(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0000172
(43) 공개일자 2022년01월03일

(51) 국제특허분류(Int. Cl.)
G06N 3/04 (2006.01) *G06N 3/08* (2006.01)
G06T 7/20 (2017.01) *G08B 13/196* (2006.01)
H04N 7/18 (2006.01)
(52) CPC특허분류
G06N 3/0454 (2013.01)
G06N 3/084 (2013.01)
(21) 출원번호 10-2020-0077811
(22) 출원일자 2020년06월25일
심사청구일자 2020년10월06일

(71) 출원인
주식회사 자비스넷
서울특별시 금천구 디지털로9길 46, 1201, 1202, 1203, 1204, 1205호 (가산동, 이앤씨드림타워7차)
(72) 발명자
박주영
경기도 시흥시 계수로 19 시흥은계우미린레이크 304-601
이동식
서울특별시 양천구 목동서로 100 목동신시가지아파트3단지 321-404
이원경
서울특별시 양천구 목동동로 411 부영그린타운3차 D동 1612호
(74) 대리인
특허법인폴라리스

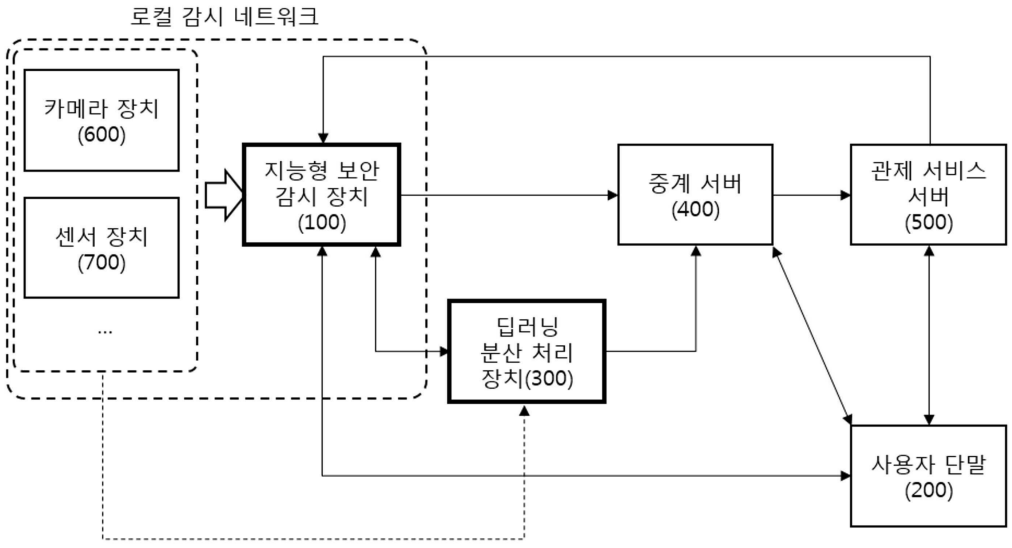
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **엣지 컴퓨팅 기반 보안 감시 서비스 제공 장치, 시스템 및 그 동작 방법**

(57) 요 약

본 발명의 실시 예에 따른 방법은, 지능형 보안 감시 장치의 동작 방법에 있어서, 보안 감시를 위한 영상 정보를 수집하는 단계; 상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 단계; 상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하는 단계; 및 상기 딥러닝 분산 처리 요청 데이터를 하나 이상의 딥러닝 분산 처리 장치로 전송하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06T 7/20 (2013.01)
G08B 13/19608 (2013.01)
H04N 7/18 (2013.01)
G06T 2207/20084 (2013.01)

명 세 서

청구범위

청구항 1

지능형 보안 감시 장치의 동작 방법에 있어서,

보안 감시를 위한 영상 정보를 수집하는 단계;

상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 단계;

상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하는 단계; 및

상기 딥러닝 분산 처리 요청 데이터를 하나 이상의 딥러닝 분산 처리 장치로 전송하는 단계를 포함하는

지능형 보안 감시 장치의 동작 방법.

청구항 2

제1항에 있어서,

상기 하나 이상의 딥러닝 분산 처리 장치로부터 상기 딥러닝 분산 처리 요청 데이터에 따라, 상기 추적 데이터 및 상기 영상 정보의 딥러닝 분석에 따른 객체 검출 정보 및 객체 분류 정보를 수신하는 단계; 및

상기 객체 검출 정보 및 상기 객체 분류 정보와, 상기 추적 데이터에 기초하여 상기 영상 정보에 대응하는 감시 이벤트를 검출하는 단계를 포함하는

지능형 보안 감시 장치의 동작 방법.

청구항 3

제1항에 있어서,

상기 초기 분석 처리는,

영상 안정화 처리, 배경 모델링 처리, 형태 연산 처리, 요소 연결 처리 및 객체 추적 처리 중 적어도 하나를 포함하는

지능형 보안 감시 장치의 동작 방법.

청구항 4

제1항에 있어서,

상기 딥러닝 분산 처리 장치는 상기 딥러닝 분산 처리 요청 데이터를 이용한 딥러닝 기반 객체 검출 및 분류 분석을 수행하는 엣지 컴퓨팅 장치인

지능형 보안 감시 장치의 동작 방법.

청구항 5

제4항에 있어서,

상기 딥러닝 분산 처리 장치는 상기 객체 검출 및 분류 분석 결과를 포함하는 딥러닝 영상 분석 정보를 중계 서버로 전송하는 장치이며,

상기 중계 서버는 상기 보안 감시 장치의 이벤트 검출 데이터가 수신된 경우, 상기 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 색인하여 상기 보안 감시 장치에 대응하여 사전 등록된 사용자 단말로 상기 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 전송하는 서버인

지능형 보안 감시 장치의 동작 방법.

청구항 6

제1항에 있어서,

상기 딥러닝 분산 처리 장치는 딥 러닝 기반의 신경 회로망을 이용하여 상기 딥러닝 분산 처리 요청 데이터에 대응하는 객체 분류 정보를 획득하며, 상기 객체 분류 정보를 상기 지능형 보안 감시 장치로 전송하는 장치로서, 딥 러닝 기반의 신경 회로망 구축을 위해 학습 영상 정보로부터 획득되는 하나 이상의 정상 이미지를 분석하여 감시 대상 객체를 식별하고, 감시 대상 객체가 식별된 정상 이미지를 저장하며, 상기 학습 영상 정보로부터 획득되는 하나 이상의 특정 이미지에서 감시 대상 객체를 식별하는 과정에서 상기 감시 대상 객체가 아닌 특정 객체가 식별된 경우 상기 특정 이미지와 하나 이상의 상기 정상 이미지 사이의 유사도를 산출하며, 상기 유사도가 미리 설정된 기준치 이상인 경우, 상기 특정 이미지에 대하여 상기 신경 회로망을 기반으로 영상 처리된 출력값 과 객체 정보 사이의 오차에 대한 오차 정보를 생성하고, 미리 설정된 역전파 알고리즘(back propagation algorithm)을 통해 상기 오차 정보를 기반으로 상기 신경 회로망을 구성하는 파라미터를 조정하는 장치인

지능형 보안 감시 장치의 동작 방법.

청구항 7

제6항에 있어서,

상기 딥러닝 분산 처리 장치는 상기 오차 정보를 기초로 상기 역전파 알고리즘을 통해 상기 신경 회로망을 구성하는 입력층, 하나 이상의 은닉층 및 출력층 사이의 연결 강도에 대한 가중치(weight) 또는 상기 입력층, 은닉층 및 출력층에 구성된 유닛의 바이어스(bias)를 가변하여 상기 감시 대상 객체에 대한 식별 오류가 최소화되도록 학습하는 장치인

지능형 보안 감시 장치의 동작 방법.

청구항 8

제1항에 있어서,

상기 딥러닝 분산 처리 요청 데이터에 따른 상기 딥러닝 분산 처리 장치의 분석 결과 정보는 상기 지능형 보안 감시 장치에서 제공하는 객체 분류, 동적 객체 추적, 트립 와이어, 침입 감지, 배회객체 감지, 통행방향 위반 감지, 무단 방치물 감지, 무단 이동물체 감지, 출입 카운팅 및 통계, 군중 밀집상태 감지, 특이행동 감지, 카메라 무단 변경 감지 중 적어도 하나의 이벤트 감지 처리에 이용되는

지능형 보안 감시 장치의 동작 방법.

청구항 9

지능형 보안 감시 장치에 있어서,

보안 감시를 위한 영상 정보를 수집하는 영상 정보 수집부;

상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 객체 추적부; 및

상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하고, 상기 딥러닝 분산 처리 요청 데이터를 딥러닝 분산 처리 장치로 전송하는 분산 데이터 처리부를 포함하는

지능형 보안 감시 장치.

청구항 10

제9항에 있어서,

상기 분산 데이터 처리부는, 상기 딥러닝 분산 처리 장치로부터 상기 딥러닝 분산 처리 요청 데이터에 따라, 상기 추적 데이터 및 상기 영상 정보의 딥러닝 분석에 따른 객체 검출 정보 및 객체 분류 정보를 수신하고,

상기 객체 검출 정보 및 상기 객체 분류 정보와, 상기 추적 데이터에 기초하여 상기 영상 정보에 대응하는 감시 이벤트를 검출하는 이벤트 검출부를 더 포함하는

지능형 보안 감시 장치.

청구항 11

제9항에 있어서,

상기 초기 분석 처리는,

영상 안정화 처리, 배경 모델링 처리, 형태 연산 처리, 요소 연결 처리 및 객체 추적 처리 중 적어도 하나를 포함하는

지능형 보안 감시 장치.

청구항 12

제9항에 있어서,

상기 딥러닝 분산 처리 장치는 상기 딥러닝 분산 처리 요청 데이터를 이용한 딥러닝 기반 객체 검출 및 분류 분석을 수행하는 엣지 컴퓨팅 장치인

지능형 보안 감시 장치.

청구항 13

제12항에 있어서,

상기 딥러닝 분산 처리 장치는 상기 객체 검출 및 분류 분석 결과를 포함하는 딥러닝 영상 분석 정보를 중계 서버로 전송하는 장치이며,

상기 중계 서버는 상기 보안 감시 장치의 이벤트 검출 데이터가 수신된 경우, 상기 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 색인하여 상기 보안 감시 장치에 대응하여 사전 등록된 사용자 단말로 상기 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 전송하는 서버인

지능형 보안 감시 장치.

청구항 14

제9항에 있어서,

상기 딥러닝 분산 처리 요청 데이터에 따른 상기 딥러닝 분산 처리 장치의 분석 결과 정보는 상기 지능형 보안 감시 장치에서 제공하는 객체 분류, 동적 객체 추적, 트립 와이어, 침입 감지, 배회객체 감지, 통행방향 위반 감지, 무단 방치물 감지, 무단 이동물체 감지, 출입 카운팅 및 통계, 군중 밀집상태 감지, 특이행동 감지, 카메라 무단 변경 감지 중 적어도 하나의 이벤트 감지 처리에 이용되는

지능형 보안 감시 장치.

청구항 15

지능형 카메라 장치에 있어서,

실시간 영상을 촬영하여 획득하는 카메라부;

상기 카메라부로부터 수신되는 실시간 영상을 보안 감시를 위한 영상 정보로 안정화 처리하는 영상 정보 안정화부;

상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 객체 추적부; 및

상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하고, 상기 딥러닝 분산 처리 요청 데이터를 하나 이상의 딥러닝 분산 처리 장치로 전송하는 분산 데이터 처리부를 포함하는

지능형 카메라 장치.

