(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년03월11일
(11) 등록번호 10-1602735
(24) 등록일자 2016년03월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/10 (2013.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2014-0195339
(22) 출원일자 2014년12월31일
심사청구일자 2014년12월31일
(56) 선행기술조사문헌
KR1020090017055 A
KR1020020096690 A

(73) 특허권자
한국기술교육대학교 산학협력단
충남 천안시 동남구 병천면 충절로 1600, 내 (한국기술교육대학교)
(72) 발명자
서희석
충청남도 천안시 동남구 병천면 충절로 1600 한국기술교육대학교
최요한
충청남도 천안시 동남구 병천면 충절로 1638, 105동 601호(신한아파트)
김민호
충청남도 천안시 서북구 오성9길 24, 1동 402호(두정동, G.N.Bill)
(74) 대리인
김정수

전체 청구항 수 : 총 1 항 심사관 : 박진아

(54) 발명의 명칭 **멀티미디어 콘텐츠 인증 시스템 및 방법**

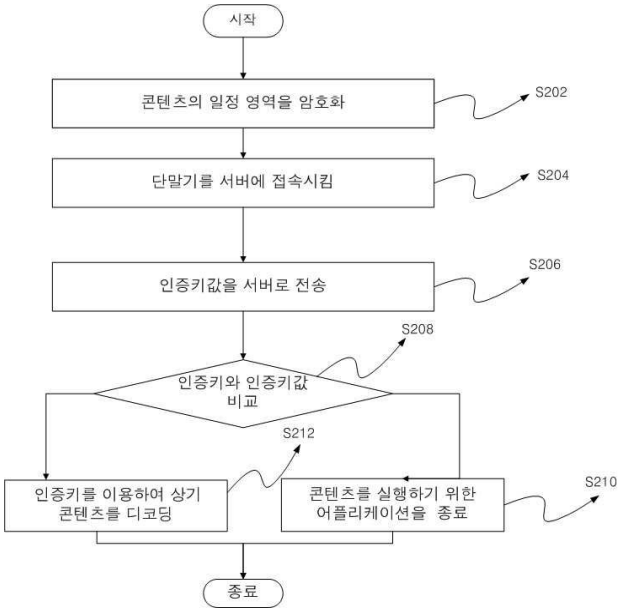
(57) 요 약

본 발명은 콘텐츠를 사용 시, 해당 콘텐츠들을 암호화하여 제공하므로 콘텐츠들의 불법 유통을 방지할 수 있는 하는 멀티미디어 콘텐츠 인증 방법에 관한 것으로서,

본 발명은 콘텐츠의 일정 영역을 선정하여 상기 선정된 콘텐츠의 일정 영역을 암호화하여 인증키를 생성하는 과

(뒷면에 계속)

대 표 도 - 도2



정; 상기 콘텐츠를 실행하기 위한 단말기를 통해 어플리케이션을 실행하고 단말기를 서버에 접속시키는 과정; 상기 단말기를 통해 실행되는 콘텐츠에 대한 인증키 값을 서버로 전송하는 과정; 상기 서버에 등록된 인증키와 상기 단말기를 통해 전송된 인증키값을 비교하는 과정; 및 상기 비교하는 과정에서의 비교 결과 상기 서버에 등록된 인증키와 상기 단말기를 통해 전송된 인증키값이 일치하는 경우 상기 어플리케이션을 이용하여 상기 콘텐츠를 실행하는 과정을 포함하여 구성되어, 콘텐츠 자료를 사용시에 해당 콘텐츠들을 암호화하여 제공하므로 콘텐츠들의 불법 유통을 방지할 수 있는 효과가 있다.

