암호화된 SVC 비트스트림에서 조건적 접근 제어 방법에 관한 연구

원용근, 배태면, 노용만

한국정보통신대학교 영상시스템 연구실
e-mail : gamja0000@icu.ac.kr

Method for Conditional Access Control in Secured SVC Bitstream

Yong Geun Won, Tae Meon Bae, Yong Man Ro

Image and Video Systems Lab, Information and Communications University

요 약

본 논문에서는 스케일러블 멀티미디어 콘텐츠에 대한 조건적 접근제어가 가능한 암호화 방법을 제안한다. 현재 표준화가 진행중인 스케일러블 비디오 코딩방법인 JSVM(Joint Scalable Video Model)은 부호화한 동영상에 대해 공간, 시간, 품질의 스케일러빌리티(Scalability)를 지원하는데, 각 스케일러빌리티를 고려한 조건적인 접근제어기술은 스케일러빌리티에 따라 사용자를 제한해야 하는 경우를 위해 필수적인 기술이다. 제안하는 방법은 공간, 시간, 품질의 세가지 스케일러빌리티를 지원하도록 부호화(Encoding)후 구성되는 NAL(Network Abstract Layer)을 지원하는 스케일러빌리티에 따라 구분하고, 구분된 NAL 의 종류에 따라 암호화 key 를 다르게 제공하는 방법을 통해 사용자의 접근제어 수준에 맞게 암호화 key 를 조합하는 방법을 적용하였다. 실험 결과 제안한 방법은 JSVM 에서 공간, 시간, 품질의 스케일러빌리티가 보장되고, 이때 생성되는 Key 의 조합으로 조건적 접근제어(Conditional access control)가 가능함을 확인하였다.

1. 서론

MCTF(Motion Compensated Temporal Filtering)와 H.264/MPEG-4 AVC 를 기반으로 비디오 전송시 QoS (Quality of Service)를 보장할 수 있도록 하는 스케일러블 부호화 방법이 ITU-T 와 ISO/IEC 의 JVT(Joint Video Team)에 의해 표준화가 진행 중이며, 현재 스케일러블 비디오 코딩 방법인 JSVM 이 발표되었다[1]. JSVM 으로 만들어지는 공간, 시간, 품질의 스케일러블 부호화 방법은 한번 부호화를 수행한 후 다양한 사용자환경에 맞추어 비디오 스트리밍 서비스를 제공하는 원 소스 멀티 유즈(one source multi-use)를 가능하게 하는 기술이며, 이러한 스트리밍 기반의 서비스는 DRM (Digital Right Management)을 통해 유통되므로 DRM 이 가능한 스케일러블 미디어의 암호화 연구가 필수적이다.[2] 실제로 암호화를 통한 멀티미디어 콘텐츠의 보호에 관해서는 많은 연구가 있어왔지만 스케일러블한 비디오 콘텐츠의 대한 암호화에 대한 연구는 미미한 상태이다. 스케일러블 콘텐츠의 경우, 암호화시 다양한 요구사항이 발생할 수 있다. 먼저 스케일러빌리티를 가지는 콘텐츠에 대해 비트스트림 또한 스케일러블한 특성을 지원하도록 암호화 되어야 한다. 또, 각 사용자에 따른 스케일러빌리티의 접근을 제한해야 할 경우를 위해 단계적으로 복호화가 가능하도록 구성되어야 한다

부호화된 정보에서 특정 부분을 추출함으로써 적합한 스케일러빌리티를 만족하는 콘텐츠를 제공하는 현재의 JSVM 의 경우, 기존의 MPEG 기반의 암호화를 통한 콘텐츠 보호방법을 그대로 적용해서는 위에서 언급한 문제를 해결할 수 없다. 따라서 본 논문에서는

JSVM 의 비트스트림의 특성을 고려한 콘텐츠 암호화 기법을 제안하며, 제안한 방법은 각 사용자의 요구에 따른 조건적 접근 제어가 가능하도록 하여 암호화 후에도 인터넷상에서 원 소스 멀티 유즈의 서비스가 가능하도록 하였다.

