Robust Image Forgery Detection Method Based on Transform Method and Clustering Algorithm

Sanjay Gupta

sanjgupta24@gmail.com

Department of computer Science & Engg.

Lecturer, Polytechnic College, Satna (M.P)

Abstract

Digital images are used in the present day for a variety of tasks and in a wide range of applications. They are crucial for the storing and transmission of visual information, particularly confidential visual information. It has become simple to alter and change the real content of the image as a result of the widespread use of digital photos, as well as the expansion of tools and software for editing them. This detecting method makes advantage of the image's texture property. The wavelet transform function is the most promising texture analysis feature and is utilised for image texture extraction. Clustering is a method used for feature creation and pattern selection. The process of clustering is an iterative unsupervised learning approach. Several genuine and fake photos are used to assess the proposed approaches. Our experimental findings show that the suggested strategies are extremely appealing. With copy-move alone, copy-move with rotation, scaling, and reflection, the forgery is accomplished. An image database made up of authentic and fake photos is also created throughout this procedure. The suggested approach achieves 100% accuracy in copy-move forgery alone (without any modification to the object's size or other attributes) forgery without post-processing and 98.43%, 86.58%, and 95.12% accuracy in copy-move forgery with rotation, scaling, and reflection, respectively.

Keyword's: - Image Forgery, Transform methods, Clustering Algorithm, DWT, MATLAB

Introduction

Image forgery detection is a new area of research in digital image forgery detection technique. In image forgery detection technique various algorithms are used such as statically method, transform based method and feature selection-based method. Now a day's used texture feature-based image forgery detection. The major issue in texture-based image forgery detection is measure the correlation of coefficient similarity. But, in today's digital age, it has become easy to change the information represented by an image without any visible traces. [1,2,3] But the truth is that with the simplicity of digital image manipulation provided by the development in computer technology, we have to be aware about what we are seeing[4,5,6,7]. Computer hardware and software (such as Adobe Photoshop, GNU Image Manipulation Program "GIMP") today offer the ability of digital image manipulation. The purpose of forgery and manipulation of digital images in many cases is to intentionally affect the awareness of the recipient. In other words, it means that the credibility of digital images is questioned and their content integrity can no longer be fully trusted. We believe that, recovering the community confidence toward digital image contents is very important. Active approach requires a special hardware implementation to mark the authenticity of the digital image such as including the digital signature in the image or encrypting the digital image. The water marking consists of hiding certain information in an image at the time of image acquisition and to check the authenticity of the image, embedded information is extracted from the image and verified with the original watermarks. Hence, this method relies on the source information beforehand. Second one is passive approach which does not require any prior information about the image and only depends on traces left on the image by different processing steps during image manipulation [8,9,10,11,12]. There are two methods of passive approach. First one is image source identification, which identifies the device used for the acquisition of the digital image. It tells that the image is computer generated or digital camera image. By using this method, the location of forgery in image cannot be determined. The approximate block matching techniques are usually based on the use of some intra component transformations, such as the discrete cosine transform (DCT) or the discrete wavelet transform (DWT) and some artificial intelligence (AI), or statistical techniques, such as the principal component analysis (PCA). Image splicing techniques significantly change the original image(s) and involve the composition of more than one image that are combined to generate a tampered image. If two images with different backgrounds are spliced, then it is relatively harder to make the boundaries imperceptible. Blind splicing detection is a challenging problem whereby the joining regions are investigated by a variety of methods. The presence of sharp edges (or changes) between different regions and their surroundings constitutes valuable clues to splicing in the image under investigation. Splicing detection methods can be roughly divided into two categories, namely region-based and boundary-based splicing detection. The boundary-based methods detect the irregular modifications at the splicing boundaries. An example is the passive method that relies on the sharp boundaries in color images. The rest of the paper describes, as in Section II, related work in image forgery detection, in Section III, the proposed methodology, in Section IV, the experimental analysis, and in Section V, conclusion and future work.

