(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 12/14 (2006.01)
G06F 15/16 (2006.01)
G06F 21/00 (2006.01)
G06F 3/06 (2006.01)

(11) 공개번호 10-2007-0015567
(43) 공개일자 2007년02월05일

(21) 출원번호 10-2006-7023333
(22) 출원일자 2006년11월07일
심사청구일자 없음
번역문 제출일자 2006년11월07일
(86) 국제출원번호 PCT/JP2005/006906
국제출원일자 2005년04월08일
(87) 국제공개번호 WO 2005/101215
국제공개일자 2005년10월27일

(30) 우선권주장 JP-P-2004-00118594 2004년04월14일 일본(JP)

(71) 출원인 마츠시타 덴끼 산교 가부시키가이샤
일본 오오사카후 가도마시 오오아자 가도마 1006

(72) 발명자 요코타 가오루
일본국 오오사카후 가도마시 오오아자 가도마 1006 마츠시타 덴끼산교 가부시키가이샤 나이
오모리 모토지
일본국 오오사카후 가도마시 오오아자 가도마 1006 마츠시타 덴끼산교 가부시키가이샤 나이
나카노 도시히사
일본국 오오사카후 가도마시 오오아자 가도마 1006 마츠시타 덴끼산교 가부시키가이샤 나이
하라다 슌지
일본국 오오사카후 가도마시 오오아자 가도마 1006 마츠시타 덴끼산교 가부시키가이샤 나이
이토 요시카츠
일본국 오오사카후 가도마시 오오아자 가도마 1006 마츠시타 덴끼산교 가부시키가이샤 나이
다카하시 쥰
일본국 오오사카후 가도마시 오오아자 가도마 1006 마츠시타 덴끼산교 가부시키가이샤 나이

(74) 대리인 김영철

전체 청구항 수 : 총 29 항

(54) 단말장치 및 저작권 보호시스템

(57) 요약

변환을 시행한 콘텐츠를 다른 기기에 이동한 경우에도, 콘텐츠의 이동 처의 기기로부터 콘텐츠의 이동원으로 다시 콘텐츠를 이동시킨 경우에, 변환 전의 콘텐츠를 이용할 수 있는 단말장치를 제공한다. 단말장치는 상기 콘텐츠를 미리 기억하고, 상기 콘텐츠에 질을 떨어뜨리는 비 가역 변환을 하여 변환콘텐츠를 생성하며, 생성한 변환콘텐츠를 상기 기록매체에 기록한다. 단말장치는 암호키를 이용하여 상기 콘텐츠의 1 블록을 암호화하여 암호화 블록을 생성하고, 상기 1 블록을 상기 암호화 블록으로 치환하며, 상기 암호키를 상기 기록매체에 기록한다.

대표도

도 2

특허청구의 범위

청구항 1.

오리지널 콘텐츠(original content)를 휴대형 기록매체(portable storage medium)에 이동시키는 단말장치로,

상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과,

상기 오리지널 콘텐츠에 비 가역 변환(irreversible conversion)을 실시하여 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과,

상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과,

암호키를 이용하여 상기 오리지널 콘텐츠의 1 블록을 암호화하여 암호화블록을 생성하고, 상기 1 블록을 상기 암호화블록으로 치환하는 암호화 수단과,

상기 암호키를 상기 기록매체에 기록하는 키 기록수단과,

상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제수단을 구비하는 것을 특징으로 하는 단말장치.

청구항 2.

제 1항에 있어서,

상기 오리지널 콘텐츠는 복수의 블록데이터마다 암호화된 암호화 콘텐츠이고,

상기 블록은 암호화된 블록데이터이며,

상기 변환콘텐츠 생성수단은 상기 암호화 콘텐츠를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 상기 오리지널 콘텐츠에 상기 비 가역 변환을 하여 변환콘텐츠를 생성하며,

상기 암호화 수단은, 상기 암호키를 이용하여 상기 암호화된 블록데이터를 암호화하여 이중 암호화 블록데이터를 상기 암호화 블록으로 생성하고, 상기 암호화된 블록데이터를 생성한 이중 암호화 블록데이터로 치환하는 것을 특징으로 하는 단말장치.

청구항 3.

제 2항에 있어서,

상기 암호화수단은, 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하고, 암호화된 블록데이터별로 이중 암호화 블록데이터로 치환하는 것을 특징으로 하는 단말장치.

청구항 4.

제 3항에 있어서,

상기 암호화 수단은, 암호화된 모든 블록데이터의 각각에 대해서 다른 암호키를 생성하고, 암호화된 블록데이터별로 각각에 대해서, 생성된 암호키를 이용하여 이중 암호화 블록데이터를 생성하며,

상기 키 기록수단은 상기 암호화수단에 의해 생성된 모든 암호키를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 5.

제 3항에 있어서,

상기 암호화수단은,

암호화된 블록데이터의 개수 미만인 소정의 개수의 암호키를 생성하고, 생성한 각 암호키를 주기적으로 이용하여 암호화된 모든 블록데이터별로 이중 암호화 블록데이터를 생성하며,

상기 키 기록수단은 상기 암호화 수단에 의해 생성된 상기 소정의 개수의 암호키를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 6.

제 3항에 있어서,

상기 복수의 암호화된 블록데이터는 재생 순위에 따라서 기억되어 있고,

상기 암호화수단은,

일 방향성 함수를 미리 기억하고 있는 함수기억부와,

키 데이터를 생성하는 제 1 키 생성부와,

상기 키 데이터에 상기 암호화된 블록데이터의 재생 순위에 따른 횟수만큼 상기 일 방향성 함수를 실시하여 상기 암호화된 블록데이터에 대한 순위 암호키를 생성하는 제 2 키 생성부와,

암호화된 블록데이터를 상기 제 2 키 생성부에서 생성한 순위 암호키를 상기 암호키로 이용하여 암호화하여 이중 암호화 블록데이터를 생성하는 암호화 블록생성부와,

상기 암호화된 블록데이터를 상기 이중 암호화블록 생성부에서 생성된 상기 이중 암호화 블록으로 치환하는 블록 치환부를 구비하고,

상기 키 기록수단은 제 1 키 생성부에서 생성된 키 데이터를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 7.

제 2항에 있어서,

상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 암호화하여 암호화 변환콘텐츠를 더 생성하고,

상기 변환콘텐츠 기록수단은, 상기 변환콘텐츠를 상기 기록매체에 기록하는 대신, 생성한 상기 암호화 변환콘텐츠와 상기 암호화 변환콘텐츠를 복호하는 복호 키 정보를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 8.

제 7항에 있어서,

상기 변환콘텐츠 기록수단은, 상기 변환콘텐츠에 포함되는 복수의 변환블록별로 암호화하여 암호화 변환블록을 생성하고, 생성한 복수의 암호화 변환블록별로 상기 기록매체에 기록함으로써, 상기 암호화 변환콘텐츠의 생성 및 기록을 행하는 것을 특징으로 하는 단말장치.

청구항 9.

제 8항에 있어서,

상기 암호화 변환콘텐츠와 상기 암호키 정보를 상기 기록매체에 기록하고, 상기 블록을 상기 암호화 블록으로 치환한 후의 단말장치로,

상기 단말장치는,

상기 기록매체에 기록되어 있는 상기 암호화 변환콘텐츠 및 상기 복호 키 정보의 소거에 관한 제어를 행하는 변환콘텐츠 소거수단과,

상기 변환콘텐츠 소거수단에서 소거에 관한 제어가 이루어진 후, 상기 기록매체로부터 상기 암호키를 판독하고, 판독한 상기 암호키를 복호 키로 이용하여 상기 이중 암호화 블록데이터를 복호하여 상기 암호화된 블록데이터를 생성하며, 상기 이중 암호화 블록데이터를 생성한 상기 암호화된 블록데이터에 재기록하는 복호수단을 더 구비하는 것을 특징으로 하는 단말장치.

청구항 10.

제 9항에 있어서,

상기 단말장치는,

상기 오리지널 콘텐츠를 재생하는 재생수단을 더 구비하고,

상기 복호수단은, 상기 모든 암호화된 블록데이터를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 상기 오리지널 콘텐츠를 상기 재생수단에 출력하는 것을 특징으로 하는 단말장치.

청구항 11.

제 1항에 있어서,

상기 오리지널 콘텐츠는 복수의 블록데이터별로 암호화된 암호화 콘텐츠이고,

상기 오리지널 콘텐츠 기억수단은 상기 복수의 암호화된 블록데이터를 재생 순위에 따라서 기억하고 있으며,

상기 변환콘텐츠 생성수단은, 상기 암호화 콘텐츠를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 상기 오리지널 콘텐츠에 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하며,

상기 암호화수단은, 재생시간 길이가 소정 시간 내가 되도록 재생 순위가 연속하는 복수의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 상기 블록으로 취득하고, 취득한 암호화블록 데이터 군에 상기 암호키를 이용하여 암호화하여 이중 암호화블록 데이터 군을 상기 암호화 블록으로 생성하며, 상기 암호화블록 데이터 군을 생성한 상기 이중 암호화 블록 데이터 군으로 치환하는 것을 특징으로 하는 단말장치.

청구항 12.

제 11항에 있어서,

상기 오리지널 콘텐츠는 동화상이 압축 부호화된 복수의 프레임 데이터로 이루어지고,

상기 프레임 데이터는 1 이상의 블록데이터로 이루어지며,

상기 블록데이터는 당해 단말장치에 고유한 장치키로 암호화되고,

상기 단말장치는, 재생시간 길이가 소정 시간 내로 이루어지고, 재생 순위가 연속하는 1 이상의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 취득하고, 상기 장치 키를 복호 키로 이용하여 취득한 암호화블록 데이터 군을 복호하여 블록데이터 군을 생성하는 블록 복호수단을 더 구비하며,

상기 암호화 수단은, 상기 블록데이터 군에 포함되는 1 이상의 프레임 데이터 중, 다른 프레임 데이터와 무 의존(無 依存)인 독립 프레임 데이터를 상기 장치 키 및 상기 암호키의 순서로 암호화하고, 다른 프레임 데이터를 상기 장치 키로 암호화함으로써 이중 암호화블록 데이터 군을 생성하고, 상기 암호화블록 데이터 군을 생성한 이중 암호화 블록 데이터 군으로 치환하는 것을 특징으로 하는 단말장치.

청구항 13.

제 1항에 있어서,

오리지널 콘텐츠를 휴대형 기록매체에 이동시키는 단말장치로,

상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과,

상기 오리지널 콘텐츠에 비 가역 변환이 실시된 변환콘텐츠가 암호화된 비 오리지널 콘텐츠(non-original content)를 기억하고 있는 비 오리지널 콘텐츠 기억수단과,

상기 변환콘텐츠에 포함되고, 상기 비 오리지널 콘텐츠의 복호에 이용하는 복호블록데이터를 상기 오리지널 콘텐츠로부터 취득하는 복호블록데이터 취득수단과,

상기 비 오리지널 콘텐츠를 상기 복호블록데이터를 이용하여 복호하여 상기 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과,

상기 변환콘텐츠 생성수단에서 생성된 상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과,

암호키를 이용하여 상기 오리지널 콘텐츠의 1 블록을 암호화하여 암호화블록을 생성하고, 상기 1 블록을 상기 암호화 블록으로 치환하는 암호화수단과,

상기 암호키를 상기 기록매체에 기록하는 키 기록수단과,

상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제수단을 구비하는 것을 특징으로 하는 단말장치.

청구항 14.

제 13항에 있어서,

상기 변환콘텐츠에 포함되는 1 변환블록데이터를 암호키로 이용하여 상기 변환콘텐츠를 암호화함으로써 상기 비 오리지널 콘텐츠가 생성되고,

상기 비 오리지널 콘텐츠가 생성된 후 상기 암호키는 소거되며,

상기 복호블록데이터 취득수단은, 상기 오리지널 콘텐츠에 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하고, 생성한 상기 변환콘텐츠로부터 상기 1 변환블록데이터를 상기 복호 블록데이터로 취득하는 것을 특징으로 하는 단말장치.

청구항 15.

제 14항에 있어서,

상기 오리지널 콘텐츠는 복수의 블록데이터별로 암호화된 암호화 콘텐츠이고,

상기 블록은 암호화된 블록데이터이며,

상기 복호블록데이터 취득수단은, 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하여 상기 복호블록데이터를 취득하는 대신, 상기 1 변환블록데이터에 대응하는 암호화된 블록데이터를 복호하고, 상기 비 가역 변환을 하여 상기 복호블록데이터를 취득하고,

상기 암호화수단은, 상기 암호키를 이용하여 상기 암호화된 블록데이터를 암호화하여 이중 암호화 블록데이터를 상기 암호화 블록으로 생성하고, 상기 암호화된 블록데이터를 생성한 이중 암호화 블록데이터로 치환하는 것을 특징으로 하는 단말장치.

청구항 16.

제 15항에 있어서,

상기 암호화수단은, 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하고, 암호화된 블록데이터별로 이중 암호화 블록데이터로 치환하는 것을 특징으로 하는 단말장치.

청구항 17.

제 16항에 있어서,

상기 암호화 수단은,

암호화된 모든 블록데이터 각각에 대해서 다른 암호키를 생성하고, 암호화된 블록데이터별로 각각에 대해서 생성된 암호키를 이용하여 이중 암호화 블록데이터를 생성하며,

상기 키 기록수단은 상기 암호화수단에서 생성된 모든 암호키를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 18.

제 16항에 있어서,

상기 암호화 수단은,

암호화된 블록데이터의 개수 미만인 소정의 개수의 암호키를 생성하고, 생성한 각 암호키를 주기적으로 이용하여 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하고,

상기 키 기록수단은 상기 암호화수단에서 생성된 상기 소정의 개수의 암호키를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 19.

제 16항에 있어서,

상기 복수의 암호화된 블록데이터는 재생 순위에 따라서 기억되어 있고,

상기 암호화 수단은,

일 방향성 함수를 미리 기억하고 있는 함수 기억부와,

키 데이터를 생성하는 제 1 키 생성부와,

상기 키 데이터에 상기 암호화된 블록데이터의 재생 순위에 따른 횟수만큼 상기 일 방향성 함수를 실시하여 상기 암호화된 블록데이터에 대한 순위 암호키를 생성하는 제 2 키 생성부와,

암호화된 블록데이터를 상기 제 2 키 생성부에서 생성한 순위 암호키를 상기 암호키로 이용하여 암호화하여 이중 암호화 블록데이터를 생성하는 암호화 블록생성부와,

상기 암호화된 블록데이터를 상기 이중 암호화블록 생성부에서 생성된 상기 이중 암호화 블록으로 치환하는 블록 치환부를 구비하고,

상기 키 기록수단은, 상기 암호키 대신, 상기 제 1 키 생성부에서 생성된 상기 키 데이터를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 20.

제 15항에 있어서,

상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 암호화하여 암호화 변환콘텐츠를 더 생성하고,

상기 변환콘텐츠 기록수단은, 상기 변환콘텐츠를 상기 기록매체에 기록하는 대신, 생성한 상기 암호화 변환콘텐츠와 상기 암호화 변환콘텐츠를 복호하는 복호 키 정보를 상기 기록매체에 기록하는 것을 특징으로 하는 단말장치.

청구항 21.

제 20항에 있어서,

상기 비 오리지널 콘텐츠 기억수단은 상기 1 변환블록 데이터를 암호키로 이용하여 상기 변환콘텐츠를 상기 복수의 변환블록별로 암호화하여 기억하고 있고,

상기 변환콘텐츠 기록수단은,

상기 암호화된 변환블록별로 복호하여 상기 변환블록을 생성하는 제 1 생성부와,

상기 제 1 생성부에서 생성된 변환블록별로 암호화하여 재 암호화 변환블록을 생성하는 제 2 생성부와,

상기 제 2 생성부에서 생성된 재 암호화 변환블록별로 상기 기록매체에 기록하는 기록부를 구비하는 것을 특징으로 하는 단말장치.

청구항 22.

제 21항에 있어서,

상기 암호화 변환콘텐츠와 상기 복호 키 정보를 상기 기록매체에 기록하고, 상기 블록을 상기 암호화 블록으로 치환한 후의 단말장치로,

상기 단말장치는,

상기 기록매체에 기록되어 있는 상기 암호화 블록콘텐츠 및 상기 복호 키 정보의 소거에 관한 제어를 행하는 변환콘텐츠 소거수단과,

상기 변환콘텐츠 소거수단에서 소거에 관한 제어가 이루어진 후, 상기 기록매체로부터 상기 암호키를 판독하고, 판독한 상기 암호키를 복호 키로 이용하여 상기 이중 암호화 블록데이터를 복호하여 상기 암호화된 블록데이터를 생성하여, 상기 제 2 암호화 블록데이터를 생성한 상기 암호화된 블록데이터에 재기록하는 복호수단을 구비하는 것을 특징으로 하는 단말장치.

청구항 23.

제 22항에 있어서,

상기 단말장치는 상기 오리지널 콘텐츠를 재생하는 재생수단을 더 구비하고,

상기 복호수단은, 상기 모든 암호화된 블록데이터를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 상기 오리지널 콘텐츠를 상기 재생수단에 출력하는 것을 특징으로 하는 단말장치.

청구항 24.

제 14항에 있어서,

상기 오리지널 콘텐츠는 복수의 블록데이터마다 암호화된 암호화 콘텐츠이고,

상기 오리지널 콘텐츠 기억수단은 상기 복수의 암호화된 블록데이터를 재생순서에 따라서 기억하고 있으며,

상기 암호화 수단은,

재생시간 길이가 소정 시간 내가 되도록 재생 순위가 연속하는 복수의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 상기 블록으로 취득하고, 취득한 암호화블록 데이터 군에 상기 암호키를 이용하여 암호화하여 이중 암호화 블록 데이터 군을 상기 암호화 블록으로 생성하고, 상기 암호화 블록 데이터 군을 생성한 상기 이중 암호화 블록 데이터 군으로 치환하는 것을 특징으로 하는 단말장치.

청구항 25.

제 24항에 있어서,

상기 오리지널 콘텐츠는 동화상이 압축 부호화된 복수의 프레임 데이터로 이루어지고,

상기 프레임 데이터는 1 이상의 블록데이터로 이루어지며,

상기 블록데이터는 당해 단말장치에 고유한 장치 키로 암호화되고,

상기 단말장치는 재생시간 길이가 소정 시간 내로 이루어지며 재생 순위가 연속하는 1 이상의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 취득하고, 상기 장치 키를 복호 키로 이용하여 취득한 암호화 블록 데이터 군을 복호하여 블록 데이터 군을 생성하는 블록 복호수단을 더 구비하며,

상기 암호화 수단은, 상기 블록 데이터 군에 포함되는 1 이상의 프레임 데이터 중, 다른 프레임 데이터와 무 의존인 독립 프레임 데이터를 상기 장치 키 및 상기 암호키의 순서로 암호화하고, 다른 프레임 데이터를 상기 장치 키로 암호화함으로써 이중 암호화블록 데이터 군을 생성하며, 상기 암호화블록 데이터 군을 생성한 이중 암호화블록 데이터 군으로 치환하는 것을 특징으로 하는 단말장치.

청구항 26.

오리지널 콘텐츠를 단말장치로부터 휴대형 이동매체에 이동시키는 저작권 보호시스템으로,

상기 단말장치는,

상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과,

상기 오리지널 콘텐츠에 비 가역 변환을 하여 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과,

상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과,

암호키를 이용하여 상기 콘텐츠의 1 블록을 암호화하여 암호화 블록을 생성하고, 상기 1 블록을 상기 암호화 블록으로 치환하는 암호화 수단과,

상기 암호키를 상기 기록매체에 기록하는 키 기록수단과,

상기 암호에 이용된 상기 암호키를 삭제하는 키 삭제수단을 구비하고,

상기 기록매체는 상기 변환콘텐츠를 기억하는 콘텐츠 기억수단을 구비하는 것을 특징으로 하는 저작권 보호시스템.

청구항 27.

오리지널의 콘텐츠를 휴대형 기록매체에 이동시키는 단말장치에 이용되는 콘텐츠 이동방법으로,

상기 단말장치는 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단을 구비하고,

상기 콘텐츠 이동방법은,

상기 오리지널 콘텐츠에 비 가역 변환을 하여 변환콘텐츠를 생성하는 변환콘텐츠 생성스텝과,

상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록스텝과,

암호키를 이용하여 상기 오리지널 콘텐츠의 1 블록을 암호화하여 암호화 블록을 생성하고, 상기 1 블록을 상기 암호화블록으로 치환하는 암호화 스텝과,

상기 암호키를 상기 기록매체에 기록하는 키 기록스텝과,

상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제스텝을 포함하는 것을 특징으로 하는 콘텐츠 이동방법.

청구항 28.

오리지널의 콘텐츠를 휴대형 기록매체에 이동시키는 단말장치에 이용되는 콘텐츠 이동 프로그램으로,

상기 단말장치는 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단을 구비하고,

상기 콘텐츠 이동프로그램은,

상기 오리지널 콘텐츠에 비 가역 변환을 하여 변환콘텐츠를 생성하는 변환콘텐츠 생성스텝과,

상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록스텝과,

암호키를 이용하여 상기 오리지널 콘텐츠의 1 블록을 암호화하여 암호화 블록을 생성하고, 상기 1 블록을 상기 암호화 블록으로 치환하는 암호화 스텝과,

상기 암호키를 상기 기록매체에 기록하는 키 기록스텝과,

상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제스텝을 포함하는 것을 특징으로 하는 콘텐츠 이동 프로그램.

청구항 29.

제 28항에 있어서,

상기 콘텐츠 이동 프로그램은 컴퓨터 판독가능한 기록매체에 기록되어 있는 것을 특징으로 하는 콘텐츠 이동프로그램.

명세서

기술분야

본 발명은 콘텐츠의 부정이용 방지를 목적으로 한 단말장치 및 휴대형 매체(portable medium)를 포함하는 저작권 보호시스템에 관한 것으로, 특히 부정이용을 방지하면서 사용자의 편리성을 향상시킨 기술에 관한 것이다.

배경기술

최근, BS 디지털 방송이나 지상파 디지털 방송의 개시에 동반하여 영화 등의 디지털 콘텐츠가 널리 배송되고 있다. 디지털 콘텐츠(이하, 콘텐츠)는 복제가 용이하므로 인터넷이나 그 밖의 매체를 통한 해적행위 및 복제 콘텐츠의 재 배송 등의 부정행위에 대한 우려가 높아지고 있고, 이들 부정행위에 대항(콘텐츠를 보호)하기 위한 기술개발이 진행되고 있다.

디지털방송 프로그램의 복제방지대책으로, 1회만 녹화가능함을 나타내는 「카피원스(Copy Once)」의 제어신호를 부가하여 암호화하여 방송된다. 이와 같이 「카피원스」의 제어신호가 부가된 디지털방송 프로그램은 CPRM(Content Protection for Recordable Media)에 대응하는 기록재생장치를 이용함으로써 녹화할 수 있다. 녹화된 디지털방송 프로그램은, 다른 기기에 더빙할 수는 없으며, 대응하는 기기에 이동(무브(move))만을 행할 수 있다.

특허문헌 1 : 일본국 특개2003-228522호 공보

비 특허문헌 1 :「현대암호이론」, 이케노 신이치(池野信一), 코야마 켄지(小山謙二), 전자통신학회

비 특허문헌 2 :「암호이론입문」, 오카모토 에이지(岡本榮司), 공립출판주식회사

그러나 디지털방송 프로그램은 데이터량이 많은 고화질 콘텐츠이므로, 이동 처가 메모리카드 등 기억용량이 작은 기기인 경우에는, 기록재생장치는 고화질 콘텐츠를 화상변환에 의해 압축하여 데이터량을 줄인 후에 메모리카드에 이동시킬 필요가 있다.

이 경우, 이동 처의 메모리카드로부터 원래의 기록재생장치로 다시 콘텐츠를 이동시킨 경우에는 이미 화상변환에 의해 원래의 고화질 콘텐츠는 상실되어 있으므로, 기록재생장치는 다시 고화질 콘텐츠를 이용할 수 없다라고 하는 문제가 있다.

발명의 상세한 설명

본 발명은 상기 문제점을 감안하여 이루어진 것으로, 변환을 한 콘텐츠를 다른 기기에 이동한 경우에도, 콘텐츠의 이동 처(move-destination)의 기기로부터 콘텐츠의 이동원(move-source)으로 다시 콘텐츠를 이동시킨 경우에, 변환 전의 콘텐츠를 이용할 수 있는 단말장치, 콘텐츠 보호시스템, 콘텐츠 이동방법 및 콘텐츠 이동 프로그램을 제공하는 것을 목적으로 한다.

상기 목적을 달성하기 위해서 본 발명은, 오리지널의 콘텐츠를 휴대형 기록매체로 이동시키는 단말장치로, 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과, 상기 오리지널 콘텐츠에 비 가역 변환을 하여 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과, 상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과, 암호키를 이용하여 상기 오리지널 콘텐츠의 1의 블록을 암호화하여 암호화 블록을 생성하고, 상기 1의 블록을 상기 암호화 블록으로 치환하는 암호화 수단과, 상기 암호키를 상기 기록매체에 기록하는 키 기록수단과, 상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제수단을 구비하는 것을 특징으로 한다.

상기에 설명한 구성에 의하면, 단말장치는 당해 단말장치에서 기억하고 있는 오리지널 콘텐츠의 1의 블록을 암호키로 암호화하여, 상기 암호키를 기록매체에 기록하고 있으므로, 사용자에 대해서 오리지널 콘텐츠를 이용하지 못하게 할 수 있다.

또, 단말장치는 오리지널 콘텐츠 기억수단에 1의 블록이 암호화된 오리지널 콘텐츠를 기억하고 있으므로, 상기 변환콘텐츠를 상기 기록매체에 이동시킨 후에도 상기 암호키를 상기 기록매체로부터 취득함으로써 변환 전의 상기 오리지널 콘텐츠를 복원할 수 있다.

여기서, 상기 오리지널 콘텐츠는 복수의 블록데이터별로 암호화된 암호화 콘텐츠이고, 상기 블록은 암호화된 블록데이터이며, 상기 변환콘텐츠 생성수단은 상기 암호화 콘텐츠를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 상기 오리지

널 콘텐츠에 상기 비 가역 변환을 하여 변환콘텐츠를 생성하며, 상기 암호화 수단은 상기 암호키를 이용하여 상기 암호화된 블록데이터를 암호화하여 이중 암호화 블록데이터를 상기 암호화 블록으로서 생성하고, 상기 암호화된 블록데이터를 생성한 이중 암호화 블록데이터로 치환해도 된다.

이 구성에 의하면, 단말장치는 암호화된 블록데이터를 이중 암호화하므로, 오리지널 콘텐츠에 대한 시큐어리티(security)를 높일 수 있다.

여기서, 상기 암호화 수단은 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하여, 암호화된 블록데이터별로 이중 암호화 블록데이터로 치환해도 된다.

이 구성에 의하면, 단말장치는 모든 암호화된 블록데이터를 이중 암호화할 수 있다.

여기서, 상기 암호화 수단은 암호화된 모든 블록데이터의 각각에 대해서 다른 암호키를 생성하고, 암호화된 블록데이터별로 각각에 대해서 생성된 암호키를 이용하여 이중 암호화 블록데이터를 생성하고, 상기 키 기록수단은 상기 암호화수단에서 생성된 모든 암호키를 상기 기록매체에 기록하는 것으로 해도 된다.

이 구성에 의하면, 단말장치는 모든 암호화된 블록데이터의 각각에 대해 다른 암호키를 이용하여 암호화하여 이중 암호화 블록데이터를 생성한다. 이에 따라, 악의의 제 3자는 블록데이터를 암호화하기 위한 키와 암호화된 블록데이터별로 대응하는 암호키 모두를 입수하지 않는 한은 오리지널 콘텐츠를 취득할 수 없으므로, 콘텐츠에 대한 시큐어리티는 향상된다.

여기서, 상기 암호화 수단은 암호화된 블록데이터의 개수 미만인 소정의 개수의 암호키를 생성하고, 생성한 각 암호키를 주기적으로 이용하여 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하고, 상기 키 기록수단은 상기 암호화 수단에서 생성된 상기 고정의 개수의 암호키를 상기 기록매체에 기록해도 된다.

이 구성에 의하면, 단말장치는 소정의 개수의 암호키 각각을 주기적으로 이용하여 암호화된 데이터블록별로 이중 암호화 블록데이터를 생성하며, 소정의 개수의 암호키를 기록매체에 기록하므로, 기록매체에 기록하는 암호키의 개수를 경감할 수 있다.

여기서, 상기 복수의 암호화된 블록데이터는 재생 순위에 따라서 기억되어 있고, 상기 암호화 수단은 일 방향성 함수를 미리 기억하고 있는 함수기억부와, 키 데이터를 생성하는 제 1 키 생성부와, 상기 키 데이터에 상기 암호화된 블록데이터의 재생 순위에 의거한 횟수 분, 상기 일 방향성 함수를 실시하여 상기 암호화된 블록데이터에 대한 순위 암호키를 생성하는 제 2 키 생성부와, 암호화된 블록데이터를 상기 제 2 키 생성부에서 생성한 순위 암호키를 상기 암호키로 이용하여 암호화하여 이중 암호화 블록데이터를 생성하는 암호화블록 생성부와, 상기 암호화된 블록데이터를 상기 이중 암호화블록 생성부에서 생성된 상기 이중 암호화 블록으로 치환하는 블록 치환부를 구비하고, 상기 키 기록수단은 제 1 키 생성부에서 생성된 키 데이터를 상기 기록매체에 기록하는 것으로 해도 된다.

이 구성에 의하면, 단말장치는 기록매체에 기록하는 암호키로 키 데이터만을 기록하므로, 기록매체에 기록하는 암호키의 개수를 경감할 수 있다.

여기서, 상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 암호화하여 암호화 변환콘텐츠를 더 생성하고, 상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 상기 기록매체에 기록하는 대신, 생성한 상기 암호화 변환콘텐츠와 상기 암호화 변환콘텐츠를 복호하는 복호 키 정보를 상기 기록매체에 기록하는 것으로 해도 된다.

이 구성에 의하면, 단말장치는 기록매체에 암호화 변환콘텐츠를 기록하므로 변환콘텐츠에 대한 시큐어리티가 높아진다.

여기서, 상기 변환콘텐츠 기록수단은 상기 변환콘텐츠에 포함되는 복수의 변환블록별로 암호화하여 암호화 변환블록을 생성하고, 생성된 복수의 암호화 변환블록별로 상기 기록매체에 기록함으로써, 상기 암호화 변환콘텐츠의 생성 및 기록을 행해도 된다.

이 구성에 의하면, 단말장치는 변환블록별로 암호화 변환블록을 생성하고, 생성한 암호화 변환블록별로 기록매체에 기록한다. 이에 따라 단말장치는 1의 암호화 변환블록을 기록하는 도중에 기록에 실패한 경우에도, 기록에 실패한 1의 암호화 변환블록에서부터 다시 처리를 행할 수 있다.

여기서, 상기 암호화 변환콘텐츠와 상기 복호 키 정보를 상기 기록매체에 기록하고, 상기 블록을 상기 암호화 블록으로 치환한 후의 단말장치로, 당해 단말장치는 상기 기록매체에 기록되어 있는 상기 암호화 변환콘텐츠 및 상기 복호 키 정보의 소거에 관한 제어를 행하는 변환콘텐츠 소거수단과, 상기 변환콘텐츠 소거수단에서 소거에 관한 제어가 이루어진 후, 상기 기록매체로부터 상기 암호키를 판독하고, 판독한 상기 암호키를 복호 키로 이용하여 상기 이중 암호화 블록데이터를 복호하여 상기 암호화된 블록데이터를 생성하고, 상기 이중 암호화 블록데이터를 생성한 상기 암호화된 블록데이터에 재기록하는 복호수단을 구비해도 된다.

이 구성에 의하면, 단말장치는 상기 암호화 변환콘텐츠 및 상기 복호 키 정보의 소거에 관한 제어를 행하고, 그 후에, 상기 이중 암호화 블록데이터를 복호하여 상기 암호화된 블록데이터를 생성하며, 상기 이중 암호화 블록데이터를 생성한 상기 암호화된 블록데이터에 재기록하므로, 변환콘텐츠로 변환하기 전의 오리지널 콘텐츠를 복호 할 수 있다.

여기서, 상기 단말장치는 상기 오리지널 콘텐츠를 재생하는 재생수단을 더 구비하고, 상기 복호수단은 상기 모든 암호화된 블록데이터를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성된 상기 오리지널 콘텐츠를 상기 재생수단에 출력해도 된다.

이 구성에 의하면, 단말장치는 모든 암호화된 데이터블록을 복호 하여 상기 오리지널 콘텐츠를 생성하고, 상기 오리지널 콘텐츠를 재생할 수 있다.

여기서, 상기 오리지널 콘텐츠는 복수의 블록데이터마다 암호화된 암호화 콘텐츠이고, 상기 오리지널 콘텐츠 기억수단은 상기 복수의 암호화된 블록데이터를 재생 순위에 따라서 기억하고 있고, 상기 변환콘텐츠 생성수단은 상기 암호화 콘텐츠를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성된 상기 오리지널 콘텐츠에 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하고, 상기 암호화수단은 재생시간 길이가 소정 시간 내가 되도록 재생 순위가 연속하는 복수의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 상기 블록으로 취득하고, 취득한 암호화블록 데이터 군에 상기 암호키를 이용하여 암호화하여 이중 암호화블록 데이터 군을 상기 암호화 블록으로 생성하고, 상기 암호화블록 데이터 군을 생성한 상기 이중 암호화블록 데이터 군으로 치환하는 것으로 해도 된다.

이 구성에 의하면, 단말장치는 재생시간 길이가 소정 시간 내인 암호화블록 데이터 군을 암호화 키를 이용하여 암호화하여 이중 암호화블록 데이터 군을 생성하고, 상기 암호화블록 데이터 군을 생성한 이중 암호화블록 데이터 군으로 치환할 수 있다. 이에 따라, 1의 암호화된 블록데이터를 이중 암호화하는 경우에 비하여 이중 암호화하는 데이터량이 많으므로 시큐어리티가 향상된다.

여기서, 상기 오리지널 콘텐츠는 동화상이 압축 부호화된 복수의 프레임 데이터로 이루어지고, 상기 프레임 데이터는 1 이상의 블록데이터로 이루어지며, 상기 블록데이터는 당해 단말장치에 고유의 장치 키로 암호화되고, 상기 단말장치는 재생시간 길이가 소정 시간 내로 이루어지고, 재생 순위가 연속하는 1 이상의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 취득하고, 상기 장치 키를 복호 키로 이용하여 취득한 암호화블록 데이터 군을 복호하여 블록데이터 군을 생성하는 블록 복호수단을 더 구비하고, 상기 암호화수단은 상기 블록데이터 군에 포함되는 1 이상의 프레임 데이터 중, 다른 프레임 데이터와 무 의존인 독립 프레임 데이터를 상기 장치 키, 상기 암호키의 순서로 암호화 및 다른 프레임 데이터를 상기 장치 치로 암호화함으로써 이중 암호화블록 데이터 군을 생성하고, 상기 암호화블록 데이터 군을 생성한 이중 암호화블록 데이터 군으로 치환해도 된다.

이 구성에 의하면, 단말장치는 독립 프레임을 이중 암호화하고, 다른 프레임을 장치 키만으로 암호화하므로 이중 암호화의 처리를 경감할 수 있다.

여기서, 오리지널 콘텐츠를 휴대형 기록매체에 이동시키는 단말장치로, 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과, 상기 오리지널 콘텐츠에 비 가역 변환이 실시된 변환콘텐츠가 암호화된 비 오리지널 콘텐츠를 기억하고 있는 비 오리지널 콘텐츠 기억수단과, 상기 변환콘텐츠에 포함되고 상기 비 오리지널 콘텐츠의 복호에 이용하는 복호블록 데이터를 상기 오리지널 콘텐츠로부터 취득하는 복호블록 데이터 취득수단과, 상기 비 오리지널 콘텐츠를 상기 복호블록 데이터를 이용하여 복호하여 상기 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과, 상기 변환콘텐츠 생성수단에서 생성된 상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과, 암호키를 이용하여 상기 오리지널 콘텐츠의 1 블록을 암호화하여 암호화 블록을 생성하고, 상기 1 블록을 상기 암호화 블록으로 치환하는 암호화 수단과, 상기 암호키를 상기 기록매체에 기록하는 키 기록수단과, 상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제수단을 구비해도 된다.

이 구성에 의하면, 단말장치는 당해 단말장치에서 기억하고 있는 오리지널 콘텐츠의 1 블록을 암호키로 암호화하여 상기 암호키를 기록매체에 기록하고 있으므로, 사용자에 대해서 오리지널 콘텐츠를 이용하지 못하게 할 수 있다.

또, 단말장치는 오리지널 콘텐츠 기억수단에 1 블록이 암호화된 콘텐츠를 기억하고 있으므로, 상기 변환콘텐츠를 상기 기록매체에 이동시킨 후에도 상기 암호키를 상기 기록매체로부터 취득함으로써 변환 전의 상기 오리지널 콘텐츠를 복원할 수 있다.

또, 단말장치는 변환콘텐츠가 암호화된 비 오리지널 콘텐츠를 미리 기억하고 있으므로 기록매체에 콘텐츠를 이동시킬 때에 오리지널 콘텐츠에 비 가역 변환을 할 필요가 없다. 이에 따라, 콘텐츠 이동시의 처리의 부하를 경감할 수 있다.

여기서, 상기 변환콘텐츠에 포함되는 1 변환블록데이터를 암호키로 이용하여 상기 변환콘텐츠를 암호화함으로써 상기 비 오리지널 콘텐츠는 생성되고, 상기 비 오리지널 콘텐츠가 생성된 후, 상기 암호키는 소거되고, 상기 복호블록 데이터 취득수단은 상기 오리지널 콘텐츠에 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하고, 생성한 상기 변환콘텐츠로부터 상기 1 변환블록 데이터를 상기 복호블록 데이터로 취득해도 된다.

이 구성에 의하면, 단말장치는 비 오리지널 콘텐츠를 복호 할 때, 오리지널 콘텐츠로부터 변환콘텐츠에 포함되는 1 변환블록 데이터를 생성하므로 비 오리지널 콘텐츠를 복호하기 위한 복호 키를 미리 기억해 둘 필요가 없다.

여기서, 상기 오리지널 콘텐츠는 복수의 블록데이터마다 암호화된 암호화 콘텐츠이고, 상기 블록은 암호화된 블록데이터이고, 상기 복호블록데이터 취득수단은 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하여 상기 복호블록 데이터를 취득하는 대신, 상기 1 변환블록 데이터에 대응하는 암호화된 블록데이터를 복호하고, 상기 비 가역 변환을 하여 상기 복호블록 데이터를 취득하고, 상기 암호화 수단은 상기 암호키를 이용하여 상기 암호화된 블록데이터를 암호화하여 이중 암호화 블록데이터를 상기 암호화 블록으로 생성하고, 상기 암호화된 블록데이터를 생성한 이중 암호화 블록데이터로 치환해도 된다.

이 구성에 의하면, 단말장치는 암호화된 블록데이터를 이중 암호화하므로 오리지널 콘텐츠에 대한 시큐어리티를 높일 수 있다.

여기서, 상기 암호화수단은 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하고, 암호화된 블록데이터마다 이중 암호화 블록데이터로 치환해도 된다.

이 구성에 의하면, 단말장치는 모든 암호화된 블록데이터를 이중 암호화할 수 있다.

여기서, 상기 암호화 수단은 암호화된 모든 블록데이터의 각각에 대해서 다른 암호키를 생성하고, 암호화된 블록데이터마다 각각에 대해서 생성된 암호키를 이용하여 이중 암호화 블록데이터를 생성하고, 상기 키 기록수단은 상기 암호화 수단으로 생성된 모든 암호키를 상기 기록매체에 기록해도 된다.

이 구성에 의하면, 단말장치는 모든 암호화된 블록데이터 각각에 대해서 다른 암호키를 이용하여 암호화하여 이중 암호화 블록데이터를 생성한다. 이에 따라, 악의의 제 3자는 블록데이터를 암호화하기 위한 키와 암호화된 블록데이터마다 대응하는 암호키 모두를 입수하지 않는 한은 오리지널 콘텐츠를 취득할 수 없으므로 오리지널 콘텐츠에 대한 시큐어리티는 향상된다.

