情 報 保 護 學 會 誌
第22卷 第3號, 2012. 5

아동보호를 위한 동영상 콘텐츠 정보보호 경량기법

나 재 훈*, 권 혁 찬*, 이 병 길*, 조 현 숙*

요 약

인터넷을 통하여 스트림 형태로 제공되는 동영상 콘텐츠에 대하여 아동의 접근을 손쉽게 제어 할 수 있는 방법은 콘텐츠에 암호화를 하는 것이다. 실시간성을 고려하여야 하는 콘텐츠들은 서버로부터 단말까지 콘텐츠의 전달 및 복호화하는 과정까지의 시간이 사전에 허용되는 한계치 내에서 서비스가 이루어지도록 설계가 되어야 한다. 이러한 요구사항에 걸맞는 암호화 방식은 부분(Selective) 암호화가 있으며, 동영상에 효율적으로 부분 암호화를 적용할 수 있도록 SVC (Scalable Video Coding) 표준이 권고 되고 있다. SVC 영상을 보호하기 위해서는 영상의 어떤 부분을 암호화 할 것인지 그리고 언제 암호화를 적용 할 것 인지를 고려해야 한다. 본 논문에서 제안한 기술은 미디어의 확장성을 유지하면서 계층별 접근 제어가 가능하며 영상의 재사용을 지원한다.

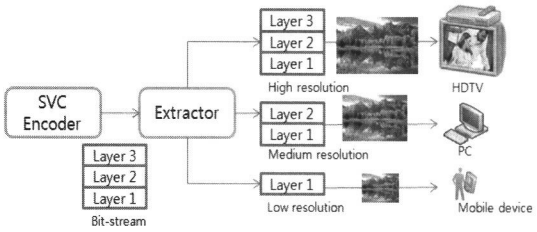
Ⅰ. 서 론

영상물 관련 아동보호 기술은 콘텐츠 자체에 대한 형태로 분류를 할 수가 있다. 정지영상과 동영상이 있고, 동영상은 방송용이 있고, 저장형이 있다. 저장형 동영상은 제작당시에 암호화를 하여서 전달되고 최종 사용자가 필요시에 복호화를 하여 사용할 수 있다는 관점에서는 비교적 아동보호가 용이하겠다고 생각 할 수 있다. 즉 저장된 영상물이 최종 사용자가 사용 권한이 있느냐를 결정할 수 있다면 아동들이 유해정보에 접근하는 것을 제어할 수 있는 수단으로 사용할 수 있다고 본다. 즉 아동들이 유해 콘텐츠에 접근하는 방법들은 많으나 본 논문에서는 인터넷을 통하여 스트리밍 기술로 전달되는 유해 동영상 서비스에 대한 접근을 보다 효율적으로 관리 할 수 있는 방법을 제시하고자 한다. 인터넷상에서 스트리밍 기법에 의한 동영상들은 패킷을 시스템의 버퍼를 통하여 화면에 표시를 하는 서비스이다. 그러므로 저장형 콘텐츠와는 달리 시간적 제한성을 갖는다. 이러한 문제는 서비스의 요소들인 서버와 네트워크 그리고 단말의 능력에 따라 다양한 양상을 보이고 있는데, 이것을 해결하고자 네트워크 전문가들은 많은 노력을 기울여 온 것이 사실이다. 그러나 점점 양질의 또 고급 서비스를 위하여 콘텐츠의 파일 용량이 점점 커지는 것이 일반적이 추세이며, 다양한 단말의 종류에 따라 별개의 서버를 구축 하는 것 또한 한계를 보이고 있고, 네트워크의 트래픽 또한 증가 추세 일변도를 보이고 있는 상황에서 기가비트 네트워크의 네트워크 구축을 국가적인 차원에서 검토를 하고 있는 것이 현재의 실정이다. 본 논문에서는 이렇듯 증가하는 단말의 종류 그리고 네트워크의 트래픽의 증가를 조율하면서 유해 콘텐츠에 대한 아동 접근은 제어할 수 있는 방안을 검토하고자 한다. 즉 동영상이 인터넷에서 방영이 되는 단계와 저장되어 재전송을 하는 단계에서 암호화된 콘텐츠를 복호와 트랜스코딩 그리고 재 암호화 하는 복잡한 과정을 거치지 않고, [그림 1]과 같이 단일한 콘텐츠를 활용하여 복수개의 단말에 맞는 동영상 서비스를 할 수 있는 서비스 구조에서 종단간 (End-to-End) 정보보호 서비스를 제공할 수 있는 메카니즘을 소개하며 이러한 기술은 유해 동영상 콘텐츠로부터 아동을 보호하는 기술로 활용할 수 있다.

