프라이버시 보호를 위한 감시카메라 시스템에 관한 연구

문해민* · 반성범**

A Study on the Surveillance Camera System for Privacy Protection

Hae-Min Moon* · Sung Bum Pan**

이 논문은 2009학년도 조선대학교 학술연구비의 지원을 받아 연구되었음

요 약

최근 테러 및 범죄의 증가로 CCTV를 이용한 보안 감시시스템에 대한 활용이 증가되고 있다. CCTV에는 얼굴이나 행동패턴과 같은 개인의 프라이버시 정보가 기록되는데, 이 정보가 노출될 시 프라이버시 침해뿐만 아니라 범죄에 이용될 수 있는 문제점이 있다. 본 논문에서는 CCTV를 이용한 감시시스템에서의 프라이버시 보호에 관한 기존 연구를 분석한 후, 프라이버시 보호가 가능한 RFID 기반 감시카메라 시스템을 제안한다. 제안한 시스템은 스크램블링(scrambling) 기술과 RFID 시스템을 사용하여 개인의 프라이버시를 보호함과 동시에 감시로써의 기능도 유지하게 되는 특징을 지닌다.

ABSTRACT

Due to increased terrors and crimes, the use of surveillance camera systems including CCTV is also increasing. Private information such as faces or behavior patterns can be recorded in CCTV and when it is exposed, it may cause infringement to privacy and crimes. This paper analyses conventional methods on protection of privacy in surveillance camera system and then suggests an RFID-based surveillance camera system that can both watch crimes and protect privacy. The proposed system protects privacy and watches crimes using scrambling and an RFID system.

키워드

감시시스템, 프라이버시 보호, 스크램블링, RFID

surveillance system, privacy protection, scrambling, RFID

* 조선대학교 정보통신공학과

** 조선대학교 제어계측로봇공학과 (교신저자)

접수일자 2009. 03. 03

심사완료일자 2009. 04. 18

Ⅰ. 서 론

행정자치부가 펴낸 정책백서에 따르면 2008년 경찰, 지방자치단체 등에서 범죄예방, 쓰레기투기 단속 등 공익적 목적을 위해 전국적으로 약 13만 여대의 CCTV가 설치·운영되고 있는 것으로 집계된다. 민간의 경우는 250만에서 300만대에 이르는 것으로 추정된다. 공공기관에 설치 중인 CCTV의 경우엔 설치 위치와 수 등이 파악되고 있지만 민간의 경우 설치사항에 대한 제한이 없기 때문에 파악이 어렵다.

영국 런던은 하루에 300번씩 무인 카메라에 찍히고 있다는 통계가 나올 정도로 CCTV가 많아 '철의 고리'라고 불리기도 한다. 프랑스의 경우엔 전국의 CCTV가 100만대 이상 설치되어 있는 것으로 알려져 있고, 대통령이 2007년 "영국 경찰의 CCTV 네트워크에 감명 받았다"고 언급한데 이어 CCTV를 3배 늘리는 계획을 추진 중이라고 한다.

CCTV등과 같은 감시시스템이 부적당한 행동을 모니터링 하는데 유용하게 사용되지만, 동시에 무해한 사람들의 프라이버시 노출이라는 문제점을 야기하고 있다[1]. 정보통신기술의 발달로 개인 정보의 수집·유통이 용이해지며 프라이버시의 개념은 전통적인 '혼자 있을 권리'라는 소극적인 개념을 넘어 '자신에 관한 정보를 통제할 수 있는 권리'로 확대 되었다[2]. A. Westin은 프라이버시를 '자신에 관한 정보가 언제, 어떻게, 얼마만큼 다른 사람과 의사소통 되어도 되는지를 그들 스스로 결정할 개인, 단체, 기관의 요구'라고 언급했다[3]. 개인이 요구할 경우 제공되는 영상데이터에는 본인 이외의 다른 사람의 영상데이터도 같이 제공되어 진다. 이럴 경우 원치 않게 자신의 얼굴이 노출되기 때문에 문제가 된다. 예를 들어 의사나 간호사의 활동 정보를 기록하기 위해 CCTV를 설치했을 때, 의사나 간호사뿐 아니라 환자들의 얼굴까지 찍히게 된다. 이럴 경우 환자의 프라이버시 침해라는 문제를 발생시킨다.

