RMP를 이용한 PVR에서의 지상파방송 디지털컨텐츠 보호 Manager 모듈 구현

The Implementation of Digital Contents Copy Protection Manager In Digital Broadcasting Using RMP

*정종진, 임태범, 김윤상,이석필
*Jung,Jong-Jin, Lim,Tae-Bum, Kim,Yun-Sang, Lee,Seok-Pil

Abstract - With the start of terrestrial digital broadcast, we can view HD digital contents in TV. Also we can record , play , redistribute digital contents over the various way. Therefore the protection of Digital Contents Right became the important issue. In this paper, we implement a manager that prevents indiscriminate digital contents redistribution of the terrestrial digital broadcast contents. For protection of Digital contents Right, we use BF(Broadcast Flag) that we can control viewing or copy digital contents with.

Key Words : BF, DRM, AES,

1장. 관련연구

1.1절 BF (Broadcast Flag)

최근 디지털 지상파 방송 프로그램의 무차별적인 재배포를 금지하고 디지털 컨텐츠의 저작권을 보호 하기 위해 FCC 에서는 2005년 7월 이후에 출시되는 모든 디지털 지상파 수신기기는 BF(Broadcast Flag) 를 인식하여 동작하도록 의무화 하는 법안을 통과 시켰다. 이를 위해 13개의 디지털 출력 보호 기술 및 녹화 방법 (e.g. DTCP, HDCP 등), 을 승인하였고, 이 승인된 방법에 의해서만이 디지털 컨테츠를 저장/녹화/출력이 가능 하도록 하였다. BF는 디지털 지상파 방송 컨텐츠에 실려오는 부가 정보로서 MPEG-2 TS 포함된 1-bit Flag이다. 아직까지 방송국 쪽에서는 BF를 방송 컨텐츠에 포함시킬지는 결정하지는 않았지만 조만간 포함하는 방향쪽으로 움직이고 있다. 또한 케이블이나 위성방송을 통한 지상파 프로그램을 재전송 하는 경우에도 지상파 프로그램에 추가된 BF가 손상되지 않고 재전송되도록 하였다. BF는 MEPG-2 TS 스트림중 EIT에 실려 전송 되어 지는 데, 그 정보는 ATSC A/65B에서 정의한 rc_descriptor라는 데이터로 전송 되어진다. 아래 그림 1은 지상파 디지털방송에 실려오는 BF에 format을 설명하고 있다.

Syntax	No.of Bit	Format

rc_descriptor() {
descriptor_tag
descriptor_length
for(;descriptor_length;i++)
rc_information()
}
	
	8
	8
	
	8
		
		0xAA
		uimsbf
		
		uimsbf

그림 1. EIT에 실려오는 BF정보(rc_descriptor)

따라서 방송국 제작자들은 그림 1에서 설명된 바와 같이 rc_desciptor를 이용하여 디지털 컨텐트에 대해 녹화/저장/복사등에 관련된 컨트롤을 할 수 있는 데이터를 실어 보낼수 있다.

아래 그림 2은 방송스트림에 같이 실려오는 BF를 수신기기가 Check하여 디지털 컨텐츠를 보호하는 BF의 동작원리를 설명하고 있다.

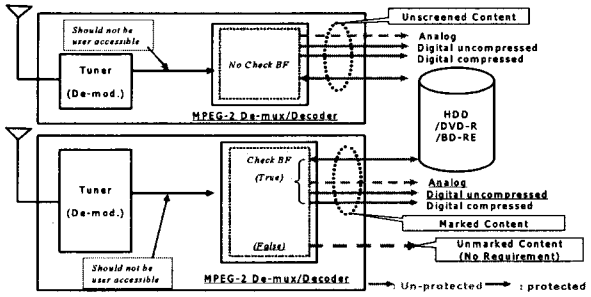

그림 2 BF 동작 원리

그림 2에서 보듯이 BFS(Broadcast Flag Solution)에서 출력으로 내보내는 컨텐트 종류는 3가지 이다.

1) Unscreened Content

BF 자체를 Check 하지 않고 컨텐트를 출력으로 내보내는 형태로서, BFS에서는 13가지 인증된 방법중 기기에 탑재된 방법으로 컨텐츠를 암호화 하여 출력으로 내보내야 한다.

