JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

기반 기술

**J. Adv. Navig. Technol.** 18(6): 588-593, Dec. 2014

# 푸시 서버와 스마트 디바이스를 이용한 영상보안 시스템

# Image Security System Using Push Server and Smart Device

**박 승 환[1] · 오 유 철[2] · 김 창 복[3*]**
[1]을지대학교 의료공학과
[2]사이냅소프트 개발부
[3]가천대학교 에너지 IT학과

**Seung-Hwan Park[1] · U-Chul Oh[2] · Chang-Bok Kim[3*]**
[1]Department of Biomedical Engineering, Eulji University, Gyeonggi-do 461-713, Korea
[2]Department of Development, SynapSoft, Seoul 184-1, Korea
[3]Department of Energy IT, Gachon University, Gyeonggi-do 461-701, Korea

**[요 약]**

최근 스마트 디바이스는 성인 대다수가 보유하고 있으며, 다양한 개인화 서비스가 제공되고 있다. 본 논문은 스마트 디바이스를 이용하여 보안이 요구되는 장소에 실시간으로 침입 여부를 감지하는 경량의 지능형 영상보안 시스템을 제안하였다. 제안 영상보안 시스템은 누적영상 기반의 차 영상과 동적 배경 갱신 알고리즘을 사용하여 침입여부를 인식하였다. 침입통지는 사용자 모바일 디바이스의 어플리케이션 단위로 메시지를 전송할 수 있는 GCM (Google cloud message) 푸시서버와 전자 메일 표준 프로토콜인 SMTP (simple mail transfer protocol) 메일서버를 이용하였다. 침입자가 발생했을 경우에, GCM 푸시서버는 실시간으로 개인 모바일 디바이스에 푸시 메시지를 전송하고, SMTP 메일서버는 침입자 사진과 침입시간이 전송하였다. 제안 영상 보안시스템은 영상 처리 알고리즘과 스마트 디바이스의 성능을 융합하여 다양한 지능형 영상 보안 분야에 응용할 수 있다.

**[Abstract]**

Recently, the smart devices has been possessed by a large majority of the adult, and offered various personalization services. This paper proposed the lightweight Intelligent Image Security System that notice the existence of any intruder in real time at the place of requiring the security by using smart device. The proposed image security system recognized whether or not intruder exists using the difference frame on the basis of Integral Image and the dynamic background updating algorithms. The intrusion notification is achieved by using the GCM push server that send massages in the application unit of user mobile device, and the SMTP mail server which is use of e-mail standard protocol. In case of the occurrence of intruder, GCM push server send an push-massage by the private mobile device, and SMTP mail server send the intruder's photograph and intrusion time. By the convergence of the various image processing algorithms and the performance of smart device, The proposed image security system can be applied to the various Intelligent Image Security field.

**Key word :** Intelligent image security, Image processing, SMTP, GCM, 3'rd party server.

**http://dx.doi.org/10.12673/jant.2014.18.6.588**



**Received** 17 November 2014; **Revised** 24 November 2014
**Accepted (Publication)** 16 December 2014 (30 December 2014)

***Corresponding Author ;** Chang-Bok Kim

**Tel :** +82-32-820-4294
**E-mail :** cbkim@gachon.ac.kr

## Ⅰ. 서 론

영상보안기술은 각종 시설물의 감시에서 부터 범죄예방, 가정 및 개인의 보안을 위해 영상을 이용하는 기술로서, 영상을 이용하는 보안에 대한 관심 증가로 응용 영역이 확대되고 있다. 기존의 영상보안은 영상을 직접 감시하거나, 영상을 저장한 후 필요에 따라 검색하는 수준이었다. 그러나 최근 영상장치의 급격한 증가로 직접감시 및 분석에 한계가 있어, 실시간으로 자동감시 및 분석이 가능하도록 지능적으로 진화하고 있다. 지능형 영상보안기술은 영상장치, 영상 분석 및 인식 기술, 광대역 통신망, IP 기반 네트워크를 결합하여, 특정객체의 탐지, 추적, 식별, 행위 분석을 통하여 객체의 행위나 상호작용을 해석하는 것이다[1].

