다중 불법콘텐츠 복제자 추적 기술 개발

Development of Forensic Marking technology for tracing multiple users

김 종 안*, 김 진 한, 김 종 흠
(Jongan Kim, Jinhan Kim and Jongheum Kim)

Abstract: Forensic Marking is the technology that enables the service providers (SP) to identify the illegal digital contents distributors by first inserting markings (data indicating the user information and playback time) in realtime into the digital contents at time of playback of digital contents, and then later by extracting inserted markings from the contents which are illegally captured from the multimedia device such as IPTV STBs and distributed over the Internet. Digital Rights Management (DRM), which is a very popular content protection technology, has the security hole that can be vulnerable because the encrypted digital contents are transformed into their original plaintext forms after the decrypting process on the STBs. Therefore Forensic Marking (FM) has now become a companion content protection solution to DRM.
This article describes a new way of tracking up to 4 illegal content users in FM implementation using the blue-difference chroma component of YCbCr color space. This FM technology has many advantages like fast processing time and easy portability to STB devices compared to that of the traditional watermarking processing in the frequency domain.

Keywords: Forensic Marking, Transactional Watermarking, fingerprinting, watermarking, DRM, content protection

I. 서론

초고속 인터넷 통신의 보급, 고성능 저가의 SoC(System on a Chip), 압축/복원 기술의 발달로 TV에서 보는 것과 동일한 프로그램을 Internet 프로토콜을 이용하여 볼 수 있는 IPTV 서비스가 점차 보편화 되고 있다. IPTV 서비스는 지상파 방송 등을 실시간으로 볼 수 있는 채널서비스, 사용자가 선택하여 콘텐츠를 재생하여 보는 VOD(Video On Demand: 주문형 비디오) 서비스, 그리고 날씨, 증권, 쇼핑 등의 양방향 서비스 등을 제공한다. IPTV 서비스 사업자는 사용자에게 전달되는 디지털 콘텐츠를 보호하기 위하여 실시간 채널서비스에는 유선 및 위성 방송에서 널리 사용되는 CAS (Conditional Access System: 수신 제한 시스템) 솔루션을, VOD 콘텐츠에는 DRM(Digital Rights Management: 디지털 저작권 관리기술)기술을 널리 사용한다.

IPTV 콘텐츠 보호에 사용되는 IPTV CAS 솔루션과 DRM 솔루션은 서비스제공업자의 헤드엔드에서 디지털 콘텐츠를 암호화하여 사용자 STB에 전송하고, 사용자의 STB에 있는 복호모듈(descrambler/decryptor)은 헤드엔드에서 전송한 복호키와 사용권한을 이용하여 암호화된 MPEG-2 TS(Transport Stream) 패킷을 복호화하고 사용권한에 맞게 콘텐츠를 재생하게 된다. 그러나 이러한 디지털 콘텐츠 보호솔루션은 오디오/비디오 재생 신호를 STB의 아날로그 출력단자(Composite, Component 단자 등)를 통해 TV로 전송하는 경로에 HDTV 수신카드 등의 디지털 캡처장비(capture devices)를 이용할 경우에는 더 이상 IPTV 콘텐츠를 보호할 수 없게 된다.

이러한 단점을 보완하기 위해서는 포렌식 마킹(Forensic Marking: 사용자 추적표시) 기술의 채택이 필요한데, 사용자 추적표시(FM) 기술은 디지털 콘텐츠 재생시점에 사용자에 관한 정보를 워터마킹 기술 등을 이용하여 실시간으로 재생되는 콘텐츠에 삽입한 후, 이 워터마킹이 삽입된 콘텐츠가 불법 복제되어 인터넷 등에 유포될 경우에 삽입된 사용자 워터마크 정보를 콘텐츠로부터 추출하여 법적 제재 근거를 마련하는 기술이다.