2) Marked Content

BF를 Check 하여 그 값이 TRUE 인 경우 인데, 1번의 경우와 마찬가지로 기기에 탑재된 인증된 방법으로 암호화하여 출력으로 내보내야 한다.

3) Unmarked Content

BF를 Check 하여 그 값이 FALSE 인 경우 인데 이 경우는 저작권과 관련해 아무런 제약이 없는 경우로서 유저가 마음껏 저장/녹화/복사 등이 가능한 형태이다.

1.2절 AES 컨텐츠 암호화 및 복호화

Digital TV stream의 암호화에는 시스템에게 많은 부하를 주지 않는 대칭 암호화 방식이 주로 사용된다. 대표적인 것이 DVB 에서 사용하는 DES이다. 그러나 컴퓨터 산업의 폭발적인 발전으로 인해 DES 의 짧은 key 길이 (56비트) 는 더 이상 보안을 보증하기 어려운 지경에 이르렀다.따라서 key 길이를 늘이면서도 시스템에 큰 부하를 주지 않도록 하는 알고리즘이 요구되었고, 이에 따라 제정된 표준이 AES 이다 AES는 DES보다 긴 Key를 사용함으로써 보안성이 뛰어난 것으로 알려져 있고, 대칭키 방식(Symmetric Encryption)을 사용하여 시스템에 부하를 적게 주는 특징을 가지고 있다.

2장. 시스템 구현

2.1 절 시스템 구성 및 설계

RMP를 이용한 PVR에서의 지상파방송 디지털컨텐츠 보호 Manager 모듈 구현을 위해서는 아래 그림 3과 같다.

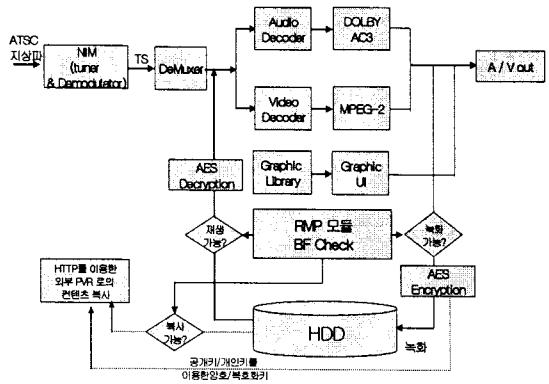

그림 3. RMP를 이용한 PVR에서의 지상파방송 디지털 컨텐츠 보호 Manager 모듈 시스템 블럭도

2.2 절 AES 알고리즘 구현

실시간으로 들어오는 컨텐츠 전체를 소프트웨어로 암호화/복호화 하는 것은 PVR의 처리 능력을 벗어나므로 (일반적으로Digital PVR의 경우 5% 이상을 암호화 하는 것은 불가능하다), 소량의 데이터를 암호화 하면서도 암호화의 효과를 극대화 할 수 있도록 그림 4과 같이 인덱스 파일의 I-picture 정보를 이용하여 암호화를 구현하였다.

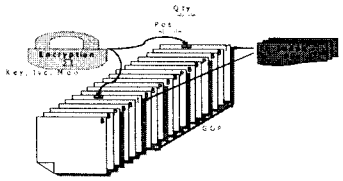

그림 4. I-Picture를 이용한 AES 암호화

그림 4과 같이 암호화하게 되면 수신자 입장에서는 암호화된 부분을 복호화해내지 못하면 손상된 I-picture를 수신한 결과가 되고, 따라서 MPEG 데이터의 특성상 IBBPBBP… 로 이어지는 전체 GOP가 쓸모 없어지게 된다. 즉, 암호화는 극소량의 데이터만을 암호화 했지만, MPEG Decoding에 있어서 가장 중요한 부분을 암호화 함으로써, 복호화 정보가 없이는 컨텐츠를 재생해낼 수 없도록 하였다. 이와 같은 방법을 쓸 경우 최소 0.01% 정도의 암호화로도 복호화 없이는 재생이 불가능하도록 만들수 있다. 암호화 용량은 Qty 인자를 이용하여 조절할 수 있는데, Qty=1 은 1 GOP 에 128-bit를 암호화했음을 의미한다. 또한 그림 3와 같은 I-picture를 이용한 암호화는 일반적인 Digital PVR에 쉽게 이식할 수 있는 특징을 가진다. 보통 Digital PVR은 Trick Play 구현을 위하여 I-picture 및 P-picture의 정보와 Time Stamp 관련 정보를 별도의 인덱스 파일로 만들어 저장한다. 따라서 이 암호화방식은 별도의 추가 정보가 없어도 일반적인 인덱스 파일만을 이용하여 구현할 수 있다.

