Detection of tampered images via stationary wavelet transform and principal component analysis

Vaishali Sharma, Amit Garg

Abstract— **Copy move (CM) is a common type of forgery which creates tampered image by covering some important part of the image by replacing it with some other part of the same image. Therefore, forgery detection techniques are required to identify tampered areas. In this paper, a copy-move forgery detection (CMFD) method is presented by utilizing Stationary Wavelet transform (SWT) for decomposing the image. After decomposition, approximation band is further subdivided into overlapping blocks and then features are extracted by using principal component analysis (PCA) for each block. In order to match the similar block pairs and identify areas that are likely to be tampered, euclidean distance is used to compute the block distance between the adjacent pair of blocks. To evaluate the performance of the proposed work uncompressed color image dataset (UCID) is used. The quantitative results have been discussed in terms of parameters true positive rate (TPR), false positive rate (FPR) and accuracy and also compared with other existing methods. For qualitative analysis detected images obtained from the proposed method is presented. From the results obtained it can be seen that the proposed method performs better in terms of all parameters as compare to existing methods.**

Index Terms— Authentication, Copy move forgery detection, Image Forensic, Tampered images.

1) INTRODUCTION

In today's world, tampering of digital images is very easy due to availability of free and accessible image manipulation software. The tampered images can be used as a misleading tool for concealing the real facts [1]. This exhibits that image forgery is a serious threat; therefore it has become a key concern for the researchers of this field to develop methods for the detection of tampered images. Initially, the research community classified the tampering detection techniques in Active and Passive techniques.

In "Active" technique the detection takes place at the source side that is within the camera. The camera embedded by a digital watermark or a digital signature chip. Any manipulation made on image can be detected by checking that watermark or signature [2]. This technique requires specialized hardware and software for processing the image. These obstacles of active techniques give rise to the passive technique.

In "passive" techniques there is no watermark or signature required for forgery detection. It works in absence of any embedded data. The researchers describe different kinds of tampering that comes under passive technique such as image splicing, image retouching, image cloning and copy move forgery (CMF) [3]. CMF is one of the mostly investigated topics in research area of Image Forensic.

In CMF, a part of image is copied and pasted into the same image in order to hide some useful information from the image. This type of forgery is quite difficult to detect because in this case the texture, background and lightening conditions of the original image and tampered image remains the same [4]. CMF passive techniques are further classified as block based method and key point based method. For feature extraction, block based method subdivide the image into rectangular regions. For each such region, a feature vector is computed and similar features vector are subsequently matched. On contrary, key point based method computes their features only on image regions with high entropy, without any subdivision of image regions. Similar feature vectors within the image are then matched [5]. Out of these two, block based method is widely used for copy move forgery detection (CMFD).

Over the past years, various methods have been carried out for the detection of block based CMF. One such method is given by Popescu et.al [6] in which firstly principal component analysis (PCA) is applied to the overlapping blocks of input image for extracting the features and then duplicated regions are detected by sorting the features lexicographically. Another method is presented by Mahmood et.al [7] in which Discrete cosine transform (DCT) is applied to the overlapping blocks of input image and DCT coefficients are calculated, afterward

Manuscript received April, 2019.

***First Author name**, Vaishali Sharma, Dr APJ Abdul Kalam technical university/ Ajay Kumar Garg Engineering College/ Department of Electronics and Communication Engineering.*

***Second Author name**, Amit Garg ,Dr APJ Abdul Kalam technical University/ Ajay Kumar Garg Engineering College/ Department of Electronics and Communication Engineering.*

Kernel principal component analysis (KPCA) is used for extracting the feature values and lexicographically sorting is performed. Again a method is given by Mahmood et.al [8] in which authors utilizes stationary wavelet transform (SWT) for decomposing the image in four frequency sub-bands. Features are extracted by DCT and sorted lexicographically; thereafter euclidean distance is used for matching the similar block pairs. Another method is given by Dixit et.al [9] in which authors utilizes SWT for decomposing the image and divide the image into overlapping blocks. In second phase singular value decomposition (SVD) is used for extracting the feature values. Sorting method used in this paper is lexicographical and blocks are matched by shift vector calculation. The main drawback with all these methods is their highly computational time due to large dimension of feature matrix and overlapping block size. Thus methods with reduced dimension of feature vectors are computationally proficient as compared with the methods having larger dimension of feature vectors.