본 논문에서는 IPTV 콘텐츠 보호 관리하는 CAS와 DRM 기술에 대해 간략히 소개하고, 동영상 프레임의 색차 변경을 이용하여 최대 4인까지의 정보를 삽입하고 추출할 수 있는 포렌식 마킹 기술에 대해 자세히 다루고자 한다.

II. 디지털 콘텐츠 보호솔루션

1. CAS 솔루션

IPTV CAS 솔루션의 구성도는 아래 그림 1에 나타나 있다.

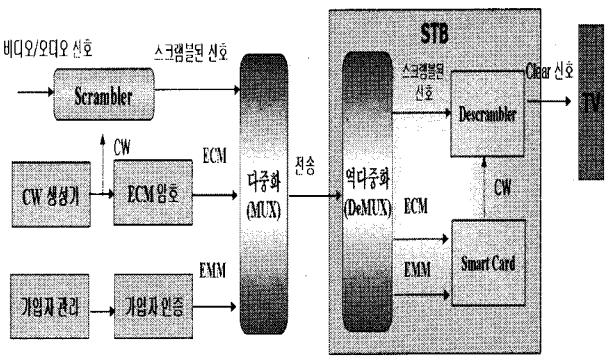


그림 1. IPTV CAS 솔루션 구성도
Fig. 1. The configuration diagram of the IPTV CAS solution

헤드엔드에 있는 인코더(H.264, MPEG-2 등)에 의해서 인코딩된 비디오와 오디오 신호는 스크램블러(scrambler)에 의해 암호화되고, 암호화된 신호는 인터넷 망을 통하여 IPTV

* 책임저자(Corresponding Author)
논문접수 : 2008. 7. 23., 채택확정 : 2008. 7. 31.
김종안*, 김진한, 김종흠 : KT 플랫폼연구소
(joankim@kt.co.kr, jinhan@kt.co.kr, jinah0719@kt.co.kr)

STB로 전달된다. 스크램블러가 채널 암호화에 사용하는 키는 CAS에서는 제어 키(Control Word: CW)로 불리며, CW 생성기(Generator)에 의해 생성된다. 채널 암호화에 사용된 CW는 채널 복호화 과정에서 사용되기 때문에, CW를 암호화하여 ECM(Entitlement Control Message: 자격 제어 메시지)에 넣은 후 인터넷 망을 이용하여 사용자 STB으로 전송한다. 채널 시청 권한은 EMM(Entitlement Management Message: 자격 관리 메시지)로 사용자 STB에게 전달되어 스마트 카드에서 ECM에 들어있는 CW를 푸는데 사용한다. 헤드엔드(HeadEnd)의 다중화 장치(MUX: Multiplexer)는 전송 효율화를 위하여 여러 개의 소스에서 오는 신호들 즉 스크램블 된 방송 신호와 ECM, EMM 메시지를 집중화해서 전송하는 역할을 한다. STB의 디스크램블러(descrambler)는 스마트카드에서 보내온 CW를 이용하여 암호화된 신호를 복호화하여 STB의 출력단자(Composite, Component 등) 단자를 이용하여 TV로 전송한다. 그러나, 실시간 채널 콘텐츠를 캡처하여 저장하고자 하는 사람들은 STB의 아날로그 단자에서 나오는 출력신호를 캡처 카드 등을 이용하여 비디오와 오디오 신호를 디지털 파일로 저장하여 인터넷에 유포하게 된다. 즉 CAS 솔루션은 서비스 제공업자의 헤드엔드 장비에서 STB내부에 이르는 경로에서만 보호기능을 제공할 뿐 STB 외부 경로에는 그 기능을 수행하지 못하는 단점이 있다.

2. DRM 솔루션

앞서 논의한 CAS 솔루션이 실시간 채널 보호에 한계가 있듯이 DRM 솔루션도 또한 VOD 콘텐츠 보호 범위가 제한적이다. 아래 그림 2는 DRM 솔루션 구성도를 보여준다.

