

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0079716

(43) 공개일자 2020년07월06일

(51) 국제특허분류(Int. Cl.)

G06F 21/62 (2013.01) G06T 3/40 (2006.01)

G06T 7/11 (2017.01)

(52) CPC특허분류

G06F 21/6245 (2013.01)

G06F 16/50 (2019.01)

(21) 출원번호 10-2018-0169146

(22) 출원일자 2018년12월26일

심사청구일자 2018년12월26일

(71) 출원인

인하대학교 산학협력단

인천광역시 미추홀구 인하로 100(용현동, 인하대학교)

(72) 발명자

이보원

서울특별시 강남구 언주로 201, 901호(도곡동)

이영선

인천광역시 미추홀구 인하로 100, 사범대학 교육학과 서호관 325호(용현동)

(74) 대리인

양성보

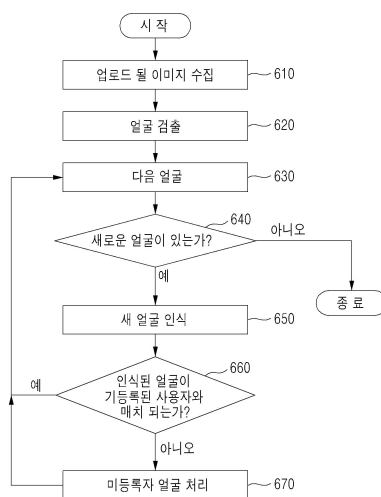
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 이미지 데이터의 개인 정보 보호를 위한 방법 및 시스템

(57) 요약

이미지 데이터의 개인 정보 보호를 위한 방법 및 시스템이 개시된다. 일 실시예에 따른 보호 시스템에 의해 수행되는 개인 정보 보호를 위한 방법은, 소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 업로드되는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검출하는 단계-상기 영상 정보는, 이미지 또는 동영상을 포함함-; 및 상기 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 비교함에 따라 미등록된 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득하는 단계를 포함할 수 있다.

대표도 - 도6



(52) CPC특허분류

G06T 3/40 (2013.01)

G06T 7/11 (2017.01)

G06T 2207/30201 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1415157013

부처명 산업통상자원부

연구관리전문기관 한국산업기술평가관리원

연구사업명 산업핵심기술개발사업

연구과제명 인간 내면상태의 인식 및 이를 이용한 인간친화형 인간-로봇 상호작용 기술 개발 (2차년도)

기 여 율 1/2

주관기관 인하대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1345284529

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 일반공동연구지원사업

연구과제명 전환기 자폐성장애 사용자를 고려한 사회-정서 지원 프로그램: 리얼타임 어널리틱스 기반 솔루션(1차년도)

기 여 율 1/2

주관기관 인하대학교 산학협력단

연구기간 2018.07.01 ~ 2019.06.30

명세서

청구범위

청구항 1

보호 시스템에 의해 수행되는 개인 정보 보호를 위한 방법에 있어서,

소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 업로드되는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검출하는 단계-상기 영상 정보는, 이미지 또는 동영상을 포함함-; 및
상기 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 비교함에 따라 미등록된 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득하는 단계

를 포함하는 개인 정보 보호를 위한 방법.

청구항 2

제1항에 있어서,

상기 영역을 검출하는 단계는,

소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 영상 정보를 업로드하고, 상기 업로드된 영상 정보로부터 프라이버시 노출 가능성이 있는 영역의 포함 여부를 검색하는 단계

를 포함하고,

상기 프라이버시 노출 가능성이 있는 영역은, 얼굴, 신체의 일부 또는 신체의 전부 중 사용자를 식별 가능한 어느 하나의 영역을 포함하는

개인 정보 보호를 위한 방법.

청구항 3

제1항에 있어서,

상기 영역을 검출하는 단계는,

상기 소셜 미디어 또는 소셜 네트워크 서비스에 업로드되는 영상 정보에서 검출되는 프라이버시 노출 가능성이 있는 영역을 공개 또는 비공개하기 위한 등록 정보를 저장하는 단계

를 포함하고,

상기 저장하는 단계에서, 상기 영상 정보에서 상기 영역을 공개하기 위한 등록 정보를 등록하는

를 포함하는 개인 정보 보호를 위한 방법.