2.3 절 암호/복호화키 생성 및 관리

2.3.1) 고정 키

고정 Key는 PVR 의 Serial ID, 사용자의 PIN code 등을 사용해서 고유한 값을 만들어서 설정해 주면 된다. 이 값은 암호화에 실제 쓰이는 time-variant key를 생성하는 기본 값으로 사용되게 된다.

2.3.2) 가변 키

고정키에서 얻어진 고정 Key만을 사용하게 되면 해킹의 위험에 쉽게 노출되므로 Key에 변화를 줄 필요가 있다. 따라서 Digital PVR의 인덱스파일 정보를 최대한 이용하기 위하여 그림 5와 같이 인덱스 파일의 정보를 활용하여 Key에 시간적 변화를 주었다.

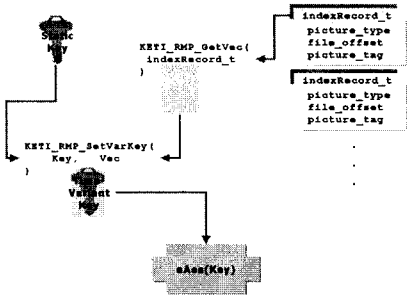

그림 5. 가변키 생성

2.4 절 RMP 매니저 모듈 구현

지상파 방송 테이타의 저작권 보호를 위한 시나리오와 이를 위한 BF 구성은 아래와 같다

①녹화가능 Check	0xF1 +"True or False"
②재생가능횟수 Check	0xF2 +"Num of View or 무제한"
③복사가능횟수 Check	0xF3 +"Num of Copy or 무제한"

그림 6. BF 구성및 시나리오

EIT중 rc_descriptor형태로 실려오는 BF를 총 3Byte로 구성하였고 이 Byte들의 값을 통해 녹화여부/녹화된 컨텐츠의 재생횟수 제한/외부기기로의 복사여부를 결정하게 된다. 그림 4와 같이 BF중 Check View Count는 play횟수를 제한할 수

있으며, PVR로 저장된 컨텐츠는 HTTP/USB를 통해 외부 PVR로 전송가능하며 이때 BF 데이터와 재생시 필요한 암호/복호화키는 공개키/개인키를 사용하여 암호화 하여 전송하게 된다. 그림 7은 이 과정을 설명하고 있다.

