AES 암호 알고리듬 기반 디지털 영상 보안 시스템의 설계

강민석[1], 배지수[2], 장태민[3], 강민섭[4]

Design of Digital Image Security System Using AES Algorithm

Min-seok Kang[1], Ji-su Bae[2], Tae-min Jang[3],Min-sup Kang[4]

요 약

본 논문에서는 AES 암호 알고리듬을 이용하여 CCTV에서 디지털 영상정보를 보호하기 위한 보안 시스템의 설계 및 구현에 관하여 기술한다. 구현된 시스템은 CCTV 와 서버 연결 구간의 영상정보에 대한 암호화가 가능하므로 종래의 CCTV 시스템에서 문제가 되는 개인의 사생활 침해는 물론 영상정보의 해킹이나 누설을 방지할 수 있다. 실험 결과를 통해서 실제 영상 데이터의 암/복호화 가 완벽하게 이루어지고, 암호화된 데이터는 Key가 없을 경우 전혀 해독할 수 없음을 확인 하였다. View Server에서의 수행될 복호화 모듈은 C++ 언어를 사용하여 구현하였고, FPGA 보드에서의 암호화 모듈은 Xilinx ISE 9.1i 툴을 사용하여 Verilog HDL로 설계하였다.

핵심어 : CCTV, 보안 시스템, 디지털 영상, AES 암호화, Verilog HDL

Abstract

In this paper, the design of digital image security system is described for CCTV system based on AES cipher algorithm. The implemented system can protect some problems such as the hacking of image data and revealing of images relating to individuals compared to existing CCTV systems. From the experimental results, we showed that the proposed system based on AES cipher algorithm is correctly operated in conventional CCTV environment. In the proposed system, a decryption module for View Server has been coded using C++ language. Also, an encryption module has been described in Verilog HDL, and it has been successfully implemented with Xilinx FPGA (Spartan XC2V200) using the ISE 9.1i tool.

Keywords : CCTV, Security system, Digital Image, AES cipher, Verilog HDL

접수일(2011년02월20일), 심사의뢰일(2011년02월21일), 심사완료일(1차:2011년03월02일, 2차:2011년03월18일)

게재일(2011년04월30일)

[1]430-714 경기도 안양시 만안구 안양5동 컴퓨터공학과 석사과정.
email: volof7lv@anyang.ac.kr

[2]430-714 경기도 안양시 만안구 안양5동 컴퓨터공학과 학부과정.
email: qowltn86@dreamwiz.com

[3]430-714 경기도 안양시 만안구 안양5동 컴퓨터공학과 박사과정.
email: tmjang@paran.com

[4](교신저자) 430-714 경기도 안양시 만안구 안양5동 컴퓨터공학과 교수.
email: mskang@anyang.ac.kr

1. 서론

CCTV(Closed Circuit Television: 폐쇄회로 TV)는 영상정보를 특정의 목적으로 특정 사용자에게 전달해 주는 시스템으로, 가정, 학교, 회사, 금융기관, 그리고 공공기관 등 산업전반으로 사용범위가 넓어지고 있다[1]. 특히 각종 범죄가 증가함에 따라 CCTV는 기하급수적으로 설치가 증가하게 되었으나, 방범 등의 목적으로 설치, 관리하는 CCTV의 개인 영상정보의 유출 위험에 무방비 상태인 것으로 언론을 통해 문제점이 심각하게 부각되고 있다[1-2].

방범용 CCTV는 인력 투입에 어려움을 쉽게 해결 할 수 있는 범죄예방수단으로 인식되고, 범죄 발생 시 CCTV에 녹화되어있는 영상은 법적인 증거물로 각종 범죄의 해결에 큰 도움이 되며, 그 밖의 범죄예방, 증거확보, 시설안전, 화재예방, 교통정보제공, 법규위반단속, 공항/항만/지하철 관리 등을 위하여 지속적으로 확대 설치되고 있다[3].