명 세 서

청구범위

청구항 1

멀티미디어 콘텐츠의 불법적인 사용 및 유출을 방지할 수 있도록 구성되는 멀티미디어 콘텐츠 인증 시스템에 있어서,

무선 또는 유선 네트워크를 통하여 외부와 통신을 수행하는 서버통신부와,

제작된 멀티미디어 콘텐츠 패키지 파일을 저장하는 데이터베이스와,

상기 데이터베이스에 저장된 콘텐츠를 미리 정해진 일정 비트 단위의 코드 단위로 구분하고, 상기 콘텐츠의 구분된 영역 중 어느 하나를 선택하여 샘플링하고 상기 샘플링된 영역을 암호화하는 것에 의해 상기 콘텐츠의 일정 영역의 콘텐츠 소스를 인증키로 선정하여 선정된 상기 콘텐츠의 일정 영역을 암호화하며, 암호화된 상기 콘텐츠에 대한 버전정보, 콘텐츠 길이정보, 콘텐츠 타입정보, 암호화 시작위치 정보와 암호화 종료위치 정보를 포함하는 암호화된 상기 콘텐츠의 헤더정보를 상기 데이터베이스에 등록하는 암호화부 및

상기 데이터베이스, 상기 암호화부 및 상기 서버통신부의 전체적인 동작을 각각 제어하는 서버제어부를 포함하여, 상기 멀티미디어 콘텐츠의 인증을 수행하는 서버; 및

무선 또는 유선 네트워크를 통하여 상기 서버로부터 수신된 인증 결과에 따라 상기 콘텐츠를 실행하기 위한 동작이 제어되도록 구성되는 어플리케이션을 포함하여 이루어지는 단말기를 포함하여 구성되고,

상기 서버는,

상기 단말기에서 상기 어플리케이션을 실행하여 상기 콘텐츠를 실행하고자 하는 요청이 수신되면, 상기 콘텐츠의 헤더정보에 포함된 상기 서버의 URL을 이용하여 상기 단말기를 상기 서버에 자동으로 접속시키고 해당 콘텐츠에 대한 인증키값을 전송하도록 제어하며,

상기 단말기로부터 인증키값이 수신되면, 상기 인증키값에 해당하는 콘텐츠 정보가 상기 데이터베이스에 존재하는지의 여부를 판단하여, 해당 콘텐츠가 상기 데이터베이스에 존재하는 경우는 상기 데이터베이스에 등록된 인증키와 상기 단말기로부터 전송된 인증키값이 일치하는지의 여부를 비교하고,

상기 데이터베이스에 등록된 인증키와 상기 단말기를 통해 전송된 인증키값이 일치하는 경우는, 상기 단말기 또는 상기 서버의 상기 인증키값 또는 상기 인증키를 이용하여 상기 콘텐츠를 디코딩하고 상기 어플리케이션을 통하여 해당 콘텐츠를 실행할 수 있도록 제어하며,

상기 데이터베이스에 등록된 인증키와 상기 단말기를 통해 전송된 인증키값이 일치하지 않는 경우는, 상기 콘텐츠를 실행하기 위한 어플리케이션을 강제종료시키도록 제어하는 처리가 수행되도록 구성되는 것을 특징으로 하는 멀티미디어 콘텐츠 인증 시스템.

청구항 2

삭제

청구항 3

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 멀티미디어 콘텐츠 인증 방법에 관한 것으로, 보다 상세하게는, 콘텐츠를 사용시 해당 콘텐츠들을 암호화하여 제공함으로써 콘텐츠들의 불법 유통을 방지할 수 있도록 구성되는 멀티미디어 콘텐츠 인증 시스템 및

방법에 관한 것이다.

배 경 기 술

[0002] 앱 스토어에서 제공되는 디지털 권리 관리(Digital rights management, DRM)에 대한 암호화가 풀릴 경우 단말에 저장된 콘텐츠의 유출로 인해 콘텐츠가 p2p(peer to peer)등을 통한 불법 유출이 발생한다. 따라서, 단말에 저장된 콘텐츠의 불법 유출을 방지하기 위한 인증 방법이 필요하다.

