Detection of Digital Image Forgery using Fast Fourier Transform and Local Features

Navdeep Kanwal
I.K.G. Punjab Technical University
Kapurthala
Punjab, India
navdeepkanwal@gmail.com

Akshay Girdhar
Department of I.T.
Guru Nanak Dev Engineering College
Ludhiana, Punjab, India
akshay1975@gmail.com

Lakhwinder Kaur
Department of CSE
Punjabi University
Patiala, India
mahal2k8@yahoo.com

Jaskaran Singh Bhullar
Applied Science
M. I. M. I. T.
Malout, India
bhullarjaskarn@gmail.com

***Abstract*—Multimedia security is one of the key challenges in today's world, as dependency on multimedia information is increasing day by day. Easily available image editing software have enabled every common user of a smart phone and computer, to hack into the information of the images and video and alter it to some extent. To authenticate the genuineness of images, detection of image tempering is need of the time. Various techniques have been proposed to use image features for detection of image forgery. The techniques of forgery detection work in two domains of image forgery; copy-move forgery detection (CMFD) and image splicing detection (ISD). This paper presents a comprehensive comparative analysis for the use of local texture descriptors i.e. local binary pattern (LBP) and local ternary pattern (LTP) for forgery detection in an image. The paper also presents a technique to integrate fast fourier transform (FFT) with local texture descriptors for image forgery detection using existing block-based methodology. Performance of the technique(s) and descriptor(s) is tested for benchmarked dataset CASIA v1.0. Results are evaluated by using standard detection metrics detection accuracy and recall. The paper also suggests a relatively better texture descriptor.**

Keywords—image forgery detection, copy-move forgery, image splicing, LBP, LTP

I. INTRODUCTION

In today's world, visual media is the primary source of communication. Visual media is paragon at explaining the situation at its best. Malicious modification of digital images with the intent to deceive for the sake of altering the public perception is termed as Digital Image Forgery. Forgery has a sole purpose of changing public perception. Forging an image takes just one thing into consideration that people usually believe what they see. Decisions can be easily manipulated by altering the images with user-friendly and easily available image editing tools [7] like Sumopaint, Paintshop Pro, Photoshop CC and HitFilm Express. These easily available tools make forgery no longer restricted to specialists. Manipulation is done so precisely that it hardly leaves any visible traces. An observer cannot sense manipulation with naked eye and needs some scientific methods to detect forgery in the image. Image is commonly manipulated with two basic operations of copy-paste or image splicing [20], [13]. Image splicing is very basic and harmful type of forgery. Image Splicing creates a composite image by blending cropped regions to same or different image. Some post processing operations like blurring are performed after pasting the region to completely merge the pasted portion with the background. Figure 1 highlights the process of image splicing and Figure 2 elaborated an example of the same. Image forgery detection can be active or passive. An active approach makes use of prior information, embedded into the image to verify its authenticity. Such information is embedded using digital watermark or digital signatures [22]. Passive approaches are prioritized over the active approach as they do not need any prior information but the image itself. These approaches have no knowledge about the origin of the image. As tampering is not visually detectable, passive approach analyzes the underlying statistical characteristic of the image which are supposed to be definitely disturbed by the manipulation process. Image forensics predominantly uses passive approach to verify image authenticity [2] [4] [15]. This paper discusses techniques to detect image splicing forgery.

(a) (b) (c)

Fig. 1. (a) Original Image; (b) Forged Image; (c) Image Retouching [25]

Fig. 2. Image Splicing by using two different images [5]

Taking into account the fact that pasting of a cropped portion onto a different image, replaces the existing micro edge patterns of the host image with its own patterns, which make the pasted portion different from the rest of the image and such disturbance is peculiar along its boundary, visual descriptor LBP and its variants are used to encode the micro edge patterns and DCT is used to encode the frequency content with respect to each blocks LBP value. This approach utilizes the chrominance component of the RGB image which is believed to capture the disturbance created by forgery better than any other color channel [18], [8]. A technique of forgery detection is presented that uses fast fourier transform of the chrominance component for extracting local features of the image. SVM Classifier is used for classifying the images as forged or authentic.

