情報保護學會論文誌
第16卷 第3號, 2006. 6

암호화된 SVC 비트스트림에서 조건적 접근제어 방법*

원 용 근†, 배 태 면, 노 용 만‡
한국정보통신대학교, 영상 및 비디오 시스템 연구실

Conditional Access Control for Encrypted SVC Bitstream*

Yong-Geun Won,† Tae-Meon Bae, Yong-Man Ro‡
IVY Lab., Information and Communications University (ICU)

요 약

본 논문에서는 암호화된 SVC (Scalable video coding) 비트스트림을 이용한 조건적 접근제어 방법을 제안한다. 제안한 방법은 새로운 비디오 코딩 기법인 SVC에 적합한 암호화와 암호화된 SVC 비트스트림에서 비트스트림 추출 (Extraction) 후 복호화를 통해 효과적인 조건적 접근제어(Conditional Access Control) 방법을 제공하는데 그 목적이 있다. 제안하는 SVC 조건적 접근제어는 SVC 비트스트림의 암호화에 대한 요구사항을 분석하여 SVC 코딩기법에 적합하게 암호화를 시행하고 암호화된 SVC 비트스트림의 적응변환 수행 시 비트스트림 추출과 선택적 복호화를 통해 수행 된다. 본 논문은 SVC 비트스트림에 대해 암호화를 시행한 후 다양한 비디오로 접근을 시도하는 실험을 통하여 제안한 방법의 유효성을 검증하였다.

ABSTRACT

In this paper, we propose a method of conditional access control for encrypted SVC(scalable video coding) bitstream. The main purpose of the proposition is to provide a SVC suitable encryption algorithm and a efficient method for conditional access control using encrypted SVC bitstream. We analyzed requirements for conditional access control of a SVC bitstream. And based on the analysis, we proposed encryption algorithm suitable for SVC bitstream and a method of conditional access control of the encryped bitstream. The proposed conditional access control for encrypted SVC bitstream is performed by bitsream extraction and selective decryption. We verified the usefulness of the proposed method through experiments.

Keywords : *conditional access control, scalable protection, scalable video coding, video encryption*

Ⅰ. 서 론

최근의 단말 기기와 네트워크의 발달은 다양한 사용자 환경을 가져다주었다. 단말의 성능, 네크워크의 속도, 유저 선호도는 모두 최근의 발달로 인해 만들어진 다양한 사용자 환경이며 이러한 다양한 사용자 환경으로 인해 콘텐츠에서 최상의 Quality of Service (QoS)를 보장하기 위한 개별 단말기기로의 적응변환은 많은 관심을 끌고 있다.

기존의 비디오 코딩기술은 적응변환에 있어서 문제점을 가지고 있었다. 즉, 각 단말이 가진 환경에 맞도

접수일: 2006년 2월 8일; 채택일: 2006년 5월 31일
* 본 연구는 삼성전자-ICU 공동연구센터 과제의 지원으로 수행되었습니다.
† 주저자, gamja0000@icu.ac.kr
‡ 교신저자, yro@icu.ac.kr

록 적응하기 위해서 매번 재 인코딩을 하거나, 미리 특정 적응변환을 위한 다양한 비디오를 적응서버에서 보유하고 있어야 했는데 이러한 기존의 적응 과정은 적응서버에 많은 부하를 준다. 이러한 적응과정의 문제를 극복하기 위해 다양한 단말에 쉽게 적응할 수 있는 스케일러블 코딩 방법이 연구되기 시작하였다.

스케일러블 코딩 기법은 한번 인코딩 후 다양한 단말에 적응 시 재인코딩 없이 적응환경에 맞도록 비트스트림을 추출(Extraction)을 통하여 디코딩함으로써 다양한 비디오를 생성할 수 있다. 현재 스케일러블 코딩 기법을 사용한 다양한 코딩 기법들이 제안되었는데 대표적인 기법이 스케일러블 이미지 코딩 기법인 JPEG2000과 스케일러블 비디오 코딩 기법인 MPEG-4 FGS이다. MPEG-4 FGS는 비디오 코딩기법 중 효과적으로 스케일러빌리티를 제공하는 비디오 코딩 기법이었으나 품질과 시간의 제한된 스케일러빌리티를 제공하며 충분한 코딩 효율을 제공하지 못하였다. 따라서 MPEG 과 ITU-T 의 Joint Video Team (JVT)에서는 더욱 우수한 스케일러블 코딩 기법에 대해 논의 하였고 그 결과 시간, 공간, 품질의 완전한 스케일러빌리티를 제공하며 충분한 코딩 효율을 가지는 스케일러블 코딩 기법인 Scalable Video Coding (SVC)을 발표하여 현재 계속해서 표준화를 진행하고 있다.

유연한 적응변환을 위한 스케일러블 콘텐츠 코딩 기술과 함께 현재 많은 연구가 이루어지는 분야가 콘텐츠 보호 및 관리 기술이다. 현재의 콘텐츠 분배와 소비는 네트워크의 발달과 더불어 자유롭게 이루어지고 있으며 이러한 자유로운 콘텐츠 분배와 소비환경으로 콘텐츠 보호 및 관리 시스템에 대해 활발하게 연구하고 있다. 최근 MPEG 에서는 MPEG-2 와 MPEG-4에 대한 Digital Right Management (DRM) 프레임워크인 Intellectual Property Management and Protection (IPMP-X) 를 표준화 했고[1,2] Open Mobile Alliance (OMA) 에서도 무선 시스템을 위한 DRM 시스템을 도입했다.[3] 또한 스케일러블 이미지 코딩인 JPEG2000 에서도 파트 8에 JPSEC 이라는 보호 프레임워크를 구성하여 콘텐츠 보호에 대한 연구를 진행하고 있다.[4]

콘텐츠 보호 시스템에서 콘텐츠 암호화 기술은 가장 기본적이며 중요한 기술이다. 특별히 멀티미디어 콘텐츠는 복잡한 인코딩/디코딩 과정을 가지고 있으며 비교적 큰 데이터 사이즈를 가지고 있기 때문에 일반적으로 중요한 부분에 대해 부분 암호화(selective algorithm)를 하거나 인코딩 기법을 변경하는 방법(scrambling)을 사용한다. 따라서 멀티미디어 콘텐츠의 암호화는 일반적인 데이터와는 다른 암호화 요구사항을 고려하여 연구되고 있다.[5,6]

본 논문에서는 SVC로 부호화된 스케일러블 콘텐츠를 보호하기 위한 암호화 방법과 암호화된 SVC 비트스트림을 소비하기 위한 조건적 접근제어 방법을 제안한다. 현재의 비디오 콘텐츠 암호화 방법은 SVC의 비트스트림 확장구조와 스케일러빌리티 변환을 위한 비트스트림 추출과정을 고려하고 있지 않기 때문에 기존의 암호화 방법을 적용할 경우 암호화 후 비트스트림을 추출시 SVC의 스케일러빌리티를 유지할 수 없다. 이러한 문제를 해결하기 위해 기존의 비디오 콘텐츠 암호화 방법을 바탕으로 SVC 콘텐츠의 특징을 분석하여 SVC 비트스트림 확장구조와 비트스트림 추출과정에 적용할 수 있는 암호화 방법을 제안한다.

