A Novel Copy-Move Forgery Detection Using Combined ORB-PCA Approach

Krishna H. Hingrajiya and Ravi K. Sheth

***Abstract*—The integration of digital images in various forms is become essential in daily life. At the same time, it presents the serious concern about the authenticity of these images when they are used to convey important information. It became very easy to modify the information presented in an image with the availability of different editing tools and techniques. And hence the detection of forged image is much needed with efficient image forgery detection technique. In current work, an effective approach combining Principal Component Analysis and Oriented FAST and Rotated BRIEF is used to detect copy move forgery. Principle Component Analysis (PCA) is used to reduce the dimension of the features and then Oriented FAST and Rotated BRIEF (ORB) is applied to extract the key points. The results showcased the ability of presented approach in form of robustness in feature extraction and matching the key points with less computation time compared to SIFT and SURF.**

***Index Terms*—Image forgery detection, copy-move, image splicing, PCA, ORB.**

I. Introduction

Image forensics is a well-developed field which aims to analyses the authenticity of digital images. Due to easily accessible software through which images are easily forged this results to mislead its meaning and also violates its authenticity. With the huge development of technology, the usage of the image has been expanding day by day in our daily lives. Because of this, forgery of the digital image has turned out to be increasingly straightforward and indiscoverable. Image forgery implies altering the digital image to some meaningful or valuable data. Basically it can describe as the technique of adding or removing the precise features from an image without any evidence of modifying and to avoid for malicious purposes. In some cases, it is complicated to recognize the altered image part from the authenticate image. The identification of a forged image is essential for originality and to preserve truthfulness of the image [1].

The ability to create image forgery is nearly as old as photography itself. Over a two- decade, photography is the normal and fascinating art which turned out for creating portraits and by that portrait photographers can earn money by making forgery possible by enhancing deals by retouching their photographs. It is rapid and better-known domain due to its executions of real-time applications in various areas like intelligence, news reporting, medical imaging, etc. An image can be forged by varying the image features characteristics such as brightness, darkness or image parameters [2], [3]. It gained more consideration and challenging due to modern software that become difficult to confirm whether an image is tempered by naked eyes. Image forgery detection plays an important role in forensics to give authenticity to the image. The image forgery detection techniques are portioned into two approaches [4].

The active approach includes pre-processing operations such as watermark embedded or signatures for a digital image which are used during the generating image. Digital watermarking [5] and signature are two remarkable techniques for the security of image forgery. It identify the image is tampered, and to provide security and extract the specific feature contained in the image. Passive approach is complicated in digital filed and it does not require any digital signature to be created or to be embedded any watermark apart from the pictures themselves and does not require any prior data or background accessible as for the concerned image. So it is named as visually impaired pictures or passive image [3], [6].

A. Image Forgery Detection

An image can be forged by various attacks. These attacks are categorized in to malicious and non-malicious attack. Malicious attacks are those used for improvement of images and to make images memory efficient. Non-Malicious attacks are applied on image to change its meaning. The classification of coy-move forgery detection is presented in Fig. 1.

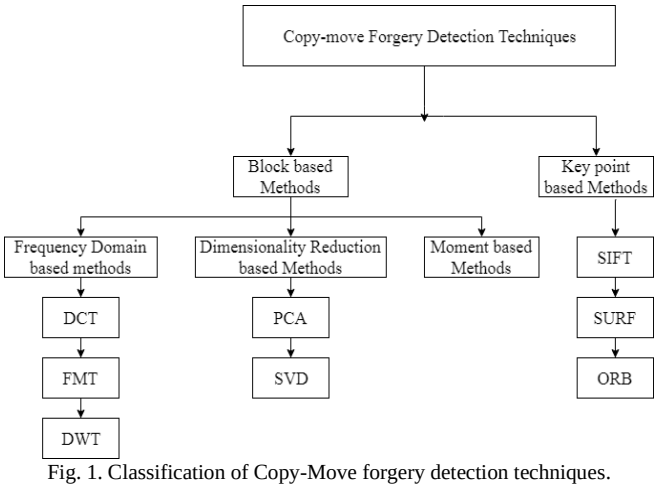

Fig. 1. Classification of Copy-Move forgery detection techniques.

B. Image Splicing

Image splicing is the process of incorporating two unique pictures to generate another image. But it is critical to integrate the ideal image for forgery. Splicing is more com-

Manuscript received October 14, 2021; revised January 2, 2022.

