무결성 보장을 위한 AES-CCM 기반의 멀티미디어 데이터 보호

이은지, 김학재, 이성주, 정용화
고려대학교 컴퓨터정보학과
e-mail : achee@korea.ac.kr

Ensuring Integrity of Multimedia Data Using AES-CCM

Eun-Ji Lee, Hakjae Kim, Sung-Ju Lee, Yongwha Chung
Dept. of Computer and Information Science, Korea University

요 약

대용량의 MPEG 비디오 스트림을 보호하고 암호화의 연산량을 줄이기 위한 방법으로 몇 가지 부분 암호화 기법이 보고되었다. 그러나, 멀티미디어 데이터의 무결성을 보장하기 위해서는 암호화 표준으로 이용되고 있는 HMAC 등의 메시지 인증 기법을 추가적으로 적용할 필요가 있다. 본 논문에서는 현재 암호화 표준으로 이용되고 있는 CCM을 이용하여 멀티미디어 데이터의 무결성을 보장하는 시스템을 제안한다. 또한, 제안한 시스템은 인코딩 및 디코딩의 실시간 요구사항을 만족하기 위하여 부분 암호화 기법으로 이용되는 SECMPEG 보안레벨 3와 호환이 이루어지도록 CCM을 MPEG의 계층적 구조를 고려하여 적용한다. 실험 결과를 통하여 제안 방법은 멀티미디어 데이터의 기밀성 및 무결성을 보장하면서 실시간 처리 성능을 제공함을 확인하였다.

1. 서론

멀티미디어 기술의 발전으로 멀티미디어 콘텐츠는 카메라가 장착된 휴대폰이나 디지털 카메라와 같은 휴대용 장치로 손쉬운 제작이 가능해졌다. 또한, 컴퓨터로 간편하게 수정하여 바로 온라인을 통해 여러 사람과 공유함으로써 훼손되어서는 안되는 데이터의 조작으로 사생활이 침해될 수 있다.

이러한 문제를 해결하기 위해, 멀티미디어 데이터의 기밀성을 보장하는 방법으로써 실시간 수행을 위한 부분 암호화 기법이 제안되고 있다[1]. 그러나 이러한 방법은 단순히 데이터를 암/복호화 하기 때문에 HMAC(Keyed-Hash Message Authentication Code)과 같은 메시지 인증 기법을 추가적으로 적용할 필요가 있다. 따라서, 메시지 인증을 할 수 있는 암호화 알고리즘[2]을 적용하여 멀티미디어 데이터의 무결성[3]을 보장해야 한다.

본 논문에서는 실시간 수행을 만족하기 위해 멀티미디어 콘텐츠의 압축과 보호가 밀결합(tightly-coupled)되고, 다양한 장치에서 이용 가능한 SECMPEG(Secure MPEG) 보안레벨 3를 적용한다. SECMPEG[4]는 여러 분야에서 응용되는 MPEG-2 인코더에 대용량 멀티미디어 콘텐츠의 보호와 성능을 동시에 고려한 선택적 암호화 방식이다. 또한, 위변조를 방지하기 위하여 AES[5]기반의 운용모드인 CCM(Counter with CBC-MAC)을 적용하여 메시지 무결성을 보장한다.

CCM은 주로 대칭키 암호화 기법인 AES와 함께 이용되고 있으며, AES-CCM은 암/복호화 하는데 수행속도가 빠르고, 한번의 수행만으로 기밀성과 메시지의 무결성을 동시에 보장할 수 있는 특성을 갖는다. 따라서, SECMPEG 보안레벨 3에 CCM을 적용한다면, 단 한차례의 수행만으로 대용량 멀티미디어 데이터의 기밀성과 무결성을 동시에 보장할 수 있다. 실험을 통하여, 선택적 암호화 기법과 CCM을 적용함으로써 대용량 멀티미디어 데이터의 기밀성과 무결성을 보장하면서 실시간 수행까지 가능함을 확인하였다.

2장에서는 선택적 암호화 방식의 SECMPEG과 무결성을 보장하는 기법에 대해서 설명하고, 3장에서는 AES-CCM을 SECMPEG에 효율적으로 적용하는 방법을 설명한다. 4장에서는 제안한 내용을 바탕으로 실제 구현된 시스템의 성능을 실험하고 그 결과를 분석한다. 마지막 5장에서의 결론으로 논문을 마친다.

