DOI 10.15276/imms.v11.no3.147
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 3, pp. 147-161

MULTIPLE ACCESS STEGANOGRAPHIC METHOD BASED ON CODE CONTROL AND FREQUENCY ARRANGEMENTS

A.V. Sokolov

National Odessa Polytechnic University
Ukraine, Odessa, 65044, Shevchenko Ave., 1, e-mail: radiosquid@gmail.com

The development, as well as the wider practical application of modern steganography, leads to the need to create steganographic methods with multiple access, which would be able to ensure the simultaneous transmission and division of information from several users in a steganographic channel. The currently known multiple-access steganographic methods are based on MC-CDMA technology and do not show how exactly the embedding and extraction of additional information should be performed. The purpose of this paper is to develop a multiple-access steganographic method based on code control and frequency arrangements. This purpose was achieved through the development of a steganographic method with code control and the use of frequency arrangements based on double-cyclic Reed-Solomon codes over Galois fields GF(q), which provides separate embedding of information by each user at any time which is convenient for him using a personal frequency arrangement. It was proposed to construct the frequency arrangements on the basis of Reed-Solomon codes over the Galois fields GF(5) and GF(13). The characteristics of the developed method are researched, within which it is shown that the PSNR of the resulting steganographic message depends on the number of users simultaneously transmitting information through the steganographic channel. With the number of simultaneously operating users N≤8, the PSNR values remain at an acceptable level. During the operation of the proposed steganographic method, the occurrence of intra-system interference in the steganographic channel was detected with the number of users simultaneously transmitting information N>q, however, when using frequency arrangements based on the Reed-Solomon code over the GF(13), their effect is insignificant with a practically justified number of divided channels. The developed steganographic method is a rational solution if it is necessary to organize a steganographic channel with multiple access and can provide flexible resource allocation: the operation of the required number of users with a given bandwidth and the required perception reliability.

Keywords: steganography, code control, multiple access, code division, frequency arrangement.

Introduction and statement of the problem

Steganography is one of the most important components of modern information security systems [1], which not only makes it impossible to read information without the presence of a secret key, but also allows to hide the very fact of secret information transference. The rapid development of the theory and practice of steganography, which is currently taking place, has led to the emergence of many effective steganographic methods with a high level of performance [2], resistance to common attacks (lossy compression, noise, blurring, scaling, etc.) [3...6], as well as providing a high level of reliability of steganographic message perception [7]. A property of these methods is the ability to transmit additional information in a steganographic message, intended for one specific user.

Nevertheless, in order to solve some practical tasks [8, 9], it becomes necessary to transmit in one steganographic message information intended for more than one user, i.e. organize in the steganographic channel a multiple access. One of the effective methods for solving this problem is the use of MC-CDMA technology using the Walsh-Hadamard transform, which was proposed in [8], and was further developed in [10]. The disadvantages of this technology include the fact that the number of users is strictly regulated and equal to $N = 2^k = 2,4,8,16,...$. MC-CDMA technology does not show exactly how the embedding and extraction of additional information should be performed, which is another significant disadvantage of the mentioned method of code division of channels.

As it is shown in this paper, the mentioned disadvantages of using MC-CDMA technology in steganographic methods can be eliminated by combining the advantages of the steganographic method with code control, as well as the frequency arrangement technology used to build asynchronous address communication systems based on time-frequency matrices (TFM signals) [11]. Such signals are used in terrestrial, satellite and other communication systems, in command radio control systems as well as in the air traffic control systems.

The purpose of this paper is to develop a multiple-access steganographic method based on code control and frequency arrangements.

Definitions and constructions

The proposed in this paper method uses the relationship established in [3] between the two-dimensional and one-dimensional Walsh-Hadamard transforms: up to a coefficient $1/N$, the two-dimensional Walsh-Hadamard transform $W = H'XH'^T$ can be represented in terms of the one-dimensional Walsh-Hadamard transform using the following relation $\tilde{W} = \tilde{X}H_{N_2}$, where H_N is the Walsh-Hadamard matrix of order $N = 2^k$, which is constructed according to Sylvester's construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix},\ H_1 = 1, \tag{1}$$

while $H'_N = \frac{1}{\sqrt{N}} H_N$, and operator $\tilde{A}$ denotes writing the matrix A of order $N \times N$ as a row vector of length N^2 by sequential rows concatenation.

As the basis of the developed steganographic method with multiple access, it is proposed to use the steganographic method with the code control [3], the main idea of which is to use the linearity property of the Walsh-Hadamard transform

$$\begin{gathered} \tilde{M} = \tilde{X} + \tilde{D}; \\ \tilde{M}H_{N^2} = \tilde{X}H_{N^2} + \tilde{D}H_{N^2}, \end{gathered} \tag{2}$$

where X is a block of a matrix-container of size $\mu \times \mu$, D is a block of additional information of size $\mu \times \mu$, M is a block of a steganographic message of size $\mu \times \mu$. In this paper we consider the block size $\mu \times \mu = 8 \times 8$.

Using additional coding of the matrix D with codes having a given form of Walsh-Hadamard transform coefficients, it is possible to embed the additional information into a given Walsh-Hadamard transform coefficient of the container image X. Thus, by modifying the codewords that represent the bits of the steganographic message, it is possible to manipulate the properties of the steganographic method: the embedding of information into medium or low frequencies makes it possible to achieve resistance to attacks by compression, noise, and blurring, while the embedding of information into higher frequency components allows a higher probability to guarantee the reliability of the steganographic message perception.