SVC는 한번의 코딩으로 다양한 디바이스에 적용이 가능한 OSMU (One Source Multi Use) 기능을 지원하며 단말과 네트워크의 상태에 맞도록 미디어의 형식변환(transcoding)을 지원하는 스마트TV를 위한 코덱으

본 연구는 방송통신위원회 및 정보통신기술협회의 표준개발지원사업(2012-PK10-008:유무선 환경의 이종 웹 정보보호 표준개발)의 일환으로 수행되었습니다.

* 한국전자통신연구원 사이버융합보안연구단 ({jhnah, hckwon, bglee, hscho}@etri.re.kr)



〔그림 1〕 SVC 기반의 비디오 서비스의 예

로 등장하고 있다.

현재 JPEG2000, MPEG-4 FGS, SVC 등 다양한 형태의 스케일러블 미디어가 존재한다. JPEG2000[1]은 웨이블릿 방식의 스케일러블 이미지 코딩 방법으로 다중의 해상도로 변환을 지원하고 있다. MPEG-4 FGS은 SNR 및 시간적 확장성(temporal scalability)을 지원하는 코딩방법이다. 그러나 MPEG-4 FGS는 스케일러블 타입과 코딩 효율성 측면에 한계가 있어 그리 많이 사용되지 못하고 있다.

SVC[2]는 ITU-T 및 ISO/IEC가 공동 작업을 통해 표준화한 H.264/MPEG-4 AVC 표준의 Annex G에 정의된 표준이다. SVC는 기본 레이어 (base layer)와 추가적인 확장 레이어 (enhancement layer)로 영상을 압축하여 해상도, 화질, 프레임률을 자유로이 변환 할 수 있는 구조를 갖는다. [그림 1]은 SVC 기반의 비디오 서비스 중 공간 확장성을 지원하는 서비스의 예를 보여준다.

본 논문의 구성은 다음과 같다. 2장은 SVC의 3가지 암호화 방식을 분석하며, 3장에서는 하이브리드 방식의 계층별 접근제어 기술 및 성능분석을 제시하고 4장에서 결론을 맺는다.

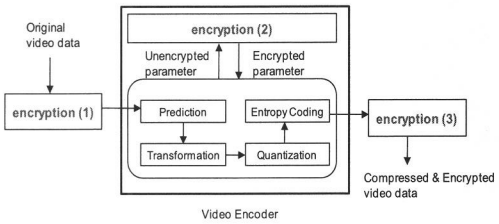
Ⅱ. 계층적 영상 암호화 방식

SVC 영상을 보호하기 위해서는 두 가지 이슈를 고려해야 한다.

첫 번째는, 영상의 어떤 부분을 암호화 할 것인지를 고려해야 한다. 비디오 데이터는 보통 대용량이며 고속의 전송률을 요구하기 때문에 비디오 전체를 암호화 하는 방식은 비디오 스트리밍 데이터에 적합하지 않다. 특히 SVC의 경우 H.264 등 확장성이 없는 코덱에 비해 데이터의 사이즈가 매우 크기 때문에 영상의 암호화를 최소화 하는 작업이 필요하다. 본 논문에서는 이를 위해 선택적 암호화를 적용한다.

두 번째는, 언제 영상에 암호를 적용 할 것 인지를 고려해야 한다. [3]은 암호화를 적용하는 시점을 기준으로 다음의 3가지 종류로 암호화 기술을 분류하였다.

(1) Precomreppsion 방식의 암호화: 인코딩 이전에 암호화 적용 (2) Incomreppsion 방식의 암호화: 인코딩 과정에서 암호화 적용 (3) Postcomreppsion 방식의 암호화: 인코딩 이후에 암호화 적용



〔그림 2〕 암호화 적용 시점에 따른 분류

상기의 3가지 암호화 방식을 분석하기 위해 본 논문에서는 [3]에서 제시한 평가기준의 일부를 활용하였다. [3]에서 제시한 평가 기준 중 본 논문에서 사용한 항목은 다음과 같다.