여기서, 상기 암호화수단은 암호화된 블록데이터의 개수 미만인 소정의 개수의 암호키를 생성하고, 생성한 각 암호키를 주기적으로 이용하여 암호화된 모든 블록데이터마다 이중 암호화 블록데이터를 생성하고, 상기 키 기록수단은 상기 암호화 수단에서 생성된 상기 소정의 개수의 암호키를 상기 기록매체에 기록해도 된다.

이 구성에 의하면, 단말장치는 소정 개수의 암호키 각각을 주기적으로 이용하여 암호화된 데이터 블록마다 이중 암호화 블록데이터를 생성하고, 소정의 개수의 암호키를 기록매체에 기록하므로, 기록매체에 기록하는 암호키의 개수를 경감할 수 있다.

여기서, 상기 복수의 암호화된 블록데이터는 재생 순위에 따라서 기억되어 있고, 상기 암호화수단은 일 방향성 함수를 미리 기억하고 있는 함수기억부와, 키 데이터를 생성하는 제 1 키 생성부와, 상기 키 데이터에 상기 암호화된 블록데이터의 재생 순위에 의거한 횟수 분, 상기 일 방향성 함수를 실시하여 상기 암호화된 블록데이터에 대한 순위 암호키를 생성하는

제 2 키 생성부와, 암호화된 블록데이터를 상기 제 2 키 생성부에서 생성한 순위 암호키를 상기 암호키로 이용하여 암호화하여 이중 암호화 블록데이터를 생성하는 암호화 블록생성부와, 상기 암호화된 블록데이터를 상기 이중 암호화블록 생성부에서 생성된 상기 2중 암호화 블록으로 치환하는 블록 치환부를 구비하고, 상기 키 기록수단은 상기 암호키 대신에 제 1 키 생성부에서 생성된 상기 키 데이터를 상기 기록매체에 기록해도 된다.

이 구성에 의하면, 단말장치는 기록매체에 기록하는 암호키로 키 데이터만을 기록하므로 기록매체에 기록하는 암호키의 개수를 경감할 수 있다.

여기서, 상기 변환콘텐츠 기록수단은 또 상기 변환콘텐츠를 암호화하여 암호화 변환콘텐츠를 생성하고, 상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 상기 기록매체에 기록하는 대신, 생성한 상기 암호화 변환콘텐츠와, 상기 암호화 변환콘텐츠를 복호하는 복호 키 정보를 상기 기록매체에 기록해도 된다.

이 구성에 의하면, 단말장치는 기록매체에 암호화 변환콘텐츠를 기록하므로 변환콘텐츠에 대한 시큐어리티가 높아진다.

여기서, 상기 비 오리지널 콘텐츠 기억수단은 상기 1 변환블록 데이터를 암호키로 이용하여 상기 변환콘텐츠를 상기 복수의 변환블록별로 암호화하여 기억하고 있고, 상기 변환콘텐츠 기록수단은 상기 암호화된 변환블록별로 복호하여 상기 변환블록을 생성하는 제 1 생성부와, 상기 제 1생성부에서 생성된 변환블록별로 암호화하여 재 암호화 변환블록을 생성하는 제 2생성부와, 상기 제 2생성부에서 생성된 재 암호화 변환블록별로 상기 기록매체에 기록하는 기록부를 구비해도 된다.

이 구성에 의하면, 단말장치는 변환블록별로 암호화 변환블록을 생성하고, 생성한 암호화 변환블록별로 기록매체에 기록한다. 이에 따라, 단말장치는 1 암호화 변환블록을 기록하는 도중에 기록에 실패한 경우에도 기록에 실패한 1 암호화 변환블록에서부터 다시 처리를 할 수 있다.

여기서, 상기 암호화 변환콘텐츠와 상기 복호 키 정보를 상기 기록매체에 기록하고, 상기 블록을 상기 암호화 블록으로 치환한 후의 단말장치로, 당해 단말장치는 상기 기록매체에 기록되어 있는 상기 암호화 변환콘텐츠 및 상기 복호 키 정보의 소거에 관한 제어를 행하는 변환콘텐츠 소거수단과, 상기 변환콘텐츠 소거수단에서 소거에 관한 제어가 이루어진 후, 상기 기록매체로부터 상기 암호키를 판독하고, 판독한 상기 암호키를 복호 키로 이용하여 상기 이중 암호화 블록데이터를 복호하여 상기 암호화된 블록데이터를 생성하고, 상기 이중 암호화 블록데이터를 생성한 상기 암호화된 블록데이터에 재기록하는 복호수단을 더 구비해도 된다.

이 구성에 의하면, 단말장치는 상기 암호화 변환콘텐츠 및 상기 복호 키 정보의 소거에 관한 제어를 실행하고, 그 후에, 상기 이중 암호화 블록데이터를 복호하여 상기 암호화된 블록데이터를 생성하며, 상기 이중 암호화 블록데이터를 생성한 상기 암호화된 블록데이터에 재기록하므로, 변환콘텐츠로 변환하기 전의 오리지널 콘텐츠를 복호 할 수 있다.

여기서, 상기 단말장치는 상기 오리지널 콘텐츠를 재생하는 재생수단을 더 구비하고, 상기 복호수단은 상기 모든 암호화된 블록데이터를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 상기 오리지널 콘텐츠를 상기 재생수단에 출력해도 된다.

이 구성에 의하면, 단말장치는 모든 암호화된 데이터블록을 복호 하여 상기 오리지널 콘텐츠를 생성하고, 상기 오리지널 콘텐츠를 재생할 수 있다.

여기서, 상기 오리지널 콘텐츠는 다수의 블록데이터별로 암호화된 암호화 콘텐츠이고, 상기 오리지널 콘텐츠 기억수단은 상기 복수의 암호화된 블록데이터를 재생 순위에 따라서 기억하고 있고, 상기 암호화 수단은 재생시간 길이가 소정 시간 내가 되도록 재생 순위가 연속하는 복수의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 상기 블록으로 취득하고, 취득한 암호화블록 데이터 군에 상기 암호키를 이용하여 암호화하여, 이중 암호화블록 데이터 군을 상기 암호화 블록으로 생성하고, 상기 암호화블록 데이터 군을 생성한 상기 이중 암호화블록 데이터 군으로 치환해도 된다.

이 구성에 의하면, 단말장치는 재생시간 길이가 소정 시간 내인 암호화블록 데이터 군을 암호화 키를 이용하여 암호화하여 이중 암호화블록 데이터 군을 생성하고, 상기 암호화블록 데이터 군을 생성한 이중 암호화블록 데이터 군으로 치환할 수 있다. 이에 따라 1 암호화된 블록데이터를 이중 암호화하는 경우에 비하여 이중 암호화하는 데이터량이 많으므로 시큐어리티가 향상된다.

여기서, 상기 오리지널 콘텐츠는 동화상이 압축 부호화된 복수의 프레임 데이터로 이루어지고, 상기 프레임 데이터는 1 이상의 블록데이터로 이루어지고, 상기 블록데이터는 당해 단말장치에 고유의 장치 키로 암호화되고, 상기 단말장치는 재생

시간 길이가 소정 시간 내로 이루어지고, 재생 순위가 연속하는 1 이상의 암호화된 블록데이터를 포함하는 암호화블록 데이터 군을 취득하고, 상기 장치 키를 복호 키로 이용하여 취득한 암호화블록 데이터 군을 복호하여 블록데이터 군을 생성하는 블록 복호수단을 더 구비하고, 상기 암호화 수단은 상기 블록데이터 군에 포함되는 1 이상의 프레임 데이터 중, 다른 프레임 데이터와 무 의존인 독립 프레임 데이터를 상기 장치 키, 상기 암호키의 순서로 암호화 및 다른 프레임 데이터를 상기 장치 키로 암호화함으로써, 이중 암호화블록 데이터 군을 생성하고, 상기 암호화블록 데이터 군을 생성한 이중 암호화블록 데이터 군으로 치환해도 된다.

이 구성에 의하면, 단말장치는 독립 프레임을 이중 암호화하고, 다른 프레임을 장치 키만으로 암호화하므로 이중 암호화의 처리를 경감할 수 있다.

또, 본 발명은 오리지널 콘텐츠를 단말장치로부터 휴대형 기록매체에 이동시키는 저작권 보호시스템으로, 상기 단말장치는 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과, 상기 오리지널 콘텐츠에 비 가역 변환을 하여 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과, 상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과, 암호키를 이용하여 상기 콘텐츠의 1 블록을 암호화하여 암호화블록을 생성하고, 상기 1 블록을 상기 암호화블록으로 치환하는 암호화 수단과, 상기 암호키를 상기 기록매체에 기록하는 키 기록수단과, 상기 암호에 이용된 상기 암호키를 삭제하는 키 삭제수단을 구비하고, 상기 기록매체는 상기 변환콘텐츠를 기억하는 콘텐츠 기억수단을 구비하는 것을 특징으로 한다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 당해 단말장치에서 기억하고 있는 오리지널 콘텐츠의 1 블록을 암호키로 암호화하고, 상기 암호키를 기록매체에 기록하고 있으므로, 사용자에 대해서 오리지널 콘텐츠를 이용하지 못하게 할 수 있다.

또, 저작권 보호시스템의 단말장치는 오리지널 콘텐츠 기억수단에 1 블록이 암호화된 오리지널 콘텐츠를 기억하고 있으므로, 상기 변환콘텐츠를 상기 기록매체에 이동시킨 후에도 상기 암호키를 상기 기록매체로부터 취득함으로써 변환 전의 상기 오리지널 콘텐츠를 복원할 수 있다.

실시예

1. 제 1 실시 예

이하, 본 발명에 관한 제 1 실시 예로서의 저작권 보호시스템(1)에 대해서 도면을 참조하여 설명한다.

1. 1 저작권 보호시스템(1)의 개요

저작권 보호시스템(1)은, 도 1에 도시한 바와 같이, 기록재생장치(10), 콘텐츠 공급장치(11), 모니터(12), 스피커(13), 휴대형 기록매체(20)(이하, 「휴대형 매체」라고 한다) 및 휴대정보 단말(30)로 구성되어 있다.

콘텐츠 공급장치(11)는 방송국에 설치되어 있고, 디지털방송 프로그램인 콘텐츠를 방송함으로써 콘텐츠를 공급한다.

기록재생장치(10)는 콘텐츠 공급장치(11)로부터 방송된 콘텐츠를 수신하고, 수신한 콘텐츠를 기록 및 재생한다. 또, 기록재생장치(10)는 기록되어 있는 콘텐츠를 휴대형 매체(20)에 무브(이동)하고, 또, 휴대형 매체(20)에 기록되어 있는 콘텐츠를 다시 당해 기록재생장치(10)에 무브한다.

휴대정보 단말(30)은 휴대형 매체(20)에 무브된 콘텐츠를 재생한다.

모니터(12) 및 스피커(13)는 기록재생장치(10)와 접속되어 있다.

기록재생장치(10)는 콘텐츠 공급장치(11)로부터 콘텐츠를 수신하여 기록할 때, 당해 콘텐츠를 암호화하여, 예를 들어 내장 HDD에 기록한다. 그리고 당해 콘텐츠를 이동할 때는 이동 처가 되는 휴대형 매체(20)가 정규의 휴대형 매체인지 여부를 확인(인증)한 후에 콘텐츠의 이동을 실행한다. 또, 상기 기록재생장치(10)는, 콘텐츠의 이동이 완료한 후에, 내부에 기록한 콘텐츠를 이용할 수 없는 상태로 한다. 여기서 인증기술은, 예를 들어 CPRM SD(Content Protection for Recordable Media Specification SD Memory Card Book) 규격에서 정해진 순서에 따르거나, 또는, 비 특허문헌 1 및 비 특허문헌 2에 개시된 공지의 임의의 기술로 실현 가능하므로 그 상세한 내용에 대해서는 여기서 언급하지 않는다.

1. 2 콘텐츠 공급장치(11)

콘텐츠 공급장치(11)는 방송국에 구비되어 있고, MPEG(Moving Picture Experts Group phase)-2 규격에 따라서 압축 부호화된 트랜스 포트 스트림인 콘텐츠를 방송한다. 콘텐츠 공급장치(11)로부터 방송된 콘텐츠는 기록재생장치(10)의 안테나에 의해 수신된다.

1. 3 기록재생장치(10)

기록재생장치(10)는, 도 2에 도시한 바와 같이, 콘텐츠 수신부(101), 장치기록 키 기억부(102), 제 1 암호화부(103), 암호화 콘텐츠 기록부(104), 재생부(105), 매체기록 키 생성부(106), 매체기록 키 기억부(107), 제 1 복호부(108), 암호화 콘텐츠 판독부(109), 변환부(110), 제 2 암호화부(111), 이중 암호키 생성부(112), 이중 암호키 기억부(113), 이중 암호화부(114), 이중 암호화 콘텐츠 기록부(115), 제 2 복호부(116), 기록/판독부(117) 및 입력부(118)로 구성된다.

기록재생장치(10)는 마이크로 프로세서, ROM, RAM, 하드디스크 유닛 등을 구비하는 컴퓨터 시스템이다. 상기 ROM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서는 상기 컴퓨터 프로그램에 따라서 동작함으로써 기록재생장치(10)는 그 기능을 달성한다.

여기서, 기록재생장치(10)는 구체 예로서 하드디스크 리코더이다.

(1) 콘텐츠 수신부(101)

콘텐츠 수신부(101)는 안테나를 포함하며, 콘텐츠 공급장치(11)로부터 방송된 콘텐츠를 안테나를 통해서 수신하고, 수신한 콘텐츠를 제 1 암호화부(103)에 출력한다. 또, 콘텐츠 수신부(101)가 수신하는 콘텐츠는 MPEG-2 규격에 따라서 압축 부호화된 고화질 콘텐츠이다.

(2) 장치기록 키 기억부(102)

장치기록 키 기억부(102)는 미리 내부에 장치기록 키 K1을 기억하고 있다.

장치기록 키 K1은 콘텐츠 수신부(101)가 콘텐츠 공급장치(11)로부터 수신한 콘텐츠를 제 1 암호화부(103)가 암호화할 때 암호키로 이용되고, 암호화된 콘텐츠를 복호 할 때 복호 키로 이용된다.

장치기록 키 K1은, 예를 들어 128비트의 데이터이다.

(3) 제 1 암호화부(103)

제 1 암호화부(103)는 콘텐츠 수신부(101)로부터 콘텐츠를 수신한다. 여기서 제 1 암호화부(103)가 수신하는 콘텐츠는 고화질인 MPEG-2 콘텐츠이고, 후에 설명하는 MPEG-4 콘텐츠와 구별하기 위해서 「C2」로 표기한다.

제 1 암호화부(103)는 재생시간 길이가 소정 시간 내(예를 들어 45초 이내)가 되는 데이터 사이즈(예를 들어 128비트)의 블록데이터를 콘텐츠 C2의 선두로부터 순차 판독한다. 이후, 블록데이터를 부분콘텐츠라고 부르고, 판독한 부분콘텐츠를 각각 C2[1], C2[2], C2[3],…, C2[N]이라고 표기한다. 부분콘텐츠C2[n](n = 1, 2, …, N이다. 이하 동일)의 재생시간 길이는 소정 시간 내(45초 이내)이다.

또, 제 1 암호화부(103)는 장치기록 키 기억부(102)로부터 장치기록 키 K1을 판독하고, 부분콘텐츠 C2[n]의 각각에 대해서 장치기록 키 K1을 암호키로 이용하여 암호화 알고리즘 E1을 실시하여 암호화 부분콘텐츠 EC2[n]을 생성한다. 즉, EC2[n] = E1(C2[n], K1)이다. 또, 제 1 암호화부(103)가 이용하는 암호화 알고리즘 E1의 일 예는 AES(Advanced Encryption Standard)이다. 또, AES는 공지이므로 설명은 생략한다. 여기서는 암호화하는 데이터 길이를 재생시간 길이가 소정 시간 내(예를 들어 45초 이내)가 되는 데이터 사이즈로 하고 있다.

제 1 암호화부(103)는 생성한 암호화 부분콘텐츠 EC2[1], EC2[2],…, EC2[N]을 암호화 콘텐츠 기록부(104)에 저장한다.

(4) 암호화 콘텐츠 기록부(104)

암호화 콘텐츠 기록부(104)는 구체적으로는 하드디스크 유닛이며, 암호화 콘텐츠를 기억하기 위한 영역을 갖는다.

암호화 콘텐츠 기록부(104)는 제 1 암호화부(103)로부터 암호화 부분콘텐츠 EC2[n]을 수신하면, 수신한 암호화 부분콘텐츠 EC2[n]을 순차 저장한다. 또, 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[N]으로 이루어지는 데이터를 암호화 콘텐츠 EC2로 표기한다.

도 3에 도시한 바와 같이, 암호화 콘텐츠 기록부(104)는 암호화 콘텐츠 $EC2_1$, $EC2_2$, $EC2_3$, … 을 저장하고 있다. 첨자의 수치는 단지 복수의 암호화 콘텐츠를 식별하기 위한 정보이다. 각 암호화 콘텐츠 EC2에는 각 암호화 콘텐츠를 고유하게 식별하기 위한 정보인 콘텐츠 ID가 할당되어 있고, 암호화 콘텐츠 기록부(104)는 암호화 콘텐츠와 콘텐츠 ID를 대응시켜 기억하고 있다. 구체적으로는, EC21의 콘텐츠 ID는 「CID_1」, EC22의 콘텐츠 ID는 「CID_2」, EC23의 콘텐츠 ID는 「CID_3」이다.

(5) 재생부(105)

재생부(105)는 입력부(118)로부터 콘텐츠의 지정 및 재생지시를 수신하고, 수신한 지시를 제 1 복호부(108)에 출력한다.

재생부(105)는 구체적으로는 MPEG 디코더 등을 포함하며, 제 1 복호부(108)에 의해 복호 된 콘텐츠 C2를 수신하고, 수신한 콘텐츠 C2를 디코드하여 영상신호와 음성신호를 생성한다. 재생부(105)는 생성한 영상신호를 모니터(12)에 출력하고, 생성한 음성신호를 스피커(13)에 출력한다.

(6) 매체기록 키 생성부(106)

매체기록 키 생성부(106)는 난수 생성기 등으로 구성되어 있다.

매체기록 키 생성부(106)는 입력부(118)로부터 콘텐츠의 지정과 지정된 콘텐츠의 무브 명령을 포함하는 무브 지시를 수신하면, 매체기록 키 K2를 생성한다. 매체기록 키 K2는 암호화 및 복호의 양쪽에 이용되는 128비트의 데이터이다. 매체기록 키 생성부(106)는 생성한 매체기록 키 K2와 수신한 무브 지시를 매체기록 키 기억부(107)에 출력한다.

또, 매체기록 키 생성부(106)는, 매체기록 키 K2와 수신한 지시를 출력한 후, 생성한 매체기록 키 K2를 당해 매체기록 키 생성부(106)로부터 소거한다.

또, 수신하는 무브 지시에 포함되는 콘텐츠의 지정은 구체적으로는 콘텐츠 ID이다.

(7) 매체기록 키 기억부(107)

매체기록 키 기억부(107)는 매체기록 키 K2를 기억하는 키 기억영역과 디바이스 키 DK1을 가지고 있다.

매체기록 키 기억부(107)는 매체기록 키 생성부(106)로부터 매체기록 키 K2와 무브 지시를 수신하면, 수신한 K2를 내부의 키 기억영역에 저장한다. 또, 매체기록 키 기억부(107)는 수신한 무브 지시에 포함되는 콘텐츠 ID를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록한다.

매체기록 키 기억부(107)는 휴대형 매체(20)로부터 기록/판독부(117)를 거쳐서 휴대형 매체(20)를 식별하는 매체 ID와 MKB(Media Key Block)를 판독하고, 판독한 매체ID와 MKB와, 미리 기억하고 있는 디바이스 키 DK1을 이용하여 매체 고유 키 K0을 생성하고, 생성한 매체 고유 키 K0을 이용하여 매체기록 키 K2를 암호화하여 암호화 매체기록 키 EK2를 생성한다. 여기서 매체 고유 키 K0의 생성 및 암호화 매체기록 키 EK2의 생성은 CPRM 규격에 의거하여 행해진다.

매체기록 키 기억부(107)는 생성한 암호화 매체기록 키 EK2를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록하고, 기록완료 후, 생성한 암호화 매체기록 키 EK2를 소거한다.

매체기록 키 기억부(107)는 수신한 무브 지시를 제 1 복호부(108)에 출력한다.

매체기록 키 기억부(107)는 제 1 복호부(108)로부터 암호화 부분콘텐츠의 판독에 실패하였다는 취지의 명령을 수신하면, 키 기억영역에서 기억하고 있는 매체기록 키 K2를 소거한다.

(8) 제 1 복호부(108)

제 1 복호부(108)는 매체기록 키 기억부(107)로부터 무브 지시를 수신하면 장치기록 키 K1을 판독한다.

제 1 복호부(108)는 암호화 콘텐츠 기록부(104)로부터 지정의 암호화 콘텐츠를 판독하는 판독지시를 암호화 콘텐츠 판독부(109)에 출력한다. 여기서 판독지시의 구체 예는 무브 지시에 포함되는 콘텐츠 ID이다.

제 1 복호부(108)는 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[N]을 순차 수신한다.

제 1 복호부(108)는 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 EC2[n]을 수신하면, 수신한 EC2[n]을 판독한 장치기록 키 K1을 복호 키로 이용하여 복호 알고리즘 D1을 실시하여 부분콘텐츠 C2[n]을 생성한다. 즉, C2[n] = D1(EC2[n], K1)이다. 또, 복호 알고리즘 D1은 암호화 알고리즘 E1에서 암호화된 암호문을 평문으로 변환하기 위한 알고리즘이다.

제 1 복호부(108)는 생성한 부분콘텐츠 C2[n]을 변환부(110)에 출력한다.

제 1 복호부(108)는 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠의 판독에 실패하였다는 취지의 명령을 수신하면, 수신한 명령을 매체기록 키 기억부(107)에 출력한다.

제 1 복호부(108)는 이중 암호화 콘텐츠 기록부(115)로부터 기억하고 있는 내용을 소거하는 제 1 소거지시를 수신하면 복호 된 C2[n]을 소거한다.

이에 따라, 제 1 복호부(108)는 부분콘텐츠 C2[1], C2[2], …, C2[N]을 변환부(110)에 순차 출력할 수 있다.

이하에 구체 예를 설명한다. 제 1 복호부(108)는 콘텐츠의 지정으로 콘텐츠 ID 「CID_1」을 수신하면, 콘텐츠 ID 「CID_1」을 판독지시로 암호화 콘텐츠 판독부(109)에 출력한다. 제 1 복호부(108)는 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 $EC2_{1[}1]$, $EC2_{1[}2]$,…, $EC2_{1[}N]$을 순차 수신하여 부분콘텐츠 $C2_{1[}1]$, $C2_{1[}2]$,…, $C2_{1[}N]$을 순차 생성한다. 제 1 복호부(108)는 생성한 부분콘텐츠 $C2_{1[}1]$, $C2_{1[}2]$,…, $C2_{1[}N]$을 변환부(110)에 순차 출력한다.

또, 제 1 복호부(108)는 콘텐츠의 재생시에 재생부(105)로부터 지시를 수신하면, 암호화 콘텐츠 판독부(109)를 거쳐서 암호화 콘텐츠 기록부(104)로부터 판독한 암호화 콘텐츠 EC2를 장치기록 키 K1을 이용하여 복호하고, 복호 한 콘텐츠 C2를 재생부(105)에 출력한다.

(9) 암호화 콘텐츠 판독부(109)

암호화 콘텐츠 판독부(109)는 제 1 복호부(108)로부터 판독지시를 수신하면, 지정된 암호화 콘텐츠를 판독한다. 또, 수신한 판독지시를 일시 기억한다. 구체적으로는, 제 1 복호부(108)로부터 콘텐츠 ID를 수신하고, 수신한 콘텐츠 ID와 일치하는 콘텐츠 ID를 갖는 암호화 부분콘텐츠 EC2[1], EC2[2],…, EC2[N]을 암호화 콘텐츠 기록부(104)로부터 순차 판독한다. 암호화 콘텐츠 판독부(109)는 EC2[1], EC2[2],…, EC2[N]을 제 1 복호부(108)에 순차 출력한다.

암호화 콘텐츠 판독부(109)는 이중 암호화 콘텐츠 기록부(115)로부터 제 1 소거지시를 수신하면, 암호화 콘텐츠 기록부(104)로부터 판독한 암호화 부분콘텐츠 EC2[n]을 소거한다.

이하에 구체적인 동작에 대해서 설명한다.

암호화 콘텐츠 판독부(109)는 카운터 n을 가지고 있다.

암호화 콘텐츠 판독부(109)는 제 1 복호부(108)로부터 판독지시를 수신하면, 카운터 n에 1을 설정한다.

암호화 콘텐츠 판독부(109)는 지정된 암호화 콘텐츠의 n번째의 암호화 부분콘텐츠 EC2[n]을 판독한다.

암호화 콘텐츠 판독부(109)는 암호화 부분콘텐츠 EC2[n]의 판독에 성공하였는지 여부를 판단한다.

성공하였다고 판단하는 경우에는, 암호화 콘텐츠 판독부(109)는 판독한 암호화 부분콘텐츠 EC2[n]을 일시 기억하는 동시에 제 1 복호부(108)에 출력한다. 암호화 콘텐츠 판독부(109)는 카운터 n에 1을 가산하고, 가산결과를 다시 n으로 하며, 암호화 부분콘텐츠 EC2[n]을 판독하고, 판독에 성공하였는가 여부의 판단을 다시 행한다.

실패하였다고 판단하는 경우에는, 암호화 콘텐츠 판독부(109)는 판독에 실패하였다는 취지의 명령을 제 1 복호부(108)에 출력한다.

예를 들어, 카운터 n의 값이 N+ 1인 경우에는 암호화 부분콘텐츠 EC2[n+ 1]은 존재하지 않으므로 암호화 부분콘텐츠의 판독에는 실패한다. 이에 따라, 암호화 콘텐츠 판독부(109)는 통상 카운터 n의 값이 1 이상 n이하인 경우에는 암호화 부분콘텐츠 EC2[n]이 존재하므로 판독에 성공한다. 즉, 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[N]을 순차 판독할 수 있다.

구체 예로, 암호화 콘텐츠 판독부(109)는 암호화 콘텐츠 기록부(104)로부터 콘텐츠 ID「CID_1」에 대응하는 $EC2_{1[}1]$, $EC2_{1[}2]$, …, $EC2_{1[}N]$을 순차 판독하고, 판독한 $EC2_{1[}1]$, $EC2_{1[}2]$, …, $EC2_{1[}N]$을 제 1 복호부(108)에 순차 출력한다.

(10) 변환부(110)

변환부(110)는 구체적으로는 MPEG-2의 데이터를 MPEG-4로 변환하기 위한 다운 컨버터 등으로 구성된다.

변환부(110)는 제 1 복호부(108)로부터 부분콘텐츠 C2[1], C2[2], …, C2[N]을 수신한다.

변환부(110)는 제 1 복호부(108)로부터 부분콘텐츠 C2[n]을 수신하면, 수신한 부분콘텐츠 C2[n]을 MPEG-4로 압축 변환한다. 여기서 MPEG-4로 변환된 부분콘텐츠를 C4[n]으로 표기한다.

변환부(110)는 변환된 부분콘텐츠 C4[n]을 제 2 암호화부(111)에 출력한다.

또, MPEG-2로부터 MPEG-4로의 변환은 공지기술에 의해 실현 가능하므로 설명을 생략한다.

변환부(110)는 이중 암호화 콘텐츠 기록부(115)에서 제 1 소거지시를 수신하면 변환된 부분콘텐츠 C4[n]을 소거한다.

이에 따라, 변환부(110)는 부분콘텐츠 C4[1], C4[2], …, C4[N]을 제 2 암호화부(111)에 순차 출력할 수 있다.

구체 예로, 변환부(110)는 제 1 복호부(108)로부터 $C2_{1[}1]$, $C2_{1[}2]$, …, $C2_{1}[N]$을 순차 수신하여 $C4_{1[}1]$, $C4_{1[}2]$,…, $C4_{1[}N]$을 순차 생성한다. 변환부(110)는 생성한 부분콘텐츠 $C4_{1[}1]$, $C4_{1[}2]$, …, $C4_{1[}N]$을 순차 제 2 암호화부(111)에 출력한다.

(11) 제 2 암호화부(111)

제 2 암호화부(111)는 변환부(110)로부터 부분콘텐츠 C4[1], C4[2], …, C4[N]을 순차 수신한다.

제 2 암호화부(111)는 변환부(110)로부터 부분콘텐츠 C4[N]을 수신하면, 매체기록 키 기억부(107)에 기억되어 있는 매체기록 키 K2를 판독하고, 판독한 매체기록 키 K2를 암호키로 이용하여 부분콘텐츠 C4[n]에 암호화 알고리즘 E2를 실시하여 암호화 부분콘텐츠 EC4[N]을 생성한다. 즉, EC4[N] = E2(C4[n], K2)이다. 또, 제 2 암호화부(111)가 이용하는 암호화 알고리즘 E2의 일 예는 AES이다.

제 2 암호화부(111)는 암호화 부분콘텐츠 EC4[n]을 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록하고, 내부에 존재하는 암호화 부분콘텐츠 EC4[n]을 소거한다. 이에 따라, 제 2 암호화부(111)는 암호화 부분콘텐츠 EC4[n]을 휴대형 매체(20)에 이동시킬 수 있다.

제 2 암호화부(111)는 암호화 부분콘텐츠 EC2[n]의 암호화에 이용하는 이중 암호키의 생성을 지시하는 생성지시를 이중 암호키 생성부(112)에 출력한다. 생성지시의 구체 예는 이중 암호화하는 암호화 부분콘텐츠의 번호를 나타내는 수치이다. 이중 암호화하는 암호화 부분콘텐츠가 EC2[1]인 경우에는 수치 1이 생성지시가 되고, 이중 암호화하는 암호화 부분콘텐츠가 EC2[2]인 경우에는 수치 2가 생성지시가 된다. 이중 암호화하는 암호화 부분콘텐츠가 EC2[n]인 경우에는 수치 n이 생성지시가 된다.

이에 따라, 제 2 암호화부(111)는 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N]을 휴대형 매체(20)에 순차 기록한다. 즉, 이동시킬 수 있다.

구체 예로서, 제 2 암호화부(111)는 변환부(110)로부터 부분콘텐츠 $C4_{1[}1]$, $C4_{1[}2]$, …, $C4_{1[}N]$을 순차 수신하면, 암호화 부분콘텐츠 $EC4_{1[}1]$, $EC4_{1[}2]$, …, $EC4_{1[}N]$을 순차 생성한다. 제 2 암호화부(111)는 생성한 암호화부분 $EC4_{1[}1]$, $EC4_{1}[2]$, …, $EC4_{1[}N]$을 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 순차 이동시킨다.

(12) 이중 암호키 생성부(112)

이중 암호키 생성부(112)는 난수 생성기 등으로 구성되어 있다.

이중 암호키 생성부(112)는 제 2 암호화부(111)로부터 생성지시인 수치 1, 2, …, N을 순차 수신한다.

이중 암호키 생성부(112)는 생성지시(수치n)를 수신하면, 이중 암호키 K3[n]을 생성한다.

이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록한다. 이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(113)에 출력한다.

또, 이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(113)에 출력한 후, 생성한 이중 암호키 K3[n]을 당해 이중 암호키 생성부(112)에서 소거한다.

여기서, 이중 암호키 생성부(112)는, 이중 암호키 K3[1], K3[2], …, K3[N] 각각이 다른 것이라도 좋고, 일부의 이중 암호키가 일치해도 좋다.

(13) 이중 암호키 기억부(113)

이중 암호키 기억부(113)는 이중 암호키 K3[n]을 기억하는 이중 암호키 기억영역을 구비하고 있다.

이중 암호키 기억부(113)는 이중 암호키 생성부(112)로부터 이중 암호키 K3[1], K3[2], …, K3[N]을 순차 수신한다.

이중 암호키 기억부(113)는 이중 암호키 생성부(112)로부터 이중 암호키 K3[n]을 수신하면, 수신한 이중 암호키 K3[n]을 이중 암호키 기억영역에 저장한다.

이중 암호키 기억부(113)는 암호화 지시를 이중 암호화부(114)에 출력한다. 암호화 지시의 구체 예는 이중 암호화하는 암호화 부분콘텐츠의 번호를 나타내는 수치이다.

(14) 이중 암호화부(114)

이중 암호화부(114)는 이중 암호키 기억부(113)로부터 암호화 지시인 수치 1, 2, …, N을 순차 수신한다.

이중 암호화부(114)는 암호화 지시(수치 n)를 수신하면, 이중 암호키 기억부(113)에 기억되어 있는 이중 암호키 K3[n]을 판독하고, 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 EC2[n]과 판독지시를 판독한다.

이중 암호화부(114)는 이중 암호키 K3[n]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[n]에 암호화 알고리즘 E3을 실시하여 이중 암호화 부분콘텐츠 EEC2[n]을 생성한다. 즉, EEC2[n]= E3(EC2[n], K3[n])이다. 또, 이중 암호화부(114)가 이용하는 암호화 알고리즘 E3의 일 예는 AES이다.

이중 암호화부(114)는 이중 암호화 부분콘텐츠 EEC2[n]을 생성한 후, 장치 내에 존재하는 이중 암호키 K3[n]을 소거한다. 이에 따라 이중 암호화부(114)의 내부에 존재하는 이중 암호키 K3[n] 및 이중 암호키 기억부(113)에 기억되어 있는 이중 암호키 K3[n]은 소거된다.

이중 암호화부(114)는 생성한 이중 암호화 부분콘텐츠 EEC2[n]과 암호화 콘텐츠 판독부(109)로부터 판독한 판독지시를 포함하는 기록지시를 이중 암호화 콘텐츠 기록부(115)에 출력한다. 기록지시의 구체 예는 콘텐츠 ID와 이중 암호화 부분콘텐츠에 대응하는 암호화 부분콘텐츠의 번호를 나타내는 수치를 포함하는 정보이다.

이중 암호화부(114)는 이중 암호화 콘텐츠기록부(115)로부터 제 1 소거지시를 수신하면, 암호화 콘텐츠 판독부(109)로부터 판독한 암호화 콘텐츠 EC2[n]을 소거한다.

이에 따라, 이중 암호화부(114)는 이중 암호화 부분콘텐츠 EEC2[1], EEC2[2], …, EEC2[n]을 순차 생성하여 이중 암호화 콘텐츠 기록부(115)에 순차 출력할 수 있다.

(15) 이중 암호화 콘텐츠 기록부(115)

이중 암호화 콘텐츠 기록부(115)는 이중 암호화부(114)로부터 기록지시와 이중 암호화 부분콘텐츠 EEC2[1], EEC2[2], …, EEC2[N]을 순차 수신한다.

이중 암호화 콘텐츠 기록부(115)는 이중 암호화부(114)로부터 이중 암호화 부분콘텐츠 EEC2[n]을 수신하면, 암호화 콘텐츠 기록부(104)에 기록되고 또한 기록지시에 포함되는 콘텐츠 ID 및 암호화 부분콘텐츠의 번호에 대응하는 EC2[n]을 수신한 EEC2[n]으로 덮어쓰기(overwrite)를 함으로써 암호화 콘텐츠 기록부(104)에 기록한다.

이중 암호화 콘텐츠 기록부(115)는 제 1 복호부(108), 암호화 콘텐츠 판독부(109), 변환부(110) 및 이중 암호화부(114)에 제 1 소거지시를 출력한다.

이때, 암호화 콘텐츠 기록부(104)는 이중 암호화 콘텐츠 EEC2와 콘텐츠 ID를 대응시켜 기억하고 있다.

이에 따라, 이중 암호화 콘텐츠 기록부(115)는 이중 암호화 부분콘텐츠 EEC2[1], EEC2[2], … , EEC2[N]을 암호화 콘텐츠 기록부(104)에 순차 기록할 수 있다.

또, 이중 암호화 부분콘텐츠EEC2[1], EEC2[2], … , EEC2[N]으로 이루어지는 데이터를 이중 암호화 콘텐츠 EEC2로 표기한다.

여기서 구체 예로서 암호화 콘텐츠 $EC2_1$을 이용하여 설명한다.

도 4(a)는 암호화 콘텐츠 $EC2_1$의 데이터 구조를 도시한 도면이다. 즉, 이것은 이중 암호화 부분콘텐츠 $EEC2_1$로 변환되기 전의 상태를 나타낸다.

이중 암호화 콘텐츠 기록부(115)는 이중 암호화부(114)로부터 암호화 부분콘텐츠 $EC2_{1[}1]$이 암호화된 이중 암호화 부분콘텐츠 $EEC2_{1[}1]$과 기록지시를 수신한다. 여기서, 기록지시는 콘텐츠 ID 「CID_1」과, 수치[1]을 포함한다. 이중 암호화 콘텐츠 기록부(115)는 암호화 콘텐츠 기록부(104)에 기록되고 또한 기록지시에 포함되는 콘텐츠 ID 「CID_1」 및 수치[1]에 대응하는 $EC2_{1[}1]$을 수신한 $EEC2_{1[}1]$로 덮어쓰기를 한다. 도 4(b)는 $EC2_{1[}1]$을 $EEC2_{1[}1]$로 덮어쓰기를 한 상태를 나타낸다.

이후, 이중 암호화 콘텐츠 기록부(115)는 기록지시와 이중 암호화 부분콘텐츠$EEC2_{1[}2]$, …, $EEC2_{1[}N]$을 순차 수신하면, 암호화 콘텐츠 기록부(104)에 기억되고 또한 기록지시에 포함되는 콘텐츠 ID 「CID_1」 및 수치[1]에 대응하는 $EC2_1$

[2], …, $EC2_1$[N]을 수신한 $EEC2_1$[2], …, $EEC2_1$[N]으로 순차 덮어쓰기를 한다. 도 4(c)는 암호화 콘텐츠 기록부(104)에 기억되어 있는 암호화 콘텐츠 $EC2_1$의 각 데이터를 이중 암호화 콘텐츠 $EEC2_1$의 각 데이터로 덮어쓰기를 한 상태를 나타낸다.

(16) 제 2 복호부(116)

제 2 복호부(116)는, 입력부(118)로부터 콘텐츠를 무브 백(move back) 하는 지시를 수신하면, 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록되어 있는 콘텐츠 ID를 판독한다. 여기서 무브 백은 휴대형 매체(20)로부터 기록재생장치(10)에 콘텐츠를 이동하는 것을 말한다.

제 2 복호부(116)는 콘텐츠 ID와 암호화 부분콘텐츠와 암호화 매체기록 키의 소거를 지시하는 제 2 소거지시를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 출력한다. 이에 따라, 제 2 복호부(116)는 휴대형 매체(20)의 콘텐츠 ID와 암호화 부분콘텐츠 EC4와 암호화 매체기록 키 EK2를 소거할 수 있다.

제 2 복호부(116)는 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록되어 있는 이중 암호키 K3[1], K3[2], …, K3[N]을 순차 판독한다.

제 2 복호부(116)는 이중 암호키 K3[n]을 판독할 때마다 이하의 동작을 행한다.

제 2 복호부(116)는 판독한 이중 암호키 K3[n]을 복호 키로 이용하여 암호화 콘텐츠 기록부(104)에 기억되어 있는 EEC2[n]에 복호 알고리즘 D3을 실시하여 암호화 부분콘텐츠 EC2[n]을 생성한다. 즉, EC2[n] = D3(EEC2[n], K3[n])이다. 또, 복호 알고리즘 D3은 암호화 알고리즘 E3으로 암호화된 암호문을 평문으로 변환하기 위한 알고리즘이다.

제 2 복호부(116)는 암호화 콘텐츠 기록부(104)에 기억되고 휴대형 매체(20)로부터 판독한 콘텐츠 ID에 대응하는 EEC2[n]을 생성한 암호화 부분콘텐츠 EC2[n]으로 덮어씀으로써 암호화 콘텐츠 기록부(104)에 기록한다. 또, 제 2 복호부(116)는 내부에 존재하는 이중 암호화 부분콘텐츠 EEC2[n]과 이중 암호키 K3[n]을 소거한다.

