



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0030251
(43) 공개일자 2023년03월06일

(51) 국제특허분류(Int. Cl.)
G06T 11/60 (2006.01) G06F 18/00 (2023.01)
G06F 21/62 (2013.01) G06T 3/00 (2019.01)
G06T 7/11 (2017.01) H04N 21/431 (2016.01)
(52) CPC특허분류
G06T 11/60 (2013.01)
G06F 21/6245 (2013.01)
(21) 출원번호 10-2021-0112251
(22) 출원일자 2021년08월25일
심사청구일자 2021년08월25일

(71) 출원인
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
김시호
인천광역시 연수구 송도과학로 85, Faculty House D동 912호(송도동)
차재광
인천광역시 연수구 송도과학로27번길 15, 103동 3406호(송도동, 송도아메리칸타운아이파크)
(74) 대리인
특허법인우인

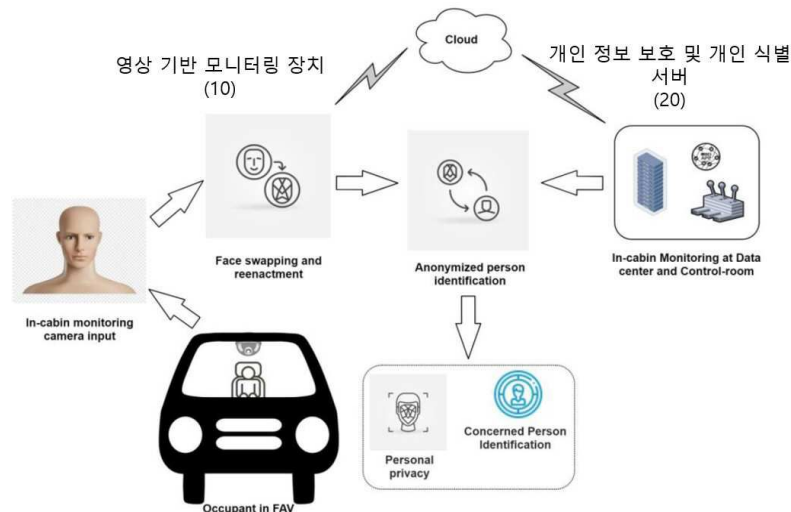
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 안면 정보 익명화 및 재식별 기능 기반 개인 정보 보호 기능을 제공하는 감시 또는 관찰 시스템

(57) 요약

본 실시 예들은 관찰 영상을 획득하는 과정에서 영상 원본을 저장하는 것이 아닌 인공지능 기술을 통해 피관찰자의 얼굴을 제3의 얼굴로 합성 또는 변환하여 익명화된 영상을 저장하고, 피관찰자 익명화 전 원본 영상으로부터 피관찰자 얼굴의 특징을 내포하며 원래 얼굴로는 복원 불가능한 식별자 특징 정보를 추출하여 익명화된 영상과 동시에 저장하는 방식을 통해 필요 상황에서 익명화된 피관찰자 신원을 재식별할 수 있는 개인 정보 보호 및 개인 식별을 위한 감시 또는 관찰 시스템을 제공한다.

대표도 - 도3



(52) CPC특허분류

G06T 3/00 (2019.01)

G06T 7/11 (2017.01)

G06V 40/168 (2022.01)

H04N 21/4318 (2013.01)

G06T 2207/30201 (2013.01)

G06T 2207/30232 (2013.01)

이 발명을 지원한 국가연구개발사업

| | |
|-------------|--|
| 과제고유번호 | 1711126107 |
| 과제번호 | 2017-0-00244-005 |
| 부처명 | 과학기술정보통신부 |
| 과제관리(전문)기관명 | 정보통신기획평가원 |
| 연구사업명 | 정보통신방송연구개발사업 |
| 연구과제명 | HMD 표정 인식 센서와 사이버 인터랙션 인터페이스 기술 (창조씨앗형 2단계)(4/5) |
| 기 여 율 | 1/1 |
| 과제수행기관명 | 연세대학교 산학협력단 |
| 연구기간 | 2021.01.01 ~ 2021.12.31 |

명세서

청구범위

청구항 1

개인 정보 보호 및 개인 식별 기능을 포함하는 영상 기반 모니터링 장치에 있어서,

원본 얼굴과 선별된 소스 얼굴을 합성 또는 변환하여 제1 익명화 얼굴을 생성하고, 상기 원본 얼굴의 식별자 특징 정보 및 제1 익명화 얼굴의 식별자 특징 정보를 매칭하여 식별자 특징 정보 쌍을 생성하는 프로세서; 및

상기 식별자 특징 정보 쌍을 개인 정보 보호 및 개인 식별 서버로 전송하는 통신 인터페이스를 포함하는 영상 기반 모니터링 장치.

청구항 2

제1항에 있어서,

상기 프로세서는 영상 장치를 통해 하나 이상의 피관찰자를 촬영한 관찰 영상을 획득하고, 상기 관찰 영상에서 상기 원본 얼굴을 검출하고 상기 검출된 원본 얼굴로부터 식별자 특징 정보를 추출하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 3

제2항에 있어서,

상기 영상 장치는 자율주행 자동차 또는 일반 자동차, 감시가 필요한 장소에 설치되는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 4

제2항에 있어서,

상기 프로세서는 (i) 프레임별 주기적인 시점에, (ii) 탑승 후 일회적인 시점에, (iii) 특정 행동이나 특정 상황이 발생한 시점에, (iv) 특정 표정이 검출되거나 얼굴 영역의 기준 크기를 만족하는 시점에, 또는 이들이 조합된 시점에, 상기 원본 얼굴을 검출하고 상기 검출된 원본 얼굴로부터 식별자 특징 정보를 추출하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 5

제1항에 있어서,

상기 프로세서는 성별, 나이, 인종, 또는 이들이 조합된 속성에 따른 복수의 소스 얼굴로부터 추출된 복수의 식별자 특징 정보와 상기 원본 얼굴의 식별자 특징 정보를 비교하고 유사도에 따라 적합한 소스 얼굴을 선별하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 6

제1항에 있어서,

상기 소스 얼굴은 인공지능을 통해 실존하지 않는 가상으로 생성된 인물의 얼굴을 포함하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 7

제1항에 있어서,

상기 프로세서는 생성자(Generator)와 판별자(Discriminator)를 갖는 적대적 생성 네트워크(Generative Adversarial Network, GAN) 모델을 이용하여 상기 제1 익명화 얼굴을 생성하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 8

제2항에 있어서,

상기 프로세서는 상기 관찰 영상에서 해당하는 위치에 상기 제1 익명화 얼굴을 출력하여 익명화 영상을 생성하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 9

제8항에 있어서,

상기 통신 인터페이스는 상기 익명화 영상을 상기 개인 정보 보호 및 개인 식별 서버로 전송하는 것을 특징으로 하는 영상 기반 모니터링 장치.

청구항 10

개인 정보 보호 및 개인 식별 서버에 있어서,

제1 익명화 얼굴이 포함된 제1 익명화 영상을 수신하고, 원본 얼굴의 식별자 특징 정보 및 상기 제1 익명화 얼굴의 식별자 특징 정보가 매칭된 식별자 특징 정보 쌍을 수신하는 통신 인터페이스;

상기 제1 익명화 영상 및 상기 식별자 특징 정보 쌍을 저장하는 저장 매체; 및

상기 통신 인터페이스와 상기 저장 매체에 신호를 송신하는 프로세서를 포함하는 개인 정보 보호 및 개인 식별 서버.

청구항 11

제10항에 있어서,

상기 통신 인터페이스는 피관찰자의 신원 확인이 필요한 상황에서 제2 익명화 얼굴이 포함된 제2 익명화 영상을 수신하고,

상기 프로세서는 상기 제2 익명화 영상으로부터 제2 익명화 얼굴을 추출하고, 상기 제2 익명화 얼굴로부터 상기 제2 익명화 얼굴의 식별자 특징 정보를 추출하고, 상기 제2 익명화 얼굴의 식별자 특징 정보 및 상기 제1 익명화 얼굴의 식별자 특징 정보를 비교하고 유사도에 따라 유력한 제1 익명화 얼굴의 식별자 특징 정보를 출력하는 것을 특징으로 하는 개인 정보 보호 및 개인 식별 서버.

청구항 12

제11항에 있어서,

상기 프로세서는 상기 유력한 제1 익명화 얼굴의 식별자 특징 정보에 매칭하는 원본 얼굴의 식별자 특징 정보를 검출하는 것을 특징으로 하는 개인 정보 보호 및 개인 식별 서버.

