ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803//tg-20210714171523

Original scientific paper
Received: 2021-07-14, Accepted: 2021-07-27

Recognition Model of Counterfeiting Digital Records of Biometric Photographic Image

Marko Maričević, Petra Ptiček*, Ivana Žganjar

Abstract: Biometric portrait as one of the most important means of identifying requirements through strict definition of dimensional relationships, preservation of realistic information about all technical characteristics of the photographic image, so that all biometric values can be digitized and used in recognition. The great variety and accessibility of applications for digital processing of digital record of a photographic image has enabled a visually convincing display of a forged photograph that leaves a different impression on the viewer and transmits a different, that is, a forged message. Due to the need to prove the authenticity of the digital record of the photographic image, methods have been developed for the analysis of the record that can detect deviations from the real record even when there are no visual signs of processing the photographic image. Not all analysis techniques can detect certain methods of photo manipulation, so multiple digital photography detection and analysis techniques need to be applied. In order to prove its authenticity, the scientific paper deals with methods for analysis and detection of forgery of digital photography with respect to the digital record and the structure of JPEG format.

Keywords: biometrics; computer forensics; JPEG; manipulation; photographic image

1 INTRODUCTION

The daily use of digital photographic images for professional or amateur purposes opens the door to new and creative ways to forge a photographic image. With the advancement of technology and the possibility of installing a digital camera in almost any electronic device, including: laptop, tablets, mobile phone and broadband Internet access have enabled very fast sharing of photographic images and their publication on the Internet. With new technologies and trends, new, simpler computer programs for processing digital photographic images have emerged. Due to this problem, there is a need to prove the authenticity of the digital photographic image. The great variety and accessibility of computer applications for digital processing of digital photographic image has enabled a visually convincing display of a forged photographic image that leaves a different impression on the viewer and transmits a different, forged message. [1, 2] Each digital photographic image is a finite binary record made by a series of mathematical algorithms. Mathematical algorithms behave according to pre-known rules and each change affects the final record of the digital photographic image. This is why it is possible to analyze a digital photographic image in search of irregularities in the structure of the digital record and in the very structure of the digital photographic image. Each digital photographic image is considered unique and should be approached in this way during the analysis. Therefore, it is not possible to create a unique model for the analysis of digital photographic images, but it is necessary to apply a number of different techniques in order to detect potential errors or manipulations. This paper deals with methods for the analysis of digital records of biometric photographic images and the detection of their forgeries with respect to the digital record and the structure of JPEG formats. In order to prove the authenticity, the paper presents a method based on the observation and comparison of the basic characteristics of a biometric portrait photographic image and the characteristics of creating a digital JPEG record. Scientific research involves the analysis and authentication with a predefined model. For the analysis, manipulated photographic images made in laboratory conditions with targeted changes are used, and based on the results, the method of accurate interpretation of information is explained. In proving, a wide range of currently known methods of manipulating the addition or deletion of digital photographic image elements are analyzed.

Biometrics is one of the most important means of identification and authentication of individuals, and as a science, it speaks of automated procedures for uniquely recognizing people based on one or more innate bodily characteristics, or characteristics of human behavior. Biometrics has been used since ancient times and has developed in accordance with the development of human knowledge, that is, technology and science, whose dizzying development in recent decades opens up unimagined possibilities of their application in the fields of identification. Classical methods of identification in the new environment gain a new, additional quality, and completely new methods are established. Biometric authentication techniques are classified according to the type of characteristics being assessed: physiological properties or behavior. Physiological biometrics is based on classifying a person according to data obtained as part of the human body, such as fingerprints, faces, or the iris of the eye. The rapid development of technology has increased the need for reliable ways to identify people. Today, identification of persons is performed in two ways: Identification by means of identification documents, identification based on a security key. The use of biometrics, or specifically unique human characteristics, has existed for hundreds of years in one form or another, whether it is a physical description of a person or perhaps more recently a photographic image. Prior to biometric documents, the classic approach to portrait photographic image for documents based on the so-called Beautiful portrait of a face, in a European or American cut. Such an approach ensures an optimal range of shadows to display facial volume, which is not enough when it comes to portrait photographic images for a document, where properly defined facial geometries need to be ensured. In this case, since the introduction of

