영상 프라이버시 보호 메커니즘에 관한 연구★

김민수* · 김종민* · 김상춘**

요 약

ICBM 산업내의 IoT기반 영역 중에서 보안(Safety)의 경우, 공공분야 뿐만 아니라 국민안전 체감도가 안전에 대한 불안감이 극에 달하면서, 재난 및 안전 관리와 관련하여 보안 서비스에 대한 수요가 증가하고 있다. 이와 같이 안전을 위한 하나의 보안 서비스로서 CCTV를 활용하여 사회질서 유지, 범죄예방 등의 목적을 위해 설치·운영되고 있으며, 특히 녹화된 영상이 범죄의 결정적 증거로 제시되면서 보급이 급증하고 있는 추세이다. 하지만 영상정보처리기의 역기능으로써 본래의 목적을 그대로 수행하면서 의도하지 않은 개인의 정보가 유출되거나 이러한 기술들을 악용할 경우 개인 프라이버시 침해 우려가 매우 높기 때문에, 영상 프라이버시 보호를 위해 다각적으로 결합된 메커니즘에 대한 연구가 필요하다.

A Study on the Video Privacy Protective Mechanism

Minsu Kim* · Jongmin Kim* · Sang-Choon Kim**

ABSTRACT

In case of security of IoT-based areas in ICBM industry, the anxiety about safety goes to extremes in public and national safety area, so that the demand for security service related to disaster/safety management is increasing. Like this, as a security service for safety, CCTVs are installed/operated for the purpose of maintenance of public order and crime prevention. Especially, as the recorded images are presented as crucial evidences of crimes, they are rapidly inc reasing. However, as adverse effects of CCTVs, it is highly possible to unintentionally leak personal information in th e process of performing the original purpose, or to violate someone's privacy in case when such technologies are abu sed. Therefore, it would be necessary to have researches on the multilaterally-combined mechanism for the protection of image privacy.

Key words : ICBM, Privacy, CCTV, Video Surveillance, Security Codec

접수일(2017년 11월 30일), 수정일(1차: 2017년 12월 22일), 게재확정일(2017년 12월 29일)

★ 본 논문은 2017년도 강원대학교 대학회계 학술연구조성비로 연구하였음.(관리번호-620170050)
This study was supported by 2017 Research Grant from Kangwon National University.(No. 620170050)

* 경기대학교 융합보안학과
** 강원대학교 정보통신공학부(교신저자)

1. 서 론

지식정보사회로의 급속한 전환은 IT(Information Technology) 기술의 발전이 바탕이 되어 사회적, 경제적으로 큰 변화를 가져오게 되었다. 특히 IT 기술의 특성인 네트워크화, 지능화, 내재화를 활용하여 기술 및 산업간 융합화가 이루어지면서 ICBM(IoT, Cloud, Big Data, Mobile)을 새로운 성장동력으로 주목받는 가운데 주요국은 국가 경쟁력의 핵심으로 인식하고, 시장 주도권 확보에 주력하고 있는 실정이다.

사물인터넷인 IoT(Internet of Things) 영역의 경우 조선, 의료 에너지, 자동차, 기계, 보안 등 다양한 분야에 활용되면서 융합산업의 새로운 전기를 마련하게 되었으며, 지금까지 추진되어 오던 다양한 융합산업의 패러다임이 변화되고 있다.

이러한 ICBM 산업내의 IoT기반 영역 중에서 보안(Safety)의 경우, 공공분야 뿐만 아니라 국민안전 체감도가 안전에 대한 불안감이 극에 달하면서, 재난 및 안전 관리와 관련하여 보안 서비스에 대한 수요가 증가하고 있다.

이와 같이 안전을 위한 하나의 보안 서비스로서 CCTV를 활용하여 사회질서 유지, 범죄예방 등의 목적을 위해 설치·운영되고 있으며, 특히 녹화된 영상이 범죄의 결정적 증거로 제시되면서 보급이 급증하고 있는 추세이다. 영상정보처리기 영역의 경우 CCTV 이외에도 차량에 설치된 블랙박스, 드론(Drone), Google Glass 등을 통해 얻어진 영상정보를 연계하여 각종 범죄 수사에 적극적으로 활용하고 있다.

