(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04N 5/913 (2006.01)

(45) 공고일자 2007년08월06일
(11) 등록번호 10-0746018
(24) 등록일자 2007년07월30일

(21) 출원번호	10-2001-7011504	(65) 공개번호	10-2002-0022131
(22) 출원일자	2001년09월10일	(43) 공개일자	2002년03월25일
심사청구일자	2005년03월10일		
번역문 제출일자	2001년09월10일		
(86) 국제출원번호	PCT/US2000/006296	(87) 국제공개번호	WO 2000/54453
국제출원일자	2000년03월10일	국제공개일자	2000년09월14일

(81) 지정국

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

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

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

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

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

(30) 우선권주장

60/123,581	1999년03월10일	미국(US)
60/123,587	1999년03월10일	미국(US)
60/126,591	1999년03월26일	미국(US)
60/126,592	1999년03월26일	미국(US)
09/404,291	1999년09월23일	미국(US)
09/404,292	1999년09월23일	미국(US)

(73) 특허권자

디지맥 코포레이션
미국,오레곤97008,비버톤,에스더블유 제미니 드라이브 9405

어코우스틱 인포메이션 프로세싱 랩, 엘엘씨.
미국 와싱톤 98648, 스티븐슨, 노스이스트 세다 스트리트 110

(72) 발명자 레비,켄네스,엘.
미국,와싱톤98648,스티븐손,노스이스트세다스트리트110

(74) 대리인 이병호
장훈

(56) 선행기술조사문헌
US05721788

심사관 : 최성진

전체 청구항 수 : 총 15 항

(54) 디지털 저작권 관리를 위한 신호 프로세싱 방법들, 디바이스들, 및 응용들

(57) 요약

본 기술들은, 연산적으로 간단하고 크게 주의를 끌지 않는 방식으로(1010), 보조 데이터(1030)를 전자 컨텐트(1020; 예로서, 오디오, 비디오, 정지 이미지 등) 내에 스테가노그래피적으로 삽입하는 것을 설명한다. 삽입 데이터는 저작권 또는 다른 소유권 정보를 전달하거나, 디바이스 제어 목적들(예를 들어, 비인가 재생 방지)을 위해 사용될 수 있다. 보조 데이터의 제거에 대한 다수의 대응 수단들이 강구되며, 이는 이런 데이터가 존재할 때 컨텐트의 키 방식(keying) 사용을 포함한다. 삽입 데이터는 예로서, 매체의 특성들에 따라 삽입 데이터를 수정함으로써 부호화된 매체에 의존하여 이루어질 수 있다. 또한, 부호화도 양호하게 적용될 수 있다(1040). 재생 디바이스들은 이전에 액세스된 컨텐트로부터의 ID들을 추적하고, 사용 규칙들을 집행하기 위해 장착될 수 있다. 일부 실시예들은, 예로서 배포에 앞서 로버스트 워터마크가 부호화되어 컨텐트를 보호하고, 재생 디바이스에 의해 제 2 워터마크가 부호화되어 그 디바이스에 대해 그 컨텐트를 고유하게 링크시키도록 기능하는 등의 장점을 얻기 위해 다중 워터마크들을 사용한다. 일부 응용들은 특정 정보(예로서, 헤더로부터)를 스크램블링되지 않고 자유롭게 액세스할 수 있는 상태로 남겨두는 방식으로 컨텐트를 스크램블링하여 이점을 얻는다.

대표도

도 23

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.

데이터 신호로부터 보조 정보를 검색하는 단계로서, 상기 보조 정보는 상기 데이터 신호 내에서 부호화되고, 상기 보조 정보는 상기 데이터 신호가 비압축 형태를 포함하는 동안 상기 데이터 신호로부터 검색되는, 상기 보조 정보 검색 단계;

상기 데이터 신호를 압축하는 단계; 및

상기 검색된 보조 정보를 상기 압축된 데이터 신호 내에 삽입하는(embedding) 단계로서, 상기 압축된 데이터 신호는 상기 검색된 보조 정보를 포함하는, 상기 검색된 보조 정보 삽입 단계를 포함하는, 방법.

청구항 11.

제 10 항에 있어서,

상기 데이터 신호는 비디오를 나타내는, 방법.

청구항 12.

제 10 항에 있어서,

상기 검색된 보조 정보는 상기 비압축된 데이터 신호 내에서 스테가노그래피적으로 부호화되는(steganographically encoded), 방법.

청구항 13.

데이터 신호로부터 보조 정보를 검색하는 단계로서, 상기 보조 정보는 상기 데이터 신호 내에서 부호화되고, 상기 보조 정보는 상기 데이터 신호가 압축된 형태를 포함하는 동안 상기 데이터 신호로부터 검색되는, 상기 보조 정보 검색 단계;

압축 해제된(decompressed) 데이터 신호를 얻기 위해 상기 압축된 데이터 신호를 압축 해제하는 단계; 및

상기 검색된 보조 정보를 상기 압축 해제된 데이터 신호 내에 삽입하는 단계로서, 상기 압축 해제된 데이터 신호는 디지털 데이터를 포함하고, 그에 의해 상기 압축 해제된 데이터 신호는 그에 삽입된 상기 보조 정보를 포함하는, 상기 검색된 보조 정보 삽입 단계를 포함하는, 방법.

청구항 14.

제 13 항에 있어서,

상기 데이터 신호는 비디오를 나타내는, 방법.

청구항 15.

제 13 항에 있어서,

상기 검색된 보조 정보는 상기 압축 해제된 데이터 신호 내에서 스테가노그래피적으로 부호화되는, 방법.

청구항 16.

삭제

청구항 17.

삭제

청구항 18.

삭제

청구항 19.

삭제

청구항 20.

비디오 컨텐트의 프로세싱을 관리하는 방법으로서,

상기 비디오 컨텐트는 사용자에게 디스플레이하기 위해 렌더링될 화상 요소들을 나타내는 화상 데이터를 포함하고, 상기 화상 데이터와 함께 전달되지만 사용자에게 디스플레이하기 위해 렌더링될 화상 요소들을 나타내지 않는 보조 데이터를 포함하는, 상기 비디오 컨텐트 프로세싱 관리 방법에 있어서:

(a) 상기 보조 데이터에서 복사 제어 데이터를 검사하는 단계;

(b) 상기 복사 제어 데이터가 없는 경우에만, 상기 화상 데이터에서 디지털 워터마크를 검사하는 단계; 및

(c) 상기 복사 제어 데이터가 없고 상기 디지털 워터마크가 존재한다면, 상기 비디오 컨텐트의 프로세싱을 제한하는 단계를 포함하는, 비디오 컨텐트 프로세싱 관리 방법.

청구항 21.

분배용 비디오 컨텐트를 준비하는 방법으로서,

상기 비디오 컨텐트는 사용자에게 디스플레이하기 위해 렌더링될 화상 요소들을 나타내는 화상 데이터를 포함하고, 상기 화상 데이터와 함께 전달되지만 사용자에게 디스플레이하기 위해 렌더링될 화상 요소들을 나타내지 않는 보조 데이터를 포함하는, 상기 분배용 비디오 컨텐트 준비 방법에 있어서:

디지털 워터마크를 상기 화상 데이터 내에서 부호화하는 단계 및 복사 제어 데이터를 상기 보조 데이터 내에 포함시키는 단계를 포함하고,

순응 디코더 디바이스는 상기 복사 제어 데이터가 없는 경우에만, 화상 데이터에서 상기 디지털 워터마크를 검사하고, 상기 디지털 워터마크가 존재하는 경우, 상기 비디오 컨텐트의 처리를 제한하는 단계를 포함하는 상기 디지털 워터마크의 조사와 함께 상기 복사 제어 데이터의 검사에 기초하여 복사 제어 결정을 할 수 있는, 분배용 비디오 컨텐트 준비 방법.

청구항 22.

제 21 항에 있어서,

상기 보조 데이터는 헤더 데이터를 포함하는, 분배용 비디오 컨텐트 준비 방법.

청구항 23.

데이터 신호로부터 보조 정보를 검색하는 단계로서, 상기 보조 정보는 상기 데이터 신호에 삽입되는, 상기 검색 단계;

상기 데이터 신호를 변환하는 단계; 및

상기 변환된 데이터 신호에 상기 검색된 보조 정보를 삽입하는 단계로서, 상기 변환된 데이터 신호는 상기 검색된 보조 정보를 포함하는, 상기 삽입 단계를 포함하는 방법.

청구항 24.

제 23 항에 있어서,

상기 변환 단계는 압축을 포함하는, 방법.

청구항 25.

제 20 항에 있어서,

상기 보조 데이터는 상기 화상 데이터에 관하여 대역외인, 비디오 컨텐트 프로세싱 관리 방법.

청구항 26.

제 20 항에 있어서,

상기 디지털 워터마크는 존재 또는 부재의 2 개의 상태들만을 갖는, 비디오 컨텐트 프로세싱 관리 방법.

청구항 27.

제 21 항에 있어서,

상기 보조 데이터는 상기 화상 데이터에 관하여 대역외인, 분배용 비디오 컨텐트 준비 방법.

청구항 28.

제 21 항에 있어서,

상기 디지털 워터마크는 존재 또는 부재의 2 개의 상태들만을 갖는, 분배용 비디오 컨텐트 준비 방법.

명세서

기술분야

본 발명은 신호 프로세싱 분야에 관한 것으로, 특히, 디지털 저작권을 관리를 위하여 오디오, 비디오, 및 기타 컨텐트를 부호화하는데 유용한 기술에 관한 것이다.

배경기술

최근의 전자 정보 사용의 폭발적 성장과 함께, 저작권법의 집행이 보다 어려워지고 있다. 음악, 예술 및 다른 가치 있는 정보를 나타내는 디지털 데이터를 복사하는데 필요한 설비 비용은 감소하고 있는 반면, 용이하게 이용할 수 있는 데이터 저장 매체의 용량은 증가되고 있다. 저가의 디바이스들이 기록 가능 콤팩트 디스크들(CD-R 또는 CD-RW들), 멀티 기가바이트 하드 디스크 드라이브들, 고용량 삭제 가능 마그네틱 디스크들, 및 가까운 미래에 상용화될 디지털 다기능 디스크들(DVD들) 같은 디지털 저장 매체에 방대한 양의 데이터를 기록할 수 있다. 용이하게 이용할 수 있는 고해상도 프린터들 및 스캐너들은 대부분의 소비자가 그래픽 정보를 디지털화 및 재생할 수 있게 해준다. 그 외에도, A/D 및 D/A 변환기들을 포함하는, 용이하게 입수할 수 있는 고해상도 사운드 카드들은 대부분의 소비자가 오디오 정보를 디지털화 및 재생할 수 있게 해준다. 디지털 파일들의 복사가 간단하고 저비용일 뿐만 아니라, 인터넷은 저작권을 가진 저작품들의 비인가 배포를 촉진한다.

언제나 원본보다는 열등한 아날로그 복사본들과는 달리, 디지털 정보의 복사본은 복사로 인한 열화가 전혀 발생하지 않고 원본과 동일하다. 불법이지만 정확한 디지털 매체의 복제들과, 아날로그 매체의 거의 동일한 복제들로 인해 연간 수백만 달러가 손실되고 있다. 복사 설비가 용이하게 이용 가능하기 때문에, 비인가 복사본들을 만드는 사람들을 잡는 것이 곤란할 수 있다. 비인가 복사자가 체포되는 경우에도, 원본 문서의 생성자는 여전히, 이른바 비인가 복사본이 실제로 그의 원본 저작품으로부터 복사된 것이며, 독립적으로 생성된 것이 아니라 것을 반드시 증명하여야만 한다.

하나의 양태에서, 하기에 설명된 기술은 디지털 워터마킹(watermarking) 또는 "데이터 은폐(data hiding)" 및 불법 복사의 문제를 해결하기 위한 이용에 관련한 것이다(예로서, 복사 방지 정보나 인증 정보를 원본 데이터 내에 은폐시키는 것). 스테가노그래피(steganography)라고도 지칭되는, 보조 정보를 원본 데이터 내에 은폐시키는 방식이 수천년 동안 사용되어 왔다. 스테가노그래피에서는, 관찰자(또는, 청취자)가 메시지를 본질적으로 지각할 수 없도록, 다른 물체 또는 매체 내에 메시지가 은폐된다. 스테가노그래피는, 메시지의 존재가 통상적으로 명백하지만, 특정한 지식 없이는 그 의미를 확인할 수 없는 암호 작성법(cryptography)과 관련된 것이지만, 그것과는 다르다.

보조 데이터(auxiliary data) 또는 삽입 데이터(embedded data)라고도 지칭되는 은폐 데이터(hidden data)는, 복사 디바이스에 의해 판독가능하고 복사 디바이스가 가용한 복사본을 만들지 못하도록 지시하는 명령들을 원본 데이터 내에 삽입함으로써 비인가 복사를 방지하는데 사용될 수 있다. 또한, 은폐 데이터는 데이터를 증명하는데, 즉, 원작자를 증명하는데 사용될 수도 있다. 하나의 이런 기술은, 보조 정보를 검출 및/또는 제거하는데 보안 알고리즘 또는 코드 같은 특정 지식이 필요한 방식으로 원본 저작품 내에 보조 정보를 삽입하는 것을 수반한다. 복사자는 인증 정보를 제거할 수 없으며, 원본 생성자는 그를 저자로서 식별하는 삽입된 정보를 검색함으로써 그 저작자임을 증명할 수 있다.

데이터 은폐는 비인가 복사의 방지 및 검출 이외의 이용들이 있다. 이런 이용 중 하나는 컨텐트 강화, 즉, 컨텐트를 강화시키기 위해서 정보를 원본 데이터에 추가하는 것이다. 예로서, CD 상의 오디오 데이터 내에 가사가 삽입될 수 있다. 기존 CD 플레이어 상에서 오디오가 재생되는 동안, 특정 가라오케 기계에서 가사가 보여질 수 있다. 또한, 은폐 데이터는 DVD 상의 비디오의 상이한 시청자 선택 버전들을 가진 비디오 데이터의 상이한 세그먼트들을 연관시키는데 사용될 수도 있다. 예로서, 시청자는 아동을 위해 편집된 버전 또는 무삭제 버전 사이에서 선택될 수 있으며, 삽입 보조 데이터는, 어떤 비디오 세그먼트들을 스킵해야 하는지와, 어떤 비디오 세그먼트들이 선택된 버전에 포함되어야 하는지를 DVD 플레이어에 지시하게 된다.

보조 데이터가 은폐되는 원본 데이터는 표시 디바이스(presenting device)의 도움으로 지각될 수 있는 소정 형태의 정보를 나타낼 수 있다. 예로서, 데이터는 콤팩트 디스크 또는 오디오 DVD 플레이어를 사용하여 표시되는 음악, DVD 플레이어 상에서 표시되는 비디오 필름, 또는 프린터나 컴퓨터 스크린상에 표시되는 이미지를 나타낼 수 있다.

조합된 데이터가 통상적인 표시 디바이스에 의해 사용자에게 표시될 때, 보조 데이터는 원본 데이터의 사용을 간섭하여서는 안 된다. 이상적으로, 사용자는 보조 데이터를 전혀 지각할 수 없어야 한다. 불행히, 삽입 보조 데이터의 양의 증가나, 견고성(robustness; 즉, 공격 및 데이터 수정에 대한 지속성)의 증가는 우연히 그 지각 능력을 증가시킬 수 있다. 보조 데이터가 사용자에게 악영향을 미치지 않고 지각될 수 있는 정도는 응용 분야에 따라 변화된다. 예로서, CD 품질의 오디오에서, 원본 데이터로부터의 작은 변화는 용인할 수 없는 오디오 아티팩트들을 유발할 수 있다. 비디오 데이터에서, 원본 및 조합된 저작품들이 나란히 표시되어 비교된다면 그 작은 변화를 지각할 수 있기는 하지만, 표시된 이미지의 작은 변화는 용인될 수 있다.

보조 정보를 원본 데이터 내에 은폐하기 위한 몇 가지 기술이 공지되어 있다. 데이터는 원본 데이터에 첨부된 헤더들 또는 트레일러들로서 원본 데이터 내에 은폐될 수 있다. 보조 데이터는 쉽게 배치되며, 포맷을 변화시킴으로써 복사본으로부터 제거될 수 있기 때문에, 이런 기술들은 저작권을 가진 저작품들의 보호에 있어서 사용에 한계점을 갖는다. 더욱 정교한 기술들은 원본 데이터 전체에 보조 데이터를 분포시키고, 보조 데이터를 식별하거나 조합된 데이터로부터 제거하는 것이 어렵거나, 바람직하게는, 불가능해질 때까지 보조 데이터와 원본 데이터를 뒤섞는다.

보조 데이터를 원본 데이터 전체에 분포시키는 대부분의 데이터 은폐 기술들은 연산적인 측면이 많으며, 따라서 실행 비용이 비싸다. 많은 이들 기술은 보조 정보를 표시하기 위해 의사 랜덤 노이즈(pseudo-random noise; PN) 시퀀스들의 주기들을 신호와 가산 또는 감산하는 것을 기초로 하며, 이들 시퀀스들은 주파수 영역의 필터링(달리 말해, 정형(shaping))을 필요로 할 수 있다. 나머지들은 푸리에 변환 등에 의해서 원본 데이터가 주파수 영역으로 변환된 후에, 보조 정보를 원본 데이터에 추가하는 것을 기초로 한다. PN 시퀀스의 방식과 동일한 방식으로 보조 데이터의 에너지가 많은 주파수에 걸쳐 확산되도록 주파수 영역에 보조 정보가 추가될 수 있다. 그 외에도, 보조 정보는 주파수들에 걸쳐 정보를 확산시키거나 확산시키지 않은 상태로 주파수 성분들의 위상에 추가된다. 불행히, 데이터를 주파수 영역으로 변환하는 것 및/또는 PN 시퀀스의 에너지를 덜 지각될 수 있도록 정형하는 것은 많은 연산들을 필요로 한다.

보조 데이터를 검출하는 사용자의 능력은 상기 데이터에 의존할 뿐만 아니라, 뇌에 의한 감각 자극의 해석과 감각 기관들의 특성에도 의존한다. 어떤 데이터 은폐 기술들은 원본 데이터를 주파수 영역으로 변환하고, 원본 데이터의 주파수 스펙트럼이 삽입 데이터의 지각을 감소시키는 방식으로 보조 데이터를 삽입한다. 이 정신물리학적 효과는 마스킹이라 알려져 있다. 삽입 보조 데이터가 덜 지각될 수 있는(즉, 마스킹되는) 바람직한 주파수들을 결정하도록 원본 데이터의 주파수 분포가 사용된다. 다른 기술들은 위상을 주파수 영역의 크기만큼 정확하게 지각할 수 없다는 사실을 이용한다.

연산적인 측면에서 덜 격렬하고 여전히 보조 데이터를 원본 데이터 내에 분포시키는 소정의 데이터 삽입 기술들도 있다. 이런 기술들은 진폭 변조, 주파수 대역 소거, 개별 양자화 및 최하위 비트(LSB) 교체를 포함한다. 이들 기술들은 원본 데이터에 무관하게 미리 결정된 위치들에 데이터를 삽입하고, 따라서, 조합된 데이터의 지각적 측면의 영향들을 발생시키기 쉬워진다. 그 외에도, LSB 교체 기술은 저 레벨 노이즈에 의해 교란되기 쉽다.

삽입 데이터를 검색하는 경우에는 삽입을 위해 사용된 기술에 따라 변화된다. 어떤 데이터 은폐 및 검색 기술들은 조합된 데이터를 원본 데이터와 비교함으로써 보조 데이터를 검색한다. 다른 기술들은 원래 데이터를 은폐시키는데 사용되었던, PN 시퀀스들의 데이터 베이스를 사용하여 보조 정보를 검색한다. PN 데이터 베이스 또는 원본 데이터의 복사본이 보조 데이터 추출에 사용될 필요가 있는 기술들은 조합된 데이터가 광범위하게 분포되어 있는 응용분야에서는 사용이 제한된다. 이런 기술들은 보조 데이터가 드물게 검색되고, 단지 저작권 소유자에 의해서만 검색되는 데이터 인증 같은 일부 응용분야들에 유용하다.

삽입되는 데이터 기술들은 하기의 이유들 중 어느 하나 때문에 보조 정보가 제거되기 쉽다. 첫 번째로, 삽입 데이터의 본질은, MPEG 압축시 수행되는 것과 같은 데이터의 비지각적 양태들을 제거하는 비트율 감축(달리 말해, 압축) 방식과 양립할 수 없다. 소정의 삽입 데이터의 핵심 특성이 비지각성이기 때문에, 압축 방식은 삽입 데이터를 제거하도록 작용한다. 삽입 데이터가 현행 압축 기술을 견딜 수 있도록 설계되는 경우에도 다음 세대의 기술은 아마도 이를 제거할 것이다. 비트율 압축 방식들은 매체의 디지털 배포에서 매우 중요한 것이며, 더 많은 연구가 진행되고 있다. 두 번째로, 노이즈 감소 기술들이 삽입 데이터를 제거할 수 있을 것이다. 노이즈 감소 기술들은 주목받는 화제이며, 오래된 기록물들을 복구하는데 사용된다. 대부분의 비지각적 삽입 데이터가 노이즈에 유사하기 때문에, 이들 노이즈 감소 기술들에 의해 제거된다. 다시, 삽입 데이터가 현행 재생 기술을 견디도록 설계되어 있다 해도, 다음 세대의 기술은 이를 제거하게 될 것이다.

다른 양태에서, 본 명세서에 설명된 기술은 변조와 공격에 대해 보다 견고한 삽입 데이터를 형성하기 위한 시스템들 및 방법들에 관한 것이다.

삽입 데이터는 다양한 형태의 변조 및 공격을 받기 쉬울 수 있다. 예로서, 삽입 데이터 기술의 특성은 MPEG 압축시 수행되는 것과 같은 데이터의 비지각적 양상들을 제거하는 비트율 감축(달리 말해 압축) 방식과 상충된다. 대부분의 삽입 데이터의 특성이 그 비지각성이기 때문에, 압축 방식들은 삽입 데이터를 제거하는 경향을 갖는다. 삽입 데이터가 현행 압축 기술을 견디도록 설계되었다 하더라도 다음 세대의 기술은 이를 제거할 수 있다. 비트율 압축 방식은 매체의 디지털 분배에서 매우 중요하며, 많은 연구가 이루어지고 있다. 마찬가지로, 예로서, 오래된 오디오 레코드들을 복구할 때 사용되는 것과 같은 노이즈 감소 기술들은 삽입 데이터를 위협한다. 대부분의 비지각적 삽입 데이터는 노이즈와 유사하기 때문에 이들 노이즈 감소 기술들에 의해 제거되게 된다. 또한, 삽입 데이터가 현행 복구 기술을 견딜 수 있도록 설계되었다 하더라도, 다음 세대의 기술은 아마도 이를 제거할 것이다.

다른 양태에서, 본 명세서에 설명된 기술은 ID 할당 및 바인딩(binding)에 관한 것이다. 컨텐트 공급자들은 컨텐트를 만든 사람만이 그 컨텐트를 액세스(즉, 재생, 복사 또는 기록)할 수 있도록 허용하기를 원할 수 있다. 이를 수행하는 한가지 방법은 ID를 포함하는 컨텐트를 제공하고, 그 ID를 소비자, 랜더링 디바이스 또는 저장 유닛에 로킹(lock)하는 것이다. 그러나, 이들 ID를 사용하는 방식에 대한 이들 기존 해법들은 소비자들에게 부당한 부담을 안겨준다.

사용자 바인딩이라 공지되어 있는 한가지 기존 해법은, 은행 ATM기 작업과 같이 컨텐트를 액세스하기 위해서 개인이 ID 카드 및/또는 비밀 번호(PIN)를 가지고 있을 필요가 있다. 소비자는 은행에서 돈을 찾기 위해서는 이 해법을 받아들이며, 이때 보안은 소비자들에게도 유용하다. 그러나, 예로서 차량 스테레오에서 오디오를 재생할 때에도 컨텐트를 액세스하기 위해서 이런 요구사항들을 소비자들이 받아들일 것인지는 의심스러운 일이다. 그 외에도, 한 그룹의 사람들이 음악과 같은 컨텐트를 공유할 때, 각 개인이 그들의 음악을 듣기 이전에 카드를 찾아야 한다는 것은 불편한 일이다. 마지막으로, 이 해법은 ID를 사용자에게 링크시키는 데이터를 요구하며, 그래서, PIN들 및/또는 ID 카드들이 만들어질 수 있다. 이 데이터는 사용자들의 프라이버시가 침해되었음을 의미한다.

재생 장치 바인딩(player-binding)이라 불리는 다른 기존 해법은 컨텐트의 재생을 하나의 디바이스로 제한한다. 이 해법은 친구들의 음악을 당신의 차량 스테레오로 들을 수 없으며, 당신의 영화를 친구의 집에서 재생할 수 없다는 것을 의미한다. 이 해법은 소비자에게 불편한 것일 뿐만 아니라, 많은 사람들이 그들의 친구들과 함께 이를 재생 또는 관람한 이후 컨텐트를 구매하기 때문에 컨텐트의 판매를 감소시킨다.

매체 바인딩이라 공지되어 있는 마지막 해법은 상기 컨텐트를 저장 유닛에 링크시킨다. 저장 유닛은 자성 하드 드라이브, 광 디스크 또는 전자 메모리를 포함하지만, 이에 제한되는 것은 아니다. 이 해법은, 컨텐트가 상이한 저장 유닛 형태들 사이에서 이동되는 것이 허용되어야만 할 때 성가신 것이 된다. 예로서, 사용자인 조(Joe)가 그의 컴퓨터의 하드 드라이브로부터 그의 오디오를 그의 홈 스테레오에서 재생하기를 원할 수 있거나, 그의 차량 내에서 또는 휴대용 전자 메모리로서의 조그(jog) 상에서 오디오를 가질 수 있기를 원할 수 있다. 그러나 이 매체 바인딩 해법에서는 이 오디오는 한 장소에서만 재생될 수 있으며, 조의 스테레오로부터 그의 차량으로 오디오를 이동시키기 위해서는 그는 어디서 이것이 "체크 아웃"되었는지를 기억하여야만 한다. 그렇지 않으면, 해적판이 제어될 수 없다. 중요하게도, 소비자는 그가 원하는 대로 각각의 장소로부터 오디오를 들을 수 없다.

본 명세서에 설명된 기술의 다른 양태는 저작권 관리 기능들을 수행하기 위해서, 상이한 특성들을 가진 다중 삽입 데이터를 사용하는 방식을 포함한다.

본 명세서에 설명된 기술의 다른 양태는 컨텐트를 보호하도록 컨텐트를 스크램블링하는 것에 관한 것이다.

종종, 액세스를 제한하기 위해서 디지털 신호들을 열화시키는 것이 바람직할 수 있다. 예로서, 유료 TV 방송들은 프로그램에 대해 돈을 지불하지 않은 사람들은 화상이 깨끗하지 못해서 프로그램을 볼 수 없도록 열화시키고, 그 프로그램에 대해 돈을 지불한 사람들은 그 복구 장치가 가동되기 때문에 선명한 화상을 볼 수 있다. 최근에, 디지털 오디오 혁명의 결과로서, MP3(표준 비트율 압축 오디오 파일 포맷) 액세스를 규제할 필요가 있다. 또한, 저가의 휴대용 MP3 플레이어들을 제조하는 것이 바람직하며, 이는 원본 신호의 복구가 간단할 것을 요구한다.

디지털 컨텐트를 열화(다시 말하면, 스크램블링)하는 다양한 기존 방법들이 있다. 일부 방법들은 컨텐트를 디스크램블링하기 위한 키를 요구하지만, 어떤 것들은 그렇지 않다. 대부분의 스크램블링 또는 열화 법들은 간섭 신호를 디지털 컨텐트에 추가하거나, 비트들을 주변으로 이동시키는 것에 기초한다. 다른 방법들은 암호화를 사용하지만, 이는 연산적인 측면의 강도가 강하다.

스크램블링된 채널 상의 영화에 대한 정보가 디스크램블 정보 없이 관람자에게 디스플레이되는 경우가 유리하다.

