Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **6**, Number **2**, May **2021**

Image Splicing Detection Scheme Based on Error Level Analysis and Local Binary Pattern

Yi-Jia Zhang, Tong-Tong Shi

School of Information Science and Technology
Zhejiang Sci-Tech University
Hangzhou 310018, P. R. China
waiting@zstu.edu.cn

Zhe-Ming Lu

School of Aeronautics and Astronautics
Zhejiang University
No. 38, Zheda Road, Hangzhou 310027, P. R. China
Corresponding author: zheminglu@zju.edu.cn

Received October 2020; revised January 2021

Abstract. *Information security is one of the major challenges in today's world, as dependency on multimedia information is increasing day by day. The rapid development of science and technology makes it easy for every ordinary user to obtain image and video information through image editing software and modify it to a certain extent. In order to verify the authenticity of the image, tampering detection is required. Among them, splicing tampering is one of the more common types of tampering. This paper proposes a hybrid feature image splicing detection scheme based on Error Level Analysis (ELA) and Local Binary Pattern (LBP). The features of the two algorithms LBP and ELA focus on global features and local features respectively, so combining them can improve the accuracy. Then, we feed the mixed features into Bagged Trees for classification. We verified our scheme on three public datasets, and we also compared with a single algorithm to prove the superiority of our proposed scheme. At the same time, we also find the splicing area through the improved ELA algorithm. Experiments show that our method can accurately locate the tampered area.*
Keywords: Image splicing detection, Information security, Error Level Analysis, Local Binary Pattern, Bagged Trees

1. **Introduction.** Today, science and technology are developing rapidly in all walks of life, and people around the world have become more intelligent by using these rapidly developing science and technology. Today, all kinds of information can be uploaded directly or indirectly to computers, the Internet, or intelligent systems. Digital information includes media forms such as video, audio, and images. Today, social media is becoming more and more popular. Among them, digital images bring great convenience to people's lives, but also introduce a series of problems in network social management and judicial evidence collection. Digital images are easier to tamper with and spread than traditional film photos, which will bring huge tremendously to the identification of audio-visual materials in judicial forensics, the authenticity review of news materials in news media units, and the confirmation of false image information in the analysis of online public opinion. In view of this situation, digital image tampering detection technology has gained wide attention, and has gradually become a research hotspot in the field of

image forensics in recent years, and has been rapidly developed. Based on the in-depth study of the mainstream passive tampering detection technology, this paper proposes a series of key technologies and theoretical methods for passive stitching detection of digital images based on the statistical characteristics of the image, which is the most common way of digital image tampering.

In recent years, due to the rapid development of image forgery technology, researchers have proposed a variety of research methods, divided into active and passive directions. In an earlier study [1], a method of actively embedding watermarks in images was used to extract features. In passive detection [2], splicing forgery is a kind of pixel-based image forgery, which is also one of the most researched forgery methods. Splicing operation is mainly to splice the content of two or more images into one image. In the following paragraph, we will introduce some promising methods proposed by different researchers.

Local Binary Pattern (LBP) is an effective image texture description operator. It has been successfully applied in the field of image content classification and texture description. The well-known application of LBP features is in the field of face recognition [3]. Recently, the combination of LBP and traditional algorithms [4-6] is increasingly used in image mosaic detection. Reference [7] uses the Gray Level Co-occurrence Matrix (GLCM) to locate the tampered area of the image for feature extraction, and further uses the Euclidean distance and Hellinger distance for feature matching. This method gives an accuracy of 79.9%. Reference [8] proposed a technique called error level analysis (ELA) for image forensics, which can analyze images by varying degrees of compression. Reference [9] discusses and proves that this technique has high reliability in image splicing detection. Reference [10] proposed a method for detecting image forgery in lossy compressed digital images using ELA, and filtering its noise components through automatic wavelet soft thresholds. In [11], the ELA algorithm is combined with the Laplacian operator to achieve image tampering detection, where the Laplacian operator is used as an auxiliary algorithm to verify the accuracy of the ELA. In [12], it is demonstrated that ELA can be used for tampering detection and localization, and the localization function can be achieved by extracting the histogram features of ELA and returning the coordinates. Most of the above works are analyzed using traditional machine learning methods, but recently, deep learning methods have also been gradually applied to counterfeit detection [13]. For example, Reference [14] proposed the use of a dual-stream faster R-CNN (Region-Convolutional Neural Network) network and trained it end-to-end to detect tampered image areas. Based on the previous article, the literature [15] changed the spatial domain feature of one of the two streams to ELA, and also detected tampering regions. The use of deep learning methods to extract image features [16] has gradually been applied in various fields [17-20].