하지만 CCTV를 포함하는 크라우드 영상 디바이스를 사용하여 정보주체를 촬영하고, 저장하는 것은 정보주체의 영상정보에 대한 수집 및 처리, 열람, 정정 등의 권리를 정보주체가 모르도록 제한하여 자기정보에 대한 통제를 무력화 할 수 있으며, 개인의 사생활 침해로 이어질 가능성이 높다.

따라서 영상정보처리시스템의 역기능으로써 본래의 목적을 그대로 수행하면서 의도하지 않은 개인의 정보가 유출되거나 이러한 기술들을 악용할 경우 개인프라이버시 침해 우려가 매우 높기 때문에, 영상 프라이버시 보호를 위해 다각적으로 결합된 메커니즘에 대한 연구가 필요하다.

2. 관련 연구

2.1 선행연구의 분석

영상정보에 대한 프라이버시 보호에 있어 기술적 요구사항에 대한 선행연구를 살펴보면, 개인의 프라이버시를 침해할 수 있는 소지가 가장 높은 얼굴영상에 대하여, 마스킹(masking) 기법을 이용하여 개인 식별이 되지 않도록 하여야 한다. 이러한 마스킹 기법의 전제조건으로 입력된 영상으로부터 얼굴을 정확하게 검출할 수 있는 기술이 요구되어 진다. 또한 합법적인 이유로 원본으로 복원해야 할 경우 완벽한 복구가 어렵다는 단점이 존재한다[1].

스크램블링(scrambling) 기법을 이용한 영상 프라이버시 보호는 영상에 대한 프라이버시 보호 기법을 적용하였다 하더라도, 합법적으로 영상을 복원하여 개인을 식별해야 하는 경우 역 스크램블링 기법을 사용하여 영상을 보여주거나 저장하게 된다. 또한 스크램블의 강도를 조절할 수 있어 다양한 용도로 프라이버시 보호를 수행할 수 있지만, 스크램블을 위한 키가 유출될 경우 정보가 유출될 수 있는 단점이 존재한다[2].

비식별처리(De-identification) 기법을 이용한 영상 프라이버시 보호는 영상정보에서 사람을 검출하여 신원확인을 할 수 없도록 변형하는 기법이다[3][4]. 일반적인 마스킹 기법의 경우는 대상의 정보를 완전히 변형시킴으로써 감시대상자가 위험한 물건을 소지하거나 비정상적인 행위에 대한 인식이 어렵다. 이에 반해 본 기법은 영상정보의 손실을 최소화하여 감시 기능을 유지할 수 있도록 한다. 또한 비식별처리(De-identification) 카메라를 이용한 영상 프라이버시 보호는 지능형 영상정보처리장치에 프라이버시 보호 기능이 내장된 것으로써 영상처리를 위해 수상부로 전송 시 공격자에 의해 영상이 중간에 가로챌 수 있는 위험을 줄일 수 있다[5][6].

암호화(Encryption) 기법을 이용한 영상 프라이버시 보호는 CCTV 분야에서 효율성이 높은 H.264 코덱에 프라이버시 보호를 위해서 플렉서블마키로블럭 순서 기법(FMO, Flexible Macroblock Ordering)을 이용하게 된다. 실시간 영상데이터에 대하여 암호화 및 복호화를 수행할 수 있으며, CCTV 표준 포맷에 대하여 적용할

수 있는 장점이 있다[7].

이와 같이 영상정보에 대한 프라이버시 보호를 위한 기술적 접근방식에 대하여 각 기법별로 비교하면 <표 1>과 같다.

