METHODS OF QR CODE TRANSMISSION IN COMPUTER STEGANOGRAPHY

Vakulenko, Sergey P., *Russian University of Transport, Moscow, Russia.*
Volosova, Natalya K., *Bauman Moscow State Technical University, Moscow, Russia.*
Pastukhov, Dmitry F., *Polotsk State University, Novopolotsk, Belarus.*

ABSTRACT

The article deals with the problems of using steganography methods for transmitting data. The authors justify their approach by arguing that the importance of cryptography in terms of transfer of hidden data is obvious, however, being cryptographic, coded information maintains potential threat with the mere existence of an encrypted message, that is, an indication that it is necessary to apply cryptanalysis. With the help of steganography, mathematical methods are constructed that deprive the carrier of the potential threat of these prompts. The article proposes to transmit data encoded into a QR code, pre-masking it. In particular, for reliability of restoring the «original», it is proposed to solve the same problem by different methods through iteration using linear systems, the Radon transform, the boundary problem for the Poisson equation, and beyond this, methods based on probability theory. The advantages of this option include the possibility of using modern computer tools and software developed in the field of various types of tomography and in mathematical physics, while slightly modifying them.

Keywords: cryptography, steganography, quick response code, information security, Radon transform, Poisson equation, iterative methods.

Background. *The importance of cryptography in terms of transfer of hidden data is obvious. However, being cryptographic, it leaves the carrier of the potential threat with the mere existence of an encrypted message, that is, an indication that it is necessary to subject cryptanalysis. With the help of steganography, mathematical methods are constructed that deprive the carrier of the potential threat of these prompts. The goal is to place such a secret text in an apparently innocuous message, when there is no suspicion about hidden information. With regard to transport, for example, it is necessary to hide when and where dangerous or especially valuable goods will be transported, time and place of their storage, etc. It is necessary to make so that the information was transmitted completely unnoticed by the general mass of people with access to networks.*

In the article [1], an iterative algorithm of the inverse Radon transform is implemented using a specific example in the presence of random noise and systematic errors and malfunctions of the detectors. It is explained that the integral transformation of the function g (x, y) ideally (without noise) has the property of consistency, which imposes a certain restriction on the projections f (ξ, p) measured in different directions of the angle ξ (this function is called a synogram in tomography theory). In a rigorous formulation, the conditions of compatibility express the connection between one-dimensional moments of projections and two-dimensional moments of images. In real experimental measurements, the compatibility property is violated. Such a violation manifests itself in a large value of the residual norm; in a significant difference between the projection data and the pseudo-projections obtained by the Radon transform from the reconstructed tomograms. Taking into account the condition of compatibility of projections allows us to obtain a more accurate solution of the inverse problem.

Objective. *The objective of the authors is to consider methods of QR code transmission in computer steganography.*

Methods. *The authors use general scientific and engineering methods, comparative analysis, evaluation approach, graph construction, mathematical and computer programing methods.*

Results.

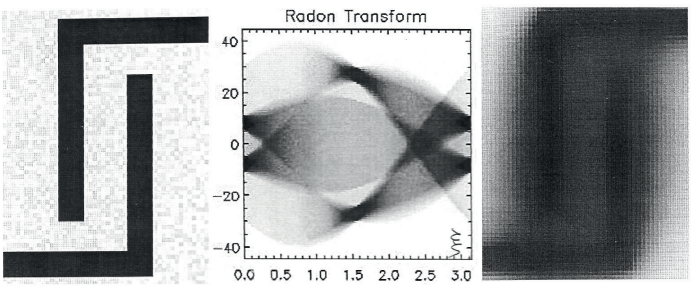
Using the Radon transform

In the work [2] it is proposed to use similar methods in another area of application – steganography. It is assumed that someone (NK) wants to send the information to the addressee (A) secretly from an outside observer encoded in a QR code.

