(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0089711
(43) 공개일자 2016년07월28일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 63/0428 (2013.01)
H04L 9/32 (2013.01)
(21) 출원번호 10-2015-0009275
(22) 출원일자 2015년01월20일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
서경주
서울특별시 강남구 영동대로114길 56 삼성래미안 1차 아파트 101동 1102호
유한일
경기도 성남시 분당구 성남대로171번길 8 청솔마을영남아파트 103동 1004호
(뒷면에 계속)
(74) 대리인
이건주, 김정훈

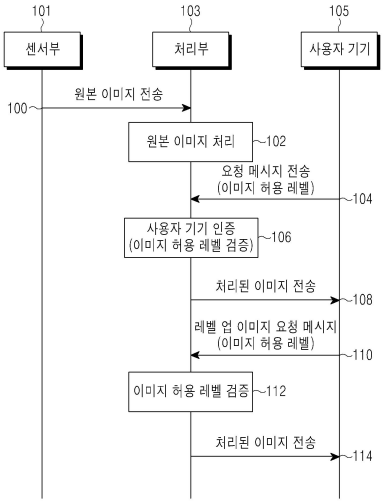
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **개인 정보 데이터 보안을 강화하는 장치 및 방법**

(57) 요 약

본 발명은 데이터 보안을 강화하는 방법에 있어서, 미리 정해진 프라이버시 레벨(privacy level)들을 기반으로 원본(raw) 이미지를 처리하여 처리된 이미지들을 생성하고, 사용자 기기로부터 제1 프라이버시 레벨에 관련된 정보가 포함된 요청 메시지가 수신되면, 상기 사용자 기기를 인증하고, 상기 인증 결과 상기 사용자 기기가 인증된 기기일 경우, 상기 제1 프라이버시 레벨에 관련된 정보를 검증하고, 상기 제1 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제1 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송한다.

대 표 도 - 도1



(72) 발명자

김상진

경기도 수원시 권선구 동수원로146번길 283 402호

박주현

서울특별시 구로구 개봉로15길 74-20

이혜진

서울특별시 동대문구 사가정로 148 SK아파트 113동 1102호

이희정

경기도 수원시 영통구 영통로290번길 25 신나무실 주공5단지아파트 512동 603호

명 세 서

청구범위

청구항 1

데이터 보안을 강화하는 방법에 있어서,

미리 정해진 프라이버시 레벨(privacy level)들을 기반으로 원본(raw) 이미지를 처리하여 처리된 이미지들을 생성하는 과정과,

사용자 기기로부터 제1 프라이버시 레벨에 관련된 정보가 포함된 요청 메시지가 수신되면, 상기 사용자 기기를 인증하는 과정과,

상기 인증 결과 상기 사용자 기기가 인증된 기기일 경우, 상기 제1 프라이버시 레벨에 관련된 정보를 검증하는 과정과,

상기 제1 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제1 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송하는 과정을 포함하는 데이터 보안 강화 방법.

청구항 2

제1항에 있어서,

상기 미리 정해진 프라이버시 레벨들은 미리 정해진 이미지 허용 레벨들을 포함하고, 상기 이미지 허용 레벨들은 상기 처리된 이미지들에 대한 접근을 허용함을 나타내며, 이미지 허용 레벨이 높을수록 상기 원본 이미지와 유사한 처리된 이미지에 대한 접근을 허용함을 특징으로 하는 데이터 보안 강화 방법.

청구항 3

제1항에 있어서,

상기 처리된 이미지보다 상기 원본 이미지와 유사한 처리된 이미지에 대한 접근을 허용하는 이미지 허용 레벨을 포함하는 제2 프라이버시 레벨에 관련된 정보가 포함된 레벨 업 요청 메시지를 수신하는 과정과,

상기 제2 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제2프라이버시 레벨을 기반으로 처리 이미지를 상기 사용자 기기에게 전송하는 과정을 포함하는 데이터 보안 강화 방법.

청구항 4

제1항에 있어서,

상기 제1 프라이버시 레벨에 관련된 정보를 검증하는 과정은, 상기 제1 프라이버시 레벨에 관련된 정보가 지시하는 프라이버시 레벨과 상기 사용자 기기에게 정책상 허용된 프라이버시 레벨을 비교하는 과정임을 특징으로 하는 데이터 보안 강화 방법.

청구항 5

제1항에 있어서,

상기 요청 메시지에 상기 제1 프라이버시 레벨에 관련된 정보가 포함되지 않을 경우, 디폴트 값의 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송하는 과정을 더 포함하는 데이터 보안 강화 방법.

청구항 6

제1항에 있어서,

상기 제1 프라이버시 레벨을 호 설정 및 등록 절차에서 세션 디스크립션 프로토콜(SDP: session description protocol) 파라미터 또는 홈 가입자 서버(HSS: home subscriber server)를 통해 미리 설정하는 과정을 더 포함하며,

이 경우 상기 요청 메시지에는 상기 제1 프라이버시 레벨에 관련된 정보가 포함되지 않음을 특징으로 하는 데이터 보안 강화 방법.

청구항 7

제1항에 있어서,

상기 사용자 기기로부터 긴급 상황의 발생과 관련된 정보가 수신되면, 상기 긴급 상황의 발생과 관련된 정보를 포함하는 긴급 상황 알림 메시지를 센서부로 전송하는 과정과,

상기 센서부로부터 상기 원본 이미지와 상기 긴급 상황의 발생과 관련된 정보가 수신되면, 상기 원본 이미지와 상기 긴급 상황의 발생과 관련된 정보를 상기 사용자 기기, 응급센터, 주변 사용자 기기 중 적어도 하나에 전송하는 과정을 더 포함하는 데이터 보안 강화 방법.

청구항 8

제7항에 있어서,

상기 원본 이미지와 상기 긴급 상황의 발생과 관련된 정보를 상기 응급센터에 전송할 때, 환자에 대한 식별자(ID: identifier), 상기 환자의 웨어러블 기기에 대한 ID, 상기 환자의 이-헬스 기기에 대한 ID 중 적어도 하나를 더 전송함을 특징으로 하는 데이터 보안 강화 방법.

청구항 9

제1항에 있어서,

상기 원본 이미지를 처리하는 과정은;

상기 원본 이미지에서 타겟 촬영 대상을 제외한 배경이 제외되도록 처리하는 과정, 상기 원본 이미지에서 촬영 대상들의 윤곽선만이 남도록 처리하는 과정, 상기 원본 이미지를 스무딩 기법을 기반으로 처리하는 과정, 및 상기 원본 이미지에서 상기 타겟 촬영 대상을 제외한 배경이 다른 배경으로 교체되도록 처리하는 과정 중 어느 하나임을 특징으로 하는 데이터 보안 강화 방법.

청구항 10

제1항에 있어서,

상기 원본 이미지에 대한 타임 스탬프(time stamp)에 관련된 정보 및 난수에 관련된 정보 중 적어도 하나를 상기 사용자 기기에게 전송하는 과정을 더 포함하며,

상기 원본 이미지에 대한 타임 스탬프 및 난수는 상기 처리된 이미지의 변조 여부를 검출하는데 사용됨을 특징으로 하는 데이터 보안 강화 방법.

청구항 11

데이터 보안을 강화하는 장치에 있어서,

미리 정해진 프라이버시 레벨(privacy level)들을 기반으로 원본(raw) 이미지를 처리하여 처리된 이미지들을 생성하고, 사용자 기기로부터 제1 프라이버시 레벨에 관련된 정보가 포함된 요청 메시지가 수신되면, 상기 사용자 기기를 인증하고, 상기 인증 결과 상기 사용자 기기가 인증된 기기일 경우, 상기 제1 프라이버시 레벨에 관련된 정보를 검증하는 처리 모듈과,

상기 제1 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제1 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송하는 송수신 모듈을 포함하는 장치.

청구항 12

제11항에 있어서,

상기 미리 정해진 프라이버시 레벨들은 미리 정해진 이미지 허용 레벨들을 포함하고, 상기 이미지 허용 레벨들은 상기 처리된 이미지들에 대한 접근을 허용함을 나타내며, 이미지 허용 레벨이 높을수록 상기 원본 이미지와 유사한 처리된 이미지에 대한 접근을 허용함을 특징으로 하는 장치.

청구항 13

제11항에 있어서,

상기 송수신 모듈은 상기 처리된 이미지보다 상기 원본 이미지와 유사한 처리된 이미지에 대한 접근을 허용하는 이미지 허용 레벨을 포함하는 제2 프라이버시 레벨에 관련된 정보가 포함된 레벨 업 요청 메시지를 수신하고, 상기 제2 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제2프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송함을 특징으로 하는 장치.

청구항 14

제11항에 있어서,

상기 처리 모듈은 상기 제1 프라이버시 레벨에 관련된 정보가 지시하는 프라이버시 레벨과 상기 사용자 기기에게 정책상 허용된 프라이버시 레벨을 비교하여 상기 제1 프라이버시 레벨에 관련된 정보를 검증함을 특징으로 하는 장치.

청구항 15

제11항에 있어서,

상기 요청 메시지에 상기 제1 프라이버시 레벨에 관련된 정보가 포함되지 않을 경우, 상기 송수신 모듈은 디폴트 값의 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송함을 특징으로 하는 장치.

청구항 16

제11항에 있어서,

상기 처리 모듈은 상기 제1 프라이버시 레벨을 호 설정 및 등록 절차에서 세션 디스크립션 프로토콜(SDP: session description protocol) 파라미터 또는 홈 가입자 서버(HSS: home subscriber server)를 통해 미리 설정하며, 이 경우 상기 요청 메시지에는 상기 제1 프라이버시 레벨에 관련된 정보가 포함되지 않음을 특징으로 하는 장치.

청구항 17

제11항에 있어서,

상기 송수신 모듈은 상기 사용자 기기로부터 긴급 상황의 발생과 관련된 정보가 수신되면, 상기 긴급 상황의 발생과 관련된 정보를 포함하는 긴급 상황 알림 메시지를 센서부로 전송하고, 상기 센서부로부터 상기 원본 이미지와 상기 긴급 상황의 발생과 관련된 정보가 수신되면, 상기 원본 이미지와 상기 긴급 상황의 발생과 관련된 정보를 상기 사용자 기기, 응급센터, 주변 사용자 기기 중 적어도 하나에 전송함을 특징으로 하는 장치.

