대한 요청들에 응답하여 전송되는 것이 방지된다.

<163> 상기 시스템의 제 1 실시예는 인터넷을 통해 전송된 이메일 메시지들을 모니터링하도록 설계된다. 상기 제 1 실시예는 기밀 이메일 메시지들을 비인증된 사용자들에게 우연히 배포하는 것을 방지하기 위해 사용된다. 제 1 실시예는 기밀 문서들을 누군가에 전송하는 것을 방지한다. 다른 실시예들은 비인증된 사용자에게 또는 비인증된 목적들로 기밀 문서의 전송을 제어한다. 예를 들면, 이메일 메시지에 어드레스를 부가하기 용이하다. 누군가가 어드레스 중에서 기밀 정보를 수신하도록 인증되지 않은 것이 있음을 알릴 필요없이 대그룹의 사람들에게 기밀 정보를 포함한 이메일 메시지를 어드레스할 수 있다. 이 시스템은 전송자가 상기 어드레스의 리스트 내에 상기한 사람들의 어드레스를 포함하고 있다라도 비인증된 사람에게 상기한 이메일이 전송되는 것을 방지할 수 있다.

<164> 종래의 기밀 문서(10)는 도 8에 나타내었다. 이 문서(10)는 이메일 메시지이거나, 또는 이메일 메시지에 첨부된 문서일 수 있다. 문서(10)는 기밀 스탬프(11) 및 텍스트의 라인들을 포함한다. 기밀 스탬프(11)는 다양한 라인들을 갖는 백그라운드 상에 중첩된 용어 "기밀"을 갖는 이미지이다. 즉, 이미지(11) 내의 백그라운드는 1998년 5월 6일 출원된 미국특허출원 제 09/074,034 호(PCT 출원 PCT/US99/08252 호에 대응함), 및 1998년 7월 31일 출원된 미국출원 제 09/127,503 호(PCT 출원 PCT/US99/14532호에 대응함)에 따라 워터마크를 갖고 있기 위해 변형된 폭으로 된 라인을 갖는다. 상기 참조된 특허출원의 개시 내용은 본 명세서에 편입되어 참조된다. 또한, 이미지(11)의 백그라운드 또는 문서(10)의 백그라운드부들은 바이너리 메시지를 PN 시퀀스로 확산 스펙트럼 변조하고, 이 변조된 시퀀스를 픽셀값당 멀티레벨의 이미지로 변환함으로써 형성된 의사랜덤 이미지 패턴과 같은 디지털 워터마크 신호를 전달하는 위브(weave) 또는 틴트(tint) 패턴을 포함할 수 있다. 또 다른 실시예에서는, 메시지에 임베딩된 이미지(11)를 갖는 대신에, 메시지가 용어 기밀을 갖는 오디오 클립을 포함할 수 있다. 이 오디오 클립은 오디오 워터마킹 기술들을 사용하여 워터마킹될 수 있다. 그러나, 본 명세서에 설명된 제 1 실시예에서, 이미지(11)는 워터마크 검출 및 판독 프로그램에 의해 판독될 수 있는 디지털 워터마크, 및 인간 판독가능 용어 "기밀" 양자를 포함한다.

<165> 물리적 워터마크 페이로드 내의 데이터 필드들 및 플래그들은 도 9에 나타내었다. 도시된 필드들 및 플래그들은 단지 대표예일 뿐이며, 이들이 많은 다른 형태들을 취할 수 있음을 이해하여야 한다. 시스템은 특정한 문서가 기밀임을 표시하기 위해 플래그 필드들 중 하나를 사용한다. 다른 필드들은 종래의 방법으로 사용될 수 있

다.

<166> 도 10은 콘텐츠를 모니터링 및 필터링하기 위한 워터마크 검출 및 판독 경로를 갖는 이메일 시스템을 나타낸다. 상대적으로 많은 수의 개별 사용자 단말(1301a 내지 1301e)가 이메일 서버(1302)와 접속된다. 이러한 접속들은 이더넷 LAN, 다이얼 업 모델들, 또는 다른 종래의 유선 또는 무선 컴퓨터 네트워크 접속에 의해 이루어질 수 있다. 이메일 서버(1302)는 인터넷(1304)과의 인터페이스(1303)를 갖고, 이것은 개별 사용자의 단말로부터 메시지를 수신하여 인터넷에 전송한다. 이메일 서버(1302) 자체는 공지된 것이지만, 서버에 의해 프로세스된 메시지의 워터마크 검출 및 판독을 가능하게 하기 위한 프로그램적 인터페이스를 갖는다. 본 발명에서는, 이메일 서버(1302)가 개별 사용자 단말(1301a 내지 1301e) 중 하나로부터 인터넷으로 메시지를 전송하기 전에, 이메일 서버가 워터마크 검출 및 판독 프로그램(1305)을 통해 메시지를 전달한다. 이메일 메시지 자체와 소정의 첨부된 문서들은 모두 상기 프로그램을 통해 통과된다. 워터마크 검출 및 판독 프로그램(1305)은 메시지가 디지털 워터마크를 포함하는가의 여부를 결정한다. 워터마크가 검출되었다면, 기밀 플래그 비트는 질문을 받는다. 플래그 비트가 "기밀"로 설정되면, 본 실시예에서는 메시지를 전송자에게 리턴시킨다. 따라서, 제 1 실시예는 어떠한 기밀 정보도 이메일 메시지의 일부로서 전송되는 것이 방지된다.

<167> 제 2 실시예는 다른 폭 넓은 어레이에 제공된다. 도 11에 나타난 바와 같이, 제 2 실시예는 데이터베이스(1401)를 포함한다. 이 데이터베이스(1401)는 잠재 메시지 전송자들의 다른 그룹들의 리스트를 포함하고, 이 리스트는 잠재 메시지 수령자의 다른 그룹, 및 메시지 내의 다양한 플래그들의 설정에 의해 표시된 가능한 카테고리들의 세트를 나타낸다. 예를 들면, 전송자들은 3개로 지정된 전송 그룹들 S1, S2, 및 S3으로 나누어진다. 잠재 수령자는 R1, R2 및 R3로 지정된 3개의 그룹들로 나누어진다. 데이터베이스(1401) 및 관련 논리(1402)는 다음의 표로 표시된 바와 같은 논리 규칙들을 실행할 수 있다.

| 전송자 그룹 | 수령자 그룹 | 플래그 상태 | 작용                                 |
|--------|--------|--------|------------------------------------|
| S1     | R1     | 011    | 메시지 전송                             |
| S1     | R2     | 110    | 메시지를 전송하지 않음을 관리자에게 통지함            |
| S1     | R2     | 001    | 메시지 전송, S1이 메시지를 R2에 전송한다는 사실을 로그함 |
| S1     | R2     | 101    | 메시지를 전송자에게 리턴시킴                    |
| S2     | R1     | 011    | 메시지 전송                             |
| S2     | R3     | 110    | 메시지를 전송하지 않고 시스템 관리자에게 통지함         |

