SVC 비디오 스트리밍을 위한 계층적 암호화 제어 기법

황재형* · 서광덕** · 정순흥***

Control of Layered Encryption for SVC Video Streaming

Jae-hyung Hwang* · Kwang-deok Seo** · Soon-heung Jung***

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행하였음.
[KI001928, 유무선 환경의 개방형 IPTV (IPTV2.0) 기술개발]

요 약

최근 다양한 서비스 환경에 대해 적응적인 비디오 품질을 제공할 수 있는 계층 부호화 기술인 SVC 압축 기법의 표준화가 완료되었다. 본 논문에서는 SVC의 비디오 계층간 중요도의 특성을 고려하여 목표로 하는 일정한 계산 복잡도로 암호화 복잡도를 제어할 수 있는 계층적 암호화 기법을 제안한다. 특히, 다양한 서비스 환경에 대해 적응적인 SVC 비디오의 NAL unit의 계층적 분류에 따른 NAL unit의 중요도 분석과 그 중요도에 적합한 암호화 강도를 적용하는 기법을 제안한다. 암호화 시간에 대한 제어 능력과 부적합한 해독키에 의해 재생된 영상의 화질 비교를 통해 제안된 계층적 암호화 기법의 성능이 우수함을 검증한다.

ABSTRACT

Recently, the standardization of SVC technology which can provide adaptive video quality in diverse service environments has been completed. This paper proposes a layered encryption technique which takes into account the prioritized layer characteristics of SVC and control constant encryption complexity satisfying the target computational complexity. In particular, it analyzes the importance of NAL unit in the SVC video layer and suggests a method to apply appropriate encryption complexity proper for it. The effectiveness of the proposed method is proved through the comparison of time required for encryption and the reconstructed video quality using imperfect decryption key.

키워드

스케일러블 비디오 부호화, 계층적 비디오 부호화, 비디오 암호화, 정보보안

Key word

Scalable video coding, layered video coding, video encryption, information security

* 어니언텍 연구원
** 연세대학교 컴퓨터정보통신공학부 교수 (교신저자, kdseo@yonsei.ac.kr)
*** 한국전자통신연구원 선임연구원

접수일자 : 2010. 01. 27
심사완료일자 : 2010. 03. 11

I. 서 론

SVC(Scalable Video Coding)는 기존의 MPEG-2, MPEG-4 등에서 시도한 계층 부호화(layered coding) 기반의 스케일러빌리티가 갖는 문제점인 낮은 압축효율, 복잡한 스케일러빌리티 지원불가, 높은 구현 복잡도의 문제를 한꺼번에 해결하기 위하여 개발된 새로운 확장형 부호화 기술이다 [1].

최근 ITU-T 에서는 보안 적용 분야를 단말, 전송 네트워크, 서비스, 콘텐츠 계층으로 분류하여 표준화를 추진하고 있다. 그러나 현재의 SVC에 대한 보안 서비스는 기존의 전통적인 메커니즘을 기반으로 제공되고 있으며 방송통신 융합에 따른 네트워크, 단말, 그리고 콘텐츠에 대하여 완전한 융합 형태의 보안 솔루션은 제시되지 않은 상태이다. SVC 콘텐츠에 대한 보안을 제공하기 위해 CAS (Conditional Access System)와 DRM (Digital Rights Management) 기술의 적용이 주종을 이루고 있지만, SVC의 확장성을 고려한 새로운 개념의 보안 기술은 여전히 개념을 정립하는 초기 단계에 머물러 있다. 기존에 제시된 관련 연구 결과로는 스케일러블 부호화의 복잡한 인코딩/디코딩 과정과 비교적 큰 사이즈의 데이터 처리 환경을 고려하여 중요한 일부 데이터에 대한 선택적 (Selective) 암호화를 적용하거나 스크램블링을 적용하였다 [2]. 또한, MPEG에서는 MPEG-2와 MPEG-4를 위한 DRM 프레임워크인 IPMP-X (Intellectual Property Management and Protection-X)를 표준화 했고 [3], OMA (Open Mobile Alliance) 에서도 무선통신 시스템을 위한 DRM 시스템을 도입했다 [4]. 스케일러블 이미지 압축 표준인 JPEG2000을 위해서 JPSEC (JPEG2000 Secured)이라는 프레임워크를 구성하여 콘텐츠 보호에 대한 연구를 진행해 왔다 [5]. 기존의 스케일러블 코딩 기법의 일종인 JPEG2000과 MPEG-4 FGS (Fine Granularity Scalability)에 관해서는 계층적 암호화 (scalable encryption)에 관련된 연구 결과가 발표 되었다 [6], [7], [8].

