Ovelapping Block-Based Algorithm for Copy-Move Forgery Detection in Digital Images

MOMCILO BRAJIC
John Naisbitt University
Faculty of Computer Science
Bul. umetnosti 29, Belgrade
SERBIA
momcilob@live.com

EVA TUBA
University of Belgrade
Faculty of Mathematics
Studentski trg 16, Belgrade
SERBIA
etuba@acm.org

RAKA JOVANOVIC
Hamad Bin Khalifa University
Qatar Environment and Energy Research Institute
PO Box 5825, Doha
QATAR
rjovanovic@qf.org.qa

Abstract: Widespread use of digital images beside many benefits has some issues. Photography has long ago lost its authenticity. It is important to demonstrate the originality of images in digital forensics, because unfortunately with the progress of the hardware and software industry a photography manipulation is increasingly easier. One of the well know forgery with digital images is so-called copy-move forgery. In this paper we proposed a method for the detection of copy-move forgery. It is a block based method that uses blocks of the size 16*16 divided in 4 smaller blocks with appropriate set of 9 characteristics. The method was tested on standard benchmark images and it proved to be very successful.

Key–Words: Digital image forensics, image forgery detection, copy-move forgery detection, block-based forgery detection algorithm

1 Introduction

We can share a variety of information around the world in a very inexpensive way, through the Internet. The world economy relies entirely on communication via the Internet. The wide availability and low price of the equipment and the technology itself are very facilitating for everyday life. But the medal still have the other side. With the rapid expansion of Internet technology in the world, Internet crime also expands. World web has enabled criminals to do all sorts of criminal activities that threaten all users on the Internet. We have variety of threats from identity, money theft to national security threats. No one is fully protected from these threats. Although many people think that there is a hundred percent protection, it is simply not so. For example, a hacker can get hold of discriminatory photos of a person that he can blackmail in different ways.

Digital forensics investigators need a reliable and stable tools to keep pace with criminals, and if possible to be one step ahead. Digital forensics encompasses many areas. The images are full of information and are very widespread on the Internet. Digital images can be quite easy to change because they do not have any form of protection. Due to the wide availability of software tools on all desktop and mobile platforms one can easily edit any image. Changing the image represents a threat to everyone because, with the help of tools, one can change the meaning and significance of the image very easily. When changed picture begins to spread on social networks that picture can make significant harm. It is therefore very important to be able to determine the originality of the picture. Determining the integrity and originality of the image content is the essence of research in digital image forensics. Digital image forensics in the last ten years has become very important. One of the important papers is the [1]. Due to the method which is reflected in the fact that the image is reversed and divided on circular blocks, the properties of the blocks are obtained by rotating the local binary patterns (LBP). The main things that digital forensics is trying to clarify is the determination of the authenticity of the source image and confirmation of the integrity of the picture. Authentication sources involves the interrogation techniques of the work whether on camera or through some algorithm. Integrity involves examining images by searching for any modification. Digital forensics is divided into active and passive.

Active digital forensics refers to control of digital signatures. The signatures are putted on the images during their creation. Any image change will also change the signature of a greater or lesser extent. Changes to the signature subsequently suggest that the image has been altered. But to determine that the picture is really changed original image as well as image which is supposedly changed are needed. In addition, it is necessary to use very expensive equipment during the verification process.

Passive forensics does not require a comparison of the original and modified images and special equipment. In the paper [2] methods that are good in detecting fraud were listed. Passive forensics in each original image sees a scheme that is permanent. When a change occurs in the image this pattern or a scheme is changing along with the image. A number of methods was given in the paper [3], where an overview of the progress of ways to detect fraud was given.

Forensics of a digital image may be based on the cameras, pixels and others. Copy-paste detection falls under the forensics of pixels. The most widespread image change technique is copy-paste where one part of the image is copied to another part of the same image. Although copies are identical to the original part the copying process can be very skillfully done, so determining the use of copy-paste method is not easy. If there is no post production, this method is a little easier to detect. Discovering this fraud becomes more difficult when the copied part is rotated, cut, extended, etc. Copy-paste technique is also known as copy-move forgery.

In this paper we propose a method for detecting copy-move forgery based on features extracted from blocks of the image. Image is divided into blocks of size 16×16 and further more each block is divided into 4 smaller and equal blocks. Nine different features from these blocks are extracted and used for detecting copy-move forgery.

