Performance Analysis of Binary Watermarking Algorithm for Color Image Protection Against Nongeometric Attacks

Zoran Veličković, Dejan Blagojević, Marko Veličković

Academy of Applied Technical and Preschool Studies, Section Niš, Niš, Serbia

E-mail address: zoran.velickovic@akademijanis.edu.rs, dejan.blagojevic@akademijanis.edu.rs, marko.velickovic@akademijanis.edu.rs

Abstract—**In this paper, the performance of the recommended algorithm for color image protection by inserting a binary watermark - QR code into the chrominance channel of the carrier image was determined. Algorithm performance is determined in cases of nongeometric attacks such as JPG compression, Gaussian noise, Speckle noise and Salt & Pepper. For certain attack intensities, differential threshold values were determined when the watermark can be extracted without errors. Values of a certain differential threshold do not cause significant degradation of image quality, and compared to the degradation caused by individual attacks, they are significantly smaller. The information encoded by the QR code can be used to identify the author and source after decoding. The results obtained in the experimental part of the work confirm the high resistance of the proposed algorithm to nongeometric attacks. The results of the experiment confirm that the presented concept can be successfully used in copyright protection, that is, in the protection of color images from copying and illegal use and distribution. In the continuation of the research, the performance of the algorithm for geometric attacks will be determined and the ability of the QR code to correct errors in extracted watermarks will be evaluated.**

Keywords - Watermarking; YCbCr color model; Nongeometrics attacks; QR code; Binary watermark; NC; Bit error

I. INTRODUCTION

In the modern world, the exchange of digital content is at its peak [1]. The exchange of multimedia content on social networks is especially intense. With the help of ubiquitous tools, the manipulation of digital multimedia contents is simple, they can be easily downloaded from the network, modified, and then illegally distributed for commercial, propaganda or other purposes [2]. The problem that is increasing every day is related to the protection of copyrights, that is, to the protection of multimedia content against copying and illegal use. On the other hand, unwary users may be offered tendentious content originating from unreliable and unverified sources. Users who do not pay attention to the sources of multimedia content can easily be misled or deceived. The most recent examples of misuse of multimedia content that have led to public disturbance have been caused by unverified information related to the COVID 19 pandemic, that is, to the war conflict in Ukraine. In [3], a secure technological concept for accessing official content and sharing it on the Web is described.

In order to prevent the illegal use of multimedia content, that is, to recognize the source of the content, numerous techniques

This paper is a revised and expanded version of the paper presented at the XX International Symposium INFOTEH-JAHORINA 2021

have been developed [4]. Among other things, multimedia content (music, images, video, ...) can be protected by the classic PKI (Public Key Infrastructure) encryption technique, but for several reasons, they are not adequate for this type of content. Insertion of invisible (secret) information - a watermark into multimedia content (watermarking) is a protection technique that solves all the problems of classic multimedia content encryption techniques [5] – [7]. For this work, it is significant that the proposed watermarking insertion technique does not require a complex PKI infrastructure. Although the proposed protection technique can be applied globally, it is very suitable for implementation in in-house solutions. A color image, grayscale image or binary image can be used as a watermark. In this work, a binary image representing coded information using one of the QR (Quick Response) codes was used as a watermark. Therefore, the watermark can be invisibly inserted into the carrier image with the proposed algorithm, while the watermark can be extracted from the protected image with the inverse algorithm, with known insertion parameters. By extracting the watermark and then decoding it, ownership of the multimedia content can be proven, that is, the real source of information can be decoded. In general, watermark insertion algorithms should not cause noticeable degradation of the carrier images. At the same time, the extraction algorithms should provide reliable extraction of the watermark, that is, the QR code that usually encodes information about the author, owner or source of the

content. These are two conflicting technical requirements that insertion/extraction algorithms need to resolve. The mathematical apparatus used in this work for inserting and extracting the watermark in the carrier image is based on CyBC transformation [8], block SVD (Singular Value Decomposition) [9] and QR coding [10]. To reduce visible image degradation, watermark insertion is performed in the Cr chrominance channel using block SVD.

If the watermark is removed from the protected image, the copyright may be compromised or even the source of the information may be falsified. Good algorithms should be resistant to attempts to remove the watermark from the image. In practice, geometric and nongeometric attacks are used to remove a watermark from a protected image. Nongeometric attacks are based on digital image processing and consist in adding interference that degrades protected carrier images but also complicates watermark extraction [11]. This paper analyzes the performance of the recommended algorithm in relation to standard nongeometric attacks. As for geometric attacks, they are based on cutting off part of the image, rotating or scaling the image and will be discussed in the continuation of the research. The performance of the proposed algorithm was measured by the quality of the extracted watermark for several standard attacks. Number of bit errors and NC (Normalized Correlation Coefficient) were used as objective parameters for measuring the quality of the extracted watermark. In the experimental part of the work, the well-known color pictures Lena, Mandril, Pepper, Airplane and Fruits were used as carriers. The proposed algorithm consists of an insertion part and a watermark extraction part. Given that the proposed algorithm allows the selection of a differential threshold T, it is varied within limits that do not cause significant degradation of the carrier image. Also, the quality of the extracted watermarks was determined for different values of the parameters used to regulate the intensity of the attacks. In particular, attacks such as JPG compression, Gaussian noise, Speckle noise and Salt & Pepper are considered. In order to effectively display the substantial number of obtained results, they are displayed in 3D graphics for all carrier images and for all analyzed types of attacks.

