논문 2009-46CI-2-7

워터마킹과 암호화를 이용한 DMB 콘텐츠의 재생 및 복사 제어를 PMP에 구현

(Implementation of Play and Copy Control of DMB contents using Watermarking and Encryption on PMP)

정 용 재*, 문 광 석**, 김 종 남**

(Yong-Jae Jeong, Kwang-Seok Moon, and Jong-Nam Kim)

요 약

최근 T-DMB의 정식 서비스는 수신기의 급속한 보급을 만들었다. T-DMB의 보급으로 T-DMB 콘텐츠의 불법 배포에 대한 문제는 커지고 있다. 본 논문에서는 T-DMB 콘텐츠의 불법 배포 방지를 위한 복사 및 재생 제어 정보를 암호화하여 T-DMB 비트스트림에 워터마킹 하는 방법을 제안하고 T-DMB 수신기를 내장한 PMP(portable multimedia player)에 이를 구현한다. 제안한 방법은 전송 스트림을 분석하여 PMT(Program Map Table) 및 PAT(Program Association Table)의 패딩 데이터 부분을 찾아 암호화된 복사 및 재생제어 정보를 워터마킹한다. 구현 결과 복사 및 재생제어 정보에 따라 콘텐츠의 사용이 제어됨을 볼 수 있었다. 제안한 방법은 이동형 T-DMB 단말기에서 T-DMB 콘텐츠의 불법 배포를 막을 수 있는 콘텐츠 보호용 소프트웨어로 활용될 수 있을 것이다.

Abstract

Recently, the regular service of a terrestrial digital multimedia broadcasting(T-DMB) made faster distribution of T-DMB receiver. The problem of an illegal distribution is increasing owing to a large distribution of T-DMB receiver. In this paper, we propose a watermarking and encryption method on T-DMB bit-stream for a copy and play control to prevent an illegal distribution of T-DMB contents. We implement our proposed method on a portable multimedia player (PMP) which has T-DMB receiver. The proposed method insert the encrypted information for control of copy and play after finding padding area of program map table (PMT) and program association table (PAT) from analysis of transport stream (TS) of T-DMB. In implementation result, we can control use of contents according to information of copy and play control. The proposed method can be used to content protection software for blocking of an illegal distribution of T-DMB contents on a mobile T-DMB receivers.

Keywords : T-DMB, Watermarking, Encryption, bit-stream, PMP

I. 서 론

최근 T-DMB의 정식 서비스로 T-DMB 단말기의 보급률이 급속도로 증가되고 있다. 이러한 T-DMB 단말기는 핸드폰, PDA, PMP와 같은 이동형 기기에 내장되어 있으며, 대부분의 T-DMB 수신기들은 플래쉬 메모리 또는 하드디스크와 같은 저장장치를 내장하고 있다. 저장장치를 가지고 있는 T-DMB 수신기들은 수신기에 저장되어 있는 콘텐츠를 저작권자 또는 제작자의 동의 없이 배포하는 불법 배포자가 될 수 있다. 이러한 이유로 T-DMB의 콘텐츠를 보호할 수 있는 기술이 필요하다. 이러한 컨텐츠를 보호 할 수 있는 기술은 콘텐츠의 배포를 사전에 차단 할 수 있는 암호화 기술과 콘텐츠의 불법 배포 후 인증을 통한 저작권을 보호할 수 있는 워터마킹 기술로 구분되어진다. 암호화 방법은 암

* 학생회원, ** 정회원, 부경대학교 전자컴퓨터정보통신공학부
(Department of Electronic Computer Telecommunication Engineering, Pukyong National University)

※ 본 연구는 중소기업청 산학현공동기술개발지원 사업(선도형)과 한국산업기술재단 지역혁신인력양성사업의 지원으로 수행되었음.
접수일자: 2009년2월20일, 수정완료일: 2009년3월6일

호화 알고리듬을 적용하는 영영에 따라 비디오 콘텐츠의 공간영역, 변환영역 그리고 비트스트림 영역으로 나눌 수 있다[1]. 워터마킹 방법은 워터마크가 은닉되는 영역에 따라 공간영역, 변환영역 그리고 비트스트림 영역으로 나눌 수 있다[2].

