A New Method for Embedding Secret Data to the Container Image Using 'Chaotic' Discrete Orthogonal Transforms

Vladimir Chernov[1], Oleg Bespolitov [2]

[1] Image Processing Systems Institute of RAS
151 Molodogvardejskaya St., 443001, Samara, Russia

[2] Samara State University

Abstract. In this paper a method for embedding the secret data into the container image is considered. The method is based on specifics of the spectral properties of ad hoc two-dimensional discrete orthogonal transform. The values of functions forming the basis of this transform are `chaotically' distributed. Two ideas provide the ground for the synthesis of these bases. Firstly, the 1D M-transforms, that were introduced and investigated in certain particular cases by H.-J. Grallert. Secondly, the application of introduced by I. Kàtai canonical number systems in finite fields to numerating the input image pixels.

1 Introduction

Many methods of embedding secret data into the container image are based on the modification of one or several least-significant bits of digital image pixels [1]-[3]. In this paper we propose an alternative method, based on modification of spectral components (components of two-dimensional orthogonal transform spectrum of the container image) [4]-[5]. Let $x(n_1,n_2); n_1,n_2 = 0,1,...,N-1$ be the container image. Let the discrete orthogonal transform be given by:

$$\hat{x}(m_1,m_2) = \sum_{n_1,n_2=0}^{N-1} x(n_1,n_2)h_{m_1,m_2}(n_1,n_2); \quad m_1,m_2 = 0,1,...,N-1\,, \tag{1}$$

$$< h_{u_1,u_2}, h_{v_1,v_2} >= \sum_{n=0}^{N-1} h_{u_1,u_2}(n_1,n_2)h_{v_1,v_2}(n_1,n_2) = \delta_{u_1,v_1}\delta_{u_2,v_2}\ . \tag{2}$$

Let $D \subset \{m_1,m_2 = 0,1,...,N-1\}$, let $\hat{s}(m_1,m_2) \in \{0,1\}; (m_1,m_2) \in D$ be the sensitive (secret) data that is to be embedded into the container $x(n_1,n_2)$. Let the spectrum of the output image (with the secret data embedded) be given by

$$\hat{y}(m_1,m_2) = \hat{s}(m_1,m_2)\hat{x}(m_1,m_2)\,. \tag{3}$$

Chernov V. and Bespolitov O. (2006).
A New Method for Embedding Secret Data to the Container Image Using 'Chaotic' Discrete Orthogonal Transforms.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 115-124

Copyright © SciTePress

Applying the inverse transform, with respect to the transform (1), we obtain the image $y(n_1, n_2)$, which contains in its spectrum (3) the secret data $\hat{s}(m_1, m_2)$.

Unfortunately, there are certain reasons that do not allow for use of 'classical' discrete orthogonal transforms (1)-(2) for the proposed approach. These transforms have several specific properties, which enable their successful application to video data encoding and make efficient certain image compressing algorithms. In particular, when these transforms are applied, the image energy is concentrated in relatively small fraction of spectral components. Thus, embedding the secret data into the container image according to the spectral technique described by (3) will result in addition of the 'structured', 'texturized', 'regular' noise (distortion) to the container. Note that this type of noise is known to be much more perceptible by human than random noise.

In the Fig. 2 example of the 'structured noise' is displayed. An example of the 'random' noise is provided in the Fig. 3.

Fig. 1. Original image.

Fig. 2. Distrortion after Hartley transform is applied.

Fig. 3. Distrortion after proposed transform is applied.

Thus, it is worth considering other types of orthogonal transforms, the transforms that don't concentrate the signal energy in few spectral components and allow for effective removal of the inessential data. In this work, we intent to consider the discrete orthogonal transform with the basis that is composed of 'noise-similar', 'chaotic' functions. For these transforms all the spectral components are 'energetically equivalent' and the image distortion associated with these transforms is similar to the additive Gaussian noise. For this transform the corresponding steganographic process (i.e. embedding of the secrete data to the container) represents addition of a low-energy Gaussian noise, and this process will be more secure than any bit-replacement technique. As during the image acquisition process, many different independent sources of Gaussian noise with varying amplitudes are superimposed onto the image, this is hard to determine whether the additional Gaussian noise is due to the channel/sensor properties or steganography [5].

