Proceedings of IT Facilities Engineering Conference, August 24-25, 2007

디지털 추적표시(For ensic Marking) 시스템 개발

Implementation of commercial digital Forensic Marking systems

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

Abstract : Digital Rights Management (DRM) technology has been widely used for protecting the digital contents over the recent years. But the digital contents protected by DRM are vulnerable to various video memory capture programs when DRM packaged contents are decrypted on the consumers' multimedia devices. To make up for this kind of DRM security holes the Forensic Marking (FM) technology is being deployed into the content protection area. Most leading DRM companies as well as big electronics companies like Thomson and Philips already have commercial FM solutions. Forensic Marking technology uses the digital watermarking to insert the user information such as user id, content playing time and etc. into the decrypted and decoded content at the playback time on the consumer devices. When the content containing watermarked user information (Forensic Mark) is illegally captured and distributed over the Internet, the FM detection system takes out the inserted FM from the illegal contents and informs contents service providers of the illegal hacker's information. In this paper the requirements and test conditions are discussed for the commercial Forensic Marking systems.

Keywords: FM (Forensic Marking), Digital Fingerprinting, DRM (Digital Rights Management), Digital Cinema

I. 서론

인터넷 접속 속도의 고속화와 멀티미디어 PC의 발달로 디지털 콘텐츠의 이용도가 나날이 높아져 가는 추세이다. 디지털 콘텐츠는 복사 후에도 원본과 동일한 품질을 유지하고, 복제 비용도 거의 들지 않기 때문에 디지털 콘텐츠 보호는 콘텐츠 소유자와 서비스 제공자(SP)에게 가장 중요한 사안 중 하나일 것이다. 현재 디지털 콘텐츠의 보호에 널리 사용되는 DRM(Digital Rights Management) 기술은 DRM으로 패키징된 디지털 파일이 사용자 기기에서 복호되는 시점에 해킹을 당할 수 있는 위험이 있다. 디지털 콘텐츠 중에서 가장 고가의 콘텐츠는 디지털시네마 영화관에서 상영되는 개봉영화일 것이다. 디지털 시네마 표준 규격을 제정하고 관리하고 있는 DCI(Digital Cinema Initiative)에서는 이러한 DRM의 문제점을 알고 있기 때문에, 이를 보완하기 위해서 Forensic Marking(추적표시) 기술을 디지털 시네마 서버에 탑재하도록 의무화 하였다.[1] 추적표시 기술은 디지털 파일을 재생하는 최종단의 재생기기 및 사용자에 관한 정보를 워터마킹 기술을 이용하여 실시간으로 재생되는 콘텐츠에 삽입하는 기술을 말한다.

본 논문에서는 DRM 기술과 워터마킹 기술에 대해서 설명하고, 워터마킹 기술 중 Forensic Marking의 상용화 기술, 상용시스템 구성요소 및 요구조건에 대해서 자세히 다루고자 한다.

1.1 DRM 솔루션과 보안 허점

DRM은 암복호화, 라이센스, 그리고 사용자 인증을 이용하여 디지털 콘텐츠를 보호하는 방법이다. DRM 솔루션은 콘텐츠 암호화를 수행하는 DRM 패키저(Packager), 복호화키와 사용권한을 담고 있는 DRM 라이센스를 발급하는 라이센스 발급 서버, 그리고 사용자 기기에 설치되어 라이센스 서버에서 보내온 라이센스에 있는 복호키를 이용하여 콘텐츠 복호화를 수행하고 사용권한에 따라 콘텐츠 이용을 제어해 하는 DRM 에이전트(Agent)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. 콘텐츠 이용자가 DRM으로 암호화된 콘텐츠를 이용하기 위해서는 지불을 해야 하며, 서비스 제공업자는 사용자 장치의 고유정보를 이용한 사용자 인증을 거친 다음에 사용자의 지불 사실이 확인되면, DRM 라이센스(복호키와 콘텐츠 사용권한을 포함)를 암호화하여 사용자에게 전달한다. 사용자 기기단에는 DRM Agent라는 프로그램이 설치되어 동작하는데, DRM 에이전트는 DRM 라이센스에 포함되어 있는 DRM 복호키를 추출하여 DRM 콘텐츠를 복호화하고 콘텐츠 사용권한에 따라 콘텐츠 사용을 제어한다. DRM 에이전트는 사용자 단말기내부에서 동작하는 미디어플레이어(Windows Media 플레이어 등)와 연계하여 콘텐츠 보호를 수행한다. DRM 에이전트가 DRM 라이센스서버에서 받은 복호키를 이용하여 DRM 파일을 복호화하는 순간에는 암호화하기 전의 원본 콘텐츠가 풀려서 비디오 메모리 등의 메모리에 존재하게 되는데, 각종 해킹 프로그램이 이 원본 콘텐츠를 추출하여 재 인코딩하여 파일로서 컴퓨터에 저장하게 된다. 원본콘텐츠와는 코딩 방식은 다르지만 유사한 품질의 복사본 콘텐츠가 탄생하게 되는 것이다. 즉 DRM Agent가 설치되어 있는 단말기가 콘텐츠를 재생하는 시점이 DRM 보안 허점이 되는 것이다. 이러한 DRM 보안 허점을 보안하기 위해 미국 6대 주요 헐리우드 영화제작사들이 만든 DCI(Digital Cinema Initiative)가 디지털 시네마 콘텐츠의 보호에 Forensic Marking 기술을 채택하는 것을 의무화함으로써 Forensic Marking 기술이 최근 DRM 및 콘텐츠 보안 업체의 관심을 끌고 있다.

