VIDEO SCRAMBLING - AN OVERVIEW

V. Bhaskaran, M. Davidov

CORPORATE RESEARCH AND DEVELOPMENT
OAK Industries Inc., Rancho Bernardo, California 92127

ABSTRACT

As cable systems evolve, they will handle diverse information sources such as revenue-generating programs (pay-per-view events), video-text, computer games and two-way services. To ensure the revenue generating potential of such services and to prevent unauthorized reception of signals, the sender and/or receiver may scramble or encrypt the signals.

In this paper, an overview of video scrambling techniqoes is provided. Each technique is asessed in terms of its scrambling depth (degree to which recognizability of an image is destroyed), security (degree to which the technique resists pirating), residual effects in descrambled video and coexistence with other scrambling schemes - in selected cases, computer simulation results are included to demonstrate the efficacy of the scrambling technique. Cost-performance tradeoffs for each scrambling technique and future trends in scrambling are also discussed.

I. INTRODUCTION

Presently, CATV systems offer from 35 to 64 or so channels of programming. Depending on the type of programming, typically there is a mix of scrambled and unscrambled channels, the primary intent of scrambling being to deny access to the unauthorized viewer (in this paper "scrambling" implies manipulation of an analog signal so as to render it unintelligible, whereas, "encryption" implies manipulation of a digital signal to achieve the same result). As addressability becomes increasingly prevalent and two-way services become a reality, two trends in CATV video transmission may emerge -

- o Video signals might be transmitted unscrambled and the HTU (home terminal unit) will be controlled to deny access to unauthorized channels. Such an approach would be best suited for an off-premise decoder and could be cost-effective in a MDU (multiple-dwelling-unit) environment. However, it may be susceptible to spoofing (fooling the upstream channel) and other easy means of piracy.
- o Video signals would be scrambled and access to a channel is provided by means of a descrambler in the HTU. Such a scheme would be cost-effective in a SDU (single-dwelling-unit).

In a CATV system, there will be mix of MDU's and SDU's. Furthermore, in the future, there will be wide variety of information sources offered such as teletext, home-banking etc. Hence, it may be cost-effective to incorporate a descrambler in each HTU and ensure that unauthorized reception of revenue generating video programming is prevented using an <u>effective video scrambling technique</u>.

There are several ways in which a video signal can be scrambled. Although the scrambling techniques vary significantly, the following attributes can be considered to be fundamental in any scrambling technique:-

- o Depth of Scrambling - The technique must not enable observable detail to the extent that programming material offers no entertainment value to the unauthorized viewer. In some instances, the nature of programming material may be such that the scrambled picture should provide no observable details to offend the unauthorized viewer.
- o Security - The technique must a) be time-varying such that real-time descrambling is not (inexpensively) possible, or, b) require very expensive or absoutely unavailable descrambling hardware.
- o Non Degrading - The results of descrambling must not exhibit component or circuit-sensitive residuals, nor be discernable in the descrambled picture.
- o System Complexity - The HTU may encompass several functions besides the descrambler and since the overall cost of the HTU should be low, descrambler hardware must be fairly simple.
- o Multiple Scrambling - As the type of programming offered changes in the CATV system, there may be a need to overlay the previous simple scrambling technique (which gives good depth of scrambling) with a hard to defeat technique (which gives good security).
- o Bandwidth Expansion - Scrambled signal bandwidth should be such that video, audio and synchronization signals can be transmitted in a 6MHz bandwidth.

Scrambling techniques that meet one or all of the attributes can be implemented at RF or BASEBAND.

First generation of video scrmablers were implemented at RF since such schemes resulted in a simple descrambler which did not require any demod-remod configurations. Most RF schemes implemented to date posess weak security and marginal scrambling depth.

Baseband techniques evolved later and are widely prevalent now. Such schemes offer flexibility in that they can be applied to a satellite, STV or CATV environment easily. Baseband schemes can be implemented using digital or analog means. When digital video signal processing becomes cost effective, digital implementation of baseband scramblers may become prevalent.

At OAK, several RF and BASEBAND scrambling techniques have been simulated on a computer. The simulation methodology is described in Section II. A brief description of various RF scrambling techniques is provided in Section III and baseband methods are described in Section IV. In Section V, cost/performance tradeoffs are given for various scrambling techniques. Future trends in scrambling and integration with non-video services in the HTU are discussed in Section VI.

