Academic Journal of Nawroz University (AJNU), Vol.12, No.3, 2023

https://doi.org/10.25007/ajnu.v12n3a1839

Image Splicing Forgery Detection using Standard Division-Local Binary Pattern Features

Barin Haval Sadiq

Department of Information Technology Management, Duhok Polytechnic, Kurdistan Region, Iraq

ABSTRACT

Numerous aspects of daily life contribute to societal stability, and the security of people's perceptions of the world online is one target of various malicious attacks. Professional forgers can now quickly create copy-move, splice, or retouch photos with the use of today's advanced tools. It has been determined that splicing, is a widespread method of manipulating images. Image forgery can also lead to substantial setbacks and challenges, some of which may have significant ethical, moral, or legal consequences. Thus, the paper proposes a system that combines SD-LBP (Standard Devision-Local Binary Pattern) based passive picture splicing detection system and ANN classifier. The SD-LBP is created to have the benefits and avoid drawbacks of Local Binary Pattern (LBP). The SD-LBP extraction is typically performed by employing proposed SD value-based thresholding instead of the center pixel, which is robust to noise and other photometric attacks. The second part of the proposed system is the ANN classifier is used that extract the feature of images to lower the error and build a model that can tell spliced images from real photos that have been digitally altered. The proposed system is creating a reliable image forgery detection technique that was implemented with CASIA V2.0 standard dataset. The results showing that it outperformed compared with other methods on the in terms of accuracy (97.8%), sensitivity (98.6%), and specificity (97.1%). Most importantly, the proposed SFD method exceeded the state-of-the-art efforts in this field in terms of accuracy.

KEY WORDS: Splicing Image, Forgery detection, Texture features, Artificial neural network, Image Processing

1. INTRODUCTION

Humans have a constant interest in imaging over the years, every type of information is now more frequently represented by photographs on a worldwide scale, yet as technology has advanced, so has the level of image manipulation. There has been an enormous rise in cyberspace, and thousands of photos, many of them fakes, are published to the Internet every day. It is important to improve approaches for detecting and localizing image forgeries because fraudulent images can be made with relatively simple image editing software and then used to spread false information[1]. The alteration of image information can take many forms, from making a selfie more attractive to falsifying scientific findings. Anyone with a basic understanding of computer software may combine two or even more different photographs to create a misleading image. This type of picture alteration is referred to as "image forging," and the area of digital image processing that focuses on identifying and analyzing such manipulations is known as "digital image forgery detection." Social media's growing importance has made image forgery detection approaches even more necessary. Investigating and verifying the authenticity of an image that is being shared on social media is becoming extremely crucial. As a result, the detection of fake images has drawn attention from researchers in the computing field [2].

While image processing technology has advanced quickly, a variety of effective image editing software applications have also appeared, making it simple to change digital photos invisibly. As a result, the validity and reliability of digital images have been subject to scrutiny in our daily lives, particularly when used as evidence in the forensics industry. In general, there are two main issues in digital image forensics: image forgery detection, which aims to find any manipulation, such as splicing, re-sampling, or copy-move [3], and image source identification, which aims to verify whether an inquiry image is generated by a computer or captured by a specific device or camera model. Image splicing forgery detection is achieved by the combination of theoretical frameworks and practical efforts. Since the primary objective of the suggested approach is to enhance the current image SFD scheme, a research framework should be proposed to manage all of the method's operations and ensure that the intended result is achieved [4] .

2. Related Work

In the paragraphs that follow, an overview of the most popular research related to the topics have been investigated and presented. most advanced learning-based techniques such as DCT (Discrete Cosine Transform) and Local Binary Patterns are recommended to identify spliced images. [5] offer a simi-lar deep learning-based approach. However, PCA (principal component analysis) is used in this approach to help minimize the dimensionality of features. A two-branch convolutional neural network (CNN) based on local feature descriptors for detecting picture splicing is proposed in [6], on the "CASIA V2.0" dataset, this technique apparently achieved an accuracy of 96.97% using the SVM classifier.

Some geometric functions were recently introduced into a novel fractional partial differential (FPDE) model for improving medical imaging by [7] The results showed that the FPDE model effectively increased the image intensities in this research. To improve readability of license plate texts, [8]suggested an image enhancement model based on the Riesz fractional model.

