Digital Image Falsification Detection System for Effective Data Communication

T. Sasilatha, K.R. Anupriya, C. Gnana Kousalya, S. Arun

Abstract: ***In this proposed system a digital imagefalsification can be identified using the combination of both adaptive over block based segmentation, feature keypointbased feature extraction algorithms(Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF)) and forgery region extraction algorithm. The proposed falsification detection algorithm comprises both block based falsification detection algorithm (adaptive over block based segmentation and block feature matching algorithm) and the keypoint based falsification detection algorithm(forgery region extraction algorithm). Adaptive over block based Segmentation algorithm adaptively segments the input digital image into separate(non overlapped) blocks in irregular manner. Scale Invariant Feature Transform (SIFT) algorithm and Speeded Up Robust Features (SURF) algorithms are used to draw out features from the segmentedblocks as a block features. Then the extracted features are matched with the feature points of other segmented block. If the feature key points are matched with any other feature point presents in the segmented blocks, then the matched feature points are marked as Labeled key Points (LKP), which can be doubted as a forged regions. Finally, the Forgery Region Extraction algorithm can be used to detect the forged region from the input digital image based on the extracted labeled feature points. The experimental outcomesdisplay that the novelfalsification detection system can accomplished the requirements compared with the existing digital imagefalsification detection methods.***

Keywords: Falsification, Forgery, SIFT, SURF, Feature key points, Segmentation, Morphological

I.INTRODUCTION

Imitations are not new to humanity, but an exceptionally old problem. It was limited to craftsmanship in the past, and yet writing did not affect the populace as a whole. A picture can be easily controlled and modified due to the advancement of automated image handling software and neutering tools thesedays. To know outwardly whether the image is real or disorted is incredibly problematic for people.Throughout mainstream media and on the Internet, there is a rapid increase throughout digitally controlled falsifications. This trend shows real flaws and reduces digital image quality.In this way, it is essential to set up procedures to verify the authenticity and truth of advanced photographs, especiallygiven that the images are presented as evidence in a court of law, as news items, as part of remedial documents, or as money-related articles.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

T. Sasilatha, Professor and Dean, Department of EEE, AMET Deemed to be University, Chennai.

K.R. Anupriya, Research Scholar, Department of EEE, AMET Deemed to be University, Chennai.

C. Gnana Kousalya, Professor and HOD, St.Joseph's Institute of Technology, Chennai.

S.Arun, Professor, Department of ECE, Prathyusa Engineering College, Chennai.

In this context, the identification of photo falsification is one of the basic aims of the forensic camera.

For copying and moving forgery operation, image processing techniques such as blurring, compression, scaling and adding noise can be used. Methods of falsification detection can be classified into two classification based on existing techniques: block-based algorithms (segmentation and segmented blocks matching algorithms)[2-12] and keypoint-based algorithms (falsification zone extraction algorithms).

In the existing block-based falsification detection algorithms, the input digital images are segmented in the form of overlapped image blocks in regular manner; then, the forged region is obtained by matching image pixel blocks or rework coefficients. A.J.Fridrich et al.[2] proposed a forgery detection method based on the block based falsification algorithm. In this the image was segmented in the form of overlapped rectangular blocks. The forged regions detected by matching the Discrete Cosine Transform coefficients of the rectangular blocks. H. Farid and A. C. Popescu et al [1] proposed Principal component Analysis (PCA) to measure the feature dimensions. W. Luo, J. Huang et al.[3] used the RGB color components and direction data as block features. G. Li, Q. Wu, D. Tu,et al.[4] proposed a system, which Combines both Discrete wavelet transform (DWT) algorithm and Singular price Decomposition (SVD) algorithm to extract the image features. B. Mahdian and S. Saic [5] proposed a algorithm, which extracted the twenty four Blurinvariant keypoints as features. X. Kang and S. Wei [7] pro[oseda algorithm which calculate the singular values of a reduced-rank approximation in every block. S. Bayram, H. T. Sencar, N. Memon et al.[6] proposed a algorithm, which uses the Fourier-Mellin transform (FMT) to extract key point features options.

