(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0133373
(43) 공개일자 2010년12월21일

(51) Int. Cl.
G06F 21/00 (2006.01)
(21) 출원번호 10-2010-7019852
(22) 출원일자(국제출원일자) 2009년02월11일
심사청구일자 없음
(85) 번역문제출일자 2010년09월06일
(86) 국제출원번호 PCT/US2009/033841
(87) 국제공개번호 WO 2009/102819
국제공개일자 2009년08월20일
(30) 우선권주장
61/027,757 2008년02월11일 미국(US)
(뒷면에 계속)

(71) 출원인
마킹, 애론
미국 오레곤 97219 포틀랜드 사우쓰웨스트 83 드라이브 10555
겔러, 케네스
미국 캘리포니아 90077 로스 앤젤레스 린다 플로라 드라이브 2070
(72) 발명자
마킹, 애론
미국 오레곤 97219 포틀랜드 사우쓰웨스트 83 드라이브 10555
겔러, 케네스
미국 캘리포니아 90077 로스 앤젤레스 린다 플로라 드라이브 2070
(74) 대리인
특허법인무한

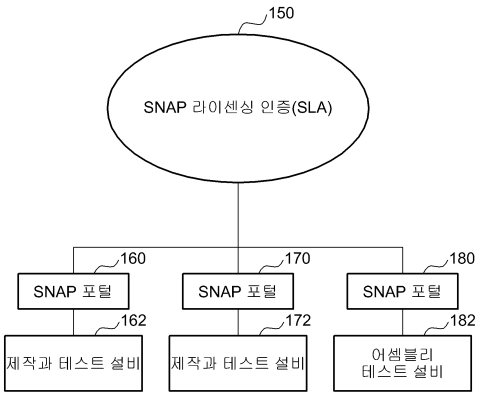
전체 청구항 수 : 총 45 항

(54) 간단 비자율 피어링 환경 워터마킹, 인증 및 바인딩

(57) 요 약

안전 비자율 피어링(SNAP; Secure Non-autonomous Peering) 시스템은 계층적 디지털 워터마킹 스킴, 중앙 라이센싱 인증, 인증된 제작자와 어셈블러를 포함한다.

대 표 도 - 도12



(30) 우선권주장
61/082,404 2008년07월21일 미국(US)
61/096,686 2008년09월12일 미국(US)
61/148,295 2009년01월29일 미국(US)

특허청구의 범위

청구항 1

디지털로 워터마크된 미디어 파일을 획득하는 단계;

메모리 장치의 메모리 부분에 상기 파일을 기록하는 단계;

상기 메모리 부분의 상기 미디어 파일과 상기 메모리 부분의 결함의 위치의 로그 파일을 생성하는 단계; 및

상기 메모리의 상이한 부분에 상기 로그 파일을 기록하는 단계;

를 포함하는 메모리 장치에 미디어 콘텐트를 프로그래밍하는 방법.

청구항 2

제1항에 있어서,

로그 파일을 생성하는 단계는, 상기 메모리의 부분에 위치한 상기 미디어 파일과 상기 메모리 부분의 상기 결함의 맵을 생성하는 단계를 포함하는 방법.

청구항 3

제1항에 있어서,

상기 로그 파일을 생성하는 단계는, 메모리에 로그 파일을 기록하는 단계 전 상기 로그 파일을 디지털로 서명하고 암호화하는 단계를 포함하는 방법.

청구항 4

호스트 장치에서 미디어 콘텐트를 저장하는 장치로 연결하는 단계;

상기 장치로부터 로그 파일을 획득하는 단계;

호스트 제어기가 복호화한 로그 파일을 생성하도록 호스트 제어기에서 상기 로그 파일을 복호화하고, 상기 디지털 서명을 인증하는 단계;

상기 호스트 제어기 복호화한 로그 파일을 메모리 제어기가 복호화한 로그 파일과 비교하는 단계; 및

매치에 따라 상기 미디어 콘텐트에 대한 접근을 허용하는 단계;

를 포함하는 미디어 콘텐트 접근 방법.

청구항 5

제4항에 있어서,

미스매치를 결정할 때, 불능화(diabling) 장치의 하나가 미디어 콘텐트 저장, 실행 정지, 보안 시스템의 갱신과 상기 미디어 콘텐트의 비인증의 교체의 청구를 실행하는 단계를 더 포함하는 미디어 콘텐트 접근 방법.

청구항 6

제4항에 있어서,

최신 업데이트된 갱신 정보를 결정하기 위해 미디어 콘텐트를 저장하는 장치의 갱신 정보와 연관된 시간과 상기 호스트 장치의 갱신 정보에 연관된 시간을 비교하는 단계; 및

결정에 따라 상기 호스트 장치 또는 미디어 콘텐트를 저장하는 장치 중 하나를 최신 업데이트된 갱신 정보로 업데이트하는 단계;를 더 포함하는 미디어 콘텐트 접근 방법.

청구항 7

제4항에 있어서,

호스트 장치에서 연결하는 단계는, 개인 컴퓨터, 셋톱박스, 미디어 플레이어, 텔레비전, 키오스크(kiosk) 또는 휴대용 장치 중 하나에서 연결하는 것을 포함하는 미디어 콘텐트 접근 방법.

청구항 8

제어기 메모리 부분에 저장된 제어기 식별자를 가지는 제어기; 및

상기 제어기와 통신하는 적어도 하나의 메모리 성분 장치;를 포함하고,

메모리 장치는 장치 메모리 부분에 저장된 칩 식별자를 가지는 메모리 장치.

청구항 9

제8항에 있어서,

상기 제어기는 제어기 메모리 부분에 저장된 칩셋 인증 수를 포함하는 메모리 장치.

청구항 10

제8항에 있어서,

상기 메모리 장치는 장치 메모리 부분에 저장된 하드웨어 인증 코드를 포함하는 메모리 장치.

청구항 11

제8항에 있어서,

상기 메모리 장치는 장치 메모리 부분에 저장된 칩셋 인증 수를 포함하는 메모리 장치.

청구항 12

제8항에 있어서,

상기 메모리 장치는 장치 메모리 부분에 저장된 미디어 파일을 포함하는 메모리 장치.

청구항 13

컴퓨터에서 제작자로부터 메모리 장치에 대한 배드 블록 데이터를 포함하는 메시지를 수신하는 단계;

상기 메모리 장치에 단일 칩 식별자를 할당하는 단계;

상기 칩 식별자와 상기 배드 블록 데이터를 사용하는 칩에 대한 공용 암호 키를 생성하는 단계;

상기 공개 암호 키를 사용하는 칩에 대한 개인 암호 키를 생성하는 단계;

상기 메모리 장치에 대한 하드웨어 인증 수를 생성하기 위해 상기 칩 식별자를 암호화하는 상기 개인 암호 키를 사용하는 단계; 및

상기 제작자에 상기 칩 식별자와 상기 하드웨어 인증 수를 전송하는 단계;

를 포함하는 메모리 장치 제작 방법.

청구항 14

제13항에 있어서,

암호 서명 태그를 생성하기 위해 상기 제작자에 특정한 암호 메시지 인증 코드를 사용하여 상기 칩 식별자를 서명하는 단계를 더 포함하는 방법.

청구항 15

제14항에 있어서,

상기 칩 식별자를 암호화하는 개인 암호 키를 사용하는 단계는, 상기 하드웨어 인증 수를 생성하기 위해 상기 칩 식별자를 가진 상기 암호 서명을 사용하는 단계를 더 포함하는 방법.

청구항 16

제13항에 있어서,

배드 블록(bad block) 데이터를 포함하는 메시지를 수신하는 단계는, 암호화된 메시지를 수신하는 단계를 포함하는 방법.

청구항 17

제16항에 있어서,

상기 방법은 상기 배드 블록 데이터를 복호화하는 단계를 더 포함하는 방법.

청구항 18

제13항에 있어서,

수신과 전송은 상기 제작자에 보유되는 전용 안전 포털(dedicated, secure portal)에서 일어나는 방법.

청구항 19

안전 포털을 통해 배드 블록을 라이센싱 인증으로 전송하는 단계;

상기 안전 포털에서 상기 라이센싱 인증으로부터 칩 식별자와 하드웨어 인증 수를 수신하는 단계;

상기 칩 식별자와 하드웨어 인증 수를 입증하는 단계; 및

입증 시 상기 칩 식별자와 하드웨어 인증 수로 상기 메모리 장치를 프로그래밍하는 단계;를 포함하는 메모리 장치 제작 방법.

청구항 20

제19항에 있어서,

상기 칩 식별자와 하드웨어 인증 수를 입증하는 단계는 상기 칩 식별자와 하드웨어 수를 복호화하는 단계를 포함하는 방법.

청구항 21

제19항에 있어서,

상기 인증 데이터의 기능성을 보장하기 위해 프로그래밍 후 상기 메모리 장치를 테스팅하는 단계를 더 포함하는 방법.

청구항 22

제19항에 있어서,

프로그래밍 단계는 일회 단일 프로세스로 상기 칩 식별자와 하드웨어 인증 수를 기록하는 단계를 포함하는 방법.

청구항 23

제22항에 있어서,

상기 일회 단일 프로세스는 상기 부분만이 독취(read-only) 되도록 상기 메모리 장치 내 메모리 어레이 부분을 물리적으로 손상시키는 단계를 포함하는 방법.

청구항 24

컴퓨터를 통해 라이센싱 인증 세션을 구축하는 단계;

상기 라이센싱 인증으로부터 제어기 식별자와 펌웨어 파일을 수신하는 단계;

상기 펌웨어를 상기 컴퓨터에 부착된 제어기에 업로드하는 단계; 및

상기 제어기 식별자로 상기 제어기를 프로그래밍하는 단계;를 포함하는 메모리 제어기 제작 방법.

청구항 25

제24항에 있어서,

세션을 구축하는 단계는 전용 안전 컴퓨터를 사용하여 세션을 구축하는 단계를 포함하는 방법.

청구항 26

제24항에 있어서,

상기 펌웨어를 제어기로 업로드하는 단계는 펌웨어 인증 업데이트를 포함하는 방법.

청구항 27

제24항에 있어서,

상기 제어기를 프로그래밍하는 단계는 상기 제어기 식별자를 일회 단일 프로세스로 기록하는 단계를 포함하는 방법.

청구항 28

제27항에 있어서,

상기 일회 단일 프로세스는 부분이 독취 되도록 상기 제어기 식별자가 기록된 곳에 상기 메모리 장치의 부분을 물리적으로 손상시키는 단계를 포함하는 방법.

청구항 29

제작자의 컴퓨터에 안전 세션을 구축하는 단계;

상기 제작자의 컴퓨터에 제어기 식별자와 펌웨어 파일을 송신하는 단계; 및

데이터베이스의 제작자와 연관된 상기 제어기 식별자를 데이터베이스에 기록하는 단계;를 포함하는 메모리 제어기 제작 방법.

청구항 30

메모리 장치와 제어기의 세트를 포털 장치로 부착시키는 단계;

상기 장치를 확인하는 단계;

상기 제어기 식별자를 독취하는 단계;

라이센싱 인증에 상기 메모리 장치를 위한 상기 제어기 식별자와 하드웨어 인증 수를 송신하는 단계;

상기 라이센싱 인증으로부터 칩셋 인증 수를 수신하는 단계; 및

상기 제어기 및 상기 메모리 장치에 상기 칩셋 인증 수를 프로그래밍하는 단계;를 포함하는 제어기에 칩셋을 바인딩하는 방법.

청구항 31

제30항에 있어서,

칩을 확인하는 단계는:

프로그래밍하고 확인 테스팅 단계;

제거와 확인 테스팅 단계;

임의의 런타임 배드 블록을 검출하기 위해 각 칩의 스페어 영역을 파싱하는 단계; 및

각 칩을 위해 하드웨어 인증 수를 인증하는 단계; 중 적어도 하나를 실행하는 방법.

청구항 32

제30항에 있어서,

상기 포털 장치에 부착된 상기 메모리 장치를 위한 모든 배드 블록의 블록 실패 로그를 계산하는 단계; 및

각 메모리 장치에 상기 블록 실패 로그를 프로그래밍하는 단계;

를 더 포함하는 방법.

청구항 33

제30항에 있어서,

상기 블록 실패 로그를 프로그래밍하는 단계는 일회 단일 프로세스로 각 메모리 장치에 상기 블록 실패 로그를 기록하는 단계를 포함하는 방법.

청구항 34

제33항에 있어서,

상기 일회 단일 프로세스는 부분을 독취만으로 만들기 위해 상기 블록 실패 로그가 기록된 상기 메모리 장치의 부분을 손상시키는 단계를 포함하는 방법.

청구항 35

제30항에 있어서,

상기 칩셋 인증 수를 프로그래밍하는 단계는 부분을 독취만으로 만들기 위해 상기 칩셋 인증 수가 기록된 상기 메모리 장치와 상기 제어기의 부분을 손상시키는 단계를 포함하는 방법.

청구항 36

적어도 제1 및 제2 글로벌 워터마크 파일을 생성하도록, 적어도 상이한 두 워터마크를 사용하여 디지털 미디어 파일을 디지털 워터마킹하는 단계;

상기 글로벌 워터마크 파일을 제2오더 세그먼트(second order segment)로 분할하는 단계;

제1오더 세그먼트(first order segment)가 유니크 인스턴스 패턴에 따라 상기 제1 및 제2 글로벌 워터마크 파일로부터 상기 제2오더 세그먼트와의 결합을 포함하도록, 상기 제2오더 세그먼트를 상기 제1오더 세그먼트와 결합하는 단계;

글로벌 세그먼트가 상기 유니크 인스턴스 패턴에 따라 상기 제1 및 제2 글로벌 워터마크 파일로부터 상기 제1오더 세그먼트를 포함하도록, 상기 제1오더 세그먼트를 상기 글로벌 세그먼트에 결합하는 단계; 및

상기 글로벌 세그먼트가 단일 미디어 인스턴스를 위한 유니크 인스턴스 패턴의 요소를 이루는, 상기 글로벌 세그먼트로부터 단일 미디어 인스턴스를 생성하는 단계;를 포함하는 디지털 파일 워터마킹 방법.

