International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 4, ISSN No. 2455-2143, Pages 12-18
Published Online August 2019 in IJEAST (http://www.ijeast.com)

EFFECTIVE DETECTION METHOD OF BOTH COPY-MOVE AND SPLICED OF TEMPERED IMAGES

Md. Ahasan Kabir
Department of Electronics and Telecommunication Engineering
Chittagong University of Engineering and Technology
Chittagong, Bangladesh

***Abstract*— In present digital world, due to increasing image processing tools, authenticity and integrity of digital images are being hampered. There are numerous detection techniques of tempered images. But most of them detect copy-move and spliced forgery images separately. These techniques are complex and less efficient. In this paper, I proposed an algorithm to detect copy-move and spliced in a forgery images. At first, Discrete Wavelet Transform (DWT) is used to transform image to detect the image edges and then reconstruct the edges of the forged regions by applying morphological operator. Secondly, the image is split into overlapping blocks to extract functionality using Local Binary Patterns (LBP) and Euclidean distance. Based on these features both copy-move and spliced forgery is detected. The proposed algorithm is comparable to the existing Speed up Robust Features (SURF) and Weber Local Descriptor (WLD). The proposed method work effectively not only for noise contamination and blurring image, but also, it is robust enough for rotation and flipping.**

Keywords— spliced image; copy-move image; dilation; DWT; LBP.

I. Introduction

Image is a representation of a physical object's visual perception. Digital image refers to a numeric representation of two dimensional images. Nowadays, imaging technology is improving day by day which provides remarkably easy manipulation of digital images. There is a lot of image processing softwares, that help to temper digital images easily, such as Adobe Photoshop, Coreldraw etc. so that, it is hard to recognize the picture is unique or not through exposed eyes, as shown in Fig. 1. The tempered images are known as forgery images. In case of identifying a tempered image, image forgery detection is mandatory. To detect image forgery researchers propose various algorithm.

Forgery detection provides verification of a digital image's authenticity. Image detection techniques for falsification are divided into the following main types: (a) active and (b) passive or blind. Computerized watermarking or advanced mark is a functioning image falsification location system utilizes a secret code inserted into an image [1]. Various watermarking techniques and digital signature have been proposed not only for authentication but also for detecting forgery [2-8].

Due to the proliferation of image processing softwares, an image forgery detector must have to be robust enough to identify any kind of tempering. Basically, the common methods used for image forgery are copy-move, compositing, splicing, enhancing etc. Furthermore, the tempered image undergoes some post-processing manipulation in order to making it original. The post-processing manipulations are lossy JPEG compression, Gaussian noise contamination, blurring, rotating etc.

There are various proposed methods for detecting forgery images along with post-processing manipulation. But there contains complexity and lack of detecting all types of manipulation, which will hamper the authenticity of the image. For example, a strategy is proposed to recognize duplicate move and grafted picture where Run Difference Method (RDM) and Discrete Wavelet Transform are utilized to identify the imitation controls in pictures including duplicate move or joining or both [9]. But in case of rotation, this method is not applicable.

Considering the previously mentioned issues, a calculation is proposed in this paper to distinguish a duplicate move picture as well as a joined picture. This strategy is strong against the picture post-handling activities, for example, obscuring, Gaussian commotion, JPEG pressure, and pivot. Sharpe edges of the fashioned pictures can be distinguished by using DWT. Morphological task (enlargement) is utilized to remake the limits of the manufactured edges. The characterized district is contrasted with different locales of the picture so as to identify duplicate move or joined fraud. Local Binary Pattern (LBP) is used in case of rotated and flipped regions.

