Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.97

영상감시 시스템에서의 얼굴 영상 정보보호를 위한 기술적·관리적 요구사항*

신 용 녀,[1†] 전 명 근[2‡]
[1]한양사이버대학교, [2]충북대학교

Technical and Managerial Requirements for Privacy Protection Using Face Detection and Recognition in CCTV Systems*

Yong-Nyuo Shin,[1†] Myung Geun Chun[2‡]
[1]Hanyang Cyber University, [2]Chungbuk National University

요 약

공공의 안전을 위한 영상 감시 시스템의 도입이 활발해짐에 따라 많은 공공시설이나 장소에 설치되어 운영되고 있다. 최근 CCTV의 성능이 좋아짐에 따라, CCTV 영상으로부터 획득된 사람의 얼굴 정보를 바탕으로 얼굴 인식 등을 통해 자동화된 처리를 시도하는 기술들이 개발되고 있다. 하지만, 이러한 기술들이 악용될 경우 중대한 개인의 프라이버시 침해 우려가 있다. 특히, 최근에는 특정 공간에 설치된 컴퓨터와 연결시켜 카메라에 찍힌 영상을 인터넷을 통해 실시간으로 보여주는 정보제공서비스까지 등장하고 있고, 시행중인 개인정보보호법에서 바이오인식정보에 대하여 안전성 확보조치 기준을 고시하고 있다. 이에, 본 논문에서는 영상 감시시스템에서 개인영상 정보보호를 위한 기술적·관리적 관점에서 영상감시 시스템에서의 개인 영상 정보보호 요구사항을 도출하고자 한다.

ABSTRACT

CCTV(Closed Circuit television) is one of the widely used physical security technologies and video acquisition device installed at specific point with various purposes. Recently, as the CCTV capabilities improve, facial recognition from the information collected from CCTV video is under development. However, in case these technologies are exploited, concerns on major privacy infringement are high. Especially, a computer connected to a particular space images taken by the camera in real time over the Internet has emerged to show information services. In the privacy law, safety measures which is related with biometric template are notified. Accordingly, in this paper, for the protection of privacy video information in the video surveillance system, the technical and managerial requirements for video information security are suggested.

Keywords: CCTV, Face Detection and Recognition, Security Requirements, Privacy

I. 서 론

CCTV는 가장 널리 사용되는 물리 보안 기술 중 하나로 특정 위치에 설치되어 다양한 목적으로 활용되고 있는 영상 수집 장치이다. CCTV 영상에서 바이오인식 기술의 하나인 얼굴 영역 검출을 통해 개인 정보를 보호하기 위해서는, CCTV, 영상 감시 관제 서버, 클라이언트로 이루어진 요소들과 그에 속한 여러 가지

접수일(2013년 10월 1일), 수정일(2013년 12월 4일), 게재확정일(2013년 12월 4일)
* 본 연구는 한국인터넷진흥원의 모바일 바이오인식 신융합 기술 표준 개발사업의일환으로 수행하였음. [2013-PM10-17]
† 주저자, ynshin@hycu.ac.kr
‡ 교신저자, mgchun@chungbuk.ac.kr (Corresponding author)

모듈이 필요하다. 최근 CCTV의 성능이 좋아짐에 따라, CCTV 영상으로부터 획득된 사람의 영상 정보를 바탕으로 얼굴 인식 등을 통해 자동화된 처리를 시도하는 기술들이 개발되고 있다.

그러나, 이러한 기술들이 악용될 경우 중대한 개인의 프라이버시 침해 우려가 있다. 이를 방지하기 위해서, CCTV에서 얻어지는 사용자 얼굴 정보를 바이오인식의 일환인 얼굴 영역 검출을 통해 획득하여, 누군지 알아볼 수 없게 모자이크 혹은 스크램블링 처리를 하여 개인 정보가 노출되지 않도록 저장한다. 또한, 역스크램블링 처리 등 응용 활용이 가능한 프라이버시 보호를 위한 기술적 요구사항이 필요하다[1][2].

이를 통해 CCTV의 본래의 목적을 그대로 수행하면서도 의도하지 않은 개인의 영상정보를 유출을 막을 수 있어 개인 정보 보호에 도움을 줄 수 있다. 이에 본 논문에서는 영상 감시시스템에서 개인영상 정보보호를 위한 기술적·관리적 대책을 제시함으로써 영상감시 시스템에서의 개인 영상 정보보호 요구사항을 도출하는 것을 목적으로 한다. 이를 위하여 2장에서는 영상 프라이버시 보호를 위한 최근의 연구 기법을 살펴보고, 3장에서 보안 위협을 기술하고 이를 토대로 기술적·관리적 요구사항을 제시하며, 4장에 결론을 제시하였다.