SVC에서는 인코딩 복잡도가 높고 비트스트림을 구성하는 NAL unit이 계층 별로 다양한 중요도를 가지기 때문에 이러한 특징을 고려한 새로운 암호화 기법이 제안되어야 한다. 따라서, 본 논문에서는 SVC의 계층별 확장적 특징을 고려하여, NAL unit에 대한 중요도를 선택적으로 판단하여 경량 및 중량 암호화를 차등 적용한다. 또한, 복잡도가 상이한 여러 암호화를 모듈화하여 네트워크 상황이나 서비스 받는 유저의 상황에 맞추어 계층적 암호화 기법을 적용하여 전체적인 암호화 복잡도를 일정하게 유지하는 방법을 제안한다. 제안된 방법은 주어진 채널 대역폭을 만족시키기 위해 SVC 비트스트림에서 NAL unit을 추출(extraction)한 후 각 NAL unit이 속하는 계층적 중요도를 바탕으로 적합한 암호화 기법을 선택/적용하며, 암호화 시간에 대한 제어 능력과 불완전한 해독키에 의해 재생된 영상의 화질 비교를 통해 제안된 계층적 암호화 기법의 성능이 우수함을 검증한다.

II. SVC 비디오 부호화 개요

SVC는 다양한 전송환경에서 콘텐츠의 적응을 용이하게 하기 위해 비트스트림을 VCL (Video Coding Layer)과 NAL (Network Abstraction Layer)로 분리하여 구성한다 [1]. VCL에서는 부호화 정보를 화면 단위로 생성하게 된다. VCL 정보는 NAL 계층에서 NAL unit으로 생성되어 SVC 비트스트림에 저장된다. SVC 부호화에 의해 생성된 부호화 정보는 NAL unit으로 비트스트림에 저장이 되는데, 그림 1에 보이듯이 기본계층에서 생성된 NAL unit과 확장계층에서 생성된 NAL unit의 헤더 구조는 서로 다르다. 확장계층에서 생성된 NAL unit 헤더의 경우 기본계층 NAL unit 헤더에 추가적으로 3바이트 크기를 갖는 새로운 헤더 필드 (NAL Unit Header Extension)가 붙게 된다.

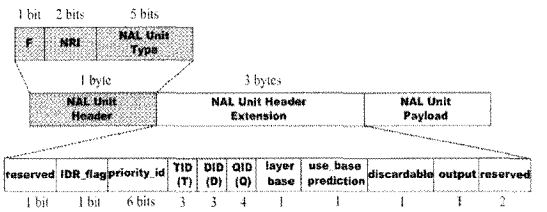


그림 1. SVC의 기본계층과 확장계층에서 사용되는 NAL unit의 헤더 구조.
Fig. 1 Structure of NAL uinit for SVC base and enhancement layer

각 SVC NAL unit이 확장계층과 갖는 연관성에 대한 정보를 비트스트림의 복호화 없이 NAL 계층에서 구분하기 위해 헤더에는 (DID,TID,QID)필드가 존재한다.

DID(Dependency_ID), TID(Temporal_ID), QID (Quality_ID) 값들의 조합으로부터 각 NAL unit이 속하게 되는 시공간적 스케일러빌리티 계층을 유도해 낼 수 있다.

Ⅲ. SVC를 위한 계층적 암호화 제어 기법

3.1 암호화 강도 분류

비디오 계층 별로 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) [9]와 SEED[10], AES (Advanced Encryption Standards)[11] 등 5가지를 적용한다.

표 1. 암호화 입/출력 비트량 및 암호화 시간측정
Table. 1 Amount of input/output bits and measure of encryption time

	입출력 비트수 (bits)	Key 크기 (bits)	라운드수	암/복호화 평균시간 (ms)
DES	64	64	Feistel 16 (32bit)	1.98
D-DES	64	128 (64*2)	Feistel 16 (32bit)	2.88
T-DES	64	128 (64*2)	Feistel 16 (32bit)	4.89
SEED	128	128	변형Feistel 16 (64bit)	4.18
AES	192	192	12라운드 (subByte-shiftrow -mixcolumn)	5.79

표 1은 각각의 암호화 기법의 특징과 암호화 속도에 대해 간략하게 비교한 결과이다. 암호화 시간 측정을 위한 테스트 환경은 인텔 Core2Duo 6320(1.86GHz) CPU와 2GB RAM이 장착된 PC 시스템이며, 일반 텍스트 데이터에 대해 암호화 및 복호화를 수행하는데 소요된 평균 시간을 측정하였다. 암호화 강도에 대한 순서 분류를 위해 우선적으로 입력 비트 수에 따른 출력 비트 수의 크기로 순위를 결정하였으며, 같은 크기의 비트가 암호화 되는 경우에는 암호화에 대한 시간 측정(tenc) 결과와 암호화 연산의 횟수를 바탕으로 암호화 강도 순위를 결정하였다.