biometric portrait photographic images for documents, diffused lighting from the direction of the camera has been used. Such a biometric portrait for documents bears biometric data about the owner of the document, that is, the complete biometrics of the person. [1] Biometric portraits are taken under precisely defined conditions, such as high quality photographic image, format (width x height), about 2/3 of the image should be occupied by the head, which must be centered on the photographic image, satisfactory contrast and sharpness, uniform background without texture and shadows. [3] This means that the photographic image must be 35 mm wide and 45 mm high. The head (from the tip of the chin to the crown / parting) should occupy about 2/3 of the image, but should not be higher than 36 mm. Hair (high hairstyles) may protrude beyond the image. The distance between the eyes (from the middle of the left eye to the middle of the right eye) is a minimum of 8 mm (optimally 10 mm). The head should be centered on the photographic images. The face must be sharply painted in all areas, full of contrast and clear. The background must be monochromatic (ideally light gray) and with sufficient contrast to the face and hair. The photographic image should show the person with a neutral facial expression and closed mouth on the frontal shot. The person in the photographic image must look directly at the camera. The eyes must be open and clearly visible, and horizontal with the x axis. Eyes, nose and mouth should not be covered with hair as shown in (Fig. 1).

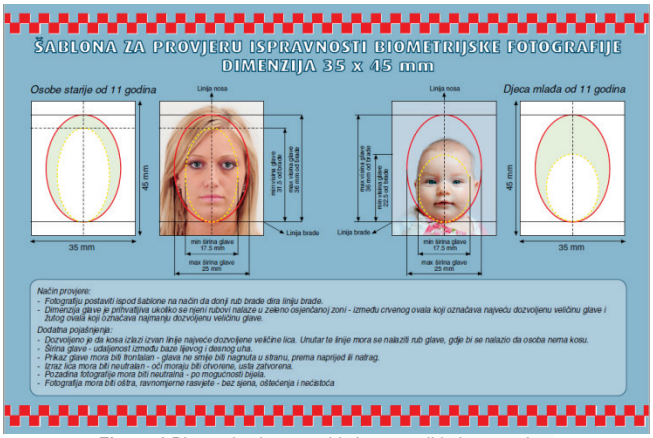

Figure 1 Biometric photographic image validation template

To ensure maximum iconicity, by recording a biometric portrait, the given conditions should be met. Shooting needs to be provided from a normal view, which means that the lens of the camera and the face of the model are in a plane-parallel position. Also, the light illuminating the model's face must be directed from the direction of the camera, to ensure that the model's face will be evenly illuminated over the entire surface without reflections and shadows with a solid background that will provide enough contrast to the face and hair. [3] As a rule, when shooting a biometric portrait photographic image for documents, general light is used, and a backlight can be used to illuminate the background, thus eliminating the possibility of shadows and increasing the brightness of the background. Since the light illuminating the model must be diffused, a softbox or white umbrella is typically used as the transparent diffuser. The digital record of a photographic image is defined in the RGB color space, which, if necessary, depending on the output unit of the system, is usually compressed into a narrower, usually sRGB color space by rendering with perceptual intentions.

Digital photography is a set of binary values stored on a storage medium according to predefined rules and algorithms. Therefore, a digital file is mathematical in nature, not physical. Examination and analysis require a certain level of expertise and a thorough knowledge of the process of creating a photographic image in order to systematically start the process of proving authenticity. [4, 5] Each photograph is unique, and thus every case of proving authenticity. The conclusions of the examination are made by the investigator, and the techniques for analyzing the photographic image are only a tool used. [6, 7] With each technique of analysis, researchers get more and more information about photography, its origin and method of production. Although biometric analysis primarily involves the technical analysis of individual parameters of a photographic image, portrait photography also presupposes a visual assessment, and falsified images are recognized in this way.

2 EXPERIMENTAL PART

In the experimental part, for the purpose of creating a reference photographic image – the original, the pictures were taken with a digital Leica Canon 5DS R camera, with a maximum shooting resolution of 50 MP in Adobe RGB color space with the correct white balance for measured light temperature, the correct exposure determined by TTL camera system and standard recording saturation. A Canon RF 50 mm f / 1.2 L USM lens was used. All photographic images were taken with a sensitivity of 100/21 ISO and stored in the finest JPEG format and at a resolution of 300 dpi. Lighting for illumination used for the characteristic standard light source - Kaiser 1000 halogen reflector. The light was measured by the TTL system of the camera by segmental measurement of light to a standard color. The following exposure elements are specified for shooting: lens aperture 2.8, exposure time 1/60 s. The resulting digital recordings of photographic images were loaded into Adobe Photoshop 2020, to maintain differences in perception for all colors with perceptual rendering and transferred from Adobe RGB to sRGB color space, which is reproducible in various digital image printing techniques, monitors and other photo output units and stored in the highest fineness of JPEG records. Photographic images prepared in the format 3.5×4.5.