A partial blur type consistency was suggested to extract local blur from projected kernels and may also be used in a portioning block-based image extraction Blur regions developed by these blocks are known as out-of-focus blocks in [9]. In this research they generally generate invariant blur values which were shown to be a useful tool for testing, a different modified variation. While reaching impressive classification accuracy, the CLBP and other LBP variants carried over some of LBP's flaws. Ref [10]claims that because of its binary pattern, the LBP is susceptible to noise and fluctuating illumination conditions (i.e. the thresholding output is 0 or 1 only). Consequently, a new LBP version known as the Local Ternary Pattern was proposed in [11]. The Completion Local Binary Pattern (CLBP) is another method was proposed in [12]based on both Steerable Pyramid Transform (SPT) and Local Binary Pattern (LBP).

All the techniques examined above differ only in the way they model the structural shifts caused by forgery. The success of a technique depends on how accurately it describes these changes. This paper suggests a method that exploits SD-LBP in a novel way to model tampering modifications.

The structure of the paper will be as follows: in section 2 the proposed method will be presented in details, Proposed system results and assessments are shown in section 3 and finally the conclusion will be drawn in section 4.

3. Proposed method

As a result of the concept of picture Splicing forgery detection and the contributions that were made, a reliable image forgery detection technique was created. In order to ensure that the suggested method actually improves upon the current picture SFD scheme, a research framework must be established to govern its many stages. This illustrates the fundamental structure of the procedure. The detection of clipped images is a fundamental part of digital image processing and the other fundamental features of image processing as shown in Figure 1.

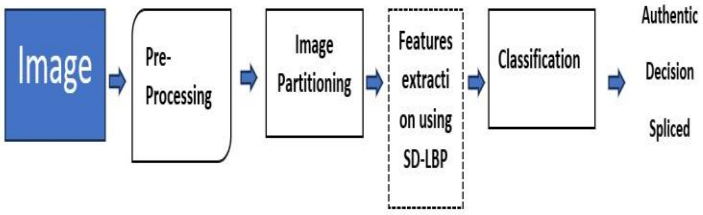


Figure. 1. Block diagram of the proposed algorithm

A. Pre-Processing

The color conversion procedure is the most often used pre-processing method for images nowadays. The major goal of the source picture representation is often to ease the workload of the next stage and boost the performance of that stage[13]. The following equation (1) describes the weighted average technique used in this study:

$$Y = 0.299R + 0.587G + 0.114B \quad (1)$$

Y represented the luminance of the R, G, and B channels of the RGB image.

B. Image Partitioning

To reduce the computational burden of an exhaustive search, this study suggests partitioning images into overlapping blocks, with the optimal size being 12x12 pixels but ranging from 9x9 to 15x15. It's not enough for a block to be larger than the smallest size at which tampering may be safely assumed. As a result, the empirical block size chosen for this study is 12 by 12. As shown in Figure 2.

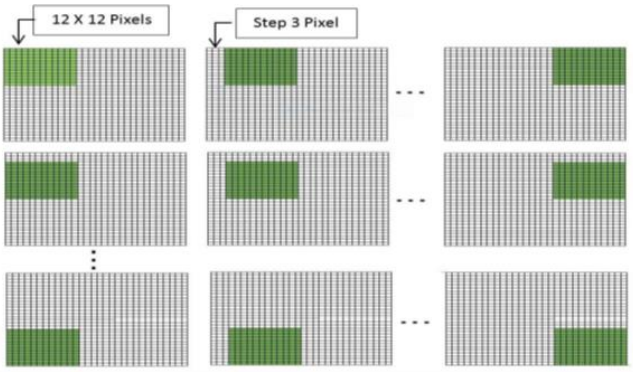


Figure. 2. Image divided into overlapping blocks of 12×12 pixels (Creating Overlapping Blocks)

The overlapping block is shifted three pixels to the left and right, beginning at the top left corner.

