SVC 비디오의 계층적 구조에 적응적인 스케일러블 암호화 기법

종신회원 서 광 덕*, 김 재 곤**, 정회원 김 진 수***

An Adaptive Scalable Encryption Scheme for the Layered Architecture of SVC Video

Kwang-deok Seo*, Jae-Gon Kim** *Lifelong Members*, Jin-soo Kim*** *Regular Member*

요 약

본 논문에서는 SVC 의 계층적 비디오 구조에 적응적인 스케일러블 암호화 기법을 제안한다. 제안하는 암호화 기법은 SVC 의 비디오 계층간 중요도 및 우선순위를 고려하여 비디오 계층 별로 차별화 되는 암호화 강도를 갖는 암호화 알고리듬을 적응적으로 결정한다. 비디오 계층의 특성에 관계없이 모든 비디오 계층에 단일의 암호화 알고리듬을 고정적으로 적용하는 기존의 방법과 달리, 비디오 계층별 중요도에 비례하여 암호화 강도를 차별적으로 설정함으로써 중요한 데이터를 포함하는 하위 비디오 계층에 대한 보안성을 높게 유지하고, 상대적으로 중요도가 떨어지는 상위 비디오 계층에 대해서는 암호화 강도가 낮은 암호화 알고리듬을 적용한다. 다양한 실험을 통하여 제안된 적응적 스케일러블 암호화 기법의 효율성을 검증한다

Key Words : Scalable Video Coding, Video Encryption/decryption, Information Security

ABSTRACT

In this paper, we propose an adaptive scalable encryption scheme for the layered architecture of SVC video. The proposed method determines an appropriate set of encryption algorihms to be applied for the layers of SVC by considering the importance and priority relationship among the SVC video layers. Unlike the conventional encryption method based on a fixed encryption algorithm for the whole video layers, the proposed method applies differentiated encryption algorithms with different encryption strength the importance of the video layers. Thereupon, higher security could be maintained for the lower video layer including more important data, while lower encryption strength could be applied for the higher video layer with relatively less important data. The effectiveness of the propsed adaptive scalable encryption method is proved by extensive simulations.

Ⅰ. 서 론

인터넷과 같은 네트워크 기술의 발달로 더욱더 다양한 형태의 디지털 콘텐츠 관련 산업 분야가 팽창하고 있으며 콘텐츠 서비스에 대한 소비자의 요구 사항 또한 고급화 및 다양화되고 있다. 이러한 기술 환경을 바탕으로 정보와 저작권이 있는 콘텐츠의 전송에 사용되는 네트워크에서도 점점 이종망 간의 융합이 이

※ 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(KRF-2008-331-D00378)
* 연세대학교 컴퓨터정보통신공학부 (kdseo@yonsei.ac.kr)
** 한국항공대학교 항공전자 및 정보통신공학부 (jgkim@kau.ac.kr)
*** 한밭대학교 정보통신컴퓨터공학부 (jskim67@hanbat.ac.kr)
논문번호 : KICS2009-12-640, 접수일자 : 2009년 12월 30일, 최종논문접수일자 : 2010년 4월 15일

루어지고 있는 추세이다. 다양한 이종적인 (heterogeneous) 서비스 환경에서 적절한 품질을 유지할 수 있는 환경 적응적인 미디어 컨버전스 기술이 요구되는데, 이를 만족시킬 수 있는 가장 효율적인 미디어 부호화 기술이 최근에 표준화가 완료된 스케일러블 비디오 부호화 (Scalable Video Coding: SVC) 기술이다. SVC는 이종의 (heterogeneous) 망 환경에서 발생하는 대역폭의 다양성 문제, 수신 단말기 성능과 해상도의 다양성 문제, 콘텐츠 소비자의 다양한 선호도 문제 등을 융합적으로 해결할 수 있는 UMA (Universal Multimedia Access) 환경의 멀티미디어 콘텐츠 서비스에 적합한 부호화 기술이다[1].

유연한 환경 적응적 미디어 서비스를 위한 SVC 기술에 관한 연구와 더불어 중요한 연구 분야가 콘텐츠 보호 및 관리 기술이다. 현재의 콘텐츠 분배와 소비는 네트워크의 발달과 더불어 자유롭게 이루어지고 있으며 이러한 자유로운 콘텐츠 분배와 소비 환경으로 콘텐츠 보호 및 관리 시스템에 대한 활발한 연구가 진행되어 왔다. MPEG에서는 MPEG-2와 MPEG-4를 위한 DRM (Digital Right Management) 프레임워크인 IPMP-X (Intellectual Property Management and Protection-X)를 표준화 했고[2], OMA (Open Mobile Alliance) 에서도 무선 통신 시스템을 위한 DRM 시스템을 도입했다[3]. 또한 스케일러블 이미지 압축 표준인 JPEG2000을 위해서 JPSEC (JPEG2000 Secured)이라는 프레임워크를 구성하여 콘텐츠 보호에 대한 연구를 진행해 왔다[4]. 기존의 스케일러블 코딩 기법의 일종인 JPEG2000과 MPEG-4 FGS (Fine Granularity Scalability)에 관해서는 계층적 암호화에 관련된 연구 결과가 발표 되었다[5],[6],[7]. JPEG2000에서는 웨이블렛 코딩 기법을 사용하므로 웨이블렛의 주파수 분해 특성을 기반으로 암호화 및 조건적 접근 제어 방법이 제안되었다. 웨이블렛 코딩 기법은 고주파 영역과 저주파 영역으로 비디오의 주파수 성분을 계층적으로 분해하므로 각각의 분해된 주파수 대역 계층에 따라 서로 다른 암호화 Key로 암호화하여 공간 스케일러빌리티에 대한 조건적 접근 제어 방법이 제시되었다[5],[6]. MPEG-4 FGS에서는 화질적 스케일러빌리에 의해 제공하는 PSNR과 비트율에 따라 여러 가지 확장영역을 구분하여 암호화하며 암호화된 비디오 정보에 대한 제한적 접근을 제어하는 방법이 제시되었다[7]. 그리고 MPEG-4 FGS의 기본계층과 확장계층 간의 중요도의 차이점을 고려하는 차별화된 암호화 기법도 제안되었다[7]. 한편, SVC에 대한 국제 표준화 과정에서 SVC 비트스트림의 계층적 구조를 고려하여 선택적으로 데이터를 보호할 수 있는 기본 프레임워크[8]가 SVC의 파일 포맷 표준의 일부로써 포함되었다[9]. 즉, SVC의 계층적 구조의 특성에 맞게 차별화된 정보 보호 기능의 필요성을 인정하여 파일 포맷에서 이 기능을 효율적으로 지원할 수 있도록 표준 규격으로 규정한 것이다.