II. 영상 감시시스템에서의 개인영상 정보보호를 위한 기술적 대책

2.1 마스킹 기법을 이용한 개인영상 정보보호

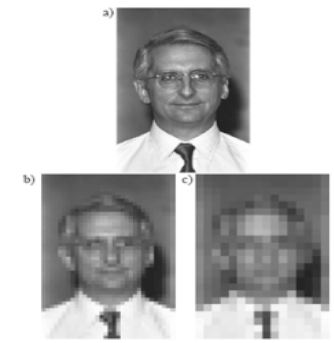
영상감시시스템에서 취득되는 영상이나, 이미 취득되어 저장되어 있는 영상에서 개인의 프라이버시를 침해 할 수 있는 소지가 가장 높은 것이 얼굴영상이다. 예를 들어, 특정 구역의 차량 출입을 감시하는 시스템의 경우, 자동차 이외의 개인을 식별할 수 있는 얼굴 영상 영역은 마스킹 기법을 이용하여 개인 식별이 되지 않도록 하여야 한다. 또한, 영상 처리를 이용하여 특정인을 감시 추적하는 경우에, 그 외 불특정 다수의 얼굴 영상은 (1)과 같은 영상처리 기법을 이용하여, 육안으로나 컴퓨터를 이용하여 개인 식별이 되지 않도록 마스킹 기법을 이용하여 처리하여야 한다.

주어진 블록사이즈(B*B)에 대해서 블록의 평균값을 이용하여 동일한 밝기 값으로 대체하거나 다음과 같이 주어지는 분산값(δ)에 따른 가우시안 평균필터

$$G(x,y)=\frac{1}{2\pi\sigma^2}e^{\frac{(x^2+y^2)}{2\sigma^2}} \quad (1)$$

등을 이용하여 Fig. 1과 같이 주어진 영상을 흐리게 만들어 개인 식별을 어렵게 하는 것이 마스킹 기법이다.

이러한 마스킹 기법의 적용을 위한 전제 조건으로는 입력된 영상으로부터 얼굴을 정확하게 검출할 수 있는 기술이 요구된다. 이러한 마스킹 기법의 단점으로는 한번 마스킹 된 영상으로부터 합법적인 이유로 인하여 본래의 영상을 복원해야할 필요성이 발생하는 경우, 이를 완벽하게 복구 할 수 없는데 있다. 그러나 비교적 구현이 용이할 뿐만 아니라, 한번 마스킹을 하여 놓으면 추가 적인 유출에 따른 프라이버시 피해가 없는 장점이 있다. 현재 Google Street View 등 상업용 시스템에서 적용되어 사용되고 있다[3].



(a) 원영상 (b) 블록사이즈 B=8 (c) 블록사이즈 B=16

(d) 가우시안 필터링 적용($\sigma=2$) (e) 가우시안 필터 ($\sigma=4$)

Fig.1. Personal image masking by blocking and blurring[4]

2.2 스크램블링 기법을 이용한 개인영상 정보보호

영상 감시 시스템의 특성상 취득된 영상의 개인 영상정보보호를 위한 조치를 취하였다 하더라도, 사후에 감시 시스템의 목적 달성을 위하여 원래의 영상을 복원하여 개인을 식별해야 하는 일이 발생 할 수 있다. 이러한 목적을 위해서는 Fig. 2와 Fig.3.과 같은 스

크램블 기법을 사용하여, 동영상을 보여주거나 저장한다[5].

본 기법의 장점은 표준 포맷 MPEG-4에서 프라이버시 영역을 추출하여, 스크램블 하더라도 합법적인 목적에 위해서 역스크램블이 가능하다는 점에 있다. 또한 스크램블의 강도를 조절할 수 있어, 단순 모니터링 용도에서, 정밀 인물 추정 용도에까지 사용될 수 있다. 그러나 스크램블을 위한 키가 유출될 경우 감추어졌던 프라이버시 정보가 유출될 수 있으므로 이를 위한 보안이 추가 적으로 요구된다.

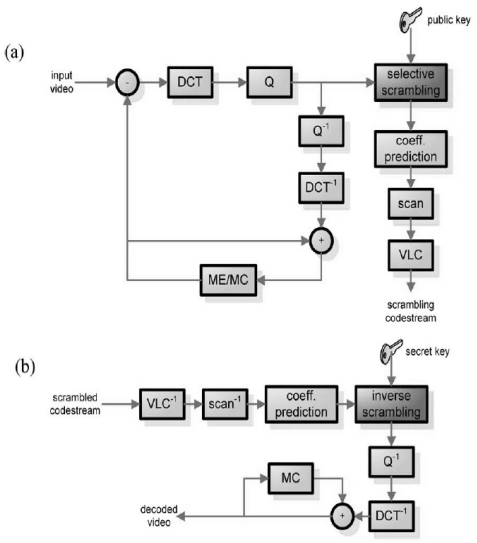


Fig.2. Scrambling scheme for image protection in MPEG-4 (a) Encoding (b) Decoding

Fig.3. Scrambling technique application for 'Hall Monitor' image

2.3 De-identification 기법을 이용한 개인영상 정보보호

De-identification 기법은 영상감시 시스템에서 사람을 검출한 후 이와 관련된 신원확인을 할 수 없도록 변형하는 기법을 말한다. 실루엣, 박스, 에지, 경계선을 이용한 단순한 마스킹 기법의 경우에는 대상의 정보를 완전히 변형시킴으로서 감시대상자가 위험한 물건을 소지하거나 비정상적인 행위를 취하더라도 감시자는 이를 인식할 수 없다. 그러나 Fig. 4.와 같은 De-identification 기법에서는 영상감시 시스템의 목적에 부합할 수 있도록, 영상정보의 손실은 최소화하고 감시 기능은 유지할 수 있도록 해야 한다[6].