T-DMB의 경우 방송되는 콘텐츠에 대하여 수신기만 있으면 특별한 절차 없이 무료로 이용할 수 있도록 구현되어져 있어서, 콘텐츠를 보호하기 위한 방법을 수신단에서 구현하여야 한다. 수신단에서 콘텐츠를 보호하려면 공간영역 또는 변환영역에서의 암호화 또는 워터마킹 기술을 사용할 수 없다.

T-DMB 수신 장치를 통하여 불법적인 유통이 발생하였을 경우 소극적인 보호 방법인 콘텐츠에 대한 저작권 확인보다 적극적으로 콘텐츠 재생 및 복사할 경우 재생을 제어할 수 있는 방법은 필요하다.

본 논문에서는 콘텐츠의 복사 및 재생을 제어할 수 있는 정보를 암호화하여 T-DMB의 재생에 영향을 미치지 않는 비트스트림의 특정 부분에 워터마킹 기법을 사용하여 은닉하고, T-DMB 수신 가능한 PMP에 복사 및 재생 제어 정보를 암호화하고 워터마킹하는 과정을 실시간으로 구현한다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서는 관련연구에 대한 기술을 하고, 복사 및 재생 제어 워터마킹 방법을 Ⅲ장에서 설명하고, Ⅳ장에서는 복사 및 재생 제어 워터마킹의 PMP에 구현하는 방법을 기술한다. 또한 Ⅴ장에서는 제안한 방법에 대한 구현 결과를 기술하고 마지막으로, Ⅵ장에서 결론을 맺는다.

Ⅱ. 관련 연구

본 논문에서 제안하는 방법을 기술하기 위하여 T-DMB, AES 암호 알고리즘 및 최근 워터마킹 기술을 소개한다.

T-DMB에서 비디오 압축 기술은 H.264/AVC의 baseline 1.3 프로파일을 기반으로 하고 있다. 이 프로파일의 특징으로 하나의 GOP(group of picture)는 30개의 프레임으로 구성되어 있고, 각 GOP는 하나의 I 프레임과 29개의 P 프레임으로 구성되어 있지만, B 프레임은 존재하지 않는다. T-DMB는 전송을 위하여 MPEG-2의 전송스트림을 채용하고 있다[3].

AES 암호화 알고리듬은 대칭키 블록 알고리즘으로 입·출력문의 크기는 128, 196, 256 비트로 가변적이며, Feistel 구조를 가지고 있다. 암·복호화 속도는 3중 DES 이상을 가지고 있는 미국에서 표준화된 세계 표준 암호화 방법이다[4].

DMB에서 사용되고 있는 비디오 압축 기술인 H.264/AVC에서의 워터마킹 방법은 많이 연구되고 있다. 2006년 Wang 등은 H.264/AVC 부호기에서 변환에 의한 계수값들의 상관관계를 이용하여 워터마킹하는 방법을 제안하였다[5]. 2006년 Nguyen 등은 H.264/AVC에서의 움직임 예측에 의한 움직임 벡터를 변화시켜 워터마크로 이용한 시스템을 제안하였다[6]. 2006년 Lu 등은 H.264 부호기에서 블록의 특성을 이용하여 블록 극성에 따라 워터마크 정보를 달리하여 은닉하는 방법을 제안하였다[7]. 2007년 Wang 등은 H.264/AVC 부호기에서 이산여현변환에 의한 계수값의 부호를 조정하는 방법으로 워터마킹을 제안하였다[8].

기존의 연구들은 대부분 압축과정에서 부호화기 및 비디오 특성을 이용하여 워터마킹하는 것이 대부분이지만, T-DMB 수신기에서는 비디오 부호화 후 전송되는 비트스트림을 분석하여 워터마킹하는 방법이 적용되어야 하기 때문에 기존의 방법은 사용하기 어렵다.

Ⅲ. 복사 및 재생 제어 정보 은닉 방법

본 장에서는 복사 및 재생 제어 정보의 워터마킹을 위한 방법에 대하여 서술한다. 그림 1은 T-DMB 콘텐츠의 전송 스트림의 구조를 나타내었다. 그림에서와 같이 T-DMB의 전송스트림은 헤더와 페이로드로 구성되어 있는 패킷의 연속임을 볼 수 있다. 하나의 패킷은 188바이트로 구성되는데, 전송스트림은 PID(program identifier)의 값에 따라서 해당 패킷의 특성이 나타나게 된다.

