

영상보안시스템 기술 동향

한 종 욱*, 조 현 속**

요 약

본 고에서는 범죄 예방 및 시설물 보호 등을 위해 다양한 분야에서 사용되고 있는 국내외 영상보안시스템 제품 및 기술 현황을 살펴보고, IP 환경으로 진화함에 따른 차세대 영상보안시스템이 가져야할 요구사항과 이에 대한 국내외 기술개발 현황을 살펴보았다. 특히, 영상보안제품의 신뢰성 확보 및 제품 경쟁력 강화를 위한 핵심기술로 부상할 보안기술에 대해서 집중적으로 분석하였다.

I. 서 론

9·11 테러 이후 테러 및 범죄예방을 위해 CCTV를 중심으로 한 영상보안시스템에 대한 수요가 폭발적으로 증가하고 있으며, 다양한 위험상황에 보다 효과적으로 대처하기 위해서 영상보안기술은 사고 대응 중심에서 사전 예방 중심으로 진화하고 있다. 사고 대응 중심의 영상보안시스템에서는 CCTV와 같은 카메라를 기반으로 하여 사람이 직접 위험상황을 모니터링하는 관제기술이 핵심이었으나, 사전 예방 중심의 영상보안시스템에서는 위험상황에 대해 실시간 대처 및 예방이 가능하게 하는 DVR 장비의 지능형 인식 솔루션이 핵심기술로 부각되고 있다.

영상보안시스템은 CCTV 중심의 폐쇄형 구조에서 오픈망을 사용하는 IP 기반의 개방형 구조로 발전하고 있으며, 카메라 장치의 기술발전 및 영상보안장비의 활용성 확대 등으로 메가픽셀급 영상의 사용이 증가할 것으로 예상된다. 이러한 변화로 인하여 기존 DVR 중심의 영상저장 장치는 DVR장치 외에 별도의 비디오 저장장치를 두는 형태로 발전하고 있으며, 영상보안시스템을 구성하는 주요 장치인 카메라는 아날로그 CCTV에서 IP기반의 네트워크 카메라로 발전하고 있다.

영상보안 시스템의 전반적인 수준은 국내 업계가 세계 정상급에 있다고 할 수 있지만, 지능형 영상보안기술만큼은 해외업체들이 강세를 보이고 있다. 향후 지능형

영상보안 솔루션이 영상보안제품의 핵심기능으로 부상할 것으로 예상되므로 국내업체들은 이에 대한 대비책을 서두를 필요가 있다. 대부분의 국내업체들이 외국의 지능형 영상인식 기술을 그대로 도입해서 차세대 영상보안제품을 개발하고 있는 실정이며, 소수의 국내 업체만이 지능형 영상 기술에 대한 기술력을 보유하고 있는 것으로 파악된다.

본 고에서는 국내업체들이 향후 진출해야 할 High-End급 영상보안시장을 고려하여, High-End급 영상보안제품이 갖추어야할 핵심기능 등을 설명하고 현재까지의 국내외 관련 업체의 상용제품 개발 현황 등에 대하여 정리하였다. 특히, 지식정보보안업체에서 관심을 가져야할 영상보안시스템용 보안기술에 대해서 집중적인 분석을 하였다.

II. 영상보안시스템의 구성

영상보안시스템은 CCTV 중심의 폐쇄형 구조에서 오픈망을 사용하는 IP 기반의 개방형 구조로 발전하고 있으며, 카메라 장치의 기술발전 및 영상보안장비의 활용성 확대 등으로 메가픽셀급 영상의 사용이 증가할 것으로 예상된다. 이러한 변화로 인하여 기존 DVR 중심의 영상저장 장치는 DVR 장치외에 별도의 비디오 저장장치를 두는 형태로 발전하고 있으며, 영상보안시스템을 구성하는 주요 장치인 카메라는 아날로그

* 한국전자통신연구원 융합서비스보안연구팀 (hanjw@etri.re.kr)

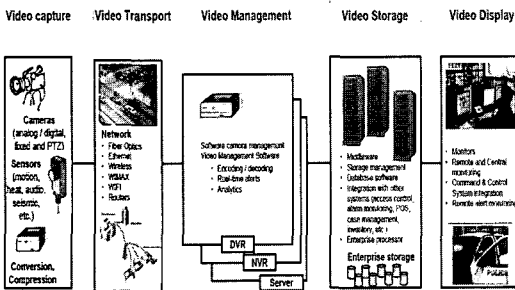
** 한국전자통신연구원 지식정보보안연구부 (hscho@etri.re.kr)

CCTV에서 IP기반의 네트워크 카메라로 발전하고 있다. CCTV는 영상수집을 위해 제한된 공간에 설치되어 수집된 영상을 폐쇄적인 유선 또는 무선망을 통해 특정한 수신자에게 전송하는 영상보안시스템용 촬영장치를 말하는 반면, IP 카메라는 수집한 영상을 IP 기반의 정보통신망을 통하여 원격지에서 실시간으로 수신 혹은 저장 등의 처리를 할 수 있게 하는 촬영장치를 의미한다. 한편, DVR은 아날로그 CCTV에서 수집된 영상을 저장하는 장치였으나, IP 기반 환경으로 발전함에 따라, IP 네트워크를 통해 전송된 영상정보를 저장하는 NVR로 발전하고 있다.

2.1 폐쇄형 방식의 영상보안시스템

아날로그 카메라가 중심이 되는 CCTV 기반의 폐쇄형 영상보안시스템은 영상 수집을 담당하는 CCTV 장치부분, 수집된 영상을 전송하는 아날로그 전송케이블 부분, 수집된 영상을 저장하는 VCR 또는 DVR 장치, 상황 모니터링을 위한 모니터 등으로 구성이 된다.