즉, 사람의 동작이나 주변 상황에 대해서는 충분히 인지 할 수 있는 정보를 제공하여야 한다. 이때, 개인 영상 영역에 대해서 다음과 같은 분류기준을 가지고 처리한다. 첫째, 얼굴영역은 개인을 식별하는데 중요한 역할을 하므로, 얼굴을 검출하고 이를 식별 할 수 없도록 만드는데 주의해야 한다. 이와 더불어 인종이나 성별과 같은 정보가 개인의 프라이버시와 밀접하게 관련되어 있으므로 이를 시스템의 목적에 부합하도록 감추어야 한다. 둘째, 몸 전체의 실루엣과 걸음새는 동영상에 있어서 개인을 식별하는데 중요하게 사용될 수 있으므로 이를 식별할 수 없도록 해야 한다. 실루엣의 경우는 몸체의 모양을 확장하거나 축소하는 등의 변형을 가하여 식별 할 수 없도록 만든다. 걸음새의 경우는 실루엣의 시간적인 흐름에 따른 변화가 예측될 수 없는 형태로 변형되어야 한다.

Fig.4. Image protection by de-identification technique

2.4 암호화 기법을 사용한 H.264 비디오에서의 실시간 얼굴영상 프라이버시 보호

H.264는 비디오 코딩에 있어서 가장 널리 사용되는 코딩 기법 중의 하나이다. 영상의 질은 그대로 이

면서 다른 코딩 표준에 비해서 낮은 비트율를 보임으로서 저장이나 전송면에서 효율성을 기할 수 있다. 이러한 이유로 CCTV 분야에서 각광을 받고 있다.

H.264 비디오에서의 특정 관심 영역의(Region of Interest)의 프라이버시 보호를 위해서 플렉서블 마크로블럭 순서기법(FMO, Flexible Macroblock Ordering)을 이용한 방법이 제안되었다[7]. H.264에서는 하나의 프레임이 최대 8개의 slice 그룹으로 나누어 지고, 각각은 slice 그룹 ID를 갖는다. 모두 7가지의 FMO 매칭 타입을 갖는데, 위의 기법은 FMO 타입-6에 ROI를 정의하도록 하였다. Fig. 5.와 같이 다양한 실시간 비디오 영상에 대해서 ROI영역을 암호화 하고, 이를 복호화 하였을때 완벽하게 복원되는 것을 알 수 있다. 이러한 기법의 장점은 현재 널리 사용되고 있는 CCTV 표준 포맷에 대해서 실시간으로 특정 얼굴영상 영역을 암호화 하고 필요에 따라 복호화 할 수 있는데 있다.

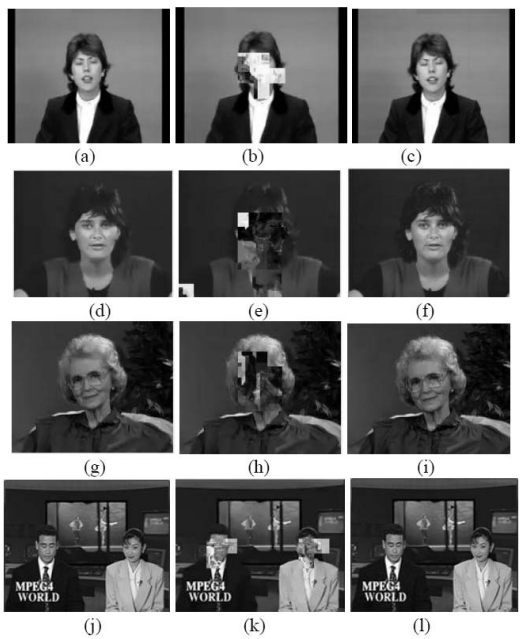


Fig.5. Facial image protection by encryption technique in H.264 (a)(d)(g)(j) Original image (b)(e)(h)(k) Protected facial image (c)(f)(i)(l) Recovered facial image

2.5 De-identification 카메라를 이용한 얼굴영상 보호

임베디드 하드웨어 기술의 발전과 더불어 지능형 CCTV 카메라의 등장으로, 프라이버시 보호 기능을 갖는 기법을 카메라에 내장하는 방법들이 개발되었다[8]. Fig. 6.에서와 같이 비디오 영상에서 사람을 검출 한 후, 전체 실루엣을 블러링하게 된다. 그런데 이러한 영상처리 소프트웨어가 Fig. 7.과 같은 Arm 코어 기반의 OMAP4 프로세서를 이용하여 카메라내에 임베디드 타입으로 구현되었다. 이러한 기법의 장점은 영상처리를 위하여 관제시스템에 전송될 시에 공격자에 의해 영상이 중간에 가로챌 수 있는 위험을 줄일 수 있는 장점이 있으나, 상대적으로 구현 비용이 증가할 수 있다.

