AN ADDRESSABLE SATELLITE ENCRYPTION SYSTEM FOR PREVENTING SIGNAL PIRACY

Orest J. Hanas
Pieter den Toonder
Frank Pennypacker
Oak Communications Inc.
Satellite Systems
Crystal Lake, IL 60014

ABSTRACT

Satellite signals which transmit television and other commercial communications can no longer be thought of as secure. The advent of low cost TVRO's has opened the door to the threat of signal piracy. In response to this threat, a signal security system was developed which masks both audio and video intelligibility. The system can effectively shield programming, control its delivery, and protect private sensitive information. Presently it is used at C-band and Ku-band with conventional TVRO's and all existing satellites. It is, of course, directly applicable for the use in the Direct Broadcast Systems in the near future.

INTRODUCTION

As each day passes, it seems that we become more and more dependent upon communications satellites. Whether they are used to relay audio signals, data signals, or distribute broadcast and private television signals, our dependence on the reliability and security of satellite links has accelerated so rapidly that we now take their service for granted. Unfortunately the same technology that has made satellite communications cost effective and dependable has also reduced the security of its transmissions.

Because of the great height of geosynchronous communications satellites, their coverage areas or "footprints" are extremely wide. As a result, a television signal or any other communication signal distributed by satellite potentially becomes available to millions of people. Until recently, the high cost of satellite earth stations had sharply reduced the accessibility of satellite signals to unauthorized persons. In the past couple of years, however, the high cost of critical earth station components has dropped dramatically and is continuing to do so now. What's more, the availability of the premium television signals that are transmitted over satellites has been widely publicized. In addition, the high cost of travel makes video teleconferencing over the satellite a very attractive alternative for corporations. Government deregulation has provided an additional incentive to private earth station ownership by discontinuing licensing requirements. Complete earth stations are now being promoted for only a few thousand dollars and some inventive do-it-your-

0098-3063/81/0631-0636 $00.75 © 1981 IEEE

selvers have unlocked the window to "free" movies and to private and privileged information for only a few hundred dollars.

While users of satellites who transmit valuable or private programming or information may be looking to legislative actions to discourage unauthorized tapping of their signals, it is not realistic to believe that this will become a practical solution. The protection of the private and privileged information is much too vital to the economic success of satellite users to be left to chance. In addition, legal ramifications resulting from signal piracy may have far reaching effects on these users. For that reason, a system has been developed utilizing advanced encryption and addressability techniques and equipment. The system has received exhaustive testing with a variety of satellites (including Westar I & III, Satcom I and II, and ANIK-B) and terminal equipment and has been successfully commercially applied for the first time in scrambling the satellite TV signals transmitting the Ali-Holmes and Leonard-Duran prizefights in October and November of 1980 respectively. It has also been demonstrated at public and private conferences in the U.S. and Canada.

The development of this low cost satellite signal decryption system has used scrambling technology similar to that used in cable and subscription television systems. The satellite signal encryption system offers a new high in the level of program security. It is a complete end-to-end system which provides for the encoding of audio and video at the up-link studio or control center and decoding of these signals at individually selected receive earth stations. The system is fully addressable, allowing for controlled delivery of information to specific decoders. Each decoder in the system carries a unique code that must be matched with digital message transmitted from the up-link. Other features of the system are:

- Time varying video and audio encryption.
- Digitized and encrypted audio.
- Compatible interface levels with existing standard satellite earth station equipment.
- Standard Baseband TV inputs (at up-link) and outputs (at down-link).
- Broadcast quality signal processing.
- Fully proven computer control of entire system.
- Multilevel (tiered) program control within the secure channel.