One-dimensional transforms (1) that provide required distribution of the signal energy were introduced in [6]. The basis functions of these transforms have only two different values. In the papers [7]-[9] application of these transforms to processing the video information was considered. Various generalizations for the scheme described in [6] were proposed by one of the authors in the papers [10]-[11] for the functions $h_m(n)$ with *k* different values.

The essence of constructing the set of the considered orthogonal transform basis function is in use of the linear recurrence

$$y(n) = a_1 y(n-1) + ... + a_r y(n-r); \quad a_j \in \mathbf{F}_q, a_r \neq 0. \tag{4}$$

This recurrence is defined over the finite field $\mathbf{F}_q$ that consists of $q = p^s$ elements (where p is prime). The period of recurrence (4) is assumed to be maximal: $N = q^r - 1$ (in this case, the recurrent sequence (4) is an *m*-sequence [12],[13]).

While constructing the basis functions of the transform (1) the elements of the sequence $y(n) \in \mathbf{F}_q$ are replaced with the real numbers $h_m(n)$ in such a way, that for the functions $h_m(n)$ the orthogonality-constraints (2) are satisfied.

One of the principle obstacles that prevents the results introduced in the cited papers from being extrapolated to the two-dimensional case is the following: for 2D case a 'good' one-dimensional numeration of the two-dimensional array $\{(n_1, n_2); n_1, n_2 \in \mathbf{Z}\}$ is hard to be constructed. In the papers [14], [15] the conception was introduced of the canonical number systems (CNS) in the ring $\mathbf{S}(\sqrt{d})$ of integers from the quadratic fields $\mathbf{Q}(\sqrt{d}) = \{z = a + b\sqrt{d}\,; a, b \in \mathbf{Q}\}$. In terms of CNS, the elements $z \in \mathbf{S}(\sqrt{d})$ may be represented in a form of the finite sum

$$z = \sum_{j=o}^{k(z)} z_j \alpha^j \,, \tag{5}$$

where the 'digits' z_j are from the certain finite subset $\mathsf{N} \subset \mathbf{Z}$, and the element α (the base of the canonical number system) is an element of the ring $\mathbf{S}(\sqrt{d})$.

In this paper, we define the one-to-one map that takes the elements of the 'caterpiller' of the *N*-periodic *m*-sequence (4):

$$\mathbf{Y}_0 = (y(0), \ldots, y(r-1)), \mathbf{Y}_1 = (y(1), \ldots, y(r)), \ldots \tag{6}$$

to the elements of the ring $\mathbf{S}(\sqrt{d})$, represented in a form of *r*-term sums (5). Using this map for processing the two-dimensional signals (images) we may construct the *one-dimensional* numeration of the points from the two-dimensional integer lattice $\mathbf{Z}^2$ and synthesize the discrete orthogonal transforms (1)-(2) with the 'chaotic' distribution of the basis functions $h_m(n)$ values.

2 Mathematical Background

The proof of the facts that are stated below may be found in [12], [13] (linear recurrences) and in [14]-[15] (canonical number systems).

Recurrent functions in the finite fields.

Let $\mathbf{F}_q$ be a finite field that consists of $q = p^s$ elements, where p is prime.

Definition 1. The function that satisfies the linear recurrence (4), where

$$a_1, ..., a_r \in \mathbf{F}_q, \quad a_r \neq 0, \quad \mathbf{Y}_0 = (y(0), ..., y(r-1)),$$

is called a linear recurrent sequence of the order r *w*ith the initial values $\mathbf{Y} = (y(0), ..., y(r-1))$. The recurrence (4) of the maximal possible period $N = q^r - 1$ is called an *m*-sequence. Elementary properties of the *m*-sequence are stated in the following Lemma.