청구항 13

제12항에 있어서,

상기 통신 인터페이스는 용의자의 사진이나 영상을 수신하고,

상기 프로세서는 상기 용의자의 사진이나 영상으로부터 후보 얼굴의 식별자 특징 정보를 추출하고, 상기 후보 얼굴의 식별자 특징 정보 및 상기 검출한 원본 얼굴의 식별자 특징 정보를 비교하고 유사도를 출력하는 것을 특징으로 하는 개인 정보 보호 및 개인 식별 서버.

발명의 설명

기술 분야

본 발명이 속하는 기술 분야는 안면 정보 익명화와 재인식 기술을 적용하여 개인 정보 보호 및 개인 식별 기능을 제공하는 감시 또는 관찰 시스템에 관한 것이다.

[0001]

배경 기술

- [0002] 기존의 카메라 기반의 감시 또는 관찰 시스템(monitoring system)은 개인의 얼굴을 카메라로 연속 촬영하여 그 영상을 그대로 저장 또는 전송하기 때문에 피사체의 개인 얼굴 정보가 노출되는 있는 문제가 있다. 기계학습에서 사용할 데이터 베이스 수집시에 얼굴 부분을 블러링 처리 또는 모자이크 처리하여 개인 안면 정보를 비식별화하는 여러가지 방법들이 개발되었으나, 이러한 방식들은 개인의 얼굴에 표현되는 표정 정보 등 많은 정보를 유실하게 된다. 인공지능 기술의 발전으로 서로 다른 사람의 얼굴을 합성하여 새로운 얼굴을 생성하는 적대적 생성 네트워크(Generative Adversarial Network, GAN)기술이 발달하여 한 개인의 얼굴 영상을 다른 얼굴로 바꾸는 안면 교환(face swap) 기술이 개발되어 딥 페이크(deep Fake) 기술이 가능해졌다.

선행기술문헌

특허문헌

- [0003] (특허문헌 0001) 한국등록특허공보 제10-1911900호 (2018.10.19)

발명의 내용

해결하려는 과제

- [0004] 본 발명의 실시 예들은 감시 또는 관찰 카메라(monitoring or surveillance camera)가 획득하는 영상에서 안면 교환(face swap) 또는 딥 페이크(deep Fake) 인공지능 기술을 통해 모니터링 대상자의 표정 정보는 보존하면서 얼굴을 존재하지 않는 제3의 가상의 얼굴과 합성하거나 제3의 얼굴로 변환하여 모니터링 대상자의 얼굴 정보를 익명화된 영상(anonymized face)으로 저장하고, 상기 관찰대상자의 원본 영상으로부터 상기 관찰대상자 얼굴의 특징을 내포하는 특징 정보를 추출하여 별도로 저장하며, 만일 익명화된 상기 관찰대상자의 신원을 식별하고자 할 때는 상기 특징 정보와 익명화된 얼굴의 영상 정보로부터 관찰 대상자를 재식별(re-identification) 하는데 주된 목적이 있다.
- [0005] 본 발명의 명시되지 않은 또 다른 목적들은 하기의 상세한 설명 및 그 효과로부터 용이하게 추론할 수 있는 범위 내에서 추가적으로 고려될 수 있다.

과제의 해결 수단

- [0006] 본 실시 예의 일 측면에 의하면 개인 정보 보호 및 개인 식별 기능을 포함하는 영상 기반 모니터링 장치에 있어서, 원본 얼굴과 선별된 소스 얼굴을 합성하여 제1 익명화 얼굴을 생성하고, 상기 원본 얼굴의 식별자 특징 정보 및 제1 익명화 얼굴의 식별자 특징 정보를 매칭하여 식별자 특징 정보 쌍을 생성하는 프로세서; 및 상기 식별자 특징 정보 쌍을 개인 정보 보호 및 개인 식별 서버로 전송하는 통신 인터페이스를 포함하는 영상 기반 모니터링 장치를 제공한다.
- [0007] 상기 프로세서는 영상 장치를 통해 관찰 대상자를 촬영한 관찰 영상을 획득하고, 상기 관찰 영상에서 상기 원본 얼굴을 검출하고 상기 검출된 원본 얼굴로부터 상기 식별자 특징 정보를 추출할 수 있다.
- [0008] 상기 영상 장치는 자율주행 자동차 또는 일반 자동차, 감시가 필요한 장소에 설치될 수 있다.
- [0009] 상기 프로세서는 (i) 프레임별 주기적인 시점에, (ii) 탑승 후 일회적인 시점에, (iii) 특정 행동이나 특정 상황이 발생한 시점에, (iv) 특정 표정이 검출되거나 얼굴 영역의 기준 크기를 만족하는 시점에, 또는 이들이 조합된 시점에, 상기 원본 얼굴을 검출하고 상기 검출된 원본 얼굴로부터 식별자 특징 정보를 추출할 수 있다.
- [0010] 상기 프로세서는 성별, 나이, 인종, 또는 이들이 조합된 속성들에 따른 복수의 얼굴 소스들로부터 추출된 복수의 식별자 특징 정보와 상기 원본 얼굴의 식별자 특징 정보를 비교하고 유사도에 따라 적합한 소스 얼굴을 선별할 수 있다.
- [0011] 상기 소스 얼굴은 인공지능을 통해 실존하지 않는 가상으로 생성된 인물의 얼굴을 포함할 수 있다.
- [0012] 상기 프로세서는 생성자(Generator)와 판별자(Discriminator)를 갖는 적대적 생성 네트워크(Generative Adversarial Network, GAN) 모델을 이용하여 상기 제1 익명화 얼굴을 생성할 수 있다.

- [0013] 상기 프로세서는 상기 관찰 영상에서 해당하는 위치에 상기 제1 익명화 얼굴을 출력하여 익명화 영상을 생성할 수 있다.
- [0014] 상기 통신 인터페이스는 상기 익명화 영상을 상기 개인 정보 보호 및 개인 식별 서버로 전송할 수 있다.
- [0015] 본 실시 예의 다른 측면에 의하면 개인 정보 보호 및 개인 식별 서버에 있어서, 제1 익명화 얼굴이 포함된 제1 익명화 영상을 수신하고, 원본 얼굴의 식별자 특징 정보 및 상기 제1 익명화 얼굴의 식별자 특징 정보가 매칭된 식별자 특징 정보 쌍을 수신하는 통신 인터페이스; 상기 제1 익명화 영상 및 상기 식별자 특징 정보 쌍을 저장하는 저장 매체; 및 상기 통신 인터페이스와 상기 저장 매체에 신호를 송신하는 프로세서를 포함하는 개인 정보 보호 및 개인 식별 서버를 제공한다.
- [0016] 상기 통신 인터페이스는 피관찰자의 신원 확인이 필요한 상황에서 제2 익명화 얼굴이 포함된 제2 익명화 영상을 수신할 수 있다.
- [0017] 상기 프로세서는 상기 제2 익명화 영상으로부터 제2 익명화 얼굴을 추출하고, 상기 제2 익명화 얼굴로부터 상기 제1 익명화 얼굴의 식별자 특징 정보를 추출하고, 상기 제2 익명화 얼굴의 식별자 특징 정보 및 상기 제1 익명화 얼굴의 식별자 특징 정보를 비교하고 유사도에 따라 유력한 제2 익명화 얼굴의 식별자 특징 정보를 출력할 수 있다.
- [0018] 상기 프로세서는 상기 유력한 제1 익명화 얼굴의 식별자 특징 정보에 매칭하는 원본 얼굴의 식별자 특징 정보를 검출할 수 있다.
- [0019] 상기 통신 인터페이스는 용의자의 사진이나 영상을 수신할 수 있다.
- [0020] 상기 프로세서는 상기 용의자의 사진이나 영상으로부터 후보 얼굴의 식별자 특징 정보를 추출하고, 상기 후보 얼굴의 식별자 특징 정보 및 상기 검출한 원본 얼굴의 식별자 특징 정보를 비교하고 유사도를 출력할 수 있다.

발명의 효과

- [0021] 이상에서 설명한 바와 같이 본 발명의 실시 예들에 의하면, 관찰 카메라 영상을 획득하는 과정에서 영상 원본을 저장하는 것이 아닌 인공지능 기술을 통해 피관찰자(또는 관찰 대상자)의 얼굴을 현존하지 않는 제3의 얼굴로 합성 또는 변환하여 익명화된 영상을 저장하고, 피관찰자의 익명화 전 원본 영상으로부터 피관찰자 얼굴의 특징을 내포하며 원래 얼굴로는 복원 불가능한 식별자 정보를 추출하여 익명화된 영상과 동시에 저장하는 방식을 통해 필요 상황에서 익명화된 피관찰자 신원을 식별할 수 있는 효과가 있다.
- [0022] 여기에서 명시적으로 언급되지 않은 효과라 하더라도, 본 발명의 기술적 특징에 의해 기대되는 이하의 명세서에서 기재된 효과 및 그 잠정적인 효과는 본 발명의 명세서에 기재된 것과 같이 취급된다.
- [0023] 본 발명의 실시 예는 자동차의 내부 카메라를 제시하였으나, 본 발명은 자동차의 차량 내부 탑승자 관찰 카메라(in-cabin monitoring camera)로 한정되지 않으며, 일반적인 관찰 또는 감시 카메라의 피관찰자 얼굴영상 익명화와 재식별에도 적용가능하다.