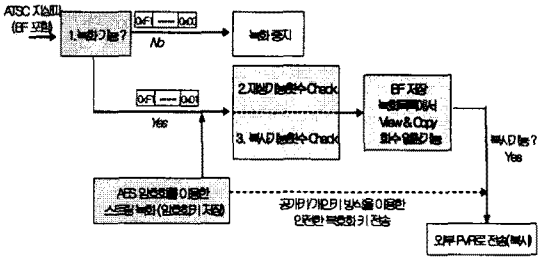

그림 7. RMP 모듈 구현 블럭도

3장. 구현 결과

3-1) HW 모듈 및 플랫폼 설계 결과

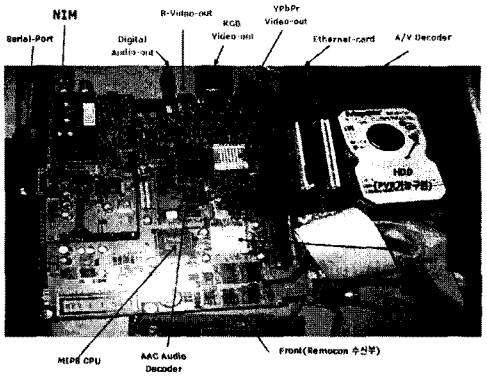

그림 8. HW 모듈 플랫폼

3-2) RMP를 이용한 PVR 기능

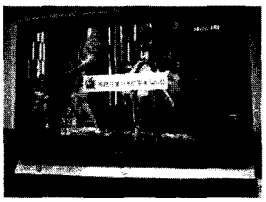

그림9-1.BF False인 방송데이타를 녹화

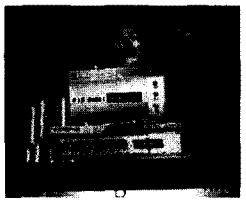

그림9-2.User Pin 코드를 입력하여 녹화

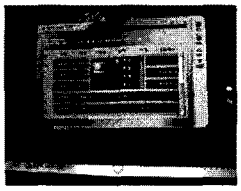

그림9-3.녹화 목록

그림9-4.외부기기로전송

그림 9은 RMP를 이용한 PVR기능에 관련된 내용이다. 9-1 은 BF가 "FALSE"인 방송 즉 녹화할수 없는 방송을 녹화하려 할 때 녹화 할수 없다는 경고 메시지와 함께 녹화가 취소되는 그림이고, 9-2는 녹화가 가능할 때 녹화한 사람만이 재생할 수 있도록 사용자 Pin code를 입력하여서 등급제한이 있는 방송인 경우 성인만 볼 수 있는 기능을 제공하고, 9-3은 현재 PVR에 녹화 저장되어 있는 녹화 목록을 열람하여 현재 저장된 스트림을 몇변 재생 또는 복사 가능한지를 보여준다. 9-4는 외부기기로 복사가 가능할 때 안전한 복호화 키 전송 및 컨텐츠 전송 상태를 보여주는 그림이다.

3-3) 고정키/가변키를 이용한 RMP 기능

그림10-1.복호화키 오류시 재생화면 깨진현상

그림10-2.올바른복호화 키로 정상적인 재생

그림 10-1은 녹화시 입력된 Pin-Code가 잘못 되거나 녹화한 PVR에서 HDD를 떼어 다른 PVR에 붙이거나 하는 경우 재생화면이 깨어져 사용자에게 볼 수 없게 하여 컨텐츠 저작권 보호를 한 결과 이다. 10-2는 정상적인 사용자 Pin-code를 입력하였을 경우 정상적인 재생화면이 보여지는 경우이다.

4. 장 결 론

진통 끝에 우리나라의 디지털 방송의 전송방식이 결정됨에 따라서 방송사에서는 디지털 방송에 대한 투자가 본격화 되고, 디지털 방송 수신기를 개발하고 있는 각 기업체에서도 개발에 박차를 가하고 있다. 이러한 분위기와 함께 사용자들의 고품질의 디지털 방송을 즐기기 위한 욕구가 증가하고,다양한 컨텐츠를 제공하여 많은 고화질의 볼거리가 제공될 것이다. 어떠한 형태로든 디지털 방송의 무분별한 재전송을 제한하여 컨텐츠 저작권 보호를 해주어야 할 것이다.

본 논문에서 구현한 RMP를 이용한 PVR에서의 지상파방송 디지털컨텐츠 보호 Manager 모듈은 HD급 고화질 A/V를 시청, 녹화 할뿐만 아니라 BF를 이용해 디지털 컨텐츠의 재전송을 제한했을 뿐만 아니라 인증된 사용자 / PVR만이 재생이 가능하여 외부기기로 불법 복제를 제한 하였다.

앞으로도 이에 관련된 연구가 많이 진행될 것이며 ,모듈개발에 관련된 많은 성과가 나타나서 제2의 MP3 파일 불법복제와 같은 문제가 없어야 할 것이다.

참 고 문 헌

[1] FCC ADOPTS ANTI-PIRACY PROTECTION FOR DIGITAL TV - FCC Release 2004

[2] ATSC Standard: Program and System Information Protocol for Terrestrial Broadcast and Cable (Revision B)

[3] TVA Specification series(1-4),TAF,2002