特輯

CATV에서의 영상정보 보호기술

朱 聖 哲
電子部品綜合技術研究所

Ⅰ. 서 론

CATV는 광대역 케이블을 매체로 사용하여 다양한 영상채널 서비스를 제공하고 있으며 홈쇼핑, 홈뱅킹 등 요구즉시형 비디오(Video-On-Demand)등 쌍방향 서비스를 제공할 수 있는 시스템으로 발전하고 있다. 다양한 유료서비스가 제공됨에 따라서 점차 더욱 정교한 정보보호 대책도 개발되어 사용되고 있다.

CATV가 단순 중계 방송으로부터 다양한 채널의 서비스를 제공하는 시스템으로 발전해 나감에 따라 무허가 시청을 방지하기 위하여 단순한 RF 트랩(trap)을 사용하는 방법으로부터 중간 주파수 대역에서의 신호처리 기법, 기저대역 어드레싱 디스크램블러(baseband addressable descrambler)로 점차 정교해지고 있다. 또한 최근 전송 용량의 증가 및 서비스 기능의 향상을 위하여 디지탈 신호압축기법(MPEG)이 채택될 예정이며 디지탈 암호화 기법이 사용될 전망이다. CATV 시스템 전반의 효과적인 정보 보호를 위해서는 도시청이 불가능한 정교한 스크램블러의 선택과 함께 정당한 가입자만이 해독이 가능하도록 하는 엄격한 가입자 허가관리 절차가 통합되어야 한다. CATV시스템에서 필요한 서비스를 신청한 가입자에게만 제공하고 이를 회계정보와 연동시키기 위해서는 광대역 케이블 시스템에 연결된 각 컨버터가 적절한 고유번호를 가지도록 설계하여야 한다. 즉 각 가입자 컨버터의 고유번호는 매 서비스마다 주어지는 패스워드(password)를 해독하는데 사용되며, 과금시스템과의 연동에도 사용하도록 해야 한다. 본 기고에서는 먼저 CATV의 스크램블 기법에 관하여 비교 토의하고 한국형 CATV 시스템의 구현 사례를 소개한다.

Ⅱ. CATV의 정보보호와 스크램블 기법

CATV의 정보보호 시스템은 배치초기에는 성공적으로 도시청을 방지할 수 있으나, 시간이 경과함에 따라 다양한 도시청 기법도 개발되므로 시스템 설계시 불법도시청 기법을 구현하는데 드는 경비가 CATV에서 제공되는 서비스나 정보에 비교하여 비싸게 되도록 설계하여야 한다. 예를 들면 대부분의 도시청 기법이 가입자 컨버터를 개조하여 구현된다는 점을 감안하여 비교적 쉽게 적은 경비로 대책을 강구하기 위하여 smart card와 같이 교체가능한 부품을 사용하여 스크램블 시스템을 설계하는 것이 좋다. CATV 정보보호를 위한 시스템 설계시 고려할 사항들은 다음과 같다

- 허가 관리(conditional access) 시스템의 지속적 운영이 가능하도록 한다.
- 비화키를 배포하여 사용한다.
- 시스템 정보가 노출된 경우에도 쉽게 보완할 수 있어야 한다.
- 한 가지 서비스가 허가된 가입자에게 제공된 정보가 다른 서비스의 도시청에 도 움이 되지 않도록 한다.
- 가입자 장비의 디스크램블러 부품은 시중에서 쉽게 구할 수 있는 부품으로 대치 가 불가능하도록 설계한다.
- CATV 스크램블 기법은 단순한 RF 트랩과 같이 간단하게 대치 가능한 기법으 로부터 기저대

역 어드레싱 시스템, 디지탈 암호화 기법 등 다양하지만, 컨버터 가격에 영향을 미치므로 초기 시스템 설계시 최적 시스템을 신중하게 선택한다.

CATV 시스템에서는 정보를 보호하기 위하여 사용되는 대표적인 스크램블 기법들은 다음과 같다.

1. RF 트랩

가장 간단한 스크램블방법으로 협대역 저지 필터(notch filter)를 사용하여 신호를 제거해 버리는 것이다. 이 트랩 방식은 negative 트랩과 positive 트랩 방식이 있다. Negative 트랩은 필터의 중심 주파수가 영상 신호의 중심 주파수에 위치하여 영상 신호를 걸러내서 불법 가입자, 즉 트랩이 설치된 가입자들에게는 신호가 공급되지 않도록 하는 것이다.

Positive 트랩 방식은 가입자들에게 유상 채널 신호를 보낼때 간섭 신호를 섞어서 보내면 적합한 가입자들의 컨버터에 부착되어 있는 트랩이 이 간섭 신호를 제거하는 방식이다. RF 트랩방식은 각 라인과 채널마다 연결 또는 비연결 트랩설치를 필요로 하므로 널리 사용되지는 않고 있다.