[그림 2]의 (a)는 VCR 장치를 사용하여 아날로그 영상 정보를 저장하는 방식이며, (b)는 아날로그 영상정보를 디지털 영상으로 변환하여 DVR 장치에 저장하는 방식이다. [그림 2]의 (c)와 같이 CCTV를 중심으로 영상보안시스템이 폐쇄형으로 구성이 되었지만, 인터넷의 활성화로 CCTV가 설치된 장소를 원격으로 모니터링하는 경우가 최근 증가하고 있다. IP 카메라를 사용하는 오픈망 기반의 영상보안시스템의 전단계라고 할 수 있다. 폐쇄형 영상보안시스템은 설치된 지역에 한하여 영상감시 서비스를 제공할 뿐 다른 지역에 설치된 이종의 영상보안시스템과의 연동은 불가능하여 확장성이 떨어지는 단점이 있다.

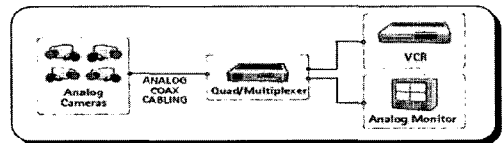


(그림 1) 영상보안시스템 구성요소

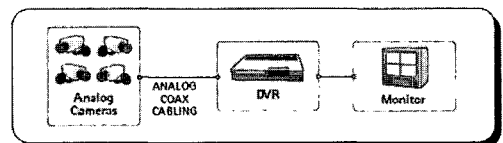
따라서, 현재의 영상보안시스템은 아날로그 환경과 IP 환경이 공존하고 있으므로 CCTV/IP 카메라 등의 카메라 장치, 전송 네트워크, DVR/NVR 장치, 비디오 저장장치, 관제장치 등으로 구성된다고 할 수 있다.

(표 1) CCTV와 IP 카메라의 비교

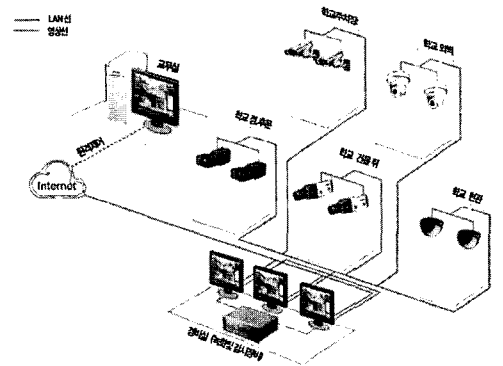
구분	CCTV	IP 카메라
인터넷 접속	불가능	가능
녹화방법	아날로그	디지털
저장위치	로컬	IP 네트워크 연결이 가능한 어디든지 가능
녹화 매체	비디어 테잎	HDD, 서버 등
영상화질	저화질	고화질
화면분할, PTZ	불가능	가능
확장성	불가능	우수
음성녹화	불가능	가능
필요한 주변장치	모니터, VCR	없음
응용분야	제한적	무제한



(a)



(b)



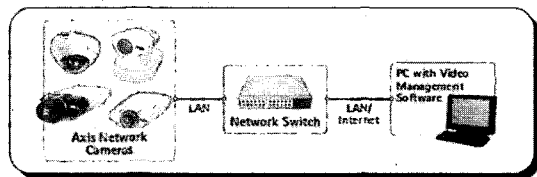
(c)

(그림 2) 폐쇄형 영상보안시스템 : (a) 기본 시스템 구성 : VCR, (b) 기본 시스템 구성 : DVR, (c) 적용 예

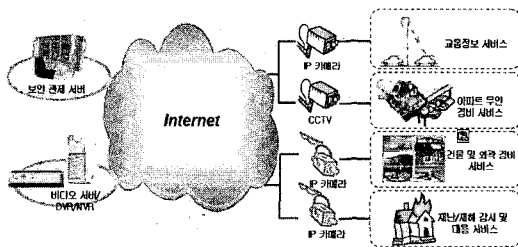
2.2 IP 기반 영상보안시스템

최근 인터넷 활성화에 힘입어 원격 모니터링이 가능하고 카메라 설치 및 운용시의 제약 문제를 해결할 수 있는 IP 기반 영상보안시스템이 각광을 받고 있다. IP 기반 영상보안시스템은 영상 수집을 담당하는 IP 카메라, 수집된 영상을 전송하는 IP 기반 유/무선 네트워크, 수집된 영상을 저장하는 DVR/NVR 장치 또는 영상저장용 서버, 상황 모니터링을 위한 모니터 등으로 구성이 된다.

IP 기반 영상보안시스템에서는 네트워크가 연결되어 있는 곳이면 어디든지 설치가 가능하므로 CCTV에 비해서 상대적으로 설치 장소의 제약을 받지 않는 장점이 있으며, 다른 장소에 설치되어 있는 IP 기반 영상보안시스템과의 연동성도 프로토콜만 호환이 된다면 충분히 가능한 장점을 갖고 있다. 또한, 다양한 IT 서비스와의 연계도 가능하여 이날로그 방식의 영상보안시스템은 IP 기반 영상보안시스템으로 전환이 빠르게 일어나고 있다.



