情 報 保 護 學 會 誌
第20卷 第3號, 2010. 6

차세대 영상보안 기술 동향

전 용 성*, 한 종 욱*, 조 현 숙**

요 약

본 논문에서는 현재 산업체뿐 만 아니라, 개인 생활에 많은 영향을 미치고 있는 영상보안 산업의 기술 현황을 살펴보고, IP 환경으로 진화함에 따른 차세대 영상보안시스템이 가져야할 요구사항과 이에 대한 국내외 기술개발 현황을 살펴보았다. 특히, 영상보안 기술의 발전 방향으로 예상되는 고해상도 네트워크 카메라, NVR, 그리고 차세대 영상보안을 선도할 스마트카메라 기술에 대해 분석하였다.

Ⅰ. 서 론

하나의 산업이 발전하는 단계를 살펴보면 점진적으로 발전하는 산업도 있지만, 어떤 산업의 경우에는 어느 한 순간 특별한 계기에 의해 갑작스러운 성장을 하거나 혹은 산업의 패러다임이 바뀌는 경우도 허다하다. 특히 IT산업의 경우는 더욱 그러하다. 한 예로 휴대폰 산업의 경우, 애플사의 "아이폰"이 출현하기 전만해도 휴대폰의 발전은 아주 점진적인 발전 단계를 거쳐왔다고 할 수 있다. 단순한 전화 기능에서 카메라 기능이 추가되고 또한 PDA기능이 휴대폰에 통합되는 등 어느 정도 예측 가능한 범위에서의 점진적인 발전단계를 밟아왔다고 할 수 있다. 그러나 애플사의 아이폰의 등장은 어느 한순간 "휴대폰"이란 이름이 "스마트폰"이라는 이름으로 바뀌는 계기를 마련하게 되었다.

또 하나의 예를 들자면 제임스 카메론감독의 "아바타"란 영화이다. 이 영화는 국내에서만 1000만 이상의 관객을 동원하고 전 세계적으로는 25억불 이상의 수익을 달성하는 큰 흥행을 거두게 된다. 이 영화를 주목해야하는 이유는 단순히 흥행에 성공한 것이 아니고 3D 영화의 르네상스를 열게 된 시발점이란 것이다. 이 영화 이후 제작되는 블록버스터 영화는 3D로 제작하는 것이 당연시되고 있다. 또한 이 영화를 계기로 3D TV산업의 문이 활짝 열리게 되었다.

이상으로 언급한 애플사의 아이폰과 제임스 카메론 감독의 아바타 영화를 통해 한 가지 중요한 사실을 알고 지나갈 필요가 있다. 그것은 이 두 가지 제품이 출시될 시점에 벌써 이 제품들을 만들 수 있을 만큼의 기술적인 수준이 충분히 성숙해 있었다는 것이다. 제임스 카메론 감독이 이야기하기를 90년 중반 아바타를 제작하고 싶었지만 그 때는 기술적인 문제가 있어서 2000년대 중반이 되어서야 시작하게 되었다고 한다. 결국, 어떤 제품(혹은 콘텐츠)을 만들기 위한 기술적인 문제가 없다고 판단되는 시점이 되면, 현재의 기술을 충분히 이용한 획기적인 제품이 출시되는 것은 시간 문제이며, 비록 그 제품의 가격이 다소 비싸더라도 시장은 새로운 제품을 선택하게 된다는 것이다.

이상으로 설명한 예를 바탕으로 이제 영상보안 산업의 현재의 기술 수준을 알아보자. 현재 영상보안 시장은 마치 애플사의 스마트 폰이 출시되기 직전의 시점, 또는 제임스 카메론 감독의 아바타가 나오기 직전의 시점이라고 할 수 있다. 즉, 기존의 아날로그 CCTV 카메라를 뛰어넘어 영상 보안 시장의 패러다임을 바꿀 수 있는 제품이 시장을 지배할 시점이 다가왔다는 것이다.