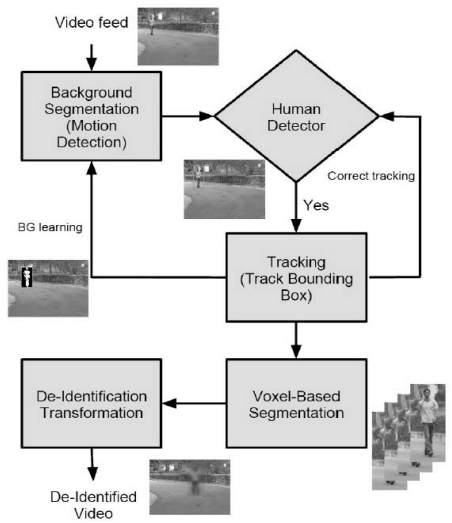


Fig.6. Image processing by embedded type privacy protective camera

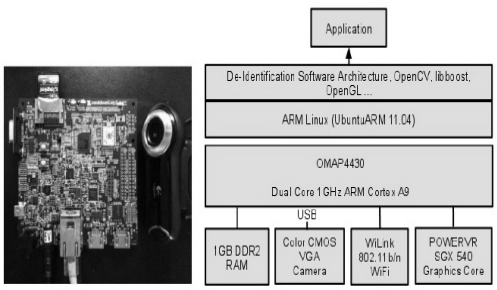
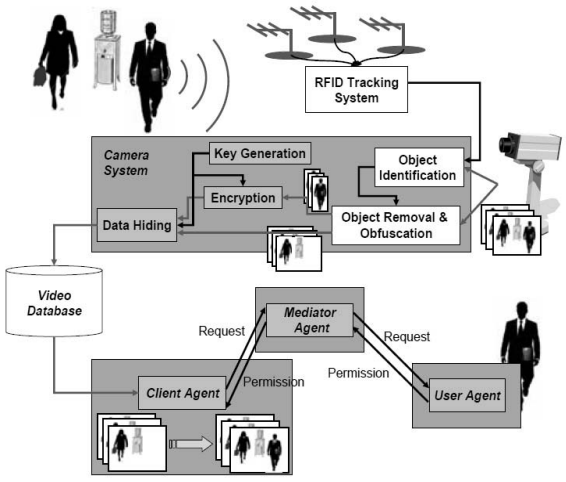


Fig.7. OMAP4 based camera and system configuration

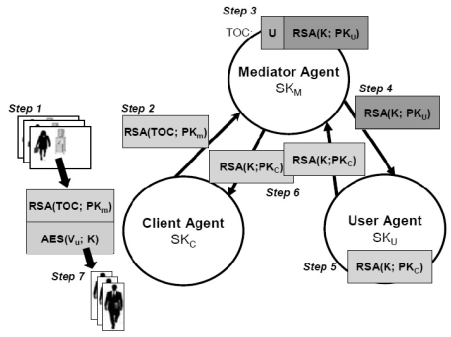
2.6 카메라 네트웍에서의 프라이버시 영상관리

CCTV를 구성함에 있어서 여러개의 카메라가 연동

하여 네트워을 이루고 있고, 또한 영상관리시스템의 대상이 되는 개개인이 RFID를 보유하여, 이와 연동된 영상에서 개인을 식별하고, 이후에 개인별도 설정된 프라이버시 레벨에 따라, 프라이버시 영상 보호를 수행하는 Fig. 8(a)와 같은 시스템이 제안 되었다[9]. 이를 위하여 Fig. 8(b)와 같이 1024비트 기반의 RSA 공개키와 128-bit AES 대칭키를 사용하여 개개인 별로 영상감시시스템내의 프라이버시 데이터를 접근할 수 있는 권한을 부여하여 관리하였다.



(a)



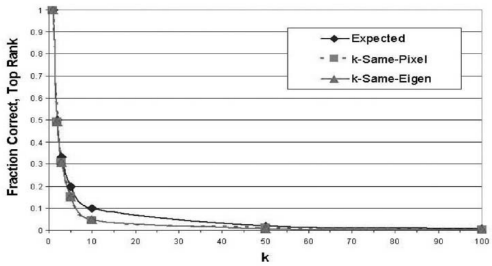
(b)

Fig.8. Privacy protection in camera network
(a) Privacy protective surveillance system
(b) Privacy information flow

2.7 유사 얼굴영상 합성을 통한 얼굴영상 보호

Newton 등[10]에 따르면 영상의 평균화나 블러링에 의한 영상의 인위적인 왜곡하에서도 얼굴인식 기법을 이용하였을 경우, 높은 인식율을 보인다고 보고하고 있다. 예를 들어 얼굴 영상의 화소를 15,20,30

(a)



(b)

Fig.9. Privacy image protection by k-same-pixel and k-same-eigen techniques
(a) Sample images of k-same-pixel and k-same-Eigen
(b) Face recognition rates according to k

