Robust Copy-Paste Detection Algorithm using SIFT for Digital Image Forensics

Monika, Dipali Bansal

Abstract**:** ***Forensics of images verifies the authenticity of digital images. Because of the easier availability of software, manipulation of images has become quicker and easier. Image composition, copy-paste, multiple cloning, splicing, etc have become a common practice. The paper proposes a robust algorithm for the detection of duplicity using Scale Invariant Feature Transform (SIFT) approach. Copied location of an image is occasionally pasted in another place of the identical image or in another image, which creates difficulties in detecting the copy-paste region and identifying the located region as well as creates inefficiency in the accuracy of forgeries. We developed an approach that shows improved techniques through runtime optimizations and compared various parameters with existing methodologies in order to obtain highly correlated image areas for detecting the manipulated regions. The proposed approach can detect copy-paste forgeries effectively with high accuracy, reliability, and inconsistencies regardless of the test scenario.***

Keywords**:** ***CMTD, Digital Image Forensic, Image Forgery Detection, Image Authentication, SIFT.***

I. INTRODUCTION

Images are the main media for information exchange. Millions of images are uploaded daily over the internet, moving towards paperless work environment, e-government services everywhere, and the use of digital videos such as CCTV camera recordings are the main sources of any kind of evidence for content security. Now, with the validation of digital images, it becomes a strong liability to identify image manipulation. However, Digital Image Forensics proves that images are original and authentic. A passive and active approach to the development of robust forgery detection, identification and tracking issues can be used to detect image tampering. [1]., highly powerful computer applications like Photoshop, Paint, and Microsoft Office make Digital Image Forensic easier, faster, and more cost-effective.**Figure.1** Represents the feature extraction approaches. **Figure.2**. Highlights the classification of forgery detection image authentication methods that can be described as 1) Pixel-based approach for pixel-level identification of all statistical anomalies, 2) Format-based mechanism for influencing statistical correlations, particularly in the system of loss compression, 3) Camera-based sensor removal techniques, camera post-processing, 4) Physically based forgery detection procedures and image authentication. Publication indexed by Scopus for Copy-Move Detection of forgery provides the number of publications in peer-reviewed journals quoted by SCOPUS in **Figure.3** over many years. **Figure.4** Explain the proposed CMTD procedure. **Figure.5**. Show an image forgery example: original images. **Figure.6**. shows an example of Tempered Images, **Figure.7**. Show matching Duplicated regions. **Figure.8** Shows runtime analysis of the method proposed and **Figure.9** represents the proposed method's comparative results analysis of accuracy.

Digital images via digital camera, scanner and computer graphics [2], the integrity of information are the main requirement as it affects the judgment. The main objective is to find that something has been copied or hidden [3], since the copied part has the same compatibility approaches proposed by copy-move tampered detection with the rest of the image [4] find correlation between original and tempered images, Authors [5] proposed a blur feature invariant algorithm that represents sorting for efficiency improvement. Authors [6] used DCT to find the spatial offset in the image by sorting block coefficients. In [7], FMT is used by a related approach to detect forgery such as resize, scaling, etc. Authors in the proposed methods [7] include the MICC-F220 and MICC-F2000 test datasets containing tempered images in terms of locations and dimensions, image area and use a different algorithm, analyzing the 100% TPR cut-off threshold. The extract features for testing block similarity are the main issues with previous techniques. In the background of various forgeries, copy-move tampered detection algorithms based on DCT algorithms, Log-Polar transform algorithms, texture algorithms on the basis of intensity, invariant key-point algorithms, PCA algorithms, Invariant moments of image algorithms, SVD algorithms and other algorithms. **Table.1.** Represent comparison with existing SIFT methodologies. **Table.2**. Evaluate the description and calculation of the proposed method, where True Positive matches provide a number of images correctly detected as forged, False Positive matches provide a number of images falsely detected as forged, False Negative matches Provide a number of falsely missed but forged images and False Positive matches provide a number of falsely missed but tampered images. **Table.3** represents an analysis of runtime using different state-of-the-art methodologies. This paper presents verifications of copy-Paste tampered detection (CPTD) algorithms, map detected. The paper has arranged for the first part to review previous and current copy-Paste tampered detection (CPTD) algorithms and the second part to give the copy-Paste tampered detection (CPTD) concept using SIFT. The third part fully explains the proposed method with the performance parameter and experimental results calculation highlights uniqueness, paper contribution, final conclusion, and scope of the future. This paper presents a precise objective of analyzing all types of existing methodologies of forgery detection and we have presented dedicated approaches for fast processing and reduction of computational complexities.

Revised Manuscript Received on November 15, 2019

Monika, Assistant Professor, Manav Rachna International Institute of Research and Studies, Faridabad, NCR, India.

Dipali Bansal, Associate Dean - Academics with Manav Rachna International Institute of Research and Studies, Faridabad, NCR, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

We categorized the work as the original features of all the original images were first calculated and gradient calculations were performed for the image pixels. After that draw the features on the images so that matching features are easy to perform where Gaussian is applied to a smooth result image which helps to obtain the features and descriptors that are done in the following steps:

1. Dog (degree of the gradient) pyramid is calculated by providing interval number per octave is 3 and the default cubic method is applied by assuming blur is 0.5 and the smallest top-level distance is about 8 pixels. The next dog and Gaussian pyramid are performed where Bio-signal provides the maximum steps of key-point interpolation are only 5 and the accurate key-point location is obtained by taking the high threshold ratio of principle extreme curvature in 26 adjacent pixels.
2. Guidance Assignment calculated by a 2-D Orientation histogram for the descriptor feature and sorting the descriptor by reducing the order of the scale.
3. Next, convert histogram to the descriptor and obtained histogram entry interpolation to interpolate the location of an extreme space scale and scale the initial global sigma.
4. Remove from first to second all edge-like points and match descriptor and return to matching an index.
5. With respect to the second nearest neighbor with distance ratio 0.6, matched vector angles to each nearest one.
6. Successfully calculating the histogram of orientation and smoothing the histogram.

COPY-MOVE TAMPERED DETECTION (CPTD):

It is the most common technique of tampering used to alter image information. Copy-Move forgery image processing operations include rotation, reflections, changes in luminance and chrominance, scaling, noise adding, blurring, JPEG compression and mirroring. Copy-Move forgery carried out by inserting part of the image in the same image or elsewhere in another image. The inherent characteristics of the tempered region, such as pattern noise, are highly similar in the color palette. This paper's main objective is to analyze the work that highlights the recent trend in DIF research.

II. RELATED WORK

Tampering of copy-paste is also known as tampering of copy-move. In digital image forensics, numerous techniques are proposed for detecting image forgery. These are categorized as techniques on the basis of key points and techniques on the basis of blocks. Copy moving forgery is a widespread method of creating image forgery where some parts are copied and pasted to the other location in the same image. This section reviews some of the techniques used to detect manipulation by copy-paste.

