



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년03월17일

(11) 등록번호 10-1604201

(24) 등록일자 2016년03월10일

(51) 국제특허분류(Int. Cl.)

H04N 21/2347 (2016.01) H04N 19/40 (2014.01)

H04N 21/236 (2011.01)

(21) 출원번호 10-2014-0183676

(22) 출원일자 2014년12월19일

심사청구일자 2014년12월19일

(56) 선행기술조사문헌

WO2006025322 A1*

KR1020110003133 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

동국대학교 경주캠퍼스 산학협력단

경상북도 경주시 석장동 707

(72) 발명자

송유진

대전광역시 유성구 상대로 17 한라비발디아파트
303동 1701호

김의창

경상북도 경주시 황성동 광증길 73-16 현진에버빌
102-802

구석모

경기도 군포시 당산로 132번길 16

(74) 대리인

특허법인청맥

전체 청구항 수 : 총 18 항

심사관 : 이성현

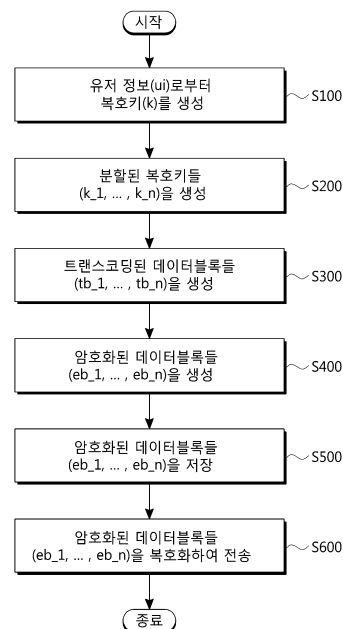
(54) 발명의 명칭 분산 트랜스코딩 방법 및 이를 이용한 분산 트랜스코딩 시스템

(57) 요약

데이터의 기밀성을 향상시킨 분산 트랜스코딩 방법 및 이를 이용한 분산 트랜스코딩 시스템이 개시된다. 이러한 분산 트랜스코딩 방법은 n개의 데이터노드들(DataNode_1, ..., DataNode_n)을 통해 임의의 데이터를 분산하여 트랜스코딩(transcoding)하는 방법에 관한 것으로(단, n은 2 이상의 정수임), 유저 단말기(User_i)에서 제공된

(뒷면에 계속)

대표도 - 도1



유저 정보(ui)로부터 복호키(k)를 생성하는 단계; 상기 유저 단말기(User_i)에 저장된 데이터(data_i)에서 분할된 n개의 데이터블록들(d_1, ..., d_n)을 트랜스코딩하여 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계; 상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 암호화하여 암호화된 데이터블록들(ed_1, ..., ed_n)을 생성하는 단계; 및 상기 암호화된 데이터블록들(ed_1, ..., ed_n)을 상기 데이터노드들에 각각 저장하는 단계를 포함한다. 이로써, 상기 데이터(data_i)가 상기 복호키(k)를 통해 암호화되어 저장됨에 따라, 상기 데이터노드들(DataNode_1, ..., DataNode_n)을 관리하는 내부 관리자에게 상기 콘텐츠 데이터가 노출되는 것이 억제할 수 있다.

명세서

청구범위

청구항 1

n개의 데이터노드들(DataNode_1, ..., DataNode_n)을 통해 임의의 데이터를 분산하여 트랜스코딩(transcoding)하는 분산 트랜스코딩 방법에 있어서(단, n은 2 이상의 정수임),

유저 단말기(User_i)에서 제공된 유저 정보(ui)로부터 복호키(k)를 생성하는 단계;

상기 유저 단말기(User_i)에 저장된 데이터(data_i)에서 분할된 n개의 데이터블록들(d_1, ..., d_n)을 트랜스코딩하여 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계;

상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 암호화하여 암호화된 데이터블록들(ed_1, ..., ed_n)을 생성하는 단계;

상기 암호화된 데이터블록들(ed_1, ..., ed_n)을 상기 데이터노드들에 각각 저장하는 단계; 및

임의의 단말기로부터 제공된 유저 입력 정보(ui_input)를 이용하여 상기 암호화된 데이터블록들(ed_1, ..., ed_n)을 복호화하여 상기 임의의 단말기로 전송하는 단계를 포함하고,

상기 암호화된 데이터블록들(ed_1, ..., ed_n)을 복호화하여 상기 임의의 단말기로 전송하는 단계는

상기 유저 입력 정보(ui_input)를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed_1, ..., ed_n)의 복호화 가능 여부를 판단하는 단계;

상기 유저 입력 정보(ui_input)에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_input)로부터 입력 복호키(ik)를 생성하는 단계;

상기 입력 복호키(ik)를 이용해 상기 암호화된 데이터블록들(ed_1, ..., ed_n)을 복호화하여 복호화된 데이터블록들(dd_1, ..., dd_n)을 생성하는 단계; 및

상기 복호화된 데이터블록들(dd_1, ..., dd_n)을 상기 임의의 단말기로 전송하는 단계를 포함하며,

상기 유저 정보(ui)는

m개의 유저 개별 정보들(ui_1, ..., ui_m)을 포함하고(단, m은 2 이상의 정수임),

상기 암호화된 데이터블록들(ed_1, ..., ed_n)의 복호화 가능 여부를 확인하는 단계에서는,

상기 유저 개별 정보들(ui_1, ..., ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 임계치 t 이상인 경우, 상기 암호화된 데이터블록들(ed_1, ..., ed_n)의 복호화가 가능하다고 판단하고(단, t는 1 이상 m 이하의 정수임),

상기 유저 개별 정보들(ui_1, ..., ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 상기 임계치 t 미만인 경우, 상기 암호화된 데이터블록들(ed_1, ..., ed_n)의 복호화가 불가능하다고 판단하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 2

제1항에 있어서, 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계는

상기 데이터(data_i)를 분할하여 상기 데이터블록들(d_1, ..., d_n)을 생성하는 단계; 및

상기 데이터블록들(d_1, ..., d_n)을 트랜스코딩하여 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계를 포함하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 3

제1항에 있어서, 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계에서는,

상기 분할된 n 개의 데이터블록들($d_1, \dots, d_n$)을 HEVC(High Efficiency Video coding)로 트랜스코딩하여 상기 트랜스코딩된 데이터블록들($td_1, \dots, td_n$)을 생성하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 4

제1항에 있어서, 상기 복호키(k)를 분할하여 분할된 복호키들($k_1, \dots, k_n$)을 생성하는 단계를 더 포함하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 5

제4항에 있어서, 상기 암호화된 데이터블록들($ed_1, \dots, ed_n$)을 생성하는 단계에서는,

상기 분할된 복호키들($k_1, \dots, k_n$)을 통해 상기 트랜스코딩된 데이터블록들($td_1, \dots, td_n$)을 각각 암호화하여 상기 암호화된 데이터블록들($ed_1, \dots, ed_n$)을 생성하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

제1항에 있어서, 상기 임계치 t 를 결정하는 단계를 더 포함하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 11

제1항에 있어서, 상기 데이터($data_i$)는 원본 영상 데이터를 포함하고,

상기 복호화된 데이터블록들($dd_1, \dots, dd_n$)은 상기 임의의 단말기에서 상기 원본 영상 데이터와 대응되는 합성 영상 데이터를 형성하며,