도면의 간단한 설명

- [0024] 도 1은 자동차 내부에서 발생한 비정상 내지는 돌발 상황을 예시한 도면이다.
- 도 2는 개인 정보 보호와 개인 식별 간의 딜레마를 예시한 도면이다.
- 도 3은 본 발명의 실시 예들에 따른 피관찰자 모니터링 시스템을 예시한 블록도이다.
- 도 4는 본 발명의 실시 예들에 따른 영상 기반 모니터링 장치, 개인 정보 보호 및 개인 식별 서버를 구현하는 장치를 예시한 도면이다.
- 도 5는 본 발명의 실시 예들에 따른 영상 기반 모니터링 장치의 동작을 예시한 흐름도이다.
- 도 6은 본 발명의 실시 예들에 따른 개인 정보 보호 및 개인 식별 서버의 동작을 예시한 흐름도이다.
- 도 7은 본 발명의 실시 예들에 따른 피관찰자 모니터링 시스템의 식별자 특징 정보 매칭 동작을 예시한 도면이다.
- 도 8은 본 발명의 실시 예들에 따른 피관찰자 모니터링 시스템의 동작을 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0025] 이하, 본 발명을 설명함에 있어서 관련된 공지기능에 대하여 이 분야의 기술자에게 자명한 사항으로서 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하고, 본 발명의 일부 실시 예들을 예시적인 도면을 통해 상세하게 설명한다.
- [0026] 도 1은 자동차 내부에서 발생한 비정상 내지는 돌발 상황을 예시한 도면이다.
- [0027] 자율주행 자동차의 피관찰자는 운전자가 아닌 승객으로 구성된다. 자율주행차 피관찰자는 승객으로써 운행되는 교통 상황에 책임을 지지 않으므로, 운행중 뿐만 아니라 운행 전후에도 보안과 안전을 확보하는게 중요하다. 자동차 내부에서 일부 피관찰자에 의하여 악의적인 행동이나 위협이 발생할 수 있다. 비정상적인 상황에서 역시 피관찰자의 보호가 필요하다.
- [0028] 자동차 내부를 모니터링하는 방식을 통해 피관찰자를 보호할 수 있다. 피관찰자들을 모니터링할 때 프라이버시 측면과 보안 측면에서 고려할 사항이 있다.
- [0029] 도 2는 개인 정보 보호와 개인 식별 간의 딜레마를 예시한 도면이다.
- [0030] 먼저 Case1에서 마스크 처리한 얼굴을 이용한 모니터링 방식은 중요한 얼굴 정보가 손실되는 문제가 있다. 다음으로 Case2에서 실제 얼굴을 이용한 모니터링 방식은 개인 안면 정보가 그대로 노출되는 문제가 있다. 마지막으로 Case3에서 종래의 익명화된 얼굴을 이용한 모니터링 방식은 사후에 피관찰자의 개인 식별이 곤란한 문제가 있다.
- [0031] 본 발명 기술인 "안면 정보 익명화 및 재식별 기능 기반 개인 정보 보호 기능을 제공하는 감시 또는 관찰 시스템"의 실시 예에 따른 피관찰자 모니터링 시스템은 개인 정보 보호를 위한 익명화 작업과 개인 식별을 위한 특징 매칭을 통해 개인 정보 보호 측면의 요구와 개인 식별 측면의 요구를 모두 만족시킨다.
- [0032] 도 3은 본 발명의 실시 예들에 따른 피관찰자 모니터링 시스템을 예시한 블록도이다.
- [0033] 피관찰자 모니터링 시스템은 관찰 영상을 획득하는 과정에서 영상 원본을 저장하는 것이 아닌, 인공지능 기술을 통해 피관찰자의 얼굴을 제3의 얼굴로 합성하거나 변환하여 익명화한 영상을 저장하고, 필요 상황에서의 익명화된 피관찰자 신원 식별의 문제를 해소하기 위해 피관찰자 익명화 전 원본 영상으로부터 피관찰자 얼굴의 특징을 내포하며, 원래 얼굴로는 복원 불가능한 식별자 특징 정보를 추출하여 익명화된 영상과 동시에 저장한다.
- [0034] 피관찰자 모니터링 시스템은 영상 기반 모니터링 장치(10), 개인 정보 보호 및 개인 식별 서버(20)를 포함한다.
- [0035] 도 4는 본 발명의 실시 예들에 따른 영상 기반 모니터링 장치, 개인 정보 보호 및 개인 식별 서버를 구현하는 장치를 예시한 도면이다.
- [0036] 장치(110)는 적어도 하나의 프로세서(120), 컴퓨터 판독 가능한 저장매체(130) 및 통신 버스(170)를 포함한다.
- [0037] 프로세서(120)는 최적화 장치(110)로 동작하도록 제어할 수 있다. 예컨대, 프로세서(120)는 컴퓨터 판독 가능한 저장 매체(130)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 컴퓨터 실행 가능 명령어는 프로세서(120)에 의해 실행되는 경우 장치(110)로 하여금 예시적인 실시 예에 따른 동작들을 수행하도록 구성될 수 있다.
- [0038] 컴퓨터 판독 가능한 저장 매체(130)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보는 입출력 인터페이스(150)나 통신 인터페이스(160)를 통해서도 주어질 수 있다. 컴퓨터 판독 가능한 저장 매체(130)에 저장된 프로그램(140)은 프로세서(120)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시 예에서, 컴퓨터 판독 가능한 저장 매체(130)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 최적화 장치(110)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.
- [0039] 통신 버스(170)는 프로세서(120), 컴퓨터 판독 가능한 저장 매체(130)를 포함하여 최적화 장치(110)의 다른 다양한 컴포넌트들을 상호 연결한다.
- [0040] 장치(110)는 또한 하나 이상의 입출력 장치를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(150) 및 하나 이상의 통신 인터페이스(160)를 포함할 수 있다. 입출력 인터페이스(150) 및 통신 인터페이스(160)는

통신 버스(170)에 연결된다. 입출력 장치(미도시)는 입출력 인터페이스(150)를 통해 최적화 장치(110)의 다른 컴포넌트들에 연결될 수 있다.