[0003] 이와 같은 문제점을 해결하기 위하여 대한민국 등록특허 제10-1439757로 등록된 "서버와 연동하여 불법 복제된 모바일 앱의 실행을 차단할 수 있는 단말장치, 및 상기 단말장치에서의 모바일 앱 실행 제어 방법"(인용발명)에서는 서버와 연동하여 불법 복제된 모바일 앱의 실행을 차단할 수 있는 단말장치, 및 상기 단말장치에서의 모바일 앱(어플리케이션) 실행 제어 방법이 개시된다. 개시된 단말장치는 정상 구매된 모바일 앱과 대응되는 제1 저작권 정보 및 불법 복 제된 모바일 앱과 대응되는 제2 저작권 정보 중 어느 하나인 저작권 정보가 삽입된 모바일 앱의 실행을 제어하는 제어부; 및 상기 제어부에 의해 제어되며, 상기 서버와 통신을 수행하는 통신부;를 포함하되, 상기 제어부는, 상기 모바일 앱의 실행요청이 발생한 시점에서 상기 단말장치가 기준위치로부터 기 설정된 거리 이상 떨어진 지점에 위치하는 경우, 상기 통신부가 상기 삽입된 저작권 정보를 상기 서버로 전송하고 상기 삽입된 저작권 정보의 전송에 대응하여 상기 서버로부터 상기 모바일 앱의 실행제어 메시지를 수신하도록 제어하며, 상기 수신된 실행제어 메시지에 기초하여 상기 모바일 앱의 실행을 제어하고, 상기 단말장치가 기준위치로부터 기 설정된 거리 이상 떨어져 있지 않는 경우, 상기 제어부는, 상기 통신부가 상기 삽입된 저작권 정보를 상기 서버로 전송하지 않도록 제어하는 것을 특징으로 하는 단말장치에 대하여 개시하고 있다.

[0004] 전술한 인용발명은 앱의 실행을 차단하기 위한 구성으로 해당 모바일 앱이 단말장치 내에 설치된 시점에서의 위치 등과 같은 위치를 판단하여 설정된 지역 이외의 지역인 것으로 판단되면 앱의 저작권 정보를 판단하여 정상적인 사용자인지의 여부를 판단하는 구성이다. 그러나 인용발명의 경우 어플리케이션(앱)에 저작권 정보를 판단하므로 어플리케이션에 의해 제공되는 콘텐츠에 대해서는 별도의 판단을 하지 않으므로 불법사용 콘텐츠에 대해서는 규제할 방법이 없는 문제점이 있다. 또한 어플리케이션이 실행된 위치와 설정된 위치의 범위를 판단하고 이와 같은 범위를 벗어난 경우에만 불법복재인지의 여부를 판단하므로 생활패턴이 비슷한 범주 내에서 사용하는 불법 사용자의 불법 사용에 대해서는 검출해 낼 수 없는 문제점이 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 등록특허 제10-1439757호 (발명의 명칭: 서버와 연동하여 불법 복제된 모바일 앱의 실행을 차단할 수 있는 단말장치, 및 상기 단말장치에서의 모바일 앱 실행 제어 방법)

발명의 내용

해결하려는 과제

[0006] 따라서 본 발명은 전술한 종래기술의 문제점을 해결하기 위한 것으로서, 콘텐츠, 예컨대, 만화, 음악, 서적, 지도, 네비게이션 정보, 영화, 동영상, 그림, 클립아트, 사진 등의 자료를 사용시에 해당 콘텐츠들을 암호화하여 제공하므로 콘텐츠들의 불법 유통을 방지하는 멀티미디어 콘텐츠 인증 방법을 제공하는 것을 목적으로 한다.

[0007] 또한, 본 발명은 서버에서 인증절차를 진행하므로 콘텐츠의 불법적인 사용을 원천적으로 차단할 수 있는 멀티미디어 콘텐츠 인증 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0008] 상기 과제를 해결하기 위한 본 발명의 실시 예에 따른 멀티미디어 콘텐츠 인증 방법은, 콘텐츠의 일정 영역을 선정하여 상기 선정된 콘텐츠의 일정 영역을 암호화하여 인증키를 생성하는 과정; 상기 콘텐츠를 실행하기 위한 단말기를 통해 어플리케이션을 실행하고 단말기를 서버에 접속시키는 과정; 상기 단말기를 통해 실행되는 콘텐츠에 대한 인증키 값을 서버로 전송하는 과정; 상기 서버에 등록된 인증키와 상기 단말기를 통해 전송된 인증키 값을 비교하는 과정; 및 상기 비교하는 과정에서의 비교 결과 상기 서버에 등록된 인증키와 상기 단말기를 통해 전송된 인증키값이 일치하는 경우 상기 어플리케이션을 이용하여 상기 콘텐츠를 실행하는 과정을 포함한다.

