(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G06F 17/40

(45) 공고일자 2003년08월09일
(11) 등록번호 10-0394177
(24) 등록일자 2003년07월28일

(21) 출원번호 10-2000-0015753
(22) 출원일자 2000년03월28일

(65) 공개번호 특2001-0014639
(43) 공개일자 2001년02월26일

(30) 우선권주장 99-124182 1999년04월30일 일본(JP)

(73) 특허권자
가부시끼가이샤 도시바
일본국 도꾜도 미나또꾸 시바우라 1쪼메 1방 1고

(72) 발명자
가미바야시도루
일본가나가와켄치가사키시혼주쿠쵸3-18-108

다무라마사후미
일본도쿄도쵸후시쵸후가오카1-18-76-706

가토다쿠
일본가나가와켄가마쿠라시조메이지3-12-20

이시바시야스히로
일본도쿄도오메시신마치9-4-1루미에루-신마치1-313

야마다히사시
일본가나가와켄요코하마시도츠카쿠도츠카쵸2709-3

도마히데유키
일본도쿄도오메시신마치9-2031-1구레아레-도시바-오메비506

(74) 대리인
이상섭
나영환
김승호
안성탁

심사관 : 조영갑

(54) 콘텐츠 관리 방법 및 콘텐츠 관리 장치

요약

기억 매체(13)에 기억할 수 있는 복제 콘텐츠의 수를 규제하기 위한 콘텐츠 관리 방법에 있어서, SMS(2)는 상기 콘텐츠마다 미리 정해진 복제 가능 콘텐츠 수를 부여하여, 상기 기억 매체(13)로의 복제 기록 지시를 수신하면, 상기 복제 가능 콘텐츠 수에 잔여수가 있을 때, 상기 기억 매체(13)에 상기 복제 콘텐츠를 기록하고, 그 때, 상기 기억 매체(13)에 복제 콘텐츠를 하나 기록할 때마다 상기 복제 가능 콘텐츠 수로부터 1 감산하며, 또, 상기 기억 매체(13)의 상기 복제 콘텐츠의 소거 지시를 수신하면, 상기 기억 매체(13)로부터 상기 복제 콘텐츠를 하나 소거할 때마다 상기 복제 가능 콘텐츠 수를 1 가산한다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 기억 매체에 기억할 수 있는 복제 콘텐츠의 수를 규제하기 위한 콘텐츠 관리 방법을 이용한 음악 콘텐츠 이용 관리 시스템(LCM)의 구성예를 도시한 도면.
도 2는 메모리 영역의 구성예를 도시한 도면.
도 3은 기록 재생 장치(PD)의 내부 구성예를 도시한 도면.
도 4a 내지 도 4c는 3종류의 기억 매체의 특징을 설명하기 위한 도면.
도 5는 미디어 인터페이스(I/F)부의 내부 구성예를 도시한 도면.
도 6은 체크인후의 기억 매체의 기록 내용을 설명하기 위한 도면.
도 7a 내지 도 7c는 LCM의 은닉 영역에 저장되어 있는 숙박부의 기억예를 도시한 도면.
도 8a 및 도 8b는 LCM의 은닉 영역에 저장되어 있는 숙박부의 다른 기억예를 도시한 도면.
도 9는 체크인/체크아웃 처리 순서를 설명하기 위한 흐름도로, 미디어의 종별을 판별하여, 그 종별에 따른 처리를 선택하기까지의 순서를 나타낸 도면.
도 10은 기억 매체의 종별이 레벨 2인 경우의 체크아웃 순서를 설명하기 위 한 도면.
도 11은 기억 매체의 종별이 레벨 2인 경우의 체크인 순서를 설명하기 위한 도면.
도 12는 기억 매체의 종별이 레벨 2인 경우의 재생 순서를 설명하기 위한 도면.
도 13은 기억 매체의 종별이 레벨 1인 경우의 체크아웃 순서를 설명하기 위한 도면.
도 14는 기억 매체의 종별이 레벨 1인 경우의 재생 순서를 설명하기 위한 도면.
도 15는 기억 매체의 종별이 레벨 0인 경우의 체크아웃 순서를 설명하기 위한 도면.
도 16은 기억 매체의 종별이 레벨 0인 경우의 체크인 순서를 설명하기 위한 도면.
도 17은 기억 매체의 종별이 레벨 0인 경우의 재생 순서를 설명하기 위한 도면.
도 18a 내지 도 18c는 LCM의 은닉 영역에 저장되어 있는 숙박부의 또 다른 기억예를 도시한 도면으로, 플래그를 포함하는 숙박부를 도시한 도면.
도 19는 플래그를 이용한 체크인 처리의 개략을 설명하기 위한 흐름도.
도 20은 공개키 암호화 방식을 이용한 인증 순서를 설명하기 위한 도면.
도 21은 네트워크를 통해 기억 매체로의 복제 콘텐츠의 기록을 행하는 경우 의 기기 구성예를 도시한 도면.
도 22는 타임아웃 판정부의 내부 구성예를 도시한 도면.
도 23은 타임아웃 판정 처리의 일례를 설명하기 위한 흐름도.
도 24는 은닉 영역을 구성하기 위한 파일 시스템을 설명하기 위한 도면.
도 25는 은닉 영역 드라이버의 동작을 설명하기 위한 흐름도.
도 26은 섹터 배치 갱신시의 은닉 영역 드라이버의 동작을 설명하기 위한 흐름도.
<도면의 주요부분에 대한 부호의 설명>
1 : 콘텐츠 이용 관리 시스템
2 : 보안 콘텐츠 서버(SMS)
3 : EMD 인터페이스부
4 : 타임아웃 판정부
5 : PD 인터페이스(I/F)부
6 : 미디어 인터페이스(I/F)부
7 : 은닉 영역 드라이버
8 : 숙박부 저장부
9 : 라이센스 저장부
10 : 음악 데이터 저장부
11 : CD 인터페이스(I/F)부
12 : 기록 재생 장치(PD)
13 : 기억 매체(MC)

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 기억 매체에 기억할 수 있는 음악이나 영화 등의 복제 콘텐츠의 수를 규제하기 위한 콘텐츠 관리 방법 및 그것을 이용한 콘텐츠 관리 장치에 관한 것이다.
종래로부터 콘텐츠(저작물 등)는 복사 관리가 행해져 왔다. 복사 세대 관리나 복사의 수를 관리함으로써, 저작권 보호와 이용 편의의 밸런스를 잡아 왔다.
또, 복사 관리 대신에, 「이동」의 개념이 등장했다. 복사가 오리지널 데이터를 소거하지 않는 것과 대조적으로, 이동은 다른 장소(미디어)에 데이터를 전송하는 동시에, 오리지널 데이터를 소거한다. 콘텐츠의 디지탈화와 네트워크 등의 보급이, 이동에 의한 복사 보호가 등장한 배경에 있다.
최근, 네트워크 등을 통한 오리지널의 충실한 복사가 가능하게 되었기 때문에, 복사 관리만으로는 저작권 보호가 곤란하게 되고 있다. 또한, 미디어에서 미디어로의 무제한적 이동, 예컨대, 데이터의 영리 목적의(이동에 의한) 배포는 저작권 관리를 할 수 없다.
이와 같이, 오리지널 데이터(특히, 저작권 보호의 대상이 되는 콘텐츠)의 복제를 확실하게 관리하는 것이 곤란하게 되었다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은 기억 매체에 기록할 수 있는 복제 콘텐츠의 수를 규제함으로써 콘텐츠의 복제를 제한하여, 콘텐츠의 저작권을 보호할 수 있는 콘텐츠 관리 방법 및 그것을 이용한 콘텐츠 관리 장치를 제공하는 데에 있다.

발명의 구성 및 작용

본 발명의 한 관점에 따르면, 상기 콘텐츠마다 미리 정해진 복제 가능 콘텐츠 수를 부여하고, 상기 기억 매체로의 복제 기록 지시를 수신하면, 상기 복제 가능 콘텐츠 수에 잔여수가 있을 때, 그 기억 매체에 상기 복제 콘텐츠를 기록하고, 상기 기록시에, 상기 기억 매체에 복제 콘텐츠를 하나 기록할 때마다 상기 복제 가능 콘텐츠 수로부터 1 감산하며, 또 상기 기억 매체의 상기 복제 콘텐츠의 소거 지시를 수신하면, 그 기억 매체로부터 상기 복제 콘텐츠를 하나 소거할 때마다 상기 복제 가능 콘텐츠 수를 1 가산하는 것을 특징으로 하는 기억 매체에 기억할 수 있는 복제 콘텐츠의 수를 규제하기 위한 콘텐츠 관리 방법이 제공된다.
상기 방법은 또한, 상기 기억 매체의 기억 영역에 설치된 은닉된 특정 순서에 의해 액세스 가능한 은닉 영역에, 상기 복제 콘텐츠를 재생하기 위해 필요한 정보를 기록하는 것을 포함하고 있더라도 좋다.
상기 방법은 또한, 상기 콘텐츠마다의 적어도 상기 복제 가능 콘텐츠 수를 은닉된 특정 순서에 의해 액세스 가능한 은닉 기억 영역에 기록하는 것을 포함하고 있더라도 좋다.
상기 방법은 또한, 상기 콘텐츠마다의 적어도 상기 복제 가능 콘텐츠 수와 복제 콘텐츠를 기억한 기억 매체의 식별 정보를 은닉된 특정 순서에 의해 액세스 가능한 은닉 기억 영역에 기억하여, 상기 은닉 기억 영역에 상기 기억 매체의 식별 정보가 기억되어 있을 때에만 그 기억 매체로부터 상기 복제 콘텐츠를 소거하는 것을 포함하고 있더라도 좋다.
상기 방법은 또한, 상기 기억 매체에 상기 복제 콘텐츠를 기록할 때, 그 기억 매체의 기억 영역에 설치된 은닉된 특정 순서에 의해 액세스 가능한 은닉 영역에, 상기 복제 콘텐츠를 재생하기 위해 필요한 정보와 상기 복제 콘텐츠의 이동의 가부를 나타내는 플래그 정보를 기록하고, 상기 플래그 정보를 참조하여, 상기 복제 콘텐츠의 이동의 가부를 판단하는 것을 포함하고 있더라도 좋다.
상기 방법은 또한, 상기 기억 매체에 대한 데이터의 판독 혹은 기록 처리에 걸리는 시간이 소정 시간 이내가 아닐 때, 이후의 처리를 중단하는 것을 포함하고 있더라도 좋다.
상기 방법에 있어서, 상기 기억 매체로서, 그 기억 영역 내에, 은닉된 특정한 순서만에 의해 액세스 가능한 은닉 영역이 설치되는 동시에 그 기억 매체의 식별 정보가 기억된 제1 종별의 기억 매체와, 상기 은닉 영역을 구비하지 않지만 그 기억 매체의 식별 정보는 갖고 있는 제2 종별의 기억 매체와, 상기 은닉 영역 및 상기 기억 매체의 식별 정보를 갖지 않는 제3 종별의 기억 매체가 있더라도 좋다. 이 경우, 상기 기억 매체에 복제 콘텐츠를 기록할 때 및 상기 기억 매체로부터 복제 콘텐츠를 소거할 때 및 상기 기억 매체에 기억된 복제 콘텐츠를 재생할 때에는, 그 기억 매체의 종별을 판별하고 나서, 그에 따른 처리를 실시한다.
본 발명의 다른 관점에 따르면, 기억 매체에 기억할 수 있는 복제 콘텐츠의 수를 규제하기 위한 콘텐츠 관리 장치에 있어서, 상기 콘텐츠마다 미리 정해진 복제 가능 콘텐츠 수를 부여하여, 상기 기억 매체로의 복제 기록 지시를 수신하면, 그 복제 가능 콘텐츠 수에 잔여수가 있을 때, 상기 기억 매체에 상기 복제 콘텐츠를 기록하고, 그 때, 상기 기억 매체에 복제 콘텐츠를 하나 기록할 때마다 상기 복제 가능 콘텐츠 수로부터 1 감산하는 복제 콘텐츠 기록 수단과; 상기 기억 매체의 상기 복제 콘텐츠의 소거 지시를 수신하면, 상기 기억 매체로부터 상기 복제 콘텐츠를 하나 소거할 때마다 상기 복제 가능 콘텐츠 수를 1 가산하는 복제 콘텐츠 이동 수단을 포함하는 것을 특징으로 하는 콘텐츠 관리 장치를 제공한다.
상기 장치는 또한, 상기 기억 매체의 기억 영역에 설치된 은닉된 특정 순서에 의해 액세스 가능한 은닉 영역에, 상기 복제 콘텐츠를 재생하기 위해 필요한 정보를 기록하는 수단을 갖추고 있더라도 좋다.
상기 장치는 또한, 상기 콘텐츠마다의 적어도 상기 복제 가능 콘텐츠 수를 은닉된 특정 순서에 의해 액세스 가능한 은닉 기억 영역에 기록하는 수단을 갖추고 있더라도 좋다.

