ISSN (Online) 2456-1290

International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)

Vol 5, Issue 12, December 2020

Copy-Move Image Forgery Detection using Scale Invariant Feature Transform

[1] P. Parimala, [2] Mrs. A. Naveena

[1] M.Tech student, ETM Dept., GNITS, Hyderabad, India
[2] Assistant Professor, ETM Dept., GNITS, Hyderabad, India
[1] palaneni.pari@gmail.com, [2] naveenaambidi@gmail.com

***Abstract*---Digital image forgery is a one of multimedia security whose objective is to show the wicked manipulations in digital images. Among different types of image forgery, copy–move forgery detection (CMFD) is the most popular one where a part of the original image is copied and pasted at another position in the same image. Various methods have been developed in the past few years. to achieve geometric transformation like rotation and scaling, a novel methodology based on Scale Invariant Features Transform (SIFT) is proposed.**

The proposed algorithm mainly involves in feature matching in which features are extracted from each block by computing the dot product between the unit vectors. Random Sample Consensus (RANSAC) algorithm is used to remove the false positive matches. The experimental results of the algorithm are presented to confirm that the technique can extract more accurate results compared with existing forgery detection methods.

***Keywords*--- SIFT, RANSAC, CMFD, KEYPOINT MATCHING**

I. INTRODUCTION

Digital images are widely used everywhere in the world. Newspapers, magazines, apparel industry, medical field, science field, forensic labs etc. are relied on digital images. Exchanging soft copies of several documents may be normal practice in the present scenario. So, there is a chance of forgery while exchanging such sort of documents.

Detection of image manipulation is extremely important because an image is often used as legal evidence, in forensics investigations, and in many other fields. The pixel-based image forgery detection aims to verify the authenticity of digital images with no prior knowledge of the first image.

II. COPY-MOVE IMAGE FORGERY DETECTION:

An image forgery is called as Copy-Move forgery [5] if some part of an image is copied and pasted within that same image. This is usually done to suppress some information of the image. There must be a possibility that one or more regions are copied and moved into the image. Due to the duplicated portion or portions comes from the same image, the properties of the duplicated region will be same as the original region. detection methods must be consistent with the statistical measures presented in each part of the images. the example of copy-move image forgery detection shown in the Figure 1.

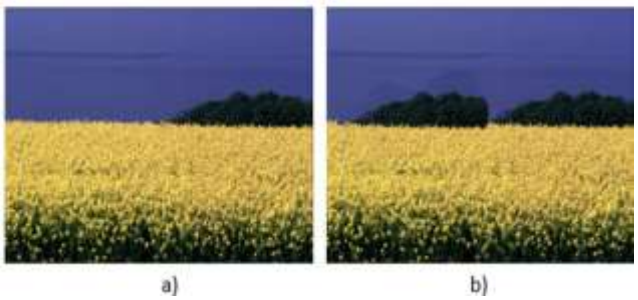

Fig 1: Copy Move Forgery a) Original image b) Tampered image

The figure 1 is a example of the cloning technique where the region of image is copied and pasted within the image in such a way that it is not recognizable with naked eye. this process is considered as an illegal act, the appropriate technique must be developed to detect the forged region accurately.

III. RELATED WORK

In the copy-move forgery detection, block-based methods that is DCT (discrete cosine transform) [8], DWT (discrete wavelet transform) [11]gives the proper results only when the copied region is directly pasted i.e. duplication is performed without any transformations. If the copied region is transformed geometrically then block based methods fail to detect the forgery [3]. so, to detect the tampered region accurately even after applying geometric transformation like rotation and scaling and to reduce the computational complexity, key based technique i.e. SIFT (scale invariant feature transform) [4] is proposed.

IV. PROPOSED ALGORITHM

To overcome the issues existing in block-based methods used for copy move image forgery detection. obtain geometric transformation like rotation and scaling by using key based technique. to reduce computational complexity, improve accuracy and precision by implementation of SIFT technique [1].

Copy move image forgery detection using Scale Invariant Feature Transform is a key based method. SIFT [6] is an algorithm used to extract features from digital images. these features are scale invariant and rotation invariant. SIFT works on geometric transformations of an image like scaling, rotation. Key points descriptor matching can find region duplication detection. tampered detection is possible irrespective of its size and angle with proposed method [12].