<169> 시스템은 FIRST-IN, FIRST OUT 형태로 서버를 통과하는 메시지를 버퍼링하는 버퍼(1403)를 포함한다. 이 버퍼는 메시지들 자체를 저장하거나, 또는 서버의 파일 디렉토리 구조 내의 그들의 위치들에 대한 포인터들을 저장할 수 있다. 워터마크 판독 프로그램(1404)은 메시지 및/또는 첨부물들을 판독하고, 디지털 워터마크 또는 임베딩된 스테가노그래픽 메시지의 검출을 시도하여, 검출된 경우에는, 영구 메시지 페이로드 정보를 데이터베이스 질의 프로그램(1405)에 공급한다. 전송자/수령인 필터 프로그램(1402)은 전송자 및 수령인 어드레스들을 필터링하는 제어 로직(control logic)을 실행하고, 이들을 이전에 할당된 그룹핑에 맵핑한다. 이 프로그램은 특정 메시지용 정보를 질의 프로그램에 제공하고, 이에 응답하여, 메시지 페이로드 플래그들 및 전송자/수령인 코드들을 사용하여 상기 메시지와 연관된 연관 제어 작용을 록업한다. 이 시스템은 버퍼(1403) 내의 메시지와 함께 특정한 작용을 취하도록 서버에게 프로그램적으로 지시하는 메시지 분배 제어 메커니즘(1406)에 제어 작용을 전송한다.

<170> 요컨대, 시스템은 메시지 송신자, 메시지 수령인, 및 작용이 취해져야 하는가를 결정하기 위한 플래그의 상태를 고려한다. 시스템은 상술한 것과 더불어 많은 다른 것들을 포함하거나, 또는 시스템은 몇 개의 다른 것들만을 포함할 수 있다. 예를 들면, 시스템은 "기밀"로 설정된 기밀 플래그를 갖는 메시지를 수신하기 위해 인증된 어드레스의 리스트만을 포함할 수 있다. 이러한 시스템은 기밀 문서들이 선택된 어드레스들에만 전송되도록 한다. 선택적으로 또는 더불어서, 시스템은 기밀 문서들을 전송하기 위해 인증된 개별 리스트를 포함할 수 있다. 시스템은 상기 리스트에 대한 전송자를 검사하기만 할 수 있거나, 대안적으로는 상기 메시지들이 나타날 때 패스워드가 입력되는 것을 요구할 수 있다.

<171> 상기 표에서는 대표적인 규칙들만을 나타내었음을 유념한다. 실제적인 시스템에서는, 훨씬 많은 그룹들이 있을 수 있고, 일부 그룹들이 단일 개별 리스트를 포함할 수 있다. 또한, 상기 표는 훨씬 많은 라인들을 가질 수 있다. 상기 표는 3개의 플래그 비트만을 나타내었다. 시스템은 특정한 시스템의 필요에 따라 더 많거나 적은 플

래그 비트를 가질 수 있다.

- <172> 대안적인 실시예들에서, 기밀 스탬프(confidentiality stamp)는 상술한 바와 같이 라인 폭 또는 하프톤 도트 변조를 사용하는 것 이외의 수단에 의해 이미지 내의 워터마크를 포함할 수 있다. 스탬프의 백그라운드는 디지털 워터마크를 갖고 있는 이미지를 포함할 수 있다.
- <173> 대안적인 실시예에서, 디지털 워터마크에 대한 검사보다도, 시스템은 "기밀" 같은 텍스트 스트링(text string)에 대해 검사하고, 상기 텍스트 스트링의 위치화에 응답하여 작용을 취할 수 있다. 또한, 시스템은 라인들 또는 단락들의 말단에서의 공간들의 숨겨진 스테거노그래픽 패턴에 대해 검사할 수 있다.
- <174> 이상 설명한 실시예들은 이메일 시스템들에 적용하였지만, 유사한 조치가 FTP 서버들 또는 웹 서버들과 함께 취해질 수 있다.
- <175> **디지털 워터마크들을 사용하는 콘텐츠 필터링 및 인텍싱 시스템**
- <176> 도 12는 콘텐츠 필터링 및 인텍싱 시스템을 예시한 도면이다. 본 시스템에서, 디지털 워터마크 임베더(digital watermark embedder)는 디지털 워터마크들을 이미지, 비디오 또는 오디오 같은 콘텐츠에 임베딩하여, 디지털 워터마크가 최종-사용자들에게 렌더링(예를 들면, 프린트, 디스플레이, 재생 등)될 때 콘텐츠 내에서 지각 불가능하거나 또는 실질적으로 지각 불가능하도록 한다. 이러한 임베딩의 형태는 임베딩된 워터마크 신호를 인간 지각 모델에 기초한 호스트 매체 신호(host media signal)에 지각적으로 적용하는 것을 포함한다. 워터마크 콘텐츠 마커(1502, 1504)로 불리우는 임베더는 웹 서버들, 스트리밍 매체 서버들, FTP 서버들 등과 같은 콘텐츠 서버들에 통합되어, 상기 서버들 상에 콘텐츠를 마크를 한다. 임베더(embedder)는 바람직하게는 콘텐츠 전반에 걸쳐 반복적으로 워터마크 페이로드들을 임베딩하여, 다른 시간 또는 공간적 부분들이 임베딩된 콘텐츠와 관련하여 동일하거나 또는 다른 페이로드를 갖도록 한다. 예를 들면, 콘텐츠 타입 플래그들은 광고에서 프로그래밍, 및 한 등급에서 다른 등급(콘텐츠 타입에 따른 G, PG, R, X)으로의 콘텐츠 타입 변화들에 따라 변화할 수 있다.
- <177> 이 후, 상기 콘텐츠는 웹 브라우저(1512), 이메일 판독기(1514), 매체 플레이어 등의 다른 시스템에 통신 네트워크(1510)를 통해 전송된다. 통신 경로를 따라, 콘텐츠는 방화벽(1516) 및 LAN(1518)을 통과할 수 있다. 워터마크 콘텐츠 필터들(1520, 1522, 1524)로 나타낸 디지털 워터마크 판독기 프로그램들은 디지털 워터마크용 콘텐츠를 스캔하여, 워터마크들이 발견되면, 상기 워터마크들의 메시지 페이로드를 디코딩한다. 메시지 페이로드는 콘텐츠 소유자(소유자 ID), 분배자(분배자 ID), 및/또는 트랜잭션(트랜잭션 ID, 수신 기기 ID, IP 어드레스, 전송자/수령자 어드레스 또는 사용자 ID)에 관한 정보를 포함한다. 더불어, 이 페이로드는 성인 콘텐츠 등급들, 제한된 액세스 등급들 등과 같은 콘텐츠 타입을 표시하는 콘텐츠 플래그를 포함한다.
- <178> 워터마크 콘텐츠는 그 전송을 제어하거나, 또는 콘텐츠 플래그에 응답하여 렌더링함으로써 필터 콘텐츠를 필터링한다. 또한, 이들은 임베딩된 ID 및 콘텐츠 타입 정보를 데이터베이스 내의 각 필터링 이벤트에 관한 정보에 로그하는 탐색가능한 데이터베이스(1530)에 전송한다. 시스템은 검출 이벤트의 네트워크 어드레스 전송자 및 수령인 어드레스, 사용자명 등의 콘텐츠가 검출된 기기 또는 파일 헤더 같은 밴드 데이터 외부로부터 유도된 부가 이벤트 정보에 로그한다. 콘텐츠 필터들은 콘텐츠 렌더링 및 전송 제어를 위한 규칙들의 세트를 실행한다. 예를 들면, 방화벽들용 콘텐츠 필터는 워터마크 페이로드시 소정의 플래그들 또는 플래그들 세트의 조합을 갖는 콘텐츠 파일의 전송을 방지한다. 방화벽은, 예를 들면, 회사 네트워크 상에 성인 콘텐츠가 전송되는 것을 방지하기 위해 사용될 수 있다.
- <179> 웹 브라우저용 콘텐츠 필터들, 이메일 판독기들 및 매체 플레이어들은 필터가 통합된 소프트웨어 애플리케이션 내에 확립된 규칙들 및 콘텐츠 플래그들에 기초하여 콘텐츠의 렌더링을 방지한다. 예를 들면, 사용자 규정된 규칙들은 어린이에 의해 사용되는 컴퓨터 상에 성인 콘텐츠가 렌더링되는 것을 차단하기 위해 사용될 수 있다. 이러한 규칙들은 사용자가 애플리케이션에 로그인할 때 활성화되어, 특정한 사용자가 상기 애플리케이션을 사용하고 있는 필터를 나타내는 사용자 ID, 및 이 사용자 ID가 활성화될 때 적용되는 소정의 규칙들을 공급한다.
- <180> 마찬가지로의 방식이 콘텐츠에 대해 더 높은 가입료를 지불한 사용자용의 콘텐츠로부터 광고를 필터링하기 위해 사용될 수 있다. 이 경우, 광고 플래그를 포함한 콘텐츠는 워터마크를 통해 검출되고, 렌더링 전에 삭제된다. 마찬가지로, 소정 타입들의 콘텐츠가 사용자의 기기 상에 렌더링되는 것이 차단될 수 있는데, 이 기기의 사용자가 가입자는 내부에 삽입된 특정한 콘텐츠 플래그 타입을 갖는 콘텐츠의 재생을 인증하지 않는다. 콘텐츠 필터는 콘텐츠 내의 플래그 및 사용자의 가입권에 기초하여 콘텐츠의 렌더링을 가능하게 또는 불가능하게 하기 위해 사용될 수 있다. 이러한 방식은 특히 사용자가 많은 다른 피어 컴퓨터들로부터 콘텐츠를 수신할 수 있는 분배식