Krishna H. Hingrajiya is with School of IT, Artificial Intelligence and Cyber Security, Rashtriya Raksha University, India, and Computer Engineering Department, Gandhinagar Institute of Technology, India (e-mail: krishna.hingrajiya@git.org.in).

Ravi K. Sheth is with School of IT, Artificial Intelligence and Cyber Security, Rashtriya Raksha University, India (e-mail: ravi.sheth@rru.ac.in).

DOI: 10.7763/IJCTE.2022.V14.1313

plicated than copy-move for forgery manipulation and furthermore in detection [7]. The basic idea of splicing detection is searching the images being conflicting with a camera or image features. Regions which are re-sampled, double compressed, blur disparities or sharpness differences contrasts are required for splicing. Shah & El-Alfy [8], proposed DCT methods and Multi-Scale LBP for splicing forgery detection. The preprocessing is applied on the input image for the conversion of RGB images into YCbCr components and to remove the noise. Multi-Scale LBP is applied for texture analysis which generates a binary code for 3 × 3 block and the image is separated into M × M blocks and DCT is applied to every block. The extracted image is applied to Support vector Machine (SVM) for splicing image forgery detection. SVM is per-formed based on Radial-Basis Function (RBF) with separating hyper plane between two classes to classify the positive (forgery image) and negative (original image). The simulation results are performed on CASIA v1.0 and CASIA v2.0 and devaluated in terms of accuracy in which LBP method shows the efficiency of 96% and accuracy of 99% under the ROC curve for detecting splicing images. The main limitations of this method lie in the selection of kernel choice for large datasets. Xu *et al*. [9], proposed a splicing method for merged features in chroma space. The steganalysis image features are evaluated in which the features are selected and the DCT Markov features are employed to detect the splicing forgery in Chroma channel. The SVM is employed for classification regions in which the RBF kernel of LibSVM and gamma are automatically selected using fivefold cross-validation to classify the splicing region. The simulations show the efficient result for the proposed method to detect the splicing forgeries with minimum error rate.

Alahmadi *et al*. [10], analyzed the splicing image forgery detection. The splicing image forgery detection based passive approach is developed by Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT). The input image is partitioned into overlapping blocks and LBP is applied and converted into frequency domain by employing DCT. Support Vector Machine (SVM) is used to classify the forgery and authenticate image. The simulation results show that the efficient splicing forgery detection with accuracy of 97%. The limitations of this method are selection of kernel and over fitting problems lead to inefficient classification of forgery images. Shen *et al*. [11] developed a spliced image forgery detection that depends on Grey Level Co-Occurrence Matrices to detect the texture features Difference Block Discrete Cosine Transform (DBDCT) arrays are implemented by decomposing an image into several blocks to evaluate the GLCM for extracting the textural features such as mean, standard deviation and spatial relationship between image pixels. These measures are used as feature vectors in SVM classifier to differentiate the original and spliced forgery image. The results are evaluated on CASIA v1.0 and CASIA v2.0 in terms of certain parameters and the obtained result shows that the GLCM for texture extraction achieves the effective results of 98% with reduced dimensionality of feature vector and computational complexity.

C. Copy Move Forgery

Copy Move forgery is the popular and widely used forgery image techniques in real time applications. Copy-move forgery type is the process of copying one portion of the image in the same image and pasting in another image as by hiding the significant information. It is exceptionally hard to recognize the image is forged or authentic. Pandey *et al*. [12] analyzed the video processing based copy-move forgery to recognize the forge region of the video. This strategy used distinctive pre-processing for elimination of noise and classification steps to recognize the forged area. The SIFT algorithm is utilized to form the edges in the feature extraction process. The experimental outcomes exhibit the skillful noise reduction processes to upgrade the image quality. This method works effectively for transient images with efficient classification accuracy rate. Ranjani *et al*. [13], proposed forgery detection by utilizing Discrete Cosine Transform (DCT) Techniques and Inverse Discrete Cosine Transform Techniques dependent on row and column reduction method. The new method decreases the computational complexity related to time, cost and the capability of the image. At first, the input image is partitioned into grids as rows and columns. In which DCT is related with each row and columns with the help of lines and segments and it changed into different pieces with various estimations. Finally, the copied picture gets managed from viewpoint of is repression respect. Li *et al*. [14], built up a Polar Harmonic Transform (PHT) based on block coordinating for copy-move forgery detection. The features extracted by PHT from the circular blocks are used to give indefinite image features. These blocks are compared with PHT features. The input images are collected from the openly accessible datasets and simulated by MATLAB. The performance results show that the proposed method is strong to noise, JPEG compression, and object rotation. Shiva kumar *et al*. [7], proposed a Harris Interest Point detector alongside SIFT descriptors and KD-Tree for coordinating similarity to identify copy-move forgery. The Harris detector is mostly used for autocorrelation function to choose areas where the distinctions of signal in one or two directions exist. The KD-tree is utilized for distinguishing the closet neighbors and it pre-processes data into an information structure enabling us to make proficient range queries. The experimental outcomes accomplish the reliable results with lower false negative rates and the less detection time and the matching similarity is performed relying upon threshold values.