Al-Qershi *et al* [7] (2013) different state-of-the-art blind detection such as forgery of moving replicas in digital images have been demonstrated. The current forgeries for robust passive copy-move detection are discussed. **Ramesh Chand Pandey** *et al* [8] (2015) proposed methodology with different image characteristics such as SURF-HOG, SIFT-HOG, SIFT, and accuracy obtained is 95.5 percent, 98.5 percent, 91.7 percent, respectively. The authors made the second attempt to detect copy-paste manipulation using the SURF & SIFT feature for high accuracy and very fast speed, but they needed to maintain a dynamic threshold. **ZHEN ZHANG** *et al* [9] (2008) examined many passive-blind image forgery methods and came to the conclusion of runtime problems requiring effective resolution of these problems and expertise from a variety of fields such as imaging sensors, computer graphics, Vision of computers, processing of signals, machine learning, and mechanical systems. Researchers at the same time needed a new way of working in this area. **Mohammad Farukh Hashmi** *et al* [10] (2014) developed a forgery detection algorithm using Discrete Wavelet Transform and SIFT extract key characteristics with a vector descriptor and achieved accuracy of only 94%, compared with existing **Zhang**[11] (2008) 77.32 % accuracy with changed region size 64x64 and Popescu1 method (2004). Authors achieved an accuracy of about 90% for a modified block size of 128x128 and an image size of 512x512 with a quality factor of 85 by **Li**[12]- 2009 was just 47.21% accuracy.

Mohammad Farukh Hashmi *et al* [13] (2014) authors used to Transform Dyadic Wavelet and Invariant Scale Feature to improve their work. **Shiv Prasad** *et al* [14] (2016) proposed a method using SIFT-HOG and SURF-HOG to achieve detection accuracy of 99.09% and 97.72% respectively. **Sondos M.Fadl** *et al* [15] (2014) suggested the Fast k-means clustering technique to detect blurring, JPEG compression, rotation and scaling reprocessing only up to 50 percent robustness.

Irene Amerini *et al* [16] (2014) proposed first digit features and SVM classifiers for effective w.r.t tampering detection, forgery dimensions, various compressions of quality and multiple forgeries. **Ashima Gupta** *et al* [17] (2013) suggested forgery detection using DCT for copy-move attacks with a highly textured image. Authors split an image into blocks that overlap to search the image's replicated blocks. **Tariq BASHIR** *et al* [18] (2017) present an intelligent parameter estimation methodology based on RR-IQA just by rearranging discrete cosine transformation (RDCT). **Gajanan K. Birajdar** *et al* [19] (2013) presented a summary of the complete survey of digital image manipulation detection and the existing reference analysis of blind image manipulation methods using passive techniques with further recommendations for future research.

Krittachai Boonsivanon *et al* [20] (2016) presented an improved key-point detection algorithm called IKDSIFT for recognition of objects, non-uniform SIFT-based illumination and morphological operations was proposed. **Rinky B P.** *et al* [21] (2012) proposed a novel pre-processed technique where feature extraction calculation is evaluated on the basis of pre-processed images using Discrete Wavelet Transform and feature selection optimization to achieve Binary Particle Swarm Optimization. **Priyanka Prasad**[22] (2012) presented a new passive fine-grained approach for forgery detection by measuring the presence of demosaicing artifacts even at the lowest block level and interpreting the local absence of CFA artifacts as confirmation of manipulation. **Anil Dada Warbhe** *et al* [23] (2015) proposed a way to detect and locate forged regions in the presence of rotation and scaling operations with small factors using customized Normalized Cross-Correlation (NCC) but not entirely robust.

Leida Li *et al* [24] (2014) proposed the method for circular pattern matching calculation extracts Polar Harmonic

Transform (PHT) from each block by filtering and dividing blocks into circular size, rotation, and scale-invariant features. Experimental results show the method's efficiency, but for blurred, AWGN, JPEG compressed images need better feature extraction methods. **Amerini** *et al* [25] (2015) suggested the transformation of the scale-invariant feature (SIFT) to detect forged regions where any region is copied variation in rotation and scaling. Authors used a low-pass filter over images and divide it into circular block overlapping sizes where PSTs are calculated lexicographically sorted to compare feature vectors for each block and feature vectors and tried to search for similar block pairs. By using the post-processing filter and the morphological map, this mechanism reduces false matches.

Mohammad Farukh Hashmi *et al* [26] (2014), Proposed algorithm using Dyadic Wavelet Transform and Scale Invariant Feature Transform (SIFT) to extract more key points that more effectively detect copy-move forgery and have better results than Discrete Wavelet Transform (DWT), authors use DWT to break down the input image into four different sub-bands such as LL, LH, HL and HH. Because most information in the lower frequency band is available therefore presented in the Sub-band of low frequency, i.e. LL band is divided into overlapping blocks. This has reduced the number of blocks and accelerated the overall process. **Li** *et al* [27] (2015) discussed computational load reduction techniques.

E-Sayed M *et al* [28] (2014) proposed an enhanced blind detection technique that extracts and combines Markov's spatial and discrete cosine features to transform the domain to remove artifacts and reduce overall computational complexity due to high dimensionality. By optimized vector support machine to categorize the image as manipulated or authentic.

A. Annis Fathima. *et al* [29] (2014) authors presented image cloning with Invariant SIFT moments to reduce time and computational complexity. The proposed method, therefore, detects overlapping regions to extract matching points use gradient-based extraction of the dominant edge and invariant moments. **Reza Davarzani** *et al* [30] (2013) authors present multi-resolution Local binary patterns (MLBP) that are robust to geometric deviations and copied area lighting changes, Authors divide the overall images into overlapping fixed blocks, vectors for each block extracted from LBP operators to sort them based on lexicographic order helped to determine duplicated regions even after rotation, scale-alteration, JPEG compression, blur and added noise still The proposed method can-not detect randomly rotated replicated regions.

Jian Li *et al* [31] (2015) presented a CMFD sift image segmentation scheme for CMFD but only a few patches need matching transform matrix re-estimation and only 11.9% of false-negative matches,13.8% of false-positive matches. **Ewerton Silva** *et al* [32] (2015) present a multi-scale digital image analysis and voting processes. Authors conducted an in-depth analysis of cloning detection issues of interest with clustering, multi-scale examination, and a voting procedure attempted to reduce the manipulated regions' search space and presented a comparative analysis of the results of various existing state-of-the-art methodologies, particularly detection maps using 90 and 70 JPEG compression factors. **Nor Bakiah Abd. Warifv** *et al* [33] (2017). The geometric transformation attacks investigated, reflective attacks and evaluation parameters are calculated on the basis of multi-scale SIFT testing and matched patches to recover simple transformation. Reflection-based attacks compared to existing methods and not over 80 percent F-score on average for all geometric changes, including normal transformation, reflective attacks with the exception of rotational reflection with an average 65.3% f-score.

Ram Kumar Karsh *et al* [34] (2017) presents a DWT-SVD image hash and a spectral residual model based on a ring partition that was invariant to the distance vector and Invariant rotation for arbitrary angles but very sensitive to corner changes, the authors finally used HSV colour space for suitable performance JPEG compression, brightness, contrast and watermarking, against large-scale rotation, etc. In addition, sensitivity to malicious actions such as deletion, insertion, and replacement is not capable of detecting color forgery with regard to translation. **Mahdian** *et al* [35] (2006) present a comprehensive bibliography of approaches to detection of blind image forgery using invariants blur moment. The proposed method for detecting replicated areas of the blur with noise.

Bayram *et al* [36] (2009) authors used Fourier-Mellin Transform shows invariant scale rotation for forgery detection as copy-move forgery was computationally efficient and capable of detecting forgery even when images are highly compressed were presented. **Huang** *et al* [38] (2008) employed Invariant Scale Feature Transform descriptors for extraction of features Descriptors of different regions match each other to find possible forgeries in images. Li *et al* [39] (2015) proposed a sorted neighborhood approach based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD), applying DWT over the image and SVD is then used to calculate components of low frequency to reduce their characteristic dimensions.

