



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년01월25일
(11) 등록번호 10-2629848
(24) 등록일자 2024년01월23일

(51) 국제특허분류(Int. Cl.)
G06F 18/00 (2023.01) G06T 3/40 (2024.01)
G06T 5/00 (2024.01) G06T 7/11 (2017.01)
G06V 10/40 (2022.01)
(52) CPC특허분류
G06V 40/172 (2022.01)
G06T 3/40 (2024.01)
(21) 출원번호 10-2021-0113143
(22) 출원일자 2021년08월26일
심사청구일자 2021년08월26일
(65) 공개번호 10-2023-0030907
(43) 공개일자 2023년03월07일
(56) 선행기술조사문헌
CN109670491 A*
KR1020200091799 A*
KR1020210069388 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
윤주범
서울특별시 송파구 충민로4길 19, 704동 401호(장지동, 송파파인타운7단지)
김수빈
서울특별시 광진구 동일로24길 5, 제103동 1803호(화양동, 화양동현대아파트)
(뒷면에 계속)
(74) 대리인
두호특허법인

전체 청구항 수 : 총 9 항

심사관 : 노용완

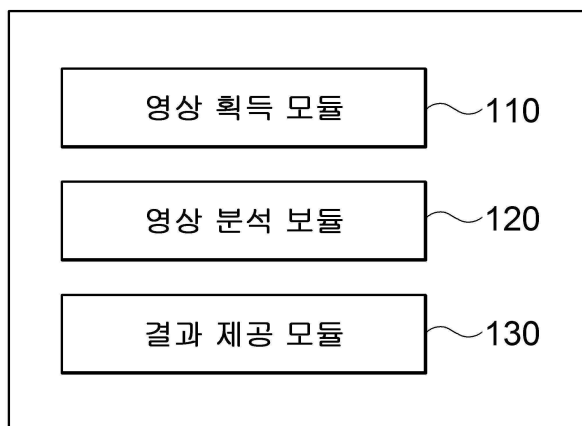
(54) 발명의 명칭 **가짜 영상 탐지 방법 및 이를 수행하기 위한 장치**

(57) 요약

가짜 영상 탐지 방법 및 이를 수행하기 위한 장치가 개시된다. 본 발명의 일 실시예에 따른 가짜 영상 탐지 방법 및 이를 수행하기 위한 장치는 하나 이상의 프로세서들; 메모리; 및 하나 이상의 프로그램들을 포함하고, 상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며, 상기 하나 이상의 프로그램들은, 의심 영상을 획득하기 위한 명령, 상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하기 위한 명령 및 상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하기 위한 명령을 포함한다.

대표도 - 도1

100



(52) CPC특허분류

- G06T 5/70 (2024.01)
- G06T 7/11 (2017.01)
- G06V 10/40 (2023.08)
- G06V 40/168 (2022.01)
- G06T 2207/30201 (2013.01)

정윤성

경기도 광주시 회안대로 637-35, 101동 1805호(탄
별동, 경남아너스빌 1단지)

(72) 발명자

김성진

서울특별시 광진구 천호대로 537, 정익제이타워 2
차 916호(중곡동)

강병준

충청남도 천안시 동남구 풍세로 705, 102동 509호
(신방동, 현대아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711126109
과제번호	2018-0-01423-004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터지원사업
연구과제명	지능형 비행로봇 융합기술 연구
기 여 율	1/2
과제수행기관명	세종대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711126138
과제번호	2020-0-01602-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성(R&D)
연구과제명	지능형 사이버 위협 대응 기술 개발 및 인력양성
기 여 율	1/2
과제수행기관명	송실대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

명세서

청구범위

청구항 1

하나 이상의 프로세서들;

메모리; 및

하나 이상의 프로그램들을 포함하고,

상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며,

상기 하나 이상의 프로그램들은,

의심 영상을 획득하기 위한 명령;

상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하기 위한 명령; 및

상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하기 위한 명령을 포함하며,

상기 분석하기 위한 명령은,

상기 획득한 의심 영상의 프레임에서 얼굴 이미지를 추출하여 데이터 세트를 생성하기 위한 명령; 및

머신러닝(Machine Learning) 모듈을 이용하여 상기 데이터 세트를 입력받고, 상기 데이터 세트로부터 상기 의심 영상의 위변조 여부를 분류하기 위한 명령을 더 포함하며,

상기 의심 영상의 위변조 여부를 분류하기 위한 명령은,

노이즈 제거 모듈을 이용하여 상기 데이터 세트를 입력 받고, 상기 데이터 세트에 포함된 각각의 얼굴 이미지에서 노이즈를 제거하여 노이즈 제거 이미지를 생성하기 위한 명령;

특징 추출 모듈을 이용하여 상기 노이즈 제거 이미지를 입력 받고, 상기 노이즈 제거 이미지의 특징값을 추출하기 위한 명령; 및

분류 모듈을 이용하여 상기 노이즈 제거 이미지의 특징값을 입력 받고, 상기 노이즈 제거 이미지의 특징값을 기반으로 상기 의심 영상에 대한 위변조 여부를 분석하기 위하여 카테고리 분류를 수행하기 위한 명령을 더 포함하며,