그림 1은 디지털시네마 시스템에서 DRM이 적용된 디지털 시네마 파일이 복호화되고, Forensic Mark가 삽입과정이 일어

* 책임저자(Corresponding Author)
논문접수 : 2007.7.21, 채택확정 : 2007.7.31
김종안*, 김진한, 김종흠 : KT 미래기술연구소*, KT BcN본부
(joankim@kt.co.kr, jinhan@kt.co.kr, jinah0719@kt.co.kr)

나는 디지털 시네마 서버 내부 구조도를 보여준다. 시네마 미디어 서버 내부에 있는 저장소(local storage)에는 DRM으로 암호화된 디지털 시네마 파일이 저장되어 있다. 영화상영을 위해 시네마 플레이어가 DRM 모듈을 호출하면, DRM 모듈은 라이센스 내부에 있는 복호키를 추출하여 DRM 파일을 복호화한다. 복호화된 콘텐츠 스트림을 비디오 메모리에 보내면 비디오 메모리 부문을 캡처(capture)하여 저장하는 각종 캡처 프로그램에 의하여 콘텐츠가 누출되기 때문에, 복호화된 콘텐츠는 바로 Forensic Marking 삽입모듈을 통과 하도록 구현되어 있다. FM 삽입 모듈은 실시간으로 시네마 미디어 서버 기기번호, 재생시각 등의 정보를 추가한다. 디지털 시네마 서버에 장착되는 FM 모듈은 하드웨어 (FPGA: Field Programmable Gate Array)로 구현되어 있다.