Rajeev Kaushika *et al* [40] (2015) in order to reduce the dimensional feature vectors, the authors proposed 2D-discrete cosine transformation. Computational complexity improved but could not reduce the computational cost of the method of sorting. **Mohsen Zandi** *et al* [41] (2016) proposed a key-point interest detector with filtering algorithm analysis to detect falsely matched regions effectively. **Anil Dada Warbhe** *et al* [42] (2015) presented a copy-paste detection survey based on key-point approaches using algorithms such as SIFT and SURF. **Luisa Verdoliva** *et al* [43] (2014) use camera-based localization manipulation technique. The authors calculate residuals using high-pass filtering, quantify residuals, and then calculate co-occurrence histograms to make a smooth decision.

Guzin Ulutas *et al* [44] (2017) suggested medical image manipulation detection based on the key-point selection using local binary patterns that are invariant to the rotation with SIFT to highlight texture information. **Shiji.T.P** *et al* [45] (2017) proposed a segmentation algorithm for automatic segmentation of breast ultrasound images with SIFT to obtain only 90.1 percent True Positive Rate, which helps to effectively segment tumor regions with good accuracy. **Reshma Raj** *et al* [46] (2016) proposed a CMFD using an EM-based algorithm to segment an image into semi-independent patches by partial matching.

Sudhakar.K *et al* [47] (2016) present an effective methodology for the detection of copy-moving forgery by using SIFT to reduce time complexity by up to 95,88% by reducing the number of key points. **K. Sitara** *et al* [48]

(2016) presents a video forensics survey and identifies some open issues for identifying new research areas in the detection of passive video manipulation. **Gupta S.** *et al* [49-55] I[76, 77, 78, 79, 80, 81, 82] (2015, 2016 and 2017) describe medical image registration using different optimization techniques and the scope of these techniques can be developed for digital image forensic copy-paste tampering detection.

III. SIFT: SCALE–INVARIANT FEATURE TRANSFORMATION

Invariant Scale Feature Transformation algorithm is a robust approach to detection in different changes in rotation, lighting, scaling, etc. SIFT allows copy-move forgery to be understood and recovered from geometric transformation used for cloning. SIFT estimates geometric transformation with high reliability for multiple cloning and the SIFT approach performs the best rotational computation and scaled image changes. The methodologies described locally are invariance changes in illumination, changes in scale under rotation, changes in a blur, noise, translation, affine transformation in relation to other transformations. Scale Invariant Feature Transform was found to yield the best results by extracting distinctive invariant features from images that match different object or scene views reliably.

The Scale Invariant Feature Transformation procedure contains four procedural steps as the first is space-extreme scale detection, the second is key-point localization, the third is an assignment of orientation, and finally key-point descriptor. Initially, extreme scale-space detection in the SIFT procedure uses Gaussian Difference (DoG) as an approximate of Gaussian Laplacian(LoG) for input image with different values when used as a scaling parameter and scale-space images I(x, y, µ) is produced by converting image I(x, y) to variable scale Gaussian (x, y, µ). in accordance with the 3 & 4 equations. The difference between Gaussian and Gaussian obtained as the difference between two different images, presented in equation 5 & 6, with the next image and searched for local extremes over spatial scale where each pixel is an image with 9 previous pixels compared to its 8 neighbors and 9 next scale pixels. If it's a local extreme, it's the best possible key point. Secondly, Key-point Localization was used to obtain more accurate results using the expansion of the Taylor series with a contrast threshold in equation 7 & 8. Third, the Orientation Assignment neighborhood is calculated depending on the gradient magnitude, scale around the key-point location and dimensions in that region to obtain invariant image rotation that generates key-points of the same scale and location. Stability for matching in different directions is shown in equations 1 & 2. Finally, Key-point Descriptor helps to create 16x16 neighborhoods around the key-points and divide them into sub-block sizes of 4x4. Each sub-block considers the key-point descriptors to be an eight-bit histogram. Matching of Key-Point is done by identifying their adjacent neighbors between two images. For verification where outliers are removed and holes are filled by basic filtering like morphological operations, similarity criteria such as Euclidean distance are determined.

$$G(x,y,\sigma)=\frac{1}{2\pi\sigma^2}e^{-(x^2+y^2)/2\sigma^2}\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(1)$$

$$L(x,y,\sigma)=G(x,y,\sigma)*I(x,y)\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(2)$$

$$D(x,y,\sigma)=\big(G(x,y,k\sigma)-G(x,y,\sigma)\big)*\ I(x,y)\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(3)$$

$$=$$

$$L(x,y,k\sigma)-L(x,y,\sigma)\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4)$$

$$D(x,y,\sigma)=D(x_i,y_i,\sigma_i)+\Big(\frac{\partial D(x,y,\sigma)}{\partial(x,y,\sigma)}\Big)_{\substack{x=x_i\\y=y_i\\\sigma=\sigma_i}}^{T}\Delta+\frac{1}{2}\Delta^T\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(5)$$

$$\Delta=\begin{pmatrix}x-x_i\\y-y_i\\\sigma-\sigma_i\end{pmatrix}\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(6)$$

$$\begin{bmatrix}\hat{x}\\\hat{y}\\\hat{\sigma}\end{bmatrix}=-\left(\frac{\partial^2 D(x,y,\sigma)}{\partial(x,y,\sigma)^2}\right)_{\substack{x=x_i\\y=y_i\\\sigma=\sigma_i}}^{-1}\left(\frac{\partial D(x,y,\sigma)}{\partial(x,y,\sigma)}\right)_{\substack{x=x_i\\y=y_i\\\sigma=\sigma_i}}\dots\dots\dots\dots\dots\dots\dots\dots(7)$$

$$D_{external}=D(x_i,y_i,\sigma_i)+\frac{1}{2}\left(\frac{\partial D(x,y,\sigma)}{\partial(x,y,\sigma)}\right)_{\substack{x=x_i\\y=y_i\\\sigma=\sigma_i}}^{T^T}\begin{bmatrix}\hat{x}\\\hat{y}\\\hat{\sigma}\end{bmatrix}\dots\dots\dots\dots\dots\dots\dots\dots(8)$$

IV. PROPOSED METHOD

SIFT algorithms extract robust features for forgery detection where the tempered region is nearly the same as the original, but SIFT features can determine the maximum possible tempering by clustering key-points and matching geometric forgery detection transformation. We proposed an algorithm for cloning images that shows image authenticity with low Euclidean distance compared to others. To determine forgery detection, we found the extraction feature and key-point matching for key-point clustering.

V. EXPERIMENTAL RESULTS

The proposed algorithm shows the accuracy of any image type in this experiment, and the data set received from the internet is set to Ts=0.5 by maintaining the similarity threshold. We created a mechanism in our work that provides us with proper interpretations of the detection of copy-move forgery. We used images of various shapes and sizes to calculate the accuracy of this dedicated algorithm that can precisely detect the regions that have been affected.

VI. AUTHOR'S CONTRIBUTIONS

Image forgery detection using SIFT algorithms (Scale – Invariant Feature Transformation) was presented in [2], but in that paper, no parameters were calculated, no quantitative results were evaluated for methodologies adopted as true or false positives [1]. Another recent work by [2] authors is unable to manage the reliability transformation through different parameters with quantitative results. The proposed method demonstrates the experimental result with a reliable and inconsistent estimation of the transformation parameters, the proposed method works at a unique threshold that maintains the training procedure where extraction of key points is difficult, but the SIFT feature can determine the maximum detection of tampering by extracting features and matching key-point clustering.