최근, 디지털 오디오 혁명의 결과로서, 일부 사람들은, 컨텐트의 정확한 디지털 복사본을 만들기 쉽기 때문에 액세스 규제된 MP3(Motion Pictures Expert Group Layer Ⅲ standard bit-rate reduced audio file format)를 보고 싶어한다. 이 규제는 스크램블링 기술을 통해 구현될 수 있다. 그러나 상기 정보를 디스크램블링하지 않고도 스크램블링된 노래에 대한 정보를 규제하는 것이 바람직하며, 그 이유는 이것이 사용자들이 그 노래를 재생할 것인지 아닌지를 결정하기 전에 노래에 대해 배울 수 있게 하며, 따라서 사용자를 위한 시스템의 속도를 개선하기 때문이다. 또한, 사용자들의 재생 장치가 저작권 정보를 신속하게 판독할 수 있고, 그 후에 재생을 가능하게 할 수 있다. 또한, 저렴한 휴대용 MP3 플레이어를 제조하는 것이 바람직하며, 이는 원본 신호를 간단하게 복구할 것을 요구한다.

종래 기술은 다양한 스크램블링 및 디스크램블링 방법을 포함하고 있다. 그러나 이들 방법들은 스크램블링 및 디스크램블링 프로세스 동안 헤더 정보를 홀로 남겨 두도록 설계된 것이 아니며, 따라서, 이들은 모든 정보를 디스크램블링하지 않고 스크램블링된 오디오에 대한 정보를 복구하는 것은 불가능하다.

다음의 상세한 설명은 현재 대두하고 있는 다양한 이슈들에 관련하여, 이들 문제점들 중 일부를 보상하며, 현재까지 발명된 바 없는 새로운 기능을 제공하는 것이다.

발명의 상세한 설명

데이터 은폐 장치에 대한 서론

예시적 실시예들, 방법들 및 작동 특성들에 관하여 하기에 설명한다. 명백히 기술되거나, 정당하게 지시된 바를 제외하고는, 상기 실시예들이 다른 배열들을 배제하는 것으로 생각하여서는 안 된다.

일 실시예에 따라서, 높은 효율과 부수적 비용 감소를 제공하는 데이터 은폐 및 검색 장치 및 방법이 제공된다. 일부 실시예들에서, 데이터가 은폐되어야 하는 위치를 식별하기 위해서 정신물리학적 데이터 은폐(원본 데이터를 수정 또는 변환할 필요 없이)가 사용된다. 특정 실시예들에서, 부호화가 내용 통계시 실질적으로 검출 가능한 어떠한 변화도 유발하지 않으며, 은폐된 신호를 식별 및 제거하는 것을 더욱 어렵게 만든다.

본 기술은 지각력, 견고성 및 삽입율을 가변하는 파라미터들을 사용자가 설정하는 것을 허용하도록 구현될 수 있어서, 본 기술을 광범위한 응용분야에 사용하는 것을 가능하게 한다.

양호한 장치는 표준 퍼스널 컴퓨터 또는 DSP 보드들 상에 제공되는 저장 유닛 및 논리 프로세서를 포함한다. 이들 디바이스들은 사용자의 소정 워터마크가 삽입 및/또는 검색될 수 있도록 데이터 판독기들, 비교기 및 데이터 기록기들로서 작용한다.

양호한 프로세스는 조합 데이터를 형성하도록 보조 정보를 원본 데이터 내에 삽입 및 검색하는 단계를 포함한다. 보조 정보를 수반하도록 데이터 지점들을 파악 및/또는 조절하기 위한, 원본 데이터 내의 위치를 결정하도록 하나 이상의 검출 기준이 사용될 수 있다. 검출 기준들은 보조 데이터의 삽입이 다른 단순 프로세스들에 비해 더욱 작은 지각을 발생시키게 되는 원본 데이터 내의 위치들(국부적 마스킹 기회라 지칭됨)을 파악하도록 사용될 수 있다.

보조 데이터를 삽입할 때, 국부적 마스킹 기회의 존재를 결정하기 위해 원본 데이터 내의 데이터 지점들이 검출 기준들에 따라서 조사된다. 상기 검출 기준 또는 기준들은 예로서, 인근 지점들에 대한 데이터 지점의 관계를 시험하고, 소정 값에 대해 데이터 지점을 비교하는 단계를 포함할 수 있다. 검출 기준들이 충족되는 경우에, 인근 지점들 중 하나 이상 또는 연구된 데이터 지점이 보조 데이터의 삽입 비트의 값을 지시하도록 변화된다.

따라서, 비록 국부적 마스킹 기회에 대한 탐색이 통상적으로 데이터를 통해 한 지점씩 진행되지만, 각 지점의 조사는 그 지점의 값뿐만 아니라, 하나 이상의 인근 지점들의 값들 및/또는 하나 이상의 상기 지점들 사이의 관계를 포함할 수 있다. 지점의 조사가 국부적 마스킹 기회의 존재를 나타내는 경우에, 하나 이상의 상기 국부 지점들(즉, 조사된 지점 또는 하나 이상의 인근 지점들)의 값을 설정함으로써 데이터가 삽입된다.

예시된 실시예에서 인근 데이터 지점들에 설정되게 되는 값은 통상적으로 보조 데이터 비트의 값과 조사된 데이터 지점에 의존한다. 데이터 지점 값은 그것이 이웃 데이터 지점들과 특정 관계를 갖도록 설정될 수 있다. 상기 프로세스는 원본 데이터가 횡단될 때까지 또는 어떠한 삽입될 추가의 보조 데이터도 남아있지 않게 될 때까지 계속된다.

보조 데이터를 검색하는 것은 삽입 프로세스의 역순이다. 조합된 데이터가 국부적 마스킹 기회를 파악해내도록 검출 기준들을 사용하여 횡단된다. 각 국부적 마스킹 기회가 파악되었을 때, 삽입 비트를 지시하도록 설정된 인근 데이터 지점 또는 지점들이 판독되어 삽입 데이터를 추출한다. 상기 프로세스는 조합된 데이터가 횡단될 때까지 계속된다.

양호한 실시예들에서, 데이터 지점 또는 지점들은 인근 데이터 지점들에 대한 값으로 설정되며, 절대값으로 설정되지 않는다. 국부적 마스킹 기회에 데이터 지점들을 설정하는 것과, 원본 데이터에 무관한 값이 아닌 인근 지점들에 관한 값에 대하여 데이터 지점을 설정하는 것 양자 모두는 데이터 지각성을 감소시키는 마스킹을 제공한다. 상기 데이터는 국부적 마스킹 기회 근처의 지점 또는 지점들의 값들이나 관계들을 결정함으로써 추출된다.

하기에 설명되는 두 개의 양호한 실시예들에 대하여, 단지 큰 값들을 가진 지점들만이 최소량만큼 조절되고, 따라서, 이들 실시예들은 강한 자극에 의한 약한 자극의 마스킹에 기반한 것이다. 상기 프로세스는 아날로그 및 디지털 데이터에 적용될 수 있다. 그러나 양자 모두의 실시예들은 현재의 디지털 매체로의 전환과, 이해의 용이성 때문에 디지털 매체에 관하여서만 설명한다.

특히, 양호한 제 1 실시예는 피크가 큰 임계값 위에 있는 한, 그리고, 피크와 다음 지점 사이의 근본적 편차가 너무 크지 않은 한, 피크 레벨과 피크 이후의 데이터 지점 사이의 편차를 사용하여 보조 정보를 수반시킨다. 이 큰 임계값과 최소 편차들은 양호한 지각적 마스킹을 발생시킨다. 삽입 프로세스는 임계값 초과 피크들 이후의 지점을 조절하여 보조 데이터를 은폐시킨다. 따라서, 검색 프로세스는 각 임계값 초과 피크 레벨과 다음 데이터 지점 사이의 편차를 측정하여 보조 데이터를 검색한다.

양호한 제 2 실시예는 근본적 경사의 변화가 안전한 조절을 수용하기에 너무 크고 급격하지 않은 한, 양의 크고 급격한 임계값 교차점에 걸친 경사의 변화를 사용하여 보조 정보를 은폐한다. 다시 말하면, 큰 임계값은 양호한 지각적 마스킹을 형성한다. 실행에서, 삽입 프로세스는 데이터를 삽입하기 위해 경사의 변화를 조절하며, 검색 프로세스는 경사의 변화를 측정하여 보조 데이터를 얻는다.

일반적으로, 양호한 삽입 프로세스는 원본 데이터 전체를 통해 보조 정보의 에너지를 암시적으로 산포시킨다(spread). 이 광대역(boardband) 접근 방식은 청취 불가 주파수 범위 내에 데이터를 배치하는 부대역(sub-band) 접근 방식보다 제거가 더욱 곤란한 데이터를 생성한다. 필요시, 상기 프로세스가 마킹되지 않은 데이터와 해석적으로 동일한 보호된 데이터를 형성하도록 파라미터들이 선택될 수 있다. 중요하게, 상기 프로세스는 지각력, 부호화율 및 공격에 대한 견고성 사이의 바람직한 균형들을 형성하도록 조절될 수 있다.

이런 실시예들은 필수적이지는 않지만 푸리에 변환 같은 소정의 복잡한 데이터 변환들을 요구하지 않고 원본 데이터 상에서 작동하는 것이 바람직하다. 따라서, 원본 데이터가 시간 영역에서 정보를 나타내는 경우에, 데이터는 데이터가 삽입 및 검색될 때 시간 영역 내에 남아있을 수 있다. 물론, 본 기술은 주파수 또는 시간-주파수 영역 같은 모든 형태의 원본 데이터 상에 운용할 수 있다. 예로서, 이는 MPEG 1 및 2 명세를 포함하는 MPEG 데이터와, 시간-주파수 영역 내에 존재하는 ISO 11172-3 및 ISO 13818-7 각각에 적용될 수 있다.

마지막으로, 압축(달리 말해, 부호화) 및 압축해제(달리 말해, 복호화) 프로세스 동안, 분리된, 그러나, 동일할 수 있는 워터마크 절차들을 사용함으로써, 워터마크를 제거하는 압축이라 공지된, 비트율 감축 기술의 문제점을 피할 수 있다.

실시예

양호한 실시예들 및 방법들

일 실시예에 따른 시스템은 보조 정보(또는 데이터)를 원본 데이터 내에 은폐하고, 상기 보조 정보를 검색하기 위한 장치 및 방법을 포함한다.

도 1은 데이터를 삽입하기 위한 예시적 방법을 수행하는데 포함되는 단계들의 개요를 도시하고 있다. 도 2는 도 1의 방법을 수행하기 위해 사용될 수 있는 장치(10)의 블록도를 도시하고 있다. 장치(10)는 퍼스널 컴퓨터 또는 공학용 워크스테이션 형태의 인텔 펜티엄 또는 DEC 알파 같은 범용 프로세서, 퍼스널 컴퓨터 또는 공학 워크스테이션, 텍사스 인스트루먼츠 TMS320 라인 같은 디지털 신호 프로세서(DSP), 미디어 프로세서 같은 특정된 CPU 또는 통상적 프로세싱 회로일 수 있는 논리 프로세서(14)를 포함하고 있다. 또한, 장치(10)는 랜덤 액세스 메모리(RAM) 또는 지연들(delays)일 수 있는 저장 유닛(18)을 포함한다. 예시적 실시예에 사용된 알고리즘이 고도의 연산 능력을 요구하는 것이 아니기 때문에, 이들은 초당 백만 명령 미만 수준의 계산을 요구하며, 현대식 퍼스널 컴퓨터들이나 그와 유사한 디바이스들(예로서, 휴대용 정보 단말기(PDA), 전용 매체 재생기들 등) 등에 의해 수행될 수 있다.

하기에 언급될 원본 데이터는 각 샘플이 이진수들을 사용하여 특정 시간의 음향의 크기를 나타내는, 주기적으로 그 진폭을 샘플링함으로써 기록된 음향을 나타낼 수 있다. 마찬가지로, 상기 샘플들은 이미지 또는 비디오의 화소들을 나타낼 수 있다. 또한, 원본 데이터들은 그룹으로 연관된 일련의 이진 데이터일 수 있다. 유사하게, 양호한 보조 정보는 "1"들과 "0"들로서 나타낼 수 있는 소정의 데이터이지만, 포함된 배열을 대응적으로 개조하여 다른 심볼 알파벳들이 마찬가지로 사용될 수 있다.

도 1은 단계(20)에서, 원본 데이터의 일부가 도 2의 저장 유닛(18) 내로 판독되는 것을 도시하고 있다. 단계(24)는 샘플 데이터가 논리 프로세서(14)에 의해 순차적으로 조사되어 소정 검출 기준들에 부합되는 샘플 지점들을 파악한다. 이런 샘플 지점들은 "국부적 마스킹 기회들"의 존재를 나타내며, 그 이유는 상기 검출 기준들이, 보조 데이터를 삽입하기 위한, 상기 지점에서 또는 그 지점 인근에서의 하나의 샘플 또는 몇 개의 샘플들의 값의 변화가 음향의 청취자에 의해 일반적으로 최소한으로 지각될 수 있도록 하는 것이기 때문이다. 마스킹의 양은 데이터 형태와 사용자에 의해 선택된 설정들에 의존한다. 예로서, 마스킹은 압축되지 않은 오디오에 대해서는 커질 수 있고, MPEG 같이 비트율 감축된(디지털적으로 압축된) 오디오에 대해서는 덜해질 수 있다. 은폐 데이터를 파악하기 위한 데이터 검색 동안, 동일한 검출 기준들이 적용될 수 있다.

원본 데이터 내의 각 지점은 국부적 마스킹 기회를 나타내는지 아닌지를 결정하도록 조사되는 것이 바람직하다. 국부적 마스킹 기회를 결정하기 위한 기준 또는 기준들은 조사된 지점의 값뿐만 아니라 하나 이상의 인근 또는 이웃 지점의 값 또는 인근 지점과 조사 지점 사이의 관계도 포함할 수 있다. 검출 기준들은 예로서, 상기 조사 지점이 소정 임계값을 초과하였는지 여부 및/또는 상기 지점이 국부 최대 또는 피크 인지 여부 및/또는 상기 지점이 1차 또는 더 높은 차수의 도함수의 국부 최대인지 여부를 요구할 수 있다. 상기 기준들은 조사 지점에 연속하는 지점이 소정 양보다 낮은 수준으로 상기 조사 지점과 상이한 값을 가지는지 또는 상기 조사 지점에 대해 소정의 다른 관계를 가지는지를 필요 조건으로 포함할 수 있다.

샘플 데이터 지점들은 예로서, x-축 상의 시간과, y-축 상의 샘플의 크기를 가진 그래프 상에 그려진 것으로 간주될 수 있다. 따라서, 일련의 데이터 지점들은 소정 지점들 사이에 경사를 가진 것으로 간주될 수 있고, 상기 경사의 값이 검출 기준들의 일부가 될 수 있다. 상기 기준들은 예로서, 조사 지점과 선행 지점에 의해 형성된 경사가 특정값을 초과하는지 또는 상기 지점 이전과 이후의 경사의 변화가 특정 값을 초과하지 않는지를 조건으로 지정할 수 있다. 상기 조건들은 요구조건들의 소정의 조합을 포함할 수 있으며, 세부적인 예들은 필수적인 것이 아니며, 본 기술의 범주를 제한하는 것이 아니다.

예시된 경우들에서, 보조 데이터를 마스킹하는데 어떠한 복잡한 데이터 변환도 필요하지 않으며, 그래서, 지점을 검출 기준들과 비교하는 것이 비교적 신속하고, 비용이 많이 소모되지 않는다. 다수의 종래 기술의 방법들과는 달리, 이는 이격된 지점들을 사용하여 원본 데이터를 주파수 영역으로 변환하여, 삽입 데이터를 마스킹하는 방식을 결정하며, 예시적 실시예에서는 단지 인근 또는 이웃 지점들, 즉, 유용한 주파수 데이터를 결정하기 위해 사용되기에는 너무 근접한 지점들만을 사용하여 마스킹 기회들을 결정할 수 있다. 인근 지점들은 조사 지점에 인접한 지점들이거나, 바람직하게는 50개 미만, 더욱 바람직하게는 20개 미만의 비교적 작은 수의 지점들 이내에 있는 지점들을 포함한다. 상기 기준은 상기 지점이 임계값을 초과하는지 여부를 결정하는 매우 단순한 것이 될 수 있다.

단계(26)는 검출 기준들에 부합하는 지점이 파악되었을 때, 국부적 마스킹 기회 인근의 특정 샘플 지점 또는 샘플 지점들의 값이 삽입될 보조 데이터의 값을 반영하도록 변화되는 것을 도시한다. 비록, 변화된 샘플이 단순히 삽입 비트의 값을 의미하도록 특정 값으로 설정될 수 있지만, 새로운 값은 일반적으로 국부적 마스킹 기회를 검출하도록 조사된 인근 지점 또는 지점들과 보조 데이터 양자의 값에 의존한다. 예로서, 상기 지점은 값 또는 경사의 변화가 삽입 비트가 "1" 또는 "0"(또는 다른 심볼)인지 아닌지를 나타내도록 설정될 수 있다.

한 지점이 그 새로운 값으로 설정될 때, 상기 변화가 상기 원본 샘플 지점이 상기 검출 기준들에 계속 부합되는 것을 막지 않거나, 이 국부적 마스킹 기회가 보존되고, 검색 프로세스에서 검출되지 않게 되는 어느 한쪽인 것이 바람직하다. 달리 말해서, 삽입 보조 데이터는 검색 불가상태가 될 수 있다.

대안으로, 보조 비트를 최하위 비트로서, 또는 다른 양호하게는 하 순위 비트로서 단순히 삽입하는 것도 가능하다. 삽입 비트의 위치가 데이터가 소정 임계값보다 클 때 등의 국부적 마스킹 기회를 나타내도록 선택되기 때문에, 삽입 비트는 여전히 마스킹된다.

단계(30)는 어떠한 보조 데이터도 삽입될 필요가 없는 경우에 단계(32)에서 프로세스가 종료되는 것을 도시한다. 한편, 단계(34)는 추가의 데이터가 메모리 내에 있는 경우에, 국부적 마스킹 기회들에 대한 탐색을 계속하는 것을 나타낸다. 단계(36)는 메모리 내의 모든 데이터가 아직 다 탐색되지 않은 경우에 추가의 데이터가 메모리 내로 판독되는 것을 나타낸다. 본 기술분야의 숙련자들은 메모리 내의 데이터의 시작 또는 종료점들에서 국부적 마스킹 기회들을 놓치는 것을 방지하기 위해 메모리 내의 데이터의 소정 중첩이 필요할 수 있다는 것을 알 수 있을 것이다.

도 3은 복호화 방법을 수행하는데 포함되는 단계들을 광범위하게 도시하고 있다. 필수적이지는 않지만, 데이터 삽입에 사용된 것과 동일한 프로세서와 메모리가 데이터 검색에 사용될 수 있기 때문에, 도 3의 단계들은 도 2의 하드웨어 부품들을 사용하여 데이터를 추출하는 것을 설명한다. 단계(50)는 원본 데이터의 일부가 저장 유닛 내로 판독되는 것을 나타낸다. 단계(52)는 논리 프로세서가 각 데이터 지점을 조사하여 국부적 마스킹 기회의 존재를 결정하는 것을 나타낸다. 샘플 지점이 국부적 마스킹 기회 조건들에 부합되는 경우에, 단계(54)는 보조 데이터가 삽입되는 방식의 역 관계를 사용하여 삽입 보조 데이터의 "1" 또는 "0" 비트가 추출되는 것을 나타낸다. 단계(56)는 추가의 조합된 데이터가 메모리 내에 있는 경우에 논리 프로세서가 단계(52)로 나머지 지점들에 대한 조사를 계속하는 것을 나타낸다. 단계(58)는 메모리 내의 모든 데이터가 조사되었지만, 데이터 파일 내에 아직 조사되지 않은 조합된 데이터가 있는 경우에 단계(50)에서 추가의 데이터가 메모리 내로 판독되는 것을 나타낸다. 단계(60)는 모든 조합된 데이터가 조사되었을 때 상기 프로세스가 종료되는 것을 나타낸다.

두 개의 특정 실시예들이 간략하게 설명되었으며, 본 방법론의 특징을 예시하기 위해 하기에 상세히 설명된다. 도 4에 도시된 바와 같이, 제 1 실시예는 검출 기준들(120)로서 큰 양의 피크들을 사용하며, 피크와 다음 지점 사이의 편차(130) 내에 보조 정보가 저장된다. 도 7에 도시된 바와 같이, 제 2 실시예는 경사에 미소한 변화를 가진 크고 급격한 임계값 교차점들을 검출 기준들(140)로서 사용하며, 보조 정보(150)는 경사의 변화에 수반되게 된다.

양호한 실시예들이 디지털 데이터를 사용하고 있지만, 본 방법론은 디지털 데이터나 아날로그 데이터 양자 모두에 적용될 수 있다. 예로서, 아날로그 데이터는 나이키스트 비율(Nyquist rate)로 샘플링되어 디지털 데이터를 형성하고, 상기 디지털 데이터 내에 추가의 정보가 은폐될 수 있다. 이때, 조합된 디지털 데이터는 디지털 신호 프로세싱(DSP)에서 공지된 소정의 기존 방법에 의해 아날로그 영역으로 복귀될 수 있다. 이제, 아날로그 데이터는 삽입 데이터를 포함하고 있으며, 이는 샘플링을 사용하여 복호화될 수 있다. 이는 상술한 방법론으로 아날로그 데이터를 부호화하는 한가지 가능한 방법일 뿐이다.

또한, 상기 방법론은 오디오, 음성, 이미지, 비디오 또는 소정의 다른 지각가능한 신호들에 적용될 수 있다. 오디오 및 음성에서, 원본 데이터는 시간에 대한 압력, 주파수에 대한 크기, 또는, 시간에 대한 특정 주파수를 나타낼 수 있다. 이미지들에서, 원본 데이터는 간격에 대한 그레이코드, 간격에 대한 분리 또는 조합된 RGB 또는 등가의 값, 또는, 주파수에 대한 크기를 나타낼 수 있다. 비디오 데이터는 추가된 가용 시간의 차원으로 이미지 데이터를 감싸고 있다. 예로서, MPEG 비트-감축된 오디오 또는 이미지에서, 보조 데이터는 주파수 또는 시간이나 양자 모두에 대한 스케일링 인자들(scaling factors) 또는 주파수 계수들 내에 삽입될 수 있다.

일반적으로, 검출 기준들 중 하나는 큰 임계값이다. 16비트 오디오에서, 최소값 보다 48dB 이상 큰 임계값이 바람직하다. 이 임계값은 마스킹으로 인한 최소 지각으로 데이터를 변화시키는 것을 가능하게 한다. 마스킹은 심리학적 용어이며, 정적 상태 자극에 대한 임계값의 상승으로서 정의된다. 본 명세서에 상기 용어를 사용하는 것은 정의 보다 더 큰 의미로 사용하고 있으며, 어떻게 하나의 데이터 세트가 다른 데이터의 지각을 감소시키는 지를 설명한다. 특히, 압축되지 않은 크기-시간 데이터에서, 감각 시스템의 민감성은 입력 레벨이 증가될 때 감소하게 되며, 따라서, 이웃 데이터 지점의 작은 조절은 큰 임계값에 의해 마스킹된다. MPEG 데이터 같은 비트율 감축된 시간-주파수 데이터에 대하여서는, 비트율을 감축시키기 위해 마스킹이 사용되기 때문에, 마스킹은 미세하고 교본적 정의에 보다 가깝다.

마지막으로, 본 방법은 마스킹이 사용되지 않는 데이터에 적용될 수 있지만, 보조 정보의 검색을 위한 원본 데이터 또는 PN 시퀀스 같은 키가 필요하지 않은 프로세스의 효율이 양호하다. 요약하면, 검출 기준들의 파라미터들은 데이터율, 프로세스 복잡성 및 지각적 품질 사이의 상호작용에 의해 결정된다.

제 1 실시예

특정 제 1 실시예는 원본 데이터 내의 큰 피크들 내에 보조 정보를 은폐하는 것에 기반한다. 본 실시예에서, 보조 정보는 보다 양호한 에러 복구를 위해 워드들 사이에 동기 데이터가 배치되어 있는 N 비트 워드들로 분할되는 것이 바람직하다. 보조 정보는 노이즈나 변조된 파일들에 대한 견고성이 필요 없는 경우에, 상기 워드들 사이에 동기 펄스들을 포함할 필요가 없다.

도 4는 피크 또는 국부 최대를 검출하고, 삽입 비트의 값을 나타내도록 피크에 대한 후속 지점의 값을 설정하는 제 1 실시예를 개념적으로 도시하고 있다.

도 5는 삽입 프로세스를 위한 흐름도의 형태로 의사코드를 포함하고 있다. 상기 프로세스는 thr로 표시된 큰 임계값 위에 존재하면서, 피크 이후 dS로 표시된 상대적으로 작은 감소를 가지는, 양의 피크가 발견될 때까지 원본 데이터를 탐색함으로써 시작된다. 이 프로세스는 박스들(200, 210, 220)로 예시되어 있다. 검출 기준들은 가장 연산적으로 효율적인 순서로 검사되며, 이는 피크들이 최소한의 유사 기준이기 때문에 제일 먼저 상기 지점이 피크를 나타내는지를 찾도록 검사하는 단계를 포함한다.

양호한 피크가 발견되었을 때, 상기 피크 이후의 데이터 지점이 사용자 정의 비트 깊이(b)에 따라 조절되어 보조 정보를 수반하게 된다. 더욱 명확하게 말하면, 보조 워드의 시작인 경우에, 상기 피크 이후의 지점(x[n+1])을 피크(x[n])와 동일해지게 조절하고, 박스들(242, 230, 250)에 도시된 바와 같이, 피크와 다음 지점 사이의 최대 허용가능 변화의 절반(dS/2)을 감산함으로써, 동기화 코드가 삽입된다. 1의 보조 정보 비트는 상기 피크 이후의 지점(x[n+1])을 상기 피크(x[n])와 동일하게 되도록 조절하고, 최대 변화의 절반(dS/2)을 감산하고, 비트 깊이 크기의 절반(2^{b-1})을 가산함으로써 부호화된다. 대응하여, 0의 보조 정보 비트가 피크 이후의 지점(x[n+1])을 상기 피크(x[n])와 동일해지도록 조절하고, 최대 변화의 절반(dS/2)과, 비트 깊이 크기의 절반(2^{b-1})의 합계를 감산함으로써 부호화된다. 이 0들 및 1들의 삽입이 박스들(242, 240, 260, 270, 280)에 도시되어 있다. 데이터 삽입 이후의 두 개의 지점들은 반드시 스킵되어, 그것이 매우 느리게 변화하는(즉, 플랫) 데이터에 대한 다른 피크를 생성하지 않아야하며, 이는 박스(290)에 도시되어 있다.

이들 단계들은 보조 정보(박스 242, 240)가 원본 데이터 내에 은폐되거나 원본 데이터가 끝날 때까지 반복된다.

도 6은 특정 제 1 실시예의 검색 프로세스들을 위한 흐름도의 형태로 의사 코드를 도시하고 있다. 상기 프로세스는 thr로 표시된 큰 임계값 위에 배치되어 있으면서 피크 이후 dS로 표시된 상대적으로 작은 감소를 가지는 양의 피크가 발견될 때까지 원본 데이터를 탐색함으로써 시작된다. 이 프로세스는 박스들(300, 310, 320) 내에 예시되어 있다. 또, 상기 탐색은 효율을 향상시키기 위해 제일 먼저 피크를 찾는다.

양호한 피크가 발견되었을 때, 피크와 피크 이후의 데이터 지점 사이의 편차가 측정되어 보조 정보를 검색한다. 더욱 명확하게 말하면, 피크 마이너스 피크 이후의 지점(x[n]-x[n=1])이 최대 허용가능 변화의 절반(dS/2)에 근접하는 경우에, 새로운 보조 워드가 시작된다. 이는 박스(330, 350)에 도시되어 있다. 피크 마이너스 피크 이후의 지점(x[n]-x[n=1])이 최대 변화의 절반(dS/2)과 실질적으로 같은 경우, 비트 깊이 크기의 절반(2^{b-1})을 감산하여 1의 보조 비트가 발견된다. 이 편차(x[n]-x[n=1])가 최대 변화의 절반(dS/2)과 비트 깊이 크기의 절반(2^{b-1})의 합에 근접한 경우에, 0의 보조 비트가 검색된다. 이 0들의 검색과 1들의 검색은 박스들(340, 360, 370, 380, 382)에 도시되어 있다. 데이터 검색 직후의 두 개의 지점들은 박스(390)에 도시된 바와 같이 스킵될 수 있다.