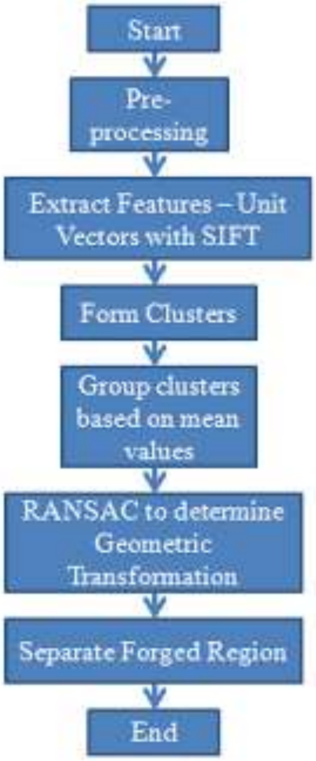
Start
Pre-processing
Extract Features – Unit Vectors with SIFT
Form Clusters
Group clusters based on mean values
RANSAC to determine Geometric Transformation
Separate Forged Region
End

Fig. 2: Proposed block diagram

Proposed model is mainly based on the SIFT algorithm which can detect tampered regions in a copy-move forged image. Firstly, input image is converted from RGB to Gray scale, which is passed as input parameter in SIFT algorithm to extract the descriptor vectors. copy-move tampering is detected by applying the matching operation on the descriptor vectors. Finally, the RANSAC algorithm is applied to remove outliers that help to reduce the false positive rate. The block diagram of our proposed model is shown in Figure 2.

1. SIFT algorithm is designed with following major steps:

1. Scale space extrema detection
2. key-point localization
3. Assignment of Orientation
4. Sift descriptor generation:
5. Clustering
6. Feature matching
7.False match removal

1.1. Scale Space Extrema Detection:

This phase of the filtering attempts to identify those locations and scales that are identifiable from different viewpoints of the same object. This can be efficiently done by using a "scale space" function. Further it has been shown under reasonable assumptions based on the Gaussian function.

The scale space is defined by the function:

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

G (x, y, σ) is a Gaussian function and I (x, y) is the input image.

Various techniques can then be used to find stable keypoint locations in the scale-space. Difference of Gaussians is one such method, locating scale-space extrema, D (x, y, σ) by calculating the difference between two images, one with scale k times the other. D (x, y, σ) is then provided by:

$$D\ (x, y, \sigma) = L\ (x, y, k\sigma) - L\ (x, y, \sigma)$$

To find the local maxima and minima of D (x, y, σ) each point is matched with its 8 neighbours at the same scale, and its 9 neighbours up and down one scale. If this significance is the minimum or maximum of all these points, then this point is an extrema.

In this step Gaussian of Difference (DoG) is used to find possible points of interest which are invariant to orientation and scaling. Efficient and stable DoG Function D (x, y, σ) is required to detect the more reliable key-points. It is computed by convolving the difference of two nearby scales separated by a constant scaling factor k with the input image as shown in the Figure 3.

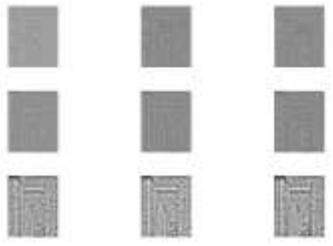

Fig 3: DoG Pyramid Formation of Approximate Image

1.2. Key-point Localization:

This stage tries to exclude more points from the list of keypoints by finding those that have low contrast or poorly localised on an edge. This is accomplished by calculating the Laplacian value for each keypoint found in stage 1. The location of extrema **z** is given by

$$\mathbf{z} = -\frac{\partial^2 D}{\partial \mathbf{x}^2}^{-1} \frac{\partial D}{\partial \mathbf{x}}$$

If the function value at **z** is below a threshold value, then this point is excluded. this removes extrema with low contrast. To eradicate extrema based on poor localisation it is noted that in these cases there is a large principle bend across the edge but a small curve in the perpendicular direction in the difference of Gaussian function. If this difference is less than the ratio of largest to smallest eigenvector, from the 2x2 Hessian matrix at the location and scale of the keypoint, the keypoint is rejected.

Low contrast key-points can be rejected by using key-point localization and on basis of image gradient orientation of key-points is done which is shown in Figure 4.