개의 단위로 묶어도 동일한 밝기값을 부여하는 Pixelation 기법의 경우, 왜곡 되지 않은 영상과 왜곡된 영상을 교차하여 인식 시킨 경우, 눈으로는 잘 판가름 할 수 없을 정도로 왜곡 되었지만, 얼굴인식 알고리즘을 통하여 인식 시킨 결과 99% 정도의 높은 인식 성능을 보이고 있다고 보고하고 있다. 이러한 인위적인 왜곡 기법 중에는 얼굴을 포함한 특정 블록을 통째로 지워버리는 'BlackOut'기법이 얼굴인식기법에 대해서 가장 강인하다고 기술하고 있다. 따라서 상기 논문에서는 Fig. 9.와 같이 영상에서 픽셀을 동일하게 하거나(k-Same-Pixel), 고유얼굴을 동일하게 하는 방법(k-Same-Eigen)을 통하여, 근본적으로 개별적인 얼굴인식을 적용하지 못하게 하는 기법을 제시하고 있다. Fig. 9-b에서 알 수 있듯이, k 값이 증가함에 따라 인식률이 급격하게 감소함을 알 수 있다. 이 기법의 단점은 합법적인 경우의 원영상 복구에 대응할 수 없는데 있다.

III. 영상감시 시스템에서의 개인 영상 정보보호를 위한 보안위협과 기술적 · 관리적 요구 사항

3.1 영상감시 시스템에서의 프라이버시 관련 보안 위협

얼굴 영역 검출을 이용한 영상감시 시스템에서의 영상감시관제서버는 CCTV로부터 얻은 영상 정보를

저장 및 관리할 뿐만 아니라 모니터링, 영상을 감시하는 서버를 일컫는다. 영상감시 서버는 복호화, 얼굴영역검출, 프라이버시 보호적용 영상, 영상저장, 모니터링 등의 모듈로 구성된다. 모니터링 모듈은 복호화 모듈 혹은 프라이버시 보호적용 영상 모듈 뒤에 위치할 수 있는데, 이는 모니터링 시 프라이버시 보호를 적용할 것인지 여부에 따라 달라질 수 있다. CCTV 시스템의 구성 요소들인 유무선 CCTV, 영상감시관제서버, 클라이언트에서 발생할 수 있는 프라이버시 관련 보안 위협 및 CCTV 시스템 상에서 유·무선 CCTV와 영상감시관제 서버 간의 영상 데이터 송수신 및 영상감시관제서버와 클라이언트간의 영상 데이터 송수신시 프라이버시와 관련된 보안 위협을 Fig. 10.에서 보이고 있다.

- 일반적인 위협
  - ○ CCTV: 무단 접속, 물리적 공격, Dos/DDoS 공격
  - ○ 영상감시관제서버: 공격자의 서버 무단 침입, 데이터베이스 유출(database compromise), Dos/DDoS 공격, 데이터 처리 중 공격자의 방해
  - ○ 클라이언트: 데이터 처리 중 공격자의 방해
    - · 휴대폰: USIM 복제, 휴대폰 복제, 모바일 악성코드를 통한 영상 취득 및 훼손
    - · 데스크탑: IP 조작(원격제어, 무단접속), 바이러스 및 악성코드, 스파이웨어 강제 설치
    - · 모바일 장비: 모바일 바이러스 및 악성코드, IP 복제(Wi-Fi), 단말기 복제
  - ○ CCTV에서 영상감시관제서버로 영상을 전송시
    - · 도청, 재전송 공격, 중간자 공격, 의안화 공격 등
  - ○ 영상감시관제서버와 클라이언트가 영상정보를 포함한 데이터를 송·수신시
    - · 도청, 재전송 공격, 중간자 공격, 의안화 공격, IP 교란, DoS·DDoS 공격 등

- 프라이버시관련 위협
  - ○ CCTV
    - · 위치정보/영상정보/신체정보 등의 미인지 개인정보 실시간 수집
    - · 몰래카메라/불법 감청 장치 등 불법 수단에 의한 개인 정보 수집
    - · 불법 위치에서의 개인 영상정보 무단 수집 및 촬영(목욕탕 등)

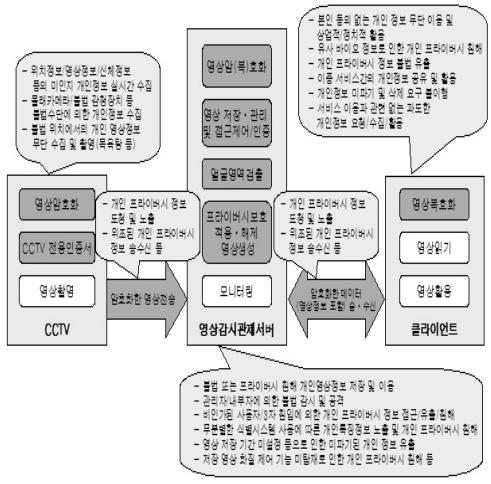


Fig.10. Security and privacy threats in video surveillance systems

  - ○ 영상감시관제서버
    - · 불법 또는 프라이버시 침해 개인영상정보 저장 및 이용
    - · 관리자/내부자에 의한 불법 감시 및 공격
    - · 비인가된 사용자 또는 3자 침입에 의한 개인 프라이버시 정보 접근/유출/침해
    - · 무분별한 식별시스템 사용에 따른 개인특징 정보 노출 및 개인 프라이버시 침해
    - · 영상 저장 기간 미설정 등으로 인한 미파기된 개인 정보 유출
    - · 저장 영상 화질 제어 기능 미탑재로 인한 개인 프라이버시 침해

