通信情報保護學會誌
第3卷 第3號, 1993.9

위성방송을 위한 TV 신호의 암호화 기술 동향

원치선*, 김재공**

1. 서 론

현재 미국, 유럽, 그리고 일본에서는 위성방송을 이용한 한정수신(conditional access) 시스템의 TV 방송이 실용화되고 있다. 한정수신 시스템은 TV 프로그램이나 데이타 서비스를 요금을 지불한 가입자(subscriber)들에게만 정상적으로 제공하고 그렇지 않은 미가입자들은 시청할 수 없도록 하는 유료방송이다. TV 프로그램의 한정수신이 가능하게 되면, 방송업자들은 특정 TV 프로그램이나 특정 채널을 시청하는 가입자의 수를 파악할 수 있고, 가입자 수에 비례한 광고비를 산정할 수 있다. 또한, 광고없이 가입자로부터 받은 시청료만으로 방송사를 운영할 수 있게 되어, 전문 채널의 탄생이 가능하다. 한정수신의 다른 용도는 방송의 수신 지역을 스크램블링(scrambling)을 통하여 한정하는 것이다. 즉, 원하지 않는 지역에 방송 전파가 도달하여 발생하는 전파월경(電波越境)의 문제를 한정수신 시스템의 도입으로 해결할 수 있다.

TV 방송의 가입자 개념은 이미 CATV(Cable TV)에 적용되고 있다. 그러나, 현존의 CATV 시스템은 아나로그 전송 방식에 기초하며, 스크램블링을 적용하여 신호를 보호할 수도 있으나, 케이블의 접속 유무에 의해 가입자와 미가입자를 쉽게 차별할 수 있다. 그러나, 인공위성의 출현이래 위성의 상업 목적의 이용 확장은 가입자 개념의 TV 방송을 CATV에서 인공위성에 의한 직접위성방송(DBS : Direct Broadcasting by Satellite)으로의 전환을 촉진시키고 있다. 직접위성방송은 무선방송으로, 가입자와 미가입자가 모두 같은 전파를 수신한다. 그러므로 암호화를 통해 신호를 변형하고 암호화된 신호를 해독할 수 있는 키(key)를 갖고 있는 수신자만 수신된 신호를 정상적인 프로그램으로 환원할 수 있게 하여, 가입자와 미가입자를 차별한다.

미래의 TV 방송을 논할때 직접위성방송과 함께 고려해야할 기술적 동향은 신호 전송의 디지탈화 추세이다. 즉, 1980년대에는 음성신호의 디지탈 전송화가 있었다면, 1990년대에는 영상신호의 디지탈 전송화가 이루어질 것으로 기대된다. 유료방송의 가입자 개념은 전송 신호를 디지탈화하므로써 더욱 높은 비화도를 갖고, 다양한 서비스가 가능하다. 또한 아나로그 신호의 스크램블링에서 볼 수 있는 신호의 열화 현상을 디지탈 신호에 대한 스크램블링에서는 발견할 수 없어 수신측에서 원래의 신호를 정확히 복원할 수 있다. 국내에서도 1995년 발사 예정인 무궁화 위성의 전송방식으로 디지탈 방식이 채택될 것으로 전망되고 있다.

본 고에서는 유료방송을 위한 TV 신호의 보호방

* 동국대학교 전자공학과 조교수
** 동국대학교 전자공학과 교수

식의 기술적 동향을 파악하고, 신호를 디지탈화하여 압축하고 디지탈 전송하는 완전 디지탈(all digital) 전송 시스템에서의 스크램블링 방식을 예견하고자 한다.

2. TV신호의 한정수신 기술

TV 신호의 한정수신 기술은 기능면에서 다음과 같이 양분될 수 있다. 첫번째는 원래의 프로그램 신호 형태를 변형하는 스크램블링(scrambling)과 변형된 신호를 수신측에서 다시 원래의 신호로 복원하는 디스크램블링(descrambling) 기술이고, 두번째 기술은 디스크램블링에 필요한 관련키와 각 수신자들의 시청 자격(entitlement)을 관리하는 자격관리 및 통제 기술이다. 자격관리 및 통제 기술은 스크램블링에 사용한 키를 암호화하고 그것과 프로그램의 취득 조건을 자격통제 메세지(entitlement checking message)내에 포함시켜 전송하는 자격통제 기능과 각 수신자의 자격 유효기간등 개별정보를 자격관리 메세지(entitlement management message)내에 포함하여 분배하는 자격관리 기능으로 구분할 수 있다.[1] 이러한 기능 블럭을 포함한 한정수신 시스템의 기본구성은 그림 1과 같다.[2]

그림 1의 기본구성에서 기술 내용이 공개된 부분은 스크램블링과 디스크램블링이다. 단일 방송 업자에 의한 방송의 난수 발생기는 보통 공개되지 않으나, 같은 수신기로 여러 방송업자의 방송을 수신할 수 있도록 하기 위해서는 난수 발생기가 공개되어 후발 방송 사업자도 공개된 방법에 맞추어 사용할 수 있도록 한다. 암호기와 복호기의 알고리즘도 같은 이유로 공개된다. 그러나, 이때 사용한 암호화 키는 방송 사업자마다 비밀로 유지한다. 본 절에서는 암호화 키의 비화도와 스크램블링 방식에 대해 기술한다.