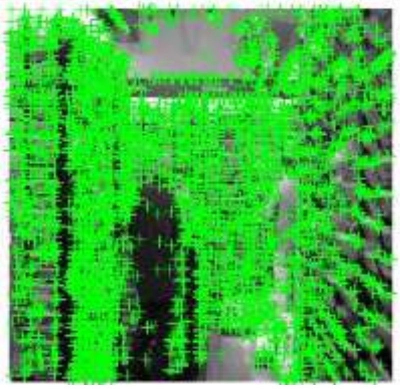

Fig 4: Initial Location of Key-points of Different Views Component

In this step more accurate key-points are selected. Taylor series expansion of scale space is applied and those extrema with intensity value less than a predefined threshold value are rejected. The accurately selected key-points on the approximate image after discarding the ones having poor contrast are shown in Figure 5.

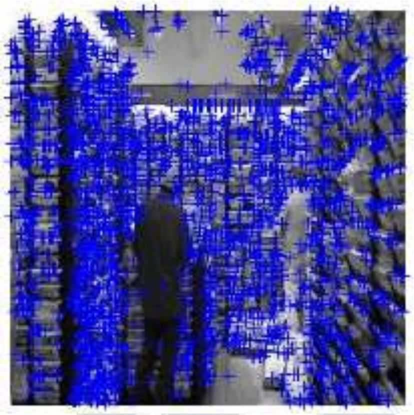

Fig 5: Accurately Selected Key-points

1.3. Assignment of Orientation:

This step aims to assign a consistent orientation to the keypoints based on local image properties. each key-point is given an orientation with respect to the local image properties. Histogram of oriented gradient is used to calculate gradient direction of feature points. Dominant direction of the local gradients is represented by orientation histogram peaks.

keypoint descriptor can then be represented relative to this orientation, to achieve the invariance to rotation. The approach taken to find an orientation is: use the key points scale to select the Gaussian smoothed image L

Compute gradient magnitude *m*

$$m(x,y) = \sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2}$$

Compute orientation θ

$$\theta(x,y) = \tan^{-1}((L(x,y+1) - L(x,y-1))/(L(x+1,y) - L(x-1,y)))$$

Form an orientation histogram from gradient orientations of sample points, the highest peak in the histogram is located. this peak is used and any other local peak within 80% of the height of this peak creates a keypoint with that orientation.

1.4. Sift descriptor generation:

Each keypoint has a location, scale, orientation. a 16x16 window around the keypoint is taken. It is divided into 16 sub-blocks of 4x4 size and compute a descriptor for the local image region about each keypoint that is highly distinctive and invariant as possible to variations such as changes in viewpoint and illumination.

This feature vector introduces a few complications. To get rid of complications before finalizing the fingerprint, 4 X 4 descriptors across 16 X 16 sample arrays were used. 4 X 4 X 8 directions gives 128 bin values. It is characterized as a feature vector to form a keypoint descriptor. The feature vector uses gradient orientations. Apparently, if the image is rotated, everything changes. All gradient orientations also change. To accomplish rotation independence, the key point's rotation is subtracted from each orientation. Thus, each gradient orientation is comparative to the key point's orientation. If threshold numbers are big, illumination independence can be achieved. So, any number (of the 128) greater than 0.2 is modified to 0.2. This resultant feature vector is normalized again. The key-point descriptors shown on the right are generated by orientation histogram over 4x4 sample regions.

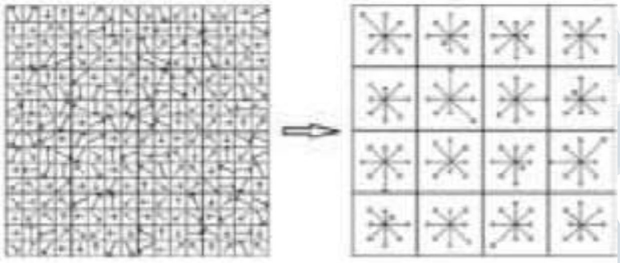

Fig.6: SIFT descriptor generation

In the figure 6 each histogram is observed in 8 directions with length corresponding to the magnitude. It has 128 elements dimension of key-point descriptors. However, it uses 4x4 array location grid and 8 orientation bins in each sample.

1.5. Clustering:

Clustering is the method of dividing objects into sets that are similar and dissimilar to the objects belonging to another set.

Two different types of clustering, each divisible into two subsets

[1] Hierarchical clustering:

- Agglomerative
- Divisive

[2] Partial clustering:

- K-means
- Fuzzy c-means

Every kind of clustering has its own purpose and numerous use cases.

In fig 7, Agglomerative clustering can be observed which is also known as a bottom-up approach. Consider it as bringing things together. Agglomerative hierarchical clustering is used to group the extracted SIFT key-point descriptors. Linkage ward method is used to complete the clustering process.

