(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년12월07일
(11) 등록번호 10-1925799
(24) 등록일자 2018년11월30일

(51) 국제특허분류(Int. Cl.)
G06F 21/84 (2013.01) *G06T 7/00* (2017.01)
H04N 21/8358 (2011.01)
(52) CPC특허분류
G06F 21/84 (2013.01)
G06T 7/0002 (2013.01)
(21) 출원번호 10-2018-0020509
(22) 출원일자 2018년02월21일
심사청구일자 2018년02월21일
(56) 선행기술조사문헌
JP2006259930 A*
(뒷면에 계속)

(73) 특허권자
주식회사 테르텐
서울특별시 구로구 디지털로26길 61, 602호(구로동, 에이스하이엔드타워2차)
(72) 발명자
이영
서울시 동작구 상도로 346-2, 207동 1503호 (상도동, 상도엠코타운 애스톤파크)
황동혁
서울특별시 구로구 디지털로 288 (구로동) 삼성래미안 아파트
최성복
서울특별시 관악구 시흥대로158길 30, 401호 (신림동, 삼성하우스)
(74) 대리인
윤재석, 한지희

전체 청구항 수 : 총 10 항 심사관 : 구대성

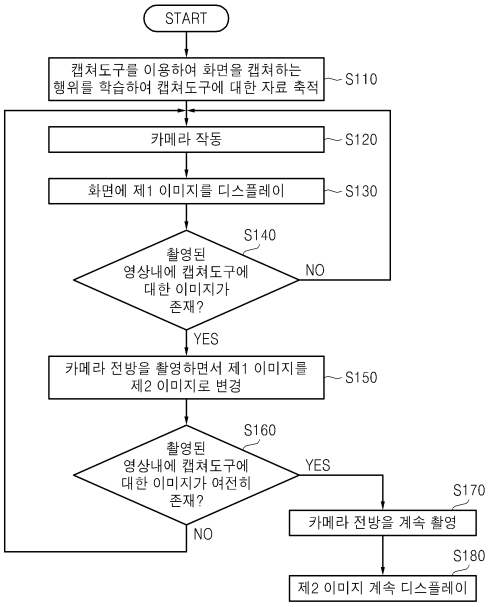
(54) 발명의 명칭 **디스플레이 장치에서 표시되는 정보의 유출을 방지하기 위한 컴퓨터 프로그램과 이를 이용한 보안 서비스 제공 방법**

(57) 요 약

하드웨어와 결합되어 컴퓨터의 디스플레이 장치에서 디스플레이되는 정보의 유출을 방지하기 위하여 저장 매체에 저장된 컴퓨터 프로그램은, 상기 컴퓨터에 연결된 카메라에 의해 획득된 제1 현재 영상을 수신하여 분석하고, 분석 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 캡쳐 카메라에 의해 진행되고 있는지를 판단하

(뒷면에 계속)

대 표 도 - 도3



고, 상기 디스플레이 장치의 상기 화면에 대한 촬영이 캡처 카메라에 의해 진행되고 있다고 판단될 때 상기 디스플레이 장치에서 디스플레이되는 제1 영상을 제2 영상으로 변경하고, 상기 카메라에 의해 획득된 제2 현재 영상을 수신하여 분석하고, 분석 결과에 기초하여 상기 디스플레이 장치의 상기 화면에 대한 촬영이 상기 캡처 카메라에 의해 계속 진행되고 있는지를 판단하고, 상기 디스플레이 장치의 상기 화면에 대한 촬영이 상기 캡처 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 디스플레이 장치에서 디스플레이되는 상기 제2 영상을 상기 제1 영상으로 복원하는 단계를 포함한다.

(52) CPC특허분류
H04N 21/8358 (2013.01)

(56) 선행기술조사문헌
KR1020160083500 A*
JP2012173913 A
JP2009237574 A
JP2014146167 A
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

하드웨어와 결합되어 컴퓨터의 디스플레이 장치에서 디스플레이되는 정보의 유출을 방지하기 위하여 저장 매체에 저장된 컴퓨터 프로그램에 있어서,

상기 컴퓨터 프로그램이 상기 컴퓨터에 연결된 카메라에 의해 획득된 영상을 분석하고, 상기 디스플레이 장치에서 디스플레이되는 정보를 상기 획득된 영상에 포함된 캡쳐 카메라를 이용하여 캡쳐하는 행위를 학습하고, 학습 결과에 따라 상기 캡쳐 카메라에 대한 영상을 스스로 학습하여 상기 컴퓨터의 메모리 장치에 저장하는 단계;

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제1 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 학습된 영상을 참조하여 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있는지를 판단하는 단계;

상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재함에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치에서 디스플레이되는 제1 영상을 제2 영상으로 변경하는 단계;

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제2 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 상기 학습된 영상을 참조하여 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있는지를 판단하는 단계; 및

상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하지 않음에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치에서 디스플레이되는 상기 제2 영상을 상기 제1 영상으로 복원하는 단계를 포함하는 컴퓨터 프로그램.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있다고 판단될 때, 상기 컴퓨터 프로그램이 상기 카메라로 하여금 상기 캡쳐 카메라에 해당하는 영상을 추적하면서 상기 카메라의 전방의 영상을 녹화하도록 상기 카메라를 제어하는 단계를 더 포함하는 컴퓨터 프로그램.

청구항 5

제4항에 있어서,

상기 컴퓨터 프로그램이 상기 녹화된 영상을 통신 네트워크를 통해 관리자 컴퓨터로 실시간으로 전송하는 단계를 더 포함하는 컴퓨터 프로그램.

청구항 6

제4항에 있어서,

상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 컴퓨터 프로그램이 상기 카메라에 의해 촬영된 영상의 녹화를 중지하는 단계를 더 포함하는 컴퓨터 프로그램.

