



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0034863
(43) 공개일자 2018년04월05일

(51) 국제특허분류(Int. Cl.)
H04N 21/258 (2011.01) G06K 19/06 (2006.01)
H04N 21/2381 (2011.01)
(52) CPC특허분류
H04N 21/25816 (2013.01)
G06K 19/06 (2013.01)
(21) 출원번호 10-2016-0124597
(22) 출원일자 2016년09월28일
심사청구일자 2016년09월28일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호
(더샵센트럴파크2단지아파트)
채기준
서울특별시 강남구 강남대로136길 34
(74) 대리인
윤귀상

전체 청구항 수 : 총 10 항

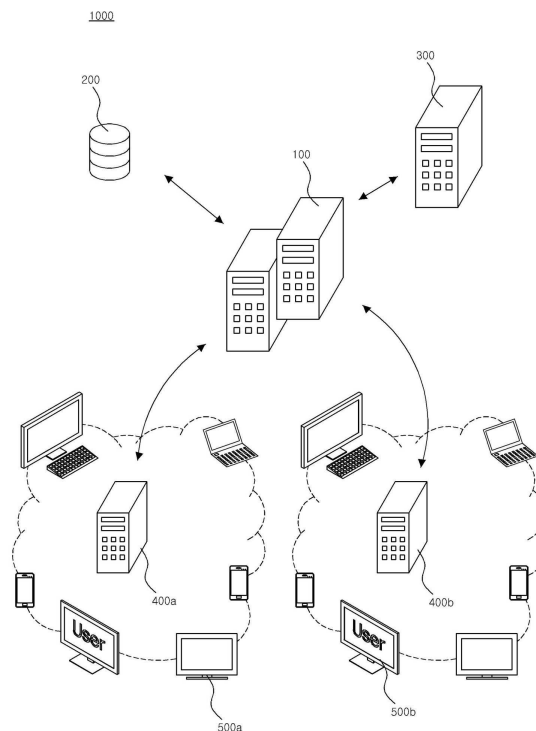
(54) 발명의 명칭 모바일 개방형 IPTV 환경에서 단말 간 통신을 수행하는 사용자 단말의 제어방법 및 사용자 단말 간 상호인증을 위한 정보를 생성하는 인증 서버의 제어방법

(57) 요약

모바일 개방형 IPTV 환경에서 사용자 단말 간의 상호인증을 위한 정보를 생성하는 인증 서버의 제어방법에 있어서, 제1 이미지 및 제2 이미지로 나누어지는 시각암호를 생성하고, 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코드를 삽입한 이미지를 생성하며, 제1 사용자 단말로 상기 제1 이미

(뒷면에 계속)

대표도 - 도1



지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제2 이미지를 전송하고, 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하며, 상기 제1 사용자 단말 및 상기 제2 사용자 단말에서 각각 시각암호에 해당하는 인증코드를 삽입한 이미지에서 인증코드를 식별하여 상기 제1 이미지 및 상기 제2 이미지를 각각 획득하고, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 인증코드를 식별하며, 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드와 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별한 인증코드의 비교 결과에 따른 상호인증 수행 결과를 확인한다.

(52) CPC특허분류

H04N 21/2381 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2012R1A1A3019459

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)-일반연구자지원사업-여성과학자

연구과제명 사물지능통신(M2M)응용분야 보안 연구

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2012.05.01 ~ 2015.04.30

명세서

청구범위

청구항 1

모바일 개방형 IPTV 환경에서 통신을 수행하는 제1 사용자 단말 및 제2 사용자 단말 간의 상호인증을 위한 정보를 생성하는 인증 서버의 제어방법에 있어서,

제1 이미지 및 제2 이미지로 나누어지는 시각암호를 생성하고, 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코드를 삽입한 이미지를 생성하며,

상기 제1 사용자 단말로 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제2 이미지를 전송하고, 상기 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하며,

상기 제1 사용자 단말 및 상기 제2 사용자 단말에서 각각 시각암호에 해당하는 인증코드를 삽입한 이미지에서 인증코드를 식별하여 상기 제1 이미지 및 상기 제2 이미지를 각각 획득하고, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 인증코드를 식별하며, 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드와 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별한 인증코드의 비교 결과에 따른 상호인증 수행 결과를 확인하는 인증 서버의 제어방법.

청구항 2

제1항에 있어서,

미리 정해진 갱신 주기에 따라 동작하는 리키잉 타이머에 따라 상기 시각암호를 갱신하되,

상기 상호인증의 수행 결과에 따라 상기 리키잉 타이머를 제어하는 것을 더 포함하는 인증 서버의 제어방법.

청구항 3

제2항에 있어서,

상기 상호인증의 수행 결과에 따라 상기 리키잉 타이머를 제어하는 것은,

사용자 단말 별로 상호인증 성공률을 나타내는 신용레벨을 부여하고, 상기 제1 사용자 단말과 상기 제2 사용자 단말의 상호인증 수행 결과를 확인한 결과, 상호인증에 실패한 것으로 확인되면, 상기 제1 사용자 단말 및 상기 제2 사용자 단말의 신용레벨이 낮아지도록 수정하며, 수정된 상기 제1 사용자 단말의 신용레벨 또는 수정된 상기 제2 사용자 단말의 신용레벨과 미리 정해진 신용레벨 임계치를 비교하고 그 결과에 따라 상기 리키잉 타이머를 제어하는 것인 인증 서버의 제어방법.

청구항 4

제3항에 있어서,

상기 제1 사용자 단말 및 상기 제2 사용자 단말의 신용레벨이 낮아지도록 수정하는 것은,

상기 제1 사용자 단말과 상기 제2 사용자 단말의 상호인증 수행 결과를 확인한 결과, 상호인증에 실패한 것으로 확인되면, 그 횟수를 카운트하고, 상호인증에 실패한 횟수와 미리 정해진 상호인증 실패 임계치를 비교하는 것을 더 포함하고,

상호인증에 실패한 횟수와 미리 정해진 상호인증 실패 임계치의 비교 결과에 따라 상기 제1 사용자 단말 및 상기 제2 사용자 단말의 신용레벨이 낮아지도록 수정하는 것인 인증 서버의 제어방법.

청구항 5

제1항에 있어서,

상기 제1 사용자 단말로 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와

상기 제2 이미지를 전송하고, 상기 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하는 것은,

상기 제1 이미지에서 상기 제1 사용자 단말 사용자의 개인정보로 이루어지는 등록 정보에 따른 위치에 상기 시각암호에 해당하는 인증코드를 삽입하여 상기 제1 사용자 단말로 전송하고, 상기 제2 이미지에서 상기 제2 사용자 단말 사용자의 개인정보로 이루어지는 등록 정보에 따른 위치에 상기 시각암호에 해당하는 인증코드를 삽입하여 상기 제2 사용자 단말로 전송하는 것인 인증 서버의 제어방법.

청구항 6

제5항에 있어서,

상기 제1 사용자 단말로 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제2 이미지를 전송하고, 상기 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하는 것은,

스테가노그래피 기법으로 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코드를 삽입하여 상기 제1 사용자 단말 및 상기 제2 사용자 단말로 각각 전송하는 것인 인증 서버의 제어방법.

청구항 7

모바일 개방형 IPTV 환경에서 단말 간 통신을 수행하는 사용자 단말의 제어방법에 있어서,

단말 간 상호인증을 위해 제1 이미지 및 제2 이미지의 한 쌍의 이미지로 이루어지는 시각암호를 생성하고, 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코드를 삽입한 이미지를 생성하는 인증 서버로부터, 콘텐츠를 공유할 다른 사용자 단말로 전송되는 제1 이미지와 쌍을 이루는 제2 이미지 및 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지를 수신하며,

상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하며, 상기 제1 이미지 및 상기 제2 이미지를 중첩하여 출력하고,

상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드와 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드를 비교하여 상기 다른 사용자 단말과의 상호인증 성공여부를 판단하는 사용자 단말의 제어방법.

청구항 8

제7항에 있어서,

상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하는 것은,

상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 상기 사용자 단말 사용자의 개인정보로 이루어지는 등록 정보에 따라 상기 시각암호에 해당하는 인증코드가 삽입된 위치를 확인하고, 해당 위치에서 인증코드에 해당하는 비트를 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하는 것인 사용자 단말의 제어방법.

청구항 9

제7항에 있어서,

상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하는 것은,

상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 스테가노그래피 기법으로 삽입된 인증코드를 식별하는 것을 포함하는 사용자 단말의 제어방법.

청구항 10

제7항에 있어서,

상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드와 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드를 비교하여 상기 다른 사용자 단말과의 상호인증 성공여부를 판단하는 것은,

상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드와 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드가 동일하면 상기 다른 사용자 단말과의 상호인증에 성공한 것으로 판단하는 것이며,

상기 다른 사용자 단말과의 상호인증에 성공한 것으로 판단하면, 상기 다른 사용자 단말과의 콘텐츠 공유를 허용하는 것을 더 포함하는 사용자 단말의 제어방법.

발명의 설명

기술 분야

[0001] 본 발명은 모바일 개방형 IPTV 환경에서 단말 간 통신을 수행하여 콘텐츠를 공유하는 사용자 단말의 제어방법 및 사용자 단말 간 통신 시 상호인증을 위한 정보를 생성하는 인증 서버의 제어방법에 관한 것이다.

배경 기술

[0002] IPTV(Internet Protocol Television)는 인터넷과 같은 패킷 교환 네트워크를 통한 인터넷 프로토콜을 이용하여 제공되는 텔레비전 서비스 시스템으로, IP 네트워크에 기반하여 셋탑박스(STB: Set-Top Box)로 방송 및 VoD(Video on Demand) 스트림을 전달한다.

[0003] 최근 이러한 IPTV는 방송과 커뮤니케이션의 통합 및 융합의 기회를 제공한다는 점에서 더욱 각광받고 있는데, 다양한 서비스를 제공하고, 무선 네트워크 및 셋탑박스를 통해 고품질의 멀티미디어 콘텐츠들을 전달함으로써 많은 고객들을 유치하며 빠르게 성장하고 있다.

[0004] 특히, IPTV는 상호작용이 가능한 사용자 맞춤형 서비스를 보장할 수 있는데, 대표적으로, 개방형 IPTV(Open IPTV)는 플랫폼 및 네트워크 자원을 개방하고, API 및 SDK를 모두에게 제공하여, 모든 사용자들이 아무런 제한 없이 콘텐츠를 생성 및 서비스할 수 있다. 또한, 모바일 IPTV(Mobile IPTV)는 유선 또는 무선 네트워크를 통해 서비스를 제공하여 이동성을 보장할 수 있다.

[0005] 이러한 개방형 IPTV 및 모바일 IPTV는 폐쇄된 방송 시스템에 비해 개방 환경에서 서비스를 제공하므로 매우 까다로운 인증 절차가 필요하다. 만약, 인증 절차가 제대로 이루어지지 않는 경우, 지속적인 공격이 이루어지는 DDOS(Distributed Denial of service) 또는 PDOS(Permanent Denial of Service)와 같은 악성 코드에 감염될 수 있다. 따라서, 모바일 개방형 IPTV는 개방성을 가지며, 디바이스의 이동 중에 서비스를 받거나 제공한다는 특징에 맞는 안전하고 경량화된 인증 메커니즘이 필요하다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일측면은 모바일 개방형 IPTV 환경에서 콘텐츠 공유를 위해 사용자 단말 간 통신을 시도하는 경우, 사용자 단말 간 상호인증을 위한 시각암호를 생성하는 인증 서버의 제어방법을 제공한다.

