UDC 004.352.242.056.5 **doi: 10.32620/reks.2022.2.13**

**Konstantin DERGACHOV, Leonid KRASNOV,
Vladislav BILOZERSKYI, Anatolii ZYMOVIN**

National Aerospace University "Kharkiv Aviation Institute", Ukraine

DEVELOPMENT OF TOOLS FOR INFORMATION PROTECTION OF OPTICAL TEXT RECOGNITION SYSTEMS

The subject of research. *There has been studying a new universal method of information protection in optical text recognition systems when transmitting confidential data over open communication channels.* ***This work develops*** *the concept of creating a modern, simple and reliable method for protecting information during its transmission over communication channels, to determine the objective criteria for the quality of its work, to create a set of algorithms for implementing the proposed method and software for conducting experimental studies. The current work puts on the concept of creation of a simple and reliable current method for protecting information when passing it through communication channels, also to define the objective criteria for assessing the tool operation quality and to exercise the dedicated programs, which implement the proposed methods and developed algorithms. Based on the results of these studies, it must evaluate the practice effectiveness of the proposed method in terms of both the transmitted data coding/decoding reliability and the secrecy of the fact of special information transmission.* ***Results****. It is described the universal concept of producing and use of the contemporary methods of information protection in optical text recognition systems in a confidential data transmission over open communication channels. The main criteria for these systems performance quality are determined. A new combined method for encrypting transmitted messages using QR-codes with subsequent masking of the fact of data transmission by various methods of LSB-steganography is proposed. To conduct experimental studies, a text recognition program based on Tesseract OCR software version 4.0 was developed. The program in Python uses the recent resources of the OpenCV library. The dedicated software technique contributed to assessing the efficiency of the algorithms, which realized the transmitted data encryption and therefore communication links privacy. There are examples of the system operation and results of the software testing in modes of messages encoding for subsequent hidden transmission.* ***Conclusion****. The case studies acknowledge the high efficiency of the proposed method of confidential data protection when transmitting them via open networks. The technique can be taken as a basis for developing software aimed at protecting information in OCR systems offered by various manufacturers.*

Keywords*: information protection in optical text recognition systems; correct text recognition probability; algorithms for preliminary processing of initial data; text information encoding; QR-code; LSB-steganography algorithms for hidden data transmission.*

1. Introduction

The development of innovative methods of information processing, which are based on using artificial intelligence systems and deep learning neural networks, affected much the rise of both the newest pure scientific approaches and algorithms and the growth of practically useful applications in various fields of activity. In the problem of pattern recognition, this, in particular, caused the introducing into practice the algorithms and programs for optical character recognition (OCR) [1 − 3]. On the market, modern optical text recognition systems have appeared. Such IT-services are successfully operated and distributed both free of charge and on a commercial basis. The most popular of them are developed and supported by the world's leading manufacturers. These are the FineReader by the Russian ABBYY company, the CuneiForm OCR system from Cognitive Technologies, the Google's Tesseract program, a number of other products [4 − 8].

Unfortunately, all these systems are imperfect for the present and have a number of significant shortcomings. Primarily, these imply absence of 100% guarantee for correct text recognition and affecting of the initial data quality on the results of the program performance (for example, different lighting condition when photographing documents, pictures geometric distortions, noise effects, etc.). But the key disadvantage is the complete or partial lack of arrangements that would protect information being recognized in the case of exchange of the confidential data in open communication channels.

The authors conducted studies with elaborating a promising system for optical recognition of high quality text documents based on the Tesseract engine. It is an open source OCR engine that uses neural networks to find and identify textual content in images. Since version

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

4.0, Tesseract uses the Long Short-Term Memory (LSTM) architecture for recurrent neural networks. The program works effectively even in conditions of interfering influences. When using this program, the key research results were gotten and lately presented [9, 10].

The current paper describes in detail the results of ongoing research. The selection and implementation of the most promising method for protecting confidential information being obtained in the result of text recognition is the purpose of the work. A specialized program supplied with the comprehensive assessment of the effectiveness, which meets information protection in text recognition systems of different manufacturers, has been practically implemented.

2. Work related analysis

The problem of OCR systems quality enhancement is composite. One can specify several fundamental ways that can significantly improve working and operational characteristics of existing systems:

- further enhancement of methods for text detection and segmentation, which are the most important and challenging goals under research in the field of computer vision;
- efficacious repair of the negative factors like images geometric distortion, shaded image fragments, poor contrast, noise, etc. when preparing text documents pictures for recognition;
- supply of a set of handy service functions (data viewing at any stage of transformations, segmentation and anonymization of individual text fragments, selecting figures, saving the results of work in standard formats, printing outcomes;
- taking comprehensive measures to secure recovered confidential information when it is next transmitted through unsafe communication channels. It is desirable to design information protection so that the routine is universal and allows one to work with any text recognition system.

In [11], it is provided a detailed overview of applications for detecting printed text with the use of a convolutional neural network (CNN). The network extracts text related features from image components. It is proposed a training mechanism for a CNN by using such information as the character label and grayscale text images. This solution includes several stages, namely the pre-processing, segmentation, feature extraction and image classification. The obstacle lies in the fact that textual information of the picture can possess whatever fonts in addition to various sizes. It is shown what techniques should be taken at the stage of data preprocessing and when training the CNN. It is important to note that yet at the stage of training a neural network, it becomes necessary to foreprocess the original images.

Of interest is a technique used to improve the quality of optical character recognition by keywords that is based on deep convolutional neural networks [12]. It is applicable to protect personal information in document images. The method involves the key characters detection and vocabulary analysis and grounds on the RetinaNet network and transfer learning. To detect key characters in the given region of the document picture, the RetinaNet involves pyramidal convolutional layers and two subnets. This framework is superior in efficiency compared to the Tesseract OCR software.

Correction of shortcomings, such as projection geometric distortion of photographs of the original image, shaded picture fragments, picture poor contrast, etc., implies preliminary processing and images improvement so as to ensure proper identification and classification of text images. The complex of such algorithms is described in detail in [9]. However, a new, more efficient binary method for estimating the level of projective distortion at a point of the reconstructed image is proposed in [13]. This allows you to significantly improve the quality for geometric transformations of the position of documents photographs. Very useful results can be reached with the use of adaptive thresholds selection in the binarization of text images before the recognition procedure. These are given in [14, 15].

A constructive and in-detail example for the set of necessary service functions production is described in [10]. The major payload is carried by interactive procedures for segmentation and anonymization of the source text, the capability for viewing of data transformations at any stage of processing, and saving the results in standard formats.

Text documents protection after recognition ordinarily consists of two portions: a − data encoding; b − masking the fact of messages transporting when using the open network.

The classical approach to the problem of encoding textual information involves the use of cryptography methods [16, 17]. Though, encoding textual information by the use of QR-codes has recently become equally popular [18, 19]. It is simpler computationally and allows you to encode large amounts of textual information. In addition, the QR-code's image binary format is well combined with the formats, which are used in LSB-steganography for the conspiracy of message transmission. This is clearly shown in [20, 21]. The authors propose a new method for protecting text data.

It is important to note the role of estimation criteria and performance indicators. The entire system effectiveness is assessed primarily by the indicator that determines the number of correctly recognized text characters relative to their total quantity. Performance is considered acceptable at the factor 99%. Equally important is the indi-

cator of QR-codes capacity under text messages encryption and the assessment of the information capacity of steganographic data while transmitting them over communication channels. A marker of system good performance is also the factor of reticence of data transmission. It is determined by the degree of difference between an empty and filled steganographic cover image. An objective indicator of this difference is MSE (mean square error). At the same time in a number of works, the factors of different perception of these differences caused by observers' vision peculiarities are also taken into account [22, 23]. HSV (human vision system) can significantly improve the quality assessment of the steganography use.

3. The structure of up-to-date text recognition system

The accepted conception when designing intended a substantial improvement in the quality of text recognition systems; it provides for the implementation of the following mandatory provisions:

- assessment and consideration of external factors that negatively affect the result of the system operation; creation of image pre-processing algorithms to effectively compensate for the disturbing corruptions;
- providing a set of service functions aimed at conveniency of source data treatment, their viewing, converting and saving in standard formats, segmenting of particular text fragments, highlighting figures, etc;
- taking measures to protect text documents' information after recognition. To do this, providing for effective data coding together with hiding the fact of information transmission (when employing insecure communication channels) by the use of steganography techniques;
- conducting a comprehensive assessment of system effectiveness by a set of the most important quality indicators.

Within the concept framework, two types of systems for optical recognition of text documents can be created - without protecting information contained in the recognition outcome and secure ones required to transmit confidential data.

The first option of the text recognition system structure is shown in Fig. 1. It contains an archive of photographs of text documents and a data pre-processing unit to improve geometric distortions, to filter a noise out of photographs and increase their contrast, and to conduct the binarization before recognition; also it can supply an option for interactive selection of figures, diagrams and tables with the ability to save them in a standard format.

The system provides a set of necessary service functions (adjusting operative parameters, viewing the results of auxiliary transformations, saving results in various formats, printing, etc.).

At present, it is advisable to create a text recognition system in the Python programming language and using the resources of the OpenCV library [24, 25]. In this case, it is convenient to perform recognitions by the Tesseract engine and the related functional of the `pytesseract` library [26]. This allows you to create complex and functional options of the OCR system.

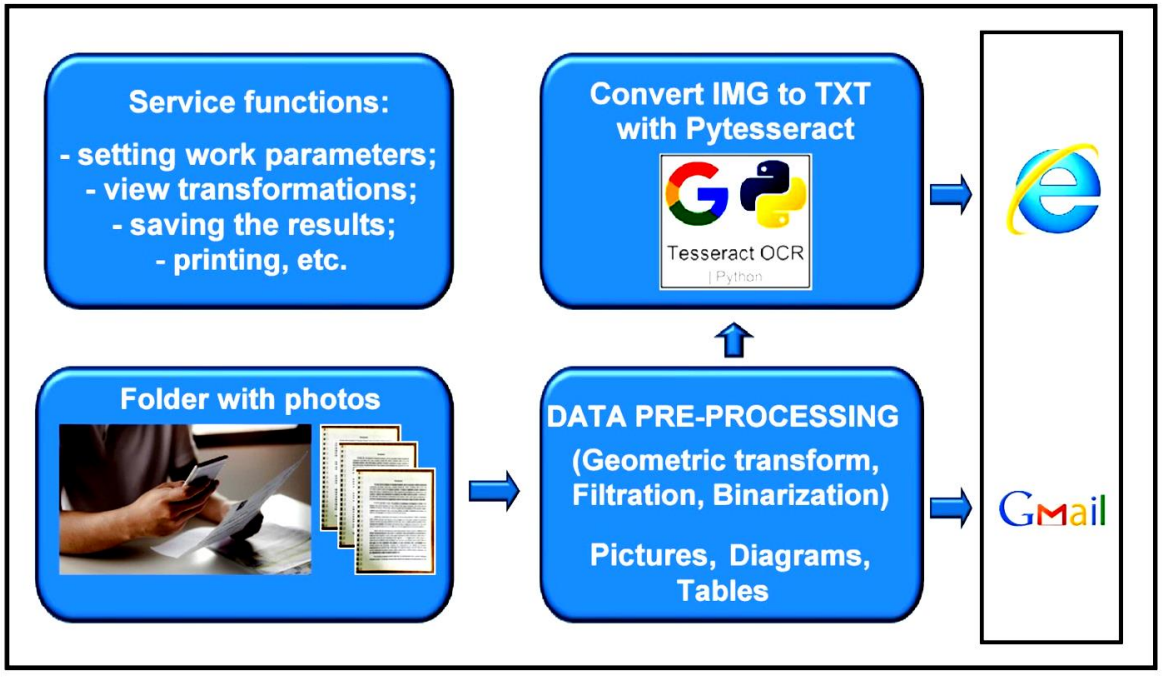


Fig. 1. Structure of textual data recognition system not getting info protection

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

During the work, the results of identification are recorded across a standard format, *.docx, and the images found in the text are extracted and saved in the *.png format. Then, as needed, these files can be sent by e-mail to users, but the information is not protected here. This is the main deficiency of the recognizing system of such a configuration.