(1) Encryption ratio: 전체 비디오 사이즈 대비 암호화 영역의 비율. 보안 수준이 유지된다면 ratio가 작을수록 좋음 (2) Compression Friendliness: 암호화를 적용해도 영상압축률에 큰 변화가 없다면 compression friendly함 (3) Format Compliance: 암호화된 데이터를 표준 디코더가 복호화 없이 디코딩 할 수 있다면 format compliance를 만족.

본 논문에서는 다음의 1가지 평가항목을 추가로 정의하여 분석하였다. (4) Security Module Independence: 인코더와 보안모듈, 디코더와 보안모듈의 독립성 여부.

2.1 Precompression 방식의 암호화 기술 분석

이 방식은 암호화를 통해 변경된 영상을 인코딩하기 때문에 디코더에 의해 충분히 인식이 가능하므로 format compliant 하다. 또한 보안 모듈의 독립성도 보장한다. 그러나 이 방식은 인코딩 전에 암호를 적용하여 원 영상이 왜곡된 후에 인코딩이 수행되므로 압축률이 크게 떨어지는 단점이 있다. 이 방식은 일반적인 IPTV, 스마트TV 등의 영상서비스에 적용하기는 어려우며 매우 특별한 응용에 제한적으로 적용이 가능하다.

예를 들어, CCTV 상에서의 프라이버시 마스킹 작업을 하는 경우 입력영상을 인코딩하기 전에 사람의 얼굴부분을 인식하여 암호화 하는 등 특수한 응용에 활용이 가능하다. Precompression 방식에서 선택적으로 암호화가 가능한 영역은 정지 영상 기준으로 이미지의 특정 부분의 암호화가 가능할 것이다.

2.2 Incompression 방식의 암호화 기술 분석

이 방식의 가장 큰 장점은 format compliance를 준수한다는 것이다. 즉, 암호화된 영상을 디코더가 복호화 없이 왜곡된 형태로 디코딩 및 플레이가 가능하다. 이 경우 암호 영역에 따라 영상의 왜곡도가 달라질 것이다. 따라서 보안콘텐츠에 대한 사용자의 구매욕을 자극하는 새로운 형태의 비즈니스 모델 적용도 가능하다. 이 방식의 또 다른 장점은 인코딩 과정에서 암호화를 적용하기 때문에 특정한 파라미터를 선택하여 암호화를 적용할 수 있어, 암호화 영역을 최소화하고 전체적인 보안 오버헤드를 크게 줄일 수 있다는 장점이 있다. 인코딩이 끝난 이후에는 파라미터 등 특정 정보의 추출에 어려움이 있기 때문이다.

이 방식의 가장 큰 단점은 보안 모듈의 독립성을 제공하지 못한다는 것이다. 인코더와 디코더에 보안모듈 탑재를 위해 인코더 및 디코더의 변경이 필요하다. 또한 보안 모듈의 업데이트를 실시할 때에도 인코더 및 디코더의 변경이 필요하다는 단점이 있다. 그러나 경량의 암호를 적용할 수 있다는 점과 format compliance 를 만족할 수 있다는 장점이 있어 실시간 미디어 전송기술로 충분히 활용이 가능할 것으로 보인다.

Incompression 방식에서 선택적으로 암호화가 가능한 영역은 Texture sign, MVD(Motion Vector Difference) 값 등이 있다.

2.3 Postcompression 방식의 암호화 기술 분석

이 방식의 가장 큰 장점은 보안 모듈의 독립성을 제공한다는 것이다. 인코딩이 완료된 후 암호화를 적용하므로 인코더와 보안모듈의 분리가 가능하다. 이 방식은 format compliance는 만족하지 않는다. 인코딩 이후 암호화가 적용되므로 표준 디코더가 암호화된 영상을 인식할 수 없기 때문이다. 또한 인코딩 후 암호화를 적용하기 때문에 압축률에 영향을 주지 않아 compression friendly 한 암호 방식이기도 하다. 선택적으로 암호화가 가능한 영역은 PPS(Picture Parameter Set), SPS (Sequence Parameter Set), IDR(Instantaneous Decoding Refresh Picture) 등의 영역이 있다. 그러나 incompression 방식에 비해서는 암호화 영역을 섬세하게 적용하지는 못한다. [표 1]은 3가지 방식을 비교하였다.