먼저, 기대할 만한 제품으로는 고해상도의 네트워크 카메라라고 할 수 있다. 아직은 기존의 아날로그 카메라가 대세를 이루고 있지만 새로운 형태의 고해상도 네트워크 카메라가 속속 출시되고 있다. 현재는 고해상도 네트워크 카메라의 시장점유율이 10%도 되지 않지만 (일부에서는 2-3%로 보고 있음) 카메라가 네트워크에 접

* 한국전자통신연구원 융합서비스보안연구팀 (ysjeon@etri.re.kr, hanjw@etri.re.kr)
** 한국전자통신연구원 지식정보보안연구부 (hscho@etri.re.kr)

속되고 해상도가 메가픽셀로 올라가는 것은 거역할 수 없는 대세일 것이다. 앞으로도 아날로그 카메라의 수요가 어느 정도는 유지되겠지만, 영상보안의 패러다임이 고해상도의 네트워크 카메라로 넘어가는 것은 시간문제일 것이다. 그 이유는 고해상도의 네트워크 카메라를 만들기 위한 기술적인 문제가 거의 대부분 해결되었기 때문이다. H.264 압축 방식이 카메라에 적용되면서 메가픽셀급의 고해상도 영상을 네트워크로 보내는 것이 훨씬 용이하게 되었다. 또한 네트워크 인프라가 급속도로 향상되었기 때문이다. 단지 고해상도 네트워크 카메라의 비용이 비싼 단점이 있지만 메가픽셀급 카메라 한 대가 저해상도 아날로그 카메라 몇 대가 담당하는 영역을 감당할 수 있기 때문에, 충분히 시장성이 있다고 판단된다. 또한 이 고해상도의 네트워크 카메라를 이용한 다양한 응용 산업의 출연도 가능하다.

또 하나의 영상보안 시장의 패러다임을 바꿀 수 있는 제품은 지능형 영상인식이 가능한 스마트 카메라일 것이다. 이 또한 지능형 영상인식을 임베디드 시스템에 접목할 수 있는 기술적인 문제가 충분히 해결되었다고 할 수 있다. 현재, 카메라에 사용되는 임베디드 CPU의 처리속도가 충분히 향상되었으며, 영상처리를 위해 별도의 코프로세서로 사용될 수 있는 DSP 또는 FPGA 등이 충분한 성능과 가격 경쟁력을 가지고 있기 때문에, 기존의 영상 인식 기능을 훨씬 뛰어 넘어 시장의 요구를 충분히 만족할 수 있는 지능형 영상인식이 가능한 스마트 카메라의 출현이 가능한 시점이라고 할 수 있다.

Ⅱ. 영상보안 산업 개요

영상보안 산업은 감시카메라 및 영상녹화장치를 기반으로 하는 보안 장비 및 서비스 산업을 지칭한다. 감시카메라의 대표적인 것으로는 CCTV(Closed Circuit Television)가 있고 영상녹화장치의 대표적인 것으로는 DVR(Digital Video Recorder)이 있다.

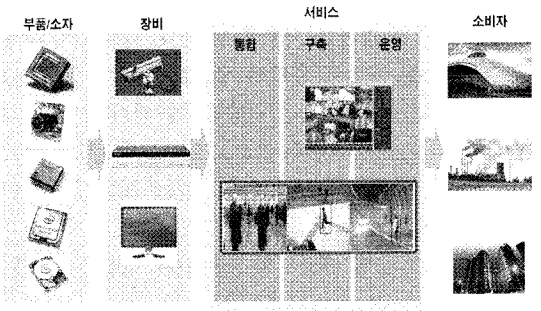
부품/소자는 CCD, 카메라모듈, 비디오 인코더/디코더 Chip, CPU, HDD, LCD 모듈 등이 이에 해당한다. 장비는 이들 부품/소자를 이용한 단일 제품으로 CCTV, IP Camera, VCR, DVR, LCD Monitor 등이 이에 해당한다. 서비스는 소비자를 대상으로 보안서비스를 제공하는 회사로 우리나라의 S1, ADT Caps와 같은 회사들이다. 이들은 장비 회사로부터 개별 장비를 납품 받아 소비자의 요구에 맞는 보안시스템을 만들어 통합, 설치(구축)하고 운영한다. 소비자는 공공부분(군, 정부기관, 공항, 항만, 도로, 철도 등)과 민간부분(공장, 백화점, 금융기관, 사업장, 주택 등)으로 나누어 볼 수 있다.