제 2 복호부(116)는 휴대형 매체(20)에 기록되어 있는 이중 암호키 K3[n]을 소거하는 제 3 소거지시를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 출력한다. 이에 따라, 제 2 복호부(116)는 휴대형 매체(20)의 K3[n]을 소거할 수 있다. 이때, 제 3 소거지시에는 소거하는 이중 암호키를 나타내는 번호가 포함되어 있다. 예를 들어 제 3 소거지시에 번호 「1」이 포함되어 있는 경우에는 소거하는 이중번호 키는 K3[1]이며, 제 3 소거지시에 번호 [n]이 포함되어 있는 경우에는 소거하는 이중 암호키는 K3[n]이다.

이에 따라, 이중 암호화 콘텐츠 EEC2를 암호화 콘텐츠 EC2로 치환할 수 있다.

여기서, 제 2 복호부(116)의 구체적인 동작에 대해서 설명한다.

제 2 복호부(116)는 카운터 n을 가지고 있다.

제 2 복호부(116)는 입력부(118)로부터 무브 백 지시를 수신하면 휴대형 매체(20)로부터 콘텐츠 ID를 판독한다.

제 2 복호부(116)는 제 2 소거지시를 휴대형 매체(20)에 출력함으로써 휴대형 매체(20)의 콘텐츠 ID와 암호화 부분콘텐츠 EC4와 암호화 매체기록 키 EK2를 소거한다. 제 2 복호부(116)는 카운터 n에 1을 설정한다.

제 2 복호부(116)는 휴대형 매체(20)로부터 이중 암호키 K3[n]을 판독한다.

제 2 복호부(116)는 이중 암호키 K3[n]의 판독에 성공하였는지 여부를 판단한다.

성공하였다고 판단하는 경우에는, 제 2 복호부(116)는 암호화 콘텐츠 기록부(104)로부터 판독한 콘텐츠 ID에 대응하는 이중 암호화 부분콘텐츠 EEC2[n]을 판독하고, 이중 암호키 K3[n]을 복호 키로 이용하여 판독한 이중 암호화 부분콘텐츠 EEC2[n]을 복호 하여 암호화 콘텐츠 EC2[n]을 생성한다. 제 2 복호부(116)는 암호화 콘텐츠 기록부(104)에 기억되고 휴대형 매체(20)로부터 판독한 콘텐츠 ID에 대응하는 EEC2[n]을 생성한 암호화 부분콘텐츠 EC2[n]으로 덮어씀으로써 암호화 콘텐츠 기록부(104)에 기록한다.

제 2 복호부(116)는 내부에 존재하는 이중 암호화 부분콘텐츠 EEC2[n]과 이중 암호화 키 K3[n]을 소거한다.

제 2 복호부(116)는 제 3 소거지시를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 출력함으로써 휴대형 매체(20)의 K3[n]을 소거한다.

제 2 복호부(116)는 카운터 n에 1을 가산하고, 가산결과를 다시 n으로 하며, 암호화 부분콘텐츠EC2[n]을 판독하고, 판독에 성공하였는지 여부의 판단을 다시 행한다.

실패하였다고 판단하는 경우에는 제 2 복호부(116)는 처리를 종료한다.

구체 예를 이하에 설명한다.

제 2 복호부(116)는 입력부(118)로부터 무브 백 지시를 수신하면, 휴대형 매체(20)로부터 콘텐츠 ID「CID_1」을 판독한다.

제 2 복호부(116)는 휴대형 매체(20)에 기록되어 있는 콘텐츠 ID「CID_1」, 암호화 부분콘텐츠 $EC4_{1[}1]$, $EC4_{1[}2]$, …, $EC4_{1[}N]$과 암호화 매체기록 키 EK2를 소거한다.

제 2 복호부(116)는 이중 암호키 K3[1], K3[2], …, K3[N]을 순차 판독하고, 판독한 이중 암호키 K3[1], K3[2], …, K3[N]을 이용하여 암호화 부분콘텐츠 $EC2_{1[}1]$, $EC2_{1[}2]$, …, $EC2_{1[}N]$을 순차 생성하여 암호화 콘텐츠 기록부(104)에 순차 기록한다.

(17) 기록/판독부(117)

기록/판독부(117)는 메모리카드 슬롯을 구비하며, 메모리카드 슬롯에 휴대형 매체(20)가 삽입되어 있는 상태에서, 제 2 암호화부(111)로부터 수신하는 암호화 부분콘텐츠EC4[N], 매체기록 키 기억부(107)로부터 수신하는 콘텐츠 ID 및 암호화 매체기록 키 EK2, 및 이중 암호키 생성부(112)로부터 수신하는 이중 암호키 K3[n]을 휴대형 매체(20)에 기록한다. 또, 기록/판독부(117)는 제 2 암호화부(111)로부터 암호화 부분콘텐츠 EC4[n]을 수신할 때마다 순차 휴대형 매체(20)에 기록한다. 또, 기록/판독부(117)는 이중 암호키 생성부(112)로부터 이중 암호키 K3[n]을 수신할 때마다 순차 휴대형 매체(20)에 기록한다. 또, 기록/판독부(117)는 제 2 복호부(116)로부터 수신하는 제 2 소거지시 및 제 3 소거지시를 휴대형 매체(20)에 출력한다.

기록/판독부(117)는 휴대형 매체(20)로부터 콘텐츠 ID를 판독하고, 판독한 콘텐츠 ID를 제 2 복호부(116)에 출력한다. 기록/판독부(117)는 휴대형 매체(20)로부터 이중 암호키 K3[n]을 판독하고, 판독한 이중 암호키 K3[n]을 제 2 복호부(116)에 출력한다. 또, 기록/판독부(117)는 휴대형 매체(20)로부터 이중 암호키 K3[n]을 판독할 때마다 순차 제 2 복호부(116)에 출력한다. 기록/판독부(117)는 휴대형 매체(20)로부터 MKB 및 매체 ID를 판독하고, 판독한 MKB 및 매체 ID를 매체기록 키 기억부(107)에 출력한다.

(18) 입력부(118)

입력부(118)는 사용자로부터의 입력에 의해 지시를 수신하고, 수신한 지시를 재생부(105), 매체기록 키 생성부(106) 및 제 2 복호부(116)에 출력한다. 구체 예로, 입력부(118)는 리모컨과 리모컨 수광부로 구성되어도 된다. 입력부(118)가 수신하는 지시는 재생지시, 무브 지시, 무브 백 지시 등이다.

재생지시는 암호화 콘텐츠 기록부(104)에 기억되어 있는 암호화 콘텐츠를 복호하여 모니터(12) 및 스피커(13)에 출력하는 것을 나타낸다. 무브 지시는 암호화 콘텐츠 기록부(104)에 기억되어 있는 암호화 콘텐츠를 압축 변환하고, 휴대형 매체(20)에 무브하는 것을 나타낸다. 무브 백 지시는 휴대형 매체(20)로부터 기록재생장치(10)에 콘텐츠를 이동하는 것을 나타낸다.

1.4 모니터(12) 및 스피커(13)

모니터(12) 및 스피커(13)는 구체적으로는 기록재생장치(10)와 접속된 디지털 텔레비전이다. 모니터(12)는 재생부(105)로부터 영상신호를 수신하면, 수신한 영상신호를 출력한다. 스피커(13)는 재생부(105)로부터 음성신호를 수신하면, 수신한 음성신호를 출력한다.

1.5 휴대형 매체(20)

휴대형 매체(20)는, 도 5에 도시한 바와 같이, 입출력부(201), 제어부(202) 및 기억부(203)로 구성되고, 기억부(203)는 기록가능영역(204) 및 판독전용영역(205)을 포함한다.

기록가능영역(204)은 암호화 콘텐츠 기억영역(210), 매체기록 키 기억영역(211), 이중 암호키 기억영역(212) 및 콘텐츠 ID 기억영역(213)을 포함하고, 판독전용영역(205)은 휴대형 매체 ID 기억영역(220) 및 MKB 기억영역(221)을 포함한다. 기록가능영역(204)은 데이터의 판독 및 기록이 가능한 영역이다. 판독전용영역(205)은 데이터의 판독만이 가능하고 데이터의 기록이 금지되어 있는 영역이다.

휴대형 매체(20)는 기록재생장치(10) 및 휴대정보 단말(30)의 메모리카드 슬롯에 삽입되어 사용되는 카드형 메모리이다. 휴대형 매체(20)의 구체 예는 SD 메모리카드이다.

휴대형 매체(20)는 기록재생장치(10)의 메모리카드 슬롯에 삽입되어 있는 상태에서 기록재생장치(10)로부터 암호화 콘텐츠가 무브된다. 무브 된 암호화 콘텐츠는 암호화 콘텐츠 기억영역(210)에 저장된다. 암호화 콘텐츠 기억영역(210)에 저장된 암호화 콘텐츠는 휴대형 매체(20)가 휴대정보 단말(30)의 메모리카드 슬롯에 삽입되어 있는 상태에서 휴대정보 단말(30)을 이용하여 재생할 수 있다. 또, 암호화 콘텐츠 기억영역(210)에 저장된 암호화 콘텐츠는 휴대형 매체(20)가 기록재생장치(10)에 장착되어 있는 상태에서 다시 기록재생장치(10)에 무브 할 수 있다.

(1) 입출력부(201)

입출력부(201)는 커넥터 핀, 인터페이스 드라이버 등으로 이루어지고, 휴대형 매체(20)가 삽입되어 있는 장치와의 사이에서 데이터의 입출력을 행하는 인터페이스이다.

이하, 휴대형 매체(20)가 기록재생장치(10)에 삽입되어 있는 상태와 휴대형 매체(20)가 휴대정보 단말(30)에 삽입되어 있는 상태로 나누어 입출력부(201)의 동작에 대해서 설명한다.

(a) 휴대형 매체(20)가 기록재생장치(10)에 삽입되어 있는 상태

입출력부(201)는 기록재생장치(10)의 기록/판독부(117)로부터 콘텐츠 ID, 암호화 부분콘텐츠 EC4[n], 암호화 매체기록 키 EK2, 이중 암호키 K3[n], 제 2 소거지시 및 제 3 소거지시를 수신하고, 수신한 각 데이터를 제어부(202)에 출력한다. 또, 입출력부(201)는 기록/판독부(117)로부터 암호화 부분콘텐츠 EC4[n]을 수신할 때마다 순차 제어부(202)에 출력한다. 입출력부(201)는 기록/판독부(117)로부터 이중 암호키 K3[n]을 수신할 때마다 순차 제어부(202)에 출력한다.

또, 입출력부(201)는 제어부(202)로부터 콘텐츠 ID를 수신하면, 수신한 콘텐츠 ID를 기록/판독부(117)에 출력한다. 입출력부(201)는 제어부(202)로부터 이중 암호키 K3[n]을 수신하면, 기록/판독부(117)에 출력한다. 또, 입출력부(201)는 제어부(202)로부터 이중 암호키 K3[n]을 수신할 때마다 순차 기록/판독부(117)에 출력한다. 입출력부(201)는 제어부(202)로부터 MKB 및 매체 ID를 수신하면 수신한 MKB 및 매체 ID를 기록/판독부(117)에 출력한다.

(b) 휴대형 매체(20)가 휴대정보 단말(30)에 삽입되어 있는 상태

입출력부(201)는 제어부(202)로부터 암호화 매체기록 키 EK2를 수신하고, 수신한 암호화 매체기록 키 EK2를 후술하는 휴대정보 단말(30)의 입출력부(302)에 출력한다. 입출력부(201)는 제어부(202)로부터 암호화 부분콘텐츠 EC4[n]을 수신하면, 수신한 암호화 부분콘텐츠 EC4[n]을 휴대정보 단말(30)의 입출력부(302)에 출력한다. 또, 입출력부(201)는 제어부(202)로부터 암호화 부분콘텐츠 EC4[n]을 수신할 때마다 순차 입출력부(302)에 출력한다. 입출력부(201)는 제어부(202)로부터 MKB 및 매체 ID를 수신하면, 입출력부(302)에 출력한다.

(2) 제어부(202)

이하, 휴대형 매체(20)가 기록재생장치(10)에 삽입되어 있는 상태와 휴대형 매체(20)가 휴대정보 단말(30)에 삽입되어 있는 상태로 나누어 제어부(202)의 동작에 대해서 설명한다.

(a) 휴대형 매체(20)가 기록재생장치(10)에 삽입되어 있는 상태

제어부(202)는 입출력부(201)로부터 수신하는 각 데이터를 기억부(203)의 각각의 영역에 기록한다. 구체적으로는, 제어부(202)는 입출력부(201)로부터 암호화 부분콘텐츠 EC4[n]을 수신할 때마다 순차 암호화 콘텐츠 기억영역(210)에 기록한다. 제어부(202)는 암호화 매체기록 키 EK2를 수신하면, 수신한 EK2를 매체기록 키 기억영역(211)에 기록한다. 제어부(202)는 이중 암호키 K3[n]을 수신할 때마다 순차 이중 암호키 기억영역(212)에 기록한다. 제어부(202)는 콘텐츠 ID를 수신하면, 수신한 콘텐츠 ID를 콘텐츠 ID 기억영역(213)에 기록한다. 제어부(202)는 입출력부(201)로부터 제 2 소거지시를 수신하면 기록가능영역(204)에 기록되어 있는 콘텐츠 ID와 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N]과 암호화 매체기록 키 EK2를 소거한다. 제어부(202)는 입출력부(201)로부터 제 3 소거지시를 수신하면 기록가능영역(204)에 기록되고 또한 제 3 소거지시에 포함되는 번호에 대응하는 이중 암호키 K3[n]을 소거한다.

제어부(202)는 휴대형 매체 ID 및 기억영역(220)에 저장되어 있는 매체 ID 및 MKB 기억영역(221)에 저장되어 있는 MKB를 판독하고, 판독한 매체 ID 및 MKB를 입출력부(201)에 출력한다.

또, 콘텐츠를 기록재생장치(10)에 무브 할 때에는 이하의 동작을 행한다.

제어부(202)는 콘텐츠 ID 기억영역(213)으로부터 콘텐츠 ID를 판독하고, 판독한 콘텐츠 ID를 입출력부(201)에 출력한다. 제어부(202)는 암호화 콘텐츠 기억영역(210)에 저장되어 있는 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N] 및 매체기록 키 기억영역(211)에 저장되어 있는 암호화 매체기록 키 EK2를 소거한다. 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N] 및 암호화 매체기록 키 EK2가 소거되면 제어부(202)는 이중 암호키 기억영역(212)으로부터 이중 암호키 K3[N]을 순차 판독하고, 판독한 K3[N]을 순차 입출력부(201)에 출력한다.

(b) 휴대형 매체(20)가 휴대정보 단말(30)에 삽입되어 있는 상태

제어부(202)는 매체기록 키 기억영역(211)에 저장되어 있는 암호화 매체기록 키 EK2를 판독하고, 판독한 암호화 매체기록 키 EK2를 입출력부(201)에 출력한다.

제어부(202)는 휴대형 매체 ID 기억영역(220)에 저장되어 있는 매체 ID 및 MKB 기억영역(221)에 저장되어 있는 MKB를 판독하고, 판독한 매체 ID 및 MKB를 입출력부(201)에 출력한다.

제어부(202)는 암호화 콘텐츠 기억영역(210)에 저장되어 있는 암호화 부분콘텐츠 EC4[n]을 판독할 때마다 판독한 암호화 콘텐츠 EC4[n]을 입출력부(201)에 출력한다.

(3) 기억부(203)

여기에서는 기억부(203)에 포함되는 암호화 콘텐츠 기억영역(210), 매체기록 키 기억영역(211), 이중 암호키 기억영역(212), 콘텐츠 ID 기억영역(213), 휴대형 매체 ID 기억영역(220) 및 MKB 기억영역(221)에 대해서 설명한다.

암호화 콘텐츠 기억영역(210)은 제어부(202) 및 입출력부(201)를 거쳐서 기록재생장치(10)로부터 수신하는 암호화 부분콘텐츠 EC4[n]을 기억한다.

매체기록 키 기억영역(211)은 제어부(202) 및 입출력부(201)를 거쳐서 기록재생장치(10)로부터 수신하는 암호화 매체기록 키 EK2를 기억한다.

이중 암호키 기억영역(212)은 제어부(202) 및 입출력부(201)를 거쳐서 기록재생장치(10)로부터 수신하는 이중 암호키 K3[n]을 기억한다.

콘텐츠 ID 기억영역(213)은 제어부(202) 및 입출력부(201)를 거쳐서 기록재생장치(10)로부터 수신하는 콘텐츠 ID를 기억한다.

휴대형 매체 ID 기억영역(220)은 매체 ID를 미리 기억하고 있다.

MKB 기억영역(221)은 MKB를 미리 기억하고 있다.

여기서, 도 6에 암호화 콘텐츠 기억영역(210), 매체기록 키 기억영역(211), 이중 암호키 기억영역(212) 및 콘텐츠 ID 기억영역(213)에 기억되는 데이터 구조의 구체 예를 나타낸다. 여기서는 암호화 콘텐츠 $EC2_1$이 무브되는 경우에 대해서 설명한다. 암호화 콘텐츠 기억영역(210)에는 제어부(202) 및 입출력부(201)를 거쳐서 기록재생장치(10)로부터 수신한 암호화 부분콘텐츠 $EC4_{1[}1]$, $EC4_{1[}2]$, …, $EC4_{1[}N]$이 기억되고, 매체기록 키 기억영역(211)에는 제어부(202) 및 입출력부(201)를 거쳐서 수신한 암호화 매체기록 키 EK2가 기억되며, 이중 암호키 기억영역(212)에는 제어부(202) 및 입출력부(201)를 거쳐서 기록재생장치(10)로부터 수신한 이중 암호키 K3[1], K3[2], …, K3[N]이 기억되어 있다. 콘텐츠 ID 기억영역(213)에는 콘텐츠 ID 「CID_1」이 기억되어 있다.

1.6 휴대정보 단말(30)

휴대정보 단말(30)은, 도 7에 도시한 바와 같이, 디바이스 키 기억부(301), 입출력부(302), 제어부(303), 표시부(304), 키 조작부(305), 통신부(306), 안테나(307), 마이크(308), 및 스피커(309)로 구성되고, 구체적으로는 무선전파를 이용하여 통신을 행하는 휴대전화기이다.

또, 휴대정보 단말(30)은 마이크로 프로세서, ROM, RAM, 하드디스크 유닛 등을 구비하는 컴퓨터 시스템이다. 상기 ROM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서는 상기 컴퓨터 프로그램에 따라서 동작함으로써 휴대정보 단말(30)은 그 기능을 달성한다.

디바이스 키 기억부(301)는 휴대정보 단말(30)에 고유한 디바이스 키 DK2를 미리 기억하고 있다.

입출력부(302)는 메모리카드 슬롯 등으로 이루어지고, 메모리카드 슬롯에 휴대형 매체(20)가 삽입되어 있는 상태에서 휴대형 매체(20)의 매체기록 키 기억영역(211)에 저장되어 있는 암호화 매체기록 키 EK2를 판독하고, 판독한 암호화 매체기록 키 EK2를 제어부(303)에 출력한다. 입출력부(302)는 메모리카드 슬롯에 휴대형 매체(20)가 삽입되어 있는 상태에서 휴대형 매체(20)의 암호화 콘텐츠 기억영역(210)에 저장되어 있는 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N]을 순차 판독하고, 판독한 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N]을 제어부(303)에 순차 출력한다.

제어부(303)는 입출력부(302)로부터 암호화 매체기록 키 EK2를 수신하면, 디바이스 키 기억부(301)로부터 디바이스 키 DK1을 판독하고, 또, 휴대형 매체(20)로부터 매체 ID 및 MKB를 판독한다. 제어부(303)는 디바이스 키 DK1과 매체 ID 및 MKB를 이용하여 암호화 매체기록 키 EK2를 복호하기 위한 매체 고유 키 K0을 생성하고, 생성한 매체 고유 키 K0을 이용하여 암호화 매체 키 EK2를 복호하여 매체기록 키 K2를 생성한다. 여기서 매체 고유 키 K0의 생성 및 암호화 매체기록 키 EK2의 복호는 CPRM 규격에 의거하여 실행된다.

제어부(303)는 암호화 부분콘텐츠 EC4[n]에 매체기록 키 K2를 복호 키로 이용하여 복호 알고리즘 D2를 실시하여 순차 부분콘텐츠 C4[n]을 생성한다. 즉, C4[n]= D2(EC4[n], K2)이다. 또, 제어부(303)가 이용하는 복호 알고리즘 D2는 암호화 알고리즘 E2를 이용하여 암호화된 암호문을 평문으로 변환하는 알고리즘이다.

제어부(303)는 생성한 부분 콘텐츠 C4[n]을 순차 디코드하여 영상신호 및 음성신호를 생성한다. 제어부(303)는 생성한 영상신호를 표시부(304)에 출력하고 생성한 음성신호를 스피커(309)에 출력한다.

여기서는 구체 예로, 제어부(303)는 암호화 부분콘텐츠 $EC4_{1[}1]$, $EC4_{1[}2]$, …, $EC4_{1[}N]$을 순차 복호하여 $C4_{1[}1]$, $C4_{1[}2]$, …, $C4_{1[}N]$을 생성하는 것으로 한다. 제어부(303)는 생성한 부분콘텐츠 $C4_{1[}N]$을 순차 디코드하여 영상신호 및 음성신호를 생성한다.

키 조작부(305), 통신부(306), 안테나(307), 마이크(308) 및 스피커(309)는 휴대전화기로서의 통상의 통화, 전자메일의 송수신 등의 기능을 담당한다. 이들 구성요소에 대해서는 공지기술에 의해 실현 가능하므로 설명을 생략한다.

1.7 저작권 보호시스템(1)의 동작 개요

여기서는 저작권 보호시스템(1)의 동작의 개요에 대해서 도 8에 도시한 흐름도를 사용하여 설명한다.

콘텐츠 공급장치(11)는 콘텐츠 C2를 방송하고(스텝 S 5), 기록재생장치(10)는 콘텐츠 C2를 수신한다(스텝 S 10).

기록재생장치(10)는 장치기록 키 K1을 암호키로 이용하여 콘텐츠 C2를 암호화하여 암호화 콘텐츠 EC2를 생성하여 기록한다(스텝 S 15).

기록재생장치(10)는 콘텐츠 C2의 재생지시를 수신하면, 장치기록 키 K1을 복호 키로 이용하여 기록하고 있는 암호화 콘텐츠 EC2를 복호 해서 콘텐츠 C2를 생성하고, 생성한 콘텐츠 C2를 디코드하여 영상신호와 음성신호를 생성하며, 생성한 영상신호를 모니터(12)에 출력하고 생성한 음성신호를 스피커(13)에 출력함으로써 콘텐츠 C2를 재생한다(스텝 S 20).

모니터(12)는 기록재생장치(10)로부터 영상신호를 수신하면, 수신한 영상신호에 의거하여 영상을 출력하고, 스피커(13)는 기록재생장치(10)로부터 음성신호를 수신하면 수신한 음성신호에 의거하여 음성을 출력한다(스텝 S 45).

기록재생장치(10)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 무브 지시를 수신하면 제 1 이동처리를 행하며, 기록하고 있는 콘텐츠를 메모리카드 슬롯에 삽입된 휴대형 매체(20)에 무브한다(스텝 S 25). 이때, 휴대형 매체(20)는, 부분콘텐츠 C2[n](n = 1, 2, …, N이다. 이하 동일)을 MPEG-4 규격에 따라서 압축 부호화한 부분콘텐츠 C4[n]이 매체기록 키 K2에 의해 암호화된 암호화 부분콘텐츠 EC4[n], 암호화 매체기록 키 EK2, 이중 암호키 K3[n] 및 콘텐츠 ID를 기억하고 있다.

휴대정보 단말(30)은 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 매체 고유 키 K0을 생성하고, 생성한 매체 고유 키 K0을 이용하여 휴대형 매체(20)에 기록되어 있는 암호화 매체 키 EK2를 복호하여 매체기록 키 K2를 생성한다. 휴대정보 단말(30)은 생성한 매체기록 키 K2를 복호 키로 이용하여 암호화 부분콘텐츠 EC4[n]을 복호하여 순차 부분콘텐츠 C4 [n]을 생성한다. 휴대정보 단말(30)은 생성한 부분콘텐츠 C4[n]을 순차 디코드하여 영상신호 및 음성신호를 생성하고, 생성한 영상신호 및 음성신호 각각에 의거하여 영상 및 음성을 출력함으로써 콘텐츠 C4를 재생한다(스텝 S 30).

기록재생장치(10)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 무브 백 지시를 수신하면 제 2 이동처리를 행하고, 휴대형 매체(20)가 기록하고 있는 콘텐츠를 당해 기록재생장치(10)에 무브한다(스텝 S 35). 이때, 기록재생장치(10)는 MPEG-2 규격에 따라서 압축 부호화된 부분콘텐츠 C2[n](n = 1, 2, …, N이다. 이하 동일)이 장치기록 키 K1으로 암호화된 암호화 부분콘텐츠 EC2[n]을 기억하고 있다.

기록재생장치(10)는 콘텐츠 C2의 재생지시를 수신하면, 장치기록 키 K1을 복호 키로 이용하여 기록하고 있는 암호화 콘텐츠 EC2를 복호하여 콘텐츠 C2를 생성하고, 생성한 콘텐츠 C2를 디코드하여 영상신호와 음성신호를 생성하며, 생성한 영상신호를 모니터(12)에 출력하고, 생성한 음성신호를 스피커(13)에 출력함으로써 콘텐츠 C2를 재생한다(스텝 S 40). 모니터(12) 및 스피커(13)는 기록재생장치(10)로부터 수신한 영상신호 및 음성신호 각각에 의거하여 영상 및 음성을 출력한다(스텝 S 45).

1.8 제 1 이동처리의 동작

여기서는 도 8의 스텝 S 25에서 실행되는 제 1 이동처리의 동작에 대해서 도 9에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(10)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 입력부(118)에서 무브 지시를 수신하면(스텝 S 100), 콘텐츠 이동처리를 행하며, 기록하고 있는 콘텐츠를 휴대형 매체(20)로 이동한다(스텝 S 105). 이때, 기록재생장치(10)는 콘텐츠 이동처리의 동작중에 콘텐츠 ID, 암호화 매체기록 키 EK2, 암호화 부분콘텐츠 EC4[n](n = 1, 2, …, N이다. 이하 동일) 및 이중 암호키 K3[n]을 휴대형 매체(20)에 출력한다.

휴대형 매체(20)는 기록재생장치(10)로부터 콘텐츠 ID를 수신하면, 수신한 콘텐츠 ID를 콘텐츠 ID 기억영역(213)에 기록한다(스텝 S 110).

휴대형 매체(20)는 기록재생장치(10)로부터 암호화 매체기록 키 EK2를 수신하면, 수신한 암호화 매체기록 키 EK2를 매체기록 키 기억영역(211)에 기록한다(스텝 S 115).

휴대형 매체(20)는 기록재생장치(10)로부터 암호화 부분콘텐츠 EC4[n]을 수신하면, 수신한 암호화 부분콘텐츠 EC4[n]을 암호화 콘텐츠 기억영역(210)에 기록한다(스텝 S 120).

휴대형 매체(20)는 기록재생장치(10)로부터 이중 암호키 K3[n]을 수신하면, 수신한 이중 암호키 K3[n]을 이중 암호키 기억영역(212)에 기록한다(스텝 S 125).

1.9 콘텐츠 이동처리의 동작

여기에서는 도 9의 스텝 S 105에서 행해지는 콘텐츠 이동처리의 동작에 대해서 도 10에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(10)의 매체기록 키 생성부(106)는 입력부(118)로부터 콘텐츠의 지정과 지정된 콘텐츠의 무브 명령을 포함하는 무브 지시를 수신하면 매체기록 키 K2를 생성한다(스텝 S 200).

기록재생장치(10)의 매체기록 키 기억부(107)는 매체기록 키 생성부(106)로부터 매체기록 키 K2와 무브 지시를 수신하면 수신한 K2를 내부의 키 기억영역에 저장한다(스텝 S 205). 또, 매체기록 키 기억부(107)는 수신한 무브 지시에 포함되는 콘텐츠 ID를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록한다(스텝 S 210). 이때, 휴대형 매체(20)는 도 9에 도시한 스텝 S 110을 행한다.

매체기록 키 기억부(107)는 휴대형 매체(20)로부터 기록/판독부(117)를 거쳐서 휴대형 매체(20)를 식별하는 매체ID와 MKB를 판독하고, 판독한 매체ID와 MKB와 미리 기억하고 있는 디바이스 키 DK1을 이용하여 매체 고유 키 K0을 생성하고, 생성한 매체 고유 키 K0을 이용하여 매체기록 키 K2를 암호화하여 암호화 매체기록 키 EK2를 생성한다(스텝 S 215).

매체기록 키 기억부(107)는 생성한 암호화 매체기록 키 EK2를 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록한다(스텝 S 220). 이때, 휴대형 매체(20)는 도 9에 도시한 스텝 S 115를 행한다.

매체기록 키 기억부(107)는 기록완료 후에는 생성한 암호화 매체기록 키 EK2를 소거한다(스텝 S 225).

기록재생장치(10)의 제 1 복호부(108)는 매체기록 키 기억부(107)로부터 무브 지시를 수신하면, 장치기록 키 K1을 판독한다(스텝 S 230).

제 1 복호부(108)는 암호화 콘텐츠 기록부(104)로부터 지정의 암호화 콘텐츠를 판독하는 판독지시를 암호화 콘텐츠 판독부(109)에 출력하고, 암호화 콘텐츠 판독부(109)는 제 1 복호부(108)로부터 판독지시를 수신하면 카운터 n에 1을 설정한다(스텝 S 235).

암호화 콘텐츠 판독부(109)는 판독지시에서 지정된 암호화 콘텐츠의 n번째의 암호화 부분콘텐츠 EC2[n]을 판독한다(스텝 S 240).

암호화 콘텐츠 판독부(109)는 암호화 부분콘텐츠 EC2[n]의 판독에 성공하였는지 여부를 판단한다(스텝 S 245).

성공하였다고 판단하는 경우에는(스텝 S 245에서의 「YES」), 암호화 콘텐츠 판독부(109)는 판독한 암호화 부분콘텐츠 EC2[n]을 일시 기억하는 동시에 부분콘텐츠 이동처리를 행하고, 판독한 암호화 부분콘텐츠 EC2[n]으로부터 생성된 암호화 부분콘텐츠 EC4[n]을 기록매체에 기록한다(스텝 S 250).

암호화 콘텐츠 판독부(109)는 카운터 n에 1을 가산하고, 가산결과를 다시 n으로 한다(스텝 S 255). 암호화 콘텐츠 판독부(109)는 암호화 부분콘텐츠 EC2[n]을 판독하고(스텝 S 260), 다시 스텝 S 245 이후를 실행한다.

실패하였다고 판단하는 경우에는 (스텝 S 245에서의 「NO」), 암호화 콘텐츠 판독부(109)는 판독에 실패하였다는 취지의 명령을 제 1 복호부(108)에 출력하고, 제 1 복호부(108)는 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠의 판독에 실패하였다는 취지의 명령을 수신하면, 수신한 명령을 매체기록 키 기억부(107)에 출력한다. 매체기록 키 기억부(107)는 제 1 복호부(108)로부터 암호화 부분콘텐츠의 판독에 실패하였다는 취지의 명령을 수신하면, 키 기억영역에서 기억하고 있는 매체기록 키 K2를 소거한다(스텝 S 265).

1.10 부분콘텐츠 이동처리의 동작

여기서는 도 10의 스텝 S 250에서 실행되는 부분콘텐츠 이동처리의 동작에 대해서 도 11에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(10)의 제 1 복호부(108)는 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 EC2[n]을 수신하면, 도 10에 도시한 스텝 S 230에서 판독한 장치기록 키 K1을 복호 키로 이용하여 수신한 EC2[n]을 복호하여 부분콘텐츠 C2[n]을 생성한다(스텝 S 300).

기록재생장치(10)의 변환부(110)는 제 1 복호부(108)로부터 부분콘텐츠 C2[n]을 수신하면, 수신한 부분콘텐츠 C2[n]을 다운 컨버트 함으로써 MPEG-4로 압축변환하여 부분콘텐츠 C4[n]을 생성한다(스텝 S 305).

기록재생장치(10)의 제 2 암호화부(111)는 변환부(110)로부터 부분콘텐츠 C4[n]을 수신하면, 매체기록 키 기억부(107)에 기억되어 있는 매체기록 키 K2를 판독하고, 판독한 매체기록 키 K2를 암호키로 이용하여 부분콘텐츠 C4[n]을 암호화하여 암호화 부분콘텐츠 EC4[n]을 생성한다(스텝 S 310).

제 2 암호화부(111)는 암호화 부분콘텐츠 EC4[n]을 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록한다(스텝 S 315). 이때, 휴대형 매체(20)는 도 9에 도시한 스텝 S 120을 행한다. 또, 제 2 암호화부(111)는 내부에 존재하는 암호화 부분콘텐츠 EC4[n]을 소거한다.

제 2 암호화부(111)는 암호화 부분콘텐츠 EC2[n]의 암호화에 이용하는 이중 암호키의 생성을 지시하는 생성지시를 이중 암호키 생성부(112)에 출력한다. 이중 암호키 생성부(112)는 생성지시(수치n)를 수신하면, 이중 암호키 K3[n]을 생성한다(스텝 S 320).

이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(113)에 출력하고, 이중 암호키 기억부(113)는 이중 암호키 생성부(112)로부터 이중 암호키 K3[n]을 수신하면 수신한 이중 암호키 K3[n]을 이중 암호키 기억영역에 저장한다(스텝 S 325). 또, 이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 휴대형 매체(20)의 이중 암호키 기억영역(212)에 기록한다. 이때, 휴대형 매체(20)는 도 9에 도시한 스텝 S 125를 행한다.

기록재생장치(10)의 이중 암호화부(114)는 이중 암호키 기억부(113)로부터 암호화 지시(수치 n)를 수신하면, 이중 암호키 기억부(113)에 기억되어 있는 이중 암호키 K3[n]을 판독하고, 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 EC2[n]과 판독지시를 판독한다. 이중 암호화부(114)는 이중 암호키 K3[n]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[n]을 암호화하여 이중 암호화 부분콘텐츠 EEC2[n]을 생성하고(스텝 S 330), 이중 암호키 K3[n]을 소거한다(스텝 S 335).

기록재생장치(10)의 이중 암호화 콘텐츠 기록부(115)는 이중 암호화부(114)로부터 기록지시와 이중 암호화 부분콘텐츠 EEC2[n]을 수신하면, 암호화 콘텐츠 기록부(104)에 기억되고 또한 기록지시에 포함되는 콘텐츠 ID 및 암호화 부분콘텐츠의 번호에 대응하는 EC2[n]을 수신한 EEC2[n]으로 덮어씀으로써 암호화 콘텐츠 기록부(104)에 기록한다(스텝 S 340).

이중 암호화 콘텐츠 기록부(115)는 제 1 복호부(108), 암호화 콘텐츠 판독부(109), 변환부(110) 및 이중 암호화부(114)에 제 1 소거지시를 출력한다. 제 1 복호부(108)는 이중 암호화 콘텐츠 기록부(115)로부터 기억하고 있는 내용을 소거하는 제 1 소거지시를 수신하면 복호 된 C2[n]을 소거한다. 암호화 콘텐츠 판독부(109)는 이중 암호화 콘텐츠 기록부(115)로부터 제 1 소거지시를 수신하면, 암호화 콘텐츠 기록부(104)로부터 판독한 암호화 부분콘텐츠 EC2[n]을 소거한다. 변환부(110)는 이중 암호화 콘텐츠 기록부(115)로부터 제 1 소거지시를 수신하면 변환된 부분콘텐츠 C4[n]을 소거한다. 이중 암호화부(114)는 이중 암호화 콘텐츠 기록부(115)로부터 제 1 소거지시를 수신하면 암호화 콘텐츠 판독부(109)로부터 판독한 암호화 콘텐츠 EC2[n]을 소거한다(스텝 S 345).

1.11 제 2 이동처리의 동작

여기서는 도 8의 스텝 S 35에서 실행되는 제 2 이동처리의 동작에 대해서 도 12에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(10)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 입력부(118)에서 무브 백 지시를 수신하면(스텝 S 400), 휴대형 매체(20)로부터 콘텐츠 ID를 판독한다(스텝 S 405). 이때, 휴대형 매체(20)는 콘텐츠 ID를 판독하고, 판독한 콘텐츠 ID를 기록재생장치(10)에 출력한다(스텝 S 410).

기록재생장치(10)는 콘텐츠 복호처리를 행한다(스텝 S 415). 이때, 기록재생장치(10)는 콘텐츠 이동처리의 동작 중에 제 2 소거지시 및 제 3 소거지시를 휴대형 매체(20)에 출력하고, 휴대형 매체(20)로부터 이중 암호키 K3[n](n = 1, 2, …, N이다. 이하 동일)를 수신한다.

휴대형 매체(20)는 기록재생장치(10)로부터 제 2 소거지시를 수신하면, 암호화 부분콘텐츠 EC4[1],EC4[2], …, EC4[N]과, 암호화 매체기록 키 EK2와, 콘텐츠 ID를 소거한다(스텝 S 420).

휴대형 매체(20)는 이중 암호키 K3 n]을 순차 판독하고, 판독한 이중 암호키K3[n]을 기록재생장치(10)에 출력한다(스텝 S 425).

휴대형 매체(20)는 기록재생장치(10)로부터 제 3 소거지시를 수신하면, 이중 암호키 K3[n]을 소거한다(스텝 S 430).

1.12 콘텐츠 복호처리

여기서는 도 12의 스텝 S 415에서 행해지는 콘텐츠 복호처리에 대해서 도 13에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(10)의 제 2 복호부(116)는 제 2 소거지시를 휴대형 매체(20)에 출력하고(스텝 S 500), 카운터 n에 1을 설정한다(스텝 S 505). 이때, 휴대형 매체(20)는 도 12에 도시한 스텝 S 420을 실행한다.

제 2 복호부(116)는 휴대형 매체(20)로부터 이중 암호키 K3[n]을 판독한다(스텝 S 510). 이때, 휴대형 매체(20)는 도 12에 도시한 스텝 S 425를 실행한다.

제 2 복호부(116)는 이중 암호키 K3[n]의 판독에 성공하였는지 여부를 판단한다(스텝 S 515).

성공하였다고 판단하는 경우에는(스텝 S 515에 있어서의 「YES」), 제 2 복호부(116)는 암호화 콘텐츠 기록부(104)로부터 판독한 콘텐츠 ID에 대응하는 이중 암호화 부분콘텐츠 EEC2[n]을 판독하고(스텝 S 520), 이중 암호키 K3[n]을 복호키로 이용하여 판독한 이중 암호화 부분콘텐츠 EEC2[n]을 복호하여 암호화 콘텐츠 EC2[n]을 생성한다(스텝 S 525).

제 2 복호부(116)는 암호화 콘텐츠 기록부(104)에 기억되고 휴대형 매체(20)로부터 판독한 콘텐츠 ID에 대응하는 EEC2[n]을 생성한 암호화 부분콘텐츠 EC2[n]으로 덮어씀으로써 암호화 콘텐츠 기록부(104)에 기록한다(스텝 S 530).

제 2 복호부(116)는 내부에 존재하는 이중 암호화 부분콘텐츠 EEC2[n]과 이중 암호화 키 K3[n]을 소거한다(스텝 S 535).

제 2 복호부(116)는 제 3 소거지시를 휴대형 매체(20)에 출력한다(스텝 S 540). 이때, 휴대형 매체(20)는 도 12에 도시한 스텝 S 430을 행한다.

제 2 복호부(116)는 카운터 n에 1을 가산하고, 가산결과를 다시 n으로 한다(스텝 S 545). 제 2 복호부(116)는 암호화 부분콘텐츠 EC2[n]을 판독하고(스텝 S 550) 스텝 S 515 이후를 행한다.

실패하였다고 판단하는 경우에는(스텝 S 515에서의 「NO」), 제 2 복호부(116)는 처리를 종료한다.

1.13 제 1 실시 예의 변형 예

(1) 상기 실시 예에서, 기록재생장치(10)는 모든 암호화 부분콘텐츠 EC2[n]을 암호화하여 이중 암호화 부분콘텐츠 EEC2[n]을 생성하여 이중 암호화 콘텐츠 EEC2로 하였으나, 이에 한정되지는 않는다.

N개의 암호화 부분콘텐츠 중 적어도 하나를 이중 암호키로 암호화해도 된다. 예를 들어 암호화 콘텐츠 EC2[1]만을 이중 암호키 K3으로 암호화해도 된다. 또는 N개의 암호화 부분콘텐츠 중, 짝수 번째에 위치하는 암호화 부분콘텐츠를 암호화해도 된다. 또는 홀수 번째에 위치하는 암호화 부분콘텐츠를 암호화해도 된다.