II. Related Work

Because so many picture blocks are employed in block-based approaches, they often have high processing costs and cannot handle geometric modifications. Contrarily, key point-based techniques can get over these two problems but struggle with smooth regions. The adaptive combination of the key point-based method and the block-based method is a unique fusion-based strategy for the detection of image fraud presented in this paper. Our system can automatically identify the right beginning region size for each image. Devanshi Chauhan and co-workers [2] Video forgeries of this nature are also practised. In this research, we review many key point-based copy-move forgery detection techniques with various parameters. Researchers will be able to better detect with the use of this survey's fresh insights and difficulties. We have found that some techniques, including scaling and rotating, are insensitive to geometric modification. Some techniques that are accurate but take a lot of work to do have also been talked about. Ardizzone and others ([3] In contrast to blocks or single points, the hybrid approach we offer in this research compares triangles. Objects are modelled as a set of connected triangles based upon interest points that are retrieved from the image. They work better in complicated situations, but they often find a lot of false matches in pictures with simple backgrounds. Tu Huynh-Kha and others [4]. The article offers a novel technique for identifying forgeries in an image caused by copy-move, splicing, or both. To determine whether the image contains any counterfeit, multi-state is used, which reduces the computing complexity. By figuring out the size of suspicious parts with blob detection, forgeries of copy-move, splicing, or both can be found by looking for places with similar RDM. In the work of Sunil Kumar and others [5], the detection of copy move fraud in the presence of contrast changes is proposed using a unique technique based on binary discrete cosine transform vectors. DCT coefficients are computed for the overlapping blocks of the image after it has been separated into blocks. The approach is based on binary DCT coefficients. With a high detection efficiency and a shift in contrast, the forged regions in the dataset's photos were found. Rajeev Kaushik and colleagues [6]In the current communication, we provide a novel method that makes use of statistical moments and a two-dimensional discrete cosine transform to identify copy-move forgery in digital photos. We slide a window around each suspicious pixel of the image first, then each window. We utilised the radix sort, which has a high computational cost, to organise the feature matrix. The most well-known data clustering algorithm, c-mean, can lower the computing cost of this sorting method. In this study, Toqeer Mahmood et al. [7] suggested a passive method for identifying the CMF in visual content. In order to locate and identify the forged areas, it decomposes an image using a discrete wavelet transform and extracts Hu moments as feature vectors from a circle block. Other approaches are contrasted with the suggested technique. The suggested procedure provides a higher accuracy ratio than other approaches. Thus, according to Gurmeet Kaur Saini et al. [8], digital images and videos serve as the primary information sources in the current digital age. However, these information carriers are easily modifiable with the aid of programmes like Adobe Photoshop, GIMP, etc. Both types of photos—bright coloured images and low-brightness images—perform well when using the hybrid approach that has been developed. Rahul Dixit and others (9) in this study. We offer a region-duplication detection method that operates by means of the Undecorated Dyadic Wavelet Transform. To detect matches between various picture blocks, the suggested method divides an image into pixel sub-matrices or blocks. The detection accuracy and false positive rate of the suggested technique have been improved. According to Khaled W. Mahmoud et al. [10], an overview of moments is provided in this work, along with an analysis and illustration of moment-based detection techniques. The robustness of these procedures against any attacks that might be used to trick the detection system is what matters most. The majority of approaches in use today have had mixed results. Sunil Kumar and others. [11] In terms of detection time, the suggested method has outperformed the current forgery detection method utilising SURF substantially. It is also invariant to post-processing procedures like rotation and scaling. The threshold for the matching procedure is manually defined based on the texture of the input image and the size of the duplicated area. There is, therefore, more room to automatically create the threshold. The number of outliers likewise rises with large rotation and scaling levels. Elif Baykal and others [12]: in this method, picture key points are first retrieved, and for each key point, a 128-dimensional feature vector called a SIFT descriptor is created. Following that, the descriptors of these key points are matched using Euclidean distance. To reduce the temporal complexity of clustering SIFT key points in this work, we adopted the k-means++ approach. According to experimental findings, the proposed technique significantly shortens execution time while maintaining accuracy ratios. As in [7], our technique also detects rotation and multiple copy move attacks. Among others, Musaed Alhussein [13], the method for detecting picture tampering suggested in this paper uses an extreme learning machine and a local texture descriptor (ELM). Both copy-move forgeries