2. 원격 제어형 트랩(Addressable Trap)

이 방법은 트랩방식에 고유번호를 부가하여 가입자의 고유번호에 따라 지정된 경우에 한하여 트랩이 기동하기 시작하여 유상채널을 보호하므로 중앙제어 가가능하도록 매 라인 및 채널마다 설치할 필요가 없어진다.

3. RF Interdiction

케이블 네트워크의 신호 송출기(headend)로 부터 제어되는 협대역 잡음 발생기(programmable noise generator)를 이용하여 대응되는 채널의 스펙트럼에 간섭신호를 혼합시킴으로써 시청을 제한하는 시스템이다.

4. 중간주파수대역 신호처리(IF Processing) 기법들

(1) 간섭 신호 삽입(Interfering Carrier)

TV 채널신호의 중간주파수대역에서 간섭신호를 삽입하는 기법이다. 수평주사 주파수의 고조파(harmonics) 주파수를 간섭신호로 사용하며 이 간섭신호는 복조기의 중간주파수 루프에서 lumi-nance carrier 위 2.5MHz에 삽입된다. 간섭 반송파를 제거하는 positive 트랩을 컨버터의 중간주파수대역 신호처리회로에 삽입하면 수신이 가능하게 된다.

(2) 영상 반전(Video Inversion)

영상반전 기법은 영상 신호를 180°위상반전시켜 전송함으로서 TV 수상기에 반전된 영상(명암과 색이 역전된 영상)이 나타나게 한다. 신호의 보안을 위하여 영상 반전주기를 예측하지 못하도록 하기 위하여 의사잡음 펄스열 (PN-pulse)을 영상반전 제어신호로 사용한다.

(3) 수평 동기 신호 압축과 이동(Horizontal Sync Suppression and Shifting)

수평 동기신호를 압축하거나 시간축상에서 이동시키는 방법으로 TV 수신기가 수평동기신호에 동기화시키지 못하도록 블랙레벨 이하로 압축한다.

CATV 시스템의 신호 송출기에서 변조시 이 방법에 의한 스크램블을 가하는데, 이때 부호기는 수평펄스열과 타이밍 시퀀스가 동일한 펄스를 만든다.

수신기에서는 진폭과 위상이 맞는 수평동기 신호용 펄스를 발생시킴으로써 원래의 동기신호를 복원할 수 있다. 보통 수직동기구간의 신호를 원래대로 전송하고 수신단에서는 이 수직동기신호를 사용하여 신호복원에 소요되는 수평동기신호의 위상을 동기화시킨다.

(4) 동기 신호 제거(Sync Removal)

동기신호를 완전히 제거하고 이 기간에 임의의 데이타 또는 정보를 전송시 키는데 사용한다. 이는 디지탈 음성정보나 스크램블 기법에 관한 정보를 포함하기도 한다. 수신기에는 동기신호 발생회로가 요구된다.

5. 기자대역 어드레싱 시스템

기저대역에서 비디오 신호에 대하여 인코딩과 디코딩을 수행한다. 기저대역 어드레싱 시스템은 적절한 비용으로 높은 신호 보안성을 얻을 수 있기 때문에 최근에 널리 사용되고 있다.

(1) Video Delay

비디오 라인의 시작시점을 무작위로 지연시키거나 빨리 전송함으로써 수신시 해독이 불가능하게 한다. 비디오 라인을 디지탈 변환후 지연시간을 조정하며, 수신부의 설계는 디지탈 변환후 역으로 조정하면 수신이 가능하다. 단 지연시간이 적은 범위에 있을 경우 수평동기신호를 지연시킴으로써 디지탈 변환이 필요없게 되므로 설계가 간편하게 된다.

(2) Cut and Invert

디지탈 변환된 비디오 라인을 임의위치에서 자르고 그 위치를 바꾼후 아날로그 전송하고 수신부에서 같

은 위치로 복원시킨다. 절단된 부위에서 고조파 신호가 발생하므로 적절한 신호처리가 이루어진다.

(3) Line Shuffling

비디오 신호를 디지탈 변환후 몇줄 또는 비디오 프레임신호 그룹에서 비디오 라인 그룹의 순서를 랜덤 패턴으로 뒤섞이게(shuffle)한후 아날로그 신호로 전송한다.

(4) Pixel Permutation

프레임이 디지탈화되고 픽셀(pixel) 위치들이 미리 약정된 알고리즘에 따라 변경한후 디지탈 비화 변경된 신호는 아날로그로 전송한다. 수신부에서는 디지탈 변환후 데이타를 원위치에 배치하여 비디오 신호를 복원한다.

6. 디지탈 비화 기법(Digital Encryption Technique)

이 기법은 매우 높은 정보 보안성을 가질 수 있으며 DES(Digital Encryption Standard)등 다양한 비화 알고리즘이 개발되어 운용되고 있으므로 디지탈 비디오 신호에 적용할 수 있다. 비디오 압축 기법(MPEG-II)을 사용하여 대화형 멀티미디어 서비스를 제공하는 차세대 CATV 시스템에서 널리 사용될 것으로 예상된다.

