A hybrid approach to find cloned objects in copy move forged images

Ashish Kumar Chakraverti*

IKG-Punjab Technical University,
Jalandhar, Punjab, India
and
ABES Institute of Technology,
Ghaziabad, UP, India
Email: ashish.me08@gmail.com
*Corresponding author

Vijay Dhir

M.K. Group of Institution,
Amritsar, Punjab, India
Email: drvijaydhir@gmail.com

Abstract: In this paper, we have proposed a new hybrid approach to detect the cloned object in images. In copy-move forgery, images are forged by making the clone of objects of the same image within the image. In our proposed work, we have integrated two states of art techniques named adhoc method and principle component analysis (PCA) based scale invariant feature transform (SIFT) method. In two step process, we have preprocessed the object image by the proposed dynamic block size technique based local contrast modification and contrast limited adaptive histogram equalisation (DBST-LCM CLAHE) up to desired PSNR and grey level and then after integrated adhoc, and PCA based SIFT algorithm to design a hybrid approach. Proposed method tested over CoMoFoD image database. Proposed method shows the better performance in comparison of the state of art techniques regarding false positive rate (FPR), true positive rate(TPR), and PSNR.

Keywords: image processing; image enhancement; ad hoc; peak signal to noise ratio; PSNR; image forgery; scale invariant feature transform; SIFT; principle component analysis; PCA; contrast limited adaptive histogram equalisation; CLAHE; noise.

Reference to this paper should be made as follows: Chakraverti, A.K. and Dhir, V. (2019) 'A hybrid approach to find cloned objects in copy move forged images', *Int. J. Forensic Software Engineering*, Vol. 1, No. 1, pp.3–20.

Biographical notes: Ashish Kumar Chakraverti pursued his Bachelor of Technology from the IEC College of Engineering and Technology, Greater Noida UP, India in 2005 and Master of Technology from the RGPV Bhopal MP, India in 2010. He is currently pursuing his PhD from the IKG-PTU Jalandhar Punjab, India and currently working as an Assistant Professor in the Department of CSE, ABES Institute of Technology, Ghaziabad UP, India since June 2018. He is a member of IEEE and IEEE Computer Society since 2013, ACM since 2014. He published more than ten research papers in reputed international journals including Thomson Reuters (ESCI and Web of Science) and conferences including IEEE. His main research work focuses on big data analytics, image processing, digital forensics and parallel computing. He has 12 years of teaching experience and two years of research experience.

Vijay Dhir pursued his Bachelor of Technology, Master of Technology, and PhD from the PTU Jalandhar. He is member of board of study in the Department of CSE IGK-PTU, Jalandhar and working as a Professor CSE in the M.K. Group of Institution, Amritsar, Punjab, India. He is a member of IEEE and IEEE Computer Society since 2009, ACM since 2010. He published more than 50 research papers in reputed international journals including Thomson Reuters (ESCI and Web of Science) and conferences including IEEE. His main research work focuses on big data analytics, image processing, digital forensics and parallel computing. He has 17 years of teaching experience and three years of research experience.

1 Introduction

In the current scenario of social media, images and videos are very powerful medium to communicate the message. Lots of images and videos are being uploaded and downloaded every second in the cyber base. These images are used to create thoughts, sense, behaviour, and response in our society. Since image and video contain more information in comparison to text data as well as these are fast to perceive and understand, so images are being used as an easy tool to spread the information in society. Due to the availability of highly advanced editing tools and technology, as well architectural support by the cloud to every one, credibility and genuineness of image spread over social media and cyber world is highly questionable. So many techniques are available to check the originality of image. In this process, many advance operation and algorithms are used these include forgery detection, feature extraction, clustering, and classifications. All the technique need some pre-processing and feature enhancement to be done on target images for better performance.

In our proposed method we have first pre-processed the target image up to the desired level of features enhancements and then use a hybrid approach of copy-move forgery detection. This section has discussed the introduction of problem and effect of the problem over society.

Here we are discussing some examples of image cloning from history.

Figure 1 Images shows copy-move forgery in 1860

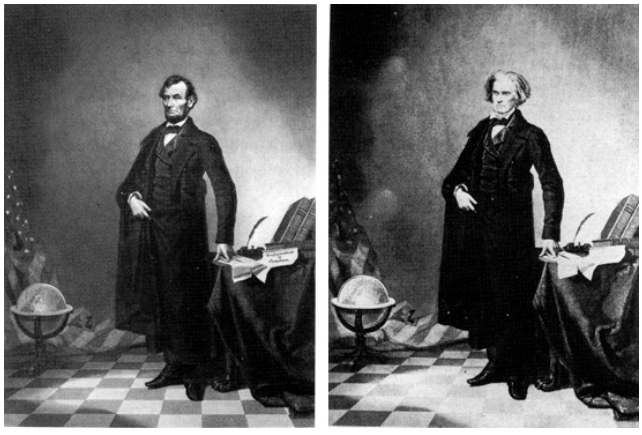


Figure 1 indicates almost notorious picture (as a lithograph) of US President Abraham Lincoln is a composite of Lincoln's head and the Southern government official John Calhoun's body falsification was done in around 1860. Figure 2 demonstrates a doctored photograph of Queen Elizabeth Bowes-Lyon – mother of Queen Elizabeth II and Canadian Prime Minister William Lyon Mackenzie King in Banff, Alberta, King George VI was expelled from the first photo in 1930. This photograph was utilised on a race blurb for the Prime Minister. It is guessed that the Prime Minister had the photograph changed because a photograph of just him and the Queen painted him in an all the more capable light.

After seeing these historic copy-move forgeries now it is obvious that if forgery was so nicely done in the era of non-computerised editing methods then nowadays its very easy to do with advanced tools and techniques. So to develop the tools and technique to detect these type of forgery is very much required to have the authenticity of images in the web world. For this purpose, we have considered the detection of cloned objects in an image which is a type of copy-move forgery detection. The ubiquitous existence of personal mobile devices and the emergence of online social media have attracted an increasing number of users. This increase is due to the active presence of social media in these mobile devices. The convergence of social media and mobile communication networks generates a considerable amount of trending media contents. Kaur (2017) says that there is a serious concern to identify whether the contents of the images are real or belong to the claimed context using associated descriptive tags. Dixit and Naskar (2017) found that the most recent decade has seen a considerable measure of research progress in the zone of computerised picture legal sciences, whereby the examination for conceivable phonies is exclusively in view of post-handling of images. There are two sorts of strategies for picture fabrications: one is an active forgery, and the other is a passive forgery. In the active forgery, the advanced picture requires a pre-processing, for example, watermark installed or marks are produced at the season of building up the picture. Passive picture forgery is typically an excellent test in picture handling procedures. Chakraverti and Dhir (2017) and Kaur (2017) explained that there is not a

particular technique that can treat every one of the cases, yet we have various techniques accessible that arrangements with a particular sort of inactive phoney. In passive forgery detection, the forged picture in view of different measurements and semantics of picture substance to confine altering of the picture is broke down deeply. Kashyap et al. (2017) writes that taking into account the methods used to make forged images, digital image forgery can be isolated into three primary classifications: copy-move forgery, image splicing, and image resampling.

