Academic Journal of Nawroz University (AJNU), Vol.9, No.3, 2020

https://doi.org/10.25007/ajnu.v9n3a780

Image Splicing Forgery Detection Scheme Using New Local Binary Pattern Varient

[1]Araz Rajab Abrahim, [2]Mohd Shafry Mohd Rahim, [3]Ahmed Saifullah Sami
[1,3] Faculty of Computing, Universiti Teknologi Malaysia (UTM), Skudai, 81310, Johor Bahru, Malaysia
[2] IRDA Digital Media Center, Universiti Teknologi Malaysia (UTM), Skudai, 81310, Johor Bahru, Malaysia
[3] Faculty of Computer Science, Duhok Polytechnic Unicersity, Duhok, Kurdistan Region of Iraq

ABSTRACT

In this research develop passive image splicing detection method based on a new descriptor called Adaptive Threshold Mean Ternary Pattern (ATMTP). It was developed based on strength and weaknesses of both Local Binary Pattern (LBP) and Local Ternary Pattern (LTP). ATMTP extraction feature is normally achieved by using proposed mean based thresholding and adaptive ternary thresholding, the former is robust to noise while the latter is robust to noise and other photometric attacks. It is designed to withstand against photometric manipulations, be it single or double attacks. In this research the ATMTP color features extracted from R, G, and B channels have revealed that the present method achieved higher accuracy on standard datasets CASIA V2.0 out of 99.03%, Sensitivity 99.6%, and specificity 98.1%. Finally, in terms of accuracy, the proposed SFD scheme outperformed the best recent works in this area.

Keywords: Splicing Image Forgery detection, Texture features, Artificial neural network.

1. Introduction

Simplicity of changing image content without leaving obvious traces behind has highly contributed to improving image forensic techniques that determine whether image being original or tampered. Image forgery defines an artistic technique adopted in photography that spans across centuries. The earlier photography years identified new avenues utilized in the designing and development of portraits. Due to the advent of advanced applications of digital image processing such as GIMP and Photoshop image manipulation becomes handy. Nowadays, armed with the sophisticated tools, any professional forgers can easily produce any kind of tampered images, be it copy-move, splicing or retouching. Splicing has been identified as a common image manipulation process also referred to as photomontage. In an effort to initiate the manipulation, the forger integrates varied areas out of different images into a single image(Redi, Taktak, & Dugelay, 2011). Additionally, image forgery can result in huge setbacks and issues that tend to eventually have ethical, moral, and legal impacts. For such reasons, image authenticity is considered a paramount issue, not only worth researching, but as a topic for avocation.

2. Related Work

Recently, many passive methods for the detection of image splicing forgeries have been proposed. In the following paragraphs, we give an overview of the representative methods. We focus only on state-of-the-art learning-based methods.

(Heikkilä, Pietikäinen, & Schmid, 2006) proposed center-symmetric LBP (CS-LBP), According to (Tan & Triggs, 2010) the LBP is sensitive to noise and varying lighting condition due to its binary pattern (i.e. the thresholding output is 0 or 1 only). Thus, a new variant of LBP proposed called Local Ternary Pattern (LTP), while other modified version called Completed Local Binary Pattern (CLBP) proposed by(Guo, Zhang, & Zhang, 2010). Despite achieving remarkable

classification accuracy, the CLBP and others version of LBP, however, inherited the LBP weaknesses.

A method of image forgery detection proposed by (Muhammad, Al-Hammadi, Hussain, & Bebis, 2014) Based on both of Steerable Pyramid Transform (SPT) and Local Binary Pattern (LBP).

Partial Blur Type Consistency as suggested by (Bahrami & Kot, 2015) may also be used through portioning block-based image by extracting local blur from estimated kernels. These blocks are called out-of-focus and generate invariant types of blur regions. Experiments have shown that this method is an applicable testing technique.