(a)



(b)

(그림 3) IP 기반 영상보안시스템 : (a) 기본 시스템 구성, (b) 적용 예

III. 영상보안시스템 기술 동향

영상보안시스템의 전반적인 수준은 국내 산업체가 세계 정상급의 기술력을 보유하고 있고, 특히, DVR 제품은 세계 1위를 고수하고 있지만, 지능형 영상보안기술만큼은 해외업체들이 강세를 보이고 있다. 대부분의 국내 업체들은 외국의 영상인식 기술을 그대로 도입해

서 지능형 영상처리 기능이 탑재된 제품을 판매하고 있는 실정이며, 극히 소수의 국내 업체만이 지능형 영상 기술에 대한 기술력을 보유하고 있는 것으로 파악된다.

3.1 국내 기술 동향

국내에서 활동하는 CCTV 관련업체는 200여개에 이르며, 그 중 대다수가 CCTV 관련 단품을 제조하는 중소기업들로 대규모 제조업체로는 삼성테크윈, 삼성전자, 하이트론씨스템즈, LG전자, 씨엔비테크 등이 있다. DVR 업체들은 네트워크 기능을 보강한 DVR 제품과 IP전용 단말기를 출시하고 있으며, DVR 업체 중 선두주자인 아이디스는 IP Trend에 맞춰 스탠드얼론 형태 제품이면서도 PC를 작동하는 것과 같은 편의성을 강조하고, 네트워크 기능을 통해 인터넷으로도 모니터링이 가능한 제품을 출시하였다.

국내 영상감시시스템 시장은 지하주차장의 영상감시시스템 의무설치 등으로 2000년 이후 연평균 15% 이상의 성장을 보이고 있다. 향후에도 은행의 무인점포 증가와 무인경비시스템의 강화, 공장자동화, 빌딩자동화 시스템 등 응용 분야의 확대로 성장세를 지속할 것으로 전망된다. 국내 민간분야 영상감시시스템 설치 현황에 대한 조사 자료는 현재 없으나 시장규모 등을 통해 추산하면 약 200만대로 추정된다.

영상감시시스템 국내수요는 연간 30만대정도로, 삼성테크윈(50%), 삼성전자(25%), LG전자, 한국하니웰, 코디콤 등 국내기업이 90% 이상 공급하고 있으며, 나머지 10%에 대하여 중소기업 혹은 외산제품이 차지하고 있다.

장비제조사별로 각기 다른 프로토콜을 제공하고 있어 호환성이 미흡하여 효율적인 운용 및 영상 장비간 인터페이스 연동에 어려운 문제점이 있다.

영상보안시스템 분야의 국내 기술은 DVR 제품에 있어서는 외국 기술을 선도하고 있으나 그 외의 기술에 대해서는 외국 기술과의 격차가 심화되고 있는 상황이다. 특히 지능형 인식기술의 경우에는 외국 기술에 대한 의존도가 매우 심각하다.

국내에서 생산되는 IP 카메라에는 보안기술이 일부 적용되고 있으나, 그 적용이 패스워드 기반의 네트워크 보안을 적용하여 프라이버시 침해 우려가 존재하고 있으며 영상보안산업의 가치사슬 구조는 카메라, H/W 부품, 서버/레코더, 모니터, S/W로 구분 된다. 카메라의

경우는 아날로그 카메라와 디지털 카메라로 나뉘며, 최근 들어서는 IP 카메라에 지능형 인식 기능 등을 탑재하기 위해 고성능 DPS 칩이 내장된 스마트 카메라에 대해서 연구를 진행하는 업체가 늘어나고 있다. 서버/레코더는 DVR 혹은 NVR 제품으로 나뉘고 있으며, DVR의 경우 Stand-Alone 타입과 PC-Based 타입 제품으로 나눌 수 있다. 모니터, S/W 측면에서 모뎀 카메라 관리 및 수집 영상 관제 등을 위한 관제용 소프트웨어가 주요 제품이며, 관리화면 구성을 위한 모니터 등이 국내에서 생산되고 있다.

국내 영상보안시스템 업체들이 중심이 되어 2008년 한국디지털CCTV연구조합이 설립되었으며, DVR 세계 1위 업체인 아이디스(주)를 비롯하여 현재까지 총 27개 회원사들이 참여하고 있고 점점 많은 업체가 참여할 것으로 예상된다. 회원사들의 주력제품은 IP 카메라, DVR, NVR, 영상인식솔루션 등으로 영상보안 관련 모든 제품들이 생산되고 있으며, 영상보안시스템간의 호환성 부재로 인한 문제를 해결하기 위해 K-Protocol이라는 한국형 프로토콜을 ETRI와 공동으로 개발하고 있다.

주요 국내업체별 현황을 정리하면 다음과 같다.

아이디스는 DVR 분야에서 세계시장 점유율 15%인 세계 1위 업체로써 PC 기반, Stand Alone, Network Server 등 다양한 DVR 제품을 생산하고 있다. 미국의 GE, 영국의 데디케이티드 마이크로스와 함께 DVR 분야의 세계 3대 업체로 평가를 받고 있는 업체이다. 국내는 에스원, 콤텍시스템 등과 국외는 ADT, Honeywell 등과 전략적인 관계를 구축하여 안정적인 매출을 올리고 있는 회사이다. 보유 기술로는 압축기술(H.263, H.263 기반의 layer 분리 및 X-frame 생성 기법), 고용량 영상 데이터베이스 운용, 다수의 카메라간 동기처리 기술, 시스템 안전을 위한 전원 제어기술등을 보유하고 있으며, DVR에서 다채널에서의 검색 기능을 제공하며, Chained Fingerprinter 암호화 기술을 보유하고 있다.

