논문 2012-49CI-3-5

생물학적 바이러스를 이용한 비디오 콘텐츠의 전염성 정보은닉 시스템 모델링

(Modeling of Infectious Information Hiding System for Video Contents using the Biological Virus)

장 봉 주*, 이 석 환**, 권 기 룡***

(Bong-Joo Jang, Suk-Hwan Lee, and Ki-Ryong Kwon)

요 약

본 논문은 생물학적 바이러스의 특성과 감염 경로 및 감염 절차를 이용한 전염성 정보은닉(infectious information hiding, IIH) 기술 기반의 비디오 콘텐츠 보호 시스템을 제안한다. 제안한 IIH 시스템에서는 비디오 콘텐츠 보호에 필요한 중요 정보들을 전염성 바이러스로 간주하며, 콘텐츠 및 코덱을 숙주 및 감염 매개체로 하는 새로운 패러다임의 비디오 콘텐츠 보호 기술을 제시하였다. 전염성 정보로써 병원체, 돌연변이 및 감염체 바이러스를 모델링 하였으며, 주요 기술도구로써 전염성 정보 인증, 커널 기반 IIH, 콘텐츠 기반 IIH 및 전염성 정보 생성 기술도구들을 정의하였다. 마지막으로 기존의 간단한 정보은닉 알고리즘들을 각각 커널기반 IIH 및 콘텐츠 기반 IIH로 간주하여 시뮬레이션 함으로써 제안한 IIH 시스템의 가능성을 검증하였다.

Abstract

In this paper, we proposed and modeled a video contents protection system based on the infectious information hiding(IIH) technique as using characteristics of biological viruses. Our proposed IIH System considered the requisite important information for video contents protection as the infectious virus, and suggested a new paradigm about video contents protection that transmitted infectious information from contents(host) or video CODECs(viral vector). Also, we modeled the Pathogen, Mutant and Contagion virus as the infectious information and defined technical tools about verification of infectious information, kernel based IIH, contents based IIH and creation/regeneration of infectious information as main techniques for our IIH system. Finally, through simulations that carried the infectious information by using conventional information hiding algorithms as kernel based and contents based IIH techniques, we verified possibilities of our proposed IIH system.

Keywords : 전염성 정보은닉(infectious information hiding, IIH), 저작권 보호(copyright protection), 비디오 워터마킹(video watermarking), 바이러스 모델링(virus modeling)

* 학생회원, *** 정회원-교신저자, 부경대학교 정보보호협동과정
(Interdisciplinary Program of Information Security. Pukyong National University)
** 정회원, 동명대학교 정보보호학과
(Department of Information Security, Tongmyong University)
※ 이 논문은 2011년도 교육과학기술부의 재원으로 한국연구재단의 일반연구자지원사업의 지원을 받아 수행된 것임 (KRF-2011-0010902).
접수일자: 2011년12월26일, 수정완료일: 2012년5월8일

Ⅰ. 서 론

최근 HD급의 공중파 방송, 디지털 극장과 TV 및 블루레이 홈시어터 등의 초고화질 영상 비스가 보편화됨에 따라, 이를 효과적으로 압축, 전송 및 저장하기 위해 많은 기존 비디오 코덱들의 성능 개선을 위한 연구와 기존 압축 기술을 압도할 수 있는 성능의 차세대 영상 압축 표준으로서 HEVC(high efficiency video coding) 기술에 대한 연구가 활발히 진행 중이다. 아울러 하나의 압축된 비디오 스트림으로부터 능동적으로 디스플레이 플랫폼과 전송환경을 고려하여 적합한 해상도와 화질, 프레임율 등을 찾아 부분 디코딩을 가능하게 하는 스케일러블 비디오 코딩 기술 역시 MPEG2 및 MPEG4-SVC(scalable video coding) 등에서 압축 기술 표준으로 확정되었다. 이것은 다양한 멀티미디어 기기 및 네트워크 시스템에서 디지털미디어로서 비디오 영상 콘텐츠가 자유롭게 상호 교환되어야 할 필요성이 있다는 것에서 그 의미가 크다. 또한 영상 화질의 수준을 뛰어넘는 사실감에 대한 요구와 입체감 있는 영상을 즐기기 위한 고화질 3D 영상압축 기술에 대한 연구 역시 이미 큰 발전을 이루면서 상용화되어 서비스되고 있을 만큼 비디오 영상 압축 기술은 새로운 패러다임의 전환점을 맞이하고 있다. 이처럼 다양한 목적과 성능을 가진 코덱들의 경이적인 발전은 현 시대에서 비디오 콘텐츠의 엄청난 사업적 가치와 시장 규모를 직접적으로 나타내는 것이며, 그로 인해 방송 영화 산업 뿐만 아니라 온/오프라인을 비롯한 UCC(user created contents), 개인 방송 및 각종 홍보영상 등에 해당하는 높은 수준의 비디오 영상 콘텐츠의 다양성을 가져왔다.

반면 이와 같은 많은 장점에도 불구하고, 시장성과 상업적 가치를 가진 비디오 콘텐츠에 대한 불법복제, 무단배포 및 허가되지 않은 편집과 발췌 등으로 인해 소유권 및 저작권에 관한 문제가 불거지게 된 것이 비디오 압축 기술의 범용화에 의한 문제점들로서 꾸준히 제기되어 왔다. 이를 해소하기 위해 2002년 이후, CCL(creative commons license)이라는 표준약관 제도를 각 국가별로 법제화하여 도입하였으나, 웹상에서의 저작권 권한 관리만을 허용하며, 음성적으로 유포되거나 복제되는 경우, 혹은 비디오 일부분만 발췌 또는 수정되었을 경우 등의 일반적이고 단순한 지적 재산권 침해에 대해 CCL로써 실질적인 보호는 매우 어려운 실정이다. 또한, 최근 많은 웹하드(webhard) 사이트와 각종 토렌트(torrent) 프로그램들 및 클라우드(cloud) 시스템이 보급되고 확산되면서, 이런 비디오 콘텐츠의 불법적인 배포, 재사용, 수정, 도용 등에 대해 적발하거나 원 저작권자의 권리를 확보하기란 사실상 불가능에 가까운 것으로 여겨지고 있다.