[0009] 상기 일정 영역을 암호화하는 과정은, 제작된 콘텐츠 패키지 파일을 수신하여 등록하는 과정; 상기 콘텐츠 중 상기 일정 영역의 콘텐츠 소스를 인증키로 선정하는 과정; 및 상기 선정된 인증키값을 이용하여 상기 콘텐츠를 암호화하는 과정을 포함하는 것이다.

[0010] 상기 비교하는 과정에서의 비교 결과 상기 서버에 등록된 인증키와 상기 단말기를 통해 전송된 인증키값이 일치하지 않는 경우 상기 콘텐츠를 실행하기 위한 어플리케이션을 종료시키는 과정을 더 포함하는 것이다.

발명의 효과

[0011] 본 발명에 따른 멀티미디어 콘텐츠 인증 방법은 콘텐츠, 예컨대, 만화, 음악, 서적, 지도, 네비게이션 정보, 영화, 동영상, 그림, 클립아트, 사진 등의 자료를 사용시에 해당 콘텐츠들을 암호화하여 제공하므로 콘텐츠들의 불법 유통을 방지할 수 있는 효과가 있다.

[0012] 또한, 본 발명에 따른 멀티미디어 콘텐츠 인증 방법은 서버에서 인증절차를 진행하므로 콘텐츠의 불법적인 사용을 원천적으로 차단할 수 있는 효과가 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 실시 예에 따른 멀티미디어 콘텐츠 인증하기 위한 시스템 구성을 나타낸 블록 구성도.

도 2는 본 발명의 일 실시예에 따른 멀티미디어 콘텐츠 인증하기 위한 인증 과정을 나타낸 순서도.

도 3은 본 발명의 일 실시예에 따른 도 2에 따라 콘텐츠를 암호하하는 과정을 나타낸 순서도.

도 4는 본 발명의 일 실시예에 따른 멀티미디어 콘텐츠의 데이터 구조를 나타낸 블록 데이터 포맷을 나타낸 도면.

발명을 실시하기 위한 구체적인 내용

[0014] 이하, 본 발명의 바람직한 실시 예의 상세한 설명은 첨부된 도면들을 참조하여 설명할 것이다. 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

[0015] 본 발명의 개념에 따른 실시 예는 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있으므로 특정 실시 예들을 도면에 예시하고 본 명세서 또는 출원에 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예를 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0016] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에

직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0017] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 설시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0018] 이하 도면을 참조하여, 본 발명의 실시 예에 따른 멀티미디어 콘텐츠 인증 시스템을 보다 상세하게 설명하도록 한다. 도 1은 본 발명의 실시 예에 따른 멀티미디어 콘텐츠 인증하기 위한 시스템 구성을 나타낸 블록 구성도이다. 도 1을 참조하면, 본 발명은 서버(110)와 단말기(120)로 구성된다. 서버(110)는 서버통신부(112), 서버제어부(114), 암호화부(116) 및 데이터베이스(118)로 구성되며, 단말기(120)는 단말통신부(122), 단말제어부(124)로 구성된다. 한편, 서버(110)와 단말기(120)는 유선 또는 무선 네트웍을 이용하여 접속되어 있다. 네트웍은 종합정보 통신망(Integrated Service Digital Network; ISDN)을 이용한 인터넷망일 수 있다.

