전염성 정보은닉 시스템을 위한 능동형 비디오 워터마킹 기법

장봉주^{*}, 이석환^{**}, 권기룡^{***}

요 약

현재까지 대부분의 비디오 콘텐츠에 대한 워터마킹 기법들은 최초의 콘텐츠에 저작권자 정보를 은닉한 후, 압축 및 각종 신호처리를 공격으로 간주하여 상대적인 강인성과 비가시성을 우수하게 설계하는 것으로서 연구되어왔다. 제안 기법은 워터마크와 제어신호를 전염성을 가진 정보로 간주하고 비디오 인코더에 은닉된 정보를 이용하여 디코더로부터 능동적으로 워터마크를 전염시키는 방법을 제안한다. 제안 기법을 위해 워터마크와 함께 화질제어 및 삽입강도 가변파라미터를 같이 은닉하는 커널 기반 워터마킹을 수행하며, 이것은 인증되지 않은 워터마크에 대해 저화질의 비디오 콘텐츠를 제공할 수 있는 장점을 가진다. 또한 비디오 디코더에서는 워터마크 복호화를 단계에서 저작권자나 사용자가 개입되지 않고 능동적으로 콘텐츠 기반의 워터마킹을 수행하여 변이된 워터마크를 전염시키는 기법으로 트랜스코딩, 재압축 등과 같은 처리에도 워터마크와 화질의 손상 없이 재배포가 가능하도록 한다. 실험결과 워터마크로 인한 압축을 저하나 워터마크의 손상 없이 비디오 콘텐츠와 코덱에 의해 완벽하게 전염됨을 확인하였다.

Active Video Watermarking Technique for Infectious Information Hiding System

Bong-Joo Jang^{*}, Suk-Hwan Lee^{**}, and Ki-Ryong Kwon^{***}

ABSTRACT

Most watermarking schemes for video contents protection have been studied to increase watermark's robustness and invisibility against such compressions and many kinds of signal processing after embedding copyright information to the original contents. This paper proposes an active watermarking that infect watermark to contents in the video decoding process using embedded infectious watermark and control signals from a video encoder side. To achieve this algorithm, we design a kernel based watermarking in video encoder side that is possible to recover the original contents and watermark in watermark detection procedure perfectly. And then, by reversible de-watermarking in video decoder side, we design the active watermark infection method using detected watermark and control signal. This means that our system can provide secure re-distributions of video contents without any quality degradation and watermark bit error against transcoding or re-encoding processing. By experimental results, we confirmed that the embedded watermark was infected by video contents and codec perfectly without any declines of compression ratio and video quality.

Key words: Infectious Information Hiding(전염성 정보은닉), Active video Watermarking(능동형 비디오 워터마킹), video Redistribution(비디오 재배포), copyright protection(저작권 보호)

※ 교신저자(Corresponding Author): 권기룡, 주소: 부산 남구 대연3동 599-1번지(608-737), 전화: 051)629-6257, FAX: 051)629-6230, E-mail: krkwon@pknu.ac.kr
접수일: 2012년 2월 23일, 수정일: 2012년 6월 4일
완료일: 2012년 6월 15일

^{*} 준회원, 부경대학교 정보보호협동과정 박사과정
(E-mail: roachbjb@korea.com)

^{**} 정회원, 동명대학교 정보보호학과 교수
(E-mail: skylee@tu.ac.kr)

^{***} 종신회원, 부경대학교 IT융합응용공학과 교수
(E-mail: krkwon@pknu.ac.kr)

※ 본 연구는 2011년도 교육과학기술부의 재원으로 한국연구재단의 일반연구자지원사업의 지원을 받아 수행된 것임 (KRF-2011-0010902, KRF-2011-0023118).

1. 서 론

현재, 또한 향후 UHDTV, 3DTV 등과 같은 무한한 잠재시장을 가진 멀티미디어 비디오 콘텐츠의 저작권 및 건전한 유통을 보호하기 위해 디지털 워터마킹(digital watermarking)과, 콘텐츠 암호화에 관한 기술들이 무수히 제안되었음에도 불구하고, 실제 상용화되는 것은 극히 일부에 불과하다. 그것은 디지털 미디어가 갖는 특성인 복사, 편집의 용이성과 밀접한 연관이 있음은 부인하기 어렵다. 디지털 워터마킹으로 대변되는 콘텐츠 내 정보은닉기술의 경우[1-9], 다양한 경로를 통해 유통되면서 발생하는 무수한 변질에 모두 대응하도록 설계하는 것은 불가능한 것으로 여겨진다. 하나의 콘텐츠에 대해서 워터마크는 해당 워터마킹 기법이 의존하는 특정 코덱이나 그 기법이 갖는 특정 환경과 조건 내에서 은닉될 수밖에 없기 때문에 그 범위를 넘어서는 콘텐츠 변질에 대해서는 워터마크 강인성이 보장될 수 없는 것이다. 이런 이유로 특정 공격을 미리 예상하여 그 공격에 한정하여 워터마킹 알고리즘을 설계하고 적용할 수 있으므로, 그로 인해 범용성을 잃게 되는 기술적인 한계가 드러났다. 또한 의료영상 및 군사용 영상에 대해 가역 워터마킹(reversible watermarking) 기술 역시 다양하게 고안되었으나, 현재 국내에서 비디오콘텐츠를 위한 가역워터마킹 기법연구는 미비한 수준이다 [6-10].

한편 멀티미디어 콘텐츠 암호화 기술 역시 많은 연구가 진행되어온 콘텐츠 보호를 위한 기술로써, 콘텐츠 내용 자체 또는 압축과 같은 특정 변환 파라미터를 암호화하여 콘텐츠 내용을 보호하는 기술이다 [11-15]. 앞서 언급한 워터마킹이 콘텐츠 내 저작권 정보를 은닉한 후 유통시키는 소극적인 콘텐츠 보호 기법이라고 한다면 콘텐츠 암호화 기술은 콘텐츠 자체의 불법유통을 막기 위한 적극적인 콘텐츠 보호 기법으로 생각할 수 있다. 대부분의 콘텐츠 압축 기법들이 콘텐츠의 공간적, 시간적 잉여성분을 이용한 에너지 집중 및 반복되는 비트열을 이용하여 압축을 수행한다. 따라서 콘텐츠 내용을 암호화하는 이런 기술들은 이러한 압축 기술들의 성능을 저해하는 요소로 작용할 수 있다. 또한 고용량의 비디오와 같은 콘텐츠를 암호화 할 경우, 암호화 키(key)의 반복 사용이 공격자로부터 암호화 키가 추정될 수 있는 근거가

