(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0119793
(43) 공개일자 2012년10월31일

(51) 국제특허분류(Int. Cl.)
G06F 21/24 (2006.01)
(21) 출원번호 10-2011-0037987
(22) 출원일자 2011년04월22일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
신준범
경기도 수원시 영통구 봉영로 1526, 살구골7단지 아파트 717동 104호 (영통동)
차병호
경기도 수원시 영통구 동탄원천로881번길 35, 507동 406호 (매탄동, 주공그린빌)
(74) 대리인
리앤목특허법인

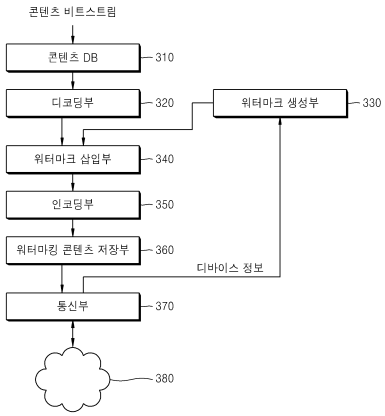
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **해킹 추적을 위한 워터 마킹 방법 및 장치 및 그를 이용한 해킹 콘텐츠 차단 방법 및 장치**

(57) 요 약

본 발명은 해킹 추적을 위한 워터 마킹 방법 및 장치 및 그를 이용한 해킹 콘텐츠 차단 방법에 관한 것으로, 본 발명의 일 실시 예는 정해진 네트워크 채널을 통해 콘텐츠를 공유할 수신 디바이스와 디바이스 정보를 송수신하는 과정, 송수신된 송수신 디바이스 정보에 기반 한 워터마크 데이터를 생성하는 과정, 생성된 워터마크 데이터를 콘텐츠에 삽입하여 워터 마킹된 멀티미디어 콘텐츠를 생성하는 과정, 해킹 콘텐츠가 발견되면 해킹 콘텐츠로부터 워터마크 데이터를 검출하는 과정, 검출된 워터마크 데이터로부터 송수신 디바이스 정보를 검출하는 과정, 송수신 디바이스 정보를 바탕으로 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회하는 과정을 포함한다.

대 표 도 - 도3



특허청구의 범위

청구항 1

해킹 추적을 위한 워터 마킹 방법에 있어서,

정해진 네트워크 채널을 통해 콘텐츠를 공유할 디바이스와 디바이스 정보를 송수신하는 과정;

상기 송수신된 디바이스 정보에 기반 한 워터마크 데이터를 생성하는 과정;

상기 생성된 워터마크 데이터를 콘텐츠에 삽입하여 워터 마킹된 멀티미디어 콘텐츠를 생성하는 과정을 포함하는 해킹 콘텐츠 추적을 위한 워터 마킹 방법.

청구항 2

제1항에 있어서, 상기 워터 마킹된 콘텐츠를 상기 수신 디바이스로 전송하는 과정을 더 포함하는 해킹 추적을 위한 워터 마킹 방법.

청구항 3

제1항에 있어서, 상기 디바이스 정보는 송신 디바이스 ID 및 수신 디바이스 ID 를 포함하는 것을 특징으로 하는 해킹 추적을 위한 워터 마킹 방법.

청구항 4

제3항에 있어서, 상기 워터마크 데이터는 상기 송수신 디바이스 정보 및 콘텐츠 공유 순서 번호들 중 적어도 하나로 구성되는 것을 특징으로 하는 해킹 추적을 위한 워터 마킹 방법.

청구항 5

제1항에 있어서, 상기 워터마크 데이터 생성 및 삽입은 콘텐츠를 공유하는 디바이스들 각각에 대해서 동일하게 수행되는 것임을 특징으로 하는 해킹 추적을 위한 워터 마킹 방법.

청구항 6

제1항에 있어서, 상기 송신 디바이스 정보 및 수신 디바이스 정보에 대한 룩-업 테이블을 구축하는 과정을 더 포함하는 해킹 추적을 위한 워터 마킹 방법.

청구항 7

제1항에 있어서, 상기 디바이스 정보를 삽입할 수 있는 워터마크 도메인을 구성하는 과정을 더 포함하는 해킹 추적을 위한 워터 마킹 방법.

청구항 8

제1항에 있어서, 워터 마킹된 멀티미디어 콘텐츠 생성 과정은,

상기 멀티미디어 콘텐츠에 디바이스 관련 정보를 삽입할 수 있는 특정 위치를 정의하고,

상기 정의된 멀티미디어 콘텐츠의 특정 위치에 워터마크 데이터를 삽입하는 것임을 특징으로 하는 해킹 추적을 위한 워터 마킹 방법.

청구항 9

제1항에 있어서, 상기 수신 디바이스 정보는 수신 디바이스로 재 전송 시 삭제되는 것임을 특징으로 하는 해킹 추적을 위한 워터 마킹 방법.

청구항 10

해킹 콘텐츠 차단 방법에 있어서,

서버에서 수집되는 콘텐츠에 대해 해킹 여부를 모니터링 하는 과정;

해킹 콘텐츠가 발견되면 상기 해킹 콘텐츠로부터 워터마크 데이터를 검출하는 과정;

상기 검출된 워터마크 데이터로부터 송수신 디바이스 정보를 검출하는 과정;

상기 송수신 디바이스 정보를 바탕으로 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회하는 과정을 포함하는 해킹 콘텐츠 차단 방법.

청구항 11

제10항에 있어서, 상기 콘텐츠의 진행 경로 추출 과정은

상기 디코딩된 디바이스 정보를 이용하여 콘텐츠가 유통되는 진행 경로를 추적하는 것임을 특징으로 하는 해킹 콘텐츠 차단 방법.

청구항 12

제10항에 있어서, 상기 해킹 디바이스를 추출하는 과정은

상기 해킹 콘텐츠로부터 정해진 횟수 이상 검출된 디바이스 정보에 해당하는 디바이스를 해킹에 사용된 디바이스로 판단하고,

상기 디바이스를 철회하는 것임을 특징으로 하는 해킹 콘텐츠 차단 방법.