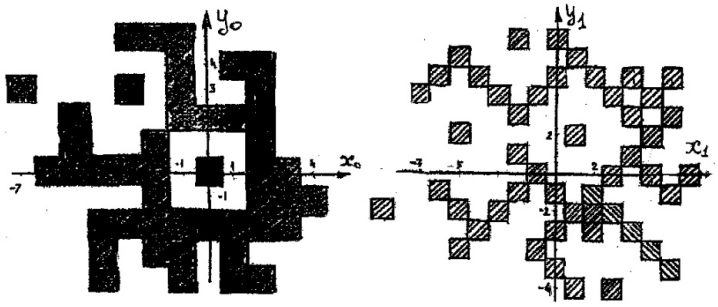
We set the function of two variables:

$$\varphi(x,y)=\begin{cases}1, & if\ (x,y)\in\Omega,\\ 0, & if\ (x,y)\notin\Omega\end{cases}, \qquad (1)$$

where Ω denotes the set of black squares in Pic. 1a, and the whole area of Pic. 1a can be represented as



Pic. 1: a) the simplest example of a fragment of a QR code; b) Radon transform; c) to the object of Pic. 1b, a 10 % model noise is placed, uniformly distributed, and then the inverse Radon transform is performed. After applying the noise cleaning program, an object is obtained that coincides with Pic. 1a to 99 %.



Pic. 2. Fragment of a QR code.
On the right is the first iteration using linear systems; a = 1, b = –1, c = 1, d = 1, e = 1, f = 2.

the union of some set of identical black and white elementary squares. The masked image is the transformed QR code, it contains the transmitted information.

Here, d_1 = 12 pixels denotes the angle thickness, and $d_2 = 1{,}7d_1$ pixels indicates the width of the gap between the corners. Grid 64 x 64 and 100 angles selected.

Then, the well-known «watermark» technology [6] is used, and a suitable, pre-specified container is transferred to «A», which has a «VO» restoration program.

We divide the entire field and the given QR code into identical elementary white and black squares (rectangles) and calculate their centers of gravity (this is the intersection point of the diagonals). We calculate the function (1).

In the work [2] some methods of preliminary masking and complication of the message were proposed. In this case, it is proposed to use another method for this purpose, namely the method used in the theory of fractals: «iteration by linear systems».

Let's organize an iterative process $x_{k+1} = e + ax_k + by_k$, $y_{k+1} = f + cx_k + dy_k$, where k = 0, 1, ... – iteration number, x_k, y_k – coordinates of the center of gravity of the elementary black squares constituting the QR code in the Cartesian coordinate system, not k-iterations. The origin, the point (0, 0) on Ω, the scale and direction of the axes relative to the graph are known only to NK and are associated with a given QR code. The same applies to the given real constants {e, a, b, f, c, d} and the selected number of iterations k. Thus, additional keys appear. Note that the structure and geometry at each iteration changes significantly, but there is a unique inverse transformation that allows to restore the original initial condition – a QR code using the formulas:

$$x_k = -(b\,f - d\,e + d\;\; x_{k+1} - b\,y_{k+1})\,/\,Dn,$$
$$y_k = -(c\,e - a\,f - c\,x_{k+1} + a\,y_{k+1})\,/\,Dn,$$
$$Dn = b\,c - a\,d \neq 0. \qquad (2)$$

We present briefly the applied algorithm [2, 3].

Remark 1. *It is proposed to construct two programs in parallel. Program 1 describes the procedure for calculating the Radon transform for the family of QR codes and calculates or specifies all the keys (necessary values of constants).*

The second program restores the original image with noise, with a probability of occurring during separation from the stegcontainer. For reliability of restoration of the «original», i.e. calculating the centers of gravity of the elementary squares that make up «O», it is proposed to solve the same problem using different methods, using iterations using linear systems, the Radon transform and the boundary problem for the Poisson equation, and then including methods for selecting the center of gravity of elementary squares based on probability theory.

In the model version in this paper three objects are considered: the original «O»: the image obtained after the integral transformation «I»: the restored original «VO». In this case, «VO» differs from «O» by an error arising due to noise and the solution of the inverse ill-posed problem.