[그림 1]에서 보듯이 장비는 서비스 업체를 통해서 소비자에 전달되므로 B2B(Business to Business) 시장으로 규정할 수 있다. 이러한 특성으로 인하여 장비시장에서 기술 장벽은 높지 않으나, 시장진입 장벽은 높다고 할 수 있다.

전 세계적으로 주요브랜드 감시 카메라 시장 규모는 2005년 475만 대에서 2008년에는 720만 대로 급격히 증가하였다. 그러다가 2009년에 경제 불황으로 인해 감소세를 보였으나 2010년부터는 성장세를 회복하여 2012년에는 전 세계적으로 825만 대가 출하될 것으로 예상되고 있다[1]. 그리고 전체 영상보안 산업에서 장비와 서비스의 시장 규모 비율은 3:7 정도로 추정하고 있다.

DVR의 경우 1997년 국내 기업들이 개발에 성공한 이후 MP3 Player, DTV Set-top-box 등과 같이 국내 중소기업들이 세계 시장을 선도하는 몇 안되는 제품 중 하나이다. 하지만 국내 DVR 산업의 경우 한때 세계시장 점유율 55%를 차지했으나 2006년에는 30%로 낮아진 상태이다. 이는 저가 시장에서 중국 및 대만 업체에 비해 가격 경쟁력이 떨어지고 있고, 고가 시장에서 미국과 일본의 업체에 기술력에서 뒤지고 있는 것으로 풀이된다.

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 예상이 된다. 이러한 변화로 인하여 기존 DVR 중



〔그림 1〕 영상보안 산업의 관계도

심의 영상저장 장치는 DVR 장치 외에 별도의 비디오 저장장치를 두는 형태로 발전하고 있으며, 영상보안시스템을 구성하는 주요 장치인 카메라는 아날로그 CCTV에서 IP기반의 네트워크 카메라로 발전하고 있다. CCTV는 영상 수집을 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. 또한 동영상을 단순히 녹화하는데 그치지 않고 객체인식, 추적, 얼굴인식 등이 가능한 지능형 제품으로 발전하고 있다[2].

Ⅲ. 영상보안 기술 전망

영상 보안 기술은 시장 수요에 부합하기 위해 급속한 발전을 거듭하고 있다. 앞 장에서 언급한 바와 같이 기존의 아날로그 카메라의 낮은 해상도에서 메가픽셀급의 고해상도 카메라로 발전하고 있다. 고해상도 카메라는 메가픽셀의 영상을 전송하기 위해, H.264압축 기술을 이용한 네트워크 카메라 형태로 자연스럽게 발전하고 있다. 또한 지능형 영상인식을 위한 스마트카메라의 필요성이 어느 때 보다 커지고 있다. 본 장에서는 이와 같은 영상보안 기술의 발전 방향에 대하여 알아본다.

3.1 메가픽셀 IP 카메라

지금까지도 카메라의 해상도는 화소 기준으로 D1급 (720 * 480, NTSC방식 기준)이 주류를 이루고 있으나, 근래에 들어 해상도가 SXGA급 (1280 * 1024)이상의 메가픽셀 카메라가 시장을 빠르게 차지하고 있다. TV에서도 이미 HDTV를 방송으로 수신하고 있는 추세이기 때문에 이제는 카메라에서의 영상을 받아들이는 화질도 매우 중요하게 되었다. TV의 디지털화와 디스플레이 모니터의 고화질화가 지속되고 있으며, 카메라의 CCD 및 영상처리 칩의 성능향상으로 고해상도 영상을 제공하는 환경도 빠르게 발전하고 있다 [3]. 또한, 메가

〔표 1〕 카메라 해상도에 따른 픽셀 수

구분	해상도	사이즈	픽셀수 (Mega)
NTSC 해상도	D1	720*480	0.35
디스플레이 해상도	XVGA	1024*768	0.79
	SXGA	1280*1024	1.3
	UXGA	1600*1200	1.9
	QXGA	2048*1536	3.1
HDTV 해상도	720p	1280*720	0.92
	1080p	1920*1080	2.1

픽셀 카메라 한대가 기존 아날로그 카메라 2-3대의 감시영역을 감당할 수 있기 때문에, 수요가 더욱 늘어날 것으로 보인다.