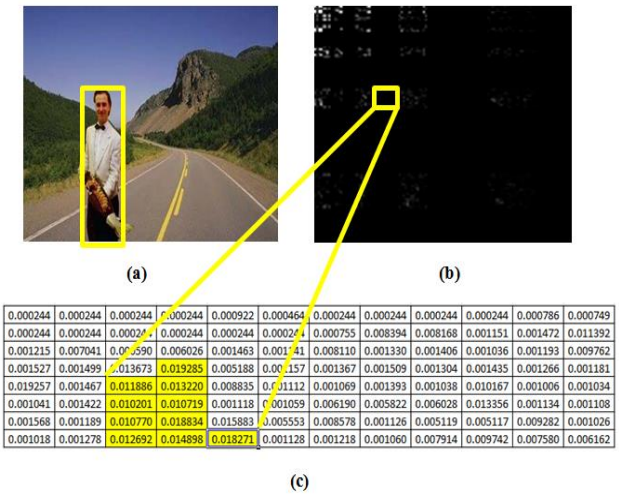
C. SD-LBP

Because of its uniqueness, the standard deviation (SD) is selected as the characteristic in this study. Equation (2) is used to calculate a standard division SD for each LBP block.

$$SD_{\square}(i,j) = \frac{1}{W \times W} \sum_{u=i}^{i+W-1} \sum_{v=j}^{j+w-1} (LBP(u,v) - SD_{\square}(i,j))^2 \quad (2)$$

where SD(i, j) is the local SD(i, j) represents the arithmetic average of the LBP values of the block size w × w and calculated using Equation (3).

$$SD(i,j) = \frac{1}{W \times W} \sum_{u=i}^{i+w-1} \sum_{v=j}^{j+w-1} LBP(u,v) \quad (3)$$



0.000244	0.000244	0.000244	0.000244	0.000922	0.000464	0.000244	0.000244	0.000244	0.000244	0.000786	0.000749
0.000244	0.000244	0.000244	0.000244	0.000244	0.000244	0.000755	0.008394	0.008168	0.001151	0.001472	0.011392
0.001215	0.007041	0.006590	0.006026	0.001463	0.001241	0.008110	0.001330	0.001406	0.001036	0.001193	0.009762
0.001527	0.001499	0.013673	0.019285	0.005188	0.001157	0.001367	0.001509	0.001304	0.001435	0.001266	0.001181
0.019257	0.001467	0.011886	0.013220	0.008835	0.001112	0.001069	0.001393	0.001038	0.010167	0.001006	0.001034
0.001041	0.001422	0.010201	0.010719	0.001118	0.001059	0.006190	0.005822	0.006028	0.013356	0.001134	0.001108
0.001568	0.001189	0.010770	0.018834	0.015883	0.005553	0.008578	0.001126	0.005119	0.005117	0.009282	0.001026
0.001018	0.001278	0.012692	0.014898	0.018271	0.001128	0.001218	0.001060	0.007914	0.009742	0.007580	0.006162

Figure. 3 The extracted SD feature for (a image, (b) SLT-decomposed block, and (c) SD feature for SLT-decomposed block

The LBP code is equal to that binary code's decimal value. An illustration of the LBP code computation process is shown in Figure 4.

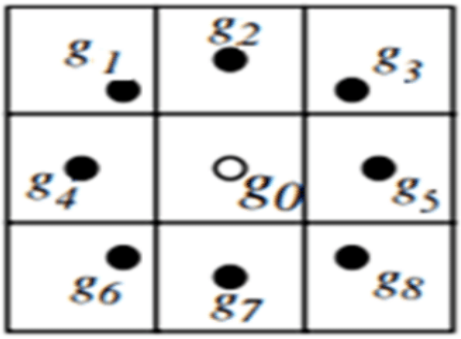


Figure. 4. The circularly symmetric neighbour set of eight pixels in a 3×3 neighborhood

In this work, a standard division (SD) value is computed from each (3x3) cell to determine the LBP's grey-scale invariance property. In this experiment, CASIA TIDE V2.0datasets were used, which comprise photos of various sizes. As a consequence, the number of features obtained from this collection is determined by the picture height and breadth in the datasets as shown in table. The shows how the number of features differs depending on the size of the photos in the datasets.

Table 1: The number of SD obtained from each dataset

Dataset Name	Height	Width	Number of SD
CASIA TIDE V2.0	600	900	150

Scatter graphs are created using 360 samples from both classes in the dataset (genuine and tampered) to analyze the behavior of extracted features, as illustrated in Figure

4.21. Scatter plots are commonly used to discover correlations between different samples of the same class utilizing extracted features that have been reduced to three dimensions using (PCA) to represent the features. The extracted features are not much overlapped and can be easily observed and segregated by the class of the image, as shown in Figure 5, which supports the features extracted using the proposed method in this research to classify the images in the dataset into two classes: tampering (blue stars in Figure 5) and authentic images (yellow stars in Figure 5).

