SECURING A SATELLITE DISTRIBUTED TELEVISION SIGNAL

Paul A. Heimbach
Director, Engineering Planning and Development
Home Box Office, Inc.
1114 Avenue of the Americas
New York, New York 10036

Satellite Scrambling Design and Implementation

Beginning this year, Home Box Office, Inc., will scramble its HBO satellite-delivered programming. The scrambling system will provide highly reliable, trouble-free operation with minimal signal degradation due to the scrambling/descrambling process. Actual system parameters conform to HBO's rigorous Satellite Security System Design Target for performance, operation and security. A very high degree of signal protection is provided by digitally achieved combinations of encryption and scrambling techniques based on the National Bureau of Standards' Data Encryption Standard. The Data Encryption Standard is the foundation for highly sophisticated encryption and key distribution functions.

Each descrambler is addressable and fully controlled from the HBO origination facility. Operator attention to the descrambler is limited to the installation, initial settings of audio and video levels, and periodic maintenance.

This paper discusses the relevant technical details of the scrambling system.

Introduction

In December of 1983 Home Box Office, Inc. (HBO) will scramble two of its satellite distributed entertainment channels using the M/A-COM Linkabit VideoCipher scrambling system. The VideoCipher system uses a combination of analog and digital techniques to process and scramble the audio and video components and, through the application of a very secure data encryption algorithm, renders the scrambled signal useless to all but authorized users.

HBO sells premium programming to cable systems in the United States. The method of program distribution is domestic geostationary satellite. Programming is uplinked to the satellite where it is translated in frequency, amplified and downlinked to the U.S. in a national coverage beam. These downlinked signals can be received by authorized and unauthorized users alike, using receiving antennae as small as three meters in diameter. Today the private user can purchase an adequate receiving system for under $2,000 U.S. According to some estimates, 30,000 private systems are already in operation and new private systems are growing at the rate of 2,000 per month. It is in this context that HBO made the decision to scramble its satellite distributed premium programming.

Securing the Signal

The primary goal of scrambling is to render the program undesirable to unauthorized users. The signal can be rendered undesirable to a degree by scrambling only the audio and/or video and made totally undesirable to an unauthorized user by scrambling both the audio and video. Value or desirability exist in both the audio and video as individual components; therefore, both should be scrambled.

Securing the Audio Signal

From HBO's experience of evaluating many satellite security systems, it is apparent the most desirable method of securing the audio portion of the signal is to first digitize the audio, apply a very secure data encryption algorithm to the digital audio bits and transmit the audio channels in a digital format. The digital stream is then decrypted at the descrambler location and converted back to the analog format for distribution. The advantage of processing and transmitting the audio digitally is that any encrypting algorithm can be completely removed by the descrambler. Artifacts of the scrambling process are virtually nonexistent. Furthermore, a much higher quality signal can be delivered to the cable headend and eventually to the individual cable subscriber. And, finally, application of digital sound in sync allows full transponder power to be devoted to both the audio and video separately, improving the video signal-to-noise ratio.

Securing the Video Signal

Securing the video portion of the signal offers a variety of methods, each with its advantages and disadvantages. There are two basic methods of scrambling the video signal: (1) Amplitude variations and (2) time shifting various components of the video waveform. While these two methods present the possibility of many variations, only basic characteristics will be discussed here, citing both advantages and disadvantages of each.

Variation of the signal amplitude can range from simple synchronizing pulse suppression or elimination to variations of the amplitude of the active portion of the video signal, such as video inversion. Both analog as well as digital techniques can be used. Generally speaking, the amplitude variation method of scrambling is easier and in some cases less expensive to implement than the time shifting technique. Fewer components are required, making the construction easier and less costly and also aids in improving the operational reliability of the equipment. This method of scrambling the video is highly sensitive to signal path nonlinearities. Therefore, one must remember that the satellite distribution link including uplink, satellite transponder and downlink receivers (up to 50 different kinds in HBO's distribution path) has the potential to be unpredictably and uniquely nonlinear for each receiving location. This nonlinearity in the system makes artifact-free reconstitution of the amplitude varied signal difficult. In scenes of low luminance levels, as often occurs in movies, as little as 1/3 IRE luminance variation is observable. If the video signal is amplitude varied in a changing pattern at line rate, the observed effect is a streaking or dancing of individual lines. Variations at field or frame rate appear as flicker. It is conceivable nonlinearity correcting circuits can be designed to compensate for the link differences. However, these circuits add to the cost, reduce reliability and raise questions as to their ability to correct all link distortions one might encounter.

