A Review on Copy-Move Image Forgery Detection Techniques

A Review on Copy-Move Image Forgery Detection Techniques

Zaid Nidhal Khudhair[1,2], Dr. Farhan Mohamed[3], Karrar A. Kadhim[1,2]

[1]Faculty of Engineering, School of Computing, University Technology of Malaysia, Johor Bahru, Malaysia
[2]Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-sadiq University, Baghdad, Iraq
[3] UTM-IRDA MaGICX, Institute of Human Centred Engineering, Universiti Teknologi Malaysia

Email: zaidnidhal88@gmail.com

Abstract. With billions of digital images flooding the internet which are widely used and regards as the major information source in many fields in recent years. With the high advance of technology, it may seem easy to fraud the image. In digital images, copy-move forgery is the most common image tampering, where some object(s) or region(s) duplicate in the digital image. The important research has attracted more attention in digital forensic is forgery detection and localization. Many techniques have been proposed and many papers have been published to detect image forgery. This paper introduced a review of research papers on copy-move image forgery published in reputed journals from 2017 to 2020 and focused on discussing various strategies related with fraud images to highlight on the latest tools used in the detection. This article will help the researchers to understand the current algorithms and techniques in this field and ultimately develop new and more efficient algorithms of detection copy-move image.

1. Introduction

Nowadays, communication media images have become very useful. There is a perception that the image expresses more meaning than the words about the event or the situation captured. Digital images play a very important role in numerous fields in the modern technological environment. Mainly, they are presented in the work of defense, news work, medical checkups, and media work. With advancements in digital image technology, for example, camera equipment, programs, and computer systems, increasing use of the internet media, a digital image can be seen as an important knowledge point at the moment.

Because of technological development and accessibility of low-price hardware and software modification equipment, and the availability of advanced manipulating tools that make the image manipulation easier with minimum effort. Images forgery becomes a major problem every day.

As a result of the exponential growth of digital image editing tools, the security of digital images has been challenged because of the ease with which such images can be modified in both their origin & content. Digital image research is the latest field of research that aims to enable the authenticity of images. There are several methods proposed in digital forensics in recent years as shown in Figure 1[1]:

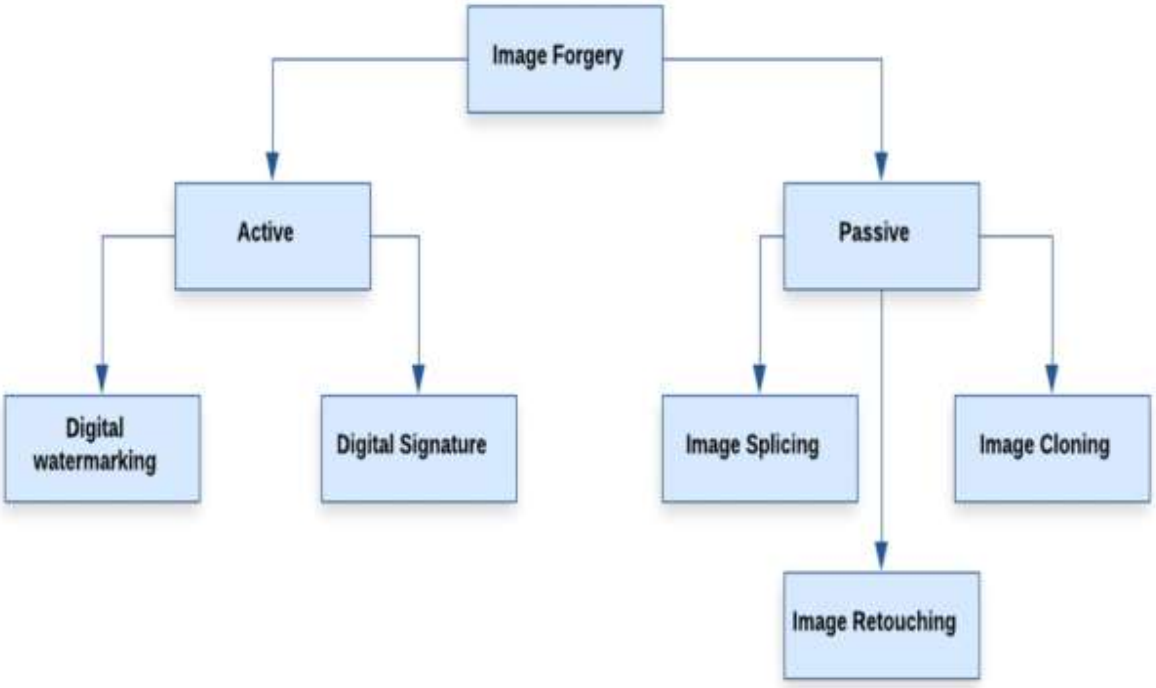

Figure 1: Types of image forgeries.

There are two types of the active methods that are digital watermarking and digital signature [2]. A digital watermark is added to the photo to identify copyright. It is the process of hiding special information (series of bits) in a digital image. The special information may be the author's serial number, company logo, meaningful text, and so on. Watermarks may be visible or inviable. Figure 2 shows an example of watermarking.

Figure 2: Digital Watermarking example

Normally, Digital messages, digital documents, and software validity are checked using a digital signature. Since the receiver may assume that the message is created by the authorized sender, based on the

valid signature. A digital signature is a mathematical technique intended to solve the problem of tampering and impersonation in digital communications.

On the other hand, passive methods include image retouching, image splicing, and copy-move attack [2]. Image retouching is considered a forgery of a minimally harmful form of the digital image. An original image does not change substantially but certain aspects of the original image have been reduced. Use this technique to manipulate the image for famous journals, in figure 3 example for image retouching.

Figure 3: Image retouching example

Splicing method is a type of falsification process to create a single image by combining two or more images. This is also called image composition, where different operations of image processing are carried out, see figure 4.

Figure 4: Splicing Method example. (a) original image. (b) spliced image.

The most common type among various forms of falsification of images is a copy-move forgery. In the digital image copy-move forgery, one or more regions are repeated at different locations within the same image. Often duplicated regions are enlarged, shrank, or rotated to make forgery more convincing, making it more difficult to detect forgery images [3] Figure 5 points to the example of copy-move forgery.

Original Image Forgery Image

Figure 5: Example of copy-move forgery

2. STUDY ON METHODS

Different image copy-move forgery detection techniques are considering and analyzed for the period range between (2017-2020) in this section. A recent study presented a method of detecting interference based on a multitexture description [4]. The Local Binary Pattern (LBP), Local Phase Quantization (LPQ), Binary Statistical Image Features, and Binary Gabor Pattern are the various texture descriptors considered. Using the image decomposition Steerable Pyramid Transform (SPT), the method captures subtle texture variations at various scales and orientations. After SPT decomposition, the different texture descriptors extracted from each subband image are combined to form the multi-texture representation. Then, to generate a compact representation, the Relief F feature selection method is applied to this high dimensional multi-texture representation. This lightweight, multi-texture representation is categorized using the classifier Random Forest.

Bin Yang *et al.* presented a feature-based copy-move forgery detection (CMFD) method [5]. A modified Scale Invariant Feature Transform (SIFT) detector is used to detect key-points. A key-point distribution strategy was created for spreading the key-points across the image. Ultimately, the improved SIFT descriptor identified the key-points for copy-move forgery detection. It presents detailed experimental findings to validate the effectiveness.

Chun-Su Park & Joon Yeon Choeh introduced a quick method that able to detect forgery with multiple geometric transformations such as region rotation, resizing, deformation, and reflection [6]. SIFT is used to extract the key-points and their descriptors to detect copy-move forgery. The suggested CMFD method has a solid theoretical background, which has better performance than the current SIFT-based algorithms. This method has good processing time.

Mohamed Abdel-Basset et al. suggested a technique that could detect the exploitation of this kind and identify the duplicated areas [7]. SIFT is based on that strategy. It is a well-known robust technique capable of detecting and matching features that belong to duplicate regions. These matched features are placed under the umbrella of a 2-level clustering strategy to ensure that features are later used to help in the geometric transformation of the duplicate areas belonging to particular clusters representing the included regions in the image.

