DOI 10.15276/imms.v12.no1-2.5
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 5-14

THE STEGANOGRAPHIC METHOD WITH MULTIPLE ACCESS BASED ON FREQUENCY-SPATIAL MATRICES

A.V.Sokolov

National Odessa Polytechnic University
Ukraine, Odesa, 65044, Shevchenko Ave., 1, radiosquid@gmail.com

The solution to some practical tasks with the help of steganography requires the organization of multiple access to a steganographic information transmission channel. At the same time, existing developments imply the use of MC-CDMA technology to solve these tasks, which has a strictly predetermined number of shared channels, requires the simultaneous embedding of additional information delivered from all users and is disintegrated with the applied steganographic algorithm. In this paper, a full-fledged steganographic method, with multiple access based on the use of frequency-spatial matrices has been developed. In the developed method, two code attributes are allocated to each user: frequency and spatial, on the basis of which codewords that are used to transmit information are generated. The total number of registered users operating in the system based on the proposed steganographic method can reach the value of J=4800, while the total number of users simultaneously transmitting information can reach the value of N=100 while supporting the practically acceptable system parameters. At the same time, the embedding of additional information by the users occurs independently of each other at any time convenient to them. To ensure the largest number of simultaneously operating users and minimize the level of intra-system interference, an S-code of spatial arrangements, as well as an F-code of frequency arrangements based on the Reed-Solomon code, are proposed. The proposed steganographic method with multiple access is characterized by flexibility in the allocation of resources of the steganographic channel: if necessary, the throughput of the steganographic channel can be increased with a decrease in PSNR values, or, conversely, the reliability of perception of the steganographic message can be increased by reducing the number of users simultaneously operating in the system.

Keywords: steganography, code control, multiple access, code division of channels, frequency-spatial matrices.

Introduction and statement of the problem

The development of modern information security systems, in addition to cryptographic tools, involves the active introduction and use of the steganographic component, which allows not only to make confidential information unreadable by unauthorized users but also to hide the very fact of its transmission.

In addition to the well-known steganographic methods, which have such properties as simplicity of algorithmic implementation [1…3], minimization of distortions introduced into the container image [4, 5], resistance to various types of attacks against the additional information (lossy compression attacks, noise, blurring) [6…8], the current stage of development of steganography is characterized by the emergence of steganographic methods with multiple access.

Thus, in [9] it is proposed to use the MC-CDMA (Multi-Code Code Division Multiple Access) technology based on the orthogonal Walsh-Hadamard transform to organize multiple access. The disadvantages of this technology include the fact that the number of users is strictly predetermined and equal to $N = 2^k = 2, 4, 8, 16, \ldots$, as well as the disintegration of multiple access technology with the steganographic method used, i.e., MC-CDMA technology does not show exactly how the embedding and extraction of additional information should be performed.

As the performed research has shown, the possibility of overcoming these shortcomings of using MC-CDMA technology in steganographic applications lies in the development of new classes of steganographic structures labelled as frequency-spatial codes, which imply the

possibility of multiple access within a common steganographic channel by using two attributes: frequency and spatial.

The *purpose* of this paper is to develop a steganographic method with multiple access based on frequency-spatial matrices.

The main idea of the developed method

The main orthogonal transform used in the proposed method is the Walsh-Hadamard transform [10], the one-dimensional version of which can be written as

$$V = YH_N, \tag{1}$$

where Y is a row vector of length N, H_N is a Walsh-Hadamard matrix of order $N = 2^k$, which can be constructed in accordance with the Sylvester construction

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

The two-dimensional version of the Walsh-Hadamard transform is determined using the following relationship

$$W = H'_N X H'^T_N, \tag{3}$$

where $H'_N = \frac{1}{N} H_N$, and X is a matrix of size $N \times N$.