그림 2는 PAT(program association table)을 나타내었다. PAT는 전송스트림의 PID가 나타내는 값이 0x0000일 경우이며, 'Section length'의 값에 따라 패킷

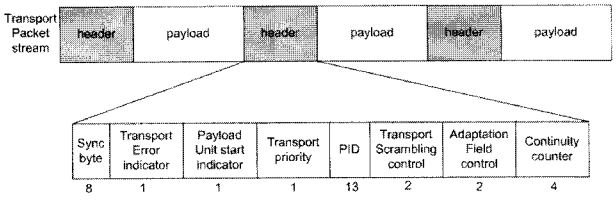


그림 1. DMB 전송 스트림 구조
Fig. 1. A structure of DMB transport stream.

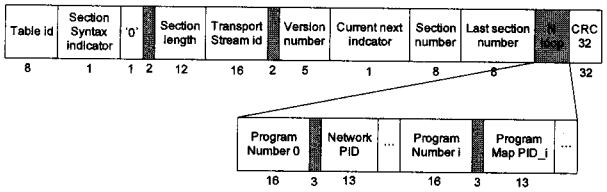


그림 2. PAT 구조
Fig. 2. A structure of PAT.

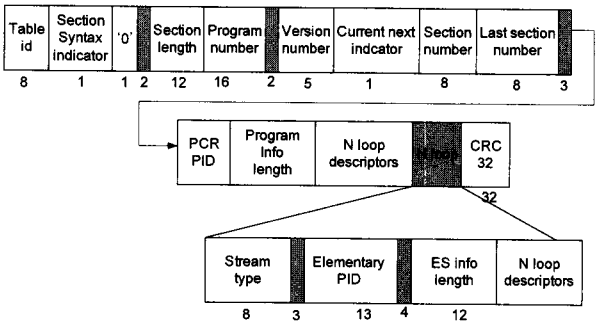


그림 3. PMT 구조
Fig. 3. A structure of PMT.

내부에 패딩 데이터의 크기를 알 수 있다.

그림 3은 PMT(program map table)을 나타내었다. PMT는 PAT에서 'Program Map PID'가 '0x0100'이고, 다음 패킷의 PID가 '0x0100'일 때 PMT 정보를 포함하고 있다. 또한 PMT의 'IOD_descriptor'를 통하여 PES (packetized elementary stream)에서 ES(elementary stream)의 정보를 찾을 수 있다. PMT에서도 'Section length'가 존재하여 이 값이 나타내는 정보를 통하여 패딩 데이터의 크기를 알 수 있다. 패딩 데이터는 패킷의 크기를 188바이트로 유지하기 위한 잉여 바이트로 T-DMB의 재생에는 무관한 정보이다.

본 논문에서는 T-DMB의 비트스트림의 특성을 분석하여 T-DMB의 재생에 영향을 미치지 않는 부분을 검출하여 복사 및 재생 제어 정보를 가지는 워터마크를 암호화하여 은닉한다. 제안하는 방법을 위하여 먼저 전송스트림의 패킷을 하나씩 분석하여 패킷 헤더의 'PID'가 '0x0000'인 패킷을 찾는다. 'PID'가 '0x0000'인 패킷은 PAT 정보를 가지고 있고, PAT를 통하여 'Section length' 정보를 알 수 있다. 'Section length' 값에 따라 패딩 데이터의 크기를 알 수 있고, 패딩 데이터에 워터마크 정보를 은닉하게 된다. 또한 PAT의 'Program Map PID' 정보가 '0x0100'이고 다음 전송 스트림의 PID 정보가 '0x0100'일 때 PMT 정보를 나타내게 되는데 PAT와 같이 'Section length'를 통하여 패딩 데이터의 크기를 검출하여 워터마크를 은닉한다. 그림 4는

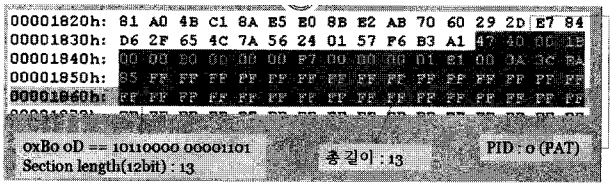


그림 4. PAT 패킷 정보의 예시
Fig. 4. A example of PAT packet.