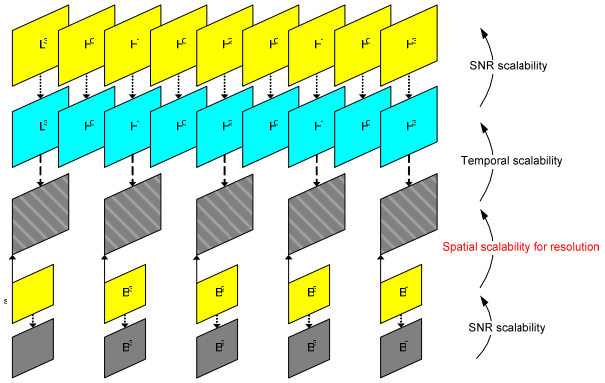
2. 멀티미디어 콘텐츠의 스케일러블 암호화

2.1 멀티미디어 보호기술

멀티미디어의 분배와 보호에 관한 연구는 최근 다양한 분야에서 이루어져 왔다. MPEG(Moving Picture Experts Group)은 IPMP (Intellectual Property Management and Protection)라는 DRM 프레임워크를 MPEG-2 와 MPEG-4 에 적용하였다. IPMP 에서는 다양한 DRM 표준의 상호호환(interoperability)를 위해 IPMP 기술자(IPMP-DS)와 IPMP 기본스트림(IPMP-ES)으로 IPMP 시스템과 MPEG 단말간의 통신을 통해 비디오 콘텐츠의 보호 및 관리의 인터페이스를 구성하여 콘텐츠에 대한 보안을 제공한다[3]. JPEG2000 에서도 part 8 의 JPSEC 에서 이미지 콘텐츠 보호에 대한 표준화 작업을 완료했다. JPSEC 에서는 보안에 대한 서비스와 그 서비스를 실현하는 Tool 들을 정의하고, 이 Tools 로 이미지 비트스트림에 대한 암호화 서비스 구현에 대한 프레임워크를 제공한다[4].

2.2 MCTF 와 H.263 확장기반 스케일러블 부호화

스케일러블 부호화는 부호화된 콘텐츠를 재 부호화 없이 비트스트림의 추출(Extraction) 만으로 다양한 버전의 콘텐츠를 생성하여 개별 단말에 적응 시킬 수 있도록 한다. 이러한 스케일러블 콘텐츠는 단말과 네트워크에 우수한 적응성으로 크게 각광받고 있으며, 현재 JPEG2000, MPEG-4 FGS, SVC 등에서 스케일러블 콘텐츠 부호화에 대한 연구가 이루어 지고 있다. MPEG 에서 논의중인 JSVM 은 (그림 1) 에서와 같이 공간, 시간, 품질의 방향으로 스케일러빌리티를 제공한다 JSVM 에서는 계층적인 부호화를 통해 공간해상도를 지원하고 있으며, MCTF 를 통해 시간적 스케일러빌리티를 지원한다. 영상화질의 경우, FGS (Fine Granular Scalability)와 CGS(Course Granular Scalability)를 통해 스케일러빌리티를 지원하고 있다[1].

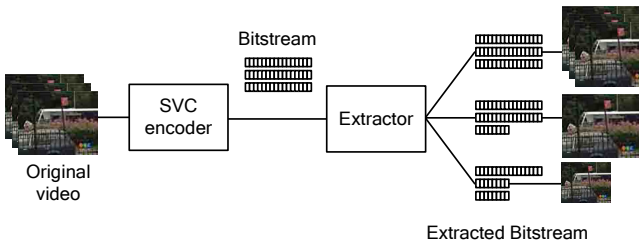


(그림 1) 공간, 시간, 품질의 스케일러빌리티를 제공하는 SVC 비트스트림 구조

NAL 단위는 H.264/ AVC 에서 부호화된 콘텐츠가 네트워크에 적응되도록 미리 일정단위로 부호화 하는 것이며 H.264/AVC 를 기반으로 하는 JSVM 에서도 비트스트림의 기본단위로 사용된다. 이는 콘텐츠에 맞추어 미리 적절한 단위로 콘텐츠를 분할 하는 것이며 이러한 NAL 단위는 콘텐츠의 특정 단위로 만들어 지므로 오류복원과 패킷화에 유리하다[5].

