INTERNATIONAL JOURNAL OF SOFT COMPUTING

MEDWELL PUBLICATIONS

Copy-Move Image Forgery Detection Techniques: A Literature Survey

[1]Hesham Ahmed Alberry, [1]Abdelfatah Hegazy and [2]Gouda I. Salama
[1]*Department of Computer Science, Faculty of Computers and Information, Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt*
[2]*Department of Computer Engineering, MTC, Cairo, Egypt*

Key words: Copy-move forgery, image forgery, forgery detection techniques, forgery attacks, block based, key point based

Corresponding Author:
Hesham Ahmed Alberry
Department of Computer Science, Faculty of Computers and Information, Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt

Page No.: 13-19
Volume: 15, Issue 1, 2020
ISSN: 1816-9503
International Journal of Soft Computing

Abstract: Digital image editing tools establishing the authenticity of multimedia content have become a challenging issue where creating digital image forgeries has become easier. Digital image forensics is an increasingly growing research field that deals with the detection of the cyber-crime and forgery by investigation of digital evidences. Thus, law enforcement and forensics experts require reliable and efficient means of detecting Image forgery. Copy move Image Forgery is one of the most common forgeries which is used to hide some important information, object or duplicate apart of the same image where some parts of the image is copied and pasted to another part in the same image. This type of forgery is more difficult than other ones because the copied part has the same characteristics as it belongs to the same image. This study presents a survey of various image forgery detection techniques.

INTRODUCTION

Digital image tampering becomes a main challenging issue with the progress of media editing software. Digital image plays a significant role in different fields on news report, forensics science in-courtrooms evidences, surveillance services, online marketing and medical diagnosis in a way that initiate retrieving trust to digital image. Forgers develop many techniques to tamper images. These techniques can be classified into three types:

Copy/move forgery: It is one of the most common forgeries which is used to hide some important information, object or even duplicate apart of the same image as shown in Fig. 1 apart of tree used to hide the truck[1].

Image splicing: Different parts from multiple images are integrated into a single image. Figure 2 shows an example of image splicing where different elements from two images are merged into a single image to create the forged image[2].

Image retouching: It includes slight change in the image for different purposes which may be commercial. Retouching is used to reduce certain features in the image, change color or blur background. Figure 3 shows an example of image retouching where real face is on the right and left shows the retouched image[2].

The image forgery detection techniques can be classified as active and passive[3]. The active techniques depend on digital signatures or water marking which require prior information about the original image and this technique is not effective and needs special cameras to

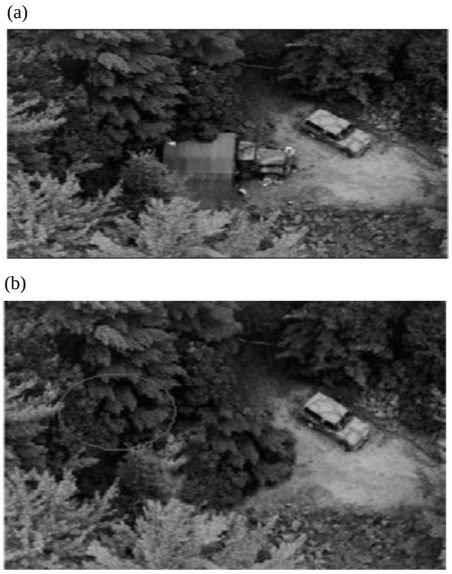

Fig. 1(a, b): Copy-move forgery in a image, (a) The orignal image and (b) The forged image

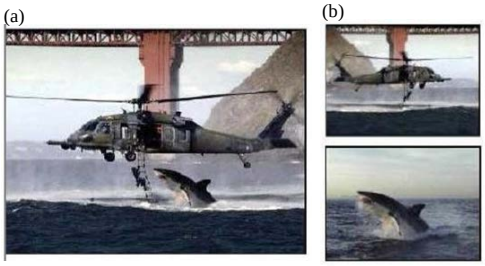

Fig. 2(a, b): Copy-move forgery in a digital image, (a) The spliced image and (b) The two original images

have water mark or signature in image capture and is easy to tamper. Passive techniques are used to analyze images without any heading information where a blind decision must be determined regarding how images have been tampered with. Most passive techniques are based on supervised learning through the extraction of specific features to differentiate the original image from tampered image. The passive image forgery techniques can be classified into the following categories[4]:

Pixel-based techniques: They analyze the correlations pixel-level which arise from a specific form of tampering.

Format-based techniques: Most cameras encode images in different format and the most common is the JPEG format. This compression scheme can be used to detect forgery by detecting how much compression is fulfilled.