The proposed steganographic method uses the relationship established in [11] between the two-dimensional and one-dimensional Walsh-Hadamard transform: up to a coefficient $1/N$, the two-dimensional Walsh-Hadamard transform (3) can be represented through the one-dimensional Walsh-Hadamard transform using the following relation $\tilde{W} = \tilde{Y}H_{N^2}$, where the operator $\tilde{A}$ denotes the representation of matrix A of order $N \times N$ as a row vector of length N^2 by sequential concatenation of its rows.

The basis of the operation of the proposed steganographic method is the linearity property of the Walsh-Hadamard transform, on the basis of which, by setting special properties of the embedded data, it is possible to selectively influence one or another transformant of the Walsh-Hadamard transform of the resulting steganographic message [11]. Indeed, if X is a container, D is additional information, and M is a steganographic message, then

$$\begin{gathered} \tilde{M} = \tilde{X} + \tilde{D}; \\ \tilde{M}H_{N^2} = \tilde{X}H_{N^2} + \tilde{D}H_{N^2}. \end{gathered} \tag{4}$$

Thus, by performing preliminary encoding of information using a special form of codewords matrices, we can get a targeted impact on one or another Walsh-Hadamard transformant of the original container image. Codewords affecting the corresponding Walsh-Hadamard transformants (*n*,*m*), as well as their corresponding frequency components $f_i, i = 1,2,...,16$ are presented in Table 1.

Let us consider the essence of the idea of the steganographic method based on frequency-spatial matrices. The operations of embedding and extraction of additional information in this method are based on dividing the image on the blocks Q_k of size $\mu \times \mu = 16 \times 16$. Each of the obtained blocks is divided into 16 more blocks q_i, $i = 1,2,...,16$ of size 4×4

$$Q_k = \begin{array}{|c|c|c|c|} \hline q_1 & q_2 & q_3 & q_4 \\ \hline q_5 & q_6 & q_7 & q_8 \\ \hline q_9 & q_{10} & q_{11} & q_{12} \\ \hline q_{13} & q_{14} & q_{15} & q_{16} \\ \hline \end{array}. \tag{5}$$

Table 1

Codewords for targeted influence for each of the Walsh-Hadamard transformants

$T^{+}_{4,(1,1)} \leftrightarrow f_0$	$T^{+}_{4,(1,2)} \leftrightarrow f_1$	$T^{+}_{4,(1,3)} \leftrightarrow f_2$	$T^{+}_{4,(1,4)} \leftrightarrow f_3$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$
$T^{+}_{4,(2,1)} \leftrightarrow f_4$	$T^{+}_{4,(2,2)} \leftrightarrow f_5$	$T^{+}_{4,(2,3)} \leftrightarrow f_6$	$T^{+}_{4,(2,4)} \leftrightarrow f_7$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
$T^{+}_{4,(3,1)} \leftrightarrow f_8$	$T^{+}_{4,(3,2)} \leftrightarrow f_9$	$T^{+}_{4,(3,3)} \leftrightarrow f_{10}$	$T^{+}_{4,(3,4)} \leftrightarrow f_{11}$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
$T^{+}_{4,(4,1)} \leftrightarrow f_{12}$	$T^{+}_{4,(4,2)} \leftrightarrow f_{13}$	$T^{+}_{4,(4,3)} \leftrightarrow f_{14}$	$T^{+}_{4,(4,4)} \leftrightarrow f_{15}$
$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

The division of user channels is performed based on two properties: frequency and spatial. In other words, to each user 2 codewords are allocated: the S-code codeword of the spatial arrangement and the F-code codeword of the frequency arrangement. At the same time, the codeword of the S-code determines the numbers of blocks q_i into which this user can embed information, while the codeword of the F-code determines those Walsh-Hadamard transformants into which this user can embed information using codewords, presented in Table 1.