The alternative method for the block based falsification detection algorithm is feature point-based falsification detection methods. In this feature point based falsification detection system key feature points are extracted and matched with the whole part of image to maintain a few image conversions while detecting the falsified regions. In [15-18], to extract the key feature points the Scale-Invariant Feature Transform algorithm[19] was used to extract the feature keypoints and then the extracted features can be matched with one another to identify the forged regions. In this SIFT algorithm, if the value of shift vector increases above the threshold value, then that group of keypoints are marked as tambered region.

The another type of feature extraction algorithm is Speeded Up Robust Features (SURF) [21], which can be used to extract the key feature points and locate the falsified regions.

Still, even though those methods can locate the matched key feature points very well, but some of the feature keypoint algorithms are not locate the falsified region well; as a result the accuracy of the falsification detection is reduced[22]

Most of the previous block-based falsification detection algorithms has drawbacks:

1) computationally expensive; 2) the existing techniques doesn't clearly show the geometrical transformations of the forged areas; Even though the existing keypoint-based forgery detection methods used to overcome two issues, which decrease the level computational complexity and detect forged regions successfully. The main disadvantage of the existing keypoint based forgery detection technique is low recall rate. In order to overcome the disadvantages of the existing methods of forgery detection, The proposed image forgery detection scheme combines the block-based(segmentation and block feature matching algorithm) and keypoint-based(feature region extraction algorithm) methods.

II.IMAGE FORGERY DETECTION SYSTEM

The proposed digital image falsification detection system combines both adaptive over block based segmentation algorithm and forgery region extraction, feature keypoint based algorithms. Fig. 1 and 2 demonstrates the structure of the proposed image falsification detection system using SURF and SIFT scheme. First, an adaptive over block based segmentation method is used to cluster the tampered image into segments in the form of non overlapped and irregular blocks. To extract features from the segmented blocks Scale Invariant Feature Transform (SIFT) algorithm and Speeded Up Robust Features (SURF) algorithm can be used. Then the extracted feature key points are matched with each another segmented block features. If the feature key points are matched with any other feature key point presents in the segmented blocks, then the matched feature points are marked as Labeled key Points (LKP), which can be suspected as a forgedregions. Finally, the Forgery Region Extraction algorithm can be used to detect the forged region from the input digital image based on the extracted labeled key points.

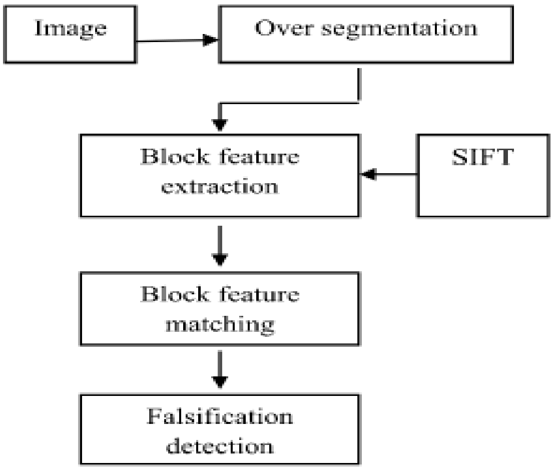

Fig. 1 Framework of the proposed digital imagefalsification detection scheme using SIFT algorithm

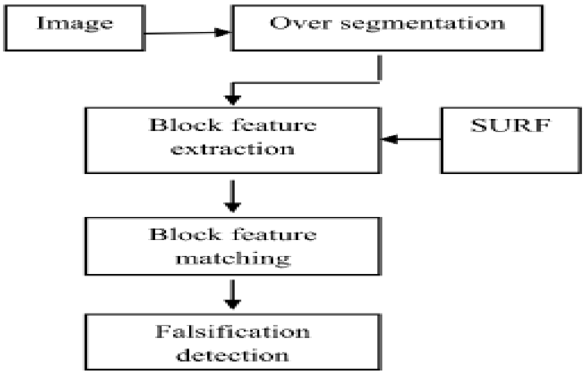

Fig. 2 Framework of the proposed digital image falsification detection scheme using SURF algorithm

Adaptive Over Block based Segmentation Algorithm

In this proposed Adaptive Over block based Segmentation algorithm, the digital input image can be segmented as anon overlapped and uneven shaped blocks.

