Journal of Korea Multimedia Society Vol. 15, No. 3, March 2012(pp. 299-311)

H.264 Scalable Extension을 위한 비디오 워터마킹 및 암호화 기반의 정보보호 기법

김원제[†], 성택영[††], 이석환[†††], 권기룡[††††]

요 약

최근, 이종 단말 및 네트워크간의 통신 환경에서도 one source, multi-user 서비스를 지원하기 위한 H.264 SE(scalable extension)가 차세대 멀티미디어 서비스를 위한 표준으로 자리매김 하고 있다. 하지만, 기존의 DRM 기법들은 네트워크 전송 환경 및 단말의 성능에 따라 전송 데이터 량을 가변하는 H.264 SE 시스템에는 적합하지 않다. 본 논문에서는 H.264 SE에 적합한 비디오 워터마킹과 암호화 기법을 결합한 정보보호 기법을 제안한다. 제안 논문에서 워터마크 삽입량 및 삽입 위치는 네트워크 및 단말의 상태에 따라 결정되는 enhancement layer들이 포함하는 프레임 수를 이용해 계산된다. 또한 비디오 워터마킹과 데이터 암호화로 인해 발생하는 비디오 부호화 과정에서의 시간지연을 최소화하기 위해 두 과정을 비디오 압축 시 동시에 수행한다. 실험 결과, 본 제안 기법은 비디오 압축 및 일반 신호 처리, 기하학적 처리에 강인함을 확인하였다.

An Information Security Scheme Based on Video Watermarking and Encryption for H.264 Scalable Extension

Won-Jei Kim[†], Teak-Young Seung[††], Suk-Hwan Lee[†††], Ki-Ryong Kwon[††††]

ABSTRACT

Recently, H.264 SE(scalable extension) has become a standard of next generation multimedia service which is one source, multi-user service in the telecommunication environment of different kinds of networks and terminal equipments. But existing DRM schemes for multimedia service are not fit for H.264 SE system. Because the amount of transmitted multimedia data is changed considering network environment and terminal equipments' performance by the system, but in the existing DRM schemes, the amount of handled multimedia data are not variable according to network environment and terminal equipments' performance. In this paper, an information security scheme combined video watermarking and encryption is presented for H.264 SE. Amount of watermarks and embedding positions are calculated by the frame number of enhancement layers which are created according to the state of networks and terminal equipments. In order to minimize delayed time by video watermarking and encryption, the video data are watermarked and encrypted in the H.264 SE compression process. In the experimental results, we confirmed that proposed scheme is robust against video compression, general signal processing and geometric processing.

Key words: Information Security(정보보호), H.264 SE, Video Watermarking(비디오 워터마킹), Encryption(암호화)

※ 교신저자(Corresponding Author) : 권기룡, 주소 : 부산광역시 남구 대연 3동 599-1 부경대학교 대연캠퍼스 (608-711), 전화 : 051)629-6257, FAX : 051)629-6230, E-mail : krkwon@spknu.ac.kr
접수일 : 2011년 1월 5일, 수정일 : 2011년 12월 6일
완료일 : 2012년 3월 5일
[†] 준회원, (주)영우DSP
(E-mail : nannaia@nate.com)
[††] 준회원, 부경대학교 정보보학협동과정
(E-mail : theage76@pknu.ac.kr)
[†††] 정회원 동명대학교 정보보호학과
(E-mail : skylee@tu.ac.kr)
[††††] 종신회원 부경대학교 IT융합응용공학과
※ 본 연구는 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단 (KRF-2009-0075855) 및 2011년도 (KRF-2011-0010902) 지원으로 수행되었음.

1. 서 론

통방융합의 세계적인 흐름과 발맞추어 유선데이터 및 방송, 무선데이터, 이동통신 등 인프라의 종류를 막론하고 모든 사업자들은 방송/통신/데이터 및 음성 서비스의 통합을 추진하고 있으며, 이런 배경 속에서 방송 서비스는 각종 이종 망과의 연동을 통한 다양한 종류의 단말을 대상으로 언제 어디서나 방송 콘텐츠의 접근 및 소비를 가능하게 하는 유비쿼터스(Ubiquitous) 방송 서비스로 진화하고 있다[1]. 이러한 서비스를 겨냥해서 기존의 코덱을 개선한 H.264 SE(scalable extension)를 비롯한 여러 가지 스케일러블 비디오 코덱(codec)들이 개발되었다. 그중, H.264 SE는 ISO/IEC 산하 MPEG (Moving Picture Experts Group)과 ITU-T 산하 VCEG (Video Coding Experts Group)가 Joint Video Team(JVT)을 이루어 MPEG-4 SVC 또는 H.264 SE 라는 이름으로 표준화가 완료된 코덱이다. 이 코덱을 통해 부호화된 비디오 자료에서 해상도와 프레임율, 그리고 화질별로 다양한 영상을 추출하여 각 단말들의 특성에 맞게 제공하게 된다[2-8].

따라서 변화하는 디지털 콘텐츠 배포 인프라에 적절히 대응하는 DRM(Digital Rights Management) 포맷의 개발 역시 중요해지고 있으며 이를 위해서 모바일 및 홈 네트워크를 위한 DVB-H CPCM(DVB-H Content Protection and Copy Management) 및 OMA DRM(Open Mobile Alliance DRM), COPP (Certified Output Protection Protocol), DTCP (Digital Transmission Content Protection)와 같은 DRM 포맷들이 등장하였다. 해당 DRM 포맷들은 기존의 DRM 기법과 마찬가지로 디지털 콘텐츠를 대칭키 기법으로 암호화하고 콘텐츠에 대한 권리를 명세한 권리 객체를 사용자의 공개키로 암호화하여 전달하는 방식을 사용하고 있다. 그러나 열거한 DRM 포맷들도 이종 망간의 콘텐츠 연동에는 별도의 해결책이 없으며 스케일러블 콘텐츠에 대한 과금 방식이 정해지지 않아 하나의 콘텐츠가 서비스 당시의 네트워크 트래픽 상태 및 단말의 성능에 따라 다양한 품질의 형태로 존재 가능한 콘텐츠 배급 환경에 제대로 대처할 수가 없다[9-13]. 따라서 H.264 SE 코덱의 범용적인 사용에 대비한 해당 코덱 기반의 보다 효과적인 정보보호 기법들이 새로이 연구되어야 한다.

DRM이 해결하지 못한 이종 망간의 연동 문제에는 인터넷을 기반으로 하는 유무선 데이터 전송망과 이동통신망 사이의 연동뿐만 아니라 각 망들의 통신 특성에 기반한 코덱들이 다르다는 것도 한 몫 하고 있다. 이를 해결하기 위해 이종 코덱들 간의 데이터 전송 환경에서 저작권 보호 및 접근 제어를 위해 정수기반 DCT 계수 값들에 대한 워터마킹 및 AES 암호화 처리를 통해 트랜스코딩 환경에 강인한 정보보호 기법이 제안되었다[14]. 해당 기법은 워터마킹과 암호화를 비디오 코덱 내에서 동시에 수행하도록 제안된 기법으로서 본 논문에서도 해당 기법이 가지는 코덱 내 정보 보호 기법의 이식성을 바탕으로 H.264 SE에서 워터마킹 및 암호화가 수행된다.

