효율적인 MPEG-4 비디오 파일의 암호화에 관한 연구

김건희° 신동규 신동일
세종대학교 컴퓨터공학과
{ghkim°, shindk, dshin}@sejong.ac.kr

A Study on Efficient Encryption of MPEG-4 Video File

Gunhee Kim0, Dongkyoo Shin, Dongil Shin
Dept. of Computer Science and Engineering, Sejong University

요 약

본 논문에서는 MPEG-4 비디오 포맷으로 인코딩(encoding)된 미디어 데이터에 적용할 수 있는 효과적인 암호화 방법에 대해서 제안하고 실험 결과에 대하여 기술한다. MPEG-4 파일로부터 추출한 I(Intra-coded)-VOP(Video Object Plane)의 매크로 블록(Macroblock)들 중의 최소부분 암호화, P(Predictive-coded)-VOP의 움직임 벡터(Motion Vector)들과 매크로블록들의 최소부분 암호화, 그리고 마지막으로 모든 VOP들의 최소 부분 암호화와 같은 3가지 암호화 방법을 구현하고 실험하였다. 이러한 방법은 모바일 또는 유비쿼터스 환경 하에서의 상용 서비스의 디지털 저작권 관리(Digital Rights Management)를 구축하는 데에 매우 용이하고 적합하게 적용되며, 주문형 비디오 서비스(Video On Demand)와 같은 비디오 스트리밍을 위한 DRM 시스템에 최소한의 부하만을 지우도록 설계되었다. 미디어 데이터의 각 VOP들의 암호화에 소요되는 시간을 측정한 결과, 이러한 방법은 상용 멀티미디어 서비스에도 충분히 적용 가능한 성능을 나타내었다.

1. 서 론

네트워크의 대역폭이 증대될수록, 상업적 멀티미디어 시스템 보안의 중요성은 증가한다. 따라서, 멀티미디어 컨텐츠의 전송을 통한 디지틀 저작권 관리(Digital Rights Management) 기술은 디지털 컨텐츠 제공자에게 가장 중요한 문제 중의 하나로 인식되고 있다. 이러한 기술들로 연구자들은 보호된 멀티미디어 자원의 지적 재산권의 남용을 부당한 크래커들로부터 막을 수 있다[1].

MPEG-4 표준 그 자체에는 데이터 암호화 스킴에 대한 규정은 없다[4]. MPEG-4 인코딩의 고유 특성인 시공간의 연관성 때문에 암호화가 쉽게 적용되지 않는다[2]. MPEG-4의 인코딩은 디코딩보다 더 많은 계산 시간이 소요되므로 비대칭 코딩이라 부른다. MPEG 전송에서 중요한 암호화 방법이 두 가지 있다. 한 가지는 비트스트림의 한 부분을 암호화 하는 것이고[7], 다른 하나는 전체 MPEG 데이터를 암호화하는 것이다[6]. 일반적인 암호화 방법은 MPEG-4 시스템에서 서비스 질 저하와 수행능력감소를 초래한다[8].

본 논문에서는 세 가지 타입의 암호화 방법을 설계하였다. 첫째는 MPEG-4 파일 포맷[5]에서 추출한 I-VOP(Video Object Planes)의 매크로 블록의 시작 8-byte만 암호화 하는 것이며, 암호화 알고리즘에는 DES(Data Encryption Standard)[3]가 사용된다. 두 번째는 첫 번째와 같은 방식으로 P-VOP을 추출하여 매크로 블록의 시작 8-byte를 암호화 하였다. 이 두 가지 방법을 결합하여, 약간의 시간 소비가 더 소요되지만, I-VOP과 P-VOP을 모두 암호화하는 세 번째 방법을 제안하고 실험하였다.

