(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G11B 20/10

(45) 공고일자 2005년06월03일
(11) 등록번호 10-0493290
(24) 등록일자 2005년05월25일

(21) 출원번호 10-2002-0006375
(22) 출원일자 2002년02월05일

(65) 공개번호 10-2002-0065376
(43) 공개일자 2002년08월13일

(30) 우선권주장 60/265,884 2001년02월05일 미국(US)

(73) 특허권자 엘지전자 주식회사
서울특별시 영등포구 여의도동 20번지

(72) 발명자 벨렌코브야체슬라브에스.
러시아191123에스티.피터스버그유아이.쉬파레르나야36오피스501

쿠즈미히브세보로드엠.
러시아191123에스티.피터스버그유아이.쉬파레르나야36오피스501

(74) 대리인 김용인
심창섭

심사관 : 장현숙

(54) 디지털 미디어의 복제 제어 방법

요약

디지털 미디어 복제 제어 방법이 개시된다. 본 발명의 방법은 디지털 미디어 데이터의 어느 유형에도 적용가능하고, 특정 미디어 특성을 취하지 않는다. 상기 방법은 하이브리드 암호 기술을 사용하여 공개키로 디지털 미디어 데이터를 보호하는 단계와, 미디어 데이터를 워터마킹하는 단계와, 인증된 핸드쉐이크 프로토콜을 통한 출력 장치 적합성 테스트 단계를 포함한다. 하이브리드 암호 기술에 따른 미디어 데이터 보호로 인해, 사용불가능한 플레이 장치는 보호된 미디어 데이터 세트를 플레이하거나 읽을수 없다. 출력장치 적합성 테스트 프로토콜은 미디어 신호가 사용불가능한 장치에 복제되는 것을 방지하기 위해 사용된다. 본 발명의 이러한 특징은 비표준 장치에 불법 복제를 할 가능성을 줄이기 위해 사용된다. 또한, 플레이되고 기록된 미디어 신호들을 수정하고, 불법적인 복제 제조기를 검출하기 위한 관련 장치들에 대한 아이디 정보의 트랙을 유지하고, 불법 데이터 세트로부터 합법적인 미디어 데이터 세트를 분리시키기 위해 데이터 워터마킹이 사용된다.

대표도

도 1

색인어

복제, 디지터 미디어 데이터, 암호 기법

명세서

도면의 간단한 설명

본 발명의 이해를 돕기 위해 포함되고 본 출원에 포함되어 본 출원의 일부분을 구성하는 첨부된 도면은 본 발명의 실시예를 설명하며, 상세한 설명과 함께 본 발명의 원리를 설명하는 역할을 한다.

도 1은 본 발명에 따른 디지털 미디어 복제 제어 방법의 제1 단계를 보여준다.

도 2는 본 발명에 따른 디지털 미디어 복제 제어 방법의 제2 단계 및 후속 단계를 보여준다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 출원은 참고로 삽입된 Vyacheslav S. Beleko와 Vsebolod M. Kumich이름으로 2001년 2월 5일에 출원된 "디지털 미디어의 복제 제어 구조"라는 명칭의 미국 가출원 번호 60/265,884을 우선권으로 한다.

본 발명은 미디어 복제 제어에 관한 것으로, 특히 하이브리드 암호 기술과 워터마킹(watermarking) 기술 및 인증된 핸드쉐이크(handshake) 프로토콜을 이용하여 디지털 미디어의 안전한 복제 제어를 제공하는 디지털 미디어 복제 제어 방법에 관한 것이다.

컴퓨터 네트워크, 원격통신 시스템, 및 기타 시스템과 같은 통신 시스템은 정보의 보안유지를 위해 암호의 이용을 증가시키고 있다. 암호 기법은 크게 대칭키 암호기법과 공개키 암호기법으로 나누어진다. 대칭키 암호기법에서는 대칭(비밀)키가 데이터 암호 및 복호 처리를 위해 사용된다. 대칭키 암호 기법의 몇 가지 효율적인 실례(implementations)가 있지만, 그러한 실례의 실제 키 운용에 있어서는 문제가 자주 발생한다.