또한 제안된 방법에 의거하여 계층적으로 암호화된 SVC 비트스트림은 비트스트림 추출 과정을 통해 스케일러빌리티가 변환된 다양한 비디오 콘텐츠로 소비 될 수 있는데 이러한 계층적으로 암호화된 비디오 콘텐츠로 접근 시 특정 접근조건에 해당하는 비디오 콘텐츠로만 접근 할 수 있도록 하는 조건적 접근제어 방법이 필요하다. 이를 위해 일반적인 스케일러블 코딩 기법의 접근제어 방법을 토대로 SVC 콘텐츠의 스케일러빌리티 확장구조에 적합한 조건적 접근제어 방법을 제안하였고 실험을 통하여 제안한 방법의 유효성을 보였다.

II. 관련 연구

1. SVC 부호화기 구조

SVC는 MPEG-4 AVC /H.264 기반의 새로운 스케일러블 코딩 기법이다.[7] SVC는 시간, 공간, 품질의 완벽한 스케일러빌리티를 제공하면서도 우수한 코딩 효율을 보장한다. SVC 비트스트림은 기본레이어(base-layer)와 확장레이어(enhancement-layer)를 가지고 있으며 기본레이어를 바탕으로 확장레이어를 추가하여 다양한 스케일러빌리티를 가진 비디오 스트림을 구성하는 구조로 구성되어 다양한 시간, 공간, 품질을 가진 비디오를 생성할 수 있다. 기본레이어는 MPEG-4 AVC/H.264코딩 기법을 사용하여 인코딩하며 공간 스케일러빌리티를 제공하기 위해 확장레이어는 기본레이어보다 높은 해상도의 영

상을 인코딩하는데, 이때 Inter-Layer 코딩 기법을 통해 코딩효율을 높인다. 시간 스케일러빌리티는 hierarchical B picture기법으로 제공하며, 선택사항으로 Motion Compensated Temporal Filtering (MCTF)기법을 확장레이어에서 적용이 가능하다. 품질 스케일러빌리티는 Fine Granularity Scalability (FGS)와 Coarse Granularity Scalability(CGS) 의 기법을 사용하여 공간 레이어 각각에 설정된 품질 레이어 수만큼 추가하여 구성된다. 그림 1은 기본레이어와 확장레이어로 구성된 대표적인 SVC 비트스트림을 보여주고 있으며 최하위의 기본레이어를 기반으로 품질, 공간, 시간 측면으로 확장을 한다. 각 확장은 특별한 순서와 방향을 가지고 있는데 이는 인코딩 기법에 기인한다.

SVC는 다양한 전송환경에 쉬운 콘텐츠의 적응을 위해 비트스트림을 Video Coding Layer (VCL)과 Network Abstraction Layer (NAL)으로 분리하여 구성한다.[8,9] VCL에서는 비디오 데이터의 내용을 효율적으로 표현하기 위해 기술되며 NAL은 다양한 네트워크와 저장장치에 전달하기 위해 적절한 헤더 정보를 제공하고 데이터를 형성하기 위해 기술된다. NAL unit 에 담겨있는 모든 데이터는 정수값으로 저장되며 하나의 NAL unit 에는 비트스트림 시스템과 패킷 기반 시스템 모두에 적용가능한 일반적인 형식으로 기술된다.

SVC 에서는 이러한 NAL 구조로 비트스트림을 구성하여 제공하며 공간, 시간, 품질의 스케일러빌리티 각각에 대한 기본레이어와 단위 확장레이어는 NAL unit 으로 구분된다. 그림 2는 SVC 에서 NAL로 구성된 비트스트림의 구조와 NAL의 세부 구조를 보여준다. 그림에 보듯이 NAL unit 은 파라메터 NAL 과 데이터 NAL 으로 구성되고 확장데이터 NAL은 시간, 공간, 품질의 확장에 대한 정보를 가지고 들어 있다.

2. 기존의 비디오 콘텐츠 암호화 기법

비디오 암호화 기법은 현재 다양하게 제안되어 왔으며, 가장 단순한 방법으로 Naïve algorithm이 있다. Naïve algorithm은 DES (data encryption standards)나 AES (advanced encryption standards)같은 일반적인 데이터 암호화 기법을 사용하여 인코딩된 모든 비트스트림을 데이터처럼 암호화 하는 방법이다.[10] 간단하게 구현이 가능하지만 높은 연산량이 필요하기 때문에 전체시스템의 복잡도를 높이며 에러 복원이 어렵다. 또 다른 방법으로 Selective algorithm이 있다. Selective algorithm은 전체가 아닌 데이터의 중요한 부분만 일반적인 데이터 암호화 기법을 사용하여 암호화 하는 방법이다. 일반적으로 비디오 데이터는 데이타량이 크며 복호화 연산량이 많기 때문에 비디오 데이터의 특정 부분만을 암호화하는 Selective algorithm이 많이 사용된다. 암호화 대상이 되는 부분은 비디오 콘텐츠의 특성에 맞는 다양한 방법들이 제안되고 있다. Selective algorithm의 가장 기본적인 방법에는 데이터의 헤더와 파라메터를 암호화하는 방법이 있다. 그러나 데이터의 헤더와 파라메터는 실제 데이터를 기반으로 추측할 수 있기 때문에 공격에 취약하다. 따라서 일반적으로 콘텐츠의 데이터를 직접 암호화 하는 방법이 많이 제안되고 있다. 비디오 콘텐츠에서 I-frame 은 영상의 기본 정보를 가진 프레임이기 때문에 I-frame은 좋은 암호화 대상이 된다. 그러나 B 나 P프레임의 I-block 을 통해 일정 정보가 누출될 수 있기 때문에 I-frame 과 I-block 을 모두 암호화 하는 방법이 제안되었다.[10] 또한 부분적 암호화의 방법으로 DC 계수값이나 저주파수 계수값을 암호화 하거나 모션 벡터 값을 이용하는 방법[11,12]등의 비디오 콘텐츠의 특성을 이용한 방법이 se-

