A new deep learning-based method to detection of copy-move forgery in digital images

Gul Muzaffer
Department of Computer Engineering
Karadeniz Technical University
Trabzon, Turkey
gulmuzaffer@ktu.edu.tr

Guzin Ulutas
Department of Computer Engineering
Karadeniz Technical University
Trabzon, Turkey
guzin@ieee.org

***Abstract*—Thanks to ease of using image manipulation programs, copy move forgery is the easiest image modification approach, which aims to duplicate or remove objects in the image. The methods to detect this type of forgeries are partitioned into; block-based, keypoint-based approach that use hand-crafted features. A new deep learning-based forgery detection scheme is presented. An existing trained model AlexNet is utilized to extract feature vectors of image overlapped subblocks. After obtaining features, the similarity between feature vectors has been investigated for the detection and localization of forgery. The method has higher accuracy rate than the considered traditional method in the literature as reported in the obtained test results.**

***Keywords*—Deep learning, AlexNet, copy move forgery**

I. INTRODUCTION

Recently the importance and usage areas of digital images have increased, so the malicious people have begun to manipulation on digital images. In literature digital image forgeries are detected by active and by passive image authentication methods. While the active forgery detection methods utilize the digital watermarks/signatures, the passive methods authenticate the images with using statistical features of image, they do not need any extra information. Copy move forgery which is a passive detection method, can be realized without requiring any expertise using PhotoShop, in Fig. 1 an example is given.

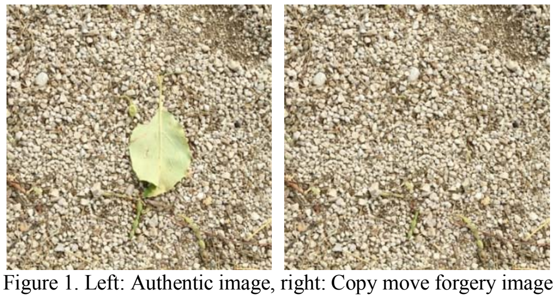

Figure 1. Left: Authentic image, right: Copy move forgery image

In literature lots of methods proposed by researchers, while keypoint-based methods use keypoints' descriptors to detect forgery clues, block-based methods utilize the overlapped image patches' features. The first method to detect this type forgeries is presented in 2008 [1]. The suspected image is split into overlapped squared blocks firstly. DCT features of the blocks are obtained and then matching of them is done. In literature lots of block-based method is proposed with different approach [2-10]. Because of the block-based method have high execution time, to cope with this problem keypoint-based methods are proposed. The methods in this class the keypoints are extracted from all input image and then match corresponding descriptors to reveal forgery. The keypoint based-methods have been proposed after the Huang and others' method [11]. The method uses SIFT (Scale invariant feature transform) to obtain interest pixels of the input image. After that the SIFT keypoints are matched with best bin first nearest neighbor approach. After this work lots of keypoint-based methods are proposed [12-20]. As a disadvantage of these methods; if the forgery operation is done with low contrast regions, keypoint-based methods cannot detect this forgery, because they cannot obtain enough keypoints on these regions. And, a hybrid method has been proposed to detection of this type of forgery [21]. All mentioned studies use hand-crafted features. In recent studies, deep learning-based methods have been implemented in image tasks for example image classification, image retrieval etc. with higher performance than hand crafted methods. In this work deep learning-based forgery detection method with higher performance is proposed

In the next section, the stages of the suggested scheme are presented in Section 2. After that the empirical study reports are given in next part and lastly Section 4 gives the conclusion.

II. PROPOSED METHOD

In Figure 2, general steps of the method are given. It consists of three basic steps:

- Deep-learning based feature extraction
- Feature matching
- Post-processing.

The details of these stages will be presented during the following sections.

