

# 제한수신시스템을 적용한 디지털 멀티미디어방송 수신시스템 구현에 관한 연구

김영빈\* · 류광렬\*

\*목원대학교 대학원 IT공학부

## A Study on the Realization of Digital Multimedia Broadcast Receiving System using Conditional Access System

Young-bin Kim\*, · Kwang-ryol Ryu\*

Mokwon University

컴퓨터비전분과

Email : ryol@mokwon.ac.kr

### 요 약

본 논문은 유료 가입자에 대해서 수신이 가능하도록 제한하는 제한수신시스템을 적용한 디지털멀티미디어방송 수신시스템 구현에 관한 연구이다. 이 시스템은 스마트카드와 소프트웨어 기법의 제한수신시스템을 사용하여 스크램블 된 전송 스트림을 역스크램블 하기 위한 제어단어를 추출하므로 강화된 안전성을 제공한다. H.264의 비디오 데이터 복호화 처리를 위한 DSP와 RISC가 있는 듀얼 프로세서 사용하여 QVGA의 비디오와 24Khz~48Khz의 오디오 방송을 평균 15f/s로 재현이 가능하다. 가입자 정보를 추가한 방송 스트림을 수신하여 제한수신의 동작 상태와 역스크램블 된 스트림을 디코딩하였을 때 정상 가입자에 대한 경우 역스크램블 과정이 정상적으로 수행되었음을 확인할 수 있었다.

### Abstract

A realization for digital multimedia receiving system using Conditional Access System is presented in this paper. The key word for descrambling is make from smart card and Conditional Access System, a Stabilization is grow up in the method. It is possible to decoding that of average 15 fame/second of H.264 video format and that 24Khz~48Khz audio sample rate using dual processor that of high performance DSP and RISC. This system is evaluated correct descrambling procedure in test stream added that signed user data.

### 키워드

Conditional Access System(CAS), Embedded system, Digital Multimedia System

### 1. 서론

위성을 이용하는 디지털 위성 방송에서 위성신호가 도달하는 지역 내에서는 그리고, 방송 수신기를 가지고 있다면 누구나 방송 신호를 수신하는 것이 가능하다. 이때 유료 가입자에 대하여 방송을 시청할 수 있도록 수신 자격을 제한하는 방법으로 이용되는 것이 제한수신시스템이다. 방

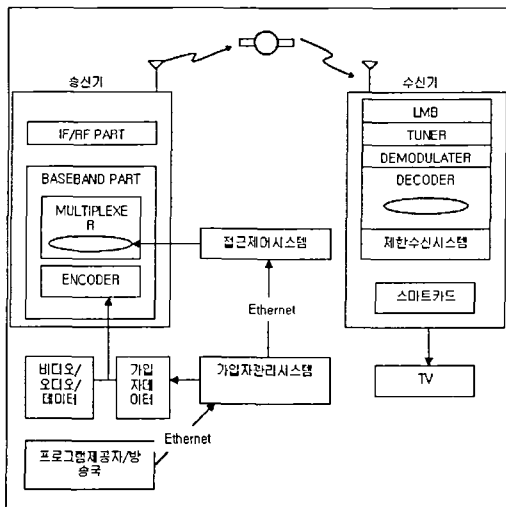
송에서의 제한수신시스템(CAS: Conditional Access System)이란 송신기에서 스크램블 된 신호를 수신측의 수신 권한을 받은 가입자만 프로그램을 시청할 수 있도록 하는 시스템으로 신호의 질을 손상시키지 않고 스크램블링/역스크램블링 하는 과정은 아날로그 신호보다는 디지털에서 더 간단하기 때문에 일반적으로 제한수신 방송시스템으로 디지털을 이용한다.[7~10] 본 논문에서는 디지털 멀티미디어 방송수신 시스템을 구현하

고 특정 가입자만이 방송을 수신할 수 있도록 스마트카드와 제한수신시스템을 적용해 보도록 한다.[1-6] 2장에서는 제한수신 시스템의 기본 구조를 설명하고, 3장에서는 제한 수신시스템을 적용한 디지털 방송수신시스템 구성에 대하여 설명하고 4장에서는 소프트웨어 구조 및 동작, 5장에서는 시스템의 테스트 및 결과 6장에서는 결론으로 글을 맺는다.