[0019] 서버(110)의 서버제어부(114)는 콘텐츠의 일정 영역을 선정하여 암호화부(116)로 하여금 상기 선정된 콘텐츠의 일정 영역을 암호화하도록 한다. 이와 같이 암호화된 정보는 서버(110)의 데이터베이스(118)에 등록된다. 데이터베이스(118)에 등록되는 정보는 암호화된 콘텐츠의 헤더 정보이며, 헤더 정보에는 버전정보, 콘텐츠 길이정보, 콘텐츠 타입정보 및 콘텐츠의 암호화 위치 정보를 포함한다. 특히 암호화 위치 정보는 콘텐츠의 암호화된 시작 위치 및 종료 위치를 포함한다.

[0020] 한편, 이와 같이 서버(110)의 데이터베이스에 등록된 정보는 단말기(110)를 통해 서버(110)의 서버통신부(112)를 통해 접속하면, 서버제어부(114)는 해당 콘텐츠 정보가 데이터베이스(118)에 있는 지의 여부를 판단하고 해당 콘텐츠가 데이터베이스(118)에 있는 경우면 해당 서버에 있는 인증키와 단말로부터 전송된 인증키가 일치하는 지의 여부를 판단하여 일치하는 경우 해당 콘텐츠를 사용할 수 있도록 암호화를 해제시키거나, 또는 일치하지 않는 경우 다른 이벤트를 발생시키지 않아 단말기(110)에서 해당 콘텐츠를 사용할 수 없도록 할 수 있다.

[0021] 단말기(120)의 단말제어부(124)는 전술한 바와 같이 해당 콘텐츠를 실행시키는 어플리케이션을 실행시키고, 어플리케이션의 실행에 따라 콘텐츠에 포함된 서버(110)의 URL(Uniform Resource Locator: 파일식별자)를 이용하여 단말통신부(122)를 통해 서버(120)에 접속한다. 접속한 이후에는 전술한 서버(110)의 인증 절차에 따라 서버(110)와 단말기(120)의 인증키가 일치하는 경우, 콘텐츠를 디코딩시켜 사용될 수 있으며, 또는 서버(110)와 단말기(120)의 인증키가 일치하지 않는 경우 콘텐츠는 암호화된 상태로 이벤트가 발생하지 않아 사용할 수 없게 된다.

[0022]

[0023] 도 2는 본 발명의 일 실시예에 따른 멀티미디어 콘텐츠 인증하기 위한 인증 과정을 나타낸 순서도이며, 도 3은 본 발명의 일 실시예에 따른 도 2에 따라 콘텐츠를 암호하하는 과정을 나타낸 순서도이다. 도 2 및 도 3을 참조하면, S202과정에서 서버(110)는 콘텐츠의 일정 영역을 선정하여 상기 선정된 콘텐츠의 일정 영역을 암호화한다.

[0024] 한편, 도 3을 참조하여 콘텐츠를 암호하하는 과정을 살펴보면, S302과정에서 암호화부(116)는 콘텐츠를 일정 비트 단위의 코드 단위로 구분한다. S304과정에서 암호화부(116)는 상기 콘텐츠의 구분된 영역 중 어느 하나를 선택하여 샘플링한다. S306과정에서 암호화부(116)는 샘플링된 영역을 암호화 한다. 암호화부(116)가 수행하는 샘

플링은 8 비트 내지 64 비트로 샘플링하고 이를 암호화 할 수 있으며, 바람직하게는, 16비트로 샘플링하여 암호화한다.

[0025] 헤더정보는 상기 서버의 URL 접속 위치를 포함하고 있다. 따라서, 단말기(120)는 단말통신부(122)를 통해 헤더정보를 이용하여 상기 서버(110)에 접속하고 상기 서버(110)의 인증 결과에 따라 상기 콘텐츠를 인증받아 사용할 수 있다.

[0026] S308과정에서 서버제어부(114)는 이와 같이 암호화된 콘텐츠의 헤더를 데이터베이스에 저장한다.

[0027] 한편, 도 2에서 보면, S204과정에서 단말기(120)에서 어플리케이션을 이용하여 해당 콘텐츠를 실행하고자 하는 요구가 입력되면, 단말기(120)를 콘텐츠의 헤더에 포함된 서버(110)의 URL을 이용하여 서버(110)에 자동으로 접속시킨다.