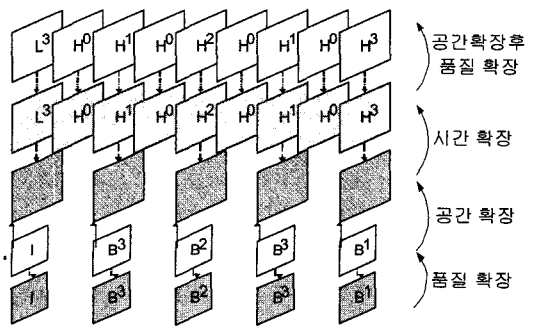


그림 1. SVC 비트스트림의 시간, 공간, 품질의 확장 구조

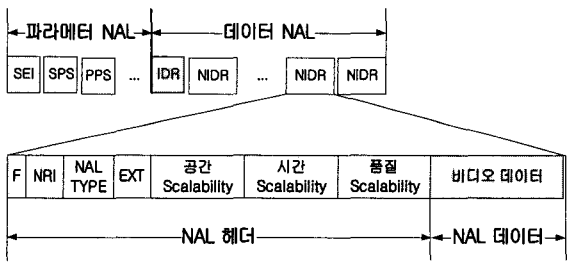


그림 2. SVC 비트스트림과 NAL 구조

lective algorithm으로 제안된 방법이다. Selective algorithm에서 암호화 영역에 대한 연구와 함께 암호화 방법에 대한 연구도 이루어지고 있는데 대표적인 방법으로 실시간 전송을 위한 빠른 연산을 위해 일반적인 데이터 암호화 방법을 적용하는 대신 sign 비트에 대해 임의적으로 반전시키는 방법이 그것이다.[13] 일반적인 데이터를 특정 영역에 맞도록 암호화 하는 대신 인코딩 파라메터를 숨기거나 인코딩 테이블을 치환하는 등의 방법도 다양한 코딩 특성에 맞추어 제안되고 있으며 통상 Scrambling algorithm이라고 한다. Scrambling algorithm방법은 인코딩 기법에 변화를 주기 때문에 압축효율의 저하나 예상치 못한 오류를 유발할 수 있다. 따라서 Scrambling algorithm 을 적용하기 위해서는 인코더에 대한 깊은 이해가 필요하다. 대표적인 방법으로 Zig-Zag 스캔 순서를 무작위로 치환 하는 방법, 모션벡터나 DCT 계수값을 무작위로 치환 하는 방법[14], VLC (variable length coding) 코드를 치환하는 방법[15] 등이 있다.

SVC에서는 높은 인코딩 복잡도와 비트스트림의 NAL unit 구성, 데이터의 다양한 구성(텍스쳐, 모션벡터, FGS)을 가지기 때문에 이러한 SVC 비트스트림 데이터의 특징을 만족할 수 있는 암호화 기법이 제안되어야 한다.

3. 기존의 스케일러블 콘텐츠의 조건적접근제어 방법

기존의 스케일러블 코딩 기법들도 코딩의 특징을 이용하여 조건적 접근제어를 수행하였다. JPEG2000 에서는 그림 3과 같이 웨이블랫 코딩 기법을 사용하며 이를 통한 암호화로 조건적 접근제어를 수행한다. 웨이브렛 코딩 기법은 고주파영역(high-frequency)과 저주파(low-frequency) 영역으로 이미지의 영역이 나누므로 각각의 나누어진 주파수(frequency)에 따라 다른 키로 암호화 하여 공간 스케일러빌리티에 따른 조건적 접근제어를 구성 할 수 있다.[4]

MPEG-4 FGS에서는 제공하는 PSNR과 비트율에 따라 임의로 확장 영역을 구분하여 조건적 접근제어를 수행한다.[4] 그림 4는 MPEG-4 FGS 의 SNR로 확장하는 비트스트림에서 PSNR과 비트율로 구분하여 조건적 접근제어를 구성하는 그림이다. PSNR과 비트율은 개별적으로 구분되는데 중첩되는 영역을 seg(PSNR, 비트율)로 설정하여 각각 다른 키로 암호화 하여 네트워크와 유저의 PSNR요구에 부합하도록 복수의 키를 제공하여 조건적 접근제어를 구성한다. 여기에서 중첩 영역 seg(PSNR, 비트율)는 MPEG-4 FGS가 확장할 수 있는 확장의 기본 단위가 된다. 즉, 낮은seg(PSNR, 비트율)를 기반으로 높은 seg(PSNR, 비트율)가 추가되어 확장 된다. 만약 그림 4에서 유저의 네트워크가 비트율4 를 지원하고 유저가 PSNR 2를 원한다면 seg(1,1), seg(1,2), seg(2,2), seg(2,3), seg(2,4) 까지 복호화 할 수 있는 5개의 키가 전송되어 네트워크와 유저의 요구를 모두 만족하는 비디오를 디코딩 할 수 있다.

SVC에서는 시간, 공간, 품질의 모든 스케일러빌리티를 제공하므로 시간, 공간, 품질 각각의 스케일러빌리티에 대한 조건적 접근제어가 가능해야 한다. 또한 시간, 공간, 품질 각각의 스케일러빌리티는 기본레이어를 기반으로 확장되는 형태를 구성하기 위해 각각 다른 코딩 기법을 사용하므로 스케일러빌리티에 따라 데이터 형식도 틀리게 구성된다. 조건적 접근제어를 위해서는 확장 단위마다 모두 암호화를 적용하고 접근 허용 조건에 따라 선택적으로 복호화를 수행해야하므로 비트스트림을 구성하는 모든 데이터 형식이 암호화 되어야 한다. 마지막으로 MPEG-4 FGS에서는 비트율과 PSNR에 대한 중첩되는 영역을 확장의 기본단

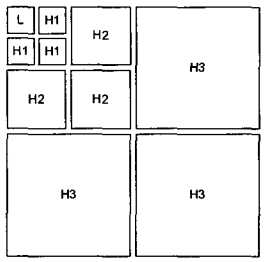


그림 3. 웨이블렛 기반의 JPEG2000에서 조건적 접근제어를 위한 주파수 영역의 구분

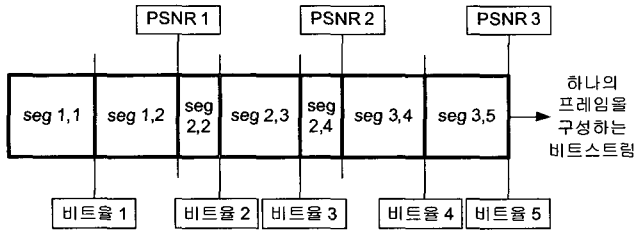


그림 4. MPEG-4 FGS 에서 조건적 접근제어를 위한 비트스트림 구성

위로 삼았으나 SVC에서는 NAL unit이 각각의 스케일러빌리티에 대한 확장의 기본단위가 되므로 이러한 NAL unit에 대한 특성과 구성을 반영해야 한다.

Ⅲ. 제안하는 조건적 접근제어 방법

1. SVC 암호화 요구사항

SVC 암호시스템은 인코더와 비트스트림 추출기, 디코더에 암호화기와 복호화기가 삽입되어 구성되며 비디오 암호화를 위한 요구사항과 SVC의 특징을 바탕으로 SVC 암호시스템에서 암호화를 위한 요구사항을 도출할 수 있다. SVC 암호화 요구사항은 다음과 같다. 먼저 SVC는 기존의 비디오 코딩 기법에 비해 상당한 복잡도와 디코딩 자원을 요구하므로 실시간 디코딩을 위한 암호화를 위해 SVC 디코더에 가능한 영향을 주지 않는 경량(Light-weight) 암호화 기법이 적용 되어야 한다. 둘째, SVC는 기본레이어를 기반으로 확장하는 구조를 가지고 있는데 이러한 확장은 레이어 단위이거나 비트단위 확장이 이루어진다. 따라서 암호화는 이러한 확장의 단위를 고려하여야 한다. 확장의 단위가 고려된 암호화는 SVC가 가지는 비트스트림 추출과정에 효과적으로 적용할 수 있다. 마지막으로 복호화가 이루어지지 않고 디코딩시에 잡음 영상을 보여줄 수 있도록 SVC의 형식에 맞는 암호화가 시행되어야 한다. 특히 SVC는 시간, 공간, 품질의 스케일러빌리티에 따라 각기 다른 코딩기법을 사용하므로 이에 적합한 암호화가 수행되어야 한다. 그림 5에는 SVC 암호시스템에서 암호화 요구사항을 보여준다.