Even in the recent literature, many tamper detection techniques are already available, but in order to develop the reliability of forgery detection, we still need to further improve the accuracy. In this paper, we propose a passive detection method based on ELA and LBP for detecting splicing and tampering in images. First, we pre-process the pictures, including re-sizing and applying ELA algorithm to transform the pictures. Secondly, perform ELA feature extraction and LBP feature extraction on the pictures respectively. Then, these features are fused and fed into the classifier, and these features are classified into real images and tampered images. In terms of the classification accuracy of the three data sets, our proposed hybrid method outperforms the performance of a single algorithm. Finally, we can accurately locate the tampered area through the improved ELA method.

The rest of the paper is organized as follows. Section 2 reports the related works and explains our proposed method in detail. Section 3 discusses the experimental result of our proposed method. Finally, Section 4 concludes the whole paper.

2. **Proposed methodology.** In this paper, we propose an efficient and accurate ELA based method for image splicing forgery detection and localization. First, pre-process the image and crop each image to the same size to facilitate subsequent experiments. Then extract the ELA and LBP features from the preprocessed image, and perform feature fusion on them. After obtaining these features, we mix the three types of features into the classifier for classification. Due to the particularity of the ELA picture, it can intuitively reflect the image tampering, so we use this method to locate the tampered area. After a series of post-processing, including morphological operations and filtering, we can get the accurate tampered area. Fig. 1 presents the framework of our proposed image forgery detection scheme.

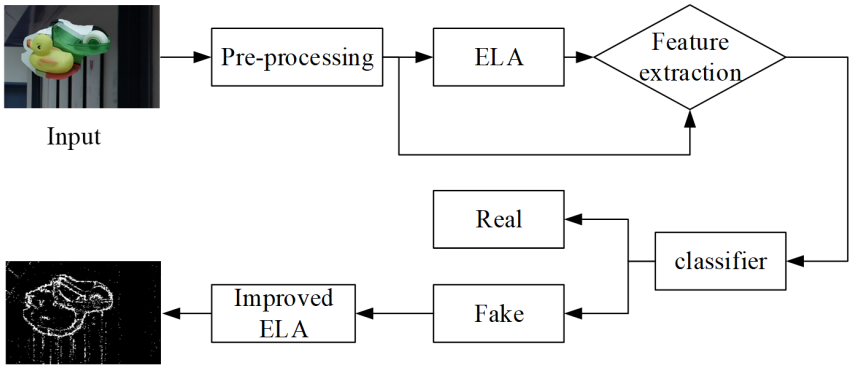


FIGURE 1. Framework of the proposed scheme

2.1. **Feature Extraction.** Feature extraction plays an important role in the detection and classification process. Different feature extraction methods have been proposed and applied in various image processing fields. In this section, a feature extraction method for image splicing detection based on ELA and LBP mixed features is presented. For the convenience and accuracy of the subsequent feature extraction process, we first pre-process the image. By resizing the input image, adjusting the picture to a size of $512 \times 512 \times 3$, and then applying the ELA algorithm to it, we can get the ELA picture.