II. Related Work

A detection technique based on the combination of LBP, discrete wavelet transforms (DWT) and principal component analysis (PCA) was proposed in [9] with support vector machine (SVM). The combination of LBP and DWT asserted for the improvement in accuracy rate in CASIAv1.0 is 97.21% and in case of Columbia dataset is 95.13%. [1] put forward another method which was also based on LBP and DCT. This method was suggested to detect copy move and image splicing forgery. It used DCT to convert the LBP image into its frequency domain, in-order to discover any chances of tampering more precisely. After that, for each block statistical measures of computed DCT coefficients are calculated. Such methods train the SVM classifier to differentiate between the authentic and forged images. This method yielded the best precision on CASIAv1.0 as 97%, CASIAv2.0 as 97.50% and CISDE dataset as 97.77%. [29] had proposed a technique to detect image splicing forgery. This technique was imitation of the magnitude component of 2D arrays which were acquired by applying multi-size block discrete cosine transform (MBDCT) on testing images, using LBP. The dimensionality of feature set was deducted by using the kernel principal component analysis (K-PCA), to ensure it to be more efficient mathematically. Using this reduced feature set, SVM was able to classify the authentic images and tampered images. This method attained a precision of 90.46%. A tampering detection technique is proposed in [21] using multi- scale LBP and DCT. This technique divide the image into non-overlapping blocks of various sizes 32*32, 64*64, 16*16. After dividing in the blocks, they were passed to DCT to extract the coefficients. In-order to build a feature set of the image, standard deviation was calculated with respect to computed coefficients. In the proposed method, the classifier was trained by using the SVM along with radial basis function (RBF) kernel. It attained the precision rate on CASIAv1.0 96% and on CASIAv2.0 97.3%. Other research paper [17] put forward another method to determine the image authenticity. It this method, Markov features were extracted discretely in all the three domains. It was the first method which combined three domains, they were – spatial domain, DCT and DWT domain. Efficient classifier used in the proposed method, reduced the computational complexity as well as yield an efficient TPR, TNR and precision rate without making use of PCA. It attained a precision rate of 99.80% on Columbia Image Splicing Detection Evaluation Dataset (CISDE).

Another method to detect image splicing forgery, by using Markov features in QDCT domain was developed in [14]. It took RGB image without converting into grey scale to avoid any color distortion and it also resulted in improved precision. Markov feature were extracted from quaternion discrete cosine transform (QDCT) frequency domain of the blocked color image. SVM classifier was trained by these extracted features. This method enhanced the precision level to 92.38%. [6] proposed a method to discover whether an image was authentic or tampered, based on spatial and DCT based Markov features. First, Markov features were extracted from spatial and DCT domains and then they were combined. In order to reduce the dimensionality, the most relevant features were extracted from combined feature set, by using a PCA. SVM along with RBF kernel method was used, to optimize the classification process. This method was determined to be more than 98% precise, when assessed on Columbia Image Splicing Detection Evaluation Dataset (CISDE). One more method to detect image splicing forgery proposed in [10] deploy quantization- based Markov feature extraction. The performance was enhanced by reducing the loss of information, so quantization is used in this method. Two Markov feature selection method made use of the summation and maximization of the color feature. The proposed method had been tested on CASIAv1.0, CASIAv2.0 and Columbia color datasets and the results were precise to be 98.95%, 97.25% and 95.24% respectively. [26] used a noise level evaluation method which was intensity dependent, to determine image splicing forgery in the digital image. Here, the base used for splicing forgery detection was a variable noise level which vary depending on image taken from different sources. This method was outstanding, as it was the only method with varying noise level of blocks taken from different image sources and captured by the same camera. For localization of image splicing, [28] had proposed another method to highlight forged region in the image. This method utilized previous noise level estimation algorithm and PCA based algorithms, in order to determine block wise noise level of a testing image. K-means clustering was used to differentiate between the spliced region and the original region. When difference between spliced region and original region was small noise, then this method attained high performance. Contrary, when the spliced region and the original region had same noise level, then this method failed to localize the tampering.

