UDC 004.75

METHODS OF FACTORIAL CODING OF SPEECH SIGNALS

Faure E. V. – Dr. Sc., Associate Professor, Vice-Rector for Research and International Relations, Cherkasy State Technological University, Cherkasy, Ukraine.

Shvydkyi V. V. – PhD, Associate Professor, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine.

Lavdanskyi A. O. – PhD, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine.

Kharin O. O. – Post-graduate student of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine.

ABSTRACT

Context. The paper outlines the methods of factorial coding of speech signals using a factorial code to provide integrated information security and to maintain a receiver and transmitter clock phase. By integrated information security, for the methods proposed in this article, we mean data protection from effects of noise in communication channel and attempts of data unauthorized access in open multiple access telecommunication networks.

Objective. The goal of the research is to provide integrated protection of real-time speech signals based on factorial coding. For this, the methods for factorial coding of speech signals and building speech codecs have been developed. These methods are based on the properties of factorial codes to keep synchronism with the working signal, to detect a significant part of errors caused by the action of noise, natural or created intentionally, to provide the ability to correct all detected errors with a finite accuracy, as well as to provide cryptographic protection against voice message unauthorized listening by hiding the law of converting speech signal samples into a permutation.

Method. The main idea of the proposed methods is to choose permutations for information transferring with a specific set of properties and features that provide the ability to correct errors detected by code and to recover speech signal samples with a finite degree of accuracy (with a nonzero aperture).

Results. The procedures for information coding/decoding have been determined. The results of the experimental evaluation of the model of such systems when working on a communication channel with both independent and multiple bit errors are presented. The magnitude of decoding noise due to the finite accuracy of speech signal samples recovery is determined as a function of bit error probability in a communication channel.

Conclusions. The proposed methods of factorial coding of a speech signal provide integrated information security and recovery with finite accuracy of speech signal samples deformed by noise in communication channel. The requirements to the quality of communication channel (to the value of bit error probability) for comfortable speech perception are determined.

KEYWORDS: factorial code, permutation, speech sample, samples recovery, decoding noise.

ABBREVIATIONS

ADC is an analog-to-digital converter;

BEP is a bit error probability;

DF is a decision feedback;

DTS is a digital transmission system;

FCDR is a factorial code with data recovery by permutation;

PDC is a primary digital channel;

SNR is a signal-to-noise ratio.

NOMENCLATURE

Δ is an interpolation step;

ΔP is a decoder SNR (dB);

ε_j is a decoding error of the j-th sample (the decoding noise, which accompanies the j-th speech signal sample);

$\varepsilon(x)$ is an n-bit error vector that damaged a permutation;

μ_{key} is a key space cardinality;

ν is a code rate;

π is a permutation;

σ is a sum of the permutation π numbers;

A_j is an amplitude of the j-th sample, formed by a source;

$A_j^{\wedge}$ is an amplitude of the j-th sample recovered by a decoder;

$A(x)$ is a data block;

B is a data linear rate;

$d(i)$ is a distance between the receives codeword and the i-th signal vector;

F_{discr} is a speech sampling rate;

h_{dec}^2 is a decoder signal-to-noise ratio;

k is a data block length;

k_{in} is an accumulation coefficient for synchronism entry;

k_{out} is an accumulation coefficient for synchronism exit;

l_r is a permutation symbol code length;

M is a permutation size;

n is a codeword size;

n_{ADC} is an ADC bit depth;

N is a shift register length;

DOI 10.15588/1607-3274-2019-4-18

P_{bg} is a probability of transition from 'bad' to 'good' state;

P_{gb} is a probability of transition from 'good' to 'bad' state;

P_w is a computing unit performance;

p_0 is a bit error probability;

p_{0b} is a bit error probability in a 'bad' state;

p_{0g} is a bit error probability in a 'good' state;

$R(x)$ is a codeword;

$R^{\wedge}(x)$ is a received codeword;

V is a number of samples in a communication session;

W_{noise} is a decoding noise power;

W_{signal} is a signal power;

X is a set of numbers $\{0,1,\ldots,M-1\}$;

Y is a time spent on enumerating all the keys of the key space.

INTRODUCTION

The intensive growth of automation of computer manufacturing equipment and the increasing degree of integration of its element base lead to an acceleration in the rate of increase in productivity and reduction in the cost of computers. The result of these processes is the use of computer systems in all areas of industrial, social and management activities of the global community. These factors generate the development of such opposing trends like the development of the sphere of computer systems application in all departments of human activity, on the one hand, and the equally active introduction of means and methods of unauthorized access of information or its deliberate modification, on the other hand.

Particularly important is the problem of ensuring the confidentiality and integrity of information on the activities of financial agencies and state law enforcement agencies (see, for example [1, 2]). Therefore, the attention of the engineering and scientific community has long been focused on this problem. This explains the interest to the work of recent years [3–16] on creating tools for integrated information security, including protection against the effects of errors in a transmission channel, protection against intentional modification of transmitted messages, and protection against unauthorized access to information.

The object of study is the process of speech data integrated protection.

The subject of study is the methods and means of factorial coding of speech signals.

The purpose of the work is to provide integrated protection of real-time speech signals based on factorial coding. Integrated protection involves:

– correction (with a nonzero aperture) of permutations, carriers of speech signal samples, received with an error and detected by the code;

– protection against unauthorized listening of voice messages.

Using factorial codes for transmission real-time speech signals leads to the need of:

– refusal from exact recovering of samples received with an error;

– transition to recovery of samples received with an error with limited accuracy (i.e., with a non-zero aperture);

– taking into account the psychophysical properties of speech perception.

1 PROBLEM STATEMENT

The task of the research is to develop methods for factorial coding and decoding of speech signals that provide integrated information protection and samples recovery with nonzero aperture.

Choosing the coding with a nonzero aperture inevitably leads to the appearance of a decoder recovery error. This error shows itself in the form of noise accompanying the received signal. The decoding error ε_j of the j-th sample (the decoding noise, which accompanies the j-th speech signal sample) is defined as follows:

$$\varepsilon_j^2 = \left(A_j - A_j^{\wedge}\right)^2.$$

We determine the decoding noise power W_{noise}:

$$W_{noise} = \sum_{j=1}^{V} \varepsilon_j^2 = \sum_{j=1}^{V} \left(A_j - A_j^{\wedge}\right)^2.$$

Note that the signal power in the same communication session will be equal to $W_{signal} = \sum_{j=1}^{V} A_j^2$.

Hence, the decoder SNR in a communication session will be equal to:

$$h_{dec}^2 = W_{signal} / W_{noise} = \sum_{j=1}^{V} A_j^2 \Bigg/ \sum_{j=1}^{V} \left(A_j - A_j^{\wedge}\right)^2.$$

This relation is a random variable. It is influenced by the following components of different physical nature:

– recovery errors due to the properties of the decoding algorithm;

– transformation (by channel noise) of the transmitted permutation into a permutation of the used part of the permutations set [14].

It is often convenient to use the logarithmic decibel scale to express SNR. In this case, decoder SNR (dB) is equal to the difference in levels of signal and decoding noise:

$$\begin{aligned} \Delta P &= P_{signal} - P_{noise} = \\ &= 10\lg\left(W_{signal}/W_{noise}\right) = 10\lg h_{dec}^2\,(dB). \end{aligned} \quad (1)$$

DOI 10.15588/1607-3274-2019-4-18

To solve the designated problem, we will take into account such a psychophysical feature of speech perception as the suppression of a weak signal by a strong signal. This means that if the speech signal is accompanied by low-level noise, then this does not prevent comfortable speech perception (essentially, in these conditions, the noise is imperceptible). Moreover, people experience discomfort in the absence of low-level noise accompanying speech. This is because the mechanism of speech perception has been formed for thousands of years in the conditions of a natural human environment with noises inherent in this environment. Therefore, a person staying in an environment with the absolute lack of interfering noise is unnatural and may cause a negative reaction of the human body. That is why the creation of comfortable speech perception is always in the field of vision of the creators of speech communication systems. Based on this, in this paper we consider a term 'comfort noise' as noise (random, uniformly distributed in amplitude and frequency oscillations. Randomness can be checked by tests and criteria [17–20]) accompanying a speech signal with the upper level of minus 30 dB and the lower level of minus 50 dB. These values define (on average) a threshold of human ear sensitivity.