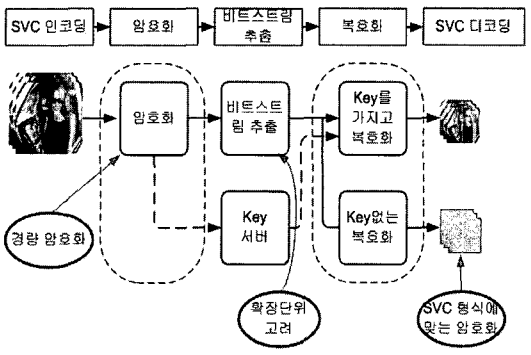


그림 5. SVC 보호 시스템에서 암호화 요구사항

2. 제안하는 SVC 비트스트림의 암호화 방법

제안된 암호화 방법은 비디오 데이터만을 경량 암호화 방법을 사용하여 인코딩이 끝나는 CABAC (Context based binary arithmetic coding) 단계에서 암호화 하는 방법이다.

SVC 암호화는 전체 시스템에 큰 무리를 주지 않는 경량(Light-weight) 암호화 방법이 제안 되어야 한다. SVC는 우수한 코딩 효율과 완전한 스케일러빌리티 제공을 위해 복잡한 인코딩 연산을 수행한다. 따라서 복잡한 연산을 요구하지 않는 경량 암호화 방법을 사용하여 암호화해야 한다. 경량 암호화 방법은 현재 주요한 비디오 암호화 요구사항인 실시간 디코딩을 가능하게 하므로 SVC 암호화에 있어서도 중요한 요구사항이 된다.

또한 SVC의 암호화 방법은 다양한 코딩 기법으로 적용된 데이터들을 모두 암호화 할 수 있어야 한다. 이미 실시간 디코딩을 목적으로 텍스쳐와 모션벡터를 동시에 경량 암호화를 통해 암호화 하는 방법은 제안되었는데 이때 텍스쳐 와 모션벡터 를 동시에 암호화 하는 이유는 텍스쳐만을 대상으로 한다면 잡음의 효율이 떨어지므로 모션벡터를 같이 암호화 대상으로 하여 잡음의 효율을 높이기 위함이다.[11] SVC는 텍스쳐 데이터와 모션벡터 데이터뿐 아니라 FGS 데이터에 대해서도 모두 암호화가 적용되어야 한다. 왜냐하면 SVC는 텍스쳐, 모션벡터, FGS등의 다양한 데이터 형식을 가지고 있으므로 특정 데이터만을 부분적 암호화로 암호화 수행 시에 상대적으로 암호화 되지 않는 영역이 생기기 때문이다. SVC는 기본레이어를 바탕으로 확장하기 때문에 기본레이어가 가장 중요한 정보이다. 특히 기본레이어는 기존의 방법인 MPEG-4 AVC/H.264코딩 기법을 사용하여 인코딩하며 기본레이어가 가지고 있는 텍스쳐 정보만을 암호화 해도 충분한 암호화 효과를 볼 수 있다. 그러나 텍스쳐 정보는 기본레이어와 공간 확장레이어, 시간 확장레이어에 존재 하는데 공간 확장레이어와 시간 확장레이어에서는 비교적 낮은 비율로 존재하기 때문에 텍스쳐 정보만 암호화 하는 경우 확장레이어의 암호화는 충분하지 않다. 또한 품질 확장레이어인 FGS 레이어는 텍스쳐 정보를 이용하지만 FGS 고유의 코딩 기법을 사용하므로 암호화 기법은 FGS 고유의 코딩 기법에 적용 가능해야 한다. 따라서 SVC의 확장 구조를 고려한 다양한 확장레이어들을 모두 암호화 할 수 있는 방법이 제안되어야 한다.

특히 FGS 레이어는 레이어 단위로 확장하는 다른 스케일러빌리티 레이어와 다른 구조를 가지고 있

는데 비트스트림 추출이 레이어 단위로 일어날 뿐 아니라 레이어 내에 목표비트율에 맞도록 비트플레인 단위로도 비트스트림 추출이 일어난다. 따라서 제안하는 암호화 방법은 암호화 후 레이어 내의 어떠한 지점에서도 비트스트림 추출이 가능해야한다.

위의 요구사항에 만족하도록 SVC를 암호화 하기 위해서는 먼저 비트스트림에서 데이터를 가진 NAL 만을 구분 해야 하는데 이는 NAL 헤더에서 nal_unit_type을 참조하여 구분한다.[7] 암호화 대상이 되는 nal_unit_type은 기본레이어의 NAL unit 에 해당하는 coded slice of IDR picture, coded slice of non-IDR picture와 확장레이어의 NAL unit 에 해당하는 coded slice of non-IDR picture in scalable extension, coded slice of IDR picture in scalable extension의 네 가지가 있으며 이들은 NAL 헤더에서 제공되는 nal_unit_type으로 구분 할 수 있다.

구분된 비디오 데이터는 텍스쳐, FGS, 모션벡터 데이터를 가지고 있으며 이 값들은 모두 인코더의 마지막 단계인 CABAC 단계에서 sign 과 absolute 값으로 구분되어 기록된다. 특히 경량 암호화를 위해 이 값들 중 sign 값을 임의로 발생시킨 랜덤 값과 XOR 연산을 통하여 임의로 반전 하는데 비디오 데이터 중 시각적인 효과가 가장 큰 sign 값만을 암호화하기 때문에 암호화는 인코더의 복잡도에 큰 영향을 주지 않으면서 큰 시각적 잡음의 효과를 가질 수 있고 XOR 암호화는 다시 XOR을 통해 복호화 가능하기 때문에 디코더의 복잡도에도 큰 영향을 주지 않는다. 본 방법의 암호학적 강인도는 XOR연산의 대상이 되는 랜덤 스트림의 길이에 따라 더욱 강인해 질수 있다.

그림 6에는 하나의 데이터 NAL unit 에서 텍스쳐, FGS, 모션벡터 값들의 sign 값을 추출하고, SEED 값으로 Pseudo-Random-Number Generator를 통해 발생시킨 랜덤값과 XOR 연산을 통해 암호화하는 방법을 보여주고 있다. 랜덤값을 발생시키는데 사용된 SEED 값은 신뢰할 수 있는 암호화 방법으로 암호화되어 비트스트림에 삽입되어 전송되는데 이때 암호화 된 SEED는 비트스트림의 데이터에 직접 추가되거나 SVC에서 제공하는 확장 신호로 전송될 수 있다. 이때 SEED를 다시 암호화 하는 이유는 SVC 비디오 스트림에서 NAL단위 슬라이스로 암호화 시 매번 동일 키로 암호화 한다면 특정 NAL의 키가 공격을 통해 노출 될 때 전체 비디오 스트림이 취약해 지는 문제가 있다. 그러나 암호화에 사용된 SEED를 매 NAL단위마다 틀리게 하고 이를 미리 지정된 키로 암호화 한다면 암호화 된 특정 NAL의 SEED가 노출 되더라도 전체 비디오 스트림은 보호 될 수 있으며 복호화 시에도 하나의 키로 전체 비디오 스트림을 복호화 가능하다.

복호화 단에서는 SEED값을 복호화 하여 랜덤값을 다시 발생시키고 XOR 연산을 통해 데이터를 복호화 한다.