To create means of protecting information, it is necessary to involve an encoding routine for secret messaging and to reliably mask with the use of steganography techniques the facts of data transmission. The general scheme for communication in secure mode is visually shown in Fig. 2. Participants in the "Sender - Receiver" process transmit and receive a stego image with a secret text embedded. A minor drawback of the method is that the "Receiver" had to gain the appropriate software to extract and decode required information. However, this method always solves reliably the problem of protecting information from unauthorized use by third parties.

Fig. 3. shows a generalized diagram of the transmitting portion of a text recognition system where software tools for encrypting text information with QR-codes and secreting the fact of data transmission with the use of LSB-steganography algorithms are depicted. In addition, the system uses a library of cover images to create steganographic files with secret messages attached to them. On-time change of the cover image contributes to additional information protection of unauthorized access. The procedure for steganographic files exchange is standard.

After text recognition, the received information must be saved in the form of a standard text file and next, if necessary, called for encoding and subsequent transmission to the network in the form of a stego image.

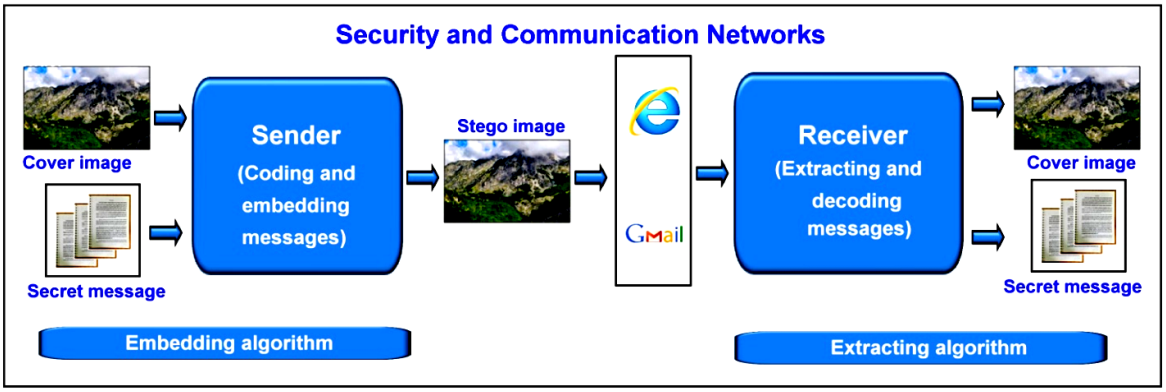


Fig. 2. General scheme of confidential data transfer in protected mode

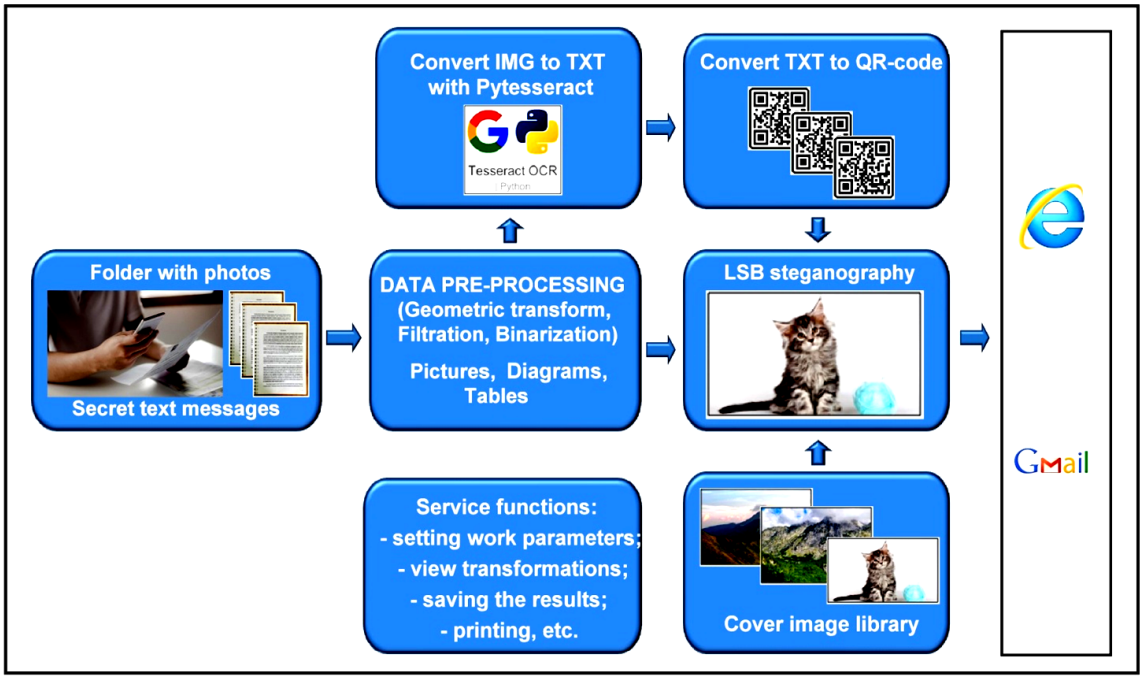


Fig. 3. Structure of the optical text recognition system with protecting information identified

4. Information treatment to supply encoding and steganography

For clarity of presentation, we take as an example of data treatment the HQ Scanner program described in detail by the authors in [9, 10]. After text recognition or calling `txt` files, the program displays text information in the dedicated preview window shown in Fig. 4. Any text recognition program should have a similar option.

In this window, you can add current text to an existing storage or create a new album by pressing the toolbar 1 button. This is important, as the volume of a recognized text document can exceed single page. Therefore, it is advisable to compose the files of individual pages into a generic album to reduce the amount of encoded data and for convenience. When necessary, one can also use the 4 and 5 buttons to change the font size of the text being viewed. Then the text is saved in "`.docx`" format by pressing the button 2.

Also, if you need secure data transfer, you can open the steganography preset window using button 4. The view of this window is shown in Fig. 5. It is seen that information about the current loading of the cover image and a set of cover images of different size is given here, as well as the ability to choose a method of steganography provided. Steganography outcomes are saved to the working directory in `*.png` format.

The HQ Scanner program applies two LSB-steganography techniques − replacing one or two least significant bits of the cover image with bits of the secret image being embedded. Therefore, the steganographic cover's filling percentage also differs by two. It is required to tend making the most of the cover volume and to replace the stego cover by the "Change cover image" button if necessary.

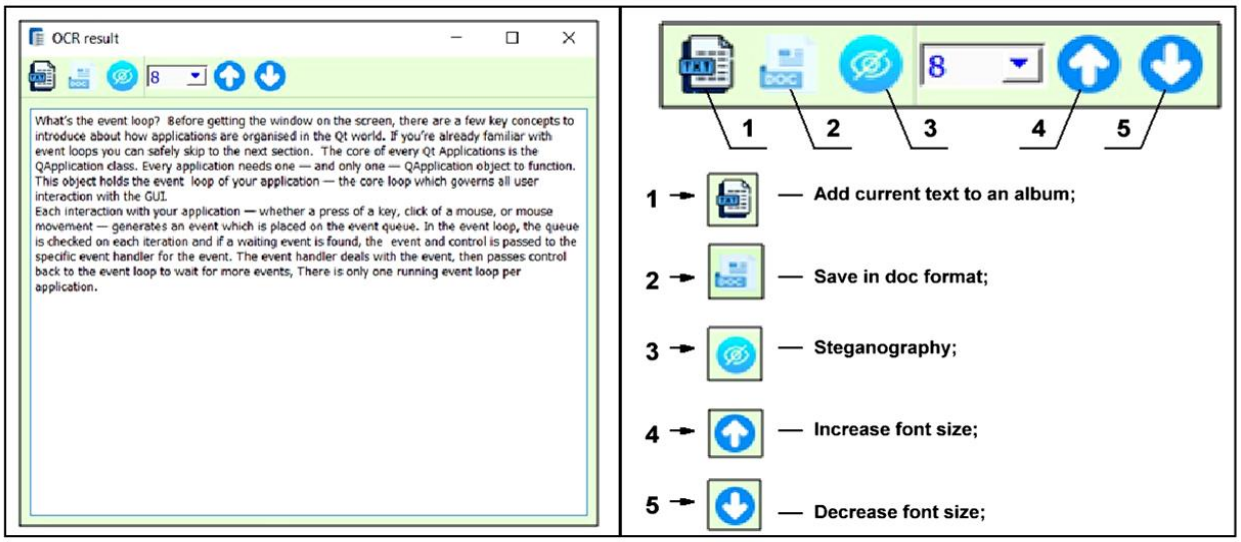


Fig. 4. Text content preview window

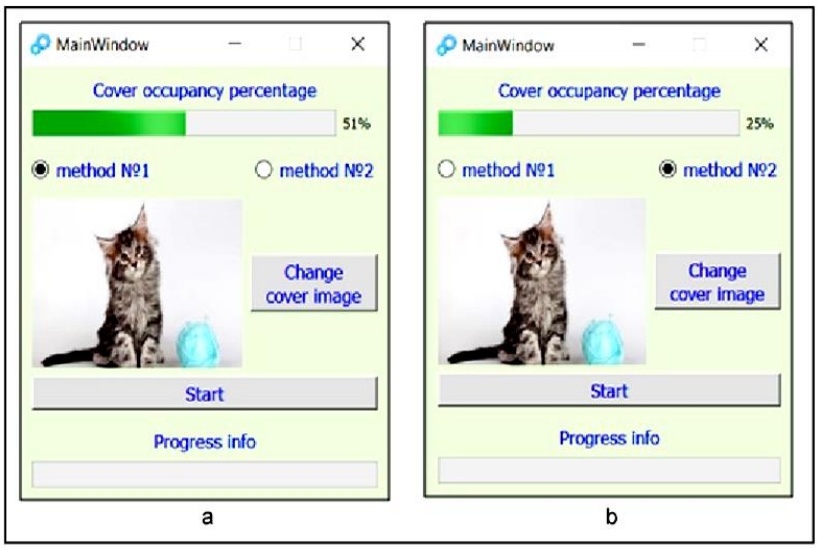


Fig. 5. Steganography settings window

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

5. Co-use of QR-codes and LSB-steganography

Text information secure transmission involves the generation of certain number of QR-codes needed to convert text data into images that mask these data on the LSB-steganography basis. At the same time, it is necessary to ensure the text segmentation into fragments, each matching the maximum possible text amount that the QR-code can fit. After, the QR-codes generated are subjected to appropriate transformations and, using LSB-steganography algorithms, are embedded in the cover image at places of the lower bits. The regular scheme for joint sharing of QR-codes and LSB-steganography is shown in Fig. 6.

Let us articulate the main challenges that inevitably arise in bringing the proposed combined method of data protection and consider the measures for their constructive solution.

