Journal of Korea Multimedia Society Vol. 16, No. 7, July 2013(pp. 841-851)
http://dx.doi.org/10.9717/kmms.2013.16.7.841

생물학적 유기체 모델을 이용한 가역 워터마킹 기반 비디오 콘텐츠 관리 및 제어 기법

장봉주[†], 이석환[††], 권기룡[†††]

요 약

생물학적 유기체 모델에서의 바이러스 특성을 이용한 전염성 정보은닉 시스템은 비디오 인코더 및 디코더에 대해 각각 최적의 워터마크 은닉 및 검출 방법을 적용하고 비디오의 재생 또는 편집 등이 발생할 때마다 워터마크를 전이시킴으로써 각종 공격에 강인하게 함으로써 비디오 콘텐츠의 안전한 유통을 가능하게 하기 위한 방법이다. 본 논문은 전염성 정보은닉 시스템을 위한 전염성 정보의 생성과 빠르고 효율적인 가역 워터마킹 기법을 제안한다. 제안 기법은 비디오 콘텐츠 기반 가역 워터마킹을 위해 제어 코드및 콘텐츠 유효기간을 워터마크와 결합하여 전염시킨 후, 비디오 재생 시에 능동적으로 콘텐츠의 화질 및 워터마크 강도를 제어할 수 있으며, 실시간성을 만족하기 위해 계산복잡도가 낮게 설계되었다. 또한, 가역 워터마크 복원을 위한 시간지연이 발생하지 않도록 매크로블록 단위의 워터마크 및 부가정보 은닉이 수행된다. 실험결과 제안 기법이 실시간성을 만족하며, 공격받지 않은 비디오 비트스트림에 대해 가역 워터마크 검출 및 영상 복원 후 워터마크 손실은 0%였으며, 복원 후의 화질은 동일한 비트율로 압축한 비디오와 거의 동일함을 확인하였다.

Reversible Watermarking based Video Contents Management and Control technique using Biological Organism Model

Bong-Joo Jang[†], Suk-Hwan Lee[††], Ki-Ryong Kwon[†††]

ABSTRACT

The infectious information hiding system(IIHS) is proposed for secure distribution of high quality video contents by applying optimized watermark embedding and detection algorithms to video codecs. And the watermark as infectious information is transmitted while target video is displayed or edited by codecs. This paper proposes a fast and effective reversible watermarking and infectious information generation for IIHS. Our reversible watermarking scheme enables video decoder to control video quality and watermark strength actively for by adding control code and expiration date with the watermark. Also, we designed our scheme with low computational complexity to satisfy it's real-time processing in a video codec, and to prevent time or frame delay during watermark detection and video restoration, we embedded one watermark and one side information within a macro-block. Experimental results verify that our scheme satisfy real-time watermark embedding and detection and watermark error is 0% after reversible watermark detection. Finally, we conform that the quality of restored video contens is almost same with compressed video without watermarking algorithm.

Key words: Infectious Information Hiding(전염성 정보은닉), Reversible Water-marking(가역 워터마킹), Video Watermarking(비디오 워터마킹)

※ 교신저자(Corresponding Author) : 권기룡, 주소 : 부산광역시 남구 대연 3동 부경대학교 대연캠퍼스 1316호(608-737), 전화 : 051) 629-6257, FAX : 051) 629-6230, E-mail : krkwon@pknu.ac.kr
접수일 : 2013년 4월 17일, 수정일 : 2013년 6월 9일
완료일 : 2013년 6월 10일
[†] 부경대학교 정보보호학협동과정
(E-mail : roachjbj@korea.com)
[††] 동명대학교 정보보호학과
(E-mail : skylee@tu.ac.kr)
[†††] 부경대학교 정보보호학협동과정
※ 본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2011-0010902, 2011-0023118).

1. 서 론

오늘날, 고화질 영상 입출력 장치의 발전에 기인하여 DVD 또는 블루레이급 화질의 비디오 콘텐츠를 넘어 UHDTV 및 3DTV 등의 실감영상 콘텐츠 산업이 급성장 중이다. 그와 함께 국내에서 서비스되던 기존의 아날로그 지상파 방송이 디지털 지상파 방송으로 전환됨에 따라 고화질 디지털 비디오 및 3D 비디오 콘텐츠 또는 고화질 IPTV 서비스 시장은 황금기를 맞이하고 있다. 그 결과 상업적인 목적의 비디오 콘텐츠가 다양화되고 수적, 질적으로 증가됨에 따라 비디오 콘텐츠의 건전한 유통과 콘텐츠의 저작권/소유권 또는 모니터링에 관한 관심 역시 비디오 콘텐츠 시장과 관련한 여러 분야에서 중요한 이슈가 되고 있다. 현재는 유료 비디오 콘텐츠에 대해 구매를 통한 별도의 과금을 부가한다거나, 인가되지 않은 사용자에 대해 콘텐츠를 암호화와 스크램블(scramble) 등의 기법으로 접근을 차단하는 방법을 주로 사용하고 있다. 여기서 암호화와 스크램블 기법의 차이는 원본 데이터로부터 보안이 적용된 데이터의 형태에 따라 구분될 수 있다. 일반적으로 암호화의 경우, 암호화 알고리즘에 의해 원본 데이터의 각 원소들이 새로운 형태로 변형되는 것을 의미하며, 반면 스크램블 기법은, 원본 데이터의 각 원소들의 형태는 유지한 채 그 위치가 뒤바뀌도록 설계하는 기법을 의미한다. 한편, 비디오 콘텐츠의 저작권 및 소유권에 관한 분쟁을 해결하기 위해 다양한 알고리즘의 워터마킹(watermarking)기법을 사용하기도 한다. 하지만 양질의 비디오 콘텐츠의 보호를 위해 그런 중요한 기술들이 꾸준히 발전하고 있음에도 불구하고, 디지털 미디어가 갖는 고유의 특성인 복제와 편집, 이동 및 관리의 용이성의 역효과로 인해 비디오 콘텐츠의 불법유통을 근절하기에는 현재까지도 어려운 점이 있다. 이러한 여러 문제들을 해결하기 위해 비디오 콘텐츠의 암호화 및 워터마킹에 대한 연구들이 진행되어 왔다[1,2].