978-1-7281-1013-4/19/$31.00 ©2019 IEEE

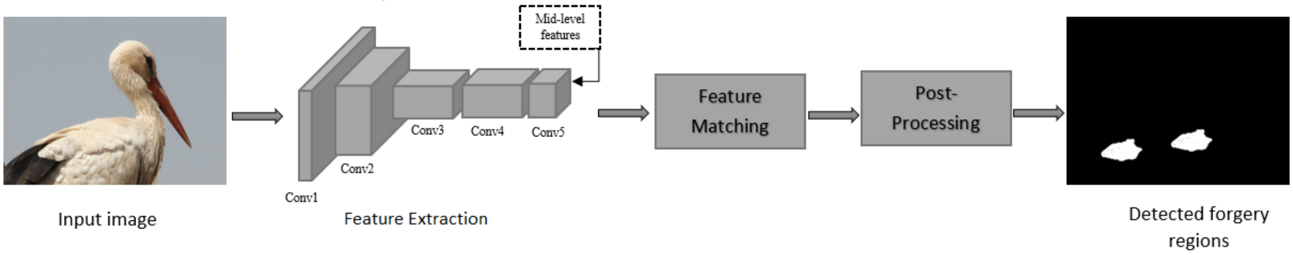

Fig.2. The main steps of the presented scheme

A. Deep-Learning Based Feature Extraction

Firstly, the overlapped sub-square blocks are obtained from the image with the size of 16. After that CNN architecture is used to obtain block features. We have chosen the pre-trained AlexNet model that have 8 layers because of having lower training time. The selected model is proposed by Krizhevsky et al. in 2012 is trained on ImageNet database [22]. We use the mid- level feature from "conv5" layer of the AlexNet model. So that 256-dimensional feature vectors are obtained represented each block. It is also applied the PCA for dimension reduction. In this way the feature vector dimensions are reduced from 256 to 20.

B. Feature Matching

After obtain feature matrix M, to reveal the existence of forgery, the similarity searching is done. For this purpose, firstly feature matrix M, is lexicographically sorted to speed up the matching step. After that the similarity of vectors are presented with Euclidean distance. The distances of vectors are compared with a predetermined threshold ∂, by given Eq. (1) so that the candidate matching vectors are determined. (We set the $\partial = 1.5$ empirically)

$$f^i = (f_1^i, f_2^i, \ldots, f_{10}^i) \ , \sqrt{\sum_{k=1}^{10} (f_k^i - f_k^j)^2} \le \partial \tag{1}$$

In the next step of matching, the candidate matches are checked according to the Euclidean distance among matched block, they must be higher than threshold represented β, to avoid false matches. When (x_i, y_i) is the upper left coordinate of f^i and (x_j, y_j) is the upper left coordinate of f^j, the distance d is calculated as $d = \sqrt{(x_{i-}x_j)^2 + (y_{i-}y_j)^2}$. And for matching of two vector the condition of $d \ge \beta$ must provide. (We set the $\beta =$ experimentally)

C. Post Processing

In this step, firstly possible false matches are eliminated. For this purpose, the shift vector between matched blocks are calculated. (x_i, y_i) and (x_j, y_j) are the upper left coordinates of the suspicious pairs the shift vectors are obtained with $|x_i - x_j|$, $|y_i - y_j|$ values. And it is checked that the number of blocks that have same shift vector whether exceeds a predetermined threshold value γ (We set the $\gamma = 32$ experimentally) If this condition is satisfied, it is proved that copy move forgery is done with the related blocks. Finally, the morphological dilation operation is applied for filling possible gaps and closing operation is applied to more accurately localization of forged by irregular regions.

III. Experimental Results

Here, the comparative test results of our method and the methods in [16, 18] are given. The test images have selected from public available image dataset GRIP, included copy move forgeries (which have textured, mixed and smooth characteristic) [23]. The success of the methods is given with pixel-based test which is about the detection of each pixels forged or not. F-measure given in Eq. 3 is used to performance evaluation of the considered and proposed methods. Higher F-measure result indicates its superior performance to marking the forged regions.

$$\text{F-measure} = 2 * \frac{T_p}{2{*}T_p + F_N + F_p} \tag{3}$$

where, T_p points out the count of detected tampered pixels truly, F_p represents the incorrectly detected tampered pixels and F_N shows the number of incorrectly non-detected pixels.

The average pixel-based performance of the method and comparison results with others is given Table 1. This table shows that the presented scheme has higher detection rate than considering techniques when selected plain copy-move forgery images.

TABLE I. Average detection results

Method	F-measure Pixel Level
[16]	0,58
[18]	0,91
Proposed method	0,93

It is also given the visual results of the methods where while correctly detected forged pixels are represented by green colour pixels, falsely detected pixels are represented with red colour and white colour represents forged regions that cannot be detected by the method.

Fig. 3(a) shows that [16] and [18] have many false alarms if forged image has similar regions and also for Fig. 3 (c) the method [16] has lots of false alarm. In contrast these methods, the proposed method have marked fake and original regions more accurately. In Fig. 3(b) a forged image is given with smooth region. The SIFT keypoint based method [16] have not detected the forgery, since the method cannot extract enough keypoints in this region. And for the examples given in (d) and (e) the presented method locates the duplicated regions more accurately. As a summary of the given visual results, it is clearly seen that our detection method detects forged regions more truly than the others [16, 18], even if the test image has similar or it has smooth regions.

