An Adaptive Algorithm for the Steganographic Embedding Information into the Discrete Fourier Transform Phase Spectrum

Oleg Evsutin, Anna Kokurina, Roman Mescheryakov
and Olga Shumskaya

Abstract On the example of digital images there are investigated properties of the discrete Fourier transform (DFT) used to embed information into the phase spectrum. The investigation helped to form a new steganografic algorithm that can be used in case of non- compressed images. Peculiarity of the algorithm is changeable size of information put into the blocks of stego-image. Characteristics of the suggested algorithm are comparable with the analog ones, they allow to get the correct information without mistakes.

Keywords Information security · Steganography · Data hiding · Digital images · Digital watermarking · Discrete Fourier transform

1 Introduction

Methods of digital steganography allows to solve wide circle of security problems by embedding different hidden information sequences into the digital objects.

According to the problems under consideration the methods could be divided into two big classes: methods meant to protect the embedding information and

---

O. Evsutin (✉) · A. Kokurina · R. Mescheryakov · O. Shumskaya
Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia
e-mail: eoo@keva.tusur.ru

A. Kokurina
e-mail: mrv@keva.tusur.ru

R. Mescheryakov
e-mail: anessa.kas@gmail.com

O. Shumskaya
e-mail: shumskaya.oo@gmail.com

A. Abraham et al. (eds.), *Proceedings of the First International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’16)*, Advances in Intelligent Systems and Computing 451, DOI 10.1007/978-3-319-33816-3_5

methods to protect the digital object used to embed the information in. In the first case, confidentiality of the information embedded is provided be transaction within digital objects, in the second the goal of embedding is authentication of the digital objects.

Further we would call any digital object stego-container not depending on the concrete application.

Digital images usually play the role of stego-containers. Such data are widely used now in the nets of general access in parallel with video- and audio-data. Still the digital images are more simple compared to the video- and audio-data [1]. To make the description shorter we would call methods and algorithms steganographic if information is embedded into digital images.

Embedding information into a digital object is done by manipulating the data elements having some redundancy. If stego-containers are used for non-compressed images it could be the natural space redundancy showing up in the proximity of the neighboring pixels. If the compressed images are used for embedding, there are changed the coefficients of frequency transform having redundancy. Important to note, that the steganographic embedding could be done also without further compression.

So, steganographic methods, as many others, could be divided into the space and the frequency ones.

LSB is one of the classic methods used to hide the confidential information in the space of digital images. Publications [2–4] provide some algorithms worked out using this method and differ by the methods to make steganographic endurance and robustness higher.

For digital images authentication there are mainly used watermarks. Examples of watermarks embedding into the digital images space are given in [5, 6]. The main goal of the investigation is to make stego-containers more resistant to geometrical distortions.

Embedding the information into the frequency area is connected with utilization of the discrete cosine transform (DCT) coefficients. An example is the widely spread method of digital images with losses compression (JPEG). Investigation base on this method and became classic is given in [7–9].

Nowadays there are being published new works meant to improve the classic ways. Among them there are attempts to minimize stego-containers distortions by optimization [10–14].

In the papers there are described algorithms to embed information into the area of the discrete wavelet transform (DWT) coefficients. In some cases optimization methods are used to improve secrecy and robustness. In [15] there was suggested steganographic algorithm based on the joint utilization of DWT and DCT.

Still there not many publications where embedding utilizes discrete Fourier transform. It concerns mainly digital images because such methods for audio data are already rather numerous [16, 17].

2 The Suggested Algorithm of Data Embedding

2.1 *Review of the Methods to Build in the Information into Digital Images Utilizing Discrete Fourier Transform*

Let's have a look at the known steganographic algorithms for embedding information into the digital images based on the discrete Fourier transform. Many of them deal with elements of amplitude Fourier spectrum.

In case of the algorithm described in [18] the space of hiding is formed of the middle frequency elements that are within a ring zone of the given width on the complex plan. In order to embed one bit of a secret message a pare of symmetric elements are changed in such a way that their difference depends on the bit.

In [19] there is described an algorithm of digital watermarks embedding. A digital watermark is formed with the help of pseudo random key sequence and looks like amplitude Fourier spectrum which elements with values of the set {–1, 1} makes a ring in the space of middle frequencies. The authors says that the property of the ring symmetry of the digital watermark provide stability in case of geometry attack like "turn of image". Embedding operation is realized by two methods—additive and multiplicative.