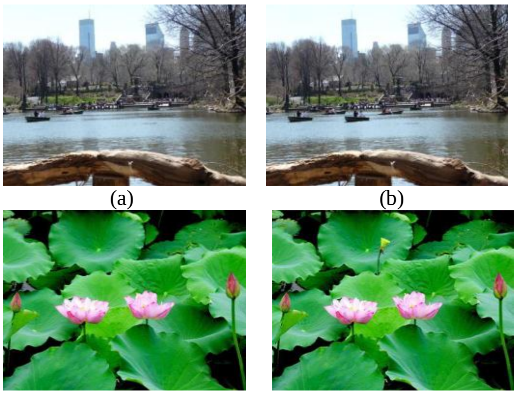
This paper is composed of pursues. The inspiration for picture fabrication identification has been examined in the main segment. The second segment portrays the methods utilized for picture phony recognition and sorts of computerized picture falsification. The third area discloses the proposed strategy to recognize duplicate move and joined fraud pictures dependent on DWT and LBP. The fourth section deals about the results and performance analysis, consequently, the final section presents conclusions and the future work.

II. FORGERY DETECTION TECHNIQUES

Passive or blind techniques are adapted for detecting image splicing, copy-move and image retouching etc. where, an image can be made by cutting a particular district from one image and sticking it into an alternate image, called grafted image, (see Fig. 1(f)). Close to this, it very well may be tempered by cutting an image area and gluing it to somewhere else in a similar image, which is called duplicate move image, (see Fig. 1(b), (d)).

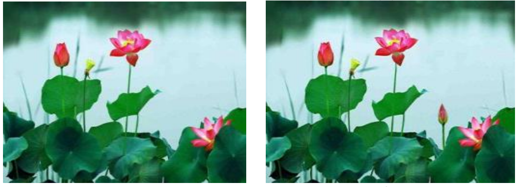
Numerous strategies have been proposed to identify duplicate move imitations utilizing discrete cosine change (DCT) [11], principle component analysis (PCA) [12], seven characteristics features [13], discrete wavelet transform (DWT) coupled with singular value decomposition (SVD) [14], improved discrete cosine transform [15], local binary patterns (LBP) [16], wavelet decomposition and principle component transformation [17], A-KAZE and SURF Features, Hierarchical Feature Point Matching work describe in [18-20]

On the contrary, support vector machine (SVM) [21], CFA interpolation [22], camera response function (CRF) [23], zero-crossing and discrete Fourier transform (DFT) [24], discrete cosine transforms and local binary pattern [25] methods are used in case of detecting spliced forgeries.



(a) (b)

(c) (d)



(e) (f)

Fig 1: Example images of Original, Copy-move and Spliced Images [10]. Original images are (a), (c) & (e); (b) & (d) are the Copy-move images of (a) & (c) respectively; (f) is the Spliced image from (c) & (e).

A couple of strategies have been distributed so far which manage both duplicate move and grafted falsification pictures. A blend of DCT and SURF is proposed which performs well on the recognition of phony limitation [26]. Another technique is distributed which is fit for recognizing duplicate move or joined imitation utilizing a multi-goals Web Law Descriptor (WLD) [27].

III. PROPOSED METHOD

The whole process is divided into two major steps: confirmation of the forgery and identification of the type of forgery (copy-move/spliced). At first some related theory is described in brief, then the proposed method will be discussed.

A. *Grayscale Image*

The proposed technique operates with grayscale image. Grayscale image comprises of two colors: black and white, with various intensity levels varying from black at the weakest intensity to white at the strongest. The pixel values of gray image are from 0 to 255.

The information shading picture is changed into dark picture since shading data doesn't help us recognizing essential edges. A RGB picture is a three channel shading picture that takes multiple times longer handling than a grayscale picture. Along these lines, shading picture handling is progressively intricate contrasting with dark picture. Hence grayscale picture is utilized in many tempered picture identification methods.

B. *Discrete Wavelet Transform*

Wavelet is small wave that decay rapidly with continuous time wave function. In present years, DWT is one of the most popular transformation processes used by many researchers. DWT helps to reduce the actual size of the input image. That is, if a square image with size $2^n \times 2^n$ is converted to a size of $2^{\frac{n}{2}} \times 2^{\frac{n}{2}}$ at the following dimension. There are single level and multilevel DWTs and the output can be varied according to the type of wavelets.