This paper presents a method for copy move forgery detection (CMFD) in which stationary wavelet transform (SWT) is used for decomposing the image in frequency sub-bands named as approximation sub-band, horizontal sub-band, vertical sub-band and diagonal sub-band. Approximation band is further subdivided into overlapping blocks, and then features are extracted by using principal component analysis (PCA) for each block. Thereafter, obtained features using PCA are sorted lexicographically that resulting all feature vectors of similar blocks close to each other. In order to match the similar block pairs and identify areas that are likely to be tampered, euclidean distance is used to compute the block distance between the adjacent pair of blocks.

The rest of the paper is summarised as follows: Section 2 describes Stationary wavelet transform; Section 3 presents proposed method including features extraction, matching and sorting. In Section 4 results has been discussed and finally in section 5 paper is concluded.

2) STATIONARY WAVELET TRANSFORM

For the detection of CMF existing techniques utilized. Discrete Wavelet transform (DWT) that intrinsically shows lack of invariance property and unimpressive results for signal analysis application such as edge detection, denoising and texture analysis because it undergoes pseudo Gibbs phenomenon [10] therefore SWT is preferred over DWT. In SWT, the input image is convolved with the low pass l[m] and high pass h[m] filters to obtain the wavelet coefficients [11]. In SWT the input image of size P×Q is decomposed into four equal sub bands named as approximation denoted by LL, vertical denoted by LH, horizontal denoted by HL and diagonal denoted by HH sub-bands which can be expressed by Eqn. (1), (2), (3) and (4).

$$LL_{i+1}= \sum_{x=-\infty}^{+\infty} \sum_{y=+\infty}^{+\infty} l_x^i \; l_y^i \; LL_i \tag{1}$$

$$LH_{i+1}= \sum_{x=-\infty}^{+\infty} \sum_{y=+\infty}^{+\infty} l_x^i \; h_y^i \; LL_i \tag{2}$$

$$HL_{i+1}= \sum_{x=-\infty}^{+\infty} \sum_{y=+\infty}^{+\infty} h_x^i \; l_y^i \; LL_i \tag{3}$$

$$HH_{i+1}= \sum_{x=-\infty}^{+\infty} \sum_{y=+\infty}^{+\infty} h_x^i \; h_y^i \; LL_i \tag{4}$$

The first level decomposition of 2D image S_i of size P×Q is shown in Fig. 1.

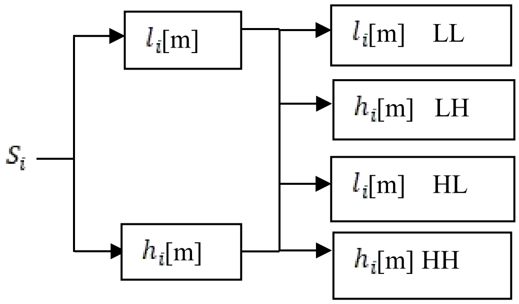


Fig.1. Decomposition of image into four equal sub-bands.

3) PROPOSED WORK

Here a method is presented for the detection of CMF by utilizing SWT and PCA. In this method the input image is decomposed into four equal sub-bands using SWT as discussed in Section 2. Further approximation band is taking as an input because it contains most of the information about the image. Secondly, features of approximation band are calculated by using PCA.

The reason behind using PCA lies in the fact that it condense the dimension of the image to characterize the information in such a form that enhance the mutual independence of components of image [12].Therefore a combination of SWT and PCA is proposed that will represent the features in more reduced form and will appears as a good option for CMFD.

The flow chart of the proposed work for CMFD is shown in Fig. 2. The steps to be followed for the CMF detection are summarized in subsequent sub-sections.

(A) Pre-Processing

The RGB image is taken as an input and then converted into a gray scale image by using the standard formula given in Eqn. (5).

$$I = 0.299R + 0.587G + 0.114B \tag{5}$$

Where R, G and B are three input channel of red, green and blue and I is the obtained gray image [13]. Thereafter SWT is applied to the gray scale image and four frequency sub-bands are obtained as LL, LH, HL and HH. The LL sub-band is used for further operation and divided into the overlapping blocks by using a sliding window of size p×q = 4×4 and is stored in new matrix T_b given in Eqn. (6)

$$T_b = (P - p + 1) \times (Q - q + 1) \qquad (6)$$

Where P and Q indicates total number of rows and column of LL band and p = 4 and q= 4.