Ⅲ. 한국형 CATV시스템의 구현사례

한국전자부품종합기술연구소(KETI)에서는 CATV 시스템의 영상정보를 보호하고 종합유선방송국 운영의 자동화를 위하여, 소요되는 스크램블러 시스템과 가입자 관리시스템을 개발하였다.

CATV 가입자 관리시스템은 다양한 채널의 서비스를 자동화하고 프로그램 및 정보의 보호는 고장 점검 및 유지 보수 서비스 등을 제공하여야 한다. 허가된 가입자에게만 TV 프로그램을 선택적으로 제공하는 허가 관리시스템은 스크램블러 제어 신호를 발생시키고, 암호 키 전송을 제어하여 허가된 가입자들만이 정상적인 프로그램 수신이 가능하도록 하였다. 허가 관리시스템은 송신기와 수신기사이에서 많은 채널과 프로그램을 제어하며, 또한 빠른 속도의 데이타 서비스, 다중 운영자와 프로그래머를 위한 제어기능을 수행하도록 하였다.

스크램블러와 기저대역 어드레싱 디코더용 디스크램블러에서 사용되는 프로그램 제어 가능한 의사불규칙(pseudo-random) 시퀀스 발생기는 Gordon, Mills, Welch에 의해 제안된 알고리즘을 기본으로 구현하였다. GMW 알고리즘은 M-시퀀스에 비해 낮은 상관값과 상당히 긴 선형구간(linear span)의 시퀀스를 발생시킨다. GMW 시퀀스 발생기는 동기화를 위하여 키 데이타(key data)와 위상 데이타(phase data)를 필요로 한다. 변환 조절기는 암호화 키 데이타를 데이타 통신 채널을 통하여 스크램블러와 가입자 컨버터내의 디스크램블러에 전송하고, 위상정보는 out-of-band 비디오 신호와 함께 in-band 신호로 전송한다. 전자품종합기술연구소에서는 정보보호를 위하여 허가된 가입자에게만 선택적으로 프로그램을 제공하는 허가 관리 시스템을 다음과 같이 구현하였다.

1. 허가 관리 시스템

(1) 가입자관리 시스템

종합유선방송의 허가 관리시스템을 구현하기 위하여 서버/클라이언트 환경하의 데이타베이스를 구축하였고 아래와 같은 가입자 관리요구기능을 플렛포옴에 관계없이 구현할 수 있도록 하였다.

- 가입자의 청약, 설치, 해지 등 가입자 이력관리
- 신청서비스, 가입자 컨버터 및 댁내설비 관리
- 과금처리 및 청구서 발행 등 요금관리
- 유지보수관리
- 유료채널(PPV) 프로그램의 편성 및 운영을 지원하는 유료채널 관리
- 기술자료 지원, 영업분석, 경영관리를 위한 통계분석관리

종합유선방송국의 운영자동화에 소요되는 기능에 따라 가입자 청약접수처리, 프로그램편성, 과금관리, 유지보수, 사업관리 등을 개발하였다. 그림 1과 같이 클라이언트 컴퓨터는 IBM-PC 또는 호환기종을 사용하였고 네트워크환경을 구축하였으며 운영자의 편의를 위하여 그래픽 인터페이스(GUI)를 사용하였다. 컨버터 제어장치(CCU)는 각 클라이언트 컴퓨터에서 운영자에 의해 입력된 데이타베이스에 근거하여 고주파 데이타모뎀을 사용하여 가입자의 컨버터를 원격제어하고 프로그램 편성자의 입력자료에 따라 스크램블러를 제어한다. 컨버터 제어명령은 각사별로 개발모델간의 호환성을 유지하기 위하여 명령코드목록집을