UN은 개인의 프라이버시 침해를 막기 위해 개인정보전산화 가이드라인을 통해 각국에 독립적인 개인 정보 감독기구를 둘 것을 권고했고, 영국·독일·프랑스 등은 개인정보보호를 위한 독립적인 감독기구를 설치하고 있다. 이러한 기구들의 활동뿐만 아니라 감시시스템에서 프라이버시를 보호해주는 기술에 대한 연구도 활발히 진행되고 있다. 감시카메라 시스템은 화면에서 대상을 찾아내거나 찾아낸 대상의 얼굴을 가려줌으로써 프라이버시를 보호해주는 지능적인 시스템으로 발전하고 있다[4-7]. 신원인증을 통해 프라이버시를 보호하거나 성능향상을 위해 기존의 프라이버시 시스템에 RFID 시스템을 결합하기도 하였다[8,9]. 영상압축을 이용한 방법은 화면에서 사람의 얼굴 같은 관심영역을 찾아내어 암호화를 함으로써 프라이버시를 보호한다[10-12].

본 논문에서는 신원이 확인되어 있는 사람과 그렇지 않은 사람이 구분되는 특정 장소에서 프라이버시 보호와 감시로써의 기능을 동시에 만족할 수 있는 비디오 감시시스템 방법을 제안한다. 제안하는 방법은 모니터링하는 단계에서 감시자나 민간인에 의한 프라이버시 침해를 막기 위해 스크램블링 기술을 사용한다. 또한 프라이버시가 보호된 화면에 대상의 정보를 제공하기 위하여 RFID 시스템을 이용한다. RFID 시스템은 대상을 신원이 확인된 내부인과 확인되지 않은 외부인을 판단하는데 이용된다. RFID 시스템은 대상의 내·외부인 정보만을 제공하기 때문에 프라이버시 침해에는 영향을 끼치지 않는다. 또한 제안하는 방법은 접근레벨에 따라 스크램블링의 강도 및 대상의 정보를 달리 제공함으로써 감시자나 일반인에 의한 프라이버시 침해를 줄일 수 있다.

본 논문의 구성은 Ⅱ장에서 프라이버시 보호 시스템에 관련된 기존 연구를 분석한다. Ⅲ장에서는 제안하는 프라이버시 보호 시스템을 소개하고, Ⅳ장에서 제안한 시스템의 실험결과를 설명한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 감시시스템에서의 프라이버시 보호

감시시스템에서 대상의 프라이버시를 보호하는 일반적인 방법은 그림 1과 같이 프라이버시 보호를 받기 원하는 대상의 얼굴을 모자이크 처리해주는 것이다. 만약 스크램블링 처리된 영상이 타인이나 외부에 노출되더라도 대상의 신원을 파악하기 어렵기 때문에 악용될 위험이 적어진다.

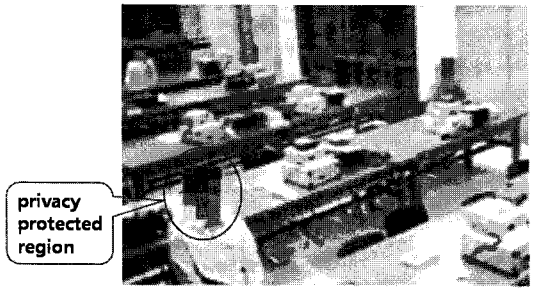


그림 1. 영상에서 프라이버시 보호
Fig. 1 Privacy protection in image

감시시스템에서 프라이버시를 보호하기 위한 많은 연구가 되고 있다. S. Tansuriyavong 등은 얼굴인식에 의해 사람을 자동적으로 확인하고, 실루엣과 같은 변형된 이미지를 화면에 보여주는 시스템을 제안하였다[5].