Discrete wavelet change can be utilized for simple and quick denoising of a loud flag. DWT decomposes an image into low pass approximation, horizontal, vertical and diagonal part [10]. Horizontal, vertical and diagonal images are the combination of edges which are high frequency components. Since DWT reduces the image size by a half.

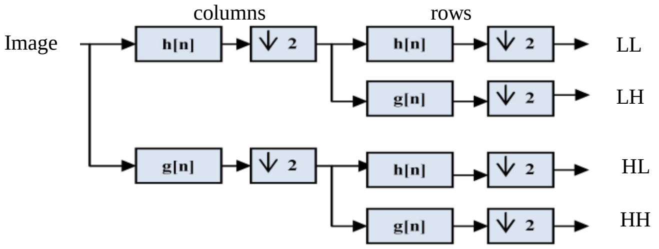
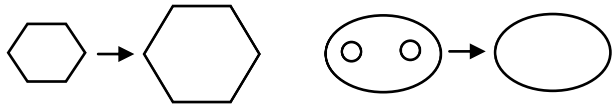


Fig. 2: One level analysis DWT filter bank.

The DWT filter bank for analysis is shown in Fig. 2. LL sub-image is further decomposed into four sub-bands in the sub sequence level [28]. In this proposed method Haar wavelet is used.

Haar wavelet is widely used in image processing and it's discrete structure are identified with a numerical process called the Haar change. The Haar change depends on a class of symmetrical lattices whose components are either 1, - 1 or 0 duplicated by forces of $\sqrt{2}$. The Haar change is a computationally effective change as the change of an N-point vector requires just 2(N-1) addition and N multiplications [29].



(a) Growing the size of the object (b) Filling the holes

Fig. 3: Typical diagram to understand morphological dilation.

C. Edge Detection

Edge represent those region in a digital image where the intensity of the image changes sharply. Using this process, the pasting region can be detected from another part of the image or from another image. For this reason edge detection is the fundamental tool to trace any copied region. Sobel, Canny, Prewitt, Roberts and fuzzy logic methods are well-known edge detection algorithms used frequently. Edges are consists of three types: horizontal, vertical and diagonal. Sobel and Prewitt edge detector helps to detect horizontal and vertical edges. On the other hand, Canny detector detects horizontal, vertical and diagonal edges. For the better detection of sharped edges, Canny edge detector is used in the proposed detection technique.

D. Morphological Operation

Morphological operation is the image processing operation used to process images based on shape. Twofold numerical morphology comprises of two essential tasks, expansion and disintegration and a few composite relations: shutting and opening. The expansion activity expels the boisterous pixels inside the closer view locale or inside the item district and yet, this widening task extends the region of the article area along the limit utilizing an organizing component. It tends to be utilized for developing highlights, filling openings and holes, Fig. 3.

Morphological operation changes shapes of the object according to the structuring element. Stucturing element is a shape mask having an origin. Image dilation helps to identify smooth boundary region, making it easier to find out the forged area. A structuring of masking operator is used for the dilation, which is shown in Fig. 4.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Fig. 4: dilation operation used in the proposed method.

E. Feature Extraction Using Local Binary Patterns (LBP)

Local Binary Pattern is used to extract the most famous and common feature. It has low computational complexity, invariance to monotonic changes in the gray scale and the ability to describe texture [30]. LBP is generally a texture descriptor that labels each pixel in the image by appling threshold in the pixels of the neighborhood and considering the result as a binary number. Then, the histogram of these label pixels can describe the texture [31].

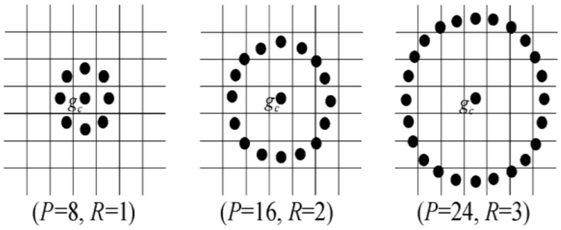
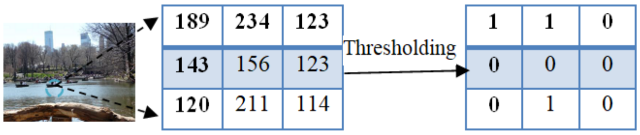


Fig. 5: Circularly symmetric neighboring sets with different (P, R) values [16].