This paper is organized as follow. In Section 2, literature review is presented. In Section 3 the description of Copy-move forgery is given. In Section 4 the proposed method is described, while in Section 5 we present the experimental results. At the end in Section 6 conclusion of this paper is given.

2 Literature Review

Digital images are widely used and represent very important part of everyday life. This is a reason of numerous applications that deal with digital images. Some applications are used for character recognition [4], [5], some are used for image enhancement [6]. Multilevel image thresholding is used in many application, so this topic is intensively researched [7], [8], [9]. Compression of images is also important topic when deals with digital images [10].

As mentioned before, digital images can be easily changed and that represents a threat. One of the possible changes is so-called copy-move forgery. One part of image is used to cover or changed another part. Many methods for detecting this kind of forgery were proposed.

In [11] method based on blocks and their features was proposed. Features based methods was used in order to improve the accuracy of detection of fraud. The proposed method uses DCT coefficients and properties of discrete Fourier transformation. Features were compared in order to detect fraud and also register the location of the region in the picture that are counterfeited.

In [1] a method where the image was divided into the round blocks was presented. The properties of round blocks were extracted by using rotating uniform local binary pattern. After that the vectors of properties were compared and rigged regions can be located by following the appropriate blocks. Experimental results show that this method was good not only for detecting the forgery on images with JPEG compression and blur, but also for images with regional exchange and flipping.

A method where the picture is divided into blocks with a fixed size and discrete cosine transform was used was proposed in [12]. Discrete cosine transformation was performed on each block and DCT coefficients representing each block. Each cosine transform block was represented by a circular block and four properties have been pulled out to reduce the dimensions of each block. Vectors are lexicographically sorted, and duplicate blocks of the image are compared with the threshold value. Experiments show that the proposed scheme in addition to good results in copy-move fraud also have good results in blurring and has low system requirements.

In [13] an approach that was based on the blocks that use texture of blocks as the basis was considered. The aim of [13] was to examine whether the texture is appropriate for the specific application. Tests were conducted on not compressed as well as on the compressed JPEG images.

In [14] a blind forensic approach for detecting copy move scams was described. Used technique was based on the implementation of the discrete wavelet transform on the input image. The goal of this step was to help in reducing the dimensions. Then, the compressed image was divided into overlapping blocks. Criteria for determining similarity of these blocks, to determine duplicate is the phase correlation. Due to the use of discrete wavelet transformation, detection is carried out at the lowest level of the image. This process significantly reduces the time of detection [14].

Another approach for copy-move detection was proposed in [15]. In that paper algorithm for precise detection of copy-move scam based on the rotational properties was proposed. Rotational properties were calculated in the image. Techniques dense fields proposed in the literature guarantee better performance with w.r.t but with the price which is reflected in a much greater time for implementation. To avoid this shortcoming patch match algorithm is used that is good for dense fields above pictures. The analysis, which used databases that are available online proves that the proposed technique was correct but also faster than other references dealing with the field [15].

Most of the techniques is not good enough to locate parts of the image where the fraud was made. Poor performance is even more the case when the show in the picture has a lot of great parts that are similar. Passive forensics for image copy-move forgery using a method based on DCT and SVD was proposed in [16]. A method that has a much higher percentage of detection with the images with such parts was described. Each image is divided into blocks of the same size and the DCT is applied to each. The results show that the proposed method can detect fraud in the figures with the same region, even when the image is further compressed.

In paper [17] a cellular automata as a way of detecting the fraud was proposed. The essence of this method is that for each block was known cellular automata rules which are related to the changing values of intensity. A similar method was also described in the paper [18]. Based on these rules, copies of blocks were found. For standard copy-move fraud a cellular automata rule was sufficient, however, if the change of the copied part of the primer block was rotated, cellular automata rules complicate significantly. But cellular automata can be used in such cases if filtering application was done before the start of the detection of the fraud [17].

In [19] Kumar et al. proposed using DCT binary vectors. Kumar et al. presented a method for fraud detection based on the contrast with the help of discrete cosine transform vectors. The image was divided into blocks and for each block DCT coefficients were calculated. Further vectors are created for each block on the basis of DCT components. The proposed method can detect fraud when the contrast of the image is changed [19].