한편, 공개키 암호기법에서는 데이터 암호 및 복호 처리가 서로 독립적으로 이루어진다. 즉, 데이터 암호 처리는 주로 "e"로 지칭되는 공개키를 필요로 하고, 데이터 복호 처리는 수학적으로는 관련있지만 다른 비밀키 "d"를 필요로 한다. 따라서, 공개키를 가지는 한 개인(entity)은 기본 형태의 메시지인 평문(plaintext)을 암호화할 수는 있지만, 암호화된 형태의 메시지인 암호문(cypertext)을 복호화할 수는 없다.

개인이 공개키를 선택하고 공개키를 공개할 경우, 누구든지 공개키를 사용하여 상기 개인의 하나이상의 메시지를 암호화할 수 있다. 그러면, 상기 개인은 비밀키를 비밀로 유지하여 자신만이 메시지의 암호문을 복호화할수 있도록 한다. 현재, 공개키 암호기법의 실례는 대칭키 암호기법의 실례보다 덜 효율적이지만 더 안전하다.

하이브리드 암호기법에서는 평문이 대칭 알고리듬에 해당하는 대칭키로 암호화되고, 대칭키는 공개 알고리듬에 해당하는 공개키로 암호화된다. 공개키가 암호화된 대칭키와 대칭키가 암호화된 데이터를 수신할 때, 수신자는 먼저 자신의 비밀키를 사용하여 대칭키를 복호화한다. 그리고 나서, 수신자는 복호화된 대칭키를 사용하여 암호화된 데이터를 복호화한다. 하이브리드 암호기법에서 원래의 데이터를 얻는 과정은 보통 공개키 암호기법보다 빠르다. 또한, 하이브리드 암호기법은 매번 다른 대칭키 사용을 가능하게 하고, 대칭 알고리듬의 보안을 상당히 향상시킨다. 이러한 이유로, 하이브리드 암호기법은 보호된 미디어 데이터를 수신자에게 안전하게 전송하기 위해 이상적이다.

워터마킹은 저작권 정보(복제 보호를 나타내는 정보)가 미디어 데이터에 겹쳐진 워터마크에 의해 표현되는 기술이다. 상기 정보는 영상 데이터와 음향 데이터를 포함하는 다양한 미디어 데이터에 포함되고, 사람에게 보이거나 들리지 않아야 한다. 미디어 데이터에 워터마크를 겹치는 목적은 저작권의 증거물을 제공하여 미디어 데이터의 불법적인 사용 및 복제가 방지될수 있도록 하기 위한 것이다. 따라서, 호스트 신호가 데이터 처리 과정에 있을때에도 저작권 정보는 호스트 신호에 안정적으로 유지되어야 한다.

미디어 데이터에 워터마크를 겹치는 기술은 워터마크 데이터의 크기 및 호스트 신호의 데이터 처리에 대한 워터마크 데이터의 불변성(invariance)에 따라 달라진다. 인간의 지각능력, 대역폭 및 로버스트(robustness) 사이에는 워터마크 고유의 모순(trade-off)이 존재한다 (즉, 데이터가 공격에서 벗어나는 정도 또는 정상적인 사용을 통해 호스트 신호에 발생하는 변환). 겹치는 데이터가 많을수록, 인코딩 처리가 덜 안전하다. 겹치는 데이터가 적을수록, 인코딩 처리가 더 안전하다.

암호기법에서, 한 개인은 다른 개인들이 인증 절차를 통해 승인되는지의 여부를 확실히한다. 상기 인증 절차는 보통 핸드쉐이크 프로토콜 형태로 실행된다. 핸드쉐이크 처리시 인증하는 개인들은 그들의 정체 아이디(ID)와 함께 무작위로 발생된 데이터를 서로 교환한다. 핸드쉐이크 처리 결과가 분석된 후, 상대편 개인의 인증 결정이 이루어진다. 핸드쉐이크 처리를 보다 안전하게 수행하고 불법복제를 못하게 하기 위해, 공개키 암호기법이 자주 사용된다.

발명이 이루고자 하는 기술적 과제

본 발명은 종래기술의 한계 및 불이익으로 인한 문제점을 실질적으로 해결하는 디지털 미디어 데이터의 복제 제어 방법에 관한 것이다.