II. COMPUTER SIMULATION PROCEDURE

Simulation procedure consists of the following steps:-

(1) A frame of monochrome video is digitized by a DeAnza image-array processor - display area of digitized frame is 512 scanlines and 512 picture elements per scanline with each picture element represented as a eight bit quantity. Digitized image can be displayed on a DeAnza monitor. This image is input to the VAX 11/780.

(2) Algorithm describing the scrambling technique is implemented on the VAX. All filtering operations and various transmitter, transmission link and descrambler functions are also modelled here.

(3) Scrambled image and descrambled image can be viewed on the DeAnza display monitor.

Simulations were performed for a still-frame of monochrome video - a test frame used in all the simulations is shown in Fig. 1. For NTSC color signals, perceived scrambling depth would be more than that depicted in the simulation results reported in this paper since even a slight modification in the video signal alters the color properties in the perceived image and tends to be annoying to the viewer.

III. RF SCRAMBLING

Conventional RF scramblers accomplish video and/or audio scrambling by jamming video signal using a tone or inverting video signal or suppressing sync in the video signal.

A. Tone Jammer Interfering carrier is placed near the video carrier, thus, causing a beat pattern in the receiver which masks the actual video signal. Scrambling depth depends on the level of the interference carrier and the frequency at which it is located. One possible tone jamming frequency is 2.25MHz above the picture carrier. Due to the manner in which the audio signal is recovered in the receiver, jamming tone at 2.25MHz yields a beat at 4.5MHz which in turn jams the audio signal also. For effective descrambling, a trap is needed to attenuate the interfering carrier - trap attenuation must be around 40 to 60dB to avoid any residual effects in descrambled video. The trap will also attenuate useful luminance energy. Scrambling depth on video is marginal. Video signal security is very weak since the scheme is not time-varying and traps can be built inexpensively. In a cable system, introduction of a tone-jamming carrier for each scrambled channel will increase the number of beats in the system and depending on the receiver front-end, may cause degradations in the non-scrambled channels also.

B. Video Inversion Scrambling is achieved by subtracting from the signal a constant RF carrier at same frequency and phase as actual RF carrier. This will result in the active video signal being treated as a sync signal in the receiver, thus yielding a jagged sync bar in the middle of the displayed picture. Video scrambling depth is marginal. Audio is not scrambled in this method. Descrambling operation is complex since RF carrier must be recovered with correct amplitude, phase and frequency. Errors in recovered carrier phase will appear as color distortions and errors in recovered carrier amplitude will cause luminance distortions. In a multipath environment it will be nearly impossible to reconstruct the carrier accurately - thus luminance and color distortions are inevitable in a multipath environment. A PLL system may be needed to regenerate the RF carrier and depending on the number of scrambled channels, the PLL system may turn out to be fairly complex.

The scheme posesses weak security since the subtraction of RF carrier is not done in a time-varying manner. Time varying scrambling can be realized by subtracting from actual carrier an RF carrier with the same frequency, amplitude and a phase which is varying on a line-by-line or scene change basis - information pertaining to phase can be sent as low level modulation on the aural carrier. If phase is varied on a line-by-line basis, the inaccuracies in reconstructed RF carrier at receiver will cause annoying flicker in displayed image.

C. Sync Suppression Sync suppression scramblers can be realized in one of two ways -

(1) Sine-Wave Scrambler: Video signal is exponentially modulated by a low-frequency sinewave; for descrambling purposes, information regarding this sinewave is transmitted as AM on the aural carrier. The phase and amplitude of the low-frequency sinewave are chosen so as to cause sync suppression. The receiver false locks on active video, thus yielding a jagged sync bar in the middle of the picture. By varying the frequency of the sinewave, time-varying scrambling is achieved.

(2) Square-wave or Gated Sync Scrambler: In this method, during the blanking interval, moulated signal is attenuated by atleast 6dB causing sync and color-burst to be below active video, thus yielding a scrambled signal similar to that

obtained with the sinewave sync suppression scheme. In descrambler, a gain of 6dB is switched in during the horizontal blanking interval - the time instants at which the gain is switched in is transmitted by modulating the aural carrier.

Depth of scrambling is identical for sinewave and squarewave sync suppression schemes. Audio is not scrambled in either method. Sinewave scheme posesses better signal security due to the time-varying manner in which the scrambling frequency can be chosen. With the advent of digital TV chip sets in TV receivers, it is possible to defeat squarewave sync suppressors since such chip sets work on standard and non-standard sync signals (provided color-burst and standard vertical blanking interval synchronization signals are available). A sinewave scheme cannot be defeated by merely reinserting sync; modulation on video must be removed as otherwise luminance and chrominance distortions will result in the descrambled signal.