한편 멀티미디어 콘텐츠의 소유권 및 저작권 보호를 위한 기술로서 1990년대 이후부터 워터마킹 및 핑거프린팅과 같은 정보은닉기술이 활발히 진행되어왔으나[1~10], 은닉되는 정보의 용량성, 신뢰성 및 그로 인한 원본 데이터의 손상 등의 한계를 극복하지 못하고 현재는 주목받지 못하는 기술로서 인식되고 있는 실정이다. 그 중 기존에 제안되었던 다양한 주파수 커널 및 비디오코덱 환경 하에서의 대표적인 비디오 기반 정보은닉 기술을 살펴보면, 먼저 Hartung 등[1]은 복호된 비디오 프레임에 공간과 시간으로 이루어진 3차원 신호를 1차원으로 라인 스캔(line scan)하여 얻은 신호에 대역확산 기법을 이용해 워터마크를 삽입하는 방법을 제안하였으며, Swanson 등[2~3]은 비디오 오브젝트 기반의 워터마킹 기법과 비디오의 시간 축에 따라 웨이블릿 변환기법을 적용한 다해상도 비디오 워터마킹 기술을 제안하였다. Serdean 등[4]은 웨이블릿 변환 기반에서 높은 용량성을 갖는 워터마킹 기법으로써 기하학적 공격에 강인한 알고리즘을 설계하였다. 또한, Wang 등[5]은 MPEG2 압축 과정상에서 DCT 변환 기반의 기하학적 공격에 강인한 워터마킹 기법을 제안하였다. 이외에도 다양한 비디오 워터마킹 알고리즘들[6~10]이 현재까지 무수히 제안되어 왔으며, 특히 비디오 콘텐츠의 경우, 대부분의 이런 정보은닉 기술들의 치명적인 약점으로서 미리 은닉한 저작권 정보의 손실이 비디오 압축과정중 양자화 단계에서 발생할 가능성이 높다. 또한, 프레임의 회전, 이동, 절삭 등 일반적인 기하학적 처리 과정에서도 저작권 정보의 강인성을 확보하기란 현실적으로 어려운 부분이므로 이런 정보은닉 기술들의 실질적인 상용화에 큰 어려움이 있다. 이러한 문제점을 보완하기 위해 비디오편집과 양자화에 의한 저작권 정보 손실을 최소화하기 위해 비디오 전송 및 저장을 위한 최종 과정인 압축과정 내에서 여러 압축 파라미터들을 이용한 정보은닉기법들이 연구되었다. 하지만, 디코딩된 비디오 콘텐츠, 혹은 다른 종류의 코덱에 의해 트랜스코딩[11]된 비디오 콘텐츠 내에서의 저작권 정보의 강인성은 매우 취약하다는 단점이 있다. 또한 국제 표준으로 제정된 코덱들[12~17] 외에도 독자적인 압축 기법들을 가진 비디오

코덱[18~19]의 다양성으로 인해 특정 코덱만을 고려한 저작권 보호 기술 역시 그 한계를 드러낸다. 멀티미디어 활용 기술이 증가됨에 따라, SVC 또는 MVC (multiview video coding) 등과 같은 계층적 압축 코덱들 역시 다양한 소스(source)와 결과영상들로 구성되기 때문에 앞선 저작권 보호 기술들만으로는 보호가 어렵다. 따라서 지속적이고 기하급수적으로 발전하고 있는 비디오 콘텐츠 시장에서 효과적이고 신뢰할 수 있는 통합적 저작권 보호 시스템의 필요성 증대되고 있다.

본 논문에서는 생물학적 바이러스를 이용한 비디오 콘텐츠의 전염성 정보은닉 시스템 모델링을 제안한다. 제안한 모델링은 각 비디오 코덱 및 콘텐츠 자체가 갖는 고유의 특성에 따라 콘텐츠의 복사, 편집, 트랜스코딩 등에도 은닉된 정보가 유지되거나 전염되는 것으로 콘텐츠를 보호할 수 있는 전염성 정보은닉이다. 본 기법은 각 비디오 코덱의 인코더(encoder) 및 디코더(decoder)를 각각의 숙주로 하여 은닉된 정보를 검출, 변이 및 재은닉의 과정을 수행함으로써 콘텐츠를 보다 안전하게 보호할 수 있게 한다. 따라서 본 논문에서는 생물학적 바이러스 개념의 비디오 콘텐츠를 위한 정보은닉 모델링을 제안하는 것으로, 생물학적 바이러스 이론을 정보은닉 이론에 결합한 새로운 비디오 콘텐츠 정보은닉 이론을 제시한다. 그러나 이에 대한 연구는 아직 초기 단계로 본 논문에서는 전염성 정보은닉 과정의 모델링에 중점을 두었으며, 향후 전염성 정보은닉 시스템의 세부 기술에 대한 연구를 진행할 것이다.

Ⅱ. 제안 IIH 시스템 모델링

제안된 IIH 기반 비디오 콘텐츠 보호 기술 시스템은 자연계에 존재하는 생물학적 바이러스의 감염성에서 착안하였으며, 그 생물학적 바이러스의 각 구성성문 및 감염절차를 이해하고 분석하여 이를 비디오 콘텐츠 보호 기술에 응용하기 위한 모델링을 수행하였다.

2.1 전염성 정보 모델링

제안 시스템에서 최우선적으로 고려되어야 하는 것은 전염성을 가진 정보를 생물학적으로 전염성이 있는 바이러스 입자를 이해함으로써 제안 시스템에서 은닉될 전염성 정보를 모델링하는 것이다[20~21]. 이에 대한 생물학적 바이러스를 이용한 제안 시스템에서의 전염성 정보 모델링은 그림 1에 나타내었다.

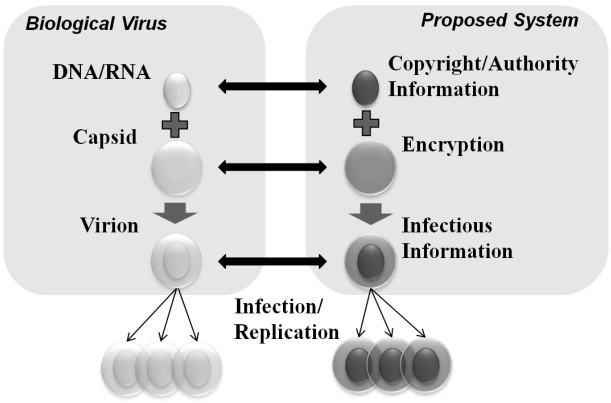

그림 1. 생물학적 바이러스 이론을 이용한 전염성 정보은닉 모델링

Fig. 1. Modelling of infectious information hiding by using biological virus theory.

우선 생물학적 바이러스 구성요소 중 가장 중요한 유전학적 물질로서 바이러스를 구성하는 성분들 중의 하나인 DNA/RNA는 제안된 시스템에서 상업적 가치를 가진 비디오 콘텐츠의 저작권 및 권한제어 정보로써 적용하였다. 또한 캡시드(capsid)는 바이러스의 유전체 핵산인 DNA/RNA를 보호하기 위해 둘러싸는 규칙적으로 배열된 단위소립자 형태의 단백질 외각으로써, 이것은 제안한 IIH 시스템에서 전염성 정보 생성 시 사용되는 소유권자 및 비디오 콘텐츠의 권한제어 정보를 염기서열로 간주하여 인위적으로 검출 및 수정/제거 할 수 없도록 하기 위한 암호화/복호화 과정으로 적용하였다. 이로써 DNA/RNA와 캡시드가 결합된 형태를 갖추어 완전한 바이러스 입자인 비리온(virion)이 생성된다. 생성된 바이러스는 감염 조건이 이루어졌을 때 비리온의 형태로 숙주로부터 전염되는데, 이 때 비리온은 감염 경로 및 형태에 따라 병원체(pathogen), 돌연변이(mutant) 및 감염체(contagion)로 구분되며 제안된 시스템에서도 동일한 의미와 이름으로 모델링하였다. 최종적으로 제안 IIH 시스템에서는 생물학적 바이러스가 갖는 소유권자 및 비디오 콘텐츠의 권한제어로써 생성된 정보들을 암호화함으로써 전염성 정보로 모델링하였다.

