AN ENHANCED RF TELEVISION SCRAMBLING SYSTEM USING PHASE MODULATION

Michael E. Long
Manager, CATV RF Engineering
Richard Citta
Manager, Electronics Systems Research and Development

Zenith Electronics Corporation

ABSTRACT

A new scrambling and descrambling system for television RF signals is presented which represents a new generation of technology for CATV service security. The new system has been designed to be low cost, easily manufactured, reliable and more secure than conventional RF technology. Through the use of complex response Surface Acoustic Wave (SAW) filters, the system employs RF Carrier Phase Modulation to enhance the economy of RF sync suppression techniques with some of the video and audio signal security attributes of Baseband systems. Additionally, the new encoding system provides an integral means of reliable, noise insensitive addressable data communication to subscribers' descramblers without the use of a separate data channel.

INTRODUCTION

Since the advent of Pay TV in both broadcast and CATV environments, a secure, effective and economical method of scrambling and descrambling Television signals has been sought. Many RF techniques, while inexpensive, have proven over time to be weak in signal security and vulnerable to program piracy. Baseband scrambling systems, by supplementing basic sync suppression with video and audio manipulation, can increase security substantially but with a corresponding increase in cost.

Over the last few years the market demands for Addressable Home Terminals have been changing. Signal security is still an important issue but not as important as is cost and user features. What the market really desires is an economical, fully featured, secure CATV Converter-Descrambler.

REQUIREMENTS

In order to study and evaluate past and present system design shortcomings and to plan development of a new enhanced CATV Converter to meet present and future market demands, a "wish list" of requirements was composed. The following list includes many of the the desirable attributes and features an ideal Home Terminal should have:

- Secure
- Reliable
- Addressable
- Reliably Manufacturable
- BTSC Stereo Compatible
- Downloadable Configuration
- High Quality Signal Restoration
- Fully Featured
- Future Friendly
- Low Cost

Most of the above features seem straightforward enough, but in order to achieve both low cost and a high degree of security a totally new TV Scrambling system must be developed.

A NEW SCRAMBLING SYSTEM

Security and low cost at first seem to be mutually exclusive parameters. Conventional RF scrambling techniques are economical but their designs are well known and have made them easy targets of "black-box" decoders used to steal CATV services. Also, many RF systems require critical timing adjustments and have performance problems with BTSC Stereo due to data and timing AM modulation of the Pay TV channel's Sound Carrier.

An ideal system would have the security attributes of a Baseband System and the economy of an RF system without performance degradation. Toward that goal, a new TV scrambling system was developed using Video Carrier Phase Modulation (PM) over a defined frequency range to scramble the TV signal and transmit data and descrambling information to subscriber terminals.

Phase Modulation - Encoding

As with other RF scrambling methods, the PM Encoder processes the Visual IF signal of the modulator and returns it for conversion to the CATV channel frequency as shown in figure 1. Modulator video is also looped through the encoder to be used as a timing reference in the scrambling process. An audio loop-through is used for the purpose of enhancing the system's Audio Masking effect. Since the modulator's sound carrier is not modified in this scheme, an Aural IF carrier is not connected through the encoder.

Figure 1

P. M. SYSTEM CONFIGURATION

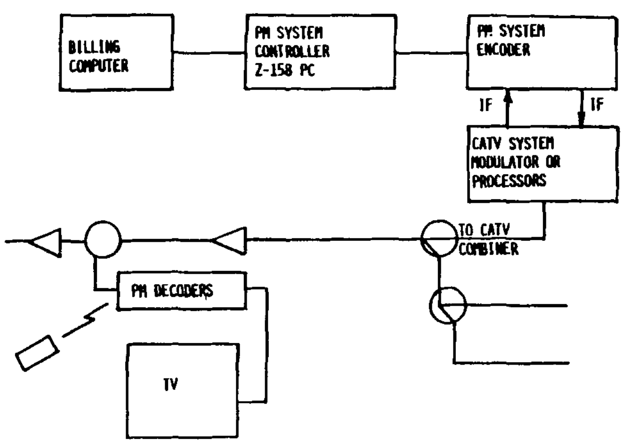
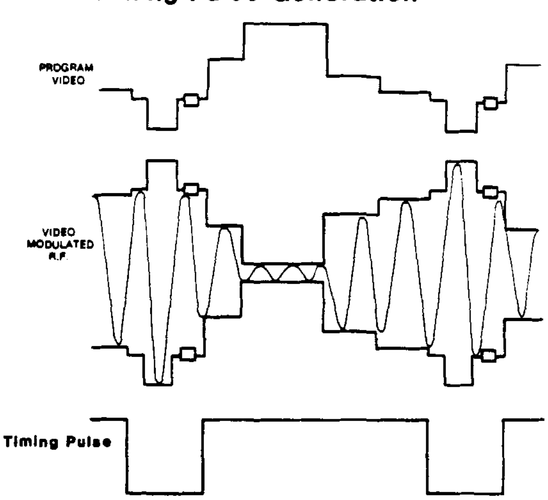