Descrambler complexity is more for sinewave scheme since in the receiver, circuitry is needed to accurately recover amplitude, phase and frequency of modulating signal. In squarewave scheme since the descrambling signal is a squarewave, such signals can be generated accurately and easily by digital methods.

Descrambler residual effects may degrade video in sinewave scheme. Since the AM signal on the aural carrier is used for descrambling, interference from in-channel chroma subcarrier, strong upper adjacent channel video carrier can cause constant luminance residuals in descrambled video if the descrambling loop bandwidth is not tight. Furthermore, in the sinewave scheme any noise in the descrambling signal is transferred onto the video during the demodulation process. In the squarewave scheme, since active video is never manipulated during the scrambling process there is no noise transfer in descrambling process - any inaccuracies in sync regeneration causes side-by-side motion of displayed picture signal.

At OAK, two other RF schemes have been investigated.

D. Frequency Inversion Inversion of video frequency spectrum leads to a scrambled signal. Frequency inversion schemes can accomplish video and audio scrambling jointly. Furthermore such a scheme can co-exist with the conventional RF schemes described previously.

E. Non-Linear Filtering Video signals can be scrambled by performing a non-linear filtering operation on the IF signal. Example of the computer simulated scrambled signal obtained with a specific non-linear filter is shown in Fig. 2a. Comparing this result with the scrambler input (Fig. 1), the scrambling depth appears to be inadequate - however in a NTSC color signal, perceived scrambling depth would be much more. Descrambling is achieved by using the inverse non-linear filter. This filter can be implemented as a passive device and such a descrambler can be very inexpensive.

If fixed nonlinear filtering is used, the scheme can be defeated fairly easily. Computer simulated result for a time-varying scrambler employing two non-linear filters randomly chosen, is shown in Fig. 2b; good scrambling depth is obtained with this method. A PN sequence can be sed for random filter selection and this sequence in encrypted form can be transmitted to the receiver thus ensuring excellent video signal security.

Residual effects on descrambled signal can be minimized if a nearly exact inverse of the transmitter non-linear filter can be realized - based on the extent of non-linearity required, this is feasible with today's technology.

In this scheme audio is not scrambled. A sync suppression scheme can be added to further enhance scrambling depth.

IV. BASEBAND SCRAMBLING

Baseband schemes posess analog and/or digital (or CCD based) implementations. Presently, most baseband techniques are implemented using analog systems; while, good scrambling depth and security can be obtained, a greater variety of scrambling techniques can be implemented using digital systems. Several baseband scramblers have been studied via computer simulations; a brief description and simulation results are included here.

A. Video Inversion/Sync-Suppression Such a scheme is used in OAK's SIGMA and ORION products and also in various other commercially available scramblers. In SIGMA, sync is suppressed, digital audio is inserted in sync interval and video is inverted randomly on a scene change basis. Even though a non-standard signal is transmitted in SIGMA, it is not easily defeated in a ITT digital TV chip set based receiver since both vertical as well as horizontal sync signals are eliminated (not suppressed) and nonstandard signals are used in VBI. In SIGMA, extremely high security obtained by digitizing and encrypting digital audio, coupled with the video scrambling scheme would thwart unauthorized viewers from deriving any entertainment value from the received signal. Due to the high performance of the HTU, such an approach will be very attractive for a CATV system.

Instead of suppressing sync, sync could be randomly inserted within each video line. This will yield a jagged bar in the middle of the picture. Since sync insertion introduces discontinuities in the video line, bandlimiting the signal will cause distortions in descrambled video.

B. Video Jitter Start time of active video of each scanline is randomly jittered. This has the effect of breaking vertical correlation in a picture. Larger values of jitter yield increased scrambling depth. Large values of jitter can be obtained by modifying blanking interval signals. Computer simulated results obtained for the video jitter scrambler with a random jitter is shown in Fig. 3. This scheme offers good scrambling depth; additional scrambling depth can be obtained using non-standard sync. The start time of jittered video is obtained from a PN sequence and this sequence is sent to HTU in encrypted form for high video security. Simulations have indicated that inaccuraccies in line start-time regeneration at the descrambler can be controlled such that negligible perceptual degradations result in the descrambled signal. For unauthorized descrambling, the receiver must estimate the amount of time-jitter. This can be done by estimating inter-line correlations and then advancing or delaying received signal until the correlation is maximized; however such computations cannot be performed inexpensively in real-time.