원본 데이터 내에서 보조 정보가 검색 완료되거나 원본 데이터가 끝날 때까지 이들 단계들이 반복된다.

임계값(thr), 비트 깊이(b) 및 경사 이후 최대 허용 가능 변화(dS)를 포함하는 세 개의 사용자 정의 파라미터들이 있다. 16 비트 오디오에 대하여, 상술한 바와 같이 상기 임계값은 일반적으로 최소 양자화 위의 48dB 정도이다. 샘플당 더 많은 비트들을 가진 데이터에 대하여, 지각을 감소시키도록 임계값이 감소될 수 있다. 비트 깊이는 데이터 삽입을 위한 샘플 지점에 대해 형성될 상대 변화의 지표이다. 따라서, 비트 깊이가 작아질수록 원본 데이터가 덜 교란되게 되고 청취자가 삽입 데

이터를 지각하기가 보다 어려워지지만, 견고성이 약해진다. 즉, 노이즈나 공격에 의해 손실되기 쉬워진다. 16비트 오디오에서 최소 지각은 비트 깊이가 1 과 6 비트들 사이일 때 발견된다. 그러나 보다 큰 지각적 열화가 생기더라도 노이즈에 대한 보다 큰 견고성을 원하는 경우에는 보다 큰 비트 깊이들이 사용될 수 있다. 피크 이후 최대 허용가능 변화(dS)는 최소한 소정 비트 깊이 크기(2^b)여야 한다. 한편, dS를 비트 깊이 크기의 두 배(2^{b+1})로 설정하면, 보다 큰 열화를 대가로 치르고서 더욱 양호한 견고성을 얻을 수 있다. 한편, 통계적 암호 해독에 대해 임계값이 검출되지 않는 상태(통계학적으로 안보임)로 유지하기를 원한다면 dS는 2^b로 설정되어야 하며, b는 가능하게는 3 비트들 미만으로 작아야 한다. dS가 2^b가 아닌 경우에, 삽입된 파일과, 정상적 파일 데이터 사이의 큰 양의 피크들과 그 다음 지점들 사이의 평균 편차의 불일치를 사용하여 파일이 삽입 데이터를 포함하는지 아닌지를 결정할 수 있다. 마지막으로, dS가 2^b 보다 큰 경우에, 삽입을 위해 적합한 더 많은 피크가 발견되기 때문에, 보조 정보 삽입 비율이 증가된다. 상술한 원리들을 사용하여 숙련자들은 특정 응용분야의 요구 조건에 적합한 값으로 사용자 정의 파라미터들을 설정할 수 있을 것이다.

상술한 바와 같이, 큰 임계값은 일반적으로 보조 정보 추가의 지각적 효과를 감소시키며, 데이터 형태에 따라 심지어 보조 데이터를 지각할 수 없게 만들 수도 있다. 그 외에도, 피크에서의 경사가 거의 0이고 데이터가 최소한으로 변화되기 때문에, 수많은 데이터 지점들이 피크와 피크 이후의 데이터 지점 사이의 작은 편차를 만족시킨다. 이 작은 편차는 조절이 임계값에 비해 작아지게 되는 것을 의미하고, 따라서, 삽입 보조 데이터를 지각하는 기회가 감소되는 것을 의미한다.

진행 경로 지시 기능(x[n+1])을 나타내는 버퍼를 사용하여 의사 코드가 도시되어 있다. 이는 프로세스를 설명하고 이해하는 것을 보다 용이하게 한다. 그러나 상기 프로세스는 n=1을 k로 대체하고, 최종 두 지점(x[k-1], x[k-2])들의 트랙을 유지함으로써 결정되는 바와 같이 인과 관계이다.

마지막으로, 피크를 결정하기 위한 더 많은 기준을 추가할 수 있다. 예로서, 피크는 각각 x[n]>x[n-2], x[n]>x[n+2], x[n]>x[n-3], x[n]>x[n+3] 등의 방향인 하나 이상의 지점에 대하여 연장되거나, 피크는 최소의 선명도, 즉, x[n]-x[n-1]>5일 수 있다. 이들 기준들 양자 모두는, 비록 피크 기준들의 변화들이 보조 데이터가 삽입될 수 있는 비율에는 영향을 미치지만, 더 많은 노이즈를 피크의 위치로 이동시키기 때문에, 노이즈에 대한 더욱 양호한 견고성 및 더 작은 왜곡을 생성한다.

삽입 데이터 밀도와 비트율은 원본 데이터와 함께, 그리고, 사용자 정의 파라미터들과 함께 변화된다. 예로서, 5000(74dB)의 임계값과 5의 비트 깊이를 사용하여, 초당 99와 268 비트들 사이의 비트율들이 CD 품질 오디오 데이터에서 달성될 수 있다. 8의 비트 깊이를 사용하고, 임계값을 5,000으로 유지하면, 평균 삽입율이 초당 1,000비트가 된다. 8의 비트 깊이에서 임계값이 2,000으로 낮아지면, 평균 삽입율은 초당 2,000비트들이 된다.

제 2 실시예

특정 제 2 실시예는 경사에 큰 변화가 없는 크고 급격한 임계값 교차점들에 보조 데이터를 은폐한다. 본 방법은 검출된 위치를 변화시키는 노이즈에 보다 강인하다. 이는 임계값 교차점이 일반적으로 정의상 거의 0에 가까운 경사를 가지는 피크에서의 경사보다 더 큰 경사를 가지기 때문에, 노이즈가 피크에 비해 임계값 교차점의 위치를 잘 변화시키지 못하기 때문이다. 제 1 실시예에 비해 더 낮은 삽입 데이터율을 발생시키는, 오디오 데이터를 사용한 테스트가 본 실시예에 예시되어 있으며, 삽입 데이터는 더 낮은 비트 깊이에서보다 쉽게 지각되지만, 대신 노이즈에 대한 견고성이 강하다. 본 응용분야에 따른 적합한 실시예를 찾을 수 있을 것이다.

도 7은 임계값 교차점에서의 경사에 대한 임계값 교차점 이후의 경사를 설정함으로써 데이터가 삽입되는 것을 개념적으로 도시하고 있다.

도 8에는 양호한 제 2 실시예를 사용한 보조 정보 은폐를 위한 의사 코드가 흐름도의 형태로 도시되어 있다. 본 프로세스는 작은 경사의 변화(dS로 표시됨)를 가진 양의, 큰, 급격한 임계값(thr로 표시됨) 교차점이 발견될 때까지 원본 데이터를 탐색함으로써 시작된다. 본 프로세스는 박스들(400, 410, 420)에 도시되어 있다.

양호한 임계값 교차점이 발견되었을 때, 임계값 교차점 이후의 데이터 지점이 사용자 정의 비트 깊이(b)에 따라 조절되어 경사의 변화에 보조 정보를 싣게 된다. 경사의 변화는 (x[n+1]-x[n])-(x[n]-x[n-1])로 정의되거나, 등가인, x[n+1]-2*x[n]+x[n-1]로 정의된다. 더욱 명확하게 말하면, 보조 워드의 시작의 경우에, 박스들(442, 430, 450)에 도시된 바와 같이, 임계값 교차점(x[n+1]) 이후의 지점을 조절하여 경사의 변화가 0이 되도록 함으로써 동기화 코드가 삽입된다. 1의 보조 비트는, 경사의 변화가 비트 깊이 크기의 절반(2^{b-1})과 동일한 양만큼 양(positive)이 되도록 임계값 교차점(x[n+1])

이후의 지점을 조절함으로써 부호화된다. 대응적으로, 0의 보조 비트는, 경사의 변화가 비트 깊이 크기(2^{b-1})와 동일한 양만큼 음이 되도록 상기 임계값 교차점 이후의 지점을 조절함으로써 부호화된다. 이 0들 및 1들의 삽입은 박스들(442, 440, 460, 470, 480)에 도시되어 있다. 박스(490)에 도시된 바와 같이 효율성을 위해 데이터 삽입 이후의 지점은 스킵될 수 있다.

이들 단계들은 보조 정보가 원본 데이터 내에 완전히 은폐되거나, 원본 데이터가 끝날 때까지 반복된다.

도 9는 양호한 제 2 실시예의 보조 정보 검색을 위한 의사 코드를 흐름도의 형태로 도시하고 있다. 상기 프로세스는 작은 경사의 변화(dS로 표시됨)를 가진 양의, 크고 급격한 임계값(thr로 표시됨) 교차점이 발견될 때까지 원본 데이터를 탐색함으로써 시작된다. 이 프로세스는 박스들(500, 510, 520)에 예시되어 있다.

양호한 임계값 교차점이 발견되었을 때, 상기 임계값 주변의 경사의 변화가 측정되어 보조 정보를 검색한다. 또한, 경사의 변화는 (x[n+1]-x[n])-(x[n]-x[n-1])로 정의되거나, 등가인, x[n+1]-2*x[n]+x[n-1]로 정의된다. 더욱 명확하게 말하면, 임계값 교차점이 거의 0의 경사 변화를 가지는 경우에, 박스들(530, 550)에 도시된 바와 같이 새로운 보조 워드가 시작된다. 임계값 교차점이 비트 깊이 크기의 절반(2^{b-1})과 실질적으로 동일한 양의 경사 변화를 가지는 경우에, 1의 보조 비트가 발견된다. 임계값 교차점이 상기 비트 깊이 크기(2^{b-1})와 실질적으로 동일한 음의 경사 변화를 가지는 경우에 0의 보조 비트가 검색된다. 이 0들과 1들의 검색은 박스들(540, 560, 570, 580, 582)에 도시되어 있다. 데이터 검색 이후의 지점은 박스(590)에 도시된 바와 같이 효율을 위해 스킵될 수 있다.

이들 단계들은 원본 데이터 내의 보조 정보가 완전히 검색되거나, 원본 데이터가 끝날 때까지 반복된다.

상술한 바에 따라서, 1은 삽입된 위치가 검출 기준들을 만족시키지 않게 되는 삽입 프로세스가 발생되지 않는다. 더욱 명확하게 말하면, 본 실시예에서는 박스(402, 520)의 검출 기준의 사전 임계값 변화 조건(x[n]-x[n-1]>dS+2^{b-1})은, 다음 데이터 지점의 조절이 상기 지점을 상기 임계값 아래로 내려가게 하지 않는 것을 필요 조건으로 한다. 선택적인 방식으로서는, 삽입 프로세스가 다음 지점이 임계값 아래로 이동하게 하는 경우에, 이 조건을 무시하고 현재 또는 다음 지점 중 어느 한쪽(x[n] 또는 x[n+1] 각각)을 상기 임계값으로 설정하는 것과, 삽입 및 검색 프로세스 양자 모두에서 임계값과 동일한 소정의 데이터 지점들을 무시하는 것이 있다. 단지 동기 신호 또는 0을 삽입할 때에는 다음 지점을 임계값 아래로 이동시키게 될 수 있다. 이들 옵션들의 제공은, 본 실시예가 프로세스가 인과 관계가 되고 그래서, 인과 관계 프로세스들의 공지된 장점을 채용하도록 선택된다.

다시, 큰 임계값 및 최대 허용 가능 경사 변화 조건(dS)은 보조 데이터 삽입의 지각을 감소시키고, 데이터 형태에 따라서 상기 삽입 프로세스는 완전히 지각불가 상태가 될 수 있다. 최대 허용 가능 경사 변화 조건(dS)은 소정의 값을 갖는다. 보다 큰 값은 보다 큰 데이터율을 가진 보다 지각되기 쉬운 왜곡을 허용하는 반면에, 더욱 작은 값은 더 낮은 데이터율을 가진 미세한 왜곡을 허용한다. 16비트 오디오에서 dS의 양호한 설정은 비트 깊이 크기(2^b)와 동일하게 되는 것이다. 또한, 6비트들 아래의 비트 깊이들은 작은 왜곡을 발생시키지만, 노이즈 및 공격에 대한 견고성을 위해 더 큰 비트 깊이들이 사용될 수 있다.

2,000(즉 66dB)의 임계값을 사용하고, 5의 비트 깊이를 사용하면, CD 품질 오디오에 대하여 초당 40 내지 100비트 사이의 데이터율이 기대되며, 평균은 초당 75비트이다. 8의 비트 깊이에서 비트율은 평균 초당 100비트로 증가된다.

수정들

특정 실시예들이 상술되었다. 그러나 각 이용에 대하여 프로세스를 최적화할 수 있는 다수의 단순한 수정들이 있다.

일부 응용 분야들에서, 매우 단순한 실시예는 단순한 임계값을 사용하여 국부적 마스킹 기회를 결정하고, 그 후, 보조 데이터를 임계값을 초과하는 지점이나, 상기 임계값을 초과하는 지점의 인근에 있는 다른 지점의 LSB내에 보조 데이터를 부호화할 수 있다. 이런 변화는 극도로 단순하지만, 종래 기술의 LSB 방법에 비해 지각성을 감소시킨다. 다른 실시예들과 마찬가지로, 1은 값의 변화가 상기 지점을 검출 기준으로부터 벗어나게 하지 않는 것을 보증한다. 이 경우에, 1은 변화가 상기 데이터를 임계값 미만으로 떨어지게 하는 곳의 삽입을 단순히 스킵하고, 데이터 지점이 검색 위상으로 스킵되도록 임계값에 대한 데이터 지점의 현재값을 변화시킬 수 있다.

공격이나 노이즈에 대한 견고성을 향상시키기 위하여, 하기의 변화들이 이루어질 수 있다(공격은 원본 데이터의 지각 수준을 열화시키지 않는 상태로 조합된 신호로부터 보조 정보를 제거하려는 인적 또는 기계적 시도로서 정의된다).

동적 임계값을 사용하는 것은 보조 정보를 제거하는 것을 더 어렵게 만든다. 동적 임계값의 예는 오프셋 사인 파형이다. 동적 임계값을 사용할 때, dS는, 상기 프로세스가 이웃 지점들 사이의 편차들의 분포를 변화시키지 않도록, 즉, 통계학적으로 발견되지 않고, 그래서 공격자가 이 데이터를 사용하여 임계값을 발견할 수 없도록 2^b에 근접하게 작아야만 한다.

또한, 1은 dS가 2^b 보다 클 때 공격자가 DC 전환(DC shift)을 사용하여 통계학적 갭들을 사용하여 임계값을 발견하도록 할 수 있다. DC 전환은 제 1 보다 제 2 실시예에 대해 보다 영향력 있는 공격이지만, 임계값이 검출 기준 중 하나일 때 제 1 실시예에도 영향을 미칠 수 있다.

(공격 저항 방법을 하기에 추가로 설명한다)

상기 프로세스는 노이즈에 대한 보다 양호한 견고성을 위하여 피크들 및 임계값 교차점들에 대하여 보다 범용적인 정의들을 사용할 수 있다. 더욱 명확하게 말하면, 피크 또는 임계값 교차점 정의는 각 측면 상의 더 많은 지점들을 포함하도록 사용될 수 있다.

마지막으로, 상기 프로세스는 견고성을 향상시키기 위하여 보조 정보의 소정 형태의 에러 보정을 사용할 수 있다.

데이터율을 향상시키기 위하여, 하기의 변화들이 이루어질 수 있다. 노이즈에 대한 견고성이 필요없는 경우에, 보조 정보는 N-비트 워드들 사이에 여분의 동기 펄스들을 포함할 필요가 없다. 그 외에도, 음방향 진행 피크들 및/또는 더 많은 임계값들이 비트율을 개선하도록 사용될 수 있다. 마지막으로, 상기 프로세스는 더 많은 정보를 부호화하도록 제 2비트의 조절에 이진 시스템 이상을 사용할 수 있다. 그러나 결과는 공격에 대하여 견고성이 덜하거나 보다 지각되기 쉬워진다.

양 및 음 피크들 및/또는 다양한 임계값들에 대해 조합된 상이한 보조 정보에 대해 인털레스팅 트위스트가 이루어질 수 있다. 그 외에도, 스테레오 파일들에서, 채널은 독립적으로 부호화될 수 있거나, 부호화가 좌우 채널들 사이에서 이동하는 연속적인 지점들을 가진 채널들 사이에서 이동될 수 있다.

보조 정보를 조합하는 것이 삽입 지점에 큰 값의 변화를 유발하는 경우에, 삽입 지점 이후의 데이터 지점을 삽입 지점의 값을 향해 이동시키는, 지각 수준을 증가시키는 변화가 이루어질 수 있다.

상술한 바와 같이, 데이터는 반드시 시간에 대한 것일 필요는 없다. 예로서, 데이터는 주파수에 대한 크기를 나타낼 수 있다. 그 외에도, 상기 데이터는 시간에 대한 특정 주파수의 크기로서 보여질 수 있다. 데이터율 향상을 위해 모든 주파수들이 포함될 수 있다. 달리 말해서, 삽입은 스펙트럼 또는 스펙트럼 사진 내에 수행될 수 있다. 본 프로세스 및 대응 장치를 사용하기 위해서, 1은 주어진 데이터의 포맷을 변화시키지 않는 것이 바람직하다.

예로서, MPEG 압축 데이터 같은 비트 감축 데이터를 고려한다. MPEG 압축 데이터는 스케일링 인자들과 주파수 계수들을 나타내는 일련의 데이터 지점들을 포함한다. 보조 데이터는 예로서 상술한 두 개의 특정 실시예들 중 하나를 사용하여 일련의 MPEG 데이터 지점들 내에 삽입될 수 있다. 특정 제 1 실시예를 사용할 때, 1은 피크를 증가시키거나, 특히, 스케일링 인자들과 함께 취급될 때 양자화 에러가 MPEG 데이터 내에서 증가되지 않도록, 피크 이후의 지점을 감소시키는 대신 그 LSB를 그 텀(term)만이 증가되도록 수정하는 것이 될 수 있다. 숙련자들은 시간 프레임들로 분할된 MPEG 데이터 같은 데이터를 사용할 때, 예로서, 스케일링 인자들 또는 연속하는 프레임들로부터의 주파수 계수들 및 하나의 프레임 내의 상이한 주파수들의 계수들과 스케일링 인자들을 나타내는 데이터 지점들을 사용할 수 있다는 것을 알 것이다. 예로서, 연속하는 프레임들 내의 특정 주파수에 대한 계수들이 일련의 연속하는 데이터 지점들로서 간주될 수 있고, 이들 데이터 지점들이 상기 일련의 데이터 지점들 내의 데이터 삽입 지점을 결정하도록 상술한 실시예들 중 하나에 따라 분석될 수 있다. 선택적인 예에서, 프레임 내의 상이한 주파수들에 대한 주파수 계수들 또는 스케일링 인자들을 나타내는 일련의 데이터 지점들이 데이터 삽입 지점을 결정하기 위해 상술한 특정 제 1 및 제 2 실시예들에 따라 분석될 수 있다.

<u>활용예들</u>

하기에 이해를 돕기 위해 예시적 알고리즘의 활용예를 설명한다. 이 리스트는 완전하지 않으며, 단지 본 기술의 유용성을 강조하기 위한 것이다. 그 외에도, 하기에 주어진 응용 분야들은 사용된 부호화의 특정 형태에 의존하지 않으며, 소정의 다른 형태의 디지털 워터마킹, 스테가노그래피 또는 데이터 은폐가 선택적으로 사용될 수 있다.

상기 프로세스는 저작권 정보를 삽입하도록 사용될 수 있다. 이 정보는 데이터가 복사될 수 있는 지를 결정하기 위한 코드를 포함할 수 있다. CD 라이터들 같은 복사 장치들 은 삽입 데이터를 해석하고 복사를 중지할 수 있는 저가의 집적 회로를 포함할 수 있다.

그 외에도, 저자 또는 예술가들의 이름 및 회사가 삽입될 수 있다. 이 이용에서, 보조 정보는 작고, 각 복제된 보조 정보들 사이에 동기 펄스들을 구비한 상태로 계속 반복될 수 있다. 선택적으로, 복사 코드가 제 1 실시예를 사용하여 삽입될 수 있고, 제 2 실시에를 사용하여 제작자의 이름과 회사가 삽입될 수 있다(즉, 복수의 삽입 데이터가 하나의 저작품 내에 양립할 수 있다).

이런 기술은 추가의 정보를 보내도록 사용될 수 있다. 본 정보는 8비트 "워드들"(32비트로서 형성된 디지털 워드들을 포함하지 않음) 및 필요에 따라, 이들 워드들 사이에 동기 펄스를 가지는 ASCII 또는 ANSI로 전송될 수 있다. 상기 정보는 비밀 메시지, 노래의 가사 또는 예술작품이 설명일 수 있다. 가사에 대하여, 이는 가라오케 기계들 및 CD나 DVD 재생 장치들에 대해 유용할 수 있다.

디지털 압축

은폐 데이터와 디지털 압축(동적 범위가 아닌 비트율 감축)이 가진 주된 문제는 데이터 은폐 프로세스가 압축으로서 공지된 디지털 비트율 감축 기술들(다시 말해, 부호화 및 복호화)과 상충된다는 것이다. 이 상충성은, 데이터 은폐의 목적이 상기 데이터를 최소한으로 지각되게 하는 것이고, 압축의 목적이 최소한으로 지각 가능한 부분을 제거하는 것이기 때문에 발생한다.

이를 위해, 도 10A 및 도 10B는 소정 지점에서 데이터가 반드시 압축되어야 하는 경우에 데이터 은폐를 위한 예시적 프로세스를 예시하고 있다. 예로서, 이는 데이터 전송 도중에 발생할 수 있다.

도 10A에서, 보조 정보가 박스(600)에 도시된 바와 같이 상술한 프로세스 또는 소정의 다른 방법을 사용하여 비압축 데이터 내에 삽입된다. 그 후, 상기 데이터가 압축될 필요가 있을 때, 보조 정보는 상술한 또는 다른 적절한 방법을 경유하여 검색되며, 상술한 프로세스 또는 다른 소정의 방법으로 압축된 데이터 내에 다시 삽입된다. 이는 박스(610)에 도시되어 있다. 압축 및 비압축 데이터 내에 데이터를 은폐하기 위한 알고리즘은 동일한 알고리즘일 수 있으며, 단지 상이한 원본 데이터를 사용하는 것만 다르다. 또는, 이들은 상이한 것들일 수 있다.

도 10B에서, 상술한 방법 및 다른 방법에 의해 압축 데이터로부터 보조 정보가 검색되고, 상기 데이터가 압축 해제되며, 박스(620)에 도시된 바와 같이 보조 정보가 비압축 데이터 내에 삽입되게 된다. 마지막으로, 필요시, 보조 정보는 박스(630)에 도시된 바와 같이, 상술한 또는 다른 방법을 사용하여 데이터로부터 검색될 수 있다. 또, 상기 압축 데이터 및 비압축 데이터 내에 데이터를 은폐하기 위한 알고리즘은, 단지 상이한 원본 데이터를 사용하는 것만 상이한 서로 동일한 알고리즘이거나, 서로 다른 알고리즘일 수 있다.

장치

상술한 바와 같이, 도 2는 세부적 프로세스가 논리 프로세서와 저장 유닛(18)을 경유하여 실행될 수 있다는 것을 예시하고 있다. 도 12는 디지털 프로세서(1200)와 디지털 메모리(1210)로 수행하는 것을 도시한다. 디지털 프로세서(1200)는 디지털 신호 프로세서(DSP), 범용 중앙 처리 유닛(CPU) 또는 매체 프로세서들을 포함하는 특정된 CPU와 그 등가의 것들로서 정의될 수 있다. 유용한 DSP 칩은 텍사스 인스트루먼츠 TMS320 제품 라인 중 하나이다. CPU는 인텔 펜티엄 라인 또는 모토롤라/IBM의 파워 PC 제품 라인 중 하나를 포함할 수 있다. 상기 디자인은 도 5 내지 도 9의 의사코드로 제공된 작업의 상태와 친숙한 사람들을 위한 것이다.

그 외에도, 도 13에 도시된 바와 같이, 본 기술 분야의 상태에 친숙한 사람은 독립적이거나, 특정 이용 집적 회로 내에 있는 아날로그 및 디지털 회로로 상기 프로세스를 수행할 수 있다. 상기 아날로그 및 디지털 회로는 하기의 디바이스들 중 소정의 조합을 포함할 수 있다. 상기 디바이스들은 디지털 아날로그 변환기(D/A), 비교기, 샘플 및 보유 회로들, 지연 소자들,

아날로그 디지털 변환기(A/D 및 프로그래머블 로직 컨트롤러들(PLC)이다. 프로그래머블 로직 어레이들(PLD들)도 마찬가지로 사용될 수 있다. 본 기술분야에 친숙한 사람들은 상술한 설명과 도 5 내지 도 9의 의사 코드로 상기 회로를 용이하게 설계할 수 있다.

도 11a 및 도 11b는 논리 프로세서와, 저장 유닛을 도시하고 있으며, 이들은 일반적으로 삽입 장치(700)와 검색 장치(770)를 포함한다. 삽입 장치(700)는 하기와 같은 것들을 포함한다. 원본 데이터(720) 판독용 데이터 판독기(710) 및 보조 데이터(730). 데이터 지점들을 공지된 값들 또는 다른 데이터 지점들과 비교하기 위한 장치 및 회로인 비교기(740). 영구적 또는 일시적 저장 매체로 조합된 데이터(760)를 기록하기 위한 데이터 기록기(750).

검색 장치(770)는 하기의 것들을 포함한다. 조합 데이터를 판독하기 위한 데이터 판독기(715). 데이터 판독기(715)는 삽입 데이터 판독기(710)와 동일할 수 있지만, 또한, 상이할 수도 있다. 비교기(745), 즉, 공지된 값들을 가진 데이터 지점들 또는 다른 데이터 지점들을 비교하고, 필요시, 보조 비트 또는 비트들을 생성하기 위한 회로 또는 디바이스. 또, 비교기(745)는 삽입 비교기(740)와 동일하거나 상이할 수 있다. 보조 정보가 메모리로부터 취해질 수 있거나, 대응하는 이용을 위해 단지 디스플레이만 될 수 있기 때문에, 데이터 기록기는 항상 필수적인 것은 아니다.

분파들(ramifications) 및 범주

상술한 바들로부터 알 수 있는 바와 같이, 그리고, CD 품질 오디오로 상기 프로세스를 시험함으로써 알 수 있는 바와 같이, 보조 정보를 원본 데이터 내에 은폐하기 위한 상술한 프로세스들 및 장치들은 효과적이며, 지각되지 않는 구성들을 가진다. 이들 장점들은 주로, 마스킹이 보조 데이터의 지각 수준을 차단 또는 감소시킬 수 있도록, 신호를 주파수 영역으로 변환시킬 필요 없이 보조 데이터를 은폐시킬 위치를 찾는 것으로 인한 것이다.

손상 및 공격 저항성

언급한 바와 같이, 본 명세서에 기술된 기술의 다른 양상은 손상 및 공격에 대한 삽입 데이터의 저항성을 향상시키기 위한 방법에 관한 것이다. 설명의 편의를 위해서, "공격"이라는 용어가 본 명세서에서 사용되지만, 이는 삽입 데이터를 제거하기 위한 고의적인 노력과, 이런 데이터의 우연한 제거를 포함하는 의미이다. 공격은 복제를 포함할 수 있으며, 이는 하나의 데이터 세그먼트로부터 다른 곳으로 삽입 데이터를 복사 또는 재현하는 것으로서 정의된다. 또한, 공격은 "복사 불가"상태로부터 "복사 허용"상태로 같은 소정 영향을 미치기 위하여 삽입 데이터를 변화시키는 것으로 정의되는 변조를 포함한다.