The same algorithm is described in [20]. The difference—the watermark looks like a circle, not a ring and operation of embedding is additive. All elements of digital watermarks are from the set {0, 1}.

In [21] a binary digital watermark having circle symmetry is formed using log-polar mapping. In the process of embedding elements of the digital image amplitude Fourier spectrum corresponding to the digital watermark 1 are recalculated by averaging within the area 3 × 3 multiplied by the amplification coefficient.

Differently from the previous publications where embedding is done into a brightness component of the color space YCbCr, in [22] is used the color space Lab and the same digital watermark is embedded into Fourier images of both chromatic components. Embedding consists of summation of amplitude spectrum elements and elements of the digital watermarks.

In [23, 24] the image is divided into blocks 2 × 2 pixels and each of them is treated by DFT. The frequency coefficient in the top left corner of the amplitude spectrum is not changed, all others are embedded in the message bits according to LSB. In [23] in addition there is used genetic algorithm to improve quality.

It is worth pointing out the paper [25] where generalization of the Fourier transform is used—fractional Fourier transform. The hidden space is formed of complex digitals coefficients of this transform. The secret message (digital watermark) is also a sequence of complex values which real and imaginary parts are normally distributed and embedded additively.

One can see two ways suggested in these papers to come to the frequency field using DFT:

1. DFT is applied to the whole image;
2. DFT is applied to small 2 × 2 pixel blocks.

Both approaches have drawbacks. In the first case utilization of the small blocks does not allow to mark out middle frequencies in the Fourier spectrum, while this part is more suitable to embed the additional information. It makes frequency domain useless. In the second case variation of every Fourier image change all the stego-container image pixels. It amplifies the embedding artifacts.

In [26] the image is split into blocks 8 × 8, part of them are used for embedding. Unfortunately it is not taken into consideration that artifacts of different blocks could differ even if the volume of information is the same.

It is necessary to point out separately that other authors don't investigate the problem of an embedded information distortion which could appear during the back transfer from the frequency area into the space one. This problem appears because after application of the back Fourier transfer to a modified Fourier image there appear real values which are rounded when the pixel matrix is formed. As a result, the formed Fourier image got after DFT application differ from the one where information was embedded. So the information could be got incorrect.

In the paper there given are results of Fourier transform steganographic properties investigation in the context of the mentioned problem. There was formed an algorithm of embedding information into the phase spectrum. The choice of the phase image is due to the fact that phases belong to the interval $[-\pi, \pi]$ and don't depend on the concrete image. So there is no need of normalizing. The paper develops the previous investigation of the authors presented in [27].

2.2 Investigation of the Discrete Fourier Transform Steganographic Properties

As an elementary steganographic operation we suggest using in this paper the turn of the radius-vector at the complex area, where we call the radius-vector the geometric interpretation of a complex spectrum separate element.

In order to solve the problem mentioned in 2.1 and connected with the frequency spectrum distortion in the process of transfer from real values to digital ones it was necessary to investigate the properties of the introduced operation.

To do this we made some calculation experiments with standard test images. These calculations meant to show the interrelation between image characteristics in space and frequency areas and properties of steganographic operation. In the paper we don't give the full description due to the lack of the space.

The calculation experiments allowed to conclude:

1. The number of bits got correctly from the stego-image before the first mistake practically does not depend on the image size. Therefore in the process of building in the image it is reasonable to split the image into the blocks of small but trivial size: from 8 × 8 to 16 × 16 pixels.
2. Uniform blocks with similar number of pixels are generally less disturbed.
3. When two radius-vectors turn by the same angle, longer vector is more stable. Therefore when the same information volume is built in into two different pixel blocks more stable is the block with bigger sum of amplitude spectrum elements. These elements correspond to elements of the phase spectrum used.

Still up to now we have not managed to find the strong dependence of building in reliability on the image statistical characteristics. We can speak only about empiric conclusions true in many cases. In order to get more reliable result one should have redundancy while building in information into the frequency area of the digital image.

The corresponding algorithm with redundancy during calculations, which consists of iterative repetition during the process of building in, is shown below.

2.3 The Suggested Algorithm of Embedding Data into Digital Images

In order to realize the suggested steganographic operation parameters φ_0, φ_1, ε, defining the two not crossing intervals: the interval $(\varphi_0 - \varepsilon, \varphi_0 + \varepsilon)$ corresponding zero bit and the interval $(\varphi_1 - \varepsilon, \varphi_1 + \varepsilon)$ corresponding unity bit, should be given. We'll call these intervals "intervals of building in".

