VOD상에서의 MPEG-1 보안에 관한 연구

임재갑*, 유황빈*, 박광진**
*광운대학교 컴퓨터과학과, **한국정보보호센터 정책지원팀

Study of MPEG-1 Security on VOD

Jae-Kap Lim*, Hwang-Bin Ryou*, Kwang-Jin Park**
*Dept of Computer Science, Kwangwoon University
**Korea Information Security Agency

요약

인터넷을 통한 모든 통신은 사용자 인증만을 가지고는 모든 데이터를 인터넷상에 그대로 노출시키는 위험이 존재한다. 즉, 허가받지 않은 사람도 얼마든지 내용을 볼 수 있을 뿐 아니라 변경도 가능하다. 이러한 문제를 해결하고자 텍스트나 정지영상 등의 소량의 데이터를 암호화하였지만, 최근 많이 사용되는 VOD의 MPEG 데이터는 대용량 데이터를 기존의 방법을 가지고 암호화하기에는 오버헤드가 많이 들고 특히 실시간 서비스에 어려움이 많다.

본 논문에서는 MPEG의 구조적 특성을 이용하여 보안 적용 강도에 따른 다단계 암호화 방법을 설계 및 구현하고 암호화 기법을 이용하여 VOD 서비스를 설계하였다. MPEG의 분석을 통하여 부분 정보만을 암호화함으로 해서 암호화에 따른 오버헤드를 줄일 수 있었고 부분정보의 보안만으로도 충분히 효과적인 데이터보안이 가능하였다. 이러한 부분정보의 암호화는 MPEG외에도 다양한 컨텐츠에 응용될 수 있을 것이다.

1. 서론

초고속 정보통신망의 발달로 인하여 인터넷을 통한 멀티미디어의 통신이 활성화되면서 주문형 비디오(Video On Demand), 화상회의, 원격진료 등

에 대한 연구와 실용화가 활발하게 진행되고 있다. 인터넷을 통한 멀티미디어 통신이 상업적으로 활용되면서 전송되는 정보에 대한 보안 문제가 점점 중요해 지고 있다. 기존에는 소극적인 보안 대책으로 패스워드를 이용한 로그 인으로 사용자 인증을 수행한 후 서비스를 하는 방법으로 보안 문제를 해결하였으나, 이러한 방법도 네트워크를 통한 패스워드 및 사용자의 정보가 인터넷상에 그대로 노출되는 위험 때문에 일회용 패스워드 등 다양한 인증 방법이 연구되어 왔다. 하지만 이러한 인증 문제의 해결만을 가지고는 네트워크에 전송되는 정보를 보호해 주지는 못한다. 중간에서 전송되는 데이터 패킷을 가로채거나 위조□변조 등의 문제가 그대로 존재하기 때문에 이를 막기 위하여 전송하는 정보를 암호화하여 전송하고 있다[5][11]. 이러한 암호화 방법은 대용량 데이터가 아닌 텍스트나 정지 화상 등의 소용량 데이터에는 적합하지만 멀티미디어와 같은 실시간 대용량 데이터에 그대로 적용하기에는 적합하지 않다.

멀티미디어 서비스에 사용되는 MPEG-1 데이터를 보호하기 위한 방법으로 MPEG 파일을 부호화하는 과정에서 암호화하는 방법이 연구되고 있다. 부호화 시에 DC 정보를 랜덤넘버(random number)를 사용하여 XOR하는 방법을 사용하여 암호화함으로써 오버헤드가 적게되는 장점은 있지만 MPEG 파일을 새로이 부호화 해야하는 부담과 보안상 취약하다는 약점이 존재한다[3][4]. 또 다른 방법으로는 공개키 방식을 이용한 시퀀스 헤더(sequence header)와 프레임 헤더(frame header) 정보를 암호화하는 방법이 제안되었다[12]. 이러한 방법은 헤더 정보만을 암호화함으로써 실시간을 보장할 수는 있지만 보안상 취약하다는 약점이 그대로 존재한다. 또한, 공개키 방식의 비효율성으로 인하여 전체 정보의 암호화 시는 많은 오버헤드와 암호화 후에 파일의 크기가 커지는 단점이 존재하고 있다[12].

