THE INFLUENCE OF STEGANOGRAPHIC METHODS AND QR CODE RESOLUTIONS ON DATA HIDING IN COVER IMAGES

Samuel ANDREJČÍK, Ľuboš OVSENÍK, Jakub ORAVEC
Department of Electronics and Multimedia Telecommunication, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, Tel. +421 55 602 4277,
E-mail: samuel.andrejcik@tuke.sk

ABSTRACT

This work deals with digital image processing using the steganography technique in real life. Various steganography techniques face data authentication, data security, and copyright issues. Due to the fact that the problem of data security is currently very topical, these techniques are often sought after. This is related to the constant development of new algorithms that provide solutions that will safely hide the secret message in the image and at the same time will be resistant to various types of attacks. The motivation for writing this work lies in the technique of representing a secret message using a Quick Response code. Later in this work is comparison between our results and results of approach made by scientific community, which works with data hiding within steganographic principles. The secret message is written in the least significant bit plane of the cover image, which ensures that the modification of the image cannot be detected by the naked eye. The proposed solution is evaluated by mathematical quality assessment parameters Peak signal-to-noise ratio, Mean squared error, Normalized cross-correlation and Structural similarity index.

Keywords: *image processing, information hiding, LSB, QR code, security, steganography*

1. INTRODUCTION

Many steganographic algorithms have been proposed so far. They all try to hide information by relying on some of the commonly known techniques [1]. In order to improve the security of steganography, new algorithms have been developed in recent years to hide information using some of these techniques. However, all information hiding techniques have their advantages and disadvantages, such as speed, security, robustness, or limitations related to the cover medium or the transmitted message [2]. Steganography, as a branch of cryptography, deals with hiding information in various carriers so that their presence is difficult to detect. This technique was originally used for secret messaging between armies or spies [3]. Currently, steganography is used in the digital environment to protect and transmit sensitive data [4].

Steganography, as the branch of cryptography is divided into several methods, which include methods based on stego medium properties, such as LSB (Least Significant Bit), or methods based on the frequency domain, such as DCT (Discrete Cosine Transform) [5]. LSB is a simple method where a hidden message is encoded into the least significant bits of a stego medium such as images or audio files [6]. DCT is a more complex method, which is mainly used when data are hiding in JPEG images. Here, the information is encoded into the frequency domain of the image through a transformation [7].

This work will describe image processing in steganography using the LSB (Least Significant Bit) method, in which information is written by a logical XOR bit operation into the LSB plane (Fig. 1) and then the quality of the proposed solution between the cover image and the stego image is evaluated using mathematical evaluations. After this evaluation, the stego image is subjected to cutting and noising attacks, while the degradation of the stego image carrying the secret message, which is represented by a QR code, is monitored. Again, the suitability of the proposed solution is compared, but this time between the original secret message and the extracted secret message.

Further, the work describes the steganographic processing of the image using the LSB replacement method, which uses an algorithm that replaces the least significant bits of the cover image with bits of the secret message. It is also one of the simplest steganographic methods [8].

An extended version is also used in this method, in which several bits of the secret message are written into the last two or more bits of the least significant bit plane, but this extended method is more susceptible to revealing the secret message, since the stego image is significantly more different from the cover image, compared to replacing only the least significant bit, therefore we did not include these procedures into our design [9].

2. THEORETICAL APPROACH TO THE ISSUE

When designing any steganographic procedure, it is important to think about preserving several principles that are characteristic of steganography. These include:

• Hidden data capacity refers to the amount of information that can be efficiently encoded into an image without the change being visible to the human eye or computer algorithm. A higher hidden data capacity allows more information to be hidden in the carrier image file. The capacity depends on the method used and the quality of the image in which the data is inserted. In connection with the capacity of hidden data, it is also important to consider data compression. Some methods allow compression of the hidden data before embedding it in the image, thus increasing the overall capacity and efficiency. However, compression can have a negative impact on the

invisibility and robustness of the system, which is important to consider when choosing a steganography method [10].