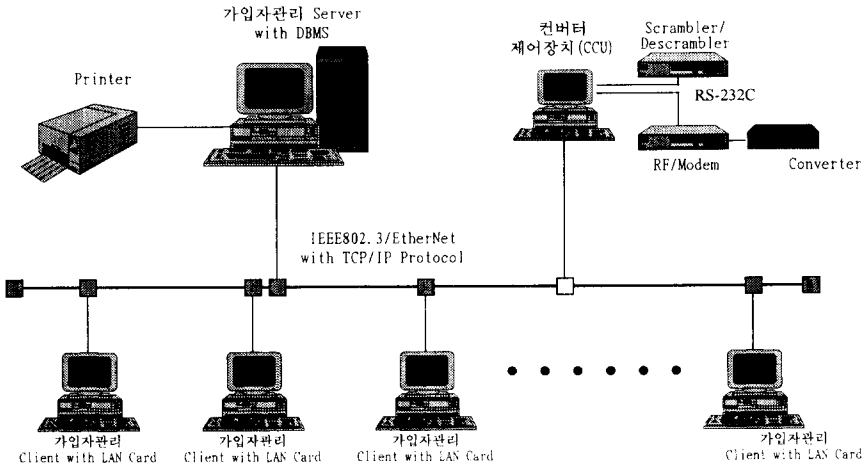

그림 1. CATV 시스템 구성도

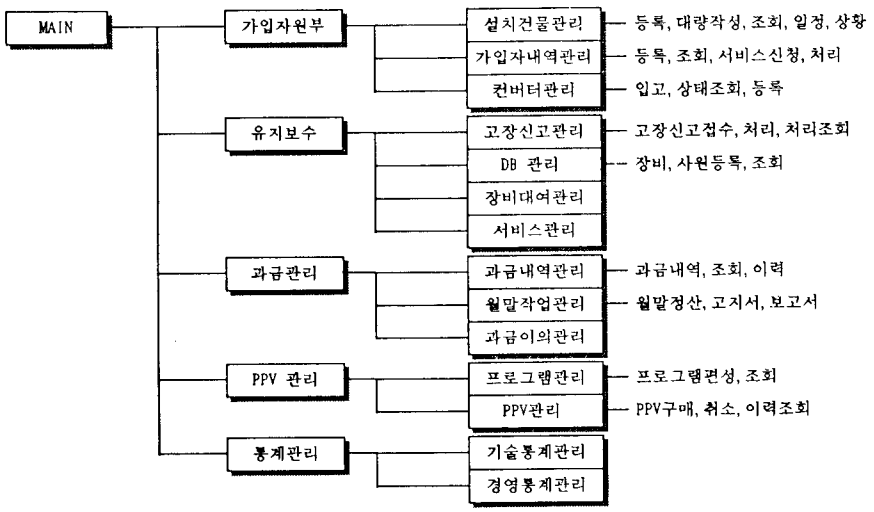

그림 2. CATV 가입자 관리 소프트웨어 구성도

종합유선방송협회 등을 통하여 배포하고 있다. 기본 소프트웨어는 가입자 원부관리, 가입자 내역관리, 컨버터관리, 유료채널관리를 포함하고 있으며 추가 소프트웨어 모듈은 추후 개발하여 보급할 예정이다.

⊙ 기본구성 및 주요특징

가입자관리 소프트웨어를 운용하기 위해 필요한 기본적인 하드웨어 및 소프트 웨어는 다음과 같다.

① 가입자관리 서버 하드웨어 :

SUN SPARC-10급 이상 서버

하드디스크(1GB이상) 및 주변기기

② 가입자관리 서버 소프트웨어 :

유닉스 운용 시스템 및 유틸리티

한글 관계형 데이타베이스 엔진 및 가입자관리 데이타베이스화일

③ 가입자관리 클라이언트 하드웨어 :

IBM PC-486 및 호환기종

Ethernet 인터페이스 카드 & 통신 프로그램

④ 가입자관리 클라이언트 소프트웨어 :

한글 WINDOW 3.1
ObjectView
Informix net PC
Ethernet 카드 및 드라이브 소프트웨어

⊙ 운영자 편의성

가입자 관리소프트웨어는 운영자의 편의를 위하여 MS-WINDOWS, ObjectView를 이용하여 그래픽 환경을 구축하였고 키보드 및 마우스 동시사용의 입출력환경을 개선하여 데이타를 입출력할 수 있도록 하였으며 전체업무(가입자관리 및 운영지원)의 일관된 화면을 구성하였다.

⊙ 가입자 규모 및 플랫포옴 선정

가입자 관리소프트웨어는 유닉스 프랫포옴을 서버로 사용하였고 관계형 데이타베이스를 사용하여 개발되어 유닉스컴퓨터 기종에 쉽게 이식이 가능하며 관계형 데이타베이스도 쉽게 교체 가능하다. 따라서 가입자의 숫자나 방송국의 규모에 따라 쉽게 시스템을 구축할 수 있다. 약 10만 가입자이내에서는 상위기종

표 1. 가입자 관리시스템 구성품

구 분	품 명	수량	기 능
하드웨어	WORKSTATION UNIT - 8 MB Main Storage - Disk Unit(400MB) - 1.2 GB Disk Unit - Catridge Unit - EIA 232/V 24 One Line20E - EIA 232/V 24 One Line - Ethernet(Thin) cable - Battery Power Unit	1 1 1 1 1 1 1 1 1	가입자관리서버(SUN SPARC-10) 주 기억 장치 보조 〃 (내장형) 보조 〃 (외장형) 카트리지 장치 통신라인 통신라인 케이블 클라이언트 접속용 전원공급 장치
	Monitor(HOST) - System Console용	1	호스트 모니터
	Client Terminal(PC-486급) - PC김용 터미날 - Ethernet Card - Ethernet Cable		사용자 터미널 겸 PC Ethernet 네트워크 연결용 Ethernet 네트워크 연결용
	프린터 - Line Printer - Serial 〃	1	고속라인 컴퓨터 24핀 시리얼 프린트
소프트웨어	운용 S/W - UNIX - 한글 모티프 - Informix RDBMS - Informix STAR - 통신용 소켓 프로그램 - 가입자관리운영 DB 구조	 1 1 1 1 1 1	 오퍼레이팅 시스템 한글 지원 데이타베이스 구축용 Informix Online Engine 전자부품연구소 프로그램 가입자관리용 데이타베이스 구조
	Client용 S/W - MS-DOS 6.0 - 한글 MS-WINDOWS 3.1 - Ethernet TCP/IP - INFORNET-PC - ObjectView - 운용 프로그램	 1 1 1 1 1 1	 오퍼레이팅 시스템 프로그램환경 통신용 프로그램 데이타베이스 접속용 운용프로그램 환경 개발 프로그램