Instead of jittering the video, random video fields can be delayed. Descrambling is achieved by delaying the fields which were not delayed in the scrambler. Even though extremely simple hardware can be used for descrambling, this scheme is unacceptable due to inadequate scrambling depth.

C. Time-Reversal Active video of each line is transmitted as is or in time-reversed manner; sync and color-burst are sent as is since unauthorized descrambling would be simple if these signals were also time-reversed. A PN sequence can be used to randomize the time-reversal process; for descrambling, the PN sequence in encrypted form is transmitted thus ensuring a high level of security. Computer simulated result for this scrambler is shown in Fig. 4a.

Good scrambling depth on the video can be obtained with such a scheme. Video security is acceptable for CATV transmissions. The scrambling technique can be defeated using correlation techniques; this requires several lines of storage and high speed logic (an expensive solution).

The scrambler and descrambler are implemented using A/D and two lines of storage. This scheme in combination with a secure audio scheme as in SIGMA is capable of offering a high performance HTU. The residual effects introduced by the descrambler are negligible (line time distortion effects only) except when the PN sequence is received with errors - the digital PN sequence can be error protected to overcome this problem.

Sync suppression can be included to enhance scrambling depth. Furthermore, since the signals are digitized, linear transformations on the digital signal can be performed to further increase the scrambling depth. In Fig. 4b, we show video scrambler output wherein video lines are randomly linear transformed and randomly time-reversed. This two-level scrambling process offers excellent signal security even though the linear transformation method by itself is insecure (an analysis of signal security of the linear transformation scrambler is described in [1]; this analysis indicates that simple operations can be performed to accurately descramble the video without knowledge of the PN sequence). In Fig. 4b, linear transformation is applied to randomly selected lines; if the inverse transformation process in the receiver is not exact, annoying flicker will be perceived in the descrambled image and to avoid this flicker, it is preferable to apply the linear transformation randomly on the basis of scene change.

D. Permutation Of Video Lines A set of video lines is randomly permuted and the re-ordered lines are transmitted. At the receiver, lines are first stored and then re-ordered. Permutation of the lines is accomplished by a PN sequence which must also be available at the receiver for correct descrambling. In Fig. 5a, we show video scrambler output when a set of 16 lines is permuted and in Fig. 5b, scrambler output with 128 line permutation is shown.

Excellent scrambling depth can be achieved with a 128 line store in transmitter and receiver. Due to storage requirements, the HTU would be fairly expensive. Storage requirements can be halved with no decrease in perceived scrambling depth by randomly time reversing some of the permuted video lines - simulation result for a 64 line permutation scheme with random line reversals is shown in Fig. 5c. Excellent signal security is also achieved since (1) unauthorized descrambling would be expensive, and (2) the PN sequence used in head-end for line permutations is encrypted and transmitted to HTU.

Since sync and color burst are not modified, secure audio transmission as per SIGMA scheme can be easily incorporated.

E. Line Dicing In this scheme, active video portion of each line is split into two fragments and these fragments are interchanged prior to transmission; length of each fragment is randomly changed on a line-by-line basis and this information is sent to the HTU. Computer simulated result for such a scrambler is shown in Fig. 6a. This scheme offers excellent scrambling depth and security. The descrambler can be implemented using digital systems or CCD's.

Since video line is fragmented and interchanged, abrupt discontinuities may be introduced in each scrambled video line causing an increase in bandwidth of scrambled signal. Bandlimiting the scrambled signal introduces distortions at the discontinuities causing segment distortions in the descrambled video. In the presence of multipath similar distortions will arise. In Fig. 6b, descrambler output is shown; in this simulation, the line diced signal was filtered by an idealized VSB filter and then transmitted over a link which posessed a multipath of 10dB, 500Nsecs (10dB is the attenuation of the reflected signal relative to the direct signal and 500Nsecs is the delay in the reflected signal relative to the direct signal). Multipath and VSB filtering causes significant segment distortions. The VSB filtering effect can be minimized by stretching a few samples between segment boundaries; however multipath impairments can still be significant.

In unscrambled video signal transmission in CATV systems, a 5% line tilt causes no visible effects, whereas with a line diced signal even a 1% tilt will cause visible low frequency noise (less than 0.5% line tilt is required for no visible noise effects).