Construction of codewords of the S-code of spatial arrangements

To solve the problem of constructing S-codes of spatial arrangements, each codeword of which contains 16 binary components that show whether the given spatial component is active (the value of the element of the codeword is $s_i = 1$) or passive (the value of the element of the codeword is $s_i = 0$), an approach based on exhaustive search has been adopted. In our case, in order to maximize the number of simultaneously operating users, as well as to ensure the highest reliability of perception, codewords of the S-code of spatial arrangements of Hamming weight $wt(\{s_i\}) = 4$ are preferred. The total number of binary vectors of length $N = 16$ and weight $wt(\{s_i\}) = 4$ is determined by the number of 4-permutations of 16 i.e. $C_{16}^{4} = 1820$ and constitute a code with the number of overlaps of active components $\lambda \le 3$.

To solve the problem of minimizing intra-system interference caused by the interference of codewords from different users, it is necessary, based on the full code of the length $N = 16$ and weight $wt(\{s_i\}) = 4$, to construct a spatial arrangements S-code, the codewords of which are characterized by the number of overlaps of active components $\lambda \le 1$.

As experiments show, the cardinality of the constructed code will depend on the order in which codewords are chosen during its construction. Let's use the following approach:

Step 1. We fix the first four possible codewords of the full code of length $N=16$ and weight $wt(\{s_i\})=4$, which have the number of overlaps of active components $\lambda=0$. Thus, by connecting new users with help of these codewords, we will ensure the complete absence of intra-system interference

$$S'=\begin{bmatrix}\{s_{1,i}\}\\ \{s_{2,i}\}\\ \{s_{3,i}\}\\ \{s_{4,i}\}\end{bmatrix}=\begin{bmatrix}\{1111000000000000\}\\ \{0000111100000000\}\\ \{0000000011110000\}\\ \{0000000000001111\}\end{bmatrix}, i=1,...,16. \quad (6)$$

Step 2. Sampling codewords from the full set of vectors of length $N=16$ and weight $wt(\{s_i\})=4$, we build 16 more codewords that have the number of overlaps $\lambda\le 1$ between themselves and relative to codewords (6). As a result, we obtain the following ensemble of cardinality $J_S=20$

$$S=\begin{bmatrix}\{s_{1,i}\}\\ \{s_{2,i}\}\\ \{s_{3,i}\}\\ \{s_{4,i}\}\\ \{s_{5,i}\}\\ \{s_{6,i}\}\\ \{s_{7,i}\}\\ \{s_{8,i}\}\\ \{s_{9,i}\}\\ \{s_{10,i}\}\\ \{s_{11,i}\}\\ \{s_{12,i}\}\\ \{s_{13,i}\}\\ \{s_{14,i}\}\\ \{s_{15,i}\}\\ \{s_{16,i}\}\\ \{s_{17,i}\}\\ \{s_{18,i}\}\\ \{s_{19,i}\}\\ \{s_{20,i}\}\end{bmatrix}=\begin{bmatrix}\{1111000000000000\}\\ \{0000111100000000\}\\ \{0000000011110000\}\\ \{0000000000001111\}\\ \{1000100010001000\}\\ \{0100010001001000\}\\ \{0010001000101000\}\\ \{0001000100011000\}\\ \{0010010010000100\}\\ \{0001100001000100\}\\ \{1000000100100100\}\\ \{0100001000010100\}\\ \{0001001010000010\}\\ \{0010000101000010\}\\ \{0100100000100010\}\\ \{1000010000010010\}\\ \{0100000110000001\}\\ \{1000001001000001\}\\ \{0001010000100001\}\\ \{0010100000010001\}\end{bmatrix}, i=1,...,16, \quad (7)$$

which will be used as the S-code.

Construction of the codewords of the F-code of frequency arrangements

As a basis for constructing the F-code of frequency arrangements in this paper we use doubly cyclic Reed-Solomon (RS) codes [12]. In order to maximize the number of users who can simultaneously operate in a steganographic channel, it is rational to use all available frequency components. For this purpose, to construct frequency arrangements, we use the second-order RS-code in the extended Galois field $GF(2^4)$, which has the following characteristics: codeword length $N=15$, number of information bits $K=2$, code distance $d=N-K+1=15-2+1=14$.