최근 모바일 디바이스는 성인 대다수가 보유하고 있으며, 다양한 개인화 서비스가 제공되고 있다. 모바일 디바이스에서 서버에 정보를 제공받기 위한 기술로서 풀(pull) 기법과 푸시(push) 기법이 있다. 푸시기법은 모바일 디바이스에 사용자가 요청하지 않아도 사용자가 원하는 정보를 실시간으로 제공하는 개인화 서비스이다. SMS (short message service)와 MMS (multimedia message service) 서비스는 발송할 때마다 비용을 지불해야 하고, 모바일 디바이스에 설치한 특정 어플리케이션을 대상으로 메시지를 발송할 수 없다. 그러나 애플의 APNs (Apple push notification service), 구글의 GCM (Google cloud message) 등은 전용 푸시 플랫폼을 이용하여, 사용자 모바일 디바이스에 특정 어플리케이션을 타겟팅하여 메시지를 전송할 수 있어 SMS와 MMS의 문제를 해결할 수 있다[2].

본 논문은 보안이 요구되는 장소에 실시간으로 침입 여부를 감지하는 지능형 영상보안 시스템을 제안하였다. 제안 시스템은 CCTV나 웹캠(web cam)과 같은 영상장치가 부착된 노트북과 침입여부를 통지하기 위한 GCM 푸시서버와 SMTP (simple mail transfer protocol) 메일서버 그리고 푸시 메시지를 전송 받기위해 어플리케이션이 저장되어 실행되고 있는 스마트 폰으로 구성하였다. 제안 시스템은 침입여부를 인식하기 위해 누적영상 기반의 차 영상과 동적 배경 갱신 알고리즘을 사용하였으며, 영상처리를 위해 인텔의 OpenCV를 이용하였다.

본 논문은 2장에서 관련연구로서 본 논문에서 사용한 움직임 검출 알고리즘과 모바일 푸시서버에 대해서 서술하였으며, 3장에서 영상보안 시스템을 제안하였다. 또한, 4장에서 영상보안 시스템을 구현하였으며, 5장에서 결론을 맺는다.

## Ⅱ. 객체 영역 검출

차 영상(difference frame)은 동영상의 프레임 간 픽셀 값의 차이를 비교하여, 변화를 감지하는 기법이다. 차 영상은 움직임을 검출할 수 있으나, 미세한 조명의 변화에 민감하고 , 객체의 위치를 판단할 수 없다[3],[4].

**그림 1.** 누적 영상을 이용한 객체 검출
**Fig. 1.** Object detection using integral image.

배경 차분(background subtraction)은 배경이미지를 저장해 놓고, 객체의 움직임이 있는 경우, 배경 프레임과 객체의 움직임이 있는 프레임의 차를 통하여 객체 영역을 검출하는 방법이다[5],[6].

$$\begin{aligned} &\text{if} \quad b_n = x : |I_n(x) - B_n(x)| > T_n(x), x \in R \\ &then \quad x\text{는 객체 이미지 픽셀} \\ &else \quad x\text{는 배경 이미지 픽셀} \end{aligned} \tag{1}$$

여기서 $I_n(x)$는 현재 프레임 픽셀, $B_n(x)$는 배경 프레임 픽셀, $T_n(x)$는 임계값이다. 즉, 배경 프레임 픽셀에서 현재 프레임의 픽셀 값을 뺀 것이 임계치보다 크면 움직인 객체의 픽셀이다. 배경차분의 정확성은 현재 배경을 얼마나 정확하게 표현하는가에 달려 있다. 영상은 조도와 휘도의 변화량에 민감하기 때문에, 정확한 배경차분을 위해서는 조도와 휘도의 변화량에 적응할 수 있는 배경모델 필요하다.