본 논문에서는 기존의 연구들에서 고려되지 않은 H.264 SE의 특성에 적합한 비디오 워터마킹 및 AES(Advanced Encryption Standard) 기반의 암호기술이 결합된 정보보호 기법을 논의하고자 한다[15- 17]. 본 기법은 H.264 SE 코덱이 지원하는 여러 가지 해상도와 프레임율, 그리고 화질의 변화에도 워터마크를 추출할 수 있으며, 최초 사용자에게는 암호화된 비디오를 제공하여 일차적인 보안을 유지하며, 이후 인증된 사용자를 통해서 비디오가 유포될 가능성을 고려하여 워터마크를 삽입함으로서 이차적인 보안까지 고려하였다. 또한 비디오 부호화 과정 중에 워터마킹 및 암호화를 수행함으로서 워터마킹 및 암호화로 인해 발생하는 시간 지연을 최소화 하였다.

본 논문의 구성은 다음과 같다. 2장에서 H.264 SE와 H.264 SE와 유사한 H.264/AVC 내에 워터마킹을 수행한 Zhang의 기법, 그리고 암호화 기법들 중 하나인 AES를 살펴본다. 3장에서 제안한 비디오 워터마킹 알고리즘에 대해 설명한다. 그리고 4장에서는 실험 결과를 통한 제안 기법의 성능에 대해 분석해 본다. 마지막으로 본 논문의 결론부에서 향후 추가되어야 할 개선점이나 연구 방향 등을 제시한다.

2. 관련 연구

2.1 H.264 Scalable Extension

스케일러블 비디오 부호화의 목적은 특정 비트율로 화질을 우화하는 것이다. 이 때 그 비트열은 임의 비트율에서도 복호화가 되어야 한다. 따라서 스케일러블 비디오 부호화기는 다양한 비트율/프레임율/영

상크기에 대한 스케일러빌러티(scalability)를 지원한다. 즉, 비디오를 공간적, 시간적, 그리고 화질적 차원의 임의 값을 가지는 비트열로 부호화한다.

기술적인 관점에서, 하나의 스케일러블 비트열은 두 개 혹은 그 이상의 의존적인 계층으로 구성될 수 있다. 이 경우, 스케일러블 코덱은 하나의 기본 계층과 스케일러블 상위 계층들로 구성된다. 그림 1은 H.264 SE에서 2계층의 예시에 해당하는 블록도를 나타내었다.

2.2 기존 비디오 워터마킹 기법 연구

Zhang 등[18]이 제안한 알고리즘은 워터마크를 생성하는 전처리 단계와 생성한 워터마크를 삽입하고 추출하는 워터마킹 단계로 나눌 수 있다. 먼저, 그림 2에서와 같이 이진영상을 그 특성에 맞게 주파수 마스킹을 수행하여 입력하게 될 워터마크 값을 계산한다.

그림 3에서는 생성된 워터마크를 H.264/AVC 내에서 삽입하는 과정을 블록도로 나타낸 것이다. 생성된 워터마크 정보3는 -1, 1값을 가지는 바이폴라 벡터로 사상된다. 그리고 4×4 DCT된 계수 값 중 중간 주파수 위치의 계수 값을 해당 블록 내의 DC계수 및 AC계수에 기반한 가중치와 워터마크비트의 곱값으로 치환한다.

Zhang의 알고리즘에서 주파수 마스킹과 변환 특성은 주목 할 만하나 회전, 절단, 그리고 축소 등의 기하학적인 공격에 대해서는 취약하다.

2.3 Advanced Encryption Standard

AES는 미국 정부 표준으로 지정된 블록 암호 형식으로서 이전의 표준인 DES를 대체하며, 미국 표준기술 연구소(NIST)가 5년의 표준화 과정을 거쳐 2002년 5월 26일부터 표준으로 효력을 발휘하기 시작했다. AES는 DES(Data Encryption Standard)의 구조와 달리 Rijndael 기법이 적용된 SPN(Substitution Permutation Network) 구조를 이용한다[19,20]. 블록길이는 128, 160, 192, 224, 256 비트 등 128비트 이상의 모든 32의 배수 비트를 사용할 수 있으며 큰

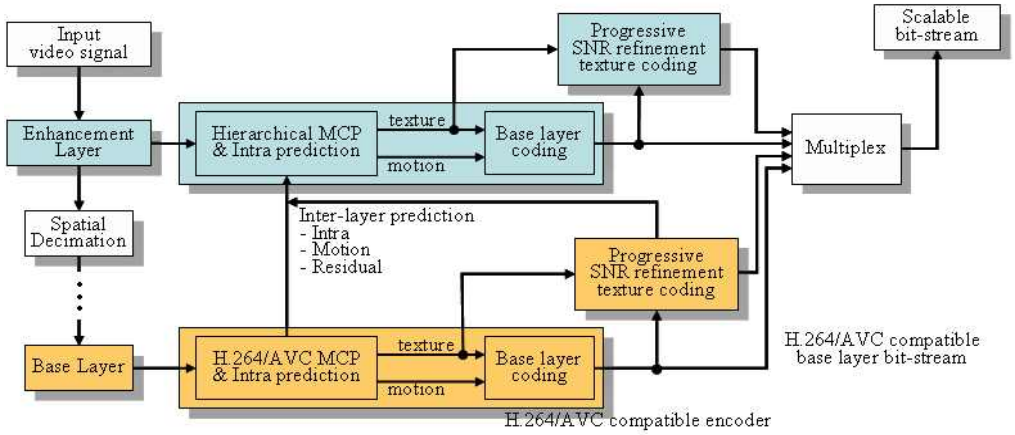


그림 1. 공간적 2 계층의 스케일러빌러티를 제공하는 H.264 SE 부호화기

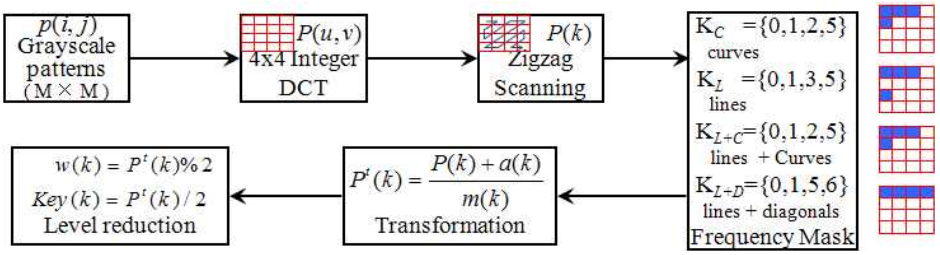


그림 2. Zhang의 알고리즘: 워터마크 전처리 단계

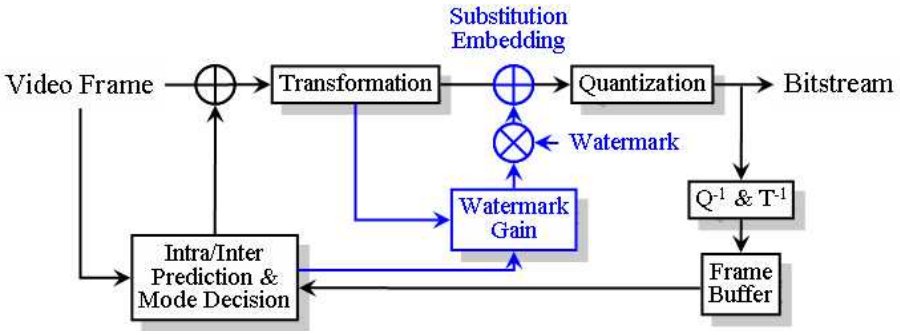


그림 3. Zhang의 알고리즘: H.264/AVC 내 워터마킹 시스템

키를 쓰거나 라운드 수를 반복할수록 안정성이 커진다. 본 논문에서는 H.264 SE의 정확한 이해를 통해 AES를 코덱 내부에 이식하였다. 아래 그림 4는 AES의 동작과정을 나타낸다.

