Possibilities for Encoding Analaogue TV Signal in Cable TV Networks

Stanimir Sadinov[1], Kiril Koitchev[2]and Stefan Nemtsov[3]

Abstract – **Cable TV causes a lot of interest which brought to searching for methods and ways of limiting the access to individual "hit" programs. This access control can be effected by encoding the analogue TV signal. The problem that demands a solution here is how to satisfy both sides, in other words the system coder-decoder should be effective and with low cost. This, in short, is the aim of the paper: to analyse analogue methods of encoding and compare them with the current conditions of utilization of cable TV networks in Bulgaria. The paper suggests a specific version which takes into account the above requirements and the "hacker" capabilities as well.**

Keywords – **CATV, TV signals, coding**

I. Introduction

At present there are several technologies for encoding analogue TV signals which are distinguished by their genuine technical solutions. In Bulgaria experiments are confined to two major systems ACS-500 and Crypt On which use Syns Supression technologies [1,2]. They feature the following advantages

- low cost of subscriber's decoder (up to $20) allowing for individual(address) encoding of the channels
- There is no deterioration in the quality of encoding
- Good compatibility of the decoder with the modulator of the main station of the cable operators and the mass TV sets.

The disadvantages include unsettled varieties of schemes which are employed by different cable operators and the lack of coordination with the current law concerning licensing and network running.

II. Presentation

A. Basic principles

With analogue methods for encoding the scrambling technology is used by means of which level slip is effected (row synchronizing pulses – RSP) In the decoder the synchro-pulses should be restored or generated.

Fig. 1 shows oscillograms of the initial signal (at the input of the coder), the encoded signal (at the output of the coder), the decoded signal(at the output of the decoder) and oscillograms of the signal with the carrying frequency which is modulated by the corresponding video signals.

Encoding and decoding can be done at two points of the tract: lower frequency (in the video signal) or higher frequency (in radio signal)

The case with lower frequency (LF):

encoding: video signal is imposed with a sequence of right angled pulses which coincide in time with RSP. As a result RSP slips in level and I the pulses go to the "grey" level;

decoding: the executing circuit of the decoder bypasses (shunts) the encoded signal thus inserting a pulse of zero level in the video signal.

With higher frequency (HF):

encoding: for a while the executing circuit of the coder decreases to the "grey" level;

decoding: during synchro-pulses (RSP) the executing circuit id the decoder makes a jump increase of the coefficient of transmission in such a way that the level of the radio signal may correspond to the maximum level.

High frequency encryption ensures the correct operation of the device for automatic gain control of the input signal (AGC), and recovery of the constant component of the signal (RCC) in the modulator. For this reason, the encryption device must be connected to the modulator using the medium frequency (specification D-38.9 MHz), i.e. after the modulator. Unfortunately, many modulators accommodate this type of connection. This is due to the fact that the decoder needs to have its own de-modulator and all related support components – a device for tuning, channel memory, remote control, etc. As a result these decoders are expensive (around $100). It is possible to make use of the TV de-modulator. However, it is then necessary to connect the decoder between its audio-channel and block of coloured. Too few TV sets have this capability, including those that have a video in/out. Typically, if there a signal detected at the video input, the processor turns off the audio signal.

The schematics discussed earlier are organized according to the "LF encryption – HF decryption" principle, what needs to be in the front is shifted to the rear and vice versa. Encryption is performed at the low frequency and decryption at

[1] Stanimir Sadinov is with the Department of Communications Technology and Equipment, Technical University of Gabrovo, str. "Hadji Dimitar" No 4, 5300 Gabrovo, Bulgaria, E-mail: murry@tugab.bg

[2] Kiril Koichev is with the Department of Communications Technology and Equipment, Technical University of Gabrovo, str. "Hadji Dimitar" No 4, 5300 Gabrovo, Bulgaria, E-mail: koichev@tugab.bg