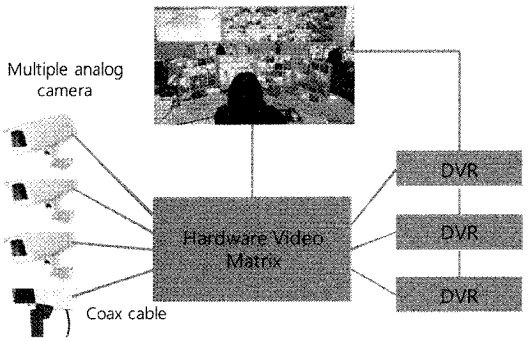
카메라 해상도가 메가픽셀로 가기 위해서는 카메라 내부에 영상을 압축하고, 이를 네트워크로 보내는 기능을 함께 가지게 된다. 따라서 메가픽셀 카메라는 자연스럽게 영상압축을 지원하는 네트워크 카메라의 형태를 띄게 된다.

그러나 메가 픽셀 카메라가 시장 점유율을 좀 더 높이기 위해서는 데이터 전송을 위한 충분한 네트워크 대역폭을 확보하여야 한다. H.264 압축방식으로 전송 데이터의 량이 현저히 줄기는 했지만, 아직은 메가픽셀이 요구하는 네트워크 대역폭을 만족시키기 위해서는 CCTV를 위한 네트워크 인프라가 좀 더 확충되어야 한다. 현재는 기가급 네트워크가 등장하는 등 네트워크 기술이 빠르게 향상되고 있고, 저장장치의 가격하락이 빠르게 진행되고 있고 있기 때문에, 향후 폭발적인 증가세를 보일 것으로 보고 있다[4].

3.2 DVR에서 NVR로

현재, 네트워크 비디오 저장 S/W 또는 NVR (Network Video Recoder)는 저장을 기반으로 하는 DVR

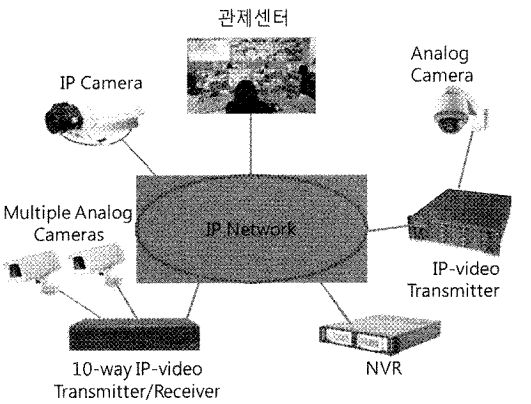
〔그림 2〕 카메라의 해상도에 따른 성능



〔그림 3〕 DVR을 이용한 아날로그 시스템 구성도

(Digital Video recoder)시장을 넘어 서고 있다. 먼저, DVR과 NVR에 대한 차이를 살펴볼 필요가 있다. DVR과 NVR 사이의 가장 분명한 차이는 DVR은 아날로그 카메라에서 제공되는 아날로그 스트림을 녹화하는 반면, NVR은 카메라에서 이미 인코딩된 비디오 스트림을 녹화한다. 따라서 NVR 상에서는 어떤 영상 커넥터도 찾을 수 없고, NVR의 입-출력은 압축되고 인코딩된 영상으로 이루어진 IP 데이터이다.

DVR은 감시영상을 디지털로 변환-저장하는 방식이다. CCTV는 잦은 비디오 테이프의 교체, 반복사용에 따른 화질열화, 화면 떨림, 잡음현상 등의 문제점을 안고 있으나 DVR에서는 이 같은 문제점이 해소된다. 또한 DVR은 녹화뿐만 아니라 동작 감지 등 각종 센서와 연결하여 각 채널의 auto plan, 제어기능 및 화상 확대, 편집 기능 등 다양한 기능을 가지며 데이터를 HDD 등의 디지털 저장 및 백업장치에 반영구적으로 보관할 수 있어 기존 아날로그 CCTV 시스템을 급속히 대체하고



〔그림 4〕 NVR을 이용한 IP 영상 네트워크 구성도

있다[5].