In the second chapter, the characteristics of binary images and QR code, which are used as watermarks in this paper, are given. The YCrCb transformation is briefly described, which will enable inserting the watermark into the chrominance component of the carrier image. The third section describes in detail the recommended algorithm for inserting, that is, extracting the watermark from protected image. In the fourth chapter, the proposed algorithm was evaluated on several color images and several characteristic nongeometric attacks. The obtained results of the performed experiment are shown in appropriate graphs. The results were analyzed based on the objective quality parameters of the extracted watermark. In the fifth chapter, appropriate conclusions are drawn on the application of the proposed concept based on the conducted tests.

II. THEORETICAL BACKGROUND

A. Binary Image

In this work, the term binary image means an image consisting of pixels that can take one of two values, black or white. This allows the value of each pixel to be stored as a single bit, that is, it can have a value of 0 or 1. Binary images occupy little memory space, for example, binary image of 256×256 pixels only need 8 kB of memory space. Binary images were previously used to transmit images in fax machines, while today they are used in business automation in barcodes. This paper uses a binary image obtained by encoding textual information. As already mentioned, the information in this work refers to the owner, the identity of the person depicted in the supporting image or the source of the information [12]. A two-dimensional QR code was used to encode this information.

B. QR code

QR (Quick Response) code is a type of two-dimensional barcode that was designed and developed by Toyota's subsidiary in 1994. Toyota used this code to track vehicles in the manufacturing process, while today the QR code is used in many areas. With the advent of smartphones, QR codes have gained importance because most of these phones have one or more cameras that can be used to scan the QR code and decode it. The QR code has the form of a two-dimensional matrix whose elements can take only two values: logical zero or logical one. If this matrix is printed on paper or displayed on a screen, it represents a binary image. This binary image is divided into different sections that are important for successful decoding. Depending on the type of data and the required information capacity, there are forty versions of QR codes. The smallest QR code in version 1 has a module size of 21×21 pixels, and it can store only 152 bits. On the other hand, version 40 has a dimension of 177×177 pixels and can store 23648 bits. In addition to data memorization, the QR code allows choice of 4 levels of error correction: low, medium, quartile and high. The QR code consists of the following sections: finder patterns, data area, alignment pattern, timing pattern, cell, quit zone, dark module, and separators. A finder pattern is a set of three pattern blocks located at top-left, top-right, and bottom-right locations. Alignment pattern is used for corrections in case of minor image changes during QR code reading. The data area is the middle area of the QR code that contains the encoded data. Separators are used to separate the find pattern from the data area. In addition, the QR code provides an improved security mechanism and has error correction algorithms, which is a significant advantage over ordinary binary images that do not have this mechanism.

C. YCbCr color model

The color images can be modeled with distinct color systems, and the most common of them are RGB, CMYK or YUV models [13]. For this paper, the YCrCb color model is interesting, which consists of three components: the luminance component (Y) and two chrominance components (**Cr** and **Cb**). The relationship between the RGB and YCrCb components of the color model is established by the expressions:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} +0.299 & +0.587 & +0.114 \\ -0.169 & -0.331 & +0.500 \\ +0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix} \qquad (1)$$

In the YCrCb color model, the Y component represents the illuminance in the form of a monochrome image, so by adding the color components **Cb** and **Cr** it can be easily transformed into the color image. In this paper, a binary watermark - QR code is inserted into one of the image color channels in the YCrCb model. The idea of inserting a watermark into the color channel is inspired by the HVS (Human Visual System) and results in less noticeable degradation of the protected image than when the
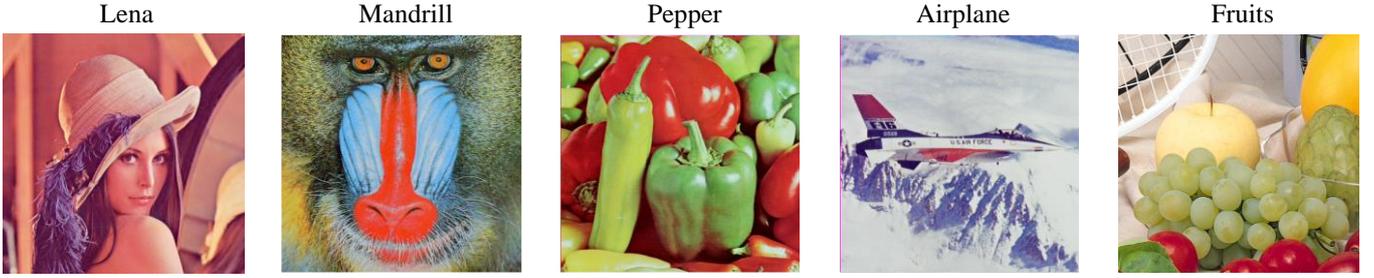
Figure 1. Layouts of original carrier images used in the work (from left to right): Lena, Mandril, Pepper, Airplane and Fruits

watermark is inserted into the Y component of the YCrCb model. With the YCrCb color model, the selection of the sampling scheme is enabled. In order to reduce the size of the image storage file, a down sampling scheme for color components can be used. This technique is standardly used when encoding video sequences. In this paper, a reduced sampling scheme is used, which is denoted as 4:2:0. This has the effect of assigning one sampled value of the color component to the pixels it is surrounded by. In this way, the size of the image storage file is reduced four times. An objectively reduced image quality cannot be subjectively observed by observation. In previous work [14], the authors inserted color watermarks by decomposing them into multiple binary images. Also, previous works analyzed the performance of algorithms that connect the user's image with his COVID credentials [3]. The previously described features of QR codes have a built-in error correction mechanism, which enables their successful use even in the event of errors.