하기에 설명된 기술은 삽입 데이터가 공격에 대해 보다 강해지도록, 삽입 데이터를 사용하는 방식을 설명하는 두 가지 예들(즉, 가능화 및 등록 프로세스)을 설명한다. 그 외에도, 복제 또는 수정에 대한 삽입 데이터의 견고성을 향상시키는 동적 로킹 및 언로킹을 포함하는 예들이 설명되어 있다.

제 1 실시예는 복사, 재생 또는 다른 랜더링 같은 작용을 가능하게 하도록 삽입 데이터를 사용하는 것을 포함하는 가능화 프로세스를 활용한다. 따라서, 삽입 데이터가 공격에 의해 제거되는 경우에, 원본 데이터가 사용불가의 상태가 되기 때문에 최종 사용자는 아무것도 얻을 수 없다. 삽입 데이터가 복제 및 수정에 대해 견고할 때 이 프로세스가 더욱 양호해진다.

제 2 실시예는 기록 디바이스가 그 등록을 데이터 내에 삽입하는 등록 프로세스를 활용한다. 본 예에서, 기록 디바이스는 CD나 DVD 버너(burner) 같은 물리적 디바이스 또는 MP3나 AAC 부호화기 같은 가상 디바이스를 지칭할 수 있다. 이 등록 프로세스는 기록 디바이스들이 구입되었을 때 등록되는 것을 가정하여, 소정의 적법한 매체들이 원본 사용자들에게로 역추적될 수 있게 한다. 적어도, 적법한 매체는 특정 기록 디바이스의 구매 장소로 역추적될 수 있으며, 법률 행사에 양호한 출발점을 제공한다.

동적 로킹 및 언로킹 예들은 기존 또는 미래의 삽입 데이터 기술들의 견고성을 복제 및/또는 수정에 대해 개선한다. 동적 로킹은 예로서, 하기의 단계들 중 하나 또는 양자 모두를 포함함으로써, 삽입 데이터가 매체에 의존하게 한다. 첫 번째 단계는 매체에 의해 보조 정보를 수정하는 것을 포함한다. 두 번째 단계는 첫 번째 단계에서 수정된 것일 수 있는 보조 정보를 부호화하는 것을 포함한다. 부호화 기술은 RSA, DES 또는 소정의 적합한 알고리즘일 수 있다. 보조 정보의 동적 로킹 이후에, 이것이 원본 데이터 내에 삽입된다. 동적 로킹의 각 단계는 그 자체의 독립적 장점들을 제공한다. 그러나 양자 모두의 단계를 통합하는 것은 매체들 사이에서 전달, 수정 또는 생성될 수 없는 보조 정보를 형성한다.

동적 언로킹 프로세스는 각 특정 단계가 동적 로킹 프로세스에서 수행된 것으로 가정하여, 역방향 단계들을 수행한다. 상기 제 1 단계는 검색된 데이터를 복호화하는 것을 포함한다. 제 2 단계는 제 1 단계가 수행되었는지 아닌지에 따라서, 제 1 단계의 출력을 또는 검색된 데이터를 직접적으로 수정 해제(unmodify)되고, 그래서 원래의 보조 데이터를 생성하는 것을 포함한다.

가능화 및 동적 로킹 프로세스 및 장치들의 다섯 가지 예시적 활용들이 개략적으로 설명되었고, 프로세스들 및 장치의 이해를 돕기 위해 하기에 상세히 설명한다. 이들 활용들은 (1) 요청자의 재생 디바이스에 의해서만 재생되도록, 압축된 매체를 배포하는 것, (2) 삽입 데이터의 존재를 사용하여 일회 복사 액세스(copy-once access)를 지정하는 것, (3) DVD 매체의 보호, (4) 사진-카드 비준 및 (5) 안전하게 비밀 메시지들을 송신하는 것이다.

제 1 활용예에서, MP3 소프트웨어 플레이어를 가진 컴퓨터 같은 매체 재생 장치는 MP3 포맷의 노래 같은 매체를 다운로드하기 위해 인터넷 사이트에 접속한다. 상기 재생 장치는 그 고유 식별자를 인터넷 사이트로 송신하고, 그곳에서, 상기 식별자는 원본 데이터를 사용하여 수정하고, 결과물이 부호화된다. 그 후, 수정 및 부호화된 식별자가 원본 데이터에 삽입되며, 조합 데이터가 재생 장치로 다운로드된다. 매체 재생 장치는 조합 데이터로부터 식별자를 추출할 수 있으며, 이를 그 자체의 식별자와 비교한다. 이 식별자들이 동일하고, 날짜 제한 같은 소정의 추가 정보가 검증되는 경우에, 상기 재생 장치는 데이터를 재생한다. 조합 데이터가 상이한 식별자를 가진 두 번째 재생 장치로 복사되는 경우에, 두 번째 재생장치는 조합 데이터를 재생하지 못한다.

허가받지 않은 사람이 식별자를 결정하는 경우에, 그 후, 그는 다른 노래들 내에 이를 조합하여 그들을 그의 재생 장치상에서 재생할 수 있다. 식별자를 부호화함으로써, 허가되지 않은 사람은 조합 데이터로부터 보조 데이터를 추출해낼 수 있는 경우에도 식별자를 결정할 수 없다. 그 외에도, 프로세스가 원본 정보와 함께 보조 정보를 수정하는 것을 포함하지 않는 경우에도, 삽입 데이터는 매체들 사이에서 복사될 수 있다. 마지막으로, 부호화 키는 적절한 취급을 요구하며 식별자는 재생 장치 식별자 이외의 추가의 정보를 포함할 수 있다.

제 2 활용예는 고유 식별자 대신 "복사 불허", "1회 복사 허용, 복사본의 복사는 불허" 및 "무제한 복사 허용" 같은 소정 복사 코드를 포함한다. 기록기는 복사 코드를 검색하고, 코드에 의해 허가되지 않는 한 복사하지 않는다. 복사는 "일회 복사 허용" 코드를 포함하지 않거나, "복사 불허" 코드를 포함한다. 브로드캐스트 업자들을 위해서, 재생 장치와 브로드캐스트 유닛은 앞선(즉, 미리 규정된) 코드를 알거나, 브로드캐스트에 코드가 포함되어 있어야 한다.

제 3 활용예에서, 두 개의 접근 방식이 설명된다. 첫 번째 접근 방식에서, DVD 재생 장치는 원본 데이터 내에 삽입된 미리 규정된 식별자를 검색하지 못하면 DVD를 재생하지 않는다. 추가의 보안을 위해서, 식별자는 복사에 가용하지 않은 DVD의 섹션 내에 또는 중앙 데이터베이스에 위치된 키로 부호화될 수 있다. 두 번째 접근 방식에서, 식별자는 허용된 복사본들의 형성의 횟수를 제어할 수 있으며, 식별자가 존재하지 않는 경우에는 복사본들이 만들어지지 않는다. 또는, 두 가지 형태의 복사 관리 양자 모두를 위해 두 겹의 식별자들이 있을 수 있다.

제 4 활용예는 운전 면허증 또는 신용 카드 같은 식별 목적용으로 사용되는 사진에서와 같이, 사진 카드의 사진에 보안 데이터를 삽입하는 것을 포함한다. 사진 카드 판독기에서 검색된 정보가 중앙 데이터베이스의 것과 일치하지 않는 경우에, 상기 카드는 위조된 것으로 간주되며, 사용이 허가되지 않는다. 정보 및 키 교환은 반드시 보안적으로 전송되어야 한다.

제 5 활용예는 매체 내에 은폐된 비밀 정보의 안전한 송신을 허용한다. 대부분의 구경꾼은 비밀 메시지가 첨부된 것을 알지 못한다. 식별 데이터가 매체와 부호화에 의존할 때는, 발견되는 경우에도, 중간 개입자에 의해 판독, 수정 및/또는 다른 매체로 전달되지 않을 수 있다. 부호화, 대칭 또는 공개/비밀 키들의 다른 형태들이 소정의 보호 또는 삽입 데이터의 인증 생성을 위해 사용될 수 있다. 이 은폐된 정보는 수신 측의 사람 또는 장치가 작동을 수행하도록 할 수 있다.

이들 프로세스들을 위한 예시적 장치는 DSP 칩들, 호스트 CPU들 또는 통상적 아날로그 또는 디지털 회로일 수 있는 논리 프로세서와 메모리를 포함한다. 상기 구성 및 장치 코드는 암호 작성법과, 전기 공학에 대한 본 기술분야의 배경 기술과, 본 명세서에 기재된 내용을 참조하여 용이하게 설계될 수 있다.

상술한 바를 세부적으로 설명하기 이전에, 소정 정의들을 고려한다. 매체 또는 컨텐트는 오디오, 비디오, 정지 이미지, 상술한 것들의 조합들 및 다른 의미들과 관련된 형태들을 포함하며, 이들에만 제한되는 것은 아니다. 매체 및 컨텐트라는 용어는 서로 교체할 수 있게 사용되고 있다. 매체는 저장 매체를 의미하는 것이 아니다. 매체 또는 컨텐트 세그먼트는 노래, 노래의 일부, 영화, 영화의 일부, 사운드 트랙의 전체 또는 일부, 정지 이미지의 전체 또는 일부, 맛, 감촉, 냄새를 포함하며, 이들에만 제한되는 것은 아니다. 원본 데이터는 보호되지 않은 원시 데이터이다. 보조 정보는 원본 데이터 내에 삽입될 소

정의 데이터를 지칭한다. 도 21의 ID(140)는 보조 정보를 지칭하고 있고, 재생장치 ID, 허용 복사본의 수, 사용 시간 또는 날짜 제한들 및 저자, 저작권, 공급자, 노래 가사 또는 이미지 세부정보 같은 컨텐트 강화 정보를 포함할 수 있으며, 이들에만 제한되는 것은 아니다. 삽입 데이터는 실질적으로 원본 데이터 내에 삽입 데이터이다. 삽입 데이터는 삽입 프로세스에 사용된 변환에 의해 보조 데이터와는 다르다. 이 변환은 동적 로킹에 수반된 수정 프로세스 및/또는 부호화와, 비트 조작들, 펄스 폭 변조 또는 주파수 확장 변환 또는 의사 랜덤 노이즈 시퀀스 같은 삽입 프로세스를 포함할 수 있다. 조합 데이터는 삽입 데이터를 원본 데이터에 추가하는 것으로부터 초래된다. 공격에 대한 견고성은 그 주변에서 삽입 데이터가 제공 또는 방지되게 되는 게팅(getting)으로서 정의된다. 마지막으로, 저작권 침해자는 불법적으로 데이터를 얻으려고 하거나 보호된 디바이스를 사용하려고 하는 사람이다.

가능화 프로세스

도 14는 바람직한 가능화 프로세스를 예시하고 있다. 이 프로세스는 도 22에 도시된 바와 같은 논리 프로세서(900)와, 메모리(910)를 사용한다. 먼저, 박스(10)에 도시된 바와 같이, 프로세서(900)는 조합 데이터(5)로부터 보조 데이터를 검색하고, 이를 메모리(910)에 저장한다. 그 후, 프로세서(900)는 박스(20)에 도시된 바와 같이, 삽입 데이터가 소정 작용을 허용하는지 여부를 결정한다. 허용하는 경우에, 박스(30)에 도시된 바와 같이 소정 작업이 허용된다. 허용하지 않는 경우에, 박스(40)에 도시된 바와 같이 소정 작업이 불허된다.

등록 프로세스

도 15는 등록 프로세스를 예시하고 있다. 이 프로세스는 고유 등록 코드(305)를 각 기록 디바이스(300)에 할당하는 단계와, 박스(310)에 도시된 바와 같이 기록될 때, 상기 등록 코드(305)를 매체 내로 삽입하는 단계를 포함한다. 그 후, 불법 매체가 개방 시장(320) 내에서 발견되었을 때, 박스(330)에 도시된 바와 같이 등록 코드(305)를 경유하여 기록 장치의 소유자를 추적할 수 있다.

상기 프로세스는 기록 디바이스가 구매시 등록되는 점에서 총의 등록과 유사하다. 최소한, 불법 매체는 기록 디바이스 및 그 구매 장소로 역추적될 수 있고, 따라서, 법 집행을 돕는다.

이 기록 디바이스는 물리적 디바이스거나, 가상 디바이스일 수 있다. 물리적 디바이스는 CD 또는 DVD 버너를 포함할 수 있다. 가상 디바이스는 프로세서(900)와 메모리(910)를 사용하여, MP3 리퍼(ripper) 또는 AAC 부호기 같은 오디오를 디지털적으로 압축(비트율 감축)하는 소프트웨어 프로그램을 포함한다. 매체는 지각된 데이터를 의미하며 저장 매체가 아님을 상기한다.

동적 로킹

도 16은 동적 로킹이 보조 데이터의 복제를 방지하는 방식을 도시하고 있다. 복제는, 컨텐트 사이의 삽입 데이터를 복사하고, 삽입 정보를 검색하고, 이를 상이한 컨텐트가 인증을 나타내도록 상이한 컨텐트 내로 재삽입하는 것들을 양쪽 비트-대-비트에 대하여 차단한다.

더욱 명확하게 말하면, 단지 보조 정보를 수정하였을 때, 저작권 침해자는 삽입 데이터를 정확하게 수정 해제 및 재수정하는 방식을 찾아내지 않고서는 삽입 데이터를 하나의 매체 세그먼트로부터 다른 것으로 이동시킬 수 없다. 단지 보조 정보를 부호화할 때, 저작권 침해자는 보조 정보를 얻을 수 없다. 저작권 침해자는 삽입 데이터를 검색할 수 있지만, 부호화되어 있기 때문에 판독하지는 못한다. 양자 모두의 단계들이 사용되었을 때, 보조 정보는 하나의 매체 세그먼트로부터 다른 것으로 옮겨질 수 없다. 이것이 직접적으로 이동되게 되면, 동적 로킹의 변형 단계는 새로운 매체 내의 삽입 데이터를 부정확하게 수정 해제되게 하며, 그 이유는 검색된 데이터를 수정 해제하는 데 사용된 새로운 매체 세그먼트 내의 값들이 데이터가 수정된 원본 매체 내의 값들과 일치하지 않기 때문이다. 저작권 침해자가 삽입 데이터를 수정 해제 및 재수정하려하는 경우에(이 세부 단계들이 공지되어 있기 때문에), 새로운 매체 세그먼트로 이를 이동시키기 위해서 그/그녀는 반드시 데이터를 복호화하기 위한 키가 있어야만 한다.

도 17은 익스클루시브-오어 함수(XOR)를 위한 입력 및 출력을 나타내고 있다. XOR은 그 자체가 가역적이며, 극도로 효율적이다.

도 18a는 동적 로킹 및 삽입 프로세스의 개요를 도시하고 있다. 전체 프로세스는 세 개의 단계들을 포함하지만, 처음의 두 단계들, 즉, 동적 로킹의 단계들 중 어느 한쪽(양자 모두는 아님)은 스킵될 수 있다. 그러나 동적 로킹 단계들 양자 모두가

수행되었을 때, 데이터 복제의 어려움이 증가된다. 그 외에도, 마지막 두 개의 단계들의 순서는 바뀔 수 있다. 이 순서 전환은 일반적으로 다른 컨텐트 보호를 목적으로 삽입 데이터를 포함하는 컨텐트가 부호화되었을 때, 또는, 수정 단계가 수정 해제를 위해 키를 요구하는 것과 같은 양호한 특성들 중 일부를 가질 때 양호하다.

제 1 단계에서, 박스(600)에서, 삽입될 보조 데이터(d)가 원본 컨텐트(c)에 기초하여 수정된다. 이 단계는 삽입 데이터가 컨텐트 사이의 비트-대-비트 복사될 수 없도록 원본 컨텐트에 의존하도록 보조 데이터를 수정시키게 설계된다. 선택된 컨텐트 비트들은 컨텐트에 중요한 것이어야 하며, 그래서, 새로운 컨텐트로 바뀌어져서 이들이 인증을 나타내게 해서는 안된다. 바람직한 함수는 익스클루시브-오어(XOR) 연산자이며, 그 이유는 이 함수가 그 자체로 가역적이며, 디지털 프로세서들 상에서 효율적으로 수행되기 때문이다.

제 2 단계에서, 박스(610)에서, 원본 보조 비트들이 삽입 데이터로부터 획득될 수 없도록 수정된 데이터가 부호화된다. 따라서, 원본 보조 비트들이 다른 컨텐트에 재삽입되어 다른 컨텐트가 인증을 나타나게 할 수 없다. 보조 데이터가 부호화되기 이전에 원본 컨텐트에 의해 수정되지 않는 경우에, 이는 원본 데이터로부터 비트-대-비트로 새로운 컨텐트로 복사되어, 새로운 컨텐트가 인증을 나타낼 수 있다. DES 및 RAS를 포함하는, 소정의 현존하거나 미래에 나오게 될 부호화 방법들이 공지된 키 관리 방법들과 함께 사용될 수 있으며, 이모든 것은 종래 기술에 잘 설명되어 있다.

제 3 단계에서, 박스(620)에서, 부호화 및 수정된(동적으로 로킹됨으로 표시되어 있음) 보조 데이터가 원본 컨텐트 내로 삽입된다.

도 18b는 보조 데이터의 검색 및 동적 언로킹에 사용되는 프로세스의 개요가 도시되어 있다. 전체 프로세스는 세 개의 단계들을 포함하며, 각 단계는 데이터 삽입시 대응하는 단계들이 수행된 경우에만 수행될 수 있다. 그 외에도, 삽입시 최종 두 단계들의 순서가 뒤바뀐 경우에, 검색 프로세스 동안 이들 두 개의 대응하는 단계들도 뒤바뀌어야만 한다.

제 1 단계에서, 박스(630)에서, 삽입 데이터가 컨텐트로부터 검색된다. 이때, 삽입 데이터는 부호화 및 수정된 보조 데이터(동적 로킹 단계들 양자 모두가 수행된 것으로 가정)로 구성되어 있다. 제 2 단계에서, 박스(640)에서, 검색된 데이터가 복호화된다. 제 3 단계에서, 박스(650)에서, 제 2 단계의 출력이 수정 해제된다. 결과는 원본 보조 데이터이다.

그 외에도, 동적 로킹 및 언로킹은 상관 데이터(correlated data)를 사용할 수 있다. 상관 데이터는 노래 가사 또는 사진 식별카드 내의 인물의 주소 같은 정보를 포함할 수 있다.

도 19는 데이터가 지각되지 않도록 삽입되었을 때(즉, 워터마킹)의 동적 로킹 및 언로킹의 수정 부분의 몇 가지 예시적 실행방법을 도시하고 있다. 비록, 수정부만이 도 19에 도시되어 있지만, 필요에 따라, 수정된 보조 정보는 삽입되기 이전에 부호화될 수 있고, 검색된 이후(그러나, 수정 해제되기 이전에)에 복호화될 수 있다. 그 외에도, 보조 정보의 수정은 스킵될 수 있고, 보조 정보는 삽입 이전에 단지 부호화만 될 수 있으며, 검색된 이후에 복호화만 될 수 있다. 암호 작성 프로세스는 본 기술분야의 숙련자들은 그 실행 방법을 용이하게 이해할 수 있기 때문에 상세히 설명하지 않는다.

도 19a는 상술한 장치에 적용될 때의 동적 로킹 및 언로킹을 도시하고 있다. 동적 로킹을 위해서, 박스(200)에서 피크값 또는 임계 교차점 값이 익스클루시브-오어(XOR) 계산에 사용되어 다음 N 보조 정보를 수정하게 되며, 여기서, N은 데이터 내의 샘플당 비트들의 수(CD 오디오에 대하여 16 비트들 같이)이다. 그 후, 이들 수정된 보조 정보의 N 비트들은 편차(Δ)의 국부적으로 마스킹된 비트 조작을 사용하여 선택적으로 부호화 및 삽입(예로서, 상술한 방법들에 의해)된다. 상기 프로세스는 N 피크들의 다음 그룹에 대해서 반복되는 등의 방식으로 전체 수정된 보조 정보들이 삽입되거나, 모든 원본 데이터들이 사용될 때까지, 수정된 보조 정보가 반복적으로 삽입된다.

삽입 데이터는 상술한 프로세스를 사용하여 검색되고, 복호(필요시) 및 수정 해제될 수 있다. 수정해제 프로세스는 수정 프로세스의 역순이다. XOR 함수가 그 자체로 가역적이기 때문에, 복호된 보조 정보 및 조합 데이터의 피크값들은 XOR 함수에 적용된다. 이들이 삽입 프로세스 동안 수정되지 않았기 때문에, 피크 값들은 원본 데이터의 그것과 동일하다는 것이 중요하다.

예로서, CD 오디오를 사용할 때, N은 16 비트들이다. 따라서, 본 예에서, 보조 정보의 첫음 16 비트들이 XOR을 사용하여 제 1 피크값에 의해 수정된다. 그 후, 이들 수정된 보조 정보 비트들은 선택적으로 부호화되고, 현재 피크 이후의 데이터 지점 및 다음 15 피크들의 데이터 지점 내에 삽입된다. 이 프로세스는 후속하는 16 피크들과 보조 정보 비트들의 그룹에 대해 반복되고, 모든 데이터가 삽입되거나 원본 데이터 모두가 사용될 때까지 계속된다. 수정 및 선택적으로 부호화된 보조 정보는 모든 비트들이 삽입된 이후에 보조 정보의 첫 번째 16 비트들로 상기 프로세스를 다시 시작함으로써, 데이터 내에 계속 반복적으로 삽입될 수 있다.

삽입 데이터는 검색, 복호화(부호화된 경우) 및 XOR 계산인, XOR 계산의 역으로 수정 해제될 수 있다. 따라서, 보조 정보의 처음 원본 16 비트들이 검색 및 복호화된 삽입 데이터와 제 1 피크 값으로 XOR 계산을 수행함으로써 얻어지게 된다. 검색 프로세스는 조합 및 삽입 데이터의 다음 16 피크들의 그룹에 대하여 계속되고, 전체 보조 정보가 발견되거나, 모든 조합 데이터들이 횡단될 때까지 계속된다.

검색 이후에 삽입 및 수정 해제를 위해 수정할 때 보조 정보내의 16 비트들의 그룹의 위치의 자취를 적절히 유지하는 것이 중요하다.

상술한 기술은 조합 데이터 내에 동기 펄스들을 가능하게 한다. 이들 동기 펄스들은 보조 정보를 보조 정보를 수정시키는데 사용되는 값과 정렬시키는데 사용될 수 있다. 예로서, 보조 정보를 수정하기 위해 사용된 피크 이후의 삽입 데이터들 대신, 동기 펄스가 삽입될 수 있고, 검색 프로세스 동안 재정렬을 위해 사용될 수 있다.

도 19b에는 본 명세서에서 참조하고 있는 잭 아리스 테크놀로직스의 잭 볼로스비즈에 의한 발명의 명칭이 "오디오 신호들내의 정보를 부호화 및 복호화하기 위한 방법 및 장치"인 특허 #5,774,452에 적용된 바와 같은 동적 로킹 및 언로킹을 도시한다. 본 경우에 대하여, 박스(220)에 도시된 펄스 폭 변조된(PWM) 비트 스트림의 삽입시 발생한 데이터 값들이 삽입 데이터를 수정 및 수정 해제하기 위해서 보조 정보를 가진 XOR 작업에 사용될 수 있다. 이 경우에, 몇 개의 데이터값들이 모든 보조 정보를 수정하기 위해 사용될 필요가 있다. 예로서, 16비트 데이터를 사용하여, 256 비트들의 보조 정보를 삽입하는 경우에, 동적 로킹 및 언로킹 프로세스는 앞선 16 원본 데이터 지점들을 사용하여 모든 보조 정보를 수정할 수 있다. 데이터가 그가 삽입될 때와 동일한 순서로 수신되는 한, 보조 정보를 수정하는데 사용된 데이터 값들이 앞서 삽입된 비트 스트림과 중첩되는 것은 문제가 되지 않는다. 상술한 것이 문제가 되는 구성을 찾게 되는 경우에는, 두 번째 삽입 비트 스트림을 스킵하고, 이를 조합 데이터 내에 스킵된 것으로 만들어 쉽게 처리될 수 있다.

도 19c는 의사 랜덤 노이즈(PN) 시퀀스에 기초한 삽입 데이터에 대한 동적 로킹 및 언로킹을 적용하는 개요를 도시하고 있다. 일 실시예에서, PN 시퀀스는 박스(250, 270)에 도시된 바와 같이 M 번째 데이터 지점을 스킵할 수 있으며, 여기서 M은 각 보조 정보 비트에 적용된 PN 시퀀스 세그먼트의 비트들의 길이와 데이터 내의 샘플당 비트 수(N)를 승산한 것과 동일한 값이다. 이 M^{th} 데이터 지점은 XOR 작업에서 보조 정보의 b 비트들과 함께 보조 정보를 수정하도록 사용될 수 있다. 예로서, 각 보조 정보 비트가 16비트 오디오 내의 PN 시퀀스의 1024비트 세그먼트로 삽입되어 있는 경우에, 보조 정보는 64비트 길이이다. 이때, 원본 데이터의 16384(M=1024비트 PN 세그먼트*16비트 오디오) 비트에 대한 PN 시퀀스 추가 이후에, 다른 원본 데이터 지점이 스킵되어 보조 정보를 수정한다. 이는 이들 세그먼트들 중 4(64비트 보조 정보/16비트 오디오)를 각 보조 정보에 삽입하데 소요하게 된다. 대등하게, 4개의 인접한 원본 데이터 지점들이 매 65536(M=1024비트 PN 세그먼트*16비트 오디오*4PN세그먼트들) 원본 데이터 지점들 마다 스킵될 수 있으며, 네 개의 PN 세그먼트들의 하나의 연속적인 스트림으로 전체 수정된 보조 정보를 삽입할 수 있다.

보조 정보의 수정 및 선택적 부호화는 스프레드 스펙트럼 기술에서 널리 공지되어 있는 바와 같이 원본 데이터에 PN 시퀀스가 추가되는 형태로 제어될 수 있다. 특히, 다수의 응용 분야에서, PN 시퀀스는 수정된 보조 정보에 의해 상 변환되거나(즉, 0의 스케일이면 PN 시퀀스의 음의 값을 추가, 1의 스케일이면, 양의 값을 추가), 보조 정보에 의해 단순히 조작될 수 있다. 검색되고나면, 수정된 보조 정보는 스킵된 데이터 지점으로 역 XOR 계산을 사용하여 수정 해제될 수 있다.

PN 시퀀스의 다른 실시예는 보조 정보가 아닌 PN 시퀀스의 다음 N 비트들을 수정시키기 위해서 스킵된 데이터 지점을 사용하는 것이다. 하나의 지점이 스킵되는 경우에, 수정된 PN 비트들의 수(M)는 데이터 내의 비트들의 수인 N과 동일해져야 한다. 두 개의 지점들이 스킵되는 경우에, M은 2*N과 동일해져야 하는 등이다. XOR 계산을 사용하여 PN 시퀀스를 수정하는 것과, 선택적으로 부호화하는 것은 하나의 방식이다. 그러나 이는 PN 시퀀스의 임의성을 감소시킬 수 있으며, 다른 수정 함수들이 임의성을 유지하는데 사용될 수 있다. 마지막으로, 수정 및 선택적으로 부호화된 PN 시퀀스는 매체 데이터 내에 삽입되고, 삽입 데이터를 검색하는데 사용된다.