III. Forgery Detection Methodology

As discussed above, multi-image forgery in the images may be detected through analysis of local texture and LBP. It has been used by various researchers [3] for detecting image forgery. Image splicing detection has been achieved in the present work by following the methodology shown in Figure 3. RGB image is firstly converted into YC_BC_R format. Chrominance part of the converted image is used for further evaluation, as chrominance part include suitable information for forgery detection [18], [8]. Two different approaches have been suggested in the methodology for forgery detection.

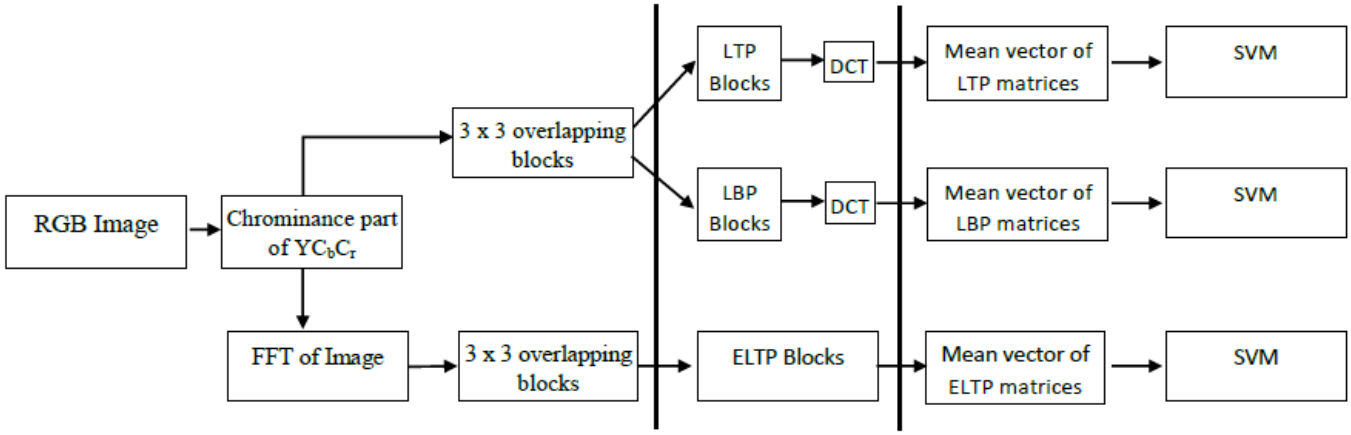

Fig. 3. Image splicing detection methodology

A. Forgery Detection using LBP and LTP

In first approach chrominance component is divided in overlapping blocks of size 3x3 and then two type of features are extracted from these blocks i.e. LBP and LTP:

1) Local Binary Pattern (LBP): LBP was initially proposed in [19] for extracting local features of an image. LBP possesses a two valued code matrix which is framed using equation 1:

$$LBP_{x,y} = \sum_{x=0}^{X-1} s(g_x - g_t)2^x$$
$$s(x) = \begin{cases} 1, if\ x \geq 0; \\ 0, otherwise \end{cases} \quad (1)$$

where 'g_x' and 'g_t' are the gray value of current neighborhood pixel and central pixel respectively. 'X' is the number of pixels in the block. A binary matrix is returned by the above equation which is then converted to decimal for convenience as shown in Figure 4.

2) Local Ternary Pattern (LTP): LBP is prone to random and quantization noise in near-uniform regions because its value depends center pixel value [24]. Local ternary pattern (LTP) was proposed as an enhancement to LBP and generates 3-valued code by following equation 2 [24].

$$s'(g_x, i_t, th) = \begin{cases} 1, & g_x \geq g_t + th \\ 0, & g_x - g_t < th \\ -1, & g_x \leq g_x - th \end{cases} \quad (2)$$

where 'th' is the constant threshold value.