청구항 16

제15항에 있어서,

상기 하나 이상의 딥러닝 분산 처리 장치는, 딥러닝 기반 영상 정보 분석부를 포함하며, 상기 지능형 카메라 장치와 분산 네트워크로 연결된 다른 지능형 카메라 장치를 포함하는

지능형 카메라 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 서비스 제공 시스템 및 그 동작 방법에 관한 것이다. 보다 구체적으로, 본 발명은 엣지(EDGE) 컴퓨팅을 기반으로 하는 보안 서비스를 제공하여 감시 성능 및 시스템 효율을 향상시키는 보안 감시 서비스 제공 장치, 시스템 및 그 동작 방법에 관한 것이다.

배 경 기 술

[0002] 현재 통신 및 영상분석 기술의 발전과 더불어 감시 대상 지역에 대한 보안을 위해 원격지에 위치하는 카메라로부터 수신된 영상에 대한 영상 분석 및 객체 식별을 통해 감시 대상 지역에 대한 보안을 제공하는 다양한 보안 시스템이 제공되고 있으며, 이를 통해 감시 대상 지역의 객체 감지시 관리자에게 위험 여부를 알리고 객체 감지에 따른 영상을 기록하는 등의 다양한 서비스를 제공하여 감시 대상 지역의 관리에 대한 편의성을 높이고 있다.

[0003] 일반적으로 보안 감시 시스템은 감시 대상 지역에 위치하는 센서를 통해 감시 대상 지역에 위치하는 감시 대상을 감지하고, 감시 대상의 감지시 해당 감시 대상의 감지와 연동하여 카메라를 통해 감시 대상을 촬영하여 생성한 영상을 제공함으로써, 센서를 통해 감지된 감시 대상을 영상을 통해 확인할 수 있도록 제공한다.

[0004] 그러나, 기존의 보안 감시 시스템의 감시 대상에 대한 센서의 감지에 따른 침입 신호 발생시 영상을 통한 확인과 별도로 관리자에게 무조건 알람이 제공되도록 동작하고 있으며, 이로 인해 감시 대상이 아닌 객체에 대해서도 알람이 제공되어 오보가 지속적으로 발생하는 문제가 있다.

[0005] 이를 방지하기 위해, 최근 보안 감시 시스템은 센서의 감지와 더불어 센서를 통해 침입 신호 발생시 카메라를 통해 촬영된 영상에서 감시 대상에 대응되는 감시 대상 객체가 식별되는 경우에 관리자에게 알람이 제공되도록 동작하도록 설정되어 보안 시스템의 오보를 최소화하고자 한다.

[0006] 그러나, 감시 대상 지역은 일반적으로 저조도의 환경이 많으며, 이로 인해 최근의 보안 시스템 역시 센서의 감시 대상 감지시 저조도 환경에서 운용되는 카메라를 통해 생성된 영상에서 객체가 뚜렷하게 나타나지 않아 감시 대상 객체가 아닌 객체에 대해서도 알람을 제공하거나 감시 대상 객체가 출현한 경우에도 감시 대상 객체가 영상을 통해 식별되지 않아 보고가 누락되는 경우가 빈번히 발생하여 오보율을 크게 개선하지 못하는 문제가 있다.

[0007] 상술한 문제점으로 인해, 보안 감시 시스템의 감시 대상 지역에 대한 침입 감지 보고에 따른 신뢰성 및 정확도가 저하되는 문제가 발생하고 있으며, 이를 해결하기위해 딥러닝 분석 기반의 영상분석 방법이 제안되고 있다.

[0008] 하지만, 딥러닝 분석 처리에는 많은 컴퓨팅 자원이 소모되기 때문에 딥러닝 분석 장치나 서버가 별도의 원격지에 외부 네트워크로 연결되어 위치한 경우가 많다. 이에 따라 영상 정보가 딥러닝 분석 서버를 통해 분석이 완료된 이후에서나 객체 분류 및 정확한 이벤트 검출이 가능하게 되므로, 컴퓨팅 비용뿐만 아니라 보안 감시 시스템에서 가장 중요한 시간 자원이 소모되게 되는 문제점이 있다.

[0009] 이는 결과적으로 현장에 설치된 감시 장비 동작을 지연시키며, 현실적으로는 딥러닝 분석이 완료되기 이전 시점에 단순 센서 기반으로 긴급한 알람 기능만을 먼저 처리해야 하므로, 여전히 오보율이 그대로인 문제점이 있다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기한 바와 같은 문제점들을 해결하고자 안출된 것으로, 현장에 설치되는 보안 감시 장치를 지능형 보안 감시 장치로 구성하여 인공지능 기반의 로컬 영상감시 시스템을 구축하되, 딥러닝 분석이 필요한 추적 데이터는 분산 데이터로 가공하여 엣지 컴퓨팅 기반의 딥러닝 분산 처리 장치로 분석 요청 및 처리하게 함으로써, 시스템 지연의 최소화 및 정확한 이벤트 검출에 따른 오보율을 최소화할 수 있는 엣지 컴퓨팅 기반 보안 감시 서비스 제공 장치, 시스템 및 그 동작 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0011] 상기한 바와 같은 과제를 해결하기 위한 본 발명의 실시 예에 따른 방법은, 지능형 보안 감시 장치의 동작 방법에 있어서, 보안 감시를 위한 영상 정보를 수집하는 단계; 상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 단계; 상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하는 단계; 및 상기 딥러닝 분산 처리 요청 데이터를 딥러닝 분산 처리 장치로 전송하는 단계를 포함한다.

[0012] 또한, 상기한 바와 같은 과제를 해결하기 위한 본 발명의 실시 예에 따른 장치는, 지능형 보안 감시 장치에 있어서, 보안 감시를 위한 영상 정보를 수집하는 영상 정보 수집부; 상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 객체 추적부; 및 상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하고, 상기 딥러닝 분산 처리 요청 데이터를 딥러닝 분산 처리 장치로 전송하는 분산 데이터 처리부를 포함한다.

[0013] 또한, 상기한 바와 같은 과제를 해결하기 위한 본 발명의 실시 예에 따른 장치는, 지능형 카메라 장치에 있어서, 실시간 영상을 촬영하여 획득하는 카메라부; 상기 카메라부로부터 수신되는 실시간 영상을 보안 감시를 위한 영상 정보로 안정화 처리하는 영상 정보 안정화부; 상기 영상 정보에 대한 초기 분석 처리에 따라, 상기 영상 정보의 객체를 추적하기 위한 추적 데이터를 획득하는 객체 추적부; 및 상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하고, 상기 딥러닝 분산 처리 요청 데이터를 하나 이상의 딥러닝 분산 처리 장치로 전송하는 분산 데이터 처리부를 포함한다.

[0014] 한편, 상기한 바와 같은 과제를 해결하기 위한 본 발명의 실시 예에 따른 방법은 상기 방법을 컴퓨터에서 실행시키기 위한 프로그램 및 상기 프로그램이 기록된 기록 매체로 구현될 수 있다.

발명의 효과

[0015] 본 발명의 실시 예에 따르면, 현장에 설치되는 보안 감시 장치를 지능형 보안 감시 장치로 구성하여 1차적인 인공지능 기반의 영상감시 시스템을 구축하되, 딥러닝 분석이 필요한 감시 데이터만 분산 데이터로 가공하여 엣지 컴퓨팅 기반의 딥러닝 분산 처리 장치로 분석 요청 및 처리하게 함으로써, 시스템 지연의 최소화 및 정확한 이벤트 검출에 따른 오보율을 최소화할 수 있는 엣지 컴퓨팅 기반 보안 감시 서비스 제공 장치, 시스템 및 그 동작 방법을 제공할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 실시 예에 따른 전체 시스템을 개략적으로 도시한 개념도이다.

도 2는 본 발명의 실시 예에 따른 지능형 감시 장치 및 딥러닝 분산 서버의 구성 및 연결관계를 보다 구체적으로 도시한 블록도이다.

도 3은 본 발명의 실시 예에 따른 이벤트 검출부의 검출 모듈을 설명하기 위한 블록도이다.

도 4는 본 발명의 실시 예에 따른 전체 시스템 동작을 설명하기 위한 래더 다이어그램이다.

도 5는 본 발명의 다른 일 실시 예에 따른 지능형 카메라 장치 기반 시스템을 설명하기 위한 개념도이다.

도 6은 본 발명의 실시 예에 따른 지능형 카메라 장치로 구현된 딥러닝 분석 시스템의 구성 및 연결관계를 보다 구체적으로 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하의 내용은 단지 본 발명의 원리를 예시한다. 그러므로 당업자는 비록 본 명세서에 명확히 설명되거나 도시되지 않았지만 본 발명의 원리를 구현하고 본 발명의 개념과 범위에 포함된 다양한 장치를 발명할 수 있는 것이

다. 또한, 본 명세서에 열거된 모든 조건부 용어 및 실시예들은 원칙적으로, 본 발명의 개념이 이해되도록 하기 위한 목적으로만 명백히 의도되고, 이와 같이 특별히 열거된 실시예들 및 상태들에 제한적이지 않는 것으로 이해되어야 한다.

[0018] 또한, 본 발명의 원리, 관점 및 실시예들 뿐만 아니라 특정 실시예를 열거하는 모든 상세한 설명은 이러한 사항의 구조적 및 기능적 균등물을 포함하도록 의도되는 것으로 이해되어야 한다. 또한 이러한 균등물들은 현재 공지된 균등물뿐만 아니라 장래에 개발될 균등물 즉 구조와 무관하게 동일한 기능을 수행하도록 발명된 모든 소자를 포함하는 것으로 이해되어야 한다.

[0019] 따라서, 예를 들어, 본 명세서의 블록도는 본 발명의 원리를 구체화하는 예시적인 회로의 개념적인 관점을 나타내는 것으로 이해되어야 한다. 이와 유사하게, 모든 흐름도, 상태 변환도, 의사 코드 등은 컴퓨터가 판독 가능한 매체에 실질적으로 나타낼 수 있고 컴퓨터 또는 프로세서가 명백히 도시되었는지 여부를 불문하고 컴퓨터 또는 프로세서에 의해 수행되는 다양한 프로세스를 나타내는 것으로 이해되어야 한다.

[0020] 또한 프로세서, 제어 또는 이와 유사한 개념으로 제시되는 용어의 명확한 사용은 소프트웨어를 실행할 능력을 가진 하드웨어를 배타적으로 인용하여 해석되어서는 아니되고, 제한 없이 디지털 신호 프로세서(DSP) 하드웨어, 소프트웨어를 저장하기 위한 롬(ROM), 램(RAM) 및 비 휘발성 메모리를 암시적으로 포함하는 것으로 이해되어야 한다. 주지관용의 다른 하드웨어도 포함될 수 있다.

[0021] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다.

[0022] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명하기로 한다.

[0024] 도 1은 본 발명의 실시 예에 따른 전체 시스템을 개략적으로 도시한 개념도이다.

[0025] 도 1을 참조하면, 본 발명의 실시 예에 따른 전체 시스템은, 지능형 보안 감시 장치(100), 사용자 단말(200), 딥러닝 분산 처리 장치(300), 중계 서버(400), 관제 서비스 서버(500), 하나 이상의 카메라 장치(600) 및 하나 이상의 센서 장치(700)를 포함한다.

[0026] 카메라 장치(600) 및 센서 장치(700)는, 보안 감시 지역에 배치될 수 있으며, 지능형 보안 감시 장치(100)와 로컬 감시 네트워크로 연결될 수 있다. 카메라 장치(600) 및 센서 장치(700)는 각각 보안 감시 지역을 촬영하거나, 보안 감시 지역 또는 그 주변에서 발생되는 감지 신호를 센싱하여, 영상 정보 및 센서 정보를 획득하고, 획득된 영상 정보 및 센서 정보를 지능형 보안 감시 장치(100)로 전송한다.