2 REVIEW OF THE LITERATURE

The methods of combining the functions of cryptography and channel coding began to develop relatively recently. In particular, these include a public-key cryptography method based on error correction codes proposed by McEliece R. J. in [3]. Osmolovskiy S. A. proposed in [4] a stochastic method of integrated information security. This method includes a cascade execution of operations of error-correcting coding and encrypting stochastic transformation. Stakhov A. P. proposed in [5–7] a method of 'golden' cryptography to provide integrated protection. Mazurkov M. I. and Chechelnytskyi V. Ya. in [8–10] proposed to use parametric secrecy of a communication system with noise-like signals in combination with channel coding to provide integrated information security.

The analysis of these works shows that:

– McEliece's cryptosystem provides a slow code speed, requires a very long key length, and is easily decrypted when a key is reused;

– Osmolovskiy's stochastic methods of data protection do not solve the problem of integrating information security functions into a single procedure; they use the XORing operation, which is not always applicable in real data transmission systems with limitations typical for stream ciphers;

– Stakhov's 'golden' cryptography determines only the direction of work and requires additional fundamental research to determine code probability characteristics, evaluate its effectiveness, select an optimal value of the coding matrix degree;

– Mazurkov's and Chechelnytskyi's methods of information security based on perfect algebraic constructions provide parametric secrecy of information transmission and its channel coding, but do not provide message authentication and are limited to use in noise-like signal communication systems.

The factorial codes used in this work are based on the works performed by researchers under the supervision of Borysenko O.A. (see, for example, [11]). They identified some basics of information transfer based on permutations. In particular, they showed that the code built on permutations is an equilibrium with all the properties that follow from this. The use of permutations for information transferring was the starting point for further research on the creation of effective factorial codes [12–16].

The basis for building effective factorial codes consists of the following properties of permutations:

– permutation π on a set of M elements is defined as a bijective function from the set X of cardinality M to itself. Elements of a finite set X are denoted by integers from 0 to $M-1$. Then $X=\{0,1,\ldots,M-1\}$, and we will write a permutation π in the form of a sequence of elements of the set X, where each of the numbers $\{0,1,\ldots,M-1\}$ is applied only once;

– the total number of permutations is equal to $M!$;

– the order of integers $\{0,1,\ldots,M-1\}$ in a permutation π is determined by a transferred information – a data block $A(x)$;

– the sum of the numbers forming a permutation π is equal to $\sigma=0.5\cdot M\cdot(M-1)$.

Given these properties, in [12–16] a number of factorial codes were proposed and their main properties were determined. Among them, we note a factorial code with data recovery by permutation [14], which is the base for the problems solved in this work. FCDR has the following properties:

– checking by the receiving station the fact of the presence in a received sequence of bits of each of the symbols $\{0,1,\ldots,M-1\}$ exactly once ensures detection of all errors of odd multiplicity and a part of errors of even multiplicity, such that create repetitions of symbols and their omissions, i.e. transform the transferred permutation to a non-permutation;

– when choosing M so that $M!\geq 2^k$, creation of replacement tables provides the possibility of bijective mapping of sets $\{A(x)\}\leftrightarrow\pi\leftrightarrow\{R(x)\}$, where $R(x)$ is an n-bit permutation on a set of M elements represented in the binary numeral system (carrier of k-bit word $A(x)$ of source);

– if replacement tables are kept secret, the interception of permutations, carriers of information, by the adversary does not allow reading the transmitted message;

– only 2^k from the full set of $M!$ permutations are used for coding/decoding. The remaining $M!-2^k$ permutations are not used by the code and are redundant. This allows to receiving station detecting errors due to the transformation of the transmitted permutation into permu-

DOI 10.15588/1607-3274-2019-4-18

tations of the unused part of the permutations set. From this it follows that FCDR does not detect only transformations of the permutation, carrier of the transferred sample, into

– another permutation of the allowed part of the set;

– counting an sum in a sliding window of M symbols provides the possibility of finding such a position of the window borders, at which this sum is equal to $\sigma = 0.5 \cdot M \cdot (M-1)$. This position of the window borders corresponds to the in-phase condition of transmitting and receiving stations, i.e. the establishment of frame synchronization of 'transmitter-receiver' tract.

Detection of all errors of odd multiplicity and a part of errors of even multiplicity [12] allows to effectively use factorial codes in data systems with DF, i.e. in systems where error detection is performed by code methods and correction (with zero aperture) is performed by repeated questioning and retransmission of a data block damaged by errors.

In turn, the use of request for error correction leads to the fact that the delivery time of a data block is a random variable. It depends on the intensity of noise in a communication channel and, consequently, on a number of requests of data blocks received with an error. Given these properties, DF systems are effective in non real-time telecommunication systems and cannot be used in real-time telecommunications systems. Such systems, in particular, include voice communication systems organized in an open for general access information transfer environment, for example, in overhead or cable lines, in radio links of any frequency range, etc.

Thus, the listed properties of factorial codes allow building data transmission systems where error correction is performed by requesting data blocks received with an error, but excludes the possibility of their use in real-time speech transmission systems.

3 MATERIALS AND METHODS

First, we will define the main parameters of digitized speech.

It is well known that the main formants of the speech signal are in the range of $\Delta F = 4000\,Hz$. Therefore, according to Kotelnikov's theorem, the speech sampling rate is $F_{discr} \geq 8000\,Hz = 8000\,samples/\sec$, and the sampling interval (the interval between two adjacent samples) is $\tau_{discr} \leq 125\mu s$. The dynamic range of the reproduced speech is at least 40 dB. It follows that the ADC resolution must lie within $n_{ADC} = (13 \div 15)$ to obtain the necessary dynamic range.

Note that the choice of ADC with $n_{ADC} = (13 \div 15)$ corresponds to common practice. We take $n_{ADC} = 15$ as a means of ensuring a better quality of speech reproduction. It follows that to satisfy the condition $M! \geq 2^k$, it is necessary to choose $M \geq 8$. To ensure minimal redundancy, we take $M = 8$. With uniform coding of permutation symbols on a set of cardinality of $M = 8$, the number of bits in each of the symbols is equal to $l_r = 3$. Then the permutation, carrier of a 15-bit sample, will contain $n = l_r \cdot M = 24$ bits, which corresponds to the code rate $\nu = k/n = 0.625$.

We take into account that each sample in a DTS is coded with 8 bits. Therefore, a data transmission rate in a communication line (data linear rate) is equal to $B_{DTS} = F_{discr} \cdot n_{ADC} = 8 \cdot 10^3 \cdot 8 = 64\,Kbit/\sec$. A digital channel with such parameters is called PDC and is the basis of all DTS. With factorial coding, each sample is coded with 24 bits (which is 3 times more than in PDC). So the data linear rate with factorial coding will also be 3 times higher and equal to $B_F = F_{discr} \cdot n = 8 \cdot 10^3 \cdot 24 = 192\,\text{Kbit}/\sec$. An increase in linear rate during factorial coding is a charge for providing integrated information security. Note that if you set the task to provide integrated protection in the end-to-end speech path based on PDC by traditional means, you will have to enter some kind of convolutional error correction code [21–25] with a coding rate (1/2–1/3), as well as use redundancy for providing frame synchronization in a continuous stream of samples. Therefore, it is very likely that the provision of integrated protection in such a tract may require more redundancy than is required in this case. In addition, in PDC, unlike a channel with factorial coding, non-linear compounding is used for coding a speech sample with 8 bits. This reduces the quality of the perceived information.

Now we will evaluate a cryptosystem strength to cracking by the brute-force attack.

The process of bijective mapping of sets $\{A(x)\}$ and $\{R(x)\}$, when the mapping law is kept secret, essentially corresponds to the process of encrypting information. The strength of such a cryptosystem is determined by the key space cardinality. If a replacement table gives the law of sets mapping, the key space cardinality is determined by the cardinality of the set of replacement tables. The redundancy of FCDR (that is equal to $M! - 2^k$ permutations) provides the possibility of creating different permutations (differing from each other in composition and the order of their placement in table). In the problem considered in this paper, the key space cardinality is equal to $\mu_{key} = C_{M!}^{2^k} \cdot (2^k!)$, where the factor $C_{M!}^{2^k}$ determines the key space cardinality due to the change in composition of permutations in the replacement table, and $2^k!$ is the key space cardinality due to the permutation of rows in the replacement table. The presented equality allows determining the cryptosystem strength to its cracking by the brute-force attack, a sequential search of all possible keys of the set μ_{key}. In particular, when $M = 8$, $k = 15$ we get $\mu_{\text{key}} = C_{8!}^{2^{15}} \cdot (2^{15}!) = 7.34 \cdot 10^{142176}$.