3.2 영상감시 시스템에서의 개인 영상 정보보호를 위한 기술적 요구 사항

3.2.1 영상 정보를 포함한 데이터의 암·복호화

CCTV 카메라는 영상을 촬영한 후, 영상을 암호화하여 영상 감시 관제 서버로 안전하게 전송하고, 영상감시 관제 서버는 수신한 암호화된 영상을 복호화 한 후 적절한 처리 절차를 거쳐 저장을 하게 된다. 클라이언트가 영상 감시 관제 서버에 영상을 요청하는 경우도 이와 마찬가지로 암호화·복호화 단계를 거치게 된다. 이때 공개키 기반구조를 이용한 공개치 암호화와 대칭키 암호화를 적용할 수 있다.

3.2.2 영상 정보를 포함한 데이터의 송·수신

CCTV 카메라와 영상 감시 관제 서버, 영상요청자와 클라이언트간 안전한 영상 정보를 포함한 데이터 송·수신을 위해서는 공인인증서, 공개 키, 대칭키 등을 기반으로 한 SSL(Secure Socket Layer)/TLS(Transport Layer Security)등과 같은 세션 키 유도 및 안전한 채널 설정, 기기인증 등을 통하여 공격자로부터 도청, 위변조 등을 막을 수 있는 안전한 영상 전송이 이루어 져야 한다.

3.2.3 영상 감시 관제 서버에서의 얼굴 영역 검출

영상 감시 관제 서버는 CCTV로부터 수신한 암호화된 영상을 복호화 한 후, 적합한 얼굴 영역 검출 알고리즘을 기반으로 얼굴 영역 검출 과정을 수행함으로써 프라이버시를 보호하는데, 얼굴 영역 검출 알고리즘에는 지식 기반 방법(knowledge-based methods), 특징 기반 방법(feature-based methods) 탬플릿 매칭 방법(template-based methods), 외형기반 방법(appearance-based methods) 등이 있다.

3.2.4 영상 감시 관제 서버에서의 프라이버시 보호 적용 및 해제 영상 생성

개인 영상 정보에 대한 프라이버시를 제공하기 위해서는 얼굴 영역 검출 기법을 통해서 검출된 얼굴 영상에 응용 목적에 맞게 앞의 2장에서 설명된 영상 프라이버시 보호 알고리즘을 사용하여 프라이버시 보호 적용 영상을 생성한다. 프라이버시 보호 적용 기법에는 암호화, 스크램블링, 마스킹 방법 등이 있으며, 이를 실시간으로 적용할 지에 따라, 카메라에서 직접 구현 여부를 결정한다. 영상 감시 관제 서버는 저장매체에 저장된 영상에 대해 복호화를 수행한 후, 적합한 프라이버시 보호 해제 알고리즘을 적용하여, 얼굴 영역을 인지할 수 있는 프라이버시 보호 해제 영상을 생성한다. 프라이버시 보호 해제를 위해서 복호화, 역스크램블링, 역마스킹 방법 등을 사용할 수 있다[11].

3.3 영상감시 시스템에서의 개인 영상 정보보호를 위한 관리적 요구 사항

영상감시시스템을 설치·운영하려는 기업 또는 개인은 정보주체의 초상권, 사생활의 비밀과 자유 등이 침해되지 않도록 영상감시시스템을 설치·운영하여야 하며, 이때 아래의 각 지침이 준수 되어야 한다. 이를 위해 Table 1와 같이 기존의 영상감시 시스템에서 개인정보보호 관련 법령 비교를 수행하였다.

Table 1. Privacy protection laws related to video surveillance systems

구분	개인정보 보호법	정보통신망법
개인정보 수집, 이용	제15조, 제16조	제22조, 제24조
개인정보의 제공	제17조, 제18조, 제 19조	제24조의2
개인정보의 파기	제21조	제29조
동의 방법 (14세미만 권리)	제22조	제26조의2, 제31조
정보주체이외의 개인정보 수집	제20조	-
민감정보 처리	제23조	제23조
고유식별정보	제24조	제23조의2
업무위탁	제26조	제25조
영업양도	제27조	제26조
개인정보취급자감독	제28조	-
기술적 보호조치	제29조	제28조
취급방침 수립	제30조	제27조의2
책임자 지정	제31조	제27조
유출시 통지	제34조	제27조의3
정보주체 권리	제35조, 제36조	제30조
비밀누설 금지	제59조	제2조의2
개인정보파일	제32조	-
개인정보 영향평가	제33조	-
국외이전	제17조	제63조

3.3.1 영상정보처리기기 설치·운영 제한 및 필요한 최소한의 촬영[8]

공개된 장소에서의 영상정보처리기기 설치는 원칙적으로 금지되고, 예외적으로 개인정보보호법 제25조에서 정하는 사유에 해당하는 경우에만 영상정보처리기기를 설치·운영할 수 있다.