일리시스는 지능형 영상감시 전문 회사로서 180/360도 파노라믹 정지영상/비디오 생성 기술 및 지능형 영상 감시 시스템 개발하고 있다. 언론자료를 근거할 때 국내 업체 중 가장 우수한 지능형 인식기술을 보유하고 있는 것으로 파악되고 있다. 단일 카메라에서의 침입 탐지 및 추적, PTZ 트래킹, 버려진 물건 및 사라진 물건 인식, 주차위반 및 자동차 번호판 인식, 객체 계수 등의 인식기능을 보유하고 있다고 하나, 아직 상용제품의 기

능 및 성능에 대한 객관적인 평가 자료가 없어 인식기술에 대한 기술보유 유무는 정확하다고 할 수 없다.

원포넷은 DVR 제품, NVR 제품과 IP 카메라 및 DVR 등을 네트워크를 통해 원격 관리하는 통합 관리 솔루션 등에 기술력을 보유하고 있다. 사람 계수기능, 특정 행위나 복장을 한 사람을 추적하는 기능 등 일부 지능형 인식기술을 보유하고 있으며, 계산대에 특화된 POS DVR 등에 대한 기술도 보유하고 있다고 한다.

에스원은 국내 최초의 무인경비시스템과 경비로봇을 통해서 국내 무인보안경비 시장을 주도하는 보안전문업체로 국내 무인경비시스템 시장의 60%를 점유하고 있다.

텔레캡서비스(주)는 에스원, ADT캡스에 이서 국내 무인경비서비스 시장 점유율 13%를 차지하고 있는 무인경비전문업체로 공동주택분야에 있어서는 에스원보다 많은 가입자를 보유하고 있다고 한다.

3.2 국외 기술 동향

국외 영상보안제품은 선진국들을 중심으로한 High-End급 제품과 중국, 대만을 중심으로한 Low-End 제품 등 크게 두 그룹으로 나눌 수 있다.

High-End급 영상보안제품의 핵심기능이라고 할 수 있는 지능형 영상처리 기술은 ObjectVideo, IOimage, Indigo 등의 업체를 중심으로 발전하고 있으며, 객체 및 상황을 인지하고 위험 객체를 추적하는 기술에 대한 연구가 활발히 진행되고 있다.

현재, 영상보안시스템간 호환성 미흡으로 실제 운영상 문제가 이슈화되고 있어 일부 선진국의 메이저 회사들을 중심으로 호환성 확보를 위한 움직임이 일어나고 있다. Cisco, GE Security, Honeywell, IBM, Panasonic, Pelco 등 19개 주요 업체가 PSIA(Physical Security Interoperability Alliance)를 설립하여 IP 기반 미디어 장비에서 지원하는 open API 규격 개발 중에 있으며, AXIS, Bosch, Sony 등 22개 업체가 ONVIF(Open Network Video Interface Forum)라는 포럼을 구성하여 네트워크 비디오 제품간의 상호호환성을 제공하기 위한 인터페이스 표준을 개발 중에 있다. 또한, 세계 보안관리 소프트웨어 시장 점유율 1위 업체인 Verint를 중심으로 보안관리 솔루션 업체들은 이기종 IP 카메라, DVR 등을 관리하기 위해 다양한 업체의 프로토콜을 수용하는 형태의 보안관리 제품을 상용화하고 있으며,

현재 PSIA나 ONVIF 보다 많은 업체의 상용제품과 호환이 가능한 상황이다.

AXIS는 1984년 설립된 스웨덴 회사로 시장 개척자 및 1위 업체로서의 인지도를 가지고 있고 다양한 제품의 line up을 형성하고 있다. 네트워크 카메라, 비디오 엔코더, 영상관리 소프트웨어 등 영상보안과 관련된 제품을 통합솔루션 형태로 제공하고 있다.

3VR Security Inc.에서는 차세대용 영상보안플랫폼을 리딩하는 업체로서 시장에서 요구하는 대부분의 기능을 탑재하고 있다. 3VR의 IVMS(Intelligence Video Management System)제품은 미국의 SIA, Frost & Sullivan, J.P Freeman 등에서 Best Video Management Product로 선정된 적이 있다. IVMS는 영상보안솔루션과 생체인식기술을 결합한 기능을 제공하며, 보관된 영상자료에서 객체 검색, 객체 탐지, 객체 인식 기능을 제공한다. 또한, 얼굴 및 사물/문자에 대한 지능형 분석 기능과 DVR/NVR의 모든 기능을 단일 플랫폼에서 제공하며, IP 카메라와 CCTV, USB 카메라 등을 1,000대 이상 연동 할 수 있다고 한다. 보안을 위해 자체 개발한 프로토콜을 사용하고 있으며, 워터마킹 기능, 프라이버시 마스킹 기능, Anti-Virus를 탑재하여 보안성을 강화하고 있다.

Panasonic System Solutions는 Analog 카메라, Network 카메라, DVR 등을 제조 생산하는 업체이며, 지능형 영상감시 및 관리 시스템도 상용화하였다. 네트워크 카메라의 경우 ID/PW를 이용한 사용자 인증 방식을, IP address를 통한 호스트 인증기능을 제공한다. 네트워크 카메라에서 프라이버시 보호를 위해 프라이버시 존을 설정할 수 있으며, 8개에서 이상의 공간을 선택할 수 있다. DVR 제품의 경우 HTTP를 통한 사용자 인증, 호스트 인증을 제공하며, FTP 포트와 HTTP 포트에 대해 보안 적용이 가능하다.