2. 배경

2.1 SECMPEG

멀티미디어 콘텐츠는 대용량의 데이터로 실시간 처리가 요구되기 때문에 전체를 암호화 하는 것은 부적절하다. 또한, 임베디드 시스템과 같은 계산처리 능력이 낮은 환경에서는 멀티미디어 데이터의 보안이 오버헤드로 적용된다. 따라서 처리 성능에 미치는 영향을 최소화하고 적절한 보안을 위한 선택적 암호화 방법이 연구되고 있다[1]. 그 중 SECMPEG[4]의 선택적 암호화는 MPEG의 데이터 구조를 이용하여 5단계의

보안레벨을 제안하였다. 보안레벨 0과 보안레벨 4는 각각 암호화를 하지 않는 것과 전체를 암호화하는 것이다. 보안레벨 1은 디코딩된 멀티미디어 데이터의 재생에 필요한 정보인 시퀀스 헤더와 프레임을 디코딩하기 위한 정보인 슬라이스 헤더를 암호화하는데, 비교적 보안성이 약하다.

일반적인 MPEG 인코더는 I-, P-, B-frame의 조합으로 GOP(Group of Picture)가 구성되고, P- 혹은 B-frame은 I-frame의 데이터에 의존하여 움직임 보상을 수행한다. 따라서 압축된 멀티미디어 데이터를 디코딩시에 I-frame의 정보 없이 P- 혹은 B-frame을 디코딩할 수 없다. 또한, DCT와 양자화가 적용되는 영상 내 부호화 블록(intra-coded block, I-block)들은 영상 내 부호화 모드(intra mode)가 시작되는 첫 번째 블록에 의존하여 부호화가 된다. SECMPEG의 보안레벨 2는 보안레벨 1과 함께 I-frame에서 영상 내 부호화 모드가 시작되는 첫 번째 영상 내 블록을 추가적으로 인코딩한다. I- 혹은 P-frame을 참조하여 P- 혹은 B-frame의 움직임 보상을 수행할 때, 움직임 예측을 통해서 유사한 블록을 찾지 못했을 경우, 해당 매크로 블록은 영상 내 부호화 모드로써 인코딩된다.

따라서 움직임이 많은 멀티미디어 데이터에 대해서는 I-frame을 암호화하여도 P- 혹은 B-frame의 영상 내 부호화 블록에서 보안이 취약할 수 있다. 이를 위해 SECMPEG의 보안레벨 3에서는 전체 I-frame과 P- 혹은 B-frame의 I-block을 암호화한다. 이와 같이 SECMPEG는 MPEG의 데이터 구조 특성을 이용하여 선택적으로 암호화한다. 또한, 암호화 알고리즘은 블록 암호화 표준인 DES를 사용하는데 본 논문에서는 보다 나은 보안성을 위해 AES를 사용한다.

표 1은 SECMPEG의 보안레벨 0부터 보안레벨 4까지의 시스템 성능 및 보안강도를 보여주고 있다.

<표 1> SECMPEG 보안레벨 비교[4]

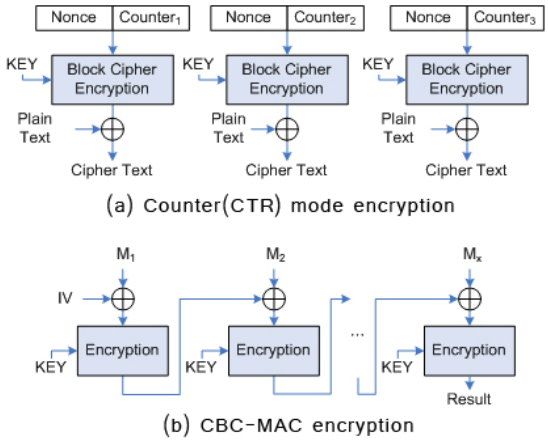
보안레벨	암호화 적용 부분	데이터 크기
0	x	x
1	Sequence Header	40byte
	GOP Header	8byte/GOP
	Picture Header	16byte/Frame
	Slice Header	6byte/Slice
2	Security Level 1	Security Level 1
	I-block 의 시작	384byte
3	I-Frame	가변적
	P-/B-Frame 의 I-block	가변적
4	인코딩 된 비디오	가변적