그 중, 배포된 콘텐츠의 저작권 또는 소유권을 보호할 수 있는 기술로써 암호화와는 다른 접근법인 비디오 워터마킹 기법들이 많이 연구되어왔다[3-6]. 비디오 콘텐츠의 저작권 및 소유권 정보를 워터마크로 생성하여 지각적인 화질의 열화 없이 은닉하는 비디오 워터마킹은 그 사용 목적에 따라 강성 워터마킹, 연성 워터마킹 및 가역 워터마킹 등으로 구분할 수 있으며, 은닉 기법에 따라, 프레임 자체에 은닉하는 콘텐츠 기반 워터마킹과 코덱 내의 변환커널 또는 움직임 벡터 등과 같은 압축파라미터들을 이용하는 코덱 기반 워터마킹으로 분류할 수 있다. 이처럼, 대부분의 워터마킹 알고리즘들은 각각의 사용목적과 은닉기법에 따라 특징지어진다. 하지만 이런 알고리즘들 중에서 트렌스코딩, 재압축, 또는 각종 영상처리 등과 같은 다양한 공격들에 대해 강인성을 모두 만족하는 것은 현실적으로 어려운 일이다.

비디오 콘텐츠의 효과적인 저작권 및 소유권 보호에 대해 이런 문제점들을 고려하여, 장봉주 등[7]은 비디오 콘텐츠를 위한 전염성 정보은닉 시스템에 대해 소개하였다. 이 시스템은 비디오 콘텐츠와 비디오 코덱들 간의 관계를 생물학적 바이러스와 숙주의 관계로 모델링함으로써, 비디오 콘텐츠가 인코딩 및 디코딩 과정이 수행될 때마다 은닉된 워터마크에 대해 검출/변이/재은닉 과정을 수행하여 비디오 콘텐츠의 편집, 영상처리, 또는 트랜스코딩 등의 과정에서 워터마크가 전염되는 특성을 갖게 한다. 본 논문에서는 전염성 정보은닉 시스템의 기술요소 중 코덱 기반 정보은닉 기술을 위한 기법으로써 비디오 압축 기반 가역 워터마킹을 제안한다. 전염성 정보은닉 시스템의 각 기술 요소들이 갖는 특징과 기존의 가역 워터마킹 기법들에 대해서는 2장에서 설명되며, 제안하는 전염성 정보은닉 시스템을 위한 비디오 콘텐츠 가역 워터마킹 기법에 대해 3장에 설명한다. 4장으로부터 실험 결과 및 고찰을 수행하며, 5장의 결론으로 본 논문은 구성된다.

2. 관련 연구

어느 하나의 워터마킹 알고리즘을 압축 또는 프레임 영역에서 가능한 모든 공격들에 대해 강인성을 모두 만족하도록 설계하는 것은 어려운 것임을 서론에서 언급하였다. 장봉주 등[7]은 이런 문제를 해결하기 위해 생물학적 바이러스의 감염 원리에 착안하여 워터마크를 바이러스로, 또한 비디오 콘텐츠를 숙주로 간주하여 은닉된 워터마크를 비디오 인코더 및 디코더에 따라 각각의 방법으로 전이시킴으로써 각종 공격에 무관하게 워터마크를 보존할 수 있게 하는 전염성 정보은닉 시스템(infectious information hid-

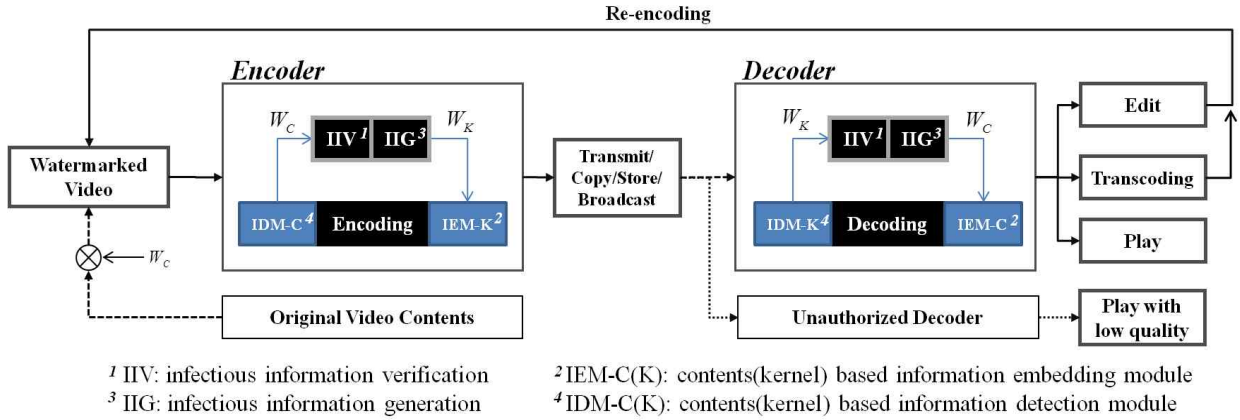


그림 1. 전염성 정보은닉 시스템 기반 비디오 콘텐츠 보안 시나리오

ing system, IIHS을 제안하였다. 그림 1로부터 IIHS의 구성과 시나리오에 대해 간략히 나타내었다.

그림 1로부터 정보의 전염은 코덱의 인코더와 디코더에 의해 수행되며, 일단 한번 워터마크가 은닉된 비디오 콘텐츠는 코덱 내에서 인코딩 단계의 전처리 과정으로 콘텐츠기반 정보검출 (contents based information detection module, IDM-C)를 통해 콘텐츠에 은닉된 강성 워터마크가 검출된다. 검출된 워터마크는 전염성 정보 인증 (infectious information verification, IIV)을 통해 인증 과정을 거친 다음, 다시 전염성 정보 생성 (infectious information generation, IIG) 단계에서 알고리즘에 적합한 워터마크로 변형/재생성된다. 그 후, 비디오 콘텐츠 인코딩 과정에서 변형된 워터마크가 IEM-K (kernel based information embedding module)를 통해 압축된 비디오 스트림에 은닉됨으로써 인코더 단에서의 정보 전염이 이루어진다. 한편, 워터마크가 은닉된 비디오 스트림에 대해 편집, 재생 등을 위한 디코딩을 수행할 때, 인코딩 시와 동일한 과정으로 워터마크 인증 및 재생산과 IDM-K 및 IEM-C를 통한 워터마크 검출 및 재은닉 과정이 수행된다.

따라서, 장봉주 등[7]에 의해 제안된 IIHS는 그림 1과 같은 순환 구조에서 워터마크는 인증 및 변형과정을 반복적으로 수행할 때마다 워터마크가 포함하는 정보가 반복적으로 갱신됨으로써 편집, 트랜스코딩 및 재압축 등에도 비디오 콘텐츠의 안전성을 보장하는 것을 목적으로 한다. 장봉주 등[7]의 IIHS 실험결과로부터 이종 코덱간의 트랜스코딩에도 워터마크는 온전하게 전염되며, 워터마크의 반복된 은닉이 화질 열화에 미치는 영향 역시 낮은 수준에서 머무르는 것을 확인하였다. 본 논문에서는 장봉주 등[7]에 의해 제안된 IIHS 모델링을 기반으로 IEM-K기법으로써 가역 워터마킹 알고리즘을 제안하고, 또한 그것을 위한 효과적인 워터마크 인증 및 활용 기법과 재생성과정을 제안하고자 한다.