- 법령에서 구체적으로 허용하고 있는 경우
- 범죄의 예방 및 수사를 위하여 필요한 경우

· 시설안전 및 화재 예방을 위하여 필요한 경우
· 교통단속을 위하여 필요한 경우
· 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

영상정보처리기기는 개인의 의사와 무관하게 초상 및 활동 정보가 수집되어 무단공개나 유출 등으로 인한 프라이버시 침해 우려가 높은 만큼 쉽게 인식할 수 있는 형태의 영상정보처리기기를 정보주체 눈에 잘 띄는 곳에 설치·운영하여야 한다. 불특정 다수가 이용하는 공개된 장소라도 현저히 사생활 침해 우려가 있는 장소는 영상정보처리기기 설치·운영이 금지하여야 한다.

3.3.2 영상정보처리기기 임의조작·녹음 금지

영상정보처리기기에는 녹음 기능을 사용할 수 없고, 설치 목적과 다른 목적으로 영상정보처리 기기를 임의로 조작하거나 다른 곳을 비춰서는 안 된다.

3.3.3 설치 시 의견수렴 및 안내판 설치를 통한 설치 사실 공지

공개된 장소에 영상정보처리기기를 설치·운영하려는 운영자는 관계전문가 및 이해관계인의 의견을 수렴하여야 한다. 영상정보처리기기의 설치 목적 변경 및 추가 설치 등의 경우에도 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다. 다만 동일 목적 내 단순히 추가적으로 설치하는 경우에는 의견수렴을 하지 않을 수 있다. 운영자는 영상정보처리기기 설치 시 정보주체가 쉽게 알아볼 수 있도록 안내판을 설치하여야 한다. 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 설치하며 안내판의 크기나 위치는 자율적으로 정하되, 정보주체가 손쉽게 인식할 수 있도록 하여야 한다. 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다. 영상정보처리기기의 효율적 관리와 정보 연계를 위하여 통합 관리하는 경우에는 설치 목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 안내판에 기재하여야 한다.

3.3.4 영상감시시스템 운영·관리 방침 수립·공개 및 책임자 지정

영상감시시스템 운영·관리 방침을 수립하고 이를 해당 기관의 인터넷 홈페이지에 게재하여 정보주체에게 공개하여야 한다. 개인영상정보의 처리에 관한 업무를 총괄하여 책임질 개인영상정보 관리책임자를 지정하여야 하며, 개인영상정보 관리책임자는 각 기관 자체적으로 지정하여 관리하는 것을 원칙으로 한다.

3.3.5 영상정보의 목적외 이용·제공 제한 및 보관·파기 철저

운영자는 법률에서 정하는 등 특별한 경우를 제외하고 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공할 수 없다. 다만, 다음 각 호의 1의 해당되는 경우는 예외로 한다.

· 정보주체의 동의를 받은 경우
· 통계작성, 언론보도, 연구 등 공공의 목적을 위해 필요한 경우로서 정보주체의 바이오인식 정보가 들어나는 않는 형태로 제공되는 경우
· 법률에 특별한 규정이 있는 경우

영상정보처리기기에 의하여 수집된 영상정보는 보유기간이 만료한 후 지체 없이 삭제하여야 한다.

3.3.6 정보주체의 영상정보 열람권 보장

정보주체는 영상정보처리기기 운영자가 처리하는 본인의 영상정보에 대하여 열람 또는 존재확인을 해당 영상정보처리기기 운영자에게 요구할 수 있다. 정보주체가 열람 등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한하며, 정보주체는 영상정보처리기기 최종 책임자에게 개인영상정보에 대하여 열람 또는 존재확인을 요구할 수 있으며, 이에 대하여 지체 없이 필요한 조치를 취하여야 한다. 열람 등 조치를 취하는 때에는 정보주체의 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우 해당되는 정보주체 이외의 타인영상정보를 알아볼 수 없도록 보호조치를 취해야 한다[12][13].

3.3.7 개인영상정보의 안전성 확보 조치 및 자체 점검 현황 등록

영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 취하여야 한다[14].

1. 개인영상정보의 안전한 처리를 위한 내부 관리 계획의 수립·시행
· 개인영상정보 관리책임자 지정
· 개인영상정보 관리책임자 및 취급자의 역할 및 책임에 관한 사항
· 안전성 확보조치에 관한 사항
· 개인영상정보 취급자 교육
· 그 밖에 개인영상정보의 안전성 확보에 필요한 조치에 관한 사항
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용(네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일에 대한 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

영상감시시스템에 의하여 수집·처리되는 영상정보로의 접근권한은 총괄책임자 및 운영책임자 등 지정된 최소한의 인원으로 제한하여야 한다.