In [3], an explicit correspondence was established between the transformants of the Walsh-Hadamard transform, as well as transformants of the discrete cosine transform (DCT), which has the following form for the case of the size of transformations $\frac{\mu}{2}\times\frac{\mu}{2}=4\times 4$

$$\begin{array}{ccc|ccc}
\text{DCT} & & \begin{array}{c}\text{Walsh-Hadamard}\\ \text{Transform}\end{array} & \text{DCT} & & \begin{array}{c}\text{Walsh-Hadamard}\\ \text{Transform}\end{array} \\
(1,1) & \leftrightarrow & (1,1) & (3,1) & \leftrightarrow & (4,1) \\
(1,2) & \leftrightarrow & (1,3) & (3,2) & \leftrightarrow & (4,2) \\
(1,3) & \leftrightarrow & (1,4) & (3,3) & \leftrightarrow & (4,4) \\
(1,4) & \leftrightarrow & (1,2) & (3,4) & \leftrightarrow & (4,2) \\
(2,1) & \leftrightarrow & (3,1) & (4,1) & \leftrightarrow & (2,1) \\
(2,2) & \leftrightarrow & (3,3) & (4,2) & \leftrightarrow & (2,3) \\
(2,3) & \leftrightarrow & (3,4) & (4,3) & \leftrightarrow & (2,4) \\
(2,4) & \leftrightarrow & (3,2) & (4,4) & \leftrightarrow & (2,2)
\end{array}. \quad (3)$$

For example, to ensure the reliability of perception, the embedding of information must be done so that just the most high-frequency Walsh-Hadamard transformants undergo modifications.

In Table 1, we present the codewords used in the steganographic method developed in this paper, which affect the transformants (1,2); (1,4); (2,1); (2,2); (2,3); (2,4); (3,2); (3,3); (3,4); (4,1); (4,2); (4,3); (4,4) (excluding the lowest-frequency transformants (1,1); (1,3); (3,1)).

Table 1

Codewords aimed at modifying the given Walsh-Hadamard transformant

$T^{+}_{4,(1,2)}$	$T^{+}_{4,(1,4)}$	$T^{+}_{4,(2,1)}$	$T^{+}_{4,(2,2)}$
$\begin{bmatrix}1&-1&1&-1\\1&-1&1&-1\\1&-1&1&-1\\1&-1&1&-1\end{bmatrix}$	$\begin{bmatrix}1&-1&-1&1\\1&-1&-1&1\\1&-1&-1&1\\1&-1&-1&1\end{bmatrix}$	$\begin{bmatrix}1&1&1&1\\-1&-1&-1&-1\\1&1&1&1\\-1&-1&-1&-1\end{bmatrix}$	$\begin{bmatrix}1&-1&1&-1\\-1&1&-1&1\\1&-1&1&-1\\-1&1&-1&1\end{bmatrix}$
$T^{+}_{4,(2,3)}$	$T^{+}_{4,(2,4)}$	$T^{+}_{4,(3,2)}$	$T^{+}_{4,(3,3)}$
$\begin{bmatrix}1&1&-1&-1\\-1&-1&1&1\\1&1&-1&-1\\-1&-1&1&1\end{bmatrix}$	$\begin{bmatrix}1&-1&-1&1\\-1&1&1&-1\\1&-1&-1&1\\-1&1&1&-1\end{bmatrix}$	$\begin{bmatrix}1&-1&1&-1\\1&-1&1&-1\\-1&1&-1&1\\-1&1&-1&1\end{bmatrix}$	$\begin{bmatrix}1&1&-1&-1\\1&1&-1&-1\\-1&-1&1&1\\-1&-1&1&1\end{bmatrix}$
$T^{+}_{4,(3,4)}$	$T^{+}_{4,(4,1)}$	$T^{+}_{4,(4,2)}$	$T^{+}_{4,(4,3)}$
$\begin{bmatrix}1&-1&-1&1\\1&-1&-1&1\\-1&1&1&-1\\-1&1&1&-1\end{bmatrix}$	$\begin{bmatrix}1&1&1&1\\-1&-1&-1&-1\\-1&-1&-1&-1\\1&1&1&1\end{bmatrix}$	$\begin{bmatrix}1&-1&1&-1\\-1&1&-1&1\\-1&1&-1&1\\1&-1&1&-1\end{bmatrix}$	$\begin{bmatrix}1&1&-1&-1\\-1&-1&1&1\\-1&-1&1&1\\1&1&-1&-1\end{bmatrix}$
$T^{+}_{4,(4,4)}$	—	—	—
$\begin{bmatrix}1&-1&-1&1\\-1&1&1&-1\\-1&1&1&-1\\1&-1&-1&1\end{bmatrix}$	—	—	—

Such a number of selected frequency components is chosen because of the fact that in this paper we consider the use of two frequency arrangement codes: the first code assumes the largest number of users operating in the system, using 13 frequency components, while the second code uses five frequency components and provides the best reliability of perception.

Note that the application of the codewords presented in Table 1 in accordance with (2) causes a targeted effect on the corresponding Walsh-Hadamard transformant, while the remaining transformants of the steganographic message remain unchanged.

Each codeword shown in Table 1 is the frequency component for the first frequency arrangement code f_{1i} and the second f_{2i}, respectively

$$\begin{array}{ccc} T^{+}_{4,(1,2)} & \leftrightarrow & f_{10} \\ T^{+}_{4,(1,4)} & \leftrightarrow & f_{11} \\ T^{+}_{4,(2,1)} & \leftrightarrow & f_{12} \\ T^{+}_{4,(2,2)} & \leftrightarrow & f_{13} \\ T^{+}_{4,(2,3)} & \leftrightarrow & f_{14} \\ T^{+}_{4,(2,4)} & \leftrightarrow & f_{15} \\ T^{+}_{4,(3,2)} & \leftrightarrow & f_{16} \\ T^{+}_{4,(3,3)} & \leftrightarrow & f_{17} \\ T^{+}_{4,(3,4)} & \leftrightarrow & f_{18} \\ T^{+}_{4,(4,1)} & \leftrightarrow & f_{19} \\ T^{+}_{4,(4,2)} & \leftrightarrow & f_{110} \\ T^{+}_{4,(4,3)} & \leftrightarrow & f_{111} \\ T^{+}_{4,(4,4)} & \leftrightarrow & f_{112} \end{array}, \quad \begin{array}{ccc} T_{4,(2,2)} & \leftrightarrow & f_{20} \\ T_{4,(2,3)} & \leftrightarrow & f_{21} \\ T_{4,(2,4)} & \leftrightarrow & f_{22} \\ T_{4,(3,2)} & \leftrightarrow & f_{23} \\ T_{4,(4,2)} & \leftrightarrow & f_{24} \end{array}. \tag{4}$$