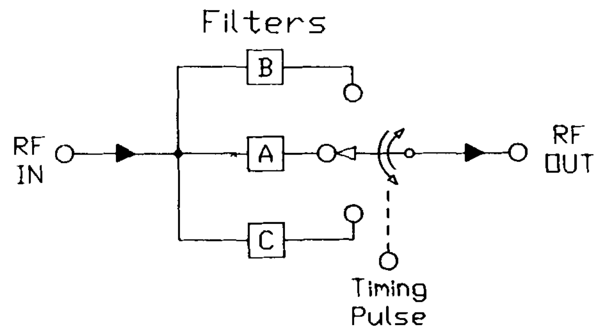
Figure 2 shows the typical IF modulation process performed in the CATV head-end channel modulator. From the modulating video a timing pulse is generated, synchronized with each Horizontal blanking period.

Figure 2
IF Modulation and Timing Pulse Generation



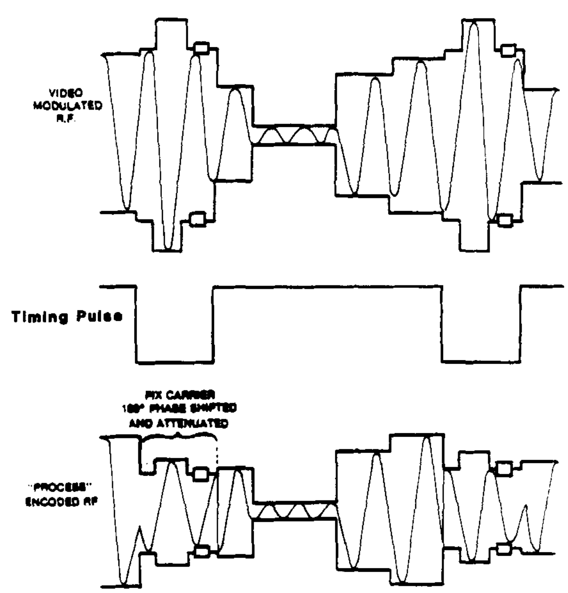
The generated timing pulse is used to dynamically switch the Video IF signal from passing through a flat response bandpass filter (A) to one of two alternate filters (B or C) as shown in figure 3.

Figure 3 RF Switch



Each of these alternate filters, corresponding to two different scrambling modes, have the characteristic of not only attenuating the IF signal at the picture carrier frequency, but to completely phase reverse it 180°, as shown in figure 4. The resulting IF output looks as if it is encoded with standard sync suppression but also contains a carrier phase reversal. This Phase and Amplitude modified Video IF is then returned to the CATV modulator for conversion and distribution to subscribers over the cable plant. This combination of sync attenuation and non-linear phase modulation provides non-authorized viewers with both video scrambling and audio distortion.