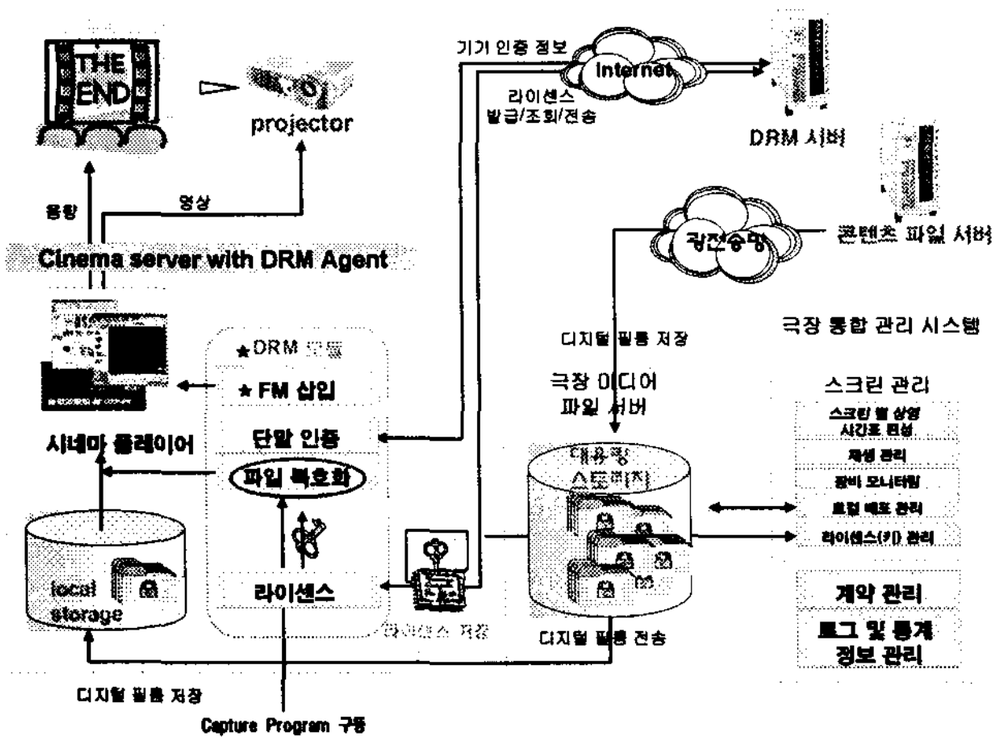


그림 1. 디지털시네마 서버의 DRM 모듈과 FM 적용도

1.2 디지털 워터마킹 기술

디지털 워터마킹 기술은 표 1과 같이 여러 가지 기준에 따라 분류될 수 있으며, 그 특성에 따라 여러 용도로 사용될 수 있다.[2)3)]

표 1. 디지털 워터마킹의 용도에 따른 분류

분류기준	방 식	비 고
워터마크 인지가능 여부	Perceptible 워터마킹	대부분 fragile 워터마킹(로고 등)에 해당
	Imperceptible 워터마킹	강인성 제공 위한 조건
강인성 제공여부	Robust 워터마킹	저작권 보호 제공
	Fragile 워터마킹	인증 / 무결성 제공
키 공개 유무	Private 워터마킹	삽입/추출시 사용된 키가 보안 필요
	Public 워터마킹	삽입/추출시 사용된 키가 공개 가능
검출 방식	Nonblind 워터마킹	검출시 원본 필요
	Blind 워터마킹	검출시 원본 불필요
워터마크의 삽입 영역	공간 영역	신호처리에 약한 특성
	주파수 영역	인간의 시각특성 고려

1.3 핑거프린팅 기술과 Forensic Marking 기술

핑거프린팅(fingerprinting) 기술은 디지털 워터마킹 기술을 이용하여 콘텐츠 소유자의 정보와 구매자의 정보도 포함하는 핑거프린팅 정보를 콘텐츠에 삽입하여 불법배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 기술이다.[2)] 핑거프린팅 기술은 콘텐츠 사용자 등의 정보를 원본 콘텐츠에 콘텐츠 제공자 측에서 구매자 정보까지 넣어 배포할 수도 있고, 사용자 단말기에서 콘텐츠 재생시점에 넣도록 할 수 있는데 후자의 방식을 DCI에서는 Forensic Marking 기술로 명명하였다. 따라서 본 논문에서는 콘텐츠 제공업자 측에서 워터마크화 된 사용자 정보를 미리 넣어서 콘텐츠를 배포하는 기술을 핑거프린팅 기술로, 사용자 기기측에서 워터마킹 기술을 이용하여 사용자 정보 등을 넣는 기술을 Forensic Marking 기술로 정의하였다. 핑거프린팅 기술은 현재 KBS 등 방송사업자가 자사의 콘텐츠가 불법으로 방영되지 않은가를 조사하는데 사용되고 있으며, 구매자의 정보까지 실시간으로 삽입하여 콘텐츠를 배포하는 비즈니스 모델은 현실적으로 어려워 보인다. 이에 비해 Forensic Marking 기술은 콘텐츠 구매자 장비의 자원을 이용하기 때문에 사용자 정보를 원본콘텐츠에 삽입할 수 있으나, 사용자의 동의가 필수적이며 사용자에게 FM(Forensic Mark) 삽입 과정이 노출되어 있기 때문에 이에 대한 보안이 핑거프린팅에 비해 더욱 필요하다.

II. 디지털 Forensic Marking 시스템

디지털 Forensic Marking을 상용화하기 위해서 필요한 시스템의 요구사항, 성능시험, 알고리즘에 대하여 다루고자 한다.

2.1 디지털 Forensic Marking 시스템 흐름도

디지털 포렌식 마킹 시스템은 그림 2와 같은 기능을 수행한다. FM 시스템은 크게 FM 인코딩 부문과 추출(detecting) 부문으로 나누어 진다. FM 인코딩은 사용자 장치(PC 등)의 콘텐츠 재생 프로그램과 연동하여 내부에서 동작하며 동영상인 경우에는 비디오와 오디오 스트림 후단에 FM 삽입기가 연결되어 FM(Forensic Mark: 사용자 정보 등을 나타내는 워터마크 신호)을 콘텐츠에 추가한다. FM이 추가된 신호를 STB 이나 오디오 장치로 송출하는 부문이다.