- [0041] 도 5는 본 발명의 실시 예들에 따른 영상 기반 모니터링 장치의 동작을 예시한 흐름도이다.
- [0042] 단계 S210에서 영상 기반 모니터링 장치의 프로세서는 영상 장치를 통해 관찰 또는 감시카메라로 한 명 이상의 피관찰자의 원본 얼굴을 검출한다. 피관찰자를 촬영한 관찰 영상을 획득하고, 관찰 상에서 원본 얼굴을 검출하고 검출된 원본 얼굴로부터 식별자 특징 정보를 추출한다. 영상 장치는 자율주행 자동차 또는 일반 자동차, 감시가 필요한 장소에 설치될 수 있다.
- [0043] 프로세서는 (i) 프레임별 주기적인 시점에, (ii) 탑승 후 일회적인 시점에, (iii) 특정 행동이나 특정 상황이 발생한 시점에, (iv) 특정 표정이 검출되거나 얼굴 영역의 기준 크기를 만족하는 시점에, 또는 이들이 조합된 시점에, 원본 얼굴을 검출하고 검출된 원본 얼굴로부터 식별자 특징 정보를 추출할 수 있다.
- [0044] 단계 S220에서 영상 기반 모니터링 장치의 프로세서는 성별, 나이, 인종, 또는 이들이 조합된 속성에 따른 복수의 소스 얼굴로부터 추출된 복수의 식별자 특징 정보와 상기 원본 얼굴의 식별자 특징 정보를 비교하고 유사도에 따라 적합한 소스 얼굴을 선별한다. 소스 얼굴은 인공지능을 통해 실존하지 않는 가상으로 생성된 인물의 얼굴을 포함할 수 있다.
- [0045] 단계 S230에서 영상 기반 모니터링 장치의 프로세서는 원본 얼굴과 선별된 소스 얼굴을 합성하여 제1 익명화 얼굴을 생성하고, 원본 얼굴의 식별자 특징 정보 및 제1 익명화 얼굴의 식별자 특징 정보를 매칭하여 식별자 특징 정보 쌍을 생성한다. 영상 기반 모니터링 장치의 통신 인터페이스는 식별자 특징 정보 쌍을 개인 정보 보호 및 개인 식별 서버로 전송한다.
- [0046] 프로세서는 생성자(Generator)와 판별자(Discriminator)를 갖는 적대적 생성 네트워크(Generative Adversarial Network, GAN) 모델을 이용하여 상기 제1 익명화 얼굴을 생성할 수 있다.
- [0047] 단계 S240에서 영상 기반 모니터링 장치의 프로세서는 관찰 영상에서 해당하는 위치에 제1 익명화 얼굴을 출력하여 익명화 영상을 생성한다. 영상 기반 모니터링 장치의 통신 인터페이스는 익명화 영상을 개인 정보 보호 및 개인 식별 서버로 전송할 수 있다.
- [0048] 도 6은 본 발명의 실시 예들에 따른 개인 정보 보호 및 개인 식별 서버의 동작을 예시한 흐름도이다.
- [0049] 단계 S310에서 개인 정보 보호 및 개인 식별 서버의 통신 인터페이스는 제1 익명화 얼굴이 포함된 익명화 영상을 수신하고, 원본 얼굴의 식별자 특징 정보 및 제1 익명화 얼굴의 식별자 특징 정보가 매칭된 식별자 특징 정보 쌍을 수신한다. 개인 정보 보호 및 개인 식별 서버의 저장 매체는 제1 익명화 영상 및 식별자 특징 정보 쌍을 저장한다. 프로세서는 통신 인터페이스와 저장 매체에 신호를 송신한다.
- [0050] 단계 S320에서 개인 정보 보호 및 개인 식별 서버의 통신 인터페이스는 피관찰자의 신원 확인이 필요한 상황에서 제1 익명화 얼굴이 포함된 익명화 영상을 수신한다. 개인 정보 보호 및 개인 식별 서버의 프로세서는 제2 익명화 영상으로부터 제2 익명화 얼굴을 추출하고, 제2 익명화 얼굴로부터 제2 익명화 얼굴의 식별자 특징 정보를 추출하고, 제2 익명화 얼굴의 식별자 특징 정보 및 제1 익명화 얼굴의 식별자 특징 정보를 비교하고 유사도에 따라 유력한 제1 익명화 얼굴의 식별자 특징 정보를 출력한다.
- [0051] 단계 S330에서 개인 정보 보호 및 개인 식별 서버의 프로세서는 유력한 제1 익명화 얼굴의 식별자 특징 정보에 매칭하는 원본 얼굴의 식별자 특징 정보를 검출한다.
- [0052] 단계 S340에서 개인 정보 보호 및 개인 식별 서버의 통신 인터페이스는 용의자의 사진이나 영상을 수신한다. 개인 정보 보호 및 개인 식별 서버의 프로세서는 용의자의 사진이나 영상으로부터 후보 얼굴의 식별자 특징 정보를 추출하고, 후보 얼굴의 식별자 특징 정보 및 검출한 원본 얼굴의 식별자 특징 정보를 비교하고 유사도를 출력할 수 있다.
- [0053] 도 7은 본 발명의 실시 예들에 따른 피관찰자 모니터링 시스템의 식별자 특징 정보 매칭 동작을 예시한 도면이고, 도 8은 본 발명의 실시 예들에 따른 피관찰자 모니터링 시스템의 동작을 예시한 도면이다.
- [0054] 영상 기반 모니터링 장치와 개인 정보 보호 및 개인 식별 서버를 포함하는 피관찰자 모니터링 시스템은 영상에서 얼굴을 추출한다. 얼굴에서 추출한 식별자 특징 정보는 N차원으로 구현될 수 있다. 예컨대, 128-차원 벡터로 구현될 수 있으며, 128-차원보다 적으면 얼굴 비교가 곤란하고 128-차원보다 크면 불필요하게 파라미터를 증가시키게 된다.

- [0055] 피관찰자 모니터링 시스템은 얼굴 특징 검출 모델을 적용한다.
- [0056] 얼굴 특징 검출 모델은 특징을 추출하고 특징을 데이터 가공 처리한다. 얼굴 검출 모델은 다수의 레이어가 네트워크로 연결되며 히든 레이어를 포함한다. 레이어는 파라미터를 포함할 수 있고, 레이어의 파라미터는 학습가능한 필터 집합을 포함한다. 파라미터는 노드 간의 가중치 및/또는 바이어스를 포함한다.
- [0057] 얼굴 특징 검출 모델은 추출을 극대화하기 위해 깊고 넓은 신경망을 사용할 수 있다. 입력 값을 받아 입력 값과 컨볼루션(convolution) 연산을 더하는 레지듀얼(residual) 연산을 적용할 수 있다.
- [0058] 얼굴 특징 검출 모델은 인물 재인식에 관한 오류를 측정하는데 사용되는 트리플 손실 함수를 적용한다. 모델은 손실 함수를 최소화하도록 파라미터를 학습한다. 트리플 손실 함수(triple loss function)은 수학식 1과 같이 표현된다.

수학식 1

$$[0059] \quad \ell(A, P, N) = \max (\|A, P\|_2 - \|A, N\|_2 + \text{margin}, 0)$$

- [0060] 익명화된 앵커 영상(A)는 이례적인 상황에서 파악된 인물을 나타내고, 익명화된 포지티브 영상(P)은 클라우드에 저장된 동일인의 영상을 나타내고, 익명화된 네거티브 영상(N)은 다른 피관찰자를 나타낸다. 데이터 쌍 간에 유클리드 거리를 적용할 수 있다. 오분류를 최소화하는 마진을 적용할 수 있다.
- [0061] 식별자 특징 정보의 유사도는 거리의 길이 등을 기준으로 측정할 수 있다. 벡터 공간의 유사도는 수학식 2와 같이 표현된다.

수학식 2

$$[0062] \quad \text{Similarity} = \min (\|R, C\|_2, \|R, D\|_2)$$

- [0063] 영상(R)은 인물을 나타내고, 영상(C)는 클라우드에 저장된 동일인의 영상을 나타내고, 영상(D)는 다른 피관찰자의 영상을 나타낸다.
- [0064] 피관찰자 모니터링 시스템은 소스 얼굴 생성 모델을 적용한다.
- [0065] 소스 얼굴 생성 모델은 교환에 필요한 대상 얼굴과 유사한 얼굴을 생성한다. 소스 얼굴 생성 모델은 성별, 나이, 인종, 또는 이들이 조합된 속성에 따른 복수의 소스 얼굴을 생성하며, 다양한 식별자 특징 정보를 표현한 가상 얼굴을 생성할 수 있다. 소스 얼굴 집합은 식별자 특징 정보 집합에 대응한다. 소스 얼굴 생성 모델은 피관찰자에 의한 행동이나 원래의 감정을 효과적으로 렌더링한다. 소스 얼굴과 대상 얼굴 간의 유사도 매칭은 모니터링에 필요한 유사 감정과 행동 의도를 상호 파악하는데 유용하다. 식별자 특징 정보 집합에서 추출된 식별자 특징 정보와 원본 얼굴의 식별자 특징 정보를 비교하여 합성용 얼굴을 선별할 수 있다.
- [0066] 피관찰자 모니터링 시스템은 얼굴 익명화 모델을 적용한다. 모델은 손실 함수를 최소화하도록 파라미터를 학습한다.
- [0067] 얼굴 익명화 모델은 대상 얼굴에서 얼굴과 헤어 영역을 구분한다. 얼굴의 랜드마크 위치를 매핑한 얼굴 영역과 헤어 영역을 분리한다.

- [0068] i번째 레이어 특징 맵($F_i \in \mathbb{R}^{C_i \times H_i \times W_i}$)에 대해서 영상 쌍(x,y)의 지각 손실(ℓ_{perc})은 수학식 3과 같이 표현된다.

수학식 3

$$\ell_{perc}(x, y) = \sum((1/C_i \times H_i \times W_i) \times \|F_i(x) - F_i(y)\|)$$

지각 손실은 미세한 얼굴 세부 정보 캡처의 오류를 추정하는데 사용된다.

영상 쌍의 재구성 손실(ℓ_{rec})은 수학식 4와 같이 표현된다.

수학식 4

$$\ell_{rec}(x, y) = \lambda_{perc} \times \ell_{perc}(x, y) + \lambda_{pixel} \times \ell_{pixel}(x, y)$$

재구성 손실은 색상 부정확성을 픽셀 단위로 평가하는데 사용된다. λ 는 하이퍼 파라미터에 대응한다.