Figure 4
Phase Modulation - Sync Suppression

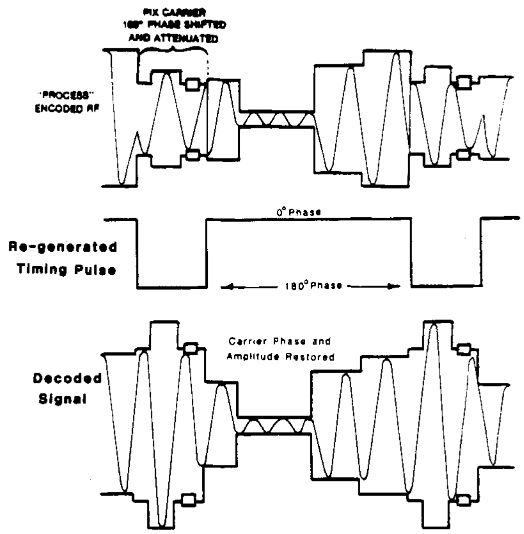


Phase Modulation - Decoding

At the subscriber's home terminal, the PM encoded channel is tuned and converted to a low VHF channel (Ch 2, 3 or 4) for processing and transfer to the home TV receiver. The phase modulated VHF signal is first filtered and passed to a PLL synchronous detector designed to be stable for both a 0° and 180° phase lock. The output of this detector, shown in figure 5, is a replication of the timing pulse originally used to encode the signal at the head-end. Since the detected timing pulse is derived directly from the encoded signal, any timing errors are insignificant.

Figure 5

Decoding - Detection of Timing



The regenerated timing pulse is then used to control an RF switch which selects the routing of the encoded VHF signal through either of two filters complementary to those used in the head-end encoder. The result at the output of the decoder RF switch is a VHF TV signal restored to its original Amplitude and Phase and passed on to the TV receiver.

Data Transmission

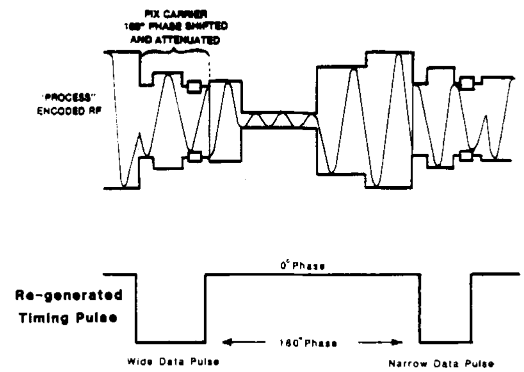
One deficiency of conventional RF TV scrambling systems is the method of data transmission. In-band timing and program tags are normally AM modulated on the channel's Aural Carrier making them prone to be noise sensitive, critical in timing adjustment and to cause performance problems with BTSC Stereo encoded audio. Out-of-Band FSK data provides a continuous communication link from the head-end but takes up valuable CATV spectrum and requires decoder safeguards to protect against loss of the data carrier. Out-of-Band Data also requires each decoder to include the extra circuitry, cost and potential unreliability of a separate data receiver.

The new Phase Modulated RF scrambling system provides a secure, reliable and relatively noise-immune in-band data transmission system inherent to the scrambling system without the need for a separate data receiver.

PSK modulation of data is widely recognized as an extremely noise insensitive method of communication. Since the basis of the new PM scrambling system is the phase modulation of the carrier 0° and 180°, data transmitted additionally in this fashion could constitute a very reliable communication link. As shown in figure 6, the PM system data is encoded as pulse-width modulation of the timing pulse itself creating 262 bits of data for every vertical field of video, one bit for each horizontal period.

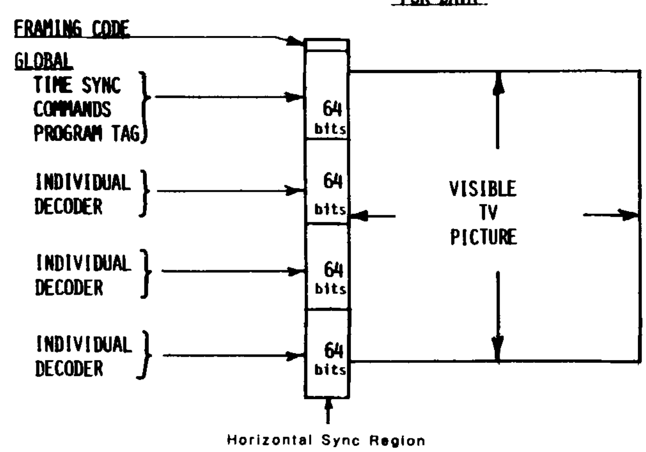
Figure 6

PM - Data Transmission



The data, encoded into the timing pulses and BPSK (Bi-phase PSK) modulated on the RF picture carrier is transmitted on all PM scrambled channels. The data is formatted into four packets of 64 bits each per video field. This is shown graphically in figure 7 as horizontal blanking interval data alongside the visible TV picture.