상기 합성 영상 데이터의 해상도는

상기 유저 개별 정보들($ui_1, \dots, ui_m$) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수에 따라 변경되는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 12

제11항에 있어서, 상기 합성 영상 데이터의 해상도는

상기 유저 개별 정보들($ui_1, \dots, ui_m$) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 m 일 경우, 상기 원본 영상 데이터의 해상도와 동일하고,

상기 유저 개별 정보들($ui_1, \dots, ui_m$) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 m 보다 작아질수록 상기 원본 영상 데이터의 해상도보다 낮아지는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 13

제1항에 있어서, 상기 복호키(k)를 분할하여 분할된 복호키들($k_1, \dots, k_n$)을 생성하는 단계; 및

상기 입력 복호키(ik)를 분할하여 분할된 입력 복호키들($ik_1, \dots, ik_n$)을 생성하는 단계를 더 포함하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 14

제13항에 있어서, 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 생성하는 단계에서는,

상기 분할된 복호키들(k₁, ..., k_n)을 통해 상기 트랜스코딩된 데이터블록들(td₁, ..., td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 생성하고,

상기 복호화된 데이터블록들(dd₁, ..., dd_n)을 생성하는 단계에서는,

상기 분할된 입력 복호키들(ik₁, ..., ik_n)을 통해 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd₁, ..., dd_n)을 생성하는 것을 특징으로 하는 분산 트랜스코딩 방법.

청구항 15

유저 단말기(User_i)로부터 제공된 유저 정보(ui)로부터 복호키(k)를 생성하는 비밀 분산 처리부; 및

데이터(data_i)로부터 분할된 n개의 데이터블록들(d₁, ..., d_n)을 상기 유저 단말기(User_i)로부터 각각 제공받아 트랜스코딩(transcoding)하여 트랜스코딩된 데이터블록들(td₁, ..., td_n)을 각각 생성하고, 상기 비밀 분산 처리부로부터 제공된 상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td₁, ..., td_n)을 각각 암호화하여 암호화된 데이터블록들(ed₁, ..., ed_n)을 각각 생성하여 저장하는 n개의 데이터노드들(DataNode₁, ..., DataNode_n)(단, n은 2 이상의 정수임)을 포함하고,

상기 비밀 분산 처리부는

임의의 단말기로부터 제공된 유저 입력 정보(ui_{input})를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed₁, ..., ed_n)의 복호화 가능 여부를 판단하고, 상기 유저 입력 정보(ui_{input})에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_{input})로부터 입력 복호키(ik)를 생성하며,

상기 데이터노드들(DataNode₁, ..., DataNode_n)은

상기 비밀 분산 처리부로부터 제공된 상기 입력 복호키(ik)를 이용해 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 각각 복호화하여 복호화된 데이터블록들(dd₁, ..., dd_n)을 각각 생성하고, 상기 복호화된 데이터블록들(dd₁, ..., dd_n)을 상기 임의의 단말기로 전송하고,

상기 유저 정보(ui)는

m개의 유저 개별 정보들(ui₁, ..., ui_m)을 포함하며(단, m은 2 이상의 정수임),

상기 비밀 분산 처리부는

상기 유저 개별 정보들(ui₁, ..., ui_m) 중 상기 유저 입력 정보(ui_{input})에 포함된 정보의 개수가 임계치 t 이상인 경우, 상기 암호화된 데이터블록들(ed₁, ..., ed_n)의 복호화가 가능하다고 판단하고(단, t는 1 이상 m 이하의 정수임),

상기 유저 개별 정보들(ui₁, ..., ui_m) 중 상기 유저 입력 정보(ui_{input})에 포함된 정보의 개수가 상기 임계치 t 미만인 경우, 상기 암호화된 데이터블록들(ed₁, ..., ed_n)의 복호화가 불가능하다고 판단하는 것을 특징으로 하는 분산 트랜스코딩 시스템.

청구항 16

제15항에 있어서, 상기 데이터노드들(DataNode₁, ..., DataNode_n)의 주소를 저장하고 있고, 상기 유저 단말기(User_i) 또는 상기 비밀 분산 처리부와 상기 데이터노드들(DataNode₁, ..., DataNode_n) 사이에서 임의의 파일의 분산 저장 및 로딩을 관리하는 네임노드(NameNode)를 더 포함하는 것을 특징으로 하는 분산 트랜스코딩 시스템.

청구항 17

제15항에 있어서, 상기 데이터노드들(DataNode₁, ..., DataNode_n)은

상기 분할된 n개의 데이터블록들(d₁, ..., d_n)을 HEVC(High Efficiency Video coding)로 각각 트랜스코딩하여 상기 트랜스코딩된 데이터블록들(td₁, ..., td_n)을 각각 생성하는 것을 특징으로 하는 분산 트랜스코딩

시스템.

청구항 18

제15항에 있어서, 상기 비밀 분산 처리부는

상기 복호키(k)를 분할하여 분할된 복호키들($k_1, \dots, k_n$)을 생성하고,

상기 데이터노드들(DataNode₁, ..., DataNode_n)은

상기 분할된 복호키들($k_1, \dots, k_n$)을 통해 상기 트랜스코딩된 데이터블록들(td₁, ..., td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 각각 생성하는 것을 특징으로 하는 분산 트랜스코딩 시스템.

청구항 19

삭제

청구항 20

삭제

청구항 21

제15항에 있어서, 상기 유저 단말기(User_i)는

유저의 입력에 의해 상기 임계치 t를 결정하여 상기 비밀 분산 처리부로 전송하는 것을 특징으로 하는 분산 트랜스코딩 시스템.

청구항 22

제15항에 있어서, 상기 데이터(data_i)는 원본 영상 데이터를 포함하고,

상기 임의의 단말기는 상기 복호화된 데이터블록들(dd₁, ..., dd_n)로부터 상기 원본 영상 데이터와 대응되는 합성 영상 데이터를 형성하며,

상기 합성 영상 데이터의 해상도는

상기 유저 개별 정보들(ui₁, ..., ui_m) 중 상기 유저 입력 정보(ui_{input})에 포함된 정보의 개수에 따라 변경되는 것을 특징으로 하는 분산 트랜스코딩 시스템.

청구항 23

제15항에 있어서, 상기 비밀 분산 처리부는

상기 복호키(k)를 분할하여 분할된 복호키들($k_1, \dots, k_n$)을 생성하고,

상기 데이터노드들(DataNode₁, ..., DataNode_n)은

상기 비밀 분산 처리부로부터 제공된 상기 분할된 복호키들($k_1, \dots, k_n$)을 통해 상기 트랜스코딩된 데이터블록들(td₁, ..., td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 각각 생성하는 것을 특징으로 하는 분산 트랜스코딩 시스템.

청구항 24

제23항에 있어서, 상기 비밀 분산 처리부는

상기 입력 복호키(ik)를 분할하여 분할된 입력 복호키들(ik₁, ..., ik_n)을 생성하고,

상기 데이터노드들(DataNode₁, ..., DataNode_n)은

상기 분할된 입력 복호키들(ik₁, ..., ik_n)을 통해 상기 암호화된 데이터블록들(ed₁, ..., ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd₁, ..., dd_n)을 각각 생성하는 것을 특징으로 하는 분산 트랜스코딩 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 분산 트랜스코딩 방법 및 이를 이용한 분산 트랜스코딩 시스템에 관한 것으로, 더욱 상세하게는 초고 해상도 콘텐츠를 분할하여 트랜스코딩하는 분산 트랜스코딩 방법 및 이를 이용한 분산 트랜스코딩 시스템에 관한 것이다.