(H. Li, Luo, Qiu, & Huang, 2017)proposed a framework to improve the performance of forgery localization via integrating tampering possibility maps. In the proposed framework, we first select and improve two existing forensic approaches, i.e., statistical feature-based detector and copy-move forgery detector, and then adjust their results to obtain tampering possibility maps DCT and Local Binary Pattern recommended by (Alahmadi et al., 2017) proposed to identify spliced image if any.

A composite manipulation detection method based on convolutional neural networks (CNNs). To our best knowledge, this is the first work applying deep learning for composite forgery detection proposed by (Choi et al., 2017) .

(Marra, Gragnaniello, Cozzolino, & Verdoliva, 2018) studied the performance of several image forgery detectors against image-to-image translation, both in ideal conditions, and in the presence of compression, routinely performed upon uploading on social networks

All the methods discussed above differ only in the way they model the structural changes caused by forgery. The success of a method depends on how accurately it represents these changes. We propose a method that exploits ATMTP in a novel way to model tampering changes.

3. Proposed Method

Concept of image Splicing forgery detection and implemented contributions lead to achieve robust image Splicing forgery detection scheme. Main goal of proposed method is improving existing image SFD scheme, research framework therefore should be proposed to control all method processes in order to verify this goal. Figure 1 illustrates the framework of proposed method. It deals with all essential aspects of digital image processing including spliced images detection.

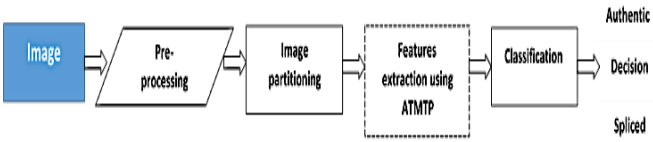


Fig. 1. Block diagram of the proposed algorithm.

3.1 Pre-processing

Among numerous existing techniques of image pre-processing, the colour conversion process is considered to be the most common one. Generally, the major objective of the source image representation is to facilitate the task of subsequent steps and to improve the next stages performance (Zandi, Mahmoudi-Aznaveh, & Mansouri, 2014) in this research the weighted average method selected as show in equation (1):

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

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

3.2 Image Partitioning

In this research image is dividing into overlapping blocks to avoid high computational cost of all-out search, block size can be determined empirically from 9×9 to 15×15 pixels where 12×12 is considered the best size.

Apparently, the use of overlapping blocks and

correlation of every block of image with other block had greatly improved neighbouring pixels' relations. Thus, it customary to divide an image into overlapping blocks extend from top-left to the right corner bottom. Size of block must be smaller than minimum size of presumed tampering. Therefore, this study has selected 12×12 pixels as empirically block size.

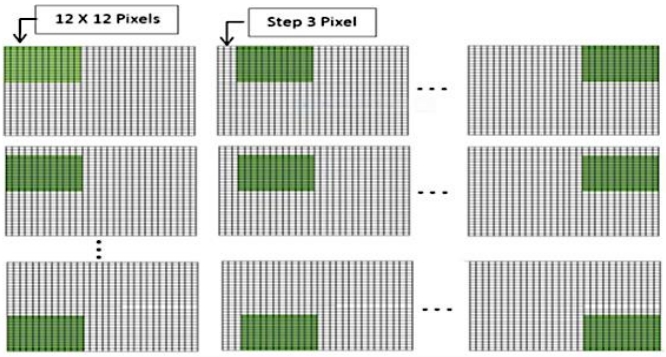


Fig. 2. Image divided into overlapping blocks of 12×12 pixels (*Creating Overlapping Blocks*)

The overlapping block is slid by three pixels along the image from the upper left corner and down to the lower right corner.

3.3 Adaptive Threshold Mean Ternary Pattern Descriptor (ATMTP)

In this research ATMTP descriptor is proposed to extract robust features to overcome the impacts of photometric attacks to detect the spliced image. Similar to the most LBP variants, ATMTP can describe a local texture pattern. In this research, the input image is partitioned into overlapping blocks of sized 12x12 pixels. Then, each overlapped block is subdivided into non-overlapping cells of sized 3x3 pixels. Subsequently, the ATMTP descriptor is applied on each cell to produce six ATMTP cell-images, which termed as sign-upper, sign-lower, magnitude-upper, and magnitude-lower, center-upper and center-lower. Following that, the ATMTP framework is given in Figure 3 below.