2.3 접근제어를 위한 기술

인증 없이 콘텐츠에 접근을 금지하거나 특정 서비스에 따라 콘텐츠의 부분적 접근만을 허용하는 조건적 접근제어 기술은 다양한 서비스 모델을 만들어 왔다. 예를 들어 콘텐츠 배포자는 낮은 품질 수준의 콘텐츠를 무료로 배포하고 높은 품질 수준의 콘텐츠를 요구할 시에 과금을 하도록 하는 것을 생각할 수 있다. 특히 비트스트림의 추출(Extraction)만으로 다양한 버전의 비디오 콘텐츠를 생성할 수 있다는 스케일러블 부호화의 특징 때문에 스케일러블 코딩 기술에 있어 조건적 접근 제어는 크게 주목 받고 있다.



(그림 2) SVC 에서 비트스트림 추출을 통한 이종단말에 적응되는 과정

조건적 접근제어가 시도되었던 대표적인 스케일러블 코딩 기술은 MPEG-4 FGS 와 JPEG2000 이 있다. MPEG-4 FGS 에서는 스케일러블 다층 FGS 암호화 (scalable multilayer FGS encryption)를 통해 품질에 대한 조건적 접근제어를 시도하였고[6], JPSEC 에서는 컴포넌트, 이미지크기, 품질, 타일 등 JPEG2000 에서 제공하는 스케일러블 요소의 조건적 접근 제어를 위해 패킷 단위의 암호화, 조건적 접근제어를 위한 비트스트림 구성 등이 연구되었다[4][7][8].

스케일러블 미디어의 조건적 접근 제어를 위한 암호화에 있어 비트스트림을 구성하는 것이다. 실제로 JPSEC 에서는 조건적 접근제어를 위해 패킷 단위로 암호화를 시행하는데 이들 패킷들은 JPEG2000 이 고품질(이미지크기, 품질, 타일 등)의 영역으로 확장되기 쉽게 구성될 수 있다.[9][10]]

2.4 비디오 암호화 알고리즘(Video Encryption algorithm)

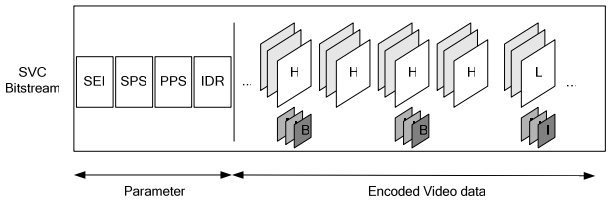
콘텐츠의 암호화에는 다양한 알고리즘이 제안되고 있으며, Naïve algorithm, selective encryption, Scrambling algorithm 등이 대표적인 방법이다. 먼저 Naïve algorithm 은 압축된 비디오 스트림의 데이터 또는 헤

더의 전체 또는 일부분을 텍스트 데이터의 암호화 기법과 같은 방법으로 DES(Data Encryption Standard)나 AES(Advanced Encryption Standard)와 같은 일반적인 암호화 기법을 사용하여 암호화하는 방법이며 선택적 암호화(selective encryption)방법은 암호화에 있어 압축된 비디오를 I 프레임이나 I 블록, 모션 벡터등의 컨텐츠에 대한 특정 중요한 부분만을 암호화하는 방법이다. 스크램블링 알고리즘(Scrambling algorithm)은 일반적인 암호화 알고리즘을 사용하지 않고 부호화 시의 파라미터를 숨기거나 부화화 파라미터 값을 특별한 방법으로 치환하여 데이터를 은닉하는 방법이다.[6][7][11][12].