Note that Galois field $GF(2^4)$ has two isomorphic representations, which are determined by two primitive irreducible polynomials $h_1(x)=x^4+x+1$ and $h_2(x)=x^4+x^3+1$. However, from the point of view of the technique for constructing a steganographic method with multiple access, the choice of a specific isomorphism of the Galois field is not of decisive importance, therefore, we will use the arithmetic of the extended Galois field, defined by the primitive irreducible polynomial $h_1(x)$. In this case, the addition and multiplication table in the field $GF(2^4)$ will take the form

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	D
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

(8)

Taking the value of the primitive element $\theta = 2$, we construct a generating RS-code polynomial in the Galois field $GF(2^4)$

$$g(z) = \prod_{i=1}^{d-1}(z-\theta^i) = \prod_{i=1}^{13}(z-2^i) =$$

$$(z+2)(z+4)(z+8)(z+3)(z+6)(z+12)(z+11)(z+5)(z+10)(z+7)(z+14)(z+15)(z+13) = \quad (9)$$

$$= 2+6z+14z^2+13z^3+11z^4+7z^5+12z^6+9z^7+3z^8+4z^9+10z^{10}+5z^{11}+8z^{12}+z^{13}.$$

Based on the obtained generating polynomial, we write the generating matrix of the RS-code

$$G = \begin{bmatrix} 2 & 6 & 14 & 13 & 11 & 7 & 12 & 9 & 3 & 4 & 10 & 5 & 8 & 1 & 0 \\ 0 & 2 & 6 & 14 & 13 & 11 & 7 & 12 & 9 & 3 & 4 & 10 & 5 & 8 & 1 \end{bmatrix}, \quad (10)$$

the first row of which is the base codeword, on the basis of which, using the properties of double cyclicity of RS-codes, it is possible to construct all other codewords by applying the operation of cyclic shift in time and cyclic shift in frequency (using Galois field $GF(2^4)$ arithmetic). In this case, the total number of codewords of the F-code of frequency arrangements constructed by us is defined as

$$J = q(q-1) = 16 \cdot 15 = 240. \quad (11)$$

In view of the fact that the length of each frequency arrangement in accordance with the construction of the steganographic method should be $n = 4$, we will truncate each codeword of the RS-code to the specified length, the resulting codewords are presented in Table 2. At the same time, for brevity, the codewords are written in hexadecimal form.

Table 2

Truncated codewords of the RS-code in the Galois field $GF(2^4)$

26ED	6EDB	EDB7	DB7C	B7C9	7C93	C934	934A	34A5	4A58	A581	5810	8102	1026	026E
37FC	7FCA	FCA6	CA6D	A6D8	6D82	D825	825B	25B4	5B49	B490	4901	9013	0137	137F
04CF	4CF9	CF95	F95E	95EB	5EB1	EB16	B168	1687	687A	87A3	7A32	A320	3204	204C
15DE	5DE8	DE84	E84F	84FA	4FA0	FA07	A079	0796	796B	96B2	6B23	B231	2315	315D
62A9	2A9F	A9F3	9F38	F38D	38D7	8D70	D70E	70E1	0E1C	E1C5	1C54	C546	5462	462A
73B8	3B8E	B8E2	8E29	E29C	29C6	9C61	C61F	61F0	1F0D	F0D4	0D45	D457	4573	573B
408B	08BD	8BD1	BD1A	D1AF	1AF5	AF52	F52C	52C3	2C3E	C3E7	3E76	E764	7640	6408
519A	19AC	9AC0	AC0B	C0BE	0BE4	BE43	E43D	43D2	3D2F	D2F6	2F67	F675	6751	7519
AE65	E653	653F	53F4	3F41	F41B	41BC	1BC2	BC2D	C2D0	2D09	D098	098A	98AE	8AE6
BF74	F742	742E	42E5	2E50	E50A	50AD	0AD3	AD3C	D3C1	3C18	C189	189B	89BF	9BF7
8C47	C471	471D	71D6	1D63	D639	639E	39E0	9E0F	E0F2	0F2B	F2BA	2BA8	BA8C	A8C4
9D56	D560	560C	60C7	0C72	C728	728F	28F1	8F1E	F1E3	1E3A	E3AB	3AB9	AB9D	B9D5
EA21	A217	217B	17B0	7B05	B05F	05F8	5F86	F869	8694	694D	94DC	4DCE	DCEA	CEA2
FB30	B306	306A	06A1	6A14	A14E	14E9	4E97	E978	9785	785C	85CD	5CDF	CDFB	DFB3
C803	8035	0359	3592	5927	927D	27DA	7DA4	DA4B	A4B6	4B6F	B6FE	6FEC	FEC8	EC80
D912	9124	1248	2483	4836	836C	36CB	6CB5	CB5A	B5A7	5A7E	A7EF	7EFD	EFD9	FD91