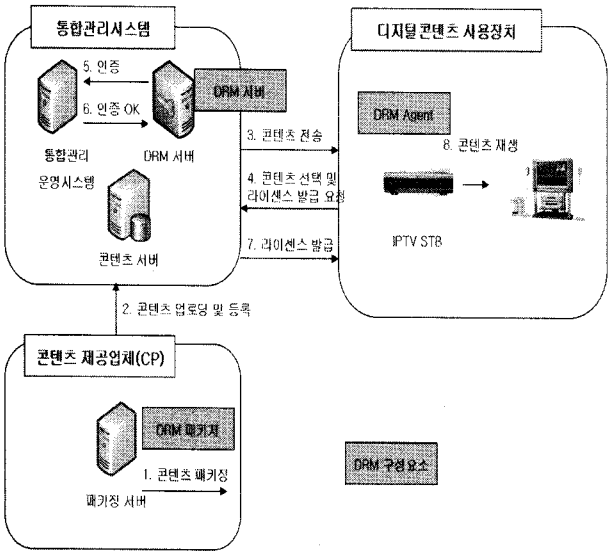


그림 2. DRM 솔루션 구성도

Fig. 2. The configuration diagram of the IPTV DRM solution

DRM은 암복호화 기술, 콘텐츠 사용권한, 그리고 사용자 인증을 이용하여 디지털 콘텐츠를 보호하는 방법이다. DRM 시스템은 콘텐츠 암호화를 수행하는 DRM 패키저(Packager: CAS 솔루션의 스크램블러와 비슷한 기능을 수행), 복호화키와 사용권한을 담고 있는 DRM 라이센스를 발급하는 DRM 서버(CAS의 EMM/ECM 생성기와 유사한 기능 수행), 그리고 DRM 서버에서 보내온 라이센스에 있는 복호키를 이용하여 콘텐츠 복호화를 수행하고 사용권한에 따라 콘텐츠 이용을 제어하는 사용자 기기에 설치되어 DRM 에이전트(Agent: CAS의 디스크램블러와 같은 기능 수행)로 이루어 진다. DRM 패키저는 통상 AES(Advanced Encryption Standard) 128 bit 암호화 알고리즘을 이용하여 디지털 콘텐츠를 암호화한다. 콘텐츠 소유자 혹은 콘텐츠 서비스 제공업체는 DRM 패키저를 이용하여 암호화된 콘텐츠를 사용자에게 제공한다. ITPV STB 장치의 고유정보를 이용한 사용자 인증을 거친 다음에 사용자의 지불 사실이 확인되면, DRM 라이센스(복호키와 콘텐츠 사용권한을 포함)를 암호화하여 사용자에게 전달한다. IPTV STB의 DRM 에이전트는 DRM 라이센스에 포함되어 있는 DRM 복호키를 추출하여 DRM 콘텐츠를 복호화하고 콘텐츠 사용권한에 따라 콘텐츠 사용을 제어한다. DRM 솔루션도 CAS와 마찬가지로 DRM 에이전트에서 복호화된 콘텐츠는 비암호화된 상태(clear content)로 STB의 아날로그 출력단자를 통해 LCD 모니터/TV 등의 화면출력장치로 전달되기 때문에, 이 출력단자를 통해 콘텐츠 복제가 가능하다.

이러한 CAS와 DRM 보안 솔루션의 허점을 보안하기 위해서 콘텐츠 사용자 정보를 재생화면에 삽입하는 포렌식 마킹(Forensic Marking) 기술이 IPTV 서비스 사업자의 많은 관심을 받고 있다.

III. 포렌식 마킹 솔루션

1. FM 솔루션 개요

디지털 포렌식 마킹 시스템은 그림 3과 같은 기능을 수행한다. FM 시스템은 크게 FM 인코딩 부문과 추출(detecting) 부문으로 나누어 진다.