한편, 가역 워터마킹은 콘텐츠 내 워터마크를 은닉함으로써 발생되는 지각적/비지각적 화질 열화에 대하여 워터마크 검출 과정에서 워터마크가 은닉되기 이전의 원영상으로 복원할 수 있게 하는 기법이다. 가역워터마킹 기술은 화질 열화에 대해 민감도가 높은 응용분야를 위해 설계되며, 주로 정지영상을 위한 알고리즘들이 연구되었으며, 최근 비디오 콘텐츠를 위한 가역 워터마킹 기법들도 연구되고 있다[8-15]. 대부분의 가역 워터마킹 알고리즘은 정지영상을 위해 제안되어왔다. 앞서 언급한 바와 같이 정지영상과 함께, 비디오 콘텐츠 또한 다른 멀티미디어 형식으로 다양한 분야에서 넓게 사용되지만 비디오를 위한 가역 워터마킹 기법들은 현재 많이 개발되지 않은 현실이다. 그 중 대부분은 비디오 프레임에 가역 워터마크를 은닉하기 위해 정지영상에서와 같은 알고리즘들 주로 사용하였다[13]. 하지만, 정지영상과는 달리 비디오는 시간축 상의 차원을 갖는다. 따라서 비디오 프레임을 단지 정지영상과 같이 취급하는 방법은 효과적이지 않다. Zeng 등[14]은 움직임 추정 및 예측에서 발생하는 오차를 확장하는 방법으로 비디오 콘텐츠에 대한 가역 워터마킹 기법을 제안하였다. 예측오차 확장에 기반 한 다른 가역워터마킹 기법들과는 달리, 움직임 추정은 이웃한 프레임들 간의 연관성을 검색하면서 각 영역들에 대한 예측 오차들을 계산함으로써 예측오차 분포를 명료하게 한다.

그런 다음, 계산된 예측오차분포를 확장하기 위해 예측오차 히스토그램 변환을 수행하여 해당 예측오차가 1로 변환되거나, 변환되지 않음으로써 1비트의 워터마크가 은닉되는 기법을 사용한다. 이 때, 워터마킹 기법의 가역성을 만족하기 위한 복원정보로써 약간의 부가정부가 생성되며 이 역시 워터마크와 함께 결합하여 비디오 콘텐츠에 은닉된다. 하지만 이 기법은 디코딩 과정에서의 순방향 워터마크 검출 및 프레임 복원을 위해 인코딩 시 시간 단위 프레임의 역순으로 워터마크가 은닉되어야 한다. 따라서 인코딩 순서와 반대되는 순서로 워터마킹을 수행하기 때문에 실시간 처리가 불가능하다. 또한 워터마크 은닉을 위해 프레임 간 예측 오차에 대한 히스토그램을 생성해야 하므로, 비디오 해상도에 따른 성능 저하 및 계산 복잡도 증가가 발생한다.

제안하는 논문은 그림 1의 전염성 정보은닉 시스템의 IEM-K와 IDM-K에 대하여 압축영역에서 수행되는 커널 기반 워터마크 은닉 및 검출 기법으로 비디오 콘텐츠의 화질 열화를 최소화하기 위해, 비디오 콘텐츠가 디코딩됨과 동시에 워터마크가 은닉된 프레임이 생성되므로 디코딩되는 압축스트림에서 워터마크가 제거되어도 문제가 되지 않는 특징을 근거로 하여 실시간성을 만족하는 가역 워터마킹 기법을 제안한다. 또한, 그림 1의 IEM-C 단계에서 워터마크의 은닉강도 및 비가시성 등을 능동적으로 제어하고, 비디오 콘텐츠의 유효기간, 또는 인가되지 않은 디코더/사용자에 따라 화질을 열화 시키기 위한 워터마크 생성/관리 기법을 제안한다.

3. 제안하는 기법

본 장에서는 전염성 정보은닉 시스템의 기술요소 중, 간단한 커널 기반 가역 워터마킹 기법과 워터마크로 표현되는 결합된 소유권 또는 저작권 정보와 유효 코덱 및 기간 인증을 위한 씨앗번호(seed number, SN), 재은닉 파라미터 등의 생성 및 관리 기법을 소개한다.

3.1 전염성 정보 생성 및 관리 기법

전염성 정보은닉 시스템에서는 프레임과 압축 파라미터로 구분되는 은닉 대상에 따라 적용되는 워터마킹 알고리즘이 콘텐츠기반 또는 커널기반으로 구분됨을 앞서 언급하였다. 그에 따라 전염성 정보로써 표현되는 워터마크의 형태 역시 각 알고리즘에 적합하게 변형되어야 한다[7,15]. [7]에서는 그림 1의 IEM-C를 위한 전염성 정보를 병원체 또는 감염체 워터마크로 정의하고, IEM-K에 은닉되는 전염성 정보를 돌연변이 워터마크로 정의하였다. 각 은닉모듈에 따라 워터마크 길이 또는 삽입 강도 등을 알고리즘에 적합하게 재생성하는 과정을 IIG 모듈에서 담당하며, 검출된 워터마크가 IIG 모듈에 의해 변이되기 전, 워터마크의 무결성을 검증하고 손상된 워터마크를 보정하는 역할을 IIV 모듈에서 수행한다. IIV 및 IIG 기술에 대해서 워터마크 은닉 모듈에 따라 의존적이므로 차후, 정보이론을 기반으로 한 연구가 필요한 부분이다. 그에 따라, 본 절에서는 이러한 IIV 및 IIG 과정이 수행된 것을 가정한 후, 제안하는 전염성 정보은닉 시스템의 가역 워터마킹 기법을 위한 '돌연변이'로 간주되는 전염성 정보의 구성을 정의한다. 전염성 정보는 기본적으로 콘텐츠의 저작권 또는 소유권 정보와, 비디오 코덱 인증을 위한 씨앗번호를 저장하며, 워터마킹 알고리즘에 따라 IEM-C 및 IEM-K에서 요구되는 파라미터 등을 각각 저장하는 제어코드(control code, cc) 저장공간을 제공한다. 또한 제안 기법은 IEM-K의 부가기능으로 전염성 정보 내에 유효기간 정보를 함께 삽입하여, 워터마크 검출 시에 인트라 프레임에서 검출한 정보를 이용하여 디코더의 시스템 시간을 검사함으로써 인터 프레임들의 화질을 열화시키는 역할을 수행하도록 설계한다. 식 (1)로부터 제안 기법을 위한 돌연변이 전염성 정보(mutant infectious information, MII)에 대하여 인트라 및 인터 프레임에 따른 구성을 나타내었다.