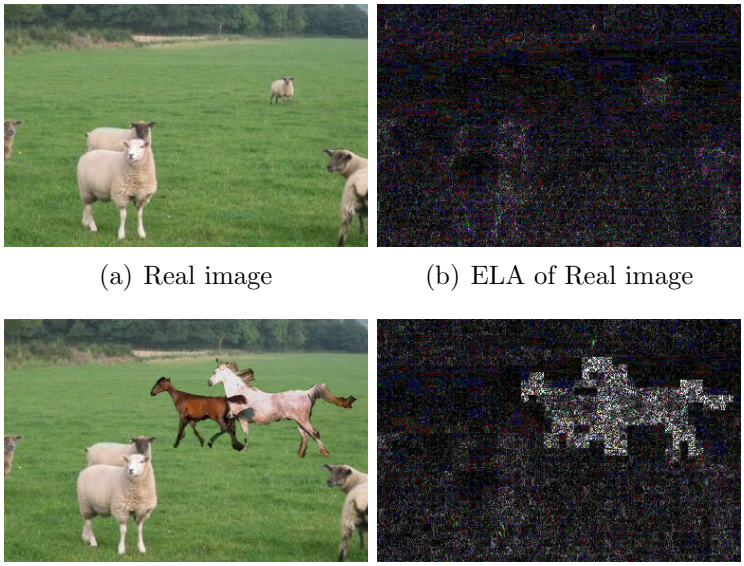
2.1.1. *Error Level Analysis (ELA).* Error Level Analysis is a forensic method to identify portions of an image with a different level of compression. The ELA algorithm works on image grids, compressed independently, having a size of 8×8 pixels. The 8×8 dimension was chosen after numerous experiments with other sizes, any matrices of sizes greater than 8×8 are harder to be mathematically manipulated or not supported by hardware, meanwhile any matrices of sizes less than 8×8 don't have enough information. They result in poor quality compressed images. The image quality can be summarized by calculating the difference between the average value (brightness) and CrCb (chroma) from the quantization table Y, as shown in Eq. (1). The graph of the quality value of the ELA algorithm is shown in Fig. 2, where the difference error level in some blocks can define the modification area.

$$\begin{aligned} \mu &= (Y + C_r + C_b)/3 \\ \Delta &= |Y - C_r| \times (1 - 0.51) + |Y - C_b| \times (1 - 0.51) \\ Q &= 100 - \Delta - \mu \end{aligned} \tag{1}$$

ELA can be used for common image forgery operations and has an active role in image forensics and copyright information. The following is an example of ELA, the forgery method is the splicing operation, as shown in Fig. 3.

81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81

FIGURE 2. The quality values in the ELA algorithm.



(a) Real image (b) ELA of Real image

(c) Fake image (d) ELA of Fake image

FIGURE 3. Example of ELA algorithm

We will extract the ELA features of the real image and the tampered image separately. The statistical characteristics such as the mean, standard deviation and kurtosis of the gray histogram and the texture characteristics such as the mean, contrast and entropy of the gray level co-occurrence matrix are used to describe different areas of the image. The calculation formula of the gray level co-occurrence matrix is shown below.

Mean (MEAN): The mean value reflects the regularity of the texture. The messy texture is difficult to describe and the value is small; the regularity is easy to describe and the value is large.

$$MEAN = \sum_{a} a \sum_{b} \delta_{\phi,d}(a,b) \tag{2}$$

where a and b mean the rows and columns of the elements of the gray level co-occurrence matrix, ϕ means the direction, d means the distance, and $\delta_{\phi,d}(a,b)$ means the joint distribution of the two pixels with spatial positional relationship.

Contrast (CON): The contrast reflects the degree of change of the gray level of the partial image. The greater the difference between gray levels in the image, the sharper the edge of the image, and the greater the contrast.

$$CON = |a-b|^k \delta_{\phi,d}^{\lambda}(a,b) \tag{3}$$

where k is often set to be 2, λ is often set to be 1.

Entropy (ENT): It is a measure of the amount of information in the target image. Texture information is also an aspect of entropy measurement. The elements in the image are more dispersed, the greater the entropy, and the smaller the conversely. The size of the entropy represents the uniformity or complexity of the target image texture.

$$ENT = \sum_{a,b} \delta_{\phi,d}(a,b) \log_2 \delta_{\phi,d}^{\lambda}(a,b) \tag{4}$$

2.1.2. *Local Binary Pattern (LBP).* LBP is an abbreviation of Local Binary Pattern, which has significant advantages such as gray scale invariance and rotation invariance. Because of its simplicity and ease of calculation, this feature has been widely used. The original LBP operator is defined as within the window of 3×3, taking the center pixel of the window as the threshold, and comparing the gray value of the adjacent 8 pixels with it. If the surrounding pixel value is greater than or equal to the center pixel value, the pixel at this position is marked as 1, otherwise it is marked as 0. In this way, the 8 points in the 3×3 neighborhood can be compared to produce 8-bit binary numbers (usually converted to decimal numbers, that is, LBP codes, a total of 256 kinds), that is, the LBP value of the center pixel of the window is obtained, and this value is used to reflect texture information for this area. It should be noted that the LBP value is a binary number composed clockwise. The LBP operator can be expressed by Eq. (5).