Figure 7 PM IN-BAND PSK DATA



The first of the four data packets is used for global command data, time sync and channel related program tag information. This global packet is encrypted for data security with a variable "session" key. The session key is one of several decryption keys periodically downloaded individually to subscriber's decoders.

The other three data packets contain information addressed to individual decoders and are encrypted with a unique "address key". The address decryption key is different for each decoder and has been factory programmed and "locked", along with the decoder's address, into each decoder's non-volatile memory. Enough address data is allocated in the individual data packets to allow for a potential of over 67 Million addresses.

With an addressing rate of three subscribers per field, up to 10,800 addressable decoders per minute can be processed. Preceding each group of four data packets is a framing code used to identify each new data group.

In addition to the rugged PSK transmission system, the data is further protected by three additional "shells" of security. First, each data bit received by the decoder's synchronous detector must meet specific timing requirements in order to be accepted by the decoder as good data. If only one bit in a packet falls out of the acceptance "window", the entire data packet is discarded by the decoder.

Secondly, every packet received by the decoder must match one in the decoder's "library" of recognized packet types in order to be accepted. For the final "shell" of data security, to further enhance noise immunity, each packet includes 16 bits of CRC (Cyclic Redundancy Code) for error detection. Noise tests of the system have shown accurate decoding at Carrier-to-Noise ratios below 14 dB.

Multi-Mode Scrambling

In order to ensure scrambling security, encrypted data and signal scrambling must be linked in some fashion. The system must be designed such that if the data link is broken, the TV signal cannot be descrambled. A good design requires that certain information must be present in the data necessary for the decoder to properly function.

In the PM system, there are two distinct levels of scrambling corresponding to two different attenuation levels of the horizontal sync interval. Each scrambling mode requires different signal switching between three complex filters (complementary to those in the encoder) at the correct time and in the correct sequence. Either mode can be used independently in a fixed format or dynamically random-switched at the Cable Operator's discretion. Encrypted downstream data is used to indicate to the individual decoders which mode is being used.

Included in the first data packet of each field is the encoder's scrambling mode definition for the next field. This data is transmitted to all decoders and encrypted with the CATV system encoder's variable "session" key. If the decoder is authorized and has the previously downloaded decryption key in its memory, it can decipher the program level and scrambling mode definition. This information is used with other available data to correctly descramble the program. If the decoder cannot decrypt the data packet or if the packet's program level does not match the corresponding downloaded decoder authorization level, the signal is not allowed to be descrambled.

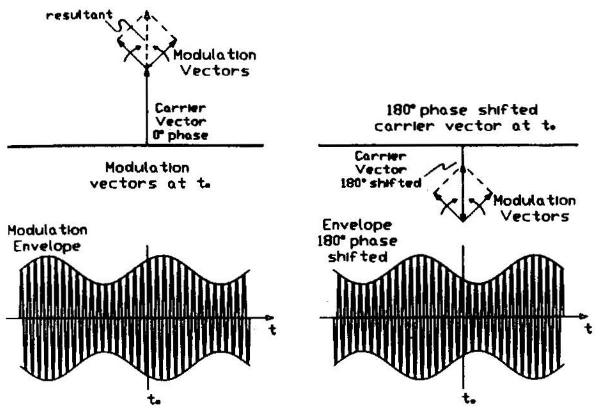
Thus, the scrambling mode and authorization system is protected with three levels of security: (1) the scrambling mode is defined by difficult-to-detect downstream data, (2) the mode definition data is encrypted with a variable "session" key, (3) in order to have access to the "session" key, the decoder address must be in the head-end data base, and (4) all information downloaded to addresses, including "session" keys, is encrypted with a unique "address key" for each decoder.