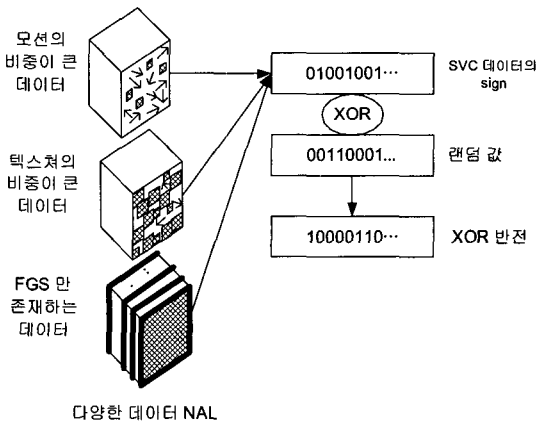


그림 6. 다양한 데이터 형식에 모두 적용할 수 있는 랜덤값과 XOR 연산을 통해 잡음을 넣는 방법.

3. 제안하는 SVC비트스트림의 조건적 접근제어 방법

스케일러블 미디어에서 조건적 접근제어는 어떤 스케일러빌리티의 조합으로도 접근을 가능하게 하는 기술이다. 스케일러블 미디어는 기본 확장 단위를 통하여 순차적, 단계적으로 확장이 이루어 지므로 조건적 접근제어에 적용 가능한 암호화는 기본 확장단위로 암호화 해야 한다.

SVC는 공간, 시간, 품질의 스케일러빌리티를 가지고 각 스케일러빌리티를 단계적으로 확장할 수 있도록 레이어와 레벨로 나누어 단계적으로 스케일러빌리티를 확장한다. 그리고 레이어, 레벨은 NAL unit으로 정의되므로 NAL unit은 SVC의 확장의 기본 단위가 된다. 따라서 제안하는 조건적 접근제어 방법은 기본 확장 단위인 NAL unit의 각각에 암호화를 하고 접근을 원하는 비디오로 확장하는데 필요한 NAL unit만을 복호화하여 접근한다. 이때 NAL unit의 스케일러빌리티에 따라 다른 키를 할당하여 암호화하는데 그림 7에서와 같이 최하위 공간영역을 기반으로 시간레벨과 품질레이어에 따라 반복되므로,

반복되는 NAL unit들을 각각 같은 키로 암호화한다. 따라서 제안하는 조건적 접근제어방법을 위해서는 하나의 비디오로 확장하는데 사용되는 모든 NAL unit을 복호화 해야 하므로 복수의 키가 필요하다.

스케일러빌리티 정보에 따라 개별 NAL에 대한 암호화를 위해서는 해당 NAL unit의 스케일러빌리티 정보가 필요한데, 이러한 NAL 스케일러빌리티 정보는 NAL unit 의 NAL header에 dependent_ID,Temporal_level, quality_layer로 명시되어 있다. 따라서 스케일러빌리티 정보를 추출하여 같은 스케일러빌리티 정보를 가진 NAL unit에 같은 키를 할당하여 효과적으로 접근제어를 위한 암호화를 구성할 수 있다.

만일 유저가 s 공간, t 시간, q 품질의 스케일러빌리를 가지는 비디오에 접근하고자 한다면 비트스트림 추출기는 원본 비트스트림을 s 공간, t 시간, q 품질의 스케일러빌리티를 가지는 비트스트림을 추출한다. 그리고 유저는 복호화 하는데 필요한 복수의 키를 수령 받아 복호화를 수행하고 원하는 비디오에 접근을 하게 된다.

그림 7은 제안하는 조건적 접근제어의 예이다. 여기서 사용된 SVC 비트스트림은 2개의 공간 (공간 0, 공간 1), 2개의 시간 (시간 0, 시간 1) 레벨, 2개의 품질 (품질 0, 품질 1)의 레이어를 가지고 있다. 조건적 접근제어를 위해서는 가장 낮은 공간레이어의 기본레이어를 기준으로 확장에 사용되는 모든 NAL들을 다른 키로 암호화한다. 그림 7에서 암호화에 사용하는 키는 Key(공간, 시간, 품질)로 표현 하였다. 즉 Key(s, t, q)는 스케일러빌리티 정보가 공간레이어는 s, 시간레이어는 t, 그리고 품질 레이어는 q인 NAL을 복호화 하는데 필요한 하나의 키를 나타낸다. 그림 7에서는 하나의 기본레이어 와 5개의 확장을 할 수 있는 확장레이어 가 있으므로 키는 모두 6개가 필요하다.

제안한 조건적 접근제어 방법에 따라 공간, 시간, 품질의 스케일러빌리티를 가지는 SVC 비트스트림을 모두 암호화 하는데 사용되는 키의 개수와, 이때 특정 스케일러빌리티를 가지는 비디오에 접근하기 위해 필요로 하는 키들의 조합은 SVC 비트스트림의 스케일러빌리티 정보로부터 알 수가 있다.

먼저 제안한 방법에 대한 수식을 세우기 위해 먼저 용어에 대해 정의 한다.

NS: 공간 레이어의 수

NQ: 품질 레이어의 수

NT: 시간 레벨의 수

NQ_s: s 번째 공간 레이어의 품질 레이어의 수

NT_s: s 번째 공간 레이어의 시간 레벨의 수

SVC는 공간, 품질, 시간레이어를 자유롭게 설정할 수 있다. 즉 공간 레이어에 따라 품질 레이어의 개수는 달라질 수 있고, 또한 공간 레이어에 따라 시간 레벨의 구성도 다를 수 있다.

식 (1)은 특정 스케일러빌리티 정보를 가진 비트스트림을 암호화 하는데 사용되는 모든 키의 개수를 계산 하는 식이다. SVC에서 품질레이어와 시간 레이어는 공간레이어에 밀접한 연관성이 있으므로 키의 개수를 계산할 때에는 이러한 연관성이 고려된다.

$$Key = \sum_{s=1}^{NS} (NQ_s \times NT_s) \tag{1}$$

식 (2)는 s 공간레이어, t 시간레이어, q 품질레

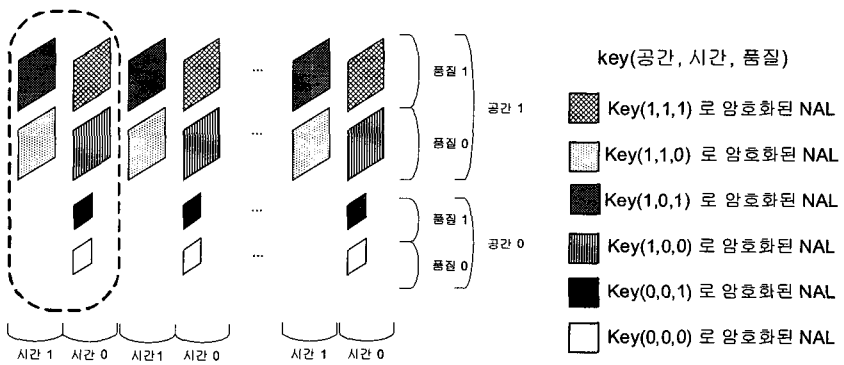


그림 7. 조건적 접근제어를 위한 NAL 단위 암호화

이어에 접근하기 위해 필요한 키 조합을 나타내고 있다.

$$KEYSET_{s,t,q} = \left\{ Key(l,m,n) \middle| \begin{array}{l} 0 \le l \le s,\ 0 \le m \le \min(t, NT_s), \\ \text{if } l = s \text{ then } 0 \le n \le q \\ \text{else } 0 \le n \le NQ_s \end{array} \right\} \quad (2)$$

공간레이어 는 0부터 s까지 접근이 가능하다. 그러나 시간레이어로 접근은 각 공간레이어 마다 가장 높은 시간레이어가 틀릴 수 있고, 이는 최초 파라메터에 전적으로 의존하므로 접근을 원하는 시간레이어와 해당 공간레이어의 가장 높은 시간레이어을 고려해야 한다. 또한 공간영역으로 확장시 높은 품질의 비트스트림을 얻기 위해서 하위 공간영역의 모든 품질확장을 수행한다. 이는 선택적 사항이나 본 수식과 실험에서는 공간 확장시 하위 공간의 모든 품질 레이어가 필요한 것으로 설정 하였다.

