(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0136531
(43) 공개일자 2019년12월10일

(51) 국제특허분류(Int. Cl.)
H04N 21/2347 (2016.01) *H04N 21/2389* (2011.01)
H04N 21/435 (2011.01) *H04N 21/4385* (2011.01)
(52) CPC특허분류
H04N 21/2347 (2019.01)
H04N 21/2389 (2013.01)
(21) 출원번호 10-2018-0062378
(22) 출원일자 2018년05월31일
심사청구일자 2018년05월31일

(71) 출원인
전남대학교산학협력단
광주광역시 북구 용봉로 77 (용봉동)
(72) 발명자
남지승
광주광역시 북구 설죽로 600, 102동 10층 1001호 (일곡동, 삼호아파트)
강미영
광주광역시 남구 서문대로627번길 9, 202동 14층 1402호(진월동, 진월2차 한국아델리움)
곽용완
광주광역시 동구 제봉로 124(장동)
(74) 대리인
특허법인아이엠

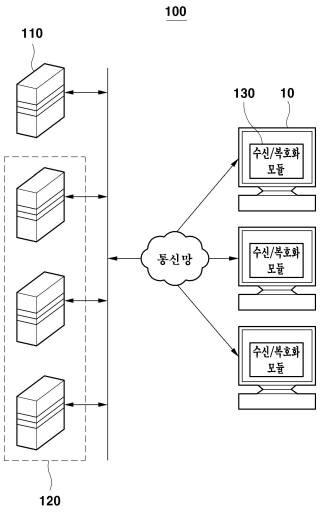
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **동영상의 보안 서비스 방법 및 시스템**

(57) 요 약

본 발명은 동영상의 보안 서비스 제공 방법 및 시스템에 관한 것으로, 보다 구체적으로는 메인 서버에서 동영상을 단위 블록으로 나누어 복수 개의 스트리밍 서버로 분할 전송하고 전송된 단위 블록들을 스트리밍 서버들이 암호화하여 저장하며, 사용자의 클라이언트 컴퓨터에 설치된 수신/복호화 모듈의 요청에 의해 사용자가 선택한 동영상의 암호화된 단위 블록들을 스트리밍 서버들로부터 수신/복호화 모듈이 수신받아 복호화 작업을 수행함으로써 보안이 강화된 동영상 서비스를 제공할 수 있는 동영상 보안 서비스 방법 및 시스템에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04N 21/4353 (2013.01)
H04N 21/4385 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1425112316
부처명 중소벤처기업부
연구관리전문기관 중소기업기술정보진흥원
연구사업명 맞춤형 기술파트너 지원사업
연구과제명 SaaS기반 법무관리시스템의 인트라망 영상처리 보안기술
기 여 율 1/1
주관기관 전남대학교산학협력단
연구기간 2017.09.20 ~ 2018.06.19

명 세 서

청구범위

청구항 1

동영상을 복수 개의 단위 블록으로 분할하여 저장하고, 상기 동영상의 암호화와 관련된 정보인 메타 데이터가 저장된 메인 서버;

상기 메인 서버의 단위 블록들을 분할 전송받고, 전송받은 단위 블록들을 암호화를 통해 보안 블록으로 생성하여 저장하는 복수 개의 스트리밍 서버; 및

상기 메인 서버와 상기 스트리밍 서버에 접속 가능한 클라이언트 컴퓨터에 설치되어 상기 메인 서버로부터 원하는 동영상의 메타 데이터와 상기 스트리밍 서버들로부터 상기 원하는 동영상의 보안 블록들을 수신하고, 수신된 메타 데이터의 정보를 이용하여 수신된 보안 블록들을 복호화하는 수신/복호화 모듈;을 포함하는 것을 특징으로 하는 동영상의 보안 서비스 시스템

청구항 2

제 1 항에 있어서,

상기 메타 데이터는 동영상의 특정 단위 블록이 전송되는 스트리밍 서버 IP 주소, 단위 블록의 데이터 사이즈, 보안 블록의 데이터 사이즈 및 보안 블록 배열 규칙 정보 등을 포함하는 것을 특징으로 하는 동영상의 보안 서비스 시스템

청구항 3

제 2 항에 있어서,

상기 메타 데이터는 해시 알고리즘을 통해 암호문으로 변환되어 저장되는 것을 특징으로 하는 동영상의 보안 서비스 시스템

청구항 4

제 3 항에 있어서,

상기 메타 데이터는 DES(Data Encryption Standard), RSA(Rivest Shamir Adleman), IDEA(Internetional Data Encryption Algorithm) 또는 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화되는 것을 특징으로 하는 동영상의 보안 서비스 시스템

청구항 5

제 1 항에 있어서,

상기 보안 블록은 상기 메인 서버로부터 수신된 단위 블록들을 각각 설정된 개수의 블록 조각으로 나누고, 나누어진 블록 조각들의 배열을 치환하여 생성되는 것을 특징으로 하는 동영상의 보안 서비스 시스템