$$LBP_{P,R}(x_c, y_c) \sum_{i=0}^{P-1} 2^i s(g_i - g_c) \tag{5}$$

where P is the number of surrounding points and R means the radius of the center pixel, in our method, we set $R = 1$, $P = 8$. (x_c, y_c) denotes the center pixel, g_c is its gray value, g_i stands for the gray value of its adjacent pixel, and s is a sign function defined as follows.

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \tag{6}$$

We use the histogram statistics of the LBP features, that is, the statistics of the proportions of the LBP features among 0 to 255, so that the dimensionality reduction of the data is performed. Then we can input a vector into the classifier for classification. However, they are 256-dimensional features. Therefore, dimensionality reduction needs to be further carried out, and thus another concept is involved here: Uniform LBP, that is, uniform mode LBP. That is, reclassify the original 256-dimensional grayscale data and count the number of transitions after displacement. When the number of transitions is less than 2 times, it is defined as a Uniform LBP. After statistics, Uniform LBP accounts for 85%∼90% of the entire LBP features, while has only a dimension of 58. That is, we can reduce the classification feature vector from dimension 256 to dimension 58. In practical applications, the vector is 59 dimensional, because adding one dimension represents those quantities that are not Uniform LBP.

2.2. **Classification.** We use the bagged trees algorithm to classify the pictures. In order to obtain a reliable and stable model, the ten-fold crossover method is used for verification.

The main idea of the bagged trees algorithm is as follows:

(1) Extract a new training set from the original data set. Each time using the method of replacing the sampled data from the original data set, n samples are drawn (in the original data set, some samples may be repeatedly sampled, and some samples may not be sampled at one time). A total of k extractions are performed to obtain k new data sets (the k new training sets are mutually independent). The size of the new data set is equal to the size of the original data set.

(2) Each time a new training set is used to get a model, and k new training sets can get a total of k new models.

(3) For the classification problem: the k models obtained in (2) are used to obtain the classification results by voting; for the regression problem: the average of the models in (2) is calculated as the result (that is, all models have the same importance).

In our paper, 10-fold cross-validation, used to test algorithm accuracy. It is a commonly used test method. Divide the data set into ten sub-sets, taking 9 of them as training data and 1 as test data in turn. Each test will give the corresponding correct rate (or error rate). The average value of the accuracy rate (or error rate) of the results of 10 times is used as an estimate of the accuracy of the algorithm.

2.3. **Forgery Localization.** In recent years, blind tamper detection has developed rapidly, and most methods are not limited to detection, but can also locate the tamper area. Due to the uniqueness and intuition of the ELA algorithm, we propose an improved ELA algorithm for tampering localization. Perform an ELA operation on the picture, and then perform post-processing operations on the obtained ELA picture. First, convert the ELA into a grayscale image, then convert it into a binary image, and finally apply a median filter operation to it. The ELA picture can be accurately located to the tampering area.

3. **Experimental Results and Discussions.** This section begins with the introduction of datasets, followed by the evaluation of our proposed algorithm, and we compare the method with a single algorithm. All the experiments are conducted on a desktop equipped with Core-i7 and 8-GB RAM, and the implementation and the experimentation of the algorithms were carried out using MATLAB® R2016a version.

3.1. **Datasets.** We chose three public datasets for evaluation, i.e., COLUMB, MICC-F220, MICC-F2000 are used to demonstrate the effectiveness of our scheme. More details can be found below.

1. COLUMB: This dataset comprises 183 original images and 180 corresponding forged images with realistic splicing manipulations, with resolutions ranging from 757×568 to 1152×768. The splicing forgery regions are some simple, large, and meaningless regions.

2. MICC-F2000: This dataset is composed by 700 tampered images and 1300 original images, where the average resolution is about 2048×1536. The splicing forgery regions are objects, which are have been subjected to various rotation, scaling, and other operations.