Superposition of S-code and F-code codewords

In order to maximize the number of available divided communication channels in a common steganographic channel, the proposed method uses the rule of superposition of the codewords of the S-code of spatial arrangements and the F-code of frequency arrangements by superimposing the frequency components of the F-code on the active positions of the S-code.

Thus, the total number of users who can be registered and theoretically simultaneously transmit information in the steganographic channel is

$$J = J_S J_F = 20 \cdot 240 = 4800 . \qquad (12)$$

Let's consider a specific example. Let the S-code codeword $\{s_{1,i}\} = \{1111000000000000\}$ is allocated to user A_1 , as well as the F-code codeword $C_1 = \{26ED\} = \{2 \quad 6 \quad 14 \quad 13\}$. To obtain codewords T^+ and T^- used for the embedding of information symbols “0” and “1”, respectively, the user performs a superposition of the S-code and F-code codewords allocated to him, for which he follows the following algorithm:

Step 1. Represent the codeword of the S-code as a matrix of size 4×4 by sequentially filling its rows.

Step 2. Sequentially write in the active positions of the matrix obtained at *Step 1* the frequency components, the indices of which are determined by the values of the F-code codeword.

Performing *Step 1* and *Step 2* of the presented algorithm for our example, we obtain the following construction

$$T^{+\prime} = \begin{bmatrix} f_2 & f_6 & f_{14} & f_{13} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} . \qquad (13)$$

Step 3. Substitute specific codewords $T_{4,(n,m)}$ presented in Table 1 based on their correspondence to frequency components f_i. In this case, instead of the values "0" in the matrix (13), zero matrices of size 4×4 are substituted. As a result, we obtain a codeword for encoding the character "0" by this user.

Step 4. To obtain a codeword T^-, we invert the codeword T^+ obtained in *Step 3*.

In the case of our example, we get the following codewords T^+ and T^-

$$T^+ = \left[\begin{array}{cccc|cccc|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 \\
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
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right], \quad
T^- = \left[\begin{array}{cccc|cccc|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 \\
-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
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right]. \qquad (14)$$

The obtained codewords T^+ and T^- are used for the embedding of information symbols “0” and “1”, respectively.

The algorithms for embedding and extraction of additional information

Each user embeds information independently of other users at a time that is convenient for him. Consider the algorithms for information embedding and extraction.

The algorithm for information embedding

Step 1. A unique code $\{\{s_{z_1,i}\}, C_{z_2}\}$ consisting of the codeword of the S-code of spatial arrangements and the codeword of the F-code of frequency arrangements is allocated to the each of the users of the steganographic system.

Step 2. Based on the set $\{\{s_{z_1,i}\}, C_{z_2}\}$, taking into account (5), as well as codewords $f_i, i = 1,2,...,16$, each user generates codewords T^+ and T^-, with the help of which the information will be transmitted.