3. 제안한 비디오 워터마킹 암호화 기법

본 논문에서 제안하는 비디오 워터마킹 및 암호화 기법이 결합된 정보보호 기법은 H.264 SE를 대상으로 해당 코덱 시스템에서 처리되는 비디오 콘텐츠에 대해 워터마킹과 암호화 처리를 수행하여 해당 콘텐츠를 이중으로 보호한다. 우선, H.264 SE 내에서 수행되는 제안 비디오 워터마킹 기법을 통해 비디오 콘텐츠 내에 소유권 및 저작권 주장을 위한 워터마크를 삽입한다. 이때 삽입되는 워터마크는 프레임 내 각 DCT 블록의 시각적 특성을 고려한 화질 복잡도를 계산하여 워터마크 삽입대상 및 삽입량을 선택한 후 프레임 내에 효과적으로 반복 삽입된다. 따라서 제안하는 워터마킹 기법은 일반적인 신호처리 공격 및 기하학적 공격에 대하여 Ⅱ-1-2 절에 소개한 기존의 비디오 워터마킹 기법에 비해 보다 강인하도록 설계되었다.

또한 사용자 접근제어를 위해 수행되는 AES 기반의 암호화는 H.264 SE를 통해 압축된 영상이 다양한 형태의 단말에서 재생될 때 화질의 열화를 일으키도록 하여 복호화 키 없이는 정상적인 영상을 재생할 수 없도록 보안성을 고려하였다. 해당 코덱을 통한 영상의 부호화시 요구되는 실시간성을 충족하기 위해 제안하는 기법에서는 H.264 SE 코덱 내에 비디오 워터마킹 및 AES 기반의 암호화 알고리즘을 적용하여 빠른 연산이 가능하도록 하였다.

3.1 H.264 SE 코덱 내 워터마킹과 암호화 시스템

H.264 SE 코덱 내에서 수행하는 워터마킹과 암호화에 대해서 아래 그림 5와 같이 블록도로 나타내었다. 스케일러블 비디오 부호화의 특성을 나타내는 기본 시스템에서 각 레이어별 부호화 과정에서 워터마킹과 암호화를 수행하게 된다.

보다 자세한 설명을 하자면 아래 그림 6과 같이 나타낼 수 있다. 세부 시스템의 입력은 전체 시스템에서 공간적 축소를 수행한 레이어이다. 이 레이어에 해당하는 각 프레임에 대해서 예측과 변환을 수행을 하고, 양자화를 거쳐서 엔트로피 부호화를 하게 된다. 입력되는 레이어의 해당 프레임에 대해서 삽입할