2.2 전염 조건 및 전염 과정 모델링

바이러스의 세포 감염 및 증식은 2.1절의 과정에서 생성된 비리온이 표적세포에 결합, 침입하여 유전 물질을 세포 안으로 전달되는 과정으로서 이루어지며[22], 제안한 시스템에서는 이 과정을 IIH 기술이 수행되는 과

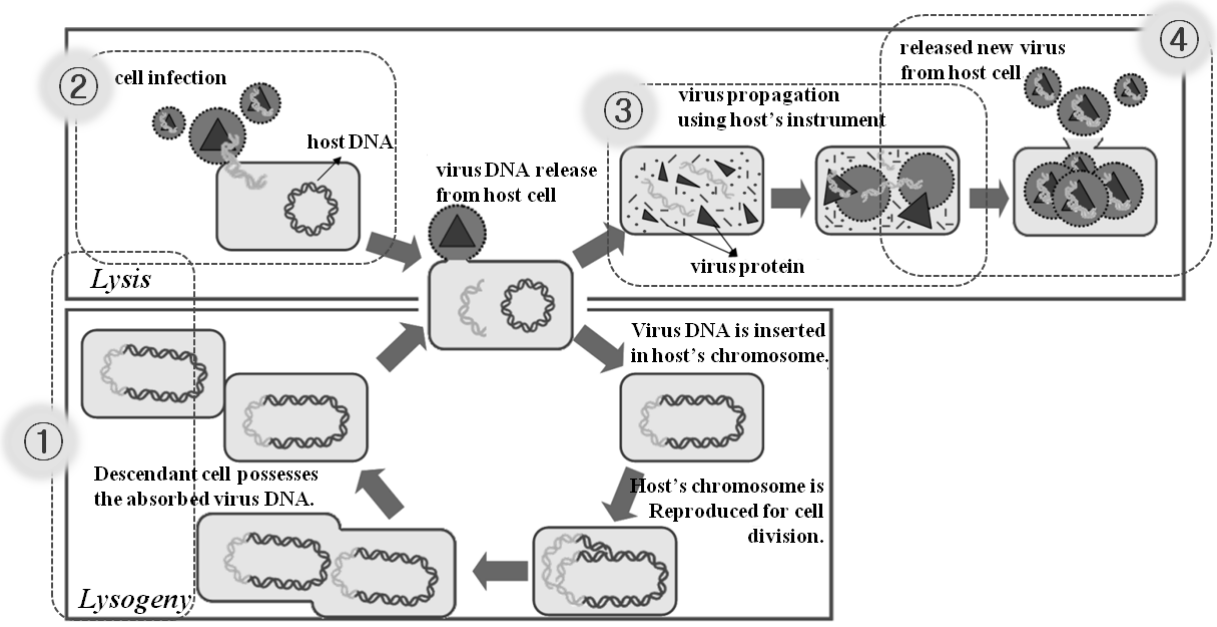

그림 2. 자연 상태에서의 바이러스 전염 과정
Fig. 2. Virus infection process in the nature.

정으로 모델링할 수 있다. 이 때, 세포 종류에 따라 자손 비리온이 만들어지는 방법이 다양하므로 이것을 제안한 시스템에서는 콘텐츠 및 코덱의 종류에 따라 다양한 호환 가능한 정보은닉 알고리즘이 접목될 수 있는 것으로서 표현할 수 있다. 또한 바이러스가 전염될 때 하나의 비리온에서 수백 개의 자손을 만드는 과정을 복제라고 하며, 이것은 제안된 플랫폼에서는 콘텐츠 복제 및 트랜스코딩 시에 은닉된 전염성 정보가 감염되는 것을 의미한다. 또한, 생물학적 바이러스는 복제를 위해 용균성(lysis) 및 용원성(lysogeny)이라는 두 가지 전략을 가지게 된다. 제안 시스템에서 전염성 정보의 감염 및 복제에 대해 생물학적 바이러스로 모델링한 것을 그림 2를 바탕으로 자세히 나타내었다. 즉, 이 그림에서는 자연 상태에서의 바이러스 전염 과정을 나타낸다. 그림 2-①은 바이러스의 감염 특성에 따라 용균성 및 용원성으로 분류한 것이다. 첫째, 바이러스가 숙주세포를 용해 또는 파괴시키는 용균성 바이러스의 경우, 제안된 시스템이서 검출된 전염성 정보를 이용하여 디스플레이 장치 혹은 디코딩된 비디오 콘텐츠 자체에서 권한 제어 코드로 사용될 수 있음으로 모델링하였다. 한편, 주변 환경에 따라 복제 조건이 될 때까지 숙주에 유전 물질을 숨겨 놓았다가 복제하는 용원성 바이러스의 경우는 은닉된 워터마크의 저작권 보호 및 사용자 인증의 의미로 적용될 수 있다. 그림 2-②의 과정은 숙주세포에 바이러스가 감염되는 과정을 나타내며, 제안 시스템에서는 전염성 정보은닉 되는 과정으로 간주된다. 그림 2-③의 과정에서 숙주세포의 구조에 따라 바이러스의 감염방법이 달라지므로, 이 때 숙주세포를 비디오 콘텐츠의 형태, 즉. 프레임 단위의 비디오 영상인지 코드워드를 갖는 압축된 비트스트림 형태인지에 따라 정보은닉 기술을 다르게 적용할 수 있는 것으로 모델링 할 수 있다. 그림 2-④의 과정에서 바이러스는 감염된 숙주에 의해 다른 세포들로 복제, 전염되며, 이것은 한번 감염된 비디오 콘텐츠는 복제되거나 트랜스코딩 되더라도 전염성 정보 역시 온전하게 전이되는 것으로 설계된다.

2.3 전염성 정보은닉 기법

자연 상태에서의 생물학적 바이러스 전염 특성을 기반으로 제안한 시스템의 기술적 정의 및 전략은 그림 3에서와 같다. 이 그림에서 정의된 제안 시스템의 4개의 중요 기술 개념은, 그림 3-①의 감염 검사 및 권한 제어를 위한 전염성 정보 인증 기술과 그림 3-②의 숙주(커널) 기반 정보 감염 기술, 그림 3-③ 재생되는 비디오 콘텐츠에 대한 콘텐츠 자체 기반 정보 감염 기술 그리고 그림 3-④ 전염성 정보 생성 및 관리 기술 등으로 구성되며, 이들 기술 각각의 정의 및 개념과 각 기술 개념에서 요구되는 세부 연구 목적을 아래에 자세히 나타내었으며, 제안한 시스템에서는 각 부분의 목적에 부응