<표 1> 영상정보 프라이버시 보호 기법 비교

구 분	마스킹	스크램블	비식별처리	암호화
프라이버시 영역	주로 얼굴	주로 얼굴	대상자 전체	주로 얼굴
복원 유무	무	유	유	유
암호화 유무	무	유	무	유

2.2 영상정보 프라이버시 요구사항

영상정보시스템에서 위협에 따른 프라이버시 보호 메커니즘을 위한 보안 요구사항은, 정보통신단체표준(TTAS)의 영상정보 프라이버시 요구사항[8]을 바탕으로 살펴보았으며 <표 2>와 같다.

<표 2> 영상정보 프라이버시 요구사항

구 분	내 용
영상정보 암·복호화	· 촬영된 영상을 영상감시관제서버로 안전하게 전송하기 위한 암호화 기법 적용 · 클라이언트의 영상 요청 시 암호화 기법 적용 · 공인인증서, 공개키, 대칭키 기반의 암호화를 적용
영상정보 송·수신	· 데이터 송·수신을 위해서는 공인인증서, 공개키, 대칭키 등을 기반으로 한 SSL/TLS 등과 같은 세션키 유도 및 안전한 채널 설정
얼굴 영역 검출	· 적합한 얼굴 영역 검출 알고리즘을 기반으로 얼굴 영역 검출 과정을 수행함으로써 프라이버시를 보호 · 지식기반 방법(knowledge-based methods), 특징기반 방법(feature-based methods), 템플릿매칭 방법(template-based methods), 외형기반 방법(appearance-based methods) 등
프라이버시 보호 및 해제	· 개인 영상 정보에 대한 프라이버시를 제공하기 위해서는 얼굴 영역 검출 기법을 통해서 검출된 얼굴 영상에 적합한 프라이버시 보호적용 알고리즘 사용 · 프라이버시 보호적용 기법 : 암호화, 스크램블링, 마스킹 방법 등
관리 및 접근제어	· 기기 식별 및 인증 등을 제공하는 X.509v3 기기인증 기법을 적용

3. 영상정보 프라이버시 보호 메커니즘

3.1 영상정보 시스템의 프라이버시 보호 메커니즘

CCTV 시스템은 위에서 언급한 바와 같이 렌즈를 통해 들어온 피사체의 형상을 촬상판에서 전기신호로 바꿔주는 촬상부, 영상정보를 CCTV, 영상감시관제센터, 클라이언트 간의 정보 전송이 이뤄지도록 하는 전송부, 영상정보 처리를 위해 전송된 영상 신호를 수신 및 재생하는 수상부, 처리된 정보를 사용자에게 제공하는 클라이언트로 이루어져 있다.

촬상부는 CCTV, 크라우드 디바이스를 포함하는 물리적 장치부로서 물리적 공격 또는 서비스 거부 공격을 통한 시스템 기능 마비, 무단접속을 통한 영상정보 유출로 인한 위협이 존재한다.