In a study by Yue Wu et al., The authors suggested a method called BusterNet, an end-to-end deep neural network (DNN) solution for detecting faked copy-move images with two branches finding the source/target [8]. Demonstrate how the training data shortage can be solved by synthesizing a large scale of practical and reliable CMFD samples from out-of-domain datasets. Results of the evaluation show that

BusterNet outperforms state-of-the-art methods by a wide margin, and is also robust against many established CMFD attacks. On the two publicly available datasets, CASIA and CoMoFoD, BusterNet outperforms state-of-the-art copy-move detection algorithms by a large margin, and that it is robust against various known attacks.

Chengyou Wang et al. proposed to use two techniques accelerated-KAZE (A-KAZE) and speed-up robust features (SURF) to detect a copy-move forgery image [9]. One of the major drawbacks of keypoints techniques is to get enough points in smooth regions. In the proposed method, the response thresholds for the feature detection stage A-KAZE and SURF are set at small values to mitigate this defect. Also, a new map of the correlation coefficient is shown, in which bounding the duplicated regions, integrating filtering, and mathematical morphology.

Toqeer Mahmooda et al. shown a new method for detection and localization of copy-move image forgery, based on stationary wavelet transform SWT and discrete cosine transformation [10]. Choosing the SWT is due to its spectral and spatial domain translation invariance and localization properties.

In 2019, Allu Venkateswara Rao et al. suggested the CMFD method to resolve the after-attachment resizing or rotation problems of the manipulated area [11]. A new deep learning method called a Generalized Approximate Reasoning Based Intelligence Control is proposed. GARIC is used to detect a forgery in digital images.

Xinyi Wang et al. presented an enhanced regional convolutionary neural network (R-CNN) mask which is attached with a Sobel filter [12]. Sobel filter is used as an additional function to enable the predicted masks to find the similar gradients of the real mask. The network overall can identify two types of image tampering, including copy-move.

N. Hema Rajini introduced an identification method for image forgery, which simultaneously dealt with splicing and copy-move forgeries [13]. The input image transformed into color space YCbCr at the initial stage. Next, block discrete cosine transformation (BDCT) and decorrelation of images occurs as the pre-processing stage, the model will be trained using fabricated images and original. Instead, a convolution neural network (CNN) is used to identify an image as a spliced form or form of copy-move.

Payal Srivastava et al. proposed a SURF algorithm for checking the image integrity [14]. The suggested procedure works for four image blocks auto-selected. The colored input forgery image preprocessed, involves converting into a gray image, and resizing to 512x512. The method for detecting the position of copy-move forgery inside images is using the SURF function. Testing with CASIA images shows that the data have been manipulated by the blocks of the images, and the matched points (greater than or equal to 2) were detected by the suggested SURF. The authors observed after analyzing different images that the respective blocks of both images with pixel differences of over 40000 are a fabricated image.

Hui-Yu Huang & Ai-Jhen Ciou suggested using SIFT to find the key-points and their descriptors [15]. The key-points similarity is calculated to get the matching pairs depending on the descriptor. Using Helmert transformation, matching pairs will be grouped based on the spatial distance and geometric constraints. Later, the copy-move image forgery detect.

Kunj Bihari Meena & Vipin Tyagi presented a new technique that has been combining two techniques [3]. The current proposal, dividing the image into two types of regions texture and smooth. SIFT used to extract key points from these texture regions. Also, the suggested method used a block based on the smooth region by using Fourier Mellin Transformation (FMT). The FMT is a good choice for detection forgery objects under rotation and scale-invariant properties. Ultimately, the patch match algorithm used to match the key point by using generalized 2 Nearest-Neighbor, and the FMT algorithm.

By comparing extracted key points, the Pooja Bhole & Dipak Wajgi introduced a method for detecting the forgery of copy-move in an image [1]. The invariant features extracted by using the SIFT algorithm from an image, then PCA analysis of main components used to extract blocks. A hybrid approach for detecting forgeries is based on the SIFT and the Principal Component Analysis (PCA). SIFT recognizes feature points and extracts them from PCA, the next step is to test the falsification, the final step is to locate the copy-move image forgery. The research and method for detecting tampering are summed up.