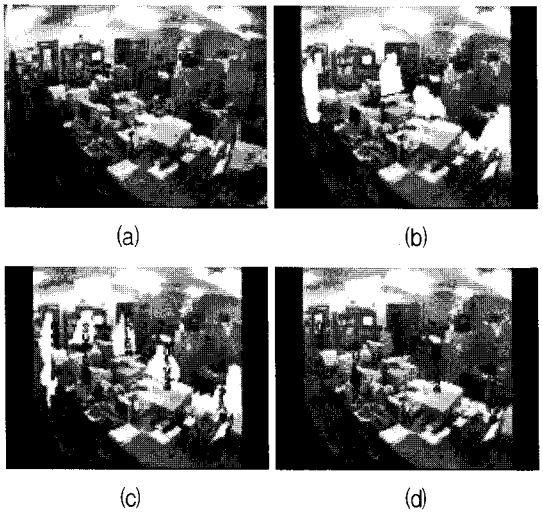


그림 2. S. Tansuriyayong 등의 시스템에서 프라이버시 보호 (a) 원본영상, (b) 실루엣으로 표시, (c) 실루엣과 대상의 이름을 표시, (d) 대상의 이름만 표시
Fig. 2 Privacy protection of S. Tansurivayong's system (a) original image (b) silhouette display (c) silhouette display with name (d) only name display

이 시스템은 입구에 설치된 카메라와 방에 설치된 카메라2대로 이루어져있다. 입구에 설치된 카메라는 대상의 얼굴을 인식하는데 사용되어지고, 방에 설치된 카메라는 일반적인 감시카메라의 역할을 한다. 입구에 설치된 카메라로 얻은 얼굴인식에 의한 정보를 이용하여 대상을 그림 2와 같이 다양한 형태로 표현해준다. 그림 2(a)는 방에 설치된 카메라에 의해 촬영된 원본 비디오 이미지이다. 그림 2(b)는 촬영된 비디오 이미지에서 사람들을 찾아 실루엣 이미지로 대체한 것이다. 그림 2(c)는 실루엣 이미지에 얼굴인식에 의해 식별된 데이터를 이용하여 대상의 이름을 나타내 주었다. 그림 2(d)는 화면에서 대상을 완전히 제거한 후 오직 대상의 이름만을 표시해주었다.

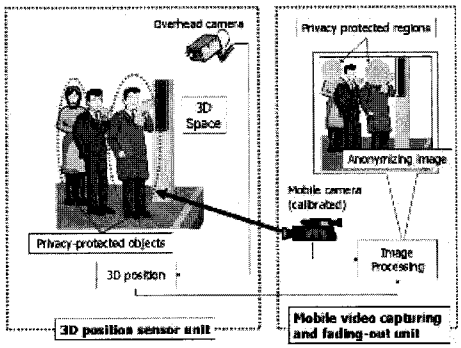


그림 3. 모바일 카메라를 가진 Stealth Vision 시스템
Fig. 3 Stealth vision system with mobile camera

RFID 시스템은 감시시스템에서 프라이버시 보호 대상을 판별하는 방법 중 하나이다[8,9]. 그림 3의 시스템은 대상의 프라이버시 보호를 위해 fade-out 시켜주는 비디오 캡쳐링 시스템이다. 모바일 카메라에 의해 촬영된 이미지에서 프라이버시 보호 영역을 탐지하는 방법은 두 가지가 있다. 하나는 단일 카메라를 사용하여 촬영된 이미지에서 프라이버시 보호 영역을 추출하는 것이다. 프라이버시 보호를 받아야할 영역은 인체와 얼굴 검출과 같은 2D영상처리 기법에 의해 탐색된다. 이러한 방법은 카메라의 조명 조건, 인간외형의 차이, 대상의 중첩에 따른 문제에 영향을 많이 받는 단점이 있다. 프라이버시 보호를 받아야할 대상이 다른 대상과 중첩이 되면 프라이버시 보호 대상자의 위치를 정확하게 찾기가 어려워진다. 중첩된 화면에서 프라이버시 보호 대상자를 찾기 위해, 이 시스템은 다중 카메라/센서를 이용함으로써 3차원공간에서 대상의 위치를 결정한다. 이 시스템은 그림 3에서 보여주는 바와 같이 두 개의 장치로 구성된다. 3D위치센서 장치는 오버헤드 카메라를 이용하여 목표물의 수와 목표물의 3D위치를 추정한다. 모바일 비디오

촬영과 fade-out 장치는 LED-ID-tags를 이용함으로써 촬영된 모바일 이미지를 조정하고, 프라이버시 보호 영역을 fade-out 시켜준다.