청구항 18

제17항에 있어서,

상기 송수신 모듈은 상기 원본 이미지와 상기 긴급 상황의 발생과 관련된 정보를 상기 응급센터에 전송할 때, 환자에 대한 식별자(ID: identifier), 상기 환자의 웨어러블 기기에 대한 ID, 상기 환자의 이-헬스 기기에 대한 ID 중 적어도 하나를 더 전송함을 특징으로 하는 장치.

청구항 19

제11항에 있어서,

상기 처리 모듈은 상기 원본 이미지에서 타겟 촬영 대상을 제외한 배경이 제외되도록 처리하는 동작, 상기 원본 이미지에서 촬영 대상들의 윤곽선만이 남도록 처리하는 동작, 상기 원본 이미지를 스무딩 기법을 기반으로 처리하는 동작, 및 상기 원본 이미지에서 상기 타겟 촬영 대상을 제외한 배경이 다른 배경으로 교체되도록 처리하는 동작 중 어느 하나를 통해 상기 원본 이미지를 처리함을 특징으로 하는 장치.

청구항 20

제11항에 있어서,

상기 송수신 모듈은 상기 원본 이미지에 대한 타임 스탬프(time stamp)에 관련된 정보 및 난수에 관련된 정보 중 적어도 하나를 상기 사용자 기기에게 전송하며, 상기 원본 이미지에 대한 타임 스탬프 및 난수는 상기 처리된 이미지의 변조 여부를 검출하는데 사용됨을 특징으로 하는 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 통신 네트워크를 통해 송수신되는 개인 정보 데이터의 보안을 강화하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 사물 인터넷(IoT: internet of things) 기기(device), 웨어러블(wearable) 기기, 이-헬스(e-health: electric-health) 기기, 스마트 홈 기기 등에서 각 기기는 인터넷과 연결되어 사용자에게 보다 다양하고 편리한 서비스들을 제공하고 있다.

[0003] 또한 각 기기는 통신 네트워크를 통해 사용자 개인의 정보, 프라이버시(privacy) 관련 정보 등을 전송할 수 있다. 그러나 이러한 정보들이 사용자 의도와 상관없이 수집될 수 있고 수집된 정보들이 위조되어 다시 전송될 수 있으므로, 통신 네트워크를 통해 사용자에게 서비스를 제공하는 기기들에게 있어서 보안은 매우 중요한 문제로 작용한다.

[0004] 따라서 차세대 통신 시스템에서는 통신 네트워크를 통해 사용자에게 서비스를 제공하는 기기들의 보안상 취약성

또는 프라이버시 침해 등을 해결할 수 있는 방안에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 통신 네트워크를 통해 송수신되는 데이터의 보안을 강화하는 장치 및 방법을 제안한다.

[0006] 또한 본 발명은 사용자 기기의 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송하는 장치 및 방법을 제안한다.

[0007] 또한 본 발명은 긴급 상황에서 원본 이미지를 사용자 기기에게 전송하는 장치 및 방법을 제안한다.

[0008] 또한 본 발명은 사용자 기기의 프라이버시 레벨을 기반으로 처리된 이미지의 변조를 검출하는 장치 및 방법을 제안한다.

과제의 해결 수단

[0009] 본 발명의 일 실시예에서 제안하는 방법은; 데이터 보안을 강화하는 방법에 있어서, 미리 정해진 프라이버시 레벨(privacy level)들을 기반으로 원본(raw) 이미지를 처리하여 처리된 이미지들을 생성하는 과정과, 사용자 기기로부터 제1 프라이버시 레벨에 관련된 정보가 포함된 요청 메시지가 수신되면, 상기 사용자 기기를 인증하는 과정과, 상기 인증 결과 상기 사용자 기기가 인증된 기기일 경우, 상기 제1 프라이버시 레벨에 관련된 정보를 검증하는 과정과, 상기 제1 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제1 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송하는 과정을 포함한다.

[0010] 본 발명에서 일 실시예에서 제안하는 장치는; 데이터 보안을 강화하는 장치에 있어서, 미리 정해진 프라이버시 레벨(privacy level)들을 기반으로 원본(raw) 이미지를 처리하여 처리된 이미지들을 생성하고, 사용자 기기로부터 제1 프라이버시 레벨에 관련된 정보가 포함된 요청 메시지가 수신되면, 상기 사용자 기기를 인증하고, 상기 인증 결과 상기 사용자 기기가 인증된 기기일 경우, 상기 제1 프라이버시 레벨에 관련된 정보를 검증하는 처리 모듈과, 상기 제1 프라이버시 레벨에 관련된 정보의 검증이 완료되면, 상기 처리된 이미지들 중 상기 제1 프라이버시 레벨을 기반으로 처리된 이미지를 상기 사용자 기기에게 전송하는 송수신 모듈을 포함한다.

발명의 효과

[0011] 본 발명은 통신 네트워크를 통해 송수신되는 데이터의 보안을 강화하도록 함으로써, 통신 네트워크를 통해 사용자에게 서비스를 제공하는 기기들의 보안상 취약성 또는 프라이버시 침해 등을 해결할 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명의 일 실시예에 따라 처리된 이미지를 사용자 기기에 전송하는 절차의 예를 나타낸 신호 흐름도,

도 2는 본 발명의 일 실시예에 따라 단말들 간에 수행되는 호 설정 및 해제 절차의 예를 나타낸 신호 흐름도,

도 3은 본 발명의 일 실시예에 따라 긴급 상황에 원본 이미지를 사용자 기기, 응급센터 및 주변 사용자 기기에 전송하는 절차의 예를 나타낸 신호 흐름도,

도 4는 본 발명의 일 실시예에 따라 처리된 이미지의 변조를 검출하는 절차의 예를 나타낸 신호 흐름도,

도 5는 처리부가 본 발명의 일 실시예에 따라 필터링된 이미지를 사용자 기기에게 전송하는 과정을 나타낸 순서도,

도 6은 처리부가 본 발명의 일 실시예에 따라 긴급 상황에 원본 이미지를 사용자 기기, 응급 센터 및 주변 사용자 기기에 전송하는 과정을 도시한 순서도,

도 7은 본 발명의 일 실시예에 따라 데이터 보안을 강화하는 처리부의 내부 구성을 나타낸 블록도,

도 8a 내지 도 8c는 본 발명의 일 실시예에 따라 데이터 보안을 강화하는 처리부를 구현하는 예를 나타낸 도면.

발명을 실시하기 위한 구체적인 내용

[0013] 이하, 본 발명의 바람직한 실시예를 첨부된 도면을 참조하여 상세히 설명한다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략한다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0014] 후술할 본 발명의 실시예에서는 사물 인터넷 기기, 웨어러블 기기, 이-헬스 기기, 스마트 홈 기기 등이 전송하는 정보에 대한 보안을 강화하기 위한 방법에 대해 보다 상세히 설명하도록 한다.

[0015] 본 발명의 실시예들을 구체적으로 설명함에 있어서 3GPP(3rd generation partnership project)를 기반으로 하는 진화된 패킷 시스템(EPS: evolved packet system), 범용 이동 통신 시스템 무선 접속 네트워크(UTRAN: UMTS(universal mobile telecommunications system) radio access network), GERAN(GSM(global system for mobile communication) EDGE radio access network), 와이파이(Wi-Fi: wireless fidelity) 네트워크, 블루투스(bluetooth) 네트워크를 이용할 것이지만, 본 발명의 주요한 요지는 유사한 기술적 배경을 가지는 여타의 통신 시스템에도 본 발명의 범위를 크게 벗어나지 않는 범위에서 약간의 변경으로 적용 가능하며, 이는 본 발명의 기술 분야에서 숙련된 기술적 지식을 가진 자의 판단으로 가능할 것이다.

[0016] 도 1은 본 발명의 일 실시예에 따라 처리된 이미지를 사용자 기기에 전송하는 절차의 예를 나타낸 신호 흐름도이다.

[0017] 도 1을 참조하면, 도시된 신호 흐름도는 이미지를 촬영하는 센서부(101), 촬영된 이미지를 처리하는 처리부(103) 및 이미지를 전달 받는 사용자 기기(105)를 포함한다. 도 1에서는 센서부(101), 처리부(103) 및 사용자 기기(105) 각각이 별도의 유닛으로 구성된 경우를 일례로 설명한다. 그러나 센서부(101)와 처리부(103)는 경우에 따라 하나의 유닛으로 구성될 수도 있고 또는 센서(101), 처리부(103) 및 사용자 기기(105) 모두가 하나의 유닛으로 구성될 수도 있다.

[0018] 홈 네트워크 시스템을 가정하면, 상기 센서부(101)는 일례로 각종 카메라 또는 홈 디바이스에 결합된 카메라 등이 될 수 있고, 상기 사용자 기기(105)는 일례로 단말이나 홈 네트워크 시스템의 제어 유닛 등이 될 수 있다.

[0019] 또한 상기 홈 디바이스는 가전기기(smart appliance), 보안기기(security device), 조명기기(lighting device), 에너지기기(energy device) 등을 포함한다. 일례로 가전기기는 텔레비전(TV: television), 에어컨, 냉장고, 세탁기, 로봇청소기, 가습기 등이 될 수 있으며, 보안기기는 도어락, 보안 카메라, CCTV(closed circuit television), 보안 센서 등이 될 수 있고, 조명기구는 LED(light emitting diode), 램프 등이 될 수 있고, 에너지기기는 난방기기, 전력측정기, 전력 소켓, 전기 콘센트, 멀티탭 등이 될 수 있다. 추가적으로 홈 디바이스는 개인 컴퓨터(PC: personal computer), 인터넷 프로토콜(IP: internet protocol) 카메라, 인터넷 전화, 유/무선 전화, 전기적으로 제어 가능한 커튼, 블라인드 등을 포함할 수 있다.