2. 배 경

하나의 장면에서 같은 객체를 가지고 있는 연속적인 VOP들은 비디오 객체(Video Object)로 불린다. MPEG-1과 MPEG-2와 유사하게, I-, P-, B-VOP은 기본적인 VOP의 타입이고, 각각의 VOP은 DCT(Discrete Cosine Transform)가 적용된 매크로블록(Macro Block)으로 분해되고, MB는 6개의 블록으로 구성되어 있는데, 이것은 8*8 픽셀로 이루어진 4개의 휘도(luminance) 블록과 2개의 색상(chrominance) 블록으로 분해된다[5,6].

2.1 전통적인MPEG 비디오 암호화 기법

현재까지 연구된 MPEG 비디오 암호화 기법들은 다음과 같이 크게 대표적으로 5 가지 방식으로 분류될 수 있다.

① 나이브 알고리즘 : DES와 같은 표준 암호화 방법에 의한 전체 MPEG 비트스트림을 암호화 하는데에 사용되는 일반적이고 간단한 알고리즘이다[6]. 평문으로된 MPEG 스트림을 처리하고 있고, MPEG 비트스트림의 구조적 특징

을 살리지 못한다.

② 선택적 알고리즘 : MPEG의 계층화된 구조의 특징들을 이용하는 방법들은 선택적 알고리즘으로 분류된다[7].

③ 지그재그 치환 알고리즘 - 암호화가 지그재그 치환 알고리즘에서 MPEG-4 압축 절차의 필수적인 부분으로 통합된다.

④ 비디오 암호화 알고리즘 - 비디오 암호화 알고리즘은 MPEG의 압축된 비디오 프레임들과 속성의 통계적 분석을 이용하는 대칭적 암호화 시스템이다[8].

⑤ 순수 치환 알고리즘 - 데이터 주파수, 다이어그램 주파수 등을 사용하기 위한 암호화분석의 어려움과 비효율성 때문에, 순수 치환 알고리즘은 간단하게 치환함으로서 바이트 스트림을 뒤섞는다.

위에 기술된 알고리즘들은 비디오 프레임의 인코딩 단계에서 수행되어야만 하는 암호화 기술이다. 따라서 만약 이미 인코딩된 후 보유하고 있는 미디어 데이터를 암호화하기를 원한다면 보유한 미디어 데이터의 디코딩이 먼저 수행되어야하고, 그 후에 암호화와 인코딩을 다시 적용해야 한다.

3. 최저 비용 암호화 기법

MPEG-4 파일 포맷의 구조적 특징을 이용하는 최저 비용 암호화 알고리즘 이라는 새로운 알고리즘을 I-, P-VOP, 그리고 전체 VOP에 대하여 암호화하는 경우로 나누어 구현하였다. 이미 보유하고 있는 인코딩된 MPEG-4 파일의 매우 작은 특정 부분만을 암호화 하더라도, 최저 비용 암호화 알고리즘을 사용하면 비디오 스트림의 실제적인 비주얼 효과는 전체 비트스트림을 암호화하는 나이브 알고리즘과 동일하다. 그러므로 많은 시간, 메모리, 컴퓨팅 파워 등의 자원을 절약할 수 있다.

VOP의 암호화를 위해서 DES(Data Encryption Standard)가 적용되었다. DES는 최소 64비트의 입력 데이터를 받아서 동일한 길이의 데이터를 출력하는 대칭적 암호화 알고리즘이기 때문에 실제적으로 암호화된 MPEG-4 파일과 보유하고 있던 원본 파일은 동일한 크기를 가진다.

3.1 최저 비용 암호화 방법-1

모든 I-VOP은 그림 1의 절차를 통해 생성된다. 이와 같은 과정을 거친 이미 인코딩된 I-VOP의 매크로 블록을 DES를 통하여 전체적으로 암호화할 수 있다. 그러나 각 VOP은 허프만(Huffman) 코딩과 RLE(Run Length Encoding)이 적용되었기 때문에 I-VOP 매크로블록의 시작 8바이트만 암호화하여도 전체 I-VOP 데이터를 시각적으로 망가뜨리기에는 충분하다. 이러한 인코딩된 매크로 블록의 시작점에서의 작은 데이터 변화는 허프만 코딩, RLE, DCT 그리고 양자화(Quantization)가 역으로 적용되는 디코딩 과정에서 전체적으로 큰 왜곡을 유발시킨다. 이렇게 일어난 데이터 왜곡은 플레이 시의 화질 붕괴로 나타난다. 따라서 허가받지 않은 사용자는 비디오 데이터를 습득하더라도 내용을 파악할 수 없게 된다.