3. MICC-F220: This dataset consists of 110 tampered images and 110 untampered images, with resolutions ranging from 722×480 to 800×600.

3.2. **Evaluation.** To evaluate the performance of tampering detection, we use the *Precision* and *Recall* which are respectively defined in Eq. (7) and Eq. (8). The *Precision* means the probability that the detected regions are relevant, and it is defined as the ratio of number of correctly detected forged pixels to the number of totally detected forged pixels; while the *Recall* means the probability that the relevant regions are detected, and it is

defined as the ratio of number of correctly detected forged pixels to the number of forged pixels in the ground-truth forged image.

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

Where TP denotes the tampered region correctly detected as tampered; FP denotes the non-tampered region incorrectly detected as tampered; and FN denotes tampered region incorrectly detected as non-tampered. Therefore, $TP + FP$ means the total detected region, and $TP + FN$ means the real tampered region, that is the ground-truth result for judgment. In addition to the *Precision* and *Recall*, we calculate the F_1 score using Eq. (9), to synthesize the Precision and Recall as a new evaluating indicator.

$$F_1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{9}$$

3.3. **Discussion.** In this section, we will discuss our experimental results in detail, and evaluate our proposed scheme by comparing different methods and experimenting on different data sets. At the same time, we also showed the results of tampering with localization. After performing experiment on database of COLUMB, we tabulated the result obtained in Table. 1.

Table 1. Performance evaluation of different methods

Algorithm	Precision	Recall	F1	Accuracy
LBP	79.13%	89.07%	83.81%	82.64%
ELA	87.89%	91.26%	89.54%	89.25%
Our LBP+ELA	89.58%	93.99%	91.73%	91.46%

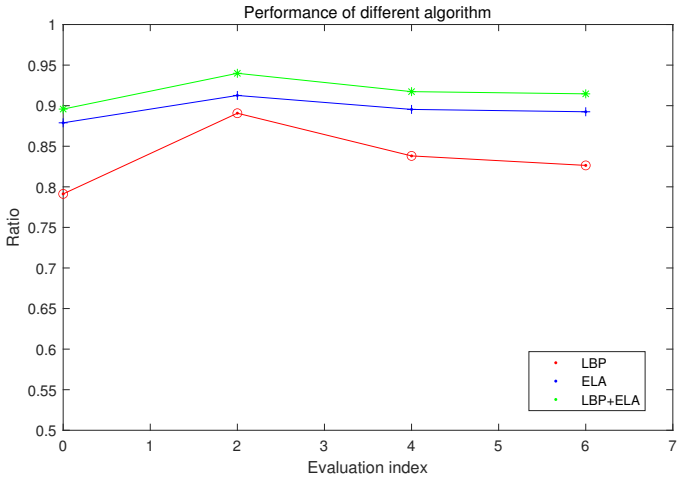
Thus, from the above tables and chart we can conclude that ELA combining LBP can provide better precision and recall. Therefore, from the above results we conclude that we can use ELA combined with LBP for detecting image splicing forgery. For further verifying the effectiveness and robustness of the proposed detection method, we also evaluate the performance of the detection methods under different datasets, as shown in Table. 2.

Table 2. Performance of the proposed method

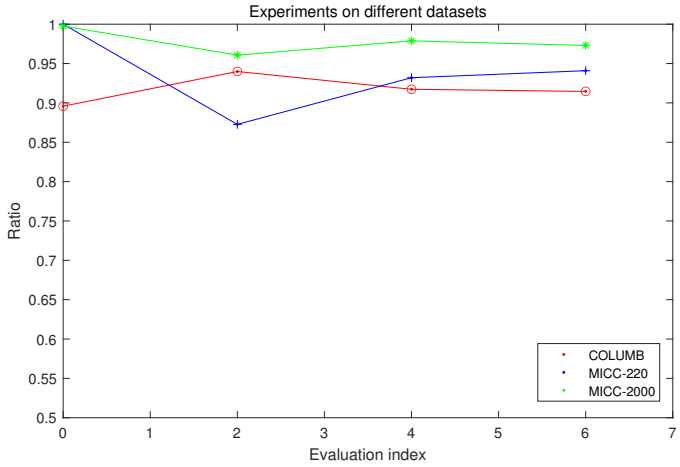
Database	Precision	Recall	F1	Accuracy
COLUMB	89.58%	93.99%	91.73%	91.46%
MICC-F220	100%	88.18%	93.72%	94.09%
MICC-2000	99.76%	96.07%	97.88%	97.30%