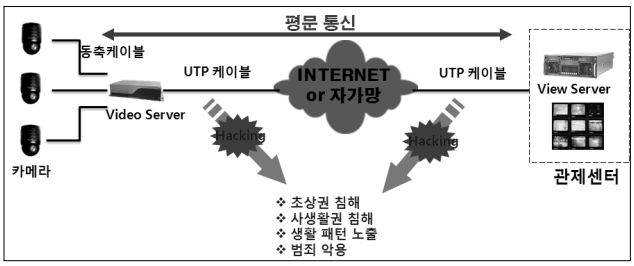
공공기관의 개인정보보호에 관한 법률을 보면 정보통신망에 의하여 송·수신하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안정성 확보에 필요한 조치를 강구해야한다. 그러나 현재 CCTV 보안은 너무 허술하여 해킹을 통하여 사생활 침해를 넘어 사실관계를 바꾸거나 결정적인 증거가 고의적으로 조작되거나 파기 될 위험성이 표출 되고 있다[3].

본 논문에서는 AES 암호 알고리듬을 이용하여 CCTV에서 디지털 영상정보를 보호하기 위한 보안 시스템의 설계 및 구현에 관하여 기술한다. 설계된 AES 암호 모듈은 개선된 S-box를 사용함으로써 하드웨어 오버헤드를 대폭 감소시켰다. View Server에서의 암호화 모듈은 C++ 언어를 사용하여 구현하였고, FPGA 암호화 모듈은 Xilinx ISE 9.1i 툴을 사용하여 Verilog HDL로 설계하였다. 구현된 시스템은 CCTV (비디오 서버)와 서버 연결 구간의 영상정보를 암호화하고, 각 CCTV와 모니터 구간 사이에 각기 다른 제품들에 독립적으로 동작 가능한 모듈을 장착함으로써 전송중인 영상정보에 대한 보안이 가능하다.

2. 기존의 CCTV 시스템

기존의 CCTV 방범 시스템은 [그림 1]과 같이 현장단의 카메라로부터 Video Server로 압축되지 않은 영상정보와 음성정보를 전송하면 Video Server는 영상 압축 알고리듬을 통하여 영상정보를 압축하여 전송한다[4].

그리고 구축되어 있는 네트워크(TCP/IP)를 통하여 관제센터에 있는 View Server로 정보가 전송이 된다. View Server는 현장단으로부터 받은 영상정보를 모니터 디스플레이를 통해 감시를 하거나 DB Server에 저장을 하게 된다. 기존의 방법은 네트워크를 통하여 현장단의 Video server에서 관제센터의 View Server로 전송되는데, 카메라로부터 전달되는 정보의 보호에 매우 취약하기 때문에 구간 케이블(UTP)에 도청 및 해킹의 위험성이 매우 높다.

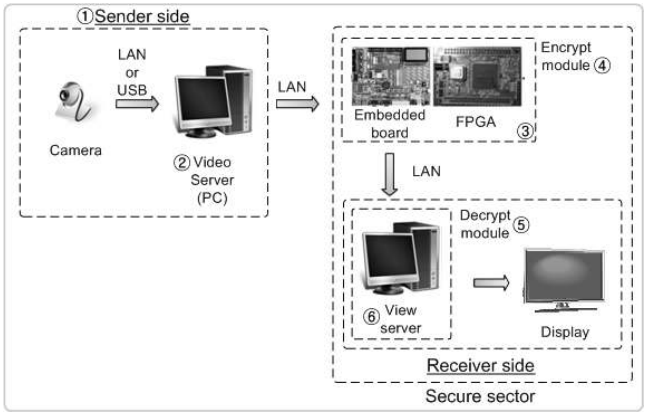


[그림 1] 기존의 CCTV시스템

[Fig. 1] Existing CCTV system

3. 제안하는 디지털 영상보안 시스템

제안하는 디지털 영상 보안 시스템은 AES 암호화 기술을 이용하여 보안이 취약한 현장단과 관제센터 구간의 네트워크상에 보안 채널을 구축하여 서로 주고받는 데이터를 암호화함으로써 보안 문제를 해결한다. [그림 2]는 제안하는 디지털 영상보안 시스템의 전체 구성도를 나타낸다. 본 논문에서 암호화는 FPGA내에서 수행하고 복호화는 View Server에서 수행한다.