본 논문에서는 SVC에 의해 압축된 비트스트림의 계층적 비디오 구조를 고려한 적응적 스케일러블 암호화 기법을 제안한다. 기존에 개발된 암호화 기법들은 SVC 비트스트림의 계층적 비디오 구조를 고려하고 있지 않기 때문에 개별적인 암호화 알고리듬을 일괄적으로 SVC 비트스트림에 적용할 경우 SVC의 스케일러빌리티 특성에 맞는 계층 별로 차별화 되는 암호화가 적용되지 못한다. 이러한 문제를 해결하기 위해서 SVC 비트스트림의 구조를 분석하여 SVC 비트스트림의 확장형 비디오 계층 구조에 효과적으로 적용할 수 있는 암호화 기법을 제안한다. 특히, 데이터의 중요도에 따라서 보안 요구 수준을 달리하기 위해 비디오 계층별 중요도에 비례하여 암호화 강도를 차별적으로 설정함으로써 중요한 데이터에 대한 보안성을 높게 유지하고, 상대적으로 중요도가 떨어지는 비디오 계층에 대해서는 암호화 강도가 낮은 암호화 알고리듬을 적용하여 중량(Heavy-weight) 암호화와 경량(Light-weight) 암호화를 차등 적용한다.

Ⅱ. SVC 비디오 부호화 개요

SVC는 해상도, 화면율, 화질측면에서 다양한 품질을 제공할 수 있는 여러 개의 비디오 계층을 하나의 비트스트림으로 통합하여 부호화한다. SVC의 계층 구조는 하나의 기본계층 (base layer) 과 기본계층 위에 연속적으로 쌓을 수 있는 확장계층 (scalable enhancement layer)으로 구성된다. SVC는 하나의 비트스트림에 MGS (Medium Grain Scalability) 기술에 의한 화질적 스케일러빌리티 뿐만 아니라 시간적, 공간적 스케일러빌리티를 위한 계층 부호화 정보를 동시에 저장할 수 있으며, 이들 스케일러빌리티에 의한 계층 부호화 정보의 유기적인 결합을 통해 광범위한 형태의 복합형 (combined) 스케일러빌리티 지원이 가능하다[1].

SVC에서는 NAL (network abstraction layer) 구조로 비트스트림을 구성하며 공간적, 시간적, 화질적 스케일러빌리티 각각에 대한 기본계층과 확장계층 부호화 정보는 연속적인 NAL unit들로 구성된다. 이와 같이, SVC 부호화에 의해 생성된 부호화 정보는 NAL

unit으로 비트스트림에 저장 되는데, 그림 1에 보이듯이 기본계층에서 생성된 NAL unit과 확장계층에서 생성된 NAL unit의 헤더 구조는 서로 다르다. 기본계층의 NAL unit은 H.264/AVC의 NAL unit 헤더 구조와 동일한 헤더필드 3가지 (F, NRI, NAL Unit Type)로 구성되며 총 1바이트 크기를 갖는다. 확장계층에서 생성된 NAL unit 헤더의 경우 기본계층 NAL unit 헤더에 추가적으로 3바이트 크기를 갖는 새로운 헤더 필드 (NAL Unit Header Extension)가 붙게 된다. 각 SVC NAL unit이 확장계층과 갖는 연관성에 대한 정보를 비트스트림의 복호화 없이 NAL 계층에서 구분하기 위하여 각 SVC NAL unit 헤더에는 (DID,TID,QID)필드가 존재한다. DID (Dependency_ID)는 공간적 스케일러빌리티의 계층간 예측에 있어서 상하위 확장계층 간의 종속 체계를 나타내고, TID (Temporal_ID)는 시간적 스케일러빌리티를 위한 시간적 계층 (temporal level) 간의 체계 (hierarchy)를 나타내며, QID (Quality_ID)는 화질적 스케일러빌리티 지원을 위한 FGS (fine granular scalabilty) 또는 MGS (medium grain scalability) 계층 간의 계층 체계를 나타낸다.