청구항 4

제1항에 있어서,

상기 최종 영상 정보를 획득하는 단계는,

상기 검색된 적어도 하나 이상의 프라이버시 노출 가능성이 있는 영역을 기 등록된 등록 정보와 비교하고, 상기 비교를 통하여 상기 기 등록된 등록 정보에 포함되지 않은 영역을 미등록 영역으로 지정하고, 상기 검색된 적어도 하나 이상의 프라이버시 노출 가능성이 있는 영역 중 하나의 영역이 상기 기 등록된 등록 정보에 포함될 경우, 다음 영역이 기 등록된 등록 정보에 포함되는지 여부를 판단하는 단계

를 포함하는 개인 정보 보호를 위한 방법.

청구항 5

제4항에 있어서,
상기 최종 영상 정보를 획득하는 단계는,
상기 지정된 미등록 영역에 블러 처리, 모자이크 처리 또는 별도의 이미지로 대체하는 단계
를 포함하는 개인 정보 보호를 위한 방법.

청구항 6

제5항에 있어서,
상기 최종 영상 정보를 획득하는 단계는,
상기 미등록 영역에 프라이버시 보호를 위한 특정 처리가 수행된 최종 영상 정보를 업로드하고, 상기 업로드된
최종 영상 정보를 출력하는 단계
를 포함하는 개인 정보 보호를 위한 방법.

청구항 7

개인 정보 보호를 위한 시스템에 있어서,
소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 업로드되는 파일에 포함된
영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검출하는 검출부-상기 영상 정보는, 이미지 또는 동영상
상을 포함함-; 및
상기 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 비교함에 따라 미등록된 미등록 영역에 프라이버시
보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득하는 출력부
를 포함하는 개인 정보 보호를 위한 시스템.

발명의 설명

기술 분야

[0001] 아래의 설명은 사람의 얼굴을 검출하고 얼굴을 인식하여 기 등록된 사용자와의 매칭을 통해서 기 등록되지 않은
사용자의 얼굴을 처리하는 이미지 및 영상 처리 기술에 관한 것이다.

배경 기술

[0003] 이미지 및 영상 데이터로부터 얼굴 검출(Face Detection) 및 얼굴 인식 (Face Recognition) 기술은 지난 수십
년간 연구 개발되어 있으며 이 기술은 관련 기술에 익숙한 사람은 누구나 기존의 기술을 활용하여 구현이 가능
하다. 기존 기술은 얼굴 검출의 정확도를 높이기 위한 방법(예: 대한민국 특허 10-1347573, "디지털 이미지 상
에서의 얼굴 검출 방법 및 장치"), 얼굴 인식의 정확도를 높이기 위한 방법(예: 대한민국 특허 10-1443031, "얼
굴 인식 서비스 제공 방법") 및 이를 기반으로 사용자의 얼굴을 인식하여 사용자 인증을 위한 서비스 제공(예:
대한민국 특허 10-1468192, "스마트워크 환경에서의 얼굴인식기반 사용자인증 기법")을 다룬다.

[0004] 검출된 얼굴 이미지의 은폐 기술과 관련하여 미국 구글사의(Alphabet Inc.) Street View 서비스의 경우 개인들
의 얼굴을 포함한 프라이버시 이미지가 무작위로 노출될 수 있으며 이는 심각한 프라이버시 문제를 초래하였다.
이에 따라서 얼굴 부위를 검출하여 그 부위를 처리하여(예: 도 1 의image blur 기법 적용) 서비스에 적용하는
방식이 일반적이다. 도 1을 참고하면, Street View 이미지에서 얼굴 검출을 통하여 검출된 얼굴을 블러 처리하
는 예이다. 이와 관련하여 얼굴 및 프라이버시 노출이 가능한 다른 정보, 예를 들어 자동차 번호판 등을 블러
처리하는 기술(예: US8,571,354, "Method of and arrangement for blurring an image")이 제시된 바 있다.

[0005] 이미지의 선택적인 배포 기술은 미국 스냅챗(Snapchat Inc.)사에서 등록한 특허(US9,396,354, "Apparatus and
method for automated privacy protection in distributed images")는 프라이버시 보호를 인식된 얼굴을 기반

으로 이미지의 배포 유무의 결정 및 채팅창에서 지속시간을 제어하는 기법에 대한 발명을 제시한다.