DOI 10.15588/1607-3274-2019-4-18

Suppose that the enumeration of keys is performed by a computing unit with a performance of $P_w = 10^{10}$ *keys* / sec. In this case, the time spent on enumerating all the keys of the key space will be $t = \mu_{key} / P_w = 7.34 \cdot 10^{142166}$ sec or $2.33 \cdot 10^{142159}$ years.

Suppose that the performance of the computing unit is increased by 5%, 10% or 15% annually. Then, in accordance with [26], the time spent on enumerating all the keys of the key space μ_{key} taking into account the increase in performance of the computing unit will be

$$Y(5\%) = \log_{\left(1+\frac{5}{100}\right)}\left[\frac{5 \cdot 7.34 \cdot 10^{142166}}{100 \cdot 10^{10} \cdot 365 \cdot 24 \cdot 60 \cdot 60} + 1\right],$$

$$= 6.71 \cdot 10^{6} \; years$$

$$Y(10\%) = 3.43 \cdot 10^{6} \; years,$$

$$Y(15\%) = 2.34 \cdot 10^{6} \; years.$$

The obtained values of strength to the brute-force attack of a voice communication cryptosystem based on data factorial coding make it possible to determine the sufficiency (or insufficiency) of security measures taken.

It should be noted that the FCDR property to ensure the constancy of permutation symbols sum, regardless of the information being transferred, makes it possible to find permutations boundaries in their continuous flow. From the point of view of ensuring the speech exchange security, this property creates the vulnerability of voice communication cryptosystems due to the easy establishment of frame synchronization by an adversary receiver. It is possible to significantly complicate for an adversary the solution of messages interception. To do this, it is enough to perform a bits permutation in a permutation π, carrier of a sample of a speech signal, according to the hidden (from an adversary) rule. This, in essence, denotes the addition of factorial coding system with a second encryption circuit.

Let us now proceed to the basic principles of error correction.

Note that error correction methods with a nonzero aperture are determined by the object to be reconstructed. In this context, it is possible to operate either with speech signal samples or with their permutation-carriers. In any case, to recover the permutations (or samples) deformed by errors, we will use not algebraic, but probabilistic error correction methods. These methods provide the maximum probability of identifying the received permutation (or the sample itself) with their true values. However, different objects of reconstruction require different statistical information about the properties of an error stream in a communication channel and a sensitivity of objects of reconstruction to these factors. This fact determines the difference from each other of the methods of decoding permutations and samples, as well as the composition of the operations performed and the results of their application, including a decoding noise level. Therefore, the main task being solved is decoding noise assessment for different information recovery algorithms. In general, approaches to reconstructing permutations or samples are reduced to replacing a permutation or sample deformed by errors with a most likely permutation or sample.

Now we will consider and analyze two methods for recovering permutations: in the Hamming metric and by linear interpolation.

The essence of the method for recovering permutations in the Hamming metric consists of comparing the permutation received from a communication channel with each of the permutations of the replacement table. For this purpose, Hamming distances from the received sequence are determined to all signal vectors used to transfer information. The result of this operation is to create a catalog of distances between the received *n*-bit sequence $R^{\wedge}(x)$ and each of the signal vectors $R_i(x)$ of the replacement table. This corresponds to the operation:

$$d(i) = R^{\wedge}(x) + R_i(x),$$

$i \in \left[0, 2^k - 1\right]$.

If we consider that $R^{\wedge}(x) = R(x) + \varepsilon(x)$, then we get $d(i) = R(x) + \varepsilon(x) + R_i(x)$ as a result. From this, it follows that with a sequential enumeration of the signal vectors $R_i(x)$ the moment inevitably comes when $R_i(x) = R(x)$ and $d(i) = \varepsilon(x)$. This means that an *n*-bit error vector $\varepsilon(x)$, which damaged the permutation $R(x)$, is necessarily present in a distance catalog.

Thus, a distance catalog can be interpreted as a catalog of error vectors that transform the transferred permutation into a received *n*-bit sequence. Among this set (with a cardinality of 2^k vectors) a real error vector is necessarily present. Now we take into account that with independent bit errors in a block of *n* bits, the probability of an error of a given weight (multiplicity of bit errors in a permutation) obeys the binomial law: $p(t) = C_n^t p_0^t q_0^{n-t}$, $q_0 = 1 - p_0$. In this case, error vectors with small multiplicity are the most likely (if an expected value of a discrete random variable $np_0 \le 1$). It follows that the permutation choosing from the replacement table by the criterion of the minimum distance to the vector of the table is equivalent to the choosing of the most probable noise vector. Based on this, permutations of the minimum distance are selected from the distance catalog and are entered into a catalog of candidates for replacement of the permutation received with an error.

If the minimum distance is provided only to one signal vector, then the received sequence is identified with the permutation corresponding to the given signal vector. A sample is recovered from it and is given to a user.

DOI 10.15588/1607-3274-2019-4-18

If there are at least two signal vectors $R_i(x)$ with the same minimum distance to the received sequence $R^{\wedge}(x)$, then the samples corresponding to these signal vectors are taken as candidates for replacement of the received sequence. The best candidate for replacing a sample received with an error is the closest, in Euclidean space, sample from the list of candidates in relation to the previous sample given to the user. If such a sample is one, then it is taken as a decoded sample. If there are several such samples, then one of the candidates for replacement is chosen randomly as a decoded sample.

The recovering procedure is complete.

The listed operations and the order of their execution ensure the achievement of the following result:

– an increase in the accuracy of speech signal recovery, since all (without exception) permutation, samples carriers, taken with error and detected by the code are subject to correction (with a finite degree of accuracy);

– the possibility of working in real-time is ensured by eliminating the need to request samples received with an error.

The method for recovering permutations by linear interpolation involves:

– selecting permutations in which decoder did not detect errors;

– extracting samples contained in permutations;

– selecting a packet of permutations with detected errors;

– recovering samples by the method of linear interpolation based on the obtained values of samples corresponding to the permutations framing the packet of permutations with detected errors, and the number of permutations in this packet.

To implement this method, an *n*-bit sequence received from a communication channel is checked for correctness. If the results of correctness verification establish that the received sequence is a permutation, then it is checked for belonging to the used subset of permutations (the set of signal vectors). If this check is positive, a sample is retrieved from the permutation obtained. This sample is written to the shift register of the device for recovering erroneous samples, containing N cells of $(k+1)$-bit words. In this case, k bits are retracted to store a sample or to store the current sequence number in a packet of permutations received with an error; and the $(k+1)$-th bit is an indicator defining the storage object in a memory cell.

The first permutation received with an error has the number 1, and the last permutation received with an error has a number corresponding to the length of the packet of signal vectors received with an error.

This allows to identify packets of permutations with detected errors and to recover samples of this packet immediately upon detection of the packet. Sampling recovery is reduced to replacing the $(k+1)$-bit word in the register with the recovered sample and, accordingly, the indicator bit.

As a result, when outputting the contents of the buffer register to the information consumer, the corrected sample stream is output. The service bit follows it. This means that, in contrast to the samples recovery in the Hamming metric, the interpolation method introduces an additional delay corresponding to the accumulation time of N samples. The value of this delay (and, therefore, the length of the package of corrected errors) is determined by several factors. First, we note that this delay should not exceed the speech correlation interval, since error correction by interpolating uncorrelated samples is meaningless. Considering that the speech autocorrelation interval is approximately 0.5 seconds [27, 28], then $N \le 4000$. In reality, the value of N should be substantially less and be determined by the frame synchronization system parameters and properties. This is because frame synchronization of systems with factorial coding is performed by selecting the time position in the window of M symbols. Their sum is $\sigma = 0.5 \cdot M \cdot (M-1)$.

It is obvious that both in the process of searching for synchronism and in the process of its retention within a window of M symbols, there can be both correctly and incorrectly accepted permutations. Therefore, the decision on the achievement or loss of synchronism must be made based on a majority decision, a decision on a majority vote. This number of votes may be different for determining the moment of achieving synchronism in the search (k_{in}) and for determining the moment of loss of synchronism (k_{out}). If the number of errors in the packet exceeds the value of k_{out} in the window of N permutations, then the frame synchronization system will perceive this event as a loss of the clock phase, stop decoding samples, and go into synchronization search mode. From this, it follows that the boundary number of signal vectors N accepted with an error corrected by the interpolation method must satisfy condition $N \le k_{out}$.