DCT is applied on these feature matrices to generate feature coefficients (LBP/LTP). Mean for every DCT block is calculated for dimensionality reduction and generating the final feature vector. This vector is then fed to SVM classifier for classifying the image as authentic or forged.

B. Forgery Detection using FFT and ELTP (FFT-ELTP)

In the second approach, chrominance component is transformed using fast Fourier transform and then segmented into overlapping bocks. Instead of using LBP or LTP for feature extraction, the present paper evaluates extension of LTP as enhanced local ternary pattern (ELTP) [27] code for these blocks to generate a feature vector:

1) Fast Fourier Transform: Fast fourier transform (FFT) is an efficient way to compute discrete fourier transform (DFT) [12]. An image matrix is transformed to discrete fourier coefficients by formulation in equation 3.

$$Y_{p+1,q+1} = \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} w_m^{jp} w_n^{kq} X_{j+1,k+1} \quad (3)$$

where 'w_m' and 'w_n' are complex root of unity, defined as $e^{-2\pi i/m}$ and $e^{-2\pi i/n}$ respectively and 'i' is the imaginary unit.

2) Enhanced Local Ternary Pattern: Yuan et. al [27] have extended the LTP to attain better features for the image by introducing ELTP. The constant value in the LTP makes it less robust for gray level transformations.

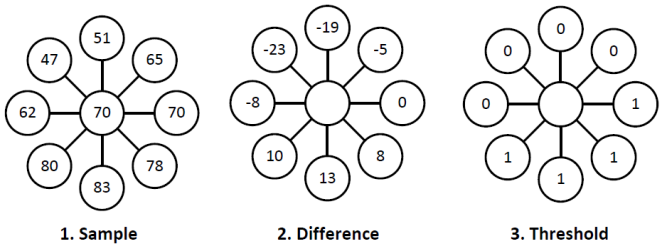

Fig. 4. Methodology to generate LBP Code

ELTP uses a dynamic threshold value based on the mean absolute deviation(mad) of the respective block. ELTP achieves significantly better results in texture classification in comparison to LBP and its variants [27]. Computation of ELTP is formulated in equation 4-5:

$$s^e(g_x, g_t^e, t^e) = \begin{cases} 1, & g_x - g_t^e \geq th^e \\ 0, & g_x - g_t^e < th^e, \quad x = 0, 1, ..., X-1 \\ -1, & g_x - g_t^e \leq -th^e \end{cases} \quad (4)$$

$$G = g_i \| i = 0, 1, ..., 8 \| \\ g_t^e = mean(G), \quad th^e = mad(G) \quad (5)$$

where *G* represents set of grey values. ELTP code is derived from ELTP matrix through equation 6-7 for the current pixel at coordinates *(X; Y).*

$$ELTP_{X,Y} = ELTP\_X_{X,Y} * (X+2) - \\ 4(ELTP\_X_{X,Y} * (ELTP\_X_{X,Y} + 1))/2 \\ + ELTP\_N_{X,Y} \quad (6)$$

where

$$ELTP\_X_{X,Y} = \sum_{x=0}^{X-1} e(s^e(g_x, g_t^e, th^e), 1), \\ ELTP\_N_{X,Y} \sum_{x=0}^{X-1} e(s^e(g_x, g_t^e, th^e), -1) \quad (7)$$

$$e(xx, yy) = \begin{cases} 1, & xx = yy \\ 0, & x \neq y \end{cases}$$

The generated feature vector in this approach will contain ELTP code for every FFT block of the image. This is fed to SVM classifier for classification of the image as authentic or forged.

IV. Experimental Analysis

A. Evaluation Metrics

The performance of the proposed methodology has been evaluated for both approaches using accuracy and recall performance measures formulated in equations 8 and 9 respectively.

$$Accuracy = 100X \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

$$Recall = \frac{TP}{TP + FN} X100 \quad (9)$$

Where TP presents true positives; the number of tampered images which are identified correctly as tempered by the technique. FP is false positives that identifies number of original images that are wrongly labeled as forged. TN denotes true negatives; total number of authentic images identified accurately, and FN is false negatives i.e. number of forged images labeled as authentic.