Chroma Inversion

As described, the PM scrambling is accomplished by switching the CATV modulator visual IF signal through complex filters which both attenuate and phase reverse it during each horizontal blanking period. In fact, the scrambling filters (and descrambling filters) used are complex multi-element SAW (Surface Acoustic Wave) devices of a proprietary design. Because of the particular design of these SAW filters only the channel's visual carrier, and not it's Chroma and Aural carriers, are phase and amplitude modified during the horizontal period. This technique produces some interesting effects on the TV detected video.

The major effect of the PM scrambling on a TV receiver is the loss of horizontal synchronization due to sync suppression into the luminance video range. But in addition to this standard RF scrambling effect, the detected video chroma becomes inverted. This is due to the fact that with common intercarrier TV detection processes, phase modulation is transferred to the modulating subcarriers if only the visual carrier is phase modulated. This can be shown graphically using the simplified AM modulation vector diagram of figure 8.

Figure 8 Chroma Phase Inversion



In figure 8, a carrier is being AM modulated by a pair of sideband modulation carriers. At the point of time described by the vector diagram, the resultant main carrier is nearing its peak in amplitude due to the addition of the modulation sideband vectors. This point in time is shown in the accompanying carrier diagram by a vertical line. If at the same point in time the main carrier vector (and not the modulating sideband vectors) is 180° phase reversed, the result is that the sideband vectors <u>subtract</u> from the main carrier envelope causing it to be near its <u>minimum</u> amplitude. The resulting envelope of the 180° phase shifted modulated carrier is a sinewave of the opposite phase from the case of a 0° phase carrier.

Thus, during the PM encoded horizontal blanking interval, when the Visual carrier is 180° phase shifted from normal, the color burst within that interval detected by a TV receiver would be phase inverted from normal. Since the TV color circuitry phase-locks to the color burst, this phenomenon would then invert the TV video chroma. In this fashion the PM scrambling system incorporates video manipulation, an attribute of Baseband Scrambling, into a low cost RF system.

<u>Audio Masking</u>

Just as the Chroma carrier becomes phase inverted during the PM encoded carrier reversal period, the Aural carrier, detected in an intercarrier TV receiver, becomes phase inverted. During the fast transitions from normal phase to inverted phase (and then back again), the TV FM sound detector experiences large frequency variations as the detector tries to track the huge carrier phase shifts. This effect produces large audio transients in the TV FM detector output, driving the detector into non-linearity. The resulting effect of the scrambling on the TV receiver audio is severe audio distortion and buzz.

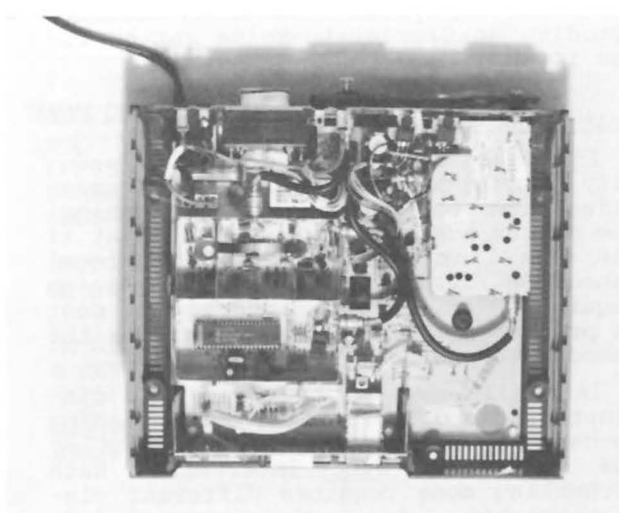
In an effort to enhance this audio distortion for unauthorized viewers a modulated audio subcarrier, similar to the BTSC stereo "SAP" subcarrier, is added by the PM Encoder to the audio signal fed to the CATV Channel modulator. Due to the severe nonlinearities that the TV Audio detector is driven to by the scrambling phase transients, the modulation of the added subcarrier becomes mixed with the buzz and detected baseband audio produced by the TV audio circuitry. This additional "garbling" effect on the TV audio is referred to as enhanced Audio Masking.

If BTSC stereo is used on the channel, effective audio masking occurs with only the standard BTSC SAP (Second Audio Program) signal. When a SAP signal is detected on the encoder audio, the Audio Masking Subcarrier is automatically turned off.