For the purpose of obtaining better forgery region detection results, the primary size of the superpixels are very important. Still, the existing segmentation algorithms don't provide best solution to calculate primary size of super pixels.

Adaptive over block based segmentation algorithm is proposed to calculate primary size of the superpixels depends on the input digital image characteristics. If the characteristics of the digital input image is non detailed, then the superpixels primary size should be set as larger value, which assure that superpixels get near to the edges and also superpixels consists of adequate feature key points to be used for the falsified region detection; moreover, greater value of superpixels indicate a tiny number of segmented blocks, when the segmented blocks are matched with each another block which will decrease the computational cost. When the characteristics of the input digital image is non smooth (detailed image), then primary size of the superpixels should be set as a relatively small value, for the better forgery detection results. Discrete Wavelet Transform (DWT) algorithm is used to evaluate frequency distribution of the input image. If the low frequency energy has large value means, the input image will seemed as a non detailed (smooth) image; If the low frequency energy has small value means, the input image will seemed as a detailed image. For this more number of investigations were conducted by exploring the relationship between superpixels primary size and frequency distribution of the input images to achieve better falsification detection.

In order to calculate high frequency energy E_{HF} and low frequency energy E_{LF} a4 level Discrete Wavelet Transform, using the 'Haar' wavelet transform can be applied on the input digitalimage. Using the the low-frequency energy E_{LF} and high-frequency energy values , the percentage of the low-frequency distribution X_{LF}can be calculated based on the primary sizeP of the super pixels.

$$E_{LF} = \sum |SA_4| \qquad (1)$$

$$E_{HF} = \sum_i (\sum |SD_j| + \sum |SH_j| + \sum |SV_j|, j=1,2,. \quad (2)$$

Where Iindicatessuper pixels primary size; M x N indicates the size of the input image; and X_{LF} indicates the percentage of the low-frequency distributionand SD_j, $SH_j$and SV_j indicates the coefficients of j^{th}level DWT, j=1,2,…4

$$X_{LF} = \frac{E_{LF}}{E_{LF}+E_{HF}} 100\% \quad (3)$$

$$P=\begin{cases} \sqrt{0.02\times M\times N}, & X_{LF}>50\% \\ \sqrt{0.01\times M\times N}, & X_{LF}\leq 50\% \end{cases} \quad (4)$$

This proposed Block based Segmentation method segments the input digital image into block segments adaptively in order to achieve better falsification detection results.

Block Feature Extraction Algorithm

The feature key points are draw out from each segmented blocks as block segment features. The feature key points are extracted using SIFT and SURF algorithms are proven that which will be robust against the digital image processing operations like rotation, scale, blurring, and compression; SIFT and SURF feature key point extraction algorithms are feature key point based falsification detection methods. In order to extract feature point as block features Scale Invariant Feature Transform (SIFT) algorithm and Speeded Up Robust Features (SURF) can be applied.

Block Feature key point Matching Algorithm

The extracted block features can be used to locate the doubted matched blocks in the segmented image blocks. The block features comprised a group of feature key points, which can be used to locate the matched image blocks as a doubted image blocks. For the matching purpose block feature matching algorithm can be used. First, the number of matched feature key points are calculated, and with the help of matched feature key points the correlation coefficient map is developed; then, the appropriate threshold value for matched blocks are calculated; based on the threshold value the matched blocks are labeled. And lastly, the matched feature key points present in the matched image blocks are draw out and marked to locate the position of the doubted forgery region. The detailed steps are explained as follows.