B. Dataset

The proposed method is evaluated using standard dataset CASIA v1.0 [5]. CASIAv1.0 is one of the most common dataset used by researchers for testing performance of forgery detection technique(s). The dataset contains 921 forged and 800 authentic images. Variety of images in dataset is helpful to examine the robustness of the method against the various types of the image information. CASIA v1.0 has eight different types of images. All the images are RGB images with size 384 x 256 or 256 x 384.

C. Classification

The results have been classified using support vector machine (SVM) classifier. SVM works in a supervised learning environment. The classifier is fed with feature vectors generated by all the images. 10-fold classification approach has been used for the evaluation. Training of the classifier is performed by choosing features of random 90% images from the data population. Remaining 10% image features are used as test data. The process is repeated for all the images on random basis. SVM may use different kernels to classify the data. Present paper works with radial basis function (RBF) kernel. FFT-ELTP approach has been evaluated by fine tuning SVM classifier by setting value of γ equal to '0.3225'. This value has been computed by cross validating the classifier on data population.

D. Results and Discussion

Images from the dataset are used for testing the performance of methodology using different image features.

1) Evaluation of LBP based approach: Dimensionality reduction of LBP features is compared for mean and standard deviation for each block. Figure 5 presents detection accuracy of the LBP based methodology for different category of images. It can be observed that mean based feature extraction outperforms the use of standard deviation.

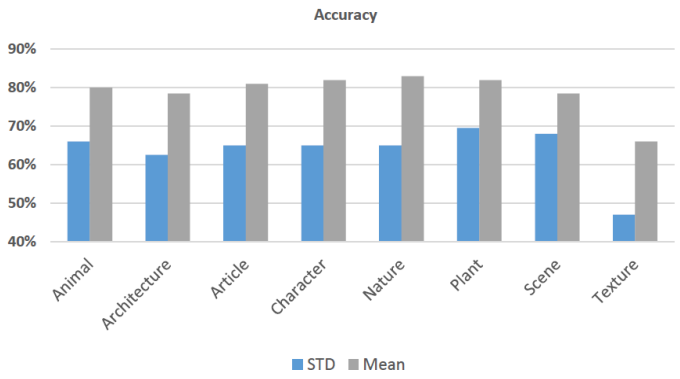

Fig. 5. Accuracy of methodology over different categories of images in CASIA v1.0

Figure 6 presents recall rate for LBP based methodology. It can be observed from this figure also that mean based dimensionality reduction produces a better recall rate. Both the comparison graphs highlight that mean may be considered as a better option for dimensionality reduction. Further, it is also visible that methodology perform well for majority of image categories except for the texture-based images.

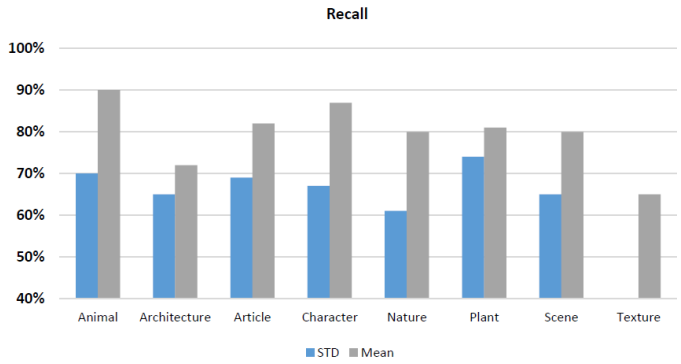

Fig. 6. Recall rate of methodology over different categories of images in CASIA v1.0

2) Comparison of LBP, LTP and FFT-ELTP based approach: All the approaches have been evaluated and compared for accuracy and recall rate. Figure 7 presents a graphical comparison for the three techniques. It can be concluded from the graph that FFT-ELTP technique performs relatively better as ELTP helps to provide a higher detection accuracy.