청구항 37

제36항에 있어서,

적어도 두 개의 상이한 워터마크는 세 개의 워터마크를 포함하는 방법.

청구항 38

제36항에 있어서,

상기 유니크 인스턴스 패턴은 다섯 성분을 가지는 방법.

청구항 39

제36항에 있어서,

상기 제2오더 세그먼트를 결합하는 단계는 제2오더 세그먼트를 상기 제1오더 세그먼트에 연관시키는 단계를 포

함하는 방법.

청구항 40

제36항에 있어서,

상기 제1오더 세그먼트를 결합하는 단계는 상기 제1오더 세그먼트를 상기 글로벌 세그먼트에 연관시키는 단계를 포함하는 방법.

청구항 41

제36항에 있어서,

상기 방법은 상기 제2오더 세그먼트를 암호화하는 단계를 더 포함하는 방법.

청구항 42

제41항에 있어서,

상기 방법은 상기 제2오더 세그먼트에 적용된 암호에 기반하여 제2오더 해쉬 테이블(hash table)을 생성하는 단계를 더 포함하는 방법.

청구항 43

제42항에 있어서,

상기 방법은 상기 제1오더 세그먼트를 암호화하는 단계를 더 포함하는 방법.

청구항 44

제43항에 있어서,

상기 방법은 상기 제1오더 세그먼트에 적용된 암호에 기반하여 제1오더 해쉬 테이블을 생성하는 단계를 더 포함하는 방법.

청구항 45

제44항에 있어서,

상기 제1오더 해쉬 테이블에 기반하여 암호화된 복합 해쉬 테이블을 생성하는 단계를 더 포함하는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 SNAP(Simple Non-Autonomous Peering) 환경 워터마킹, 인증 및 바인딩에 관한 것이다.

배 경 기 술

[0002] 사용자로부터 사용자까지 미디어를 전송하는 피어링 네트워크의 사용은 사용자 요청에 대한 접근 속도(speed of access), 네트워크를 가로지르는 대역폭 균형 및 중앙 콘텐트 저장에 필요한 대역폭 감소를 포함하는 많은 매력적인 특징을 가진다. 하지만, 사용자의 자유로운 콘텐트 교환은 콘텐트 소유자의 재산권(property right)를 침해할 수 있다.

[0003] 콘텐트 소유자는 또한 저작권 보호 콘텐트의 복사를 제한할 것을 원한다. 저작권 보호 콘텐트의 전송을 매우 어렵게 하는 많은 기술적 예가 있다. 물리적 미디어가 콘텐트를 영원히 또는 잠시 저장하는데 사용될 때(예를 들어 전자 셀 도우(sell though) 및 대여 영업 방식), 콘텐트 소유자 또는 그 사용허락자(licesee)는 다양한 암호 바인딩 방법을 사용한다. 상기 방법은 콘텐트가 복사되거나 전송되는 것으로부터 보호하기 위해 일반적으로 암호 기능의 미디어 ID를 사용한다.

[0004] 비자율 피어링 시스템의 예가 "피어링을 통한 주문형 미디어(Media on Demand Via Peering)"으로 명칭지워진 미국 특허 No.7,165,050과 미국 특허공개 No.20060064386 에서 발견될 수 있다.

발명의 내용

해결하려는 과제

[0005] SNAP 환경 또는 시스템은 특정 미디어 파일의 유니크 인스턴스(unique instance)를 생성하고, 사용자가 여러 보호층으로 잘 정의된 방법론(methodology)에 따라 다른 피어로부터 인스턴스를 '설립(build)'하는 것을 허용한다. 이것은 대여(rental), 셀-스루(sell through), PPV(pay per view), 극장 전시 및, NAND 플래시 메모리, 광 미디어, 고체 상태 하드 드라이브, 스핀들 하드 드라이브 등에 한정되지 않는 다양한 미디어 파일까지 전자 셀 스루를 포함하는 다양한 콘텐트 제정 모델(monetization model)을 가능하게 한다. 상기 기능은 파일이 폐쇄 네트워크 환경 또는 네트워크 내 다양한 피어로부터 세그먼트로 제공되는 안전 '스와밍(swarming)'을 경유하여 소비자에게 제공될 수 있거나 키오스크(kiosk) 등과 같은 점포판매(points-of-sale)를 위한 안전 전자 분포를 제공한다.

과제의 해결 수단

[0006] SNAP 시스템은 콘텐트를 NAND 플래시에 바인드하기 위해 NAND 플래시 미디어에 내재된 물리적 결함을 사용한다. NAND 플래시의 상기 결함은 배드 블록(Bad Block)이라고 불린다. NAND 플래시는 두 구별되는 물리적 저장 영역: 블록에 물리적으로 그룹된 페이지로 이루어진 데이터 영역과 데이터 영역에 속하는 논리적이고 물리적인 메타데이터와 그곳에 저장된 데이터의 저장소를 위한 "스페어(Spare)" 영역을 함유하는 비휘발성 고체 상태 메모리 타입이다. 상기 두 영역의 구성이 제작자로부터 제작자까지 다양하게 변화할 수 있는 반면, 두 영역은 모든 NAND 플래시 칩에 존재한다. NAND 플래시 칩은 한 페이지씩(page-by-page) 기초로 프로그램되고 성능을 강화하고자 하는 노력으로 블록 범위로(block-wise manner) 제거된다.

발명의 효과

[0007] 본 상세한 설명에 따른 간단 비자율 피어링 시스템(SNAP; Simple Non-Autonomous Peering System)를 사용하는 것은 권리의 남용을 방지하면서 피어링 네트워크의 장점을 제공한다.

도면의 간단한 설명

[0008] 본 발명의 실시예는 도면을 참조하여 개시를 읽음으로써 가장 잘 이해될 수 있다.

도 1은 글로벌 워터마크 버전의 다중 인스턴스를 가지는 미디어 파일의 예를 보인다.

도 2는 세그먼트로 파싱된 미디어 파일의 예를 보인다.

도 3은 타이틀 스키마를 위한 데이터 구조의 예를 보인다.

도 4는 유니크 인스턴스 패턴의 제1오더 표현(first order expression)의 예를 보인다.

도 5는 상이한 글로벌 워터마크를 가진 세 개의 유니크 인스턴스(unique instance) 패턴을 위한 제1오더 표현의 예를 보인다.

도 6은 제1오더 표현의 예의 상세도를 보인다.

도 7은 인터리브 공격(interleave attack)의 예시적 결과를 보인다.

도 8은 유니크 인스턴스 패턴의 제2오더 표현의 개략도를 보인다.

도 9는 해쉬 테이블 계층(hash table hierarchy)의 예를 보인다.

도 10 및 11은 간단 비자율 피어링 패턴 표현과 복호 경로 기반(path-based) 포렌식(forensic) 식별 방법의 비교를 보인다.

도 12는 간단 비자율 피어링 컴플라이언스(compliance) 프로세스의 성분의 제조와 조립을 위한 라이센싱과 인증 시스템의 개략도를 보인다.

도 13은 상기 칩의 물리적 결함에 유니크 칩 식별자를 바인딩하는 방법의 예를 보인다.

도 14는 메모리 제어기를 위한 유니크 제어기 식별자를 생성하는 방법의 예를 보인다.

도 15는 유니크 제어기를 메모리 칩의 유니크 세트로 바인드하는 방법의 예를 보인다.

도 16은 간단 비자율 피어링을 따르는 메모리 장치에 미디어 파일을 기록하는 방법의 예를 보인다.

도 17은 메모리 장치의 미디어 파일을 입증하는 방법의 예를 보인다.

도 18은 SNAP 라이센싱 인증의 제어 하에 콘텐트 다운로드를 요청하는 호스트 장치 사이의 트랜잭션(transaction)의 예를 보인다.

도 19는 다운로드 콘텐트를 복호화하는 것을 요청하는 호스트 장치의 예를 보인다.

도 20은 메모리 장치에 콘텐트를 인증하는 호스트 장치의 예를 보인다.

도 21은 메모리 장치로부터 콘텐트를 재생하는 호스트 장치의 예를 보인다.

발명을 실시하기 위한 구체적인 내용

[0009] 본 상세한 설명에 따른 간단 비자율 피어링 시스템(SNAP; Simple Non-Autonomous Peering System)를 사용하는 것은 권리의 남용을 방지하면서 피어링 네트워크의 장점을 제공한다. SNAP 환경 또는 시스템은 특정 미디어 파일의 유니크 인스턴스(unique instance)를 생성하고, 사용자가 여러 보호층으로 잘 정의된 방법론(methodology)에 따라 다른 피어로부터 인스턴스를 '설립(build)'하는 것을 허용한다. 이것은 대여(rental), 셀-스루(sell through), PPV(pay per view), 극장 전시 및, NAND 플래시 메모리, 광 미디어, 고체 상태 하드 드라이브, 스핀들 하드 드라이브 등에 한정되지 않는 다양한 미디어 파일까지 전자 셀 스루를 포함하는 다양한 콘텐트 제정 모델(monetization model)을 가능하게 한다. 상기 기능은 파일이 폐쇄 네트워크 환경 또는 네트워크 내 다양한 피어로부터 세그먼트로 제공되는 안전 '스와밍(swarming)'을 경유하여 소비자에게 제공될 수 있거나 키오스크(kiosk) 등과 같은 점포판매(points-of-sale)를 위한 안전 전자 분포를 제공한다.

[0010] SNAP 시스템은 콘텐트를 NAND 플래시에 바인드하기 위해 NAND 플래시 미디어에 내재된 물리적 결함을 사용한다. NAND 플래시의 상기 결함은 배드 블록(Bad Block)이라고 불린다. NAND 플래시는 두 구별되는 물리적 저장 영역: 블록에 물리적으로 그룹된 페이지로 이루어진 데이터 영역과 데이터 영역에 속하는 논리적이고 물리적인 메타데이터와 그곳에 저장된 데이터의 저장소를 위한 "스페어(Spare)" 영역을 함유하는 비휘발성 고체 상태 메모리 타입이다. 상기 두 영역의 구성이 제작자로부터 제작자까지 다양하게 변화할 수 있는 반면, 두 영역은 모든 NAND 플래시 칩에 존재한다. NAND 플래시 칩은 한 페이지씩(page-by-page) 기초로 프로그램되고 성능을 강화하고자 하는 노력으로 블록 범위로(block-wise manner) 제거된다.

[0011] NAND 플래시 메모리를 만드는데 사용되는 내재된 제작 방법으로 인해, NAND 플래시 칩이 제작 중 5.5%에 달하는 결함을 포함하는 것이 일반적이다. 이것은 ㅊ칩 제작자가 상업적으로 실행가능한 수율(production yield)을 유지하기 위해 요구된다. NAND 플래시 메모리가 블럭 단위(block-by-block) 기초로 제거되기 때문에, 페이지 프로그램 사이클 또는 블록 제거 사이클 중 검출된 결함은 잠재 데이터 오염(corruption)을 피하기 위해 전체 메모리 블록이 "배드(Bad)"로 식별되는 것을 지시한다. 결함 블록은 칩 제작자에 의해 블록의 스페어 영역에 특정값(일반적으로 000h)을 프로그래밍함으로써 엄격한 후제조 테스팅(post-manufacturing testing) 동안 식별된다. 런타임이 검출된 배드 블록은 스페어 영역에 상이한 값(일반적으로 16비트 블록에 FFFh)가 표기된다.

[0012] 후술하는 논의에서 NAND 플래시 용어와 예를 사용하는 것에 주의해야 한다. 하지만 청구범위는 NAND 플래시 장치에 한정되지 않는다. 다른 메모리 기술은 NAND 플래시 장치에 유사한 특성을 가지고 NAND 플래시 장치에 대한 어떠한 한정도 의도하지 않으며 암시되지도 않는다.

[0013] SNAP 시스템은 유니크 미디어 인스턴스를 콘텐트가 저장된 특정 블록 주소에 바인드한다. 그것은 또한 플래시 미디어와 기록된 콘텐트를 인증하기 위해, 유니크 미디어 인스턴스가 기록되거나, NAND 플래시 용어로 '프로그램된' 위치의 디지털 설명을 사용한다. 그것은 또한 플래시 미디어와 기록된 콘텐트를 인증하기 위해 배드 블록의 위치의 디지털 서명을 사용한다. 상기 서명은 유니크 미디어 인스턴스를 암호화하고 복호화하는데 요구되는 키를 암호적으로 수정하는데 또한 사용된다.

[0014] 상기 두 디지털 서명은 플래시 미디어와 콘텐트의 인증을 결정하기 위한 기초이고 상기 장치와 콘텐트의 재생을 정지하거나 취소하거나 갱신하기 위해 다양한 플레이어와 소비자 전자장치에 사용된다. 유용한 수의 NAND 플래시 장치가 동일 패턴의 배드 블록을 가질 것 같지 않으므로, SNAP 시스템은 한 NAND로부터 장치까지 다른 NAND 장치까지 비인증된 전송을 매우 어렵게 한다. SNAP 시스템은 콘텐트 소유자가 한 NAND 플래시 장치로부터 다른 NAND 플래시 장치까지 콘텐트의 전송을 할 수 있게 한다. 전송은 이동 또는 복사 트랜잭션 또는 그 둘다가 될

수 있다. 이것은 콘텐트 소유자의 비즈니스 규칙에 따라 실행될 수 있고 전송 트랜잭션을 위한 지불을 포함하거나 포함하지 않을 수 있다. 어떤 경우든, SNAP 시스템은 콘텐트가 전송될 지 그리고 안전한 방식으로 될 지를 제어한다.

[0015] SNAP 은 또한 디지털 시네마 이니셔티브(initiative)로 설명되는 전자 이론 분배 시스템에서 우리를 위해 안전한 포렌식 식별가능 콘텐트를 제공한다. SNAP의 고도의 유연성, 안정성 및 포렌식 책임성(accountability)은 플레이어와 분배 네트워크 자원에 있어 비교적 저가로 가능하다.