[0007] 본 발명의 다른 측면은 모바일 개방형 IPTV 환경에서 콘텐츠 공유를 위해 다른 사용자 단말과 통신을 시도하는 경우, 인증 서버로부터 수신하는 시각암호를 이용하여 다른 사용자 단말과 상호인증을 수행한 뒤 단말 간 통신을 수행하여 콘텐츠를 공유하는 사용자 단말의 제어방법을 제공한다.

과제의 해결 수단

[0008] 본 발명의 일측면은 모바일 개방형 IPTV 환경에서 통신을 수행하는 제1 사용자 단말 및 제2 사용자 단말 간의 상호인증을 위한 정보를 생성하는 인증 서버의 제어방법에 있어서, 제1 이미지 및 제2 이미지로 나누어지는 시각암호를 생성하고, 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코

드를 삽입한 이미지를 생성하며, 상기 제1 사용자 단말로 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제2 이미지를 전송하고, 상기 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하며, 상기 제1 사용자 단말 및 상기 제2 사용자 단말에서 각각 시각암호에 해당하는 인증코드를 삽입한 이미지에서 인증코드를 식별하여 상기 제1 이미지 및 상기 제2 이미지를 각각 획득하고, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 인증코드를 식별하며, 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드와 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별한 인증코드의 비교 결과에 따른 상호인증 수행 결과를 확인한다.

[0009] 한편, 미리 정해진 갱신 주기에 따라 동작하는 리키잉 타이머에 따라 상기 시각암호를 갱신하되, 상기 상호인증의 수행 결과에 따라 상기 리키잉 타이머를 제어하는 것을 더 포함할 수 있다. 또한, 상기 상호인증의 수행 결과에 따라 상기 리키잉 타이머를 제어하는 것은, 사용자 단말 별로 상호인증 성공률을 나타내는 신용레벨을 부여하고, 상기 제1 사용자 단말과 상기 제2 사용자 단말의 상호인증 수행 결과를 확인한 결과, 상호인증에 실패한 것으로 확인되면, 상기 제1 사용자 단말 및 상기 제2 사용자 단말의 신용레벨이 낮아지도록 수정하며, 수정된 상기 제1 사용자 단말의 신용레벨 또는 수정된 상기 제2 사용자 단말의 신용레벨과 미리 정해진 신용레벨 임계치를 비교하고 그 결과에 따라 상기 리키잉 타이머를 제어하는 것일 수 있다.

[0010] 또한, 상기 제1 사용자 단말 및 상기 제2 사용자 단말의 신용레벨이 낮아지도록 수정하는 것은, 상기 제1 사용자 단말과 상기 제2 사용자 단말의 상호인증 수행 결과를 확인한 결과, 상호인증에 실패한 것으로 확인되면, 그 횟수를 카운트하고, 상호인증에 실패한 횟수와 미리 정해진 상호인증 실패 임계치를 비교하는 것을 더 포함하고, 상호인증에 실패한 횟수와 미리 정해진 상호인증 실패 임계치의 비교 결과에 따라 상기 제1 사용자 단말 및 상기 제2 사용자 단말의 신용레벨이 낮아지도록 수정하는 것일 수 있다. 또한, 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제2 이미지를 전송하고, 상기 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하는 것은, 상기 제1 이미지에서 상기 제1 사용자 단말 사용자의 개인정보로 이루어지는 등록 정보에 따른 위치에 상기 시각암호에 해당하는 인증코드를 삽입하여 상기 제1 사용자 단말로 전송하고, 상기 제2 이미지에서 상기 제2 사용자 단말 사용자의 개인정보로 이루어지는 등록 정보에 따른 위치에 상기 시각암호에 해당하는 인증코드를 삽입하여 상기 제2 사용자 단말로 전송하는 것일 수 있다.

[0011] 또한, 상기 제1 사용자 단말로 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제2 이미지를 전송하고, 상기 제2 사용자 단말로 상기 제2 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지와 상기 제1 이미지를 전송하는 것은, 스테가노그래피 기법으로 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코드를 삽입하여 상기 제1 사용자 단말 및 상기 제2 사용자 단말로 각각 전송하는 것일 수 있다.

[0012] 한편, 본 발명의 다른 측면은 모바일 개방형 IPTV 환경에서 단말 간 통신을 수행하는 사용자 단말의 제어방법에 있어서, 단말 간 상호인증을 위해 제1 이미지 및 제2 이미지의 한 쌍의 이미지로 이루어지는 시각암호를 생성하고, 상기 제1 이미지 및 상기 제2 이미지의 특정 위치에 각각 상기 시각암호에 해당하는 인증코드를 삽입한 이미지를 생성하는 인증 서버로부터, 콘텐츠를 공유할 다른 사용자 단말로 전송되는 제1 이미지와 쌍을 이루는 제2 이미지 및 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지를 수신하며, 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하며, 상기 제1 이미지 및 상기 제2 이미지를 중첩하여 출력하고, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드와 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별한 인증코드를 비교하여 상기 다른 사용자 단말과의 상호인증 성공여부를 판단한다.

[0013] 한편, 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하는 것은, 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 상기 사용자 단말 사용자의 개인정보로 이루어지는 등록 정보에 따라 상기 시각암호에 해당하는 인증코드가 삽입된 위치를 확인하고, 해당 위치에서 인증코드에 해당하는 비트를 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하는 것일 수 있다.

[0014] 또한, 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해

당하는 부분을 추출하여 삽입된 인증코드를 식별하고 인증코드가 삽입되기 전의 상기 제1 이미지를 획득하는 것은, 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 특정 위치에 해당하는 부분을 추출하여 스테가노그래피 기법으로 삽입된 인증코드를 식별하는 것을 포함할 수 있다.

[0015] 또한, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드와 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별된 인증코드를 비교하여 상기 다른 사용자 단말과의 상호인증 성공여부를 판단하는 것은, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드와 상기 제1 이미지의 특정 위치에 상기 시각암호에 해당하는 인증코드를 삽입한 이미지에서 식별된 인증코드가 동일하면 상기 다른 사용자 단말과의 상호인증에 성공한 것으로 판단하는 것이며, 상기 다른 사용자 단말과의 상호인증에 성공한 것으로 판단하면, 상기 다른 사용자 단말과의 콘텐츠 공유를 허용하는 것을 더 포함할 수 있다.

발명의 효과

[0016] 상술한 본 발명의 일 측면에 따르면 한 쌍의 이미지로 이루어지는 시각암호에 기반하여 콘텐츠를 송수신하고자 하는 사용자 단말간 상호인증을 수행함으로써, 내부 또는 외부의 공격으로부터 안전하고, 상호인증에 필요한 연산을 최소화하여 경량화된 사용자 단말간의 상호인증이 가능하다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템의 구성을 개략적으로 도시한 블록도이다.
 도 2는 도 1에 도시된 모바일 개방형 IPTV 시스템의 사용자 단말 등록 단계를 도시한 플로우차트이다.
 도 3은 도 1에 도시된 모바일 개방형 IPTV 시스템의 단말 간 통신을 위한 단말 간 상호인증 단계를 도시한 플로우차트이다.
 도 4는 도 1에 도시된 중앙 제어 서버의 제어 블록도이다.
 도 5는 도 1에 도시된 인증 서버의 제어 블록도이다.
 도 6 및 도 7은 인증 서버에서 시각암호를 생성하는 방법을 설명하기 위한 도면이다.
 도 8 및 도 9는 도 5에 도시된 인증 서버의 제어방법을 설명하기 위한 순서도이다.
 도 10은 도 1에 도시된 사용자 단말의 제어 블록도이다.
 도 11은 사용자 단말에서 상호인증을 수행하는 방법을 설명하기 위한 도면이다.
 도 12는 도 10에 도시된 사용자 단말의 제어방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0019] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0020] 도 1은 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템의 구성을 개략적으로 도시한 블록도이다.

[0021] 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템(1000)은 복수의 사용자 단말(500) 간에 직접 콘텐츠를 송수신하는 방식으로 IPTV 서비스를 제공하는 시스템으로, 이때, 보안을 위해 콘텐츠를 송수신하는 사용자 단말(500) 간의 상호인증을 지원할 수 있다. 이를 위해, 도 1을 참조하면, 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템(1000)은 중앙 제어 서버(100), 사용자 DB(200), 인증 서버(300), 복수의 로컬 제어 서버(400a,

400b) 및 복수의 사용자 단말(500a, 500b)을 포함하여 구성될 수 있다.

