УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 7 (2017), No. 4, pp. 255-264

DEVELOPMENT OF THE STEGANOGRAPHIC METHOD FOR BINARY COVER-IMAGES

A.A. Kobozeva[1], M.V. Vornikova[1], A.V. Akhmametieva[1], O.A. Penko[2]

[1] Odesa National Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net
[2] Richelieu Lyceum,
5, Elisavetinska Str., Odesa, 65026, Ukraine

A new steganographic method for binary digital images has been developed. During the development of the method, the expediency of choosing the spatial domain of the container for introducing hiding information is justified, which avoids additional accumulation of computational error and increase in computational complexity, as compared with methods working in the field of container transformation. The developed method provides for the decoding of hiding information, its restoration in full, the increase in the efficiency of steganographic transformation of binary digital images covers, quantitatively estimated by the peak signal-to-noise ratio (PSNR) for the generated stego, in comparison with existing analogues for comparable volumes of submerged information, than by 30%.

Keywords: binary digital image, steganographic method, spatial domain, reliability of perception of stego

Introduction

The high level of development of information technologies and computer sciences has both positive and negative consequences today one of which is the unresolved adequately task of information security of widespread and everywhere used digital media [1, 2]. Traditional ways for ensuring the protection of data and resources from the possibility of illegal access, for ensuring the reliability of received data and messages are: the encryption of confidential information that is realized by means of cryptography methods and algorithms [3], the concealment of the fact of existence of confidential information by using steganographic methods [4, 5]. The combination of the two approaches when the encryption of the concealed information precedes its concealment in an inconspicuous information content-container, in particular in a digital image, followed by transmission over a hidden (steganographic) communication channel increases the security of the transmitted information, and therefore it is, as a rule, used to ensure of preventing of illegal access now.

In the present work binary images are used as a container, a binary sequence formed by a random (pseudorandom) way and considered as a result of preliminary encoding (encryption) of really transferred message is used as a confidential information. Binary digital images not being widespread in everyday life have important applied significance: various schemes, graphs, tables, some medical images are presented in the form of binary images in order to ensure their high sharpness, contrast [6, 7]. Steganographic transformation of such digital image is the difficult and unresolved task related to their specificity – they have only two gradations of brightness. The change in the brightness of a pixel by one unit can be seen visually in the presence of the original image (fig. 1). And although the developments in this direction are conducted by modern scientists [8-11] the task of ensuring the preservation of the reliability of the perception of stego that is the result of embedding of additional information into binary image-container remains actual. This is due to the fact that when

organizing a steganographic channel, one of its required properties should be to provide a significant capacity of the hidden communication channel, and the proposed existing developments, as a rule, provides an acceptable quality of stego (reliability of perception), an increase in this quality that quantitatively evaluated by various difference indices, in particular, the peak signal-to-noise ratio (PSNR) [4], by reducing the amount of transmitted information [12-15] which is extremely undesirable.

a b

Fig. 1. The result of embedding of additional information into binary digital image: a – digital image-container; b – digital image-stego

The aim of the article and setting of research problems

The *aim* of the work is to increase in efficiency of steganographic transformation of binary digital images by developing a new steganographic method that ensures the reliability of perception of the created stego.

The efficiency of a steganographic transformation in the context of this work will be quantitatively estimated by PSNR value of the stego formed by the corresponding steganographic method taking into account the provision of the required capacity of the hidden communication channel.