[0016] SNAP 환경과 미디어 인스턴스의 전처리(Pre-Processing)

[0017] 도 1은 오서되고(authored) 부호화된 매스터 미디어 파일의 다중 인스턴스의 개략도를 보인다. 시스템은 매스터(10)의 다중 복사에 상이한 글로벌(global) 워터마크를 적용한다. 글로벌 워터마크는 제로 또는 그 이상의 페이로드 데이터(payload data)를 포함할 수 있다. 상기 토론은 상이한 워터마크 버전, 여기서는 인스턴스로 칭해진, 것 사이를 구별하기 위해 컬러를 사용한다. 인스턴스(12, 14 및 16)은 상이한 워터마크, 그린 레드 및 블루 각각으로 부호화된다. 각 상이한 글로벌 워터마크는 유니크 글로벌 마크 식별자에 의해 내재적으로 식별된다. SNAP는 많은 상이한 글로벌 워터마크를 채용할 수 있다는 것에 유의해야 한다. 각 글로벌 마크는 후술할, 매스터 내 유사한(analogous) 데이터에 적용되지 않도록 매스터의 상이한 복사에 적용된다.

[0018] 매스터의 세 개의 상이한 인스턴스에 더하여, 각 워터마킹 기술은 서로서로 상이할 수 있다. 예를 들어 동일한 워터 마킹 기술의 세 개의 상이한 변형예를 가지는 대신, 사람은 세 개의 상이한 워터마킹 기술을 사용하거나 단일 워터마크 캐리어 중 페이로드를 변화시킨다.

[0019] 전체적으로, 상기 매스터 인스턴스 각각은 도 2에 도시된 대로 제2오더 세그먼트의 기 설정된 수로 파싱된다. 대체 실시예에서, 워터마크의 적용에 앞서 영화 데이터를 세그먼트로 파싱하는 것도 가능하다. 상기 방법은 워터마크 캐리어 및/또는 페이로드가 단일 세그먼트의 데이터 중 성공적으로 부호화/검출되는 것을 보장하는 것이 바람직하다. 제2 오더 세그먼트의 수는 도 3의 상세에 토론된 대로, 타이틀 스킴을 따른다. 제2 오더 세그먼트를 설립하도록 제2 오더 세그먼트를 사용하고, 유니크 인스턴스 패턴(UIP; Unique Instance Patter)을 형성할 표현을 구축하도록 제1 오더 세그먼트를 사용하는, 바텀-업(bottoms-up) 방법론을 사용한다.

[0020] 도 2의 제2오더 세그먼트는 일반적으로 데이터 범위에 따라 서로 대응할 것이다. 예를 들어, 임의의 특정 제2오더 세그먼트에 대응하는 상이한 인스턴스로부터의 데이터 범위는 컬러 중 대응한다. 예를 들어, 20, 22 및 24와 같은 도면의 왼쪽에 제2오더 세그먼트는 레드, 그린 및 블루 인스턴스(12, 14 및 16)에 대응한다는 것이다. 유사하게 26, 28 및 30과 같은 도면의 오른쪽 엔딩 제2오더 세그먼트는 인스턴스 사이의 동일 데이터 범위에 유사하게 대응한다. 워터마크가 데이터 압축 전 영화 데이터의 베이스밴드(baseband)에 적용되는지, 워터마킹 데이터가 유사한 세그먼트에 상이한 워터마크 캐리어 및/또는 페이로드 비트의 존재로 인해 상이한 파일 사이즈를 가지게 하는지에 대한 포함(inclusion)에 유의한다.

[0021] 상이한 인스턴스가 상이한 워터마크를 가질 수 있기 때문에, 어떤 어콤모데이션(accommodation)은 AES-E CBC 또는 CTR 모드와 같은 데이터 "연쇄처리(chaining)"를 사용하는 단일 키 암호 시스템(single key encryption system)이 상이한 워터마크를 가진 세그먼트 사이를 변환(transition)하는 것을 허용한다. 이것은 초기화 벡터 테이블(32)로 달성될 수 있다. 초기화 벡터 테이블(32)은 각 제2오더 세그먼트의 마지막 128 비트 사이퍼 블록(cipher block)을 기록할 수 있다. 이것은 단일 키 암호 시스템이 변환을 위한 시작 포인트를 식별하는 것을 허용한다.

[0022] CBC 모드에서, 예를 들어 사이퍼 텍스트의 각 블록은 다음 블록의 복호화에 사용되도록 앞방향으로 연결된다(chained forward). 상이한 워터마크를 포함하는 SNAP 세그먼트가 미디어 인스턴스를 형성하기 위해 연결되거나(concatenate) 다르게 결합되기 때문에, 보통 CBC 모드는 워터마크 프로세스 자체가 연결된 블록을 변화시킬 때 실패할 것이다. 적합한 128 비트 워터마크된 사이퍼 텍스트 블록을 초기화와 유사하게 주입함으로써, 벡터는 CBC 체인을 시작하곤 하였다.

[0023] 상술한 대로, 제2오더 세그먼트는 제1오더 세그먼트를 형성하도록 연결되거나 다르게 결합되었다. 제1오더 세그먼트는 글로벌 세그먼트를 형성하도록 연결되고, 각각은 유니크 인스턴스 패턴의 일 성분(element)을 표현한다. 글로벌 세그먼트는 미디어 인스턴스를 형성하도록 함께 결합된다. 사용자가 전송할 미디어 파일을 요청할 때, 시스템은 전에 언급된 타이틀 스키마에 따라 세그먼트에 접속한다. 세그먼트는 중앙 파일 서버, DVR 네트워크, 케이블 셋톱 박스 네트워크와 같은 동일 네트워크 상의 다른 사용자, 또는 키오스크(kiosk)로부터 직접 전송을 경유하는 등을 포함하는 많은 상이한 소스로부터 올 수 있다.

[0024] 상기 타이틀 스키마의 예는 도 3에 보인다. 상술한 대로, 타이틀 스키마는 바텀업 방법론을 사용한다. 여기에 사용된 타이틀 스키마의 예에서, 인스턴스(12, 14 및 16)은 40과 같은 2000 제2 오더 세그먼트에 세그먼트된다. 42, 20과 같은 제1 오더 세그먼트를 형성하기 위해, 제2오더 세그먼트는 적합한 제2 오더 세그먼트로부터 함께 연결되고, 이 경우 100 제1오더 세그먼트가 형성된다. 타이틀 스키마는 제2 오더 세그먼트의 어떤 조합이 어떤 인스턴스로부터 취해졌는지를 결정한다. 여기에 주어진 예에서, 제1 오더 세그먼트(S1)은 제2 오더 세그먼트(S1-S20)로 형성되고, 제1오더 세그먼트(S100)는 제2 오더 세그먼트(S1981-S2000)으로 형성된다.

[0025] 44와 같은 글로벌 세그먼트의 형성은 제1오더 세그먼트의 연결로부터 만들어진다. 제공된 스키마 예에서, 20 제1 오더 세그먼트의 연결은 하나의 글로벌 세그먼트를 만든다. 상기 예에서 글로벌 세그먼트(GS1 44)는 제1오더 세그먼트(S1-S20)의 연결에 의해 형성된다. 세그먼트란 용어는 제1 또는 제2 오더 세그먼트의 데이터 범위를 칭하고, 반면 용어 '표현(expression)'는 제1오더 및 글로벌 세그먼트를 이루는 세그먼트의 워터마크와 타입에 대한 세그먼트의 오더링(ordering)과 서브스턴스(substance)를 칭한다.

[0026] 제2오더 세그먼트, 제1오더 세그먼트, 글로벌 세그먼트 등의 수에 대해 여기서 주어진 특정 수는 단지 예이며 상세한 내용은 본 발명의 이해를 쉽게 하기 위한 수단으로 제공된 것임을 유의해야 한다. 유사하게 세그먼트는 여기서 연결(concatenation)을 이용하여 결합된 반면, 높은 오더 세그먼트를 형성하기 위해 더 낮은 오더 세그먼트를 함께 연결하는 다른 타입도 적용할 수 있다.

[0027] 도 3으로 돌아가면, 44와 같은 글로벌 세그먼트 중 하나는 유니크 인스턴스 패턴(UIP; Unique Instance Patter)에 사용된 한 성분에 대응할 것이다. 사용자가 다운로드되거나 전송될 것을 기대하는 미디어 파일로서 보는 것은 46과 같은 성분으로 이루어진 UIP(48)이다. 이것은 도 4를 참조하여 더 잘 이해될 것이다.

[0028] UIP의 각 성분 내에는 UIP의 제1오더 표현이 있다. 이것은 계층 워터마크 프레임워크(framework)를 생성한다. 도 4에 도시된 대로, 상기 예의 UIP는 그린-블루-레드-블루-그린 UIP를 칭할 수 있다. 상기 패턴은 제1오더 세그먼트에서 반복된다. 성분(46)을 이루는 제1오더 세그먼트(S1-S20)는 세그먼트(50, 52, 54, 56 및 58)에서 동일 패턴 내부에서 반복되었다.

[0029] 여기에 주어진 특정 예에서, UIP는 그린-블루-레드-블루-그린이다. 상기 패턴은 그린 제1오더 표현(E1)에서 반복되어, 성분(50)은 그린, 성분(52)는 블루, 성분(54)는 레드, 성분(56)은 블루 및 성분(58)은 그린이 된다. 상기 패턴은 제1오더 표현의 각각에서 반복된다.

[0030] 도 5는 제1성분과 잔여 4 성분을 위한 동일 성분에 대한 상이한 글로벌 세그먼트를 가지는 세 개의 상이한 UIP에 대해 제1성분(46)의 글로벌 표현 범위 내의 제1오더 표현을 보인다. 이것은 제1 성분의 표현 범위 내 각 상이한 성분에 대한 유니크 성분 매핑을 강조한다.

[0031] 확장되었을 때, 성분(60)은 62로 도시된 그 제1 오더 세그먼트 내 그린-블루-레드-블루-그린 패턴을 반복한다. 확장되었을 때, 성분(64)은 66으로 도시된 레드-블루-레드-블루-그린 UIP를 반복한다. 또한 성분(68)은 70으로 표시된 블루-블루-레드-블루-그린 패턴을 반복한다.

[0032] 도 6은 제1오더 표현의 더 상세한 도면을 보인다. 표현의 제1부분, A는 제1오더 오프셋이다. 제1오더 오프셋은 표현 단부(the end of the expression)에 표현 그룹 D 전 글로벌 표현 데이터 범위의 시작으로부터 제1오더 세그먼트의 수이다. 상기 예에서 오프셋은 3이다.

[0033] 표현 B의 부분은 제1오더 표현 그룹 1-5이다. 여기에 사용된 대로, 용어 '표현 그룹(expression group)'은 제1오더 세그먼트와 같은 세그먼트 수의 집합이다. 상기 예에서, 세 개의 인스턴스가 있고 UIP는 5 성분을 포함하여, 각각이 3 제1오더 세그먼트를 포함하는 5 표현 그룹이 있을 것이다.

[0034] 제1오더 오프셋 후, 제1오더 표현 그룹 오프셋을 포함하는 표현의 영역 C가 있다. SNAP는 그 내부에 제1오더 표현이 제1오더 표현 그룹 오프셋을 결정하도록 일어나는 부(parent) UIP 성분의 글로벌 워터마크에 대한 매핑을 사용한다. 예를 들어, 상기 오프셋은 부 성분(parent element)이 그린 워터마크를 포함하면, 제1오더 표현 그룹 오프셋이 0 이 되는 컨벤션(convention)에 의해 설정될 수 있다. 만약 부 성분이 레드 워터마크를 포함하면, 오프셋은 1이 될 것이고, 만약 성분이 블루 워터마크를 포함하면, 오프셋은 2가 될 것이다. 비록 그것이 모든 다섯 성분에 대해 동일하더라도, 상기 매핑은 다섯 성분 중에서 변화할 수 있다.

[0035] 제1오더 표현의 영역 D는 제1오더 테일(tail)로서 칭해질 수 있다. 상기 테일은 스플라이싱 공격(splicing attack)의 경우 UIP의 포렌식 강화를 제공한다. 도 6의 성분은 그린 워터마크된 성분이고, 따라서 테일 D은 그린이다. 후술하는 바와 같이, 이것은 상이한 표현 부분이 명확하고 함께 이어지는(spliced) 스플라이싱 공격의

경우 표현의 네이티브 워터마크(native watermark)를 체크하는 것으로 작용한다.

[0036] 예를 들어, 두 미디어 인스턴스가 샘플된 다음, 미세 입도(granularity)에서 함께 이어진다. 제1 미디어 인스턴스는 그린-블루-레드-블루-그린 인스턴스를 가지는 미디어 인스턴스로부터 제1오더 세그먼트(1-20)으로 이루어진다. 제2인스턴스는 레드-그린-그린-그린-블루의 UIP를 가진 미디어 인스턴스로부터 세그먼트 1-20으로 이루어진다. 상기 인스턴스가 함께 이어질 때, 테일은 레드와 그린 워터마크를 모두 보이고, 이것은 그것들이 이어지며 합법적 표현 그룹(legitimate expression group)이었음을 나타낸다.

[0037] 도 6에 도시된 마킹의 상기 제1오더 레벨은 전체 글로벌 세그먼트를 크레스(cress) 실행하는 인터리빙(interleaving)의 경우 파일을 공모(colluding)하는 글로벌 패턴을 식별하는 한 수단을 제공한다. 그것은 제1오더 세그먼트 레벨에서 스플라이싱에 대해 잠재적으로 취약하다(vulnerable). SNAP는 선택된 제1오더 세그먼트 내 UIP의 제2오더 표현을 사용한다. 즉, 제2오더 세그먼트가 제1오더 세그먼트를 형성하도록 함께 결합될 때, 다른 글로벌 인스턴스의 제2오더 세그먼트는 적어도 부분으로 UIP의 패턴으로 결합된다.