〔표 1〕 3가지 비디오 암호화 방식의 비교

암호방식 / 평가기준	Precompression 방식	Incompression 방식	Postcompression 방식
Encryption ratio	만족못함	매우만족	만족
Compression Friendliness	만족못함	매우만족	매우만족
Format compliance	만족못함	만족	만족못함
Security module independence	만족	만족못함	만족
Selective encryption area	정지영상 단위의 특정 영역	IPM, MVD, Texture sign Residual coefficient 등	SPS, PPS, IDR 등

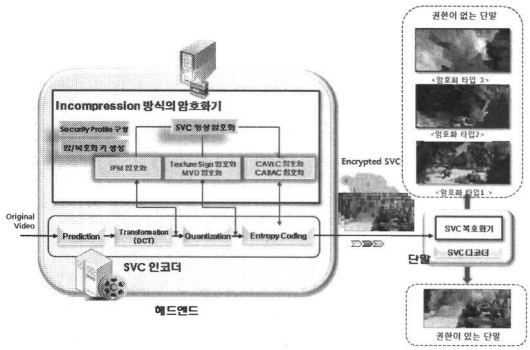
Ⅲ. 하이브리드 방식의 암호화 기술

3.1 하이브리드 방식의 SVC 미디어 보호기술

본 논문에서는 SVC 미디어의 하이브리드 방식의 계층별 접근 제어 방식을 제안한다. 하이브리드 방식은 incompression 방식과 postcompression 방식을 혼용한 방식이다. incompression 방식은 암호화 영역을 최소화하여 영상 암호화 성능을 매우 높일 수 있고, format compliance를 만족하여 암호화된 형태로 표준 디코더에 디스플레이 할 수 있다는 장점이 있다. 따라서 실시간 방송 보호를 위해 incompression 방식을 채택하였다.

[그림 3]은 하이브리드 방식의 스케일러블 영상보호 기술 중 실시간 전송구간의 구조를 보여준다. 실시간 전송을 위해 SVC 영상 암호화기는 영상의 인코딩이 진행되는 동안 영상의 복구를 위해 필요한 특정 파라미터를 암호화 한다.(incompression 방식)

본 논문에서는 암호영역에 따른 암호화 type을 정의하여 사업자의 비즈니스 모델에 따라 차등적용할 수 있도록 하였다. [그림 3]에서 각 암호화 타입별로 영상의



〔그림 3〕 하이브리드 방식의 스케일러블 영상 보호 기술 (실시간전송 구간)

왜곡도가 차이가 나는 것을 볼 수 있다.

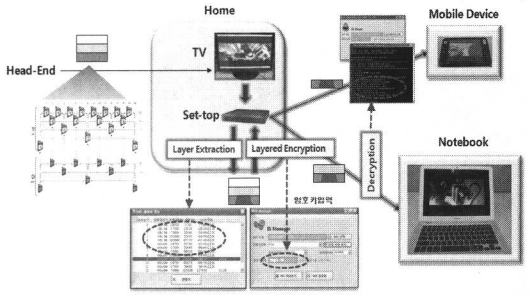
각 암호화 타입 및 암호영역은 다음과 같다.

- 타입 0 : 암호화 없음
- 타입 1 : IPM(Intra Prediction Mode) + Texture sign
- 타입 2 : MVD(Motion Vector Difference)
- 타입 3 : IPM + Texture sign + MVD

Postcompression 방식은 format compliance는 만족하지 못하지만 security module independence를 만족하는 장점이 있어 수신한 방송영상을 사용자의 다른 단말로 재사용하기 위한 재사용/재전송 기술로 채택하였다.

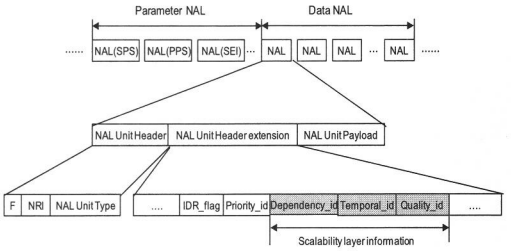
[그림 4]는 하이브리드 방식의 스케일러블 영상보호 기술 중 비실시간 전송구간의 구조를 보여준다. 비실시간 전송이란 [그림 3]과 같이 실시간으로 전송된 영상을 단말에 저장한 후 사용자의 다른 단말에서 시청하기 위해 비실시간으로 재전송하는 서비스를 말한다. 일단 인코딩이 된 후 이므로 incompression 방식의 적용은 불가능하다. 비실시간 재사용을 위해 본 논문은 postcompression 방식을 사용하였다. 우선 [그림 3]에서 수신한 영상의 암호화가 풀린 후에 재사용을 위해 저장하는 경우 추가로 postcompression 방식의 암호화가 적용된다. 본 기술은 SVC의 NAL 유닛 레벨에서 암호화하는 방식을 사용하였으며, NAL 데이터 중 IDR (Instantaneous Decoding Refresh Picture), SPS (Sequence Parameter Set), PPS(Picture Parameter Set) 데이터를 암호화 하였다.