Based on the comparison of LBP, ELA and LBP+ELA and the experiments on the three datasets, we have evaluated and compared the Precision and Recall, F1-score and Accuracy of all methods. Fig. 4(a) shows the performance comparison of these three technologies, and Fig. 4(b) shows the performance of our method on three datasets. As can be seen from the figure, the performance of our LBP+ELA technology is superior to a single algorithm, and it shows superiority on each data set, because ELA helps provide higher detection accuracy.

After classification and discrimination, we need to find the tampered area. In this paper, we use the improved ELA method to locate the tampered area. The specific experimental



(a)

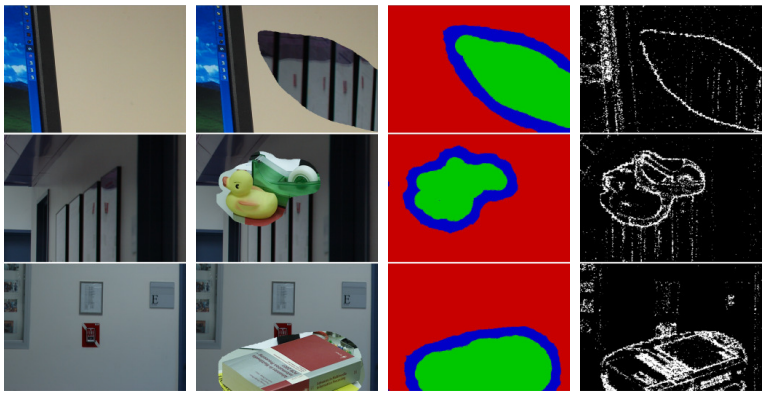


(b)

FIGURE 4. (a) Comparison of LBP, ELA and LBP+ELA on COLUMB, (b) experiments of our scheme on different datasets

results are shown in the following Fig. 5. It can be easily seen from the results that the ELA method can describe the tampered area very intuitively from Column (d).

We conducted a series of comparative experiments. The conventional ELA algorithm usually shows a lot of noise and iridescence, which represents the visible separation between the luminance and chrominance channels, such as blue, purple, and red. Because JPEG divides colors into brightness and chroma channels, the brightness that can be evaluated for rainbow is the grayscale intensity of the image, and the red and blue components identify the amount of coloring, which depends on the intensity of the full color. Many third-party software companies now introduce a lot of rainbows when adjusting images. So the appearance of a rainbow may only mean that the image has been saved using third-party software. It may not indicate that the image has been tampered with. This undoubtedly affects the detection results, so it is necessary to improve ELA and remove rainbowization. Through our series of improved operations, the tampered area can be located more clearly and intuitively. A specific example is shown in Fig. 6.



(a) (b) (c) (d)

FIGURE 5. Demonstration of test images and the corresponding detection results. (a) Authentic image; (b) Forged image through splicing operations; (c) Ground truth; (d) Detected results.

(a) (b) (c) (d)

FIGURE 6. Examples of improved positioning algorithms. (a) Authentic image; (b) Forged image through splicing operations; (c) ELA algorithm; (d) Improved ELA algorithm.

4. **Conclusion and Future Works.** This paper proposes a method for image splicing detection by mixing the features of two algorithms. Among them, LBP can provide a global feature, and ELA can reflect the local tampering feature, so the two complement each other, and combining them can better improve the accuracy of the experiment. In order to improve the classification performance, we choose the classifier as Bagged Trees, and apply 10 fold cross-validation to test the accuracy of the model. The experimental results show that our method has good performance on three common datasets. At the same time, in order to locate the tampered area, we used the ELA method again. By performing a series of post-processing operations on the method, the tampered area can be clearly observed. Compared with the existing work, the work of this paper provides a new idea for the fusion of texture features, and shows the location of image tampering in a more intuitive way, which is more practical. In future work, we will combine the popular deep learning methods to further improve the detection performance of our method.