These frequency components f_i of the size $\frac{\mu}{2} \times \frac{\mu}{2} = 4 \times 4$ are used in the developed method as elements to form codewords of size $\mu \times \mu$, which is unique for each user in accordance with the frequency arrangement rule

$$\begin{array}{|c|c|} \hline f_{i_1} & f_{i_2} \\ \hline f_{i_3} & f_{i_4} \\ \hline \end{array}, \tag{5}$$

where the vector of indices $[i_1, i_2, i_3, i_4]$ is unique for each user and is determined by the corresponding frequency arrangement.

In modern asynchronous address communication systems for constructing frequency arrangement codes with good correlation properties, non-binary cyclic Bose–Chaudhuri–Hocquenghem codes also known as Reed-Solomon codes (RS-codes) [11] have become widespread.

In this paper, considering an example of the block length $\mu \times \mu = 8 \times 8$, we present two options for generating the frequency arrangement code: the first one is constructed over the Galois field $GF(13)$, which allows you to ensure the maximum number of users operating in the system while maintaining acceptable perception reliability, and the second one is constructed over the Galois field $GF(5)$, which allows you to provide the best reliability of perception with a smaller number of users operating in the system.

Let's form the first frequency arrangement code based on the RS-code over the Galois field $GF(13)$ with the following parameters: codeword length $N=12$, number of information digits $K=2$, primitive element $\theta=2$, code distance $d=12-2+1=11$. The generating polynomial of a given code is determined by the following relationship

$$\begin{gathered} g(z)=\prod_{i=1}^{d-1}(z-\theta^i)=\prod_{i=1}^{10}(z-2^i)= \\ (z-2)(z-4)(z-8)(z-3)(z-6)(z-12)(z-11)(z-9)(z-5)(z-10)= \\ 11+7z+12z^2+9z^3+3z^4+4z^5+6z^6+10z^7+5z^8+8z^9+z^{10}. \end{gathered} \tag{6}$$

On the basis of the generating polynomial (6), we construct a generating matrix, the first row of which consists of the coefficients of the generating polynomial, the remaining $K-1$ rows are defined as a non-cyclic shift to the right by 1 of the previous row, while all unfilled elements of the generating matrix are considered as equal to 0

$$G=\begin{bmatrix} 11 & 7 & 12 & 9 & 3 & 4 & 6 & 10 & 5 & 8 & 1 & 0 \\ 0 & 11 & 7 & 12 & 9 & 3 & 4 & 6 & 10 & 5 & 8 & 1 \end{bmatrix}. \tag{7}$$

The first row in the generating matrix G will be called as the basic codeword and will be denoted as C_1. Based on the property of double cyclicity of RS-codes, we can construct all other codewords by cyclic shifts of the basic codeword in time and frequency. Further, each of the codewords of the RS-code is truncated, as a result of which we obtain its first four symbols that we will use as the frequency arrangement.

In this case, the total number of available frequency arrangements generated using the RS-code over the Galois field $GF(q)$ is

$$J=q(q-1)=13\cdot 12=156\,. \tag{8}$$

For brevity in Table 2 these frequency arrangements are presented with the radix equal to 13 ($10\to A, 11\to B, 12\to C$).

Thus, using the method of additional coding of information with codewords (5) using frequency arrangements based on the RS-code, presented in Table 2 it is theoretically possible to provide the operation of 156 users in the steganographic channel.

For example, in this case, the first user in the system will transmit information using a frequency arrangement $[\mathrm{B7C9}]\to[11 \quad 7 \quad 12 \quad 9]$, on the basis of which, in accordance with (4), we form codewords of the form (5) $[f_{111} \quad f_{17} \quad f_{112} \quad f_{19}]=[T^{+}_{4,(4,3)}, \quad T^{+}_{4,(3,3)}; \quad T^{+}_{4,(4,4)}, \quad T^{+}_{4,(4,1)}]$, where the symbol “,” means horizontal concatenation, and the symbol “;” means vertical concatenation.

Thus, the first user in the system encodes information using the following codewords (T_1^+ for transmitting bit “0” and T_1^- for transmitting bit “1”)

Table 2

Representation of the frequency arrangement code based on the RS-code over the Galois field $GF(13)$ in the form of cyclic shifts in time and frequency of the basic codeword C_1