[0027] 지능형 보안 감시 장치(100)는, 카메라 장치(600) 및 센서 장치(700)로부터 수신되는 영상 정보 및 센서 정보를 수집 및 저장 관리할 수 있으며, 영상 정보 및 센서 정보에 기초하여 보안 감시 지역에서 발생되는 하나 이상의 보안 감시 이벤트를 검출하고, 검출된 이벤트에 대응하는 감시 서비스 처리를 수행할 수 있다.

[0028] 여기서, 감시 서비스 처리는 발생된 이벤트에 대응하는 사용자 단말(200)로의 알람 메시지 전송 서비스, 경보 알림 기능 동작 또는 해제 서비스, 관제 서비스 서버(500)로의 상태정보 전송 서비스 등이 예시될 수 있다.

[0029] 이러한 감시 서비스 처리를 위해, 지능형 보안 감시 장치(100)는 중계 서버(400), 관제 서비스 서버(500) 또는 사용자 단말(200)과 유무선 네트워크로 연결될 수 있고, 상기 지능형 보안 감시 장치(100)는 상기 유무선 네트워크를 통해 통신을 수행하기 위한 하나 이상의 유무선 통신 모듈을 구비할 수 있다. 상기 유무선 통신 네트워크는 널리 알려진 다양한 통신 방식이 적용될 수 있다.

[0030] 그리고, 지능형 보안 감시 장치(100)는 영상 정보 및 센서 정보를 분석하여 이벤트를 검출하기 위한 하나 이상의 정보 처리 모듈 및 정보 분석 모듈을 포함할 수 있다.

[0031] 또한, 지능형 보안 감시 장치(100)는 정보 처리 및 분석에 따른 초기 분석 정보를 기반으로 소정의 제1 감시 이벤트들을 검출할 수 있으나, 객체의 정확한 검출 및 분류를 통해 보다 정확한 분석이 요구되는 제2 감시 이벤트에 대하여는 별도의 딥러닝 분석 처리를 하나 이상의 딥러닝 분산 처리 장치(300)와 연동하여 처리할 수 있다.

[0032] 여기서, 상기 제1 감시 이벤트 및 제2 감시 이벤트는 딥러닝 분석 처리 여부에 따라 그룹핑될 수 있으며, 제1

감시 이벤트는 센서 정보 및 영상 정보의 초기 분석에 따라 신속히 검출되는 침입 이벤트, 카메라 무단 변경 이벤트, 화재 발생 이벤트 등이 예시될 수 있고, 제2 감시 이벤트는 딥러닝 분석에 따른 정확한 객체 검출 및 분류 정보가 수반되는 동적 객체 추적 이벤트, 트립 와이어 이벤트, 배회객체 감지 이벤트, 통행방향 위반 감지 이벤트, 무단 방치물 감지 이벤트, 무단 이동물체 감지 이벤트, 출입 카운팅 및 통계 이벤트, 군중 밀집상태 감지 이벤트, 특이행동 감지 이벤트 등이 예시될 수 있다.

[0033] 다만, 이는 예시이므로, 감시 기준 및 객체 분류 설정에 따른 더욱 더 다양한 이벤트 감지가 가능할 수 있으며, 제1 감시 이벤트와 제2 감시 이벤트가 복합적으로 검출되어 신속한 복합 감시 서비스 제공에 이용될 수도 있다. 예를 들어, 지능형 보안 감시 장치(100)는, 제1 감시 이벤트 발생에 따른 초기 분석 정보를 중계 서버(400)를 통해 관제 서비스 서버(500) 또는 사용자 단말(200)로 우선 전송하고, 상기 제1 감시 이벤트와 연관된 일정 시간 범위 이내의 영상 정보의 딥러닝 분석 결과에 따라, 상기 제1 감시 이벤트에 대한 상세 분석 정보로서 제2 감시 이벤트를 검출하여 상기 중계 서버(400)를 통해 관제 서비스 서버(500) 또는 사용자 단말(200)로 제2 감시 이벤트 정보를 제공할 수 있다.

[0034] 이에 따라, 지능형 보안 감시 장치(100)는 제1 감시 이벤트에 따른 기본적 감시 서비스 처리를 신속하게 처리할 수 있을 뿐만 아니라, 지능형 보안 감시 장치(100)에서 초기 분석 처리된 데이터에 대한 분산 데이터의 딥러닝 분석 처리만을 별도의 전문화된 딥러닝 분산 처리 장치(300)로 요청하여 처리하므로, 보다 정확한 객체 분류가 가능하여야만 제공되는 제2 감시 이벤트의 발생여부 또한 데이터의 분산 처리에 따라 신속하게 검출할 수 있게 된다.

[0035] 이를 위해, 지능형 보안 감시 장치(100)는 제2 이벤트 검출 처리를 위해 딥러닝 분석이 필요한 영상 정보에 대응하는 분산 데이터를 구성하고, 딥러닝 분산 처리 장치(300)로 딥러닝 분석 처리 요청을 전송할 수 있다.

[0036] 보다 구체적으로, 지능형 보안 감시 장치(100)는, 수집된 영상 정보 상에서 제1 이벤트를 검출 가능한 초기 분석 정보를 처리하고, 상기 초기 분석 정보로부터 상기 영상 정보에 대응하는 객체를 추적하기 위한 추적 데이터를 획득할 수 있다.

[0037] 예를 들어, 상기 초기 분석 처리는, 영상 안정화 처리, 배경 모델링 처리, 형태 연산 처리, 요소 연결 처리 및 객체 추적 처리 중 적어도 하나를 포함할 수 있으며, 상기 추적 데이터는 예를 들어 영상 정보로부터 전경화소가 분리 필터링되고, 연결 성분이 라벨링되어 시각 변환 처리된 객체 추적 데이터를 포함할 수 있다.

[0038] 지능형 보안 감시 장치(100)는 상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하고, 상기 딥러닝 분산 처리 요청 데이터를 딥러닝 분산 처리 장치로 전송할 수 있다.

[0039] 딥러닝 분산 처리 장치(300)는, 네트워크를 통해 연결되어 엣지 컴퓨팅을 수행하는 하나 또는 그 이상의 장치들로 구성될 수 있으며, 상기 딥러닝 분산 처리 요청 데이터에 따라, 상기 추적 데이터 및 상기 영상 정보의 딥러닝 분석을 처리할 수 있으며, 딥러닝 분석 결과 정보를 지능형 보안 감시 장치(100)로 전달할 수 있다. 보다 구체적으로, 딥러닝 분석 결과 정보에는 상기 추적된 객체에 대응하는 객체 검출 정보 및 객체 분류 정보를 포함할 수 있다.

[0040] 이러한 객체 검출 정보 및 객체 분류 정보는, 예를 들어 사전 누적 학습된 영상 정보로부터 특정 방향으로 움직이거나 동작하는 등의 패턴에 따라 식별되는 동적 객체 정보가 예시될 수 있으며, 지능형 보안 감시 장치(100)는 상기 객체 검출 정보 및 상기 객체 분류 정보와, 상기 추적 데이터에 기초하여, 상기 영상 정보에 대응하는 제2 감시 이벤트를 검출할 수 있다.

[0041] 한편, 딥러닝 분산 처리 장치(300)는, 지능형 보안 감시 장치(100)로부터 수신되는 딥러닝 분산 처리 요청 데이터에 따른 딥러닝 영상 분석을 처리하고, 그 결과 정보를 지능형 보안 감시 장치(100)로 전달할 수 있으며, 나아가 딥러닝 영상 분석 정보는 중계 서버(400)로도 전송될 수 있다.

[0042] 딥러닝 분산 처리 장치(300)는, 딥러닝 분산 처리 요청 데이터에 기초하여, 일반적으로 기존의 보안 시스템이 저조도의 환경에서 동작하여 센서의 센싱 신호를 통해 감시 대상의 감지시 생성된 동영상에 대한 영상 분석 과정에서 객체가 검출된 경우에도 객체의 식별이 어려워 감시 대상 객체가 아닌 객체에 대한 이벤트를 생성하여 보고하거나 센서를 통해 감시 대상이 감지된 경우에도 영상에서 낮은 조도로 인해 객체가 식별되지 않아 감시 대상의 감지에 따른 보고가 누락되는 경우와 같은 오보율이 증가하는 문제점을 개선하기 위한 딥러닝 분석을 처리할 수 있다.

[0043] 딥러닝 분산 처리 장치(300)는, 딥 러닝을 통해 감시 대상 지역의 환경 특성(환경 조건)에서 나타나는 감시 대

상 객체의 특징을 지속적으로 학습하여 감시 대상 객체에 대한 식별 정확도를 높이는 동시에 감시 대상 객체가 식별된 이미지의 영상 특징을 지속적으로 학습하여 객체 식별이 용이한 최적의 이미지를 판단하고 이를 통해 감시 대상 객체가 정확하게 식별되는 이미지를 선별하여 제공함으로써 감시 대상 객체를 다른 객체와 정확히 구분하여 식별되도록 지원하여 오보율을 낮추는 동시에 감시 대상의 감지시 보고가 누락되는 경우를 방지하도록 하는 딥러닝 분석 결과 정보를 획득하고, 지능형 보안 감시 장치(100) 또는 중계 서버(400)로 분석 결과 정보를 제공할 수 있다.

[0044] 여기서, 상기 중계 서버(400)는 각지에 설치되는 지능형 보안 감시 장치(100)들로부터 영상 감시 분석 데이터를 수집하여 저장 및 관리하고, 딥러닝 분산 처리 장치(300)로부터 수신되는 딥러닝 영상 분석 결과와 상기 영상 감시 분석 데이터를 사용자 단말(200) 및 관제 서비스 서버(500)로 중계하는 서버일 수 있다.

[0045] 이러한 중계 서버(400)는 상기 지능형 보안 감시 장치(100)의 이벤트 검출 데이터가 수신된 경우, 상기 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 색인하여 상기 지능형 보안 감시 장치(100)에 대응하여 사전 등록된 사용자 단말(200)로 상기 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 전송하는 서버일 수 있다.

[0046] 또한, 상기 이벤트 검출 데이터 및 딥러닝 영상 분석 정보는 관제 서비스 서버(500)로도 전달될 수 있으며, 관제 서비스 서버(500)는 상기 이벤트 검출 데이터 및 딥러닝 영상 분석 정보에 기초한 사고 발생 신고, 화재 발생 신고, 사용자 알림, 감시 장치 제어, 실시간 모니터링 등의 다양한 관제 서비스 처리를 수행하고, 서비스 수행 정보를 사용자 단말(200)로 전송할 수 있다.

[0048] 도 2는 본 발명의 실시 예에 따른 지능형 감시 장치 및 딥러닝 분산 서버의 구성 및 연결관계를 보다 구체적으로 도시한 블록도이다.

[0049] 도 2를 참조하면, 본 발명의 실시 예에 따른 지능형 보안 감시 장치(100)는, 영상 정보 수집부(110), 배경 모델링부(120), 형태 연산 처리부(130), 요소 연결 처리부(140), 객체 추적부(150), 3차원 시점 변환부(160), 객체 분류 처리부(170), 이벤트 검출부(180), 분산 데이터 처리부(190) 및 감시 서비스 처리부(185)를 포함할 수 있으며, 분산 데이터 처리부(190)는 딥러닝 분산 처리 장치(300)와 연결될 수 있다.

[0050] 그리고, 딥러닝 분산 처리 장치(300)는 딥러닝 기반 영상 정보 분석부(310), 객체 검출부(320), 객체 분류 처리부(330)를 포함할 수 있다.