LBP can be extricated in a roundabout symmetric neighborhood (P, R), where P is the neighbor numbers and R is the range of the area. The value of P and R can be varied as Fig. 5.



189	234	123
143	156	123
120	211	114

1	1	0
0	0	0
0	1	0

Fig. 6: LBP code computation process [25].

The LBP operator is:

$$LBP_{P,R} = \sum_{i=1}^{p-1} S(p_i - p_c)2^i \qquad (1)$$

where p_c indicate the intensity of the center pixel and the thresholding condition define as:

$$S(p_i - p_c) = \begin{cases} 1 & p_i - p_c \geq 0 \\ 0 & p_i - p_c < 0 \end{cases} \qquad (2)$$

The first surface in an image is misshaped because of image duplication. Since LBP is competent to catch surface contrasts, it is a proficient instrument for imitation recognition.

F. Proposed Method

The proposed algorithm for copy-move and spliced image detection is described by the given flowchart.

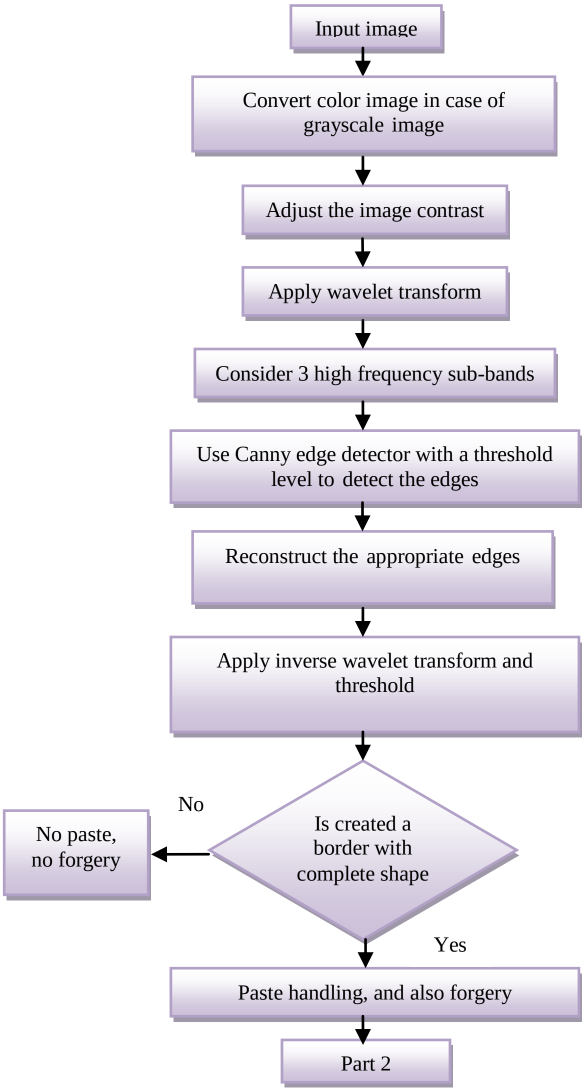

Input image
Convert color image in case of grayscale image
Adjust the image contrast
Apply wavelet transform
Consider 3 high frequency sub-bands
Use Canny edge detector with a threshold level to detect the edges
Reconstruct the appropriate edges
Apply inverse wavelet transform and threshold
Is created a border with complete shape
No
No paste, no forgery
Yes
Paste handling, and also forgery
Part 2

Fig. 6: A Flowchart to confirm the forgery in the input image.

The proposed flowchart is divided into two parts: one is the confirmation of the forgery and another one is the identification of the type of forgery (Copy-move/Spliced).