본 발명의 목적은 사용가능한(compliant) 비밀키를 갖는 사용가능한 장치들만이 미디어 데이터 세트를 플레이하거나 읽게 함으로써 디지털 미디어 데이터 세트를 보호하는 복제 제어 방법을 제공하는 것이다.

본 발명의 또다른 목적은 디지털 미디어 데이터 세트의 플레이 및 기록 처리를 디지털 워터마킹 기술을 이용하여 제어함으로써 디지털 미디어 데이터 세트를 보호하는 복제 제어 방법을 제공하는 것이다.

본 발명의 또다른 이점, 목적 및 특징은 다음의 검증을 통해 당해 기술 분야에서 통상의 기술을 가진 사람에게 명백해질 다음의 설명에서 제시되거나 본 발명의 실시로부터 알수 있을 것이다. 본 발명의 목적 및 다른 이점은 본 발명의 설명, 클레임 및 첨부된 도면에 설명된 구조에 의해 구현되고 얻어질 수 있다.

발명의 구성 및 작용

본 발명의 목적 및 이점을 달성하기 위해, 그리고 본 발명의 목적에 따라, 디지털 미디어의 제 1 복제 제어 방법은 대칭 알고리듬을 갖는 미디어키로 원래의 미디어 데이터 세트를 암호화하고 사용가능한(compliant) 장치들의 각 공개키로 상기 미디어키를 암호화하는 단계와, 상기 암호화된 미디어 데이터 세트와 상기 암호화된 미디어키를 사용가능한 플레이장치로 전달하는 단계와, 상기 플레이 장치의 비밀키로 상기 전달된 미디어키를 복호화하는 단계와, 상기 복호화된 미디어키로 상기 전달된 미디어 데이터 세트를 복호화하는 단계를 포함한다.

상기 제 1 복제 제어 방법은 상기 복호화된 데이터 세트가 "자유복제"로 표시되지 않을 경우 상기 플레이 장치의 플레이어 아이디(ID)와 플레이어 복제 제어 정보를 포함하는 플레이어 워터마크 (player watermark)를 상기 복호화된 미디어 데이터 세트에 추가하는 단계와, 상기 복호화된 미디어키로 상기 워터마크가 추가된 미디어 데이터 세트를 암호화하고 상기 사용가능한 장치의 각 공개키로 상기 복호화된 미디어키를 암호화하는 단계와, 상기 암호화된 미디어 데이터 세트와 미디어키를 사용가능한 기록장치에 패스하는 단계를 더 포함한다.

본 발명의 또다른 관점에서, 디지털 미디어의 제 2 복제 제어 방법은 대칭 알고리듬을 갖는 미디어키로 원래의 미디어 데이터 세트를 암호화하고 사용가능한 장치들의 각 공개키로 상기 미디어키를 암호화하는 단계와, 상기 암호화된 미디어 데이터 세트와 상기 암호화된 미디어키를 사용가능한 플레이 장치로 전달하는 단계와, 상기 플레이 장치의 비밀키로 상기 전달된 미디어키를 복호화하는 단계와, 상기 복호화된 미디어키로 상기 전달된 미디어 데이터 세트를 복호화하는 단계를 포함한다.

상기 제 2 복제 제어 방법은 상기 복호화된 데이터 세트가 "자유복제"로 표시되지 않을 경우 상기 플레이 장치의 플레이어 아이디(ID)와 플레이어 복제 제어 정보를 포함하는 플레이어 워터마크를 상기 복호화된 미디어 데이터 세트에 추가하는 단계와, 상기 플레이 장치와 디스플레이 장치 사이에서의 인증 핸드쉐이크(handshake) 처리를 통해 적합성 테스트를 수행하는 단계와, 상기 디스플레이 장치가 상기 테스트를 통과할 경우에 한해서 상기 워터마크가 추가된 미디어 데이터 세트를 상기 디스플레이 장치에 전송하는 단계를 더 포함한다.

전술한 총괄적인 기재사항과 후술하는 상세한 기재사항은 예시적이고 설명을 위한 것이며 청구되는 바의 본 발명의 보다 더 구체적인 설명을 제공하기 위하여 의도되는 것으로 이해되어야 한다.