<u>DECODER DESIGN</u>

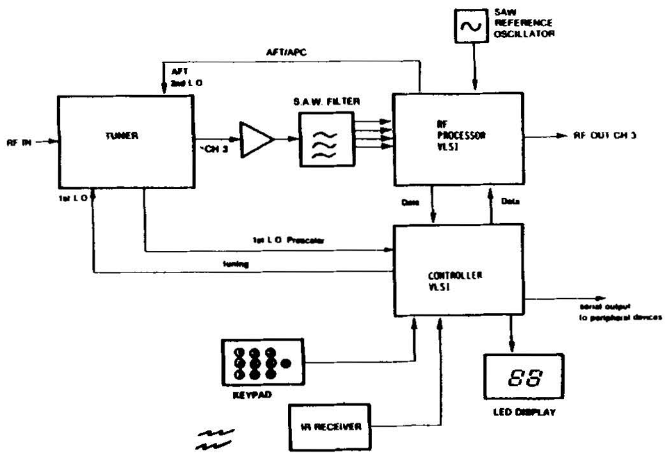
For low cost, reliability and manufacturability, the decoder design for the PM system is kept as simple as possible with few parts and minimal alignment requirements. For security, the design includes custom VLSI circuits, custom complex response SAW filters and data protection. Figure 9 is a photograph of the internal design of the decoder.

FIGURE 9
PM Decoder Internal Photo



The design uses a one board approach of minimal parts count requiring no factory electrical adjustments. In addition to the two power supply regulators, there are only three ICs on the module. The centralized microprocessor control and serial data output port in the design allows for extensive automated factory testing before shipment to ensure quality. Figure 10 shows a basic block diagram of the decoder design.

Figure 10
PM DECODER BLOCK DIAGRAM

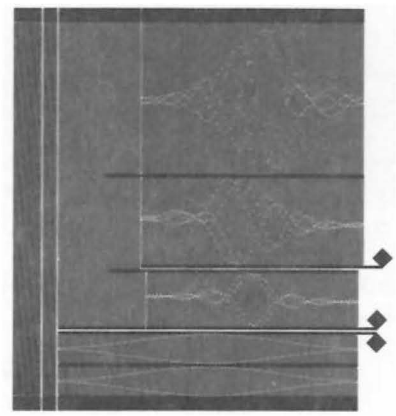


<u>Custom Multi-Element SAW Filter</u>

The prime decoder component necessary to restore the PM encoded RF carrier to its proper amplitude and phase is the SAW filter. The use of SAW filters for both encoding and decoding was decided upon due to the complex nature of the required amplitude and phase response for the scrambling system, precluding any unauthorized replication. Additionally, SAW filters do not require alignment. Once the SAW design is finalized, production devices are virtual clones of each other.

In the development of the SAW filters used in the PM system, an iterative process was used to perfect the final designs. Of primary importance was to be certain that the decoder SAW amplitude and phase ratios between modes matched those of the encoder SAW as closely as possible. To ensure tight mode matching tolerances, the SAWs actually incorporate 4 independent filter elements on the same substrate. The four elements are used for data channel filtering, unencoded filtering, and dual scrambling mode filtering. A die photograph of the decoder SAW, showing the multi-filter elements, is shown in figure 11.

FIGURE 11
PM Decoder SAW Filter



Good decoded signal quality requires tight tolerances between modes in both encoding and decoding. Not only do the video sync pulses need to be restored to the proper levels but the decoding side-effects on the color and audio signals must be minimized. Processing time delays must also be compensated for in order to accurately match-up decoding to encoding in the time domain. If scrambling dynamic mode switching is used, matching between encoder modes and decoder modes must also be accurate in order to avoid annoying flicker in the descrambled TV picture.

All of these requirements have been accomplished through the use of the system's custom proprietary SAW filters. The specific SAW characteristics and the lack of "off-the-shelf" parts make attempts to manufacture acceptable "pirate" decoders impractical.

Figure 12 diagrams in simple terms the amplitude responses required of the complementary encoder and decoder SAW filters. In the encoder, the relative amplitude of the response at the picture carrier frequency is attenuated at a level (B or C) dependant upon the defined scrambling mode, while the response at color and sound carriers is flat with no attenuation. The decoder SAW provides a relative amplification at the picture carrier compensating for the encoder attenuation (B or C), while maintaining color and sound at 0dB.