되므로, 알고리즘 설계 시에 많은 제약 조건이 따른다. 이런 조건들에 만족하는 콘텐츠 암호화를 수행한 후에도 여전히 암호화 키 유출에 대한 위험부담이 있으며, 좋은 알고리즘으로 암호화된 콘텐츠라도 한번 복호화 되어 재생된 후에 행해지는 복제, 편집 등의 처리에 대해서는 보호를 장담할 수 없다. 현재까지 압축 기술의 혁신적인 발전으로 인해, 하나의 비디오 콘텐츠에 대해, 편집, 재압축, 트랜스코딩(transcoding) 등의 일련의 유통과정에서 발생하는 변질은 특정 코덱(codec)의 '인코더(encoder)' 및 '디코더(decoder)'를 이용하여 이루어지는 것은 당연한 일이 되었다[16-22]. 그에 따라 많은 우수한 학자들이 이런 콘텐츠 압축에 대하여 워터마킹 및 콘텐츠 암호화기술들이 갖는 근본적인 문제들에 대해 고민하고 있으며, 본 논문 역시 그러한 문제에 대한 한 가지 대안을 제안하고자 한다.

한편, 비디오 콘텐츠를 대상으로 앞서 언급한 콘텐츠 보호기법들의 문제점을 해결하기 위해 최초 은닉한 정보가 편집, 재압축 및 트랜스코딩(transcoding) 등을 거쳐 재배포되는 경우에도 그대로 전달 되도록 하는 전염성 정보은닉(infectious information hiding, IHH) 시스템이 제안되었다[23]. 고용량 비디오 콘텐츠의 유통과정에서 필연적으로 '압축' 과정을 거치는 것에 착안한 이 시스템은 비디오 콘텐츠 보호를 위해 다양한 종류의 비디오 코덱을 숙주로 이용하여 비디오 인코딩 및 디코딩 과정에서 워터마크를 검출, 재은닉 함으로써 워터마크 정보를 편집 및 재배포 되는 콘텐츠에 전염시킬 수 있는 플랫폼을 제공하였다.

따라서, 본 논문에서는 효과적인 비디오 콘텐츠 보호를 위해 앞서 언급한 IHH 시스템의 플랫폼에 기반한 능동형 비디오 워터마킹(active video watermarking) 기법을 제안한다. 제안한 기법은 우선, 비디오 인코더 내에서 워터마크와 콘텐츠가 완전히 분리 가능한 가역 워터마킹 방식의 커널기반 IHH 기술로써 전염성 정보 및 제어신호를 은닉하여 비디오 압축을 수행한다. 그 후, 유통된 비디오 콘텐츠의 재생단계에서 디코더가 전염성 정보와 제어신호를 검출한 한 후, 복원된 비디오 프레임에 검출된 전염성 정보를 강성 워터마킹(robust watermarking) 기법을 이용하여 전염시킨다. 이 때, 디코더에서 검출된 제어신호를 이용하여 삽입강도, 삽입위치 등을 적용

적으로 결정하여 은닉함으로써, 디코더에서 콘텐츠 내 중요 정보에 따라 능동적으로(active) 정보은닉을 수행할 수 있게 한다. 이 단계에서 저작권자나 사용자가 개입되지 않고 능동적으로 콘텐츠 기반 IIH를 수행하여 변이된 워터마크를 전염시키는 기법으로 트랜스코딩, 재압축 등과 같은 처리에도 워터마크와 화질의 손상 없이 재배포가 가능하도록 하며, 콘텐츠 변형에 보다 적응적으로 대처할 수 있도록 한다. 실험결과 반복적으로 재은닉 되는 워터마크로 인해 최초 재은닉 시에만 1dB 미만의 한 화질 저하가 나타남을 확인하였으며, 그 이후의 워터마크 재은닉 횟수에 따른 화질 열화는 발생하지 않음을 알 수 있었다.

2. 전염성 정보은닉 시스템

전염성 정보 은닉 시스템은 비디오 콘텐츠 유통과정에서 일어날 수 있는 수정, 편집, 트랜스코딩 등의 각종 변질에 대해 효율적인 콘텐츠와 그것의 저작권 보호를 위해 고안되었다[23]. 이것은 앞서 언급한 바와 같이 기존의 비디오 콘텐츠의 저작권 보호를 위한 워터마킹 및 핑거프린팅과 같은 정보 은닉 기술들이 갖는 기술적인 한계를 극복하기 위해, 생물학적 바이러스의 개념을 적용함으로써 워터마크를 전염성을 갖는 암호화된 정보로 간주하여 비디오 콘텐츠의 변

질이 발생할 때마다 전염성 정보 역시 콘텐츠에 따라 변형, 재은닉 됨으로써 콘텐츠를 보호하는 개념이다. 이 시스템은 하나의 비디오 콘텐츠는 임의의 비디오 코덱의 인코더에 의해 압축되어 전송되고, 동일한 코덱의 디코더에 의해 재생되는 원리에 기인한다. 비디오 콘텐츠의 의도적인 변질을 위해서는 반드시 디코딩/인코딩 과정에 해당하는 재압축을 거쳐야 하며, 이 때, 전염성 정보는 코덱의 디코더로부터 또 다른 코덱의 인코더를 통해 은닉되어질 수 있는 것이다. 아래 그림 1은 전염성 정보은닉 시스템의 구성을 나타낸 것이며, 각 코덱들의 인코더 및 디코더에 각각 전염성 정보 검출 모듈(infectious information detection module, IDM)과 전염성 정보 은닉 모듈(infectious information embedding module IEM)을 탑재하였다.

IDM 및 IEM에서 사용되는 구체적인 기술 내용을 그림 1의 하단에 나타내었으며, 각각 감염 검사 및 권한 제어를 위한 전염성 정보 인증 기술(infectious information verification tool)과 숙주(커널) 기반 정보 감염 기술(kernel based IIH tool), 재생되는 비디오 콘텐츠에 대한 콘텐츠 자체 기반 정보 감염 기술(contents based IIH tool) 그리고 전염 바이러스성 정보의 워터마크 생성 및 관리 기술(infectious information generation tool) 등으로 구성된다. 이 각각

그림 1. 전염성 정보은닉기반 비디오 콘텐츠 보안 시스템 구성

의 기술들의 연동에 의해 정보가 전염되는 과정을 그림 2에 나타내었다. 이 때, 전염성 정보는 전염 시점, 전염 대상에 따라 변이될 수 있으며, 그 각각의 변이에 따라 병원체(pathogen), 돌연변이(mutant) 및 감염체(contagion)로 분류되며, 코덱의 종류에 따라, 그리고 콘텐츠의 변환영역(spatial/frequency)에 따라 워터마킹 알고리즘이 각각 설계된다.