최종적인 암호화 강도의 순위는 표 2와 같이 결정하였다. 입출력 단위 및 암호화에 걸린 시간에 따라 DES, DDES, TDES를 암호화 강도 3~5 순위에 배정하였다. 순위 3~5를 결정하기 위한 세부적 기준으로는 암호화 연산의 횟수인 Feistel 라운드 수와 암호화 평균 시간 측정 결과를 토대로 하였고, 암호화 강도 5순위에는 DES, 4순위에는 DDES, 3순위에는 TDES를 배정하였다. SEED와 TDES의 경우 암호화 시간만 비교했을 경우 SEED가 TDES보다 빠른 암호화 속도를 보이지만 암호화되는 비트의 수가 SEED가 TDES보다 많으며, SEED에서는 기존 DES의 Feistel 구조의 변형인 64비트씩 16라운드를 실행하므로 더 높은 암호화 강도를 나타내게 되고 이를 바탕으로 2순위로 설정하였다.

표 2. 암호화 강도 순위
Table. 2 Order of encryption strength

	DES	DDES	TDES	SEED	AES
입출력 비트수	64	64	64	128	192
암호화 연산	Feistel 16회X1	Feistel 16회X2	Feistel 16회X3	변형 Feistel	Rijndael 암호화
암호화 시간(ms)	1.98	2.88	4.89	4.18	5.79
암호화 강도 순위	5	4	3	2	1

3.2 SVC 비디오 계층 별 중요도 결정

제안하는 SVC를 위한 계층적 암호화 제어기법은 비트스트림을 구성하는 기본 단위인 NAL unit의 중요도를 바탕으로 계층 별로 차별화되는 암호화 강도를 적용하면서도 전체적인 암호화 복잡도는 일정하게 유지하여 서비스하는 것이 목표이다.

이때 각각의 NAL unit에 대한 중요도를 판단하여 이에 적합한 암호화 강도를 선택해야 하므로 NAL unit의 중요도를 판단하는 것은 중요하다. NAL unit의 중요도를 판단하는 근거로써 특정 계층의 NAL unit이 SVC 비디오 복호화 시에 영향을 미치게 되는 타 비디오 계층의 개수를 활용한다.

(*DID,TID,QID*) 필드를 구성하는 *DID*, *TID*,*QID* 레벨이 낮을수록 하위의 계층을 구성하게 되며, 반대로 높을수록 상위의 계층을 구성하게 된다. 만일 소비자가 D 공간, T 시간, Q 화질에 해당하는 품질의 SVC 비디오 서비스를 원할 경우 SVC 비트스트림으로부터 *DID*≤D, *TID*≤T, *QID*≤Q 조건을 동시에 만족하는 (*DID,TID,QID*) 필드를 갖는 모든 NAL unit을 각 화면의 하위계층에서부터 상위계층에 이르기까지 순차적으로 비트스트림으로부터 추출하여 서비스하게 된다. 이때, 하위 계층에 속하는 NAL unit은 상위계층에 속하는 NAL unit 보다 전송 우선순위와 중요도가 앞서기 때문에 암호화 적용시에도 보안 요구 수준을 고려하여 차등화된 암호화가 적용될 필요가 있다.

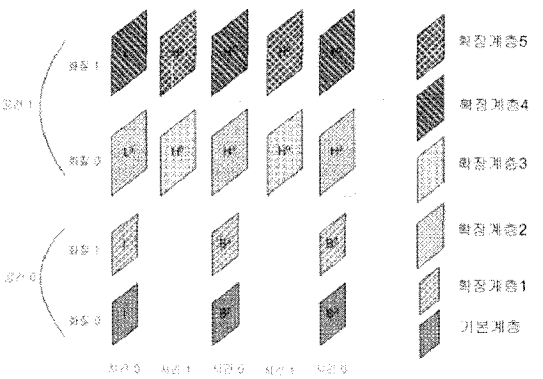


그림 2. 기본계층과 5개의 확장계층으로 이루어진 SVC 비디오 계층 구조의 예.
Fig. 2 Example of SVC video layer consisting of a base layer and five enhancement layers

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.