청구항 7

제1항에 있어서,

상기 제1 영상을 상기 제2 영상으로 변경하는 단계는 상기 컴퓨터 프로그램이 상기 제2 영상을 상기 제1 영상의 위에 오버랩시킴으로써 상기 제1 영상을 상기 제2 영상으로 변경하고,

상기 제2 영상을 상기 제1 영상으로 복원하는 단계는 상기 컴퓨터 프로그램이 상기 제1 영상 위에 오버랩된 상기 제2 영상을 제거함에 따라 상기 제2 영상을 상기 제1 영상으로 복원하는 컴퓨터 프로그램.

청구항 8

제1항에 있어서,

상기 제1 영상을 상기 제2 영상으로 변경하는 단계는 상기 컴퓨터 프로그램이 상기 디스플레이 장치로 전송되는 상기 제1 영상에 관련된 영상 신호들을 차단함에 따라 상기 제1 영상을 상기 제 2 영상으로 변경하고,

상기 제2 영상을 상기 제1 영상으로 복원하는 단계는 상기 컴퓨터 프로그램이 상기 디스플레이 장치로의 전송이 차단된 상기 제1 영상에 관련된 영상 신호들을 다시 공급함에 따라 상기 제2 영상을 상기 제1 영상으로 복원하는 컴퓨터 프로그램.

청구항 9

하드웨어와 결합되어 컴퓨터의 디스플레이 장치에서 디스플레이되는 정보의 유출을 방지하기 위하여 저장 매체에 저장된 컴퓨터 프로그램에 있어서,

상기 컴퓨터 프로그램이 상기 컴퓨터에 연결된 카메라에 의해 획득된 영상을 분석하고, 상기 디스플레이 장치에서 디스플레이되는 정보를 상기 획득된 영상에 포함된 캡쳐 카메라를 이용하여 캡쳐하는 행위를 학습하고, 학습 결과에 따라 상기 캡쳐 카메라에 대한 영상을 스스로 학습하여 상기 컴퓨터의 메모리 장치에 저장하는 단계;

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제1 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 학습된 영상을 참조하여 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있는지를 판단하는 단계;

상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재함에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치에서 디스플레이되는 제1 영상을 제2 영상으로 변경하는 단계;

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제2 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 상기 학습된 영상을 참조하여 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있는지를 판단하는 단계; 및

상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하지 않음에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치에서 디스플레이되는 상기 제2 영상을 상기 제1 영상으로 복원하는 단계를 포함하고,

상기 제1 영상을 상기 제2 영상으로 변경하는 단계는 상기 컴퓨터 프로그램이 상기 제1 영상의 디스플레이에 관련된 컴퓨터 프로그램의 실행을 종료시킴에 따라 상기 제1 영상을 상기 제2 영상으로 변경하고,

상기 제2 영상을 상기 제1 영상으로 복원하는 단계는 상기 컴퓨터 프로그램이 종료된 상기 제1 영상의 디스플레이에 관련된 컴퓨터 프로그램을 다시 실행시킴에 따라 상기 제2 영상을 상기 제1 영상으로 복원하는 컴퓨터 프로그램.

청구항 10

제1항에 있어서,

상기 컴퓨터 프로그램이, 상기 제1 영상이 상기 제2 영상으로 변경된 후, 경고 메시지를 상기 디스플레이 장치에서 디스플레이하는 컴퓨터 프로그램.

청구항 11

컴퓨터, 상기 컴퓨터에서 실행되는 컴퓨터 프로그램, 및 상기 컴퓨터에 연결된 카메라를 이용하여 상기 컴퓨터의 디스플레이 장치의 화면에서 디스플레이되는 정보의 유출을 방지하는 서비스를 제공하는 방법에 있어서,

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 영상을 분석하고, 상기 디스플레이 장치의 화면에서 디스플레이되는 정보를 상기 획득된 영상에 포함된 캡쳐 카메라를 이용하여 캡쳐하는 행위를 학습하고, 학습 결과에 따라 상기 캡쳐 카메라에 대한 영상을 스스로 학습하여 상기 컴퓨터의 메모리 장치에 저장하는 단계;

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제1 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 학습된 영상을 참조하여 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있는지를 판단하는 단계;

상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재함에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치의 화면에서 디스플레이되는 제1 영상을 제2 영상으로 변경하고, 상기 카메라로 하여금 상기 캡쳐 카메라에 해당하는 영상을 추적하면서 상기 카메라의 전방의 영상을 녹화하도록 상기 카메라를 제어하는 단계;

상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제2 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 상기 학습된 영상을 참조하여 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있는지를 판단하는 단계; 및

상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하지 않음에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치의 화면에서 디스플레이되는 상기 제2 영상을 상기 제1 영상으로 복원하고 상기 카메라에 의해 촬영된 영상에 대한 녹화를 중지하는 단계를 포함하는 서비스를 제공하는 방법.

청구항 12

제11항에 있어서,

상기 제1 영상을 상기 제2 영상으로 변경은 상기 컴퓨터 프로그램이 상기 제1 영상의 디스플레이에 관련된 컴퓨터 프로그램의 실행을 종료시킴에 따라 상기 제1 영상을 상기 제2 영상으로 변경하고,

상기 제2 영상을 상기 제1 영상으로 복원은 상기 컴퓨터 프로그램이 종료된 상기 제1 영상의 디스플레이에 관련된 컴퓨터 프로그램을 다시 실행시킴에 따라 상기 제2 영상을 상기 제1 영상으로 복원하는 서비스를 제공하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 보안 컴퓨터 프로그램에 관한 것으로, 특히 디스플레이 장치에서 표시되고 보안이 요구되는 정보를 캡쳐 카메라를 이용하여 불법적으로 그리고 무단으로 유출하는 것을 방지할 수 있는 컴퓨터 프로그램과 이를 이용한 보안 서비스 제공 방법에 관한 것이다.