2.2 무결성을 보장하는 방법

데이터의 무결성을 보장하기 위해 사용되는 방법들은 다양한 응용에서 널리 사용되고 있다. 대표적인 방법으로 데이터의 무결성 검증을 위해 입력 값이 변하면 다른 값을 만드는 해시(Hash)를 이용한 방법이 있다. 그러나 단순히 메시지를 해시된 코드와 전송한다면, 누구나 메시지를 이용하여 새로운 해시코드를 만들어 낼 수 있다. 따라서 해시를 키에 종속적으로 만든 것이 HMAC이다. HMAC은 사용하는 해시함수의 특성과 키와 해시코드의 길이에 의존하여 보안성이 결정된다.

다른 방법으로 암호화 운용모드(mode of operation)를 이용하는 방법이 있다. 블록 암호화 알고리즘은 데이터를 일정한 크기의 블록단위로 반복적으로 암호화한다. 따라서 데이터의 사이에 종속성이 약해지는 단점이 생기는데, 그것을 보안하기 위해 사용하는 것이 운용모드이다. 데이터의 무결성과 기밀성을 보장하기 위해 미국 국가기술표준국(NIST)에서는 5가지 운용모드를 표준으로 제안하고 있다[6]. 그 중 CTR(Counter mode)는 그림1의 (a)와 같이 임의의 수(Nonce)와 counter를 일정한 값으로 증가하여 암호화에 사용하기 때문에 블록 암호를 스트림 암호처럼 사용할 수 있게 해준다. 키와 Nonce를 미리 계산하여 알 수 있어 데이터를 실시간 암호화 할 수 있고, 병렬성이 뛰어난 장점이 있다.

무결성을 보장하는 방법으로 해시 기반의 운용모드를 이용하는 방법 중 가장 많이 사용되고 있는 것이 CBC-MAC이다. 그림1의 (b)에서 알 수 있듯이 블록 암호화 운용모드 중 하나인 CBC를 사용하여 마지막 블록을 메시지의 무결성을 인증하는 코드인 MAC으로 사용하는 방법이다. CBC는 블록 암호화의 약점인 데이터 사이의 독립성을 제거해 주기 때문에 일부 데이터가 변조되었을 때 나머지 데이터들도 복호화 할 수 없다. 즉, CBC의 마지막 블록을 MAC으로 사용하면 데이터의 무결성을 보장할 수 있다.



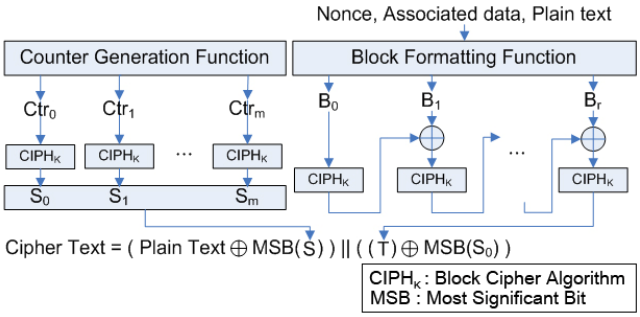
(그림 1) CTR 과 CBC-MAC 과정[2]

3. 본론

3.1 멀티미디어 적합한 AES-CCM

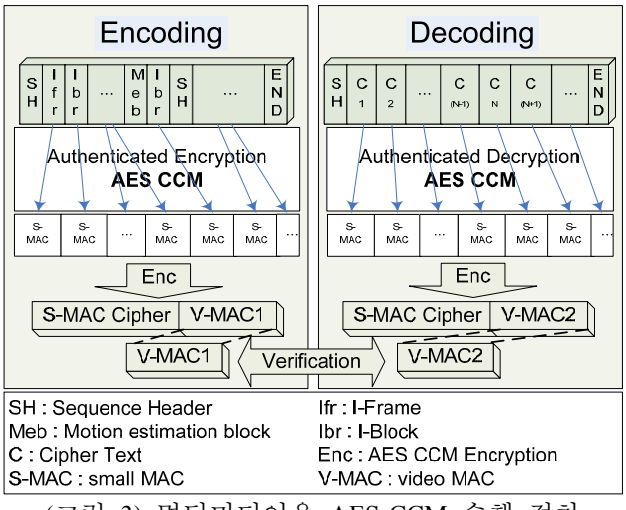
다양한 운용모드들 중에서 무결성을 보장할 수 있는 것이 CCM이다[7]. 그림 2와 같이 CCM은 운용모드 중 하나인 CTR와 인증과 무결성을 검증할 수 있는 CBC를 결합한 것이다. 이미 알려진 두 가지 기술들을 사용하기 때문에 신뢰성이 강하고 CBC-MAC에