To form a falsified biometric photographic image, a 300 dpi resolution element in the sRGB color space was added to the original photographic record.

To examine the authenticity of the digital record of the photographic image, a model was made, which is divided into two parts, the first part which will deal with the analysis of the digital file structure and the second part which will deal with the structural analysis of the digital photographic image. File structure analysis deals with the study of data about the digital record and its origin. This aims to establish the format of the digital photographic image format. The EXIF record is

then analyzed for inconsistent information. This type of examination presupposes the possibility of establishing whether the data presented are accurate or false. If the data has changed it does not necessarily mean that the content of the photographic image has been falsified but can only be an indication that the computer application for processing the photographic image has interacted with the photograph. [8]

Figure 2 Sample of not manipulated image

Figure 3 Sample of manipulated image

Table 1 Test results of EXIF and hexadecimal values

Structural file analysis	Determine file type
	Hex values
	EXIF values
Structural analysis of digital photography	Luminance Gradient
	Quality Estimation
	Error Level Analysis
	Echo Edge Filter
	Copy – Move Forgery

After the analysis of the file structure, as visible in Tab. 1 the structural analysis of the digital photographic image is performed. In structural analysis, the investigation is conducted at the pixel level in search of manipulated areas and signs of copy paste manipulation methods are sought. The applied techniques are based on statistical analysis using specialized purpose algorithms. The next part of the analysis uses techniques based on the analysis of luminance gradient, intensity, tone, color, edge detection, quality estimation, JPEG error levels, and photo image compression. Light intensity, tone and color are the properties that affect the formation of a photographic image, and their processing in the camera creates the final digital photographic image. By changing these values with computer applications for photographic image processing, the manipulated areas of the photograph may have significantly different properties from the original environment. [9, 10] Therefore, an analysis of light intensity, tone, and color is performed. Human-computer interaction is necessary in this analysis, and the algorithms used in the analysis are just a tool. The conclusion is made by the investigator who, based on the obtained results and the presentation of the photograph, determines whether there are signs of manipulation. Algorithms with high-pass filters are used in this model to detect echo edges and search for tampering in photography for thorough analysis. Also, the result is carefully considered in the search for echo edges or small errors made during manipulation. At first glance, no differences can be seen in some of the obtained results, and it is necessary to further clarify the obtained display by increasing the contrast. Creating a counterfeit photo from two or more JPEG photos can cause discrepancies in the statistics. When a photographic image is forged, it can contain various pieces that are reduced, cut, inverted to make the display as realistic as possible. In addition, parts of the photo are not compressed by the same quality factor. All these factors affect the creation of minor anomalies in digital recording. Therefore, the JPEG compression analysis technique is applied, which divides the photo into segments, and by analyzing each block of the photographic image, it looks for statistical anomalies. The examination analyzes the authenticity of the biometric portrait previously described and shown in (Fig. 2). The initial photographic image defined as the original (Fig. 2) was manipulated by inserting the chin element shown in (Fig. 3). Through the analysis with the pre-proposed model, testing is performed with all techniques and a conclusion is made depending on the overall test result.

Assumptions of the analysis of these techniques can provide sufficient evidence and signs of manipulation of the photographic image. In the first part of the analysis, open source computer applications JPGsnoop, file and stat are used, and in the second part of the analysis, due to specific needs and analysis techniques, the program code written in the programming language Python is used. Applying this model, several scenarios and the process of research and analysis of digital photographic image are presented. For recording the results, a table was made in which all the analysis techniques of that category are listed, where the success of individual analyzes is indicated. The proposed model primarily focuses on the analysis of counterfeits created by the copy paste technique. Photographic images that contain parts that are not the original part of the scene can be said with certainty to be forged. The best way to prove authenticity is to use tests using as many different analysis techniques as possible. The quality of photographic image manipulation depends mostly on the author of the manipulation, and the detection of superior manipulations requires a lot of time and patience in analysis and monitoring

of new techniques, methods and models for analysis and testing of digital photographic images for the purpose of proving authenticity.

3 REASERSCH RESULTS WITH DISCUSSION

The scientific research was conducted using a model to examine the authenticity of the digital record of a photographic image, a biometric portrait, which should be approached with great care for noticing details. The effectiveness of this model and individual techniques is presented in this chapter.