[0020] 센서부(101)는 이미지를 촬영하고 촬영된 원본(raw) 이미지를 처리부(103)에 전송한다.(100단계)

[0021] 처리부(103)는 센서부(101)로부터 전송되는 원본 이미지를 처리부에 내장된 임시 버퍼 혹은 메모리부에 저장함과 동시에 혹은 저장한 후에 처리한다.(102단계) 상기 원본 이미지의 처리에는 일례로 필터링 방식, 마스킹 방식, 연산 처리 방식등이 사용될 수 있다. 즉 처리부(103)는 상기 처리 방식들에 기반하여 원본 이미지에 관련된 데이터를 분할하여 암호화할 수 있고, 특히 상기 원본 이미지에 관련된 데이터를 보안 등급과 프라이버시 레벨 등에 따라 타겟 촬영 대상만을 포함하는 정보, 배경만을 포함하는 정보, 배경과 타겟 촬영 대상 모두를 포함하는 정보, 배경과 타겟 촬영 대상 모두를 포함하는 정보를 암호화한 정보 등으로 처리한다. 여기서 프라이버시 레벨이라 함은 일례로 이미지 허용 레벨이 될 수 있으며, 상기 이미지 허용 레벨은 처리된 이미지에 대한 접근을 허용함을 나타낸다.

[0022] 일례로 처리부(103)는 원본 이미지에서 타겟 촬영 대상, 일례로 사람을 제외한 배경이 제외되도록 처리할 수 있고, 상기 원본 이미지에서 모든 촬영 대상들의 윤곽선만이 남도록 처리할 수 있고, 상기 원본 이미지를 스무딩

(smoothing) 기법을 기반으로 상기 모든 촬영 대상들이 흐릿해지도록 처리할 수 있고, 또는 쉬프트(shift) 연산, 컨벌루셔널(convolutional) 연산 등을 통해 상기 원본 이미지에서 상기 타겟 촬영 대상을 제외한 배경이 다른 배경으로 교체되도록 처리할 수 있다.

[0023] 또한 처리부(103)는 미리 약속된 긴급 상황이거나 이미지를 전달할 사용자 기기(105)의 이미지 허용 레벨이 원본 이미지에 대한 접근을 허용함을 지시할 경우, 102단계의 처리 과정을 수행하지 않고 원본 이미지 그대로 사용자 기기(105)에게 전달할 수 있다. 상기 미리 약속된 긴급 상황은 일례로 집안의 노약자 또는 환자에게 건강상의 문제가 발생된 경우, 집안에 침입자가 발생된 경우, 집안에 가스 누출 또는 화재 등이 발생된 경우 등이 될 수 있다. 이미지 허용 레벨이 원본 이미지에 대한 접근을 허용함을 지시하는 경우는 상기 사용자 기기(105)에 내장된 센서부에서 생체 관련 정보, 예를 들어 지문 또는 심박수 등의 정보를 인식하여 상기 사용자 기기(105) 내부 인증 과정을 거친 후 생성된 원본 이미지 접근 허용 지시일 수 있다.

[0024] 사용자 기기(105)는 처리부(103)로 이미지 또는 개인 정보의 전송을 요청하는 요청 메시지를 전송한다.(104단계) 처리부(103)는 상기 요청 메시지를 전송한 사용자 기기(105)를 인증한다.(106단계) 즉 사용자 기기(105)가 인증된 기기인지 확인한다. 여기서 요청 메시지를 센서부(101)가 아닌 처리부(103)로 전송하는 이유는 사용자 기기(105)가 센서부(101)가 촬영한 원본 이미지에 접근하는 것을 방지하고 처리부(103)를 통해 처리된 이미지에만 접근할 수 있도록 함으로써 보안과 프라이버시 보호를 강화하기 위함이다.

[0025] 사용자 기기(105)는 104단계에서 요청 메시지에 이미지 허용 레벨에 관련된 정보를 포함시켜 전송할 수도 있다. 이 경우 처리부(103)는 106단계에서 요청 메시지를 전송한 사용자 기기(105)가 인증된 기기인지 확인할 때, 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보의 검증도 함께 수행할 수 있다. 이미지 허용 레벨에 관련된 정보의 검증 과정은 사용자 기기(105)가 조회를 요청한 이미지 허용 레벨, 즉 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨과 상기 사용자 기기(105)에게 정책(policy)상 허용된 이미지 허용 레벨을 비교하는 방법 등이 사용될 수 있다.

[0026] 106단계의 사용자 기기 확인 및/또는 이미지 허용 레벨 검증 과정은 사용자 기기(105)의 네트워크 환경, 일례로 이동 통신 환경, 셀룰러 통신 환경, 블루투스 환경, 와이파이 환경 등에 따라 다양한 방법이 사용될 수 있으므로, 본 발명에서의 사용자 기기 확인 및/또는 이미지 허용 레벨 검증 과정에 사용되는 방법은 다양한 네트워크 환경에 따르도록 한다.

[0027] 처리부(103)는 사용자 기기 확인 및/또는 이미지 허용 레벨 검증이 완료되면, 사용자 기기(105)에게 처리된 이미지를 전송한다.(108단계) 108단계에서 처리된 이미지라 함은 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨을 기반으로 처리된 이미지로서, 사용자 기기(105)에게 접근이 허용된 이미지를 의미한다.

[0028] 여기서는 요청 메시지에 이미지 허용 레벨에 관련된 정보가 포함되는 경우를 일례로 설명하였다. 그러나 상기 요청 메시지에 상기 이미지 허용 레벨에 관련된 정보가 포함되지 않을 경우, 처리부(103)는 디폴트(default) 값의 이미지 허용 레벨을 기반으로 처리된 이미지를 사용자 기기(105)에게 전송한다. 디폴트 값의 이미지 허용 레벨은 사용자에 의해 설정되어 있거나 가장 강력한 이미지 허용 레벨일 수 있다.

[0029] 한편, 사용자 기기(105)는 처리부(103)로 레벨 업 이미지 요청 메시지를 전송하여(110단계), 108단계에서 수신한 처리된 이미지보다 세밀화된 이미지 전송을 요청한다. 이때 상기 레벨 업 이미지 요청 메시지에는 104단계에서 전송한 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨보다 높은 이미지 허용 레벨에 관련된 정보가 포함된다. 본 발명의 실시예에서는 상기 이미지 허용 레벨이 높을수록 원본 이미지와 유사하게 처리된 이미지에 대한 접근을 허용한다고 가정한다.

[0030] 처리부(103)는 상기 레벨 업 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보를 검증한다.(112단계) 그런 다음 처리부(103)는 상기 이미지 허용 레벨에 관련된 정보의 검증이 완료되면, 사용자 기기(105)에게 처리된 이미지를 전송한다.(114단계) 114단계에서 처리된 이미지는 레벨 업 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨을 기반으로 처리된 이미지를 의미한다.

[0031] 도 1에서는 원본 이미지 처리를 수행한 이후 사용자 기기(105)로부터 요청 메시지를 수신하는 동작을 일례로 설명하였다. 그러나 상기 원본 이미지를 처리하는 단계, 즉 102단계는 요청 메시지를 수신한 이후에 수행될 수도 있다. 이 경우 처리부(103)는 사용자 기기(105)로부터 이미지 허용 레벨에 관련된 정보가 포함된 요청 메시지를 수신하고, 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨을 기반으

로 원본 이미지를 처리한다.

[0032] 도 2는 본 발명의 일 실시예에 따라 단말들 간에 통신을 수행하는 절차의 예를 나타낸 신호 흐름도이다.

[0033] 도 2를 참조하면, 도시된 신호 흐름도는 제1 사용자 단말(UE: user equipment)(201), 제1 EUTRAN(evolved UTRAN)(203), 제1 코어 네트워크(205), 인터넷 프로토콜 멀티미디어 서브시스템(IMS: IP(internet protocol) multimedia subsystem)(207), 제2 코어 네트워크(209), 제2 EUTRAN(211) 및 제2 UE(213)를 포함한다.

[0034] 제1 UE(201)와 제2 UE(213)의 영상 통화를 가정하면, 제1 UE(201)는 제2 UE(213)와의 영상 통화를 위해 호 설정 및 등록 절차를 수행한다.(200단계) 상기 호 설정 및 등록 절차는 제1 EUTRAN(203), 제1 코어 네트워크(205), IMS(207), 제2 코어 네트워크(209) 및 제2 EUTRAN(211) 각각에 포함된 복수의 엔티티들을 통해 수행되나, 상기 호 설정 및 등록 절차 자체는 본 발명과 밀접한 연관이 없으므로 여기서는 200단계와 같이 간소화하여 도시하였다.

[0035] 원본 이미지를 처리하는 동작에서 적용되는 이미지 허용 레벨에 관련된 정보는 일례로 세션 디스크립션 프로토콜(SDP: session description protocol) 파라미터를 통해 200단계에서 설정될 수 있다. 즉 제1 UE(201)는 SDP 파라미터 값을 통해 처리 동작에 적용되는 이미지 허용 레벨을 미리 설정된 이미지 허용 레벨보다 높은 이미지 허용 레벨 또는 낮은 이미지 허용 레벨로 변경할 것을 요청하고, 제2 UE(213)는 상기 요청에 대응하는 응답에 상기 이미지 허용 레벨 변경에 대한 허락 여부를 나타내는 정보를 포함시켜 전송함으로써, 상기 이미지 허용 레벨에 관련된 정보가 설정될 수 있다. 또한 상기 이미지 허용 레벨에 관련된 정보는 디폴트 값에 의해 설정될 수도 있다. 디폴트 값의 이미지 허용 레벨은 사용자에 의해 설정되어 있거나 가장 강력한 이미지 허용 레벨일 수 있다.

[0036] 원본 이미지를 처리하는 동작에서 적용되는 이미지 허용 레벨에 관련된 정보는 또 다른 예로 홈 가입자 서버(HSS: home subscriber server)를 통해 200단계에서 설정될 수 있다. 즉 HSS가 해당 UE가 설정한 디폴트 값의 이미지 허용 레벨에 관련된 정보를 가져옴으로써, 상기 이미지 허용 레벨에 관련된 정보가 설정될 수 있다. HSS를 통해 설정된 이미지 허용 레벨에 관련된 정보는 200단계에서 변경 가능하다.

[0037] 또한 원본 이미지의 처리에는 일례로 필터링 방식, 마스킹 방식, 연산 처리 방식 등이 사용될 수 있다.

[0038] 제1 UE(201)와 호 설정 및 등록 절차가 완료된 제2 UE(213)는 영상 통화를 위한 이미지 허용 레벨을 결정하고,(202단계) 결정된 이미지 허용 레벨을 기반으로 촬영된 원본 이미지를 처리한다.(204단계) 이때 이미지 허용 레벨은 사용자의 인터페이스에 의해 결정될 수도 있고, 미리 저장된 이미지 허용 레벨과 정책상 허용된 이미지 허용 레벨에 의해 자동적으로 결정될 수도 있다.