At the first stage, it is necessary to generate an arbitrary number of QR-codes used to convert text data into images followed by data hiding by means of LSB-steganography. To do this, it is important to correctly assess the maximum allowable capacity of a single QR-code and determine its most important parameters.

Recall that the entire process of QR-code generation involves several stages: encoding data, adding service information and filling, decomposition of information into blocks, introduction of correcting bytes, uniting blocks; information positioning on the QR-code.

Let's emphasize the most important procedure – adding of the service information. At this stage, you need to specify the level of correction: the higher the level, the bigger the allowable image corruption and the less information over an equal size. There are 4 levels of correction: L (maximum 7% damage is allowed), M (15%), Q (25%), and H (30%). Mostly, the level M is used.

Another important feature of a QR-code is its version (the greater it is, the bigger the size). There are 40 versions in total. The version number depends on the amount of information being encoded and on the correction level. The output size of the QR-code matrix, hence directly the maximum possible number of characters that can be encoded, depends on the version chosen. The difference between characteristics of the minimum version 1 and the maximum version 40 can be seen through Table 1 (characteristics of intermediary versions missed for brevity).

There were determined the following features for handling QR-codes during the experiments:

1. When generating QR-codes, textual information is first converted into a binary format noted in the "Binary" column of Table. 1. Therefore, the maximum possible number of encoded text characters is 2953 for the QR-code version 40 at the correction method L.

2. Conversion to binary format is performed according to the "UTF-8" standards. This means that each character of the text represents 1 to 4 bytes of information. To control the fullness of QR-codes, each character of the text is converted into a binary format, followed by a check for overflow likelihood.

3. When the QR-code is completely filled in, errors may occur during information decoding. Therefore, a decision has been made to introduce a correction component of 20 bytes in size. This value was received experimentally and made it possible to completely eliminate errors during decoding.

4. The "L" method was chosen to correct errors in QR-codes, since it allows largest amount of encoded information to be handled. When encoding and decoding QR-codes, no errors were noticed. Therefore, there is no need to increase the correction degree.

Based on the results of the research, it was determined that (2953 - 20 = 2933) bytes of information can be encoded in one QR-code of the maximum version. 20 bytes of the information constitute the correction items; these intend to prevent eventual errors when decoding a fully filled QR-code.

After generating a set of QR-codes, it is necessary to solve the task of their effective embedding in the cover image. To undertake an improvement for the method efficiency, the following features of the input and output data were taken into account:

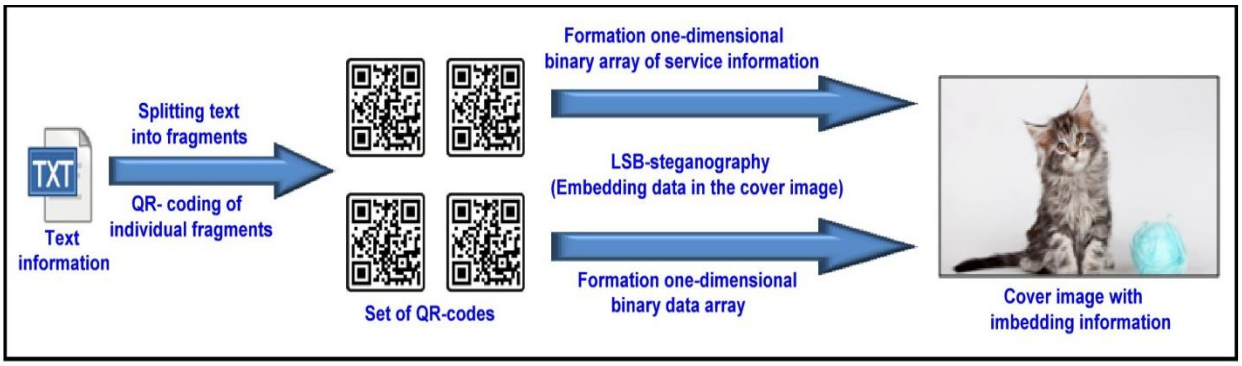


Fig. 6. Encryption with QR-codes and LSB-steganography

Table 1

Options for creating and characterizing QR-codes

Version	Modules	ECC level	Data bits (mixed)	Numeric	Alphanumeric	Binary
1	21x21	L M Q H	152 128 104 72	41 34 27 17	25 20 16 10	17 14 11 7
40	177x177	L M Q H	23648 18672 13328 10208	7089 5596 3993 3057	4296 3391 2420 1852	2953 2331 1663 1273

1. QR-code images are first converted to grayscale format. This reduces significantly the number of pixels in the image compared to the colored template (by a factor of three). Such a transformation does not introduce any errors, since the QR-code (binary by nature) is a combination of only black and white fragments.

2. In conventional LSB-steganography, each image pixel is represented in byte format followed by replacing bits of the cover image with bits of the image being embedded. However, when working with QR-codes, it is not necessary to store each bit of individual pixels. Therefore, it is proposed to encode only one data bit into the cover image instead of eight ones ('0' is assigned for black, and '1' – for white items). This approach increases the cover image potential capacity.

Feature for the data binary arrays and service information is shown in Fig. 6. The binary array of service information contains the records, which is required in the process of decoding textual information embedded in the cover image. The array size is 34 bits, in which: 24 bits declare the number of data pixels per one QR-code; 8 bits identify the number of encoded QR-codes; 2 bits determine the encoding method.

The binary data array, in turn, is a set of all the data bits for each of the encoded QR-codes. To build it, each QR-code is converted into a one-dimensional array of pixels (Fig. 7). Next the brightness index of each pixel is analyzed. As a result, one bit of data is added to the information array for each pixel of the original image, namely 0 for a black pixel, or 1 for the white pixel.

The process of encoding (embedding) this data in the cover image is conducted as follows (necessary steps are given right below).

1. The cover image is converted into a one-dimensional array of pixels, as shown in Fig. 8.

2. The service array information is put into the first 34 pixels (according to the scheme in Fig. 9).

3. The data array is being embedded into the cover image.

There are two techniques for embedding a data array. The first one supposes replacing the second last pixel bit of the cover image. It is by this method that the coding of service information takes place in Fig. 9.

The second method intends to replace the both last bits (Fig. 10) and allows you to halve the number of pixels required to embed the data of one QR-code into the cover image. The disadvantage of the second approach is a higher sensitivity to noise.

The final stage of embedding secret data is the inverse transformation of the cover image's pixel array into a three-dimensional matrix. The result is a transformed cover image with encrypted information inside.