III. BINARY WATERMARKING ALGORITHM

Binary watermark insertion is based on block SVD decomposition of the color component of the carrier image. The SVD coefficients of the color component **Cb** are modulated as a function of the values of all watermark bits. The inverse procedure is used to extract the inserted bits from which the watermark is composed. The insertion and extraction algorithm are presented in multiple IN and EX steps, respectively.

A. Insertion algorithm

Step $\mathbf{IN}_1$: Transform the carrier image I from RGB to YCrCb color model.

$$YCbCr = rgb2ycbcr(I) \qquad (2)$$

Step $\mathbf{IN}_2$: Divide the chrominance component **Cr** into nonoverlapping blocks $\mathbf{H}_{i,j}$ of size 4×4 pixels.

Step $\mathbf{I}_3$: Perform SVD decomposition for each block $\mathbf{H}_{i,j}$ from the **Cr** component:

$$H_{i,j} = U_{i,j} \times S_{i,j} \times V_{i,j}^T . \qquad (3)$$

Step $\mathbf{IN}_4$: Modify the elements from the second and third rows of the first column of each $\mathbf{U}_{i,j}$ matrix (elements $u_{2,1}$ and $u_{3,1}$) based on the value of each individual bit w from the QR code image:

$$if \ w = 1, \begin{cases} u_{2,1}^* = sign(u_{2,1}) \times \left(U_{avg} + \frac{T}{2}\right) \\ u_{3,1}^* = sign(u_{3,1}) \times \left(U_{avg} - \frac{T}{2}\right) \end{cases} \qquad (4)$$

$$else \ if \ w = 0, \begin{cases} u_{2,1}^* = sign(u_{2,1}) \times \left(U_{avg} - \frac{T}{2}\right) \\ u_{3,1}^* = sign(u_{3,1}) \times \left(U_{avg} + \frac{T}{2}\right) \end{cases} \qquad (5)$$

$$U_{avg} = \frac{(|u_{2,1}| + |u_{3,1}|)}{2} \qquad (6)$$

where T is the differential threshold, and it is parameter of the algorithm used to determine the insertion strength. The modified matrix is denoted by $\mathbf{U}^*_{i,j}$.

Step $\mathbf{IN}_5$: Perform the inverse SVD transformation of each block to obtain the block with the bit inserted from the QR code.

$$H_{i,j}^* = U_{i,j}^* \times S_{i,j} \times V_{i,j}^T \qquad (7)$$

Step $\mathbf{NI}_6$: Place the block with the inserted QR code bit in the appropriate place in the protected carrier image of the person. Repeat steps $\mathbf{IN}_4$ and $\mathbf{IN}_5$ for all bits from the QR code.

$$RGB^* = ycbcr2rgb(I^*) \qquad (8)$$

In this way, all bits from the QR code are inserted into the carrier image. In order to extract the watermark inserted in this way, it is not necessary to have the originals of either the image or the watermark, so this algorithm belongs to the class of BLIND algorithms. The algorithm for extracting a watermark from a protected image is shown in a series of EX steps.

B. Extraction algorithm

Step $\mathbf{EX}_1$: Perform transformation of protected carrier image I' from RGB to YCrCb color model.

$$YCbCr = rgb2ycbcr(I') \qquad (9)$$

Step $\mathbf{EX}_2$: Divide the **Cb** component of the protected image into nonoverlapping blocks $\mathbf{H'}_{i,j}$ of dimensions 4×4 pixels.

Step $\mathbf{EX}_3$: Perform SVD decomposition over all blocks $\mathbf{H'}_{i,j}$ carrying image.

$$H_{i,j}' = U_{i,j}' \times S_{i,j}' \times V_{i,j}'^T \qquad (10)$$

Step $\mathbf{E}_4$: The value of the corresponding extracted watermark bit w' is obtained by applying the following expressions:

$$w' = \begin{cases} 0, \ if \ u_{2,1}' > u_{3,1}' \\ 1, \ if \ u_{2,1}' \leq u_{3,1}' \end{cases} \qquad (11)$$

Step $\mathbf{EX}_5$: Set the extracted bit value to the proper location in the watermark.

Step $\mathbf{EX}_6$: Repeat steps $\mathbf{EX}_4$ and $\mathbf{EX}_5$ for all blocks of the protected carrier image and form the complete binary image of the QR code. The resulting binary image represents the extracted QR code.