피어 투 피어 모델들에 적합하다.

- <181> 콘텐츠 필터링 시스템은 또한 탐색 가능한 데이터베이스가 콘텐츠의 카피들을 발견할 수 있는 컴퓨터 어드레스들(URL들 또는 IP 어드레스들)을 표시하는 콘텐츠의 탐색가능한 인덱스를 유지하도록 한다. 예컨대, 상기 시스템은 사용자가 콘텐츠 타입, 콘텐츠 ID, 분배자 또는 콘텐츠 ID와 링크된 다른 속성들을 탐색하도록 하고, 콘텐츠 아이템들 및 그 대응하는 어드레스들을 발견할 수 있도록 인터넷을 통해 액세스 가능한 탐색 엔진을 생성하기 위하여 사용될 수 있다.
- <182> 도 13은 분배식 워터마크 검출기 시스템을 예시하는 도면이다. 본 시스템에서, 디지털 워터마크 검출기(1602, 1604, 1606, 1608)는 워터마크용 콘텐츠를 스크리닝하고, 이것이 발견되었을 때, 이벤트(콘텐츠의 네트워크 어드레스, 사용자 정보, 시간 및 일자 등)에 관한 정보 및 워터마크 페이로드로부터의 정보를 인터넷(1612)에 첨부된 서버 상에서 실행하는 중앙 스파이더 프로그램(1610)에 보고하는 스파이더 스레드 프로그램으로서 구현된다. 스레드 프로그램은 회사의 LAN 상의 콘텐츠 데이터베이스 같은 내부 시스템들(1602), LAN 상의 방화벽들(1604), 브라우저들이나 오퍼레이팅 시스템들과 같은 소프트웨어 애플리케이션들 또는 LAN들 내의 콘텐츠 필터들(1606), 및 다량의 링크된 웹페이지들에 폐지하고, 그 콘텐츠들에 기초하여 페이지들을 인덱스하는 웹 크롤러 같은 탐색 엔진(1608) 내에서 구현된다.
- <183> 스파이더 프로그램(1610)은 데이터베이스(1612) 내에 워터마크 페이로드 및 이벤트 정보를 저장한다. 스파이더 프로그램은 또한 콘텐츠 타이틀명, 소유자명, 아티스트, 가사, 관련 웹사이트들의 URL들 등의 콘텐츠 속성 정보와 워터마크 페이로드로부터의 콘텐츠 ID를 연관시키는 부가 데이터베이스에 워터마크 검출 이벤트로부터 컴파일된 데이터베이스 정보를 교차 참조한다. 이로써 사용자는 스파이더 프로그램에 액세스하여, 타이틀 또는 소정의 다른 속성에 기초하여 콘텐츠를 탐색한 후, 콘텐츠가 발견된 네트워크 어드레스에 교차 참조한다.
- <184> 상기 시스템은 광대하고 복잡한 네트워크들을 거쳐 장치상의 콘텐츠의 깊은 링크를 가능하게 한다. 이 시스템은 인터넷과 접속된 컴퓨터들, 음악 파일 공유 네트워크 상에 링크된 음악 기기들, 셋톱 박스 및 비디오 파일 공유 네트워크상에 링크된 개인 비디오 레코더들 같은 장치들에 적용될 수 있다. 일부 시스템들에서, 분배식 스파이더들이 위치한 노드들이 콘텐츠 서버들로서 작용한다. 사용자가 탐색가능한 데이터베이스(1612)의 자동화된 탐색을 통해 콘텐츠의 일부를 발견하면, 사용자는 요구를 콘텐츠가 위치한 콘텐츠 서버에 전송하고, 콘텐츠 서버로부터의 콘텐츠 파일을 사용자의 컴퓨터 또는 음악 기기, 셋톱 박스, 무선 전화 등과 같은 다른 장치에 전송을 요구한다.
- <185> 상술된 분배식 콘텐츠 필터링 및 스파이더링 시스템에는 많은 잠재적인 개선들 또는 변형들이 있게 된다. 워터마크에 기초하여 콘텐츠를 필터링할 때, 워터마크 페이로드는 데이터베이스에 저장된 콘텐츠 타입 기술자들을 포함한 콘텐츠 타입 플래그 또는 인덱스를 포함할 수 있다. 후자의 경우, 시스템은 기술자 데이터베이스에 질의하여 콘텐츠의 속성을 정의하는 기술자를 결정한다. 콘텐츠 플래그들이나 또는 기술자들이 콘텐츠 타입에 의해 네트워크상에 분배된 콘텐츠를 인덱스하기 위해 탐색 엔진에 의해 사용될 수 있다.
- <186> 도 13의 시스템에서 스파이더의 데이터베이스를 확장하기 위하여, 시스템은 또한 링크된 웹 사이트들의 자동화된 크롤(crawl)을 수행하고, 워터마크된 콘텐츠에 대한 사이트를 스크리닝한 후, 콘텐츠의 탐색가능한 인덱스를 그 타입에 의해 생성하기 위해 페이로드에 의해 인덱스된 콘텐츠 기술자들 또는 페이로드 내의 콘텐츠 플래그들을 사용하는 프로그램을 포함한다. 이 후, 사용자들은 상기 인덱스를 탐색하여, 콘텐츠 타입 기준들과 매치하는 콘텐츠를 발견하고, 이 콘텐츠의 어드레스와 함께 상기 기준들과 매치하는 콘텐츠의 리스트를 얻는다.
- <187> 필터가 렌더링을 제어하는 방식을 변화될 수 있다. 예를 들면, 워터마크 필터는 전체적으로 재생을 방지하고, 재생을 스크램블링하거나, 또는 콘텐츠 타입 플래그 또는 기술자에 기초하여 거부 가능한 부분만을 스크램블링할 수 있다. 워터마크는 콘텐츠의 프레임 전체에 걸쳐 반복되기 때문에, 필터는 오디오 또는 비디오의 프레임을 스크램블 또는 차단하거나, 또는 정지 이미지 부분을 차단하는 미세 그레인 제어(fine grained control)를 제공할 수 있다. 또한, 필터는, 예를 들면, 사용자에 의해 공급된 사용자 선호에 기초하여 세대, 위치 등의 사용자 데모그래픽에 기초하여 콘텐츠의 프레임들 내에서 스와핑(swapping)함으로써 렌더링되는 콘텐츠의 타입을 선택적으로 제어할 수 있다. 콘텐츠의 스와핑을 위해, 콘텐츠 전달 메커니즘은 필터의 제어 신호들에 응답하여 대안적인 프레임들을 스트리밍할 수 있다.
- <188> 워터마크 필터는 관련 정보와의 링크를 위해 워터마크 페이로드를 사용할 수 있다. 우선, 워터마크 관독기는 디폴트 웹페이지 같은 디폴트 네트워크 리소스에 콘텐츠를 링크시킬 수 있다. 특히, 워터마크 페이로드는 데이터베이스 엔트리(database entry)를 인덱스하는 식별자를 포함한다. 상기 엔트리는 디폴트 웹페이지의 URL을