[실시예]

본 발명의 바람직한 실시예가 첨부된 도면을 참조하여 상세히 설명될 것이다. 가능하다면 동일한 요소나 유사한 요소에 대해서는 도면을 통해 동일한 참조부호가 사용될 것이다.

디지털 미디어 복제 처리는 두단계로 나누어질 수 있다. 첫째, 플레이 장치는 미디어 데이터 세트를 읽으며(플레이키며), 플레이된 데이터 세트는 디스플레이 장치에 출력되거나 기록장치에 의해 기록된다. 도 1 및 도 2는 본 발명에 따른 디지털 미디어 복제 제어 방법의 제1단계, 제2단계 및 후속 단계를 각각 보여준다. 도면에서, 실선, 사선 및 점선은 미디어 데이터 스트림, 복제 제어 시스템 적용 결과 및 복제 제어 시스템에 의해 필터링된 데이터 스트림을 나타낸다.

미디어 데이터 세트가 하이브리드 암호 기술을 사용하여 암호화될 때, 사용가능한 플레이 장치들만이 암호화된 미디어 데이터 세트를 플레이시킬수 있다. 하이브리드 암호 기법에서, 미디어 데이터 세트는 대칭 알고리듬에 해당하는 미디어키(대칭키)로 암호화된다. 대칭키는 또한 사용가능한 플레이 장치의 공개키를 사용하여 공개키 알고리듬으로 암호화된다. 그리고나서, 암호화된 대칭키와 암호화된 미디어 데이터 세트는 하나의 이상의 목표 플레이 장치에 전달된다. 대칭키의 암호처리는 각각의 사용가능한 플레이 장치의 공개키에 대해 수행된다. 각각의 사용가능한 플레이 장치는 자신의 비밀키를 사용하여 암호화된 미디어키(대칭키)를 복호화시킨다. 미디어키의 공개-키 암호화 및 미디어 데이터 세트의 미디어-키 암호화의 암호화 레벨이 선택되어 암호화된 데이터가 알려진 유형의 공격에 대항하여 충분히 안전하게 유지될 수 있도록 한다. 상기 설명된 암호 기법은 도 1 및 도 2에 도시된 디지털 미디어 보호 시스템 (Digital Media Protection System(DMPS))이라 지칭된다.

사용가능한 플레이 장치가 원래의 미디어 데이터 세트를 플레이시킬 때, 사용가능한 플레이 장치는 워터마킹 능력을 가질 경우 플레이어 워터마크 (player watermark)를 플레이된 미디어 신호에 포함시킬수 있다. 원래의 미디어 신호는 소유자 아이디 (owner identification) 및 복제 제어 정보를 포함하는 소유자 워터마크 (W1)를 포함하여야 한다. 플레이어 워터마크는 소유자 복제 제어 정보로부터 파생된 변형된 복제 제어 정보 및 플레이어 아이디를 포함한다. "자유복제(free copy)"로 표시된 미디어 데이터 세트에 대해서는 사용가능한 플레이 장치가 플레이어 워터마크를 포함하지 않는다.

사용가능한 플레이 장치가 암호화된 미디어 데이터 세트를 복호화하고 이어서 플레이어 워터마크를 미디어 데이터 세트에 추가한 후, 상기 플레이 장치는 디지털 미디어 신호를 일반적으로 디지털 디스플레이장치 및 디지털 기록장치 중 하나인 출력장치로 패스한다. 미디어 신호가 디지털 디스플레이 장치로 출력될 때, 미디어 신호는 DMPS에 의해 보호되지 않는다. 반면에, 미디어 신호가 기록장치로 출력될 때, 미디어 신호는 DMPS에 의해 보호되어야 한다. 즉, 미디어 신호는 플레이 장치와 기록장치의 적합성(compliance)을 제공하기 위해 DMPS 구조를 포함하여야 한다. 또한, 미디어 데이터 세트가 디스플레이 장치에 전송될 때, 데이터 세트는 "디스플레이만 허용(for display only)"으로 세팅된 복제 제어 정보 세트로 구성된 플레이어 워터마크를 포함하여야 한다.