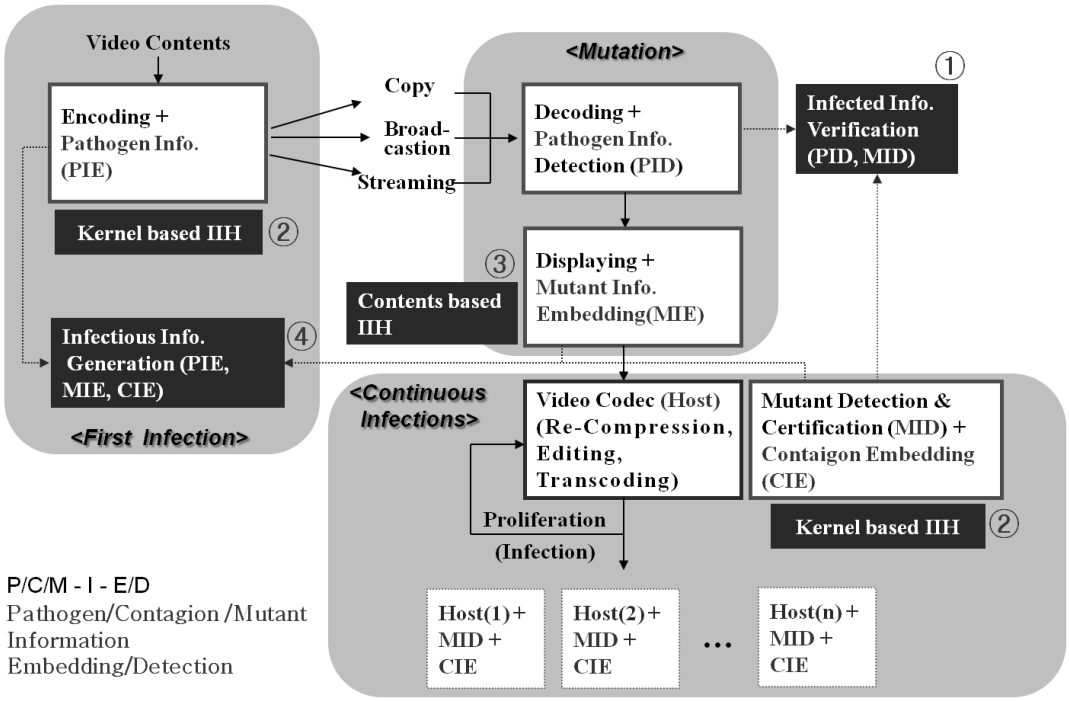

그림 3. 제안 시스템의 기술적 정의 및 비디오 콘텐츠 보안 전략
Fig. 3. Technical definitions of proposed scheme and security strategy of video contents.

하는 정보은닉 기술들을 다양하게 적용할 수 있게 한다. 그림 3을 바탕으로 각 세부 기술 도구들을 아래와 같이 정의하였다.

2.3.1 감염 검사 및 권한 제어를 위한 전염성 정보인증 기술

이 기술은 해당 비디오 콘텐츠가 디코딩/인코딩 될 때 전염성 정보 검출과정을 통해 감염 여부를 검사하는 기술이다. 해당 비디오가 감염되었다고 판단될 때, 검출된 정보로부터 소유권자/저작권자 및 권한제어 정보를 검증하기 위한 도구로서 정의한다. 이것은 검출된 워터마크의 신뢰성을 검증하기 위한 기술도구로써 코덱으로부터 검출된 정보를 검사하여 손상된 정보를 보정하여 유지하거나 변환된 콘텐츠에 재은닉하기 위해 사용된다.

2.3.2 코덱 기반 전염성 정보은닉 기술

다양한 비디오 압축 기술에 대한 코덱 기반의 전염성 정보 감염 기술로서 정의한다. 이 경우, 코덱이 전염성 정보의 숙주로 간주되며, 비디오 재압축 및 트랜스코딩 시에 정보의 전염이 수행된다. 이 기술을 위해 비디오 부호화 과정에서 수행되는 양자화와 DCT/DWT 커널 혹은 ME/MC(motion estimation/motion compensation) 과정에서 생성되는 주파수 계수 및 움직임벡터 등을 이용할 수 있다. 또한 가역 워터마킹 기법을 이용하여, 압축 영역에서의 콘텐츠 암호화도 가능케 할 수 있다.

2.3.3 콘텐츠 기반 전염성 정보은닉 기술

프레임 단위로 디코딩되어 재생되는 비디오 콘텐츠에 대해서 콘텐츠 자체를 숙주로 한 전염성 정보은닉 기술로 정의된다. 이 과정은 원시 비디오 데이터가 생성될 때, 또는 디코더로부터 비디오 프레임이 생성 될 때, 검출된 병원체 및 감염체 정보를 이용하여 돌연변이 정보로 변환하여 전염시킬 수 있다. 따라서 일반적인 영상처리와 기하학적 변환에 강인하도록 주파수 변환 및 공간영역에서의 정보은닉 기술이 요구된다.

2.3.4 전염성 정보의 생성 및 관리기술

비디오 콘텐츠의 저작권 및 권한제어 관리를 위하여 다양한 형태들의 전염성 정보를 생성 및 관리하는 기술을 정의한다. 앞서 정의한 숙주의 형태에 따라 각각 병원체(감염체) 및 돌연변이로 간주되는 전염성 정보를 생성하는 기술로 정의한다. 여기서 병원체 및 감염체는 비디오 인코딩 시에 은닉되는 정보를 의미하며, Video

콘텐츠가 처음 인코딩될 때 최초 제작자/저작권자로부터 생성되어 은닉되는 전염성 정보를 병원체로 정의하였다. 반면 비디오 편집 등을 거친 후 재압축 과정에서 전염되는 정보에 대해서 비디오 코덱에 의해 감염되는 감염체로 정의하였다. 2.2절에서 나타낸 바와 같이, 병원체(감염체) 정보는 그 자체를 암호화 키로 사용하여 비디오 콘텐츠의 암호화 알고리즘으로도 사용 가능(용균성)하도록 설계할 수 있다. 한편, 이 기술도구에서는 비디오 디코딩 과정에서 검출된 병원체(감염체) 정보를 이용하여 디코딩된 비디오 프레임에 대해 은닉되는 정보로서 돌연변이 정보를 생성한다. 이것은 코덱으로부터 인코딩되는 비디오에 은닉되는 정보와는 달리 2.3.3절에서 설명한 비디오 프레임 기반에서 은닉되므로 병원체(감염체)와 다른 형태를 가질 수 있기 때문에 본 논문에서는 이러한 특징을 갖는 은닉정보를 돌연변이 정보로 정의하였다.

Ⅲ. 제안한 전염성 정보 은닉 알고리즘

제안 시스템의 효과적인 연구를 위해 앞선 장에서 정의한 각각의 기술도구들에 대한 심층적인 연구가 뒤따라야 할 것이며, 여기서 기존의 다양하고 우수한 정보은닉 알고리즘들을 재해석하고 응용하여 제안 시스템에 적용함으로써 보다 향상된 기술로 진화할 수 있을 것으로 기대한다. 이러한 관점에서 본 논문은 비디오 콘텐츠 보안을 위한 전염성 정보은닉 기술이라는 하나의 새로운 패러다임과 시스템을 제안하였으며, 이 장에서는 제안 시스템의 검증을 위해 2장에서 정의한 내용을 기반으로 시나리오를 설정하고, 코덱 기반 및 콘텐츠 기반의 정보 은닉 알고리즘을 각각 나타내었다.