누적 영상(integral image)은 보다 효율적인 배경모델을 위하여, 여러 개의 배경프레임 픽셀 값에 대한 평균값을 이용하는 것이다[7]. 누적영상의 평균값은 배경으로 구분하며, 픽셀 값 0 (검은색)으로 마킹한다. 이때, 어떠한 객체가 움직임이 발생하면, 배경 평균값과 큰 차이가 발생하며, 픽셀값 255(흰색)으로 마킹한다. 결국 흰색으로 마킹된 부분이 객체의 위치가 된다. 그림 1에 누적 영상을 이용한 객체 검출에 대해서 나타냈다.

## Ⅲ. 푸시서비스

풀기법은 사용자가 원하는 정보를 서버에게 요청하는 기법으로, 정보의 사용과 목적지에 대한 최종결정을 사용자가 지정한다. 그러나 푸시기법은 사용자가 요청하지 않아도 사용자에게 자동으로 특별한 정보를 제공한다. 즉, 풀 기법은 사용자가 정보 취득 및 접촉을 통제할 수 있으나, 푸시 기법은 정보를 전달하는 쪽에서 정보의 흐름을 통제할 수 있다.특히, 푸시 기법은 사용자가 서버에 등록되어, 등록된 사용자 정보에 의해 정보를 전송할 수 있기 때문에, 정보의 맞춤화 및 개인화가 가능하다는 장점이 있다[8].

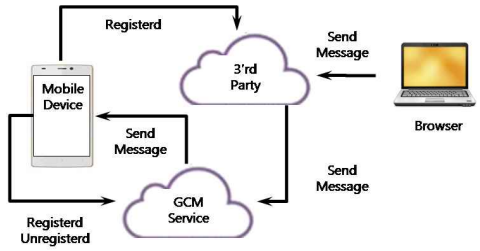


**그림 2.** GCM 푸시서비스의 구조
**Fig. 2.** Structure of GCM push service.

대표적인 푸시서비스인. SMS와 MMS은 발송할 때마다 비용을 지불해야 하고, 모바일 디바이스에 설치한 특정 어플리케이션을 대상으로 메시지를 발송할 수 없다. 그러나 애플의 APNs, 구글의 GCM 등 푸시 플랫폼을 이용하여 이와 같은 문제를 해결할 수 있다.

최근 XML 기반 메시지 지향 미들웨어용 통신 프로토콜인 XMPP (extensible messaging and presence protocol)를 이용하여, 자신만의 푸시 서비스를 제공할 수 있다. XMPP를 이용한 대중적인 서버 종류는 djabberd, ejabberd, jabberd, jabberd2, Openfire, Prosody, Tigase 등이 있다[8].

GCM 푸시서비스는 모바일 디바이스, 3'rd party 어플리케이션 서버, GCM 서버 등으로 구성된다. 모바일 디바이스는 GCM을 사용하는 안드로이드 어플리케이션을 실행하는 장치로서, Google play store가 설치되고, 2.2 이상의 안드로이드 디바이스여야 한다. 3'rd party 서버는 개발자가 GCM 기능을 구현한 어플리케이션 서버이다. 3rd party 어플리케이션 서버는 GCM 서버를 경유해 모바일 디바이스의 어플리케이션에 메시지를 전송한다. 또한, GCM 서버는 3'rd party 서버에서 메시지를 수신하여, 모바일 디바이스의 어플리케이션에 메시지 전송하는 서버이다. 그림 2에 안드로이드 기반 GCM 푸시 서비스의 구조에 대해서 나타냈다.

GCM 라이프 사이클은 GCM 활성화, 메시지 전송, 메시지 수신 등이 있다[9]. GCM 활성화는 모바일 디바이스에서 실행되는 어플이 푸시 메시지를 수신하기 위해서 등록하는 과정에서 발생된다. GCM 활성화 과정은 다음과 같다.

