[5A-108]

H.264/AVC 기반 컨텐츠의 보안을 위한 네트워크-적응적 암호화 기법

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

Network-Adaptive Ciphering Scheme for H.264/AVC Based Contents

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

요 약

본 논문에서는 H.264/AVC 기반 컨텐츠를 위한 효과적인 암호화 방법을 제안하였다. 코덱 및 암호화에 따른 많은 연산량을 고려하여 DCT 영역에서 중요한 정보를 갖으면서 인접 블록 및 프레임으로 파급 효과가 큰 DCT 및 차분부호 계수들을 선정하고 압축률을 고려하여 부분적으로 암호화하였다. 암호화 알고리즘은 다중모드 SEED, AES, DES를 선택적으로 사용하였다. C++ 언어를 이용하여 구현한 암호화 소프트웨어와 VM을 이용하여 약 1000여개의 영상을 대상으로 실험 하였다. 그 결과 암호화에 필요한 데이터와 연산시간을 최대 1/64에서 최소 1/64×4×N(N : 암호화시킬 블록간격)만큼 감소시켰음에도 불구하고 암호화 효과는 우수하였다.

I. 서 론

정보화 사회가 진전되면서 인터넷을 이용한 문자, 오디오, 비디오 등의 정보 전달 매체들이 복합적으로 형성된 멀티미디어가 디지털 데이터의 전송에 사용되는 비율이 증가되었다. 이와 같이 유/무선을 통한 서로 다른 컴퓨터 통신망 사이의 상호 접속이 빈번해짐에 따라 개인정보와 영상 컨텐트 등의 유료정보에 대한 접근권한과 보호가 중요한 사항으로 대두되었다. 정보보호를 포함해서 정보전달 및 저장형태를 정보 공학적으로 발전시키기 위한 방안으로 암호학을 이용하고 있다.

정보 보호 대책으로 DRM(Digital Right Management)이 논의 되고 있지만 해킹(hacking)등으로 정보가 유출되는 경우를 고려한 정보의 접근권한 자체의 통제 기능이 부가적으로 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 복호화 하기 위해서는 적은양의 중요한 데이터를 선택적으로 암호화해서야 한다. 이를 위해서는 암/복호화 할 데이터 영역을 신중히 선택해야 한다.

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.

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 코덱과 암호화 방법을 설명하고 3장에서 DCT 및 차분부호계수의 부분적인 암호화 방법을 설명한다. 4장에서 원 영상과 암호화된 영상을 비교해 놓은 시뮬레이션 결과를 보이며 5장에서 요약하며 결론을 맺는다.

II. H.264/AVC 코덱 및 암호화

2-1 H.264/AVC 코덱

그림 1과 그림 2의 H.264/AVC의 인코더 및 디코더를 나타내었다.

영상을 압축할 경우 DCT 및 양자화 단계를 거친 영상은 IDCT 및 역양자화 단계를 거쳐서 복원된다. 움직임 추정기는 복원된 영상과 다음에 입력되는 영상과 중복을 비교한 후 움직임 벡터를 출력한다. 압축효율의 향상을 위해서 인트라 매크로 블록내의 모든 블록과 차 영상의 오차가 크게 발생한 매크로 블록내의 블록에 대해서만 DCT를 수행해서 DCT계수들에 대한 정보를 차 영상에 대한 정보로 전송한다. 나머지 매크로 블록들에 대해서는 움직임 추정기에서 참조 프레임의 움직임 추정 범위내의 매크로 블록간 오차를 비교해서 두 종류로의 매크로 블록으로 부호화한다. 오차 비교 결과, 참조프레임의 인트라 매크로 블록과 매우 유사한 매크로 블록들에 대해서는 데이터를 전송시키지 않고 임계값 이상의 오차값을 보이는 매크로 블록까지의 주소 증가치만 VLC해서 전송한다. 이러한 매크로