(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년06월01일
(11) 등록번호 10-1626546
(24) 등록일자 2016년05월26일

(51) 국제특허분류(Int. Cl.)
H04N 7/18 (2006.01) *H04N 5/232* (2006.01)
H04N 5/262 (2006.01)
(52) CPC특허분류
H04N 7/18 (2013.01)
H04N 5/232 (2013.01)
(21) 출원번호 10-2015-0175134
(22) 출원일자 2015년12월09일
심사청구일자 2015년12월09일
(56) 선행기술조사문헌
JP10136247 A
KR1020120066393 A
JP10136247 A
KR1020120066393 A

(73) 특허권자
주식회사 베스트디지탈
경기도 의왕시 경수대로 209, 월드비젼아파트형공장 801호 (고천동)
(72) 발명자
박영석
경기도 안양시 동안구 경수대로883번길 33, 105동 2601호 (비산동,비산한화꿈에그린아파트)
박재용
경기도 안양시 동안구 시민대로159번길 62, 206동 1301호 (비산동,은하수벽산아파트)
(74) 대리인
전종학

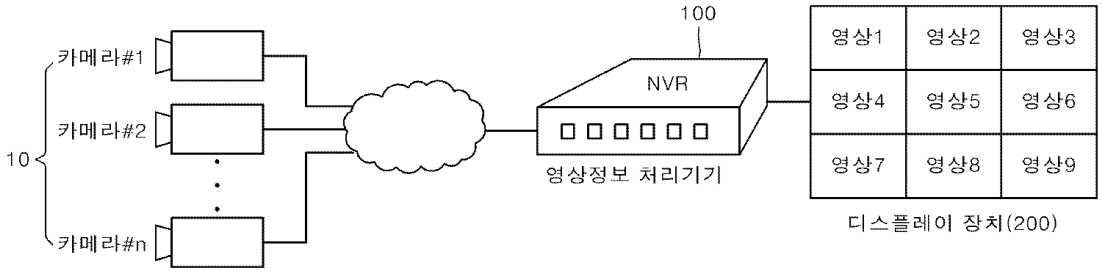
전체 청구항 수 : 총 7 항 심사관 : 박재학

(54) 발명의 명칭 **개인정보 보호를 지원하는 영상정보 처리기기 및 방법**

(57) 요 약

본 발명은 개인정보 보호를 지원하는 영상정보 처리기기 및 방법에 관한 것으로서, 더욱 상세히는 감시 카메라를 통해 촬영된 영상정보가 저장된 영상정보 처리기기로부터 외부로 영상을 제공해야 하는 경우 개인정보에 해당하는 부분을 처리하여 제공하거나 감시 카메라 운용시 미리 지정된 규칙에 따라 개인정보를 침해하지 않는 범위 내에서 운용되도록 유도하여 효과적으로 개인정보를 보호할 수 있는 개인정보 보호를 위한 영상정보 처리기기 및 방법에 관한 것이다. 본 발명은 영상정보를 통해 개인정보가 유출되지 않도록 영상정보에서 개인정보 보호가 필요한 객체를 마스킹 처리하여 제공함과 동시에 감시 카메라의 동작 범위에 따른 법률 위반 여부를 판단할 수 있도록 규칙을 설정하여 개인의 사생활 침해가 이루어지지 않는 범위에서 감시 카메라가 운용될 수 있도록 지원함으로써, 개인정보가 효과적으로 보호되도록 지원할 수 있는 효과가 있다.

대 표 도



(52) CPC특허분류
H04N 5/262 (2013.01)
H04N 7/181 (2013.01)

명 세 서

청구범위

청구항 1

하나 이상의 감시 카메라로부터 영상정보를 수신하고, 외부 장치와 네트워크를 통해 연결되는 통신부;

상기 영상 정보를 저장하는 저장부;

사용자 입력을 수신하는 인터페이스부;

개인정보 보호를 위한 미리 설정된 객체 관련 설정정보에 대응되어 상기 영상정보에 대한 영상 분석을 통해 개인정보 보호가 필요한 객체를 인식하고, 상기 영상 정보에서 상기 객체에 대응되는 영역을 마스킹 처리하여 마스킹 영상정보를 생성하는 영상 처리부; 및

상기 인터페이스부 또는 상기 통신부를 통해 상기 저장부에 저장된 영상정보를 전송하거나 재생하기 위한 제어신호 또는 상기 각 감시 카메라 중 적어도 하나를 제어하기 위한 동작정보 수신시 상기 제어신호에 따라 상기 영상 처리부를 통해 마스킹 처리된 상기 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하고, 개인정보 보호를 위해 상기 각 감시 카메라의 동작 범위가 설정되어 미리 저장된 규칙정보를 상기 동작정보에 따른 감시 카메라의 동작 상태와 비교하여 상기 동작 범위를 벗어나는 경우 알림정보를 출력하는 제어부를 포함하고,

상기 영상 처리부는 상기 영상정보에서 차분영상 방법, GMM(Gaussian Mixture Models)을 이용하는 MOG(Model of Gaussian) 알고리즘 또는 코드북(Codebook) 알고리즘을 이용한 객체와 배경을 분리하기 위한 배경 모델링을 통해 객체 후보 영역을 추출하고, 추출된 객체 후보 영역에서 HOG(histogram of oriented gradient), Harr-like 특징, Co-occurrence HOG, LBP(local binary pattern) 또는 FAST(features from accelerated segment test) 중에서 선택된 어느 하나의 객체 특징 추출 알고리즘을 이용하여 객체의 특징에 대한 객체 특징 정보를 생성한 후, 미리 설정된 객체 관련 설정정보와 비교하여 객체 관련 설정정보와 일치하거나 유사도가 미리 설정된 기준치 이상인 객체를 상기 개인정보 보호가 필요한 객체로 인식하며,

상기 제어부는 상기 영상정보의 접근권한에 대한 미리 설정된 권한 정보를 상기 인터페이스부를 통한 사용자 입력 또는 상기 통신부를 통해 외부 장치로부터 수신된 인증 정보와 비교하여 권한 인증시 상기 제어신호를 기초로 상기 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하고,

상기 제어신호와 동작 정보 중 적어도 하나와 이에 대응되는 상기 인증정보를 기초로 로그 정보를 생성하며, 해당 로그정보를 상기 저장부에 저장하는 로그정보 수집부를 더 포함하며,

상기 제어부는 상기 로그정보 수집부와 연동하여 인증되지 않은 사용자 또는 외부 장치에 의한 제어신호 또는 동작정보에 대한 로그정보가 생성되거나 상기 규칙정보에 따른 동작범위를 벗어나는 경우에 대응되는 동작정보에 대한 로그정보 생성시 해당 로그정보를 이벤트 정보로 상기 저장부에 저장하고, 상기 저장부에 저장된 이벤트 정보를 취합하여 이벤트 현황에 대한 통계정보를 생성하여 제공하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리기기.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 제어부는 상기 인증정보를 암호화 정보로 이용하며, 상기 영상정보 또는 마스킹 영상정보를 상기 암호화 정보를 기초로 암호화하여 상기 외부 장치로 전송하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리기기.

청구항 6

청구항 1에 있어서,

상기 제어부는 상기 동작 정보를 수신한 감시 카메라로부터 상기 동작 정보에 따라 변경된 현재의 상기 동작 상태에 대한 동작 상태 정보를 수신하고, 해당 동작 상태 정보를 상기 규칙정보에 따른 감시 카메라의 동작 범위와 비교하여 상기 동작 범위를 벗어나는지 여부를 판단하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리기기.

청구항 7

청구항 1에 있어서,

상기 제어부는 상기 저장부에 상기 마스킹 영상정보를 저장하기 위한 별도의 저장영역을 설정하여 상기 저장영역에 상기 마스킹 영상정보를 저장하며, 상기 제어 신호 수신시 상기 저장영역에 저장된 마스킹 영상정보를 제공하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리기기.

청구항 8

청구항 1에 있어서,

상기 동작 범위는 각 감시 카메라의 촬영 가능 영역, PTZ 동작 범위, 용도를 포함하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리기기.

청구항 9

청구항 1에 있어서,

상기 규칙정보는 감시 카메라별로 복수의 동작 범위 및 서로 다른 상기 동작 범위에 대응되어 서로 다른 알림정보가 설정되며,

상기 제어부는 상기 규칙정보와 동작 상태를 비교하여 상기 동작상태에 해당되는 동작 범위에 설정된 상기 알림정보를 상기 통신부에 연결되는 디스플레이 장치를 통해 출력하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리기기.