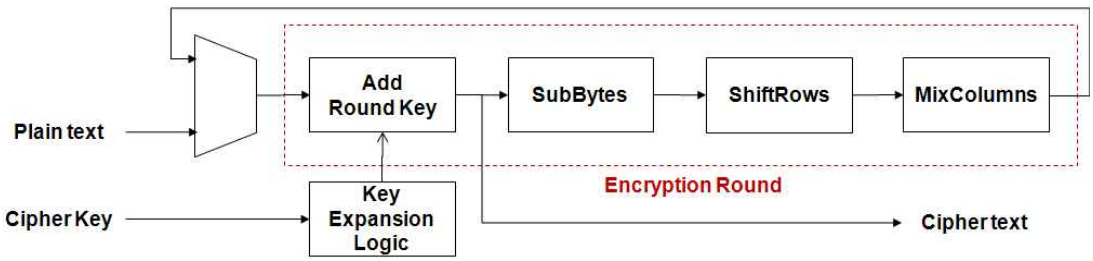


그림 4. AES의 동작 과정

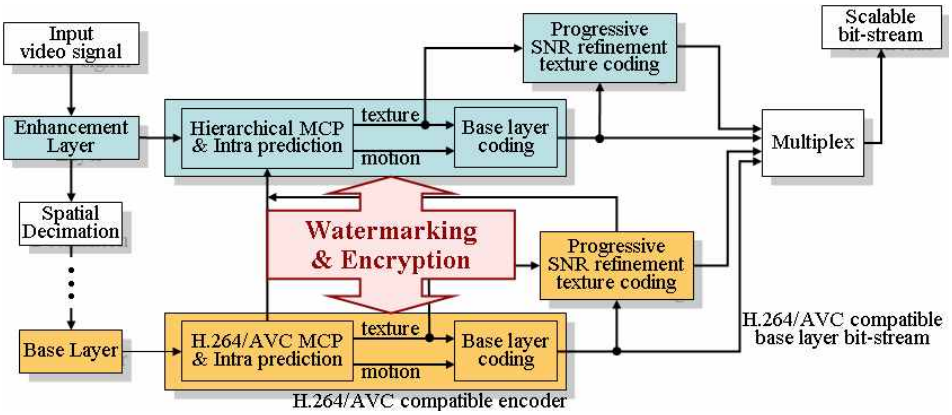


그림 5. 제안한 워터마킹과 암호화 알고리즘을 적용한 H.264 SE 전체 시스템

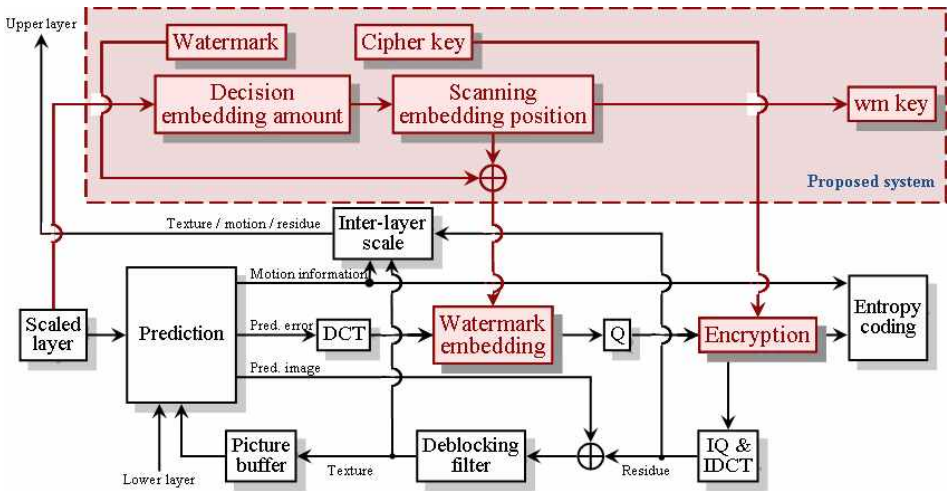


그림 6. 제안한 워터마킹과 암호화 기법을 적용한 H.264 SE 세부 시스템

워터마크 비트량을 결정하고 그 양만큼의 삽입 위치를 선별하여 키 값으로 저장을 한다. 이렇게 선별된 위치에 DCT 된 데이터를 사용하여 워터마크를 삽입하게 된다. 이 때, base layer에만 워터마크가 삽입될 경우, spatial scalability 부호화기의 경우에는 워터마크 역시 영상 해상도에 따른 업 샘플링이 되며 Base layer와 enhancement layer간의 차분치가 잡음의 형태로 워터마크에 추가된다. 또한, temporal scalability 부호화기의 경우에는 프레임율의 변화에 따라 워터마크가 삽입된 프레임이 제거되어 손실될 가능성이 크고 FGS(fine grain scalability) 부호화기의 경우에는 QP값을 계층별로 다르게 할당하여 비트플레인 방식을 이용하여 부호화하는데 이 때 양자화 스텝 사이즈와 더불어 양자화 오차가 증가하면서 영상의 화질 열화가 발생한다. 따라서 FGS계층 가변 시 프레임의 고주파 성분에 해당하는 데이터 손실이 증가하여 워터마크를 검출하는 것이 어려워진다. 만약 base layer에만 워터마크를 삽입한다면 enhancement layer로 전파된 워터마크는 해상도 가변으로 인한 데이터 손실 및 변형이 발생하여 검출이 어려워지므로 본 논문에서는 base 및 enhancement layer 두 곳에 다 워터마크를 삽입한다. 그 후, 워터마크가 삽입된 데이터를 양자화하고 엔트로피 부호화를 하기 전에 암호키에 의한 암호화를 거치게 된다.

3.2 워터마크 삽입 알고리즘

본 절에서는 H.264 SE 내에서 워터마크를 삽입하는 알고리즘에 대해서 설명한다. 워터마크의 삽입은

크게 워터마크 삽입량 결정, 위치 선정 그리고 삽입으로 나눠진다.

우선, 워터마크 삽입량 결정은 입력된 비디오 프레임으로부터 $Block_n$을 구하고 이 값을 가지고 C_W와 wm_amount를 구하여, 마지막으로 워터마크를 삽입하게 될 위치 값 wm_key를 저장한다. 이렇게 저장한 wm_key값은 워터마크가 삽입된 영상으로부터 워터마크를 추출할 때 키 값으로 사용되어진다. 입력되는 각 프레임별로 워터마크를 삽입할 양은 아래 식 (1)로부터 결정하게 된다.

$$Block\_n = \frac{w_f \times h_f}{16} \tag{1}$$

여기서 w_f와 h_f는 각각 프레임의 수평 해상도와 수직 해상도를 뜻한다. 프레임 내 모든 DCT 블록의 개수 $Block_n$은 전체 프레임의 크기로부터 4×4 블록을 겹치지 않게 나누어진 개수를 의미한다.

$$C_W = floor\left[\frac{Block\_n}{wm\_length} \times m\right] \tag{2}$$

식 (2)에서 wm_length는 삽입하고자 하는 워터마크 비트열의 길이를 뜻하는 것으로 4×4 블록 당 한 개의 비트씩 삽입된다. 여기서 한 개의 프레임 내에 존재하는 4×4 블록의 개수로부터 wm_length를 나누어 줌으로서 삽입 가능한 전체 워터마크의 개수를 알 수 있다. 본 논문에서는 워터마크가 삽입된 영상의 화질을 고려하여 전체에 삽입하지 않고, 한 개의 프레임의 m에 해당하는 영역에만 워터마크를 삽입한다. 이로써 워터마크가 반복되는 회수 C_W를 결정하게 된다.

$$wm\_amount = C_W \times wm\_length \tag{3}$$

식 (3)은 삽입하고자 하는 워터마크 비트열의 길이와 그 반복 회수의 곱으로서 한 개의 프레임 내에 삽입하게 될 총 워터마크 비트량 wm_amount를 구할 수 있게 된다.

다음으로 워터마크를 삽입하게 될 위치를 결정하게 되는데, 한 개의 프레임을 $Block_n$만큼 4×4 정수 DCT 를 수행한다. 각 DCT 된 계수 값들을 식 (4)과 같이 계산하여 각각의 4×4 블록 내 화질의 복잡도 S_i를 구한다.

$$S_i = \sum_{1 \le u,v \le 3} |x_i(u,v)|, 0 \le i < \tag{4}$$

여기서, $x_i(u,v)$는 i번째 Intra DCT Block 내의 계수값을 뜻하며, S_i는 i번째 Intra DCT Block 내의 AC 계수들의 절대 크기 합이다. 이렇게 구해진 S_i는 아래 그림 7과 같은 과정을 거치게 된다. S_order_i는 S_i의 크기에 따라 내림차순으로 정렬한 값이며, wm_amount만큼 추출한 값이 $S_order_{i_max}$이다. 마지막으로 $S_order_{i_max}$를 좌표 매핑을 통해서 워터마크를 삽입하고자 하는 위치값 wm_key를 구해낸다.

앞서 구한 wm_key값에 해당하는 위치에 워터마크를 삽입하기 위해 식 (5), 식 (6)을 사용한다.

$$wx_i = \frac{\sum_{1 \le u,v \le 3} |x_i(u,v)|}{9} \cdot (w_i + \alpha) \tag{5}$$

$$x_i(ku_i, kv_i) = wx_i \tag{6}$$

여기서, xw_i는 w_i 및 AC 계수합으로 생성된 새로운 AC 계수이며, α는 워터마크 삽입강도, u, v는 AC 계수의 좌표이며, ku_i, kv_i는 생성된 xw_i가 치환될 DCT Block 내의 좌표이다.

해당 과정을 거쳐 산출된 xw_i는 영상복잡도를 고려하여 S_i의 크기가 큰 순서대로 삽입되므로 압축과정에서 나타나는 기본적인 화질 열화 및 필터링, 잡음추가, 콘트라스트 변환 등에 쉽게 삭제되지 않으며 프레임 내 선택된 블록별로 중복 삽입 과정을 거치므로 절삭 및 회전 공격을 통해 프레임의 일부분이 삭제되더라도 워터마크 검출시 요구되는 워터마크 동기화가 쉽사리 무력화 되지 않는다는 장점을 가지고 있다.

3.3 워터마크 추출 알고리즘

워터마크 추출은 복호된 영상으로부터 수행할 수 있다. 워터마크 삽입시에 사용했던 워터마크 키 값을

그림 7. 워터마크 삽입 위치 결정 과정

이용하여 워터마크가 삽입된 위치를 찾아 해당 위치의 계수 값으로부터 워터마크 비트를 결정할 수 있으며, 해당하는 수식은 아래 식 (7), 식 (8)과 같다.

$$\hat{w}_i = \begin{cases} 1, & \text{if } \tilde{x}_i(ku_i, kv_i) \geq th \\ 0, & otherwise \end{cases} \quad (7)$$

$$th = \frac{\sum_{1 \leq u,v \leq 3} |\tilde{x}_i(u,v)|}{9} \quad (8)$$

3.4 암호화 알고리즘

워터마크 삽입을 통해 저작권 또는 소유권에 대한 정보 삽입이 완료된 비디오 프레임들에 대해 사용자 접근제한 기능을 추가하기 위하여 암호화를 수행한다. 사용한 암호화 알고리즘은 AES이며, 사용한 키의 길이는 128 비트이다. H.264 SE 내에 암호화를 수행하는 방법은 아래 그림 8과 같이 나타낼 수 있다.