Note that a similar situation occurs when correcting errors in the Hamming metric. If the length of the permutation packet received with a detected error exceeds the synchronization system value k_{out}, then the event of clock synchronization loss will be fixed and the transition to the clock phase search mode will occur. Thus, any of the considered methods of speech signal recovery is aimed at correcting errors in the packet of permutations with the length that does not exceed the value of k_{out}. Usually $k_{out} \le 10$ in systems of multiple access with time division of channels.

4 EXPERIMENTS

A software model with tract "speech source – voice encoder – communication channel – speech decoder – speech receiver" has been developed to assess the main technical characteristics of the proposed above methods for recovering samples deformed by noise in a communication channel. The model provides an assessment of the speech tract basic parameters: the probability of error

DOI 10.15588/1607-3274-2019-4-18

detection/non-detection by FCDR decoder, an estimate of the value of sample recovery error. Based on these data, decoding noise power and speech signal security are determined. The main result of the experiment for determining the noise accompanying the decoded speech is the dependence between decoder SNR by (1) and BEP in a communication channel. The model used FCDR with parameters $M = 8$, $k = 15$, $n = 24$, $\nu = 0.625$.

The first version of the codec model implements the decoding algorithm in the Hamming metric. Fig. 1 illustrates a block diagram of such receiving device.

First, we note that binary sequences of digitized speech signal samples transmitted over a communication channel with noise are distorted at a channel output. The fronts of individual packets are randomly shifted from their nominal position; as a result, the duration of packets is a random variable. Therefore, first, it is necessary to restore the time relationship between the elements of a signal, the packets. For this, pre-processing, regeneration, is performed. For this purpose, the receiver contains a clock synchronization system 8. This system ensures synchronization between receiver and transmitter clock generators. Regenerator 1 strobes (polls) the received binary symbol in the least noise susceptible part, in its middle, with synchronous clock cycles. Then regenerator 1 stores it until the next strobing moment. This ensures maximum reliability of bit sequence reception and restores time ratios of packets in their continuous sequence. As a result, a sequence of bits is formed at the output of the regenerator 1. It may contain errors due to the effect of noise in a communication channel at the time of strobing. This sequence is fed to the input of a frame synchronization system 9 and to the input of a selector 2. The frame synchronization system 9 counts in a sliding window the sum of M symbols of the received permutation. If this sum is equal to $\sigma = 0,5 \cdot M \cdot (M-1)$, then, most likely, the permutation boundary is correctly defined; and if not, then, most likely, it is not defined correctly. The clause 'most likely' says that it is impossible to make a decision on the establishment (or loss) of the clock phase in one observation since the sum of symbols in a window is a random value under the influence of noise. The decision can be made on the basis of calculating an expectation of this random process or in the case when most of the samples confirm or refute one of the hypotheses on an observation interval (synchronism is established or synchronism is lost). When a cycle synchronism state is reached, the receiver proceeds to process a sequence of permutations received from a channel carrying speech signal samples. A sample received from a channel and recorded in the selector 2 is checked for correctness. If the received sequence is correct, i.e., it is a permutation, then it is issued to decoder 3 via bus 1. The decoder 3 determine if the permutation belongs to the allowed set of the replacement table. If this check has a positive result, a corresponding sample is extracted from the permutation and sent to the recipient via bus 1 of decoder 3 through connection block 7.

If the received permutation is not contained in the replacement table, i.e., belongs to the non-allowed part of the permutations set, then it is fed via bus 2 of decoder 3 to the first input of the first connection block 4. To the second input of the first connection block 4 the output of selector 2 is connected via bus 2.

As a result, n-bit words of non-permutations and permutations from the non-allowed part of the permutations set are fed to the input of a distance catalog former 5.

The distance catalog former 5 determines Hamming distances between the permutation received from communication channel and each of the permutations of the replacement table. The distance catalog is output to an error correction block 6. In this block, the permutation list is arranged, for example, in the order of decreasing the distance. Permutations with the minimum Hamming distance are separated into a separate list. This list is a list of candidates for replacement received with an error permutation.

If there is only one candidate permutation in this list, then a sample is extracted from it. This sample is output to the consumer through the second connection block 7.

If there are several candidates for a replacement, a sample is extracted from each of them. As a result, a list of candidates for replacement of the sample is formed. A previous sample is extracted from the decoder's memory. An arithmetic difference of the amplitudes of the previous sample and each candidate sample is calculated. The candidate sample with the minimum amplitude difference value is taken as the most probable value of the transmitted sample. It is fed to the consumer. This completes the error correction procedure. The decoder goes into standby mode to receive the next permutation from communication channel. The decoding process is repeated according to the above algorithm.

Decoding of factorial code with recovery of samples received with an error by interpolation is performed using a device, which block diagram is shown in Fig. 2.

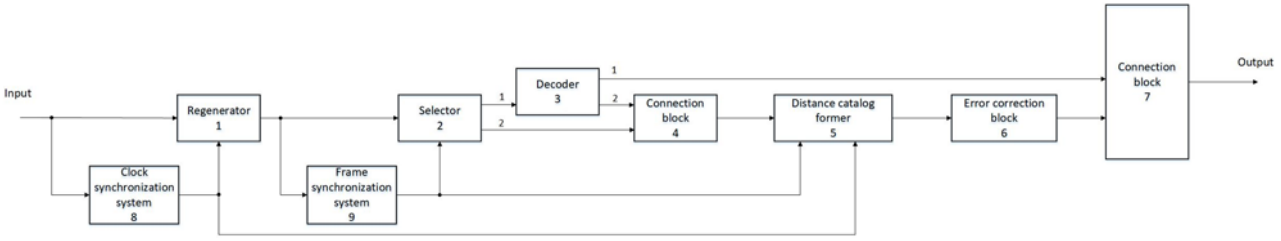

Figure 1 – The block diagram of speech signal receiving device with permutations recovery in the Hamming metric

DOI 10.15588/1607-3274-2019-4-18

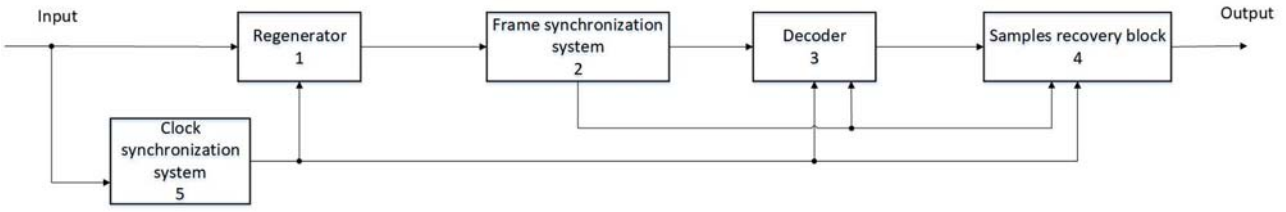

Figure 2 – The block diagram of speech signal receiving device with permutations recovery by interpolation

The receiving device contains a clock synchronization system 5, a regenerator 1, and a frame synchronization system 2, which in this device are made identically with the same device blocks in the Hamming metric and perform the same functions.

After the frame synchronization procedure is completed, 24-bit sequences received from a channel are input to the decoder 3. Decoder 3 performs a validation of the received permutation.

If the received sequence is a signal vector, a sample, a word of 15 bits, is extracted from it. The 16th service bit that is an indicator of the contents of this memory cell is added to the sample (for example, a logical zero).

If the received sequence is not a permutation or a permutation not used for transferring voice information, a word of 15 bits representing the sequence number in a packet of permutations received with errors is entered into the memory cell instead of a sample. The 16th service bit, a content indicator of the memory cell, is assigned to the binary one.

Thus, if several consecutive permutations affected by errors are received, the last number will determine the length of error packet N. This sequence of 16-bit words from the output of the decoder 3 is transmitted to a samples recovery block 4 for correcting error packets. A block diagram of the block 4 is shown in Fig. 3.