## II. 제한수신시스템

### 2.1 디지털 위성방송시스템의 구성

유료 위성디지털방송시스템은 방송 사업자, 방송국 인터 페이스인 방송 분배망을 통해서 연결되는 송신국, 가입자 관리 시스템 및 제한 수신 시스템, 전송 매체로 위성, 수신 안테나, 셋탑박스, 스마트 카드, 수신용 모니터 등을 포함한 수신부, 그리고 특정 지역에 가입자의 인증을 위한 관리 센터로 구성된다. 방송 사업자는 방송 분배망을 통해서 송신국에 전송될 프로그램 데이터를 전달하며 송신국에서는 제어 단어를 이용하여 원시 프로그램을 스크램블링하여 위성 전송 장치를 이용하여 위성을 통해서 수신부에 전송한다. 관리 센터는 지역별로 일정한 가입자를 관리하며 인증한다. 관리 센터에서는 가입자 등록 데이터를 송신부의 가입자 관리 시스템으로부터 주기적으로 다운로드 받으며, 비밀 키를 생성하고, 센터가 관장하는 지역의 가입자들과의 통신을 통해서 가입자들에 대한 인증 기능을 수행 한다. 실제로 가입자는 스마트카드를 셋탑박스 내에 삽입하여 관리 센터로부터 생성된 키를 분배 받아 제어 단어를 얻어내야만 수신된 프로그램을 제어 단어를 이용하여 역스크램블링 함으로서 수신 모니터를 통하여 방송을 시청할 수 있다. 그림1에서 디지털 위성방송의 송/수신에 대한 개념을 보이고 있다.



### 그림1. 디지털 위성방송시스템의 기능적 블록도

### 2.2 제한수신시스템의 구성

제한수신시스템은 스마트카드, 디멀티플렉서, 필터, 역스크램블러, 소프트셀, 제한수신타스크로 연결되어 동작한다. 소프트셀은 스마트카드와 디멀티플렉서, 필터, 역스크램블러, 제한수신타스크와 연결된 모듈이다. 제한수신타스크는 소프트셀과 미들웨어간의 인터페이스를 제공하는 모듈이다. 스마트카드는 스마트카드 드라이버를 통하여 소프트셀과 데이터를 주고받게 된다.

각 모듈간의 상호 동작 과정에서 소프트셀은 스마트카드로부터 시스템ID를 읽어오고, 시스템 ID는 가입자별 고유의 ID에 해당한다. 소프트셀에서는 시스템ID를 메시지에 담아 제한수신타스크에 보내고, 제한수신타스크는 이 시스템ID를 사용하여 CAT와 PMT를 파싱하여 해당 채널의 PID를 찾는다. 이때 CAT는 EMM을 필터링할 PID를 제공하게 되고, PMT는 ECM을 필터링할 PID를 제공하게 된다. 소프트셀은 EMM/ECM PID를 소프트셀로 보내면 소프트셀에서는 디멀티플렉서로 EMM/ECM 필터를 세팅하고, 필터링된 EMM과 ECM을 받아 스마트 카드로 보낸다. 스마트카드에서 ECM에 대한 응답으로 제어단어가 들어오며, 이 제어단어는 Demux를 통하여 역스크램블러로 로드되어 스크램블 되어 있는 데이터를 역스크램블 하게 된다. 그림2는 제한수신시스템에서 각 모듈의 연결을 보이고 있다.