DCT 된 데이터에 워터마크가 삽입되고 양자화를 거친 데이터에 대해서 암호화를 수행한다. 해당 블록의 계수에 암호화 키를 사용하여 암호화된 블록의 계수를 생성해서 치환한 후 엔트로피 부호화로 내보내게 된다.

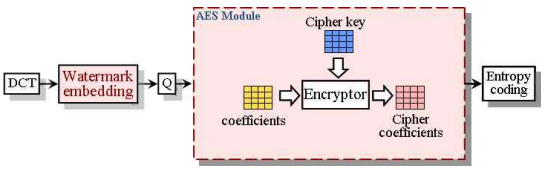


그림 8. H.264 SE 내 적용한 AES 기법 블록도

4. 실험결과 및 고찰

본 장에서는 비가시성과 강인성을 실험하기에 앞서 SE 특성에 대한 워터마크의 강인성을 확인해 보고 이후 본 논문에서 제안하는 알고리즘의 우수성을 Zhang 등이 제안한 알고리즘과 비교하여 보고 그 결과에 대해 고찰해본다.

4.1 실험 방법

본 논문에서 제안하는 비디오 워터마킹 알고리즘의 비가시성과 강인성을 실험은 H.264 SE JSVM 9.8 참조 소프트웨어를 사용하여 수행하였다[19]. 실험 영상은 Foreman, Container, Crew, Mobile을 사용하였으며, 해상도는 QCIF(176×144), CIF(352×288) 그리고 4CIF(704×576), 프레임율은 초당 30 프레임을 가지도록 하였다[20]. 부호화 환경은 GOP 구조는 IPBBB… 형태의 8 크기를 가지도록 하였으며, 반복되는 인트라 픽처의 경우 32의 주기를 가지도록 하여 각 영상별로 전체 100 프레임을 실험에 사용하였다. 실험을 수행한 하드웨어 사양은 인텔 펜티엄 4, CPU 3GHz, 램 2GB 이며, 소프트웨어 사양은 비주얼 스튜디오 2005를 사용하였다. 워터마크가 삽입된 영상의 비가시성을 평가하기 위하여 부호화하지 않은 원본 영상과 PSNR(Peak Signal to Noise Ratio)을 사용하여 나타내었으며, 강인성에 대한 평가는 삽입된 워터마크 비트와 공격 후 추출한 워터마크 간의 정규화된 상관도(normalized correlation)를 사용하여 수행하였다.

4.2 Scalable extension 특성에 대한 만족도 평가

제안하는 알고리즘은 H.264 SE 코덱 내에서 수행하므로 SE 특성을 만족하는지를 먼저 확인하였다. 그 결과 값을 표 1과 같이 정리하였다.

각 특성별 강인성 평가는 BER(bit error ratio)로 나타내었다. 대부분의 수치가 0%를 나타내는데 반해 공간적 스케일러빌러티의 QCIF 크기에서 나타나는 수치는 그 이상임을 알 수 있다. 본 논문에서 제안하는 알고리즘에 대한 연구가 CIF 크기 위주임을 감

표 1. SE 특성에 따른 영상에 대한 워터마크의 강인성 (측정기준: BER / 단위: %)

Test Video	Spatial Scalability			Temporal Scalability	
	QCIF	CIF	4CIF	30Hz	15Hz
Foreman	4.69	0.0	0.0	0.0	0.0
Container	3.13	0.0	0.0	0.0	0.0
Crew	1.56	0.0	0.0	0.0	0.0
Mobile	0.0	0.0	0.0	0.0	0.0

안하여 다소 작은 영상인 QCIF 크기에서 CIF 크기에서 보다 적은 양의 워터마크가 삽입됨으로서 발생하는 오류로 판단된다. 하지만 그 수치는 전체 데이터의 10% 미만으로 SE 특성에 충분히 만족하도록 알고리즘이 적용되었음을 알 수 있다. 이 실험을 통해 각 변환 특성에 따라 생성된 영상에 대한 비가시성과 각 영상의 워터마크에 대한 공격 등은 CIF 크기의 영상으로 판단이 가능하다는 것을 확인하였으므로 이후 실험 영상의 크기는 CIF 만을 사용하였다.

4.3 영상에 대한 비가시성 평가

본 논문에서 워터마크가 삽입되고 난 후에 영상의 열화를 알아보기 위하여 그 수치를 30 프레임에 대한 평균 PSNR로 알아보았다. 워터마크를 삽입하지 않고 양자화 값 30을 사용하여 부호화 한 영상(좌측 막대그래프)과 Zhang의 알고리즘(중앙 막대그래프), 제안한 알고리즘(우측 막대그래프)으로 워터마크를 삽입한 후의 영상의 열화를 그림 9와 같이 나타내었다. 그래프를 보게 되면 Mobile 영상에서 비교적 큰 화질의 열화를 볼 수 있는데, 이는 영상 자체가 지니는 복잡한 화면 구성에 의한 것으로 판단된다.

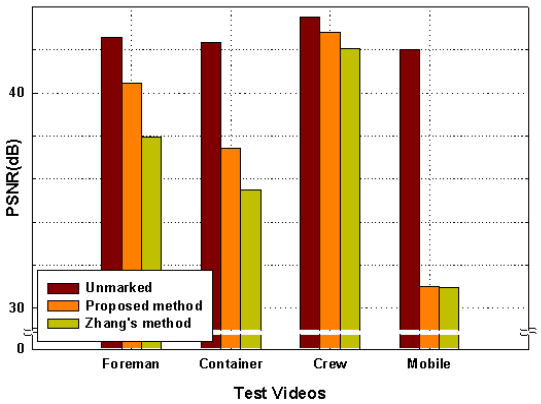


그림 9. 양자화 값 30 로 부호화 후 워터마크가 삽입되지 않은 영상과 각 영상 별 워터마크 삽입 후의 PSNR 비교

4.4 워터마크에 대한 강인성 평가

본 논문에서 제안한 알고리즘의 강인성을 Zhang이 제안한 알고리즘과 실험으로 비교하여 보았다. 원본 영상에 대해서 두 가지의 알고리즘을 워터마크를 삽입한 후 부호화, 일반적인 신호처리, 기하학적인 공격 등을 수행하여 추출한 워터마크를 원본 워터마크와의 정규상관도로 그 강인성을 평가하였다. 아래의 그림 10과 그림 11은 원본 영상에 대해서 가해지는 공격 후 영상의 변화 결과를 나타내는 것으로서 본 실험에서는 4개의 실험 영상에 대해서 공격을 가하였다. 실험 결과를 통해 제안하는 기법은 일반적인 신호처리 공격에 비해 부호화 공격이나 기하학적인 공격에서 보다 높은 강인성을 보이는 것을 확인할 수 있었다.