청구항 6

메인 서버, 스트리밍 서버 및 수신/복호화 모듈을 이용하여 동영상의 보안 서비스를 제공하는 방법으로서,

메인 서버에 저장된 동영상 파일로부터 복수 개의 단위 블록 및 상기 동영상의 암호화와 관련된 정보인 메타 데이터를 생성하는 단계;

상기 단위 블록들을 복수 개의 스트리밍 서버로 분할 전송하는 단계;

상기 스트리밍 서버가 전송받은 단위 블록을 여러 개의 블록 조각으로 나누고 나누어진 여러 개의 블록 조각의 배열을 치환하여 보안 블록을 생성하는 단계;

클라이언트 컴퓨터에 설치된 수신/복호화 모듈을 통해 사용자가 원하는 해당 동영상의 메타 데이터를 수신받는

단계;

상기 수신/복호화 모듈이 상기 메타 데이터에 저장된 해당 영상의 블록 데이터가 전송된 스트리밍 서버들의 주소를 검색하고 검색된 주소의 스트리밍 서버로부터 보안 블록을 전송받는 단계; 및

상기 수신/복호화 모듈이 상기 보안 블록들을 상기 메타 데이터를 이용하여 복호화하는 단계;를 포함하는 것을 특징으로 하는 동영상의 보안 서비스 제공 방법

청구항 7

제 6 항에 있어서,

상기 메타 데이터는 동영상의 특정 단위 블록들이 전송되는 스트리밍 서버 IP 주소, 단위 블록의 데이터 사이즈, 보안 블록 데이터 사이즈 및 보안 블록 배열 규칙 정보 등을 포함하는 것을 특징으로 하는 동영상의 보안 서비스 제공 방법

청구항 8

제 7 항에 있어서,

상기 복수 개의 단위 블록 및 메타 데이터를 생성하는 단계는,

상기 메타 데이터를 해시 알고리즘을 통해 암호문으로 변환하며, 변환된 메타 데이터는 DES(Data Encryption Standard), RSA(Rivest Shamir Adleman), IDEA(Internetional Data Encryption Algorithm) 또는 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화되는 것을 특징으로 하는 동영상의 보안 서비스 제공 방법

발명의 설명

기 술 분 야

[0001] 본 발명은 동영상의 보안 서비스 제공 방법 및 시스템에 관한 것으로, 보다 구체적으로는 메인 서버에서 동영상을 단위 블록으로 나누어 복수 개의 스트리밍 서버로 분할 전송하고 전송된 단위 블록들을 스트리밍 서버들이 암호화하여 저장하며, 사용자의 클라이언트 컴퓨터에 설치된 수신/복호화 모듈의 요청에 의해 사용자가 선택한 동영상의 암호화된 단위 블록들을 스트리밍 서버들로부터 수신/복호화 모듈이 수신받아 복호화 작업을 수행함으로써 보안이 강화된 동영상 서비스를 제공할 수 있는 동영상 보안 서비스 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 스트리밍 서비스이란 인터넷에서 영상, 음향, 애니메이션 등의 파일을 하드디스크 드라이브에 다운로드 받아 재생하던 것을 다운로드 없이 사용자의 단말기에 설치된 미디어 플레이어를 통해 실시간으로 재생해주는 기법을 말한다.

[0003] 또한, 스트리밍 서비스는 동영상을 작은 파일 단위로 쪼개어 전송함으로써 사용자가 전체 데이터를 다운받을 필요 없이 실시간으로 재생할 수 있도록 하는 데이터 전송방식 중 하나이다.

[0004] 이러한, 스트리밍 서비스는 사용자가 전체 데이터를 다운받을 필요 없이 실시간으로 재생할 수 있기 때문에 재생 시간을 단축할 수 있다는 점과 동영상이 사용자의 PC에 저장되지 않기 때문에 동영상의 불법 유통을 방지할 수 있다.

[0005] 한편, 컴퓨터 네트워크의 발달 및 멀티미디어에 대한 수요 증가 인해서 스트리밍 서비스는 증가하고 있으나, 스트리밍 서비스의 증가는 스트리밍 데이터에 대한 보안의 문제를 부각시켰다.

[0006] 일반적으로, 대부분의 스트리밍 서비스는 사용자에게 동영상을 제공할 경우 동영상의 위치 정보를 기록해야만 사용자들이 이용할 수 있으며, 이 위치 정보가 노출될 경우 동영상이 유출된다는 문제점이 있으며, 네트워크 상의 데이터 전송시 또는 동영상을 제공하는 서비스 클라이언트 단에서의 해킹에 취약한 편이다.

[0007] 위와 같은 해킹으로부터 동영상 데이터를 보호하기 위해 방화벽과 같은 외부 접속 클라이언트의 IP 확인 후 동영상의 접근을 차단하여 동영상의 보안을 지원하는 동영상 암호화 기술이 개발되어 왔으나 동영상의 암호화와 복호화에 요구되는 성능에서는 여전히 미흡하거나 화질이 변형되는 문제가 발생하고 특히 다수의 사용자에게 실

시간 인터넷 서비스에 적합한 성능을 제공하는 것이 어렵다.