$$MII=\begin{cases}\{SN(0), t_e, \mathbf{C_A}(M, K_A), cc\}, & \text{if } I\,Frame\\ \{SN(f\%gop), \mathbf{C_A}(M, K_A), cc\}, & \text{if } P \text{ or } BFrame\end{cases} \quad (1)$$

이 때, 씨앗번호를 생성하는 인덱스는 인트라 프레임일 때 '0'으로 고정하였으며, 인터프레임 일 때 GOP(group of picture)와 프레임번호 f에 대해 의존적으로 생성하여 디코딩 과정에서 의도적인 프레임 누락이 발생할 경우 코덱 인증이 불가하도록 설계하였다. 또한 유효기간 정의하는 시스템 시간을 t_e로써 MII에 포함하였다. 소유권 또는 저작권 정보 M은 그림 1의 정보 전염 과정에서 노출되는 것을 방지하기 위하여 사전에 대칭키 암호화 모듈 $\mathbf{C}_A(\bullet)$으로써 보호되며, 비디오 콘텐츠에 의한 분쟁이 일어날 경

우, 저작권자 또는 소유권자가 유일하게 소유한 복호화 키 K_A로부터 권한을 인증할 수 있다. cc는 IEM-C 또는 다른 IEM-K 알고리즘에 따라 삽입강도 등을 조절하는 파라미터 값을 저장하는 버퍼공간으로 사용된다. 워터마킹 알고리즘이나 비디오 콘텐츠의 해상도에 따라 가변되는 워터마크 용량성에 기인하여, M과 cc의 길이는 가변 할 수 있으며, 이렇게 조합되어진 MII는 인코더 및 디코더가 가진 동일한 암•복호화 키 K_V에 의해 대칭키 암호화 모듈 $\mathsf{C}_V(\bullet)$로써 식 (2)와 같이 암호화된 전염성 정보 X가 생성된다

$$X = \mathsf{C}_V(MII, K_V) \tag{2}$$

한편, IEM-K 및 IEM-D에 의해 비디오 콘텐츠의 유효시간을 제어하기 위해 유효시간변수 t_e와 코덱의 현재 시스템 시간 t_c를 이용하여 해당 프레임의 씨앗번호에 대한 워터마크 은닉 및 검출 키 k_C를 식 (3)과 같이 생성한다.

$$k_C = (-1)^u \bullet SN(i), \quad 0 \le i < gop, \tag{3}$$
$$u = \begin{cases} 0, & \text{if } i = 0 \text{ or } t_e - t_c > 0 \\ 1, & \text{otherwise} \end{cases}$$

생성된 k_C는 가역 워터마크 은닉 및 검출 시에 워터마크 위치를 결정하는 데 사용되며, 제안 기법에서는 식 (3)에 의해 워터마크 검출 시 디코더의 시스템 시간으로부터 유효시간이 경과된 경우 워터마크 은닉 시의 키 k_C와 다른 값이 생성되므로 워터마크 검출 및 비디오 복원이 불가능하게 할 수 있다

3.2 커널기반 가역 워터마크 은닉 기법

그림 1의 전염성 정보은닉 시스템에서 코덱기반 실시간 가역 워터마킹을 위해 제안 기법은 워터마크 비트를 주파수 변환 및 양자화 과정을 거친 계수들 중 선택하여 은닉하고, 이 때 생성되는 부가정보(side information) 역시 임의 계수에 함께 은닉한다. 은닉된 부가정보는 가역 워터마크 검출과정에서 비디오 콘텐츠의 복원을 위해 사용된다. 비디오 압축을 위한 대부분의 코덱들은 공통적으로 시공간 영역 상의 예측, 주파수변환 양자화, 스캐닝 및 엔트로피 코딩의 과정을 거치며, 제안하는 가역워터마킹 기법은 그림 2와 같이 그 중, 엔트로피 코딩 이전 단계에서 수행된다.

일반적으로 DCT(discrete cosine transform) 커

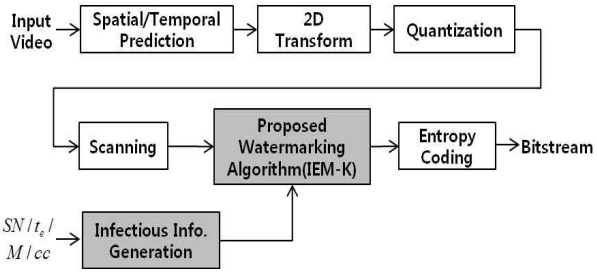


그림 2. 일반적인 비디오 인코딩 과정에서의 제안한 가역 워터마킹 기법

널을 사용하는 비디오 코덱에서는 하나의 MB가 여러개의 휘도신호 및 색차신호에 대한 주파수 변환 블록들로 구성되며, 이 때 1 MB 당 휘도신호의 주파수변환 블록 수(*LTB, luminance transform blocks*)는 세부 알고리즘에 따라 4개 또는 16개로 결정된다. 비디오의 인코딩 및 디코딩 과정에서 가역워터마킹의 실시간성을 만족하기 위해 제안하는 기법에서는 MPEG2 및 AVC 코덱에서의 기본적인 예측단위가 되는 MB(macro-block)을 기준으로 MB 내 조건을 만족하는 주파수 변환블록 당 1비트의 워터마크를 은닉한다. m번째 MB내에서 워터마크 은닉 후보 블록 $B_{W,m}$을 결정하는 것은 식 1로써 수행된다.

$$B_{W,m,n} = \begin{cases} B_{m,j}, & z_{i,B_{m,j}} \neq 0 \\ NULL, & z_{i,B_{m,j}} = 0 \end{cases}, \quad 4 \le i < 2^d,$$
$$d = \begin{cases} 6, & \text{if } LTB = 4 \\ 4, & \text{if } LTB = 16 \end{cases}, \tag{4}$$
$$\begin{cases} 0 \le j < LTB/2, & \text{if } seed(R(k_C)+m) = '1' \\ LTB/2 \le j < LTB, & \text{if } seed(R(k_C)+m) = '0' \end{cases}$$

여기서 k_C는 전염성 정보은닉 시스템에서 비디오 코덱의 인코더 및 디코더에서 각각 식 (3)에 의해 생성되는 고유의 키 값으로써 가역 워터마크 은닉 및 검출 알고리즘이 동일하며, 워터마크 검출 및 원영상 복원이 가능케 하여 해당 코덱이 전염성 정보은닉시스템에 의해 인증되었음을 검증하기 위해 사용된다. 식 (4)로부터 k_C에 의해 생성되는 난수 $R(k_C)$와 m을 이용하여 1 비트의 씨앗값(seed)를 추출한 후, 워터마크 은닉 블록 후보 $B_{W,m}$들이 결정된다. 또한, 1 비트의 워터마크 은닉에 따른 1비트의 복원정보를 은닉하기 위한 m번째 MB내의 후보 블록 $B_{S,m}$은 $B_{W,m}$와 대응되는 블록으로써 식 (5)로부터 결정된다.