2.1. 비화도(Level of Security)

비화도는 미가입자들이 스크램블링된 TV 신호를 불법으로 디스크램블링하여 원래 신호의 복원을 시도하는 일의 난이도를 말한다. 군용시스템의 암호화는 높은 비화도를 가지며 사용하다가 비화도가 저하되면, 상용화 조건을 충족하도록 다소의 수정과 보완을 가한후, 상용화되는 것이 일반적이다. 그러므로 현재의 위성방송용 암호화 방법을 포함하여 일반적으로 상용화된 통신용 암호화는 군용보다 비화도가 낮다. 참고로 방송 분야의 암호화는 암호키가

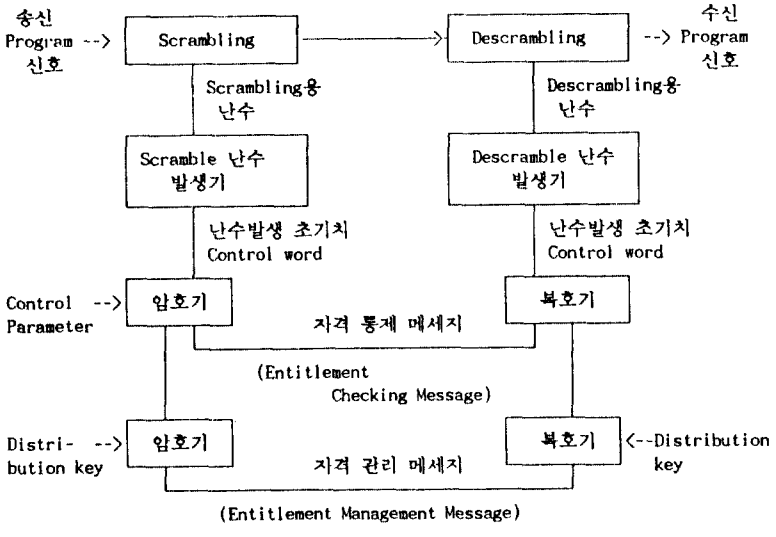

그림 1. 한정수신 시스템의 기본구성

누설되어 도시청(hacker)이 발생하여도 수신자들에게 직접적으로 가해지는 피해가 불명확하다는 것이 일반 통신용 암호화와 다른 점이다.

한정수신 시스템은 통제취득(controlled access)과 공개취득(open access)으로 나눌 수 있는데, 예를 들어, 각 수신자의 자격조건을 전파로 별도의 채널을 통해 전송하는 전파 어드레싱(addressing) 방식에서는 방송업자가 각 수신자의 디스크램블러를 강제로 ON/OFF 시킬 수 있다. 반면에 공개취득에서는 사용자의 디스크램블러를 시스템 소유자가 통제할 수 없다. 그래서 통제취득이 공개취득보다 비화도가 높다. 최근 TV 신호가 디지탈화되면서 가입자들에 대한 시청 서비스를 프로그램 제공자가 통제할 수 있는 통제취득 시스템이 채택되고 있다.

2.2. 스크램블링

신호의 스크램블링은 영상, 음성, 데이타등 신호의 종류에 따라 다르며 신호의 전송 및 처리형태가 디지탈이냐 아나로그냐에 따라서도 달라진다. 본 고에서는 신호가 디지탈 신호로 바뀌어 스크램블링되면 디지탈 스크램블링으로 부르고 그렇지 않으면 아나로그 스크램블링으로 부른다. 디지탈 스크램블링에서도 특히 전송시 제한된 대역을 고려하여 비트 전송율을 낮추는 데이타 압축을 포함하고 디지탈 신호를 디지탈 변조하여 전송하는 완전 디지탈 TV 시스템에서의 스크램블링 방식은 구별한다.