The images considered for research are taken for CoMoFoD (Tralic et al., 2013) image repository. CoMoFoD consists of 260 forged image sets. Every image set includes a forged image, two masks, and an original image. Images are grouped into five categories according to applied manipulation: translation, rotation, scaling, combination, and distortion.

Figure 2 Images shows copy-move forgery in 1930

We have organised rest of our paper as follows. Section 2 contains the review of existing state-of-art technique of detection of copy-move forgery detection. in Sections 3 and 4 we proposed a method to improve the accuracy of copy-move forgery detection by hybridisation of two methods first ad-hoc and second scale invariant feature transform (SIFT). Before hybridisation target image is pre-processed by proposed dynamic block size technique-based local contrast modification and contrast limited adaptive histogram equalisation (DBST-LCM CLAHE), this is discussed in Section 3. Section 4 presents the detail about the proposed method and related algorithms. Implementation, experiment, and results are discussed in Section 4. Finally, we have compiled our conclusion and future work in this area in Section 5.

2 Related work

Kulkarni et al. (2013), Patel et al. (2014) and Yu et al. (2015) suggested contrast-based picture coordinating, which is a vital part of numerous PC-based applications. Distinctive calculations are utilised for picture handling like SIFT, speeded

up robust features (SURF), oriented features from accelerated segment test (FAST) and rotated binary robust independent elementary feature (BRIEF) (ORB), ORB calculation utilises the oFAST calculation to distinguish the component focuses, which is the FAST administrator that has bearing. Karami et al. (2017) have compared the performance of SIFT, SURF ORB and FAST over distorted images and found that ORB is the fastest algorithm while SIFT performs the best in the most scenarios. Chaudhari and Garg (2017) claimed that in ORB, the features are mostly concentrated in objects at the centre of the image while in SURF, SIFT and FAST key point detectors are distributed over the image. Aglave and Kolkure (2015) and Rublee et al. (2011) says that ORB can also be used in image mosaicking. ORB and FAST are combined to get high-performance feature extraction. Adel et al. (2015) found that these algorithms can also be used for image stitching in which two images are used to make the single and relevant image. Sonka et al. (1993) and Senthilkumaran and Rajesh (2009) suggest that beside all these advance processes, pre-processing is also required to get better results.

Wo et al. (2016) claim that all above discussion about component extraction, include improvement and pre-processing is especially required to recognise imitation effectively. Copy move forgery, which clone the piece of a picture to another piece of a similar picture, is a standout amongst the most commonly used image altering operations. Kuznetsov and Myasnikov (2017) proposed a new hash-based copy-move detection algorithm that can be applied to transformed duplicates detection due to a special pre-processing procedure. In this procedure, author implements fundamental image transformation to incorporate the changes produced by a transform algorithm on the second stage. Lin et al. (2017) proposed a strategy that incorporates the essential locale duplication identification. In the essential district duplication location, a picture is separated into non-covered fixes by utilising SLIC. At the point when the estimation flops, in the supplementary locale duplication recognition, a changing grid is endeavored to be estimated from a couple of key points by the proposed keypoint contexts (KC) approach. Park and Choeh (2017) proposed a quick and vigorous approach that can deal with a few geometric changes including pivot, scaling, shearing, and reflection. Zhang et al. (2017) proposed a hybrid procedure. Right off the bat, author's prior strategy is utilised to identify whether a hopeful picture is produced or not. Also, for those undetected pictures after the initial step, joint probability density matrix (JPDM) is processed for each difference cluster to demonstrate the connections among adjoining discrete cosine transform (DCT) coefficients, and the normal of these grids are registered as highlight vectors to additionally uncover altering traces. Yang et al. (2017a) proposed copy-move forgery discovery method based on mixture highlights. A strong intrigue point indicator KAZE is acquainted and joined with SIFT with separate more component focuses. Jin and Wan (2017) proposed another arrangement of choosing the key points by area rather than differentiate. To this end, creator first separate the keypoint discovery and determination forms. Second, creator applies the rival scale-invariant component change descriptor to upgrade the discriminative energy of key points by including shading data. Yang et al. (2017b) propose another multi-granularity superpixel coordinating-based calculation for the precise identification and confinement of copy-move forgery, which coordinated the benefits of keypoint-based and piece-based fraud recognition approaches. The author uses the concept of superpixel highlights, which is quaternion type minutes magnitudes, are removed from each coarse-granularity superpixel, and author locates the coordinating coarse granularity superpixels (suspected fabrication area sets) quickly utilising the exact euclidean locality sensitive hashing

(E2LSH). Nedjah (2017) proposed a plan in which creator consolidates the square-based techniques and the keypoint-based strategies to build up a mixture system.