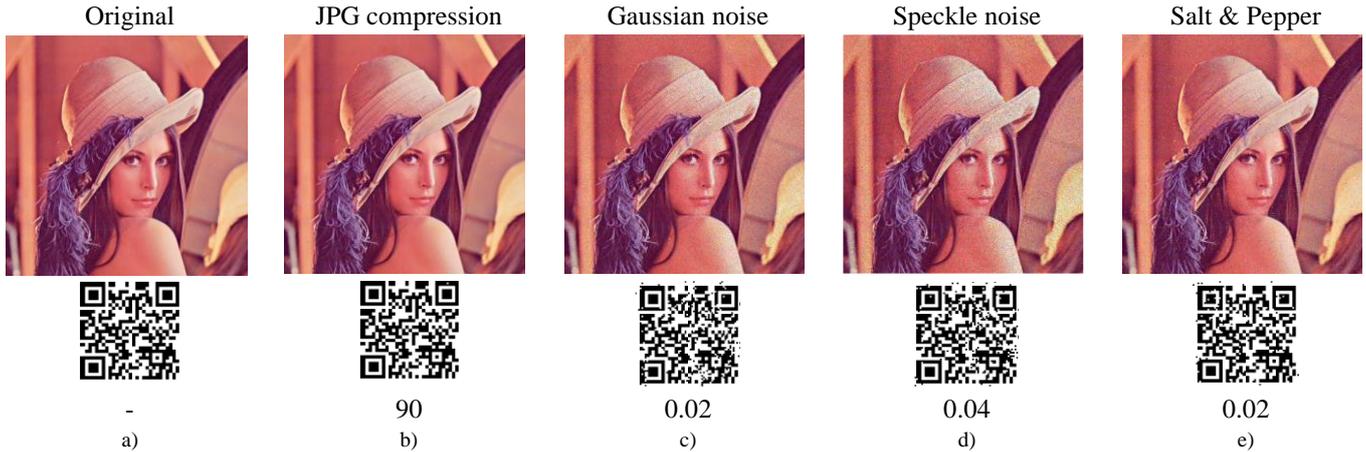| Original	JPG compression	Gaussian noise	Speckle noise	Salt & Pepper
-	90	0.02	0.04	0.02
a)	b)	c)	d)	e)

Figure 2. Layouts a) unprotected carrier image "Lena" and original watermark b) protected image "Lena" with nongeometric attack in the form of JPG compression defined quality 90 and extracted watermark c) protected image "Lena" with nongeometric attack in the form of Gaussian noise with variance 0.02 and extracted watermark d) protected image of "Lena" with nongeometric attack in the form of Speckle noise with variance 0.04 and extracted watermark d) protected image of "Lena" with nongeometric attack in the form of Salt &Pepper and noise density 0.02 and extracted watermark.

IV. EXPERIMENTAL RESULTS

In the experimental part of this work, the well-known color images of Lena, Mandrill, Pepper, Airplane and Fruits were used in a resolution of 512×512×3 pixels. Layouts of these images, which were used as carrier images, are shown in Fig. 1. The selected carrier images belong to the standard test images used in digital image processing. Each of them has its own specificities and enables a detailed evaluation of the proposed algorithms.

A binary watermark is inserted into all carrier images using the proposed algorithm. As already explained, a watermark obtained by encoding the text "Lena Forsen (Sjooblom), Swedish model" with a QR code was used. In this way, a binary image with dimensions of 64×64 pixels were created. The layouts of the original carrier image Lena and the original binary watermark are shown in Fig. 2a.

The proposed insertion algorithm allows selection of the insertion strength, so that for each carrier image a series of protected images with different values of the differential threshold T is created. A higher value of the differential threshold T will cause a greater degradation of the protected image, but also the extraction of a better-quality watermark. The proposed algorithm defines that the watermark is inserted only in the chrominance channel of the carrier image Cr. In the experiment, 6 protected images with different differential insertion threshold $T = [0.1\ 0.15\ 0.2\ 0.25\ 0.3\ 0.35]$ were generated for all carrier images. In total, thirty different protected images were generated, on which different nongeometric attacks are applied. Watermarks of different quality are extracted from such attacked protected images.

In previous works, the problem of choosing the differential threshold T was considered and its optimal value was determined without the presence of attacks [15]. In the conditions of attacks on protected images, a higher value of the differential threshold T must be chosen to ensure high quality of the extracted watermark. In the experimental part of the work, nongeometric attacks were analyzed, which include JPG compression, Gaussian noise, Speckle noise and Salt & Pepper noise. The quality of the extracted watermarks is evaluated based on objective parameters based on the absolute number of bit errors ERROR and normalized correlation coefficients NC in relation to the original watermark. The number of errors in the extracted watermark, which is considered a bit image, is determined according to the expression (12).

$$ERROR(w, w') = \sum_{k=1}^{K} \sum_{l=1}^{L} [w(k, l) \otimes w'(k, l)] \quad (12)$$

where $w(k, l)$ refers to the original and $w'(k, l)$ refers to the extracted watermark. The variables K and L are the dimensions of the watermark, while $\otimes$ is the XOR operator.

The normalized correlation coefficient NC is determined according to expression (13).

$$NC(w, w') = \frac{\sum_{k=1}^{K} \sum_{l=1}^{L} [w(k, l) \times w'(k, l)]}{\sqrt{\sum_{k=1}^{K} \sum_{l=1}^{L} w^2(k, l)} \times \sqrt{\sum_{k=1}^{K} \sum_{l=1}^{L} w^2(k, l)}} \quad (13)$$

In Fig. 2b) to 2e) shows the layout of the protected images of Lena for all considered attacks: JPG Compression, Gaussian noise, Speckle noise and Salt & Pepper. Below the protected image are shown the layouts of the extracted watermarks. The intensity of individual attacks is shown below each of the extracted watermarks. Bit errors in the extracted watermarks can be observed on them. These errors can make it difficult to decode QR codes and will be the subject of further research. In Fig. 2 is shown only smaller than the results obtained in the experiment.