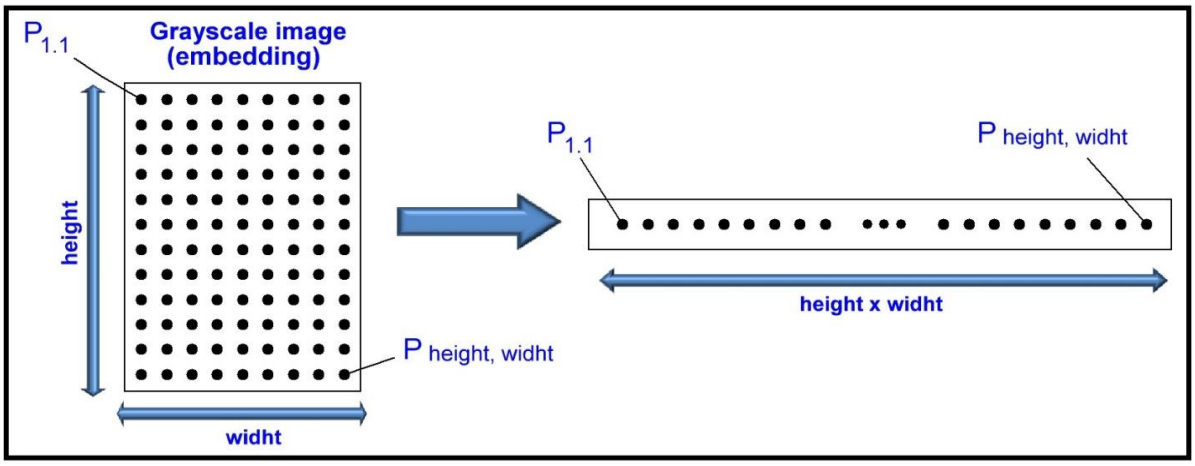


Fig. 7. Converting a grayscale image to a one-dimensional array

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

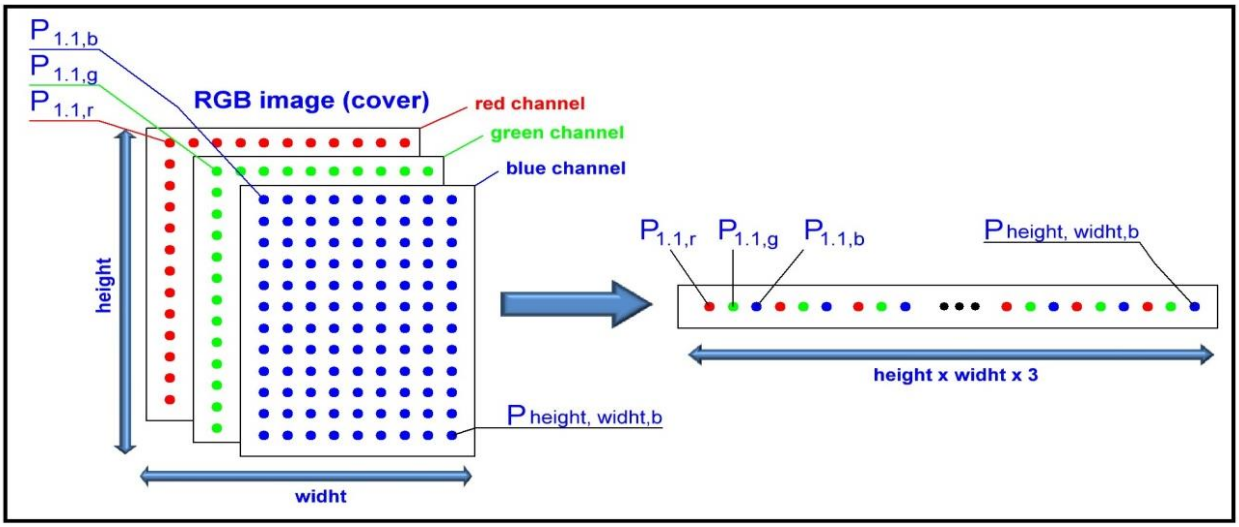


Fig. 8. Converting a color image to a one-dimensional array

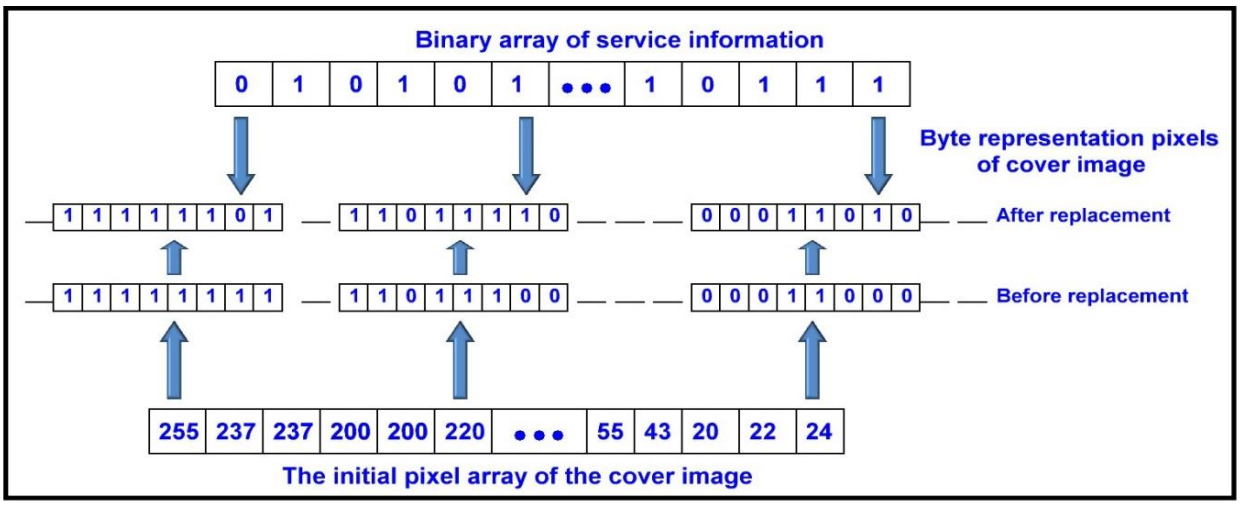


Fig. 9. Encoding service information

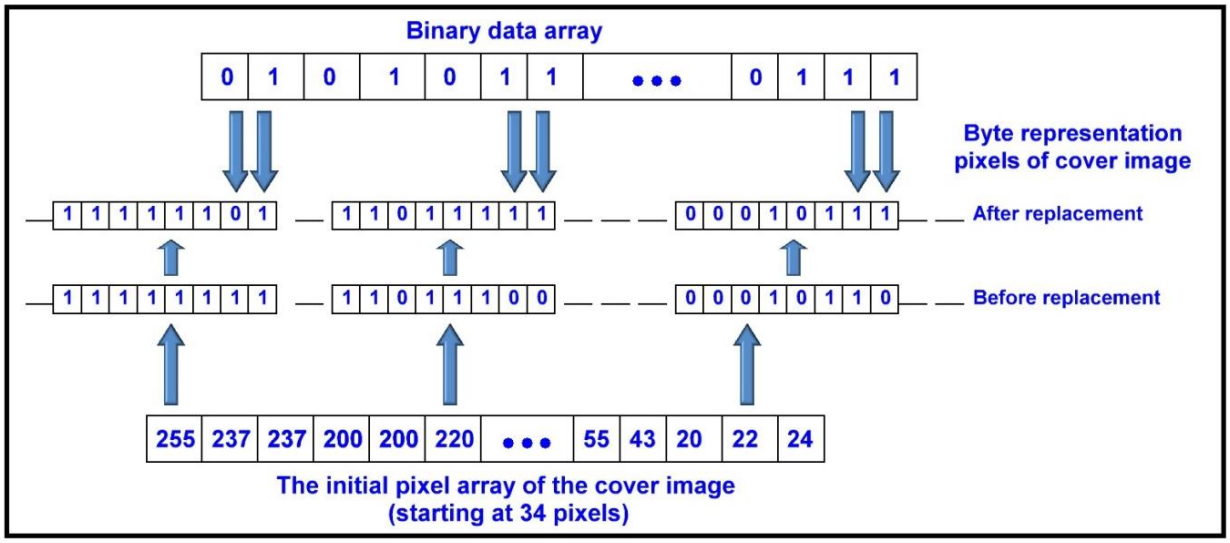


Fig. 10. Core data encryption

To extract textual information from the cover image, a reverse pass should be performed according to the scheme shown in Fig. 6. The service array is selected and decrypted from the cover image, and then the size and number of encoded QR-codes are determined.

6. Assessing measures for information protection

The efficiency of optical text recognition systems is assessed comprehensively with taking into account the quality of character recognition, the information steganography carriers' capacity, the extent of secrecy of transmitted data in communication sessions. The quality of OCR work was evaluated theoretically and experimentally. The OCR working quality was being evaluated theoretically and experimentally. That was described in detail in authors' previous paper [9]. Here we articulate the next two indicators.

6.1. Determination of the communication channel capacity

To evaluate the textual information coding efficiency, we introduce an indicator of information capacity. It reveals the loading of one pixel of the cover image:

$$I_c = \frac{N_{bytes}}{N_{pixels}},$$

where I_c gives the information capacity; N_{bytes} is the number of bytes of text that is encoded in the cover image; N_{pixels} is the number of pixels in the cover image.

Note that this indicator depends both on the encoding method chosen and the size of the cover image. This is due to the fact that the cover image has such number of pixels that was set freely before encrypting a QR-code. However, there are always present unused pixels that result in the assessment change as regards the maximum possible information capacity of this cover image. As for the QR-code images size, it was found in the course of experimental studies that its optimal value is 350x350 pixels. Using this size would allow you to avoid the errors, which occur while decoding a QR-code and trying to further compress its size.

Compare the information capacity estimates for two encoding methods applied to the cover images of standard sizes (Table 2).

It is obvious that the best information capacity can be achieved using 1024 x 768 cover images. This is due to the small number of unused pixels. The indicator values for the cover image of sizes 1280 x 1024, 1600 x 900, 1920 x 1080 are also well acceptable. The worst results were received for the 600 x 400 cover image. This is due to too many unused pixels at relatively small cover sizes.

One can also see a noticeable increase in the information capacity when using the second encoding method. This is due to a decrease in the actual number of pixels required to hide a single QR-code. It is worth to note that Table 2 shows the maximum possible values for each option of the cover image size. This can only be achieved if there are enough QR-codes. Therefore, in order to maximize the value of information capacity under working conditions, it is necessary to select the smallest container that can accommodate the required number of QR-codes.

6.2. Analysis of steganographic image quality

In practice, there are several popular indicators for assessing the quality of steganographic images. Principally, one can choose, when designing a communication system, any of them [22, 23]. Here are the most common measures that are used to compare embedded stego images S and cover images C of size $M \times N$:

1. **Peak-signal-to-noise ratio (PSNR)** is used as a statistical measure of the image quality, which is applied to estimate the cover image corruption due to extra embedding. Large PSNR gives rise a small distortions magnitude and leads to high image quality, while small values result in noticeable changes in steganographic images. Using the Human Visual System facility, this can be easily detected. PSNR is defined by the formula

Table 2

Information capacity of cover images with different sizes

Cover image size	Method 1		Method 2	
	Ic^{max}, bytes/pixel	Pixels remainder	Ic^{max}, bytes/pixel	Pixels remainder
600 x 400	$2.04 \cdot 10^{-2}$	107 466	$4.48 \cdot 10^{-2}$	46 216
800 x 600	$2.24 \cdot 10^{-2}$	92 466	$4.68 \cdot 10^{-2}$	31 216
1024 x 768	$2.36 \cdot 10^{-2}$	31 762	$4.72 \cdot 10^{-2}$	31762
1280 x 1024	$2.38 \cdot 10^{-2}$	12 126	$4.77 \cdot 10^{-2}$	12 126
1600 x 900	$2.37 \cdot 10^{-2}$	32 466	$4.75 \cdot 10^{-2}$	32 466
1920 x 1080	$2.35 \cdot 10^{-2}$	95 766	$4.76 \cdot 10^{-2}$	34 516

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}},$$

where the mean square error (MSE) is given by

$$\mathrm{MSE} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\mathrm{S}-\mathrm{C})^2 .$$

2. **Normalized-cross-correlation (NCC)**. NCC shows how strongly the steganographic image correlates with the cover. The NCC value ranges from 0 to 1. If the NCC value is 1, it means that stegoimages are completely resistant to various attacks while image processing. NCC is represented by the formula

$$\mathrm{NCC} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\mathrm{S}(i,j)\times\mathrm{C}(i,j)) \,/\, \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\big(\mathrm{S}(i,j)\big)^2 .$$

3. **Structural similarity index measurement (SSIM)**. SSIM is an image quality metric that compares two images (stego and cover) to conclude similarity between them; it is added as a PSNR improvement. SSIM takes form

$$\mathrm{SSIM}(\mathrm{C},\mathrm{S}) = \frac{(2\mu_\mathrm{C}\mu_\mathrm{S}+\mathrm{c}_1)\times(2\sigma_{\mathrm{CS}}+\mathrm{c}_2)}{(\mu_\mathrm{C}^2+\ \mu_\mathrm{S}^2+\mathrm{c}_1)\times(\sigma_\mathrm{C}^2\sigma_\mathrm{S}^2+\mathrm{c}_2)},$$

where μ_C is the mean C of the cover pixels, μ_S is the mean S of the stegoimage pixels, σ_C^2 is the variance of C, σ_S^2 is the variance of S, σ_{CS} is the covariance of C and S, $\mathrm{c}_1 = (\mathrm{K}_1\mathrm{L})^2$ and $\mathrm{c}_2 = (\mathrm{K}_2\mathrm{L})^2$ – two variables that stabilize the division when the denominator is close to zero, L – dynamic range of pixel values, K_1=0.01 and K_2=0.03 by default.

4. **Universal index Q** is used to assess images **visual quality**. Large values Q mean that the embedded image and the cover image are highly correlated and the difference between them is small. The universal quality index Q can be calculated using

$$\mathrm{Q} = \frac{4\sigma_{\mathrm{x,y}}\bar{\mathrm{x}}\bar{\mathrm{y}}}{\big(\sigma_\mathrm{x}^2+\sigma_\mathrm{y}^2\big)[(\bar{\mathrm{x}})^2+(\bar{\mathrm{y}})^2]},$$

where

$$\bar{\mathrm{x}} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\big(\mathrm{x}_{ij}\big),\ \bar{\mathrm{y}} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\big(\mathrm{y}_{ij}\big),$$

and the variance of individual components are calculated by the formulas:

$$\sigma_\mathrm{x}^2 = \frac{1}{(\mathrm{M}\times\mathrm{N})-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\big(\mathrm{x}_{ij}-\bar{\mathrm{x}}\big)^2,$$

$$\sigma_\mathrm{y}^2 = \frac{1}{(\mathrm{M}\times\mathrm{N})-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\big(\mathrm{y}_{ij}-\bar{\mathrm{y}}\big)^2,$$

$$\sigma_{\mathrm{xy}}^2 = \frac{1}{(\mathrm{M}\times\mathrm{N})-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\big(\mathrm{x}_{ij-}\bar{\mathrm{x}}\big)\big(\mathrm{y}_{ij}-\bar{\mathrm{y}}\big),$$

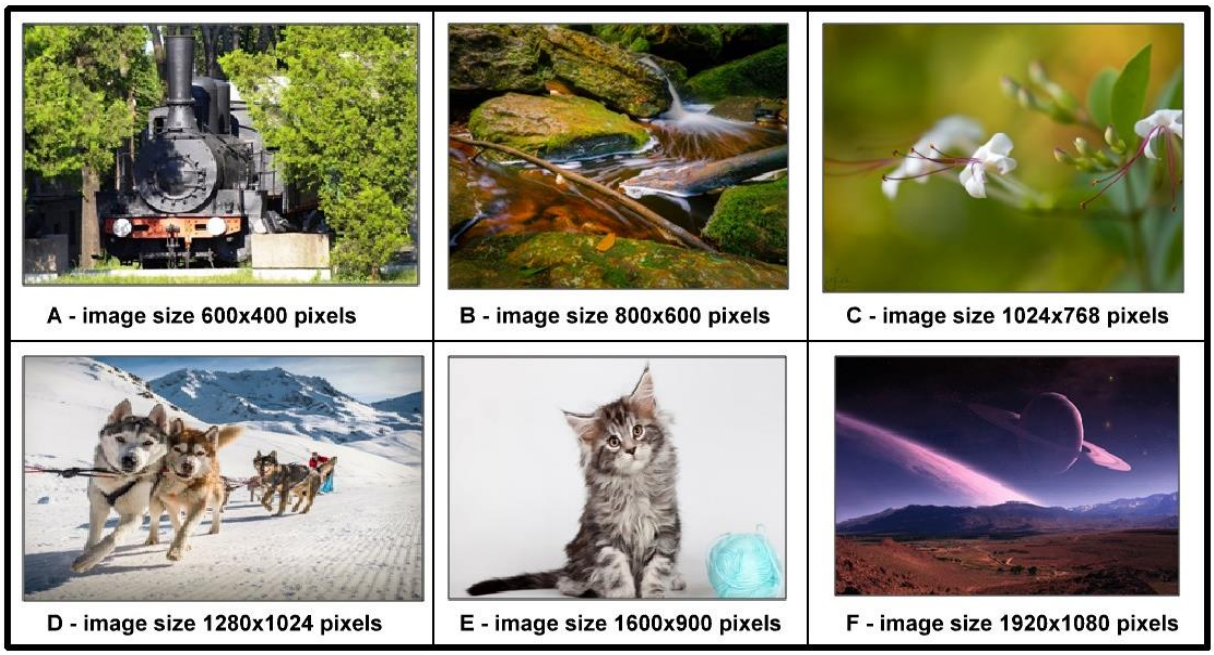
where x is the pixel value of the cover image, y is the pixel value of the stego image, $\bar{x}$ is the *x* mean, $\bar{\mathrm{y}}$ is the *y* mean, and σ_x^2, σ_y^2 and σ_{xy}^2 are the variance and covariance of x and y images, respectively.