- 어플리케이션이 GCM 서버에 registration intent 발송.
- registration intent는 API 콘솔로 부터 획득한 프로젝트 ID인 Sender ID와 안드로이드 어플리케이션을 타켓팅 할 application ID를 포함한다.
- 등록 프로세스는 라이프 사이클 메소드가 없기 때문에 미등록 된 경우만 등록한다.
- 등록이 성공하면 GCM서버에서 리턴 값으로 안드로이드 어플에 대한 registration ID를 부여 받는다.
- registration ID는 어플리케이션이 갖고 있으며, 3rd party 서버로 전송하고, 데이터베이스에 저장되어, 어플리케이션이 메시지를 받기 위해 등록된 각 모바일 디바이스를 식별하는 데 사용한다.

메시지 전송을 위해서는 GCM 활성화 과정에서 생성된 registration ID와 API key가 필요하다. 3'rd party 서버가 메시지를 보낼 때 발생하는 이벤트 순서는 다음과 같다.

- 3rd party 서버가 GCM 서버에 메시지를 보낸다.
- 모바일 디바이스가 오프라인 상태인 경우에 대비해 구글이 메시지를 저장하고 대기열에도 저장한다.
- 모바일 디바이스가 온라인 상태가 되면, 구글이 해당 모바일 디바이스에 메시지를 보낸다.
- 모바일 디바이스는 적절한 권한을 가진 안드로이드 어플리케이션의 intent broadcast를 사용해서 메시지를 브로드캐스트함으로써 대상 어플리케이션만 메시지를 받는다.

모바일 디바이스에 설치된 어플이 메시지를 수신하는 이벤트의 순서는 다음과 같다.

- 모바일 디바이스는 전송된 메시지를 수신 메시지의 페이로드에서 원시 키-밸류 쌍을 추출한다.
- 키-밸류 쌍을 com.google.android.c2dm.intent.RECEIVE Intent에서 엑스트라의 세트로 대상 어플리케이션에 전달한다.
- 어플리케이션은 com.google.android.c2dm.intent.RECEIVE Intent에서 키의 원시 데이터를 추출하고 처리한다.

## Ⅳ. 제안 영상 보안시스템

제안 영상 보안시스템은 CCTV나 웹캠으로부터 영상을 입력받아, 노트북으로 영상처리와 침입 인지를 하였으며, 모바일 디바이스로 침입 여부를 실시간으로 통지하도록 하였다. 침입 통지는 사용자 디바이스 내 어플리케이션 단위로 타겟팅을 하여 메시지를 전송할 수 있는 SMTP 메일서버와 GCM 푸시서버를 이용하였다. 그림 3에 본 논문에서 제안한 영상 보안시스템의 구성에 대해서 나타냈다.

본 논문은 배경 프레임 뿐 아니라 조명에 민감한 영상에서 효과적으로 객체 검출을 위해 휘도(luminance) 진폭 값에 대한 누적 영상을 구하였다. 휘도 진폭 값의 평균을 구하는 공식은 다음과 같다[10].

```
for(i=1 : i <=20 ; i++){
  currentImg = current Img input
  Temp = currentImg - avgImg;
  Temp = √(Temp²)
  lumImg = lumImg +Temp;
}
lumImg = lumImg × 1/20
```


**그림 3.** 영상 보안 시스템 구조
**Fig. 3.** Image security system structure.

또한, 환경변화에 유연하게 대처할 수 있도록 동적 배경 갱신을 수행하였다. 동적 배경 갱신은 조명 변화가 생길 경우, 이미 구해진 배경을 새롭게 갱신하는 것이다. 배경차분 구하기 위하여 다음과 같은 연산을 수행하였다[10].

$$acc(x,y) \leftarrow (1-\alpha) \times acc(x,y) + \alpha \times img(x,y) \qquad (2)$$