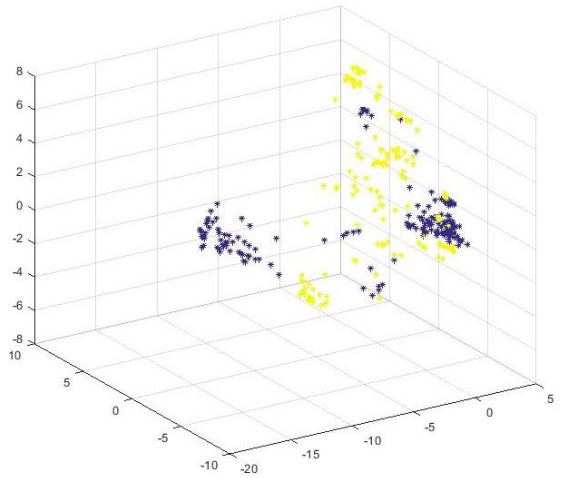


Figure 5. 3D-Scatter plots of extracted standard deviations

Following the extraction of the major characteristics and the symbolization of each sample by a feature set, the dataset samples are classified into two groups: genuine image and spliced image.

When this procedure is finished, SD-LBP will be executed by drawing feature vectors from each block. When looking at a large area in an image, the LBP data will be too faint to make out. Therefore, in this research, the input image is divided into overlapping blocks of 12x12 pixels. Then, 3x3-pixel cells are created so that no two adjacent blocks overlap. Then, SD-LBP cell pictures are generated by applying the descriptor to each cell. As seen in Figure 6, there are three primary stages to the procedure: To do this, we first divide each block into 16 cells, with a 33-pixel size; then we apply the SD-LBP descriptor to each of these cells to generate 16 additional SD-LBP cells for each block (i.e., 166); and finally, we generate feature vectors for each color channel. As a result, it is crucial to use the three channels to obtain the necessary features and information to distinguish spliced photos from the genuine ones before feeding them to the ANN classifier.

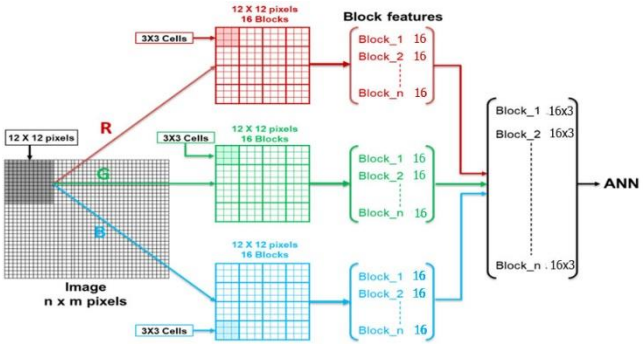


Figure. 6.Feature vectors extraction.

4. Experimental results

A. System Evaluation

If you're planning on developing a strategy to outsmart a classifier or pattern recognition system, you should definitely use certain industry-accepted metrics to gauge your success. The baseline for this investigation should be the generalization accuracy of the classifications. The percentage of test instances that were properly labeled is known as the prediction accuracy. The proposed method was evaluated using the CASIA Tampered Image Detection Evaluation (TIDE) V2.0, which found that all classification results, including those that didn't involve fabrication, were subject to some degree of mistake. Normalized relative error is typically described as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN)). The sensitivity metric is the ratio of correctly recognized spliced images to the total number of spliced images in the FN-dependent dataset. Specificity, on the other hand, refers to the ratio of correctly detected authentic images to the total number of authentic images in a dataset where FP is crucial. The accuracy of the suggested identification method is then defined as a precision measure. Sensitivity, specificity, and accuracy can be determined using the following equations:

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \quad (4)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (5)$$

$$Specifity = \frac{TN}{TN + FP} \quad (6)$$

Figure 7 shows that, compared to Red-(SD-LBP) and Green-(SD-LBP), Blue-(SD-LBP) has the superior detection performance by a wide margin (SD-LBP). These findings provide credence to the claim the proposed SD-LBP increases the detection rate of picture forgeries by spotting evidence of manipulation that are invisible to the naked eye.

When the performance of Red- (SD-LBP), Green- (SD-LBP), and Blue- (SD-LBP) is combined, the results improve even more, whether the attack is single or double photometric.