• Invisibility focuses on how well the data is hidden in the image carrier, that is, how well the steganographic system is able to mask the existence of hidden data. Ideally, it should be impossible to distinguish the modified image from the original image based on visual observation or statistical tests. Different methods achieve different levels of invisibility depending on the algorithm used and the quality of the image. Some methods may cause changes in the distribution of colors or textures, which may increase the risk of detection by stegoanalysis [11]. Therefore, it is necessary to optimize steganographic algorithms to minimize changes in the visual and statistical properties of the image.

• Robustness refers to the resistance of a steganographic system to attacks or detection attempts. A robust steganographic system should be able to resist attacks such as stegoanalysis, compression, noise, filtering, or other image manipulations that could lead to the disclosure or destruction of hidden data. Robustness is critical in situations where the edited image is likely to be exposed to attacks or unwanted changes [12].

• Security in the context of steganography refers to the system's ability to protect hidden data from unauthorized access or misuse. A secure steganographic system can be supplemented with strong encryption and authentication methods to prevent hidden data from being discovered, decoded or misused. Encrypting data before inserting it into the image increases the level of security and makes it more difficult for attackers who would try to gain access to this data [13]. Another important aspect of security is the use of watermarks and digital signatures. Watermarks and digital signatures can be used to verify the integrity and authenticity of hidden data, as well as to protect against forgery or unauthorized manipulation.

• The performance of algorithms in image steganography can be evaluated based on several factors, such as the speed and complexity of the algorithm, the quality of the image after embedding hidden data, and the ability to withstand attacks. A steganographic algorithm should achieve an optimal balance between these factors in order to be practically usable and resistant to detection attempts. Algorithm speed and complexity are important to the effectiveness of steganographic systems. Algorithms with less complexity and faster processing enable faster insertion and extraction of hidden data, which is useful in real-time applications [14].

• Image quality after embedding hidden data is another important factor when evaluating the performance of algorithms. Methods that significantly degrade image quality can increase the risk of detection and reduce the overall efficiency of the system. Ideally, a steganographic algorithm should insert hidden data into the image in such a way that the change is minimal and invisible to the human eye and to computer algorithms [15].

While subjective methods are based on human judgment and operate without other explicit criteria, objective methods are based on comparisons using explicit numerical criteria. To mathematically evaluate the quality of the proposed system, we use the parameters PSNR (Peak signal-to-noise ratio), NCC (Normalized cross-correlation) and SSIM (Structural similarity index).

PSNR is a quantity that expresses the difference between two images in decibels. The higher this value is, the better the quality of the stego image. We calculate the PSNR according to the equation:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX) - 10 \cdot \log_{10}(MSE) \end{aligned} \quad (1)$$

The NCC value can range from <-1;1> and can be calculated using the following formula:

$$NCC = \frac{\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}(I(x,y)-\bar{I})(K(x,y)-\bar{K})}{\sqrt{\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}(I(x,y)-\bar{I})^2 \cdot \sum_{x=0}^{H-1}\sum_{y=0}^{W-1}(K(x,y)-\bar{K})^2}} \quad (2)$$

where *x* and *y* are the coordinates of the rows and columns in the images, *H* and *W* are the height and width of images. *I* and *K* represent the original image and $\bar{I}$ and $\bar{K}$ are the arithmetic means of their intensities.

SSIM is a well-known quality metric used to measure the similarity between two images. Instead of using traditional error summation methods, SSIM is designed by modeling any image distortion as a combination of three factors, which are correlation loss, luminance distortion, and contrast distortion. We calculate the SSIM according to the equation:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \quad (3)$$

where:

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (4)$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_x^2 + C_2} \quad (5)$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (6)$$

The first term is the luminance comparison function (see equation (4)), which measures the closeness of the mean luminance of two images.

The second term is the contrast comparison function (see equation (5)), which measures the closeness of the contrast of two images.

The third term is the texture comparison function (see equation (6)), which measures the correlation coefficient between two images x and y.

3. RELATED WORK

In the past, several papers dealt with topics similar to our proposal. Wu et. al. in 2013 [16] described a data embedding scheme to camouflage the existence of QR code. Experimental results showed that the proposed

scheme hides the QR code successfully. Moreover, the quality of stego-images was nearly to 30 dB.