발명의 내용

해결하려는 과제

- [0007] 소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 업로드 되는 이미지 중에서 비자발적으로 촬영된 사람들의 사적인 정보(예: 얼굴 및 신체)가 드러난 영상이나 이미지가 당사자의 의도와 무관하게 무제한적으로 노출되는 경우에 비자발적인 노출이 일어나는 경우의 개인의 사적인 정보를 보호하기 위한 방법 및 시스템을 제시한다.

과제의 해결 수단

- [0009] 보호 시스템에 의해 수행되는 개인 정보 보호를 위한 방법은, 소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 업로드되는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검출하는 단계-상기 영상 정보는, 이미지 또는 동영상을 포함함-; 및 상기 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 비교함에 따라 미등록된 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득하는 단계를 포함할 수 있다.
- [0010] 상기 영역을 검출하는 단계는, 소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 영상 정보를 업로드하고, 상기 업로드된 영상 정보로부터 프라이버시 노출 가능성이 있는 영역의 포함 여부를 검색하는 단계를 포함하고, 상기 프라이버시 노출 가능성이 있는 영역은, 얼굴, 신체의 일부 또는 신체의 전부 중 사용자를 식별 가능한 어느 하나의 영역을 포함할 수 있다.
- [0011] 상기 영역을 검출하는 단계는, 상기 소셜 미디어 또는 소셜 네트워크 서비스에 업로드되는 영상 정보에서 검출되는 프라이버시 노출 가능성이 있는 영역을 공개 또는 비공개하기 위한 등록 정보를 저장하는 단계를 포함하고, 상기 저장하는 단계에서, 상기 영상 정보에서 상기 영역을 공개하기 위한 등록 정보를 등록할 수 있다.
- [0012] 상기 최종 영상 정보를 획득하는 단계는, 상기 검색된 적어도 하나 이상의 프라이버시 노출 가능성이 있는 영역을 기 등록된 등록 정보와 비교하고, 상기 비교를 통하여 상기 기 등록된 등록 정보에 포함되지 않은 영역을 미등록 영역으로 지정하고, 상기 검색된 적어도 하나 이상의 프라이버시 노출 가능성이 있는 영역 중 하나의 영역이 상기 기 등록된 등록 정보에 포함될 경우, 다음 영역이 기 등록된 등록 정보에 포함되는지 여부를 판단하는 단계를 포함할 수 있다.
- [0013] 상기 최종 영상 정보를 획득하는 단계는, 상기 지정된 미등록 영역에 블러 처리, 모자이크 처리 또는 별도의 이미지로 대체하는 단계를 포함할 수 있다.
- [0014] 상기 최종 영상 정보를 획득하는 단계는, 상기 미등록 영역에 프라이버시 보호를 위한 특정 처리가 수행된 최종 영상 정보를 업로드하고, 상기 업로드된 최종 영상 정보를 출력하는 단계를 포함할 수 있다.
- [0015] 개인 정보 보호를 위한 시스템은, 소셜 미디어(Social Media) 또는 소셜 네트워크 서비스(Social Network Service)에 업로드되는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검출하는 검출부-상기 영상 정보는, 이미지 또는 동영상을 포함함-; 및 상기 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 비교함에 따라 미등록된 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득하는 출력부를 포함할 수 있다.

발명의 효과

- [0017] Social Networking 에서 무분별하게 업로드 되는 이미지 중에서 비자발적으로 촬영된 사람들의 사적인 정보(예: 얼굴 및 신체)가 드러난 영상이나 이미지가 당사자의 의도와 무관하게 노출되는 경우를 원천적으로 방지할 수 있다.

[0018] 사용자가 무분별하게 영상이나 이미지를 업로드하는 경우라 하더라도 시스템 상에서 사용자의 디바이스에 기 등록된 얼굴이 아닌 경우에 비자발적으로 촬영된 해당자의 사적인 정보를 보호하는 것이 가능하다.

도면의 간단한 설명

[0020] 도 1은 스트리트 뷰 이미지에서 얼굴 검출을 통하여 검출된 얼굴을 블러 처리하는 것을 나타낸 예이다.
 도 2는 얼굴 이미지에 이미지 처리를 수행하여 개인 정보를 보호하는 것을 나타낸 예이다.
 도 3은 얼굴 이미지를 변장 또는 변경하여 개인 정보를 보호하는 것을 나타낸 예이다.
 도 4는 일 실시예에 따른 보호 시스템의 구성을 설명하기 위한 블록도이다.
 도 5는 일 실시예에 따른 보호 시스템에서 영상 정보의 프라이버시를 보호하는 방법을 설명하기 위한 흐름도이다.
 도 6은 일 실시예에 따른 보호 시스템에서 영상 정보의 프라이버시를 보호하는 구체적인 방법을 설명하기 위한 흐름도이다.
 도 7은 일 실시예에 따른 보호 시스템에서 기 등록된 등록 정보의 여부에 따라 특정 처리를 수행하는 것을 나타낸 예이다.