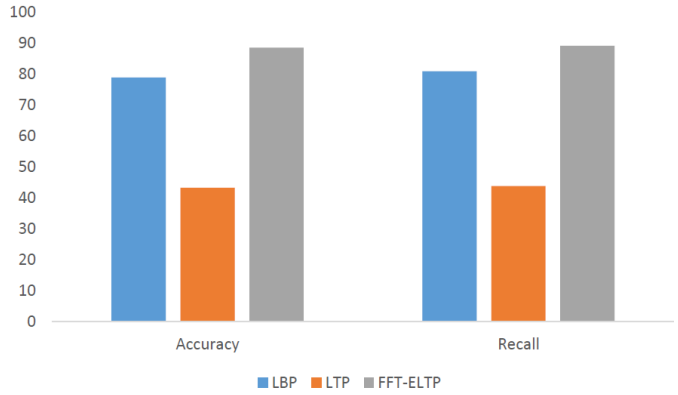

Fig. 7. Comparison of LBP, LTP and FFT based ELTP features

3) Comparison with existing techniques: As FFT-ELTP has come out as better technique according to comparison presented above, it has been further compared with the existing techniques of image splicing detection. The summary of comparison has been tabulated in Table I below:

The comparison in the table I presents that FFT-ELTP is a better performing technique which delivers higher accuracy than recent techniques too. FFT-ELTP methodology can be preferred for detecting image splicing in the images.

V. Conclusion

Image forgery detection is need of the time due to increasing image editing tools and reliance on multimedia information.

TABLE I. Comparison of FFT-ELTP Technique with Existing Techniques for CASIA V1.0

Method	Accuracy
He Z. et. al (2011) [11]	80.58%
Su. Bo et. al (2014) [23]	87.5%
Mayer et. al (2018) [16]	83.8%
FFT-ELTP	88.62%

The paper has presented two approaches for detecting image splicing. Both the approaches use overlapping blocks to extract image features. First approach extracts LBP or LTP features based on gray values of the image chrominance whereas second approach extract the ELTP features from fast fourier transform of the chrominance channel. Results of these techniques have been presented in comparative manner. It can be observed that LBP and ELTP perform as better features to classify the image as forged or authentic. ELTP in particular comes out to be a significantly better feature in comparison to existing image splicing detection techniques. The FFT-ELTP technique perform fairly by achieving an accuracy of 88.62% on compressed images of CASIAv1.0 dataset. However, all of the presented approaches involve complex transformations like DCT and FFT which increases the complexity of the methodology. Future work in the same direction may be to

reduce the need of such complex operations. Localization of the forgery in the image is also area to be explored in the further research.

ACKNOWLEDGMENT

I.K.G. Punjab Technical University, Kapurthala for providing the opportunity to do research in this field.

REFERENCES

[1] 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 and Video Processing, vol. 11, no. 1, pp. 81–88, 2017.

[2] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital investigation, vol. 10, no. 3, pp. 226–245, 2013.

[3] Cavalin and L. S. Oliveira, "A review of texture classification methods and databases," in Graphics, Patterns and Images Tutorials (SIBGRAPIT), 2017 30th SIBGRAPI Conference on. IEEE, 2017, pp. 1–8.

[4] A. Doegar, M. Dutta, and G. Kumar, "A review of passive image cloning detection approaches," in Proceedings of 2nd International Conference on Communication, Computing and Networking. Springer, 2019, pp. 469–478.

[5] J. Dong, W. Wang, and T. Tan, "Casia image tampering detection evaluation database," in Signal and Information Processing (ChinaSIP), 2013 IEEE China Summit & International Conference on. IEEE, 2013, pp. 422–426.

[6] E.-S. M. El-Alfy and M. A. Qureshi, "Combining spatial and dct based markov features for enhanced blind detection of image splicing," Pattern Analysis and Applications, vol. 18, no. 3, pp. 713–723, 2015.

[7] H. Farid, "Digital doctoring: how to tell the real from the fake," pp. 162–166, 2006.