Taking into account the fact that all steganographic methods are divided into those that embeds additional information into the spatial domain of the digital image and those that use different transformation domains for steganographic transformation, and also taking into account the features of the formal representation of the binary digital image (the presence of only two brightness gradations) for achievement of the aim it is necessary to solve the following *problems*:

1. To define an area for embedding of additional information into a binary digital image (spatial, transform);

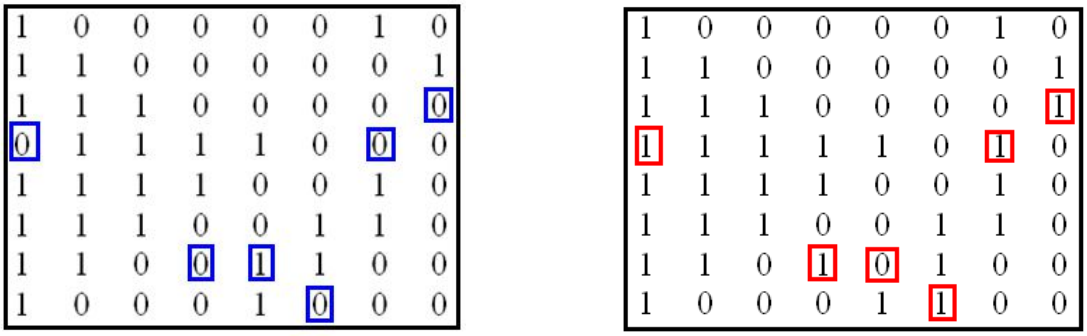
2. To determine the formal parameters of the image in the selected area which are the least sensitive to the perturbing influence consisting in embedding of additional information.

Main part

For embedding of additional information into the image-container, both the spatial and the transform domain can be used, which can be the frequency domain of the digital image, domain of various matrix expansions: singular, spectral, etc. [16]. In [17] it was shown that in order to provide certain required properties of stego, including the reliability of its perception, it does not matter in principle into which domain of the container the embedding of additional

information occurs, but it is important to which perturbations of singular numbers and singular vectors of the matrix (blocks of the matrix) of a container it will lead, where exactly within the formal parameters of singular expansion of a matrix (blocks of the matrix) these perturbations will be localized. At the same time, in case of the organization of steganographic transformation into transform domain of the digital image additional computational expenses and the accumulation of additional computational errors arise due to the execution of "transitions" from the spatial to the transform domain, and then in the reverse order [16].

For binary digital images the selection of the transform domain for embedding of additional information is connected to additional difficulties arising owing to rounding of the brightness values of the pixels when inverse transformation carrying out (return to the spatial domain of the image). If brightness change in the field of real numbers is very insignificant but it is more than 0.5 it can lead to inverse of color: 0 will be replaced by 1 or 1 will be replaced by 0. The illustration to told is given in fig. 2 in case of the discrete cosine transform (DCT) of one 8×8 block of the digital image shown in Fig. 1, a. Minor changes in the matrix of DCT coefficients (the spectral norm of the perturbation matrix was only 2.3 here) led to visually discernable changes in the spatial domain of the image (fig. 2).



a b

Fig. 2. The result of distortion of the binary digital image due to insignificant perturbations of the DCT coefficients: a – the block of the original binary image; b – the corresponding block of the binary digital image whose matrix norm is 2.3, after a perturbation carried out in the DCT domain

Thus, the spatial domain of a binary digital image-container is preferable in comparison with the transform domain of the container for embedding of additional information both from the point of view of computational complexity estimation, both from the point of view of estimation of computational error, and therefore it is used to organize steganographic transformation in the method being developed in the work.

Traditionally [5] to reduce the visual distortion of a color or grayscale image when embedding of additional information, a steganographic path is used which containes pixels belonging to the contours (significant differences in brightness values) presented in the image. The specificity of a binary digital image does not make this embedding method such which guarantees the reliability of the perception of a stego because here due to steganographic transformation a contour shift and a change in its shape can occur which will be visually obviously visible even without the presence of the original image-container.

For practical confirmation of the last statement in the Matlab environment a computational experiment was carried out in which 400 binary images of size 1000×1500 were used, forming a set which is called experimental below. During the experiment embedding of additional information into the pre-selected contour of digital images additively modulo 2 was carried out. By subjective ranging violation of reliability of perception of some stegos (the example is given in fig. 3) was revealed. The mean value of PSNR for all received

stegos was only 17.68 dB that is much lower than the value considered acceptable for the organization of the steganographic communication channel – 37 dB [4].

