Software model for the synthesis of increased volumes of systems of discrete orthogonal code sequences

A V Studenikin¹, A P Zhuk¹
¹North-Caucasus Federal University, Stavropol, Pushkin str., 1, 355017, Russia

E-mail azhuk@ncfu.ru

Abstract. To ensure high structural secrecy of information transmission systems with MA and CDM, it is necessary to use many ensembles of stochastic discrete orthogonal code sequences differing from each other. The purpose of the article is to develop a program for studying the correlation and statistical characteristics of ensembles of stochastic discrete orthogonal sequences described by the eigenvectors of symmetric matrices, with random filling of the diagonal coefficients. Assessment of the statistical and correlation indicators of sequence ensembles obtained on the basis of the developed program showed their random nature.

Keywords: stochastic discrete orthogonal sequences; structural secrecy; code division multiplexing systems.

1. Introduction

In accordance with GOST 50922-2006 in the field of information security, which regulates information security issues, information security is understood as the state of information security, in which its confidentiality, availability and integrity are ensured.

In the modern world, radio channels are present everywhere, the prospects of their use are undeniable. The advantages and disadvantages of radio communication are also known. However, due to the specificity of the propagation of radio waves in space, one of the problems in transmitting information over radio channels is to ensure its confidentiality.

It is known that the confidentiality of message transmission over radio channels can be achieved by providing [1,2,3,10]:

- energy secrecy of signals - carriers of information.
- structural secrecy of these signals.
- information secrecy of the message itself.

A special place among wireless systems for information transmission is occupied by systems with multiple access (MA) and code division multiplexing (CDM). This is because they provide efficient use of the allocated frequency range, simultaneously providing information exchange in the interests of a large number of users [11-16]. These systems are subject to threats typical of wireless information transmission systems, therefore, they require additional information protection mechanisms, taking into account the group nature of the use of these systems. A comparative analysis of possible means of protecting information in networks with multiple access and code division of channels showed that it is advisable to use not all of the above criteria for the security of systems with MA and CDM, but only those that relate to the assessment of structural secrecy [7,9,10, 18].
It is possible to provide high structural secrecy of information transmission systems with MA and CDM on the basis of using a large number of different ensembles of stochastic discrete orthogonal code sequences, which are randomly replaced when used [8,18].

In this case, an important condition of the systems under consideration is that in addition to the statistical characteristics of the system of discrete orthogonal code sequences, they must also have correlation and spectral characteristics, taking into account the parameters of the communication channel in which they will be used [1-6].

In papers [8,17,18], approaches to the synthesis of discrete orthogonal code sequences are proposed, taking into account the requirements for their number and dimension, however, the issue of automating the procedure for assessing their statistical and correlation characteristics in them is not fully resolved.

The purpose of the article is to develop a program for studying the correlation and statistical characteristics of ensembles of stochastic discrete orthogonal sequences (ESDOS) described by the eigenvectors of symmetric matrices, with random filling of diagonal coefficients.

2. The solution of the problem

The criteria for assessing the structural secrecy of the ITS with CDM are:

1. Difficulty of solving the structure of sequence ensembles.
2. Sufficiency of the number of structures of ensembles of sequences for their automatic change and the presence of a single algorithmic basis for their formation.
3. The presence of "good" correlation characteristics of signal ensembles.

The analysis showed that the most rational option for increasing the structural secrecy of the ITS with MA and CDM is to use the vector synthesis method to obtain signal ensembles [10, 18]. Taking this into account, the developed software model is designed to study the correlation and statistical characteristics of the ESDOS described by the eigenvectors of symmetric matrices, with random filling of the diagonal coefficients.

The software model for the synthesis of increased volumes of systems of discrete orthogonal code sequences is based on the stochastic modeling algorithm ESDOS.

Let us consider the algorithm of stochastic modeling of ESDOS using the example of a bidiagonal symmetric matrix $A$ of the 4th order described by expression (1). It should be noted that the diagonal coefficients of the symmetric matrix $A$ of the form (1) have the following property $a_{ij} = a_{ji}$.

$$
A = \begin{bmatrix}
0 & a_{12} & 0 & 0 \\
a_{21} & 0 & a_{23} & 0 \\
0 & a_{32} & 0 & a_{34} \\
0 & 0 & a_{43} & 0
\end{bmatrix}
$$