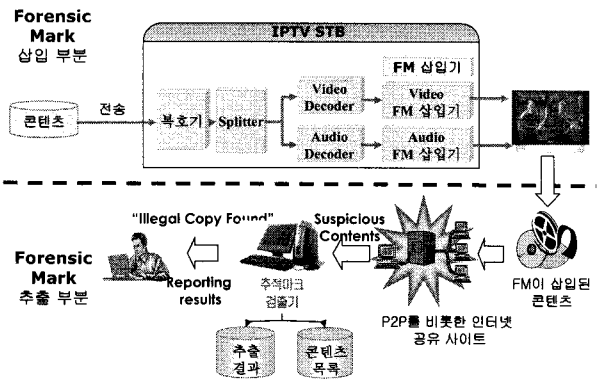


그림 3. FM 솔루션 구성도

Fig. 3. The configuration diagram of the DRM solution

FM 삽입부문의 핵심은 사용자 장치(PC, STB 등)에 설치되는 FM 삽입기로서 콘텐츠 재생 프로그램(미디어 플레이어)과 연동하여, 헤드엔드 장비에서 DRM 혹은 CAS 솔루션으로 보호된 콘텐츠를 복호화한 후 디코딩 과정을 거친 비디오와 오디오 스트림에 FM(Forensic Mark: 사용자 정보 등을 나타내는 워터마크 신호)를 추가하는 역할을 한다. FM 추출 부

문은 FM 인코딩 부문에서 들어간 사용자 정보가 삽입된 콘텐츠가 불법으로 획득되어 P2P 공유사이트에 유통되고 있는 콘텐츠를 추적마크 검출기로 처리하여 FM 정보를 추출하는 부문이다.

2. FM 구현 알고리즘

일반적으로 컴퓨터에서 사용하는 이미지 파일 또는 동영상 파일은 R(Red), G(Green), B(Blue)의 세가지 영역(domain)의 조합으로 색을 표현한다. 예를 들어 24비트 이미지는 세 영역마다 8비트의 정보를 지니므로 각각 0 에서 255 사이의 값을 지니게 된다. YUV 영역도 마찬가지로 색을 표현하는 방식으로서, 인간의 시각시스템 (HVS: Human Visual System)은 휘도 성분인 Y에 시각적으로 매우 민감하고, 색차 신호 UV에 둔감하므로 이 부분에 사용자 정보를 삽입하는데 많이 사용된다. RGB에서 YUV로의 변환 공식은 아래 (1)과 같다.

$$Y = 0.299R + 0.587G + 0.114B$$
$$U = -0.169R - 0.332G + 0.5B \quad (1)$$
$$V = 0.5R - 0.419G - 0.813B$$

그림 4는 샘플 동영상 "foreman.avi"의 U영역과 RGB 영역의 통계치를 비교한 자료이다.