Denoted in the two-dimensional formulation by g(x, y) the unknown function is to be defined as «VO»; through f(ξ, p) – «I», the integrals of this function along the family of parallel lines extending at an angle ξ to the OX axis: «impact parameter» p is the distance from the ray from the family of lines to the origin (with a sign). The connection between the function f(ξ, p) «I» with the function g(x, y) «O» was established by I. Radon in 1917 as a Fourier transform written in the polar coordinate system. Radon transform becomes a method for solving the inverse problem of integral geometry, the essence of which is in restoring (reconstructing) multidimensional functions according to their integral «I» characteristics. A special case of the transformation used in [2] is:

$$\mathrm{f}(\xi, \mathrm{p}) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x, y)\,\delta(\mathrm{p} + \mathrm{x}\sin\xi - \mathrm{y}\cos\xi)\,dx\,dy. \qquad (3)$$

However, this method was not widely used until the first tomograph appeared in 1972. Mastering tomography has led to progress in medicine, diagnosis of diseases, crystallography, the study of the structure of molecules, in geophysics, astrophysics, etc. Now steganography is added to this list [1, 6].

Let's denote by

$$W = \left\{ x_{ij}, y_{ij}, i = 1,\ldots,n,\ \mathrm{j} = 1,\ldots,m \right\}$$

the set of centers of gravity of white and black elementary squares in the domain Ω. Separately, we single out the set V of pairs of indices (ð, ν) of the centers of gravity of only black elementary squares (rectangles) in the region.

Remark 2. *In the known calculations, the coordinates of the centers of gravity of the elementary squares were specified in the programs manually. This explains the fact that calculations were made for a particular fragment and its two iterations (Pic. 2). V. V. Pikalov, in correspondence with the authors, expressed his opinion that the most complex and cumbersome unresolved part of the proposed complex of algorithms is a program for automatically*

determining the centers of gravity of elementary squares for each next representative from the family of QR codes.

Note that a library of synograms for models composed, in particular, of rectangles in Mathlab and Python (a shell with the Anaconda interpreter), is available in [15]. Difficulties may arise when restoring «I» with a lot of noise, distributed according to an unknown law (see Remark 1).

We emphasize that for the same purpose, it is promising to use a weighted Fourier transform (weighted Radon transform) [7]. The weight function in this transformation is also an additional «key» preventing unauthorized reconstruction of «VO».

Definition. *The masking function is called the function $\chi(x, y)$, which sets the coordinates of the centers of gravity of the new black squares that did not previously exist in the given QR code and complement the set in Ω.*

Inclusion of a boundary value problem for the Poisson equation

Instead of the Radon transform, the solution of the Dirichlet boundary value problem for the Poisson equation proposed in [3] is possible. Interest in problems in areas of complex shape exists in various applications [16].

Remark 3. *The solution of the Dirichlet boundary value problem for the Poisson equation in a rectangle using the Green function and the Fourier series method is known to be written. In practice, in order to achieve the required accuracy of calculations, it is necessary to sum more than one hundred members of an oscillating series with slowly decreasing coefficients. We also have to calculate the integrals of such sums.*

Another direction of research of this problem, from the point of view of the authors, lies in development of the approaches outlined in [4].

In our case, we will show how this algorithm can be implemented.

Above it was proposed to break the entire field and the given QR code into white and black elementary squares and calculate their centers of gravity. That is, using formula (1), we construct a function of two variables $\phi(x, y)$.

Step 1. *There are two options here.*

In the first case, *we choose a two-step grid pattern, necessary for difference approximation of the boundary value problem. Most often, the quadrangle of the minimum area, covering all the shaded elementary squares that make up the QR code, turns out to be a rectangle.*

Set for definiteness:

$$x \in [x_{\min}, x_{\max}],\ y \in [y_{\min}, y_{\max}],$$
$$x_{\max} > 0,\ y_{\max} > 0,\ x_{\min} < 0,\ y_{\min} < 0.$$