- [0022] 구체적으로는, 중앙 제어 서버(100)는 사용자 DB(200) 및 인증 서버(300)와 네트워크로 연결될 수 있다. 또한, 복수의 로컬 제어 서버(400a, 400b)와 네트워크로 연결되어 복수의 로컬 제어 서버(400a, 400b)를 통해 복수의 사용자 단말(500a, 500b)과 소정의 정보를 송수신할 수 있다.
- [0023] 중앙 제어 서버(100)는 복수의 사용자 단말(500a, 500b)의 정보 및 복수의 사용자 단말(500a, 500b)에서 각각 생성하는 콘텐츠 리스트를 사용자 DB(200)에 저장하여 관리할 수 있으며, 제1 사용자 단말(500a)로부터 특정 콘텐츠 제공 요청 신호를 수신하는 경우, 해당 콘텐츠를 제공할 수 있는 제2 사용자 단말(500b)과 제1 사용자 단말(500a)간의 상호인증이 수행되도록 제어할 수 있다.
- [0024] 인증 서버(300)는 중앙 제어 서버(100)의 요청에 응답하여 단말 간 상호인증을 위한 정보를 생성하는데, 상호인증을 위한 정보는 한 쌍의 이미지로 이루어지는 시각암호(Visual Cryptography)일 수 있으며, 이때, 각 이미지에 시각암호에 해당하는 인증코드와 동일한 인증코드를 스테가노그래피(Steganography) 기법으로 삽입하여 상호인증을 수행할 각 단말로 전송할 수 있다. 인증 서버(300)는 또한 상호인증 결과에 따라 시각암호를 갱신할 수 있다.
- [0025] 한편, 복수의 로컬 제어 서버(400a, 400b)는 각각 하나의 홈 네트워크에 연결되는 복수의 사용자 단말(500a, 500b)을 관리할 수 있으며, 복수의 사용자 단말(500)은 이러한 로컬 제어 서버(400)를 통해 중앙 제어 서버(100)와 연결될 수 있다. 이때, 동일한 로컬 제어 서버(400a)에 의해 관리되는 사용자 단말(500a), 즉, 동일한 홈 네트워크에 접속된 사용자 단말(500a) 간에 콘텐츠를 공유하는 경우에는 상호인증 단계를 생략하여도 무방하다.
- [0026] 사용자 단말(500)은 통신이 가능하고, 정보의 입출력이 가능하고, 휴대가 가능한 단말기로서 다양한 형태로 구현될 수 있으며, 예를 들면, 스마트폰, 태블릿 pc 등으로 구현될 수 있다. 특히, 사용자 단말(500)은 콘텐츠의 생성 및 배포가 가능하고, 이동 중에 다른 사용자 단말(500)로부터 콘텐츠를 수신하여 출력할 수 있다.
- [0027] 이와 같은, 도 1에 도시된 모바일 개방형 IPTV 시스템(1000)에 따른 IPTV 서비스 방식에 대하여 도 2 및 도 3을 참조하여 구체적으로 설명하기로 한다.
- [0028] 도 2는 도 1에 도시된 모바일 개방형 IPTV 시스템의 사용자 단말 등록 단계를 도시한 플로우차트이고, 도 3은 도 1에 도시된 모바일 개방형 IPTV 시스템의 단말 간 통신을 위한 단말 간 상호인증 단계를 도시한 플로우차트이다.
- [0029] 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템은 IPTV 서비스에 가입한 사용자 단말(500) 간에 직접 통신하여 콘텐츠를 공유하는 시스템으로, 이를 위한 각 사용자 단말(500)에서 제공 가능한 콘텐츠를 등록 및 관리하는 사용자 단말 등록 단계와 콘텐츠 공유를 위해 단말 간 통신을 요청하는 경우 단말 간 상호인증을 수행하는 상호인증 단계를 포함할 수 있다.
- [0030] 먼저, 도 2를 참조하면, 사용자 단말(500)은 로컬 제어 서버(400)로 IPTV 서비스 등록을 요청할 수 있다. 예를 들면, 사용자 단말(500)은 아이디 및 패스워드와 같은 개인 정보로 이루어지는 등록 정보를 로컬 제어 서버(400)로 전송할 수 있다.
- [0031] 로컬 제어 서버(400)는 사용자 단말(500)의 등록 정보를 중앙 제어 서버(100)로 전달할 수 있으며, 중앙 제어 서버(100)는 사용자 DB(200)에 사용자 단말(500)의 등록 정보, 예를 들면, 해당 사용자 단말(500)의 아이디 및 패스워드를 저장할 수 있다.
- [0032] 그리고, 중앙 제어 서버(100)는 사용자 단말(500)로 해당 단말에서 제공 가능한 콘텐츠 리스트를 요청할 수 있다. 이때, 중앙 제어 서버(100)는 로컬 제어 서버(400)를 통해 사용자 단말(500)로 콘텐츠 리스트를 요청할 수 있다.
- [0033] 사용자 단말(500)은 다른 단말로 제공할 수 있는 콘텐츠 리스트, 즉, 해당 단말에서 생성하는 콘텐츠 리스트를 중앙 제어 서버(100)로 전송할 수 있으며, 중앙 제어 서버(100)는 사용자 단말(500)로부터 수신하는 콘텐츠 리스트를 사용자 DB(200)에 해당 사용자 단말(500)의 등록 정보와 매칭하여 저장할 수 있다.
- [0034] 중앙 제어 서버(100)는 이와 같은 방식으로 복수의 사용자 단말(500)로부터 수신하는 콘텐츠 리스트를 취합하여 사용자 DB(200)에 등록된 모든 사용자 단말(500)로 배포할 수 있다.
- [0035] 사용자 단말(500)은 중앙 제어 서버(100)로부터 수신하는 콘텐츠 리스트 중 사용자로부터 특정 콘텐츠를 선택

받으면, 중앙 제어 서버(100)로 해당 콘텐츠의 수신을 요청할 수 있다.

- [0036] 중앙 제어 서버(100)는 사용자 단말(500)로부터 특정 콘텐츠 수신을 요청받으면, 사용자 DB(200)에서 해당 콘텐츠를 제공하는 사용자 단말(500)을 검색할 수 있으며, 검색 결과에 따라 해당 콘텐츠를 제공하는 사용자 단말(500)로 해당 콘텐츠의 제공을 요청 받았음을 알릴 수 있다.
- [0037] 그리고, 중앙 제어 서버(100)는 특정 콘텐츠의 수신을 요청한 사용자 단말, 이하, 제1 사용자 단말(500a)과 해당 콘텐츠를 제공하는 사용자 단말, 이하, 제2 사용자 단말(500b) 간에 상호인증단계를 진행할 수 있다. 이와 관련하여, 도 3을 참조하여 설명하기로 한다.
- [0038] 도 3을 참조하면, 중앙 제어 서버(100)는 인증 서버(300)로 제1 사용자 단말(500a) 및 제2 사용자 단말(500b) 간의 상호인증을 위한 시각 암호를 요청할 수 있다. 이때, 중앙 제어 서버(100)는 인증 서버(300)로 제1 사용자 단말(500a) 및 제2 사용자 단말(500b) 각각의 등록 정보와 함께 시각 암호를 요청할 수 있다. 또는, 인증 서버(300)에서 사용자 DB(200)에 접속하여 제1 사용자 단말(500a) 및 제2 사용자 단말(500b) 각각의 등록 정보를 획득할 수 있다.
- [0039] 인증 서버(300)는 중앙 제어 서버(100)의 요청에 응답하여 한 쌍의 이미지로 이루어지는 시각 암호를 생성할 수 있다. 즉, 인증 서버(300)는 제1 이미지 및 제2 이미지로 이루어지는 시각 암호를 생성할 수 있다. 이때, 제1 이미지 및 제2 이미지가 중첩되면 시각 암호에 해당하는 인증코드의 식별이 가능하다.
- [0040] 그리고, 인증 서버(300)는 제1 이미지에 제1 인증코드가 삽입된 이미지 및 제2 이미지에 제2 인증코드가 삽입된 이미지를 생성할 수 있다. 인증 서버(300)는 제1 이미지에서 제1 사용자 단말(500a)의 등록 정보에 따른 위치에 스테가노그래피 기법으로 제1 인증코드를 삽입하고, 제2 이미지에서 제2 사용자 단말(500b)의 등록 정보에 따른 위치에 스테가노그래피 기법으로 제2 인증코드를 삽입할 수 있다. 이때, 제1 인증코드 및 제2 인증코드는 제1 이미지와 제2 이미지가 중첩되는 경우 식별 가능한 인증코드와 동일하다.
- [0041] 인증 서버(300)는 시각 암호를 구성하는 제1 이미지 및 제2 이미지와, 제1 이미지에 제1 인증코드가 삽입된 이미지 및 제2 이미지에 제2 인증코드가 삽입된 이미지를 모두 중앙 제어 서버(100)로 전송할 수 있다.
- [0042] 중앙 제어 서버(100)는 제1 사용자 단말(500a)로 제1 이미지에 제1 인증코드가 삽입된 이미지 및 제2 이미지를 전송하고, 제2 사용자 단말(500b)로 제2 이미지에 제2 인증코드가 삽입된 이미지 및 제1 이미지를 전송할 수 있다. 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)은 중앙 제어 서버(100)로부터 각각 제1 이미지에 제1 인증코드가 삽입된 이미지 및 제2 이미지에 제2 인증코드가 삽입된 이미지를 수신하면, 각각 자신의 등록 정보에 따른 위치에 삽입된 제1 인증코드 및 제2 인증코드를 인식할 수 있으며, 해당 정보를 저장할 수 있다. 이때, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)은 각각 제1 인증코드 또는 제2 인증코드를 추출한 제1 이미지 및 제2 이미지를 획득할 수 있다. 그리고, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)은 각각 제1 이미지와 제2 이미지를 중첩시켜 출력할 수 있다. 이와 같은 경우, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)의 사용자는 각각 제1 이미지와 제2 이미지의 중첩된 이미지로부터 특정 인증코드를 시각적으로 식별할 수 있으며, 식별된 인증코드가 각각 제1 인증코드 및 제2 인증코드와 일치하는지를 판단하고 그 결과를 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)로 입력할 수 있다. 또는, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)의 사용자는 식별되는 인증코드를 그대로 입력하고, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)에서 입력 받은 인증코드가 각각 제1 인증코드 및 제2 인증코드와 일치하는지를 판단할 수 있다.
- [0043] 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)은 각각 제1 이미지와 제2 이미지의 중첩된 이미지에서 식별되는 인증코드를 각각 제1 인증코드 및 제2 인증코드와 비교하여 상호인증 성공여부를 판단할 수 있다. 즉, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)에서 제1 이미지와 제2 이미지의 중첩된 이미지에서 식별되는 인증코드가 각각 제1 인증코드 및 제2 인증코드와 동일한 것으로 판단되면, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b) 간에 상호인증이 성공한 것으로 간주할 수 있으며, 이와 같은 경우, 제1 사용자 단말(500a)은 제2 사용자 단말(500b)로부터 콘텐츠를 수신하여 출력할 수 있다.
- [0044] 한편, 인증 서버(300)는 미리 정해진 알고리즘에 따라 시각암호를 갱신할 수 있다. 이때, 다양한 이유로 의도적으로 상호인증에 실패하는 사용자들이 존재하는데, 이에 인증 서버(300)는 사용자 단말(500) 별로 신용레벨을 부여하고, 상호인증에 실패할 때마다 신용레벨을 수정함과 동시에 시각암호의 갱신 주기를 조정하는 방식으로 시각암호를 갱신할 수 있다. 이와 관련하여 구체적인 설명은 후술하기로 한다.
- [0045] 이와 같이, 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템(1000)은 개방된 환경에서 사용자 단말(500) 간의 통신이 이루어지므로 사용자 단말(500) 간의 상호 인증이 중요하며, 사용자 단말(500)의 에너지 소비 측면

에서 연산량을 최소화하는 것이 중요한데, 한 쌍의 이미지로 이루어지는 시각암호에 기반하여 콘텐츠를 송수신하고자 하는 사용자 단말(500)간 상호인증을 수행함으로써, 내부 또는 외부의 공격으로부터 안전하고, 연산을 최소화하여 경량화된 사용자 단말(500)간의 상호인증이 가능하다.