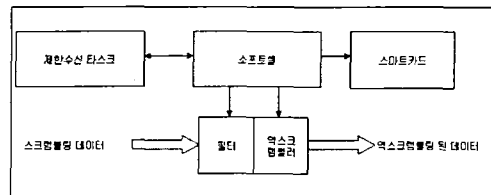


그림2. 제한수신시스템의 블록도

## III. 디지털 방송 수신 시스템

디지털방송수신시스템은 수신한 스크램블링 데이터를 역스크램블링하는 과정과 이 과정에서 역스크램블링 되어진 H.264 데이터를 디코딩 하는 과정을 수행하게 된다. 본 시스템에서는 RISC 프로세서와 고속 연산이 가능한 DSP 프로세서가 함께 내장된 듀얼 프로세서를 사용한다.

### 3.1 듀얼 프로세서의 구조

RISC와 DSP가 하나의 프로세서로 구성되어 있는 듀얼 프로세서 시스템의 구조는 그림3과 같다.

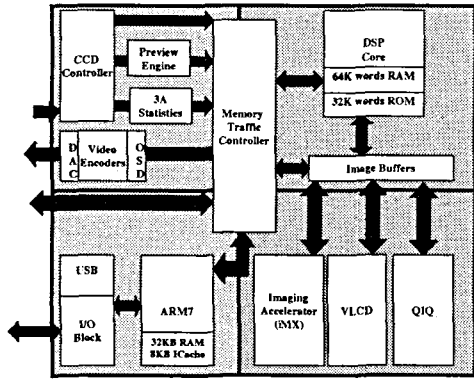


그림 3. 듀얼프로세서의 내부 구조

RISC 프로세서는 ARM7TDMI 코어로 내부 메모리로 SRAM과 8K byte의 인스트럭션 캐시를 가지고 있고 내부의 I/O 블록을 제어하기 위해서는 I/O 레지스터를 사용한다. 주변 인터페이스 기능으로 MMC/SD 카드 인터페이스와 UART 인터페이스, CCD 인터페이스 컨트롤러가 있다. DSP 부분은 C54x 프로세서를 가지고 있으며 Host Port Interface Block(HPIB)을 사용하여 RISC 프로세서와 인터페이스하게 된다. 디코딩 과정에서 많은 양의 데이터를 신속하게 처리하기 위해서는 RISC와 DSP 와 데이터 메모리를 공유하게 되는데 이때 메모리 트래픽 컨트롤러(MTC)를 사용하여 RISC와 DSP 그리고 CF와 SDRAM과의 인터페이스를 제어하게 된다. DSP 코어 부분에는 Image Extension coprocessor(iMX)와 variable length coding/decoding accelerator(VLCD)가 있어 고속의 이미지 처리가 가능하다.

### 3.2 시스템의 하드웨어 구조

본 논문에서 구현하는 시스템의 프로세서는 RISC와 DSP의 듀얼 프로세서 뿐만 아니라 주변 장치들을 제어하기 드라이버 디바이스가 집적되어 있는 SoC(System On Chip)로 주변 인터페이스 회로를 최소화 할 수 있다. 주변회로 및 구현 시스템의 하드웨어 블록도는 그림4에 보이고 있다. RF H/W 블록은 안테나로 받은 RF 신호를 디지털 신호로 변환하여 출력하고, 에러정정 과정을 수행하며 신호의 상태를 프로세서에서 관측하여 제어할 수 있다. 역스크램블러에서는 선택된 채널의 전송 스트림을 역스크램블 하는데 하나의 채널에는 하나의 패킷 ID를 가지고 역스크램블 하게 된다. 역스크램블러 과정을 거친 전송 스트림은 필터와 demux에서 패킷을 검사하여 필요한 PID의 스트림을 선택적하여 스마트카드로 보내져 역스크램블에 필요한 제어단어를 추출하게 된다. 추출된 제어단어는 다시 역스크램블러로 보내져 사용된다. 디코더에서는 H.264 디코딩을 수행하여

비디오/오디오 신호를 TV로 출력한다. 그림4는 구현시스템의 전체 블록도이다.