6.3. Results of experimental studies

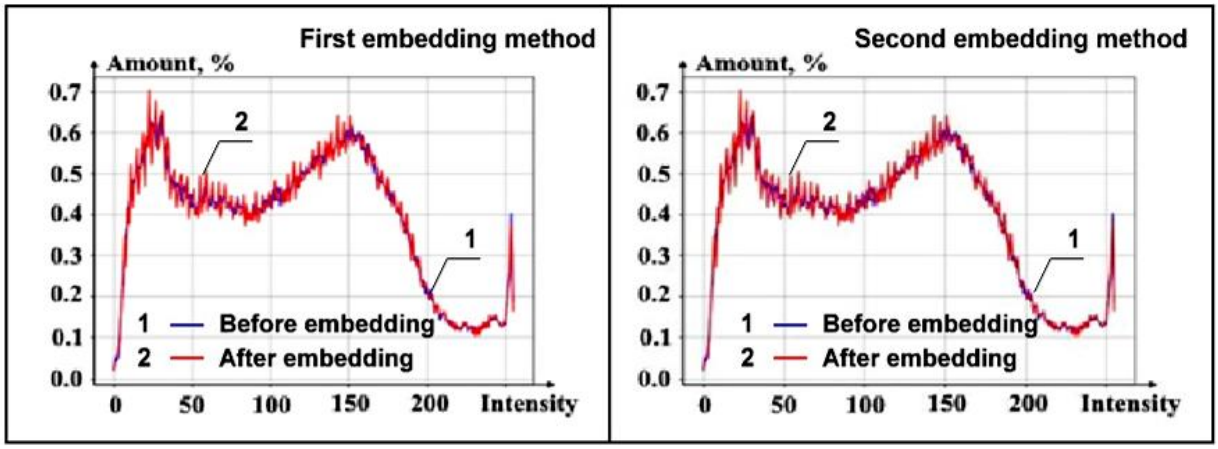
As secrecy of the fact of data transmission is that intends the most important indicator of the information protection system, experimental studies were carried out to evaluate corruption of the cover image after embedding a confidential image. To provide this, a library of cover images of various sizes and with scenes of different lightness (light and dark pictures) was created. A set of these images shown in Fig. 11, a.

To conduct research, the visual and objective characteristics of the cover image were applied before and after the procedure for embedding QR-code images with confidential text; the proposed two LSB-steganography encryption techniques were involved. On the authors, the most descriptive characterization of the attributes and view of the cover image before and after steganographic transformations is the normalized histogram for the brightness distribution. For ease of collation, the histograms before and after conversion are shown in different colors in one window using the direct overlay method. The case study diagrams are shown in Fig. 11, b … g. The analysis verifies that the proposed procedures for embedding QR-codes with encrypted text do not introduce noticeable distortions into the cover image, regardless of its size and brightness distribution in the picture field. These distortions constitute fractions of a percent of the total number of pixels of related brightness. Therefore, we can confidently suppose that these deformations will not be noticeable when using both the first and second methods of substituting the byte's least significant bits for each pixel (one or two bits, correspondingly). Note that the deviations of the two histograms of the cover image are of a chaotic noise nature.

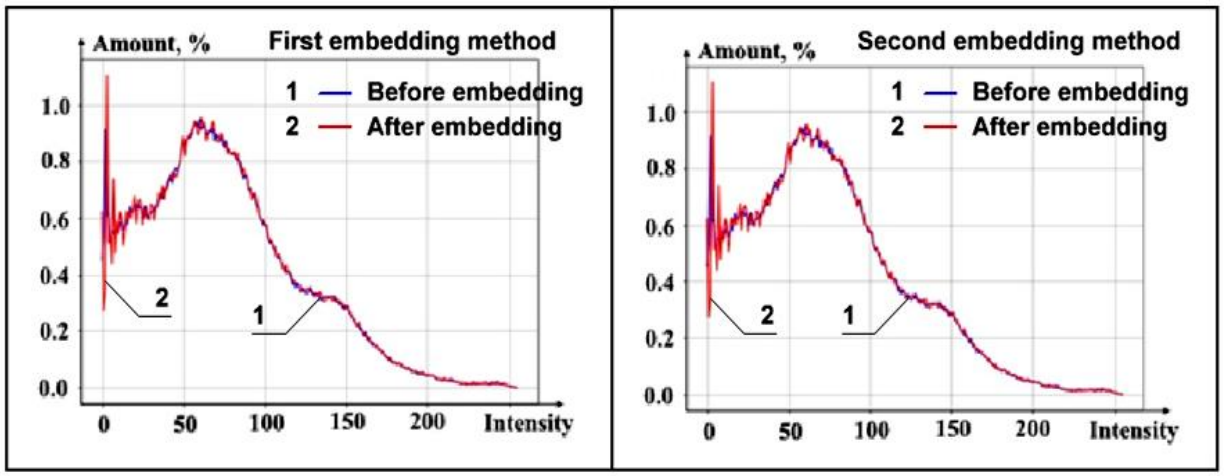
Quantitative analysis of errors, which result through steganographic transformations, utilized statistical methods. It was examined the relationship between the PSNR index and the number of QR-code images of maximum information capacity nested in a cover image of known size. The results of these studies are summarized in Fig. 12. Herein there are presented the options used to calculate the PSNR index for the both ways of LSB-steganography; these were offered to replace the least significant bits in the string of bits that characterize every pixel brightness values. It is clear that the most advantageous PSNR values (large ones that get on 55 ... 60 dB level) are typical for a small number of embedded



a − Cover images library for testing quality of steganographic transformations



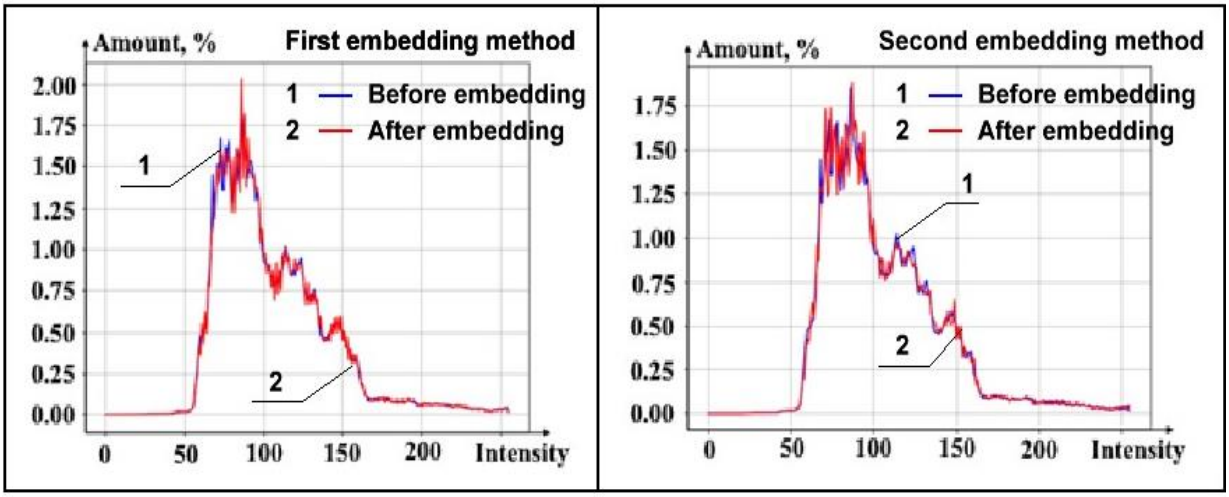
b – histograms for A cover image



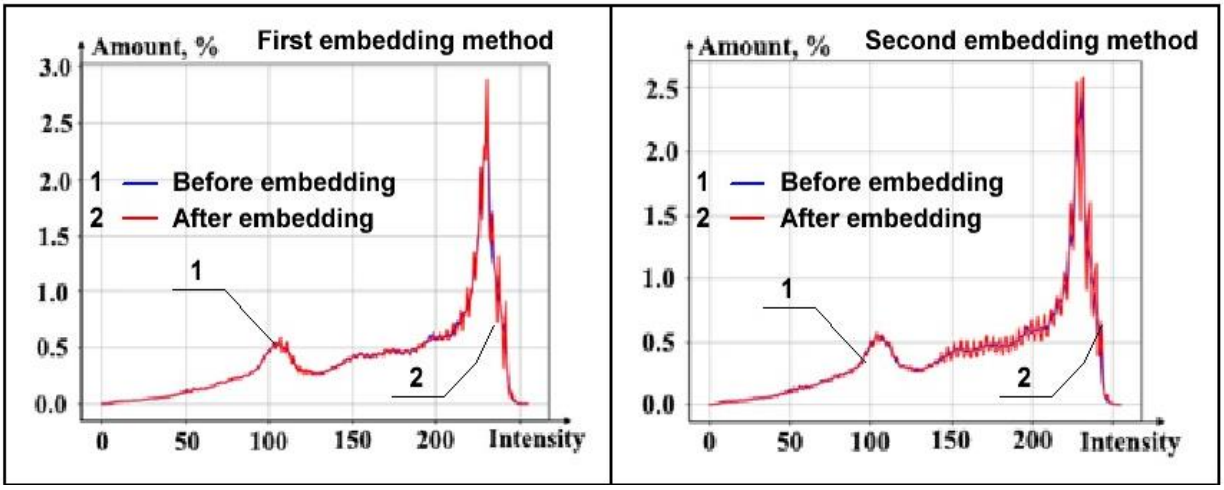
c – histograms for B cover image

Fig. 11. Library cover images of different dimensions and their histograms before and after steganography