[0051] 먼저, 영상 정보 수집부(110)는, 센서 장치(700)로부터 수신되는 보안 감시 영역 센싱 정보와 카메라 장치(600)로부터 수신되는 보안 감시 영역 촬영 영상 데이터를 수집하고, 영상 데이터에 카메라의 촬영영상 내 프레임의 흔들림이 존재하는 경우, 흔들림 보정에 따른 영상 정보의 안정화를 처리할 수 있다. 여기서, 안정화 처리는 카메라로부터 촬영된 영상을 블록으로 분할하여 특징점을 추출하고, 특징점의 움직임벡터 산출을 통해 영상의 흔들림을 보정하여 안정된 영상을 획득하는 처리가 예시될 수 있다.

[0052] 그리고, 배경 모델링부(120)는 안정화 처리된 영상 정보에 대응하는 배경 영역을 모델링 처리할 수 있다. 카메라 장치(600)는 복수 개 구비될 수 있으며, 배경 모델링부(120)는 각 카메라 장치(600)에서 촬영된 영상 영역별로 영상의 배경을 모델링할 수 있다. 배경 모델링부(120)는 배경 모델링에 따라, 전경에 대응하는 객체를 식별하고, 추적될 수 있도록 하는 배경 영역 데이터를 연산할 수 있다.

[0053] 이러한 배경 모델링부(120)는 복잡한 환경에서 객체를 정확히 검출할 수 있도록, 잘 알려진 가우시안 혼합 모델(Gaussian Mixutre Model)을 기반으로 하는 배경 확률 모델을 영상 데이터로부터 생성할 수 있다. 이는 조명의 변화, 배경에 첨가되거나 제거되는 객체, 흔들리는 나뭇가지나 분수 등의 움직임을 가지는 배경, 통행량이 많은 영역 등의 많은 변수를 반영하여 배경 영역 데이터로 생성할 수 있도록 한다.

[0054] 보다 구체적으로 배경 모델링부(120)는 카메라 장치(600)의 영상 정보로부터 연속적 영상 프레임이 입력되면, 배경 감산 처리를 통해 시간 t에 대한 통계학적 확률에 따른 픽셀당 배경 모델을 구성할 수 있다. 배경 모델링부(120)는 현재 프레임의 영상 정보에서 가우시안 혼합 모델에 따라 구성된 배경 정보를 차감하고, 상기 배경 정보를 픽셀당 배경 모델에 누적 업데이트 하는 방식으로 이루어지는 MOG(Mixtrue of Guassians) 방식에 따라 배경 감산 처리를 수행할 수 있다.

[0055] 배경 모델링부(120)의 배경 감산 처리에 따라, 배경이 차감된 영상 정보에는 전경 픽셀 정보가 남게 되는 바, 이를 블롭(blob) 이미지라고 할 수 있으며, 블롭 이미지는 전경 픽셀에 대응하는 이진 맵 데이터라고도 할 수

있다.

[0056] 형태 연산 처리부(130)는, 배경 모델링부(120)에서의 배경 모델링에 따라 차감 출력되는 전경 픽셀 정보의 이진 맵 데이터로부터, 형태 영역 정보를 결정하는 형태 연산 처리를 수행할 수 있다. 형태 영역 정보는 복수의 픽셀들을 하나 이상의 형태 구조 요소로 그룹핑하는 그룹핑 정보일 수 있다.

[0057] 예를 들어, 형태 연산 처리부(130)는 하나 이상의 형태론적 연산 필터들을 상기 전경 픽셀 정보의 이진 맵 데이터에 적용함에 따라 상기 형태 영역 정보를 결정할 수 있다. 여기서 하나 이상의 형태론적 연산 필터는 이진 침식(erosion) 연산 필터 및 이진 팽창(dilation) 연산 필터를 포함할 수 있는 바, 각 필터들은 이진 맵 데이터 내 밝은 영역의 크기를 사전 결정된 형태 구조 요소의 크기 정보에 비례하여 확장하거나 축소시키는 연산 처리를 수행할 수 있다. 팽창 연산 필터 적용시 형태 구조 요소보다 작은 어두운 영역이 제거되고, 반대로 침식 연산 필터 적용시 형태 구조 요소보다 작은 밝은 영역들이 제거될 수 있으며, 동시에, 제거되지 않는 큰 영역들의 크기도 줄거나 커지게 형성될 수 있다.

[0058] 그리고, 사전 특정된 크기의 객체 검출을 위해, 형태 연산 처리부(130)는 이진 개방 필터 및 폐쇄 필터를 이용하여, 상기 형태 구조 요소보다 큰 영역의 크기는 그대로 유지한 채, 작은 영역들만 제거시키는 처리를 수행할 수도 있다.

[0059] 그리고, 요소 연결 처리부(140)는, 형태 연산 처리부(130)에서 특정된 형태 구조 요소에 대응하는 영상 정보를 획득하고, 각 형태 구조 요소들을 연결 처리하여 독립적인 객체 연결 영역들로 분류하며, 분류된 객체 연결 영역에 대응하는 고유의 라벨 값들을 할당하는 연결 성분 라벨링 처리를 수행할 수 있다. 이러한 연결 성분 라벨링 처리는 특히 이진 맵 데이터에서 효과적으로 이용될 수 있다.

[0060] 요소 연결 처리부(140)는 분류된 객체 연결 영역들을 고유의 라벨 값으로 구분하고, 각 객체 영역의 크기, 위치, 방향, 둘레와 같은 영역의 특징값들을 결정하여 출력할 수 있다. 요소 연결 처리부(140)는 순환적 알고리즘 또는 순차적 알고리즘을 적용하여, 연결 성분 라벨링 처리를 수행하고, 객체 연결 영역들을 분류할 수 있다.

[0061] 예를 들어, 순차적 알고리즘은 각 전경 화소의 픽셀 데이터에 대해 그 화소의 상단 화소와 왼쪽 화소의 라벨을 검색하여 현재 화소의 라벨을 결정하는 알고리즘일 수 있다. 상기 상단 화소와 상기 왼쪽 화소를 포함하는 이웃 화소들은 라벨링 과정에서 이미 처리된 화소일 수 있다.

[0062] 여기서, 요소 연결 처리부(140)는 이웃 화소들이 모두 전경 화소가 아닌 경우에는 현재 화소에 새로운 라벨값을 할당할 수 있다. 그리고, 요소 연결 처리부(140)는 두 이웃 화소 중 하나의 화소만 전경 화소인 경우에는 그 화소의 라벨값을 현재 화소에 할당할 수 있다. 그리고, 요소 연결 처리부(140)는, 두 이웃 화소가 모두 전경 화소이면서 같은 라벨값을 갖는 경우에는 동일한 라벨값을 현재 화소에 할당할 수 있다.

[0063] 그러나, 두 화소가 전경 화소지만 서로 다른 라벨값을 갖는 경우에는 이 두 영역은 현재 화소에 의해 서로 연결되는 영역이므로 동일한 라벨값으로 병합되어야 한다. 따라서 요소 연결 처리부(140)는 두 화소의 라벨값 중 더 작은 값을 현재화소의 라벨값으로 할당하고, 두 라벨은 동치 테이블에 동치 라벨로 등록할 수 있다. 이러한 첫 번째 라벨링 과정의 수행이 종료되면 동치 테이블에는 동일한 영역으로 병합되어야 하는 라벨에 대한 정보가 저장될 수 있다. 요소 연결 처리부(140)는, 이 동치 테이블을 이용하여 두 번째 라벨링 과정에서 각 객체 연결 영역의 모든 화소에 동일한 라벨을 할당할 수 있다.

[0064] 이에 따라, 요소 연결 처리부(140)는 전경 픽셀 데이터를 포함하는 블롭(blob) 이미지 데이터와 함께 연결 성분 라벨링 처리에 따른 객체 연결 영역 정보를 출력할 수 있는 바, 객체 연결 영역 정보는 각 객체 연결 영역에 대응하는 특성 정보(위치 정보, 크기 정보, 방향 정보, 둘레 정보 등)를 포함할 수 있다.

[0065] 그리고, 객체 추적부(150)는 블롭(blob) 이미지 데이터 및 객체 연결 영역 정보에 기초하여, 영상 정보 내 객체 정보를 추적하기 위한 추적 데이터를 획득할 수 있다. 추적 데이터는 영상 내에서 발견 및 추적된 객체의 리스트 정보를 포함할 수 있다. 보다 구체적으로, 객체 추적부(150)는 시간 t에서의 블롭 이미지와 t-1에서의 블롭 이미지를 누적 매칭시켜, 객체 연결 영역에 대응하는 객체를 식별 처리하고, 리스트에 산입할 수 있는 바, 칼만 필터 방식으로 추적 처리하는 것이 예시될 수 있다. 칼만 필터는 시간에 따라 진행한 측정을 기반으로 입력 데이터를 재귀적으로 누적시켜 선형 역학계의 상태를 검출하는 필터이다.

[0066] 이에 따라, 객체 추적부(150)는 영상 정보 내 식별되는 객체 추적 데이터를 출력할 수 있다. 객체 추적 데이터는 객체의 리스트 정보와 함께, 식별된 각 객체의 크기 정보 및 이동 속도 정보를 포함할 수 있다.

[0067] 그리고, 시점 변환부(160)는 전술한 객체 추적 데이터 내 각 객체의 크기 정보 및 이동 속도 정보를 카메라 장

치별 3차원 시점 조건에 따른 실제적 수치로 변환 처리한다. 즉 객체 추적부(150)의 추적 데이터는 객체의 크기와 속도 정보를 갖고 있으나 픽셀간의 상대적 값이므로, 시점 변환부(160)는 이미지의 픽셀 좌표를 실제 현실 공간상의 좌표로 변환처리할 수 있는 바, 캘리브레이션을 통해 미리 지정된 화각, 높이 등의 카메라 특성 정보를 이용한 변환 처리가 수행될 수 있다.

[0068] 이에 따라, 시점 변환부(160)는 객체 추적 데이터 내 리스트된 객체들의 크기 정보 및 속도 정보를 변환하여 실제 현실 공간상의 크기 정보 및 속도 정보로 변환 처리할 수 있다.

[0069] 한편, 객체 분류 처리부(170)는, 사전 설정된 분류 기준에 기초하여, 상기 객체 추적 데이터에서 식별된 객체에 분류 정보를 할당하는 처리를 수행할 수 있다. 다만, 분류 기준 자체를 설정하거나, 분류 기준에 대응하는지 여부를 정확히 판단하는 프로세스는, 로컬 감시 네트워크에 설치되는 지능형 보안 감시 장치(100)보다는 별도의 딥러닝 분산 처리 장치(300)에서 처리되는 것이 보다 효율적일 수 있다.

[0070] 즉, 외부의 다양한 영상 정보의 누적 학습을 통해 저조도의 환경 등에서도 객체를 정확히 분류 검출할 수 있도록 하기 위하여 객체 분류 처리부(170)는 분산 데이터 처리부(190)를 통해 객체 분류 처리를 위한 상기 추적 데이터 및 영상 정보를 포함하는 딥러닝 분석 처리 요청을 딥러닝 분산 처리 장치(300)로 전달하고, 딥러닝 분산 처리 장치(300)로부터 분석 결과 정보를 수신하며, 수신된 분석 결과 정보를 이용한 객체 분류 처리를 수행할 수 있다.