Input: stego-container—full-color or halftone digital image; secret information $L = l_1 l_2 \ldots l_n$, $l_i \in \{0, 1\}$; parameters of building in φ_0, φ_1, ε; maximal number of iterations with one block; threshold value of elements of frequency block spectrum A_{crit} average amplitude.

Output: stego-image.

Step 1: Go to the YCbCr color model and split matrix $\mathbf{Y}$ into not crossing blocks 8 × 8.

Step 2: Initialize counter of the built in bits $k \leftarrow 0$.

Step 3: While $k < n$ do the follow:

Step 3.1: Do DFT of the matrix $\mathbf{Y}$ next block 8 × 8 getting matrix of complex numbers $\mathbf{F} = (f_{ij})_{i=1,j=1}^{8,8}$. Calculate matrix of amplitudes $\mathbf{A} = (a_{ij})_{i=1,j=1}^{8,8}$ and phases $\mathbf{\Phi} = (\varphi_{ij})_{i=1,j=1}^{8,8}$.

Step 3.2: Calculate average A_{mean} of elements a_{ij}, $i = \overline{2,7}$, $j = \overline{2,4}$, whose phases φ_{ij} are in one of building in intervals. If $A_{mean} < A_{crit}$ go to 3.3, otherwise to 3.1.

Step 3.3: Emphasize 18 bit long substring L' in the line L.

Step 3.4: Perform building in of secret bits. If the number of bits built in the block $q = 0$ go to 3.5, otherwise to 3.6.

Step 3.5: Treat the empty block.

Step 3.6: Calculate $k \leftarrow k + q$ and make $L \leftarrow l_{k+1} l_{k+2} \ldots l_n$.

Step 3.7: Make IDFT of the transformed block and modernize the values of the corresponding block in matrix $\mathbf{Y}$.

Step 4: Go to the RGB color model and finalize the algorithm.

Algorithms of matrix $\mathbf{Y}$ separate blocks processing used at steps 3.4 and 3.5 are investigated separately.

Algorithm of secret blocks building in.

Input: matrix of DFT complex coefficients is $\mathbf{F} = \left(f_{ij}\right)_{i=1,j=1}^{8,8}$; the corresponding matrix of phases is $\mathbf{\Phi} = \left(\varphi_{ij}\right)_{i=1,j=1}^{8,8}$; bit line is $L' = l_1 l_2 \ldots l_{18}$; maximal number of iterations is τ .

Output: matrix $\mathbf{F} = \left(f_{ij}\right)_{i=1,j=1}^{8,8}$ is the matrix with built in bits or the same as the initial matrix; the number of built in bits is q.

Step 1: Make matrixes $\mathbf{G} = \left(g_{ij}\right)_{i=1,j=1}^{8,8}$, $\mathbf{P} = \left(p_{uv}\right)_{u=1,v=1}^{6,3}$, $p_{uv} = -1$, $u = \overline{1,6}$, $v = \overline{1,3}$. Write matrix $\mathbf{F}$ into matrix $\mathbf{G}$. Initialize counter of built in bits $q \leftarrow 0$.

Step 2: For all $i = \overline{2,7}$, $j = \overline{2,4}$ do as follows:

Step 2.1: If $\varphi_{ij} \notin (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon)$ and $\varphi_{ij} \notin (\varphi_1 - \varepsilon, \varphi_1 + \varepsilon)$, take the next element of matrix $\mathbf{\Phi}$.

Step 2.2: $p_{i-1,j-1} \leftarrow l_{q+1}$, $q \leftarrow q + 1$.

Step 2.3: If φ_{ij} is in an interval corresponding the built in bit, go to 2.1.

Step 2.4: If $l_q = 0$, $\varphi_{ij} \leftarrow \varphi_0$, otherwise $\varphi_{ij} \leftarrow \varphi_1$.

Step 2.5: Turn radius-vectors corresponding elements f_{ij} and $f_{9-i,9-j}$ of matrix $\mathbf{F}$ taking DFT properties into consideration.

Step 3: Initialize counter of iterations $t \leftarrow 0$.

Step 4: Make matrix $\mathbf{F}$ IDFT getting the changed block of luminosity components $\mathbf{Y}$.

Step 5: Go to the RGB color model forming the block of pixels.