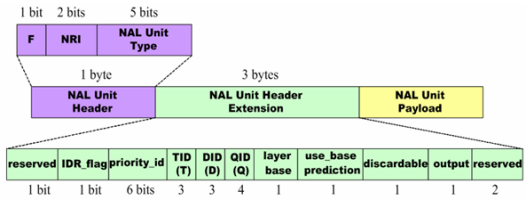

그림 1. SVC의 NAL unit의 헤더 구조

Ⅲ. 제안된 적응적 스케일러블 암호화 기법

3.1 비디오 계층 별로 차별화된 스케일러블 암호화 알고리듬 적용

SVC의 압축 과정에서 계층적 B-픽처 (hierarchical B-picture) 구조와 계층간 예측 부호화의 적용으로 SVC의 하위 계층은 상위의 계층이 원활히 복호화 되기 위한 필수적인 정보이다. 이러한 비디오 계층 간의 공간적, 시간적, 화질적 상관 관계는 II장에서 설명한 (DID,TID,QID)필드에 의해 구분이 가능하다. 따라서, DID, TID, QID 레벨이 낮을수록 하위의 계층을 구성하게 되며, 반대로 높을수록 상위의 계층을 구성하게 된다. SVC에서는 공간적, 시간적, 화질적 계층을 자유롭게 구성할 수 있으며, 각 공간계층마다 시간 계층의 수와 화질 계층의 수를 서비스 목적에 맞게 구성할 수 있다. 그림 2는 2개의 공간 계층이 존재하고, 각각의 공간 계층마다 2개의 화질 계층, 그리고 2개의 시간 계층을 포함하는 SVC 비트스트림의 계층 구조를 나타내는데, 전체적으로 6개의 계층으로 분해가 가능하다. 즉, 공간0 (DID=0), 화질0 (QID=0)와 시간0 (TID=0) 의 조합에 의한 기본계층, 공간0 (DID=0), 화질1 (QID=1)과 시간0 (TID=0)의 조합에 의한 확장계층1, 공간1 (DID=1), 화질0 (QID=0)와 시간0 (TID=0)의 조합에 의한 확장계층2, 공간1 (DID=1), 화질0 (QID=0)와 시간1 (TID=1)의 조합에 의한 확장계층 3, 공간1 (DID=1), 화질1 (QID=1)과 시간0 (TID=0)의 조합에 의한 확장계층 4, 공간1 (DID=1), 화질1 (QID=1)과 시간1 (TID=1)의 조합에 의한 확장계층 5로 구성된다.

그림 2의 6개 계층에 대한 정보보안 측면에서의 중요도 순서는 계층간 의존성을 고려했을 때, 기본계층, 확장계층1, 확장계층2, 확장계층 3, 확장계층 4, 그리고 확장계층 5의 순으로 정할 수 있다. 본 논문에서는 이러한 계층간 의존성을 고려하여, 가장 많은 계층이 의존하게 되는 기본계층에 대해 가장 강한 암호화 알고리듬을 적용하고, 확장계층1~확장계층 5에 대해서는 암호화 강도가 순차적으로 낮은 암호화 알고리듬을 적용하게 된다.

상기의 비디오 계층별로 요구되는 서로 다른 암호화 강도를 만족시킬 수 있는 복수의 암호화 알고리듬으로서 본 논문에서는 블록 암호화 기법들인 DES (Data Encryption Standards), DDES (Double DES) 및 TDES (Triple DES)[10]와 SEED[11], AES (Advanced Encryption Standards)[12] 등 5가지를 적용한다. 표 1에 이 5가지 암호화 기법에 대한 기본적인 주요 사양을 요약하였다. 또한, 표 1에 암호화 엔진에

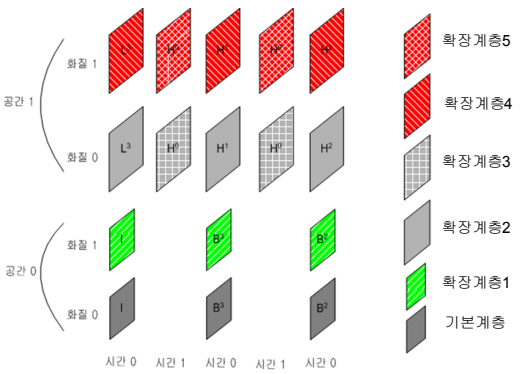

그림 2. 기본계층과 5개의 확장계층으로 이루어진 SVC비디오 계층 구조의 예

표 1. 암호화 알고리듬 별 주요 사양과 암호화 강도 순위

암호화 알고리듬	입력 비트 크기 (bits)	출력 비트 크기 (bits)	암호화 Key 크기 (bits)	암호화 처리 속도 (bytes/sec)	암호화 강도 순위
No_Enc (암호화 안함)	-	-	-	암호화 엔진 입력 데이터 속도와 같음	6
DES	64	64	64	721,472	5
DDES	64	64	128 (64×2)	517,644	4
TDES	64	64	128 (64×2)	336,276	3
SEED	128	128	128	352,170	2
AES	128	128	192	256,582	1

서 각 암호화 알고리듬에 의한 암호화 처리 속도와 암호화 강도 순위를 나타내었다. 암호화 처리 속도 측정을 위해 암호화 엔진이 구현된 시스템 환경은 윈도우 XP 운영체제와 1GB 메모리가 장착된 QuadCore (2.6 GHz) 펜티엄 컴퓨터이며, 평문 (plain text) 기반의 데이터에 대해 암호화를 수행하여 1 초당 암호화 처리가 완료되는 데이터량을 측정하였다. 측정 결과 DES, DDES, TDES, SEED, AES의 순서로 암호화 처리 속도가 감소하였다. 키 길이가 동일한 블록 암호화 알고리듬은 암호화 Key의 길이가 길어질수록 암호화 강도가 강해지지만 key 길이가 동일한 블록 암호화 간에는 암호화 강도의 단순 비교가 불가능하므로 암호화 처리 속도를 통해 암호화 강도 순위를 결정해야 한다.