[그림 2] 제안된 디지털 영상보안 시스템 구성도

[Fig. 2] Configuration of digital image security system

[그림 2]에서 CCTV 카메라와 암호화 모듈(Encrypt module) 간의 연결은 일반적으로 Video Server를 연결해서 사용한다. 그러나 비디오 서버를 사용하기 위해서는 비디오 서버의 소스와 패킷의 스펙을 확보할 수 있어야 하는 문제점이 있다. 이에 기존 Video Server의 CCTV로부터 촬영되는 영상 데이터를 코덱을 통한 영상 압축 기법을 사용하여 압축하는 기능, TCP/IP통신 규격에 의거한 데이터 통신 부분, 각 부분을 제어 할 수 있는 어플리케이션 부분 모두를 Windows 기반의 PC를 Video Server로 대체함으로써 문제를 해결하였다. 그리고 AES 복호화 부분은 하드웨어가 아닌 고성능의 View Server에서 소프트웨어(C++ 언어 사용)로 구현하여 복호화 문제를 해결하였다.

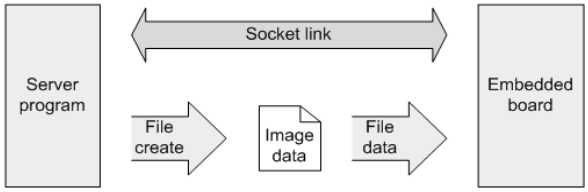
전체 데이터의 흐름을 간단히 언급하면, Sender side에서는 CCTV를 통한 영상 촬영이 이루어지며 이 데이터는 USB 또는 LAN을 통하여 Video Server(PC)로 전송한다. Sender Side의 Video Server는 Receiver Side의 View Server와의 통신 연결을 통해 데이터를 전송하게 되며, 중간에 Embedded Board와 FPGA Board를 통하여 Encrypt 과정을 거치게 된다. View Server에서는 해당 데이터를 받아 Decrypt 하여 저장하고 모니터링을 할 수 있도록 Display한다.

4. 모듈별 시스템 구성

[그림 2]에 나타난 시스템의 구성도를 모듈별로 분할하여 살펴보면 다음과 같다.

4.1 송신측 (Sender side)

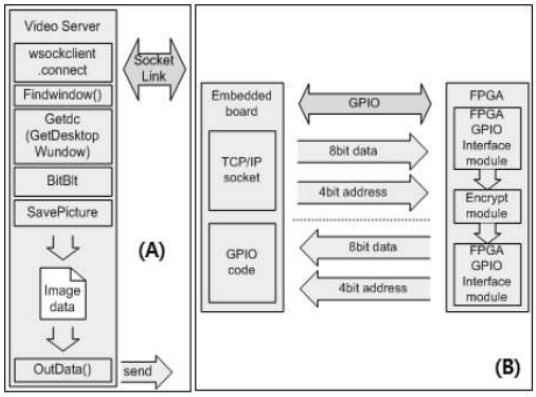
[그림 3]은 비디오 Server와 Embedded Board 사이에 Socket 통신을 이용하여 Camera의 이미지 데이터를 전송하는 비디오 서버단의 구성도를 나타낸다.



[그림 3] 비디오 서버단의 데이터 흐름도

[Fig. 3] Data flow of Video Server module

4.2 Video Server (영상처리)



[그림 4] 비디오 서버(A)와 임베디드 보드(B) 간의 통신

[Fig. 4] Communication between Video Server(A) and Embedded Board(B)

