제25회 한국정보처리학회 춘계학술발표대회 논문집 제13권 제1호 (2006. 5)

Scalable Video Coding 에서의 조건적 접근제어를 위한 키 관리 기법

원용근, 배태면, 노용만

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

Key Management Scheme for Conditional Access Control in Scalable Video Coding

Yong Geun Won, Tae Meon Bae, Yong Man Ro

Image and Video Systems Lab, Information and Communications University

요 약

본 논문에서는 암호화된 Scalable Video Coding (SVC) 비트스트림에서의 조건적 접근제어을 위한 키 관리 기법을 제안한다. 스케일러블 비디오 코딩 기술은 한번 인코딩 후 비트스트림 추출을 통해 다양한 확장성(scalabbility)을 가지는 비디오를 생성 할 수 있는 기술로 확장하는 단위마다 다른 키로 암호화 하여 조건적 접근제어를 구성 할 수 있다. 그러나 기존의 조건적 접근제어 기술은 암호화 시 복수의 키가 필요하며 이는 키의 관리와 분배에 어려움을 준다. 이러한 문제를 해결하기 위해 본 논문에서는 기존의 스케일러블 코딩기법에서 조건적 접근제어를 위한 키 관리기법을 살펴보고 SVC 의 확장 구조에 맞는 키 관리 기법을 제안한다. 제안한 방법은 SVC 를 이용한 스트리밍 테스트베드에서 구현되어, 조건적 접근제어를 위한 키 관리기능의 유용성을 확인하였다.

1. 서론

현재 고성능 단말기와 다양한 네트워크 환경은 다양한 사용자 환경을 가져다 주었고 이러한 다양한 사용자 환경으로 인해 멀티미디어 콘텐츠의 적응변환은 주요한 문제가 되었다. 기존의 비-스케일러블 코딩 기술은 사용자 환경에 따른 적응변환 시 매번 재 인코딩이 필요했고 이 때문에 적응변환이 용이한 새로운 코딩기술을 요구하게 되었다. 새로운 스케일러블 코딩 기술은 한번의 인코딩 후 비트스트림 추출만으로 다양한 사용자 환경에 쉽게 적응시킬 수 있고 적응서버에 거의 부담을 주지 않기 때문에 현재 많은 기대를 받고 있는 코딩 기술이다.

스케일러블 콘텐츠의 용이한 적응변환은 스케일러블 콘텐츠가 기본레이어를 바탕으로 높은 품질로 확장하는 확장구조에 기인하며 이때 상위레이어가 절삭되어도 하위레이어 만으로 디코딩이 가능하기 때문에 특정 비트율에 맞도록 상위레이어를 절삭하여 전송함으로 적응변환을 제공할 수 있다.

스케일러블 콘텐츠는 비트스트림에서 확장의 단위로 구분하고 확장하는 부분을 다른 키로 암호화 하여 사용자가 확장하고자 하는 부분만 복호화 할 수 있도록 키의 조합을 제공함으로 조건적 접근제어를 구성할 수 있다.[1] 이때 조건적 접근제어를 위해서는 사용자에게 복수의 키를 전송해야 하는데 스케일러블 코딩 기술이 제공하는 확장성(Scalability)과 해당 확장성에 해당하는 레이어가 많이 설정된다면 암/복호화에 사용될 키의 개수가 늘어나게 되므로 사용자 단말과 키 서버단에 복잡도를 유발할 수 있다.[2]

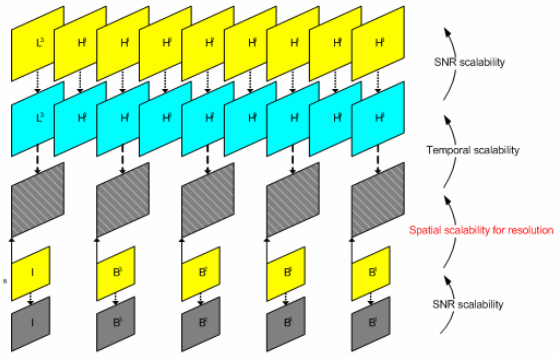
본 논문에서는 SVC 조건적 접근제어 방법에 대한 기존의 연구를 바탕으로 하나의 “Master Key” 에서 각 확장성에 대한 레이어의 암/복호화에 사용될 키를 생성하는 방법을 제안한다. 제안하는 방법은 SVC 의 확

장 구조에 적합하므로 SVC 비트스트림에서 조건적 접근제어 시 효과적으로 적용 가능하다.