발명을 실시하기 위한 구체적인 내용

[0021] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0023] 실시예에서는 얼굴 검출 및 인식 기술을 기반으로 한 미등록 사용자의 프라이버시를 보호하기 위한 새로운 방법 및 시스템을 설명하기로 한다.

[0024] 도 4는 일 실시예에 따른 보호 시스템의 구성을 설명하기 위한 블록도이다.

[0025] 보호 시스템(100)의 프로세서는 데이터 입력부(410), 얼굴 검색부(420), 비교부(430), 검출부(440), 처리부(450) 및 출력부(460)를 포함할 수 있다. 이러한 프로세서의 구성요소들은 보호 시스템에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다.

[0026] 데이터 입력부(410)는 소셜 미디어 또는 소셜 네트워크 서비스에 업로드되는 영상 정보가 입력됨을 수신할 수 있다. 데이터 입력부(410)는 사용자로부터 이미지 또는 동영상의 입력됨을 인식할 수 있다. 예를 들면, 데이터 입력부(410)는 사용자로부터 입력되는 영상 정보가 이미지 또는 동영상인지 여부를 식별할 수 있다. 데이터 입력부(410)는 사용자로부터 입력되는 영상 정보가 이미지일 경우, 이미지 모드로 전환할 수 있고, 사용자로부터 입력되는 영상 정보가 동영상일 경우, 동영상 모드로 전환할 수 있다. 이때, 이미지 모드와 동영상 모드에서 수행되는 프로세스는 거의 동일하나, 동영상 모드는 각각의 프레임마다 프라이버시 노출 가능성이 있는 영역을 검출하게 된다.

[0027] 검색부(430)는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검색할 수 있다. 검색부(430)는 프라이버시 노출 가능성이 있는 영역으로 얼굴, 신체의 일부 또는 신체의 전부 중 사용자를 식별 가능한 어느 하나의 영역을 검출할 수 있다. 검색부(430)는 프라이버시 노출 가능성이 있는 영역으로 얼굴을 검출하는 얼굴 검색부(420)를 포함할 수 있다.

[0028] 얼굴 검색부(420)는 이미지 또는 동영상으로부터 프라이버시 노출 가능성이 있는 얼굴을 검색할 수 있다. 예를 들면, 얼굴 검출 및 인식 기술은 매우 잘 알려진 기술로 다양한 기존 기술이 존재하며 실시예에서는 기존 기술 중에서 적절한 기술을 적용하는 것으로서 구현이 가능하다. 얼굴 검색부(420)는 OpenFace(<https://cmusatyalab.github.io/openface/>) 등의 Open Source 코드를 사용하여 구현할 수 있다. 또는, 얼굴 검색부(420)는 얼굴의 색상 정보에 기초하여 얼굴을 검색할 수도 있다. 또한, 얼굴 검색부(420)는 얼굴 이외에도 사용자를 식별할 수 있는 고유 정보를 검색할 수도 있다.

[0029] 비교부(430)는 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 함께 비교할 수 있다. 이때, 저장부(미

도시됨)는 사전에 프라이버시 노출 가능성이 있는 영역을 공개 또는 비공개하기 위한 등록 정보를 저장해놓을 수 있다. 예를 들면, 저장부는 영상 정보에 영역을 공개하기 위한 등록 정보를 등록할 수 있다. 다시 말해서, 저장부에 등록된 영역은 추후에 공개가 허용된 영역을 의미할 수 있다. 이에 따라, 추후에 등록 정보에 포함되지 않는 영역에 영상 처리가 수행될 수 있다. 또한, 저장부에 등록되는 등록 정보가 업데이트될 때마다 영상 정보로부터 검출된 영역과 등록 정보를 비교할 수 있다. 반대로, 저장부는 영상 정보에 영역을 비공개하기 위한 등록 정보를 등록하여, 추후에 등록 정보에 포함되는 영역에 영상 처리가 수행될 수도 있다.