Ustubioglu *et al*. [15] suggested a method to evaluation threshold automatically. The threshold is used to compare the feature vectors similarity. The Discrete Cosine Transform (DCT) is employed to limit the feature vector elements and Benford's generalized law also utilized to establish the image under test. The technique utilizes element-by-element equity among the feature vectors rather than Euclidean distance or cross-connection and uses the image under test to identify the threshold value consequently. Experimental results demonstrate that the strategy can recognize the copied and pasted regions under various situations and achieves higher precision ratios with minimum false negative rate compared to existing algorithms. Davarzani *et al*. [16] proposed tampering detection method by using Local Binary Pattern. The copied regions are recognized and also detect the forged region affected by noise, blurring, JPEG compression, scaling or rotation in products of 90-degree. The input image

is converted into gray scale and divided into overlapping blocks. The Multi-resolution Local Binary Pattern (MLBP) is employed on each block to find the features by applying the LBP operators. The feature matrices are sorted lexicographically and the matching blocks are identified by k-d tree strategy. Table I shows the relative survey of different methods for identification of copy move forgery. This table shows that various strategies utilized for copy move forgery recognition and the achieved limits.

TABLE I: TECHNIQUES USED FOR COPY-MOVE FORGERY DETECTION

Authors	Techniques Used	Demerits
Pandey *et al*. [12]	SIFT and SURF	Not good in case of multiple cloning or copied part with rich texture or background
Ranjani *et al*. [13]	DCT and Inverse DCT by Row and Column Reduction method	High computational complexity related to time and cost
Li *et al*. [14]	Polar Harmonics Transform	Slow in execution and occurrence of false positives results
Shiva kumar *et al*. [7]	SIFT, SURF, and Harris for triangles blocks	Not efficient in matching similarity result and no interest points are detected
Mahdian & Saic [17]	Blur Invariant Feature (BLUR)	The high computation time of the algorithm
Zhang *et al*. [18]	Discrete Wavelet Transform (DWT)	More noisy and compressed image
Huang *et al*. [19]	Scale Invariant Feature Transform (SIFT)	Time complexity and inefficient to detect the false result
Ghorbani *et al*. [20]	DCT-DWT	Not efficient for highly compressed image and poor-quality image
Huynh-Kha *et al*. [21]	DWT and feature extraction	DWT does not give a result for rotational transformation

D. ORB (Oriented FAST and Rotated BRIEF)

Oriented FAST and Rotated BRIEF (ORB) is a combination of FAST as key point identification and BRIEF to enhance the performance. Firstly the FAST is used to search the key points, at that point Harris corner measure to find top N points between them. Multi scale-features can be generated through pyramids. Yet, FAST is not productive for computing the direction. It calculates the intensity weighted centroid of the fix which is representing addressing corner as middle. The orientation is obtained through the path vector from this corner point to the centroid. The moments are identified with coordinates x and y in order to enhance the rotation invariance [22].

BRIEF is not effective for rotation hence ORB improves the performance of BRIEF with the positioning of key points. For any feature set of n binary tests at area (xi, yi), define a 2×n matrix, S which contains the coordinates of these pixels. Then using the orientation of patch, θ, its rotation matrix is found and rotates the S to get steered (rotated) version S_θ. ORB discretize the angle to additions of π/30 (12 degrees), and develop a query table of pre computed BRIEF patterns. However long as the key point orientation θ is reliable across views, the correct set of points S_θ will be utilized to process its descriptor [23]. BRIEF has a significant property that every feature is with major difference and a mean close to 0.5. Yet, whenever it is arranged along key point direction, it becomes circulated and by losing this property. The features with higher fluctuations make it more discriminative, as it responds differently to inputs. Another important property is to have the tests uncorrelated, as each test will contribute to the result. To define all these, a greedy search is run by ORB between all possible binary tests to determine the once with higher difference and means closer to 0.5, as well as being uncorrelated. The conclusion is known as rBRIEF [23].