청구항 13

제12에 있어서, 상기 해킹 콘텐츠에 기록된 디바이스 정보로부터 마지막에 기록된 디바이스를 해킹에 사용된 디바이스로 판단하여 그 디바이스를 철회하는 것임을 특징으로 하는 해킹 콘텐츠 차단 방법.

청구항 14

제10에 있어서, 상기 워터마크 데이터는 전송 디바이스 정보 및 수신 디바이스 정보 및 콘텐츠 공유 순서 번호들 중 적어도 하나를 포함하는 것을 특징으로 하는 해킹 콘텐츠 차단 방법.

청구항 15

해킹 추적을 위한 워터 마킹 장치에 있어서,

콘텐츠 비트 스트림을 디코딩 하는 디코딩부;

수신 디바이스로부터 수신된 디바이스 정보와 자신의 디바이스 정보를 이용하여 워터마크 데이터를 생성하는 워터마크 생성부;

상기 워터마크 생성부에서 생성된 워터마크 데이터를 디코딩부에서 디코딩된 콘텐츠에 삽입하여 워터마킹 콘텐츠를 생성하는 워터마크 삽입부;

상기 워터마크 삽입부에서 생성된 워터마킹 콘텐츠를 인코딩 하여 워터마킹된 콘텐츠 비트 스트림으로 변환하는 인코딩부를 포함하는 해킹 추적을 위한 워터 마킹 장치.

청구항 16

제15항에 있어서, 정해진 네트워크로 연결된 수신 디바이스와 상기 디바이스 정보를 송수신하고 상기 인코딩 부에서 인코딩된 콘텐츠 비트 스트림을 상기 수신 디바이스로 전송하는 통신부를 더 포함하는 해킹 추적을 위한 워터 마킹 장치.

청구항 17

해킹 콘텐츠 차단 장치에 있어서,

서버에서 수집된 콘텐츠에 대해서 해킹 콘텐츠를 모니터링 하는 모니터링부;

상기 모니터링 부로부터 발견된 해킹 콘텐츠로부터 워터마크 데이터를 검출하는 워터마크 검출부;

상기 워터마크 검출 부에서 검출된 워터마크 데이터로부터 사용자 디바이스 정보를 추출하는 디바이스 정보 추출부;

상기 디바이스 정보 추출 부에서 추출된 디바이스 정보로부터 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회하는 해킹 콘텐츠 처리부를 포함하는 해킹 콘텐츠 차단 장치.

청구항 18

제 1항 내지 제 14항 중 어느 한 항의 방법을 구현하기 위한 프로그램이 기록된 컴퓨터로 읽을 수 있는 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명은 해킹 콘텐츠 추적 방법 및 장치에 관한 것이며, 특히 해킹 추적을 위한 워터 마킹 방법 및 장치 및 그를 이용한 해킹 콘텐츠 차단 방법에 관한 것이다.

배 경 기 술

[0002] 통신 속도의 비약적 발전과 대용량 저장 매체 및 다양한 휴대용 멀티미디어 재생 장치들의 확산에 따라 멀티미디어 콘텐츠의 수요는 날로 증가되고 있다.

[0003] 그에 따라 다양한 콘텐츠 제공자들이 등장하여 멀티미디어 콘텐츠를 다양한 방식으로 제공하고 있으나, 멀티미디어 콘텐츠는 특성상 원본과 동일한 사본이나 변형된 형태의 사본을 쉽게 만들어 낼 수 있을 뿐 만 아니라 다양한 경로를 통해 쉽게 배포될 수 있다. 이에 따라 인터넷을 통한 해킹 콘텐츠가 광범위한 범위로 유통되고 있다.

[0004] 따라서 멀티미디어 콘텐츠를 보호하기 위해 해킹에 의한 콘텐츠 유출을 근본적으로 차단하는 기술이 필요하다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 과제는 콘텐츠에 해킹 추적을 위한 워터 마크를 실시간으로 삽입함으로서 해킹 콘텐츠를 효율적으로 차단할 수 있는 해킹 추적을 위한 워터 마킹 방법 및 장치 및 그를 이용한 해킹 콘텐츠 차단 방법 및 장치를 제공하는 데 있다.

[0006] 상기의 과제를 해결하기 위하여, 본 발명의 일 실시 예에 따른 해킹 추적을 위한 워터 마킹 방법에 있어서,

[0007] 정해진 네트워크 채널을 통해 콘텐츠를 공유할 수신 디바이스와 디바이스 정보를 송수신하는 과정;

[0008] 상기 송수신된 송수신 디바이스 정보에 기반 한 워터마크 데이터를 생성하는 과정;

[0009] 상기 생성된 워터마크 데이터를 콘텐츠에 삽입하여 워터 마킹된 멀티미디어 콘텐츠를 생성하는 과정을 포함한다.

[0010] 바람직하게는 본 발명의 일 실시 예에 따른 해킹 추적을 위한 워터 마킹 방법은 상기 워터 마킹된 콘텐츠를 상기 수신 디바이스로 전송하는 과정을 더 포함한다.

[0011] 바람직하게는 상기 디바이스 정보는 송신 디바이스 ID 및 수신 디바이스 ID 를 포함한다.

[0012] 바람직하게는 상기 워터마크 데이터는 상기 송수신 디바이스 정보 및 콘텐츠 공유 순서 번호를 포함하는 것을 특징으로 한다.

[0013] 바람직하게는 상기 워터마크 데이터 생성 및 삽입은 정해진 보안 채널로 연결된 복수개 디바이스들 각각에 대해서 수행되는 것임을 특징으로 한다.

[0014] 바람직하게는 해킹 추적을 위한 워터 마킹 방법은 상기 송신 디바이스 정보 및 수신 디바이스 정보를 저장하는 룩-업 테이블을 구축하는 과정을 더 포함한다.

[0015] 바람직하게는 해킹 추적을 위한 워터 마킹 방법은 상기 디바이스 정보를 삽입할 수 있는 워터마크 도메인을 구성하는 과정을 더 포함한다.