$$B_{S,m,n} = \begin{cases} B_{m,LTB-j-1}, & z_{i,B_{m,LTB-j-1}} \neq 0 \\ NULL, & z_{i,B_{m,LTB-j-1}} = 0 \end{cases}, \quad 4 \le i < 2^d,$$

$$d=\begin{cases}6, & \text{if } LTB=4\\ 4, & \text{if } LTB=16\end{cases}, \quad (5)$$

$$\begin{cases}0\le j<LTB/2 & , \text{ if } seed(R(k_C)+m)='1'\\ LTB/2\le j<LTB, & \text{if } seed(R(k_C)+m)='0'\end{cases}$$

워터마크 은닉을 위한 MB 내의 $B_{W,m}$ 및 $B_{S,m}$ 후보들이 결정되면, 식 (6)에 의해 실제 워터마크와 부가정보가 은닉될 블록 $B_{T,l}$이 최종적으로 결정된다..

$$B_{T,l}=\{B_{W,l}, B_{S,l}\}|(B_{W,m,n}\neq NULL) \text{ and } (B_{S,m,n}\neq NULL) \quad (6)$$

식 (6)에 의해 하나의 인코딩 되는 프레임에 대해 각각 l개의 워터마크와 부가정보 비트가 은닉되는 주파수변환 블록을 결정할 수 있다. 워터마크 은닉을 위한 주파수 변환 블록 가 결정되면, 해당 $B_{W,m}$내에 워터마크 은닉 계수 또한 식 (7)과 같이 선택된다.

$$\begin{cases}c_{W,l}=First\,NZCof\,z_{B_{Wl}}(j)\\ c_{S,l}=First\,NZCof\,z_{B_{Sl}}(j)\end{cases},\ 4\le j<2^d \quad (7)$$

식 (7)로부터 식 (6)의 조건에 만족하는 휘도블록에 대한 주파수 계수들의 1차원 스케닝 된 결과값 z에 대해 4번째 계수 이후의 0이 아닌 최초의 계수(First NZC, first non zero coefficient)를 워터마크 또는 부가정보 은닉 계수로 결정한다. 주파수 변환블록 내에서 DC 계수 및 최저주파 계수 AC0, AC1 및 AC2에 대하여 워터마크와 부가정보 은닉에서 제외하는 것은 그림 1에서와 같이 IDM-K가 적용되지 않는 코덱이거나, k_C가 일치하지 않는 디코더에 대해 저주파 계수들만으로 디코딩을 수행하게 함으로써 저화질의 비디오 콘텐츠를 제공하는 서비스에 응용할 수 있게 하기 위해서이다.

최종적으로 주파수 블록 $B_{T,l}$와 $B_{T,l}$ 내의 워터마크 은닉 계수 $c_{W,l}$ 및 부가정보 은닉 계수 $c_{S,l}$이 선택 되면, 우선 식 (5)를 통해 $c_{W,l}$의 부호값을 이용하여 식 (2)의 워터마크 X의 각 비트 x_l를 은닉하게 되며,

$$c^*_{W,l}=\begin{cases}|c_{W,l}| & , \text{ if } x_l='1'\\ -1\bullet|c_{W,l}|, & \text{if } x_l='0'\end{cases} \quad (8)$$

이 때, 워터마크가 은닉 계수 $c_{W,l}$는 워터마크 w_l에 의해 $c^*_{W,l}$로 변환되는데 가역 워터마킹을 위해 워터마크 검출 시에 원래의 계수 값으로 복원해야 하므로 부가정보 s_l이 요구된다. 부가정보 s_l는 워터마크 x_l로 인한 $c_{W,l}$의 변경 여부에 따라 식 (9)으로부터 결정된다.

$$s_l=\begin{cases}'1', & \text{if } c_{W,l}=c^*_{W,l}\\ '0', & \text{if } c_{W,l}\neq c^*_{W,l}\end{cases} \quad (9)$$

1 비트의 부가 정보 s_l은 하나의 MB 내에서 $c_{W,l}$와 쌍을 이루는 $c_{S,l}$에 은닉된다. s_l은 자체적으로 검출되어야 하는 정보이며, 식 (9)를 통해 워터마크 검출 후 $c^*_{W,l}$로부터 원래의 계수값 $c_{W,l}$를 복원하는 역할을 한다. 부가정보 s_l가 은닉되는 과정을 식 (10)으로 나타내었다.

$$\begin{aligned}&\text{if } (s_l='1')\\ &\quad c^*_{S,l}=(c_{S,l}\ll 1)+1\\ &else\\ &\quad c^*_{S,l}=c_{S,l}\ll 1\end{aligned} \quad (10)$$

3.3 커널기반 가역 워터마크 검출 및 비디오 복원 기법

제안한 기법에서 가역 워터마크 검출 및 비디오 복원은 그림 2의 역과정으로써 수행된다. 우선, 수신된 비트스트림으로부터 I-프레임의 엔트로피 디코딩을 수행할 때 검출되는 워터마크로부터 추출한 유효시간 정보와 현재의 시스템 시간에 대해 식 (3)을 이용하여 디코더에 포함 된 난수 생성기로부터 k^*_C를 생성하고, 이후 프레임에 대해 k_C를 이용하여, (4)-(7)의 과정을 거침으로써 워터마크와 부가정보가 은닉된 계수들을 찾는다. 우선 단일 계수값 만으로 검출 가능한 부가정보 비트 $\bar{s}_l$를 검출하기 위해 식 (11)의 과정으로부터 엔트로피 디코딩 된 계수값 $\hat{c}_{S,l}$의 LSB를 판별하는 방법을 사용한다.

$$\bar{s}_l=\begin{cases}'1', & \text{if } LSB\ of\ \hat{c}_{S,l}\ is\ '1'\\ '0', & \text{if } LSB\ of\ \hat{c}_{S,l}\ is\ '0'\end{cases} \quad (11)$$

이 때, 식 (10)으로부터의 역과정에 의해 $\hat{c}_{S,l}$는 인코딩 과정에서의 $c_{S,l}$와 동일한 $\overline{c_{S,l}}$가 식 (12)로부터 복원된다.

$$\overline{c_{S,l}}=\hat{c}_{S,l}\gg 1 \quad (12)$$

그 후, 워터마크가 은닉된 계수 $\hat{c}_{W,l}$로부터 워터마크 $\bar{w}_l$는 식 (13)에 의해

$$\bar{w}_l=\begin{cases}'1', & \text{if } \hat{c}_{W,l}>0\\ '0', & \text{if } \hat{c}_{W,l}<0\end{cases} \quad (13)$$

로 검출되며, 식 (11)에 의해 검출된 $\bar{s}_l$와 식 (14)을 이용하여 $\hat{c}_{W,l}$를 복원함으로써 $\overline{c_{W,l}}$를 얻을 수 있다.