청구항 10

하나 이상의 감시 카메라와 네트워크를 통해 연결되어 각 감시 카메라의 영상정보를 수신하는 영상정보 처리기기의 개인 정보 보호를 위한 영상정보 처리 방법에 있어서,

하나 이상의 감시 카메라로부터 영상정보를 수신하여 저장하는 단계;

외부 장치로 상기 영상정보를 전송 또는 재생하기 위한 제어신호를 수신하는 경우 개인정보 보호를 위해 미리 설정된 객체 관련 설정정보에 대응되어 상기 영상정보에 대한 영상 분석을 통해 개인정보 보호가 필요한 객체를 인식하고, 상기 영상 정보에서 상기 객체에 대응되는 영역을 마스킹 처리하여 생성된 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하는 단계;

사용자 입력 또는 외부 장치로부터 상기 각 감시 카메라 중 적어도 하나를 제어하기 위한 동작정보 수신시 상기 개인정보 보호를 위해 상기 각 감시 카메라의 동작 범위가 설정되어 미리 저장된 규칙정보를 상기 동작정보에 따른 감시 카메라의 동작 상태와 비교하여 상기 규칙정보에 따른 동작 범위를 벗어나는 경우 알림정보를 출력하는 단계를 포함하고,

상기 개인정보 보호가 필요한 객체를 인식하는 것은 상기 영상정보에서 차분영상 방법, GMM(Gaussian Mixture Models)을 이용하는 MOG(Model of Gaussian) 알고리즘 또는 코드북(Codebook) 알고리즘을 이용한 객체와 배경을 분리하기 위한 배경 모델링을 통해 객체 후보 영역을 추출하고, 추출된 객체 후보 영역에서 HOG(histogram of oriented gradient), Harr-like 특징, Co-occurrence HOG, LBP(local binary pattern) 또는 FAST(features from accelerated segment test) 중에서 선택된 어느 하나의 객체 특징 추출 알고리즘을 이용하여 객체의 특징에 대한 객체 특징 정보를 생성한 후, 미리 설정된 객체 관련 설정정보와 비교하여 객체 관련 설정정보와 일치하거나 유사도가 미리 설정된 기준치 이상인 객체를 상기 개인정보 보호가 필요한 객체로 인식하는 과정을 통해 이루어지며,

상기 외부 장치로 전송하거나 재생하는 단계는 상기 영상정보의 접근권한에 대한 미리 설정된 권한 정보를 사용자 입력 또는 외부 장치로부터 수신된 인증 정보와 비교하여 권한 인증시 상기 제어신호를 기초로 상기 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하고,

상기 제어신호와 동작 정보 중 적어도 하나와 이에 대응되는 상기 인증정보를 기초로 로그 정보를 생성하되, 인증되지 않은 사용자 또는 외부 장치에 의한 제어신호 또는 동작정보에 대한 로그정보가 생성되거나 상기 규칙정보에 따른 동작범위를 벗어나는 경우에 대응되는 동작정보에 대한 로그정보 생성시 해당 로그정보를 이벤트 정보로 저장하고, 저장된 이벤트 정보를 취합하여 이벤트 현황에 대한 통계정보를 생성하여 제공하는 단계를 더 포함하는 것을 특징으로 하는 개인정보 보호를 지원하는 영상정보 처리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 개인정보 보호를 지원하는 영상정보 처리기기 및 방법에 관한 것으로서, 더욱 상세히는 감시 카메라를 통해 촬영된 영상정보가 저장된 영상정보 처리기기로부터 외부로 영상을 제공해야 하는 경우 개인정보에 해당하는 부분을 처리하여 제공하거나 감시 카메라 운용시 미리 지정된 규칙에 따라 개인정보를 침해하지 않는 범위 내에서 운용되도록 유도하여 효과적으로 개인정보를 보호할 수 있는 개인정보 보호를 위한 영상정보 처리기기 및 방법에 관한 것이다.

배 경 기 술

[0002] 현재 감시 카메라와 연결되어 영상정보를 관리하는 DVR이나 NVR과 같은 영상정보 처리기기의 지속적인 발전과 더불어 이를 포함하는 영상 관리 시스템이 다양한 장소에 적용되고 있으며, 고화질의 영상과 다양한 기능을 제공하고 있다.

[0003] 그러나, 이러한 영상 관리 시스템의 증가에 따라 개인이 지속적으로 다양한 감시 카메라에 노출되어 사생활을 침해당하는 경우가 빈번하게 발생하고 있으며, 감시 카메라를 통해 획득된 영상이 공유되는 과정에서 개인의 모습이 그대로 노출된 상태로 제공되어 개인정보에 대한 침해 사례가 급격히 증가하고 있다.

[0004] 이와 같은 영상을 통한 개인정보의 침해 사례를 방지하기 위해 현재 영상 관리 시스템의 운용을 개인정보 보호가 이루어지는 범위 내에서 제한하기 위한 법규정이 마련되어 있으며, 이러한 법규정의 일례로서 개인정보 보호법이나 영상정보 처리기기의 설치 및 운영과 관련된 가이드라인에 따르면 개인정보가 보호된 영상만 공유 또는 재생되도록 제한하고 있으며, 감시 카메라의 운용시 감시 카메라의 용도, 촬영 범위 등에 대한 동작 범위를 개인정보의 침해가 이루어지지 않는 범위 내로 제한하고 있다.

[0005] 그러나, 현재 영상 관리 시스템을 운용하는 관리자는 이러한 법규정을 대부분 인지하지 못하고 있으며, 이에 따라 개인정보가 그대로 드러난 영상이 외부로 유출되거나 감시 카메라의 운용시 사생활 침해가 발생할 우려가 있는 촬영 범위로 촬영하거나 PTZ 기능을 제한 없이 활용하는 등과 같은 개인정보의 침해에 따른 불법 행위가 지속적으로 발생하고 있다.

[0006] 따라서, 이러한 불법 행위를 방지하고, 개인정보를 안전하고 보호할 수 있도록 하기 위한 대안이 요구되고

있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국공개특허 제10-2009-0084633호

발명의 내용

해결하려는 과제

[0008] 본 발명은 감시 카메라를 통해 촬영된 영상을 저장하는 영상정보 처리기기로부터 해당 영상을 외부 장치로 전송하거나 영상정보 처리기기에서 해당 영상을 재생해야 하는 경우 상기 영상에 포함된 개인정보를 보호한 상태에서 전송 또는 재생되도록 함으로써 개인정보를 효과적으로 보호하는데 그 목적이 있다.

[0009] 또한, 본 발명은 감시 카메라의 운용시 개인정보 보호가 이루어지는 범위 내에서 감시 카메라의 동작을 제한하기 위한 규칙을 설정하고, 해당 규칙을 벗어나는 감시 카메라의 동작시 불법임을 관리자가 인지할 수 있도록 명시하여, 개인 정보 보호가 이루어지는 범위 내에서 감시 카메라를 운용할 수 있도록 제공함으로써 개인정보를 효과적으로 보호하는데 그 목적이 있다.

[0010] 더하여, 본 발명은 감시 카메라의 운용에 따른 로그를 기록하고, 이러한 로그를 기초로 불법이 발생한 시점을 파악하여 책임소재를 추적할 수 있도록 지원하는 동시에 감시 카메라의 운용이 불법적으로 이루어지지 않도록 사전에 방지하여 개인정보를 효과적으로 보호하는데 그 목적이 있다.

과제의 해결 수단

[0011] 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기는 하나 이상의 감시 카메라로부터 영상정보를 수신하고, 외부 장치와 네트워크를 통해 연결되는 통신부와, 상기 영상 정보를 저장하는 저장부와, 사용자 입력을 수신하는 인터페이스부와, 개인정보 보호를 위한 미리 설정된 객체 관련 설정정보에 대응되어 상기 영상정보에 대한 영상 분석을 통해 상기 객체를 인식하고, 상기 영상 정보에서 상기 객체에 대응되는 영역을 마스킹 처리하여 마스킹 영상정보를 생성하는 영상 처리부 및 상기 인터페이스부 또는 상기 통신부를 통해 상기 저장부에 저장된 영상정보를 전송하거나 재생하기 위한 제어신호 또는 상기 각 감시 카메라 중 적어도 하나를 제어하기 위한 동작정보 수신시 상기 제어신호에 따라 상기 영상 처리부를 통해 마스킹 처리된 상기 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하고, 개인정보 보호를 위해 상기 각 감시 카메라의 동작 범위가 설정되어 미리 저장된 규칙정보를 상기 동작정보에 따른 감시 카메라의 동작 상태와 비교하여 상기 동작 범위를 벗어나는 경우 알림정보를 출력하는 제어부를 포함할 수 있다.

[0012] 본 발명과 관련된 일 예로서, 상기 제어부는 상기 영상정보의 접근권한에 대한 미리 설정된 권한 정보를 상기 인터페이스부를 통한 사용자 입력 또는 상기 통신부를 통해 외부 장치로부터 수신된 인증 정보와 비교하여 권한 인증시 상기 제어신호를 기초로 상기 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하는 것을 특징으로 할 수 있다.

[0013] 본 발명과 관련된 일 예로서, 상기 영상정보 처리기기는 상기 제어신호와 동작 정보 중 적어도 하나와 이에 대응되는 상기 인증정보를 기초로 로그 정보를 생성하며, 해당 로그정보를 상기 저장부에 저장하는 로그정보 수집부를 더 포함하는 것을 특징으로 할 수 있다.

[0014] 본 발명과 관련된 일 예로서, 상기 제어부는 상기 로그정보 수집부와 연동하여 인증되지 않은 사용자 또는 외부 장치에 의한 제어신호 또는 동작정보에 대한 로그정보가 생성되거나 상기 규칙정보에 따른 동작범위를 벗어나는 경우에 대응되는 동작정보에 대한 로그정보 생성시 해당 로그정보를 이벤트 정보로 상기 저장부에 저장하고, 상기 저장부에 저장된 이벤트 정보를 취합하여 이벤트 현황에 대한 통계정보를 생성하여 제공하는 것을 특징으로 할 수 있다.

[0015] 본 발명과 관련된 일 예로서, 상기 제어부는 상기 인증정보를 암호화 정보로 이용하며, 상기 영상정보 또는 마스킹 영상정보를 상기 암호화 정보를 기초로 암호화하여 상기 외부 장치로 전송하는 것을 특징으로 할 수 있다.

[0016] 본 발명과 관련된 일 예로서, 상기 제어부는 상기 동작 정보를 수신한 감시 카메라로부터 상기 동작 정보에 따라 변경된 현재의 상기 동작 상태에 대한 동작 상태 정보를 수신하고, 해당 동작 상태 정보를 상기 규칙정보에 따른 감시 카메라의 동작 범위와 비교하여 상기 동작 범위를 벗어나는지 여부를 판단하는 것을 특징으로 할 수 있다.

[0017] 본 발명과 관련된 일 예로서, 상기 제어부는 상기 저장부에 상기 마스킹 영상정보를 저장하기 위한 별도의 저장영역을 설정하여 상기 저장영역에 상기 마스킹 영상정보를 저장하며, 상기 제어 신호 수신시 상기 저장영역에 저장된 마스킹 영상정보를 제공하는 것을 특징으로 할 수 있다.