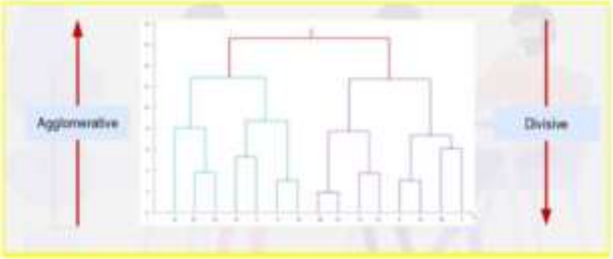

Fig 7: Hierarchical clustering

1.6. Feature matching:

The most basic approach is to take a given keypoint in the query and find the keypoint that is closest to the target. the contest in comparing keypoints between query image and database of images. A minor improvement on top of this is to neglect those points which match well with many other points in the target. Such points considered as non-descriptive.

The extracted Scale invariant feature transform features in the irregular blocks are matched by computing the Dot products between unit vectors. this dot product calculates the sequence of two equal lengths and in return it gives a single number. It only matches the vector angles ratio which is less than the distance ratio of nearest and second nearest neighbour. The dot product is given as

$$a.b = |ab^T|$$

It must be checked whether the nearest neighbour has angle less than distance ratio.

$$a.b = |a||b|\cos(\theta)$$

Now apply inverse cosine transform to the Dot product and match the nearest neighbour. It is observed in fig 8.

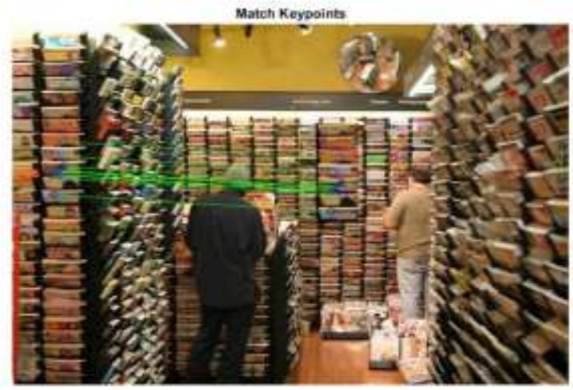

Fig 8: Key point matching within single image

1.7. False Matches Removal:

This algorithm is used to remove false positive matches. RANSAC [7] is used as the mismatched points or outliers can obstruct the estimated homography. In the RANSAC algorithm, a set of matched points are randomly selected and then the homography is estimated. 8 After that other remaining matched points are transformed and then compared in terms of distance with their respective matches. A threshold value is set. If this distance is less than threshold value it is marked as inliers and if it is above the threshold is catalogued as outliers. the estimated transformation which is associated with the higher number of inliers is chosen 50 after predefined number of iterations. it has been set to 1000 and the threshold to 0.05; this is 52 This transformation is applied independently to both two areas. a constatation is that the info consists of "inliers", i.e., data whose distribution are often 39 explained by some set of model parameters, though could also be subject to noise, and outliers that don't fit the perfect. The outliers can come, for instance, from extreme values of the noise or incorrect hypotheses about the interpretation of knowledge. RANSAC also assumes that, given a small set of inliers, exists a procedure which may estimate the parameters of a model that optimally fits this data.

V. DATA COLLECTION:

Proposed model is designed to detect multifarious types of copy-move forgery such as copy-move without geometric translation, with geometric transformation including rotation and scaling, a dataset of images is required which contains both the original images and forged images. To meet the requirement, the MICC-F220[2] dataset which has 110 original images and 110 forged images has been chosen. Moreover, the proposed model can detect forgeries in images having blur or noise.

VI. RESULTS AND DISCUSSION:

Proposed model applied over the standard dataset MICC-F220[2] as well as some own images. The outputs of the existing and the proposed system simulated using MATLAB is presented here. gray scale image is given as an input parameter in the SIFT algorithm to extract the descriptor vectors. Conclusively, matching operation is performed on the descriptor vectors to detect copy-move tampering.

The performance of the proposed model is observed by calculating accuracy, specificity, sensitivity and false positive rate.