Kirchner et al. in [20] proposed a method of detection of fraud where the picture instead of blocks is divided into triangles. Triangles are matched on the basis of their properties, specifically on the color and vectors. The method is designed to cope with the geometric information. Results are made simultaneously with testing the latest methods for comparing blocks [13]. Kirchner et al. underlined that rectangular blocks for detecting the copy-move forgery is not the only way to divide the image.

3 Copy-Move Forgery

Advanced cameras along with software tools allow anyone to easily edit the image. Community professionals dealing with photography began to try to prevent easy manipulation of images with digital signatures, but with no greater success. However the downside of technique with signature is that image needs to be preprocessed before it is printed because of the signature entered. Therefore, the application of signature are very limited. This scam can be detected in the following manner as in the work [21].

Copy-move forgery is an cunning way of changing the image in the sense that part of the image is copied and placed in another part of the image to hide the specific object. Because the copied part of the picture and all of its properties such as texture match the rest of the picture, it is very difficult to detect this kind of fraud. However, every day a new combination of methods appears that facilitate finding the fraud. Thus, the combination of methods dyadic wavelet transform (DyWT) and scale invariant feature transform (SIFT) gives good results as presented in the paper [22].

Copy move forgery is predominantly used for changing the content of pictures, usually to the contours of the area the one in the picture and replaced with some other element which is in the same picture. The simplest way to solve this problem is to use the extensive search, which means that the original image is compared with a cyclic version of the image. This technique requires a large hardware power. This method with blocks is quite prevalent method. The image is divided into blocks that overlap. Then, on the basis of common characteristics blocks that face one another are recognized. The analysis of the blocks is carried out and only those pairs of blocks that are the same distance are recorded. There are different methods to investigate copy-move fraud. One of them is the discrete cosine transform (DCT). The virtue of this method is that the signal energy is reserved for a few coefficients, and the compression operation, for example, should not affected the result greatly. DCT does not work, if the geometric transformation is applied to the duplicated regions. Principal component analysis (PCA) can also be used to display different blocks. This method has proven to be resistant to compression, but rotation can affect the final results. Also, this method can be investigated in a slightly different way [23].

3.1 Features

The basic step in the techniques of protection from copy-move scam is to divide images on the blocks.

The next step is determining the properties of the original blocks to be able to compare them with potential copies to detect the slightest modification. Different properties or features of blocks were used in recent research.

Already mentioned discrete cosine transform (DCT) coefficient can be used. DCT is used because the signal power located on the first few coefficients, while others are smaller. As a result, operations such as the compression will not affect adversely on the first coefficients.

The next method is the Principal component analysis. In this method the coefficients of the blocks in the matrix and calculates the appropriate matrix. There is a new base thanks to eigenvectors of matrix. In order to reduce the dimensions, blocks that go to basic vectors with higher values are used. These results are resistant to compression, however, the rotation would affect the final results.

The next method proposed is discrete wavelet transform (DWT), which divides the image into four smaller. It divides lower frequency components in the blocks that overlap in order to reduce their number and speed up the process of finding the same regions. In these regions singular value decomposition (SVD) are applied. Because the SVD and PCA are similar, SVD will behave in certain situations as well as PCA.

Another way that circumvents the methods used in the compression ratio is to use a method that is based on the colors of the blocks. These colors include red, green and blue. Another set of blocks is divided into two parts in 4 continents. The intensity of a block in relation to the total number of blocks is calculated. Experiments have shown that this method can well cope with JPEG compression, or with Gaussian blurring.

It can be also applied to the method of Fourier Mellin transform (FMT) on the blocks. First, find the value of Fourier Mellin transform for each block and then the results are transferred to coordinate. The vector can be calculated based on the polar values and these values are used for the properties. The tests proved that this method carries well with excellent compression ratio. There are also other methods that are listed in the paper [24]. Method that was presented allows making it easier to find the location of deception. An interesting method was explained in the paper [15], where method uses a densely compacted neighboring fields. Method facilitates easier detection of fraud in the picture.

4 Our Proposed Method

As already mentioned copy-move detection is usually based on overlapping blocks. In [25] a similar method was proposed. After obtaining the vectors of features that represent the blocks, vectors are sorted lexicographically in order to facilitate detection. Blocks whose vectors are similar and close can be easily detected by shift vector.