[3] Stefan Nemtsov is with the Department of Communications Technology and Equipment, Technical University of Gabrovo, str. "Hadji Dimitar" No 4, 5300 Gabrovo, Bulgaria, E-mail: stefan@tugab.bg

the audio frequency. The channel decoder is connected between the source of the video signal and the modulator input. It alters the level of the regular synchronization signal (ACS-500), or altogether removes the synchronization signal and inserting the constant “grey” level (Crypt On). In addition, the control signals for subscriber decoders are inserted in the last rows of every image, at frequency of about 3MHz. This signal, along with the video signal is fed into the modulator of the CRT (Cathode Ray Tube) of the TV set at 20-30 V. This enables the subscriber decoder, placed next to the TV set, to pick up the control signal using a special antenna. Therefore, the decoder need not be connected to the internal schematic of the TV set. The decoder is connected between the subscriber’s connection to the cable network and the TV set’s antenna input. The decoder’s antenna is placed in the rear of the TV set along with the board of the CRT. When the TV set is switched to any channel, the decoder accepts only the inputs of the encryption device for that channel. This the decoder can restore the signal if the signal ”permitted” is received (the subscriber has paid for the program), or to pass through the encrypted signal if the signal “forbidden” is received, or in the absence of the signal “permitted”. The design of the decoder modulates the audio signal using the control signals (Fig. 1), which is equivalent to shifting the level of the video signal. Thus, RSP are “inserted” directly in the audio frequency signal.

Fig. 1 shows the audio frequency signal of a given television channel. In fact, signals from several channels are present at the input of the decoder and the decoder has no frequency selection ability, which is why RSP are inserted simultaneously in the signal of all channels. However, the output signals at the base station are not synchronized and therefore, the encryption devices are also not synchronized. As a result the decoder recovers only the signal on the channel to which the TV set is tuned. On the other channels, RSP are inserted not at their appropriate place, but in a random position. The result is that the other encrypted signals at the output of the decoder are “even more encrypted” – in addition to their “own” RSP, they now also contain “foreign” RSP. Furthermore, if the TV set is tuned to an encrypted channel, then all unencrypted channels at its input (the decoder output) will also be “encrypted”. It is therefore not possible to use the same decoder with several TV sets simultaneously.

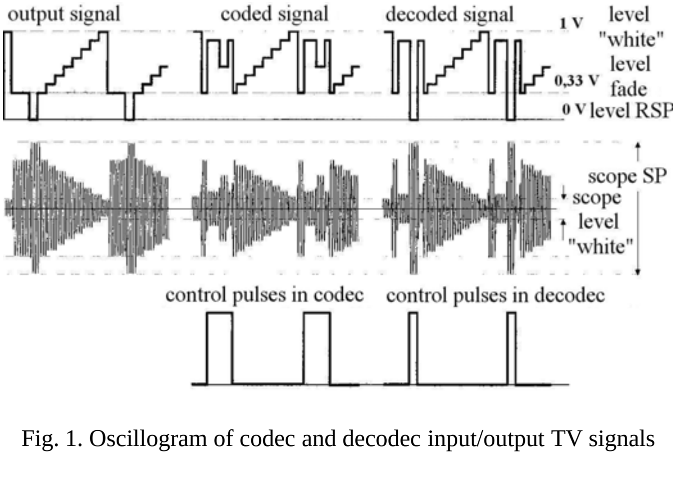

Fig. 1. Oscillogram of codec and decodec input/output TV signals

B. *Possible problems in the transmission and reception area*

This type of “reverse” system has two large advantages: the encryption device can be connected to every modulator and the decoder to any TV set. However, there are shortcomings. At the transmission end some parts of the modulator may interact with the encryption device signal in unintended ways:

— The automatic gain control of the input signal (AGC). It is designed to maintain a constant level of the video signal at the input of its own modulator, despite any random fluctuations in the input signal. However, the level in the active area of the horizontal rows may change from a low “fade out” level to a high “white” level depending on the contents of the image. This is why AGC regulates the overall level, taking into account the range of RSP. However, in the encrypted signal RSP exist only in the frame fade pulse (FFP) and are not present in the active horizontal rows. If the time constant of AGC is small enough, in the active area of an image AGC will register the RSP level as too low and will amplify the image. Therefore, if the modulator has an AGC device at the input, it must be disabled.

— Recovery of the constant component of the signal (RCC). The signal between the source and the modulator (i.e. modulator as a functional element and not an actual device), passes through a number of distribution capacitors, which, along with the input resistors connected to them constitute discriminating units. If the time constant of these units is small, the constant component of the video signal is lost. As a result, the video signal with a range of 0 to 1 V becomes a signal with a range of -0.5 V to 0.5 V. At the same time the level of the synchronizing signal, which is constant in the initial signal, will change from pulse to pulse depending on the contents of every row. Figure 2 shows a ”black and white horizontal bands” signal that has passed through the discriminating units (extreme distortion is apparent). The carrier frequency of such a signal must not be modulated. Instead, the constant signal component must be restored – the low levels of the synchronizing pulses must be “placed” on a horizontal line at 0V. Because of this, it is necessary to use RCC schematic, during RSP the signal is connected to “ground”. Since in the encrypted signal RSP are not present, the RCC schematic needs to be modified.