[0016] 바람직하게는 워터 마킹된 멀티미디어 콘텐츠 생성 과정은,

[0017] 상기 멀티미디어 콘텐츠에 디바이스 관련 정보를 삽입할 수 있는 특정 위치를 정의하고,

[0018] 상기 정의된 멀티미디어 콘텐츠의 특정 위치에 워터마크 데이터를 삽입하는 것임을 특징으로 한다.

[0019] 바람직하게는 상기 수신 디바이스 관련 정보는 수신 디바이스로 재 전송 시 삭제되는 것임을 특징으로 한다.

[0020] 상기의 다른 과제를 해결하기 위하여, 본 발명의 일 실시 예에 따른 해킹 콘텐츠 차단 방법에 있어서,

[0021] 서버에서 수집되는 콘텐츠에 대해 해킹 여부를 모니터링 하는 과정;

[0022] 해킹 콘텐츠가 발견되면 상기 해킹 콘텐츠로부터 워터마크 데이터를 검출하는 과정;

[0023] 상기 검출된 워터마크 데이터로부터 송수신 디바이스 정보를 검출하는 과정;

[0024] 상기 송수신 디바이스 정보를 바탕으로 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회하는 과정을 포함한다.

[0025] 바람직하게는 상기 콘텐츠의 진행 경로 추출 과정은

[0026] 상기 디코딩된 디바이스 정보를 이용하여 콘텐츠가 유통되는 진행 경로를 추적하는 것임을 특징으로 한다.

[0027] 바람직하게는 상기 해킹 디바이스를 추출하는 과정은

[0028] 상기 해킹 콘텐츠로부터 통계적으로 정해진 횟수 이상 검출된 디바이스 ID에 해당하는 디바이스를 해킹에 사용된 디바이스로 판단하고,

[0029] 상기 디바이스를 철회하는 것임을 특징으로 한다.

[0030] 바람직하게는 상기 해킹 콘텐츠에 기록된 디바이스 정보로부터 마지막에 기록된 디바이스를 해킹에 사용된 디바이스로 판단하여 그 디바이스를 철회하는 것임을 특징으로 한다.

[0031] 바람직하게는 상기 워터마크 데이터는 전송 디바이스 정보 및 수신 디바이스 정보 및 콘텐츠 공유 순서 번호들 중 적어도 하나를 포함하는 것을 특징으로 한다.

[0032] 상기의 또 다른 과제를 해결하기 위하여, 본 발명의 일 실시 예에 따른 해킹 추적을 위한 워터 마킹 장치에 있어서,

[0033] 콘텐츠 비트 스트림을 디코딩하는 디코딩부;

[0034] 수신 디바이스로부터 수신된 디바이스 정보와 자신의 디바이스 정보를 이용하여 워터마크 데이터를 생성하는 워터마크 생성부;

[0035] 상기 워터마크 생성부에서 생성된 워터마크 데이터를 디코딩부에서 디코딩된 콘텐츠에 삽입하여 워터마킹 콘텐츠를 생성하는 워터마크 삽입부;

[0036] 상기 워터마크 삽입부에서 생성된 워터마킹 콘텐츠를 인코딩하여 워터마킹된 콘텐츠 비트 스트림으로 변환하는 인코딩부를 포함한다.

[0037] 바람직하게 본 발명의 일 실시 예에 따른 해킹 추적을 위한 워터 마킹 장치는 정해진 네트워크로 연결된 수신 디바이스와 상기 디바이스 정보를 송수신하고 상기 인코딩부에서 인코딩된 콘텐츠 비트 스트림을 상기 수신 디바이스로 전송하는 통신부를 더 포함한다.

[0038] 상기의 또 다른 과제를 해결하기 위하여, 본 발명의 일 실시 예에 따른 해킹 콘텐츠 차단 장치에 있어서,

[0039] 서버에서 수집된 콘텐츠에 대해서 해킹 콘텐츠를 모니터링하는 모니터링부;

[0040] 상기 모니터링부로부터 발견된 해킹 콘텐츠로부터 워터마크 데이터를 검출하는 워터마크 검출부;

[0041] 상기 워터마크 검출부에서 검출된 워터마크 데이터로부터 사용자 디바이스 정보를 추출하는 디바이스 정보 추출부;

[0042] 상기 디바이스 정보 추출부에서 추출된 디바이스 정보로부터 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회하는 해킹 콘텐츠 처리부를 포함한다.

도면의 간단한 설명

[0043] 도 1은 본 발명의 일 실시 예에 따른 해킹 추적을 위한 네트워크 시스템을 도시한 것이다.

도 2는 도 1의 클라이언트 네트워크 시스템을 도시한 것이다.

도 3은 본 발명의 일 실시 예에 따라 해킹 추적을 위한 워터 마킹 기술을 구현하는 사용자 디바이스의 상세 블록도 이다.

도 4는 본 발명의 일 실시 예에 따른 콘텐츠 프로바이더의 해킹 콘텐츠 차단장치의 상세 블록도 이다.

도 5는 도 2의 사용자 디바이스들에서 해킹 추적을 위한 워터 마킹 콘텐츠를 구현하기 위한 개념도 이다.

도 6은 본 발명의 일 실시 예에 따른 해킹 추적을 위한 워터 마킹 방법을 보이는 흐름도 이다.

도 7은 본 발명의 일 실시 예에 따른 해킹 콘텐츠 차단 방법을 보이는 전체 흐름도 이다.

도 8은 본 발명의 일 실시 예에 따른 해킹 콘텐츠 차단 방법을 보이는 상세 흐름도 이다.

발명을 실시하기 위한 구체적인 내용

[0044] 이하 첨부된 도면을 참조로하여 본 발명의 바람직한 실시예를 설명하기로 한다.

[0045] 도 1은 본 발명의 일 실시 예에 따른 해킹 추적을 위한 네트워크 시스템을 도시한 것이다.