Emam et al. (2017) proposed a strong area duplication imitation discovery strategy in view of extricating nearby extrema focuses on difference of Gaussians (Pooch) administrator. Canine is utilised in light of the fact that it is a decent estimate for the Laplacian of Gaussian (LoG) and much speedier to ascertain. To separate the unmistakable highlights and consequently enhance the coordinating execution, multi-support region order-based gradient histogram (MROGH) descriptor is embraced. Mursi et al. (2017) proposed a visually impaired duplicate move altering location and confinement technique author demonstrates its potential to reveal and restrict altered areas of various sizes and shapes by joining SIFT, principle component analysis (PCA) and density-based spatial clustering of application with noise (DBSCAN) procedures. Warif et al. (2017) proposed a powerful CMF discovery technique, called SIFT-symmetry, that inventively joins the SIFT-based CMF discovery technique with symmetry-based coordinating. Creator assessed the Filter Symmetry with three set up techniques that depend on SIFT, multi-scale investigation, and fix coordinating utilising two new datasets that cover basic change and reflection-based assaults. Dixit et al. (2017) display a novel approach for discovery of duplicate move fabrication utilising stationary wavelet transform (SWT) which, dissimilar to most wavelet changes (e.g., discrete wavelet change), is move invariant, and aides in finding the likenesses, i.e., matches and dissimilarities, i.e., commotion, between the pieces of a picture, caused because of obscuring. The pieces are spoken to by highlights removed utilising singular value decomposition (SVD) of a picture. Additionally, the idea of shading-based division utilised by creator in this work accomplishes obscure invariance. Mahmood et al. (2017) exhibited an effective method for duplicate move imitation recognition (CMFD) through local binary pattern variance (LBPV) over the low guess parts of the stationary wavelets. CMFD procedure introduced in this paper is connected over the roundabout locales to address the conceivable post preparing activities better. Manu and Mehtre (2017) proposed a technique in light of relative change property protection of grouped key points in the picture, which incorporates the tests for collinearity and separation proportion safeguarding. According to the creator tests, strategy is additionally ready to identify numerous duplicate move frauds inside a picture. Creator tried his strategy against four picture altering identification datasets. Thirunavukkarasu et al. (2017) presented a strong system by methods for discrete stationary wavelet change alongside multi-dimension scaling to distinguish recognisable class of duplicate move picture altering. Lai et al. (2017) proposed an improved block-based matching algorithm (IBMA) to take care of the issue. Alberry et al. (2018) and Bi and Pun (2018) proposed a new technique of copy move forgery detection to speed-up the forgery detection technique. Liu and Pun (2018), Mahmood et al. (2018) and Pun and Chung (2018) worked on localisation of the forged object in digital images. Novozamsky and Sorel (2018) and Sharma and Ghanekar (2018) presented novel methods to detect modification done by copy move forgery in digital images. Most of the technique discussed here have concentrated on feature extraction stages but our technique uses hybridisation of rigorous pre-processing and feature extraction.

3 Proposed hybrid approach to find cloned objects in copy move forged images

In this section, we present details of the proposed method of HE for the de-noising nonmonotonous image. Image categories taken for the experiments are shown in Figure 3. Figures 4 and 5 shows the CLAHE and LCM-CLAHE operation flow chart. Flowchart of the proposed method of HE used in our cloned object detection procedure is shown in Figure 6. In the following subsection, we have given details of the proposed method. After that in next subsection, we have discussed the proposed hybrid approach to find the cloned object in forged images

Figure 3 Categories of images base on feature distribution, (a) non-monotonous image with nose (b) non-monotonous image without noise (c) monotonous image (see online version for colours)

(a) (b) (c)

Figure 4 Operational flow chart of CLAHE (see online version for colours)

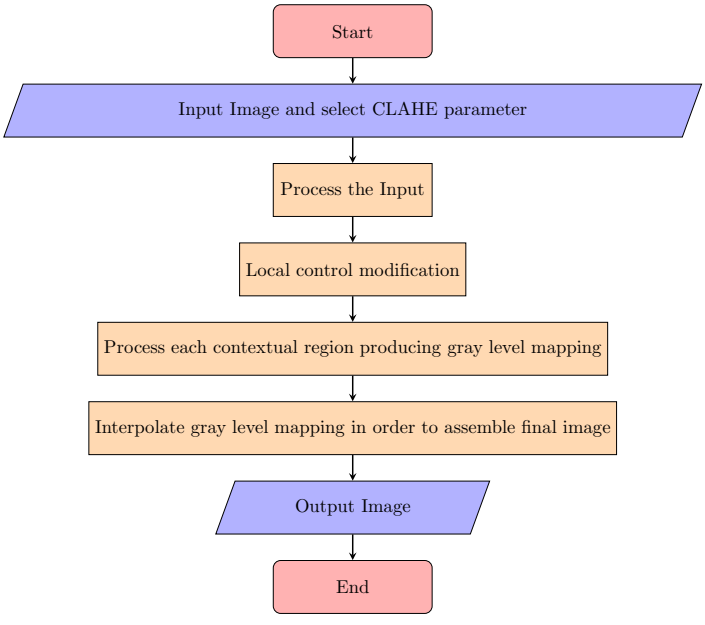


Figure 5 Operational flow chart of LCM-CLAHE (see online version for colours)

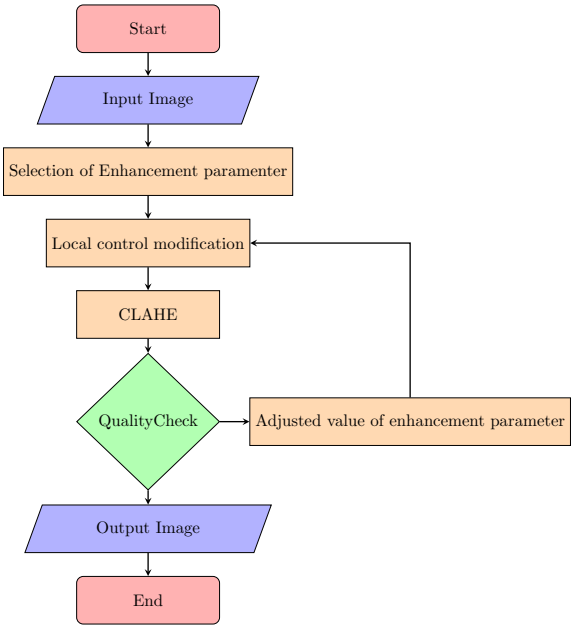
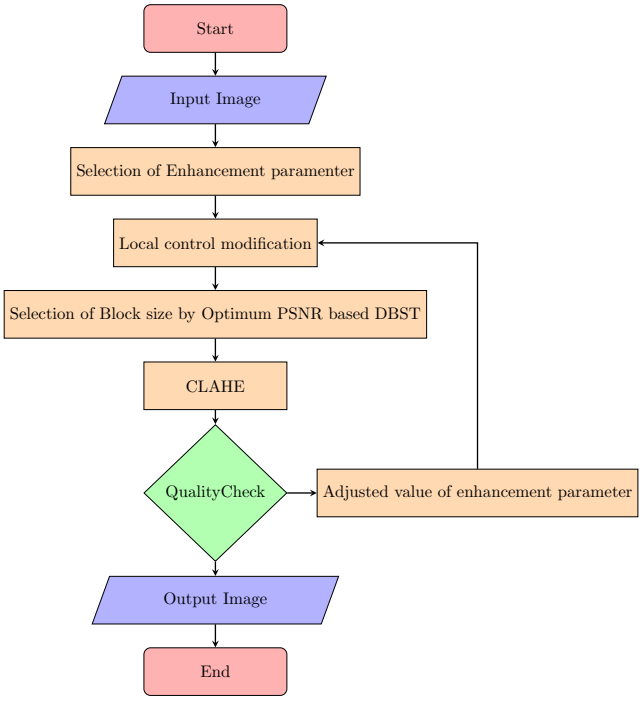


Figure 6 Operational flow chart of proposed DBST-LCM-CLAHE (see online version for colours)



3.1 Pre-processing of images by proposed DBST-LCM-CLAHE

This step involves the selection of parameter of the image to be enhanced like contrast, brightness etc. here in our example, we have taken contrast as enhancement parameter. In image processing, contrast enhancement is very common operation and it is very useful to process scientific images like satellite images and X-rays images. This is also useful in forgery detection where images are enhanced to improve the details up to the desired level. HE is one of the most common methods to enhance the contrast.