그림 2는 IIIH 시스템 상에서 각각의 해당기술 부분과 전염성 정보은닉이 수행되는 과정을 나타낸 것이다. 그림 2에서는 최초 생성된 비디오 콘텐츠로부터 병원체 정보를 은닉하여 압축을 수행한 후, 배포 및 편집, 트랜스코딩을 거쳐 재배포 되는 상황에서 전염성 정보가 재은닉 되는 과정을 상세히 표현한다. 이 시스템에서는 전염성 정보은닉을 위해, 은닉하고자 하는 워터마크를 감염체 정보로 생성하여 최초의 비디오 콘텐츠 압축 과정에서 은닉한다. 이 때, 감염체 워터마크는 실시간성과 화질을 유지하기 위해 주파수 변환 커널에 기반한 가역 워터마킹 알고리즘으로써 은닉된다. 따라서 DWT(discrete wavelet transform), DCT (discrete cosine transform) 등과 같이 비디오 코덱이 사용하는 주파수 변환 커널에 따라 알고리즘이 각각 설계되어야 한다.

커널기반 IIIH에 의해 은닉된 병원체 및 감염체 정보는 비디오 콘텐츠의 복사, 스트리밍(streaming) 등의 배포 및 재생 과정에서 동일 코덱의 디코더에 의해 검출된다. 검출된 전염성 워터마크는 검증 및 손상된 워터마크의 재생 과정을 거쳐 콘텐츠 기반 IIIH

에 적합한 형태의 워터마크로 변이된다. 그 후, 디코더는 디코딩된 비디오 프레임에 대해 콘텐츠 기반 강성 워터마킹 알고리즘을 수행하며 돌연변이 워터마크를 재생되는 비디오 프레임에 재은닉 한다. 마지막으로 디코딩 된 비디오 프레임에 대한 편집 및 트랜스코딩이 수행된 후, 이종 코덱으로 재압축 될 때, 해당코덱의 인코더로부터 돌연변이 워터마크는 검출, 검증 및 보정된 후, 감염체 워터마크로서 커널기반 IIIH 기술을 통해 재은닉 된다. 결론적으로 IIIH 시스템에서는 코덱들의 인코딩 및 디코딩 과정에서 워터마크 은닉과 검출이 수행되므로 각 코덱들 고유의 특성에 따라 커널기반 IIIH 기술을 설계하는 것이 중요하다.

3. 제안하는 능동형 워터마킹 기법

2장에서 살펴 본 IIIH 시스템에 대하여 본 논문은, 그림 2의 과정 중 커널기반 IIIH 기법으로부터 시작하여 콘텐츠기반 IIIH 기법으로 이어지는 전염과정에 대해 효과적인 기법을 능동형 비디오 워터마킹 기법으로서 제안한다. 제안 기법에서는 비디오 압축과정에서 병원체 혹은 감염체 워터마크를 가역성을 가진 커널기반 IIIH 기법으로 은닉하여 전송한다. 그 후, 재생을 위해 전송된 비디오 콘텐츠를 디코딩하는 과정에서 검출된 워터마크와 복원된 비디오 콘텐츠를 이용하여 콘텐츠 기반 IIIH를 통해 비디오 재생단계에서 능동적으로 돌연변이 워터마크를 전염시킨다.

그림 2. IIIH 시스템 상에서 각 기술들의 연동에 의한 비디오 콘텐츠의 정보전염

여기서 기존의 워터마킹 기법들[1-5]은 삽입 강도, 삽입 위치를 처음 결정한 후 고정된 값으로 변경이 불가능하지만, 제안 기법에서는 병원체 워터마크 내에 화질제어, 삽입강도 등의 제어코드정보를 함께 은닉함으로써 비디오 디코더에서 워터마크 복호화 및 콘텐츠 재생 단계에서 저작권자나 사용자가 개입되지 않고 능동적으로 콘텐츠 기반 IIIH 기법을 수행하여 변이된 워터마크를 전염시키는 기법으로 트랜스코딩, 재압축 등과 같은 처리에도 워터마크와 화질의 손상 없이 재배포가 가능한 장점이 있다.

비디오 인코더 및 디코더에서 제안하는 능동형 워터마킹 기법이 수행되는 과정을 그림 3에 도식화 하였다. 그림 3에서 나타내었듯이, 비디오 인코더에서는 돌연변이 워터마크 은닉을 위한 제어코드가 포함된 감염체 워터마크를 가역 워터마킹에 기반한 커널 기반 IIIH 기법으로 은닉하여 전송한다. 그 후, 디코더에서는 수신된 비디오의 디코딩 과정에서 은닉된 정보를 검출하고 원본 비디오를 복원한 다음, 복원된 비디오와 검출된 정보로부터 변형된 돌연변이 워터마크와 제어정보를 추출하여 기존의 콘텐츠 기반의 워터마킹 알고리즘[5]을 이용해 능동적으로 비디오 재생단계에서 정보를 전염시킨다. 여기서 병원체 또는 감염체 워터마크 삽입 위치를 결정하기 위한 동일

한 의사 키(pseudo key)가 동일한 코텍의 인코더와 디코더에 각각 주어진다. 이 때 중요한 것은, 제안하는 능동형 비디오 워터마킹 기법의 일부로서 새로운 가역성을 가진 커널 기반 IIIH 알고리즘을 적용하여 비디오 인코딩 단계에서 압축에 의한 워터마크 손상이나 워터마크에 의한 화질 열화를 최소화 한다는 것이다. 또한 제안 기법에서 적용한 커널 기반 IIIH 알고리즘은 비디오 콘텐츠 내용에서 중요하다고 간주되는 부분이나, 하이라이트 장면(highlight scene)에 대해 의도적으로 워터마크 삽입강도를 조절하여 능동적으로 비디오 콘텐츠의 화질을 열화 시키거나 개선시킬 수 있는 장점을 가진다. 아울러 일반적으로 모든 비디오 콘텐츠가 상업적 가치가 뛰어나거나 저작권 보호를 필요로 하는 것은 아니기 때문에, 이 기법을 이용함으로써 화질이 열화 시키거나 저해상도의 콘텐츠로 변환하여 상업적 가치가 없는 비디오 서비스를 가능하게 한다.