and picture splicing are examples of image tampering. On the CASIA datasets, the suggested strategy was assessed and contrasted with two other relevant approaches. The suggested approach had an accuracy rate of 95.67% in the CASIA v1.0 database and 97.3% in the CASIA v2.0 database. These accuracy levels are the best that these two databases have seen. Bihan Wen and others [14] a brand-new sparsely-based metric for accurately determining fake quality is also something we suggest. According to experimental findings, (a) common forgery detection techniques perform poorly over coverage, and (b) the suggested sparsely-based measure most closely resembles human detection abilities. The aim of this work is to distinguish the forged region from SGOs using COVERAGE, a novel CMFD database with annotations. In addition to CV and VP-based CMFD performance, there are a number of other ways to measure the quality of a forgery. [15] Ye Zhu and his associates Existing Copy-Move Forgery Detection (CMFD) techniques that match the key points/blocks based just on pair similarity in the scene are put to the test by this. In this research, an effective method named SHFD was put out and compared to two cutting-edge techniques. According to the findings, only SHFD was able to identify photos that had SGO and copy-move forgeries. Additionally, it chooses the geometric adjustments and post-processing carried out on the forged sections. [16] Neetu Yadav and colleagues Even though picture editing and augmentation are commonplace, when they tend to alter the image's meaning, they are referred to as attempts at digital image fabrication. Copy move forgery (CMF) is a straightforward technique that is supported by a variety of well-designed capabilities in image-editing software. The proposed method can demonstrate efficacy in detecting copy-move forged regions in the image when used to combine RST alterations. By applying the image segmentation method, the cluster formation period has been prolonged. Anuja Dixit and colleagues [17]In this fake, an image piece is duplicated and then placed over the original image in a different place. Although academics have suggested a number of ways, it might be challenging to spot forged portions that are diverse in size and situated throughout an image. To address these issues, we introduced that the effectiveness of the suggested strategy has been evaluated in terms of false match rate and detection accuracy. It is found that the suggested algorithm is very good at finding forgeries, even when the block size is small. All in all, Khaled Mahmoud [18] This study examines the effectiveness and capability of employing pseudo-Zernike moments (PZM) and Zernike moments (ZM) to identify this kind of fraud. An extensive and realworld dataset is tested in order to gauge how well various strategies perform. The images that were tested cover all possible situations, such as copying an object more than once, copying several objects, and changing the duplicated objects in different ways, such as by scaling, rotating, blurring, adding noise, etc. A year old, others include YoungJin Go. [19] The dispersed remote car diagnostic system that was created in this study would gather and analyse analogue, B-CAN, and CCAN signals. Additionally, this study guaranteed the accuracy of vehicle data with performance that differed from that of standard equipment through synchronisation with CAN communication and analogue signal. It can be seen that forward error correction codes are methods that operate effectively over the AGWN channel. Digital wireless communication systems often use convolution code to find problems with the signal and fix them. [20] This study by Elham Mohebbian and others develops a DCT-based technique to identify fake images. Taking the input image's complexity into account, for the purpose of duplicate region detection, smooth and complicated images are separated into two groups. No matter how complicated the image is, our technique has shown to be more effective than other methods at finding fake images, whether they are smooth or complicated. In this study, we propose a local phase quantization (LPQ) texture operator and an entropy filter-based passive picture forgery detection approach. The entropy filter draws attention to the haphazard variations in the images that aid in identifying forged parts. When classifying forged and no forged images, the LPQ operator offers information on the internal statistics of this entropy filtered image. Our technology successfully detects both copy-move and spliced images as forms of counterfeit imagery. Among others, Rajeev Rajkumar [22] notes that these methods typically employ two strategies: block-based and key-point-based. This paper reviews several strategies for copy mark forgery detection. The crucial stages a copy move forgery detection system takes are its two distinct methods—point-based and block-based approaches—are also explored. This field of study is currently active, and it has a wide range of applications. The project's output is the ability to distinguish genuine photographs from stolen ones. Among others, Beste Ustubioglu [23] improved the effectiveness of the key point extraction techniques. The method uses the LPQ (Local Phase Quantization) operator to extract the structural texture information from the test image. In this work, SIFT is used to extract the key points from the texture image. Key point-based approaches are unable to identify forgeries on smooth sections since they rely on structural information like picture texture. The suggested method uses LPQ before SIFT to focus on texture information and is based on key point selection.