[0028] S206과정에서 서버 제어부(112)는 단말기(110)를 통해 실행되는 콘텐츠에 대한 인증키값을 단말통신부(122)를 통해 서버(110)로 전송하도록 한다.

[0029]

[0030] S208과정에서 서버제어부(114)는 서버(110)에 등록된 인증키와 단말기(120)를 통해 전송된 인증키값을 비교한다.

[0031] 서버제어부(114)는 S208과정에서의 비교 결과 서버(110)의 데이터베이스(118)에 등록된 인증키와 단말기(120)를 통해 전송된 인증키값이 일치하는 경우 단말기(120) 또는 서버(110)의 인증키값 또는 인증키를 이용하여 상기 콘텐츠를 디코딩한다(S210과정). 사용자는 어플리케이션을 이용하여 상기 콘텐츠를 실행할 수 있도록 한다.

[0032] 서버제어부(114)는 S208과정에서의 비교 결과 서버(110)의 데이터베이스(118)에 등록된 인증키와 단말기(120)를 통해 전송된 인증키값이 일치하지 않는 경우 상기 콘텐츠를 실행하기 위한 어플리케이션을 강제적으로 종료시킨다(S212과정).

[0033] 도 4는 본 발명의 일 실시예에 따른 멀티미디어 콘텐츠의 데이터 구조를 나타낸 블록 데이터 포맷을 나타낸 도면이다. 도 4를 참조하면, 본 발명의 멀티미디어 콘텐츠는 헤더와 데이터로 구성되며, 헤더(400)는 콘텐츠 헤더정보(402), 버전정보(404), 콘텐츠 길이정보(406), 콘텐츠 타입정보(408) 및 콘텐츠의 암호화 정보(410)를 포함한다. 콘텐츠(420)는 인증키값(422) 및 콘텐츠 데이터(424)를 포함한다.

[0034] 콘텐츠 헤더정보(402)는 콘텐츠의 복호화를 위한 암호키 및 권한 정보를 제공하는 서버(110)의 위치정보, 즉 서버(110)의 URI 정보가 기록되며, 콘텐츠 암호화 방식 정보, 콘텐츠 이름 정보, 콘텐츠에 대한 간단한 내용 설명정보, 상기 콘텐츠의 간단한 설명정보는 예를 들어 콘텐츠가 MP3 파일인 경우 가수명 또는 노래 제목 등과 같은 정보를 포함할 수 있다.

[0035] 버전정보(404)는 콘텐츠의 버전 및 부가 정보가 기록된다. 부가 정보는 콘텐츠의 제작과 관련된 정보 및 콘텐츠 타입 정보가 기록된다.

[0036] 콘텐츠 길이정보(406)는 콘텐츠 데이터의 길이 정보가 기록된다. 예컨대, 10.2M의 만화 파일인 경우면, 헤더

(400)의 길이가 0.2M이고 콘텐츠(420)의 길이가 10M임을 구분하여 표시할 수 있다.

[0037] 콘텐츠 타입정보(408)는 콘텐츠의 파일 형식 예를 들어, 해당 콘텐츠가 MP3파일, 영화파일 또는 그림파일들의 집합인 만화 파일인지 등의 콘텐츠 타입정보가 기록되게 된다.

[0038] 콘텐츠의 암호화 정보(410)는 상기 암호화하는 과정에서 상기 암호화된 데이터의 위치정보를 포함하고 있으며, 암호화가 시작되는 위치 및 끝나는 위치에 대한 정보를 포함한다.

[0039]

[0040] 한편, 이상에서는 본 발명의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해 되어져서는 안될 것이다.

