HUITIEME COLLOQUE SUR LE TRAITEMENT DU
SIGNAL ET SES APPLICATIONS

NICE du 1er au 5 JUIN 1981

DIGITAL ENCRYPTION OF SPEECH USING MULTIPLICATIVE MASKING PATTERNS

Dr. NABIL ELNADY

MILITARY TECHNICAL COLLEGE, CAIRO, EGYPT

RESUME

L'article suivant suggére un nouveau from d'un équipment pour chiffere utilisé sur les canaux étroits et compatibles dans la band CCITT. La théorie et l'appaceil proposés doivent être puissant en comparaison avec l'état à'art de chiffre de la voix et l'équipment d'escalade. En travaillant sur le signal de parole-pour assurer un haut taux d'information-les croisements dés zéros de lònde de parole sont d'abord developpés aprés la transformation l'onde en un signal total de zéro réel. Les zéros redonants obtenus par le generateur du code de mot synchrone et horloge controlé sont alors additionnés au zéro qui transverse le diagramme de l'onde de parole pour produire un signal multiplicativement masqué que ne resemble jamais l'onde d'origine.

SUMMARY

The following paper suggests a new form of ciphering equipment that can be used on narrow-band CCITT-compatable channels. The proposed theory and apparatus might prove to be potent compared to the state-of- art of voice ciphering and scrambling equipments. Working on the speech signal itself, "thus securing high information rate" ,the zero crossings of the speech waveform are first processed" after transforming the waveform to a wholly real zero signal [2] ". Redundant zeros obtained from a clock controlled synchronous code word generator are then added to the zero crossing pattern of the speech waveform to yield a multiplicatively masked signal with no whatsoever resemblence to the original waveform.

At the receiving terminal the redundant zeros are extracted by a complementary procedure and the original zero pattern is produced. These original zero crossings are being then interpolated by the real zero interpolator suggested by the auther [2].

So narrow-band secure voice communication is affected by this method without the need of a vocal tract model " e.g. using a vocoder" to decrease the bit rate as in the case of voice ciphering equipments.

Digital Encryption Of Speech Using Multiplicative Masking Patterns

In order to achieve secure voice communications we may revert to either scrambling or speech ciphering equipment. The security of voice scrambling cannot be considered absolute owing to the large information elements which may provide clues for cryptoanalysis to a listener with special technical equipment.
Voice ciphering may be regarded as a cryptologically secure process. Its major drawback is that about ten times more bandwidth is required than for analog clear speech transmission.

Assuming a voice signal bandwidth of 3KHz, a sampling frequency of at least 6KHz will be required. Using at least 3bits per sample for quantization, a minimum bit rate of 18 kbit/s results. To use voice ciphering on narrow-band CCITT compatable channels, the bit rate of the digital voice signal must be reduced by redundancy e.g. vocoder.

The vocoders extract and digitize the parameters of the speech waveform according to a vocal tract model. The bit rate of the encoded voice message is thus reduced to the order of 2400 to 9600 bit/s as implemented in conventional modems. On normal telephone and radio channels with a bandwidth of approximately 3300 Hz, the rate should not exceed 4800 bit/s. This limitation already defines the technical complexity and consequently the price of the voice cipher system.

In the propesed encrypter/decrypter system the speech digitizing parf operates on the speech waveform itself, resulting in a relatively high information rate.The encrypted signal is annalog,thus can be transmitted with reduced bandwidth much smaller than that for digital encoded signals out of the ciphering device.

Refering to the block scheme of the encrypting device shown in Fig.1, the sppch waveform is sampled each time interval T.During this time window additional zeres are added. These redundant zeros are being obtained from a triggered code word generator which may utilize read-only-memory ROM circuitry or even use a rolling code. The number of code combinations N for M divisions of the time window:

$N = M! \; 2^M$, each of which is effective

In comparison with T-scramblers using similar bandsplitting combinations, we find that 90% of which are redundant. The additional zeros being added to the original zeros of the speech waveform will yield a completely different signal out of the real zero interpolator RZI. This is equivalent to multiplying the eriginal speech waveform by a cyclically varying masking signal.