$\alpha$ 값은 갱신 속도로서 1에 가까울수록 갱신 속도가 빨라진다. 동적 배경 갱신은 배경영역과 객체영역에 별도로 수행된다. 본 논문에서는 배경영역에 0.2, 객체 영역에 0.005로 설정하였다. 이는 배경영역이 객체영역보다 현재영상에 대한 가중치가 상대적으로 높은 것을 의미하고 그만큼 갱신은 빠르게 일어나게 된다. 배경영역에 대한 갱신을 빠르게 함으로써 조명변화와 같은 환경변화에 민감도를 낮출 수 있는 장점이 있다.

이와 같이 누적영상 기반의 차 영상과 동적 배경 갱신 알고리즘을 사용하여, 객체가 검출되면, 침입자가 발생한 것으로 간주하고, 푸시서버와 메일 서버를 이용하여, 모바일 디바이스에 침입자 여부 및 침입자 사진이 전송되도록 하였다.

침입자 감지 시 WinInet을 이용한 MFC 어플리케이션에서 3rd-party 서버로 침입 메시지를 POST 방식으로 전송하고, 3rd-party 서버에서는 GCM 서버로 결과 값을 전송한다. 최종적으로 GCM 서버는 등록된 단말기에 결과 값을 전송하여 사용자에게 침입여부를 통지하게 된다. MFC POST 전송 소스 코드는 다음과 같다.

RequestPost(_T("http://192.168.0.6:8080/TestServer/certificate"), strSendMsg, strOutMsg);

RequestPost 메서드는 우선 AfxParseURL 메서드를 이용하여 서버 IP, 포트번호, 목적페이지 주소 등을 파싱한다. 또한, 파싱 결과 값을 이용하여, 세션을 확보한 후 OpenRequest 메서드를 사용하여 서버에 접속을 요청한다. 이 때 첫 번째 인자로 사용하고자 하는 메서드를 지정한다. 본 시스템은 3rd-party server 단에 있는 /TestServer/certificate 객체로 메시지를 전달함으로, HTTP_VERB_POST를 첫 번째 인자로, 두 번째 인자로는 전달하고자 하는 메시지를 주었다. 최종 요청은 SendRequest 메서드를 통해 메시지와 함께 내용이 전달된다. 그림 3에 제안 침입자 검출 시스템의 흐름도를 나타냈다.

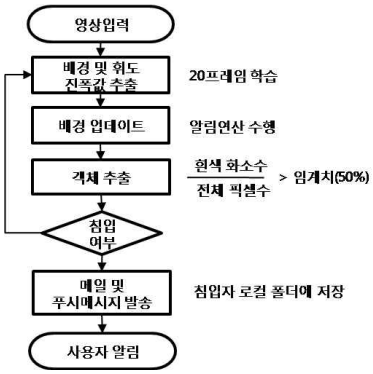


**그림 4.** 시스템의 흐름도
**Fig. 4.** Flowchart of system.

## Ⅳ. 영상 보안 시스템 구현

본 논문의 영상 보안 시스템은 마이크로소프트사의 비쥬얼 스튜디오 2010을 사용하였으며, 영상처리를 위해 인텔의 OpenCV를 이용하였다. 영상입력은 노트북의 웹캠을 이용하였으며, 영상처리 알고리즘은 노트북에서 실행하였다. 또한, GCM 푸시서버는 개인용 컴퓨터를 이용하였으며, 사용자의 모바일 디바이스를 이용하여 푸시 메시지를 전송 받는다. 표 1에 본 논문에서 사용된 영상 보안 시스템 구현환경에 대해서 나타냈다. 또한, 그림 5에 영상처리 시스템의 초기화면에 대해서 나타냈다.