These problems are only relevant in rare special cases.

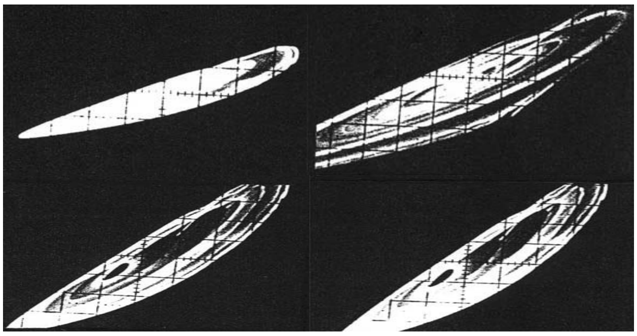

Fig. 2. Video signal at the input and output of the discriminating unit

Typically, the modulation system is implemented with inexpensive modulators, where RCC and AGC are simply not present. The modulator could function without AGC since the input resistance of the steps, when build with modern, components is high. In addition using the appropriate values for the discriminating capacitors can eliminate the need for RCC.

— The decoder receives control signals from the CRT modulator using its antenna. However, during FFP the modulators are turned off – this is necessary, or else all control signals contained in FFP (teletext, signals for test rows, image and color synchronization signals SECAM, etc.) would be visible during the reverse phase of the vertical signal. Therefore, the control data for the decoders are transmitted not through FFP, but in the active rows, the last few rows in every image. As a result, during certain TV setups (vertical sizing) the control data are visible on the screen – an array of apparently random black and white bands at the bottom of the screen.

— In some cases, the above-mentioned method is inappropriate. It is then necessary to hook up a connection at the port for video output of the TV set. If such a port is not available, the hook up is directly with the internal circuits – this method is neither convenient nor safe.

C. Consistent and reliable protection from "unauthorized" access

Despite the inexpensive implementation the solution discussed is pirate proof and can be used in networks where the access tariffs are not too high.

When designing encryption systems one must take into account its cost, and in addition, the demand for this type of technology and its potential for enhancements.

Fig. 3 shows a schematic of a simple pirate decoder suitable for the early types of encryption, where the row synchronizing pulses (RSP) are mixed at level [3]. The graphs in Fig. 1 indicate that in order to recover the signal, it is sufficient to increase the transmission coefficient in the decoder during the reverse phase of the horizontal signal. This is accomplished through the use of a variable attenuator (R4) and resistance of diode VD1. Through the sequence R1, C1, R2 the reverse phase of the signal in L1, is applied at the base of transistor VT1. L1 essentially consists of several coils placed directly over the coils of the output transformer for row scanning.

The polarity of L1 must be such that, during the reverse phase of the signal, the voltage at the base of VT1 must be positive. During the regular phase VT1 does not let the signal through, the collector voltage is the same as the emitter voltage and the current flows through R3, VR1 and VD1. The resistance of VD1 and therefore the rate of transmission between RF-in and RF-out is also small.

The reverse phase of the signal turns VT1 on, and the voltage at the collector is close to zero. The diode VD1 does not let current through and as its resistance rises, so does the transmission coefficient of the decoder. In practice the decoder does not distinguish between modified RSP (active field) and RSP with image fade-out interval, which is constant. In addition, it is very difficult and dangerous to connect L1 to the TV set. In conclusion Fig. 3 represents a rather simple illegal decoder.