Denote by $m_1 = |x_{\max}| + |x_{\min}|$, $m_2 = |y_{\min}| + |y_{\max}|$. If it is a square, then go to the second case with one constant step. To obtain a square non-degenerate matrix after the difference approximation of the boundary problem, we use the masking function $\chi(x, y)$, adding elementary black squares to the QR code, achieving the absence of linearly dependent rows and columns in the matrix, which certainly ensures the nondegeneracy of the transformation (2). Naturally, the coordinates of the centers of gravity of such elementary squares are written in programs 1 and 2 into some arrays, similar to those mentioned in remark 1. The entire area is divided into elementary rectangles by a two-dimensional grid. We introduce a two-dimensional uniform grid:

$$\omega_{n_1 n_2} = \left\{ \begin{array}{l} x_m = x_{\min} + m h_1,\ y_m = y_{\min} + n h_2, \\ m = \overline{0, n_1},\ n = \overline{0, n_2},\ h_1 = \dfrac{x_{\max} - x_{\min}}{n_1}, \\ h_2 = \dfrac{y_{\max} - y_{\min}}{n_2} \end{array} \right\}. \quad (4)$$

Note also that the lengths of the sides of an elementary black (white) rectangle designated in the program as h_{11}, h_{22}, are multiples of the grid steps h_1, h_2, and the axes of the x, y coordinate system in the graphs constructed by the program have identifiers X, Y respectively (Pic. 3).

Step 2. *The function specified in (1) has a discontinuity. We introduce the function $f(x, y) = \phi(x, y) + \chi(x, y)$, continuously differentiable using the sum of two-dimensional Gaussians:*

$$f(x,y) = \left\{ \begin{array}{l} \sum\limits_{(\delta,\nu)\in V} e^{-\left(\frac{x-x_\delta}{h_1 0{,}5}\right)^2 - \left(\frac{y-y_\nu}{h_2 0{,}5}\right)^2}, (\delta,\nu) \in V, (x_\delta, y_\nu) \in W. \\ 0. \end{array} \right. \quad (5)$$

Center of squares x_i, y_j are determined by formula (4), and where the coefficients ($h_{11} \cdot 0{,}5$; $h_{22} \cdot 0{,}5$ are half sides of the elementary rectangle) locally control the variance of the Gaussian distribution; (x_i, y_j) are the centers of black squares on a uniform coordinate grid.

Note that in the design program, an array of indicator amplitude function

$$F_{ij} = \begin{cases} 1, (i,j) \in N_1^2 \equiv W_{i,j} \\ 0, (i,j) \in N_2^2 \end{cases}$$

is stored, which is used for technical, auxiliary purposes. Here N_1^2 is a two-dimensional integer set of nodes-centers of black squares corresponding to a set V, N_2^2 is a two-dimensional integer set of nodes-centers of white squares

$$N_1^2 \cup N_2^2 = \left\{(i,j) \in i = \overline{0, n_1},\ j = \overline{0, n_2}\right\}.$$

Constants in terms of exponential functions that determine variance may not be uniquely defined.

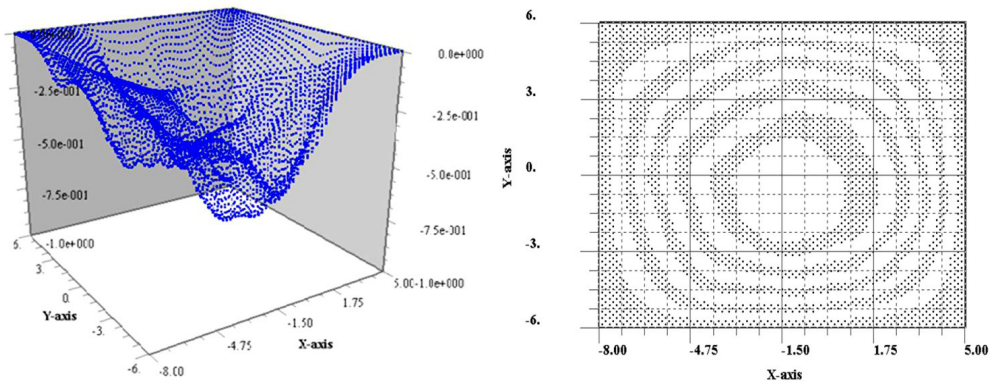
We write the two-dimensional Poisson equation in a rectangle $0 < x < |aa| + bb,\ 0 < y < |cc| + dd$ with zero boundary conditions:

$$u(0, y) = 0,\ u(a, y) = 0,\ u(x, 0) = 0,$$
$$u(x, b) = 0,\ \Delta u(x, y) = f(x, y), \quad (6)$$