배 경 기 술

[0002] 캡쳐 방지 프로그램은 캡쳐 프로그램에 의한 캡쳐를 차단하는 기능을 갖고 있다. 어떤 캡쳐 방지 프로그램은 디스플레이 장치에서 디스플레이되는 보안이 요구되는 데이터를 보호하기 위해 워터마크를 삽입하는 기능을 가지

고 있다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 등록특허공보: 등록번호 10-1643936호 (2016.08.01 공고)

발명의 내용

해결하려는 과제

[0004] 본 발명이 이루고자 하는 기술적인 과제는, 컴퓨터의 디스플레이 장치에서 표시되는 보안이 요구되는 제1화면을 캡쳐 카메라를 이용하여 불법적으로 무단으로 캡쳐할 때 상기 제1화면에 대한 캡쳐를 차단하기 위해 상기 제1화면을 제2화면으로 변경할 수 있는 컴퓨터 프로그램과 상기 컴퓨터 프로그램을 이용한 보안 서비스를 제공하는 것이다.

[0005] 본 발명이 이루고자 하는 기술적인 과제는, 컴퓨터의 디스플레이 장치에서 표시되는 보안이 요구되는 정보를 캡쳐 카메라를 이용하여 불법적으로 그리고 무단으로 유출하려는 행위자의 행위(예컨대, 상기 캡쳐 카메라로 사진을 찍는 행위 또는 동영상을 녹화하는 행위)를 상기 컴퓨터에 연결된 카메라를 이용하여 검출하고, 검출 결과에 따라 상기 디스플레이에서 표시되는 상기 정보를 실시간으로 변경하는 동시에 상기 카메라를 이용하여 상기 행위자에 대한 증거 영상을 실시간으로 촬영할 수 있는 컴퓨터 프로그램과 상기 컴퓨터 프로그램을 이용한 보안 서비스를 제공하는 것이다.

과제의 해결 수단

[0006] 본 발명의 실시 예에 따른, 하드웨어와 결합되어 컴퓨터의 디스플레이 장치에서 디스플레이되는 정보의 유출을 방지하기 위하여 저장 매체에 저장된 컴퓨터 프로그램은, 상기 컴퓨터 프로그램이 상기 컴퓨터에 연결된 카메라에 의해 획득된 영상을 분석하고, 상기 디스플레이 장치에서 디스플레이되는 정보를 상기 획득된 영상에 포함된 캡쳐 카메라를 이용하여 캡쳐하는 행위를 학습하고, 학습 결과에 따라 상기 캡쳐 카메라에 대한 영상을 스스로 학습하여 상기 컴퓨터의 메모리 장치에 저장하는 단계와, 상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제1 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 학습된 영상을 참조하여 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있는지를 판단하는 단계와, 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재함에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치에서 디스플레이되는 제1 영상을 제2 영상으로 변경하는 단계와, 상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제2 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 상기 학습된 영상을 참조하여 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있는지를 판단하는 단계와, 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하지 않음에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치에서 디스플레이되는 상기 제2 영상을 상기 제1 영상으로 복원하는 단계를 포함한다.

[0007] 삭제

[0008] 삭제

[0009] 본 발명의 실시 예에 따라, 컴퓨터, 상기 컴퓨터에서 실행되는 컴퓨터 프로그램, 및 상기 컴퓨터에 연결된 카메라를 이용하여 상기 컴퓨터의 디스플레이 장치의 화면에서 디스플레이되는 정보의 유출을 방지하는 서비스를 제공하는 방법은 상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 영상을 분석하고, 상기 디스플레이 장치의

화면에서 디스플레이되는 정보를 상기 획득된 영상에 포함된 캡쳐 카메라를 이용하여 캡쳐하는 행위를 학습하고, 학습 결과에 따라 상기 캡쳐 카메라에 대한 영상을 스스로 학습하여 상기 컴퓨터의 메모리 장치에 저장하는 단계와, 상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제1 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 학습된 영상을 참조하여 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있는지를 판단하는 단계와, 상기 제1 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재함에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 진행되고 있다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치의 화면에서 디스플레이되는 제1 영상을 제2 영상으로 변경하고, 상기 카메라로 하여금 상기 캡쳐 카메라에 해당하는 영상을 추적하면서 상기 카메라의 전방의 영상을 녹화하도록 상기 카메라를 제어하는 단계와, 상기 컴퓨터 프로그램이 상기 카메라에 의해 획득된 제2 현재 영상을 수신하고, 상기 컴퓨터 프로그램에 의해 스스로 학습된 후 상기 메모리에 저장된 상기 캡쳐 카메라에 대한 상기 학습된 영상을 참조하여 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하는지를 판단하고, 판단 결과에 기초하여 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있는지를 판단하는 단계와, 상기 제2 현재 영상 내에 상기 캡쳐 카메라의 영상이 존재하지 않음에 따라 상기 디스플레이 장치의 화면에 대한 촬영이 상기 캡쳐 카메라에 의해 계속 진행되고 있지 않다고 판단될 때, 상기 컴퓨터 프로그램이 상기 디스플레이 장치의 화면에서 디스플레이되는 상기 제2 영상을 상기 제1 영상으로 복원하고 상기 카메라에 의해 촬영된 영상에 대한 녹화를 중지하는 단계를 포함한다.

발명의 효과

[0010] 본 발명의 실시 예에 따른 컴퓨터 프로그램은 컴퓨터의 디스플레이 장치에서 표시되는 보안이 요구되는 제1화면을 캡쳐 카메라를 이용하여 불법적으로 무단으로 캡쳐할 때 상기 제1화면에 대한 캡쳐를 차단하기 위해 상기 제1화면을 제2화면으로 변경할 수 있는 효과가 있다.