[그림 4]와 같이 셋톱에서 영상을 수신하여 재생되는 동안 이를 재사용 하기위해 저장하라는 요청을 받으면 SVC 영상을 대상 단말에 맞게 형식변환(transcoding) 하고 추출된 레이어를 NAL기반으로 암호화 한 후 이



〔그림 4〕 하이브리드 방식의 스케일러블 영상 보호 기술 (비실시간 재전송 구간)

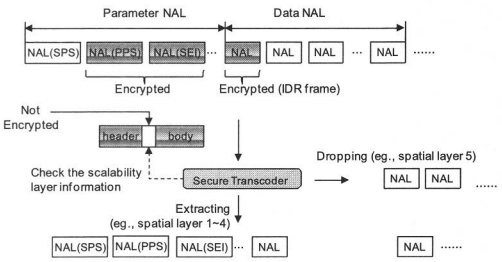
를 대상 단말로 전달하게 된다. [그림 5]는 암호화 적용 대상인 NAL의 구조를 보여준다.



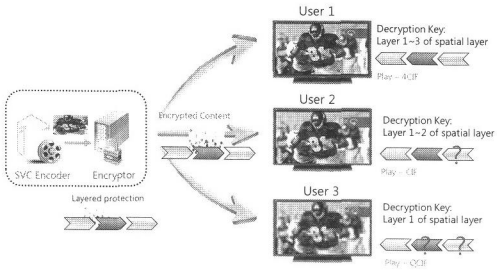
〔그림 5〕 SVC의 NAL 데이터 유닛

[그림 5]의 NAL Unit Header extension은 H.264 형식 중 SVC를 위한 확장 헤더에 포함된 정보로 각기 spatial, temporal, quality 레이어 정보가 포함되어 있다. 본 기술에서는 이 정보를 암호화하지 않기 때문에 암호화된 형태로 특정 레이어를 추출하는 것이 가능하며 이를 통해 영상의 형식변환이 가능하게 된다. NAL 암호화를 적용하는 경우 암호화된 영상의 형식변환의 예를 [그림 6]에서 볼 수 있다.

본 기술은 또한 SVC의 계층별 접근제어를 위해 계층별로 암호화 키를 차등 적용하여 배포하는 기술을 적용하였다.



〔그림 6〕 NAL 암호화 적용 영상의 형식변환 과정



〔그림 7〕 계층별 레이어 보호 기술 적용을 통한 차등화된 영상서비스의 예 및 결과화면 (공간 확장성에 적용)

[그림 7]에서 볼 수 있듯이 각 사용하는 보유한 키 소유 권한에 따라 차등화된 영상서비스를 제공받게 된다. 예를 들어, 레이어 1~3까지의 복호화키를 보유한 사용자는 HD급의 영상 시청이 가능하며, Layer 1 키만 보유한 User3의 경우 CIF급 영상만의 시청이 가능하다. 동일한 영상에 대해 권한보유여부에 따라 차등화된 서비스를 제공하는 것이다. User3는 추가 비용을 지불하여 Layer 2~3에 대한 복호화 키를 습득한 후 HD급 영상의 시청이 가능하게 된다.

3.2 성능분석

본 논문에서는 각각의 암호화(incompression 및 postcompression 방식)를 경량화 하기 위해 특정한 정보만을 추출하여 암호화 하였다. 3장에서 기술한 바와 같이 incompression 방식의 경우, IPM, Texture sign, MVD, Entropy coding 파라미터 등을 암호화 타입분류에 따라 조합하여 암호화를 수행하였으며, Postcompression 방식의 경우, IDR, SPS, PPS NAL을 암호화 하였다.

선택적 암호화를 적용하여 보안 모듈을 경량화 한 결과 보안 오버헤드는 3%이내의 좋은 성능을 보였다.