At the first stage of the algorithm, a procedure for generating random numbers is implemented for the subsequent assignment of random values to the coefficients of the second diagonal of the bidiagonal symmetric matrix $A$, which is illustrated as follows. The random number generator at time $t_i$ performs the procedure for generating the $i$-th set of random numbers

$$
rnd_{i} \rightarrow \{..., \text{rnd}_{i1}, \text{rnd}_{i2}, \text{rnd}_{i3}, ...\}.
$$

At the second stage of the algorithm, the generated $i$-th set of random numbers is assigned to the coefficients of the second diagonal of the matrix $A$.

$$
rnd_{i1} \rightarrow a_{12}, \text{rnd}_{i2} \rightarrow a_{21}, \text{rnd}_{i3} \rightarrow a_{32}.
$$

At the third stage of the algorithm $i$-th set of eigenvectors of the matrix $A$ is calculated.
The set of eigenvectors of the form (4) of the matrix $A$ has the property of orthogonality and is the ESDO model.

At the fourth stage of the algorithm, the procedure for calculating the correlation and statistical characteristics of the obtained $i$-th ESDO model, such as the autocorrelation function $R_i(\tau)$, correlation dimension, correlation entropy and Hurst $H$ exponent, is implemented.

At the fifth stage of the algorithm, the ESDOS is selected, the correlation and statistical characteristics of which meet the specified requirements and criteria.

At the sixth stage of the algorithm, the display of the selected ESDOS and its correlation and statistical characteristics is realized.

At the seventh stage of the algorithm, the selected ESDOS and its correlation and statistical characteristics are recorded into the computer database.

Depending on the required limit value of the number of ESDOS $K$ structures required to use ensembles of stochastic discrete orthogonal code sequences differing from each other during a communication session, further repetition of the main stages of the algorithm described above is performed. The algorithm will be implemented until $K$ ensembles of stochastic discrete orthogonal sequences with given correlation and statistical characteristics are generated in the computer database. After that, from the database, at the user's request $K$ SDOS ensembles are issued for use in the information transmission system with MA and CDM.

In a generalized form, the main stages of the proposed algorithm can be presented as shown in Figure 1.

Analysis of Fig. 1 shows that the ESDOS stochastic modeling algorithm includes two main blocks:

Block 1. Development of a software complex for modeling ESDOS.

Block 2. Assessment of ESDOS properties using the Fractan program.

The first block includes the following stages:

1. Input of diagonal coefficients - loading from a file, or manual input of diagonal coefficients of a symmetric matrix.

2. Generation of a pseudo-random sequence - loading from a file or using one of the five proposed algorithms for generating pseudo-random numbers to obtain the sign structure of the coefficients of the symmetric matrix.

3. Calculation of an ensemble of stochastic discrete orthogonal sequences.

4. Conversion of calculations of ensembles of discrete orthogonal sequences for subsequent analysis in the Fractan program.

The second block includes:

1. Calculation of the correlation dimension, which is used to check for the presence of a chaotic component in a time series.

2. Calculation of the correlation entropy, which shows the degree of divergence of close phase trajectories and allows you to estimate the amount of information required to predict the behavior of the time series in the future.

3. Calculation of the Hurst exponent used in the analysis of time series. This amount decreases when the delay between two identical pairs of values in the time series increases.

4. Building a graph of ensembles of stochastic discrete orthogonal sequences and displaying a graphical implementation.
Let us describe the program interface, the procedure for entering initial data and presenting the calculation results.

The interface of the main menu of the program is shown in Figure 2.

![Figure 2. The main menu of the software model for the synthesis of increased volumes of ESDOS](image)

With the help of this menu, in the first window, the dimension of the matrix $A$ of the form (1) and, accordingly, the dimension of the ESDOS basis are set. In the second window, a pseudo-random number generator (PRNG) is selected and its parameter is set - the number of samples. The third window is intended for starting calculations by manually or randomly setting the coefficients of the matrix $A$ and converting the data.

When entering the initial data in one of the selected ways, the entered data is displayed in a special program window as shown in Figure 3.

![Figure 3. The main window of the program](image)
After specifying the initial data, the software model for the synthesis of systems of discrete orthogonal code sequences of increased volumes carries out the statistical and correlation indicators of the model of the ensemble of sequences and displays the results of the calculations.

Figure 4 illustrates the results of calculating the correlation dimension of the obtained sequence model.

Figure 5 illustrates the results of calculating the correlation entropy of the obtained sequence model.

Figure 6 illustrates the results of calculating the Hurst exponent of the resulting sequence model.