A feature point detector has two sections.

1. Locator: It identify the images with shift, scale, rotation and identifies the location in form of x, y coordinates of these points. The locator utilized the ORB detector is called FAST.

2. Descriptor: The locator only gives the points and hence descriptor is used to encode the identified points such that it can be differ from other points. An array of number is calculated using the descriptor. Ideally, the similar actual point in two images should have the similar descriptor. ORB utilized a modified version of the feature descriptor called BRISK [24].

The ORB image matching algorithm is having three parts: feature point extraction, creating feature point descriptors and feature point matching. The steps involved in ORB are presented in Fig. 2.

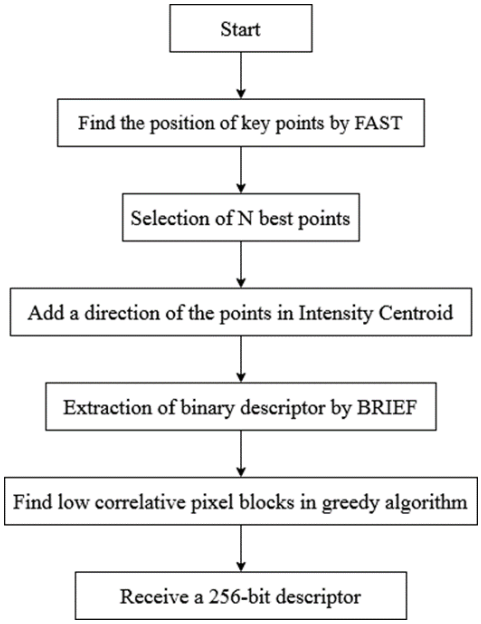

Fig. 2. The working of ORB Algorithm.

E. Dimensionality Reduction Based Methods

The fundamental point of this procedure is to lessen the dimension of the input image by following algorithms [25]. Principal Component Analysis (PCA) -The dimensionality of the information in given image can be decreased by reducing the deficiency of data or distortion which projects data onto axes of maximal information change. This algorithm is strong to minor difference in the image because of added noise or JPEG compression [26]. The linear subspace can be determined by orthogonal vectors that structure another coordinate system, called the 'principal components'. The principal components are orthogonal, linear transformations of the original data points, so there can be close to n of them.

II. Results and Discussions

The proposed technique is applied on the standard dataset CASIA v2.0. Dataset contains 7491 authentic and 5123 tampered color images having of size 240×160 to 900×600 pixels. It contains the various categories of classes like animal category, architecture, characters, indoor, nature, plants, texture. Due to lack of space, we presented only few samples among them [27].

The opencv-python 3.2.0.8 software with 4GB Ram and Intel core i3 processor is used. Initially, PCA is applied on the dataset and principal component of the decomposed image is given as input to ORB algorithm to extract the descriptor vectors. Finally, key points matching operation is processed to identify the copy move forgery. Fig. 3 presents the original images, forged images, and the output after detection of forged region.

The performance of the presented method is evaluated by considering the factors namely average time per image, specificity, precision, accuracy, recall, and F1 score. The method is applied on 100 images from the dataset CASIV 2.0. Table II presents the comparative results [28]. Fig. 4 demonstrates the comparison of proposed method with other methods.