- [0046] 이하에서는, 도 4 내지 도 11을 참조하여 도 1에 도시된 모바일 개방형 IPTV 시스템(1000)에 포함되는 각 구성 요소에 대하여 구체적으로 설명하기로 한다.
- [0047] 먼저, 도 4는 도 1에 도시된 중앙 제어 서버의 제어 블록도이다.
- [0048] 도 4를 참조하면, 중앙 제어 서버(100)는 중앙 제어 서버 통신부(110), 중앙 제어 서버 제어부(120) 및 중앙 제어 서버 메모리부(130)를 포함하여 구성될 수 있으며, IPTV 서비스에 가입된 사용자들을 관리하고, 사용자 단말(500)간의 통신이 이루어질 수 있도록 일련의 단계를 제어할 수 있다. 이러한 중앙 제어 서버(100)는 도 4에 도시된 구성요소보다 많은 구성요소에 의해 구현될 수 있다. 이하, 상술한 구성요소들에 대해 구체적으로 설명하기로 한다.
- [0049] 중앙 제어 서버 통신부(110)는 중앙 제어 서버(100)와 로컬 제어 서버(400) 또는 인증 서버(300) 간의 통신을 가능하게 하고, 사용자 DB(200)로의 접속을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다.
- [0050] 중앙 제어 서버 통신부(110)는 로컬 제어 서버(400)를 통해 사용자 단말(500)로부터 IPTV 서비스 가입 요청 신호 또는 다른 단말로 제공할 수 있는 콘텐츠 리스트를 수신하거나, 사용자 단말(500)로 다른 단말로부터 수신할 수 있는 콘텐츠 리스트를 전송하거나, 상호인증을 위한 정보를 전송할 수 있다. 이때, 중앙 제어 서버 통신부(110)는 로컬 제어 서버(400)를 거치지 않고 바로 사용자 단말(500)과 통신할 수 있다. 또한, 중앙 제어 서버 통신부(110)는 인증 서버(300)로 단말 간 상호인증을 위한 시각암호 생성 요청 신호를 송신하거나, 인증 서버(300)로부터 시각암호를 수신할 수 있다.
- [0051] 중앙 제어 서버 제어부(120)는 중앙 제어 서버(100)의 전반적인 동작을 제어할 수 있다. 특히, 중앙 제어 서버 제어부(120)는 IPTV 서비스에 가입한 사용자 단말(500)들의 정보를 관리하고, 콘텐츠를 송수신할 사용자 단말(500) 간의 통신이 이루어지도록 제어할 수 있다. 이를 위해, 중앙 제어 서버 제어부(120)는 콘텐츠 리스트 취합부(121), 콘텐츠 제공 단말 검색부(122) 및 시각암호생성 요청부(123)를 포함할 수 있다.
- [0052] 콘텐츠 리스트 취합부(121)는 사용자 단말(500)로부터 IPTV 서비스 가입 요청 신호를 수신하면, 해당 사용자 단말(500)의 등록 정보를 사용자 DB(200)에 저장하고, 해당 사용자 단말(500)에서 다른 단말로 제공 가능한 콘텐츠 리스트를 요청할 수 있다. 이때, 사용자 단말(500)의 등록 정보에는 사용자의 ID 및 패스워드 등의 사용자 개인 정보를 포함할 수 있다.
- [0053] 콘텐츠 리스트 취합부(121)는 사용자 단말(500)로부터 다른 단말로 제공 가능한 콘텐츠 리스트를 수신하면, 사용자 DB(200)에 접속하여 해당 사용자 단말(500)의 등록 정보와 해당 사용자 단말(500)로부터 수신한 콘텐츠 리스트를 매칭하여 저장할 수 있다.
- [0054] 콘텐츠 리스트 취합부(121)는 이와 같은 방식으로 IPTV 서비스에 가입한 복수의 사용자 단말(500)로부터 각각 콘텐츠 리스트를 수신하고 사용자 DB(200)에 저장하며, 이를 취합하여 IPTV 서비스에서 제공 가능한 콘텐츠 리스트를 생성하고, IPTV 서비스에 가입한 모든 사용자 단말(500)로 전송할 수 있다.
- [0055] 이와 같은 경우, 사용자 단말(500)은 중앙 제어 서버(100)로부터 수신한 콘텐츠 리스트를 출력하며, 사용자로부터 콘텐츠 리스트 중 특정 콘텐츠를 선택 받고 해당 정보를 중앙 제어 서버(100)로 전송할 수 있다.
- [0056] 콘텐츠 제공 단말 검색부(122)는 사용자 단말(500)로부터 특정 콘텐츠의 수신 요청 신호를 수신하면, 해당 콘텐츠를 제공하는 사용자 단말(500)을 검색할 수 있다. 콘텐츠 제공 단말 검색부(122)는 사용자 DB(200)에 접속하여 해당 콘텐츠의 제공이 가능한 사용자 단말(500)을 검색하고, 해당 사용자 단말(500)로 콘텐츠의 전송 요청이 있음을 알릴 수 있다. 예를 들면, 콘텐츠 제공 단말 검색부(122)는 콘텐츠를 제공할 사용자 단말(500)로 해당 콘텐츠 정보와 해당 콘텐츠를 요청한 사용자 단말(500)의 정보를 전송할 수 있다.
- [0057] 시각암호생성 요청부(123)는 단말 간 통신을 요청한 사용자 단말(500)의 상호인증을 위한 시각암호생성 요청 신호를 생성하여 인증 서버(300)로 전송할 수 있다. 예를 들면, 시각암호생성 요청부(123)는 제1 사용자 단말(500a)로부터 특정 콘텐츠의 수신 요청 신호를 수신하면, 사용자 DB(200)에 접속하여, 해당 콘텐츠를 송신할 수 있는 제2 사용자 단말(500b)을 검색할 수 있다. 그리고, 시각암호생성 요청부(123)는 제1 사용자 단말(500a)과 제2 사용자 단말(500b) 간의 콘텐츠 송수신을 위한 통신 수행 시 보안을 강화하기 위해 상호인증을 수행할 수

있도록, 인증 서버(300)로 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)의 정보와 함께 상호인증을 위한 시각암호생성 요청 신호를 생성하여 인증 서버(300)로 전송할 수 있다.

- [0058] 중앙 제어 서버 메모리부(130)는 중앙 제어 서버(100)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다.
- [0059] 한편, 사용자 DB(200)는 데이터 저장장치로, 특히, 중앙 제어 서버(100)로부터 전송되는 IPTV 서비스에 가입한 사용자 단말(500)의 등록 정보를 저장하고, 등록된 사용자 단말 별로 제공 가능한 콘텐츠 리스트를 저장할 수 있다. 이러한 사용자 DB(200)에 저장된 정보는 중앙 제어 서버(100) 및 인증 서버(300)에서 접속하여 열람 가능하다.
- [0060] 또한, 로컬 제어 서버(400)는 상술한 바와 같이 홈 네트워크를 관리하는 일반적인 형태의 제어 서버로, 특히, 홈 네트워크에 연결되는 사용자 단말(500)과 중앙 제어 서버(100) 간의 중계 서버 역할을 수행할 수 있다.
- [0061] 한편, 도 5는 도 1에 도시된 인증 서버의 제어 블록도이고, 도 6 및 도 7은 인증 서버에서 시각암호를 생성하는 방법을 설명하기 위한 도면이다.
- [0062] 도 5를 참조하면, 인증 서버(300)는 인증 서버 통신부(310), 인증 서버 제어부(320)를 및 인증 서버 메모리부(330)를 포함하여 구성될 수 있으며, 중앙 제어 서버(100)의 요청에 응답하여 사용자 단말(500)간 인증을 위한 시각암호를 생성할 수 있다. 이러한 인증 서버(300)는 도 5에 도시된 구성요소보다 많은 구성요소에 의해 구현될 수 있고, 그보다 적은 구성요소에 의해 구현될 수 있다. 이하, 상술한 구성요소들에 대해 구체적으로 설명하기로 한다.
- [0063] 인증 서버 통신부(310)는 인증 서버(300)와 중앙 제어 서버(100) 간의 통신을 가능하게 하고, 사용자 DB(200)로의 접속을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다.
- [0064] 인증 서버 통신부(310)는 중앙 제어 서버(100)로부터 사용자 단말(500)간 인증을 위한 시각암호의 생성 요청 신호를 수신하거나, 중앙 제어 서버(100)로 시각암호의 생성 요청 신호에 응답하여 생성한 시각암호를 전송할 수 있다. 또한, 인증 서버 통신부(310)는 사용자 DB(200)에 접속을 가능하게 하며, 상호인증을 수행한 사용자 단말(500)로부터 상호인증 성공여부와 관련된 정보를 수신할 수 있다.
- [0065] 인증 서버 제어부(320)는 인증 서버(300)의 전반적인 동작을 제어할 수 있다. 특히, 인증 서버 제어부(320)는 사용자 단말(500) 간의 상호인증을 위한 시각암호를 생성할 수 있으며, 사용자 단말(500) 간의 상호인증 성공여부에 따라 시각암호를 갱신할 수 있다. 이를 위해, 인증 서버 제어부(320)는 시각암호 생성부(321) 및 시각암호 갱신부(322)를 포함할 수 있다.
- [0066] 시각암호 생성부(321)는 중앙 제어 서버(100)로부터 수신하는 시각암호 생성 요청 신호에 응답하여 시각암호를 생성할 수 있다. 이때, 중앙 제어 서버(100)로부터 수신하는 시각암호 생성 요청 신호에는, 상호인증이 필요한 두 사용자 단말(500)에 대한 정보가 포함될 수 있다.
- [0067] 시각암호 생성부(321)는 제1 이미지 및 제2 이미지로 이루어지는 시각암호를 생성하는데, 제1 이미지 및 제2 이미지가 중첩되는 경우, 육안으로 시각암호의 식별이 가능하다. 이때, 시각암호는 예를 들면 4자리 숫자 형태의 인증코드를 포함하는 이미지일 수 있다.
- [0068] 구체적으로는, 시각암호는 사람의 시각에 의해 관독될 수 있는 인증코드로, 이에 따라 암호화 또는 복호화 시 복잡한 계산이 필요없다는 장점을 가져 사용자 단말(500)과 같이 에너지 사용에 제한이 있는 단말에서의 인증 알고리즘으로 사용되기 적합하다.
- [0069] 시각암호는 두 개의 이미지로 나누어지는데, 각 이미지는 시각암호를 나타내는 픽셀들의 서브픽셀들로 이루어지며, 이에 두 개의 이미지를 중첩시키면 시각암호에 해당하는 인증코드의 식별이 가능하다. 반면, 각 이미지만으로는 시각암호의 관독이 불가능하다.
- [0070] 예를 들어, 도 6을 참조하면, RCode의 검정 픽셀은 서로 반전되는 서브 픽셀로 이루어지는 두 개의 이미지로 나누어질 수 있으며, 서로 반전되는 서브 픽셀로 이루어지는 두 개의 이미지가 중첩되면 검정 픽셀로 보여질 수 있다. 또는, RCode의 흰색 픽셀은 동일한 서브 픽셀로 이루어지는 두 개의 이미지로 나누어질 수 있으며, 동일한 서브 픽셀로 이루어지는 두 개의 이미지가 중첩되면 밝은 회색으로 보여질 수 있다.
- [0071] 시각암호 생성부(321)는 이와 같이 두 개의 이미지로 나누어지는 시각암호를 생성할 수 있다. 그리고, 시각암호

생성부(321)는 시각암호를 구성하는 두 개의 이미지에서 각각 상호인증을 수행하고자 하는 두 사용자 단말(500)의 등록 정보에 따른 위치에 스테가노그래피 기법을 적용하여 인증코드를 삽입한 이미지를 생성할 수 있다.

[0072] 구체적으로는, 시각암호 생성부(321)는 시각암호를 구성하는 제1 이미지 및 제2 이미지를 생성하면, 제1 이미지 및 제2 이미지에 스테가노그래피 기법을 이용하여 시각암호에 해당하는 인증코드를 삽입한 이미지를 생성할 수 있다. 이때, 인증코드의 삽입 위치는 상호인증을 수행하고자 하는 두 사용자 단말(500)의 등록 정보에 따라 정해질 수 있다. 이를 위해, 시각암호 생성부(321)는 사용자 DB(200)에 접속하여, 중앙 제어 서버(100)로부터 수신하는 시각암호 생성 요청 신호에 포함되는 상호인증이 필요한 두 사용자 단말(500)의 등록 정보를 확인할 수 있으며, 두 사용자 단말(500) 각각의 등록 정보를 이용하는 미리 정해진 소정의 알고리즘에 따라 제1 이미지 및 제2 이미지에서 각각 인증코드를 삽입할 위치를 설정하고, 해당 위치에 스테가노그래피 기법을 이용하여 시각암호에 해당하는 인증코드를 삽입할 수 있다.