상기 장치는 또한, 상기 콘텐츠마다의 적어도 상기 복제 가능 콘텐츠 수와 복제 콘텐츠를 기억한 기억 매체의 식별 정보를 은닉된 특정 순서에 의해 액세스 가능한 은닉 기억 영역에 기억하는 수단과, 상기 은닉 기억 영역에 상기 기억 매체의 식별 정보가 기억되어 있을 때에만 상기 기억 매체로부터 상기 복제 콘텐츠를 소거하는 수단을 구비하고 있더라도 좋다.
상기 장치는 또한, 상기 기억 매체의 기억 영역에 설치된 은닉된 특정 순서 에 의해 액세스 가능한 은닉 영역에, 상기 복제 콘텐츠를 재생하기 위해 필요한 정보와 상기 복제 콘텐츠의 이동의 가부를 나타내는 플래그 정보를 기록하는 수단과, 상기 플래그 정보를 참조하여, 상기 복제 콘텐츠의 이동의 가부를 판단하는 수단을 구비하고 있더라도 좋다.
상기 장치는 또한, 상기 기억 매체에 대한 데이터의 판독 혹은 기록 처리에 걸리는 시간이 소정 시간 이내가 아닐 때, 이후의 처리를 중단하는 수단을 갖추고 있더라도 좋다.
상기 장치는 또한, 상기 기억 매체에 복제 콘텐츠를 기록할 때 및 상기 기억 매체로부터 복제 콘텐츠를 소거할 때 및 상기 기억 매체에 기억된 복제 콘텐츠를 재생할 때에는 상기 기억 매체가, 그 기억 영역 내에 은닉된 특정 순서에 의해 액세스 가능한 은닉 영역이 설치되는 동시에 상기 기억 매체의 식별 정보가 기억된 제1 종별의 기억 매체인지, 상기 은닉 영역을 구비하지 않지만 상기 기억 매체의 식별 정보는 갖고 있는 제2 종별의 기억 매체인지, 상기 은닉 영역 및 상기 기억 매체의 식별 정보를 갖지 않는 제3 종별의 기억 매체인지를 판별하는 판별 수단을 갖추고 있더라도 좋다. 이 경우, 상기 장치는 또한, 상기 판별 수단에 의해 판별된 상기 기억 매체의 종별에 따른 처리를 실시하는 수단을 갖추고 있더라도 좋다.
이하, 본 발명의 실시예에 관해서, 도면을 참조하여 설명한다.
도 1은 본 실시예에 따른 기억 매체에 기억할 수 있는 복제 콘텐츠의 수를 규제하기 위한 콘텐츠 관리 방법을 이용한 음악 콘텐츠 이용 관리 시스템(이하, 간단히 LCM이라고 부르는 경우가 있음)(1)의 구성예를 도시한 것이다. 또, 여기서는 콘텐츠로서 음악을 일례로서 이용하고 있지만, 이 경우에 한정하지 않고, 영화나, 게임 소프트 등이라도 좋다. 또한, 미디어로서 메모리 카드(MC)를 이용하고 있지만, 이 경우에 한정하는 것은 아니며, 플로피 디스크, DVD 등의 각종 기억 매체라도 좋다.
EMD(Electronic Music Distributor)는 음악 신호 전송 서버 또는 음악 신호 전송 방송국이다.
콘텐츠 이용 관리 시스템(1)은 예컨대, 퍼스널 컴퓨터(PC)이며, 복수의 EMD(여기서는, EMD #1 #3)에 대응한 수신부(#1 #3)를 구비하고 있고, EMD가 신호 전송하는 암호화 콘텐츠 또는 그 라이센스(이용 조건과 암호화 콘텐츠 복호키) 등을 수신한다. 수신부(#1 #3)는 재생 기능이나 요금 부과 기능을 갖고 있더라도 좋다. 신호 전송된 음악 콘텐츠를 시청(試聽)하기 위하여 재생 기능이 이용된다. 또, 요금 부과 기능을 이용하여, 마음에 든 콘텐츠를 구입하는 일이 가능하다.
LCM(1)은 보안 · 콘텐츠 · 서버(여기서는, Secure Music Server: SM으로, 이하, 간단히 SMS이라 부르는 경우가 있음)(2)를 구비하며, 이용자가 구입한 콘텐츠는 EMD 인터페이스(I/F)부(3)를 경유하여 SMS(2)에 축적된다. 음악 콘텐츠는 필요에 따라서 EMD I/F부(3)에서 복호되어, 형식 변환이나 재암호화가 행해진다. SMS(2)가 암호화 콘텐츠를 수취하면, 그것을 음악 데이터 저장부(10)에 저장하고, 음악 데이터 복호키를 라이센스 저장부(9)에 저장한다. SMS(2)가 재생 기능을 갖고 있더라도 좋다. 그 재생 기능에 의해, SMS(2)가 관리하는 음악 콘텐츠를 PC 상에서 재생할 수 있다.
SMS(2)는 미디어(이하, 간단히 MC(Memory Card)라 부르는 경우가 있음)(13)에 대하여 콘텐츠 데이터를 출력하는 기능을 갖고 있다. MC(13)를 기록 재생 장치(이하, 간단히 PD(Portable Device)라 부르는 경우가 있음)(12)에 셋트하여, MC(13)에 기록된 콘텐츠를 재생할 수 있다.
SMS(2)에서 MC(13)로의 콘텐츠의 기록은 미디어(MC) 인터페이스(I/F)부(6)를 통해 직접 행해지거나, 또는 PD(12)을 경유하여 행할 수 있다.
MC(13)는 그 미디어 고유 또한 재기록 불능의 식별 정보 MID를 갖고 있으며, MC(13)에 저장되는 콘텐츠는 MC(13)에 의존하는 콘텐츠 복호키에 의해 암호화된다.
콘텐츠 복호키는 미디어 I/F부(6) 및 PD(12) 내부에 저장되어 있는 암호키(Kp)에 의해 암호화되어, MC(13)에 기록된다.
MC(13) 내의 콘텐츠 및 콘텐츠 복호키는 별개의 임의의 기억 매체(이하, MCb라 부름)에 복사하는 일이 가능하지만,
1. 정통한 PD(12)만이 암호키(Kp)를 갖는 것으로부터, MCb에 저장된 콘텐츠는 정통한 PD(12)가 아니면 정확하게 재생되지 않는다. 그런데,
2. MC(13)의 식별 정보 MID는 복사할 수 없는 것으로부터, MCb의 식별 정보 MID는 복사원(source)의 MC(13)의 식별 정보 MID와는 상이하고, 결국, MCb에 복사된 콘텐츠를 정확하게 재생할 수 없다. 즉, SMS(2)이 MC(13)에 기록한 복제 콘텐츠가, 차례로 별도의 MC에 복사되어 이용되는 일이 방지되고 있다.
이상이 종래부터 생각되고 있는 LCM(1)의 구성이지만, 다음에, 본 발명에 관한 방법 및 구성부에 관해서 설명한다.
우선, 체크인/체크아웃에 관해서, 도 1의 LCM(1)에 입각하여 설명한다.
체크아웃이란, LMS1이 「부모」로서의 콘텐츠를 저장하고 있고, MC(13)에, 그 복제를 「자식」 콘텐츠로서 복사하는 것을 말한다. 「자식」 콘텐츠는 PD(12)에 의해 자유롭게 재생하는 일이 가능하지만, 「자식」에서 「손자」 콘텐츠를 작성하는 일은 허락되지 않는다. 「부모」가 몇 「자식」을 낳는가는 「부모」의 속성으로서 정의된다. 또한, 체크인이란, 예컨대, MC(13)를 LCM(1)에 접속하여, LCM(1)이 「자식」 콘텐츠를 소거(또는 이용 불능)함으로써, LCM(1) 내의 「부모」 콘텐츠는 「자식」을 하나 만드는 권리를 회복하는 것을 말한다. 이것을 「부모」에게 체크인한다라고도 한다.
이 체크인/체크아웃을 단순히, 종래부터의 LCM(1)으로 실현하고자 하면, 실제로, 다음과 같은 '공격(attack)'이 존재한다. 즉, MC(13)에 저장된 「자식」을 별도의 기억 미디어에(MID를 제외) 퇴피(退避)시켜 두고, MC(13)의 「자식

」을 「부모」에 체크인한다. 계속해서, 앞서 퇴피해 둔 「자식」을 상기 MC(13)에 재기록한다. 이미 체크인은 완료되어 있기 때문에, LCM(1) 상의 「부모」는 별도의 MC(13)에 「자식」을 복사해도 좋다. 이 방법으로, 임의의 갯수만큼 이용 가능한「자식」을 만드는 일이 가능하다.

전술한 「공격」에는 MC(13)와 LCM(1)과의 데이터 전송시에 인증을 행함으로써, 대항할 수 있다. 즉, MC(13)는 정당한 LCM(1) 이외로부터의 데이터 전송을 접수하지 않고, LCM(1)이 정당한 MC(13) 이외로부터의 데이터 전송을 접수하지 않는다고 가정한다. 이 경우, MC(13) 내의 「자식」을 다른 미디어에 퇴피시킬 수는 없다. 또, LCM(1)에 대하여, 거짓으로 체크인할 수도 없다. 따라서, 상술한 「공격」은 파탄(破綻)된다

그런데, 실은 LCM(1)과 MC(13)와의 인증을 전제로 하더라도, 체크인/체크아웃은 실현되지 않는다. 다음과 같은 「공격」이 존재하기 때문이다. 즉, 우선, LCM(1) 상의 「부모」가 「자식」을 만들고 있지 않은 상태에서, LCM(1)의 데이터(특히, 라이센스 저장부(9)의 정보)를 다른 기억 미디어에 백업한다. MC(13)에 「자식」을 복사한 후, 백업한 LCM(1)의 데이터를 복귀한다. LCM(1)의 「부모」는 「자식」을 만들기 전의 상태로 되돌아가므로, 다른 MC(13)에 「자식」을 작성할 수 있다. 이렇게 하여, 임의 수의 「자식」을 작성하는 일이 가능하게 된다.

이어서, 체크인/체크아웃을 실현하는 데에 있어서 생기는 문제점 이외의 문제점에 관해서 설명한다. 즉, 인터넷 등의 소정의 통신로를 경유한 MC(13)로의 기록이다. EMD에 의한 정규 인터넷 신호 전송은 저작권 소유자의 허락을 얻어 행하는 정당한 신호 전송이므로 문제는 없다. 그런데, 도 21과 같은 형태로, 인터넷 경유로 MC(13)로의 콘텐츠의 기록을 행할 수 있게 된다. 도 21에 있어서의 퍼스널 컴퓨터(PC) 상의 통신부(201)는 단순히 MC(13)로의 기록 프로토콜을 중계하고 있을 뿐이다. LCM(1)은 상기 LCM(1)이 가동하는 PC#2에 직접 접속되어 있는 PD(12)와, 통신부(201)를 통해 리모트 접속되어 있는 LCM(1)의 가동하는 PC#2에 접속되어 있는 PD(12)를 구별할 수 없기 때문에, 인터넷 등의 네트워크를 통한 콘텐츠의 (위법적인) 배포가 가능하다.

이하, 본 발명의 요지인, 체크인/체크아웃과, 네트워크를 통한 MC(13)로의 콘텐츠 기록을 규제하기 위한 수단 등에 관해서, 다음에 도시하는 항목의 순으로 설명한다.

1. 체크인/체크아웃
(1-1) 체크인/체크아웃
(1-2) 레벨 2의 MC를 이용한 복제 콘텐츠의 체크인/체크아웃
(1-3) 숙박부(guest book)에 의한 복제 콘텐츠의 다른 관리 방법
(1-4) 레벨 2의 MC에 기억된 복제 콘텐츠의 재생
(1-5) 레벨 1의 MC를 이용한 복제 콘텐츠의 체크인/체크아웃, 복제 콘텐츠의 재생
(1-6) 레벨 0의 MC를 이용한 복제 콘텐츠의 체크인/체크아웃, 복제 콘텐츠의 재생
2. 네트워크를 통한 MC로의 복제 콘텐츠의 기록을 규제하기 위한 수단
3. 은닉 영역

(체크인/체크아웃)

체크인/체크아웃을 실현하기 위해서, MC(13) 내의 기억 영역에, 공개된 순서로는 기록 및 판독할 수 없는 영역(은닉 영역)을 설치하여, 거기에 콘텐츠 복호에 필요한 정보를 기록한다(도 2 참조). 또한, LCM(1)의 기억 영역(예컨대, LCM(1)이 PC로 구성되어 있는 경우에는, 하드디스크(HDD)) 상에 비공개 순서로밖에 액세스할 수 없는 영역(은닉 영역)을 설치하여, 후술하는 것과 같은 숙박부를 상기 은닉 영역에 저장한다(도 2 참조). 또한, PD(12)의 기억 영역 상에도 비공개 순서로밖에 액세스할 수 없는 영역(은닉 영역)을 설치하여, 거기에 콘텐츠 복호에 필요한 정보를 기록하도록 하더라도 좋다(도 2 참조). 또, 여기서는 기억 영역 중의 은닉 영역 이외의 통상 순서로 액세스 가능한 영역을 공개 영역이라고 부른다.

도 1에 도시한 바와 같이, LCM(1)에서는 은닉 영역에는 숙박부 저장부(8)가 설치되어, SMS2에 의해 이 숙박부 저장부(8)에 액세스하기 위한 은닉된 특정한 순서가 행해진 후, 은닉 영역으로부터 데이터를 판독하기 위한 은닉 영역 드라이버(7)를 구비하고 있다.

도 4c에 도시한 바와 같이, MC(13)는 그 식별 정보 MID를 저장하기 위한 외부로부터는 재기록이 불가능하고, 복사도 불가능한 구성으로 되어 있는 식별 정보 저장부(13b)와, 은닉 영역(13c)과, 공개 영역(13a)과, 은닉 영역(13c)에 액세스될 때마다 인증부(13d)에서 인증을 행하여, 정당한 상대라고 확인되었을 때에 비로소 은닉 영역(13c)에 액세스 가능하도록 게이트를 개방하는 스위치(SW)(13e)를 구비한다. 또, 본 실시예에서 이용 가능한 MC(13)는 3종류 있으며, 도 4c에 도시한 바와 같은, 식별 정보 MID와 은닉 영역을 모두 겸비하고 있는 MC(13)의 종별을 '레벨 2'라 부른다. 은닉 영역은 갖고 있지 않지만 식별 정보 MID는 갖는 도 4b에 도시한 바와 같은 MC(13)의 종별을 '레벨 1'이라 부른다. 은닉 영역도 식별 정보도 갖지 않는 도 4a에 도시한 바와 같은 MC(13)의 종별을 '레벨 0'이라 부르기로 한다. 이들 종별은 예컨대, 식별 정보 MID의 유무에 의해 레벨 0과 그 이외의 종별이 판별 가능하며, 또한, 식별 정보 MID의 구성으로부터 레벨 1과 레벨 2를 판별한다. 예컨대, 식별 정보가 연속된 수치일 때, 소정치 이상은 레벨 2라 한다.

이하, 특별히 거부되지 않는 한, 레벨 2의 MC(13)의 경우를 예로 들어 설명한다.

이 MC(13)는 LCM(1)에 접속된 PD(12)에 셋트하여 이용하는 경우와 LCM(1)에 직접 셋트하여 이용하는 경우가 있다.

도 3은 PD(12)의 구성예를 도시한 것으로, MC(13)는 미디어 인터페이스(I/F부)(12f)에 셋트된다. LCM(1)가 PD(12)를 통해 MC(13)에 기록 및 판독하는 경우에는 PD(12) 내의 은닉 영역 액세스부를 경유하여 MC(13)의 은닉 영역에 액세스한다. 미디어 I/F부(12f)에는 MC(13)의 은닉 영역에 액세스하기 위한 은닉 영역 액세스부를 구비하고 있다. PD(12) 내의 은닉 영역은 플래쉬 메모리(12d)에 설치되어 있더라도 좋다. ROM(12c)에는 MC(13)와의 사이에서 상호 인증을 행하기 위한 프로그램이나, MC(13)의 종별을 판별하기 위한 프로그램도 기록되어 있어, 이 프로그램에 따라서, CPU(12a)의 제어하에, MC(13)와의 사이에서의 상호 인증, 종별 판별 등의 처리를 실행하도록 되어 있다.