Time shifting various components of the video signal is based on the concept that the link characteristics, while variant with video amplitude are invariant over short periods of time ranging from line time to field time. In other words a video line transmitted over the link at time t_0 or t_0 +4 lines will be transmitted in essentially an identical manner, and will not be degraded simply because of the timing of its transmission. Line permutation or rotation are two methods whereby the video signal is shifted in time. Virtually artifact-free reconstitution of a time shifted signal can be accomplished. While time shifting can be done both digitally and using analog methods, it appears to be more expensive and complex than amplitude variation systems.

An approach suggested but quickly dismissed was one in which the video is digitized; each bit of the digital video signal "exclusive or'ed" with a pseudorandom bit stream, converted back to an analog signal and transmitted. Reconstitution is performed using the same method and same pseudorandom bit stream. Unfortunately, this scrambling technique has the potential of generating frequency components well outside the normal video bandwidth, making it impractical for use on most video transmission links.

Degree of Security

Because the downlinked signal is available to all who wish to receive and try to descramble it, the degree of security must be exceptionally high. To this end, nonchanging scrambling methods, such as constant video inversion or fixed line permutation or changing scrambling patterns based on a limited number of fixed patterns, are totally unacceptable. Through the appropriate application of proven encryption algorithms, apparently random patterns can be generated and applied to both the audio and video components. The mere fact alone that millions upon millions of scrambling combinations can be generated provides all the needed security. The basic security system must be based on an encryption algorithm still unbroken. However, if the algorithm should be broken, manufacture of unauthorized descramblers on a small scale must be prohibitively expensive.

HBO's Selected System

HBO selected the scrambling system demonstrated by MA-COM Linkabit, a U.S. manufacturer of high technology devices including data encryption systems and devices that brought back pictures from Jupiter and Saturn. The M/A-COM Linkabit system meets or exceeds the design goals set forth in a 57-page document prepared by HBO. The design goals included audio and video performance, operational characteristics, reliability and security requirements and environmental considerations.

The video signal is processed digitally, with scrambling accomplished by time shifting various portions of the video signal. Sampling of the video signal is at four times color subcarrier in the scramblers and descramblers, with the scramblers and the descramblers sampling to eight bits. The digitized scrambled signal is converted back to analog form closely resembling a standard NTSC signal for transmission. The reconstituted analog signal does not contain frequency components outside the standard NTSC video spectrum. Tests conducted on satellite link simulators, actual satellite links and through devices capable of adding controlled distortions have shown that the reconstitution of the scrambled video signal is free of artifacts.

The video signal is scrambled in any one of 50 million ways each frame time, with the actual scrambling pattern selected by the judicious applications of a pseudorandom binary sequence. Pattern changes are made many thousands of times a second, rendering the picture unrecognizable and impervious to descrambling attacks, such as line correlation techniques and pattern recognition.

With the output of the scrambler connected to the input of the descrambler, the system exhibits a minimum weighted video S/N of 57 dB,

differential phase and gain less than 2° and 2 percent respectively and a frequency response of ± .5 dB, DC to 4.5 Mhz. All additional standard video parameters are specified and held to tight tolerances.

Two channels of audio are linearly sampled at a rate of 44.056 k samples/second, with 15 bits per sample. The digitized audio channels are then companded and error correcting codes are applied to the resulting bits prior to transmission. Scrambling of the audio channels is done by "exclusive oring" each audio bit with a bit from a pseudorandom bit sequence.

The digital audio channels, as well as the control and message channels, are transmitted in the scrambled video signal during the time normally occupied by the horizontal sync pulses. A residual sync tip of about one microsecond remains in the transmitted signal for use in circuits with sync tip clamps. Placing the digital audio channels in the horizontal sync interval allows 100 percent of the uplink and downlink power to be applied to both the audio and video channels. Approximately 2 dB of video S/N improvement is gained, along with the elimination of interference caused by co-resident subcarriers. Data capacity is also limited by the data in sync transmission, but the need for more than two very high fidelity audio channels does not currently exist in the U.S. Furthermore, if additional data capacity is needed at a later date, co-resident data carriers can be added within the transponder without obsoleting the existing scrambling system.