가역성을 가진 커널 기반 IIIH 알고리즘에서 워터마크는 그림 4와 같이 매 프레임마다 DCT, 양자화 및 지그재그 스캔(zig-zag scan) 과정을 거친 후, 각각의 MB(macro block)에 각 한 비트 씩 은닉된다. 이것은 각 코텍의 특성에 따라 다른 크기의 변환 블록, 혹은 다른 주파수 커널을 사용하기 때문에 움직임추

그림 3. IIIH 시스템 상에서 각 기술들의 연동에 의한 비디오 콘텐츠의 정보전염

그림 4. 능동형 비디오 워터마킹을 위한 인코더 측 커널 기반 IIIH 모듈

정 및 보상(motion estimation/ compensation, ME/MC)의 기준이 되는 MB 단위를 사용함으로써 서로 다른 코덱들 간에 제안 알고리즘을 적용하는 데 있어 호환성을 유지할 수 있게 한다. 또한, 가역 워터마킹 기법은 은닉하고자 하는 워터마크 외에 워터마크 검출 시 원래의 콘텐츠를 복원하기 위한 부가정보(side information)를 생성하여 저장하여야 한다. 그러나 비디오 콘텐츠의 특성 상 매 프레임마다 워터마크가 은닉됨에 따라 그에 따른 부가 정보 역시 크기가 커지기 때문에 제안 기법에서는 각 MB에서 생성된 부가정보를 다음 순서의 MB에 워터마크 비트와 함께 은닉하는 방법을 사용한다. 앞서 언급한 IIIH 시스템에서 능동형 워터마킹을 수행하기 위한 과정을 3.1절과 3.2절을 통해 설명한다. 그 중 비디오 인코더에서의 커널기반 IIIH 알고리즘 수행 과정을 그림 4 및 그림 5에 자세히 나타내었다. 제안한 능동형 워터마킹 기법은 전염성 정보 감염의 매개체로써 사용되므로, 기존의 가역 워터마킹 알고리즘들[5-10]과는 달리 워터마크 이외에 정보 전염을 위한 제어신호 역시 함께 은닉된다. 전염의 매개체로써 은닉되는 돌연변이 정보는 압축된 DCT 계수에 은닉되므로, 비디오 콘텐츠의 디코딩과정을 거치지 않는 동안 안전하게 보호되며, 디코딩과 동시에 전염되므로, 워터마크에 대한 공격에 강인한 특성을 갖는다. 또한 제안 기법에서는 기존 가역 워터마킹 기법에서 워터마크 검출 시 콘텐츠 복원과정에서 사용되는 부가정보를 워터마크 정보와 함께 이용하여, 비상업적 목적으로 사용될 수 있는 콘텐츠의 화질 제어 기능으로써 사용되어질 수 있도록 새로운 알고리즘으로 설계하였다.

그림 5에서 나타내었듯이, 능동형 워터마킹 기법을 위해 제안한 가역성을 가진 커널기반 IIIH는 비디

오 내의 인트라(intra) 프레임과 인터(inter)프레임에 대해 각기 다른 삽입강도 $\alpha_{r, Intra}$, 및 $\alpha_{r, Inter}$,를 사용하며, 워터마크 정보 역시 프레임의 종류에 따라 달라진다. 이렇게 함으로써, 커널/콘텐츠 기반 IIIH 기법들에서 GOP 단위로 능동적으로 삽입강도 및 화질 열화 정도를 조절할 수 있다. 또한 α_C 는 콘텐츠 기반 IIIH에서 돌연변이가 워터마크 은닉을 위한 삽입강도로써 사용되는 정보를 포함한다. 감염체 워터마크 W_p 는 이진 비트열로 구성되며, 비디오 유통과정 혹은 정보 전염과정에서의 유출을 막기 위해 저작권 정보 M 과 사용자 개인 키 K_I 로서 식 (1)과 같이 암호화 되며,

$$W_p = C(M, K_I) \quad (1)$$

식 (1)의 $C(\cdot)$ 은 개인키 K_I 로서 암호화를 수행하는 암호화기 함수로써 XOR, AES, DES, ARIA 등의 알고리즘으로 사용될 수 있다.

3.1 능동형 워터마킹을 위한 커널기반 IIIH 기법

제안한 능동형 워터마킹에서 커널기반 IIIH의 워터마크 은닉은 원본 콘텐츠가 복원 가능한 가역 워터마킹 방식으로 설계되기 때문에 워터마크 정보 외에도 콘텐츠 복원을 위한 부가정보도 필요하다. 비디오 콘텐츠의 경우, 워터마크를 은닉할 때 마다 생성되는 부가정보를 저장하거나 워터마크 검출기로 전달하는 것이 용량성 문제에 영향을 미칠 수 있다. 제안 기법은 워터마크 검출 시 원본을 필요로 하지 않는 블라인드 워터마킹을 만족하고, 부가정보로 인한 용량성을 줄이기 위해, 하나의 MB 내 임의 계수에 1비트의 워터마크를 은닉하며, 이 때 발생한 1비트의 부가정보 s 를 다음 MB에 워터마크와 함께 은닉하는

그림 5. 능동형 비디오 워터마킹 기법에서 커널기반 IIIH 수행 과정

방법을 사용한다. 이 방법을 사용하면 워터마크가 은닉되는 마지막 MB는 원본으로 복원이 불가능하지만, 전체 비디오의 크기에 비해 무시될 수 있다.

인트라/인터 프레임에 대한 워터마크 은닉은 우선 식 (2)와 같이 B 개의 휘도 DCT 블록으로 이루어진 j 번째 MB에 대해서 워터마크가 은닉될 DCT 계수 $c_{t,j}$ 을 선택함으로써 이루어진다.

$$\begin{aligned} c_{t,j} &= c_{b_p, z_j}, \quad b_j = k_p^s(j), \\ z_j &= \begin{cases} \text{First nonZero Order} | z_j > (l - \alpha_r), \\ \text{if } k_p^s(j, 0) = 1 \\ \text{Last nonZero Order}, \\ \text{if } k_p^s(j, 0) = 0 \end{cases} \end{aligned} \quad (2)$$