Step 6: Go to the YCbCr color model and perform DFT getting matrix $\mathbf{F} = \left(f_{ij}\right)_{i=1,j=1}^{8,8}$. Calculate matrix of phases $\mathbf{\Phi} = \left(\varphi_{ij}\right)_{i=1,j=1}^{8,8}$.

Step 7: Initialize the counter of errors $s \leftarrow 0$.

Step 8: For all $i = \overline{2,7}$, $j = \overline{2,4}$ do as follows:

Step 8.1: If $p_{i-1,j-1} = -1$ and $\varphi_{ij} \in (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon)$ or $\varphi_{ij} \in (\varphi_1 - \varepsilon, \varphi_1 + \varepsilon)$, $f_{ij} \leftarrow g_{ij}$, $f_{9-i,9-j} \leftarrow g_{9-i,9-j}$, $s \leftarrow s + 1$ and take the next element of the matrix $\mathbf{\Phi}$.

Step 8.2: If $p_{i-1,j-1} = 0$ and $\varphi_{ij} \notin (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon)$, $\varphi_{ij} \leftarrow \varphi_0$.

Step 8.3: If $p_{i-1,j-1} = 1$ and $\varphi_{ij} \notin (\varphi_1 - \varepsilon, \varphi_1 + \varepsilon)$, $\varphi_{ij} \leftarrow \varphi_1$.

Step 8.4: Turn radius-vectors corresponding elements f_{ij} and $f_{9-i,9-j}$ of the matrix $\mathbf{F}$ taking DFT properties into consideration and make $s \leftarrow s + 1$.

Step 9: If $s = 0$ go to 13, otherwise $t \leftarrow t + 1$.

Step 10: If $t < \tau$ go to 4.

Step 11: Write matrix **G** into matrix **F** and make $q \leftarrow q - 1$.

Step 12: If $q > 0, L' \leftarrow l_1 l_2 \ldots l_q$ and go to 1.

Step 13: Return matrix **F** and q back and finish the algorithm.

The case when L or L', during the operation, are shorter than 18 bits we don't consider to make the consideration easier.

Algorithm of an empty block processing

Input: matrix of the DFT complex coefficients $\mathbf{F} = \left(f_{ij}\right)_{i=1,j=1}^{8,8}$.

Output: changed matrix $\mathbf{F} = \left(f_{ij}\right)_{i=1,j=1}^{8,8}$.

Step 1: Make matrix **F** IDFT getting the changed block of luminosity components **Y.**

Step 2: Go to the to the RGB color model forming the block of pixels.

Step 3: Go to the YCbCr color model and perform DFT getting matrix $\mathbf{F} = \left(f_{ij}\right)_{i=1,j=1}^{8,8}$. Calculate matrix of phases $\mathbf{\Phi} = \left(\varphi_{ij}\right)_{i=1,j=1}^{8,8}$.

Step 4: Initialize the counter of the "false" bits $s \leftarrow 0$.

Step 5: For all $i = \overline{2,7}$, $j = \overline{2,4}$ do as follows:

Step 5.1: If $\varphi_{ij} \in (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon)$ or $\varphi_{ij} \in (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon)$ generate a random value r out of the mentioned interval and make $\varphi_{ij} \leftarrow r$.

Step 5.2: Turn radius-vectors corresponding elements f_{ij} and $f_{9-i,9-j}$ of the matrix **F** taking DFT properties into consideration and make $s \leftarrow s + 1$.

Step 6: If $s = 0$ go to 7, otherwise to 1.

Step 7: Return matrix **F** and finalize the algorithm.

Algorithm of extraction is obvious and is not described here.

2.4 Experiments

In this part there are given results of some calculation using the suggested steganographic algorithm. All calculations we are done with 10 full-color images with 256 × 256 pixels (classic test images Airplane, Baboon, Goldhill, Lenna, Peppers and so on). The main parameters of building in were $\varphi_0 = -\frac{\pi}{2}$, $\varphi_1 = \frac{\pi}{2}$, $\varepsilon = 1$.

Figure 1a show the averaged dependence of the building in quality (PSNR) on the length of message for $\tau = 20$ and $A_{crit} = 0,8$. One can see that even if the volume of building in is big there are no distortions of stego-container.

Graphics in Fig. 1b show that PSNR decrease only slightly if the number of iterations grows.