3. JSVM 비트스트림을 고려한 조건적 접근을 위한 스케일러블 암호화

3.1 스케일러빌리티를 고려한 NAL 의 구분 및 암호화

JSVM 의 스케일러블 특성을 보존하며 효과적으로 암호화 하기 위해서는 스케일러블 특성을 제공할 수 있는 NAL 단위로 암호하는 것이 콘텐츠의 스케일러블 특성을 보존하기에 적합하다.



(그림 3) NAL 로 구성된 SVC 비트스트림

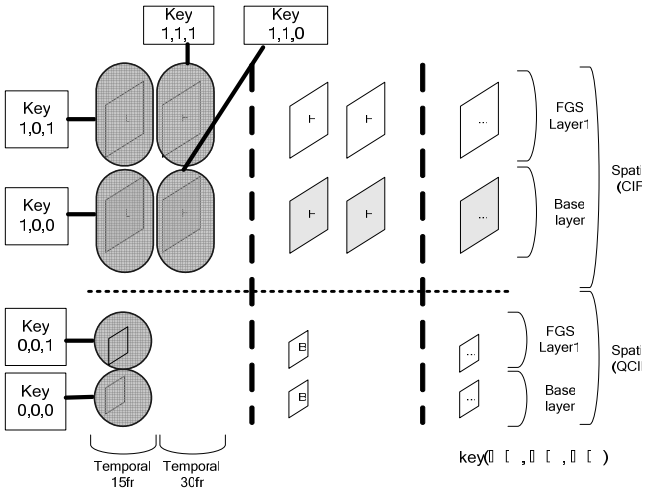
(그림 3)은 공간, 시간, 품질의 스케일러빌리티를 제공하는 SVC 의 비트스트림이 NAL 로 구성되었음을 보여주고 있다. 기본적인 NAL 구성은 한 프레임의 공간, 시간, 품질이 확장되는 요소마다 하나씩 구성된다. 따라서 각 NAL 단위는 공간, 시간, 품질의 스케일러빌리티를 제공하는 기본단위가 되며 NAL 단위 암호화는 접근제어를 위한 암호화를 제공할 수있다

암호화 알고리즘의 적용에 있어서는 암호화 속도와 코덱에 호환성의 측면에서 생각할수 있다. 일반적으로 큰 데이터를 가진 비디오 컨텐츠는 실시간 전송(Real time video delivery)측면에서 암호화 속도가 큰 문제가 된다. 실제로 DES 나 AES 는 속도측면에서 실시간 전송에 적합하지 못하며 이러한 문제에 대해 경량암호화(light-weight encryption)라 불리는 빠른 속도를 위한 스크램블 기법의 연구가 이루어 지고 있다.[13] 스크램블 기법은 비디오나 이미지의 부호화 과정에서 만들어진 값들을 코덱의 형식에 맞게 변형 또는 치환하기 때문에 코덱의 호환성 문제에 있어서도 유리하다. 암호화된 비트스트림의 코덱의 호환성은 암호화 시스템의 구성과 다양한 서비스 모델에 있어 넓은 적용성을 가질수 있다.

본 논문에서는 JPSEC 에서 사용된 스크램블 기법인 비트스트림의 부호(sign)을 랜덤하게 반전시키는 (Pseudo-random invese)기법을 적용하여 비디오 컨텐츠의 텍스쳐 계수값에 잡음을 넣는 암호화 기법을 적용하였다.[7]

3.2 암호화를 통한 key 생성 및 접근

특정 스케일러블 방향으로 비디오 콘텐츠를 확장시키기 위해서는 확장에 기여하는 모든 NAL 단위들이 같은 key 로 암호화 되어야 한다. 예를 들어 QCIF 를 CIF 로 확장시키고자 한다면 비디오 콘텐츠의 모든 프레임에서 CIF 확장에 기여하는 부분이 같은 key 로 암호화 되어야 하는데 하나의 key 로써 CIF 공간의 확장에 기여하는 NAL 들을 모두 복호화 할 수 있기 때문이다.