[0018] 본 발명과 관련된 일 예로서, 상기 동작 범위는 각 감시 카메라의 촬영 가능 영역, PTZ 동작 범위, 용도를 포함하는 것을 특징으로 할 수 있다.

[0019] 본 발명과 관련된 일 예로서, 상기 규칙정보는 감시 카메라별로 복수의 동작 범위 및 서로 다른 상기 동작 범위에 대응되어 서로 다른 알림정보가 설정되며, 상기 제어부는 상기 규칙정보와 동작 상태를 비교하여 상기 동작 상태에 해당되는 동작 범위에 설정된 상기 알림정보를 상기 통신부에 연결되는 디스플레이 장치를 통해 출력하는 것을 특징으로 할 수 있다.

[0020] 본 발명의 실시예에 따른 하나 이상의 감시 카메라와 네트워크를 통해 연결되어 각 감시 카메라의 영상정보를 수신하는 영상정보 처리기기의 개인 정보 보호를 위한 영상정보 처리 방법은, 하나 이상의 감시 카메라로부터 영상정보를 수신하여 저장하는 단계와, 외부 장치로 상기 영상정보를 전송 또는 재생하기 위한 제어신호를 수신하는 경우 개인정보 보호를 위해 미리 설정된 객체 관련 설정정보에 대응되어 상기 영상정보에 대한 영상 분석을 통해 상기 객체를 인식하고, 상기 영상 정보에서 상기 객체에 대응되는 영역을 마스킹 처리하여 생성된 마스킹 영상정보를 상기 외부 장치로 전송하거나 재생하는 단계 및 사용자 입력 또는 외부 장치로부터 상기 각 감시 카메라 중 적어도 하나를 제어하기 위한 동작정보 수신시 상기 개인정보 보호를 위해 상기 각 감시 카메라의 동작 범위가 설정되어 미리 저장된 규칙정보를 상기 동작정보에 따른 감시 카메라의 동작 상태와 비교하여 상기 규칙정보에 따른 동작 범위를 벗어나는 경우 알림정보를 출력하는 단계를 포함할 수 있다.

발명의 효과

[0021] 본 발명은 영상정보를 통해 개인정보가 유출되지 않도록 영상정보에서 개인정보 보호가 필요한 객체를 마스킹 처리하여 제공함과 동시에 감시 카메라의 동작 범위에 따른 법률 위반 여부를 판단할 수 있도록 규칙을 설정하여 개인의 사생활 침해가 이루어지지 않는 범위에서 감시 카메라가 운용될 수 있도록 지원함으로써, 개인정보가 효과적으로 보호되도록 지원할 수 있는 효과가 있다.

[0022] 또한, 본 발명은 감시 카메라의 운용에 따른 로그를 기록하고, 이러한 로그를 기초로 불법이 발생한 시점 및 불법 운용 대상을 파악하여 책임소재를 추적할 수 있도록 지원함으로써, 감시 카메라의 운용이 불법적으로 이루어지지 않도록 사전에 방지하여 개인정보를 효과적으로 보호할 수 있는 효과가 있다.

[0023] 더하여, 본 발명은 감시 카메라를 통해 촬영된 영상정보의 반출시 해당 영상정보를 암호화하여 제공함으로써, 상기 영상정보에 대한 접근권한이 있는 사용자에 한해 상기 영상정보에 접근할 수 있도록 제한할 수 있으며, 이를 통해 영상정보 관리에 대한 보안성을 높일 수 있는 효과가 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상 관리 시스템의 구성도.

도 2는 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기의 상세 구성도.

도 3 및 도 4는 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기의 영상정보에 포함된 개인정보 보호처리에 대한 동작 예시도

도 5는 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기의 영상정보 반출시 암호화 처리에 대한 동작 예시도.

도 6은 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기의 감시 카메라 운용시 불법 여부 판단 및 불법 여부에 대한 알림 동작에 대한 예시도.

도 7은 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기에서 로그정보를 기초로 생성한

통계정보에 대한 예시도.

도 8은 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리 방법에 대한 순서도.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 도면을 참고하여 본 발명의 상세 실시예를 설명한다.

[0026] 우선, 도 1은 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상 관리 시스템의 구성도로서, 도시된 바와 같이 하나 이상의 감시 카메라(10)와 유무선 네트워크(통신망)를 통해 연결되는 영상정보 처리기기(100)를 포함하며, 상기 영상정보 처리기기(100)는 상기 각 감시 카메라(10)의 영상을 수신하여 저장하고, 상기 영상정보 처리기기(100)와 연결되는 디스플레이 장치(200)를 통해 각 감시 카메라(10)의 영상을 출력할 수 있다.

[0027] 이때, 상기 디스플레이 장치(200)는 멀티 스크린으로 구성될 수 있으며, 상기 영상정보 처리기기(100)는 스크린별로 서로 다른 감시 카메라(10)의 영상을 실시간으로 동시에 출력할 수 있다.

[0028] 또한, 상기 감시 카메라는 IP(Internet Protocol) 카메라, CCTV(closed circuit television) 카메라 등과 같은 다양한 카메라가 적용될 수 있다.

[0029] 또한, 상기 영상정보 처리기기(100)는 NVR(Network Video Recorder) 또는 DVR(Digital Video Recorder)로 구성될 수 있으며, 상기 네트워크를 통해 외부 장치(300)와 상호 통신할 수도 있다.

[0030] 또한, 상기 외부 장치(300)는 상기 네트워크를 통해 상기 영상정보 처리기기(100)와 연결되어 통신하는 서버, PC, NVR, DVR 등과 같은 다양한 원격 외부 장치를 포함할 수 있으며, 상기 영상정보 처리기기(100)에 구성된 인터페이스를 통해 직접 연결되는 USB, 외장 HDD(Hard Disk Drive) 등과 같은 다양한 플러그인 장치(plug-in unit)을 포함할 수 있다.

[0031] 이때, 상기 디스플레이 장치(200)는 상기 외부 장치(300)에 포함될 수도 있다.

[0032] 또한, 상기 유무선 네트워크는 TCP/IP(Transfer control protocol/Internet protocol)를 비롯한 널리 알려진 다양한 유무선 통신방식이 적용될 수 있다.

[0033] 상술한 구성에서, 상기 영상정보 처리기기(100)는 상기 각 감시 카메라(10)로부터 수신되는 영상정보를 로우 데이터(Raw Data)로 저장할 수 있으며, 외부 장치(300)에 대한 상기 영상정보의 전송이나 상기 디스플레이 장치(200)를 통한 상기 영상정보의 재생을 수행할 수 있다.

[0034] 그러나, 상기 영상정보를 그대로 전송하거나 재생하는 경우 상기 영상정보에 포함된 개인의 영상이 그대로 노출된 상태로 제공되므로 개인정보 보호와 관련된 법률에 저촉될 수 있다.

[0035] 이를 방지하기 위하여, 상기 영상정보 처리기기(100)는 상기 영상정보의 전송이나 재생시 상기 영상정보에 포함된 객체 중 개인정보 보호가 필요한 객체를 마스킹(masking) 처리하여 제공함으로써, 영상을 통해 개인정보가 유출되지 않도록 보호할 수 있다.

[0036] 한편, 상기 감시 카메라(10)의 동작 제어시 개인의 사생활 침해와 같은 개인정보의 침해가 우려되는 감시 영역이 존재할 수 있으며, 이로 인해 상술한 바와 같이 개인정보 보호 및 감시 카메라(10) 운용과 관련된 법률에 저촉될 수 있다.

[0037] 이를 방지하기 위해, 상기 영상정보 처리기기(100)는 상기 각 감시 카메라(10)의 동작 제어와 관련되어 개인정보 보호를 위한 동작 범위가 규칙정보로서 상기 영상정보 처리기기(100)에 설정될 수 있으며, 상기 감시 카메라(10)의 동작 제어시 상기 동작 제어와 관련된 동작정보를 상기 규칙정보와 비교하여, 상기 동작정보에 따른 감시 카메라의 동작 상태가 상기 규칙정보에 따른 불법에 해당되는 동작범위에 속하는 경우 법률 위반에 대한 알림정보를 생성하여 출력할 수 있다.

[0038] 이때, 상기 영상정보 처리기기(100)는 상기 디스플레이 장치(200) 또는 상기 영상정보 처리기기(100)와 연결된 다양한 출력 장치를 통해 상기 알림정보를 출력할 수 있으며, 자체적으로 상기 알림정보에 따른 경고신호를 출력할 수도 있다.

[0039] 이를 통해, 상기 영상정보 처리기기(100)는 관리자가 감시 카메라(10)의 운용시 법률 위반 여부를 용이하게 판단할 수 있도록 지원하며, 이에 따라 관리자는 법률 위반이 이루어지지 않는 범위 내에서 감시 카메라(10)를 운용할 수 있다.

[0040] 상술한 바와 같이, 본 발명은 영상정보를 통해 개인정보가 유출되지 않도록 마스킹 처리하여 제공함과 동시에 감시 카메라(10)의 동작 범위에 따른 법률 위반 여부를 판단할 수 있도록 규칙을 설정하여 개인의 사생활 침해가 이루어지지 않는 범위에서 감시 카메라(10)가 운용될 수 있도록 지원함으로써 개인정보가 효과적으로 보호되도록 지원할 수 있다.

[0041] 이하, 상술한 구성을 바탕으로 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기(100)의 상세 구성 및 동작을 설명한다.

[0042] 도 2는 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기(100)의 상세 구성도로서, 도시된 바와 같이 통신부(110), 저장부(120), 영상 처리부(130), 로그정보 수집부(140), 인터페이스부(160) 및 제어부(150)를 포함할 수 있다.

[0043] 우선, 상기 통신부(110)는 상기 각 감시 카메라(10)와 네트워크를 통해 연결되어 유무선 통신을 수행할 수 있으며, 상기 각 감시 카메라(10)의 영상정보를 수신할 수 있다.