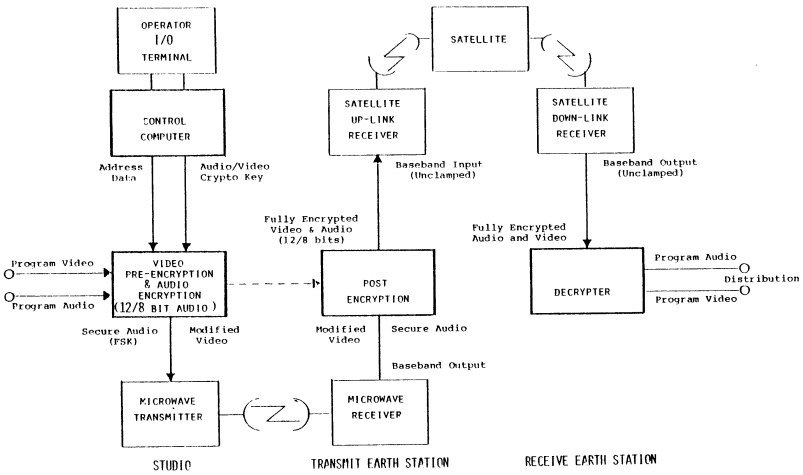

Figure 1 Satellite Signal Encryption System

- Optional second encrypted audio channel.

- Optional data channel and TVRO control units.

When an unauthorized viewer attempts to tune-in the encoded signal, the video signal will appear severely scrambled and without sync. The digitized and encrypted audio channel will be received as white noise. Even if the unauthorized viewer has a decoder system, unless that specific decoder has been "turned on" by the up-link operator, no decoding will take place. In addition, decoding intelligence always requires two levels of authorization.

Unique information stored in the micro-computer memory of each decoder, plus a second digital code transmitted as data, are required for decryption. The encryption can be changed as often as desired and can be varied with time in a pseudo-random fashion, under computer control. For added security, the receive decoders are tamper-proof.

The system can provide many levels of tiering, permitting a time-shared use of multiple satellite transponder channels by several classes of authorized subscribers. In addition, any decoder can be remotely denied access to all tiers by the authorized controlling party.

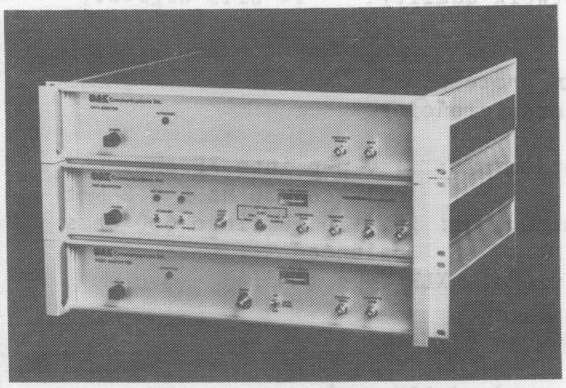

Figure 2 Encrypter

SYSTEM OPERATION

A block diagram of the satellite signal scrambling system is illustrated in Figure 1.

It consists of the following subsystems:

A. Control center equipment
B. Up-link earth station equipment
C. Receiving site equipment

Figures 2 and 3 show photographs of the actual encryption and decryption equipment, respectively.

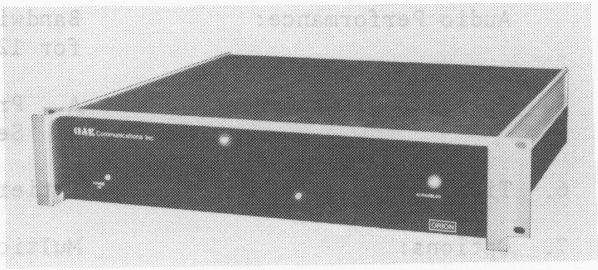

Figure 3 Decrypter

At the Control Center, the video is partially scrambled, the baseband audio is digitized and encrypted (using an advanced technique similar to that used by banks for electronic funds transfers) and the addressing information is formatted.

At the up-link earth station, the video signal undergoes further encryption to completely mask its recognizable features for security. There, the address channel, the encrypted audio and the scrambled video are combined, modulated and transmitted to the satellite.