그림 3.실험에 사용한 1280×544@24fps 비디오 영상

$$\overline{\overline{c_{W,l}}}=\begin{cases}\widehat{c_{W,l}} & , \text{ if } \overline{s_l}='1' \\ \widehat{c_{W,l}}\bullet(-1), & \text{if } \overline{s_l}='0'\end{cases} \quad (14)$$

이 때, 콘텐츠의 유효기간이 만료되었다고 판단되거나, 디코더의 난수 생성기가 인코더의 것과 다름으로 인해 인증되지 않은 디코더로 간주 될 경우에 k_C^*는 인코딩에서 사용된 k_C과 전혀 다른 값을 가지게 된다. 따라서, k_C와 다른 값을 갖는 k_C^*로부터 워터마크 은닉 위치를 알 수 없게 되어 식 (12) 및 (14)에 의해 워터마크가 은닉되지 않은 주파수 계수를 변형시키게 되며, 워터마크로 인해 변형된 계수 역시 복원되지 않으므로, 전체적인 화질의 열화가 발생하게 된다.

최종적으로 검출 및 복호화 과정을 거친 *MII* 정보는 [7]의 기법에서 제안된 것과 같은 컨텐츠 기반 강성 워터마크 전염 모듈 IEM-C을 위한 전염성 정보로써 변이될 수 있으며, 이 때, 제어코드 cc로부터 IEM-C의 삽입강도, 은닉위치 및 기타 알고리즘의 파라미터를 결정하기 위해 사용된다.

4. 실험 결과

제안한 전염성 정보은닉을 위해 IEM-K 및 IDM-K 모듈에 적용되는 가역 워터마킹 기법의 성능 평가를 위해 MPEG2 비디오 코딩 방식을 사용하였으며, 그림 3과 같이 1280×544 @24fps 비디오 45 프레임에 대해 GOP=15로 설정한 후 실험을 수행하였다.

제안한 가역 워터마킹 기법에서 워터마크 길이는 대상 비디오 영상의 해상도와 압축율에 따라 식 (1)의 제어신호 및 저작권 정보의 길이를 조절함으로써 결정할 수 있다. 제안 기법에서 식 (6)의 조건을 이용하여 그림 3의 비디오에 대해 워터마크 용량성을 계산하여 그림 4에 나타내었다.

그림 4로부터 그림 3의 비디오 영상에 대해 프레임당 총 5440개의 MB 중 평균 2300여개 정도의 MB에 대해 워터마크 은닉이 가능하므로, 제안 기법이 높은 수준의 워터마크 용량성을 확보할 수 있음을 확인하였다. 또한 비트율 제어 알고리즘에 의해 I-frame 이후의 프레임에 대해 낮은 워터마크 용량성을 보임에 따라, 제안 기법의 워터마크 용량성이 영상의 공간 해상도 뿐 아니라, 압축율에 따라서도 좌우됨을 확인하였다. 그에 따라, 그림 3의 비디오 해상도에 대한 실험을 위해 식 (1)로부터 256비트의 암호화된 저작권 정보와 64비트의 유효시간정보 t_e 및 32비트의 씨앗값, 그리고 IEM-C를 위한 제어신호로써 임의로 생성된 160비트가 결합된 총 512비트의 돌연변이 전염성 정보 MII를 생성하였다. 이 MII를 이용