B7C9	7C93	C934	9346	346A	46A5	6A58	A581	5810	810B	10B7	0B7C
C80A	80A4	0A45	A457	457B	57B6	7B69	B692	6921	921C	21C8	1C80
091B	91B5	1B56	B568	568C	68C7	8C7A	C7A3	7A32	A320	3209	2091
1A2C	A2C6	2C67	C679	6790	7908	908B	08B4	8B43	B431	431A	31A2
2B30	B307	3078	078A	78A1	8A19	A19C	19C5	9C54	C542	542B	42B3
3C41	C418	4189	189B	89B2	9B2A	B2A0	2A06	A065	0653	653C	53C4
4052	0529	529A	29AC	9AC3	AC3B	C3B1	3B17	B176	1764	7640	6405
5163	163A	63AB	3AB0	AB04	B04C	04C2	4C28	C287	2875	8751	7516
6274	274B	74BC	4BC1	BC15	C150	1503	5039	0398	3986	9862	8627
7385	385C	85C0	5C02	C026	0261	2614	614A	14A9	4A97	A973	9738
8496	4960	9601	6013	0137	1372	3725	725B	25BA	5BA8	BA84	A849
95A7	5A71	A712	7124	1248	2483	4836	836C	36CB	6CB9	CB95	B95A
A6B8	6B82	B823	8235	2359	3594	5947	9470	470C	70CA	0CA6	CA6B

$$T_1^+ = \left[\begin{array}{cccc|cccc} 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \end{array}\right], \quad T_1^- = \left[\begin{array}{cccc|cccc} -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ \hline -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \end{array}\right]. \tag{9}$$

Let us now proceed to the construction of the second frequency arrangement code, for which we construct a RS-code over the Galois field $GF(5)$ with the following parameters: codeword length $N=4$, number of information digits $K=2$, primitive element $\theta=3$, code distance $d=N-K+1=3$. We define the generating polynomial of the given code

$$\begin{aligned} g(z) &= \prod_{i=1}^{d-1}(z-\theta^i) = \prod_{i=1}^{2}(z-3^i) = \\ &= (z-3)(z-4) = 2+3z+z^2. \end{aligned} \tag{10}$$

Similarly, to the case of the first frequency arrangement code, based on the generating polynomial (10), we construct the generating matrix

$$G = \begin{bmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{bmatrix}, \tag{11}$$

on the basis of which we construct all the $J = 20$ codewords of the Reed-Solomon code (Table 3). Since each of these codewords has a length $N = 4$ that corresponds to construction (5), for this code the codewords do not need to be truncated and can be used unchanged.

Table 3

Representation of the RS-code over the Galois field $GF(5)$

$C_1 = [2\ \ 3\ \ 1\ \ 0]$	$C_6 = [3\ \ 1\ \ 0\ \ 2]$	$C_{11} = [1\ \ 0\ \ 2\ \ 3]$	$C_{16} = [0\ \ 2\ \ 3\ \ 1]$
$C_2 = [3\ \ 4\ \ 2\ \ 1]$	$C_7 = [4\ \ 2\ \ 1\ \ 3]$	$C_{12} = [2\ \ 1\ \ 3\ \ 4]$	$C_{17} = [1\ \ 3\ \ 4\ \ 2]$
$C_3 = [4\ \ 0\ \ 3\ \ 2]$	$C_8 = [0\ \ 3\ \ 2\ \ 4]$	$C_{13} = [3\ \ 2\ \ 4\ \ 0]$	$C_{18} = [2\ \ 4\ \ 0\ \ 3]$
$C_4 = [0\ \ 1\ \ 4\ \ 3]$	$C_9 = [1\ \ 4\ \ 3\ \ 0]$	$C_{14} = [4\ \ 3\ \ 0\ \ 1]$	$C_{19} = [3\ \ 0\ \ 1\ \ 4]$
$C_5 = [1\ \ 2\ \ 0\ \ 4]$	$C_{10} = [2\ \ 0\ \ 4\ \ 1]$	$C_{15} = [0\ \ 4\ \ 1\ \ 2]$	$C_{20} = [4\ \ 1\ \ 2\ \ 0]$

A steganographic system with multiple access based on the presented Reed-Solomon code (Table 3) can theoretically ensure the operation of $J = 20$ users with help of five frequency components.

Algorithms for embedding and extraction of information

Based on the theoretical material presented, we will describe algorithms for embedding and extraction of information for the developed steganographic method with multiple access.

Information embedding algorithm

Step 1. An ensemble of codewords of size $\frac{\mu}{2} \times \frac{\mu}{2}$ is formed (Table 1), which are acting purposefully on the given transformants of the Walsh-Hadamard transform, as well as an ensemble of frequency arrangements based on the RS-code over the Galois field $GF(q)$ (Table 2 or Table 3). The choice of the base q depends on the number of users operating in the system, as well as on the number of modified Walsh-Hadamard transformants participating in the transmission of information.

Step 2. To each user A_z, $z = 1, 2, ..., J$ registered in the steganographic system, a frequency arrangement is allocated for transmitting information over the steganographic channel. On the basis of given frequency arrangement, in accordance with construction (5) and Table 1, the user generates codewords T_z^+ and T_z^- of size $\mu \times \mu$.

Step 3. Each of the users A_z splits the container image into blocks of size $\mu \times \mu$ and embeds one bit $d_{z,k}$ of the additional information into each of the container blocks X_k by applying the summation operation, i.e. each block of a steganographic message is calculated as

$$M_k = X_k + D_k . \qquad (12)$$

The undoubted advantage of the developed steganographic method is the fact that different users, using their frequency arrangements, can embed information independently of each other at any time convenient for them. The number of subscribers simultaneously operating in the system can also be easily scaled.

Let's consider a specific example of information embedding using the developed steganographic method.