표 2. 가입자 원부 관리 기능

기 능	주 요 내 용	비 고
가입자 자료 입력/수정	- 이름, 전화번호, 주민번호, 컨버터 비밀번호등 입력 - 가입자 과금 주기 및 거주형태 입력 - 신청서비스 등록	가입자 번호 자동발행
가입자 자료 조회	- 가입자 번호, 주민번호, 이름, 전화번호, 주소별 선택조회 • 일반 인적사항 • 신규 설치 일시 • 작업지시 내용 및 완료 여부 • 신청서비스 현황 • 요금내역 및 현황 • 설치 컨버터 내역 • 유료채널 신청 내역 • 고장신고 조회 • 요금 청구서 • 하우스 내역	작업지시 #별 관리
가입자 원부 출력	- 가입자 이력을 여러 기준에 의하여 분류 출력 • 신청 서비스기준 가입자 원부 • 댁내 설비 기준 가입자 원부 • 전화번호 리스트 출력	Sales Tool Parameter를 상세히 분류 선택하여 대상 선정
가입자 서신 작성및 발송	• DM 발송을 위한 주소 테이블 인쇄 • 가입자 서신 작성후 대상가입자 인쇄 발송	

의 워크스테이션으로 시스템 구현이 가능할 것으로 추정된다 그림 2는 가입자관리 소프트웨어 구성도이며, (표 1)에서 (표 6)까지는 각 모듈별 소프트웨어의 주요기능을 요약하여 설명하였다.

(2) 허가 관리 절차

그림 3은 허가 관리 시스템의 상향과 하향 제어 데이타의 흐름을 보인다. 먼저 상향의 흐름을 살펴보면 다음과 같다. 허가된 가입자가 프로그램을 요구하면 MCU에서 요구신호를 상향데이타 통신채널(24-30 MHz)중 지정채널을 통하여 전송하게 된다. 이 전송된 요구신호는 동축케이블을 통하여 헤드엔드의 모뎀을 통하여 컨버터 제어장치(CCU)에서 디코드되고 허가된 가입자인지를 확인받게 된다. 컨버터 제어장치는 서버에서 받은 가입자 원부를 검토하여 가입자의 서비스 요구가 타당한가를 확인하고 허가된 가입자이면 승인을 받아 서버에 있는 가입자관리 소프트웨어에 의하여 서비스를 받게 된다. 서버는 가입자원부관리, 유지보수, 유료채널관리업무를 수행한다. 허가된 가입자일 경우 하향데이타 통신채널(126.15-137 MHz)중 지정된 채널을 통하여 프로그램 태그와 PN_Key 어드레스를 디스크램블러로 전송한다. 한편 스크램블러는 프로그램 편성관리 계획에 따라 주어진 PN_Key 어드레스를 가지고 비디오 소스를 스크램블한다.

스크램블된 비디오 프로그램 태그와 PN_Phase는 통신채널(50-450 MHz)중 지정된 채널을 통하여 컴바이너로 인입된다. 프로그램 태그, PN_Key 어드레스, 비디오 프로그램 태그 및 PN Phase는 컴바인되

표 3. 작업처리 및 유지보수 관리

기 능	주 요 내 용	비 고
작업 환경설정	- 작업 가능시간 설정 • 작업 종류별 할당시간 설정 (Q코드) ・신규설치/서비스 추가/삭제 ・서비스 재개시 ・철거 ・연체자 서비스 차단 ・고장 신고 ・특별작업 신청 - 휴일 입력 관리	신규작업 접수시 잔여 가능 시간 고려 접수
작업 접수	- 작업 종류별 설치 작업 ・신규설치/이전/해지 ・가입자 인적사항 변경 - 기설치 등록된 장비의 유지 보수	자동 작업지시 # 생성 컨버터 교체
작업배정 및 처리	- 접수된 작업지시서 발행 ・일별 ・미해결 총 리스트 - 작업지시를 각 기술자에게 배정 - 각 기술자가 작업완료 입력 처리	기술자의 잔여작업 가능 시간 참조후 작업 배정
유지보수관리	- 기 설치된 장비의 유지 보수 ・재고장비 현황 출력 ・반품장비 현황 출력 ・장비이동 현황 출력 ・기술자에게 할당된 장비 현황 출력 - 고장 신고 처리 ・고장신고 내용 분석 ・고장 원인별 빈도 현황 ・지역별 고장 현황 - 일 및 월별 설치/철거현황 출력	