상기 특징 추출 모듈은,

입력 영상으로부터 노이즈 제거 이미지를 입력받고, 정상 영상의 노이즈 제거 이미지와 위변조 영상의 노이즈 제거 이미지를 비교하여 특징점 영역을 설정하며, 상기 설정된 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 상기 입력 영상으로부터 입력된 노이즈 제거 이미지의 특징값을 추출하도록 학습되며,

상기 특징점 영역은, 상기 노이즈 제거 이미지에서 인접 픽셀들간의 RGB값의 급격한 변화에 따라 일관성을 판단하여 설정되는, 컴퓨팅 장치.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 데이터 세트를 생성하기 위한 명령은,
 상기 획득한 의심 영상에 포함된 각각의 영상 프레임을 추출하기 위한 명령;
 상기 추출된 각각의 영상 프레임에서 얼굴 영역을 추출하여 상기 얼굴 이미지를 생성하기 위한 명령; 및
 상기 얼굴 이미지를 각각 동일한 픽셀로 크기를 조정하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 4

삭제

청구항 5

삭제

청구항 6

청구항 1에 있어서,
 상기 분류 모듈은,
 상기 추출된 노이즈 제거 이미지의 특징값을 입력받고, 상기 정상 영상으로부터 추출된 노이즈 제거 이미지의 특징값 및 상기 위변조 영상으로부터 추출된 노이즈 제거 이미지의 특징값을 기반으로 상기 입력 영상으로부터 추출된 노이즈 제거 이미지의 특징값에 대한 카테고리를 분류하도록 학습되는, 컴퓨팅 장치.

청구항 7

청구항 1에 있어서,
 상기 분석 정보를 생성하기 위한 명령은,
 상기 분석 결과를 기반으로 상기 의심 영상에서 얼굴 영역에 대한 위변조 확률 및 위변조 의심 영역을 표시하여 사용자에게 제공하기 위한 명령; 및
 상기 분석 결과에 따라 상기 사용자에게 신고 기능을 제공하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 8

하나 이상의 프로세서들, 및
 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 가짜 영상 탐지 방법으로서,
 의심 영상을 획득하는 단계;
 상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하는 단계; 및
 상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하는 단계를 포함하며,
 상기 분석하는 단계는,
 상기 획득한 의심 영상의 프레임에서 얼굴 이미지를 추출하여 데이터 세트를 생성하는 단계; 및
 머신러닝(Machine Learning) 모듈을 이용하여 상기 데이터 세트를 입력받고, 상기 데이터 세트로부터 상기 의심 영상의 위변조 여부를 분류하는 단계를 더 포함하며,
 상기 의심 영상의 위변조 여부를 분류하는 단계는,
 노이즈 제거 모듈을 이용하여 상기 데이터 세트를 입력 받고, 상기 데이터 세트에 포함된 각각의 얼굴 이미지에

서 노이즈를 제거하여 노이즈 제거 이미지를 생성하는 단계;

특징 추출 모듈을 이용하여 상기 노이즈 제거 이미지를 입력 받고, 상기 노이즈 제거 이미지의 특징값을 추출하는 단계; 및

분류 모듈을 이용하여 상기 노이즈 제거 이미지의 특징값을 입력 받고, 상기 노이즈 제거 이미지의 특징값을 기반으로 상기 의심 영상에 대한 위변조 여부를 분석하기 위하여 카테고리 분류를 수행하는 단계를 더 포함하며,

상기 특징 추출 모듈은,

입력 영상으로부터 노이즈 제거 이미지를 입력받고, 정상 영상의 노이즈 제거 이미지와 위변조 영상의 노이즈 제거 이미지를 비교하여 특징점 영역을 설정하며, 상기 설정된 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 상기 입력 영상으로부터 입력된 노이즈 제거 이미지의 특징값을 추출하도록 학습되며,

상기 특징점 영역은, 상기 노이즈 제거 이미지에서 인접 픽셀들간의 RGB값의 급격한 변화에 따라 일관성을 판단하여 설정되는, 가짜 영상 탐지 방법.

청구항 9

삭제

청구항 10

청구항 8에 있어서,

상기 데이터 세트를 생성하는 단계는,

상기 획득한 의심 영상에 포함된 각각의 영상 프레임을 추출하는 단계;

상기 추출된 각각의 영상 프레임에서 얼굴 영역을 추출하여 상기 얼굴 이미지를 생성하는 단계; 및

상기 얼굴 이미지를 각각 동일한 픽셀로 크기를 조정하는 단계를 더 포함하는, 가짜 영상 탐지 방법.

청구항 11

삭제

청구항 12

삭제

청구항 13

청구항 8에 있어서,

상기 분류 모듈은,

상기 추출된 노이즈 제거 이미지의 특징값을 입력받고, 상기 정상 영상으로부터 추출된 노이즈 제거 이미지의 특징값 및 상기 위변조 영상으로부터 추출된 노이즈 제거 이미지의 특징값을 기반으로 상기 입력 영상으로부터 추출된 노이즈 제거 이미지의 특징값에 대한 카테고리를 분류하도록 학습되는, 가짜 영상 탐지 방법.

청구항 14

청구항 8에 있어서,

상기 분석 정보를 생성하는 단계는,

상기 분석 결과를 기반으로 상기 의심 영상에서 얼굴 영역에 대한 위변조 확률 및 위변조 의심 영역을 표시하여 사용자에게 제공하는 단계; 및

상기 분석 결과에 따라 상기 사용자에게 신고 기능을 제공하는 단계를 더 포함하는, 가짜 영상 탐지 방법.