Maheswari et. al. in 2015 [17] proposed a frequency domain steganography based information hiding technique using Fresnelet transform (FT). In this method, the Fresnelet coefficients of the Least Significant Bit (LSB) at high frequency subbands are used to embed the QR coded secret message. This approach yields an average PSNR of 45.40 dB.

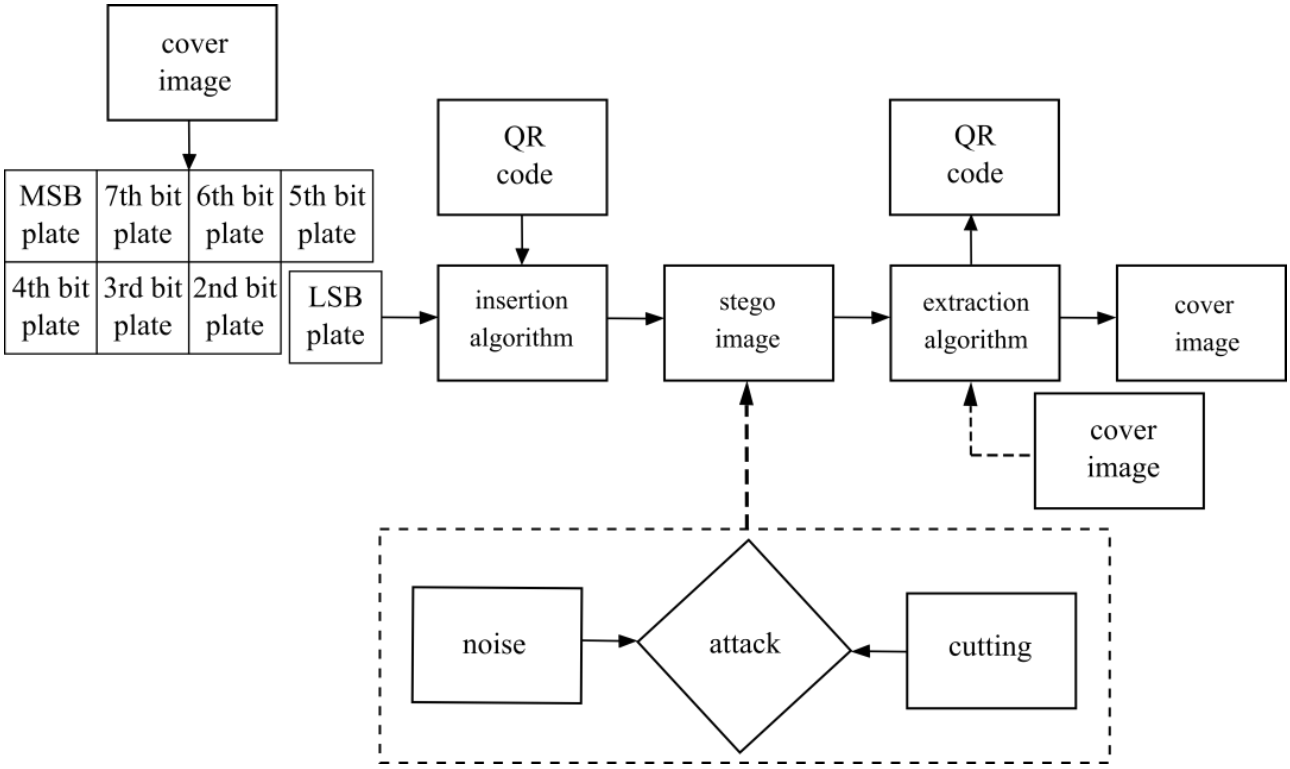


Fig. 1 Design of a steganographic solution and the attack on it

Hajduk et. al. in 2016 [18] discussed about embedding of encoded secret message using Quick Response Code (QR) code into image data. Discrete Wavelet Transformation (DWT) domain was used for the embedding of QR code, while embedding process was additionally protected by Advanced Encryption Standard (AES) cipher algorithm. Their approach had PSNR between 54.31 dB to 71.44 dB.

Using a simpler technique in our solution yields satisfactory results and could also be more advantageous in terms of its computational complexity.