어 동축케이블을 통하여 컨버터에 도착하게 된다. 도착된 신호는 수신부의 필터에 의하여 (50-450 MHz)와 (126.15-137.85 MHz)의 두 통신채널로 나누어져 각각 튜너와 모뎀으로 인입된다. 모뎀으로 들어온 신호는 프로그램 태그와 PN_Key 어드레스로 변환되어 MCU로 전송되고 MCU에서는 디스크램블러에 PN_Key를 공급하게 된다. 한편 튜너로 전송된 신호는 스크램블된 비디오 프로그램 태그와 PN_Phase로 변환되어 디스크램블러에 공급된다. 디스크램블러는 공급받은 PN_Key, 프로그램 태그 및 PN_Phase를 가지고 디스크램블과정을 수행하여 비디오 신호를 정상적으로 수신할 수 있도록 한다.

(3) 스크램블러 및 디스크램블러 설계

스크램블러와 디스크램블러에서는 송신단에서 사용하기 위한 독립적인 랜덤변수의 샘플 시퀀스(sample sequence)와 수신단에서 사용하기 위한 샘플 시퀀스를 발생시켜야 한다. 효율적인 정보보호를 위하여 높은 선형복잡성(linear complexity)과 낮은 상관함수값(correlation value)을 가지는 의사불규칙 이진 시퀀스가 필요하다. 한국형 CATV 가입자 관리시스

표 4. 요금관리

기 능	주 요 내 용	비 고
요금 계산	- 각 가입자별 요금 선정 • 월정 요금 • 특수채널 요금 • 유료채널 요금 • 유지 보수료	유료채널 시청일 조정기에서 데이타 수신후 요금 산정
요금 청구서 발행	- 과금 작업항목 설정 • 청구일 기준으로 과금 주기 설정 • 작업 예정일 설정 - 청구서 발행	
수금 처리	- 수금내역 입력 • 일괄 수금내역 입력 • OTC 개별 입력 • 자동 이체 (bank draft) 등 - 수금내역 수정 - 수금내역 조회 및 현황 출력	작업건별 번호 및 운용자 자동 등록
요금 이의 신청 처리	- 가입자별 요금 이의 접수 확인 및 조치	
체납자 관리	- 가입자 요금 청구액 기준으로 체납자 선별 • 1 단계 · 체납자 연체 통지문 발송 · 체납자 출력 • 2 단계 · 체납자에게 최후 고지서 발송 · 가입자 킨비터 기능 자동 삭제 • 3 단계 · 가입자 서비스 철거 · 가입자 킨비터 철수	

템에서는 GMW 시퀀스를 사용하여 스크램블러 시스템을 구축하였다. GMW 시퀀스의 클락은 비디오 신호의 수평동기주기와 동기화하였으며 스크램블 범위는 선택가능하도록 논리회로와 통합구현하였다.

① GMW 시퀀스 특징 및 정의

GMW 시퀀스는 같은 주기의 M-시퀀스와 동일한 자기상관성을 가진 동일 주기의 M-시퀀스보다 매우 높은 선형복잡성을 가진다. 또한 GMW 시퀀스는 시퀀스가 낮은 선형복잡도를 가질때 시퀀스의 짧은 구간으로부터 전체의 시퀀스를 예측할 수 있는 Berlekamp-Massey알고리즘을 사용하는 공격에 대해 높은 수준의 암호학적인 보안성을 제공한다. GMW 시퀀스는 다음과 같이 정의된다.

M을 합성정수(M=JK)라 하면 GMW 시퀀스 $\{b_n\}$은 다음과 같이 정의한다.

$$b_n = tr_1^J\left\{\left[tr_J^M(a^n)\right]^r\right\}$$

여기서, a:GF(2^M)의 원시원(primitive element)
r: 2^J-1과 서로소($1 \le r < 2^J-1$)

여기서, 내부에 있는 trace함수 $b_n = tr_J^M(a^n)$ 는 유한체 GF(2^J)의 원소를 가지며 주기 2^M-1인 M-시퀀스이고, 만약 r = 1이면 전체의 시퀀스 {bn}은 M-시퀀

표 5. 유료 채널관리

기 능	주 요 내 용	비 고
프로그램 관리	- 유료채널 프로그램 작성 • 프로그램명, 시간 • 채널 및 태그 지정 • 스크램블 송신 및 신청 가능 시간 지정 - 자동 프로그램 활성화 - 할인 프로그램 별도 관리 • 야간 시청 프로그램 • 패키지 프로그램	컨버터 콘트롤러로 송신
유료채널 내역 수신	- 컨버터 킨트롤러에 접수된 가입자 유료채널 신청 내역 수신 - 가입자별 유료채널 내역 처리	
유료채널 시청현황 통계	- 프로그램별 유료채널 시청내역 통계 분석 • 요약 • 상세 출력	
연체 가입자 관리	- 서비스요금 이납자에 대한 유료채널 신청 기능삭제 - Credit Authorization 기능	