Pelco사는 1987년 설립되어 영상 보안시장에서 메이저 업체로 성장한 회사로 네트워크 카메라, DVR, NVR 제품을 상용화한 회사이다. 네트워크 카메라 제품에 경쟁력을 갖고 있는 회사로 프라이버시 보호를 위해 PTZ 카메라에 Window Blanking 기능을 이용하여 자동으로 창문을 blanking 처리할 수 있다. 각 네트워크 카메라는 HTTPS, FTP, SSL 등 다양한 보안 프로토콜을 제공하고 있으며, 사용자인증에는 ID/PW 방식을, Host 인증에는 IP Address 방식을 사용하고 있다. 지능형 인식

기술로 객체 추적, 객체 탐지 등 다양한 탐지 기능을 제공한다.

Bosch Security Systems는 통합 지능형 영상감시 시스템 솔루션을 개발하는 업체로 네트워크 카메라의 경우 다양한 인코더를 지원하여 MPEG-4, H.264, MJPEG 등 다양한 포맷을 제공한다. 프라이버시 마스킹 기능을 가지고 있으며, IVA(Intelligent Video Analysis)는 영상을 분석 및 메타데이터를 생성하고, 메타데이터 분석을 통해 빠른 영상 추출을 실현하였으며, 모션캡처, 카메라 떨림 보정, 열감지 지원, 카메라의 임의 조작 감지, 감지 및 대상 영역 설정 가능 등의 기능을 제공한다.

Sony는 IP 네트워크와 고해상도 이미징 및 오디오 기술을 접목한 DEPA(Distributed enhanced Processing Architecture) 플랫폼 개발하였다. 네트워크 카메라에서 고해상도 이미징기술을 가지고 있으며, AES 기반의 보안기능을 제공한다. 이전 1개 프레임과 비교하여 현재 프레임에서의 동작 유무를 감지해내던 기본 방식을 이전 15 프레임과의 차이를 분석하는 방식으로 구현하여 지능형 동작 감시기능에 있어서 오경보를 최소화시켰다고 한다.

Cisco의 물리보안솔루션은 HD 카메라부터 관제제품까지 다양한 영상보안제품을 상품화하였다. Cisco의 주력 제품인 네트워크 장비기술을 영상보안시스템분야에 특화시켜 스트리밍과 인코딩을 통합하여 다수의 비디오 스트림을 지원할 수 있게 만든 물리보안용 다중 서비스 플랫폼을 상용화하였다. 물리보안용 다중 서비스 플랫폼은 최대 24TB의 저장용량을 제공할 수 있으며, 최대 300개의 비디오 스트림까지 지원할 수 있다고 한다.

Objectvideo는 야간 환경에서 다수의 카메라를 이용하여 사람과 물체를 추적하는 시스템과 이상 조명효과(Strange lighting effects), 저조도 수준 및 이동 차량 전 조등과 같은 환경에서 정상 작동하는 기술을 개발하였다. 물체를 분석, 탐지, 식별, 실시간 통보 가능하며, 불법침입, 사라짐, 나타남, 가상의 경계선, 장면의 변화, 가상의 영역 설정, Trip Wire, Trip Wire Zone 생성 기능, 배회, 절도, 투척, 다수의 경계선, 모니터링 기능 등을 제공한다.

이스라엘의 IOimage에서 개발한 Video Analytics는 영상에 다양한 검출 기능을 제공한다. 경계선에 외부인이 침입하면 경고음을 내고, 특정 장소에 출입하는 사람

의 수 및 이동경로를 추적할 수 있으며, Intrusion Detection, Baggage Detection, Object Removal Detection, Autonomous PTZ Tracking, Vehicle Detection 등 다양한 응용 탐지 기능을 제공하며, 탐지된 객체에 대한 행위 이벤트, 이동 이벤트 등 다양한 이벤트 처리 가능하다.

ADT는 영상보안서비스인 'ADT 비디오'를 통해 무인경비서비스와 CCTV를 통해 감시, 녹화 기능을 제공하는 무인경비서비스를 결합한 서비스를 제공하며 DVR 영상 검색은 물론 인터넷과 휴대폰을 통해 실시간 영상 모니터링 기능 등을 지원한다. 전 세계 500대 기업의 90%에 서비스 제공, 현재 세계 무인경비서비스 시장 점유율 70%로 1위, 국내 무인경비서비스 시장 점유율은 30% 정도이다.

최근들어, 고성능 H/W 사양을 갖는 카메라를 기반으로 지능형 인식기능, 보안기능 등을 추가하는 스마트 카메라가 차세대 카메라로 주목을 받고 있다. CPU, DSP, 코덱 등이 내장된 TI의 다빈치 칩이 발매되면서 급격히 스마트 카메라 관련 연구가 늘어나고 있으나 IP 기반 환경에서 활용될 수 있는 진정한 스마트 카메라는 아직 상용화되지 못하고 있다. 향후, IP 카메라는 스마트 카메라로 진화할 수 밖에 없다고 생각된다.

IV. 영상보안시스템 보안이슈

국내의 경우 공공기관의 개인정보 보호에 관한 법률이 개정·공포되어 2008년 11월 부터 시행되고 있다. 이번 개정에는 개인 정보의 범위와 대상을 CCTV에 의해 처리되는 화상정보까지로 확대되었는데 이로 인해 CCTV의 무분별한 설치가 제한될 것으로 보인다. 행정안전부에 따르면 공공기관이 공익 목적으로 설치, 운영하고 있는 CCTV는 약 11만대 정도로 파악하고 있다. 앞으로는 범죄예방, 교통단속 등 공익을 위해 꼭 필요한 경우에 한하여 설치가 허용되며, 설치할 때에는 지역 주민 같은 이해관계자의 의견수렴을 반드시 거쳐야 하도록 했다. 한편, 수집에서 폐기에 이르기까지의 모든 화상정보를 개인정보에 준하는 수준으로 관리할 것으로 명시하고 있으므로, 정보 유출로 인한 사생활 침해 문제는 개선될 것으로 보인다.