포함한다. 그러나, 콘텐츠 소유자/분배자는 소유자의 웹사이트에 전용의 새로운 URL 같은 식별자에 대한 새로운 기기 상태를 지정하기 위해 데이터베이스 엔트리를 동적으로 갱신할 수 있다.

<189> **컴퓨터 실행들을 위한 오퍼레이팅 환경**

<190> 도 7은 상술한 워터마킹 시스템들의 소프트웨어 실행들을 위한 오퍼레이팅 환경으로 작용하는 컴퓨터 시스템의 일례를 예시한다. 임베더 및 검출기는 C/C++로 실행되며, 많은 다른 컴퓨터 시스템들에 부착될 수 있다. 도 7은 일반적으로 상기한 시스템의 일례를 도시한다.

<191> 도 7에 나타난 컴퓨터 시스템은 프로세싱 유닛(1221), 시스템 메모리(1222) 및 시스템 메모리를 포함한 다양한 시스템 구성요소들을 프로세싱 유닛(1221)과 상호접속시키는 시스템 버스(1223)를 포함한 컴퓨터(1220)를 포함한다.

<192> 시스템 버스는 메모리 버스 또는 메모리 제어기, 주변 버스, 및 PCI, VESA, MCA(Microchannel), ISA 및 EISA로 명칭된 버스 구조를 사용한 로컬 버스를 포함한 여러가지 타입들의 버스 구조들 중 임의의 것을 포함할 수 있다.

<193> 시스템 메모리는 판독 전용 메모리(ROM)(1224) 및 랜덤 액세스 메모리(RAM)(1225)를 포함한다. 예를 들면, 시동 중에 컴퓨터(1220) 내의 소자들 사이의 정보 전송에 도움을 주는 기본 경로들을 포함하는 기본 입/출력 시스템(1226)(BIOS)이 ROM(1224)에 저장된다.

<194> 컴퓨터(1220)는 하드디스크 드라이브(1227), 예를 들면, 소거가능한 디스크(1229)에 판독 또는 기입을 위한 자기디스크 드라이브(1228), 예를 들면, CD-ROM 또는 DVD 디스크(1231)를 판독하거나 또는 다른 광학적 매체를 판독 기입하기 위한 광디스크 드라이브(1230)를 더 포함한다. 하드디스크 드라이브(1227), 자기디스크 드라이브(1228), 및 광디스크 드라이브(1230)는 하드디스크 드라이브 인터페이스(1232), 자기디스크 드라이브 인터페이스(1233), 및 광 드라이브 인터페이스(1234) 각각에 의해 시스템 버스(1223)와 접속된다. 드라이브들 및 이와 연관된 컴퓨터 판독 가능 매체는 데이터의 비휘발성 저장 장치, 데이터 구조들, 컴퓨터 실행 가능 명령들(동적 링크 라이브러리들(dynamic link libraries), 및 실행 가능 파일들 등의 프로그램 코드) 등을 컴퓨터(1220)에 제공한다.

<195> 상기 컴퓨터 판독 가능 매체의 설명을 하드디스크, 소거가능 자기디스크 및 광디스크에 관하여 언급하였지만, 자기 카세트들, 플래시 메모리 카드들, 디지털 비디오 디스크들 등의 컴퓨터에 의해 판독될 수 있는 다른 타입들의 매체를 포함할 수도 있다.

<196> 다수의 프로그램 모듈들이 오퍼레이팅 시스템(1235), 하나 이상의 애플리케이션 프로그램(1236), 다른 프로그램 모듈(1237), 및 프로그램 데이터(1238)를 포함한 RAM(1225) 및 드라이브들에 저장될 수 있다.

<197> 사용자는 키보드(1240) 및 마우스(1242)와 같은 포인팅 장치를 통해 명령 및 정보를 퍼스널 컴퓨터(1220)에 입력할 수 있다. 다른 입력 장치들은, 마이크로폰, 사운드 카드, 라디오 또는 텔레비전 튜너, 조이스틱, 게임 패드, 위성 접시(satellite dish), 디지털 카메라, 스캐너 등을 포함할 수 있다. 디지털 카메라 또는 스캐너(43)는 상술한 검출 공정을 위해 타겟 이미지를 캡처하기 위해 사용될 수 있다. 카메라 및 스캐너는 각각 표준 인터페이스(44)를 통해 컴퓨터에 접속된다. 현재, USB(Universal Serial Bus), PCI(Peripheral Component Interconnect) 및 병렬 포트 인터페이스와의 인터페이스를 위해 설계된 디지털 카메라가 있다. 카메라용의 2개의 표준 주변 인터페이스들이 USB2 및 1394(또는, 방화벽 및 iLink로 공지됨)를 포함한다.

<198> 카메라 또는 스캐너와 더불어, 워터마킹된 이미지들 또는 비디오는 네트워크 접속 및 텔레비전 튜너 등으로부터 매체를 스트리밍하는 패키징된 매체 장치들(예를 들면, CD, DVD, 플래시 메모리 등)과 같은 다른 소스들로부터 제공될 수 있다. 마찬가지로, 워터마킹된 오디오는 매체, 라디오 튜너, 사운드 카드들 등을 스트리밍하는 패키징된 장치들로부터 제공될 수 있다.