[0038] 예를 들어, 상술한 그린-블루-레드-블루-그린 UIP를 사용하여, 제1오더 세그먼트는 상기 UIP를 흉내해는 표현에 결합된다. 또한 제1오더 세그먼트 내부에, 제2오더 세그먼트는 상기 패턴을 또한 나타낸다. 상술한 스플라이싱과 같은 공모 어택(collusion attack)을 탑재하기 위해, 해적(pirate)은 워터마크된 패턴의 입도를 식별할 능력이 필요하다. 하지만, SNAP는 포렌식 워터마크를 검출하거나 독취하는 플레이어의 능력에 의존하지 않고, 대신 상이하게 마크된 데이터를 식별하는 암호화된 복합 해쉬 테이블을 사용하여, 모든 마크를 검출하고 독취하는 공격자의 능력은 거의 가능하지 않다.

[0039] 도 7은 대체 데이터가 워터마크 패턴을 지우고 미디어 인스턴스에 접근을 얻으려는 노력으로, 재결합된 두 소스 파일로부터 샘플되어진 미디어 인스턴스의 부분을 보인다. 제1 오더 세그먼트(80)는 상술한 대로 UIP 그린-블루-레드-블루-그린을 가지는 미디어 인스턴스로부터 제1오더 세그먼트(1-20)의 데이터 범위로 이루어진 제1성분이다. 제1오더 세그먼트(82)는 레드-그린-그린-그린-블루의 UIP를 가지는 미디어 인스턴스로부터 제1오더 세그먼트(1-20)의 데이터 범위로 이루어진 제1성분이다.

[0040] 제1오더 세그먼트(84)는 워터마크를 지우려는 의도로 프레임 단위로 인터리브된 상기 제1오더 세그먼트(1-20)의 '공모된(colluded)' 버전이다. 만약 컬러로 되어 있다면, 그것은 데이터의 교체되는 레드 및 그린 '스트라이프(stripe)'이다. 세그먼트는 뒤섞이고 UIP의 실제 제1성분으로서 작동하지 않는다. SNAP의 강력한 면 중 하나는, 하지만, 세그먼트가 미디어 인스턴스를 복호화하도록 타이틀 스키마 내부에서 사용가능하지 않기 때문에 공격을 궁극적으로 실패하게 하는 그 능력 뿐만 아니라, 영화 데이터가 "명확하게 분리된(ripped to the clear)" 경우 두 이어진 파일의 소스의 식별을 허용할 수 있다는 것이다.

[0041] 성분(84)의 오프셋 영역 0의 분석은 레드 및 그린 워터마크가 존재하고, 공모 파일이 레드 워터마크된 파일로부터의 1 성분 E1 과 그린 워터마크된 파일로부터의 1 성분 E1을 의미한다는 것을 보인다. 상기 오프셋의 다른 분석은 상기의 경우 단지 두 공모 파일만 있고, UIP를 가진 파일이 레드로 시작하고, 다른 것이 그린으로 시작한다는 것을 보인다. 부분(2-5)의 분석은 레드로 시작하는 UIP가 레드-그린-그린-그린-블루의 UIP이고, 그린으로 시작하는 UIP가 그린-블루-레드-블루-그린 UIP로 식별되는 결과를 나타낸다. 테일 섹션 T는 상기 분석을 확인한다.

[0042] 상술한 바와 같이, SNAP 환경과 스키마는 파일의 사용을 불능화(diabling)할 뿐만 아니라, 시스템 내 미디어 인스턴스의 포렌식 트래킹을 위한 공모된 파일의 소스를 식별할 수 있다. 이것은 UIP의 성분의 제1 오더 표현을 사용하여 달성되었다. 제1오더 세그먼트 내 제2오더 세그먼트의 표현을 결정하는데 채용된 방법론은 심지어 더 많은 입도(granularity)를 허용한다.

[0043] 도 8은 UIP의 제2오더 표현의 개략도를 보인다. 이것은 다중 미디어 인스턴스로부터 완전한 제1오더 세그먼트가 제1오더 워터마킹 패턴을 제거하고자 하는 시도로 함께 이어지는 중간 입도 공격을 위한 보호를 제공한다. 제2오더 표현은 스와밍 분포(swarming distribution)를 위한 네트워크 효율성을 유지하기 위해 개별 제1오더 세그먼트에 의해 일반적으로 바운드된다. 이것은 제한으로 의도되지 않으며, 제2오더 표현이 글로벌 표현의 방식으로 제1오더 세그먼트 경계를 확장하는 것이 가능하다. 일반적으로, 제1오더 표현 그룹 내부에 UIP의 제2오더 표현을 포함하는 하나의 제1오더 세그먼트가 있을 것이다. 상술한 대로, 패턴 오프셋은 표현 그룹으로부터 표현 그룹까지 임의추출(randomize)하는 것이 바람직하다.

[0044] 도 8의 예에서, 제1오더 세그먼트는 그것들이 제1오더 표현 그룹을 통해 다중 오프셋에서 일어날 수 있도록 표현 그룹 오프셋의 증가하는 형태(incrementing form)을 사용하여 제2 오더 표현 그룹에 대해 선택될 것이다. 내

부적으로, 제1오더 표현 그룹은 제2오더 표현 그룹 오프셋을 사용한다. 제2 오더 표현 그룹 오프셋은 UIP 를 통해 성분 단위를 기초로 각 성분의 상이한 글로벌 워터마크에 매핑된다.

[0045] 도 8은 그린-블루-레드-블루-그린의 글로벌 UIP 48을 가지는 예시 파일로부터 제1오더 세그먼트(1-20)을 보인다. 각 제2오더 세그먼트 표현은 20 제2오더 세그먼트의 연결이고, 최초 오프셋 부분과 트레일링 테일 부분(trailing tail portion) 다음, 성분값 E1-E5 내에 그것 안의 그린-블루-레드-블루-그린의 UIP를 모방한다. 제2오더 표현 그룹(90)은 제1오더 표현 그룹의 제1 세그먼트(92)에 해당하고, 제2오더 표현 그룹(94)은 제1오더 표현 그룹의 9번째 세그먼트(96)에 대응한다. 제1오더 표현 그룹의 결정은 제2 오더 표현 그룹이 컨벤션에 의해 설정되는 타이틀 스키마와 오프셋에 의해 구동되는 것에 의해 이루어진다.

[0046] SNAP 해쉬 테이블(hash table)

[0047] SNAP 환경이 워터마크를 생성하고 유지하는 것을 허용하는 한 성분이 해쉬 테이블이다. 상기 해쉬 테이블은, SNAP 포렌식 워터마크 또는 미디어 인스턴스 패턴을 검출하거나 해석할 수 있는 애플리케이션 없이, 그것들이 타이틀 스키마에 의해 구동되는 피어로부터 적절한 데이터를 선택하도록, 스와밍 애플리케이션의 행동을 조절하는데 사용된다.

[0048] 또한, SNAP 는 일반적으로 CMAC(cipher-based message authentication code) 태그를 채용한다. 상기 태그는, 수신될 때, 그것들이 매치되는 것을 보장하기 위해 그것이 전달된 저장 미디어의 물리적 특성(attribute)에 암호적으로 바운드되는 키를 사용하여 메시지로부터 생성된 태그에 비교된다. 상기 태그는 갱신가능하다. 워터마크되고 암호화된 데이터가 새 CMAC 키로 해쉬될 때, 디스크립터(descriptor) 메타데이터의 완전 갱신이 일어난다. 이것은 선행하여 전달된 영화를 무효화하지 않고, 키 공유 어택의 경우 사용자간 키 및/또는 디스크립터 메타데이터의 교환을 허용하지 않는다. CMAC 태그는 또한 데이터의 인증과 에러 보정을 제공한다.

[0049] 유니크 미디어 인스턴스 내 모든 세그먼트의 CMAC 태그는 미디어 인스턴스를 위한 복합 해쉬 테이블에 포함된다. 워터마킹과 같이 해쉬 테이블 생성은 도 9에 도시된 바텀 업 방법론을 채용하기 때문에, 그것은 복합 해쉬 테이블로서 칭해진다.

[0050] 도 9는 하나의 워터마킹 방법에 대응하는 하나의 미디어 인스턴스를 위한 해쉬 테이블 계층의 개략도를 보인다. 상기 예에서 미디어 인스턴스는 블루 워터마크된 인스턴스이다. 프로세스는 제2오더 세그먼트로 시작한다. 제2오더 키는 갱신가능한 타이틀 크립토(crypto) CMAC 키를 사용하여 제1 해싱 플레인텍스트(hashing plaintext) 제2오더 세그먼트에 의해 계산된 배치(batch)이다. 각 세그먼트의 CMAC 태그는 비가역적 결합 기능을 사용하여 100과 같은 매스터 키 제2오더 해쉬 테이블(HT^2)로부터 유사 태그로 결합된다. 매스터 키 제2오더 해쉬 테이블은 구조에 있어 테이블을 가지는 제1오더 키와 유사하지만, 유니크 임의값(random value)로 채워진다(populate). 매스터 키 제2오더 해쉬 테이블의 한 세트는 모든 미디어 인스턴스에 사용될 수 있다.

[0051] 상술한 바와 같이, 더 많은 공통 SHA-1 또는 MD5 플레인 해싱보다 CMAC를 사용하는 하나의 장점은 CMAC가 타이틀 크립토 CMAC 키를 변화시킴으로써 키 생성 프로세스를 반복함으로써 SNAP가 타이틀 키셋트를 빠르게 갱신하는 것을 가능하게 한다는 것이다. 상기 프로세스는 타이틀이 리매스터링(re-mastering)을 요구하지 않고 네트워크에 릴리즈(release)된 후에도 일어날 수 있다.

[0052] 제1 오더 세그먼트를 이루는 제2오더 세그먼트의 각 그룹을 위한 CMAC 태그는 102와 같은 제1오더 키 해쉬 테이블에 기록된다. 각 CMAC 태그는, 결과적 값이 유니크 세그먼트 키로서 사용될 수 있도록 제1오더 세그먼트 매스터 키 해쉬 테이블로부터 대응하는 임의 아날로그(analog)와 결합된다. SNAP는 그런 다음 그 대응하는 키에 각 제2오더 세그먼트를 암호화한다.

[0053] 해쉬 충돌(collision)을 나타내는 어떠한 데이터도 공개되지 않은 것을 보장하는 전처리(pre-processing)의 각 상태 후, 모든 해쉬와 임의값이 유니크로서 검증되는 것이 바람직하다. 해쉬 충돌은 두 상이한 세그먼트가 매칭 해쉬를 가질 때 일어난다. 만약 이것이 일어나면, 한 인스턴스는 그것이 유니크 해쉬를 리턴하도록 사용자가 인지하지 못하는 방식으로 그것이 데이터를 수정하게 해야 한다. 이것은 태그가 그것이 설명하는 세그먼트를 위한 유니크 식별자로서 기능할 수 있고, 엔지니어 해싱 알고리즘 행동을 뒤집어 결과적으로 암호화된 키 생성 방법을 발견하기 위해 해싱 충돌을 사용할 수 있는 공격자로부터 보호하는 것을 보장한다.

[0054] 부가 보호로서, 102와 같은 제1 오더 키 해쉬 테이블은 크로스 매핑된다. 크로스 매핑은 제2 오더 세그먼트를 생성하기 위해 다른 워터마크된 미디어 인스턴스로부터 유사한 제2오더 세그먼트를 위한 CMAC 태그를 사용하는 것과 연관된다. 예를 들어, 블루 제2오더 세그먼트를 위한 키는 유사한 레드 제2오더 세그먼트의 해쉬를 사용하

여 생성된다. 레드 제2오더 세그먼트 키는 그린 제2 오더 세그먼트의 해쉬로 생성되고, 그린 제2오더 세그먼트는 그 키를 블루 제2 오더 세그먼트로부터 유도한다. 상기 방식으로 키는 어떠한 개별 미디어 플레이어도 소유할 수 없는 정보를 사용하는 방식으로 유도된다.

[0055] 제2오더 세그먼트의 암호화 후, 그것들은 제1오더 세그먼트를 생성하도록 서로 연결된다. 결과적인 제1오더 세그먼트는 제2오더 해쉬 테이블을 기록하는데 사용되는 동일 CMAC를 사용하여 해쉬된다. CMAC 태그는 그런 다음 제1오더 해쉬 테이블에 기록된다. 앞서 생성된 제2오더 해쉬 테이블은 제1오더 해쉬 테이블(HT^1)(104) 중 그것들의 각각의 제1 오더 세그먼트 CMAC 태그 하에 네스트될 수 있다(nested).

[0056] 104와 같은 제1오더 해쉬 테이블은 블루 글로벌 해쉬 테이블(106)을 생성하도록 결합된다. 블루 글로벌 해쉬 테이블은 그런 다음 블루 워터마크된 세그먼트를 이용하여 미디어 인스턴스를 재형성하기 위해 임의의 블루 제1 및 제2 오더 세그먼트를 설명하는 모든 필요한 정보를 포함한다. 레드 및 그린 블루 해쉬 테이블에 연결 사용될 때, 다중 글로벌 워터마크를 사용하는 미디어 인스턴스는 복호화된다.

[0057] 도 10 및 11은 SNAP의 패턴 표현과 복호화 경로 및 시퀀스 키 기반(SKB; sequence key based) 시스템에 의해 생성된 패턴의 비교를 보인다. 도 10은 SKB 시스템에 기반한 포렌식 패턴을 보인다. 미디어 플레이어(110), 미디어 키 번들(112) 및 시퀀스 키 번들(114)와 같은 장치에서 장치 키를 사용하여, EVOB(enhanced video object)의 변형예가 패턴화된 결과적인 오디오 비디오 스트림(116)에 위치한다.