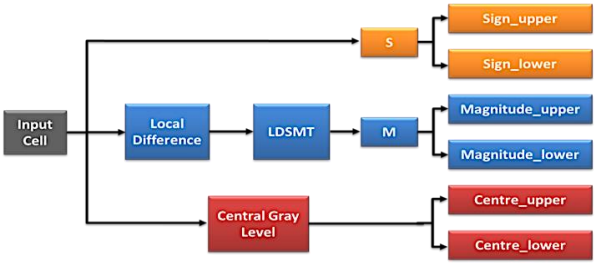


Fig. 2. The framework of ATMTP.

For ease of discussions, let's assume that the adaptive ternary threshold (t) is equaled 7; p = 0,1,2,…,7 is a neighboring pixel of the center pixel; g_{mean} represents the mean gray value of the cell pixel; c^{up} are the thresholds which signify the mean values of the upper magnitude of the cells; c^{lower} are the thresholds which signify the mean values of the lower magnitude of the cell.

To calculate the Sign-upper code, compare all neighboring pixels with a threshold value, which is the mean of the cell plus t, using Equation 2:

$$Sign_{upper} = \sum_{p=0}^{7} s\left(g_p - (g_{mean} + t)\right)2^p,\ S = \begin{cases} 1, g_p \geq g_{mean} + t, \\ 0\ , otherwise \end{cases} \quad (2)$$

And for the Sign-lower code, compare all the neighboring pixels (g_p) with another threshold value (i.e. mean of the cell minus t) using Equation (3):

$$Sign_{lower} = \sum_{p=0}^{7} s\left(g_p - (g_{mean} - t)\right)2^p,\ S = \begin{cases} 1, g_p < g_{mean} - t, \\ 0\ , otherwise \end{cases} \quad (3)$$

The Magnitude-upper, it is performed in three sequences namely, local difference, averaging and thresholding: (a) Local difference - deduct the g_p from

$$M_{upper} = \sum_{p=0}^{7} t(m_p^{upper}, c)2^p, t(m_p^{upper}, c^{up}) = \{^{1, |g_p - (g_{mean} + t)| \geq c}_{0, |g_p - (g_{mean} + t)| < c} \quad (4)$$

(mean plus t) to generate upper magnitudes, (b) Averaging - compute the average of the all upper magnitudes, and (c) Thresholding - threshold the upper magnitude against the average to generate magnitude-upper code. The process is performed using Equation (4):

And for Magnitude-lower, again, it is performed in three sequences namely, local difference, averaging and

thresholding: (a) Local difference - deduct the from (mean minus t) to generate lower magnitudes, (b) Averaging - compute the average of the all lower magnitudes, and (c) Thresholding - threshold the lower magnitude against the average to generate magnitude-lower code. The process is performed using Equation (5):

$$M_{lower} = \sum_{p=0}^{7} t(m_p^{lower}, c)2^p, t(m_p^{lower}, c^{lower}) = \{^{1, |g_p - (g_{mean} - t)| \geq c}_{0, |g_p - (g_{mean} - t)| \prec c} \quad (5)$$

The Centre-upper code, it is performed in two sequences: (1) Find the average of all pixel values (including the center pixel) of the original cell, and (2) threshold against the average plus *t*, to generate center-upper code. The process is accomplished using Equation (6):

$$Center_{upper} = \sum_{p=0}^{7} s(g_p - (g_{mean} + t)2^p, Center_{upper} = \{^{1,\ g_p \geq g_{mean} + t,}_{0,\ otherwise} \quad (6)$$