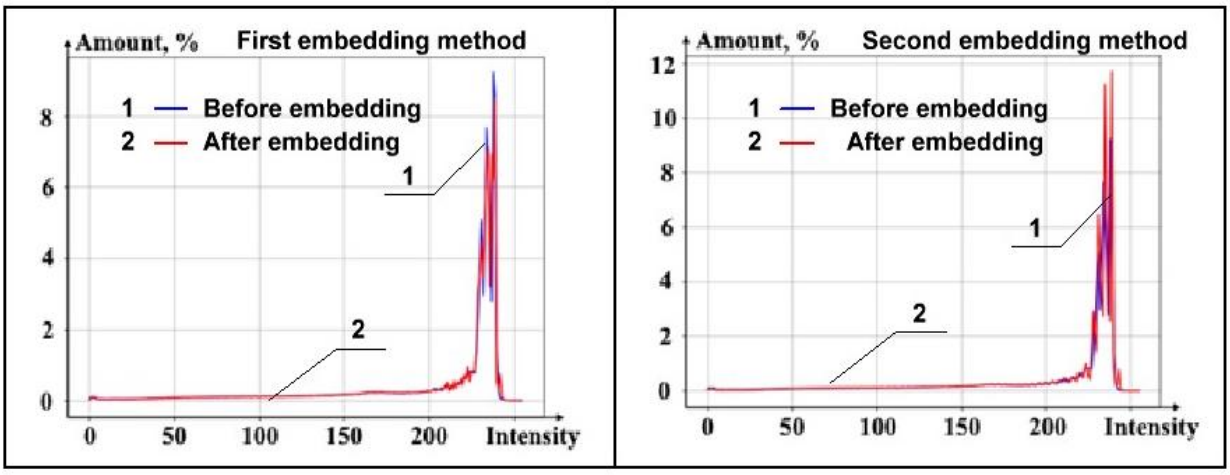
ISSN 1814-4225 (print)
ISSN 2663-2012 (online)



d − histograms for C cover image

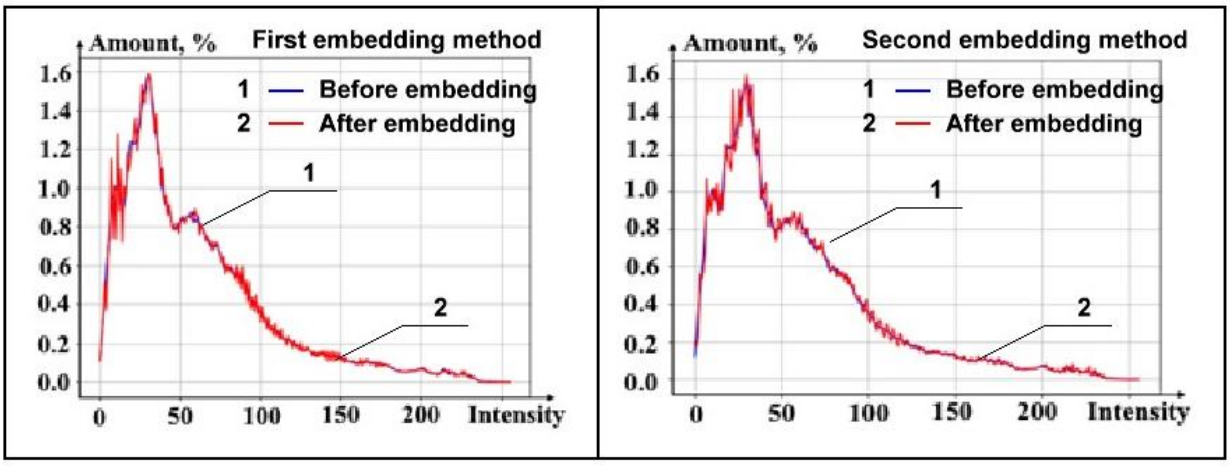


e − histograms for D cover image



f − histograms for E cover image

Fig. 11. Library cover images of different dimensions and their histograms before and after steganography



g – histograms for F cover image

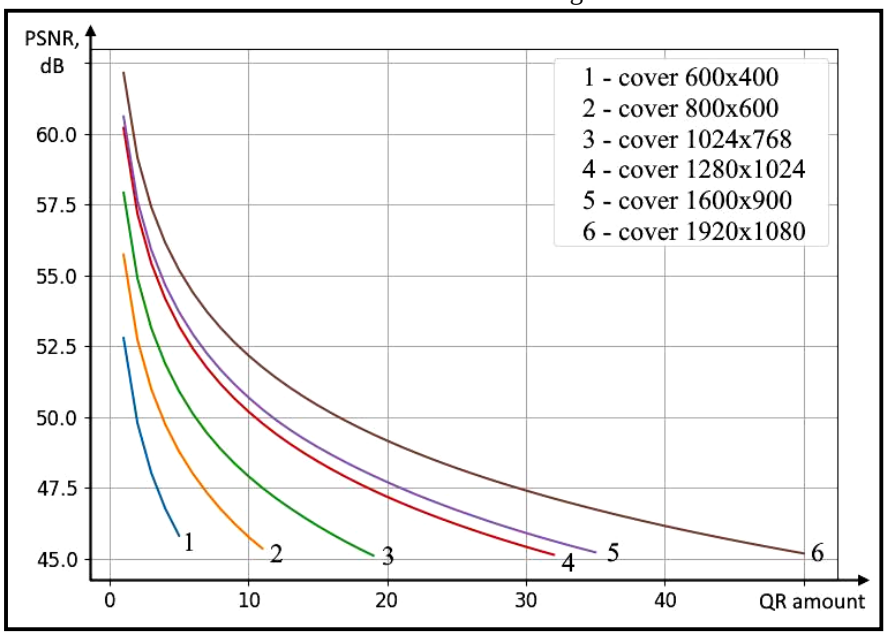
Fig. 11. Library cover images of different dimensions and their histograms before and after steganography

QR-codes, since the area of the embedded image occupied is the least. The PSNR indicator drops exponentially as the number of QR-codes being embedded increases, hence the masking quality of facts of the secret messages transmission decreases. The most appropriate choice is a large cover and a relatively small number of QR-codes.

Fig. 13 shows the influence of the number of QR-codes nested in the container image of various sizes on the CCN index. This effect was examined for the both discussed methods of the least significant bits embedding into a byte that represents the pixel brightness of the cover image.

For both encryption techniques, the correlation between them is very high (NCC ~ 0.9999) and it depends a little on the increase in the number of embedded QR-codes. The decrease in NCC brings a linear fashion. A high degree of cross-correlation between the stego image and the cover image provides resistance to various attacks while image processing, which indicates the correct approach to choose between data encoding techniques.

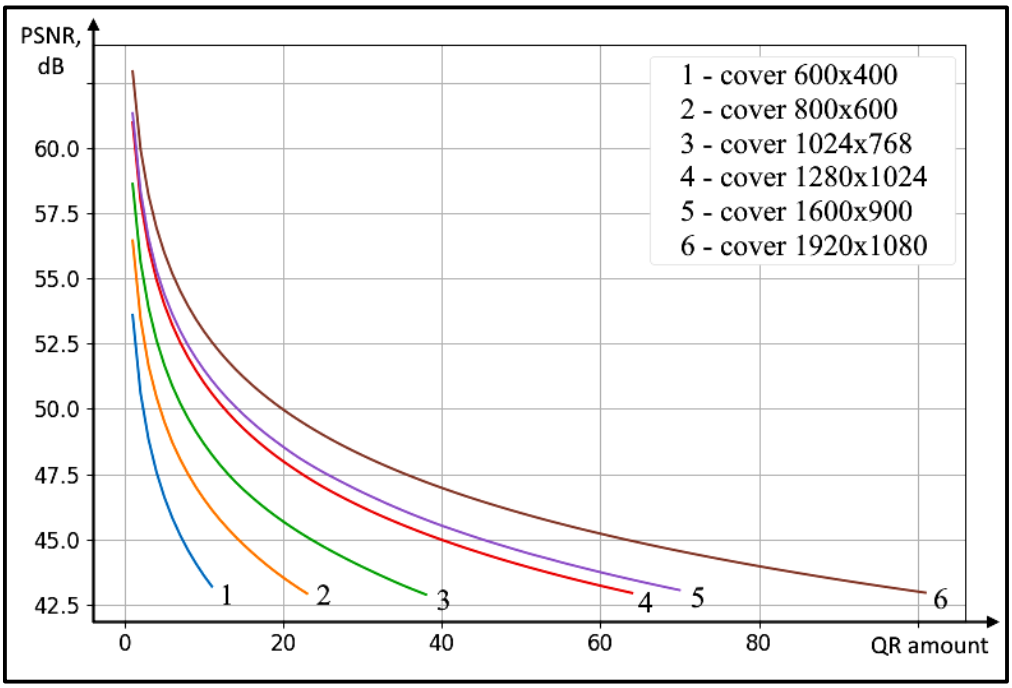
According to the experimental studies results, it can be concluded that the proposed methods for encrypting information using QR-codes are greatly effective. Corresponding images contain a lot text data. The data transmission masking by LSB-steganography provides good secrecy along with a minimum level of distortion of the cover image.



a – first embedding method

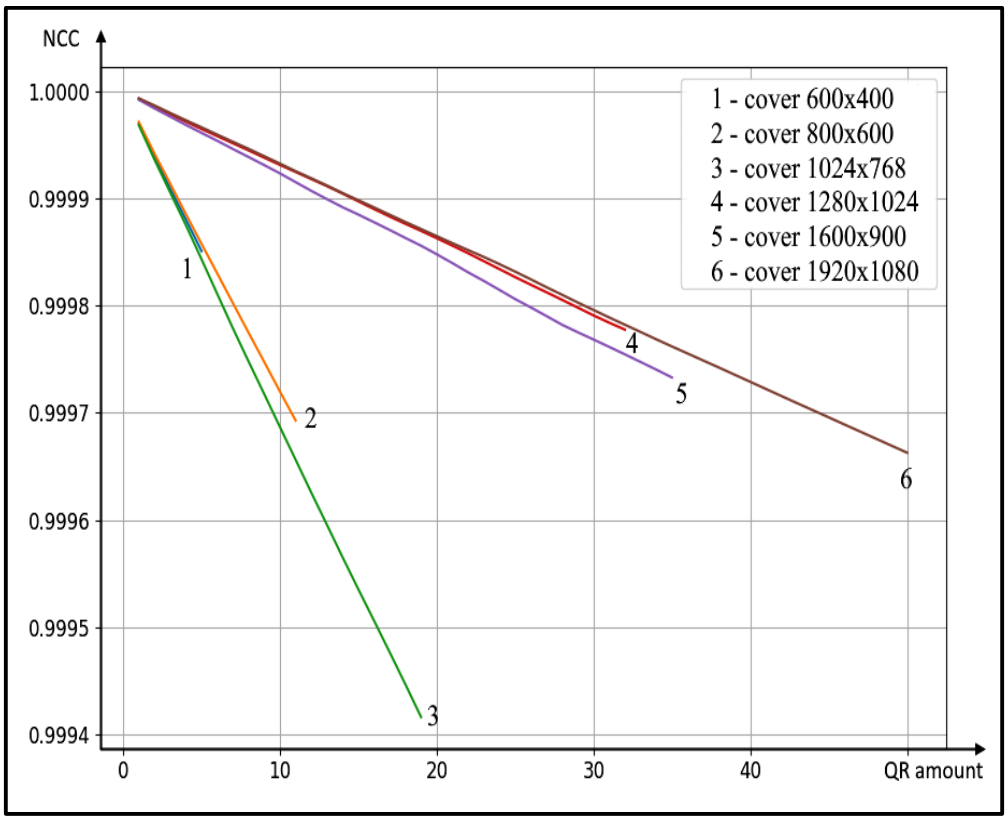
Fig. 12. The number of embedded QR-codes effect on PSNR