It should be noted that the use of contour pixels as a steganographic path can significantly limit the capacity of a hidden communication channel that is extremely unwanted, and also increases the probability of detection the presence of embedded additional information by means of steganalysis, obviously localizing within the boundaries of the digital image its location area expected on the basis of practical experience.

All of the above makes it reasonable to choose as steganographic path those pixels that are not directly related to the scene of the image.

a b

Fig. 3. Visual distortions when embedding of additional information into the contour of the container: a – digital image-container; b – digital image-stego

As it appears from above the use of binary digital images as containers cannot provide a significant capacity of a hidden communication channel in principle. Taking this into account, as well as the fact that during the organization of steganographic transformation for reduction of computational complexity of the corresponding steganographic algorithms, the digital image-container matrix is usually broken up into not crossed blocks, and the embedding of a certain fixed bit count of additional information occurs block-by-block, it is proposed in the developed method after the preliminary standard partitioning of the matrix on 8×8-blocks to embed additional information into the block no more than one bit of information.

By subjective ranking during the computational experiment it was found that the change of even one pixel in a monochrome block, i.e. block, the matrix of which contained only zeros or only ones, does not preserve the reliability of image perception therefore further such blocks do not participate in the process of steganographic transformation.

For localization in 8×8-block of the pixel used for steganographic transformation which perturbation least of all will visually affect on digital image-stego the computational experiment was performed on the basis of digital images from the experimental set. During the experiment the original image-container was broken into 8×8-blocks, into all blocks of the image, except those that consisted completely of zeros or ones, information was embedded by inverse of brightness value of the pixel located at position (1,1). For each digital image-stego the PSNR value was defined. Similar actions were carried out for accounting of all possible options for selecting a pixel within the block to embed the information bit: the pixel at position (1,2), (1,3), ..., (8,1), …, (8,8). As a result of the experiment, it was found that when embedding information in the pixels of the category 1 of the block (fig. 4), the image quality taking into account PSNR, where the average value was 26 dB, was significantly better than in the case of pixels for the categories 2 and 3: the average value of PSNR here was 21 dB and 17 dB, respectively.

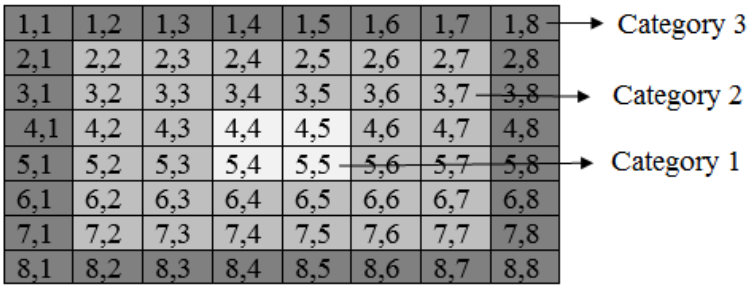


Fig. 4. The categories of pixels of 8×8-blocks of binary digital images used for embedding of additional information

During the experiment described above it was found that visually changes in digital image as a result of embedding of additional information occur not only when it embeds into a monochrome block pixel, but can also occur when the block contains a small quantity of ones/zeros, and the embedding is carried out by inversion of the zero/one presented there. For accounting of it in the developed steganographic method two parameters p_0 and p_1 are introduced which values allow controlling the process of selecting the next block for embedding the next bit of the transmitted information. Each of parameters accepts values from 1 to 63, herewith p_0 sets minimum possible quantity of zeros, and p_1 - minimum possible quantity of ones in the block used in the process of a steganographic transformation, i.e. if the number of zeros/ones in the block appears less than p_0 / p_1 such block is not used for embedding of additional information. Thus, the more there will be values p_0, p_1, the less there will be a capacity of the organized hidden communication channel as with increase of p_0, p_1 the number of blocks which are not used in the process of a steganographic transformation will grow, but at the same time the probability of ensuring the reliability of perception of the created stego will increase due to increasing PSNR value.