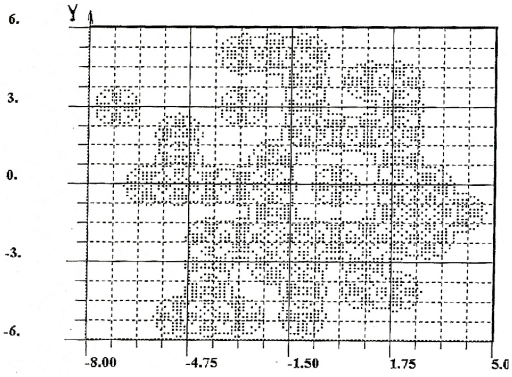
where by $\Delta = \dfrac{\partial^2}{\partial x^2} + \dfrac{\partial^2}{\partial y^2}$ the Laplace operator is denoted.

For the simplicity of approximation of the problem in this example, we choose the simplest five point pattern of the difference scheme «cross» and obtain the difference equation for two different steps in directions on the grid (4), which is given in many papers, for example, in [4], [8, 9, 11, 12]. In [13], the well-proven method of upper relaxation was put into practice. In English literature, it is called Successive QverRelaxation (SOR) method. For brevity, we write it in the case of a uniform grid with a step h:

$$u_{m-1,n}^{k+1} - \frac{4}{\omega} u_{m,n}^{k+1} + u_{m,n-1}^{k+1} =$$
$$= -(u_{m+1,n}^{k} + u_{m,n+1}^{k}) + 4(1 - 1/\omega)\, u_{m,n}^{k} - h^2 f_{m,n}. \quad (7)$$



Pic. 3. The solution of problem (6) in isometry corresponds to the QR code shown in the left fragment of Pic. 2. $n_1 = 104$, $n_2 = 96$, aa = –8, bb = 5, cc = –6, dd = 6 and level lines. The number of iterations k = 2000.



Pic. 4. Grid nodal points falling on a fragment of a QR code.

To implement this method, knowledge of the spectrum of problems is not required, and the optimal value of the parameter ω is determined in the course of a numerical experiment. The authors of [4] proposed to generalize the method and repeatedly tested it on problems in which the right-hand side is an analytic function and compared the results with the data from [8, 11, 12].

In the course of solving the problem (6), we build an iterative process with the iteration number k, using the analogy with method (7) and the method of alternating directions [4, 8, 9, 11, 12]. For concreteness, we present an iterative formula in one of the directions on the grid (4):

$$\frac{h_2^2}{2(h_1^2+h_2^2)}u_{m-1,n}^{k+1} - u_{m,n}^{k+1} + \frac{h_2^2}{2(h_1^2+h_2^2)}u_{m+1,n}^{k+1} = \\ = \frac{-h_1^2}{2(h_1^2+h_2^2)}(u_{m,n-1}^{k} + u_{m,n+1}^{k}) + f_{m,n}\frac{h_1^2h_2^2}{2(h_1^2+h_2^2)} + O(h_1^2h_2^2). \quad (8)$$

Here $f_{m,n}$ denotes the difference approximation of the smoothed formula (5). It is obvious that at each iteration we have a three-diagonal matrix and, therefore, we can use the formulas of the algorithmic Gauss method, or the formulas of the right sweep. In fact, the well-known stability condition of this method is satisfied. It lies in the fact that the fulfillment of the inequality «the diagonal dominance of the matrix elements over the sum of the modules of the non-diagonal elements» [9] is ensured. The error of the solution is indicated in formula (8).

Further, the text file for solving the problem (6) can be used in the technology of embedded «watermarks» [6]. A suitable, previously agreed stegocontainer is transferred to «A» with the «VO» recovery program.