가장 많은 계층이 의존하게 되는 기본계층에 대해 가장 강한 암호화 알고리듬을 적용하고, 확장계층1~확장계층 5에 대해서는 암호화 강도가 순차적으로 낮은 암호화 알고리듬을 적용하게 된다. 이를 통해 정보 보안상의 중요도가 높은 기본계층에 대해서는 보안 안전도를 높이고 중요도가 낮은 확장계층에 대해서는 강도가 낮은 암호화를 적용함으로써 암호화 엔진에서의 평균적인 부하를 목표 수준으로 유지하면서 암호화 엔진 입력 데이터율을 실시간적으로 처리할 수 있도록 암호화 처리 속도를 제어할 수 있다.

3.3 제안하는 계층적 암호화 기법

그림 3은 제안하는 SVC를 위한 계층적 암호화 제어 시스템의 송신측 동작 구조도를 나타낸다. 그림 3에서 SVC 비트스트림은 SVC Extractor에 의해서 기본계층의 NAL unit과 각각의 확장계층의 NAL unit으로 분리되어 추출된다. 추출된 NAL unit은 NAL unit 헤더의 *DID, TID, QID*의 값을 확인하여 NAL unit이 포함되는 비디오 계층을 파악하게 되며 이를 바탕으로 NAL unit의 중요도에 합당한 암호화 기법을 적응적으로 선택 적용한다.

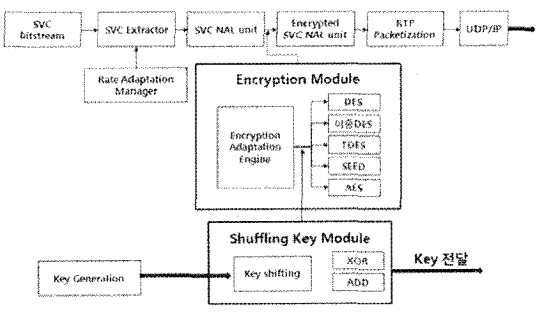


그림 3. 계층적 암호화 기법의 송신측 구조.
Fig. 3 Sender structure of the proposed layered encryption scheme

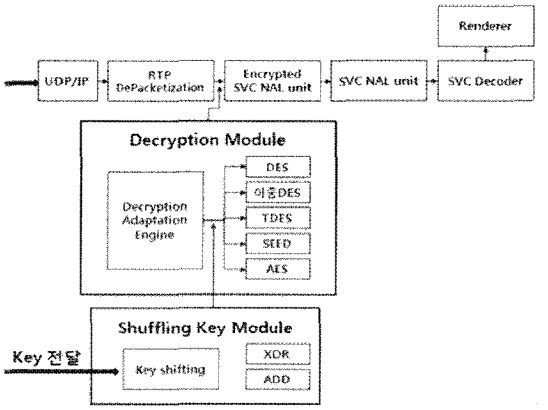


그림 4. 계층적 암호화 기법의 수신측 구조.
Fig. 4 Receiver structure of the proposed layered encryption scheme

그림 4는 그림 3의 송신측에서의 암호화 구조에 대응되는 수신측에서의 복호화 (decryption) 구조를 나타낸다. SVC 에서 변화하는 QoS(Quality of Service)에 맞추어 일정한 암호화 복잡도를 유지하는 부분이 그림 3의 "Encryption Adaptation Engine"이다. "Encryption Adaptation Engine"은 하나의 GOP(Group of Picture) 단위로 처리되며, 암호화 시간 Threshold를 설정하여 이 Threshold 이내에서 암호화 가능한 NAL unit에 대해 중요도에 따른 암호화를 실시하도록 설계하였다. 암호화 Threshold 값은 각 GOP 단위로 설정이 가능하다. 전체적인 암호화 복잡도를 일정하게 유지하기 위해 GOP 내의 모든 NAL unit의 개수를 α로 놓고, GOP 내에서 AES가 적용될 NAL unit의 개수를 β, TDES가 적용될 NAL unit 개수를 γ, DDES가 적용될 NAL unit 개수를 δ, SEED가 적용될 NAL unit 개수를 ε, DES가 적용될 NAL unit 개수를 ζ로 놓으면 아래와 같은 관계를 얻게 된다.