[0073] 예를 들면, 시각암호 생성부(321)는 제1 이미지 및 제2 이미지의 가로 길이가 'l'이고, 세로 길이가 'h'이면, 아래의 알고리즘에 따라 제1 이미지 및 제2 이미지에서 각각 인증코드를 삽입할 위치를 설정하고, 해당 위치에 스테가노그래피 기법이 적용된 인증코드에 해당하는 비트를 생성하여 삽입할 수 있다.

```
x = id ⊕ pw; // 사용자의 id, password
if(x > l) location = x mod l;
else if(x < l) location = l mod x;
location 위치에 해당하는 위치에 세로로 h 비트를 생성하여 insert
h = 인증코드비트 || pad (길이가 부족한 경우 padding 추가)
```

[0074]

[0075] 스테가노그래피 기법은 파일, 메시지, 이미지 또는 비디오를 또 다른 파일, 메시지, 이미지 또는 비디오에 숨기는 기법으로, 일반적으로 노이즈 이미지들 또는 사운드 파일의 최하위 비트 안에 메시지를 숨기는 데 널리 사용되고 있다. 예를 들면, 도 7을 참조하면, 스테가노그래피 기법으로 다크 그린 이미지에 "Aha!"라는 시크릿 메시지를 숨기는 방식으로, 다크 그린 이미지를 나타내는 각 픽셀들의 최하위 비트(LSB: Least Significant Bit)를 시크릿 메시지에 해당하는 비트로 대체할 수 있다.

[0076] 시각암호 생성부(321)는 이와 같은 스테가노그래피 기법을 이용하여 시각암호를 구성하는 제1 이미지 및 제2 이미지에 시각암호에 해당하는 인증코드를 삽입할 수 있으며, 그 위치는 각각 제1 이미지 및 제2 이미지를 수신하는 사용자 단말(500)의 등록 정보에 기반하여 정해질 수 있다.

[0077] 시각암호 생성부(321)는 시각암호를 구성하는 제1 이미지 및 제2 이미지를 중앙 제어 서버(100)로 전송할 뿐만 아니라, 제1 이미지에 인증코드가 삽입된 이미지 및 제2 이미지에 인증코드가 삽입된 이미지 또한 중앙 제어 서버(100)로 전송할 수 있다. 이때, 중앙 제어 서버(100)는 제1 이미지에 제1 사용자 단말(500a)의 등록 정보에 따른 위치에 인증코드가 삽입된 이미지 및 제2 이미지를 제1 사용자 단말(500a)로 전송하고, 제2 이미지에 제2 사용자 단말(500b)의 등록 정보에 따른 위치에 인증코드가 삽입된 이미지 및 제1 이미지를 제2 사용자 단말(500b)로 전송할 수 있다.

[0078] 이와 같은 경우, 제1 사용자 단말(500a)은 자신의 등록 정보에 따라 제1 이미지에 인증코드가 삽입된 이미지에서 인증코드가 숨겨진 위치를 확인하고 해당 위치에서 인증코드에 해당하는 비트를 추출하여 인증코드를 인식하며, 인증코드가 삽입되기 전의 제1 이미지를 획득할 수 있다. 제2 사용자 단말(500b) 또한 자신의 등록 정보에 따라 제2 이미지에 인증코드가 삽입된 이미지에서 인증코드가 숨겨진 위치를 확인하고 해당 위치에서 인증코드에 해당하는 비트를 추출하여 인증코드를 인식하며, 인증코드가 삽입되기 전의 제2 이미지를 획득할 수 있다. 이후, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)은 각각 제1 이미지와 제2 이미지를 중첩시켜 출력할 수 있다. 이때, 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)의 각 사용자는 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)에 각각 출력되는 제1 이미지와 제2 이미지의 중첩된 이미지로부터 시각암호에 해당하는 인증코드를 식별하고, 식별한 인증코드를 제1 사용자 단말(500a) 및 제2 사용자 단말(500b)에 각각 입력할 수 있다.

제1 사용자 단말(500a) 및 제2 사용자 단말(500b)은 사용자로부터 입력 받은 인증코드와, 제1 이미지 및 제2 이미지에 인증코드가 삽입된 이미지에서 각각 인식한 인증코드가 동일한지 확인하고, 동일한 경우 상호인증에 성공한 것으로 간주하고 통신을 수행할 수 있다.

- [0079] 시각암호 갱신부(322)는 이와 같은 사용자 단말(500) 간의 상호인증 성공여부에 따라 상호인증의 보안성을 높일 수 있도록 시각암호를 갱신할 수 있다.
- [0080] 구체적으로는, 시각암호 갱신부(322)는 미리 정해진 갱신 주기에 따라 시각암호, 즉, 시각암호에 해당하는 인증코드를 갱신할 수 있다. 이를 위해, 시각암호 갱신부(322)는 미리 정해진 갱신 주기에 따라 동작하는 리키잉(Rekeying) 타이머 모듈을 포함할 수 있다. 시각암호 갱신부(322)는 이와 같은 리키잉 타이머 모듈이 "0"이 되면 시각암호를 갱신할 수 있다.
- [0081] 여기에서, 시각암호 갱신부(322)는 두 사용자 단말(500)간 상호인증을 위해 시각암호가 배포되면, 상호인증의 성공여부를 확인할 수 있다. 그리고, 시각암호 갱신부(322)는 두 사용자 단말(500) 간의 상호인증에 성공한 것으로 확인되면, 미리 정해진 갱신 주기에 따라 시각암호를 갱신할 수 있다.
- [0082] 한편, 일반적으로, 모바일 개방형 IPTV 시스템(1000)에 있어서, 특정한 목적을 가지고 사용자 단말(500)간 상호인증을 의도적으로 실패하는 경우가 종종 발생하는데, 이는 모바일 개방형 IPTV 시스템(1000)의 전체적인 성능을 저하시킨다는 문제점이 있다. 이에 따라, 시각암호 갱신부(322)는 사용자 단말(500) 별로 상호인증 성공률을 나타내는 신용레벨을 부여할 수 있다. 이때, 시각암호 갱신부(322)는 사용자 단말(500) 각각의 신용레벨을 사용자 DB(200)에 저장할 수 있다.
- [0083] 시각암호 갱신부(322)는 두 사용자 단말(500)간의 상호인증에 실패한 것으로 확인되면, 그 횟수를 카운트할 수 있다. 이때, 시각암호 갱신부(322)는 미리 정해진 시간 이내에 두 사용자 단말(500)간의 통신이 이루어지지 않는 경우, 두 사용자 단말(500) 간의 상호인증에 실패한 것으로 확인할 수 있다. 그리고, 시각암호 갱신부(322)는 상호인증에 실패한 횟수와 미리 정해진 상호인증 실패 임계치를 비교하고, 상호인증에 실패한 횟수가 미리 정해진 상호인증 실패 임계치와 같거나, 미리 정해진 상호인증 실패 임계치보다 많은 경우, 상호인증에 실패한 두 사용자 단말(500)의 신용레벨을 수정할 수 있다. 이때, 시각암호 갱신부(322)는 사용자 DB(200)접속하여, 상호인증에 실패한 두 사용자 단말(500)의 신용레벨을 낮출 수 있다.
- [0084] 그리고, 시각암호 갱신부(322)는 수정된 두 사용자 단말(500)의 신용레벨을 미리 정해진 신용레벨 임계치와 비교할 수 있다. 시각암호 갱신부(322)는 수정된 두 사용자 단말(500)의 신용레벨이 미리 정해진 신용레벨 임계치와 같거나, 미리 정해진 신용레벨 임계치보다 낮은 경우, 미리 정해진 갱신 주기를 수정할 수 있다. 시각암호 갱신부(322)는 예를 들면, 리키잉 타이머를 조정하여 미리 정해진 갱신 주기를 짧게 할 수 있다.
- [0085] 시각암호 갱신부(322)는 이와 같이 상호인증의 성공 여부에 따라 시각암호의 갱신 주기를 조정하여 시각암호의 갱신을 수행함으로써, 상호인증의 보안성을 높일 수 있다.
- [0086] 다시, 도 5를 참조하면, 인증 서버 메모리부(330)는 인증 서버(300)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다.
- [0087] 이하, 도 8 및 도 9를 참조하여, 도 5에 도시된 인증 서버(300)의 제어방법에 대하여 설명하기로 한다.
- [0088] 도 8 및 도 9는 도 5에 도시된 인증 서버의 제어방법을 설명하기 위한 순서도이다.
- [0089] 먼저, 도 8을 참조하면, 인증 서버(300)는 중앙 제어 서버(100)로부터 시각암호 생성 요청을 수신하면(800), 제1 이미지 및 제2 이미지로 이루어지는 시각암호를 생성할 수 있다(810). 이때, 인증 서버(300)는 중앙 제어 서버(100)로부터 시각암호 생성 요청을 수신하지 않더라도(800), 리키잉 타이머를 확인하여(860), 시각암호를 갱신할 수 있다(880).
- [0090] 그리고, 인증 서버(300)는 사용자 DB(200)에 접속하여 상호인증을 수행할 제1 사용자 단말(500a) 및 제2 사용자 단말의 등록 정보를 확인하고(820), 제1 이미지에서 제1 사용자 단말(500a)의 등록 정보에 해당하는 위치 및 제2 이미지에서 제2 사용자 단말(500b)의 등록 정보에 해당하는 위치에 각각 스테가노그래피 기법을 이용하여 시각암호에 해당하는 인증코드를 삽입한 이미지를 생성할 수 있다(830).
- [0091] 인증 서버(300)는 시각암호를 구성하는 제1 이미지 및 제2 이미지와, 제1 이미지 및 제2 이미지에 각각 시각암호에 해당하는 인증코드가 삽입된 이미지를 중앙 제어 서버(100)로 전송할 수 있다(840). 이와 같은 경우, 중앙 제어 서버(100)에 의해 제1 이미지에 시각암호에 해당하는 인증코드가 삽입된 이미지 및 제2 이미지는 제1 사용

자 단말(500a)로 전송되고, 제2 이미지에 시각암호에 해당하는 인증코드가 삽입된 이미지 및 제1 이미지는 제2 사용자 단말(500b)로 전송되어, 제1 사용자 단말(500a)과 제2 사용자 단말(500b)간에 상호인증이 수행될 수 있다.

[0092] 인증 서버(300)는 제1 사용자 단말(500a)과 제2 사용자 단말(500b) 간에 상호인증에 성공하였는지 여부를 확인하고(850), 상호인증에 성공한 것으로 확인되면, 리키잉 타이머가 0에 도달하였는지를 확인하여(860), 시각암호를 갱신할 수 있다(880).

[0093] 한편, 인증 서버(300)는 제1 사용자 단말(500a)과 제2 사용자 단말(500b) 간에 상호인증에 실패한 것으로 확인되면(850), 리키잉 타이머를 제어하고(865), 리키잉 타이머가 0에 도달하였는지를 확인하여(860), 시각암호를 갱신할 수 있다.

[0094] 이와 관련하여, 도 9를 참조하여 구체적으로 설명하면, 인증 서버(300)는 상호인증 실패 횟수를 카운트할 수 있다(910). 인증 서버(300)는 상호인증 실패 횟수가 상호인증 실패 임계치와 같거나, 상호인증 실패 임계치보다 많은 것으로 확인되면(920), 사용자 DB(200)에 접속하여, 상호인증에 실패한 두 사용자 단말(500)의 신용레벨을 수정할 수 있다(930).