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)



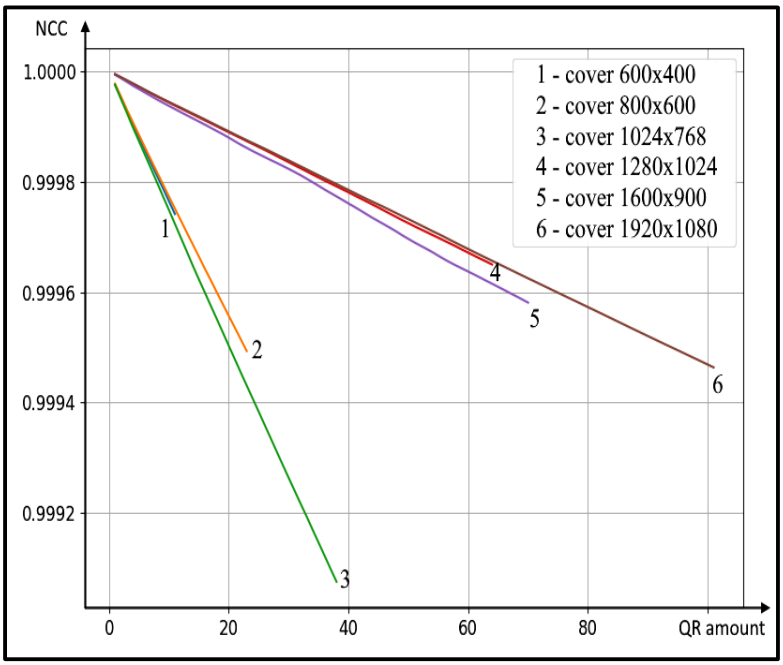
b - second embedding method

Fig. 12. The number of embedded QR-codes effect on PSNR



a − first embedding method

Fig. 13. NCC− cross-correlation index research



b – second embedding method

Fig. 13. NCC– cross-correlation index research

6.4. Main conclusions based on the results of experimental studies

One of the main requirements of the concept formulated by the authors for the construction of modern OCR systems is measures to protect information after recognition of text documents. This implies efficient encryption of confidential data and reliable masking of information transmission over insecure communication channels. These goals can be achieved in various ways. Therefore, the effectiveness of certain technical solutions can only be evaluated experimentally and comprehensively.

Noise-immune QR-codes make it possible to relatively simply and reliably encode large amounts of text data. One QR-code allows you to encode ~ 3 Kb of information, which is more than a page of standard typewritten text. This is much preferable to using complex cryptographic algorithms.

The effectiveness of data transmission secrecy by steganography methods is evaluated by a set of the most important quality indicators. They are divided into two groups – objective (based on the analysis of the statistical characteristics of stegan tools) and visual. They must take into account the properties of the HVS (human visual system). In addition, indicators of information load (information capacity) of cover image pixels are also very important. It should be noted that for the first time the authors used an original visual quality marker – normalized histograms of the cover image brightness distribution before and after steganographic transformations, displayed in one window using the direct overlay method. This clearly shows the nature of the distortions introduced when embedding images of QR-codes in the cover image.

Note also that the use of algorithms LSB-steganography in combination with encryption of text data with QR codes gives good results in terms of quality. This approach is in no way inferior to methods such as color image steganography based on adaptive directional pixel value difference (P-ADPVD) methods for embedding a secret message in different directions of edges of cover images and oriented gradient histogram (HOG) methods. However, the proposed method for combining LSB steganography with QR-codes is much simpler in terms of computation.

According to the results of the research, we recommend using the visualization of the main quality indicators (PSNR, correlation CCN-index, etc.) when developing or upgrading modern OCR systems at the stage of selecting and configuring steganography algorithms. This will estimate the expected level of distortion, and if necessary, you can choose a cover image of other sizes. This will allow you to effectively manage the process of transferring messages in secure mode.

Conclusion

Currently, information security has become one of the most important problems due to the sharp increase in data transmission through social networks and cloud services. The Internet is used to transmit large amounts of data over open networks and insecure channels. This exposes personal and sensitive data to a serious risk, which

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

means that it is necessary to develop technologies for protecting confidential messages. Therefore, the research carried out is relevant and useful. Sharing Guidelines QR-codes and LSB-steganography methods for encoding and covert transmission of text information are universal in nature and can be used to build new and upgrade existing optical text recognition systems. The work has a clearly expressed practical orientation. The proposed algorithms are implemented as software modules in the Python programming language and the OpenCV library. The indicators of the quality of work of various methods of coding and data protection have been experimentally studied.

The authors plan to further explore other digital image-based steganographic approaches as cover for transmitted data using various evaluation metrics, including stealth, visual quality, and security.

Contribution of the authors: analysis of present information resources related to quality of text recognition systems improvement, setting the task of studying methods and algorithms required to protect information in optical text recognition systems; requirements development for practical implementation of the tools – **K. Dergachov;** encryption with using QR-codes of confidential information received in the result of text recognition; applying of LSB-steganography algorithms when transmitting the information via open communication channels (e.g., e-mail); several protection algorithms suggested have been implemented – **L. Krasnov;** selection, involvement and optimization of modern programming techniques and relevant information resources for implementation of advanced information protection algorithms; run and testing of the developed software; conducting experiments – **V. Bilozerskyi;** formulation of the main conclusions on the results of the study and recommendations for their practical use, general editing of the article, translation of source materials from Ukrainian into English – **A. Zymovin**. All the authors have read and agreed on publication for manuscript version.

References (GOST 7.1:2006)

1. A Study on Optical Character Recognition-Techniques [Text] / N. Sahu, M. Sonkusare // The International Journal of Computational Science, Information Technology and Control Engineering (IJCSITCE). – 2017. – Vol. 4, No. 1. – 14 p. DOI: 10.5121/ijcsitce.2017.4101.

2. Offline optical character recognition (OCR) method: An effective method for scanned documents [Text] / Mujibur Rahman Majumder et al. // 22nd International Conference on Computer and Information Technology (ICCIT) – 2019. – P. 1-5. DOI: 10.1109/ICCIT48885.2019.9038593.

3. Improved OCR quality for smart scanned document management system [Text] / Anh Phan Viet et al. / Journal of Science and Technique − Le Quy Don Technical University. – 2020. − No. 210. – P. 51-67.

4. Tesseract − ocr/Tesseract [Electronic resource]. – Available at: https://github.com/tesseract-ocr/tesseract. − 17.01.2022.

5. Python-tesseract − Optical character recognition (OCR) tool for Python [Electronic resource]. – Available at: https://pypi.org/project/pytesseract/. − 17.01.2022.

6. Image to Text Conversion Using Tesseract [Text] / N. Pawar, Z. Shaikh, P. Shinde, Y. Warke // International Research Journal of Engineering and Technology (IRJET). – 2019, – Vol. 6, iss. 2. – P. 516-519.

7. Abby Fine Reader (Сканер с искусственным интеллектом для оцифровки в PDF и распознавания текста): [Электронный ресурс]. – Режим доступа: https://www.abbyy.com/ru/finereader/. – 17.01.2022.

8. OCRopus − OCR-система для распознавания текстов tesseract на базе [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/OCRopus – 17.01.2022.

9. Data pre-processing to increase the quality of optical text recognition systems [Text] / K. Dergachov et al. // Радіоелектронні і комп'ютерні системи. − 2021. – № 4(100). – С. 183-198. DOI: 10.32620/reks.2021.4.15.

10. Methods and algorithms for protecting information in optical text recognition systems [Text] / K. Dergachov, et al. // Радіоелектронні і комп'ютерні системи. − 2022. – № 1(101). – P. 154-169. DOI: 1032620/reks.2022.1.12.

11. Optical Character Recognition Techniques: A Review [Text] / S. Srivastava, A. Verma, S. Sharma // IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). − 2022. – P. 1- 6. DOI: 10.1109/SCEECS54111.2022. 9740911.

12. Keyword Detection Based on RetinaNet and Transfer Learning for Personal Information Protection in Document Image [Text] / G.-S. Lin et al. // Appl. Sci. – 2021. – Vol. 11, Iss. 20. – Article No. 9528. DOI: 10.3390/app11209528.

13. A Method of Image Quality Assessment for Text Recognition on Camera-Captured and Projectively Distorted Documents [Text] / J. Shemiakina, et al. // Mathematics. – 2021. – Vol. 9, Iss. 17. – Article No. 2155. DOI: 10.3390/ math9172155.

14. Business Process Automation: A Workflow Incorporating Optical Character Recognition and Approximate String and Pattern Matching for Solving Practical Industry Problems [Text] / C. de Jager et al. // Appl. Syst. Innov. – 2019. – Vol. 2, No. 4. – Article No. 33. DOI: 10.3390/asi2040033.

15. Manual character recognition with OCR [Text] / Sasmitha Kumari Sahu et al. // Project. – 2021. DOI: 10.13140/RG.2.2.32608.81927.

16. A New Approach of Cryptography for Data Encryption and Decryption [Text] / K. I. Masud, et al. // 5th International Conference on Computing and Informatics (ICCI). – 2022. − P. 234-239. DOI: 10.1109/ ICCI54321.2022.9756078.

17. Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content [Text] / P. William, et al. // International Conference on Electronics and Renewable Systems (ICEARS). – 2022. – P. 918-922. DOI: 10.1109/ICEARS53579.2022. 9751932.

18. Ahamed, M. S. A Secure QR Code System for Sharing Person-al Confidential Information [Text] / M. S. Ahamed, H. Mustafa Asiful // International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2). – 2019. – P. 1-4. DOI: 10.1109/IC4ME247184.2019.9036521.

19. Some Methods of QR code Transmission using Steganography [Text] / D. F. Pastukhov et al. // World of transport and transportation. − 2019. – Vol. 17, Iss. 3. – P. 16–39.

20. QR code image steganography (LSB BIT) with secret image (MSB BIT) using AES cryptography and JPEG compression [Text] / R. Rituraj et al. // Recent Scientific Research. − 2019. – Vol. 9, Iss. 7. – P. 27820-27826.

21. Efficiency Assessment of the Steganographic Coding Method with Indirect Integration of Critical Information [Text] / O. Yudin et al. // IEEE Internation-al Conference on Advanced Trends in Information Theory (ATIT). – 2019. – P. 36-40. DOI: 10.1109/ATIT49449. 2019.9030473.

22. Li, F. Two-step providing of desired quality in lossy image compression by SPIHT [Text] / F. Li, S. Krivenko, V. Lukin // Радіоелектронні і комп'ютерні системи. − 2020. – № 2(94). – С. 22-32. DOI: 10.32620/reks.2020.2.02.

23. Objective Quality Metrics in Correlation with Subjective Quality Metrics for Steganography [Text] / R. Wazirali et al. // Asia-Pacific Conference on Computer Aided System Engineering. – 2015. – P. 238-245. DOI: 10.1109/APCASE.2015.49.

24. Python Developer's Guide [Electronic resource]. – Available at: http://python.org. – 17.01.2022.

25. OpenCV Tutorials − Image Processing (imgproc module) [Electronic resource]. – Available at: https://opencv.org/ – 17.01.2022.

26. Python-tesseract − Optical character recognition tool for Python [Electronic resource]. – Available at: https://pypi.org/ project/pytesseract/. − 17.01.2022.

References (BSI)

1. Sahu, N., Sonkusare, M. A Study on Optical Character Recognition-Techniques. *The International Journal of Computational Science, Information Technology and Control Engineering* (IJCSITCE), 2017, vol. 4, no. 1. 14 p. DOI: 10.5121/ijcsitce.2017.4101.