멀티미디어 기술의 이용 증가와 더불어, 영상 압축은 새로운 기능과 보다 나은 성능을 필요로 한다. JPEG2000은 기존의 표준기술보다 높은 압축률에서 영상성능면의 우수성을 제공한다. 많은 데이터를 저장해야하는 감시시스템에서 효율적인 압축은 필수적이다. 뿐만 아니라 영상에서 사용자가 특정 관심영역을 정의 및 암호화하는 작업인 관심영역 암호화는 프라이버시를 보호하는데도 적합하다. JPEG2000과 같은 관심영역 암호화는 현재 많은 연구가 진행되고 있다[10-12].

그림 4. JPEG2000을 이용한 프라이버시 보호 시스템
Fig. 4 Privacy protection system using JPEG2000

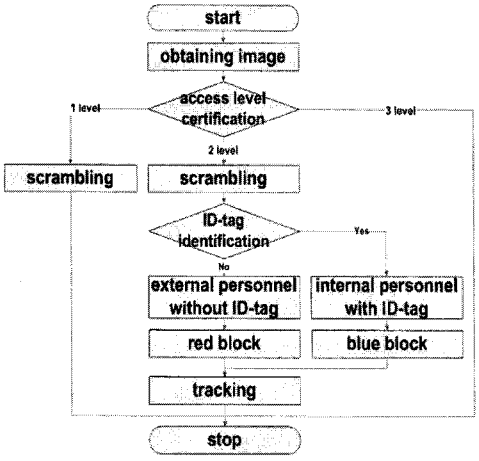
I. Martinez-Ponte 등은 감시시스템에서 프라이버시를 보호하기위해 마스크 페이스에 강인한 시스템을 제안했다[10]. 이 시스템은 분석 모듈과 Motion JPEG2000 인코딩 모듈로 구성된다. 분석 모듈은 화면에서 얼굴과 같은 관심영역을 추출하고, Motion JPEG2000 인코딩 모듈은 추출된 관심영역을 압축한다. 그림 4는 JPEG2000의 ROI(Region of Interest) 암호화 기술을 이용한 프라이버시 보호의 예이다. JPEG2000 이미지 압축 프레임워크는 품질 층을 규정하는 것이 가능하다. 규정된 품질 층에서 관심영역으로부터 데이터를 분리하면 분리된 데이터 층의 질은 암호화 프레임에서 다른 모든 품질 층의 질보다 떨어진다. 그림 4와 같이 감시자가 영상의 첫 번째 데이터층만을 디코딩하게 되면 얼굴은 프라이버시 보호된다.