Acknowledgment. This work is partially supported by Science Foundation of Zhejiang Sci-Tech University(ZSTU) under Grant No.19032458-Y. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Z. M. Lu, C. H. Liu, and H. Wang, Image retrieval and content integrity verification based on multipurpose image watermarking scheme, *International journal of innovative computing, information and control*, vol.3, No.3, pp.621–630, 2007.

[2] H. Farid, Image forgery detection, *IEEE Signal processing magazine*, vol.26, no.2, pp.16-25, 2009.

[3] Y. Y. Wang, and Y. Wang, A new face feature extraction method based on fusing LBP and DBNS features, *International Journal of Innovative Computing Information and Control*, vol.12, no.4, pp.1353–1364, 2016.

[4] Y. Zhang, C. Zhao, Y. Pi, and S. Li, Revealing image splicing forgery using local binary patterns of DCT coefficients, *Communications Signal Processing and Systems*, Springer, New York, pp.181–189, 2012.

[5] S. Agarwal, and S. Chand, Texture operator based image splicing detection hybrid technique, *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, IEEE, pp.116–120, 2016.

[6] N. Kanwal, A. Girdhar, L. Kaur, and J. S. Bhullar, Detection of digital image forgery using fast fourier transform and local features, *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, London, United Kingdom, pp.262–267, 2019.

[7] S. Walia, and K. Kumar, Characterization of splicing in digital images using gray scale co-occurrence matrices, *2019 Twelfth International Conference on Contemporary Computing (IC3)*, IEEE, pp.1–6, 2019.

[8] N. Krawetz, and H. F. Solutions, A picture's worth, *Hacker Factor Solutions*, vol.6, no.6, pp.2, 2007.

[9] N. B. A. Warif, M. Y. I. Idris, A. W. A. Wahab, and R. Salleh, An evaluation of error level analysis in image forensics, *2015 5th IEEE International Conference on System Engineering and Technology (ICSET)*, IEEE, pp.23–28, 2015.

[10] D. C. Jeronymo, Y. C. C. Borges, and L. D. S. Coelho, Image forgery detection by semi-automatic wavelet soft-thresholding with error level analysis, *Expert Systems with Applications* 85, pp.348–356, 2017.

[11] E. Ramadhani, Photo splicing detection using error level analysis and laplacian-edge detection plugin on GIMP, *Journal of Physics: Conference Series*, vol.1193, no.1, pp.012–013, 2019.

[12] T. S. Gunawan, S. A. M. Hanafiah, M. Kartiwi, and N. Ismail (eds.), Development of photo forensics algorithm by detecting photoshop manipulation using error level analysis, *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol.7, no.1, pp.131–137, 2017.

[13] Z. J. Barad, and M. M. Goswami, Image forgery detection using deep learning: A survey, *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, pp.571-576, 2020.

[14] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, Learning rich features for image manipulation detection, *Conference on Computer Vision and Pattern Recognition*, IEEE, pp.1053–1061, 2018.

[15] R. E. Yancey, N. Matloff, and P. Thompson, Multi-linear Faster RCNN with ELA for Image Tampering Detection, *arXiv preprint*, vol.1904, pp.08484, 2019.

[16] E. K. Wang , X. Zhang, F. Wang (eds.), Multilayer Dense Attention Model for Image Caption, *IEEE Access*, PP.1-1, 2019.

[17] K. K Tseng, R. Zhang, C. M. Chen, M. M. Hassan, DNetunet: a semi-supervised CNN of medical image segmentation for super-computing AI service, *The Journal of Supercomputing*, pp.1–22, 2020.

[18] E. K. Wang, C. M. Chen, M. M. Hassan, and A. Almogren, A deep learning based medical image segmentation technique in internet-of-medical-things domain, *Future Generation Computer Systems*, vol.108, pp.135–144, 2020.

[19] E. K. Wang, F. Wang, S. Kumari (eds.), Intelligent monitor for typhoon in IoT system of smart city, *The Journal of Supercomputing*, pp.1–20, 2020.

[20] E. K. Wang, C. M. Chen, F. Wang, M. K. Khan, and S. Kumari, Joint-learning segmentation in Internet of drones (IoD)-based monitor systems, *Computer Communications*, vol.152, pp.54-62, 2020.