For the initial random sequence of numbers, which served to generate symmetric matrices, using the developed program, the following indicators were calculated:
- Correlation dimension $D = 8.02$.
- Correlation entropy $K = 0.69$.
- Hurst exponent $H = 0.53$.

Based on the initial random sequence, ESDOS was simulated and the main indicators were calculated:
- Correlation dimension $D = 4.70$.
- Correlation entropy $K = 2.56$.
- Hurst exponent $H = 0.21$. 
The data obtained indicate the random nature of the representation of the eigenvectors of symmetric matrices obtained on the basis of the initial random sequence of numbers.

This conclusion is encouraging, however, for a detailed assessment of the statistical and correlation indicators of sequence ensembles obtained on the basis of the developed program, additional research is needed.

Conclusions:

1. To solve the problem of developing a software model for the synthesis of increased volumes of systems of discrete orthogonal code sequences, the known numerical methods for calculating the eigenvectors of symmetric matrices were investigated and the most acceptable of them was chosen.

2. Created an algorithm for modeling ensembles of stochastic discrete orthogonal signals of increased volumes.

3. A software model for the synthesis of increased volumes of systems of discrete orthogonal code sequences has been developed, which allows calculating the statistical and correlation indicators of sequence ensembles and displaying the calculation results.

4. The results of a preliminary assessment of the statistical and correlation indicators of sequence ensembles obtained on the basis of the developed program showed the random nature of the sequences obtained, and further research is needed for a more accurate assessment of these indicators.

3. Conclusion

It is possible to provide high structural secrecy of information transmission systems with MA and CDM based on the use of a large number of different ensembles of stochastic discrete orthogonal code sequences, which are randomly replaced when used.

In this article, a program has been developed for studying the correlation and statistical characteristics of the ESDOS described by the eigenvectors of symmetric matrices, with random filling of the diagonal coefficients.

A preliminary assessment of the statistical and correlation indicators of sequence ensembles obtained on the basis of the developed program showed their random nature.

4. Acknowledgment

The reported study was funded by Russian Ministry of Science (information security), project number 29/2020.

References

[1] Viterbi A J 1995 CDMA: Principles of spread spectrum communication (Reading, MA: Addison-Wesley)

[2] Proakis J 2001 Digital Communications (N. Y.: McGraw-Hill)

[3] Sklar B. 1988 Digital Communications. Fundamentals and Applications (Upper Saddle River NJ, Prentice-Hall)

[4] Varakin L E 1978 Complex signals theory (Moscow, Soviet radio)

[5] Petrovich N T, Razmahin M K 1969 Telecommunication systems with noise-like signals (Moscow, Soviet radio)

[6] Golomb S W, Gong G 2005 Signal design for good correlation for wireless communication, cryptography, and radar (Cambridge: University Press)

[7] Dyatlov A P, Dyatlov P A, Kulbikayan B H 2004 Electronic warfare with satellite radio navigation systems (Moscow, Radio and communications)

[8] Orel D V 2013 Modeling of stochastic systems of binary quasi-orthogonal code sequences based on the method of functional transformations (Ph.D. thesis on 05.13.18 Mathematical modeling, numerical methods and software packages. Stavropol, North Caucasus Federal University)

[9] Pashintsev V P, Kalmykov I A, Zhuk A P, Orel D V, Zhuk E P 2018 Formation Algorithms and Properties of Binary Quasi-Orthogonal Code Sequence of Modern Satellite Systems International Journal of Engineering & Technology vol 7 (4.38) pp 1205-1209 DOI: 10.1117/12.2324249
[10] Zhuk A P, Ivanov A S 2011 Increasing the structural secrecy of the information transmission system with code separation of channels *High-tech technologies in Earth space research* No1 pp 26-28

[11] Golomb S 1964 *Digital communications with space applications* (Upper Saddle River NJ, Prentice-Hall)

[12] Golomb S 1967 *Shift Register Sequences* (San Francisco: Holden-Day)

[13] Ziemer R. E., Peterson R. L., Borth D. E. Introduction to spread spectrum communications. – Englewood Cliffs, NJ: Prentice Hall, 1995. – 695 p.

[14] Nunn C J, Coxson G E 2009 *Polyphase pulse compression codes with optimal peak and integrated sidelobes* IEEE Transactions on Aerospace and Electronic Systems Vol. AES-45, No 2. pp 775-781

[15] Rushanan J 2006 *Weil sequences: a family of binary sequences with good correlation properties* (Seattle convention center. Seattle)