2. 관련연구

2.1 스케일러블 코딩 기술 (Scalable video coding)

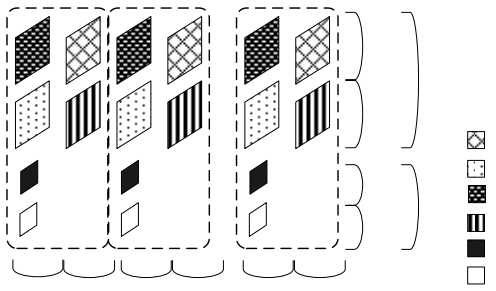
스케일러블 코딩기술은 부호화된 콘텐츠를 재 부호화 없이 비트스트림의 추출(Extraction) 만으로 다양한 버전의 콘텐츠를 생성하여 개별 단말에 적응 시킬 수 있도록 한다. 현재 스케일러블 비디오 코딩 기술인 SVC 가 MPEG 에서 활발하게 논의 중인데 SVC 는 H.264/AVC 를 기반으로 우수한 코딩 효율을 보장하면서도 시간,공간,품질의 확장성을 제공하기 때문에 현재 가장 크게 기대 받고 있는 코딩 기술이다.[3] (그림 1)은 SVC 비트스트림이 기본레이어를 바탕으로 시간, 공간, 품질 확장성으로 확장하는 구조를 보여주고 있다.



(그림 1) 공간, 시간, 품질의 확장성(scalability)을 제공하는 SVC 비트스트림 구조

2.2 암호화된 SVC 비트스트림을 이용한 조건적 접근 제어 방법

SVC 에서 다양한 비디오를 생성하는 방법은 확장단위에 따라 다른 키를 할당하여 암호화 하는 것이다. SVC 에서 확장 단위는 NAL 단위가 되고 각 NAL 은 고유한 확장정보를 가지고 있다. 따라서 고유한 확장정보를 가진 NAL 들을 같은키로 암호화 하여 조건적 접근제어를 구성할수 있다. (그림 2)는 SVC 에서 조건적 접근제어를 위해 동일한 확장정보를 가진 NAL 을 동일한 키로 암호화한 그림이다. 이때 점선은 기본레이어가 확장할수 있는 범위를 보여주고 있으며 점선 내의 모든 NAL 들은 다른 키로 암호화 된다.[1]



(그림 2) 조건적 접근제어를 위한 SVC 비트스트림의 암호화

2.3 기존의 스케일러블 멀티미디어에서의 키 관리 기법

스케일러블 콘텐츠는 제공하는 확장성을 의미하는 타입과 각 타입이 몇 개로 분할된 레이어로 구성된다. 스케일러블 콘텐츠의 특정 레이어에 접근에 있어서는 높은 레이어의 접근을 위해서는 그보다 낮은 레이어에 접근이 허용되어야 하지만 낮은 레이어에서 그보다 높은 레이어로의 접근은 금지되어야 한다. 이러한 스케일러블 비트스트림에서의 접근 특징을 고려하여 기존의 연구에서는 Scalable Layered Access Control(SLAC)라는 프레임워크를 통해 스케일러블 콘텐츠에 대한 계층적인 접근과 각 계층에 대한 효과적인 키 생성 및 할당을 보여주었다.[4] SLAC 방법은 일반적인 스케일러블 콘텐츠의 타입과 레이어에 따른 키 관리와 접근의 방법에 대해 설명한다.

스케일러블 콘텐츠의 키 관리방법을 설명하기 위해 먼저 용어를 정의한다.

n	확장 가능한 타입의 갯수
n_j	j 번째 타입의 레이어 수
$L_{i,j}$	j 번째 타입의 i 번째 레이어
K	"Master Key" 모든 비트스트림으로 접근할수 있는 키
$K_{i,j}$	"레이어 키" j 번째 타입의 i 번째 레이어에 접근할수 있는 키
K_j	"타입 키" j 번째 타입의 가장 높은 레이어를 암호화 하는데 사용되는 키
a‖b	결합연산자, 코드 a 와 코드 b 의 결합에사용됨
$H(x)$	x 에 대한 암호학적 해쉬 코드