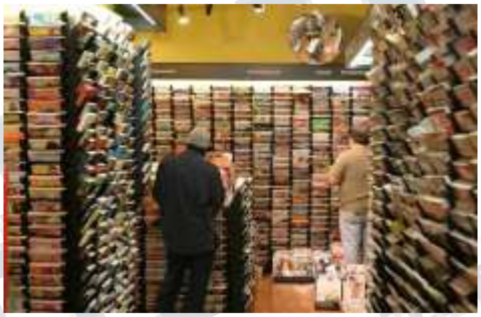

Fig 9: Original image

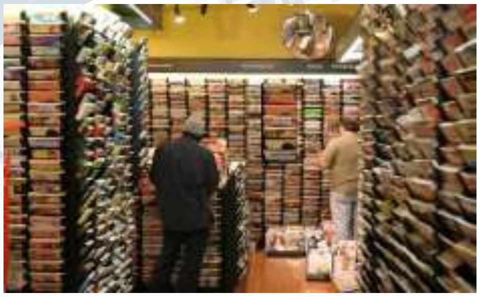

Fig 10: Forged image

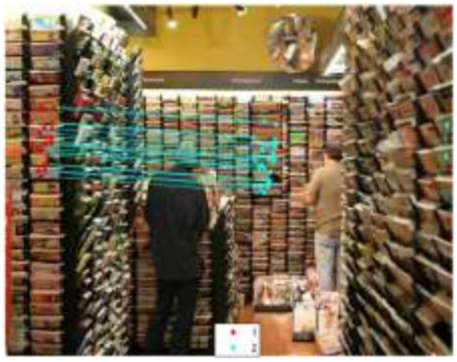

Fig 11: Forged part detected after implementing SIFT algorithm

Figure 9 is the original image and Figure 10 is the forged image and Figure 11 is the resultant image in which forged part is accurately detected after applying the SIFT algorithm on forged image.

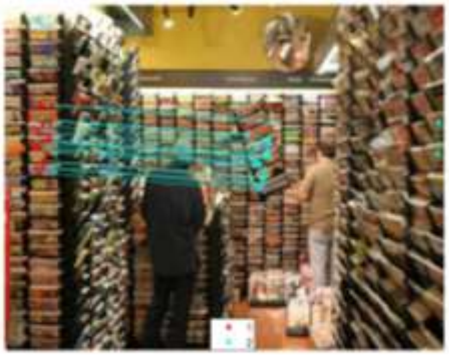

Fig 12: Forged region detected after applying geometric transform(rotation).

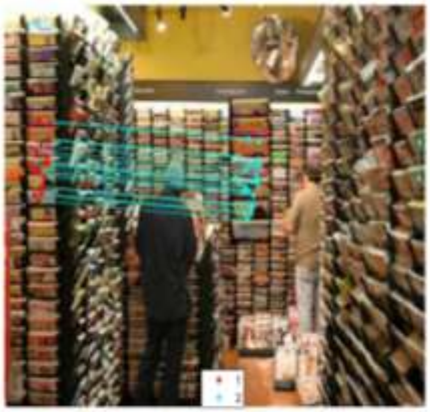

Fig 13: Forged region detected after applying geometric transform (scaling).

By observing Figure 12 ,13 it is noticed that forged part is detected accurately even by applying geometric transform (rotation, scaling), which shows the robustness of proposed method.

Performance Analysis of Proposed model:

Confusion matrix in fig 14 is a table which describes the performance of proposed algorithm.

Formulas are given to calculate the image accuracy, sensitivity, and specificity to verify the algorithm.

- TP = true positive = Number of forged images detected as forged
- TN = true negative = Number of authentic images identified as authentic
- FN = false negative = Number of forged images identified as authentic
- FP = false positive = Number of authentic images identified as forged
- TPR = TP/(TP+FN).
- TNR = TN/(TN+FP).
- Accuracy = (TP+TN)/(TP+TN+FP+FN).
- Sensitivity = TPR.
- Specificity = TNR.
- False positive rate (FPR) = 1-specificity.
- False negative rate (FNR) = 1- TPR

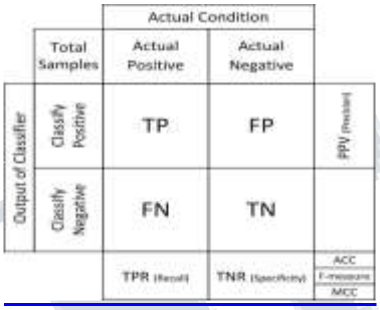

Fig 14: Confusion matrix

TABLE 1: comparison of Performance evaluation between proposed method and existing method

METHOD	SENSITIVITY	SPECIFICITY	ACCURACY	FPR (%)	TPR (%)
DCT	90%	91%	90%	6%	90%
SIFT	90%	96%	93%	4%	90%

TABLE 2: Comparison of robustness between proposed method and existing method

METHOD	WITHOUT ROTATION SCALING	SCALING	ROTATION	NOISE IMAGE
DCT	YES	NO	NO	NO
SIFT	YES	YES	YES	YES

Proposed method is compared with existing method in terms of performance evaluation and found better result which is shown in Table 1. Proposed method works perfectly in terms of rotation, scaling and noisy image. Robustness of proposed method is compared with existing method which is shown in Table 2 [14].