도 5는 LCM(1)의 미디어 I/F부(6)의 구성을 나타낸 것으로, MC(13)와의 사이에서 상호 인증을 행하기 위한 인증부(6c)와, MC(13)의 종별을 판별하는 미디어 판별부(6b)와, 이들 전체를 제어하기 위한 제어부(6a)로 구성되어 있다. 인증부(6c)는 MC(13)의 은닉 영역에 액세스하기 위한 은닉 영역 액세스부이다.
다음에, LCM(1)의 은닉 영역에 저장되는 숙박부에 관해서 설명한다.
SMS(2)에서 유지하는 모든 음악 콘텐츠는 그 각각을 식별하기 위한 식별 정보인 콘텐츠 ID(TID)와, 미리 정해진 복제 가능 콘텐츠의 수, 즉, 자식의 잔여수와 체크아웃 리스트를 그 속성 정보로서 갖는다. 이 속성 정보를 숙박부(guest book)라고 부른다. 숙박부는 은닉 영역에 설치된 숙박부 저장부(8)에 도 7a에 도시한 바와 같은 형태로 기록되어 있다.
도 7a에 있어서, 예컨대, 콘텐츠 ID 「TID1」인 자식의 잔여수는 「2」이며, 그 체크아웃 리스트는 L1이다.
체크아웃 리스트는 복제 콘텐츠(자식)를 기록한 MC(13)의 식별 정보의 리스트이며, 예컨대, 도 7a에 있어서, 체크아웃 리스트(L1)에는 「m1」과 「m2」라고 하는 식별 정보를 갖는 2개의 MC(13)에 콘텐츠 ID 「TID1」인 콘텐츠의 자식이 체크아웃되어 있는 것을 알 수 있다.
(레벨 2의 MC를 이용한 복제 콘텐츠의 체크인/체크아웃)
다음에, 도 4c에 도시한 것과 같은 구성의 레벨 2의 MC(13)를 이용한 체크인/체크아웃에 관해서, 도 9 내지 도 11을 참조하여 설명한다.
MC(13)가 LCM(1)의 미디어 I/F부(6), 혹은, PD(12)에 셋트되면, 미디어 IF부(6)와 MC(13)와의 사이, 혹은, PD(12)와 MC(13)와의 사이에서 상호 인증이 행해져(도 9의 단계 S1), 쌍방에서 정당한 상대라고 판단되었을 때(단계 S2), 미디어 I/F부(6) 혹은 PD(12)는 MC(13)로부터 판독한 식별 정보 MID를 기초로, MC(13)의 종별을 판별한다(단계 S3). 여기서는, MC(13)의 종별은 레벨 2이기 때문에, 미디어 I/F부(6) 혹은 PD(12)는 그 종별에 따른 체크인/체크아웃 처리를 실행한다(단계 S6).
체크아웃의 지시가 LCM(1)의 사용자 인터페이스(I/F)부(15)를 거쳐, 혹은, PD(12)를 거쳐, SMS(2)에 이루어진 경우에 관해서, 도 10을 참조하여 설명한다. SMS(2)는 숙박부의 체크아웃 요구가 있었던 콘텐츠(예컨대 콘텐츠 ID가 「TID1」이라 함)의 자식의 잔여수(n)를 조사하여(단계 S101), n＞0일 때, 필요하면, MC(13)와의 사이에서 상호 인증을 행하고(단계 S102), 서로 정당성이 확인되면, 이어서, MC(13)로부터, 그 식별 정보 MID(예컨대, MID=m0으로 함)를 전송받는다(단계 S103).
SMS(2)에서는 난수 r을 발생하여, 이 난수 r과, MC(13)의 식별 정보 m0과, 정당한 MC(13)와 LCM(1)과의 사이에서 공유하는 키 생성 알고리즘(W)을 이용하여, 암호화 키(w)를 생성한다. 또, 키 생성 알고리즘(W)은 2개의 인수(여기서는, r과 m0)를 취하여, 암호화 키(w)를 매회 변화시키는 역활을 한다. 또한, SMS(2)에서는 암호화된 콘텐츠를 복호하기 위한 콘텐츠 복호키(K(C))를 MC(13)와 LCM(1)과의 사이에서 공유하는 암호키(Kp)와 앞서 생성한 암호화 키(w)에 의해 암호화한다. 그것을 w[Kp[k(C)]]로 나타낸다. 또한, 콘텐츠(C)를 키(K(C))에 의해 암호화한다. 그것을 K(C)[C]로 나타낸다(단계 S104).
SMS(2)는 MC(13)의 기억 영역에, 예컨대 「TID1」라는 이름의 폴더를 작성하면(단계 S105), 상기 폴더의 공개 영역에 암호화된 콘텐츠 K(C)[C]와, 암호화된 콘텐츠 복호키 w[Kp[k(C)]]를 기록한다(단계 S106, 단계 S107).
다음에, SMS(2)는 MC(13)의 은닉 영역(13c)에 액세스하도록, MC(13)와의 사이에서 상호 인증을 행하여, 쌍방의 정당성이 확인되어 스위치(13e)에 의해 은닉 영역(13c)으로의 게이트가 열리면, 난수 r을 은닉 영역(13c) 내의 폴더 「TID1」에 대응하는 영역에 기록한다(단계 S108 내지 단계 S109). 그것이 종료하면 은닉 영역(13c)으로의 액세스를 가능하게 하고 있었던 게이트가 스위치(13e)에 의해 폐쇄되는 구조로 되어 있다. 또한, 단계 S108에 있어서, 난수 r을 은닉 영역(13c)에 전송하기까지의 경로는, 난수 r을 암호화하는 등으로 전송 보호하는 것이 바람직하다.
마지막으로, SMS(2)는 도 7b에 도시한 바와 같이, 숙박부의 체크아웃 요구가 있었던 콘텐츠 ID 「TID1」의 콘텐츠의 자식의 잔여수(n)로부터 「1」을 감산하여, 체크아웃 리스트(L1)에, 상기 MC(13)의 식별 정보 「m0」을 추가한다(단계 S110).
이상의 처리가 종료되었을 때의 MC(13)의 기억 내용을 도 6에 나타낸다.
체크인의 지시가 LCM(1)의 사용자 인터페이스(I/F)부(15)를 거쳐, 혹은, PD(12)을 거쳐, SMS(2)에 이루어진 경우에 관해서, 도 11을 참조하여 설명한다.
SMS(2)는 필요하면, MC(13)와의 사이에서 상호 인증을 행하여(단계 S201), 서로 정당성이 확인되면, 이어서, MC(13)로부터, 그 식별 정보 MID(예컨대, MID=m0으로 함)를 전송받는다(단계 S202).
SMS(2)는 체크인 요구가 이루어진 콘텐츠(예컨대 콘텐츠 ID가 「TID1」이라 함)의 숙박부로부터, 그 체크아웃 리스트에 상기 MC(13)의 식별 정보, 즉, 여기서는 「m0」이 등록되어 있을 때, 난수 r1, 난수 r2를 발생시킨다(단계 S203). 그리고, MC(13)의 공개 영역(13a)의 상기 콘텐츠의 폴더(여기서는, 폴더 「TID1」)에 대응하는 영역에 기억되어 있는 정보를 난수 r2로 덮어씀(overwrite)으로써 소거하고(단계 S204), 또, SMS(2)는 MC(13)의 은닉 영역(13c)에 액세스하도록, MC(13)와 의 사이에서 상호 인증을 행하여, 쌍방의 정당성이 확인되어 스위치(13e)에 의해 은닉 영역(13c)으로의 게이트가 열리면, 은닉 영역(13c) 내의 폴더 「TID1」에 대응하는 영역을 난수 r1로 덮어씀으로써 소거한다(단계 S205). 그것이 종료되면 은닉 영역(13c)으로의 액세스를 가능하게 하고 있었던 게이트가 스위치(13e)에 의해 폐쇄하는 구조로 되어 있다. 또한, 단계 S205에 있어서, 난수 r1을 은닉 영역(13c)에 전송하기까지의 경로는 난수 r1을 암호화하는 등으로 전송 보호하는 것이 바람직하다.
그 후, SMS(2)에서는 덮어쓰기 소거를 확인하기 위해, MC(13)로부터 덮어쓰기후의 각 영역의 값을 전송받고(단계 S206), 그것이 난수 r1, r2와 일치하는지의 여부를 체크한다(단계 S207). 덮어쓰기 소거의 확인이 이루어지면, MC(13)로부터 폴더 「TID1」을 소거한다(단계 S208).

마지막으로, 도 7c에 도시한 바와 같이, 숙박부의 체크인 요구가 있었던 콘텐츠 ID 「TID1」의 콘텐츠의 자식의 잔여수(n)에 1을 가산하여, 체크아웃 리스트(L1)로부터, 상기 MC(13)의 식별 정보 m0을 삭제한다(단계 S209).

MC(13) 내의 은닉 영역(13c)에 기록된 난수 r은 (인증에 의한 정당성을 확인할 수 없기 때문에) 별도의 기억 미디어에 퇴피할 수는 없다. 따라서, 「TID1」이라고 하는 콘텐츠의 체크인후, MC(13)에 복귀된 콘텐츠를 이용할 수는 없다. 또, LCM(1)의 은닉 영역에서 기억되는 숙박부도(인증에 의한 정당성을 확인할 수 없기 때문에) 별도의 미디어에 퇴피할 수 없다. 따라서, 「TID1」이라고 하는 콘텐츠를 체크아웃한 후에, 숙박부를 체크아웃전의 상태로 돌릴 수는 없다. 이와 같이, 본 발명은 상술한 공격에 대한 대책을 제공한다.

또, 체크인시, MC(13)의 은닉 영역의 내용을 난수로 덮어쓰는 것은 안전상 중요하다. MC(13)의 은닉 영역에 기록을 행할 수 있는 것은 정통한 SMS(2)뿐이지만, 반대로 정통한 SMS(2)는 반드시 은닉 순서에 의해 은닉 영역에 기록을 행한다. 은닉 순서에 의한 기록이 성공함으로써, MC(13)의 정통성이 보증된다. 즉, 부정한 체크인을 방지하는 일이 가능하다. 안전성을 높이기 위해서, SMS(2)는 은닉 영역을 임의의 난수로 덮어쓰기한 후, 그 내용을(은닉 순서에 의해) 판독, 덮어쓰기한 난수임을 확인하도록 하고 있다.

(숙박부에 의한 복제 콘텐츠의 다른 관리 방법)

또, SMS(2)는 숙박부에 없는 타이틀(콘텐츠 ID)의 콘텐츠를 체크인하도록 하더라도 좋다. 또, 체크아웃 리스트에 없는 MC(13)로부터의 체크인을 인정하더라도 좋다. 이 경우, 숙박부는 각 콘텐츠에 대한 체크아웃 리스트를 갖지 않는다. 체크아웃 리스트는 「기억이 없는」 MC(13)로부터의 체크인을 방지하기 위해 참조되는 것이기 때문이다. 이 경우의 숙박부의 기억 내용을 도 8a에 도시한다.

도 8a에 도시한 바와 같이, 각 콘텐츠의 숙박부에는 그 콘텐츠 ID와 자식의 잔여수만이 등록되어 있다.

지금, TID7이라고 하는 콘텐츠 ID를 갖는 콘텐츠를, 미디어 식별 정보 MID=m0을 갖는 MC(13)로부터 체크인하는 경우를 고려한다. 즉, 상기 MC(13)에는 현재, 별도의 SMS(2)로부터 체크아웃된 콘텐츠 ID 「TID7」인 콘텐츠가, 도 6에 도시한 것과 같은 형태로 기억되어 있다.

LCM(1)은 도 11에 나타낸 순서 중, 단계 S203의 체크아웃 리스트를 참조하지 않고서 MC(13) 내의 은닉 영역, 공개 영역의 기억 내용을 소거하는 동시에, 폴더 「TID7」을 삭제한다. 그리고, 숙박부에 새로운 콘텐츠의 숙박부(TID7, 1)를 등록한다.

LCM(1)이 숙박부에 없는 콘텐츠를 체크인함으로써, 예컨대 다음과 같은 경우가 가능하게 된다. 자택 PC에 의해 구성되는 LCM(1)가 저장하는 「부모」 콘텐츠가 「자식」을 2개 갖을 수 있다고 하자. 자택 PC로부터 MC(13)로 「자식」을 하나 체크아웃하여, 친구집의 PC에 체크인한다. 자기가 구입한 「부모」가 「자식」을 만드는 수를 하나 줄여, 친구에게 콘텐츠를 선물한 것으로 된다. 이와 같이, LCM(1)이 숙박부에 없는 콘텐츠의 체크인을 가능하게 하면, 「자식」의 콘텐츠가 LCM(1)을 거쳐 「이동」하는 것이 가능하다. 이것은 사용자에게 있어서는 편리한 기능이지만, 콘텐츠의 중고 시장이 성립되는 원인을 만들기도 한다. 실제로, 다음과 같은 중고 콘텐츠 매매가 성립된다. 즉, 사용자가 EMD로부터 신작 콘텐츠를 구입하여, 짧은 기간 소지한 후에, 중고 데이터 판매점의 LCM(1)에 상기 콘텐츠를 체크인한다. 이 때, 상기 사용자는 대금을 받는다. 중고 데이터 판매점은 다른 구입 희망자에게, EMD의 정규 가격보다 싼 값으로 데이터를 판매한다.

이와 같이, 콘텐츠의 저작권을 컨트롤할 수 없는 「중고 시장」의 성립은 카피라이트 홀더에 있어서 바람직하지 못하다. 따라서, 카피라이트 홀더가 다른 LCM(1)으로의 체크인을 컨트롤할 수 있도록, 각 콘텐츠에 체크아웃 속성 플래그 f를 갖게 하더라도 좋다.

이 경우의 LCM(1)이 갖는 숙박부의 형식을 도 18a에 도시한다.

도 18a에 도시한 바와 같이, 각 콘텐츠의 숙박부에는, 그 콘텐츠 ID와 자식의 잔여수와 체크아웃 리스트와 체크아웃 속성 플래그 f가 등록되어 있다.

플래그 f가 「1」인 경우, 상기 콘텐츠는 다른 LCM(1)에 체크아웃, 체크인 가능하지만, 플래그 f가 「0」일 때에는 상기 콘텐츠는 적어도 다른 LCM(1)에 체크인할 수 없다.

예컨대, 콘텐츠 ID 「TID6」이라고 하는 콘텐츠를 체크아웃하는 경우를 고려해보자. 우선 SMS(2)는 숙박부를 조사하여, 상기 콘텐츠의 체크아웃 속성 플래그가 「1」임을 확인한다. 여기서는 이 값이 「0」일 때, 상기 LCM(1)에서는 상기 콘텐츠를 체크아웃하지 않게 한다. 플래그 f가 「1」일 때에는, 도 10에 나타낸 순서와 마찬가지로 하여, 콘텐츠 ID 「TID6」의 숙박부의 자식의 잔여수로부터 「1」 감산하여 「1」로 한다(도 18b 참조). 덧붙여서 말하면, 체크아웃 리스트(L6)는 공백(Φ라 표기함)이고, 더구나 플래그 f는 「1」이며, 상기 콘텐츠는 다른 PC 상의 설치된 LCM(1)에 체크인 가능하므로, 체크아웃 리스트를 지닐 필요가 없다. 또한, 플래그 f는 MC(13)의 은닉 영역에 난수 r과 동시에 기록되는 것으로 한다.

이어서, 콘텐츠 ID 「TID6」이라고 하는 콘텐츠를, 체크아웃한 LCM(1)과 동일한 LCM(1), 혹은 다른 LCM(1)에, 체크인하는 경우에 관해서, 도 19에 나타내는 흐름도를 참조하여 설명한다.

도 11에 도시한 순서에 의해, MC(13)와 LCM(1)과의 사이에서 상호 인증을 행하여(단계 S11), MC(13)의 식별 정보 MID를 취득한다(단계 S12).

SMS(2)는 체크인 요구가 있었던 콘텐츠가 숙박부에 등록되어 있는지의 여부와는 상관없이, MC(13)의 은닉 영역(13c)에 전술한 은닉 순서(MC(13)와의 사이에서 상호 인증을 행하여, 쌍방의 정당성이 확인되고 스위치(13e)에 의해 은닉 영역(13c)으로의 게이트가 열림)를 행하여, 은닉 영역(13c)으로부터 플래그 f를 판독한다(단계 S13). 플래그 f가 「1」일 때에는(단계 S14), 도 11의 단계 S204 내지 단계 S208를 행하고(단계 S15 내지 단계 S16), 플래그 f가 「0」일 때에는, 처리를 종료한다. 그리고, 마지막으로, 숙박부에 상기 콘텐츠가 등록되어 있을 때에는 그 콘텐츠의 자식의 잔여수를 「1」로 한 「TID6」의 새로운 숙박부(TID6, 1, Φ, 1)를 등록하고, 숙박부에 상기 콘텐츠가 등록되어 있을 때에는 그 콘텐츠의 자식의 잔여수에 「1」을 가산한다(단계 S17).