여기서, b_j 는 MB내에서 워터마크가 은닉되는 DCT 블록을 지시하며, z_j 는 DC계수를 제외한 DCT블록의 지그재그 스캔 순서를 의미한다. 또한 l 은 각 코덱이 가지고 있는 주파수변환 계수블록의 길이를 의미한다. 이 때, 워터마크 삽입기와 검출기에 주어진 의사 키 k_p^s 에 대한 씨앗(seed) 정보인 s 을 이용하여 k_p^s 로부터 최종적으로 은닉되는 DCT 계수 $c_{t,j}$ 를 선택할 수 있다. 여기서, 인트라 프레임의 경우 그 자체의 값으로 워터마크를 검출해야 하므로 $s=0$ 으로 고정된다. 또한 α_r 을 이용하여 워터마크의 삽입강도를 조절할 수 있는데, 이는 워터마크 검출기를 통과하지 않은 콘텐츠에 대해 화질 열화의 세기를 결정함으로써, 비상업적 목적으로 사용되는 콘텐츠의 화질을 결정할 때 용이하게 사용될 수 있다. α_r 은 프레임 종류

$$\begin{aligned} c_{\epsilon,j} &= c_{b_{j+1}, z_{j+1}}, \quad b_{j+1} = \text{inv}(k_p^s(j+1)), \\ z_j &= \begin{cases} \text{First nonZero Order} | z_j > (l - \alpha_r), \\ \text{if } k_p^s(j+1, 1) = 1 \\ \text{Last nonZero Order}, \\ \text{if } k_p^s(j+1, 1) = 0 \end{cases} \end{aligned} \quad (3)$$

에 따라 $\alpha_{r, Intra}$ 와 $\alpha_{r, Inter}$ 로 구분된다. 또한, 부가정보 ϵ_j 를 $j+1$ 번째 MB에 은닉하기 위한 DCT 계수 $c_{\epsilon,j}$ 역시 식 (2)로부터 변형하여 식 (3)으로 정의하였다

이 때, 중요한 것은 워터마크와 부가정보가 같은 블록 내 같은 계수위치에 삽입되는 것을 방지하기 위해 식(3)에서는 k_p^s 의 역수를 취함으로써 같은 블록 내에 삽입되는 것을 방지한다. 식 (2)와 식 (3)으로부터 선택된 계수들에 대해 워터마크와 부가정보를 은닉하게 되며, 우선 프레임 종류에 따라 은닉되는 워터마크 비트열 $W = \{w_0, w_1, w_2, \dots, w_j\}$ 을 식 (4)와 같이 결정한다.

$$W = \begin{cases} \text{MUX}(W_p, s, \alpha_c, \alpha_{r, Inter}), & \text{if } I\text{-Frame} \\ \text{repeat}(W_p), & \text{otherwise} \end{cases} \quad (4)$$

식 (2), (3) 및 (4)에 의해 최종 결정된 워터마크 부가정보와 그에 따른 삽입계수들을 이용하여 가역 워터마킹을 수행하는 과정을 식 (5)에 나타내었다.

$$\hat{c}_{t,j} = \begin{cases} \text{abs}(c_{t,j}), & \text{if } w_j = 1 \\ -\text{abs}(c_{t,j}), & \text{otherwise} \end{cases} \quad (5)$$

식 (5)에서와 같이 워터마크는 해당 MB로부터 선택된 계수값 $c_{t,j}$ 의 부호를 변경시킴으로써 은닉된다. 이 때, 워터마크가 은닉된 계수 $\hat{c}_{t,j}$ 에 의해 콘텐츠 복원 정보 ϵ_j 는 식 (6)으로써 생성된다.

$$\epsilon_j = \begin{cases} 1, & \text{if } c_{t,j} \neq \hat{c}_{t,j} \\ 0, & \text{if } c_{t,j} = \hat{c}_{t,j} \end{cases} \quad (6)$$

이 때, 워터마크가 은닉됨에 따라 부가정보 ϵ_j 이 무한히 생성되는 것을 방지하기 위해, 식 (7)과 같이 이전 MB에서 생성된 ϵ_{j-1} 과의 XOR 연산을 통해 한 비트를 생성한 후 부가정보를 위한 계수 $c_{\epsilon,j}$ 에 삽입하도록 설계한다.

$$\overline{c_{\epsilon,j}} = \begin{cases} |c_{\epsilon,j}|, & \text{if } \epsilon_j \otimes \epsilon_{j-1} = 1, \quad j > 0 \\ -|c_{\epsilon,j}|, & \text{otherwise} \end{cases} \quad (7)$$

만약 $j=0$ 일 때, $\overline{c_{\epsilon,0}}$ 는 오직 ϵ_0 에 의해 결정되어진다. 워터마크와 부가정보가 은닉되는 과정을 그림 6으로서 간단히 도식화하였다.

3.2 전염성 정보온닉을 위한 커널기반 워터마크 검출 및 재은닉 기법

앞서 설명한 방법으로 워터마크가 은닉된 비디오 압축 스트림은 그림 3과 같이 전송된 후 디코더로부터 워터마크 키 k_p^s 를 이용하여 워터마크와 부가정보가 검출된다, 그 후 부가정보로부터 비디오 콘텐츠를 워터마크가 은닉되기 전으로 복원한 후 최종적으로 I 프레임에 은닉된 정보들을 이용하여 능동형 워터마킹을 수행한다. 그 일련의 과정을 그림 7에 도식화하였다.

이 때, 워터마크 검출 및 비디오 복원을 위해 다음 MB를 참조해야 하므로, 비디오 디코딩 시 1 MB만큼의 지연이 발생하며, 워터마크 검출 및 복원과정은 앞서 언급한 워터마크 은닉과정의 역과정으로 이루어진다.

그림 6. 제안된 커널기반 IHH에서 워터마크와 부가정보의 은닉 위치와 순서

그림 7. 능동형 워터마킹을 위한 디코더 단에서의 워터마크 처리과정

어진다. 그림 7로서, 제안한 가역 워터마킹의 역 과정을 통해 복원된 비디오 프레임과 능동형 워터마킹을 위한 W_p 및 α_C 를 추출한다. 추출된 W_p 는 콘텐츠 기반 IHH 기법에 사용되는 형식의 돌연변이 W_M 으로 변이되고, α_C 는 W_M 을 은닉하기 위한 삽입강도로서 사용된다. 이렇게 함으로서 워터마크로 인한 화질열화를 최소화 할 수 있으며, 압축에 의한 워터마크 손실역시 최소화 할 수 있다. 최종적으로 비디오콘텐츠가 유통된 후에도 미리 설정한 삽입강도 및 콘텐츠 내용에 따라 콘텐츠 사용자 측에서 능동적으로 은닉될 수 있으며. 이후에 발생하는 다른 코덱에 의한 콘텐츠의 변질에도 능동적으로 대처할 수 있게 한다.

제안 알고리즘의 시뮬레이션을 위해 콘텐츠 기반 IHH 알고리즘으로서 [5]의 방법을 적용하였다. 이 기법은 이중 멀티미디어 서비스 상에서 비디오 콘텐츠의 저작권 보호를 제공하기 위해, MPEG-4 SVC 및 멀티미디어 트랜스코딩에 강인한 블라인드 비디오 워터마킹 기법으로서 제안되었다. W_M 은 [5]의 방법을 통해 콘텐츠에 은닉되며, 이로써, 디코딩된 비디오 콘텐츠는 불법적인 트랜스코딩에 대해 강인성을

가질 수 있다.