3.1.1 Local contrast modification

In this step, local contrast enhancement on the input image is applied. The function of this step is designed in such a way that it takes global and local information both to produce the enhanced image. Transformation functions are as follows.

$$T = \frac{E \ * \ M}{\sigma} \tag{1}$$

$$g = T * \ (f - m) + m \tag{2}$$

where f and g are input image and LCM enhanced image respectively. E is enhancement parameter, M and m are global and local mean of the image respectively. Now here we give the expression for local mean and standard deviation for the user-defined local window of size n * n.

$$m(x,y) = \frac{1}{n \ * \ n} \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} f(x,y) \tag{3}$$

$$\sigma = \sqrt{\frac{1}{n \ * \ n} \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} (f(x,y) - m(x,y))^2} \tag{4}$$

After the calculation of local mean m and standard deviation σ from equations (3) and (4) for all windows defined by user, average of these values is used to get the finer details of image by equations (1) and (2). Image with finer details is given as input to modified CLAHE which will use DBST to optimise the peak signal to noise ratio (PSNR) of image during HE.

3.1.2 Selection of block size by optimum PSNR-based DBST

In our research work, we found very interesting fact that there a remarkable relationship between block size used in block-based HE technique and PSNR of the output image after HE. The relationship is shown in Figure 8. Figure 8(b) shows that for every different image there is a unique block size which produces maximum PSNR for that image.

$$i = max_{i=0}^{n-1} PSNR_i \tag{5}$$

By using equation (5) find the suitable value of i for which PSNR is maximum. Where i is the selection of block size as i * i for HE. Now give this i as input to CLAHE as the block size for the image which is used to calculate the i.

3.1.3 Applying CLAHE

After calculating the value of i we apply CLAHE on the object image with block size i. This is designed correctly for nonmonotonous images with noise. All the steps used for CLAHE are shown in Figure 4.

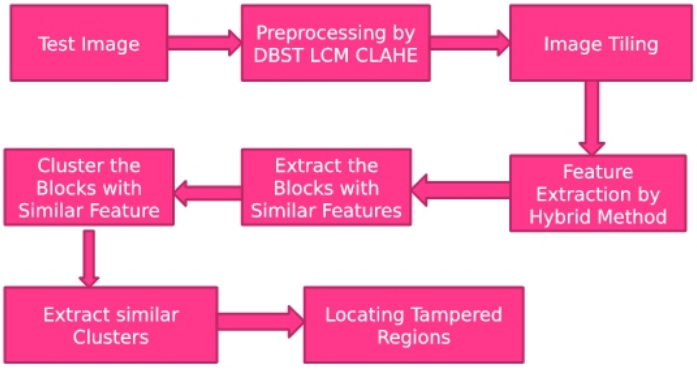
3.1.4 Algorithm

We have named proposed method as DBST-LCM CLAHE since it uses dynamic block size. Block size in our proposed method is not fixed for all images. These are decided on the basis of categories of images based on feature distribution and noise. Algorithmic representation of the proposed method is given as follows.

Algorithm 1 DBST-LCM-CLAHE

Result: HE image
Inputs: Fine detailed image from LCM, enhancing parameter;
begin;
Step 1: Obtain inputs like number of regions, dynamic range and clip limit;
Step 2: Clculate optimum block size i using $i = max_{i=0}^{n-1} PSNR_i$;
Step 3: Process the inputs;
Step 4: Process each contextual region producing gray level mapping;
Step 5: Intepolate gary level mapping in order to assemble final image;
end;

Figure 7 Flow graph of proposed method (see online version for colours)



3.2 Proposed method of cloned object detection in copy move forged images

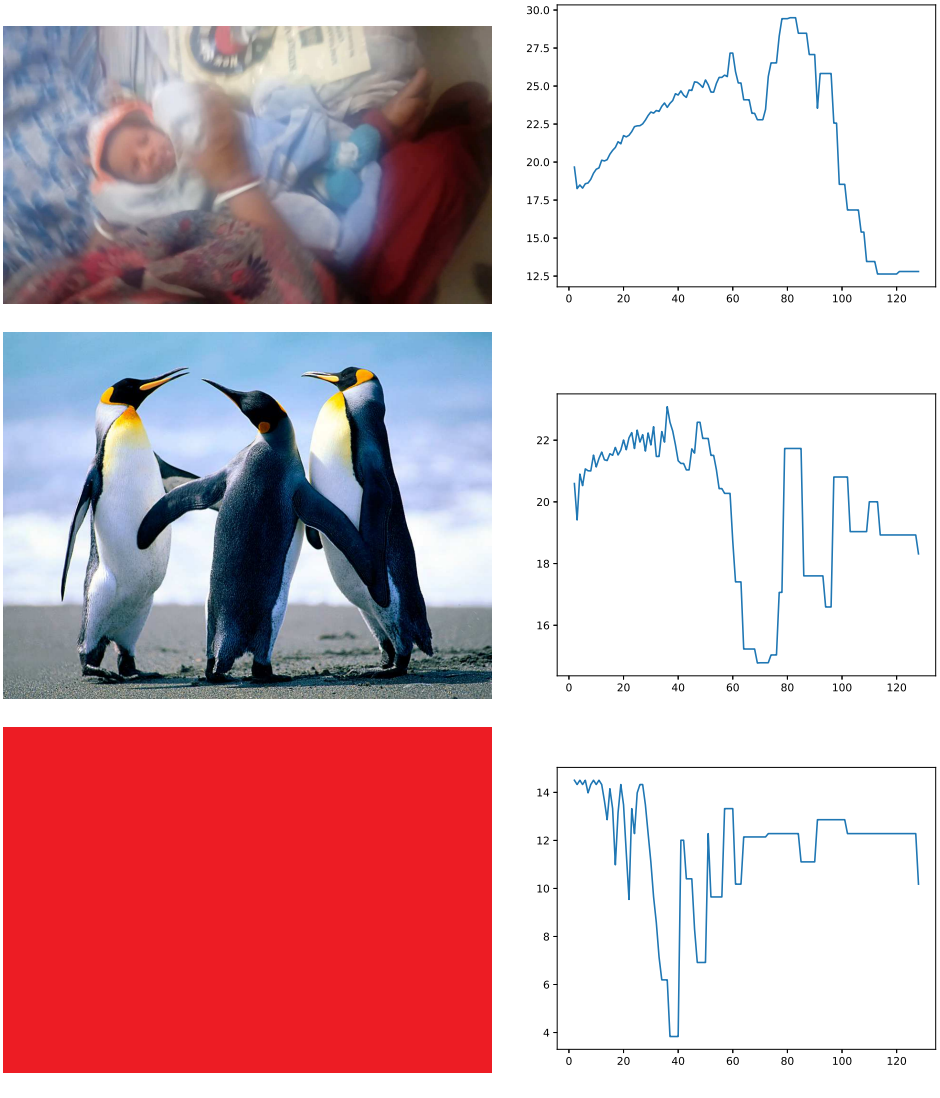
We have named proposed method as hybrid copy move forgery detection since it uses varying contrast as well as hybridisation of ad hoc, PCA and SIFT method. The contrast in our proposed method is not fixed for all images. These are decided on the basis of categories of images based on feature distribution and noise. Hybrid approach provides the accuracy in term of F_Score. Flow graph of the proposed method is given in Figure 7.