[0044] 또한, 상기 통신부(110)는 상기 외부 장치(300) 중 플러그인 장치, 디스플레이 장치(200)와 같은 로컬 외부 장치와의 연결을 지원하여 로컬 외부 장치와 통신할 수 있으며, 상기 외부 장치(300) 중 네트워크를 통해 연결되는 원격 외부 장치와 통신을 수행할 수 있다. 이때, 상기 통신부(110)는 상기 로컬 외부 장치 및 원격 외부 장치와의 통신을 지원하는 통신 인터페이스(interface)가 구성될 수 있다.

[0045] 또한, 상기 저장부(120)는 상기 영상정보를 저장할 수 있으며, 다양한 종류의 메모리 및 저장매체가 적용될 수 있다.

[0046] 또한, 상기 영상 처리부(130)는 개인정보 보호를 위한 객체 관련 설정정보가 미리 설정되며, 상기 영상정보에서 상기 설정정보에 따른 객체를 영상 분석을 통해 인식(식별)하고, 상기 영상정보에서 인식된 객체에 대응되는 영역을 마스킹 처리하여 마스킹 영상정보를 생성할 수 있다.

[0047] 이때, 마스킹 처리 과정의 상세 실시예로서, 상기 영상 처리부(130)는 상기 영상정보에서 차분영상 방법, GMM(Gaussian Mixture Models)을 이용하는 MOG(Model of Gaussian) 알고리즘, 코드북(Codebook) 알고리즘 등과 같은 객체와 배경을 분리하기 위한 배경 모델링을 통해 객체에 해당하는 객체 후보 영역을 추출할 수 있다.

[0048] 또한, 상기 영상 처리부(130)는 상기 영상 정보에서 추출된 해당 객체 후보 영역에서 HOG(histogram of oriented gradient), Harr-like 특징, Co-occurrence HOG, LBP(local binary pattern), FAST(features from accelerated segment test) 등과 같은 객체 특징 추출 알고리즘을 이용하여 객체의 특징에 대한 객체 특징 정보를 생성한 후 미리 설정된 객체 관련 설정정보와 비교하여, 객체 관련 설정정보와 일치하거나 유사도가 미리 설정된 기준치 이상인 객체를 개인정보 보호가 필요한 객체로 인식할 수 있다.

[0049] 이후, 상기 영상 처리부(130)는 상기 영상정보에서 인식된 객체에 대한 객체 후보 영역을 블라인드(blind), 블러(blur) 등과 같은 마스킹 기법으로 마스킹 처리하여 상기 마스킹 영상정보를 생성할 수 있다.

[0050] 이때, 상기 영상 처리부(130)는 상기 영상정보에서 이동하는 객체에 대하여 칼만필터와 같은 객체 추적 알고리즘을 이용하여 객체를 추적하면서 영상정보의 각 프레임에서 객체에 해당하는 영역을 마스킹 처리할 수도 있다.

[0051] 더하여, 상기 인터페이스부(160)는 사용자 입력을 직접 수신하여 사용자 입력에 따른 제어신호를 생성하거나, 사용자 입력에 대한 입력정보를 생성하는 키보드, 조이스틱과 같은 입력 장치와의 연결되어 사용자 입력에 따른 제어신호를 수신할 수 있다.

[0052] 한편, 상기 제어부(150)는 상기 통신부(110)를 통해 수신된 영상정보를 상기 저장부(120)에 저장하고, 상기 인터페이스부(160)를 통한 사용자 입력에 따라 상기 통신부(110)에 연결되는 외부 장치(300)에 상기 저장부(120)에 저장된 영상 정보를 전송하거나 상기 디스플레이 장치(200)를 통해 상기 영상정보를 재생하기 위한 제어 신호를 수신한 경우 상기 영상 처리부(130)를 통해 상기 영상정보를 마스킹 처리하여 마스킹 영상정보를 생성하고, 이를 상기 외부 장치(300)로 전송하거나 재생할 수 있다.

[0053] 이를 통해, 상기 제어부(150)는 상기 영상정보에 포함된 개인정보가 노출되지 않도록 하여 개인정보를 효과적으로 보호할 수 있다.

[0054] 또한, 상기 제어부(150)는 상기 통신부(110)를 통해 연결되는 외부 장치(300)로 상기 영상정보를 전송하는 경우에도 상기 영상 처리부(130)를 통해 마스킹 처리된 마스킹 영상정보를 전송할 수 있으며, 이에 따라 영상정보의

반출시 개인정보가 노출되지 않도록 방지할 수 있다.

[0055] 더하여, 상기 제어부(150)에는 개인정보 보호를 위해 상기 각 감시 카메라(10)의 개인 정보 보호를 위한 동작 범위에 대한 규칙정보가 미리 설정될 수 있다.

[0056] 일례로, 상기 규칙정보는 개인정보의 침해가 발생하지 않는 감시 카메라(10)별 적법한 동작범위와, 개인정보의 침해가 발생되는 감시 카메라(10)별 불법한 동작범위에 대한 정보가 포함될 수 있다.

[0057] 또한, 상기 제어부(150)는 상기 인터페이스부(160)를 통한 사용자 입력을 기초로 상기 각 감시 카메라(10)의 동작을 제어하기 위한 동작정보를 생성하여 상기 통신부(110)를 통해 사용자가 선택한 감시 카메라(10)로 전송할 수 있으며, 상기 통신부(110)를 통해 상기 외부 장치(300)가 감시 카메라(10)의 제어를 위해 생성한 동작정보를 수신할 수도 있다.

[0058] 이에 따라, 상기 제어부(150)는 상기 동작정보의 생성 또는 수신시 상기 동작정보에 따른 감시 카메라의 동작 상태를 상기 규칙정보와 비교하여 상기 동작정보에 따른 동작 상태가 상기 규칙정보에 따른 불법에 해당하는 동작 범위에 속하거나 적법한 동작 범위를 벗어나는 경우 상기 디스플레이 장치(200)를 통해 개인정보의 노출 위험에 대한 알림정보(경고 정보)를 출력할 수 있으며, 이를 통해 관리자의 감시 카메라(10) 운용시 적법한 동작 범위를 벗어나지 않도록 지원 및 유도할 수 있다.

[0059] 이때, 상기 제어부(150)는 상기 통신부(110)를 통해 상기 각 감시 카메라(10)로부터 상기 동작정보에 따라 동작한 결과인 현재 동작 상태에 대한 동작 상태 정보를 수신하여, 상기 동작 상태 정보를 기초로 각 감시 카메라(10)의 동작 상태를 판단할 수 있다.

[0060] 또한, 상기 제어부(150)는 감시 카메라(10)별로 최근 동작 상태를 기록하여 동작 상태 정보로 저장하고, 상기 인터페이스부(160)를 통한 사용자 입력에 따라 동작 정보를 수신하거나 상기 통신부(110)를 통해 외부 장치로부터 동작 정보 수신시 상기 최근 동작 상태에 상기 동작 정보를 적용 및 연산하여 기존 동작 상태 정보를 갱신할 수 있으며, 갱신된 동작 상태 정보를 기초로 상기 동작 정보에 대응되는 감시 카메라(10)의 현재 동작 상태를 판단할 수 있다.

[0061] 또한, 상기 동작정보는 상기 감시 카메라(10)의 PTZ 제어(PTZ 제어 수치)나 사용자에 의해 설정된 촬영 영역으로의 변경, 촬영모드 변경(일례로, 적외선 모드, 가시광 모드 등)과 같은 동작 제어에 대한 정보일 수 있으며, 상기 동작 상태 정보는 상기 PTZ 제어에 따른 PAN, TILT, ZOOM 각각에 대한 설정수치, 상기 촬영 영역 변경에 따른 현재 촬영 영역에 대한 정보, 상기 촬영모드 변경에 따른 현재 촬영모드에 대한 정보 등에 대한 정보를 포함할 수 있다.

[0062] 이에 따라, 상기 제어부(150)는 상기 감시 카메라(10)의 운용시 발생할 수 있는 개인정보 침해를 사전에 방지할 수 있다.

[0063] 한편, 상기 로그정보 수집부(140)는 상기 제어부(150)와 연동하여 각 감시 카메라(10)의 동작 제어 및 영상정보의 재생이나 전송과 관련된 제어신호를 수집하고, 해당 동작정보 및 제어신호를 로그정보로 생성할 수 있으며, 이를 상기 저장부(120)에 저장할 수 있다.

[0064] 이를 통해, 상기 영상정보 처리기기(100)는 감시 카메라(10)의 조작이나 영상정보의 관리 내역에 대한 기록을 로그정보로 저장하고, 이를 기초로 불법이 발생한 시점이나 불법 발생 대상에 대한 정보를 제공할 수 있는데, 이는 이하에서 상세히 설명한다.

[0065] 한편, 상술한 구성을 토대로 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기(100)의 동작 구성을 이하 도면을 통해 상세히 설명한다.

[0066] 도 3은 본 발명의 실시예에 따른 개인정보 보호를 지원하는 영상정보 처리기기(100)의 영상정보에 포함된 개인정보 보호처리에 대한 동작 예시도로서, 도시된 바와 같이 상기 제어부(150)는 상기 통신부(110)를 통해 외부 장치(300) 및 디스플레이 장치(200)와 통신할 수 있다.

[0067] 또한, 상기 제어부(150)는 상기 영상정보에 포함된 개인정보의 노출을 방지하기 위하여, 상기 영상 처리부(130)를 제어하여 상기 저장부(120)에 저장된 영상정보에서 상기 객체 관련 설정정보에 따라 인식된 객체를 마스킹 처리할 수 있으며, 이를 통해 마스킹 영상정보를 생성하여 상기 저장부(120)에 저장되도록 할 수 있다.

[0068] 이때, 상기 제어부(150)는 상기 저장부(120)에 마스킹 영상정보를 저장하기 위한 별도의 저장영역을 설정하고, 상기 영상 처리부(130)와 연동하여 상기 저장부(120)에 설정된 저장영역에 상기 마스킹 영상정보가 저장되도록

할 수 있다.