[0008] 따라서, 외부의 해킹으로부터 동영상을 안전하게 보호할 수 있으면서, 동영상의 화질 변형 없이 사용자들에게 실시간으로 동영상을 제공할 수 있는 방법이 필요하다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 상술한 문제점을 해결하기 위해 안출된 것으로 외부의 해킹으로부터 동영상을 안전하게 보호하여 관리할 수 있으며 사용자에게 동영상 화질의 변형과 재생의 끊김 없이 실시간으로 동영상을 제공하는 데 있다.

과제의 해결 수단

[0010] 상술한 목적을 달성하기 위해 본 발명은 동영상을 복수 개의 단위 블록으로 분할하여 저장하고, 상기 동영상의 암호화와 관련된 정보인 메타 데이터가 저장된 메인 서버; 상기 메인 서버의 단위 블록들을 분할 전송받고, 전송받은 단위 블록들을 암호화를 통해 보안 블록으로 생성하여 저장하는 복수 개의 스트리밍 서버; 및 상기 메인 서버와 상기 스트리밍 서버에 접속 가능한 클라이언트 컴퓨터에 설치되어 상기 메인 서버로부터 원하는 동영상의 메타 데이터와 상기 스트리밍 서버들로부터 상기 원하는 동영상의 보안 블록들을 수신하고, 수신된 메타 데이터의 정보를 이용하여 수신된 보안 블록들을 복호화하는 수신/복호화 모듈;을 포함하는 것을 특징으로 하는 동영상의 보안 서비스 시스템을 제공한다.

[0011] 바람직한 실시예에 있어서, 상기 메타 데이터는 동영상의 특정 단위 블록이 전송되는 스트리밍 서버 IP 주소, 단위 블록의 데이터 사이즈, 보안 블록의 데이터 사이즈 및 보안 블록 배열 규칙 정보 등을 포함한다.

[0012] 바람직한 실시예에 있어서, 상기 메타 데이터는 해시(Hash) 알고리즘을 통해 암호문으로 변환되어 저장된다.

[0013] 바람직한 실시예에 있어서, 상기 메타 데이터는 DES(Data Encryption Standard), RSA(Rivest Shamir Adleman), IDEA(Internetional Data Encryption Algorithm) 또는 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화된다.

[0014] 바람직한 실시예에 있어서, 상기 보안 블록은 상기 메인 서버로부터 수신된 단위 블록들을 각각 설정된 개수의 블록 조각으로 나누고, 나누어진 블록 조각들의 배열을 치환하여 생성된다.

[0015] 또한, 본 발명은 메인 서버, 스트리밍 서버 및 수신/복호화 모듈을 이용하여 동영상의 보안 서비스를 제공하는 방법으로서, 메인 서버에 저장된 동영상 파일로부터 복수 개의 단위 블록 및 상기 동영상의 암호화와 관련된 정보인 메타 데이터를 생성하는 단계; 상기 단위 블록들을 복수 개의 스트리밍 서버로 분할 전송하는 단계; 상기 스트리밍 서버가 전송받은 단위 블록을 여러 개의 블록 조각으로 나누고 나누어진 여러 개의 블록 조각의 배열을 치환하여 보안 블록을 생성하는 단계; 클라이언트 컴퓨터에 설치된 수신/복호화 모듈을 통해 사용자가 원하는 해당 동영상의 메타 데이터를 수신받는 단계; 상기 수신/복호화 모듈이 상기 메타 데이터에 저장된 해당 영상의 블록 데이터가 전송된 스트리밍 서버들의 주소를 검색하고 검색된 주소의 스트리밍 서버로부터 보안 블록을 전송받는 단계; 및 상기 수신/복호화 모듈이 상기 보안 블록들을 상기 메타 데이터를 이용하여 복호화하는 단계;를 포함하는 것을 특징으로 하는 동영상의 보안 서비스 제공 방법을 더 제공한다.

[0016] 바람직한 실시예에 있어서, 상기 메타 데이터는 동영상의 특정 단위 블록들이 전송되는 스트리밍 서버 IP 주소, 단위 블록의 데이터 사이즈, 보안 블록 데이터 사이즈 및 보안 블록 배열 규칙 정보 등을 포함한다.

[0017] 바람직한 실시예에 있어서, 상기 복수 개의 단위 블록 및 메타 데이터를 생성하는 단계는, 상기 메타 데이터를 해시 알고리즘을 통해 암호문으로 변환하며, 변환된 메타 데이터는 DES(Data Encryption Standard), RSA(Rivest Shamir Adleman), IDEA(Internetional Data Encryption Algorithm) 또는 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화된다.