Figure 12
Encoder - Decoder
SAW Amplitude Response

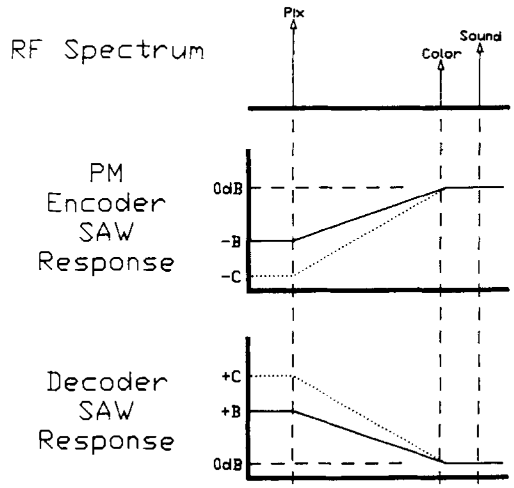
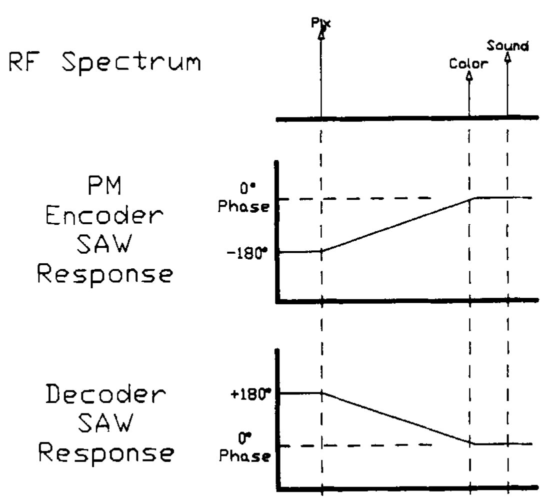


Figure 13 shows the encoder and decoder filter phase responses. Note that the encoder phase response adds a 180° phase shift at the picture carrier frequency while maintaining a 0° phase shift at color and sound carriers. The decoder response is such that it corrects for the encoder response.

Figure 13
Encoder - Decoder
SAW Phase Response



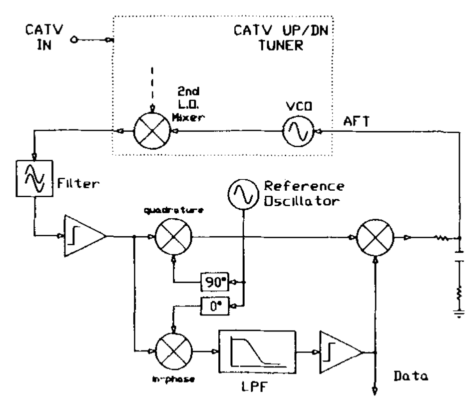
Custom RF Processing IC

The PM scrambling system phase shifts the encoded channel's Visual carrier by 180° during the video horizontal blanking interval. In order to recreate the timing signal necessary for accurate descrambling and to receive the BPSK headend data, the decoder needs to monitor and accurately track the phase of the incoming RF signal. Common PLL (Phase Lock Loop) technology has no difficulty with locking to normal signal modulation, but a signal having rapid 0° to 180° phase changes represents a problem. A Phase Lock Loop capable of being stable at both 0° and 180° phase states is necessary.

Such is the case in the custom, proprietary RF processing IC incorporated in the PM system decoder. Included in this IC is a patented FPLL (Frequency and Phase Lock Loop) which is Bi-Phase stable. The IC's FPLL serves two purposes: it not only detects the PM signal's phase modulation for timing and data but it also provides AFT for the converter CATV tuner.

Figure 14 is a simplified block diagram of the FPLL system.