III. Proposed Methodology

The extracted partial feature passes through glow-worm algorithm. the partial feature map into glow-worm search space. Each glow-worm i encode the object function value J(xi(t)) at its current location xi(t) into α luciferin value li and broadcasts the same within it neighbourhood. The set of neighbour (Ni(t)) of glow-worm i consist of those glow-worm that have relatively higher luciferin value that are located within a dynamic decision domain and updating by formula 1 at each iteration [11].

Local decision range update is given by equation 1

$$r_d^i(t+1) = min\left\{rs, max\left\{0, r_d^i(t) + \beta(nt - |Ni(t)|)\right\}\right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

And $r_d^i(t+1)$ is glowworm is local decision range at the t+1 iteration, rs is the sensor range, nt is the neighborhood range. The number of glow in local decision range is given by equation (2)

$$N_{i(t)=\left\{j:\|xi(t)-xi(t)\|<r_d^i;li(t)<li(t)\right\}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

And xi(t) is the glow-worm I position at the t iteration(t) is the glow-worm i luciferin at the t iteration the set of neighbour of glow-worm i consist of those glow-worm that have relatively higher luciferin value and that are located within dynamic decision domain whose range r_d^i is bounded above by a circular sensor range.

Each glow-worm is given in equation (3)

$$p_{ij(t)=\frac{l_{i(t)-l_{i(t)}}}{\sum_{k\in Ni(t)} lk(t)-li(t)}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Movement update is given in equation (4)

$$x_{i(t+1)=xi(t)+s\left(\frac{sj(t)-xi(t)}{\|xj(t)-xi(t)\|}\right)} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Luciferin update is given in equation (5)

$$l_{i(t)=(1-\rho)li(t-1)+\gamma j(xi(t))} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

And li(t) is a luciferin value of glow-worm i at the t iteration, P belong (0,1) lead to the reflection of the cumulative kindness of the path followed by the glow-worm in their current luciferin values the parameter Y only scale the function values, J(xi(t)) is the value of test function. Finally gets the optimal feature. The optimal feature passes through matching of original image.