위성방송의 음성신호는 디지탈화된 음성신호에 의사 랜덤 이진열(pseudo random binary sequence)을 연속적으로 가산하는 방식으로 암호화하는 것이 일반적이다. 수신측에서는 같은 의사 랜덤 이진열을 발생하여 원래의 신호를 복원한다. 의사 랜덤 이진열의 초기치는 암호화되어 전송되고 일정주기로 변화된다. 예를들어, 유럽의 multiplxed analog component (MAC) 방송의 EuroCypher에서는 음성신호를 디지탈화하여 의사 랜덤 이진열(PRBS)을 가산하여 암호화하고, 이때 사용한 PRBS의 초기치는 DES(Data Encryption Standard)로 암호화되어 전송된다. 미국의 MA/COM에서 개발된 Digi-Cipher Ⅱ는 DES 방법으로 음성신호를 암호화하여 높은 비화도를 얻는다.

종래의 비디오 스크램블링 방식은 TV의 비화상 부분, 즉 동기신호(sync pulse)등을 변형하거나, 영상신호를 특정 파형의 신호로 변형을 가하거나, 파형을 반전(inverting)하는 등의 아나로그 스크램블링 방식을 사용하였다. 그러나 아나로그 방식으로 스크램블링하면 디스크램블링시 화질열화가 발생할 수 있고 동기(sync) 신호를 삭제 또는 변형하였으므로 VCR에 녹화할 수 없는 등의 단점이 있다. 최근에는 주사선 이동, 주사선 회전, 또는 주사선 교환등의 디지탈 스크램블링 방식을 사용하여 주사선 내 또는 주사선 간의 정보의 위치를 바꾸어 비화도를 높이고 있다.[3,4] 이때 스크램블링된 영상 정보를 전송하는 순서는 발생된 의사 난수로 정하였다. 발생된 의사 난수의 초기치는 암호화되어 각 수신자에게 전송된다. 초기치의 암호화를 위해 모든 디스크램블러가 서비스 키를 가지고 있으며 이 서비스 키는 스마트 카드(smart card)내의 IC나 기판상의 RAM 등에 기록되어 있으며 디스크램블러가 공개되면 그 내용이 지워지도록 설계되어 외부로부터의 불법 복제를 통제하고 있다. 서비스 키는 시스템 소유자에게만 알려져 있으며 그 코드를 이용하여 난수의 초기치를 암호화하는데 사용된 키가 암호화 된다. 스크램블링용 관련 키의 암호화는 다음 절의 자격통제 및 관리에서 다시 설명한다. 대표적인 비디오스크램블링 방식을 표1에 제시하였다.

표1의 주사선 이동, 주사선 회전, 주사선 교환 방식은 디지탈 스크램블링 방식으로 분류될 수 있다. 그 외에 가산 암호 방식, 인덱스 치환 방식, DCT (Discrete Consine Transform) 계수의 암호화 방식 및 그들의 혼합 방식들이 있다.[4] 가산 암호 방식은 의사 난수 계열과 원신호의 이진 수열을 가산하여 암호화하는 것이다. 인덱스 치환 방식은 벡터 양자화기의 코드북 인덱스를 치환하는 것이다. 이들 방법들은 디지탈화된 신호에 쉽게 적용될 수 있으나, 영상의 높은 중복성(redundancy) 때문에 비화도가 떨어지므로 여러 방법의 혼합된 형태로 사용한다. DCT계수의 암호화 방식은 DCT의 에너지 집중 특성을 이용하여 DCT의 저주파 성분만 암호화한다.

비디오 신호가 디지탈화되고 블럭 단위로 압축되어

표 1. 비디오 스크램블링 방식

스크램블링방식	방 법 및 효 과	특 징
극성 반전	line, field, 혹은 frame 단위로 비디오 신호의 극성을 반전 => 동기신호가 안맞아 신호가 흐름.	디스크램블링시 열화 발생
방해파 중첩	TV 신호 대역의 임의의 좁은 대역 (보통 2.25MHz 주위)에 잡음신호 삽입 => 화면내 비트현상 및 음성의 방해 잡음 발생함.	수신측 Notch filter 사용시 화질 열화
정현파 승산	송신측에서 정현파로 변조된 신호를 수신측에서는 그 정현파의 180° 위상차를 갖는 정현파를 더하여 복원 => 화면의 중앙에 동기 부가 위치함.	수신측에서 정현파를 정확히 재생할 수 없을 때 화질 열화 발생
동기신호 제거	수평 동기 신호를 임의의 크기로 감쇄시킴. 감쇄 정도는 부호화하여 영상 신호와 함께 전송 => 동기가 고정되지 않고 흐름.	화질 열화 적음
주사선 이동	영상신호의 시작점을 매 주사선마다 좌우로 이동시킴 => 영상이 수평 방향으로 흩어짐.	처리가 용이함(shift register 사용)
주사선 회전 (line retation)	주사선마다 임의의 신호 구간을 중심으로 신호의 전송 순서를 바꿈 => 영상이 수평 방향으로 흩어짐.	비화도가 상대적으로 높음
주사선 교환 (line permutation)	한 화면내 주사선의 전송순서를 임의로 바꿈 => 화면이 수직 방향으로 흩어짐.	교환 주사선의 수가 많을수록 비화도가 높아지나 라인 메모리의 수가 증가하여 가격 상승