[0039] 이후 제2 UE(213)는 202단계에서 결정된 이미지 허용 레벨을 기반으로 처리된 이미지를 제1 UE(201)에게 전송하여, 제1 UE(201)와의 통신, 즉 영상 통화를 수행한다. 처리된 이미지를 전송한 제2 UE(213)는 제1 UE(201)와의 통신을 종료하기 위해 제1 UE(201)와 호 해제 절차를 수행한다.(208단계)

[0040] 도 3은 본 발명의 일 실시예에 따라 긴급 상황에 원본 이미지를 사용자 기기, 응급센터 및 주변 사용자 기기에 전송하는 절차의 예를 나타낸 신호 흐름도이다.

[0041] 도 3을 참조하면, 도시된 신호 흐름도는 이미지를 촬영하는 센서부(301), 촬영된 이미지를 처리하는 처리부(303), 이미지를 수신하는 사용자 기기(305), 응급센터(307) 및 주변 사용자 기기(309)를 포함한다. 도 3에서는 센서부(301), 처리부(303) 및 사용자 기기(305) 각각이 별도의 유닛으로 구성된 경우를 일례로 설명하나, 센서부(301)와 처리부(303)는 경우에 따라 하나의 유닛으로 구성될 수도 있고 또는 센서(301), 처리부(303) 및 사용자 기기(305) 모두가 하나의 유닛으로 구성될 수도 있다.

[0042] 도 3에서는 홈 네트워크 시스템에서 집안의 환자에게 건강상의 문제가 발생된 경우의 긴급 상황을 가정하여 설명하도록 한다. 그러나 도 3에서 설명하는 절차는 약간의 변경으로 그 밖의 다른 긴급 상황들에도 적용할 수 있다.

[0043] 사용자 기기(305), 일례로 단말, 웨어러블 기기, 이-헬스 기기 등은 집안의 환자에게 건강상의 문제가 발생되었

음을 감지하면,(300단계) 처리부(303)에게 긴급 상황 알림 메시지를 전송하여 긴급 상황이 발생되었음을 통지한다.(302단계) 즉 사용자 기기(305)는 상기 긴급 상황 알림 메시지에 긴급 상황의 발생과 관련된 정보를 포함시켜 전송함으로써, 긴급 상황의 발생을 처리부(303)에게 통지한다. 상기 긴급 상황의 발생을 통지하는 예로서 사용자 기기(305)는 긴급 상황 알림 메시지에 긴급 상황이 발생되었음을 지시하는 지시자를 포함시켜 전송하거나, 상기 긴급 상황 알림 메시지를 구성하는 비트들 중 긴급 상황의 발생과 관련된 특정 비트를 설정하여 전송할 수 있다.

[0044] 여기서 긴급 상황 알림 메시지를 센서부(301)가 아닌 처리부(303)로 전송하는 이유는 사용자 기기(305)가 센서부(301)가 촬영한 원본 이미지에 접근하는 것을 방지하고 처리부(303)를 통해 처리된 이미지에만 접근할 수 있도록 함으로써 보안과 프라이버시 보호를 강화하기 위함이다.

[0045] 또한 사용자 기기(305)는 응급센터(307)에 긴급 상황 알림 메시지와 집안의 환자에 대한 정보를 전송한다.(304단계) 상기 환자에 대한 정보는 상기 환자를 식별하는 환자 식별자(ID: identity)와 웨어러블 기기, 이-헬스 기기 등을 통해 측정한 환자의 건강 상태에 관련된 정보 등을 포함한다.

[0046] 사용자 기기(305)로부터 긴급 상황의 발생을 통지 받은 처리부(303)는 상기 사용자 기기(305)를 인증한다.(306단계) 즉 사용자 기기(305)가 인증된 기기인지 확인한다.

[0047] 또 다른 예로 사용자 기기(305)는 상기 302단계에서 전송되는 긴급 상황 알림 메시지에 이미지 허용 레벨에 관련된 정보를 포함시켜 전송할 수도 있다. 이 경우 처리부(303)는 사용자 기기(305)가 인증된 기기인지 확인할 때, 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보의 검증도 함께 수행한다. 이미지 허용 레벨에 관련된 정보의 검증 과정은 사용자 기기(305)가 조회를 요청한 이미지 허용 레벨, 즉 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨과 상기 사용자 기기(305)에게 정책상 허용된 프라이버시 레벨을 비교하는 방법 등이 사용될 수 있다.

[0048] 306단계의 사용자 기기 인증 및/또는 이미지 허용 레벨 검증 과정은 사용자 기기(305)의 네트워크 환경, 일례로 이동 통신 환경, 셀룰러 통신 환경, 블루투스 환경, 와이파이 환경 등에 따라 다양한 방법이 사용될 수 있으므로, 본 발명에서의 사용자 기기 확인 및/또는 이미지 허용 레벨 검증 과정에 사용되는 방법은 다양한 네트워크 환경에 따르도록 한다.

[0049] 처리부(303)는 302단계에서 수신한 긴급 상황 알림 메시지에 긴급 상황이 발생되었음을 지시하는 지시자가 포함되어 있는지 또는 상기 긴급 상황 알림 메시지를 구성하는 비트들 중 긴급 상황의 발생과 관련된 특정 비트가 설정되어 있는지 판단하여 긴급 상황의 발생 여부를 검증한다.(308단계)

[0050] 상기 검증 결과 긴급 상황이 발생되었음을 확인한 처리부(303)는 센서부(301)에게 긴급 상황 알림 메시지를 전송하여 긴급 상황이 발생되었음을 통지한다.(310단계) 즉 처리부(303)는 상기 긴급 상황 알림 메시지에 긴급 상황의 발생과 관련된 정보를 포함시켜 전송함으로써, 긴급 상황의 발생을 센서부(301)에게 통지한다. 상기 긴급 상황의 발생을 통지하는 예로서 사용자 기기(305)는 긴급 상황 알림 메시지에 긴급 상황이 발생되었음을 지시하는 지시자를 포함시켜 전송하거나, 상기 긴급 상황 알림 메시지를 구성하는 비트들 중 긴급 상황의 발생과 관련된 특정 비트를 설정하여 전송할 수 있다.

[0051] 처리부(303)로부터 긴급 상황의 발생을 통지 받은 센서부(301)는 촬영된 원본 이미지와 긴급 상황의 발생과 관련된 정보를 처리부(303)로 전송한다.(312단계) 상기 긴급 상황의 발생과 관련된 정보는 일례로 긴급 상황이 발생되었음을 지시하는 지시자, 긴급 상황의 발생과 관련된 특정 비트 등이 될 수 있다. 312단계에서 원본 이미지를 긴급 상황의 발생과 관련된 정보와 함께 전송하는 이유는 이후 절차에서 원본 이미지 즉 현재 긴급 상황에 대한 정확한 정보 가 신속하게 전송되도록 하기 위함이다.

[0052] 처리부(303)는 센서부(301)로부터 전송되는 원본 이미지를 저장함과 동시에 처리한다.(314단계) 상기 원본 이미지의 처리에는 일례로 필터링 방식, 마스킹 방식, 연산 처리 방식 등이 사용될 수 있다. 일례로 처리부(303)는 원본 이미지에서 타겟 촬영 대상, 일례로 사람을 제외한 배경이 제외되도록 처리할 수 있고, 상기 원본 이미지에서 모든 촬영 대상들의 윤곽선만이 남도록 처리할 수 있고, 상기 원본 이미지를 스무딩 기법을 기반으로 상기 모든 촬영 대상들이 흐릿해지도록 처리할 수 있고, 또는 쉬프트 연산, 컨벌루셔널 연산 등을 통해 상기 원본 이미지에서 상기 타겟 촬영 대상을 제외한 배경이 다른 배경으로 교체되도록 처리할 수 있다.

[0053] 한편 처리부(303)는 센서부(301)로부터 긴급 상황의 발생과 관련된 정보가 수신될 경우, 314단계의 처리 동작을 수행하지 않고 원본 이미지 그대로 사용자 기기(305), 응급센터(307), 주변 사용자 기기(309) 각각에 전송한다. 따라서 긴급 상황에서의 처리 동작(314 단계)은 상기 원본 이미지를 사용자 기기(305), 응급센터(307), 주변 사

용자 기기(309) 각각에 전송하는 과정과 동시에 수행되거나 생략될 수 있다.

[0054] 즉 센서부(301)로부터 긴급 상황의 발생과 관련된 정보를 수신한 처리부(303)는 원본 이미지와 긴급 상황의 발생과 관련된 정보를 사용자 기기(305), 일례로 단말, 웨어러블 기기, 이-헬스 기기 등으로 전송한다.(316단계)

[0055] 또한 센서부(301)로부터 긴급 상황의 발생과 관련된 정보를 수신한 처리부(303)는 원본 이미지와 긴급 상황의 발생과 관련된 정보를 응급센터(307)로 전송한다.(318단계) 이때 처리부(303)는 응급센터에서 환자에 대한 응급처치가 가능하도록 환자 ID, 환자의 웨어러블 기기 ID, 및 환자의 이-헬스 기기 ID 중 적어도 하나를 응급센터(307)로 전송할 수 있다. 318단계에서 처리부(303)의 전송 동작은 처리부(303)에 등록된 응급센터의 ID 또는 IP 주소(address), 또는 사용자 기기(305)로부터 전송 받은 응급센터의 ID 또는 IP 주소 등을 이용하여 수행된다.

[0056] 또한 센서부(301)로부터 긴급 상황의 발생과 관련된 정보를 수신한 처리부(303)는 원본 이미지와 긴급 상황의 발생과 관련된 정보를 주변 사용자 기기(309)로 전송한다.(320단계) 상기 주변 사용자 기기(309)는 환자의 가족, 친지, 이웃 등의 사용자 기기가 될 수 있으며, 320단계에서 처리부(303)의 전송 동작은 처리부(303)에 등록된 환자의 가족, 친지, 이웃 등의 통신 ID 또는 IP 주소, 또는 사용자 기기(305)로부터 전송 받은 환자의 가족, 친지, 이웃 등의 통신 ID 또는 IP 주소 등을 이용하여 수행된다.