[0095] 그리고, 인증 서버(300)는 상호인증에 실패한 두 사용자 단말의 각 신용레벨이 신용레벨 임계치보다 작거나, 신용레벨 임계치와 같은 것으로 확인되면(940), 리키잉 타이머를 제어할 수 있다(940). 즉, 인증 서버(300)는 상호인증에 실패한 두 사용자 단말 중 어느 하나의 신용레벨이 신용레벨 임계치보다 작거나, 신용레벨 임계치와 같은 것으로 확인되면 리키잉 타이머를 제어하여 시각암호 갱신 주기를 짧게 할 수 있다.

[0096] 한편, 도 10은 도 1에 도시된 사용자 단말의 제어 블록도이고, 도 11은 사용자 단말에서 상호인증을 수행하는 방법을 설명하기 위한 도면이다.

[0097] 먼저, 도 10을 참조하면, 사용자 단말(500)은 사용자 단말 통신부(510), 사용자 단말 입력부(520), 사용자 단말 출력부(530), 사용자 단말 제어부(540), 사용자 단말 메모리부(550), 전원 공급부(560) 및 인터페이스부(570)를 포함할 수 있다. 사용자 단말(500)은 모바일 개방형 IPTV 서비스에 가입한 사용자가 소지하고 있는 단말로, 동일한 IPTV 서비스에 가입한 다른 사용자가 소지하고 있는 사용자 단말(500)과 직접 통신하여, 콘텐츠를 송신하거나, 콘텐츠를 수신하여 출력할 수 있으며, 이때, 콘텐츠를 송수신하는 다른 사용자 단말(500)과의 상호인증을 수행할 수 있다. 이러한 사용자 단말(500)은 도 10에 도시된 구성요소보다 많은 구성요소에 의해 구현될 수 있고, 그보다 적은 구성요소에 의해 구현될 수 있다. 이하, 상술한 구성요소들에 대해 구체적으로 설명하기로 한다.

[0098] 사용자 단말 통신부(510)는 사용자 단말(500)과 로컬 제어 서버(400) 또는 중앙 제어 서버(100) 간의 통신을 가능하게 하고, 또는 다른 사용자 단말(500)과의 통신을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다.

[0099] 사용자 단말 통신부(510)는 로컬 제어 서버(400)로 사용자 등록 정보를 포함하는 IPTV 서비스 가입 요청 신호를 전송하거나, 사용자 단말(500)에서 생성하여 다른 단말로 제공할 수 있는 콘텐츠 리스트를 전송할 수 있으며, 로컬 제어 서버(400)로부터 IPTV 서비스에서 이용 가능한 콘텐츠 리스트를 수신하거나, 상호인증을 위한 정보를 수신할 수 있다. 이때, 사용자 단말 통신부(510)는 로컬 제어 서버(400)를 거치지 않고 바로 중앙 제어 서버(100)와 통신할 수 있다. 또한, 사용자 단말(500)은 콘텐츠를 공유할 다른 사용자 단말(500)로부터 상호인증을 위한 정보를 수신하거나, 콘텐츠를 송수신할 수 있다.

[0100] 사용자 단말 입력부(520)는 사용자로부터 사용자 단말(500)의 각종 동작 제어를 위한 신호를 입력 받아 입력 데이터를 발생시킬 수 있으며, 이를 위해, 사용자 단말 입력부(520)는 키 패드, 돔 스위치, 터치 패드, 조그 휠, 조그 스위치 등으로 구현될 수 있다. 예를 들면, 사용자 단말 입력부(520)는 사용자로부터 사용자 등록 정보를 입력 받거나, IPTV 서비스 가입 요청 신호를 입력 받을 수 있다. 또한, 사용자는 사용자 단말 입력부(520)를 통해 콘텐츠를 직접 생성할 수 있으며, 해당 콘텐츠 리스트를 중앙 제어 서버(100)로 전송할 수 있다. 또한, 사용자 단말 입력부(520)는 사용자로부터 콘텐츠 리스트 중 하나의 콘텐츠를 선택 받을 수 있다. 또한, 사용자 단말 입력부(520)는 사용자로부터 시각암호의 식별 결과를 입력 받을 수 있다.

[0101] 사용자 단말 출력부(530)는 사용자 단말(500)에서 발생하는 오디오 신호 또는 비디오 신호를 출력할 수 있으며, 이를 위해, 디스플레이, 음향 출력 모듈 등을 포함하여 구현될 수 있다. 예를 들면, 사용자 단말 출력부(530)는 다른 단말로부터 수신하는 콘텐츠를 출력할 수 있다. 또한, 사용자 단말 출력부(530)는 사용자 등록 정보를 입력 받기 위한 화면을 출력할 수 있다. 또한, 사용자 단말 출력부(530)는 다른 단말로부터 제공받을 수 있는 콘

텐츠 리스트를 출력할 수 있다. 또한, 사용자 단말 출력부(530)는 시각암호를 출력할 수 있다.

[0102] 사용자 단말 제어부(540)는 사용자 단말(500)의 전반적인 동작을 제어할 수 있으며, 특히, 다른 단말과의 상호 인증을 수행할 수 있다. 이를 위해, 사용자 단말 제어부(540)는 상호인증 요청부(541), 인증코드 식별부(542) 및 인증코드 비교부(543)를 포함할 수 있다.

[0103] 상호인증 요청부(541)는 사용자 단말 입력부(520)를 통해 사용자로부터 다른 단말로부터 제공받을 수 있는 콘텐츠 리스트 중 적어도 하나를 선택 받으면, 해당 정보를 중앙 제어 서버(100)로 송신함과 동시에 선택한 콘텐츠를 제공할 수 있는 다른 단말과의 상호인증을 요청할 수 있다. 이와 같은 경우, 중앙 제어 서버(100)로부터 선택한 콘텐츠를 제공할 수 있는 다른 단말에 대한 정보를 수신할 수 있다. 또는, 콘텐츠를 제공하는 입장의 사용자 단말(500)의 경우, 중앙 제어 서버(100)로부터 다른 단말의 정보와 함께 다른 단말에서 요청하는 특정 콘텐츠에 대한 정보를 수신할 수 있다.

[0104] 인증코드 식별부(542)는 중앙 제어 서버(100)로부터 상호인증 요청에 응답한 이미지를 수신하면, 해당 이미지에 삽입된 인증코드를 식별할 수 있다. 또한, 인증코드 식별부(542)는 상호인증을 수행할 다른 단말과 공유하는 이미지를 사용자 단말 출력부(530)를 통해 출력하고, 사용자로부터 출력된 이미지에서 식별되는 시각암호를 입력 받을 수 있다.

[0105] 구체적으로는, 도 11의 (c)를 참조하면, 인증코드 식별부(542)는 중앙 제어 서버(100)로부터 하나의 시각암호를 구성하는 제1 이미지 및 제2 이미지 중 하나의 이미지를 수신할 수 있다. 또한, 인증코드 식별부(542)는 중앙 제어 서버(100)로부터 제1 이미지에 시각암호에 해당하는 인증코드가 삽입된 이미지 및 제2 이미지에 시각암호에 해당하는 인증코드가 삽입된 이미지 중 하나의 이미지를 수신할 수 있다. 이때, 사용자 단말(500)은 다른 단말로 콘텐츠를 제공하는 입장이거나, 다른 단말로부터의 콘텐츠 수신을 요청한 입장일 수 있다. 예를 들면, 인증코드 식별부(542)는 제1 이미지에 인증코드가 삽입된 이미지와 제2 이미지를 수신할 수 있다. 이와 같은 경우, 제2 이미지에 인증코드가 삽입된 이미지와 제1 이미지는 상호인증을 수행할 다른 사용자 단말(500)로 전송될 수 있다.

[0106] 한편, 상술한 바와 같이, 도 11의 (a) 및 (b)를 참조하면, 시각암호를 생성하는 인증 서버(300)는 시각암호를 구성하는 제1 이미지 및 제2 이미지를 생성하고, 제1 이미지 및 제2 이미지 각각 시각암호에 해당하는 인증코드를 스테가노그래피 기법으로 삽입할 수 있으며, 그 위치는 각 이미지를 수신하는 사용자 단말(500)의 등록 정보에 따라 정해질 수 있다.

[0107] 이에 따라, 도 11의 (d)를 참조하면, 인증코드 식별부(542)가 중앙 제어 서버(100)로부터 제1 이미지에 시각암호에 해당하는 인증코드가 삽입된 이미지 및 제2 이미지를 수신한 경우, 인증코드 식별부(542)는 먼저 제1 이미지에 인증코드가 삽입된 이미지에서 자신의 등록 정보에 따라 인증코드가 삽입된 위치를 확인하고, 해당 위치에서 인증코드에 해당하는 비트를 추출하고, 소정의 복호와 작업을 수행하여 스테가노그래피 기법으로 숨겨진 인증코드를 인식하며, 인증코드가 삽입되기 전의 제1 이미지를 획득할 수 있다. 이때, 인증코드 식별부(542)는 예를 들면 아래의 알고리즘에 따라 인증코드가 삽입된 위치를 확인하고, 해당 위치에서 세로로 h 비트를 뽑아내고, 인증코드의 길이만큼 잘라내어 인증코드를 인식함과 동시에 해당 비트열을 뽑아낸 인증코드가 삽입되기 전의 제1 이미지를 획득할 수 있다.

```
x = id ⊕ pw; // 사용자의 id, password
if(x > l) location = x mod l;
else if(x < l) location = l mod x;
location 위치에 해당하는 위치에 세로로 h 비트를 생성하여 insert
h = 인증코드비트 || pad (길이가 부족한 경우 padding 추가)
```

[0108]

[0109] 인증코드 식별부(542)는 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드를 사용자 단말 메모리부(550)에 임시로 저장해둘 수 있다. 예를 들면, 인증코드 식별부(542)는 제1 이미지에 인증코드가 삽입된 이미지에서 "3598"의 인증코드를 식별할 수 있다.