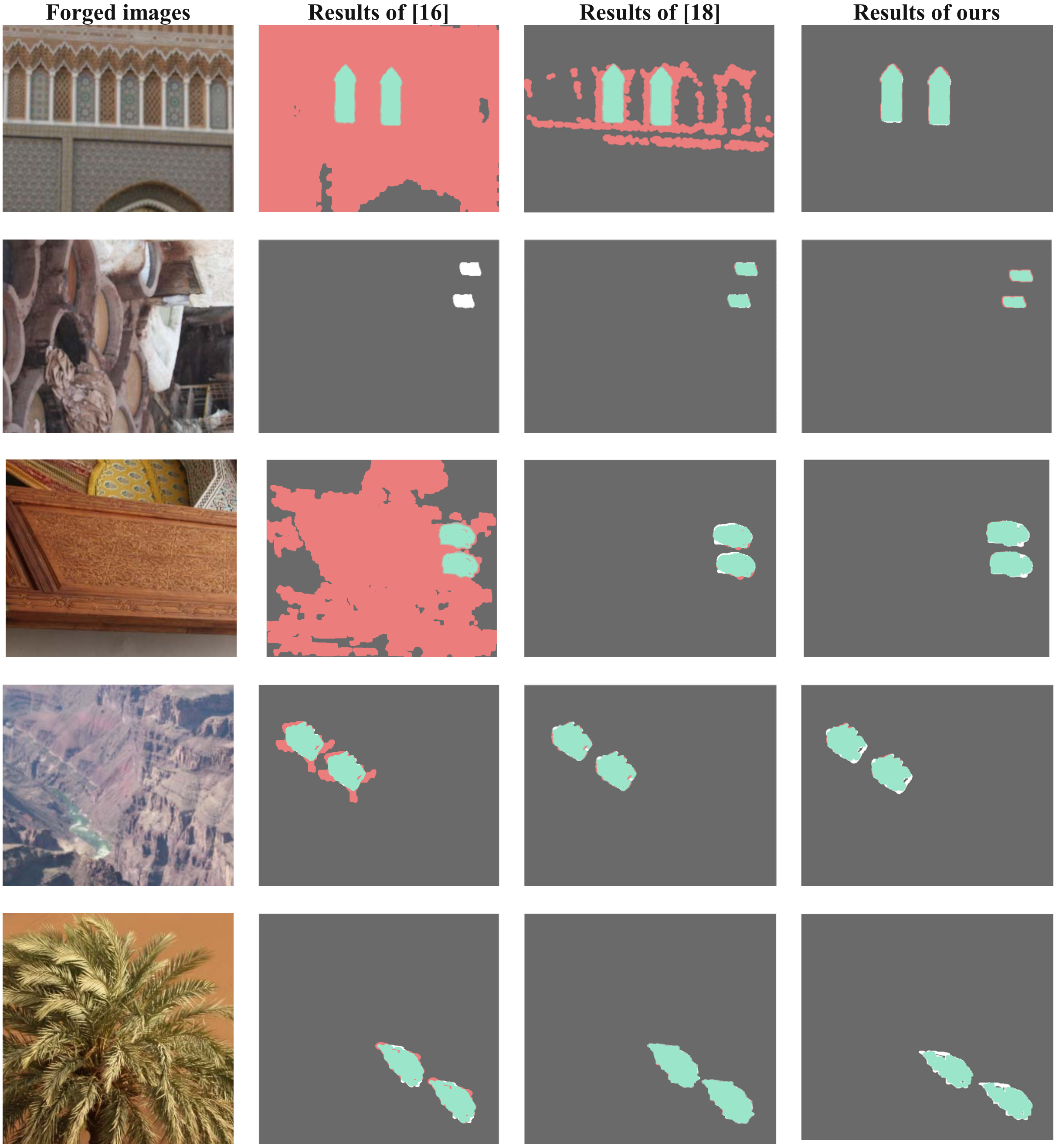

Figure. 3. The obtained outputs on some forgery examples from the database. The results are obtained by the methods from left to right: [16], [18] and proposed method.