(2) 상기 실시 예에서, 기록재생장치(10)는 N개의 암호화 부분콘텐츠 EC2[n]에 대해서 N개의 이중 암호키 K3[n]을 생성하고, 휴대형 매체(20)에 기록하였으나, 이에 한정되지는 않는다.

기록재생장치(10)는 암호화 부분콘텐츠의 수 미만인 소정의 수(예를 들면 5개)의 이중 암호키 K3[1], K3[2], …, K3[5]를 생성하고, 생성한 5개의 이중 암호키를 휴대형 매체 (20)에 기록해도 된다. 또, 소정의 수는 1 이상이고, 또한 암호화 부분콘텐츠의 수 미만인 수라도 되며, 2 이상이고, 또한 암호화 부분콘텐츠의 수 미만인 수라도 된다.

이때, 기록재생장치(10)는 5개의 이중 암호키를 주기적으로 이용한다. 예를 들어 기록재생장치(10)는 EC2[1]을 암호화하는 경우에는 K3[1]을 이용하고, EC2[2]를 암호화하는 경우에는 K3[2]를 이용하며, …, EC2[5]를 암호화하는 경우에는 K3[5]를 이용하고, EC2[6]을 암호화하는 경우에는 K3[1]을 이용하며, EC2[7]을 암호화하는 경우에는 K3[2]를 이용하고, 이하 주기적으로 K3[m](m = 1, 2, …, 5)를 이용한다.

(3) 또는, 기록재생장치(10)는 1개의 이중 암호키 K3[1]을 생성하고, 휴대형 매체(20)에 기록해도 된다. 이 경우, 이하와 같이 하여 모든 암호화 부분콘텐츠 EC2[n]을 이중 암호화한다.

<이중 암호키 생성부(112)>

이중 암호키 생성부(112)는 수치가 1인 생성지시를 수신하면 이중 암호키 K3[n]을 생성한다. 이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 기록/판독부(117)를 거쳐서 휴대형 매체(20)에 기록한다. 이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(113)에 출력한다. 또, 이중 암호키 생성부(112)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(113)에 출력한 후, 생성한 이중 암호키 K3[n]을 당해 이중 암호키 생성부(112)에서 소거한다.

이중 암호키 생성부(112)는 수치가 m(m = 2, 3, …, N)인 생성지시를 수신하면 생성지시를 수신하였다는 취지의 명령을 이중 암호키 기억부(113)에 출력한다.

<이중 암호키 기억부(113)>

이중 암호키 기억부(113)는 이중 암호키 생성부(112)로부터 이중 암호키 K3[1] 및 생성지시를 수신하였다는 취지의 명령을 수신한다.

이중 암호키 기억부(113)는 이중 암호키 생성부(112)로부터 이중 암호키 K3[1]을 수신하면, 수신한 이중 암호키 K3[1]을 이중 암호키 기억영역에 저장한다.

이중 암호키 기억부(113)는 암호화 지시를 이중 암호화부(114)에 출력한다. 암호화 지시의 구체 예는 이중 암호화하는 암호화 부분콘텐츠의 번호를 나타내는 수치이다.

이중 암호키 기억부(113)는 이중 암호화 콘텐츠 기록부(115)로부터 제 1 소거지시를 수신하면 이중 암호키 K3[n]을 소거한다.

<이중 암호화부(114)>

이중 암호화부(114)는 일 방향성 함수 F와, 이중 암호키를 일시 기억하는 일시 기억영역을 갖는다.

이중 암호화부(114)는 이중 암호키 기억부(113)로부터 암호화 지시인 수치 1, 2, …, N을 순차 수신한다.

이중 암호화부(114)는 수치가 1인 암호화 지시를 수신하면, 이중 암호키 기억부(113)에 기억되어 있는 이중 암호키 K3[1]을 판독하고, 암호화 콘텐츠 판독부(109)에 의해 암호화 부분콘텐츠 EC2[1]과 판독지시를 판독한다. 이중 암호화부(114)는 이중 암호키 K3[1]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[1]을 암호화하여 이중 암호화 부분콘텐츠

EEC2[1]을 생성한다. 이중 암호화부(114)는 판독한 이중 암호키 K3[1]을 일시 기억영역에 기억한다. 이중 암호화부(114)는 생성한 이중 암호화 부분콘텐츠 EEC2[1]과, 암호화 콘텐츠 판독부(109)로부터 판독한 판독지시를 포함하는 기록지시를 이중 암호화 콘텐츠 기록부(115)에 출력한다.

이중 암호화부(114)는 수치가 m(m = 2, 3, …, N)인 암호화 지시를 수신하면, 일시 기억영역에 기억하고 있는 이중 암호키 K3[m-1]을 판독하고, 암호화 콘텐츠 판독부(109)로부터 암호화 부분콘텐츠 EC2[m]과 판독지시를 판독한다. 이중 암호화부(114)는 이중 암호키 K3[m-1]에 대해서 일 방향성 함수 F를 실시하여 이중 암호키 K3[m]을 생성한다. 즉, K3[m] = F(K3[m-1])이다. 이중 암호화부(114)는 생성한 K3[m]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[m]을 암호화하여 이중 암호화 부분콘텐츠 EEC2[m]을 생성한다. 이중 암호화부(114)는 판독한 이중 암호키 K3[m]을 일시 기억영역에 기억한다. 이중 암호화부(114)는 생성한 이중 암호화 부분콘텐츠 EEC2[m]과 암호화 콘텐츠 판독부(109)로부터 판독한 판독지시를 포함하는 기록지시를 이중 암호화 콘텐츠 기록부(115)에 출력한다.

이에 따라 이중 암호화부(114)는 이중 암호키 K3[1]에 일 방향성 함수 F를 n-1회 실시함으로써 이중 암호키 K3[n]을 생성할 수 있다.

(4) 상기 (3)에서, 이중 암호키 K3[1]에 일 방향성 함수 F를 n-1회 실시하여 생성한 K3[n]을 이용하여 암호화 부분콘텐츠 EC2[n]을 이중 암호화하였으나, 이에 한정되지는 않는다.

기록재생장치(10)는 이중 암호키로서 K3[0]을 생성하고, 생성한 이중 암호키 K3[0]을 휴대형 매체(20)에 기록하며, 이중 암호키 K3[0]에 일 방향성 함수 F를 n회 실시하여 생성한 K3[n]을 이용하여 암호화 부분콘텐츠 EC2[n]을 이중 암호화해도 된다.

(5) 상기 실시 예에서, 기록재생장치(10)는 암호화 부분콘텐츠 EC2[n]을 이중 암호화 부분콘텐츠 EEC2[n]으로 덮어썼으나, 이것에 한정되지는 않는다.

이중 암호화 부분콘텐츠 EEC2[n]을 암호화 콘텐츠 기록부(104) 내에서 암호화 콘텐츠 EC2가 기록되어 있는 영역과는 다른 영역에 기록하고, EC2[n]을 소거해도 된다.

(6) 상기 실시 예에서, 기록재생장치(10)의 암호화 콘텐츠 판독부(109)는 128비트로 이루어지는 암호화 부분콘텐츠 EC2[n]을 판독하였지만, 이것에 한정되지는 않는다.

재생시간 길이의 합계가 소정 시간 내(45초 내)가 되도록 암호화 콘텐츠 EC2의 선두로부터 순서대로 1 이상의 암호화 부분콘텐츠를 판독해도 된다. 이때, 판독된 1 이상의 암호화 부분콘텐츠를 동일한 이중 암호키를 이용하여 이중 암호화한다.

구체적으로는, 암호화 콘텐츠 판독부(109)는 재생시간 길이의 합계가 소정 시간 내(45초 내)가 되도록 EC2[1], EC2[2], …, EC2[10]을 판독한다. 제 1 복호부(108)는 EC2[n1](n1 = 1, 2, …, 10이다. 이하 동일)을 복호한다. 변환부(110)는 복호된 C2[n1]을 C4[n1]로 변환한다. 제 2 암호화부(111)는 매체기록 키 K2를 이용하여 C4[n1]을 암호화하여 EC4[n1]을 순차 생성하고, 휴대형 매체(20)에 순차 기록한다. 이중 암호키 생성부(112)는 이중 암호키 K3[1]을 생성하여 휴대형 매체(20) 및 이중 암호키 기억부(113)에 기록한다. 이중 암호화부(114)는 이중 암호키 K3[1]을 이용하여 암호화 부분콘텐츠 EC2[n1]을 순차 암호화하여 이중 암호화 부분콘텐츠 EEC2[n1]을 생성한다. 이중 암호화 콘텐츠 기록부(115)는 암호화 부분콘텐츠 EC2[n1]을 이중 암호화 부분콘텐츠 EEC2[n1]로 순차 덮어쓴다.

기록재생장치(10)는 상기 동작을 암호화 부분콘텐츠 EC2[N]이 이중 암호화 부분콘텐츠 EEC2[N]으로 덮어써질 때까지 행한다.

(7) 상기 (6)에서, 재생시간 길이의 합계가 소정 시간 내(45초 내)가 되도록, 취득한 복수의 암호화 부분콘텐츠의 각각에 대응하는 부분콘텐츠를 결합하고, 결합한 부분콘텐츠에 포함되는 I 픽처만을 이중 암호화해도 된다.

이하, 상기(6)에서 설명한 구체 예를 사용하여 설명한다.

기록재생장치(10)의 이중 암호화부(114)는 제 1 복호부(108)에서 복호 된 복수의 부분콘텐츠 C2[n1] 각각을 결합하여 결합부분 콘텐츠 CC2[1]을 생성한다. 이중 암호화부(114)는 생성한 결합부분 콘텐츠 CC2[1]로부터 1 이상의 I 픽처를 취득하고, 취득한 1 이상의 I 픽처를 먼저 장치기록 키 K1로 암호화하여 ECI2[1]을 생성하며, 생성한 ECI2[1]을 이중 암호키로 암호화하여 EECI2[1]을 생성한다. 또, 기록재생장치(10)는 생성한 결합부분 콘텐츠 CC2[1]로부터 1 이상의 B

픽처 및 1 이상의 P 픽처를 취득하고, 취득한 1 이상의 B 픽처를 장치기록 키 K1로 암호화하여 ECB2[1]을 생성하며, 취득한 1 이상의 P 픽처를 장치기록 키 K1로 암호화하여 ECP2[1]을 생성한다. 기록재생장치(10)는 암호화 콘텐츠 EC2[1], …, [10]을 생성한 EECI2[1], ECB2[1] 및 ECP2[1]로 이루어지는 이중 암호화 부분콘텐츠에 재기록한다.

또, 기록재생장치(10)는 무브 백 지시를 수신하면, 휴대형 매체(20)에 기록되어 있는 암호화콘텐츠 EC4 및 암호화 매체기록 키 EK2를 소거하고, 그 후, 각 이중 암호화 부분콘텐츠를 복호하여 콘텐츠 C2를 생성한다. 기록재생장치(10)는 생성한 콘텐츠 C2를 128비트 단위로 암호화하여 EC2[1], EC2[2], …, EC2[N]을 생성하고, 이중 암호화 콘텐츠를 암호화 콘텐츠 EC2로 치환한다.

(8) 암호화 콘텐츠 EC2의 부분콘텐츠 단위로 복호 및 다운 컨버트 하여 휴대형 매체(20)에 기록하였으나, 이에 한정되는 것은 아니다.

이하와 같은 동작에 따라서 각 부분콘텐츠 EC4[n]을 휴대형 매체(20)에 기록해도 된다.

기록재생장치(10)는 암호화 콘텐츠 EC2를 복호하여 콘텐츠 C2를 생성하고, 생성한 콘텐츠 C2를 다운 컨버트 하여 콘텐츠 C4를 생성한다. 기록재생장치(10)는 생성한 콘텐츠 C4를 부분콘텐츠로 분할하고(예를 들어 128비트 단위로 분할), 암호화하여 각 부분콘텐츠 EC4[n]을 생성하여, 생성한 부분콘텐츠 EC4[n]을 순차 휴대형 매체(20)에 기록한다.

2. 제 2 실시 예

이하, 본 발명에 관한 제 2 실시 예로서의 저작권 보호시스템(2)에 대해서 도면을 참조하여 설명한다.

2.1 저작권 보호시스템(2)의 개요

저작권 보호시스템(2)은, 도 14에 도시한 바와 같이, 기록재생장치(50), 콘텐츠 공급장치(11), 모니터(12), 스피커(13), 휴대형 매체(20), 및 휴대정보 단말(30)로 구성되어 있다.

저작권 보호시스템 2는, 저작권 보호시스템 1과 마찬가지로, 방송국에 설치된 콘텐츠 공급장치(11)로부터 방송되는 디지털방송 프로그램인 콘텐츠를 기록재생장치(50)가 수신하고, 수신한 콘텐츠를 기록 및 재생하며, 또, 기록재생장치(50)에 기록되어 있는 콘텐츠를 휴대형 매체(20)에 무브(이동)하고, 무브 된 콘텐츠를 휴대정보 단말(30)에 의해 재생한다. 또, 휴대형 매체(20)에 기록되어 있는 콘텐츠를 다시 기록재생장치(50)에 무브하는 시스템이다.

콘텐츠 공급장치(11), 모니터(12), 스피커(13), 휴대형 매체(20) 및 휴대정보 단말(30)은 각각 저작권 보호시스템 1에서의 장치와 동일한 기능 및 구성을 가지므로 여기에서는 설명을 생략한다.

이하에서는 특히, 저작권 보호시스템 1과의 차이점인 기록재생장치(50)에 대해서 설명한다.

2.2 기록재생장치(50)

기록재생장치(50)는, 도 15에 도시한 바와 같이, 콘텐츠 수신부(501), 장치기록 키 기억부(502), 제 1 암호화부(503), 암호화 콘텐츠 기록부(504), 제 1 변환부(505), 부분정보 선택부(506), 변환용 데이터 암호화부(507), 변환용 데이터 기억부(508), 재생부(509), 매체기록 키 생성부(510), 매체기록 키 기억부(511), 제 1 복호부(512), 콘텐츠 판독부(513), 제 2 변환부(514), 변환 키 기억부(515), 변환용 데이터 복호부(516), 제 2 암호화부(517), 이중 암호키 생성부(518), 이중 암호키 기억부(519), 이중 암호화부(520), 이중 암호화 콘텐츠 기록부(521), 제 2 복호부(522), 기록/판독부(523) 및 입력부(524)로 구성된다.

기록재생장치(50)는 마이크로 프로세서, ROM, RAM, 하드디스크 유닛 등을 구비하는 컴퓨터 시스템이다. 상기 ROM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써 기록재생장치(50)는 그 기능을 달성한다.

여기서, 기록재생장치(50)는 구체 예로서 하드디스크 리코더이다.

(1) 콘텐츠 수신부(501)

콘텐츠 수신부(501)는 안테나를 포함하고, 콘텐츠 공급장치(11)로부터 방송된 콘텐츠 C2를 안테나를 거쳐서 수신하여, 수신한 콘텐츠 C2를 제 1 암호화부(503) 및 제 1 변환부(505)에 출력한다. 또, 콘텐츠 수신부(501)가 수신하는 콘텐츠는 MPEG-2 규격에 따라서 압축 부호화된 고화질 콘텐츠이다.

(2) 장치기록 키 기억부(502)

장치기록 키 기억부(502)는 제 1 실시 예에서 설명한 장치기록 키 기억부(102)와 동일하므로 설명을 생략한다.

또, 이후의 설명에 있어서, 장치기록 키 기억부(502)에 미리 기억되어 있는 장치기록 키는 K1로 한다.

(3) 제 1 암호화부(503)

제 1 암호화부(503)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신한다.

제 1 암호화부(503)는 재생시간 길이가 소정 시간 내(예를 들어 45초 이내)가 되는 데이터 사이즈(예를 들어 128비트)의 블록 데이터 C2[1], C2[2],C2[3], …, C2[N]을 콘텐츠 C2의 선두에서부터 순차 판독한다. 이하, 이 블록데이터를 부분콘텐츠라고 부른다. 부분콘텐츠 C2[n](n = 1, 2, …, N이다. 이하 동일)의 재생시간 길이는 소정 시간 내(45초 이내)이다.

또, 제 1 암호화부(503)는 장치기록 키 기억부(502)로부터 장치기록 키 K1을 판독하고, 부분콘텐츠 C2[n]의 각각에 대해서 장치기록 키 K1을 암호키로 이용하여 암호화 알고리즘 E1을 실시하여 암호화 부분콘텐츠 EC2[n]을 생성한다. 즉, EC2[n] = E1(C2[n], K1)이다. 또, 제 1 암호화부(503)가 이용하는 암호화 알고리즘 E1의 일 예는 AES(Advanced Encryption Standard)이다. 또, AES는 공지이므로 설명은 생략한다. 여기서는 암호화하는 데이터 길이를 재생시간 길이가 소정의 기간 내(예를 들어 45초 이내)가 되는 데이터 사이즈로 하고 있다.

제 1 암호화부(503)는 생성한 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[N]을 암호화 콘텐츠 기록부(504)에 저장한다.

제 1 암호화부(503)는 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[N]의 저장이 완료한 후, 내부에 존재하는 콘텐츠 C2를 소거한다.

(4) 암호화 콘텐츠 기록부(504)

암호화 콘텐츠 기록부(504)는 제 1 실시 예에서 설명한 암호화 콘텐츠 기록부(104)와 동일하므로 설명은 생략한다.

또, 본 실시 예에서, 제 1 실시 예와 마찬가지로, 암호화 부분콘텐츠를 EC2[1], EC2[2], …, EC2[N]으로 표기하고, 암호화 부분콘텐츠를, EC2[1], EC2[2], …, EC2[N]으로 이루어지는 데이터를, 암호화 콘텐츠 EC2로 표기한다.

또, 이후의 설명에서, 필요하다면, 도 3에 도시한 암호화 콘텐츠 $EC2_1$, $EC2_2$, $EC2_3$, …을 이용한다.

(5) 제 1 변환부(505)

제 1 변환부(505)는 구체적으로는 MPEG-2의 데이터를 MPEG-4로 변환하기 위한 다운 컨버터 등으로 구성된다.

제 1 변환부(505)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신하면, 수신한 콘텐츠 C2를 MPEG-4로 압축 변환하여 변환콘텐츠 C4를 생성한다.

제 1 변환부(505)는 재생시간 길이가 소정 시간 내(예를 들면 45초 이내)가 되는 데이터 사이즈(예를 들면 128비트)의 블록데이터 C4[1], C4[2], C4[3], …, C4[N]을 콘텐츠의 선두에서부터 순차 판독한다. 이하, 이 블록데이터를 부분변환콘텐츠라고 부른다. 부분변환콘텐츠 C4[n](n = 1, 2, …, N이다. 이하 동일)의 재생시간 길이는 소정 시간 내(45초 이내)이다.

제 1 변환부(505)는 부분변환 콘텐츠 C4[n]을 일시 기억하고, 선택지시를 부분정보 선택부(506)에 출력한다.

또, 제 1 변환부(505)는 변환콘텐츠 C4의 생성 후, 콘텐츠 C2를 소거한다.

또, 제 1 변환부(505)는 변환용 데이터 암호화부(507)로부터 변환데이터 소거지시를 수신하면 일시 기억하고 있는 부분변환콘텐츠 C4[n]을 소거한다.

또, 이하에서 부분변환콘텐츠를 단지 부분콘텐츠라고 한다.

(6) 부분정보 선택부(506)

부분정보 선택부(506)는 제 1 변환부(505)로부터 선택지시를 수신하면, 제 1 변환부(505)에 기억되어 있는 변환콘텐츠 C4의 선두 블록데이터, 즉, 부분콘텐츠 C4[1]을 판독하고, 판독한 부분콘텐츠 C4[1]을 부분정보 PC4로 변환용 데이터 암호화부(507)에 출력한다.

부분정보 선택부(506)는 부분정보 PC4를 출력한 후, 내부에 존재하는 부분정보 PC4를 소거한다.

(7) 변환용 데이터 암호화부(507)

변환용 데이터 암호화부(507)는 변환콘텐츠 C4로부터 변환용 데이터를 생성한다. 여기서 변환용 데이터는 변환콘텐츠가 암호화된 것이다.

변환용 데이터 암호화부(507)는 부분정보 선택부(506)로부터 부분정보 PC4를 수신하면, 제 1 변환부(505)로부터 부분콘텐츠C4[n]을 순차 판독한다.

변환용 데이터 암호화부(507)는 판독한 부분콘텐츠 C4[n]을 수신한 부분정보 PC4를 암호키로 이용하여 암호화 알고리즘 E1_1을 실시하여 암호화 부분변환콘텐츠 EC4_1[n]을 생성한다. 즉, EC4_1[n]= E1_1(C4[n], PC4)이다. 또, 변환용 데이터 암호화부(507)가 이용하는 암호화 알고리즘 E1_1의 일 예는 AES이다. 또, AES는 공지이므로 설명은 생략한다. 이하에서는 암호화 부분변환콘텐츠를 단지 암호화 부분콘텐츠라고 한다.

변환용 데이터 암호화부(507)는 생성한 암호화 부분콘텐츠 EC4_1[1], EC4_1[2],…, EC4_1[N]을 변환용 데이터 기억부(508)에 저장한다.

변환용 데이터 암호화부(507)는 암호화 부분콘텐츠 EC4_1[1], EC4_1[2],…, EC4_1[N]의 저장이 완료하면 내부에 존재하는 부분콘텐츠 C4[n] 및 부분정보PC4를 소거한다. 또, 변환용 데이터 암호화부(507)는 변환데이터 소거지시를 제 1 변환부(505)에 출력한다.

(8) 변환용 데이터 기억부(508)

변환용 데이터 기억부(508)는 구체적으로는 하드디스크 유닛이고, 변환콘텐츠C4가 암호화된 암호화 변환콘텐츠를 기억하기 위한 영역을 갖는다.

변환용 데이터 기억부(508)는 변환용 데이터 암호화부(507)로부터 암호화 부분콘텐츠 EC4_1[n]을 수신하면, 수신한 암호화 부분콘텐츠EC4_1[n]을 순차 저장한다. 또, 암호화 부분콘텐츠 EC4_1[1], EC4_1[2],…, EC4_1[N]으로 이루어지는 데이터를 암호화 변환콘텐츠 EC4_1로 표기한다. 이하에서는 암호화 변환콘텐츠를 단지 암호화 콘텐츠라고 한다. 또, 암호화 콘텐츠 EC4_1이 상기에 설명한 변환용 데이터가 된다.

도 16에 도시하는 바와 같이, 변환용 데이터 기억부(508)는 암호화 콘텐츠 $EC4\_1_1$, $EC4\_1_2$, $EC4\_1_3$, … 을 저장하고 있다. 첨자의 수치는 단지 복수의 암호화 콘텐츠를 식별하기 위한 정보이다. 각 암호화 콘텐츠 EC4_1에는 암호화 콘텐츠 EC4_1의 고화질 콘텐츠인 EC2에 할당된 콘텐츠 ID가 대응되어 있다. 구체적으로는, $EC2_1$의 콘텐츠 ID인 「CID_1」가 $EC4_1_1$에 대응되고, $EC2_2$의 콘텐츠 ID인 「CID_2」가 $EC4_1_2$에 대응되며, $EC2_3$의 콘텐츠 ID인 「CID_3」이 $EC4_1_3$에 대응되어 있다.

(9) 재생부(509)

재생부(509)는 제 1 실시 예에서 설명한 재생부(105)와 동일하므로 설명은 생략한다.

(10) 매체기록 키 생성부(510)

매체기록 키 생성부(510)는 제 1 실시 예에서 설명한 매체기록 키 생성부(106)와 동일하므로 설명은 생략한다.

또, 매체기록 키 생성부(510)에서 생성되는 매체기록 키는 K2로 한다.

(11) 매체기록 키 기억부(511)

매체기록 키 기억부(511)는 매체기록 키 K2를 기억하는 키 기억영역과 디바이스 키 DK1을 가지고 있다.

매체기록 키 기억부(511)는 매체기록 키 생성부(510)로부터 매체기록 키 K2와 무브 지시를 수신하면, 수신한 K2를 내부의 키 기억영역에 저장한다. 또, 매체기록 키 기억부(511)는 수신한 무브 지시에 포함되는 콘텐츠 ID를 기록/판독부(523)를 거쳐서 휴대형 매체(20)에 기록한다.

매체기록 키 기억부(511)는 휴대형 매체(20)로부터 기록/판독부(523)를 거쳐서 휴대형 매체(20)를 식별하는 매체 ID와 MKB(Media Key Block)를 판독하고, 판독한 매체 ID와 MKB와, 미리 기억하고 있는 디바이스 키 DK1을 이용하여 매체 고유 키 K0을 생성하며, 생성한 매체 고유 키 K0을 이용하여 매체기록 키 K2를 암호화하여 암호화 매체기록 키 EK2를 생성한다. 여기서 매체 고유 키 K0의 생성 및 암호화 매체기록 키 EK2의 생성은 CPRM 규격에 의거하여 행해진다.

매체기록 키 기억부(511)는 생성한 암호화 매체기록 키 EK2를 기록/판독부(523)를 거쳐서 휴대형 매체(20)에 기록하고, 기록완료 후, 생성한 암호화 매체기록 키 EK2를 소거한다.

매체기록 키 기억부(511)는 수신한 무브 지시를 제 1 복호부(512)에 출력한다.

매체기록 키 기억부(511)는 변환용 데이터 복호부(516)로부터 암호화 부분콘텐츠의 판독에 실패하였다는 취지의 명령을 수신하면, 키 기억영역에서 기억하고 있는 매체기록 키 K2를 소거한다.

(12) 제 1 복호부(512)

제 1 복호부(512)는 매체기록 키 기억부(511)로부터 무브 지시를 접수하면, 장치기록 키 기억부(502)로부터 장치기록 키 K1을 판독한다.

제 1 복호부(512)는 암호화 콘텐츠 기록부(504)로부터 지정의 암호화 콘텐츠의 선두에 위치하는 부분콘텐츠를 판독하는 선두 판독지시를 콘텐츠 판독부(513)에 출력한다. 여기서 선두 판독지시의 구체 예는 무브 지시에 포함되는 콘텐츠 ID이다.

제 1 복호부(512)는 콘텐츠 판독부(513)로부터 암호화 부분콘텐츠 EC2[1]을 수신하면, 장치기록 키 기억부(502)로부터 판독한 장치기록 키 K1을 복호 키로 이용하여 복호 알고리즘 D1을 실시하여 부분콘텐츠 C2[1]을 생성한다. 즉, C2[1]= D1(EC2[1], K1)이다. 또, 복호 알고리즘 D1은 암호화 알고리즘 E1으로 암호화된 암호문을 평문으로 변환하기 위한 알고리즘이다.

제 1 복호부(512)는 생성한 부분콘텐츠 C2[1]을 제 2 변환부(514)에 출력한다.

제 1 복호부(512)는 부분콘텐츠 C2[1]을 제 2 변환부(514)에 출력한 후, 복호된 C2[1]을 소거한다.

이하에 구체 예를 설명한다. 제 1 복호부(512)는 콘텐츠의 지정으로 콘텐츠 ID「CID_1」을 수신하면, 콘텐츠 ID「CID_1」을 선두 판독지시로 하여 콘텐츠 판독부(513)에 출력한다. 제 1 복호부(512)는 콘텐츠 판독부(513)로부터 암호화 부분콘텐츠 $EC2_{1[}1]$을 수신하고, 부분콘텐츠 $C2_{1[}1]$을 생성한다. 제 1 복호부(512)는 생성한 부분콘텐츠 $C2_{1[}1]$과, 매체기록 키 기억부(511)로부터 수신한 무브 지시에 포함되는 콘텐츠 ID를 제 2 변환부(514)에 출력한다.

또, 제 1 복호부(512)는 콘텐츠의 재생시에 재생부(509)로부터 지시를 받아서, 콘텐츠 판독부(513)를 거쳐서 암호화 콘텐츠 기록부(504)로부터 판독한 암호화 콘텐츠 EC2를 장치기록 키 K1을 이용하여 복호하고, 복호 한 콘텐츠 C2를 재생부(509)에 출력한다.

(13) 콘텐츠 판독부(513)

콘텐츠 판독부(513)는 제 1 복호부(512)로부터 선두 판독지시를 수신하면, 지정된 암호화 콘텐츠의 선두에 위치하는 암호화 부분콘텐츠를 판독한다. 또 수신한 선두 판독지시를 일시 기억한다. 구체적으로는, 콘텐츠 판독부(513)는 제 1 복호부(512)로부터 콘텐츠 ID를 수신하고, 수신한 콘텐츠 ID와 일치하는 콘텐츠 ID를 갖는 암호화 부분콘텐츠 EC2[1]을 암호화 콘텐츠 기록부(504)로부터 판독한다. 콘텐츠 판독부(513)는 EC2[1]을 제 1 복호부(512)에 출력한다. 콘텐츠 판독부(513)는 EC2[1]을 제 1 복호부(512)에 출력한 후, 판독한 암호화 부분콘텐츠 EC2[1]을 소거한다.

또, 콘텐츠 판독부(513)는 이중 암호화부(520)로부터 지정된 콘텐츠의 n번째에 위치하는 암호화 부분 EC2[n]의 판독을 지시하는 콘텐츠 판독지시를 수신하면, 일시 기억하고 있는 선두 판독지시에 포함되는 콘텐츠 ID와 일치하는 콘텐츠 ID를 갖는 암호화 콘텐츠를 구성하는 암호화 부분콘텐츠 중, 수신한 콘텐츠 판독지시에서 지정된 n번째의 부분콘텐츠 EC2[n]을 판독한다. 콘텐츠 판독부(513)는 판독한 암호화 부분콘텐츠 EC2[n]을 이중 암호화부(520)에 출력한다.

콘텐츠 판독부(513)는 이중 암호화 콘텐츠 기록부(521)로부터 기억하고 있는 내용을 소거하는 제 1 소거지시를 수신하면, 판독한 암호화 부분콘텐츠 EC2[n]을 소거한다.

(14) 제 2 변환부(514)

제 2 변환부(514)는 구체적으로는 MPEG-2의 데이터를 MPEG-4로 변환하기 위한 다운 컨버터 등으로 구성된다.

제 2 변환부(514)는 제 1 복호부(512)로부터 부분콘텐츠 C2[1]과 콘텐츠 ID를 수신하면, 수신한 콘텐츠 C2[1]을 MPEG-4로 압축 변환하여 부분콘텐츠 C4[1]을 생성한다.

제 2 변환부(514)는 생성한 부분콘텐츠 C4[1]을 부분정보 PC4로 하여 변환 키 기억부(515)에 저장하고, 콘텐츠 ID를 변환 키 기억부(515)에 출력한다. 여기서 부분정보 PC4는 암호화 변환 부분콘텐츠로부터 변환 부분콘텐츠를 생성하는 변환키가 된다.

제 2 변환부(514)는 부분정보 PC4(=C4[1])을 변환 키 기억부(515)에 저장한 후 생성한 C4[1]을 소거한다.

(15) 변환 키 기억부(515)

변환 키 기억부(515)는 부분정보 PC4를 기억하기 위한 영역을 갖는다.

변환 키 기억부(515)는 제 2 변환부(514)로부터 콘텐츠 ID를 수신한다.

또, 변환 키 기억부(515)는 제 2 변환부(514)로부터 부분정보 PC4를 수신하면 수신한 부분정보 PC4를 저장한다.

변환 키 기억부(515)는 EC4_1[n]의 복호를 지시하는 복호 지시를 변환용 데이터 복호부(516)에 출력한다. 여기서, 복호 지시는 제 2 변환부(514)로부터 수신한 콘텐츠 ID를 포함한다.

변환 키 기억부(515)는 변환용 데이터 복호부(516)로부터 암호화 부분콘텐츠의 판독에 실패하였다는 취지의 명령을 수신하면, 기억하고 있는 복호 키 PC4(=C4[1])을 소거한다.

(16) 변환용 데이터 복호부(516)

변환용 데이터 복호부(516)는 변환 키 기억부(515)로부터 복호 지시를 수신하면, 변환용 데이터 기억부(508)로부터 암호화 부분콘텐츠 EC4_1[1], EC4_1[2], …, EC4_1[N]을 순차 판독한다.

변환용 데이터 복호부(516)는 판독한 암호화 부분콘텐츠 EC4_1[n]을 변환 키 기억부(515)에 기억되어 있는 부분정보 PC4(=C4[1])을 복호 키로 이용하여 복호 알고리즘 D1_1을 실시하여 부분콘텐츠 C4[n]을 생성한다. 즉, C4[n]= D1_1(EC4_1[n], PC4)이다. 또, 복호 알고리즘 D1_1은 암호화 알고리즘 E1_1로 암호화된 암호문을 평문으로 변환하기 위한 알고리즘이다.

변환용 데이터 복호부(516)는 생성한 부분콘텐츠 C4[n]을 제 2 암호화부(517)에 출력한다.

변환용 데이터 복호부(516)는 암호화 부분콘텐츠의 판독에 실패하면, 판독에 실패하였다는 취지의 명령을 매체기록 키 기억부(511) 및 변환 키 기억부(515)에 출력한다.

변환용 데이터 복호부(516)는 이중 암호화 콘텐츠 기록부(521)로부터 제 1 소거지시를 수신하면 복호 한 C4[n]을 소거한다.

이에 따라, 변환용 데이터 복호부(516)는 암호화 부분콘텐츠 EC4_1[n]을 순차 복호함으로써, 변환용 데이터, 즉, 암호화 콘텐츠 EC4_1을 복호 할 수 있다. 또, 변환용 데이터 복호부(516)는 복호 한 부분콘텐츠 C4[1], C4[2], …, C4[n]을 제 2 암호화부(517)에 순차 출력할 수 있다.

이하에 구체적인 동작에 대해서 설명한다.

변환용 데이터 복호부(516)는 카운터 n을 가지고 있다.

변환용 데이터 복호부(516)는 변환 키 기억부(515)로부터 복호 지시를 수신하면, 카운터 n에 1을 설정한다.

변환용 데이터 복호부(516)는 변환용 데이터 기억부(508)로부터 지정의 암호화 콘텐츠의 n번째의 암호화 부분콘텐츠 EC4_1[n]을 판독한다.

변환용 데이터 복호부(516)는 암호화 부분콘텐츠 EC4_1[n]의 판독에 성공하였는지 여부를 판단한다.

성공하였다고 판단하는 경우에는, 변환용 데이터 복호부(516)는 변환 키 기억부(515)로부터 부분정보 PC4를 판독하고, 변환용 데이터 기억부(508)로부터 판독한 암호화 부분콘텐츠 EC4_1[n]을 부분정보 PC4를 복호 키로 이용하여 복호하여 부분콘텐츠 C4[n]을 생성한다. 변환용 데이터 복호부(516)는 생성한 부분콘텐츠 C4[n]을 제 2 암호화부(517)에 출력한다.

변환용 데이터 복호부(516)는 카운터 n에 1을 가산하고, 가산결과를 다시 n으로 하며, 변환용 데이터 기억부(508)로부터 암호화 부분콘텐츠 EC4_1[n]을 판독하고, 판독에 성공하였는지 여부의 판단을 다시 행한다.

실패하였다고 판단하는 경우에는, 변환용 데이터 복호부(516)는 판독에 실패하였다는 취지의 명령을 매체기록 키 기억부(511) 및 변환 키 기억부(515)에 출력한다.

예를 들어, 카운터 n의 값이 N+ 1인 경우에는 암호화 부분콘텐츠 EC4_1[N+ 1]은 존재하지 않으므로 암호화 부분콘텐츠의 판독에는 실패한다. 이에 따라 변환용 데이터 복호부(516)는 통상, 카운터 n의 값이 1 이상 n 이하인 경우에는 암호화 부분콘텐츠 EC4_1[n]이 존재하므로 판독에 성공한다. 즉, 암호화 부분콘텐츠 EC4_1[1], EC4_1[2], …, EC4_1[N]을 순차 판독할 수 있다.

구체 예로, 변환용 데이터 복호부(516)는 변환용 데이터 기억부(508)로부터 콘텐츠 ID「CID_1」에 대응하는 $EC4\_1_{1[}1]$, $EC4\_1_{1[}2]$, …, $EC4_1_{1[}N]$을 순차 판독하면, 순차 복호하여 $C4_{1[}1]$, $C4_{1[}2]$, …, $C4_{1[}N]$을 생성한다. 변환용 데이터 복호부는 생성한 $EC4_{1[}1]$, $EC4_{1[}2]$, …, $EC4_{1[}N]$을 제 2 암호화부(517)에 순차 출력한다.

(17) 제 2 암호화부(517)

제 2 암호화부(517)는 변환용 데이터 복호부(516)로부터 부분콘텐츠C4[1], C4[2], …, C4[N]을 순차 수신한다.

제 2 암호화부(517)는 변환용 데이터 복호부(516)로부터 부분콘텐츠 C4[n]을 수신하면, 매체기록 키 기억부(511)에 기억되어 있는 매체기록 키 K2를 판독하고, 판독한 매체기록 키 K2를 암호키로 이용하여 부분콘텐츠 C4[n]에 암호화 알고리즘 E2를 실시하여 암호화 부분콘텐츠 EC4[n]을 생성한다. 즉, EC4[n]= E2(C4[n], K2)이다. 또, 제 2 암호화부(517)가 이용하는 암호화 알고리즘 E2의 일 예는 AES이다.

제 2 암호화부(517)는 암호화 부분콘텐츠 EC4[n]을 기록/판독부(523)를 거쳐서 휴대형 매체(20)에 이동시킨다. 즉, 제 2 암호화부(517)는 암호화 부분콘텐츠 EC4[n]을 휴대형 매체(20)에 기록하고, 내부에 존재하는 암호화 부분콘텐츠 EC4[n]을 소거한다.

제 2 암호화부(517)는 암호화 부분콘텐츠 EC2[n]의 암호화에 이용하는 이중 암호키의 생성을 지시하는 생성지시를 이중 암호키 생성부(518)에 출력한다. 생성지시의 구체 예는 이중 암호화하는 암호화 부분콘텐츠의 번호를 나타내는 수치이다. 이중 암호화하는 암호화 부분콘텐츠가 EC2[n]인 경우에는 수치 n이 생성지시가 된다.

이에 따라, 제 2 암호화부(517)는 암호화 부분콘텐츠 EC4[1], EC4[2], …, EC4[N]을 휴대형 매체(20)에 순차 이동시킬 수 있다.

구체 예로, 제 2 암호화부(517)는 변환용 데이터 복호부(516)로부터 부분콘텐츠 $C4_{1[}1]$, $C4_{1[}2]$, …, $C4_{1[}N]$을 순차 수신하면, 암호화 부분콘텐츠 $EC4_{1[}1]$, $EC4_{1}[2]$, …, $EC4_{1[}N]$을 순차 생성한다. 제 2 암호화부(517)는 생성한 암호화부분 $EC4_{1[}1]$, $EC4_{1[}2]$, …, $EC4_{1[}N]$을 기록/판독부(523)를 거쳐서 휴대형 매체(20)에 순차 이동시킨다.

(18) 이중 암호키 생성부(518)

이중 암호키 생성부(518)는 제 1 실시 예에서 설명한 이중 암호키 생성부(112)와 동일하므로 설명은 생략한다.

(19) 이중 암호키 기억부(519)

이중 암호키 기억부(519)는 제 1 실시 예에서 설명한 이중 암호키 기억부(113)와 동일하므로 설명은 생략한다.

이하에서, 이중 암호키 기억부(519)에 기억되어 있는 이중 암호키는 K3[n]으로 한다.

(20) 이중 암호화부(520)

이중 암호화부(520)는 이중 암호키 기억부(519)로부터 암호화 지시인 수치 1, 2, …, N을 순차 수신한다.

이중 암호화부(520)는 암호화 지시(수치 n)를 수신하면, 이중 암호키 기억부(519)로부터 이중 암호키 K3[n]을 판독하고, 콘텐츠 판독부(513)로부터 선두 판독지시를 판독한다.

이중 암호화부(520)는 수신한 암호화 지시인 수치 n을 콘텐츠 판독지시로서 콘텐츠 판독부(513)에 출력한다.