4 Experiment results and discussion

4.1 Results of proposed DBST-LCM-CLAHE

We have implemented our proposed method in Python 3.6 and image packages of Python like skimage, OpenCV, and other science packages, ubuntu 16 operated i3 core system as a hardware platform. We have used three generalises category of images shown in Figure 1.

Figure 8 Effect of block size over PSNR in HE (see online version for colours)

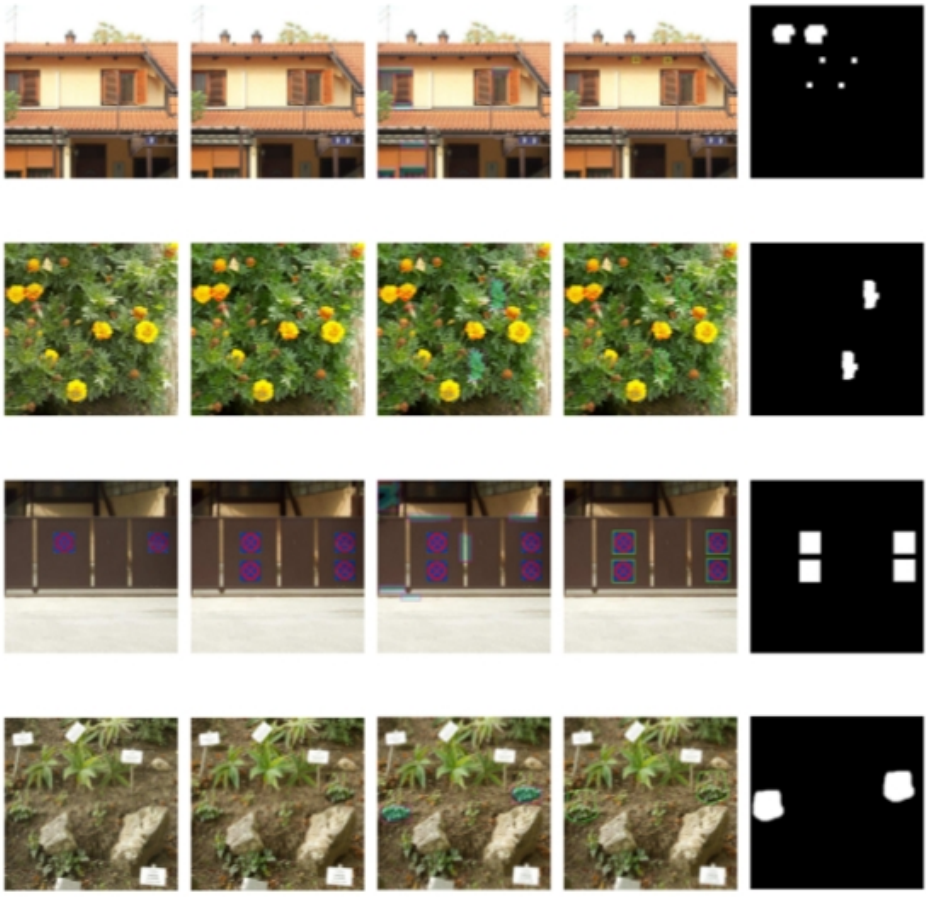


(a) (b)

4.1.1 Performance measurement of DBST-LCM-CLAHE

We have measured the performance of our proposed method on the basis of the very critical parameter related to image quality like PSNR, mean square error (MSE), normalise root mean square error (NRMSE), structure similarity index map (SSIM) and entropy. The higher value of PSNR, SSIM, and entropy shows better quality of image whereas the lower value of MSE and NRMSE promise the better quality of the image.

Figure 9 Results of proposed method over distorted images, (a) original images (b) tampered images (c) detection by state of art technique (d) detection by proposed method (e) localisation of tampered region by proposed method (see online version for colours)



(a) (b) (c) (d) (e)

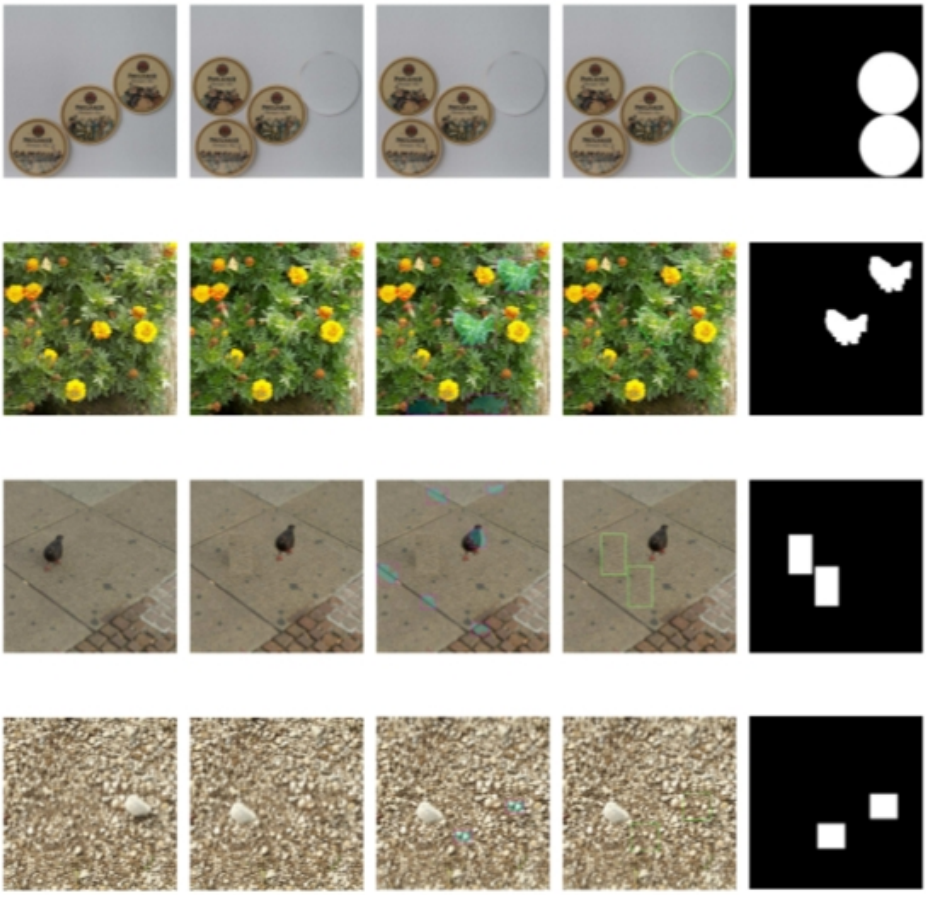
4.1.2 Compairing with existing techniques of pre-processing