이러한 제도적 장치 외에도 사생활을 보호하면서도 영상감시가 가능하도록 하는 보안기술, IP 기반 환경으

로 발전함에 따른 네트워크 보안 및 시스템 보안기술, 물리적인 공격으로부터 영상보안시스템을 보호하기 위한 물리보안기술 등 다양한 보안기술들이 영상보안시스템의 신뢰성 및 제품 경쟁력 강화를 위해 필요한 상황이며, 향후 영상보안제품에 반드시 탑재되어야 할 필수 기능으로 부상될 것으로 예상된다.

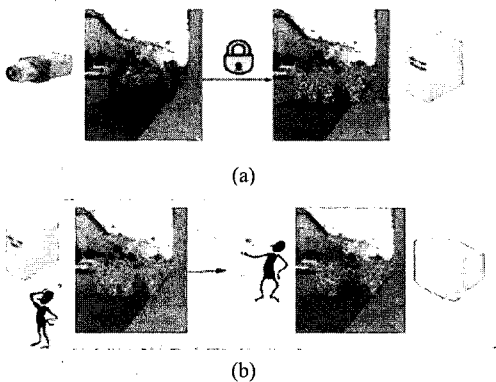
4.1 프라이버시 보호기능

영상감시시스템을 통해 얻을 수 있는 범죄 예방과 같은 순기능도 많지만, 프라이버시 침해와 같은 역기능 문제도 발생되므로 영상보안시스템의 활성화를 위해서는 역기능 문제 해결을 위한 보안기술 도입이 필요하다. CCTV의 천국이라 불리는 영국에서도 프라이버시 침해 문제가 논란이 되고 있으며 최근 공공기관에서 영상보안시스템 구입시 필수 기능으로 프라이버시 마스킹기능의 탑재가 요구되고 있는 상황이다. 미국 Homeland Security에서는 프라이버시 보호를 위해 CCTV 설치 및 운용에 대한 가이드라인을 발표한바 있고, 유럽연합 의회에서도 1995년 개인정보의 수집목적 외 사용금지, 자신의 정보 접근권, 과다 정보수집 금지, 개인정보의 정확성과 안전성, 제3자 제공시 본인동의 등에 대한 '개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침'을 제정했다. 이에 따라 영국, 프랑스, 독일 등은 정보통신 활용기술에 따른 프라이버시 보호문제를 법률로 규제하고 프라이버시 보호 기구와 구제 절차를 명확히 하고 있다. 벨기에, 덴마크, 스웨덴, 네덜란드 등 나머지 유럽국가들도 종업원의 의료정보와 의료검진, 감시장비 도입, 이메일과 전화감시 등에 대해 법으로 금지하고 있다. 그리고 프라이버시 보호를 위한 방안으로 이러한 법적, 도덕적 가이드라인에 그치는 것이 아니라, 새로운 기술개발도 활발히 진행되고 있다. CCTV로 촬영한 영상에서 사람의 모습만을 지우고 저장하는 기술이라든지, 카메라가 스스로 사람의 특정 움직임을 인식하고 필요한 순간에만 DVR에 저장하는 기술 등이 그 예이다.

스위스 EMITALL Surveillance SA에서는 수집되는 영상에 찍힌 사람들의 프라이버시를 보호하기 위해 실시간 영상혼합화기술을 개발하였다. 즉, 영상분석 모듈이 사람이나 자동차의 번호판 같은 사생활과 밀접한 정보가 나타나는 장면을 확인하고, 이와 관계된 구역에 혼합화 기술을 적용하여 암호화된 화면이 나타나도록 하

는 기술이다. 이 혼합화 기술의 특징은 암호화 키를 가진 허가받은 사람만이 원본 화면을 볼 수 있고, 키가 없는 일반인은 사적인 정보가 지워진 왜곡된 화면만을 볼 수 있다는 점이다.

[그림 4]의 (a)에서와 같이 EMITALL 사의 영상 혼합화 기술로 움직이는 사람과 물체를 감지하고, 이들을 모두 혼합화한다. CCTV가 촬영한 영상에서 사람, 자동차 등을 감지하면 암호화 키를 사용하여 스크램블링함으로써 영상을 혼합화 하고, 혼합된 채로 DVR에 저장된다. 사용된 암호화 키를 알고 있는 사람은 키를 입력하여 혼합된 영상을 복호화 함으로써 CCTV가 촬영한 원본 화면을 볼 수 있고, 암호화 키를 알지 못하면 혼합화된 영상만을 볼 수 있다.



(그림 4) 영상혼합화 기능 개념 : (a) 혼합화 과정, (b) 복원 과정

[그림 4]의 (b)에서는 혼합된 영상을 복원하는 것을 보여준다. 불법행위가 감지되면, 영상을 혼합할 때 사용한 암호화 키를 보관하고 있는 신뢰할 만한 기관에서 혼합영상을 복원하기 위한 결정을 내릴 수 있다. 이때, 하나 혹은 여러 개의 암호화 키들을 사용해 시스템은 고소된 개인과 일치하는 영역만을 복원하거나, 영상 전체를 복원할 수 있다. 암호화 키가 혼합된 물체들을 보호하고, 법률기관이나 신뢰할만한 제 3자에 의해 보호된다면 프라이버시는 더욱 안전하게 보호될 수 있을 것이다.