표 6. 통계관리

기 능	주 요 내 용
채널별 시청 현황	- 프로그램별 시청 현황 - 특정시간 각 채널별 시청 현황
유료채널 프로그램 시청 현황	- 유료채널 프로그램별 시청 현황 및 요금 현황
가입자 증감 현황	- 일별 가입자 증감 현황 - 기간별 가입자 증감 현황
서비스 신청 현황	- 가입자별 서비스 접수 현황 - 서비스별 가입자 현황
가입자 동록 현황	- 가입자 인적사항 출력
댁내 설비 현황	- 가입자 댁내설비 원부
입금 및 수금 현황	- 건별 입금 현황 - 기간별 입금 현황

스가 된다. 결국 GMW 시퀀스 $tr_1^J\left\{\left[tr_J^M(a^n)\right]^r\right\}$는 GF(2)로 매핑되는 M-시퀀스 $tr_1^M(a^n)$ 중 선택된 시퀀스를 선형결합한 것이다.

GMW 시퀀스의 주요 성질을 살펴보기로 한다.

• 자기상관특성(Auto-correlation Properties) : d_n 이 다음과 같은 실수집합의 원소를 가지는 GMW 시퀀스라 할 때

$$tr_1^J\left\{\left[tr_1^M(a^n)\right]^r\right\}, \quad a_n=(-1)$$

여기서, a는 $GF(2^M)$의 원시원이고 r는 2^J-1과 서로소($0 \le r < 2^J-1$)이어야 한다. $\{a_n\}$의 주기적 자기상관함수 $P(\tau)$는 다음과 같다.

$$P(\tau)=\sum_{n=0}^{2^M-2}a_{n+r}a_n=\begin{cases}2^M-1, & \tau=0 \bmod 2^M-1\\ -1, & \tau\neq 0 \bmod 2^M-1\end{cases}$$

이러한 결과는 모든 GMW 시퀀스의 주기적 자기상관함수가 M-시퀀스와 동일하고 r의 선택에 의존함을 알 수 있다. r = 1인 경우에는 이상적인 M-시퀀

스와 완전히 일치하게 된다.

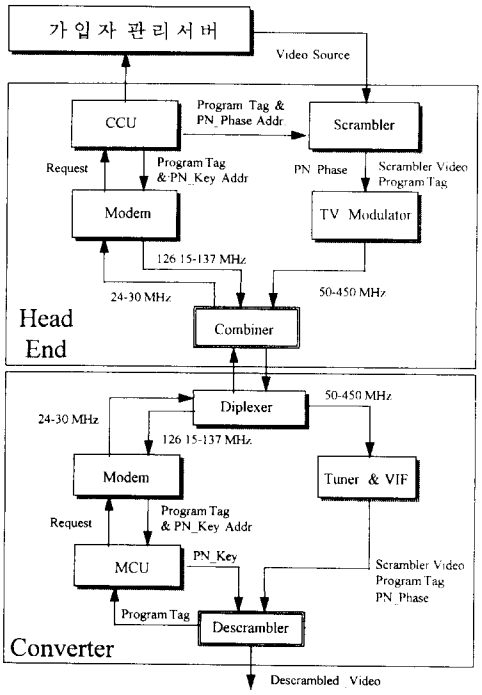

그림 3. 허가관리절차

• 선형 구간(Linear Span) :

시퀀스 {bn}의 선형 구간은 시퀀스{bn}에 의해 만족되는 선형 연속방정식이 존재하기 위한 최소차수를 나타낸다. 주기가 2^M-1이고 GF(2)의 원소들로 구성된 GMW 시퀀스 {bn}의 선형 구간은 다음과 같다.

$$L = J\left(\frac{M}{J}\right)^{w(r)}$$

여기서, w(r)는 r의 이진표현에서 1의 갯수를 나타낸다.

• Balance Property :

GF(2)에서 k-tuple을 c라 하고, {bn}의 한 주기 내에서 c의 발생횟수를 Nc라 할 때

$$(b_j, b_{j+1}, b_{j+2}, \cdots, b_{j+k-1}) = c$$

하나의 c만을 제외한 모든 경우에 대해 $Nc = 2^{M-k}$을 만족하면, {bn}은 "k-tuple balanced"라고 한다. GMW 시퀀스의 Nc는 다음과 같다.

$$N_c = \begin{cases} 2^{M-k} \; for \; c \neq 0, \; 1 \le k \le M/J \\ 2^{M-k} - 1 \; for \; c = 0, \; 1 \le k \le M/J \end{cases}$$

② 비디오 신호처리부의 설계

GMW 시퀀스는 비디오 신호의 위상반전제어에 사용된다. 따라서 각 비디오 라인간의 위상과 증폭이 잘 제어되어야 하며 정확한 동기를 이루어야 한다. 이를 위하여 반전시킨 신호와 원 신호간 differential gain과 differential phase는 각각 0.4 %, 1° 미만이 되어야 한다. (세부설계자료는 연구보고서 [18] 참고 바람)

