[9-82] H.264/AVC 기반 영상 컨텐츠의 보안을 위한 효율적인 암호화 기법

윤홍준, 서영호, 김동욱
광운대학교 전자재료공학과 디지털 설계 및 테스트 연구실
redsemi@kw.ac.kr http://ddntlab.kw.ac.kr

A Efficient Ciphering Scheme for H.264/AVC Based Video Contents

Hong-Jun Yun, Young-Ho Seo, and Dong-Wook Kim
Department of Electronic Materials Eng., Kwangwoon University

요 약

본 논문에서는 H.264/AVC[1] 기반 영상 컨텐츠의 보안을 위한 효과적인 암호화 방법을 제안하였다. H.264/AVC는 기존 MPEG계열과는 다른 정수(Integer) DCT를 사용한다. 이러한 특징을 이용하여 코덱 및 암호화의 많은 연산량을 줄이는 방법으로 주파수 영역에서 중요한 정보를 갖으면서 인접 블록 및 프레임으로 파급 효과가 큰 DC계수를 선정하고 압축률을 고려하여 부분적으로 암호화 하였다. 암호화 알고리즘은 다중모드 SEED, AES, DES[2][3][4]를 선택적으로 사용하였다. 암호화 검증은 C++언어를 이용하여 구현한 암호화 소프트웨어와 H.264/AVC 참조 소프트웨어를 이용하여 약 400여개 영상을 대상으로 실험 하였다. 그 결과 암호화에 필요한 데이터와 연산시간을 최대 1/256에서 최소 1/64만큼 감소 시켰음에도 불구하고 암호화 효과는 우수 하였다. 제안된 암호화 방법은 지금 연구와 표준화 과정을 거치고 있는 IPMP와 더불어 비디오 컨텐츠 보안 방법으로 많은 연구가 기대된다.

I. 서 론

정보화 사회가 급진전되면서 유/무선 네트워을 통한 문자, 영상, 오디오, 비디오 등의 정보 전달 매체들이 복합적으로 형성된 멀티미디어가 디지털 데이터 전송에 사용되는 비율이 증가되었다. 이와 같이 유/무선을 통한 서로 다른 컴퓨터 및 통신망 사이의 상호 접속이 빈번해짐에 따라 개인정보와 영상 컨텐츠 등의 유료정보에 대한 접근권한과 보호가 중요한 사항으로 대두되었다. 이에 따라서 정보보호를 포함한 정보전달 및 저장형태의 보안을 위한 방안으로 암호학을 이용하고 있다[5].

정보 보호 대책으로 DRM(Digital Right Management)이 논의 되고 있지만 해킹(hacking)등으로 정보가 유출되는 경우를 고려한 정보의 접근권한 자체의 통제 기능이부가적으로 요구되어야 한다.

H.264/AVC 기반의 코덱은 DCT 및 움직임 추정, 움직임 보상과 같은 많은 연산량을 필요로 한다. 블록암호 알고리즘 역시 암호화 강도는 높으나 많은 연산량을 필요로 한다. 따라서 이들 컨텐츠를 블록암호 알고리즘을 이용해서 많은 지연을 갖지 않도록 효율적으로 암호 및 복호화하기 위해서는 적은양의 중요한 데이터를 선택적으로 암호화해서야 한다. 이를 위해서는 암/복호화 할 데이터 영역을 신중히 선택해야 한다.

H.264/AVC에서는 화면내 예측(Intra Prediction)과 화면간 예측(Inter Prediction)을 사용 한다. 즉 참조 하는 계수가 암호화 되어 있으면 예측 부호화된 블록은 원영상과 전혀 다른 영상이 된다

먼저 암/복호화 할 데이터는 영상의 중요한 정보이어야 하며, 인접 픽셀 및 매크로 블록, 프레임에 많은 파급효과를 가져야 암호효과를 쉽게 전파시킬 수 있다. 또한 암호화후 압축률이 감소하지 말아야 하며 네트워크 상으로 전송 시 문제가 되지 않는 비트스트림을 제공해야 한다. 이를 위해 MPEG 비트스트림의 암/복호를 위한 연구는 1998년 이래, 활발히 진행되어 왔다.

Changgui와 Bhargava은 I 프레임의 DCT 도메인에서의 DC계수만 암호화 하였으나 인트라 매크로블록이 많은 B와 P 프레임에서는 효율적이지 못하다[6]. Lintian quiao 및 Nahrstedt는 DCT 후의 스캔순서(Scan order)를 암호화하였으나 이는 런길이 코딩(Run-length coding, RLC)을 고려할때 압축률을 감소시킬 수 있다[7].

Jiantao 및 Severa는 가변길이 코드의 인덱스를 그룹단위로 뒤섞어서 암호화 시켰다. 그러나 암호화 효과는 뛰어나나 연산 시간이 많고, 그를 위한 제어가 복잡하며 디코더에서 복호 시 디코딩 자체가 되지 않는다[8].

본 논문에서는 블록암호 알고리즘과 코덱의 많은 연산량을 고려해서 적은양의 데이터만 강도 높게 암호화함으로써 최대의 암호화 효과를 갖게 하는 H.264/AVC 기반의 유료영상 컨텐츠를 보호하기 위한 암호화 알고리즘을 제안하였다. 본 논문 2장에서 암호화 시스템이 삽입된 코덱의 구조를 제시하고 3장에서 DCT 계수의 부분적인 암호화 방법을 설명한다. 4장에서 원 영상과 암호화된 영상을 비교해 놓은 시뮬레이션 결과를 보이며 5장에서 요약하며 결론을 맺는다.