(레벨 2의 MC에 기억된 복제 콘텐츠의 재생)
다음에, 도 4c에 나타낸 것과 같은 구성의 레벨 2의 MC(13)에 기억된 복제 콘텐츠의 재생에 관해서, 도 12를 참조하여 설명한다. MC(13)를 PD(12)에 셋트하면, PD(12)는 MC(13)로부터, 그 식별 정보 MID(예컨대, MID=m0으로 함)를 전송받는다(단계 S301). 이 때, 식별 정보 MID=m0을 기초로, MC(13)의 종별을 판별이 레벨 2임을 판별할 수 있다. 그래서, PD(12)는 MC(13)의 공개 영역으로부터 w[Kp[k(C)]]를 판독하는 동시에(단계 S302), MC(13)의 은닉 영역(13c)에 액세스하도록, MC(13)와의 사이에서 상호 인증을 행하여, 쌍방의 정당성이 확인되고 스위치(13e)에 의해 은닉 영역(13c)으로의 게이트가 열리면, 은닉 영역(13c) 내의 폴더 「TIDl」에 대응하는 영역으로부터 난수 r을 판독한다(단계 S303). 그것이 종료되면 은닉 영역(13c)으로의 액세스를 가능하게 하고 있었던 게이트가 스위치(13e)에 의해 폐쇄되는 구조로 되어 있다.
PD(12)는 난수 r과, MC(13)의 식별 정보 m0과, 정당한 MC(13)와 PD(12)와의 사이에서 공유하는 키 생성 알고리즘(W)을 이용하여, 암호화 키(w)를 생성한다. 암호화 키(w)와, MC(13)와 LCM(1)과의 사이에서 공유하는 암호키(Kp)와, MC(13)로부터 판독된 w[Kp[k(C)]]로부터 콘텐츠 복호키(K(C))를 복호한다(단계 S304).
그리고, PD(12)는 MC(13)의 공개 영역으로부터 암호화된 콘텐츠 K(C)[C]를 판독하고(단계 S305), 복호부(12g)에서 콘텐츠(C)를 복호하여, 디코더(12h)에서 디코드하고, D/A 변환부에서 디지털 신호로부터 아날로그 신호로 변환하여, 음악을 재생한다(단계 S306).
(레벨 1의 MC를 이용한 복제 콘텐츠의 체크인/체크아웃, 복제 콘텐츠의 재생)
이어서, 도 4b에 나타낸 것과 같은 구성의 레벨 2의 MC(13)를 이용한 체크인/체크아웃에 관해서, 도 9, 도 13을 참조하여 설명한다. 또, 레벨 1의 MC(13)는 은닉 영역을 갖지 않기 때문에, 체크인을 할 수 없다.
MC(13)가 LCM(1)의 미디어 I/F부(6), 혹은, PD(12)에 셋트되고 나서, MC(13)의 종별이 판별될 때까지는 도 9와 마찬가지이다.
여기서는, MC(13)의 종별은 레벨 1이기 때문에, 미디어 I/F부(6) 혹은 PD(12)는 그 종별에 따른 체크인/체크아웃 처리를 실행한다(단계 S5).
체크인의 지시가 LCM(1)의 사용자 인터페이스(I/F)부(15)를 거쳐, 혹은 PD(12)를 거쳐, SMS(2)에 이루어진 경우, MC(13)의 종별이 레벨 1이라고 판별되고 있기 때문에, 그 지시는 거부된다.
체크아웃의 지시가 LCM(1)의 사용자 인터페이스(I/F)부(15)를 거쳐, 혹은 PD(12)를 거쳐, SMS(2)에 이루어진 경우에 관해서, 도 13을 참조하여 설명한다.
SMS(2)는 숙박부의 체크아웃 요구가 있었던 콘텐츠(예컨대 콘텐츠 ID가 「TID1」이라 함)의 자식의 잔여수(n)을 조사하여(단계 S401), n＞0일 때, 필요하면, MC(13)와의 사이에서 상호 인증을 행하고(단계 S402), 서로 정당성이 확인되면, 이어서, MC(13)로부터 그 식별 정보 MID(예컨대, MID=m0이라 함)를 전송받는다 (단계 S403).
SMS(2)는 레벨 2인 경우와 마찬가지로 난수 r의 발생, 암호화 키(w)의 생성, 콘텐츠 키를 w와 Kp를 이용하여 암호화, 콘텐츠(C)의 암호화를 행하여(단계 S404), MC(13)의 기억 영역(여기서는, 공개 영역만)에, 예컨대 「TID1」이라고 하는 이름의 폴더를 작성한다(단계 S405). 그리고, 상기 폴더에 암호화된 콘텐츠 K(C)[C]와, 암호화된 콘텐츠 복호키 w[Kp[k(C)]]와 난수 r을 기록한다(단계 S406 내지 단계 S408).
마지막으로, SMS(2)는 도 7b에 도시한 바와 같이, 숙박부의 체크아웃 요구가 있었는 콘텐츠 ID 「TID1」의 콘텐츠의 자식의 잔여수(n)에서 「1」 감산하여, 체크아웃 리스트(L1)에, 상기 MC(13)의 식별 정보 「m0」을 추가한다(단계 S409).
다음에, 레벨 1의 MC(13)에 기억된 복제 콘텐츠의 재생에 관해서, 도 14를 참조하여 설명한다. MC(13)를 PD(12)에 셋트하면, PD(12)는 MC(13)로부터, 그 식 별 정보 MID(예컨대, MID=m0으로 함)를 전송받는다(단계 S501). 이 때, 식별 정보 MID=m0을 기초로, MC(13)의 종별을 판별이 레벨 1임을 판별할 수 있다. 그래서, PD(12)는 MC(13)의 기억 영역(공개 영역만)으로부터 w[Kp[k(C)]], 난수 r을 판독하고(단계 S502 내지 단계 S503), 난수 r과, MC(13)의 식별 정보 m0과, 정당한 MC(13)와 PD(12)와의 사이에서 공유하는 키 생성 알고리즘(W)을 이용하여, 암호화 키(w)를 생성한다. 암호화 키(w)와, MC(13)와 LCM(1)와의 사이에서 공유하는 암호키(Kp)와, MC(13)로부터 판독된 w[Kp[k(C)]]로부터 콘텐츠 복호키(K(C))를 복호한다(단계 S504).
그리고, PD(12)는 MC(13)의 기억 영역(공개 영역만)으로부터 암호화된 콘텐츠 K(C)[C]를 판독하고(단계 S505), 복호부(12g)에서 콘텐츠(C)를 복호하며, 디코더(12h)에서 디코드하고, D/A 변환부에서 디지털신호로부터 아날로그 신호로 변환하여, 음악을 재생한다(단계 S506).
(레벨 0의 MC를 이용한 복제 콘텐츠의 체크인/체크아웃, 복제 콘텐츠의 재생)
다음에, 도 4a에 도시한 것과 같은 구성의 레벨 0의 MC(13)를 이용한 체크인/체크아웃에 관해서, 도 9, 도 15 내지 도 16을 참조하여 설명한다.
레벨 0의 MC(13)는 PD(12)를 이용해서밖에 체크인/체크아웃 및 재생을 행할 수 없다. 또한, 식별 정보 MID를 갖지 않기 때문에, 대신에 체크인/체크아웃에 있어서, PD(12)의 식별 정보 PID가 이용된다.
MC(13)가 PD(12)에 셋트되고 나서, MC(13)의 종별이 판별될 때까지는 도 9와 마찬가지이다.
여기서는, MC(13)의 종별은 레벨 0이기 때문에, PD(12)는 그 종별에 따른 체크인/체크아웃 처리를 실행한다(단계 S4).
체크아웃의 지시가 PD(12)를 거쳐, SMS(2)에 이루어진 경우에 관해서, 도 15를 참조하여 설명한다.
SMS(2)는 숙박부의 체크아웃 요구가 있었던 콘텐츠(예컨대 콘텐츠 ID가 「TID1」이라고 함)의 자식의 잔여수(n)을 조사하고(단계 S601), n＞0일 때, PD(12)와의 사이에서 상호 인증을 행하여(단계 S602), 서로 정당성이 확인되면, 이어서, PD(12)로부터 그 식별 정보 PID를 전송받는다(단계 S603).

SMS(2)는 레벨 2인 경우와 마찬가지로, 난수 r의 발생, 암호화 키(w)의 생성, 콘텐츠 키를 w와 Kp를 이용하여 암호화, 콘텐츠(C)의 암호화를 행한다(단계 S604). 단, 여기서는 키 생성 알고리즘(W)이 취하는 2개의 인수는 r과 PID이다.
다음에, MC(13)의 기억 영역(여기서는, 공개 영역만)에, 예컨대 「TID1」이라고 하는 이름의 폴더를 작성한다(단계 S605). 그리고, 상기 폴더에 암호화된 콘텐츠 K(C)[C]와, 암호화된 콘텐츠 복호키 w[Kp[k(C)]]를 기록한다(단계 S606 내지 단계 S607). 난수 r은 PD(12)의 은닉 영역에 기록한다(단계 S608). 단계 S608에 있어서, 난수 r을 PD(12)의 은닉 영역에 전송할 때까지의 경로는 난수 r을 암호화하는 등으로 전송 보호하는 것이 바람직하다.
마지막으로, SMS(2)는 도 7b에 도시한 바와 같이, 숙박부의 체크아웃 요구가 있었던 콘텐츠 ID 「TID1」의 콘텐츠의 자식의 잔여수(n)에서 「1」 감산하여, 체 크아웃 리스트(Ll)에, PD(12)의 식별 정보 「PID」를 추가한다(단계 S609).
체크인의 지시가 PD(12)를 거쳐, SMS(2)에 이루어진 경우에 관해서, 도 16을 참조하여 설명한다.
SMS(2)는 PD(12)와의 사이에서 상호 인증을 행하여(단계 S701), 서로 정당성이 확인되면, 이어서, PD(12)로부터 그 식별 정보 PID를 전송받는다(단계 S702).
SMS(2)는 체크인 요구가 이루어진 콘텐츠(예컨대 콘텐츠 ID가 「TID1」이라 함)의 숙박부로부터, 그 체크아웃 리스트에 상기 PD(12)의 식별 정보 「PID」가 등록되어 있을 때, 난수 r1, r2를 발생시킨다(단계 S703). 그리고, MC(13)의 공개 영역(13a)의 상기 콘텐츠의 폴더(여기서는, 폴더 「TID1」)에 대응하는 영역에 기억되어 있는 정보를 난수 r2로 덮어씀으로써 소거하고(단계 S704), 또한, SMS(2)은 PD(12)의 은닉 영역에 액세스하도록, PD(12)와의 사이에서 상호 인증을 행하여, 쌍방의 정당성이 확인되고 은닉 영역으로의 게이트가 열리면, 은닉 영역(13c)내의 폴더 「TID1」에 대응하는 영역을 난수 r1로 덮어씀으로써 소거한다(단계 S705). 그것이 종료되면 은닉 영역에의 액세스를 가능하게 하고 있던 게이트가 닫힌다. 또한, 단계 S705에 있어서, 난수 r1을 은닉 영역에 전송할 때까지의 경로는 난수 r1을 암호화하는 등으로 전송 보호하는 것이 바람직하다.
그 후, SMS(2)에서는 덮어쓰기 소거의 확인해야 할, MC(13)로부터 덮어쓰기후의 값을 전송받고, 또한, PD(12)의 은닉 영역으로부터도 상기 소정의 은닉 순서를 행하여, 상기 영역의 덮어쓰기후의 값을 판독하며(단계 S706), 그것이 난수 r1, r2와 일치하는지의 여부를 체크한다(단계 S707). 덮어쓰기 소거의 확인이 이루어 지면, MC(13)로부터 폴더 「TID1」을 소거한다(단계 S708) .
마지막으로, 도 7c에 도시한 바와 같이, 숙박부의 체크인 요구가 있었던 콘텐츠 ID 「TID1」의 콘텐츠의 자식의 잔여수(n)에 「1」 가산하여, 체크아웃 리스트(L1)로부터, PD(12)의 식별 정보 「PID」를 삭제한다(단계 S709).
이어서, 레벨 0의 MC(13)에 기억된 복제 콘텐츠의 재생에 관해서, 도 17을 참조하여 설명한다. MC(13)를 PD(12)에 셋트하면, PD(12)는 MC(13)로부터, 그 식별 정보 MID의 전송을 요구하지만, MC(13)은 식별 정보를 갖고 있지 않기 때문에, PD(12)는, 상기 MC(13)는 레벨 0이라고 판별할 수 있다. 그래서, PD(12)는 MC(13)의 기억 영역(공개 영역만)으로부터 w[Kp[k(C)]]를 판독하여(단계 S801), PD(12) 자신의 식별 정보 「PID」와, 그 은닉 영역에 저장되어 있는 난수 r과 키 생성 알고리즘 W를 이용하여, 암호화 키 w를 생성한다. 그리고, 암호화 키 w와, 암호키 Kp와, MC(13)로부터 판독된 w[Kp[k(C)]]로부터 콘텐츠 복호키(K(C))를 복호한다(단계 S802).
PD(12)는 MC(13)의 기억 영역(공개 영역만)으로부터 암호화된 콘텐츠 K(C)[C]를 판독하여(단계 S803), 복호부(12g)에서 콘텐츠(C)를 복호하고, 디코더(12h)에서 디코드하여, D/A 변환부에서 디지털 신호로부터 아날로그 신호로 변환하여, 음악을 재생한다(단계 S804).
(네트워크를 통한 MC로의 복제 콘텐츠 기록을 규제하기 위한 수단)
본 발명의 2번째 문제점을 해결하기 위해서, 즉, 네트워크를 경유한 콘텐츠의 MC(13)로의 기록을 규제하기 위해서, 본 발명에서는 도 1에 도시한 바와 같이 타임아웃 판정부(4)를 설치하고 있다.
타임아웃 판정부(4)에서는 MC(13)로의 기록 및 판독(어느 한쪽, 또는 양쪽) 순서에 있어서, 일정한 제한 시간을 설정하여, 처리가 제한 시간 내에 끝나지 않으면 처리를 중단한다. 네트워크를 통한 통신은 통상, 직접 접속된 기기와의 통신에 비교하여 훨씬 긴 시간이 필요하기 때문에, 타임아웃 기능에 의해서, 네트워크를 통한 위법 복사에 대항할 수 있다. 또, 대역 제한을 이용할 수도 있다. 기기와의 통신 대역을 일정 이상으로 가정하면, 어떤 사이즈의 데이터를 기기에 전송할 때에 걸리는 시간의 상한을 계산할 수 있다. 실제의 전송 시간이 그것을 상회한 경우, 처리를 중단한다.
도 22에 도시하는 타임아웃 판정부(4)의 구성과 도 23에 도시하는 흐름도를 참조하여, 좀더 구체적으로 설명한다. 미리 타임아웃 시간을 t로 설정하기로 하고, 예컨대, LCM(1)과 PD(12)와의 사이의 통신 대역폭을 b로 한다. 예컨대, PD(12)에 셋트되어 있는 MC(13)와의 사이에서 체크아웃을 행하는 경우를 예로 들어, 타임아웃 판정부(4)의 처리 동작에 관해서 설명한다.
우선, PD(12)에 셋트되어 있는 MC(13)와의 사이의 체크아웃을 위한 순서에 있는 임의의 하나의 기록 및 판독 처리 동작의 개시와 함께, SMS(2)로부터 판정 개시 신호 입력부(102)를 거쳐 판정 개시 신호가 입력되고(단계 S20), 그와 함께, SMS(2)로부터 PD(12)와의 사이에서 교환이 이루어지는 패킷 데이터의 사이즈(s)가 데이터 사이즈 입력부(101)로부터 입력되며(단계 S21), 제어부(105)는 시각 취득부(106)를 거쳐 시계(107)로부터 현재 시각(T)을 취득한다(단계 S22). 이에 따라, 대역폭 저장부(108)로부터 대역폭 b를 취득하여(단계 S23), 종료 예정 시각 T'을 산출하고(단계 S24), 최종 예정 시각 저장부(111)에 저장한다(단계 S25).
종료 예정 시각 T'은 대역폭 b와 데이터 사이즈 s로부터 T'=T+s/b로 구할 수 있다.
PD(12)에 셋트되어 있는 MC(13)와의 사이의 기록 및 판독 처리 동작의 종료와 동시에, SMS(2)로부터 판정 종료 신호 입력부(103)를 거쳐 판정 종료 신호가 입력되면(단계 S26), 다시, 현재 시각 T를 취득하고(단계 S27), 앞서 산출된 종료 예정 시각 T'과 현재 시각 T와의 차와 타임아웃 시간 t를 비교한다(단계 S28). 상기 차가 타임아웃 시간 t를 초과하고 있을 때에는 「NG」라 판정하여, 그 취지를 SMS(2)에 통지한다(단계 S30). 만약에 PD(12)가 도 21에 도시