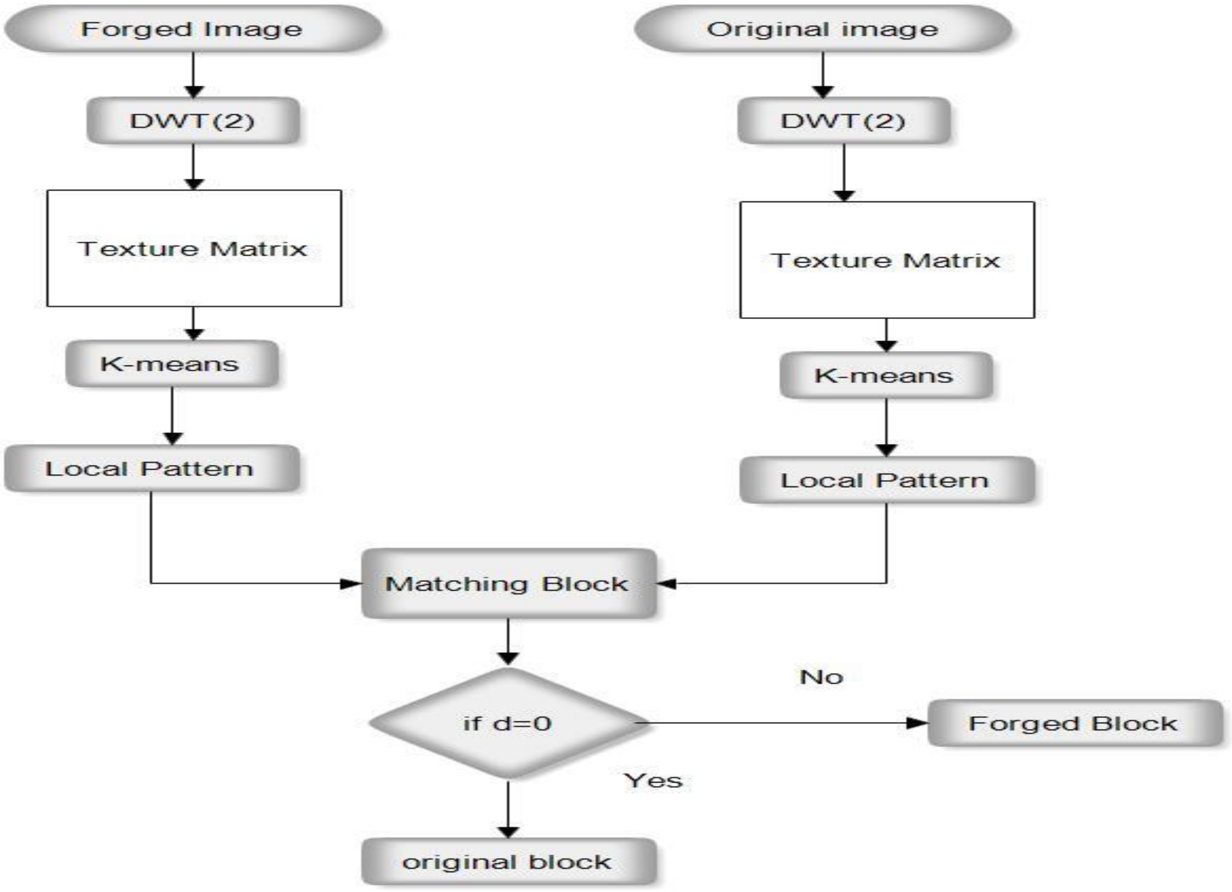

Figure 1 proposed model for image forged image

IV. Experimental Analysis

To validate the proposed algorithm for forgery detection performance has been evaluated and compared with existing DWT [23] and DCT [22]. The processing of forged database images is trained and then tested. In training process, 250 authentic images and 250 forged images are used for proposed model and the images are selected as randomly. In testing, the whole 500 images are divided into 5 sets of images and each set consists of 100 images. Each and every set is trained and tested. The performance is evaluated in terms of False negative and false positive. The all-simulation process done in MATLAB environments with windows operating system and I7 processors.

Table:1 Shows that the performance evaluation using DCT, DWT and proposed methods.

Types of Images	Method Name	FN	FP
DataSet-1	DCT	38.56	53.47
	DWT	26.58	49.32
	PROPOSED	23.46	35.24
DataSet-2	DCT	21.54	33.56
	DWT	15.64	31.89
	PROPOSED	13.96	27.32
DataSet-3	DCT	25.65	41.25
	DWT	21.87	36.78
	PROPOSED	18.32	25.64

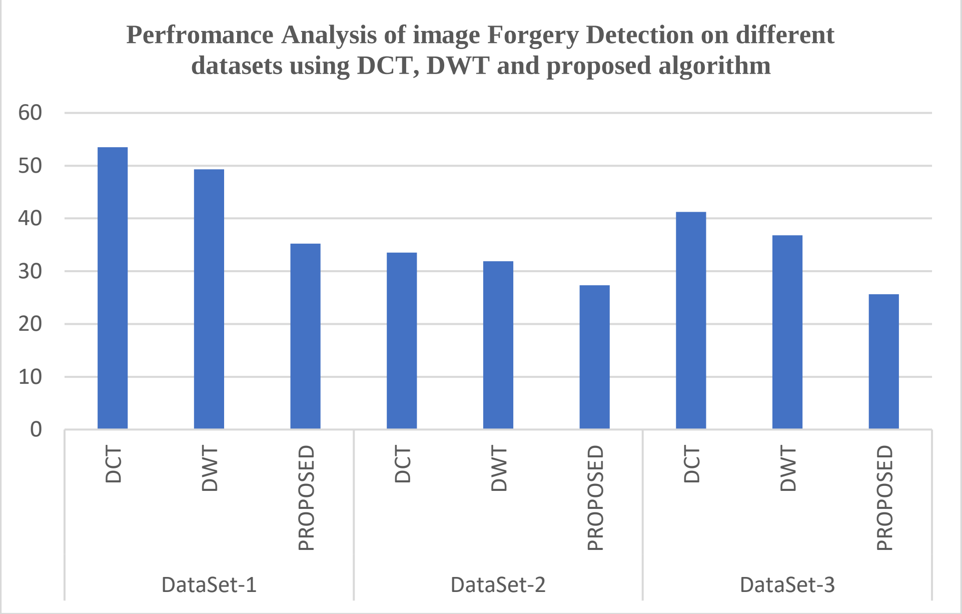

Figure:3 Shows that the comparative performance evaluation of FN with using DCT, DWT and Proposed methods with using DataSet-1, DataSet-2, DataSet-3.