실험 결과를 살펴보면 절단(Crop.) 및 회전(Rota.) 공격들에 대해 제안 알고리즘이 Zhang의 알고리즘보다 월등히 강인한 것으로 나타나고 있다. 이는 워터마크 삽입 영역 선정 방식의 차이에 기인한 것으로써 Zhang의 기법의 경우, 워터마크가 프레임 내 전 영역에 임의로 삽입이 되나 본 기법에서는 전처리 과정을 통해 선택된 m개의 선택된 블록 단위별로 워터마크가 중복 삽입되어 절단 및 회전 공격을 통해 프레임 내 일부분이 열화 되더라도 Zhang의 기법에 비해 워터마크 복원능력이 우수하기 때문이다. 그러나 워터마크가 삽입될 DCT 블록 내의 주파수 계수의 선정 방식은 두 기법이 유사하므로 절단(Crop.) 및 회전(Rota.) 공격을 제외한 나머지 공격들에서는 근소한 차이로 제안 기법이 강인함을 확인하였다.

4.5 영상에 대한 보안성 평가

워터마크를 삽입하고 난 후 사용자의 접근 제어를 위해서 암호화를 수행하고 그 결과 값을 원본 영상과 비교해 보았다. 좌측 (a) 영상이 원본 영상이며 우측 (b) 영상이 암호화된 영상으로 그림 12, 그림 13, 그림 14, 그림 15에 나타내었으며, 그 순서는 Foreman, Container, Crew, 그리고 Mobile 순이다. 그림에서 보는 바와 같이 각 영상들은 암호화에 의해 지각적으로 식별이 불가능한 보안성을 확인할 수 있었다.

4.6 부호화에 대한 속도 평가

마지막으로 부호화 시 실시간 처리를 만족하기 위한 실험을 수행하였다. 실험조건은 CIF 사이즈의 각 영상들을 양자화 값 30을 사용하여 100프레임에 대해서 부호화하였다. 각 막대그래프는 왼쪽부터 순서대로 알고리즘을 적용하지 않고 수행되는 시간과 워터마킹 적용시, 암호화 적용시, 그리고 워터마킹과 암호화 둘 다 수행시의 시간을 측정해서 그림 16에

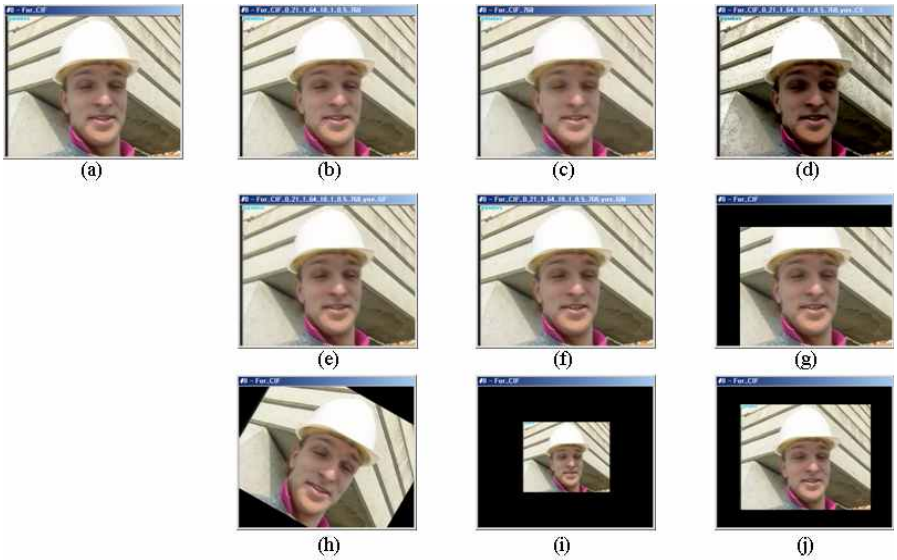


그림 10. Foreman 영상에 대한 다양한 공격 결과 (a) Original (b) Encoding (c) Trans-coding (d) Contrast Enhancement (e) Gaussian Filtering (f) Gaussian Noise (g) Cropping (h) Rotation (i) 0.5 Scaling (j) 0.75 Scaling.

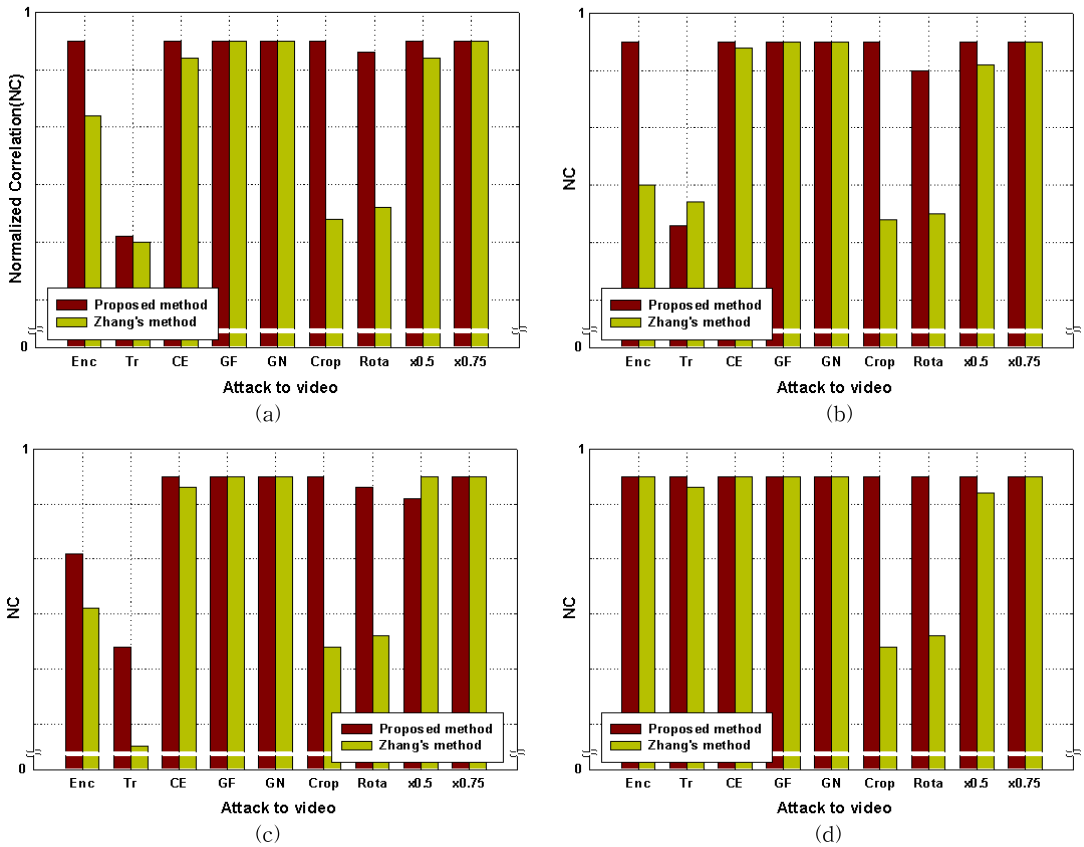
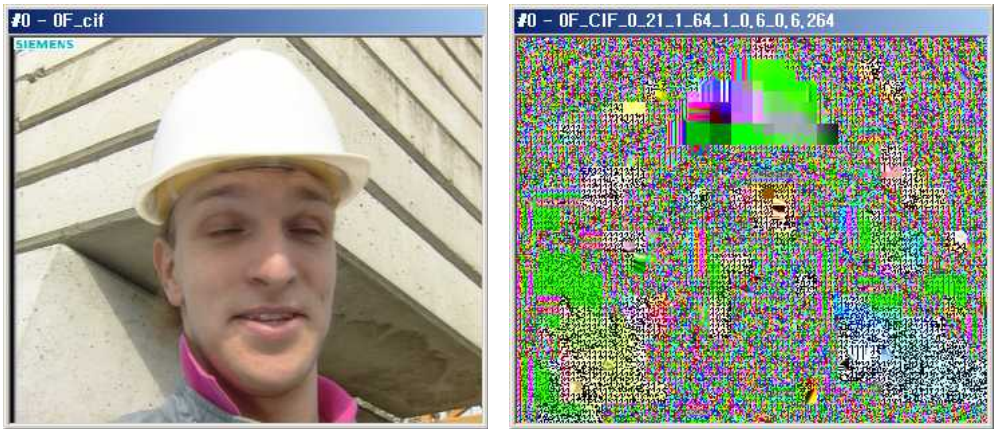
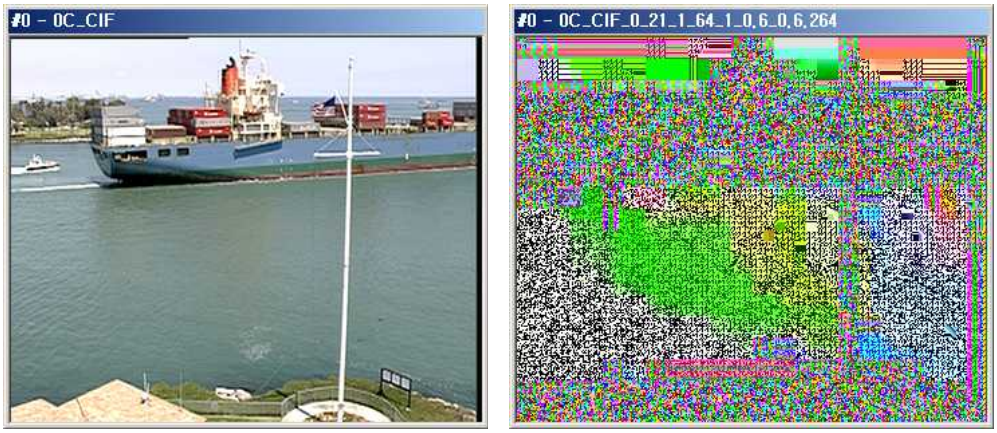