디지탈 전송되는 완전 디지탈 전송 TV에서는 한 화면 또는 화면내 블럭에서 데이타의 전송 순서를 바꾸는 것이 용이하여 스크램블링을 쉽게 구현할 수 있다. 그런데 영상 데이타를 압축하면서 버퍼(buffer) 통제를 원활히하고, 가변장 부호화(variable length coding) 채택시 정보의 량에 따른 적절한 비트 할당을 위해 압축전 DCT 블럭을 혼합(shuffling)하여 정보량을 분산시킨다거나,[5] ECC 부호화후 전송전에 데이타를 혼합하여 전송로에서의 군집 에러(burst error)를 수신측에서 ECC 복호화 이전에 데이타 정렬(deshuffling)로 랜덤(random)화하는 등의 데이타 혼합 기법이 완전 디지탈 시스템의 영상 압축 및 전송을 위해 이미 제안되었으므로 이들 방법과 연계하여 암호화 스크램블링을 하면 더욱 경제적으로 다기능의 스크램블링을 이룩할 수 있을 것이다. 예컨대, 미국의 HDTV 방식 제안자 중의 하나인 Zenith와 AT&T의 DSC-HDTV는 완전 디지탈 전송방식을 채택하고 있으며 전송 포맷은 마치 NTSC의 그것과 유사하다. 즉, NTSC의 한 프레임당 525개의 주사선에 해당하는 525개의 데이타 세그먼트(data segment)가 1/29.97 초 동안 전송된다. 이때 DSC-HDTV의 심볼은 1bit 또는 2bit로 구성된 디지탈 데이타이며, 한 주사선 시간(63.5μsec)과 같은 시간에 전송되는 한개의 데이타 세그먼트는 684개의 심볼로 이루어져 있다. 이 데이타 세그먼트는 마치 디지탈 신호 전송의 패킷(packet) 단위로 볼 수 있으며 262 또는 263개의 데이타 세그먼트가 모여 마치 한 필드(field)에 해당되는 데이타를 이루고 525개의 데이타 세그먼트가 1/29.97초 만에 전달되어 하나의 프레임(frame)에 해당되는 데이타를 형성한다.[6] DSC-HDTV에서는 각 데이타 세그먼트당 10 byte까지의 에러를 정정할 수 있는 RS 코드를 부여하고 있지만 전송시 채널 간섭등의 원인으로 발생하는 군집 에러에 대비하여 전송전 데이타를 혼합하는

인터리브(interleave)를 사용한다. 즉, 130 데이타 세그먼트를 단위로 한 세그먼트간 인터리브(inter-segment interleave)나 데이타 세그먼트내 인터리브(intra-segment interleave)를 한다. General Instrument사가 미국의 HDTV의 표준안으로 제안한 Digicipher 시스템도 완전 디지탈 전송 시스템이며 전송전에 데이타를 섞는 인터리브 과정을 포함하여 군집에러를 랜덤 에러화한다. Digicipher 시스템의 부호기는 그림 2에서와 같이 트렐리스(Trellis) 부호화와 RS 부호화를 결합한 연접 부호화(Concatenated coding)로서 트렐리스 부호화는 내부호로 RS 부호화는 외부로로 사용한다.[7] 인터리브 #1에서는 트렐리스 디코더에 의해 발생되는 군집에러를 확산시켜 RS 디코더의 성능을 향상시키고 인터리브 #2에서는 외부 충격에 의한 군집에러를 정정하는데 사용된다. 물론, Digicipher나 DSC-HDTV가 모두 NTSC의 525 라인의 주사선에 해당하는 전송 패킷을 갖고 있으므로 기존의 주사선 회전 및 주사선 교환의 개념이 [illegible]HDTV에도 적용될 수 있다. 또한 이들 [illegible] 전송 포맷이 NTSC의 전송 포맷과 유사하고 [illegible] 대역내로 전송되는 HDTV와 NTSC의 동시방송(simulcast) 방식을 채택하고 있으므로 NTSC의 디지탈 전송도 같은 포맷을 갖도록 영상 신호가 압축될 것이며, NTSC의 디지탈 위성방송으로부터 HDTV의 방송까지 같은 스크램블링 방식이 사용될 수 있다.