[0058] 결과적인 복잡성이 미디어 인스턴스를 보호하기 위해 그 면에 일어나는 반면, 패턴 누설은 더욱 임계적(critical)이다. EVOB는 포렌식 워터마킹 패턴의 경계를 직접 표현하는 이산 파일(discrete file)이다. 이것은 해커에게 포렌식 패턴의 스푸프(spoof)를허용하는 패턴 정보를 제공한다. 이것은 교대로 복호화 플레이어를 포렌식하게 검출하는 능력을 이룬다.

[0059] 대조적으로, 도 11에 도시된 미디어 인스턴스(120)은 암호화된 복합 해쉬 테이블(122)에 의해서만 표시된다. 실제 결과적인 미디어 스트림(126)은 유니크 암호화된 복합 키 번들(124)를 요구하는, 상술한 두 다른 레벨에서 다른 암호화의 결과이다. 이런 식으로, 해쉬 테이블 생성과 복합화(compositing)뿐만 아니라 미디어 인스턴스 레벨을 통해 UIP의 다중 레벨 워터마킹과 사용에서, SNAP 환경은 해커 보호의 더 높은 레벨을 가질 뿐만 아니라 복호화 플레이어를 검출하는 포렌식 능력을 가지는 미디어 인스턴스에 대해 안전 인증 환경을 제공한다.

[0060] 상술된 SNAP 환경의 한 면은 어느 특정 미디어 플레이어로부터 복호화와 키의 분리이다. 일반적인 안전 환경에서, 요청하는 플레이어는 플레이어가 원하는 미디어 스트림을 복호화하는 것을 허용하는 키 및/또는 해쉬 테이블을 수신한다. SNAP 환경에서, 복호화 능력은 플레이어에 독립적이 되어 어떤 특정 장치에 키가 남게 하는데 더 강건하고(more robust) 더 저항적이게(more resistant) 만든다.

[0061] 하지만 상술한 바와 같이, 콘텐트가 물리적 미디어에 저장될 때 그것이 인증없이 전송될 수 없도록 콘텐트와 키를 미디어에 바인드하는 것이 중요하다. SNAP 암호화된 유니크 미디어 인스턴스와 분리 키는 인증되지 않은 전송이 한 NAND 플래시 장치로부터 다른 NAND 플래시 장치로 가는 것을 방지하기 위해 미디어에 암호적으로 바운드될 필요가 있다. 이것은 SNAP 안전 호스트 환경에 더 상세히 후술한다.

[0062] SNAP 안전 호스트 환경(Secure Host Environment)

[0063] SNAP 안전 호스트 환경은 플레이어 호스트의 안전 프로세서 또는 NAND 플래시 카드 제어기 또는 그 둘 다에 저장되는 코드, SNAP 갱신 로직(Renewable Logic)을 가진다. SNAP 갱신 로직은 특정 암호 데이터 생성을 위한 데이터와 템플릿을 포함한다. SNAP 갱신 로직은 그 호스트 애플리케이션과 SNAP 가능 NAND 플래시 장치 사이의 통신과 암호 계산을 위한 공지된 암호 환경을 제공하는 중간자(intermediary)이다.

[0064] SNAP 갱신 로직은 각 NAND 플래시 장치를 위해 상이하게 암호 데이터를 변환한다. SNAP 갱신 로직에 대한 입력은: 1) 장치 배드 블록, 칩 ID, SNAP 체인 로그, SNAP 세그컨트 체인과 2) SNAP 갱신 스트링을 포함한다. SNAP 갱신 로직의 출력은 SNAP HAK(hardware authentication key)이고, 이것은 SNAP HAN(hardware authentication number)를 인증하고 암호적으로 보호하는데 사용된다. SNAP 갱신 로직은, 입력 변수가 NAND 플래시 장치로부터 NAND 플래시 장치까지 변화하는 상기 1)에 리스트되기 때문에, 각 NAND 플래시 장치에 상이하게 실행된다.

[0065] 임의의 두 NAND 플래시 장치가 동일한 방식으로 동일 인증과 암호를 사용하지 않기 때문에, 이것은 공격자를 위해 더 복잡한 레벨을 제공한다. SNAP 갱신 스트링은 로직, SNAP 프로세싱에 사용된 알고리즘과 변수를 변화시킨다. 상기 SNAP 갱신 스트링은 유니크 미디어 인스턴스와 개별 키가 NAND 플래시 장치의 결함에 암호적으로 바운드되는 방식을 스투디오(Studio)가 변화시킬 수 있는 주기적 기초 상에서 업데이트될 수 있다.

[0066] 비휘발성 저장 미디어의 인증(Authenticating Non-Volatile Storage Media)

[0067] 일 실시예에서, 트러스트 트랜섹션이 비휘발성 저장 미디어 상에 배드 블록의 임의 성질을 사용하여 실행될 수 있다. 일반적으로, 플래시(flash)와 다른 저장 미디어의 제작자는 장치가 구조에 따른 물리적 메모리의 배드 블록을 식별하는 것을 허용하는 배드 블록 식별 방법을 사용한다. 그렇게 함으로써, 제작자는 장치를 여전히 판매할 수 있고, 배드 블록이 메모리의 남은 '양호한(good)' 블록에 접근하는 처리 장치를 위해 마크되고 식별되므로, 그것은 의도한 대로 동작할 것이다.

[0068] 후 제조(post manufacture) 테스팅 중, 물리적 메모리의 각 블록은 다중 '프로그램', '독취(read)' 및 '제거(erase)' 작용을 거친다. 메모리 블록을 이루는 임의의 또는 모든 페이지가 실패할 때, 전체 블록은 블록에 관련된 스페어 영역(Spare Area) 내부와 함께, 배드 블록의 페이지 내 특정 값(예, 'ooh')를 기록함으로써 배드(bad)로 마크된다. 제조에서 검출된 상기 배드 블록은 장치의 연속된 소비자 조작 중 검출된 배드 블록과 상이하게 된다. 소비자 조작 중 식별된 배드 볼록은 블록의 페이지와 스페어 영역에 상이한 값(예 'Foh')을 기록함으로써 식별된다.

[0069] 제조 중 식별된 배드 블록의 패턴이 무작위이기 때문에, 상기 정보는 유니크 인증과 암호 메커니즘을 제공하는데 유용한 유니크 값을 제공한다. 배드 블록의 패턴은 유니크 인증 값을 생성하기 위해 장치의 유니크 미디어 ID와 결합될 수 있다. 메모리의 블록 내에서 실패한 특정 페이지를 식별하는 것이 또한 가능할 수 있고, 그 값은 상기 인증의 강건함(robustness)을 강화하는데 또한 유용할 수 있다. 이것은 제조에서 유니크 인증을 허용하지만, 인프라구조의 어떤 종류는 상기 유니크 값이 모조되거나 다르게 복사되는 것을 방지하도록 모니터되고 트래킹되는 것을 보장하는데 도움이 될 수 있다.

[0070] 상기 장치의 제조는 중앙 라이센싱 인증 하에 허용될 수 있고, 라이센싱 인증은 장치가 'SNAP 컴플라이언트(compliant)'임을 보장한다. 상기 시스템의 개략이 도 12에 도시된다. 도 12에서, SNAP 라이엔싱 인증 또는 SLA(150)은 제조 체인 중 다양한 포인트에서 이용가능한 포털(portal)를 통해 안전한 연결을 가진다. 160, 170 및 180과 같은 상기 포털은 SLA에 대한 안전하고 인증된 링크를 제공한다. 이것은 모조 제작자(roge fabricator) /해적(pirate)이 상기 두 엔티티 사이의 교환된 정보를 해킹하거나 다른 식으로 파괴하는(subvert)하려는 시도의 어려움을 증가시킨다.

[0071] 일반적으로, 제작 체인은 적어도 세 개의 부분을 가진다. SNAP 포털(160)은 NAND 플래시 메모리 칩을 생산하는 칩 제작자에게 있다. NAND 플래시 메모리에 대한 칩 용어의 사용은, 그것이 이산 IC 패키지된 상품 메모리 칩의 형태인지 또는 MCP(Multi Chip Package) 또는 SoC(Solution on a Chip)의 경우와 같은 다른 장치에 집적되는지에 관계없이, 폭넓게 모든 NAND 플래시 메모리 어레이(다이)를 커버하는 것으로 간주된다. SLC 또는 MLC NAND 플래시의 다중 평면(muliple plane)을 포함하는 다중 평면 장치는 그 메모리 어드래싱 행동(단일 또는 멀티 장치 어드레싱)과 일치하는 방식으로 처리되는 평면을 가진다.

[0072] SNAP 포털(170)은 메모리 제어기 제조 설비에 있다. 대부분의 비휘발성 메모리 제품은 제품 상 다양한 메모리 구조의 데이터의 들어가고 나가는 이동을 관리하는 온-보드(on-board) 제어기를 가진다. 본 논의에서, 상기 제어기는 SNAP 프로토콜에 따라 제조될 것이고, SNAP 컴플라이언트(compliant)로 칭해질 수 있다.

[0073] SNAP 포털(180)은 소비자 제품, 예를 들어 메모리 제품(SD 카드, 플래시 썸 드라이브(thumb drive) 등), 디지털 미디어 콘텐트 플레이어, 예를 들어 MP3 플레이어, 영화 또는 음악이 가능한 비디오 게임 플레이어 또는 디지털 콘텐트를 저장하는 비휘발성 메모리를 사용하는 다른 제품에 메모리 장치 세트와 제어기를 결합하는 어셈블러에 존재한다. 상기 논의의 목적을 위해, 각 엔티티는 분리된 엔티티처럼 설명될 것이며, 그것들은 엔티티의 조합 또는 한 장소에 모두가 있는 것으로 이해된다. 구획(compartmentalization)은, 그것이 안전성의 부가층을 추가하기 때문에 바람직하다. 각 엔티티는 라이센스를 요구한다. 메모리 제작자는 칩 바인딩 라이센스를 가질 것이고, 제어기 제작자는 제어기 바인딩 라이센스를 가질 것이며, 어셈블러는 칩셋 바인딩 라이센스를 가질 것이다. 만약 한 엔티티가 모든 세 개의 기능을 실행하면, 그 엔티티는 모든 세 개의 라이센스를 가질 것이고, 이는 위반(breach) 리스크를 증가시킨다.

[0074] 도 13은 메모리 칩 상의 유니크 칩 식별자(ID)를 생성하고 임프린트(imprint)하는 방법의 예를 보인다. 청구항에 사용된 '칩(chip)'이라는 용어는 메모리의 개별화된 부분을 칭한다.

[0075] 도면에서, 도면의 왼쪽 블록은 제작자에서 행해지고 오른쪽 블록은 SLA에서 행해진다. 프로세스는 제작자가 완료된 메모리 칩을 테스트할 때 190에서 시작하고, 상술한 대로 그 배드 블록을 결정한다. 배드 블록 데이터는 SLA에서 192에서 수신한다. SLA는 그런 다음 유니크 칩 ID를 194에서 칩으로 할당하고, 배드 블록 데이터를 196

에서 복호화한다. 만약 메모리가 한 번에 한 칩에서 프로그래밍된다면, 제작자는 메모리 제작자일 수 있다. 대체적으로, 메모리 칩이 함께 그룹핑되면, 제작자는 제어기와 칩 셋 프로그래밍에 관해 후술하는 대로 또한 어셈블러일 수 있다.

[0076] SLA는 그런 다음 칩을 위한 유니크 식별자를 생성하기 위해, 칩 ID 와 조합되거나 또는 단일로, 배드 블록 상에서 적어도 한 번 조작을 실행한다. 칩 ID는 200에서 제작자를 위해 벤더-특정 CMAC 키를 사용하여 SLA에 의해 서명된다. 서명 프로세스는 그것이 SLA 보다 장치에 의해 인증되도록 공개 키를 채용할 수 있거나, 단지 SLA 만이 그것을 인증할 수 있도록 비밀 키를 채용할 수 있다. 결과적인 CMAC 다이제스트는 칩 CMAC로서 여기에 칭해진다.

[0077] 칩의 개인 키를 사용하여, SLA는 칩 ID를 암호화하고, 204에서 HAN(Hardware Authentication Number)를 생성하는 서명이 된다. SLA는 그런 다음 206에서 칩 ID 와 HAN을 서명하고 그것들을 암호화한다. 암호화된 HAN과 ID는 그런 다음 208에서 제작자에서 SNAP 포털로 송신된다.

[0078] 제작자로 돌아가서, SNAP 포털은 210에서 HAN을 복호화하고 승인한다. SNAP 포털의 제어 또는 SNAP 포털 그 자체 내에 가능하게, 칩은 HAN과 칩 ID로 프로그램된다. 프로그래밍은 '한 번 기록(write once)' 전략에 연관될 수 있고, 여기서 메모리 내 게이트 세트(NAND 플래시 메모리 내 NAND 게이트와 같음)는 독취만(read-only)하도록 물리적으로 손상된다. 그것이 칩 ID 또는 HAN의 변화를 방지하기 때문에, 이것은 다른 안전층을 추가한다.

[0079] SLA-중심 칩 식별 프로세스와 달리, 제어기를 위한 프로세스는 제작자를 위해 어느 정도 더 관련된다. 상기 프로세스의 예는 도 14에서 도시된다. 220에서, SNAP 제어기는 제어기 제작자에서 SNAP 포털에 연결된다. SLA 또는 SNAP 포털, 또는 둘다는 222로서 세션으로서 설립된다. SLA는 그런 다음 제어기 ID와 펌웨어를 224에서 제작자로 송신한다. SLA는 232에서 후에 모니터링과 트래킹을 위해, 제작자와 연관되어, 제어기 ID 를 데이터베이스 또는 다른 타입의 저장소(storage)에 기록할 수 있다.

[0080] 반면, 제작자는 226에서 SNAP를 통해 제어기 ID와 펌웨어를 수신하였다. SNAP 포털은 그 자체로 또는 제작자의 기계를 제어함으로써, 제어기로 펌웨어를 업로드하고, 이것은 228에서 제어기를 SNAP 제어기로 만든다. SNAP 제어기는 그런 다음 230에서 제어기 ID로 프로그램된다.