본 논문에서는 MPEG 파일을 부호화하는 과정에서 암호화하는 방법을 개선하여 MPEG 파일의 구조적 특성을 이용하여 헤더 정보뿐만 아니라 프레임 단위의 암호화하는 다단계(4 단계) 암호화 방법을 제안한다. 제안된 다단계 암호화 방법은 암호화의 효율성을 높이기 위해서 암호화 시에는 대칭키 방식을 이용하고 키의 전달을 위하여 공개키 방식을 사용한다. 제안된 암호화 방법을 VOD 시스템에 적용한 결과 레벨 1과 레벨 2의 경우는 MPEG 데이터의 모든 정보가 아니 부분 정보만을 암호화함으로써 암호화 효율을 높이고 실시간 성을 보장할 수 있었다. 레벨 3의 경우는 전체 정보를 보호하는 측면에서는 뛰어나지만 실시간 성을 보장하기에는 많은 오버헤드가 있었다.

2. MPEG-1 암호화

2.1 MPEG 암호화의 필요성

인터넷을 통한 비디오의 전송에는 많은 문제가 있다. 비단 비디오파일뿐만 아닌 인터넷을 통한 모든 전송은 같은 문제를 가지고 있다. 즉 전송중인 파일을 중간에서 가로채거나 관찰(스누핑)하여 단순히 파일의 내용을 유출시킬 수 도 있고 원본 파일을 변경하여 전송하는 것도 가능하다. 인터넷을 통한 통신은 방해, 가로채기, 불법수정, 위조와 같은 보안 취약점을 가지고 있다.

방해(Interruption) : 시스템의 일부가 파괴되거나 사용할 수 없게 되는 경우로 가용성에 대한 공격으로서, 예를 들면 하드디스크 같은 하드웨어의 일부가 파괴되거나, 통신의 선이 절단되거나, 또는

파일 관리 시스템이 무력화되는 경우 등이다.

가로채기(interception) : 비인가자들의 불법적인 접근에 의한 신뢰성에 대한 공격으로서, 비인가자란 사람이나 프로그램 또는 컴퓨터일 수 있다. 네트워크 상에서 데이터를 가로채기 위한 도청과 파일 또는 프로그램의 불법 복사 등을 예로 들 수 있다.

불법수정(Modification) : 비인가자들의 불법접근뿐만 아니라 불법적인 변경에 의한 무결성에 대한 공격으로서, 예를 들면 데이터 파일내의 값 변경, 프로그램의 다른 기능수행을 위한 변조, 그리고 네트워크 상에서 전송중인 메시지 내용의 수정 등이 있다.

위조(Fabrication) : 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격으로서, 예를 들면 네트워크 상에 위조된 메시지를 삽입하거나 파일에 레코드를 추가하는 경우 등이 있다.

2.2 MPEG의 구조

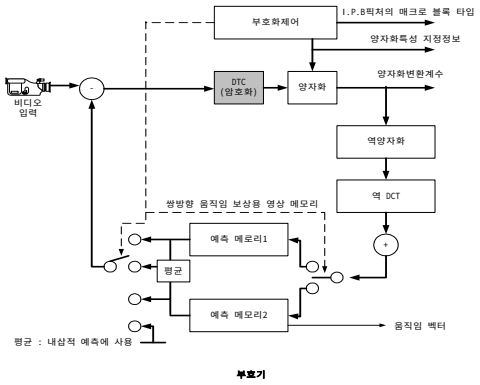
MPEG(Moving Picture Experts Group)표준은 MPEG-1, MPEG-2, MPEG-4를 포함해서 많은 멀티미디어 응용에 사용된다. MPEG 표준은 비디오, 오디오, 스트림 제어 메커니즘을 포함한다. MPEG의 데이터 구조는 계층 구조을 가지고 있다. 시퀀스층 , GOP층, 픽처층, 슬라이스층, 매크로블록층, 블록층으로 구성되어 있다.