배경 기술

- [0002] 네트워크 기술의 발달로 기존 콘텐츠보다 우수한 고화질 콘텐츠를 사용자에게 제공하는 것이 가능해지고 있다. 최근 제작되고 있는 초고해상도 콘텐츠는 부호화 과정 없이 현재의 네트워크 대역폭으로 전송하는 것은 불가능하다. 따라서 압축률이 매우 높은 HEVC(High Efficiency Video Coding) 부호화 기법을 이용하여 초고해상도 콘텐츠를 전송할 수 있도록 압축해야 한다.
- [0003] 한편, 초고해상도 콘텐츠를 부호화하는 트랜스코딩 시스템은 단일 시스템으로 부호화 처리하는 것이 쉽지 않기 때문에 다수의 노드를 이용하여 부호화 처리하는 분산 트랜스코딩 시스템을 구성할 필요가 있다. 이러한 분산 트랜스코딩 시스템은 초고해상도 콘텐츠를 전송 가능한 상태로 트랜스코딩을 수행한 후, 실시간 스트리밍 프로토콜을 이용하여 사용자가 소유하고 있는 다양한 형태의 디바이스로 전송하고 있다.
- [0004] 하지만, 위와 같은 스트리밍 서비스는 사용 권한이 없는 사용자의 접근을 차단하기 어렵다. 또한, 상기 스트리밍 서비스를 제공하는 서버로부터 사용자에게 전송하는 과정에서, 악의적인 공격자가 데이터 스트림을 분석하여 원본 영상을 쉽게 취득할 수 있다는 문제점이 발생할 수 있다.
- [0005] 더 나아가, 상기 분산 트랜스코딩 시스템은 콘텐츠를 블록 단위로 분산 처리하기 위해 다수의 노드에 분산 저장되어 있기 때문에, 콘텐츠 소유자는 어떤 노드에 자신의 데이터가 저장되어 있는지 확인할 수도 없다.
- [0006] 그러나, 현재의 분산 트랜스코딩 시스템에서, 내부 관리자는 특정 데이터를 선별적으로 검색하여 정보를 확인하는 것이 가능하고, 분산되어 있는 블록의 위치 정보까지 확인할 수 있다. 그 결과, 상기 분산 트랜스코딩 시스템이 기밀성이 보장되지 않은 상태로 사용될 경우, 악의적인 내부관리자에 의해 중요한 콘텐츠가 외부로 유출될 수도 있다.

발명의 내용

해결하려는 과제

- [0007] 따라서, 본 발명은 이러한 문제점을 해결하기 위한 것으로, 본 발명의 해결하고자 하는 과제는 데이터의 기밀성을 향상시킨 분산 트랜스코딩 방법을 제공하는 것이다.
- [0008] 또한, 본 발명의 해결하고자 하는 다른 과제는 상기 분산 트랜스코딩 방법을 이용한 분산 트랜스코딩 시스템을 제공하는 것이다.

과제의 해결 수단

- [0009] 본 발명의 일 실시예에 의한 분산 트랜스코딩 방법은 n 개의 데이터노드들(DataNode_1, ..., DataNode_n)을 통해 임의의 데이터를 분산하여 트랜스코딩(transcoding)하는 방법에 관한 것으로(단, n 은 2 이상의 정수임), 유저 단말기(User_i)에서 제공된 유저 정보(ui)로부터 복호키(k)를 생성하는 단계; 상기 유저 단말기(User_i)에 저장된 데이터(data_i)에서 분할된 n 개의 데이터블록들(d_1, ..., d_n)을 트랜스코딩하여 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계; 상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 암호화하여 암호화된 데이터블록들(ed_1, ..., ed_n)을 생성하는 단계; 및 상기 암호화된 데이터블록들(ed_1, ..., ed_n)을 상기 데이터노드들에 각각 저장하는 단계를 포함한다.
- [0010] 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계는 상기 데이터(data_i)를 분할하여 상기 데이터블록들(d_1, ..., d_n)을 생성하는 단계; 및 상기 데이터블록들(d_1, ..., d_n)을 트랜스코딩하여 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계를 포함할 수 있다.
- [0011] 상기 트랜스코딩된 데이터블록들(td_1, ..., td_n)을 생성하는 단계에서는, 상기 분할된 n 개의 데이터블록들(d_1, ..., d_n)을 HEVC(High Efficiency Video coding)로 트랜스코딩하여 상기 트랜스코딩된 데이터블록들

(td₁, ... , td_n)을 생성할 수 있다.

- [0012] 상기 분산 트랜스코딩 방법은 상기 복호키(k)를 분할하여 분할된 복호키들(k₁, ... , k_n)을 생성하는 단계를 더 포함할 수 있다.
- [0013] 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성하는 단계에서는, 상기 분할된 복호키들(k₁, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성할 수 있다.
- [0014] 상기 분산 트랜스코딩 방법은 임의의 단말기로부터 제공된 유저 입력 정보(ui_input)를 이용하여 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 복호화하여 상기 임의의 단말기로 전송하는 단계를 더 포함할 수 있다.
- [0015] 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 복호화하여 상기 임의의 단말기로 전송하는 단계는 상기 유저 입력 정보(ui_input)를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화 가능 여부를 판단하는 단계; 상기 유저 입력 정보(ui_input)에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_input)로부터 입력 복호키(ik)를 생성하는 단계; 상기 입력 복호키(ik)를 이용해 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 복호화하여 복호화된 데이터블록들(dd₁, ... , dd_n)을 생성하는 단계; 및 상기 복호화된 데이터블록들(dd₁, ... , dd_n)을 상기 임의의 단말기로 전송하는 단계를 포함할 수 있다.
- [0016] 상기 유저 정보(ui)는 m개의 유저 개별 정보들(ui₁, ... , ui_m)을 포함할 수 있다(단, m은 2 이상의 정수임).
- [0017] 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화 가능 여부를 확인하는 단계에서는, 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 임계치 t 이상인 경우, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화가 가능하다고 판단할 수 있고(단, t는 1 이상 m 이하의 정수임), 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 상기 임계치 t 미만인 경우, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화가 불가능하다고 판단할 수 있다.
- [0018] 상기 분산 트랜스코딩 방법은 상기 임계치 t를 결정하는 단계를 더 포함할 수 있다.
- [0019] 상기 데이터(data_i)는 원본 영상 데이터를 포함할 수 있고, 상기 복호화된 데이터블록들(dd₁, ... , dd_n)은 상기 임의의 단말기에서 상기 원본 영상 데이터와 대응되는 합성 영상 데이터를 형성할 수 있다. 이때, 상기 합성 영상 데이터의 해상도는 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수에 따라 변경될 수 있다.
- [0020] 상기 합성 영상 데이터의 해상도는 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 m일 경우, 상기 원본 영상 데이터의 해상도와 동일할 수 있고, 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 m보다 작아질수록 상기 원본 영상 데이터의 해상도보다 낮아질 수 있다.
- [0021] 상기 분산 트랜스코딩 방법은 상기 복호키(k)를 분할하여 분할된 복호키들(k₁, ... , k_n)을 생성하는 단계; 및 상기 입력 복호키(ik)를 분할하여 분할된 입력 복호키들(ik₁, ... , ik_n)을 생성하는 단계를 더 포함할 수 있다.
- [0022] 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성하는 단계에서는, 상기 분할된 복호키들(k₁, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성할 수 있다. 또한, 상기 복호화된 데이터블록들(dd₁, ... , dd_n)을 생성하는 단계에서는, 상기 분할된 입력 복호키들(ik₁, ... , ik_n)을 통해 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd₁, ... , dd_n)을 생성할 수 있다.
- [0023] 이어서, 본 발명의 일 실시예에 의한 분산 트랜스코딩 시스템은 비밀 분산 처리부 및 n개의 데이터노드들(DataNode₁, ... , DataNode_n)(단, n은 2 이상의 정수임)을 포함한다.
- [0024] 상기 비밀 분산 처리부는 유저 단말기(User_i)로부터 제공된 유저 정보(ui)로부터 복호키(k)를 생성한다. 상기 데이터노드들(DataNode₁, ... , DataNode_n)은 데이터(data_i)로부터 분할된 n개의 데이터블록들(d₁, ... , d_n)을 상기 유저 단말기(User_i)로부터 각각 제공받아 트랜스코딩(transcoding)하여 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 각각 생성하고, 상기 비밀 분산 처리부로부터 제공된 상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 각각 암호화하여 암호화된 데이터블록들(ed₁, ... , ed_n)을 각