Lemma 1 Let the recurrence (4) with non-zero initial values $\mathbf{Y}_0$ be an *m*-sequence, then

0. if the n runs the full period of the sequence (4), that is equal $N = q^r - 1$, then among the generated elements any element $0 \neq a \in \mathbf{F}_q$ will occur q^{r-1} times, and the zero element $0 \in \mathbf{F}_q$ will occur $q^{r-1} - 1$ times;
1. in the entire period of the "caterpillar" (6) of the recurrent sequence (4) every non-zero *r*-component vector from the space $\left(\mathbf{F}_q\right)^r$ occurs only once.

Canonical number systems (CNS) in quadratic fields.

Let $\mathbf{Q}(\sqrt{d}) = \{z = a + b\sqrt{d};\ a, b \in \mathbf{Q}\}$ be a quadratic $\mathbf{Q}$ extension field, d be a square-free integer number. Note that if $d > 0$, the quadratic field is called real; if $d < 0$, it is called imaginary. If the trace $\mathbf{Tr}(z) = \left(a + b\sqrt{d}\right) + \left(a - b\sqrt{d}\right) = 2a \in \mathbf{Z}$ and the norm $\mathbf{Norm}(z) = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2 \in \mathbf{Z}$ of the element $z = a + b\sqrt{d} \in \mathbf{Q}(\sqrt{d})$ are integer, then the element z is called the algebraic integer in $\mathbf{Q}(\sqrt{d})$. Denote by $\mathbf{S}\left(\sqrt{d}\right)$ the subring of the integers from $\mathbf{Q}(\sqrt{d})$.

Definition 2. The algebraic integer $\alpha = A + B\sqrt{d}$ is called *the base of the canonical number system* in the ring of integers from the field $\mathbf{Q}(\sqrt{d})$, if every integer z in $\mathbf{Q}(\sqrt{d})$ can be uniquely represented in a form of the finite sum

$$z = \sum_{j=0}^{k(z)} z_j \alpha^j, \ z_j \in \mathsf{N} = \left\{0, 1, ..., \left| \ \mathbf{Norm}\left(\alpha\right) \ \right| - 1\right\}.$$

The pair $\{\alpha, \mathsf{N}\}$ is called *the canonical number system* (CNS) in the ring $\mathbf{S}(\sqrt{d})$ of integers from $\mathbf{Q}(\sqrt{d})$. Below there are several examples of canonical number systems.

1. Let $\mathbf{Norm}(\alpha) = 2$, then there exist only three imaginary quadratic fields with the rings of integers where binary canonical number systems exist, namely:

(a) the field $\mathbf{Q}(i)$ with the base $\alpha = -1 \pm i$; (b) the field $\mathbf{Q}(i\sqrt{7})$ with the base $\alpha = (-1 \pm i\sqrt{7})/2$; (c) the field $\mathbf{Q}(i\sqrt{2})$ with the base $\alpha = \pm i\sqrt{2}$.

2. Let $\mathbf{Norm}(\alpha) = 3$, then there exist only three imaginary quadratic fields with the rings of integers where exist ternary canonical number systems, namely:
(a) the field $\mathbf{Q}(i\sqrt{2})$ with the bases $\alpha = -1 \pm i\sqrt{2}$; (b) the field $\mathbf{Q}(i\sqrt{3})$ with the base $\alpha = (-3 \pm i\sqrt{3})/2$; (c) the field $\mathbf{Q}(i\sqrt{11})$ with the base $\alpha = \left(-1 \pm i\sqrt{11}\right)/2$.

3 M-transforms

In [1] the orthogonal *M*-transform (1) was introduced. The *M*-transform basis functions $h_m(n)$ are 'very similar' to random noise. Particularly, the functions $h_m(n)$ are randomly equal to one of two values, and the relative frequencies of these values are almost equal. In the paper [1] construction of the set of the basis functions was grounded on use of the *m*-sequence (3) for $p = 2$. For prime $p = 2$ the basis functions of this transform may be constructed using the following scheme.