한 바와 같이 체크아웃을 행하는 PC#1에 있는 LCM(1)과 네트워크에 의해 접속된 다른 PC#2에 접속된 것이라고 하면, 「NG」라고 하는 판정 결과를 얻을 수 있기 때문에, PC#1의 LCM(1)에서는 그 이후의 체크아웃을 위한 처리를 중단한다.
혹은, 종료 예정 시각 T'이 경과하더라도 상기 기록 및 판독 처리 동작이 종료되지 않고 있을 때, 판정 결과를 「NG」로 하더라도 좋다.
혹은, 타임아웃 판정부(4)는 2개의 모드로 동작한다. 하나는 데이터 사이즈 입력부(101)에 데이터 사이즈 s가 입력되었을 때이고, 이 때, 타임아웃 판정부는 종료 예정 시각 T'=T+s/b를 산출하여, 그것을 종료 예정 시각 저장부(111)에 저장한다. 타임아웃 판정부(4)는 판정 종료 신호를 수취하면, 현재 시각 T와 종료 예정 시각 저장부가 저장하는 시각 T'을 비교한다. 전자가 후자보다 작은 경우, 타 임아웃 판정부(4)는 판정 결과 OK를 SMS(2)에 통지한다. 그 외의 경우에는 판정 결과 NG를 SMS(2)에 통지한다.
다른쪽 모드의 동작은 판정 개시 신호 입력부(102)에 판정 개시 신호가 입력된 경우에, 타임아웃 판정부(4)는 현재 시각 T+타임아웃 시간 t를 종료 예정 시각 저장부(111)에 저장한다. 타임아웃 판정의 동작은 상기 한쪽 모드의 경우와 마찬가지이다.
(은닉 영역)
본 발명의 LCM(1)에서는 체크인/체크아웃을 위한 숙박부를 저장하기 위해서 은닉 영역을 이용한다. LCM(1)을 PC로 구성하는 경우, 이 은닉 영역은 하드디스크(HDD) 상에 작성된다.
여기서는, HDD 상의 은닉 영역에 관해서 설명한다.
HDD 상에는 통상 파티션이 존재한다. 파티션은 OS로부터 하나의 드라이브로서 인식된다. 각 파티션 내에 복수의 섹터가 존재하고, 데이터는 섹터 상에 기록된다. 섹터 내의 데이터 배치를 논리 포맷이라 부른다. 파일 시스템은 통상 파일 배치 테이블을 갖는다. 파일 배치 테이블에는 각 파일 및 디렉토리의 섹터 상의 위치가 기록되어 있다. OS는 파일 배치 테이블을 참조하여, 액세스 대상 파일의 위치를 취득하여, 대상 파일에 도달한다. 섹터의 물리적 배치를 물리 포맷이라고 부른다. 각 파티션은 다른 물리 포맷을 지닐 수 있다. 섹터의 위치는 헤드의 위치에 의해 식별된다. 각 섹터의 개시 위치는 자기적인 마크에 의해서 식별된다.
OS가 서포트하는 파일 시스템에 관해서, OS는 드라이버를 가지고 있다. 드 라이버는 상기 파일 시스템의 물리 포맷 및 논리 포맷을 인식하고 있으며, 파티션 내의 섹터를 찾아가 파일 배치 테이블이나 각 파일에 도달하여, 그 내용을 기록 및 판독할 수 있다.
본 발명의 은닉 영역을 구성하기 위한 파일 시스템을 도 24에 도시한다. 통상의 파일 시스템에서는 섹터는 등간격으로 배치되지만, 본 파일 시스템에서는 그렇게 되고 있지 않다. 제1 섹터 SC1의 선두에는 섹터 배치 테이블이 있다. 섹터 배치 테이블은 다음 형태로 섹터 위치가 기록되어 있다.
헤드 위치 #2, 헤드 위치 #3, …, 헤드 위치 #n
순으로, 제2 섹터 SC2, 제3 섹터 SC3, …, 제n 섹터 SCn의 위치를 나타내고 있다.
섹터 배치 테이블은 암호화되어 있다. 이 암호화를 푸는 키는 시스템의 고유 ID에 의존한다. 시스템 고유의 ID로서는, 예컨대 OS의 ID, BIOS의 ID 혹은 CPU의 ID 등이 이용된다.
또한, 제2 섹터 SC2의 선두에는 파일 배치 테이블 FT가 존재한다. 이것은 다음 형식이다.
(파일1, (섹터 번호, 섹터내 위치)),
(파일2, (섹터 번호, 섹터내 위치)),
…
섹터내 위치는 섹터 선두에서부터의 바이트수이다. 파일 배치 테이블 FT도 역시 암호화되어 있다. 이 암호키도 역시 시스템 고유의 ID에 의존하고 있다.
본 발명의 파일 시스템에 대한 액세스는 특별한 드라이버(도 1의 은닉 영역 드라이버(7))를 이용하여 행한다. 은닉 영역 드라이버(7)의 동작을 도 25에 도시한다. 상기 드라이버(7)는 역시 섹터 배치를 변경하는 기능을 갖고 있다. 섹터 배치 갱신시의 은닉 영역 드라이버(7)의 동작을 도 26에 도시한다.
(인증)
이상의 설명에 있어서, 예컨대, LCM(1)에 MC(13)를 셋트했을 때에 행해지는 상호 인증이나, 은닉 영역에 액세스할 때에 행해지는 인증 처리의 일례를 예로 든다. 이것은 종래부터 있는 것으로, 공개키 암호 방식을 이용한 인증이지만, 본 발명은 이에 한정되는 것은 아니다.
도 20에 있어서, 2개의 기기(예컨대, LCM(1)과 MC(13)) 사이에서 A로부터 A로 액세스하려고 하고 있는 B를 인증하는 경우에 관해서 설명한다.
이 경우, 기기 A는 공개키 kp를 유지하고 있으며, 기기 A에 액세스 가능하다면, 기기 B는 공개키 kp에 대응하는 은닉키 ks를 유지하고 있다. 기기 B는 기기 A에서 발생된 난수 R을 수취하면, 그것을 은닉키 ks에서 암호화하여(ks[R]이라 나타냄), ks[R]을 기기 A에 돌려준다. 기기 A에서는 공개키를 이용하여, ks[R]을 복호하고, 복호 결과가 앞서 발생한 난수 R과 동등하다면, 기기 B는 올바른 상대라고 판정한다.
그 후, 상기와 동일한 것을 기기 B로부터 기기 A에 대하여 행함으로써 상호 인증을 행할 수 있다. 이 경우, 기기 B는 공개키를 유지하고, 기기 A는 은닉키를 유지하며, 기기 A가 기기 B에 의해 발생한 난수를 은닉키로 암호화하고 그것을 기기 B에서 공개키를 이용하여 복호하여, 앞서 발생한 난수와 동등한지를 확인한다.

발명의 효과

이상 상술한 바와 같이, 본 발명에 따르면, 복제 콘텐츠의 수를 효율적으로 규제하여, 콘텐츠의 저작권 보호를 가능하게 한다.

(57) 청구의 범위

청구항 1.
복사 가능 회수를 제어할 수 있는 콘텐츠 관리 방법에 있어서,
소정의 복사 가능 회수가 부여된 콘텐츠를, 이 복사 가능 회수와 함께 기억 장치(8, 10)에 기억시켜 두고,
상기 기억 장치(8, 10)에 기억되어 있는 상기 콘텐츠가 어떤 기록 매체(13)상에 복사될 때, 상기 기억 장치(8, 10)에 기억되어 있는 상기 복사 가능 회수를 감산하고,
상기 기록 매체(13) 상의 상기 복사된 콘텐츠가 이 기록 매체(13)로부터 소거될 때, 상기 기억 장치(8, 10)에 기억되어 있는 상기 복사 가능 회수를 가산하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 2.
제1항에 있어서, 상기 콘텐츠를 재생하기 위해 필요한 정보를, 특정 수속으로 액세스할 수 있는 기억 영역에 기록하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 3.
제1항에 있어서, 상기 콘텐츠에 부여되어 있는 상기 복사 가능 회수를, 특정 수속으로 액세스할 수 있는 기억 영역에 기록하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 4.
제1항에 있어서, 상기 기억 장치(8, 10)에 기억되어 있는 상기 콘텐츠가 상기 기록 매체(13)상에 복사될 때, 이 기록 매체(13)의 식별 정보를 특정 수속으로 액세스할 수 있는 기억 영역에 기록하고,
상기 기록 매체(13)의 식별 정보가 상기 기억 영역에 기억되어 있는 경우에 한해, 상기 복사된 콘텐츠를 상기 기록 매체(13)로부터 소거할 수 있도록 하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 5.
제1항에 있어서, 상기 기록 매체(13)상의 상기 복사된 콘텐츠를 소거할 수 있는지 여부를 나타내는 플래그 정보를, 특정 수속으로 액세스할 수 있는 기억 영역에 기록하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 6.
제1항에 있어서, 상기 기록 매체(13)에 대한 데이터의 판독 또는 기록 처리에 걸리는 시간이 소정 시간 이내가 아닐 때, 이후의 처리를 중단하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 7.
제1항에 있어서, 상기 기록 매체(13)로서, 그 기억 영역 내에, 특정 수속만으로 액세스할 수 있는 기억 영역이 설치되는 동시에 이 기록 매체(13)의 식별 정보가 기억된 제1 종별의 기록 매체와, 상기 기억 영역을 구비하지 않지만 이 기록 매체의 식별 정보는 가지고 있는 제2 종별의 기록 매체와, 상기 기억 영역 및 이 기록 매체의 식별 정보를 갖지 않는 제3 종별의 기록 매체가 있는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 8.
제7항에 있어서, 상기 기록 매체(13)상에 상기 콘텐츠를 복사할 때 및 이 기록 매체(13)상의 상기 복사된 콘텐츠를 소거할 때 및 이 기록 매체(13)상의 상기 복사된 콘텐츠를 재생할 때에는, 이 기록 매체(13)의 종별을 판별하고 나서, 그것에 따른 처리를 행하는 것을 특징으로 하는 콘텐츠 관리 방법.

청구항 9.
복사 가능 회수를 제어할 수 있는 콘텐츠 관리 장치에 있어서,
소정의 복사 가능 회수가 부여된 콘텐츠를 이 복사 가능 회수와 함께 기억하고 있는 기억 장치(8, 10);
상기 기억 장치(8, 10)에 기억되어 있는 상기 콘텐츠가 어떤 기록 매체(13)상에 복사될 때, 상기 기억 장치(8, 10)에 기억되어 있는 상기 복사 가능 회수를 감산하는 한편, 상기 기록 매체(13)상의 상기 복사된 콘텐츠가 이 기록 매체(13)로부터 소거될 때, 상기 기억 장치(8, 10)에 기억되어 있는 상기 복사 가능 회수를 가산하는 복사 관리 장치(2)를 더 구비하는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 10.
제9항에 있어서, 상기 콘텐츠를 재생하기 위해 필요한 정보를, 특정 수단으로 액세스할 수 있는 기억 영역에 기록하는 수단을 더 구비하고 있는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 11.
제9항에 있어서, 상기 콘텐츠에 부여되어 있는 상기 복사 가능 회수를, 특정 수단으로 액세스할 수 있는 기억 영역에 기록하는 수단을 더 구비하고 있는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 12.
제9항에 있어서, 상기 기억 장치(8, 10)에 기억되어 있는 상기 콘텐츠가 상기 기록 매체(13)상에 복사될 때, 이 기록 매체(13)의 식별 정보를 특정 수단으로 액세스할 수 있는 기억 영역에 기록하고, 상기 기록 매체(13)의 식별 정보가 상기 기억 영역에 기억되어 있는 경우에 한해, 상기 복사된 콘텐츠를 상기 기록 매체(13)로부터 소거할 수 있도록 하는 수단을 더 구비하고 있는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 13.

제9항에 있어서, 상기 기록 매체(13)상의 상기 복사된 콘텐츠를 소거할 수 있는지 여부를 나타내는 플래그 정보를, 특정 수단으로 액세스할 수 있는 기억 영역에 기록하는 수단을 더 구비하고 있는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 14.

제9항에 있어서, 상기 기록 매체(13)에 대한 데이터의 판독 혹은 기록 처리에 걸리는 시간이 소정 시간 이내가 아닐 때, 이후의 처리를 중단하는 수단을 더 구비하고 있는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 15.

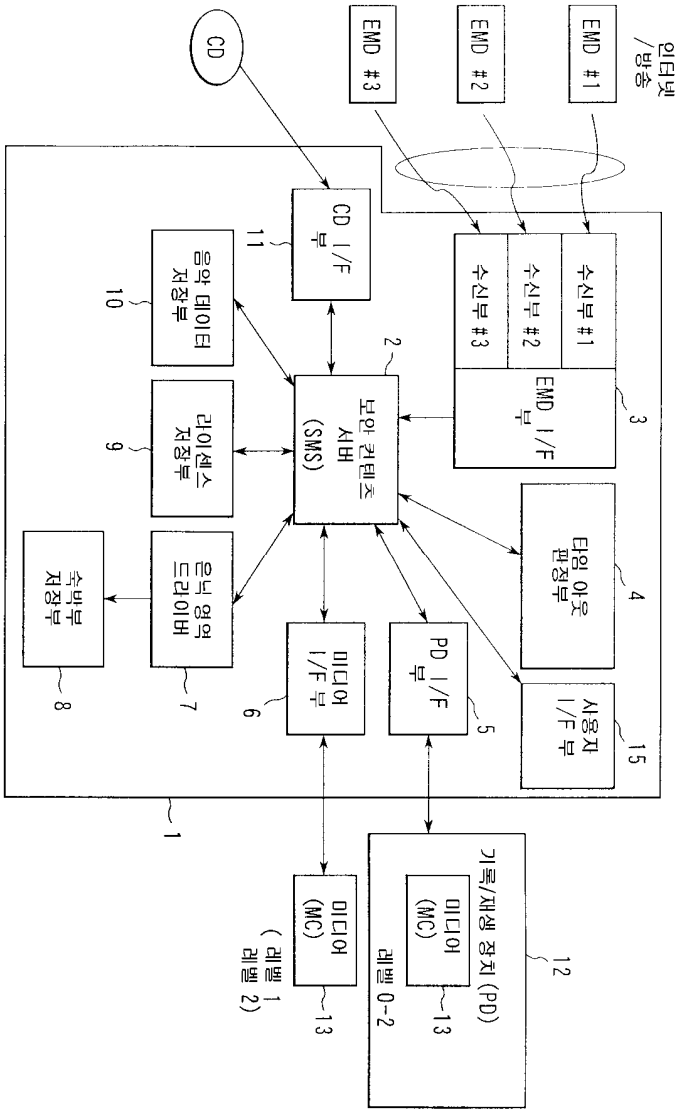
제9항에 있어서, 상기 기록 매체(13)로서, 그 기억 영역 내에, 특정 수속만으로 액세스할 수 있는 기억 영역이 설치되는 동시에 이 기록 매체(13)의 식별 정보가 기억된 제1 종별의 기록 매체와, 상기 기억 영역을 구비하지 않지만 이 기록 매체의 식별 정보는 가지고 있는 제2 종별의 기록 매체와, 상기 기억 영역 및 이 기록 매체의 식별 정보를 갖지 않는 제3 종별의 기록 매체가 있는 것을 특징으로 하는 콘텐츠 관리 장치.

청구항 16.