2. Mujibur Rahman Majumder et al. Offline optical character recognition (OCR) method: An effective method for scanned documents. *22nd International Conference on Computer and Information Technology (ICCIT)* – 2019, pp. 1-5. DOI: 10.1109/ICCIT48885. 2019. 9038593.

3. Viet, Anh Phan. et al. Improved OCR quality for smart scanned document management system. *Journal of Science and Technique − Le Quy Don Technical University*, 2020, no. 210, pp. 51-67.

4. *Tesseract − ocr/Tesseract.* Available at: https://github.com/tesseract-ocr/tesseract. (accessed 17.01.2022).

5. *Python-tesseract − Optical character recognition (OCR) tool for Python*. Available at: https: //pypi.org/project/ pytesseract/. (accessed 17.01.2022).

6. Pawar, N., Shaikh, Z., Shinde, P., Warke, Y., Image to Text Conversion Using Tesseract. *International Research Journal of Engineering and Technology (IRJET)*, 2019, vol. 6, iss. 2, pp. 516-519.

7. Abbyy Finereader (Skaner s iskusstvennym intellektom dlya otsifrovki v PDF i raspoznavaniya teksta) [Abbyy Finereader (Scanner with artificial intelligence for digitizing to PDF and OCR)]. Available at: https://www.abbyy.com/ru/finereader/ (accessed 17.01.2022).

8. OCRopus − OCR-sistema dlya raspoznavaniya tekstov na baze tesseract [OCRopus − tesseract based OCR system for text recognition]. Available at: https://ru.wikipedia.org/wiki/Cognitive_Technologies (accessed 17.01.2022).

9. Dergachov, K. et al. Data pre-processing to increase the quality of optical text recognition systems. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2021, no. 4(100), pp. 183-198. DOI: 10.32620/reks.2021.4.15.

10. Dergachov, K. et al. Methods and algorithms for protecting information in optical text recognition systems. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2022, no. 1(101), pp. 154-169. DOI: 1032620/reks.2022.1.12.

11. Srivastava S., Verma A., Sharma, S. Optical Character Recognition Techniques: A Review. *IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2022. pp. 1-6. DOI: 10.1109/SCEECS54111.2022. 9740911.

12. Lin, G.-S. et al. Keyword Detection Based on RetinaNet and Transfer Learning for Personal Information Protection in Document Image. *Appl. Sci.*, 2021, vol. 11, iss. 20, article no. 9528. DOI: 10.3390/app11209528.

13. Shemiakina, J. et al. A Method of Image Quali-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ty Assessment for Text Recognition on Camera-Captured and Projectively Distorted Documents. *Math-ematics*, 2021, vol. 9, iss. 17, article no. 2155. DOI: 10.3390/math9172155.

14. De Jager, C. et al. Business Process Automation: A Workflow Incorporating Optical Character Recognition and Approximate String and Pattern Matching for Solving Practical Industry Problems. *Appl. Syst. Innov.*, 2019, vol. 2, no. 4, article no. 33. DOI: 10.3390/asi2040033.

15. Sasmitha Kumari Sahu et al. Manual character recognition with OCR. *Project*, 2021. DOI: 10.13140/RG.2.2.32608.81927.

16. Masud, K. I. et al. A New Approach of Cryptography for Data Encryption and Decryption. *5th International Conference on Computing and Informatics (ICCI)*, 2022, pp. 918-922. DOI: 10.1109/ICEARS53579. 2022.9751932.

17. William, P. et al. Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content. *International Conference on Electronics and Renewable Systems (ICEARS)*, 2022, pp. 918-922. DOI: 10.1109/ICEARS 53579.2022. 9751932.

18. Ahamed, M. S., Asiful, Mustafa H. A Secure QR Code System for Sharing Personal Confidential Information. *International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*, 2019, pp. 1-4. DOI: 10.1109/IC4ME 247184.2019.9036521.

19. Pastukhov, D. F. et al. Some Methods of QR code Transmission using Steganography. *World of transport and transportation*, 2019, vol. 17, Iss. 3, pp. 16–39.

20. Rituraj, R. et al. QR code image steganography (LSB BIT) with secret image (MSB BIT) using AES cryptography and JPEG compression. *International Journal of Recent Scientific Research*, 2019, vol. 9, Iss. 7, pp. 27820-27826.

21. Yudin, O. et al. Efficiency Assessment of the Steganographic Coding Method with Indirect Integration of Critical Information. *IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, 2019, pp. 36-40. DOI: 10.1109/ATIT49449.2019. 9030473.

22. Li, F., Krivenko, S., Lukin, V. Two-step provsding of desired quality in lossy image compression by spiht. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 2(94), pp. 22-32. DOI: 10.32620/reks.2020.2.02.

23. Wazirali, R. et al. Objective Quality Metrics in Correlation with Subjective Quality Metrics for Steganography. *Asia-Pacific Conference on Computer Aided System Engineering*, 2015, pp. 238-245, DOI: 10.1109/APCASE.2015.49.

24. *Python Developer's Guide*. Available at: http://python.org (accessed 17.01.2022).

25. *OpenCV Tutorials − Image Processing (imgproc module)*. Available at: https://opencv.org/ (accessed 17.01.2022).

26. *Python-tesseract − Optical character recognition (OCR) tool for Python*. Available at: https: //pypi.org/project/pytesseract/.(accessed 17.01.2022).

Надійшла до редакції 19.02.2022, розглянута на редколегії 15.04.2022

РОЗРОБКА ЗАСОБІВ ІНФОРМАЦІЙНОГО ЗАХИСТУ ДЛЯ СИСТЕМ ОПТИЧНОГО РОЗІЗНАННЯ ТЕКСТУ

К. Ю. Дергачов, Л. О. Краснов, В. О Білозерський., А. Я. Зимовин

Предмет досліджень. Вивчалася можливість створення сучасного універсального методу захисту для систем оптичного розпізнавання текстів при передачі конфіденційних даних по відкритих каналах зв'язку. **Мета роботи** – сформулювати концепцію створення сучасного простого та надійного методу захисту інформації при її передачі каналами зв'язку, визначити об'єктивні критерії якості його роботи, створити набір алгоритмів для реалізації запропонованого методу та програмне забезпечення для проведення експериментальних досліджень. За результатами цих досліджень необхідно оцінити ефективність практичного використання запропонованого методу як у плані надійності кодування/декодування даних, що передаються, так і в плані скритності фактів передачі інформації. **Отримано такі результати**. Сформульовано універсальну концепцію створення та використання сучасних методів захисту інформації в системах оптичного розпізнавання текстів при передачі конфіденційних даних по відкритих каналах зв'язку. Визначено основні критерії якості цих систем. Запропоновано новий оригінальний комбінований метод кодування повідомлень, що передаються, за допомогою QR-кодів з подальшим маскуванням фактів передачі даних різними способами LSB-стеганографії. Для проведення експериментальних досліджень було розроблено програмне забезпечення для розпізнавання текстів, яке базується на програмі оптичного розпізнавання символів (OCR) Tesseract версії 4.0. Програма написана мовою Python з використанням сучасних ресурсів бібліотеки OpenCV. Програмно реалізована методика оцінки ефективності роботи алгоритмів кодування даних і скритності сеансів зв'язку. Наведено приклади роботи системи та результати тестування програмного забезпечення в режимі кодування та потайної передачі повідомлень. **Висновки**. Аналіз експериментальних досліджень показав високу ефективність запропонованого методу захисту під час обміну конфіденційними даними у відкритих мережах. Ці результати можуть

бути взяті за основу розробки програмного забезпечення захисту інформації, отриманої в системах оптичного розпізнавання текстів від різних виробників.

Ключові слова: захист інформації в системах оптичного розпізнавання текстів; можливість правильного розпізнавання тексту; алгоритми попередньої обробки вихідних даних; кодування текстової інформації QR-кодами; алгоритми LSB-стеганографії для потайної передачі даних.

РАЗРАБОТКА СРЕДСТВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ДЛЯ СИСТЕМ ОПТИЧЕСКОГО РАСПОЗНАВАНИЯ ТЕКСТА

К. Ю. Дергачёв, Л. А. Краснов, В. А. Билозерский, А. Я. Зимовин

Предмет исследований. Изучалась возможность создания современного универсального метода защиты информации для систем оптического распознавания текстов при передаче конфиденциальных данных по открытым каналам связи. **Цель работы** – сформулировать концепцию создания современного простого и надежного метода защиты информации при её передаче по каналам связи, определить объективные критерии качества его работы, создать набор алгоритмов для реализации предложенного метода и программное обеспечение для проведения экспериментальных исследований. По результатам этих исследований необходимо оценить эффективность практического использования предложенного метода как в плане надежности кодирования/декодирования передаваемых данных, так и в плане скрытности фактов передачи информации. **Получены следующие результаты**. Сформулирована универсальная концепция создания и использования современных методов защиты информации в системах оптического распознавания текстов при передаче конфиденциальных данных по открытым каналам связи. Определены основные критерии качества работы этих систем. Предложен новый оригинальный комбинированный метод кодирования передаваемых сообщений с помощью QR-кодов с последующей маскировкой фактов передачи данных различными способами LSB-стеганографии. Для проведения экспериментальных исследований было разработано программное обеспечение для распознавания текстов, базирующееся на программе оптического распознавания символов (OCR) Tesseract версии 4.0. Программа написана на языке Python с использованием современных ресурсов библиотеки OpenCV. Программно реализована методика оценки эффективности работы алгоритмов кодирования передаваемых данных и скрытности сеансов связи. Приведены примеры работы системы и результаты тестирования программного обеспечения в режиме кодирования и скрытной передачи сообщений. **Выводы**. Анализ экспериментальных исследований показал высокую эффективность предложенного метода защиты при обмене конфиденциальными данными в открытых сетях. Эти результаты могут быть взяты за основу при разработке программного обеспечения защиты информации, полученной в системах оптического распознавания текстов от различных производителей.

Ключевые слова: защита информации в системах оптического распознавания текстов; вероятность правильного распознавания текста; алгоритмы предварительной обработки исходных данных; кодирование текстовой информации QR-кодами; алгоритмы LSB-стеганографии для скрытной передачи данных.

Дергачов Костянтин Юрійович − канд. техн. наук, старш. наук. співроб., зав. каф. систем управління літальних апаратів, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Краснов Леонід Олександрович – канд. техн. наук, старш. наук. співроб., доцент каф. систем управління літальних апаратів, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Білозерський Владислав Олександрович – студент каф. систем управління літальних апаратів, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Зимовін Анатолій Якович − канд. техн. наук, проф., проф. каф. систем управління літальних апаратів, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Konstantin Dergachov − Candidate of Technical Science, Senior Researcher, Head of the Department «Aircraft Control Systems», National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: k.dergachov@khai.edu, ORCID: 0000-0002-6939-3100.

Leonid Krasnov – Candidate of Technical Science, Senior Researcher, Assistant Professor of Department «Aircraft Control Systems», National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: leonid.krasnov.1947@gmail.com, ORCID: 0000-0003-2607-8423.

Vladislav Bilozerskyi – student, of Department «Aircraft Control Systems», National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: b1llays123@gmail.com, ORCID: 0000-0002-5503-3163.

Anatolii Zymovin − Candidate of Technical Science, Professor, Professor of Department «Aircraft Control Systems», National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: zim301g@gmail.com, ORCID: 0000-0001-8580-2317.