3. 실험 결과

제안한 능동형 워터마킹 기법의 성능 평가를 위해 그림 8과 같이 CIF@30fps 해상도를 갖는 Mobile, Foreman, Crew 비디오 영상에 대해 실험을 수행하였으며, 제안 기법의 커널기반 IHH를 적용하기 위해 MPEG-2 Part2의 비디오 코딩 방식을 사용하였다. 실험에 사용된 파라미터로써 워터마크 W_p 로는 암호화된 256길이를 갖는 비트열을 사용하였고, 인트라 프레임의 삽입강도 $\alpha_{r, Intra} = 56$ 로 설정하였다. 인터 프레임에 대한 삽입강도 $\alpha_{r, Inter}$ 에 대해서는 GOP 단위로 변경이 가능하지만, 제안한 기법의 비교를 위해 동일한 프레임에 각각 $\alpha_{r, Inter} = 60$ 및 $\alpha_{r, Inter} = 52$ 로 설정하여 가역워터마킹 복호화 과정을 거치지 않은 콘텐츠에 대해 그 결과를 나타내었다. 또한 k_p^s 로서 의사난수 생성을 통해 생성된 2^{16} 길이를 갖는 비트열을 MPEG2 인코더 및 디코더에 각각 저장하였다. 인트라 프레임의 씨앗정보 s 는 16bit를 갖도록 하였다.

그림 8. 실험에 사용된 CIF@30fps 해상도의 비디오 콘텐츠, (a) Mobile, (b) Foreman 및 (c) Crew

각 비디오 콘텐츠에 대해 커널기반 IIIH를 수행하고, 각각의 복호화 결과를 그림 9와 그림 10 및 그림 11에 나타내었다. 그림 9, 그림 10 및 그림 11에서 보듯이 커널기반 IIIH 복호화 후의 비디오 콘텐츠가 워터마킹 과정 없이 압축되어 디코딩 된 비디오 콘텐츠와 동일함을 확인할 수 있다. 아래 표 1은 그림 8의 실험 비디오들에 대해 300 프레임에 대한 커널기반 IIIH 복호화 후에 검출된 워터마크 W_p 와 콘텐츠 복원을 위한 부가정보 ϵ_j 에 대해서 오류 비트 수를 나타낸 것이다.

표 1로써 알 수 있듯이, 제안한 기법으로 은닉한 워터마크가 완벽히 검출됨을 확인하였다. 한편, 부가정보 ϵ_j 에 대해 각 비디오에서 1 bit씩의 오류가 발생했는데, 이는 제안 기법이 MB 당 은닉되는 워터마크로부터 생성되는 복원용 부가정보 ϵ_j 가 다음 순서의 MB에 은닉됨에 기인한다. 따라서 최종적으로 워터마크가 은닉되고 압축되는 MB에 대해서 ϵ_j 를 저장할 공간이 없으므로 여기서 1비트 오류가 발생하는 것이다. 하지만, 이는 전체 비디오 콘텐츠에서 극히 작은 부분이므로 무시될 수 있는 수치이다.

그림 9. Mobile에 대한 실험 결과, (a) 워터마킹 없이 디코딩된 영상, (b) 커널기반 IIIH 후 복호화하지 않고 디코딩한 영상, (c) 커널기반 IIIH 후 복호화 한 영상

그림 10. Foreman에 대한 실험 결과, (a) 워터마킹 없이 디코딩된 영상, (b) 커널기반 IIIH 후 복호화하지 않고 디코딩한 영상, (c) 커널기반 IIIH 후 복호화 한 영상

표 1. 각 실험비디오에 대해 검출된 워터마크 및 부가정보에 대한 오류 비트 수

구 분	Mobile	Foreman	Crew
워터마크	0	0	0
부가정보	1	1	1

반면, 커널기반 IHH 후 복호화 되지 않은 영상은 그림 9, 10 및 11의 각 (b) 그림과 같이 심한 블로킹 현상이 발생함을 확인하였다. 제안 기법에서는 인증된 전염성 정보 검출알고리즘이 적용되지 않은 디코더에서 디코딩거나, 워터마크 손상으로 인한 오류비트가 발생한 경우의 콘텐츠에 대해 $\alpha_{r, Intra}$ 및 $\alpha_{r, Inter}$ 를 조절함으로써 저화질의 콘텐츠를 서비스 할 수 있게 하였다. 그림 9, 10 및 11의 각 (b) 그림에서 블로킹 현상을 없애는 것은 비디오 디코딩 시 워터마크가 은닉되었을 것으로 간주되는 계수 영역들을 제거함으로써 가능하다. 이렇게 함으로써 워터마크가 제거된 상업적 가치를 결정하기 힘든 저화질의 비디오 콘텐츠를 제공할 수 있다. 앞서 설정한 삽입강도에

대해 64개의 계수 길이를 갖는 DCT 블록에서 15번째 이후의 블록들을 제거하여 얻은 결과를 그림 12, 13 및 14에 나타내었다.

그림 12, 13 및 14로부터 정량적 화질 열화 측정을 위해 전체 프레임이 갖는 평균 PSNR(peak signal to noise ratio)를 표 2에 나타내었다. 그림 12, 13 및 14와 표 2로부터 몇몇 제거되지 않은 워터마크 혹은 부가정보들로 인해 여전히 블로킹 현상 어느 정도 존재하지만, 콘텐츠의 내용을 알 수 있을 정도의 결과를 얻을 수 있음을 확인하였다. 하나의 콘텐츠 내에서도 삽입강도를 가변함으로써 인가되지 않은 디코더로 비디오를 재생할 경우, 중요 내용을 가리는

표 2. 커널기반 IHH 디코딩 시 워터마크 제거 후 열화된 비디오 콘텐츠의 PSNR 비교[dB]

구 분	Mobile	Foreman	Crew
워터마크 미은닉 비디오	33.09	34.45	36.95
$\alpha_{r, Inter} = 52$	18.28	23.21	30.17
$\alpha_{r, Inter} = 60$	16.64	22.55	28.98

그림 11. Crew에 대한 실험 결과, (a) 워터마킹 없이 디코딩된 영상, (b) 커널기반 IHH 후 복호화하지 않고 디코딩한 영상, (c) 커널기반 IHH 후 복호화 한 영상

그림 12. 커널기반 IHH 복호화를 거치지 않은 비디오 콘텐츠 서비스 예, (a) 디코딩된 Mobile 비디오, (b) $\alpha_{r, Inter} = 52$ 일 때의 결과, (c) $\alpha_{r, Inter} = 60$ 일 때의 결과

그림 13. 커널기반 IIIH 복호화를 거치지 않은 비디오 콘텐츠 서비스 예, (a) 디코딩된 Foreman 비디오, (b) $\alpha_{r,Inter} = 52$ 일 때의 결과, (c) $\alpha_{r,Inter} = 60$ 일 때의 결과

그림 14. 커널기반 IIIH 복호화를 거치지 않은 비디오 콘텐츠 서비스 예, (a) 디코딩된 Crew 비디오, (b) $\alpha_{r,Inter} = 52$ 일 때의 결과, (c) $\alpha_{r,Inter} = 60$ 일 때의 결과

스크램블(scramble) 기능을 수행할 수 있음을 확인하였다.