[표 2]와 [표 3]은 각각 선택적 암호화 적용에 따른 incompression 방식과 postcompression 방식의 보안 오버헤드를 보여준다. [표 2]의 경우 보안 오버헤드 값은 암호화를 적용하지 않은 암호타입 0에 비해 암호화를 적용한 경우의 초당평균 디코딩 프레임수의 감소 비율을 계산하여 산정하였다. 디코더의 성능은 초당 디코딩 프레임 수에 의해 좌우된다. 초당 디코딩 프레임수가 높을수록 더 좋은 디코더의 성능을 보이는 것이다.

〔표 2〕 Incompression 방식의 보안 오버헤드

테스트영상 (해상도)	암호타입	초당평균 디코딩 프레임수	보안 오버헤드
1280*960	0	20.18	-
	1	20.16	0.10%
	2	19.93	1.24%
	3	19.9	1.39%
640*480	0	80.86	-
	1	80.76	0.12%
	2	79.44	1.76%
	3	79.34	1.88%

〔표 3〕 Postcompression 방식의 보안 오버헤드

테스트영상 (해상도)	암호 유/무	시간 (ms)		보안 오버헤드
1280*960	X	1프레임 평균 디코딩 시간	49.56	
	O	1프레임 평균 복호화 시간	0.922	1.86%
640*480	X	1프레임 평균 디코딩 시간	12.36	
	O	1프레임 평균 복호화 시간	0.375	3.03%

성능결과를 요약하면 Incompression 방식의 경우 HD급 및 SD 급 영상 모두 2% 이내의 보안 오버헤드를, Postcompression 방식의 경우, 약 3% 이내의 오버헤드를 보였다.

3.3 선행연구와의 비교

기존의 영상콘텐츠 보호기술인 CAS, DRM 등은 인코딩이 완료된 영상에 대해 암호화를 적용한다. 만약 SVC와 같은 스케일러블 영상을 기존 방식으로 암호화하는 경우 이후 암호화된 영상의 형식변환(계층적 구조)과 추가적인 암호화가 불가능하다. 암호화된 영상데이터에서 레이어 정보의 확인 및 추출이 불가능하기 때문이다. 그러나 본 논문의 기술은 인코딩 과정에서 암호화를 하거나 NAL 단위로 레이어 정보를 보존하며 암호화를 하기 때문에 암호화된 영상의 형식변환과 추가적인 암호화가 가능하다. CAS, DRM 등의 기존 기술에 SVC를 포함한 스케일러블 미디어를 지원하기 위해 본 기술의 적용이 가능할 것으로 예상된다.

선행연구로 [4]는 incompression 방식의 암호 기술이며, H.264/AVC 영상에 대해 IPM값과 MVD값을 암호화하는 방식을 사용하였다. 그러나 IPM과 MVD 값만을 암호화하는 경우 replacement attack 즉 표준 디코더의 도움을 받아 상당부분의 원영상을 복원할 수 있다는

단점이 있다. 이는 기준이 되는 키 프레임 즉 IDR 프레임이 암호화되지 않기 때문에 움직임 벡터에 해당하는 MVD 값을 유추할 수 있기 때문이다.

[7]은 postcompression 방식의 암호화 방식을 제안하였다. [7]에서는 SPS, PPS 헤더, IDR 프레임, 매크로블록의 슬라이스 헤더와 DC 계수의 차분 값 등을 암호화 하였다. 본 논문에서 제안한 IDR, SPS, PPS 값에 암호화를 적용한 경우와 유사한 효과를 기대할 수 있다.

아직까지 Incompression과 Postcompression 을 혼용하여 실시간 및 비실시간 재사용을 지원하는 보안 기술에 대한 연구 사례는 없다.

본 논문의 제안방식은 [표 1]의 Incompression 방식과 Postcompression 방식을 수용하면서 실시간 및 비실시간 콘텐츠 전송에 대한 보안성 및 접근제어 기능을 추가로 제공하는 장점을 갖는다.

Ⅳ. 결 론

본 논문에서 제시한 동영상 정보보호 경량기법은 콘텐츠 유통과정에서 유해성 등급판정이 내려진 모든 콘텐츠를 암호화 하여 방영을 하면서 이에 대한 권한인증(성인인증)을 받은 사용자들에게 서비스 제공 및 이용자 측면에서 효율적으로 시청을 할 수 있도록 기술적 성능 개선된 (오버헤드 3%이내) 방법임을 보였다.