그러나 카메라의 설치 숫자가 수백대를 넘어서는 경우에는, 카메라의 모니터링을 위하여 기존의 DVR로는 구조적인 해결이 어렵게 된다. 이러한 환경에서는 기존의 DVR을 이용한 시스템 구성으로는 어려움이 있고 NVR을 이용하는 것이 당연한 해결책으로 제시된다.

NVR은 녹화와 재생을 동시에 수행하고, 한 장치에 녹화된 것은 네트워크 전체에 걸쳐 동시에 흩어진 다수의 허가받은 운영자들이 원격으로 살펴볼 수 있는데, 각자 독립적이기 때문에 서로 영향을 미치지 않는다. 그리고 NVR을 이용하면 네트워크상의 어떤 지점에서 녹화가 필요하면 운영자에 의해 끊임없이 영상을 수집할 수 있다. 또한 NVR은 확장이 용이하기 때문에, 시스템 전체에 걸쳐 많은 수의 NVR을 보유하고 있더라도 하나의 NVR을 더 추가하기 위해서는 단지 네트워크에 접속만 하면 된다[6].

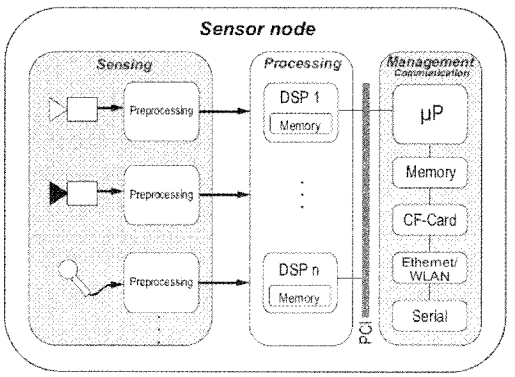
NVR의 가장 큰 경쟁력은 서로 다른 제조사의 IP 카메라와의 호환성을 들 수 있다. 이 호환성을 확보하기 위해서는 protocol 표준화 (ONVIF, PSIA)가 이루어져야 한다. 현재 국내에서도 "K-Protocol" 이란 이름의 영상보안 기기간의 호환성을 위한 protocol 표준화작업이 이루어지고 있다.

3.3 영상인식기능을 위한 스마트 카메라

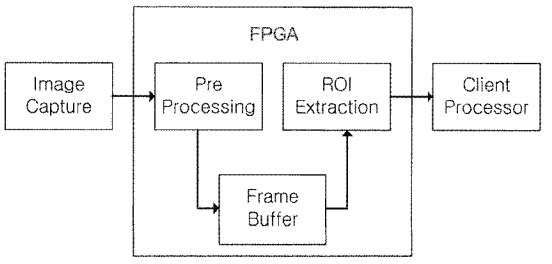
최근 유비쿼터스 기술의 등장은 CCTV 카메라 및 DVR 기술에서도 많은 변화를 가져오고 있다. 앞서 설명한 바와 같이 기존의 DVR 제품은 점차적으로 네트워크를 강화한 NVR 제품으로 전환되고 있는 추세이다. CCTV 카메라 또한 통신 및 기본적인 영상처리 모듈을 내장하는 등 스마트 카메라기술로 발전하고 있다. 스마트 카메라 기술은 최근의 IP 카메라, 임베디드 시스템의 발전과 급속한 영상 감시 카메라의 보급에 따른 영상인식 성능향상 및 분산처리 기술의 필요성에 따라 새롭게 이슈화되고 있다. 스마트 카메라는 가시 및 적외선 영상의 센서레벨 융합, 스테레오 영상의 획득, 영상 전처리, 움직임 추적, 영상 검출 및 추적 등 특정 응용 영역에 관계 없이 요구되는 카메라 레벨의 공통 영상처리 모듈을 구현하여 카메라 장치에 내장하는 기술을 연구하고 있다. 기본적으로 스마트 카메라는 임베디드 컴퓨터 기술을 전제로 하고 있어서, 최근만 해도 시

스템의 성능상 제약으로 구현 가능한 알고리즘은 매우 제한적이었다[7].