Step 3. Each user A_z splits the container image into the blocks of size $\mu \times \mu = 16 \times 16$ and embeds one bit $d_{z,k}$ of additional information into each of the container blocks X_k by applying the summation operation, i.e., each steganographic message block is calculated as

$$M_k = X_k + D_k. \tag{15}$$

The algorithm for information extraction

Step 1. The user who received the steganographic message splits it into blocks M_k of size $\mu \times \mu = 16 \times 16$, each of which is sequentially processed in order to extract a bit of information $d_{z,k}$ consigned for this user.

Step 2. The user finds the difference matrix Δ_k between each block of the received steganographic message M_k and the container image X_k.

Step 3. Each block of the difference matrix Δ_k is divided by the user into 16 subblocks of size $\frac{\mu}{4} \times \frac{\mu}{4} = 4 \times 4$ in accordance with construction (5). From the received subblocks, the user selects those whose number corresponds to the position numbers of the codeword of the S-code of spatial arrangements belonging to this user $\{s_{z_1,i}\}$, on which it takes the value 1 (when it is represented as a matrix of size 4×4 by sequentially filling of its rows). In view of the fact that all codewords of the S-code have weight $w = 4$, each of the users at this step chooses four subblocks of size 4×4. The user represents each of the received subblocks as a vector $\{\delta_{z,i}\}, i = 1,2,...,16$ of length $4^2 = 16$ by successive concatenation of its rows.

Step 4. In accordance with the code of frequency arrangements C_{z_2} allocated to this user, he selects the rows of the Walsh-Hadamard matrix H_{16}, which are designated as $\{h_{z,1}\}, \{h_{z,2}\}, \{h_{z,3}\}, \{h_{z,4}\}$.

Step 5. The user A_z calculates the vector P according to the following formula

$$\begin{gathered} P_{z,k} = [p_1 \quad p_2 \quad p_3 \quad p_4], \\ p_i = \sum_{k=1}^{\mu^2} \delta_{j,k} h_{j,k}, i = \{1,2,3,4\}. \end{gathered} \tag{16}$$

Step 6. The user calculates the data bit consigned for him, embedded in the block M_k using the following formula

$$d_{z,k} = sign\left(\sum_{i=1}^{4} p_i \right). \tag{17}$$

Characteristics of a steganographic method with multiple access based on frequency-spatial matrices

To estimate the level of perturbation of the container image when additional information is embedded into it using the proposed steganographic method, we use the difference indicator PSNR, which is defined as

$$\mathrm{PSNR} = 20 \lg\left(\frac{255}{\sqrt{\mathrm{MSE}}} \right), \tag{18}$$

where

$$\mathrm{MSE} = \frac{1}{nm}\sum_i \sum_j \left| X(i,j) - M(i,j) \right|^2 , \tag{19}$$

where n and m represent the size of the original message.

By construction of the proposed steganographic method, it becomes clear that the PSNR of a steganographic message will depend on the number of users in the system simultaneously transmitting information, as well as on the type of S-code and F-code codewords allocated to them. When connecting users in the order of presentation of codewords (7) and Table 2, the graph of PSNR dependence on the number of users simultaneously functioning in the system, will have the form shown in Fig 1.

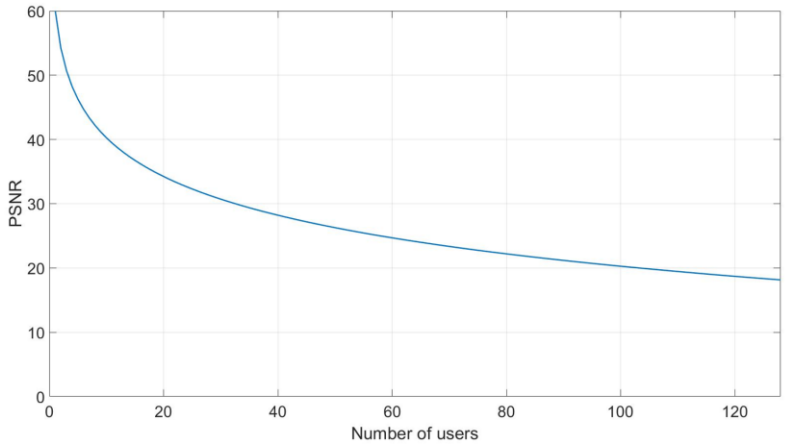

Fig. 1. Dependence graph of the PSNR of a steganographic message on the number of users simultaneously transmitting information using the steganographic channel