[0030] 검출부(440)는 검색된 적어도 하나 이상의 프라이버시 노출 가능성이 있는 영역을 기 등록된 등록 정보와 비교함에 따라 기 등록된 등록 정보에 포함되지 않은 영역을 미등록 영역으로 지정할 수 있다.

[0031] 처리부(450)는 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행할 수 있다. 처리부(450)는 미등록 영역에 블러 처리, 모자이크 처리 또는 별도의 이미지로 대체할 수 있다. 도 2를 참고하면, 크롭된 얼굴 이미지를 나타낸 것으로, 크롭된 얼굴 이미지를 블러 처리한 것과 모자이크 처리한 것을 나타낸 예이다. 사적인 정보를 보호하기 위한 이미지 처리 기법을 통칭하여 De-identification 으로 포괄할 수 있으며 이를 위한 다양한 기법들이 존재한다. 예를 들면, 얼굴 이미지가 존재하는 경우 이미지 블러(image blur) 혹은 모자이크(mosaic) 기법 등을 사용하여 사적인 정보 보호가 가능하다. 또는, 얼굴 이미지를 변형하지 않고 헤어 스타일을 바꾸거나 변장을 시키거나 복장을 변경하거나 얼굴을 다른 얼굴로 교체하는 방법도 존재한다. 도 3을 참고하면, 얼굴 이미지에 대하여 변장하거나, 헤어스타일 및 얼굴/복장을 변경한 것을 나타낸 예이다. 이와 같이, 얼굴이 인식된 경우 신체 인식도 가능하며 신체도 얼굴과 마찬가지로 다양한 방법으로 de-identification 이 가능하다. 예를 들면, "De-identification for privacy protection in multimedia content: A survey", Slobodan Ribaric, Aladdin Ariyaeenia, Nikola Pavesic, Signal Processing: Image Communication, Volume 47, 2016, Pages 131-151 의 리뷰 논문에 도 2 및 도 3을 포함하는 다양한 De-identification 기법들에 대해서 제시되어 있다.

[0032] 출력부(460)는 미등록된 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득할 수 있다. 출력부(460)는 소셜 미디어 또는 소셜 네트워크 서비스에 최종 영상 정보가 게시될 수 있다. 다시 말해서, 출력부(460)는 소셜 미디어 또는 소셜 네트워크 서비스에 사용자로부터 등록되지 않은 정보가 보호된 상태로 이미지 또는 동영상을 제공할 수 있다.

[0033] 도 5는 일 실시예에 따른 보호 시스템에서 영상 정보의 프라이버시를 보호하는 방법을 설명하기 위한 흐름도이다.

[0034] 영상 정보의 프라이버시를 보호하는 방법은 보호 시스템에 의하여 수행될 수 있으며, 보호 시스템에 대한 설명은 도 4를 참고하기로 한다.

[0035] 단계(510)에서 보호 시스템은 소셜 미디어 또는 소셜 네트워크 서비스에 업로드되는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역을 검출할 수 있다. 이때, 영상 정보는 이미지 또는 동영상을 포함할 수 있다. 보호 시스템은 사용자로부터 소셜 미디어 또는 소셜 네트워크 서비스에 영상 정보가 업로드되는 것을 수신할 수 있다. 일례로, 보호 시스템은 소셜 미디어 또는 소셜 네트워크 서비스에 업로드되는 파일의 확장자 정보에 기초하여 영상 정보의 여부를 식별할 수 있다. 예를 들면, 보호 시스템은 jpg, mpeg, tif 등과 같이, 동영상 또는 이미지와 관련된 확장자 정보에 기초하여 영상 정보임을 확인할 수 있다. 보호 시스템은 업로드되는 영상 정보로부터 프라이버시 노출 가능성이 있는 영역의 포함 여부를 검색할 수 있다. 보호 시스템은 프라이버시 노출 가능성이 있는 영역으로 얼굴, 신체의 일부 또는 신체의 전부 중 사용자를 식별 가능한 어느 하나 이상의 영역을 검색할 수 있다. 이때, 보호 시스템은 업로드되는 영상 정보에서 검출되는 프라이버시 노출 가능성이 있는 영역을 공개 또는 비공개하기 위한 등록 정보를 사전에 저장하고 있을 수 있다. 이때, 각각의 사용자에게 의하여 동의(허용)된 정보에 대하여 등록 정보로 등록될 수 있다. 예를 들면, 보호 시스템은 영상 정보에서 영역을 공개하기 위한 등록 정보를 등록할 수 있다.