각 생성하여 저장한다.

- [0025] 상기 분산 트랜스코딩 시스템은 상기 데이터노드들(DataNode_1, ... , DataNode_n)의 주소를 저장하고 있고, 상기 유저 단말기(User_i) 또는 상기 비밀 분산 처리부와 상기 데이터노드들(DataNode_1, ... , DataNode_n) 사이에서 임의의 파일의 분산 저장 및 로딩을 관리하는 네임노드(NameNode)를 더 포함할 수 있다.
- [0026] 상기 데이터노드들(DataNode_1, ... , DataNode_n)은 상기 분할된 n개의 데이터블록들(d_1, ... , d_n)을 HEVC(High Efficiency Video coding)로 각각 트랜스코딩하여 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 생성할 수 있다.
- [0027] 상기 비밀 분산 처리부는 상기 복호키(k)를 분할하여 분할된 복호키들(k_1, ... , k_n)을 생성할 수 있고, 상기 데이터노드들(DataNode_1, ... , DataNode_n)은 상기 분할된 복호키들(k_1, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 생성할 수 있다.
- [0028] 상기 비밀 분산 처리부는 임의의 단말기로부터 제공된 유저 입력 정보(ui_input)를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화 가능 여부를 판단하고, 상기 유저 입력 정보(ui_input)에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_input)로부터 입력 복호키(ik)를 생성할 수 있다. 또한, 상기 데이터노드들(DataNode_1, ... , DataNode_n)은 상기 비밀 분산 처리부로부터 제공된 상기 입력 복호키(ik)를 이용해 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 복호화하여 복호화된 데이터블록들(dd_1, ... , dd_n)을 각각 생성하고, 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 상기 임의의 단말기로 전송할 수 있다.
- [0029] 상기 유저 정보(ui)는 m개의 유저 개별 정보들(ui_1, ... , ui_m)을 포함할 수 있다(단, m은 2 이상의 정수임). 이때, 상기 비밀 분산 처리부는 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 임계치 t 이상인 경우, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화가 가능하다고 판단할 수 있고(단, t는 1 이상 m 이하의 정수임), 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 상기 임계치 t 미만인 경우, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화가 불가능하다고 판단할 수 있다.
- [0030] 상기 유저 단말기(User_i)는 유저의 입력에 의해 상기 임계치 t를 결정하여 상기 비밀 분산 처리부로 전송할 수 있다.
- [0031] 상기 데이터(data_i)는 원본 영상 데이터를 포함할 수 있고, 상기 임의의 단말기는 상기 복호화된 데이터블록들(dd_1, ... , dd_n)로부터 상기 원본 영상 데이터와 대응되는 합성 영상 데이터를 형성할 수 있다. 이때, 상기 합성 영상 데이터의 해상도는 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수에 따라 변경될 수 있다.
- [0032] 상기 비밀 분산 처리부는 상기 복호키(k)를 분할하여 분할된 복호키들(k_1, ... , k_n)을 생성할 수 있다. 이때, 상기 데이터노드들(DataNode_1, ... , DataNode_n)은 상기 비밀 분산 처리부로부터 제공된 상기 분할된 복호키들(k_1, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 생성할 수 있다.
- [0033] 상기 비밀 분산 처리부는 상기 입력 복호키(ik)를 분할하여 분할된 입력 복호키들(ik_1, ... , ik_n)을 생성할 수 있다. 이때, 상기 데이터노드들(DataNode_1, ... , DataNode_n)은 상기 분할된 입력 복호키들(ik_1, ... , ik_n)을 통해 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 각각 생성할 수 있다.

발명의 효과

- [0034] 이와 같이 본 발명에 의한 분산 트랜스코딩 방법 및 이를 이용한 분산 트랜스코딩 시스템에 따르면, 비밀 보호를 원하는 콘텐츠 데이터가 분산 트랜스코딩되어 데이터노드들(DataNode_1, ... , DataNode_n)에 각각 저장될 때, 유저 정보(ui)에 의해 생성된 복호키(k)를 통해 암호화되어 저장됨에 따라, 상기 데이터노드들(DataNode_1, ... , DataNode_n)을 관리하는 내부 관리자에게 상기 콘텐츠 데이터가 노출되는 것이 억제될 수 있다.
- [0035] 또한, 상기 콘텐츠 데이터를 전송받기 원하는 사용자가 임의의 단말기를 통해 상기 유저 정보(ui)와 대응되는 유저 입력 정보(ui_input)를 입력하면, 비밀 분산 처리부가 상기 유저 입력 정보(ui_input)에 의해 복호화가 가

능한지 여부를 판단한 후 입력 복호화(ik)를 생성하고, 상기 데이터노드들(DataNode_1, ..., DataNode_n)은 상기 입력 복호화(ik)를 이용하여 복호화하여 상기 임의의 단말기로 전송할 수 있다.

[0036] 또한, 상기 유저 정보(ui) 및 상기 유저 입력 정보(ui_input)가 서로 일치하는 정보의 개수가 임계치 t 이상일 경우에만 복호화되도록 설정하여 기밀성을 향상시킬 수 있다.

[0037] 또한, 상기 유저 정보(ui) 및 상기 유저 입력 정보(ui_input)가 서로 일치하는 정보의 개수가 상기 임계치 t 이상에서 증가될수록 복호화되는 데이터의 질 또는 양, 예를 들어 영상의 해상도가 증가되도록 설정할 수도 있다. 따라서, 암호화되어 분산 저장되어 있는 데이터가 무엇인지 확인만 원하는 사용자는 상기 임계치 t 정도의 정보만 입력함으로써, 완전한 데이터를 복호화하여 확인하지 않고 낮은 질 또는 적은 양의 데이터로 복호화하여 신속히 확인할 수 있다.

도면의 간단한 설명

[0038] 도 1은 본 발명의 일 실시예에 의한 분산 트랜스코딩 방법을 설명하기 위한 순서도이다.