<199> 상기한 것과 다른 입력 장치들은 종종 직접 또는 간접적으로 시스템 버스와 결합된 포트 인터페이스(1246)를 통해 프로세싱 유닛(1221)과 접속된다. 이러한 인터페이스의 예들로는 직렬 포트, 병렬 포트, 게임 포트 또는 범용 직렬 버스(USB)를 포함한다.

<200> 모니터(1247) 또는 다른 타입의 디스플레이 장치는 또한 비디오 어댑터(1248)와 같은 인터페이스를 통해 시스템 버스(1223)와 접속된다. 모니터와 더불어, 퍼스널 컴퓨터는 일반적으로 스피커들 및 프린터들과 같은 다른 주변 출력 장치(미도시)를 포함한다.



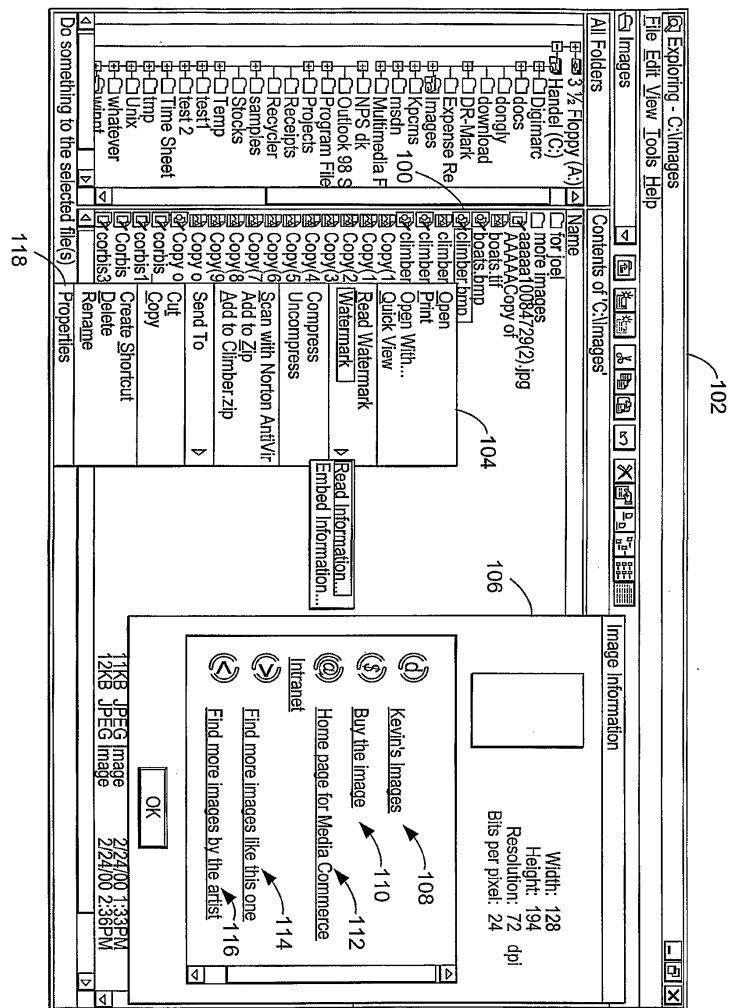
- <201> 컴퓨터(1220)는 원격 컴퓨터(1249) 같은 하나 이상의 원격 컴퓨터들과의 논리 접속들을 사용하여 네트워킹된 환경에서 동작한다. 원격 컴퓨터(1249)는 서버, 라우터, 피어 장치 또는 다른 공통 네트워크 노드일 수 있으며, 일반적으로는 메모리 저장 장치(1250)만이 도 7에 예시되었지만, 컴퓨터와 관련해 설명한 소자의 대부분 또는 모두를 포함한다. 도 7에 도시된 논리 접속들은 로컬 에리어 네트워크(LAN)(1251) 및 와이드 에리어 네트워크(WAN)(1252)를 포함한다. 이러한 네트워킹 환경은 사무실, 기업-와이드 컴퓨터 네트워크, 인트라넷 및 인터넷에서는 일반적이다.
- <202> LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1220)는 네트워크 인터페이스 또는 어댑터(1253)를 통해 로컬 네트워크(1251)와 접속된다. WAN 네트워킹 환경에서 사용될 때, 퍼스널 컴퓨터(1220)는 일반적으로 모뎀(1254) 또는 인터넷 같은 와이드 에리어 네트워크(1252)를 통해 통신을 확립하기 위한 다른 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀(1254)은 직렬 포트 인터페이스(1246)를 통해 시스템 버스(1223)에 접속된다.
- <203> 네트워킹된 환경에서, 퍼스널 컴퓨터(1220) 또는 그 일부와 관련해 도시된 프로그램 모듈들은 원격 메모리 저장 장치에 저장될 수 있다. 상술한 프로세스는 병렬 프로세스들과 같이 분배식 형태로 실행될 수 있다. 도시된 네트워크 접속들은 예시적인 것이며, 컴퓨터들간에 통신 링크를 확립하기 위한 다른 수단들이 사용될 수 있다.
- <204> **다른 형태들의 매체 객체 링크링으로의 확장들**
- <205> 상술한 방식들은 이미지, 그래픽, 비디오 및 오디오 파일 또는 2개 이상의 다른 매체 타입들을 갖는 파일들을 포함한 매체 객체 파일들에 대해서 실행될 수 있다. 또한, 매체 객체는 객체 내에 임베딩된 워터마크 외의 데이터 구조들을 통해 그 메타데이터와 링크될 수 있다. 예를 들면, 객체 식별자는 워터마크 내에 삽입될 필요가 없으며, 대신에 파일 헤더 같은 매체 객체 파일 도처에 배치될 수 있다. 상기 식별자는 코딩된 헤더 또는 압축된 파일들의 헤더에 삽입될 수 있다. 식별자를 추출하기 위하여, 디코더는 헤더를 분석하여, 객체 식별자를 추출한다. 이후, 디코더는 직접적으로, 또는 웹 브라우저와 같은 다른 애플리케이션을 론칭시킴으로써 상기 식별자를 메타데이터 서버에 포워딩하여, 메타데이터 요구를 발행하고, 메타데이터 서버로부터 리턴된 데이터 및/또는 해석 코드를 출력한다.
- <206> **결론**
- <207> 특정한 실시예들을 참조하여 기술의 원리들을 설명하고 예시하였지만, 이 기술이 많은 다른 형태로 실행될 수 있음을 인식할 것이다. 본 명세서를 지나치게 연장하지 않고 포괄적인 개시를 제공하기 위하여, 출원인은 본 특허 및 상기 참조된 특허출원을 편집한다.
- <208> 상술한 실시예에서 엘리먼트 및 특성의 특정한 조합은 일례일 뿐이며, 상기한 학습을 다른 학습 및 본원에 편집된 참조 특허/출원과 상호교환하고 대체하여 또한 구현될 수 있다.
- <209> 본 발명의 원리가 적용될 수 있는 다양한 실시예들에 있어서, 상세 실시예들은 예시적인 것일 뿐이며, 본 발명의 범주를 제한하려는 의도는 아니다. 오히려, 본 발명은 다음의 클레임의 범주와 사상 내에서 모든 상기 실시예들 및 이와 동등한 실시예들을 포함할 수 있다.
- 도면의 간단한 설명**
- <17> 도 1은 오퍼레이팅 시스템 또는 다른 애플리케이션 프로그램 내에 워터마크 디코더를 통합함으로써 가능하게 된 사용자 인터페이스 특징들의 일례를 나타내는 도면.
- <18> 도 2는 도 1의 파일 브라우저 내의 메타데이터를 디스플레이하기 위한 사용자 인터페이스의 대안적인 실시예를 나타내는 도면.
- <19> 도 3은 인터넷 브라우저 내에 워터마크 디코더를 통합함으로써 가능하게 된 사용자 인터페이스 특징들의 일례를 나타내는 도면.
- <20> 도 4는 워터마크를 통해 매체 객체와 링크된 옵션들의 확장된 메뉴로서 도 3의 일례를 나타내는 도면.
- <21> 도 5는 매체 플레이어 내에 워터마크 디코더를 통합함으로써 가능하게 된 사용자 인터페이스 특징들의 일례를 나타내는 도면.
- <22> 도 6은 오퍼레이팅 시스템 또는 다른 애플리케이션 프로그램 내에 워터마크 인코더를 통합함으로써 가능하게 된 사용자 인터페이스 특징들의 일례를 나타내는 도면.
- <23> 도 7은 워터마크 인코더/디코더 인에이블 애플리케이션들의 소프트웨어 실행들을 위한 오퍼레이팅 환경으로서