[0071] 분산 데이터 처리부(190)는, 시점 변환부(160)를 통해 획득되는 초기 분석에 따른 상기 추적 데이터 및 상기 영상 정보에 기초하여, 딥러닝 분산 처리 요청 데이터를 생성하고, 상기 딥러닝 분산 처리 요청 데이터를 딥러닝 분산 처리 장치로 전송 처리할 수 있으며, 상기 딥러닝 분산 처리 장치(300)로부터 수신되는 딥러닝 기반 영상 정보 분석 결과를 수신하여, 객체 분류 처리부(170)로 전달할 수 있다.

[0072] 딥러닝 분산 처리 장치(300)는, 딥 러닝 방식에 따라 사전 학습된 영상 정보로부터 신경망 데이터를 구축하는 딥러닝 기반 영상 정보 분석부(310), 상기 신경망 데이터를 이용하여 상기 분산 처리 요청 데이터에 대응하는 객체 정보를 검출하는 객체 검출부(320) 및 검출된 객체 정보의 분류 정보를 결정하는 객체 분류 처리부(330)를 포함할 수 있다.

[0073] 딥러닝 기반 영상 정보 분석부(310)는 예를 들어, DNN(Deep Neural Network) 기반의 딥 러닝 알고리즘에 따른 신경 회로망이 설정되고, 해당 신경 회로망은 입력층(Input Layer), 하나 이상의 은닉층(Hidden Layers) 및 출력층(Output Layer)으로 구성될 수 있다. 여기서, 상기 딥 러닝 알고리즘은 DNN 이외의 다른 신경망이 적용될 수도 있으며, 일례로, CNN(Convolution Neural Network)이나 RNN(Recurrent Neural Network)과 같은 신경망이 적용될 수 있다.

[0074] 여기서, 상기 딥러닝 분산 처리 장치(300)의 딥러닝 기반 영상 정보 분석부(310)는, 딥 러닝 기반의 신경 회로망을 통해 상기 영상 정보로부터 획득되는 하나 이상의 정상 이미지를 분석하여 감시 대상 객체를 식별하고, 감시 대상 객체가 식별된 정상 이미지를 저장할 수 있다.

[0075] 보다 구체적으로, 예를 들어, 딥러닝 기반 영상 정보 분석부(310)는, 학습 영상 정보로부터 획득되는 하나 이상의 특정 이미지에서 감시 대상 객체를 식별할 수 있으며, 상기 감시 대상 객체가 아닌 특정 객체가 식별된 경우 상기 특정 이미지와 하나 이상의 상기 정상 이미지 사이의 유사도를 산출하며, 상기 유사도가 미리 설정된 기준치 이상인 경우, 상기 특정 이미지에 대하여 상기 신경 회로망을 기반으로 영상 처리된 출력값과 객체 정보 사이의 오차에 대한 오차 정보를 생성하고, 미리 설정된 역전파 알고리즘(back propagation algorithm)을 통해 상기 오차 정보를 기반으로 상기 신경 회로망을 구성하는 파라미터를 조정할 수 있다.

[0076] 여기서 이미지 사이의 유사도 비교 방식으로는 히스토그램 매칭(Histogram

[0077] matching)이나, 상기 이미지에서 식별된 객체에 지정된 템플릿 매칭(Template matching) 또는 상기 이미지에서 상기 신경 회로망을 통해 추출된 특징점 비교 등을 이용하여 유사도를 비교하는 것이 예시될 수 있다.

[0078] 그리고, 상기 딥러닝 기반 영상 정보 분석부(310)는 상기 오차 정보를 기초로 상기 역전파 알고리즘을 통해 상기 신경 회로망을 구성하는 입력층, 하나 이상의 은닉층 및 출력층 사이의 연결 강도에 대한 가중치(weight) 또는 상기 입력층, 은닉층 및 출력층에 구성된 유닛의 바이어스(bias)를 가변하여 상기 감시 대상 객체에 대한 식별 오류가 최소화되도록 학습처리할 수 있다.

[0079] 또한, 딥러닝 기반 영상 정보 분석부(310)는 상기 신경회로망을 통해 지능형 보안 감시 장치(100) 또는 다른 다양한 영상 장치로부터 지속적으로 수신된 이미지를 반복 학습하여 상기 객체정보를 갱신할 수 있으며, 이를 통

해 상기 감시 대상 지역의 환경 변화(환경 조건 변화(일례로, 조도, 장애물))에 따라 상기 이미지에 나타나는 객체 특징 변화에 적응하여 상기 이미지에서 상기 객체 정보에 포함된 객체 특징별 파라미터에 대응되는 객체를 정확하게 식별할 수 있다.

[0080] 그리고, 객체 검출부(320)는, 상기 학습된 신경망(또는 신경회로망) 데이터에 기초하여 딥러닝 분산 처리 요청 데이터로부터 획득되는 추적 데이터 및 영상 정보로부터 식별된 하나 이상의 객체를 검출할 수 있고, 객체 분류 처리부(330)는, 객체별로 이미지상 위치별 크기, 색상 분포, 외곽선 등에 대한 다양한 객체 특징별 파라미터를 포함하는 객체 분류 정보를 생성할 수 있으며, 생성된 객체 분류 정보를 지능형 보안 감시 장치(100)의 분산 데이터 처리부(190)로 전송할 수 있다.

[0081] 딥러닝 분산 처리 장치(300)는 별도의 사용자 입력부 또는 통신부를 포함할 수 있으며, 딥러닝 분산 처리 장치(300)는 상기 사용자 입력부를 통한 사용자 입력 관련 제어정보나, 상기 통신부를 통해 외부로부터 수신된 제어정보를 기초로 상기 객체 분류 처리부(330)에 의해 분류된 하나 이상의 객체 중 어느 하나를 감시 대상 객체로 설정할 수 있으며, 이에 대한 설정정보를 저장할 수 있다.

[0082] 이러한 처리를 통해, 지능형 보안 감시 장치(100)는, 딥러닝 분산 처리 장치(300)에서 제공되는 분산 데이터의 분석 처리를 통해, 고성능 딥러닝 연산의 처리결과만을 수신하여 신속하게 이벤트 검출부(180)로 전달할 수 있는 바, 지능형 보안 감시 장치(100) 자체의 신속한 데이터 처리와 함께 복잡한 딥러닝 분석이 필요한 데이터만 별도의 데이터 가공을 통해 분산 처리함으로써, 지능형 보안 감시 장치(100)에 고성능 분석장비를 탑재하지 않고도 딥러닝 영상 분석의 장점과 데이터 처리의 신속성을 확보할 수 있다.

[0083] 이러한 분산 데이터 처리는 지능형 보안 감시 장치(100)와 딥러닝 분산 처리 장치(300)를 연동한 엣지(edge) 컴퓨팅 방식으로 처리될 수 있는 바, 딥러닝 분산 처리 장치(300)는 분산 데이터 처리부(190)와의 데이터 처리 지연 시간을 최소화하기 위한 최소한의 데이터만을 수집 및 분석 처리함으로써, 빠른 서비스 처리를 제공할 수 있는 엣지 장치일 수 있으며, 이를 제공할 수 있는 분산된 개방형 아키텍처로 구축될 수 있다.

[0084] 또한, 딥러닝 기반 영상 분석은 감시 대상 객체에 대한 반복 학습을 통한 감시 대상 객체의 식별에 대한 정확도를 높일 수 있을 뿐만 아니라 감시 대상 지역의 환경 특성이 반영된 동영상 또는 이미지에서 나타나는 감시 대상 객체의 특징 변화를 학습하고, 이를 기초로 보안 시스템의 운용 특성상 일반적으로 저조도 환경에서 운용되는 카메라를 통해 촬영된 감시 대상을 정확하게 식별할 수 있도록 감시 대상지역에서 나타나는 감시 대상 객체의 특징에 맞추어 딥 러닝 알고리즘을 최적화하여 객체 식별 정확도를 높일수 있으며, 이를 통해 감시 대상 객체 이외의 객체를 정확하게 구분하여 감시 대상이 아닌 객체를 감시 대상으로 오판하여 오보가 발생하지 않도록 지원할 수 있다.

[0085] 그리고, 이벤트 검출부(180)는 수집된 센서 정보와, 상기 영상 정보의 추적 데이터 및 분산 데이터 처리부(190)로부터 객체 분류 처리부(170)를 통해 전달된 상기 객체 분류 정보 중 적어도 하나에 따라 획득되는 하나 이상의 이벤트를 검출하고, 검출된 이벤트 정보는 감시 서비스 처리부(185)로 전달될 수 있다. 감시 서비스 처리부(185)는, 각 이벤트 정보에 따라 사전 결정된 감시 서비스 프로세스를 수행할 수 있는 바, 이에 대하여는 도 3을 참조하여 보다 구체적으로 설명하도록 한다.

[0087] 도 3은 본 발명의 실시 예에 따른 이벤트 검출부의 검출 모듈을 설명하기 위한 블록도이다.

[0088] 도 3을 참조하면, 본 발명의 실시 예에 따른 이벤트 검출부(180)는 딥러닝 분산 처리 장치(300)에 의해, 영상 내 움직이는 객체들을 특정 행동을 하는 사람, 특정 형태의 차량 등으로 보다 정확하게 분류할 수 있게 됨에 따라, 보다 다양한 형태의 이벤트 검출을 수행할 수 있고, 감시 서비스 처리부(185)는 각 이벤트 검출에 적합한 사용자 단말(200)로의 알림 서비스 또는 중계 서버(400)로의 전송 서비스 처리, 관제요청 서비스 처리 등을 수행할 수 있다.

[0089] 이에 따라, 이벤트 검출부(180)는 추적 데이터 및 객체 분류 정보로부터 영상 정보 내 동적 객체 추적(Dynamic Object Tracking)을 수행하고, 동적 객체 추적 정보에 따라 하나 이상의 이벤트를 검출 또는 감지하는 검출부 또는 감지부를 포함할 수 있다.

[0090] 즉 이벤트 검출부(180)는, 객체 추적부(150)의 추적 데이터와 분산 데이터 처리부(190)로부터 수신된 딥러닝 기반 객체 분류 정보를 매핑하고, 이를 이용하여 카메라 가시영역(Filed of View) 내에서 움직이는 모든 객체를 개별적으로 추적함으로써 트립 와이어 또는 관심영역(Area of Interest) 통과순간을 파악할 수 있으며, 나아가

객체별 이동 궤도(Trajectory)를 분석해 매장에서의 고객 흐름 분석 등에 이용되는 감지 또는 통계 정보를 출력할 수도 있다.

[0091] 보다 구체적으로, 이벤트 검출부(180)는 트립 와이어 검출부를 포함할 수 있다. 트립 와이어 검출부는 가상의 경계선을 설정하고, 상기 동적 객체 추적을 통해 외곽경계(Perimeter Detection)를 위한 침입감지(Intrusion Detection)나 특정 영역내 침입감지를 처리할 수 있다.

[0092] 트립 와이어 검출부는 상기 경계선을 통과(침입)하는 객체 카운팅(Object Counting)도 처리할 수 있는 바, 트립 와이어를 기준으로 지면상에서 통과하는 객체(사람, 차량 또는 기타 물체)가 있을 때 감지하되, 그 움직임의 방향(양방향 또는 단방향) 추적을 통해 제1 방향에서 제2 방향으로 이동하다가 트립 와이어를 통과(침입)했는지를 확인하여, 이벤트 발생여부를 결정할 수 있다.

[0093] 그리고, 이벤트 검출부(180)는 침입 감지부를 포함할 수 있다. 침입 감지부는, 상기 트립 와이어 검출부를 이용하여 경계선 기반의 침입을 감지하거나, 사전 설정된 관심 영역에 대응하는 객체 움직임이 검출된 경우, 침입을 감지하는 등의 관심영역 기반 침입 감지 처리를 수행할 수 있다. 경계 울타리(Perimeter), 바다 또는 해안, 공중(하늘), 출입구 등은 트립 와이어 방식이 바람직하며, 건물 내에서는 관심영역을 사용해 침입 감지를 하는 것이 바람직할 수 있다. 또한, 칩임 감지부는 트립 와이어와 관심영역 기반 침입 감지 처리를 동시에 수행할 수도 있다.