[0046] 도 1의 네트워크 시스템은 콘텐츠 프로바이더(110), 클라이언트 네트워크(120), P2P 서버(130)로 구성된다.

[0047] 콘텐츠 프로바이더(110)는 자신이 관리하는 클라이언트 네트워크(120)내 사용자 디바이스들에게 콘텐츠를 공급하고, P2P 서버(130)에서 수집된 콘텐츠에 대해 해킹 콘텐츠 여부를 모니터링하고, 해킹 발생 시 해킹 콘텐츠에 삽입된 워터마크로부터 디바이스 관련 정보를 검출하고, 그 디바이스 관련 정보로부터 콘텐츠의 진행 경로를 추출하고 해킹 된 사용자 디바이스를 철회한다.

[0048] 클라이언트 네트워크(120)는 복수개의 사용자 디바이스들(사용자 디바이스1, 2, 3)을 포함한다. 각 사용자 디바이스들은 서로 정해진 네트워크 채널로 콘텐츠및 디바이스 정보를 주고받으며, 콘텐츠 프로바이더(110)로부터 수신된 콘텐츠에 송수신 디바이스 정보에 해당하는 워터마크를 삽입한다. 또한 각 사용자 디바이스들은 P2P 서버(130)로 콘텐츠를 업-로드한다.

[0049] P2P 서버(130)는 클라이언트 네트워크(120)내 복수개 사용자 디바이스 들로부터 콘텐츠를 수집한다.

[0050] 도 2는 도 1의 클라이언트 네트워크 시스템을 도시한 것이다.

[0051] 클라이언트 네트워크 시스템은 복수개의 사용자 디바이스들(210, 220, 230, 240, 250, 260)을 구비하며, 각 사용자 디바이스들은 정해진 쌍방향 보안 채널(secured channel)로 연결되어 서로 콘텐츠 및 디바이스 정보를 공유한다. 또한 각 사용자 디바이스들은 디바이스 ID를 구비한다.

[0052] 일 예로, 사용자 디바이스 1(210)은 "A1"의 디바이스 ID를 구비하고, 사용자 디바이스 2(220)는 "B1"의 디바이스 ID를 구비하고, 사용자 디바이스 3(230)은 "B2"의 디바이스 ID를 구비하고, 사용자 디바이스 4(240)는 "C1"의 디바이스 ID를 구비하고, 사용자 디바이스 5(250)는 "C2"의 디바이스 ID를 구비하고, 사용자 디바이스 6(260)은 "A2"의 디바이스 ID를 구비한다.

[0053] 또한 각 사용자 디바이스는 콘텐츠를 공유할 상대방 사용자 디바이스와 각 디바이스 정보를 송수신하고, 콘텐츠 공유 순서를 전송한다.

[0054] 각 사용자 디바이스들은 콘텐츠에 송수신 디바이스 정보(또는 DRM 키 정보)에 해당하는 워터마크를 삽입하고 그 워터마킹 된 콘텐츠를 인코딩 한다. 이때 각 사용자 디바이스 마다 디바이스 정보를 삽입할 수 있는 워터마크 도메인을 구성하고 콘텐츠내에 디바이스 정보를 삽입하기 위한 위치를 정의한다.

[0055] 예를 들면, 사용자 디바이스 1(210)은 쌍 방향 채널을 통해 사용자 디바이스 2(220)로부터 디바이스 ID(B1)를 수신하고 자신의 디바이스 ID(A1)을 사용자 디바이스 2(220)로 전송한다. 이어서, 사용자 디바이스 1, 2(210, 220)는 자신의 디바이스 ID와 상대방 디바이스 ID, 콘텐츠 공유 순서 번호들중 적어도 하나를 바탕으로 워터마크 데이터를 생성하고 그 워터마크 데이터를 공유할 콘텐츠에 삽입한다.

[0056] 결국, 각 사용자 디바이스들은 전송 및 수신 디바이스 정보에 해당하는 워터마크 정보를 콘텐츠에 삽입함으로써 해킹 발생 시 콘텐츠 프로바이더(110)에 의해 해킹에 사용된 디바이스로써 검출될 수 있다.

[0057] 도 3은 본 발명의 일 실시 예에 따라 해킹 추적을 위한 워터 마킹 기술을 구현하는 사용자 디바이스의 상세 블록도 이다.

[0058] 도 3의 사용자 디바이스는 콘텐츠 데이터 베이스(310), 디코딩부(320), 워터마크 생성부(330), 워터마크 삽입부(340), 인코딩부(350), 워터마크 콘텐츠 저장부(360), 통신부(370)를 구비한다.

[0059] 콘텐츠 데이터 베이스(310)는 콘텐츠 프로바이더(110)로부터 수신되는 콘텐츠 비트 스트림을 저장한다. 여기서, 콘텐츠 데이터 베이스(310)는, 예를 들면 하드 디스크 등의 자기 기록매체나 EEPROM, 플래시 메모리 등의 불 휘발성 메모리를 들 수 있지만, 상기에 한정되지는 않는다.

[0060] 디코딩부(320)는 콘텐츠 데이터 베이스(310)에 저장된 콘텐츠 비트 스트림을 디코딩 한다.

[0061] 워터마크 생성부(330)는 통신부(370)로부터 정해진 네트워크 채널을 통해 콘텐츠를 공유할 수신 디바이스로부터 디바이스 정보를 수신하고, 그 수신된 디바이스 정보와 자신의 디바이스 정보를 이용하여 워터마크 데이터를 생성한다.

[0062] 일 실시 예로, 워터마크 생성부(330)는 워터마크 패턴을 결정하고, 그 워터마크 패턴을 영상 데이터 형식으로 변환하여 워터마크 데이터를 생성한다. 이때 워터마크 패턴은 원본 영상 또는 원본 영상의 재생과 관련된 정보에 기초하여 결정된다. 예를 들어, 워터마크 패턴은 전송 디바이스 정보와 수신 디바이스 정보를 나타낼 수 있다. 워터마크 패턴은 난수열의 형태로 생성될 수 있다.