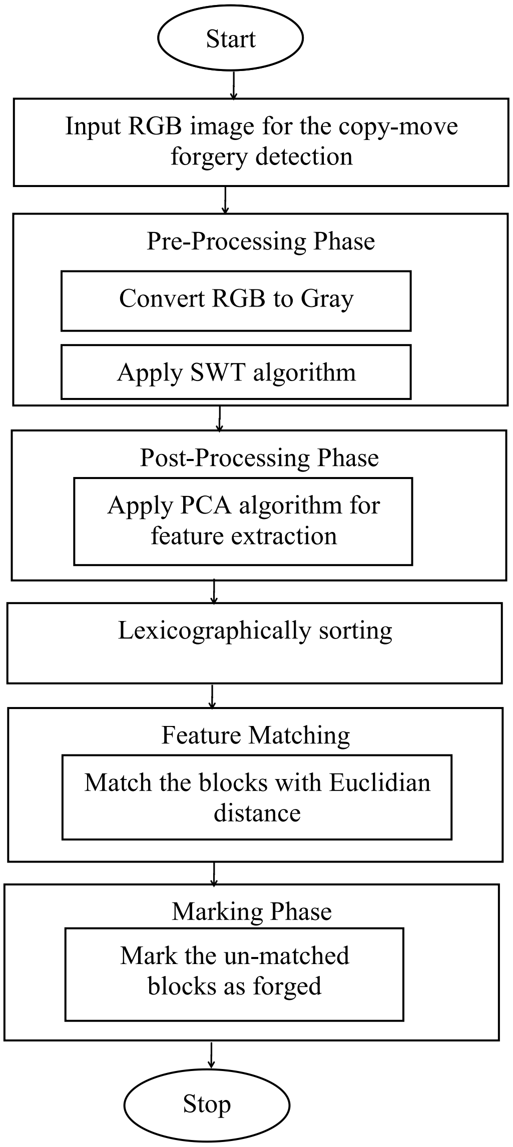

Start
Input RGB image for the copy-move forgery detection
Pre-Processing Phase
Convert RGB to Gray
Apply SWT algorithm
Post-Processing Phase
Apply PCA algorithm for feature extraction
Lexicographically sorting
Feature Matching
Match the blocks with Euclidian distance
Marking Phase
Mark the un-matched blocks as forged
Stop

Fig.2. Flow chart of proposed work

(B) Feature Extraction

For block based CMFD methods, the computational complexity is a major concern which is directly related to feature dimensions [14] and overlapping blocks of image. Applying the lexicographical sorting in high dimensional feature causes complexity [15]. Therefore a reduced dimension for feature vector is obtained by applying 4×4 blocks PCA. The block size used for this work is of 4×4 that will reduce the dimension of feature vector and decrease the computational time for extracting the features.

(C) Formation of feature matrix

A feature matrix f_m of size T_b×4 is formed by placing the entire feature vector corresponding to each B_p extracted using PCA as in Eqn. (7).

$$f_m = [f_{1,z}, f_{2,z} \cdots\cdots f_{Tb,z}] \qquad (7)$$

Where z= 1, 2.....4.

The feature matrix f_m is lexicographically sorted from top left corner of each B_p before performing the procedure for matching the block pairs [16]. The feature matrix f_m after lexicographical sorting is represented as f_s.

(D) Matching of similar blocks pairs

Since forged areas are supposed to be non-intersecting, and the image blocks in this approach are overlapping, therefore to meet the requirement of CMFD the following two constraints are used:

1. Block distance threshold

Block distance threshold is used to match the identical blocks that are supposed to be forged. Using the matrix f_s obtained after lexicographical sorting the proposed CMFD method computes block distance between the adjacent pair of blocks as defined in Eqn. (8).

$$\Omega = \sqrt{\sum_{i=1}^{i=\infty}(f_i^l - f_j^l)^2} \qquad (8)$$

If the block distance exceeds the pre-defined block distance threshold (b_{th}) then the CMFD method will compute the block similarity threshold between the pairs of block.

2. Block similarity threshold

If the pair of blocks holds the criterion that is mentioned in Eqn.(8), then the method will further finds the similarity between the feature vectors of corresponding blocks as formulated in Eqn. (9).

$$f_{si}= [f_i^1, f_i^2, f_i^3, f_i^4] \tag{9}$$

$$f_{sj}= [f_j^1, f_j^2, f_j^3, f_j^4] \tag{10}$$

$$\Omega=\sqrt{\sum_{i=1}^{i=4}(f_i^l - f_j^l)^2} \tag{11}$$

If the distance of similarity is lesser than the pre-determined threshold of similarity (s_{th}), after that the block of pair is considered as candidate of forgery. And this process of feature matching and filtering is repeated for all the feature vectors f_m related to each B_p, the proposed method will determine whether the image blocks are tampered and then stored all the filtered pair in a set Ω.