청구항 15

비일시적 컴퓨터 판독 가능한 저장 매체(non-transitory computer readable storage medium)에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 하나 이상의 명령어들을 포함하고, 상기 명령어들은 하나 이상의 프로세서들을 갖는 컴퓨팅 장치에 의해 실행될 때, 상기 컴퓨팅 장치로 하여금,

의심 영상을 획득하고;

상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하고; 그리고

상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하도록 하며,

상기 컴퓨터 프로그램은, 상기 분석하기 위하여, 상기 컴퓨팅 장치로 하여금,

상기 획득한 의심 영상의 프레임에서 얼굴 이미지를 추출하여 데이터 세트를 생성하고, 그리고

머신러닝(Machine Learning) 모듈을 이용하여 상기 데이터 세트를 입력받고, 상기 데이터 세트로부터 상기 의심 영상의 위변조 여부를 분류하도록 하며,

상기 컴퓨터 프로그램은, 상기 의심 영상의 위변조 여부를 분류하기 위하여, 상기 컴퓨팅 장치로 하여금,

노이즈 제거 모듈을 이용하여 상기 데이터 세트를 입력 받고, 상기 데이터 세트에 포함된 각각의 얼굴 이미지에서 노이즈를 제거하여 노이즈 제거 이미지를 생성하고,

특징 추출 모듈을 이용하여 상기 노이즈 제거 이미지를 입력 받고, 상기 노이즈 제거 이미지의 특징값을 추출하고, 그리고

분류 모듈을 이용하여 상기 노이즈 제거 이미지의 특징값을 입력 받고, 상기 노이즈 제거 이미지의 특징값을 기반으로 상기 의심 영상에 대한 위변조 여부를 분석하기 위하여 카테고리 분류를 수행하도록 하며,

상기 특징 추출 모듈은,

입력 영상으로부터 노이즈 제거 이미지를 입력받고, 정상 영상의 노이즈 제거 이미지와 위변조 영상의 노이즈 제거 이미지를 비교하여 특징점 영역을 설정하며, 상기 설정된 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 상기 입력 영상으로부터 입력된 노이즈 제거 이미지의 특징값을 추출하도록 학습되며,

상기 특징점 영역은, 상기 노이즈 제거 이미지에서 인접 픽셀들간의 RGB값의 급격한 변화에 따라 일관성을 판단하여 설정되는, 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 가짜 영상 탐지 기술과 관련된다.

배경 기술

[0003] 디지털 카메라 및 모바일 폰의 발전으로 누구나 고화질의 디지털 이미지를 생성할 수 있게 되었으며, 특히 소셜 네트워크 서비스 (Social Network Services, SNS)의 영향으로 이미지를 업로드하고 공유하여 타인에게 사진을 유통할 수 있다.

[0004] 또한, 어도비 포토샵 (Adobe PhotoShop)과 같은 정교한 이미지 편집 소프트웨어와 소셜 네트워크 서비스 자체 이미지 편집 기능, 그리고, 다수 이미지 편집 어플리케이션 (application)의 보급으로 인해 원본 이미지를 쉽게 수정할 수 있게 되었다.

[0005] 최근에는 딥러닝 기술의 발전으로 특정 인물의 얼굴 등을 특정 영상에 합성하는 딥페이크(Deepfake)가 늘어나고 있으며, 특히, 딥페이크는 간단하고 정교하게 이루어지고 있어 이로 인한 피해 역시 늘어나고 있다.

[0006] 그러나, 이러한 가짜 이미지 또는 가짜 영상을 일일이 확인하기 어려울 뿐만 아니라 육안으로 위변조 여부를 파악하기 어려운 실정이다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허공보 제10-1159164(2012.06.18.)

발명의 내용

해결하려는 과제

[0009] 본 발명의 실시예들은 딥러닝 기술을 이용하여 업로드된 영상의 위변조 여부를 탐지하기 위한 것이다.

[0010] 또한, 본 발명의 실시예들은 업로드된 영상의 탐지 결과를 제공하고 신고 기능을 제공하기 위한 것이다.

과제의 해결 수단

[0012] 본 발명의 예시적인 실시예에 따르면, 하나 이상의 프로세서들, 메모리, 및 하나 이상의 프로그램들을 포함하고, 상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행 되도록 구성되며, 상기 하나 이상의 프로그램들은, 의심 영상을 획득하기 위한 명령, 상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하기 위한 명령 및 상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하기 위한 명령을 포함하는 컴퓨팅 장치가 제공된다.

[0013] 상기 분석하기 위한 명령은 상기 획득한 의심 영상의 프레임에서 얼굴 이미지를 추출하여 데이터 세트를 생성하기 위한 명령 및 머신러닝(Machine Learning) 모듈을 이용하여 상기 데이터 세트를 입력받고, 상기 데이터 세트로부터 상기 의심 영상의 위변조 여부를 분류하기 위한 명령을 더 포함할 수 있다.

[0014] 상기 데이터 세트를 생성하기 위한 명령은 상기 획득한 의심 영상에 포함된 각각의 영상 프레임을 추출하기 위한 명령, 상기 추출된 각각의 영상 프레임에서 얼굴 영역을 추출하여 상기 얼굴 이미지를 생성하기 위한 명령 및 상기 얼굴 이미지를 각각 동일한 픽셀로 크기를 조정하기 위한 명령을 더 포함할 수 있다.