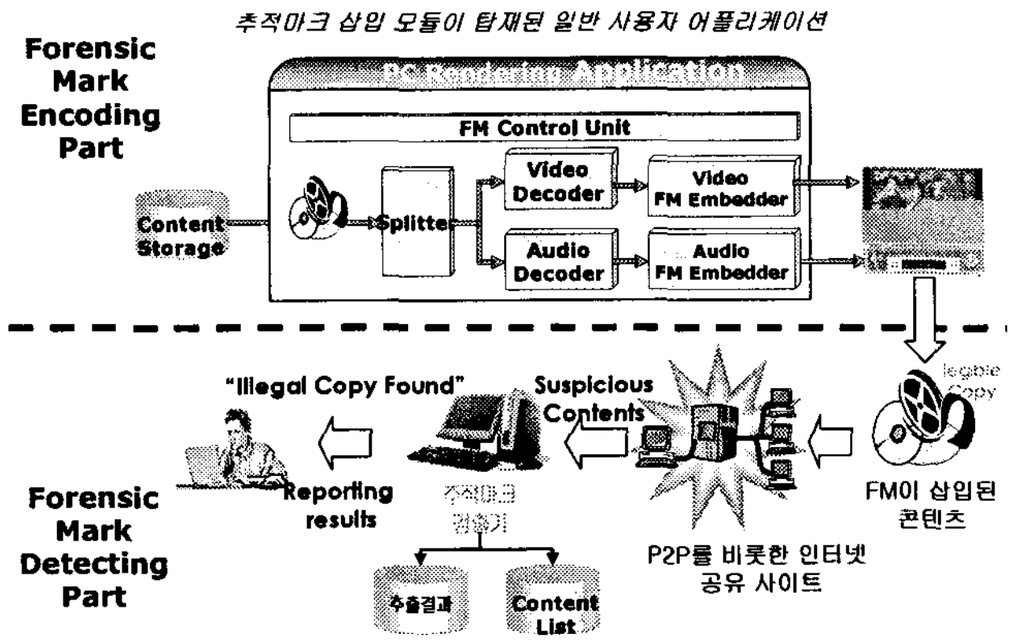


그림 2. 디지털시네마 Forensic Marking 시스템 흐름도

FM 추출 부문은 STB 이나 오디오 장치에서 불법 콘텐츠

를 생성하여 P2P 공유사이트에 유통되는 콘텐츠를 추적마크 검출기로 처리하여 FM 정보를 추출하는 부문이다.

2.2 디지털 Forensic Marking 시스템의 성능 규격

그림 2에서와 같이 디지털 FM 시스템은 Encoding과 Decoding 모듈로 이루어져 있다. 표 2는 포렌식 마킹 삽입(Encoding) 성능 규격을 표 3과 4는 비디오/오디오 추출(Decoding) 시스템 성능 및 요구 규격을 각각 나타낸다.

표 2. 추적마크 삽입 시스템의 요구사항

요구항목	세부 내용
일반 규격	● 장치 식별자 또는 사용자 식별자 삽입 가능 ● 사용자 정보는 64bits ~ 128bits 이내 ● 저작권 추적 정보는 실시간으로 삽입 가능
시간 정보	● 콘텐츠의 상대적인 시간 또는 GMT 기준 등 절대 시간 삽입 가능 ● 콘텐츠 SP 서버로부터 전송 받은 시간 정보 삽입 가능
FM 삽입 구간	● WMS(Watermark Minimum Segment)는 최대 3분 이하로 결정. 즉 3분 이내에 식별자 및 시간 정보가 1회 이상 삽입 ● 추출기에서 3분 단위의 클립에서 한번 이상의 식별자와 시간정보가 추출 가능
비인지성 (Imperceptibility)	● 비디오 영상에 대해 저작권 추적 정보 삽입 후 시각적으로 인지 불가. ● 오디오 데이터에 대해 저작권 추적 정보 삽입 후 청각적으로 인지 불가
확장성 (Scalability)	Forensic Mark의 변경이나 삽입 가능
Multiple Layer 지원	다수의 구매자 정보 삽입 가능
Codec 비종속성	● 오디오/비디오 코덱에 비 종속적으로 저작권 추적 정보 삽입 가능 ● MPEG-2, H.264 등의 코덱에 독립적으로 동작
저작권 추적 정보 삽입 스위칭 기능	● 필요에 따라 저작권 정보를 삽입하지 않도록 저작권 추적 삽입 모듈을 On/Off 할 수 있는 기능 구현 ● 즉 DRM으로 보호되지 않은 사용자 Self-Made 콘텐츠나 다른 보호되지 않은 콘텐츠에는 저작권 추적 정보를 삽입하지 않는 수단 제공 ● 저작권 추적 정보가 삽입되지 않을 경우 바이패스 기능 제공
강인성 (Robustness)	다양한 신호처리와 기하학적 변형에도 워터마크의 검출 가능

표 3. 비디오 FM 추출 시스템 요구사항

요구항목	세부 내용
Payload 크기	64bits/1.0 minutes
강인성	● Recompression to MPEG-2, MPEG-4, H.264, DiVX, WMV etc. ● Shifting, cropping, scaling ● Noise addition, D/A conversion, noise filtering, median filtering
비실시간 추출	FM 추출은 비실시간 처리가 가능하다.