VII. CONCLUSION

Although a large number of algorithms were proposed to resolve issues related to image authenticity, this paper is dedicated to select the best performance CPTD algorithms and features. The experiments are performed on different images. Compared to others, the proposed work shows better results for the effective detection of forged images. It takes 241 seconds to calculate the SIFT keys and their descriptors and finds a total of 705 matches. Future research will focus on improvement for multiple images cloned detection and extremely identical textures where key points were not recovered through the SIFT technique.

Table 1 Analysis of Comparative existing methodologies Using SIFT.

References	Approaches	Advantages	Limitations
Xunyu Pan *et al.* [2010]	Duplicate Region Detection by Feature Matching is collected for finding the fine transform between matched key-points. Correlated region mapped to locate duplicated regions	Multiple duplicated regions are detectable.	Difficult to detect Visual structure regions with a high true negative rate.
E.Ardizzone *et al.* [2010]	Using SIFT key-point clustering, Similar cluster matching and texture-based analysis detection of multiple tampering is possible to match an automatic step approach for the hierarchical tree Clustering process.	Robust jpeg compression analyzed to differentiate the matching process.	Clusters with very few points to detect Similarity of the detected points.
Irene Amerini *et al.* [2011]	SIFT algorithm used for the extraction of features, similar components, geometric transformation and clustering of hierarchies. The 2NN generalized iterative test used to detect similar key points.	Multiple cloned regions are detectable.	Not able to detect uniform texture having salient key-points.
Baina Su *et al.* [2012]	Lpp-SIFT plus Locality Preserving Projections used to obtain reduced feature dimension descriptors.	speed up the process of CMF detection using the dimension reduction method	Flat surfaces with the small area are not effectively detectable the forged regions.
Lu Liu *et al.* [2014]	Improved detection by using a SIFT-based approach and Clustering Colour Filter Array (CFA) features of broad first search neighbors.	Discriminates original and forged regions for multiple cloning.	Not able to detect flat CMFD.
TakwaChihaoui *et al.* [2014]	CMFD using Sift Descriptors and Svd-Matching Calculating correlation and vector proximity matrix and matching points create a fusion step for calculation.	Automatically helpful for finding duplication in image regions.	False point matching Problems are reduced.
Sudhakar. K *et al.* [2014]	SIFT-based Copy Move Forgery Detection uses segmented image using a chan-vase segmentation method to speed up the level set approach and key points for ROI are matched for copy-moved region detection.	A robust and simple implementation of Multiple-forged object Detection.	The fixed threshold used for the matching process and boundary Properties are not including the regional properties.
Ramesh Chand Pandey *et al.* [2014]	Detection of forgery based on SURF and SIFT by using extraction features through the g2NN procedure to detect similar feature components.	Detection of forgery by fusing two features that help to increase robustness inefficiency	For the detection of multiple cloned regions where patch textures are highly uniform, the runtime was high and inefficient.

Mohammad FarukhHashmi *et al*. [2014]	DWT and SIFT Features dimensionality reduced where Sift features to extract the LL part of the DWT to an analyzed image.	Reduced the complexity computation with high accuracy.	The efficiency of block-based methods affected by image size.
Jian Li *et al*. [2015]	Segmentation-based forgery detection by confirming the existence of CMF via a transform matrix to find doubtful matches with rough transform matrix.	Detecting only the very small size of 32x32	The re-estimation of the Transformation matrix is very slow in speed detection.
Proposed Method	SIFT features and descriptors detect the similar features matching techniques using interpolation, smoothing orientation histogram and sorting descriptor by reducing scale order	Obtained high accuracy for finding duplication in image regions.	Calculation time needs to be reduced.

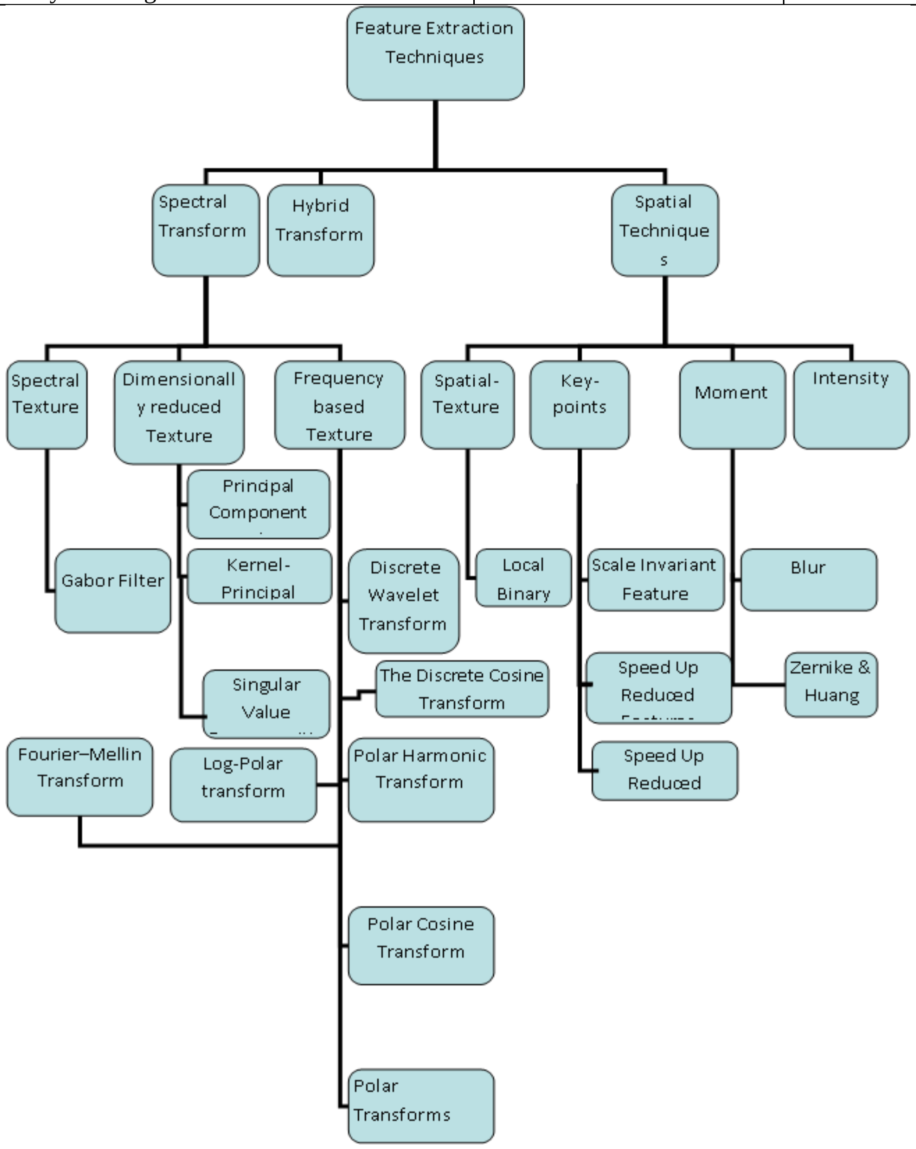


Figure 1. Feature Extraction Approaches.