[0015] 상기 의심 영상의 위변조 여부를 분류하기 위한 명령은 노이즈 제거 모듈을 이용하여 상기 데이터 세트를 입력 받고, 상기 데이터 세트에 포함된 각각의 얼굴 이미지에서 노이즈를 제거하여 노이즈 제거 이미지를 생성하기 위한 명령, 특징 추출 모듈을 이용하여 상기 노이즈 제거 이미지를 입력 받고, 상기 노이즈 제거 이미지의 특징값을 추출하기 위한 명령 및 분류 모듈을 이용하여 상기 노이즈 제거 이미지의 특징값을 입력 받고, 상기 노이즈 제거 이미지의 특징값을 기반으로 상기 의심 영상에 대한 위변조 여부를 분석하기 위하여 카테고리 분류를 수행하기 위한 명령을 더 포함할 수 있다.

[0016] 상기 특징 추출 모듈은 입력 영상으로부터 노이즈 제거 이미지를 입력받고, 정상 영상의 노이즈 제거 이미지와 위변조 영상의 노이즈 제거 이미지를 비교하여 특징점 영역을 설정하며, 상기 설정된 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 상기 입력 영상으로부터 입력된 노이즈 제거 이미지의 특징값을 추출하도록 학습될 수 있다.

[0017] 상기 분류 모듈은 상기 추출된 노이즈 제거 이미지의 특징값을 입력받고, 상기 정상 영상으로부터 추출된 노이즈 제거 이미지의 특징값 및 상기 위변조 영상으로부터 추출된 노이즈 제거 이미지의 특징값을 기반으로 상기 입력 영상으로부터 추출된 노이즈 제거 이미지의 특징값에 대한 카테고리를 분류하도록 학습될 수 있다.

[0018] 상기 분석 정보를 생성하기 위한 명령은 상기 분석 결과를 기반으로 상기 의심 영상에서 얼굴 영역에 대한 위변조 확률 및 위변조 의심 영역을 표시하여 사용자에게 제공하기 위한 명령 및 상기 분석 결과에 따라 상기 사용자에게 신고 기능을 제공하기 위한 명령을 더 포함할 수 있다.

- [0019] 본 발명의 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 가짜 영상 탐지 방법으로서, 의심 영상을 획득하는 단계, 상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하는 단계 및 상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하는 단계를 포함하는 가짜 영상 탐지 방법이 제공된다.
- [0020] 상기 분석하는 단계는 상기 획득한 의심 영상의 프레임에서 얼굴 이미지를 추출하여 데이터 세트를 생성하는 단계 및 머신러닝(Machine Learning) 모듈을 이용하여 상기 데이터 세트를 입력받고, 상기 데이터 세트로부터 상기 의심 영상의 위변조 여부를 분류하는 단계를 더 포함할 수 있다.
- [0021] 상기 데이터 세트를 생성하는 단계는 상기 획득한 의심 영상에 포함된 각각의 영상 프레임을 추출하는 단계, 상기 추출된 각각의 영상 프레임에서 얼굴 영역을 추출하여 상기 얼굴 이미지를 생성하는 단계 및 상기 얼굴 이미지를 각각 동일한 픽셀로 크기를 조정하는 단계를 더 포함할 수 있다.
- [0022] 상기 의심 영상의 위변조 여부를 분류하는 단계는 노이즈 제거 모듈을 이용하여 상기 데이터 세트를 입력 받고, 상기 데이터 세트에 포함된 각각의 얼굴 이미지에서 노이즈를 제거하여 노이즈 제거 이미지를 생성하는 단계, 특징 추출 모듈을 이용하여 상기 노이즈 제거 이미지를 입력 받고, 상기 노이즈 제거 이미지의 특징값을 추출하는 단계 및 분류 모듈을 이용하여 상기 노이즈 제거 이미지의 특징값을 입력 받고, 상기 노이즈 제거 이미지의 특징값을 기반으로 상기 의심 영상에 대한 위변조 여부를 분석하기 위하여 카테고리 분류를 수행하는 단계를 더 포함할 수 있다.
- [0023] 상기 특징 추출 모듈은 입력 영상으로부터 노이즈 제거 이미지를 입력받고, 정상 영상의 노이즈 제거 이미지와 위변조 영상의 노이즈 제거 이미지를 비교하여 특징점 영역을 설정하며, 상기 설정된 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 상기 입력 영상으로부터 입력된 노이즈 제거 이미지의 특징값을 추출하도록 학습될 수 있다.
- [0024] 상기 분류 모듈은 상기 추출된 노이즈 제거 이미지의 특징값을 입력받고, 상기 정상 영상으로부터 추출된 노이즈 제거 이미지의 특징값 및 상기 위변조 영상으로부터 추출된 노이즈 제거 이미지의 특징값을 기반으로 상기 입력 영상으로부터 추출된 노이즈 제거 이미지의 특징값에 대한 카테고리를 분류하도록 학습될 수 있다.
- [0025] 상기 분석 정보를 생성하는 단계는 상기 분석 결과를 기반으로 상기 의심 영상에서 얼굴 영역에 대한 위변조 확률 및 위변조 의심 영역을 표시하여 사용자에게 제공하는 단계 및 상기 분석 결과에 따라 상기 사용자에게 신고 기능을 제공하는 단계를 더 포함할 수 있다.
- [0026] 본 발명의 또 다른 예시적인 실시예에 따르면, 비일시적 컴퓨터 판독 가능한 저장 매체(non-transitory computer readable storage medium)에 저장된 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은 하나 이상의 명령어들을 포함하고, 상기 명령어들은 하나 이상의 프로세서들을 갖는 컴퓨팅 장치에 의해 실행될 때, 상기 컴퓨팅 장치로 하여금, 의심 영상을 획득하고, 상기 의심 영상에서 얼굴 영역을 추출하고, 상기 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 상기 의심 영상의 위변조 여부를 분석하고, 그리고, 상기 의심 영상의 위변조 여부를 분석한 분석 결과를 기반으로 분석 정보를 생성하도록 하는 컴퓨터 프로그램이 제공된다.