픽셀 손실(ℓ_{pixel})은 수학식 5와 같이 표현된다.

수학식 5

$$\ell_{pixel}(x, y) = \|x - y\|$$

얼굴 익명화 모델은 생성자(Generator)와 판별자(Discriminator)를 갖는 적대적 생성 네트워크(Generative Adversarial Network, GAN) 모델을 이용하여 익명화 얼굴을 생성할 수 있다.

생성자와 판별자 간의 적대적 손실(ℓ_{adv})은 수학식 6과 같이 표현된다.

수학식 6

$$\ell_{adv}(G, D) = \min(\max(\sum \ell_{GAN}(G, D))$$

$$\ell_{GAN}(G, D) = E_{(x, y)}[\log D(x, y)] + E_x[\log(1 - D(x, G(x)))]$$

적대적 손실은 생성된 이미지를 개선하여 사실적인 모습을 제공한다. $E(x, y)$ 는 모든 실제 데이터 인스턴스에 대한 예상 값이고, E_x 는 생성자에 대한 모든 임의 입력에 대한 예상 값을 나타낸다.

생성 손실(ℓ_{RG})은 수학식 6과 같이 표현된다.

수학식 7

$$\ell_{RG} = \ell_{perc} + \ell_{rec} + \ell_{adv}$$

기준 교차 엔트로피 손실(ℓ_{CE})은 수학식 7과 같이 표현된다.

수학식 8

$$\ell_{CE} = -\sum(t_i \times \log(P_i))$$

[0083]

i번째 클래스에 대해서 검증 레이블 t_i 와 소프트맥스 확률 P_i 로 정의된다.

[0084]

영역 생성 손실(ℓ_{SG})은 수학식 9와 같이 표현된다.

[0085]

수학식 9

$$\ell_{SG} = \ell_{CE} + \ell_{pixel}$$

[0086]

모델은 대상 영상의 얼굴 및 헤어 영역을 기반으로 불완전 부분을 평가하고 채운다. 인페인팅 생성 손실(ℓ_{IP})은 수학식 10과 같이 표현된다.

[0087]

수학식 10

$$\ell_{IP} = \ell_{rec} + \ell_{adv}$$

[0088]

모델은 완전히 재연된 얼굴을 블렌딩하여 교환한 얼굴이 원래 대상 얼굴과 같은 배경 환경과 일치하도록 한다.

[0089]

얼굴 블렌딩 손실(ℓ_B)은 수학식 11과 같이 표현된다.

수학식 11

$$\ell_B = \ell_{perc} + \ell_{adv}$$

[0090]

피관찰자 모니터링 시스템은 각 피관찰자에 해당하는 식별 서명을 생성한다. 예컨대, 실제 얼굴에 대한 식별자 특징 정보와 익명화된 영상에 대한 식별자 특징 정보에 해당하는 식별 서명 쌍을 생성한다. 얼굴 익명화 처리 후 비디오 프레임은 피관찰자의 식별 서명 쌍과 함께 클라우드를 통해 서버로 전송된다.

[0091]

비정상적 상황에서 식별자 특징 정보를 획득하는 알고리즘 1이 표 1에 나타난다.

[0092]

표 1

Pseudocode 1. Algorithm for obtaining the ID of the person involved in abnormal situation.

Definitions: Faces of the occupant (F); Target face (T); Appropriate source face (S); Anonymized face (A); Identity features (ID): real face ID (ID_R); anonymized face ID (ID_A); ID of occupant caused abnormal situation (ID_{A_AS}); abnormal situation (AS) in-cabin.

Functions: \mathbb{F} = face detector; \mathbb{S} = source detector; \mathbb{A} = anonymizer; \mathbb{I} = ID extractor.

Input: video frames (in-cabin)

```

1. for  $i = 1$  to range of the occupant:
     $T(i) = \mathbb{F}(\text{Input})$ ,  $S(i) = \mathbb{S}(T(i))$ 
     $A(i) \leftarrow \mathbb{A}(T(i), S(i))$ 
     $ID_R(i) = \mathbb{I}(T(i))$ ,  $ID_A(i) = \mathbb{I}(A(i))$ 
2. store:  $ID(i) \leftarrow (ID_R(i); ID_A(i))$ 
3. At datacenter: monitor event and behavior for AS:
    if occupant  $j$  is involved in AS, then:
        generate ( $ID_{A\_AS}(j)$ )
        match ID:
            for ID from 1 to range of the ID:
                 $k = \text{argmin}(\|ID_{A\_AS}(j), ID_A(:)\|_2)$ 
4. Map:  $ID_R(k) \leftarrow ID_A(k)$ 
return ( $ID_R(k)$ )

```

[0093]

[0094] 시스템은 카메라 등을 이용하여 피관찰자 모니터링 영상을 획득한다.

[0095] 시스템은 영상을 입력으로 받아 영상 내 모든 탑승객의 특징을 출력으로 내보내고, 입력 영상의 얼굴로부터 특징(ID) 추출한다. 검출된 얼굴 당 128-차원의 벡터 특징을 추출할 수 있다.

[0096] 시스템은 영상을 입력으로 받아 영상 내 모든 탑승객의 얼굴 위치를 출력으로 내보낸다.

[0097] 시스템은 획득된 영상을 입력으로 받아 익명화된 영상을 출력으로 내보낸다. 익명화는 원본 영상 내에 존재하는 각각의 원본 얼굴(대상 얼굴)과 기 저장된 소스 얼굴의 합성을 통해 이루어진다

[0098] 익명화를 통해 원본 얼굴은 원본 얼굴과 소스 얼굴이 적절히 혼합된 중간 형태의 얼굴로 익명화된다. 이는 적대적 생성 신경망(GAN) 등을 통해 구현될 수 있다.

[0099] 시스템은 입력 영상으로부터 원본 얼굴들의 위치들을 알아낸다

[0100] 시스템은 원본 얼굴들의 ID를 추출한다. 익명화를 위한 소스 얼굴은 기 지정된 수만큼 장치에 저장되어 있으며, 이 역시 인공지능을 통해 가상으로 생성된 인물일 수 있다. 소스 얼굴로부터 추출된 ID와 영상의 원본 얼굴로부터 추출된 ID간 유사도(or 거리)를 측정하여 원본 얼굴과 가장 유사한 소스 얼굴을 찾는다. 영상 내의 각 원본 얼굴과 가장 유사한 소스 얼굴을 이용하여 각 위치의 원본 얼굴의 익명화를 진행한다

[0101] 시스템은 획득한 원본 영상과 획득한 익명화 영상으로부터 추출된 전체 탑승객의 ID를 서버로 송신한다. 이 때, 영상 내 동일 인물에 대해 원본 ID와 익명화 ID를 쌍으로 묶어(개인 식별 정보), 획득한 익명화 영상과 같이 서버로 송신한다.

[0102] 비정상적 상황에서 인물의 증거를 찾는 알고리즘 2가 표 2에 나타난다.

표 2

Pseudocode 2. Algorithm for evidence of the person involved in the abnormal situation.

Definitions: Target face (occupant's face) captured during investigation (T_{inv}); ID of the occupant's face obtained during investigation (ID_{inv}); ID of the person involved in the abnormal situation (ID_R); Real face of the occupant involved in the abnormal situation (O).

Functions: $\textcircled{1}$ = ID extractor.

Input: T_{inv} ; ID_R

```

1. At investigation:
    for  $i$  from 1 to range of the target faces:
         $ID_{inv}(i) = \textcircled{1}(T_{inv}(i))$ 
        match ID:
             $j = \text{argmin}(\|ID_R, ID_{inv}(\cdot)\|_2)$ 
2. Map:  $O \leftarrow j$ 
return ( $O$ )

```

[0103]

[0104]

시스템은 장치로부터 식명화된 모니터링 영상과 영상의 해당 프레임의 개인 식별 정보를 받아 저장한다.

[0105]

시스템은 피관찰자 신원 확인이 필요한 사건 발생 시 식명화된 영상으로부터 식명화된 피관찰자 개개의 특징을 추출한다(ID획득). 추출된 ID와 저장된 식명화 ID간 유사도를 계산하여 가장 유사한 식명화 ID를 알아낸다. 해당 식명화 ID와 쌍으로 저장된 원본 ID를 알아낸다. 사건의 유력 용의자의 다른 사진으로부터 ID를 추출해내어 저장되어 있는 원본 ID와 유사도를 대조한다.