이중 암호화부(520)는 콘텐츠 판독부(513)로부터 암호화 부분콘텐츠 EC2[n]을 수신하면, 이중 암호키 K3[n]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[n]에 암호화 알고리즘 E3을 실시하여 이중 암호화 부분콘텐츠 EEC2[n]을 생성한다. 즉, EEC2[n]= E3(EC2[n], K3[n])이다. 또, 이중 암호화부(520)가 이용하는 암호화 알고리즘 E3의 일 예는 AES이다.

이중 암호화부(520)는 이중 암호화 부분콘텐츠EEC2[n]을 생성한 후, 장치 내에 존재하는 이중 암호키 K3[n]을 소거한다. 이에 따라 이중 암호화부(520)의 내부에 존재하는 이중 암호키 K3[n] 및 이중 암호키 기억부(519)에 기억되어 있는 이중 암호키 K3[n]은 소거된다.

이중 암호화부(520)는, 생성한 이중 암호화 부분콘텐츠 EEC2[n]과, 콘텐츠 판독부(513)로부터 판독한 선두 판독지시를 포함하는 기록지시를 이중 암호화 콘텐츠 기록부(521)에 출력한다. 기록지시의 구체 예는 콘텐츠 ID와 이중 암호화 부분콘텐츠에 대응하는 암호화 부분콘텐츠의 번호를 나타내는 수치를 포함하는 정보이다.

이에 따라, 이중 암호화부(520)는 이중 암호화 부분콘텐츠 EEC2[1], EEC2[2], …, EEC2[N]을 순차 생성하고, 이중 암호화 콘텐츠 기록부(521)에 순차 출력할 수 있다.

(21) 이중 암호화 콘텐츠 기록부(521)

이중 암호화 콘텐츠 기록부(521)는 제 1 실시 예에서 설명한 이중 암호화 콘텐츠 기록부(115)와 동일하나, 제 1 소거지시의 출력 처가 다르다.

이중 암호화 콘텐츠 기록부(521)는 제 1 소거지시를 콘텐츠 판독부(513), 변환용 데이터 복호부(516) 및 이중 암호화부(520)에 출력한다.

(22) 제 2 복호부(522)

제 2 복호부(522)는 제 1 실시 예에서 설명한 제 2 복호부(116)와 동일하므로 설명은 생략한다.

(23) 기록/판독부(523)

기록/판독부(523)는 제 1 실시 예에서 설명한 기록/판독부(117)와 동일하므로 설명은 생략한다.

(24) 입력부(524)

입력부(524)는 제 1 실시 예에서 설명한 입력부(524)와 동일하므로 설명은 생략한다.

2.3 저작권 보호시스템(2)의 동작 개요

여기서는 저작권 보호시스템(2)의 동작의 개요에 대해서 도 17에 도시한 흐름도를 사용하여 설명한다.

콘텐츠 공급장치(11)는 콘텐츠 C2를 방송하고(스텝 S 600), 기록재생장치(50)는 콘텐츠 C2를 수신한다(스텝 S 605).

기록재생장치(50)는 콘텐츠 기록처리를 행하고, 수신한 콘텐츠 C2에 대해서 암호화 콘텐츠 EC2 및 EC4를 생성하여 각각을 기록한다(스텝 S 610).

기록재생장치(50)는 콘텐츠 C2의 재생지시를 수신하면, 장치기록 키 K1을 복호 키로 이용하여 기록하고 있는 암호화 콘텐츠 EC2를 복호하여 콘텐츠 C2를 생성하고, 생성한 콘텐츠 C2를 디코드하여 영상신호와 음성신호를 생성하며, 생성한 영상신호를 모니터(12)에 출력하고, 생성한 음성신호를 스피커(13)에 출력함으로써 콘텐츠 C2를 재생한다(스텝 S 615).

모니터(12)는 기록재생장치(50)로부터 영상신호를 수신하면, 수신한 영상신호에 의거하여 영상을 출력하고, 스피커(13)는 기록재생장치(50)로부터 음성신호를 수신하면, 수신한 음성신호에 의거하여 음성을 출력한다(스텝 S 640).

기록재생장치(50)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 무브 지시를 수신하면, 제 1 이동처리를 행하고, 기록하고 있는 콘텐츠를 메모리카드 슬롯에 삽입된 휴대형 매체(20)에 무브한다(스텝 S 620). 이때, 휴대형 매체(20)는 부분콘텐츠 C2[n](n = 1, 2, …, N이다. 이하 동일)을 MPEG-4 규격에 따라서 압축 부호화된 부분콘텐츠 C4[n]이 매체기록 키 K2로 암호화된 암호화 부분콘텐츠 EC4[n], 암호화 매체기록 키 EK2, 이중 암호키 K3[n] 및 콘텐츠 ID를 기억하고 있다.

휴대정보 단말(30)은 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 매체 고유 키 K0을 생성하고, 생성한 매체 고유 키 K0을 이용하여 휴대형 매체(20)에 기록되어 있는 암호화 매체 키 EK2를 복호하여 매체기록 키 K2를 생성한다. 휴대정보 단말(30)은 생성한 매체기록 키 K2를 복호 키로 이용하여 암호화 부분콘텐츠 EC4[n]을 복호하여 순차 부분콘텐츠 C4[n]을 생성한다. 휴대정보 단말(30)은 생성한 부분콘텐츠 C4[n]을 순차 디코드하여 영상신호 및 음성신호를 생성하고, 생성한 영상신호 및 음성신호의 각각에 의거하여 영상 및 음성을 출력함으로써 변환콘텐츠 C4를 재생한다(스텝 S 625).

기록재생장치(50)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 무브 백 지시를 수신하면, 제 2 이동처리를 행하여, 휴대형 매체(20)가 기록하고 있는 콘텐츠를 당해 기록재생장치(50)에 무브한다(스텝 S 630). 이때, 기록재생장치(50)는 MPEG-2 규격에 따라서 압축 부호화된 부분콘텐츠 C2[n](n = 1, 2, …, N이다. 이하 동일)이 장치기록 키 K1으로 암호화된 암호화 부분콘텐츠 EC2[n]을 기억하고 있다.

기록재생장치(50)는 콘텐츠 C2의 재생지시를 수신하면, 장치기록 키 K1을 암호 키로 이용하여 기록하고 있는 암호화 콘텐츠 EC2를 복호하여 콘텐츠 C2를 생성하고, 생성한 콘텐츠 C2를 디코드하여 영상신호와 음성신호를 생성하여, 생성한 영상신호를 모니터(12)에 출력하고, 생성한 음성신호를 스피커(13)에 출력함으로써 콘텐츠 C2를 재생한다(스텝 S 635). 모니터(12) 및 스피커(13)는 기록재생장치(50)로부터 수신한 영상신호 및 음성신호의 각각에 의거하여 영상 및 음성을 출력한다(스텝 S 640).

2.4 콘텐츠 기록처리의 동작

여기서는 도 17의 스텝 S 610에서 행해지는 콘텐츠 기록처리의 동작에 대해서 도 18에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(50)의 제 1 암호화부(503)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신하면, 재생시간 길이가 소정 시간 내(예를 들어 45초 이내)가 되도록 콘텐츠 C2의 선두로부터 분할하여 부분콘텐츠 C2[1], C2[2], …, C2[N]을 생성한다. 또, 제 1 암호화부(503)는 장치기록 키 기억부(502)로부터 장치기록 키 K1을 판독하고, 장치기록 키 K1을 암호키로 이용하여 부분콘텐츠 C2[n]의 각각을 암호화하여 암호화 부분콘텐츠 EC2[n]을 생성하며, 생성한 암호화 부분콘텐츠 EC2[n]을 암호화 콘텐츠 기록부(504)에 순차 저장한다(스텝 S 700).

기록재생장치(50)의 제 1 변환부(505)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신하면, 수신한 콘텐츠 C2를 다운 컨버트 하여 변환콘텐츠 C4를 생성한다(스텝 S 705).

제 1 변환부(505)는 재생시간 길이가 소정 시간 내(예를 들면 45초 이내)가 되도록 변환콘텐츠 C4의 선두로부터 분할하고, 부분변환콘텐츠 C4[1], C4[2], …, C4[N]을 생성한다(스텝 S 710).

기록재생장치(50)의 부분정보 선택부(506)는 제 1 변환부(505)로부터 선택지시를 수신하면, 제 1 변환부(505)에 기억되어 있는 변환 콘텐츠 C4의 선두에 위치하는 부분콘텐츠 C4[1]을 판독하여, 판독한 부분콘텐츠 C4[1]을 부분정보 PC4로 한다(스텝 S 715).

기록재생장치(50)의 변환용 데이터 암호화부(507)는 부분정보 선택부(506)로부터 부분정보 PC4를 수신하면, 제 1 변환부(505)로부터 부분콘텐츠 C4[n]을 순차 판독한다. 변환용 데이터 암호화부(507)는 수신한 부분정보 PC4를 암호키로 이용하여 판독한 부분콘텐츠 C4[n]을 암호화하여 암호화 부분콘텐츠 EC4_1[n]을 생성한다(스텝 S 720). 변환용 데이터 암호화부(507)는 생성한 암호화 부분콘텐츠 EC4_1[1], EC4_1[2], … , EC4_1[N]을 변환용 데이터 기억부(508)에 순차 저장한다(스텝 S 725).

기록재생장치(50)의 제 1 암호화부(503)는 내부에 존재하는 콘텐츠 C2를 소거하고, 제 1 변환부(505)는 내부에 존재하는 콘텐츠 C2 및 부분변환콘텐츠C4[n]을 소거하며, 부분정보 선택부(506)는 내부에 존재하는 PC4를 소거하고, 변환용 데이터 암호화부(507)는 내부에 존재하는 부분콘텐츠 C4[n] 및 부분정보 PC4를 소거한다(스텝 S 730).

2.5 제 1 이동처리 동작

여기서는 도 17의 스텝 S 620에서 행해지는 제 1 이동처리 동작에 대해서 도 19에 도시한 흐름도를 이용하여 설명한다.

기록재생장치(50)는 휴대형 매체(20)가 메모리카드 슬롯에 삽입된 상태에서 입력부(524)에서 무브 지시를 수신하면(스텝 S 750), 콘텐츠 이동처리를 행하여, 기록하고 있는 콘텐츠를 휴대형 매체(20)에 이동한다(스텝 S 755). 이때, 기록재생장치(50)는 콘텐츠 이동처리의 동작 중에 콘텐츠 ID, 암호화 매체기록 키 EK2, 암호화 부분콘텐츠 EC4[n](n = 1, 2, …, N이다. 이하 동일) 및 이중 암호키 K3[n]을 휴대형 매체(20)에 출력한다.

휴대형 매체(20)는 기록재생장치(50)로부터 콘텐츠 ID를 수신하면, 수신한 콘텐츠 ID를 콘텐츠 ID 기억영역(213)에 기록한다(스텝 S 760).

휴대형 매체(20)는 기록재생장치(50)로부터 암호화 매체기록 키 EK2를 수신하면, 수신한 암호화 매체기록 키 EK2를 매체기록 키 기억영역(211)에 기록한다(스텝 S 765).

휴대형 매체(20)는 기록재생장치(50)로부터 암호화 부분콘텐츠 EC4[n]을 수신하면, 수신한 암호화 부분콘텐츠 EC4[n]을 암호화 콘텐츠 기억영역(210)에 기록한다(스텝 S 770).

휴대형 매체(20)는 기록재생장치(50)로부터 이중 암호키 K3[n]을 수신하면, 수신한 이중 암호키 K3[n]을 이중 암호키 기억영역(212)에 기록한다(스텝 S 775).

2.6 콘텐츠 이동처리의 동작

여기서는 도 19의 스텝 S 755에서 실행되는 콘텐츠 이동처리의 동작에 대해서 도 20 및 도 21에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(50)의 매체기록 키 생성부(510)는 입력부(524)로부터 무브 지시를 수신하고, 매체기록 키 K2를 생성한다(스텝 S 800).

기록재생장치(50)의 매체기록 키 기억부(511)는 매체기록 키 생성부(510)로부터 매체기록 키 K2와 무브 지시를 수신하면, 수신한 K2를 내부의 키 기억영역에 저장한다(스텝 S 805). 또, 매체기록 키 기억부(511)는 수신한 무브 지시에 포함되는 콘텐츠 ID를 휴대형 매체(20)에 기록한다(스텝 S 810). 이때, 휴대형 매체(20)는 도 19에 도시한 스텝 S 760을 행한다.

매체기록 키 기억부(511)는 휴대형 매체(20)로부터 매체 ID와 MKB를 판독하고, 판독한 매체 ID와 MKB와 미리 기억하고 있는 디바이스 키 DK1을 이용하여 매체 고유 키 K0을 생성하여, 생성한 매체 고유 키 K0을 이용하여 매체기록 키 K2를 암호화하여 암호화 매체기록 키 EK2를 생성한다(스텝 S 815).

매체기록 키 기억부(511)는 생성한 암호화 매체기록 키 EK2를 휴대형 매체(20)에 기록한다(스텝 S 820). 이때, 휴대형 매체(20)는 도 19에 도시한 스텝 S 765를 행한다.

매체기록 키 기억부(511)는 기록완료 후, 생성한 암호화 매체기록 키 EK2를 소거한다(스텝 S 825).

기록재생장치(50)의 제 1 복호부(512)는 매체기록 키 기억부(511)로부터 무브 지시를 수신하면, 장치기록 키 K1을 판독한다(스텝 S 830).

제 1 복호부(512)는 암호화 콘텐츠 기록부(504)로부터 선두 판독지시를 콘텐츠 판독부(513)에 출력한다. 콘텐츠 판독부(513)는 제 1 복호부(512)로부터 선두 판독지시를 수신하면, 선두 판독지시에 지정된 암호화 콘텐츠 EC2의 선두의 암호화 부분콘텐츠 EC2[1]을 판독한다(스텝 S 835).

제 1 복호부(512)는 콘텐츠 판독부(513)로부터 암호화 부분콘텐츠 EC2[1]을 수신하면, 스텝 S 830에서 판독한 장치기록 키 K1을 복호 키로 이용하여 수신한 암호화 부분콘텐츠 EC2[1]을 복호하여 부분콘텐츠 C2[1]을 생성한다(스텝 S 840).

기록재생장치(50)의 제 2 변환부(514)는 제 1 복호부(512)로부터 부분콘텐츠C2[1]과 콘텐츠 ID를 수신하면, 수신한 콘텐츠 C2[1]을 다운 컨버트 하여 부분콘텐츠 C4[1]을 생성한다(스텝 S 845).

제 2 변환부(514)는 생성한 부분콘텐츠 C4[1]을 부분정보 PC4로 변환 키 기억부(515)에 저장한다(스텝 S 850).

변환용 데이터 복호부(516)는 변환 키 기억부(515)로부터 복호 지시를 수신하면 카운터 n에 1을 설정한다(스텝 S 855).

변환용 데이터 복호부(516)는 변환용 데이터 기억부(508)로부터 지정된 암호화 콘텐츠의 n번째의 암호화 부분콘텐츠 EC4_1[n]을 판독한다(스텝 S 860).

변환용 데이터 복호부(516)는 암호화 부분콘텐츠 EC4_1[n]의 판독에 성공하였는지 여부를 판단한다(스텝 S 865).

성공하였다고 판단하는 경우에는(스텝 S 865에 있어서의 「YES」), 기록재생장치(50)는 부분콘텐츠 이동처리를 행하고, 판독한 암호화 부분콘텐츠 EC2[n]에서 생성된 암호화 부분콘텐츠 EC4[n]을 기록매체에 기록한다(스텝 S 870).

변환용 데이터 복호부(516)는 카운터 n에 1을 가산하고, 가산결과를 다시 n으로 한다(스텝 S 875). 변환용 데이터 기억부(508)로부터 암호화 부분콘텐츠 EC4_1[n]을 판독하고(스텝 S 880), 다시 스텝 S 865 이후를 실행한다.

실패하였다고 판단하는 경우에는(스텝 S 865에 있어서의 「NO」), 변환용 데이터 복호부(516)는 판독에 실패하였다는 취지의 명령을 매체기록 키 기억부(511) 및 변환 키 기억부(515)에 출력하고, 매체기록 키 기억부(511)는 매체기록 키 K2를 소거하며, 변환 키 기억부(515)는 부분정보 PC4를 소거한다(스텝 S 885).

2.7 부분콘텐츠 이동처리의 동작

여기서는 도 21의 스텝 S 870에서 실행되는 부분콘텐츠 이동처리의 동작에 대해서 도 22에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(50)의 변환용 데이터 복호부(516)는 변환 키 기억부(515)로부터 부분정보 PC4를 판독하고, 변환용 데이터 기억부(508)로부터 판독한 암호화 부분콘텐츠 EC4_1[n]을 부분정보 PC4를 복호 키로 이용하여 복호하고, 부분콘텐츠 C4[n]을 생성한다(스텝 S 900).

기록재생장치(50)의 제 2 암호화부(517)는 변환용 데이터 복호부(516)로부터 부분콘텐츠 C4[n]을 수신하면, 매체기록 키 기억부(511)에 기억되어 있는 매체기록 키 K2를 판독하고, 판독한 매체기록 키 K2를 암호키로 이용하여 부분콘텐츠 C4[n]을 암호화하여 암호화 부분콘텐츠 EC4[n]을 생성한다(스텝 S 905).

제 2 암호화부(517)는 암호화 부분콘텐츠 EC4[n]을 휴대형 매체(20)에 기록한다(스텝 S 910). 이때, 휴대형 매체(20)는 도 19에 도시한 스텝 S 770을 행한다. 제 2 암호화부(517)는 내부의 존재하는 암호화 부분콘텐츠 EC4[n]을 소거한다.

이중 암호키 생성부(518)는 제 2 암호화부(517)로부터 생성지시(수치 n)를 수신하면, 이중 암호키 K3[n]을 생성한다(스텝 S 915).

이중 암호키 생성부(518)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(519) 및 휴대형 매체(20)의 이중 암호키 기억영역(212)에 저장한다(스텝 S 920). 이때, 휴대형 매체(20)는 도 19에 도시한 스텝 S 775를 행한다.

이중 암호화부(520)는 암호화 지시(수치 n)를 수신하면, 이중 암호키 기억부(519)로부터 이중 암호키 K3[n]을 판독하고, 콘텐츠 판독부(513)로부터 선두 판독지시를 판독한다. 이중 암호화부(520)는 수신한 암호화 지시인 수치 n을 콘텐츠 판독지시로 콘텐츠 판독부(513)에 출력한다. 이중 암호화부(520)는 콘텐츠 판독부(513)로부터 암호화 부분콘텐츠 EC2[n]을 수신하면, 이중 암호키 K3[n]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[n]에 암호화 알고리즘 E3을 실시하여 이중 암호화 부분콘텐츠 EEC2[n]을 생성하고(스텝 S 925), 이중 암호키 K3[n]을 소거한다(스텝 S 930).

기록재생장치(50)의 이중 암호화 콘텐츠 기록부(521)는 이중 암호화부(520)로부터 기록지시와 이중 암호화 부분콘텐츠 EEC2[n]을 수신하면, 수신한 EEC2[n]을, 암호화 콘텐츠 기록부(504)에 기억하고 또한 기록지시에 포함되는 콘텐츠 ID 및 암호화 부분콘텐츠의 번호에 대응하는 EC2[n]에 대하여 덮어씀으로써, 암호화 콘텐츠 기록부(504)에 기록한다(스텝 S 935).

이중 암호화 콘텐츠 기록부(521)는 콘텐츠 판독부(513), 변환용 데이터 복호부(516) 및 이중 암호화부(520)에 제 1 소거지시를 출력한다. 콘텐츠 판독부(513)는 제 1 소거지시를 수신하면, 암호화 콘텐츠 기록부(504)로부터 판독한 암호화 부분콘텐츠 EC2[n]을 소거한다. 변환용 데이터 복호부(516)는 제 1 소거지시를 수신하면, 복호 한 C4[n]을 소거한다. 이중 암호화부(520)는 제 1 소거지시를 수신하면, 암호화 콘텐츠 EC2[n]을 소거한다(스텝 S 940).

2.8 제 2 이동처리의 동작

도 17의 스텝 S 630에서 실행되는 제 2 이동처리는 제 1 실시 예에 있어서의 도 12에 도시한 흐름도와 동일한 동작을 하므로 설명은 생략한다.

2.9 콘텐츠 복호처리의 동작

도 17의 스텝 S 630에서 행해지는 제 2 이동처리 동작 중에 기록재생장치(50)에서 행해지는 콘텐츠 복호처리는 제 1 실시 예에서의 도 13에 도시한 흐름도와 동일한 동작이므로 설명은 생략한다.

2.10 제 2 실시 예의 변형 예

제 2 실시 예에서, 변환콘텐츠 C4를 부분변환콘텐츠C4[1], C4[2], …, C4[n]으로 분할하고, 각 부분변환콘텐츠 C4[n]을 암호화하여 암호화 콘텐츠 EC4_1[n]을 생성하여 기록하였으나, 이에 한정되지는 않는다.

기록재생장치는 부분정보 PC4(= C4[1])를 암호키로 이용하여 변환콘텐츠 C4에 암호화 알고리즘 E1_2를 실시하여 암호화 변환콘텐츠 EC4_2를 생성하여 기록해도 된다. 여기서 EC4_2 = E1_2(C4, PC4)이다. 암호화 알고리즘 E1_2의 일 예는 AES이다. 또, AES는 공지이므로 설명은 생략한다.

이 경우에 있어서의 기록재생장치(50a)의 구성 및 동작에 대해서 상기에 설명한 기록재생장치(50)와의 차이점을 중심으로 설명한다.

기록재생장치(50a)의 구성요소는, 도 23에 도시한 바와 같이, 기록재생장치(50)의 구성요소 중, 제 1 변환부(505), 변환용 데이터 암호화부(507), 변환용 데이터 기억부(508) 및 변환용 데이터 복호부(516)가 후술하는 제 1 변환부(505a), 부분정보 선택부(506a), 변환용 데이터 암호화부(507a), 변환용 데이터 기억부(508a) 및 변환용 데이터 복호부(516a)로 변경된다.

이하, 제 1 변환부(505a), 부분정보 선택부(506a), 변환용 데이터 암호화부(507a), 변환용 데이터 기억부(508a), 및 변환용 데이터 복호부(516a)에 대해서 설명한다. 또, 다른 구성요소에 대해서는 제 2 실시 예에 설명한 각 구성요소의 동작 및 기능과 동일하므로 여기에서 설명은 생략한다.

(1) 제 1 변환부(505a)

제 1 변환부(505a)는 구체적으로는 MPEG-2의 데이터를 MPEG-4로 변환하기 위한 다운 컨버터 등으로 구성된다.

제 1 변환부(505a)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신하면, 수신한 콘텐츠 C2를 MPEG-4로 압축 변환하여 변환콘텐츠 C4를 생성한다.

제 1 변환부(505a)는 변환콘텐츠 C4를 일시 기억하고, 선택지시를 부분정보 선택부(506a)에 출력한다.

또, 제 1 변환부(505a)는 변환콘텐츠 C4의 생성 후, 콘텐츠 C2를 소거한다.

또, 제 1 변환부(505a)는 변환용 데이터 암호화부(507a)로부터 변환데이터 소거지시를 수신하면, 일시 기억하고 있는 변환콘텐츠 C4를 소거한다.

(2) 부분정보 선택부(506a)

부분정보 선택부(506a)는 제 1 변환부(505a)로부터 선택지시를 수신하면, 제 1 변환부(505)에 기억되어 있는 변환콘텐츠 C4를 판독하고, 판독한 변환콘텐츠 C4의 선두위치로부터 재생시간 길이가 소정 시간 내(예를 들어 45초)인 부분콘텐츠 C4[1]을 취득한다.

부분정보 선택부(506a)는 취득한 부분콘텐츠 C4[1]을 부분정보 PC4로 변환용 데이터 암호화부(507a)에 출력한다.

부분정보 선택부(506a)는 부분정보 PC4를 출력 후, 내부에 존재하는 변환콘텐츠 C4 및 부분정보 PC4를 소거한다.

(3) 변환용 데이터 암호화부(507a)

변환용 데이터 암호화부(507a)는 부분정보 선택부(506a)로부터 부분정보 PC4를 수신하면, 제 1 변환부(505a)로부터 변환콘텐츠 C4를 판독한다.

변환용 데이터 암호화부(507a)는 판독한 변환콘텐츠 C4를 수신한 부분정보 PC4를 암호키로 이용하여 암호화 알고리즘 E1_2를 실시하여 암호화 변환콘텐츠 EC4_2를 생성한다.

변환용 데이터 암호화부(507a)는 생성한 암호화 변환콘텐츠 EC4_2를 변환용 데이터 기억부(508a)에 저장한다.

변환용 데이터 암호화부(507a)는 암호화 변환콘텐츠 EC4_2의 저장이 완료하면 내부에 존재하는 변환콘텐츠 C4 및 부분정보 PC4를 소거한다. 또, 변환용 데이터 암호화부(507a)는 변환 데이터 소거지시를 제 1 변환부(505a)에 출력한다.

(4) 변환용 데이터 기억부(508a)

변환용 데이터 기억부(508a)는 구체적으로는 하드디스크 유닛이고, 암호화 변환콘텐츠 EC4_1을 기억하기 위한 영역을 구비하고 있다.

변환용 데이터 기억부(508a)는 변환용 데이터 암호화부(507a)로부터 암호화 변환콘텐츠 EC4_2를 수신하면, 수신한 암호화 변환콘텐츠 EC4_2를 저장한다.

암호화 변환콘텐츠 EC4_2에는 암호화 콘텐츠 EC4_2의 고화질 콘텐츠인 EC2에 할당된 콘텐츠 ID가 대응되어 있다.

(5) 변환용 데이터 복호부(516a)

변환용 데이터 복호부(516a)는 변환 키 기억부(515)로부터 복호 지시를 수신하면, 변환용 데이터 기억부(508a)로부터 암호화 변환콘텐츠 EC4_2를 판독한다.

변환용 데이터 복호부(516a)는 판독한 암호화 변환콘텐츠 EC4_2를 변환 키 기억부(515)에 기억되어 있는 부분정보 PC4(=C4[1])를 복호 키로 이용하여 복호 알고리즘 D1_2를 실시하여 변환콘텐츠 C4를 생성한다. 즉, C4 = D1_2(EC4_2, PC4)이다. 또, 복호 알고리즘 D1_2는 암호화 알고리즘 E1_2로 암호화된 암호문을 평문으로 변환하기 위한 알고리즘이다.

변환용 데이터 복호부(516a)는 재생시간 길이가 소정 시간 내(예를 들어 45초 이내)가 되도록 변환콘텐츠 C4의 선두로부터 분할하여, 부분변환 콘텐츠 C4[1], C4[2], C4[3], …, C4[N]을 생성한다. 부분변환콘텐츠 C4[N](n = 1, 2, …, N이다. 이하 동일)의 재생시간 길이는 소정 시간 내(45초 이내)이다.

변환용 데이터 복호부(516a)는 생성한 부분변환콘텐츠 C4[n]을 순차 제 2 암호화부(517)에 출력한다.

변환용 데이터 복호부(516)는 이중 암호화 콘텐츠 기록부(521)로부터 제 1 소거지시를 수신하면, 제 2 암호화부(517)에 출력한 C4[n]을 소거한다.

또, 변환용 데이터 복호부(516a)는 암호화 변환콘텐츠 EC4_2를 복호하여, 변환콘텐츠 C4를 생성한 후, 내부에 존재하는 암호화 변환콘텐츠 EC4_2를 소거한다.

변환용 데이터 복호부(516a)는 부분콘텐츠 C4[1], C4[2], …, C4[N]을 제 2 암호화부(517)에 출력한 후, 모든 부분콘텐츠의 출력이 완료하였다는 취지의 명령을 매체기록 키 기억부(511) 및 변환 키 기억부(515)에 출력한다. 또, 이때, 매체기록 키 기억부(511) 및 변환 키 기억부(515)에서는 당해 명령을 수신하면, 매체기록 키 기억부(511)는 매체기록 키 K2를 소거하고, 변환 키 기억부(515)는 부분정보 PC4를 소거한다.

이에 따라, 변환용 데이터 복호부(516a)는 부분콘텐츠 C4[1], C4[2], …, C4[N]을 제 2 암호화부(517)에 순차 출력할 수 있다.

(6) 콘텐츠 기록시의 기록재생장치(50a)의 동작

기록재생장치(50a)는 콘텐츠를 기록할 때, 도 17의 스텝 S 610에서 행해지는 동작, 즉, 도 18에 도시한 콘텐츠 기록처리를 행하는 대신, 도 24에 도시한 기록처리의 동작을 행한다. 이하, 기록처리의 동작을 도 24에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(50a)의 제 1 암호화부(503)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신하면, 장치기록 키 기억부(502)로부터 장치기록 키 K1을 판독하고, 수신한 콘텐츠 C2를 장치기록 키 K1로 암호화하여 암호화 콘텐츠 EC2를 생성하여, 암호화 콘텐츠 기록부(504)에 기록한다(스텝 S 1000). 또, 제 1 암호화부(503)의 상세한 동작에 대해서는 제 2 실시 예에서 설명하였으므로 여기서는 상세한 설명은 생략한다.

기록재생장치(50a)의 제 1 변환부(505a)는 콘텐츠 수신부(501)로부터 콘텐츠 C2를 수신하면 수신한 콘텐츠 C2를 다운컨버트 하여 변환콘텐츠 C4를 생성한다(스텝 S 1005).

기록재생장치(50a)의 부분정보 선택부(506a)는 제 1 변환부(505a)로부터 선택지시를 수신하면, 변환콘텐츠 C4의 선두에 위치하는 부분콘텐츠 C4[1]을 취득하고, 취득한 부분콘텐츠 C4[1]을 부분정보 PC4로 한다. 기록재생장치(50a)의 변환용 데이터 암호화부(507a)는 부분정보 선택부(506a)로부터 부분정보 PC4를 수신하면, 제 1 변환부(505a)로부터 변환콘텐츠 C4를 판독한다. 변환용 데이터 암호화부(507a)는 수신한 부분정보 PC4를 암호키로 이용하여 판독한 변환콘텐츠 C4를 암호화하여 암호화 변환콘텐츠 EC4_2를 생성한다(스텝 S 1010).

변환용 데이터 암호화부(507a)는 생성한 암호화 부분콘텐츠 EC4_2를 변환용 데이터 기억부(508a)에 저장한다(스텝 S 1015).

기록재생장치(50a)의 제 1 암호화부(503)는 내부에 존재하는 콘텐츠 C2를 소거하고, 제 1 변환부(505a)는 내부에 존재하는 콘텐츠 C2 및 변환콘텐츠 C4를 소거하며, 부분정보 선택부(506a)는 내부에 존재하는 PC4(= C4[1])을 소거하고, 변환용 데이터 암호화부(507a)는 내부에 존재하는 부분콘텐츠 C4 및 부분정보 PC4를 소거한다(스텝 S 1020).

(7) 무브 지시의 수신시의 기록재생장치(50a)의 동작

기록재생장치(50a)는 휴대형 매체(20)에 콘텐츠를 이동할 때, 도 19의 스텝 S 755에서 행해지는 동작, 즉, 도 20 및 도 21에 도시한 콘텐츠 이동처리를 행하는 대신, 도 25에 도시한 이동처리의 동작을 행한다. 이하, 이동처리의 동작을 도 25에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(50a)의 매체기록 키 생성부(510)는 입력부(524)로부터 무브 지시를 수신하면, 매체기록 키 K2를 생성한다. 기록재생장치(50a)의 매체기록 키 기억부(511)는 매체기록 키 생성부(510)로부터 매체기록 키 K2와 무브 지시를 수신하면, 수신한 K2를 내부의 키 기억영역에 저장한다(스텝 S 1100).

또, 매체기록 키 기억부(511)는 수신한 무브 지시에 포함되는 콘텐츠 ID를 휴대형 매체(20)에 기록한다(스텝 S 1105).

기록재생장치(50a)의 제 1 복호부(512)는 매체기록 키 기억부(511)로부터 무브 지시를 수신하면, 장치기록 키 K1을 판독하고, 판독한 K1을 이용하여 암호화 콘텐츠 EC2의 선두블록에 위치하는 암호화 부분콘텐츠 EC2[1]을 복호하여 부분정보 PC2(= C2[1])을 생성한다(스텝 S 1110).

기록재생장치(50a)는 변환처리를 행하여 변환콘텐츠 C4를 생성한다(스텝 S 1115).

기록재생장치(50a)의 제 2 암호화부(517)는 변환콘텐츠 C4를 매체기록 키 K2로 암호화하여 암호화 콘텐츠 EC4를 생성하고, 생성한 암호화 콘텐츠 EC4를 휴대형 매체(20)의 암호화 콘텐츠 기억영역(210)에 기록한다(스텝 S 1120). 또, 당해 스텝의 상세한 동작은 후술한다.

기록재생장치(50a)는 장치 내에 존재하는 부분정보 PC2, PC4 및 변환콘텐츠 C4를 소거한다(스텝 S 1125).

매체기록 키 기억부(511)는 매체 고유 키 K0을 생성하고, 생성한 매체 고유 키K0을 이용하여 매체기록 키 K2를 암호화하여 암호화 매체기록 키 EK2를 생성하며, 생성한 EK2를 휴대형 매체(20)의 매체기록 키 기억영역(211)에 기록한다(스텝 S 1130).

기록재생장치(50a)는 장치 내에 존재하는 매체기록 키 K2 및 암호화 매체기록 키 EK2를 소거한다(스텝 S 1135).

(8) 변환처리의 동작

여기서는 도 25의 스텝 S 1115에서 행해지는 변환처리의 동작에 대해서 도 26에 도시한 흐름도를 사용하여 설명한다.

기록재생장치(50a)의 제 2 변환부(514)는 부분정보 PC2를 다운 컨버트 하여 부분정보 PC4(= C4[1])를 생성한다(스텝 S 1200). 제 2 변환부(514)는 생성한 부분정보 PC4를 변환 키 기억부(515)에 저장한다.

기록재생장치(50a)의 변환용 데이터 복호부(516a)는 변환 키 기억부(515)로부터 복호 지시를 수신하면, 부분정보 PC4를 복호 키로 하여 암호화 변환콘텐츠 EC4_2를 복호하여 변환콘텐츠 C4를 생성한다(스텝 S 1205). 변환용 데이터 복호부(516a)는 재생시간 길이가 소정 시간 내(예를 들어 45초 이내)가 되도록 변환콘텐츠 C4의 선두로부터 분할하여 부분변환 콘텐츠 C4[1], C4[2], C4[3], …, C4[N]을 생성한다.

(9) 부분변환 콘텐츠의 암호화 시의 기록재생장치(50a)의 동작

여기서는 도 25에 도시한 스텝 S 1120의 상세한 동작에 대해서 도 27에 도시한 흐름도를 이용하여 설명한다.

기록재생장치(50a)는 n = 1, 2, …, N에 대해서 스텝 S 1305로부터 스텝 S 1340까지를 반복한다(스텝 S 1300).

기록재생장치(50a)의 제 2 암호화부(517)는 변환용 데이터 복호부(516a)로부터 부분콘텐츠 C4[n]을 수신하면, 매체기록 키 기억부(511)에 기억되어 있는 매체기록 키 K2를 판독하고, 판독한 매체기록 키 K2를 암호키로 이용하여 부분콘텐츠 C4[n]을 암호화하여 암호화 부분콘텐츠 EC4[n]을 생성한다(스텝 S 1305).

제 2 암호화부(517)는 암호화 부분콘텐츠 EC4[n]을 휴대형 매체(20)에 기록한다(스텝 S 1310). 제 2 암호화부(517)는 내부에 존재하는 암호화 부분콘텐츠 EC4[n]을 소거한다.

이중 암호키 생성부(518)는 제 2 암호화부(517)로부터 생성지시(수치 n)를 수신하면, 이중 암호키 K3[n]을 생성한다(스텝 S 1315).

이중 암호키 생성부(518)는 생성한 이중 암호키 K3[n]을 이중 암호키 기억부(519) 및 휴대형 매체(20)의 이중 암호키 기억영역(212)에 저장하다(스텝 S 1320).

이중 암호화부(520)는 암호화 지시(수치 n)를 수신하면, 이중 암호키 기억부(519)로부터 이중 암호키 K3[n]을 판독하고, 콘텐츠 판독부(513)로부터 선두 판독지시를 판독한다. 이중 암호화부(520)는 수신한 암호화 지시인 수치 n을 콘텐츠 판독지시로 콘텐츠 판독부(513)에 출력한다. 이중 암호화부(520)는 콘텐츠 판독부(513)로부터 암호화 부분콘텐츠 EC2[n]을 수신하면, 이중 암호키 K3[n]을 암호키로 이용하여 암호화 부분콘텐츠 EC2[n]에, 암호화 알고리즘 E3을 실시하여 이중 암호화 부분콘텐츠 EEC2[n]을 생성하고, 이중 암호키 K3[n]을 소거한다(스텝 S 1325).

기록재생장치(50a)의 이중 암호화 콘텐츠 기록부(521)는 이중 암호화부(520)로부터 기록지시와 이중 암호화 부분콘텐츠 EEC2[n]을 수신하면, 수신한 EEC2[n]을, 암호화 콘텐츠 기록부(504)에 기억하고 또한 기록지시에 포함되는 콘텐츠 ID 및 암호화 부분콘텐츠의 번호에 대응하는 EC2[n]에 대해서 덮어씀으로써, 암호화 콘텐츠 기록부(504)에 기록한다(스텝 S 1330).

이중 암호화 콘텐츠 기록부(521)는 콘텐츠 판독부(513), 변환용 데이터 복호부(516a), 제 2 암호화부(517), 이중 암호키 기억부(519) 및 이중 암호화부(520)에 제 1 소거지시를 출력한다. 콘텐츠 판독부(513)는 제 1 소거지시를 수신하면, 암호화 콘텐츠 기록부(504)로부터 판독한 암호화 부분콘텐츠 EC2[n]을 소거한다. 변환용 데이터 복호부(516a)는 제 1 소거지시를 수신하면 제 2 암호화부(517)에 출력한 C4[n]을 소거한다. 제 2 암호화부(517)는 제 1 소거지시를 수신하면, 암호화 부분콘텐츠 EC4[n]을 소거한다. 이중 암호키 기억부(519)는 제 1 소거지시를 수신하면, 이중 암호키 K3[n]을 소거한다. 이중 암호화부(520)는 제 1 소거지시를 수신하면, 암호화콘텐츠 EC2[n]을 소거한다(스텝 S 1335).

3. 그 밖의 변형 예

또, 본 발명을 상기 실시 예에 의거하여 설명하였지만, 본 발명은 상기 실시 예에 한정되는 것은 아니다. 이하와 같은 경우도 본 발명에 포함된다.

(1) 상기 실시 예에서는 기록재생장치로부터 휴대형 매체로 콘텐츠를 이동하는 구성을 구비하고 있으나, 본 발명은 기록재생장치로부터 휴대형 매체로의 콘텐츠의 이동에 한정되지 않으며, 예를 들어 기록재생장치로부터 다른 기록재생장치로 콘텐츠를 이동하는 구성이라도 된다. 이 경우에서의 시스템의 구성의 일 예를 저작권 보호시스템(1)의 변형 예로서 도 28에 저작권 보호시스템(3)으로 도시한다. 기록재생장치 10으로부터 기록재생장치 1000으로 콘텐츠를 이동할 때, 이동 처가 되는 기록재생장치(1000)가 정규의 휴대형 매체인가 여부를 확인(인증)한 후에 콘텐츠의 이동을 실행한다. 또, 상기 기록재생장치(10)는 콘텐츠의 이동이 완료한 후에, 내부에 기록하는 콘텐츠를 이용할 수 없는 상태로 한다. 여기서, 인증기술은 예를 들어 DTCP 규격으로 정해진 인증순서에 따른다. 또, DTCP 규격에 의거한 인증은 공지이므로 그 상세에 대해서는 여기서는 언급하지 않는다.

콘텐츠 공급장치(11), 모니터(12), 스피커(13), 휴대형 매체(20) 및 휴대정보 단말(30)은 제 1 실시 예와 동일하므로 설명은 생략한다.

기록재생장치(1000)는 MPEG-4 규격에 따라서 압축 부호화된 콘텐츠를 재생하는 장치이고, 제 1 실시 예에 설명한 휴대형 매체(20)의 구성요소와 휴대정보 단말(30)의 제어부(303)를 구비한다. 여기서, 기록재생장치(1000)는 매체 ID의 대신, 기록재생장치(1000)를 식별하는 기기 ID를 기억하고 있다.