Analysis of the data presented in Fig. 1 shows that with the number of users simultaneously transmitting information $N \le 32$, it is possible to achieve a PSNR value of more than 30 dB. With the simultaneous operation of $N \le 100$ users, the PSNR level of the steganographic message does not fall below 20 dB. In view of the fact that the codewords of the S-code of spatial arrangements (7) allow no more than one overlap in space, as well as the codewords of the F-code of frequency arrangements (Table 2) allow no more than one overlap in frequency, the occurrence in the steganographic system of intra-system interference is inevitable. The level of intra-system interference will be directly proportional to the number of users simultaneously transmitting information. It is also clear that the level of intra-system interference will depend on the specific codewords of the S-code and F-code of users who are currently transmitting information through the steganographic channel.

Fig. 2 shows a graph of the dependence of the number of errors in the steganographic channel arising due to the action of intra-system interference on the number of simultaneously operating users when they are connected in the order in which codewords are presented in (7) and Table 2.

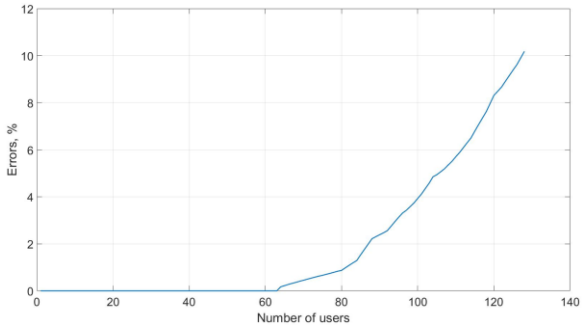

Fig. 2. Graph of the dependence of the number of errors in the steganographic channel arising due to the action of intra-system interference on the number of simultaneously operating users

Analysis of the data presented in Fig. 2 shows that with the selected order of connection of users for their number $N \le 64$, there are no intra-system interference, as a result of which all

information is transmitted without distortion. In the case of the number of users $N \le 100$, the number of errors that occur due to intra-system interference does not exceed the level of 4%, which is acceptable.

Conclusions

We note the main results of the research:

1. A full-fledged steganographic method with multiple access based on frequency-spatial matrices is proposed, which provides separate embedding (or its absence) of information by each user at any time convenient for them. Dividing of user channels is performed according to two properties: spatial and frequency, based on S-codes of spatial arrangements and F-codes of frequency arrangements. In this paper, we construct an S-code of spatial arrangements of cardinality $J_S = 20$ with the property of no more than one overlap, as well as an F-code of frequency arrangements based on the Reed-Solomon code of cardinality $J_F = 240$ in the Galois field $GF(2^4)$, which also has the property of no more than one overlap.

2. The possible total number of registered in the steganographic system with multiple access users is equal to $J = 4800$, while the characteristics of the developed steganographic method directly depend on the number of users simultaneously transmitting information. So, with the number of users simultaneously transmitting information $N \le 32$, the PSNR value does not exceed the level of 30 dB, while with the number of users $N \le 64$ there is no intra-system interference.

3. The proposed steganographic method with multiple access is characterized by flexibility in the distribution of steganographic channel resources: if necessary, the throughput of the steganographic channel can be increased with a decrease in PSNR values, or, conversely, the reliability of perception of a steganographic message can be increased by reducing the number of users simultaneously operating in the system. In this case, the embedding of information into the container by each of the users, occurs independently.