Centre-lower code, it is also performed in two sequences: (1) Find the average of all pixel values (including the center pixel) of the original cell, and (2) threshold against the average minus *t*, to generate center-lower code. The process is accomplished using Equation (7):

$$Center_{lower} = \sum_{p=0}^{7} s(g_p - (g_{mean} + t)2^p, Center_{lower} = \{^{1,\ g_p \prec g_{mean} - t,}_{0,\ othrewise} \quad (7)$$

After completion, the next operation is to execute ATMTP by extract feature vectors from each block. The process involves three main steps as given in Figure 4 below: (1) Each block is subdivided into sixteen cells – each one of them has size of 3×3 pixels ; (2) The ATMTP descriptor is applied on each 3*3 cells to generate six new ATMTP cells of sized 3×3 pixels, which are termed as sign-upper (SU), sign-lower (SL), magnitude-upper (MU), magnitude-lower (ML), center-upper (CU) and center-lower (CL) cells– in total, the process produces 96 ATMTP cells for each block (i.e. 16×6); (3) Feature vectors for each color channel are generated then are (APA 6th) (APA 6th) (APA 6th)

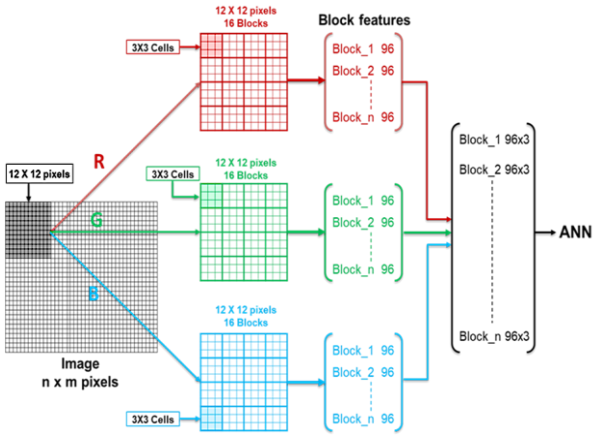
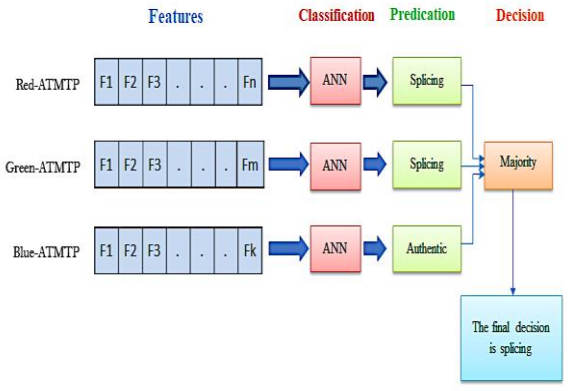


Fig. 3. Feature vectors extraction.

3.4 Classification

The spliced images are detected and segregated from the authentic ones. Having good features alone would not necessarily produce the best results – it requires a suitable classifier. This research has adopted and incorporated Artificial Neural Networks (ANN) within proposed image splicing detection. Neutral networks entail a type of simple elements of processing, lofty interconnection level, adaptive interface amid elements, plus upon a failure by any of the neutral network's element; it progresses with no difficulties due to their parallel nature(Aizenberg, Butakoff, Karnaukhov, Merzlyakov, & Milukova, 2003).

An ANNs is an information processing system that is inspired by the way biological nervous systems, such as the brain, process information (Ahmed & Brifcani, 2015). In this classifier, two classes have been taken as training data (spliced class and authentic class). The extracted textures feature of these images will be fed to the ANN to



reduce the error and allow implementing a suitable model that can help to identify spliced images from the authentic one. In testing stage, the features of test image will be fed to training model to identify whether it spliced or authentic. Figure 5 illustrate the process.