Algorithm: Block Feature key point Matching algorithm

Block Features (BF) are used as inputs and this algorithm results Labeled key Points (LKP) as suspected falsified region.

STEP-1:

Block features $FB = \{FB_1, FB_2, ...$can be loaded and then correlation coefficients can be calculated for the each segmented blocks.

STEP-2:

The threshold value for block matching can be calculated based on the correlation coefficientsT_B.

STEP-3:

The matched blocks can be located based on the threshold valueT_B.

STEP-4:

After that the matched feature key points are labeled to detect the suspected forgery regions.

The Matching algorithm uses two threshold values to match the segmented blocks and feature key points: the feature key points matching threshold value T_P and the segmented block matching threshold valueT_B , which will avoid the false matching.

Forgery Region Extraction Algorithm

The labeled key points are the suspected locations of the forgery region. In order to detect exact forgery regions forgery region extraction algorithm can be used. This forgery region extraction algorithm replaced labeled feature points with small super pixels to detect the suspected forgery regions. First, the local color attributes of the superpixels can be calculated to improve recall and precision, if thelocal color attributes are similar to the local color attribute of the doubted (suspected) regions, then the matched feature block superpixels can be merged with the suspected doubted regions. Then the morphological operations can be applied to detect the forged regions.

Algorithm: Forgery Region Extraction

Labeled key Points (LKP)are used as input and labeled Forgery Regions as output.

STEP-1:

Labeled key Points (LKP) can be loaded; SLIC clustering algorithm can be applied to the input digital image with the primary size P, which will segment the input image blocks in to small super pixels, which will be considered as a feature blocks; then labeled key points are matched with each blocks to generate the doubted forged regions. If the labeled key points are matched with any block key points means this will be marked as a doubted regions(DR).

STEP-2:

The local color attributes of the small superpixels can be measured for the neighboring blocks of the doubted regions. If the local color attributes are matched with the doubted regions, then, which can be merged with the matched doubted regions, as a result merged doubted regions were created.

STEP-3:

The morphological operations can be applied to the merged doubted regions in order to generate the tampered or forged region.

III.RESULTS AND DISCUSSION

The input image is read from the folder using user interface get file method. This work accepts one input for its process. The image is the color image which contains R,G and B channels.

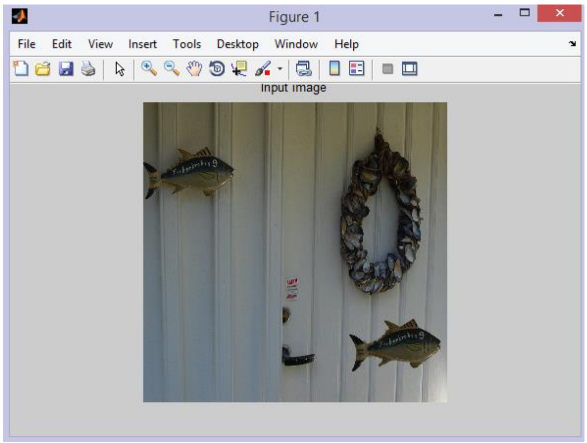

Fig. 3 Input digital image

SLIC clustering algorithm used to cluster the input digital image into uneven the host image in to irregular super pixelswith primary size P.