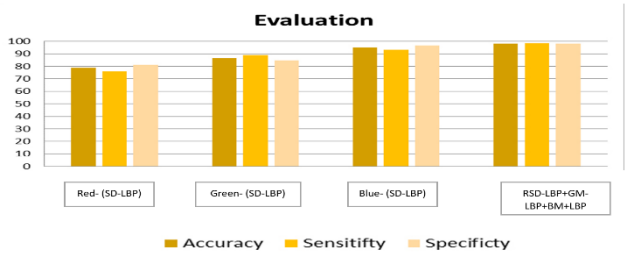


Figure 7. Experimental results from tampered images detection CASIA TIDE V 2.0.

As can be seen in Table 1, when comparing the detection performance of Blue/ SD LBP, Green/ SD LBP, and Red-SD LBP, Blue/ SD LBP clearly outperformed the other two. These findings corroborate our earlier discussion that the suggested SD-LBP improves the detection rate of picture forgeries by capturing the tampering traces that are invisible to the naked eye.

Together, their improved performance counteracts the effects of shallow depth blurring and photometric noise attacks.

B. Classification

Spliced photos are identified and separated from the originals. The best outcomes can't be guaranteed even with the best features; a good classifier is also required. Artificial neural networks (ANN) have been used and implemented into the suggested picture splicing detection system in this study. When it comes to the nuts and bolts, neutral networks have a simple set of processing elements, a high level of interconnection, and an adaptable interface; and when one of the neural network's components fails, the rest of the network continues to function normally because of its parallel architecture [14].

In this context, "artificial neural networks" (ANNs) refer to computer systems designed to perform tasks similar to those performed by human brains [15]This classifier uses training data split into two categories (spliced class and authentic class). The ANN will be fed the extracted textures feature for those images in an effort to lower the error and create a viable model for distinguishing between the manipulated and original images. The trained model will be fed the attributes of the test image to determine if the image was spliced or not.

Training data for this classifier comes from only two categories (spliced class and authentic class). To begin, we will feed the ANN the extracted textures feature of these images in an effort to lower the error and create an appropriate model to help distinguish spliced images from the genuine ones. To check for joined Ness and accuracy, the test image's features will be loaded into the training model during the testing phase. The method is depicted in Figure 8.

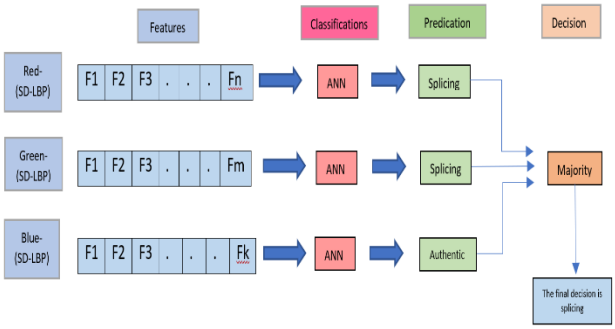


Figure. 8.Illustrates the ANN process

The classifier will get all of these features, and it will base its decisions on how the feature components vote. The conclusion would be focused on the class with the most votes receiving the highest number of votes. Because we are trying to deal with binary classification, always using the majority vote scheme for feature combinations results in an obvious decision. Read-SD-LBP, Green-SD-LBP, and Blue-SD-LBP have been fused.

Comparison with other works

This research framework uses a 2-layer backpropagation neural network. The network trained with 60% of the data, 30% of which was used for validation, and 30% of which was used for testing. in Figure 9, you can see the validation performance at its best.

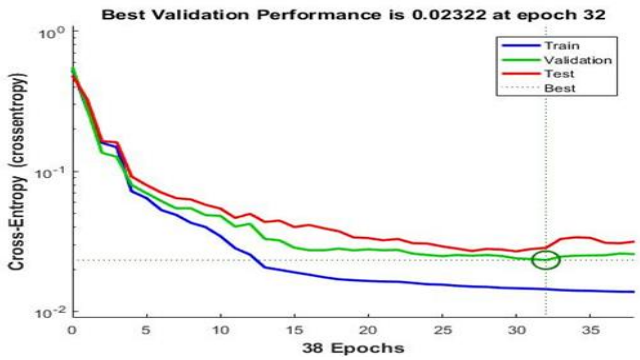


Figure 9. Training, Validation and Testing performance at epoch 32 shows the high validation performance (0.02322).