표 1은 특정 스케일러빌리티를 가진 암호화된 SVC 비디오에 접근하기 위해 필요한 키 조합을 식 (2)를 통해 계산한 예로써, 그림 7을 참고하여 2개의 공간레이어, 각각의 공간레이어 마다 2개의 품질 레이어, 2개의 시간레이어를 가진 SVC 비트스트림의 각 접근경우에 대해 필요한 키 조합을 표시하였다.

표 1. 그림 7의 비트스트림 구조에서 특정 시간, 공간, 품질의 스케일러빌리티에 접근하기 위해 필요한 키 조합

시간 / 공간(품질)		시간0	시간1
공간0	품질0	{k(0,0,0)}	Not exist
	품질1	{key(0,0,0),key(0,0,1)}	Not exist
공간1	품질0	{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)}
	품질1	{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(1,0,1) key(1,1,1),key(1,1,0)}

Ⅳ. 실 험

제안한 방법의 검증을 위해 SVC 암호화와 조건적 접근제어에 관한 실험을 수행하였다. 실험은 JSVM (joint scalable video model)2.0으로 수행하였고 테스트 영상은 SVC 테스트 영상인 "BUS"를 사용하였다. 각각의 데이터 형식에 대한 암호화시 시각적 잡음정도와 PSNR로 제안한 방법의 유효성을 검증 하였다. 그리고 제안한 조건적 접근제어 방법에 대해 접근 조건을 두고 다양한 접근권한에 따른 다양한 키의 조합으로 접근을 시도하였다.

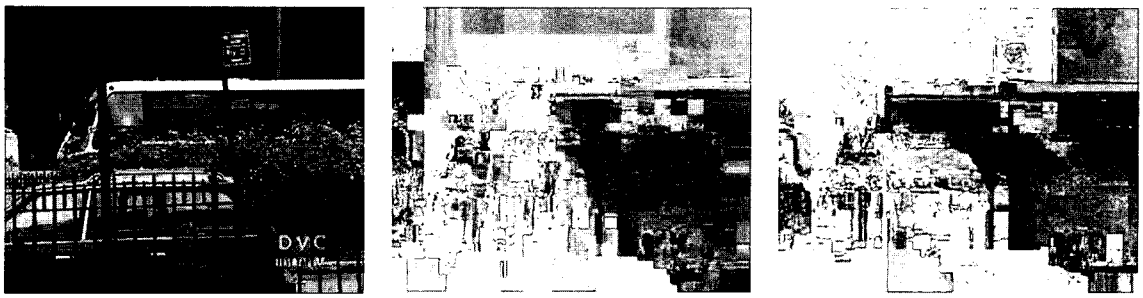
1. 제안하는 방법의 암호화 방법 실험

암호화는 NAL unit의 텍스쳐, 모션벡터, FGS 데이터를 각각 암호화한 경우와 세가지 데이터를 모두 암호화 했을 때를 비교하였다. 그림 8과 표 2는 각 경우의 시각적 잡음효과를 보여주는 영상과 PSNR 결과를 각각 보여주고 있다. 표 2에서와 같이 텍스쳐만 암호화 했을 때 더 낮은 PSNR, 즉 더 좋은 암호화 결과를 얻었으나 물체의 윤곽이 유지되므로 실제의 시각적 잡음은 텍스쳐와 모션벡터를 같이 암호화했을 때가 더 효과적이다. 한 비디오 시퀀스에서 첫 번째 프레임은 모션벡터가 없이 텍스쳐로만 이루어 져 있으므로 모션벡터만 암호화 했을 때에는 첫 번째 프레임은 암호화 되지 않는다.

표 2. 다양한 데이터 형식에 암호화를 적용한 PSNR 결과

암호화 대상	PSNR Y	PSNR U	PSNR V
없음	28.9284	38.6394	39.3413
텍스쳐+모션벡터+FGS	7.5795	26.6918	29.5904
텍스쳐	6.1385	26.4774	30.3554
모션벡터	15.0754	32.9199	32.2043
FGS	23.5881	35.5645	35.2926

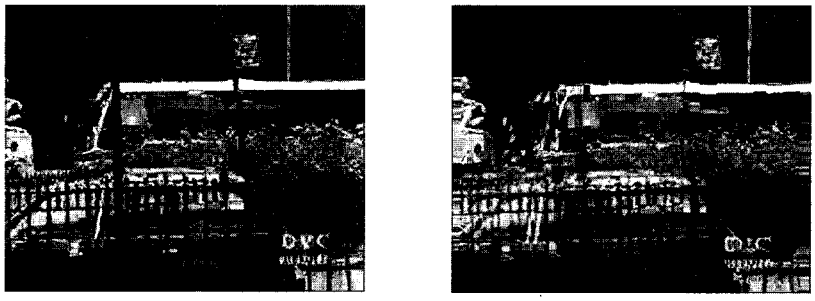
그림 9는 기본레이어가 암호화 되지 않을때 텍스쳐만 암호화한 경우와 텍스쳐와 모션벡터 를 동시에 암호화한 결과를 보여주고 있으며, 표 3은 이에 해당하는 PSNR 결과이다. 실험결과에서 보듯이 텍스쳐 만 암호화시 기본레이어가 암호화 되지 않으면 시각적 잡음 정도가 상당 수준 낮아지며 이를 보완하기 위해 모션벡터도 암호화해야 하는 것을 알 수 있다.