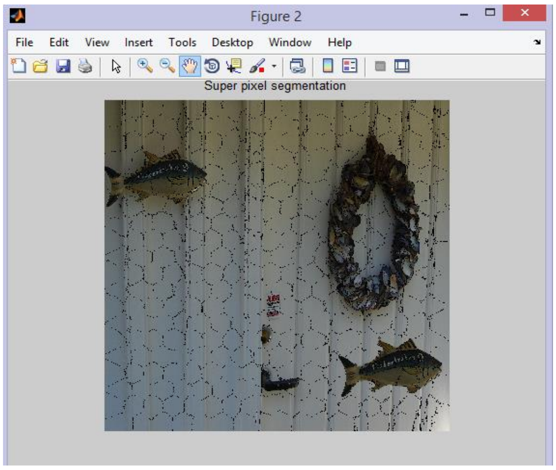

Fig. 4 Super pixel segmentation

SURF and SIFT feature key point draw out algorithms are used to extract the feature key points from each clustered image block and each image block is characterized by SURF/SIFTkey points that were draw out from the corresponding clustered image block.

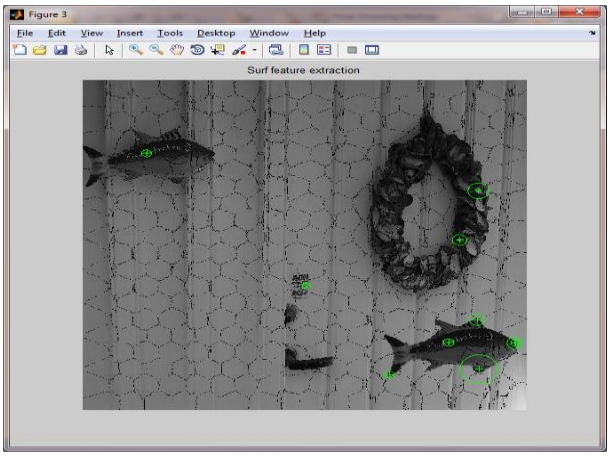

Fig. 5 SURF feature points as block features

The matched keypoints are draw out from the corresponding clustered image blocks and which can be labeled in order to locate or marked the doubted forged regions.

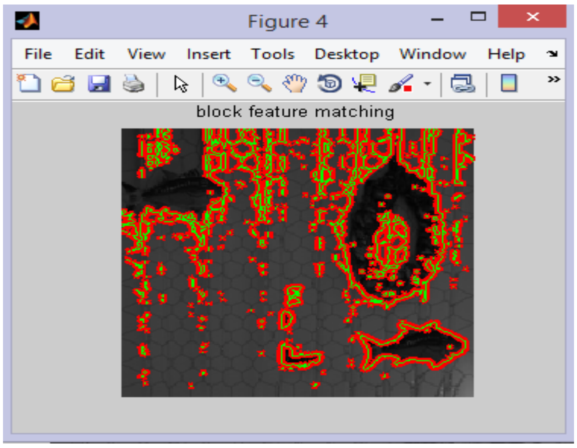

Fig. 6 Block Feature matching

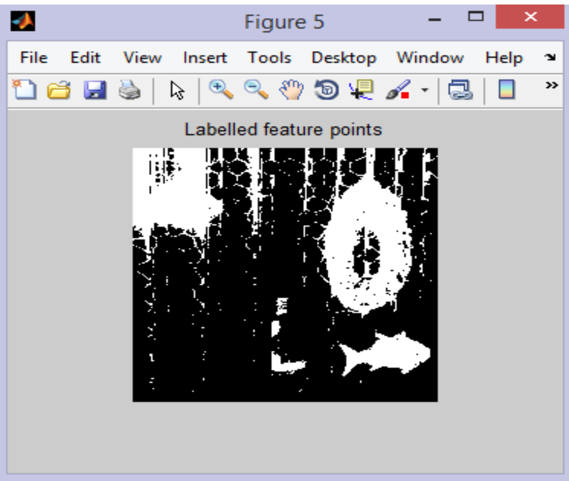

Fig. 7 Labeled feature points

The local color attributes of the corresponding super pixels (that are neighbors to the doubted regions) were measured, ; if the local color attributes are matched with the attributes of the doubted forged regions, then the matched superpixels are merged with the doubted forged regions. This will results the merged forgery region.