발명의 효과

- [0028] 본 발명의 실시예들에 따르면, 딥러닝 기술을 이용하여 업로드된 영상의 위변조 여부를 탐지함으로써, 누구나 영상의 위변조 여부를 확인할 수 있으며, 빠르게 위변조 여부를 확인하고, 탐지 정확도를 높일 수 있다.
- [0029] 또한, 본 발명의 실시예들에 따르면, 업로드된 영상의 탐지 결과 및 신고 기능을 제공함으로써, 사용자가 간편하게 신고할 수 있다.

도면의 간단한 설명

- [0031] 도 1은 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치를 나타낸 블록도
- 도 2는 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치의 영상 분석 모듈을 설명하기 위한 블록도
- 도 3은 본 발명의 일 실시예에 따른 가짜 영상 탐지 방법을 설명하기 위한 흐름도

도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

- [0032] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.
- [0033] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 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. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.
- [0034] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다. 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.
- [0035] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.
- [0037] 도 1은 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치를 나타낸 블록도이다.
- [0038] 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치(100)는 영상 획득 모듈(110), 영상 분석 모듈(120) 및 결과 제공 모듈(130)을 포함할 수 있다.
- [0039] 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 "모듈"은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것은 아니다.
- [0040] 영상 획득 모듈(110)은 위변조가 의심되는 영상(의심 영상)을 획득할 수 있다. 예를 들어, 영상 획득 모듈(110)은 위변조된 영상을 발견한 사용자 단말로부터 의심 영상을 획득할 수 있다. 또한, 영상 획득 모듈(110)은 외부서버(예를 들어, 소셜 네트워크 서비스(SNS))에 업로드된 영상 중에서 의심 영상을 획득할 수 있다. 여기서, 의심 영상은 특정 인물의 얼굴 등을 특정 영상에 합성한 딥페이크(Deepfake) 영상일 수 있다.
- [0041] 영상 획득 모듈(110)은 획득한 의심 영상을 영상 분석 모듈(120)로 제공할 수 있다.
- [0043] 영상 분석 모듈(120)은 의심 영상에서 얼굴 영역을 추출하고, 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 의심 영상의 위변조 여부를 분석할 수 있다. 영상 분석 모듈(120)의 동작 및 구성에 대한 자세한 설명은 도 2를 참조하여 후술하기로 한다.
- [0045] 결과 제공 모듈(130)은 영상 분석 모듈(120)로부터 출력된 분석 결과를 기반으로 분석 정보를 생성하여 사용자

에게 제공할 수 있다. 예를 들어, 결과 제공 모듈(130)은 획득한 의심 영상에서 얼굴 영역에 대한 위변조 확률을 표시하고, 위변조 의심 영역에 대한 정보를 사용자에게 제공할 수 있다. 여기서, 위변조 의심 영역에 대한 정보는 위변조 의심 영역을 표시하고, 변조 흔적이 탐지된 의심 영역에 대한 상세 이미지 등일 수 있다.

[0046] 또한, 결과 제공 모듈(130)은 분석 결과에 따라 신고 기능을 제공할 수 있다. 예를 들어, 결과 제공 모듈(130)은 분석 정보를 문서 수정이 불가하게 처리된 pdf 파일로 사용자에게 제공할 수 있다. 또한, 결과 제공 모듈(130)은 분석 결과에 따라 의심 영상이 위변조 영상으로 판단된 경우, 신고 기능을 활성화할 수 있다. 이를 통하여 사용자는 신고 기능을 통하여 사이버 수사대의 사이버범죄 신고시스템(Electronic Cybercrime Report & Management system; ECRM)으로 연결될 수 있으며, 결과 제공 모듈(130)에서 제공하는 분석 정보(pdf 파일)를 이용하여 ECRM으로 위변조 영상을 신고할 수 있다.

[0047] 따라서, 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치는 딥러닝 기술을 이용하여 업로드된 영상의 위변조 여부를 탐지함으로써, 누구나 영상의 위변조 여부를 확인할 수 있으며, 빠르게 위변조 여부를 확인하고, 탐지 정확도를 높일 수 있다.

[0048] 또한, 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치는 업로드된 영상의 탐지 결과 및 신고 기능을 제공함으로써, 사용자가 간편하게 신고할 수 있다.

[0050] 도 2는 본 발명의 일 실시예에 따른 가짜 영상 탐지 장치의 영상 분석 모듈을 설명하기 위한 블록도이다.

[0051] 도 2를 참조하면, 영상 분석 모듈(120)은 전처리 모듈(121) 및 머신러닝 모듈(122)을 포함할 수 있다.