[0057] 도 3에서는 316단계, 318단계, 및 320단계의 동작이 순차적으로 진행되는 것을 일례로 설명하였으나, 316단계, 318단계, 및 320단계의 동작은 병렬적으로 진행될 수도 있다.

[0058] 응급센터(307)는 처리부(303)로부터 전송되는 긴급 상황의 발생과 관련된 정보를 확인하고, 추가적으로 전송되는 환자 ID, 환자의 웨어러블 기기 ID, 및 환자의 이-헬스 기기 ID 등을 인증한다.(322단계)

[0059] 이후 응급센터(307)는 304단계에서 수신된 환자에 대한 정보와 320단계에서 수신된 원본 이미지와 같은 긴급 상황 정보를 처리한다. 상기 처리된 긴급 상황 정보는 환자에게 가장 적절한 응급처치를 실행하기 위해 사용될 수 있다. 즉 환자에게 필요한 의료진을 보내거나 구급차를 보내는 등의 응급처치를 수행하는데 사용될 수 있다.

[0060] 도 4는 본 발명의 일 실시예에 따라 처리된 이미지의 변조를 검출하는 절차의 예를 나타낸 신호 흐름도이다.

[0061] 도 4를 참조하면, 도시된 신호 흐름도는 이미지를 촬영하는 센서부(401), 촬영된 이미지를 처리하는 처리부(403) 및 이미지를 수신하는 사용자 기기(405)를 포함한다. 도 4에서는 센서부(401), 처리부(403) 및 사용자 기기(405) 각각이 별도의 유닛으로 구성된 경우를 일례로 설명한다. 그러나 센서부(401)와 처리부(403)는 경우에 따라 하나의 유닛으로 구성될 수도 있고 또는 센서(401), 처리부(403) 및 사용자 기기(405) 모두가 하나의 유닛으로 구성될 수도 있다.

[0062] 홈 네트워크 시스템을 가정하면, 상기 센서부(401)는 일례로 각종 카메라 또는 홈 디바이스에 결합된 카메라 등이 될 수 있고, 상기 사용자 기기(405)는 일례로 단말이나 홈 네트워크 시스템의 제어 유닛 등이 될 수 있다.

[0063] 사용자 기기(405)는 처리부(403)로 이미지 또는 개인 정보의 전송을 요청하는 요청 메시지를 전송한다.(400단계) 처리부(403)는 상기 요청 메시지를 전송한 사용자 기기(405)를 인증한다.(402단계) 즉 사용자 기기(405)가 인증된 기기인지 확인한다. 여기서 요청 메시지를 센서부(401)가 아닌 처리부(403)로 전송하는 이유는 사용자 기기(405)가 센서부(401)가 촬영한 원본 이미지에 접근하는 것을 방지하고 처리부(403)를 통해 처리된 이미지에만 접근할 수 있도록 함으로써 보안과 프라이버시 보호를 강화하기 위함이다.

[0064] 또 다른 예로 사용자 기기(405)는 400단계에서 요청 메시지에 이미지 허용 레벨에 관련된 정보를 포함시켜 전송할 수도 있다. 이 경우 처리부(403)는 400단계에서 요청 메시지를 전송한 사용자 기기(405)가 인증된 기기인지 확인할 때, 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보의 검증도 함께 수행한다. 이미지 허용 레벨에 관련된 정보의 검증 과정은 사용자 기기(405)가 조회를 요청한 이미지 허용 레벨, 즉 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨과 상기 사용자 기기(405)에게 정책상 허용된 이미지 허용 레벨을 비교하는 방법 등이 사용될 수 있다.

[0065] 402단계의 사용자 기기 확인 및/또는 이미지 허용 레벨 검증 과정은 사용자 기기(405)의 네트워크 환경, 일례로 이동 통신 환경, 셀룰러 통신 환경, 블루투스 환경, 와이파이 환경 등에 따라 다양한 방법이 사용될 수 있으므로, 본 발명에서의 사용자 기기 확인 및/또는 이미지 허용 레벨 검증 과정에 사용되는 방법은 다양한 네트워크 환경에 따르도록 한다.

[0066] 처리부(403)는 사용자 기기 확인 및/또는 이미지 허용 레벨 검증이 완료되면, 이미지 또는 개인 정보의 전송을

요청하는 요청 메시지를 센서부(401)로 전송한다.(404단계) 이때 상기 요청 메시지에는 센서부(401)가 사용자 기기(405)에서의 데이터 변조를 검출할 수 있도록, 사용자 기기(405)의 ID, IP 주소, 통신 ID등과 같은 사용자 기기(405)에 관련된 정보가 포함될 수 있다.

[0067] 처리부(403)로부터 요청 메시지를 수신한 센서부(401)는 촬영된 원본 이미지를 처리부(403)에 전송한다.(406단계)

[0068] 처리부(403)는 상기 원본 이미지를 저장함과 동시에 혹은 저장한 후 처리한다.(408단계) 상기 원본 이미지의 처리에는 일례로 필터링 방식, 마스킹 방식, 연산 처리 방식 등이 사용될 수 있다. 즉 처리부(403)는 원본 이미지에 관련된 데이터를 분할하여 암호화하며, 특히 상기 원본 이미지에 관련된 데이터를 보안 등급과 이미지 허용 레벨 등에 따라 촬영 대상만을 포함하는 정보, 배경만을 포함하는 정보, 배경과 촬영 대상 모두를 포함하는 정보, 배경과 촬영 대상 모두를 포함하는 정보를 암호화한 정보 등으로 처리한다.

[0069] 일례로 처리부(403)는 원본 이미지에서 타겟 촬영 대상, 일례로 사람을 제외한 배경이 제외되도록 처리할 수 있고, 상기 원본 이미지에서 모든 촬영 대상들의 윤곽선만이 남도록 처리할 수 있고, 상기 원본 이미지를 스무딩 기법을 기반으로 상기 모든 촬영 대상들이 흐릿해지도록 처리할 수 있고, 또는 쉬프트 연산, 컨벌루셔널 연산 등을 통해 상기 원본 이미지에서 상기 타겟 촬영 대상을 제외한 배경이 다른 배경으로 교체되도록 처리할 수 있다.

[0070] 센서부(401)는 사용자 기기(405)에서의 데이터 변조를 검증 할 수 있도록, 원본 이미지 전송에 관련된 정보, 일례로 타임 스탬프(time stamp) 또는 난수 등에 관련된 정보를 사용자 기기(405)로 전송한다.(410단계)

[0071] 이후 처리부(403)는 400단계에서 수신된 요청 메시지에 포함된 이미지 허용 레벨에 관련한 정보가 지시하는 이미지 허용 레벨을 기반으로 처리된 이미지를 사용자 기기(405)에게 전송한다.(412단계) 여기서는 요청 메시지에 이미지 허용 레벨에 관련된 정보가 포함되는 경우를 일례로 설명하였다. 그러나 상기 요청 메시지에 상기 이미지 허용 레벨에 관련된 정보가 포함되지 않을 경우, 처리부(403)는 디폴트 값의 이미지 허용 레벨을 기반으로 처리된 이미지를 사용자 기기(405)에게 전송한다. 디폴트 값의 이미지 허용 레벨은 사용자에 의해 설정되어 있거나 가장 강력한 이미지 허용 레벨일 수 있다.

[0072] 사용자 기기(405)는 412단계에서 수신한 처리된 이미지의 변조 여부를 검증한다.(414단계) 414단계의 검증 동작은 410단계에서 수신된 타임 스탬프, 난수 등에 관련된 정보를 이용하여 수행된다. 즉 사용자 기기(405)는410단계에서 수신된 원본 이미지 전송에 관련된 정보가 지시하는 타임 스탬프 및 난수를 412단계에서 수신된 처리된 이미지에 대한 타임 스탬프 및 난수와 비교하고, 상기 원본 이미지의 타임 스탬프 및 난수가 상기 처리된 이미지의 타임 스탬프 및 난수와 상이할 경우, 상기 처리된 이미지가 변조된 것으로 간주한다. 이후 사용자 기기(405)는 412단계에서 수신된 처리된 이미지를 신뢰하지 않으며, 처리부(403)의 전송 과정에 대한 에러 검출(detection) 동작을 수행한다.

[0073] 한편, 사용자 기기(405)는 처리부(403)로 레벨 업 요청 메시지를 전송하여(416단계), 412단계에서 수신한 처리된 이미지보다 세밀화된 이미지 전송을 요청한다. 이때 상기 레벨 업 요청 메시지에는 400단계에서 전송한 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨보다 높은 이미지 허용 레벨에 관련된 정보가 포함된다. 본 발명의 실시예에서는 상기 이미지 허용 레벨이 높을수록 원본 이미지와 유사한 처리된 이미지에 대한 접근을 허용한다고 가정한다.

[0074] 처리부(403)는 상기 레벨 업 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보를 검증한다.(418단계) 그런 다음 처리부(403)는 상기 이미지 허용 레벨에 관련된 정보의 검증이 완료되면, 사용자 기기(405)에게 처리된 이미지를 전송한다.(420단계) 420단계에서 처리된 이미지는 레벨 업 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨을 기반으로 처리된 이미지를 의미한다.

[0075] 도 5는 처리부가 본 발명의 일 실시예에 따라 처리된 이미지를 사용자 기기에게 전송하는 과정을 나타낸 순서도이다.

[0076] 도 5를 참조하면, 501단계에서 처리부는 센서부로부터 촬영된 원본 이미지를 수신하고, 503단계에서 상기 원본 이미지를 미리 정해진 프라이버시 레벨들을 기반으로 처리한다. 상기 원본 이미지의 처리에는 일례로 필터링 방식, 마스킹 방식, 연산 처리 방식 등이 사용될 수 있다.

[0077] 505단계에서 처리부는 사용자 기기로부터 이미지 또는 개인 정보의 전송을 요청하는 요청 메시지를 수신한다.

507단계에서 처리부는 상기 요청 메시지를 전송한 사용자 기기를 인증한다. 즉 상기 사용자 기기가 인증된 기기인지 확인한다.