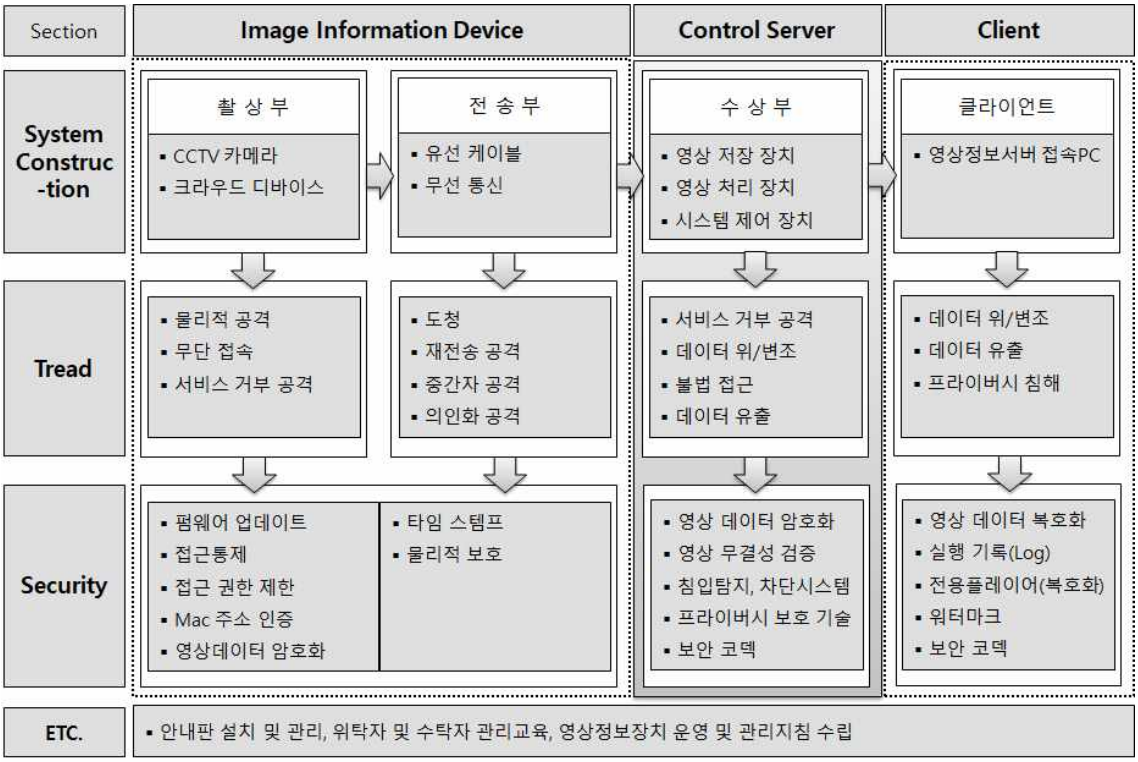
전송부는 영상정보를 전송하는 유·무선 통신을 말하며, 통신 과정 중 영상의 정보 도청, 정당한 사용자로 인식하도록 하여 전송된 내용을 다시 전송하도록 하는 재전송 공격, 중간에 전송되는 정보를 조작하는 중간자 공격 등으로 인한 데이터 유출의 위험이 있다.

촬상부와 전송부에 대해 적용 가능한 보안 기법은 서비스 거부 공격과 같은 기능 무효화 방지를 위한 촬상부 기기의 펌웨어 업데이트, 접근 권한 외의 접근 요청에 대해 통제하는 접근통제, 접근권한 관리자의 역할에 따라 접근 가능한 영역을 제한하는 접근 권한 제한, 허가된 장치만이 접근 가능하도록 하는 Mac 주소 인증, 전송부를 통해 수상부로 전해지는 과정에서 해킹에

의한 데이터 유출을 방지하기 위한 영상 데이터 암호화, 데이터가 특정 시간에 존재하고 변경되지 않았음을 증명하는 타임스탬프, 외적 충격으로부터 촬상부 및 전송부를 보호하는 물리적 보호 등을 사용할 수 있다.

수상부는 영상 저장 장치, 영상 처리 장치, 시스템 제어 장치 등의 영상정보 제어계통의 시스템을 말하여, 서비스 거부 공격을 통한 기능 마비, 데이터의 위/변조를 통한 데이터의 무결성 훼손, 데이터 유출을 통한 기밀성 훼손, 제 3자의 영상정보로 인한 프라이버시 침해 위협이 존재한다. 이를 대비하기 위해서는 촬상부로부터 전송받은 영상 데이터의 수정을 위한 복호화 과정 및 수정이 끝난 데이터의 보관 및 전송과정에서 영상 데이터의 보안을 보장하는 영상 데이터 암호화, 데이터 위/변조에 대해 무결성을 보장하는 영상 무결성 검증, 허가되지 않은 제 3자로부터의 접근을 제어하는 침입탐지 및 차단 시스템, 영상내 제 3자에 대한 마스킹 등의 기법을 통한 영상 프라이버시 적용, 인증을 통해 영상을 열람할수 있도록 하는 보안 코덱의 적용이 요구된다.