[0069] 이에 따라, 상기 제어부(150)는 사용자가 선택한 영상정보를 상기 디스플레이 장치(200)를 통해 재생하거나 상기 외부 장치(300)로 전송하고자 하는 경우 상기 저장부(120)에 저장된 영상정보 중 상기 인터페이스부(160)를 통해 수신된 사용자 입력에 따른 제어 신호를 기초로 사용자에 의해 선택된 영상정보에 대응되는 마스킹 영상정보를 상기 저장부(120)에 설정된 상기 저장영역으로부터 추출하여 상기 디스플레이 장치(200)를 통해 재생하거나 상기 외부 장치(300)로 전송할 수 있다.

[0070] 또한, 상기 제어부(150)는 상기 통신부(110)를 통해 상기 외부 장치(300)로부터 상기 제어 신호를 수신할 수도 있으며, 상기 제어신호를 기초로 외부 장치(300)에 의해 선택된 영상정보에 대응되는 마스킹 영상정보를 상기 저장영역으로부터 추출하여 상기 제어 신호를 전송한 외부 장치(300)로 전송할 수 있다.

[0071] 이를 통해, 상기 제어부(150)는 상기 영상정보에서 개인정보에 해당하는 객체를 마스킹 처리하여 개인정보가 노출되지 않도록 방지할 수 있다.

[0072] 이때, 도 4에 도시된 바와 같이 상기 제어부(150)는 상기 영상 처리부(130)와 연동하여 상기 영상 처리부(130)에 설정된 설정정보에 따라 자동으로 개인정보에 해당하는 객체에 마스킹 처리가 이루어지도록 하거나, 상기 인터페이스부(160)를 통한 사용자 입력을 기초로 상기 영상 처리부(130)를 제어하여 사용자가 원하는 영역에 대한 마스킹 처리를 수동으로 수행할 수도 있다.

[0073] 한편, 본 발명의 실시예에 따른 영상정보 처리기기(100)는 영상정보 또는 마스킹 영상정보 제공시 인증된 사용자 또는 외부 장치(300)에 한해 해당 영상정보 또는 마스킹 영상정보를 제공하고, 인증된 사용자 또는 외부 장치(300)에 한해 상기 영상정보 또는 마스킹 영상정보에 접근할 수 있도록 상기 영상정보 또는 마스킹 영상정보를 암호화하여 제공함으로써 보안성을 높일 수 있는데 이를 도 5를 통해 상세히 설명한다.

[0074] 도 5에 도시된 바와 같이, 상기 영상정보 처리기기(100)의 제어부(150)는 미리 인증된 각 관리자에 대응되어 미리 설정된 ID와 암호를 포함하는 권한정보를 저장할 수 있으며, 상기 인터페이스부(160)를 통한 사용자 입력을 기초로 상기 ID와 암호를 포함하는 인증정보를 수신한 경우 상기 인증정보를 상기 권한정보와 비교하여 관리자를 인증할 수 있다.

[0075] 이에 따라, 상기 제어부(150)는 상기 인터페이스부(160)를 통한 관리자 입력에 따른 제어신호를 기초로 상기 저장부(120)에 저장된 영상정보 중 관리자에 의해 선택된 영상정보를 마스킹 처리없이 상기 통신부(110)를 통해 외부 장치(300)에 전송하여 저장하거나 상기 디스플레이 장치(200)에 상기 영상정보를 출력하여 재생할 수 있다.

[0076] 이때, 상기 제어부(150)는 상기 영상정보 대신 마스킹 영상정보를 상기 외부 장치(300)에 전송하거나 디스플레이 장치(200)를 통해 출력할 수도 있다.

[0077] 또한, 상기 제어부(150)는 상기 영상정보 또는 마스킹 영상정보에 대한 접근 권한 있는 미리 인증된 각 외부 장치(300)에 대한 IP 주소 또는 시리얼 번호와 같은 식별정보를 포함하는 권한정보를 저장할 수 있으며, 통신부(110)를 통해 외부 장치(300)로부터 상기 식별정보를 포함하는 인증정보를 수신한 경우 해당 인증정보를 상기 권한정보와 비교하여 외부 장치(300)에 대한 인증을 수행할 수 있으며, 인증된 외부 장치(300)로부터 수신된 제어 신호를 기초로 상기 저장부(120)에 저장된 영상정보 중 선택된 상기 영상정보 또는 마스킹 영상정보를 상기 외부 장치(300)로 전송할 수 있다.

[0078] 이때, 상기 제어부(150)는 인증된 관리자의 입력을 기초로 상기 영상정보 또는 마스킹 영상정보를 상기 관리자가 지정한 외부 장치(300)의 IP 주소로 전송할 수 있다.

[0079] 상술한 구성에서, 상기 제어부(150)는 상기 영상정보 또는 마스킹 영상정보 전송 이전에 상기 영상정보 또는 마스킹 영상정보를 암호화하기 위한 암호화정보를 상기 관리자 입력을 기초로 수신하거나 상기 식별정보를 상기 암호화정보로 이용하여, 상기 암호화정보를 기초로 상기 영상정보 또는 마스킹 영상정보를 미리 설정된 암호화 알고리즘에 따라 암호화한 후 전송할 수 있다.

[0080] 이에 따라, 관리자는 자신이 입력한 암호화정보를 기초로 상기 암호화된 영상정보 또는 마스킹 영상정보를 복호화할 수 있으며, 상기 영상정보를 수신한 외부 장치(300)는 상기 식별정보를 이용하여 상기 암호화된 영상정보 또는 마스킹 영상정보를 복호화하여 상기 외부 장치(300)에 연결된 별도의 디스플레이 장치(310)를 통해 복호화된 영상정보 또는 마스킹 영상정보를 출력하여 재생할 수 있다.

[0081] 이를 통해, 상기 영상정보 처리기기(100)는 상기 영상정보 또는 마스킹 영상정보를 암호화하여 제공함으로써, 상기 영상정보 또는 마스킹 영상정보에 대한 접근권한이 있는 사용자에 한해 상기 영상정보 또는 마스킹 영상정보에 접근할 수 있도록 제한할 수 있으며, 이를 통해 영상정보 관리에 대한 보안성을 높일 수 있다.

[0082] 한편, 상기 개인정보 보호를 지원하는 영상정보 처리기기(100)는 각 감시 카메라(10)에 대하여 개인정보의 보호를 위한 동작범위를 설정하고, 해당 동작 범위를 기초로 개인정보의 침해가 발생하는 동작 제어가 발생하는 경우 이를 감지하여 개인정보 침해에 따른 불법 여부를 알림정보로 사용자에게 통지할 수 있는데 이를 상술한 구성을 토대로 도 6 내지 도 7을 통해 설명한다.

[0083] 우선, 도 6에 도시된 바와 같이 상기 영상정보 처리기기(100)의 구성에 따라, 제어부(150)에는 상기 각 감시 카메라(10)의 적법한 동작범위에 대한 규칙정보가 설정될 수 있다.

[0084] 이때, 상기 규칙정보는 각 감시 카메라(10)에 대응되어 촬영 가능 영역(또는 범위), PTZ(PAN/TILT/ZOOM) 동작 가능 범위, 용도 등이 설정될 수 있다.

[0085] 또한, 상기 제어부(150)는 상기 인터페이스부(160)를 통한 사용자 입력에 따라 상기 영상정보 처리기기(100)와 네트워크를 통해 연결된 하나 이상의 감시 카메라(10) 중 사용자에 의해 선택된 감시 카메라(10)를 제어하기 위한 동작정보를 생성할 수 있다.

[0086] 또한, 상기 제어부(150)는 상기 동작정보를 상기 선택된 감시 카메라(10)로 통신부(110)를 통해 전송하여, 상기 선택된 감시 카메라(10)가 사용자 입력에 따라 제어되도록 할 수 있다.

[0087] 이에 따라, 감시 카메라(10)는 상기 동작정보를 네트워크를 통해 수신하여 상기 동작정보에 따라 동작할 수 있으며, 동작정보에 따른 감시 카메라(10)의 현재 동작 상태에 대한 동작 상태정보를 생성하여 네트워크를 통해 상기 영상정보 처리기기(100)로 전송할 수 있다.

[0088] 이때, 도시된 바와 같이 감시 카메라(10)가 동작정보에 따라 동작하는 과정에서 현재 동작 상태에 따른 촬영 영역이 상기 규칙정보에 따른 동작 범위 내에 포함되는 경우에는 문제가 없으나, 상기 현재 동작 상태에 따른 상기 감시 카메라(10)의 촬영 영역이 상기 규칙정보에 따른 적법한 동작 범위를 이탈하는 경우 개인정보의 침해가 발생할 수 있다.

[0089] 이를 방지하기 위해, 상기 제어부(150)는 사용자 입력에 따라 생성한 상기 동작정보에 따른 감시 카메라(10)의 동작 상태 정보를 상기 규칙정보에 따른 감시 카메라(10)의 동작범위와 비교하여, 상기 동작 상태 정보가 규칙정보에 따른 동작범위를 벗어나는지 여부를 판단할 수 있다.

[0090] 이에 따라, 상기 제어부(150)는 상기 판단 결과에 따라 불법 여부를 알리기 위한 알림정보를 상기 디스플레이 장치(200)를 통해 출력할 수 있다.

[0091] 이를 통해, 상기 제어부(150)는 사용자에게 감시 카메라(10)의 운용을 개인정보가 보호되는 범위 내에서 운용하도록 유도할 수 있다.

[0092] 한편, 상기 감시 카메라(10)마다 설정된 제어 채널을 통해 상기 각 감시 카메라(10)와 네트워크를 통해 연결된 외부 장치(300)가 상기 각 감시 카메라(10)를 네트워크를 통해 제어할 수도 있으며, 상기 외부 장치(300)는 상기 각 감시 카메라(10)를 개별 제어하기 위한 동작정보를 상기 제어 채널로 전송할 수 있다.