발명의 효과

[0018] 본 발명의 동영상의 보안 서비스 방법 및 시스템에 의하면 복수 개의 스트리밍 서버에 메인 서버가 동영상의 단위 블록을 분배하여 전송하고, 상기 스트리밍 서버들은 전송된 단위 블록을 조각으로 나누고 상기 단위 블록의 조각 배열 순서를 치환함으로써 보안 블록을 생성하며, 동영상을 원본으로 복원하기 위한 정보가 저장된 메타 데이터가 암호화되어, 인증되지 않는 외부의 해킹으로부터 안전하게 동영상을 보호할 수 있을 뿐만 아니라 화질

의 변형 없이 사용자에게 동영상을 제공할 수 있다는 장점이 있다.

[0019] 또한, 본 발명의 동영상의 보안 서비스 방법 및 시스템에 의하면 사용자의 클라이언트 컴퓨터는 복수 개의 스트리밍 서버로부터 각각의 보안 블록들을 전송받기 때문에 상기 클라이언트 컴퓨터와 스트리밍 서버들 간의 전송 부하를 효율적으로 분산시킬 수 있고, 이를 통해 보안 블록의 복호화를 효율적으로 수행할 수 있어 높은 해상도의 동영상도 실시간으로 끊김 없이 제공할 수 있다는 장점이 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일 실시예에 따른 동영상 보안 서비스 제공 시스템의 구성을 보여주는 도면,

도 2는 본 발명의 일 실시예에 따른 동영상 보안 서비스 제공 방법의 흐름도를 보여주는 도면,

도 3은 본 발명의 일 실시예에 따른 단위 블록들이 스트리밍 서버들로 전송되는 과정을 보여주는 도면,

도 4는 본 발명의 일 실시예에 따른 보안 블록 생성 과정을 설명하기 위한 도면,

도 5는 본 발명의 일 실시예에 따른 보안 블록의 복호화 과정을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명에서 사용되는 용어는 가능한 현재 널리 사용되는 일반적인 용어를 선택하였으나, 특정한 경우는 출원인이 임의로 선정한 용어도 있는데 이 경우에는 단순한 용어의 명칭이 아닌 발명의 상세한 설명 부분에 기재되거나 사용된 의미를 고려하여 그 의미가 파악되어야 할 것이다.

[0022] 이하, 첨부한 도면에 도시된 바람직한 실시예들을 참조하여 본 발명의 기술적 구성을 상세하게 설명한다.

[0023] 도 1은 본 발명의 일 실시예에 따른 동영상 보안 서비스 시스템의 구성을 보여주는 것으로 도 1을 참조하면 본 발명의 동영상 보안 서비스 시스템(100)은 메인 서버(110), 복수의 스트리밍 서버(120)를 포함하고, 상기 메인 서버(110)와 상기 스트리밍 서버들(120)을 통신망을 통해 클라이언트 컴퓨터(10)와 연결된다.

[0024] 또한, 상기 각 클라이언트 컴퓨터(10)에는 수신/복호화 모듈(130)이 구비된다.

[0025] 또한, 상기 동영상 보안 서비스 시스템(100)은 상기 클라이언트 컴퓨터(10)로 동영상을 전송하는데, 상기 동영상은 예를 들면 법무와 관련된 동영상일 수 있다.

[0026] 상기 메인 서버(110)는 동영상을 복수 개의 단위 블록으로 분할하여 저장한다.

[0027] 여기서, 상기 단위 블록들은 동일한 사이즈의 크기로 분할된다.

[0028] 또한, 상기 메인 서버(110)에는 상기 동영상의 암호화와 관련된 정보인 메타 데이터가 저장된다.

[0029] 상기 메타 데이터는 동영상의 특정 단위 블록이 전송되는 스트리밍 서버의 IP 주소, 단위 블록의 데이터 사이즈, 아래에서 설명할 보안 블록의 데이터 사이즈 및 보안 블록 배열 규칙 정보 등을 포함한다.

[0030] 또한, 상기 메타 데이터는 해쉬(Hash) 알고리즘을 통해 암호문으로 변환되어 상기 메인 서버(110)에 저장된다.

[0031] 또한, 상기 메타 데이터는 암호화 알고리즘인 DES(Data Encryption Standara), RSA(Rivest Shamir Adleman), IDEA(International Data Encryption Algorithm) 또는 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화된다.

[0032] 상기 스트리밍 서버(120)는 복수 개로 이루어지며, 상기 메인 서버(110)로부터 단위 블록들을 분할 전송받는다.

[0033] 또한, 상기 스트리밍 서버들(120)은 전송받은 단위 블록들을 암호화하여 보안 블록들을 생성한다.

[0034] 여기서, 상기 단위 블록들은 치환(Permutation) 기법으로 암호화되며, 상기 치환 기법은 전송받은 단위 블록을 각각 설정된 개수의 조각으로 나누고, 나누어진 블록 조각의 배열을 치환하는 암호화 기법으로, 이때, 상기 블록 조각의 배열이 치한된 단위 블록을 보안 블록이라 한다.