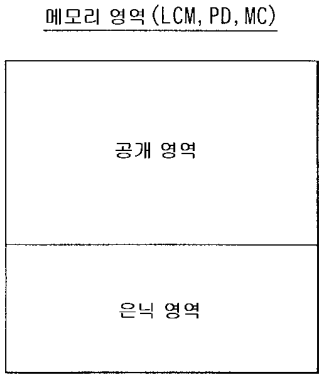
제15항에 있어서, 상기 기록 매체(13)상에 상기 콘텐츠를 복사할 때 및 이 기록 매체(13)상의 상기 복사된 콘텐츠를 소거할 때 및 이 기록 매체(13)상의 상기 복사된 콘텐츠를 재생할 때, 이 기록 매체(13)의 종별을 판별하는 수단을 구비하고 있는 것을 특징으로 하는 콘텐츠 관리 장치.

도면

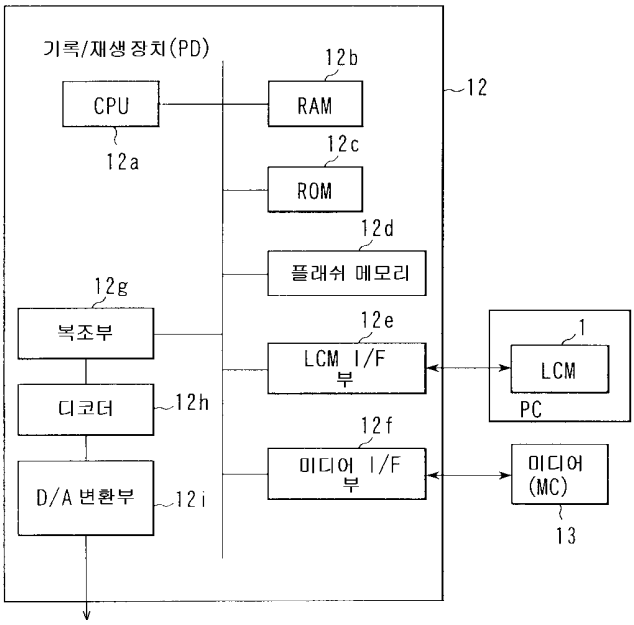
도면1



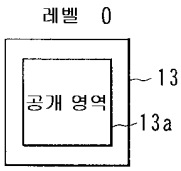
도면2



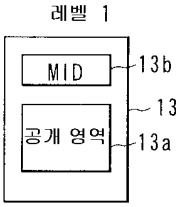
도면3



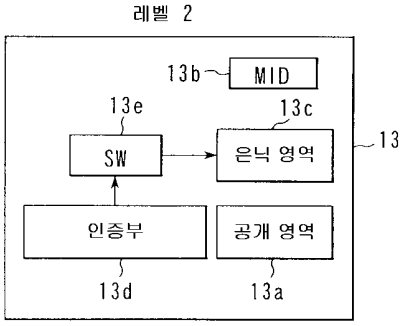
도면4a



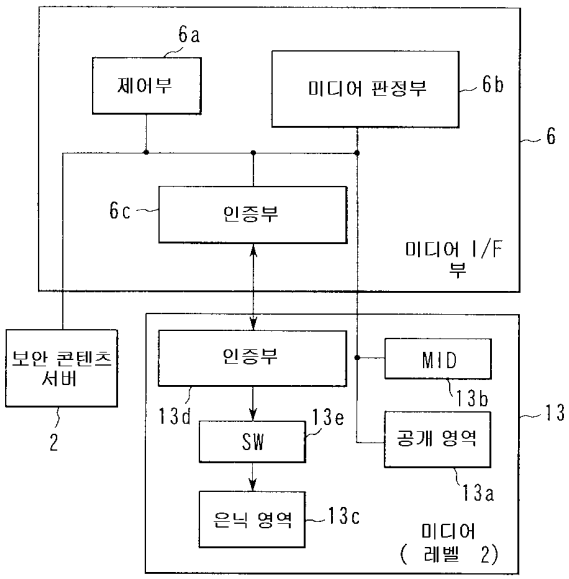
도면4b



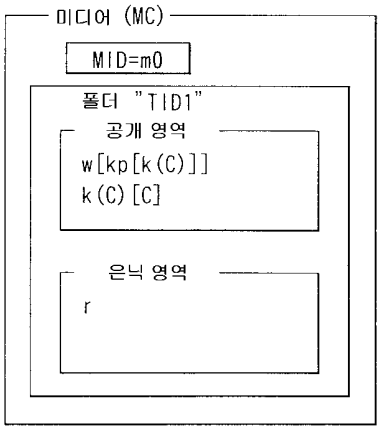
도면4c


레벨 2
13b
MID
13e
13c
SW
은닉 영역
13
인증부
공개 영역
13d
13a

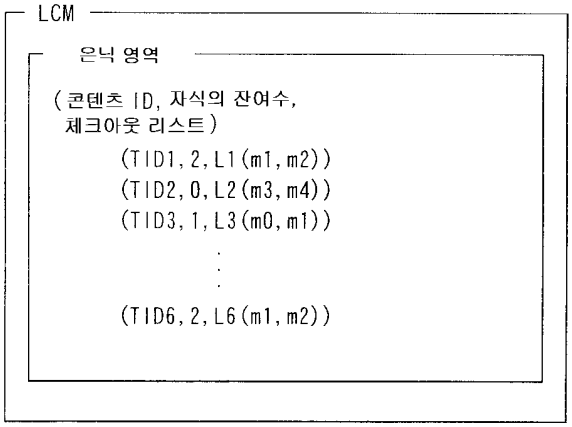
도면5


6a
제어부
미디어 판정부
6b
6
6c
인증부
미디어 I/F 부
보안 콘텐츠 서버
2
인증부
MID
13b
13d
13e
SW
공개 영역
13a
13
은닉 영역
13c
미디어 (레벨 2)

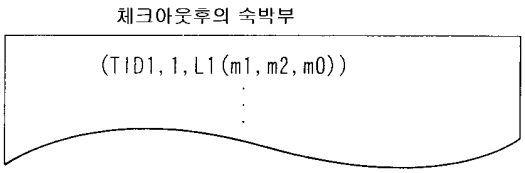
도면6


미디어 (MC)
MID=m0
폴더 "TID1"
공개 영역
w[kp[k(C)]]
k(C)[C]
은닉 영역
r

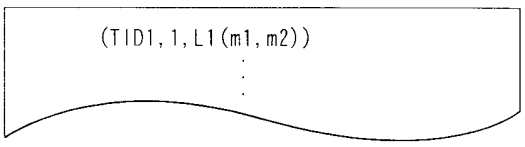
도면7a



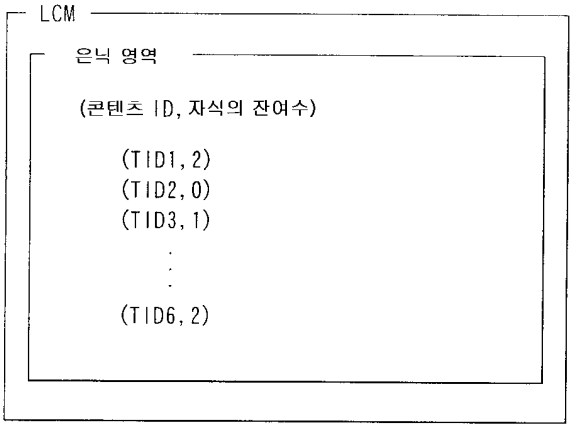
도면7b



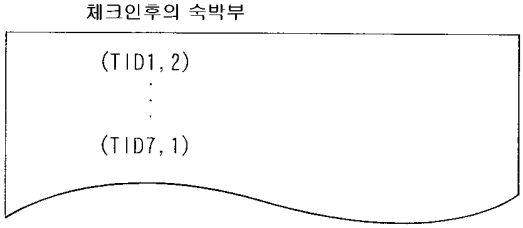
도면7c



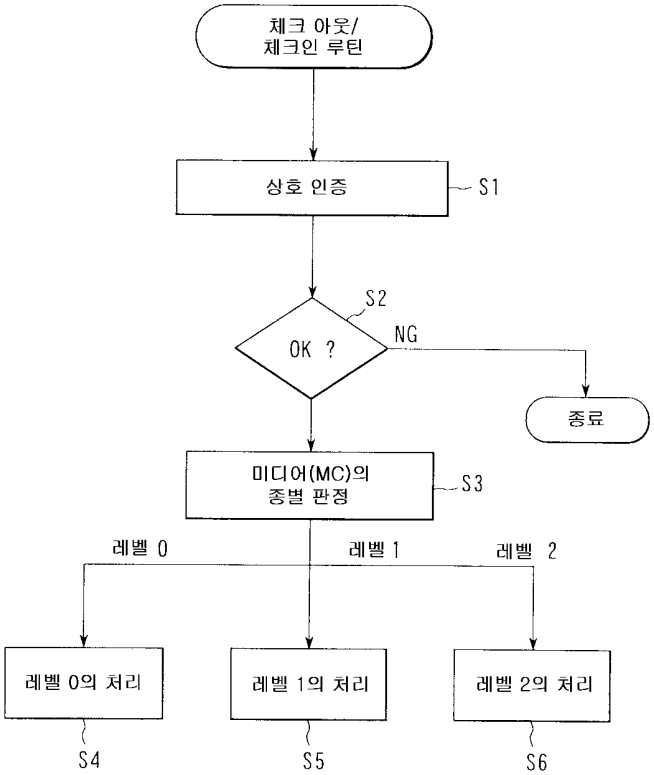
도면8a



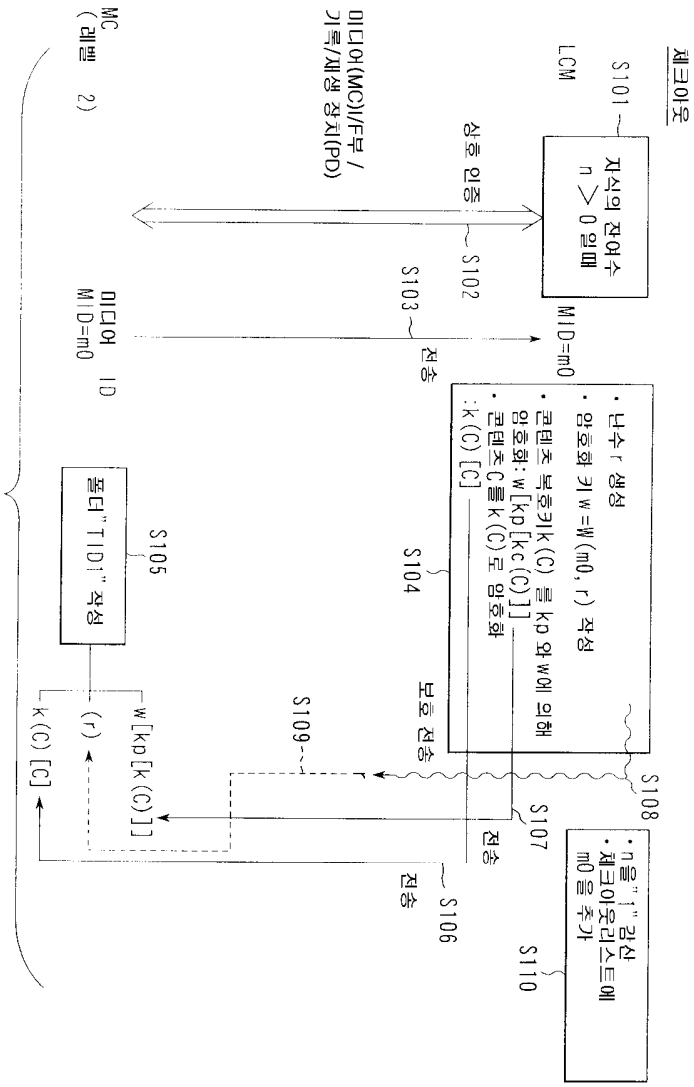
도면8b



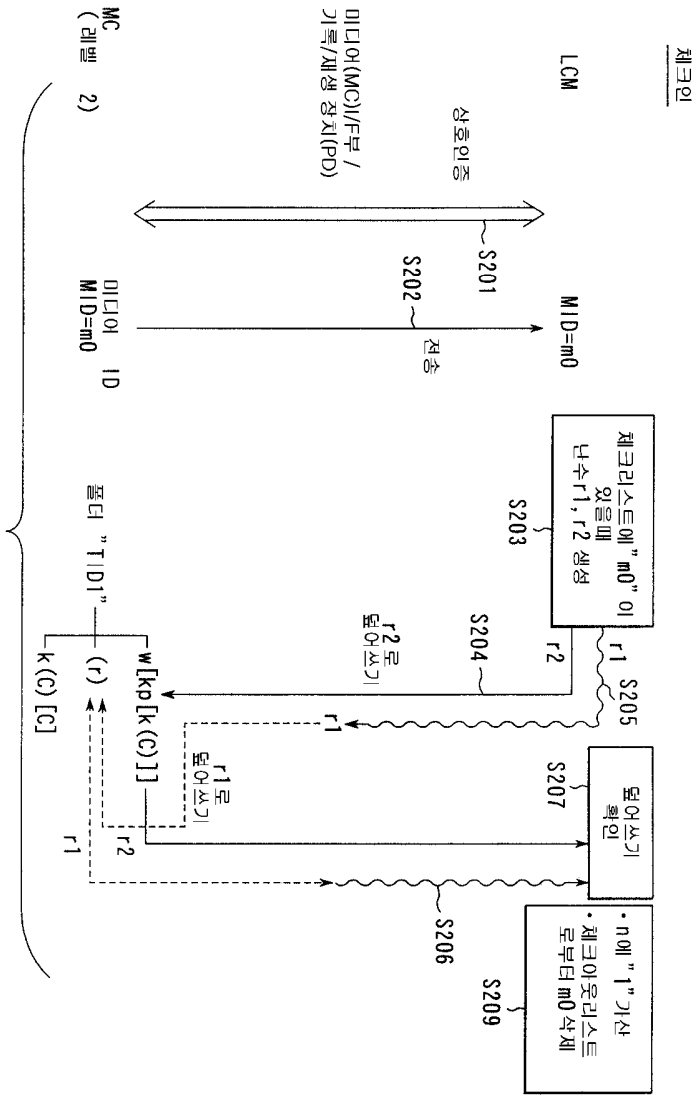
도면9


체크 아웃/
체크인 루틴
상호 인증
S1
S2
OK ?
NG
종료
미디어(MC)의
종별 판정
S3
레벨 0
레벨 1
레벨 2
레벨 0의 처리
레벨 1의 처리
레벨 2의 처리
S4
S5
S6