마지막으로, 동적 로킹의 실행 방법에서, 이는 원본 데이터 내에 보조 정보를 배치하는 위치를 결정하기 위해, 가능하게는, 주파수 영역으로 변환된 이후에, PN 시퀀스들을 사용하는 삽입 방법에 적용된다. 이런 방법은 본 명세서에서 참조하고 있는 다이스 컴퍼니의 마크 쿠프만과 스코트 모스코위츠에 의한 발명의 명칭이 "스테가노그래픽 방법 및 장치"인 특허 #5,613,004 및 #5,687,236과, AT&T 랩스의 특허출원 기술인 EP889471(래시 J. 퀘겐부시, SR. 레이브만 AR, 셔어 D., 신더 JH의 1998년 "워터마킹을 지각적 부호화와 조합하는 방법" ICASSP'98 시에틀, 워싱턴)에 세부적으로 기재되어 있다. 이들 방법들에 대하여, 데이터 삽입에 사용되는 PN 시퀀스는 N 개 이상의 연속적 삽입 비트들을 요구하지 않으며, 비삽입 비트로 시작하고, 여기서, N은 또한 원본 데이터 내의 샘플당 비트들의 수이다. 그 후, 제 1 삽입 비트 이전의 인접한 원본

데이터 지점들이 보조 정보의 다음 N 비트들을 수정한다. 이 프로세스는 모든 원본 데이터들이 삽입될 때까지, 수정된 보조 정보가 반복적으로 삽입되도록 반복될 수 있다. 예로서, 저주파수로부터 고주파수로의 주파수 영역에 16비트 데이터와 32비트 보조 데이터를 삽입할 때, 제 1 삽입 비트 바로 아래의 주파수 빈(frequency bin) 내의 비삽입 비트가 다음 16 보조 정보 비트들을 수정시키도록 사용된다. 그 후, 17번째 삽입 비트 바로 아래의 주파수 빈내의 비삽입 비트는 다음 16 보조 정보 비트들을 수정시키도록 사용된다. 다음에, 33번째 삽입 비트 바로 아래의 주파수 빈내의 비삽입 비트는 첫 번째 16 보조 정보 비트들을 수정시키도록 사용되는 등이다.

동일한 방식에서, PN 시퀀스는 매 다른 또는 k 번째(여기서 k< 원본 데이터 내의 샘플당 비트수 N) 데이터 지점에 적용될 수 있으며, 그래서, PN 시퀀스에 어떠한 제한도 적용될 필요가 없다. 상기 프로세스는 N번째 삽입 비트 다음에 비삽입 비트를 갖게 되는 것을 보증하며, 이전 방법과 동일한 형태로 실행된다.

PN 시퀀스들을 사용한 동적 로킹 방법들에 대해서, 동적 언로킹 프로세스는 역순이며, 본 기술분야의 숙련자들은 상술한 바에 따라 명확히 알 수 있을 것이다.

도 20은 컨텐트가 아닌 헤더 내에 삽입 데이터에 종적 로킹 및 언로킹을 적용하는 방법을 예시하고 있다. 도 20a는 동적 로킹 프로세스를 위한 의사 코드를 도시하고 있다. 일반적으로, 길이가 L인 보조 데이터 비트들은 로킹되고, 컨텐트의 프레임들의 헤더 내에 배치되고, 반복적으로 삽입된다.

더욱 명확하게 말하면, 도 20a의 프로세스는 컨텐트 비트들(박스 700)과 보조 데이터 비트들(박스 705)의 시작에서 시작된다. 그 후, L 보조 데이터 비트들이 XOR 또는 적용가능한 함수를 사용하여 컨텐트의 L 비트들과 함께 수정되는 것에 의해 로킹 및/또는 부호화(735)된다. 이들 L 컨텐트 비트들은 파일 포맷 및 컨텐트 중 어느 한쪽 또는 양자 모두에 중요한 것이어야 하며, 그래서, 이를 교란시키지 않고 다른 매체 세그먼트 내에 이들이 복제될 수 없어야 한다. 다음에, 로킹된 보조 데이터의 M 비트들은 프레임 헤더 내에 삽입된다(박스 710). 이들 M 비트는 L 보다 작아야 하며, L이 M에 의해 나눠질 수 있고, 그래서, L 비트들이 L/M 프레임 헤더들 내에 삽입되는 것이 바람직하다. L이 M으로 나눠질 수 없는 경우에, 본 기술분야의 숙련자들은 용이하게 오프셋을 취급할 수 있을 것이다. 그 후, 더 많은 프레임이 존재하는지를 알기 위해 컨텐트가 점검된다(박스 715). 어떠한 컨텐트 프레임도 남지 않은 경우에, 프로세스는 완료된다(박스 730). 컨텐트 프레임들이 남아있는 경우에, 보조 데이터는 소정의 앞서 수정된 비트들이 존재하는지를 찾도록 점검된다(박스 720). 앞서 수정된 보조 비트들이 남아있는 경우에, 다음 프레임이 판독되고(박스 725), 상기 프로세스는 박스(710)에서 계속된다. 어떠한 앞서 수정된 보조 비트들도 남아있지 않은 경우에, 다음 컨텐트 프레임이 판독되고(박스 740), 보조 데이터가 비트 0에서 재시작되며(박스 705), 프로세스는 박스(710)에서 계속된다.

이 프로세스는 설명의 용이성을 위해, 보조 정보의 길이가 L이고, L 충분히 짧다는 것을 가정한다. 매우 큰 수의 보조 비트들이 있는 경우에, 그들을 길이 L의 세그먼트들로 분할하고, 각각 제 1 보조 비트에서 시작하는 대신, k 번째 세그먼트에서 시작할 수 있다는 것은 명백하다. 이를 위해서, 보조 비트들은 데이터 내에 삽입되고, 길이 L의 세그먼트들로 분할되며, 각 세그먼트가 L/M 프레임 헤더들 내에 삽입된다.

공격에 대한 견고성을 증가시키기 위해서, 의사 랜덤 노이즈(PN) 비트 시퀀스가 사용될 수 있고, 1의 대응하는 PN 비트값을 가진 첫 번째 N 개의 중요한 컨텐트 비트들이 보조 정보를 수정시키기 위해 사용될 수 있다.

선택적으로, 각 프레임에 M 로킹된 보조 데이터를 삽입할 때, 매 L/M 프레임들 마다 L 비트들 대신 각 프레임 내의 첫 번째 중요한 M 컨텐트 비트들만이 XOR 계산에 사용된다. 이 경우에, 보조 데이터 비트들은 특히, 도 20a의 박스(725, 710) 사이에서 각 프레임 내에서 수정된다. 또, PN 시퀀스는 원본 오디오의 M 비트들이 사용되는 것을 랜덤화하도록 사용될 수 있다. 새로운 컨텐트 내의 오류 보정이 변화될 필요가 있는 모든 컨텐트 비트들을 수선하여, 보조 데이터의 비트-대-비트 전달이 새로운 컨텐트가 인증을 나타내도록 만들 수 없도록 충분히 M이 커야만 한다는 것이 중요하다. M의 값은 프레임 크기 및 소정 비트율에 의존한다.

특히, 각각 본원에 참조로서 관련되는 MPEG 1 및 2 명세들, ISO 11172-3 및 ISO 13818-7을 포함하는 MPEG 2 명세에 열거된 바와 같은 Layer III(MP3) 또는 AAC 오디오와 같은 MPEG 데이터와 같은 압축된 컨텐트를 사용할 때, 프레임들 및 헤더 비트들은 미리 결정된다. 따라서, 비공개의, 저작권이 있는 또는 부수적인 비트들이 데이터를 삽입하는데 사용될 수 있다. 원시 PCM 오디오, 데이터베이스 또는 소프트웨어 응용들과 같은 미리 결정된 프레임들이 없는 컨텐트를 사용할 때, 프레임들은 간단하게 형성될 수 있다. 예를 들면, 컨텐트는 삽입 데이터에 대한 헤더 비트들을 갖는 1024비트 프레임들로 임의적으로 분할될 수 있다.

선택적으로, 로킹된 보조 데이터는 완성 파일을 위한 헤더로서 규정된 글로벌 헤더에만 배치될 수 있다. 상기 두 개의 경우는 파일 전체를 통해 데이터를 삽입하는 것보다 덜 안전하다. 비트들이 보다 많다는 것은 데이터가 난폭한 힘에 의한 공격에 더욱 견고성을 갖는다는 것을 의미한다. 브로드캐스트 컨텐트에 있어서, 데이터는 상술한 바와 같이 컨텐트 전체를 통해 삽입되어야 하므로, 지각 디바이스 또는 사람은 보조 정보를 수신할 수 있으며, 따라서 브로드캐스트 내의 임의의 지점으로부터 응답할 수 있다.

도 20b는 도 20a에 삽입 보조 데이터를 위한 동적 언로킹 프로세스 및 복구를 위한 의사 코드를 도시한다. 일반적으로, 보조 데이터 비트들은 반복적인 방식으로 컨텐트 프레임들의 헤더로부터 판독하여 언로킹함으로써 복구된다.

구체적으로는, 도 20b의 프로세스는 컨텐트 비트들(박스 750) 및 보조 데이터 비트들(박스 755)에서 개시된다. 다음, 도 22의 메모리(910)에서와 같이, N 컨텐트 비트들이 저장되므로, 상기 비트들은 다음 N 검색된 보조 데이터를 언로킹하는데 사용될 수 있다(박스 785). 다음, M 비트들의 로킹된 보조 데이터는 프레임 헤더(박스 760)로부터 판독된다. 다음, 상기 컨텐트는 기존 프레임들에 대해 검사된다(박스 765). 컨텐트 프레임들이 남아있지 않으면, 프로세스는 종료된다(박스 780). 컨텐트 프레임들이 남아 있으면, 보조 데이터 비트들이 존재하는지를 확인하기 위해 검사된다(박스 770). 보조 비트들이 남아있지 않으면, 다음 프레임이 판독되고(박스 775), 프로세스는 박스(760)에서 계속된다. 보조 비트들이 남아있지 않으면, 검색된 보조 데이터는 언로킹되며(박스 790), 다음 프레임이 판독되며(박스 795), 보조 데이터는 비트 0에서 재개시되며(박스 755), 다른 N 컨텐트 비트들이 저장되며(박스 785), 프로세스는 박스(760)에서 계속된다.

본 예에서, 검색된 삽입 데이터(박스 790)를 언로킹하는 것은 박스(785)에 저장된 N 컨텐트 비트들 및 최종 N 복구된 삽입 데이터 비트들에 XOR 연산(왜냐하면, 그 자신의 역이기 때문이다)을 수행하는 것을 포함할 수 있으며, 원한다면 복호화하는 것을 포함할 수 있다. 또한, 데이터는 각각의 프레임에 반복적으로 삽입되기 때문에, 복구 프로세스는 수신된 최종 비트 이후의 보조 데이터 비트들을 오버레이 해야 하며(박스 790), 보조 데이터 비트들이 파일 전체에 걸쳐 변화되지 않는 것을 보장해야 한다. 보조 데이터 비트들이 파일 전체에 걸쳐 변화되면, 파일은 인증되지 않는다.

선택적으로, 다른 수정 기능이 사용되면, 그의 역이 사용되어야 한다. 중요하게는, 동일한 복구 보조 비트들 및 원본 컨텐트 비트들이 수정 연산에 사용된 바와 같이 역 연산에 사용되어야 한다. 프레임의 첫 번째의 M 오디오 비트들이 보조 데이터를 수정하는데 사용되는 삽입 예에서, 프레임의 첫 번째의 M 오디오 비트들은 복구되며 복호화된 수정 보조 데이터를 수정하지 않는데 사용되어야 한다. PN 시퀀스가 보조 데이터를 수정하는데 사용되면, 동일한 PN 시퀀스가 데이터를 수정하지 않는데 사용되어야 한다.

선택적인 삽입 단계가 사용되면, 보조 데이터들은 그에 따라 복구된다. 예를 들면, 비트들이 글로벌 헤더 또는 링크된 파일에 삽입되면, 상기 비트들은 글로벌 헤더 또는 링크된 파일로부터 각각 판독된다.

최종적으로, 보조 데이터가 L 보다 길거나 L이 M에 의해 제산 불가능하면, 적합한 단계들이 취해져야 한다. 상기 단계들은 동적 로킹 및 언로킹에 대한 상기 설명으로 공지된 기술 분야의 숙련자들에게는 명백할 것이다.

활용예

상기 5개의 예시적인 활용예들은 동적 로킹 프로세스 및 장치를 가능화하는 것에 대한 이해를 돕기 위해 설명되었다. 상기 예들에 대한 일반적인 기초의 프로세스는 도 21에 도시되며, 대응하는 장치는 도 22 및 도 23에 도시된다. 일반적으로, 상기 프로세스는 박스(11)에 도시한 바와 같이 ID(140)를 동적 로킹하며 박스(120)에 도시한 바와 같이 매체 내에 로킹된 ID를 삽입하는 전송 디바이스(100)로 개시된다. 개시 단락 부분에서 정의한 바와 같이, 용어 ID는 통상 식별자를 지칭하는 것이지만, 임의의 보조 정보를 포함할 수 있다. 전송 디바이스(100)는 부호화기, 기록기, 전송기, 저장 매체 등일 수 있다.

다음, 상기 매체는 박스(160)에 도시한 바와 같이 로킹된 ID가 복구되며, 박스(170)에 도시한 바와 같이 동적으로 언로킹되는 수신 디바이스(130)로 전송된다. 다음, 박스(180)에 도시한 바와 같이 복구된 ID(140)에 의해 허용되면, 적합한 작용이 가능화된다. 수신 디바이스(130)는 복호화기, 플레이어, 기록기 등일 수 있다.

동적 로킹 및 언로킹 프로세스는 부호화 및 복호화를 포함하며, 복호화 키는, 박스(151, 152 및 153)에 도시한 바와 같이, 소정 위치에 배치되어 안전하게 전송되어야 한다. 키(key)를 안전하게 전송하는 것은 암호학 분야에 정통한 사람에게 잘 이해될 수 있을 것이다. 키의 위치는 활용예에서의 요구에 좌우된다. 5개의 활용예들은 다양한 키 위치를 나타낸다. 대부분의 활용예에서, 키는 3개의 가능한 위치 중 하나에만 사용할 수 있다. 게다가, 부호화 및 복호화 키는 통상 동일(대칭적)

하며, 하기에는 부호화 키로서 언급한다. 그러나 공개/비밀 키 부호화가 상기 상황들 중 다수에 사용될 수도 있다. 하기에서 비밀/공개 부호화를 설명할 때, 키는 공개 또는 비밀 부호화 키로서 설명될 것이다. 최종적으로, 임의의 활용예에서는 값들이 미리 결정되기 때문에, 보조 정보를 전송할 필요가 없다.

또한, ID(140)의 사용 및 위치, 전송 디바이스(100) 및 수신 디바이스(130)의 형태는 이러한 활용예에서 또한 더욱 상세히 설명된다.

5개의 예시적인 활용예들은 MP3 데이터의 배포(distribution), 브로드캐스트 데이터에 대한 1회 복사 액세스(copy-once access), DVD 복사 방지, 사진 카드 증명 및, 비밀 데이터 전송을 포함한다. 이러한 설명으로부터 다수의 다른 응용이 명백해진다.

MP3 데이터 배포와 관련하여, 본 개념은 다수의 시나리오를 사용하여 설명한다. 모든 시나리오는 소프트웨어 PC-기반 및 휴대용 MP3 오디오 플레이어 및 인터넷을 통한 배포 모두를 포함한다.

제 1 시나리오에서, MP3 데이터는 인터넷 상에 존재하며 최종 사용자에 의해 획득된다. 전달 시스템(delivery system)이 최종 사용자의 플레이어와 상호 작용하여, 박스(151)에 도시한 ID(140) 및 부호화 키를 수신 디바이스로부터 전송 디바이스로 확실하게 전달하며, MP3 데이터 내에 ID(140)를 부호화를 포함하는 동적 로킹한다. 상기 시나리오에서, 박스(151)에 도시한 부호화 키는 최종 사용자의 플레이어에 위치한다. MP3 파일이 전달(즉, 다운로드)된 후, 다른 플레이어들은 다른 ID를 갖기 때문에 최종 사용자의 플레이어에서만 데이터를 재생할 수 있다. 휴대용 및 PC 기반 플레이어는 ID(140)를 공유할 수 있으며, 이는 소프트웨어 프로그램 및 EPROM 또는 플래시 메모리와 같은 현재의 디지털 전자 기기에 의해 용이하게 실시될 수 있다. ID(140)는 동적으로 로킹되기 때문에, 최종 사용자는 ID(140)를 추출할 수 없으며, 이를 사용하여 다른 노래 또는 MP3 파일을 사용할 수 없다.

다른 시나리오에서, MP3 부호화기 및 플레이어는, CD, DVD 또는 브로드캐스트 오디오를, 부호화를 포함하는 동적 로킹된 ID(140)를 수용하는 삽입 데이터를 갖는 MP3 오디오로 변환시키는 하나의 소프트웨어 프로그램의 부분일 수 있다. 이러한 예에서, 박스(151)에 도시한 바와 같이 부호화 키 및 ID(140)를 교환할 필요가 없다. 상기 소프트웨어 응용은, 키 및 ID(140)가 소프트웨어 분야에서 공지된 바와 같이 최종 사용자로부터 보호되도록 프로그램되어야 한다. 또한, 박스(151)에 도시한 키는 최종 사용자의 플레이어 내에 위치된다. 변환된 MP3 오디오는 최종 사용자의 시스템 및/또는 휴대용 플레이어에서만 재생될 수 있으며, 상술한 바와 같이, ID(140)를 다른 노래에 이동시키는 것이 불가능하다.

또 다른 시나리오에서, 키는 박스(152)에 도시한 바와 같이 중앙 데이터베이스에 위치될 수 있다. 이러한 구성은 각각의 플레이어와 MP3 오디오 샘플에 대한 상이한 키를 허용한다. 이러한 구성은, 각각의 노래에 대해 새로운 키를 사용하기 때문에 공격에 대한 견고성을 증가시키지만, 추가의 관리 도구 및 책임(responsibility)을 수반한다.

MP3 오디오에 대한 최종 시나리오에서, ID(140)는 초과시에 오디오를 재생시킬 수 없는 오디오를 청취 시간 제한 또는 데이터 제한을 포함할 수 있다. 플레이어는 노래가 재생된 횟수 또는 기한이 만료되었는지의 여부를 계속 추적할 수 있다. ID(140)는 노래를 하나의 플레이어에만 제한시키지 않는 데모 코드를 포함할 수 있다.

1회 복사 액세스(시간 전환의 목적으로 최종 사용자가 매체를 1회만 복사하도록 허용하는 것으로 정의되는)와 관련하여, 본 개념은 영화의 브로드캐스트와 관련하여 설명한다. 브로드캐스트 매체에 있어서, 모든 사람이 동일한 부호화 키를 공유하면 가장 바람직하다. 박스(153)에 도시한 바와 같이, 키는 영화에 삽입된 브로드캐스트일 수 있으며, 각각의 브로드캐스트에 대해 변화될 수 있다. 게다가, 삽입 데이터가 부호화되지 않으면, 키를 사용할 필요가 없으며, 따라서 전송이 단순화된다. 최종적으로, 1회 복사 ID(140)는 미리 결정될 수 있으며, 이는 도 21에 도시한 바와 같이 ID(140)가 전송 디바이스 내의 선택적인 위치를 갖는 전송 및 수신 디바이스에 미리 결정되어 있다는 것을 의미한다. 브로드캐스트가 수신되면, 검색된 ID(140)는 데이터를 기록할 수 있게 하며, 기록기는 영화를 기록할 수 있으며, 1회 복사 ID(140)를 제거하거나, 매체가 1회 복사된 다른 기록기를 구별하는 소정의 코드로 ID(140)를 변화시킨다.

DVD 복사 방지와 관련하여, 두 개의 시나리오가 있다. 제 1 시나리오에서, 플레이어는 삽입 ID가 작동하지 않으면, 매체를 재생하지 않는다. 박스(153)에 도시한 바와 같이, 부호화 키는 비복사 액세스 위치에서 DVD 상에 수신된다. 이는 플레이어가 정확한 ID를 검색하지 않으면 DVD 데이터를 재생하지 않기 때문에, 사용자가 DVD 디스크가 존재할 때만 매체를 재생할 수 있다는 것을 의미한다. 삽입 데이터를 복호화하기 위한 키는 검색되지 않으며 상기 키가 없으면 플레이어가 작동하지 않기 때문에, 전체 DVD의 복사(복사할 수 없기 때문에 부호화 키를 제외한) 또는 컨텐트 파일의 복사는 불가능하다.

또한, 키는 중앙 액세스 가능한 데이터베이스에 위치될 수 있으며, 박스(152)에 도시한 바와 같이 요구되는 최종 사용자 플레이어에 링크될 수 있다. 이러한 구성은 키에 대한 액세스가 모니터링되기 때문에 공격에 대한 견고성을 증가시키지만, 컨텐트 제공자에 대한 추가의 취급 책임 및 최종 사용자에 대한 추가의 시간을 수반한다. 키는 폴 슈넥에 허여된 미국 특허 제 5,933,498호(본원에 참조로서 관련됨)에 개시된 바와 같이 당신의 플레이어의 키에 의해 획득되며 부호화될 수 있다. 마찬가지로, ID(140)는 미리 결정될 수 있으며 전송 디바이스(100)에 존재할 수 있다.

다른 시나리오에서, 미리 결정된 ID(140)는 기록기를 사용 가능하게 하는데 사용될 수 있으며, 소정 횟수의 복사 발생 또는 복제 방지 부호화로 공지된 원본 만의 복사를 허용하는데 사용될 수 있다. ID(140)는 DVD가 기록될 때마다 1회 적은 기록 발생을 허용하도록 수정될 수 있다. 기록 발생 및 원래 허용된 카운트의 트랙을 유지하거나 허용된 카운트를 감소시키는 것도 가능하다. 복제 방지 부호화에 있어서, 워터마크가 제 2 세대 DVD에서 제거될 수 있다. 이러한 접근에서, 워터마크가 존재하지 않으면, 복사할 수 없다는 것을 주목해야 한다. 최종적으로, 복제 방지의 양 형태에 대해 2층(two-layered) ID(140s)가 사용될 수 있다.

상기 사진 카드 활용예는 ID(140)가 삽입 사진 카드에 화상을 갖는 것을 포함한다. 정확한 정보가 존재하지 않으면, 상기 카드는 위조이며, 사용을 위해 허가되지 않는다. 이러한 방법의 보안을 증가하기 위해 동적 로킹이 적용된다; ID(140)는 사진에 의해 반전 가능하게 수정되거나 대응하는 이름 및 주소와 같은 데이터에 접속되며, 정보가 카드 사이에 복사될 수 없도록 또는 합법적인 카드로부터 불법 카드로 복사되지 않도록 부호화된다. 일치하는 ID(140)와 부호화 키는 단지 모든 전송 디바이스에 의해(즉, 전송 디바이스에) 액세스 가능한 데이터 베이스에 저장될 수 있으며, RSA 키 교환 또는 암호학 분야에 공지된 임의의 다른 방법을 사용하여, 데이터베이스와 사진 카드 판독 디바이스 사이로 안전하게 전송된다. 다른 부호화 기술과 마찬가지로 안전성에 추가하여, 본 프로세스의 다른 장점은 짧은 ID(140)와 부호화 키를 포함하는 최소의 데이터의 전송을 필요로 한다는 것이다.

마지막 활용예는 매체 내에 은폐된 ID(140)의 비밀 정보의 안전한 전송을 허용한다. 대부분의 방관자는 기밀 메시지가 첨부되어 있다는 것을 인식하지 못한다. 수신 디바이스가 은폐된 메시지를 추출하면, 수신 디바이스, 접속 디바이스 또는 사람은 ID(140) 내에 포함된 은폐 정보에 의해 가능화될 수 있다. 발견되면, 은폐 정보는 다른 매체 세그먼트들로 이동되는 것 및/또는 다양한 동적 로킹 기구들을 갖는 동적 로킹을 사용하여 해독되는 것이 방지될 수 있다. 예를 들면, 비밀 정보가 당신의 공개 키에 의해 부호화되면, 당신만이 복구할 수 있을 것이다. 또한, 비밀 정보가 당신의 비밀 키에 의해 부호화되면, 당신의 공개 키를 사용하여 메시지를 수신하는 사람들 또는 디바이스들은 그 정보가 당신에 의해 승인된 것이며 인증된 것이라는 것을 인식하게 된다. 상기 비밀 정보가 대칭적인 키에 의해 부호화되면, 키의 홀더만이 메시지를 작성하고 판독할 수 있다. 최종적으로, 동적 로킹의 수정 단계가 사용되면, 수신자는 메시지가 상이한 매체 세그먼트로부터 전송되지 않았다는 것을 인식하게 된다.

장치

도 22는 가능화, 등록 및 동적 로킹 프로세스들을 실시하는데 사용되는 예시적인 장치를 도시한다. 하드웨어는 논리 프로세서(900)와 메모리(910)를 포함한다. 상기 논리 프로세서(900)는 디지털 신호 프로세서(DSP), 일반적인 이용의 중앙 처리 유닛(CPU) 또는 특정된 ASIC 칩의 등가물로서 정의될 수 있다. 사용 가능한 DSP 칩은 텍사스 인스트루먼츠 TMS320 제품 중 하나이다. CPU는 인텔 펜티엄 제품 또는 모토로라/IBM 파워PC 제품 중 하나를 포함할 수 있다. 이러한 디자인은 상기 프로세스들의 설명에 의해 공지된 기술 분야의 숙련자들에게는 자명한 것이다. 메모리(910)는 임의의 형태의 메모리를 포함한다.

도 23은 동적 로킹을 위한 장치의 상세를 도시한다. 구체적으로는, 논리 프로세서(900) 및 메모리(910)는 수정기(modifier; 1010) 및 부호화기(1040)로서 작용하도록 함께 작동해야 한다. 수정기(1010)는 동적 로킹의 수정 단계를 수행한다. 부호화기(1040)는 동적 로킹의 부호화 단계를 수행한다.

도 24는 동적 언로킹을 위한 장치의 상세를 도시한다. 구체적으로는, 논리 프로세서(900) 및 메모리(910)는 복호화기(1045) 및 수정 해제기(1015)로서 작용하도록 함께 작동해야 한다. 복호화기(1045)는 동적 언로킹의 복호화 단계를 수행한다. 수정 해제기(1015)는 동적 언로킹의 수정 해제 단계를 수행한다. 동적 언로킹의 수정 해제기(1015) 및 복호화기(1045)는 동적 로킹의 수정기(1010) 및 부호화기(1040)와 동일하거나 상이한 회로를 사용할 수 있다. 그러나 동일한 회로가 사용될 때, 동적 로킹 및 언로킹 프로세스들은 상이한 제어 프로그램들을 사용할 것이다.

바인딩 및 ID 할당

상술한 바와 같이, 본원에 설명된 기술의 다른 양상은, 예를 들면 침해를 제어하는 동안 소비자들이 보호된 컨텐트에 합법적으로 액세스하는 방식의 매체 바인딩에 관한 것이다. 기본 개념은 컨텐트가 특정 사용자 또는 브로드캐스트에 대해 로킹되는 ID를 포함하며, 랜더링 디바이스가 현재 및 이전에 랜더링된 ID들 및 규칙들에 기초하여 컨텐트가 액세스될 수 있는지의 여부를 자동적으로 결정한다는 것이다. 이러한 기술은 컨텐트 제공자들을 위해 증가된 컨텐트의 판매를 야기할 수 있다.

상기 기술의 한 양상은 현재 및 이전의 액세스된 컨텐트 모두에 포함되는 ID들의 트랙을 유지하는 랜더링 디바이스를 갖는 것이다. 이는 새로운 컨텐트의 ID, 컨텐트가 제공된 규칙들(컨텐트 제공자들에 의한) 및/또는 디바이스 내의 규칙들 및, 디바이스에 의해 이전에 랜더링된 컨텐트로부터의 ID들에 기초하여, 랜더링 디바이스가 새로운 컨텐트에 대해 제어 액세스하는 것을 허용한다.

상기 ID는 사용자 또는 브로드캐스트에 링크될 수 있다. 사용자 ID들은 사용자의 지속 사용을 위해 판매되는 컨텐트를 위해 양호하게 작동되며, 반면 브로드캐스트 ID들은 브로드캐스트로부터 사용자에 의해 기록되는 컨텐트를 위해 양호하게 작동된다.

예시적인 실시예는 다음과 같다. 사용자 링크 컨텐트에 있어서, 랜더링 디바이스는, 각각의 사용자 ID에 의해 컨텐트가 이미 액세스된 횟수에 의해 영향을 받을 수 있는 소정의 횟수 동안 액세스될 수 있는 상이한 사용자 ID들에 의한 컨텐트 트랙의 수를 제한하는 제약들(constraints)을 가진다. 브로드캐스트 컨텐트에 있어서, 브로드캐스트 ID들 및 선택적으로 포함되는 규칙들은 각각의 브로드캐스트의 랜더링 또는 복사를 제한하는데 사용된다. 달리 말해, 브로드캐스트 ID들에 의해, 상기 제한들은 브로드캐스트 ID들의 총 수가 아니라 기한 또는 ID가 재생된 횟수에 기초한다.