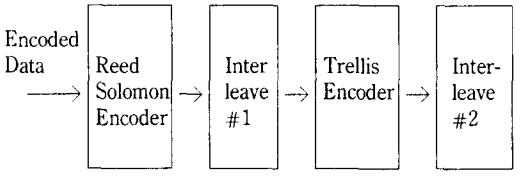

그림 2. Digicipher의 부호화기 블럭 다이어그램

2.3. 자격의 통제 및 관리

자격(entitlement)의 통제 및 관리는 프로그램을 디스크램블링하는데 필요한 관련키와 수신자의 시청 자격을 통제 및 관리하는 것으로 자격통제(entitlement checking)와 자격관리(entitlement management)로 대별할 수 있다.[1,8] 자격통제는 난수 발생의 초기치인 콘트롤 워드(control word)를 암호화하고 그것을 자격통제 메세지 내에 넣어 전송한다. 자격통제 메세지는 보통 한개의 데이타 패킷으로 구성되어 주기적(예컨데, 매 0.5초)으로 전송되며 그 때마다 새로운 콘트롤 워드가 암호화되어 전송된다. 콘트롤 워드(즉, 의사 난수 발생기의 초기치)를 주기적으로 바꾸는 것은 스크램블링의 의사 난수의 규칙성을 쉽게 찾을 수 없도록하여 비화도를 높이려는 것이다. 자격통제 메세지 내에는 암호화된 콘트롤 워드 외에 프로그램 정보와 취득 파라미터(access parameter)가 함께 전송된다. 모든 수상기는 발송된 자격통제 메세지를 수신하며 그중 콘트롤 워드와 취득 조건(access condition)을 수상기와 접속된 스마트 카드로 전달하고 스마트 카드에서는 프로그램 취득 조건 및 자격을 심사한 후 정당한 수신자로 판정되면, 스마트 카드내의 서비스 키를 이용하여 콘트롤 워드를 해독하고 디스크램블링에 필요한 난수의 초기치를 발생한다. 자격통제 메세지의 송수신은 자격 통제 메세지 내의 주기 계수기(period counter)에 의해 방송 프로그램과 동기화된다.

자격관리는 수상기의 보안 장치인 스마트 카드 내의 자격을 부여하거나 갱신하는 기능을 맡고 있으며 확장된 자격관리 시스템에서는 각 수신자의 어드레싱 기능을 이용하여 수신자들의 서비스 키를 바꾸거나 통제하는 통제취득도 가능하다. 자격관리 기능은 미래의 프로그램 수신자격에 대한 정보관리 기능이므로 배치(batch) 동작으로 실행된다. 그러므로 자격관리 정보는 자격통제 메세지와는 달리 프로그램과 동기화되어 전달될 필요는 없고 자격관리 메세지(entitlement management message)를 형성하여 특수채널을 통해 방송되거나 우편등의 매체로 전달된다.

자격의 전송 기술의 관점에서 보면 프로그램 정보는 프로그램과 동기되어 정확한 정보를 보내기 위해 전송시 발생하는 오류에 대한 대책이 중요하고, 반면에 자격 관리(개별정보)는 각 가입자에게 해당 정보를 전송하므로 많은 용량의 정보를 보내기 위한 기술과 계약내용 등을 고치지 못하게하는 기술 등이 중요하다.

자격은 상용화의 형태에 따라 가입(subscription)과 Pay-per-view(PPV)로 나눌 수 있다. 가입은 수신 가능 기간을 표시하여 자격 통제 메세지 내의 취득 파라미터가 현 방송 프로그램의 일시를 나타내고 그 파라미터가 스마트 카드 내의 수신가능 기간 내에 있는지 확인하여 자격을 통제한다. PPV는 이벤트(event)를 단위로 프로그램을 선택하는 것으로 사용 가능 토큰의 수로 자격을 통제한다.

3. 시스템의 사례 연구

현재 스크램블링 방식을 도입한 유료방송은 북미, 유럽, 그리고 일본에서 실용화되고 있다. 그동안 여러 스크램블링 방식이 제안되었지만 핵커(Hacker)의 탈생과 디지탈 TV 신호 처리의 기술 및 반도체의 발달로 새로운 스크램블링 방식이 계속 제안되고 있다. 본 절에서는 이들을 지역별로 나누어 살펴보기로 한다.