$$\alpha = \beta + \gamma + \delta + \varepsilon + \zeta \quad (1)$$

제안된 기법에서 AES, TDES, DDES, SEED 및 DES를 적용하였을 때의 평균 암호화 시간을 각각 B, C, D, E, F로 가정할 경우 하나의 GOP에서의 전체적인 시간적 복잡도는 $\beta B + \gamma C + \delta D + \varepsilon E + \zeta F$로 계산된다. 만약, 암호화에 A 시간 만큼 소요되는 특정 암호화 기법을 GOP 내에 존재하는 모든 NAL unit에 대해 일괄적으로 적용하였을 때 걸리게 되는 시간인 αA를 암호화 Threshold 값으로 설정할 경우 제안된 기법은 아래와 같은 관계를 만족시키게 된다.

$$\beta B + \gamma C + \delta D + \varepsilon E + \zeta F \leq \alpha A = \text{Threshold} \quad (2)$$

그림 5는 제안된 계층적 암호화 제어 기법의 전체 동작 흐름도를 나타낸다. 먼저, SVC 비트스트림 데이터가 입력되면, GOP의 시작여부를 판단하게 된다.

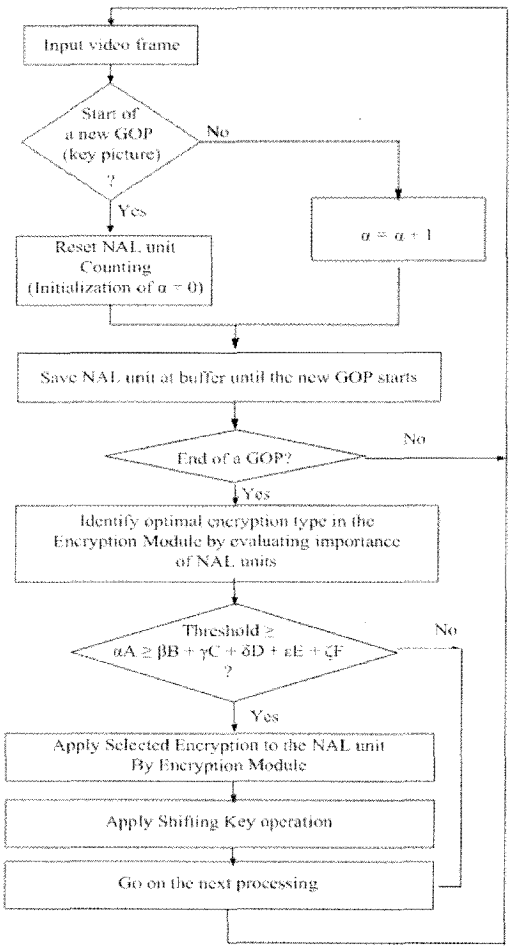


그림 5. 계층적 암호화 기법의 동작 흐름도.
Fig. 5 Flowchart of the proposed layered encryption scheme

현재의 제안된 암호화 기법은 GOP 단위로 처리가 되기 때문에 GOP의 시작에 해당하는 NAL unit이 입력으로 들어오면 하나의 GOP 내의 모든 NAL unit 개수인 α 값이 파악 되도록 다음의 새로운 GOP의 시작시점까지 입력되는 NAL unit을 버퍼에 저장한다. 하나의 GOP가 버퍼에 저장되면 α값을 기반으로 버퍼에 저장된 NAL unit에 대해 *DID, TID, QID* 값을 추출한 뒤 이 값을 바탕으로 계층 별로 차별화 되는 암호화 기법을 적용한다. 기본계층에 해당하는 NAL unit에 대해서는 AES를 적용하고, 확장계층에 해당하는 NAL unit에 대해서는 계층 별 순서에 따라 TDES, DDES, SEED 및 DES 를 암호화 시간의 최대값으로 설정된 Threshold를 넘지 않는 시간 범위 내에서 순차적으로 적용한다. 적용된 암호화에 사용될 암호화 Key 값은 다음 절에서 설명될 shifting 연산을 바탕으로 생성이 되며 현재 GOP에 대한 암호화 처리가 완료되면 다음 GOP에 대해서 동일한 과정을 반복한다.

Ⅳ. 실험 결과

제안하는 계층적 암호화 제어 기법의 성능 분석을 위하여 SVC의 최신 참조 소프트웨어인 JSVM 9.13을 사용하였다 [14]. 테스트 영상 시퀀스로는 City 및 Crew 영상을 사용하였고 이들을 JSVM 9.13으로 압축하여 생성된 비트스트림을 대상으로 실험을 실시하였다.