Physically based technique: The brightness through various sides of the image can be used as forgery detection techniques.

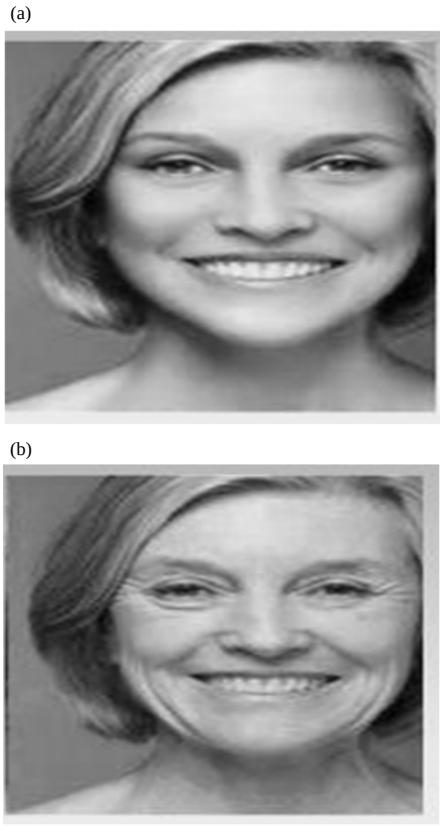

Fig. 3(a, b): Example of image retouching, (a) Forged image and (b) The orignal image

Camera-based techniques: Color filter array and Chromatic Aberration can be used to detect forgery.

Geometric-based techniques: They depend on the projection of the camera center onto the image plane which is near the center of the image. This study discusses the pixel-based technique for the copy-move forgery as it is the most common forgery type. This survey study is organized as follows.

Copy-move forgery attacks: Practically, Forgers do not just copy and move region in images. They may involve more than a simple duplicating operation. Several image processing attacks could be involved in copy-move forgery as shown in Fig. 4. These attacks are divided into two categories: copied part attacks and whole image attacks. Copied part attacks are used to provide changes in the copied regions during the forgery operation. The copied part attacks could be rotation, scaling, mirroring or brightness adjustments. Practically, two or more copied part attacks can be combined. The whole image attacks such as the additive noise, JPEG compression or blurring are used to remove any assigned traces of the copy-move operation in the whole image such as sharp edges or color differences[3].

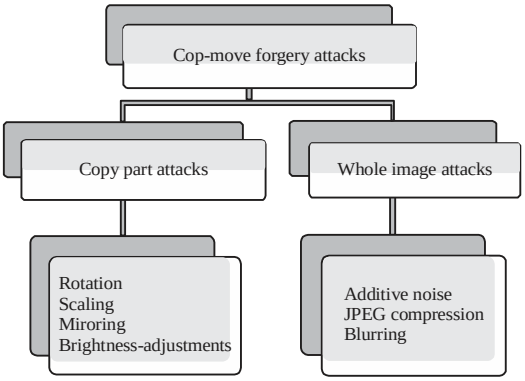

Fig. 4: Types of copy-move frogery attacks

Available datasets: There are limited available datasets designed for copy move image forgery such dataset should contain different original and tampered images with different attacks that affect detection process accuracy like image rotation, scaling, blurring, brightness adjustment and adding noise. The available data sets may not be enough to the needs of researchers; the researchers may use some editing software such as adobe photoshop to prepare images for evaluating their techniques. An example of The most common existing data sets[5] is the MICC-F220 dataset which contains 220 image and MICC- F2000 which contains 2000 image. These datasets contain images with limited attacks. Only different combinations of scaling and rotation attacks are already applied to each forged image of the dataset. In each of these datasets, half of the images are tampered. Other researchers use a subset from the CoMoFoD database which contains total number of 260 images that have applied attacks like translation, rotation, scale, distortion and combine between them.

PERFORMANCE EVALUATION

The performance of detection methods have many types of calculations to know the accuracy of detecting. It is required to know the number of original and forged image and different attacks that occur on image on data sets. The most commonly evaluation criteria use True Positive Rate (TPR), False Positive Rate (FPR)[6] where:

$$\text{TPR} = \frac{\text{Images detected as forged being forged}}{\text{Total number of forged images}}$$

$$\text{FPR} = \frac{\text{Images detected as forged being orignal}}{\text{Total number of orignal images}}$$

TPR is the percentage of forged images which are correctly identified. FPR is the percentage of the original images which are wrongly identified as forged. Another related performance measure is the Success rate[7] by using the following equation:

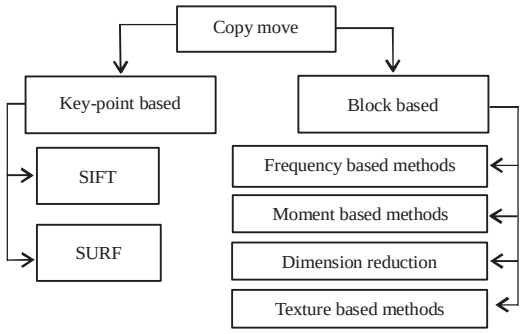

Fig. 5: Copy-move frogery detection classfication

$$\text{Success rate} = \frac{\text{Tp}}{\text{Tp+Fp+Fn}}$$

where, Tp indicates the number of images correctly identified as forged and Fp are the number of images falsely identified forged and FN are the number of forged images where forgery could not be detected. Other researchers use Pixel Detection Accuracy (PDA) and Pixel False Positive (PFP) rate[8] for evaluation of localization performance at pixel-level. These standard procedures define the ratio of correctly detected duplicated regions and the ratio of regions incorrectly selected as duplicate, this evaluation procedures defined as follows:

$$\text{PDA} = \frac{\text{Duplicate region} \cap \text{detected region}}{\text{duplicate region}}$$

$$\text{PDA} = \frac{\text{Duplicate region} - \text{detected region}}{\text{duplicate region}}$$

COPY-MOVE FORGERY DETECTION

The problem of copy-move forgery detection is faced by considering different methods which are categorized as either key-point based methods or block based methods as[4] shown in Fig. 5.

The two methods and the different algorithms for each method will be explained in the following section.

Block-based image forgery detection techniques: These methods are based on using blocks of image for analyzing the forgery. Most block based methods have the same main steps[9] as shown in the common workflow Fig. 6. First, get the input image and apply pre-processing step which is important for improvement of image data and it also enhances image features which are important for further detection. The input image converted into grey-scale. The image is then divided into fixed or overlapping blocks and features are for each block. The regions of copy-move pairs are identified by searching blocks with high similarity by matching feature detectors which can be regarded as duplicated regions.

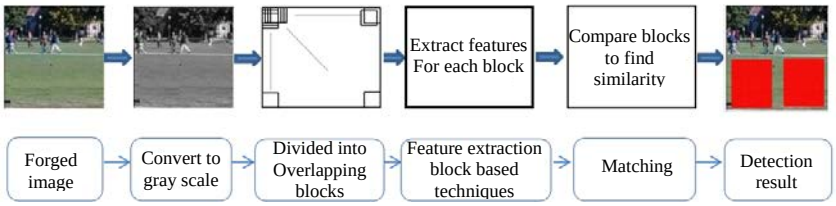

Fig. 6: Typical workflow for block based frogery detection

Block based techniques suffer from high computational complexity due to the number of divided image blocks and the time it takes for matching. Another limitation of these methods is the weakness of discovering the forgery done with some operation on the copied region such as scaling and rotation. Block-based techniques are categorized into four main categories: Frequency Based methods, moment based methods, Dimensionality reduction based and texture based methods.

Frequency based methods: The most common used technique in frequency-based methods is DCT (Discrete Cosine Transform). Other frequency-based techniques that are also used in copy-move forgery are Discrete Wavelet Transform (DWT), Fourier-Mellin Transform (FMT), Polar Harmonic Transform (PHT) and Local Binary Pattern (LBP). Frequency-based techniques robust to multiple copy move forgery, noise contamination, Gaussian blurring and very slight rotation and scaling. Kumar *et al*.[7] proposed a method that uses the DCT coefficients to represent the overlapping block. The proposed algorithm is tested with a dataset of 100 images, The dataset consists of images with different resolutions and contrasts. The size of the forged region is also varied in the dataset.

Some images in the dataset are taken from the benchmark dataset. For evaluating the robustness of the algorithm against added noise, zero mean Gaussian noise is added to the forged images with Signal to Noise Ratio (SNR) ranging from 90-40 dB. Also JPEG compressed images with different quality factors are used in the evaluation. Double duplication is performed on some of the images. The proposed method detects with 100% success rate for SNR above 50 dB. The success rate is decreased to 90% for SNR down to 40 dB. Below 40 dB, success rate is decreased to <50%. Robustness against JPEG compression is also checked and 100% success rate is observed up to quality factor 8. The success rate is decreased to 50% for JPEG quality factor 7.5. The proposed algorithm is robust against slight scaling and rotation up to 2%. Moreover, the detection efficiency highly depends upon the size of the copy moved region, especially, in case of rotation and scaling. So, the robustness decreases with the decrease in the size of copy moved region. The average execution time for this research is 25 sec for an image of size 640×480.