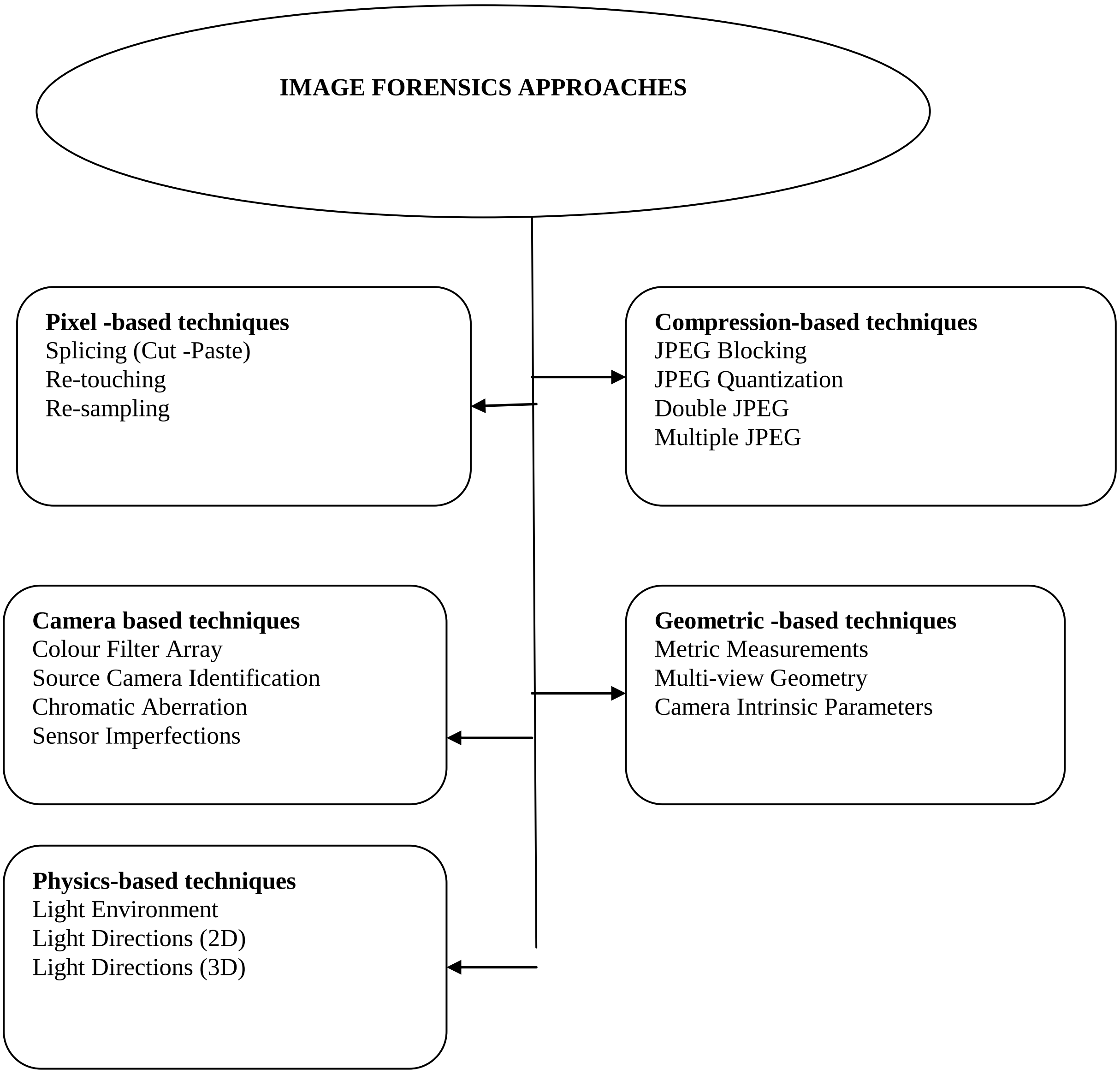


Figure 2. Classification of Forgery detection Image Authentication methods.

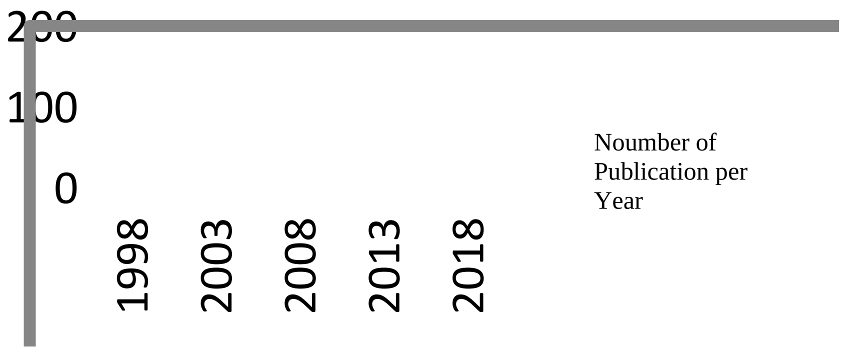


Figure 3: Number of Publication Indexed by Scopus for Copy-Move Tempering Detection.

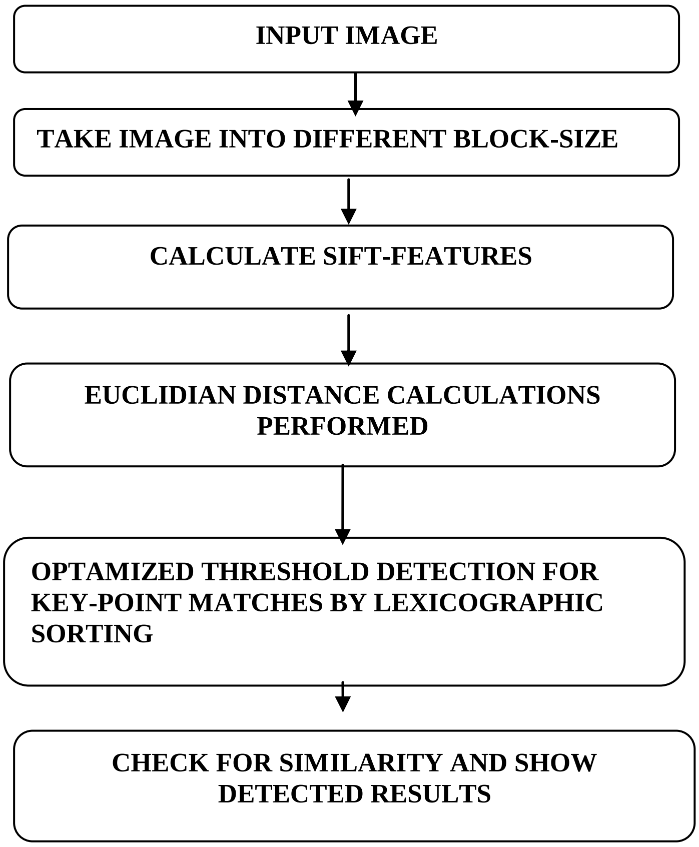

INPUT IMAGE
TAKE IMAGE INTO DIFFERENT BLOCK-SIZE
CALCULATE SIFT-FEATURES
EUCLIDIAN DISTANCE CALCULATIONS PERFORMED
OPTAMIZED THRESHOLD DETECTION FOR KEY-POINT MATCHES BY LEXICOGRAPHIC SORTING
CHECK FOR SIMILARITY AND SHOW DETECTED RESULTS

Figure 4. Proposed Procedure for the CMTD.

Table 2. Accuracy and precision of the proposed method calculation.