Let an ensemble of codewords of size 4×4 to be formed, which consists of codewords $T_{4,(2,2)}, T_{4,(2,3)}, T_{4,(2,4)}, T_{4,(3,2)}, T_{4,(4,2)}$, as well as an ensemble of frequency arrangements (Table 2). Consider the operation of two users A_1 and A_2 with the following frequency arrangements: $C_1 = \begin{bmatrix} 2 & 3 & 1 & 0 \end{bmatrix}$ and $C_2 = \begin{bmatrix} 3 & 4 & 2 & 1 \end{bmatrix}$. Let these users perform embedding of information bits $d_{1,k} = 1, d_{2,k} = -1$ into the block of the container image

$$X_k = \begin{bmatrix} 213 & 214 & 215 & 216 & 215 & 214 & 214 & 214 \\ 214 & 215 & 215 & 216 & 215 & 214 & 216 & 214 \\ 214 & 214 & 215 & 215 & 214 & 213 & 214 & 214 \\ 215 & 215 & 216 & 217 & 214 & 214 & 214 & 214 \\ 214 & 214 & 215 & 215 & 214 & 217 & 216 & 216 \\ 214 & 214 & 215 & 215 & 216 & 216 & 214 & 216 \\ 215 & 216 & 215 & 216 & 215 & 215 & 214 & 216 \\ 214 & 216 & 215 & 214 & 215 & 215 & 216 & 215 \end{bmatrix}. \tag{13}$$

On the basis of a given frequency arrangement C_1, as well as an ensemble of codewords of size 4×4, the first user generates codewords of size 8×8 intended for transmitting an additional information bit $d_{1,k}$

$$T_1^+ = \left[\begin{array}{rrrr|rrrr} 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{array}\right], \quad T_1^- = \left[\begin{array}{rrrr|rrrr} -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \end{array}\right], \tag{14}$$

while the second user generates his codewords based on the frequency arrangement C_2

$$T_2^+ = \left[\begin{array}{rrrr|rrrr} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ \hline 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \end{array}\right], \quad T_2^- = \left[\begin{array}{rrrr|rrrr} -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \hline -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \end{array}\right]. \tag{15}$$

Based on (12), the first user embeds a bit of information $d_{1,k} = 1$, while the second user embeds a bit of information $d_{2,k} = -1$, as a result of which we get a steganographic message

$$M_k = X_k + T_1^+ + T_2^- = \begin{bmatrix} 213 & 214 & 213 & 218 & 215 & 214 & 214 & 214 \\ 212 & 217 & 215 & 216 & 217 & 212 & 218 & 212 \\ 216 & 212 & 215 & 215 & 214 & 213 & 214 & 214 \\ 215 & 215 & 218 & 215 & 212 & 216 & 212 & 216 \\ 214 & 216 & 215 & 213 & 214 & 215 & 218 & 216 \\ 214 & 212 & 215 & 217 & 216 & 218 & 212 & 216 \\ 215 & 218 & 215 & 214 & 215 & 213 & 216 & 216 \\ 214 & 214 & 215 & 216 & 215 & 217 & 214 & 215 \end{bmatrix}. \tag{16}$$

We note here that the degree of perturbation of the container image when embedding information by the developed method depends on the following factors: the number of users simultaneously transmitting the additional information, and specific values of the additional information bits.

Remark. In view of the fact that most of the images used today are represented using the RGB model, where 1 byte is allocated for encoding of each color (each color component is represented by numbers in the range $[0,...,255]$), in the case of the presence in the block of boundary values for this range (0 or 255), the mentioned block is not used in the process of steganographic transformation.

Let's move on to the information extraction algorithm.

<u>Information Extraction Algorithm</u>

Step 1. In accordance with the relationship between the two-dimensional and one-dimensional Walsh-Hadamard transforms, each user A_z of the steganographic system, in accordance with the frequency arrangement code issued to him, selects the rows of the Walsh-Hadamard matrix H_{N^2} of the order N^2, which are denoted as $\{h_{z,1}\},\{h_{z,2}\},\{h_{z,3}\},\{h_{z,4}\}$.

Step 2. The user finds the difference matrix of the steganographic message M and the container image X, splits the resulting difference matrix into blocks Δ_k of size $\mu \times \mu$.

Step 3. The user divides each of the blocks of the difference matrix Δ_k into 4 sub-blocks of size $\frac{\mu}{2} \times \frac{\mu}{2}$, in accordance with the construction (5). By sequentially concatenating the rows, each of the resulting four subblocks is represented as a vector $\{\delta_{z,i}\}, i = \{1,2,3,4\}$ of length μ^2.

Step 4. The user A_z calculates the vector P in accordance with the following formula

$$\begin{gathered} P_{z,k} = [p_1 \quad p_2 \quad p_3 \quad p_4], \\ p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k}, i = \{1,2,3,4\}. \end{gathered} \tag{17}$$

Step 5. The user calculates the intended data bit embedded in the block Δ_k using the following formula

$$d_{z,k} = sign\left(\sum_{i=1}^{4} p_i \right). \tag{18}$$

As an example, let us extract the information embedded by the first and second users in the steganographic message (16). To do this, in accordance with the selected frequency arrangement codes, we form a set of Walsh functions for the first user

$$\begin{aligned}
\{h_{1,1}\} &= \{+1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\};\\
\{h_{1,2}\} &= \{+1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\};\\
\{h_{1,3}\} &= \{+1\ \ +1\ \ -1\ \ -1\ \ -1\ \ -1\ \ +1\ \ +1\ \ +1\ \ +1\ \ -1\ \ -1\ \ -1\ \ -1\ \ +1\ \ +1\};\\
\{h_{1,4}\} &= \{+1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\},
\end{aligned} \tag{19}$$

and also, for the second user

$$\begin{aligned}
\{h_{2,1}\} &= \{+1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\};\\
\{h_{2,2}\} &= \{+1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\ \ +1\ \ -1\};\\
\{h_{2,3}\} &= \{+1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\ \ +1\ \ -1\ \ -1\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\};\\
\{h_{2,4}\} &= \{+1\ \ +1\ \ -1\ \ -1\ \ -1\ \ -1\ \ +1\ \ +1\ \ +1\ \ +1\ \ -1\ \ -1\ \ -1\ \ -1\ \ +1\ \ +1\}.
\end{aligned} \tag{20}$$