제안 시스템은 비디오 콘텐츠 처리를 위한 대다수의 소프트웨어들이 컴퓨터 운영체제의 제어 하에서 디바이스 드라이버 형태로 해당 비디오 코덱 라이브러리를 호출하는 특성을 이용한다. 그에 따라 코덱 라이브러리의 인코더/디코더 상에 전염성 정보은닉 및 검출 알고리즘을 탑재하고, 감염된 비디오 콘텐츠를 이용하는 소프트웨어 상에서 전염성 정보를 캡시드 형태로 저장하였다가 비디오 트랜스코딩 시 그것을 전염시키는 시스템을 검증과정으로 간주하였다. 제안한 시스템 및 알고리즘들에 대한 실험을 위해, 현재까지 연구된 다양한 비디오 코덱 중 알고리즘 집적도 및 계산복잡도가 높은 측에 속하며 디코딩된 비디오 데이터에 대해서 트랜스코딩이 유용한 H.264 SE/MPEG-4 SVC 코덱을 최초의 숙주로 간주하였다. 또한 디코딩 SVC 비디오를 이용하는 H.264 및 MPEG-2 비디오 코덱들을 감염체로 간주하여 전염성 정보를 은닉 및 감염시키는 것으로 실험을 수행한다. 그림 4로서 제안 시스템의 검증을 위한 시나리오를 나타내었다. 그림 4로부터, 우선 최초 생성된 비디오 데이터는 SVC 인코더 내의 전염성 정보은닉 알고리즘에 의해 병원체 정보로써 최초 감염된다. 그렇게 감염된 비디오 콘텐츠가 유통된 후 SVC 디코더에 의해 디코딩되면서 병원체 정보가 검출되고, 이는 다시 디코더 내의 전염성 정보은닉 알고리즘에 의해 디코딩 된 비디오 콘텐츠에 돌연변이의 형태로 재감염되는 방식으로 지속적으로 콘텐츠의 저작권 및 정상적인 유통이 보장될 수 있다.

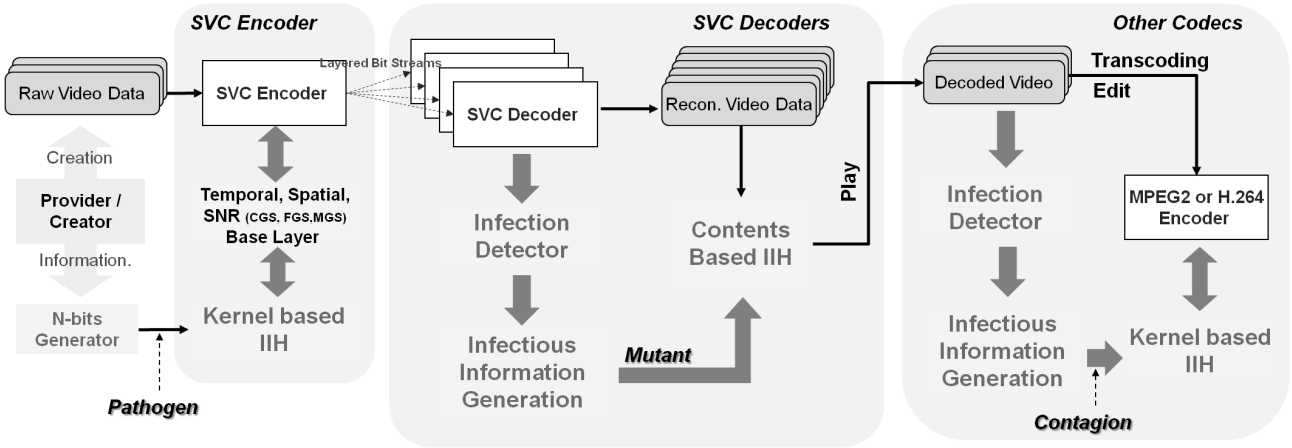

그림 4. 제안한 정보은닉 시나리오
Fig. 4. Information hiding scenario of proposed scheme.

3.1 전염성 정보 생성

병원체 및 감염체로 불리는 전염성 정보는 전염 과정에 의해 이름이 구분되지만, 실제 비디오 코덱을 기반으로 전염되어진다는 점에서 같은 형태의 이진 정보 코드를 가질 수 있지만, 생물학적 바이러스가 전염될 때 병원체와 감염체의 캡시드가 달라지는 경우가 발생한다. 따라서 제안한 IIH 시스템에서도 암호화 기법이 달라질 때, 병원체 워터마크의 비트스트림 형태가 감염체의 비트스트림과 달라질 수 있다.

그림 4의 시뮬레이션을 위해 여기서는 저작권자 및 권한제어 정보로써 임의 값을 갖는 64비트 길이의 정보를 사용하였으며 암호화키를 통해 Virion에 해당되는 암호화 과정으로서 간단히 XOR 암호화하여 병원체 정보 $W^P=\{w_i^P \in [-1,1]\}, 0<i<63$을 생성하였다. 시뮬레이션의 복잡성을 줄이기 위하여 병원체 정보 W^P, 돌연변이 정보 W^M 및 감염체 정보 W^C들은

$$W^P \equiv W^M \equiv W^C \tag{1}$$

와 같이 동일하게 사용된다.

4.2 커널 기반 IIH 알고리즘

본 논문에서는 제안 시스템의 시뮬레이션을 위해 병원체 및 감염체 정보를 전염시키기 위한 커널 기반 IIH 기술도구로서 간단하면서도 몇몇 파라미터만 변경하여 다양한 비디오 압축 알고리즘에 적용 가능한 워터마킹 알고리즘을 고안하였다. 이 기법은 H.264 SE/MPEG-4 SVC 비디오 압축 알고리즘 내에서 인트라 프레임의 4×4 DCT 변환 블록의 화질 복잡도를 계산한 후, 복잡도가 높은 DCT 블록 내에서 임의의 AC 계수 값에 워터마크를 은닉하는 알고리즘이다. 이 알고리즘은 비디오 압축과정에서 DCT 주파수를 이용한 화질복잡도를 계산함으로써 화질 열화를 줄이고, 비교적 간단한 연산을 수행하므로 압축과정의 실시간성을 유지할 수 있다는 장점이 있다. 제안 IIH 시스템에서 은닉되는 정보의 신뢰성을 높이기 위해 인트라 프레임들의 주기 f_{intra}와 병원체 정보 W^P의 비트수 I^{W^P}, 그리고 한 프레임 내에서 수평, 수직 방향에 대한 각각의 DCT 블록의 수 b_h 및 b_v를 이용하여 프레임 주기 f_{intra}에 따라 주기적으로 은닉되는 워터마크 비트 수 R^{W^P}를

$$R^{W^P} = I^{W^P} \times floor\left[\frac{b_h \times b_v}{I^{W^P}} \times f_{intra}\right] \tag{2}$$

와 같이 결정한다. 여기서 f_{intra} 및 I^{W^P}는 각각 1과 64로 정한 후, 실험을 수행하였다.