4. PROPOSED SOLUTION

The aforementioned block diagram (Fig. 1) shows the sequence of the proposed solution. A cover image from a list of commonly known images used to verify new steganographic procedures enters the algorithm.
The proposed algorithm should hide the secret information as best as possible, which is represented by a QR code with a resolution of 2100 x 2100, respectively 21 x 21 image elements. The proposed solution is simulated for images that do not undergo lossy compression. The entire design of the solution, including algorithms and simulation, was implemented in the MATLAB platform.

The solution can be implemented on color images as well as on grayscale images. Also, the solution is not limited by the resolution of the cover image. Since images that will not be square are calculated, i.e. they will be oriented either horizontally or vertically, there is a part of the code in the algorithm that detects the orientation of the image and ensures an even distribution of the QR code over the entire image (Fig. 2) so that there is no unnecessarily large loss of transmitted information. Those data that are still lost after the attacks are subsequently restored thanks to the self-correcting Reed-Solomon coding, which ensures redundant writing of QR code data.

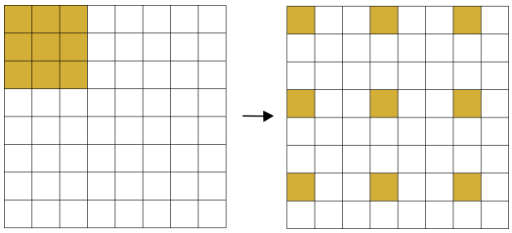


Fig. 2 Demonstration of the distribution of the written bits of the secret message into the LSB plane of the cover image

5. WRITING DATA TO THE IMAGE USING THE XOR METHOD

After successfully writing the information to the LSB plane of the cover image, all the bit planes can be combined again to form a stego image, that is, an image

that consists of the original cover image and the now inserted information represented by the QR code.

Table 1 Assessment of the quality of the stego image after inserting a QR code with information about the length of 1000 characters with use of a XOR method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	64.9239	$1\text{-}1.7\cdot10^{-5}$	$1\text{-}3.3\cdot10^{-6}$
baboonG.bmp	60.1526	$1\text{-}1.7\cdot10^{-4}$	$1\text{-}1.7\cdot10^{-5}$
barbaraG.bmp	60.1526	$1\text{-}3.5\cdot10^{-4}$	$1\text{-}4.5\cdot10^{-4}$
f16.bmp	64.9239	$1\text{-}1.6\cdot10^{-4}$	$1\text{-}5.4\cdot10^{-6}$
lena.bmp	64.9239	$1\text{-}2.5\cdot10^{-5}$	$1\text{-}3.6\cdot10^{-4}$
lenaG.bmp	60.1527	$1\text{-}5.0\cdot10^{-4}$	$1\text{-}1.7\cdot10^{-5}$
peppers.bmp	64.9239	$1\text{-}1.1\cdot10^{-5}$	$1\text{-}3.4\cdot10^{-6}$
sailboat.bmp	64.9239	$1\text{-}2.9\cdot10^{-5}$	$1\text{-}2.3\cdot10^{-6}$

The first experiment was performed with a cutting attack on a newly created stego image. This image was subjected to zeroing at all bit levels, resulting in the corners of the stego image being cut. Fig. 3 represents the stego image after the cutting attack and the QR code extracted from this image.



Fig. 3 Stego image after cutting attack and QR code extracted from stego image

As can be seen, the percentage damage of the stego image is the same for the QR code. This is due to the even distribution of the QR code over the image. If the QR code was placed in the upper left corner without adding the uniform shift function, the loss on the decoded QR code would be much higher.

Table 2 Assessment of the quality of the extracted QR code at 8% cutting from the stego image with use of a XOR method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	14.0974	0.917710	0.92082
baboonG.bmp	14.1129	0.916953	0.92111
barbaraG.bmp	13.8099	0.919813	0.91691
f16.bmp	14.0475	0.916559	0.91997
lena.bmp	14.0666	0.917995	0.92040
lenaG.bmp	14.1051	0.918102	0.92104
peppers.bmp	13.9756	0.916153	0.91861
sailboat.bmp	14.1167	0.918428	0.92127
Average	14.0218	0.917378	0.91961

The proposed solution also faced noise attacks using Salt & Pepper noise with a noise density of 0.05, which affects approximately 5% of all pixels. Noise was applied to the entire stego image.