(a) 암호화되지 않은 비디오 (b)텍스처 + 모션벡터 + FGS 암호화 (c) 텍스처 암호화

(d) 모션벡터 암호화 (e) FGS 암호화

그림 8. 암호화 되지 않은 비디오와 텍스쳐와 모션벡터, FGS 의 암호화에 따른 시각적 잡음



(a) 텍스쳐만 암호화 된 경우 (b) 텍스쳐와 모션벡터가 암호화 된 경우

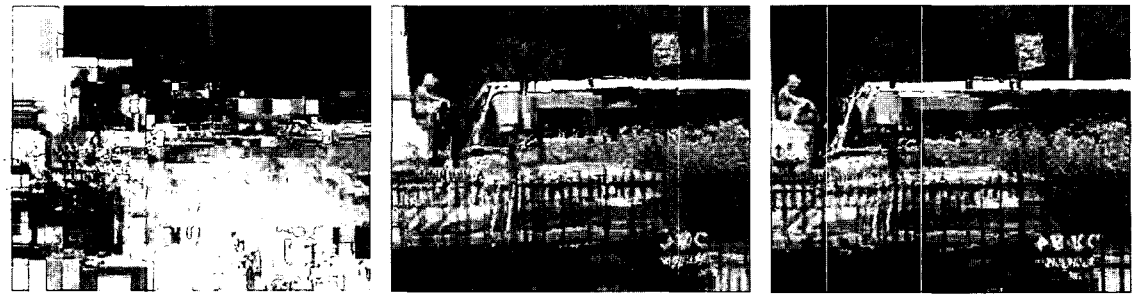
그림 9. 기본레이어가 암호화 되지 않았을 경우 텍스쳐와 모션벡터에 따른 시각적 잡음

표 3. 기본레이어가 암호화 되지 않았을 경우 텍스쳐만 암호화 한 경우와 텍스쳐+모션벡터를 암호화 한 경우에 대한 PSNR 결과

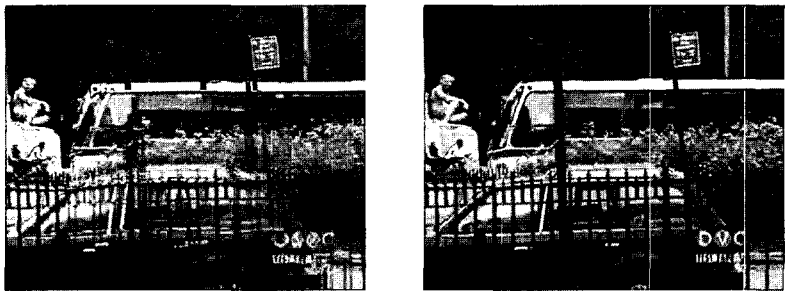
암호화 대상	PSNR Y	PSNR U	PSNR V
텍스쳐	21.7585	37.3057	38.0141
텍스쳐 + 모션벡터	18.8713	35.7341	35.4734

2. 조건적 접근제어 실험

제안하는 조건적 접근제어 방법의 검증을 위해 암호화된 SVC 비트스트림에서 접근 조건을 설정하고 다양한 접근권한으로 접근을 시도하였다. 실험에 사용된 비디오 영상은 두개의 공간(QCIF, CIF), 두 개의 시간(15 fps, 30 fps), 두 개의 품질(base, FGS)로 스케일러빌러티를 가지도록 SVC로 인코딩되고, 제안한 방법으로 암호화되었다. 암호화된 비트스트림은 설



(a) case 1 (b) case 2 (c) case 3



(d) case 4 (e) case 5

그림 10. 접근 조건에 대해 설정된 접근권한에 따른 키의 조합으로 접근을 시도한 영상

정된 접근 조건인 CIF, 30fps, 기본품질로 비트스트림 추출 과정을 거친다. 추출된 비트스트림은 암호화된 상태이며 표 4의 각 접근권한이 가지고 있는 키 조합으로 복호화를 시도하여 디코딩을 하였다.

표 4는 접근조건과 다섯 가지의 서로 다른 접근권한을 보여주고 있다. case 5는 설정된 접근조건을 모두 복호화 할 수 있는 경우로 디코딩을 통해 잡음이 없는 영상을 얻을 수 있고 case 1,2,3,4는 접근 조건을 만족하는 키를 모두 갖추지 못한 경우로 그림 10에서 보듯이 접근조건에 따라 부분적으로 복호화 되지 않아서 각각 상이한 잡음을 가진 영상을 보여주게 된다.

표 4. 설정된 접근 조건에 따른 키 할당

접근조건	case	접근권한	키 할당
CIF 30fps base	1	접근권한 없음	No key
	2	QCIF, 15fps, Base	{key(0,0,0)}
	3	QCIF, 15fps, FGS	{key(0,0,0), key(0,0,1)}
	4	CIF, 15fps, Base	{key(0,0,0), key(0,0,1), key(1,0,0)}
	5	CIF, 30fps, Base	{key(0,0,0), key(0,0,1), key(1,0,0) ,key(1,1,0)}

표 5는 표 4에서 설정한 접근조건과 접근권한에 대하여 두 가지 품질을 계산하여 비교하고 있다. 접근권한이 보장하는 품질은 접근 권한이 가질 수 있는 최대 품질을 의미하며 원본비디오와 SVC로 인코딩된 접근권한의 스케일러빌리티를 가지는 비디오 간의 PSNR값이다. 원본 비디오는 접근권한의 스케일러빌리티를 가지는 비디오와 PSNR을 계산하기 위해 동일한 레졸루션과 프레임율로 변환되고 계산된다. 특히 표 5에서 case4와 case5의 경우 공간(CIF)과 품질(Base) 스케일러빌리티는 동일하고 시간 스케일러빌리티가 각각 15fps 와 30fps인 경우인데 SVC의 Hierarchical B-Picuture는 15fps에서 프레임간 예측을 통해 30fps로 확장하는 구조를 가지므로 case 5의 경우는 case 4에 비해 미세하게 낮은 PSNR 값을 보여주게 된다. 접근 조건으로 강제 접근 시 품질은 접근조건을 접근권한에 해당하는 키로 강제 접근시킨 비디오와 원본비디오 간의 PSNR 값이다. 원본 비디오는 접근조건에 해당하는 스케일러빌리티로 변환되고 계산된다. 본 예에서는 case 5는 모든 접근조건을 복호화 할 수 있는 키를 가지고 있는 접근권한이기 때문에 모든 레이어가 정

상적으로 복호화 된 경우이며 case 5의 접근권한이 보장하는 품질과 동일하지만 case 1,2,3,4의 경우는 접근조건을 모두 복호화 하지 못하는 경우이며 표 5에서 보듯이 낮은 PSNR값을 보여주게 된다.

표 5 접근 권한에 따라 접근권한이 보장하는 품질과 접근조건으로 강제 접근시 품질의 PSNR 값

(a) 접근권한이 보장하는 품질

case	PSNR Y	PSNR U	PSNR V
1	0	0	0
2	27.3808	38.3680	38.4299
3	28.3098	39.6567	40.0774
4	27.0986	38.0180	38.4488
5	26.7798	37.9623	38.4204

(b) 접근 조건으로 강제접근시 품질

case	PSNR Y	PSNR U	PSNR V
1	8.7364	25.2576	28.4450
2	18.3491	34.6364	34.0368
3	18.4750	35.7254	35.1707
4	22.1120	36.0828	36.0237
5	26.7798	37.9623.	38.4204

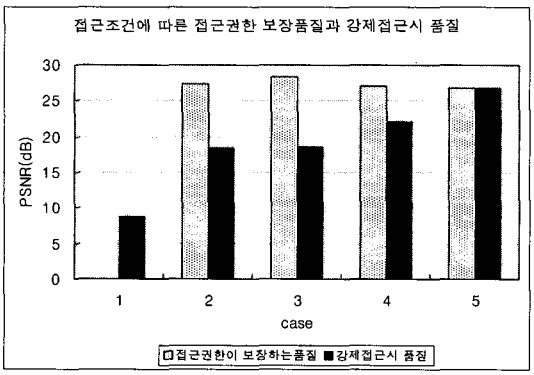


그림 11. 접근조건에 따른 접근권한보장 품질 및 강제 접근시 품질의 비교표

실험에서 보듯이 각 접근권한은 접근권한에 해당하는 최대 품질인 접근권한 보장품질을 가지고 있으며 접근권한 이상의 접근조건으로 강제 접근 시 접근권한 최대품질보다 낮은 품질을 가진 비디오를 보여주게 된다. 또한 더 많은 확장레이어가 복호화 될수록 즉, 높은 접근 권한을 가질수록 영상의 품질은 향상되는 효과를 보여주고 있으며 이는 SVC 콘텐츠의 단계적인 확장구조에 기반하고 있다.