The first part, confirmation of forgery is divided into different steps, Fig. 6. A color image is transformed into a gray image at first. Color information does not help to identify important edges. Then the contrast image is adjusted before the decomposition of applied adjusting image contrast helps to find out duplicated edges easily. The adjusted image undergoes by DWT transformation. The image is divided into four sub-bands through this transformation. LH, HL, HH are sub-bands of high frequency used to detect edge. So, to find out the shape edge, they are considered; a real image has many edges or boundaries. It is therefore necessary to collect the edges caused by pasting. A threshold is set up based on each image texture. After filtering, the remaining edges are detected by canny edge detector. Next, the detected edges are dilated to reconstruct edges or boundaries in all three high frequency sub-bands. Consequently, the low frequencies in the LL sub-band are ignored by setting them to zero in order to detect the cutting / pasting parts. Therefore, from these four sub-bands, Inverse Discrete Wavelet Transform (IDWT) displays an image with only edges and boundaries. This is this part's final step, the decision step. If there are any feasible edge - covered shapes, this is caused by a fastening so that a falsification is confirmed. The number of forged regions is the number of finished shapes. The image is original, otherwise.

The confirmation in the forgery type is divided into five major steps in the second part, Fig. 7. First, the image is split into overlapping blocks to calculate the extraction of features in each block. Then feature extraction is accomplished using LBP of each block and use lexicographical sorting to store all feature vectors. Thirdly, the Euclidean distance of the feature vectors is computed to find out corresponding blocks and thus find out the matched blocks. Finally, with a specially designed filter and morphological operations, the false matches are reduced, producing the detection map. The last step is to declare the forgery type. The results may be in three cases: (I) copy - moving if there is at least one other place with a similar characteristic to the fake one, (ii) splicing if there is no similar region, (iii) both copy - moving and splicing regions or more than one copy - moving regions if there are at least two forged regions.

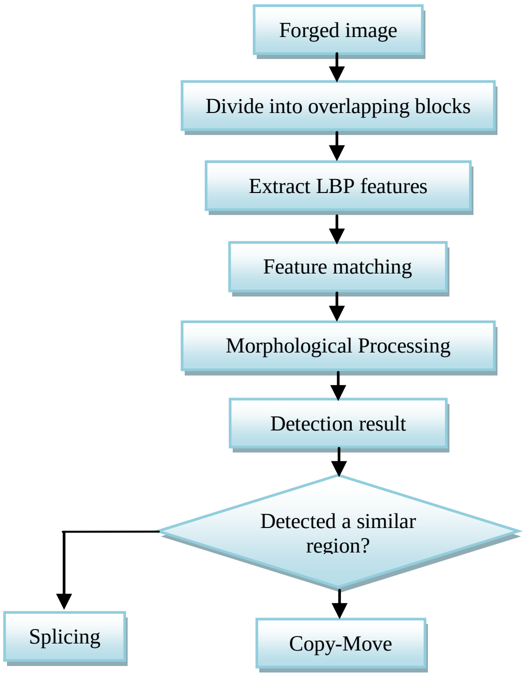


Fig. 7: The forgery confirmation; copy - move and splicing.

IV. EXPERIMENTED RESULTS

The proposed algorithm is simulated using Matlab2013a software with hp laptop, Intel(R) Core(TM) i3 - 3110 M CPU @ 2.40GHz and 4.00 GB RAM on a personal computer. The test images are collected from dataset MICC-F220 [32] and also forgeries are performed using Photoshop.

After performing the proposed DWT and LBP based method on Database of MICC-F220, the performance is compared with the previous method in [33], which is tabulated in Table I, where accuracy is calculated by the following equation,

$$Accuracy = 100 \times \frac{TP + TN}{TP + TN + FN + FP} \quad (3)$$

Where,

TP = True Positive, the number of tempered images
TN = True Negative, the number of original
FN = False Negative images, the number of tempered images classified as original images
FP = False Positive, the number of original images classified as tempered images

TABLE I. PERFORMANCE COMPARISON OF THE PROPOSED METHOD

Parameters	TP	TN	FP	FN	Accuracy
SURF	77	88	22	33	75%
DWT+SURF	71	88	21	39	72.6%
D_yWT+SURF	84	84	25	26	76.71%
Proposed Method (DWT & LBP Based)	91	100	10	19	86.82%