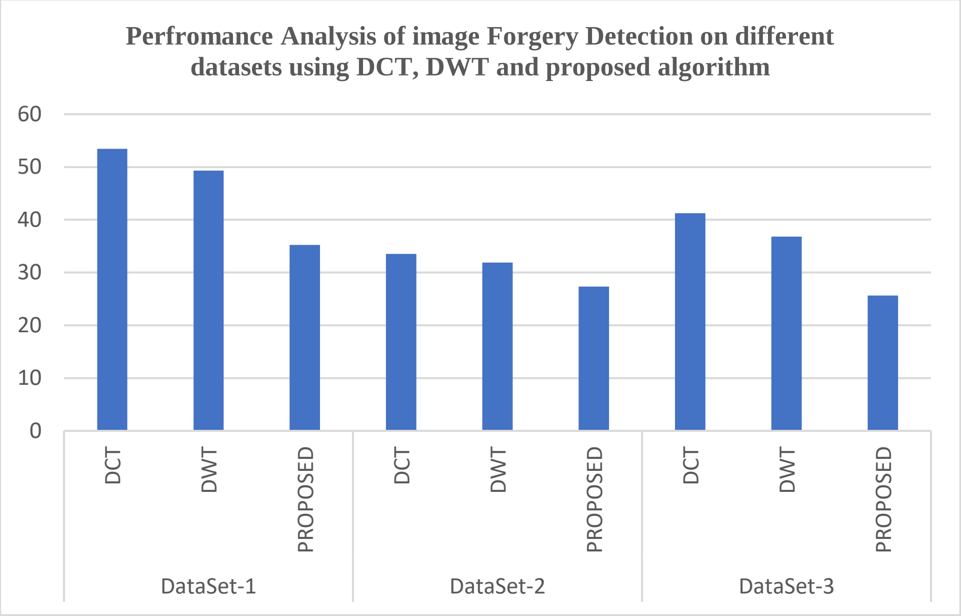

Figure 4 Shows that the comparative performance evaluation of FP with using DCT, DWT and Proposed methods with using DataSet-1, DataSet-2, DataSet-3.

V. Conclusion & Future Work

The proposed image forgery used wavelet transform function for the extraction of feature of original and forged image. The extracted feature passes through glow-worm optimization technique for the generation of local pattern. The local pattern passes though matching block and measure distance of two similar and dissimilar blocks. The proposed image forged detection technique is very efficient in compression of local pattern and transform function-based technique. The proposed methods are evaluated on many original and forged images. According to our experimental results the proposed methods are quite attractive. The forgery is done with just copy-move, copy-move with rotation, with scaling, and reflection. In this process, an image database that consists of original and forged images is also developed. The proposed method achieves 100% accuracy in just copy-move forgery (without any change in the size or characteristics of the object) forgery without post-processing and 97.43%, 66.58%, and 99.12% accuracies in copy-move forgery with rotation, scaling, and reflection, respectively. Also, to ensure more efficiency, we have added some random noise on the images, the detection accuracy achieved 98.23%. While the proposed method performs well even with additive white Gaussian noise post-processing

Reference

[1] Zheng, Jiangbin, Yanan Liu, Jinchang Ren, Tingge Zhu, Yijun Yan, and Heng Yang. "Fusion of block and keypoints based approaches for effective copy-move image forgery detection." Multidimensional Systems and Signal Processing 27, no. 4 (2016): 989-1005.

[2] Chauhan, Devanshi, Dipali Kasat, Sanjeev Jain, and Vilas Thakare. "Survey on keypoint based copy-move forgery detection methods on image." Procedia Computer Science 85 (2016): 206-212.

[3] Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. "Copy–move forgery detection by matching triangles of keypoints." IEEE Transactions on Information Forensics and Security 10, no. 10 (2015): 2084-2094.

[4] Huynh-Kha, Tu, Thuong Le-Tien, Synh Ha-Viet-Uyen, Khoa Huynh-Van, and Marie Luong. "A robust algorithm of forgery detection in copy-move and spliced images." International Journal of Advanced Computer Science and Applications 7, no. 3 (2016).

[5] Kumar, Sunil, J. V. Desai, and Shaktidev Mukherjee. "Copy move forgery detection in contrast variant environment using binary DCT vectors." International Journal of Image, Graphics and Signal Processing 7, no. 6 (2015): 38.