2.3 MPEG-1 암호화 방법

MPEG-1의 암호화 방법은 크게 2가지로 나눌 수 있다. 첫 번째는 비디오 데이터의 부호화 시 암호화하는 방법이고 두 번째는 비디오 데이터의 부호화가 이후 즉, MPEG-1 데이터를 암호화하는 방법이다.

2.3.1 MPEG-1의 부호화 시 암호화 방법

MPEG-1 비디오 데이터의 부호화 시 암호화 방법은 원시 동영상 데이터를 MPEG-1 방식으로 부호화할 때 함께 암호화하는 방법이며, MPEG-1 방식으로 암호화 된 데이터는 다시 복호화하여 원시 동영상 데이터를 변환한 후 다시 부호화를 수행하면서 암호화하는 방법이다. 이 방법은 오프라인으로 MPEG-1 비디오 데이터를 미리 암호화하여 저장한 후 필요시 암호화된 비디오 데이터를 전송하는 방식으로, 암호화하는데 오버헤드가 적고, 복호화하는 데도 오버헤드가 적게 된다. 그러나, 이 방법은 비디오 데이터를 부호화할 때 암호화를 함께 수행하여야 하기 때문에 암호화 기능이 포함된 부호기 필요하며, 클라이언트에서도 암호화된 비디오 데이터를 복호화하기 위하여 복호화 기능이 포함된 부호기 필요하다. 또한, 평문 공격에 취약하다.



[그림 1] MPEG 부호기

[그림 1]은 MPEG-1 비디오 데이터를 부호화하기 위한 부호기 구조로서, 암호화 과정은 MPEG-1 비디오 데이터를 부호화할 때 DCT 계수의 sign 비트만을 암호화하는 방법으로서, 랜덤

넘버를 생성하여 DCT계수의 sign 비트와 XOR함으로써 암호화가 수행되는 방법이다[4].

2.3.2 MPEG-1 부호화 이후 암호화 방법

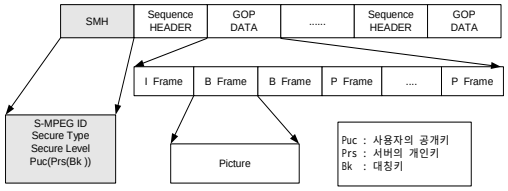
MPEG-1 비디오 데이터의 부호화 이후에 암호화하는 방법은 MPEG-1 방식으로 압축된 비디오 데이터를 전송할 경우 즉시 암호화를 수행하여 전송하는 방법으로 실시간 성이 보장되어야 한다. 기존에 연구된 방법은 암호화를 시행하지 않는 단계(0 단계), 프레임 정보만 암호화하는 단계(1 단계), 헤더 정보만 암호화하는 단계(2 단계), 전체 정보를 암호화하는 단계(4 단계) 등 4 단계로 나누어 암호화하는 방법을 제안하였다. 1 단계와 2 단계 암호화에서는 오버헤드가 적어 실시간 서비스가 가능하고, 키 분배 문제를 해결할 수 있다. 그러나, 3 단계와 4 단계 암호화에서는 오버헤드가 크며, 현재의 시스템으로는 실시간성이 보장되지 않고, 1 단계와 2 단계 암호화의 경우는 보안상 취약점이 있다.[12]

3. 제안된 MPEG-1 암호화 방법

제안하는 암호화 방법은 공개키 알고리즘을 이용한 암호화 방법 대칭키 알고리즘을 이용한 암호화 방법을 같이 사용하였다. 대용량 파일의 암호화에는 대칭키 알고리즘을 사용하고 키 전달에는 공개키 알고리즘을 사용함으로 해서 보안 효과와 속도면 에서 뛰어나다.

3.1 시스템 구성 및 암호화 방법

보안 서비스를 제공하는 패킷의 구조는 [그림 2]와 같다. SMH(Secure MPEG Header)에 암호화 정보를 추가한다.