[0011] 본 발명의 실시 예에 따른 컴퓨터 프로그램은 컴퓨터의 디스플레이 장치에서 표시되는 보안이 요구되는 정보를 캡쳐 카메라를 이용하여 불법적으로 그리고 무단으로 유출하려는 행위자의 행위(예컨대, 상기 캡쳐 카메라로 사진을 찍는 행위 또는 동영상을 녹화하는 행위)를 상기 컴퓨터에 연결된 카메라를 이용하여 검출하고, 검출 결과에 따라 상기 디스플레이에서 표시되는 상기 정보를 실시간으로 변경하는 동시에 상기 카메라를 이용하여 상기 행위자의 상기 행위에 대한 증거 영상을 실시간으로 촬영할 수 있는 효과가 있다.

[0012] 본 발명의 실시 예에 따른 컴퓨터 프로그램을 이용한 정보 유출 방지 서비스는 디스플레이에서 표시되는 보안이 요구되는 정보를 유출하는 사람에 대한 영상을 실시간으로 촬영하고, 촬영된 영상을 관리자의 컴퓨터로 전송할 수 있으므로, 상기 관리자는 상기 정보를 유출하려는 사람에 대한 증거 자료를 용이하게 확보할 수 있는 효과가 있다.

도면의 간단한 설명

[0013] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 실시 예에 따른 컴퓨터 프로그램을 이용한 보안 서비스 제공 방법을 설명하는 보안 서비스 제공 시스템의 블록도이다.

도 2는 캡쳐 카메라를 이용하여 디스플레이 장치의 화면을 캡쳐할 때와 캡쳐 하지 않을 때 상기 디스플레이 장치의 화면에서 디스플레이되는 영상을 나타낸다.

도 3은 도 1에 도시된 보안 서비스 제공 시스템의 작동을 설명하는 플로우 차트이다.

도 4는 본 발명의 실시 예에 따른 컴퓨터 프로그램에 의해 학습된 캡쳐 도구와 상기 학습된 캡쳐 도구에 대한 이미지를 설명하기 위한 표이다.

발명을 실시하기 위한 구체적인 내용

[0014] 도 1은 본 발명의 실시 예에 따른 컴퓨터 프로그램을 이용한 보안 서비스 제공 방법을 설명하는 보안 서비스 제공 시스템의 블록도이다. 도 1을 참조하면, 보안이 요구되는 정보(또는 보안 데이터)의 유출을 방지하기 위한 서비스를 제공하는 보안 서비스 제공 시스템(또는 보안 데이터 유출 방지 시스템; 100)은 컴퓨터(200)와 카메라(210)를 포함하고, 통신 네트워크(260)를 통해 컴퓨터(200)와 신호들을 주고받는 관리자 단말기(270)를 포함한

다.

[0015] 컴퓨터(200)는 PC 또는 모바일 장치(mobile device 또는 portable device)를 의미하고, 카메라(210)는 PC 카메라, 웹캠(webcam), 또는 상기 모바일 장치의 카메라를 의미할 수 있다. 관리자 단말기(270)는 데이터베이스(280)에 저장된 또는 저장될 데이터를 관리(예컨대, 저장, 검색, 리드(read), 또는 업데이트)할 수 있는 장치 또는 관리 서버를 의미할 수 있다. 상기 모바일 장치는 스마트폰, 모바일 인터넷 장치(mobile internet device(MID)), 또는 사물 인터넷(Internet of Things(IoT)) 장치를 의미할 수 있다.

[0016] 컴퓨터(200)는 본 명세서에서 설명될 캡쳐 방지 프로그램(230)을 실행할 수 있는 CPU(220), CPU(220)에서 생성(또는 처리)된 정보(또는 데이터)를 수신하여 디스플레이할 수 있는 디스플레이 장치(또는 모니터; 235), 컴퓨터(200)에 필요한 컴퓨터 프로그램(캡쳐 방지 프로그램(230)을 포함함)을 저장하는 메모리 장치(240), 및 통신 네트워크(260)에 연결되는 인터페이스를 제공하는 통신 장치(모뎀 또는 송수신기; 250)를 포함할 수 있다.

[0017] 여기서 정보는 디지털 신호들 또는 데이터를 의미하고, 메모리 장치(240)는 하드디스크 드라이브(HDD) 또는 솔리드 스테이트 드라이브(SSD)와 같은 불휘발성 메모리 장치와, DRAM과 같은 휘발성 메모리 장치를 포함한다.

[0018] 도 2는 캡쳐 카메라를 이용하여 디스플레이 장치의 화면을 캡쳐할 때와 캡쳐 하지 않을 때 상기 디스플레이 장치의 화면에서 디스플레이되는 영상을 나타내고, 도 3은 도 1에 도시된 보안 서비스 제공 시스템의 작동을 설명하는 플로우 차트이고, 도 4는 본 발명의 실시 예에 따른 컴퓨터 프로그램에 의해 학습된 캡쳐 도구와 상기 학습된 캡쳐 도구에 대한 이미지를 설명하기 위한 표이다.

[0019] 도 1 내지 도 4를 참조하면, 하드웨어(예컨대, CPU(220)와 결합되어 컴퓨터 (200)의 디스플레이 장치(235)에서 디스플레이되는 보안이 요구되는 정보의 유출을 방지하기 위하여 저장 매체(예컨대, CPU(220) 또는 메모리 장치(240))에 저장된 컴퓨터 프로그램(예컨대, 캡쳐 방지 프로그램(230))은, 디스플레이 장치(235)에서 디스플레이되는 보안이 요구되는 정보(또는 디스플레이 장치(235)의 화면)를 다양한 캡쳐 도구들 각각을 이용하여 캡쳐(정지 영상으로 촬영 또는 동영상으로 촬영)하는 행위를 학습하고, 학습 결과에 따라 상기 다양한 캡쳐 도구들 각각에 대한 영상 자료를 축적하여 메모리 장치(240)에 저장할 수 있다(S110).