[0081] 어떻게 유니크 ID를 메모리 칩과 메모리 제어기로 할당하는 지를 본 다음, 논의는 이제 칩 세트 바인딩으로 칭해진, 메모리 칩 세트를 가진 유니크 제어기를 바인딩하는 차례로 넘어간다. 상기 프로세스의 예는 도 15에 도시된다.

[0082] 240에서, 메모리 칩과 제어기를 모두 포함한 장치는 프로그래밍을 위해 SNAP 포털로 연결된다. 칩은 모조 SNAP 컴플라이언트 칩을 검출하기 위해 각 칩 상에 프로그램/검증(program/verify) 및 제거/검증(erase/verify) 테스팅을 실행함으로써 전형적으로 검증된다. 이것은 배드 블록 태그를 제거함으로써 달성될 수 있다. 만약 이것이 검출되면, 장치는 모조(counterfeit)로 거절된다. 다른 테스팅은 임의의 런타임 배드 블록의 존재를 검출하기 위해 칩의 스페어 영역을 파싱하는 것을 포함할 수 있다. SNAP 포털은 또한 HAN 필드 파싱에 따라 칩의 HAN을 인증할 수 있다.

[0083] 칩의 검증시, SNAP 포털은 244에서 제어기 ID를 독취하고 246에서 제어기 ID와 모든 HAN을 SLA로 송신한다. SLA는 그런 다음 상이한 HAN(Hardware Authentication Code)를 계산하고 그것을 248에서 SNAP로 리턴한다. 포털은 그런 다음 예를 들어 상술한 일회 기록(write once) 전략을 사용하여 SNAP 제어기와 각 칩에 HAN을 프로그램한다. 안전성의 추가된 측정으로서, SNAP 제어기와 SNAP 포털은 칩셋 내 모든 칩을 위한 모든 배드 블록 주소를 포함하는 암호화된 블록 실패 로그를 계산하고, 그것들을 미래 참조를 위해 각 구성 칩의 시스템 영역에 기록할 수 있다. SNAP에 적용되는 칩과 상기 제어기를 포함하는 장치의 모든 사용은 칩과 제어기 모두가 장치가 유효함을 보장하도록 매칭 HAN을 가진다.

[0084] 일단 상술한 프로세스로부터 제조된 SNAP 컴플라이언트 장치가 이용가능해지면, 그것들은 미디어 내용을 사용자에게 제공하도록 사용될 수 있다. 상기 프로세스의 예가 도 16에 도시된다. 도 16에서, 미디어 파일이 획득된다. 미디어 파일은 바람직하게 도 1-11에 관해 상술한 워터마킹 계층을 사용한 것들일 수 있다. 워터마크된 인스턴스 또는 인스턴스들은 그런 다음 262에서 메모리에 기록된다.

[0085] 미디어 파일을 포함하는 마감된 제품의 제작은 데이터베이스에 기록될 수 있다. 데이터베이스는 콘텐트의 복사의 트래킹을 허용할 것이고, 라이센스 로열티를 수신하도록 콘텐트 제공자를 위한 근거를 제공할 것이다.

[0086] 일단 파일이 메모리에 기록되면, 로그가 생성될 수 있고, 이것은 266에서 메모리 내 파일의 논리적이고 물리적

인 위치를 바인딩한다. 상기 로그는 그런 다음 접근 시 메모리 콘텐트의 인증을 검증하고 확인하는데 사용될 수 있다. 상기 프로세스의 예가 도 17에 보인다.

[0087] 도 17에서, SNAP 제어기의 제어 하에 메모리 칩에 포함된 워터마크된 콘텐트를 가지는 SNAP 컴플라이언트 장치가 호스트 장치에 연결된다. 이것은 컴퓨터, 셋톱박스, 키오스크, 텔레비전, 미디어 플레이어, 휴대용 장치 등일 수 있다. 상기 프로세스는 각 장치 상의 업데이트 파일의 날짜에 따라, 장치 또는 호스트 장치의 업데이트와 연관될 수 있다.

[0088] 제조 중, 호스트 장치는 상술한 대로 워터마킹 알고리즘에 대한 최신 정보가 제공되고, 또한 사용자, 미디어 또는 장치 등을 위해 미디어 키 번들, 라이센스 취소가 제공된다. 유사하게, 미디어 인스턴스를 수신한 때, 장치는 그 시점의 최신 정보를 수신한다. 장치와 호스트 장치가 연결될 때, 어떤 것이 최신 정보인지에 대한 결정이 이루어지고, 무엇을 하든 간에 그것은 그 정보를 다른 장치로 제공한다. 이런 식으로, 라이센스, 취소 및 알고리즘에 대한 최신 정보가 SNAP 컴플라이언트 장치를 통해 전파된다. 호스트 장치는, 장치에 대한 외부 연결에 의해 또는 미디어 인스턴스가 네트워크를 통해 다운로드될 때, 새로운 미디어와 연결될 때마다 업데이트될 수 있다.

[0089] 일단 업데이트가 270에서 완료될 때, 호스트 장치는 272에서 메모리로 미디어 인스턴스의 기록 중 생성된 위치와 파일의 로그 파일을 획득한다. 상기 로그 파일은, 274에서 메모리 내 그 위치에 기반한 미디어 파일을 인증하도록 해석화/복호화된다.

[0090] 반면 메모리 제어기는 로그 파일 상에 동일 작업을 실행할 것이고, 두 결과는 276에서 비교된다. 만약 두 결과가 278에서 매치되면, 미디어 인스턴스의 재생이 282에서 허용된다. 만약 두 결과가 매치되지 않으면, 장치는 불능이 되거나 미디어 인스턴스가 280에서 불능이 된다.

[0091] SNAP 인프라구조의 다양한 성분과 방법을 구축한 다음, 호스트 장치 리퀘스트로서 일어나는 이벤트를 토론하는 것과 그런 다음 영화, 오디오 파일 등과 같은 콘텐트를 플레이하는 것이 유용하다. 이것들은 도 18-21에서의 영화에 있어 논의될 것이고, 콘텐트는 다운로드 가능한 형태인 모든 타입의 보호 콘텐트이다.

[0092] 도 18에서 호스트 제어기는 SNAP 라이센싱 인증(SLA) 서버로부터 콘텐트를 다운로드할 것을 요청한다. 상기 다운로드는, 앞서 매우 상세히 설명된 대로, 실제 피어 장치로부터 온 것일 수 있으나, SLA 서버의 제어 하에 있다. 290에서, 재생 장치의 제어기는 SLA 서버와 접촉하고, 예를 들어 영화와 같은 콘텐트를 요청한다.

[0093] 서버는 292에서 논의된 대로 유니크 인스턴스 패턴(UIP; unique instance patter)을 생성하고, 296에서 UIP와 연관된 해쉬 테이블을 생성한다. 300에서, 서버는 상기 해쉬 테이블을 호스트 제어기로 송신하고, 그런 다음 서버 측에서 UIP와 함께 호스트 제어기의 제어기 ID를 저장한다. 이것은 상술한 공모된 공격과 같이 나타나는 UIP의 인스턴스 식별을 허용하고, 도난(pirate)된 세그먼트의 소스의 트래킹을 허용한다.

[0094] 298에서, 호스트 제어기는 해쉬 테이블을 수신한다. 302에서, 호스트 제어기는 해쉬 테이블의 요구를 만족시키기 위해, 어디에 위치해 있든 영화의 다양한 세그먼트를 위치시킨다. 어떤 세그먼트는 피어(peer)로부터 얻어질 수 있고, 다른 것들은 콘텐트 제공자 등으로부터 얻을 수 있다. 306에서, 호스트 제어기는 세그먼트 체인 로그를 생성한다. 세그먼트 체인 로그는 영화 인스턴스의 모든 세그먼트의 위치의 로그이다. 세그먼트 체인 로그는 영화의 스토리지의 호스트 제어기에 의해 부가된 플래시 장치로, 또는 심지어 그 자신의 비휘발성 메모리로 생성될 수 있다. 체인 로그는 영화 인스턴스의 특정 세그먼트가 NAND 플래시 칩에 저장되는 물리적(칩/블록/페이지) 주소의 시퀀셜 로그이다. 체인 로그는 장치, 영화와 같은 콘텐트의 세그먼트 또는 완전한 피스(piece)와 연관될 수 있다.

[0095] 해쉬 테이블을 완성하고 모든 필요한 세그먼트를 획득한 다음, 호스트 제어기는 이제 암호화된 세그먼트에 접근을 허용하는 모든 필요한 키를 획득할 것이다. 이것은 도 19에 도시된다.

[0096] 310에서, 호스트 제어기는 SLA 서버에 접촉하고 다운로드되는 UIP 를 위한 키 번들을 요청한다. 서버는 312에서 UIP를 검색하고 316에서 키 번들을 생성한다. 반면, 호스트 제어기는 318에서 모든 세그먼트의 수신 시 생성된 체인 로그를 송신한다. SLA 서버는 320에서 체인 로그를 수신한다.

[0097] SLA 서버는 324에서 상술한 대로 SNAP 갱신 로직을 예로 들고, 326에서 갱신 스트링을 사용하여 그것을 초기화한다. 이것은 SNAL 갱신가능한 로직이 키 생성에 사용되는 프로세스를 '리프레쉬(refresh)'하고, 그것들을 파괴에 더 강하게 만드는 것을 보장한다. 328에서, SLA 서버는 세그먼트가 상기 장치 속성(attribute)에 대한 키를 바인드하게 저장되는 장치 중 위치를 식별하는 체인 로그를 사용한다. 상기 전체 번들은 330에서 암호화되고,

334에서 호스트 장치로 갱신 스트링과 함께 리턴된다.

[0098] 호스트 제어기는 332에서 바운드 키 번들과 갱신 스트링을 수신한다. 도 16에 관해 설명된 대로, 갱신 스트링은 갱신과 취소에 관한 최신 정보의 일부로서 연결 시 한 장치에서 다른 장치로 이동될 수 있다. 335에서 호스트 장치는 키 번들, 갱신 스트링 및 프로그램 세그먼트를 플래시 장치로 프로그램한다.

[0099] 콘텐트는 이제 플래시 장치에 있고, 적합한 호스트 장치에 의해 접근되도록 준비된다. 상기 프로세스의 예가 도 20에 도시된다. 336에서, 호스트 장치는 플래시 장치에 안전한 세션을 구축한다. 호스트 장치는 338에서 SNAP 갱신 로직을 예로 들고, 340에서 플래시 장치에 저장된 영화의 재생을 요청한다. 플래시 장치는 영화의 해시 테이블과 암호화된 키 번들을 344에서 호스트 장치로 제공한다. 호스트 제어기는 콘텐트의 복제가 합법적임을 보장하기 위해 346에서 영화의 세그먼트 체인 로그를 인증한다. 인증 시, 호스트는 영화를 플레이할 수 있다.

[0100] 영화 또는 다른 콘텐트의 플레잉은 인증과 안전 구조에 있어 최종 프로세스를 시작한다. 이것의 예는 도 21에 도시된다. 호스트 제어기는 346에서 플래시 장치로 앞서 다운로드된 영화 세그먼트를 요청함으로써 영화를 플레이한다. 세그먼트는 348에서 수신된다. 상기 세그먼트는 워터마킹에 대해 상술한 대로 제2오더 세그먼트일 수 있다.

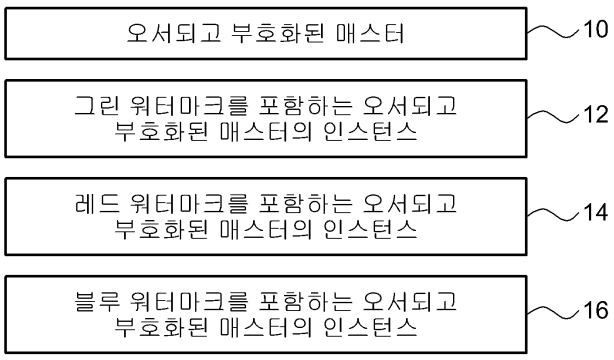
[0101] 세그먼트의 해쉬는 350에서 암호화된 해쉬 테이블 내 선행 제공된 값에 대항하여 인증된다. 상기 세그먼트를 위한 체인 로그는 플래시 장치로부터 352에서 제공되고, 이것을 제어기가 354에서 상기 세그먼트를 위한 키를 계산하기 위해 사용한다. 일단 키가 컴퓨터라면, 호스트 제어기는 356에서 세그먼트를 해석하고 콘텐트를 사용자에게 렌더링한다.

[0102] 이런 식으로, 메모리 칩셋을 위한 콘텐트 워터마킹으로부터 유니크 식별자의 생성까지의 안정성의 다중 레벨, 콘텐트가 저장될 제어기와 칩셋은 콘텐트 제공자를 그들의 콘텐트 도적으로부터 보호한다. 미디어 파일의 워터마킹과 로딩으로부터 미디어 파일에 대한 제품 성분의 제조와 바인딩까지, 여기서 논의한 트랜섹션은 트랙되고 기록되며, 이것은 권리의 보호와 상기 권리로부터 흐르는 이익(revenue)을 보장하면서 콘텐트의 분포를 허용한다.

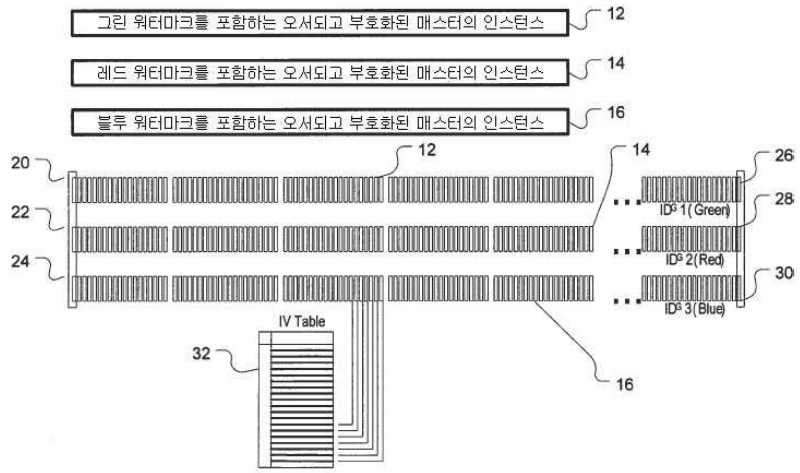
[0103] 따라서, 비록 SNAP 환경, 다중 레벨의 디지털 데이터 워터마킹 및 장치 이송의 인증을 위한 방법 및 장치에 대한 특정 실시예를 설명했으나, 상기 특정 참조가 다음의 청구항에 전개된 범위를 제외하고 본 발명의 범위에 대한 제한으로 고려되는 것을 의도하지는 않는다.