In this section, we compare state of the art technology with our proposed method in terms of PSNR, MSE, NRMSE, SSIM, and entropy. The results of the comparison are shown in Table 1, which prove the promising improvements.

Table 1 HE performance comparison table (see online version for colours)

Image	*HE technique*	*PSNR*	*MSE*	*NRMSE*	*SSSIM*	*Entropy*
	• CLAHE	• 18.86	• 844.79	• 0.21	• 0.88	• 22.40
	• LCM-CLAHE	• 11.23	• 4,888.0	• 0.52	• 0.58	• 22.31
	• Proposed method	• 29.36	• 75.29	• 0.06	• 0.93	• 22.40
	• CLAHE	• 20.82	• 537.39	• 0.14	• 0.81	• 22.95
	• LCM-CLAHE	• 20.82	• 537.39	• 0.14	• 0.81	• 22.95
	• Proposed method	• 22.02	• 408.00	• 0.12	• 0.78	• 22.96
	• CLAHE	• 38.58	• 9.00	• 0.03	• 0.99	• 19.06
	• LCM-CLAHE	• 19.50	• 729.00	• 0.30	• 0.96	• 19.06
	• Proposed method	• 19.50	• 2,401.0	• 0.53	• 0.91	• 19.06

Figure 10 Results of proposed method over images having translation attack, (a) original images (b) tampered images (c) detection by state of art technique (d) detection by proposed method (e) localisation of tampered region by proposed method (see online version for colours)

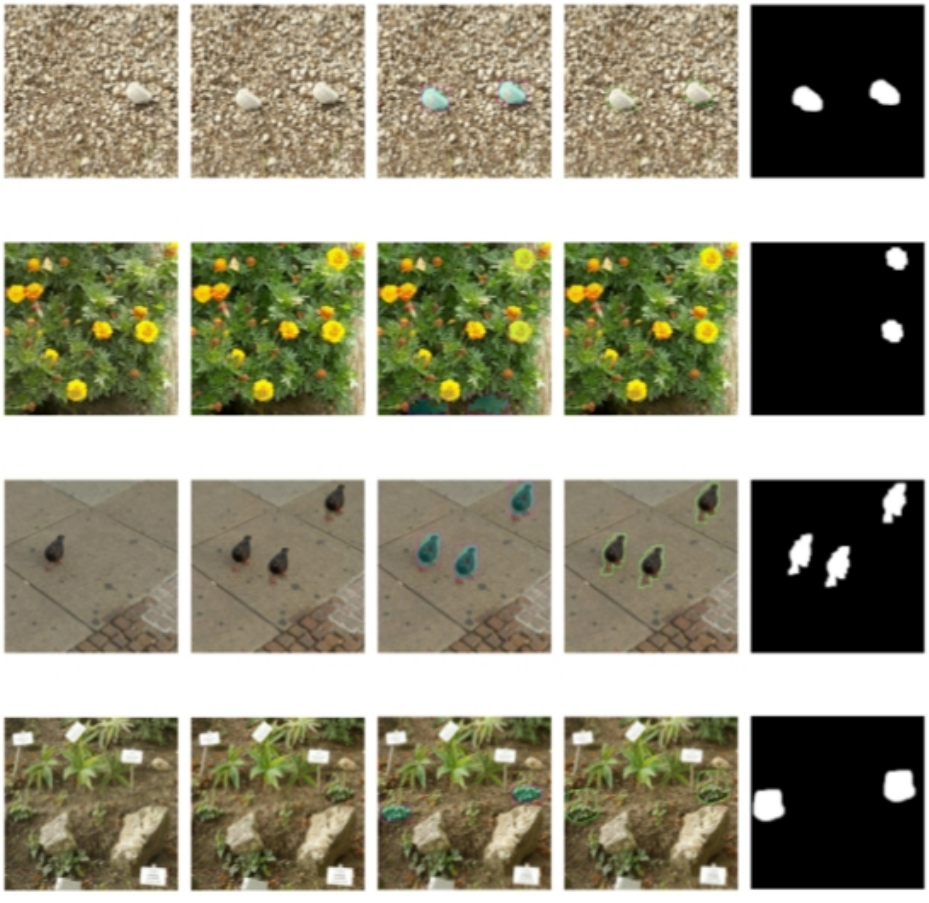


(a) (b) (c) (d) (e)

4.1.3 Improvements in DBST-LCM-CLAHE

As we have promised in the section of the proposed method for remarkable improvements in PSNR, so it is clear from performance comparison Table 1, that our proposed method have remarkable positive improvements.