[0052] 전처리 모듈(121)은 영상 획득 모듈(110)로부터 입력된 영상의 프레임에서 얼굴 이미지(의심 영상에서 얼굴 영역을 추출한 이미지)를 추출하여 데이터 세트를 생성할 수 있다. 구체적으로, 전처리 모듈(121)은 영상 획득 모듈(110)로부터 입력된 영상에 포함된 각각의 영상 프레임을 추출하고, 추출된 각각의 영상 프레임에서 얼굴 영역을 추출하여 데이터 세트를 생성할 수 있다. 한편, 전처리 모듈(121)은 기 공지된 얼굴 검출 기법을 이용하여 얼굴 영역을 추출할 수 있다. 예를 들어, 전처리 모듈(121)은 얼굴을 검출해내는 Face Detection 태스크, 눈, 코 입의 좌표를 알아내는 Face Alignment 태스크 및 얼굴 위치를 나타내는 박스의 위치를 세밀하게 조절해주는 Bounding box regression 태스크 중 적어도 하나를 이용할 수 있다. 또한, 전처리 모듈(121)은 추출된 얼굴 영역을 각각 동일한 크기(예를 들어, 380 * 380)로 재조정할 수 있다.

[0053] 전처리 모듈(121)은 생성된 데이터 세트를 머신러닝 모듈(122)로 전달할 수 있다.

[0055] 머신러닝 모듈(122)은 전처리 모듈(121)로부터 제공된 데이터 세트가 입력되면, 머신러닝(Machine Learning) 기반 기술을 사용하여 의심 영상의 위변조 여부를 분류(REAL 또는 FAKE)하도록 학습된다. 즉, 머신러닝 모듈(122)은 전처리 모듈(121)로부터 데이터 세트를 입력 받고, 데이터 세트에 포함된 각각의 얼굴 이미지의 특징값을 추출하여 의심 영상의 위변조 여부를 분류하도록 학습된 머신러닝 모델로 구현될 수 있다.

[0056] 예시적인 실시예에서, 머신러닝 모듈(122)은 노이즈 제거 모듈(122a), 특징 추출 모듈(122b) 및 분류 모듈(122c)을 포함할 수 있다.

[0057] 노이즈 제거 모듈(122a)은 머신러닝 모듈(122)의 일부를 구성하는 신경망일 수 있다. 노이즈 제거 모듈(122a)은 입력되는 데이터 세트에 포함된 각각의 얼굴 이미지에 대한 노이즈를 제거할 수 있다.

[0058] 예시적인 실시예에서, 노이즈 제거 모듈(122a)은 전처리 모듈(121)로부터 데이터 세트를 입력받아 데이터 세트에 포함된 각각의 얼굴 이미지에서 노이즈를 제거하여 노이즈 제거 이미지(노이즈가 제거된 얼굴 이미지)를 생성할 수 있다. 이 때, 노이즈 제거 모듈(122a)은 데이터 세트를 입력받고, 데이터 세트에 포함된 얼굴이미지 중에서 적대적 이미지(adversarial image)의 노이즈(왜곡)를 제거하도록 학습될 수 있다. 예를 들어, 노이즈 제거 모듈(122a)은 NSL(Neural Structured Learning) 알고리즘을 이용하여 얼굴 이미지에 대한 노이즈를 제거할 수 있다. 여기서, 적대적 이미지란 샘플(이미지)을 잘못 분류하도록 이미지의 손실 함수를 최대화한 이미지일 수 있다. 즉, 딥페이크 영상에는 머신러닝 모델에서 위변조 탐지를 오도(誤導)하도록 노이즈가 추가되어 있을 수 있다. 이러한 노이즈에 의하여 머신러닝 모듈(122)이 딥페이크 영상에서 얼굴 이미지를 왜곡하여 인식하게 됨으로써, 의심 영상에 대한 위변조 탐지율이 저하될 수 있다. 따라서, 노이즈 제거 모듈(122a)은 NSL(Neural Structured Learning) 알고리즘을 이용하여 얼굴 이미지에 대한 노이즈를 제거함으로써, 머신러닝 모듈(122)의 탐지 정확도가 높아질 수 있다. 한편, 본 발명에서는 NSL 알고리즘을 이용하여 노이즈를 제거하였으나, 이에 한정되는 것은 아니다.

[0059] 특징 추출 모듈(122b)은 머신러닝 모듈(122)의 일부를 구성하는 신경망일 수 있다. 특징 추출 모듈(122b)은 노

이즈 제거 이미지의 특징값을 추출할 수 있다.