클라이언트는 영상정보를 저장한 서버에 접속 가능한 디바이스를 의미하며, 비인가된 사용자의 영상데이터 서버에 접속하여 수정 및 삭제를 통한 데이터 위/변조, 다운받은 영상데이터의 타 저장장치로의 전송을 통한 데이터 유출, 영상정보에 존재하는 프라이버시의 침해 위협이 있으며, 이를 위해 적용 가능한 보호 기법은 수상부로부터 전송받은 암호화된 영상 데이터의 복호화를 통해 최종 사용자만이 영상을 성공적으로 전송받도록 하는 영상 데이터 복호화, 수상부 접속기록에 대해 기록을 남겨 부인 방지를 적용하는 실행기록 저장, 허가받은 전용의 플레이어에서만 영상이 재생되도록 하는 전용 플레이어, 영상데이터 및 접근자에 대한 정보를 영상 내부에 포함시키는 워터마크 등의 기법이 존재한다.



(그림 1) 영상정보시스템 프라이버시 보호 메커니즘

3.2 프라이버시 보호 메커니즘 세부내용

3.2.1 펌웨어 업데이트

하드웨어 내부의 제어 부분에 만들어진 저장 공간에 논리 회로의 기능을 보강하거나, 대신할 수 있는 프로그램을 넣도록 한 펌웨어는 지속적인 업데이트를 통해 보안 정책을 강화할 수 있으며 기기의 성능까지도 향상시킬 수 있다.

3.2.2 접근통제

이용자의 영상 데이터에 대한 접근을 감시 및 식별하고, 영상 데이터의 접근 유무를 기록하며 영상보안시스템 운영정책에 근거하여 접근자의 승인 혹은 거부함으로써 불법적인 데이터접근 및 보안위협을 예방하는 하드웨어 및 소프트웨어를 의미한다.

3.2.3 접근 권한 제한

영상 데이터에 대해 접근이 인가된 접속자에 대해 접근 권한을 부여하되, 접속자마다 접근 영역을 제한함으로서 접속자의 접근 권한을 벗어나는 영상 데이터에 대한 요청을 거부하도록 하여 영상 데이터의 무분별한 유출을 방지한다.

3.2.4 Mac 주소 인증

Mac 주소는 하나의 장치가 가지는 고유한 이더넷의 물리적 주소이기에 사전에 정의된 Mac 주소 이외의 접근 요청에 대해 거부할 수 있으며, 접속하는 기기의 정당성 인증이 가능하다.

3.2.5 영상 데이터 암호화

영상 데이터는 촬상부에서 디지털 신호로 변환하여, 전송부를 통해 수신부로 전송하게 되는데, 이 과정에서 제 3자의 사이버 공격에 의해 데이터 유출의 염려가 있으므로, 데이터를 전송하는 부에서 데이터를 암호화하여, 데이터를 수신하는 부에서 복호화하는 과정이 요구된다. 이를 통해 데이터 전송과정에서의 보안성을 보장한다.

3.2.6 타임 스탬프

타임스탬프는 제 3의 신뢰할 수 있는 기관이 시각정보를 부여하는 방식으로 과거 시각으로의 재발급이 불가능하므로 영상데이터가 특정 시각에 존재하고 있었다는 존재의 증명 및 그 시각 이후 데이터의 변경이 없었음을 증명하는 내용 증명의 역할을 가진다.

3.2.7 침입 탐지 및 차단 시스템

비인가된 침입자의 시스템 접근, 데이터의 위/변조 등 의심스러운 행위에 대한 감시 및 침입자의 조기 발견, 실시간 처리를 위해 침입 탐지 시스템을 적용할 수 있으며, 침입 차단 시스템을 이용하여 외부 네트워크로부터 내부 네트워크로 침입하는 네트워크 패킷에 대해 차단을 적용함으로서 비인가자에 대한 접근을 제한할 수 있다.

3.2.8 프라이버시 보호 기술

프라이버시 보호 기술은 영상 데이터 중 프라이버시가 포함되는 영상 정보에 대해 마스킹, 스크램블링, 비식별처리, 암호화 등의 기법을 적용하여 피촬영자를 인식할 수 있는 정보에 대해 타인 및 시스템이 인식하지 못하도록 영상 데이터를 변경하고, 접근이 인가된 사용자에 의해서만 원 영상으로의 복원 기능을 수행하여 원래의 이미지를 제공하도록 한다.