[0035] 상기 수신/복호화 모듈(130)은 사용자의 클라이언트 컴퓨터(10)에 설치되어 상기 클라이언트 컴퓨터(10)가 상기 메인 서버(110) 및 상기 스트리밍 서버들(120)과 접속이 가능하게 한다.

[0036] 즉, 상기 수신/복호화 모듈(130)은 상기 메인 서버(110)로부터 상기 메타 데이터를 수신받을 수 있으며, 상기 스트리밍 서버들(120)로부터 보안 블록들을 수신받을 수 있다.

[0037] 또한, 상기 수신/복호화 모듈(130)은 수신받은 메타 데이터와 상기 보안 블록의 암호를 해독하는 복호화 기능을 수행하여 사용자에게 동영상을 제공할 수 있다.

[0038] 이하에서는 도 2 내지 도 5를 참조하여 메인 서버, 스트리밍 서버 및 수신/복호화 모듈을 이용하여 동영상의 보안 서비스 제공 방법을 상세히 설명한다.

[0039] 도 2는 본 발명의 일 실시예에 따른 동영상의 보안 서비스 제공 방법을 설명하기 위한 흐름도로, 도 2를 참조하면, 먼저, 상기 메인 서버는 동영상을 복수 개의 단위 블록으로 나누어 생성하고, 상기 동영상의 암호화와 관련된 정보인 메타 데이터를 생성한다(S1000).

[0040] 또한, 상기 메타 데이터는 전술한 바 있듯이 동영상의 특정 단위 블록이 전송되는 스트리밍 서버의 IP 주소, 단위 블록의 데이터 사이즈, 아래에서 설명할 보안 블록의 데이터 사이즈 및 보안 블록 배열 규칙 정보 등을 포함하는 데이터이며, 생성된 메타 데이터는 해쉬(Hash) 알고리즘을 통해 암호문으로 변환되어 저장되고, 변환된 메타 데이터는 암호화 알고리즘을 통해 다시 한번 암호화된다.

[0041] 여기서, 상기 암호화 알고리즘은 DES(Data Encryption Standard), RSA(Rivest Shamir Adleman), IDEA(International Data Encryption Algorithm) 또는 AES(Advanced Encryption Standard)이 사용될 수 있다.

[0042] 다음, 상기 메인 서버는 상기 단위 블록들을 스트리밍 서버들로 분할 전송하고(S2000), 상기 각 스트리밍 서버들은 보안 블록들을 생성한다(S3000).

[0043] 더욱 자세하게는, 도 3을 참조하면, 도 3은 본 발명의 일 실시예에 따른 단위 블록들이 스트리밍 서버들로 전송되는 과정을 보여주는 것으로 상기 단위 블록 및 메타 데이터 생성 이후에는, 상기 메인 서버에 저장된 단위 블록들(B)을 복수 개의 스트리밍 서버들로 균일하게 라운드 로빈(Round Robin) 방법으로 분배하여 전송하게 되며, 상기 스트리밍 서버들은 전송된 단위블록들(B)을 암호화하여 보안 블록들(SB)을 생성하게 된다.

[0044] 또한, 도 4를 참조하여 상기 보안 블록들의 생성 방법을 자세하게 설명하면, 도 4는 본 발명의 일 실시예에 따른 보안 블록 생성 과정을 설명하기 위한 도면으로 도 4를 참조하면, 상기 보안 블록의 암호화는 단위 블록(B0)을 설정된 개수의 블록 조각(P0,P1,P2,P3,P4,P5,...)으로 나누고, 나누어진 블록 조각들(P0,P1,P2,P3,P4,P5,...)의 배열을 치환함으로써 보안 블록(SB0)을 생성한다.

[0045] 따라서, 본 발명의 동영상 보안 서비스 및 시스템은 동영상의 암호화 정보가 저장된 메타 데이터가 이중으로 암호화 되어있으며, 동영상의 단위 블록들이 각각의 스트리밍 서버로 분산되고, 분산된 단위 블록들을 단순한 치환 기법을 적용하여 보안 블록을 만들어냄으로써, 외부의 해킹으로부터 안전하게 동영상이 유출되는 것을 방지할 수 있다.

[0046] 또한, 본 발명의 동영상 보안 서비스 및 시스템은 단순히 단위 블록의 조각들을 치환하여 보안 블록을 생성하기 때문에 다른 고도화된 암호화 알고리즘과 달리 복호화 과정에서 데이터의 변형 또는 손실을 줄일 수 있어 동영상의 화질 변형이 없이 사용자에게 제공할 수 있다는 장점이 있다.

[0047] 다음, 사용자가 클라이언트 컴퓨터를 통해 원하는 동영상을 선택하게 되면 수신/복호화 모듈은 상기 메인 서버로 해당 동영상의 전송을 요청하게 된다(S4000).

[0048] 다음, 상기 메인 서버는 상기 수신/복호화 모듈로 해당 동영상의 메타 데이터를 상기 수신/ 복호화 모듈로 전송한다(S5000).