앞선 실험 결과로부터, 검출된 워터마크 W_p 와 α_C 를 이용하여 콘텐츠 재생 직전의 콘텐츠에 디코더 스스로 워터마크를 은닉하게 함으로서 능동형 비디오 워터마킹 기법은 완성된다. 본 논문에서는 능동형 비디오 워터마킹 시뮬레이션을 위해 [5]의 알고리즘을 콘텐츠반 IIIH로써 사용하였다. 이 알고리즘은 워

터마크 삽입 시 이진 비트열을 사용하기 때문에 $W_M = W_p$ 로써 은닉하였다. 그림 15에 [5]의 알고리즘에 의해 능동적으로 워터마크가 은닉된 결과 영상과 각각의 PSNR을 나타내었다. 여기서는 커널기반 IIIH 복호화된 비디오를 원본으로 하여 PSNR을 계산하였다. 또한, 콘텐츠기반 IIIH를 통해 은닉된 워터마크의 압축률 및 다양한 시공간 변환에 대한 워터마크 강인성은 [5]의 실험결과로부터 증명되었으며, 특히

그림 15. 능동형 비디오 워터마킹 결과 영상, (a) Mobile, PSNR=34.62, (b) Foreman, PSNR=33.75, (c) Crew, PSNR=35.27

본 논문에서는 전염성 정보은닉을 위해 재압축 시 사용되는 코덱의 인코더에서 검출되어 감염체로 다시 은닉되기 때문에 압축율에 따른 워터마크 손상이 발생하지 않음을 실험을 통해 표 3으로부터 확인하였다. 표 3은 그림 2로부터 MPEG-2 코덱에 제안한 능동형 비디오 워터마킹을 탑재한 IIIH 시스템을 적용하여 콘텐츠 재배포 시 압축율을 5Mbps, 1Mbps 및 500kbps로 점진적으로 높였을 때를 시뮬레이션하여 각 재배포 단계에서의 전염성 정보 손상율을 나타낸 것이다.

더욱이, 그림 2의 재배포 과정이 반복되면서 돌연변이 및 감염체에 의한 반복적인 워터마크 은닉에도 최초 은닉된 돌연변이 워터마크에 대한 결과로부터 더 이상의 심각한 화질열화는 발생하지 않는 장점이 있음을 표 4를 통해 확인하였다. 표 4는 워터마크 재은닉으로 인한 화질 열화정도를 측정하기 위해 동일한 압축율로 그림 2의 재배포 과정을 반복했을 때 화질 측정 결과를 PSNR로 나타낸 것이다. 화질 측정은 각 단계의 돌연변이 워터마크 은닉 직후에 수행하였다. 그림 2로부터 제안된 IIIH 시스템이 재배포 횟수에 따라 워터마크 역시 반복적으로 삽입되는 것처럼 보인다. 하지만, 실제 커널기반 IIIH에서는 가역워터마킹이 수행되어 워터마크 검출 시 원 비디오 콘텐츠 역시 복원되므로 워터마크로 인한 화질의 열화는 발생하지 않았다. 또한, 콘텐츠 기반 IIIH의 경우 역시, 표 4에서와 같이 최초 은닉된 돌연변이 워터마크에 의해 일부 화질의 열화 발생하지만 2차 3차 재은닉 시에는 화질열화는 일어나지 않았다. 이것은 비디

오 콘텐츠 압축과정 중 양자화로 인해 컷오프(cut-off)되는 에너지와 재은닉 되는 워터마크의 상쇄효과로 얻어지는 결과로 분석된다. 따라서 비디오 프레임으로부터 검출된 돌연변이 워터마크는 감염체 워터마크로 변이되어 양자화 이후에 은닉되기 때문에 제안 기법을 적용하여 실제 워터마크 손실과 워터마크 재은닉으로부터 발생하는 더 이상의 화질의 열화를 방지할 수 있었다.

5. 결 론

본 논문은 비디오 콘텐츠 보호를 위한 전염성 정보은닉 시스템의 일부로서, 병원체 워터마크 내에 화질제어, 삽입강도 등의 정보를 함께 은닉함으로써 비디오 디코딩 과정에서 돌연변이 워터마크를 은닉할 때 능동적으로 은닉될 수 있는 능동형 비디오 워터마킹 기법을 제안하였다. 제안 기법은 특히, 원본 비디오를 복원할 수 있는 비디오 인코딩 상에서의 가역성을 가진 커널기반 IIIH를 제안하였으며, 워터마크는 비디오 인코딩 과정에서 은닉된다. 전송된 비디오 스트림에 대해 디코더에서 가역 워터마킹 복호화를 거쳐 최종 재생 단계에서 능동적으로 워터마크를 전염시키는 기법을 제안하였다.

기존의 가역워터마킹 알고리즘들이 워터마크 검출 시 비디오 콘텐츠와 워터마크가 완전히 분리되는 기법임과는 달리, 본 논문에서 제안한 기법은 전염성 정보 감염의 매개체로써 사용된다. 따라서 비디오 콘텐츠의 디코딩 과정을 거치지 않는 이상, 워터마크와 전염을 위한 제어 정보는 안전하게 보호되며 또한 디코딩과 동시에 전염되므로 워터마크에 주파수 및 공간영역 변환 과정 중 워터마크 손실이 발생하지 않는 장점이 있었다. 또한 감염체 워터마크를 위한 콘텐츠기반 IIIH에서는, 일반적인 비디오 신호처리에 강인한 알고리즘을 적용함으로써, 화질열화, 트랜스 코딩 및 스케일러빌리티 등에 강인하게 설계할 수 있는 장점이 있었다. 실험결과 반복적으로 재은닉 되는 워터마크로 인해 최초 재은닉 시에만 1dB 미만의 한 화질 저하가 나타남을 확인하였으며, 이에 따라 워터마크 재은닉 횟수에 따른 화질 열화는 발생하지 않음을 알 수 있었다. 또한 워터마크로 인한 압축 효율 역시 증가하지 않으며, 재은닉 과정에서 워터마크 오류율 역시 0%로 비디오 콘텐츠와 코덱에 의해 완