[6] Kaushik, Rajeev, Rakesh Kumar Bajaj, and Jimson Mathew. "On image forgery detection using two dimensional discrete cosine transform and statistical moments." Procedia Computer Science 70 (2015): 130-136.

[7] Mahmood, Toqeer, Tabassam Nawaz, Mohsin Shah, Zakir Khan, Rehan Ashraf, and Hafiz Adnan Habib. "Copy-move forgery detection technique based on DWT and Hu Moments." International Journal of Computer Science and Information Security (IJCSIS) 14, no. 5 (2016).

[8] Ooi, Shih Yin, Andrew Beng Jin Teoh, Ying Han Pang, and Bee Yan Hiew. "Image-based handwritten signature verification using hybrid methods of discrete radon transform, principal component analysis and probabilistic neural network." Applied Soft Computing 40 (2016): 274-282.

[9] Dixit, Rahul, and Ruchira Naskar. "DyWT based copy-move forgery detection with improved detection accuracy." In 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 133-138. IEEE, 2016.

[10] Mahmoud, K., and Arwa Husien Abu Al-Rukab. "Moment based copy move forgery detection methods." Int J Comput Sci Inf Secur (IJCSIS) 14, no. 7 (2016).

[11] Kumar, Sunil, J. V. Desai, and Shaktidev Mukherjee. "A fast keypoint based hybrid method for copy move forgery detection." arXiv preprint arXiv:1612.03989 (2016).

[12] Baykal, Elif, Beste Ustubioglu, and Guzin Ulutas. "Image forgery detection based on SIFT and k-means++." In 2016 39th international conference on telecommunications and signal processing (TSP), pp. 474-477. IEEE, 2016.

[13] Alhussein, Musaed. "Image tampering detection based on local texture descriptor and extreme learning machine." In 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim), pp. 196-199. IEEE, 2016.

[14] Wen, Bihan, Ye Zhu, Ramanathan Subramanian, Tian-Tsong Ng, Xuanjing Shen, and Stefan Winkler. "COVERAGE—A novel database for copy-move forgery detection." In 2016 IEEE international conference on image processing (ICIP), pp. 161-165. IEEE, 2016.

[15] Zhu, Ye, Tian-Tsong Ng, Xuanjing Shen, and Bihan Wen. "Revisiting copy-move forgery detection by considering realistic image with similar but genuine objects." arXiv preprint arXiv:1601.07262 (2016).

[16] Abd Warif, Nor Bakiah, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, and Kim-Kwang Raymond Choo. "Copy-move forgery detection: survey, challenges and future directions." Journal of Network and Computer Applications 75 (2016): 259-278.

[17] Dixit, Anuja, Rahul Dixit, and R. K. Gupta. "Detection of copy-move forgery exploiting LBP features with discrete wavelet transform." International Journal of Computer Applications 153, no. 3 (2016): 0975-0987.

[18] Mahmoud, Khaled, and Arwa Husien. "Copy-move forgery detection using zernike and pseudo zernike moments." Int. Arab J. Inf. Technol. 13, no. 6A (2016): 930-937.

[19] Das, Bikramaditya, Bidyadhar Subudhi, and Bibhuti Bhusan Pati. "Cooperative formation control of autonomous underwater vehicles: An overview." International Journal of Automation and computing 13, no. 3 (2016): 199-225.

[20] Mohebbian, Elham, and Mahdi Hariri. "Increase the efficiency of DCT method for detection of copy-move forgery in complex and smooth images." In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 436-440. IEEE, 2015.

[21] Agarwal, Saurabh, and Satish Chand. "Image forgery detection using multi scale entropy filter and local phase quantization." International journal of image, graphics and signal processing 7, no. 10 (2015): 78.

[22] Rajkumar, Rajeev, Thounaojam Angaleima Chanu, and Ningthoujam Nejit Singh. "Copy move Forgery Detection Approaches: A Survey." ADBU Journal of Engineering Technology 3 (2015).

[23] Ustubioglu, Beste, Gul Muzaffer, Guzin Ulutas, Vasif Nabiyev, and Mustafa Ulutas. "A novel keypoint based forgery detection method based on local phase quantization and SIFT." In 2015 9th International Conference on Electrical and Electronics Engineering (ELECO), pp. 185-189. IEEE, 2015.