[0020] 다양한 캡쳐 도구들은 각각은 서로 다른 모양(또는 디자인)을 갖는 카메라들, 캠코더들 또는 스마트폰들을 의미할 수 있다. 예컨대, 카메라들, 캠코더들 또는 스마트폰들은 제조사에 따라 서로 다른 모양을 갖거나 모델에 따라 서로 다른 모양을 갖는다.

[0021] 캡쳐 방지 프로그램(230)은 다양한 캡쳐 도구들에 대한 영상들을 포함하거나, 캡쳐 방지 프로그램(230)이 메모리 장치(240)로 다운로드될 때 함께 다운로드된 다양한 캡쳐 도구들에 대한 영상들을 이용하거나, 다양한 캡쳐 도구들에 대한 영상들을 스스로 학습할 수 있다.

[0022] 예컨대, 관리자 단말기(270) 대신에 사용되는 관리자 서버(270)는 미리 학습된 다양한 캡쳐 도구들 각각에 대한 영상을 데이터베이스(280)로부터 리드하여 통신 네트워크(260)를 통해 컴퓨터(200)로 전송할 수 있다. 실시 예들에 따라 캡쳐 방지 프로그램(230)은 카메라(210)에 의해 획득(또는 촬영)된 영상을 분석하고, 상기 영상에 포함된 캡쳐 도구에 대한 영상(또는 모양)을 학습하고, 학습 결과를 메모리 장치(240)에 저장할 수 있다.

[0023] 캡쳐 방지 프로그램(230)은 컴퓨터(200)에 부착(또는 연결)된 카메라(210)를 작동시킨다(S120). 캡쳐 방지 프로그램(230)은 디스플레이 장치(235) 또는 디스플레이 장치(235)의 화면에 제1 영상을 디스플레이한다(S130).

[0024] 제1 영상은 보안이 요구되는 데이터(예컨대, 워드프로세서에 의해 작성된 문서 또는 파일), 정지 영상 또는 동영상 등으로서 디스플레이 장치(235)에서 시각적으로 디스플레이되는 모든 정보를 총칭하고, 시간이 지남에 따라 변하는 복수의 영상들을 포함한다.

[0025] 캡쳐 방지 프로그램(230)은 컴퓨터(200)에 연결되고 정상적으로 작동하는 카메라(210)에 의해 획득된 제1 현재 영상을 수신하여 분석하고, 분석 결과에 기초하여 디스플레이 장치(235)에서 디스플레이되는 제1 영상에 대한 촬영이 캡쳐 카메라 (51)에 의해 진행되고 있는지를 판단한다(S140).

[0026] 캡쳐 카메라(51)는 사용자(50)가 사용하는 카메라 또는 카메라를 포함하는 모바일 장치를 의미하고, 캡쳐 도구라고 불릴 수 있다.

[0027] 캡쳐 방지 프로그램(230)은 카메라(210)에 의해 촬영된 제1 현재 영상(예컨대, 제1 시점에서 촬영된 영상) 내에 캡쳐 카메라(51)에 대한 영상이 존재하는지를 판단한다(S140). 예컨대, 캡쳐 방지 프로그램(230)은 이미 학습된 영상을 참조하여 상기 제1 현재 영상 내에 캡쳐 카메라(51)의 영상이 존재하는지를 판단하고, 상기 제1 현재 영

상에 캡쳐 카메라(51)의 영상이 존재할 때 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)에서 디스플레이되는 제1 영상에 대한 촬영이 캡쳐 카메라 (51)에 의해 진행되고 있다고 판단한다.

[0028] 예컨대, 도 2에 도시된 바와 같이 사용자(50)가 캡쳐 카메라(예컨대, 스마트폰(51))로 디스플레이 장치(235)에서 디스플레이되고 있는 제1 영상을 촬영하고 있을 때, 캡쳐 방지 프로그램(230)은 에지 검출 알고리즘을 이용하여 제1 현재 영상으로부터 스마트폰(51)의 에지를 검출하고, 검출된 에지의 모양과 사전에 학습된 에지의 모양을 서로 비교하고, 검출된 에지의 모양과 사전에 학습된 에지의 모양이 동일 또는 유사할 때 제1 현재 영상 내에 스마트폰(51)에 해당하는 영상(또는 에지)이 존재한다고 판단한다.

[0029] 따라서 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)에서 디스플레이되는 제1 영상에 대한 촬영이 캡쳐 카메라(51)에 의해 진행되고 있다고 판단한다. 예컨대, 에지 검출 알고리즘은 제1 현재 영상에 포함된 윤곽선에 해당하는 픽셀들 각각의 밝기 값이 낮은 값으로부터 높은 값으로 변하거나 그 반대로 변하는 부분을 에지로서 검출하는 알고리즘으로서, 본 발명에서 제1 현재 영상 내에 캡쳐 카메라 (51)에 해당하는 영상이 존재하는지를 판단하는 알고리즘은 에지 검출 알고리즘에 한정되지 않는다.

[0030] 제1 현재 영상 내에 캡쳐 카메라(51)에 해당하는 영상이 존재하지 않을 때 (S140의 NO), 카메라(210)는 그 전방의 영상을 촬영하여 이를 CPU(220)로 전송하고 (S120), 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)의 화면에 제1 영상을 디스플레이한다(S130).

[0031] 제1 현재 영상 내에 캡쳐 카메라(51)에 해당하는 영상이 존재할 때(S140의 YES), 카메라(210)는 그 전방의 영상을 촬영하고, 촬영된 영상을 CPU(220)로 전송하고, 캡쳐 방지 프로그램(230)은 수신된 영상을 녹화하면서 디스플레이 장치(235)의 화면에서 디스플레이되는 제1 영상(IM1)을 제2 영상(IM2)으로 변경한다(S150).