(그림 4) NAL 단위 암호화를 통한 Key 생성

(그림 4)는 30, 15 의 프레임율과 QCIF, CIF 의 공간해상도, 각 공간해상도별로 하나의 품질 확장에 기여하는 FGS 레이어를 포함하는 비디오이다. Key(*t,s,q*)는 *t* 시간, *s* 공간, *q* 품질 계층의 암호화 된 NAL 을 복호화 하는데 사용되는 key 를 의미한다. 위의 비디오는 6 개의 NAL 을 가진, 스케일러빌리티를 제공하는 최소단위의 반복으로 생각할 수 있다. 즉, *Key(0,0,0)*은 QCIF 공간영역의 15 프레임의 시간영역의 base layer 의 품질영역을 복호화 하는데 사용된다. 만일 사용자가 품질의 향상을 요구한다면 QCIF 공간의 품질 향상 계층을 암호화한 *Key(0,0,1)*가 필요하다.

따라서 N 공간영역과 N 공간영역에 따른 n_q 품질영역, N 공간영역에 따른 n_t 시간영역을 가진 스케일러블 비디오의 암호화에 사용되는 key 의 총 개수 Key_{total} 은 식(1)과 같다.

$$Key_{total} = \sum_{n=0}^{N-1} n_q * n_t \qquad \text{(식 1)}$$

여기서 N 은 공간(spatial) 영역의 스케일러블 계층 수, n_q 은 n 번째 공간영역의 품질(FGS) 계층 수, 그리

고 n_t 는 n 번째 공간영역의 시간(temporal) 계층 수를 나타낸다. 특정 s 공간영역, q 품질영역, t 시간 영역에 접근 하기 위해 필요한 NAL 은 $NAL(i,j,k)$ 로 표현 할 수 있는데 i 번째 공간계층과 i 번째 공간계층에 따른 j 번째 품질계층, i 번째 공간계층에 따른 t 번째 시간 계층을 나타내며, 각 NAL 은 암호화에 사용된 *key(i, j, k)* 와 대응된다. (그림 4)에서는 *key*(*i, j, k*)가 여섯 개이고, 각 NAL 은 6 개의 Key 중 하나로 암호화 되므로, 한 비트스트림에서 추출을 통해 만들어진 비디오들은 NAL 의 조합으로 표현할수 있고 또한 *key*(*i ,j, k*)의 조합으로 복호화 할 수 있다

공간, 시간, 품질에서 각기 필요한 key 의 종류와 수는 식 2 를 통해 표 1 에서 보여진다.

<표 1> 추출을 통해 생성된 비디오에 접근하기 위해 필요한 key

Spatial	Quailty	15 fps	30 fps
QCIF	Base	{*k(0,0,0)*}	Not exist
	FGS	{*key(0,0,0),key(0,0,1)*}	Not exist
CIF	Base	{*key(0,0,0),key(0,0,1) key (1,0,0)* }	{*key(0,0,0),key(0,0,1) Key(1,0,0),key(1,1,0)*}
	FGS	{*key (0,0,0),k(0,0,1) key (1,0,0),key(1,0,1)*}	{*key(0,0,0),key(0,0,1) key(1,0,0),key(1,0,1) key(1,1,1),key(1,1,0)*}

<표 1>에서는 계층적으로 암호화 된 비디오들의 복호화시 key 들의 조합이 필요함을 보여주고 있다.

4. 실험 및 분석

제안한 방법의 유효성을 확인하기 위해 JSVM ver. 2.0 을 이용하여 부호화 된 비트스트림에 NAL 단위로 암호화를 수행하였다. 실험에 사용된 비디오는 "bus" SVC 테스트 영상이다. 테스트에 사용된 비트스트림은 QCIF 와 CIF 의 2 개의 spatial layer 를 가지고 있으며 QCIF 는 base layer 로써 hierarchical B picture 구조로 15fps 로 부호화된다. CIF 의 경우, 30fps 의 동영상을 2 temporal level 로 구성하여 부호화하였고 QCIF, CIF 각각에 대해 1 개씩의 FGS layer 를 두어 품질에 대한 스케일러빌리티를 지원하도록 하였다. 암호화 방법은 비트스트림에서 데이터의 레지듀얼(Residual) 에 대한 계수값의 부호를 랜덤하게 반전시키는 스크램블링 방법(Pseudo-random inverse)[7]을 사용하여 효과적으로 잡음을 삽입하였고, 적절한 key 없이 복호화시에는 암호된 영상이 나타나도록 하였다.