- In the process of the functions $h_0(n)$ construction, the $y(n)$ sequence elements are replaced with the real numbers

$$\varphi : y(n) \mapsto h_0(n) = \begin{cases} A, & \text{if } y(n) = 1 \in \mathbf{F}_2; \\ B, & \text{if } y(n) = 0 \in \mathbf{F}_2. \end{cases} \tag{7}$$

- The functions $h_m(n)$ may be obtained from the function $h_0(n)$ applying the circular shift of the argument

$$h_m(n) = h_0(m+n);\ m = 0,1,\ldots,N-1;\ N = \left(2^r - 1\right). \tag{8}$$

- The numbers *A* and *B* are selected so that for the functions $\{h_m(n)\}$ the condition on the function orthogonality (2) is satisfied.

The essential technical obstacle is the difficulty to obtain the relations from where *A* и *B* may be easily determined. The following theorem generalizes the results of the paper [6].

Theorem 1. Let $q = p^s$, where p is prime, $N = q^r - 1$, the numbers $A_0, \ldots, A_{q-1}$ are such that $A_k = k\lambda + A_0$, $\lambda = (q-1)^{-1}\left(A_{q-1} - A_0\right), (k = 0,\ldots,q-1)$. Let the functions $h_m(n)$ be given by $h_0(n) = A_k$, if $y(n) = k$; $h_m(n) = h_0(m+n)$. Then there exist efficiently computable constants A_0 and λ, such that

(a) the set of functions $\{h_m(n); m,n = 0,1,\ldots,N-1\}$ forms an orthonormal basis;

(b) the constants $A = A_0$ and λ are the solution of the following system of equations

$$\begin{cases} N == A^2\left(\dfrac{N+1}{q}-1\right)+\left(\dfrac{N+1}{q}\right)\displaystyle\sum_{k=1}^{q-1}\left(A+\lambda k\right)^2, \\ 0=\displaystyle\sum_{i=0}^{q-1}\sum_{j=0}^{q-1}(A+Ci)(A+Cj)S_{ij}(\tau); \end{cases}$$

$$S_{ij}(\tau) == \begin{cases} q^{r-2}-1, & \text{if} \quad (i,j)=(0,0); \\ q^{r-2}, & \text{if} \quad (i,j)\neq(0,0). \end{cases}$$

4 The Synthesis of M-transform Basis Functions

For application of the introduced *M*-transforms to the steganography tasks it is required to represent the two-dimensional array of pixels in 1D form.

Let $N = q^r - 1 = q^{2\rho} - 1$. We assume that values of the brightness function of the digital image are elements from the following set

$$\Delta_N = \left\{\left(n_1, n_2\right) \in \mathbf{Z}^2 : 0 \le n_1, n_2 \le q^r - 1; \left(n_1, n_2\right) \neq \left(0,0\right)\right\}$$

Applying the theory of canonical number system it is possible (using the following algorithm) to construct the numeration of the elements (points) of the set Δ_N and to calculate the values of basis functions $\left\{h_m(n)\right\}$.

Numeration algorithm.

Step 1. Let $z = a + b\sqrt{d} = \mathbf{Rat}(z) + \sqrt{d}\,\mathbf{Irr}(z) \in \mathbf{S}\left(\sqrt{d}\right)$. Consider the map $(*) : \mathbf{S}\left(\sqrt{d}\right) \to \mathbf{Z}^2$, where

$$(*) : z \mapsto z^* = \left(n_1(z), n_2(z)\right) = \begin{cases} \left(\mathbf{Rat}(z), \mathbf{Irr}(z)\right), & \text{if } d \equiv 2,3 \left(\operatorname{mod} 4\right); \\ \left(2\mathbf{Rat}(z), 2\mathbf{Irr}(z)\right), & \text{if } d \equiv 1 \left(\operatorname{mod} 4\right). \end{cases} \tag{9}$$

Step 2. Let in $\mathbf{S}\left(\sqrt{d}\right)$ exist the *q*-nary CNS with the base α. Consider the *m*-sequence (4) of the degree $r = 2\rho$ (and the period $N = p^{2\rho} - 1$) and the 'caterpillar' (6).