작용하는 컴퓨터 시스템의 도면.

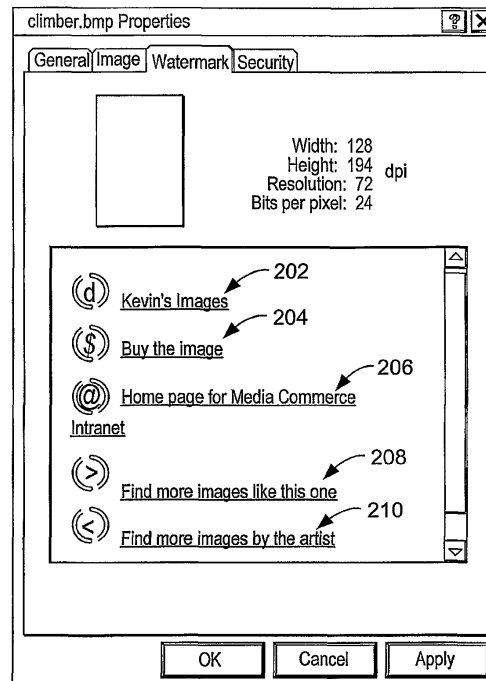
- <24> 도 8은 용어들 "기밀(Confidential)"을 포함한 이미지를 갖는 도면.
- <25> 도 9는 종래의 디지털 워터마크에서의 필드들의 도면.
- <26> 도 10은 종래의 이메일 시스템의 도면.
- <27> 도 11은 도 10에 나타난 워터마킹 판독 및 검출 프로그램의 더 상세한 도면.
- <28> 도 12는 워터마크 콘텐츠 필터들을 갖는 콘텐츠 필터링 및 인덱싱 시스템을 예시하는 도면.
- <29> 도 13은 분배된 워터마크 디코더 시스템(watermark decoder system)을 예시하는 도면.