III. 제안하는 프라이버시 보호 시스템

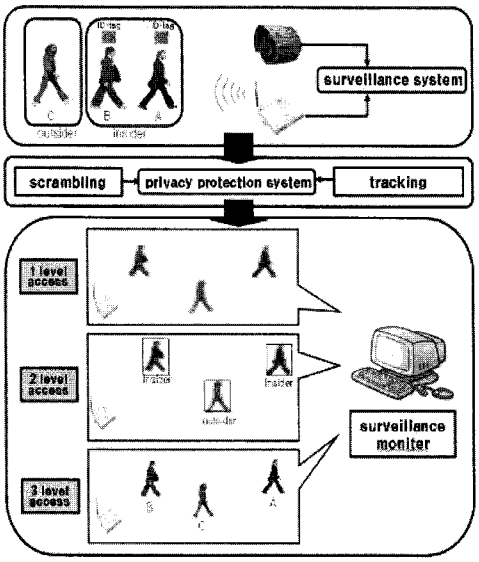
기존의 감시시스템은 모니터링 하는 단계에서 감시자나 감시시스템과 전혀 관계없는 일반인에 의한 프라이버시 침해가 발생할 수 있다. 본 논문에서는 모니터링 단계에서의 프라이버시 노출을 막기 위해 기존의 감시시스템에 스크램블링 기술과 RFID 시스템을 적용하여 프라이버시 보호와 감시시스템으로써의 기능을 동시에 가능하게 한다. 감시자에 의한 프라이버시 침해를 막기 위해서는 기본적으로 프라이버시 보호된 화면을 제공해야 한다. 동시에 범죄와 같은 위급한 상황에 대하여 프라이버시 보호 기능을 해제한 후, 신속하게 원본영상을 볼 수 있어야 한다. 또한 개인의 프라이버시를 보호하면서 감시자가 원활히 임무를 수행하기 위해선 감시자에게 프라이버시를 침해하지 않는 대상의 정보도 제공되어야한다[17]. 이와 같은 결과로 감시시스템에는 다음과 같은 조건이 요구된다.

- ○ 감시카메라에 촬영되어지는 대상은 프라이버시 보호 처리가 되어야 한다.
- ○ 프라이버시 보호 중에도 감시로써의 기능을 유지할 수 있어야 한다.
- ○ 접근레벨에 따른 스크램블링의 강도 변화가 있어야 한다.

그림 5(a)는 제안하는 시스템의 흐름을 나타낸다. 감시시스템이 동작하게 되면 감시카메라는 현재영상을 획득한 후 사용자의 접근레벨을 판단하게 된다. 접근레벨은 사용자의 인증번호에 따라 달라지는데 1레벨 접근을 제외한 2레벨 접근과 3레벨 접근을 하기위해선 미리 정해진 인증번호가 필요하다. 접근레벨에 따라 시스템은 스크램블링 처리 및 대상의 신분을 판단하게 되는데, 그림 5(b)에서와 같이 접근레벨에 따라 다양한 형태로 표현된다. 1레벨 접근일 경우는 프라이버시 보호기능에 대상의 정확한 신원을 파악할 수 없고, 2레벨 접근은 그림 5(b)에서와 같이 프라이버시를 보호함과 동시에 내부인과 외부인에 대한 정보를 각각 다른 색을 이용하여 표시해준다. 3레벨의 경우에는 어떠한 프라이버시 보호기능이 적용되지 않아 대상에 대한 정확한 신원을 판단할 수 있다.



(a)



(b)

그림 5. 제안하는 프라이버시 보호 시스템
(a) 시스템 흐름도, (b) 시스템 구조
Fig. 5 Proposed privacy protection system
(a) system block diagram, (b) system structure

A. 객체의 추출

감시시스템에서 대상의 프라이버시 보호를 위해선 객체의 추출이 필수적이다. 이를 위해 얼굴인식이나 특정마크를 이용한 객체추출 방법들이 많이 연구되고 있다[13,14]. 이밖에도 객체를 추출하는 방법에는 실시간 영상에서 배경 영상과 입력 영상을 구분하여 움직인 객체를 추출하거나, 블록정합기법, 배경 영상을 이용한 방법 등이 있다. 본 논문은 배경영상을 이용한 방법을 사용한다. 배경영상을 이용한 방법은 현재 프레임과 기준이 되는 배경영상의 차이를 구하는 방법이다. 이 방법은 배경이 되는 원본영상을 추출하거나 카메라의 흔들림에 의한 배경영상과 현재영상의 비교 불가능과 같은 문제점을 지닌다. 우리는 기존의 감시카메라는 대부분 고정된 채로 설치 되어있는 것을 알 수 있다. 이는 배경영상을 추출하거나 카메라의 흔들림에 의해 발생할 수 있는 문제를 피할 수 있다.