다음으로 영상의 화질을 고려하여 각 인트라 프레임 내 4×4 DCT 블록의 화질 복잡도 s_n는

$$s_n = \sum_{0 \le u,v}^{d} |x_n(u,v)| - \sum_{0 \le u,v}^{1} |x_n(u,v)|, \quad 0 \le n < N,\ N = b_h \times b_v \tag{3}$$

와 같이 구하여지며, 다양한 영상 압축 알고리즘에서 사용되는 DCT 블록 크기에 따라 u, v 및 d가 결정된다. 또한, DCT 계수 중 저주파 영역으로 판단되는 지그재그 순서의 0, 1, 2 및 3번째 계수는 해당 블록의 복잡도에 큰 영향을 주지 않으므로 복잡도 계산에서 제외된다. 여기서, $x_n(u,v)$는 인트라 프레임 내에서 n번째 DCT 블록 내 각각의 계수 값을 나타내며, $S=\{s_0, s_1, s_2, \cdots s_{N-1}\}$은 해당 DCT 블록 내에서 저주파 계수를 제외한 DCT 계수들의 절대 크기의 합이다. 다음 단계에서는 모든 DCT 블록의 화질 복잡도 s_n들을 최대값 $\max(s_n)$으로부터 내림차순 정렬하여 워터마크 은닉을 위한 r^{W^P}개의 블록 $K_{ordered}=\{k_0, k_1, k_2, \cdots k_{R^{W^P}-1}\}$을 추출한다. 추출된 DCT 블록 k_r, $0 \le r < R^{W^P}$ 들 상에 워터마크가 은닉된 임의의 계수 값 $x_{k_r}^w$는

$$x_{k_r}^w = \frac{s_{k_r}}{m_{k_r}} \bullet (w_{k_r} + \alpha) \tag{4}$$

와 같다. 여기서 m_{k_r}은 앞서 언급하였듯이 k_r번째 DCT 블록에서 0, 1, 2 및 3번째 계수 값을 제외하고, 나머지 0이 아닌 계수 값들의 개수를 의미한다. w_{k_r}은 해당 블록에 할당된 워터마크 비트를 의미하며, α는 삽입강도와 화질 사이의 상호 보완관계를 결정하기 위한 인자로써 사용된다. 마지막으로 식 (4)에 의해 생성된 임의의 AC 계수 값 $x_{k_r}^w$을 각 블록에 할당된 임의의 사용자 정의 키값 $e_{k_r}^u$ 및 $e_{k_r}^v$에 의해

$$x_{k_r}(e_{k_r}^u, e_{k_r}^v) = x_{kr}^w \tag{5}$$

와 같이 해당 블록 k_r의 계수 값으로 치환된다.

워터마크 검출 알고리즘은 워터마크 은닉 시 사용한 사용자 정의 키값 $e_{k_r}^u$ 및 $e_{k_r}^v$을 이용하여

$$\hat{w_i}= \begin{cases} 1, \text{if } \widetilde{x_{k_r}}(e_{k_r}^u, e_{k_r}^v) \geq th_{k_r} \\ 0, otherwise \end{cases} \quad (6)$$

$$th_{k_r} = \frac{\widetilde{s_{k_r}}}{\widetilde{m_{k_r}}} \quad (7)$$

와 같이 수행된다.

4.3 콘텐츠 기반 정보 감염 알고리즘

원본 비디오 영상 또는 비디오 코덱으로부터 디코딩되는 비디오 데이터에 대해 본 논문에서 제안한 콘텐츠 기반 IIH 기술을 구현하기 위한 콘텐츠 기반 정보은닉 기법을 설계하였다. 이 기법은 H.264 SE/MPEG-4 SVC 압축에 강인하게 설계된 알고리즘으로서 각종 압축 및 트랜스코딩에 강인한 특성이 있음을 실험을 통해 확인하였다. 이 방법은 H.264 SE/MPEG-4 SVC 압축을 고려해, 압축 전에 원본 영상으로 생성된 공간영역상에서의 L_MAX 개의 레이어 중 기본계층(spatial base layer) $f_{L_0}(x,y)$와 상위 계층들(spatial enhancement layers) $f_{L_n}(x,y)$, $1 \leq n < L\_MAX$ 모두를 워터마킹에 이용하여. 기본계층에 워터마크를 은닉한 후 보간법과 양자화 테이블을 이용하여 상위계층들에 대해 워터마크를 은닉하는 특징을 가진다. 제안한 IIH 시스템에서는 H.264 SE/MPEG-4 SVC의 각 공간해상도 뿐 아니라, 트랜스코딩 이후의 다양한 공간해상도에 대해 적응적인 알고리즘을 제안하였다. 돌연변이 정보를 전염시키기 위해 우선, 영상의 해상도에 따라 각 프레임 내에서 ROI

$$r(i,j) \in f(x,y), \quad (8)$$

$$a \leq i < (a+R^h),\ b \leq j < (b+R^v)$$

을 결정한다. 여기서 R^h 및 R^v는 프레임 크기로부터 스케일링 인자 η, $0 < \eta \leq 1$에 의해 결정된 ROI의 수직 및 수평 크기를 나타내며, a, b는 프레임 내에서 선택된 ROI의 수평, 수직 좌표에 대한 기준 좌표를 나타낸다. 각 프레임에서 ROI가 선택된 후, 선택된 ROI에 대해 DCT 계수 $c(u,v)$를 획득한다.

한편, 제안 기법을 위해 워터마크 삽입키로서 MPEG 2의 인트라 DCT 양자화 테이블 $q(g,k)$, $0 \leq g,k < 8$을 식 (9) 및 식 (10)을 이용하여 ROI의 수직 및 수평 크기인 R^h, R^v의 크기만큼 각각 보간한다.

$$qt^{ROI}(i,j) = \begin{cases} q(i,m), \text{if } j = l_H \times m \\ \lfloor (q(i,m)+q(i,m+1))/2 \rfloor, \\ \qquad \text{if } j = \lfloor (l_H(2m+1))/2 \rfloor \\ \vdots, \vdots \\ q(i,7), \text{if } j = \eta \cdot (R^h/2^n)/8 - 1 \end{cases} \quad (9)$$

$$qt^{ROI}(i,j) = \begin{cases} q(m,j), \text{if } i = l_V \times m \\ \lfloor (q(m,j)+q(m+1,j))/2 \rfloor, \\ \qquad \text{if } i = \lfloor (l_V(2m+1))/2 \rfloor \\ \vdots, \vdots \\ q(7,j), \text{if } i = \eta \cdot (R^v/2^n)/8 - 1 \end{cases} \quad (10)$$

이 때, 수평 수직 보간에 사용되어지는 각각의 가중치 l_H 및 l_V는

$$\begin{cases} l_H = \lfloor \eta \bullet (R^h/2^n)/8 \rfloor \\ l_V = \lfloor \eta \bullet (R^v/2^n)/8 \rfloor \end{cases} \quad (11)$$

와 같이 계산되어지며, m, $0 \leq m < 7$은 보간된 양자화테이블 $qt^{ROI}(i,j)$에 치환될 $q(g,k)$의 위치값이다.