1. False Positive Rate (FPR) = False Positive / (True Negative + False Positive)
2. False Negative Rate (FNR) = False Positive / (True Positive + False Positive)
3. Sensitivity (TPR) = True Positive / (True Positive + False Negative)
4. Specificity (TNR) = True Negative / (True Negative + False Positive)
5. Precision = True Positive / (True Positive + False Positive)
6. Accuracy = True Positive + True Negative /(True Positive + True Negative + False Positive+ False Negative)
7. Final score =2 True Positive / (2 True Positive + False Positive + False Negative)

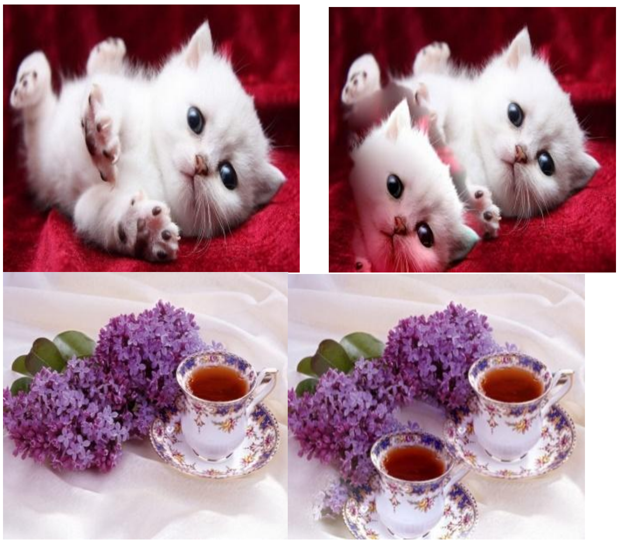


Figure 5. Original Images and Tempered Images.

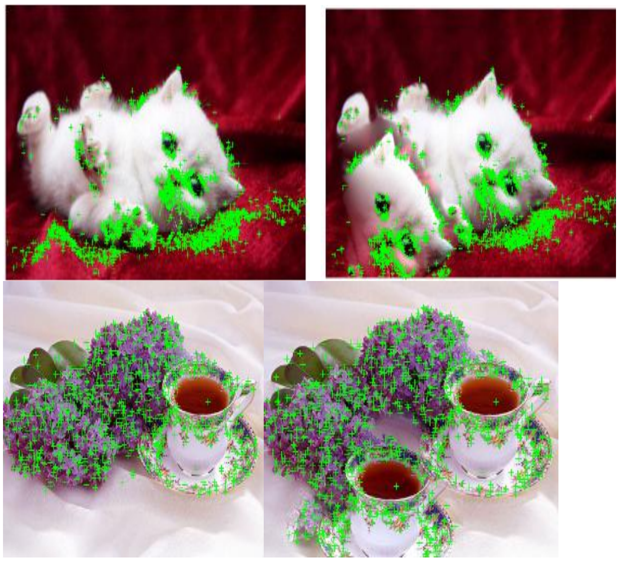


Figure6. Images with key points mapped onto it.

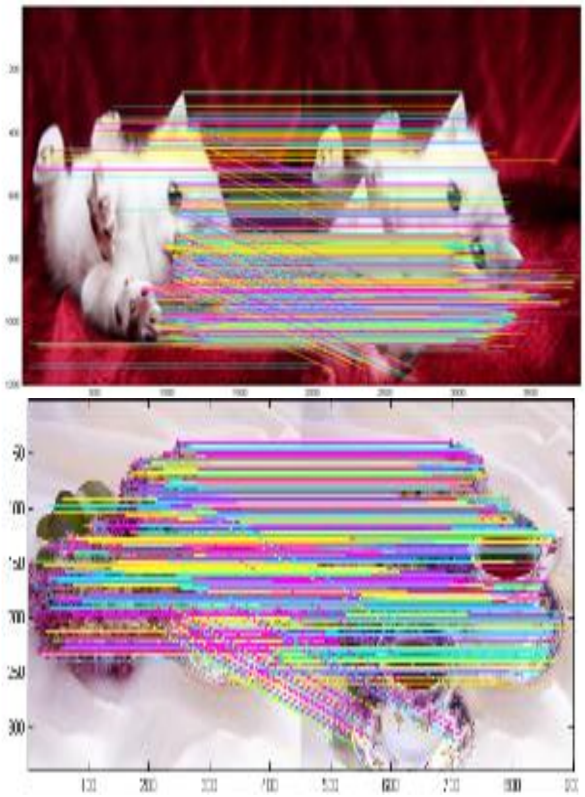
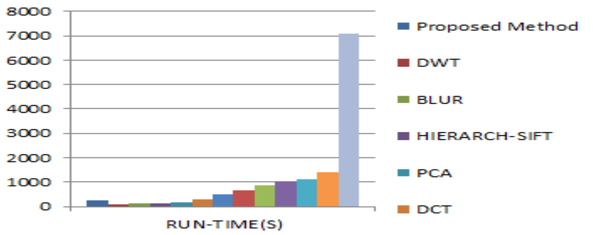


Figure 7. Duplicated regions match.



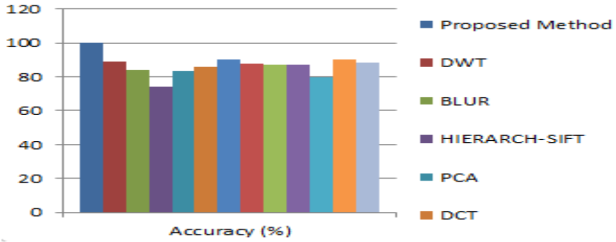


Figure8. Execution Time Comparative Result Analysis.
Figure 9. Accuracy Comparative Result Analysis of Proposed Method.

Table3. Run time Comparison with existing work of the proposed work.

Method	References	Time (s)	Accuracy (%)
Proposed Method		241.00	99.08
DWT	Bashar *et al* [56]. [2010]	96.60	89.22
BLUR	Mahdian and Saic *et al* [35]. [2006]	113.19	84.09
HIERARCH-SIFT	Amerini *et al* [3]. [2011]	142.13	73.95
PCA	Popescu and Farid *et al* [1]. [2004]	180.11	83.47

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

DCT	**Fridrich** *et al*[2]**. [2003]**	**296.74**	**86.00**
Malty scale analysis	**Silva, E** *et al*[32]**. [2015]**	**515.00**	**90.00**
Overseg	**C.-M. Pun** *et al*[78]**. [2010]**	**683.00**	**88.00**
KPCA	**Bashar** *et al*[39]**. [2010]**	**880.00**	**87.44**
SURF	**B.L. Shivakumar,** *et al*[4]**. [2011]**	**1052.00**	**87.00**
SIFT	**I. Amerini** *et al*[75]**. [2013]**	**1098.00**	**80.00**
ZERNIKE2	**Ryu** *et al*[69]**. [2013]**	**1418.68**	**90.10**
ZERNIKA	**Ryu** *et al*[70]**. [2010]**	**7065.00**	**88.08**