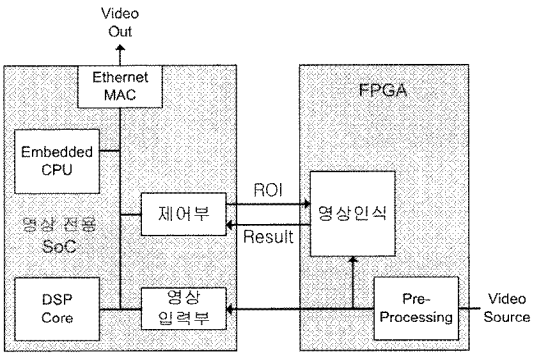
기존의 스마트카메라는 PC기반의 영상시스템을 기반으로 하는 것이 대부분이다. PC기반 스마트 카메라에서, 카메라는 웹캠 또는 CCTV 카메라와 같이 일반적인 카메라이고, 이들 카메라의 영상 출력이 동축 케이블, USB, 이더넷 등과 같은 통신 수단을 이용하여 PC와 연결되는 형태이다[8]. 그러나 이와 같은 형태는 많은 단점을 가지고 있다. 즉, 일반 PC는 고해상도 및 높은 프레임 전송률을 가지는 비디오 출력을 처리하기에는 한계가 있다. 또한, 카메라 영상을 압축 없이 PC와 연결하는 경우에는 PC와 카메라 사이의 전송 대역폭은 감당하기 어려울 정도로 높아지게 된다. 따라서 스마트 카메라 내부에 프로세서를 내장함으로써, 고해상도 및 높은 프레임 전송이 필요한 영상을 직접 처리하는 것이 보다 좋은 방법이라고 할 수 있다. 또한 카메라 내부에 영상 압축 기능을 구현함으로써 카메라의 전송 대역폭을 감소시킬 수 있다. 뿐만 아니라 현재의 스마트 카메라는 지능형 인식뿐 아니라 영상압축 등과 같은 많은 기능을 필요로 하고 있다.



〔그림 5〕 DSP를 이용한 스마트 카메라



〔그림 6〕 FPFA를 이용한 스마트 카메라

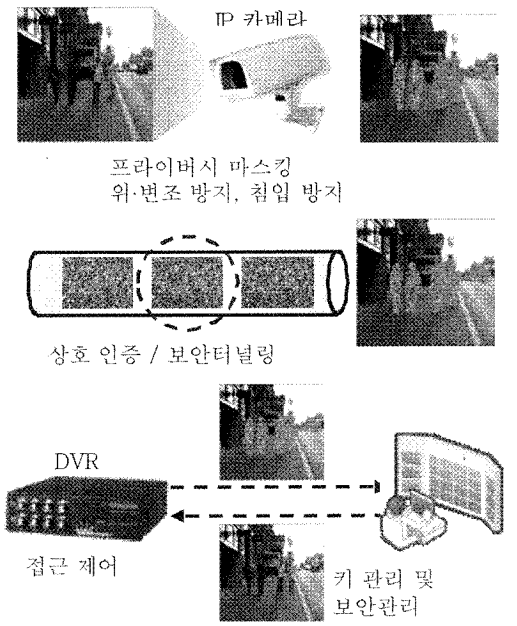


〔그림 7〕 영상전용 SoC와 FPGA의 융합 구조를 가지는 스마트 카메라

현재의 영상시스템 요구사항들은 기존의 임베디드 프로세서만을 이용하는 스마트 카메라 구조로는 감당할 수가 없게 되었다. 이를 위해 [그림 5]와 [그림 6]과 같은 DSP 또는 FPGA를 이용한 스마트 카메라의 설계 방법이 제시되고 있다[9, 10]. 또한, 프로세서 내에 DSP 뿐만 아니라 영상압축 기능까지도 내장한 영상보안용 SoC 제품이 출시되고 있다. 이와 같이 DSP 및 영상압축 기능을 하나의 칩으로 구현한 영상전용 프로세서로는 TI사의 DaVinci칩이 대표적이라고 할 수 있다 [11]. 보다 고도화된 영상 처리 기능이 가능한 스마트 카메라를 위해서는 [그림 7]과 같은 스마트카메라 구조를 생각해 볼 수도 있다. 이 구조에서는 영상 전용 Soc와 FPGA를 융합하여 좀 더 고성능의 영상인식이 가능한 스마트 카메라를 구현할 수 있다. 이미지 센서로부터 획득된 영상은 FPGA를 거쳐서 영상전용 SoC로 입력된다. 이 때 FPGA에서는 영상의 전처리 및 영상인식 기능을 담당하고, 영상 전용 프로세서에서는 영상의 압축, 압축된 영상의 네트워크를 통한 전송, 그리고 기타 보안 기능 등을 수행하게 된다. 이와 같은 영상전용 SoC와 FPGA의 융합 설계는 스마트카메라에 필요한 요구사항을 두 개의 소자에 적절히 분배함으로써 스마트 카메라의 기능을 극대화할 수 있는 장점을 가진다.