[0032] 제2 영상(IM2)은 제1 영상(IM1)의 유출을 방지하기 위해 제1 영상(IM1)을 보이지 않게 하는 데이터, 정지 영상 또는 동영상 등으로서 디스플레이 장치(235)에서 시각적으로 디스플레이되는 모든 정보를 총칭하고, 시간이 지남에 따라 변하는 복수의 영상들을 포함한다.

[0033] 실시 예들에 따라, 캡쳐 방지 프로그램(230)은, 제1 영상(IM1)이 제2 영상 (IM2)으로 변경된 후, 시각적 경고 메시지를 디스플레이 장치(235)에 디스플레이하거나 스피커를 이용하여 청각적 메시지를 출력할 수 있다.

[0034] 따라서, 보안이 요구되는 제1 영상(IM1)은 불법적인 무단 유출을 차단하기 위해 제2 영상(IM2)으로 변경된다. 카메라(210)에 의해 실시간으로 촬영되는 영상은 디스플레이 장치(235)에서 표시되는 제1 영상(IM1) 또는 제2 영상(IM2)을 캡쳐 카메라(51)를 이용하여 촬영하는 사용자(50)에 대한 영상을 포함하고, 캡쳐 방지 프로그램(230)은 카메라(210)에 의해 촬영된 영상을 메모리 장치(240)에 저장하거나 통신 장치(250)와 통신 네트워크(260)를 통해 관리자 컴퓨터(또는 관리 서버; 270)로 실시간으로 전송할 수 있다.

[0035] 제1 현재 영상 내에 캡쳐 카메라(51)에 대한 영상이 존재할 때(S140의 YES), 캡쳐 방지 프로그램(230)은 카메라(210)로 하여금 캡쳐 카메라(51)에 대한 영상(또는 캡쳐 카메라(51)의 에지)을 추적하면서 카메라(210)의 전방의 영상을 녹화하도록 카메라(210)를 제어한다. 캡쳐 방지 프로그램(230)은 영상(또는 움직임) 추적 알고리즘을 이용하여 캡쳐 카메라(51)를 추적할 수 있다.

[0036] 실시 예들에 따라 캡쳐 방지 프로그램(230)은 제2 영상(IM2)을 제1 영상 (IM1)의 위에 오버랩시킴으로써 제1 영상(IM1)을 제2 영상(IM2)으로 변경할 수 있다. 제2 영상(IM2)에 의해 제1 영상(IM1)은 사용자(50) 또는 캡쳐 카메라(51)에 의해 인식될 수 없다.

[0037] 실시 예들에 따라 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)로 전송되는 제1 영상(IM1)에 관련된 영상 신호들을 차단함에 따라 제1 영상(IM1)을 제2 영상(IM2)으로 변경할 수 있다.

[0038] 실시 예들에 따라 캡쳐 방지 프로그램(230)은 제1 영상(IM1)의 디스플레이에 관련된 컴퓨터 프로그램(예컨대, 워드프로세서 프로그램)의 실행을 종료시킴에 따라 제1 영상(IM1)을 제2 영상(IM2)으로 변경할 수 있다.

[0039] 캡쳐 방지 프로그램(230)은 카메라(210)에 의해 획득된 제2 현재 영상(예컨대, 제1 시점보다 늦은 제2 시점에서 촬영된 영상)을 수신하여 분석하고, 분석 결과에 기초하여 디스플레이 장치(235)에 대한 촬영(또는 제2 영상(IM2)에 대한 촬영)이 캡쳐 카메라(51)에 의해 계속 진행되고 있는지를 판단한다(S160).

[0040] 캡쳐 방지 프로그램(230)은 이미 학습된 영상을 참조하여 제2 현재 영상 내에 캡쳐 카메라(51)에 해당하는 영상이 존재하는지를 판단하고, 상기 제2 현재 영상 내에 캡쳐 카메라(51)에 해당하는 영상이 존재하지 않을 때 (S160의 NO), 디스플레이 장치(235)에 대한 촬영이 캡쳐 카메라(51)에 의해 계속 진행되고 있지 않다고 판단한

다.

[0041] 디스플레이 장치(235)에 대한 촬영이 캡쳐 카메라(51)에 의해 계속 진행되고 있지 않다고 판단될 때(S160의 NO), 캡쳐 방지 프로그램(230)은 디스플레이 장치 (235)에서 디스플레이되는 제2 영상(IM2)을 제1 영상(IM1)으로 복원(또는 복구)한다.

[0042] 이때, 캡쳐 방지 프로그램(230)은 카메라(210)에 의해 촬영된 제3 현재 영상(예컨대, 제2시점보다 늦은 제3 시점에 촬영된 영상)에 대한 녹화를 중지한다.

[0043] 실시 예들에 따라 캡쳐 방지 프로그램(230)은 제1 영상(IM1) 위에 오버랩된 제2 영상(IM2)을 제거하여 제2 영상(IM2)을 제1 영상(IM1)으로 변경할 수 있다. 제2 영상(IM2)이 제거됨에 따라 제1 영상(IM1)은 사용자(50)에게 보인다.

[0044] 실시 예들에 따라 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)로 제1 영상(IM1)에 관련된 영상 신호들을 다시 전송함에 따라 제2 영상(IM2)을 제1 영상 (IM1)으로 변경할 수 있다.

[0045] 실시 예들에 따라 캡쳐 방지 프로그램(230)은 제1 영상(IM1)의 디스플레이에 관련된 컴퓨터 프로그램(예컨대, 워드프로세서 프로그램)을 다시 실행시켜 제2 영상(IM2)을 제1 영상(IM1)으로 변경할 수 있다.