[0093] 이때, 상기 영상정보 처리기기(100)는 상기 외부 장치(300)에서 전송하는 동작정보를 상기 네트워크를 통해 수신하거나 상기 외부 장치(300)와 직접 네트워크를 통해 연결되어 상기 동작정보를 수신할 수 있으며, 상기 외부 장치(300)의 동작정보를 기초로 각 감시 카메라(10)의 동작을 감시하여 상기 외부 장치(300)의 동작정보에 따른 상기 동작 상태 정보가 상기 규칙정보에 따른 동작범위를 벗어나는지 여부를 확인하고, 이에 따라 불법 여부를 판단하여 결과를 표시함으로써 외부 장치(300)를 통한 감시 카메라(10)의 운용이 개인정보의 보호가 이루어지는 범위 내에서 운용되도록 제한할 수 있다.

[0094] 이를 상세히 설명하면, 도시된 바와 같이 상기 제어부(150)는 상기 통신부(110)를 통해 상기 외부 장치(300)의 감시 카메라(10) 제어를 위한 동작정보를 수신할 수 있다.

[0095] 상기 제어부(150)는 상기 외부 장치(300)의 감시 카메라 제어를 위한 동작정보에 따라 변경된 감시 카메라의 동작 상태 정보를 상기 규칙정보에 따른 감시 카메라(10)의 동작 범위와 비교할 수 있으며, 상술한 바와 같이 상기 동작 상태 정보가 상기 규칙정보에 따른 동작범위를 벗어나는지 여부에 따라 상기 디스플레이 장치(200)를

통해 불법 여부에 대한 상기 알림정보를 출력할 수 있다.

[0096] 상술한 구성에서, 상기 제어부(150)는 동작 상태 정보가 규칙정보에 따른 동작범위를 벗어나지 않는 경우에도 알림정보를 출력하여 현재 감시 카메라(10)에 대한 제어가 적법한 것임을 알릴 수 있다.

[0097] 또한, 상기 제어부(150)는 상기 디스플레이 장치(200)를 통해 상기 동작정보에 따라 동작하는 감시 카메라(10)의 영상과 함께 상기 알림정보를 출력할 수 있음은 물론이다.

[0098] 더하여, 상기 제어부(150)는 상기 디스플레이 장치(200)를 통해 표시된 복수의 감시 카메라(10) 각각에 대응되는 영상과 함께 상기 각 감시 카메라(10)에 대응되는 알림정보를 출력할 수 있다.

[0099] 이를 통해, 관리자는 상기 디스플레이 장치(200)에 출력되는 복수의 감시 카메라(10) 중에서 불법이 발생한 감시 카메라(10)를 용이하게 파악할 수 있다.

[0100] 한편, 상기 규칙정보는 도 6 및 도 7에 도시된 바와 같이 서로 다른 동작 범위 각각에 대응되어 서로 다른 단계가 설정될 수 있으며, 각 단계에 대응되어 알림정보가 설정될 수 있다. 이때, 서로 다른 단계에 대응되어 서로 다른 알림정보가 설정될 수 있다.

[0101] 이에 따라, 상기 제어부(150)는 상기 규칙정보에 따른 서로 다른 동작 범위 중 상기 동작 상태 정보에 대응되는 동작 범위를 판단하고, 상기 동작범위에 대응되는 단계를 식별하여 해당 단계에 설정된 알림정보를 출력할 수 있다.

[0102] 일례로, 상기 제어부(150)는 상기 동작 상태 정보가 규칙정보에 따른 동작범위 중 '경계'에 해당하는 단계의 동작범위에 해당하는 경우 해당 '경계'에 해당하는 단계에 설정된 알림정보를 출력하여, 현재 감시 카메라(10)의 동작 범위가 불법임을 알릴 수 있다.

[0103] 또한, 상기 제어부(150)는 상기 동작 상태 정보가 규칙정보에 따른 동작 범위 중 '정상'에 해당하는 단계의 동작범위에 해당하는 경우 해당 '정상'에 해당하는 단계에 설정된 알림정보를 출력하여, 현재 감시 카메라(10)의 동작범위가 적법임을 알릴 수 있다.

[0104] 상술한 구성에서, 상기 동작 상태 정보와 규칙정보 비교시 상호 동일한 감시 카메라(10)를 대상으로 비교됨은 물론이다.

[0105] 한편, 상술한 구성에서 상기 로그정보 수집부(140)는 상기 제어부(150)에 의해 사용자 입력에 따라 생성되는 동작정보 또는 상기 외부 장치(300)로부터 전송되어 상기 제어부(150)에 수신되는 동작정보를 기초로 로그정보를 생성하여 상기 저장부(120)에 저장할 수 있다.

[0106] 또한, 상기 로그정보 수집부(140)는 상기 제어부(150)에 설정된 권한정보를 기초로 인증되지 않은(비인가된) 사용자 또는 외부 장치(300)를 검출할 수 있으며, 해당 비인가된 사용자 또는 외부 장치(300)의 동작정보 또는 제어신호를 검출할 수 있다.

[0107] 이에 따라, 로그정보 수집부(140)는 비인가된 사용자 또는 외부 장치(300)의 동작정보 및 제어신호 중 적어도 하나와 해당 비인가된 사용자 또는 외부 장치(300)의 인증정보(일례로, IP 주소, MAC 주소, ID 등)를 포함하는 로그정보를 생성하여 상기 저장부(120)에 저장할 수 있다.

[0108] 이때, 상기 로그정보 수집부(140)는 인가된 사용자 또는 외부 장치(300)의 제어신호 및 동작정보 중 적어도 하나와 인가된 사용자의 인증정보를 포함하는 로그정보를 생성할 수도 있으며, 이를 저장부(120)에 저장할 수 있다.

[0109] 또한, 상기 제어부(150)는 상기 저장부(120)에 저장된 로그정보를 미리 설정된 기간 단위로 수집하여 도 7에 도시된 바와 같이 상기 동작정보에 따른 동작 제어의 종류에 대한 통계정보를 산출하고, 이를 상기 통신부(110)에 연결된 디스플레이 장치(200)를 통해 출력할 수 있다.

[0110] 더하여, 상기 제어부(150)는 상기 로그정보 수집부(140)와 실시간으로 연동하여 상기 규칙정보에 따른 동작범위를 벗어나는 동작 상태를 야기한 동작 정보에 따른 로그정보가 발생하거나 비인가된 사용자 또는 외부 장치(300)에 의한 제어신호 및 동작정보 중 적어도 하나에 대한 로그정보 발생시마다 해당 로그정보를 이벤트 정보로 생성하여 저장부(120)에 저장할 수 있다.

[0111] 이때, 상기 제어부(150)는 상기 비인가된 사용자 또는 외부 장치(300)에 대응되는 로그정보 생성시 이에 대응되는 알림정보를 디스플레이를 통해 출력하여 비인가된 사용자 또는 외부 장치(300)에 의한 해킹 위협을 통지할

수 있다.

[0112] 더하여, 상기 각 권한정보에는 영상정보의 이용 범위에 대한 이용 범위 정보가 설정될 수 있으며, 상기 이용 범위 정보는 영상정보 또는 마스킹 정보의 이용가능 시간, 영상정보 또는 마스킹 영상정보에 적용 가능한 제어신호의 종류(변경, 삭제, 전송 등), 감시 카메라(10) 중 이용 가능한 감시 카메라(10)의 식별정보(일례로, IP 주소) 등과 같은 정보를 포함할 수 있다.

[0113] 이에 따라, 상기 제어부(150)는 상기 로그정보 수집부(140)와 연동하여 인가된 사용자라 하더라도 상기 인가된 사용자에 대응되는 권한정보에 포함된 이용 범위 정보에 따른 이용 가능 범위를 벗어나는 제어신호가 발생한 경우 이에 대응되는 로그정보 및 알림정보를 생성하여 로그정보를 이벤트 정보로 저장부(120)에 저장하고 해당 알림정보를 디스플레이 장치(200)를 통해 출력할 수 있다.

[0114] 또한, 상기 제어부(150)는 상기 저장부(120)에 저장된 복수의 이벤트 정보를 취합하고, 취합된 이벤트 정보를 기초로 시간대별 이벤트 발생현황 및 이벤트 종류별 통계에 대한 통계정보를 산출하여 상기 디스플레이 장치(200)를 통해 출력할 수도 있다.

[0115] 한편, 상술한 구성에서, 상기 제어부(150)는 상기 동작정보를 기초로 상기 규칙정보에 따른 동작범위를 벗어나는 감시 카메라(10)를 자동 식별할 수 있으며, 식별된 감시 카메라(10)에 대하여 상기 규칙정보에 따른 적법한 동작 범위 내로 상기 감시 카메라(10)를 제어하기 위한 복귀제어 정보를 생성하여 상기 식별된 감시 카메라(10)로 전송할 수도 있다.

[0116] 이에 따라, 상기 복귀제어 정보를 수신한 감시 카메라(10)는 상기 복귀제어 정보를 기초로 동작하여 상기 규칙정보에 따른 적법한 동작 범위 내로 복귀할 수 있다.

[0117] 이를 통해, 상기 영상정보 처리기기(100)는 자동으로 개인정보의 침해가 우려되는 감시 카메라(10)의 동작을 변경하여, 적법한 동작 범위 내로 복귀시켜 개인정보 보호를 지원할 수 있다.

[0118] 상술한 구성에 따라, 영상정보 처리기기(100)는 개인정보 보호를 위한 감시 카메라(10)의 동작 범위를 설정하고, 해당 동작 범위를 벗어나는 감시 카메라(10)의 동작이 발생하는 경우 이에 대한 알림정보를 표시하여, 사용자가 감시 카메라(10)를 동작시키면서 현재 감시 카메라(10)의 동작 상태가 개인정보 보호범위를 벗어나는지 판단할 수 있도록 지원하는 동시에 개인정보 보호가 이루어지는 적법한 동작 범위 내에서 감시 카메라(10)를 운용하도록 사용자를 유도할 수 있다.