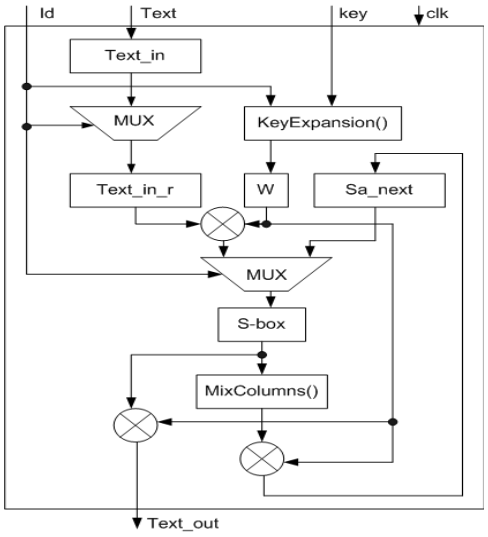
[그림 4]는 Video Server내의 영상처리 및 TCP/IP 어플리케이션 흐름도를 순서도화 한 것이다. wsockclient.connet()는 [그림 7]의 View server의 wsockserver.listen()과 소켓 통신이 가능하도록 연결해주고, 캡처할 윈도우를 찾는 Findwindow() 함수를 통해 CCTV(Webcam)을 인식하고 Getdc(GetDesktopWindow)를 통하여 DC를 읽고, BitBlt을 이용하여 화면 RGB값을 얻은 후 영상파일로 저장하여 OutData()를 통해 소켓을 정보를 내보내게 된다.

4.3 Embedded Board와 FPGA Board

[그림 4]는 Embedded Board와 암호화 처리를 위한 FPGA내의 데이터 흐름도를 나타낸다. Server로부터 받은 TCP/IP 프로토콜 기반의 패킷을 Embedded Board에서 FPGA로 GPIO 제어를 통하여 데이터와 주소 정보를 전송하고, FPGA에서는 해당 정보를 AES 128bit 기반의 암호화를 통하여 암호화한 후 다시 GPIO 신호를 이용하여 Embedded Board로 전송하게 된다. Embedded Board는 암호화되어 회신된 정보를 LAN을 통하여 Decrypt Module(View Server)로 전송한다.

4.4 Encrypt Module(FPGA 내의 회로 구성)

CCTV 영상 보안 시스템을 위한 AES 암호 알고리듬은 영상 정보에 대한 암·복호화를 수행하여야 한다. 따라서 연산의 효율성과 면적 감소를 통하여 수행 속도 및 크기에 대해서 고려한 구현이 필요로 하게 된다[5-8].

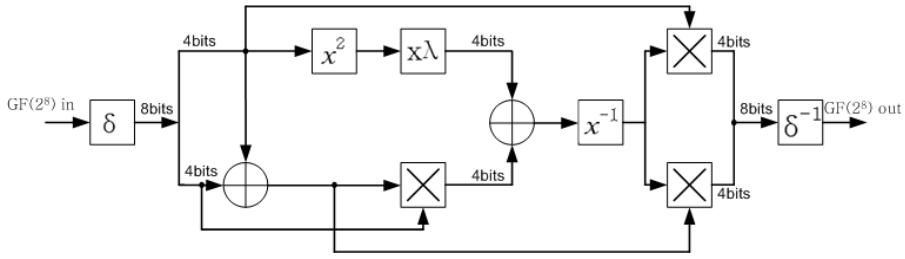


[그림 5] 제안하는 AES 암호화 모듈의 전체 구성도

[Fig. 5] Proposed AES encryption module

암·복호화 과정은 마지막 10라운드를 제외하고 각 라운드마다 4개의 연산 블록을 수행하며, 암호화 경우 SubBytes(), ShiftRows(), MixColumns(), AddroundKey()과정으로 진행 된다. 본 논문에서는 AES 암호 암고리듬에 있어 큰 면적을 차지하는 S-box를 테이블 형태인 LUT[6]가 아닌 유한체 연산으로 구현 하였고 복잡한 유한 체 행렬의 연산이 필요한 MixColumns()는 xtime()이란 함수부를 도입하여 설계하였다. [그림 5]는 개선된 S-box를 사용하여 제안하는 AES 암호화 모듈의 전체 구성도를 나타낸다.