표 4. 오디오 FM 추출 시스템 요구사항

요구항목	세부 내용
Payload 크기	32 bits/30 seconds
강인성	● D/A and A/D conversion ● MP3, AAC, WMA encoding/decoding ● All-pass/band-pass filtering ● Echo addition ● Amplitude compression ● Re-sampling, Speed change, Noise addition

2.3 비디오 FM 삽입/추출 알고리즘

그림 3은 비디오 추적마크 시스템의 근간을 이루고 있는 삽입/추출 알고리즘을 보여준다. 좌측은 삽입 알고리즘을 우측은 비디오 추적마크 추출 알고리즘을 나타낸다.

2.3.1 비디오 FM 삽입 알고리즘 구성

ROI Selection: ROI Selection 부는 비디오 데이터의 특성상 프레임의 모든 데이터에 정보를 삽입하는 것은 시스템 리소스가 충분히 확보되지 않는 이상 현실적으로 어렵기 때문에 입력되는 전체 프레임 영상으로부터 정보가 삽입될 부분 영상을 추출하는 기능을 수행한다. 입력되는 영상 크기에 따라 추출되는 Sub-Image(KT FM 개발 시스템은 160*120 크기를 사용)를 결정한다.

Feature Calculation: 인간의 시각 특성이 복잡한 영상(Texture Image)에 대해서 변화에 둔감하고 Monotone 영상에 대해서는 변화에 민감할 뿐만 아니라 색이나 휘도에 대해서도 각 대역마다 인간의 시각적인 특성이 다르게 인지되기 때문에 이를 반영하여 인간의 시각에 민감하지 않은 영역에 워터마크를 강하게 삽입할 수 있도록 필터링을 통해 각 픽셀 단위로 스케일링 계수를 확보하는 기능을 수행한다.

SRNG(Pseudo-Random Number Generator): 워터마크를 구성에 사용될 랜덤 넘버를 생성하는 기능을 수행한다.

Sync Mark Generation: 저작권 추적 정보가 콘텐츠 내에 삽입된 후 영상의 회전, 이동, 축소 및 확대 등의 다양한 환경에 노출될 수 있기 때문에 이런 환경으로부터 저작권 추적 정보를 추출하기 위해서 영상을 원래의 형태로 복원을 해야 한다. Sync Mark Generation 부는 영상을 복원할 수 있는 동기화 정보를 생성한다.

Message Encoding: 저작권 추적 정보를 구성하는 기능을 수행한다. 장치 또는 사용자 식별자와 시간 정보를 조합하여 저작권 추적 정보를 구성하고 그 구성된 정보를 추출 단에서 에러 여부를 판정하고 에러가 발생하였을 경우 이를 정정할 수 있도록 한다. 에러 추출 코드는 CRC(Cyclic Redundancy Check)를 사용하고 에러 정정 코드는 Turbo 코드를 사용한

다.