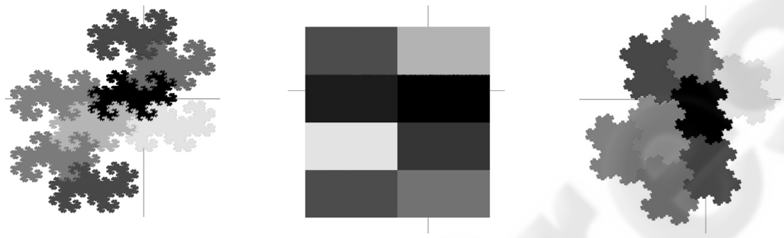
Step 3. Using the 'caterpillar' sequence (6), we can construct the following sequence

$$z(k) = y(k)\alpha^0 + y(k+1)\alpha^1 + \ldots + y(k+r-1)\alpha^{r-1}. \tag{10}$$

of elements from the ring $\mathbf{S}\left(\sqrt{d}\right)$. Denote by Ω the set $\Omega = \left\{z(k); k = 0,1,\ldots N-1\right\} \subset \mathbf{S}\left(\sqrt{d}\right)$. The elements of the sequence $z^*(k) \in \mathbf{Z}^2$, that is given by (8) will form a certain 'fundamental domain' Ω^* in the lattice $\mathbf{Z}^2$.

Step 4. Consider the equality $\Omega+\alpha^r\mathbf{S}\left(\sqrt{d}\right)=\left\{z+\alpha^r v : z\in\Omega,\ v\in\mathbf{S}\left(\sqrt{d}\right)\right\}=\Omega+\Sigma$. It may be easily verified that for the map of sets inducted by the map (8), the following relation holds $\left(\Omega+\alpha^r\mathbf{S}\left(\sqrt{d}\right)\right)^*=\mathbf{Z}^2\setminus\left(\alpha^r\mathbf{S}\left(\sqrt{d}\right)\right)^*=\mathbf{Z}^2\setminus\Sigma^*$. In other words, the additive shifts of the domain Ω^* cover 'almost' all the points of the discrete lattice $\mathbf{Z}^2$, with the exception for the points that belong to the set Σ^*.

Step 5. We say that the points $z^*=\left(z_1,z_2\right), w^*=\left(w_1,w_2\right)\in\mathbf{Z}^2$ are congruent $\left(\bmod\,\Sigma\right)$, if for their prototypes given by (8) the following relation holds: $z-w\in\Sigma$. It can be shown that every point $w^*=\left(w_1,w_2\right)\in\Delta_N$ is congruent $\left(\bmod\,\Sigma\right)$ to some point $z^*=\left(z_1,z_2\right)\in\Omega^*$ of the fundamental domain. In their turn, for the points from the fundamental domain Ω^* there exists a one-to-one map to the elements of the set Ω that are numerated using (9).



Ring $\mathbf{S}(i)$ Ring $\mathbf{S}(i\sqrt{2})$ Ring $\mathbf{S}(i\sqrt{7})$

Fig. 4. Fundamental domains Ω, associated with the binary CNS in $\mathbf{S}(i\sqrt{d})$.

Step 6. Therefore, summarizing the above-stated facts, a new numeration of the points from the set Δ_N may be obtained:

$$
\begin{gathered}
w^*\in\Delta_N\xrightarrow{(\bmod\,\Sigma)}z^*=\left(z_1,z_2\right)\in\Omega^*\xrightarrow{(Eq.(8))}\\
\xrightarrow{(Eq.(8))}z=z\left(n\right)\xrightarrow{(Eq.(9))}n\in\mathbf{Z}.
\end{gathered}
\tag{11}
$$

The above-constructed functions $h_m(n)$ generate the basis functions $H_m(\nu_1,\nu_2)$, that are defined in the two-dimensional domain Δ_N. In fact, consider, for example, $h\left(n\right)=h_0\left(n\right)$. Similar to (10), we obtain:

$$
\begin{gathered}
n\xrightarrow{(Eq.(9))}z(n)\leftrightarrow\left(\mathbf{Rat}\ z(n),\mathbf{Irr}\ z(k)\right)\xrightarrow{(Eq.(12))}\\
\xrightarrow{(Eq.(12))}(n_1,n_2)\in\Omega^*\xrightarrow{(\bmod\,\Sigma)}(\nu_1,\nu_2)\in\Delta_N
\end{gathered}
$$

and the assume that $h_0(n)=H_0(\nu_1,\nu_2)$. The examples of these basis functions are provided in the Fig.5.