[0106]

본 실시 예에 따른 영상 기반 모니터링 장치, 개인 정보 보호 및 개인 식별 서버에 의하면 식명화 얼굴을 통해 타인의 개인 프라이버시를 보호하면서, 실제 얼굴과 식명화 얼굴의 얼굴 식별 특징 정보를 이용한 매칭을 통해 비정상적인 상황에서 관련된 사람을 찾을 수 있는 방안을 제공한다.

[0107]

영상 기반 모니터링 장치, 개인 정보 보호 및 개인 식별 서버는 하드웨어, 펌웨어, 소프트웨어 또는 이들의 조합에 의해 로직회로 내에서 구현될 수 있고, 범용 또는 특정 목적 컴퓨터를 이용하여 구현될 수도 있다. 장치는 고정배선형(Hardwired) 기기, 필드 프로그램 가능한 게이트 어레이(Field Programmable Gate Array, FPGA), 주문형 반도체(Application Specific Integrated Circuit, ASIC) 등을 이용하여 구현될 수 있다. 또한, 장치는 하나 이상의 프로세서 및 컨트롤러를 포함한 시스템온칩(System on Chip, SoC)으로 구현될 수 있다.

[0108]

영상 기반 모니터링 장치, 개인 정보 보호 및 개인 식별 서버는 하드웨어적 요소가 마련된 컴퓨팅 디바이스 또는 서버에 소프트웨어, 하드웨어, 또는 이들의 조합하는 형태로 탑재될 수 있다. 컴퓨팅 디바이스 또는 서버는 각종 기기 또는 유무선 통신망과 통신을 수행하기 위한 통신 모듈 등의 통신장치, 프로그램을 실행하기 위한 데이터를 저장하는 메모리, 프로그램을 실행하여 연산 및 명령하기 위한 마이크로프로세서 등을 전부 또는 일부 포함한 다양한 장치를 의미할 수 있다.

[0109]

도 5 및 도 6에서는 각각의 과정을 순차적으로 실행하는 것으로 기재하고 있으나 이는 예시적으로 설명한 것에 불과하고, 이 분야의 기술자라면 본 발명의 실시 예의 본질적인 특성에서 벗어나지 않는 범위에서 도 5 및 도 6에 기재된 순서를 변경하여 실행하거나 또는 하나 이상의 과정을 병렬적으로 실행하거나 다른 과정을 추가하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이다.

[0110]

본 실시 예들에 따른 동작은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능한 매체에 기록될 수 있다. 컴퓨터 판독 가능한 매체는 실행을 위해 프로세서에 명령어를 제공하는 데 참여한 임의의 매체를 나타낸다. 컴퓨터 판독 가능한 매체는 프로그램 명령, 데이터 파일, 데이터 구조 또는 이들의 조합을 포함할 수 있다. 예를 들면, 자기 매체, 광기록 매체, 메모리 등이 있을 수 있다. 컴퓨터 프로그램은 네트워크로 연결된 컴퓨터 시스템 상에 분산되어 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수도 있다. 본 실시 예를 구현하기 위한 기능적인(Functional) 프로그램, 코드, 및 코드 세그먼트들은 본 실시 예가 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있을 것이다.

[0111]

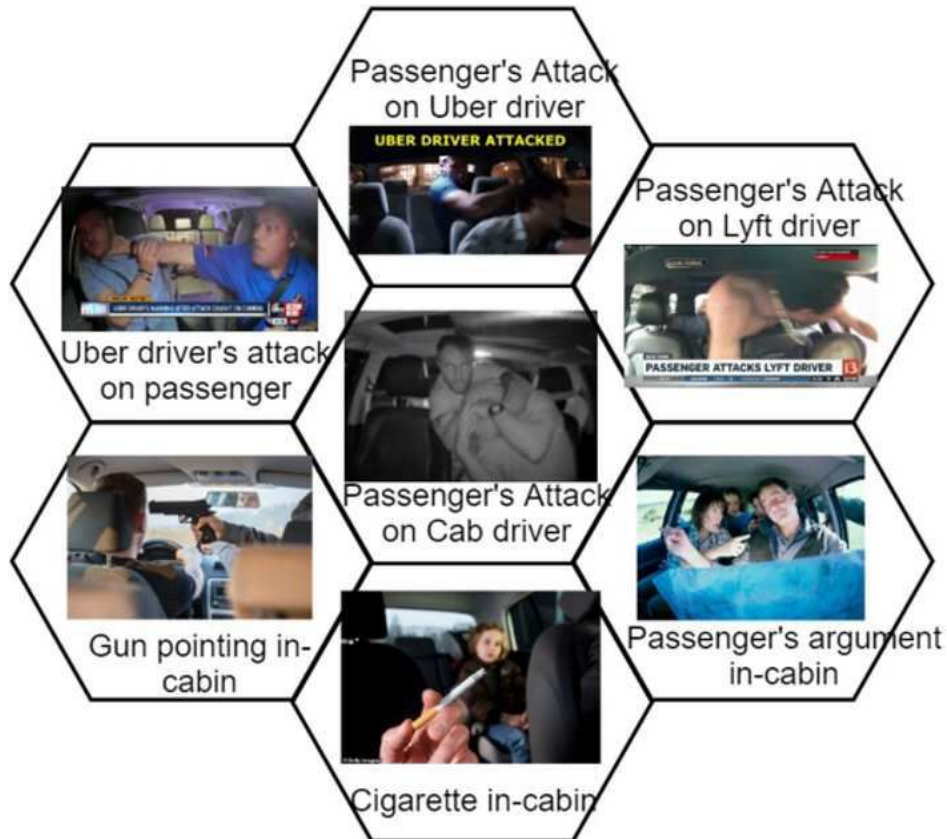
본 실시 예들은 본 실시 예의 기술 사상을 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 실시 예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시 예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시 예의 권리범위에 포함되는 것으로 해석되어야 할

것이다.

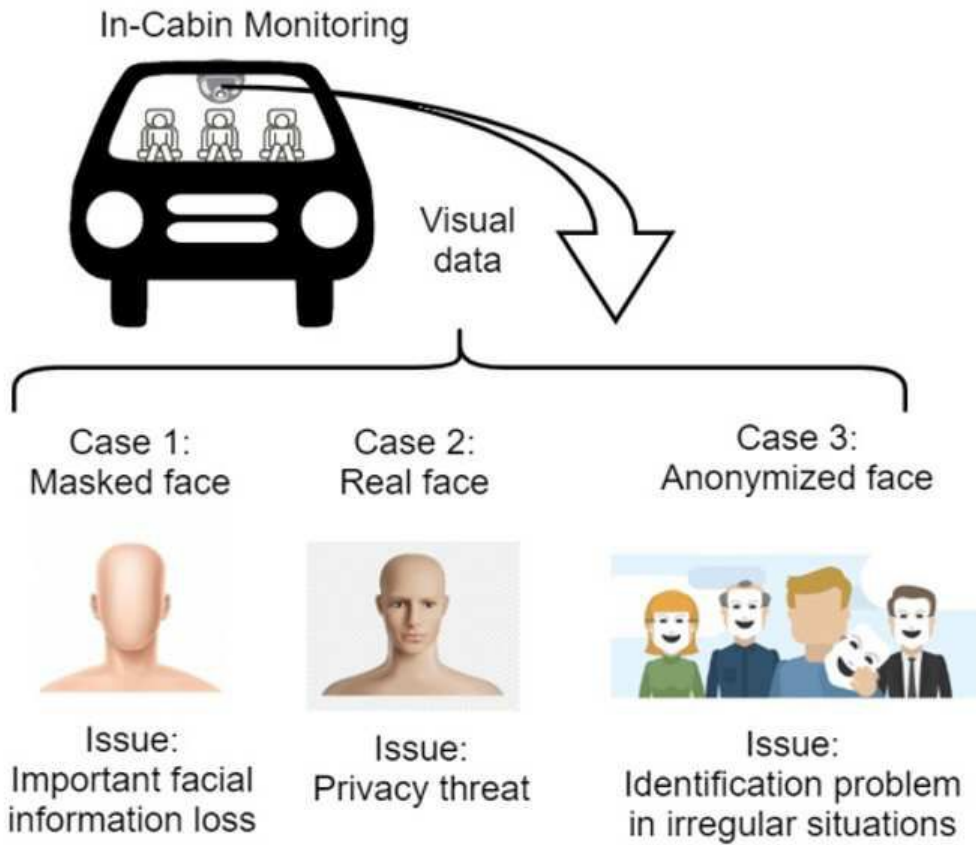
[0112] 본 발명의 실시 예는 자동차의 내부 카메라를 제시하였으나, 본 발명은 자동차의 차량 내부 탑승자 관찰 카메라 (in-cabin monitoring camera)로 한정되지 않으며, 일반적인 폐쇄 회로 TV (CCTV) 등의 관찰 또는 감시 카메라의 피관찰자 얼굴영상 익명화와 재식별에도 적용 가능하다.