The audio output of the descrambler is presented in both an analog format and a digital format. If a descrambler is not authorized, the analog audio outputs sound like white noise, and the digital outputs appear to be random bit streams with no relationship to the original program audio. The audio S/N is at least 60 dB reference to 0 dBM. Clipping occurs at +20 dBM and the system frequency response is ±.25 dB, 20 Hz to 15 Khz, with total harmonic distortion less than .2 percent.

U.S. cable operators generally operate their receiving equipment to present a carrier-to-noise ratio greater than 11 dB. Under these circumstances there is no impairment to the audio and video signals. To provide a margin of safety, the system operates reliably at a carrier-to-noise ratio of 9 dB, exhibiting no more than one audio click in a ten-minute period per channel, solid video reconstruction, no loss of descrambler synchronization and less than one second for descrambler synchronization acquisition. Test results have shown the M/A-COM Linkabit system continues to present acceptable audio and video at carrier-to-noise ratios of less than 9 dB.

Within the next year, the scrambling system will be in the HBO signal path that feeds 11 million subscribers. Reliability of the equipment is, therefore, very important. At the HBO uplink, the scramblers will be installed in a primary/hot backup configuration. If a deviation from normal operation is detected in the primary scrambler, all audio, video and control inputs will automatically switch to the backup scrambler. The input of the uplink exciter will switch from the output of the primary scrambler to the output of the backup scrambler. Should the backup unit fail while it is online, the system will switch to complete signal bypass. In this mode, the video is fed unscrambled to the uplink exciter, the stereo audio channels are combined to form a monaural channel which is fed to the 6.8 Mhz aural subcarrier modulator, auxillary contacts turn on the aural channel and the program is transmitted unscrambled as it is today. In the event of a partial failure, both the scramblers and descramblers revert to a special mode, which is as secure but does not require computer management.

Each descrambler is able to recognize a scrambled or unscrambled transmission. If the signal is scrambled, only authorized descramblers will descramble the audio and video. Unscrambled transmissions, however, cause all descramblers to go to bypass mode. The audio and video outputs from the satellite receiver are routed around the descrambler's electronics and presented at the descrambler's video and analog audio output connectors.

In HBO's application of the scrambling system, descramblers will be located at unmanned sites, some inaccessible for three or four months out of the year due to weather conditions. The descramblers, therefore, are reliable, maintenance free and rugged. The design of the descramblers provides a calculated Mean Time Between Failure (MTBF) of 16,000 hours. Experience has shown that standard MTBF calculations are pessimistic and an even greater MTBF can be expected. Like the scramblers, the descramblers can be installed in a primary/automatic backup configuration. This feature is optional, to be used at the descretion of the cable operator. If this option is elected, the MTBF of the descrambler configuration is increased many fold.

Periodic adjustment of the descramblers is not required. At the time of installation, the audio and video gains of the descrambler are adjusted to be compatible with the associated satellite receiver and CATV modulator. No further adjustments are required throughout the operational period of this configuration. Additionally, all descrambling control information is transmitted to each descrambler by the scrambled signal path, thus freeing the cable operator from the responsibility of having to enter the descrambling messages.

Generation of the scrambling/descrambling pseudorandom bit streams and distribution of descrambling messages are the foundations of the system's security. Message distribution is

complicated by the fact that it is sent in band along with the scrambled signal. A very effective approach to maintaining security integrity uses a combination of very secure data encryption algorithms and a unique identity for each descrambler.

The National Bureau of Standards' Data Encryption Standard (DES) is used to secure all message transmissions as well as generate the necessary pseudorandom bit sequences. The DES algorithm has been available to the U.S. public for a number of years, and despite repeated attacks has not been compromised. We feel confident the application of the DES algorithm meets HBO's security needs. Furthermore, because the bit sequences change many times a second, the possibility of code pattern detection is virtually impossible.

Assigning a unique identity to each descrambler offers protection against duplication of authorized descramblers. Cloned descramblers, once identified, can very easily be traced back to the parent authorized descrambler's identity. Once the authorized descrambler is identified, it is simply deactivated. As a result, the authorized as well as the duplicate units will cease to operate. Addressability is also made possible by the assignment of unique descrambler identities. Very large quantities of descramblers in any quantity and combination can be activated on an apparent instantaneous basis.

HBO's intention is to install a scrambling system that is virtually transparent to the audio and video signals, highly secure, reliable and capable of future growth. Additionally, HBO hopes to have defined a system that will meet most users' needs and be capable of forming the core of signal scrambling devices. Years of effort, research and working with manufacturers has gone into this system, and we are confident the M/A-COM VideoCipher will meet all these requirements.