- [0110] 그리고, 도 11의 (d) 및 (e)를 참조하면, 인증코드 식별부(542)는 중앙 제어 서버(100)로부터 수신한 제2 이미지와, 인증코드에 해당하는 비트열을 뽑아내어 획득한 인증코드가 삽입되기 전의 제1 이미지를 중첩하여 사용자 단말 출력부(530)를 통해 출력할 수 있다.
- [0111] 여기에서, 상술한 바와 같이, 제1 이미지와 제2 이미지가 중첩되면 육안으로 시각암호를 식별할 수 있다. 이에 따라, 사용자 단말 출력부(530)로 출력되는 제1 이미지와 제2 이미지의 중첩된 이미지로부터, 사용자는 시각암호를 식별할 수 있다. 이때, 인증코드 식별부(542)는 사용자 단말 입력부(520)를 통해 사용자로부터 제1 이미지와 제2 이미지의 중첩된 이미지로부터 식별되는 시각암호를 입력 받을 수 있다. 예를 들면, 사용자 단말 출력부(530)에는 도 11의 (e)와 같이 "3598"이 식별 가능한 제1 이미지와 제2 이미지의 중첩된 이미지가 출력될 수 있다.
- [0112] 인증코드 비교부(543)는 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드와, 사용자로부터 입력 받은 제1 이미지와 제2 이미지의 중첩된 이미지로부터 식별된 인증코드를 비교할 수 있다. 인증코드 비교부(543)는 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드와, 사용자로부터 입력 받은 인증코드가 동일하면, 다른 단말과의 상호 인증에 성공한 것으로 판단할 수 있으며, 다른 단말로부터의 콘텐츠 수신을 허용하거나, 다른 단말로의 콘텐츠 전송을 허용할 수 있다.
- [0113] 예를 들면, 도 11과 같이, 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드가 "3598"이고, 사용자로부터 입력 받은 인증코드가 "3598"로 동일하면 인증코드 비교부(543)는 상호인증에 성공한 것으로 판단할 수 있다.
- [0114] 또는, 인증코드 비교부(543)는 제1 이미지와 제2 이미지의 중첩된 이미지로부터 식별되는 인증코드가 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드와 동일한지 여부를 사용자가 직접 판단할 수 있도록, 사용자 단말 출력부(530)를 통해 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드와 제1 이미지와 제2 이미지의 중첩된 이미지를 동시에 출력할 수 있으며, 사용자의 판단 결과를 입력 받아 상호인증의 성공 여부를 판단할 수 있다.
- [0115] 다시 도 10을 참조하면, 사용자 단말 메모리부(550)는 사용자 단말(500)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다.
- [0116] 또한, 전원 공급부(560)는 사용자 단말(500)의 각 구성요소들의 동작에 필요한 전원을 공급할 수 있다. 예를 들면, 전원 공급부(560)는 사용자 단말 제어부(540)의 제어에 의해 사용자 단말(500) 내부 또는 외부의 전원을 인가받아 사용자 단말(500)의 각 구성요소로 공급할 수 있다.
- [0117] 인터페이스부(570)는 사용자 단말(500)에 연결되는 모든 외부기기와의 인터페이스 역할을 수행할 수 있으며, 이를 위해, 인터페이스부(570)는 유/무선 헤드셋 포트, 외부 충전지 포트, 유/무선 데이터 포트, 메모리 카드 포트, 식별 모듈이 구비된 장치를 연결하는 포트, 오디오 I/O 포트, 비디오 I/O 포트, 이어폰 포트 등이 포함될 수 있다.
- [0118] 이하, 도 12를 참조하여, 도 10에 도시된 사용자 단말(500)의 제어방법에 대하여 설명하기로 한다.
- [0119] 도 12는 도 10에 도시된 사용자 단말의 제어방법을 설명하기 위한 순서도이다.
- [0120] 도 12를 참조하면, 사용자 단말(500)은 로컬 제어 서버(400)를 통해 중앙 제어 서버(100)로 사용자의 개인 정보로 이루어지는 등록 정보를 전송하여 IPTV 서비스 가입을 요청할 수 있다(1200).
- [0121] 중앙 제어 서버(100)는 이러한 등록 정보에 응답하여 사용자 단말(500)로 사용자 단말(500)에서 다른 단말로 제공 가능한 콘텐츠 리스트를 요청할 수 있으며, 사용자 단말(500)은 중앙 제어 서버(100)의 요청에 응답하여 사용자 단말(500)에서 다른 단말로 제공 가능한 콘텐츠 리스트를 생성하여 중앙 제어 서버(100)로 전송할 수 있다(1201). 이와 같은 경우, 중앙 제어 서버(100)는 사용자 DB(200)에 사용자 단말(500)의 등록 정보 별로 콘텐츠 리스트를 매칭하여 저장할 수 있고, 복수의 사용자 단말(500)로부터 수신하는 콘텐츠 리스트를 취합하여, IPTV 서비스에서 공유하는 콘텐츠 리스트를 생성할 수 있으며, 생성한 콘텐츠 리스트를 IPTV 서비스에 가입한 모든 사용자 단말(500)로 전송할 수 있다.
- [0122] 사용자 단말(500)은 중앙 제어 서버(100)로부터 수신 가능한 콘텐츠 리스트를 수신하여 출력할 수 있으며(1202), 출력한 콘텐츠 리스트 중 사용자로부터 입력 받는 콘텐츠 요청 신호를 중앙 제어 서버(100)로 송신할 수 있다(1203).

- [0123] 여기에서, 중앙 제어 서버(100)는 사용자 DB(200)에 접속하여 사용자 단말(500)로부터 요청 받은 콘텐츠를 공유할 수 있는 다른 사용자 단말(500)을 검색하고, 다른 사용자 단말(500)로 이러한 사실을 알릴 수 있으며, 인증 서버(300)로 콘텐츠를 공유할 두 사용자 단말(500) 간의 상호인증을 위한 정보를 요청할 수 있다.
- [0124] 인증 서버(300)에서는 제1 이미지 및 제2 이미지의 한 쌍의 이미지로 이루어지는 시각암호를 생성하고, 각 이미지에서 콘텐츠를 공유할 두 사용자 단말(500) 각각의 등록 정보에 따른 위치에 시각암호에 해당하는 인증코드를 스테가노그래피 기법으로 삽입한 이미지를 생성할 수 있다.
- [0125] 사용자 단말(500)은 중앙 제어 서버(100)를 통해 인증 서버(300)로부터 콘텐츠를 공유할 다른 사용자 단말(500)로 전송되는 제1 이미지와 쌍을 이루는 제2 이미지 및 제1 이미지에 인증코드가 삽입된 이미지를 수신할 수 있다(1204).
- [0126] 그리고, 사용자 단말(500)은 인증 서버(300)로부터 수신한 제1 이미지에 인증코드가 삽입된 이미지에서 특정 위치에 해당하는 부분을 추출하여 삽입된 인증코드를 식별하고, 인증코드가 삽입되기 전의 제1 이미지를 획득할 수 있다 (1205). 구체적으로는, 사용자 단말(500)은 제1 이미지에 인증코드가 삽입된 이미지에서 사용자 단말(500) 사용자의 개인정보로 이루어지는 등록 정보에 따라 인증코드가 삽입된 위치를 확인하고, 해당 위치에서 인증코드에 해당하는 비트를 추출하여 삽입된 인증코드를 식별하며, 인증코드가 삽입되기 전의 제1 이미지를 획득할 수 있다.
- [0127] 그리고, 사용자 단말(500)은 제1 이미지 및 제2 이미지를 중첩하여 출력할 수 있다(1206).
- [0128] 그리고, 사용자 단말(500)은 사용자로부터 두 이미지의 중첩된 이미지로부터 식별되는 인증코드를 입력받을 수 있다(1207).
- [0129] 사용자 단말(500)은 제1 이미지에 인증코드가 삽입된 이미지에서 식별한 인증코드와, 두 이미지의 중첩된 이미지로부터 식별되는 인증코드가 동일한지를 확인하고(1208), 동일한 경우, 다른 사용자 단말(500)과의 콘텐츠 공유를 허용하고(1209), 그렇지 않은 경우, 다른 사용자 단말(500)과의 콘텐츠 공유를 차단할 수 있다(1210).
- [0130] 이와 같은, 본 발명의 일 실시예에 따른 모바일 개방형 IPTV 시스템(1000)에 포함되는 각 구성요소의 제어방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.
- [0131] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0132] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0133] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드 뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0134] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

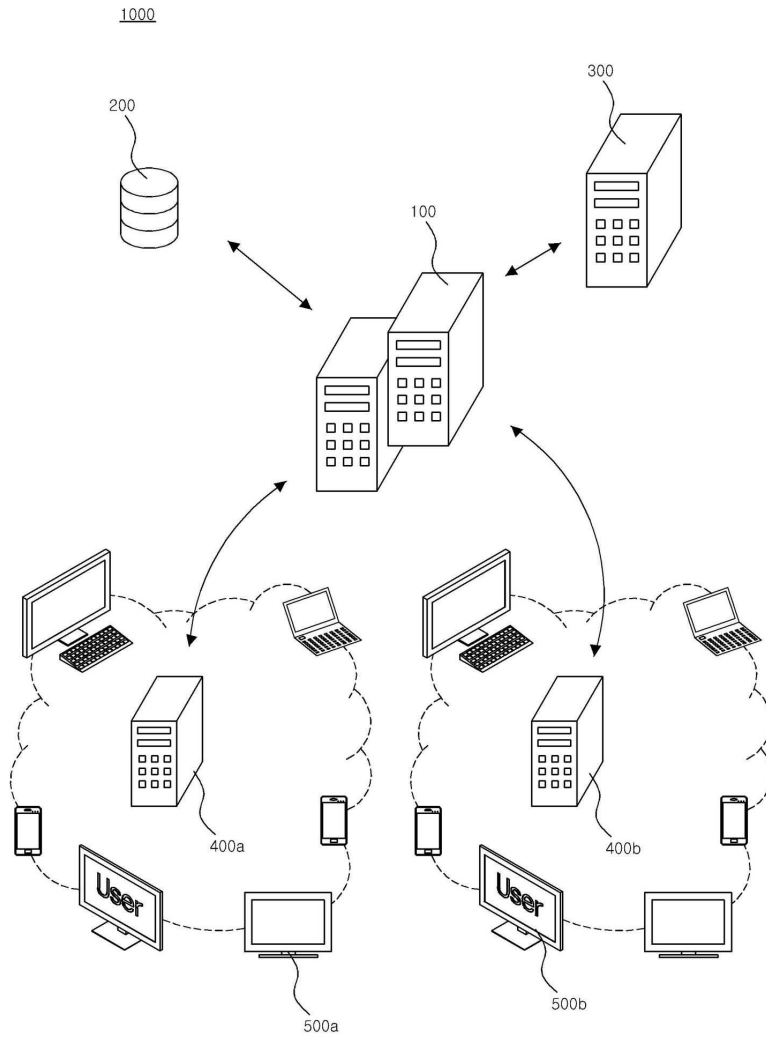
부호의 설명

- [0135] 1000: 모바일 개방형 IPTV 시스템
- 100: 중앙 제어 서버
- 200: 사용자 DB
- 300: 인증 서버
- 400a, 400b: 로컬 제어 서버