도 2는 도 1의 분산 트랜스코딩 방법 중 복호화 과정을 상세하게 설명하기 위한 순서도이다.

도 3은 도 1의 분산 트랜스코딩 방법을 이용한 분산 트랜스코딩 시스템을 설명하기 위한 블록도이다.

도 4는 도 3의 분산 트랜스코딩 시스템을 통해 암호화 과정의 일 예를 설명하기 위한 도면이다.

도 5는 도 3의 분산 트랜스코딩 시스템을 통해 복호화 과정의 일 예를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0039] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다.

[0040] 그러나, 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.

[0041] 본 출원에서 사용한 용어는 단지 특정한 실시예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0042] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예들을 보다 상세하게 설명한다.

[0043] 도 1은 본 발명의 일 실시예에 의한 분산 트랜스코딩 방법을 설명하기 위한 순서도이다.

[0044] 도 1을 참조하면, 본 실시예에 의한 분산 트랜스코딩 방법은 n개의 데이터노드들(DataNode_1, ..., DataNode_n)을 통해 임의의 데이터를 분산하여 트랜스코딩(transcoding)하는 방법에 관한 것으로, 임의의 컴퓨터 시스템에서 수행될 수 있다. 여기서, n은 2 이상의 정수이다.

[0045] 상기 분산 트랜스코딩 방법으로, 우선 유저 단말기(User_i)에서 제공된 유저 정보(ui)로부터 복호키(k)를 생성한다(S100).

[0046] 상기 유저 정보(ui)는 m개의 유저 개별 정보들(ui_1, ..., ui_m)을 포함할 수 있다. 여기서, m은 2 이상의 정수이다. 예를 들어, 상기 유저 개별 정보들(ui_1, ..., ui_m)에는, 유저 아이디(User ID), 매체 접근 제어 주소(MAC_add), 콘텐츠 문맥(Content Context) 등이 포함될 수 있다. 또한, 상기 콘텐츠 문맥에는, 예를 들어, 콘텐츠의 제목, 재생 시간, 사용 코덱, 해상도, 비트 전송률, 프레임 속도, 오디오 채널정보, 오디오샘플 속도 등이 포함되어 있을 수 있다. 한편, 상기 유저 개별 정보들(ui_1, ..., ui_m)에는, 유저가 정한 암호문, 유저

에 관한 개인 정보, 유저에 관한 기타 정보 등도 포함되어 있을 수도 있다.

- [0047] 이어서, 상기 복호키(k)를 분할하여 분할된 복호키들(k₁, ... , k_n)을 생성한다(S200).
- [0048] 본 실시예에서, 상기 복호키(k)는 keygen 함수에 의해 분할되어 상기 분할된 복호키들(k₁, ... , k_n)을 생성할 수 있다. 예를 들어, 상기 분할된 복호키들(k₁, ... , k_n)은 상기 복호키(k)가 n개로 동일하게 분할된 값들일 수 있지만, 상기 복호키(k)와 동일한 값들일 수도 있으면, 상기 복호키(k)에서 임의의 부분이 수정, 삭제, 또는 추가된 값들일 수도 있다.
- [0049] 이어서, 상기 유저 단말기(User_i)에 저장된 데이터(data_i)에서 분할된 n개의 데이터블록들(d₁, ... ,d_n)을 트랜스코딩하여 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 생성한다(S300).
- [0050] 구체적으로, 상기 데이터(data_i)를 분할하여 상기 데이터블록들(d₁, ... ,d_n)을 생성한 후, 상기 데이터블록들(d₁, ... ,d_n)을 트랜스코딩하여 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 생성할 수 있다.
- [0051] 본 실시예에서, 상기 데이터(data_i)가 초고화질 영상이라고 할 때, 상기 트랜스코딩은 HEVC(High Efficiency Vidio coding)로의 트랜스코딩을 의미할 수 있다.
- [0052] 상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 암호화하여 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성한다(S400).
- [0053] 구체적으로, 상기 분할된 복호키들(k₁, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성할 수 있다.
- [0054] 한편, 상기 S200 단계가 생략될 경우, 상기 S400 단계에서, 상기 복호키(k) 하나를 가지고 상기 트랜스코딩된 데이터블록들(td₁, ... , td_n) 모두를 암호화하여 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 생성할 수도 있다.
- [0055] 이어서, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 상기 데이터노드들에 각각 저장한다(S500).
- [0056] 이후, 임의의 단말기로부터 제공된 유저 입력 정보(ui_input)를 이용하여 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 복호화하여 상기 임의의 단말기로 전송한다(S600).
- [0057] 본 실시예에서, 상기 임의의 단말기는 상기 유저 입력 정보(ui_input)를 제공함으로써 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 복호화하여 제공받기 원하는 단말기로, 상기 유저 단말기(User_i)일 수도 있고, 그 외 다른 단말기일 수도 있다.
- [0058] 도 2는 도 1의 분산 트랜스코딩 방법 중 복호화 과정을 상세하게 설명하기 위한 순서도이다.
- [0059] 도 2를 참조하여, 상기 S600 단계에 대해 상세하게 설명하고자 한다.
- [0060] 우선, 상기 유저 입력 정보(ui_input)를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화 가능 여부를 판단한다(S610).
- [0061] 구체적으로, 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 임계치 t 이상인 경우, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화가 가능하다고 판단할 수 있다. 여기서, t는 1 이상 m 이하의 정수이다.
- [0062] 반면, 상기 유저 개별 정보들(ui₁, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 상기 임계치 t 미만인 경우, 상기 암호화된 데이터블록들(ed₁, ... , ed_n)의 복호화가 불가능하다고 판단할 수 있다.
- [0063] 이어서, 상기 유저 입력 정보(ui_input)에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_input)로부터 입력 복호키(ik)를 생성한다(S620).
- [0064] 이어서, 상기 입력 복호키(ik)를 분할하여 분할된 입력 복호키들(ik₁, ... , ik_n)을 생성한다(S630).
- [0065] 이어서, 상기 입력 복호키(ik)를 이용해 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 복호화하여 복호화된 데이터블록들(dd₁, ... , dd_n)을 생성한다(S640).
- [0066] 구체적으로, 상기 분할된 입력 복호키들(ik₁, ... , ik_n)을 통해 상기 암호화된 데이터블록들(ed₁, ... , ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd₁, ... , dd_n)을 생성할 수 있다.