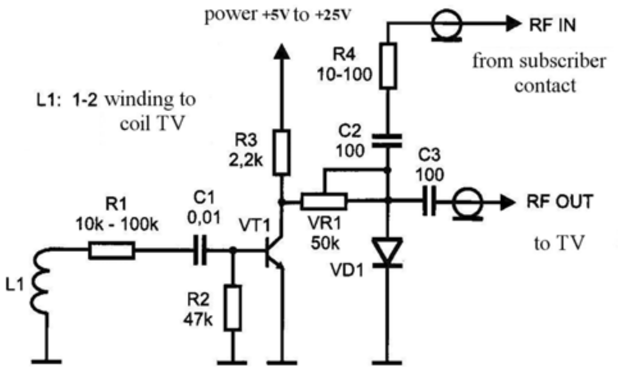

Fig. 3. Schematic of an illegal ("pirate") decoder

The "Crypt On" encryption devices separate RSP from the signal and instead replace them with a signal with a constant level. The recovery of such a signal is rather complex as it is necessary to generate RSP all over again. In order to recover RSP it is possible to use a phase locked loop generator (PLL). The generator is synchronized using the RSP during the image fade-out interval, which are not removed, or modified.

Similar technology is used to recover the color carriers in PAL decoders. They take up 3.5% of the length of a row, which is sufficient to synchronize the signal phase and frequency of the PLL and the junction (support) generator. Then, the entire active segment of the support generator row signal is used by two synchronous phase detectors for color discrimination signals. IFS take up 12.5% of the field, and as a result the phase and frequency synchronization using PLL in the active segment of the field is more stable then when using a PAL decoder.

Various websites list detailed information on illegal decoder schematics for this type of encryption. Therefore, this method can be enhanced to provide a higher degree of protection by adding an image synchronizer to each decoder. This will allow small changes in the length of the row. The image

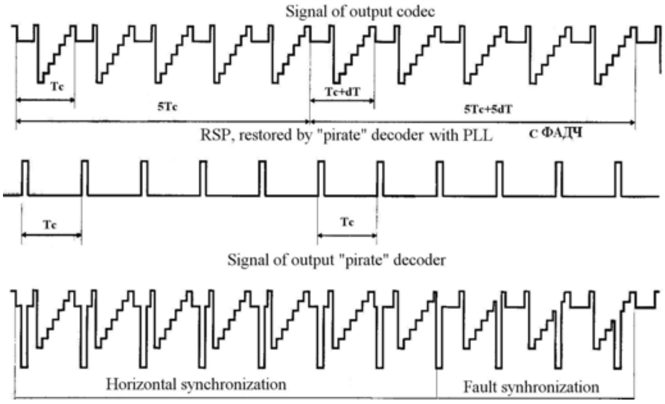
Signal of output codec
Tc
5Tc
Tc+dT
5Tc+5dT
RSP, restored by "pirate" decoder with PLL
с ФАДЧ
Tc
Tc
Signal of output "pirate" decoder
Horizontal synchronization
Fault synhronization

Fig. 4. Enhancement to the encryption system

synchronizer is controlled by the decoder. As a result the encrypted signal is not only separated from RSP, but the row length may be change by small amounts. The change is done by a pseudo-random process generated by the encryption device. For example, beginning with the i-th row, the length N of the row is increased by dT1 and beginning with $i + N$ row the length of the row M is reduced by dT2, etc. The change is small enough so that geometric changes are visible on the screen.

Using the variable row length method of encryption above, it is difficult to decode the signals through RSP recovery and PLL. This is evident in Fig. 4. In section 5T the row length is constant and all decoders whether legal or illegal operate normally. In the area from 5Tc+5dT the length of the row varies by dT. The legal decoder, will be instructed by the encryption device to change the frequency of the recovered RSP. The PLL system dynamically changes the frequency of the RSP so that they are in-synch with the decoder and the image is synchronized. The illegal decoder will continue to generate RSP with phase Tc and thus the RSP will be “mixed” and as a result the horizontal synchronization will be disrupted.

III. Conclusion

The reviewed system for encrypting analog TV signal has several advantages including inexpensive implementation and satisfactory operation, which would make illegal access difficult.

At the moment, however, many cable operators are faced with problems related to the changes in the telecommunications and licensing legislation. In addition, the creditworthiness of many subscribers is poor, which slows down or even obviates the need for encryption at this stage. Hopefully, in the future both the legal and economic environment will improve, along with new and ingenious solutions to the encryption-decryption problem. One such solution, which can be used to implement a stable and inexpensive encryption system, was presented here.

References

[1] Visockii G. Particularity system coding ACS-500 and Cripton, “Telesputnik Media”, St. Petersburg, 9-2000.

[2] Visockii G. System Pay per View, “Telesputnik Media”, St. Petersburg, 8-2000.

[3] Visockii G. System Restrictive access in CATV, “Telesputnik Media”, St. Petersburg, 7-2000.