[0094] 또한, 이벤트 검출부(180)는, 배회객체 감지부를 포함할 수 있다. 배회객체 감지부는, 사람 또는 차량과 같은 배회객체를 감지(Loitering)하여 배회객체 이벤트 정보를 획득하고, 배회객체 이벤트 정보를 감시 서비스 처리부(185)로 전달할 수 있다.

[0095] 예를 들어, 배회객체 감지부는 주요 보안시설, 보안 경계지역, 고가품 보관시설 등을 관찰할 때 이용될 수 있다. 이벤트 검출부(180)는 배회객체 감지부를 통해, 외부인 또는 외부차량 등의 객체가 출입제한지역 주변을 일정 시간 이상 배회하고 있지 여부를 감지하고, 일정 시간 이상 배회하는 객체를 배회객체로 감지할 수 있다. 배회하는 사람이나 차량은 사고를 발생시킬 수 있는 가능성이 있으므로 집중 감시대상이 되며, 이를 통해 사고를 미연에 방지할 수 있다.

[0096] 한편, 이벤트 검출부(180)는 통행방향 위반 감지부를 포함할 수 있다. 통행방향 위반(Wrong Directions) 감지부는 공항과 같은 통행 방향 준수 지역에서의 통행 위반 객체를 감지할 수 있다. 이벤트 검출부(180)는 통행 방향 위반 객체를 검출할 수 있으며, 이러한 통행 방향 위반 객체 검출부는 들어오는 방향과 나가는 방향이 서로 다르게 지정되어 있는 극장, 공연장에 대하여도 동작할 수 있다. 차량에 대해 적용할 경우 통행 방향 위반 객체 검출부는 역주행 감지 등을 처리하여 역주행 차량 객체를 통행 방향 위반 객체로서 검출할 수 있다.

[0097] 그리고, 이벤트 검출부(180)는 무단 방치물 감지부를 포함할 수 있다. 무단 방치물(Unattended Object)부는 사전 서정된 관심영역 내에 누군가에 의해 방치된 객체(짐꾸러미, 가방, 카트 등)가 등장한 후 지정 시간이 초과한 이후에도 계속 정지된 상태로 존재하는 무단 방치물을 감지하고, 감지된 무단 방치물 객체 정보를 감시 서비스 처리부(185)로 전달할 수 있다. 이는 특히 공항, 터미널, 역사 플랫폼, 주요 행사장 등에 테러를 위해 폭발물을 임의 방치하는 것을 사전에 감지해 예방할 수 있게 한다.

[0098] 또한, 이벤트 검출부(180)는, 무단 이동물체 감지부를 포함할 수 있다. 무단 이동물체 감지부는 박물관, 전시회, 고가품 디스플레이, 공항, 매장, 창고 등 도난이 자주 발생하는 곳에서 사전 지정해 놓은 물체들이 영상 객체에서 사라져 버린 경우, 이를 감지하여 획득된 이벤트 정보를 감시 서비스 처리부(185)로 전달할 수 있다.

[0099] 그리고, 이벤트 검출부(180)는 출입 카운팅 및 통계부를 포함할 수 있다. 출입 카운팅(Object Counting) 및 통계부는 백화점, 쇼핑센터 등 매장, 박물관, 전시회, 극장 등 공공시설물의 입장객수와 퇴장객수 통계정보를 획득하여 감시 서비스 처리부(185)로 전달할 수 있다. 감시 서비스 처리부(185)는, 실시간 카운팅과 함께 시간대별 출입자 통계 정보를 사용자 단말(200) 또는 중계 서버(400)를 통해 관제 서비스 장치(500)로 제공할 수 있는 바, 사용자는 통계 정보를 경영상 고객관리, 매장배치관리에 필요한 기본적인 정보로 활용할 수 있다. 또한, 사용자 단말(200)에서는 상기 출입자 통계 정보에 기초하여 획득된 입장 고객수 대비 매출액을 비교하는 통계 정보를 출력할 수도 있다. 나아가, 출입 카운팅 및 통계부는 특정 도로 상에서 차선별 통행 차량수를 자동산출하는 처리를 수행할 수도 있으며, 감시 서비스 처리부(185)는 시간대별 통행 차량수 통계자료등을 사용자 단말(200) 또는 중계 서버(400)나 관제 서비스 서버(500) 로 제공할 수도 있다.

[0100] 한편, 이벤트 검출부(180)는 군중 밀집상태 감지부를 포함할 수 있다. 군중 밀집상태(Crowd Density) 감지부는,

사전 설정된 관심영역 내에서 지정한 군중 밀집규모보다 초과되는 군중(Overcrowd) 규모로 발전하는 이벤트를 감지할 수 있다.

[0101] 이를 위해, 이벤트 검출부(180)는 객체 추적 데이터 및 분류 정보로부터 실시간으로 현재의 밀집상태를 확인할 수 있으며, 밀집상태에 대응하는 이벤트 정보를 감시 서비스 처리부(185)로 전달할 수 있다. 감시 서비스 처리부(185)는 이벤트 정보에 기초한 밀집상태 정보를 사용자 단말(200) 또는 중계 서버(400)나 관제 서비스 서버(500)로 전송할 수 있다. 예를 들어, 관리자는 밀집상태 정보를 확인하고, 매장, 공항, 극장 등에서는 군중이 초과 밀집상태로 커질 경우 출입문 또는 계산대를 추가로 개방할 것인지를 결정할 수 있고, 시위, 집회가 잦은 장소에서는 방어요원을 추가로 배치할 것인지 결정할 수 있다. 군중 밀집상태 카운팅은 일정 시간에 관심영역 내에서 분류된 모든 사람을 카운팅하는 방식이 이용될 수 있다.

[0102] 그리고, 이벤트 검출부(180)는 특이 행동 감지부를 포함할 수 있다. 특이 행동(Suspicious Behavior) 감지부는 예를 들어, 미끄러지거나 걸려서 넘어진 사람, 싸우고 있는 사람, 달리는 사람 등 특이 행동을 하는 사람을 감지할 수 있다.

[0103] 이러한 특이 행동 감지를 위해, 이벤트 검출부(180)는 딥러닝 분산 처리 장치(300)의 딥러닝 분석 정보와 객체 분류 정보를 활용할 수 있는 바, 딥러닝 분산 처리 장치(300)는 영상 정보의 신경망 학습을 통해, 미끄러지거나 쓰러짐 감지(Slip & Fall), 싸우는 사람 감지(Fighting), 달리는 사람 감지(Running) 등의 특정 행동에 대한 분류 처리가 가능할 수 있다.

[0104] 특히, 이벤트 검출부(180)는 미끄러지거나 걸려 넘어진 사람 감지를 통해 이벤트 발생을 처리하고, 감시 서비스 처리부(185)로 전달할 수 있는 바 이는 실버타운이나 요양원에서 고령자 모니터링에 효과적으로 이용될 수 있다. 또한, 감시 서비스 처리부(185)는 도움을 줄 수 있는 사람이 즉시 오지 않는다면 고령자는 넘어진 후 생명이 위험할 수 있으므로 이에 대응하는 사용자 단말(200) 또는 관제 서비스 서버(500)로의 알림 요청 정보 또는 관제 요청 정보를 전송할 수 있다.

[0105] 한편, 이벤트 검출부(180)는 카메라 무단 변경 감지부를 포함할 수 있다. 카메라 무단 변경(Camera Tampering) 감지부는, 제3자에 의한 카메라 케이블 단락, 렌즈 무단 조작에 의한 초점 흐려짐, 손이나 타물체로 카메라 렌즈를 가리는 경우, 또는 렌즈를 다른 방향으로 임의로 돌려 버리는 경우 등의 카메라 무단 변경을 감지할 수 있으며, 딥러닝 분산 처리 장치(300)는 카메라 무단 변경 감지를 위한 특정 상황별 영상 학습을 사전 처리하여 신경망 데이터로 구축할 수 있다.

[0107] 도 4는 본 발명의 실시 예에 따른 전체 시스템 동작을 설명하기 위한 래더 다이어그램이다.

[0108] 도 4를 참조하면, 본 발명의 실시 예에 따른 사용자 단말(200)는 지능형 보안 감시 장치(100) 및 관제 서비스 서버(500)에 사전 사용자 등록 처리를 수행한다(S101).

[0109] 사용자 등록 처리는, 예를 들어 지능형 보안 감시 장치(100)를 사용하는 관리자로서의 사용자 정보 및 휴대폰 정보 등록 처리 등이 예시될 수 있으며, 사용자 단말(200)은 지능형 보안 감시 장치(100)의 처리 정보 및 관제 서비스 서버(500)의 관제 서비스 처리 정보를 수신하여 출력하거나, 사용자 단말(200)의 입력 정보를 지능형 보안 감시 장치(100) 또는 관제 서비스 서버(500)로 전달하기 위한 입출력 장치로서, 컴퓨터, 스마트폰, 태블릿 PC, 네비게이션 등의 다양한 전자장치가 예시될 수 있다.

[0110] 그리고, 지능형 보안 감시 장치(100)는 하나 이상의 카메라 장치로부터 수집되는 영상 정보를 수집 및 안정화 처리한다(S103).

[0111] 이후, 지능형 보안 감시 장치(100)는 안정화 처리된 영상 정보의 배경 모델링 처리를 수행하며(S105), 배경 모델링 처리에 따라 배경 이미지가 차감된 전경 이진 데이터의 형태 요소 영역을 검출하는 형태 연산 처리를 수행하고(S107), 형태 요소 영역들을 객체 연결 영역으로 연결하여 라벨링하는 요소 연결 처리를 수행하며(S109), 객체 연결 영역들에 대응하는 객체 리스트를 구성하는 객체 추적 처리를 수행한다(S111).

[0112] 그리고, 지능형 보안 감시 장치(100)는, 상기와 같은 S103 내지 S111 단계의 초기 분석에 따라 획득된 영상 정보 내 객체 리스트를 포함하는 객체 추적 정보와, 상기 영상 정보를 딥러닝 분산 처리 요청 데이터로 가공하여, 딥러닝 분산 처리 장치(300)로 전달한다.

[0113] 이후, 딥러닝 분산 처리 장치(300)에서는 딥러닝 분산 처리 요청 데이터의 객체 추적 정보 및 영상 정보를 사전

구축된 신경망 데이터에 적용하여, 딥러닝 분석 기반의 객체 검출 처리를 수행하고(S115), 검출된 객체의 패턴 등을 식별하여 분류 처리를 수행한다(S117).

[0114] 그리고, 딥러닝 분산 처리 장치(300)는 딥러닝 기반 분석에 따른 객체 검출 정보 및 분류 정보를 지능형 보안 감시 장치(100)로 응답 처리한다(S119).

[0115] 여기서, 상기 객체 검출 정보 및 분류 정보는 전술한 이벤트 검출부(180)에서의 이벤트 검출에 이용되는 정보를 포함할 수 있으며, 예를 들어 트립 와이어를 통과하는 객체의 종류 및 패턴, 침입 감지한 객체의 종류 및 패턴, 배회객체의 종류 및 패턴, 통행방향위반 객체의 종류 및 패턴, 무단 방치물의 종류 및 패턴, 무단 이동물체의 종류 및 패턴, 출입 카운팅 및 통계 산출에 이용된 객체의 종류 및 패턴, 군중 밀집상태 감지의 근거가 되는 객체의 종류 및 패턴, 특이행동에 대응하는 객체의 종류 및 행동 패턴, 카메라 무단 변경 감지를 나타내는 객체의 종류 및 패턴 등의 다양한 검출 정보 및 분류 패턴 정보를 포함할 수 있다.