기록재생장치(10)는 제 1 실시 예에 설명한 동작 및 기능에 부가하여, 콘텐츠를 기록재생장치(1000)에 이동하는 동작 및 기능과 기록재생장치(1000)로부터 콘텐츠를 당해 기록재생장치(10)에 이동하는 동작 및 기능을 구비하고 있다. 또, 콘텐츠를 기록재생장치(1000)에 이동하는 동작 및 기능은 제 1 실시 예에서 설명한 콘텐츠를 휴대형 매체(20)에 이동하는 동작 및 기능과 동일하므로 설명은 생략한다. 또, 기록재생장치(1000)로부터 콘텐츠를 당해 기록재생장치(10)에 이동하는 동작 및 기능은 제 1 실시 예에서 설명한 휴대형 매체(20)로부터 콘텐츠를 당해 기록재생장치(10)에 이동하는 동작 및 기능과 동일하므로 설명은 생략한다. 또, 기록재생장치(10)가 암호화 키 K0을 생성하는 경우에는 디바이스 키 DK1과 기록재생장치(1000)로부터 판독한 MKB와 기기 ID를 이용하여 생성한다.

(2) 상기 실시 예에서, 매체기록 키 K2를 암호화하였으나, 이에 한정되지는 않는다. 기록재생장치는 매체기록 키 K2를 암호화하지 않고, 휴대형 매체(20)에 기록해도 된다.

(3) 상기 실시 예에서 매체기록 키 K2는 난수 생성기에서 생성하였으나, 이에 한정되지는 않는다.

기록재생장치는 디바이스 키 DK1과 휴대형 매체(20)로부터 판독한 MKB 및 매체 ID를 이용하여 매체기록 키 K2를 생성해도 된다. 즉, 매체 고유 키 K0을 매체기록 키 K2로 해도 된다.

(4) 상기 실시 예에서, 휴대형 매체(20)에는 하나의 암호화 콘텐츠를 기록하였으나, 이에 한정되지는 않는다. 휴대형 매체(20)에 복수의 암호화 콘텐츠를 기록해도 된다.

예를 들어, 휴대형 매체(20)의 기록가능영역(204)을 도 29에 도시한 기록가능영역(204b)으로 변경해도 된다.

이하, 기록가능영역(204b)에 대해서 설명한다.

기록가능영역(204b)은 암호화 콘텐츠 기억영역(210b), 매체기록 키 기억영역(211b) 및 이중 암호키 기억영역(212b)을 가지고 있다.

암호화 콘텐츠 기억영역(210b)은 암호화 콘텐츠 EC4를 1 이상 기억하기 위한 영역을 갖는다. 도 29에 도시한 바와 같이, 암호화 콘텐츠 기억영역(210b)은 암호화 콘텐츠 $EC4_1$, $EC4_2$, … 를 저장하고 있다. 첨자의 수치는 단지 복수의 암호화 콘텐츠를 식별하기 위한 정보이다. 각 암호화 콘텐츠 EC4에는 암호화 콘텐츠 EC4의 고화질 콘텐츠인 EC2에 할당된 콘텐츠 ID가 대응되어 있다. 구체적으로는, $EC2_1$의 콘텐츠 ID인 「CID_1」이 $EC4_1$에 대응되며, $EC2_2$의 콘텐츠 ID인 「CID_2」가 $EC4_2$에 대응되어 이다.

매체기록 키 기억영역(211b)은 암호화 매체기록 키 EK2를 1 이상 기억하기 위한 영역을 구비하고 있다. 도 29에 도시한 바와 같이, 매체기록 키 기억영역(211b)은 암호화 매체기록 키 $EK2_1$, $EK2_2$, … 를 저장하고 있다. 첨자의 수치는 단지 복수의 암호화 매체기록 키를 식별하기 위한 정보이다. 각 암호화 매체기록 키 EK2에는 대응하는 암호화 콘텐츠 EK4에 할당된 콘텐츠 ID가 대응되어 있다. 구체적으로는, $EC4_1$의 콘텐츠 ID인 「CID_1」이 $EK2_1$에 대응되며, $EC4_2$의 콘텐츠 ID인 「CID_2」가 $EK2_2$에 대응되어 있다.

이중 암호키 기억영역(212b)은 이중 암호키 K3을 1 이상 기억하기 위한 영역을 구비하고 있다.

도 29에 도시한 바와 같이, 이중 암호키 기억영역(212b)은 이중 암호키 $K3_1$, $K3_2$ … 를 저장하고 있다. 여기서 이중 암호키 $K3_1$은 이중 암호키 $K3_{1[}1]$, $K3_{1[}2]$, …, $K3_{1[}N]$으로 이루어지는 데이터이며, 이중 암호키 $K3_2$는 이중 암호키$K3_{2[}1]$, $K3_2[2]$, …, $K3_{2[}N]$으로 이루어지는 데이터이다. 첨자의 수치는 단지 복수의 매체기록 키를 식별하기 위한 정보이다. 각 이중 암호키 K3에는 대응하는 암호화 콘텐츠 EK4에 할당된 콘텐츠 ID가 대응되어 있다. 구체적으로는, $EC4_1$의 콘텐츠 ID인 「CID_1」이 $K3_1$에 대응되고, $EC4_2$의 콘텐츠 ID인 「CID_2」가 $K3_2$에 대응되어 있다.

기록재생장치(10)는 무브 백 지시의 수신시에 무브 백 하는 콘텐츠의 콘텐츠 ID를 수신한다. 기록재생장치(10)는 수신한 콘텐츠 ID에 대응하는 암호화 콘텐츠 EC4 및 암호화 매체기록 키 EK2를 소거한다. 기록재생장치(10)는 휴대형 매체(20)의 이중 암호키 기억영역(212b)으로부터 수신한 콘텐츠 ID에 대응하는 이중 암호키 K3[n]을 순차 판독하고, 판독한 이중 암호키 K3[n]을 이용하여 수신한 콘텐츠 ID에 대응하고 또한, 암호화 콘텐츠 기록부(104)에 기록하고 있는 암호화 콘텐츠 EEC2[n]을 순차 복호한다.

(5) 상기 실시 예에서, 휴대형 매체(20)를 SD카드로 하였으나, 이에 한정되지는 않는다. 재기록 가능한 DVD나 기록가능한 DVD 등과 같은 매체라도 된다. 이때, DVD로의 기록이나 데이터의 소거는 기록재생장치(10)가 DVD의 영역에 대해서 직접 실행한다.

(6) 상기 실시 예에서, 부분콘텐츠의 재생시간 길이는 45초로 하였으나, 이에 한정되지는 않는다. 부분콘텐츠의 재생시간 길이는 1분 이내이면 된다.

(7) 본 발명의 실시 예에서는 기록재생장치에서 휴대형 매체로 콘텐츠를 이동하거나, 또는, 휴대형 매체에서 기록재생장치로 콘텐츠를 이동하는 구성으로 하였지만, 본 발명은 그 구성에 한정되는 것은 아니다. 예를 들어 기록재생장치로부터 다른 기록재생장치로 콘텐츠를 이동하는 구성이라도 된다.

(8) 본 발명의 실시 예에서는 휴대형 매체로부터 기록재생장치로 콘텐츠를 이동할 때, 휴대형 매체에 기록하는 각종 데이터를 소거하는 구성으로 하였지만, 본 발명은 그 구성에 한정되는 것은 아니다. 예를 들어 휴대형 매체에 기록하는 암호화 콘텐츠는 소거하지 않고, 복호에 필요한 키만을 소거하여, 상기 암호화 콘텐츠를 이용 불가상태로 하는 구성이라도 된다. 또, 데이터의 소거가 아닌, 데이터의 일부를 파괴하여 이용할 수 없는 상태로 하는 구성이라도 된다.

(9) 본 발명의 실시 예에서, 기록재생장치가 콘텐츠의 이동처리에서의 상태천이를 기억하는 기억부를 구비하는 구성이라도 된다. 기록재생장치는 콘텐츠의 이동이 정상적으로 완료하지 않은 경우, 상기 기억부에 기억하는 상태천이에 의거하여 콘텐츠의 이동처리를 계속해서 행하거나, 콘텐츠의 이동처리를 최초부터 다시 할지를 판단하는 구성이라도 된다. 또, 기록재생장치는 상기 기억부에 기억하는 상태천이를 이용자에게 통지하는 통지부를 구비하는 구성이라도 된다. 이 경우, 정상적으로 완료하지 않았다는 취지를 이용자에게 통지하여, 이용자로부터의 지시에 의거하여 콘텐츠의 이동처리를 계속할지 또는 콘텐츠의 이동처리를 최초부터 다시 할지를 결정하는 구성이라도 된다.

(10) 본 발명의 실시 예에서, 기록재생장치 및 휴대형 매체가 키를 이동 후에 소거하는 경우, 키의 수신 측이 키의 송신 측에 대해서 올바르게 수신할 수 있었음을 통지하고, 송신 측은 상기 통지에 의거하여 수신을 확인한 후에 키를 소거하는 구성이라도 된다.

(11) 본 발명의 실시 예에서, 콘텐츠는 당해 콘텐츠를 고유하게 식별하기 위한 식별자가 부여되어 있고, 휴대형 매체에 이동시킨 콘텐츠를 원래의 기록재생장치로 되돌리는 경우, 상기 기록재생장치는 자신이 보유하는 암호화 콘텐츠의 식별자 및 휴대형 매체에 기록하는 암호화 콘텐츠의 식별자가 일치하는지 여부를 판정하여, 일치한 경우에 한해서 콘텐츠를 기록

재생장치에 이동시키는 것을 허가하는 구성이라도 된다. 또, 콘텐츠에는 콘텐츠를 고유하게 식별하는 식별자 대신에, 이동원의 기록재생장치를 고유하게 식별하는 식별자가 부여되어 있는 구성이라도 된다. 이 경우, 기록재생장치는 콘텐츠에 부여되어 있는 기록재생장치의 식별자와, 자신의 식별자가 일치하는지 여부를 판정하여, 일치한 경우에 한해서 콘텐츠를 기록재생장치에 이동시키는 것을 허가하는 구성이라도 된다.

(12) 본 발명의 실시 예에서는, 콘텐츠는 외부의 콘텐츠 공급장치에 의해 공급되는 구성으로 하였지만, 본 발명은 그 구성에 한정되는 것은 아니다. 예를 들어 기록재생장치에 삽입된 기록매체로부터 콘텐츠를 판독하는 구성이라도 된다.

(13) 기록재생장치(10)가 암호화 매체기록 키 EK2를 휴대형 매체(20)에 기록하는 타이밍은 암호화 콘텐츠 기록부(104)로부터 암호화 콘텐츠의 판독에 실패하였다고 판단한 후에 행해도 된다. 또, 암호화 매체기록 키 EK2가 휴대형 매체(20)에 기록된 후에 장치 내의 암호화 매체기록 키 EK2 및 매체기록 키 K2는 소거된다.

(14) 기록재생장치(10)가 이중 암호키 K3[n]을 휴대형 매체(20)에 기록하는 타이밍은 이중 암호화 콘텐츠 기록부(115)가 암호화 콘텐츠EC2[n]을 이중 암호화 콘텐츠 EEC2[n]에 덮어쓰기를 행한 후에 행해도 된다. 또, 이중 암호키 K3[n]이 휴대형 매체(20)에 기록된 후에 장치 내의 이중 암호키 K3[n]은 소거된다.

(15) 상기 제 2 실시 예에서, 기록재생장치(50)가 암호화 변환콘텐츠 EC4_1을 생성할 때에 암호키로 부분콘텐츠 C4[1]을 이용하였으나, 이에 한정되지는 않는다. 기록재생장치(50)는 부분 콘텐츠 C4[1], C4[2], …, C4[N] 중 어느 하나를 암호키로 이용해도 된다.

(16) 상기 제 2 실시 예에서, 기록재생장치(50)는 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[N] 각각을 이중 암호화하였으나, 이에 한정되지는 않는다. 기록재생장치(50)는 적어도 암호화 콘텐츠 EC4_1을 복호하기 위해서 이용하는 부분정보를 이중 암호화해도 된다.

(17) 상기 제 2 실시 예에서, 기록재생장치(50)의 변환용 데이터 복호부(516)는 128비트로 이루어지는 암호화 부분콘텐츠 EC4[n]을 판독하였으나, 이에 한정되지는 않는다.

변환용 데이터 복호부(516)는 재생시간 길이의 합계가 소정 시간 내(45초 내)가 되도록, 암호화 콘텐츠 EC4의 선두에서부터 순서대로 1 이상의 암호화 부분콘텐츠를 판독해도 된다.

이하에 구체 예를 이용하여 설명한다.

변환용 데이터 복호부(516)는 재생시간 길이의 합계가 소정 시간 내(45초 내)가 되도록 EC4_1[1], EC4_1[2], …, EC4_1[10]을 판독하고, 판독한 EC4_1[n1](n1 = 1, 2, …, 10이다. 이하 동일)을 복호한다. 제 2 암호화부(517)는 매체기록 키 K2를 이용하여 C4[n1]을 암호화하여 EC4[n1]을 순차 생성하고, 휴대형 매체(20)에 순차 기록한다. 이중 암호키 생성부(518)는 이중 암호키 K3[1]을 생성하고, 휴대형 매체(20) 및 이중 암호키 기억부(519)에 기록한다. 이중 암호화부(520)는 콘텐츠 판독부(513)를 거쳐서 EC4_1[1], EC4_1[2], …, EC4_1[10]에 대응하는 암호화 부분콘텐츠 EC2[1], EC2[2], …, EC2[10]을 취득한다. 이중 암호화부(520)는 이중 암호키 K3[1]을 이용하여 암호화 부분콘텐츠 EC2[n1]을 순차 암호화하여 이중 암호화 부분콘텐츠 EEC2[n1]을 생성한다. 이중 암호화 콘텐츠 기록부(521)는 암호화 부분콘텐츠 EC2[n1]을 이중 암호화 부분콘텐츠 EEC2[n1]로 순차 덮어쓴다.

기록재생장치(50)는 상기 동작을 암호화 부분콘텐츠 EC2[N]이 이중 암호화 부분콘텐츠 EEC2[N]으로 덮어써질 때까지 행한다.

(18) 상기 실시 예에서, 기록재생장치는 콘텐츠 C2를 장치 키 K1로 암호화하여 암호화콘텐츠 C2를 기록하였으나, 이에 한정되지는 않는다.

기록재생장치는 콘텐츠 C2를 장치 키로 암호화하지 않고 기록해도 된다. 이때, 기록재생장치는 무브 지시를 수신하면, 이중 암호키 K3으로 각 C2[n]을 암호화하여 암호화 부분콘텐츠를 생성하고, 대응하는 부분콘텐츠 C2[n]을 생성한 암호화 부분콘텐츠로 재기록한다.

(19) 상기 실시 예에서, 기록재생장치는 매체기록 키 K2를 이용하여 콘텐츠 C4를 암호화하여 암호화 콘텐츠 EC4를 휴대형 매체에 기록하였으나, 이에 한정되지는 않는다. 기록재생장치는 콘텐츠 C4를 휴대형 매체에 기록해도 된다.

(20) 상기 제 2 실시 예에 있어서, 기록재생장치(50)는 암호화 콘텐츠 EC4_1의 복호에 이용하는 부분정보에 대응하는 부분콘텐츠 EC2[1]만을 복호하여 다운 컨버트 하여 부분정보 PC4(= C4[1])를 생성하였으나, 이에 한정되지는 않는다.

이하와 같은 동작에 의해 각 부분콘텐츠 EC4[n]을 휴대형 매체(20)에 기록해도 된다.

기록재생장치(10)는 암호화 콘텐츠 EC2를 복호하여 콘텐츠 C2를 생성하고, 생성한 콘텐츠 C2를 다운 컨버트 하여 콘텐츠 C4를 생성한다. 기록재생장치(10)는 생성한 콘텐츠 C4로부터 부분정보 PC4를 취득한다.

(21) 본 발명은 상기에 설명한 방법이라도 된다. 또, 이들 방법을 컴퓨터에 의해 실현하는 컴퓨터 프로그램이라도 되며, 상기 컴퓨터 프로그램으로 이루어지는 디지털 신호라도 된다.

또, 본 발명은 상기 컴퓨터 프로그램 또는 상기 디지털 신호를 컴퓨터 판독가능한 기록매체, 예를 들어, 플렉시블 디스크, 하드디스크, CD-ROM, MO, DVD, DVD-ROM, DVD-RAM, BD(Blu-ray Disc), 반도체 메모리 등에 기록한 것이라도 된다. 또, 이들 기록매체에 기록되어 있는 상기 컴퓨터 프로그램 또는 상기 디지털 신호라도 된다.

또, 본 발명은 상기 컴퓨터 프로그램 또는 상기 디지털 신호를 전기통신회선, 무선 또는 유선통신회선, 인터넷을 대표로 하는 네트워크 등을 경유하여 전송하는 것으로 해도 된다.

또, 본 발명은 마이크로 프로세서와 메모리를 구비한 컴퓨터 시스템으로, 상기 메모리는 상기 컴퓨터 프로그램을 기억하고 있고, 상기 마이크로 프로세서는 상기 컴퓨터 프로그램에 따라서 동작하는 것으로 해도 된다.

또, 상기 프로그램 또는 상기 디지털 신호를 상기 기록매체에 기록하여 이송함으로써, 또는 상기 프로그램 또는 상기 디지털 신호를 상기 네트워크 등을 경유하여 이송함으로써, 독립된 다른 컴퓨터 시스템에 의해 실시해도 된다.

(22) 상기 실시 예 및 상기 변형 예를 각각 조합해도 된다.

4. 정리

종래, 콘텐츠의 보호기술에 관한 규격으로서, 예를 들어 DTCP(Digital Transmission Content Protection)가 있다. DTCP는 콘텐츠를 디지털 전송할 때에, 콘텐츠를 암호화하는 등에 의해 부정한 복제를 방지하는 기술이다. DTCP와 같은 콘텐츠 보호기술에서는, 콘텐츠에 「Copy No More」, 「Copy One Generation」 등의 카피제어정보(CCI: Copy Control Information)를 부여한다. 「Copy No More」는 콘텐츠의 카피가 금지되어 있는 것을 나타내고, 「Copy One Generation」은 콘텐츠의 카피가 1회만 허가되어 있는 것을 나타낸다. 따라서, 카피제어정보로서 「Copy One Generation」이 부여된 콘텐츠를 카피하면, 카피에 의해서 새로이 얻어진 콘텐츠에는 카피제어정보로서 「Copy No More」가 부여된다.

한편, 카피제어정보로서 「Copy No More」가 부여된 콘텐츠라도, 다른 기록매체, 또는 다른 장치로 이동시키고 싶다고 하는 요망이 있다. 예를 들어 디지털 텔레비전에 내장되어 있는 HDD(Hard Disk Drive)에 기록되어 있는 콘텐츠를 DVD-RAM에 이동시켜서 보존 판으로 보존해 두고 싶은 경우이다. 이때(HDD로부터 DVD-RAM에 콘텐츠를 이동시킨 경우), 디지털 텔레비전 내장 HDD의 당해 콘텐츠는 당연히 재생할 수 없는 상태가 되지 않으면 안 된다. 예를 들어 내장 HDD로부터 DVD-RAM에 콘텐츠를 카피한 후에, 내장 HDD에 기록되어 있는 콘텐츠를 소거하는 등으로 하여 콘텐츠를 무효화한다. 즉, 콘텐츠를 이용할 수 없는 상태로 하는 방법 등이 고려된다. 그러나 콘텐츠의 이동에 앞서서, 디지털 텔레비전으로부터 내장 HDD를 추출하고, 이것을 퍼스널 컴퓨터에 접속하여 백업을 작성하며, 콘텐츠를 이동한 후에 백업해 둔 데이터를 내장 HDD에 되돌린다고 하는 조작이 행해지면, 콘텐츠를 몇 번이라도 이동할 수 있게 되어, 사실상 부정한 복제를 방지할 수 없게 된다.

또, 콘텐츠의 이동 중에, 전원 단절 등의 원인에 의해 이동원과 이동 처의 콘텐츠가 모두 손상되어, 콘텐츠로서 이용할 수 없게 되는 것은 콘텐츠를 이용하는 사용자에게 있어서는 불편하다. 또, 이와 같이 하여 이용할 수 없게 된 콘텐츠를 다시 입수하기 위하여 지출이 필요한 경우에는 경제적인 손실도 발생한다.

상기 과제를 해결하기 위한 종래기술로서, 부정카피를 방지하면서 콘텐츠의 상실을 초래하지 않고, 콘텐츠의 이동을 가능하게 하는 기술이 있다.

그러나 이동원의 콘텐츠가 고화질 콘텐츠이고, 콘텐츠의 사이즈에 비해서 이동 처의 기억용량이 작은 경우에는, 콘텐츠의 이동 전에 그 화질을 열화 시키는 등에 의해 사이즈를 작게 압축 변환하고 나서 이동을 행하는 것이 통례이지만, 상기 구성과 같이 콘텐츠를 소거하는 등에 의해 이동원의 콘텐츠를 무효화하는 경우, 압축변환된(화질이 열화 한) 콘텐츠만이 사용자에게 남게 된다.

즉, 다시 기록용량이 큰 내장 HDD에 콘텐츠를 되돌리는(이동하는) 경우에도, 화질이 열화 된 콘텐츠를 고화질 콘텐츠로 변환하기는 불가능하고, 원래의 고화질 콘텐츠는 복원되지 않으므로, 이것은 콘텐츠를 이용하는 사용자의 편리성을 해치는 것으로 이어진다.

본 발명에서의 저작권 보호시스템은 상기 과제를 해결하기 위한 것으로, 부정한 복제를 방지하면서, 콘텐츠의 상실을 초래하지 않고, 콘텐츠의 이동을 가능하게 하며, 또, 사이즈를 작게 하는 압축 변환 후에 당해 콘텐츠를 이동원으로 되돌리는 경우에도 원래의 고화질 콘텐츠의 복원을 가능하게 한다.

본 발명의 저작권 보호시스템은, 콘텐츠를 공급하는 콘텐츠 공급장치와, 상기 콘텐츠를 획득하여 콘텐츠의 기록 및 재생을 행하고, 또 콘텐츠의 이동을 실행하는 기록재생장치와, 상기 이동하는 콘텐츠를 획득하는 기록재생장치와, 휴대형 매체로 구성되고, 콘텐츠의 이동시에 당해 콘텐츠를 소정 단위로 나누어 이동시킨다.

본 발명은 콘텐츠를 사용자에게 배송하는 산업, 콘텐츠를 기록재생하는 장치를 제조하는 제조업, 콘텐츠를 기록재생하는 장치를 판매하는 판매업에서, 화상 변환한 콘텐츠를 다른 장치에 무브 해도 원래의 콘텐츠를 복원할 수 있으므로 사용자의 편리성을 저해하지 않고, 콘텐츠의 저작권을 보호하는 구조로 이용할 수 있다.

본 발명에 관한 저작권 보호시스템은, 콘텐츠의 이동원의 기록재생장치가 콘텐츠의 이동을 블록단위로 행함으로써, 콘텐츠 이동중의 전원 단절 등에 의한 콘텐츠 소실의 위험이 없고, 또한, 사용자가 콘텐츠 이동처리중에 기록재생장치를 해석하여 복호 된 평문 콘텐츠의 부정 입수를 시도해도, 얻어지는 평문 콘텐츠는 콘텐츠 전체의 아주 일부에 불과하여 피해는 적어진다. 즉, 이동중의 콘텐츠의 소실을 방지하면서, 이동중의 평문 콘텐츠 취득에 안전하다고 하는 효과를 가지며, 사용자 편리성과 안전성의 양쪽을 해치지 않고, 저작권 보호시스템의 실현에 유용하다.

본 발명에 의하면, 콘텐츠의 이동원의 기록재생장치가 콘텐츠의 이동시에 당해 콘텐츠의 부분정보를 이동시킴으로써, 기록재생장치 내의 콘텐츠를 모두 소거하지 않고도 이용이 불가능한 상태로 하며, 이동한 콘텐츠를 다시 당해 기록재생장치에 되돌리는 경우에는 상기 부분정보를 원래로 되돌림(이동시키다)으로써 원래의 고화질 콘텐츠를 복원 가능(이용가능)하게 할 수 있다.

본 발명은, 단말장치가 보유하는 제 1 포맷의 콘텐츠를 제 2 포맷의 콘텐츠로 휴대형 매체에 이동할 수 있고, 또한, 상기 휴대형 매체에 이동한 제 2 포맷의 콘텐츠를 상기 단말장치에 제 1 포맷의 콘텐츠로서 이동하는 제 2 이동처리가 가능한 저작권 보호시스템으로, 상기 휴대형 매체는 데이터를 기억하는 기억부를 구비하고, 상기 단말장치는 제 1 포맷의 콘텐츠를 기억하는 콘텐츠 기억부와, 상기 제 1 포맷의 콘텐츠를 상기 제 2 포맷의 콘텐츠로 변환하는 포맷 변환부와, 복원용 데이터를 생성하는 복원용 데이터 생성부와, 상기 제 2 포맷의 콘텐츠와 상기 복원용 데이터를 상기 휴대형 매체 내의 기억부로 이동하는 이동부와, 상기 이동부에 의한 데이터 이동 후에 상기 제 1 포맷의 콘텐츠 및 상기 제 2 포맷의 콘텐츠 및 상기 복원용 데이터를 소거하는 소거부를 구비하는 것을 특징으로 한다.

여기서, 상기 단말장치는 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 복원용 데이터를 판독하는 판독부와, 상기 복원용 데이터를 기초로 상기 제 1 포맷의 콘텐츠를 복원하여 상기 콘텐츠 기억부에 기록하는 복원부와, 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 제 2 포맷의 콘텐츠와 상기 복원용 데이터를 소거하는 소거부를 더 구비해도 된다.

여기서, 상기 단말장치는 적어도 상기 복원용 데이터와 상기 제 1 포맷의 콘텐츠로부터 복원용 기본데이터를 생성하는 복원용 기본데이터 생성부와, 상기 복원용 기본데이터 생성부를 기억하는 복원용 기본데이터 기억부를 더 구비해도 된다.

여기서, 상기 단말장치는 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 복원용 데이터를 판독하는 판독부와, 상기 복원용 데이터와 상기 복원용 기본데이터를 기초로 상기 제 1 포맷의 콘텐츠를 복원하여 상기 콘텐츠 기억부에 기록하는 복원부와, 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 제 2 포맷의 콘텐츠와 상기 복원용 데이터를 소거하는 소거부를 더 구비해도 된다.

또, 본 발명은, 단말장치가 보유하는 제 1 포맷의 콘텐츠를 제 2 포맷의 콘텐츠로 휴대형 매체에 이동할 수 있고, 또한, 상기 휴대형 매체에 이동한 제 2 포맷의 콘텐츠를 상기 단말장치에 제 1 포맷의 콘텐츠로서 이동하는 제 2 이동처리가 가능한 저작권 보호시스템으로, 상기 휴대형 매체는 데이터를 기억하는 기억부를 구비하고, 상기 단말장치는 제 1 포맷의 콘텐츠를 기억하는 콘텐츠 기억부와, 상기 콘텐츠 기억부에 기억하는 상기 제 1 포맷의 콘텐츠로부터 콘텐츠의 포맷에 의거하여 결정된 소정의 데이터 사이즈의 제 1 포맷의 부분콘텐츠를 추출하는 부분콘텐츠 추출부와, 상기 제 1 포맷의 부분콘텐츠를 제 2 포맷의 부분콘텐츠로 변환하는 포맷 변환부와, 상기 제 1 포맷의 부분콘텐츠에 대응하는 부분콘텐츠 복원용 데이터를 생성하는 부분콘텐츠 복원용 데이터 생성부와, 상기 제 2의 포맷의 부분콘텐츠와 상기 부분콘텐츠 복원용 데이터를 상기 휴대형 매체 내의 기억부에 이동하는 이동부와, 상기 이동부에 의한 데이터 이동 후에 상기 단말장치 내의 상기 제 1 포맷의 부분콘텐츠 및 상기 제 2 포맷의 부분콘텐츠 및 상기 부분콘텐츠 복원용 데이터를 소거하는 소거부를 구비하는 것을 특징으로 한다.

여기서, 상기 단말장치는, 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 부분콘텐츠 복원용 데이터를 판독하는 판독부와, 상기 부분콘텐츠 복원용 데이터를 기초로 상기 제 1 포맷의 콘텐츠를 복원하여 상기 콘텐츠 기억부에 기록하는 복원부와 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 제 2 포맷의 콘텐츠와 상기 부분콘텐츠 복원용 데이터를 소거하는 소거부를 더 구비해도 된다.

여기서, 상기 단말장치는 적어도 상기 부분콘텐츠 복원용 데이터와 상기 제 1 포맷의 부분콘텐츠로부터 부분콘텐츠 복원용 기초 데이터를 생성하는 부분콘텐츠 복원용 기본데이터 생성부와, 상기 부분콘텐츠 복원용 기본데이터 생성부를 기억하는 부분콘텐츠 복원용 기본데이터 기억부를 더 구비해도 된다.

여기서, 상기 단말장치는 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 부분콘텐츠 복원용 데이터를 판독하는 판독부와, 상기 부분콘텐츠 복원용 데이터와 상기 부분콘텐츠 복원용 기본데이터를 기초로 상기 제 1 포맷의 콘텐츠를 복원하여 상기 콘텐츠 기억부에 기록하는 복원부와, 상기 휴대형 매체의 데이터 기억부에 기억하는 상기 제 2 포맷의 콘텐츠와, 상기 부분콘텐츠 복원용 데이터를 소거하는 소거부를 더 구비해도 된다.

여기서, 상기 부분콘텐츠 복원용 데이터 생성부는 난수를 생성하여 상기 부분콘텐츠 복원용 데이터로 하고, 상기 부분콘텐츠 복원용 기본데이터 생성부는 상기 부분콘텐츠 복원용 데이터를 이용하여 상기 제 1 포맷의 부분콘텐츠를 암호화하여 상기 부분콘텐츠 복원용 기본데이터로 해도 된다.

또, 본 발명은, 외부로부터 주어지는 제 1 포맷의 콘텐츠 데이터를 기록, 재생하는 단말장치가, 필요에 따라서, 상기 제 1 포맷으로 기억하는 콘텐츠를 제 2 포맷의 콘텐츠에 포맷 변환하여 휴대형 매체로 이동할 수 있는 저작권 보호시스템으로, 상기 단말장치는 상기 제 1 포맷의 콘텐츠 데이터를 암호화하여 암호화 콘텐츠 데이터로 하는 제 1 암호화부와, 상기 암호화 콘텐츠 데이터를 기억하는 암호화 콘텐츠 기억부와, 상기 제 1 포맷의 콘텐츠 데이터를 제 2 포맷의 콘텐츠 데이터로 변환하는 포맷 변환부와, 상기 제 2 포맷의 콘텐츠 데이터를 기초로 변환 키를 생성하는 변환 키 생성부와, 상기 변환 키를 이용하여 상기 제 2 포맷의 콘텐츠 데이터를 암호화하여 변환용 데이터로 하는 제 2 암호화부와, 상기 변환용 데이터를 기억하는 기억부를 구비하는 것을 특징으로 한다.

또, 본 발명은, 콘텐츠를 보유하며, 휴대형 매체에 콘텐츠를 이동할 수 있는 단말장치로 상기 단말장치는 제 1 포맷의 콘텐츠를 기억하는 콘텐츠 기억부와, 상기 제 1 포맷의 콘텐츠를 제 2 포맷의 콘텐츠로 변환하는 포맷 변환부와 복원용 데이터를 생성하는 복원용 데이터 생성부와, 상기 제 2 포맷의 콘텐츠와 상기 복원용 데이터를 상기 휴대형 매체 내의 기억부에 이동하는 이동부와, 상기 이동부에 의한 데이터 이동의 후에 상기 제 1 포맷의 콘텐츠, 상기 제 2 포맷의 콘텐츠 및 상기 복원용 데이터를 소거하는 소거부를 구비하는 것을 특징으로 한다.

또, 본 발명은, 콘텐츠를 보유하며, 휴대형 매체에 콘텐츠를 이동할 수 있는 단말장치로, 상기 단말장치는 제 1 포맷의 콘텐츠를 기억하는 콘텐츠 기억부와, 상기 콘텐츠 기억부에 기억하는 상기 제 1 포맷의 콘텐츠로부터 콘텐츠의 포맷에 의거하여 결정된 소정의 데이터 사이즈의 제 1 포맷의 부분콘텐츠를 추출하는 부분콘텐츠 추출부와, 상기 제 1 포맷의 부분콘텐츠를 제 2 포맷의 부분콘텐츠로 변환하는 포맷 변환부와, 상기 제 1 포맷의 부분콘텐츠에 대응하는 부분콘텐츠 복원용 데이터를 생성하는 부분콘텐츠 복원용 데이터 생성부와, 상기 제 2 포맷의 부분콘텐츠와 상기 부분콘텐츠 복원용 데이터를 상기 휴대형 매체 내의 기억부로 이동하는 이동부와, 상기 이동부에 의한 데이터 이동 후에, 상기 단말장치 내의 상기 제 1 포맷의 부분콘텐츠, 및 상기 제 2 포맷의 부분콘텐츠 및 상기 부분콘텐츠 복원용 데이터를 소거하는 소거부를 구비하는 것을 특징으로 한다.

또, 본 발명은, 오리지널 콘텐츠를 단말장치로부터 휴대형 기록매체에 이동시키는 저작권 보호시스템으로, 상기 단말장치는 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과, 상기 오리지널 콘텐츠에 비 가역 변환을 하여 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과, 상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과, 암호키를 이용하여 상기 콘텐츠의 1 블록을 암호화하여 암호화 블록을 생성하고, 상기 1 블록을 상기 암호화 블록으로 치환하는 암호화수단과, 상기 암호키를 상기 기록매체에 기록하는 키 기록수단과, 상기 암호에 이용된 상기 암호키를 삭제하는 키 삭제수단을 구비하고, 상기 기록매체는 상기 변환콘텐츠를 기억하는 콘텐츠 기억수단을 구비하는 것을 특징으로 한다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 당해 단말장치에서 기억하고 있는 오리지널 콘텐츠의 1 블록을 암호키로 암호화하며, 상기 암호키를 기록매체에 기록하고 있으므로, 사용자에 대해서 오리지널 콘텐츠를 이용하지 못하게 할 수 있다.

또, 저작권 보호시스템의 단말장치는 오리지널 콘텐츠 기억수단에 1 블록이 암호화된 오리지널 콘텐츠를 기억하고 있으므로, 상기 변환콘텐츠를 상기 기록매체에 이동시킨 후에도, 상기 암호키를 상기 기록매체로부터 취득함으로써 변환 전의 상기 오리지널 콘텐츠를 복원할 수 있다.

여기서, 상기 오리지널 콘텐츠는 복수의 블록 데이터마다 암호화된 암호화 콘텐츠이고, 상기 블록은 암호화된 블록데이터이며, 상기 변환콘텐츠 생성수단은 상기 암호화 콘텐츠를 복호하여 상기 오리지널 콘텐츠를 생성하고, 생성한 오리지널 콘텐츠에 상기 비 가역 변환을 하여 변환콘텐츠를 생성하고, 상기 암호화 수단은 상기 암호키를 이용하여 상기 암호화된 블록데이터를 암호화하여 이중 암호화 블록데이터를 상기 암호화 블록으로 생성하고, 상기 암호화된 블록데이터를 생성한 이중 암호화 블록데이터로 치환해도 된다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 암호화된 블록 데이터를 이중 암호화하므로 오리지널 콘텐츠에 대한 시큐어리티를 높일 수 있다.

여기서, 상기 변환콘텐츠 기록수단은, 상기 변환콘텐츠를 암호화하여 암호화 변환콘텐츠를 더 생성하고, 상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 상기 기록매체에 기록하는 대신, 생성한 상기 암호화 변환콘텐츠와, 상기 암호화 변환콘텐츠를 복호하는 복호 키 정보를 상기 기록매체에 기록하고, 상기 콘텐츠 기억수단은 상기 변환콘텐츠를 기억하는 대신, 상기 암호화 변환콘텐츠와 상기 복호 키 정보를 기억해도 된다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 기록매체에 암호화 변환콘텐츠를 기록하므로 변환콘텐츠에 대한 시큐어리티가 높아진다.

여기서, 상기 저작권 보호시스템은 휴대정보 단말을 더 포함하고, 상기 휴대정보 단말은 상기 콘텐츠 기억수단에 상기 복호 키 정보 및 상기 암호화 변환콘텐츠가 기억된 상기 기록매체로부터 상기 암호화 변환콘텐츠와 상기 복호 키 정보를 판독하고, 판독한 상기 암호화 변환콘텐츠를 상기 복호 키 정보를 이용하여 복호하며, 상기 변환콘텐츠를 생성하여, 생성한 상기 변환콘텐츠를 재생해도 된다.

이 구성에 의하면, 저작권 보호시스템의 휴대정보 단말은 오리지널 콘텐츠에 비 가역 변환을 한 변환콘텐츠를 재생할 수 있고, 단말장치는 오리지널 콘텐츠를 재생할 수 없다. 이에 따라, 오리지널 콘텐츠에 대한 저작권을 보호할 수 있다.

여기서, 오리지널 콘텐츠를 단말장치로부터 휴대형 기록매체에 이동시키는 저작권 보호시스템으로, 상기 단말장치는 상기 오리지널 콘텐츠를 기억하고 있는 오리지널 콘텐츠 기억수단과, 상기 오리지널 콘텐츠에 비 가역 변환이 실시된 변환콘텐츠가 암호화된 비 오리지널 콘텐츠를 기억하고 있는 비 오리지널 콘텐츠 기억수단과, 상기 변환콘텐츠에 포함되고, 상기 비 오리지널 콘텐츠의 복호에 이용하는 복호블록 데이터를 상기 오리지널 콘텐츠로부터 취득하는 복호블록 데이터 취득수단과, 상기 비 오리지널 콘텐츠를 상기 복호블록 데이터를 이용하여 복호하여 상기 변환콘텐츠를 생성하는 변환콘텐츠 생성수단과, 상기 변환콘텐츠 생성수단에서 생성된 상기 변환콘텐츠를 상기 기록매체에 기록하는 변환콘텐츠 기록수단과 암호키를 이용하여 상기 오리지널 콘텐츠의 1 블록을 암호화하여 암호화블록을 생성하고, 상기 1 블록을 상기 암호화블록으로 치환하는 암호화수단과, 상기 암호키를 상기 기록매체에 기록하는 키 기록수단과, 상기 암호화에 이용된 상기 암호키를 내부로부터 삭제하는 키 삭제수단을 구비하고, 상기 기록매체는 상기 변환콘텐츠를 기억하는 콘텐츠 기억수단을 구비해도 된다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 당해 단말장치에서 기억하고 있는 오리지널 콘텐츠의 1 블록을 암호키로 암호화하고, 상기 암호키를 기록매체에 기록하고 있으므로, 사용자에 대해서 오리지널 콘텐츠를 이용하지 않게 할 수 있다.

또, 저작권 보호시스템의 단말장치는 오리지널 콘텐츠 기억수단에 1 블록이 암호화된 오리지널 콘텐츠를 기억하고 있으므로, 상기 변환콘텐츠를 상기 기록매체에 이동시킨 후에도, 상기 암호키를 상기 기록매체로부터 취득함으로써 변환 전의 상기 오리지널 콘텐츠를 복원할 수 있다.

또, 저작권 보호시스템의 단말장치는 비 오리지널 콘텐츠를 미리 기억하고 있으므로, 기록매체에 콘텐츠를 이동시킬 때에 오리지널 콘텐츠에 비 가역 변환을 할 필요가 없다. 이에 따라 콘텐츠 이동시의 처리의 부하를 경감할 수 있다.

여기서, 상기 변환콘텐츠에 포함되는 1 변환블록 데이터를 암호키로 이용하여 상기 변환콘텐츠를 암호화함으로써 상기 비 오리지널 콘텐츠가 생성되고, 상기 비 오리지널 콘텐츠가 생성된 후, 상기 암호키는 소거되며, 상기 복호블록 데이터 취득수단은 상기 오리지널 콘텐츠에 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하고, 생성한 상기 변환콘텐츠로부터 상기 1 변환블록 데이터를 상기 복호블록 데이터로 취득해도 된다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 비 오리지널 콘텐츠를 복호 할 때에, 오리지널 콘텐츠로부터 변환콘텐츠에 포함되는 1 변환블록 데이터를 생성하므로, 비 오리지널 콘텐츠를 복호하기 위한 복호 키를 미리 기억해 둘 필요가 없다.