- [0067] 한편, 상기 S630 단계가 생략될 경우, 상기 S640 단계에서, 상기 입력 복호키(ik) 하나를 가지고 상기 암호화된 데이터블록들(ed_1, ... , ed_n) 모두를 복호화하여 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 생성할 수도 있다.
- [0068] 본 실시예에서, 상기 S200 단계가 생략되는 경우, 상기 S630 단계도 함께 생략될 수 있다.
- [0069] 이어서, 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 상기 임의의 단말기로 전송한다(S650).
- [0070] 본 실시예에서, 상기 분산 트랜스코딩 방법은 상기 임계치 t를 결정하는 단계를 더 포함할 수 있다. 상기 임계치 t는 일정한 상수값으로 결정되거나, m에 대해 일정한 비율에 따른 값을 가질 수도 있으며, 상기 유저 단말기(User_i)에서 제공되어 결정될 수도 있다.
- [0071] 본 실시예에서, 상기 데이터(data_i)는 원본 영상 데이터를 포함할 수 있고, 상기 복호화된 데이터블록들(dd_1, ... , dd_n)은 상기 임의의 단말기에서 상기 원본 영상 데이터와 대응되는 합성 영상 데이터를 형성할 수 있다. 이때, 상기 합성 영상 데이터의 해상도는 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수에 따라 변경될 수 있다.
- [0072] 구체적으로, 상기 합성 영상 데이터의 해상도는 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 m일 경우, 상기 원본 영상 데이터의 해상도와 동일할 수 있고, 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 m보다 작아질수록 상기 원본 영상 데이터의 해상도보다 낮아질 수 있다.
- [0073] 이하, 위에서 설명한 분산 트랜스코딩 방법을 이용한 분산 트랜스코딩 시스템의 일 예를 상세하게 설명하고자 한다.
- [0074] 도 3은 도 1의 분산 트랜스코딩 방법을 이용한 분산 트랜스코딩 시스템을 설명하기 위한 블록도이다.
- [0075] 도 3을 참조하면, 상기 분산 트랜스코딩 시스템은 상기 유저 단말기(User_i)(10)과 접속되어 상기 유저 단말기(User_i)(10)에 저장된 상기 데이터(data_i)를 분산 트랜스코딩하여 저장하는 시스템으로, 비밀 분산 처리부(100), n개의 데이터노드들(DataNode_1, ... , DataNode_n)(200) 및 네임노드(NameNode)(300)을 포함할 수 있다.
- [0076] 상기 비밀 분산 처리부(100)는 상기 유저 단말기(User_i)(10)로부터 제공된 상기 유저 정보(ui)로부터 상기 복호키(k)를 생성할 수 있다.
- [0077] 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 데이터(data_i)로부터 분할된 상기 n개의 데이터블록들(d_1, ... , d_n)을 상기 유저 단말기(User_i)로부터 각각 제공받아 트랜스코딩(transcoding)하여 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 생성하고, 상기 비밀 분산 처리부(100)로부터 제공된 상기 복호키(k)를 이용해 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 생성하여 저장할 수 있다.
- [0078] 상기 네임노드(NameNode)(300)는 상기 데이터노드들(DataNode_1, ... , DataNode_n)의 주소를 저장하고 있고, 상기 유저 단말기(User_i) 또는 상기 비밀 분산 처리부와 상기 데이터노드들(DataNode_1, ... , DataNode_n) 사이에서 임의의 파일의 분산 저장 및 로딩을 관리할 수 있다.
- [0079] 본 실시예에서, 상기 네임노드(NameNode)(300) 및 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 하나의 분산 파일 시스템, 예를 들어 HDFS(Hadoop Distributed File System)을 구성할 수 있다. 즉, 상기 네임노드(NameNode)(300)는 메타 데이터, 예를 들어 파일의 경로와 크기, 소유자의 소유 그룹, 속성, 블록 ID, 블록을 보유하고 있는 데이터노드(DataNode) 등의 정보 등을 저장하고 관리할 수 있다. 또한, 상기 네임노드(NameNode)(300)는 HDFS의 사용 상황과 데이터노드(DataNode)의 다운 여부, 클라이언트의 처리 요청 접수 등을 수행할 수 있다.
- [0080] 상기 비밀 분산 처리부(100)는 상기 복호키(k)를 분할하여 상기 분할된 복호키들(k_1, ... , k_n)을 생성할 수 있다. 이때, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 분할된 복호키들(k_1, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 생성할 수 있다.
- [0081] 상기 비밀 분산 처리부(100)는 상기 임의의 단말기로부터 제공된 상기 유저 입력 정보(ui_input)를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화 가능 여부를 판단하고, 상기 유

저 입력 정보(ui_input)에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_input)로부터 상기 입력 복호키(ik)를 생성할 수 있다.

[0082] 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 비밀 분산 처리부(100)로부터 제공된 상기 입력 복호키(ik)를 이용해 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 각각 생성하고, 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 상기 임의의 단말기로 전송할 수 있다.

[0083] 상기 비밀 분산 처리부는 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 상기 임계치 t 이상인 경우, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화가 가능하다고 판단할 수 있고, 반면 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수가 상기 임계치 t 미만인 경우, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화가 불가능하다고 판단할 수 있다.

[0084] 상기 유저 단말기(User_i)(10)는 유저의 입력에 의해 상기 임계치 t를 결정하여 상기 비밀 분산 처리부(100)로 전송할 수 있다. 이와 다르게, 상기 비밀 분산 처리부(100)는 상기 임계치 t를 자체적으로 결정할 수도 있다. 예를 들어, 상기 비밀 분산 처리부(100)는 상기 임계치 t를 일정한 상수값으로 결정하거나, m에 대해 일정한 비율에 따른 값으로 결정할 수 있다.

[0085] 상기 비밀 분산 처리부(100)는 상기 복호키(k)를 분할하여 상기 분할된 복호키들(k_1, ... , k_n)을 생성할 수 있다. 이때, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 비밀 분산 처리부(100)로부터 제공된 상기 분할된 복호키들(k_1, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 생성할 수 있다.

[0086] 또한, 상기 비밀 분산 처리부(100)는 상기 입력 복호키(ik)를 분할하여 상기 분할된 입력 복호키들(ik_1, ... , ik_n)을 생성할 수 있다. 이때, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 분할된 입력 복호키들(ik_1, ... , ik_n)을 통해 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 각각 생성할 수 있다.

[0087] 이하, 위에서 설명한 분산 트랜스코딩 시스템에 의해 데이터가 암호화되어 저장되는 과정의 일 예를 설명하고자 한다.

[0088] 도 4는 도 3의 분산 트랜스코딩 시스템을 통해 암호화 과정의 일 예를 설명하기 위한 도면이다.

[0089] 도 4를 참조하면, 우선 상기 유저 단말기(User_i)(10)는 자신이 저장하고 있는 상기 데이터(data_i)를 분산 트랜스코딩하여 저장하겠으니, 상기 데이터(data_i)를 수신해달라는 요청 신호를 상기 비밀 분산 처리부(100)로 전달할 수 있다.

[0090] 이어서, 상기 비밀 분산 처리부(100)는 상기 데이터(data_i)의 분산 저장에 앞서 필요한 상기 유저 정보(ui)를 제공해달라는 요청 신호를 상기 유저 단말기(User_i)(10)로 전송할 수 있다.

[0091] 이어서, 상기 유저 단말기(User_i)(10)는 유저의 입력에 의해 작성된 상기 유저 정보(ui)를 상기 비밀 분산 처리부(100)로 전송할 수 있다. 이때, 상기 유저 단말기(User_i)(10)는 유저의 입력에 결정된 상기 임계치 t도 함께 상기 비밀 분산 처리부(100)로 전송할 수도 있다.

[0092] 이어서, 상기 비밀 분산 처리부(100)는 상기 유저 정보(ui)로부터 키생성 함수를 이용하여 상기 복호키(k)를 생성할 수 있다.

[0093] 이어서, 상기 비밀 분산 처리부(100)는 상기 복호키(k)를 키분할 함수를 이용하여 상기 분할된 복호키들(k_1, ... , k_n)을 생성할 수 있다.

[0094] 이어서, 상기 네임노드(NameNode)(300)는 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)의 주소를 상기 비밀 분산 처리부(100)로 제공할 수 있다. 여기서, 상기 네임노드(NameNode)(300)에 의한 주소 제공은 상기 복호키(k)가 분할된 이후가 아니라, 그 이전에 어느 단계에도 수행될 수 있고, 본 암호화 과정이 수행되지 전에 수행될 수도 있다.