The graphic in Fig. 1c got for $\tau = 20$ shows that the threshold of the block frequency elements average amplitude suitable for building in influence the quality of stego-image. Therefore $A_{crit} > 1.5$ are not recommended.

So, we can conclude that the suggested algorithm allows not only escape distortions but also provide high quality of building in.

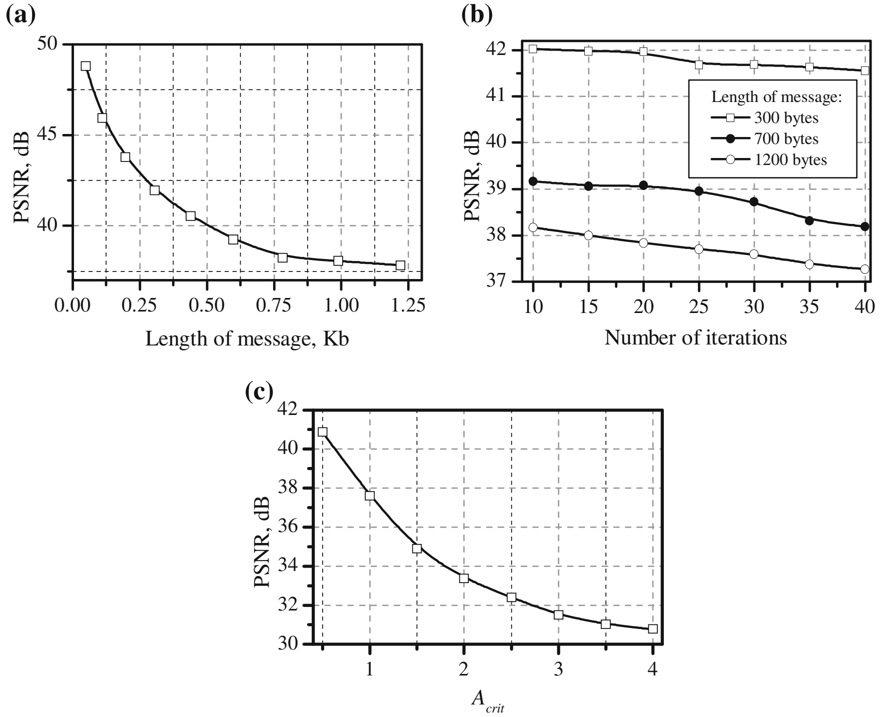

Fig. 1 Influence of the suggested algorithm parameters on the stego-image quality: length of message (**a**); number of iterations τ (**b**); threshold A_{crit} (**c**)

3 Conclusion

There were investigated steganographic properties of the discrete Fourier transform in case of building in information into the phase spectrum. As the basic steganographic operation there is used the turn of the radius-vector at the complex plane.

The main peculiarity of the investigation is solving the problem of information distortion while information is built in into the digital area of the digital image. Distortions appear in the process of the transform from the frequency area into the space and is due to rounding the real values to digital.

The problem mentioned is typical not only for the introduced steganographic operation but also for other operations connected with building in information into the frequency area of digital images. Unfortunately there are no publications on the subject.

We received algorithm that allows to get information without mistakes using unequal building in parts of information in image blocks and iterative procedure. Such characteristic as capacity and quality of building in the algorithm is comparable to the analogs described in 2.1.

Further investigation can make the process of building in more effective on the bases of optimization.

Acknowledgments This work was supported by the Ministry of Education and Science of the Russian Federation within 1.3 federal program « Research and development in priority areas of scientific-technological complex of Russia for 2014-2020 » (grant agreement № 14.577.21.0153 on November 28, 2014; identifier RFMEFI57714X0153).