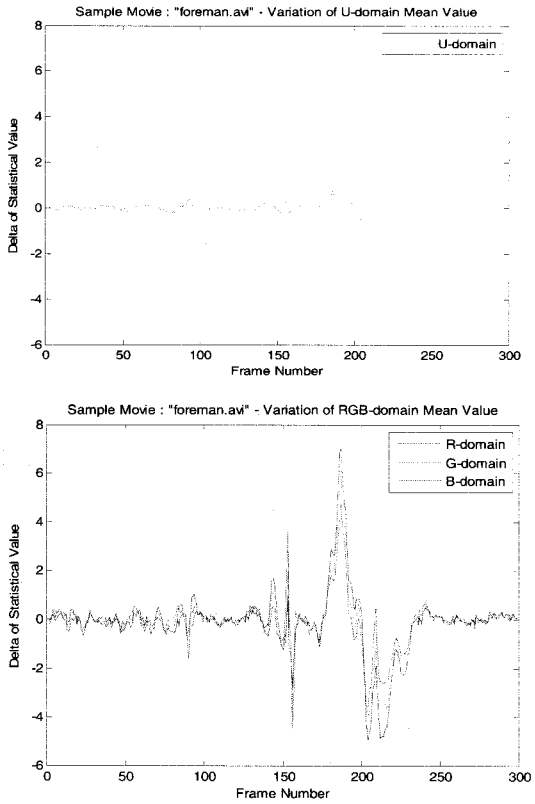


그림 4. U와 RGB 영역의 통계치 비교

Fig. 4. Comparison of Statistical Value of U and RGB domain

위 그림 4에서 샘플 동영상의 U 영역 통계치는 변동폭이 작은 반면, RGB 영역값의 변경폭은 상당히 크다는 것을 알 수 있다. 일반적으로 동영상의 U영역은 그 연속성에서 RGB영역보다 더 뛰어나고, 또한 같은 정도의 연속성을 가지고 있다고 해도 U 영역에 워터마크를 삽입하면 이로 인한 원본영상의 변화가 RGB 영역에 나뉘어서 적용되므로 비가시성 (Imperceptibility) 측면에서도 더 우수하므로 본 논문에서는 U 영역에 워터마크를 삽입하였다.

2.1 다중 사용자 FM 삽입(embedding) 알고리즘

본 논문에서 제안하는 FM삽입 알고리즘은 동영상의 이미지를 YUV로 변환하고 U혹은 V값 평균의 시간적인 차이를 워터마크 삽입에 이용한다.

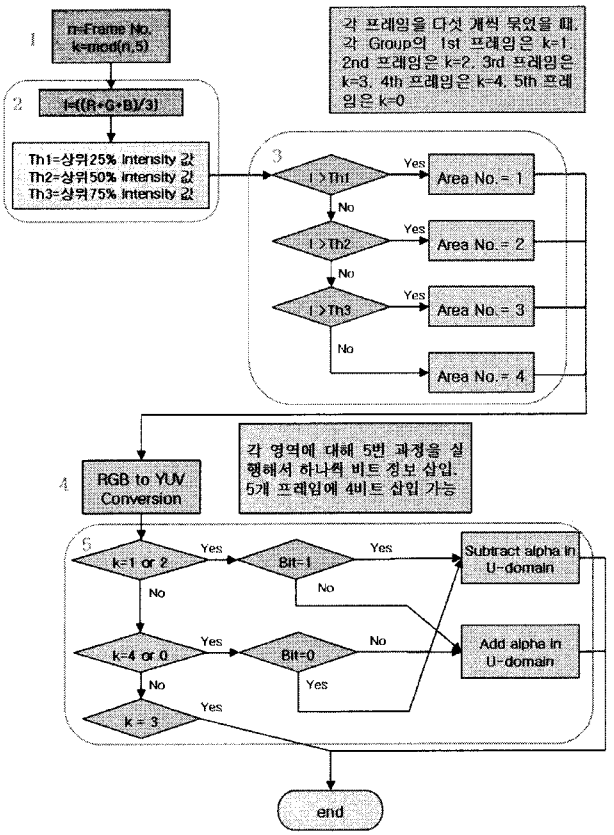


그림 5. 다중 사용자 FM 삽입 알고리즘 흐름도

Fig. 5. The flow chart of FM embedding algorithm for multiple users

위 그림 5는 다중 콘텐츠 사용자를 기록하기 위한 포렌식 마크 삽입 알고리즘 흐름도를 나타낸다. 원본 동영상의 프레임들을 배열 순서에 N(N>=5인 홀수)개의 프레임들을 하나의 그룹으로 나눈다. 그림에서는 N을 5로 택했을 경우를 예로 들었다. 프레임을 5개씩 그룹 지어서 프레임 번호에 따라 모듈로(modulo) 연산을 통해 그룹 내 번호(k)를 배정한 다음, 프레임을 YUV 영역으로 변환한 후 프레임의 각 픽셀들의 RGB 영역에서의 세기(Intensity)를 구해서 임계치(Threshold)를 구한다(2). 다음 수식 (2)는 세기를 구하는 공식이다.