B. 프라이버시 보호 대상 판별 및 정보 유지

프라이버시가 보호되는 시스템이라고 해도 감시카메라에서 감시자로써의 임무를 원활이 수행하기 위해서 화면상에 충분한 정보를 제공해야 한다. 그림 5에서와 같이 화면상에 대상에 대한 충분한 정보를 제공하기 위해 RFID 시스템을 이용한다. 그림 5와 같이 화면에 A, B, C라는 사람이 있다. A와 B는 회사 내부인에 해당하여 ID-tag를 소유하고 있고, 대상 C는 외부인으로써 ID-tag를 소유하고 있지 않다. 대상이 RFID 리더기가 설치된 장소를 지나게 되면 시스템은 대상의 ID-tag소유 여부에 따라 내·외부인을 판단한다. 이는 객체추적에 의해 내부인의 경우 빨간색 블록을 외부인의 경우 파란색 블록을 이용하여 나타냄으로써 대상의 내·외부인 정보를 유지하게 된다.

비디오 영상에서 대상의 내·외부인 정보를 유지하기 위해서는 트래킹 기술이 필수적이다[15,16]. 트래킹은 비디오 영상에서 하나의 영상과 다른 영상 사이의 특정 객체를 찾거나 추적 대상의 행동이나 특징을 감시하는 등의 여러 분야에서 사용되는 기술이다. 본 논문에서는 이전 프레임과 현재 프레임의 특징을 이용한 간단한 트래킹 방법을 사용해서, 대상이 화면에서 완전히 사라지는 동안 대상의 내·외부인 정보를 유지한다.

C. 접근레벨에 따른 프라이버시 보호 강도조절

기존의 감시시스템에 프라이버시 보호 기능을 적용하게 되면, 본래 감시카메라가 수행해야 할 감시로써의 기능이 취약해질 수 있다. 감시시스템과 전혀 관계없는 사람이 감시 모니터에 접근했을 때 화면을 통한 대상의 프라이버시 노출이나 범죄와 같은 위험한 상황에서 정확한 정보의 제공을 위한 프라이버시 보호 기능을 해제

할 수 있는 시스템이 요구된다. 본 논문에서는 강도 조절이 가능한 스크램블링 기술을 사용한다. 제안하는 방법은 인증번호에 의한 접근레벨에 따라 모니터의 시각화를 달리할 수 있다. 접근레벨의 단계는 총 3단계로 나누어진다. 1레벨 접근은 모니터 상에 어떠한 정보도 제공되지 않아 대상의 얼굴이나 신원을 확인할 수 없다. 2레벨 접근은 위에서 언급한바와 같이 감시자는 대상의 정확한 신원파악은할 수 없지만 ID-tag의 소유 여부를 판별하여 내·외부인을 판단할 수 있다. 마지막으로 3레벨 접근은 어떠한 프라이버시 보호 처리도 적용되지 않은 상태로 카메라에서 받아들인 현재영상을 보여준다.

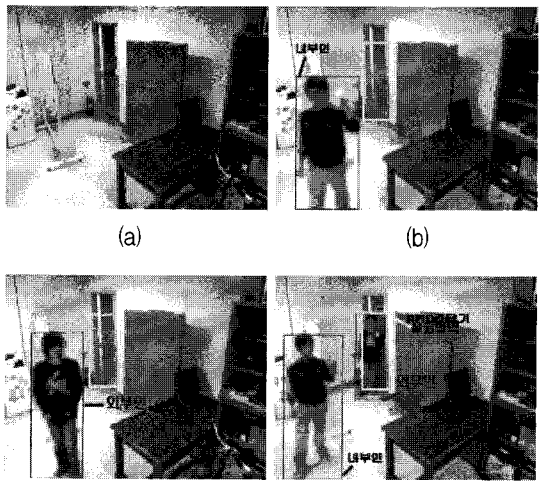
Ⅳ. 실험결과

제안하는 시스템의 접근레벨에 따른 시뮬레이션 결과를 영상을 그림 6, 7, 8에 나타내었다. 실험 장소는 출입이 제한되는 임의의 장소이고, 카메라는 외부의 영향을 받지 않는 고정된 장소에 설치되어져 있다. 실험을 위해 ID-tag를 소유한 내부인과 ID-tag를 소유하지 않는 외부인이 무작위로 출입을 하였고, 각각 시스템의 접근레벨에 따른 프라이버시 보호의 변화에 따른 결과를 추출하였다.