Ⅳ. 영상보안시스템 보안이슈

국내의 경우 공공기관의 개인정보 보호에 관한 법률이 개정·공포되어 2008년 11월부터 시행되고 있다. 이번 개정에는 개인 정보의 범위와 대상을 CCTV에 의해



〔그림 8〕 영상보안시스템 보안 이슈들

처리되는 화상정보까지로 확대되었는데 이로 인해 CCTV의 무분별한 설치가 제한될 것으로 보인다. 행정안전부에 따르면 공공기관이 공익 목적으로 설치, 운영하고 있는 CCTV는 약11만대 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 환경으로 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 탑재되어야할 필수 기능으로 부상될 것으로 예상된다[2].

4.1 보안 요구사항

영상보안 시스템에서 요구되는 보안 요구사항을 나열하면 다음과 같다[12].

가. 프라이버시 마스킹

영상수집 모듈에 의해서 수집되고 저장되는 영상 정보에는 사람, 자동차 및 개인 사생활 공간정보가 포함되어 있기 때문에, 이러한 정보를 보호하고 불법 노출을 방지할 수 있는 기술이 필요하다. 프라이버시 마스킹은 창문 등과 같이 고정된 관심 지역을 보호하기 위한 정적 프라이버시 마스킹 방식과 사람, 자동차 번호판 등과 같이 움직이는 영역을 보호하기 위한 동적 프라이버시 마스킹 방식이 있다. 다음 절에서는 이 프라이버시 마스킹 기술에 대한 구체적인 내용을 기술한다.

나. 사용자/디바이스 인증

영상보안 시스템을 구성하는 영상수집 모듈, 영상저장 모듈, 영상서비스 모듈은 공용 IP망을 기반으로 동작하기 때문에 이들 모듈간의 신뢰관계를 구축할 필요가 있다. 또한 시스템에 접근하는 사용자를 인증하기 위한 사용자 인증 모듈이 필요하다.

다. 보안 터널링

공용 IP망을 통해서 전송되는 모든 영상 정보를 외부의 불법 접근에 그대로 노출될 수 밖에 없기 때문에, 이러한 문제점을 해결하기 위해서는 통신하는 두 모듈 간 신뢰할 수 있는 채널을 설립하고 이를 기반으로 암호화된 영상정보를 전송할 수 있어야 한다.

라. 접근 제어

비록 영상 정보를 관리하고 제어할 수 있는 그룹에 속한 사용자라 할지라도 각기 다른 접근 권한을 부여함으로써, 영상정보의 안정성과 신뢰할 수 있는 운용을 보장할 수 있어야 한다.

마. 침입방지

내-외부의 불법 침입으로부터 영상정보를 보호하고 개인 사생활 정보의 침입을 방지하기 위해서는 침입을

실시간 탐지하고 대응할 수 있는 침입 방지 기술이 필요하다. 침입 방지 방식은 기존 IT망을 통한 침입에 대응하기 위한 논리적 침입방지 기술과 영상보안장비에 근원적으로 접근을 방지하기 위한 물리적 침입방지 기술로 구분될 수 있다.

4.2 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, 유럽연합의회에서도 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 유럽 국가들도 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 하는 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.

국내의 경우, ETRI에서는 H.264 기반 영상보안시스템용 실시간 프라이버시 마스킹기술이 개발 중에 있다. EMITALL사의 제품에 비해서 안전성이 뛰어난 장점을 갖고 있으며, 어떠한 H.264 코덱과도 연결할 수 있어 코덱 의존성을 갖는 EMITALL사 기술에 비해 우수하다고 할 수 있다.