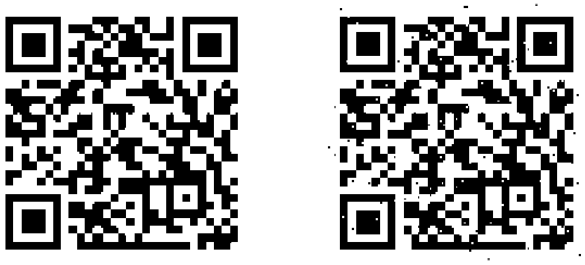


Fig. 4 The original QR code and the QR code extracted from the stego image after the noise attack

Fig. 4 shows the original and extracted QR code, which declares that even in the case of a noise attack, the proposed solution is robust, since after reading the information from both of these QR codes, it is possible to declare that the transmitted information was not lost.

Table 3 Assessment of the quality of the extracted QR code with 5% noise of stego image with use of a XOR method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	16.0356	0.806646	0.94924
baboonG.bmp	15.8757	0.805920	0.94736
barbaraG.bmp	16.0841	0.805704	0.94981
f16.bmp	15.9876	0.807500	0.94870
lena.bmp	16.2016	0.820067	0.95113
lenaG.bmp	16.1766	0.813924	0.95090
peppers.bmp	15.9461	0.804019	0.94818
sailboat.bmp	16.0055	0.802430	0.94897
Average	16.0151	0.785502	0.94901

6. WRITING DATA TO THE IMAGE USING THE LSB REPLACEMENT METHOD

When the secret information is written in the LSB plane of the cover image, a part of the algorithm follows, which mathematically evaluates the proposed solution by comparing the cover image and the newly created stego image. From the results, it can be said that the solution proposed by us meets the basic requirements for a steganographic system and appears to be secure.

Table 4 Assessment of the quality of the stego image after inserting a QR code with information about the length of 1000 characters with use of a LSB replacement method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	75.8413	0.945416	0.94652
baboonG.bmp	72.5432	0.936545	0.94561
barbaraG.bmp	73.6345	0.945616	0.93523
f16.bmp	74.4236	0.944255	0.93654
lena.bmp	72.5224	0.955492	0.92565
lenaG.bmp	73.6445	0.946301	0.94561
peppers.bmp	75.7356	0.925654	0.91861
sailboat.bmp	74.7248	0.946526	0.94451
baboon.bmp	75.8413	0.945416	0.94652

Subsequently, the stego image is subjected to the first attack - a cutting attack, in which all 8 bit planes are subjected to zeroing, resulting in the corners of the stego image being cut. Fig. 5 represents the stego image after

the cutout attack and the QR code extracted from this image.



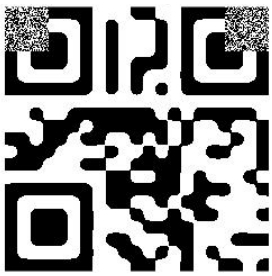


Fig. 5 Stego image after cutting attack and QR code extracted from stego image

As with the previous testing, the damage ratio of the stego image is directly proportional to the damage of the QR code. Even in this case, the equal distribution, which was used in both cases, is responsible for this, so that the results can be as relevant as possible.

Table 5 Assessment of the quality of the extracted QR code at 8% cutting from the stego image with use of a LSB replacement method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	43.1129	0.937511	0.93685
baboonG.bmp	44.0666	0.936853	0.95710
barbaraG.bmp	42.9756	0.935710	0.91691
f16.bmp	43.1167	0.935452	0.91997
lena.bmp	44.5873	0.936989	0.92040
lenaG.bmp	42.1799	0.937015	0.92401
peppers.bmp	44.7956	0.939517	0.91242
sailboat.bmp	43.9211	0.937243	0.92362
Average	43.6713	0.936627	0.92975