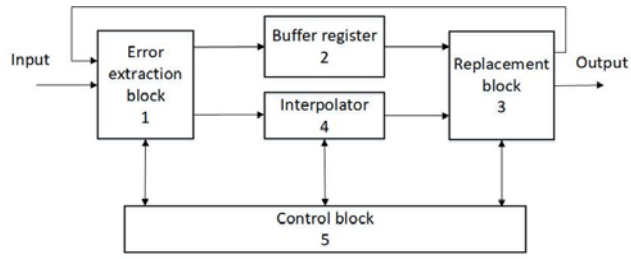

Figure 3 – The block diagram of a samples recovery block

The words coming from the decoder get into the error extraction block 1. The main purpose of this block is to extract the following three words from an incoming stream: samples $A_j^{\wedge}$ and $A_{j-(N+1)}^{\wedge}$ that frame a packet of errors and an error packet length indicator N.

From this data, an interpolation step $\Delta = \left(A_j^{\wedge} - A_{j-(N+1)}^{\wedge}\right) \Big/ (N+1)$ is calculated and transferred to interpolator 4. Thus, after receiving the first permutation without detected error that closes a packet of permutations with detected errors, the values $A_j^{\wedge}$, $A_{j-(N+1)}^{\wedge}$, N, and Δ are loaded into the interpolator 4. This allows to start an interpolation procedure, a procedure for calculating and replacing samples that correspond to error-corrupted permutations. To do this, the procedure of replacing the contents of the cell with a 15-bit word of the recovered sample is performed in the replacement block 3, in the interval between two samples (equal to 125 microseconds), as well as changing a service symbol from a binary one to zero.

Control block 5 controls this process.

Calculating the restored sample involves performing operation $A'_{j-(N+1-i)} = A'_{j-(N+1)} + [i\Delta]$, where $[A]$ denotes rounding to the nearest integer of A.

Thus, the proposed algorithm for the samples recovery using the linear interpolation method ensures the correction of a packet of errors due to the effect of noise in a communication channel with finite accuracy. This means that a decoded speech will be accompanied by additional decoding noise. The presence of decoding noise with a level from minus 30 dB to minus 50 dB corresponds to conditions for speech transmission in an environment with natural noise.

5 RESULTS

The developed software models allow to change the nature of noise in a communication channel. The simulation of voice information transmission for channels with independent bit errors and channels with multiple bit errors caused by multiplicative noise has been performed in order to determine the main parameters of the proposed methods of speech signals factorial coding. The source used a fixed sample of a real speech signal.

The channel model with independent bit errors used a binomial law of their distribution with one parameter p_0.

The channel model with multiple errors used a Gilbert-Elliott model [29, 30]. This model assumes two channel states, ‘good’ and ‘bad’. The law of channel states changing is described by a Markov chain of order one. The simulation was performed for cable channels. In this case, an absolute (average) BEP [31, 32] $p_0 = \left(P_{bg} \Big/ \left(P_{bg} + P_{gb}\right)\right) \cdot p_{0g} + \left(P_{gb} \Big/ \left(P_{bg} + P_{gb}\right)\right) \cdot p_{0b}$ was used to estimate the decoding methods under conditions of multiple errors caused by multiplicative noise.

The results of testing of two models of factorial code decoder show the decoder SNR depending on BEP in communication channel and the nature of noise. Fig. 4–6 graphically illustrates the test results.

DOI 10.15588/1607-3274-2019-4-18

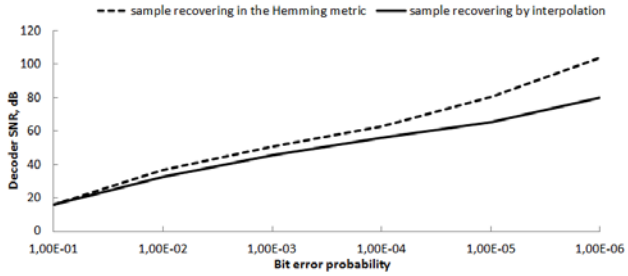

Figure 4 – Decoder SNR vs BEP in channels with independent bit errors

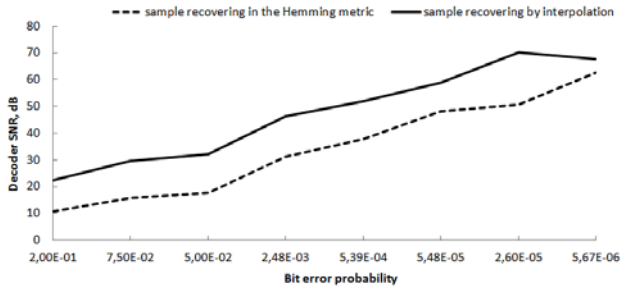

Figure 5 – Decoder SNR vs BEP in channels with multiple errors caused by multiplicative noise

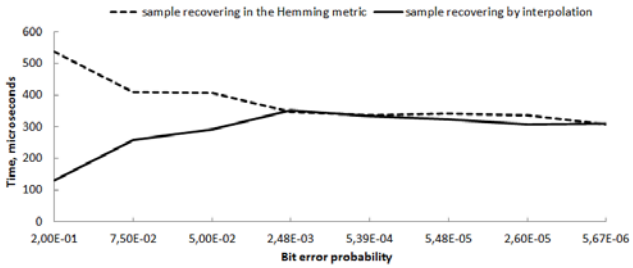

Figure 6 – Graph of average time of samples recovery vs BEP

6 DISCUSSION

It can be concluded, from the above graphs, that each of the decoding methods is oriented to different types of channels in their statistical properties of error appearing.

From Fig. 4, it can be seen that SNR of decoder with samples recovery in the Hamming metric is higher than SNR of decoder with samples recovery by interpolation in the whole range of BEP values in a communication channel with independent bit errors. Channels organized in underground cable lines including fiber-optic belong to this category. It also includes microwave radio lines operating in favorable weather conditions and without applying electronic countermeasures to them.

In turn, from Fig. 5, it can be seen that decoder with samples recovery by interpolation is oriented to channels with multiple bit errors and provides a greater level of SNR in comparison with decoder in the Hamming metric. Radio channels of the short-wave range in normal conditions and radio channels of any radio-frequency range in the conditions of electronic countermeasures can be referred to this category of channels.

We would like also to point out that the sample recovering procedure by interpolation is simpler to implement and requires fewer resources than the recovery in the Hamming metric. From Fig. 6 it can be seen that the performance of decoder with samples recovery by interpolation is significantly higher when $10^{-3} < p_0 \le 10^{-1}$. With the improvement of a channel quality, mostly single errors increasingly begin to occur and the performance of both algorithms becomes identical.

It should be noted that the noise accompanying the recovered speech signal using the recovery algorithm in the Hamming metric for channels with independent errors and the interpolation method for channels with multiple bit errors can be categorized as comfort noise for $10^{-4} \le p_0 \le 10^{-2}$. Decoding noise can be ignored when improving the quality of communication channel.

It follows from this that the threshold value of the transmission reliability at which the specified quality indicators are ensured in terms of the decoding noise level is $p_0 \le 10^{-2}$.

Note also that the proposed coding methods provide better SNR for high BEP compared with turbo codes [33–36]. For example, turbo codes [36] used in the GSM standard have lower SNR when $10^{-3} < p_0 \le 10^{-2}$.

Finally, we would like to admit that the methods proposed in this research provide a code rate of 0.65. Convolutional codes [21–26] as the most widely used codes in speech coding, have a relatively low code rate of 1/2–1/3. In addition, convolutional codes do not provide cryptographic protection, since it contains information bits in a code sequence.

CONCLUSIONS

The urgent problem of integrated protection against unauthorized access and channel errors of real-time speech signals based on factorial coding is solved.

The scientific novelty of obtained results is that two methods of factorial coding of speech information with permutations recovery are firstly proposed. These methods involve converting, for example, by substitution table, samples of speech information into permutations. These permutations after encoding to a binary code are transmitted over a communication channel. The decoding process is to replace a permutation to a speech signal sample. In the case of damage of the received permutation, according to the first method for recovering permutations in the Hamming metric, speech signal is restored by finding the signal vector closest to the permutation in the Hamming metric. If there are several such signal vectors, then one which sample is closest in Euclidean metric to the predecoded sample is selected. The method for recovering permutations by linear interpolation involves restoring a speech signal by linear interpolation based on known adjacent samples. These methods allow to detect and correct errors in real-time with non-zero aperture. This in turn allows using factorial coding for real-time data. The strength to cracking of the protection system by brute-force attack is estimated in millions of years.