**표 1.** 영상 보안 시스템 구현 환경
**Table 1.** Image security system implementation environment.

| | |
|---|---|
| 영상처리 시스템 | 시스템 플랫폼 : 윈도우 |
| | 영상 캡처 및 영상 처리 |
| | 프로그래밍 언어 : MFC, OpenCV 2.4.2 |
| | 개발환경 : 비쥬얼 스튜디오 2010 |
| 서버 | 시스템 플랫폼 : 리눅스 |
| | 3rd party 어플리케이션 서버 |
| | 데이터베이스 : MySQL |
| | 프로그래밍 언어 : 자바, JSP |
| | 개발환경 : 이클립스 |
| | 라이브러리 : GCM |
| 클라이언트 | 디바이스 단말기 : 삼성 갤럭시 S3 |
| | 모바일 플랫폼 : 안드로이드 SDK |
| | 프로그래밍 언어 : 자바 |
| | 개발환경 : 이클립스 |
| | 라이브러리 : GCM |


**그림 5.** 초기화면
**Fig. 5.** Initial screen.

Start Detection 버튼을 누르면 사용자가 검출 영역에서 벗어나기 위해 일정시간이 지연된 후에 침입 감지를 시작하게 된다. 타이머는 1초에 1번 호출되도록 설정하였다. 그리고 타이머에 cvAcc() 메서드가 포함되어, 20프레임에서 배경영상을 구하는 알고리즘을 실행하게 하였다. Hide Program 버튼은 침입 감지 프로그램의 실행을 보이지 않게 한다. 그림 6에 침입자 감지 및 캡처된 영상을 저장된 결과를 나타냈다. 침입자 영상은 침입자 검출이 되는 즉시 하드디스크에 저장되며, 사용자가 설정한 e-mail로 전송된다. 저장 경로는 D:\\Picture\IDS_SAVE 폴더로 지정했으며 만약, 폴더가 없을 시 자동 생성된다. 그림 7에 사용자에게 침입사실을 e-mail로 전송한 결과를 나타냈다.

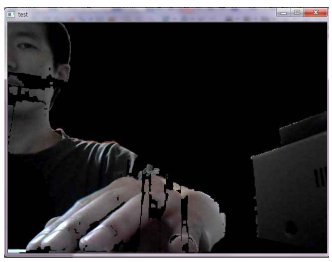

**그림 6.** 침입 감지 및 캡처 영상 저장
**Fig. 6.** Intrusion detection and capture image save.

**그림 7.** 침입 알림
**Fig. 7.** Intrusion notice.


**그림 8.** 푸시메시지 화면
**Fig. 8.** Notification screen.

그림 8은 침입자가 감지되었을 경우 GCM 푸시서버에서 모바일 디바이스에 전송된 푸시메시지 결과이다.

이와 같이 제안 영상 보안 시스템은 노트북으로 영상처리와 침입 인지를 하였으며, 모바일 디바이스로 침입 여부를 GCM 푸시서버와 SMTP 메일서버를 이용하여 실시간으로 통지하도록 하였다. 메일 서버는 사용자가 확인해야 하기 때문에 실시간으로 침입자를 확인할 수 없는 경우가 있다. 그러나 푸시 서비스는 사용자에게 침입 사실을 실시간으로 전송할 수 있다. 따라서 사용자는 침입사실을 푸시서비스를 통해 모바일 디바이스에서 확인한 후, 메일서버를 통해서 침입자 사진을 확인할 수 있다.