$$\text{Intensity} = (R+G+B)/3 \quad (2)$$

세기(Intensity)의 임계치에 따라 프레임의 각 픽셀들을 4개의 영역으로 나눈다. 세기는 0~255의 값을 가지며 영역 분할의 기준이 된다(3). 프레임을 YUV 영역으로 변환하여 U 영역에 워터마크 삽입한다(4). 해당 영역에 삽입하려는 비트 정보 및 그룹 내 번호(k)에 따라 U 영역 전체에 특정한 상수값

(alpha)을 더하거나 빼는 방법을 통해 각 그룹 내에서 시간에 따른 U영역 통계값의 변화가 일정한 경향을 보이도록 하는 방식으로 워터마크를 삽입한다. N이 5일 경우에, 삽입하고자 하는 bit 값이 1일 때는 k=1, 2번 프레임의 U영역값에다 상수값을 빼고 4, 5번 프레임에는 상수값을 더해서 5개 프레임내에서U 영역 통계값이 점점 커지는 경향을 보이도록 한다. 비트 정보가 0일 때는 반대 과정으로 U영역 통계값이 점점 작아지는 경향을 보이도록 하여 사용자 정보를 인코딩 한다.

2.2 다중 사용자 FM 추출(detection) 알고리즘

FM 추출은 콘텐츠에 삽입되어 있는 정보를 추출하는 과정으로 그림 6과 같다. FM 삽입과정에서와 같이 먼저 프레임을 5개씩 묶어서 프레임 번호에 따라 그룹내 번호를 지정한다(1). 다음 프레임의 각 픽셀들의 RGB영역에서의 세기(Intensity)를 식 (2)에 따라 구한 다음(2)에 임계치(Threshold)에 따라 프레임의 픽셀들을 4개의 영역으로 나눈다(3). 프레임을 YUV 영역으로 변환한다(4).

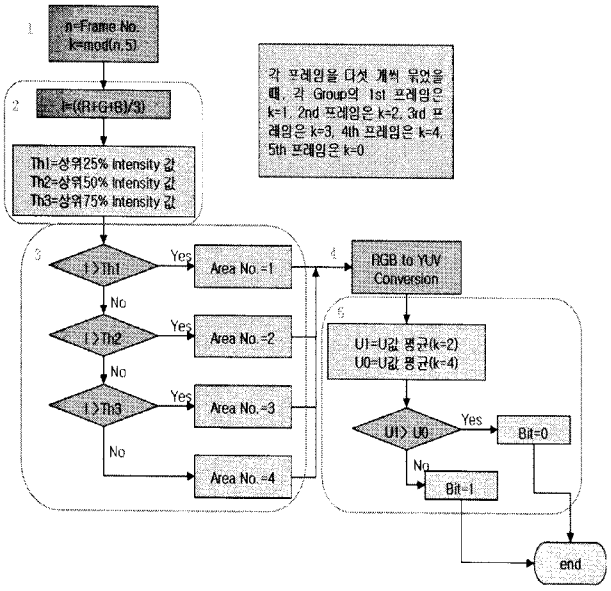


그림 6. 다중 사용자 FM 추출 알고리즘 흐름도
Fig. 6. The flow chart of FM detecting algorithm for multiple users

프레임의 그룹내의 2번, 4번 프레임의 U영역 통계값을 비교함으로써 그룹내의 U영역 통계치 경향을 비교하여 U값이 3번 프레임을 중심으로 증가하면 bit 1이 삽입되어 있는 것으로 판단하고, 감소하면 bit 0가 삽입되어 있는 것으로 판단한다(5).