[0078] 509단계에서 처리부는 상기 505단계에서 수신한 요청 메시지에 제1 프라이버시 레벨에 관련된 정보가 포함되는지 여부를 검사한다. 509단계의 검사 결과 상기 요청 메시지에 상기 제1 프라이버시 레벨에 관련된 정보가 포함되면, 처리부는 511단계로 진행하여 상기 제1 프라이버시 레벨에 관련된 정보가 지시하는 제1 프라이버시 레벨을 검증한다. 513단계에서 처리부는 상기 검증한 제1 프라이버시 레벨을 기반으로 처리된 이미지를 사용자 기기에게 전송한다.

[0079] 509단계 검사 결과 상기 요청 메시지에 상기 제1 프라이버시 레벨에 관련된 정보가 포함되지 않으면, 처리부는 515단계로 진행하여 디폴트 값의 프라이버시 레벨을 기반으로 처리된 이미지를 사용자 기기에게 전송한다. 디폴트 값의 프라이버시 레벨은 사용자에 의해 설정되어 있거나 가장 강력한 프라이버시 레벨일 수 있다.

[0080] 한편, 517단계에서 처리부는 513단계에서 전송되는 처리된 이미지보다 세밀화된 원본 이미지에 가까운 이미지 전송을 요청하는 레벨 업 이미지 요청 메시지가 수신되는지 여부를 검사한다. 이때 517단계의 검사 결과 사용자 기기로부터 상기 레벨 업 이미지 요청 메시지가 수신되지 않으면 처리부는 진행중인 동작을 종료한다.

[0081] 그러나 517단계의 검사 결과 사용자 기기로부터 상기 레벨 업 이미지 요청 메시지가 수신되면, 처리부는 519단계로 진행하여 상기 레벨 업 이미지 요청 메시지에 포함된 제2 프라이버시 레벨에 관련된 정보가 지시하는 제2 프라이버시 레벨을 검증한다. 여기서 상기 제2 프라이버시 레벨은 상기 제1 프라이버시 레벨보다 원본 이미지에 근접한 이미지에 대한 접근을 허용하는 레벨을 의미한다. 521단계에서 처리부는 상기 제2 프라이버시 레벨을 기반으로 처리된 이미지를 사용자 기기에게 전송한다.

[0082] 도 5에서는 처리부가 원본 이미지 처리를 수행한 이후 사용자 기기로부터 요청 메시지를 수신하는 동작을 일례로 설명하였다. 그러나 상기 원본 이미지를 처리하는 단계, 즉 503단계는 요청 메시지를 수신한 이후에 수행될 수도 있다. 이 경우 처리부는 사용자 기기로부터 프라이버시 레벨에 관련된 정보가 포함된 요청 메시지를 수신하고, 상기 요청 메시지에 포함된 이미지 허용 레벨에 관련된 정보가 지시하는 이미지 허용 레벨을 기반으로 원본 이미지를 처리한다.

[0083] 도 6은 처리부가 본 발명의 일 실시예에 따라 긴급 상황에 원본 이미지를 사용자 기기, 응급 센터 및 주변 사용자 기기에 전송하는 과정을 도시한 순서도이다.

[0084] 도 6을 참조하면, 601단계에서 처리부는 사용자 기기로부터 이미지 또는 개인 정보의 전송을 요청하는 요청 메시지를 수신하고, 603단계에서 상기 요청 메시지를 전송한 사용자 기기가 인증된 기기인지 확인한다.

[0085] 605단계에서 처리부는 상기 601단계에서 수신한 요청 메시지에 긴급 상황 발생과 관련된 정보가 포함되는지 여부를 검사한다. 여기서는 홈 네트워크 시스템에서 집안의 환자에게 건강상의 문제가 발생된 경우의 긴급 상황을 가정하여 설명하며, 상기 긴급 상황 발생과 관련된 정보는 일례로 긴급 상황이 발생되었음을 지시하는 지시자, 긴급 상황의 발생과 관련된 특정 비트 등이 될 수 있다. 이때 605단계의 검사 결과 상기 요청 메시지에 상기 긴급 상황 발생과 관련된 정보가 포함되지 않으면, 처리부는 601단계로 진행하여 요청 메시지 수신을 대기한다.

[0086] 605단계의 검사 결과 상기 요청 메시지에 상기 긴급 상황 발생과 관련된 정보가 포함되면, 처리부는 607단계로 진행하여 센서부에게 긴급 상황 발생과 관련된 정보가 포함된 요청 메시지를 전송한다.

[0087] 609단계에서 처리부는 상기 요청 메시지에 대한 응답으로 센서부로부터 촬영된 원본 이미지와 긴급 상황 발생과 관련된 정보를 수신한다. 611단계에서 처리부는 상기 수신한 원본 이미지와 긴급 상황 발생과 관련된 정보를 사용자 기기, 응급센터, 주변 사용자 기기 중 적어도 하나에 전송한다. 이때 처리부는 응급센터에서 환자에 대한 응급처치가 가능하도록 환자 ID, 환자의 웨어러블 기기 ID, 및 환자의 이-헬스 기기 ID 중 적어도 하나를 추가로 전송할 수 있다.

[0088] 도 7은 본 발명의 일 실시예에 따라 데이터 보안을 강화하는 처리부의 내부 구성을 나타낸 블록도이다.

[0089] 도 7을 참조하면, 도시된 처리부(700)는 별도의 유닛으로 도시하였으나, 처리부(700)와 센서부와 사용자 기기는 적용 예에 따라 각각이 별도의 유닛으로 구성될 수도 있고, 센서부와 처리부(700)가 하나의 유닛으로 구성될 수도 있고, 센서부, 처리부(700), 사용자 기기 모두가 하나의 유닛으로 구성될 수도 있다.

[0090] 도시된 처리부(700)는 송수신 모듈(702)과 처리 모듈(704)을 포함한다. 상기 처리 모듈(704)은 상기 처리부(700)의 전반적인 동작에 관여하여 한다. 특히 처리 모듈(704)은 본 발명의 일 실시예에 따른 데이터 보안 강화와 관련된 전반적인 동작을 수행하도록 한다. 여기서 데이터 보안 강화와 관련된 전반적인 동작에 대해서는 도 1 내지 도 6에서 설명한 바와 동일하므로, 여기서는 그 상세한 설명을 생략하도록 한다.

[0091] 상기 송수신 모듈(702)은 상기 처리 모듈(704)의 제어에 따라 각종 메시지 등을 전송한다. 여기서 상기 송수신 모듈(702)이 전송하는 각종 메시지 등은 도 1 내지 도 6에서 설명한 바와 동일하므로, 여기서는 그 상세한 설명을 생략하도록 한다.

[0092] 도 8a 내지 도 8c는 본 발명의 일 실시예에 따라 데이터 보안을 강화하는 처리부를 구현하는 예를 나타낸 도면이다. 도 8a는 센서부(801)와 처리부(803)가 하나의 유닛(800)으로 구성되는 예를 나타내었다. 여기서 상기 처리부(803)는 센서로부터 데이터를 입력, 또는 수신 받는 입력 모듈(805), 처리 모듈(807) 및 사용자 기기의 디스플레이 등으로 데이터를 전송하는 송신 모듈(809)을 포함한다.

[0093] 도 8a의 구성 예는 카메라 등과 같은 센서가 장착된 로봇 청소기 또는 상기 센서가 장착된 냉장고 등에 적용될 수 있다. 별도의 엔티티로 구분된 사용자 기기(811)는 일례로 웨어러블 기기, 이-헬스 기기 등의 전자 기기가 될 수 있다.

[0094] 도 8b는 센서부(820), 처리부(831), 사용자 기기(841)가 각각의 유닛(830,840,850)으로 구성되는 예를 나타내었다. 여기서 상기 처리부(831)는 입력 모듈(833), 처리 모듈(835) 및 송신 모듈(837)을 포함한다.

[0095] 도 8b의 구성 예는 개인 정보 데이터의 보안, 사생활 보호 측면에서 별도의 엔티티로 구분하여 운영하는 경우에 적용된다. 별도의 엔티티로 구분된 사용자 기기(841)는 일례로 웨어러블 기기, 이-헬스 기기 등의 전자 기기가 될 수 있다. 도 3의 사용자 기기(305)는 별도의 엔티티로 구분된 사용자 기기에 해당한다.

[0096] 만약 사용자 기기(841)가 별도의 엔티티로 구분되지 않고 다른 기능 블록과 함께 구성된다고 가정하면, 이 경우 사용자 기기(851)는 일례로 스마트폰 등이 될 수 있다. 도 1의 사용자 기기(105)는 다른 기능 블록과 함께 구성된 사용자 기기에 해당한다.

[0097] 도 8c는 센서부(851), 처리부(853), 사용자 기기(861) 모두가 하나의 유닛(850)으로 구성되는 예를 나타내었다. 여기서 상기 처리부(853)는 입력 모듈(855), 처리 모듈(857) 및 사용자 기기의 디스플레이 등이 한 유닛 안에 들어 있어 데이터를 디스플레이 부분으로 전송하는 출력 모듈(859) 혹은 송신 모듈을 포함한다. 구현에 따라서 내부 인터페이스 형태로 구현되면 출력 모듈 형태로 구현되고, 데이터 전송을 하는 형태로 구현되면 송신 모듈의 특성을 지니는 형태로 구현된다.