[0049] 다음, 상기 메타 데이터에 저장된 해당 동영상의 단위 블록이 전송된 스트리밍 서버의 IP 주소를 이용하여 스트리밍 서버들을 검색하여 접속하고(S6000), 상기 스트리밍 서버들로부터 보안 블록들을 요청한다(S7000).

[0050] 한편, 상기 수신/복호화 모듈에는 암호화된 메타 데이터를 복호화할 수 있는 암호화 정보가 미리 저장되어 있어, 상기 메인 서버로부터 수신받은 메타 데이터를 복호화하여 암호를 해독할 수 있다.

[0051] 다음, 해당 동영상의 보안 블록들을 소유하고 있는 스트리밍 서버들은 저장된 보안 블록들을 상기 수신/복호화 모듈로 전송한다(S8000).

[0052] 다음, 상기 보안 블록들을 전송받은 수신/복호화 모듈은 상기 메타 데이터에 저장된 정보들을 이용하여 상기 보안 블록을 복호화한다(S9000).

[0053] 더욱 자세하게는 도 5를 참조하면, 도 5는 본 발명의 일 실시예에 따른 보안 블록의 복호화 과정을 설명하기 위한 도면으로, 도 5를 참조하여 복호화 과정을 상세히 설명하면, 상기 메타 데이터에 저장된 보안 블록 배열 규

칙 정보에 따라 상기 수신/복호화 모듈(130)이 각각의 스트리밍 서버로부터 수신되는 보안 블록들(SB0, SB1, SB2, SB3, SB4, SB5, ...)의 블록 조각들을 원상태로 재배열하여, 상기 보안 블록들(SB0, SB1, SB2, SB3, SB4, SB5, ...)을 각각 이전의 단위 블록들(B0,B1,B2, ...)로 재생성하고, 생성된 단위 블록들(B0,B1,B2, ...)은 클라이언트 컴퓨터(10)에 설치된 미디어 플레이어(11)로 전송되면서 동영상이 재생된다.

[0054] 따라서, 본 발명의 동영상 보안 서비스 방법 및 시스템은 클라이언트 컴퓨터가 수신/복호화 모듈을 통해 복수개의 스트리밍 서버로부터 보안 블록들을 전송받기 때문에 상기 클라이언트 컴퓨터와 스트리밍 서버들 간의 전송 부하를 효율적으로 분산시킬 수 있으며, 이를 통해 보안 블록들의 복호화를 효율적으로 수행할 수 있어 높은 해상도의 동영상도 실시간으로 끊김없이 제공할 수 있다는 장점이 있다.

[0055] 이상에서 살펴본 바와 같이 본 발명은 바람직한 실시예를 들어 도시하고 설명하였으나, 상기 실시예에 한정되지 아니하며 본 발명의 정신을 벗어나지 않는 범위 내에서 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변경과 수정이 가능할 것이다.