It should be noted that in the process of a steganographic transformation of the block it is possible when the block after embedding of bit of additional information (therefore values of brightness of pixels/pixel will change) will be already such for which the conditions imposed by parameter values p_0, p_1 on the number of zero and ones, may not be executed. I.e. when reviewing such block in a stego the quantity of ones/zeros in it can appear less than p_0 / p_1 that will make more difficult to recognize the block participating in the process of steganographic transformation of the digital image when decoding additional information and will demand the organization of additional accounting of blocks containing in themselves bits of the transmitted data.

The embedding of the additional information bit into the 8×8-block of the binary digital image in the developed method depends on the parity/oddness of the sum of all the elements of the block, i.e. the quantity of ones in the block: the additional information, which embeds in the block bit and is equal to 1/0 must correspond to the odd/even sum of the elements values of the block.

Let F is a $n\times m$-matrix of a binary digital image-container, $d_1, d_2, ..., d_t$, $d_i \in \{0,1\}$, $i = \overline{1,t}$ – the binary sequence which is result of encoding of the transferred confidential message, $\overline{F}$ – $n\times m$-matrix of a binary digital image-stego. For accounting of the blocks participating in the steganographic transformation in the developed method a binary $\left[\frac{n}{8}\right]\times\left[\frac{m}{8}\right]$ – matrix T with elements t_{ij} each of which corresponds to the corresponding block of digital image is created. The matrix T formed during the embedding

of additional information is a part of the secret key for the developed method in case of its algorithmic implementation and is transmitted over a secure communication channel.

The main steps of the proposed steganographic method further called by SMBI look as follows.

Embedding of additional information

Step 1. Split the matrix F of digital image-container in a standard way into uncrossed 8×8-blocks $B^{(kl)}$, $k=\overline{1,\left[\frac{n}{8}\right]}, l=\overline{1,\left[\frac{m}{8}\right]}$, where $[\bullet]$ is the integer part of the argument. Form the original form of the $\left[\frac{n}{8}\right]\times\left[\frac{m}{8}\right]$-matrix T, which is part of the secret key:

$$T=0.$$

Step 2. Set the values of the parameters $p_0, p_1 \in \{1,2,3,...,63\}$ (this can be done taking into account the required size of the transmitted confidential information, the minimum/maximum permissible distortion requirement of the digital image while steganographic transformation, the totality of these requirements, etc.).

Step 3. For the next block $B^{(kl)}$ with elements $b_{ij}^{(kl)}$, $i,j=\overline{1,8}$, of the matrix F:

3.1. (*Conclusion about the suitability of the block for steganographic transformation*).

Find

$$s_1=\sum_{i,j=1}^{64} b_{ij}^{(kl)};\ s_0=64-s_1.$$

If

$$(s_1\geq p_1)\&(s_0\geq p_0),$$

then

the block $B^{(kl)}$ is used for embedding the next bit of additional information;

$$t_{kl}=1,$$

else

the block $B^{(kl)}$ does not used for embedding the next bit of additional information.

3.2. (*Embedding the next bit of additional information into the container block*).

If

the block $B^{(kl)}$ is used for steganographic transformation and d_i is the next bit of additional information,

then

if

$(s_1=2n)\&(d_i=1)\vee(s_1=2n-1)\&(d_i=0)$, where n is a natural number,

then

$$b_{5,5}^{(kl)}=\left|b_{5,5}^{(kl)}-1\right|.$$

3.3. Go to the next block.

Decoding of additional information

Step 1. Split the matrix F of digital image-stego in a standard way into uncrossed 8×8-blocks $\overline{B}^{(kl)}$, $k=\overline{1,\left[\frac{n}{8}\right]}, l=\overline{1,\left[\frac{m}{8}\right]}$.