Further, both users calculate the matrix of the difference between the steganographic message and the container image, and divide it into blocks of size $\mu \times \mu$. In the case of our example, the considered block will have the form

$$\Delta_k = M_k - X_k = \begin{bmatrix} 0 & 0 & -2 & 2 & 0 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 & 2 & -2 & 2 & -2 \\ 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & -2 & 2 & -2 & 2 \\ 0 & 2 & 0 & -2 & 0 & -2 & 2 & 0 \\ 0 & -2 & 0 & 2 & 0 & 2 & -2 & 0 \\ 0 & 2 & 0 & -2 & 0 & -2 & 2 & 0 \\ 0 & -2 & 0 & 2 & 0 & 2 & -2 & 0 \end{bmatrix}. \tag{21}$$

Based on the obtained matrix Δ_k, the first and second users select the corresponding vectors $\{\delta_{z,i}\}, i = \{1,2,3,4\}$

$$\begin{aligned}
\{\delta_{1,1}\} &= \begin{bmatrix}0 & 0 & -2 & 2 & -2 & 2 & 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 & 2 & -2\end{bmatrix};\\
\{\delta_{1,2}\} &= \begin{bmatrix}0 & 0 & 0 & 0 & 2 & -2 & 2 & -2 & 0 & 0 & 0 & 0 & -2 & 2 & -2 & 2\end{bmatrix};\\
\{\delta_{1,3}\} &= \begin{bmatrix}0 & 2 & 0 & -2 & 0 & -2 & 0 & 2 & 0 & 2 & 0 & -2 & 0 & -2 & 0 & 2\end{bmatrix};\\
\{\delta_{1,4}\} &= \begin{bmatrix}0 & -2 & 2 & 0 & 0 & 2 & -2 & 0 & 0 & -2 & 2 & 0 & 0 & 2 & -2 & 0\end{bmatrix}.
\end{aligned} \tag{22}$$

Further, using (17), as well as his own set of vectors $\{h_{1,i}\}$ (19), the first user calculates the vector $P_{1,k}$, as well as, in accordance with expression (18), the data bit intended for him

$$P_{1,k} = \begin{bmatrix} 16 & 16 & 16 & 16 \end{bmatrix} \rightarrow d_{1,k} = 1. \tag{23}$$

Similarly, the vector $P_{2,k}$, as well as the intended data bit, is calculated by the second user

$$P_{2,k} = \begin{bmatrix} -16 & -16 & -16 & -16 \end{bmatrix} \rightarrow d_{2,k} = -1. \tag{24}$$

Characteristics of the developed multiple-access steganographic method

One of the most important properties of the developed steganographic method is the possibility of simultaneous operation of such a number of users, which is necessary at the given moment, with the total number J of registered users, each of which has its own frequency arrangement.

Nevertheless, with an increase in the number of simultaneously operating users in the system, the information load on the image-container increases, and, accordingly, its quality deteriorates. As a measure of the quality of a steganographic message, we will take the PSNR [1] indicator, which is determined in accordance with the following formula

$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \tag{25}$$

Where

$$MSE = \frac{1}{nm}\sum_i \sum_j \left| X(i,j) - M(i,j) \right|^2 . \tag{26}$$

In Fig. 1 a graph of the dependence of PSNR of steganographic messages on the number of simultaneously operating in the system users is shown.

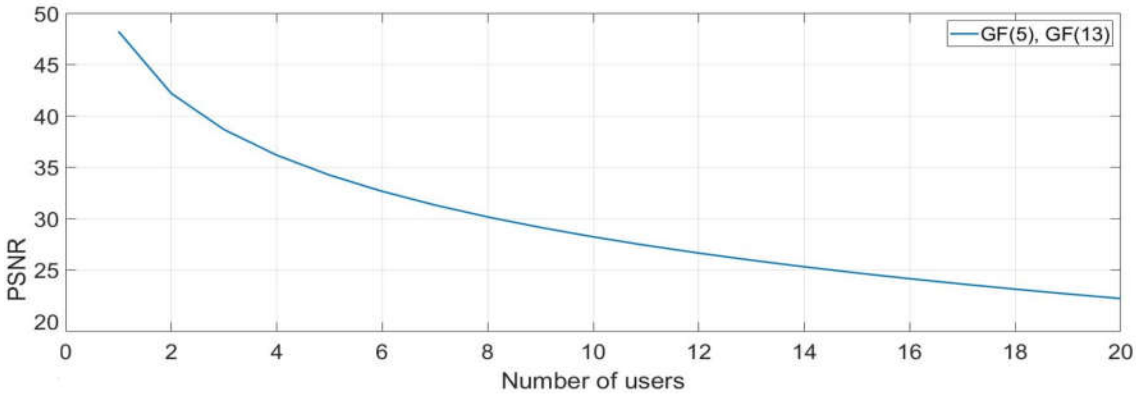
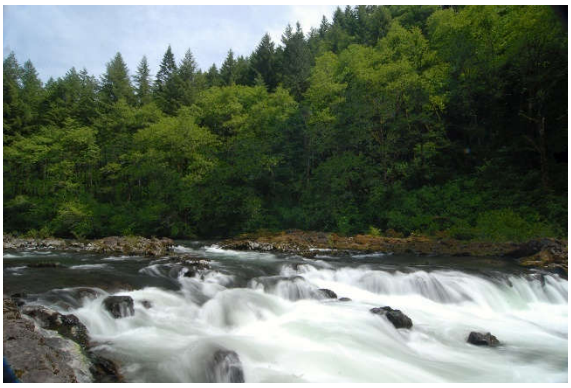


Fig. 1. Graph of dependence of PSNR of steganographic message on the number of simultaneously operating users

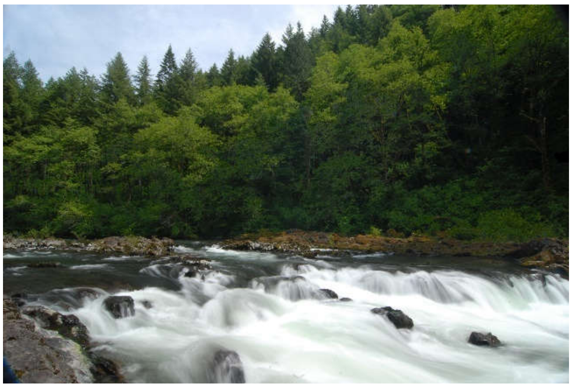
To obtain this data, an experiment was performed using 500 lossless TIFF images from the NRCS database [12], into each of which information coming from a different number of users was embedded, after which the PSNR of the received steganographic message was measured.