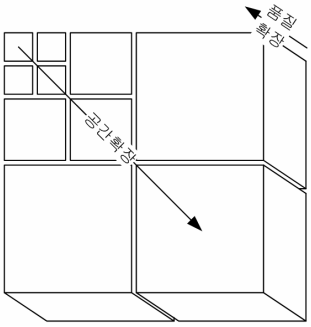
높은 접근 레이어는 곧 그보다 낮은 레이어에 대한 접근이 허용됨을 의미하는데 예를 들어 레이어 $L_{a,j}$ 는 동일한 타입인 j 의 레이어 a 보다 낮은 모든 레이어 $\{L_{i,j} | i < a\}$ 에 접근 가능하다. 타입 j 의 타입키인 K_j 는 "Master Key"인 K 와 타입에 따라 (식 1)에 의해 생성된다. (식 1)은 마스터키로 타입 키를 발생시키는 식이다. 이때 "‖"는 결합연산자 이며 두 값을 결합하는데 사용되는데 실제로 결합 시에는 두 코드 사이에 구분자를 두어서 이후 복원이 가능하도록 하고 있다. $H(x)$ 는 x 에 대한 암호학적 해쉬함수로 일방향 특성을 가지고 있기 때문에 출력값으로 입력값을 예측하기 불가능한 특성을 가진다. (식 1) 을 통해 생성된 타입키 K_j 는 레이어 키를 생성하는데 사용되며 레이어 키는 (식 2)에서 보듯이 레이어수 n_j 만큼 해쉬함수의 반복을 통해서 발생된다.

$$K_j = H(K \| j) \qquad \text{(식 1)}$$

$$K_{i,j} = H(K_{i+1,j}) = H^{n_j+1-i}(K_{n_{i+1},j}), 1 \le i \le n_j \quad \text{(식 2)}$$

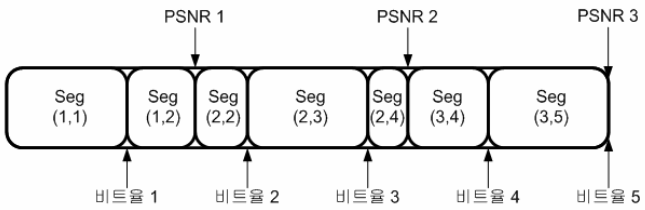
(식 1)과 (식 2)에서 보듯이 SLAC 방법은 "Master Key" K 를 통해 각 타입에 대한 타입 키를 발생시키고 각 타입 키를 통해 타입내의 레이어에 대한 레이어 키를 순차적으로 발생시키는데 레이어 키의 발생시에는 암호학적 해쉬 함수를 사용하여 발생시키므로 해당 레이어 키로 하위 레이어 키를 생성 가능하나 상위레이어 키를 생성이 불가능하므로 접근권한 이상의 접근을 차단할수 있다.

(그림 3)은 JPEG2000 에서 공간, 품질 타입과 각 레이어를 보여주는 그림이다. JPEG2000 의 공간(j=1), 품질(j=2) 두 가지 타입에 SLAC 방법을 적용한다면 공간 품질의 레이어는 서로 상관성이 없기 때문에 위의 방법을 그대로 적용할 수 있고 하나의 Master Key 로 두 개의 타입 키와 $n_1 \times n_2$ 개의 레이어 키를 생성할 수 있다.[4] 따라서 해당레이어에 생성한 해당 키를 할당 하는 것으로 조건적 접근제어를 구성할 수 있다.



(그림 3) JPEG2000 에서 웨이브렛 기반의 공간확장 및 비트플레인 기반의 품질확장

MPEG-4 FGS 는 PSNR(j=1) 과 프레임율(j=2)의 두 가지 타입을 가지고 있고 SLAC 방법을 통해 키를 발생시키면 두 개의 타입 키와 $n_1 \times n_2$ 개의 레이어 키가 발생한다. 이때 PSNR 과 프레임율은 서로 중첩되기 때문에 중첩되는 영역으로 분할 하고 분할된 영역은 해당 PSNR 과 비트율에 해당하는 두 개의 키를 결합하여 암호화 한다. (그림 4)는 비트율과 PSNR 로 구분한 MPEG-4 FGS 비트스트림이며 두 타입의 중첩영역은 Seg (PSNR, 비트율) 로 표시하고 있다. 그림의 예에서 Seg (2,3)에 접근하기 위해 필요한 키는 $K_{seg(2,3)} = K_{2,1} \| K_{3,2}$ 으로 표시할 수 있다. [5] 복호화시에는 다시 키를 분리하고 분리된 키의 해쉬값을통해서 하위 중첩영역을 복호화 할수 있다.



(그림 4) MPEG-4 FGS 에서 PSNR 과 비트율의 중첩영역으로 분할

이때 생성되는 키의 개수는 $n_1 \times n_2$ 가 되지만 실제로 사용되는 키는 $n_1 + n_2 + 1$ 개가 되고 두 개의 키는 타입키 이므로 암호화에 사용되는 키는 $n_1 + n_2 - 1$ 개가 된다.