[0063] 워터마크 삽입부(340)는 워터마크 생성부(330)에서 생성된 워터마크 데이터를 디코딩부(320)에서 디코딩 된 콘텐츠 데이터에 실시간으로 삽입하여 워터마킹 콘텐츠를 생성한다. 일 실시 예로 블록 단위의 픽셀들에 공간 도메인에 기반한 워터마킹 기술을 이용하여 워터마크가 삽입된다. 통상적으로 워터마크의 유형은 외부적인 공격 또는 변형에 견디는 정도에 따라 강인한 워터마크(Robust Watermark), 세미 워터마크(Semi Watermark), 연약한 워터마크(Fragile Watermark)로 구분될 수 있다.

[0064] 인코딩부(350)는 워터마킹 된 콘텐츠를 인코딩 하여 워터마킹된 콘텐츠 비트 스트림으로 변환한다.

[0065] 워터마킹 콘텐츠 저장부(360)는 인코딩부(350)에 의해 인코딩된 콘텐츠 비트 스트림을 저장한다. 여기서, 워터마킹 콘텐츠 저장부(360)는, 예를 들면 하드 디스크 등의 자기 기록매체나 EEPROM, 플래시 메모리 등의 불휘발성 메모리를 들 수 있지만, 상기에 한정되지는 않는다.

[0066] 통신부(370)는 콘텐츠 공유를 위해 보안 네트워크(380)로 연결된 수신 사용자 디바이스로 콘텐츠 비트 스트림을 전송하고, 수신 사용자 디바이스로 자신의 디바이스 정보를 송신하고, 수신 사용자 디바이스로부터 수신 디바이스 정보를 수신하여 워터마크 생성부(330)로 입력시킨다.

[0067] 따라서, 본 발명의 일 실시 예에 따르면 사용자 디바이스는 해킹 추적용 워터마크 정보를 콘텐츠에 실시간으로 삽입할 수 있다.

[0068] 도 4는 본 발명의 일 실시 예에 따른 콘텐츠 프로바이더의 해킹 콘텐츠 차단장치의 상세 블록도 이다.

[0069] 도 4의 콘텐츠 프로바이더는 모니터링부(410), 디코딩부(420), 워터마크 검출부(430), 디바이스 정보 추출부(440), 해킹 콘텐츠 처리부(450)를 구비한다.

[0070] 모니터링부(410)는 서버로부터 수집된 멀티미디어 콘텐츠 비트 스트림에 대해 해킹된 콘텐츠 여부를 모니터링 한다.

[0071] 디코딩부(420)는 모니터링부(410)로부터 발견된 해킹 콘텐츠 비트 스트림을 디코딩 한다.

[0072] 워터마크 검출부(430)는 디코딩부(420)에서 디코딩된 콘텐츠로부터 워터마크 데이터를 검출한다.

[0073] 디바이스 정보 추출부(440)는 워터마크 검출부(430)에서 검출된 워터마크 데이터로부터 디바이스 정보를 추출한다. 이때 디바이스 정보는 송신 디바이스 ID, 수신 디바이스 ID, 콘텐츠 공유 순서를 포함한다.

[0074] 해킹 콘텐츠 처리부(450)는 추출된 디바이스 정보로부터 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회한다.

[0075] 도 5는 도 2의 사용자 디바이스들에서 해킹 추적을 위한 워터 마킹 워터 콘텐츠를 구현하기 위한 개념도 이다.

[0076] 제1사용자 디바이스(510), 제2사용자 디바이스(520), 제3사용자 디바이스(530)는 정해진 쌍 방향 채널을 통해 서로 콘텐츠 및 디바이스 정보를 공유한다. 이때 제1사용자 디바이스(510) "B1"의 디바이스 ID를 갖고 있으며, 제2사용자 디바이스(520)는 "C1"의 디바이스 ID를 갖으며, 제3사용자 디바이스(530)는 "B2"의 디바이스 ID를 갖는다.

[0077] 먼저, 제1사용자 디바이스(510)는 콘텐츠 공유 순서(1), 송신 디바이스 정보("B1"), 수신 디바이스 정보(C1)에 기반 한 워터마크 데이터를 생성하고, 그 워터마크 데이터를 콘텐츠(512)에 삽입하고, 그리고 워터마킹 된 콘텐츠를 제2사용자 디바이스(520)로 전송한다.

[0078] 이어서, 제2사용자 디바이스(520)는 제1사용자 디바이스(510)로부터 콘텐츠를 수신하고, 콘텐츠 공유 순서(2), 송신 디바이스 정보(C1), 수신 디바이스 정보(B2)에 기반 한 워터마크 데이터를 생성하고, 그 워터마크 데이터를 제1사용자 디바이스(510)로부터 수신된 콘텐츠(522)에 삽입한다. 그리고 워터마킹된 콘텐츠를 제3사용자 디바이스(520)로 전송한다. 여기서 제1사용자 디바이스(510)와 공유된 콘텐츠에 송신 디바이스 정보(C1)가 이미 기록되어 있으므로 송신 디바이스 정보(C1)는 생략 가능하다.

[0079] 이어서, 제3사용자 디바이스(530)는 제2사용자 디바이스(520)로부터 콘텐츠를 수신하고, 콘텐츠 공유 순서(3) 및 송신 디바이스 정보(B2)에 기반 한 워터마크 데이터를 생성하고, 그 워터마크 데이터를 제2사용자 디바이스(520)로부터 수신된 콘텐츠(532)에 삽입한다. 콘텐츠(532)에는 제1사용자 디바이스(510) 및 제2사용자 디바이스(520)의 디바이스 정보들(B1, C1, B2)이 콘텐츠 공유 순서대로 기록되어 있다.

[0080] 다른 실시 예로, 수신 디바이스로 수신 디바이스 정보를 콘텐츠를 재 전송 시 수신 디바이스 정보를 삭제할 수 있다.

[0081] 이때, 제3사용자 디바이스(530)의 콘텐츠가 해킹 되었다고 가정하자.