REFERENCES

1. A.C. Popescu, H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Tech. Rep. TR 2004-515, Dept. of Computer Science –Dartmouth College, Hanover, USA.2004.
2. J. Fridrich, D. Soukal, J. Lukas, "Detection of copy-move forgery in digital images, in: Digital Forensic Research" Workshop (DFRWS), Cleveland, USA, pp.134–137.2003.
3. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 PART 2, pp. 1099–1110, 2011.
4. B.L. Shivakumar, S. Baboo, "Detection of region duplication forgery in digital images using SURF", Int. J. Comput. Sci. Issues 8 PP.199–205, 2011.
5. Anon, Wang, Xiaofeng; Pang, Kemu; Zhou, Xiaorui; Zhou, Yang; Li, Lu; X -- "A Visual Model-Base" IEEE Transactions on Information Forensics and Security Volume 10 issue 7.pdf.2015.
6. S. Amtullah and D. A. Koul, "Passive Image Forensic Method to detect Copy Move Forgery in Digital Images," IOSR J. Comput.Eng., vol. 16, no. 2, pp. 96–104, 2014.
7. O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic Sci. Int., vol. 231, no. 1–3, pp. 284–295, 2013.
8. R. C. Pandey, S. K. Singh, K. K. Shukla, and R. Agrawal, "Fast and robust passive copy-move forgery detection using SURF and SIFT image features," 9th Int. Conf. Ind. Inf. Syst. ICIIS 2014, 2015.
9. J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Sci. Int., 2013.
10. Hashmi, M.F., Hambarde, A.R. &Keskar, A.G., "Copy move forgery detection using DWT and SIFT features."International Conference on Intelligent Systems Design and Applications, ISDA, pp.188–193.2014.
11. Zhang, Z. et al., "A survey on passive-blind image forgery by doctor method detection". Proceedings of the 7th International Conference on Machine Learning and Cybernetics, ICMLC, 6(July), pp.3463–3467.2008.
12. H.-J. Lin, C.-W.Wang, Y.-T.Kao, "Fast copy-move forgery detection," WSEAS Trans. Signal Process. (WSEAS-TSP) PP.188–197. 2009.
13. M. F. Hashmi, V. Anand, and A. G. Keskar, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform," AASRI Procedia, vol. 9, no. Csp, pp. 84–91, 2014.
14. S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," 2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc., pp. 706–710, 2017.
15. S. M. Fadl and N. A. Semary, "A proposed accelerated image copy-move forgery detection," 2014 IEEE Vis. Commun. Image Process.Conf. VCIP 2014, pp. 253–257, 2015.
16. I. Amerini, R. Becarelli, R. Caldelli, and A. Del Mastio, "Splicing forgeries localization through the use of first digit features," 2014 IEEE Int. Work. Inf. Forensics Secur.WIFS 2014, pp. 143–148, 2015.
17. A. Gupta, N. Saxena, and S. K. Vasistha, "Detecting Copy move Forgery using DCT," Int. J. Sci. Res. Publ., vol. 3, no. 5, pp. 3–6, 2013.
18. T. Bashir, I. Usman, S. Khan, and J. Rehman, "Intelligent reorganized discrete cosine transform for reduced reference image quality assessment Tariq BASHIR," pp. 1–25, 2017.
19. G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digit. Investig., vol. 10, no. 3, pp. 226–245, 2013.
20. K. Boonsivanon and A. Meesomboon, "IKDSIFT: An Improved Keypoint Detection Algorithm Based-on SIFT Approach for Non-uniform Illumination," ProcediaComput. Sci., vol. 86, no.March, pp. 269–272, 2016.
21. B. P. Rinky, P. Mondal, K. Manikantan, and S. Ramachandran, "DWT based Feature Extraction using Edge Tracked Scale Normalization for Enhanced Face Recognition," Procedia Technol., vol. 6, pp. 344–353, 2012.
22. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics," ProcediaComput. Sci., vol. 79, pp. 458–465, 2016.
23. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A Survey on Keypoint Based Copy-paste Forgery Detection Techniques," Phys. Procedia, vol. 78, no. December 2015, pp. 61–67, 2016.
24. L. Li, S. Li, H. Zhu, and X. Wu, "Detecting copy-move forgery under affine transforms for image forensics," Comput. Electr.Eng., vol. 40, no. 6, pp. 1951–1962, 2014.
25. I. Amerini, R. Becarelli, R. Caldelli, and M. Casini, "A Feature-Based Forensic Procedure for Splicing Forgeries Detection," vol. 2015, 2015.
26. M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," Int. Conf. Intell. Syst. Des. Appl. ISDA, pp. 188–193, 2014.
27. J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 507–518, 2015.
28. E. S. M. El-Alfy and M. A. Qureshi, "Combining spatial and DCT based Markov features for enhanced blind detection of image splicing," Pattern Anal. Appl., vol. 18, no. 3, pp. 713–723, 2015.
29. A. Annis Fathima, R. Karthik, and V. Vaidehi, "Image stitching with combined moment invariants and sift features," ProcediaComput.Sci., vol. 19, no.Ant, pp. 420–427, 2013.
30. R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," Forensic Sci. Int., vol. 231, no. 1–3, pp. 61–72, 2013.
31. J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 507–518, 2015.
32. E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," J. Vis. Commun. Image Represent., vol. 29, pp. 16–32, 2015.
33. N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Salleh, and F. Othman, "SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack," J. Vis. Commun. Image Represent., vol. 46, pp. 219–232, 2017.
34. R. K. Karsh, R. H. Laskar, and Aditi, "Robust image hashing through DWT-SVD and spectral residual method," EURASIP J. Image Video Process., vol. 2017, no. 1, p. 31, 2017.
35. B. Mahdian, S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants", Forensic Sci. Int. PP. 180–189, 2006.
36. S. Bayram, H.T. Sencar, N. Memon, "An efficient and robust method for detecting copy-move forgery", in: Intl. Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1053–1056. 2009.
37. D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image," ProcediaComput. Sci., vol. 85, no.Cms, pp. 206–212, 2016.
38. H. Hailing, G. Weiqiang, and Z. Yu, "Detection of copy-move forgery in digital images using sift algorithm," in Proceedings - 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA 2008, 2008.