그림 6은 350 Kbps, 300 Kbps 등의 다양한 전송 대역폭을 만족시키기 위해 SVC 비트스트림으로부터 추출된 City 영상의 NAL unit들에 대해 SEED만을 적용하였을 때의 암호화 시간과 SEED만을 적용하였을 때의 평균 암호화 시간을 Threshold로 설정하여 제안된 계층적 암호화 기법을 적용하였을 때의 암호화 시간을 비교한 결과이다. 그림의 결과에서 알 수 있듯이 SEED 암호화를 모든 NAL unit들에 대해 일괄적으로 적용할 경우 하나의 GOP 내에 해당하는 NAL unit의 갯수가 많아질 경우 암호화 시간이 불안정하게 늘어나게 되어 일정한 암호화 시간을 유지 할 수 없게 된다. 이에 반하여 제안된 기법은 SEED 암호화에 의한 평균적 암호화 시간으로 설정된 Threshold에 매우 근접하게 암호화 시간을 안정적으로 일정하게 유지하도록 제어함을 할 수 있다.

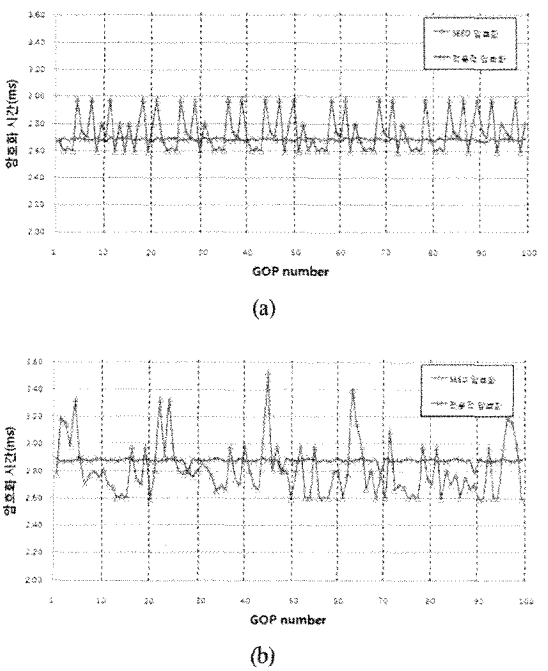
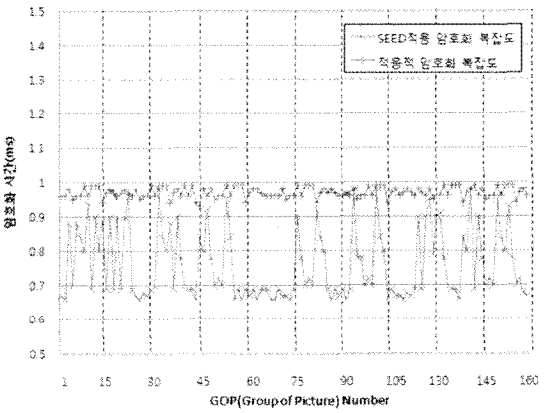
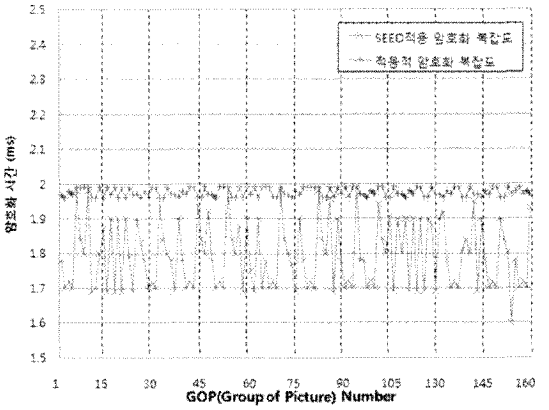


그림 6. City 영상에 대한 암호화 시간 비교: (a) 350 Kbps인 경우, (b) 300 Kbps인 경우
Fig. 6 Comparison of encryption time for City video sequence: (a) for 350 Kbps, (b) for 300 Kbps

그림 7은 City 영상에 대해 각 GOP 별 암호화 시간 Threshold를 각각 1ms와 2ms로 설정한 상태에서 SEED 암호화를 적용하였을 경우와 제안된 기법을 적용 하였을 경우의 Threshold 값을 만족시키는 제어 성능을 비교한 결과이다. SEED 암호화를 일괄적으로 적용할 경우 Threshold 이내에서 암호화 시간을 제어하기 위해 차 상위 계층의 NAL unit에 대해서는 SEED 암호화를 적용하지 못하여 전체적으로 Threshold 보다 훨씬 낮게 암호화 시간이 제어되는 결과를 나타낸다. 그러나, 제안된 기법의 경우 경량 암호화 기법들을 상위의 확장계층에 적용하기 때문에 보다 미세한 암호화 복잡도를 효과적으로 만족시킬 수 있다.