[그림 5]의 ld는 입력 신호 값을 나타내며 Text와 Key는 각각 128비트 입력 데이터와 키 값을 나타낸다. Text_in과 Text_in_r은 초기 입력 값을 임시 저장하는 레지스터 버퍼이며, Sa_next는 내부 연산 128비트 데이터 값을 임시 저장하는 레지스터 버퍼 역할을 한다. KeyExpansion()부는 AES 암호 키를 입력 받아 128비트 라운드 키 W를 생성하는 역할을 하며 S-box는 개선된 S-box를 사용하여 치환 연산을 수행한다. MixColumns()부는 xtime()함수를 사용하여 연산을 수행한다. [그림 6]은 효율적인 저 면적의 S-box 구현을 위해 제안한 블록도를 나타낸다.



[그림 6] 제안한 S-box의 블록도

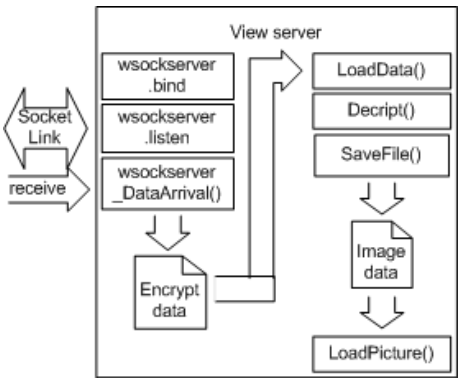
[Fig. 6] Block diagram of proposed S-box

4.5 Decrypt Module(Server 내의 Application)

Decrypt Module에서 사용한 암호 알고리듬은 AES 이다. 복호화는 InvShiftRows(), InvSubBytes(), AddRoundKey(), InvMixColumns() 순으로 복호화 데이터를 연산 한다[8]. 본 논문에서는 암호화는 FPGA내에서 수행하고 복호화는 View Server에서 수행한다.

4.6 View Side(Receiver's Hardware & Software)

TCP/IP 소켓통신이 연결되면 View Server는 Sender side의 Video Server로부터 영상 데이터를 전송받고 해당 영상 데이터를 실시간으로 Display하여 [그림 2]의 ⑤와 같은 하드웨어 내에 Application으로 동작한다.



[그림 7] View Server의 어플리케이션 흐름도
[Fig. 7] Application flow of View Server

[그림 4]의 wsockclient.connet()과 연결된 [그림 7]의 wsockserver.listen()이 소켓통신을 제어하고 wsockServer_DataArrival()이 해당 영상 데이터를 수신하게 된다. 수신된 데이터는 암호화된 데이터로서 LoadData()로 읽어들여 Decrypt()하여 원본 데이터로 복구하고 Image data로 View Server에 저장하게 되고, 해당 데이터는 LoadPicture()에 의해 디스플레이하여 볼 수 있도록 한다.

5. 디지털 영상보안 시스템 구현 및 검증

Video Server의 구현은 PC를 이용하였으며, View Server에서의 암호화 모듈은 Win XP 운영체제 상에서 C++ 언어를 사용하여 구현하였다. Embedded 시스템은 Linux(kernel 2.6.1) 기반의 Eddy DK Board를 사용하였고 C언어로 프로그래밍 되어있다. FPGA 암호화 모듈은 Verilog로 기술하였고, 논리 합성 및 검증은 KAIST의 IDEC 에서 지원 받은 툴인 Xilinx ISE 9.1i 와 Modelsim을 사용하였다. 여기에서 사용된 타겟 디바이스는 .Xilinx Spartan xc2v200을 사용하였다. FPGA 모듈의 H/W 동작 검증을 위한 시뮬레이션은 을 사용하였다. 구현된 전체 시스템은 [그림 8]과 같으며, 동작 순서는 다음과 같다.

[그림 8] 구현된 시스템의 동작 테스트
[Fig. 8] Verification of Implemented system

Webcam(4)를 통해 영상 데이터가 들어오면, Video Server(2)는 들어온 데이터를 Embedded 시스템으로 전송하게 된다. 다음에 Embedded 시스템과 FPGA Encrypt모듈(3)에서는 전송되어오는 영상 데이터를 Embedded 시스템이 실시간으로 받고 GPIO를 통하여 FPGA Encrypt모듈로 전송한다. FPGA Encrypt 모듈은 데이터를 128bit key를 이용, AES 알고리듬으로 암호화하여 다시 GPIO를 통해 Embedded 시스템으로 전송하게 된다. Embedded 시스템은 TCP/IP를 통해 Receiver side의 View Server(1)로 전송한다. View Server는 해당 데이터를 실시간으로 AES 알고리듬으로 128bit key를 이용, 복호화 하여 디스플레이를 해주고 있다.