[0036] 단계(520)에서 보호 시스템은 영상 정보로부터 검출된 영역과 기 등록된 등록 정보와 함께 비교함에 따라 미등록된 미등록 영역에 프라이버시 보호를 위한 특정 처리를 수행하여 최종 영상 정보를 획득할 수 있다. 보호 시스템은 검색된 적어도 하나 이상의 프라이버시 노출 가능성이 있는 영역을 기 등록된 등록 정보와 비교하고, 비교를 통하여 기 등록된 등록 정보에 포함되지 않은 영역을 미등록 영역으로 지정할 수 있다. 보호 시스템은 지정된 미등록 영역에 블러 처리, 모자이크 처리 또는 별도의 이미지로 대체할 수 있다. 보호 시스템은 미등록 영역에 프라이버시 보호를 위한 특정 처리가 수행된 최종 영상 정보를 업로드하고, 상기 업로드된 최종 영상 정보를 출력할 수 있다. 또한, 보호 시스템은 소셜 미디어 또는 소셜 네트워크 서비스에 게시된 영상 정보에 대

해서도 프라이버시 보호를 위한 특정 처리가 적용될 수 있다.

- [0037] 도 6은 일 실시예에 따른 보호 시스템에서 영상 정보의 프라이버시를 보호하는 구체적인 방법을 설명하기 위한 흐름도이다.
- [0038] 보호 시스템은 사용자로부터 동영상이나 이미지를 포함하는 영상 정보가 업로드되는 경우, 업로드 과정에서 사전에 사용자로부터 기 등록된 얼굴이 아닌 제 3자의 얼굴이 검색되는 경우, 다양한 기법을 사용하여 해당 얼굴의 사적인 정보를 보호하기 위한 방법을 구체적으로 설명하기로 한다. 도 6에서는, 영상 정보로 이미지를 예를 들어 설명하기로 한다. 이때, 동영상에도 마찬가지로의 프로세스가 적용될 수 있다.
- [0039] 보호 시스템은 사용자로부터 소셜 미디어 또는 소셜 네트워크 서비스에 업로드될 이미지를 수집할 수 있다(610). 이때, 사용자의 디바이스에 소셜 미디어 또는 소셜 네트워크 서비스를 위한 어플리케이션을 실행함에 따라 이미지가 업로드될 수 있다. 또는, 소셜 미디어 또는 소셜 네트워크 서비스를 위한 웹 검색을 통하여 해당 소셜 미디어 또는 소셜 네트워크 서비스에 접속함에 따라 이미지가 업로드될 수 있다.
- [0040] 보호 시스템은 업로드되는 이미지로부터 얼굴을 검출할 수 있다(620). 예를 들면, 얼굴 이외에도 신체의 일부, 신체의 전부 등과 같이 사용자를 검출할 수 있다. 또한, 보호 시스템은 이미지로부터 하나의 얼굴을 검출함에 따라 또 다른 얼굴들이 존재하는지 판단하여, 다음 얼굴을 검출할 수 있다(630). 만약, 보호 시스템은 미지로부터 복수 개의 얼굴이 감지됨에 따라 차례로 하나의 얼굴을 검출한 후, 다른 얼굴을 검출할 수 있다. 예를 들면, 업로드되는 이미지의 사이즈에 기초하여 기준점을 설정하고, 상, 하, 좌, 우의 순서로 얼굴이 존재하는지 여부를 감지할 수 있다. 또는, 시계 방향 또는 반시계 방향으로 얼굴이 존재하는지 여부를 감지할 수도 있다. 보호 시스템은 새로운 얼굴이 존재하는지 여부를 판단할 수 있다(640). 보호 시스템은 새로운 얼굴이 존재하지 않을 경우, 프로세스를 종료할 수 있다. 보호 시스템은 새로운 얼굴이 존재할 경우, 새로운 얼굴을 인식할 수 있다(650).