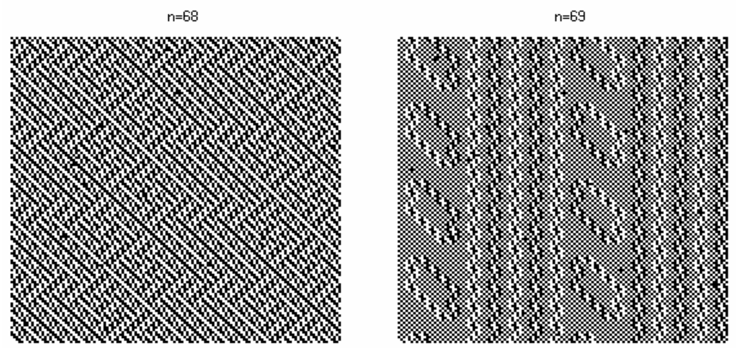


Fig. 5. *M*-transform basis functions, $d = 1$

5 The Results of the Experiments

In the Figs 1-3 the typical experimental results are displayed. Into the container 'Lena' image (256x256 pixels, Fig. 1) using the relation (1) we embedded the same secret data using three different discrete orthogonal transforms:

- two-dimensional discrete Hartley transform;
- two-dimensional discrete Hadamard transform;
- *M*-transform in the version, described in this work.

In the array of the container image spectrum about 20% of spectral components were changed. In the Figs.2, the "structured" nature of the decoding error is noticeable. For the images in the Figs. 3 and 8, the decoding error is similar to the random 'non-structured noise'. The images in these figures were obtained using the *M*-transform instead of classical orthogonal transforms.

The structure of the distortion, that is revealed in the decoded image when certain subset of the M-transform spectral components $\hat{x}(m)$ are "lost"/"modified", this structure becomes more clear, if certain probabilistic interpretation is used (the authors do not claim the absolute mathematically correctness of this interpretation).

Let the basis functions $h_m(n)$ be interpreted as random variables. These random values are not correlated as the transform has its orthogonality property. For the input signal $x(n)$ and for the distorted signal $x^*(n)$ the following relations hold

$$x^*(n) = x(n) + \sum_{\tau \in T} \hat{x}(\tau) h_\tau(n) = x(n) + \xi(n,T),$$

where T is a set of the indices corresponding to the lost spectral components. The random value $\xi(n,T)$ is linear combination of the random values (the values that has the same distribution) and therefore for practical tasks $\xi(n,T)$ may be interpreted as a Gaussian noise with the parameters that may be easily calculated.

Fig. 6. Error-field for discrete Hartley transform.

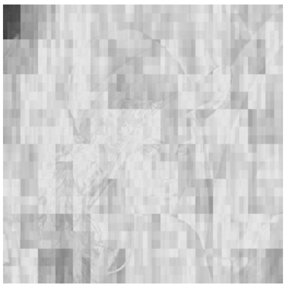


Fig. 7. Error-field for discrete Hadamard transform.

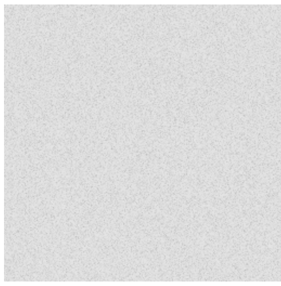


Fig. 8. Error-field for discrete *M*-transform.

In the figures 9-11 the autocorrelation functions (autocorrelation of the field of errors for the used transform) is displayed.

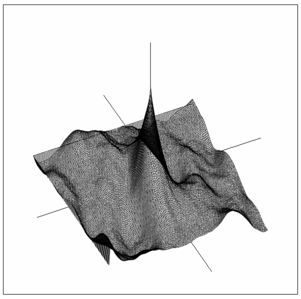


Fig. 9. Autocorrelation function of the field of errors for Hartley transform.