[0095] 이어서, 상기 비밀 분산 처리부(100)는 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)의 주소를 상기 유저 단말기(User_i)(10)로 제공할 수 있다.

- [0096] 이어서, 상기 유저 단말기(User_i)(10)는 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)의 개수와 대응되도록 상기 데이터(data_i)를 n개로 분할하여 상기 데이터블록들(d_1, ... ,d_n)을 생성할 수 있다.
- [0097] 이어서, 상기 유저 단말기(User_i)(10)는 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)의 주소를 이용하여, 상기 데이터블록들(d_1, ... ,d_n)을 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)로 각각 전송할 수 있다.
- [0098] 이어서, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 데이터블록들(d_1, ... ,d_n)을 각각 HEVC로 트랜스코딩하여 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 생성할 수 있다.
- [0099] 이어서, 상기 비밀 분산 처리부(100)는 상기 분할된 복호키들(k_1, ... , k_n)을 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)로 각각 전송할 수 있다. 여기서, 상기 비밀 분산 처리부(100)에 의한 상기 분할된 복호키들(k_1, ... , k_n)의 전송은 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)이 생성된 후가 아니라, 그 이전의 어느 단계에서도 수행될 수 있다.
- [0100] 이어서, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 분할된 복호키들(k_1, ... , k_n)을 통해 상기 트랜스코딩된 데이터블록들(td_1, ... , td_n)을 각각 암호화하여 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 생성하여 저장할 수 있다.
- [0101] 이하, 위에서 설명한 분산 트랜스코딩 시스템에 의해 데이터가 암호화되어 저장되는 과정의 일 예를 설명하고자 한다.
- [0102] 도 5는 도 3의 분산 트랜스코딩 시스템을 통해 복호화 과정의 일 예를 설명하기 위한 도면이다.
- [0103] 도 5를 참조하면, 우선 상기 데이터(data_i)를 제공받기 원하는 상기 임의의 단말기(User_k)(20)는 유저의 입력에 의해 작성된 상기 유저 입력 정보(ui_input)을 상기 비밀 분산 처리부(100)로 전송할 수 있다.
- [0104] 이어서, 상기 비밀 분산 처리부(100)는 상기 임의의 단말기로부터 제공된 상기 유저 입력 정보(ui_input)를 상기 유저 정보(ui)와 비교하여, 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화 가능 여부를 판단할 수 있다.
- [0105] 이어서, 상기 비밀 분산 처리부(100)는 상기 유저 입력 정보(ui_input)에 의한 복호화가 가능하다고 판단되면, 상기 유저 입력 정보(ui_input)로부터 키생성 함수를 이용하여 상기 입력 복호키(ik)를 생성할 수 있다.
- [0106] 이어서, 상기 비밀 분산 처리부(100)는 상기 입력 복호키(ik)를 키분할 함수를 통해 분할하여 상기 분할된 입력 복호키들(ik_1, ... , ik_n)을 생성할 수 있다.
- [0107] 이어서, 상기 비밀 분산 처리부(100)는 상기 분할된 입력 복호키들(ik_1, ... , ik_n)을 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)로 각각 전송할 수 있다.
- [0108] 이어서, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 분할된 입력 복호키들(ik_1, ... , ik_n)을 통해 상기 암호화된 데이터블록들(ed_1, ... , ed_n)을 각각 복호화하여 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 각각 생성할 수 있다.
- [0109] 이어서, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 암호화된 데이터블록들(ed_1, ... , ed_n)의 복호화가 완료되어 전송할 수 있는 신호를 상기 네임노드(NameNode)(300)로 전송할 수 있다.
- [0110] 이어서, 상기 네임노드(NameNode)(300)는 상기 임의의 단말기(User_k)(20)의 주소를 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)로 각각 전송할 수 있다. 여기서, 상기 임의의 단말기(User_k)(20)의 주소는 그 이전 단계에 이미 상기 네임노드(NameNode)(300)에 저장되어 있어야 한다. 예를 들어, 상기 임의의 단말기(User_k)(20)의 주소는 상기 유저 입력 정보(ui_input)가 상기 임의의 단말기(User_k)(20)에서 상기 비밀 분산 처리부(100)로 전송될 때 함께 또는 그 이전에 전송된 후, 다시 상기 네임노드(NameNode)(300)로 전송되어 저장되어 있을 수 있다.
- [0111] 이어서, 상기 데이터노드들(DataNode_1, ... , DataNode_n)(200)은 상기 임의의 단말기(User_k)(20)의 주소를 이용하여, 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 상기 임의의 단말기(User_k)(20)로 전송할 수 있다.
- [0112] 이어서, 상기 임의의 단말기(User_k)(20)는 상기 복호화된 데이터블록들(dd_1, ... , dd_n)을 합성하여 실행시킬 수 있다.

[0113] 본 실시예에서, 상기 데이터(data_i)는 원본 영상 데이터를 포함한다고 할 때, 상기 임의의 단말기(User_k)(20)는 상기 복호화된 데이터블록들(dd_1, ..., dd_n)을 통해 상기 원본 영상 데이터와 대응되는 합성 영상 데이터를 형성한 후, HEVC 디코더 프로그램을 통해 영상을 표시할 수 있다.

[0114] 한편, 상기 임의의 단말기(User_k)(20)에서 형성되어 표시되는 상기 합성 영상 데이터의 해상도는 상기 유저 개별 정보들(ui_1, ... , ui_m) 중 상기 유저 입력 정보(ui_input)에 포함된 정보의 개수에 따라 변경될 수 있다.

[0115] 이와 같이 본 실시예에 따르면, 상기 유저 단말기(User_i)(10)에 저장되어 있는 상기 데이터(data_i)가 분산 트랜스코딩되어 상기 데이터노드들(DataNode_1, ..., DataNode_n)(200)에 각각 저장될 때, 상기 유저 정보(ui)에 의해 생성된 상기 복호키(k)를 통해 암호화되어 저장됨에 따라, 상기 데이터노드들(DataNode_1, ..., DataNode_n)(200)을 관리하는 내부 관리자에게 상기 데이터(data_i)가 노출되는 것이 억제될 수 있다.

[0116] 또한, 상기 데이터(data_i)를 전송받기 원하는 사용자가 상기 임의의 단말기(User_k)(20)를 통해 상기 유저 정보(ui)와 대응되는 상기 유저 입력 정보(ui_input)를 입력하면, 상기 비밀 분산 처리부(100)가 상기 유저 입력 정보(ui_input)에 의해 복호화가 가능한지 여부를 판단한 후 상기 입력 복호화(ik)를 생성하고, 상기 데이터노드들(DataNode_1, ..., DataNode_n)(200)은 상기 입력 복호화(ik)를 이용하여 복호하여 상기 임의의 단말기(User_k)(20)로 전송할 수 있다.

[0117] 또한, 상기 유저 정보(ui) 및 상기 유저 입력 정보(ui_input)가 서로 일치하는 정보의 개수가 임계치 t 이상일 경우에만 복호화되도록 설정하여 기밀성을 더욱 향상시킬 수 있다.