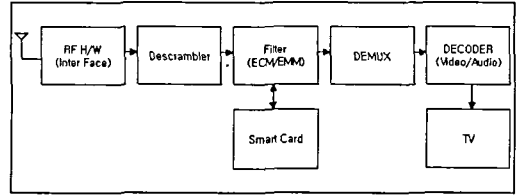


그림4. 구현된 제한수신 방송수신 시스템의 블록도

## IV. 소프트웨어 시스템

디지털 멀티미디어방송 수신시스템의 구성은 실시간 OS 환경을 기반으로 콘텐츠를 재생 및 시스템 정보를 운용하기 위한 사용자 인터페이스가 있고, 튜너에서 입력된 데이터는 스크램블링되어 있으므로 제한수신타스크와 소프트웨어, 역스크램블러, 필터에서 역스크램블링 처리한다. 메모리 관리기에서는 역스크램블링 되어진 데이터와 디코딩된 데이터를 데이터 버퍼에 관리한다.

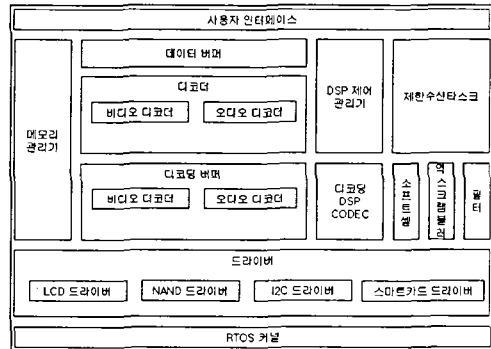


그림 5. 소프트웨어의 기능적 블록도

사용자 인터페이스는 시청하고자 하는 채널의 목록을 나타내거나 채널의 편성 정보 등을 선택하여 시스템이 디코딩을 시작하도록 한다. 수신하고자 하는 채널을 선택 하면 튜너를 통하여 디지털로 변환된 전송스트림은 메모리 관리기에 의해 관리되고 제한수신타스크에서 가입여부를 판단하게 된다. 가입이 확인되면 역스크램블 하기 위한 제어단어를 스마트카드와 소프트웨어에서 추출하고 역스크램블을 시작한다. 역스크램블 되어진 멀티미디어 데이터는 데이터 버퍼에 쌓는다. DSP 제어 관리기는 DSP 프로세서에 디코딩 하고자 하는 코덱을 로딩하여 데이터 버퍼의 압축된 비디오 데이터를 복호화 하게 된다. H.264를 디코딩 하기 위한 코덱은 라이브러리 형태로 상용화된 엔진을 사용한다. DSP 프로세서에서 복호화 된

데이터는 메모리의 디코더 부분의 오디오 버퍼와 비디오 버퍼에 보관되어 지고 RISC 프로세서는 디코딩된 데이터를 디코딩 버퍼로 순차적으로 전달한다. 디코딩 버퍼의 데이터가 충분히 쌓이게 되면 TV측으로 출력하여 멀티미디어 파일을 재생하게 된다. 그림5는 전체적인 소프트웨어 구조를 보인다.

### V. 실험 및 결과

구현 시스템의 제한수신시스템의 성능을 평가하기 위하여 수신 가능한 특정 가입자에 대한 가입자정보를 멀티미디어 방송 스트림에 포함하여 송출하고 송출된 방송 신호를 수신하였을 때 제한수신시스템이 가입자인지 정확히 판별하여 동작하는지 확인 하였다. 시스템의 멀티미디어 디코딩 성능은 H.264 비디오와 AAC 오디오 형태의 방송 스트림을 디코딩 하였을 때 비디오의 Macro block과 오디오의 끊김 및 노이즈 발생 여부를 판단하였다. 테스트에는 3종류의 스트림을 5분 동안 수신하여 디코딩 하도록 하였고, 동일한 방법으로 50회 반복하여 테스트를 수행하였다.