Jun Young Park et al. suggested an improved key-points algorithm to detect a copy-move image forgery [16]. The suggested method uses histogram SIFT and reduced LBP. The reduced LBP is ten levels produced

from 256 levels which are collected from the oriented local window at the key point. A 138-dimensional for detecting copy-move forgery is created for a key point. This method is checked by using different image datasets and equates the accuracy of the detection of these techniques. The efficiency of the suggested scheme is more efficient than other forgery detection methods used in copy-move. The proposed approach also exhibits a consistent detection efficiency for different types of tested datasets.

Abdullah M. Moussa suggested a precise algorithm for detecting forgery by copy-move [17]. A block-based approach to detecting potential forgery is suggested using the KD-tree data structure and a basic but effective function vector. The results demonstrated state-of-the-art methods in this research, thus providing a significant acceleration. The suggested technique is in the block-matching class CMFD.

3. COMPARATIVE ANALYSIS

Comparing accuracy of the different methods published in the papers in recent years are summarized in Table 1. In addition, the advantages and disadvantages of these methods also shown in the table.

Table 1: Comparative analysis of different image forgery methods.

Ref.	Method	Forgery detection	Characteristics	Published year
[18]	Detection image forgery using a pixel-based algorithm	Detection Copy-move and splicing image forgery	This method has good accuracy and high reliability. On the other side, this method needs more time and has less accuracy to detect forgery from the noisy image.	2017
[19]	Combine two techniques, key-point based and block-based	Copy-move image forgery	It is a robust method with less complexity. But, it is less accurate and did not work well with complicated background and texture.	2017
[20]	Deep learning mechanism	Copy-move image detection	It is a highly efficient method with fewer false positives. But the accuracy is less.	2018
[21]	Using LCA and algorithm for block matching.	Detect image forgery based on analyzing the problem of the hypothesis test.	It is more efficient with less complexity. But it is not a proper method for the noisy image. The estimated error will increase.	2018
[22]	Passive digital image forensic approaches	Image forgeries detected by using the artifacts.	This method consumes minimum time and has a good ability for	2018

			generalizing. Despite it suffers from performance degradation and faces difficulties in most forgery cases.	
[23]	Using CNN and support vector machine, K nearest neighbor and Naïve Bayes	Detecting Spliced image forgery	Has good accuracy and ability to find the location of the forgery region. But it does not work well for copy-move image forgery and requires a system with high performance to handle this algorithm.	2019
[24]	Convolutional neural network (C2RNet) and diluted adaptive Clustering	Detect Spliced image forgery	It decreases the time and complexity. One of the disadvantages of this method is poorer in Recall than many other comparison algorithms.	2019
[25]	Deep learning and wavelet transformation.	Detect forgery	This method increases accuracy and reduced computational cost. But it is not robust, with high time complexity.	2019
[26]	Mathematical morphological filter detector	Detect splicing image forgery	It is highly accurate and robust to image compression. But has complexity for mathematical and time.	2020
[27]	AttentionDM for CISDL	Detect splicing image forgery	This algorithm improved the performance and computational. At the same time, it reduces the detection rate.	2020
[28]	CNN	Image splice detection and localization scheme	It is highly accurate and robust to image compression (JPEG). The disadvantage is very high complexity.	2020

Also, Table 2 summarized the accuracy of detection copy-move forgery, when using 40% forgery images out of the tested images. Comparing precision for several methods summarized in Table 3.

Table 2: Detection accuracy for various methods used in detection copy-move image forgery.

Methods	Maximum Detection Accuracy (%)
BusterNet	93.02
SPT	96.99
PCA	97.7945
Enhanced SURF	98
SVD	98.8730
PCA-DCT	98.9776
DCT	98.0624
Improved DCT	98.5882
Efficient DCT	98.5934
DyWT	98.7438
CNN	99.03

Table 3: comparing the precision for different recent methods.