여기서, 상기 오리지널 콘텐츠는 복수의 블록 데이터 단위로 암호화된 암호화 콘텐츠이고, 상기 블록은 암호화된 블록 데이터이며, 상기 복호블록 데이터 취득수단은 상기 비 가역 변환을 하여 상기 변환콘텐츠를 생성하여 상기 복호블록 데이터를 취득하는 대신, 상기 1 변환블록 데이터에 대응하는 암호화된 블록데이터를 복호하고, 상기 비 가역 변환을 하여 상기 복호블록 데이터를 취득하고, 상기 암호화수단은 상기 암호키를 이용하여 상기 암호화된 블록 데이터를 암호화하여 이중 암호화 블록 데이터를 상기 암호화 블록으로 생성하고, 상기 암호화된 블록 데이터를 생성한 이중 암호화 블록데이터로 치환해도 된다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 암호화된 블록데이터를 이중 암호화하므로 오리지널 콘텐츠에 대한 시큐어리티를 높일 수 있다.

여기서, 상기 변환콘텐츠 기록수단은, 상기 변환콘텐츠를 암호화하여 암호화 변환콘텐츠를 생성하고, 상기 변환콘텐츠 기록수단은 상기 변환콘텐츠를 상기 기록매체에 기록하는 대신, 생성한 상기 암호화 변환콘텐츠와 상기 암호화 변환콘텐츠를 복호하는 복호 키 정보를 상기 기록매체에 기록하고, 상기 콘텐츠 기억수단은 상기 변환콘텐츠를 기억하는 대신, 상기 암호화 변환콘텐츠와 상기 복호 키 정보를 기억해도 된다.

이 구성에 의하면, 저작권 보호시스템의 단말장치는 기록매체에 암호화 변환콘텐츠를 기록하므로 변환콘텐츠에 대한 시큐어리티가 높아진다.

여기서, 상기 저작권 보호시스템은 휴대정보 단말을 더 포함하고, 상기 휴대정보 단말은 상기 콘텐츠 기억수단에 상기 복호 키 정보 및 상기 암호화 변환콘텐츠가 기억된 상기 기록매체로부터 상기 암호화 변환콘텐츠와 상기 복호 키 정보를 판독하고, 판독한 상기 암호화 변환콘텐츠를 상기 복호 키 정보를 이용하여 복호하여 상기 변환콘텐츠를 생성하고, 생성한 상기 변환콘텐츠를 재생해도 된다.

이 구성에 의하면, 저작권 보호시스템의 휴대정보 단말은 오리지널 콘텐츠에 비 가역 변환을 한 변환콘텐츠를 재생할 수 있고, 단말장치는 오리지널 콘텐츠를 재생할 수 없다. 이에 따라, 오리지널 콘텐츠에 대한 저작권을 보호할 수 있다.

산업상 이용 가능성

상기에서 설명한 저작권 보호시스템은, 콘텐츠를 사용자에게 배송하는 산업, 콘텐츠를 기록재생하는 장치를 제조하는 제조업, 콘텐츠를 기록재생하는 장치를 판매하는 판매업에서 경영적, 즉, 반복적이면서 계속적으로 이용할 수 있다.

도면의 간단한 설명

도 1은 저작권 보호시스템(1)의 전체를 도시한 도면.

도 2는 기록재생장치(10)의 구성을 도시한 블록도.

도 3은 암호화 콘텐츠 기록부(104)가 기억하고 있는 정보를 도시한 도면.

도 4는 암호화 콘텐츠 $EC2_1$로부터 이중 암호화 부분콘텐츠 $EEC2_1$로의 변환을 도시한 도면.

도 5는 휴대형 매체(20)의 구성을 도시한 블록도.

도 6은 기록가능영역(204)이 기억하고 있는 정보를 도시한 도면.

도 7은 휴대정보 단말(30)의 구성을 도시한 블록도.

도 8은 저작권 보호시스템(1)의 전체의 동작을 도시한 흐름도.

도 9는 제 1 이동처리의 동작을 도시한 흐름도.

도 10은 콘텐츠 이동처리의 동작을 도시한 흐름도.

도 11은 부분콘텐츠 이동처리의 동작을 도시한 흐름도.

도 12는 제 2 이동처리의 동작을 도시한 흐름도.

도 13은 콘텐츠 복호처리의 동작을 도시한 흐름도.

도 14는 저작권 보호시스템(2)의 전체를 도시한 도면.

도 15는 기록재생장치(50)의 구성을 도시한 블록도.

도 16은 변환용 데이터 기억부(508)가 기억하고 있는 정보를 도시한 도면.

도 17은 저작권 보호시스템(2)의 전체 동작을 도시한 흐름도.

도 18은 저작권 보호시스템(2)에서의 콘텐츠 기록처리의 동작을 도시한 흐름도.

도 19는 저작권 보호시스템(2)에서의 제 1 이동처리의 동작을 도시한 흐름도.

도 20은 저작권 보호시스템(2)에서의 콘텐츠 이동처리의 동작을 도시한 흐름도. 도 21로 이어진다.

도 21은 저작권 보호시스템(2)에서의 콘텐츠 이동처리의 동작을 도시한 흐름도. 도 20에서 이어진다.

도 22는 저작권 보호시스템(2)에서의 부분콘텐츠 이동처리의 동작을 도시한 흐름도.

도 23은 기록재생장치(50a)의 구성을 도시한 블록도.

도 24는 기록재생장치(50a)에서 행해지는 기록처리의 동작을 도시한 흐름도.

도 25는 기록재생장치(50a)에서 행해지는 이동처리의 동작을 도시한 흐름도.

도 26은 기록재생장치(50a)에서 행해지는 변환처리의 동작을 도시한 흐름도.

도 27은 기록재생장치(50a)가 암호화 콘텐츠 EC4를 생성하고, 휴대형 매체(20)에 기록하는 동작을 나타내는 흐름도.

도 28은 저작권 보호시스템(3)의 전체를 도시한 도면.

도 29는 기록가능영역(204b)이 기억하고 있는 정보를 도시한 도면.

(부호의 설명)

1 저작권 보호시스템 10 기록재생장치

11 콘텐츠 공급장치 12 모니터

13 스피커 20 휴대형 매체

30 휴대정보 단말 50 기록재생장치

101 콘텐츠 수신부 102 장치기록 키 기억부

103 제 1 암호화부 104 암호화 콘텐츠 기록부

105 재생부 106 매체기록 키 생성부

107 매체기록 키 기억부 108 제 1 복호부

109 암호화 콘텐츠 판독부 110 변환부

111 제 2 암호화부 112 이중 암호키 생성부

113 이중 암호키 기억부 114 이중 암호화부

115 이중 암호화 콘텐츠 기록부 116 제 2 복호부

117 기록/판독부 118 입력부

201 입출력부 202 제어부

203 기억부 204 기록가능영역

205 판독전용영역 210 암호화 콘텐츠 기억영역

211 매체기록 키 기억영역 212 이중 암호키 기억영역

213 콘텐츠 ID 기억영역 220 휴대형 매체 ID 기억영역

221 MKB 기억영역 301 디바이스 키 기억부

302 입출력부 303 제어부

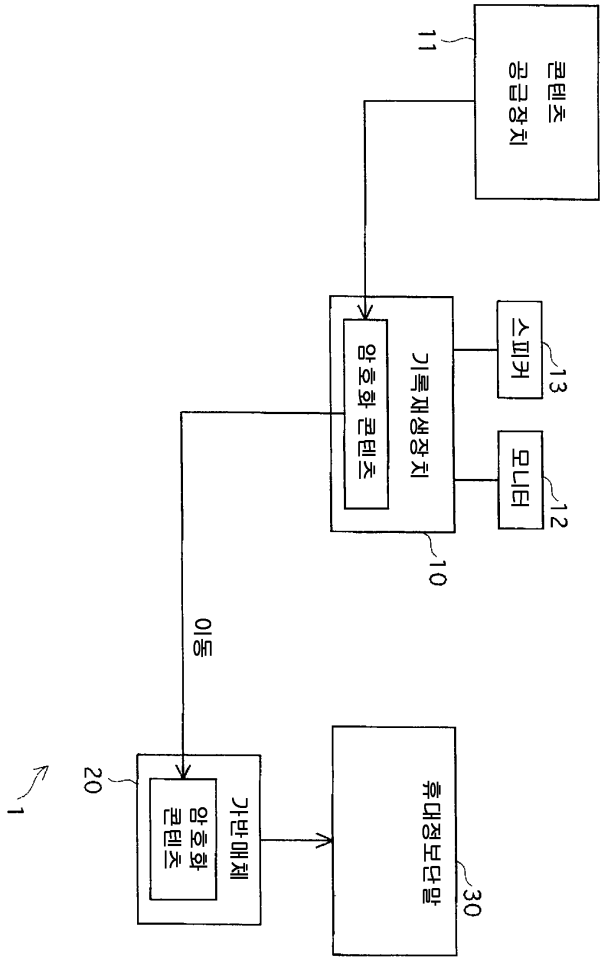
304 표시부 305 키 조작부

306 통신부 307 안테나

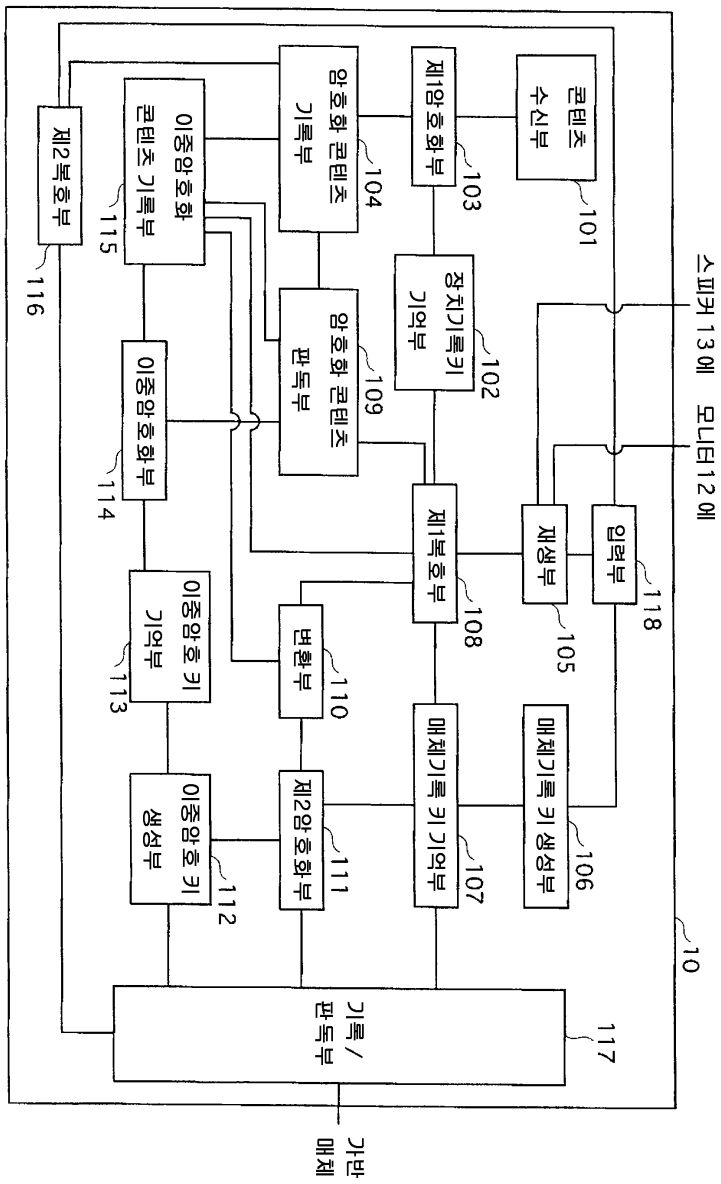
308 마이크 309 스피커

도면

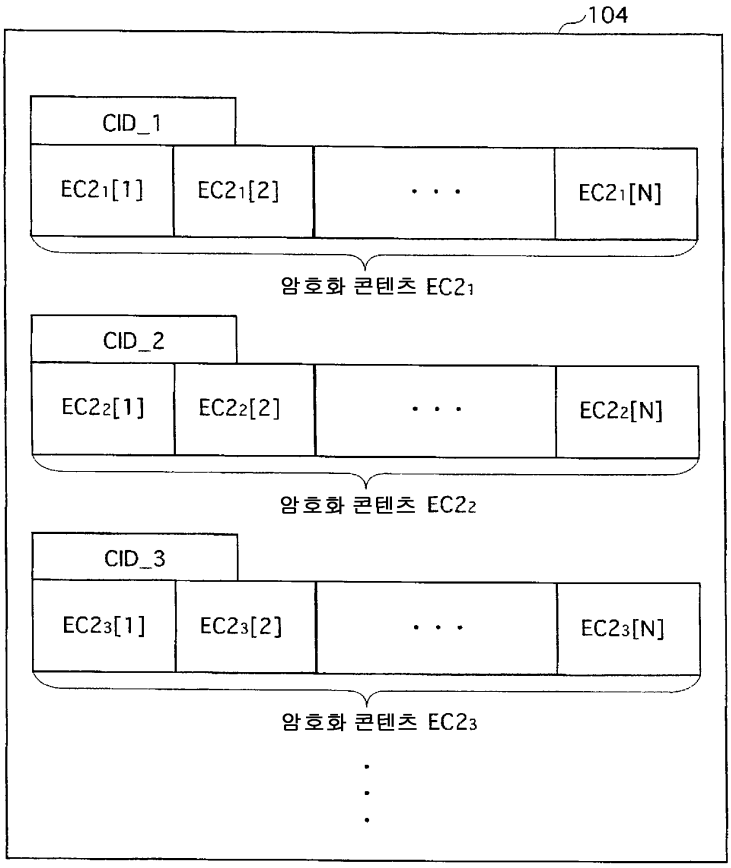
도면1


콘텐츠
공급장치
11
기록재생장치
암호화 콘텐츠
스피커
13
모니터
12
10
이동
1
20
가방매체
암호화
콘텐츠
휴대정보단말
30

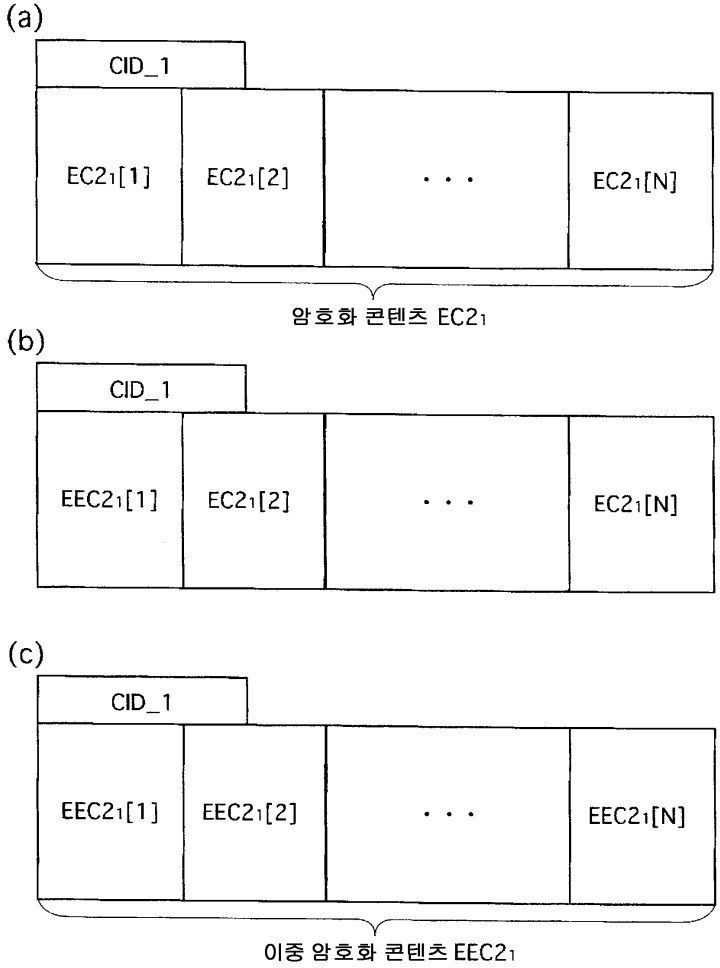
도면2


콘텐츠 수신부
101
제1암호화부
103
암호화 콘텐츠 기록부
104
이중암호화 콘텐츠 기록부
115
제2복호부
116
장치기록키 기억부
102
암호화 콘텐츠 판독부
109
이중암호화부
114
제1복호부
108
재생부
105
입력부
118
스피커 13 에
모니터 12 에
이중암호키 기억부
113
변환부
110
이중암호키 생성부
112
제2암호화부
111
매체기록 키 기억부
107
매체기록 키 생성부
106
기록 / 판독부
117
10
가반 매체

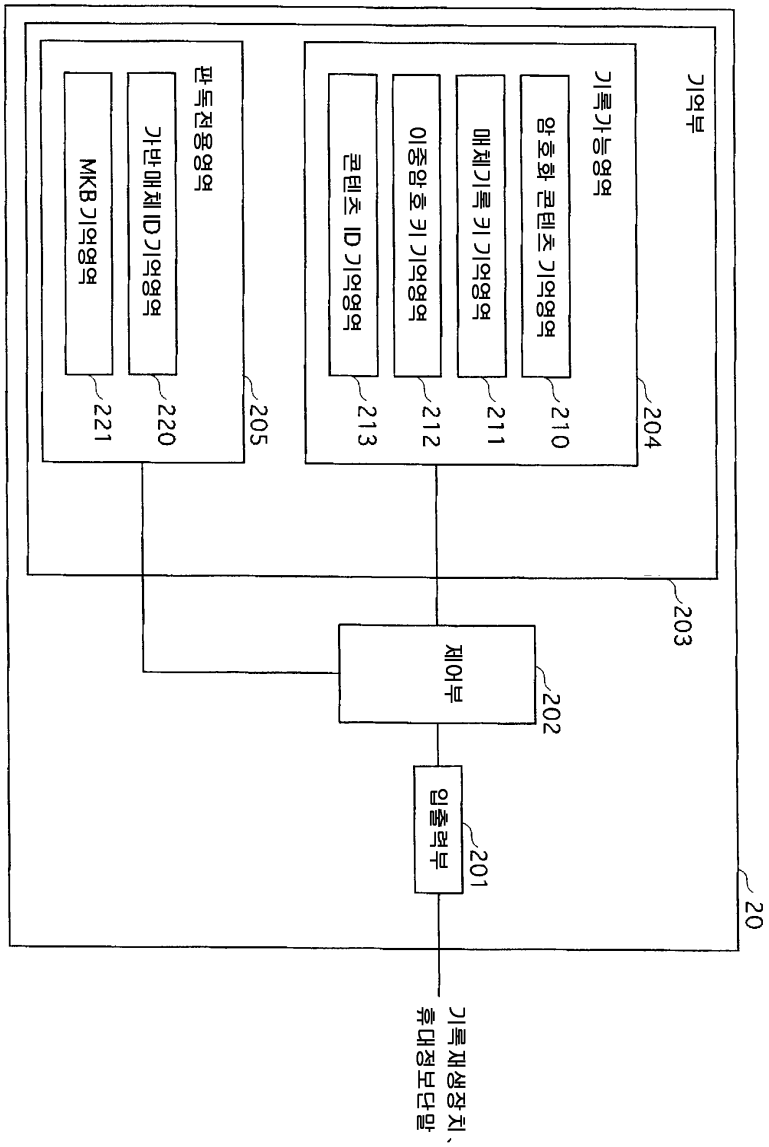
도면3


104
CID_1
EC2₁[1]
EC2₁[2]
· · ·
EC2₁[N]
암호화 콘텐츠 EC2₁
CID_2
EC2₂[1]
EC2₂[2]
· · ·
EC2₂[N]
암호화 콘텐츠 EC2₂
CID_3
EC2₃[1]
EC2₃[2]
· · ·
EC2₃[N]
암호화 콘텐츠 EC2₃

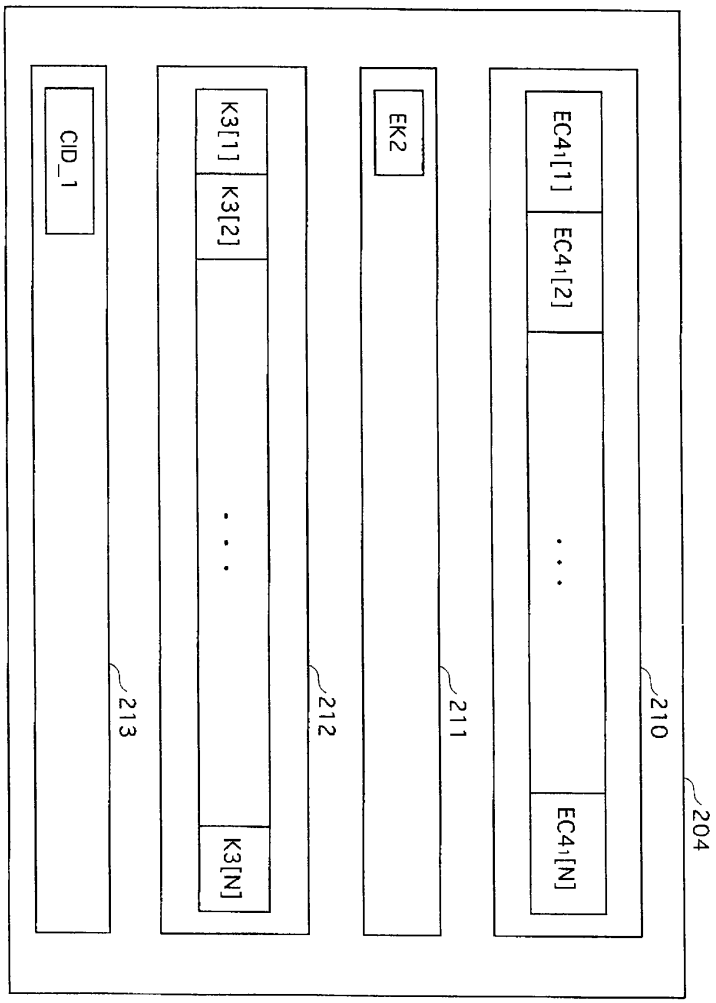
도면4


(a)
CID_1
EC2₁[1]
EC2₁[2]
· · ·
EC2₁[N]
암호화 콘텐츠 EC2₁
(b)
CID_1
EEC2₁[1]
EC2₁[2]
· · ·
EC2₁[N]
(c)
CID_1
EEC2₁[1]
EEC2₁[2]
· · ·
EEC2₁[N]
이중 암호화 콘텐츠 EEC2₁

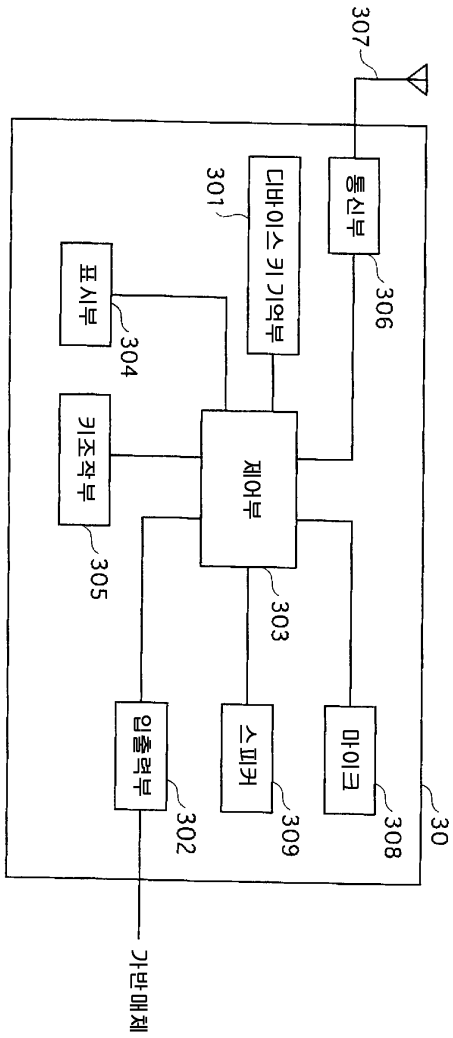
도면5


20
기억부
203
기록가능영역
204
암호화 콘텐츠 기억영역
210
매체기록 키 기억영역
211
이중암호 키 기억영역
212
콘텐츠 ID 기억영역
213
판독전용영역
205
가반매체 ID 기억영역
220
MKB 기억영역
221
제어부
202
입출력부
201
기록재생장치、
휴대정보단말

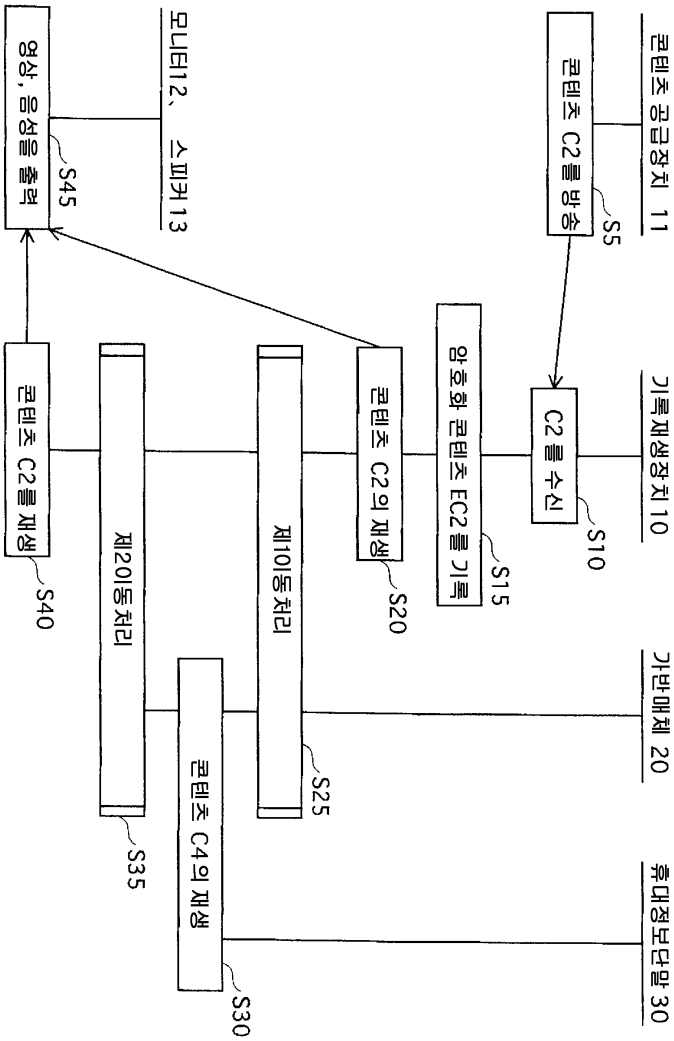
도면6



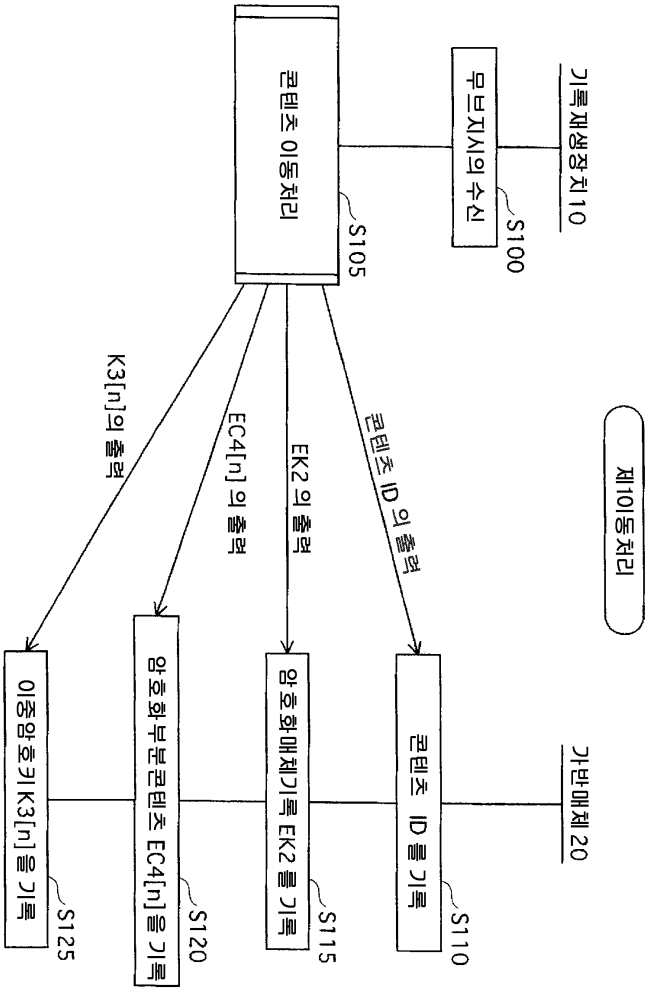
도면7


307
통신부
306
디바이스 키 기억부
301
표시부
304
키조작부
305
제어부
303
입출력부
302
스피커
309
마이크
308
30
가반매체

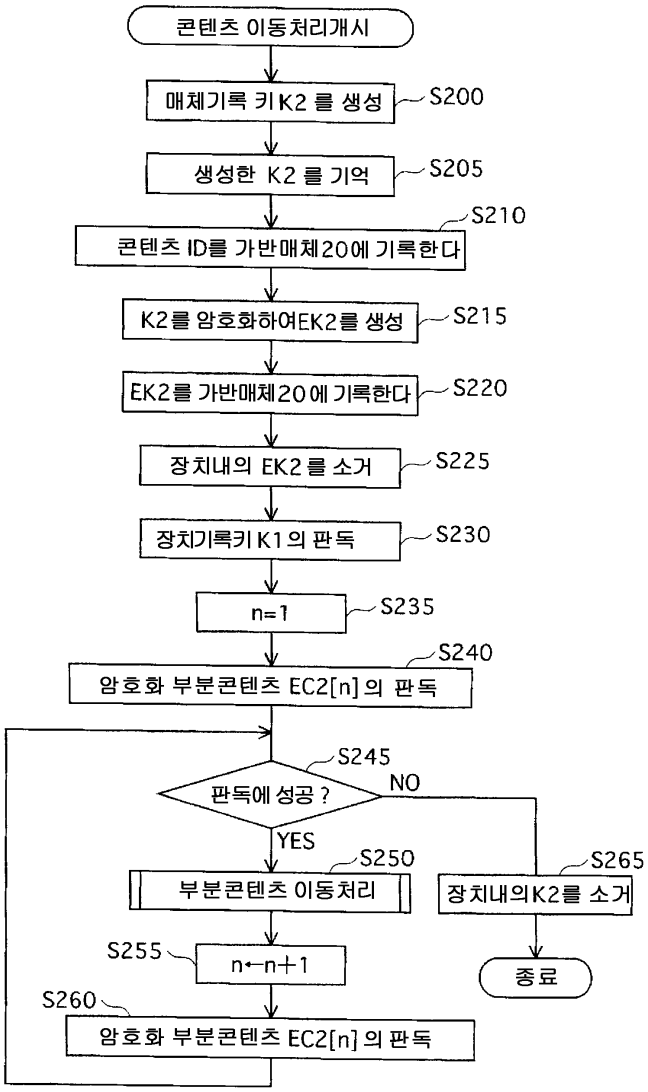
도면8


콘텐츠 공급장치 11
콘텐츠 C2를 방송
S5
기록재생장치 10
C2 를 수신
S10
암호화 콘텐츠 EC2 를 기록
S15
콘텐츠 C2의 재생
S20
제1이동처리
S25
가반매체 20
콘텐츠 C4의 재생
S30
휴대정보단말 30
제2이동처리
S35
콘텐츠 C2를 재생
S40
영상, 음성을 출력
S45
모니터12、 스피커 13

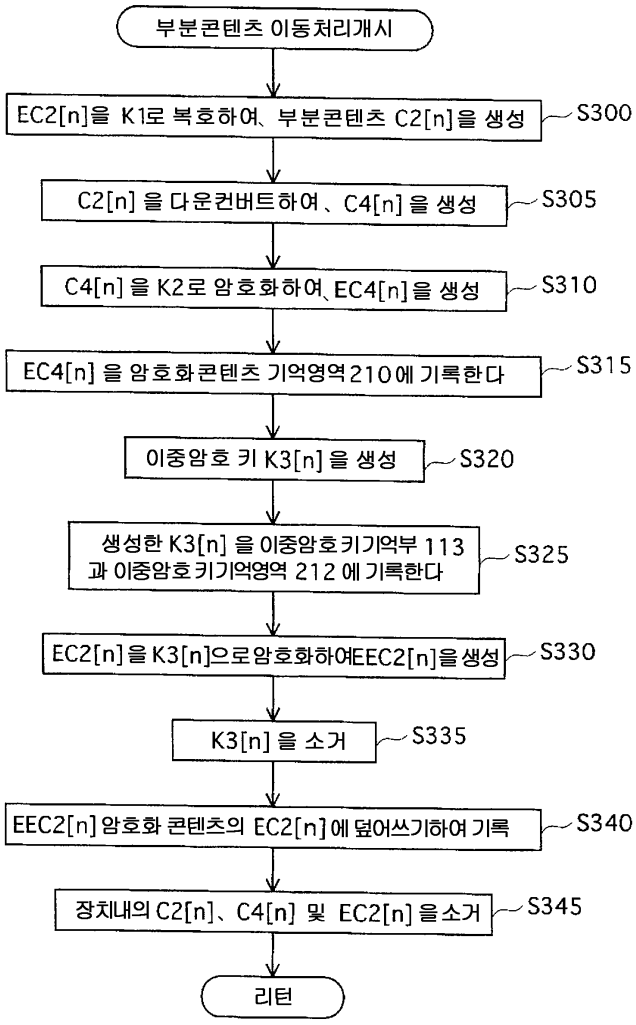
도면9


제10동처리
기록재생장치10
가반매체 20
무브지시의 수신
S100
콘텐츠 이동처리
S105
콘텐츠 ID 의 출력
EK2 의 출력
EC4[n] 의 출력
K3[n]의 출력
콘텐츠 ID 를 기록
S110
암호화매체기록 EK2 를 기록
S115
암호화부분콘텐츠 EC4[n]을 기록
S120
이중암호키 K3[n]을 기록
S125

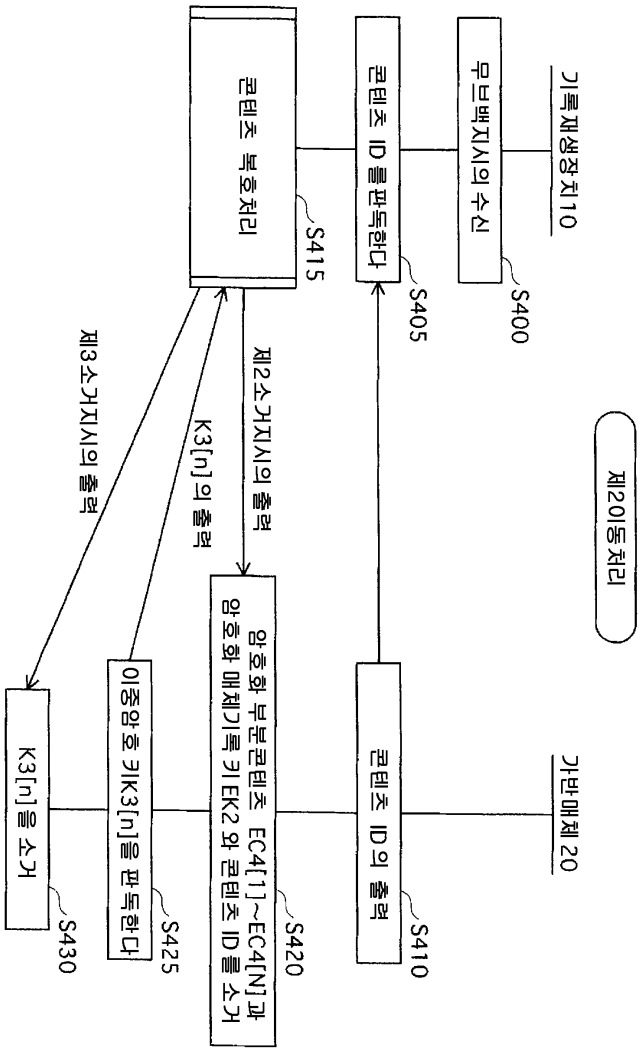
도면10


콘텐츠 이동처리개시
매체기록 키 K2 를 생성
S200
생성한 K2 를 기억
S205
콘텐츠 ID를 가반매체20에 기록한다
S210
K2를 암호화하여EK2를 생성
S215
EK2를 가반매체20에 기록한다
S220
장치내의 EK2 를 소거
S225
장치기록키 K1의 판독
S230
n=1
S235
암호화 부분콘텐츠 EC2[n]의 판독
S240
판독에 성공 ?
S245
NO
YES
부분콘텐츠 이동처리
S250
장치내의K2를 소거
S265
n←n+1
S255
종료
암호화 부분콘텐츠 EC2[n]의 판독
S260

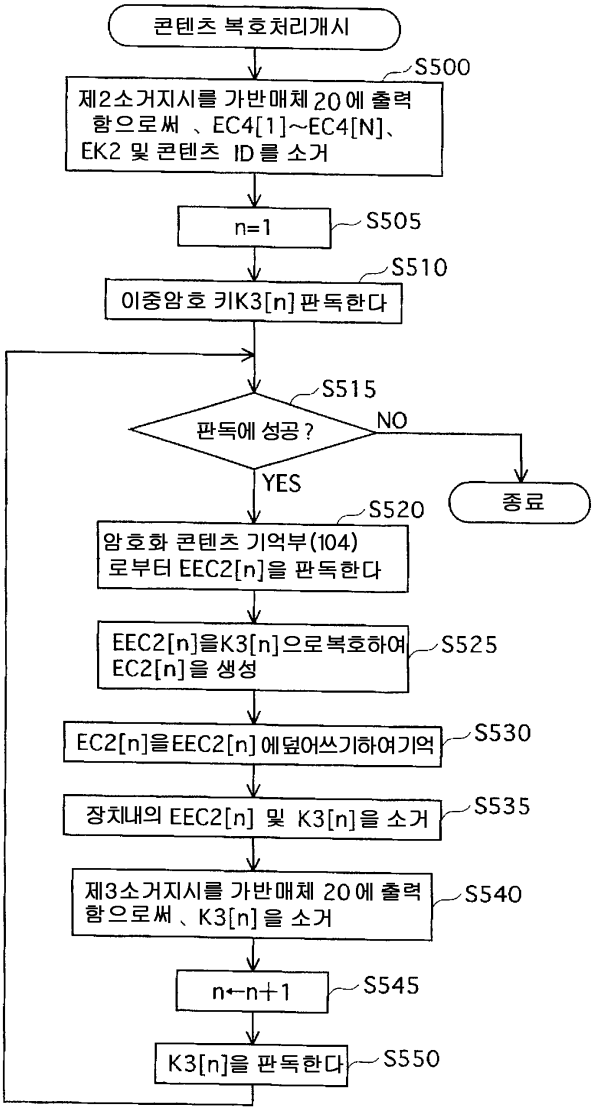
도면11


부분콘텐츠 이동처리개시
EC2[n]을 K1로 복호하여, 부분콘텐츠 C2[n]을 생성
S300
C2[n]을 다운컨버트하여, C4[n]을 생성
S305
C4[n]을 K2로 암호화하여, EC4[n]을 생성
S310
EC4[n]을 암호화콘텐츠 기억영역 210에 기록한다
S315
이중암호 키 K3[n]을 생성
S320
생성한 K3[n]을 이중암호키기억부 113과 이중암호키기억영역 212에 기록한다
S325
EC2[n]을 K3[n]으로암호화하여EEC2[n]을생성
S330
K3[n]을 소거
S335
EEC2[n]암호화 콘텐츠의 EC2[n]에 덮어쓰기하여 기록
S340
장치내의 C2[n], C4[n] 및 EC2[n]을소거
S345
리턴