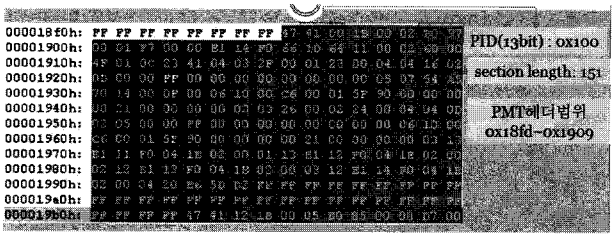


그림 5. PMT 패킷 정보의 예시
Fig. 5. A example of PMT packet.

PAT의 패딩데이터의 예를 나타내었다. 그림에서 'Section length'의 값은 13이기 때문에 PAT 정보의 길이는 13바이트가 되고 그 외 나머지 부분은 패딩 데이터로 채워지게 된다.

그림 5는 PMT에 대한 예시를 나타내었다. 그림에서 PID는 '0x0100'로 PMT를 나타내고, 'Section length'는 151을 나타내므로 'Section length'가 가리키는 크기 이후는 패딩 데이터로 채워지게 된다.

Ⅳ. 제안된 방법을 PMP에 구현

본 논문에서 구현에 사용되는 T-DMB 수신기는 T-DMB칩을 내장하고 있는 PMP이고, Homecast사에서 제작되었다. 사용된 PMP의 내부 프로세서는 DM320으로 100Mhz의 동작속도를 가지는 DSP(digital signal processor)이다. 압축된 T-DMB 데이터를 처리하기 위하여 내부 프로세서의 자원을 대부분 소비하기 때문에 실시간으로 하기 위하여 압축된 비디오의 디코딩(decoding)단계 이전의 비트스트림을 분석하는 단계에서 이루어져야 한다. 본 구현에서의 PMP의 소프트웨어 구조를 그림 6에 나타내었다. PMP에서 T-DMB를 재생하기 위하여 그림 6에서와 같이 4개의 쓰레드(thread)를 사용한다. 각 쓰레드는 BSI, BSO, MAF, GUI로 구성되어 있다. GUI는 PMP에서 버튼 조작이 있을 경우 그 조작에 대한 핸들과 미디어 파일을 불렀을 때 시작 이벤트를 BSI, BSO, MAF에 각각 보내어 동작의 시작을 알린다. BSI는 GUI에서 시작된 이벤트

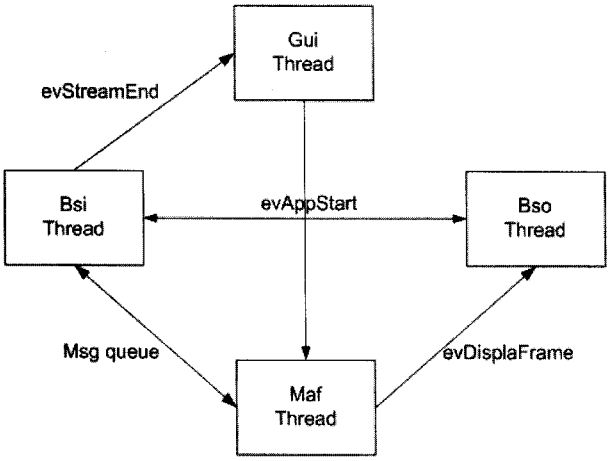


그림 6. PMP 내부 쓰레드 블록도
Fig. 6. Internal thread block diagram in PMP.

가 지시하는 동작에 따라서 비디오의 프레임 정보를 MAF에 전달하고 MAF는 DSP를 이용하여 동영상을 디코딩하여 공유 버퍼에 저장한다.

이 때 저장되어 있는 비디오 프레임의 영상형태는 YCbCr(4:2:2)의 형태로 저장되어 있고, BSO는 저장된 비디오 프레임을 RGB의 형태로 변환하여 재생 가능하도록 만들어 준다. 수신되는 DMB 스트림을 처리하기 위하여 BSI 쓰레드는 DMB 스트림을 분석하고 분석된 스트림에서 현재 지정하고 있는 채널의 데이터만을 내부 버퍼에 저장한다. 내부 버퍼에 저장된 데이터는 MAF 쓰레드를 통하여 비디오 디코딩에 대한 처리를 하거나 녹화 프로세서를 통하여 내부 저장장치에 스트림이 저장된다. MAF 쓰레드를 통하여 처리된 데이터는 BSO 쓰레드를 통하여 화면에 재생된다.