IV. 결 론

개인정보보호법에서는 개인 정보의 안전성 확보조치 기준 고시 제 2조에서 바이오정보라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함하는 것으로 규정하고 있다. 또한, 암호화 대상으로 고유식별정보, 비밀번호, 바이오정보를 규정하고 양방향 암호화 기준을 규정하고 있다. 영상정보처리기기란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로써 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 의미한다. 카메라 및 네트워크 기술의 발전에 따라 영상정보처리기기를 통해 원거리에서 사람식별, 실시간 추적 등이 가능해 짐으로서 촬영 중이나 촬영된 영상에 포함된 개인영상 정보에 기인한 프라이버시 침해에 대처하기 위한 정보보호 조치는 필수적이라고 하겠다. 이에 본 논문에서는 영상 감시시스템에서 개인영상 정보보호를 위한 국내외 연구동향을 제시하고, 기술적·관리적 대책을 제시함으로써 영상감시 시스템에서의 개인 영상 정보보호 요구사항을 도출하였다.

References

〔1〕 "installation and operation guidelines for the CCTV of the public organigation" Ministry of security and public administration, 2012.

〔2〕 Cha Gun Sang, Shin Yong Tae, "Personal Video Privacy Issue to Increasing CCTV Installation," Journal of Computing Science and Engineering, Vol. 27 No. 12, 2009.

〔3〕 A. Frome, et. al., "Large-scale Privacy Protection in Google Street View," IEEE International Conference on Computer Vision (ICCV), pp. 2373-2380, 2009.

〔4〕 F. Dufaux, T. Ebrahimi, "A Framework for the Validation of Privacy Protection Solutions in Video Surveillance," IEEE International Conference on Multimedia and Expo (ICME), pp. 66-71, 2010.

〔5〕 F. Dufaux, T. Ebrahimi, "Scrambling for Privacy Protection in Video Surveillance Systems," IEEE Trans. on Circuits and Systems for Video Technology, Vol. 18, No.8, pp. 1168-1174, 2008.

〔6〕 P. Agrawal, P.J. Narayanan, "Person De-identification in Videos," IEEE Trans. on Circuits and Systems for Video Technology. Vol. 21, No.3, pp. 299-310, 2011.

〔7〕 F. Peng, X. Zhu, M. Long, "A ROI Privacy Protection Scheme for H.264 Video Based on FMO and Chaos," P. Agrawal, P.J. Narayanan, IEEE Trans. on Information Forensics and Security, Vol. 8, No.10, pp. 1688-1699, 2013.

〔8〕 Mrityunjay, P.J. Narayana, "The De-identification Camera, Conference on Computer Vision," Pattern Recognition, Image Processing and Graphics, pp. 192-195, 2011.

〔9〕 S. Cheung, et. al., "Managing Privacy Data in Pervasive Camera Networks," IEEE Int. Conference on Image Process-

ing, pp. 1676-1679, 2008.
〔10〕 E. M. Newton, et. al., "Preserving Privacy by De-identifyuing Face Images," IEEE Trans. on Knowledge and Data Engineering, Vol. 17, No.2, pp. 232-243, 2005.
〔11〕 Mun Hae Min, Ban Sung Bum, "The Analysis of De-identification for Privacy Protection in Intelligent Video Surveillance System," Journal of korea institute of information technology, Vol.9 No. 7, pp. 189-200, 2011. 7.
〔12〕 Yong-Nyuo Shin, Hale Kim, Myung-Geun Chun, "Privacy reference architecture and International standardization trend," Korea Institute of Information Security and Cryptology. Vol. 21, No. 5, pp. 12-20, 2011.
〔13〕 Han Bung Jin, Hale Kim, Yong-Nyuo Shin, Myung-Geun Chun,, "Biometric standardization trend - Focus on International standardization Organization," Korea Institute of Information Security and Cryptology Vol. 21, No. 2, pp. 61-69, 2011.
〔14〕 "Privacy protection guidelines(Labor personnel, Institution, Medical organization, CCTV Installation and operation Area)," Ministry of security and public administration, 2012.

〈저자소개〉

신 용 녀 (Yong-Nyuo Shin) 종신회원
1999년 2월: 숭실대학교 컴퓨터학과 졸업
2001년 9월: 고려대학교 컴퓨터학과 석사
2008년 2월: 고려대학교 컴퓨터학과 박사
2002년 1월~2009년 6월: 한국정보보호진흥원 주임연구원
2009년 7월~2010년 7월: 한국은행 전자금융팀 과장
2010년 9월~현재: 한양사이버대학교 컴퓨터공학과 교수
2009년~현재: TTA PG505 표준위원회 부위원장
2008년~현재: ISO/IEC SC27 정보보호표준화전문위원
〈관심분야〉 바이오인식, 개인정보보호, 정형기법

전 명 근 (Myung-Geun Chun) 종신회원
1987년 2월: 부산대학교 전자공학과 졸업
1989년 2월: KAIST 전기 및 전자공학과 석사
1993년 2월: KAIST 전기 및 전자공학과 박사
1993년~1996년: 삼성전자 자동화연구소 선임연구원
2000년~2001년: University of Alberta(캐나다) 방문교수
2011년~2012년: Temple University(미국) 방문교수
1996년~현재: 충북대학교 전자공학부 교수
2008년~현재: TTA PG505 표준위원회 전문위원
2007년~현재: ISO/IEC SC27 정보보호표준화전문위원
〈관심분야〉 바이오인식, 개인정보보호, 지능시스템