## Ⅴ. 결 론

본 논문은 보안이 요구되는 장소에서 사용자의 스마트 디바이스에 실시간으로 침입 여부를 감지하는 경량의 영상보안 시스템을 제안하였다. 제안 시스템은 스마트 디바이스의 보안에 대한 다양한 기능으로 확장할 수 있다. 즉, 스마트 디바이스에서 모바일 디바이스에 침입 여부에 대해 단방향 전송에서 양방향 전송이 가능한 시스템으로 확장 수 있다. 예를 들어, 침입자가 감지된 경우, 모바일 디바이스에서 침입자에게 노트북을 통해 음성 전송, 노트북 경고음 발생 등의 확장뿐만 아니라 노트북에서 스마트폰을 제어하는 기능까지 확장 가능하다. 즉, 모바일 디바이스 분실 시 노트북에서, 모바일 디바이스의 카메라를 구동시키거나 위치추적 및 경고음을 울리는 등의 다양한 기능을 추가할 수 있다. 또한, 제안 시스템은 각종 시설물 보안과 화재 검출 등 다양한 보안에 응용할 수 있다.

## 참고문헌

[1] J. H. Yu, G. Y. Moon and H. S. Cho, "Intelligent image security technology status and trend," *Telecommunication Trend Analysis*, Vol. 23, No. 4 pp. 80-87, Aug. 2008.

[2] http://ko.wikipedia.org/wiki/%ED%91%B8%EC%8B%9C_%EA%B8%B0%EB%B2%95.

[3] S. C. Shin and S. H. Han, "An ambient light controls system using the image difference between video frames," *The Korea Society for Simulation*, Vol. 19, No. 3, pp. 7-16, Sep. 2010.

[4] B. H. Lee, D. J. Kim, I. Choi, and G. J. Jeon, "Tracking a moving object using an active contour model based on a frame difference map," *The Institute of Electronics and Information Engineers,* Vol. 41, No.5, pp.153-163, Sep. 2004.

[5] W. Y. An, J. H. Lee , S. W. Lee , and J. K. Paik , "Robust moving object detection using motion-based background subtraction," in *Proceedings of The Institute of Electronics and Information Engineers*, Jeju: Korea, pp.1017-1018, Jun. 2012.

[6] A. M. Mclvor, "Background subtraction techniques," in *Proceedings of Image and Vision Computing New Zealand 2000 IVCNZ'00*, Auckland: New Zealand, Vol 1, No.3, pp. 155-163. 2000.

[7] H. S. Kim, T. S. Ko, K. M. Lim and J. S. Lee, "Trajectory indication of moving object using cumulated edge image," in *Proceedings of The Korean Institute of Communications and Information Sciences*, Jeju: Korea, pp. 172-175, Jul. 2008.

[8] K. Smith, P. S. Andre and R. Troncon, *XMPP : The Definitive Guide Building Real-Time Applications with Jabber Technologies,* California, CA: O'Reilly Media, pp. 253-254, 2009.

[9] http://developer.android.com/google/gcm/gcm.html

[10] Y. C. Oh and C. B. Kim, "A study on real-time intrusion detection system using adaptive background model," in *Proceedings of The Korean Institute Of Information Technology*, Soonchunhyang University: Korea, pp. 522-525, Mar. 2013.

**박승환**(Seung-Hwan Park)

1984년 2월 : 인하대학교 전자공학과 (공학사)
1990년 2월 : 인하대학교 전자공학과 (공학석사)
1995년 8월 :인하대학교 전자공학과 (공학박사)
1995년 ~ 현재 : 을지대학교 의료공학과 교수
※관심분야 : 임베디드MCU응용, 신호처리, 의료기기 시스템.

**오유철**(U-Chul Oh)

2013년 2월 :가천대학교 정보공학부 (공학사)
2013년 2월 ~ 현재 : 사이냅 소프트 개발부
※관심분야 : 정보보안, 영상처리, 분산처리시스템

**김 창 복** (Chang-Bok Kim)

1986년 2월 : 단국대학교 전자공학과 (공학사)
1989년 2월 : 단국대학교 전자공학과 (공학석사)
2008년 2월 : 인천대학교 컴퓨터 공학과 (공학박사)
1994년 ~ 현재 : 가천대학교 IT대학 에너지 IT학과 교수
※관심분야 : 인터넷보안, 클라우드 컴퓨팅, 분산처리시스템