그림 11. 각 영상별 다양한 공격 후 워터마크 강인성 평가 (a) Foreman (b) Container (c) Crew (d) Mobile



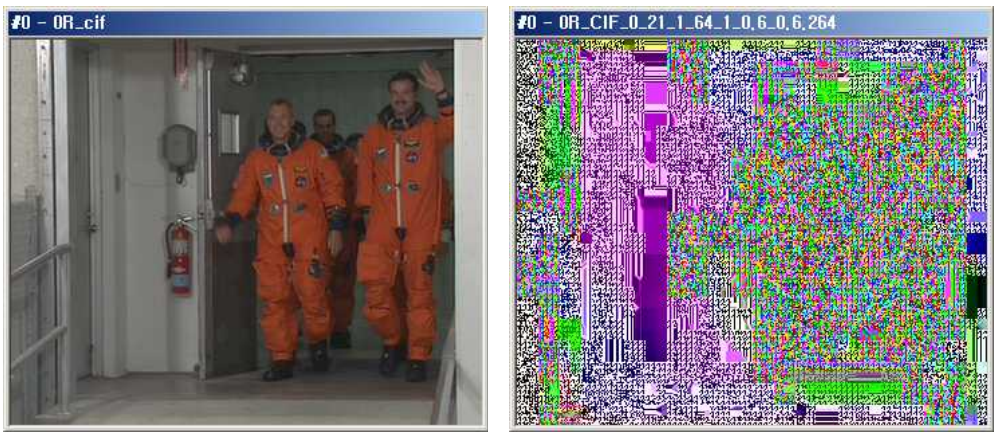
(a) (b)

그림 12. Foreman의 (a) 원본영상과 (b) 암호화된 영상



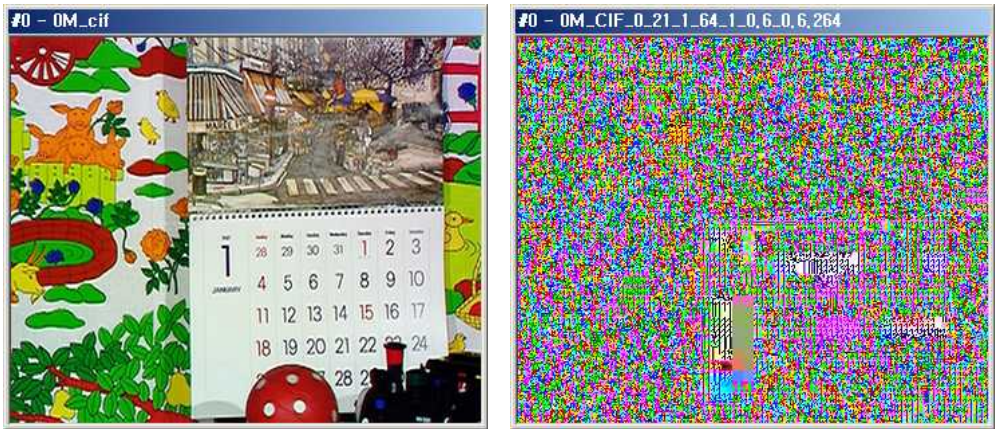
(a) (b)

그림 13. Container의 (a) 원본영상과 (b) 암호화된 영상



(a) (b)

그림 14. Crew의 (a) 원본영상과 (b) 암호화된 영상



(a) (b)

그림 15. Mobile의 (a) 원본영상과 (b) 암호화된 영상

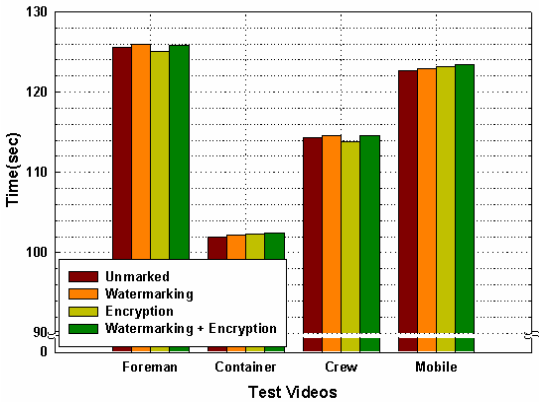


그림 16. 각 영상별 부호화 수행시간 (QP: 30)

나타내었다. 측정 결과는 각 영상에 대해 부호화된 시간(초)로 나타내었으며, 1 프레임의 평균 지연시간은 1/100 초 미만으로 처리시간을 만족함을 확인하였다. 그림 16를 보게 되면 원본 부호화시 시간에 비해 암호화 수행시간이 Foreman과 Crew 영상에서 짧게 나타난 것을 확인 할 수 있었다. 이러한 부호화 시간의 감소는 원본 데이터가 암호화를 통해 데이터 변형이 일어나면서 엔트로피 부호화 과정에서 시간의 변화가 일어난 것으로 판단된다.