본 논문에서는 SVC 비트스트림의 비디오 계층에서 요구되는 보안 수준을 고려하여 중요도가 높은 하위계층에서부터 중요도가 상대적으로 낮은 상위계층에 이르기까지 순차적으로 AES, SEED, TDES, DDES 및 DES를 적용할 수 있다. 그러나, AES, SEED 등과 같은 암호화 알고리듬의 경우 암호화 처리 속도가 상대적으로 느리므로 암호화 엔진의 계산 속도가 실시간 비디오 서비스의 데이터 처리율을 만족시켜야 한다는 조건을 고려하여 적합한 암호화 강도를 갖는 암호화 알고리듬 (No_Enc (암호화 안함) 포함)의 조합을 표 1로부터 선택하여 계층 별로 차별화 되게 적용한다.

3.2 적응적 스케일러블 암호화 기법

제안하는 적응적 스케일러블 암호화 기법은 SVC의 비디오 계층 별로 암호화 강도를 차별화하여 적용하며, 암호화 엔진에서 처리되는 데이터율이 암호화 엔진 입력 데이터율 보다 작아지지 않는 한도까지 암호화 강도를 각 계층 별로 적응적으로 차별화하여 적용한다. 따라서, 본 논문에서는 암호화 엔진에서의 계산 속도가 서비스에서 요구되는 SVC 비디오의 전송 데이터율을 만족시키면서 계층 별로 차별화된 암호화 적용이 가능한 암호화 알고리듬의 조합을 판별하게 되고, 이 결과를 바탕으로 암호화를 계층 별로 차별화하여 유연하게 적용할 수 있는 스케일러블 암호화 기법을 제안한다.

그림 3은 N개의 비디오 계층 중에서 k번째 비디오 계층을 처리하기 위한 제안된 스케일러블 암호화 기법의 동작 흐름도를 나타낸다. k번째 비디오 계층의 암호화를 위해서 암호화 알고리듬 E_k (No_Enc도 포함) 가 적용된다. 암호화 알고리듬 간의 암호화 강도는 중요한 하위 계층의 보안 강화를 위해서 $E_1 \geq E_2 \geq E_3 \cdots \geq E_N$의 관계가 성립 되도록 한다. k번째 비디오 계층에 포함되는 NAL unit의 총 개수는 M_k이고, i번째 NAL unit은 $NU_k^i (1 \leq i \leq M_k)$로 표시되며, NU_k^i의 크기는 P_k^i로 표현된다. 그리고 크기가 P_k^i인 NU_k^i가 점유하는 시간(sec)은 t_k^i로 표시된다. 제안된 기법은 GOP 단위로 처리가 되는데, 하나의 GOP단위가 차지하는 단위 시간 TG는 다음과 같이 계산된다.

$$T_G = \frac{GOP\_size}{frame\_rate} \tag{1}$$

식 (1)에서 GOP_size는 GOP의 크기를 나타내며 frame_rate는 1초당 서비스되는 화면율 (frames/sec)을 의미한다. 단위 시간(TG)당 입력되는 N개의 비디오 계층의 NAL unit을 암호화하기 위한 암호화 엔진에서의 처리 속도 S(bytes/sec)는 각각의 계층에 적용되는 암호화 알고리듬 E_k의 암호화 처리 속도 S_k의 선형적인 조합으로 계산되므로 다음과 같이 나타낼 수 있다.

$$S = \frac{1}{T_G} \cdot \sum_{k=1}^{N} \left(S_k \times \sum_{i=1}^{M_k} t_k^i \right) \tag{2}$$

식 (2)에서 M_k와 t_k^i는 단위 시간 TG 구간 내에서 값이 변하는 확률변수이므로 S의 평균값 $\overline{S}$은 다음과 같이 계산된다.

$$\begin{aligned} S &= \frac{1}{T_G} \cdot \sum_{k=1}^{N} \left(S_k \times E\left\{ \sum_{i=1}^{M_k} t_k^i \right\} \right) \\ &= \frac{1}{T_G} \cdot \sum_{k=1}^{N} \left(S_k \times \overline{M_k} \times \overline{t_k} \right) \end{aligned} \tag{3}$$

식 (3)에서 $E\{\bullet\}$는 확률변수의 평균값을 나타내고, $\overline{M_k}$는 k번째 비디오 계층에서의 NAL unit이 TG 시간 동안 평균적으로 발생하는 횟수이고, $\overline{t_k}$는 k번째 비디오 계층에서의 NAL unit의 평균 점유 시간을 의미한다. 한편 k번째 비디오 계층에서의 NAL unit의 평균적 크기인 $\overline{P_k}$는 암호화 엔진으로의 데이터 입력 속도인 R_{in} (bytes/sec)과 다음의 관계를 갖는다.

$$\overline{P_k} = R_{in} \times \overline{t_k} \tag{4}$$

식 (4)의 결과로부터 식 (3)의 $\overline{t_k}$에 $\overline{P_k}/R_{in}$을 대입하면 다음과 같은 관계가 얻어진다.

$$\overline{S} = \frac{1}{T_G \bullet R_{in}} \bullet \sum_{k=1}^{N} \left(S_k \times \overline{M_k} \times \overline{P_k} \right) \tag{5}$$

식 (5)에서 사용되는 $\overline{M_k}$와 $\overline{P_k}$는 주어진 SVC 비트스트림의 각 계층별 NAL unit을 분석하면 쉽게 계산할 수 있는 정보이고, S_k는 암호화 엔진에서의 실제 측정을 통해 표 1에 제시되어 있는 값이다. 또한 TG는 식 (1)에 의해 계산되고 암호화 엔진으로의 데이터 입력 속도인 R_{in}은 실시간 비디오 서비스를 고려할 경우에는 비디오 서버의 데이터 전송률과 동일한 값으로 설정할 수 있다. 한편, 특수한 경우로써 모든 계층에 대해 No_Enc (암호화 적용 안함)를 적용할 경우 $S_k = R_{in}$이므로 식 (5)는 다음과 같이 표현된다.