도면

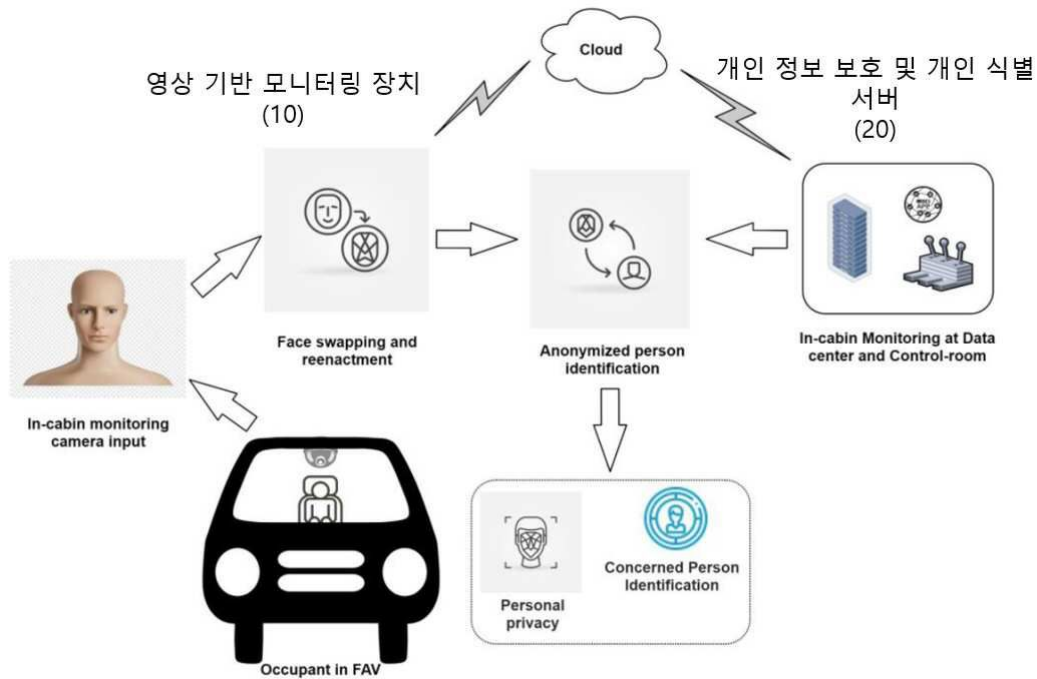
도면1



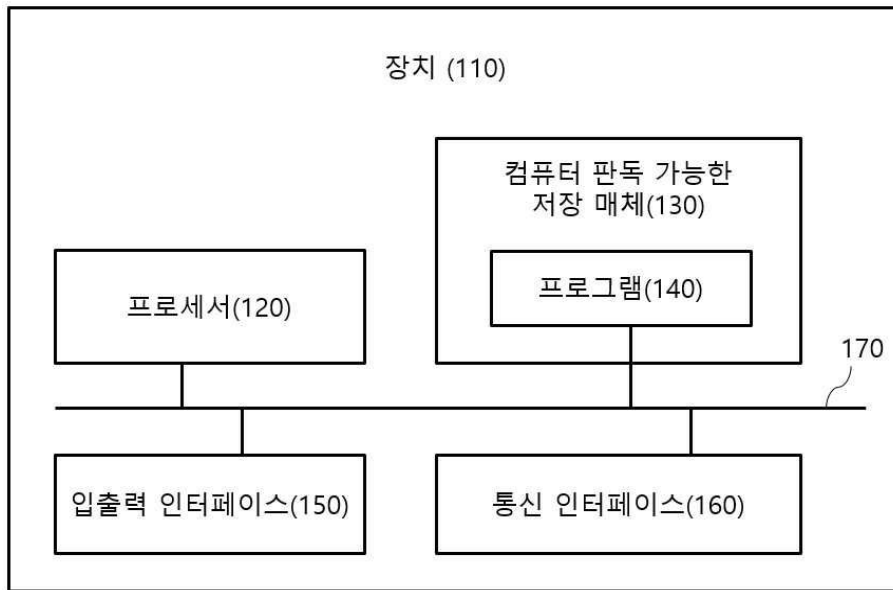
도면2



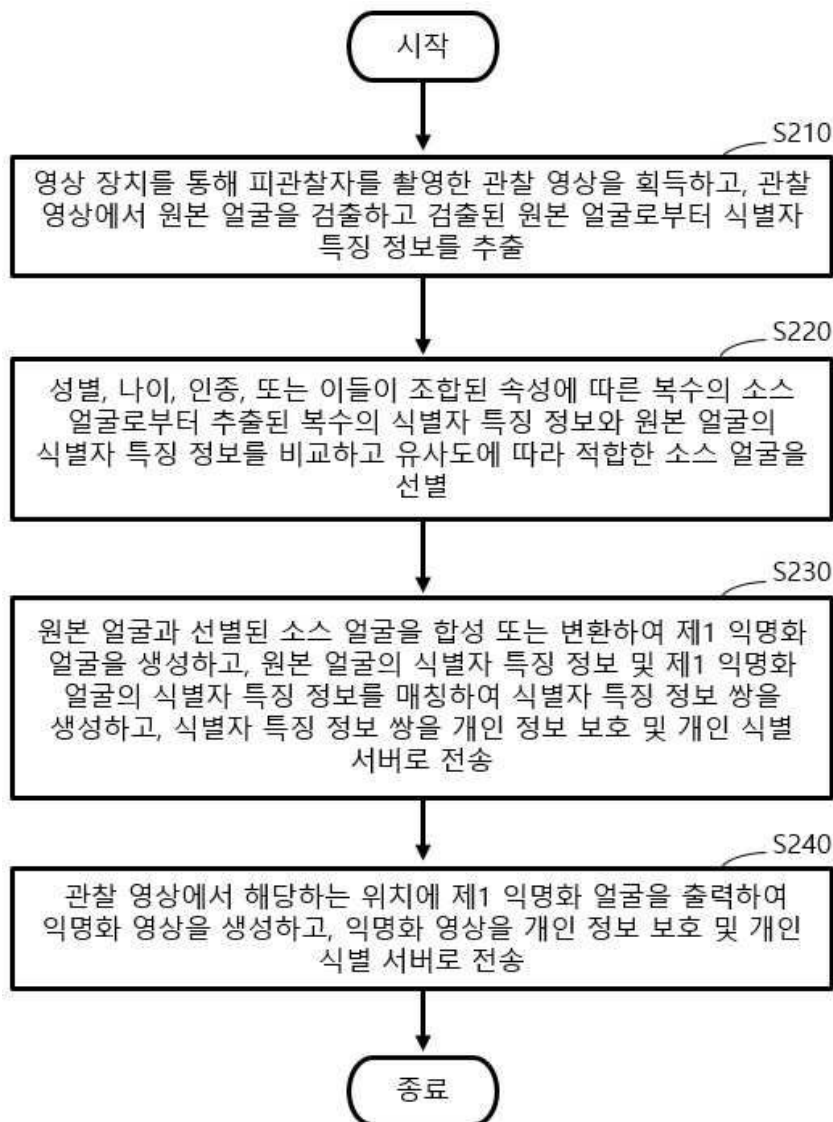
도면3



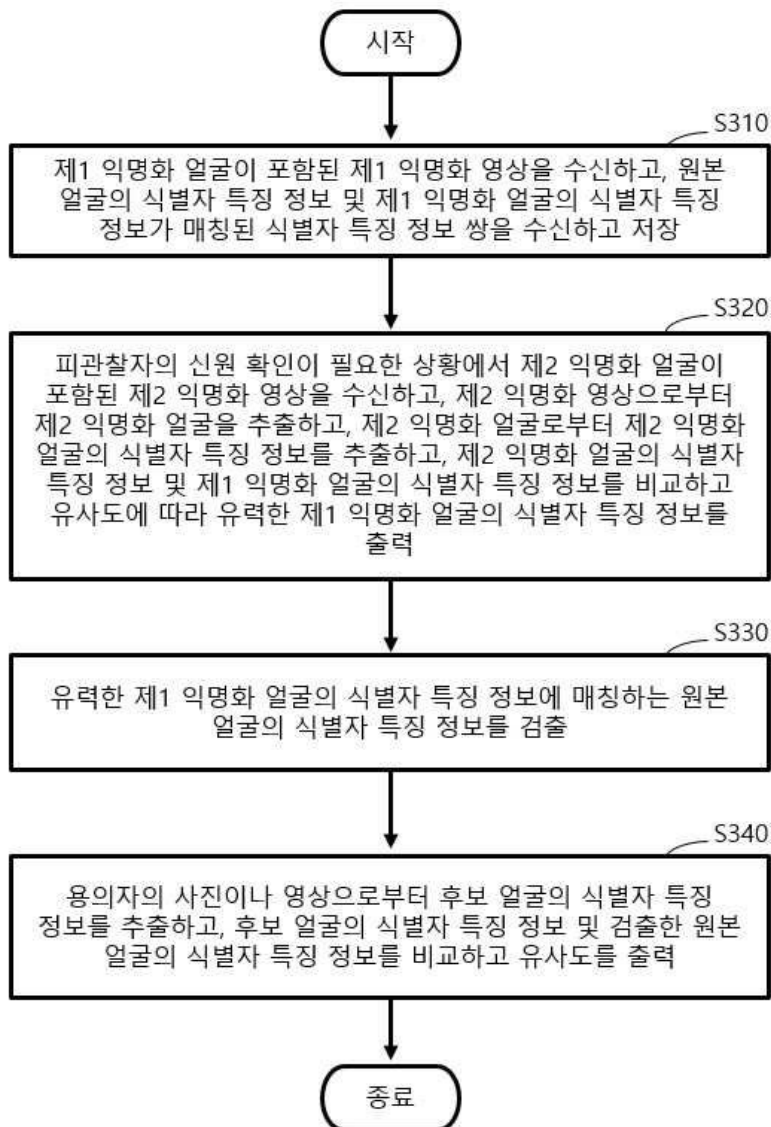