4) EXPERIMENTAL RESULTS

To evaluate the performance of this work a uncompressed color image database UCID [17] is used. UCID contains 1338 original and tampered test images. Three images of bear, statue and pigeon are acquired from UCID dataset is used with proposed CMFD algorithm. Quantitative and qualitative results are presented for the proposed CMFD technique. For quantitative analysis parameters True Positive Rate (TPR), False Positive Rate (FPR) and Accuracy are used and compared with existing methods given in [6-9]. For qualitative analysis forged images and detected images are presented for the proposed method. All the experiments are performed over Matlab 2014b.

(A) Simulation Parameters

Here input parameter values are set as block size (b) =4, number of neighboring feature to compare (N_r) =5, block distance threshold (b_{th}) =26 for PCA and block similarity threshold (s_{th})=26.

(B) Quantitative Performance Evaluation

The Quantitative parameters on which the performance of the CMFD method is evaluated are discussed below:

1. *True Positive Rate* - True positive rate (TPR) measures the proportion of actual positives that are correctly identified. TPR is calculated by using Eqn. (12).

$$\text{TPR} = \frac{TP}{TP+FN} \tag{12}$$

2. *False Positive Rate* - False positive rate (FPR) measures the proportion of actual negatives that are correctly identified. FPR is given by using Eqn. (13).

$$\text{FPR} = \frac{FP}{TN+FP} \tag{13}$$

3. *Accuracy* - When the image is detected as a forged image by using some algorithm then its accuracy can be measure by using Eqn. (14)

$$\text{Accuracy} = \frac{TP+TN}{TN+FP+TP+FN} \tag{14}$$

Where T_p denotes the number of images that are detected as forged, T_n denotes the authentic image which are detected as authentic, F_P denotes the number of image which are authentic but detected as forged and F_n denote the forged image detected as authentic. For the effective and better performance of an algorithm, value of TPR must be equal to 1, value of FPR must be near to 0 and Accuracy should be maintain near to 100.

Table I shows quantitative performance comparison of three images of bear, statue, and pigeon taken from UCID database for quantitative analysis which is based on parameters TPR, FPR, and Accuracy. All these images are tested with existing methods mentioned in [6-9] and with proposed method. Results shows that with proposed method the value of TPR for bear image is 0.996 which is more close to 1, value of FPR is 0.011 which is more close to 0, and accuracy is 99.40 which is more close to 100 as compared with other methods. Secondly for statue image the value of TPR with proposed method is 0.990 which is nearly equals to 1, value of FPR is 0.015 which is nearly equals to 0, and accuracy is 98.80 which is nearly equals to 100 as compared with other methods. And finally for third image that is for pigeon image the value for TPR with proposed method is 0.993 which is very much close to 1, value for FPR is 0.013 which is very much close to 0, and accuracy is 99.11 which is very much close to 100 as compared with other methods. All these results show that proposed method outperforms better in terms of all parameters as compared with other existing methods by providing more desirable results.