$$\overline{S_{No\_Enc}} = \frac{1}{T_G} \bullet \sum_{k=1}^{N} \left(\overline{M_k} \times \overline{P_k} \right) \tag{6}$$

실시간으로 SVC 비디오 서비스가 원활하게 이루어지기 위해서는 암호화 엔진 입력 데이터율 보다 암호화 엔진의 데이터 처리율이 높아야 손실없이 모든 NAL unit들을 암호화할 수 있기 때문에 $\overline{S}$는 다음과 같은 관계를 만족시켜야 한다.

$$\overline{S} \geq R_{in} \tag{7}$$

식 (5)를 식 (7)에 대입하면 다음과 같은 관계식을 얻을 수 있다.

$$\sum_{k=1}^{N} \left(S_k \times \overline{M_k} \times \overline{P_k} \right) \geq T_G \bullet R_{in}^2 \tag{8}$$

따라서, 식 (8)의 관계식을 만족시키는 데이터 처리율을 갖는 암호화 알고리듬들의 조합으로부터 $E_1, E_2, E_3, \cdots, E_N$로 설정될 암호화 알고리듬을 적응적으로 판별하게 된다. 이때, 계층 별로 차별화 되는 암호화 강도의 적용을 위해서, $E_1, E_2, E_3, \cdots, E_N$ 간의 암호화 강도가 표 1의 결과를 참조하여 $E_1 \geq E_2 \geq E_3 \cdots \geq E_N$의 관계를 갖도록 $E_1, E_2, E_3, \cdots, E_N$에 대한 암호화 알고리듬을 정하게 된다. 예를 들어, 그림 2의 SVC 비디오 계층 구조에 대해 기본계층부터 순차적으로 AES→SEED →TDES→DDES→DES→No_Enc 를 적용했을 때 식 (8)을 만족한다면, E_1은 AES 로 결정되고 E_2~E_6은 순서대로 SEED, TDES, DDES, DES, No_Enc 로 결정된다. 만약 식 (8)을 만족시키지 못한다면, 암호화 처리 속도를 더 빠르게 적용할 수 있도록 기본계층부터 순차적으로 SEED→TDES→DDES→DES→No_Enc

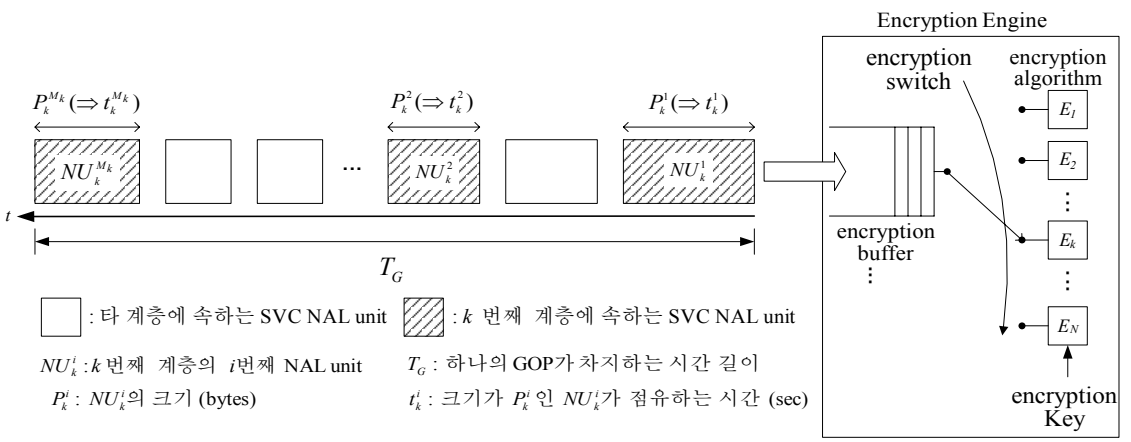

그림 3. k번째 비디오 계층을 처리하기 위한 암호화 흐름도

→No_Enc 를 적용하게 된다. 이러한 방법을 통해서 식 (8)을 만족시키는 암호화 알고리듬의 조합을 적응적으로 결정하게 된다. 한편, 제안된 기법에서는 사용될 암호화 알고리듬을 식 (8)을 활용하여 GOP 마다 적응적으로 결정하게 되는데, SVC의 비디오 계층 구조가 변하지 않을 경우 동일한 비디오 시퀀스 내에 포함되는 거의 모든 GOP에 대해 동일한 조합의 암호화 알고리듬들이 최종적으로 적용될 암호화 알고리듬으로 결정된다. 일부의 GOP에서 암호화 알고리듬의 조합이 변경되는 경우는 특정 GOP 내에 포함되는 NAL unit의 평균적인 길이가 다른 GOP의 NAL unit 과 매우 상이한 경우에 발생하게 된다. 또한, 식 (8)에 적용되는 GOP 당 NAL unit의 평균적 개수는 SVC의 스케일러빌리티를 위해 설정한 비디오 계층 구조가 변하지 않는 한 일반적으로 고정적이다. 그리고 식 (8)에 적용되는 NAL unit의 평균적인 길이는 SVC 비트스트림을 콘텐츠 파일로 저장하기 위한 표준 포맷인 SVC 파일 포맷[14]의 메타데이터인 "Sample Table Box (stbl)"내에 존재하는 "sample sizes (stsz)" 필드를 통해 사전에 계산할 수 있으므로, GOP 단위의 처리로 인해 발생 가능한 처리 지연 시간을 막을 수 있다. 즉, 특정 GOP에 포함되는 모든 NAL unit을 암호화 엔진이 입력 받은 후에 NAL unit들의 평균적 크기를 계산할 필요 없이 NAL unit 의 크기를 나타내는 "sample sizes (stsz)" 필드를 통해 별도로 또는 사전에 계산할 수 있다.