Table 2. Illustrates outcomes of comparison between method proposed by this research and other methods

Methods	CASIA v2.0
Li et al. [17]	92.38%
Alahmadi et al.[2]	97.5%
Our Method	97.8%

Using Casia V2.0, an approach developed by Ahmadi et al. (2017) that relies on DCT and LBP features achieves 97.5% accuracy in detection. Comparatively, the detection accuracy of a Markov in the quartering discrete cosine transformation (QDCT) domain version of (LI ET AL., 2017) is 92.38% when using the Casia V2.0 Database, while the detection accuracy of the method described in this study is 99.3% when using the same database.

5. CONCLUSION

The proposed method has shown a sensitivity of 98.6%, specificity of 97.1%, and accuracy rate of 97.8% in detecting picture splicing clearly outperform the state-of-the-art works published recently in this field that was applied to the CASIA V2.0 standard datasets, which include examples of images that have been edited in various ways (blurring shallow depth, additive noise, edge smoothing, and homogenous region, to name a few).

Reference

[1] X. Bi, Z. Zhang, and B. Xiao, "Reality transform adversarial generators for image splicing forgery detection and localization," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2021, pp. 14294–14303.

[2] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," *Signal Process Image Commun*, vol. 39, pp. 46–74, 2015.

[3] H. Yao, S. Wang, X. Zhang, C. Qin, and J. Wang, "Detecting Image Splicing Based on Noise Level Inconsistency," *Multimed Tools Appl*, vol. 76, no. 10, pp. 12457–12479, 2017, doi: 10.1007/s11042-016-3660-3.

[4] Y. Li and S. Lyu, "Obstructing DeepFakes by Disrupting Face Detection and Facial Landmarks Extraction," *Deep Learning-Based Face Analytics*, pp. 247–267, 2021.

[5] E. I. A. El-Latif, A. Taha, and H. H. Zayed, "A passive approach for detecting image splicing using deep learning and haar wavelet transform," *International Journal of Computer Network and Information Security*, vol. 11, no. 5, pp. 28–35, 2019.

[6] Y. Rao, J. Ni, and H. Zhao, "Deep learning local descriptor for image splicing detection and localization," *IEEE access*, vol. 8, pp. 25611–25625, 2020.

[7] R. W. Ibrahim, H. A. Jalab, F. K. Karim, E. Alabdulkreem, and M. N. Ayub, "A medical image enhancement based on generalized class of fractional partial differential equations," *Quant Imaging Med Surg*, vol. 12, no. 1, p. 172, 2022.

[8] A. Raghunandan, P. Raghav, and H. V. R. Aradhya, "Object detection algorithms for video surveillance applications," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, 2018, pp. 563–568.

[9] K. Bahrami, A. C. Kot, L. Li, and H. Li, "Blurred image splicing localization by exposing blur type inconsistency," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 999–1009, 2015.

[10]X. Tan and B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting conditions," *IEEE transactions on image processing*, vol. 19, no. 6, pp. 1635–1650, 2010.

[11]Z. Guo, L. Zhang, and D. Zhang, "A completed modeling of local binary pattern operator for texture classification," *IEEE transactions on image processing*, vol. 19, no. 6, pp. 1657–1663, 2010.

[12]G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Mach Vis Appl*, vol. 25, pp. 985–995, 2014.

[13]M. Zandi, A. Mahmoudi-Aznaveh, and A. Mansouri, "Adaptive matching for copy-move

forgery detection," in *2014 IEEE international workshop on information forensics and security (WIFS)*, IEEE, 2014, pp. 119–124.

[14]I. Aizenberg, T. Bregin, C. Butakoff, V. Karnaukhov, N. Merzlyakov, and O. Milukova, "Type of blur and blur parameters identification using neural network and its application to image restoration," in *ICANN*, 2002, pp. 1231–1236.

[15]J. A. Ahmed and A. M. A. Brifcani, "A new internal architecture based on feature selection for holonic manufacturing system," *International Journal of Industrial and Manufacturing Engineering*, vol. 9, no. 8, pp. 1549–1552, 2015.

[16] C. Li, Q. Ma, L. Xiao, M. Li, and A. Zhang, "Image splicing detection based on Markov features in QDCT domain," *Neurocomputing*, vol. 228, pp. 29–36, 2017.

[17] C. Li, Q. Ma, L. Xiao, M. Li, and A. Zhang, "Image splicing detection based on Markov features in QDCT domain," *Neurocomputing*, vol. 228, pp. 29–36, 2017.

[18] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal Image Video Process*, vol. 11, no. 1, pp. 81–88, 2017.