Fig.5. Illustrates the ANN process

4. Experiment Al Result

4.1 CASIA Dataset V2.0 Tampered Image Evaluation

Likewise, this thesis has utilized the CASIA TIDE V2.0 for detecting spliced picture assessment since contains substantial numbers of high-resolution pictures that tampered utilizing advanced methods. Furthermore, this dataset has been broadly utilized as part of previous studies for assessing tampered pictures identification approaches. It an extensive dataset which contains 7,491of authentic pictures and 5,123 of tampered color pictures. Pictures in diverse resolutions that varying from 240 x 160 to 900 x 600 pixels in various configurations (i.e. BMP, TIFF, JPEG). Tampered pictures incorporated into dataset are outcome of disguised splicing process, sometimes utilizing an obscure process over tampered picture and are more comprehensive and challenging than that of CASIA TIDE V1.0. Figure 6 demonstrates a case of a few pictures taken from CASIA TIDE V2.0 with primary row presents authentic pictures and second row demonstrates their tampered counterparts.

Fig. 6. samples of CASIA TIDE V2.0 Top row represents set of authentic images, while bottom row displays respective spliced image.

Accompanying standards considered while producing spliced pictures in CASIA TIDE V2.0:

- Spliced pictures must be reasonable to human eyes, however as much as be expected by utilizing those characterized manipulations in Photoshop.
- Spliced picture is gained from two diverse authentic pictures.
- Most of tampered locales are random contour characterized via picture producers.
- Cropped picture areas(s) are processing with rotation, scaling, other deformation processes (characterized via Photoshop users) before pasting to create a spliced picture.
- Post processing like obscuring could be used in the wake of creating spliced picture.
- Blurring/filing can be used along tampered area borders or anyplace else in created picture.
- Various sizes (little, medium and vast) of tampered districts are considered while creating spliced pictures.

4.2 Evaluation

Evaluating performance of any procedure proposed to solve a pattern recognition scheme or a classifier would require adoption of standard evaluation measures. In this research first use overall classification accuracy. Accuracy rate refers to proportion of number of successfully classified test cases to total number of tested cases. After implementing assessment of proposed method on the tampered Image Detection Evaluation CASIA TIDE V2.0 where all classification results could have error rate in terms of forgery identification failure, or successful detection even in absence of any forgery. Commonly, this error rate is described via True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) consequently. Sensitivity measure represents proportion of quantity of accurately detected spliced images to aggregate number of spliced images

found in dataset highly dependent on FN. Conversely, specificity signifies proportion of quantity of accurately detected authentic images to aggregate number of genuine images found in dataset highly dependent on FP. Then, precision measure defined as rightness of proposed identification technique. Equations (8), (9) and (10) used in calculating each of sensitivity, specificity, and accuracy presented as follows:

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \quad (8)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (9)$$

$$Specifity = \frac{TN}{TN + FP} \quad (10)$$

It can be observed from Figure 5 that Blue-ATMTP achieved the best detection performance with significant differences compared to Red- ATMTP and Green-ATMTP because each channel has specific and important information about image . These results support that the proposed ATMTP enhances the detection rate of image forgeries due to its ability to capture the tampering traces that are not visible by human eyes affected by single or double photometric attacks, The performance of Red-ATMTP, Green-ATMTP, and Blue-ATMTP together further improves the results.

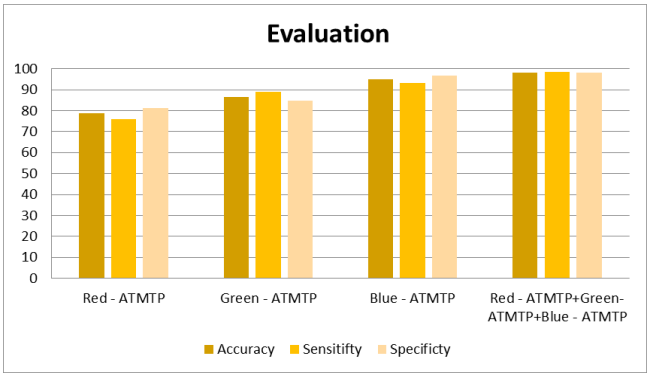


Fig. 7. Experimental results from tampered images detection CASIA TIDE V 2.0.