그림 6은 시스템에 1레벨 접근의 결과 영상이다. 그림 6(a)는 카메라에 의해 등록되어지는 배경영상이고, 그림 6(b)는 내부인과 외부인의 구별 없이 대상을 모두 스크램블링 처리를 해준다. 이는 스크램블링에 의해 대상의 프라이버시 침해에 관한 정보가 제공되지 않기 때문에 프라이버시 침해를 막을 수 있다.

(a) (b)

그림 6. 1레벨 접근의 결과영상
(a) 배경영상, (b) 내·외부인 출입
Fig. 6 Result image of 1 level access
(a) background image, (b) internal personnel entrance with external personnel



(a) (b)

(c) (d)

그림 7. 2레벨 접근의 결과영상
(a) 배경영상, (b) 내부인 출입, (c) 외부인 출입,
(d) 내·외부인 출입
Fig. 7 Result image of 2 level access
(a) background image, (b) internal personnel entrance, (c) external personnel entrance, (d) internal personnel entrance with external personnel

그림 7은 시스템에 2레벨 접근의 결과 영상이다. 그림 7(a)와 같이 배경영상을 등록하게 된다. 이후 사용자는 그림 7(b)와 같이 RFID 리더기가 설치된 영역을 노란색 블록으로 설정할 수 있다. 이때 ID-tag를 소유한 내부인이 출입하게 되면 시스템은 대상을 판별하여 파랑색 블록으로 표시해준다. 그림 7(c)는 ID-tag를 소유하지 않은 외부인이 출입 했을 때 빨강색 블록으로 표시해준 것이다. 제안하는 시스템은 대상의 ID-tag의 소유여부에 관계없이 항상 스크램블링을 해준다. 그림 7(d)에서와 같이 스크램블링에 의해 대상의 정확한 신원을 확인할 수 없었지만 대상의 내·외부인은 판단할 수 있었다. 이때 ID-tag는 대상의 상세한 신원정보를 얻기 위한 것이 아니라 단지 내·외부인을 판단하기 위해 이용되기 때문에 ID-tag에 의한 프라이버시 침해는 발생하지 않는다.

그림 8은 시스템에 3레벨 접근일 때의 결과 영상으로 어떠한 프라이버시 보호 처리도 적용되지 않은 현재영상을 그대로 보여준다. 이는 범죄와 같은 위급한 상황에 대상의 정보를 정확하게 확인해야 하는 경우만 이용된다.

(a) (b)

그림 8. 3레벨 접근의 결과영상
(a) 배경영상, (b) 내·외부인 출입
Fig. 8 Result image of 3 level access
(a) background image. (b) internal personnel entrance with external personnel

V. 결론

본 논문에서는 프라이버시 보호와 감시로써의 기능을 동시에 만족할 수 있는 비디오 감시시스템 방법을 제안하였다. 제안한 방법은 접근레벨에 따른 프라이버시의 강도를 조절함으로써 감시자나 감시시스템과 관계없는 일반인에 의한 프라이버시 침해를 줄일 수 있었고, RFID 시스템을 이용하여 대상의 내·외부인을 구분함으로써 프라이버시 보호 처리된 화면에서도 감시자가 빠르고 정확하게 내·외부인을 구분할 수 있었다. 또한, 감시카메라에서 대상이 모두 프라이버시 보호가 되었을 때 감시자가 해야 할 감시로써의 임무를 수행하기에 적합함도 확인하였다.

제안하는 시스템은 한 대의 카메라에 한 대의 RFID 리더기를 설치를 해야 한다는 문제점을 가진다. 향후에는 한 대의 RFID 리더기를 이용하여 대상의 내·외부인을 판단·저장한 후 저장된 정보를 바탕으로 다수의 카메라에서 원거리 얼굴인식이나 행동인식 등을 이용하여 내·외부인을 판단할 수 있는 시스템으로 확장할 계획이다.

참고문헌

[1] M. Langheinrich, "Privacy invasions in ubiquitous computing," In Proc. Workshop on Socially-Informed Design of Privacy Enhancing Solutions in Ubiquitous Computing, Oct. 2002.