서 인증과 암호화에 다른 키를 사용하는 것과 다르게 한 개의 키로 두 가지 모두 사용 가능하다. 또한 인증만 필요한 데이터가 포함된 경우 추가적인 암호문 오버헤드 없이 암호화할 수 있어서 인증을 해야 하는 데이터를 다루기가 쉽다[8]. 뿐만 아니라 CCM은 암호화 함수 하나를 사용하여 암호화와 복호화를 모두 수행하기 때문에 비교적 작은 크기의 코드를 필요로 한다. 이러한 특성의 CCM은 다른 운용모드들에 비해 융통성 있는 적용이 가능하다.



(그림 2) CCM의 블록 다이어그램[7]

그림 3은 멀티미디어 데이터에 AES-CCM을 적용하여 메시지 인증을 위한 V-MAC과 S-MAC을 생성하는 과정을 보여주고 있다. V-MAC은 비디오 무결성을 위한 Video MAC으로써 멀티미디어 데이터의 전체적인 무결성을 검증하고, S-MAC은 선택적 암호화가 되는 부분 데이터 각각의 MAC으로써 전체 동영상 중 변조된 부분을 찾는 역할을 수행한다. 인코딩할 때 생성된 S-MAC의 암호문과 V-MAC은 MPEG-2 데이터와 함께 저장된다. 검증을 필요로 하는 MPEG-2 데이터의 디코딩 결과로 만들어지는 S-MAC을 이용하여 인코딩과 같은 방법으로 V-MAC을 생성한다. 이러한 방법은 데이터 전체의 무결성 검증이 필요로 할 때, V-MAC만 사용하여 각각의 S-MAC을 확인하는 오버헤드를 줄일 수 있다. 그러나 부분적인 무결성 검증이 필요한 경우 S-MAC 사이의 무결성을 V-MAC이 보장해 주기 때문에 선택적으로 암호화해서 만들어진 S-MAC도 무결성을 검증할 수 있다.

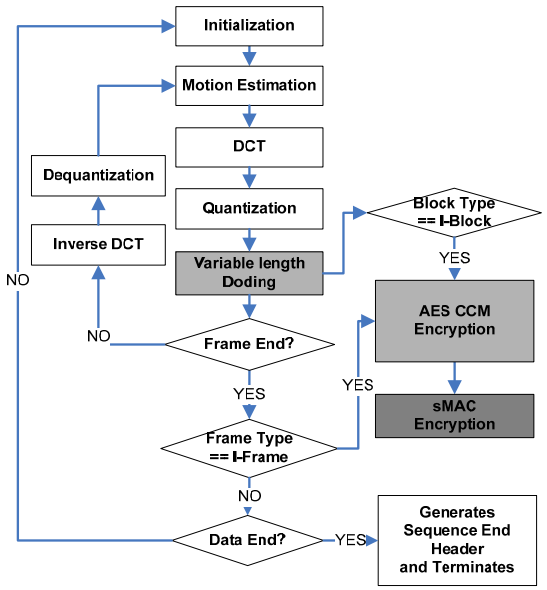


(그림 3) 멀티미디어용 AES-CCM 수행 절차

3.2 AES-CCM을 이용한 멀티미디어 보호

본 논문에서는 SECMPEG 보안레벨 3에 AES-CCM을 적용하는 방법을 제안한다. SECMPEG의 보안레벨 3의 경우, P- 혹은 B-frame의 모든 I-block과 I-frame을 암호화 하기 때문에 인코딩과 밀결합하여 수행되어야 한다. 특히, 본 논문에서는 기존의 DES 알고리즘을 대신하여 데이터의 무결성 보장과 보다 나은 보안성을 위해 AES-CCM을 사용한다. 이와 같은 방법으로 멀티미디어 데이터가 인코딩되는 동안 데이터를 보호하기 위한 암호화 작업이 함께 수행된다.