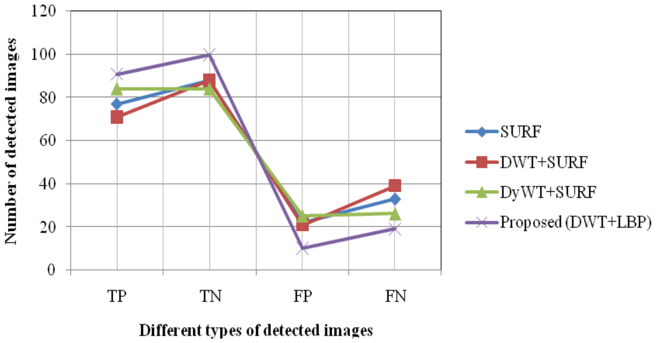


Fig. 8: Graphical representation of different types of detected images using SURF, DWT+SURF, DyWT+SURF and proposed DWT+LBP method.

The performance of the proposed method is compare with the existing methods in Table 1. The proposed DWT coupled with LBP procide better acuracy 86.82% then SURF 75%, DWT with SURF 72.6% and D_yWT+SURF 76.71%. The proposed method provide better result because DWT is used to detect sharp edges which notify the trace of duplication. Through this it is ensured that the defined image is duplicated or not. If the image is tempered, it undergoes extraction of LBP feature in which the features of the image are extracted and saved in a matrix of features. Then the corresponding features are being matched together and finally there comes a confirmation whether the tempered image is spliced or copy-move. My proposed methode is tested on MICC-F220 image database. I found efficient performance in detecting true tempered image and original image. The Graphical representation of different types of detected images using SURF, DWT+SURF, DyWT+SURF and proposed DWT+LBP method are shown in Fig. 8. The Graphical representation of the comparison of the detection performance using various methods shown in the Table I is given below (Fig. 9):

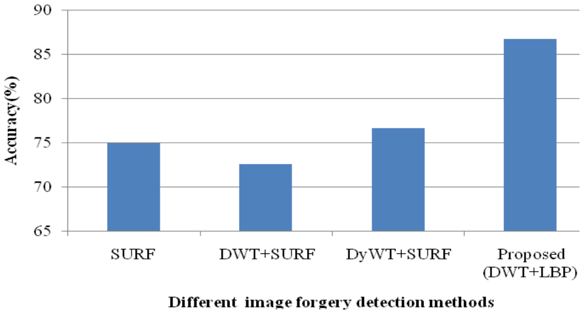


Fig. 9: Graphical comparison of performance among different types of forgery detection methods.

V. Conclusion

Due to the development and availability of image processing software, image duplication is now an easier task for any person in the digital world. It is therefore a challenge to detect any kind of image forgery successfully. The proposed method is helpful enough to find out almost all types of forgery with better accuracy. The proposed method provide better accuracy 86.82% compared with existing SURF (75%), DWT+SURF (72.6%) and D_yWT+SURF (76.71%). This proposed algorithms not only robust for traditional image processing operations, but also for rotation and flipping.

The advantage of the proposed technique is that the forgeries are effectively detect when the tempered region is rotated by general angles. Modifying the proposed method for detecting random region rotations is the future work.

VI. References

[1] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, pp. 226-245, 2013.

[2] C. T. Hsieh, Y. K. Wu, and K. M. Hung, "Geometric invariant semi-fragile image watermarking using real symmetric matrix," vol. 10, pp. 211-220, 2007.

[3] C. T. Hsieh, Y. K. Wu, and K.-M. Hung, "An adaptive image watermarking system using complementary quantization," WSEAS Transactions on Information Science and Applications, vol. 3, pp. 2392-2397, 2006.

[4] K.-m. Hung, C.-t. Hsieh, and K.-t. Yeh, "Multi-Purpose Watermarking Schemes for Color Halftone Image Based on Wavelet and Zernike Transform," in WSEAS Transaction on Computer, 2007.

[5] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, vol. 87, pp. 1079-1107, 1999.