The first step in researching a digital photographic image is to examine the structure of the digital image to determine if the file complies with the JPEG recording rules at all. This test is performed because the computer does not know the difference in naming files, so it is possible to arbitrarily name any file and extension. The result shows that the JPEG record is correct. The test was performed with the computer application file and stat, and the obtained results are JPEG image data, JFIF standard 1.02. Also, the obtained results show the standard used in the recording of JPEG photographic image. The results are shown in Tab. 2.

Table 2 Results of digital record format testing

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait	×		

For analysis and review of EXIF and hexadecimal values, the computer application JPEGsnoop was used, which displays the parameters of the photographic image in detail. In Tab. 3, the obtained results are shown. With the JPEGsnoop computer application, it is possible to see all the parameters of the photographic image, from the camera model to each individual element of exposure when creating a digital photo image. The results show possible signs of manipulation, as a record of the interaction of the computer application and the examined photographic image was found among the EXIF data. Part of the EXIF data contains information about the manufacturer and model of the camera and the time of creation, that is, the last time of interaction between the computer application and the photographic image. However, the EXIF record only recorded the interaction of the photographic image and the computer program, but not the actual change in the photographic image itself. In these cases, there is only the possibility that the digital photo image has been resized.

Table 3 Results of EXIF and hexadecimal values

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait		×	

Light intensity analysis is used to detect manipulation of the copy paste technique from several different photographic images. Namely, if two photographic images are recorded with two different cameras under different lighting conditions, a difference will be created that is, not visible to the naked eye. Analysis of light gradient will reveal the difference in areas that have different degrees of illumination at the same optical distance. Tab. 4 shows the results obtained by this analysis, and shows the deviations of luminance gradient, which is why there is a suspicion that it occurred in different light conditions, which indicates the first signs of manipulation of the copy paste technique.

Table 4 Results of luminance gradient analysis

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait		×	

By quality estimation analyzing, quantization tables are used to estimate last saved JPEG quality. Manipulated areas pasted on the original photo may have different JPEG quality. Therefore, this technique is applied, and the results are shown in Tab. 5.

Table 5 Results of Quality Estimation analysis

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait	×		

Applying error level analysis looks for areas of photography that differ in JPEG compression quality. In this analysis, it is necessary to determine the contrast threshold of block recognition due to the existence of noise in the photographic image. The value of the threshold can be between 0% and 100%, and it is best to start with a threshold level of 50%, depending on the need to increase or decrease the threshold by 5%. The results of this analysis (shown in Tab. 6 and Fig. 4) show that there is an area that stands out significantly from the surrounding and it is possible to conclude that there is an area of manipulation.

Table 6 Results of error level analysis

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait		×	

Table 7 Results of echo edge filters

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait			×

Echo edges or JPEG are created when pasting objects of lower compression quality to the original photo. This method has proven most effective in searching for manipulated areas. [11, 12] Tab. 7 shows the obtained results, which show that the JPEG echo edge was observed, that is, it is suspected that the original photographic image was subsequently simulated and processed by inserting the chin element (Figs. 4 and 5). In addition to the analysis of luminance gradient and error level with which there was a possibility of photo manipulation in the same area, this analysis provides even stronger evidence for the existence of manipulation.

