[5A-95]

DCT-기반 영상/비디오 컨텐츠를 위한 보안전용 고속 암호화 시스템의 하드웨어 구현

박성호, 최현준, 윤홍준, 서영호, 김동욱
광운대학교 전자재료공학과 디지털 설계 및 테스트 연구실
psh12280@explore.kw.ac.kr

Hardware Implementation of High-Speed Crypto System for Security of DCT-Based Image/Video Contents

Sung-Ho Park, Hyun-Jun Choi,Hong-Jun Yun,
Young-Ho Seo, Dong-Wook Kim
Digital Design & Test Lab. Kwangwoon University

요 약

본 논문에서는 MPEG과 JPEG등의 이산여현변환(Discrete Cosine Transform, DCT)기반 영상/비디오 컨텐츠를 위한 보안전용 고속 암호화 시스템을 하드웨어로 구현하였다. 영상/비디오 코덱의 많은 연산량을 고려하여 구현된 암호화 시스템은 DC 및 DPCM계수의 일부분만 암/복호화 시킨다. 그 결과 암호화 비용을 $(1/448\sim1/64+N_I)\times N_{Bp}\times N_{Bn}/5$($N_I$: B 와 P 프레임내의 인트라 매크로 블록의 비율, N_{Bp} : 암호화 시킬 블록의 간격, N_{Bn} : 암호화시킬 DPCM계수의 비트수, MB_{Hor} : 영상의 가로방향의 인트라 매크로블록의 수, $0\le N_I\le 1/448$, $0\le N_{Bp}\le MB_{Hor}$, $0\le N_{Bn}\le 5$)만큼 감소시켰다. 한편 암호화 후 압축률은 불과 1.6% 감소했으며 원 영상을 인식할 수 없을 정도의 암호화 효과를 얻었다. 암호화 알고리즘은 다중모드 SEED, AES, DES를 선택적으로 사용하였다.

보안전용 고속 암호화 시스템은 하이닉스 0.25μm CMOS 팬텀-셀 라이브러리를 이용해서 Synopsys™의 디자인 컴파일러로 합성했다. Cadence™의 Verilog-XL을 이용하여 타이밍 시뮬레이션을 수행했으며 동작주파수 100MHz 이상에서 안정적으로 동작함을 확인하였다. 구현된 하드웨어는 DCT-기반 영상/비디오 코덱에서 뿐만 아니라 IPSec등의 인터넷 보안 프로토콜을 위한 보안전용 프로세서로도 활용할 수 있도록 IP화 하였다. 그러므로 현재 중요한 문제로 대두되고 있는 종단 간(end-to-end)보안에 대한 좋은 해결책으로 유용하게 사용될 수 있으리라 기대된다.

I. 서 론

현재 멀티미디어(multimedia) 기술은 정보산업뿐만 아니라 경제, 문학등 사회 각처에서 활용되고 있을 정도로 우리 생활의 중요한 요소로 자리 잡고 있다. 멀티미디어의 핵심 미디어는 영상과 음향이다. 특히 영상데이터는 그 양이 방대하므로 PCM(Pulse Code Modulation)으로 이들을 처리할 경우 저장매체의 과다한 용량이 요구된다. 또한 한정된 대역폭(bandwidth)의 유/무선 네트워크를 통해서 전송시에도 많은 어려움이 따른다[1][2]. 이러한 문제점을 극복하기 위해서 영상/비디오 압축부호화에 관한 기술개발 및 표준 제정활동은 꾸준히 진행되어 왔다.

영상/비디오 압축부호화에 관한 국제 표준의 예로 ITU-T(International Telecomunication Union - Telecomunication standardization)의 MPEG(Moving Picture Experts Group) 및 JPEG(Joint Photographic Experts Group), H.26X계열등의 DCT 기반 표준들을 들 수 있다[3][4][5]. 그림 1에서 ITU-T의 영상/비디오 압축 부호화에 관한 표준제정을 시대 순으로 나열하였다.

영상/비디오 압축부호화에 기술발전과 더불어 유/무선통신 기술도 급속히 발전하면서 서로 다른 컴퓨터 간 접속이 빈번해졌고 영상/비디오 데이터의 교류는 더욱 활발해졌다. 따라서 점차 X-ray사진등의 개인정보와 영상 컨텐츠등의 사업적 이윤을 목적으로 하는 유료정보, 공공 기관의 비밀정보등에 대한 접근권한과 보호가 중요한 사항으로 대두되었다.

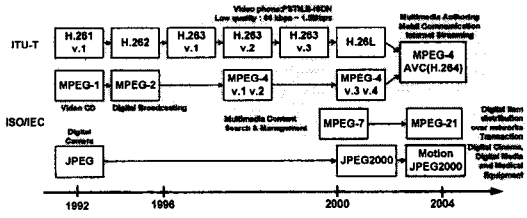

그림 1. ITU-T의 영상/비디오 압축 부호화에 관한 표준제정

정보의 보호를 포함해서 전달 및 저장형태의 보안을 위해서 암호학을 이용하고 있다. 암호화 알고리즘은 크게 공개키 암호화 알고리즘, 블록암호 알고리즘(block chipher), 해쉬(hash) 알고리즘으로 분류될 수 있다[6]. 이외 카오스(chaotic) 시스템도 암호화의 수단으로 사용된다. 그러나 이는 일정한 패턴(pattern)을 갖는 암호화 데이터를 출력함으로써 brute-force 공격[6]에 취약하므로 응용이 제한적이다[7].

블록암호 알고리즘을 이용한 DCT-기반 영상/비디오 컨텐츠의 암/복호화를 위한 연구는 1998년부터 현재까지 계속 진행되어 왔다. Changgui와 Bhargava은 인트라(Intra, I) 프레임(frame)의 DCT영역에서 DC계수만 암호화 하는 방법[8]을 제안하였고 Lintian Quiao 와 Nahrstedt는 DCT후의 스캔(scan)순서를 암호화하였다. 이외 많은 연구가 선행되었지만 암호화후의 압축률 감소, 복잡한 제어, LCA(Linear Crypto Analysis)공격[6]에 취약하다는 단점 때문에 응용이 제한적이다. 저자는 이