[6] P. Meerwald and A. Uhl, "Survey of wavelet-domain watermarking algorithms," in Photonics West 2001-Electronic Imaging, 2001, pp. 505-516.

[7] L. Wei, F.-L. Chung, and L. Hongtao, "Blind fake image detection scheme using SVD," IEICE transactions on communications, vol. 89, pp. 1726-1728, 2006.

[8] M. Schneider and S.-F. Chang, "A robust content based digital signature for image authentication," in Image Processing, 1996. Proceedings., International Conference on, 1996, pp. 227-230.

[9] Y. Sutcu, B. Coskun, H. T. Sencar, and N. Memon, "Tamper detection based on regularity of wavelet transform coefficients," in 2007 IEEE International Conference on Image Processing, 2007, pp. I-397-I-400.

[10] T. Huynh-Kha, T. Le-Tien, S. Ha-Viet-Uyen, K. Huynh-Van, and M. Luong, "A Robust Algorithm of Forgery Detection in Copy-Move and Spliced Images," International Journal of Advanced Computer Science & Applications, vol. 1, pp. 1-8, 2016.

[11] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, 2003.

[12] A. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image region [Technical Report]. 2004-515," Hanover, Department of Computer Science, Dartmouth College. USA, p. 32, 2004.

[13] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in 18th International Conference on Pattern Recognition (ICPR'06), 2006, pp. 746-749.

[14] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in 2007 IEEE International Conference on Multimedia and Expo, 2007, pp. 1750-1753.

[15] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic science international, vol. 206, pp. 178-184, 2011.

[16] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, pp. 46-56, 2013.

[17] A. Kashyap and S. D. Joshi, "Detection of copy-move forgery using wavelet decomposition," in Signal

Processing and Communication (ICSC), 2013 International Conference on, 2013, pp. 396-400.

[18] Y. Li and J. Zhou, "Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1307-1322, May 2019.

[19] Z. Zhang, C. Wang and X. Zhou, "A Survey on Passive Image Copy-Move Forgery Detection," Journal of Information Processing Systems, vol. 14, no. 1, pp. 6~31, 2018. DOI: 10.3745/JIPS.02.0078.

[20] C. Wang, Z. Zhang, and X. Zhou, “An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features,” *Symmetry*, vol. 10, no. 12, p. 706, Dec. 2018.

[21] T. T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on, 2004, pp. V-688-V-691 Vol. 5.

[22] Z. Fang, S. Wang, and X. Zhang, "Image splicing detection using camera characteristic inconsistency," in 2009 International Conference on Multimedia Information Networking and Security, 2009, pp. 20-24.

[23] Y.-F. Hsu and S.-F. Chang, "Camera response functions for image forensics: an automatic algorithm for splicing detection," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 816-825, 2010.

[24] G. K. Birajdar and V. H. Mankar, "Blind Authentication of Resampled Images and Rescaling Factor Estimation," in Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on, 2013, pp. 112-116.

[25] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE, 2013, pp. 253-256.

[26] S. D. Lin and T. Wu, "An integrated technique for splicing and copy-move forgery image detection," in Image and Signal Processing (CISP), 2011 4th International Congress on, 2011, pp. 1086-1090.

[27] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, "Image forgery detection using multi-resolution Weber local descriptors," in EUROCON, 2013 IEEE, 2013, pp. 1570-1577.

[28] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," in Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on, 2013, pp. 188-193.

[29] S. Jayaraman, S. Esakkirajan, and T. Veerakima, "Digital image processing, ed iii," ed: Tata McGraw Hill Education private limited, New Delhi, 2009.

[30] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," Pattern recognition, vol. 29, pp. 51-59, 1996.

[31] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," IEEE transactions on pattern analysis and machine intelligence, vol. 28, pp. 2037-2041, 2006.

[32] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, pp. 1099-1110, 2011.

[33] M. F. Hashmi, V. Anand, and A. G. Keskar, "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms," in Computer and Communication Technology (ICCCT), 2014 International Conference on, 2014, pp. 147-152.