[2] 이철호, "Privacy protection and RFID," 한국콘텐츠학회 2006 추계종합학술대회 논문집, vol. 4, pp. 443-446, 2006.

[3] A. Westin, "Privacy and freedom," New York: Atheneum, 1967.

[4] Y. Chang, R. Yan, D. Chen, and J. Yang, "People identification with limited labels in privacy-protected video," In *Proc. IEEE Int. Conf. Multimedia and Expo*, pp. 1005-1008, July 2006.

[5] S. Tansuriyavong, and S. I. Hanaki, "Privacy protection by concealing persons in circumstantial video image," In *Proc. Perceptive User Interfaces*, pp. 1-4, 2001.

[6] R. Venkatesh Babu, and A. Makur, "Object-based surveillance video compression using foreground motion compensation," *IEEE Control, Automation Robotics and Vision*, pp. 1-6, Dec. 2006.

[7] F. Matusek, and R. Reda, "Efficient secure storage of privacy enhanced video surveillance data in intelligent video surveillance systems," In *Proc. IEEE Int. Symposium on Computer and Information Sciences*, vol. 23, pp. 1-5, Oct. 2008.

[8] I. Kitahara, K. Kogure, and N. Hagita, "Stealth vision for protecting privacy," In *Proc. Int. Conf. Pattern Recognition*, vol. 4, pp. 404-407, 2004.

[9] I. Kitahara, "Interactive video surveillance by using environmental and mobile cameras," *IEEE Automation Congress*, pp. 1-6, Oct. 2008.

[10] I. Martinez-Ponte, X. Desurmont, J. Meessen, and J. Delaigle, "Robust human face hiding ensuring privacy," In *Proc. Int. Workshop on Image Analysis for Multimedia Interactive Services*, 2005.

[11] F. Dufaux, M. Ouaret, Y. Abdeljaoued, A. Navarro, F. Vergnenegre, and T. Ebrahimi, "Privacy enabling technology for video surveillance," In *Proc. SPIE Mobile Multimedia/Image Processing for Military and Security Applications*, vol. 6250, May 2006.

[12] F. Dufaux, and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 18, no. 8, pp. 1168-1174, Aug. 2008.

[13] J. Schiff, M. Meingast, Deirdre K. Mulligan, S. Sastry, and K. Goldberg, "Respectful cameras: Detecting visual markers in real-time to address privacy concerns," *IEEE Intelligent Robots and Systems*, pp. 971-978, Oct. 2007.

[14] L. Bourdev, and J. Brandt, "Robust object detection via soft cascade," In *Proc. of IEEE Conf. Computer Vision and Pattern Recognition*, vol. 2, pp. 236-243, June 2005.

[15] D. Comaniciu, V. Ramesh, and P. Meer, "Kernel-based object tracking," *IEEE Trans. Pattern Analysis Machine Intelligence*, vol. 25, no. 5, pp. 564-575, 2003.

[16] I. Matthews, T. Ishikawa, and S. Baker, "The template update problem," *IEEE Trans. Pattern Analysis Machine Intelligence*, vol. 26, no. 6, pp. 810-815, 2004.

[17] 문해민, 김종구, 임성진, 반성범, "프라이버시 보호 기능을 제공하는 RFID 기반 감시카메라 시스템에 관한 연구," 정보통신분야학회 합동학술대회, pp. 235-237, Nov. 2008.

저자소개

문해민(Hae-Min Moon)

2009년 조선대학교 공학사
2009년~현재 조선대학교
정보통신공학과 석사과정

※관심분야 : 영상압축, 영상처리, 워터마킹

반성범(Sung Bum Pan)

1991년 서강대학교 공학사
1995년 서강대학교 공학석사
1999년 서강대학교 공학박사
2005년 한국전자통신연구원
정보보호연구단
생체인식기술연구팀 팀장

2005년~현재 조선대학교 제어계측로봇공학 조교수
※관심분야 : 바이오 인식, 영상처리,
VLSI 신호처리