플레이 장치와 디스플레이 장치 사이에 데이터 차단(interception)을 방지하기 위해, 복제 방지된 디지털 전송 프로토콜(예를들어, AKE로 구성된 1394)이 사용되어야 한다. 상기 프로토콜은 인증된 핸드쉐이킹 처리를 통해 상기 장치들 사이에 적합성 테스트를 제공한다. 디스플레이 장치의 인증이 승인되지 않을 경우, 미디어 데이터 세트는 디스플레이 장치에

전송되어서는 안된다. 실제로, 정당한 장치 인증을 갖는 일반적인 기록장치가 디스플레이 장치를 대신할 수도 있고 AKE처리를 잘못되게 할수도 있다. 따라서, 본 발명에 따른 상기 복제 제어 시스템은 이론적으로 해결가능한 것으로 간주될수 있고, 불법 복제가 그러한 방식으로 이루어질 수도 있다. 물론, 복제는 소유자 워터마크와 플레이어 워터마크를 포함한다.

플레이 장치가 미디어 데이터 세트를 기록장치에 패스할 때, 플레이 장치는 DMPS 보호된 형태로 세팅된 데이터를 원래의 미디어 데이터 세트에 저장된 데이터 세트로서 출력한다. 따라서, 추가적인 데이터 전송 보호가 요구되지 않는다. 임의의 기록장치가 플레이 장치로부터 수신된 데이터 세트를 위한 "복사만가능한" ("dump-only") 장치가 될 것이기 때문에 기록장치의 적합성 테스트는 선택적이다.

합법적인 미디어 복제가 사용가능한 플레이 장치에서 이루어질 때, 디지털 미디어 복제 제어 시스템 (Digital Media Copy Control System (DMCCS))이 동작한다. 서로 관련이 없는 복제 제어 정보를 갖는 소유자 워터마크와 플레이어 워터마크를 미디어 데이터 세트가 포함할 경우, 또는 플레이어 워터마크가 "디스플레이만 허용"으로 표시될 경우, 미디어 데이터 세트는 플레이 장치에 의해 거부된다. 원래의 미디어 데이터 세트 또는 그 복제가 기록장치로 전송되려고 할 때, 플레이 장치의 DMCCS는 먼저 워터마크 복제 제어 정보를 확인하고, 미디어 데이터 세트가 "복제방지(no copy)"로 표시되어 있을 경우 복제되는 것을 방지한다.

합법적인 미디어 데이터 세트 및 그 복제는 DMPS에 의해 보호되므로 사용불가능한(non-compliant) 플레이 장치와 호환되지 않는다. 같은 이유로 불법적인 복제는 사용가능한 플레이 장치와 호환되지 않는다. 따라서, 본 발명의 이러한 특징은 일반 사용자가 미디어 데이터 세트의 불법 복제하는 행위를 막는다. 또한, 플레이어 워터마크는 모든 플레이 장치의 개별적인 아이디를 포함하여 불법적인 복제의 출처가 확인될 수 있도록 한다.

본 발명의 기술사상 또는 범위를 벗어남 없이 본 발명에 다양한 변형 및 수정이 이루어질 수 있다는 것이 당해 기술 분야에서 통상의 기술을 가진 사람에게는 명백할 것이다. 따라서, 본 발명의 변형이 및 수정이 첨부된 클레임 및 그 등가물의 범위내에 있다는 것을 전제로 본 발명은 그 변형 및 수정을 포함한다는 것이 의도된다.

발명의 효과

상기 내용에 포함되어 있음.

(57) 청구의 범위

청구항 1.