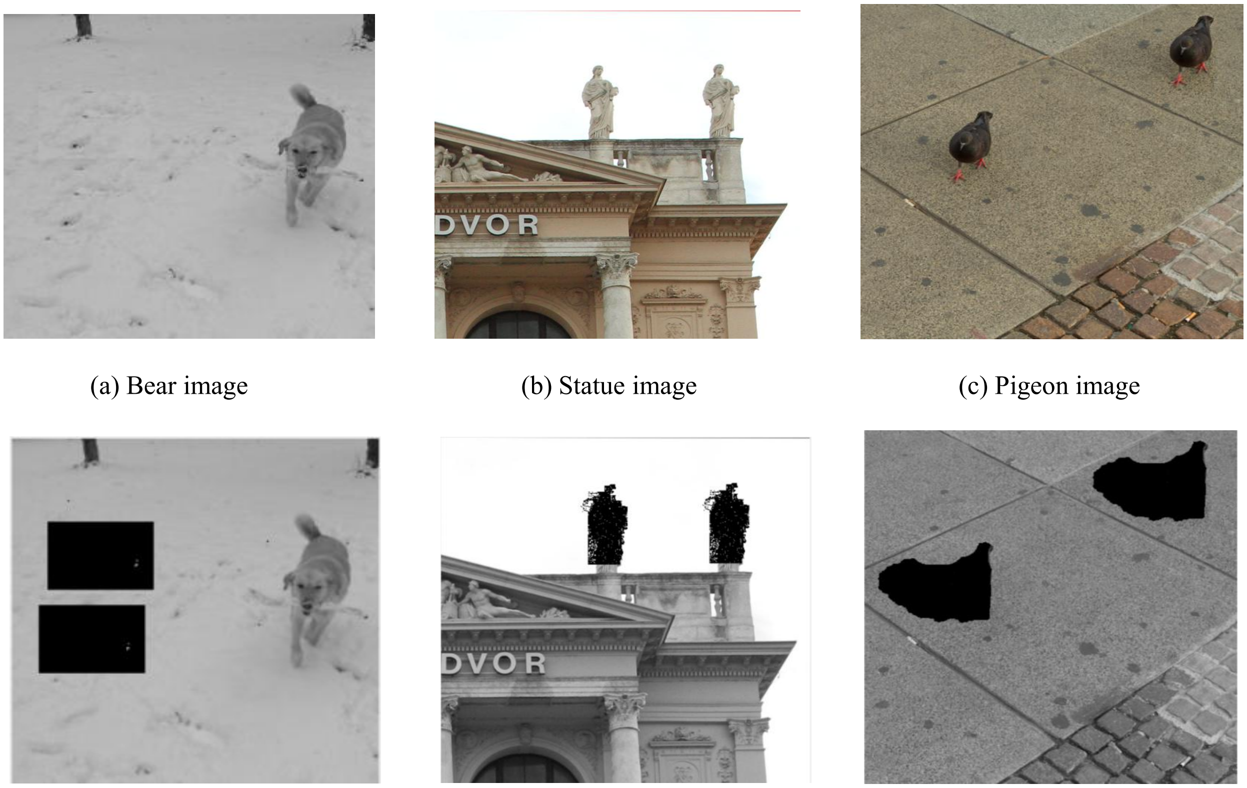
(C) Qualitative analysis

Qualitative analysis shows visual results after applying the algorithm. Fig. 3 shows the qualitative results of the proposed method, in which Fig. 3 (a) shows a forged Bear image, Fig. 3 (b) shows a forged statue image and Fig. 3 (c) shows a forged Pigeon image. Then algorithm is applied to each image and obtained results are shown in Fig. 3 (d), (e), and (f) in terms of detecting the copy-move part of each image. From the qualitative results it can be seen that the proposed CMFD algorithm detects the forgery by detecting and marking copy move part of the image with black colour.

TABLE I

Performance evaluation of Bear image, Statue image and Pigeon image in terms of TPR, FPR, and Accuracy with existing techniques [6-9] and proposed method

Name of the image	Methods used	True positive rate (TPR)	False positive rate (FPR)	Accuracy
Bear image	Popescu et.al [6]	0.975	0.03	97.01
	Mahmood et.al [7]	0.964	0.026	97.99
	Mahmood et.al [8]	0.983	0.019	98.21
	Dixit et.al [9]	0.985	0.017	98.14
	Proposed method	0.996	0.011	99.40
Statue image	Popescu et.al [6]	0.967	0.024	97.02
	Mahmood et.al [7]	0.954	0.036	95.32
	Mahmood et.al [8]	0.978	0.019	97.93
	Dixit et.al [9]	0.965	0.018	97.14
	Proposed method	0.990	0.015	98.80
Pigeon image	Popescu et.al [6]	0.952	0.024	96.77
	Mahmood et.al [7]	0.945	0.031	92.23
	Mahmood et.al [8]	0.975	0.032	97.22
	Dixit et.al [9]	0.956	0.016	95.44
	Proposed method	0.993	0.013	99.11



(a) Bear image (b) Statue image (c) Pigeon image

(d) Detected Bear image (e) Detected Statue image (f) Detected Pigeon image

Fig. 3.Qualitative results, (a)Bear image, (b)Statue image and (c) Pigeon image are input images and (d) Detected Bear image, (e) Detected Statue image, and (f) Detected Pigeon image are the output image.

5) CONCLUSION

In this paper a new method for CMFD is presented. CMF detection for digital image is investigated by utilizing SWT and PCA. Images obtained from UCID dataset is used as test images. Quantitative results are obtained for the proposed method in terms of parameters TPR, FPR and accuracy and also a comparison based on these parameters between existing methods and proposed method is presented which shows that proposed methods provides more desirable results. For qualitative performance evaluation forged images and detected images are presented.