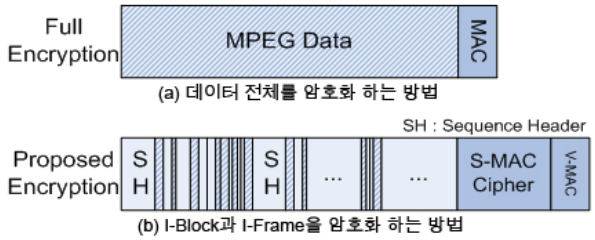
그림 4는 본 논문에서 제안하는 MPEG-2 인코더의 SECMPEG 보안레벨 3에서 DES 알고리즘 대신 AES-CCM 적용 과정을 보여준다. SECMPEG의 보안레벨 3는 전체 데이터를 모두 암호화 하지 않고, I-block과 I-frame만을 선택적으로 암호화함으로써 수행속도를 향상시킨다. 따라서 CCM 운용모드를 SECMPEG과 같이 AES로 암호화된 데이터에만 적용하고, 암호화된 I-block과 I-frame은 각각 S-MAC을 생성한다. 또한, 생성된 S-MAC은 다시 한번 AES-CCM을 적용하여 동영상 전체의 V-MAC을 생성한다. 따라서 S-MAC와 V-MAC는 모두 AES로 암호화 되어있기 때문에 정당하지 못한 사용자는 MAC의 내용을 알지 못하게 된다. 그리고 동영상의 내용 중 일부가 변조가 된다면 디코딩 과정에서 S-MAC 및 V-MAC이 일치하지 않아 콘텐츠가 변조되었음을 확인 할 수 있다. 또한, S-MAC은 각각의 I-block 및 I-frame 마다 생성되기 때문에, 변조된 콘텐츠의 정확한 위치까지 파악 할 수 있다.



(그림4) AES-CCM기반 SECMPEG

전체적인 멀티미디어 데이터를 암호화하는 방법과 제안 방법의 차이는 그림 5를 통하여 확인할 수 있다. 제안 방법은 동영상의 전체를 암호화하지 않고 I-block과 I-frame만을 암호화 하여 수행 시간을 단축시킨다. 또한, 메시지 인증을 위해서 CCM 운용모드를 I-block과 I-frame에만 적용함으로써 MAC을 생성할

때 필요한 오버헤드를 최소화 시킬 수 있다.

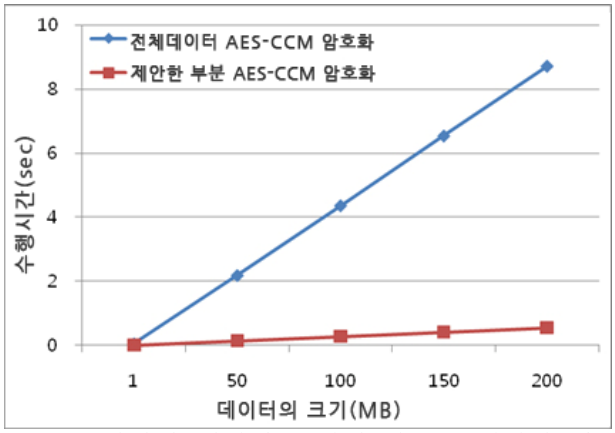


(그림 5) 전체 데이터를 암호화하는 방법과 제안 방법의 비교

4. 실험

본 논문에서는 실험을 위하여 다양한 크기의 MEPG-2 멀티미디어 콘텐츠를 이용하였다. 동영상 내의 정지영상 크기는 한 픽셀당 24bit이고, 가로 세로의 길이는128×128이다. 또한, SECMPEG의 보안레벨 3에서 AES-CCM이 실제 적용되는 I-block과 I-frame의 비율은 평균 2%이었다. 실험환경의 PC는 CPU 2GHz, RAM 512MByte에서 수행하였다.