In this paper we divide image into blocks of size 16×16 and each of these blocks is represented with the 9 characteristics. These characteristics are as follows. First, the average value of the intensity of the block is calculated. Then, each block division is divided into to four identical subblocks and the remaining 8 characteristics concerning the relationship between block and subblock. Four characteristics mark the ratio of the average intensity of each of the washers with the block, and the remaining four indicate the difference of the average intensity of each subblock and block of which they are part. This can be formally written as:

$$f_i = \begin{cases} f_i = Ave(B) & \text{if } i = 1, \\ Ave(S_{i-1})/(4Ave(B) + \varepsilon_1) & \text{if } 2 \le i \le 5, \\ f_i = Ave(S_{i-5}) - Ave(B) & \text{if } 6 \le i \le 9. \end{cases}$$

Thus obtained characteristics are normalized to the rank of 0 to 255. This is done by the following formula:

$$x_i = \begin{cases} \lfloor f_i \rfloor & \text{if } i = 1, \\ \lfloor 255 \times f_i \rfloor & \text{if } 2 \le i \le 5, \\ \lfloor 255 \times \frac{f_i - m_2}{m_1 - m_2 + \varepsilon_2} \rfloor & \text{if } 6 \le i \le 9, \end{cases}$$

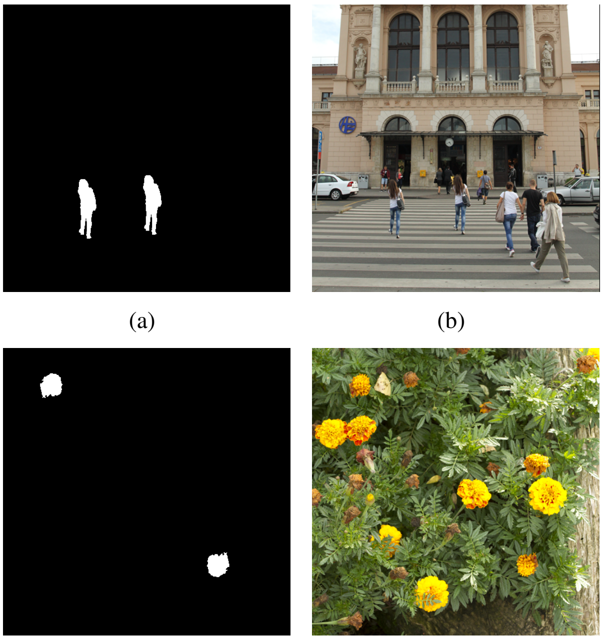
where $m_1 = \text{max} f_i,\ 6 \le i \le 9$ and $m_2 = \text{min} f_i,\ 6 \le i \le 9$

In order to increase the chance of image protection from different modifications, it is easier to manipulate the image when is divided into blocks of size 16x16 using the vector with nine dimensions, which can be moved as a block, which consists of four blocks of equal size S_a, S_b, S_c, S_d. So f1 has an average intensity of the block B, and f2, f3, f4, f5 are intensities blocks of S_a, S_b, S_c, S_d. These 9 values sometimes contain duplicate information, they have a greater chance to prevent changes to the image, such as for example is compression. Rotating is discovered by leveraging image with its rotated versions. The examples are based on 270 and 180 degrees. If this is how we are working we can detect fraud at any angle. To find a copied image, we combine the three versions of the image that are rotated with the original image and with these combined images the fraud is found.

5 Experimental Results

Experiments were performed on computer with following performances: Intel ® Core$^{\text{TM}}$ i7-3770K CPU at 4GHz, 8GB RAM, Windows 10 Professional OS. Proposed method was implemented in Matlab version R2015a.

In this paper we used the database for a copy-moved forgery detection proposed in [26]. The dataset consists of 260 forged image sets. Every image set includes forged image, two masks and original image. Images are grouped in 5 categories according to applied manipulation: translation, rotation, scaling, combination and distortion. Also, post-processing methods, such as JPEG compression, blurring, noise adding, color reduction etc., are applied at all forged and original images. Examples of dataset are shown in Fig. 1.