도면4



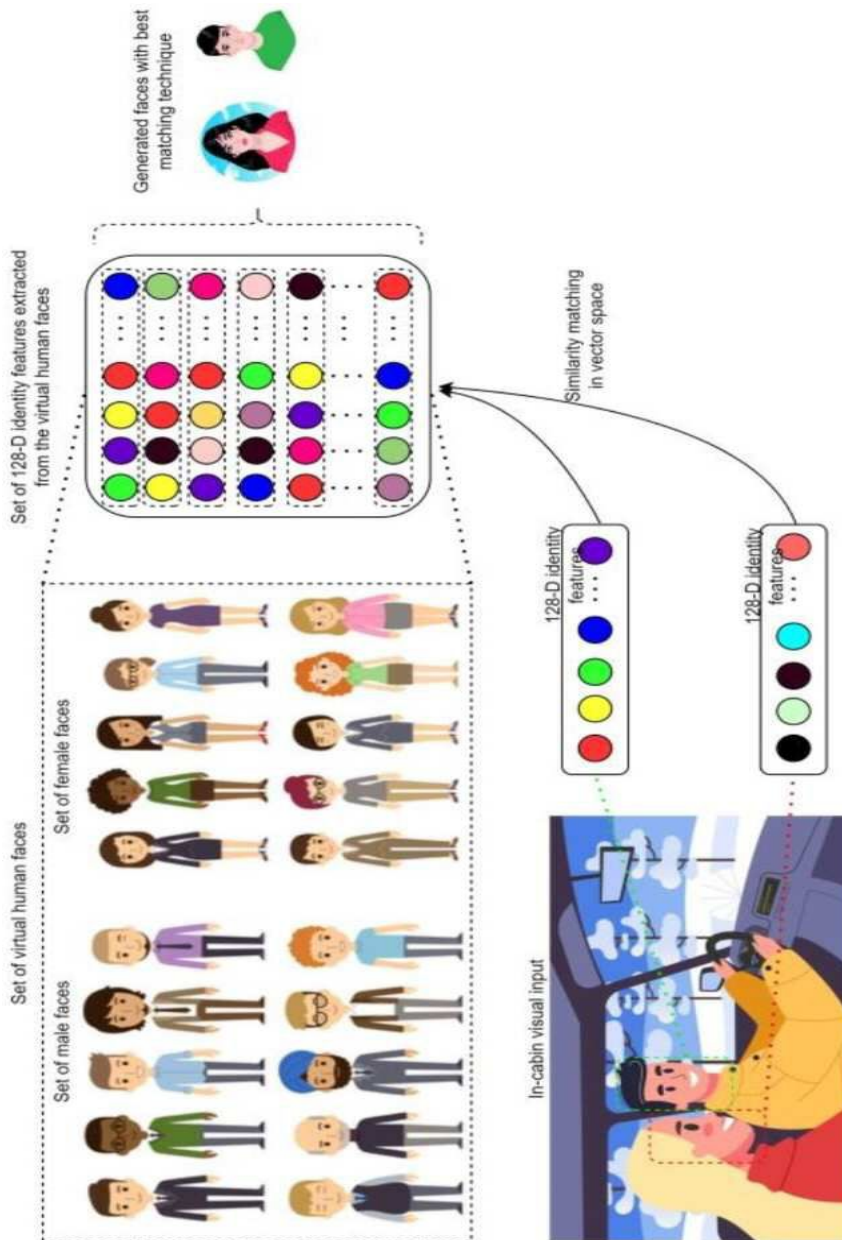
도면5



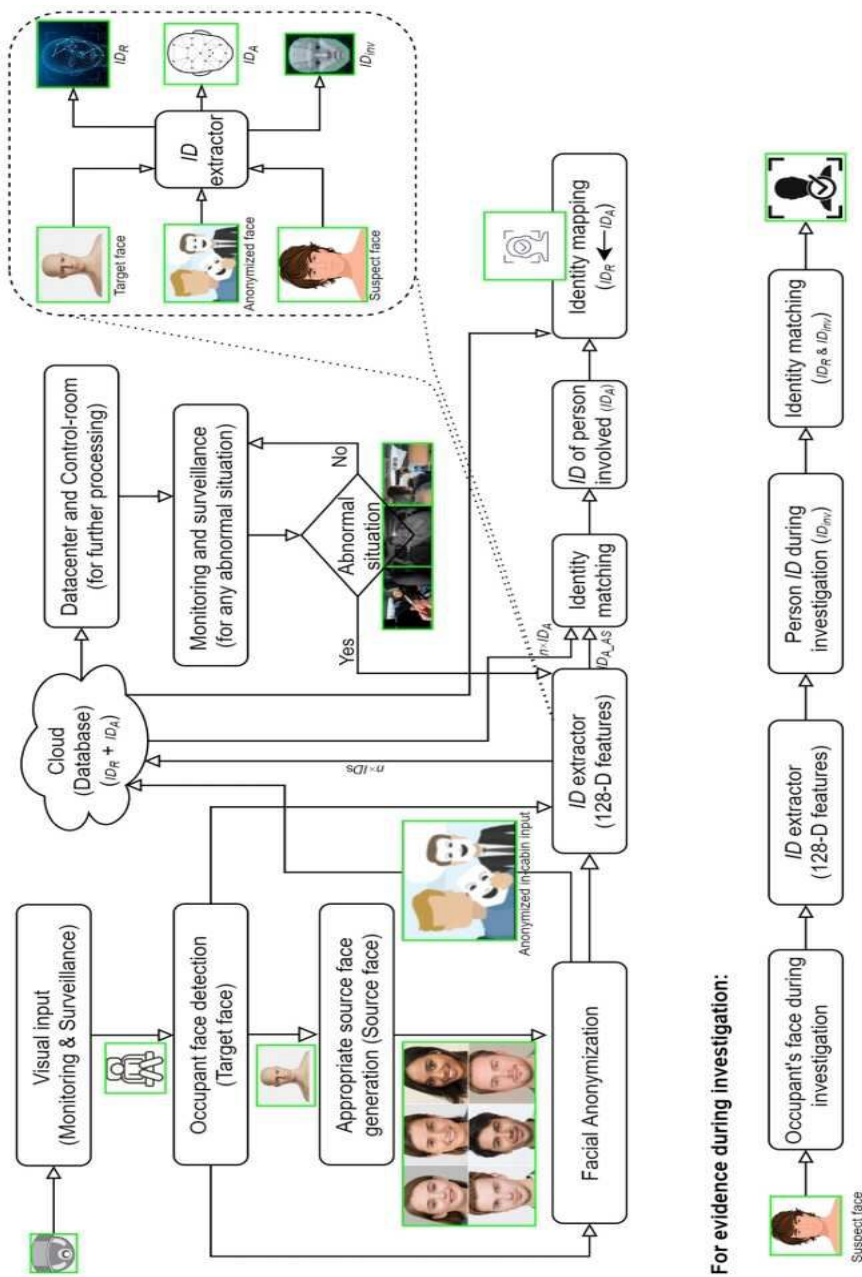
도면6



도면7



도면8



For evidence during investigation: