HARD ENCRYPTED VIDEO AND AUDIO TELEVISION SYSTEM

Michael F. Jeffers
Joseph B. Glaab
John T. Griffin

GENERAL INSTRUMENT CORPORATION

There are many considerations involved in the design of a truly secure scrambled television signal. In the encoded mode, recognition of any portion of the original video and audio signals must be obliterated by the scrambling method. The recovery of both these signals must be protected by ecryption techniques developed within a robust transmission system. The circuitry to reconstruct the signals must be reliable and consistent; and its cost must be in line with the benefit. Above all, the quality of the descrambled signals must match the original. We are confident that we have achieved these goals. In the following paragraphs we will discuss the problem areas and our solutions.

Development work on this system started in the second quarter of 1983. The choice of scrambling and descrambling a baseband signal was obvious for several reasons. Signal processing techniques were well understood; both AM and FM systems could be used for transmission; and the ability to transfer from a satellite system to a CATV or MATV system without descrambling was inherent. A modified NTSC format was chosen to stay within the six MHZ bandwidth needed for cable and to keep device costs at a minimum. From the start, highly integrated VLSI circuits were the only choice for the final product. The plan required a minimum of two audio channels and an address/authorization scheme to serve sixteen million subscribers.

All of this information was to be in a digital format. For audio, the Dolby adaptive delta modulation system was chosen because of its proven high performance at moderate bit rates. To assure a robust system forward error correction was included; for security the audio bits were encrypted.

The first test at transmission of this baseband signal used frequency modulation simulating a satellite service. The digital audio and address information modulated a 6.2 MHZ subcarrier as QPSK. The subcarrier became part of the baseband which then frequency modulated a 70 MHZ exciter. Results were very poor. The power required for satisfactory performance of the information on the subcarrier at low carrier-to-noise worsened the threshold level of video by 2.5 db. This was unacceptable. Separately we experimented with a line rotation form of video scrambling and were reasonably successful in descrambling it. It was decided to reformat the audio channels and the address/authorization data to fit within the video signal. Making use of all the horizontal intervals was required; the information content we needed greatly exceeded the time available in the vertical interval. The vertical interval is used for synchronization, AGC for AM systems, and for level references. All information carried in the VBI needed for proper system operation is contained in the first nine lines leaving all remaining lines to be used by the system operator for any service he chooses - Teletext is an obvious option. System tests using this approach were extremely successful. There was no loss of video power since no subcarriers are needed. In fact, the lack of subcarriers and synchronizing pulses improves the carrier-to-noise subjective threshold by one to two db compared to standard NTSC.

With the background established, the following detail is presented.

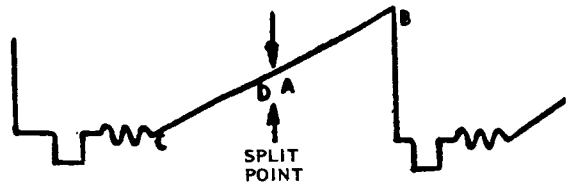
VIDEO SCRAMBLING

A line splice and section rotation system was used. The system allows for a single video line to be spliced at any one of more than one-hundred locations linearly spaced along the line.

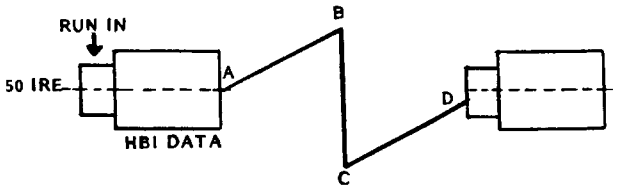
Figure 1 shows an example of the method used.

To accomplish this, the video is processed through an analog to digital converter. The digital samples are stored in a high speed RAM capable of one video line of memory. The splice point is determined from a synchronous stream cipher decryptor using non-linear sequential logic. In effect, the splice point is chosen from a random bit stream in the encryption circuit which is synchronous with the decryptor at the receive end of the system. A time varying encryption is achieved by establishing a new encryptor seed every frame. The stored digital samples are taken from the memory starting at the splice point to the end of the stored line and then, from the start of the line to the splice point. This sequence is passed through a digital to analog converter for transmission. The transmission can be for many services: satellite, cable, microwave, MMDS. At the receive site, after demodulation, the process is reversed.

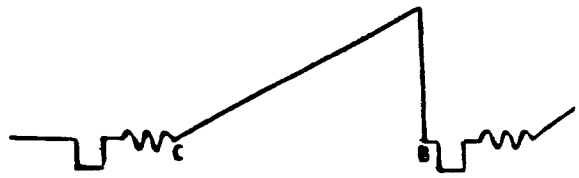
The scrambled baseband signal goes through an analog to digital converter and is stored in a high speed RAM. The original splice location is known at the receive site via the synchronous encryption stream. The memory location for the start of the line is the complement of this number. As an example,



SOURCE



ENCODED VIDEO



DECODED VIDEO

FIGURE 1

there are about 752 memory locations for the active video portion of a line. If the splice were taken one quarter of the way across the line at location 188 then the start of the line would be its complement at location 564 (752-188). The digital information is then taken out of memory beginning at this location and the line is reconstructed to its original form. If the subscriber is authorized to receive programs, the signal is passed through a digital to analog converter for presentation at the video output. In actual practice, the complement algorithm is used at the transmitter to allow for a less complex recovery at the descrambler.

THE HORIZONTAL INTERVAL

It is important for this system that the video signal comply with the EIA Standard RS170A color television standards. To assure this, it is recommended that the source video be processed through a frame synchronizer. A phase locked loop circuit senses the color burst at the video input port of the scrambler. All timing for this system is derived from this reference. The horizontal blanking interval from the source video is stripped clean of sync and color burst. The interval is reconstructed to include digital information starting with a 16 bit run-in code plus 66 bits representing two digital audio channels, address information and data. This interval is referenced to a 50 IRE level. Included in the 66 bits are two interleaved "2 for 3" forward error correctors. We use two level data. The combination results in a very robust transmission system; error free until very low carrier-to-noise ratio are reached. The remaining 44 bits serve the following functions:

13	right audio Dolby
13	left audio Dolby
1	step size (audio)
1	slope (audio)
8	address authorization
1	encryptor seed
1	video invert key
6	data - (or 2 on-screen display and 4 data)

The 26 audio bits are encrypted. The 8 address bits per horizontal is equivalent to a 126 K bits/sec rate or a cycle rate of 2.7 million subscribers per hour.

At the receive site the information in the horizontal interval is processed and the horizontal interval is reconstructed with clean sync and color burst to the RS170A specification. The same is true of the vertical interval. These clean synchronizing signals maintain the video in stable lock down to levels of zero db carrier-to-noise. The audio will show distortion at about 5 to 6 db carrier-to-noise but is intelligible to 4 db. The complete descrambler consists of four major integrated circuits: a custom codec; a custom video processor; a control microprocessor with peripheral; and the audio digital to analog chip.

Other important circuits included in the design are:

1) A video AGC.

2) A clamp circuit.

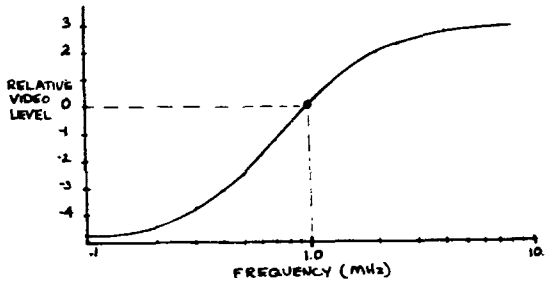
3) A line tilt correction circuit.

The AGC circuit will maintain an accurate one volt peak-to-peak video output signal for $\pm$ 3 db variation of the input. This will compensate for varying deviations in FM systems and for sloppy R.F. AGC's in AM systems.

Line tilt is the nemesis of line rotation systems. Experience with both FM and AM tests indicate that this is not a problem for our systems. We attribute this benefit to the format we use in the horizontal interval where the information is centered around the 50 IRE level thereby maintaining an average level across the complete line scan. Nevertheless, we have incorporated a line tilt correction circuit for insurance.

PRE-EMPHASIS/DE-EMPHASIS

For satellite transmission, the format of the scrambled signal allowed for optimization of the pre-emphasis and de-emphasis circuits. After extensive calculation and subjective tests we established that the curve presented in Figure 2 gave a high quality picture for a clear sky condition while it enhanced the bit error rate and gave a significant subjective improvement at low carrier-to-noise levels. Subjectively, it greatly reduces the size of the comet tails caused by impulse noise.



SUMMARY

The techniques discussed result in a practical cost effective scrambling system which features hard encrypted video with hard encrypted stereo audio to insure longevity. The two level, forward error corrected data assures a robust system operating down to low carrier-to-noise ratios. The reconstructed picture is a replica of the original at normal operating levels. It is a baseband system proven in both the FM and AM transmission modes. The line rotation method of video scrambling maintains a very secure signal even in the presence of sync reinsertion defeat mechanisms and digital television chip sets. The use of digital processing methods avoids distortions inherent in analog techniques. The format used allows for special pre and de-emphasis circuits which are optimized to minimize bit error rates and improve the subjective effect of impulse noise. The work effort has met all the goals required for an excellent operating system.