국내의 경우, ETRI에서는 H.264 기반 영상보안시스템용 실시간 프라이버시 마스킹기술이 개발 중에 있다. 2009년 11월경이면 개발이 완료될 예정으로 EMITALL 사의 제품에 비해서 안전성이 뛰어난 장점을 갖고 있

며, 어떠한 H.264 코덱과도 연결할 수 있어 코덱 의존성을 갖는 EMITALL사 기술에 비해 우수하다고 할 수 있다.

4.2 영상보안시스템 보호기능

영상보안시스템은 다양한 영상 정보를 수집하고 가공하여 저장하며, 필요시 인가된 사용자에게만 해당하는 영상 정보를 제공해야 한다. 영상감시시스템이 수집하고 저장하는 모든 영상 정보는 안전하게 처리되어야 하며, 수행 절차 또한 내·외부의 위협으로부터 보호되어야 한다.

특히 IP 기반 영상보안시스템은 공중망을 통해 수집된 영상 정보를 전송하므로 다양한 인터넷 해킹 공격기술이 그대로 적용될 수 있는 문제점을 내포하고 있으므로 IT 보안기술의 도입을 통해 영상보안시스템의 안전성을 확보하는 게 매우 중요하다고 할 수 있다.

영상보안시스템에서는 전송 중인 영상정보에 대한 보호는 물론 저장되고 가공되어 사용자에게 제공되는 영상정보에 대해서도 신뢰할 수 있는 안전한 메커니즘을 제공해야 한다. 따라서, 영상정보 보안 요구사항을 만족하기 위한 보안 기술은 크게 전송되는 영상정보를 보호하기 위한 전송 보안기술과 영상정보를 수집하고 저장하는 카메라 및 DVR 장치 등의 보호를 위한 시스템 보호 기술로 나눌 수 있다.

전송 보안기능은 수집된 영상정보의 안전한 전송 및 신뢰성을 보장하기 위한 보안터널링 기능과 위·변조 방지기능으로 나눌 수 있다. 보안 터널링 기술은 현재 가장 널리 사용되고 안전성이 검증된 IPsec 프로토콜이나 SSL/TLS 프로토콜 등을 활용할 수 있겠지만 IP 카메라의 리소스 제한을 고려할 때 좀더 효율적인 방안의 개발이 필요하다고 생각된다. CCTV나 IP 카메라의 경량화된 사양을 고려하여 상대적으로 무거운 보안터널링 프로토콜의 도입이 어려운 경우, 전송영상에 대한 위·변조 행위를 막기 위한 보안기능이 사용될 수 있다. 물론, 기밀성 등의 기본 보안기능도 필요하지만 다양한 IP 카메라가 여러 응용 환경에서 사용되고 있는 현실을 고려하여 경량 카메라를 위해서는 최소한 위·변조 방지 기능은 제공되어야 한다는 관점에서 기본 보안기능으로 탑재되어야 하겠다.

영상보안시스템용 시스템 보호 기술은 네트워크 칩

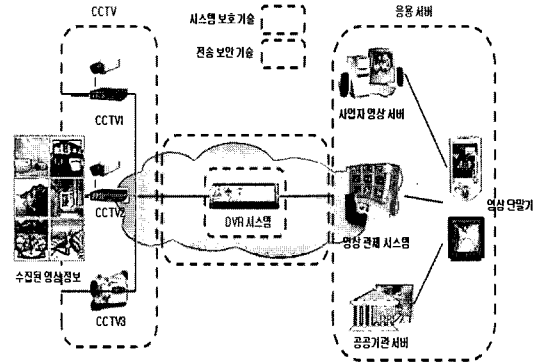
입방지기술, 물리적인 보호기술, 접근제어기술 등으로 구분할 수 있다. 카메라에서 수집되는 영상이 법정에서 디지털 증거로 사용되는 사례가 늘어나고 있으므로 IP 카메라에 대한 네트워크 공격을 통해 제어권을 확보하여 불법적으로 영상을 수집하거나, 또는 수집된 영상을 위·변조하는 경우가 발생할 수 있다. 따라서, IP 카메라를 목표로 하여 발생하는 네트워크 침입을 탐지하고 침입에 적극적으로 대응할 수 있는 네트워크 침입방지 기능 탑재가 필요하다. DVR이나 관제시스템 등은 상대적으로 출입이 제한된 지역이나 Firewall 과 같은 네트워크 보안제품에 의해 보호되는 공간에 설치되는 경우가 많으므로 IP 카메라에 비해서는 네트워크 침입에 대한 대응책이 마련되어 있다고 할 수 있다. 하지만 IP 카메라는 공개된 외부 환경에 노출되어 설치되는 경우가 많으므로 파손 등과 같은 고의적인 물리 공격에 대응할 수 있는 물리보호기능이 요구된다. 특히, 영상보안시스템의 안전성 확보를 위해 암호화 등의 보안기능이 탑재되는 경우, 안전성의 열쇠가 되는 비밀정보가 카메라에 저장될 수 있으므로 물리적인 공격에 의해 비밀정보가 노출되지 않도록 물리보호기능이 반드시 요구되는 기능이라고 할 수 있다. 카메라 하우징부터 물리보호를 고려하여 설계가 되어야 하며 진동이나 광센서 등을 내장하여 물리적인 공격을 감지하여 대처할 수 있도록 해야 한다.