- [0041] 보호 시스템은 새로운 얼굴, 다시 말해서, 인식된 얼굴이 기 등록된 사용자와 매치되는지 여부를 판단할 수 있다(660). 예를 들면, 보호 시스템은 새로운 얼굴이 기 등록된 사용자의 얼굴과 매치될 경우, 단계(630)의 다음의 얼굴을 검출할 수 있다. 이와 같이, 보호 시스템은 새로운 얼굴이 기 등록된 사용자의 얼굴과 매치될 경우, 이미지에 존재하는 또 다른 얼굴을 감지하고, 새로운 얼굴이 있을 경우, 새로운 얼굴이 기 등록된 사용자의 얼굴과 매치되는지 여부를 판단할 수 있다. 보호 시스템은 새로운 얼굴, 다시 말해서, 인식된 얼굴이 기 등록된 사용자와 매치되는지 않을 경우, 새로운 얼굴을 미등록 얼굴로 인식하여 미등록 얼굴에 대하여 특정 처리를 수행할 수 있다(670). 다시 말해서, 보호 시스템은 미등록 얼굴에 대하여 블러 처리, 모자이크 처리 등과 같은 특정 처리를 통하여 미등록 얼굴을 감출 수 있다. 예를 들면, 보호 시스템은 사용자로부터 미등록 얼굴에 대한 특정 처리를 위한 유저 인터페이스를 제공할 수 있고, 유저 인터페이스를 통하여 사용자의 조작에 의하여 미등록 얼굴에 대한 특정 처리가 이루어질 수 있다. 사용자는 유저 인터페이스를 통하여 외부에서 사용자가 원하는 이미지를 블러와 사용자가 원하는 이미지를 중첩시키거나, 시스템에서 제공하는 이미지(예를 들면, 이모티콘, 캐릭터, 스티커 등)를 미등록 얼굴에 대체할 수 있다. 또는, 사용자는 유저 인터페이스를 통하여 사용자가 직접 그린 그림을 미등록 얼굴 위에 부가할 수 있다.
- [0042] 도 7을 참고하면, 기 등록된 등록 정보의 여부에 따라 특정 처리를 수행하는 것을 나타낸 예이다. 예를 들면, 이미지에 존재하는 우측의 인물은 기 등록된 얼굴이며 좌측의 인물은 기 등록되지 않은 얼굴로 총 2개의 검출된 얼굴 중 기 등록되지 않은 사용자의 얼굴을 모자이크 처리 하거나 블러 처리한 경우를 나타낸다. 이러한 예시에 한정되는 것은 아니며, 제시하지 않은 다양한 기법을 사용하여 개인 정보 보호가 가능하다.
- [0043] 일 실시예에 따른 보호 시스템은 이미지의 배포는 하되 이미지 데이터 안에서 기 등록자의 프라이버시 정보는 노출하고 비 등록자의 프라이버시 정보만을 제거한 후 배포함으로써 개인 정보 보호가 가능하다. 또한, 네트워크와는 별도로 모든 처리를 로컬 디바이스에서 처리할 수 있다.
- [0044] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를