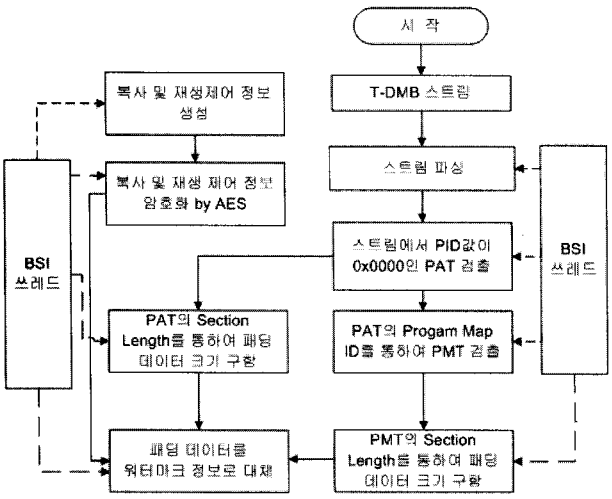


그림 7. PMP에서 정보 은닉 구현도
Fig. 7. A diagram of information hiding on PMP.

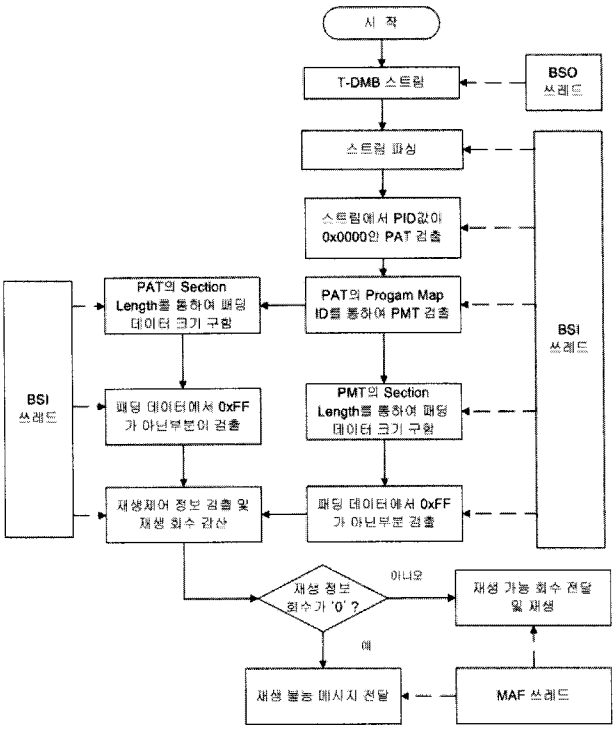


그림 8. PMP에서 정보 검출 구현도
Fig. 8. A diagram of information extracting on PMP.

그림 7은 본 논문에서 제안하는 방법을 PMP에 구현하는 과정을 나타내었다. T-DMB 수신기로 들어오는 스트림은 BSI 쓰레드를 통하여 파싱되는데 이 때 파싱 정보를 분석하여 제안한 방법을 적용하게 된다. 파싱하는 과정에서 제안하는 방법을 적용하기 때문에 시간적 지연은 거의 없다. 또한 복사 및 재생 제어 정보의 암호화는 AES 알고리듬을 사용하는데 이 알고리듬은 16바이트를 암호화할 경우 소모되는 시간이 4μs정도이기 때문에 지연시간은 거의 없다. 그림 8은 은닉된 정보를 검출하는 과정을 도시화 하였다. 그림에서와 같이 저장된 T-DMB 콘텐츠는 BSO 쓰레드를 통하여 불러오게 되고, BSI 쓰레드를 사용하여 T-DMB 스트림을 파싱하게 된다. 파싱 과정에서 PAT와 PMT의 'Section Length'의 크기로 패딩 데이터의 위치를 판단하고 패딩 데이터의 시작위치부터 검색하여 패딩 데이터가 아닌 부분을 검출하게 된다. 검출된 데이터는 AES 알고리즘을 통하여 복호화 한 다음 복사 및 재생 정보를 확인하여 그 결과를 화면에 보여주게 된다.