3.2.9 실행 기록(Log)

영상 데이터의 전송, 보관, 실행, 삭제 등의 정보를 시간에 따라 저장함으로서 실행 과정 중 영상 데이터에 대한 접근 기록 및 수정 기록을 확인 할 수 있어 차후 포렌식 수사기법에 이용되어 사이버 공격 및 데이터 유출에 대해 공격자 또는 유출자를 찾는 자료로 이용된다.

3.2.10 전용 플레이어

전용 플레이어는 수신부로부터 전송받은 암호화된 영상 데이터에 대해 복호화 기능을 가진 영상 플레이어를 의미하며, 영상은 전용 플레이어를 가진 사용자에 한해서만 복호화되므로 제 3자에 의한 영상 유출 가능성을 낮출 수 있다.

3.2.11 워터마크

동영상에 영상의 데이터 및 사용자의 정보 등의 비

밀 정보를 영상에 삽입하여 관리하는 기술로서 삽입된 영상 정보의 분석을 통한 위/변조 판별, 영상에 삽입된 사용자의 정보를 통한 불법 복제 추적 등의 분야에 사용된다.

3.2.12 보안 코덱

영상정보 프라이버시 보호를 위한 메커니즘 설계는 영상처리 침해사례, 영상처리 보호기술, 상용제품 기능 및 성능을 분석한 결과 영상에 대한 암호화 기술을 기반으로 마스킹 기법, 스크램블링 기법, 비식별처리 기법 등의 기존 프라이버시 보호 기술을 활용하여 영상 등급화를 통해 정보주체의 자기영상정보 열람권 보장부터 하가된 제3자의 영상확인을 할 수 있다.

또한, 열람에 대한 인증을 위해 전용 코덱을 개발하여 영상데이터에 대한 인증 절차를 진행하여 개인영상정보의 안전성을 확보하여, 영상정보의 목적 외 이용 및 제공을 제한할 수 있다. 그리고 영상에 대한 파기 기간에 대해 인증절차를 진행하는 서버에서 관리할 수 있어야 한다.

4. 결 론

CCTV를 포함하는 크라우드 영상 디바이스를 사용하여 정보주체를 촬영하고, 저장하는 것은 정보주체의 영상정보에 대한 수집 및 처리, 열람, 정정 등의 권리를 정보주체가 모르도록 제한하여 자기정보에 대한 통제를 무력화 할 수 있으며, 개인의 사생활 침해로 이어질 가능성이 높다.

현재 CCTV는 기업은 물론 가정까지도 적용이 되는 대중적인 물리 보안 장치로서 손쉬운 접근성으로 인해 허가하지 않은 정보주체에 대한 촬영정보가 증가하고 있다. 영상 감시시스템이 IP 환경에서 사용할 수 있도록 변화함으로서 기존의 인터넷 해킹 기법을 적용하여 영상 정보를 유출하거나 위/변조하는 방법이 가능해짐에 따라 증가하고 있는 촬영정보에 대한 보안 문제가 부각되고 있으며, 촬영주체에 대한 인권 보장을 위한 보안 방법이 요구된다.

촬영주체에 대한 보안 방안으로 현재 사용되는 것은 영상장치에서 촬영된 정보 내의 얼굴 영역을 검출하고, 검출된 영역을 영상처리하여 타인이 촬영주체에 대해 알 수 없도록 하는 방법을 사용하며, 영역에 대한 보안 방안으로는 사생활과 관련된 영역을 부분적으로 촬영하지 못하도록 하는 방법이 사용된다.