The practical significance of the research is that the algorithms and block diagrams of speech signal receiving devices have been developed. This allows their practical

DOI 10.15588/1607-3274-2019-4-18

implementation. 2. The experimental results show that an optimal area of application of the method for recovering permutations in the Hamming metric is communication channels with independent bit errors and BEP $p_0 \le 10^{-2}$. Under these conditions, the Hamming decoder shows the best results, and the decoding noise does not exceed the values of the comfort noise level. An optimal area of use of the method for recovering permutations by linear interpolation is communication channels with multiple bit errors caused by multiplicative noise, in particular, radio channels of the short-range radio band or radio channels of any radio band with an unfavorable noise situation. When using the proposed algorithms in optimal conditions with the BEP $p_0 \le 10^{-2}$, the decoding noise level does not exceed the values of the comfort noise level.

Prospects for further research are to study the effectiveness of the proposed methods in real-world conditions by developing prototype devices.

ACKNOWLEDGEMENTS

The authors express their sincere appreciation to Dc.Sc. Techn., Professor Volodymyr Rudnytskyi and Ph.D., Associate Professor Anatoly Shcherba for the full support of this area of work, constructive comments and suggestions when writing the work, and useful discussion of the results.

REFERENCES

1. Gnatyuk S. Critical Aviation Information Systems Cybersecurity, *Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security*, 2016, Vol. 47, No. 3, pp. 308–316. DOI: 10.3233/978-1-61499-716-0-308
2. Gnatyuk S., Kinzeryavyy V., Kyrychenko K. et al. Secure Hash Function Constructing for Future Communication Systems and Networks, *Advances in Intelligent Systems and Computing*, 2019, Vol. 902, pp. 561–569. DOI: 10.1007/978-3-030-12082-5_51
3. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Theory, *The Deep Space Network Progress Report, DSN PR 42–44,* 1978, pp. 114–116.
4. Osmolovskij S. A. Stoxasticheskaya informatika: innovacii v informacionnyx sistemax. Moscow, Goryachaya liniya-Telekom, 2012, 321 p.
5. Stakhov A. P., Massingue V., Sluchenkova A. Introduction into Fibonacci Coding and Cryptography. Kharkov, Osnova, 1999, 234 p.
6. Stakhov A. P. Fibonacci Matrices, a Generalization of the 'Cassini Formula', and a New Coding Theory, *Chaos, Solitons & Fractals*, 2006, Vol. 30, No. 1, pp. 56–66. DOI: 10.1016/j.chaos.2005.12.054
7. Stakhov A. P. .: The 'Golden' Matrices and a New Kind of Cryptography, *Chaos, Solitons & Fractals*, 2007, Vol. 32, No. 3, pp. 1138–1146. DOI: 10.1016/j.chaos.2006.03.069
8. Mazurkov M. I., Chechel'nitskii V. Ya., Murr P. Information security method based on perfect binary arrays, *Radioelectronics and Communications Systems*, 2008, Vol. 51, No. 11, pp. 612–614. DOI: 10.3103/S0735272708110095
9. Mazurkov M. I., Chechelnytskyi V. Ya., Meleshkevich A. N. et al. Methods of improving information security by integrating multiplexing, ciphering and channel encoding operations, *Radioelectronics and Communications Systems*, 2011, Vol. 54, No. 5, pp. 227–240. DOI: 10.3103/S0735272711050013
10. Mazurkov M. I. Composite matrix cipher based on perfect binary arrays, *Radioelectronics and Communications Systems,* 2013, Vol. 56, No. 3, pp. 133–140. DOI: 10.3103/S0735272713030047
11. Borisenko A. A., Gorjachev A. E., Lopatchenko B. K. et al. Perestanovki v telekommunikacionnyx setyax, *Visnik Sums'kogo derzhavnogo universitet*u, 2013, No. 2, pp. 15–22.
12. Faure E. V., Shvydkyi V. V., Shcherba A. I. Information integrity control based on the factorial number system, *Journal of Baku engineering university – Mathematics and computer science*, 2017, Vol. 1, No. 1, pp. 3–13.
13. Faure E. V., Shvydkyi V. V., Shcherba V. O. Combined factorial coding and its properties, *Radio Electronics, Computer Science, Control,* 2016, No. 3, pp. 80–86. DOI: 10.15588/1607-3274-2016-3-10
14. Faure E. V. Faktorial'noe kodirovanie s vosstanovleniem dannyx, *Visnyk Cherkas'kogo derzhavnogo tehnologichnogo universytetu*, 2016, No. 2, pp. 33–39. DOI: 10.24025/bulletinchstu.v1i2.82932
15. Faure E. V. Factorial coding with error correction, Radio Electronics, Computer Science, Control, 2017, No. 3, pp. 130–138. DOI: 10.15588/1607-3274-2017-3-15
16. Faure E. V., Shcherba A. I., Kharin A. A. Factorial Code with a Given Number of Inversions, Radio Electronics, Computer Science, Control, 2018, No. 2, pp. 143–153. DOI: 10.15588/1607-3274-2018-2-16
17. Marsaglia G. DIEHARD battery of tests of randomness [Electronic resource]. Access mode: http://www.stat.fsu.edu/pub/diehard
18. Rukhin A., Soto J., Nechvatal J. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: Spec. Pub. 800–22 rev. 1a, National Institute of Standards and Technology. Gaithersburg, MD, 2010, 153 p.
19. L'ecuyer P., Simard R. TestU01: A C Library for Empirical Testing of Random Number Generators, *ACM Transactions on Mathematical Software*, 2007, Vol. 33, No. 4, 40 p. DOI: 10.1145/1268776.1268777
20. Faure E. V., Shcherba A. I., Rudnytskyi V. M. The Method and Criterion for Quality Assessment of Random Number Sequences, *Cybernetics and Systems Analysis,* 2016, Vol. 52, pp. 277–284. DOI: 10.1007/s10559-016-9824-3
21. Hagelbarger D. W. Recurrent codes: Easily Mechanized, Burst-Correcting, Binary Codes, The Bell System Technical Journal, 1959, Vol. 38, Issue 4, pp. 969–984. DOI: 10.1002/j.1538-7305.1959.tb01584.x
22. Hagelbarger D. W. Error Detection Using Recurrent Codes, *AIEE Winter General Meeting.* New York, 31 January–5 February 1960. : Proceedings. – New York, IEEE, 1960.
23. Pereira F., Guardia G., Assis F. Classical and Quantum Convolutional Codes De-rived from Algebraic Geometry Codes, *IEEE Transactions on Communications,* 2019, Vol. 67, No. 1, pp. 73–82. DOI: 10.1109/TCOMM.2018.2875754
24. Yang Q., Liew C. Asynchronous Convolutional-Coded Physical-Layer Network Coding, *IEEE Transactions on Wireless Communications*, 2015, Vol. 14, No. 3, pp. 1380–1395. DOI: 10.1109/TWC.2014.2365822
25. Nooraiepour A., Duman T. M. Randomized Convolutional Codes for the Wiretap Channel, *IEEE Transactions on*

DOI 10.15588/1607-3274-2019-4-18

Communications, 2017, Vol. 65, No. 8, pp. 3442–3452. DOI: 10.1109/TCOMM.2017.2704586
26. Lavdanskyi A. O. Time assessment of formation of number sequences under increase of calculation unit performance, *The scientific potential of the present: International Scientific Conference, St Andrews, Scotland, United Kingdom, 1 December 2016 : proceedings*. St Andrews, Scotland, United Kingdom, 2016, pp. 123–126.
27. Rabiner L. R., Schafer R. W. Introduction to Digital Speech Processing. Delft, now Publishers Inc., 2007, 200 p. DOI: 10.1561/2000000001
28. Wang L., Doclo S. Correlation Maximization-Based Sampling RateOffset Estimation for Distributed Microphone Arrays, *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 2016, Vol. 24, No. 3, pp. 571–582. DOI: 10.1109/TASLP.2016.2517326
29. Gilbert E. N. Capacity of a Burst-Noise Channel / E.N. Gilbert // *Bell System Technical Journal*, 1960, Vol. 39, Issue 5, pp. 1253–1265. DOI: 10.1002/j.1538-7305.1960.tb03959.x
30. Elliott E.O. Estimates of Error Rates for Codes on Burst-Noise Channels, *Bell System Technical Journal*, 1963, Vol. 42, Issue 5, pp. 1977–1997. DOI: 10.1002/j.1538-7305.1963.tb00955.x
31. Hasslinger G., Hohlfeld O. The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet, *Measurement, Modelling and Evalutation of Computer and Communication Systems: 14th GI/ITG Conference, Dortmund, Germany, 31 March – 2 April 2008 : proceedings*, VDE VERLAG, 2008.
32. Ellis M., Pezaros D. P., Kypraios T. et al. Modeling of packet loss and delay and their effect on real-time multimedia service quality, *Computer Networks*, 2014, Vol. 70, pp. 384–399. DOI: 10.1016/j.comnet.2014.05.013
33. Heegard C. Turbo Coding / C. Heegard, S.B. Wicker. – Norwell: Kluwer Academic Publishers, 1999. – 476 p. DOI: 10.1007/978-1-4757-2999-3
34. Weithoffer S., Nour C. A., When N. et al. 25 Years of Turbo Codes: From Mb/s to beyond 100 Gb/s, *Turbo Codes and Iterative Information Processing: 10th IEEE International Symposium, Hong Kong, China, 3–7 December 2018 : proceedings.* IEEE Computer Society, 2018. DOI: 10.1109/ISTC.2018.8625377
35. Babar Z., Chandra D., Nguyen H. V. et al.] Duality of quantum and classical error correction codes: Design principles and examples, *IEEE Communications Surveys and Tutorials*, 2019, Vol. 21, Issue 1, pp. 970–1010. DOI: 10.1109/COMST.2018.2861361
36. Panayiotis D. P., Thomas A. S., Prabodh V. et al. Turbo Coded Modulation over GSM Channels, *Third Generation Wireless and Beyond: International Conference, San Francisco, California, 6–8 June 2001, Proceedings.* San Francisco, IEEE, 2001.