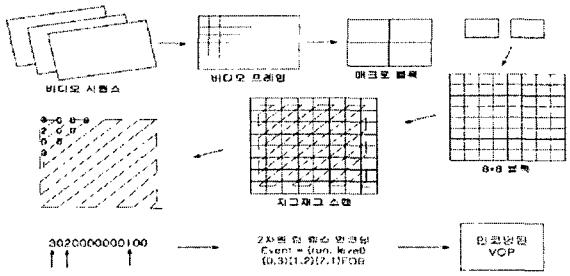

그림 1 I-VOP이 인코딩되는 과정

암호화된 I-VOP을 포함한 비디오는 그림 2의 왼쪽 그림처럼 간간히 깨진 이미지들이 나타나며, 오른쪽에는 원본 비디오 이미지를 보여주고 있다.

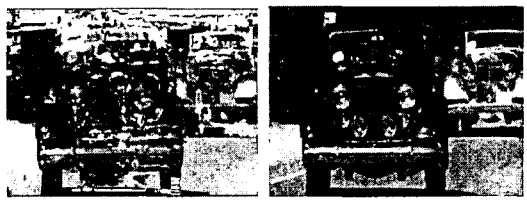

그림 2 암호화된 I-VOP으로 깨어진 장면

3.2 최저 비용 암호화 방법-2

P-VOP은 정확성과 효율성을 위해 I-블록을 포함할 수 있다. 만약 VOP이 암호화 되지 않은 I 블록을 가지고 있다면, 참조 블록을 사용하는 다음 VOP의 블록들은 다음 암호화된 I-VOP까지 정확하게 디코딩 된다. 그림 3는 방법-2를 사용한 암호화 결과를 보여준다.

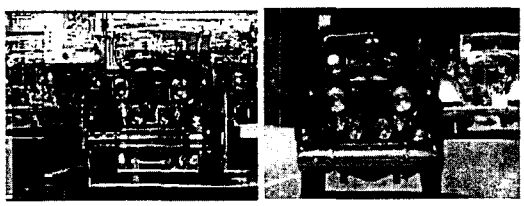

그림 3 암호화된 P-VOP으로 깨어진 장면

3.3 최저 비용 암호화 방법-3

I-VOP과 P-VOP 암호화를 동시에 결합하면 관랑자는 전체 비디오스트림을 거의 볼 수 없게 된다. P-VOP과 I-VOP과 같은 다른 VOP들이 암호화 될 때 B-VOP는 거의 무시될 수 있다. B-VOP은 I-VOP과 P-VOP사이에 위치해 있고, 전후에 위치한 I-,P-VOP에 따라 내용이 달라지기 때문이다. 그림 4는 이러한 3번째 암호화 방법의 결과를 보여준다.

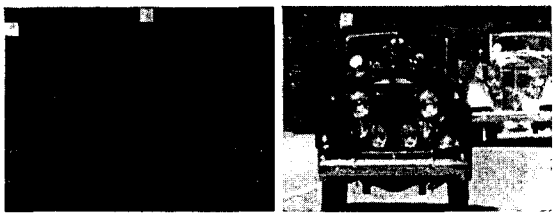

그림 4 암호화된 I-VOP,P-VOP으로 깨어진 장면

4. 성 능

(표 1) 암호화 속도 측정

암호화 범위	전체 VOP의 수	방법	해당 VOP의 수	평균 암호화 시간(second)	전체 암호화 시간(second)
MB의 8바이트	2471	1	160	0.0001516290	0.0242606425
		2	2311	0.0001136825	0.2627203701
		3	2471	0.0001203616	0.2974135023
전체 MB	2471	1	160	0.0005734991	0.0917598600
		2	2311	0.0002804336	0.6480821198
		3	2471	0.0003315408	0.8192373502