The ROC (Receiver Operating Characteristics) curve illustrates performance of algorithm by charting rates of true and false positives in which deemed as varied discrimination threshold. Likewise, in process of designating performance of proposed algorithm where this research avoids specifying loss which it incurs when a false positive versus a false negative occurred. The results show that connected of the Red-ATMTP, Green-ATMTP and Blue-ATMTP features leads to a high level of accuracy. A predictive method has been improved by taking features for example (xx) is a certain feature of spliced pictures that to award classification y(x) =1y(x) =1 or y(x)=0y(x)=0 that matches with no-spliced.

Values $x * x *$ choses classification are called discrimination threshold.

$$y(x) = 1y(x) = 1 \text{ if } x \succ x * x \succ x * \quad (11)$$

Equation (11) is a features prediction of spliced image.

$$y(x) = 0y(x) = 0 \text{ if } x \prec x * x \prec x * \quad (12)$$

Equation (12) is a features prediction no spliced image. Despite discrimination threshold x ∗ x ∗chosen but cannot separate that have been spliced from those have not complied with rule. However, reduction of false negative rate may come at the expense of increasing false positive rate (part of green distribution on the right vertical line).Thus, chosen discrimination threshold deemed as a swap between rates of false positive and false negative. Thus, if a given image spliced, that would consider a prediction. However, familiar envision is knowing right circulation of concentrations in pictures that been spliced y=1y=1, but without spliced y=0y=0 independently.

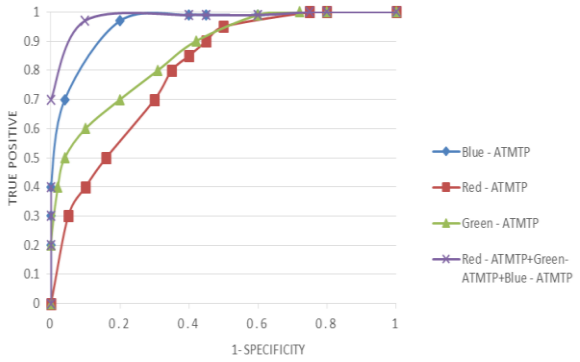


Fig. 8. Illustrate the ROC curve for the proposed system

Table 1
illustrate the Area under the curve for each feature.

Red-ATMTP	Green-ATMTP	Blue-ATMTP	(Red-ATMTP + Green-ATMTP + Blue-ATMTP)
0.84	0.94	0.95	0.98

It can be observed from Table 1 that Blue-ATMTP achieved the best detection performance with significant differences compared to Green-ATMTP and Red-ATMTP. These results support what we discussed before that the proposed ATMTP enhances the detection rate of image forgeries due to its ability to capture the tampering traces that are not visible by human eyes affected by blurring shallow depth and noise photometric attacks, the performance of three together further improves the results.

4.3 Performance

A 2-layer backpropagation neural network has been used in this research framework. The network was trained with70% training, validation 15 % and testing 15% sample. Figure 9 shows the best validation performance.

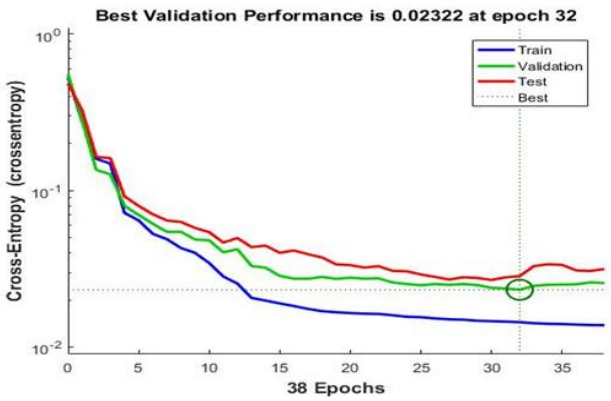


Fig. 9. Training, Validation and Testing performance at epoch 32 shows the high validation performance (0.02322).