The analysis of data displayed on Fig. 1 shows that an increase in the number of simultaneously operating users leads to a drop in the PSNR of a steganographic message, and this process is the same both for the case of using the frequency arrangement code based on the RS-code over the Galois field $GF(5)$ and over the Galois field $GF(13)$. Note that with the number of simultaneously operating users $N \le 8$, the PSNR values remain at an acceptable level. In the case of using frequency arrangements based on the RS-code over the Galois field $GF(5)$, information is embedded into the high-frequency components, therefore, even with a value $PSNR \approx 30\,dB$, the reliability of perception remains at a sufficient level, which can be clearly seen in Fig. 2.

Moreover, in Fig. 2 into the blue RGB component of an image of size 2592x3872 with a total number of shared channels $N = 20$ we embedded in total a $20 \cdot 324 \cdot 484$ bits=3136320 bits = 382.85 KB of information.



a)



b)

Fig. 2. An example of a steganographic message with embedded information from $N = 20$ users (a), as well as the original container (b)

Subjective ranking of the images shown in Fig. 2 does not reveal any artifacts or visual differences from the original container image in the steganographic message.

A property of asynchronous address communication systems, which is reflected in the developed steganographic method with multiple access, is the presence of intra-system interference: forming into a common stream, pulses of other channels can accidentally form a code combination of a given channel, leading to the appearance of a corresponding interference. Another type of intra-system noise is interference suppression and nonlinear pulse suppression.

The experiments performed show that intra-system interference appears when the number of users simultaneously operating in the system exceeds the value q. In Fig. 3 we show the dependence of the number of errors (in %) occurring in the communication channel (channel of each of the users) depending on the number of users operating in the system for frequency arrangement codes based on RS-codes over the Galois fields $GF(5)$ and $GF(13)$.

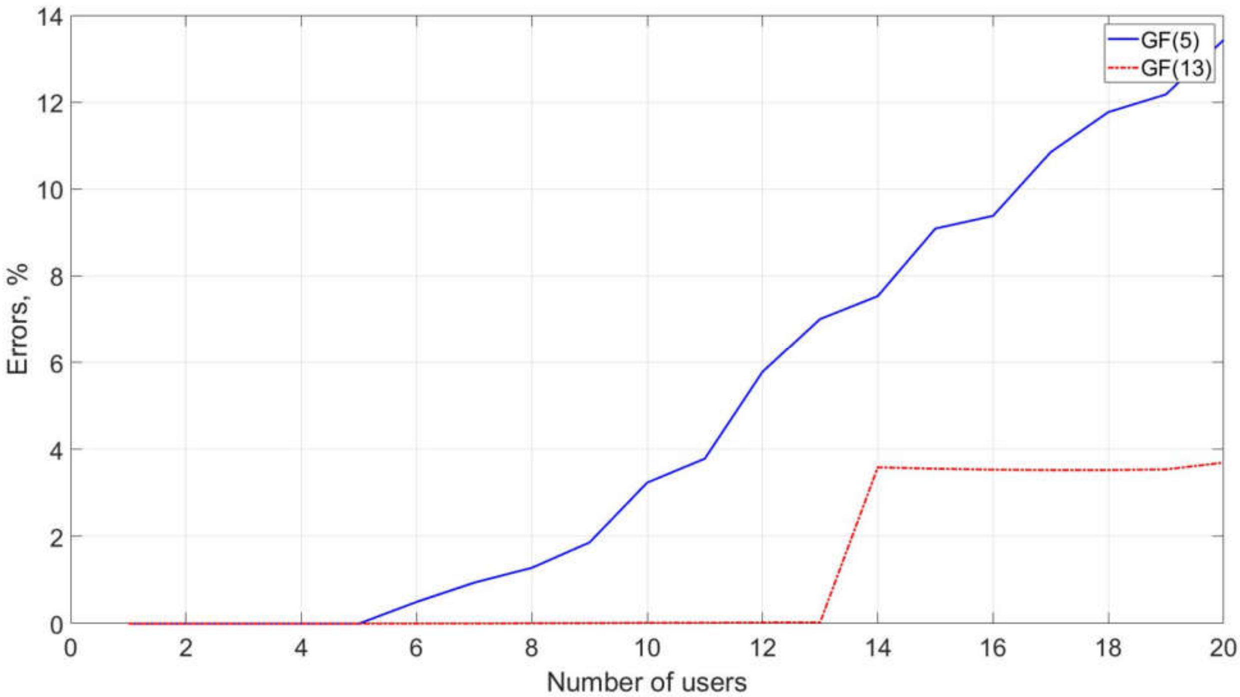


Fig. 3. Graphs of the dependence of the percentage of errors resulting from intra-system interference on the number of users

Analysis of the data presented in Fig. 3 shows that frequency arrangements based on the RS-code over the Galois field $GF(5)$ allow simultaneous operation of $N=5$ users without the occurrence of intra-system interference, while frequency arrangements based on the RS-code over the Galois field $GF(13)$ allow simultaneous operation of $N=13$ users without the occurrence of intra-system interference, however, even for values of the number of simultaneously operating users $N=20$ for these frequency arrangements (Table 2), the level of intra-system interference remains acceptable, and the number of errors that occur does not exceed 3.7%.