[8] F. Hakimi, M. Hariri, and I. Azad, "Image-Splicing Forgery Detection Based on Improved LBP and K-Nearest Neighbors Algorithm," no. September 2015, 2015.

[9] F. Hakimi, M. Hariri, and F. GharehBaghi, "Image splicing forgery detection using local binary pattern and discrete wavelet transform," in Knowledge-Based Engineering and Innovation (KBEI), 2015 2nd International Conference on. IEEE, 2015, pp. 1074–1077.

[10] J. G. Han, T. H. Park, Y. H. Moon, and I. K. Eom, "Quantizationbased markov feature extraction method for image splicing detection," Machine Vision and Applications, vol. 29, no. 3, pp. 543–552, 2018.

[11] Z. He, W. Sun, W. Lu, and H. Lu, "Digital image splicing detection based on approximate run length," Pattern Recognition Letters, vol. 32, no. 12, pp. 1591–1597, 2011. [Online].

[12] P. Heckbert, "Fourier transforms and the fast fourier transform (fft) algorithm," Computer Graphics, vol. 2, pp. 15–463, 1995.

[13] N. Kanwal, A. Girdhar, L. Kaur, and J. Bhullar, "A Taxonomy and Analysis of Digital Image Forgery Detection Techniques," Journal of Engineering, Science and Technology, 2017.

[14] 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.

[15] X. Lin, J.-H. Li, S.-L. Wang, F. Cheng, X.-S. Huang et al., "Recent advances in passive digital image security forensics: A brief review," Engineering, vol. 4, no. 1, pp. 29–39, 2018.

[16] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1762–1777, 2018.

[17] R. Mehta and N. Agarwal, "Splicing detection for combined dct, dwt and spatial markov-features using ensemble classifier," Procedia Computer Science, vol. 132, pp. 1695–1705, 2018.

[18] G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," Machine Vision and Applications, vol. 25, no. 4, pp. 985–995, 2014.

[19] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Transactions on pattern analysis and machine intelligence, vol. 24, no. 7, pp. 971–987, 2002.

[20] J. A. Redi, W. Taktak, and J. L. Dugelay, "Digital image forensics: A booklet for beginners," Multimedia Tools and Applications, vol. 51, no. 1, pp. 133–162, 2011.

[21] A. Shah and E.-S. El-Alfy, "Image splicing forgery detection using dct coefficients with multi-scale lbp," in Computing Sciences and Engineering (ICCSE), 2018 International Conference on. IEEE, 2018, pp. 1–6.

[22] K. Sreenivas and V. K. Prasad, "Fragile watermarking schemes for image authentication: a survey," International Journal of Machine Learning and Cybernetics, vol. 9, no. 7, pp. 1193–1218, 2018.

[23] Su, Q. Yuan, S. Wang, C. Zhao, and S. Li, "Enhanced state selection markov model for image splicing detection," EURASIP Journal on wireless communications and networking, vol. 2014, no. 1, p. 7, 2014.

[24] 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.

[25] Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD – New Database for Copy-Move Forgery Detection," Proceedings of 55th International Symposium ELMAR-2013, no. September, pp. 25–27, 2013.

[26] H. Yao, S. Wang, X. Zhang, C. Qin, and J. Wang, "Detecting image splicing based on noise level inconsistency," Multimedia Tools and Applications, vol. 76, no. 10, pp. 12 457–12 479, 2017.

[27] J.-H. Yuan, H.-D. Zhu, Y. Gan, and L. Shang, "Enhanced local ternary pattern for texture classification," in International Conference on Intelligent Computing. Springer, 2014, pp. 443–448.

[28] H. Zeng, Y. Zhan, X. Kang, and X. Lin, "Image splicing localization using pca-based noise level estimation," Multimedia Tools and Applications, vol. 76, no. 4, pp. 4783–4799, 2017.

[29] Y. Zhang, C. Zhao, Y. Pi, and S. Li, "Revealing image splicing forgery using local binary patterns of dct coefficients," in Communications, Signal Processing, and Systems. Springer, 2012, pp. 181–189.