[0046] 상기 제2 현재 영상 내에 캡쳐 카메라(51)에 해당하는 영상이 계속 존재할 때(S160의 YES), 캡쳐 방지 프로그램(230)은 카메라(210)에 의해 촬영되는 영상을 메모리 장치(240)에 저장하거나 통신 장치(250)와 통신 네트워크(260)를 통해 관리자 컴퓨터(또는 관리 서버; 270)로 실시간으로 전송할 수 있다(S170). 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)에 제2 영상(IM2)을 계속 디스플레이한다 (S180).

[0047] 사용자(50)가 캡쳐 카메라(51)를 이용하여 디스플레이 장치(235)의 화면을 촬영할 때 또는 캡쳐 방지 프로그램(230)이 디스플레이 장치(235)에서 디스플레이되는 제1 영상(IM1)이 캡쳐 카메라(51)에 의해 촬영되고 있다고 판단할 때, 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)에서 디스플레이되는 보안이 요구되는 제1 영상(IM1)을 제2 영상(IM2)으로 변경하고, 카메라(210)에 의해 촬영된 영상들을 녹화한다.

[0048] 그 후 사용자(50)가 캡쳐 카메라(51)를 치웠을 때 또는 캡쳐 방지 프로그램 (230)이 디스플레이 장치(235)에서 디스플레이되는 제2 영상(IM2)이 캡쳐 카메라 (51)에 의해 촬영되고 있지 않다고 판단할 때, 캡쳐 방지 프로그램(230)은 디스플레이 장치(235)에서 디스플레이되는 제2 영상(IM2)을 제1 영상(IM1)으로 변경하고, 카메라(210)에 의해 촬영된 영상들을 녹화하지 않는다.

[0049] 즉, 디스플레이 장치(235)의 화면이 캡쳐 카메라(51)에 의해 촬영되는 동안에만, 제2 영상(IM2)이 디스플레이 장치(235)에서 디스플레이되고, 카메라(210)의 전방에 대한 영상들이 녹화된다.

[0050] 도 1과 도 4를 참조하면, 캡쳐 방지 프로그램(230)은 각 캡쳐 도구(SM1~SMn, n은 자연수)에 대한 각 이미지(CIM1~CIMn)를 참조하여 사용자(50)의 캡쳐 카메라 (51)에 해당하는 이미지가 해당 캡쳐 도구의 이미지와 동일 또는 유사한지를 판단할 수 있다.

[0051] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0052] 100: 보안 서비스 제공 시스템