Figure 11 Results of proposed method over images having combined attach attack, (a) original images (b) tampered images (c) detection by state of art technique (d) detection by proposed method (e) localisation of tampered region by proposed method (see online version for colours)



(a) (b) (c) (d) (e)

4.2 Results of the proposed method of cloned object detection in copy move forged images

Here we are discussing the formulation of parameters used for performance measurement

$$TPR = \frac{imgfd}{imgf} \tag{6}$$

$$FPR = \frac{imgod}{imgo} \tag{7}$$

$$F_{Score} = \frac{TPR}{TPR + FPR} * 100 \tag{8}$$

where

$imgfd$ images detected as forged being forged

$imgf$ number of forged images

$imgod$ images detected as forged being original

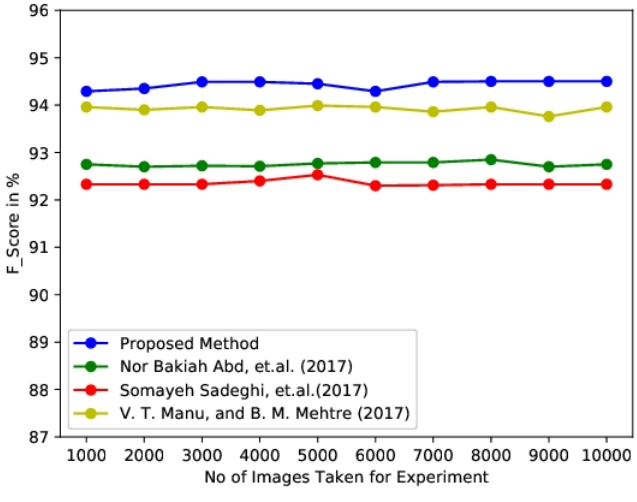
$imgo$ original images

We have used CoMoFoD (Tralic et al., 2013) database for evaluation of proposed scheme. Experimental results show the promising improvements in the compassion of state of the art techniques. Performance comparison is done on the basis of true positive rate (TPR), false positive rate (FPR), and F_Score.

4.2.1 Comparison with state of art technique of duplicate object detection in images

As we have promised in the section of the proposed method for remarkable improvements in F_score. Figure 12 shows the rigorous evaluation evidence for improvement in the proposed method that our proposed method has remarkable positive improvements. Existing techniques (Sadeghi et al., 2017; Warif et al., 2017; Manu and Mehtre, 2017) have F_scores 92.75, 92.33, and 93.96 respectively. Our proposed method shows 94.29 F_score. More F_score promise robust detection technique.

Figure 12 Graph showing performance of proposed method with respect to state of art techniques (see online version for colours)



5 Conclusions and future work

In our research work, we have developed a new method of HE to de-noise, and the same is presented in this paper. Our method is based on dynamic block size selection for HE by CLAHE to de-noise the image up to optimum PSNR. In our research work, we have taken three categories of images one non-monotonous image with noise, the second nonmonotonous image without noise third monotonous image. The proposed method is evaluated by the different measuring feature of the image like MSE, NRMSE, and SSIM. As shown in Subsection 4.1.2 and Table 1 our method is proved for remarkable improvement in PSNR, MSE, NRMSE and SSIM in case of the non monotonous image with noise specially.

In future this research may be carried forward towards making the automatic selection of block size depending on the feature of the input image and use of the proposed method in pre-processing phase of copy-move forgery detection to improve the performance of state of the art techniques. In addition to the above, we aimed to develop a new approach to cloned object detection and have developed it, and the same is presented in this paper. Our method is based on the integration of pre-processing, hybridisation of feature extraction techniques and rigorous pre-processing of the image before applying detection method. In our experiment, we have evaluated our proposed method by using CoMoFoD image database. Results show promising improvement regarding TPR, FPR, and F_score. In our experiment we have compared three state of the art techniques (Sadeghi et al., 2017; Warif et al., 2017; Manu and Mehtre, 2017). Our method shows better performance as described in Figure 12 in comparison to these state of art techniques. Figures 9, 10, and 11 illustrate the improvement in detection and localisation of copy and move forgery, and Figure 12 shows the graphical representation of performance comparison with state of the art techniques mentioned here. In future, this research may be carried forward towards making automatic detection of image forgery that depends on the feature of the input image and use of the proposed method in pre-processing phase of copy-move forgery detection to improve the performance of state of the art techniques.

References

Adel, E., Elmogy, M. and Elbakry, H. (2015) 'Image stitching system based on ORB feature-based technique and compensation Blending', *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 9, pp.55–62.

Aglave, P. and Kolkure, V.S. (2015) 'Implementation of high performance feature extraction method using oriented fast and rotated brief algorithm', *International Journal of Research in Engineering and Technology*, Vol. 4, No. 2, pp.394–397.

Alberry, H.A., Hegazy, A., Salama, G.I. (2018) 'A fast SIFT based method for copy move forgery detection', *Future Computing and Informatics Journal*, DOI: 10.1016/j.fcij.2018.03.001.

Bay, H., Tuytelaars, T. and Gool, L.V. (2006) 'SURF: speeded up robust features', *ECCV 2006, Part I, LNCS 3951*, Springer-Verlag, Berlin, Heidelberg, pp.404–417.

Bi, X. and Pun, C-M. (2018) 'Fast copy-move forgery detection using local bidirectional coherency error refinement', *Pattern Recognition*, Vol. 81, pp.161–175.

Chakraverti, A.K. and Dhir, V. (2017) 'A review on image forgery and its detection procedure', *International Journal of Advanced Research in Computer Science*, Vol. 8, No. 4, pp.440–443.

Chaudhari, K. and Garg, D. (2017) 'An enhanced approach in image mosaicing using ORB method with alpha blending technique', *International Journal of Advanced Research in Computer Science*, Vol. 8, No. 5, pp.917–921.

Dixit, R. and Naskar, R. (2017) 'Review, analysis, and parameterization of techniques for copy-move forgery detection in digital images', *IET Image Processing*, DOI: 10.1049/iet-ipr.2016.0322.

Dixit, R., Naskar, R. and Mishra, S. (2017) 'Blur-invariant copy-move forgery detection technique with improved detection accuracy utilizing SWT-SVD', *IET Image Processing*, DOI: 10.1049/iet-ipr.2016.0537.

Emam, M., Han, Q., Li, Q., Zhang, H. and Emam, M. (2017) 'A robust detection algorithm for image copy-move forgery in smooth regions', *International Conference on Circuits, System, and Simulation (ICCSS)*, IEEE, London, UK, DOI: 10.1109/CIRSYSSIM.2017.8023194.

Jin, G. and Wan, X. (2017) 'An improved method for SIFT-based copy-move forgery detection using non-maximum value suppression and optimised J-Linkage', *Signal Processing: Image Communication*, [online] http://dx.doi.org/10.1016/j.image.2017.05.010.

Karami, E., Prasad, S. and Shehata, M. (2017) *Image Matching Using SIFT, SURF, BRIEF and ORB: Performance Comparison for Distorted Images*, arXiv:1710.02726v1, Faculty of Engineering and Applied Sciences, Memorial University, Canada.

Kashyap, A., Parmar, R.S., Agarwal, M. and Gupta, H. (2017) *An Evaluation of Digital Image Forgery Detection Approaches*, arXiv:1703.09968v2 [cs.MM], Cornell University Library.

Kaur, N. (2017) 'A review paper on copy move forgery detection techniques', *International Journal of Advanced Research in Computer Science*, Vol. 8, No. 7, pp.157–161.