Step 2. For the next block $\overline{B}^{(kl)}$ with elements $\overline{b}_{ij}^{(kl)}$, $i,j=\overline{1,8}$, of the matrix $\overline{F}$:

2.1. (*Conclusion about the presence of additional information bit in the block*).

If

the corresponding to the block $\overline{B}^{(kl)}$ element of the secret key matrix T

$$t_{kl} = 1,$$

then

block $\overline{B}^{(kl)}$ contains additional information,

else

block $\overline{B}^{(kl)}$ does not contain additional information.

2.2. (*Extraction of the next bit of additional information from the stego block*).

If

block $\overline{B}^{(kl)}$ contains additional information,

then

extract $\overline{d}_i$ - the next bit of additional information.

Find $$\overline{s}_1 = \sum_{i,j=1}^{64} \overline{b}_{ij}^{(kl)};$$

If

$\overline{s}_1 = 2n$, where n is a natural number,

then

$$\overline{d}_i = 0,$$

else

$$\overline{d}_i = 1.$$

2.3. Go to the next block.

When testing of the proposed method when carrying out a computing experiment in the environment of Matlab its algorithmic implementations with different parameter values p_0, p_1 were used. The results of the experiment in which digital images from the experimental set were used, characterized by the PSNR value for the created stego-images and the length of the embedded message (in bits) depending on the values of the parameters p_0, p_1 are shown in Table 1, 2, respectively. The numbers presented in tables correspond to the mean value of the corresponding parameter for all digital images from the experimental set at fixed values p_0, p_1.

Since the stego was saved without loss when decoding additional information all the bits of the embedded message were restored correctly.

Table 1.

PSNR value (dB) for stego generated by algorithmic implementations of the SMBI method for various parameter values p_0, p_1

p_0 / p_1	1	5	10	20	30
1	31.71	32.13	32.36	35.86	33.54
5	32.83	33.16	33.50	34.16	35.14
10	33.78	34.41	34.57	35.44	36.52
20	33.38	35.93	36.50	37.79	39.89
30	34.34	37.73	38.59	40.79	46.98

Table 2.

Length of the embedded message (in bits) in stego generated by algorithmic implementations of the SMBI method for various parameter values p_0, p_1

p_0 / p_1	1	5	10	20	30
1	8815	8310	7833	6969	6940
5	7151	6645	6169	5305	4376
10	5914	5409	4933	4068	3139
20	4274	3769	3292	2428	1499
30	3089	2583	2107	1243	314

From these results it is visible that if both parameters have values not less than 10 then PSNR values are that that provide reliability of perception of a stego [4]. The length of the embedded message naturally decreases with increasing values p_0, p_1 remaining considerable for a binary digital image-container when at least one of the parameters during steganographic transformation is less than 30.

For algorithmic implementation of the developed method (in case of $p_0 = 5$, $p_1 = 5$) the comparative analysis of its efficiency (from the point of view of ensuring the reliability of perception of the created stego) with the modern analogs [1, 12-15] was carried out. The values of the parameters p_0, p_1 were chosen in such a way as to ensure the correctness of the comparison, i.e. analogous to the conditions of testing given in [1, 12-15] (steganographic transformation occurred due to the change of slightly more than 300 pixels in binary digital images-containers which were used in [1, 12-15]). The results of the experiment speaking about increase in efficiency of a steganographic transformation of binary digital images from the point of view of increase in PSNR value, other things being equal, are given in Table 3.

Table 3.