200: 컴퓨터

220: CPU

230: 캡쳐 방지 프로그램

235: 모니터 또는 디스플레이 장치

240: 메모리 장치

250: 통신 장치

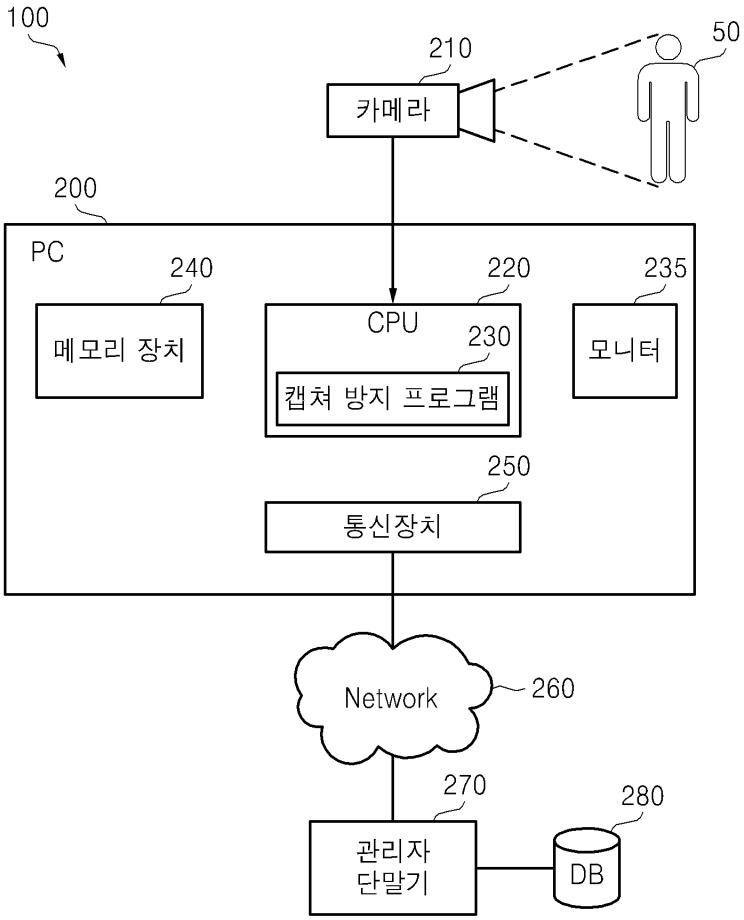
260: 통신 네트워크

270: 관리자 단말기 또는 관리 서버

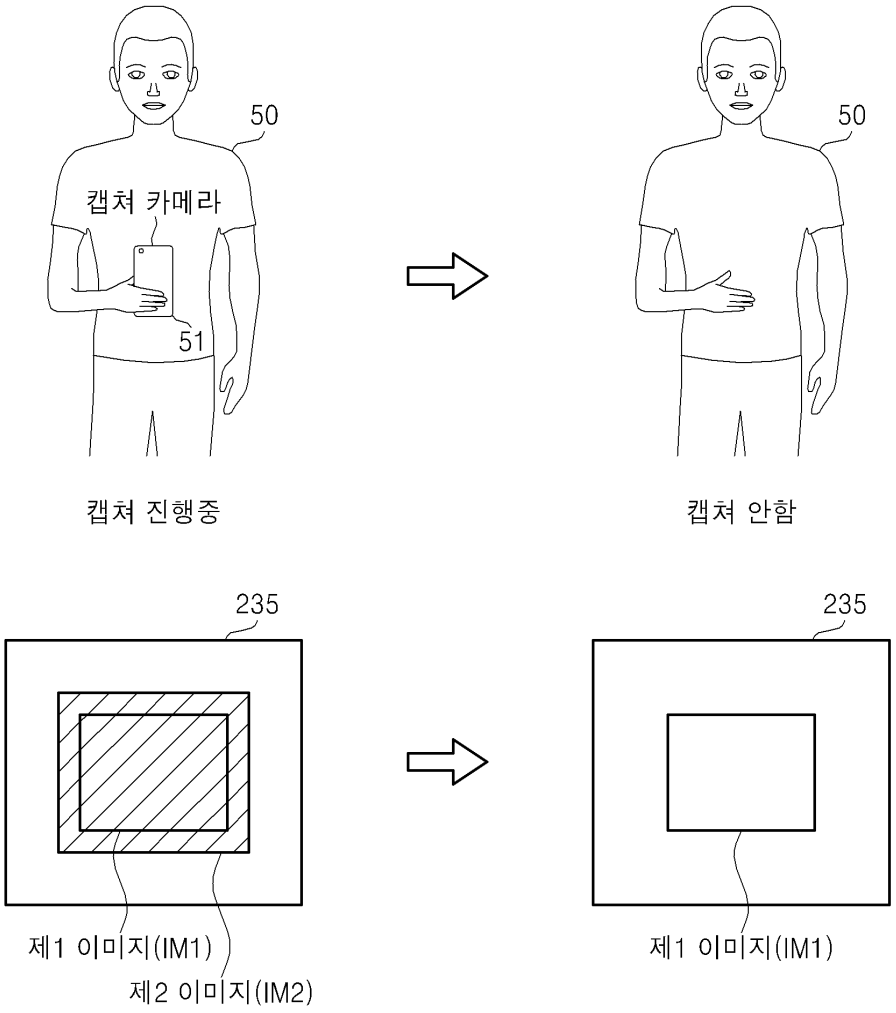
280: 데이터베이스

도면

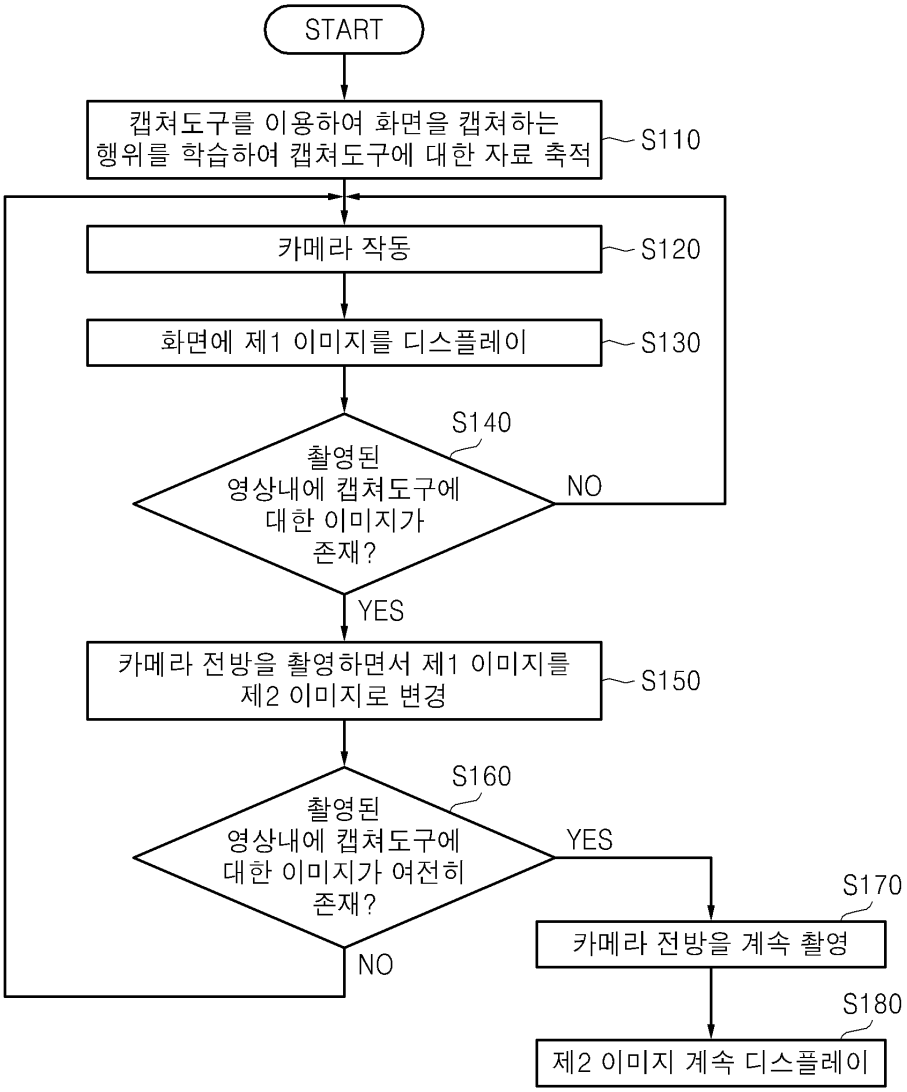
도면1



도면2


50
캡쳐 카메라
51
캡쳐 진행중
50
캡쳐 안함
235
제1 이미지(IM1)
제2 이미지(IM2)
235
제1 이미지(IM1)

도면3



도면4

230A

캡쳐도구	캡쳐도구 이미지
SM1	CIM1
SM2	CIM2
⋮	⋮
SMn	CIMn