In order to compare the results of the attack by cutting out a stego of the image, we decided to add another attack, but this time we did not attacked the corners of the image, but attacked the entire image along its sides, cutting out a strip along the entire length of the image symmetrically on both sides. Thus, 8% of the image was cut out just as much as the previous attack. The results of this attack are presented below

Table 6 Assessment of the quality of the extracted QR code at cutting 8% alongside symetrically from the stego image with use of a LSB replacement method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	41.1327	0.912526	0.91665
baboonG.bmp	42.0819	0.915858	0.92702
barbaraG.bmp	39.9512	0.916740	0.89674
f16.bmp	41.1252	0.912453	0.90967
lena.bmp	42.5938	0.915928	0.90091
lenaG.bmp	41.1298	0.918012	0.89429
peppers.bmp	41.7565	0.917521	0.89225
sailboat.bmp	39.9911	0.928248	0.89367
Average	41.2203	0.917161	0.90390

In order to be able to compare with older outputs, we also used a noise attack using Salt & Pepper noise with a noise density of 0.05, which affects approximately 5% of all image elements. Noise was applied to all 8 bit planes of the stego image.



Fig. 6 Extracted QR code from stego image after noise attack

Fig. 6 shows the extracted QR code, which declares that even in the case of a noise attack, the proposed solution is robust and will withstand this type of attack, since after reading the information from this QR code, it is possible to declare that the transmitted information has not been lost.

Table 7 Assessment of the quality of the extracted QR code with 5% noise of stego image with use of a LSB replacement method

Image	PSNR (dB)	SSIM	NCC
baboon.bmp	42.1369	0.871654	0.95919
baboonG.bmp	39.3474	0.912211	0.93731
barbaraG.bmp	39.5516	0.913764	0.93949
f16.bmp	43.9825	0.881502	0.93895
lena.bmp	41.8669	0.922026	0.95134
lenaG.bmp	40.6252	0.906995	0.94012
peppers.bmp	40.2475	0.829059	0.96864
sailboat.bmp	41.0151	0.915435	0.95895
Average	40.9955	0.887647	0.94601

7. CONCLUSIONS

In this work, the main task was to design a new steganographic system that would ensure the hiding of a QR code carrying a secret message with 1000 characters in images that are often used in testing steganographic procedures.

When implementing the solution, the secret message was hidden in the LSB plane of the cover image using the XOR method, while working with a QR code with a resolution of 2100 x 2100 pixels. In the second proposed solution, the message was hidden using the LSB replacement method and a new QR coder that generates QR codes with a resolution of only tens of pixels.

Cutting and noising attacks were performed on the given stego image. While with the first solution, the results indicated the need to replace the coder as it was necessary to implement subsampling in the current design, the results of the second designed algorithm brought satisfactory mathematical results, especially the PSNR, the value of which increased in some cases by over 20% compared to the design with a fixed QR code resolution.

However, thanks to Reed-Solomon coding, the messages were not damaged enough to be unreadable in any of the attacks. In conclusion, we can claim that the smaller the resolution of the QR code entering the algorithm, the better the mathematical quality evaluations we can expect at the output.

ACKNOWLEDGMENTS

This work was supported by following research grants: APVV-22-0400 - Extension of the autonomous applications of monitoring through multi-band UWB sensors and VEGA 1/0260/23 - Artificial intelligence, robust MANET and multi-hop D2D networks integrated into 6G network.

REFERENCES

[1] RERHMAN, A. – SABA, T. – MAHMOOD, T. – MEHMOOD, Z. – SHAH, M. – ANJUM, A.: Data hiding technique in steganography for information security using number theory, in *J. of Information Science*, Saudi Arabia, 2018.

[2] MAHMOOD, T. – MEHMOOD, Z. – SHAH, M. – SABA, T.: A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform, in *J. of Vis. Commun. and Image Represent.*, Pakistan, 2018.

[3] JOHNSON, N. F. – JAJODIA, S.: Exploring steganography: Seeing the unseen, Computer, vol. 31(2), pp. 26-34, 1998.

[4] BHAYA, W. S. – HABBAL, A.: A comprehensive survey on steganography and steganalysis techniques and tools, in *Int. J. of Computer Science and Information Security*, vol. 14(5), pp. 287, 2016.