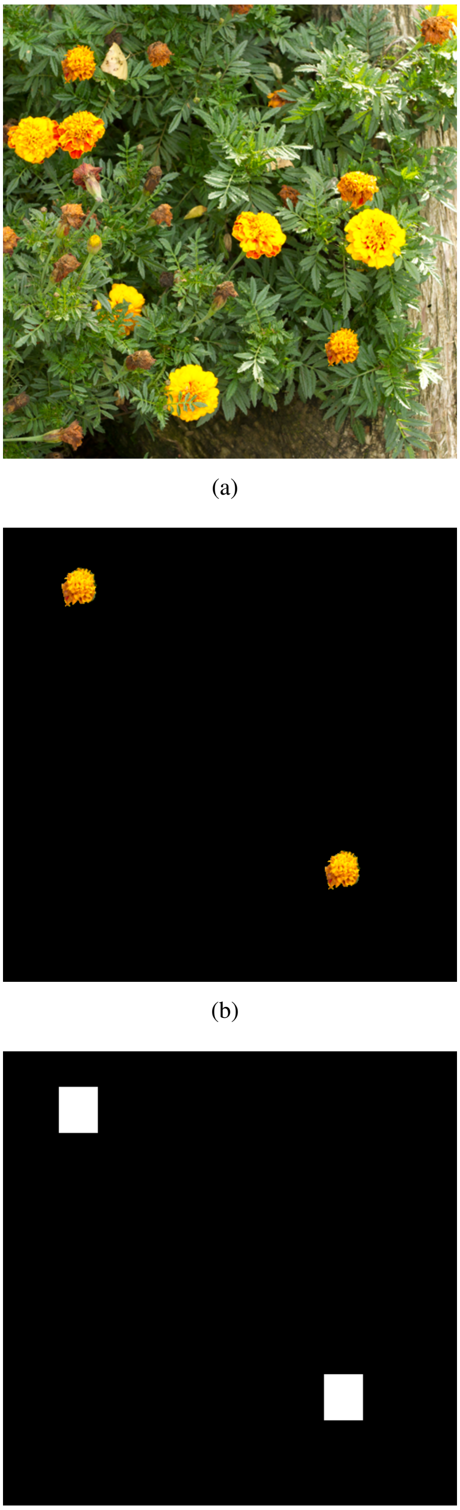


(a) (b)

(c) (d)

Figure 1: Example of dataset

In Fig. 2, Fig. 3 and Fig. 4 the result of our proposed algorithm are shown. Fig. 2(a) is a picture of nature where the flower is copied. Copied parts are shown in Fig. 2(b). Our algorithm detect copied figures as it can been seen in Fig 2(c). Proposed algorithm was able to recognize copied regions. Fig. 3 represents second example where the car is copied. Similar to Fig. 2, Fig. 3(a) is an image that contain copy-move forgery, while in Fig. 3(b) copied regions are shown. Recognition of proposed algorithm is represented in Fig. 3(c). In this case our proposed algorithm was also showed as good. The third example shows the copied pigeon and it is presented in Fig. 4. It can been seen that our proposed algorithm successfully detects image manipulation.