[0082] 그러면 해킹 된 콘텐츠(532)에 마지막으로 기록된 송신 디바이스 정보(B2)로부터 제3사용자 디바이스(530)가 해킹에 사용된 디바이스임을 알 수 있다.

[0083] 따라서, 본 발명의 일 실시 예에 따르면 각 사용자 디바이스들에서 송신 및 수신 관련 워터마크 정보를 콘텐츠에 삽입함으로써 특정 사용자 디바이스에서 정보 유출시 해당 사용자 디바이스를 철회(revocation)시킬 수 있다.

[0084] 도 6은 본 발명의 일 실시 예에 따라 사용자 디바이스에서 해킹 추적을 위한 워터 마킹 방법을 보이는 흐름도 이다.

[0085] 먼저, 보안 네트워크 채널을 통해 콘텐츠를 공유할 수신 디바이스와 디바이스 관련 정보를 송수신한다(610 과정). 일 실시 예로 디바이스 관련 정보는 송신 디바이스 ID, 수신 디바이스 ID를 포함할 수 있으나, 이에 한정하지 않는다.

[0086] 이어서, 송신 디바이스 관련 정보 및 수신 디바이스 관련 정보를 저장하는 룩-업 테이블을 구축한다(620 과정).

[0087] 이어서, 수신 디바이스 관련 정보와 수신 디바이스 관련 정보에 기반한 워터마크 데이터를 생성한다(630 과정). 일 실시 예로, 디바이스 관련 정보를 삽입할 수 있는 워터마크 도메인이 구성된다. 워터마크 도메인은 공간 분리(spatial separation), 시간 분리(time separation), 주파수 분리(frequency separation)등을 이용한다. 또한 워터마크 구성 정보는 송신 디바이스 정보, 수신 디바이스 정보에 콘텐츠 공유 순서 번호들중 적어도 하나를 포함한다.

[0088] 이어서, 콘텐츠 프로바이더에서 제공되는 콘텐츠 비트 스트림을 디코딩 한다(640 과정).

[0089] 이어서, 디코딩된 콘텐츠에 워터마크 데이터를 삽입하여 워터 마킹된 콘텐츠를 생성한다(650 과정). 일 실시 예로, 콘텐츠내에 디바이스 관련 정보를 삽입할 수 있는 특정 위치를 정의하고, 정의된 콘텐츠의 특정 위치에 워터마크 데이터를 삽입한다.

[0090] 이어서, 워터 마킹된 콘텐츠를 인코딩하여 워터마킹 된 콘텐츠 비트 스트림으로 변환한다(660 과정).

[0091] 따라서, 본 발명의 일 실시 예에 따르면 콘텐츠에 해킹 추적을 위한 워터 마크를 실시간으로 삽입함으로서 해킹 콘텐츠를 효율적으로 차단할 수 있다.

[0092] 도 7은 본 발명의 일 실시 예에 따른 해킹 콘텐츠 차단 방법을 보이는 전체 흐름도이다.

[0093] 먼저, 서버에서 수집되는 콘텐츠에 대해 해킹 여부를 모니터링 한다(710 과정).

[0094] 이때, 해킹 콘텐츠가 발견되면 그 해킹 콘텐츠로부터 워터마크 데이터를 검출한다(720 과정).

[0095] 이어서, 검출된 워터마크 데이터로부터 송수신 디바이스 정보를 검출한다(730 과정).

[0096] 이어서, 송수신 디바이스 정보를 이용하여 콘텐츠의 진행 경로를 추출하고 해킹 디바이스를 철회한다(740 과정).

[0097] 도 8은 본 발명의 일 실시 예에 따른 해킹 콘텐츠 차단 방법을 보이는 상세 흐름도이다.

[0098] 먼저, 서버에서 수집되는 멀티미디어 콘텐츠들에 대해 해킹 콘텐츠 여부를 모니터링 한다(810 과정).

[0099] 이어서, 해킹 콘텐츠가 발견되었는가를 체크한다(820 과정).

[0100] 이어서, 해킹 콘텐츠가 발견되면 해킹 콘텐츠로부터 해킹 추적을 위한 복수개의 워터마크 데이터를 검출한다(830 과정).

[0101] 이어서, 워터마크 데이터로부터 송수신 디바이스 정보를 추출한다(840 과정). 일 실시 예로 송수신 디바이스 정보는 송신 디바이스 ID, 수신 디바이스 ID, 콘텐츠 공유 순서 번호들중 적어도 하나를 포함한다.

[0102] 이어서, 서버에 등록된 사용자 디바이스 리스트와 추출된 송수신 디바이스 정보를 비교한다(850 과정). 예를 들면 서버에 등록된 사용자 디바이스 ID 리스트와 추출된 사용자 디바이스 ID를 비교한다.

[0103] 이어서, 사용자 디바이스 리스트와 추출된 송수신 디바이스 정보간의 비교 결과에 따라 해킹 디바이스인가를 체크한다(860 과정). 즉, 추출된 사용자 디바이스 ID가 서버에 등록된 사용자 ID와 일치하면 그 추출된 사용자 디바이스 ID에 해당하는 사용자 디바이스를 해킹 디바이스로 결정한다.

[0104] 이어서, 서버에 등록된 사용자 디바이스 리스트로부터 해킹 디바이스를 철회하고 그 디바이스 정보를 이용하여 콘텐츠가 유통되는 진행 경로를 추출한다(870 과정).

[0105] 디바이스 철회 과정의 일 실시예로, 해킹 콘텐츠로부터 통계적으로 정해진 횟수 이상 검출된 사용자 디바이스 ID를 해킹에 사용된 사용자 디바이스로 판단하고, 그 사용자 디바이스를 철회한다.

[0106] 디바이스 철회 과정의 다른 실 시 예로, 해킹 콘텐츠에 기록된 디바이스 정보로부터 마지막에 기록된 사용자 디바이스를 철회한다.