이상의 과정을 통해 각 계층 별로 적용될 암호화 알고리듬이 결정되면, 각 계층별 암호화에 필요한 암호화 Key가 필요하다. 암호화 Key는 각 계층의 공간(s),시간(t),화질(q)의 레벨을 구분하여 Key (s,t,q)로 표현된다. 특정 스케일러빌리티 구조를 갖는 SVC 비트스트림을 암호화하는데 사용되는 암호화 Key의 개수는 다음 식과 같이 계산된다.

$$Key = \sum_{s=1}^{NS} \left(NQ_s \times NT_s \right) \qquad (9)$$

식 (9)에서 NS는 공간 계층의 수, NQ_s는 s번째 공간 계층에서의 화질 계층의 수, NT_s는 s번째 공간 계층에서의 시간 계층의 수를 나타낸다. 그림 2의 계층 구조의 경우 0번째 공간 계층에서는 화질 계층의 수가 2개이고 시간 계층의 수는 1개이므로 총 2개의 암호화 Key가 필요하며, 1번째 공간 계층에서는 화질 계층의 수가 2개이고 시간 계층의 수가 2개이므로 총 4개의 Key가 필요하다. 따라서 그림 2의 예에서는 총 6 (=2+4)개의 Key가 필요하며 기본계층의 암호화에는 Key(0,0,0)이 적용되고, 확장계층1~5까지는 차례대로 Key(0,0,1), Key(1,0,0), Key(1,1,0), Key(1,0,1), Key(1,1,1)이 적용된다. 표 2는 그림 2의 계층 구조를 갖는 SVC 비디오의 특정 공간(s),시간(t),화질(q)에 해당하는 품질에 접근하기 위해 필요한 암호화 Key의 조합을 표시하였다.

표 2. 그림 2의 계층 구조를 갖는 SVC 비디오의 특정 공간(*s*), 시간(*t*), 화질(*q*)에 해당하는 품질에 접근하기 위해 필요한 Key(s,t,q)의 조합

s/*q* \ *t*		*t*=0	*t*=1
s=0	*q*=0	{Key(0,0,0)}	Not Available
	q=1	{Key(0,0,0), Key(0,0,1)}	Not Available
s=1	*q*=0	{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)}
	q=1	{Key(0,0,0), Key(0,0,1), Key(1,0,0), Key(1,0,1)}	{Key(0,0,0), Key(0,0,1), Key(1,0,0), Key(1,1,0) Key(1,0,1), Key(1,1,1)}

Ⅳ. 실험 결과

제안된 적응적 스케일러블 암호화 기법의 성능을 검증하기 위해서 JSVM (Joint Scalable Video Model) 9.13으로 압축된 SVC 비트스트림을 활용하였다[13]. 실험에서는 GOP의 크기가 16으로 구성된 CREW, SOCCER 등 2가지 종류의 테스트 영상을 사용하였다. 이들 영상은 2 개의 공간적 스케일러빌리티 (CIF, 4CIF)를 가지며, 각각의 공간적 스케일러빌리티마다 2가지의 시간적 스케일러빌리티 (15 fps, 30 fps) 및 3 가지의 화질 (기본화질+2 MGS) 을 제공하도록 SVC로 부호화 되었다.

첫 번째 실험은 CREW 영상에 대해 4CIF, 30 fps, 3.0 Mbps로 실시간 비디오 전송 서비스가 이루어지도록 하였다. 이 조건에 해당하는 비디오 계층 구조는 그림 2와 유사하며, 화질 계층의 경우 SVC Extractor가 기본계층과 공간적 확장계층 모두 하나의 MGS가 포함되도록 NAL unit을 SVC 비트스트림으로부터 추출하게 된다.

그림 4는 3.0 Mbps의 데이터율로 암호화 엔진에 입력되는 NAL unit에 대해 제안된 적응적 스케일러블 암호화 기법에 의해 암호화 한 경우의 암호화 처리 속도와 모든 계층에 대해 고정된 암호화 알고리듬을