표 3. MPEG-2 압축율에 따른 전염성 정보 손상율(BER, bit error rate)

구 분	5Mbps	1Mbps	500kbps
Mobile	0%	0%	0%
Foreman	0%	0%	0%
Crew	0%	0%	0%

표 4. MPEG-2 압축율 5Mbps로 고정하였을 때 워터마크 재은닉 횟수에 따른 PSNR 비교[dB]

구 분	1차 배포	2차 배포	3차배포
Mobile	34.62	34.51	34.51
Foreman	33.75	33.70	33.70
Crew	35.27	35.19	35.19

전하게 정보가 전염됨을 확인하였다. 또한 인가되지 않은 디코더를 사용하였을 때 20dB 전후의 급격한 화질 열화를 줌으로써 비디오 콘텐츠를 자체 보호할 수 있음을 확인하였다. 향후, 제안 알고리즘을 개선하고, 전염성 정보은닉 시스템을 완성함으로써 급격히 발전하고 있는 고화질, 고차원 비디오 콘텐츠에 대한 건전한 유통에 이바지 할 수 있을 것으로 기대한다.

참 고 문 헌

- [1] M.D. Swanson, B. Zhu, and A.H. Tewfik, "Multiresolution Scene-Based Video Watermarking using Perceptual Models," *IEEE Journal on Selected Areas in Communications*, Vol. 16, Issue 4, pp. 540-550, 1998.
- [2] C.V. Serdean, M.A. Ambroze, M. Tomlinson, and J.G. Wade, "DWT-based High-capacity Blind Video Watermarking, Invariant to Geometrical Attacks," *IEEE Proc. Vision, Image and Signal Processing*, Vol. 150, Issue 1, pp. 51-58, 2003.
- [3] Y. Wang and A.I. Pearmain, "Blind MPEG-2 Video Watermarking Robust Against Geometric Attacks: A Set of Approaches in DCT Domain," *IEEE Trans. on Image Processing*, Vol. 15, No. 6, pp. 1536-1543, 2006.
- [4] 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.
- [5] 윤지선, 이석환, 송윤철, 장봉주, 권기룡, 김민환, "MPEG-4 스케일러블 비디오 코딩 및 멀티미디어 트랜스코딩에 강인한 블라인드 비디오 워터마킹," 멀티미디어학회논문지, 제11권, 10호, pp. 1347-1358, 2008.
- [6] 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.
- [7] B. Yang, M. Schmucker, C. Busch, X. Niu, and S. Sun, "Approaching Optimal Value Expansion for Reversible Watermarking," *Proc. of the 7-th Workshops on Multi-media and Security*, pp. 95-102, 2004.
- [8] B. Yang, M. Schmucker, X. Niu, C. Busch, and S. Sun, "Reversible Image Watermarking by Histogram Modification for Integer DCT Coefficients," *Proc. of the IEEE 6th Workshop on Multimedia Signal Processing*, pp. 143-146, 2004.
- [9] J.M. Zain, L.P. Baldwin, and M. Clarke, "Reversible Watermarking for Authentication of Dicom Images," *Proc. of the 26th Annual International Conference of the Engineering in Medicine and Biology Society*, pp. 3237-3240, 2004.
- [10] Xiao Zeng, Zhen-Yong Chen, Ming Chen, and Zhang Xiong, "Reversible Video Watermarking using Motion Estimation and Prediction error expansion," *Journal of Information Science and Engineering*, Vol. 27, pp. 465-479, 2011.
- [11] Zhenyong Chen, Zhang Xiong, and Long Tang, "A Novel Scrambling Scheme for Digital Video Encryption," *Proc. of Pacific-Rim Symposium on Image and Video Technology (PSIVT)*, pp. 997-1006, 2006.
- [12] Zheng Liu and Xue Li, "Motion Vector Encryption in Multimedia Streaming," *Proc. of 10Th international Conference of Multimedia Modelling Conference*, pp. 64-71, 2004.
- [13] B. Furht and D. Kirovski, *Multimedia Security Handbook*, CRC Press LLC, 2004.
- [14] C. Shi and Bharat Bhargava, "A Fast MPEG Video Encryption Algorithm," *Proc. of ACM Multimedia*, pp. 81-88, 1998.
- [15] A. Shamir, "How to share a secret," *Proc. of Communications of the ACM*, Vol. 2, pp. 612-613, 1979.
- [16] *Coding of audio-visual objects-Part 2: Visual, ISO/IEC 14492-2 (MPEG-4 Visual)*, ISO/IEC JTC 1, Version 1: 1999, Version 2: 2000, Version 3: 2004.
- [17] *Advanced Video Coding for Generic Audiovi-*

sual Services, ITU-T Rec. H.264 and ISO/IEC 14496-10 (MPEG-4 AVC), ITU-T and ISO/IEC JTC-1, Version 1: 2003, Version 2: 2004, Version 3: 2005, Version 4: 2005, Version 5 and Version 6: 2006, Version 7: 2007.

- [18] Jan Bormans and Keith Hill, *MPEG-21 Overview v.5*, ISO/IEC JTC1/SC29/WG11 /N5231, 2002,
- [19] H. Schwarz, D. Marpe, and T Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," *IEEE Trns. on Circuits and Systems for Video Technology*, Vol. 17, pp. 1103-1120, 2007.
- [20] <http://www.bbc.co.uk/opensource/projects/dirac/>, 2011.
- [21] <http://www.xvid.org/>, 2011.
- [22] Anthony Vetro, "Transcoding Scalable Coding and Standardized Metadata," *8th International Workshop of Visual Content Processing and Representation*, Vol. 2849, pp. 15-16, 2003.
- [23] 장봉주, 이석환, 권기룡, "생물학적 바이러스를 이용한 비디오 콘텐츠의 전염성 정보은닉 시스템 모델링," *전자공학회논문지*, 제49권 CI 3호, pp. 34-45, 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 전자공학과 박사

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~2005년 부산외국어대학교 디지털정보공학부 부교수

2011년~2012년 Colorado State Univ., Visiting Scholar

2006년~현재 부경대학교 IT융합응용공학과 교수

2012년~현재 한국멀티미디어학회 총무및조직담당부회장

관심분야: 멀티미디어정보보호, 디지털영상처리, 멀티미디어통신신호처리