IV. Conclusion

In this study, deep learning-based framework is presented to detection and localization of copy move forgeries instead of using tradition features extraction techniques. The method uses the Pretrained AlexNet convolutional neural network to obtain image sub-blocks' features. After that, matching of them are realized, and finally false match elimination is done. It is proven with the test results that the proposed scheme more successful than referenced works. It is aimed to propose more robust method to obtain better performance under several conditions in our next work.

References

[1] Fridrich, A. J., Soukal, B. D. and Lukáš, A. J., Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop (DFRWS), 2003.

[2] Popescu, A. and Farid, H., Exposing Digital Forgeries by Detecting Duplicated Image Regions, Tech. Rep., TR2004-515, Dartmount Collage, 2004.

[3] S. Khan, A. Kulkarni, "Detection of copy-move forgery using multiresolution characteristic of discrete wavelet transform", Proc. Int. Conf. Workshop Emerg. Trends Technol. (ICWET), pp. 127-131, 2011.

[4] Mahdian, B. and Saic, S., Detection of Copy-Move Forgery Using a Method Based on Blur Moment Invariants, Forensic Sci. Int., 171 (2007) 180–189.

[5] Bayram, S., Sencar, H. T. and Memon, N., An Efficient and Robust Method for Detecting Copy-Move Forgery, IEEE International Conference on Acoustics, Speech and Signal Processing, Nisan 2009, New York, 1053 – 1056.

[6] L. Li, S. Li, and H. Zhu, “An efficient scheme for detecting copy-move forged images by local binary patterns,” Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 46–56, 2013.

[7] J. Zhang, Z. Feng and Y. Su, “A new approach for detecting copy-move forgery in digital images,” 11th IEEE Singapore International Conference on the Communication Systems, ICCS, 2008.

[8] Bravo-Solorio, S. and Nandi, A.K., Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling, Intl. Conference on Acoustics, Speech and Signal Processing, May 2011, Prague, 1880–1883.

[9] Ryu, S., Kirchner, M, Lee, M. and Lee, H., Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments, IEEE Transaction on Information Forensics and Security 8, 8 (2013) 1355–1370.

[10] H. Moradi-Gharghani, and M. Nasri, “A new block-based copy-move forgery detection method in digital images”, In: Proc. of International Conf. On Communication and Signal Processing, pp.1208-1212, 2016.

[11] Huang, Y., Lu, W., Sun, W. and Long, D., Improved DCT Based Detection of Copy Move Forgery in Images, Forensic Science International, 206 (2011) 178–184.

[12] Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D. and Serra, G., A SIFT-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery, IEEE Transactions on Information Forensics and Security, 6, 3 (2011) 1099–1110

[13] 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. 659–1669, 2013.

[14] X. Bo, W. Junwen, L. Guangjie, D. Yuewei, "Image copy-move forgery detection based on SURF", *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, pp. 889-892, Nov. 2010.

[15] Zhu, Y., Shen, X. and Chen, H., Copy-Move Forgery Detection Based on Scaled ORB, Multimedia Tools and Applications, 75, 6 (2015) 1-15.

[16] Li J, Li X, Yang B (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf. Forensics Secur 10(3):507–518.

[17] S. Wenchang, Z. Fei, Q. Bo, and L. Bin, “Improving image copy-move forgery detection with particle swarm optimization techniques,” in Proc. in China Communications, vol. 13, no. 1, pp. 139-149, Jan. 2016.

[18] M. Zandi, A. Mahmoudi-Aznaveh and A. Talebpour, “Iterative Copy -Move Forgery Detection Based on a New Interest Point Detector,” Transactions on Information Forensics and Security, 2016.

[19] Li, Y., Zhou, J. 2016. “Image copy-move forgery detection using hierarchical feature point matching”, APSIPA Transactions on Signal and Information Processing.

[20] F. Yang, J. Li, W. Lu, J. Weng, ‘Copy-move forgery detection based on hybrid features’, Engineering Applications of Artificial Intelligence, Volume 59, 73-83, 2017.

[21] Zheng J, Liu Y, Ren J, Zhu T, Yan Y, Yang H (2016) Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidim Syst Sign Process 1-17.

[22] A. Krizhevsky, I. Sutskever, and G. Hinton, “Imagenet classification with deep convolutional neural networks,” in Advances in neural information processing systems, pp. 1097–1105, 2012.

[23] D. Cozzolino, G. Poggi, and L. Verdoliva, “Copy-move forgery detection based on PatchMatch,” in IEEE International Conference on Image Processing, Paris, France, 27-30 Oct. 2014.