IV. 포렌식 마킹 솔루션 성능 평가

1. FM 공격 종류 및 실행방법

표1은 사용자 정보를 담고 있는 포렌식 마크에 가해질 수 있는 공격의 종류와 세부사항을 보여준다.

표 1. FM 공격종류 및 시험방법
Table 1. FM attacks and their testing methods

종류		세부 내용
DA/AD 변환		디지털 영상에 대해 아날로그로 변환한 후 다시 디지털화 하였을 경우 FM 검출 여부를 시험하는 것으로 DAC/ADC (Digital to Analog Conversion)을 2회 이상 하여 검출 수행.
Recompression		아날로그 출력 포트에서 캡처한 영상을 MPEG2/4, H.264, DivX 코덱으로 재 압축하여 FM 강인성 시험.
Geometric Transform	Rotation	2°, 5° 회전 후 FM 검출시험
	Resizing	● 횡축: <1/2 종축: < 1/2 Letterbox, aspect ratio 변화 등이 해당 ● 원본 대비 50%, 150%로 크기 변경 후 FM 검출시험
	Cropping	● 저작권 추적 정보가 삽입된 원영상에서 ROI(관심영역, Region of Interest)를 포함하는 임의의 크기를 Cropping 하였을 경우 FM 추출 시험 ● Cropping: ROI x 0.9 수행 ● 본 영상의 8%를 삭제 후 FM 검출 시험
Filtering		여러 종류의 필터링(Low pass, Median, Wiener etc)을 사용하는 추적마크 제거 공격과 Gaussian Noise를 사용하는 잡음 첨가 공격을 DirectShow Translation Filter로 수행
Digital Capturing		컴퓨터 영상파일 캡처 프로그램을 이용한 FM 검출 시험

2. FM 성능 평가 결과

아래 표 2 는 4 개의 동영상에 대한 PSNR(Peak signal-to-noise ratio)이 39dB 과 41dB 인 경우의 실험결과이다. 통상 비디오 압축의 경우에 PSNR 값은 30~50dB 이며, 값이 높을 수록 품질이 좋을 것을 나타낸다. 본 시험에 사용한 39dB 의 경우에는 41dB 에 비해 FM 삽입강도가 비교적 강한 것을 의미하며, 재생 되는 프레임의 U 값을 크게 변화시켰음을 의미한다. 결과치는 입력 문자로 "KTCINEMA" 8 글자를 4 개의 영역(그림 5 의 삽입 알고리즘에서 분류한 Th1, Th2, Th3, Th4 으로 나누어진 4 개의 영역)에 각각 2 개 문자씩 삽입했을 경우 검출되는 글자수를 나타낸다. 필터링(Filtering)의 Gauss R1, R2 은 각각 반지름(Radius)이 1 과 2 인 Gaussian Low Pass Filter 로 디지털 필터링 공격을 실행하였음을 나타낸다.

표 2의 결과치를 살펴보면 Highway 동영상을 제외하고서는 모든 FM 공격에서 삽입강도가 39dB/41dB인 경우에 8개

의 삽입 문자에 대해 8개의 문자가 정확히 검출되었다. Highway 영상을 D/A, A/D Conversion시에는 삽입강도가 39dB일 경우에는 입력 8글자가 검출시 모두 검출(8/8)되었으나, 41dB의 경우에는 올바른 검출(0/8)이 이루어 지지 않음을 볼 수 있었는데, 이는 시험영상의 색감 자체가 FM의 삽입 전 후의 차이가 캠코더(camcorder)가 인지할 수 있을 만큼 크지 못했음을 나타낸다.