PSNR values (dB) of the developed method and existing analogs

Steganographic method / Stego	SMBI (2017)	Do Van Tuan (2012)	CTL (2005)	TCP (2000)	Ki-Huyun Jung (2009)	Venkatesan et al.`s (2007)
Baboon	27.49	-	-	-	16.32	16.36
Aircraft	32.09	-	-	-	21.50	21.25
Lena	29.92	22.90	22.16	22.88	20.51	20.45
Boat	30.76	-	-	-	20.45	20.56

As can be seen from Tabl. 3 we managed to increase the PSNR value from 30.7% (for digital image “Lena” in comparison with the DoVanTuan method (2012)) up to 68% for digital image “Baboon” in comparison with Venkatesan et al.'s (2007) in case of comparable amounts of the embedded message.

Conclusions

The result of this work is an increase in the efficiency of steganographic transformation of binary digital images-containers by developing a new steganographic method SMBI which provides an increase in the difference in PSNR for estimating the reliability of perception of

the created stego in comparison with existing analogs for comparable amounts of embedded information by a minimum of more than 30%.

During development of the SMBI method expediency of a choice of spatial domain of binary digital images for embedding of additional information is justified that allows to avoid additional accumulation of a computing error and increase in computing complexity in comparison with the methods working in the transformation domain of a container.

As a result of the computational experiment, it was set that at the maximum amount of embedded information ($p_0 = 1$, $p_1 = 1$), the average value of the PSNR for the digital images from the experimental set was 32 dB. When decoding additional information was restored correctly in full.

The capacity of the organized hidden communication channel is still insufficient when working with binary digital images, search of methods to increase of it is an object of research by the authors at the present time.

References

1. Chang, Chin-Chen. Hiding Data in Binary Images / Chin-Chen Chang, Chun-Sen Tseng, Chia-Chen Lin. // ISPEC 2005: Information Security Practice and Experience. — 2005. — Pp. 338-349.
2. Wu, M.Y. A Novel Data Embedding Method for Two-color Facsimile Images / J.H. Lee, M.Y. Wu. // Proc. Int. Symp. On Multimedia Information Processing. — Chung-Li (Taiwan), 1998. — Pp. 138–149.
3. Баричев, С. Г. Основы современной криптографии. – 3-е изд. / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — М.: Диалог-МИФИ, 2011. — 176 с.
4. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А. Ю. Пузыренко. — К.: МК—Пресс, 2006. — 288 с.
5. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
6. Федоров, А. Бинаризация черно-белых изображений: состояния и перспективы развития [Электронный ресурс] / А. Федоров. // CLAIM – научно-образовательный кластер. Режим доступа: http://it-claim.ru/Library/Books/ITS/wwwbook/ist4b/its4/fyodorov.htm/ (Дата обращения 08.08.2017).
7. Фурман, Я.А. Цифровые методы обработки и распознавания бинарных изображений / Я.А. Фурман, А.Н. Юрьев, В.В. Яншин. — Красноярск: Краснояр. ун-та, 1992. — 248 с.
8. Guo, Fu Gui. A New Asymmetric Watermarking Scheme for Copyright Protection / Gui Fu Guo, Ling Ge Jiang, Chen He. // IECE Trans. Fundamentals. — 2006. — Vol. E89-A, No. 2. — Pp. 147–153.
9. Lee, Y.K. Capacity Image Steganographic Model / Y.K. Lee, L.H. Chen. // Proc. of IEE International Conference on Vision, Image and Signal Processing. — 2000. — Vol. 147, No. 3. — Pp. 288–294.
10. Smitha, B. Spatial Domain – High Capacity Data Hiding in ROI Images / B. Smitha, K.A. Navas. // IEEE – ICSCN 2007. — Chennai, India, Feb, 2007. — Pp. 528–533.
11. Tzeng, C.H. Adaptive Data Hiding in Palette Image by Color Ordering and Mapping with Security Protection / C.H. Tzeng, Z.F. Yang, W.H. Tsai. // IEEE Transactions on Communications. — 2004. — Vol. 52, No. 5. — Pp. 791–800.
12. Tseng, Y.C. A secure Data Hiding Scheme for Binary Images / Y.C. Tseng, Y.Y. Chen, K.H. Pan. // IEEE Transactions on Communications. — 2002. — Vol. 50, No. 8. — Pp. 1227–1231.
13. Do Van Tuan. A Novel Data Hiding Scheme for Binary Images / Do Van Tuan, Tran Dang Hien, Pham Van At. // International Journal of Computer Science and Information Security. — 2012. — Vol. 10, No. 8. — Pp. 33–38.
14. Venkatesan, M. A new data hiding scheme with quality control for binary images using block parity / M. Venkatesan, P. Meenakshidevi, K. Duraiswamy, K. Thiagarajah. // 3rd Inter. Symposium on Information Assurance and Security. — 2007. — Pp. 468–471.
15. Jung, Ki-Hyun. Data Hiding Method with Quality Control for Binary Images / Ki-Hyun Jung, Kee-Young Yoo. // Journal of Software Engineering & Applications. — 2009. — Vol. 2. — Pp. 20–24.