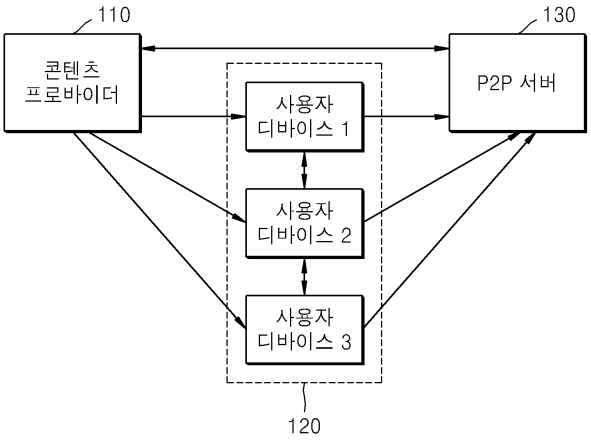
[0107] 결국, 콘텐츠에 삽입된 해킹 추적용 워터 마크에 의해 해킹 콘텐츠가 효율적으로 차단된다.

[0108] 또한 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

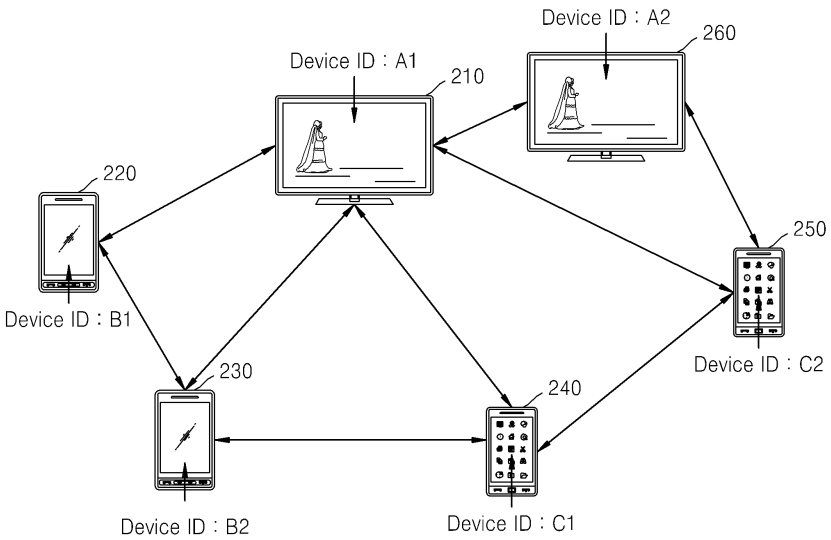
[0109] 이상의 설명은 본 발명의 일 실시예에 불과할 뿐, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명의 본질적 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현할 수 있을 것이다. 따라서, 본 발명의 범위는 전술한 실시예에 한정되지 않고 특허 청구 범위에 기재된 내용과 동등한 범위내에 있는 다양한 실시 형태가 포함되도록 해석되어야 할 것이다.

도면

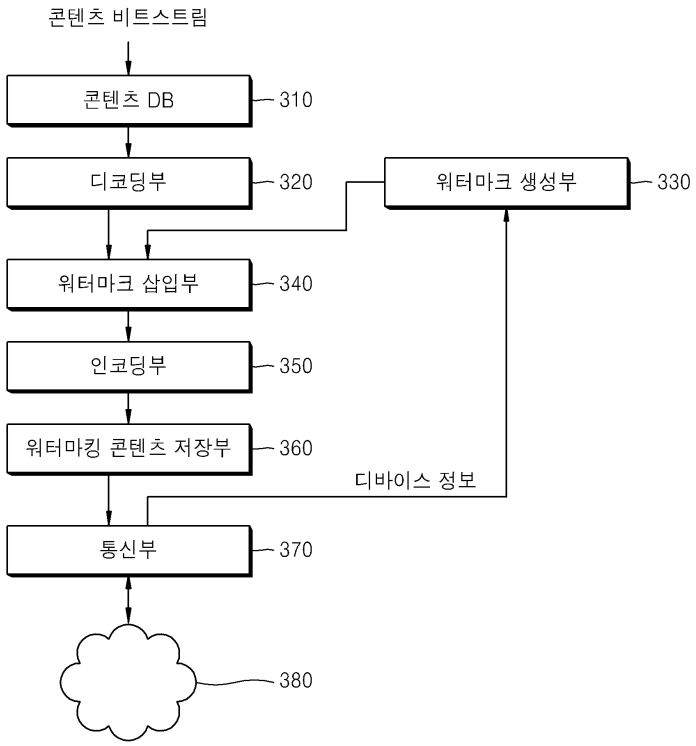
도면1


110
콘텐츠
프로바이더
130
P2P 서버
사용자
디바이스 1
사용자
디바이스 2
사용자
디바이스 3
120

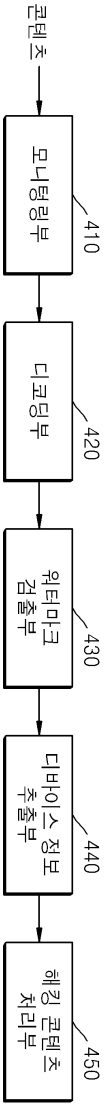
도면2


Device ID : A2
260
Device ID : A1
210
220
250
Device ID : B1
Device ID : C2
230
240
Device ID : B2
Device ID : C1