접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0045] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

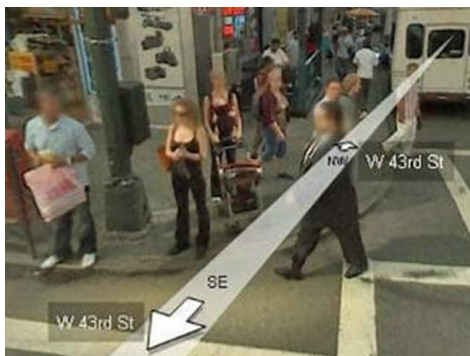
[0046] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0047] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

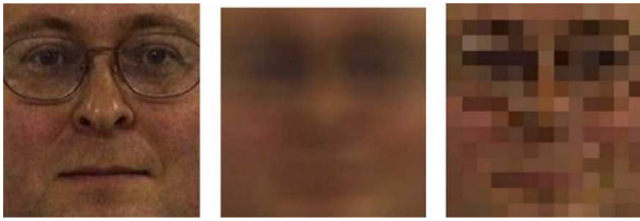
[0048] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

도면1



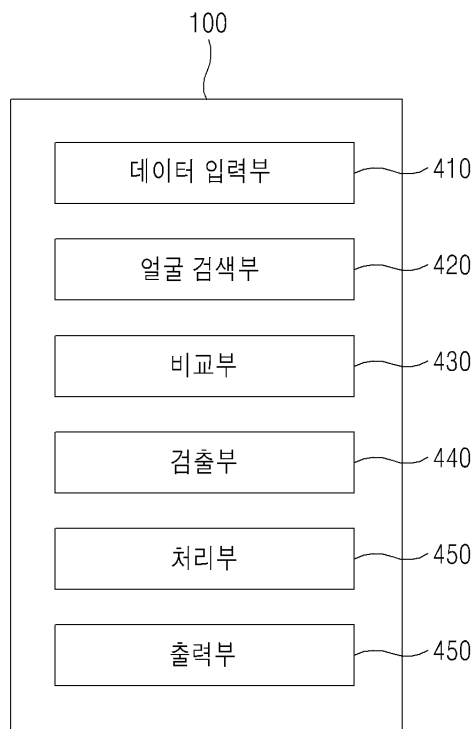
도면2



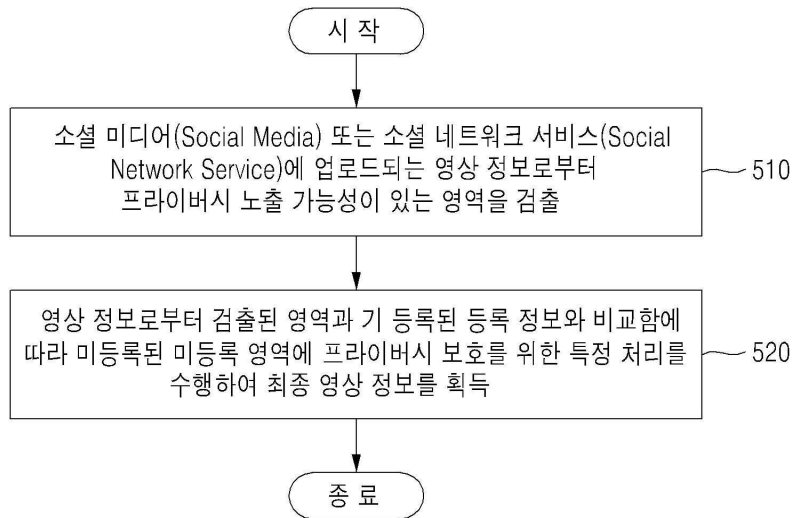
도면3



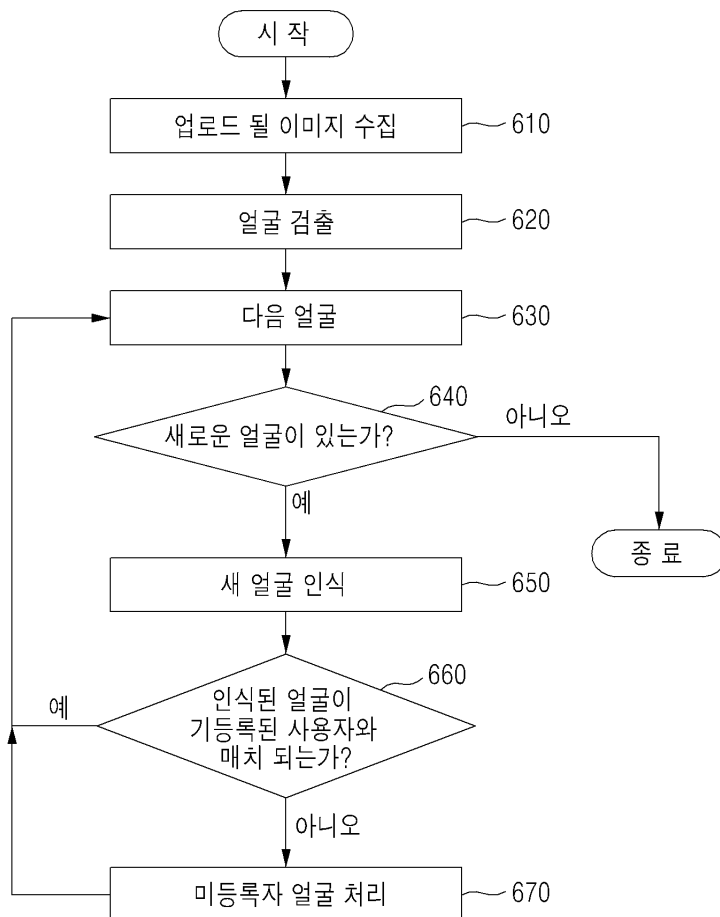
도면4



도면5



도면6



도면7