스트림 S1은 스크램블 하지 않은 전송 스트림으로 가입자 정보에 대한 데이터가 포함되지 않은 스트림이다. 따라서 제한수신시스템이 동작하지 않더라도 디코딩이 가능하다. 스트림 S2는 가입자에 대한 수신 제한된 정보를 방송 스트림에 포함한 스트림으로 처음 30초는 스크램블 되지 않은 상태이고 이후 30초에서 5분까지는 스크램블 된 상태의 스트림이다 따라서 스트림이 시작된 이후 30초 경과 후 제한수신시스템이 동작하여 역스크램블 여부를 판단하였다. 스트림 S3는 S2의 스크램블 되지 않은 구간과 스크램블 된 구간을 30초 마다 반복하도록 한 스트림이다. 따라서 스트림의 처음 30초 동안은 제한수신시스템이 동작하지 않고 30초에서 1분 동안은 제한수신 시스템이 동작하는 식의 과정이 반복된다. 표1은 테스트에 사용한 스트림과 테스트 결과를 보이고 있다.

표 1. 구현시스템에서 테스트 스트림에 대한 테스트 결과

구분	테스트 스트림	제한수신 시스템동작	비디오/오디오 상태
S1	스크램블 되지 않은 채널	정상	정상
S2	스크램블 된 채널	정상	정상
S3	스크램블이 구간별로 반복	정상	정상

### VI. 결론

본 논문은 유료 가입자에 대해서 수신 가능한하도록 제한하는 제한수신시스템을 적용하여 임의의 지역, 다수의 시청자를 대상으로 송출되는 방송에서도 수신 가능한하도록 제한하는 디지털 멀티미디어방송수신시스템이다. 이 시스템은 스마트카드와 소프트웨어 기법의 수신제한시스템을 사용하여 스크램블 된 전송 스트림을 역스크램블 하기 위한 키를 추출하므로 강화된 안전성을 제공한다. 구현된 시스템은 H.264 복호화 처리를 위한 DSP와 RISC가 있는 듀얼 프로세서를 사용하여 QVGA의 비디오와 24Khz~48Khz의 오디오 방송을 평균 15f/s로 재현이 가능하다.

### 참고문헌

- [1] Rafael C. Gonzalez and Richard E. Woods, Digital Image Processing, Prentice-Hall, 2002.
- [2] Fernando Pereira, Touradj Ebrahimi, The MPEG-4 Book, Prentice-Hall PTR.
- [3] Texas Instruments, TMS320DM270 CPU and Peripherals Technical Reference Manual, 2003.
- [4] 전형국, 마평수, "TI DSP 64x에서의 인코딩 시스템 및 디코딩 시스템 구현", 한국정보과학회 2003.10. VOL.30 NO.2-3 pp.316-318
- [5] 김범호, 마평수, "RISC와 DSP 듀얼 프로세서의 효율적인 비디오 신호처리 방법", 한국정보과학회 2003.10. VOL.30 NO.2-3 pp.676-678
- [6] steve furber, ARM system-on-chip architecture second edition, Addison-Wesley, 2000.
- [7] 이장원, 조현숙, "디지털 위성방송에서 IC 카드를 이용한 Pay-TV 서비스를 위한 가입자의 인증", 한국정보처리학회 '96추계학술발표 논문집, VOL.03 NO.01, pp.417~420, 1996.04
- [8] 조지만, 조현숙, "제한수신시스템을 위한 스마트카드에서의 가입자 인증", 한국정보처리학회 '96추계학술발표 논문집, VOL.03 NO.02, pp.850~853, 1996.10
- [9] 조지만, 조현숙, "관용 암호방식 사용 스마트카드의 해킹 대비 알고리즘 고찰", 한국정보처리학회 '97추계학술발표 논문집, VOL.04 NO.02, pp.1349~1353, 1997.10
- [10] 조현숙, 이상호, "제한수신시스템을 위한 키 관리 메카니즘과 성능향상 방안", 한국정보처리학회 논문지 VOL.05 NO.10 pp.2641~2653, 1998 . 10