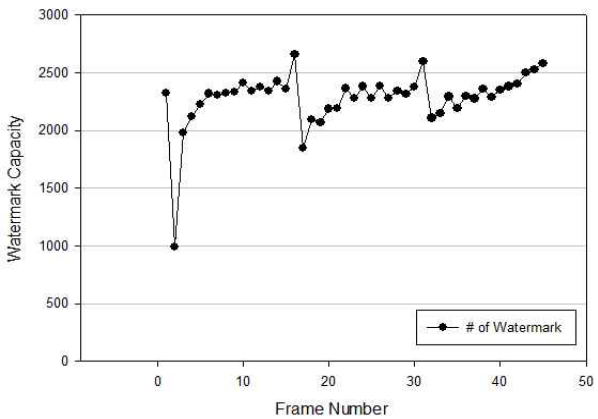


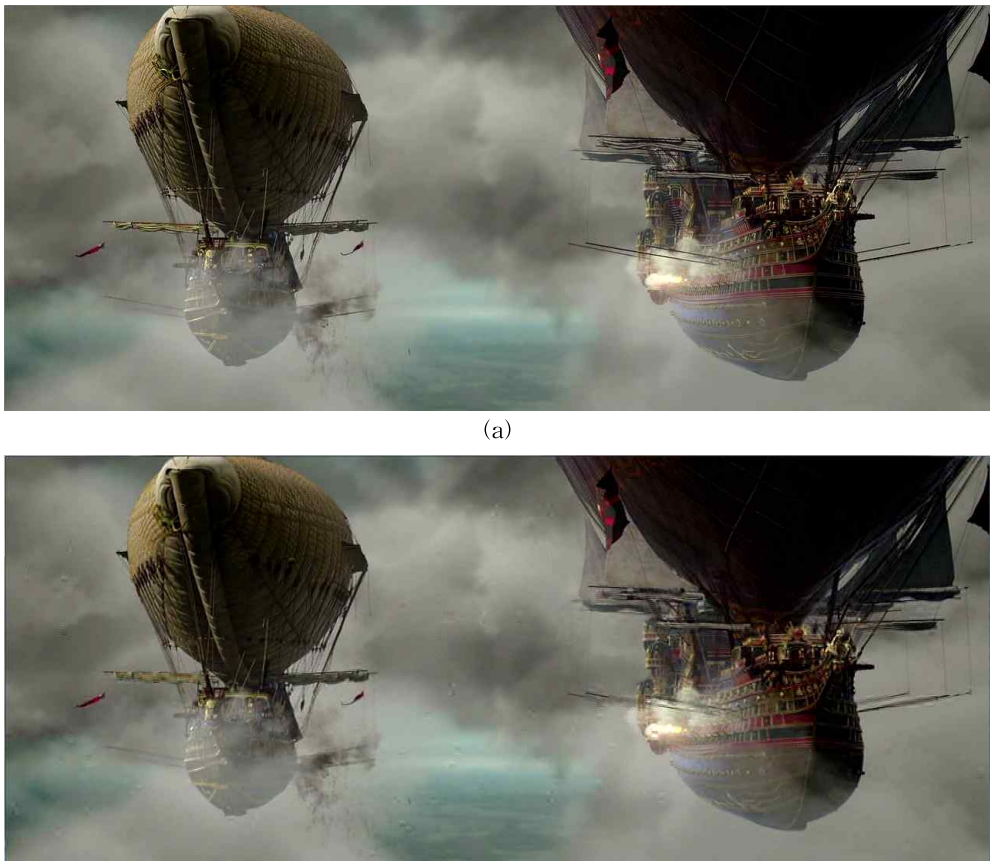
그림 4. 제안한 가역 워터마킹 기법의 그림 3에 대한 워터마크 용량성

하여, 식(2)로부터 128bit DES 블록암호화 된 512 bit 길이의 워터마크 X를 생성하였으며, 그림 4로 나타낸 대상비디오의 용량성에 따라 워터마크 X가 반복적으로 삽입되도록 하였다.

제안한 기법은 기존의 비디오 기반 가역 워터마킹 기법들이 갖는 문제점 중의 하나였던 부가정보 검출 및 원영상 복원 시 발생하는 수 개의 MB 또는 프레임 딜레이, 심지어 콘텐츠 재생 역순으로 워터마크를 검출해야하는 문제점을 해결하고, 코덱 내에서 워터마킹 기법의 계산복잡도를 낮추기 위해 양자화된 주파수 계수에 대해 하나의 MB에 워터마크와 원영상 복원을 위한 부가정보 모두를 은닉한다. 실험 결과, 프레임 당 기존 인코딩 및 디코딩 시간 대비 제안한 알고리즘을 적용한 후 각각 평균 0.003ms 및 0.001 ms의 시간 지연이 발생하였다. 이로써, 제안 가역 워터마킹 기법이 실시간성을 만족함을 확인하였다,

제안 기법은 비디오 디코딩과 동시에 워터마크 정보가 검출되어 콘텐츠 기반 워터마킹 알고리즘으로써 전염성 정보를 전이시키기 위한 전염성 정보은닉 시스템의 코덱기반 가역 워터마킹으로 수행되므로 디코딩 된 프레임 영역에서의 공격은 평가대상에서 제외하였다, 따라서, 압축 비트스트림 상에서의 공격 강인성을 평가하기 위해, 그림 5로부터 정상적으로 워터마크 검출 및 복원이 수행된 비디오와 공격으로 간주되는 임의의 워터마크를 다시 은닉한 후, 복원 과정을 수행하였을 때의 비디오를 나타낸 것이다.

그림 5에서처럼, 압축 비트스트림 상에서 워터마크 제거 또는 다른 워터마크에 의한 공모공격 등이 발생할 경우, 식 (4) 및 식 (5)로부터 워터마크 검출 위치를 결정하는 씨앗값 및 키 값의 손상이 야기되어 결과적으로 부가정보와 워터마크의 손상 뿐 아니라 정확히 검출되지 못한 워터마크와 부가정보로 인한 블록킹 현상이 발생한다. 매 프레임마다 산발적으로 발생하는 이런 블록킹 현상은 특히 고해상도의 동영상 서비스에서 심각한 화질 열화를 초래하므로 제안 기법이 압축 스트림 상에서의 공격에 대한 내성을



(a)

(b)

그림 5. 제안한 가역 워터마킹 기법에서 (a) 정상적으로 워터마크 검출 및 복원된 비디오 프레임과 (b)워터마크 재은닉 공격에 의한 복원 오류로 인한 블록킹 현상이 발생한 비디오 프레임

가짐을 알 수 있다.

앞서 식 (3)에 의해 워터마크 검출 및 비디오 복원 키 k_C의 생성을 위해 적용된 코덱의 시스템 시간 t_e이 경과된 이후의 디코딩이나, 인가되지 않은 디코더에 의한 비디오 재생 시 DCT 레벨에서 워터마크 및 부가정보에 의한 블로킹을 제거함으로써 제안 기법이 저화질 또는 낮은 해상도의 비디오 서비스를 가능케 함을 그림 6으로 나타내었다.

한편, 비디오 워터마킹에서는 워터마크로 인한 비디오 콘텐츠의 압축효율 변화에 주목할 필요가 있다. 압축 비트스트림 또는 양자화 테이블을 수정하는 워터마킹 알고리즘들은 사전 정의된 비트율에 따를 경우, 워터마킹으로 인한 화질열화가 발생할 수 있다. 엔트로피 코딩 단계에서 워터마킹으로 데이터 수정이 가해졌을 때 의도치 않은 비트율 증가가 발생하며, 그것은 다음 압축 단계에서 더 높은 양자화 파라미터 값을 요구하게 된다. 제안한 기법 역시 그림 2에서와 같이 엔트로피 코딩 단계에서 워터마크를 은닉

(a)

(b)

(c)

그림 6. 제안 기법에서 비인가된 디코더 또는 유효기간 만료 이후의 비디오 콘텐츠의 화질 열화 서비스 제공, (a) 워터마크 검출 및 복원 영상, (b) 비인가코덱 및 유효기간 만료에 따른 저화질 비디오 서비스, (c) (b)의 저화질 영상을 낮은 해상도로 변환한 비디오

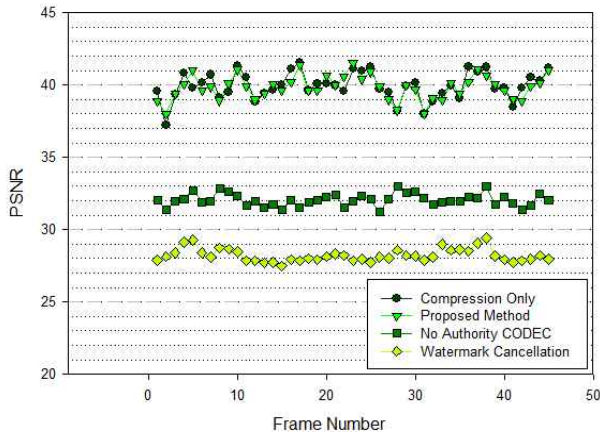


그림 7. 제안한 가역워터마킹 기법으로 인한 화질 열화 비교

하므로 비트율 증가로 인한 화질 저하를 예상하여 원영상 및 가역 워터마크 복원, 그리고 그림 5-(b) 및 6-(b)의 화질열화 된 비디오에 대해 각각의 PSNR을 그림 7로써 비교하였다.