영상 감시 장치는 크게 촬상부, 전송부, 수상부, 클라이언트로 이루어져 있으며, 각각의 영역에 대한 보안이 요구된다. 촬상부는 영상감시 시스템 중에서도 촬영기기와 같은 물리적 장치부로 직접 접근 혹은 직접적 피해에 대한 물리적 보안이 요구되며, 전송부는 유선 혹은 무선을 통한 통신단계로 전송과정 중의 무결성이 보장되어야 한다. 영상 정보를 처리하는 수상부는 영상 정보를 처리하고 저장하는 단계로서 시스템 유출에 대한 대비 및 무효화를 목적으로 하는 공격을 차단해야 한다. 클라이언트는 사용자가 수상부로부터 영상 데이터를 전송받는 디바이스로서 디바이스에 전송된 영상의 유출 및 위/변조에 대한 보안이 적용되어야 한다.

현재 보급되어 있는 대다수의 영상감시 장치는 영역에 대한 감시의 기능을 우선적으로 하며, 감시 영역 내 정보주체에 대한 프라이버시 보안에 대해서는 많이 적용이 되지 않은 상태이다. 하지만 영상감시 시스템의 프라이버시 문제는 개인주의적 사회가 되어감에 따라 타인에 대한 불신의 증가로 인해 증가되는 영상감시 시스템의 증가에 따라 지속적으로 제기되어오던 것으로 영국에서는 이를 해결하기 위하여 영상감시 시스템 구입 시 필수적으로 프라이버시 마스킹을 적용할 것을 요구하고 있으며, 미국의 국토안보부에서는 프라이버시 보호를 위한 CCTV 설치 및 운용에 대한 가이드라인을 발표하였다.

이는 영상감시 시스템에 있어 프라이버시 보안은 필수적이라는 것을 단적으로 보여주는 예시로서 영상정보 내의 정보공개가 요구되는 대상을 제외한 촬영주체에 대한 프라이버시가 보장이 되어야만 국민을 대상으로 공개하는 사회안전서비스가 성립될 수 있을 것이다.

참고문헌

[1] A. Frome, et. al., “Large-scale Privacy P rotection in Google Street View,” IEEE In ternational Conference on Computer Visio n (ICCV), pp. 2373-2380, 2009.

[2] F. Dufaux, T. Ebrahimi, “Scrambling for P rivacy Protection in Video Surveillance Sy stems,” IEEE Trans. on Circuits and Syst ems for Video Technology, Vol. 18, No.8, pp. 1168-1174, 2008.

[3] J. Schiff, M. Meingast, Deirdre K. Mullig an, S. Sastry, and K. Goldberg, "Respectf ul Cameras: Detecting Visual Markers in Real-time to Address Privacy Concerns", in Proc. IEEE Int. Conf. Intelligent Robots and Systems, pp. 971-978, Oct. 2007.

[4] E. Newton, L. Sweeney, and B. Malin, "Pr eserving Privacy by De-identifying Facial Images", Carnegie Mellon University, Tec hnical Report CMU-CS-03-119, 2003.

[5] P. Agrawal, P.J. Narayanan, “Person De-i dentification in Videos,” IEEE Trans. on Circuits and Systems for Video Technolog y. Vol. 21, No.3, pp. 299-310, 2011.

[6] Mrityunjay, P.J. Narayana, “The De-identi fication Camera, Conference on Computer Vision,” Pattern Recognition, Image Proce ssing and Graphics, pp. 192-195, 2011.

[7] F. Peng, X. Zhu, M. Long, “A ROI Privac y Protection Scheme for H.264 Video Bas ed on FMO and Chaos,” P. Agrawal, P.J. Narayanan, IEEE Trans. on Information F orensics and Security, Vol. 8, No.10, pp. 1 688-1699, 2013.

[8] “얼굴 영역 검출을 이용한 CCTV 영상 정 보 프라이버시 보호를 위한 보안 요구 사 항”, 한국정보통신기술협회(TTA), 2010.

〔저자소개〕

김 민 수 (Minsu Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : fortcom@hanmail.net

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : dyuo1004@gmail.com

김 상 춘(Sang-Choon Kim)

1999년 8월 충북대 이학박사
1983년 ~ 2001년: ETRI 선임
2001년 ~ 2010년: ETRI초빙연구원
2001년 ~ 현 강원대학교 정교수

e-mail : kimsc@kangwon.ac.kr