- [0060] 예시적인 실시예에서, 특징 추출 모듈(122b)은 노이즈 제거 모듈(122a)로부터 노이즈 제거 이미지를 입력받아 노이즈 제거 이미지에서 기 설정된 특징점 영역을 추출하고, 해당 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 노이즈 제거 이미지의 특징값을 추출할 수 있다. 이 때, 특징 추출 모듈(122b)은 입력 영상(정상 영상 또는 위변조 영상)으로부터 노이즈 제거 이미지를 입력받고, 정상 영상의 노이즈 제거 이미지와 위변조 영상의 노이즈 제거 이미지를 비교하여 특징점 영역을 설정하여 해당 특징점 영역에 포함된 픽셀들의 RGB값을 기반으로 해당 노이즈 제거 이미지의 특징값을 추출하도록 학습될 수 있다. 여기서, 특징점 영역은 얼굴 영역(얼굴 이미지)에서 인접 픽셀들 간의 일관성을 판단(학습)하여 설정할 수 있으며, 일관성 여부의 판단은 인접 픽셀들 간의 RGB의 급격한 변화에 따라 결정될 수 있다. 예를 들어, 특징 추출 모듈(122b)은 CNN(Convolutional Neural Network)을 이용하여 노이즈 제거 이미지의 특징값을 추출할 수 있다. 한편, 본 발명에서는 CNN을 이용하여 이미지의 특징을 추출하였으나, 이에 한정되는 것은 아니다.
- [0061] 분류 모듈(122c)은 머신러닝 모듈(122)의 일부를 구성하는 신경망일 수 있다. 분류 모듈(122c)은 추출된 노이즈 제거 이미지의 특징값을 기반으로 의심 영상에 대한 위변조 여부를 분석하기 위하여 카테고리 분류를 수행할 수 있다.
- [0062] 예시적인 실시예에서, 분류 모듈(122c)은 특징 추출 모듈(122b)로부터 노이즈 제거 이미지의 특징값을 입력받아 의심 영상이 진실(real)인지 또는 거짓(fake)인지와 같은 위변조 여부를 분류할 수 있다. 이 때, 분류 모듈(122c)은 입력 영상(정상 영상 또는 위변조 영상)으로부터 추출된 노이즈 제거 이미지의 특징값을 입력받고, 정상 영상으로부터 추출된 노이즈 제거 이미지의 특징값 및 위변조 영상으로부터 추출된 노이즈 제거 이미지의 특징값을 기반으로 입력 영상으로부터 추출된 노이즈 제거 이미지의 특징값에 대한 카테고리를 분류(진실(정상 영상으로부터 추출된 특징값과 유사) 또는 거짓(위변조 영상으로부터 추출된 특징값과 유사))하도록 학습될 수 있다. 즉, 분류 모듈(122c)은 추출된 노이즈 제거 이미지의 특징값이 입력되는 경우, 머신러닝 모델에 의해 노이즈 제거 이미지의 특징값을 기반으로 의심 영상을 기 저장된 카테고리(진실, 거짓)에 따라 분류할 수 있다. 예를 들어, 분류 모듈(122c)은 SVM(Support Vector Machine)을 이용하여 카테고리 분류를 수행할 수 있다. 한편, 본 발명에서는 SVM을 이용하여 카테고리 분류를 수행하였으나, 이에 한정되는 것은 아니다.
- [0064] 도 3은 본 발명의 일 실시예에 따른 가짜 영상 탐지 방법을 설명하기 위한 흐름도이다. 도 3에 도시된 방법은 예를 들어, 전술한 가짜 영상 탐지 장치에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.
- [0065] 영상 획득 모듈(110)은 위변조가 의심되는 영상(의심 영상)을 획득한다(S302). 예를 들어, 영상 획득 모듈(110)은 위변조된 영상을 발견한 사용자 단말로부터 의심 영상을 획득할 수 있다. 또한, 영상 획득 모듈(110)은 외부서버(예를 들어, 소셜 네트워크 서비스(SNS))에 업로드된 영상 중에서 의심 영상을 획득할 수 있다. 여기서, 의심 영상은 특정 인물의 얼굴 등을 특정 영상에 합성한 딥페이크(Deepfake) 영상일 수 있다.
- [0066] 그 다음, 영상 분석 모듈(120)은 의심 영상에서 얼굴 영역을 추출하고, 추출된 얼굴 영역으로부터 머신러닝(Machine Learning) 기반 기술을 사용하여 의심 영상의 위변조 여부를 판단한다(S304). 구체적으로, 영상 분석 모듈(120)은 영상 획득 모듈(110)로부터 입력된 의심 영상의 프레임에서 얼굴 이미지(의심 영상에서 얼굴 영역을 추출한 이미지)를 추출하여 데이터 세트를 생성하고, 머신러닝 모듈(122)을 통하여 데이터 세트에 포함된 각각의 얼굴 이미지의 특징값을 추출하여 의심 영상의 위변조 여부를 분류할 수 있다. 머신러닝 모듈(122)은 데이터 세트로부터 의심 영상의 위변조 여부를 분류하도록 학습되는 머신러닝 모델을 포함할 수 있다.
- [0067] 마지막으로, 결과 제공 모듈(130)은 영상 분석 모듈(120)로부터 출력된 분석 결과를 기반으로 분석 정보를 생성하여 사용자에게 제공한다(S306). 예를 들어, 결과 제공 모듈(130)은 획득한 의심 영상에서 얼굴 영역에 대한 위변조 확률을 표시하고, 위변조 의심 영역에 대한 정보를 사용자에게 제공할 수 있다. 여기서, 위변조 의심 영역에 대한 정보는 위변조 의심 영역을 표시하고, 변조 흔적이 탐지된 의심 영역에 대한 상세 이미지 등일 수 있다.
- [0069] 도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

- [0070] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 가짜 영상 탐지 장치(100)일 수 있다.
- [0071] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.
- [0072] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)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 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.
- [0073] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.
- [0074] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.
- [0075] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