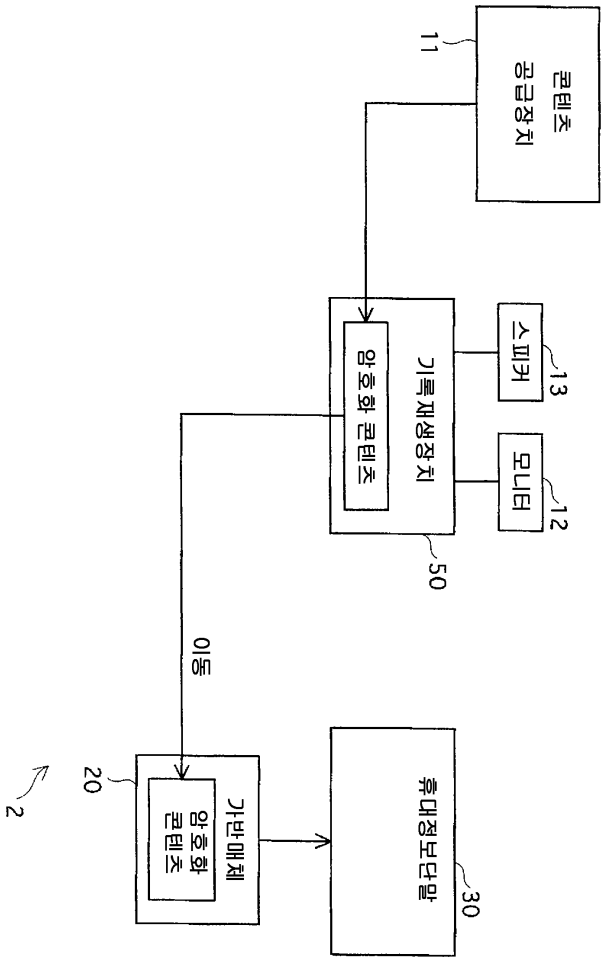
도면12


제2이동처리
기록재생장치10
무브백지시의 수신
S400
콘텐츠 ID를 판독한다
S405
콘텐츠 복호처리
S415
제2소거지시의 출력
K3[n]의 출력
제3소거지시의 출력
콘텐츠 ID의 출력
S410
암호화 부분콘텐츠 EC4[1]~EC4[N]과 암호화 매체기록 키 EK2 와 콘텐츠 ID를 소거
S420
이중암호 키K3[n]을 판독한다
S425
K3[n]을 소거
S430
가반매체 20

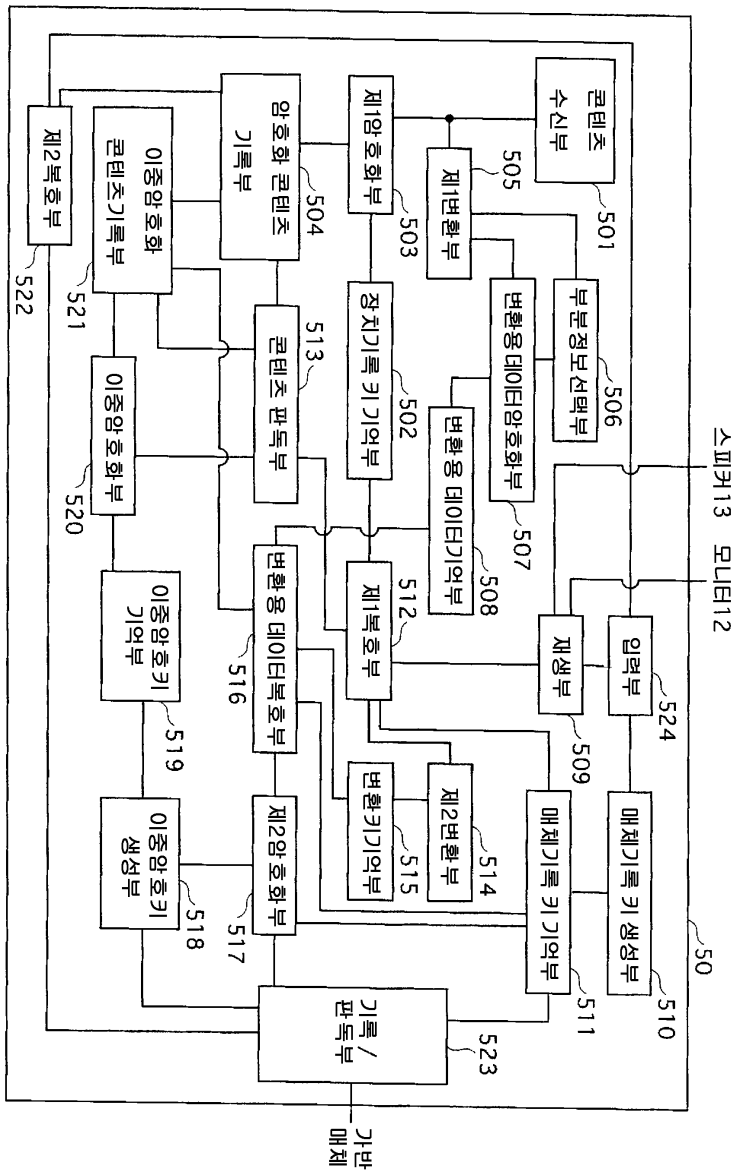
도면13


콘텐츠 복호처리개시
S500
제2소거지시를 가반매체 20에 출력함으로써 、EC4[1]~EC4[N]、EK2 및 콘텐츠 ID를 소거
n=1
S505
S510
이중암호 키K3[n]판독한다
S515
판독에 성공?
NO
종료
YES
S520
암호화 콘텐츠 기억부(104)로부터 EEC2[n]을 판독한다
EEC2[n]을K3[n]으로복호하여EC2[n]을 생성
S525
EC2[n]을EEC2[n]에덮어쓰기하여기억
S530
장치내의 EEC2[n] 및 K3[n]을 소거
S535
제3소거지시를 가반매체 20에 출력함으로써、K3[n]을 소거
S540
n←n+1
S545
K3[n]을 판독한다
S550

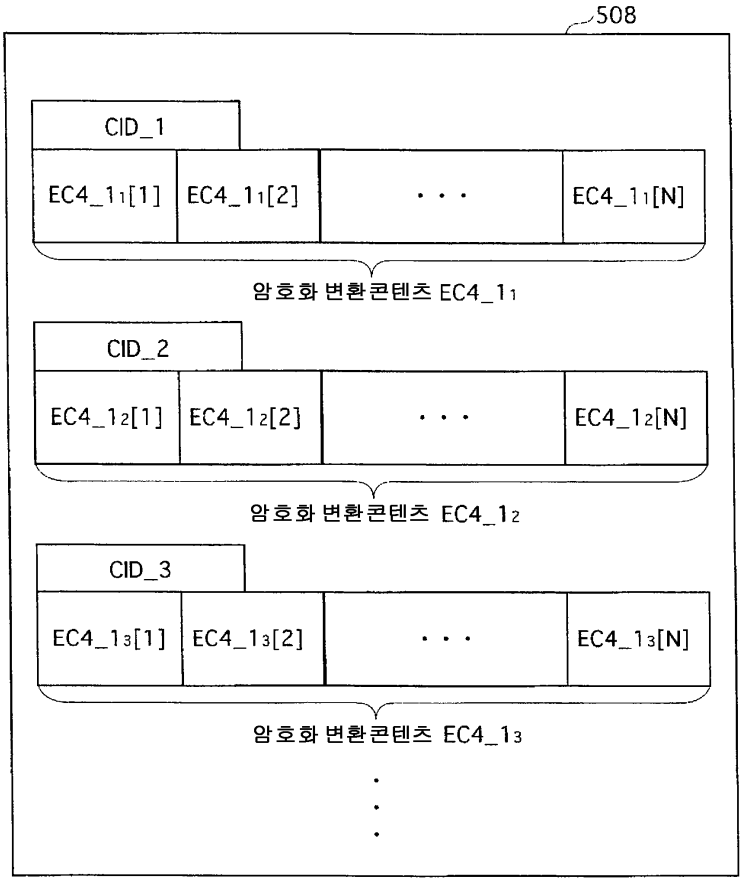
도면14


콘텐츠
공급장치
11
기록재생장치
암호화 콘텐츠
50
스피커
13
모니터
12
이동
2
20
가반매체
암호화
콘텐츠
휴대정보단말
30

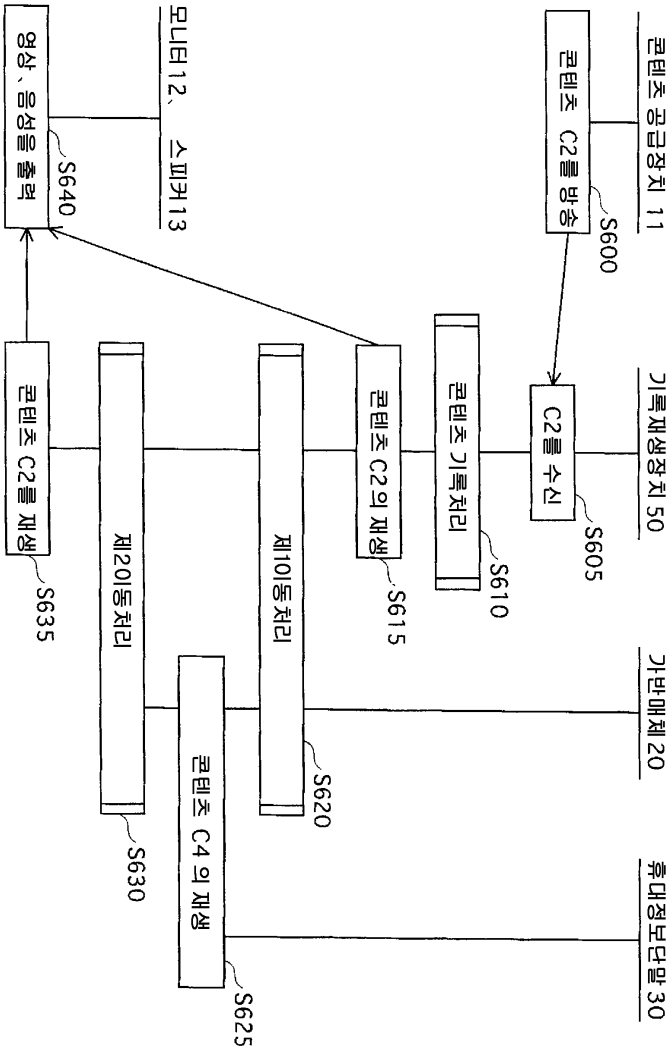
도면15


콘텐츠 수신부
501
제1변환부
505
부분정보선택부
506
변환용 데이터암호화부
507
변환용 데이터기억부
508
재생부
509
매체기록 키 생성부
510
매체기록 키 기억부
511
제1복호부
512
변환키기억부
515
제2변환부
514
입력부
524
스피커13
모니터12
50
제1암호화부
503
장치기록 키 기억부
502
암호화 콘텐츠 기록부
504
콘텐츠 판독부
513
변환용 데이터복호부
516
제2암호화부
517
기록/판독부
523
가반매체
제2복호부
522
이중암호화 콘텐츠기록부
521
이중암호화부
520
이중암호키 기억부
519
이중암호키 생성부
518

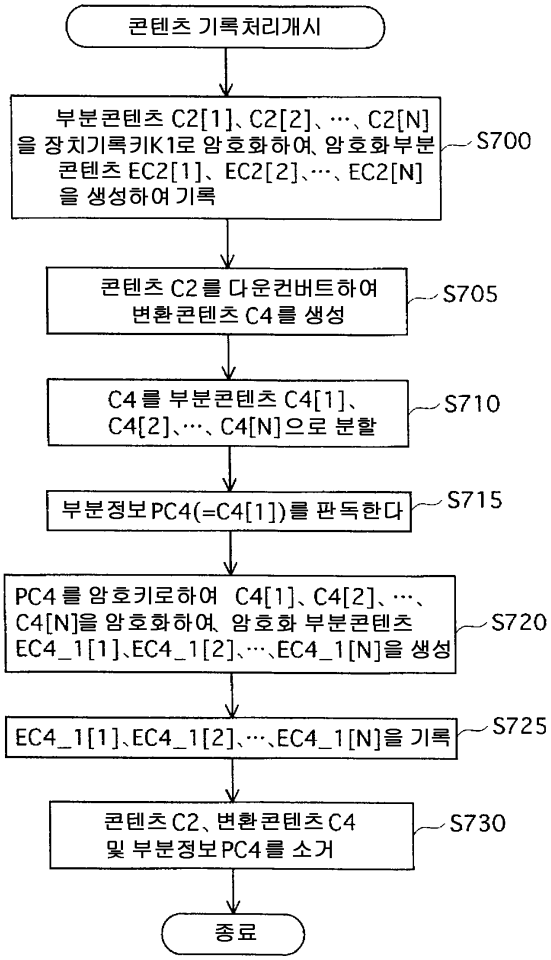
도면16


508
CID_1
EC4_11[1]
EC4_11[2]
· · ·
EC4_11[N]
암호화 변환콘텐츠 EC4_11
CID_2
EC4_12[1]
EC4_12[2]
· · ·
EC4_12[N]
암호화 변환콘텐츠 EC4_12
CID_3
EC4_13[1]
EC4_13[2]
· · ·
EC4_13[N]
암호화 변환콘텐츠 EC4_13

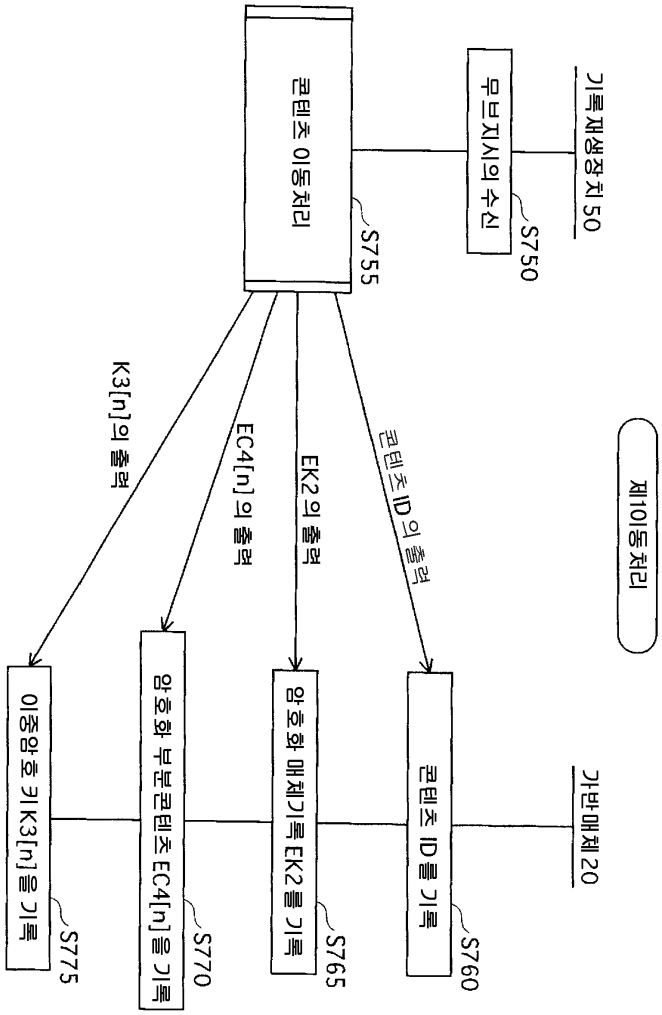
도면17


콘텐츠 공급장치 11
콘텐츠 C2를 방송
S600
기록재생장치 50
C2를 수신
S605
콘텐츠 기록처리
S610
콘텐츠 C2의 재생
S615
제1이동처리
S620
가반매체 20
콘텐츠 C4 의 재생
S625
휴대정보단말 30
제2이동처리
S630
콘텐츠 C2를 재생
S635
영상、음성을 출력
S640
모니터12、스피커13

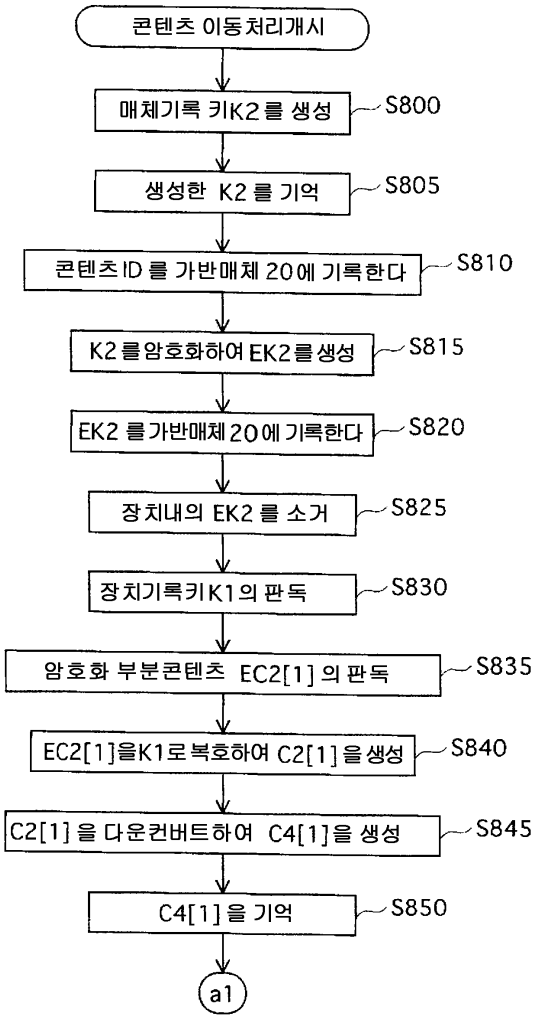
도면18


콘텐츠 기록처리개시
부분콘텐츠 C2[1]、C2[2]、…、C2[N]을 장치기록키K1로 암호화하여、암호화부분콘텐츠 EC2[1]、EC2[2]、…、EC2[N]을 생성하여 기록
S700
콘텐츠 C2를 다운컨버트하여 변환콘텐츠 C4를 생성
S705
C4를 부분콘텐츠 C4[1]、C4[2]、…、C4[N]으로 분할
S710
부분정보 PC4(=C4[1])를 판독한다
S715
PC4를 암호키로하여 C4[1]、C4[2]、…、C4[N]을 암호화하여、암호화 부분콘텐츠 EC4_1[1]、EC4_1[2]、…、EC4_1[N]을 생성
S720
EC4_1[1]、EC4_1[2]、…、EC4_1[N]을 기록
S725
콘텐츠 C2、변환콘텐츠 C4 및 부분정보 PC4를 소거
S730
종료

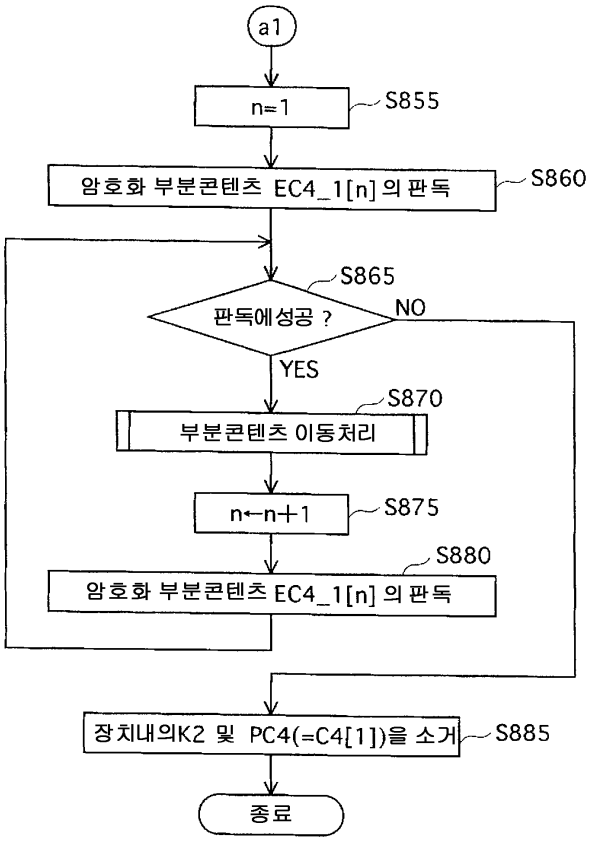
도면19


제1이동처리
기록재생장치 50
무브지시의 수신
S750
콘텐츠 이동처리
S755
K3[n]의 출력
EC4[n]의 출력
EK2의 출력
콘텐츠 ID의 출력
가반매체 20
이중암호 키K3[n]을 기록
S775
암호화 부분콘텐츠 EC4[n]을 기록
S770
암호화 매체기록 EK2를 기록
S765
콘텐츠 ID를 기록
S760

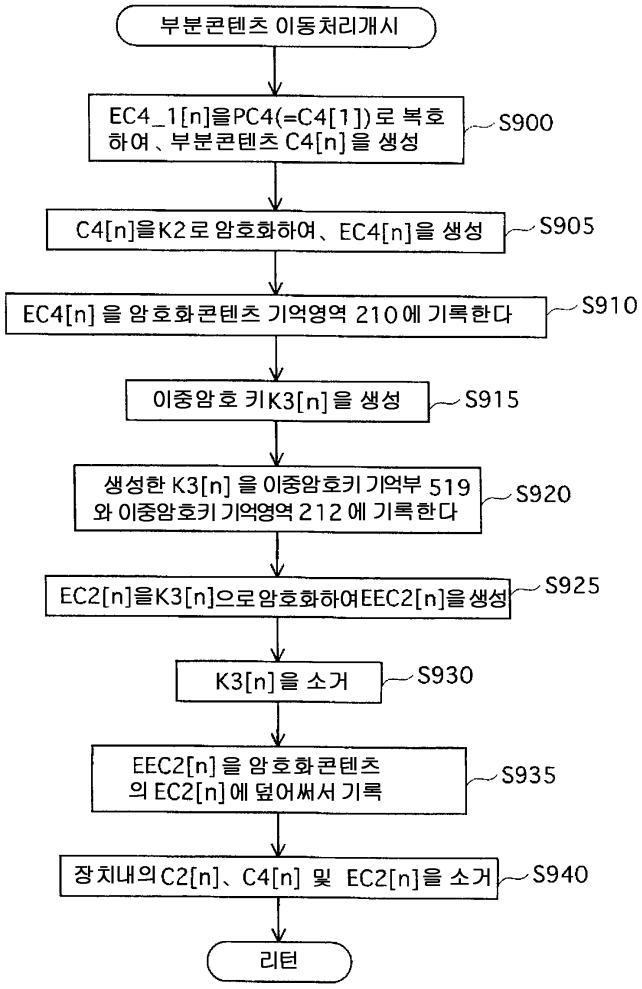
도면20


콘텐츠 이동처리개시
매체기록 키K2 를 생성
S800
생성한 K2 를 기억
S805
콘텐츠ID 를 가반매체 20에 기록한다
S810
K2 를암호화하여 EK2를생성
S815
EK2 를가반매체 20에 기록한다
S820
장치내의 EK2 를 소거
S825
장치기록키K1의 판독
S830
암호화 부분콘텐츠 EC2[1] 의 판독
S835
EC2[1]을K1로 복호하여 C2[1] 을생성
S840
C2[1] 을 다운컨버트하여 C4[1]을 생성
S845
C4[1] 을 기억
S850
a1

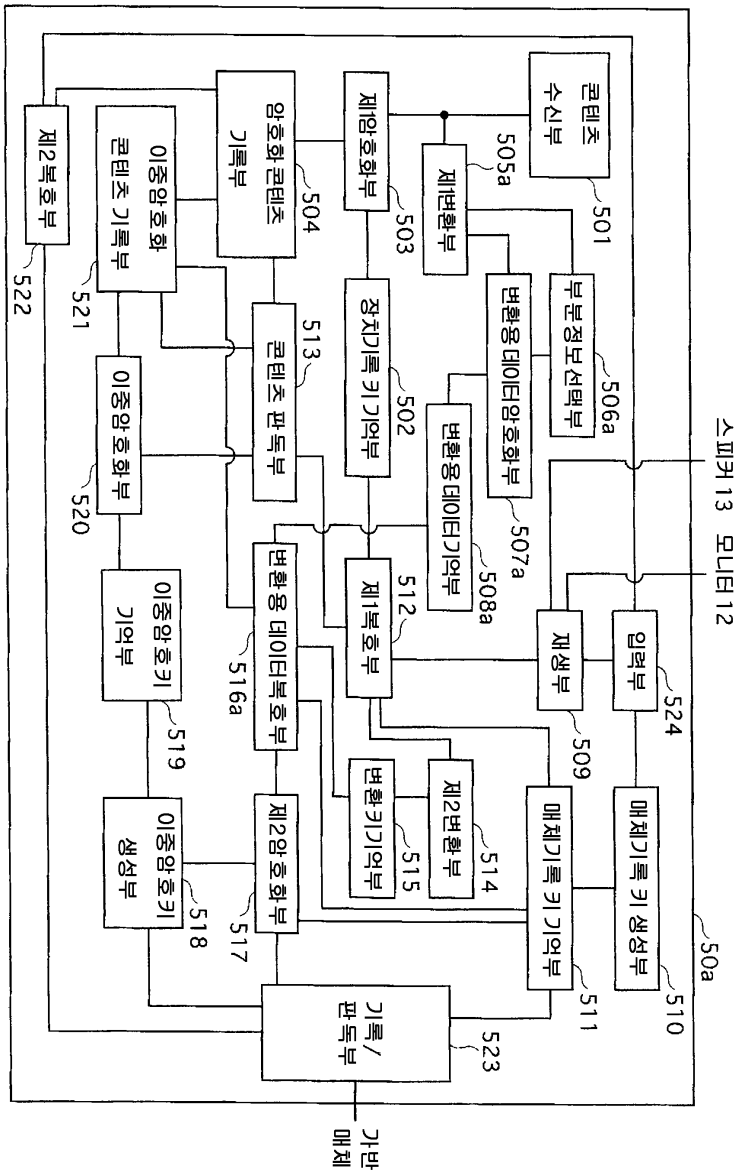
도면21


a1
n=1
S855
암호화 부분콘텐츠 EC4_1[n]의 판독
S860
S865
판독에성공 ?
NO
YES
S870
부분콘텐츠 이동처리
n←n+1
S875
S880
암호화 부분콘텐츠 EC4_1[n]의 판독
장치내의K2 및 PC4(=C4[1])을 소거
S885
종료

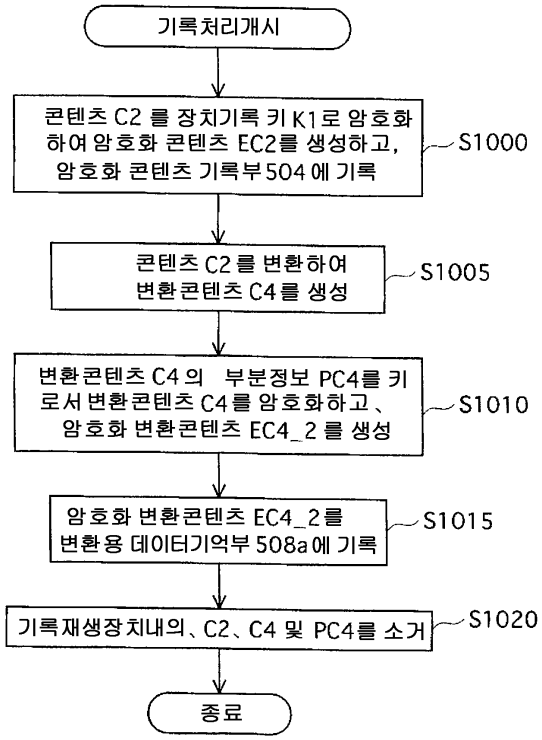
도면22


부분콘텐츠 이동처리개시
EC4_1[n]을PC4(=C4[1])로 복호하여、부분콘텐츠 C4[n]을 생성
S900
C4[n]을K2로 암호화하여、EC4[n]을 생성
S905
EC4[n] 을 암호화콘텐츠 기억영역 210에 기록한다
S910
이중암호 키K3[n]을 생성
S915
생성한 K3[n] 을 이중암호키 기억부 519와 이중암호키 기억영역 212에 기록한다
S920
EC2[n]을K3[n]으로암호화하여EEC2[n]을생성
S925
K3[n]을 소거
S930
EEC2[n] 을 암호화콘텐츠의 EC2[n]에 덮어써서 기록
S935
장치내의C2[n]、C4[n] 및 EC2[n]을 소거
S940
리턴

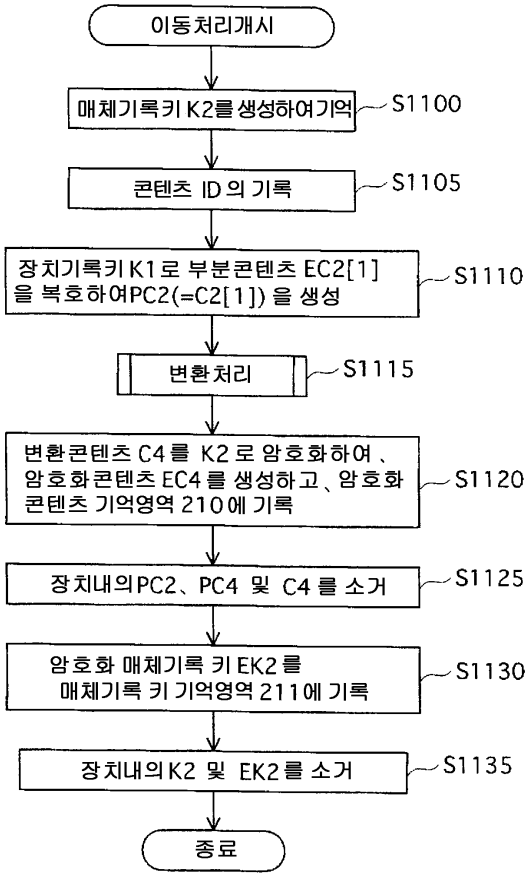
도면23


콘텐츠 수신부
501
제1변환부
505a
제1암호화부
503
암호화 콘텐츠 기록부
504
제2복호부
522
이중암호화 콘텐츠 기록부
521
이중암호화부
520
이중암호키 기억부
519
이중암호키 생성부
518
부분정보선택부
506a
변환용 데이터암호화부
507a
변환용 데이터기억부
508a
장치기록 키 기억부
502
콘텐츠 판독부
513
변환용 데이터복호부
516a
제1복호부
512
재생부
509
입력부
524
매체기록 키 생성부
510
매체기록 키 기억부
511
제2변환부
514
변환키기억부
515
제2암호화부
517
기록/판독부
523
스피커 13
모니터 12
50a
가반 매체

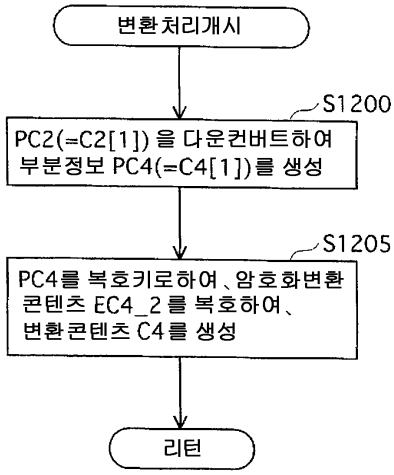
도면24


기록처리개시
콘텐츠 C2 를 장치기록 키 K1로 암호화 하여 암호화 콘텐츠 EC2를 생성하고, 암호화 콘텐츠 기록부 504 에 기록
S1000
콘텐츠 C2 를 변환하여 변환콘텐츠 C4 를 생성
S1005
변환콘텐츠 C4 의 부분정보 PC4를 키로서 변환콘텐츠 C4 를 암호화하고, 암호화 변환콘텐츠 EC4_2 를 생성
S1010
암호화 변환콘텐츠 EC4_2를 변환용 데이터기억부 508a에 기록
S1015
기록재생장치내의 C2, C4 및 PC4를 소거
S1020
종료

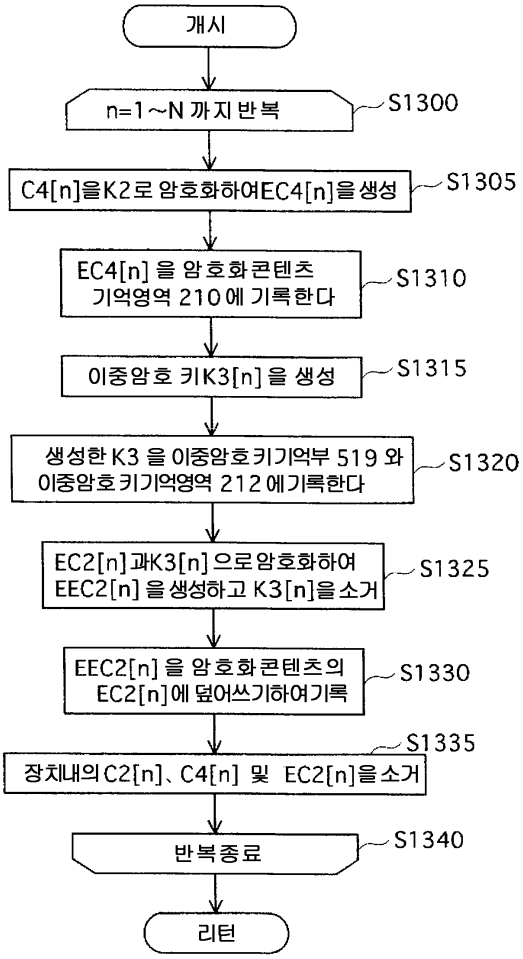
도면25


이동처리개시
매체기록키 K2를 생성하여기억
S1100
콘텐츠 ID의 기록
S1105
장치기록키 K1로 부분콘텐츠 EC2[1]을 복호하여PC2(=C2[1]) 을 생성
S1110
변환처리
S1115
변환콘텐츠 C4를 K2로 암호화하여, 암호화콘텐츠 EC4를 생성하고, 암호화콘텐츠 기억영역 210에 기록
S1120
장치내의PC2, PC4 및 C4를 소거
S1125
암호화 매체기록 키 EK2를 매체기록 키 기억영역 211에 기록
S1130
장치내의K2 및 EK2를 소거
S1135
종료

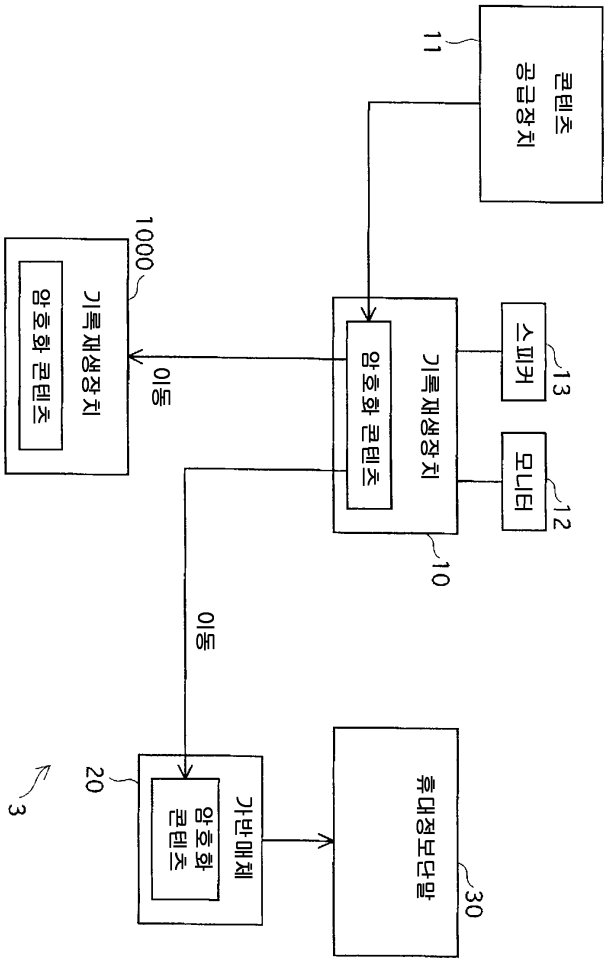
도면26


변환처리개시
S1200
PC2(=C2[1]) 을 다운컨버트하여 부분정보 PC4(=C4[1])를 생성
S1205
PC4를 복호키로하여, 암호화변환콘텐츠 EC4_2를 복호하여, 변환콘텐츠 C4를 생성
리턴

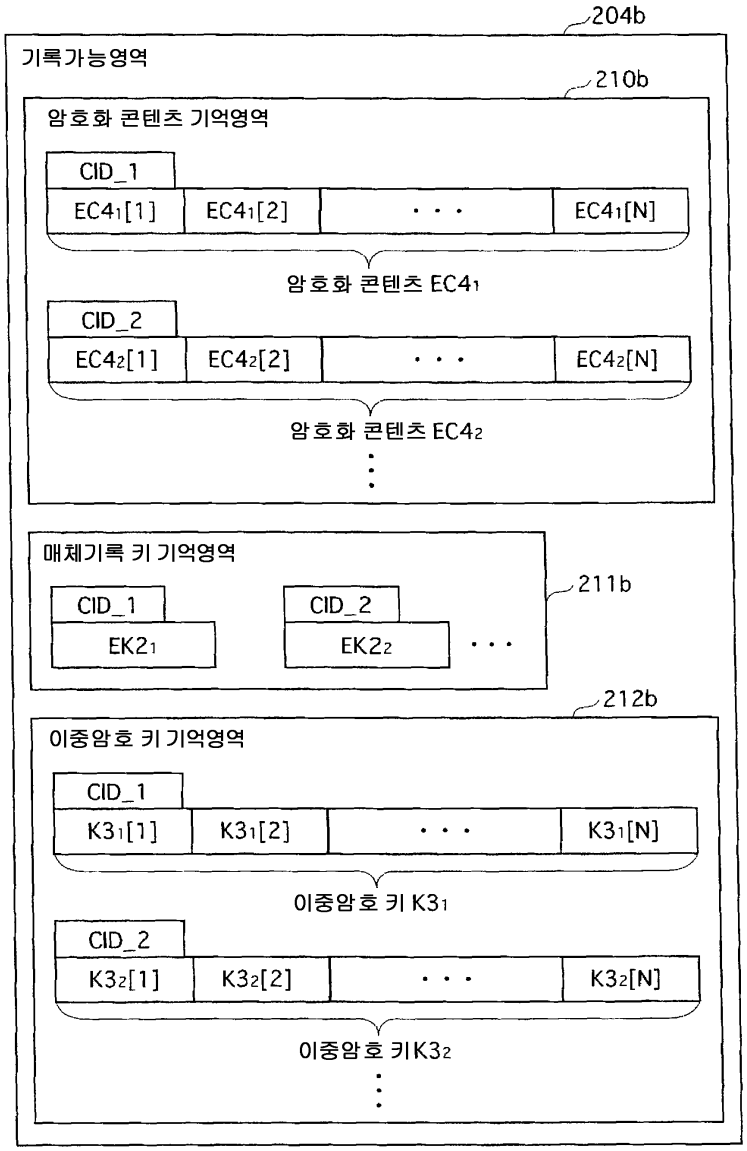
도면27


개시
n=1~N 까지 반복
S1300
C4[n]을K2로 암호화하여EC4[n]을생성
S1305
EC4[n] 을 암호화콘텐츠 기억영역 210에 기록한다
S1310
이중암호 키K3[n] 을 생성
S1315
생성한 K3 을 이중암호키기억부 519 와 이중암호키기억영역 212에기록한다
S1320
EC2[n]과K3[n]으로암호화하여 EEC2[n] 을생성하고 K3[n]을소거
S1325
EEC2[n] 을 암호화콘텐츠의 EC2[n]에 덮어쓰기하여기록
S1330
장치내의C2[n]、C4[n] 및 EC2[n]을소거
S1335
반복종료
S1340
리턴

도면28


콘텐츠
공급장치
11
1000
기록재생장치
암호화 콘텐츠
이동
기록재생장치
암호화 콘텐츠
스피커
13
모니터
12
10
이동
3
20
가반매체
암호화
콘텐츠
휴대정보단말
30

도면29


204b
기록가능영역
210b
암호화 콘텐츠 기억영역
CID_1
EC4₁[1]
EC4₁[2]
• • •
EC4₁[N]
암호화 콘텐츠 EC4₁
CID_2
EC4₂[1]
EC4₂[2]
• • •
EC4₂[N]
암호화 콘텐츠 EC4₂
매체기록 키 기억영역
211b
CID_1
EK2₁
CID_2
EK2₂
• • •
212b
이중암호 키 기억영역
CID_1
K3₁[1]
K3₁[2]
• • •
K3₁[N]
이중암호 키 K3₁
CID_2
K3₂[1]
K3₂[2]
• • •
K3₂[N]
이중암호 키K3₂