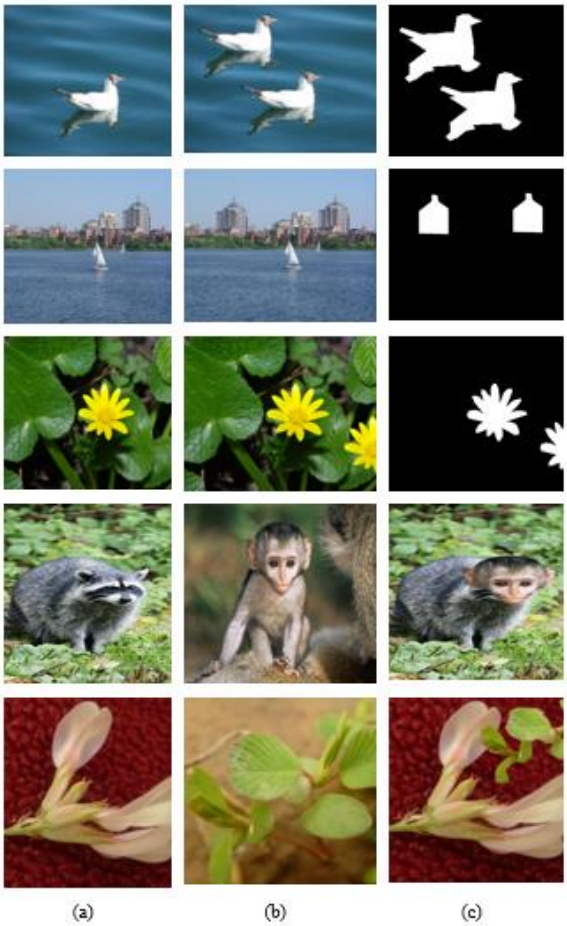

Fig. 3. (a) the original image (b) forged image (c) the output after detection of forged region.

TABLE II: Comparative Result of Proposed Approach

Techniques	Average time per image (sec)	Specificity	Precision	Accuracy	Recall	F1 score
SIFT-PCA	0.984	53.124	70.246	68.610	81.680	76.670
SURF-PCA	0.884	58.210	59.326	63.682	70.110	63.246
ORB	0.684	63.124	73.241	68.468	78.640	72.486
ORB-PCA	0.587	87.624	86.510	80.412	82.324	81.632

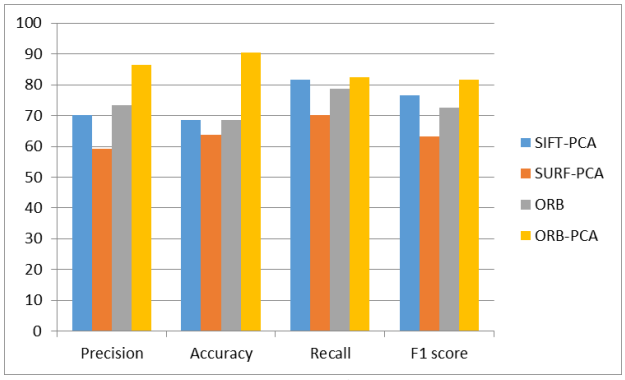

Fig. 4. Comparative result of proposed approach.

The computation time increases with increase in number of images selected from the dataset. And hence, limited images are selected for the comparison. The accuracy of the proposed method is better with less computation time compared to other presented approaches in past.

III. Conclusions

With the advancement in technology and software, an authentic image is very important to convey the information for various means. On the other side, it is essential to establish the genuineness of an image as the image forgery becomes so easy with the availability of various modern tools. One such forgery reported in many instances is copy move image forgery. In past, many techniques have been utilized to detect the copy move forgery in an image. However, these techniques suffer from high computation time, less detection accuracy, etc. Hence an effort has been made to identify copy mover forgery even if the image is slightly changed with minor modification.

In the presented work, a novel approach combining PCA and ORB is utilized to detect the image forgery. The PCA is used for the reduction of dimensionality of the particular features of an image and ORB is applied to the extract the image features by identifying the key points. It is observed that ORB has resulted in less computation time and better real time performance compared to other methods. However, the performance of ORB can be improved by combining it with an efficient algorithm to improve the matching speed.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Krishna H. Hingrajiya developed the methodology of work, analyzed the data and wrote the paper. Dr. Ravi K. Sheth provided guidance in the preparation of the paper. All the authors had approved the final version.

References

[1] S. Murali, G. B. Chittapur, and B. S. Anami, "Comparision and analysis of photo image forgery detection techniques," arXiv preprint arXiv:1302.3119, 2013.

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

[3] T. Qazi, K. Hayat, S. U. Khan, S. A. Madani, I. A. Khan, J. Kołodziej, and C. Z. Xu, "Survey on blind image forgery detection," *IET Image Processing*, vol. 7, no. 7, pp. 660-670, 2013.