[0119] 또한, 영상정보 처리기기(100)는 감시 카메라(10) 또는 영상정보의 불법적인 운용에 따른 이벤트 정보를 생성하여 기록하고 이를 통계화하여 제공함으로써, 사용자가 기존에 감시 카메라(10) 운용에 따라 발생한 불법 운용 현황을 용이하게 파악하여 책임소재를 추궁하고 감시 카메라(10)의 불법 운용을 사전에 차단할 수 있도록 지원할 수 있다.

[0120] 도 8은 본 발명의 실시예에 따른 하나 이상의 감시 카메라(10)와 네트워크를 통해 연결되어 각 감시 카메라(10)의 영상정보를 수신하는 영상정보 처리기기(100)의 개인 정보 보호를 위한 영상정보 처리 방법에 대한 순서도이다.

[0121] 우선, 영상정보 처리기기(100)는 하나 이상의 감시 카메라(10)로부터 영상정보를 수신하여 저장할 수 있다(S1).

[0122] 또한, 상기 영상정보 처리기기(100)는 외부 장치(300)로 상기 영상정보를 전송 또는 재생하기 위한 제어신호를 수신하는 경우(S2) 개인정보 보호를 위해 미리 설정된 객체 관련 설정정보에 대응되어 상기 영상정보에 대한 영상 분석을 통해 상기 객체를 인식할 수 있다(S3).

[0123] 이후, 상기 영상정보 처리기기(100)는 상기 영상 정보에서 상기 객체에 대응되는 영역을 마스킹 처리하여 생성된 마스킹 영상정보를 상기 외부 장치(300)로 전송하거나 재생할 수 있다(S4).

[0124] 또한, 상기 영상정보 처리기기(100)는 상기 감시 카메라(10)의 동작 제어에 대한 동작정보를 수신한 경우(S5) 개인정보 보호를 위한 상기 각 감시 카메라(10)의 개인정보 보호를 위한 동작 범위가 설정되어 미리 저장된 규칙정보를 상기 동작정보에 따른 감시 카메라의 동작 상태와 비교하여(S6) 상기 규칙정보에 따른 동작 범위를 벗어나는 경우(S7) 알림정보를 출력할 수 있다(S8).

[0125] 본 명세서에 기술된 다양한 장치 및 구성부는 하드웨어 회로(예를 들어, CMOS 기반 로직 회로), 펌웨어, 소프트웨어 또는 이들의 조합에 의해 구현될 수 있다. 예를 들어, 다양한 전기적 구조의 형태로 트랜지스터, 로직게이트 및 전자회로를 활용하여 구현될 수 있다.

[0126] 전술된 내용은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0127] 10: 감시 카메라 100: 영상정보 처리기기

110: 통신부 120: 저장부

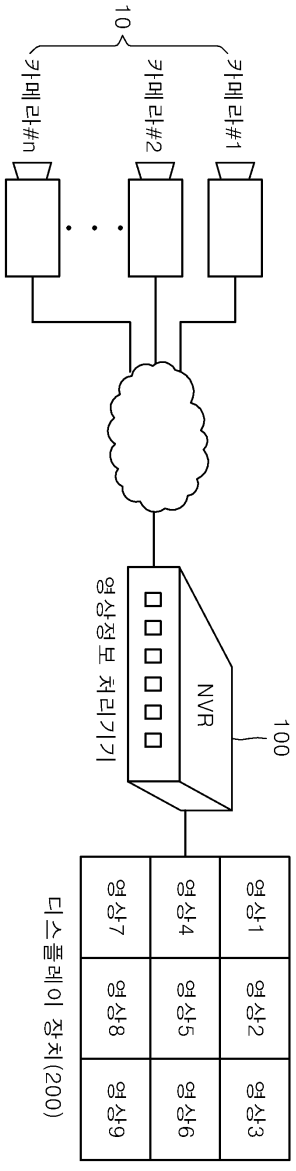
130: 영상 처리부 140: 로그정보 수집부

150: 제어부 160: 인터페이스부

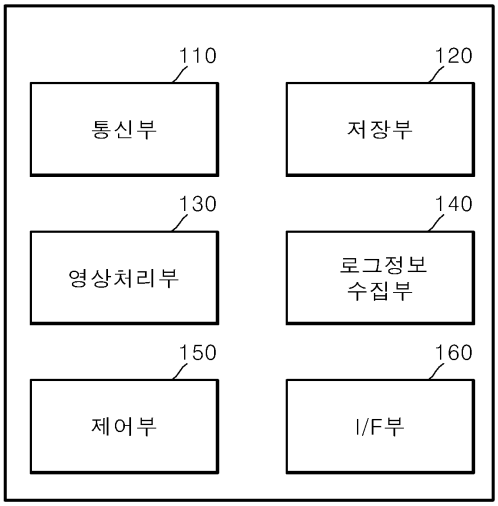
200: 디스플레이 장치 300: 외부 장치

도면

도면1

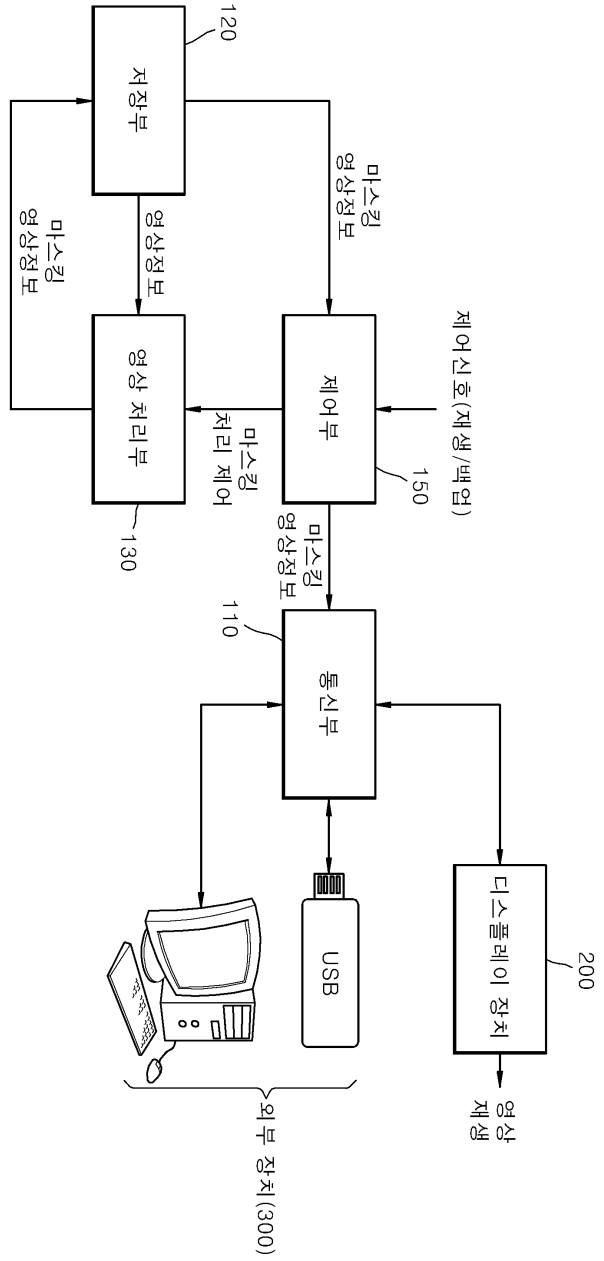


도면2

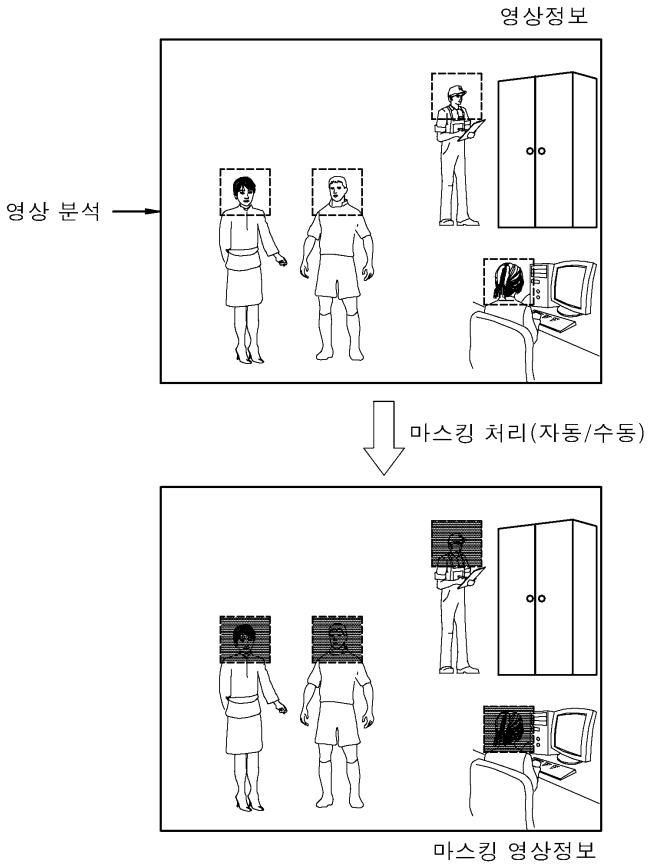


영상정보 처리기기(100)