또한 성인인증에 있어서 보다 나은 인증방법에 대한 연구가 병행되어야 한다. 즉 단순 아이디/패스워드 보다, 또 핸드폰, 인증서, e-메일 인증보다 더 강인한 메카니즘이 개발이 되어서 아동에게 유해한 콘텐츠에 대한 접근 제어가 보다 강력하게 관리되어야 한다.

참고문헌

[1] ITU-T, Information technology -JPEG 2000 image coding system: Secure JPEG 2000, ITU-T Recommendation T.807, 2006.

[2] ITU-T, Advanced video coding for generic audiovisual services, ITU-T Recommendation H.264, 2007.

[3] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, J.-J. Quisquater, Overview on selective encryption of image and video: challenges and perspectives, EURASIP Journal on Information Security, Volume 2008, Jan. 2008.

[4] S.Lian, J. Sun, G.Liu, "Efficient Video Encryption Scheme based on Advanced Video Coding", Multimedia Tools and Applications, vol. 38, Issue 1, May 2008.

[5] Yong Geun Won, Tae Meon Bae, and Young Man Ro, "Scalable Protection and Access Control in Full Scalable Video Coding", IWDW 2006, LNCS 4283, 2006.

[6] Su-Wan Park, Sang-Uk Shin, "Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding(SVC)", 2008 Fourth International Conference on Networked Computing and Advanced Information Management, 2008.

[7] Tuo Shi, Brian King, and Paul Salama, "Selective encryption for H.264/AVC Video Coding", Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 6072, 2006.

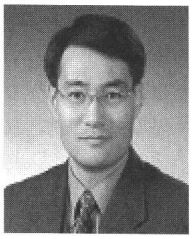
[8] Wu, C.-P. and Kuo, C.-C. J., "Efficient Multimedia Encryption via Entropy Codec Design," Proceedings of SPIE Security and Watermarking of Multimedia Content III, Volume 4314, San Jose, CA, January 2001.

[9] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming Enabling Transcoding Without Decryption, IEEE Inter. Conf. on Image Processing (ICIP), Sept. 2001.

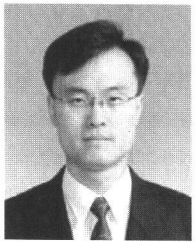
[10] Nithin M Thomas, Damien Lefol, David R Bull, David Redmil, "A Novel Secure H.264 Transcoder Using Selective Encryption", 2007 ICIP, 2007.

[11] Chunhua Li et. al, NAL Level Encryption for Scalable Video Coding, PCM 2008, LNCS 5353, 2008.

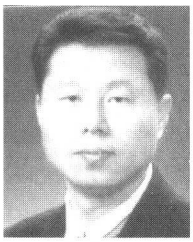
〈著者紹介〉



나 재 훈 (Jae Hoon Nah)
종신회원
1985년: 중앙대학교 컴퓨터공학과 졸업
1987년: 중앙대학교 컴퓨터공학과 석사
2005년: 한국외국어대학교 전자정보공학과 박사
1987년~현재: 한국전자통신연구원 사이버융합보안연구단 전문위원/책임연구원
2009년~현재: ITU-T SG17 Q7 Rapporteur
2011년~현재: 한국정보보호학회 학회지 편집위원장
<관심분야> IPv6/MIPv6, P2P, IPTV, 매시업 웹 보안



권 혁 찬 (Hyeokchan Kwon)
정회원
1994년: 서원대학교 전자계산학과 공학사
1996년: 충남대학교 전산학과 석사
2001년: 충남대학교 컴퓨터과학과 박사
2001년~현재: 한국전자통신연구원 스마트객체보안연구팀 책임연구원



이 병 길 (Byung-Gil Lee)
정회원
1991년: 경북대학교 전자공학과 (학사)
1993년: 경북대학교 전자공학과 (석사)
2003년: 경북대학교 전자공학과 (박사)
2001년~현재: 한국전자통신연구원 융합보안연구팀 팀장/책임연구원
<관심분야> IT융합 보안기술, 통합, 보안관제, 콘텐츠 및 웹보안

조 현 숙 (Hyun Sook Cho)
종신회원
1979년: 전남대학교 수학교육과 졸업
1989년: 충북대학교 컴퓨터과학과 석사
2001년: 충북대학교 컴퓨터과학과 박사
1982년~현재: 한국전자통신연구원 사이버융합보안연구단 단장/책임연구원
<관심분야> 암호학, 보안 프로토콜, 네트워크 보안