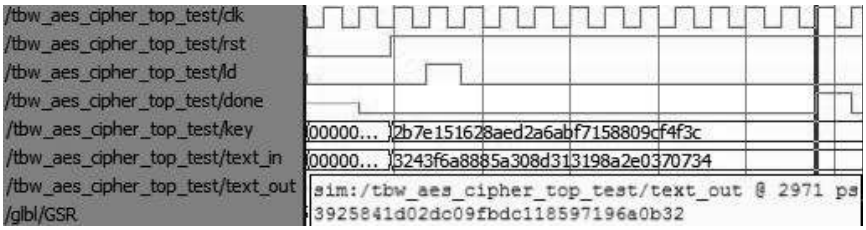
5.1 FPGA 보드내에서의 암/ 복호화 시뮬레이션

구현한 AES 암호 알고리듬의 최대 동작 속도는 64.763MHz를 가지며, 958개의 슬라이스를 사용하였다. [표 1]은 기존의 LUT 를 이용한 S-box의 구현 방법[5, 6]과 제안한 방법에 대한 성능 비교를 나타낸다.

[표 1] S-box 에 대한 성능 비교
[Table 1] Comparison of three methods for S-box

	Ref. [5]	Ref. [6]	Proposed S-box
# ROMS	256x8-bit	-	16x4-bit
# Slices	72	-	33
# Gates	1,200	4,248(s-box 8개)	351
# Delay	22.716ns	-	20.513ns

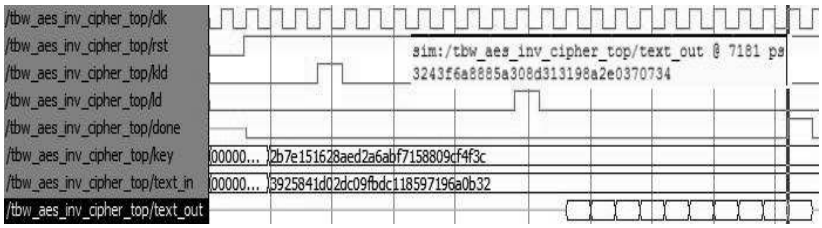
[표 1]에서 Ref. [5]은 64비트 데이터 패스로 8개의 S-box를 사용 한 것이며, Ref. [6]은 LUT를 사용한 방법이다. 제안한 방법은 단지 1개의 S-box를 사용하여 구현한 결과를 나타낸다. [표 1]에서 알 수 있듯이 게이트 수의 비교에 있어서 제안한 방법이 대폭 감소됨을 알 수 있다. [그림 9]는 시스템의 동작을 검증하기 위해서 Spartan xc2s200 소자를 이용한 암호화에 대한 시뮬레이션 결과를 나타낸다.



[그림 9] 영상 데이터의 암호화에 대한 시뮬레이션 결과
[Fig. 9] Simulation result for the encryption of image data

사용된 입력 값은 평문 “328831e0435q3137f6309807a88da234” 이며, 키 값은 “2b28ab097eaef7cf15d 2154f16a6883c" 이다. 시뮬레이션 결과로부터 암호화된 “3902dc1925dc116a

8409850b1dfb9732”를 결과로 얻을 수 있었으며, FPGA 보드상에서 시스템의 동작 검증을 위해 SRAM 데이터를 이용하여 동작을 확인하였다. [그림 10]은 복호화에 대한 시뮬레이션 결과를 나타낸다.