References

1. Salomon, D.: Data Compression: The Complete Reference, 4th edn. Springer, London (2007)
2. Gorbachev, V.N., Kainarova, E.M., Denisov, L.A.: Embedding of Binary Image in the Gray Planes. Comput. Opt. **37**, 385–390 (2013)
3. Wang, Z.H., Chang, C.C., Li, M.C.: Optimizing least-significant-bit substitution using cat swarm optimization strategy. Inf. Sci. **192**, 98–108 (2012)
4. Kanan, H.R., Nazeri, B.: A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst. Appl. **41**, 6123–6130 (2014)
5. Glumov, N.I., Mitekin, V.S.: A new semi-fragile watermarking algorithm for image authentication and information hiding. Comput. Opt. **35**, 262–267 (2011)
6. Verichev, A.V., Fedoseev, V.A.: Digital image watermarking on triange grid of feature points. Comput. Opt. **38**, 555–563 (2014)
7. Zhao, J., Koch, E.: Embedding robust labels into images for copyright protection. In: International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, pp. 242–251. R. Oldenbourg Verlag, Munich (1995)
8. Holliman, M., Memon, N., Yeo, B.L., Yeung, M.: Adaptive public watermarking of DCT-based compressed images. Int. Soc. Opt. Eng. **3312**, 284–295 (1998)
9. Westfeld, A.: High capacity despite better steganalysis (F5-A Steganographic Algorithm). In: 4th International Workshop on Information Hiding, pp. 289–302. Springer, London (2001)
10. Yu, L., Zhao, Y., Ni, R., Zhu, Z.: PM1 steganography in JPEG images using genetic algorithm. Soft. Comput. **13**, 393–400 (2009)
11. Huang, F., Huang, J., Shi, Y.Q.: New channel selection rule for JPEG steganography. IEEE Trans. Inf. Forensics Secur. **7**, 1181–1191 (2012)
12. Ejaz, N., Anwar, J., Ishtiaq, M., Baik, S.W.: Adaptive image data hiding using transformation and error replacement. Multimedia Tools Appl. **73**, 825–840 (2013)
13. Li, F., Zhang, X., Yu, J., Shen, W.: Adaptive JPEG steganography with new distortion function. Ann. Telecommun. **69**, 431–440 (2014)
14. Evsutin, O.O., Kokurina, A.S., Shelupanov, A.A., Shepelev, I.I.: An improved algorithm for data hiding in compressed digital images based on PM1 method. Comput. Opt. **39**, 572–581 (2015)
15. Soliman, M.M., Hassanien, A.E., Onsi, H.M.: An adaptive watermarking approach based on weighted quantum particle swarm optimization. Neural Comput. Appl. **27**, 469–481 (2016)
16. Rekik, S., Guerchi, D., Selouani, S.A., Hamam, H.: Speech steganography using wavelet and fourier transforms. EURASIP J. Audio Speech Music Process. **20**, 14 (2012)
17. Natgunanathan, I., Xiang, Y., Rong, Y., Peng, D.: Robust patchwork-based watermarking method for stereo audio signals. Multimedia Tools Appl. **72**, 1387–1410 (2013)
18. Cedillo-Hernandez, M., Garcia-Ugalde, F., Nakano-Miyatake, M., Perez-Meana, H.: Robust watermarking method in DFT domain for effective management of medical imaging. SIVIP **9**, 1163–1178 (2015)

19. Solachidis, V., Pitas, I.: Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Trans. Image Process. **10**, 1741–1753 (2001)
20. Poljicak, A., Mandic, L., Agic, D.: Discrete fourier transform-based watermarking method with an optimal implementation radius. J. Electron. Imaging **20**, 033008-1–033008-8 (2011)
21. Ridzon, R., Levicky, D.: Content protection in grayscale and color images based on robust digital watermarking. Telecommun. Syst. **52**, 1617–1631 (2013)
22. Rabie, T.: Digital Image Steganography: An FFT Approach. In: Benlamri, R. (ed.) NDT 2012. Communications in computer and information science, vol. 294, pp. 217–230. Springer, Heidelberg (2012)
23. Mandal, J.K., Khamrui, A.: A Genetic Algorithm Based Steganography in Frequency Domain (GASFD). In: International Conference on Communication and Industrial Application, pp. 1–4, IEEE (2011)
24. Bhattacharyya, D., Kim, T.: Image Data Hiding Technique Using Discrete Fourier Transformation. In: Kim, T., Adeli, H., Robles, R.J., Balitanas, M. (eds.) UCMA 2011. Communications in computer and information science, vol. 151, pp. 315–323. Springer, Heidelberg (2011)
25. Savelonas, M.A., Chountasis, S.: Noise-resistant watermarking in the fractional fourier domain utilizing moment-based image representation. Sig. Process. **90**, 2521–2528 (2010)
26. Chen, W.Y.: Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. Appl. Math. Comput. **196**, 40–54 (2008)
27. Evsutin, O.O., Kozlova, A.S., Meshcheryakov, R.V., Kokurina, A.S.: Information embedding into the phase spectrum of the discrete fourier transform. In: 25th International Crimean Conference on Microwave & Telecommunication Technology, pp. 371–372, Sevastopol (2015)