Due to degradations caused by VSB filtering, multipath and line-tilt, line-dice scrambling may not be viable in a CATV system.

F. MAC A,B or C Several MAC formats have been proposed for video and audio transmissions over a satellite link. MAC formats by the manner in which it is created, yields a scrambled signal; the scrambling depth can be enhanced by using any one of the baseband techniques we have described in this paper. In its present form, the MAC signal is not directly applicable to CATV transmissions since baseband bandwidths are in the neighborhood of 6MHz. Furthermore, with VSB-AM modulation, there is greater potential for crosstalk within the luminance and chrominance channels (assuming imperfect detection in the receiver).

V. VIDEO SCRAMBLING METHODS - SUMMARY

Various attributes of the video scramblers discussed in this paper are summarized in Table 1. For a CATV system, the scrambling method will be selected based on the performance and whether the type of programming warrants extremely high scrambling depth or moderate scrambling depth which could be realized at a lower cost.

VI. FUTURE TRENDS IN VIDEO SCRAMBLING

It would be attractive to use a video scrambling method which would work well in a satellite, STV and CATV environment so that widespread dissemination of the signals is possible without any intermediate decode/re-encode processing; clearly, a baseband scrambling method would be preferred. With the development of low-cost, high-speed digital signal processors, baseband scramblers would be implemented in the digital domain.

Looking further into the future, fully digital video transmissions will be accomplished in CATV systems. Here, digitized video would be encrypted prior to transmission. When a DES-like encryption algorithm is applied to the digitized video signals of Fig. 1, computer simulated encrypted signal is as shown in Fig. 7. Encryption offers unsurpassed scrambling depth and security. In a CATV environment, most of the proposed new services (e.g. teletext, home-banking, digital audio etc) are essentially digital information. These sources can be time-division multipexed with digital video - the HTU architecture will now resemble a small but powerful computer which is capable of performing a myriad of functions such as decryption, error-correction, noise-reduction etc.

REFERENCES

[1] D. Rayhaudhuri and L. Schiff, "Unauthorized Descrambling of a Random Line Inversion Scrambled TV Signal," IEEE Trans. Commun., vol. COM-31, pp. 816-821, June 1983.

TABLE 1

SUMMARY OF SELECTED VIDEO SCRAMBLING METHODS

Scrambling Technique	Scrambling Depth	Video Security	Residual Effects in Descrambled Video	Descrambler Hardware Complexity	Cost
RF METHODS					
1. Tone Jammer	Marginal. Scrambles Audio also	Inadequate	Useful luminance energy lost	Low. 1 Trap per scrambled channel	Low
2. Video Inversion	Marginal	Inadequate	Luminance and chrominance distortions due to imperfect carrier recovery	Complex	High
3. Sinewave sync suppression	Adequate	Adequate	Noise transfer from descrambling signal to video	Low	Low
4. Squarewave sync suppression	Adequate	Inadequate (sync easily restored)	Video jitter due to inaccurate timing	Low	Low
5. Frequency Inversion	Good. Scrambles Audio also	Good	Scrambled picture due to inaccurate timing	Moderate	Moderate
6. Nonlinear Filter	Good	Good	Distortions due to filter mismatch	Low	Low
BASEBAND METHODS					
1. Video Inversion/ Sync Suppression	Adequate	Adequate	Distortions due to inaccurate DC restoration	Moderate	Moderate
2. Video Jitter	Good	Excellent	Jittered video due to inaccurate timing	Moderate	High
3. Line Reversals	Good	Adequate	Negligible	Low	Moderate
4. Line Permutations	Excellent	Excellent	Negligible	High	High
5. Line Dicing	Excellent	Excellent	Significant segment distortions in CATV links due to VSB filtering and multipath	High	High
6. MAC A,B or C	Good - in conjunction with other scrambling methods	Good	Not presently applicable to 6MHz CATV links	Not Known	Not Known