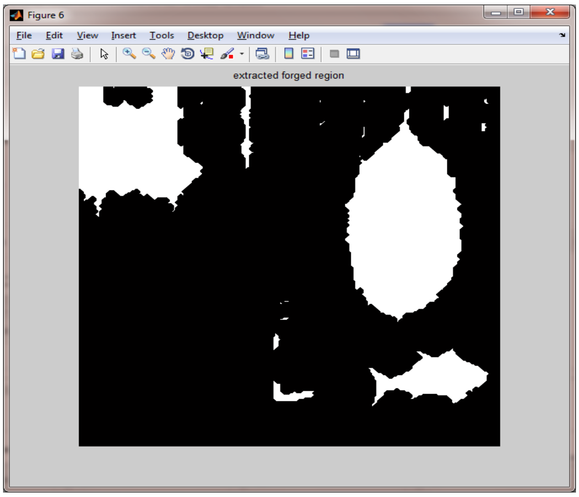

Fig. 8 Extacted forged region

At the end, the morphological operation is enforced in the merged doubted forgery region to to generate the detected forgery regions.

IV.PERFORMANCE EVALUATION

Performance is evaluated between existing system and the proposed system. Existing system make use of SIFT registration. Proposed work uses SURF registration to make the work better. The experiment is carried out using CASIA database. The tabulation is made four images from that database. The performance metric carried out in this work are sensitivity, specificity, accuracy, MCC and precision.

Sensitivity is defined as number of positive pixels identified correct.

$$sensitivity = \frac{t_p}{p}$$

Where

$$t_p = no.ofpositivepixels\ identifiedaspositivep$$
$$= totalno.ofpositivepixelsinreferenceimage$$

Specificity is defined as number of negative pixels identified correct.

$$specificity = \frac{t_n}{n}$$

Where $t_n =$
$noofnegativeimagesclassifiedasnegativen =$
$totalnumberofnegativeimages$

Accuracy is the number positive and negative pixels identified correct.

$$accuracy = \frac{t_p + t_n}{N}$$

Where,

$$t_p = No.ofpositiveimagesclassifiedas + ve$$
$$t_n = noofnegativeimagesclassifiedas - ve$$
$$N = Totalnumberofimages$$

The MCC (Mathews Correlation Coefficient) is a correlation coefficient between the rectified and distorted fingerprint.

$$MCC = \frac{(t_p * t_n - f_p * f_n)}{\sqrt{(t_p + f_p) * (t_p + f_n) * (t_n + f_p) * (t_n + f_n)}}$$

Where,$t_n =$
$no.ofpositivepixelsclassifiedasnegativet_p =$
$no.of + ve\ pixelsclassifiedaspositive$
$f_p = noofnegativepixelsclassifiedasnegative$
$f_n = no.ofnegativepixelsclassifiedaspositive$

Precision denotes how accurately the forged regions are extracted.

$$precision = \frac{t_p}{t_p + f_p}$$

Table. 1 Comparision Between Performance Metrices For Various Forged Images Using Sift And Surf Algorithms

Performance metric	Sensitivity		Specificity		Accuracy		MCC		Precision	
	SIFT	SURF	SIFT	SURF	SIFT	SURF	SIFT	SURF	SIFT	SURF
Image1	0.1735	0.2048	0.1923	0.962	0.1735	0.2047	0.0665	0.0688	0.9927	0.9930
Image2	0.1670	0.1933	0.2863	1	0.1755	0.2015	0.0453	0.0495	0.3456	1
Image3	0.1546	0.2443	0.7890	1	0.1547	0.2443	0.0024	0.0031	0.5641	1
Image4	0.1209	0.1654	0.892	0.992	0.1554	0.1982	0.0728	0.0875	0.9997	0.9998

The table represents the values for the performance metrices sensitivity, specificity, accuracy, MCC and precision for various images using SURF and SIFT algorithms.