Kulkarni, A.V., Jagtap, J.S. and Harpale, V.K. (2013) 'Object recognition with ORB and its implementation on FPGA', *International Journal of Advanced Computer Research*, Vol. 3, No. 3, pp.164–169.

Kuznetsov, A. and Myasnikov, V. (2017) 'A new copy-move forgery detection algorithm using image preprocessing procedure', *Procedia Engineering* Vol. 201, pp.436–444, DOI: 10.1016/j.proeng.2017.09.671.

Lai, Y., Huang, T., Lin, J. and Lu, H. (2017) 'An improved block-based matching algorithm of copy-move forgery detection', *Multimedia Tools Appl.*, DOI: 10.1007/s11042-017-5094-y.

Lin, C., Lu, W., Sun, W., Zeng, J., Xu, T. and Lai, J-H. (2017) 'Region duplication detection based on image segmentation and keypoint contexts', *Multimedia Tools Appl.*, DOI: 10.1007/s11042-017-5027-9.

Liu, B. and Pun, C-M. (2018) 'Locating splicing forgery by fully convolutional networks and conditional random field', *Signal Processing: Image Communication*, Vol. 66, No. 8, pp.103–112.

Mahmood, T., Irtaza, A., Mehmood, Z. and Mahmood, M.T. (2017) 'Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images', *Forensic Science International* [online] http://dx.doi.org/10.1016/j.forsciint.2017.07.037.

Mahmood, T., Mehmood, Z., Shah, M. and Saba, T. (2018) 'A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform', *Journal of Visual Communication and Image Representation*, Vol. 53, pp.202–214.

Manu, V.T. and Mehtre, B.M. (2017) 'Copy-move tampering detection using affine transformation property preservation on clustered keypoints', *SIViP*, DOI: 10.1007/s11760-017-1191-7.

Mursi, M.F.M., Salama, M.M. and Habeb, M.H. (2017) 'An improved SIFT-PCA-based copy-move image forgery detection method', International Journal of Advanced Research in Computer Science and Electronics Engineering, Vol. 6, No. 3, pp.23–28.

Nedjah, N. (2017) 'Editorial new trends for pattern recognition: theory & applications', *Neurocomputing*, DOI: 10.1016/j.neucom.2017.05.080.

Novozamsky, A. and Sorel, M. (2018) 'Detection of copy-move image modification using JPEG compression model', *Forensic Science International*, Vol. 283, pp.47–57.

Park, C-S. and Choeh, J.Y. (2017) 'Fast and robust copy-move forgery detection based on scale-space representation', *Multimedia Tools Appl.* [online] https://doi.org/10.1007/s11042-017-5248-y.

Patel, A., Kasat, D.R., Jain, S., Thakare, V.M. (2014) 'Performance analysis of various feature detector and descriptor for real-time Video-based face tracking', *International Journal of Computer Applications*, Vol. 93, No. 1, pp.34–41.

Pun, C-M. and Chung, J-L. (2018) 'A two-stage localization for copy-move forgery detection', *Information Sciences*, 9 June 2018, Vols. 463–464, pp.33–35.

Rublee, E., Rabaud, V., Konolige, K. and Bradski, G. (2011) 'ORB: an efficient alternative to SIFT or SURF', *International Conference on Computer Vision*, Barcelona, Spain, 6–13 November, DOI: 10.1109/ICCV.2011.6126544.

Sadeghi, S., Jalab, H.A., Wong, K., Uliyan, D. and Dadkhah, S. (2017) 'Keypoint based authentication and localization of copy-move forgery in digital image', *Malaysian Journal of Computer Science*, Vol. 30, No. 2, pp.117–133.

Senthilkumaran, N. and Rajesh, R. (2009) 'Edge detection techniques for image segmentation – a survey of soft computing approaches', *Int. J. of Recent Trends in Engineering and Technology*, Vol. 1, No. 2, pp.250–254.

Sharma, S. and Ghanekar, U. (2018) 'A hybrid technique to discriminate natural images, computer generated graphics images, spliced, copy move tampered images and authentic images by using features and ELM classifier', *Optik*, Vol. 172, pp.470–483.

Sonka, M., Hlavac, V. and Boyle, R. (1993) 'Image pre-processing', *Image Processing, Analysis and Machine Vision*, pp.56–111.

Thirunavukkarasu, V., Kumar, J.S., Chae, G.S. and Kishorkumar, J. (2017) 'Non-intrusive forensic detection method using DSWT with reduced feature set for copy-move image tampering', *Wireless Pers Commun.*, DOI: 10.1007/s11277-016-3941-1.

Tralic, D., Zupancic, I., Grgic, S., and Grgic, M. (2013) 'CoMoFoD – new database for copy-move forgery detection', in *Proc. 55th International Symposium ELMAR-2013*, pp.49–54.

Vinay, A., Kumar, C.A., Shenoy, G.R., Murthy, K.N.B. and Natarajan, S. (2015) 'ORB-PCA based feature extraction technique for face recognition', in *Procedia Computer Science*, Vol. 58, pp.614–621.

Warif, N.B.A., Wahab, A.W.A., Idris, M.Y.I., Salleh, R. and Othman, F. (2017) 'SIFT-symmetry: a robust detection method for copy-move forgery with reflection attack', *J. Vis. Commun. Image R.* [online] http://dx.doi.org/10.1016/j.jvcir.2017.04.004.

Wo, Y., Yang, K., Han, G., Chen, H. and Wu, W. (2016) 'Copy–move forgery detection based on multi-radius PCET', *IET Image Processing*, DOI: 10.1049/iet-ipr.2016.0229.

Yang, F., Li, J., Lu, W. and Weng, J. (2017a) 'Copy-move forgery detection based on hybrid features', *Engineering Applications of Artificial Intelligence*, Vol. 59, pp.73–83 [online] http://dx.doi.org/10.1016/j.engappai.2016.12.022.

Yang, H-Y., Niu, Y., Jiao, L-X., Liu, Y-N., Wang, X-Y. and Zhou, Z-L. (2017b) 'Robust copy-move forgery detection based on multi-granularity superpixels matching', *Multimedia Tools Appl.*, DOI: 10.1007/s11042-017-4978-1).

Yu, L., Yu, Z. and Gong, Y. (2015) 'An improved ORB algorithm of extracting and matching features', *International Journal of Signal Processing, Image Processing, and Pattern Recognition*, Vol. 8, No. 5, pp.117–126.

Zhang, D., Liang, Z., Yang, G., Li, Q., Li, L. and Sun, X. (2017) 'A robust forgery detection algorithm for object removal by exemplar-based image inpainting', *Multimedia Tools Appl.*, DOI: 10.1007/s11042-017-4829-0.