[0098] 도 8c의 구성 예는 스마트폰, 모바일폰, 태블릿 기기 등과 같은 디바이스나 고성능/고사양의 웹캠 또는 로봇 청소기 등과 같이 이동성이 있는 디바이스 등에 적용될 수 있다

[0099] 한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 안되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

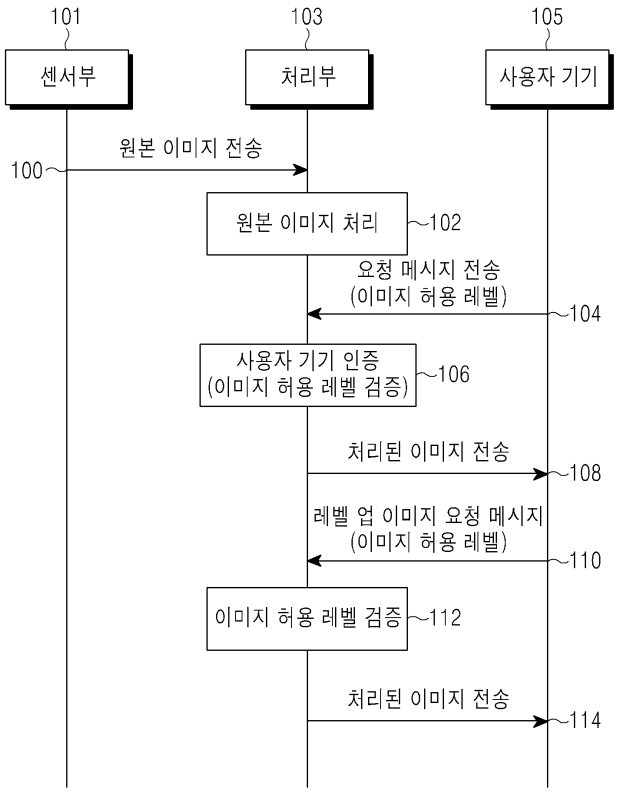
[0100] 또한 본 발명의 실시예에 따른 데이터 보안 강화 방법 및 장치는 하드웨어, 소프트웨어 또는 하드웨어 및 소프트웨어의 조합의 형태로 실현 가능하다는 것을 알 수 있을 것이다. 이러한 임의의 소프트웨어는 예를 들어, 삭제 가능 또는 재기록 가능 여부와 상관없이, ROM 등의 저장 장치와 같은 휘발성 또는 비휘발성 저장 장치, 또는 예를 들어, RAM, 메모리 칩, 장치 또는 집적 회로와 같은 메모리, 또는 예를 들어 CD, DVD, 자기 디스크 또는 자기 테이프 등과 같은 광학 또는 자기적으로 기록 가능함과 동시에 기계(예를 들어, 컴퓨터)로 읽을 수 있는 저장 매체에 저장될 수 있다. 본 발명의 그래픽 화면 갱신 방법은 제어부 및 메모리를 포함하는 컴퓨터 또는 휴대 단말에 의해 구현될 수 있고, 상기 메모리는 본 발명의 실시 예들을 구현하는 지시들을 포함하는 프로그램 또는 프로그램들을 저장하기에 적합한 기계로 읽을 수 있는 저장 매체의 한 예임을 알 수 있을 것이다.

[0101] 따라서, 본 발명은 본 명세서의 임의의 청구항에 기재된 장치 또는 방법을 구현하기 위한 코드를 포함하는 프로그램 및 이러한 프로그램을 저장하는 기계(컴퓨터 등)로 읽을 수 있는 저장 매체를 포함한다. 또한, 이러한 프로그램은 유선 또는 무선 연결을 통해 전달되는 통신 신호와 같은 임의의 매체를 통해 전자적으로 이송될 수 있고, 본 발명은 이와 균등한 것을 적절하게 포함한다

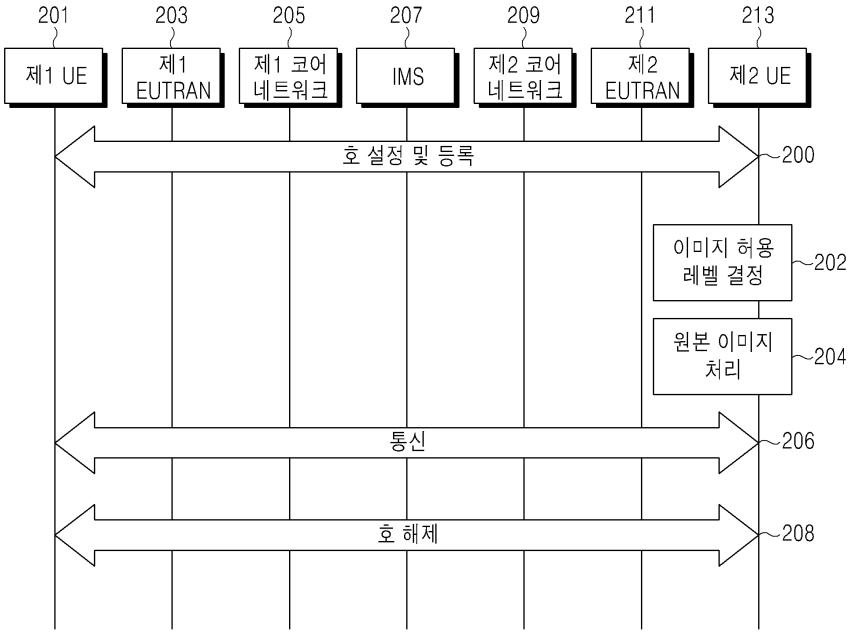
[0102] 또한 본 발명의 실시예에서는 데이터 보안을 강화하는 장치로부터 상기 프로그램을 수신하여 저장할 수 있다. 상기 프로그램 제공 장치는 그래픽 처리 장치가 기 설정된 컨텐츠 보호 방법을 수행하도록 하는 지시들을 포함하는 프로그램, 컨텐츠 보호 방법에 필요한 정보 등을 저장하기 위한 메모리와, 상기 그래픽 처리 장치와의 유선 또는 무선 통신을 수행하기 위한 통신부와, 상기 그래픽 처리 장치의 요청 또는 자동으로 해당 프로그램을 상기 송수신 장치로 전송하는 제어부를 포함할 수 있다.

도면

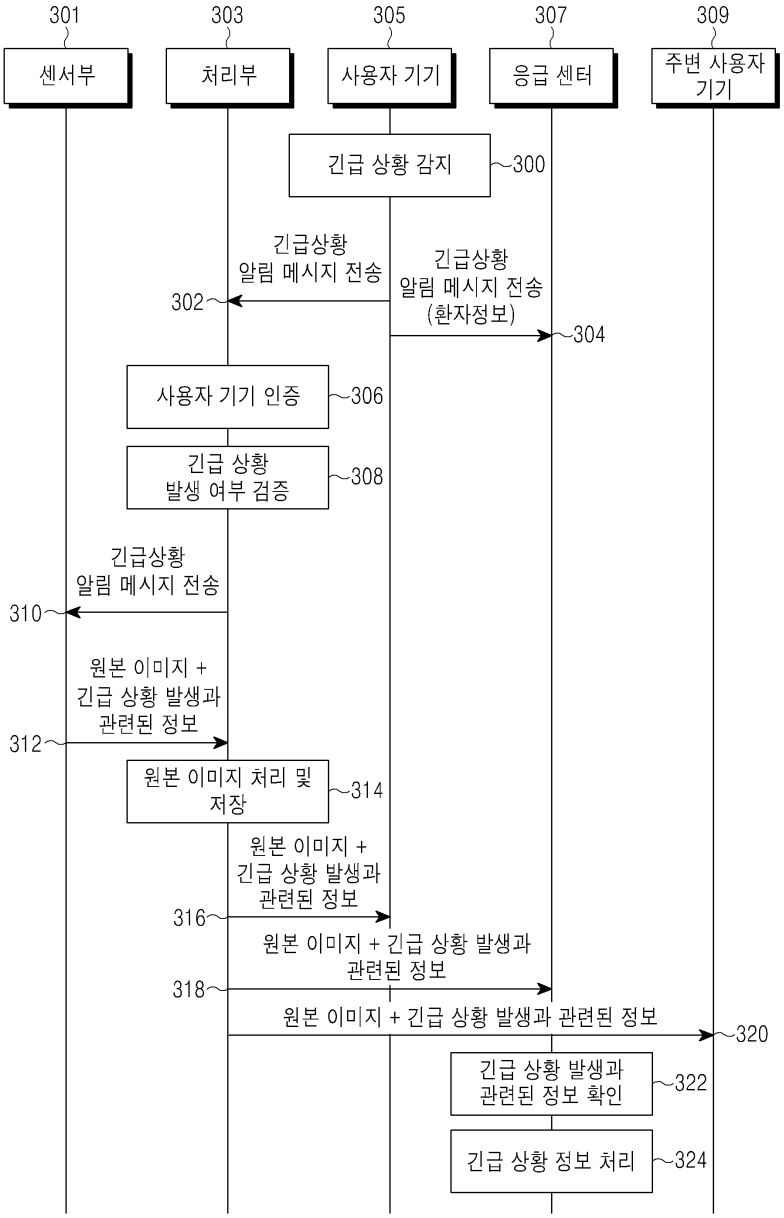
도면1



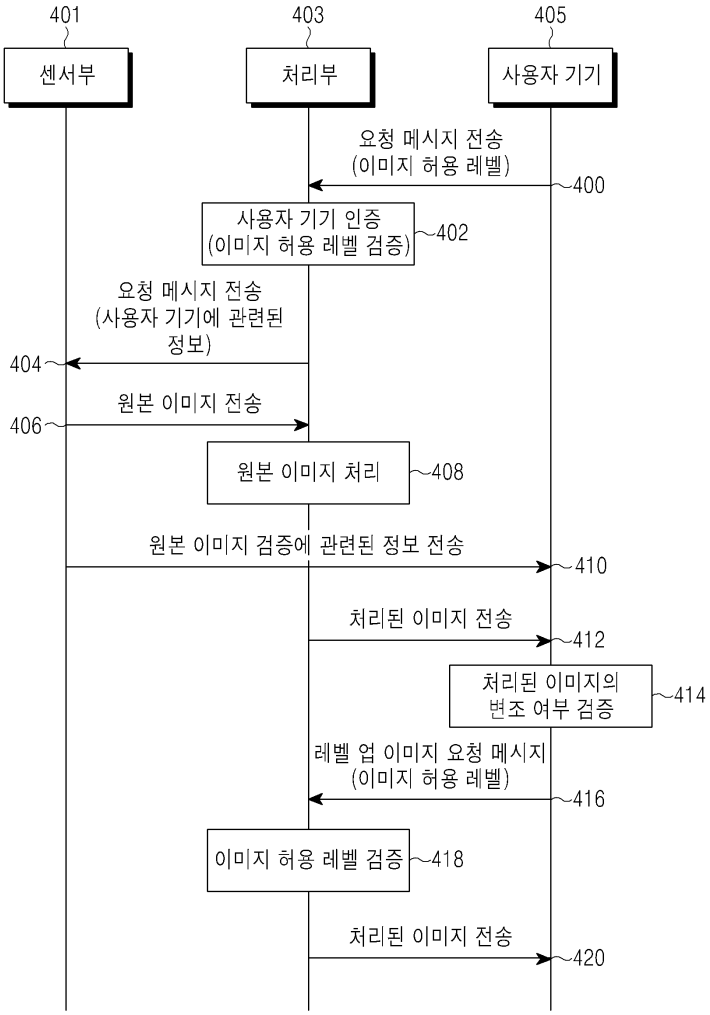
도면2


201
203
205
207
209
211
213
제1 UE
제1 EUTRAN
제1 코어 네트워크
IMS
제2 코어 네트워크
제2 EUTRAN
제2 UE
호 설정 및 등록
200
이미지 허용 레벨 결정
202
원본 이미지 처리
204
통신
206
호 해제
208