The complete results of the experiment are shown by a series of graphs in Fig. 3 and Fig. 4 related to nongeometric attacks: JPG Compression, Gaussian noise, Speckle noise and Salt & Pepper noise. For the nongeometric attack JPG Compression, the degree of compression was determined by the parameter Quality JPG, which was assigned the following discrete values 50, 60, 70, 80 and 90. For the nongeometric attack Gaussian noise the noise variance had the following discrete values 0.005, 0.01, 0.015, 0.02, 0.025, and for Speckle noise, 0.01, 0.02, 0.03, 0.04 and 0.05. For the nongeometric Salt & Pepper attack, the noise density is varied by the following discrete values: 0.02, 0.04, 0.06, 0.08 and 0.1. The 3D plots in Fig. 3 show the quality of the extracted watermarks based on the absolute number of

errors in the extracted watermarks. From Fig. 3, it can be seen that the number of errors in the extracted binary watermark increases with the decrease of the differential threshold, which was expected.

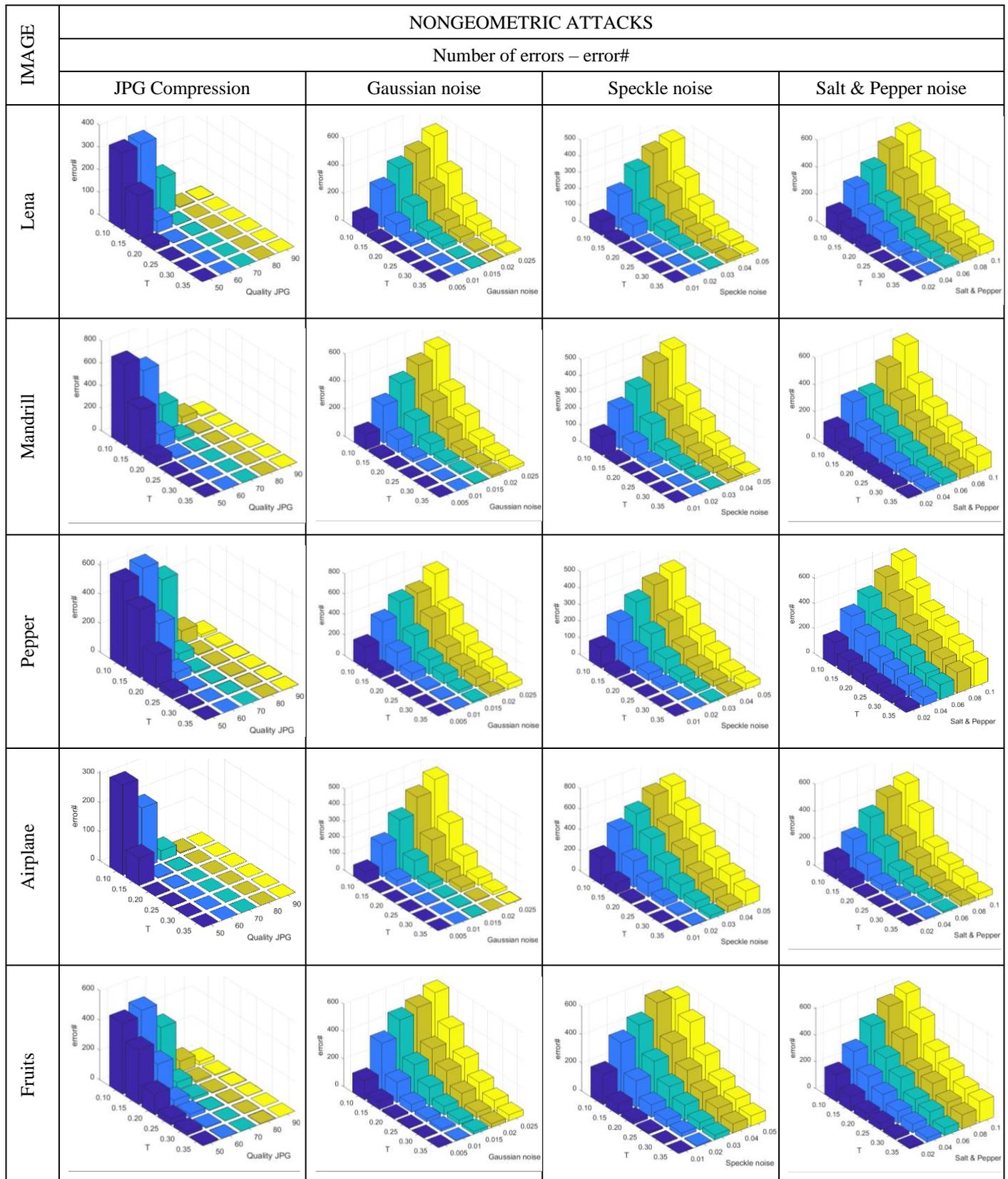| IMAGE	NONGEOMETRIC ATTACKS			
	Number of errors – error#			
	JPG Compression	Gaussian noise	Speckle noise	Salt & Pepper noise
Lena				
Mandrill				
Pepper				
Airplane				
Fruits				

Figure 3. Number of errors in the extracted watermark for all carrier images as a function of differential threshold T and attack intensity: JPG Compression, Gaussian noise, Speckle noise and Salt & Pepper noise.