Received 19.06.2019.
Accepted 25.09.2019.

УДК 004.75

МЕТОДИ ФАКТОРІАЛЬНОГО КОДУВАННЯ МОВНИХ СИГНАЛІВ

Фауре Е. В. – д-р техн. наук, доцент, проректор з науково-дослідної роботи та міжнародних зв'язків Черкаського державного технологічного університету, Черкаси, Україна.

Швидкий В. В. – канд. техн. наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Лавданський А. О. – канд. техн. наук, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Харін О. О. – аспірант кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

АНОТАЦІЯ

Актуальність. У роботі викладено методи факторіального кодування мовних сигналів, що використовують факторіальний код для забезпечення інтегрованого захисту інформації та підтримки циклової фази розподільників приймання/передавання. Під інтегрованим захистом розуміється захист інформації від впливу завад у каналі зв'язку і спроб несанкціонованого доступу у відкритих телекомунікаційний мережах множинного доступу.

Мета роботи. Метою цієї роботи є забезпечення інтегрованого захисту мовних сигналів реального часу на основі факторіального кодування. Для цього в роботі розроблено методи факторіального кодування мовних сигналів і побудови мовних кодеків, що базуються на властивостях факторіальних кодів утримувати тактовий і цикловий синхронізм за робочим сигналом, виявляти значну частину помилок, обумовлених впливом завад природного походження або створених навмисно, забезпечувати можливість виправлення всіх виявлених кодом помилок зі скінченною точністю, а також забезпечувати криптографічний захист від несанкціонованого прослуховування мовного повідомлення за рахунок приховування закону перетворення вибірок мовного сигналу в сигнал – перестановку.

Метод. Основна ідея запропонованих методів полягає у виборі для перенесення інформації перестановок з певним набором властивостей і ознак, що забезпечують максимальну виявляючу здатність коду, здатність виправлення виявлених кодом помилок і відновлення вибірок мовного сигналу зі скінченним ступенем точності (з ненульовий апертурою).

Результати. Визначено процедури кодування/декодування інформації, що забезпечують виявлення та виправлення на приймальній станції вибірок мовного сигналу з ненульовий апертурою. Викладено результати експериментальної оцінки моделі таких систем під час роботи каналом зв'язку як з незалежними бітовими помилками, так і з пакетуванням помилок. Визначено величину шуму декодування, обумовленого скінченною точністю відновлення прийнятих з помилкою вибірок мовного сигналу, як функції ймовірності помилки в послідовності біт під час передавання інформації каналом зв'язку.

Висновки. Запропоновано методи факторіального кодування мовного сигналу, що забезпечують інтегрований захист інформації і відновлення зі скінченною точністю вибірок мовного сигналу, деформованих завадами в каналі зв'язку. Визначено вимоги до якості каналу зв'язку (до значення ймовірності бітової помилки в каналі зв'язку), за якого забезпечується комфортне сприйняття мови.

DOI 10.15588/1607-3274-2019-4-18

КЛЮЧОВІ СЛОВА: факторіальний код, перестановка, таблиця замін, вибірка мовного сигналу, відновлення вибірок, шум декодування.

УДК 004.75

МЕТОДЫ ФАКТОРИАЛЬНОГО КОДИРОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ

Фауре Э. В. – д-р техн. наук, доцент, проректор по научно-исследовательской работе и международным связям Черкасского государственного технологического университета, Черкассы, Украина.

Швыдкий В. В. – канд. техн. наук, доцент, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Лавданский А. А. – канд. техн. наук, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Харин А. А. – аспирант кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

АННОТАЦИЯ

Актуальность. В работе изложены методы факториального кодирования речевых сигналов, использующие факториальный код для обеспечения интегрированной защиты информации и поддержки цикловой фазы распределителей приема/передачи. Под интегрированной защитой понимается защита информации от воздействия помех в канале связи и попыток несанкционированного доступа в открытых телекоммуникационный сетях множественного доступа.

Цель работы. Целью данной работы является обеспечение интегрированной защиты речевых сигналов реального времени на основе факториального кодирования. Для этого в работе разработаны методы факториального кодирования речевых сигналов и построения речевых кодеков, основанные на свойствах факториальных кодов удерживать тактовый и цикловой синхронизм по рабочему сигналу, выявлять значительную часть ошибок, обусловленных влиянием помех естественного происхождения или созданных искусственно, обеспечивать возможность исправления всех выявленных кодом ошибок с конечной точностью, а также обеспечивать криптографическую защиту от несанкционированного прослушивания речевого сообщения за счет скрытия закона преобразования выборок речевого сигнала в сигнал-перестановку.

Метод. Основная идея предлагаемых методов состоит в выборе для переноса информации перестановок с определенным набором свойств и признаков, обеспечивающих максимальную обнаруживающую способность кода, способность исправления обнаруженных кодом ошибок и восстановления выборок речевого сигнала с конечной степенью точности (с ненулевой апертурой).

Результаты. Определены процедуры кодирования/декодирования информации, обеспечивающие обнаружение и исправление на приемной станции выборок речевого сигнала с ненулевой апертурой. Изложены результаты экспериментальной оценки модели таких систем при работе по каналу связи как с независимыми, так и с пакетирующимися битовыми ошибками. Определена величина шума декодирования, обусловленного конечной точностью восстановления принятых с ошибкой выборок речевого сигнала, как функции вероятности ошибки в последовательности бит при передаче информации по каналу связи.

Выводы. Предложены методы факториального кодирования речевого сигнала, обеспечивающие интегрированную защиту информации и восстановление с конечной точностью выборок речевого сигнала, деформированных помехами в канале связи. Определены требования к качеству канала связи (к значению вероятности битовой ошибки в канале связи), при котором обеспечивается комфортное восприятие речи.

КЛЮЧЕВЫЕ СЛОВА: факториальный код, перестановка, таблица замен, выборка речевого сигнала, восстановление выборок, шум декодирования.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Gnatyuk S. Critical Aviation Information Systems Cybersecurity / S. Gnatyuk // Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. – 2016. – Vol. 47, № 3. – P. 308–316. DOI: 10.3233/978-1-61499-716-0-308
2. Secure Hash Function Constructing for Future Communication Systems and Networks / [S. Gnatyuk, V. Kinzeryavyy, K. Kyrychenko et al.] // Advances in Intelligent Systems and Computing. – 2019. – Vol. 902. – P. 561–569. DOI: 10.1007/978-3-030-12082-5_51
3. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Theory / R. J. McEliece // The Deep Space Network Progress Report, DSN PR 42–44. – 1978. – P. 114–116.
4. Осмоловский С. А. Стохастическая информатика: инновации в информационных системах / С. А. Осмоловский. – М. : Горячая линия-Телеком, 2012. – 321 с.
5. Stakhov A. P. Introduction into Fibonacci Coding and Cryptography / A. P. Stakhov, V. Massingue, A. Sluchenkova. – Kharkov : Osnova, 1999. – 234 p.
6. Stakhov A. P. Fibonacci Matrices, a Generalization of the ‘Cassini Formula’, and a New Coding Theory / A. P. Stakhov // Chaos, Solitons & Fractals. – 2006. – Vol. 30, № 1. – P.56–66. DOI: 10.1016/j.chaos.2005.12.054
7. Stakhov A. P. The ‘Golden’ Matrices and a New Kind of Cryptography / A. P. Stakhov // Chaos, Solitons & Fractals. – 2007. – Vol. 32, № 3. – P. 1138–1146. DOI: 10.1016/j.chaos.2006.03.069
8. Mazurkov M. I. Information security method based on perfect binary arrays / M. I. Mazurkov, V. Ya. Chechel’nitskii, P. Murr // Radioelectronics and Communications Systems. – 2008. – Vol. 51, № 11. – P. 612–614. DOI: 10.3103/S0735272708110095
9. Methods of improving information security by integrating multiplexing, ciphering and channel encoding operations / [M. I. Mazurkov, V. Ya. Chechelnytskyi, A. N. Meleshkevich et al.] // Radioelectronics and Communications Systems. – 2011. – Vol. 54, № 5. – P. 227–240. DOI: 10.3103/S0735272711050013
10. Mazurkov M. I. Composite matrix cipher based on perfect binary arrays / M. I. Mazurkov // Radioelectronics and