우선, 동영상 전체를 암호화하는 기존의 방식과 선택적 암호화 방법이 적용된 제안된 방법을 다양한 동영상 크기에 따라 비교하였다. 1MB당 암/복호화 수행시간은 제안한 방법(평균0.0024초)이 기존의 방법(평균0.042초) 보다 약 17배 정도 감소함을 확인할 수 있다. 또한, 그림 6과 같이 수행시간은 동영상 크기가 증가함에 따라 선형적으로 증가하기 때문에 제안 방법은 대용량 동영상 데이터에 보다 효율적으로 적용될 수 있다.



(그림 6) 다양한 데이터 크기에 따른 수행시간 비교

표 2는 실제 환경에서 동영상의 크기가 10MB, 100MB, 500MB일 때의 암/복호화되는 수행 시간을 측정하였다. 동영상의 크기가 500MB일 때 수행 시간은 1.36초이고, I-block 크기 476KB, I-frame의 평균 크기 21MB이다. 또한, S-MAC의 크기는 동영상의 크기에 따라 증가하지만, 전체 동영상 크기에 비해 매우 작기 때문에 무시할 만한 수준이다. 따라서 본 논문에서 제안한 방법은 동영상의 인코딩 및 디코딩을 수행할 때 큰 성능 저하 없이 AES-CCM을 실제 응용에 적용함으로써 동영상의 위변조를 방지할 수 있다.

<표 2> 실제환경에서 AES-CCM 의 수행시간 측정

동영상 크기	*10MB*	*100MB*	*500MB*
I-block 크기	9KB	95KB	476KB
I-frame 크기	440KB	4,387KB	21,928KB
sMAC 의 총 크기	0.84KB	8.39KB	41.93KB
MAC 생성시간	0.0001sec	0.0014sec	0.0052sec
수행시간	0.43sec	0.27sec	1.36sec

5. 결론

본 논문에서는 현재 암호화 표준으로 이용되고 있는 CCM을 이용하여 멀티미디어 데이터의 무결성을 보장하는 시스템을 제안하였다. 즉, 제안 시스템은 인코딩 및 디코딩의 실시간 요구사항을 만족하기 위하여 부분 암호화 기법으로 이용되는 SECMPEG 보안레벨 3과 호환이 이루어지도록 CCM을 MPEG의 계층적 구조를 고려하여 적용하였다. 실험을 통하여, 제안 방법은 멀티미디어 데이터의 기밀성 및 무결성을 보장하면서 1MB당 암/복호화 수행시간이 기존 방법 보다 약 17배 정도 감소함을 확인하였다. 또한, 무결성 검증을 위한 S-MAC의 크기는 동영상의 크기가 10MB~500MB까지 0.84KB~42KB정도로 매우 작기 때문에 무시할 수 있는 수준이다. 따라서 제안한 방법은 대용량 동영상 데이터 보호 시스템에 큰 성능저하 없이 기밀성과 무결성을 동시에 보장하는 방법으로 효과적으로 적용될 수 있을 것으로 기대된다. 향후 연구로는 멀티코어 임베디드 시스템에서 부하균등 기법을 이용하여 보다 효율적으로 처리 가능한 방법을 연구 중이다.

감사의 말

본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성.지원사업의 연구결과로 수행되었음

참고문헌

[1] B. Furth and D. Kirovshi, *Multimedia Security Handbook*, CRC Press, 2005.
[2] J. Black, “Authenticated Encryption,” 2003.
[3] D. Stinson, *Cryptography: Theory and Practice*. CRC Press, Boca Raton, third edition, 2005.
[4] I. Agi and L. Gong, “An Empirical Study of Secure MPEG Video Transmissions,” *Proc. of Symposium on Network and Distributed Systems Security*, pp. 137~144, 1996.
[5] U. S. National Institute of Standards and Technology, “The Advanced Encryption Standard,” *Federal Information Processing Standard(FIPS) 197*, 2002.
[6] NIST Special Publication 800-38A, “Recommendation for Block Cipher Modes of Operation - Methods and Techniques,” *U.S. DoC/NIST*, 2001.
[7] N. Dworkin, “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality,” *NIST Special Publication 800-38C*, 2002.
[8] J. Jonsson, “On the Security of CTR+CBC-MAC,” *LNCS 2595 – Proc. of SAC*, pp. 76–93, 2002.