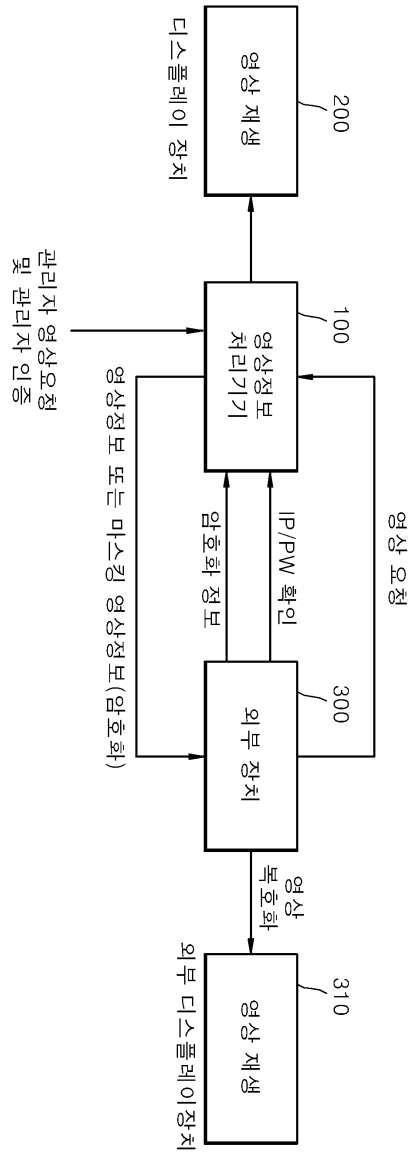
도면3


120
저장부
마스킹
영상정보
영상정보
마스킹
영상정보
영상 처리부
130
마스킹
처리 제어
제어부
150
제어신호(재생/백업)
마스킹
영상정보
110
통신부
USB
외부 장치(300)
디스플레이 장치
200
영상
재생

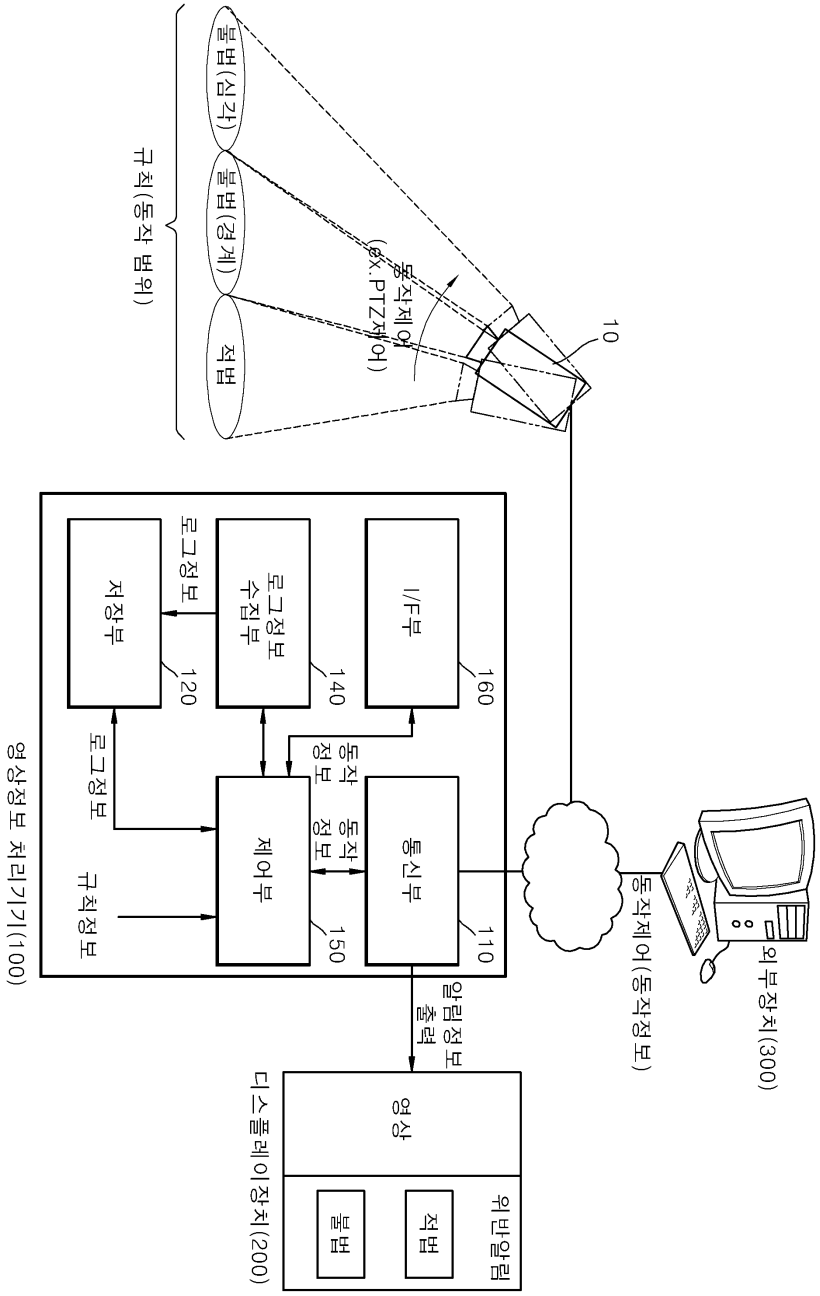
도면4



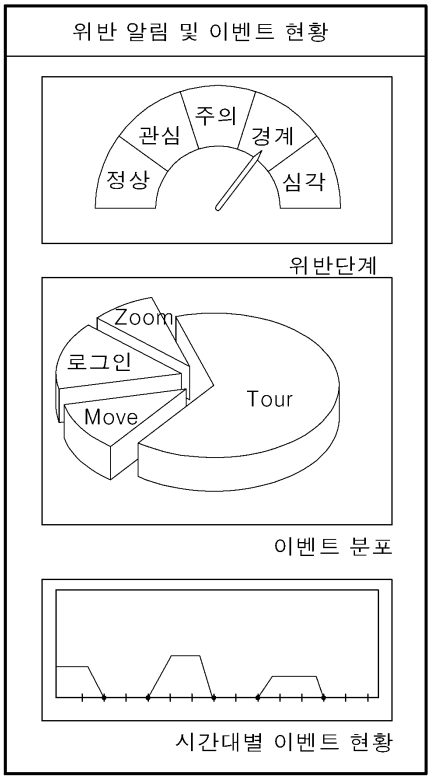
도면5


영상 재생
디스플레이 장치
200
관리자 영상요청
및 관리자 인증
영상정보
처리기기
100
영상정보 또는 마스킹 영상정보(암호화)
암호화 정보
IP/PW 확인
영상 요청
외부 장치
300
영상
복호화
영상 재생
외부 디스플레이장치
310

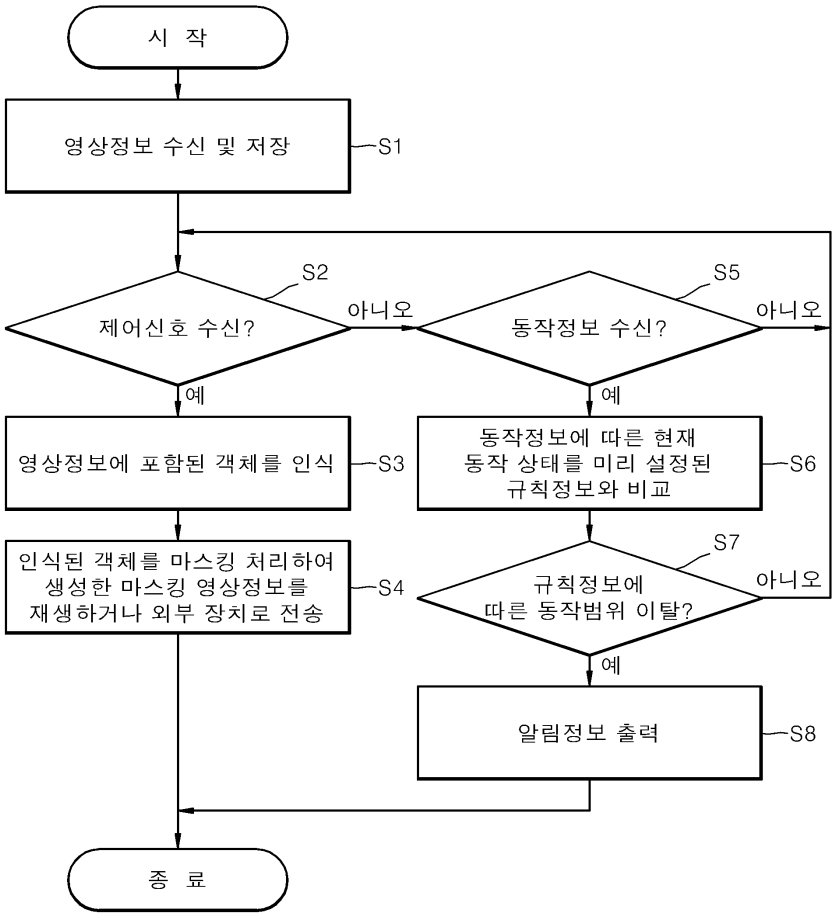
도면6


규칙(동작 범위)
물범(심각)
물범(경계)
적법
동작제어
(ex.PTZ제어)
10
영상정보 처리기(100)
저장부
120
로그정보
로그정보
수집부
140
I/F부
160
로그정보
동작
정보
제어부
동작
정보
통신부
110
규칙정보
150
알림정보
출력
디스플레이장치(200)
영상
위반알림
불법
적법
동작제어(동작정보)
외부장치(300)

도면7


위반 알림 및 이벤트 현황
주의
관심
경계
정상
심각
위반단계
Zoom
로그인
Tour
Move
이벤트 분포
시간대별 이벤트 현황

도면8


시 작
영상정보 수신 및 저장
S1
S2
제어신호 수신?
아니오
예
S5
동작정보 수신?
아니오
예
영상정보에 포함된 객체를 인식
S3
동작정보에 따른 현재
동작 상태를 미리 설정된
규칙정보와 비교
S6
인식된 객체를 마스킹 처리하여
생성한 마스킹 영상정보를
재생하거나 외부 장치로 전송
S4
S7
규칙정보에
따른 동작범위 이탈?
아니오
예
알림정보 출력
S8
종 료