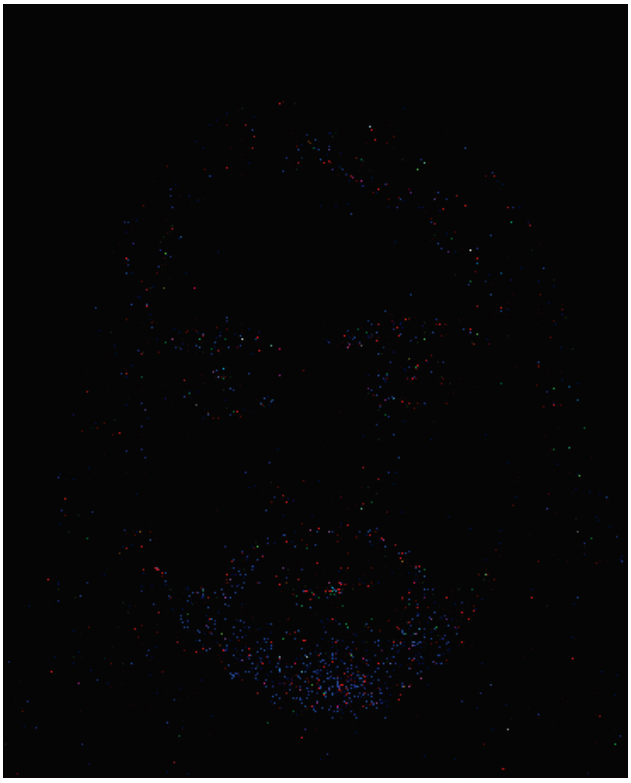

Figure 4 Results of error level analysis

Figure 5 Results of echo edge filters

Adding new elements to an existing photo image changes the JPEG statistics. By analyzing and detecting echo edges with high-pass filters, the result obtained shows the area of manipulation, a large inconsistency of data in the facial area is noticed, which, among other evidence, indicates that the photographic image is forged. The results are shown in Tab. 8.

Table 8 Results of echo edge filters

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait			×

Applying copy paste analysis looks for cloned area detection of photography. In this analysis, it is necessary to determine the response rate, matching rate, distance rate and clusters for the BRISK type detector. The value of the rates can be between 0% and 100%. The results of this analysis (shown in Tab. 9 and Fig. 6.) show that there is an area with possibility of copy paste elements and it is possible to conclude that there is an area of manipulation.

Table 9 Results of error level analysis

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait			×

Figure 6 Results of Copy move forgery

After a detailed investigation and application of the proposed model, the final result is determined by the investigator. The application of analysis techniques from the proposed model serves only as a tool that makes it easier for the researcher to display certain information about the photographic image, and thus draw conclusions. The results of scientific research are shown in Tab. 10.

Table 10 Final results of scientific research

Case	Insufficient signs for manipulation	Possible signs of manipulation	Certain signs of manipulation
Biometric portrait			×

The model used to investigate was divided into two parts. The task of the first part of the investigation was to determine the integrity of the digital record, and from the EXIF data it was possible to decide on the further course of the research. In the example where the analysis was performed, advanced manipulation techniques were not used, so the record structure and EXIF data were not changed in order to conceal traces of the use of computer applications for digital processing of photographic images. When concealing traces of manipulation in the record structure, it is necessary to have a lot of knowledge and skills in manipulation and to know the structure of the file record itself. In the second part of the research, all techniques and methods were intended to search for subsequently pasted or erased elements of photography. Most photographic image manipulations occur because one wants to conceal something or add it to the original scene, so analysis techniques that are an integral part of the proposed model are chosen. The techniques of luminance gradient and quality estimation analysis belong to simple analyzes due to simple and fast algorithms. In certain cases, by applying only these analysis techniques, possible manipulation can be sensed. In other techniques, the applied algorithms are much more complex, and the analysis itself requires much more time, which increases proportionally to the resolution of the photographic image.

4 CONCLUSION

This paper describes and applies techniques that can be used for forensic analysis of digital records of photographic images, with the aim of proving the authenticity and integrity of digital records of photographic images. After describing and explaining the techniques in the theoretical part of the paper, a model was developed according to which the analysis of the structure of the digital file record and the analysis of the structure of the digital photographic image were performed. The results of application of the proposed model and techniques for analysis and proving the authenticity of digital photographic image record show the possibility of successful detection of manipulations on digital photographic images. Forensics of the digital record of a photographic image makes it possible to prove the authenticity of the photographic image and the origin of its origin. Proof of authenticity does not depend only on the applied analysis techniques but is a major factor in the whole process of examination by the investigator. The researcher is a person who should be very well acquainted with the process of digital photographic image creation, familiar with the analysis techniques applied, able to distinguish the obtained results and draw the conclusion of each examination. In the proposed model for testing digital photographic images, techniques are applied that cover the area of structural analysis of the digital file and structural analysis of the digital photographic image itself. The speed of analysis increases in proportion to the resolution of the digital photographic image, and this was taken into account when creating this model. The goal was to create an efficient model that does not require much time for the overall analysis of a digital photographic image. The developed model proved to be very efficient and quickly met all expectations in the analysis. The test was based on the authentication of JPEG records with an emphasis on the detection of copy paste manipulation techniques. This manipulation technique is currently the most widely used method of manipulation with a very convincing result and is mostly imperceptible to the human eye.