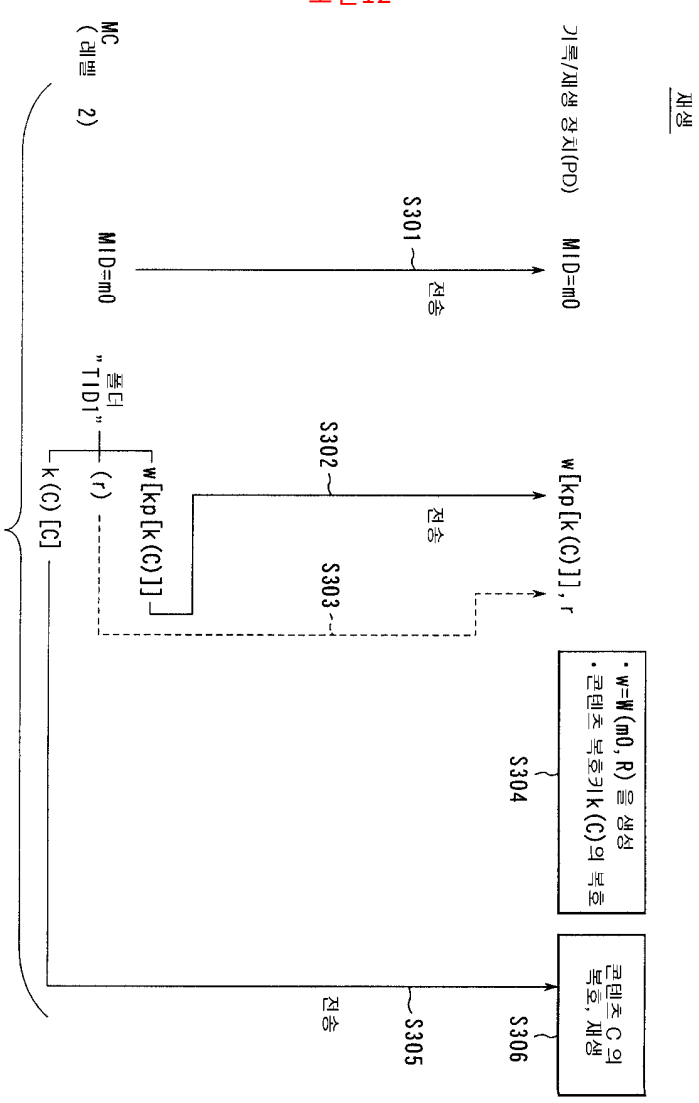
도면10


체크아웃
S101
지식의 잔여수
n > 0 일때
LCM
상호 인증
S102
미디어(MC)I/F부 /
기록/재생 장치(PD)
MC
(레벨 2)
S103
MID=m0
전송
미디어 ID
MID=m0
• 난수 r 생성
• 암호화 키 w=W(m0, r) 작성
• 콘텐츠 복호키 k(C) 를 kp 와 w에 의해
암호화 : w[kp[kc(C)]]
• 콘텐츠 C를 k(C)로 암호화
:k(C) [C]
S104
보호 전송
S105
폴더"TID1" 작성
w[kp[k(C)]]
(r)
k(C) [C]
S109
S107
전송
S106
전송
S108
• n을 "1" 감산
• 체크아웃리스트에
m0을 추가
S110

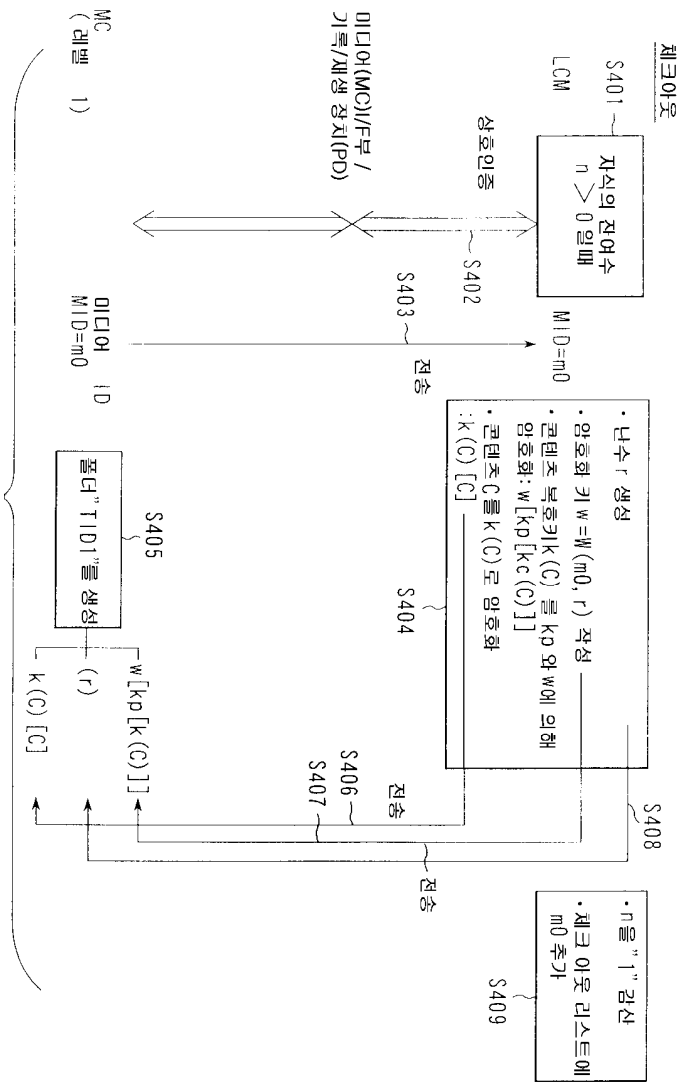
도면11


체크인
LCM
미디어(MC)I/F부 / 기록/재생 장치(PD)
상호인증
S201
S202
MID=m0
전송
미디어 ID
MID=m0
MC
(레벨 2)
체크리스트에 "m0" 이 있을때 난수r1, r2 생성
S203
r1
r2
S204
r2로 덮어쓰기
S205
r1
r1로 덮어쓰기
S207
덮어쓰기 확인
r2
r1
S206
S209
・n에 "1" 가산
・체크아웃리스트로부터 m0 삭제
w[kp[k(C)]]
(r)
k(C)[C]
풀더 "TID1"

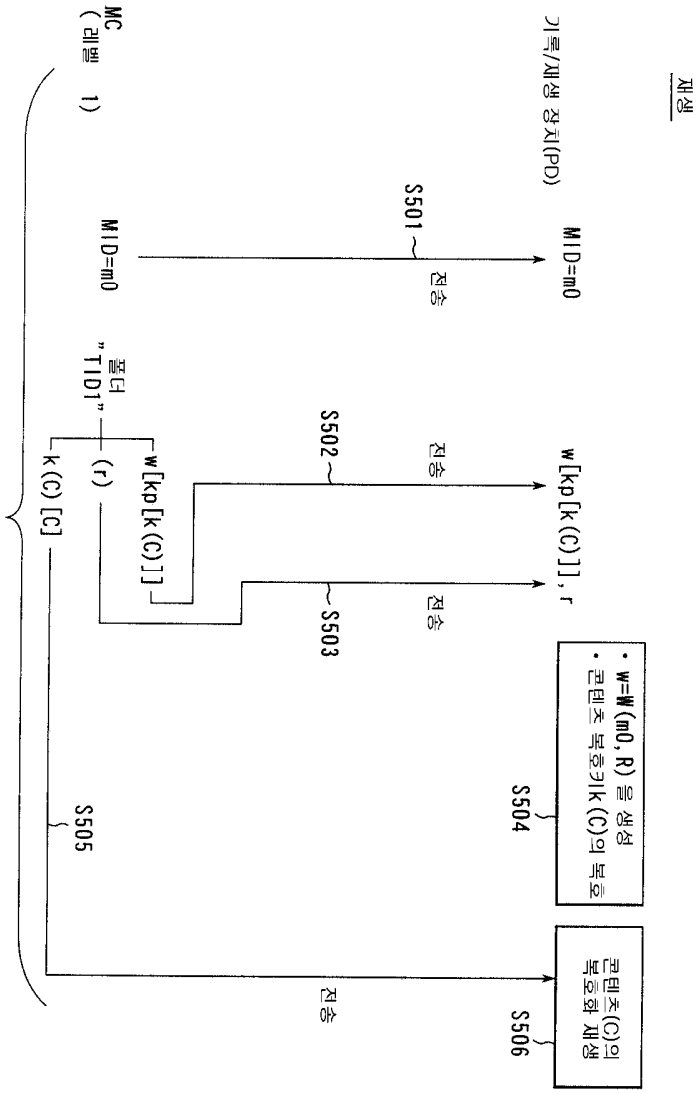
도면12


재생
기록/재생 장치(PD)
MC
(레벨 2)
MID=m0
S301
전송
MID=m0
폴더
"TID1"
(r)
k(C) [C]
S302
w[kp[k(C)]]
전송
w[kp[k(C)]], r
S303
• w=W(m0, R) 을 생성
• 콘텐츠 복호키 k(C)의 복호
S304
콘텐츠 C 의
복호, 재생
S305
전송
S306

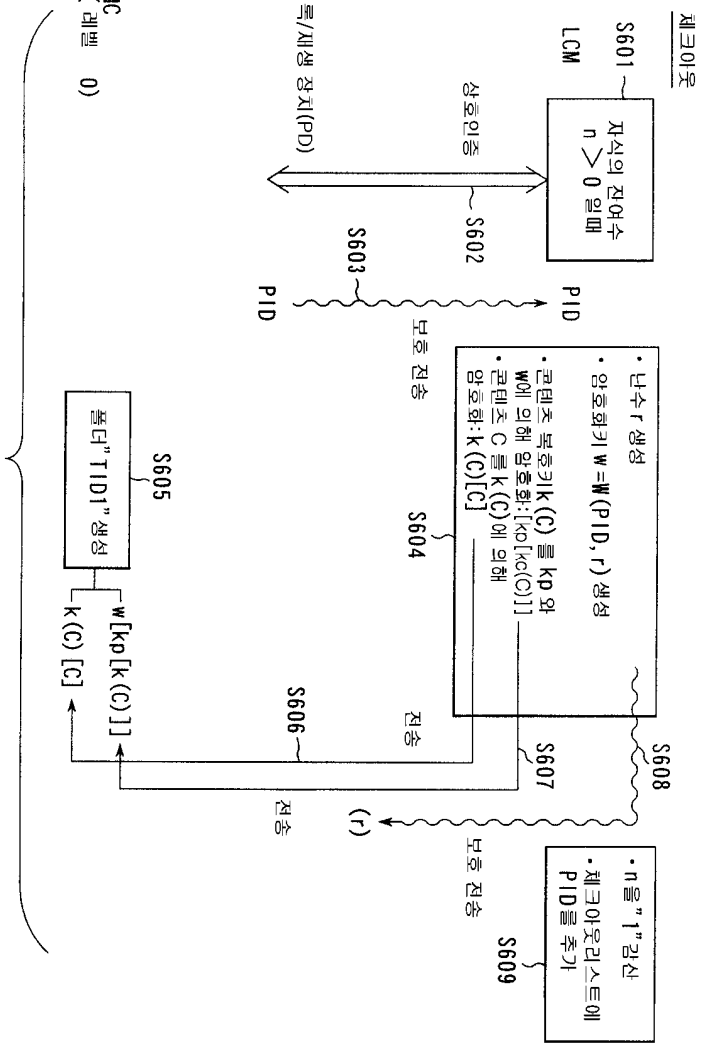
도면13


체크아웃
S401
LCM
자신의 잔여수 n > 0 일때
상호인증
S402
미디어(MC)I/F부 / 기록/재생 장치(PD)
MC (레벨 1)
S403
MID=m0
전송
미디어 MID=m0 ID
S404
• 난수 r 생성
• 암호화 키 w=W(m0, r) 작성
• 콘텐츠 복호키 k(C) 를 kp 와 w에 의해 암호화 : w[kp[kc(C)]]
• 콘텐츠 C를 k(C)로 암호화 : k(C) [C]
S405
폴더 "TID1"를 생성
(r)
w[kp[k(C)]]
k(C) [C]
S406
S407
전송
전송
S408
• n을 "1" 감산
• 체크 아웃 리스트에 m0 추가
S409

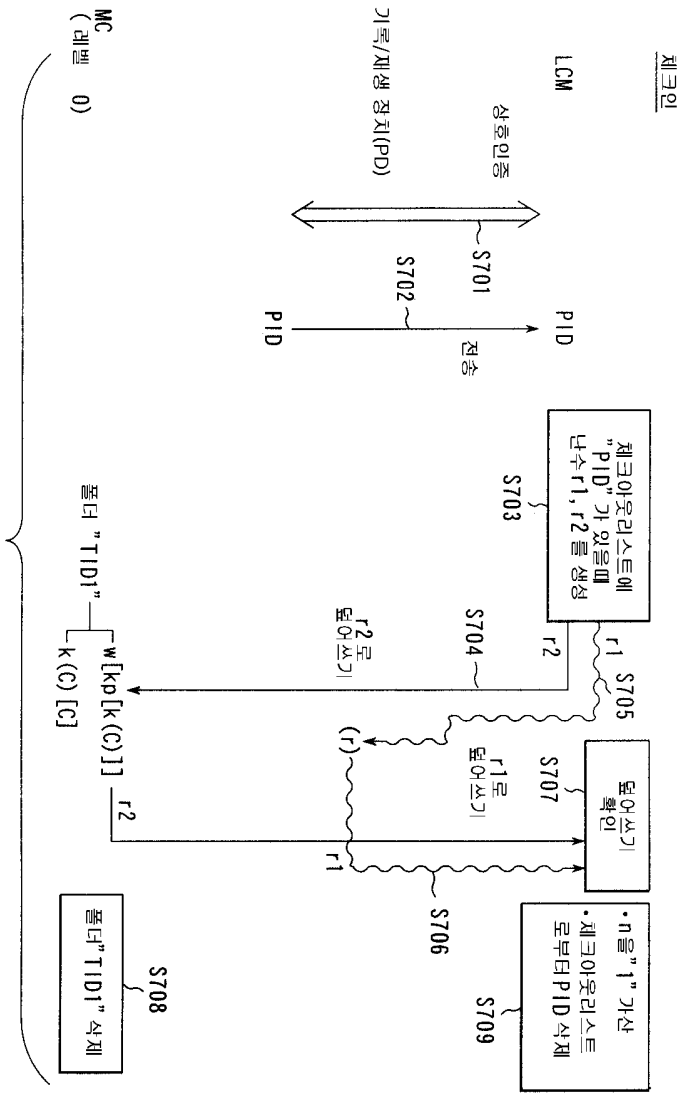
도면14


재생
기록/재생 장치(PD)
MC
(레벨 1)
MID=m0
S501
전송
MID=m0
폴더
"TID1"
(r)
k(C) [C]
S502
전송
w[kp[k(C)]]
w[kp[k(C)]], r
S503
전송
• w=W(m0, R) 을 생성
• 콘텐츠 복호키 k(C)의 복호
S504
S505
콘텐츠(C)의
복호화 재생
S506
전송

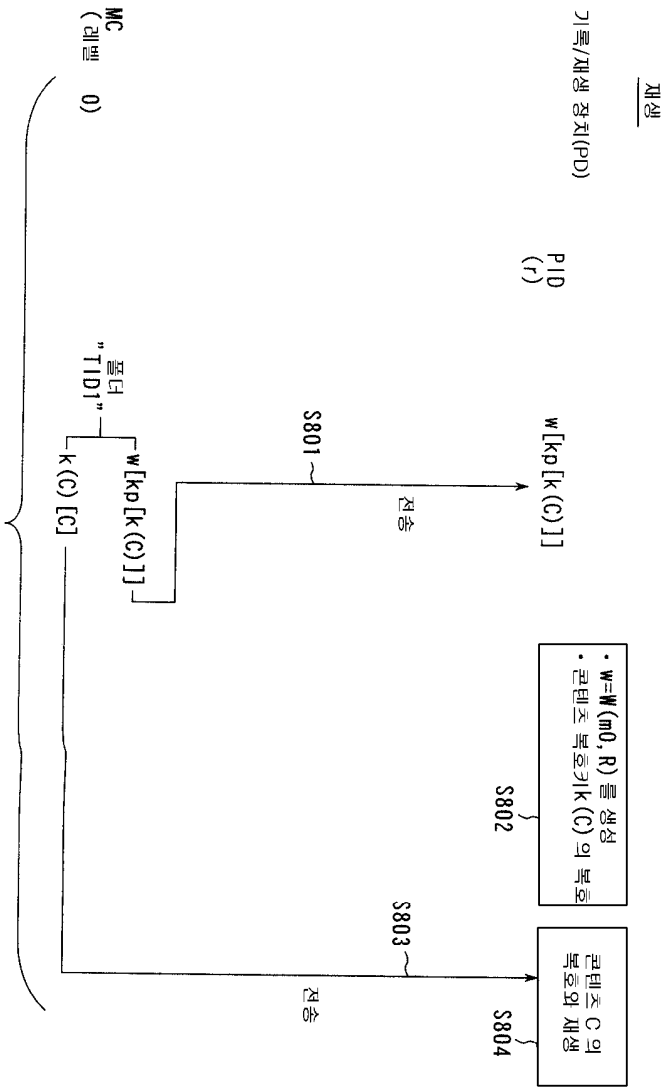
도면15


체크아웃
S601
LCM
자식의 전여수
n > 0 일때
상호인증
S602
기록/재생 장치(PD)
S603
PID
PID
보호 전송
• 난수 r 생성
• 암호화키 w=W(PID, r) 생성
• 콘텐츠 복호키 k(C) 를 kp 와 w에 의해 암호화:[kp[k(C)]]
• 콘텐츠 C 를 k(C)에 의해 암호화:k(C)[C]
S604
전송
S605
폴더"TID1"생성
w[kp[k(C)]]
k(C)[C]
S606
전송
S607
(r)
S608
보호 전송
• n을"1"감산
• 체크아웃리스트에 PID를 추가
S609
MC
(레벨 0)