표 1은 매크로블럭 전체를 암호화하는 것과 매크로블럭 중의 8바이트만을 암호화하는 시간을 비교한 실험결과를 보여준다. DES 암호화 알고리즘을 사용함으로써, 제안한 3가지 방법을 통한 암호화된 파일의 크기는 원본과 같다. 그러나 암호화된 파일을 복호화 하는 부가적 계산 시간 때문에 원본 파일과 동일한 화면을 재생하기까지에 소요되는 시간은 약간 더 생길 수밖에 없다. MPEG-4 비디오 스트림을 재생할 수 있는 대부분의 클라이언트에서는 재생지연을 해결하기 위한 적절한 버퍼링 공간을 가지고 있어서, 복호화 계산에 필요한 매우 작은 시간 부하는 무시할 수 있을 정도이다.

원본 파일과 암호화된 파일의 동일한 크기 덕분에, 비디오 컨텐츠 제공자들은 어떤 데이터 구조나 보안에 관련된 소프트웨어, 하드웨어 도구들을 바꿀 필요 없이 제안된 방법들을 지원할 수 있다.

5. 결 론

본 논문에서는 DES 알고리즘을 암호화 툴로 이용한 MPEG-4 비디오 데이터 보안 기법인 '최저 비용 암호화 기법'을 제안하였다. VOP의 매크로블럭의 처음 8바이트를 암호화 하는 방법은 MPEG-4 비디오 데이터를 암호화 하는 빠르고 가벼운 기법이다. 방법-1과 방법-2는 각각 MPEG-4 파일 포맷에 포함된 I-VOP, P-VOP을 암호화하는 방법이다. 마지막 방법-3은 가장 높은 품질의 암호화 기법이다. 암호화 처리에 상대적으로 적은 계산 시간이 소요되고, MPEG-4 파일 구조의 재구성을 하지 않아도 되기 때문에, 제안된 기법은 블루투스나 IRDA와 같은 무선 데이터 서비스에 적합하게 사용될 수 있는 적절한 솔루션이다. 또한 변하지 않는 파일 크기와 동일한 구조 때문에, 클라이언트에서 필요한 복호화 처리를 위한 키 분배 도구를 제외하고 암호화된 MPEG-4 파일을 조작하기 위한 어떤 추가 도구도 필요하지 않다.

6. 참 고 문 헌

[1] F. Hartung and F. Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications", IEEE Communications Magazine, 78-84, Nov. 2000.

[2] B. M. Macq and J. J. Quisquater, "Cryptology for Digital TV Broadcasting", Proceedings of the IEEE, Vol 83(6), 944-957, June. 1995.

[3] "Data Encryption Standard (DES)", FIPS PUB 46-3, Oct. 25. 1999.

[4] "Information Technology - Coding of Audio-Visual Objects - Part 2: Visual, ISO/IEC 14496-2", ISO/IEC/SC29/WG11, Nov. 1998.

[5] "Information Technology - Coding of Audio-Visual Objects - Part 1: Systems, ISO/IEC 14496-1:2001", ISO/IEC/SC29/WG11. 2001.

[6] I. Agi and L. Gong, "An Empirical Study of Mpeg Video Transmissions", In Proceedings of the Internet Society Symposium on Network and Distributed System Security, San Diego, 137-144, CA, February. 1996.

[7] T.B. Maples and G.A. Spanos, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video", Proceedings of 4th International Conference on Computer Communications and Networks, Las Vegas, Nevada, September. 1995.

[8] L. Qiao and K. Nahrstedt, "A New Algorithm for MPEG Video Encryption" Proceedings of The First International Conference on Imaging Science, Systems, and Technology (CISST'97), Las Vegas Nevada, 21-29, July. 1997.