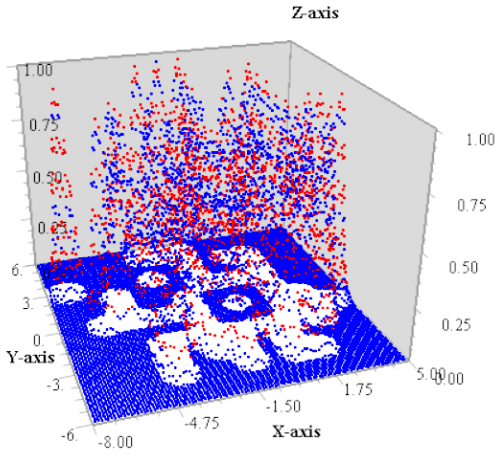
The inverse transformation is performed by finding the local maxima and minima of the Laplacian. The points of the centers of gravity of elementary black squares are calculated, and then the squares themselves are restored by «hands in the program».

In [4, 8, 11], methods for solving problem (6) with increased accuracy were developed.

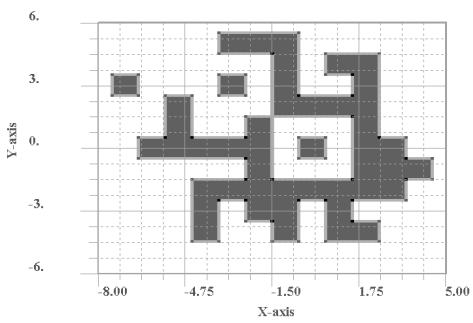
In particular, a 9-point cross pattern was considered there and iterative formulas were constructed. The proof of sufficient stability conditions $\lambda_s < 1$, and the proof of convergence of the iterative process by the principle of contraction mappings [10] are given. The programs on the modern version of the Fortran language [12], supporting maximum arrays for the solution function (8) and the Chebyshev calculating norm of the discrepancy between the difference solution and the projection of the exact solution onto the grid were compiled.

The second case with one grid step. *With the help of the masking function χ(x, y) we supplement the QR code to a large square, that is, we achieve that the obtained matrix of the function f(x, y) = ϕ(x, y) + χ(x, y), containing units, was square and nondegenerate (see formulas (1), (5)). If a given QR code contains duplicate rows or columns of squares (linearly dependent), then using the masking function, you can add a certain minimum number of shaded squares to the QR code and normalize the situation. Of course, the coordinates of the centers of gravity of the introduced new squares with the help of the function χ(x, y) must be memorized in programs 1 and 2 (see remark 2). Further, in the formulas given earlier, the grid steps should be set equal to h. Then follow the algorithm described in the first case.*

Conclusions. *There are options for hiding information in the new direction of development of steganography, which provide a fan of possibilities for applying various mathematical results from other areas of applications. The reliability of the results is confirmed by the rigor of mathematical constructions in the works mentioned, their many years of practical application, including tomography of various types in medicine, tomography in plasma physics, in the theory and methodology of pattern recognition, inverse scattering methods, in mathematical physics, electro- and magnetostatics, hydrodynamics etc. The method*



Pic. 5. Isometry of difference approximation of function (5).



Pic. 6. m = 2000, n_1 = 104, n_2 = 96, m_1 = 13, m_2 = 12, a = –8, b = 5, c = –6, d = 6, n = max (n_1, n_2). In the center of the point of each local maximum of the Laplace operator, the «hands in the program» are restored, an elementary black square is constructed with sides parallel to the coordinate axes, i.e. the right smooth part of the Laplace equation is again replaced by a discontinuous function with discontinuities of the first kind at the edges of elementary rectangles (see the beginning of the article).

has the advantage of being capable to apply tools and software, developed in above mentioned fields of applications.

REFERENCES

1. Pikalov, V. V., Kazantsev, D. I. Iterative reconstruction of a sinogram perturbation in the Radon space for steganography problems [*Iteratsionnoe cosstanovlenie vozmushcheniya sinogrammy v prostranstve Radona dlya zadach steganografii*]. *Vychislitelnie metody i programmirovanie*, 2008, Iss. 1, pp. 1–9.

2. Volosova, N. K. Use of the Radon transform in steganography [*Primenenie preobrazovaniya Radona v steganografii*]. *7I[st] international conference «Herzen readings»*. St. Petersburg, 2018, pp. 234–238.

3. Volosova, N. K. Radon transform and the Poisson equations in computer steganography [*Preobrazovanie Radona i uravneniya Puassona v komp'yuternoi steganografii*]. *International Conference on Differential Equations and Dynamical Systems*, Suzdal, 2018, p. 61.