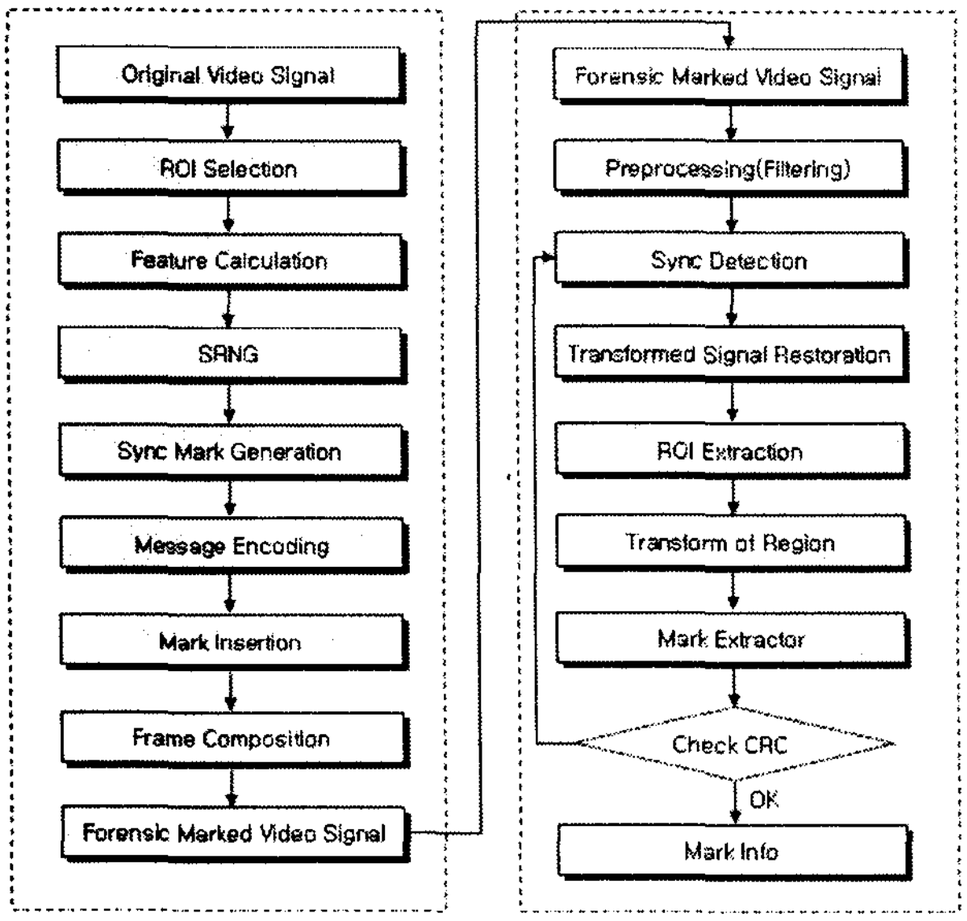


그림 3. 비디오 추적마크 삽입/추출 알고리즘 흐름도

Mark Insertion: 생성된 워터마크를 선택된 영역의 데이터에 삽입하는 기능을 수행한다.

Frame Composition: 저작권 추적 정보가 삽입되어 원본 데이터가 변경된 ROI Selection 부에서 선택된 영상과 선택되지 않은 영역의 영상을 재조합하는 기능을 수행한다.

2.3.2 비디오 FM 추출 알고리즘 구성

다음은 비디오 추적마크 추출 알고리즘의 블록에 관한 설명이다.

Preprocessing(Filtering): 영상 성분을 제거하고 워터마크 성분을 예측하는 기능을 수행한다.

Sync Detection: 저작권 추적 삽입 시스템에서 삽입된 동기화 정보를 토대로 워터마킹 채널에서 변형된 영상에 대한 복원하는 기능을 수행한다. 복원 과정에서 기하학적인 변형에 대한 매개변수들을 추출하여 Geometric Restoration 부에 전달한다.

Transformed Signal Restoration: Sync Detection 부에서 생성한 Sync 정보를 기반으로 영상에 대한 복원 작업을 수행한다.

ROI Extraction: 복원된 영상으로부터 저작권 추적 정보가 삽입되어 있는 영역을 추출하는 기능을 수행한다. 변형된 영상에 대한 정보가 복원이 되어야만 저작권 추적 삽입 시스템에서 삽입이 된 영역을 파악할 수 있기 때문에 변형이 복원 후에 ROI 를 추출하는 단계를 위치시킨다.

Transform of Region: 저작권 추적 정보를 생성하는 영역이 Transform 영역이었다면 이를 추출하기 위한 영역도 Transform 영역이어야 하므로 저작권 추적 정보를 추출하기 위해 Transform 을 수행한다.

Mark Extractor: 저작권 추적 정보 삽입 알고리즘이 사용했던 영역을 판별하고 추출된 영역으로부터 정보를 추출하는 기능을 수행한다.

Error Correction: 추출된 정보의 에러 수정 및 정확성 판단을 한다. 구성은 먼저 에러 정정을 수행하고 그 다음 에러 검출 과정을 수행한다.

2.4 오디오 FM 삽입/추출 알고리즘

그림 4 는 오디오 추적마크 삽입/추출 알고리즘 흐름도를 나타낸다.