ACKNOWLEDGMENT

Authors are thankful to Ajay Kumar Garg Engineering College (AKGEC), Ghaziabad for providing the necessary research environment.

REFERENCES

[1] I. Amerini, L. Ballan, R. Caldelli, A.D Bimbo, L.D Tongo, and G. Serra, “Copy-move forgery detection and localization by means of robust clustering with J-Linkage,” Signal Processing: Image Communication, vol.28, Issue no 6, pp. 659–669, 2013.

[2] X. Lin, J.H Li, S.L Wan, A.W Chung Liew, F. Cheng, and X.S Huang, “Recent Advances in Passive Digital Image Security Forensics: A Brief Review,” Journal of Engineering, vol.4, Issue no 1, pp. 29-39, 2018.

[3] I. Amerini, L. Ballan, R. Caldelli, A.D Bimbo, and G. Serra, “A SIFT-Based Forensic method for Copy Move Attack Detection and Transformation Recovery,” IEEE transaction on Information Forensic and Security, vol.6, Issue no 3, pp. 1099-1110, 2011.

[4] N. Bakiah, A. Warif, A.W.A Wahab, M.Y IdnaIdris, R. Ramli, R. Salleh, S. Shamshirband, and K.R Choo, “Copy-move forgery detection: Survey, challenges and future directions,” Journal of Network and Computer Applications, vol.75, pp.259-278, 2016.

[5] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An Evaluation of Popular Copy-Move Forgery Detection Approaches,” IEEE transaction on Information Forensic and Security, vol.7, Issue no 6, pp. 1841- 1854, 2012.

[6] A. Popescu, and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Technical Report, Department of computer science, Dartmouth College, pp. 1-11, 2004.

[7] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. Mahmood, “Copy-move forgery detection technique for forensic analysis in digital images,” Mathematical Problems in Engineering, vol.2016, Article ID 8713202, pp.1-13, 2012.

[8] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, “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, vol.53, Issue no 7, pp. 201-214, 2018.

[9] R. Dixit, R. Naskar, and S. Mishra, “Blur-invariant copy-move forgery detection technique with improved detection accuracy utilizing SWT-SVD,” Journal of Institution of Engineering and Technology, vol.11, Issue no 10, pp. 301-309, 2017.

[10] G. Muhammuda, M. Hussaina, and G. Bebis, “Passive copy move image forgery detection using un-decimated dyadic wavelet transform,” Journal of digital investigation, vol.9, Issue no 1, pp. 49-57, 2012.

[11] G. Lynch, F. Shih, and H.Y Liao, “An efficient expanding block algorithm for image copy-move forgery detection,” Journal of information sciences, vol.239, Issue no 1, pp. 253-265, 2013.

[12] K. Hayat, and T. Qazi, “Forgery detection in digital images via discrete wavelet and discrete cosine transforms,” Journal of computers and Electrical Engineering, vol.62, pp. 448–458, 2017.

[13] 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,” Multimedia and Expo, IEEE International Conference, 2-5 July, pp. 1750–1753, 2007.

[14] D. Cozzolino, G. Poggi, and L. Verdoliva, “Efficient dense-field copy-move forgery detection,” IEEE transactions on information forensics and security, vol.10, Issue no 11, pp. 1-14, 2015.

[15] X.L Bi, and C.M Pun, “Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching,” IEEE Transactions on Information Forensics and Security, vol.10, Issue no 8, pp. 1705–1716, 2015.

[16] J.C Lee, “Copy-move image forgery detection based on Gabor magnitude,” Journal of Visual Communication and Image Representation, vol.31, Issue no 8, pp.320–334, 2015.

[17] G. Schaefer and M. Stich, “UCID: an uncompressed color image database,” proceeding volume 5307, storage and retrieval methods and application for multimedia 2004; (2003), Electronic Imaging event, pp 472–480.

Vaishali Sharma received her Bachelor in Technology degree in Electronics & Communication Engineering from Raj Kumar Goel Institute of Engineering and Technology in 2017. She is presently pursuing his Masters of Technology in Electronics & Communication Engineering from Ajay Kumar Garg Engineering College, Ghaziabad, affiliated from Dr. APJ Abdul Kalam Technical University, Lucknow.

Her working field is Image Processing in which she is currently working on Image Forensic.