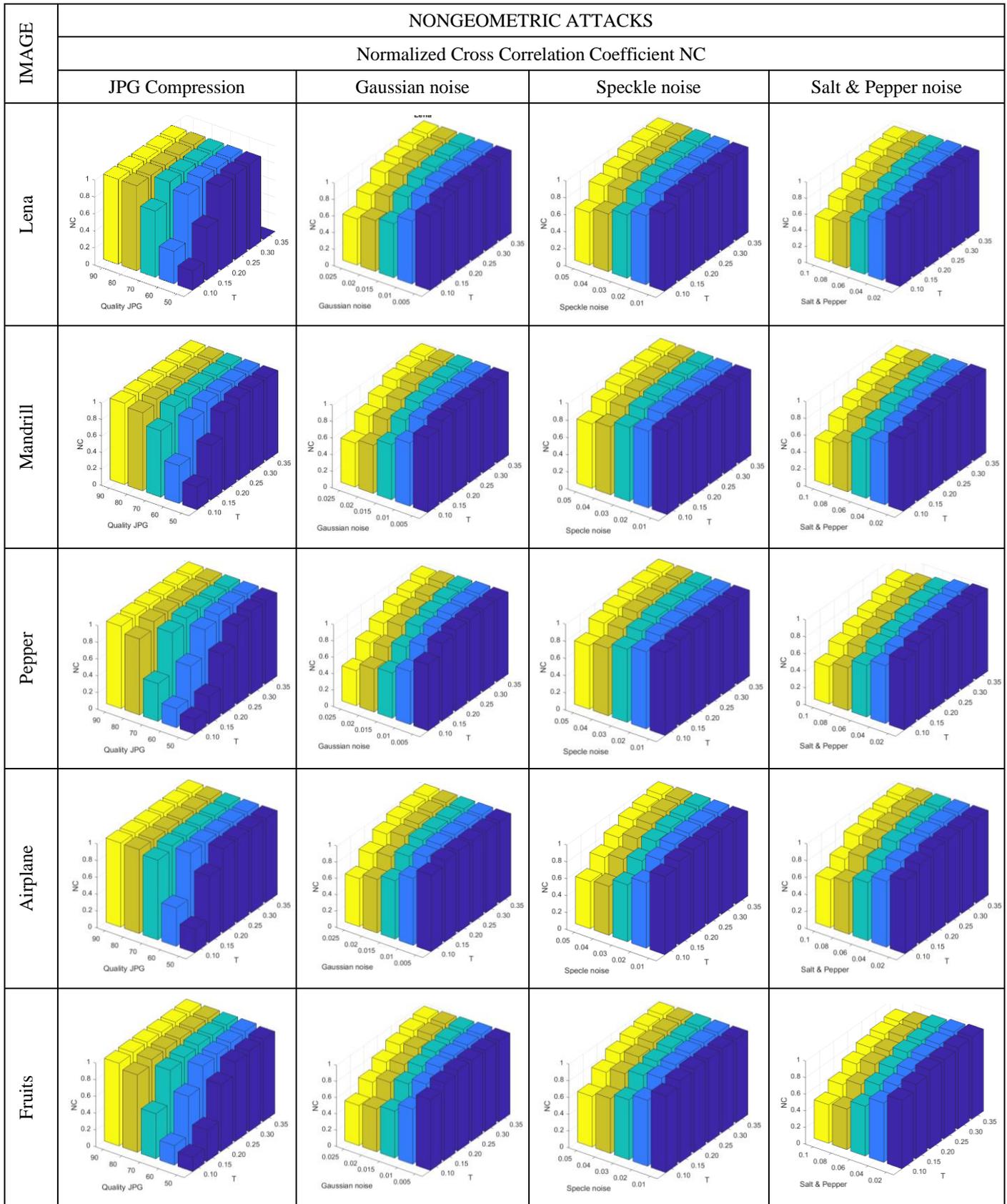| IMAGE	NONGEOMETRIC ATTACKS			
	Normalized Cross Correlation Coefficient NC			
	JPG Compression	Gaussian noise	Speckle noise	Salt & Pepper noise
Lena				
Mandrill				
Pepper				
Airplane				
Fruits				

Figure 4. Normalized Cross Correlation Coefficients NC in the extracted watermark for all carrier images as a function of differential threshold T and nongeometric attack intensity: JPG Compression, Gaussian noise, Speckle noise and Salt & Pepper noise.

TABLE I. NUMBER OF ERRORS IN EXTRACTED WATERMARK AS A FUNCTION OF JPG QUALITY AND DIFFERENTIAL THRESHORD T

Carrier image	T	Quality JPG				
		50	60	70	80	90
Lena	0.1	339	347	162	3	2
	0.15	196	51	1	0	0
	0.2	17	1	1	0	0
	0.25	1	1	0	0	0
	0.3	0	0	0	0	0
	0.35	0	0	0	0	0
Mandril	0.1	721	602	225	57	9
	0.15	409	122	28	6	1
	0.2	73	14	4	2	1
	0.25	11	3	1	1	1
	0.3	3	1	1	1	1
	0.35	2	1	1	1	1
Pepper	0.1	585	631	500	95	19
	0.15	468	321	61	6	9
	0.2	226	56	10	6	3
	0.25	45	8	3	4	4
	0.3	11	1	2	2	2
	0.35	2	0	0	1	1
Airplane	0.1	311	207	34	3	0
	0.15	95	3	1	0	0
	0.2	1	1	0	0	0
	0.25	1	0	0	0	0
	0.3	0	0	0	0	0
	0.35	0	0	0	0	0
Fruits	0.1	476	515	351	75	25
	0.15	366	222	51	12	8
	0.2	139	49	18	4	2
	0.25	42	26	2	4	1
	0.3	27	7	1	1	0
	0.35	8	2	1	2	0