3. 제안하는 키 생성 기법

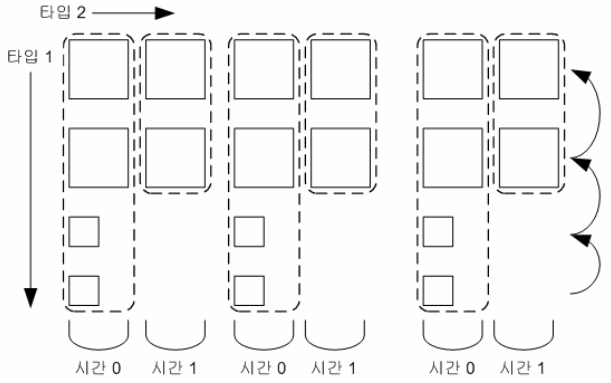
SVC 는 시간, 공간, 품질의 확장성을 가지고 있으므로 세 개의 타입 키를 발생시킬 수 있고 각 타입이 가지는 레이어의 개수만큼의 레이어 키를 발생시킬 수 있다. 즉, 시간 공간 품질에 각각 l, m, n 개씩의 레이어가 있다면 $l \times m \times n$ 개의 키가 발생 하게 된다.

SVC 에 적용하는 방법으로 MPEG-4 FGS 에서와 같이 생성한 키를 결합하여 직접 적용하는 방법을 생각할 수 있다. SVC 의 모든 확장레이어는 공간(j=1), 시간(j=2), 품질(j=3)의 확장성을 가지고 있으므로 특정 공간 a, 시간 b, 품질 c 에 접근하는데 필요한 키는 $K(a,\mathrm{b},\mathrm{c}) = K_{a,1} \| K_{b,2} \| K_{c,3}$ 로 생성할 수 있다. 생성된 키로 암호화를 하면 계산된 하나의 키를 전송함으로 하위레이어를 모두 복호화 할수 있다. 예를들어 (그림 2)에서 공간 1, 시간 0, 품질 1 로 접근하고자 할 때 기존의 방법으로는 Key(0,0,0), Key(0,0,1), Key(1,0,0), Key(1,0,1)의 4 개의 키가 필요했으나 SLAC 방법은 Key(1,0,1)만 전송해서 (식 3)에 의해 각 타입키로 분리시키고 분리된 키에서 하위키를 발생시켜 하위키의 조합으로 복호화에 필요한 4 개의 키를 생성할 수 있다.

그러나 이러한 방법은 SVC 의 품질확장레이어의 확장 특성을 반영하지 못한다. 즉, SVC 는 공간 확장을 위해 하위 공간영역의 모든 품질 레이어가 필요하므로 (그림 2)에서 기본레이어(하위공간레이어)와 공간확장레이어의 복호키인 Key(0,0,0)과 Key(1,0,0) 뿐 아니라 하위공간 레이어의 모든 품질레이어에 해당하는 복호키인 K(0,0,1)도 필요하다.

따라서 SVC 코딩 기법의 확장특성을 고려한 새로운 키 생성 기법이 필요하다. (그림 5)는 SVC 확장기법에 따른 제안하는 키 생성 기법을 표현하고 있다. 제안하는 방법은 SVC 의 공간, 시간, 품질의 세 가지 타입을 공간 시간 의 두 가지 타입으로 생각하고 품질 확장레이어를 공간과 시간의 타입에 종속된 레이어로 생각하여 키를 생성하는 방법이다.

<표 1>에서 key(a,b,c)는 공간 a, 시간 b, 품질 c 에 접근하기 위해 필요한 키 이며 접근에 필요한 키 들은 서로 연관성을 가지고 있지 않고 임의로 생성한 값이다. <표 2>에서 $K_1(a,c) \| K_2(b)$ 는 공간 a, 시간 b, 품질 c 에 접근하기 위해 필요한 키이며 높은 레이어가 낮은 레이어를 생성할 수 있다.



(그림 5) SVC 키 생성을 위해 세 개의 타입을 두 개의 타입으로 두고 키를 생성하는 그림

<표 1>은 키 생성기법을 사용하지 않고 조건적 접근제어를 구성한 표이며 <표 2>는 키 생성기법을 사용하여 조건적 접근제어를 구성한 표이다. 키 생성기법을 사용하지 않을 시 1~6 개까지 키가 전송되고 키 생성기법을 사용할 시 결합된 1 개의 키만으로 조건적 접근제어를 구성할 수 있다.