4. Pastukhov, D. F., Pastukhov, Yu. F. Approximation of the Poisson equation on a rectangle of increased accuracy [*Approksimatsiya uravneniya Puassona na pryamougolnike povyshennoi tochnosti*]. *Vestnik of Polotsk State University. Series: Fundamental Sciences. Maths*, 2017, Iss. 12, pp. 62–77.

5. Tikhonov, A. N., Arsenin, V. Ya., Timonov, A. A. Mathematical analysis of computed tomography [*Matematicheskiy analiz komp'yuternoi tomografii*]. Moscow, Nauka publ., 1987, 160 p.

6. Shelukhin, O. I., Kanaev, S. D. Steganography. Moscow, Goryachaya liniya-Telecom publ., 2017, 592 p.

7. Novikov, R. G. Weighted ray transform and application Conference handbook and proceedings. *Quasilinear Equations, Inverse Problems and Their Applications*, MIPT, Russia, 05–07.12.2017.

8. Bakhvalov, N. S., Lapin, A. V., Chizhonkov, E. V. Numerical methods in tasks and exercises [*Chislennye metody v zadachah i uprazhneniyah*]. Moscow, Vysshaya shkolla publ., 2000, 190 p.

9. Samarsky, A. A., Vabishchevich, P. N. Numerical methods for solving inverse problems of mathematical physics: Study guide [*Chislennye metody resheniya obratnyh zadach matematicheskoi fiziki. Ucheb. posobie*]. Moscow, Izd-vo LKI, 2014, 480 p.

10. Kolmogorov, A. N., Fomin, S. V. Elements of the theory of functions and functional analysis [*Elementy teorii funktsii i funktsionalnogo analiza*]. 7[th] ed. Moscow, Fizmatlit publ., 2004, 572 p.

11. Volkov, K. N., Deryugin, Yu. N., Emelyanov, V. N. [*et al*]. Methods of accelerating gas-dynamic calculations on unstructured grids [*Metody uskoreniya gazodinamicheskih raschetov na nestrukturirovannyh setkah*]. Moscow, Fizmatlit publ., 2013, 536 p.

12. Bakhmetyev, O. V. Modern Fortran [*Sovremenniy Fortran*]. Moscow, Dialog-MEPI, 2000, 449 p.

13. Fedorenko, R. P. Relaxation method for solving difference elliptic equations [*Relaksatsionniy metod resheniya raznostnyh ellipticheskih uravnenii*]. *Zhurnal vychislitelnoi matematiki i matematicheskoi fiziki*, 1961, Iss. 5, pp. 922–927.

14. Mitskevich, M. N. Detection of image areas for embedded digital watermarks using wavelet transform [*Obnaruzhenie oblastei izobrazhenii dlya vstraivaemyh vodyanyh znakov s pomoshchyu veivlet-preobrazovaniya*]. *Voprosy zashchity informatsii*, 2015, Iss. 1, pp. 81–83.

15. Tereshchenko, S. A. Methods of computed tomography [*Metody vychislitelnoi tomografii*]. Moscow, Fizmatlit publ., 2004, 320 p.

16. Basarab, M. A., Kravchenko, V. M. Semi-analytic coordinate sequences for solving Dirichlet boundary-value problems in regions of complex shape [*Poluanaliticheskie koordinatnye posledovatelnosti dlya resheniya kraevyh zadach Dirichle v oblastyah slozhnoi formy*]. *Reports of the Russian Academy of Sciences*, 2004, Iss. 2, pp. 172–176.

Information about the authors:
Vakulenko, Sergey P. – Ph.D. (Eng), professor, director of Institute of Management and Information Technologies of Russian University of Transport, Moscow, Russia, k-gdsu@mail.ru.
Volosova, Natalya K. – Master's student of Bauman Moscow State Technical University, Moscow, Russia, navolosova@yandex.ru.
Pastukhov, Dmitry F. – Ph.D. (Physics and Mathematics), associate professor of the department of Programming technologies of Polotsk State University, Novopolotsk, Belarus, dmitrij.pastuhov@mail.ru.

Article received 05.07.2018, revised 17.10.2018, accepted 19.10.2018.