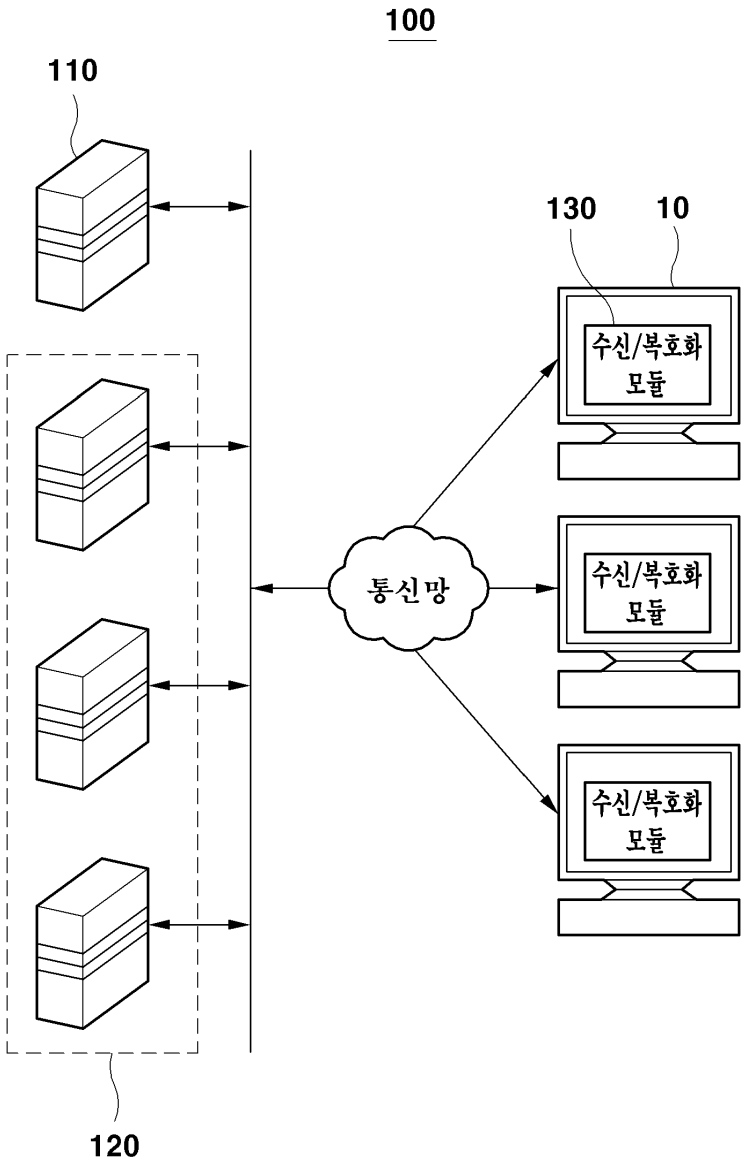
부호의 설명

[0057] 100:동영상 보안 서비스 시스템 110:메인 서버

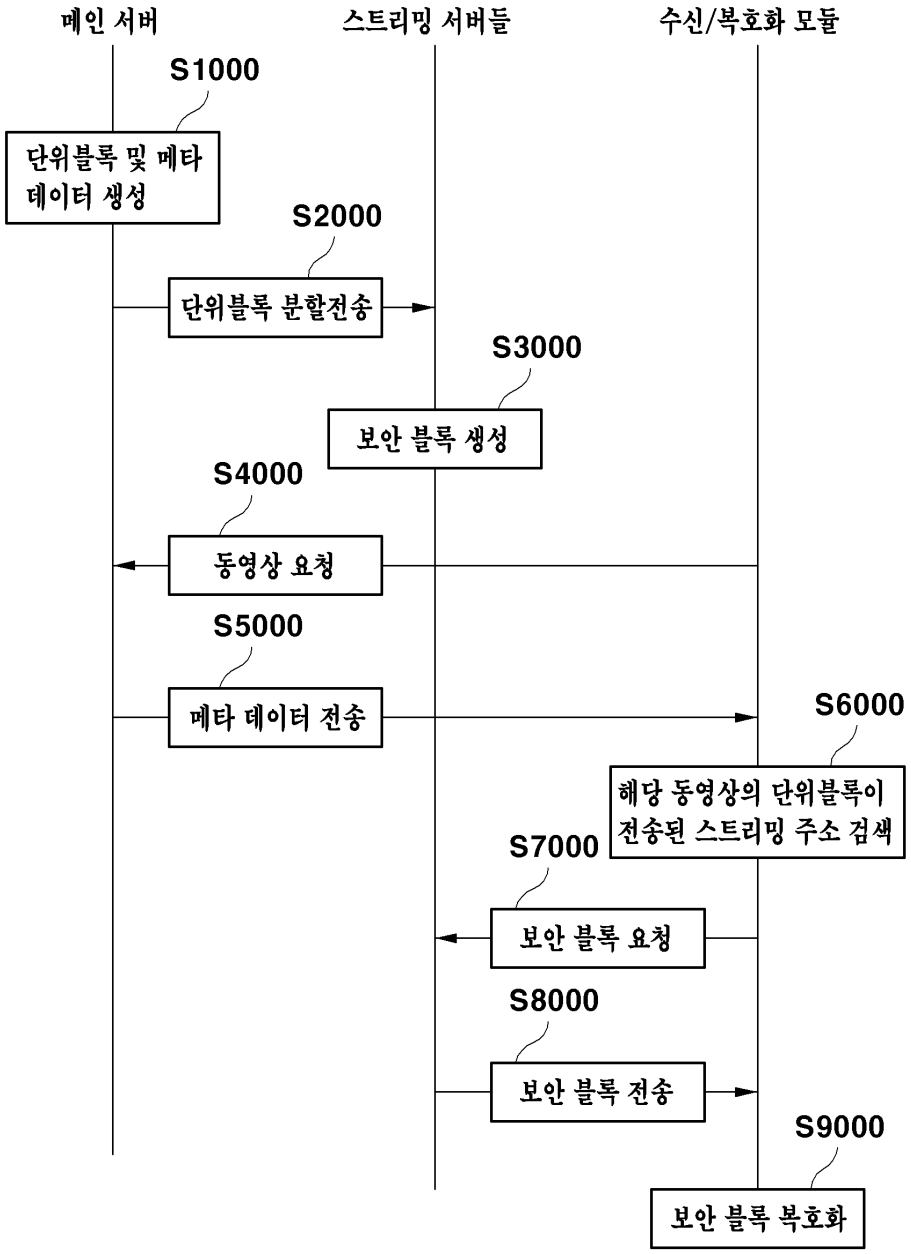
120:스트리밍 서버 130:수신/복호화 모듈

도면

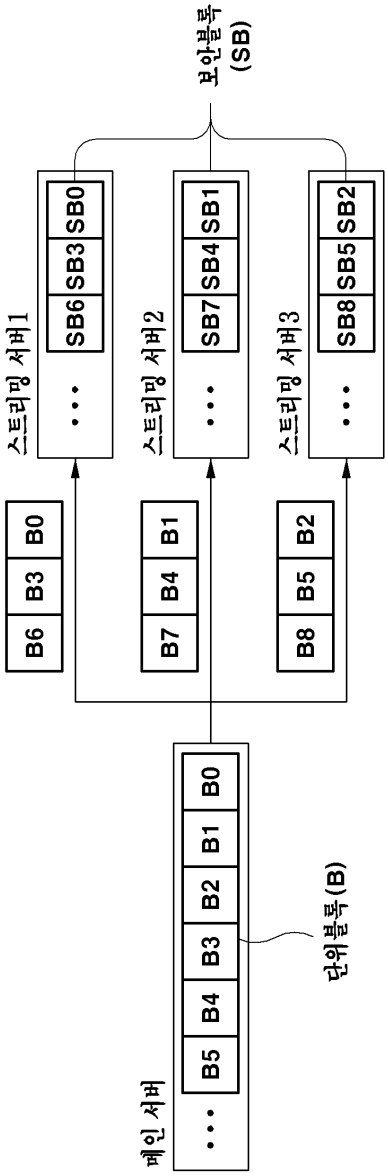
도면1



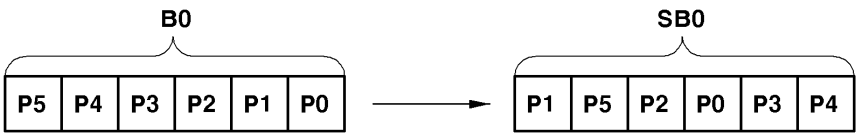
도면2


메인 서버
스트리밍 서버들
수신/복호화 모듈
S1000
단위블록 및 메타 데이터 생성
S2000
단위블록 분할전송
S3000
보안 블록 생성
S4000
동영상 요청
S5000
메타 데이터 전송
S6000
해당 동영상의 단위블록이 전송된 스트리밍 주소 검색
S7000
보안 블록 요청
S8000