V. 구현 결과

제안한 방법의 성능을 평가하기 위하여 다음과 같은

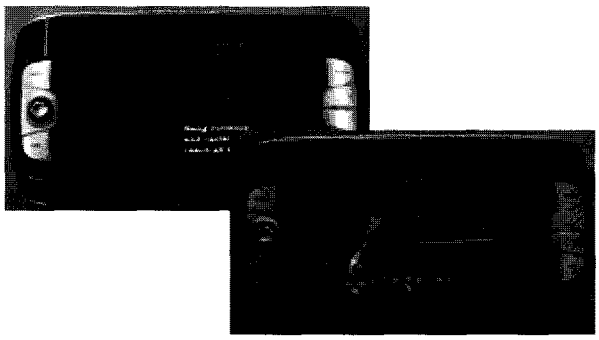


그림 9. 구현에 사용된 PMP
Fig. 9. Used PMP for an implementation.

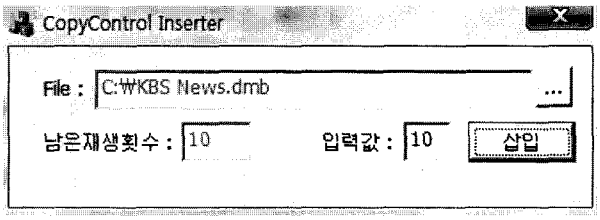


그림 10. 재생 횟수 설정 프로그램
Fig. 10. A configuration program for a play counter.

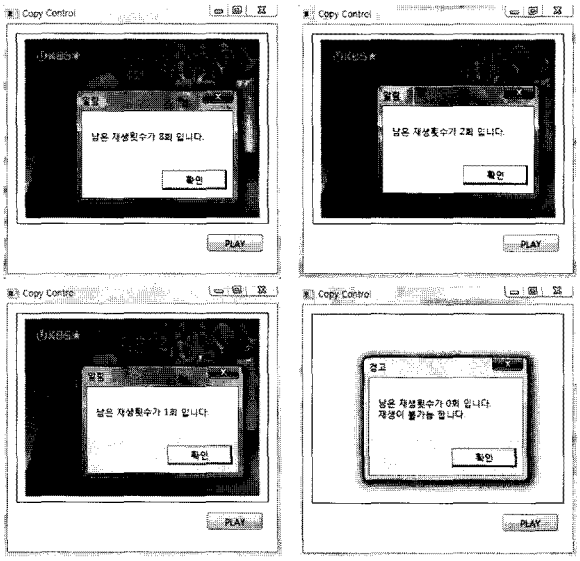


그림 11. PMP에서 복사 및 재생 제어 정보 검출 화면
Fig. 11. A extracting shots of a copy and play control information on PMP.

조건에서 실험하였다. DMB 스트림 암호화 구현에 사용된 PMP는 Homecast사의 Tvus HM-900이고, Microsoft Platform Builder 5.0과 Embedded Visual C++ 4.0을 이용하여 프로그램을 구현하였다. 그림 9는 실험에 사용된 Homecast사의 PMP이다.

그림 10은 복사 및 재생 제어 정보의 은닉을 테스트하기 위하여 PC에서 구현된 프로그램이다. 프로그램을 구현하기 위하여 Intel Pentium-4 2.8GHz CPU, 1Gbyte RAM 그리고 Microsoft Window XP SP3로 구성되어 있는 PC를 사용하였고, Microsoft Visual C++ 9.0에서 프로그래밍 하였다. 그림에서 테스트를 위하여 PMP를 통하여 저장된 T-DMB 콘텐츠에 복사 및 재생 제어가 가능한 정보를 AES로 암호화 하여 PMT 및 PAT의 패딩 데이터에 은닉한다.

그림 11은 그림 10을 통하여 은닉된 정보에 대한 PMP에서의 결과를 나타내었다. 그림의 결과에서는 복사 및 재생 제어 정보를 '10'이라는 숫자 형태로 은닉하고 PMP에서 재생 할 때마다 숫자가 줄어드는 것을 확인 할 수 있다. 그림 11의 오른쪽 아래 그림의 경우 T-DMB 콘텐츠에 은닉되어 있는 정보를 검출한 결과 남아 있는 재생 가능한 횟수가 '0'로 더 이상 재생할 수 없게되어 그림과 같은 메시지를 PMP화면에 띄우게 되고 T-DMB 콘텐츠는 더 이상 재생이 안 되게 된다.