VII. CONCLUSION

In the proposed work, a SIFT algorithm is implemented to detect the copy move forgery in digital images. Proposed algorithm is tested on various images of standard dataset. simulation results show that the forged region is detected accurately by using the SIFT algorithm. Robustness is also checked by applying the geometric transform to the copied region of an image. the accuracy rate has been found higher than the existing algorithm.

It is concluded that the proposed system shows considerably high improvement than the existing systems. Average time is calculated as 45 seconds to process the input by the proposed system which is again less than that of existing systems. In proposed work, clusters and their mean values are used to find the forged area within the image to reduce the overall processing time. Proposed system also shows good accuracy in the images that contain forgery with geometric transformations.

VIII. FUTURE SCOPE:

The proposed model can be further enhanced to minimize the processing time to detect the forgery in the images to few seconds or even microseconds. false positive rate can also be reduced by applying some other techniques. The proposed system can also be improved in such a way that it can detect forgery even for low powered images. Proposed system takes more computational time for high resolution images and it cannot detect the forgery in the images when geometric transformation (rotation and scaling) are performed simultaneously. Proposed system working can be enhanced by combining with E-SIFT or SURF [15] algorithms to deal with above issues and make the system work more efficiently..

REFERENCES

[1] Amerini, Irene, et al. “A SIFT-based forensic method for copy-move attack detection and transformation recovery”, Information Forensics and Security, IEEE Transactions on 6.3 (2011): 1099-1110.

[2] Amerini, Irene & Ballan, Lamberto & Caldelli, Roberto & Del Bimbo, A & Serra, Giuseppe. (2013). MICC-F220.

[3] Chi-Man Pun, Xiao-Chen Yuan and Xiu-Li Bi, “Image forgery detection using Adaptive over segmentation and feature point matching”, IEEE Trans.Inf. Forensics Security, vol. 10, Aug 2015.

[4] D. G. Lowe, “Object recognition from local scale-invariant features”, in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999, pp. 11501157.

[5] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukas,” Detection of copy-move forgery in digital images”, In Proceedings of Digital Forensic Research Workshop, Cleveland, OH, USA, pp. 55-61, August 2003.

[6] H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm”, in Proc. Pacific-Asia Workshop Compute. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272276.

[7] J. J. Lee and G. Y. Kim. “Robust estimation of camera homography using fuzzy RANSAC”. In ICCSA ’07: International Conference on Computational Science and Its Applications, 2007.

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, “Detection of image region duplication forgery using model with circle block”, in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2009, pp. 25–29.

[9] Lowe, David G., "Distinctive image features form scale-invariant key-points", national journal of computer vision, vol. 60, no. 2, pp. 91-110, 2004.

[10] Li, Guohui, Qiong Wu, Dan Tu, and Shaojie Sun. “A sorted neighbour- hood approach for detecting duplicated regions in image forgeries based on DWT and SVD”, In Proceedings of IEEE International Conference on Multimedia and Expo., pp.1750-1753,2007.

[11] Mohmmad Farukh Hasmi, Aaditya R. Hambarde, Avinash G. Keskar, “copy move forgery detection using DWT and SIFT features”, 2013, Int. Conf. Intelligent systems design and applications.

[12] Popescu, A1in c., and Hany Farid,” Exposing digital forgeries by detecting duplicated image regions”, Department of Computer Science, Dartmouth College, Technical Report. TR2004-515, August 2004.

[13] R. Hartley and A. Zisserman. “Multiple View Geometry in Computer Vision”. Cambridge University Press, second edition, 2003).

[14] S.Bravo-Solorio and A. K. Nandi, “Exposing duplicated regions affected by reflection, rotation and scaling”, in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2011, pp. 1880–1883.

[15] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, “Image copy-move forgery detection based on SURF”, in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2010, pp. 889892.