보다 구체적으로는, 휴대용 MP3 플레이어는 각각의 노래의 사용자 ID의 트랙을 유지할 수 있으며, 이전에 재생된 노래가 N 개의 상이한 사용자 ID들 보다 많이 포함하면, 플레이어는 과거의 사용자 ID의 기한 및 ID에 의해 재생된 노래의 횟수에 기인하여 과거의 사용자 ID를 새로운 ID로 대체할 수 있는지를 판단한다. 유사하게, 브로드캐스트 ID가 메모리 내에 포함되면, MP3 플레이어는 사용자가 오디오를 X회 재생하였으며, 브로드캐스트에 의해 Y회 허용 가능하다거나 기한이 브로드캐스트의 허용 가능한 사용 기한을 경과하였다고 기록한다.

이를 위해, 소비자가 ID 카드를 소지할 필요가 없기 때문에 소비자가 디바이스를 사용하는 것이 용이하다. 게다가, 사용자를 ID에 링크시키는 글로벌 데이터베이스가 필요 없으며, 따라서, 사용자의 프라이버시가 침해되지 않는다. 예를 들면, 사용자가 ID를 분실하면, 이전의 컨텐트로부터 획득할 수 있다. 그러나 사용자 또는 브로드캐스트 ID는 비밀을 유지할 수 있으며, 다른 프라이버시 방법이 사용될 수 있다. 더욱 중요한 것은, 컨텐트 제공자가 원한다면, 매체에 대한 액세스가 제한되지만, 사용자는 불편을 느끼지 않는다는 것이다.

재차, 관련 용어를 정리하겠다. 랜더링 디바이스는 재생, 검토 또는 데이터 상에 유사 작용을 수행하는 디바이스이다. 상기 랜더링 디바이스는 이미지, 오디오 및 비디오를 포함하지만, 이에 한정되는 것은 아닌 임의의 형태의 지각 데이터를 제공할 수 있다. 랜더링 디바이스가 MP3 플레이어와 같은 휴대용 섹션을 가지면, 랜더링 디바이스에 컨텐트를 위치시키는 로더가 랜더링 디바이스의 일부로 고려될 수 있다. ID는 사용자 또는 브로드캐스트 ID일 수 있다. 예를 들면, 다수의 MP3 플레이어들은 또한 기록 브로드캐스트들일 수 있으며, 상기 브로드캐스트들은, 장래에 디지털 브로드캐스트들을 갖는 워터마크들 또는 헤더 데이터와 같은 삽입 브로드캐스트 ID들을 포함할 수 있다. 컨텐트는 소정의 오디오, 비디오, 이미지 또는 다른 관련된 지각 데이터를 지칭한다. 컨텐트 제공자는 레코드 라벨들, 영화 스튜디오들 및, 독립 아티스트들을 포함하지만, 이에 한정되는 것은 아니다. ID는 헤더 파일 또는 워터마크 내의 비트와 같은 컨텐트 내에 삽입될 수 있으며, 또는 ID는 컨텐트의 부호화 및 복호화에 링크될 수 있다. 최종적으로, 상기 자동 ID 관리는 매체 바인딩과 같은 다른 방법과 함께 사용될 수 있다.

도 25는 자동 ID 관리 프로세스의 개요도이다. 상기 프로세스에서, 랜더링 디바이스(100)는 이전에 액세스된 컨텐트 내에 포함된 ID들의 트랙을 유지한다(박스 100). 규칙들(120)은 디바이스 하드웨어 내에 제공될 수 있으며 및/또는 컨텐트를 포함할 수 있다. 상기 규칙들(120)은 디바이스가 그의 ID에 기초하여 새로운 컨텐트를 액세스할 수 있는지의 여부를 판단한다(박스 130).

랜더링 디바이스가 MP3 플레어와 같은 휴대용 섹션을 가지면, 랜더링 디바이스의 부분으로서 상술한 로더는 휴대용 섹션 내에 요구되는 메모리의 양을 감소시키는데 사용될 수 있으며, 따라서 비용을 절감한다. 이는 휴대용 랜더링 디바이스에서, 휴대용 섹션은 이러한 자동 ID 관리를 수행하는데 요구되는 모든 메모리 및 프로세싱 하드웨어(하기에 설명함)를 포함할 수 있으며, 또는 하드웨어가 로더와 휴대용 섹션 사이에 분할될 수 있다는 것을 의미한다. 예를 들면, 컴퓨터가 휴대용

MP3 플레이어 상에 MP3 파일을 위치시키는 소프트웨어 로더를 사용하면, 상기 로더는 컴퓨터상에 ID들에 대한 모든 정보를 저장할 수 있으며, 랜더링 디바이스가 수행해야 할 것은 각각의 노래가 재생된 횟수의 카운트 및 컨텐트의 현재 리스트를 위한 기한 정보의 유지이다.

도 26은 프로세스의 예를 실시하기 위한 의사 코드를 도시한다. 본 실시예에서, 규칙들(120)은 컨텐트 제공자에 의해 특정됨에 따라 컨텐트 내에 포함되는 제약들(245) 뿐만 아니라 렌더링 장치 하드웨어에 포함되는 디폴트 규칙을 포함한다. 제약들(245)은 컨텐츠(200)로부터 검색된다(박스 240). 상기 제약들(245)은 디바이스가 설정된 시간 기간 동안 상이한 ID들에 의해 액세스 가능한 컨텐트 트랙들의 수를 제한할 수 있다. 제약들(245)은 특정 ID에 의해 컨텐트가 액세스되는 횟수에 따라 ID가 저장되는 시간 간격을 변화시킬 수도 있다. 제약들(245)은 컨텐트 내에 삽입되거나 헤더 정보 또는 링크 파일로서 첨부될 수 있다.

사용의 경우, 사용자를 혼란하게 할 수 있기 때문에, 상기 제약들을 노래마다 변화시키지 않는 것이 양호하다. 바람직하게는, 상기 제약들은 부합되어야 하며 랜더링 디바이스 내에 설정되어야 한다. 그러나 컨텐트 내에 규칙들을 포함할 수도 있다.

본 예시적인 프로세스를 더욱 상세하게 설명하기 전에, 도시한 장치는 자동 ID 관리 프로세스(도 27)를 실시하기 위한 장치임을 이해하는 것이 중요하다. 하드웨어는 논리 프로세서(300) 및 메모리(310)를 포함한다. 논리 프로세서(300)는 디지털 신호 프로세서(DSP), 일반적인 이용의 중앙 처리 유닛(CPU) 또는 매체 프로세서를 포함하는 특정된 CPU의 등가물로서 정의될 수 있다. 마찬가지로, 사용 가능한 DSP 칩은 텍사스 인스트루먼츠 TMS320 제품 중 하나이다. CPU는 인텔 펜티엄 제품 또는 모토로라/IBM 파워PC 제품 중 하나를 포함할 수 있다. 논리 프로세서(300)를 제어하기 위한 코드의 디자인은 상기 의사 코드 및 설명에 의해 공지된 기술 분야의 숙련자들에게는 간단한 것이다.

또한, 당 기술 분야의 숙련자들은 아날로그 및 디지털 회로, 개별 또는 주문형 집적 회로(ASIC)를 사용하여 논리 프로세서(300)를 실시할 수 있다. 아날로그 및 디지털 회로는 하기의 디바이스들, 즉 디지털 아날로그 변환기(D/A), 비교기, 샘플-홀드 회로, 지연 소자, 아날로그 디지털 변환기(A/D) 및 프로그램 가능 논리 제어기(PLC)의 임의의 조합체를 포함한다. 프로그램 가능 논리 어레이(PLDs)가 마찬가지로 사용될 수 있다.

메모리(310)는 ID들, 최종 재생 날짜 및, 각각의 ID에 의해 컨텐트가 액세스된 횟수와 같은 규칙들(120)에 의해 요구되는 정보를 저장한다. 메모리(310)는 표준 컴퓨터 랜덤 액세스 메모리(RAM)로 구성될 수 있다. 메모리(310)가 백업을 갖는 ROM 및 충전식 배터리 전원, 또는 EPROM과 같은 전원 없이도 안정적인 메모리를 사용하여 랜더링 디바이스에 전원이 없을 때조차 상기 정보를 유지하면 또한 바람직하다. 상술한 바와 같이, 메모리(310)는 휴대용 섹션 및 로더를 사용할 때 두 개의 개별 모듈로 구성될 수 있다.

이제, 예시적인 프로세스를 상세히 설명한다. 새로운 컨텐트(200)를 수신하는 디바이스(100)로부터 설명한다. 컨텐트(200)로부터 ID(210)가 검색된다. ID(210)는 사용자 또는 브로드캐스트 ID인지 확인하기 위해 검사된다(박스 215).

사용자 ID에 있어서는, 다음과 같이 기능한다. ID(210)가 디바이스(100)의 메모리(310)에 이미 존재하면(박스 220), 재생 카운트 및 최종 액세스 날짜가 갱신되며(박스 222), 컨텐트(200)는 랜더링된다(박스 230). ID(210)가 메모리(310) 내에 존재하지 않으면(박스 220), 규칙들(120)이 검사된다. 다른 ID가 메모리(310) 내에 존재할 수 있으면(박스 250), ID(210) 및 현재 날짜가 메모리(310)에 가산되며(박스 260), 컨텐트는 랜더링된다(박스 230). 다른 ID가 가산될 수 없으면, 규칙들(120)은 임의의 존재하는 ID들이 너무 오래되었기 때문에 대체될 수 있는지를 확인하기 위해 검사된다(박스 270). 임의의 ID들이 대체될 수 있으면, 과거의 ID는 ID(210)로 대체되며(박스 280), 컨텐트는 랜더링된다(박스 230). 어떤 ID들도 대체될 수 없으면, 사용자는 경고를 받게 되며, 액세스가 거부되거나 제한된다(박스 290). 또한, 컨텐트를 구매하도록 사용자에게 링크가 제공될 수도 있다(박스 290).

보다 구체적으로는, 상기 규칙들은 디바이스가 10 개의 ID들을 저장하도록 할 수도 있으며, ID들은 1주 동안 액세스하지 않으면 대체될 수 있다.

또한, ID가 랜더링된 횟수는 과거의 ID를 새로운 ID로 대체해야 하는지의 여부를 결정하는데 사용될 수 있다. 상기 카운트 값은 ID가 메모리(310)에 유지되는 시간 기간에 영향을 줄 수 있으며, 따라서 ID(210)를 저장된 ID로 대체할 수 있게 한다{박스들(270, 280). 예를 들면, 저장된 ID와 관련된 컨텐트가 1주 동안 액세스되지 않았으면, 교체될 수 있다. 역으로, 저장된 ID와 관련된 컨텐트가 적어도 7회 재생되었으면, 그의 최종 액세스 이후로 적어도 한 달 동안 유지되어야 한다.

컨텐트 제공자의 특정 요구에 부합되도록 설계될 수 있는 다수의 다른 단순한 규칙들이 존재한다. 그 중 몇몇은 ID가 대체될 수 있는지의 여부를 판단하는데 상이한 수식을 사용하는 것을 포함한다. 예를 들면, ID에 대한 카운트는 ID를 포함하는 컨텐트의 각각의 랜더링을 위해 1일 만큼 감소되며 1 만큼 증분될 수 있으며, ID는 카운트가 0 미만이거나 최종 액세스 날짜가 1주를 초과하면 대체될 수 있다(박스 270).

브로드캐스트 ID들에 있어서는, 하기와 같이 기능한다. ID(210)는 메모리(310) 내에 존재하는지를 확인하기 위해 검사된다(박스 255). 존재하지 않으면, ID(210) 및 현재 날짜는 렌더링 디바이스들 메모리(310)에 가산되며(박스 265), 컨텐트는 랜더링된다(박스 230). ID(210)가 메모리 내에 존재하면, 컨텐트가 랜더링될 수 있는지를 확인하기 위해 재생 카운트 기록 날짜 및/또는 최종 액세스 날짜가 검사된다(박스 275). 브로드캐스트는 2회의 랜더링만을 허용하거나, 1주 랜더링 또는 특정 날짜까지의 랜더링만을 허용할 수 있다. 브로드캐스트의 랜더링이 허용되면, 카운트 및 최종 액세스 날짜는 갱신되며(박스 285), 컨텐트는 액세스된다(박스 230). 브로드캐스트의 랜더링이 허용되지 않으면, 사용자는 경고를 받으며, 액세스는 제한되며, 가능하다면 브로드캐스트 또는 유사 컨텐트를 구매하는 링크가 제공될 수 있다(박스 295).

게다가, 상기 디바이스는 ID들, 날짜 및, 카운트와 같은 모든 정보를 리셋하는 소정의 방식을 가질 수 있어야 한다. 리셋 기능은 의사 랜덤식 비밀 번호를 요구하며, 따라서 디바이스를 리셋하도록 사용자가 접촉 지지되는 것을 요구한다. 예를 들면, 비밀 번호는 자동 시스템으로부터 획득된 날짜 및 햇수에 의존할 수 있다. 리셋 버튼은 또한 모든 현재의 컨텐트 뿐만 아니라 ID 정보도 삭제할 수 있다. 이는 사람들로 하여금 다수의 친구와 그룹으로 하나의 휴대용 플레이어를 사용할 수 있게 하지만, 컨텐트의 손실은 성가시기 때문에 이러한 저작권을 방해할 수 있을 것이다.

도 28은 상술한 의사 코드를 실시하는 장치를 포함하는 휴대용 MP3 플레이어(400)를 도시한다. 이 경우, 논리 프로세서(300)는 개별 프로세서일 수 있으며, 또는 오디오를 압축 해제하는 프로세서를 갖는 공유 액세스일 수 있다. 상기 디바이스는 또한 플레이어(400)가 전원이 없을 때조차, ID, 날짜 및, 카운트를 저장할 수 있도록 필수 메모리(310)를 포함한다. 상기 디바이스는 상기 메모리를 소프트웨어 로더와 공유할 수 있다.

마지막으로, 임의의 랜더링 디바이스에서, 논리 프로세서(300)는 개별 프로세서, 또는 디지털 컨텐트의 압축 및 압축 해제와 같은 디바이스를 위한 컨텐트를 취급하는 시간 공유 프로세서일 수 있다.

다중 워터마크들

다양한 장점은 단지 하나의 워터마크 대신에 다중 워터마크들을 사용함으로써 발생될 수 있다. 예시적인 시스템에서, 하나의 워터마크는 견고성이며, 매체가 보호되는 것을 표방한다. 상기 워터마크는 매체가 MP3와 같은 소정의 포맷에 부호화될 때 삽입된다. 이는 워터마크가 가산된 워터마크의 강도는 오디오에 1회만 가산되며 배포자에 의해 오디오로 복사되기 때문에 중요하지 않다는 것을 의미한다.

다른 워터마크는 매체를 재생 또는 기록하는데 양호한 것을 표방한다. 상기 워터마크는 효율적이며, 제거되어도 아무런 장점을 제공하지 않기 때문에 제거할 필요가 없다. 이러한 워터마크의 효율은 인터넷을 통한 다운로드와 같은 오디오 재생시마다 매체를 사용자, 플레이어, 기록기 및/또는 저장 디바이스에 링크시키도록 워터마크가 삽입되어야 하기 때문에 바람직하다. 따라서, 배포자를 위해 복사 관리 비용을 매우 감소시킬 수 있다. 게다가, 이러한 효율적인 워터마크를 찾아야만 하기 때문에, 플레이어의 비용을 줄인다. 워터마크가 존재하지 않을 때만, 플레이어는 오디오가 연산적으로 강렬한 워터마크가 아니라 견고성에 의해 보호되는지의 여부를 결정하는데 요구된다.

더욱 중요하게는, 비보호 매체는 워터마크를 포함하지 않으며, 임의의 메모리로부터 임의의 디바이스에 의해 재생될 수 있다.

더욱 상세하게는, 도 29는 두 개의 워터마크들을 사용하는 프로세스를 도시한다. 매체(100)는 불안정한 포맷 내에 존재하며, 이는 임의의 복사 보호 및/또는 인증 워터마크를 포함하지 않을지라도 디바이스가 매체(100)를 재생할 수 있다는 것을 의미한다. 이는 MP3와 같은 몇몇 아티스트들이 그들의 컨텐트를 자유롭게 배포시키고자 하는 포맷이다. 그러나 자유롭게 복사되며 재배포되는 것을 허용하지 않는 동일 포맷 내의 그들의 매체가 배포되는 것을 원하지 않는 이해 당사자들이 존재한다.

워터마크(110)는 매체가 보호되는 것을 표방한다. 워터마크(110)는 제거가 극단적으로 곤란하며, 연산적인 측면의 강도를 허용한다. 다수의 기존 워터마크 방법들은 이러한 설명에 부합되며, 장래의 방법들도 확실하게 설계될 것이다.

워터마크(120)는 사용자, 플레이어, 기록기 및/또는 저장 디바이스에 매체를 링크시킨다. 상기 링크는 사용자가 매체를 복사 및/또는 재생하는지의 여부를 결정한다. 워터마크(120)는 모방이 어려운 연산적인 측면에서 효율적인 방법일 수 있다.

도 29 및 도 30에 도시한 바와 같이, 두 개의 워터마크들이 재현(reproduction) 프로세스의 특정 시간에 삽입된다. 워터마크(110)는 오디오가 부호화될 때 삽입되며, 배포될 때 오디오에 의해 복사된다. 따라서, 가산되는 워터마크의 연산적인 측면의 강도는 중요하지 않다. 워터마크(120)는 영구적인 메모리에 배포 및 제공되는 것과 같이, 매체가 재생될 때 삽입되거나, 퍼스널 부호화 디바이스에 의해 선택적인 형태로부터 부호화된다. 재현이라는 용어는 매체의 합법적인 수정 또는 배포를 지칭하며, 반면에 복사라는 용어는 개인이 합법 또는 불법 사용을 위해 매체의 정확한 비트-대-비트 복제본을 제조하는 것을 지칭한다. 워터마크(120)는 매체가 재현될 때마다 삽입되기 때문에 그의 효율은 비용의 감소를 야기한다. 워터마크(120)는 워터마크(110) 다음에 삽입되기 때문에, 현행 기술에서 가능한 바와 마찬가지로 워터마크들을 적층할 수 있어야 한다.

선택적으로, 상기 워터마크들은 도 29 및 도 31에 도시한 바와 같이 특정 순서로 탐색 및 검색된다. 먼저, 매체가 워터마크(120)를 위해 탐색된다(박스 300). 워터마크(120)가 검색되면(박스 310), 삽입 정보가 평가된다(박스 320). 삽입 정보가 정확하면, 소정의 작용이 가능화된다(박스 330). 선택적으로, 삽입 정보가 정확하지 않으면, 소정의 작용이 불능화된다(박스 340). 워터마크(120)가 발견되지 않는 경우에만, 매체는 연산적인 측면에서 강한 워터마크(110)를 탐색하도록 요구된다(박스 350). 워터마크(110)가 매체 보호를 표방하면, 소정의 작용이 불능화된다(박스 340). 워터마크(120)가 존재하지 않으면(또는 매체가 자유를 표방하면), 소정의 작용이 허용된다(박스 330).

상술한 프로세스는 매체의 복사 및/또는 재생을 제한하는데 사용될 수 있다.

도 32는 본 발명의 프로세스들을 실시하는데 사용될 수 있는 하드웨어 장치를 도시한다. 상기 하드웨어는 논리 프로세서(400)와 저장 유닛(410)을 포함한다. 논리 프로세서(400)는 디지털 신호 프로세서(DSP), 일반적인 이용의 중앙 처리 유닛(CPU) 또는 매체 프로세서들을 포함하는 특정된 CPU의 등가물로서 정의될 수 있다. 사용 가능한 DSP 칩은 텍사스 인스트루먼츠 TMS320 제품 중 하나이다. CPU는 인텔 펜티엄 제품 또는 모토로라/IBM 파워PC 제품 중 하나를 포함할 수 있다. 이러한 디자인은 상기 의사 코드 및 설명에 의해 공지된 기술 분야의 숙련자들에게는 단순한 것이다. 저장 유닛(410)은 디지털 프로세서를 사용할 때 RAM을 포함한다.

또한, 당 기술 분야의 숙련자들은 아날로그 및 디지털 회로, 개별 또는 주문형 집적 회로(ASIC)를 사용하여 프로세스를 선택적으로 실시할 수 있다. 아날로그 및 디지털 회로는 하기의 디바이스들, 즉 디지털 아날로그 변환기(D/A), 비교기, 샘플-홀드 회로, 지연 소자, 아날로그 디지털 변환기(A/D) 및 프로그램 가능 논리 제어기(PLC)의 임의의 조합체를 포함한다. 프로그램 가능 논리 어레이(PLDs)가 마찬가지로 사용될 수 있다.

<u>컨텐트 스크램블링</u>

상술한 바와 같이, 컨텐트 신호들을 스크램블링하는 것이 종종 바람직하다. 하기의 설명은 이러한 스크램블링 기술에 대한 소정의 개선을 고찰한다.

이러한 스크램블링 기술 중 하나는, 검출 범주의 위치에 영향을 주지 않거나 원래 신호가 복구될 수 있도록 공지된 방식으로 검출 범주의 위치에 영향을 주면서, 검출 범주에 대한 원본 디지털 데이터에 의한 탐색 및 그 후의 컨텐트 열화에 대한 인접한 지점들의 조절을 포함한다. 검출 범주는 다수의 지점들 사이의 관계를 포함할 수 있으며, 또는 단순히 임계 교차점이거나, 모든 M번째 지점을 포함할 수 있다. 인접한 지점들의 조절은 단순히 임계 교차점 이후의 지점에 N을 곱하는 것일 수 있다. N이 1 미만이지만 0이 아닌 경우, 포화되기 때문에 유리하며, 0인 데이터 지점들은 문제가 되지 않으며, 임계값이 양의 값이면 데이터는 임계 횡단 도중에 0으로 감소된다.

상기 프로세스는 검출 범주에 대한 데이터에 의한 탐색 및 그 후의 그의 원래 값으로의 인접한 지점들의 조절을 포함할 수 있다. 예를 들면, 열화 프로세스에서의 조절이 N 만큼의 곱을 사용하면, 복구 프로세스는 1/N을 곱한다.

하기의 설명에서, 디지털 컨텐트는 오디오, 비디오 및, 이미지를 포함하지만 이에 한정되는 것은 아닌 지각된 물리적 아이템을 나타내는 디지털 데이터로서 언급한다. 디지털 데이터는 순간 시간에서의 원본 디지털 컨텐트의 샘플을 나타내는 비트("1"들 또는 "0"들)의 그룹화로서 언급한다. 각각의 비트 그룹은 데이터 포인트 또는 샘플로서 동일하게 언급된다. 상기 데이터 지점들은 순서대로 배치되며, 대부분의 경우 시퀀스 대 시간 또는 주파수를 나타낸다. 또한, 데이터 지점들은, MPEG 표준 압축된 디지털 오디오 및 비디오의 경우와 같이, 시퀀스 대 주파수 대 시간을 나타내는데 사용될 수 있는 하위

그룹을 형성하도록 재차 그룹화될 수 있다. 더욱 중요하게는, 디지털 데이터는 데이터의 탐색이 가능하도록 시작 및 종료를 갖는 순서를 가지며, 인접한 지점들은 서로에 대해 근접한 지점으로서 정의될 수 있다. 최종적으로, 지점(들)은 하나 또는 다수의 지점들을 지칭한다.

도 36은 열화 및 복구 프로세스의 개략도를 도시하며, 도 37은 상기 장치에 의해 실시되는 대응 의사 코드를 도시한다.

디지털 컨텐트를 열화시키기 위해(박스 100), 샘플들이 검출 범주(박스들 200, 210, 220)에 대해 탐색된다. 탐색은 버퍼 내의 최종 데이터 지점이 검사된 후 정지되며(박스 210), 가능하다면 새로운 버퍼가 제공될 수 있다. 당 기술 분야에 공지된 바와 같이, 데이터 값들은 버퍼들 사이에 저장되어야 하며, 초기 지점들이 적절하게 탐색되도록 제 1 버퍼에 대해 적합하게 초기화되어야 한다.

검출 범주가 발견될 때, 이웃의 데이터 지점(들)은 컨텐트 열화를 발생시키기 위해 조절된다(박스 230). 상기 지점들의 조절은 검출 범주의 위치를 변화시키지 않거나 공지된 방식으로 변화시켜야 하며, 그렇지 않으면 원래 값으로의 데이터의 재조절에 대한 정확한 위치의 검출(복구)은 용이하지 않게 된다. 또한, 조절에 의해 포화를 발생시키거나 0의 값이 되게 하는 것을 방지하는 것이 바람직한데, 이는 그렇지 않으면 원본 데이터 지점(들)이 용이하게 복구될 수 없기 때문이다.

원본 디지털 컨텐트를 복구하기 위해(박스 110), 열화된 데이터는 열화 프로세스에 의해 규정된 검출 범주에 대해 탐색된다(박스 200, 210, 220). 열화 프로세스가 공지된 방식으로 검출 범주를 변화시키면, 복구를 위한 박스(220)의 검출 범주는 열화에서 사용된 것과 상이해 진다. 범주 위치가 발견되면, 이웃 데이터 지점(들)은 열화 프로세스에 사용된 방법을 역순으로 재조절된다(박스 230).

이러한 프로세스의 예는 도 38 및 도 39에 도시된다. 이러한 경우(박스들 300 310), 검출 범주는 양의 임계값(thr>0)을 갖는 임계 교차값(c-언어 표기법을 사용하면: x[n-1]>thr && x[n]<thr)이다. 이웃 지점(들)은 임계 교차값 이후의 지점만을 포함한다(박스 430). 데이터를 열화시키기 위해, 상기 조절은 N이 1 미만일 때, 임계 교차값(x[n]) 이후의 데이터 지점에 N을 곱하는 것을 포함한다(박스 430). 상기 데이터 지점의 값을 감소시킴으로써, 검출 범주 위치는 변화되지 않는다. 또한, N이 0에 근접할수록(하지만, 0은 아님), 디지털 컨텐트가 더욱 열화된다. 원본 디지털 데이터를 복구하기 위해, 임계 교차값(x[n]) 이후의 지점은 1/N 만큼 곱해진다(박스 430).

사용될 수 있는 다른 단순한 검출 범주가 존재한다. 예를 들면, 모든 M번째 데이터 지점이 열화될 수 있다. 이 경우, 복구를 위한 동기화는 정확한 열화 위치들이 발견될 때까지, M 지점들에 대한 데이터의 스캐닝을 요구할 수 있다. 또한, 피크값들이 사용될 수 있으며, 피크 이후의 지점은 그 값만큼 감소될 수 있다. 원하는 바와 같이, 이는 복구 프로세스를 위한 검출 범주에 영향을 미치지 않는다. 선택적으로, 음의 임계값을 갖는 임계 교차값 및 0에 수렴되는 데이터를 사용할 수 있다. 또한, 임계값 이후의 데이터 지점은 절대값 만큼 감소되지만 0은 아니다. 상기 두 개의 경우들에 있어서, 복구를 위한 동기화는 데이터를 스캐닝할 때 자동적으로 발생한다.

상기 실시예에서, 검출 범주는 원본 디지털 데이터의 열화와 복구 사이에서 변화하지 않았지만, 이는 필수적인 것은 아니다. 검출 범주는, 복구 프로세스가 열화 프로세스와 상이한(그러나, 공지된) 검출 범주를 사용하도록 공지된 방식으로 변화될 수 있다. 달리 말해, 박스(420; 또는 220, 상술한 바와 같음)는 열화 및 복구 프로세스에 있어 상이할 수 있다.