VI. 결 론

본 논문에서는 이동형 기기를 통한 DMB 콘텐츠의 배포를 제한 할 수 있는 암호화 및 워터마킹 기술을 사용하여 복사 및 재생 제어 할 수 있는 방법을 제안하고, 이동형 T-DMB 기기 중 PMP에 구현하였다. 제안한 방법은 전송 스트림에서 패딩 데이터 부분을 검출하고, 검출된 패딩 데이터에 AES 알고리즘을 이용하여 암호화된 복사 및 재생 제어 정보를 워터마킹 기술을 이용하여 은닉 및 검출하였다. 실험 결과 PMP에서 T-DMB 콘텐츠 시청 중 실시간으로 워터마크 삽입에 소비되는 시간지연은 거의 없었고, PMP를 통하여 재생 제어 정보가 삽입된 T-DMB 콘텐츠를 재생하였을 경우 복사 및 재생 제어 정보에 따라 제어 가능함을 알 수 있었다. 제안한 방법은 이동형 DMB 단말기에서 DMB 콘텐츠의 불법 배포를 방지하기 위한 콘텐츠 보호용 소프트웨어로 활용 될 수 있을 것이다.

참 고 문 헌

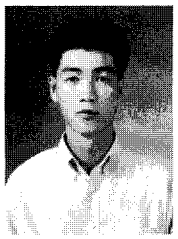
[1] 김종협, 이선근, 김환용, "멀티미디어 통신에 적합한 HiSSR 블록암호 시스템 설계에 관한 연구," 전자공학회논문지, 제 40권 TE편 제 3호, 54-63쪽, 2003년 9월
[2] 김덕령, 박성한, "멀티미디어 데이터 소유권 보호를 위한 워터마킹 기술," 전자공학회논문지, 제26

권 제 7호, 61-69쪽, 1999년 7월
[3] "TTA, 초단파 디지털라디오방송 비디오 송수신 정합표준," TTA S.KO-07.0026, 2004년 8월
[4] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," Springer-Verlag, 2002.
[5] T. Lu, W. Hsu, and P. Chang, "Blind Video Watermarking for H.264," Conference on Electrical and Computer Engineering, pp. 2353-2356, 2006.
[6] W. Meihua, F. Kefeng, Y. Bin, and Y. Xiaojun, "A Content Protection Scheme for H.264-based Video Sequence," Eighth ACIS International Conference on SNPD, Vol 3, pp. 388-393, 2007.
[7] C. Nguyen, T. Tay and G. Deng, "A Fast Watermarking System for H.264/AVC Video," IEEE Asia Pacific Conference on Circuits and Systems, pp. 81-84, 2006.
[8] T. Wang and Y. Zhang, "A Digital Watermarking Method in H.264 Video Transmission," International Conference on Communication Technology, pp. 1-3, 2006.

저 자 소 개

정 용 재(학생회원)
1999년 부경대학교 전자공학과 학사 졸업.
2002년 부경대학교 전자공학과 석사 졸업.
2008년 부경대학교 전자공학과 박사 수료.
<주관심분야 : 워터마킹, 영상 및 비디오 신호처리>

문 광 석(정회원)
1979년 경북대학교 전자공학과 학사 졸업.
1981년 경북대학교 전자공학과 석사 졸업.
1989년 경북대학교 전자공학과 박사 졸업.
1988년 일본 동경대학교 학부 연구원
1997년~1998년 미국 Jackson State University 객원교수
1990년~현재 부경대학교 전자컴퓨터정보통신 공학부 교수
<주관심분야 : 영상신호처리, 적응신호처리 등>



김 종 남(정회원)
1995년 금오공과대학교 전자공학과 학사 졸업.
1997년 광주과학기술원 정보통신 공학과 석사 졸업.
2001년 광주과학기술원 기전공학과 박사 졸업.
2001년~2004년 KBS 기술연구소 선임연구원
2003년~현재 (주)홈캐스트 사외이사
2004년~현재 부경대학교 전자컴퓨터정보통신 공학부 교수
<주관심분야 : 영상신호처리, 멀티미디어 보안 등>