At the receive site, a conventional satellite receiver (TVRO) converts the satellite frequency modulated (FM) signal to a baseband TV signal. The encrypted signal may be distributed throughout an entire distribution installation, or it may be decrypted in the decrypter and then distributed.

Table I lists the Major performance parameters of the Satellite Signal Encryption System.

1.	Control and Encryption:	In-Channel
2.	Addressing:	* Rate: 7,200 subscribers/minute * Number of possible subscribers: 2,000,000 * Method: Digital Data within video signal * Compatibility: Preserves Teletext, Teledon, VITS, VIRS, source ID and Captioning.
3.	Video Encryption:	Analog, with time-varying encryption controlled by central computer.
	Video Performance:	Meets RS250-B specification
4.	Audio Encryption:	Digital with time-varying encryption, using 12 to 8 bits companded.
	Audio Performance:	Bandwidth: 12 KHz for 12/8 bit, 60 dB S/N for 12/8 bit; Distortion 1.% for 12/8 bit
5.	Operational Sequence:	A. Pre-authorize all subscribers B. Send decryption data
6.	Tiering:	7 tiers are available
7.	Options:	Multichannel Audio A. One broadcast quality: 12/8 bits digital, encrypted B. One network quality: 14 bits digital, encrypted
8.	Applications:	Pay program protection Secure teleconferencing
9.	Interface:	Video Input/Output: 1 v p-p into 75 ohms unbalanced 30 Hz - 4.2 MHz Audio Input/Output: 0, +10 dBm into 600 ohms balanced
10.	Input/Output connection:	BNC type (video), XLR type (Audio)
11.	Power requirements:	105-130 VAC, 60 Hz
12.	Mechanical:	Mounts in standard 19" rack Pre-encrypter: 3½" high Post-encrypter: 3½" high Decrypter: 3½" high

TABLE 1 PERFORMANCE PARAMETERS

For distribution in a CATV system, the decoded signals may be again scrambled, using the locally available security system. Addressing, at the CONTROL CENTER, directs the delivery of the information to authorized receivers. The digital addressing information is inserted in the video during vertical blanking interval.

This digital information consists of a series of messages...one for each decoder in use. Each message contains a number, which identifies the specific decoder, followed by a program authorization code telling the decoder what programs it is to decode. The system will send out these messages, one after another, until all of the decoders have been addressed. Up to 7,200 decoders can be addressed in one minute. (Higher rate of addressing is achievable, if required.) The addressing is controlled automatically by a computer into which all the authorization data has been programmed.

RECEIVE SITE

A standard satellite TVRO (television receive-only earth station) is used for converting the satellite-transponded FM signal into a TV signal.

The output of the TVRO contains (at baseband) encrypted video and audio signals and address data. This signal is fed into the decoder at standard TV baseband interface levels. After decoding it is distributed to the TV monitors, or cable system modulators, as required.

PRINCIPLES OF THE ENCRYPTION SYSTEM

The principle behind the TV signal encryption system is based on the fact that television signals are quite redundant and portions of the waveform follow a given pattern. If these patterns are modified, a standard TV receiver will become confused and will try to lock on maximum video (which never occurs). Within the decoder, a circuit extracts a hidden and encrypted digital message and uses it to restore the normal patterns to the scrambled signal, restoring the original video. Before this circuit can be activated, the decoder must recognize its unique address and decoding data. Since the digital messages are time varied in a pseudo-random fashion, decryption of the signal is essentially impossible by a non-authorized decrypter.

The digitized broadcast-quality audio signal consists of two bytes sampled at a 31 KHz rate. To improve sound quality, the audio is compressed from 12 to 8 bits per sample. The 8 bit signal is encrypted, inserted in the video signal. The original audio subcarrier in the satellite channel is unused and open for other applications. The optional 14 bit network-quality audio signal, however, requires the use of the subcarrier in the satellite channel. It is digitized using 14 bits per sample and is encrypted for security. FSK modulation of the subcarrier is used to transmit this digitized encrypted audio signal.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.