V. 결 론

본 논문에서는 SVC에 대한 효과적인 암호화 알고리즘과 암호화된 SVC 비트스트림을 이용한 조건적 접근제어 방법을 제안했다. SVC에 대한 암호화를 위해 먼저 SVC 암호화를 위한 요구사항을 분석하였다. SVC 암호화는 암호화 후에도 스케일러빌리티가 유지되어 비트스트림 추출과정에 적용 가능하도록 기본 확장단위를 고려해야 하고, SVC의 비트스트림의 데이터 형식을 고려해야 하며 디코더의 연산량을 고려한 경량 암호화 방법을 사용해야 한다. 제안된 암호화 방법은 이러한 SVC 암호화 요구사항을 만족하며, 시각적 잡음과 PSNR 결과로부터 제안한 방법이 효과적임을 보여주고 있다.

또한 본 논문에서는 제안된 방법으로 계층적으로 암호화된 비트스트림을 소비하기 위해서 접근권한에 따라 제한적으로 접근하게 하는 조건적 접근제어 방법을 제안 하였다. 제안하는 방법은 SVC에서 각 레이어를 암호화하고 암호화 후에 접근권한으로 접근 가능한 비트스트림만을 선택적으로 복호화 하여 디코딩 하게 한다. 이 때 접근권한에 따른 키로 복호화 할 수 있는 비트스트림은 제한되어 있기 때문에 접근권한 이상의 비트스트림으로 강제 접근시 복호화 되지 않은 영역으로 인해 잡음을 가진 영상이 디코딩되므로 효과적으로 접근을 제어 할 수 있음을 실험을 통하여 보여주었다. 그러나 조건적 접근제어에서 다중 키를 통한 접근은 서버와 유저 간에 복잡도를 높일 수 있고, 매번 접근 시에 필요한 키 조합을 계산해야 하는 문제가 있다. 그러므로 키의 복잡도를 줄이고 전송이 용이한 키 관리기술에 대한 연구가 추가적으로 요구된다.

참 고 문 헌

[1] ISO/IEC JTC 1/SC 29/WG 1113818-11:2003(E), Information Technology Generic Coding of Moving Pictures and Associated Audio Information-Part11, "IPMP on MPEG-2 Systems," 2003.

[2] ISO/IEC JTC 1/SC 29/WG 1114496-

13:2004(E), Information Technology Coding of Audio-Visual Object-Part13 "Intellectual Property Management and Protection(IPMP) Extensions," 2004.

[3] Open Mobile Alliance (OMA) DRM specification candidate version 2.0 - 15 Sep 2005 www.openmobilealliance.org

[4] ISO/IEC JTC 1/SC 29/WG 1N 3480: JPSEC Final Committee Draft Version 1.0

[5] Bin B. Zhu, Mitchell D. Swanson, and Shipeng Li, "Encryption and Authentication for Scalable Multimedia: Current State of the Art and Challenges," *Proc. SPIE* vol. 5601, pp. 157-170, Philadelphia PA, Oct. 2004.

[6] Bin B.Zhu, Chun Yuan, Yidong Wang, and Shipeng Li "Scalable Protection for MPEG-4 Fine Granularity Scalability," *IEEE Transaction on Multimedia* VOL. 7, NO.2, April 2005

[7] ISO/IEC JTC 1/SC 29/WG 11N 7084 : Joint Scalable Video Model (JSVM) 2.0 Reference Encoding Algorithm Description, April (2005), Buzan, Korea

[8] Thomas Wiegand, Gary J. Sullivan, Ajay Luthra, Aharon Gill, Text of ISO/IEC FDIS 14496-10: Information Technology Coding of audio-visual objects Part 10: "Advanced Video Coding," ISO/IEC FDIS 14496-10:2003, March 2003

[9] Thomas Stockhammer, Miska M. Hannuksela, Stephan Wenger "H.26L /JVT coding network abstraction layer and ip-based transport," *IEEE ICIP*, Vol. 2, pp. 485-488, 2002

[10] Iskender Agi, Li Gong, "An Empirical Study of Secure MPEG Video Transmissions," *in proc. Internet society symposium. Network & Distributed system security*, pp. 137-144, Feb. 1996,

[11] Xiliang Liu, Ahmet M. Eskicioglu, "Selective Encryption of Multimedia Contents in Distribution Network: Challenges and New Directions," *IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003)*, Scottsdale, AZ, November 17-19, 2003

[12] Changgui Shi, Sheng-Yih Wang, Bharat Bhargava "MPEG video encryption in Real-Time Using Secret Key cryptography," *1999 International Conference on Parallel and Distributed Processing Technique and Applications(PDPTA'99)*, Las Vegas, NY, June 1999

[13] Changghi Shi, Bharat Bhargava "A fast MPEG video encryption algorithm," *Proceedings of the sixth ACM international conference on Multimedia* 1998

[14] W.Zeng and S.Lei, "Efficient frequency domain video scrambling for content access control," *ACM int.Conf. Multimedia*, pp. 285-294, Oct, 1999

[15] J.Wen, M.severa, W. Zeng, M.H.Luttrell, and W.Jin, "A format-compliant configurable encryption frame work for access control of video," *IEEE Trans Circuits systems video technology* vol 12, no 6, pp545-557, Jun 2002

〈著者紹介〉

원 용 근 (Yong Geun Won) 학생회원
2003년 2월 : 중앙대학교 전자전기공학부 졸업
2004년 3월~현재 : 한국정보통신대학교 석사과정
〈관심분야〉 Scalable Video Coding, Video Adaptation, Multimedia Security

배 태 면 (Tae Meon Bae) 학생회원
1996년 2월 : 경북대학교 전자공학과 졸업
1998년 2월 : 경북대학교 전자공학과 석사
2000년 8월 : 경북대학교 박사과정
2000년 9월~2001년 3월 : Togabi 기술 연구원
2001년 3월~현재 : 서울대학교 컴퓨터기술연구소 연구원
2002년 9월~현재 : 한국정보통신대학교 박사과정
〈관심분야〉 Scalable Video Coding, Video Adaptation, Watermarking, Multimedia Security

노 용 만 (Yong Man Ro) 정회원
1985년 2월 : 연세대학교 전자공학과 졸업
1987년 2월 : KAIST 전기공학과 석사
1992년 2월 : KAIST 전기공학과 박사
1992년~1995년 : Dept. of Radiogical Science, University of California, Irvine, 초빙연구원
1996년 : Dept. of Electronical Eng. and Computer Science, University of California, Berkeley 연구원
1997년~현재 : 한국정보통신 대학교 정교수
〈관심분야〉 이미지/비디오 처리 및 분석, MPEG-7, 특징인식, 이미지/비디오 인덱싱