## 도면

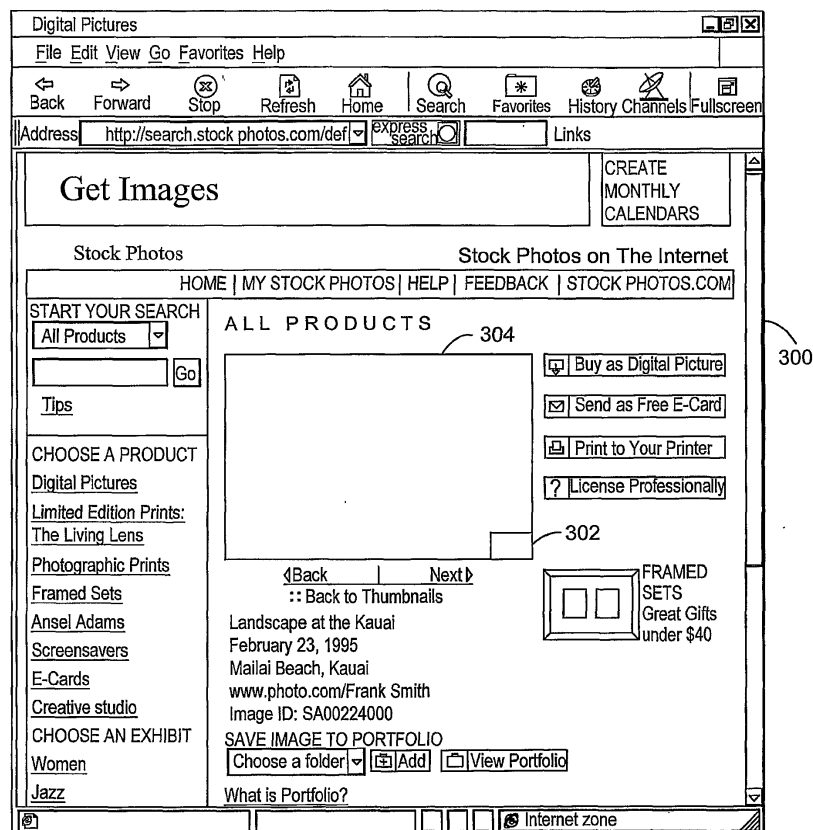
도면1



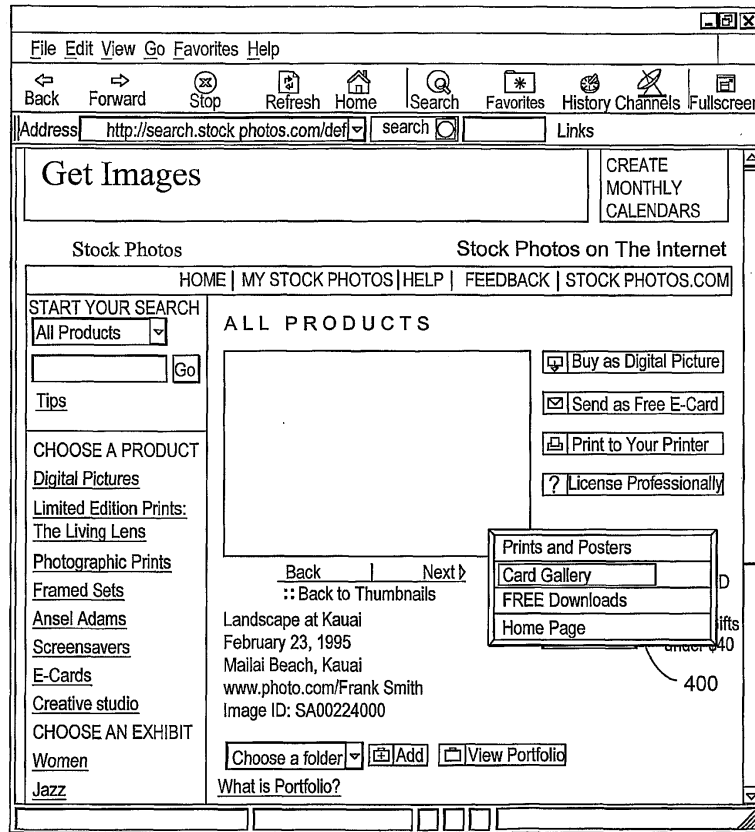
도면2



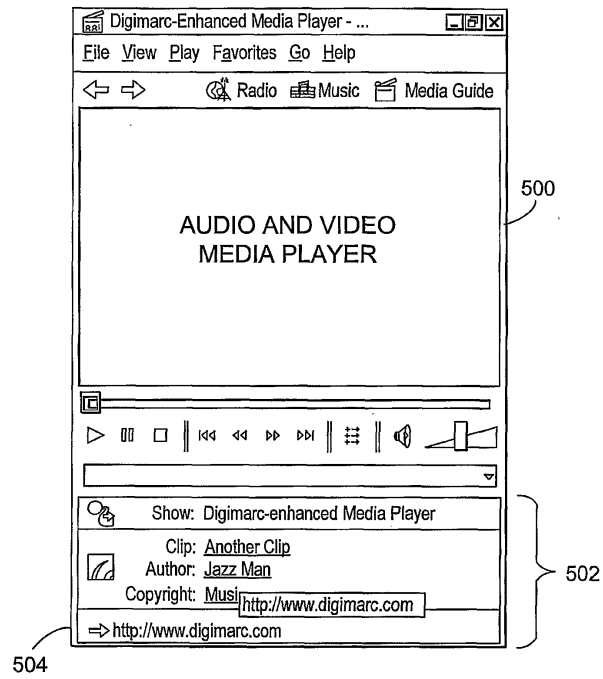
도면3



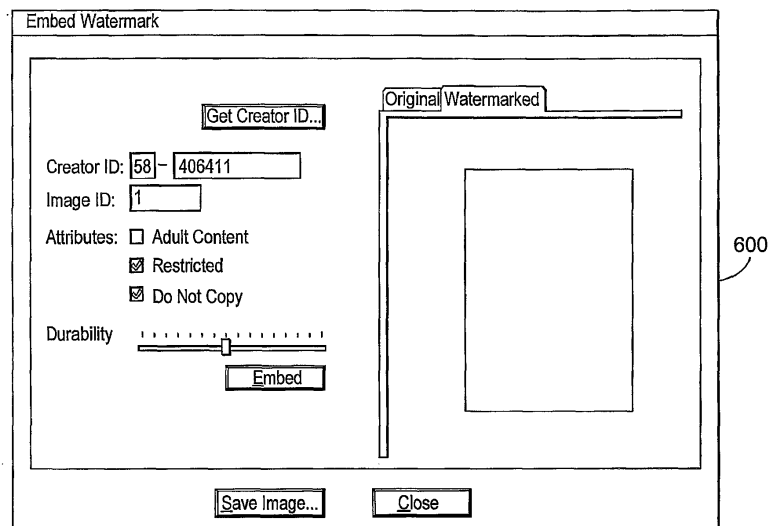
도면4



도면5

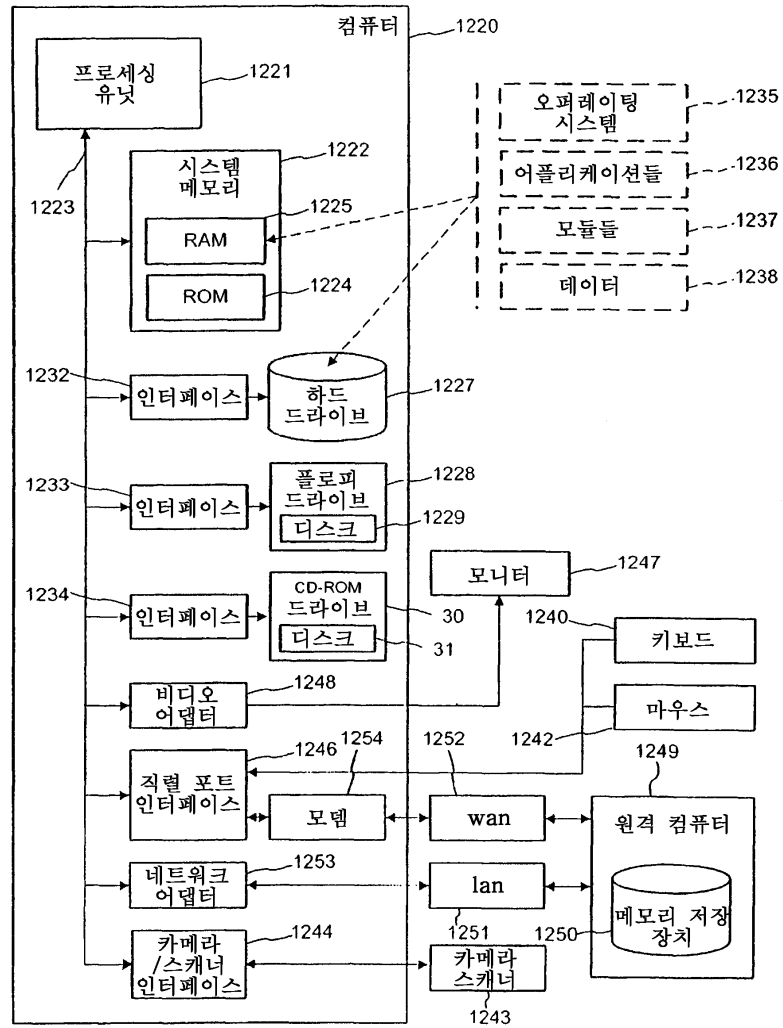


도면6