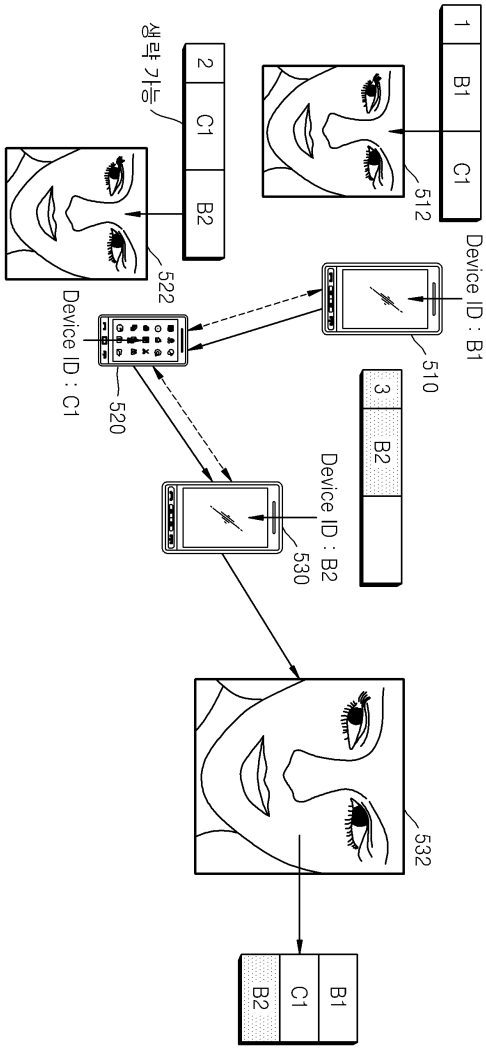
도면3


콘텐츠 비트스트림
콘텐츠 DB
310
디코딩부
320
워터마크 생성부
330
워터마크 삽입부
340
인코딩부
350
워터마킹 콘텐츠 저장부
360
디바이스 정보
통신부
370
380

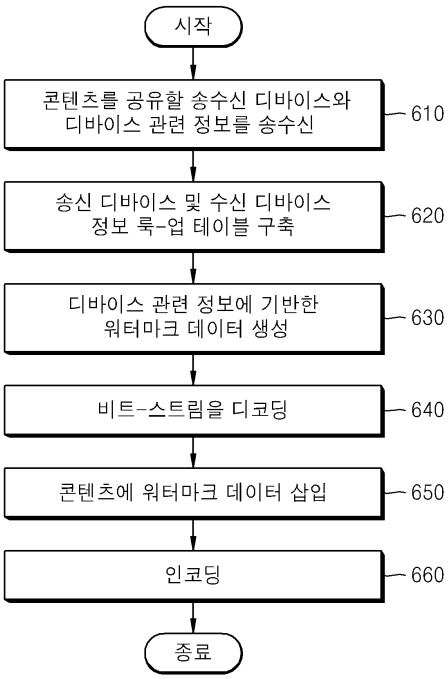
도면4


콘텐츠
모니터링부
410
디코딩부
420
워터마크 검출부
430
디바이스 정보 추출부
440
헤킹 콘텐츠 처리부
450

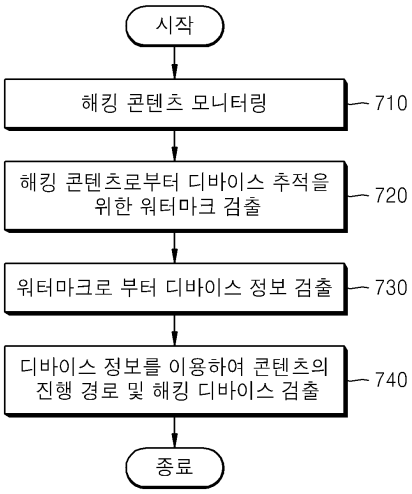
도면5


1
B1
C1
512
Device ID : B1
510
생략 기능
2
C1
B2
522
Device ID : C1
520
3
B2
Device ID : B2
530
532
B1
C1
B2

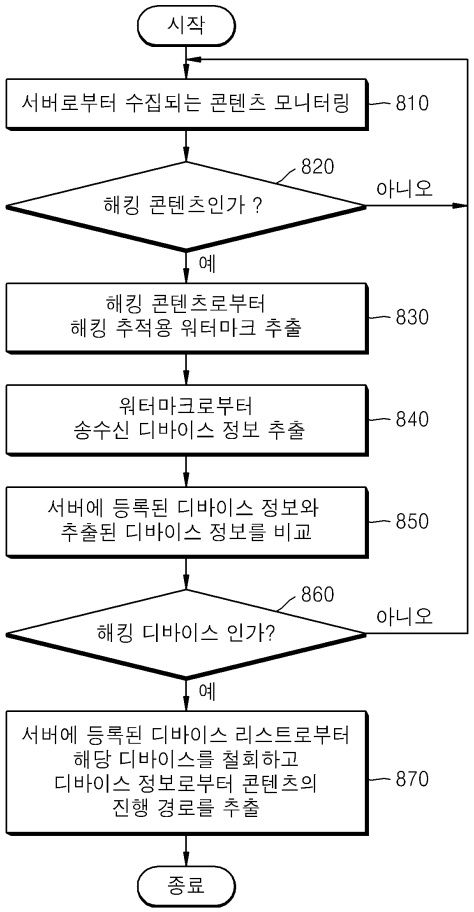
도면6


시작
콘텐츠를 공유할 송수신 디바이스와 디바이스 관련 정보를 송수신
610
송신 디바이스 및 수신 디바이스 정보 룩-업 테이블 구축
620
디바이스 관련 정보에 기반한 워터마크 데이터 생성
630
비트-스트림을 디코딩
640
콘텐츠에 워터마크 데이터 삽입
650
인코딩
660
종료

도면7


시작
해킹 콘텐츠 모니터링
710
해킹 콘텐츠로부터 디바이스 추적을 위한 워터마크 검출
720
워터마크로 부터 디바이스 정보 검출
730
디바이스 정보를 이용하여 콘텐츠의 진행 경로 및 해킹 디바이스 검출
740
종료

도면8


시작
서버로부터 수집되는 콘텐츠 모니터링
810
820
해킹 콘텐츠인가 ?
아니오
예
해킹 콘텐츠로부터
해킹 추적용 워터마크 추출
830
워터마크로부터
송수신 디바이스 정보 추출
840
서버에 등록된 디바이스 정보와
추출된 디바이스 정보를 비교
850
860
해킹 디바이스 인가?
아니오
예
서버에 등록된 디바이스 리스트로부터
해당 디바이스를 철회하고
디바이스 정보로부터 콘텐츠의
진행 경로를 추출
870
종료