Fig. 1 Scrambler Input

Fig. 2a Fixed Nonlinear Filter

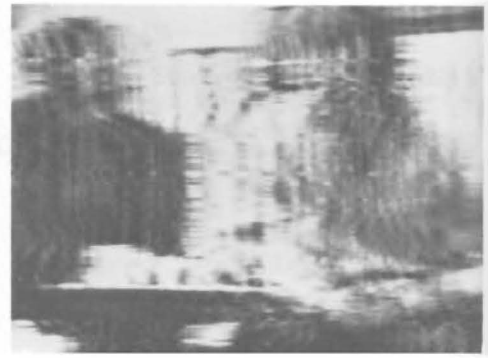

Fig. 2b Time-varying Nonlinear Filter

Fig. 3 Video Jitter

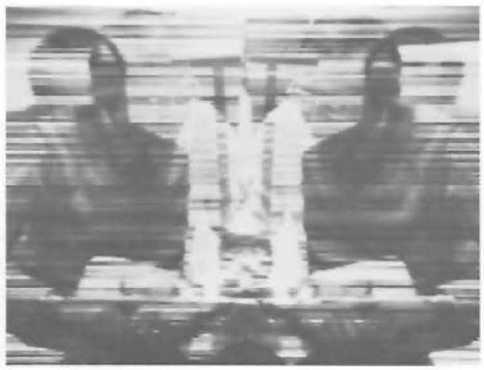

Fig. 4a Random Line Reversals

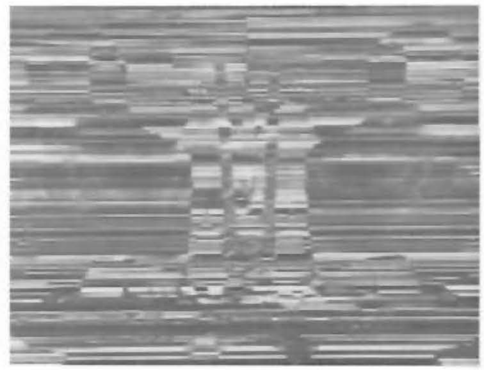

Fig. 4b Random Line Reversals, Random Line Transformation

Fig. 5a 16 Line Permutations

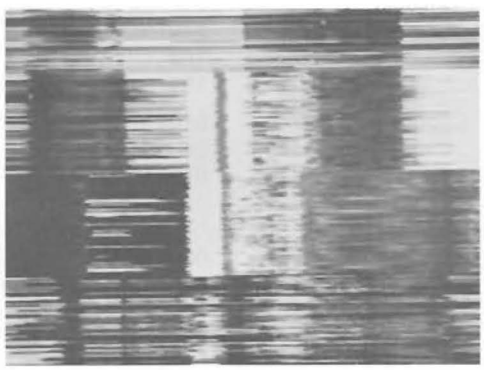

Fig. 5b 128 Line Permutations

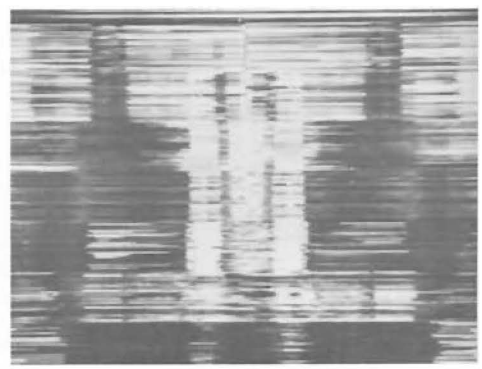

Fig. 5c 64 Line Permutations, Random Line Reversals

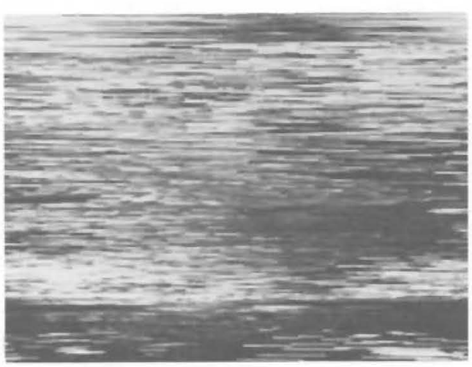

Fig. 6a Line Dicing

Fig. 6b Line Dicing Descrambler Output VSB Filter Effects, Multipath (10dB, 500nsecs)

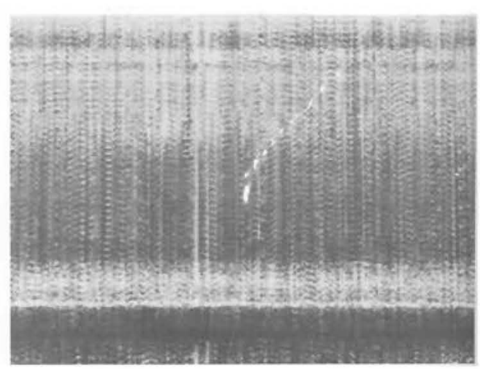

Fig. 7 Encrypted Video