[0116] 객체 검출 정보 및 분류 정보와, 객체 추적 정보에 기초하여 지능형 보안 감시 장치(100)는 이벤트 검출을 판단한다(S123). 이벤트 검출 판단에는 전술한 센서 장치(700)의 센서 정보도 함께 이용될 수 있다.

[0117] 이벤트가 검출된 경우, 지능형 보안 감시 장치(100)는 사용자 단말(200)로 이벤트 알림 메시지를 전송하거나(S125), 또는 중계 서버(400)로 이벤트 검출 데이터를 전달할 수 있다(S127).

[0118] 한편, 딥러닝 분산 처리 장치(300)는 영상 분석 정보를 중계 서버(400)로 전달하여 사전 저장 및 관리 처리할 수 있는 바(S121), 이는 사용자 단말(200)로 이벤트 검출 데이터에 대응하는 딥러닝 영상 분석 정보를 제공하는 데 이용될 수 있다(S129).

[0119] 이에 따라, 사용자 단말(200)에서는 이벤트 알림 메시지와 함께, 딥러닝 기반의 해당 이벤트 분석 정보를 포함하는 알림 인터페이스가 출력될 수 있다(S131). 사용자는 이벤트의 종류에 따른 경계, 해제, 경보 등의 적절한 지능형 보안 감시 장치(100)의 처리 정보를 입력할 수 있으며(133), 입력된 처리 정보는 지능형 보안 감시 장치(100) 또는 관제 서비스 서버(500)로 전달될 수 있다.

[0120] 그리고, 지능형 보안 감시 장치(100)는 사용자 입력 정보에 따른 처리를 수행하고, 처리 결과 정보를 사용자 단말(200)로 전달한다(S135).

[0121] 한편, 중계 서버(400)는 지능형 보안 감시 장치(100) 또는 사용자 단말(200)의 사용자 입력에 따른 관제 서비스 요청 정보를 수신하고(S137), 수신된 요청 정보 및 이벤트 검출 데이터에 기반한 관제 서비스 요청을 사전 지정된 관제 서비스 서버(500)로 전송할 수 있다(S139).

[0122] 그리고, 관제 서비스 서버(500)에서는 관제 서비스 요청에 따른 지능형 보안 감시 장치(100) 위치로의 긴급출동 서비스, 화재 또는 침입 신고 서비스, 실시간 영상 모니터링 서비스, 주변 알림 서비스, 지능형 보안 감시 장치(100)의 제어 서비스 등의 관제 서비스를 처리하며(S141), 처리 결과 정보를 포함하는 관제 처리 데이터를 지능형 보안 감시 장치(100) 또는 사용자 단말(200)로 전송한다(S143, S145).

[0124] 도 5는 본 발명의 다른 일 실시 예에 따른 지능형 카메라 장치 기반 시스템을 설명하기 위한 개념도이며, 도 6은 본 발명의 실시 예에 따른 지능형 카메라 장치로 구현된 딥러닝 분석 시스템의 구성 및 연결관계를 보다 구체적으로 도시한 블록도이다.

[0125] 도 5 및 도 6을 참조하면, 본 발명의 다른 일 실시 예에 따른 지능형 보안 감시 장치(100)는, 보안 네트워크로 연결된 지능형 카메라 장치일 수 있으며, 카메라부(105)가 직접 내장된 형태의 보안 카메라로서 기능할 수 있다. 따라서 본 발명의 실시 예에 따른 지능형 보안 감시 장치(100)는 엣지 컴퓨팅을 수행하는 지능형 IP 카메라일 수 있는 바, 전술한 지능형 보안 감시 장치(100)의 영상 정보 안정화, 배경 모델링, 형태 연산 처리, 요소 연결 처리, 객체 추적, 시점 변환, 객체 분류 처리 및 이벤트 검출 처리 중 하나 이상을 수행하기 위한 분석 모듈을 구비하는 제1 지능형 카메라 장치(100) 일 수 있으며, 나머지 분석 모듈은 또 다른 제2 지능형 카메라 장치(300)로 분산되어 구비되어 있을 수 있다.

[0126] 특히, 제2 지능형 카메라 장치(300)는 별도의 카메라부(305)가 직접 내장된 형태의 또 다른 보안 카메라일 수도 있으며, 전술한 딥러닝 기반 영상 정보 분석부(310), 객체 검출부(320) 및 객체 분류 처리부(330)를 포함하는 딥러닝 분산 처리 장치(300)의 구성 중 적어도 하나를 포함할 수 있다.

[0127] 따라서, 본 발명의 실시 예에 따른 보안 감시 시스템은, 엣지 컴퓨팅을 수행하는 지능형 IP 카메라로서 제1 지

능형 카메라 장치(100) 및 제2 지능형 카메라 장치(300)를 포함하는 엣지 컴퓨팅 네트워크로 구축될 수 있는 바, 기존의 지능형 영상 감시 장치보다 정확도는 뛰어나면서도 컴퓨팅 네트워크의 구축 및 장비 비용은 최소화할 수 있는 보안 감시 네트워크를 구축할 수 있다.

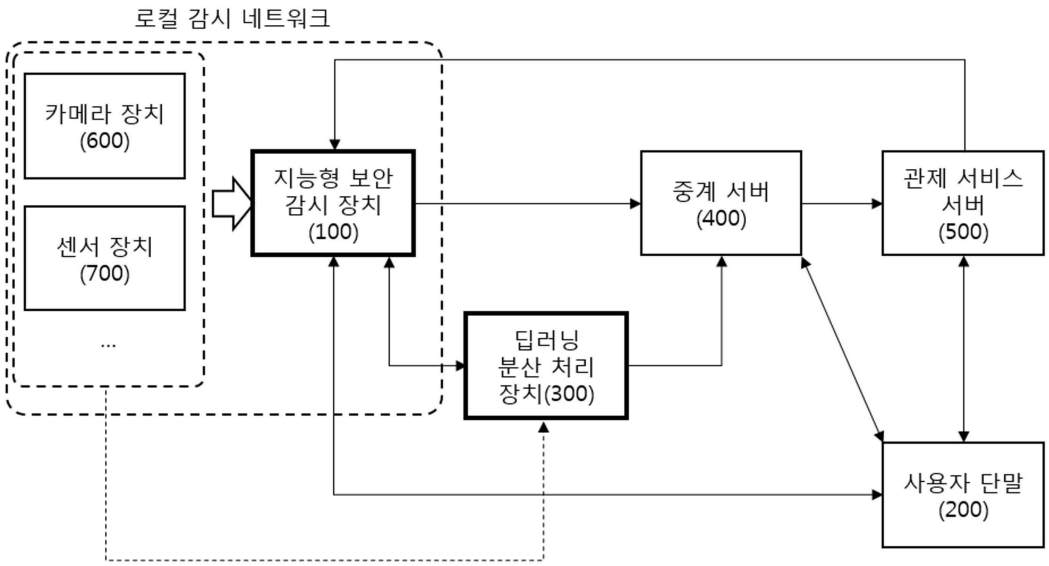
[0129] 상술한 본 발명에 따른 방법은 컴퓨터에서 실행되기 위한 프로그램으로 제작되어 컴퓨터가 읽을 수 있는 기록 매체에 저장될 수 있으며, 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장장치 등이 있다.

[0130] 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고, 상기 방법을 구현하기 위한 기능적인(function) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

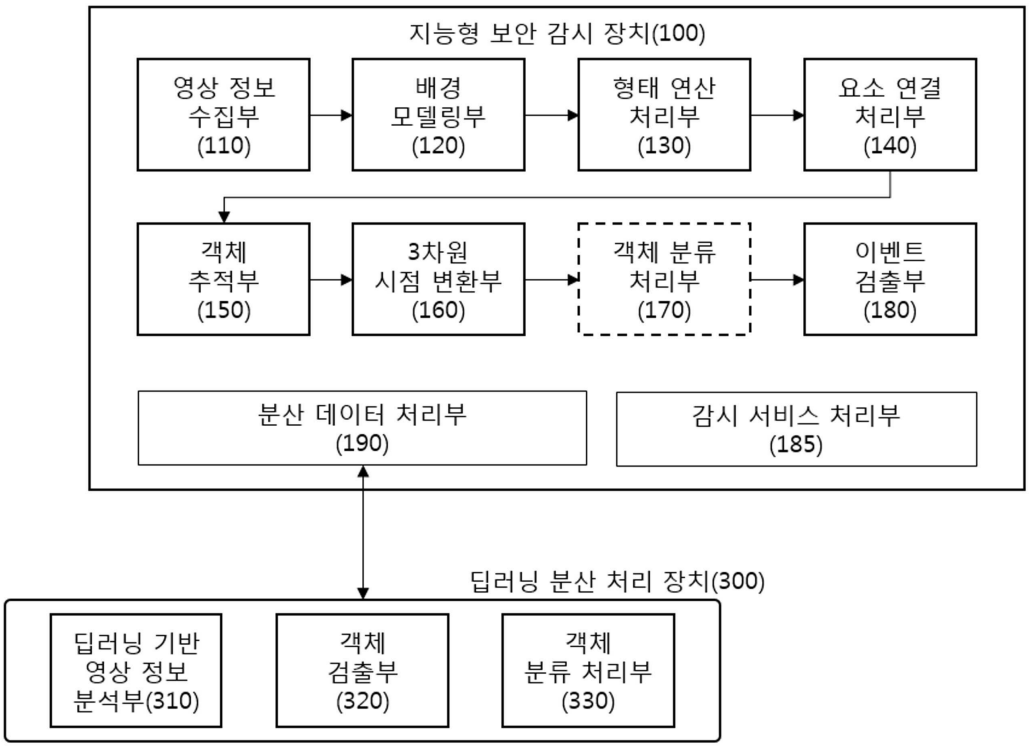
[0131] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형 실시가 가능한 것은 물론이고, 이러한 변형 실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어서는 안될 것이다.