(a)



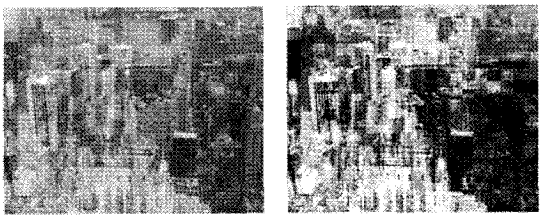
(b)

그림 7. City 영상에 대한 Threshold 값 제어 성능 비교: (a) 1ms Threshold, (b) 2ms Threshold
Fig. 7 Comparison of Threshold control performance for City video sequence: (a) 1ms Threshold, (b) 2ms Threshold

그림 8은 SEED만 적용한 경우와 제안된 기법을 적용한 경우의 암호화 강도를 시각적으로 비교하기 위해 암호화된 비디오 데이터에 대해 적합한 해독 Key를 확보하지 못한 상태에서 얻을 수 있는 화질을 비교한다.

Threshold=1ms Threshold=2ms

(a)



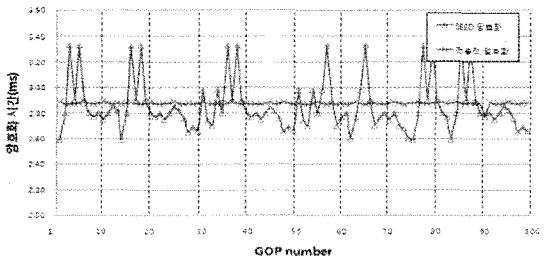
Threshold=1ms Threshold=2ms

(b)

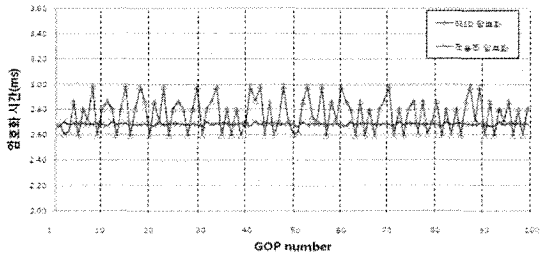
그그림 8. City 영상에 대한 암호화 화질 비교: (a) SEED만 적용, (b)제안된 암호화 기법 적용
Fig. 8 Comparison of encrypted visual quality for City video sequence: (a) applied SEED only, (b) applied proposed encryption method

그림 9는 350 Kbps, 300 Kbps 등의 다양한 전송 비트율에 의해 SVC 비트스트림으로부터 추출된 Crew 영상의 NAL unit들에 대해 SEED만을 적용하였을 때의 암호화 시간과 SEED만을 적용하였을 때의 평균 암호화 시간을 Threshold로 설정하여 제안된 계층적 암호화 기법을 적용하였을 때의 암호화 시간을 비교한 결과이다. 제안된 계층적 암호화 기법은 SEED 암호화에 의한 평균적 암호화 시간으로 설정된 Threshold에 매우 근접하게 암호화 시간을 일정하게 유지하도록 제어함을 할 수 있다.

그림 10은 Crew 영상에 대해 암호화된 비디오 데이터에 대해 적합한 해독 Key 를 확보하지 못한 상태에서 얻을 수 있는 화질을 비교한다. 그림 10에 보이듯이, 동일한 Threshold에 대해 SEED만을 적용한 경우보다 제안된 기법으로 암호화된 비디오 데이터에 대해 부적합한 해독 Key를 통해 접근을 시도할 경우 훨씬 왜곡된 화질을 얻게 된다.