5. 결 론

본 논문에서는 네트워크 환경 및 단말의 성능에 따라 데이터 전송량을 가변적으로 조절 가능한 H.264 SE를 위하여 비디오 워터마킹 및 AES 암호화 기법을 해당 코덱 시스템 내에 적용한 정보보호 기법을 제안하였다.

불법 배포에 따른 저작권 보호를 위한 제안 비디오 워터마킹 알고리즘에 대하여 다양한 주파수 특성을 가진 실험 영상들에 대해 적용한 후 워터마크 강인성 평가를 통해 제안 비디오 워터마킹 알고리즘의 강인성이 우수함을 확인하였으며, 원본 비디오와 워터마크가 삽입된 비디오의 PSNR을 비교하여 비가시성 또한 우수함을 확인하였다.

사용자 접근 제어를 위해서 워터마크가 삽입된 데이터를 암호화할 때 사용한 알고리즘은 인증된 표준 AES 알고리즘을 사용하였으며, 실험 영상의 암호화 결과를 통해 암호화 된 영상들의 내용들을 지각적으로 식별 불가능함을 확인하였고 이를 통해 전통적 DRM에서 요구하는 보안성을 제안 기법이 가짐을 확인하였다.

마지막으로 기존의 H.264 SE 부호화 시간과 제안한 기법이 적용된 H.264 SE로 부호화 후 발생한 지연시간의 비교를 통해 워터마킹 및 암호화 처리 없이 H.264 SE로 코딩한 처리 시간과 커다란 차이가 없음을 확인하였으며 이를 통해 코덱 부호화 시 요구되는 실시간성을 만족함을 알 수 있었다.

현재까지의 비디오 코덱 발달 과정을 살펴보면 앞으로 H.264 SE 코덱이 모바일 및 일반 웹환경을 포괄하는 비디오 콘텐츠 배포 시장에서 보다 일반화되고 범용성을 띄게 될 것임을 쉽게 예측할 수 있다. 제안하는 정보보호 기법은 기존 DRM 기법들이 처리할 수 없는 H.264 SE의 가변적 데이터 전송 특성을 만족

하므로 향후 비디오 콘텐츠 배포 환경에서 적용 가능한 비디오 콘텐츠 정보보호 기법이라 할 수 있겠다.

참 고 문 헌

[1] 강정원, 김재곤, 홍진우, "통방융합 유비쿼터스 콘텐츠 서비스 기술," 전자통신동향분석, 제21권, 제4호, pp.34-44, 2006.

[2] A. Vetro, C. Christopoulos, and H. Sun "Video Transcoding Arghitectures and Techniques: An Overview," *IEEE Signal Processing Mag.*, Vol.20, No.1, pp. 18-29, 2003.

[3] M. Wien, H. Schwarz, and T. Oelbaum, "Performance Analysis of SVC," *IEEE Trans. Circuits Sys. Video Tech.,* Vol.17, No.9, pp. 1194-1203, 2007.

[4] S. Pateux, Y.K. Wang, M. Hannuksela, and A. Eleftheriadis, "System and Transport Interface of the Emerging SVC Standard," *IEEE Trans. Circuits Sys. Video Tech.,* Vol.17, No. 9, pp. 1149-1163, 2007.

[5] S. Wenger and T. Schierl, "RTP Payload for SVC," *IEEE Trans. Circuits Sys. Video Tech.,* Vol.17, No.9, pp. 1204-1217, 2007.

[6] D. Singer, T. Rathgen, and P. Amon, "File Format for SVC," *IEEE Trans. Circuits Sys. Video Tech.,* Vol.17, No.9, pp. 1174-1185, 2007.

[7] J.R. Ohm, "Advances in Scalable Video Coding," *Proc. IEEE,* Vol.93, No.1, pp. 42-56, 2005.

[8] M. Winken, H. Schwarz, D. Marpe, and T. Wiegand, "Adaptive Refinement of Motion information for Fine-Granular SNR Scalable Video Coding," pp.161-164, *Proc. of EuMob '06*, 2006.

[9] *Digital Video Broadcasting Content Protection & Copy Management(DVB-CPCM)*, DVB Document A094 Rev. 1, 2007.

[10] *Open Mobile Alliance, Digital Rights Management 2.0* (OMA DRM2.0), 2006.

[11] HDCP (High-bandwidth Digital Content Protection System), http://en.wikipedia.org/wiki/HDCP

[12] COPP(Certified Output Protection Protocol), http://msdn2.microsoft.com/en-us/library/Aa468617.aspx

[13] DTCP(Digital Transmission Content Protection), http://en.wikipedia.org/wiki/DTCP

[14] 윤지선,이석환,송윤철,장봉주,권기룡,김민환, "MPEG-4 스케일러블 비디오 코딩 및 멀티미디어 트랜스코딩에 강인한 블라인드 비디오 워터마킹," *멀티미디어학회논문지*, 제11권 제10호, pp.1347-1358, 2008년 10월

[15] Nicolas Courtois and Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations," *Proc. of ASIACRYPT 2002*, pp. 267-287, 2002.

[16] Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag Berlin, 2002.

[17] Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer-Verlag Berlin, 2009.

[18] Jing Zhang, Anthony, T.S. Ho, Gang Qiu, and Pina Marziliano, "Robust Video Watermarking of H.264/AVC," *IEEE Trans. Circuits Sys. Video Tech.,* Vol.54, No.2, pp. 205-209, 2007.

[19] J. Reichel, H. Schwarz, and M. Wien, *JSVM 9.8 Software*, Joint Video Team of ISO/IEC MPEG and ITU-T VCEG N9212, Geneva, 2007.

[20] ftp://ftp.tnt.uni-hannover.de/pub/svc/testsequences/

김 원 제

2004년 부산외국어대학교 전자공학과 학사 졸업(공학사)
2009년 부경대학교 컴퓨터공학과 석사 졸업(공학석사)
2009년~2011년 (주)지엑스 연구원
2012년 현재 (주)영우DSP 연구원

관심분야 : 임베디드시스템SW, 멀티미디어 정보처리

성 택 영

2004년 부산외국어대학교 전자공학과 학사 졸업(공학사)
2006년 부산외국어대학교 전자컴퓨터공학과 석사 졸업(공학석사)
2007년~현재 부경대학교 정보보호학협동과정 박사과정

관심분야 : 멀티미디어 신호처리, 워터마킹

이 석 환

1999년 경북대학교 전자공학과 학사 졸업(공학사)
2001년 경북대학교 전자공학과 석사 졸업(공학석사)
2004년 경북대학교 전자공학과 박사 졸업(공학박사)

2005년~현재 동명대학교 정보보호학과 조교수
관심분야 : 워터마킹, DRM, 영상신호처리

권 기 룡

1986년 경북대학교 전자공학과 학사 졸업(공학사)
1990년 경북대학교 전자공학과 석사 졸업(공학석사)
1994년 경북대학교 전자공학과 박사 졸업(공학박사)

2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2006년 부산외국어대학교 디지털정보공학부 부교수
2011년~2012년 Colorado State Univ., Visiting Scholar
2006년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 멀티미디어정보보호, 영상처리, 멀티미디어 통신 및 신호처리