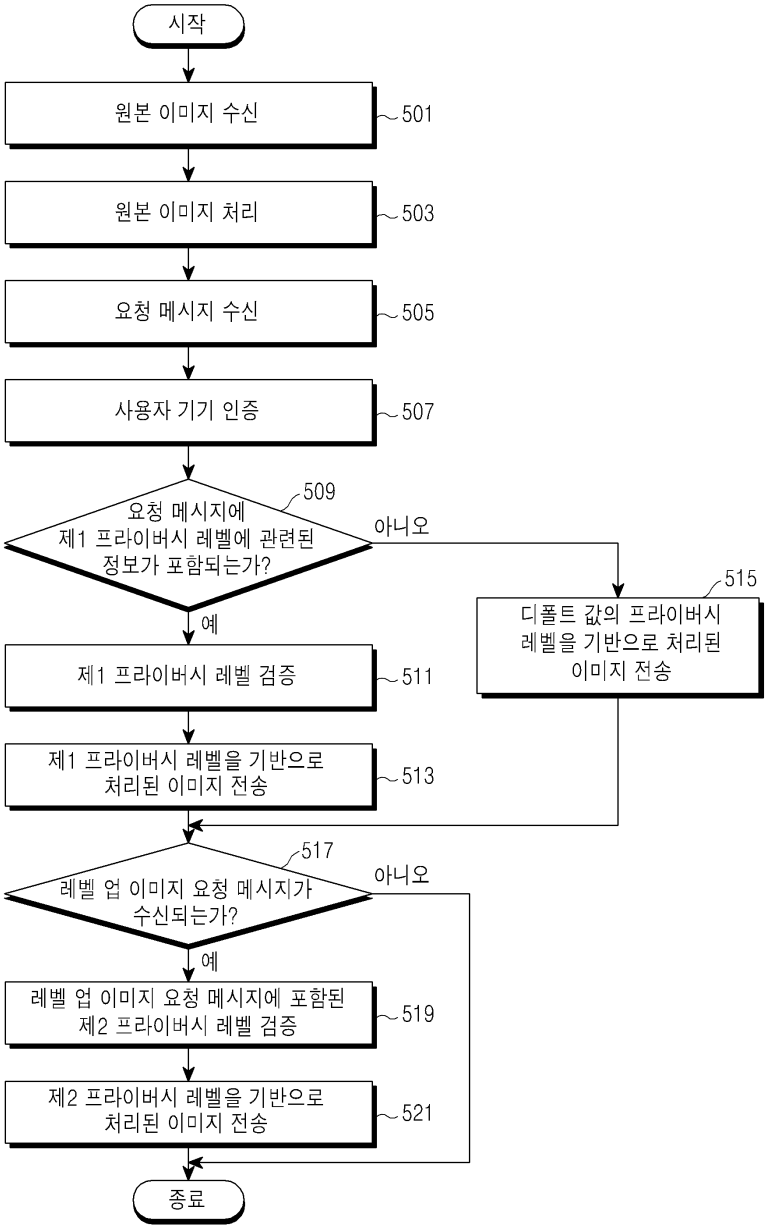
도면3


301
303
305
307
309
센서부
처리부
사용자 기기
응급 센터
주변 사용자 기기
긴급 상황 감지
300
긴급상황 알림 메시지 전송
302
긴급상황 알림 메시지 전송 (환자정보)
304
사용자 기기 인증
306
긴급 상황 발생 여부 검증
308
긴급상황 알림 메시지 전송
310
원본 이미지 + 긴급 상황 발생과 관련된 정보
312
원본 이미지 처리 및 저장
314
원본 이미지 + 긴급 상황 발생과 관련된 정보
316
원본 이미지 + 긴급 상황 발생과 관련된 정보
318
원본 이미지 + 긴급 상황 발생과 관련된 정보
320
긴급 상황 발생과 관련된 정보 확인
322
긴급 상황 정보 처리
324

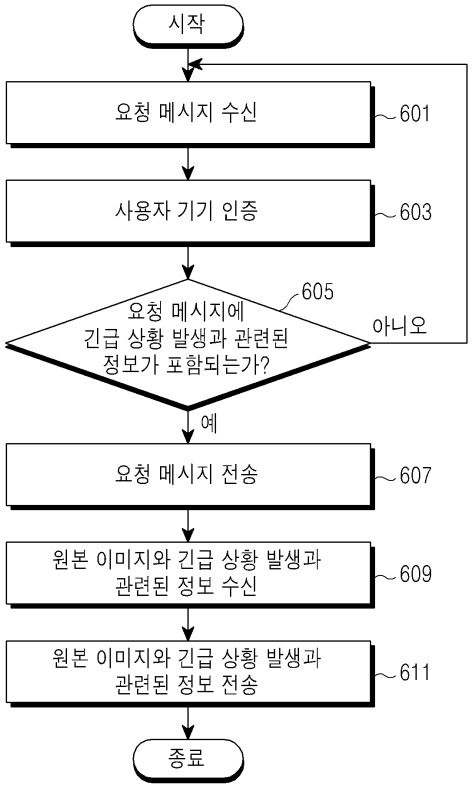
도면4


401
403
405
센서부
처리부
사용자 기기
요청 메시지 전송
(이미지 허용 레벨)
400
사용자 기기 인증
(이미지 허용 레벨 검증)
402
요청 메시지 전송
(사용자 기기에 관련된
정보)
404
원본 이미지 전송
406
원본 이미지 처리
408
원본 이미지 검증에 관련된 정보 전송
410
처리된 이미지 전송
412
처리된 이미지의
변조 여부 검증
414
레벨 업 이미지 요청 메시지
(이미지 허용 레벨)
416
이미지 허용 레벨 검증
418
처리된 이미지 전송
420

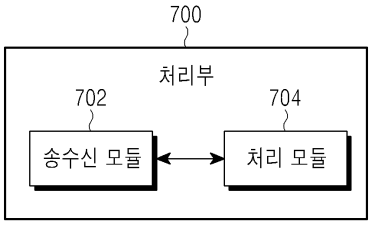
도면5


시작
원본 이미지 수신
501
원본 이미지 처리
503
요청 메시지 수신
505
사용자 기기 인증
507
509
요청 메시지에
제1 프라이버시 레벨에 관련된
정보가 포함되는가?
아니오
예
515
디폴트 값의 프라이버시
레벨을 기반으로 처리된
이미지 전송
제1 프라이버시 레벨 검증
511
제1 프라이버시 레벨을 기반으로
처리된 이미지 전송
513
517
레벨 업 이미지 요청 메시지가
수신되는가?
아니오
예
레벨 업 이미지 요청 메시지에 포함된
제2 프라이버시 레벨 검증
519
제2 프라이버시 레벨을 기반으로
처리된 이미지 전송
521
종료

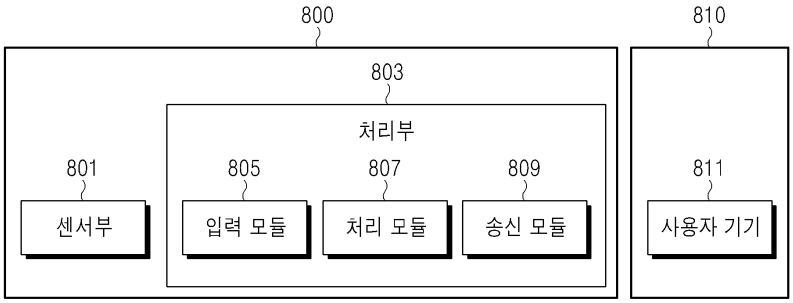
도면6


시작
요청 메시지 수신
601
사용자 기기 인증
603
605
요청 메시지에
긴급 상황 발생과 관련된
정보가 포함되는가?
아니오
예
요청 메시지 전송
607
원본 이미지와 긴급 상황 발생과
관련된 정보 수신
609
원본 이미지와 긴급 상황 발생과
관련된 정보 전송
611
종료

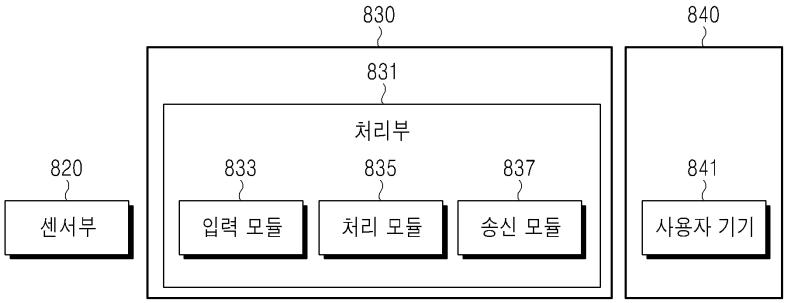
도면7


700
처리부
702
704
송수신 모듈
처리 모듈

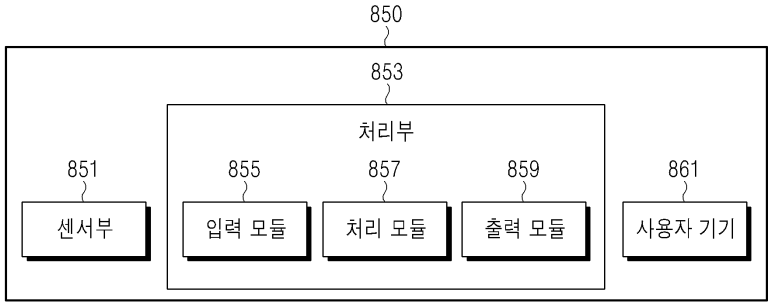
도면8a


800
810
803
처리부
801
805
807
809
811
센서부
입력 모듈
처리 모듈
송신 모듈
사용자 기기

도면8b


830
840
831
처리부
820
833
835
837
841
센서부
입력 모듈
처리 모듈
송신 모듈
사용자 기기

도면8c


850
853
처리부
851
855
857
859
861
센서부
입력 모듈
처리 모듈
출력 모듈
사용자 기기