표 2. FM 강인성 시험 결과 (PSNR: 39dB/*41dB)
Table 2. FM robustness test result against FM attacks (PSNR: 39dB/41dB)

공격 유형		시험동영상 (검출 문자수/삽입 문자수)			
		Boat	Foreman	Highway	News
DA/AD 변환		8/8	8/8	8/8(*0/8)	8/8
Recompression	MPEG4	8/8	8/8	8/8	8/8
	H.264	8/8	8/8	8/8	8/8
	Xvid	8/8	8/8	8/8	8/8
Geometric Transform	Rotation 2°	8/8	8/8	8/8	8/8
	Rotation 5°	8/8	8/8	8/8	8/8
	Resizing 50%	8/8	8/8	8/8	8/8
	Resizing 150%	8/8	8/8	8/8	8/8
	Cropping 8%	8/8	8/8	8/8	8/8
Filtering	Guass R1	8/8	8/8	8/8	8/8
	Gauss R2	8/8	8/8	8/8	8/8
Digital Capturing		8/8	8/8	8/8	8/8

V. 결론

본고에서는 IPTV의 콘텐츠 보호솔루션인 CAS, DRM의 허점과, 이를 보완하기 위한 FM 솔루션에 대해 설명하였다. 최대 4인까지의 공모 공격 (collusion attack)에 대비하여 각 프레임을 세기(Intensity) 크기에 따라 4개의 영역으로 나누고, 각 영역에 포렌식 마크 정보를 삽입하는 FM 솔루션을 제시하였다. 각 영역에 정보를 삽입하기 위하여 프레임을 일정 홀수개의 그룹으로 나누고, 삽입하고자 하는 정보값이 '1' 경우에는 각 그룹안에 속한 프레임의 U값이 중심 프레임을 기준으로 증가하도록 하고, '0'일 경우에는 감소하도록 U값을 변경하였다.

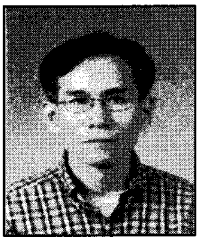
본 논문에서 다중 불법복제자 추적 FM 솔루션은 주파수 영역에서의 삽입방식보다 계산과 검출이 간단하고, 다양한 FM 공격에도 강인하여 IPTV STB 등에서도 구현 가능한 장점을 지니고 있다. ■

VI. 참고문헌

[1] *LLC member representative committee*, "Digital Cinema System specification v1.0", July 20, 2005

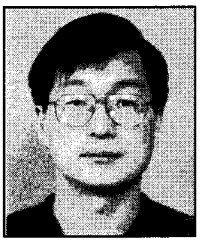
[2] 김종안 외 2인, "디지털 추적표시(Forensic Marking) 시스템 개발" , 2007년 정보통신설비 학술대회, pp. 142~146, 2007년8월

[3] 김종안 외 2인, "디지털미디어 서비스플랫폼 콘텐츠의 불법 유출 추적시스템 개발" , 한국통신학회 KNOM 2008 Conference, pp. 2008년4월.



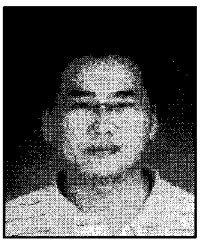
김 종 안

1984년 고려대학교 전기공학과 졸업.
1988년 고려대학교 대학원 전자공학과 (공학석사)
1988년 ~ 현재 KT 플랫폼연구소 수석연구원, 관심분야는 DRM, 워터마킹(핑거프린팅, Forensic Marking), CAS 등임.



김 진 한

1986년 고려대학교 전자공학과 졸업
1988년 한국과학기술원 전기및전자공학과(공학석사)
1992년 한국과학기술원 전기및전자공(공학박사)
1992년 ~ 현재 KT 플랫폼연구소 수석연구원, 관심분야는 DRM, IPTV, 미디어 공통플랫폼, On-Demand 서비스, 디지털컨텐츠, WiBro 등임.



김 종 흠

1999년 포항공과대학교 전자전기공학과 졸업
2001년 포항공과대학교 전기전자공학과(공학석사)
2004년 ~ 현재 KT 플랫폼연구소 전임연구원, 관심분야는 DRM, CAS, 암호화 알고리즘 등임.