[0118] 또한, 상기 유저 정보(ui) 및 상기 유저 입력 정보(ui_input)가 서로 일치하는 정보의 개수가 상기 임계치 t 이상에서 증가될수록 복호화되는 데이터의 질 또는 양, 예를 들어 영상의 해상도가 증가되도록 설정할 수도 있다. 따라서, 암호화되어 분산 저장되어 있는 데이터가 무엇인지 확인만 원하는 사용자는 상기 임계치 t 정도의 정보만 입력함으로써, 완전한 데이터를 복호화하여 확인하지 않고 낮은 질 또는 적은 양의 데이터로 복호화하여 신속히 확인할 수도 있다.

[0119] 앞서 설명한 본 발명의 상세한 설명에서는 본 발명의 바람직한 실시예들을 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자 또는 해당 기술분야에 통상의 지식을 갖는 자라면 후술될 특허청구범위에 기재된 본 발명의 사상 및 기술 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

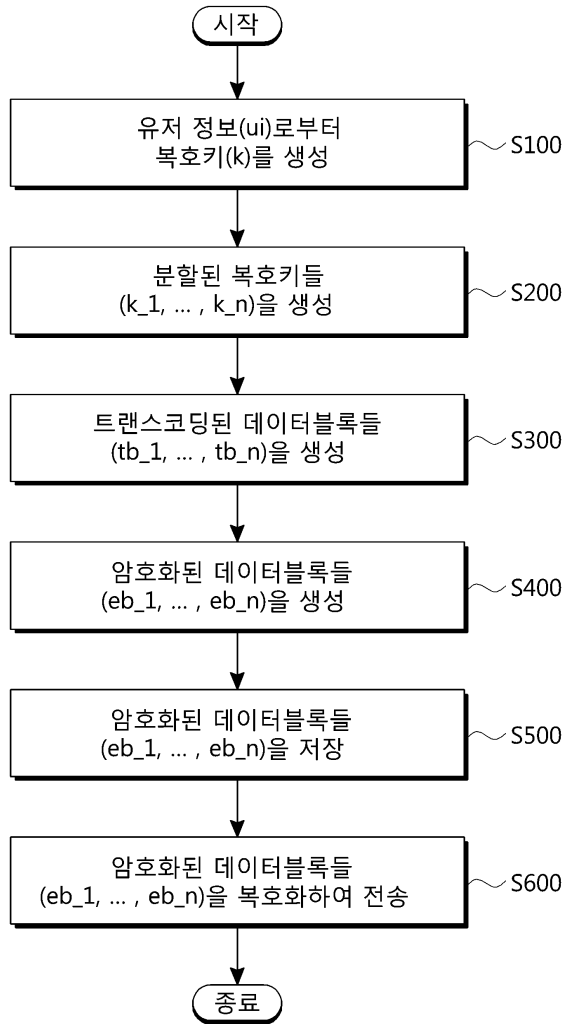
부호의 설명

[0120]

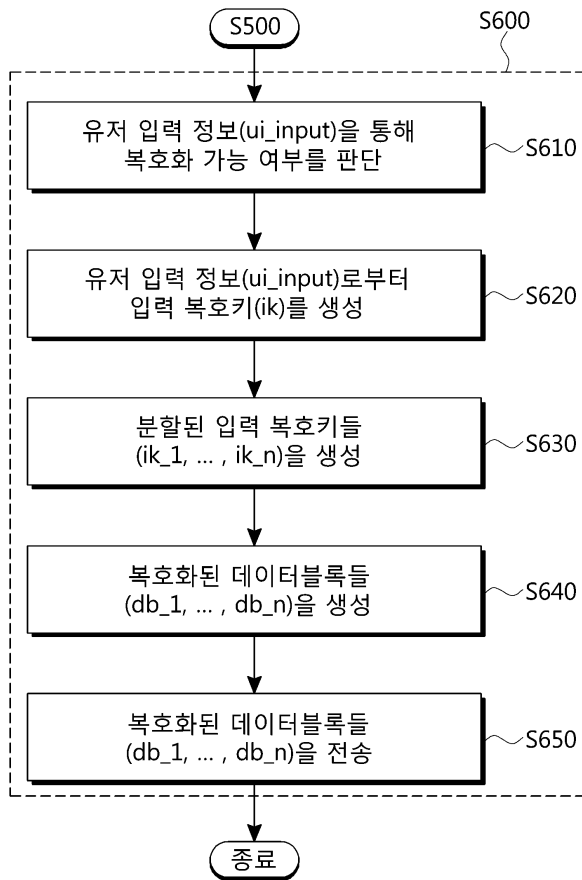
10 : 유저 단말기	20 : 임의의 단말기
100 : 비밀 분산 처리부	200 : 데이터노드
300 : 데이터노드	

도면

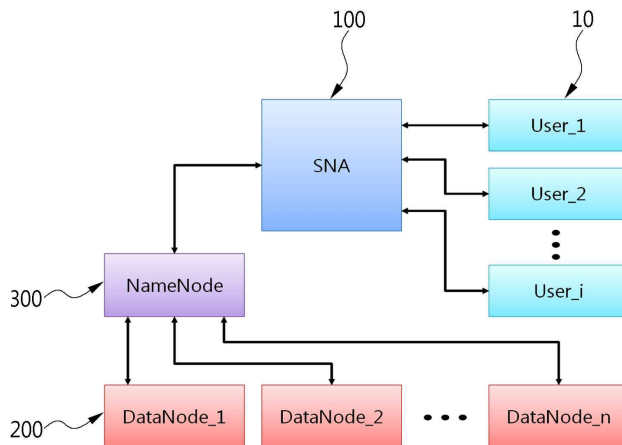
도면1



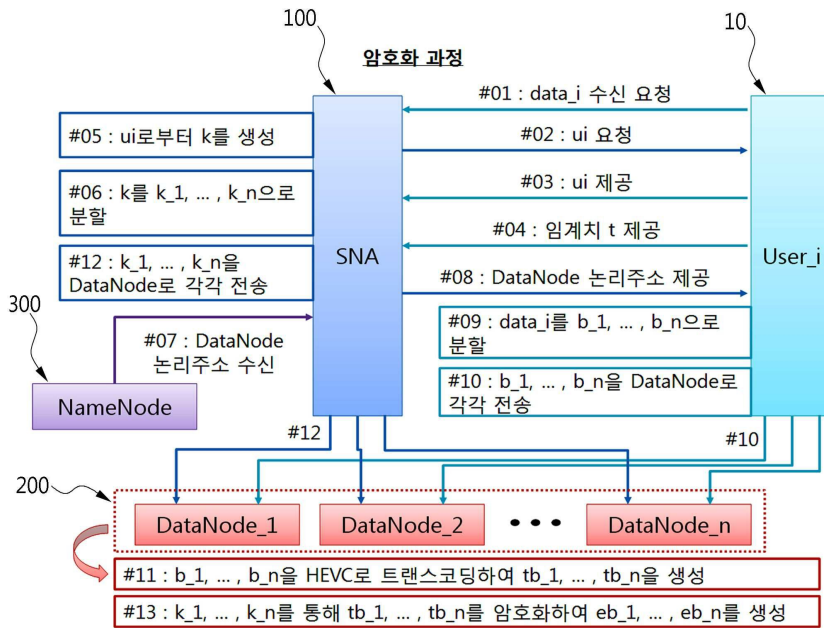
도면2



도면3



도면4



도면5