(a)

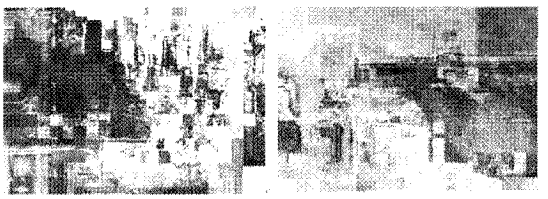


(b)

그림 9. Crew 영상에 대한 암호화 시간 비교: (a) 350 Kbps인 경우, (b) 300 Kbps인 경우
Fig. 9 Comparison of encryption time for Crew sequence: (a) for 350 Kbps, (b) for 300 Kbps

Threshold=1ms Threshold=2ms

(a)



Threshold=1ms Threshold=2ms

(b)

그림 10. Crew 영상에 대한 암호화 화질 비교: (a) SEED만 적용, (b)제안된 암호화 기법 적용
Fig. 10 Comparison of visual quality for Crew sequence: (a) SEED only, (b) proposed encryption method

V. 결 론

본 논문에서는 SVC의 비디오 계층간 차별화되는 중요도의 특성을 유지시키면서 일정한 수준으로 암호화 복잡도를 제어할 수 있는 계층적 암호화 기법을 제안하였다. 본 논문에서 제안된 SVC 적응적 암호화 기법 제어는 각 비디오 계층 마다 암호화 강도가 차별화 되는 암호화 기법을 적용하여 기존의 암호화보다 더 견고한 암호화를 걸어줌과 동시에 암호화 복잡도를 일정한 수준으로 유지할 수 있게 한다.

감사의 글

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행하였음. [KI001928, 유무선 환경의 개방형 IPTV (IPTV2.0) 기술개발]

참고문헌

[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, Sep. 2007.

[2] E. Lin, A. Eskicioglu, R. Lagendijk, and E. Delp, "Advances in digital video contgent protection," *Proc. of the IEEE,* vol. 93, no. 1, pp. 171-183, Jan. 2005.

[3] ISO/IEC JTC1/SC29/WG11 14496-13: Information technology generic coding of moving pictures and associated audio information－Part 13, "Intellectual property management and protection (IPMP) extensions," 2004.

[4] W. Buhse, and J. Meer, "The open mobile alliance (OMA) digital rights management," *IEEE Signal Processing Magazine,vol.* 24, no. 1,pp. 140-143, Jan. 2007.

[5] ISO/IEC JTC1/SC29/WG 1/N3853, JPSEC (JPEG 2000 Security) Final Draft of International Standard, Feb. 2006.

[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] B. Zhu, M. Feng, and S. Li, "An efficient key scheme for layered access control of MPEG-4 FGS video," in *Proc. IEEE Int. Conf. Multimedia and Expo,* pp. 443-446, June 2004.

[9] M. Smid, and D. Branstad, "Data Encryption Standard: past and future," *Proc. of the IEEE,* vol. 76, no. 5, pp. 550-559, May 1988.

[10] 한국정보보호센터 (KISA), 128비트 블록 암호 알고리듬 (SEED) 개발 및 분석 보고서, 1998년 12월.

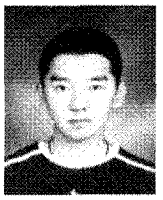
[11] Announcing the Advanced Encryption Standard (AES) (Nov. 2001). Available online at http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf.

[12] Y. Won, T. Bae, and Y. Ro, "Scalable protection and access control in full scalable video coding," *Lecture Notes in Computer Science,* vol. 3283, pp. 407-421, 2006.

[13] P. Kitos, N. Sklavos, and O. Koufopavlou, "Hardware implementation of the SAFER+ encryption algorithm for the Bluetooth system," *IEEE Int. Symp. Circuits and Systems,* vol. 4, pp. 878-881, May 2002.

[14] J. Reichel, H. Schwarz, and M. Wien, "Joint scalable video model (JSVM)," *Joint Video Team, Doc. JVT-X202,* Geneva, Switzerland, July 2007.

저자소개



황재형(Jae-hyung Hwang)

2006 연세대학교 컴퓨터정보통신공학부 학사
2010 연세대학교 컴퓨터정보통신공학부 석사
2010~현재 (주)어니언텍 연구원
※관심분야 : SVC, 영상 오류 제어, 영상통신, 영상보안

서광덕(Kwang-deok Seo)

1996 KAIST 전기및전자공학과 학사
1998 KAIST 전기및전자공학과 석사
2002 KAIST 전자전산학과 박사
2002~2005 LG전자 선임연구원
2005~현재 연세대학교 컴퓨터정보통신공학부 부교수
※관심분야: IPTV, SVC, 영상통신, 디지털 방송

정순흥(Soon-heung Jung)

2001 부산대학교 전자공학과 학사
2003 KAIST전자전산학과 석사
2003~2005 LG전자 주임연구원
2005~현재 ETRI IPTV연구부 선임연구원
※관심분야: IPTV, SVC, 영상부호화, 디지털방송