39. M. M. Isaac and M. Wilscy, "Image Forgery Detection Based on Gabor Wavelets and Local Phase Quantization," ProcediaComput. Sci., vol. 58, pp. 76–83, 2015.
40. R. Kaushik, R. K. Bajaj, and J. Mathew, "On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments," ProcediaComput.Sci., vol. 70, pp. 130–136, 2015.
41. M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 11, pp. 2499–2512, 2016.
42. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "Computationally Efficient Digital Image Forensic Method for Image Authentication," ProcediaComput. Sci., vol. 78, no.December 2015, pp. 464–470, 2016.
43. L. Verdoliva, D. Cozzolino, and G. Poggi, "A feature-based approach for image tampering detection and localization," 2014 IEEE Int. Work. Inf. Forensics Secur.WIFS 2014, pp. 149–154, 2015.
44. G. Ulutas, A. Ustubioglu, B. Ustubioglu, V. V. Nabiyev, and M. Ulutas, "Medical Image Tamper Detection Based on Passive Image Authentication," J. Digit.Imaging, pp. 1–15, 2017.
45. T. P. Shiji, S. Remya, and V. Thomas, "Computer Aided Segmentation of Breast Ultrasound Images Using Scale Invariant Feature Transform (SIFT) and Bag Of Features," ProcediaComput. Sci., vol. 115, pp. 518–525, 2017.
46. R. Raj and N. Joseph, "Keypoint Extraction Using SURF Algorithm For CMFD," Procedia - ProcediaComput.Sci., vol. 93, no.September, pp. 375–381, 2016.
47. K. Sudhakar, V. M. Sandeep, and S. Kulkarni, "Shape Based Copy Move Forgery Detection Using Level Set Approach," 2014 Fifth Int. Conf. Signal Image Process., pp. 213–217, 2014.
48. K. Sitara and B. M. Mehtre, "Digital video tampering detection: An overview of passive techniques," Digit. Investig., vol. 18, pp. 8–22, 2016.
49. Sunanda Gupta, Naresh Grover, Zaheerudin. "A Novel Approach For Intensity Based Non- rigid Image Registration Using Powell's Algorithm". Int. J. Biomedical Engineering and Technology, United KingdomVol. 24, No. 2, pp.103–120.2017.
50. Sunanda Gupta, S. K. Chakarvarti, Zaheerudin ,"Medical image registration based on fuzzy c-means clustering segmentation approach using SURF". Int. J. Biomedical Engineering and Technology, United Kingdom, Vol. 20, No. 1, pp.33–50. 2016.
51. Sunanda Gupta, Naresh Grover, Zaheerudin"A New Optimization Approach Using Smoothed Images Based On ACO for Medical Image Registration". International Journal of Information Engineering and Electronic Business (IJIEEB), Hong Kong, Vol.8, No.2 , pp. 30-36. March 2016.
52. Sunanda Gupta, S. K. Chakarvarti, Zaheerudin"Medical Image Registration Using Cauchy- Schwarz Inequality via Template Matching".American Journal of Algorithms and Computing, Vol. 3 No. 1, pp. 14-25.2016.
53. Sunanda Gupta, S. K. Chakarvarti, and Zaheerudin, "Feature Points Extraction of an Image based on Ant Colony Optimization Technique" International Conference on Paradigm Shift in Management and Technology (PSIMT-2015) at YMCA on April 3-5.2015.
54.] Sunanda Gupta, S. K. Chakarvarti, and Zaheerudin, **"**Image Registration Methods: A Short Review" American Journal of Algorithms and Computing (2013) Vol. 1 No. 1, Dec. pp. 39-49.2013 .
55. Sunanda Gupta, Charu Gupta, S.K. Chakarvarti, "Image Edge Detection: A Review" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) ISSN: 2278 – 1323, Volume 2, Issue 7, pp 2246-2251,2013.
56. M. Bashar, K. Noda, N. Ohnishi, K. Mori,"Exploring duplicated regions in natural images, Trans. Image Process." 2010.
57. M. J. Malachowski and J. Zmija, "Organic field-effect transistors," Opto-Electronics Rev., vol. 18, no. 2, pp. 121–136, 2010.
58. A. V. Malviya and S. A. Ladhake, "Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto ColorCorrelogram," ProcediaComput. Sci., vol. 79, pp. 383–390, 2016.
59. E. Matsuyama et al., "A Modified Undecimated Discrete Wavelet Transform Based Approach to Mammographic Image Denoising," J. Digit. Imaging, vol. 26, no. 4, pp. 748–758, 2013.
60. M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal Process. Image Commun., vol. 39, pp. 46–74, 2015.
61. G. Lynch, F. Y. Shih, and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Inf. Sci. (Ny)., vol. 239, 2013.
62. J.-W. Wang, G.-J.Liu, Z. Zhang, Y.-W. Dai, Z.-Q. "Wang, Fast and robust forensics for image region-duplication forgery,"Acta Automat.Sinica35 , PP.1488–1495. 2010.
63. M. Kirchner, P. Schöttle, and C. Riess, "Thinking beyond the block: block matching for copy-move forgery detection revisited," vol. 9409, p. 940903, 2015.
64. A. Kuznetsov and V. Myasnikov, "A new copy-move forgery detection algorithm using image preprocessing procedure," Procedia Eng., vol. 201, pp. 436–444, 2017.
65. A. Li, W. Jiang, W. Yuan, D. Dai, S. Zhang, and Z. Wei, "An Improved FAST + SURF Fast Matching Algorithm," Procedia - ProcediaComput. Sci., vol. 107, no.Icict, pp. 306–312, 2017.
66. W. Lin et al., "Survey on blind image forgery detection," IET Image Process., vol. 7, no. 7, pp. 660–670, 2013.
67. Lowe, G., "SIFT - The Scale Invariant Feature Transform."International Journal, 2, pp.91–110.2004.
68. A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, "Vision of the unseen," ACM Comput.Surv., vol. 43, no. 4, pp. 1–42, 2011.
69. S.-J. Ryu, M. Kirchner, M.-J.Lee, H.-K. Lee, "Rotation invariant localization of duplicated image regions based on zernike moments", Trans. Inform. Forensics Secur.(T.IFS) 8 (8) PP.1355–1370.2013.
70. S.-J. Ryu, M.-J.Lee, H.-K. Lee, "Detection of copy-rotate-move forgery using zernike moments", in: Intl. Workshop in Information Hiding (IHW), pp.51–65.2010.
71. S. C. Satapathy, B. N. Biswal, S. K. Udgata, and J. K. Mandal, "Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014," Adv. Intell. Syst. Comput., vol. 327, pp. 659–666, 2014.
72. X. Song, S. Wang, S. Yiu, L. Jiang, and X. Niu, "Detection of image region duplication using spin image," IEICE Trans. Inf. Syst., vol. E96–D, no. 7, pp. 1565–1568, 2013.
73. [73] B. Su and K. Zhu, "Detection of copy forgery in digital images based on LPP-SIFT," Proc. 2012 Int. Conf. Ind. Control Electron.Eng. ICICEE 2012, pp. 1773–1776, 2012.
74. [74] D. Tralic, S. Grgic, X. Sun, and P. L. Rosin, "Combining cellular automata and local binary patterns for copy-move forgery detection," Multimed. Tools Appl., vol. 75, no. 24, pp. 16881–16903, 2016.
75. B. Ustubioglu, G. Ulutas, M. Ulutas, and V. V. Nabiyev, "A new copy-move forgery detection technique with automatic threshold determination," AEU - Int. J. Electron.Commun., vol. 70, no. 8, pp. 1076–1087, 2016.
76. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics," ProcediaComput. Sci., vol. 79, pp. 458–465, 2016.
77. X.B. Kang, S.M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", in: International Conference on Computer Science and Software Engineering, 2008, vol. 3, pp. 926–930. 2010.
78. C.-M. Pun, X.-C.Yuan, and X.-L. Bi, "Image forgery detection using adaptive over-segmentation and feature points matching," IEEE Trans. Inf. Forensics Security, vol. PP, pp. 1-1.2015.
79. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," Signal Process. Image Commun., 2013.

AUTHORS PROFILE

Ms Monika received her B. Tech degree in application of Electronics and Communication Engineering in 2007and M. Tech degree in ECE in 2011 both from MDU Rohtak, Haryana. From 2007 to 2019, she was an Assistant Professor in Manav Rachna International Institute of Research and Studies, Faridabad, NCR, India. She is currently working towards the PhD degree in ECE at MRIIRS FARIDABAD. Her research interest includes image processing, image forensics, Digital Logics.

Dr Dipali Bansal is the Director-IQAC and Associate Dean - Academics with Manav Rachna International Institute of Research and Studies, Faridabad, NCR, India. Dr Bansal is a doctorate in Bio signal processing from Jamia Milia University, New Delhi and an upcoming and young scientist. She has got a distinguished career in teaching and industry spanning 22 years and her research work has found prominent recognition and has been published in many national and international journals and conferences (80 papers). She has attended many International conferences abroad primarily at Washington D.C and Los Angeles USA and Italy (Florence). She is a Reviewer of many journals including the journal of Medical and Biological Engineering and Computing (Springer), Computers in Biology and Medicine, Elsevier Journal (Science Direct), and Journal of Circuits, Systems, and Signal Processing.