Ref	Method	Precision %	F measure %
[29]	convolutional neural networks	94.89	
[30]	FASTER RCNN WITH ELA (Error Level Analysis)	90	
[31]	Combined features	81.82	87.83
[32]	A-KAZE and SURF Features	91.76	94.54
[11]	deep learning approach	95.38	96.75
[3]	Fourier-Mellin and scale-invariant feature transforms	94.12	96.97
[33]	owSURF	96	
[34]	Speeded-Up Robust Feature (SURF) and Binary Robust Invariant Scalable Keypoints (BRISK)	94.03	
[4]	Using various texture descriptors (LBP, LPQ, Binary Statistical Image Features, and Binary Gabor Pattern)	94.39	
[35]	SURF	93.3	90.3
[36]	Mirror-SIFT		89.4
[8]	deep neural network	78.22	75.98

4. Conclusion

In the current proposal, the presentation and explanation to image forgery are introduced, and we focused on copy-move image forgery detection. Many recent algorithms (published in 2017-2020) presented and compared. Most papers presented in the last years focused on using SIFT algorithm. Also, most algorithms detect the copy-move forgery when the copy region did not scale or rotate. Also, most of them did not study the effect of image illumination variation. Most of the best accuracy algorithms having a very complex procedure for detection forgery.

References

[1] Pooja Bhole, Dipak Wajgi, 2020, An Image Forgery Detection using SIFT-PCA, International Journal of Engineering Research & Technology.

[2] Akram Hatem Saber, Mohd Ayyub Khanl, Basim Galeb Mejbel, 2020, A Survey on Image Forgery Detection Using Different Forensic Approaches, Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 361-370 (2020).

[3] Kunj Bihari Meena and Vipin Tyagi, A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale-invariant feature Transforms, Multimedia Tools and Applications, 2020, DOI: https://doi.org/10.1007/s11042-019-08343-0.

[4] Divya S. Vidyadharan and Sabu M. Thampi, Digital image forgery detection using compact multi-texture representation, Journal of Intelligent & Fuzzy Systems 32 (2017) 3177–3188 DOI:10.3233/JIFS-169261.

[5] Bin Yang, Xingming Sun, Honglei Guo, Zhihua Xia, and Xianyi Chen, 2017, A copy-move forgery detection method based on CMFD-SIFT, Springer Science+Business Media New York 2017.

[6] Chun-Su Park, Joon Yeon Choeh, 2017, Fast and robust copy-move forgery detection based on scale-space representation, Springer Science+Business Media, LLC 2017.

[7] Mohamed Abdel-Basset, Gunasekaran Manogaran, Ahmed E. Fakhry, and Ibrahim El-Henawy, 2018, 2-Levels of clustering strategy to detect and locate copy-move forgery in the digital image, Springer Science+Business Media, LLC, part of Springer Nature 2018.

[8] Yue Wu, Wael Abd-Almageed, and Prem Natarajan, BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization, European Conference on Computer Vision, ECCV 2018: Computer Vision – ECCV 2018 pp 170-186.

[9] Chengyou Wang, Zhi Zhang, and Xiao Zhou, 2018, An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features, Symmetry 2018, 10, 706; DOI:10.3390/sym10120706.

[10] Toqeer Mahmooda, Zahid Mehmoodb, Mohsin Shahc, Tanzila Saba,2019, A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform, Journal of Visual Communication and Image Representation.

[11] Allu Venkateswara , Chanamallu Srinivasa , Dharma Raj Cheruku, An Innovative And Efficient Deep Learning Algorithm For Copy Move Forgery Detection In Digital Images, International Journal of Advanced Science and Technology Vol. 29, No. 05, (2020), pp. 10531 – 10542.

[12] Xinyi Wang, He Wang, Shaozhang Niu and Jiwei Zhang, 2019, Detection and localization of image forgeries using improved mask regional convolutional neural network, Mathematical Biosciences, and Engineering.

[13] N. Hema Rajini, 2019, Image Forgery Identification using Convolution Neural Network, International Journal of Recent Technology and Engineering.

[14] Payal Srivastava, Manoj Kumar, Vikas Deep, Purushottam Sharma, 2019, A Technique to Detect Copy-Move Forgery using Enhanced SURF, International Journal of Engineering and Advanced Technology.

[15] Hui-Yu Huang, Ai-Jhen Ciou, 2019, Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation, EURASIP Journal on Image and Video Processing.

[16] Jun Young Park, Tae An Kang, Yong Ho Moon, and Kyu Eom, 2020, Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram, Symmetry 2020, 12, 492; DOI:10.3390/sym12040492.