Figure 14 FPLL Block Diagram



In this diagram, the RF signal tuned by the CATV tuner is amplified, limited and supplied to two multipliers. The upper multiplier, used as a normal PLL phase detector, is compared to a 90° (quadrature) phase shifted reference oscillator at the picture carrier frequency. The lower second multiplier acts as an in-phase detector comparing the input signal to the 0° phase shifted reference oscillator. If the input signal is nearly in-phase with the 0° reference oscillator, the output of the lower (in-phase) multiplier produces a "+1" signal to the third multiplier in the chain. The output of this third multiplier then linearly reproduces the phase error from the upper (quadrature) multiplier and supplies it to the tuner 2'nd local oscillator as an AFT/APC.

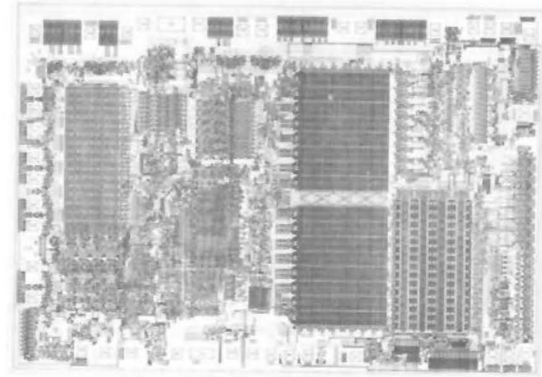
This system effectively locks the tuner output frequency to the reference oscillator, a stable SAW resonator design. If the input signal shifts 180° in phase, as in the PM encoding scheme, the second (lower) multiplier produces a "-1" signal to the third multiplier in the chain. That multiplier then inverts the phase error control signal supplied to the tuner maintaining phase lock stability. The +1 and -1 output signal from the in-phase multiplier is in fact a re-creation of the timing pulse originally used in the head-end encoding for PM scrambling. This output from the FPLL is used then as the received PM data for further processing.

Custom Micro-Controller IC

The processing of the PM data is one of the tasks of the third key component in the decoder design, the microprocessor. Largely due to security reasons, a custom microprocessor-controller was designed for the product and manufactured exclusively for Zenith.

A primary concern in the decoder design was tamper protection for the authorization and decoder address memory. "Off the shelf" parts, standard external memory ICs and battery back-up systems can all be security weaknesses in an addressable Pay-TV Descrambler. For this reason, the PM decoder microprocessor incorporates its own internal non-volatile read-write memory, not requiring a battery back-up. Part of the memory is user accessible for features such as "favorite channel scan memory". However, most of it is used for Pay TV and IPPV authorization level storage, downloadable converter characteristics and decoder address memory. As an additional security measure, the section of memory used to store the decoder address and address decryption key are permanently sealed off from future modification after initially being loaded in the decoder factory.

In addition to secure information storage, the microprocessor has the functions of PM data processing, decryption and error detection along with subscriber interface and head-end interface through Store-Forward IPPV data communication. Keyboard, IR remote control and LED display processing is controlled for customer features and converter tuning functions. An internal tuning PLL and a self diagnostic routine help assure reliable service. In order to make the product "future-friendly" several input/output ports are provided for feature flexibility through head-end control of future peripheral equipment, for Master-Slave operation and for a data communication link.



CONCLUSION

A novel approach to low cost RF addressable Pay-TV scrambling has been shown which enhances premium service security over conventional RF scrambling techniques. Through the use of carrier Phase Modulation (PM) and proprietary SAW filter responses a scrambling effect is produced having video and audio alteration in addition to typical sync suppression properties. The full-featured PM decoder design, incorporating considerations for reliability, addressing data security and noise immunity, signal quality and BTSC stereo compatibility is meeting expectations from initial installations in Cable Systems.

BIOGRAPHY

Michael Long graduated from the University of Illinois in 1969 with a BSEE and has a Master of Electrical Engineering degree from Midwest College of Engineering. He is presently Manager of RF Product Engineering for the CATV Engineering department of Zenith Electronics Corporation. In his 17 years with the company, he has held positions in Research and Development, Color TV Engineering, and VCR-Video Disc Engineering. Mr. Long holds four U.S. Patents and has three additional patents pending.

Richard Citta obtained his BSEE degree in 1969 from Illinois Institute of Technology and his MSEE degree in 1971 from the University of Washington. He is presently a Manager in the Electronic Systems Research and Development department of Zenith Electronics Corporation. Mr. Citta has published several technical papers and holds 12 U.S. patents with 6 patents pending.