제안 기법이 워터마크 은닉 시 계수의 부호값 만을 변경시키며 부가정보를 은닉 할 때 '0'이 아닌 값을 갖는 계수들을 이용함으로써 엔트로피 코딩의 효율 저하를 최소화하였다. 그로 인해 그림 7에서 나타낸 바와 같이 워터마크를 은닉하지 않았을 때와 비교하여 거의 동일한 PSNR을 가지는 것을 확인하였다.

5. 결 론

제안한 기법은 비디오 콘텐츠의 안전한 유통을 위해 비디오 코덱을 기반으로 하는 전염성 정보은닉 시스템을 위한 전염성 정보의 생성과 빠르고 효율적인 가역 워터마킹 기법을 제안하였다. 제안 기법은 정보 전염을 위해 IEM-C 알고리즘을 위한 제어 코드와 함께 정보은닉 키로써 콘텐츠 유통 유효기간 정보를 함께 사용함으로써 정보의 전염 시 능동적으로 콘텐츠의 화질 및 워터마크 강도를 제어할 수 있게 한다. 또한 실시간성을 만족하기 위해 양자화된 주파수 계수에 대해 하나의 MB에 워터마크와 원영상 복원을 위한 부가정보 모두를 은닉하므로, 계산복잡도가 낮으며, 부가정보 검출 및 원영상 복원을 위해 MB 또는 프레임 딜레이가 발생하지 않는 장점이 있다. 또한 제안 가역워터마킹 기법이 임의의 비트스트림 공격이 발생할 경우 복원정보의 손상을 일으켜 비디오 화질 훼손을 발생시키므로, 비디오 콘텐츠에 대한 공격시도를 차단할 수 있는 역할을 함을 실험을 통해 확인하였다. 공격받지 않은 비디오 비트스트림에 대해 가역 워터마크 검출 및 영상 복원 후 워터마크 손실은 0%였으며, 복원 후의 비디오 콘텐츠의 화질은 동일한 비트율로 압축한 비디오와의 PSNR 비교에서 수치상 미소한 차이를 보였으나, 평균적으로 거의 동일함을 확인하였다. 또한 제안 기법으로 인가되지 않은 디코더를 사용하였을 때, 혹은 콘텐츠 유효기간이 지났을 경우, 가역워터마킹 제거 및 디블로킹 과정을 수행하여 절반의 해상도나 PSNR 30dB 이하의 저화질 영상을 제공함으로써, 콘텐츠 홍보, 무료 재생 서비스 등의 다양한 응용이 가능함을 확인하였다. 향후, 제안한 가역 워터마크를 디코딩 한 후, 검출된 정보와 제어코드 등을 이용한 콘텐츠 기반 강성 워터마킹에 대한 알고리즘을 개선하고, 전염성 정보 구성 및 오류 복원에 대한 연구를 진행함으로써 급격히 발전하고 있는 고화질, 고차원 비디오 콘텐츠에 대한 보다 건전한 유통에 기여 할 수 있을 것으로 기대한다.

참 고 문 헌

[1] Zheng Liu and Xue Li, "Motion Vector Encryption in Multimedia Streaming," *Proc. of 10Th international Conference of Multimedia Modelling Conference*, pp. 64-71, 2004.

[2] B. Furht and D. Kirovski, *Multimedia security handbook*, CRC Press LLC, Boca Raton, FL USA, 2004.

[3] A.M. Alattar, "Reversible Watermark using the Difference Expansion of a Generalized Integer Transform," *IEEE Trans. Image Process.*, Vol. 13, No. 8, pp. 1147-1156, 2004.

[4] J.M. Zain, L.P. Baldwin, and M. Clarke, "Reversible Watermarking for Authentication of Dicom Images," *Proc. the 26th Annual International Conference of the Engineering in Medicine and Biology Society*, pp. 3237-3240, 2004.

[5] 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.

[6] 윤지선, 이석환, 송윤철, 장봉주, 권기룡, 김민환, “MPEG-4 스케일러블 비디오 코딩 및 멀티미디어 트랜스코딩에 강인한 블라인드 비디오 워터마킹,” 멀티미디어학회논문지, 제11권, 제10호, pp. 1347-1358, 2008.

[7] 장봉주, 이석환, 권기룡, “생물학적 바이러스를 이용한 비디오 콘텐츠의 전염성 정보은닉 시스템 모델링,” 전자공학회논문지, 제49권, 제CI3호, 2012.

[8] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, “Lossless Generalized-LSB Data Embedding,” *IEEE Trans. on Image Processing*, Vol. 14, No. 2, pp. 253-266, 2005.

[9] D.M. Thodi and J.J. Rodriguez, “Expansion Embedding Techniques for Reversible Watermarking,” *IEEE Trans. on Image Processing*, Vol. 16, No. 3, pp. 721-730, 2007.

[10] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding,” *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 16, No. 3, pp. 354-362, 2006.

[11] W.C. Kuo, D.J. Jiang, and Y.C. Huang, “Reversible Data Hiding Based on Histogram,” *International Conference on Intelligent Computing, Lecture Notes in Artificial Intelligence*, Vol. 4682, pp. 1152-1161, 2007.

[12] D.G. Yeo, H.Y. Lee, and B.M. Kim, “High Capacity Reversible Watermarking using Differential Histogram Shifting and Predicted Error Compensation,” *Journal of Electronic Imaging*, SPIE, Vol. 20, No. 1, 2011.

[13] J. Tian, “Reversible Data Embedding using a Difference Expansion,” *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896, 2003.

[14] X. Zeng, Z.Y. Chen, M. Chen, and Z. Xiong, “Reversible Video Watermarking using Motion Estimation and Prediction Error Expansion,” *Journal of Information Science and Engineering,* Vol. 27, No. 2, pp. 465-479, 2011.

[15] 장봉주, 이석환, 권기룡, “전염성 정보은닉 시스템을 위한 능동형 비디오 워터마킹 기법,” 멀티미디어학회논문지, 제15권, 제8호, pp. 1017-1030, 2012.

장 봉 주

2002년 부산외국어대학교 전자공학과 학사
2004년 부산외국어대학교 전자컴퓨터 공학과 석사
2007년~현재 부경대학교 정보보호협동과정 박사과정

관심분야 : 영상압축, 멀티미디어 정보보호,

이 석 환

1999년 경북대학교 전자공학과 학사
2001년 경북대학교 전자공학과 석사
2004년 경북대학교 전자공학 박사

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

권 기 룡

1986년 경북대학교 전자공학과 학사
1990년 경북대학교 전자공학과 석사
1994년 경북대학교 전자공학과 박사

1996년~2005년 부산외국어대학교 디지털정보공학부 부교수
2006년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 멀티미디어 정보보호, 영상처리, 멀티미디어 통신 및 신호처리