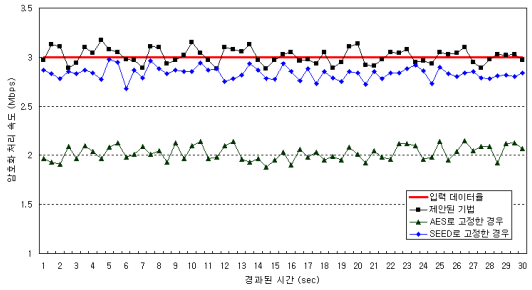

그림 4. CREW 영상에 대한 다양한 암호화 기법 간의 암호화 처리 속도 비교

적용한 경우의 암호화 처리 속도를 비교한 결과를 보인다. 실험에 적용된 고정된 암호화 알고리듬은 각각 AES와 SEED 이다. AES와 SEED의 경우 암호화 강도가 높기 때문에 계산 복잡도가 높고 암호화 처리 속도가 낮다. 따라서, AES 와 SEED를 모든 계층에 대해 일괄적으로 적용할 경우 암호화 엔진에서의 계산 복잡도 증가로 인해 입력 데이터율을 원활한 속도로 암호화를 처리하지 못하고 입력 데이터율인 3.0 Mbps 보다 낮은 암호화 처리 속도를 나타낸다. 그림 4에 나타난 실험 결과에서 AES의 경우 평균적으로 2.03 Mpbs 로 처리 속도가 측정 되었으며, SEED의 경우 평균적으로 2.81 Mbps 정도로 처리 속도가 측정 되었다. 이에 반해서, 제안된 적응적 스케일러블 암호화 기법의 경우 그림 4의 결과에 보이듯이 암호화 엔진에 입력되는 데이터율을 만족시키는 적절한 속도로 계층별로 차별화된 암호화를 적용하여 평균적으로 2.97 Mbps 정도의 처리 속도를 제공함을 관찰할 수 있다. 한편, 암호화 처리 속도가 빠른 DES를 모든 계층에 일괄적으로 적용할 경우는 표 1을 참조할 경우 DES의 암호화 처리 속도가 5.76 Mbps에 달하므로 실험 유무와 상관없이 3.0 Mbps의 데이터율로 입력되는 NAL unit을 실시간적으로 처리하는데는 아무런 문제가 없다. 그러나 모든 계층에 대해 보안 강도가 가장 약한 DES를 적용하고 있기 때문에 보안에 있어서는 가장 취약한 성능을 나타낼 수 밖에 없다. 따라서, 제안된 기법에 의해 비디오 서비스에 적합한 처리 속도를 유지함과 동시에 계층적으로 차별화된 암호화를 적용하여 암호화 강도를 요구 수준에 맞게 유지하는 효과적인 암호화 처리 결과를 얻을 수 있음을 알 수 있다.

두 번째 실험은 SOCCER 영상에 대해 4CIF, 30 fps, 3.4 Mbps로 실시간 비디오 전송 서비스가 이루어지도록 하였다. 화질 계층의 경우 SVC Extractor가 기본계층과 공간적 확장계층 모두 하나의 MGS가 포함되도록 NAL unit을 SVC 비트스트림으로부터 추출하게 된다. 그림 5는 3.4 Mbps의 데이터율로 암호화 엔진에 입력되는 NAL unit에 대해 제안된 적응적 스케일러블 암호화 기법에 의해 암호화 한 경우의 암호화 처리 속도와 모든 계층에 대해 고정된 암호화 알고리듬을 적용한 경우의 암호화 처리 속도를 비교한 결과를 보인다. 첫 번째 실험 결과인 그림 4와 유사한 결과를 관찰할 수 있는데, AES와 SEED를 고정적으로 모든 계층에 적용한 경우에는 이들 암호화 알고리듬의 낮은 처리 속도로 인해 실시간 데이터 처리가 불가능하다. AES를 고정적으로 적용한 경우에는 평균적으로 2.05 Mbps의 암호화 처리 속도를 나타내며, SEED의 경우 평균적으로 2.86 Mbps의 처리 속도를 보인다. 제안된 기법의 경우 적절한 암호화 강도를 갖는 암호화 알고리듬의 조합을 선택하여 암호화 엔진에 입력되는 데이터율을 만족시키는 충분한 속도로 계층별로 차별화된 암호화를 적용하여 평균적으로 3.36 Mbps 정도의 처리 속도를 제공함을 관찰할 수 있다. 따라서, 제안된 암호화 기법의 적용으로 실시간 비디오 서비스에 적합한 처리 속도를 유지함과 동시에 계층적으로 차별화된 암호화를 적용하여 암호화 강도를 요구 수준에 맞게 유지하는 효과적인 암호화 처리 결과를 얻을 수 있음을 알 수 있다.

그림 6은 그림 5의 실험에서 제안된 기법에 의해 암호화된 비트스트림에 대해 접근하기 위하여 부적합한 암호화 Key로 접근을 시도한 경우와 완벽한 암호화 Key로 접근을 시도한 경우에 얻을 수 있는 비디오 화질을 비교한다. 30 fps의 4CIF 해상도와 고화질 (MGS 계층이 포함된 경우)의 비디오 품질에 대한 완벽한 접근을 위해서는 모든 계층에 대한 암호화 Key를 확보하고 있어야 하는데, 본 실험에 적용된 공간적, 시간적, 화질적 스케일러빌리티에 의한 비디오 계층 구조를 고려할 때 식 (9)에 의해 총 6개의 암호화 Key가 필요하다. 그림 6(a)는 적합한 6개의 암호화 Key를

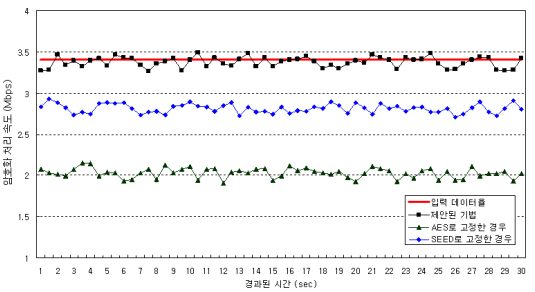

그림 5. SOCCER 영상에 대한 다양한 암호화 기법 간의 암호화 처리 속도 비교

(a) 접근권한이 없는 경우

(b) 완벽한 접근 권한을 갖춘 경우

그림 6. 암호화된 SOCCER 영상에 대한 접근권한이 없는 경우와 완벽한 접근권한을 갖춘 경우에 얻을 수 있는 비디오 화질 비교

확보하지 못하여 접근 권한이 확보되지 못한 경우에 얻게 되는 영상을 나타내며, 그림 6(b)는 요구되는 6개의 암호화 Key인 {Key(0,0,0), Key(0,0,1), Key(1,0,0), Key(1,1,0), Key(1,0,1), Key(1,1,1)}를 모두 확보하여 완벽한 접근 조건을 확보한 경우에 암호화 해독 및 SVC 복호화를 차례대로 적용하여 얻을 수 있는 영상을 나타낸다.