[17] Abdullah M. Moussa, 2020, KD-Tree Based Algorithm for Copy-Move Forgery Detection, International Journal of Scientific & Technology Research Volume 9, ISSUE 03, March 2020.

[18] A. Kashyap, R. S. Parmar, M. Agrawal, and H. Gupta, "An Evaluation of Digital Image Forgery Detection Approaches," arXiv preprint arXiv:1703.09968, 2017.

[19] N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on, 2017, pp. 1-7.

[20] T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, B. Manjunath, et al., "Boosting Image Forgery Detection using Resampling Detection and Copy-move analysis," arXiv preprint arXiv:1802.03154, 2018.

[21] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," IEEE Transactions on Information Forensics and Security, 2018.

[22] X. Lin, J.-H. Li, S.-L. Wang, F. Cheng, and X.-S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review," Engineering, 2018.

[23] Ankit Kumar Jaiswal and Rajeev Srivastava, "Image Splicing Detection using Deep Residual Network," 2nd International Conference on Advanced Computing and Software Engineering (ICACSE-2019).

[24] Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, andJianfeng Ma, "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering " Elsevier Information Sciences, 2019.

[25] Thuong Le-Tien, Hanh Phan-Xuan, Thuy Nguyen-Chinh, and Thien Do-Tieu, " Image Forgery Detection: A Low Computational-Cost and Effective Data-Driven Model " International Journal of Machine Learning and Computing, Vol. 9, No. 2, April 2019.

[26] Giulia Boato, Duc-Tien Dang-Nguyen, and Francesco G. B. Denatale, " Morphological Filter Detector for Image Forensics Applications" IEEE Access 2020.

[27] Yaqi Liu, and Xianfeng Zhao, "Constrained Image Splicing Detection and Localization With Attention-Aware Encoder-Decoder and Atrous Convolution" IEEE Access2020.

[28] Yuan Rao, Jiangqun Ni, and Huimin Zhao, "Deep Learning Local Descriptor for Image Splicing Detection and Localization" IEEE Access2020.

[29] Younis E. Abdalla, M. T. Iqbal, and M. Shehata, Image Forgery Detection Based on Deep Transfer Learning, EJECE, European Journal of Electrical and Computer Engineering Vol. 3, No. 5, September 2019, DOI: http://dx.doi.org/10.24018/ejece.2019.3.5.125.

[30] Robin Elizabeth Yancey, Norman Matloff, Paul Thompson, MULTI-STREAM FASTER RCNN WITH ELA FOR IMAGE TAMPERING DETECTION, arXiv:1904.08484v2 [cs.CV] 20 Jun 2019

[31] Lin, Cong, et al. "Copy-move forgery detection using combined features and transitive matching." Multimedia Tools and Applications 78.21 (2018): 30081-30096.

[32] Wang, Chengyou, Zhi Zhang, and Xiao Zhou. "An image copy-move forgery detection scheme based on akaze and surf features." Symmetry 10.12 (2018): 706.

[33] D. Mistry and A. Banerjee, "Comparison of Feature Detection and Matching Approach: SIFT and SURF," GRD Journals- Global Research and Development Journal for Engineering, vol. 2, no. 4, pp. 7-13, 2017.

[34] Soad Samir, Eid Emary, Khaled Elsayed, Hoda Onsi, Copy-Move Forgeries Detection and Localization Using Two Levels of Keypoints Extraction, Journal of Computer and Communications, Vol.7 No.9, September 2019, DOI: 10.4236/jcc.2019.79001.

[35] Zhang W, Yang Z, Niu S, Wang J. Detection of copy-move forgery in flat region based on feature enhancement. In: Shi Y, Kim H, Perez-Gonzalez F, Liu F, editors. Digital Forensics and Watermarking, IWDW 2016. Lecture Notes in Computer Science, vol 10082. Springer, Cham; 2017. 2017:159–171.

[36] Abdul Warif NB, Abdul Wahab AW, Idna Idris MY, Fazidah Othman RS. SIFT-Symmetry: A robust detection method for copy-move forgery with a reflection attack. J Vis Commun Image Represent, 2017;46:219–232.