[그림 2] 암호화 패킷의 구조

Secure MPEG Header는 Secure Type, Secure Level, Puc(Prs(Bk)) 3가지로 구성된다.

① Secure Type : 암호화에 사용된 공개키 알고리즘과 대칭키 알고리즘을 명시

② Secure Level : 보안레벨을 설정

③ Puc(Prs(Bk)) : 대칭키를 서버의 개인키와 사용자의 공개키로 암호화

3.2 암호화 레벨

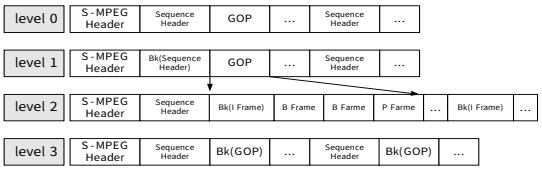
① 레벨 0 : 암호화 시행하지 않는다.

② 레벨 2 : 시퀀스 헤더 정보를 암호화한다.

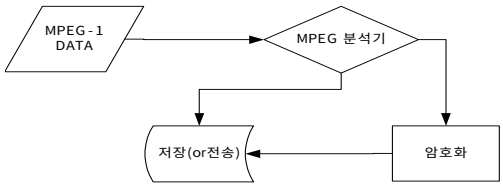
③ 레벨 3 : GOP 중 I 프레임만 암호화한다.

④ 레벨 4 : GOP 프레임 전체를 암호화한다.

[그림 3]은 각 레벨의 암호화 위치를 나타내고 [그림 4]는 저정된 MPEG-1 데이터를 MPEG 분석기를 통하여 암호화할 위치를 파악하여 암호화한 후에 저장하거나 전송한다.



[그림 3] 암호화 레벨



[그림 4] MPEG 분석기를 통한 암호화 과정

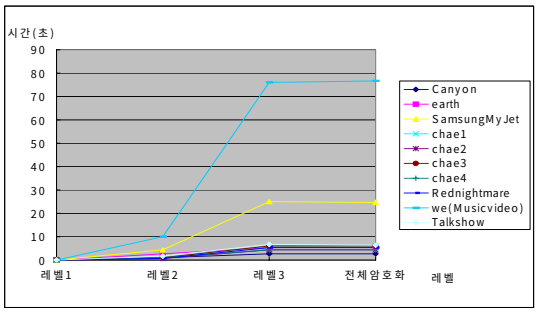
3.3 성능분석

성능 측정은 암호화를 하지 않았을 때 걸리는 시간을 0으로 보고 각각의 레벨에 따라 암호화 할 때의 시간을 측정하였다. 또한 파일의 크기에 따른 암호화 속도를 비율로 나타내었다.

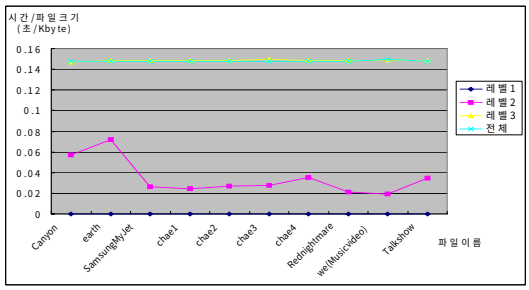
[표 1] 실험 데이터

파일명	GOP 개수	I 프레임	B 프레임	P프레임	파일크기 (Byte)
Canyon	294	294	1171	293	1744060
earth	121	121	479	120	3512363
Samsung Myjet	235	235	1873	1639	16762884
chae1	80	80	480	400	3962003
cahe2	60	60	360	300	2971549
chae3	80	80	840	400	3962003
chae4	60	60	300	360	2971547
Rednightmare	41	41	1088	81	3619896
we (Musicnideo)	729	727	7278	2913	51085316
Talkshow	65	65	641	258	4382832