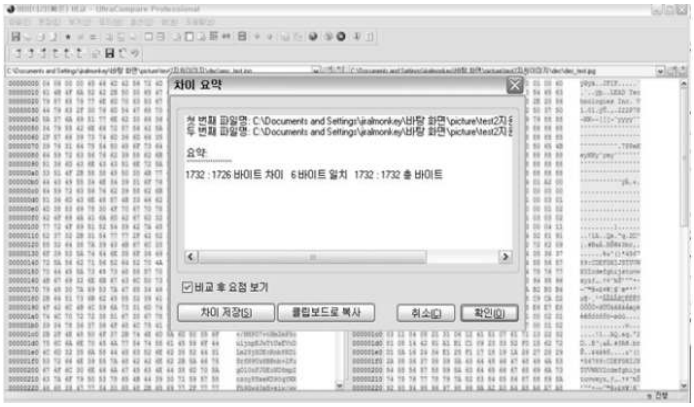
[그림 10] 영상 데이터의 복호화에 대한 시뮬레이션 결과

[Fig. 10] Simulation result for the decryption of image data

5.2 카메라와 Host Server(Viewer) 간의 데이터 검증

5.2.1 암호화 기능만을 동작시켜 데이터 통신을 한 경우

[그림 11]은 FPGA 모듈 내의 암호화 기능을 사용하여 나온 데이터가, View Server의 복호화 기능이 동작하지 않은 데이터와 99.7%의 불일치를 보이며 전혀 다른 파일임을 보여준다.

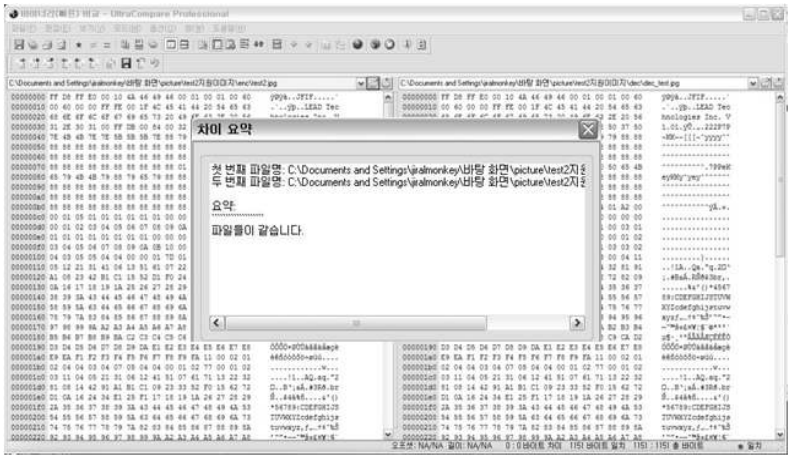


[그림 11] 암호화만 동작한 패킷의 검증

[Fig. 11] Verification of a Packet for encryption

5.2.2 암/ 복호화 기능을 동작시켜 데이터 통신을 한 경우

[그림 12]의 카메라 영상 데이터가 암호화 모듈과 복호화 모듈을 통하여 암/복호화 과정을 모두 거친 데이터와의 패킷 검증이다. 그림을 통해 알 수 있듯이 암/복호화 과정을 모두 거친 데이터는 초기의 원본 데이터와 완전히 같음을 확인할 수 있다.



[그림 12] 암/복호화가 모두 동작한 패킷의 검증

[Fig. 12] Verification of a Packet for encryption and decryption

5.2.3 암호화 및 복호화 적용 상태에서의 영상 정보

[그림 13]의 (A)는 영상 데이터 원본이다. 해당 데이터가 [그림 11]에서 확인된 암호화 기능을 통과하면 (B)와 같이 헤더 정보와 데이터가 모두 암호화 되어 전혀 알아볼 수 없는 데이터로 변환됨을 확인 할 수 있다. 또한 (B)데이터가 복호화 기능까지 통과하면 (C)의 영상 데이터가 나타난다. (A)와 (C) 패킷비교는 [그림 12]에 나타나 있다.