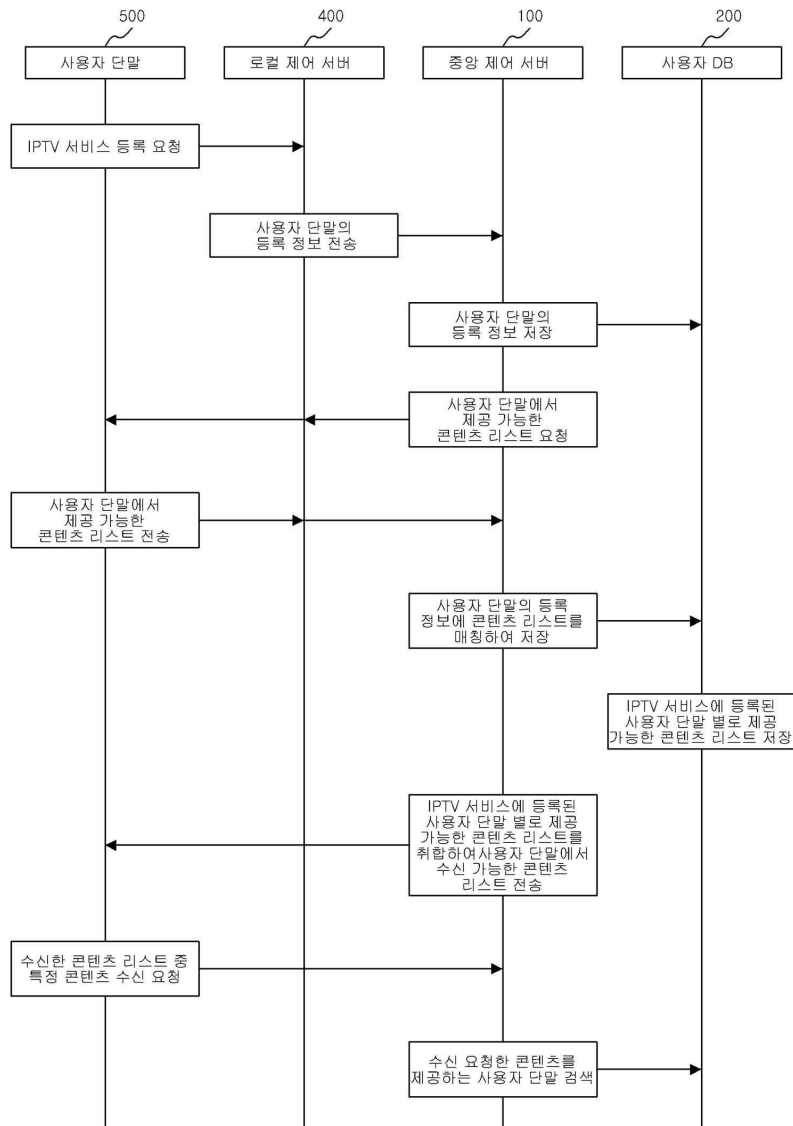
500a, 500b: 사용자 단말

도면

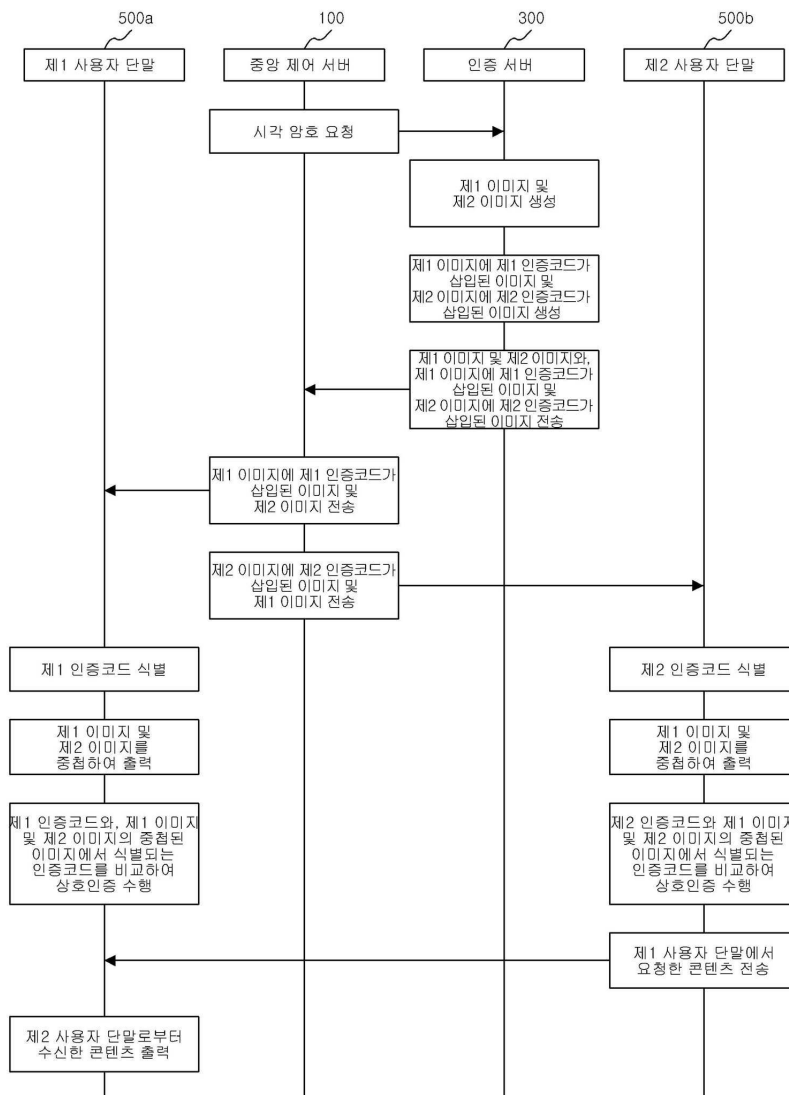
도면1



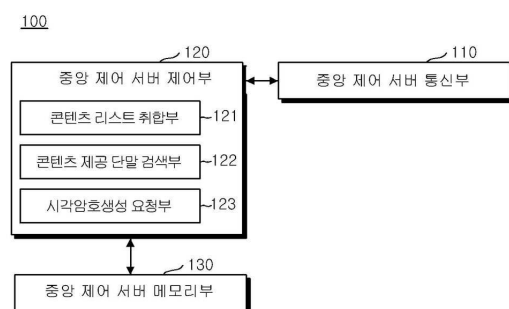
도면2



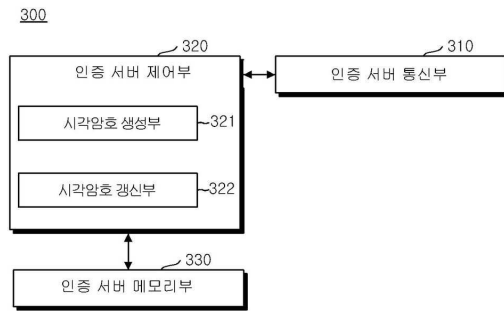
도면3



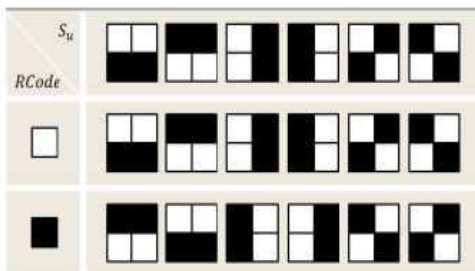
도면4



도면5



도면6

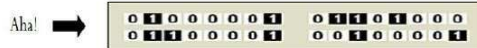


도면7

Define a dark green pixel :



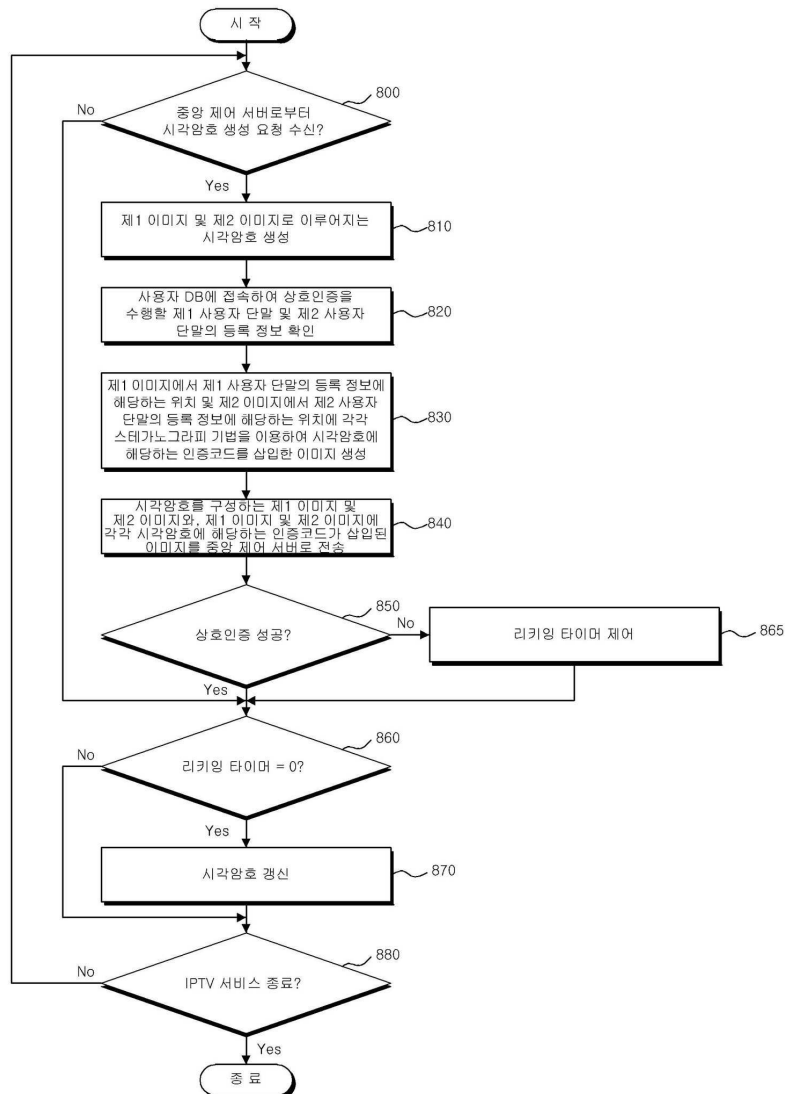
Secret message :



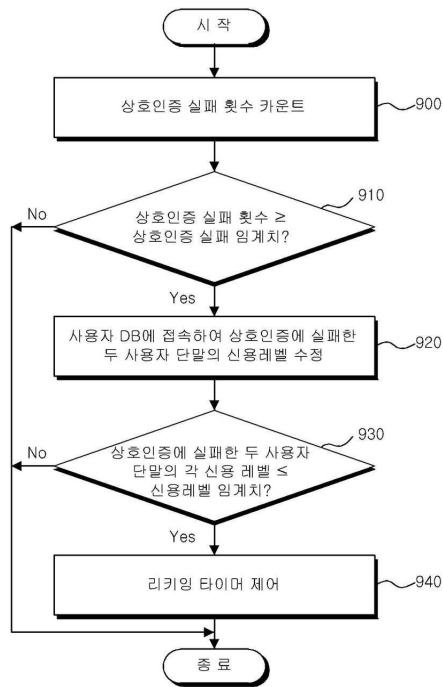
A dark green background encrypting Aha!:

Pixel	Byte 1 - Red	Byte 2 - Green	Byte 3 - Blue
1	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
2	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
3	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
4	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
5	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
6	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
7	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
8	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
9	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
10	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
11	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0

도면8



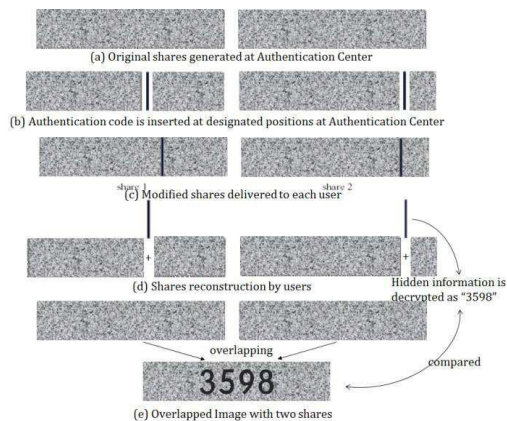
도면9



도면10



도면11



도면12