16. Костырка, О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В. Костырка. // Інформатика та математичні методи в моделюванні. — 2013. — Т. 3, № 3. — С. 275–282.
17. Кобозєва, А.А. Аналіз захищеності інформаційних систем [Текст]: підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. — К.: ДУІКТ, 2010. — 316 с.

РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДУ ДЛЯ БІНАРНИХ КОНТЕЙНЕРІВ-ЗОБРАЖЕНЬ

А.А. Кобозєва[1], М.В. Ворнікова[1], Г.В. Ахмаметьєва[1], О.А. Пенко[2]

[1] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net
[2] Рішельєвський ліцей,
вул, Єлісаветинська, 5, Одеса, 65026, Україна

Розроблено новий стеганографічний метод для бінарних цифрових зображень (ЦЗ). В ході розробки методу обґрунтовано доцільність вибору просторової області контейнера для вбудови додаткової інформації, що дозволяє уникнути додаткового накопичення обчислювальної похибки і збільшення обчислювальної складності, в порівнянні з методами, які працюють в області перетворення контейнера. Розроблений метод забезпечує при декодуванні додаткової інформації її відновлення в повному обсязі, підвищення ефективності стеганоперетворення бінарних ЦЗ-контейнерів, яка кількісно оцінюється піковим відношенням «сигнал-шум» (PSNR) для формованих стеганоповідомлень, в порівнянні з існуючими аналогами при порівнянних обсягах вбудованої інформації, мінімально більш, ніж на 30%.
Ключові слова: бінарне цифрове зображення, стеганографічний метод, просторова область, надійність сприйняття стеганоповідомлення

РАЗРАБОТКА СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ДЛЯ БИНАРНЫХ ИЗОБРАЖЕНИЙ-КОНТЕЙНЕРОВ

А.А. Кобозева[1], М.В. Ворникова[1], А.В. Ахмаметьева[1], Е.А. Пенко[2]

[1] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net
[2] Ришельевский лицей,
ул. Елисаветинска, 5, Одесса, 65026, Украина

Разработан новый стеганографический метод для бинарных цифровых изображений (ЦИ). В ходе разработки метода обоснована целесообразность выбора пространственной области контейнера для внедрения дополнительной информации, что позволяет избежать дополнительного накопления вычислительной погрешности и увеличения вычислительной сложности, по сравнению с методами, работающими в области преобразования контейнера. Разработанный метод обеспечивает при декодировании дополнительной информации ее восстановление в полном объеме, повышение эффективности стеганопреобразования бинарных ЦИ-контейнеров, количественно оцениваемой пиковым отношением «сигнал-шум» (PSNR) для формируемых стеганосообщений, по сравнению с существующими аналогами при сравнимых объемах погруженной информации, минимально более, чем на 30%.
Ключевые слова: бинарное цифровое изображение, стеганографический метод, пространственная область, надежность восприятия стеганосообщения