부호의 설명

[0041] 110 : 서버 112 : 서버통신부

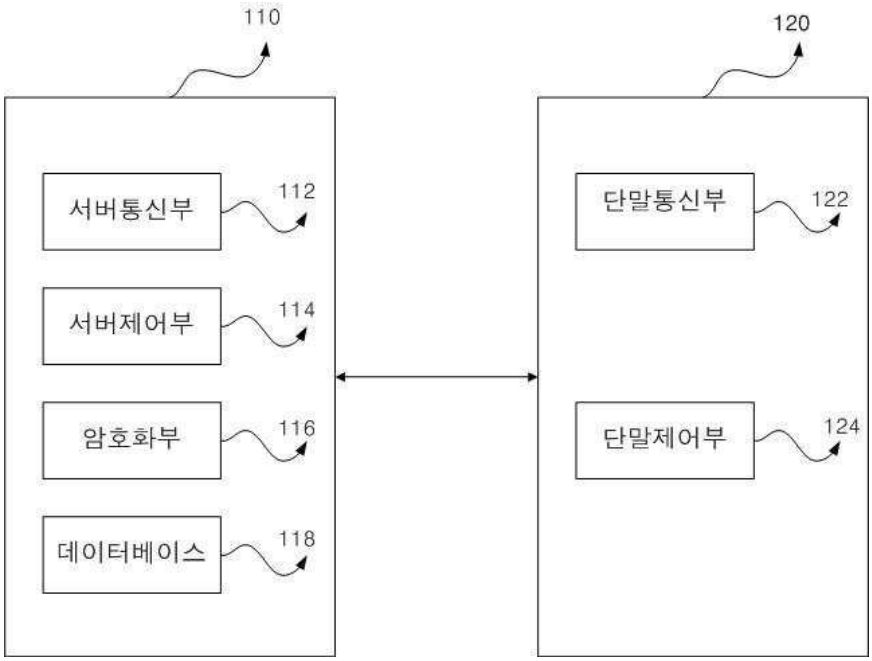
114 : 서버제어부 116 : 암호화부

118 : 데이터베이스 120 : 단말기

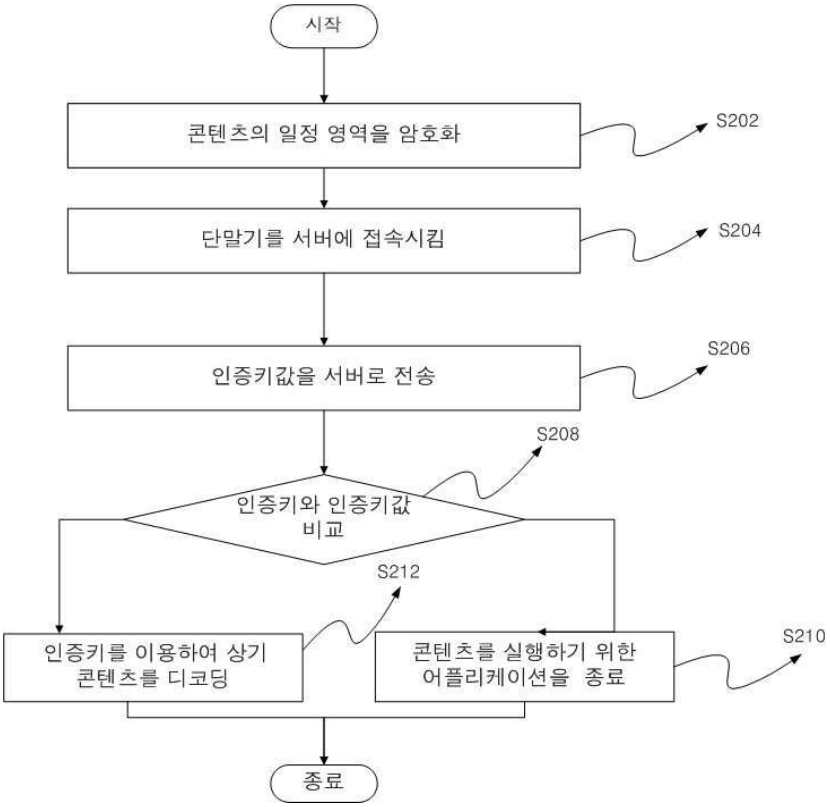
122 : 단말통신부 124 : 단말제어부

도면

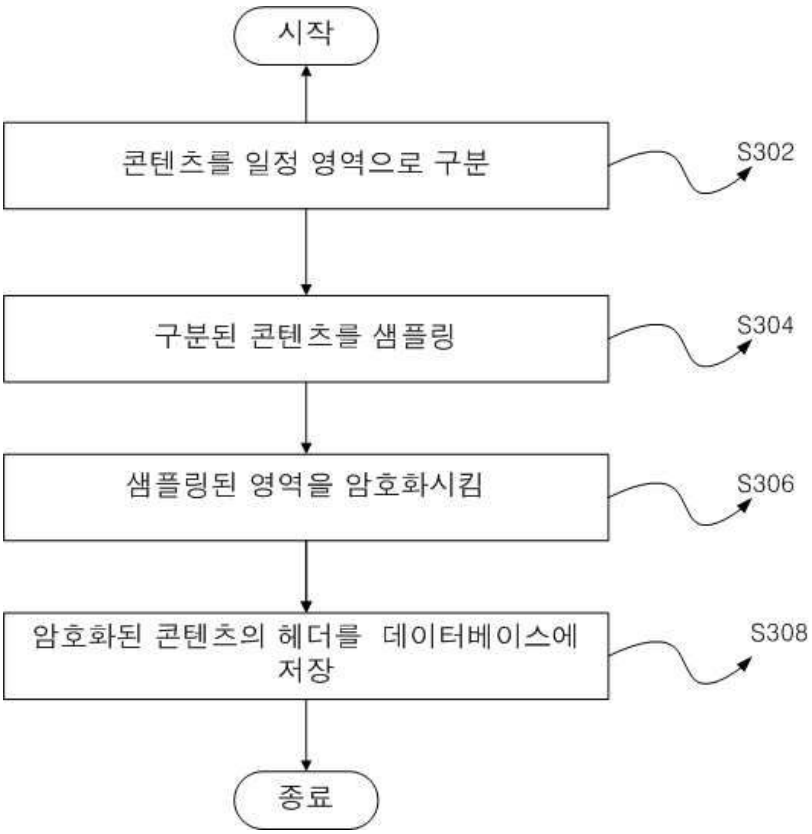
도면1



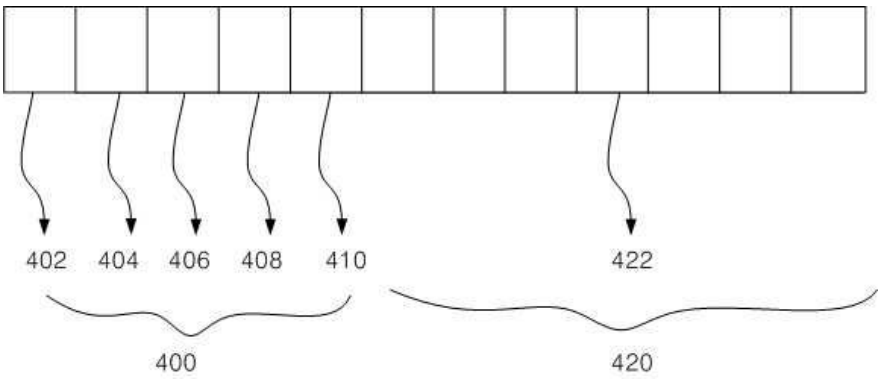
도면2


시작
콘텐츠의 일정 영역을 암호화
S202
단말기를 서버에 접속시킴
S204
인증키값을 서버로 전송
S206
S208
인증키와 인증키값 비교
S212
인증키를 이용하여 상기 콘텐츠를 디코딩
콘텐츠를 실행하기 위한 어플리케이션을 종료
S210
종료

도면3


시작
콘텐츠를 일정 영역으로 구분
S302
구분된 콘텐츠를 샘플링
S304
샘플링된 영역을 암호화시킴
S306
암호화된 콘텐츠의 헤더를 데이터베이스에 저장
S308
종료

도면4


402
404
406
408
410
422
400
420