실험은 <표 1>의 NAL 의 구분에 따라 각각 할당된 key 를 통해 암호화를 수행하고, 각 접근제어 수준에 맞게 비트스트림을 추출하는 과정을 거친다. 추출된 비트스트림과 임의로 할당된 key 에 따라서 복호화가 가능한지의 접근 여부를 실험을 하였다

<표 2> 암호화 된 영역에 접근하기 위한 key 할당과 접근여부

접근제어조건	Key 할당	접근가능 여부
CIF , 30fps, FGS	*{key(0,0,0),key(0,0,1) key(0,1,0),key(0,1,1) key(1,1,1),}*	접근 불가
CIF 15fps, Base	*{key(0,0,0),key(0,0,1) key(0,1,0),key(0,1,1)}*	접근 가능
Qcif ,15 fps FGS	*{key(0,0,0),key(0,0,1)}*	접근 불가

<표 2>는 특정 추출을 통해 생성된 비디오 접근하기 위해서는 특정 key 의 조합이 필요함을 보여준다.

5. 결론

본 연구에서는 멀티미디어의 부호화뿐 아니라 암호화 시에도 스케일러빌리티를 제공하기 위해 NAL 단위의 암호화를 시행하였다. 스케일러빌리티를 제공하는 최소단위의 NAL 을 개별적으로 암호화 한다면 암호화 후에도 충분히 스케일러빌리티를 제공할 수 있음을 실험을 통하여 보여주었다. 이때 생성된 Key 들은 특정 수준에 접근이 필요할 시 적절히 조합될 필요가 있으며 Key 생성과 관리에 관계된 새로운 기술이 적용될 필요가 있다. 이러한 NAL 단위 암호화는 스케일러블 코딩 시스템의 구성시 암호화된 비트스트림 추출 과정에도 쉽게 적용 가능하다.

Acknowledgements

본 논문은 삼성전자의 차세대 복합 멀티 미디어 보호 및 관리기술 연구 과제에 의해 지원 되었음.

참고문헌

[1] ISO/IEC JTC 1/SC 29/WG 11 N 7311"Joint Scalable Video Model (JSVM) 3.0"

[2] Bin B. Zhu, Mitchell D. Swanson, Shipeng Li "Encryption and Authentication for Scalable Multimedia- Current State of the art and challenges"

[3] ISO/IEC JTC 1/SC 29/WG 11 14496-13 :2004(E), Information Technology – Coding of Audio-Visual Object – Part13: Intellectual Property Management and Protection (IPMP) Extensions, 2004.

[4] ISO/IEC JTC1/SC29/WG1 N 3480 "JPSEC Final Committee Draft - Version 1.0"

[5] ISO/IEC FDIS 14496-10: Information Technology – Coding of audio-visual objects – Part 10: Advanced Video Coding

[6] Bin B. Zhu, Chun Tuan, Yidong Wang, and Shipeng Li. "Scalable Protection for MPEG-4 Fine Granularity Scalability"

[7] Rapha¨el Grosbois, Pierre Gerbelot and Touradj Ebrahimi "Authentication and access control in the JPEG2000 compressed domain"

[8] Eobert H. Deng, Yongdong Wu, Di Ma "Securing JPEG2000 Code-Stream"

[9] Hongjun Wo, Di Ma "Effeicent and Secure encryption scheme for JPEG2000"

[10] Susie J. Wee and John G.Apostolopoulos "secure scalable streaming enabling transcoding without decryption"

[11] I.Agi and L. Gong "An empirical study of secure MPEG video transmissions"

[12] L. Qiao, K.Nahrstedt"A new algorithm for MPEG video encryption"

[13] Jiangtao Wen, Michael Severa, Wenjun Zeng, Maximilian H.Luttrell, Weiyin Jin "A Format-Compliant Configurable Encryption Framework for Access Control of Video"