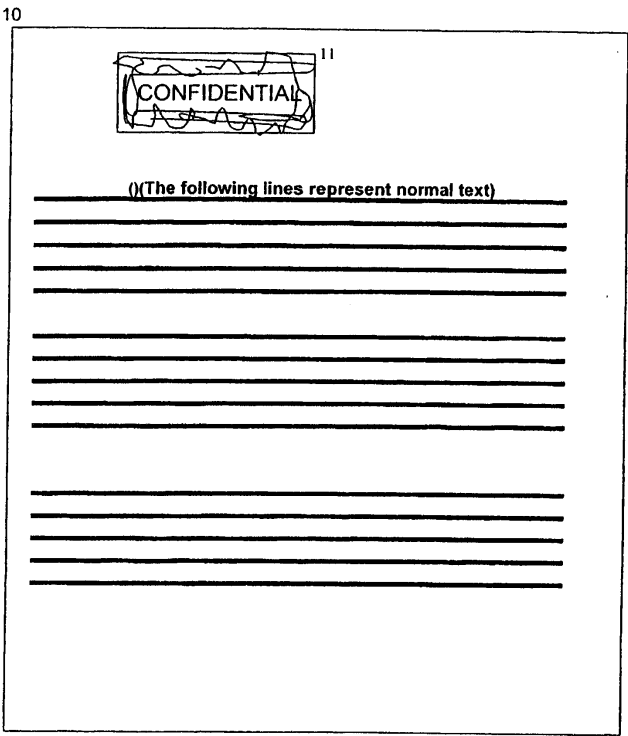




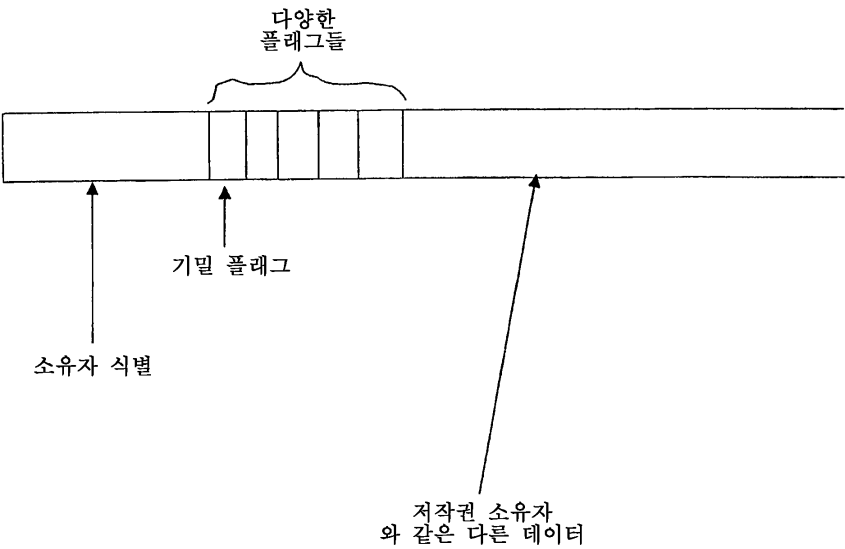
도면7



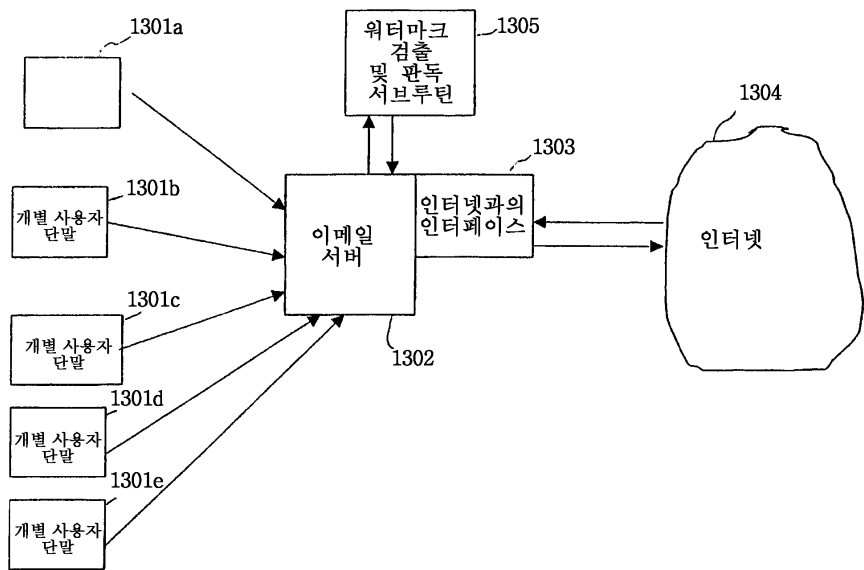
도면8



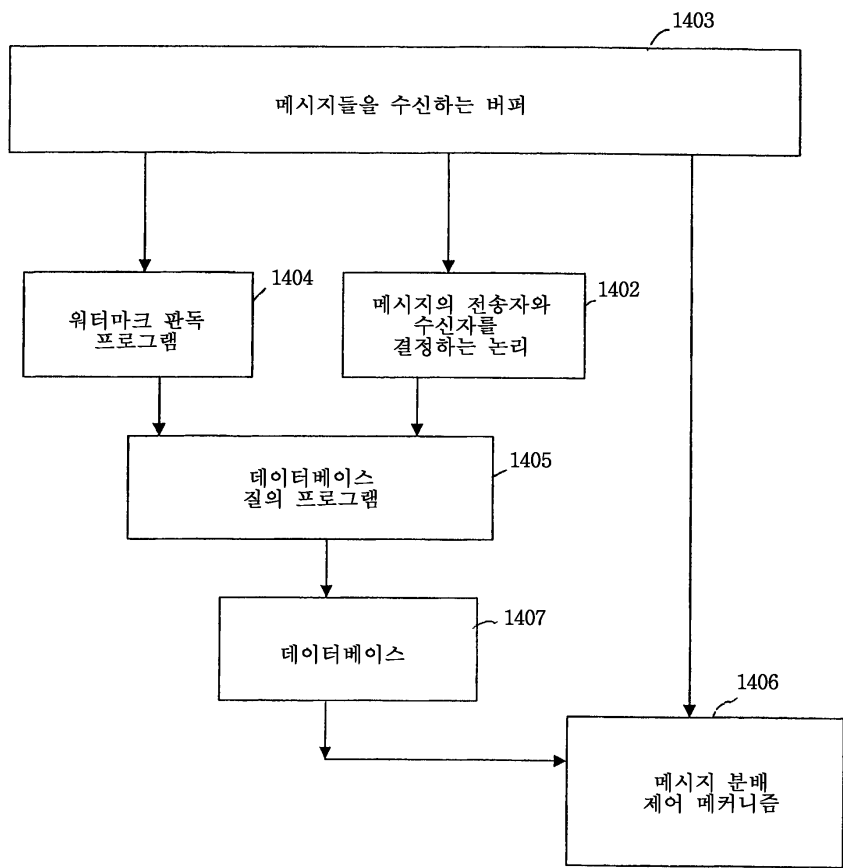
도면9



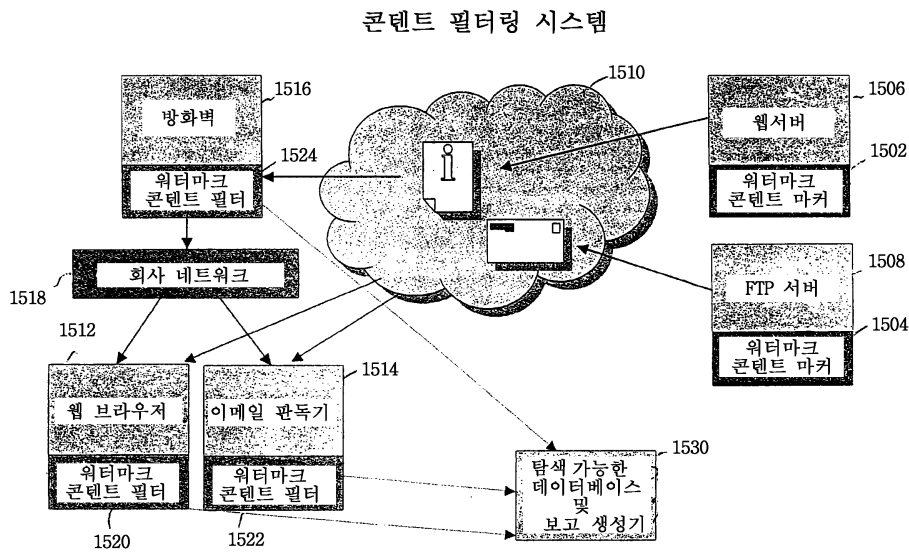
도면10



도면11



도면12



도면13