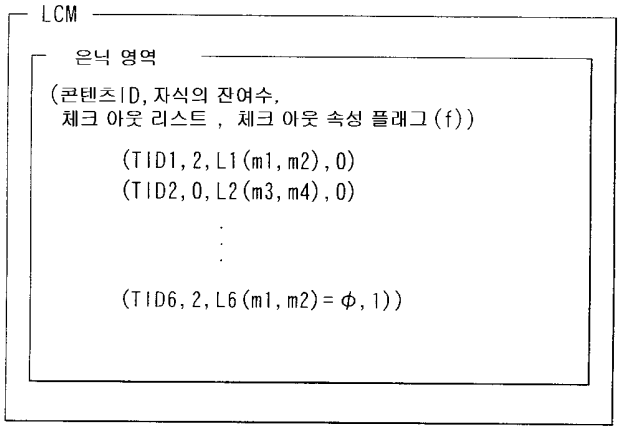
도면16


체크인
LCM
상호인증
기록/재생 정지(PD)
S701
S702
PID
PID
전송
S703
체크아웃리스트에 "PID"가 있을때 난수 r1, r2 를 생성
r1
r2
S704
r2 로 덮어쓰기
S705
MC (레벨 0)
폴더 "TID1"
k(C) [C]
w[kp[k(C)]]
r2
(r)
r1
S706
S707
덮어쓰기 확인
r1로 덮어쓰기
S708
폴더"TID1" 삭제
S709
• n을 "1" 가산
• 체크아웃리스트로부터 PID 삭제

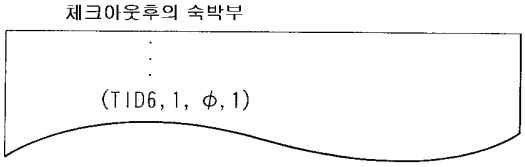
도면17



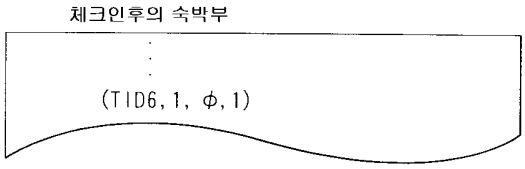
도면18a



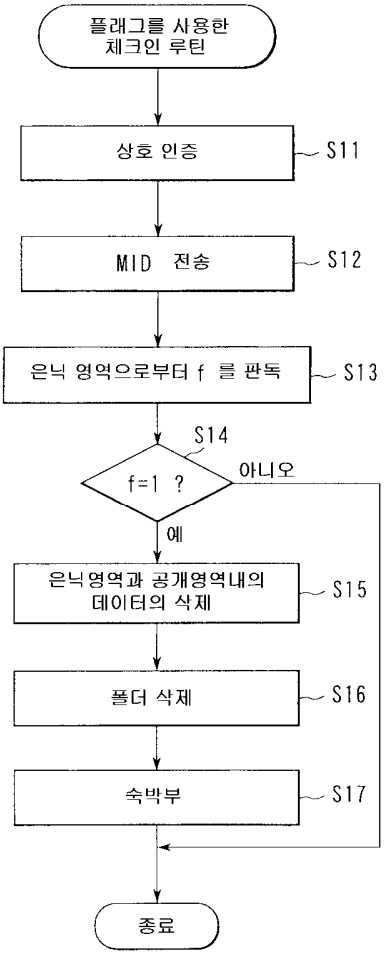
도면18b



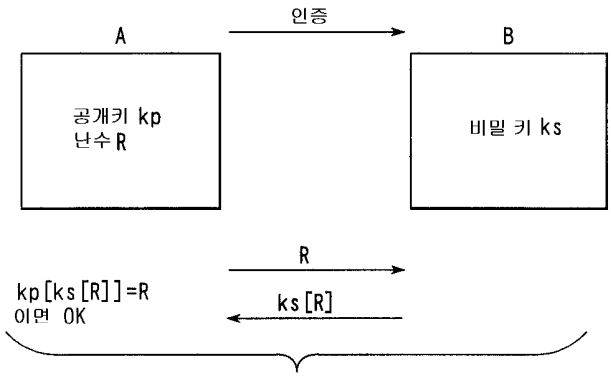
도면18c



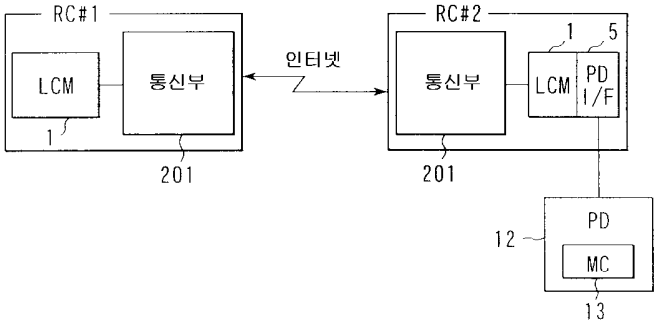
도면19



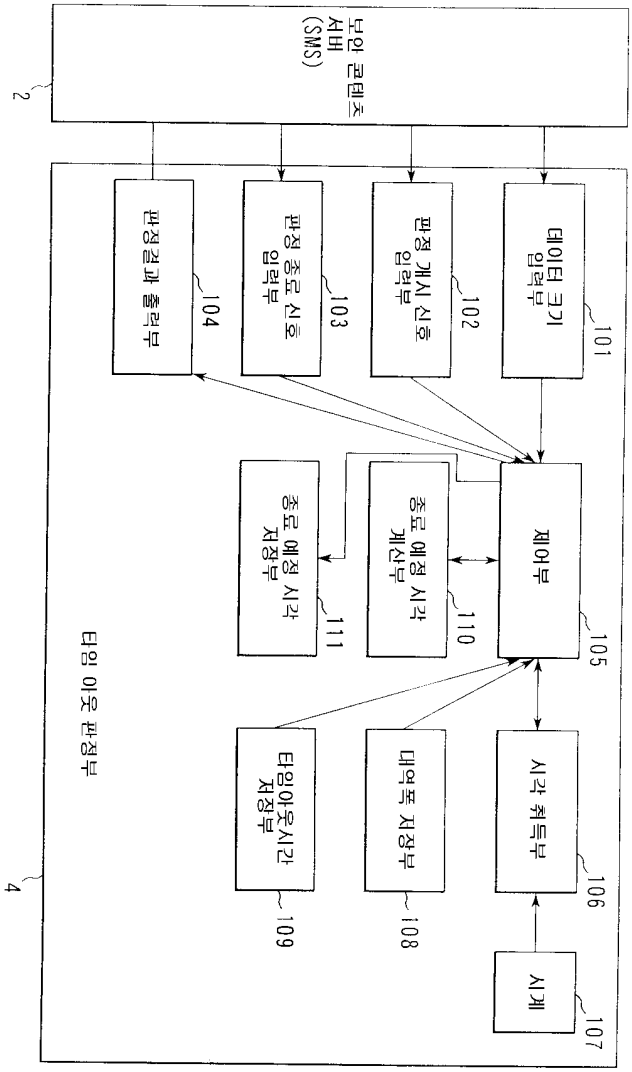
도면20



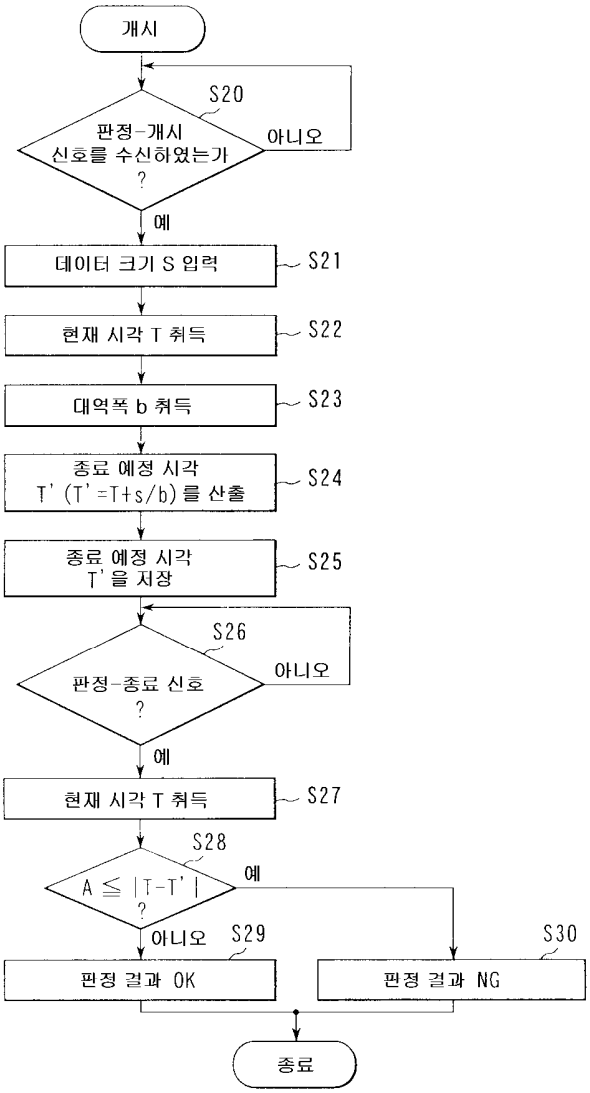
도면21


RC#1
LCM
통신부
1
201
인터넷
RC#2
통신부
LCM
PD I/F
1
5
201
PD
MC
12
13

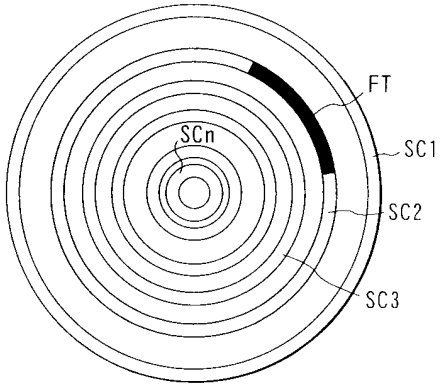
도면22


무인 콘텐츠 서버 (SMS)
2
타임 이웃 판정부
4
판정결과 출력부
104
판정 종료 신호 입력부
103
판정 개시 신호 입력부
102
데이터 크기 입력부
101
제어부
105
종료 예정 시각 계산부
110
종료 예정 시각 저장부
111
타임아웃시간 저장부
109
대역폭 저장부
108
시각 취득부
106
시계
107

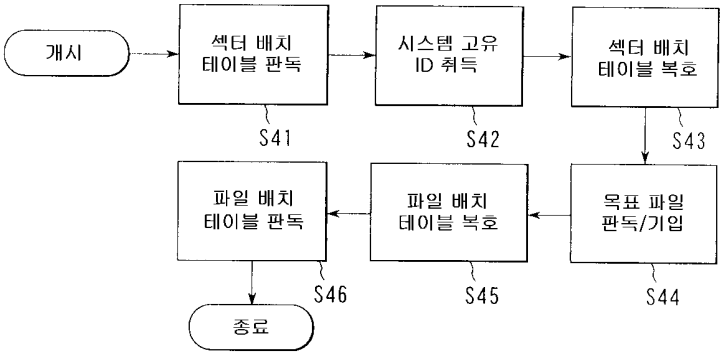
도면23


개시
S20
판정-개시 신호를 수신하였는가 ?
아니오
예
데이터 크기 S 입력
S21
현재 시각 T 취득
S22
대역폭 b 취득
S23
종료 예정 시각 T' (T'=T+s/b) 를 산출
S24
종료 예정 시각 T' 을 저장
S25
S26
판정-종료 신호 ?
아니오
예
현재 시각 T 취득
S27
S28
A ≦ |T-T'| ?
예
아니오
S29
판정 결과 OK
S30
판정 결과 NG
종료

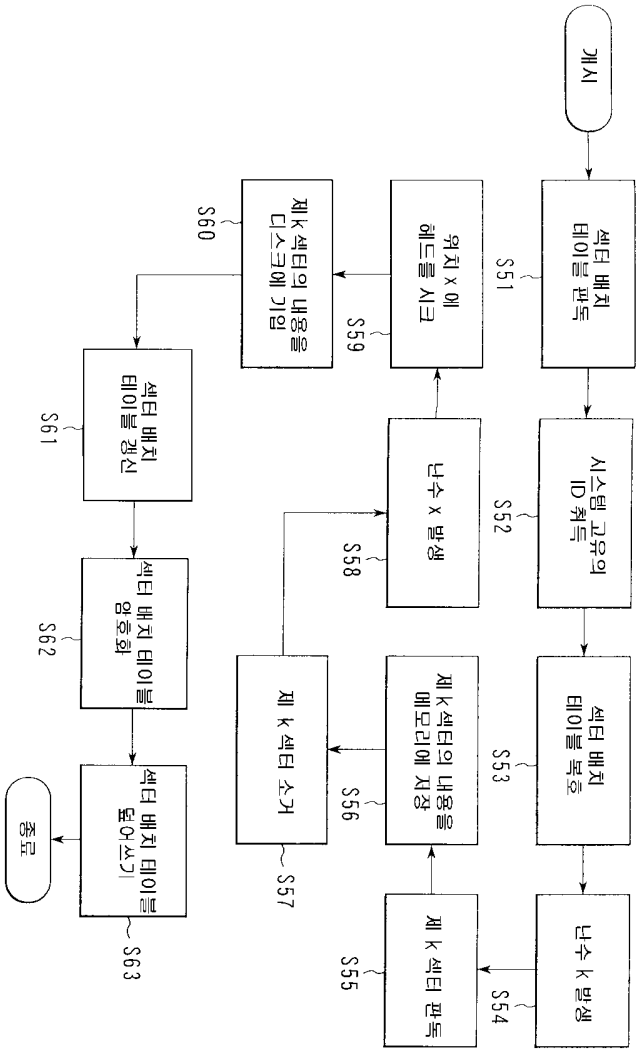
도면24


FT
SCn
SC1
SC2
SC3

도면25


개시
섹터 배치 테이블 판독
S41
시스템 고유 ID 취득
S42
섹터 배치 테이블 복호
S43
목표 파일 판독/기입
S44
파일 배치 테이블 복호
S45
파일 배치 테이블 판독
S46
종료

도면26


개시
섹터 배치 테이블 판독
S51
시스템 고유의 ID 취득
S52
섹터 배치 테이블 복호
S53
난수 k 발생
S54
제 k 섹터 판독
S55
제 k 섹터의 내용을 메모리에 저장
S56
제 k 섹터 소거
S57
난수 x 발생
S58
워치 x 에 헤드를 시크
S59
제 k 섹터의 내용을 디스크에 기입
S60
섹터 배치 테이블 갱신
S61
섹터 배치 테이블 암호화
S62
섹터 배치 테이블 덮어쓰기
S63
종료