References

1. Astuti Y. P. et al. Simple and secure image steganography using LSB and triple XOR operation on MSB. *International Conference on Information and Communications Technology (ICOIACT). IEEE*. 2018. P. 191-195.

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. Li W. et al. Shortening the cover for fast JPEG steganography. *IEEE Transactions on Circuits and Systems for Video Technology*. 2019. Vol. 30. No. 6. P. 1745-1757.

4. Singh N. High PSNR based image steganography. *Int J Adv Eng Res Sci (IJAERS)*. 2019. Vol. 6, No. 1. P. 109-115.

5. Krishnaveni N., Periyasamy S. Image steganography using LSB embedding with chaos. *International Journal of Pure and Applied Mathematics*. 2018. Vol. 118, No. 8. P. 505-509.

6. Qiao T. et al. Robust steganography resisting JPEG compression by improving selection of cover element. *Signal Processing*. 2021. Vol. 183. P. 108048.

7. Zhu Z. et al. Robust steganography by modifying sign of DCT coefficients. *IEEE Access*. 2019. Vol. 7. P. 168613-168628.

8. Bao Z. et al. A robust image steganography on resisting JPEG compression with no side information. *IETE Technical Review*. 2018. Vol. 35, No. sup1. P. 4-13.

9. 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.

10. Horadam K. J. Hadamard matrices and their applications. Princeton university press, 2012. 280 p.

11. Kobozeva A. A., Sokolov A. V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele Energeticii Regionale.* 2021. Vol. 52, No. 4. P. 115-130.

12. Mazurkov M. I., Broadband Radio Communication Systems. Odessa: Science and Technology, 2010. 340 p.

СТЕГАНОГРАФІЧНИЙ МЕТОД З МНОЖНИМ ДОСТУПОМ НА ОСНОВІ ЧАСТОТНО-ПРОСТОРОВИХ МАТРИЦЬ

А.В. Соколов

Національний університет "Одеська політехніка"
Україна, Одеса, 65044, пр-т Шевченка, 1, radiosquid@gmail.com

Вирішення низки завдань із застосуванням стеганографії вимагає організації множинного доступу до стеганографічного каналу передачі інформації. При цьому існуючі розробки мають на увазі використання технології MC-CDMA, яка характеризується строго регламентованою кількістю каналів, що розділяються, вимагає одночасного вбудовування інформації від усіх абонентів, а також є дезінтегрованою із застосованим стеганографічним алгоритмом. У цій статті розроблено повноцінний стеганографічний метод з множинним доступом, заснований на застосуванні частотно-просторових матриць — кожному користувачеві виділяються дві кодові ознаки: частотна і просторова, на основі яких відбувається генерація кодових слів, що застосовуються для передачі інформації. Загальна кількість абонентів, зареєстрованих у працюючій на основі запропонованого стеганографічного методу системі, може досягати J=4800, у той час як загальна кількість абонентів, що одночасно передають інформацію, може досягати значення N=100 при практично прийнятних параметрах системи. При цьому вбудовування інформації абонентами відбувається незалежно один від одного в будь-який зручний для них час. Для забезпечення найбільшої кількості абонентів, що одночасно працюють, а також з метою мінімізації рівня внутрішньосистемних перешкод, запропоновано S-код просторових розстановок, а також F-код частотних розстановок на основі коду Ріда-Соломона. Розроблений стеганографічний метод з множинним доступом характеризується гнучкістю в розподілі ресурсів стеганоканалу: у разі необхідності пропускну спроможність стеганоканалу може бути збільшено зі зменшенням значень PSNR, або ж, навпаки, може бути збільшена надійність сприйняття стеганоповідомлення за рахунок зменшення кількості абонентів, що одночасно працюють.

Ключові слова: стеганографія, кодове управління, множинний доступ, кодовий розподіл каналів, частотно-просторові матриці.