도면

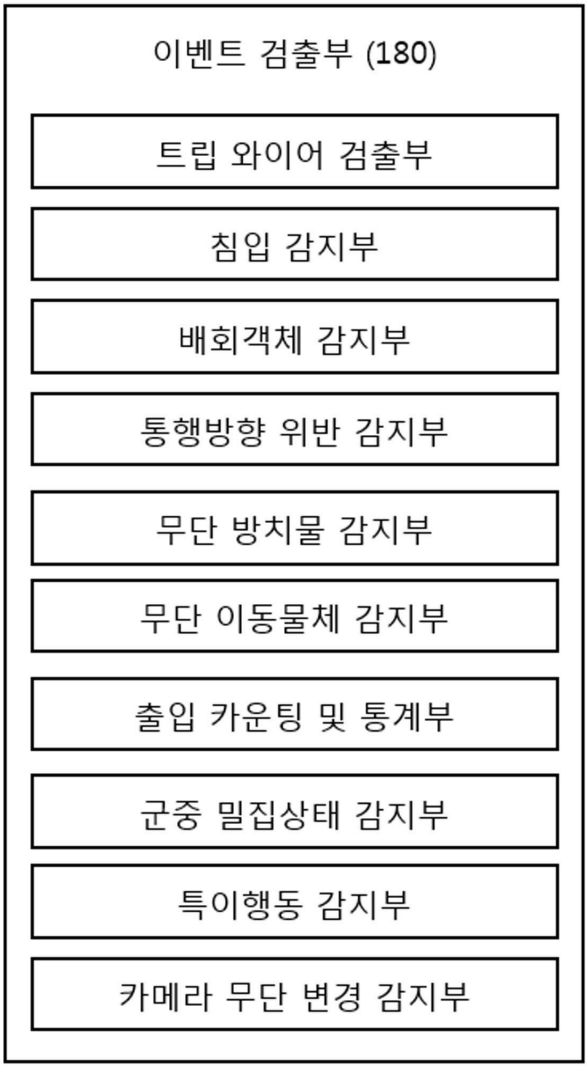
도면1



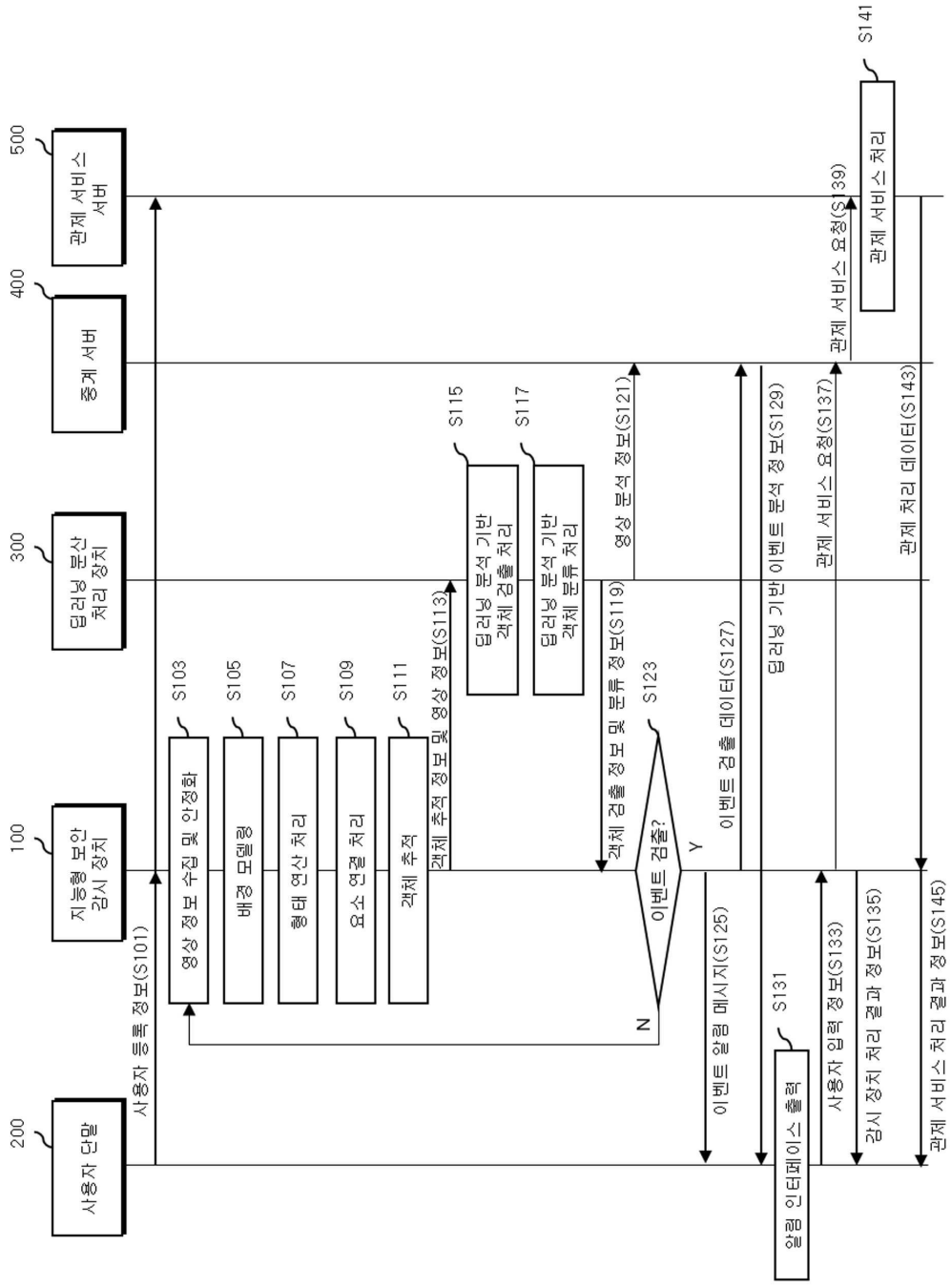
도면2


지능형 보안 감시 장치(100)
영상 정보 수집부 (110)
배경 모델링부 (120)
형태 연산 처리부 (130)
요소 연결 처리부 (140)
객체 추적부 (150)
3차원 시점 변환부 (160)
객체 분류 처리부 (170)
이벤트 검출부 (180)
분산 데이터 처리부 (190)
감시 서비스 처리부 (185)
딥러닝 분산 처리 장치(300)
딥러닝 기반 영상 정보 분석부(310)
객체 검출부 (320)
객체 분류 처리부 (330)

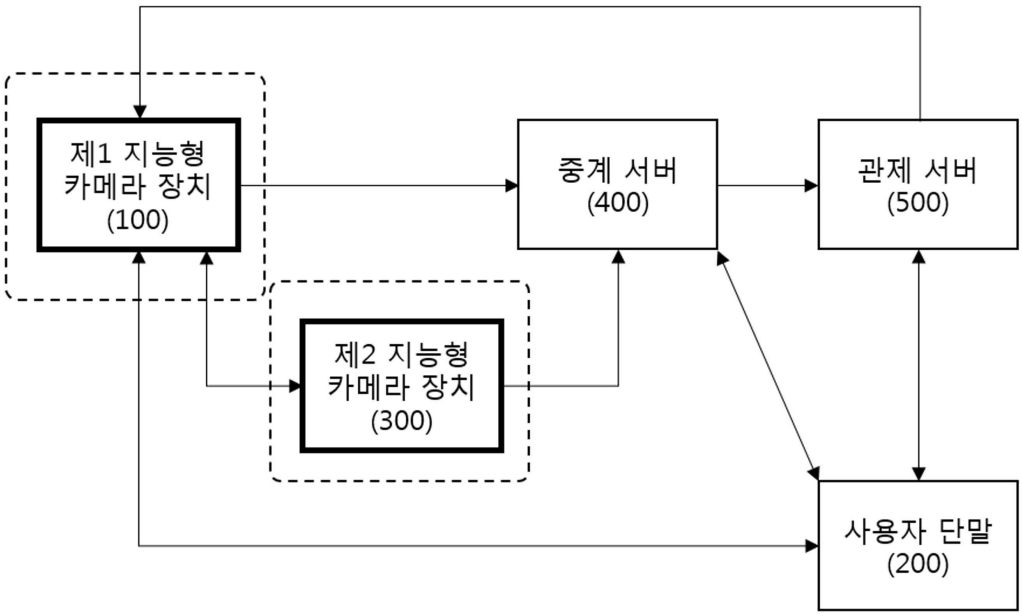
도면3


이벤트 검출부 (180)
트립 와이어 검출부
침입 감지부
배회객체 감지부
통행방향 위반 감지부
무단 방치물 감지부
무단 이동물체 감지부
출입 카운팅 및 통계부
군중 밀집상태 감지부
특이행동 감지부
카메라 무단 변경 감지부

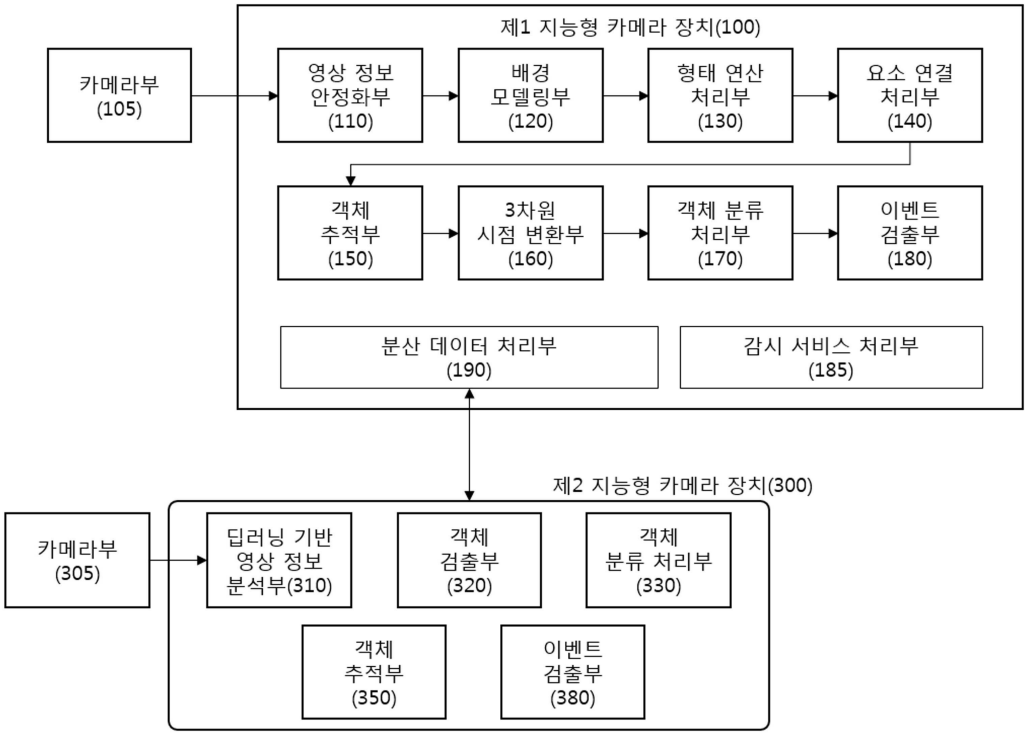
도면4


200
사용자 단말
100
지능형 보안 감시 장치
300
딥러닝 분산 처리 장치
400
중계 서버
500
관제 서비스 서버
사용자 등록 정보(S101)
S103
영상 정보 수집 및 안정화
S105
배경 모델링
S107
형태 연산 처리
S109
요소 연결 처리
S111
객체 추적
객체 추적 정보 및 영상 정보(S113)
S115
딥러닝 분석 기반 객체 검출 처리
S117
딥러닝 분석 기반 객체 분류 처리
영상 분석 정보(S121)
객체 검출 정보 및 분류 정보(S119)
S123
이벤트 검출?
N
Y
이벤트 검출 데이터(S127)
딥러닝 기반 이벤트 분석 정보(S129)
관제 서비스 요청(S139)
S141
관제 서비스 처리
관제 서비스 요청(S137)
관제 처리 데이터(S143)
이벤트 알림 메시지(S125)
S131
알림 인터페이스 출력
사용자 입력 정보(S133)
감시 장치 처리 결과 정보(S135)
관제 서비스 처리 결과 정보(S145)

도면5


제1 지능형
카메라 장치
(100)
중계 서버
(400)
관제 서버
(500)
제2 지능형
카메라 장치
(300)
사용자 단말
(200)

도면6


제1 지능형 카메라 장치(100)
카메라부
(105)
영상 정보
안정화부
(110)
배경
모델링부
(120)
형태 연산
처리부
(130)
요소 연결
처리부
(140)
객체
추적부
(150)
3차원
시점 변환부
(160)
객체 분류
처리부
(170)
이벤트
검출부
(180)
분산 데이터 처리부
(190)
감시 서비스 처리부
(185)
제2 지능형 카메라 장치(300)
카메라부
(305)
딥러닝 기반
영상 정보
분석부(310)
객체
검출부
(320)
객체
분류 처리부
(330)
객체
추적부
(350)
이벤트
검출부
(380)