Conclusions

Let us note the main results obtained in this paper:

1. In contrast to the well-known analogs that perform code division of channels regardless of the embedding of information into the container, in this paper we developed a fully-fledged steganographic method with multiple access based on code control and frequency arrangements. The developed steganographic method that provides the separate embedding (absence of the embedding) of information by each user at any time which is convenient for him using a personal frequency arrangement. It is proposed to use RS-codes over the Galois fields $GF(5)$ and $GF(13)$ as the frequency arrangement codes, which ensure the maximum reliability of perception and the largest number of simultaneously operating users.

2. The characteristics of the developed method are researched, within the framework of which it is shown that the PSNR of the resulting steganographic message depends on the number of users simultaneously transmitting information through the steganographic channel. With the number of simultaneously operating users $N \le 8$, the PSNR values remain at an acceptable level. The existence of intra-system interference in the steganographic channel was detected with the number of simultaneously transmitting information users $N > q$. However, in the case of using frequency arrangements based on RS-codes over the Galois field $GF(13)$ with the number of users $N=20$, the number of errors generated by intra-system interference does not exceed 3.7%.

3. The developed steganographic method is a rational solution if it is necessary to organize a steganographic channel with multiple access and can provide flexible resource allocation: the operation of the required number of users with a given bandwidth (by allocating several communication channels to individual users) and the necessary reliability of perception (by increasing or reducing the number of simultaneously operating users).

References

1. Kobozeva A.A., Horoshko V.A. Information security analysis. Kiev: GUIKT, 2009. 251 p. (Original text in Russian)
2. Su A., Ma S., Zhao X. Fast and secure steganography based on J-UNIWARD. IEEE Signal Processing Letters. 2020. Vol. 27. P. 221-225.
3. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130. (Original text in Russian)
4. Melnik M.A. Compression-resistant steganographic algorithm. Information security. 2012. №2(8). P. 99-106. (Original text in Russian)
5. Chang C.C., Lin C.C., Hu Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. International Journal of Innovative Computing, Information & Control, 2007.Vol. 3, No. 3. P. 609-620.
6. Chanu Y.J., Singh Kh.M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. International Journal of Information & Computation Technology, 2014. Vol. 4, No. 7. P. 717-726.
7. Singh N. High PSNR based image steganography. Int J Adv Eng Res Sci (IJAERS). 2019. Vol. 6. No. 1. P. 109-115.
8. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. International Conference on Signal Acquisition and Processing. Singapore, 2011. Vol. 2. P. 1-5.
9. Czvetkov K.Yu., Fedoseev V.E., Korovin V.M., Abazina E.S. Model of a covert channel code division multiple coder using Frank-Walsh, Frank-Chrestenson signaling sequences. Proceedings of the Radio Research Institute. 2015. No. 1. P. 2-11. (Original text in Russian).
10. Kobozeva A.A., Sokolov A.V. Efficient Coding of the Embedded Signal in Steganographic Systems with Multiple Access. Problemele energeticii regionale. 2021. No. 2 (50). P. 101-113. (Original text in Russian)
11. Mazurkov M.I. Broadband radio systems. Odessa: Science and Technology, 2010. 340 p. (Original text in Russian)
12. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

СТЕГАНОГРАФІЧНИЙ МЕТОД МНОЖИННОГО ДОСТУПУ НА ОСНОВІ КОДОВОГО УПРАВЛІННЯ ТА ЧАСТОТНИХ РОЗСТАНОВОК

А.В. Соколов

Національний Університет «Одеська політехніка»
Одеса, 65044, пр.Шевченка, 1, e-mail: radiosquid@gmail.com

Розвиток, а також ширше практичне застосування сучасної стеганографії призводить до необхідності створення стеганографічних методів з множинним доступом, які могли б забезпечити одночасну передачу і розділення у стеганографічному каналі інформації від декількох користувачів. Відомі на сьогоднішній день стеганографічні методи з множинним доступом засновані на технології MC-CDMA і не показують, як саме має відбуватися вбудовування та вилучення додаткової інформації. Метою цієї статті є розробка стеганографічного методу з множинним доступом на основі кодового управління та частотних розстановок. Поставлена мета була досягнута за рахунок розробки стеганографічного методу з кодовим управлінням та застосуванням частотних розстановок на основі двічі циклічних кодів Ріда-Соломона над полями Галуа GF(q), що забезпечує роздільне вбудовування інформації кожним користувачем у будь-який зручний для нього час з використанням особистої частотної розстановки. При цьому частотні розстановки запропоновано будувати за допомогою РС-кодів над полями GF(5) і GF(13). Досліджено характеристики розробленого методу, в рамках чого показано, що PSNR результуючого стеганоповідомлення залежить від кількості користувачів, що одночасно передають інформацію через стеганографічний канал. При кількості одночасно працюючих абонентів $N \leq 8$, значення PSNR залишаються на допустимому рівні. Під час роботи запропонованого стеганографічного методу виявлено виникнення внутрішньосистемних перешкод у стеганографічному каналі при кількості абонентів $N > q$, що одночасно передають інформацію, однак при використанні частотних розстановок на основі РС-коду над полем GF(13), їх вплив є несуттєвим при практично обґрунтованій кількості каналів, що розділяються. Розроблений стеганографічний метод є раціональним рішенням у разі необхідності організації стеганографічного каналу з множинним доступом і може забезпечити гнучкий розподіл ресурсів: роботу потрібної кількості абонентів із заданою пропускною здатністю та необхідною надійністю сприйняття.

Ключові слова: стеганографія, кодове управління, множинний доступ, кодове розподілення каналів, частотні розстановки.