원본 컨텐트는, 자명한 바와 같이, 디지털 샘플들 대 시간에 의해 나타낼 필요는 없다. MPEG 압축(즉, MP3 오디오)의 사용과 같은 다수의 경우에, 디지털 샘플들은 주파수들 대 시간의 하위 그룹들을 나타낸다. 이 경우, 데이터는 각각의 하위 그룹에 대한 교차 주파수 또는 각각의 주파수에 대한 교차 시간, 또는 임의의 다른 양호하게 규정된 조합을 탐색할 수 있다. 데이터는 주파수 크기 또는 대응하는 스케일링 인자들을 또한 나타낼 수 있다.

그 외에도, 지각 열화의 대부분을 제거하는 동안 데이터를 복구하는 다른 방법들이 있다. 예를 들면, 데이터를 복구하기 위해 저대역 통과 필터를 사용할 수 있다. 복구된 디지털 데이터는 원본 디지털 데이터와 정확하게 일치하지는 않지만, 그의 지각은 허용 가능할 것이다. DSP 기술 분야의 숙련자들에게 공지된 바와 같이, 형태 및 순서와 같은 필터 특징들은 복구된 데이터에 영향을 미친다.

대안적으로, 검출 범주(박스 220) 또는 데이터의 조절 또는 재조절(박스 230)을 설정하기 위해 의사 랜덤 시퀀스들(다시 말하면, 키)을 사용할 수 있다. 이러한 무작위성은 데이터를 합법적으로 복구하는 것을 더욱 곤란하게 한다. 예를 들면, 0보다 크지만 1 보다 작은 의사 랜덤 수가 스케일링 값(N)으로서 사용될 수 있다(박스 430). 또는 최소 및 최대 임계값 사이

의 의사 랜덤 수가 임계값을 위해 사용될 수 있다(박스 420). 가장 중요한 것은 열화 및 복구 프로세스가 동일한 의사 랜덤 시퀀스를 사용한다는 것이다. 그러나 이러한 구성은 데이터를 따라 키를 전송하는 것을 필요로 한다. 상기 키는 원본 데이터를 열화된 데이터로부터 복구할 수 있도록, 공지된 기술을 사용하여 데이터 내에 삽입될 수 있다.

도 40은 상술한 열화 및 복구 프로세스들을 실시하는데 사용되는 예시적인 하드웨어를 도시한다. 상기 하드웨어는 논리 프로세서(500)와 저장 유닛(510)을 포함한다. 상기 논리 프로세서(500)는 디지털 신호 프로세서(DSP), 일반적인 이용의 중앙 처리 유닛(CPU) 또는 매체 프로세서들을 포함하지만 이에 제한되는 것은 아닌 특정된 CPU의 등가물로서 정의될 수 있다. 사용 가능한 DSP 칩은 텍사스 인스트루먼츠 TMS320 제품 중 하나이다. CPU는 인텔 펜티엄 제품 또는 모토로라/IBM 파워PC 제품 중 하나를 포함할 수 있다. 논리 프로세서(500)를 제어하기 위한 코드의 디자인은 상기 의사 코드 및 설명에 의해 공지된 기술 분야의 숙련자들에게는 단순한 것이다. 저장 유닛(510)은 디지털 프로세서를 사용할 때 RAM을 포함하며, 검출 범주에 대한 이전의 지점(들) 및/또는 현재의 버퍼를 저장하도록 요구된다.

또한, 당 기술 분야의 숙련자들은 아날로그 및 디지털 회로, 개별 또는 주문형 집적 회로(ASIC)를 사용하여 논리 프로세서(500)를 실시할 수 있다. 아날로그 및 디지털 회로는 하기의 디바이스들, 즉 디지털 아날로그 변환기(D/A), 비교기, 샘플-홀드 회로, 지연 소자, 아날로그 디지털 변환기(A/D) 및 프로그램 가능 논리 제어기(PLC)의 임의의 조합체를 포함할 수 있다.

스크램블링 기술에 대한 다른 개선에 따르면, 헤더 또는 컨텐트에 대한 다른 중요한 정보의 스크램블링을 방지하는 프로세스가 제공된다. 헤더를 단독으로 남겨 두는 것에 의한 장점은 응용들 또는 디바이스들이 컨텐트를 디스크램블링 및 액세싱하기 전에 컨텐트에 대한 정보를 신속하게 판독할 수 있다는 것이다. 예를 들면, 스크램블링된 MP3 파일에 있어서, 사용자는 디스크램블링을 선택하여 재생하기 전에 노래의 길이, 아티스트, 해결(resolution) 등에 대해 신속하게 숙지할 수 있다. 선택적으로, 헤더는 재생 전에 플레이어의 검사가 요구되는 저작권 정보를 포함할 수 있다.

스크램블링 프로세스는 몇몇 또는 모든 비헤더 컨텐트를 스크램블링한다. 단지 몇몇의 비헤더 컨텐트만 스크램블링되면, 이는 만일 존재한다면 교정될 수 있는 에러 보정보다 많아야 한다. 동영상 전문가 그룹(MPEG)에 의해 압축된 오디오 또는 비디오에서 같이, 컨텐트가 각각 자신의 헤더를 갖는 프레임들을 포함하면, 각각의 프레임의 헤더는 몇몇 또는 모든 비헤더 컨텐트를 스크램블링 하는 동안 회피된다. 디스크램블링 프로세스는 헤더 정보를 유사하게 회피하면서, 스크램블링된 컨텐트로부터 원본 컨텐트를 복구한다.

예시적인 프로세스는 각각의 프레임의 헤더들을 회피하면서, 컨텐트를 스크램블링하는 의사 랜덤 노이즈(PN) 시퀀스 및 XOR 기능을 사용하는 것을 포함한다. 디스크램블러(de-scrambler)는 XOR 기능의 역(inverse)이 XOR 기능이기 때문에 동일하다.

재차, 관련 용어를 정리하겠다. 파일의 헤더는 파일에 대한 중요한 정보를 포함한다. 상기 정보는 파일의 형태, 저자, 출처, 출시 날짜, 최종 수정 데이터, 파일 크기, 구조 할당들, 저작권 코드들, 유일한 ID들, 사용 규칙들 등을 포함할 수 있다. 헤더는 파일의 개시부, 파일 내의 프레임들의 개시부 또는 파일 개시부 및 프레임들의 개시부 모두에만 존재할 수 있다. 프레임들은 MPEG 오디오 및 비디오와 같은 압축 디지털 매체에 공유된다. 보다 구체적으로는, MP3 데이터에 있어서, 헤더는 헤더로서의 소정의 MPEG 표준 라벨들, 에러 보정 및 사이드 정보를 포함할 수 있다. 또한, 컨텐트가 프레임들 또는 헤더를 포함하지 않으면, 이러한 데이터는 새로운 구성 파일 포맷 내에 용이하게 형성될 수 있다.

도 33a는 스크램블링 프로세스의 개요를 도시한다. 파일이 글로벌 헤더 또는 동기화(sync) 코드들이 없는 공지된 크기의 프레임들만을 가지면, 헤더들은 스크램블링 단계(박스 110) 중에 파악되며 스킵된다(박스 105). 달리 말해, 동기화 코드를 확인할 필요가 없다(박스 100). 스크램블링 단계는 비헤더 컨텐트의 일부 또는 모두를 스크램블링 할 수 있다. 파일이 추가의 동기화 코드들에 의해 프레임들로 분열되면, 프레임들을 규정하는 동기화 코드들이 발견되며(박스 100), 헤더 정보는 스킵되며(박스 105), 컨텐트는 스크램블링된다(박스 110). 통상적으로, 헤더는 동기화 코드가 데이터 내에 또한 임의적으로 발생될 때, 다음 동기화 코드를 파악하는 것을 보조하는 프레임 크기에 대한 정보를 포함할 수 있다. 재차, 스크램블링 단계는 비헤더 컨텐트의 일부 또는 모두를 스크램블링 할 수 있다.

스크램블링 단계는 종래 사용된 방법으로 구성될 수 있다. DES or RSA와 같은 표준의 현대식 부호화가 탁월한 선택이다. 이러한 부호화에 의해, 강제적으로 하나의 파일을 스크램블링할 수는 있을지라도, 다른 파일은 동일한 키를 사용할 때조차 안전하게 유지될 수 있다. 다른 스크램블링 옵션들은 승산, 가산, 감산 또는 익스클루시브-오어(XOR)와 같은 PN 시퀀스를 갖는 단순한 수학적 연산을 포함할 수 있다. 제산(division)은 신중하게 사용되어야 하는데, 이는 한정된 비트 길이 제산의 부정확한 특성에 기인하여 비트 에러를 발생시킬 수 있기 때문이다.

도 33b는 디스크램블링 프로세스의 개요를 도시한다. 디스크램블링은 스크램블링의 역이며, 스크램블링된 컨텐트 비트들만이 디스크램블링되어야 한다. 파일이 글로벌 헤더 또는 동기화(sync) 코드가 없는 공지된 크기의 프레임들만을 가지면, 헤더들은 디스크램블링 프로세스(박스 106) 중에 파악되며 스킵된다(박스 155). 달리말해, 동기화 코드를 확인할 필요가 없다(박스 150). 파일이 동기화 코드에 의해 프레임들로 분열되면, 프레임들을 규정하는 동기화 코드들이 발견되며(박스 150), 헤더 정보는 스킵되며(박스 155), 프레임 내의 잔류하는 컨텐트의 일부 또는 모두가 디스크램블링된다(박스 160). 통상적으로, 헤더는 동기화 코드가 유일하지 않을 수 있기 때문에 데이터 내에 발생되는 동기화 코드의 파악을 보조하는 프레임 크기에 대한 정보를 포함한다. 디스크램블링 단계는 스크램블링된 것에 의존하여 비헤더 컨텐트의 일부 또는 모두를 디스크램블링할 수 있다.

디스크램블러는 스크램블러에 의해 사용된 기능의 역을 사용해야 한다. 표준의 현대식 부호화에 의해 스크램블링될 때, 디스크램블러는 복호화 키를 필요로 하며, 상기 키는 부호화 키와는 상이하다. 수학적 연산에서, 감산 및 가산은 반전되며, XOR은 자신의 역이며, 제산은 승산의 역이다. 제산은 디스크램블링에서는 사용될 수 있는데, 이는 제산자가 스크램블링 프로세스의 승산자이기 때문에 나머지가 없다는 것이 이미 공지되어 있기 때문이다.

스크램블링 및 디스크램블링 모두에서, 키는 트랙이 노래 또는 영화로 구성될 수 있는 전체 컨텐트 트랙 및 다수의 프레임에 대해 동일하게 잔류하도록 기대된다. 따라서, 브로드캐스트들에 있어서, 키는 각각의 트랙에서 변화될 수 있으며, 암호학 기술 분야의 숙련자들에게는 키를 전송하는 다수의 방법이 공지되어 있다. PN 시퀀스들을 사용할 때, 하기에 설명하는 바와 같이, PN 시퀀스를 위한 키는 함수 발생기이며, 각각의 MP3 노래에 대해 변화되지 않는다, 즉 트랙으로서 규정된다. 함수 발생기는 각각의 시간마다 동일한 랜덤 시퀀스를 발생시키며, 암호학 기술 분야에 공지되어 있다는 것을 주목해야 한다. 선택적으로, 노래와 같은 모든 컨텐트 트랙은 한정된 글로벌 리스트로부터 하나 이상의 키를 사용할 수 있다.

도 34a는 스크램블링 또는 디스크램블링 프로세스의 예를 위한 의사 코드를 도시한다. 본 예에서, 컨텐트는 동기화 코드를 개시하는 프레임들을 포함하며, 헤더가 각각의 프레임에 존재한다. XOR 기능의 역은 그 자신이기 때문에, 스크램블링 및 디스크램블링 프로세스를 위한 의사 코드는 동일하다.

이러한 단순한 예에 의해 스크램블링 또는 디스크램블링된 컨텐트는 Layer III(MP3) 또는 AAC와 같은 MPEG 오디오 데이터를 포함할 수 있다. MPEG 오디오 동기화 코드는 '1111 1111 1111'이다. 이러한 접근들의 장점은 다양하다. 예를 들면 휴대용 플레이어는 사용자가 노래를 재생하려고 하기 전에, 노래의 길이, 아티스트, 해결 등에 대한 정보를 신속하게 표시할 수 있다. 마찬가지로, 헤더는 플레이어가 재생 전에 검사되도록 요구되는 저작권 정보를 포함할 수 있다.

프로세스는 컨텐트의 개시부에서 시작된다(박스 200). 다음, 통상 컨텐트의 첫 번째의 수 비트들(few bits)인 동기화 코드가 발견된다(박스 205). 다음, 동기화 코드 이후의 데이터로부터 자신의 크기를 판독할 수 있는 헤더 데이터가 스킵된다(박스 210). 다음, M 컨텐트 비트들 및 PN 시퀀스의 M 비트들을 갖는 XOR 연산을 사용하여 프레임에 대한 M 컨텐트 비트들이 스크램블링된다(박스 215). 도 34b는 XOR 기능을 위한 입력 및 출력을 보여준다. 다음, 컨텐트는 다른 프레임이 존재하는지를 확인하기 위해 검사된다(박스 220). 다른 프레임이 존재하면, 프로세스는 다음 동기화 코드가 파악되는 박스(205)에서 계속된다. 통상적으로, 프레임의 크기는 다음 동기화 코드를 탐색하는 것을 보조하는 프레임의 헤더로부터 판독될 수 있다. 컨텐트가 남아있지 않으면, 프로세스는 종료된다(박스 225).

본 예에서, M의 크기는 공격자의 의도가 원본 컨텐트를 획득하는 것인 난폭한 공격에 대한 견고성을 결정한다. M이 클수록, 스크램블링된 컨텐트의 공격에 대한 견고성이 보다 높아진다. 그러나 M이 작을수록, 스크램블링 및 디스크램블링 프로세스들이 더욱 효율적이 된다. M은 에러 보정에 의해 교정될 수 있는 비트들의 수보다 크며 프레임에 대한 비헤더 컨텐트의 수보다 작은 임의의 수일 수 있다.

프레임 내에서 스크램블링되는 M 비트들의 위치가 인식되어야 하며, 컨텐트의 강도에 대해 임계적인 비트들을 포함하여야 한다. 상기 비트들은 헤더 이후의 M 비트들일 수 있다. 그러나 MP3 데이터에서, 프레임 데이터는 헤더 이후에 개시되지 않을 수 있다. 이 경우, 스크램블링된 비트들은 프레임을 위한 데이터의 제 1의 M 비트들일 수 있다. 상기 비트들은 오디오 비트들의 할당을 결정하며, 파일의 보전에 대한 임계값이다.

도 35는 스크램블링 또는 디스크램블링 프로세스를 실시하는데 사용되는데 적합한 하드웨어를 도시한다. 상기 하드웨어는 논리 프로세서(300)와 메모리(310)를 포함한다. 상기 논리 프로세서는 상기 프로세스를 위한 연산 및 논리를 수행한다. 상기 논리 프로세서(300)는 디지털 신호 프로세서(DSP), 일반적인 이용의 중앙 처리 유닛(CPU) 또는 매체 프로세서들을 포함하는 특정된 CPU 또는 주문형 반도체(ASIC)의 등가물로서 정의될 수 있다. 사용 가능한 DSP 칩은 텍사스 인스트루먼츠 TMS320 제품 중 하나이다. CPU는 인텔 펜티엄 제품 또는 모토로라/IBM 파워PC 제품 중 하나를 포함할 수 있다.

ASIC는 상기 의사 코드 및 설명에 의해 공지된 기술 분야의 숙련자들에 의해 용이하게 설계될 수 있다. 논리 프로세서(300)를 제어하기 위한 코드의 디자인은 상기 의사 코드 및 설명에 의해 공지된 기술 분야의 숙련자들에게는 또한 단순한 것이다. 메모리(310)는 디지털 프로세서를 사용할 때 RAM을 포함할 수 있으며, 프로그램 및 다른 필요한 변수들을 저장하는데 사용된다.

결론

다양한 실시예들을 참조하여 본원의 기술의 원리들을 설명하고 도시하였지만, 이러한 원리들로부터 일탈하지 않는 장치 및 상세의 수정이 가능하다는 것은 명백하다.

예를 들면, 상기 실시예들 중 다수는 대상물 또는 컨텐트를 식별하기 위해 워터마크 기술을 사용하였지만, 이는 필수적인 것은 아니다. 다른 마킹 기술들이 적합한 상황들에 사용될 수 있다.

유사하게, 소정의 프로세스들은 사용자와 관련된 소정의 위치에서 수행되는 것으로 설명하였지만, 이러한 프로세스들의 위치는 일반적으로 특정적인 것은 아니다. 즉, 태스크들이 상황에 가장 적합되는 프로세싱 디바이스들 중에 할당될 수 있다(보안 문제가 적합하게 처리되는 한).

이미지들 및 비디오에 관련된 응용들에 의해 참조하였지만, 예시적인 오디오 응용들에 초점을 맞추는 것은 이러한 사실을 모호하게 할 수 있다. 따라서, 상술한 기술들은 오디오 이외의 다른 형태의 매체에 동일하게 응용 가능하다는 것을 상기해야 한다.

상술한 실시예는 단일 샘플들의 값들을 변화시키는 것으로서 설명하였지만, 다른 실시예들에서, 예를 들면 변조가 존재하는 워터마크의 내구성을 증가시키기 위해 복수의 이웃의 샘플들의 값들을 변화시키는 것이 바람직할 수도 있다.

유사하게, 상술한 실시예들은 보조 데이터가 컨텐트에 삽입되는 것으로서 설명하였지만, 보조의 표시 형태는 상세히 설명하지 않았다. 몇몇 실시예들에서는, N 비트들의 유효 부하(payload)가 M 비트들로서 부호화될 수 있으며, 여기서 M>N 이다(즉, 부분적인 또는 완전한 러던던시를 갖는다). 러던던시는 컨텐트를 통한 N 비트들의 유효 부하의 반복, 견고성 및/또는 에러 보정을 제공하기 위한 N 비트들의 BCH-코딩, 터보-코딩, 길쌈-코딩 및 CRC 또는 ECC 코드들 등을 포함할 수 있다.

상술한 실시예들은 다수의 부품의 시스템들이지만, 그의 개별 부품들에도 신규성이 존재한다는 것을 인식할 수 있을 것이며, 이러한 부품들은 다른 시스템들 및 디바이스들에 또한 사용될 수 있다.

상술한 실시예들의 소자들 및 특징들의 특정 조합은 단지 예시적인 것이며, 참조 및 관련 문헌들을 참조하여 다른 실시예들에 의한 수정 및 대체도 고려할 수 있다.

상술한 원리들 및 특징들이 응용될 수 있는 광범위한 실시예의 관점에서, 상술한 기술은 단지 예시적인 것이며, 본 발명의 범위를 한정하는 것은 아니라는 것은 명백하다. 오히려, 본 출원인은 이러한 모든 수정들은 하기의 청구범위 및 그의 등가물의 범위 및 정신에 의해 수행될 수 있다는 것을 주장한다.

도면의 간단한 설명

도 1은 예시적 삽입 기술에서 사용되는 작업들을 도시하는 흐름도.

도 2는 도 1의 방법에 사용하는 데이터 삽입 또는 검색에 사용되는 장치를 도시하는 블록도.

도 3은 예시적 복호화 기술에서 사용되는 작업들을 도시하는 흐름도.

도 4는 예시적 제 1 실시예의 작업을 그래픽적으로 도시하는 도면.

도 5는 점선들이 보조 데이터와의 상호작용을 나타내고 있는, 예시적 제 1 실시예에 따른 데이터 삽입을 도시하는 흐름도.

도 6은 점선들이 보조 데이터와의 상호작용을 나타내고 있는, 데이터의 복호화를 도시하는 흐름도.

도 7은 예시적인 제 2 실시예의 작업을 그래픽적으로 도시하는 도면.

도 8은 점선들이 보조 데이터와의 상호작용을 도시하고 있는, 예시적인 제 2 실시예에 따른 데이터 삽입을 도시하는 도면.

도 9는 점선들이 보조 데이터와의 상호 작용을 도시하고 있는, 데이터 복호화를 도시하는 흐름도.

도 10은 디지털 압축 기술들과 연관된 예시적 실시예의 양태들을 도시하는 도면.

도 11a 및 도 11b는 예시적 실시예에 따른 삽입 및 검색 장치를 도시하는 두 개의 블록도.

도 12는 데이터 삽입을 위한 도 2의 장치의 예시적 실시예를 도시하는 도면.

도 13은 데이터 검색을 위한 도 2의 장치의 예시적 실시예를 도시하는 도면.

도 14는 공격 저항성에 관한 설명에 참조되는 가능화(enabling) 프로세스를 위한 블록도.

도 15는 등록 프로세스를 위한 블록도를 도시하는 도면.

도 16은 동적 로킹이 보조 데이터의 복제를 방지하는 방식을 예시하는 도면.

도 17은 익스클루시브-오어(XOR) 기능을 위한 입력 및 출력을 도시하는 도면.

도 18a는 보조 데이터의 삽입 및 동적 로킹의 프로세스의 개요를 도시하는 도면.

도 18b는 보조 데이터의 검색 및 동적 언로킹의 프로세스의 개요를 도시하는 도면.

도 19a는 국부적으로 마스킹된 삽입 데이터를 위한 동적 로킹의 변조 단계를 도시하는 도면.

도 19b는 펄스 폭 변조(PWM) 삽입 데이터를 위한 동적 로킹의 변조 단계를 도시하는 도면.

도 19c는 PN 시퀀스들에 기반한 실시예들을 위한 동적 로킹의 변조 단계를 도시하는 도면(보조 데이터는 약자 aux.로 도시됨).

도 20a는 헤더 블록들을 사용하는 보조 데이터 삽입 및 로킹을 위한 흐름도 형태로 의사코드를 도시하는 도면.

도 20b는 헤더 블록을 사용하는 보조 데이터의 검색 및 언로킹을 위한 흐름도 형태로 의사코드를 도시하는 도면.

도 21은 예시적 활용들의 이면의 기본 프로세스를 도시하는 도면(점선 박스들은 선택적이다. 쇄선 박스들은 유사한 항목들을 그룹으로 분류하고 있다. 그 외에도, 비록 세 개의 키 위치들이 도시되어 있지만, 일반적으로 단지 하나의 키가 사용되고, 그 위치는 활용의 요구조건들에 따른다. 마지막으로, 약자 ID가 사용되며, 이는 대부분 식별기를 지칭하지만, 소정의 보조 정보를 지칭할 수도 있다).

도 22는 이들 견고한 데이터 삽입 기술들을 위해 사용될 수 있는 장치들을 도시하는 도면.

도 23은 동적 로킹을 위한 도 22의 장치의 실시예를 도시하는 도면.

도 24는 동적 언로킹을 위한 도 22의 장치의 실시예를 도시하는 블록도.

도 25는 자동 ID 관리 프로세스의 개요도.

도 26은 예시적 자동 ID 관리 프로세스를 실행하기 위한 의사 코드를 도시하는 도면.

도 27은 자동 ID 관리를 실행하기 위한 장치를 도시하는 도면.

도 28은 도 27의 장치를 포함하는 휴대용 MP3 오디오 플레이어를 도시하는 도면.

도 29는 두 개의 워터마크들을 사용하는 프로세스의 개요도.

도 30은 도 29의 삽입 프로세스를 위한 의사 코드를 도시하는 도면.

도 31은 도 29의 검색 프로세스를 위한 의사 코드를 도시하는 도면.

도 32는 도 29의 프로세스와 연관되어 사용될 수 있는 장치를 도시하는 도면.

도 33a는 스크램블링 프로세스의 개요를 도시하는 도면(점선 박스들은 선택적임).

도 33b는 디스크램블링 프로세스의 개요를 도시하는 도면(점선 박스들은 선택적임).

도 34a는 예시적 스크램블링 또는 디스크램블링 프로세스를 위한 의사코드를 도시하는 도면.

도 34b는 익스클루시브-오어(XOR) 기능을 위한 입력 및 출력을 도시하는 도면.

도 35는 스크램블링 또는 디스크램블링 프로세스들을 수행하기 위한 예시적 장치를 도시하는 도면.

도 36은 열화 및 복구 프로세스의 개요도.

도 37은 도 36의 열화 및 복구 프로세스를 위한 의사코드를 도시하는 도면.

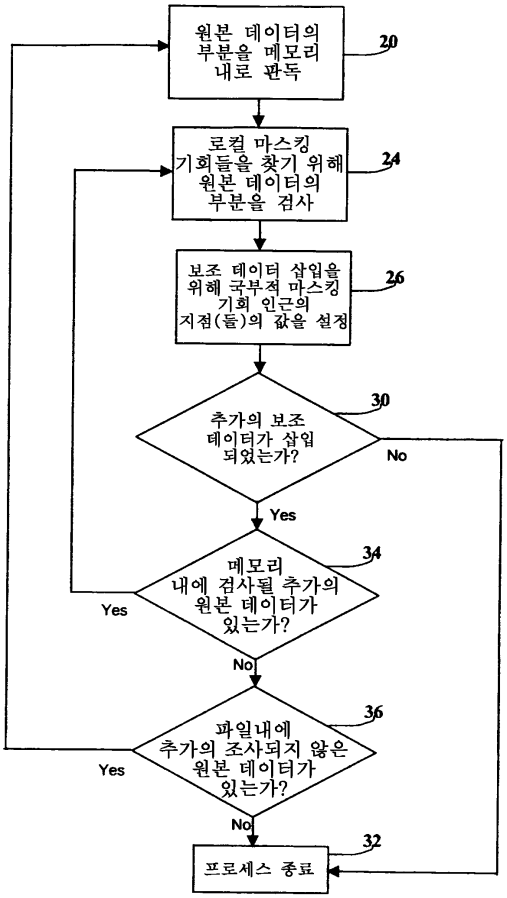
도 38은 임계값 교차점을 사용하고, 단지 그 다음 지점만을 조절하는 열화 및 복구 프로세스의 단순하고 효과적인 예를 도시하는 도면.

도 39는 도 38의 열화 및 복구 프로세스를 위한 의사 코드를 도시하는 도면.

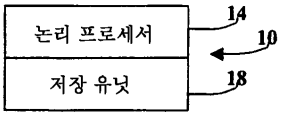
도 40은 도 36 내지 도 39의 프로세스를 수행하는데 적합한 장치의 개요를 도시하는 도면.