Ⅳ. 결 언

CATV는 광대역 케이블을 매체로 하는 뉴미디어로서 기존의 매스미디어와 비교할때 보다 전문화되고 다양한 정보를 원하는 수요자에게 선별적으로 제공하는 시스템이다. CATV 시스템은 다양한 서비스를 제공하기 위하여 쌍방향 시스템으로 발전하였고, 차후 대화형 멀티미디어 서비스가 도입될 것으로 전망된다. 따라서 가입자의 다양한 서비스 요구에 부응하기 위해서는 가입자 관리시스템의 자동화가 요구되며 고가의 정보를 보호할 수 있는 정보보호시스템이 통합 운영될 수 있어야 한다. 한국형 CATV 가입자 관리시스템은 스크램블러와 허가 관리시스템, 그리고 주요 종합유선방송국의 운영자동화에 필요한 소프트웨어를 통합하는 시스템으로 개발되어 시험운영되고 있다. CATV는 정보화 시대에 부응하여 도입되는 뉴미디어로서 고도정보화시대가 진행되면서 더욱 광대역화되고 서비스도 더욱 전문화되고 다양해 질 것이다. 현재 개발진행중인 대화형 CATV 시스템은 요구즉시형 비디오, 홈쇼핑, 채택교육 등 다양한 서비스를 전제로 하여 비디오 압축기술을 채택한 디지탈 시스템이 될 것이다. 효율적인 차세대 CATV 가입자 관리시스템의 개발을 위해서는 암호기술은 물론 통신기술, 신호처리기술, 소프트웨어기술, 데이타베이스기술 등 다양한 기술이 필요하며 방송운영기술도 긴밀하게 협의하여 통합하여야 한다. 이미 개발된 한국형 CATV 가입자 관리시스템은 CATV 뿐만 아니라, 데이타베이스시스템, ADSL(Asymmetric Digital Subscriber Line)을 사용한 요구즉시형 비디오시스템 등에도 사용될 수 있을 것이다. 이를 위하여 개량

개발 및 지속적인 정보보호기술에 관한 연구가 진행되어야 할 것이다.

參 考 文 獻

[1] 서울대학교 자연과학대학, "CATV 가입자관리 시스템 기초연구", 전자부품종합기술연구소, 1993.

[2] 전자부품종합기술연구소, "KCATV 개발단 연수회 보고서", 1992.

[3] 성균관대학교 부설 과학기술연구소, "PN 시퀀스 발생기를 이용한 Scramble 기법에 관한 연구", 전자부품종합기술연구소, 1993.

[4] Zenith Electronics Corporation, "Zenith Command Series PM Controller", 1990.

[5] John McCormac, "Enropean Scrambling Systems(Circuits, Tactics and Techniques)", Waterford University Press, 1991.

[6] Brent Gale and Frank Baylin, "Satellite and Cable TV Scrambling and Descrambling", 1986.

[7] Rudolf F. Graf and William Sheets, "Video Scrambling & Descrambling for Satellite & Cable TV", Howard W. SAMS & Company, 1987.

[8] Graham S. Stubbs, "Conditional for Compression Systems : desirable attributes and selection criteria", pp. 18-19, 34-35, Communication Technology, November, 1993.

[9] Tomy Wechselberger, "Conditional Access and Encryption Options for Digital Systems", pp. 20-22, 36, 38-39, Communication Technology, November, 1993.

[10] The Great Lakes Data Systems, "Enhanced Cable Billing Systems", 1993.

[11] Information Systems Development Inc., "Cable Master", 1993.

[12] Zenith Electronic Cor., "Addressable Control System : Cable Products", 1993.

[13] Cable Data International , "Managing Subscribers, Growth & Service", 1993.

[14] Titan Cor., "Titan Cable Television Security Systems", 1993.

[15] Titan Cor., "Integrated Solutions : Supporting Cable Wireless and Interactive Multimedia Applications", 1993.

[16] Sky Channels CATV 센터 계산기부, "제 2회 호텔단말 강습회 자료", 1993.

[17] (주)국제항업, "LCAP : CATV 케이블망 설계 지원 시스템", 1993.

[18] 전자부품종합기술연구소, "한국형 CATV 가입자 관리시스템 개발에 관한연구", 1994.

筆 者 紹 介

朱 聖 哲

1951年 5月 21日生
1974年 2月 서울대학교 전자공학과 졸업(학사)
1991年 8月 Univ. of California, Irvine(박사)

1976年 10月 ~ 1977年 7月 현대조선
1977年 8月 ~ 1985年 12月 국방과학연구소
1986年 3月 ~ 1991年 12月 Univ. of California, Irvine
1992年 10月 ~ 현재 전자부품종합기술연구소

주관심 분야 : DSP, CATV, 전자의료기기