It can be observed that the proposed SFD scheme outperformed the best recent works in this area.

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

Methods	CASIA v2.0
(C. Li, Ma, Xiao, Li, & Zhang, 2017)	92.38%
(Alahmadi et al., 2017)	97.5%
Our Method	99.03%

A method of (Alahmadi et al., 2017) based on DCT and LBP features give 97.5 % accuracy detection through CASIA v2.0.

A method of (Li et al., 2017) derived from Markov in Quaternion Discrete Cosine Transform (QDCT) domain give 92.38% accuracy detection through CASIA v2.0 database

While our method proposed by this research provides 99.3% accuracy through CASIA v2.0. Which has outperformed both previous methods

5. Conclusion

In this research, the standard datasets CASIA V2.0 which contain all kinds of splicing tactics such as (blurring shallow depth, additive noise, edge smoothing, homogeneous region, and combined attacks et cetera) to reconcile the copied area with the full image, were experimented to gauge performance of proposed method. It evident that, image-level of image splicing detection, the present method outperformed the best of the latest works in this area with accuracy rate of 99.03%, sensitivity 99.6%, and specificity 98.1%.

6. References

1. Ahmed, J. A., & Brifcani, A. M. A. (2015). A new internal architecture based on feature selection for holonic manufacturing system. *International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering*, *2*(8), 1431.
2. Aizenberg, I., Butakoff, C., Karnaukhov, V., Merzlyakov, N., & Milukova, O. (2003). Type of Blur and Blur Parameters Identification Using Neural Network and its Application to Image Restoration, 1–7.
3. Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G., & Mathkour, H. (2017). Passive detection of image forgery using DCT and local binary pattern. *Signal, Image and Video Processing*, *11*(1), 81–88.
4. Bahrami, K., & Kot, A. C. (2015). Image Splicing Localization Based on Blur Type Inconsistency, 1042–1045.
5. Choi, H., Jang, H., Kim, D., Son, J., Mun, S., Choi, S., & Lee, H. (2017). Detecting Composite Image Manipulation

based on Deep Neural Networks, 0–4.

6. Guo, Z., Zhang, L., & Zhang, D. (2010). A completed modeling of local binary pattern operator for texture classification. *IEEE Transactions on Image Processing*, *19*(6), 1657–1663.
7. Heikkilä, M., Pietikäinen, M., & Schmid, C. (2006). Description of interest regions with center-symmetric local binary patterns. In *Computer vision, graphics and image processing* (pp. 58–69). Springer.
8. Li, C., Ma, Q., Xiao, L., Li, M., & Zhang, A. (2017). Image splicing detection based on Markov features in QDCT domain. *Neurocomputing*, *228*, 29–36.
9. Li, H., Luo, W., Qiu, X., & Huang, J. (2017). Image forgery localization via integrating tampering possibility maps. *IEEE Transactions on Information Forensics and Security*, *12*(5), 1240–1252.
10. Marra, F., Gragnaniello, D., Cozzolino, D., & Verdoliva, L. (2018). Detection of GAN-generated fake images over social networks. In *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)* (pp. 384–389).
11. Muhammad, G., Al-Hammadi, M. H., Hussain, M., & Bebis, G. (2014). Image forgery detection using steerable pyramid transform and local binary pattern. *Machine Vision and Applications*, *25*(4), 985–995.
12. Redi, J. A., Taktak, W., & Dugelay, J. L. (2011). Digital image forensics: A booklet for beginners. *Multimedia Tools and Applications*, *51*(1), 133–162. https://doi.org/10.1007/s11042-010-0620-1
13. Tan, X., & Triggs, W. (2010). Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE Transactions on Image Processing*, *19*(6), 1635–1650.
14. Zandi, M., Mahmoudi-Aznaveh, A., & Mansouri, A. (2014). Adaptive matching for copy-move Forgery detection. In *Information Forensics and Security (WIFS), 2014 IEEE International Workshop on* (pp. 119–124).