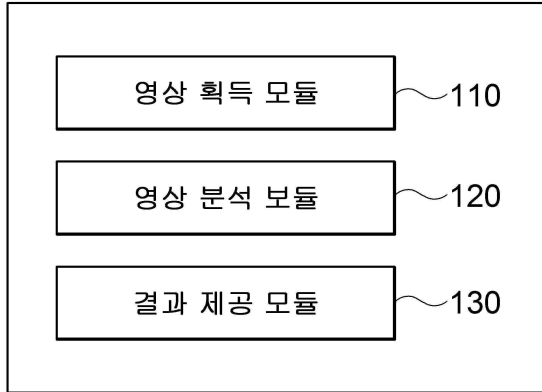
부호의 설명

- [0077] 100 : 가짜 영상 탐지 장치
- 110 : 영상 획득 모듈
- 120 : 영상 분석 모듈
- 121 : 전처리 모듈
- 122 : 머신러닝 모듈
- 122a : 노이즈 제거 모듈
- 122b : 특징 추출 모듈
- 122c : 분류 모듈
- 130 : 결과 제공 모듈

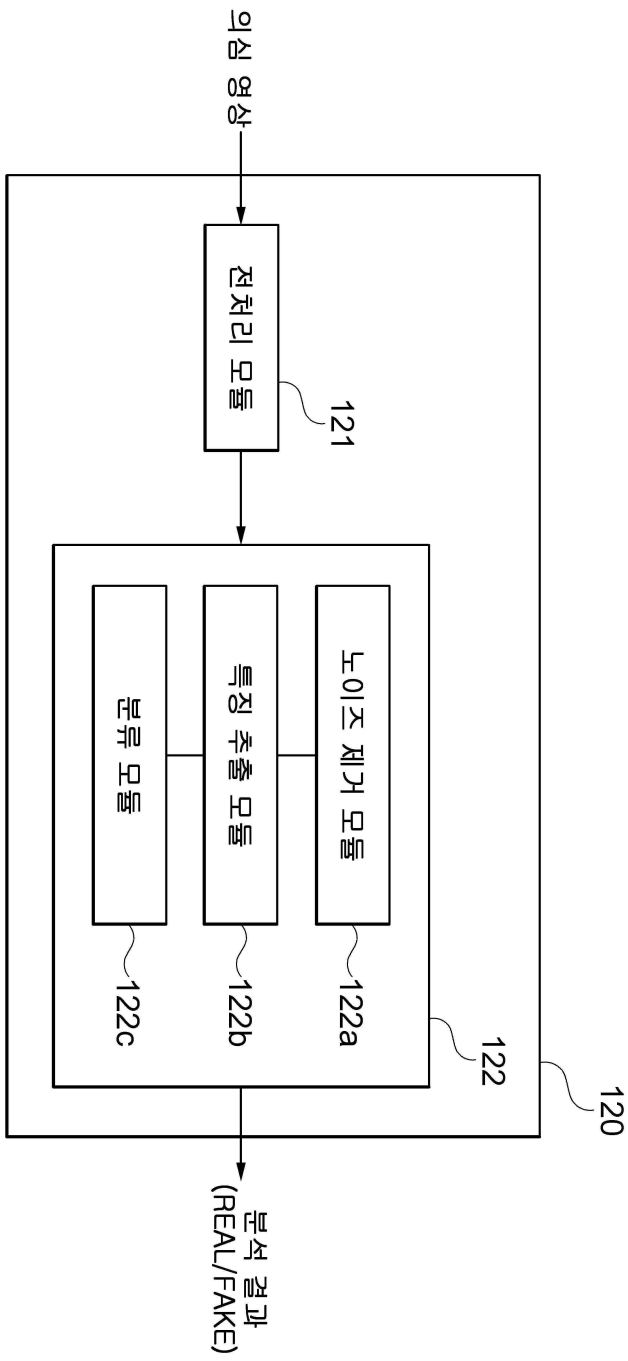
도면

도면1

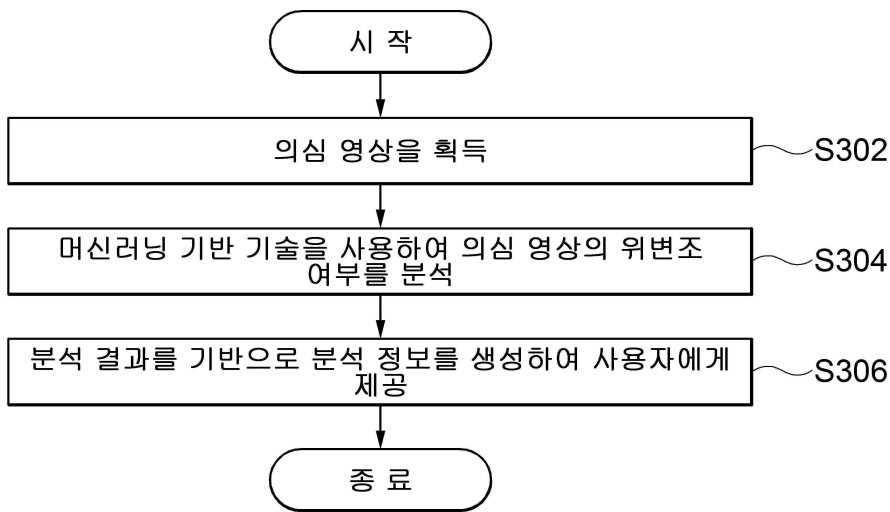
100



도면2



도면3



도면4

10