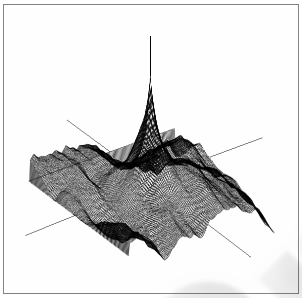


Fig. 10. Autocorrelation function of the field of errors for Hadamard transform.

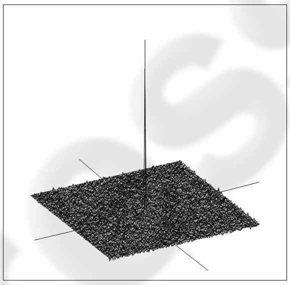


Fig. 11. Autocorrelation function of the field of errors for M-transform .

6 Conclusion

The major contributions of this article arise from development of the mathematical fundamentals for application of canonical number systems and discrete orthogonal transforms to the tasks of steganography. The proposed approach is based on a new mathematical technique, namely on the theory of canonical number systems that so far has not been applied to this tasks of digital signal processing. The empirical and theoretical results are provided that if the proposed transform is used for embedding the secrete data, then to the container image additive random noise is added, that is much less perceptible than 'regular', 'structured' noise typical for classical discrete orthogonal transforms.

Acknowledgements

This research was financially supported by the RF Ministry of Education and U.S. Civilian Research & Development Foundation (CRDF Project SA-014-02) as part of the joint Russian-American program "Basic Research and Higher Education" (BRHE), and by Russian Foundation for Basic Research (Project # 06-01-00722)

References

1. Nikolaidis N., Pitas I. Robust image watermarking in the spatial domain. Signal Processing, Special Issue on Copyright Protection and Control. 1998. Vol. 66. № 3. P. 385-403.
2. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for Data Hiding. IBM Systems Journal. 1996. Vol. 35.
3. Marvel L., Boncelet C., Retter J. Reliable Blind Information Hiding for Images. Proceedings of 2nd Workshop on Information Hiding. Lecture Notes in Computer Science. 1998.
4. R. Chandramouli, A mathematical framework for active steganalysis, ACM/Springer Multimedia Systems Special Issue on Multimedia Watermarking, vol. 9, pp. 303—311
5. J. Fridrich and M. Goljan, Practical Steganalysis of Digital Images -- State of the Art", Security and Watermarking of Multimedia Contents, vol. SPIE-4675, pp. 1-13, 2002
6. H.-J. Grallert, Application of orthonormalized m-sequences for data reduced and error protected transmission of pictures, In Proc. IEEE Int Symp. on Electromagnetic Compability, 1980,Baltimore, MD, pp.282-287..
7. H.-J. Grallert, Source encoding and error protected transmission of pictures with help of orthonormalized m-sequences. In Proc.12th Int. Television Symp., Montreux, Switzerland, 1981, 441-454.
8. W.G.Keesen, U.Riemann, H.-J. Grallert, Codierung von Farbensehsignalen mittels modifizierten M-Transformmationen fuer die Uebertragung ueber 34-Mbit/s-Kanaele. Frequenz, vol. 38, No10, 238-243, 1984 (in German)
9. H. G. Musmann, P.Pirsch, H.J. Grallert, Advances in picture coding, IEEE Proc., 1985, vol.73, No 4, pp.523-548.
10 A.G.Dmitryev, V.M.Chernov Two-dimensional Discrete Orthogonal Transforms with the "Noise-like" Basis Functions. In Proc. Int. Conf. GraphiCon 2000. pp.36-41
11. A.G.Dmitriev, V.M.Chernov. Generating Pseudo-stochastic Basis Function for Discrete Orthogonal Transforms. Pattern Recognition and Image Analysis. V.11, No1, 2001..155-157.
12. G.Birkhoff, T.C.Bartee, Modern Applied Algebra, McGraw-Hill, NY, 1970.
13. R.Lidl, H.Niederreiter. Finite Fields, Reading, Mass., 1983
14. Katai I., Kovacs B. Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen, Acta Sci.Math.(Szeged) 42, 1980, pp. 99–107.
15. Kátai I., Kovács B. Canonical Number Systems in Imaginary Quadratic Fields, Acta Math. Acad. Sci. Hungaricae, v.37, 1981, pp.159-164.