워터마크 키로 사용될 양자화 테이블 $qt^{ROI}(i,j)$가 생성되면, DCT 변환된 ROI $c(u,v)$를 에 대해 지그재그스캔 한 후 각각의 계수값 c_z 및 qt_z를 이용하여

$$Q(c_z^*) = \begin{cases} \lfloor c_z/(qt_z \bullet \alpha) \rfloor \,\|\, (1 \ll \delta), \text{if } w = 1 \\ \lfloor c_z/(qt_z \bullet \alpha) \rfloor \,\&\&\, \sim (1 \ll \delta), \\ \qquad otherwise \end{cases} \quad (12)$$

와 같이 양자화하고 대상 계수 값의 특정 비트를 트리거함으로써 워터마크를 은닉한다. 여기서 양자화 강도를 조절하기 위한 α 및 워터마크 비트를 트리거 하기 위한 δ로써 워터마크 삽입강도를 조절하고 화질을 고려해 지그재그 스캔 된 1차원 계수 값들 중 10번째 계수 값부터 $9 \leq z < 73$의 범위에 64비트의 워터마크(돌연변이 정보)를 은닉하였다. 워터마크가 삽입된 양자화 ROI를 역양자화 및 역DCT 과정을 거친 후 원본 프레임에 치환함으로써 정보은닉이 완료된다.

워터마크 검출은 은닉과정과 동일한 순서를 거쳐 각 계수 값들의 δ번째 비트의 값을 검사함으로써

$$\hat{w}=\begin{cases}1\ ,\mathrm{if}\left(\left\lfloor \widetilde{c_z}/(qt_z\cdot\alpha)\right\rfloor\ \&\&\ (1<<\delta)\right)=1\\ 0\ ,otherwise\end{cases} \tag{13}$$

와 같이 수행된다.

Ⅳ. 실험 결과 및 고찰

제안 IIH 시스템의 실험을 위해 사용된 커널 기반, 및 콘텐츠기반의 정보은닉 기술을 앞서 설명하였다. 이 장에서는 제안한 IIH의 패러다임에서 중요한 정보의 전염성에 대한 검증을 위해 그림 4에서 이미 나타내었듯이, H.264 SE/MPEG-4 SVC를 최초 콘텐츠 생성 시 사용한 코덱으로 간주한다. 병원체가 감염된 콘텐츠를 SVC 디코딩한 후 MPEG-2 재압축 후, 전염된 정보를 검증하고, 다시 H.264로 재압축하는 과정을 거치면서 병원체, 돌연변이 및 감염체 정보가 손실없이 전염됨을 실험하였다. 실험에 사용한 두 가지 영상을 그림 5에 나타내었다.

(a) (b)

그림 5. 제안한 IIH 시스템 실험에 사용한 영상;
(a) 4CIF@30fps CREW 영상
(b) CIF@30fps FOREMAN 영상

Fig. 5. Test image sequences for evaluating the proposed IIH system; (a) 4CIF@30fps CREW image (b) CIF@30fps FOREMAN image.

실험에서 H.264 SE/MPEG-4 SVC를 위한 커널기반 IIH 기술은 시간, 공간 및 화질 스케일러빌리티를 위한 기본계층(base layer)에 대해 수행된다. SVC의 각 레이어의 비트열은 독립적으로 인코딩되며, 따라서 기본계층에 은닉된 정보로써 모든 레이어에서 검출 가능하므로, 본 실험에서는 복잡성을 피하기 위해 시간 및 화질에 대한 레이어는 모두 1계층으로 고정하였다. 그림 4의 각 감염경로에서 각각의 코덱을 거치기 전, 후의 전염성 정보를 검출하여 그 결과를 표 1에 나타내었다. 표 1에 나타낸 바와 같이, 각 코덱의 인코더 및 디코더 각각에서 전염된 정보를 검출, 변이, 재은닉의 과정을 거침으로써 모든 경로 상에서 압축률에 상관없이 최초에 은닉하였던 64bit의 정보가 비트오류 없이 온전히 전염됨을 확인하였다.

또한 제안 IIH 시스템의 특성상 인코딩 시 설정하는 압축율과 관계없이 전염되므로, 각 표 1에서 나열한 각 코덱으로부터 고화질 압축을 수행하면서 전염된 정보에 의한 화질 열화 정도를 표 2에 나타내었다. 객관적 화질척도로써 PSNR(peak signal to noise ratio)를 사용하였다. 표 2에서 나타내었듯이 비디오 콘텐츠를 고화질로 트랜스코딩을 수행했을 경우 화질의 열화는 객관적으로 큰 차이가 없음을 확인할 수 있다. 하지만, 1차 전염이 일어났을 때 화질 열화가 비교적 크게 발생함을 확인하였다. 이는 1차 전염이 발생할 때 콘텐츠 기반 IIH가 수행되면서 돌연변이 정보에 대한 정보은닉 알고리즘이 병원체 IIH 알고리즘과 다르고, 본 실험에서 사용한 알고리즘의 특성 상 은닉된 정보의 강인성이 우선적으로 고려되었기 때문에 야기된 것으로 확인되었다. 반면에, 표 2로부터 2차 전염 이후부터는 전염성 정보의 재생, 유지 특성으로 인해 더 이상의 화질 열화가 발

표 1. 각 감염경로에서 감염체 및 돌연변이 정보의 전염 결과

Table 1. Experimental infected results of contagion and mutation information (watermark) in each infection way.

Test Sequence	Layer	*Host*	*1st Infection*		*2nd Infection*	
		SVC	MPEG-2		H.264	
		Decoded (Mutant 1)	Encoded (감염체)	Decoded (Mutant 2)	Encoded (감염체)	Decoded (Mutant 3)
CREW	4CIF	*All Infected with No Bit Error*				
	CIF					
	QCIF					
FOREMAN	CIF					
	QCIF					

표 2. 이종 코덱으로의 트렌스코딩 시 전염된 정보에 의한 화질열화 비교(PSNR, dB)
Table 2. Comparison of image degradation (PSNR, dB) by the infected information in transcoding to heterogenous codec.

Test Sequence	Layer	Host		1st Infection		2nd Infection	
		SVC		MPEG-2		H.264	
		Com-pression	Infection	Com-pression	Infection	Com-pression	Infection
CREW	4CIF	41.16	39.41	39.62	35.26	39.50	35.07
	CIF	43.23	40.57	41.45	36.43	41.15	36.44
	QCIF	47.52	42.20	42.12	36.60	42.09	36.45
FOREMAN	CIF	44.29	41.95	42.54	36.48	42.38	36.30
	QCIF	49.81	44.60	45.07	37.30	45.05	37.23

생되지 않음을 확인할 수 있었다.

기존의 비디오 워터마킹에서는 트랜스코딩시 워터마크 삽입 알고리즘에 따라 워터마크의 부분 손실 또는 완전 손실이 발생될 수 있다. 예를 들어, 8×8 DCT 기반의 워터마크 삽입 알고리즘 경우, 트랜스코딩 과정에서 DCT 블록 크기가 달라지거나 혹은 주파수 변환커널이 DWT로 변경되면, 워터마크 손실이 커진다. 제안 시스템에서는 이와 같은 트랜스코딩시 문제점을 최대한 보완하기 위하여 워터마크 전염성을 이용하여 트랜스코딩 수행 전에 워터마크가 검출이 되고, 트랜스코딩 되는 코덱, 혹은 시공간 해상도 변경에 따라 적응적으로 재은닉함으로써 워터마크 손실이 일어나지 않도록 하였다. 이상의 실험 결과로부터 제안 시스템에서 워터마크 손상이 전혀 발생하지 않음을 확인할 수 있었다.