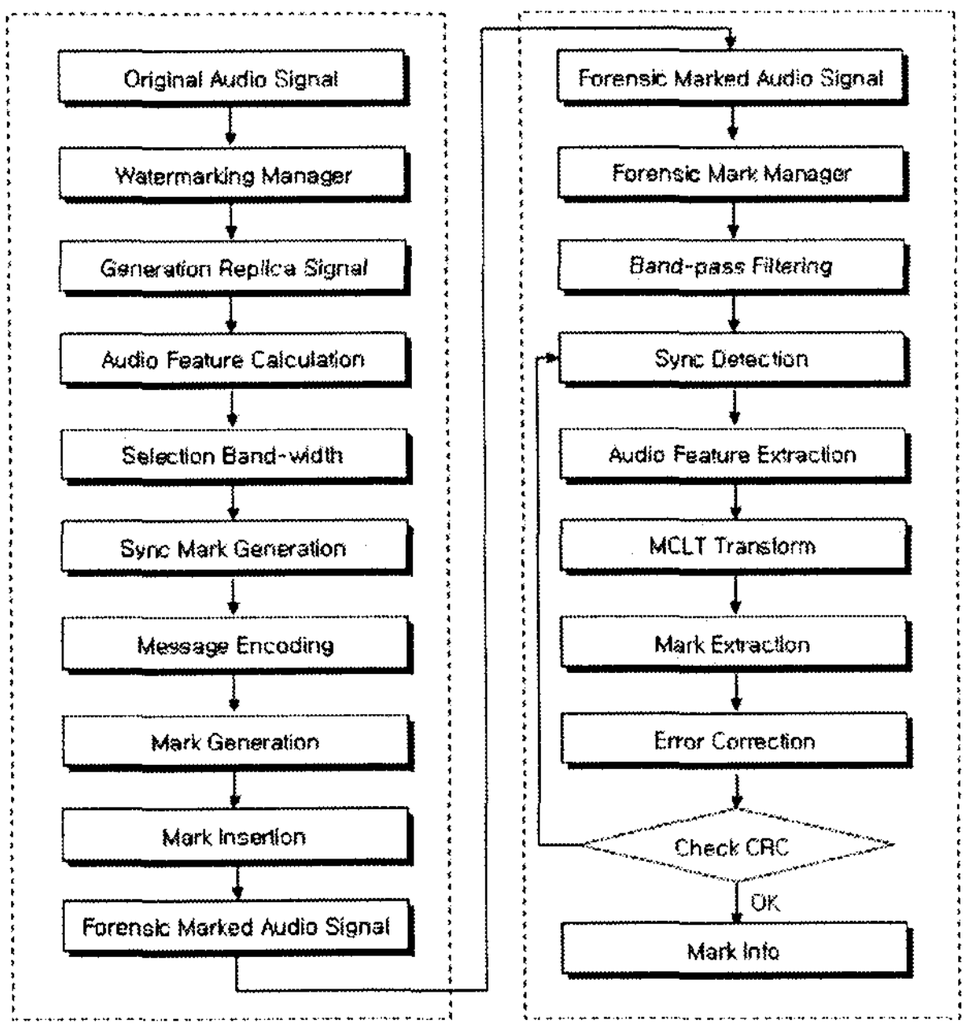


그림 4. 오디오 추적마크 삽입/추출 알고리즘 흐름도

비디오 추적마크 알고리즘과 거의 유사하며 그 차 이점은 아래와 같다.

2.4.1 비디오 FM 삽입 알고리즘 구성

Generation Replica Signal: 오디오 신호에 저작권 정보를 삽입하기 위해서 오디오 신호 중에서 가장 외부 공격에 강인한 영역의 주파수 성분만을 추출을 한다. 이렇게 추출된 신호는 원본 오디오 신호와 거의 유사한 특징을 갖고 있으며 오디오 신호 전체에 워터마크 신호를 삽입하지 않으므로 음원의 훼손을 최소화할 수 있는 이점이 있다.

Audio Feature Calculation: 입력된 오디오 신호의 특성값을 구하여 양자화시킬 때 최적의 삽입 강도를 결정하는 데에 도움을 준다.

Selection Band-width: 비디오의 ROI 에 해당되며, Generation Replica Signal 부에서 생성된 Replica 중에서 현재 오디오 신호에 가장 적합한 Frequency 영역을 결정한다.

2.4.2 오디오 FM 추출 알고리즘 구성

Forensic Mark Manager: 저작권 추적 검출 시스템을 전체적으로 제어하는 기능을 수행하며, 저작권 추적 삽입 시스템에서 사용했던 비밀키, 단위 프레임 사이즈 정보 등의 Parameter 들을 가지고 있다.

Band-pass: 입력된 오디오 신호에서 워터마크 삽입에 사용된 주파수 영역의 신호만을 추출하여 외부의 노이즈 등의 신호들을 배제시킨다.