(a) 대칭 알고리듬을 갖는 미디어키로 암호화하고자 하는 원래의 미디어 데이터 세트를 암호화하고 사용가능한(compliant) 각 플레이 장치가 갖는 공개키로 상기 미디어키를 암호화하는 단계와,

(b) 상기 암호화된 미디어 데이터 세트와 상기 암호화된 미디어키를 사용가능한 플레이장치로 전달하는 단계와,

(c) 상기 플레이 장치의 비밀키로 상기 전달된 미디어키를 복호화하는 단계와,

(d) 상기 복호화된 미디어키로 상기 전달된 미디어 데이터 세트를 복호화하는 단계와,

(e) 상기 복호화된 데이터 세트가 "자유복제"로 표시되지 않을 경우 상기 플레이 장치의 플레이어 아이디(ID)와 플레이어 복제 제어 정보를 포함하는 플레이어 워터마크 (player watermark)를 상기 복호화된 미디어 데이터 세트에 추가하는 단계와,

(f) 상기 복호화된 미디어 키로 상기 워터마크가 추가된 미디어 데이터 세트를 암호화하고 상기 사용가능한 장치의 각 공개키로 상기 복호화된 미디어키를 암호화하는 단계와,

(g) 상기 (f) 단계에서 암호화된 상기 미디어 데이터 세트와 미디어키를 사용가능한 기록장치에 패스하는 단계를 포함하여 구성되는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 2.

제 1항에 있어서, 상기 각 공개키는 비대칭 알고리듬에 해당하는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 3.

제 1항에 있어서, 상기 원래의 미디어 데이터 세트는 소유자 아이디와 소유자 복제 제어 정보를 포함하는 소유자 워터마크를 포함하는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 4.

제 3항에 있어서, 상기 플레이어 복제 제어 정보는 소유자 복제 제어 정보로부터 파생된 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 5.

(a) 대칭 알고리듬을 갖는 미디어키로 암호화하고자 하는 원래의 미디어 데이터 세트를 암호화하고 사용가능한(compliant) 각 플레이 장치가 갖는 공개키로 상기 미디어키를 암호화하는 단계와,

(b) 상기 암호화된 미디어 데이터 세트와 상기 암호화된 미디어키를 사용가능한 플레이장치로 전달하는 단계와,

(c) 상기 플레이 장치의 비밀키로 상기 전달된 미디어키를 복호화하는 단계와,

(d) 상기 복호화된 미디어키로 상기 전달된 미디어 데이터 세트를 복호화하는 단계와,

(e) 상기 복호화된 데이터 세트가 "자유복제"로 표시되지 않을 경우 상기 플레이 장치의 플레이어 아이디(ID)와 플레이어 복제 제어 정보를 포함하는 플레이어 워터마크 (player watermark)를 상기 복호화된 미디어 데이터 세트에 추가하는 단계와,

(f) 상기 플레이 장치와 디스플레이 장치 사이에서의 인증 핸드쉐이크(handshake) 처리를 통해 적합성 테스트를 수행하는 단계와,

(g) 상기 디스플레이 장치가 상기 테스트를 통과할 경우에 한해서 상기 워터마크가 추가된 미디어 데이터 세트를 상기 디스플레이 장치에 전송하는 단계를 포함하여 구성되는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 6.

제 5항에 있어서, 상기 각 공개키는 비대칭 알고리듬에 해당하는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 7.

제 5항에 있어서, 상기 원래의 미디어 데이터 세트는 소유자 아이디와 소유자 복제 제어 정보를 포함하는 소유자 워터마크를 포함하는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 8.

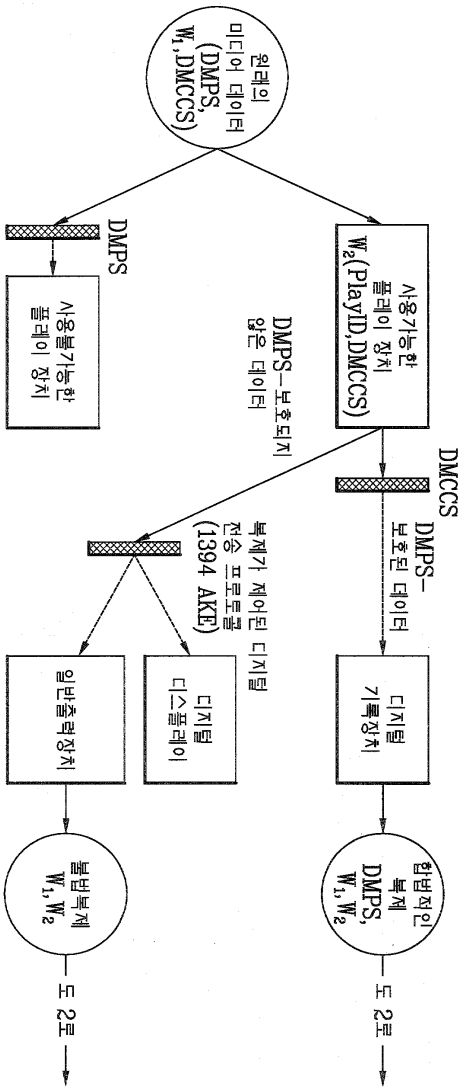
제 7항에 있어서, 상기 플레이어 복제 제어 정보는 상기 소유자 복제 제어 정보로부터 파생된 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