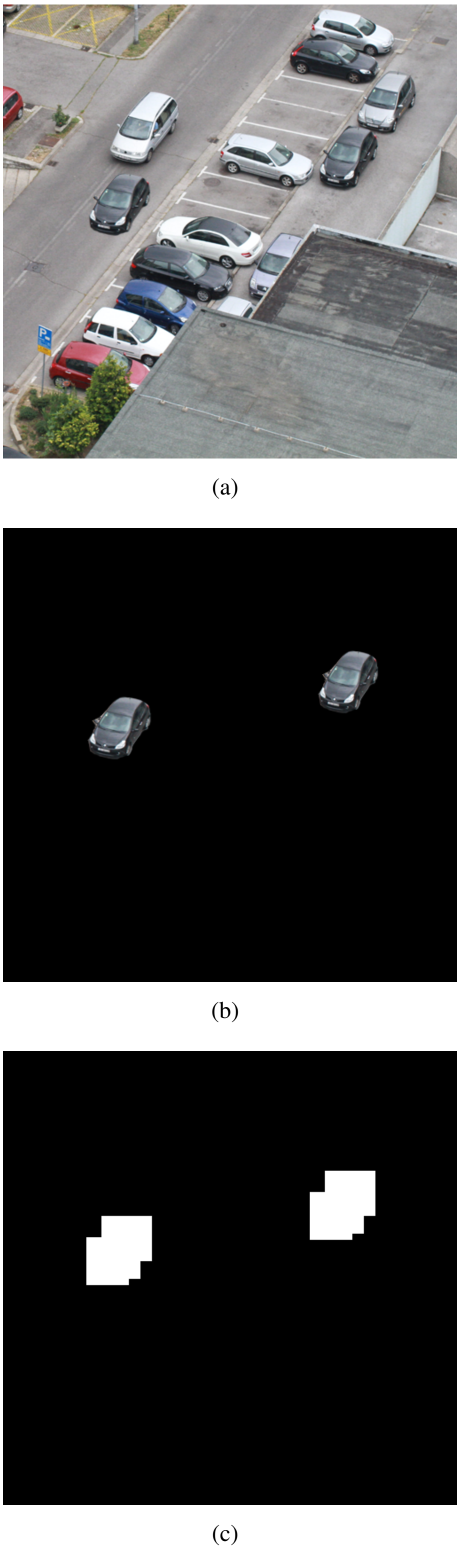


(a)

(b)

(c)

Figure 2: Experimental results (a) Original, (b) Mask, (c) Recognized regions

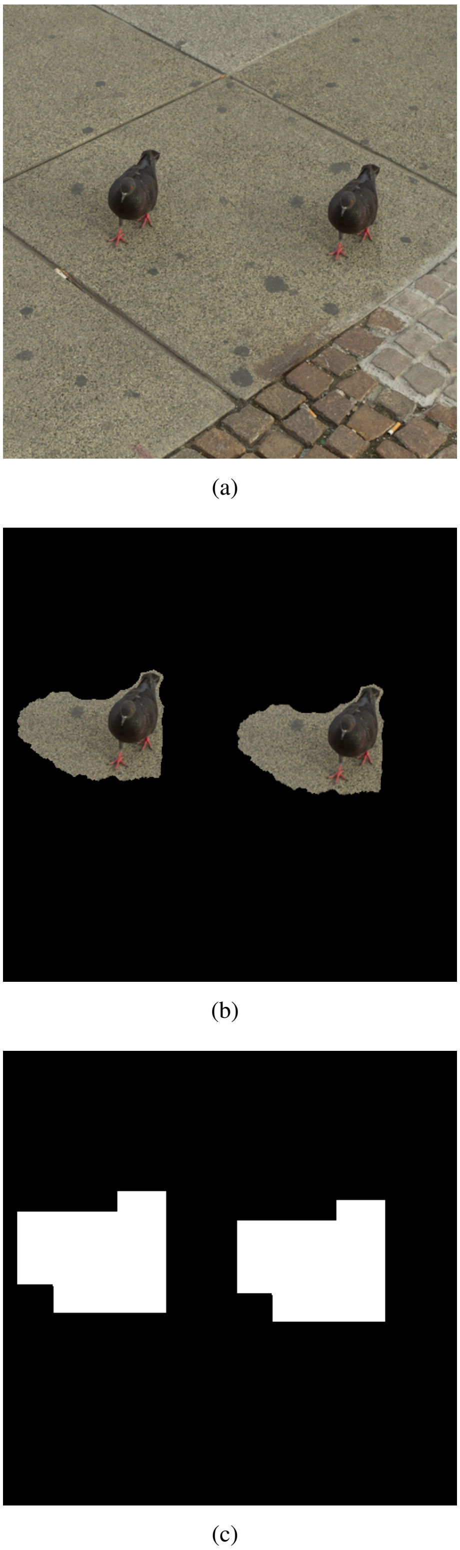


(a)

(b)

(c)

Figure 3: (a) Original, (b) Mask, (c) Recognized regions



(a)

(b)

(c)

Figure 4: (a) Original, (b) Mask, (c) Recognized regions

6 Conclusion

In this paper we proposed an algorithm for copy-move forgery detection. Proposed method is based on block analysis. It divides an image into blocks of the size 16x16 using the vector with nine elements which are determined from four smaller blocks of equal size

4x4. Proposed method was tested on standard benchmark images from [26]. In all cases it successfully detected copy-move forgery, including cases with rotation and compression. Future research may include different features extracted from 4 sub-blocks or different divisions into sub-blocks as well as the size of the original block.

References:

[1] L. Li, S. Li, H. Zhu, and X. Wu, "Detecting copy-move forgery under affine transforms for image forensics," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1951–1962, 2014.

[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on information forensics and security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[3] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," *Forensic science international*, vol. 231, no. 1, pp. 284–295, 2013.