도면

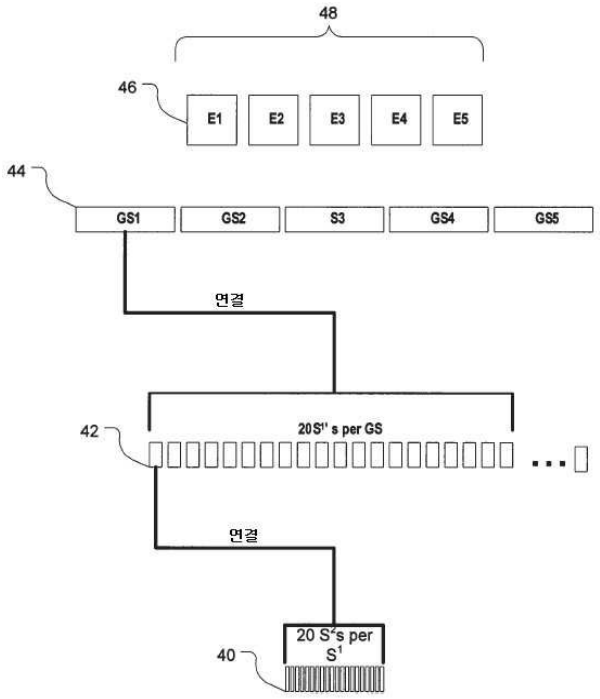
도면1



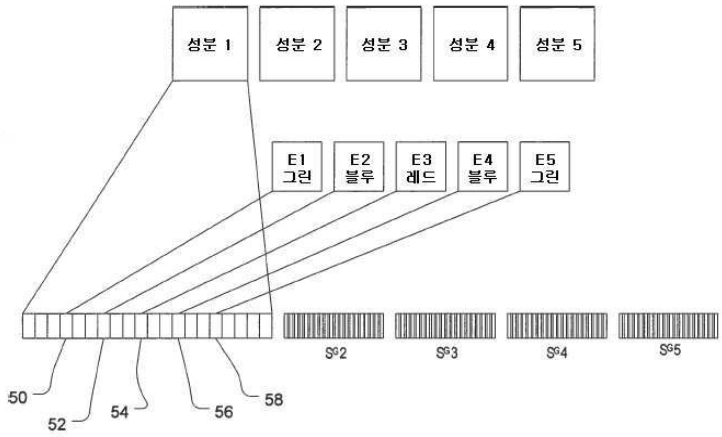
도면2


그린 워터마크를 포함하는 오서되고 부호화된 매스터의 인스턴스
12
레드 워터마크를 포함하는 오서되고 부호화된 매스터의 인스턴스
14
블루 워터마크를 포함하는 오서되고 부호화된 매스터의 인스턴스
16
20
22
24
12
14
26
28
30
ID^S 1(Green)
ID^S 2(Red)
ID^S 3(Blue)
IV Table
32
16

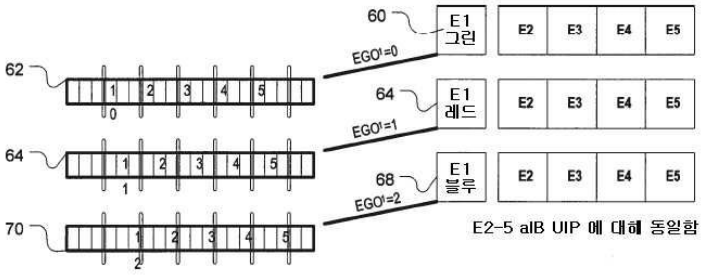
도면3


48
46
E1
E2
E3
E4
E5
44
GS1
GS2
S3
GS4
GS5
연결
42
20 S^1's per GS
연결
20 S^2s per S^1
40

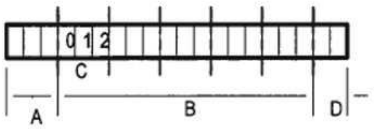
도면4



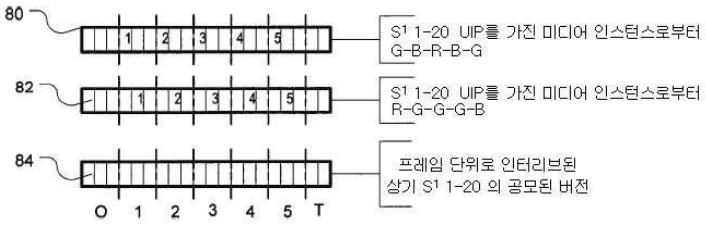
도면5



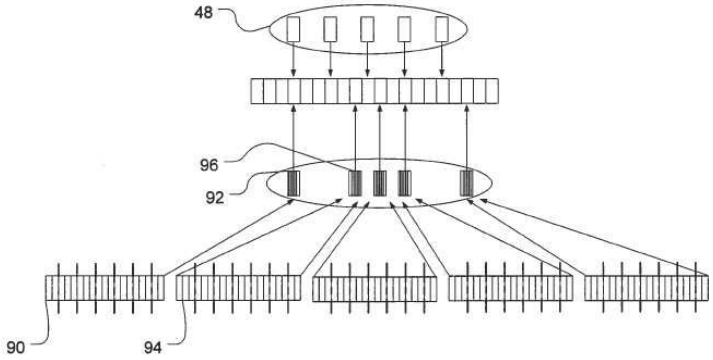
도면6



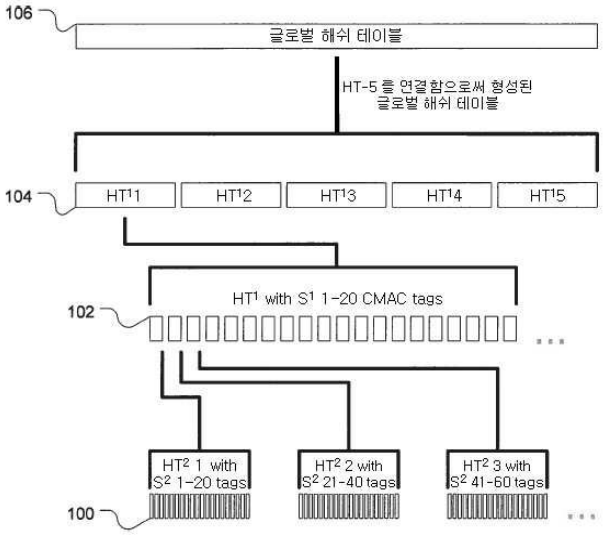
도면7



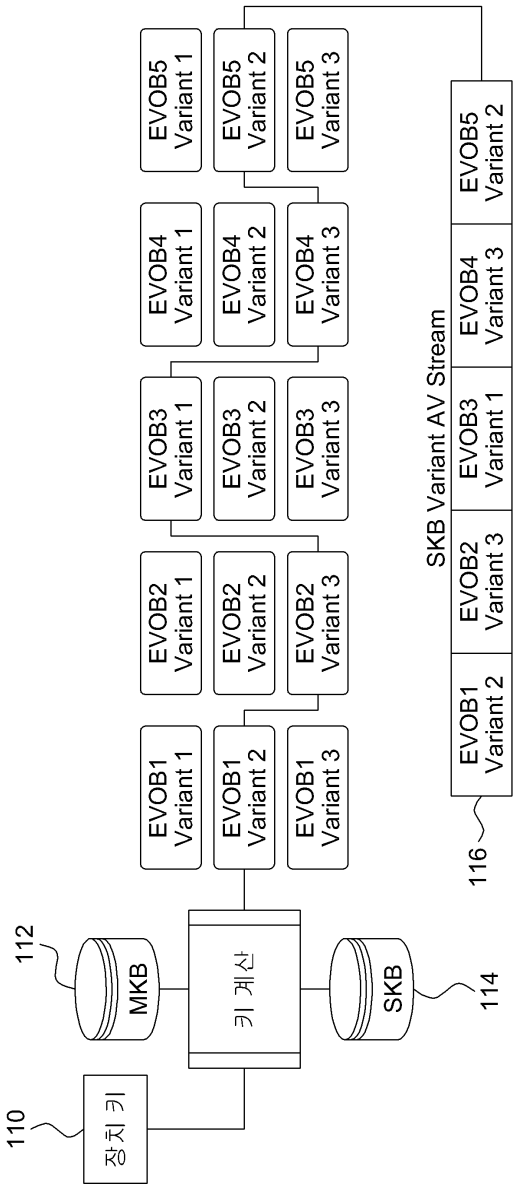
도면8


48
96
92
90
94

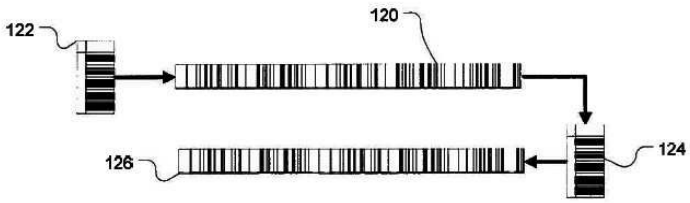
도면9


106
글로벌 해쉬 테이블
HT-5 를 연결함으로써 형성된
글로벌 해쉬 테이블
104
HT1 1
HT1 2
HT1 3
HT1 4
HT1 5
102
HT1 with S1 1-20 CMAC tags
HT2 1 with S2 1-20 tags
HT2 2 with S2 21-40 tags
HT2 3 with S2 41-60 tags
100

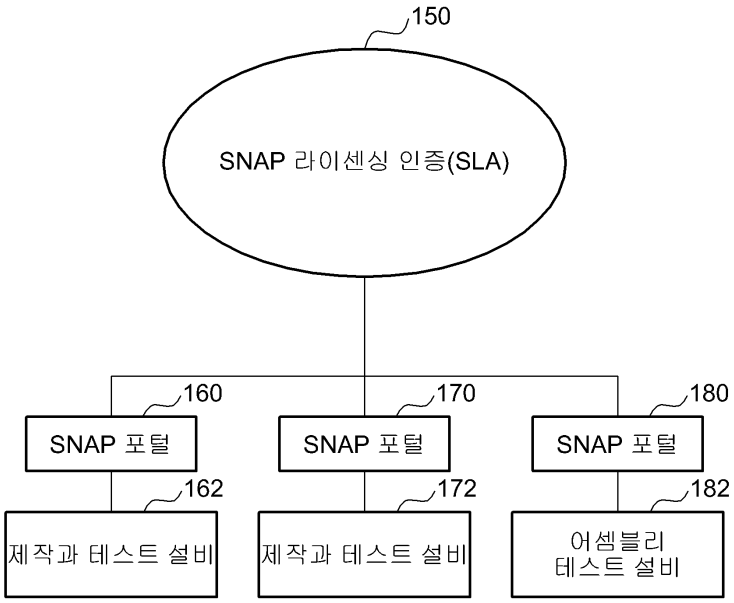
도면10


EVOB5 Variant 1
EVOB5 Variant 2
EVOB5 Variant 3
EVOB4 Variant 1
EVOB4 Variant 2
EVOB4 Variant 3
EVOB3 Variant 1
EVOB3 Variant 2
EVOB3 Variant 3
EVOB2 Variant 1
EVOB2 Variant 2
EVOB2 Variant 3
EVOB1 Variant 1
EVOB1 Variant 2
EVOB1 Variant 3
SKB Variant AV Stream
EVOB5 Variant 2
EVOB4 Variant 3
EVOB3 Variant 1
EVOB2 Variant 3
EVOB1 Variant 2
116
112
MKB
키 계산
SKB
114
110
장치 키