4.3 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. 물

론, 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 침입방지기술, 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 발생되는 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 암복화 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 적절한 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 보안사고에 대한 해결책이 될 수 있겠다.

외국의 경우, IP 카메라 등에 이미 보안 터널링이나 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.

V. 결 론

본 논문에서는 영상보안 산업의 기술 현황을 살펴보고, IP 환경으로 진화함에 따른 차세대 영상보안시스템이 가져야할 요구사항과 이에 대한 국내외 기술개발 현황을 살펴보았다. 특히, 영상보안 기술의 발전 방향으로 예상되는 고해상도 네트워크 카메라, NVR, 그리고 차세대 영상보안을 선도할 스마트카메라 기술에 대해 분석하였다.

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 예상이 된다. 따라서 지식정보보안업체들이 좀더 관심을 갖고 투자해야할 분야라고 생각된다.

또한, 지능형 영상 인식을 위한 영상보안 application에 PC기반의 머신 비젼 요구는 향후에도 여전할 것으로 판단된다. 하지만 기술의 발달에 따라 스마트 카메라의 성능은 급속하게 개선될 것이다. 따라서 PC 기반 기술을 사용하는 지능형 영상인식 영역에 스마트카메라가 진입하는 것은 시간문제일 것이다.

참고문헌

[1] 최신 IT 동향, 정보통신산업진흥원, 2009년

[2] 한종욱, 조현숙, "영상보안시스템 기술 동향", 정보보호학회지, 2009년 10월.

[3] 이강석, "네트워크 영상시스템의 변화", CCTV저널, 2009년 7월.

[4] 메가 픽셀 or HDTV 카메라?", 시큐리티 월드, 2009년 11월.

[5] DVR 시장 동향 및 국내외 개발 현황, ETRI 전자통신동향 분석, 24(3), 2009년 6월.

[6] 디지털영상저장시스템_DVR_Vs_NVR.doc,http://www.viewrunip.co.kr/board/board.php?board=gongji&page=6&command=body&no=18

[7] 유장희, 문기영, 조현숙, "지능형 영상보안 기술 현황 및 동향", ETRI 전자통신동향분석, 23(4), 2008년 8월.

[8] Y. Shi and T. Tsui, "An FPGA-based smart camera for gesture recognition in HCI applications," Computer Vision - ACCV 2007, Springer Berlin / Heidelberg, pp. 718-727, 2007.

[9] Y. M. Mustafah, A. Bigdeli, A. W. Azman, and B. C. Lovell, "Smart cameras enabling automated face recognition in the crowd for intelligent surveillance system," International workshop in distributed smart cameras, 2006.

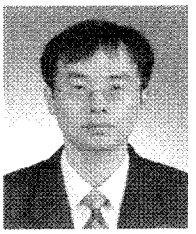
[10] M. Bramberger, A Doblander, A. Maier, B. Rinner, and H. Schwabach, "Distributed embedded smart cameras for surveillance applications," IEEE computer magazine, vol. 39, no. 2, pp68-75, Feb. 2006.

[11] 비디오 감시를 위한 TI 다빈치의 사용, http://www.tikorea.co.kr/article/08sep_num02.asp

[12] 김건우, 한종욱, "안전한 영상보안시스템을 위한 보안 요구사항", 한국통신학회 하계학술대회, 2009년 6월.

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

〈著者紹介〉



전 용 성 (Jeon, Yong Sung)
정회원

1990년 2월: 경북대학교 전자공학과 졸업
1992년 2월: 경북대학교 전자공학과 석사
1992년 3월~1999년 10월: 국방과학연구소 선임연구원
1999년 11월~현재: 한국전자통신연구원 책임연구원
<관심분야> 물리보안, 스마트카메라

한 종 욱 (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

조 현 숙 (Cho, Hyun Sook)
정회원

1979년 2월: 전남대학교 수학교육과 졸업
2001년 2월: 충북대학교 박사
1982년 3월~현재: 한국전자통신연구원 책임연구원/지식정보보안연구부장, 정보보호연구본부장 역임
<관심분야> 정보보안