DVR, NVR, 영상저장 서버 등에 저장되어 있는 수집된 정보들을 적정한 절차에 의해 허가된 관계자만이 접근할 수 있도록 접근제어기능이 제공되어야 한다. 또한, 접근제어 기능은 관제시스템에서 영상수집 및 저장, 관찰 등에 대한 오남용방지기능의 역할도 제공할 수 있다. 즉, 카메라를 임의로 조작하여 특정 영상을 확대하여 본다든지 불법적으로 수집된 영상을 저장하는 사례가 발생할 수도 있으므로 접근제어기능이 이러한 보안 사고에 대한 해결책이 될 수 있겠다.

외국의 경우, IP 카메라 등에 이미 보안터널링이나 인증기술 등이 적용된 상용제품이 판매되고 있지만, 국내에서는 일부 업체에서 독자적인 보안 알고리즘 및 프로토콜을 사용해서 구현한 사례가 있다. 하지만 안전성 및 호환성에 문제가 발생할 수 있으므로 안전성이 검증되고 공개적으로 표준화할 수 있는 보안 프로토콜이 사용될 필요가 있다고 생각된다.

ETRI에서는 한국디지털CCTV연구조합 등과 공동으

로 영상보안시스템에 적용될 수 있는 보안기술들을 개발하고 있으며, 2010년에는 개발된 보안기능이 탑재된 상용제품이 판매될 것으로 예상된다.



(그림 5) 영상보안시스템 보호기능 개념

V. 결 론

본 고에서는 국내업체들이 향후 진출해야 할 High-End급 영상보안시장을 고려하여, High-End급 영상보안제품이 갖추어야 할 핵심기능 등을 설명하고 현재까지의 국내외 관련 업체의 상용제품 개발 현황 등에 대하여 정리하였다. 특히, 지식정보보안업체에서 관심을 가져야 할 영상보안시스템용 보안기술에 대해서 집중적인 분석을 하였다.

향후 영상보안시스템이 IP 환경으로 진화함에 따라 관련 시장규모가 더욱 급격히 증가할 것이라고 예상되고 있으며, 관련 제품의 신뢰성 확보 및 제품 경쟁력 강화를 위해서는 보안기술의 탑재가 필수적이 될 것으로 예상된다. 따라서, 지식정보보안업체들이 좀더 관심을 갖고 투자해야 할 분야라고 생각되며 특히, 사생활 침해 문제는 영상보안제품 활성화에 실질적인 장애가 될 수 있으므로 프라이버시 마스킹 솔루션은 최우선적으로 영상보안시스템용 보안제품으로 활성화될 가능성이 높은 제품이라고 생각된다.

참고문헌

- [1] 이민영, CCTV 규제 현황과 그 시사점, 정보통신정책 제18권 12호, 2006.
- [2] 이민영, 방법용 CCTV 운용에 대한 항고소송검토,

정보통신정책 제16권 23호, 2004.

[3] ETRI, 영상감시시스템의 안전성 확보를 위한 보안기술연구, 2008.

[4] <http://epic.org/privacy/surveillance>.

[5] http://pi.gn.apc.org/issues/cctv/_index.html.

[6] http://mvqst.hubweb.net/html/camera1/Docu/convert_cctv_to_IP_sur.pdf.

[7] http://www.boannews.com/know_how/view.asp?idx=2372&search=title&find=CCTV.

[8] http://www.boannews.com/know_how/view.asp?page=1&gpage=1&idx=2369&numm=2005&search=title&find=&kind=03&order=ref.

[9] http://www.boannews.com/know_how/view.asp?page=1&gpage=1&idx=1681&numm=1353&search=title&find=카메라&kind=03&order=ref.

[10] http://cafe.naver.com/yk6494.cafe?iframe_url=/ArticleRead.nhn%3Farticleid=1418.

[11] Stephen Russell, Searchable Surveillance, 국제통합보안&지능형 감시솔루션 구축전략 컨퍼런스, 2008.

[12] 이승노, IP 기반 지능형 보안체계 구축방법과 활용방안, 국제통합보안&지능형 감시솔루션 구축전략 컨퍼런스, 2008.

[13] 최수기, 지능형 영상분석기술과 국내 대형사이트의 적용사례, 국제통합보안&지능형 감시솔루션 구축전략 컨퍼런스, 2008.

[14] 한종욱, 물리보안과 IT보안의 융합화 추세, 국제통합보안&지능형 감시솔루션 구축전략 컨퍼런스, 2008.

[15] 공공기관에서의 지능형 CCTV 운영 패러다임의 변화와 구축사례, 국제통합보안&지능형 감시솔루션

구축전략 컨퍼런스, 2008.

[16] Herman Kruegle, CCTV Surveillance, Second Edition: Video Practices and Technology, Butterworth-Heinemann, 2006.

[17] Damjanovski, Digital CCTV : A Security Professional's Guide, Butterworth-Heinemann, 2007.

[18] <http://www.emitall.com/>.

〈著者紹介〉

한종욱 (Han, Jong Wook)

정회원

1985년 2월: 광운대학교 전자공학과 졸업

1991년 2월: 광운대학교 전자공학과 석사

2001년 2월: 광운대학교 전자공학과 박사

1991년 3월~현재: 한국전자통신연구원 책임연구원/융합서비스보안연구팀장

<관심분야> 융합보안, 물리보안



조현숙 (Cho, Hyun Sook)

정회원

1979년 2월: 전남대학교 수학교육과 졸업

2001년 2월: 충북대학교 박사

1982년 3월~현재: 한국전자통신연구원 책임연구원/지식정보보안연구부장, 정보보호연구본부장 역임

<관심분야> 정보보안