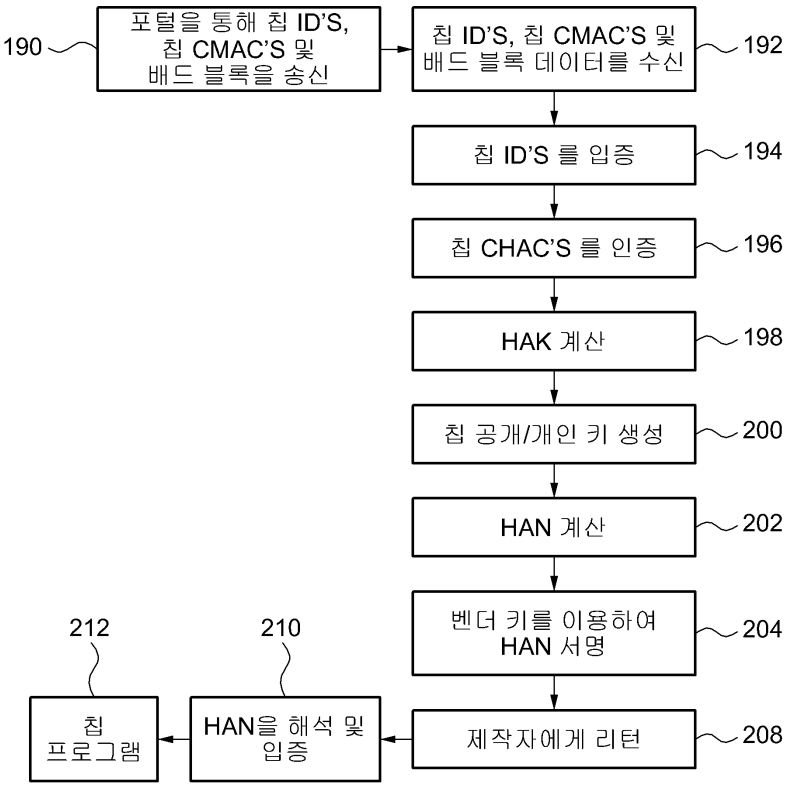
도면11


122
120
126
124

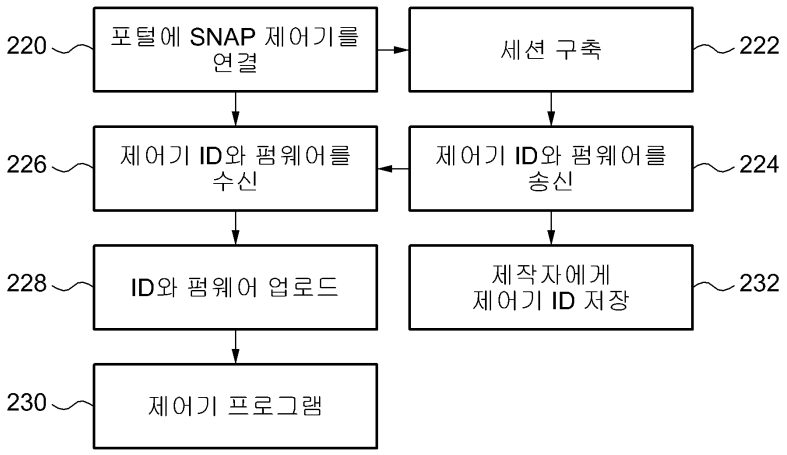
도면12


150
SNAP 라이센싱 인증(SLA)
160
SNAP 포털
162
제작과 테스트 설비
170
SNAP 포털
172
제작과 테스트 설비
180
SNAP 포털
182
어셈블리
테스트 설비

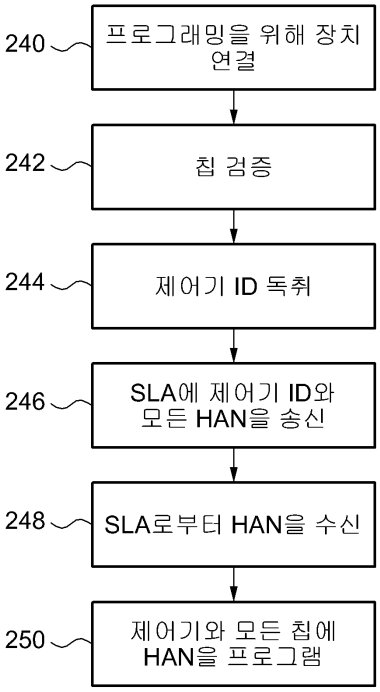
도면13


190
포털을 통해 칩 ID'S,
칩 CMAC'S 및
배드 블록을 송신
칩 ID'S, 칩 CMAC'S 및
배드 블록 데이터를 수신
192
칩 ID'S 를 입증
194
칩 CHAC'S 를 인증
196
HAK 계산
198
칩 공개/개인 키 생성
200
HAN 계산
202
벤더 키를 이용하여
HAN 서명
204
제작자에게 리턴
208
HAN을 해석 및
입증
210
칩
프로그램
212

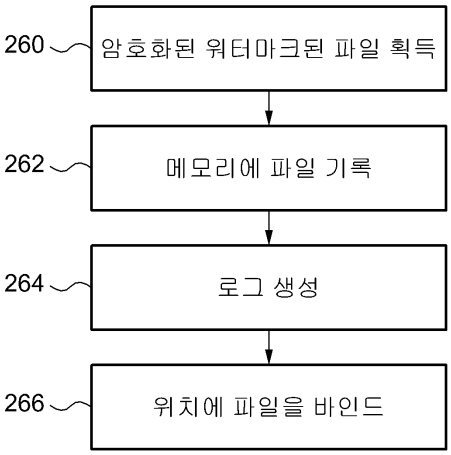
도면14


220
포털에 SNAP 제어기를 연결
222
세션 구축
226
제어기 ID와 펌웨어를 수신
224
제어기 ID와 펌웨어를 송신
228
ID와 펌웨어 업로드
232
제작자에게 제어기 ID 저장
230
제어기 프로그램

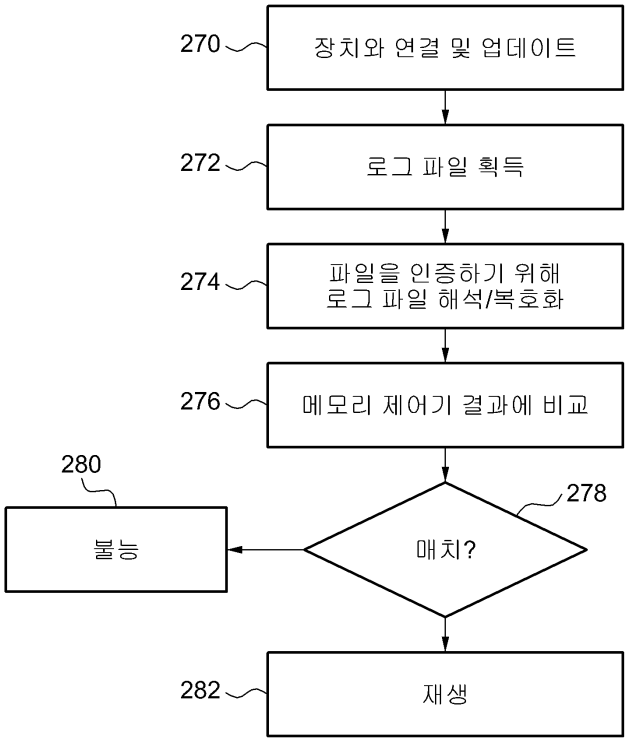
도면15


240
프로그래밍을 위해 장치 연결
242
칩 검증
244
제어기 ID 독취
246
SLA에 제어기 ID와 모든 HAN을 송신
248
SLA로부터 HAN을 수신
250
제어기와 모든 칩에 HAN을 프로그램

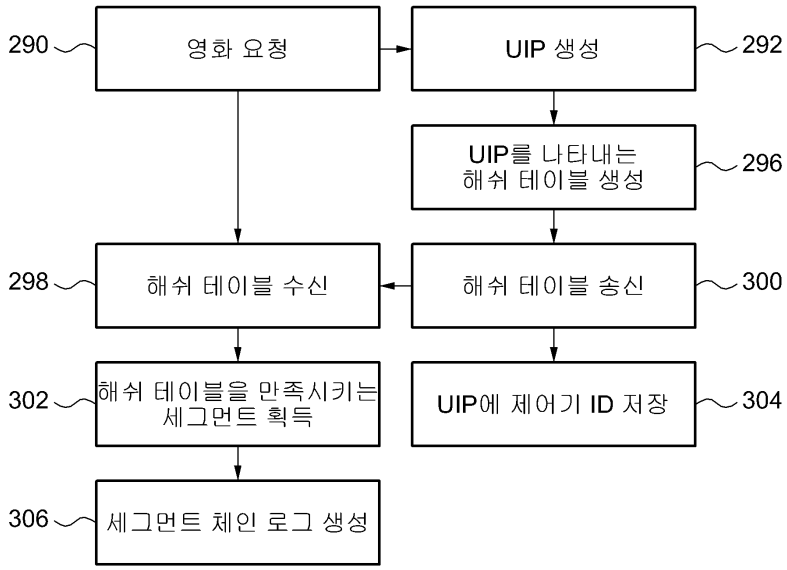
도면16


260
암호화된 워터마크된 파일 획득
262
메모리에 파일 기록
264
로그 생성
266
위치에 파일을 바인드

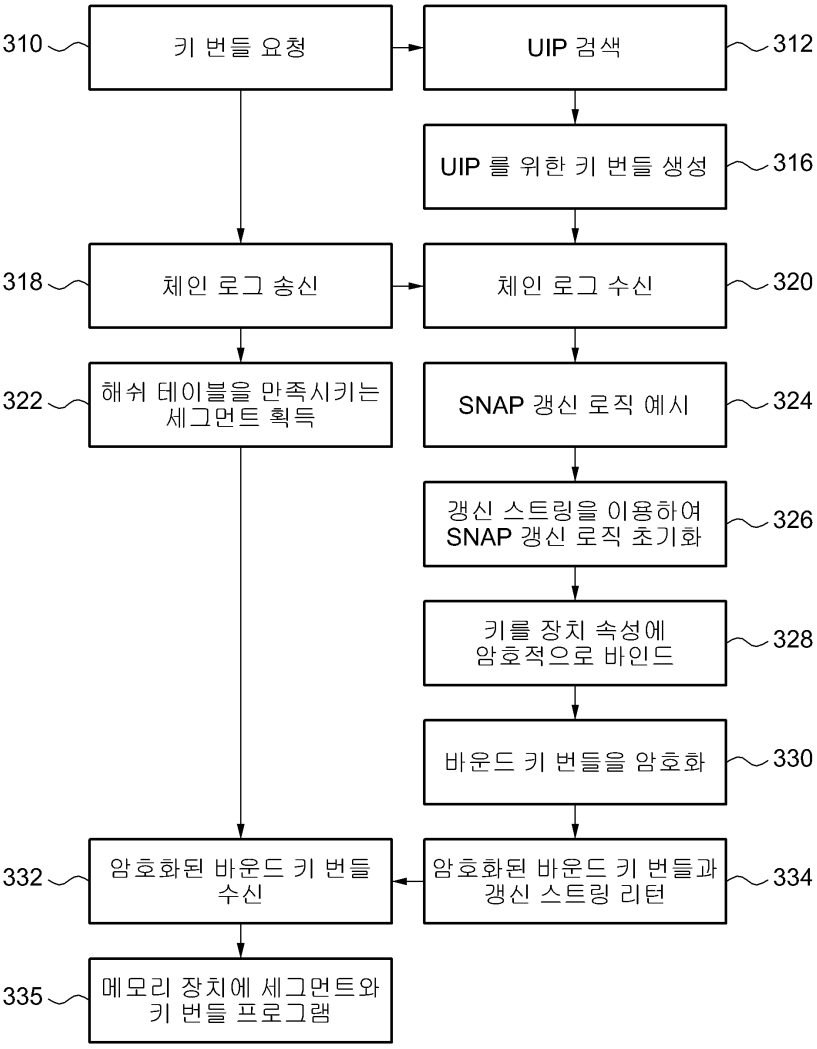
도면17


270
장치와 연결 및 업데이트
272
로그 파일 획득
274
파일을 인증하기 위해
로그 파일 해석/복호화
276
메모리 제어기 결과에 비교
280
불능
278
매치?
282
재생

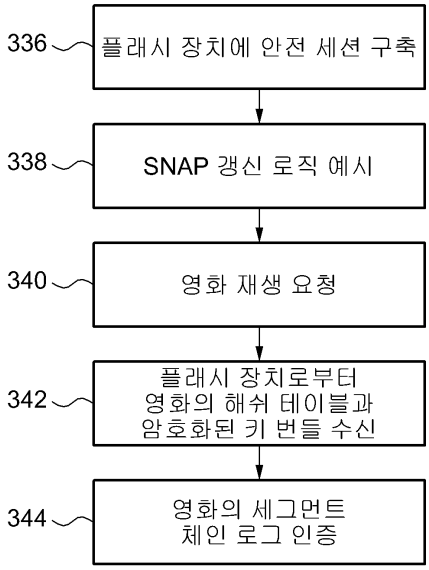
도면18


290
영화 요청
UIP 생성
292
UIP를 나타내는
해쉬 테이블 생성
296
298
해쉬 테이블 수신
해쉬 테이블 송신
300
302
해쉬 테이블을 만족시키는
세그먼트 획득
UIP에 제어기 ID 저장
304
306
세그먼트 체인 로그 생성

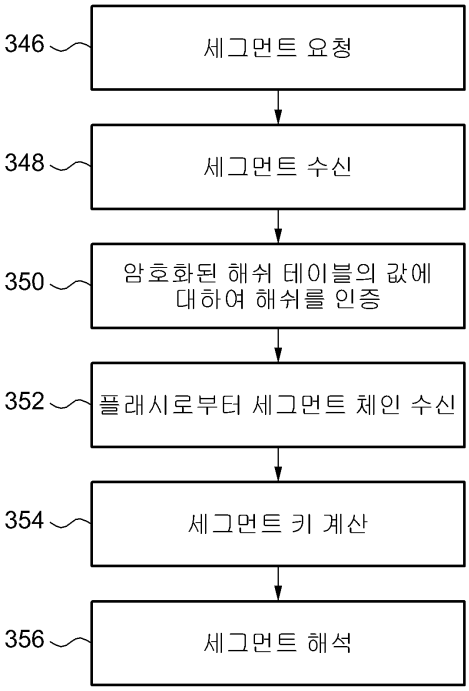
도면19


310
키 번들 요청
UIP 검색
312
UIP 를 위한 키 번들 생성
316
318
체인 로그 송신
체인 로그 수신
320
322
해쉬 테이블을 만족시키는
세그먼트 획득
SNAP 갱신 로직 예시
324
갱신 스트링을 이용하여
SNAP 갱신 로직 초기화
326
키를 장치 속성에
암호적으로 바인드
328
바운드 키 번들을 암호화
330
332
암호화된 바운드 키 번들
수신
암호화된 바운드 키 번들과
갱신 스트링 리턴
334
335
메모리 장치에 세그먼트와
키 번들 프로그램

도면20


336
플래시 장치에 안전 세션 구축
338
SNAP 갱신 로직 예시
340
영화 재생 요청
342
플래시 장치로부터
영화의 해쉬 테이블과
암호화된 키 번들 수신
344
영화의 세그먼트
체인 로그 인증

도면21


346
세그먼트 요청
348
세그먼트 수신
350
암호화된 해쉬 테이블의 값에
대하여 해쉬를 인증
352
플래시로부터 세그먼트 체인 수신
354
세그먼트 키 계산
356
세그먼트 해석