청구항 9.

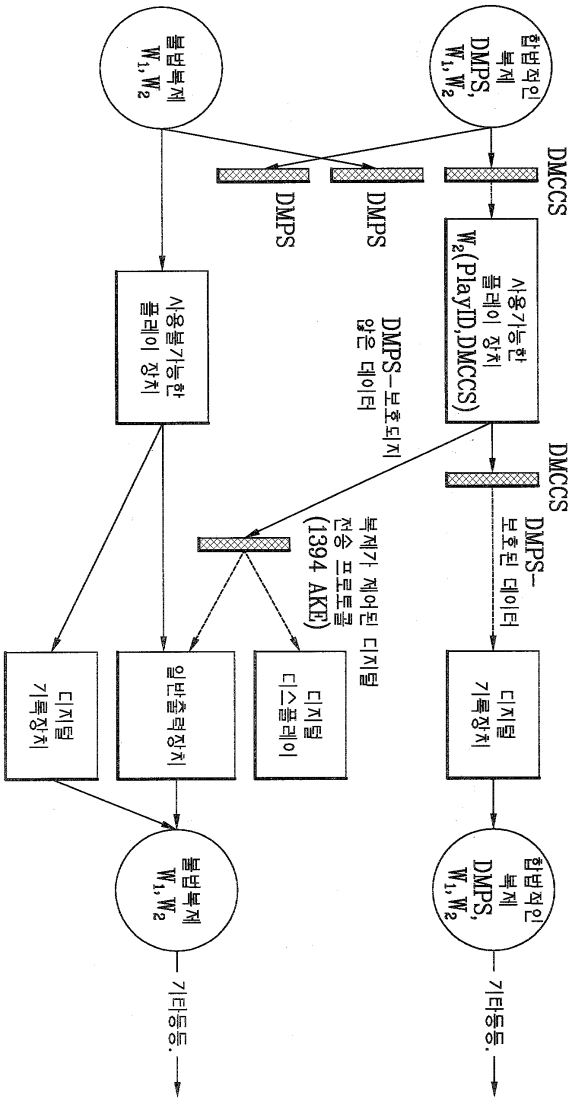
제 5항에 있어서, 상기 플레이어 복제 제어 정보는 "디스플레이만 허용(for display only")으로 세팅되는 것을 특징으로 하는 디지털 미디어의 복제 제어 방법.

도면

도면1


원래의
미디어 데이터
(DMPS,
W1,DMCCS)
DMPS
사용불가능한
플레이 장치
사용가능한
플레이 장치
W2(PlayID,DMCCS)
DMPS-보호되지
않은 데이터
DMCCS
DMPS-
보호된 데이터
복제가 제어된 디지털
전송 프로토콜
(1394 AKE)
일반출력장치
디지털
디스플레이
디지털
기록장치
불법복제
W1,W2
합법적인
복제
DMPS,
W1,W2
도 2로
도 2로

도면2


합법적인 복제 DMPS, W1, W2
불법복제 W1, W2
DMCCS
DMPS
DMPS
사용가능한 플레이 장치 W2(PlayID,DMCCS)
사용불가능한 플레이 장치
DMPS-보호되지 않은 데이터
DMCCS
DMPS-보호된 데이터
복제가 제어된 디지털 전송 프로토콜 (1394 AKE)
디지털 기록장치
일반출력장치
디지털 디스플레이
디지털 기록장치
불법복제 W1, W2
합법적인 복제 DMPS, W1, W2
기타등등.
기타등등.