Sync Detection: 비디오와 달리 오디오의 신호는 워터마크를 삽입하는 단위 신호 길이를 설정을 하고, 오디오 스트림에서 워터마크를 삽입하기 시작한 위치를 판별한다.

Audio Feature Extraction: 워터마크의 기본 정보를 세부 시간 단위로 쉬프트하면서 오디오 특성값을 추출한다. 여기서 추출된 오디오 특성값을 양자화하여 향후에 워터마크 정보를 검출하게 된다.

MCLT(modulated complex lapped transform) 변환: 오디오 신호에 Time Scaling 또는 Pitch Shift가 발생한 경우에 오디오 프레임의 동기화를 재조정하기 위한 정보를 검출한다.

2.5 FM 삽입/추출 시스템 성능평가

포렌식 마킹 삽입/추출 시스템의 성능은 FM 삽입 후에 영상이미지의 손상 정도와 FM 이 각종 공격 후에 얼마나 정확히 검출되는 가로 판단할 수 있다. 이 중 FM 비인지성은 현재 정량화하기 어렵기 때문에, 성능 평가는 FM 공격에 대한 강인성으로 평가된다. FM 공격의 종류는 표5에 나타난다.

표 5 . FM 공격 종류

종류	세부 내용
Compression	녹화된 영상에 대한 압축 공격에 대해 강인성을 가져야 한다
Noise Addition	● 사용자의 녹화과정에서 발생할 수 있는 Noise에 대해 강인성을 가져야 한다. ● PSNR > 28dB
DAC/ADC	● 원영상의 디지털 영상에 대해 아날로그로 변환한 후 다시 디지털화 하였을 경우 저작권 정보를 검출 할 수 있어야 한다. ● DAC/ADC(Digital to Analog Conversion) 변환 2회 이상에서 검출이 이루어져야 한다.
Resizing	● 횡축: <1/2, 종축: < 1/2 ● Letterbox, aspect ratio 변화 등이 해당
Cropping	● 저작권 추적 정보가 삽입된 원영상에서 ROI를 포함하는 임의의 크기를 Cropping 하였을 경우 저작권 추적 정보가 검출 되어야 한다. ● Cropping: ROI x (1/2 x 1/2)

III. 결론

본 논문에서는 DRM, 워터마킹, 핑거프린팅, Forensic Marking 기술에 대한 차이점과 상관관계에 대해서 논하였다. 또한 상용화에 필요한 디지털 Forensic Marking 시스템 기술 요구사항과 FM 삽입/추출 알고리즘 흐름도를 보여주었다. 알고리즘 흐름도에서 설명한 블록을 구현하기 위해서는 Robust 워터마킹 기술과 동일한 기술이 사용될 수 있으나, 포렌식 마킹 기술로 사용되기 위해서는 사용자의 시스템 성능을 고려해야 한다는 점과 실시간으로 동작해야 한다는 조건을 만족해야 한다. DRM 보호기술은 서비스 제공자에게 불편함을 못 느끼게 하는 기술이지만, 사용자에게는 DRM 기술 표준 부재로 인해 단말기간에 콘텐츠를 호환해서 사용할 수 없는 등 불편함을 초래하고 있다. 이에 반해 Forensic Marking 기술은 서비스 제공자 및 사용자에게는 전혀 눈에 띄지 않으면서 저작권 권리에 관한 분쟁을 해결해 줄 수 있는 기술로서 사용자 기기의 성능이 높아짐에 따라 디지털 콘텐츠 보호 기술로 점차 큰 역할을 수행하리라고 예견된다.

참고문헌

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

[2] 김원겸 외 2인, "불법 복제 콘텐츠 추적을 위한 핑거프린팅 기술 동향", 전자통신동향분석 제18권 제4호 2003년 8월 82~94

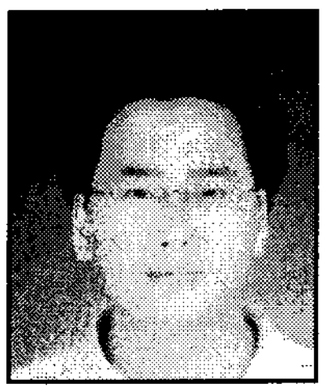
[3] Michael Arnold, "*Techniques and Applications of Digital Watermarking and Content Protection*", Artech House 2003

김 종 안

1984년 고려대학교 전기공학과 졸업.
1988년 고려대학교 대학원 전자공학과 (공학석사)
1988년~현재 KT 미래기술연구소 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 BcN본부 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 BcN본부 전임연구원, 관심분야는 DRM, CAS, 암호화 알고리즘 등임.