[그림 5]의 결과와 같이 레벨 1에서는 암호화에 따른 오버헤드가 거의 없었고 레벨 2에서는 I 프레임의 개수에 따란 변동이 있었지만 실시간 서비스가 가능하다. 레벨 3의 겨우는 전체암호화 방법과 속도의 차가 거의 없거나 오히려 높았기 때문에 파일의 크기가 큰 경우는 실시간 서비스가 어렵다



[그림 5] 암호화 속도비교



[그림 6] 암호화 시간/파일크기

[그림 6]에서와 같이 I 프레임의 비율에 따라 레벨2의 암호화의 속도가 다르게 나타나지만 일반적으로 파일의 크기가 클수록 암호화 효과가 높다.

4. 결론

통신기술의 발달로 인하여 인터넷을 통한 서비스가 다양해지고 있다. 특히 멀티미디어 서비스와 같은 대용량 데이터의 전송이 활발해지고 있고 이를 상용화하는 서비스도 시작되었다. 그러나 인터넷의 특성상 이러한 모든 정보들이 전송될 때 인가되지 않은 사용자의 접근이 가능하다. 이를 보

호하기 위해서는 전송데이터의 암호화만이 유일한 대책이다. 본 논문에서는 MPEG-1의 구조에 따른 다단계 암호화 방법을 제안하였다. 데이터의 중요도에 따라 4가지 레벨로 나누어서 부분적으로 암호화를 하는 방법이다. MPEG-1의 특성상 부분정보의 암호화를 통해서도 보안효과를 얻을 수 있었다. 향후의 연구과제로 다양한 암호화 알고리즘의 수용과 MPEG-1이외의 대용량 데이터 처리방법에 대한 연구가 계속되어야 할 것이다. 점점 데이터의 용량이 커지는 추세에 있기 때문에 이와 같이 부분정보의 암호화를 통한 전체 정보의 보안을 만족시키는 방법에 관한 연구가 많이 연구되어야 할 것이다.

참고문헌

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC press, 1997.

[2] Bharat Bhargava, Shunge Li, Shalab Goel and Jin Huai,"A Distributed Video-on-Demand System for Video Conferencing." In Proceedings of the International Conference on Multimedia Information Systems (MULTIMEDIA 96), IETE, pages 83-93, New Delhi, India, Feb., 1996.

[3] C. Shi, B. Bhargava "A Fast MPEG Video Encryptio Algorithm" ACM 98 Electronic proceeding

[4] C. Shi , B. Bargava, "Light-weight MPEG Video Encryption Algorithm" In proc. of Int'lconf. on Multimedia(Multimeda98, Shaping the future) IETE, January, 1998, pages 55-61, New Delhi, India.

[5] Derek Atkins, Paul Buis and et al, "Internet Security." New Riders Publishing, Indianapolis, USA., 1996

[6] Diffe W., "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, May 1998.

[7] Douglas R. Stinson, "Cryptography Theory and Practice." CRC Press, Inc., New York, 1995.

[8] Lei Tang, "Methods for Encrypting and Decrypting MPEG Video 데이타 Efficiently." In Proceedings of the ACM Multimedia96, pages 219-229, Boston, Nov., 1996.

[9] T.D.C. Little and D. Venkatesh, "Prospects for Interactive Video-on-demand." JOURNAL= IEEE, Multimedia, 1(3):14-2, September, 1994.

[10] Willian Stallings, "Cryptography and Network Security : Principles and Practice(Second Edition)", Prentice-Hall, Inc., 1999

[11] Willian Stallingx, "Network and Internetwork Security :Principles and Practice", Prentice-Hall, Inc., 1995

[12] 박재석 "VOD시스템에서 공개키 암호화 알고리즘을 이용한 MPEG비디오 소스의 다단계 암호화 기법" 숭실대학교, 1998

[13] 이승윤, "대화형 비디오 서비스를 위한 효율적인 VBR비디오 전송 기법" 광운대학교, 1999

[14] 한성민, "VOD 시스템의 인증에 관한 연구" 광운대학교, 1999