3.1. 북 미

미국의 사실상의 표준 방식으로 사용되었던 VideoCipher Ⅱ는 음성신호를 디지탈화하고 DES(Data Encryption Standard)로 암호화하여 높은 비화도를 주고, 영상신호는 기존의 아나로그 방식을 사용하여 보통수준(moderate level)의 비화도를 유지한다. 즉, 영상정보보다 음성정보의 비화도를 높게하고 있다. 그 이유는 음성은 영상보다 디지탈화가 쉽고 처리가 경제적이기 때문이다. 또한, 디스크램블러용 디코더(decoder)가 일반 소비자들의 내구성 소모품으로 취급되어 가격이 저렴해야 한다는 전제조건이 있기 때문이다. 그러나 최근 미국에서 HDTV의 방식 선정에 TV 신호의 스크램블러 제작업체인 General Instrument사가 완전 디지탈 전송 방식의 DigiCipher를 제안하므로써 완전 디지탈 전송시스템용 새로운 스크램블러의 탄생을 예고하고 있다. 완전 디지탈 전송시스템에서의 스크램블러는 현재의 TV 신호를 A/D, D/A하여 스크램블링하던 디지탈 TV 때보다는 더욱 저렴하게 제작할 수 있고, 반도체 가격의 하락과 함께 더욱 높은 비화도의 새로운 스크램블러가 탄생될 것으로 기대된다. VideoCipher Ⅱ에서 영상 신호의 수평 동기 신호는 제거되고 88bit의 디지탈 데이타로 대치된다. 이 디지탈 데이타에는 56bit의 키 암호화 관련 데이타(콘트롤 워드)를 포함, 스테레오 디지탈 오디오, 서비스 정보, 그리고 동기신호 발생정보 등을 싣고 있다. 이와같이 음성신호는 디지탈 암호화되고, 영상신호는 수평 동기신호가 제거되고, 비디오 신호는 반전되어(inverted) 아나로그 스크램블링된다.

VideoCipher Ⅱ가 미국의 많은 프로그램 제공자들에 의해 사용되면서 대중화되고, 또한 많은 핵커가 발생하여 VideoCipher Ⅱ의 비화도를 크게 떨어뜨려서 General Instrument사는 비화도를 높인 Video Cipher Ⅱ+를 1990년에 발표하였다. VideoCipher Ⅱ에서는 암호화를 위해 프로그램 제공자가 사용할 수 있는 bit의 수가 56개였는데 VideoCipher Ⅱ+에서는 256 개로 늘어났고, pay-per-view(PPV) 채널을 위한 Viedo Pal unit을 선택사양으로 쓰고 있다.

VideoCipher Ⅱ+의 존속 기간은 예측하기 어렵지만 VideoCipher Ⅱ+의 제안자인 General Instrument사가 완전 디지탈 전송시스템을 위한 DigiCipher를 미국의 HDTV(NTSC 포함)의 규격으로 제안하고 있어, VideoCipher Ⅱ와 VideoCipher Ⅱ+가 사멸하고 DigiCipher (또는 그에 상응하는 완전 디지탈 전송 시스템)를 위한 새로운 방식이 제안될 가능성이 높다. 완전 디지탈전송 시스템을 위한 새로운 스크램블링 방식은 영상 신호의 비화도를 높이는 방식이 될 것이다.

3.2. 유 럽

유럽의 여러 스크램블링 방식 중에 대표적인 시스템은 VideoCrypt, EuroCypher, EuroCrypt D2 MAC/P 등이다.[9] VideoCrypt 시스템의 영상 스크램블링 방식은 주사선 회전(line rotation) 방식을 사용한다. 즉, 각 비디오 주사선상에 256개의 가능한 절단점(cut point)을 선정하여 절단점을 중심으로 회전시키는 방식이다. 절단점은 난수 발생기로부터 얻고, 난수 발생기의 초기치는 RSA 알고리즘에 의해 암호화된다. VideoCrypt의 디스크램블러는 스마트

카드내에 장착되어 있는 서비스 키와 자격조건들을 바탕으로 디스크램블링한다. 각 가입자의 스마트 카드는 3개월마다 갱신되어 우편으로 전달된다. VideoCrypt의 음성 신호는 스크램블링되지 않는다.

EuroCypher는 북미의 VideoCypher의 유럽식 변형으로 유럽의 D-MAC 시스템에 사용되고 있다. D2MAC/P-EuroCrypt는 EuroCypher와 유사한 방식으로 D2MAC에서 채택하고 있다. MAC 방식의 영상신호는 휘도신호와 색차신호가 시분할 다중되어 있으므로 EBU에서는 MAC/Packet을 위해 절단점이 휘도와 색차신호 대역에 각각 한개씩 있는 2-cut 주사선 회전 방식의 스크램블링을 추천하고 있다. 디지탈 음성 신호는 의사 난수 발생기로 발생된 난수와 가산되어 암호화되고 의사 난수 발생기의 초기치는 DES 알고리즘으로 암호화된다. 자격관리를 위한 개별정보는 전파, 스마트 카드, 혹은 키보드(key board)로 전달된다.