[그림 13] 원본(A), 암호화 후(B), 복호화 후(C)

[Fig. 13] Original (A), after encryption (B), after decryption (C)

6. 결론

본 논문에서는 AES 암호 알고리듬을 이용하여 CCTV에서 디지털 영상정보를 보호하기 위한 보안 시스템의 설계 및 구현에 관하여 기술하였다. 구현된 시스템은 기존 설치되어있는 디지털 CCTV (Webcam)에 보안 기능을 쉽게 적용할 수 있도록 Embedded 기반의 보드와 AES 기반 FPGA 암호화 모듈 및 View Server 복호화 모듈을 설계하였다. 실험 결과를 통해서 실제 영상 데이터의 암/복호화 (128비트) 가 완벽하게 이루어지고, 암호화된 데이터는 Key가 없을 경우 전혀 해독할 수 없음을 확인하였다. View Server에서의 암호화 모듈은 C++ 언어를 사용하여 구현하였고, FPGA 암호화 모듈은 Xilinx ISE 9.1i 툴을 사용하여 Verilog HDL로 설계하였다. 구현된 시스템은 CCTV (비디오 서버)와 서버 연결 구간의 영상정보를 암호화하고, 각 CCTV와 디스플레이 구간 사이에 각기 다른 제품들에 독립적으로 동작 가능한 모듈을 장착함으로써 전송중인 영상 정보에 대한 보안이 가능하다. 본 논문은 중소기업청 주관의 2009년도 산학공동기술개발사업의 일환으로 수행되었다.

참고문헌

[1] 최인섭, “주요 국가의 강력범죄 발생추세 비교분석”, 한국형사정책연구원 연구총서 04-23, pp. 3, 2004.

[2] 김석기, “방범용 CCTV의 범죄예방효과 제고방안에 관한 연구”, 석사학위논문, 동국대학교 경찰행정학, 2007.

[3] 정길원, 방은하, 김보람, 권자경, 강윤경, 유성민, “정보보호 동향”, KISA-WP-2007-0005, 2007.11.

[4] 전황수, “DVR 시장 동향 및 국내외 개발 현황”, 한국전자통신연구원, 전자통신동향분석 제 24권 제3호 2009.

[5] FIPS, "Announcing the ADVANED ENCRYPTION STANDARD", Federal Information Processing Standards Publication 197, November 26, 2001.

[6] 구본석, 유권호, 양상운, 장태주, 이상진, “RFID 태그를 위한 초소형 AES 연산기의 구현”, 정보처리학회 논문집, 제16권, 제5호, 정보처리학회, 2006.

[7] 양현창, 신경욱, “합성체 기반의 S-box와 하드웨어 공유를 이용한 저면적/고성능 AES 프로세서 설계”, 전자공학회논문지, 제45권 SD편, 제8호, 전자공학회, 2008.

[8] 전병찬, 장태민, 이남기, 강민섭, “개선된 AES 암호 프로세서 기반 RFID Reader 및 Tag Core 설계”, 대한전자공학회 논문집, 추계학술대회, 제31권, 제2호, 대한전자공학회, 2008.

저자 소개

강민석 (Min-seok Kang)

2010년 안양대학교 컴퓨터공학과(공학학사)
2010년 ~ 현재 안양대학교 컴퓨터공학과(석사과정)
관심분야 : 정보보안, 스마트그리드, 임베디드 설계

배지수 (Ji-su Bae)

2005 ~ 현재 안양대학교 컴퓨터공학과(학부과정)
관심분야 : 정보보안, 임베디드 설계

장태민 (Tae-min Jang)

2006년 방송통신대학교 컴퓨터과학과(학사)
2008년 안양대학교 컴퓨터공학과(공학석사)
2008년 ~ 현재 안양대학교 컴퓨터공학과(박사과정)
2008년 ~ 현재 안산1대학 디지털정보통신과 겸임교수
관심분야 : VLSI 설계, 암호프로세서 설계, 임베디드 설계, IBS 통신 보안, RFID/USN

강민섭 (Min-sup Kang)

1979년 광운대학교 전자통신공학과(학사)
1984년 한양대학교 전자공학과(공학석사)
1992년 일) 오사카대학교 전자공학과(공학박사)
1984~1992년 한국전자통신연구원 선임연구원
2001~2002년 University of California, Irvine 전기전자공학과 객원교수
1993년 ~ 현재 안양대학교 컴퓨터공학과 교수
관심분야 : ASIC 설계, 암호프로세서 설계, 신호처리, 네트워크 보안, 스마트그리드, RFID/USN