V. 결 론

본 논문에서는 생물학적 바이러스의 특성과 감염 절차를 이용하여 전염성 정보은닉(IIH) 기술 기반의 비디오 콘텐츠 보호 시스템을 제안하였다. 아울러 새로운 패러다임으로서의 IIH에 대한 개념 및 기반 기술들을 소개하였다. 제안한 IIH 시스템에서는 은닉되는 정보를 전염성 바이러스로, 콘텐츠 및 코덱을 숙주 및 감염 매개체로 하는 비디오 콘텐츠 보호 기술을 모델링 하였다. 또한 제안 시스템의 각 기술들에 대해 비디오 워터마킹 알고리즘들을 적용하여 시뮬레이션 함으로써 제안 시스템의 가능성을 실험을 통해 검증하였다. 또한 현재 및 향후의 연구 계획으로서 비디오 콘텐츠 편집/녹화 도구들을 감염 매개체로 하여 비디오 콘텐츠의 접근 권한 제어, 다양한 비디오 편집, 두 가지 이상의 비디오 콘텐츠의 조합 및 비디오 화질 개선을 위한 후처리 등에 대해서도 강인하고, 효율적인 시스템으로 발전시키는 것을 목적으로 하고 있다. 아직 심층적인 연구가 미비하고 실험에 대한 정량적, 객관적 평가와 평가기준이 보완되어야 할 부분이 많지만, 본 논문에서 제안한 IIH 시스템의 지속적이고 심층적인 연구를 통해 기존의 우수한 비디오 콘텐츠 보호 기법들의 재해석과 그러한 기술들을 실제 응용 가능한 기술로의 발전 등을 가능케 할 것으로 기대하며, 꾸준히 강조되어온 비디오 DRM 및 정보 보호 기술 분야 등에서 On/Off-line 접근권한 제어, 저작권 및 소유권 검증 및 사용자 인증, 실시간 모니터링 및 워터마킹/핑거프린팅 위·변조 방지, 무결성 및 표준안 제시 등 여러 기능들을 발전시킬 수 있을 것으로 기대한다.

Reference

[1] F. Hartung and B. Girod, “Watermarking of Uncompressed and Compressed Video,” *Signal Processing*, Vol. 66 no. 3, pp. 283-301, May 1998.

[2] M.D. Swanson, B. Zhu, B. Chau, and A.H. Tewfik, “Object-based Transparent Video Watermarking,” *IEEE First Workshop on Multimedia Signal Processing*, pp. 369-374, 1997.

[3] 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.

[4] C.V. Serdean, M.A. Ambroze, M. Tomlinson, and J.G. Wade, “DWT based High- Capacity Blind Video Watermarking, Invariant to Geometrical Attacks,” *IEEE Proceedings Vision, Image and*

Signal Processing, Vol. 150, Issue 1, pp. 51-58, Feb. 2003.
[5] Y. Wang and Al. 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, June 2006.
[6] 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, Feb. 2007.
[7] 박혜정, 최준림, "H.264/AVC 비디오 보호를 위한 비가시적 워터마킹의 설계 및 검증," 대한전자공학회논문지, SD편, 제 45권 제 6호, 74-79쪽, 2008년 6월.
[8] 박현, 이성현, 문영식, "영상 특성을 이용한 3D-DCT 기반의 적응적인 비디오 워터마킹," 대한전자공학회논문지, SP편, 제 43권 제 3호, 68-75쪽, 2006년 5월.
[9] 박재연, 임재혁, 원치선, "MPEG-2 비트열에서의 인증 및 조작위치 검출을 위한 디지털 워터마킹 기법," 대한전자공학회논문지, SP편, 제 40권 제 5호, 76-85쪽, 2003년 9월.
[10] J.S. Yoon, S.H. Lee, Y.C. Song, B.J. Jang, K.R. Kwon, and M.H. Kim, "Video Watermarking Scheme for Scalable Video Coding using ROI," *Jour. of Korea Multimedia Society*, vol. 11, no. 6, pp.796-806, June 2008.
[11] J. Xin, C.-W. Lin, and M.-T. Sun, "Digital Video Transcoding," *Proceeding of IEEE*, vol. 93, no. 1, pp. 84-97, Jan. 2005.
[12] Generic Coding of Moving Pictures and Associated Audio Information-Part 2: Video, ITU-T Rec. H.262 and ISO/IEC 13818-2 (MPEG-2 Video), ITU-T and ISO/IEC JTC 1, Nov. 1994.
[13] Video Coding for Low Bit Rate Communication, ITU-T Rec. H.263, ITU-T, Version 1: Nov. 1995, Version 2: Jan. 1998, Version 3: Nov. 2000.
[14] Coding of audio-visual objects-Part 2: Visual, ISO/IEC 14492-2 (MPEG-4 Visual), ISO/IEC JTC 1, Version 1: Apr. 1999, Version 2: Feb. 2000, Version 3: May 2004.
[15] Advanced Video Coding for Generic Audiovisual Services, ITU-T Rec. H.264 and ISO/IEC 14496-10 (MPEG-4 AVC), ITU-T and ISO/IEC JTC 1, Version 1: May 2003, Version 2: May 2004, Version 3: Mar. 2005, Version 4: Sept. 2005,Version 5 and Version 6: June 2006, Version 7: Apr. 2007.
[16] ISO/IEC JTC1/SC29/WG11/N5231, Multimedia Framework (MPEG-21), 2004.
[17] ISO/IEC JTC1/SC29/WG11/N5231, Applications and Requirements of Scalable Video Coding N6830, Palma de Mallorca, Spain, Oct. 2004.
[18] http://www.bbc.co.uk/opensource/projects/dirac/
[19] http://www.xvid.org
[20] Matthews, *R.E.F. Plant virology (3rd ed.)*, Academic press.
[21] Virus taxonomy, Reports of the ICTV, http://www. ictvonline.org/
[22] Virology introduction, http://home.inje.ac.kr /~lecture/virology/ch1introd/2003virch1.htm

저 자 소 개

장 봉 주(학생회원)

2002년 부산외국어대학교 전자공학과 학사 졸업.
2004년 부산외국어대학교 전자컴퓨터공학과 석사 졸업.
2007년～현재 부경대학교 정보보호협동과정 박사과정 수료.

<주관심분야 : 영상압축, 멀티미디어 정보보호>

권 기 룡(정회원)-교신저자

1986년 경북대학교 전자공학과 학사 졸업.
1990년 경북대학교 전자공학과 석사 졸업.
1994년 경북대학교 전자공학과 박사 졸업.
1996년～2006년 부산외국어대학교 디지털정보공학부 부교수
2006년～현재 부경대학교 IT융합응용공학과 교수

<주관심분야 : 멀티미디어 정보보호, 영상처리, 멀티미디어통신 및 신호처리>

이 석 환(정회원)

1999년 경북대학교 전자공학과 학사 졸업.
2001년 경북대학교 전자공학과 석사 졸업.
2004년 경북대학교 전자공학과 박사 졸업.
2005년～현재 동명대학교 정보보호학과 부교수

<주관심분야 : 워터마킹, DRM, 영상신호처리>