TABLE II. NC OF EXTRACTED WATERMARK IN FUNCTION OF JPG QUALITY AND DIFFERENTIAL THRESHORD T

Carrier image	T	Quality JPG				
		50	60	70	80	90
Lena	0.1	0.2275	0.3813	0.7766	0.9980	0.9985
	0.15	0.6105	0.9252	0.9995	1.0000	0.9995
	0.2	0.9762	0.9995	0.9995	1.0000	1.0000
	0.25	0.9995	0.9995	1.0000	1.0000	1.0000
	0.3	1.0000	1.0000	1.0000	1.0000	1.0000
	0.35	1.0000	1.0000	1.0000	1.0000	1.0000
Mandril	0.1	0.2745	0.4580	0.8040	0.9480	0.9871
	0.15	0.6596	0.8957	0.9767	0.9931	0.9990
	0.2	0.9306	0.9876	0.9980	0.9975	0.9995
	0.25	0.9881	0.9985	0.9995	0.9990	0.9995
	0.3	0.9980	0.9995	0.9995	0.9990	0.9995
	0.35	0.9990	0.9995	0.9995	0.9990	0.9995
Pepper	0.1	0.1744	0.2300	0.4500	0.9068	0.9831
	0.15	0.3290	0.6153	0.9380	0.9940	0.9936
	0.2	0.7130	0.9310	0.9916	0.9955	0.9985
	0.25	0.9351	0.9896	0.9980	0.9970	0.9980
	0.3	0.9861	0.9990	0.9985	0.9990	0.9990
	0.35	0.9975	1.0000	1.0000	0.9995	0.9995
Airplane	0.1	0.2807	0.4569	0.9489	0.9980	1.0000
	0.15	0.7917	0.9871	0.9995	1.0000	1.0000
	0.2	0.9995	0.9995	1.0000	1.0000	1.0000
	0.25	0.9995	1.0000	1.0000	1.0000	1.0000
	0.3	1.0000	1.0000	1.0000	1.0000	1.0000
	0.35	1.0000	1.0000	1.0000	1.0000	1.0000
Fruits	0.1	0.1732	0.2332	0.5372	0.9246	0.9862
	0.15	0.3765	0.7012	0.9365	0.9876	0.9960
	0.2	0.7982	0.9429	0.9703	0.9980	0.9990
	0.25	0.9469	0.9658	0.9980	0.9980	0.9995
	0.3	0.9608	0.9837	0.9985	0.9995	1.0000
	0.35	0.9807	0.9980	0.9995	0.9990	1.0000

Also, the number of errors increases with the intensity of attacks. With JPG compression, as the JPG quality parameter increases, the number of errors decreases and vice versa. The graph clearly shows the parameter space in which there are no bit errors in the extracted watermarks. The forms of the graphics are similar, but the details can differ significantly - all depending on the carrier image.

In Fig. 4 shows an example of a 3D graphic related to the normalized correlation coefficients NC as a function of the differential threshold and the intensity of the applied nongeometric attack. From all the graphs in Figure 4, it can be observed that the NC values tend to one with the increase in the differential threshold and the decrease in the intensity of individual nongeometric attacks.

Similar forms of 3D graphics in Fig. 4 are obtained for all carrier images, and the specific values of the NC coefficients depend on the specific carrier image. The form of the graphics is mainly determined by the type of nongeometric attack. Regarding the graphics, it can be said that for the displayed values of nongeometric attacks, they have similar forms regardless of the type of nongeometric attacks.

All displayed graphs in Fig. 4 have a similar shape, and the values of the NC coefficients tend to one in a similar way, as stated previously. TABLE I shows the obtained numerical results related to the number of errors in the extracted watermark for all tested carrier images and for all values of the difference threshold parameter *T* when the image is exposed to nongeometric attack Compression JPG. TABLE II shows the obtained numerical results related to the NC coefficient of the extracted watermark for all tested carrier images and for all

values of the difference threshold parameter *T* when the image is exposed to nongeometric attack Compression JPG.

TABLE I and TABLE II hold only part of the experimental data that refers to only one type of attack - Compression JPG. Similar tables can be formed for each type of nongeometric attack. If we look at TABLE I related to the nongeometric attack JPG Compression and the image of Lena, for the value of the parameter Quality JPG = 50 and the value of the parameter *T* = 0.10, the number of errors is very high ERROR=339, so the extracted watermark with these insert parameters is not usable. However, when the value of the parameter *T* is increased to 0.25, a small number of errors is obtained, ERROR = 1 and the extracted watermark is very usable.

If we look at TABLE II related to the nongeometric attack JPG Compression and the image Lena, for the value of the parameter Quality JPG = 50 and the value of the parameter *T* = 0.10, the NC coefficient is exceptionally low NC = 0.2275, so the extracted watermark with these insert parameters is not usable. However, when the value of the parameter *T* increases to 0.25, a high NC coefficient value of 0.9995 is obtained and the extracted watermark is very usable.

A detailed analysis of TABLE I and TABLE II shows that the data in these tables are correlated. So, for the extracted error-free watermarks, it can be observed that the coefficient NC = 1. This is expected considering that these are objective methods of image quality assessment. The presented algorithm enables the desired performance by selecting the appropriate differential threshold. A higher value of the differential threshold can provide greater resistance to attempts to remove the watermark from the protected image. From the attached graphics in Fig. 3

and Fig. 4, it can be concluded that the performance depends on the carrier image, but that they do not have a considerable influence on the behavior of the algorithm itself. The degradation of carrier images caused by nongeometric attacks is far more significant than the degradation caused by watermark insertion alone. This has the effect that the watermark inserted by the recommended algorithm can be extracted even in conditions of large attacks.