한편, 상기의 실험에서는 SVC 비디오 서버에 제안된 암호화 기법을 장착하여 실험을 수행하여 제안된 기법의 효율성을 검증하였는데, 제안된 암호화 기법을 비디오 전송 도중에 거치게 되는 게이트웨이 또는 라우터에 장착하여도 그 효율성을 기대할 수 있다. 게이트웨이에서도 게이트웨이에 입력되는 데이터율을 실시간적으로 처리할 수 있는 암호화 기법의 필요성이 존재한다. 게이트웨이에 입력되는 NAL unit의 경우 그림 1에 보이듯이 헤더 부분에 (DID,TID,QID)필드가 존재하므로, 암호화 처리 대상이 되는 NAL unit의 비디오 계층 정보를 알 수 있다. 이를 바탕으로 제안된 암호화 기법을 적용할 경우 상기의 실험 결과와 유사한 효율성을 얻을 수 있을 것이다. 다만, 서버와 게이트웨이 간에 존재하는 패킷의 도착 지연과 패킷 간의 지터 (jitter)에 의한 영향은 별도의 추가적인 연구가 필요할 것이다.

V. 결 론

본 논문에서는 SVC 의 계층적 비디오 구조를 고려한 적응적인 스케일러블 암호화 기법을 제안하였다. 제안된 암호화 기법에 의해 비디오 계층별 중요도에 비례하여 암호화 강도를 차별적으로 설정함으로써 중요한 데이터에 대한 보안성을 높게 유지하고, 상대적으로 중요도가 떨어지는 비디오 계층에 대해서는 암호화 강도가 낮은 암호화 알고리듬을 적용한다. 계층별로 적용되는 암호화 알고리듬의 종류는 암호화 엔진에서의 데이터 처리율이 암호화 엔진에 입력되는 SVC NAL unit의 입력 데이터율을 실시간적으로 처리할 수 있도록 적응적으로 결정 되므로 실시간 비디오 전송 서비스를 만족시킬 수 있다.

참 고 문 헌

〔1〕 H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," *IEEE Trans. Circuits and Syst. for Video Technol.*, Vol.17, No.9, pp.1103-1120, Sept. 2007.

〔2〕 ISO/IEC JTC1/SC29/WG11 13818-11: Information technology generic coding of moving pictures and associated audio information—Part 11, "IPMP on MPEG-2 Systems," 2003

〔3〕 W. Buhse, and J. Meer, "The open mobile alliance (OMA) digital rights management," *IEEE Signal Process. Magazine*, Vol.24, No.1, pp.140-143, Jan. 2007.

〔4〕 ISO/IEC JTC1/SC29/WG 1/N3853, JPSEC (JPEG2000 Security) Final Draft of International Standard, Feb. 2006.

〔5〕 D. Engel, T. Stutz, and A. Uhl, "Format-compliant JPEG2000 encryption in JPSEC," *EURASIP Journal on Information Security*, Vol.

2007, Article ID: 94565, 2007.
〔6〕 R. Norcen, and A. Uhl, “Selective encryption of the JPEG2000 bitstream,” *Lecture Notes in Computer Science*, Vol.2828, pp.194-204, 2003.
〔7〕 B. Zhu, C. Yuan, Y. Wang, and S. Li, “Scalable protection for MPEG-4 fine granularity scalability,” *IEEE Trans. Multimedia*, Vol.7, No.2, pp.222-233, Apr. 2005.
〔8〕 Hendry, M. Kim, S. Hahm, K. Lee, K. Park, “Layered Protection of SVC Bitstream: Application and Requirements (revisiting),” ISO/IEC JTC1/SC29/WG11/M13638, Klagenfurt, Austria, July2006.
〔9〕 ISO/IEC 14496-15, ISO/IEC 14496-15 AMENDMENT 2: File format support for scalable video coding (SVC).
〔10〕 M. Smid, and D. Branstad, “Data Encryption Standard: past and future,” *Proc. of the IEEE*, Vol.76, No.5, pp.550-559, May 1988.
〔11〕 한국정보보호센터 (KISA), 128비트 블록 암호 알고리듬 (SEED) 개발 및 분석 보고서, 1998년 12월.
〔12〕 Announcing the Advanced Encryption Standard (AES) (Nov. 2001). Available online at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
〔13〕 J. Reichel, H. Schwarz, and M. Wien, “Joint scalable video model (JSVM),” JVT-X202, Geneva, Switzerland, July 2007.

서 광 덕 (Kwang-deok Seo) 종신회원

1996년 KAIST 전기및전자공학과 학사
1998년 KAIST 전기및전자공학과 석사
2002년 KAIST 전기및전자공학과 박사
2002년~2005년 LG전자 단말연구소 선임연구원
2005년~현재 연세대 컴퓨터정보통신공학부 부교수
<관심분야> 영상부호화, 영상통신, 디지털방송

김 재 곤 (Jae-Gon Kim) 종신회원

1990년 경북대학교 전자공학과 학사
1992년 KAIST 전기및전자공학과 석사
2005년 KAIST 전기및전자공학과 박사
1992년~2007년 ETRI 선임연구원/팀장
2001년~20002년 뉴욕 콜롬비아대학교 연구원
2007년~현재 한국항공대학교 항공전자 및 정보통신공학부 조교수
<관심분야> 비디오 신호처리/부호화, 디지털방송 미디어, 미디어 컨버전스, 멀티미디어통신

김 진 수 (Jin-soo Kim) 정회원

1991년 경북대학교 전자공학과 학사
1993년 KAIST 전기및전자공학과 석사
1998년 KAIST 전기및전자공학과 박사
1995년~2000년 삼성전자 Network 팀 선임연구원
2008년~2009년 텍사스 주립대학교 방문연구원
2000년~현재 한밭대 정보통신컴퓨터공학부 교수
<관심분야> 영상부호화, 영상통신, 디지털방송