<표 1> 키 생성 기법을 사용하지 않는 경우 접근에 필요한 키

Spatial	Quailty	15 fps	30 fps
QCIF	Base	{*key(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 2> 제안하는 키 생성기법을 사용할 경우 접근에 필요한 키

Spatial	Quailty	15 fps	30 fps
QCIF	Base	$K_1(0,0) \| K_2(0)$	Not exist
	FGS	$K_1(0,1) \| K_2(0)$	Not exist
CIF	Base	$K_1(1,0) \| K_2(0)$	$K_1(1,0) \| K_2(1)$
	FGS	$K_1(1,1) \| K_2(0)$	$K_1(1,1) \| K_2(1)$

4. 실험 및 분석

제안하는 방법의 유효성을 검증하기 위해 SVC 코딩기법으로 인코딩 된 콘텐츠에 대해 제안하는 방법으로 키를 생성한 후 암/복호화를 시도하였다. 인코딩은 QCIF 와 CIF 의 2 개의 공간 레이어를 가지고 있으며 QCIF 는 base layer 로써 hierarchical B picture 구조로 15fps 로 부호화된다. CIF 의 경우, 30fps 의 동영상을 2 시간 레벨로 구성하여 부호화하였고 QCIF, CIF 각각에 대해 1 개씩의 FGS 레이어를 두어 품질에 대한 확장성을 지원하도록 하였다.

실험 방법은 SVC 로 인코딩된 비트스트림을 SLAC 방법과 제안하는 방법의 두 가지 방법으로 키를 생성하여 각 확장단위마다 암호화하였고 설정된 접근조건에 따라 비트스트림 추출된 암호화된 비트스트림과 해당하는 접근키를 테스트베드 송신단에서 송신하였다. 수신단에서는 접근키를 계산하여 복호키를 생성하고 비트스트림을 복호화 시도 하였다.

<표 3>과 <표 4>는 각각 SLAC 방법과 제안하는 방법으로 접근키를 계산하고 접근키로 레이어키를 추출하여 해당 접근조건에 대해 복호화를 시도한 실험 결과이다. 실제 필요한 키는 <표 1>과 같으며 표에서 보듯이 SLAC 방법으로는 공간 확장 시(QCIF 에서 CIF 로 확장) 품질확장 복호 키를 추출할 수가 없어서 완전한 접근을 할 수 없다.

<표 3> 접근조건에 따라 SLAC 방법으로 키를 할당하고 할당된 키에서 레이어 키를 추출한 결과

접근조건	접근키	추출된 레이어 복호키	접근 여부
QCIF,15fps,FGS	$K_{0,s} \| K_{0,t} \| K_{1,q}$	*key(0,0,0),key(0,0,1)*	*가능*
CIF,15fps,base	$K_{1,s} \| K_{0,t} \| K_{0,q}$	*key(0,0,0),Key(1,0,0)*	*불가*
CIF, 30fps,base	$K_{1,s} \| K_{1,t} \| K_{0,q}$	*key(0,0,0)key(1,0,0)* *key(0,1,0),key(1,1,0)*	*불가*

<표 4> 접근조건에 따라 제안하는 키 생성기법으로 키를 할당하고 할당된 키에서 레이어 키를 추출한 결과

접근조건	접근키	추출된 레이어 복호키	접근 여부
QCIF,FGS,15fps	$K_1(0,1) \| K_2(0)$	*Key(0,0,0),key(0,0,1)*	*가능*
CIF,base,30fps	$K_1(1,0) \| K_2(0)$	*key(0,0,0),key(0,0,1)* *Key(1,0,0)*	*가능*
CIF,base,30fps	$K_1(1,0) \| K_2(1)$	*key(0,0,0),key(0,0,1)* *key(1,0,0),key(1,1,0)*	*가능*

5. 결 론

본 논문에서는 SVC 코딩기법에 적합한 키 관리 기법을 제안하였다. 기존 스케일러블 콘텐츠의 키 관리 기법은 SVC 가 지원하는 시간, 공간, 품질 확장성에 대한 구조를 고려하지 않고 설계되어 SVC 에 직접 적용하기에는 문제가 있다. 이를 해결하기 위해 본 논문에서는 SVC 확장구조를 분석하여 SVC 의 공간과 시간 타입에 대한 품질 타입의 상관성에 기반한 키 관리 기법을 제안하였고 실험을 통해 제안한 방법의 유효성을 검증 하였다.

Acknowledgements

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

참고문헌

[1] 원용근, 배태면, 노용만,“암호화된 SVC 비트스트림에서 조건적 접근제어 방법에 관한 연구”

[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 N 7311”Joint Scalable Video Model (JSVM) 3.0”

[4] Bin B. Zhu, Shipeng Li, Min Feng, “A Framework of Scalable Layered Access Control for Multimedia”

[5] Bin B. Zhu, Min Feng, Shipeng Li, “An Efficient Key Scheme for Layered Access Control of MPEG-4 FGS Video”