보안 블록 전송
S9000
보안 블록 복호화

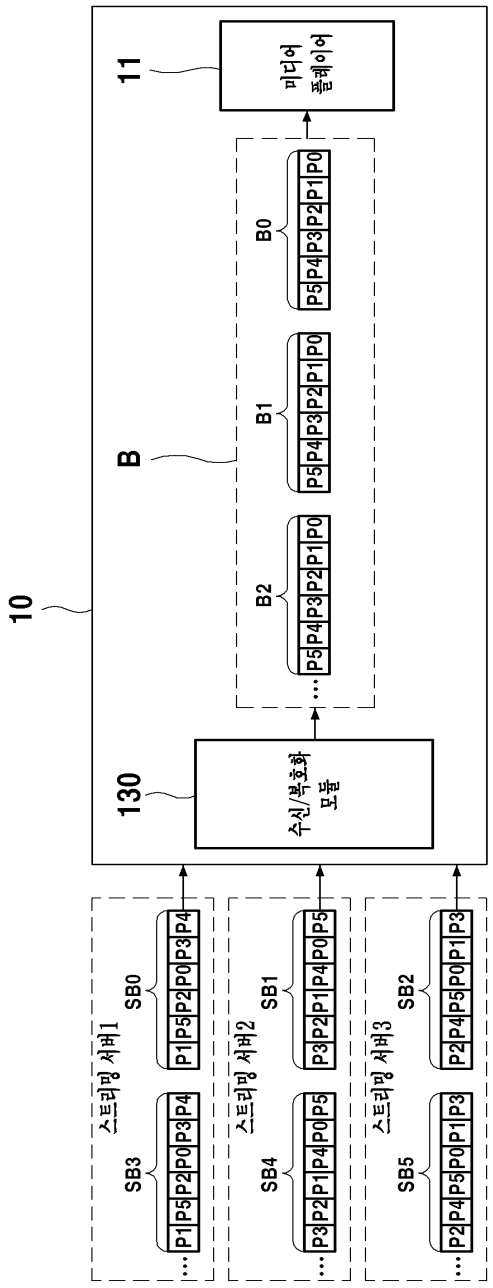
도면3


보안블록
(SB)
스트리밍 서버1
스트리밍 서버2
스트리밍 서버3
SB0
SB3
SB6
SB1
SB4
SB7
SB2
SB5
SB8
B0
B3
B6
B1
B4
B7
B2
B5
B8
메인 서버
B0
B1
B2
B3
B4
B5
단위블록(B)

도면4


B0
P5
P4
P3
P2
P1
P0
SB0
P1
P5
P2
P0
P3
P4

도면5


10
11
미디어 플레이어
B
B0
B1
B2
P5 P4 P3 P2 P1 P0
130
수신/복호화 모듈
스트리밍 서버1
스트리밍 서버2
스트리밍 서버3
SB0
SB1
SB2
SB3
SB4
SB5
P1 P5 P2 P0 P3 P4
P3 P2 P1 P4 P0 P5
P2 P4 P5 P0 P1 P3