The recommended algorithm can provide a compromise between insertion strength, carrier image degradation, desired quality of the extracted watermark, and nongeometric attack intensity.

V. CONCLUSION

In this paper, the performance of the recommended color image protection algorithm against copying and illegal use was analyzed. A binary watermark in the form of a QR code obtained by encoding the desired information is inserted into the chrominance Cr component of the carrier image. The performance of the recommended algorithm when trying to remove the watermark from the image was analyzed. The resistance of the recommended algorithm to nongeometric attacks, which are standardly used for watermark removal, is discussed. By varying the strength of insertion and the intensity of the attacks, it was established that it is possible to extract the watermark without errors for all types of considered attacks. By decoding the extracted QR code, information about the source or owner of the image can be obtained. In further research, the additional ability of QR codes to correct possible errors in the extracted watermark will be considered, so it can be influenced by lowering the value of the differential threshold in the insertion process. The results of the experiment confirm that the presented concept can be successfully used in copyright protection, that is, in the protection of color images from copying and illegal use and distribution.

REFERENCES

[1]   Cisco Annual Internet Report (2018–2023), White paper.

[2]   S. Piotr, "Piracy of Digital Content", Organisation for Economic Co-operation and Development, 2009.

[3]   Z. Veličković, S. Veličković, Z. Milivojević, „Application of Watermark in the Form of QR Code in COVID Certificate Validation", Journal of Mechatronics, Automation and Identification Technology JMAIT, Vol. 6, No. 2, pp. 1 – 5, 2021.

[4]   M. Begum, M. S. Uddin, "Digital Image Watermarking Techniques: A Review", Information 2020, https://doi.org/10.3390/info11020110.

[5]   C. Neubauer, J. Herre, "Advanced Watermarking and its Applications", Fraunhofer Institute for Integrated Circuits IIS, https://www.iis.fraunhofer.de, 30.01.2023.

[6]   S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela and H. Jelodar, "An intelligent and blind dual color image watermarking for authentication and copyright protection", Applied Intelligence, Springer Science+Bussiness Media, 2020.

[7]   A. M. Cheema, S. M. Adnan, Z. Mehmood, "A novel Optimized Semi-Blind Scheme for Color Image Watermarking", IEEE Acces, Vol. 8, pp. 3169525-169547, 2020

[8]   C. Patvardhan, P. Kumar, C. V. Lakshmi, "Effective color image watermarking scheme using YCbCr color space and QR code", Multimed. Tools Appl. (2018) 77:12655–12677.

[9]   B. Wang, P. Zhao, "An Adaptive Image Watermarking Method Comining SVD and Wang-Landau Sampling in DWT Domain,", Mathematics, 2020, 8, 691, doi:10.3390/math80506

[10] P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code", Int. J. Electron. Commun. (AEÜ) 69 (2015) 1074–1084.

[11] S. Stanković, I. Orović, E. Sejdić, Multimedia Signals and Systems, Springer, 2012.

[12] Z. S. Veličković, S. M. Veličković and M. Z. Veličković, "Application of QR code as a watermark in multi-modal person's identification" 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), 2022, pp. 1-4, doi: 10.1109/ICEST55168.2022.9828615.I.

[13] E. Richardson, The H.264 Advanced Video Compression Standard, John Wiley & Son Ltd, 2010.

[14] Z. Velickovic, Z. Milivojevic, D. Blagojevic, „Resilience of MDCS Watermarking Algorithm in Wireless Network Environment", ADVANCED COMPUTER INFORMATION TECHNOLOGIES - ACIT 2020. DOI: 10.1109/ACIT49673.2020.9208832

[15] Z. S. Veličković, D. R. Blagojević and M. Z. Veličković, "Binary Watermark Application in Color Image Protection," 2023 27th International Conference on Information Technology (IT), Zabljak, Montenegro, 2023, pp. 1-4, doi: 10.1109/IT57431.2023.10078501.

Zoran S. Veličković was born on October 19, 1958 in Nis, Republic of Serbia. At the Faculty of Electrical Engineering, Niš University, in 1997, he received M. Sc and Magister degree. He received the Ph.D degree from Faculty of Electrical Engineering Banja Luka University in 2011. Since 1993, he has been employed at Professional Electronics, Holding Ei, and since 2004, at the Academy of Technical - Educational Vocational Studies in Niš. He is a regular member of the Engineering Academy of Serbia.

Dejan Blagojević was born on September 6th 1970 in Belgrade, Republic of Serbia. At the Faculty of Electrical Engineering, Niš University, in 2003, he received M. Sc and master's. He received the Ph.D degree from Faculty of Technical Sciences Čačak, University of Kragujevac in 2008. Since 2004, he has been employed at the Academy of Technical - Educational Vocational Studies in Niš.

Marko Veličković was born on July 30, 1993 in Nis, Republic of Serbia. At the Academy of Technical - Educational Vocational Studies in Nis in 2013, he received M.Sc degree. He received the award for the best student at the master's vocational studies in Multimedia Comunication Technolgies. He is currently employed at the Academy of Technical - Educational Vocational Studies as a software engineer.