Structural analysis of the digital file record examines the file that contains the information that represents the digital record of the photographic image. Each file type has a different structure and stores information differently. By checking the integrity of the file, it is possible to determine whether the structure of the JPEG photo image format is correct, and this can lead to the conclusion of how the digital photo image was created. By checking the EXIF record, it is possible to obtain the first signs of possible manipulation of the digital photographic image because computer programs can leave traces if they were in interaction with the examined photographic image. Techniques applied in the structural analysis of digital photographic image record have proven to be very successful in the search for manipulated areas. The most successful technique in searching for manipulated areas in a digital photographic image is the analysis of JPEG echo edge filter and copy-move detection that identified a suspicious area while other techniques hinted at the possible existence of manipulation. Systematic examination of the digital record of the photographic image according to the proposed model has successfully revealed manipulations on the photographic images.

This model can be extended to make the analysis even more detailed by applying other techniques described in this paper. Extending this model of analysis should also take into account the time required to examine digital photographic images.

5 REFERENCES

[1] Jajin, A., Hong, L., & Pankanti, S. (2000). Biometric Identification. *Communications of the ACM, 43*(2), 91-98. https://doi.org/10.1145/328236.328110

[2] Mikota, M. (2016). Fotografija - Tehnički i semantičko-sintaktički izazovi medija u novom okruženju. *Tiskarstvo & Dizajn 2016,* 175-178. (in Croatian)

[3] https://mup.gov.hr/gradjani-281562/moji-dokumenti-281563/putovnica-330/primjeri-ispravno-i-neispravno-snimljenih-fotografija/378

[4] Itier, V., Strauss, O., Morel, L., & Puech, W. (2021). Colour noise correlation-based splicing detection for image forensics. *Multimedia Tools and Applications, 9*(80), 13215-13233. https://doi.org/10.1007/s11042-020-10326-5

[5] Alkawaz, M. H., Sulong, G., Saba, T., & Rehman, A. (2018). Detection of copy-move imageforgery based on discrete cosine transform. *Neural Comput. Appl. 30*(1), 183-192. https://doi.org/10.1007/s00521-016-2663-3

[6] Finkelstein, N. S., Levy, O., & Levi, A. (2021). Photographic comparison of surface topography as a viable solution when

physical match is challenging. *Journal of Forensic Sciences, 1*(80), 295-302. https://doi.org/10.1111/1556-4029.14561

[7] Popescu, C. & Farid, H. (2004). Statistical tools for digital forensics. Proceedings of the 6th International Conference on Information Hiding (IH'04), Springer-Verlag, Berlin, Heidelberg, 128-147. https://doi.org/10.1007/978-3-540-30114-1_10

[8] Maričević, M., Žeželj, T., Mikota, M., & Žiljak Stanimirović, I. (2016). Strukturalna forenzička analiza JPEG zapisa fotografske slike. *Proceedings of the International Conference MATRIB*, 210-217. (in Croatian)

[9] Martlin, B. & Rando, C. (2020). Reflectance Transformation Imaging (RTI) for the Documentation of Saw Mark Characteristics. *Journal of Forensic Sciences, 5*(65), 1692-1697. https://doi.org/10.1111/1556-4029.14330

[10] Dua, S., Singh, J., & Parthasarathy, H. (2020). Detection and localization of forgery using statistics of DCT and Fourier components. *Signal Processing: Image Communication, 82*, 115778. https://doi.org/10.1016/j.image.2020.115778

[11] Zhang, W. C., Kosiorek, D. A., & Brodeur, A. N. (2020). Application of Structured-Light 3-D Scanning to the Documentation of Plastic Fingerprint Impressions: A Quality Comparison with Traditional Photography. *Journal of Forensic Sciences, 3*(65), 784-790. https://doi.org/10.1111/1556-4029.14249

[12] Bakas, J., Ramachandra, S., & Naskar, R. (2020). Double and triple compression-based forgery detection in JPEG images using deep convolutional neural network. *Journal of Electronic Imaging, 2*(29), 23006-23006. https://doi.org/10.1117/1.JEI.29.2.023006

Authors' contacts:

Marko Maričević
University of Zagreb, Faculty of Graphic Arts,
Getaldićeva 2,
10000 Zagreb, Croatia
e-mail: marko.maricevic@grf.unizg.hr

Petra Ptiček
University of Zagreb, Faculty of Graphic Arts,
Getaldićeva 2,
10000 Zagreb, Croatia
e-mail: pticekpetra@gmail.com

Ivana Žganjar, PhD,
University of Zagreb, Faculty of Graphic Arts,
Getaldićeva 2,
10000 Zagreb, Croatia
e-mail: ivana.zganjar@grf.unizg.hr