3.3. 일 본

일본은 현재 NTSC 위성방송 2채널, JSB 1채널, 그리고 하이비젼에 1채널을 할당하고 있다. 일본 최초의 유료 방송인 JSB는 현재 방송시간의 약 80% 정도를 스크램블링을 이용하여 유료로 방송하고 있다.[10] 일본의 유료 방송을 위한 스크램블링 방식은 1988년 전기통신 기술 심의회에서 표준안을 고시하였다.[2] 고시안에 따르면 영상 스크램블링 방식은 주사선 회전(line rotation)이나 주사선 교환(line permutation) 혹은 두 방식의 혼합형태를 사용한다.

주사선 회전 방식에서는 NTSC 신호를 $4f_{sc}$ (14.3MHz)로 표본화하여 744개의 유효 샘플(동기신호와 color burst신호는 제외)을 얻고 이들중 4개의 샘플을 1개의 블럭으로 묶어 모두 186 블럭의 유효 블럭을 단위로 하여 8bit의 의사 난수에 의해 지정된 절단점을 1개 선정하여 절단점을 중심으로 주사선 내의 신호정보를 교환한다. 주사선 회전 방식은 전송로나 수신기의 특성상 복원된 영상의 절단점 부위에 화질 열화가 발생할 수 있으므로 절단점을 부가 샘플로 연장하고 raised cosine 처리한다.

주사선 교환 방식은 TV의 수평 주사선중 유효 화면부에 해당하는 주사선을 54 라인 메모리를 사용하여 전송 순서를 의사 난수에 의해 바꾼다. 수신측에서는 6bit의 의사 난수로 지정된 라인 메모리의 내용을 읽고, 읽어가고 빈 라인 메모리에 수신된 신호를 차례로 기입하므로써 디스크램블링한다. 주사선 교환 방식은 주사선 내에 절단점이 없어 신호의 열화가 없다.

신호의 스크램블링은 영상과 음성 모두 디지탈 처리되지만 영상압축은 하지않고, 전송시에 영상은 아나로그로 음성은 PCM 디지탈로 전송된다. 음성의 스크램블링은 디지탈 음성에 의사 난수를 직접 가산하는 방식을 채택한다. 의사 난수의 초기치는 매 1초 마다 변경되어 비화도를 높인다.

자격 관리를 위한 개별정보의 전송은 전송율 32 kbps를 갖는 위성방송의 데이타 채널을 사용한다. 각 수신자에게 전송되는 개별 정보 데이타 패킷은 디코더 ID에 32bit, 의사 난수 발생기의 초기치를 암호화하는데 사용한 키를 위해 56bit, 그리고 각 수신자의 개별계약 내용을 위해 68bit를 할당한다. 한개의 데이타 패킷이 전송되는데 걸리는 시간이 9 ms일때 매초당 100개, 1개월에 약 2억 6천만개의 정보를 보낼 수 있어 1개월의 갱신 주기를 갖고 있을 때 가입자의 수가 2억 6천만 미만이면 1개월에 적어도 한번씩 각 가입자의 자격관리 정보가 갱신된다. 실제로는 개별정보의 전송 시간을 줄이기 위해 23인분의 개별정보를 한개의 패킷으로 공유토록하여 1개월 동안 각 가입자에게 반복하여 자격관리 정보를 전송하여 확인하고, 최대 가입자 수도 약 42억이 될 수 있도록 한다.[11]

일본의 HDTV인 MUSE를 스크램블링할 경우에는 MUSE의 디지탈 신호처리 단계에서 스크램블링하는 것이 적당하다. 이때, NTSC에서 사용된 주사선 회전이나, 주사선 교환 방식을 사용할 수 있다. 그러나, MUSE에서의 색신호와 휘도신호가 시분할 다중되어 전송되므로 휘도신호와 색신호 각각의 중간에 절단점을 설정하는 2-cut 방식이 추천되고 있다. 또한 절단점에서 화질의 열화를 방지하기 위해 부가했던 신호(overlap신호)는 MUSE에서는 여유시간이 없어 사용 불가능하지만 MUSE에서는 샘플 값이 전송되므로 절단점에 의한 화질 열화가 상대적으로 작다.

주사선 교환 방식도 NTSC때와 유사하게 사용될 수 있으나, MUSE에서는 주사선의 수가 많아 라인 메모리의 수가 증대될 수 있다.