V.CONCLUSION AND FUTURE SCOPE

Digital falsification of images created by using copy and move operations are challenging task to identify. This digital falsification detection system proposed a novel copy and move falsification detection algorithm using adaptive over block based method and feature key point based method. Adaptive Over block based Segmentation algorithm can be used to improve the accuracy of the falsification detection. This segmentation algorithm determine the primary size of the digital image block to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Using the Matching algorithm, the block key features are matched with one another to locate the marked key points; this procedure can approximately indicate the doubted forgery regions. Subsequently, to detect the more accurate forgery regions.the Forgery Region Extraction algorithm is used to generate the detected forgery regions effectively. This scheme achieve much better detection outcomes for copy and move forgery images under various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling, compared with the existing state-of-the-art copy-move forgery detection schemes.

Future work could focus on applying the forgery detection scheme based on adaptive over-segmentation and feature-point matching on other types of forgery, such as splicing or other types of media, for example, video and audio.

REFERENCES

1. A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College,Tech. Rep. TR2004-515, 2004.
2. A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in in Proceedings of DigitalForensic Research Workshop, 2003.
3. W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in PatternRecognition, 2006. ICPR 2006.

18th International Conference on,2006, pp. 746-749.
4. G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Multimedia and Expo, 2007 IEEE InternationalConference on, 2007, pp. 1750-1753.
5. B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic scienceinternational, vol. 171, pp. 180-189, 2007.
6. S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech andSignal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.
7. X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in ComputerScience and Software Engineering, 2008 International Conference on, 2008, pp. 926-930.
8. J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," ActaAutomaticaSinica, vol. 35, pp. 1488-1495, 2009.
9. J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, 2009, pp. 25-29.
10. S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in Acoustics, Speechand Signal Processing (ICASSP), 2011 IEEE International Conference on, 2011, pp. 1880-1883.
11. H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, pp. 188-197,2009.
12. S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding, 2010, pp. 51-65.
13. S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," Ieee Transactions on Information Forensics andSecurity, vol. 8, pp. 1355-1370, Aug 2013.
14. H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in ComputationalIntelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, 2008, pp. 272-276.
15. X. Y. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," Ieee Transactions on Information Forensics andSecurity, vol. 5, pp. 857-867, Dec 2010.
16. 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," Information Forensics and Security,IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.
17. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia InformationNetworking and Security (MINES), 2010 International Conference on, 2010, pp. 889-892.
18. P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," InformationForensics and Security, IEEE Transactions on, vol. 7, pp.1018-1028, 2012.
19. D. G. Lowe, "Object recognition from local scale-invariant features," in Computer vision, 1999. The proceedings of the seventhIEEE international conference on, 1999, pp. 1150-1157.
20. B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSIInternational Journal of Computer Science Issues, vol. 8, 2011.
21. H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in Computer Vision–ECCV 2006, ed: Springer, 2006, pp. 404-417.
22. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," Ieee Transactions on Information Forensics andSecurity, vol. 7, pp. 1841-1854, Dec 2012pp. 188-197,2009.
23. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," Ieee Transactions on Information Forensics andSecurity, vol. 7, pp. 1841-1854, Dec 2012
24. R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," IEEE Trans Pattern Anal Mach Intell, vol. 34, pp. 2274-82, Nov 2012.
25. GaneshKumar K., Arivazhagan D. “New cryptography algorithm with for effective data communication”, Indian Journal of Science and Technology, 2016.
26. Mir S.A., Padma T. “Fuzzy decision support system for evaluation and prioritisation of critical success factors for the development of agricultural DSS”, International Journal of Multicriteria Decision Making,2017.

AUTHORS PROFILE

T. Sasilatha, Professor and Dean, Department of EEE, AMET Deemed to be University, Chennai

K.R. Anupriya, Research Scholar, Department of EEE, AMET Deemed to be University, Chennai

C. Gnana Kousalya, Professor and HOD, St.Joseph’s Institute of Technology, Chennai

S. Arun, Professor, Department of ECE, Prathyusa Engineering College, Chennai