도면

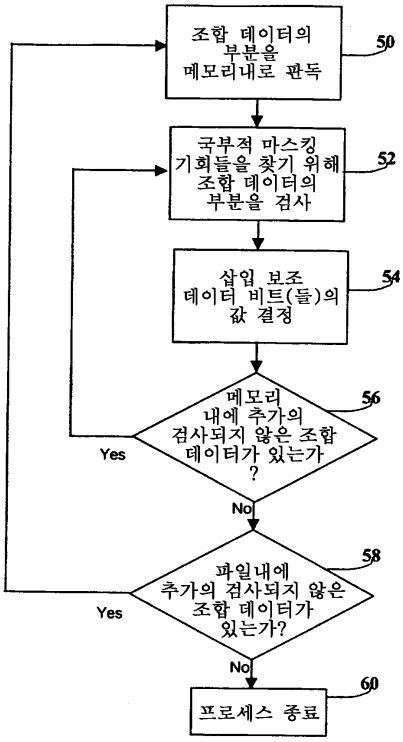
도면1


원본 데이터의 부분을 메모리 내로 판독
20
로컬 마스킹 기회들을 찾기 위해 원본 데이터의 부분을 검사
24
보조 데이터 삽입을 위해 국부적 마스킹 기회 인근의 지점(들)의 값을 설정
26
추가의 보조 데이터가 삽입 되었는가?
30
No
Yes
메모리 내에 검사될 추가의 원본 데이터가 있는가?
34
Yes
No
파일내에 추가의 조사되지 않은 원본 데이터가 있는가?
36
Yes
No
프로세스 종료
32

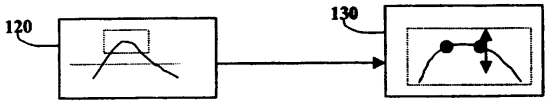
도면2


논리 프로세서
14
10
저장 유닛
18

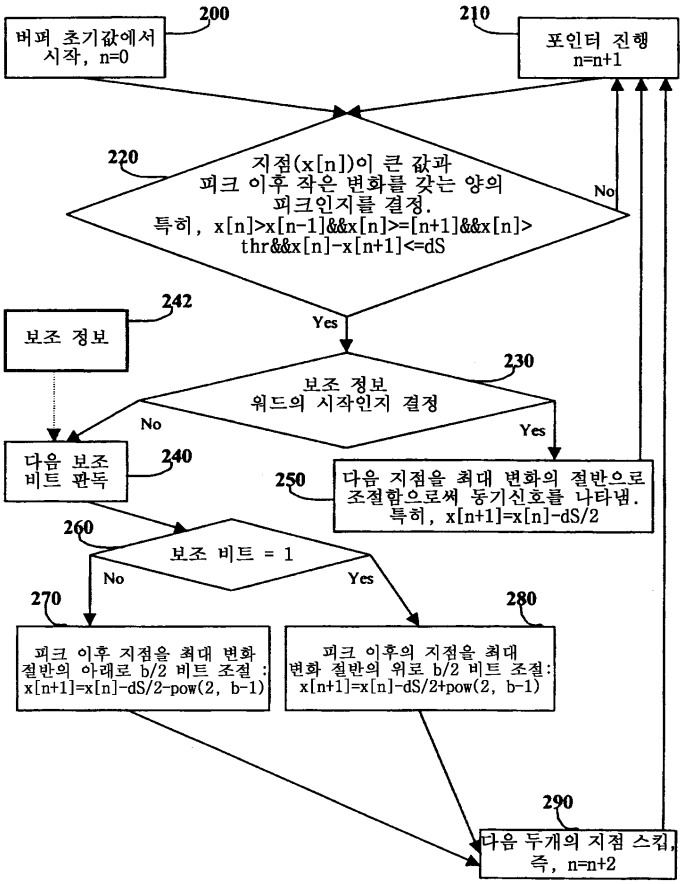
도면3


조합 데이터의 부분을 메모리내로 판독
50
국부적 마스킹 기회들을 찾기 위해 조합 데이터의 부분을 검사
52
삽입 보조 데이터 비트(들)의 값 결정
54
메모리 내에 추가의 검사되지 않은 조합 데이터가 있는가 ?
56
Yes
No
파일내에 추가의 검사되지 않은 조합 데이터가 있는가?
58
Yes
No
프로세스 종료
60

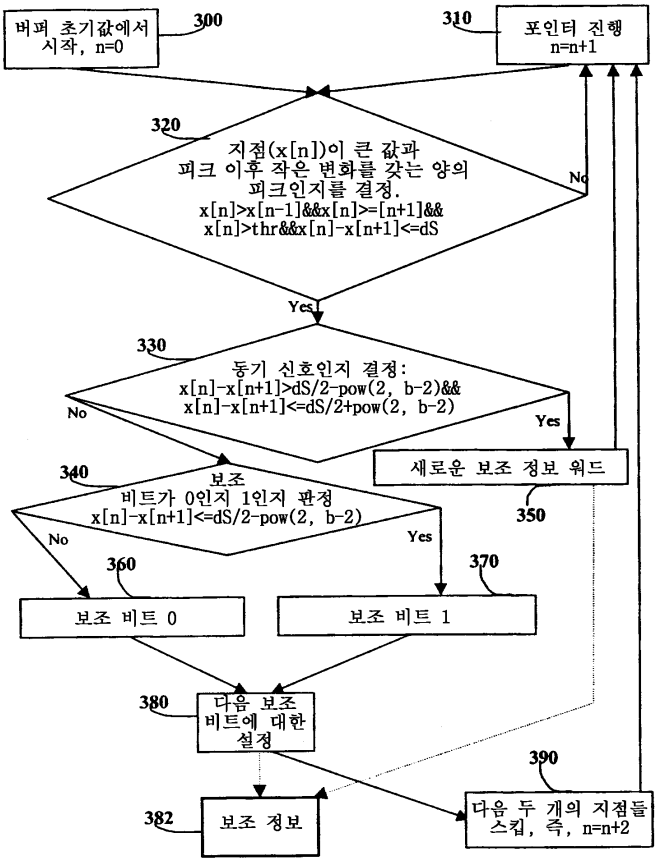
도면4


120
130

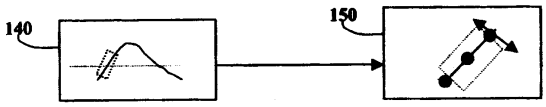
도면5


200
버퍼 초기값에서 시작, n=0
210
포인터 진행 n=n+1
220
지점(x[n])이 큰 값과 피크 이후 작은 변화를 갖는 양의 피크인지를 결정. 특히, x[n]>x[n-1]&&x[n]>=[n+1]&&x[n]>thr&&x[n]-x[n+1]<=dS
No
Yes
242
보조 정보
230
보조 정보 워드의 시작인지 결정
No
Yes
다음 보조 비트 판독
240
250
다음 지점을 최대 변화의 절반으로 조절함으로써 동기신호를 나타냄. 특히, x[n+1]=x[n]-dS/2
260
보조 비트 = 1
No
Yes
270
피크 이후 지점을 최대 변화 절반의 아래로 b/2 비트 조절 : x[n+1]=x[n]-dS/2-pow(2, b-1)
280
피크 이후의 지점을 최대 변화 절반의 위로 b/2 비트 조절: x[n+1]=x[n]-dS/2+pow(2, b-1)
290
다음 두개의 지점 스킵, 즉, n=n+2

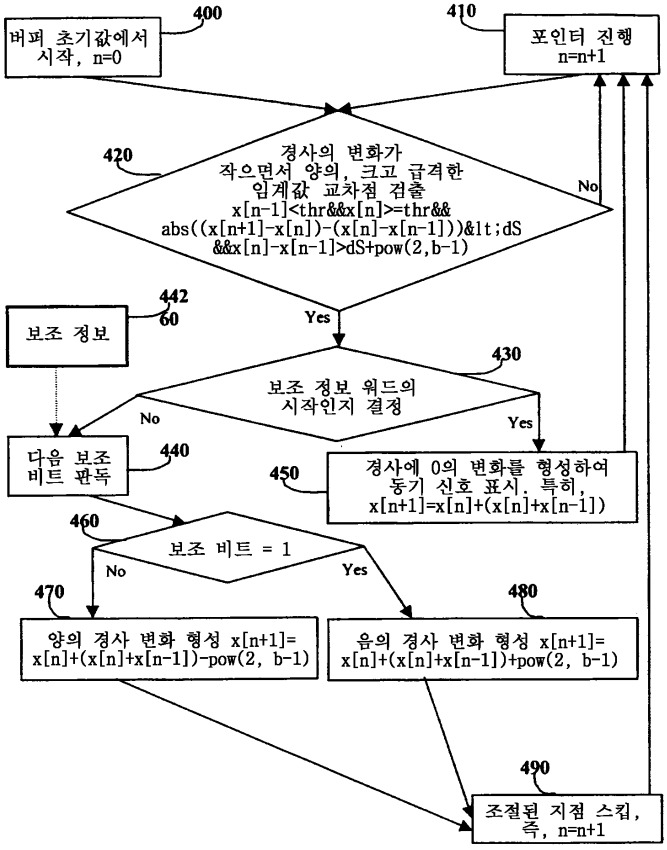
도면6


버퍼 초기값에서 시작, n=0
300
310
포인터 진행 n=n+1
320
지점(x[n])이 큰 값과 피크 이후 작은 변화를 갖는 양의 피크인지를 결정. x[n]>x[n-1]&&x[n]>=[n+1]&& x[n]>thr&&x[n]-x[n+1]<=dS
No
Yes
330
동기 신호인지 결정: x[n]-x[n+1]>dS/2-pow(2, b-2)&& x[n]-x[n+1]<=dS/2+pow(2, b-2)
No
Yes
새로운 보조 정보 워드
350
340
보조 비트가 0인지 1인지 판정 x[n]-x[n+1]<=dS/2-pow(2, b-2)
No
Yes
360
370
보조 비트 0
보조 비트 1
380
다음 보조 비트에 대한 설정
382
보조 정보
390
다음 두 개의 지점들 스킵, 즉, n=n+2

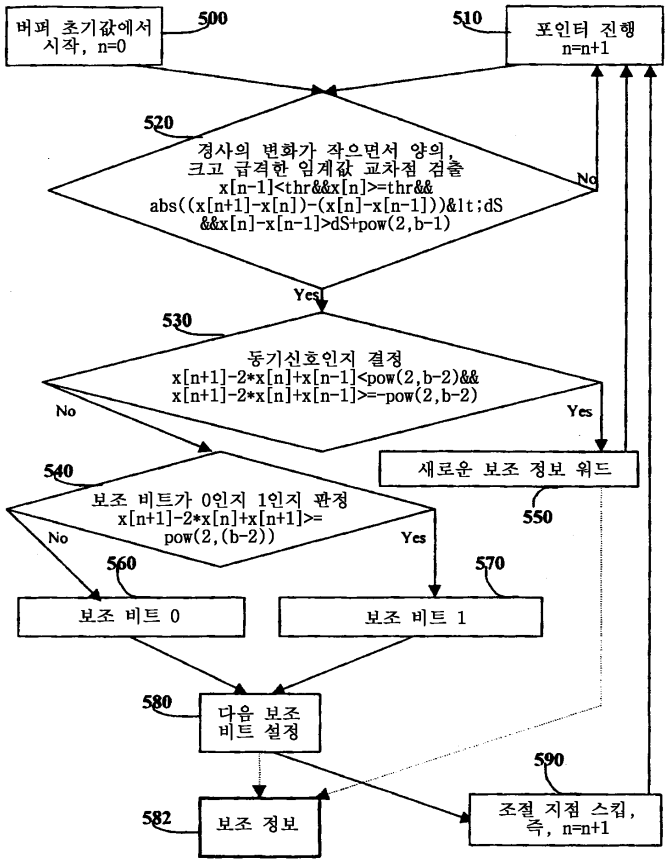
도면7


140
150

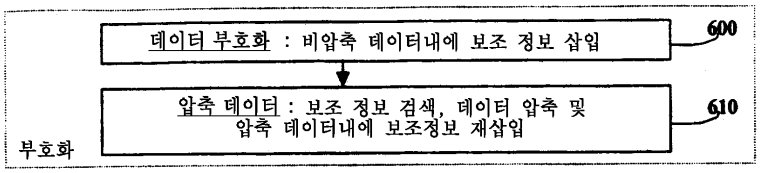
도면8


400
버퍼 초기값에서 시작, n=0
410
포인터 진행 n=n+1
420
경사의 변화가 작으면서 양의, 크고 급격한 임계값 교차점 검출
x[n-1]<thr&&x[n]>=thr&&
abs((x[n+1]-x[n])-(x[n]-x[n-1]))<dS
&&x[n]-x[n-1]>dS+pow(2,b-1)
No
Yes
442
60
보조 정보
430
보조 정보 워드의 시작인지 결정
No
Yes
다음 보조 비트 판독
440
450
경사에 0의 변화를 형성하여 동기 신호 표시, 특히, x[n+1]=x[n]+(x[n]+x[n-1])
460
보조 비트 = 1
No
Yes
470
양의 경사 변화 형성 x[n+1]= x[n]+(x[n]+x[n-1])-pow(2, b-1)
480
음의 경사 변화 형성 x[n+1]= x[n]+(x[n]+x[n-1])+pow(2, b-1)
490
조절된 지점 스킵, 즉, n=n+1

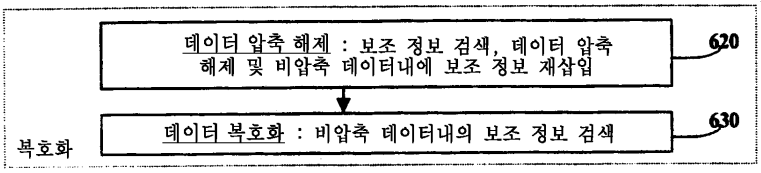
도면9


500
버퍼 초기값에서 시작, n=0
510
포인터 진행 n=n+1
520
경사의 변화가 작으면서 양의, 크고 급격한 임계값 교차점 검출
x[n-1]<thr&&x[n]>=thr&&
abs((x[n+1]-x[n])-(x[n]-x[n-1]))<dS
&&x[n]-x[n-1]>dS+pow(2,b-1)
No
Yes
530
동기신호인지 결정
x[n+1]-2*x[n]+x[n-1]<pow(2,b-2)&&
x[n+1]-2*x[n]+x[n-1]>=-pow(2,b-2)
No
Yes
새로운 보조 정보 워드
550
540
보조 비트가 0인지 1인지 판정
x[n+1]-2*x[n]+x[n+1]>=
pow(2,(b-2))
No
Yes
560
570
보조 비트 0
보조 비트 1
580
다음 보조 비트 설정
582
보조 정보
590
조절 지점 스킵, 즉, n=n+1

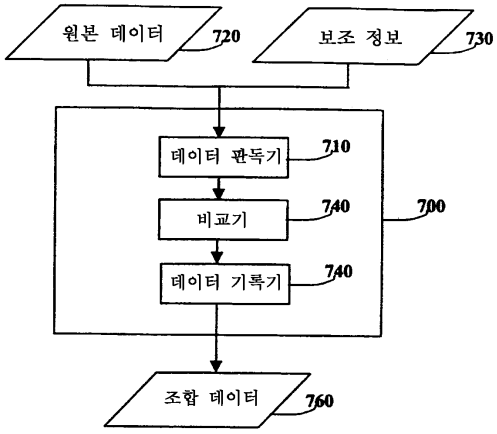
도면10a



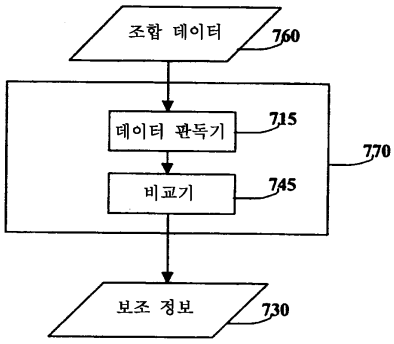
도면10b



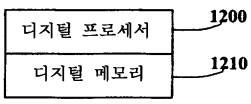
도면11a



도면11b



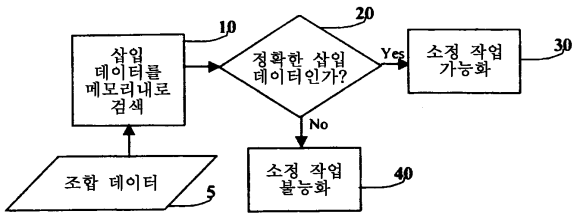
도면12



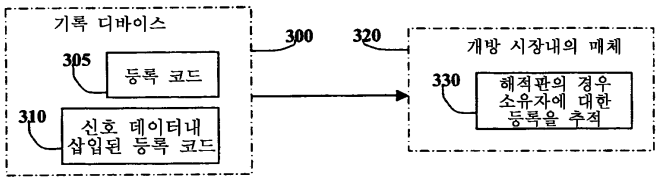
도면13

A/D 변환기	샘플 및 보유	D/A 변환기
비교기	PLC	지연

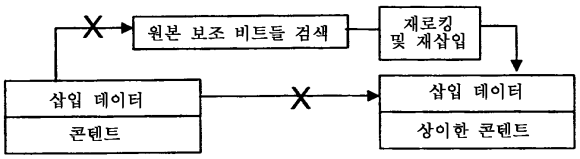
도면14



도면15



도면16

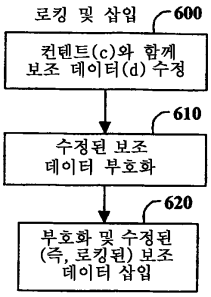


도면17

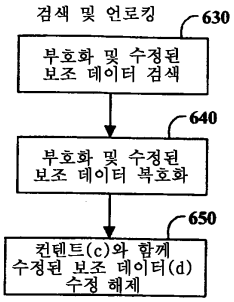
XOR

d	c	f(d,c)
1	1	0
1	0	1
0	1	1
0	0	0

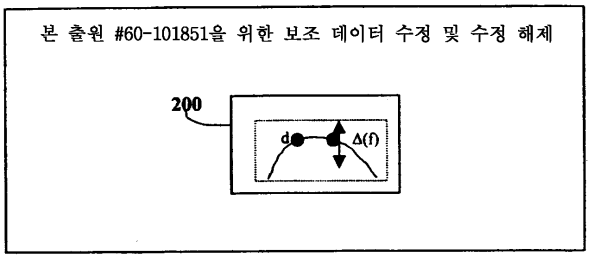
도면18a



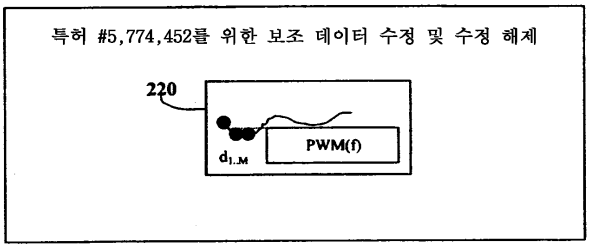
도면18b



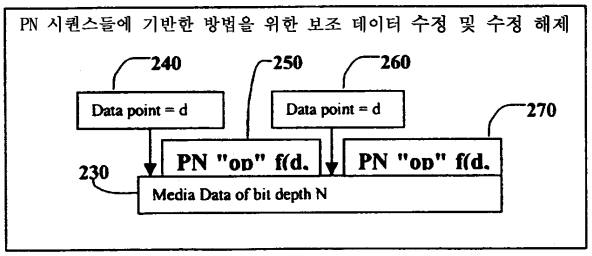
도면19a



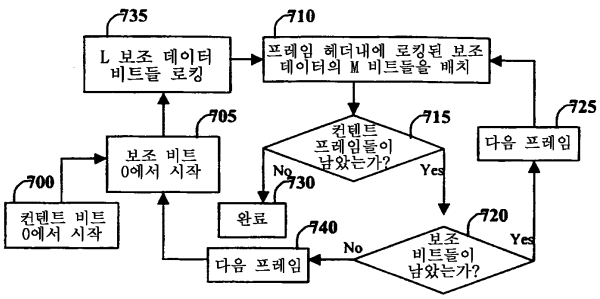
도면19b



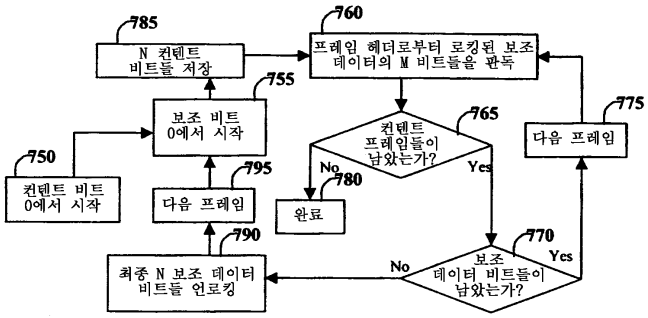
도면19c



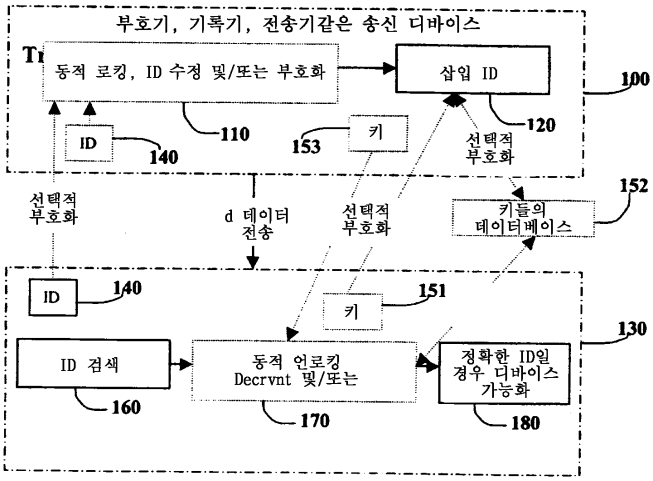
도면20a



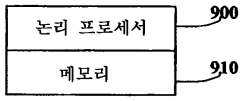
도면20b



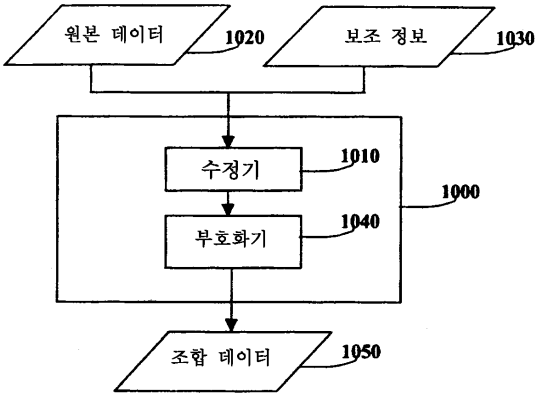
도면21



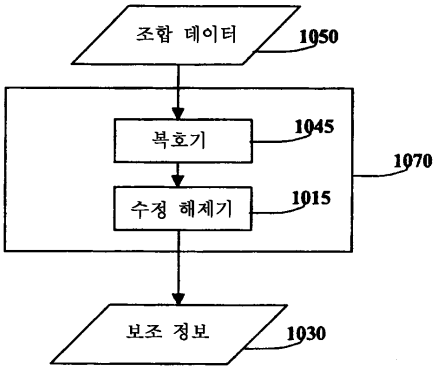
도면22



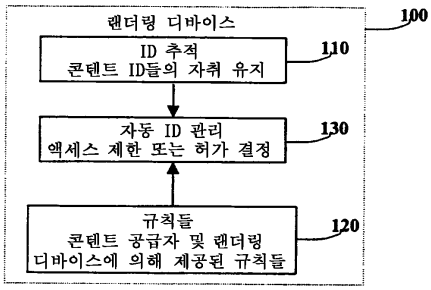
도면23



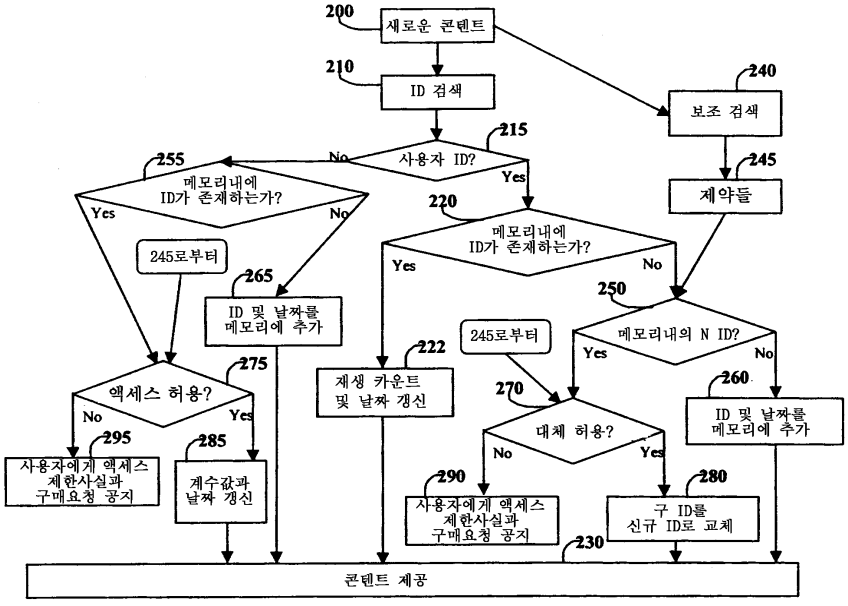
도면24



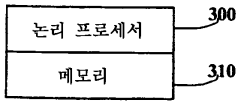
도면25



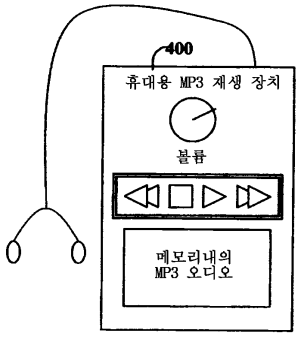
도면26



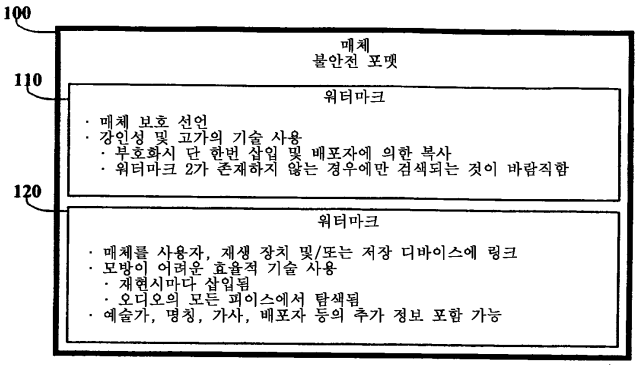
도면27



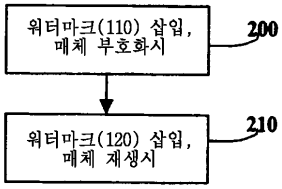
도면28



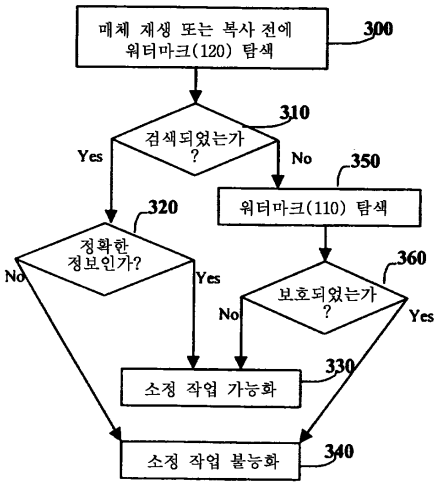
도면29



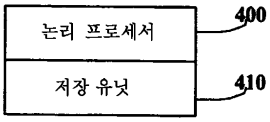
도면30



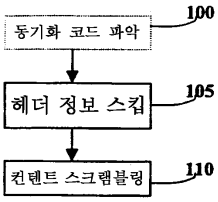
도면31



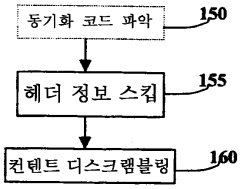
도면32



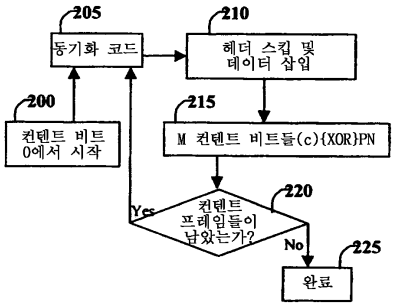
도면33a



도면33b



도면34a

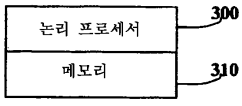


도면34b

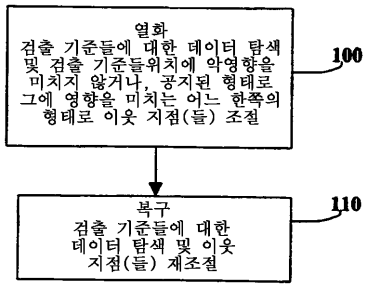
XOR

c	PN	f(c,PN)
1	1	0
1	0	1
0	1	1
0	0	0

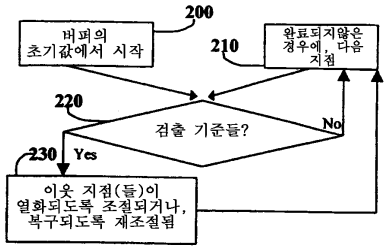
도면35



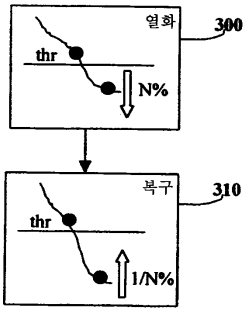
도면36



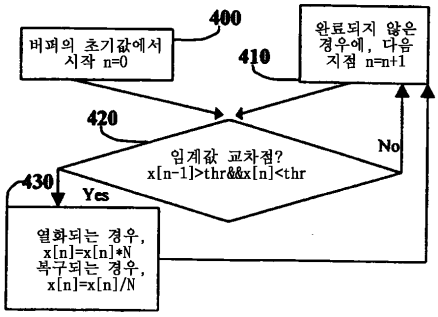
도면37



도면38



도면39



도면40