The nucleus of this device is the so-called RZI device first suggested by Dr.H.B. Voelcker [1]. This device is capable of allotting a minimum bandwidth waveform to a sequence of impulses. In other words it can reconstruct the original signal if impulses at its zero locations are fedto it. The auther suggested a new version of this device which is implemented in this system.[2]. The block scheme of the RZI suggested by the auther is illustrated in Fig.2,

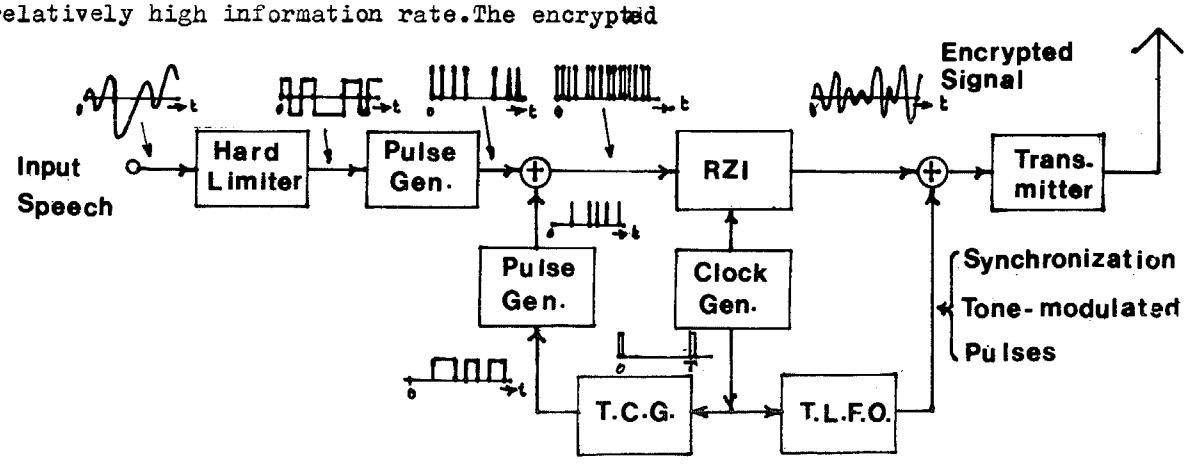

Fig.1 : Block Diagram Of The Encrypting Device

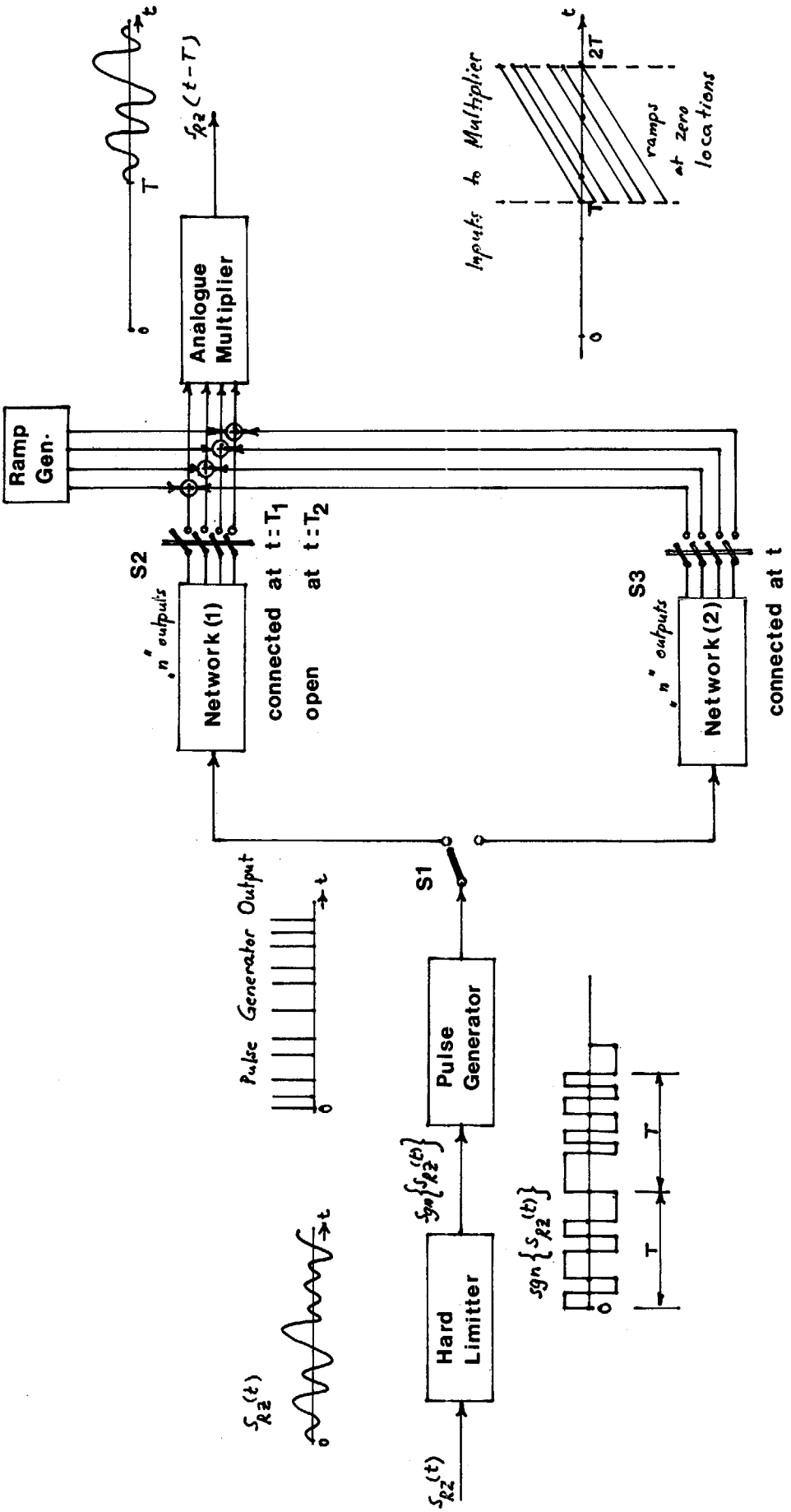

Fig. 2: Block Scheme Of The RZI (Real Zero Interpolator); [2]

Digital Encryption Of Speech Using Multiplicative Masking Patterns

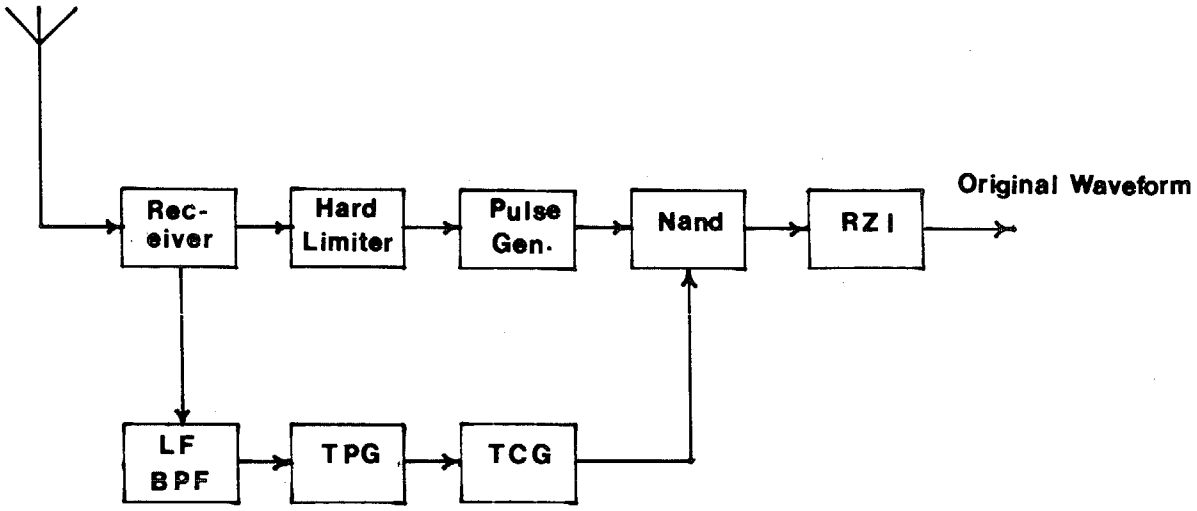

Fig. 3, Block Diagram Of The Decrypting Device

The voice decrypting device shown in Fig.3 extracts the redundant zeros, thus retrieving the original zero train. This zero train is then fed to the RZI which reconstructs the original speech waveform.

Provision of a synchronizing pulse "a low frequency tone" at the beginning of each time interval ensures exact removal of the redundant zeros with the help of the NAND gate.

The above described secure voice communication system proves to be a potent low -priced device capable of securing demands otherwise obtainable only through very complex and expensive systems.

B I B L I O G R S C H Y:

1. VOELCKER, H.B.: "Towards a unified theory of modulation", Proc. IEEE, vol.54, pp. 340-353, March 1966, and pp. 735-755, May 1966.

2. ELNADY, N: "A new version of the RZI", Septieme Colloque Sur Le Traitement Du Signal Et Ses Applications" pp. 36/1-6, Nice 1979.