[4] S. S. Patil, A. N. Patil, N. P. Patil, J. D. Dhongde, and B. S. Khade, "Digital image forgery detection using basic manipulations in Facebook," *Int. J. Sci. Technol. Res.*, vol. 3, pp. 356-359, 2014.
[5] K. Mahmoud and A. H. A. Al-Rukab, "Moment based copy move forgery detection methods," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 14, no. 7, 2016.
[6] V. P. Nampoothiri and N. Sugitha, "Digital image forgery—A threaten to digital forensics," in *Proc. 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1-6, IEEE, March 2016.
[7] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," in *Proc. the 9th Workshop on Multimedia & Security*, pp. 51-62, September 2007.
[8] A. Shah and E. S. El-Alfy, "Image splicing forgery detection using DCT coefficients with multi-scale LBP," in *Proc. 2018 International Conference on Computing Sciences and Engineering (ICCSE)*, pp. 1-6, IEEE, March 2018.
[9] B. Xu, G. Liu, and Y. Dai, "Detecting image splicing using merged features in chroma space," *The Scientific World Journal*, 2014.
[10] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and local binary pattern," in *Proc. 2013 IEEE Global Conference on Signal and Information Processing*, pp. 253-256, IEEE, December 2013.
[11] X. Shen, Z. Shi, and H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices," *IET Image Processing*, vol. 11, no. 1, pp. 44-53, 2016.
[12] R. C. Pandey, S. K. Singh, and K. K. Shukla, "Passive copy-move forgery detection in videos," in *Proc. 2014 International conference on computer and communication technology (ICCCT)*, pp. 301-306, IEEE, September 2014.
[13] M. B. Ranjani and R. Poovendran, "Image duplication copy-move forgery detection using discrete cosine transforms method," *International Journal of Applied Engineering Research*, vol. 11, no. 4, pp. 2671-2674, 2016.
[14] L. Li, S. Li, and J. Wang, "Copy-move forgery detection based on PHT," in *Proc. 2012 World Congress on Information and Communication Technologies*, pp. 1061-1065, IEEE, November 2012.
[15] B. Ustubioglu, G. Ulutas, M. Ulutas, and V. V. Nabiyev, "A new copy move forgery detection technique with automatic threshold determination," *AEU-International Journal of Electronics and Communications*, vol. 70, no. 8, pp. 1076-1087, 2016.
[16] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," *Forensic Science International*, vol. 231, no. 1-3, pp. 61-72, 2013.
[17] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic Science International*, vol. 171, no. 2-3, pp. 180-189, 2007.
[18] J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copy-move forgery in digital images," in *Proc. 2008 11th IEEE Singapore International Conference on Communication Systems*, pp. 362-366, IEEE, November 2008.
[19] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Proc. 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, pp. 272-276, IEEE, December 2008.
[20] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in *Proc. 2011 18th International Conference on Systems, Signals and Image Processing*, pp. 1-4, IEEE, June 2011.
[21] T. K. Huynh, K. V. Huynh, T. Le-Tien, and S. C. Nguyen, "A survey on image forgery detection techniques," in *Proc. The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF)*, pp. 71-76, IEEE, January 2015.
[22] R. Kaur and A. Kaur, "Copy-move forgery detection using ORB and SIFT detector," *International Journal of Engineering Development and Research*, vol. 4, no. 4, pp. 804-813, 2016.
[23] C. Luo, W. Yang, P. Huang, and J. Zhou, "Overview of image matching based on ORB algorithm," *Journal of Physics: Conference Series*, vol. 1237, no. 3, p. 032020, IOP Publishing, June 2019.
[24] S. Gupta, M. Kumar, and A. Garg, "Improved object recognition results using SIFT and ORB feature detector," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 34157-34171, 2019.
[25] L. Juan and O. Gwun, "A comparison of SIFT, PCA-SIFT and SURF," *International Journal of Image Processing (IJIP)*, vol. 3, no. 4, pp. 143-152, 2009.
[26] K. Pearson, "Principal components analysis," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 6, no. 2, p. 559, 1901.
[27] N. T. Pham, J. W. Lee, G. R. Kwon, and C. S. Park, "Hybrid image-retrieval method for image-splicing validation," *Symmetry*, vol. 11, no. 1, p. 83, 2019.
[28] A. Vinay, C. A. Kumar, G. R. Shenoy, K. B. Murthy, and S. Natarajan, "ORB-PCA based feature extraction technique for face recognition," *Procedia Computer Science*, vol. 58, pp. 614-621, 2015.

Krishna H. Hingrajiya is an assistant professor at Gandhinagar Institute of Technology and pursuing Ph.D. in the area of image processing and machine learning form School of IT, Artificial Intelligence and Cyber Security, Rashtriya Raksha University. Her area of interest includes image processing, cyber security, machine learning, etc.

Ravi K. Sheth is having more than 13 years of teaching experience. Currently Dr. Sheth is working as an assistant professor in School of IT, AI and Cyber Security at Rashtriya Raksha University, Gandhinagar. His keen area of interest is in multimedia security, machine learning, pattern recognition, VAPT and Cyber Forensics.