4. 향후 전망

미래의 스크램블링 방식은 HDTV와 디지탈 전송을 포함하는 완전 디지탈 TV의 출현으로 새로운 장을 펼칠 것으로 기대된다. 즉, 미국의 HDTV는 조만간에 완전 디지탈 방식이 발표된 것이며, 유럽 공동체도 유럽의 HDTV로 완전 디지탈 방식의 채택을 발표한 바 있다. 일본은 이미 아나로그 전송 방식의 MUSE를 방송하고 있지만 미래의 완전 디지탈 방식의 전환을 위해 연구 중에 있다. 이 시스템들은 모두 디지탈 영상 압축 기술과 ECC 코드를 갖추고 있어, 종래의 주사선 교환이나 회전등의 방법이 영상 압축 블럭 단위의 혼합(shuffling)이나, 버스트 에러의 랜덤화를 위한 인터리빙방식과 연계되어 다기능의 스크램블링을 이룩할 수 있으며, 이들의 디스크램블링을 위한 알고리즘이 스마트 카드내에서 실행되는 방식이 될 것으로 전망 된다.

새로운 스크램블링 방식은 비화도와 디스크램블러의 가격(cost)간의 상보관계(tradeoff)가 고려되어야 한다. 즉, 많은 디스크램블러가 팔리면 같은 비화도를 싼 가격으로 공급할 수 있고, 반면에 디스크램블러의 가격이 초기에 너무 비싼 가격으로 책정되면 많은 공급이 이루어질 때까지 시간이 걸리고 같은 비화도를 비싼 가격으로 공급할 수 밖에 없다. 이를 해결하기 위해서는 초기에 방송 프로그램 제공자가 디스크램블러를 대여해 준다거나, 아니면 초기 스크램블링 방식은 어드래싱 기능 등이 없는 단순한 방식으로 시작하고 점차 다기능의 시스템으로 확대될 수 있도록 초기에 확장성을 고려하여 제안되어야 할 것이다. 또한, 가격 하락을 위해 방송 사업자 간에 스크램블링 방식의 표준화가 이루어져야 한다.

위성방송을 위한 스크램블링 방식은 신호의 비화도가 높고, 스크램블링으로 인한 신호의 열화가 없으며, 회로의 규모가 작고 가격이 싸야하는 등의 조건이 만족되어야 하는데, 결국 이런 조건은 완전 디지탈 전송 방송의 출현으로 만족될 것이다. 또한, 관련 정보 및 암호화된 키의 전송중 발생되는 오류에 대한 대책도 완전 디지탈 전송 시스템에서는 더욱 용이하게 마련될 수 있다.

참 고 문 헌

1. D. Angebaud and J-L Giachetti, "Conditional Access Mechanisms for All-Digital Broadcast Signals," IEEE Trans. on Consumer Electronics, Vol.38, No.3, pp.188-194, 1992.

2. テレビジョン畫像情報工學 ハンドブック, テレビジョン學會, 1990.

3. 難波誠一, "放送における情報セキュリティ", テレビジョン學會誌, Vol.42, pp.1291-1298, 1988.

4. 이경호, 정지원, 원동호, "영상 정보의 보호에 관한 소고," 통신정보보호학회지, 제3권 제1호, pp.42-53, 1993.

5. S.i. Kim, et.al., "Bit Rate Reduction Algorithm for a Digital VCR," IEEE Trans. CE, pp. 267-274, 1991.

6. Zenith, AT&T, "Digital Spectrum Compatible : Technical Details," 1991.

7. General Instrument, "Digicipher HDTV System Description," 1991.

8. F. Coutrot and V. Michon, "A Single Conditional Sccess System for Satellite and Terrestrial TV," IEEE Trans. on Consumer Electronics, Vol.35, No.3, 464-468, 1989.

9. F. Baylin, R. Maddox, and J. McCormac, "World Satellite TV and Scrambling Methods," Baylin Publication, 1991.

10. 직접위성방송 도입을 위한 정책연구, 한국방송개발원, 1992.

11. 小林喜三朗, "BSによるスクランブル放送", テレビジョン學會誌, Vol.46, No.4, pp.387-391, 1992.

□ 著者紹介

元 致 善

1982.2 高麗大學校 電子工學科, 學士
1986.2 Univ. of Massachusetts, 電氣 및 컴퓨터, 碩士
1990.2 Univ. of Massachusetts, 電氣 및 컴퓨터, 博士
1985. 1～1989.10 Univ. of Massachusetts, 研究助教
1989.11～1992. 8 金星社, 先任研究員
1992. 9～현재 東國大學校 電子工學科 助教授

金 在 功

1961. 3 漢陽大學校 工科大學 電氣工學科 卒業
1964. 8 同 大學院 電氣工學科 卒業 (工學 碩士)
1966. 4 日本國 早稻田 大學 電氣通信科 研究
1970. 3～현재 東國大學校 電子工學科 教授
1976. 3 工學博士
1980. 2～1990. 2 英國 Loughborough大學校 電子工學科 研究