[4] Z. Haddad, Y. Chen, and J. L. Krahe, *Image Processing and Pattern Recognition Tools for the Automatic Image Transcription*, pp. 197–203. Cham: Springer International Publishing, 2016.

[5] E. Tuba and N. Bacanin, "An algorithm for handwritten digit recognition using projection histograms and SVM classifier," in *23rd Telecommunications Forum Telfor (TELFOR)*, pp. 464–467, Nov 2015.

[6] M. Jordanski, A. Arsic, and M. Tuba, "Dynamic recursive subimage histogram equalization algorithm for image contrast enhancement," in *23rd Telecommunications Forum Telfor (TELFOR)*, pp. 819–822, Nov 2015.

[7] M. Tuba, "Multilevel image thresholding by nature-inspired algorithms-a short review," *The Computer Science Journal of Moldova*, vol. 22, no. 3, pp. 318–338, 2014.

[8] I. Brajevic and M. Tuba, *Cuckoo Search and Firefly Algorithm Applied to Multilevel Image Thresholding*, pp. 115–139. Cham: Springer International Publishing, 2014.

[9] M. Tuba, N. Bacanin, and A. Alihodzic, "Multilevel image thresholding by fireworks algorithm," in *25th International Conference Radioelektronika (RADIOELEKTRONIKA)*, pp. 326–330, April 2015.

[10] M. Tuba and N. Bacanin, "Jpeg quantization tables selection by the firefly algorithm," in *Multimedia Computing and Systems (ICMCS), 2014 International Conference on*, pp. 153–158, April 2014.

[11] R. Singh, A. Oberoi, and N. Goel, "Copy move forgery detection on digital images," *International Journal of Computer Applications*, vol. 98, no. 9, pp. 17–22, 2014.

[12] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic science international*, vol. 214, no. 1, pp. 33–43, 2012.

[13] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgery detection via texture description," in *Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence*, pp. 59–64, ACM, 2010.

[14] E. S. Khan and E. A. Kulkarni, "An efficient method for detection of copy-move forgery using discrete wavelet transform," *International Journal on Computer Science and Engineering*, vol. 2, no. 5, pp. 1801–1806, 2010.

[15] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense field copy-move forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284–2297, 2015.

[16] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic science international*, vol. 233, no. 1, pp. 158–166, 2013.

[17] D. Tralic, P. L. Rosin, X. Sun, and S. Grgic, "Copy-move forgery detection using cellular automata," in *Cellular Automata in Image Processing and Geometry*, pp. 105–125, Springer, 2014.

[18] D. Tralic, S. Grgic, X. Sun, and P. L. Rosin, "Combining cellular automata and local binary patterns for copy-move forgery detection," *Multimedia Tools and Applications*, pp. 1–23, 2015.

[19] S. Kumar, J. Desai, and S. Mukherjee, "Copy move forgery detection in contrast variant environment using binary DCT vectors," *International Journal of Image, Graphics and Signal Processing*, vol. 7, no. 6, pp. 38–44, 2015.

[20] M. Kirchner, P. Schöttle, and C. Riess, “Thinking beyond the block: block matching for copy-move forgery detection revisited,” in *SPIE/IS&T Electronic Imaging*, pp. 940903–940903, International Society for Optics and Photonics, 2015.

[21] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, “Copy-move forgery detection and localization by means of robust clustering with j-linkage,” *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 659–669, 2013.

[22] V. Anand, M. F. Hashmi, and A. G. Keskar, “A copy move forgery detection to overcome sustained attacks using dyadic wavelet transform and sift methods,” in *Asian Conference on Intelligent Information and Database Systems*, pp. 530–542, Springer, 2014.

[23] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, “Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes,” *Journal of Visual Communication and Image Representation*, vol. 29, pp. 16–32, 2015.

[24] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, “Copy move forgery detection using DWT and SIFT features,” in *13th International Conference on Intellient Systems Design and Applications*, pp. 188–193, IEEE, 2013.

[25] H.-J. Lin, C.-W. Wang, Y.-T. Kao, *et al.*, “Fast copy-move forgery detection,” *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188–197, 2009.

[26] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, “CoMoFoD - new database for copy-move forgery detection,” in *55th International Symposium ELMAR*, pp. 49–54, Sept 2013.