[5] ZAIDOON, K. H. – ABID, H. S. – ZAIDAN, B. B.: A review on intelligent procestwo concealment approaches: Steganography and cryptography, in *Int. J. of Pure and Applied Mathematics*, vol. 117(22), pp. 473-485, 2017.

[6] WANG, R. Z., – WANG, S. J.: Image hiding by optimal LSB substitution and genetic algorithm, in *Pattern Recognition*, vol. 37(3), pp. 469-480, 2004.

[7] CHEN, W. C. – HSU, C. F.: A new steganographic method for data hiding in Microsoft Word documents by a change tracking technique, in *IEEE Transactions on Information Forensics and Security*, vol. 3(1), pp. 24-30, 2008.

[8] TORKAMAN, M. R. N. – KAZAZI, N. S. – ROUDDINI, A.: Innovative Approach to Improve Hybrid Cryptography by Using DNA Steganography, in *Int. J. on New Computer Architectures and Their Applications*, Malaysia, 2012.

[9] WESTFELD, A. – PFITZMANN, B.: Attacks on steganographic systems, in *Int. Workshop on Information Hiding*, pp. 61-76, Springer, 1999.

[10] PROVOS, N. – HONEYMAN, P.: Hide and seek: An introduction to steganography, in *IEEE Security & Privacy*, vol. 1(3), pp. 32-44, 2003.

[11] LI, B. – HE, J. – HUANG, J. – SHI, Y. Q.: A survey on image steganography and steganalysis, in *J. of Information Hiding and Multimedia Signal Processing*, 2(2), 142-172, 2008.

[12] KODOVSKÝ, J. – FRIDRICH, J. – HOLUB, V.: Ensemble classifiers for steganalysis of digital media, in *IEEE Transactions on Information Forensics and Security*, vol. 7(2), pp. 432-444, 2012.

[13] FRIDRICH, J. – KODOVSKÝ, J.: Rich models for steganalysis of digital images, in *IEEE Transactions on Information Forensics and Security*, vol. 7(3), pp. 868-882, 2012.

[14] MORKEL, T. – ELOFF, J.H.P. – OLIVIER, M.S.: An Overview of Image Steganography, in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA 2005)*, Sandton, South Africa, 2005.

[15] CHEDDAD, A. – CONDELL, J. – CURRAN, K. – MC KEVITT, P.: Digital image steganography: Survey and analysis of current methods, in *Signal Processing*, vol. 90(3), pp. 727-752, 2010.

[16] WU, W. – LIN, Z. – WONG, W.: Application of QR-Code Steganography Using Data Embedding Technique, in *Information Technology Convergence*, pp. 597-605, 2013, DOI: 10.1007/978-94-007-6996-0_63.

[17] MAHESWARI, S. – HEMANTH, D.: Frequency domain QR code based image steganography using Fresnelet transform, in *Int. J. of Electronics and Communications*, vol. 69(2), pp. 539-544, 2015, DOI: 10.1016/j.aeue.2014.11.004.

[18] HAJDUK, V. – BRODA, M. – KOVÁČ, O. – LEVICKÝ, D.: Image steganography with using QR code and cryptography, in *Int. Conf. Radioelektronika*, pp. 4, 2016, DOI: 10.1109/RADIOELEK.2016.7477370.

Received November 9, 2023, accepted January 29, 2024

BIOGRAPHIES

Samuel Andrejčík received his M.Sc. degree from Faculty of Electrical Engineering and Informatics, Technical University of Košice in 2021 and now he continues as PhD student. His research interests include image processing, hiding of data in images within steganography principles.

Ľuboš Ovseník received his M.Sc. and PhD. degrees from Faculty of Electrical Engineering and Informatics, Technical University of Košice in 1990 and 2002, respectively. He works at the Technical University of Košice, now as an Associate Professor. His research

interests include photonics, fiber optic communication systems and sensor networks.

Jakub Oravec received his M.Sc. and PhD. degrees from Faculty of Electrical Engineering and Informatics, Technical University of Košice in 2015 and 2019, respectively. Nowadays, he serves as an Assistant Professor, his research interests include image encryption algorithms, steganography and digital image processing.