DOI 10.15588/1607-3274-2019-4-18

Communications Systems. – 2013. – Vol. 56, № 3. – P. 133–140. DOI: 10.3103/S0735272713030047
11. Перестановки в телекоммуникационных сетях / [А. А. Борисенко, А. Е. Горячев, Б. К. Лопатченко и др.] // Вісник Сумського державного університету. – 2013. – № 2. – С. 15–22.
12. Faure E. V. Information integrity control based on the factorial number system / E. V. Faure, V. V. Shvydkyi, A. I. Shcherba // Journal of Baku engineering university – Mathematics and computer science. – 2017. – Vol. 1, № 1. – P. 3–13.
13. Faure E. V. Combined factorial coding and its properties / E. V. Faure, V. V. Shvydkyi, V. O. Shcherba // Radio Electronics, Computer Science, Control. – 2016. – № 3. – P. 80–86. DOI: 10.15588/1607-3274-2016-3-10
14. Фауре Э. В. Факториальное кодирование с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – № 2. – С. 33–39. DOI: 10.24025/bulletinchstu.v1i2.82932
15. Faure E. V. Factorial coding with error correction / E. V. Faure // Radio Electronics, Computer Science, Control. – 2017. – № 3. – P. 130–138. DOI: 10.15588/1607-3274-2017-3-15
16. Faure E. V. Factorial Code with a Given Number of Inversions / E. V. Faure, A. I. Shcherba, A. A. Kharin // Radio Electronics, Computer Science, Control. – 2018. – № 2 – P. 143–153. DOI: 10.15588/1607-3274-2018-2-16
17. Marsaglia G. DIEHARD battery of tests of randomness [Electronic resource] / G. Marsaglia. – Access mode: http://www.stat.fsu.edu/pub/diehard.
18. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: Spec. Pub. 800-22 rev. 1a / [A. Rukhin, J. Soto, J. Nechvatal et al.] / National Institute of Standards and Technology. – Gaithersburg: MD, 2010. – 153 p.
19. L'ecuyer P. TestU01: A C Library for Empirical Testing of Random Number Generators / P. L'ecuyer, R. Simard // ACM Transactions on Mathematical Software. – 2007. – Vol. 33, № 4. – 40 p. DOI: 10.1145/1268776.1268777
20. Faure E. V. The Method and Criterion for Quality Assessment of Random Number Sequences / E. V. Faure, A. I. Shcherba, V. M. Rudnytskyi // Cybernetics and Systems Analysis. – 2016. – Vol. 52. – P. 277–284. DOI: 10.1007/s10559-016-9824-3
21. Hagelbarger D. W. Recurrent codes: Easily Mechanized, Burst-Correcting, Binary Codes / D. W. Hagelbarger // The Bell System Technical Journal. – 1959. – Vol. 38, Issue 4. – P. 969–984. DOI: 10.1002/j.1538-7305.1959.tb01584.x
22. Hagelbarger D. W. Error Detection Using Recurrent Codes / D. W. Hagelbarger // AIEE Winter General Meeting, New York, 31 January – 5 February 1960 : Proceedings. – New York, IEEE, 1960.
23. Pereira F. Classical and Quantum Convolutional Codes Derived from Algebraic Geometry Codes / F. Pereira, G. Guardia, F. Assis // IEEE Transactions on Communications. – 2019. – Vol. 67, № 1. – P. 73–82. DOI: 10.1109/TCOMM.2018.2875754
24. Yang Q. Asynchronous Convolutional-Coded Physical-Layer Network Coding / Q. Yang, C. Liew // IEEE Transactions on Wireless Communications. – 2015. – Vol. 14, № 3. – P. 1380–1395. DOI: 10.1109/TWC.2014.2365822
25. Nooraiepour A. Randomized Convolutional Codes for the Wiretap Channel / A. Nooraiepour, T. M. Duman // IEEE Transactions on Communications. – 2017. – Vol. 65, № 8. – P. 3442–3452. DOI: 10.1109/TCOMM.2017.2704586
26. Lavdanskyi A. O. Time assessment of formation of number sequences under increase of calculation unit performance / A. O. Lavdanskyi // The scientific potential of the present: International Scientific Conference, St Andrews, Scotland, United Kingdom, 1 December 2016 : proceedings. – St Andrews, Scotland, United Kingdom, 2016. – P. 123–126.
27. Rabiner L. R. Introduction to Digital Speech Processing / L. R. Rabiner, R. W. Schafer. – Delft: now Publishers Inc., 2007. – 200 p. DOI: 10.1561/2000000001
28. Wang L. Correlation Maximization-Based Sampling RateOffset Estimation for Distributed Microphone Arrays / L. Wang, S. Doclo // IEEE/ACM Transactions on Audio, Speech, and Language Processing. – 2016. – Vol. 24, № 3. – P. 571–582. DOI: 10.1109/TASLP.2016.2517326
29. Gilbert E. N. Capacity of a Burst-Noise Channel / E. N. Gilbert // Bell System Technical Journal. – 1960. – Vol. 39, Issue 5. – P. 1253–1265. DOI: 10.1002/j.1538-7305.1960.tb03959.x
30. Elliott E. O. Estimates of Error Rates for Codes on Burst-Noise Channels / E. O. Elliott // Bell System Technical Journal. – 1963. – Vol. 42, Issue 5. – P. 1977–1997. DOI: 10.1002/j.1538-7305.1963.tb00955.x
31. Hasslinger G. The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet / G. Hasslinger, O. Hohlfeld // Measurement, Modelling and Evalutation of Computer and Communication Systems: 14th GI/ITG Conference, Dortmund, Germany, 31 March – 2 April 2008 : proceedings. – VDE VERLAG, 2008.
32. Modeling of packet loss and delay and their effect on real-time multimedia service quality / [M. Ellis, D. P. Pezaros, T. Kypraios et al.] // Computer Networks. – 2014. – Vol. 70. – P. 384–399. DOI: 10.1016/j.comnet.2014.05.013
33. Heegard C. Turbo Coding / C. Heegard, S. B. Wicker. – Norwell: Kluwer Academic Publishers, 1999. – 476 p. DOI: 10.1007/978-1-4757-2999-3
34. 25 Years of Turbo Codes: From Mb/s to beyond 100 Gb/s / [S. Weithoffer, C.A. Nour, N. When et al.] // Turbo Codes and Iterative Information Processing: 10th IEEE International Symposium, Hong Kong, China, 3–7 December 2018 : proceedings. – IEEE Computer Society, 2018. DOI: 10.1109/ISTC.2018.8625377
35. Babar Z. Duality of quantum and classical error correction codes: Design principles and examples / [Z. Babar, D. Chandra, H. V. Nguyen et al.] // IEEE Communications Surveys and Tutorials. – 2019. – Vol. 21, Issue 1. – P. 970–1010. DOI: 10.1109/COMST.2018.2861361
36. Turbo Coded Modulation over GSM Channels / [D. P. Panayiotis, A. S. Thomas, V. Prabodh et al.] // Third Generation Wireless and Beyond: International Conference, San Francisco, California, 6–8 June 2001 : proceedings. – San Francisco, IEEE, 2001.

DOI 10.15588/1607-3274-2019-4-18