Moment based methods: The Moment-based methods detect copy-move forgery, even with attacks like blurring, rotation, noise addition or contrast changes in the duplicated regions. The most common technique for moment-based method uses Zernike moments to detect copy-move forgery in forged images. Other moment-based techniques that are also used in copy-move forgery are Hu moments and BLUR moments. Ryu *et al*.[8] propose a forensic technique to localize duplicated image regions based on Zernike moments of image blocks. Within this paper, four major achievements greatly advance the field of CRM (Copy-Rotate-Move) detection and get rid of some of the defects of other techniques. First, they represent individual blocks by Zernike moments up to an accurate order. A rotation-invariant magnitude makes these moments particularly bright CRM detection features. The second accievement is an efficient block matching procedure based on Locality Sensitive Hashing (LSH) method. Third, they transfer the phase of Zernike moments into a feature space error-reduction procedure to increase accuracy. Finally, test setup is based on a set of 1000 images results in a complete benchmark to insure the CRM detection methods. In particular, they clearly distinguish between ‘smooth’ and ‘textured’ duplicated regions. Researches regard both pixel-level localization and image-level detection of manipulations, respectively, different sizes of images and duplicated regions tested as well as robustness against some representative distortions and attacks. They use a randomly selected subset of the BOSS image database for their evaluation. They use Pixel Detection Accuracy (PDA) and Pixel False Positive (PFP) rate for evaluation of localization performance at pixel-level. They get accuracy result with average of 99.4 for rotation up to 900. In addition, they get accuracy average of 96 with scaling options from 50-150%. It also gives high accuracy in case of JPEG compression and applied white Gaussian noise and that achieves >98 but with lower accuracy in case of blurring with such 86°. The computation time of this technique, achieves 342 sec for images with size of 512×512 pixels.

Dimension reduction: Dimension reduction techniques are commonly used with domain features to reduce the dimensionality of the image and to improve the complexity. Dimension reduction techniques are like PCA (principal component analysis), Singular Value Decomposition (SVD) and Locally Linear Embedding (LLE). Dimension reduction techniques robust to various operations like rotation, scaling, Gaussian noise and filtering. However, they have poor results in loss of image details resulting in the low performance in JPEG compression. Ting and Rang-Ding[10] proposed a method based on SVD. The algorithm has low computational complexity and is more robust against attacks such as scaling, rotation, noise contamination and Gaussian blurring. This study limitation are with detection forgery with JPEG compression and it fails to explain which part is copied and which is pasted in duplication regions.

Texture based methods: Texture-based approach uses texture features to detect copy move forgery. There are many texture descriptors like statistical descriptors, edge histogram, Tamura descriptors, Gabor Descriptors and Haralick descriptors. These texture-based techniques are poor in forgery detection with high degrees of rotation and scaling to the copied regions. Lee[11] proposed a method based on Gabor magnitude. The main advantages of their method are that the Histogram of Orientated Gabor Magnitude (HOGM) has high efficiency in detecting and accurately locating multiple instances of copy-move forgery within a single image. In addition, they develop a noise detector for the removal of false blocks. Moreover, the proposed technique is able to accurately locate duplicated regions affected by common post-processing techniques such as image rotation, scaling, JPEG compression, blurring and brightness adjustment. In most cases, this method achieves better performance than other well-known approaches. In addition, the method is even effective in dealing with images of high resolution. The method also has reduced computational complexity by using lower feature vector. This study evaluated using two publicly available databases designed for image forgery detection. The first one was the CoMoFoD database and the second dataset is comprised of several color PNG images released from the Image Manipulation Dataset. The performance of this algorithm evaluated using two evaluation criteria, Correct Detection Ratio (CDR) and False Detection Ratio (FDR). CDR indicates the performance of the algorithm in terms of accurately locating the pixels of copy-move regions in the forged image while FDR reflects the percentage of pixels that are not contained in the duplicated region but are regarded as duplicated. This copy-move forgery detection algorithm has detection results with noise detector using CoMoFoD dataset with average CDR .954 and detection results without noise detector using CoMoFoD dataset 0.804 and detection results using forged images distorted by scaling the average CDR is 0.71. Also, it has detection results of forged images distorted by JPEG compression with average CDR of 0.76 and with Image blurring by average of 0.946 and with Brightness adjustment by average of CDR 0.971. The proposed algorithm gives poor detection outcome with great rotation, scaling and noise addition. This makes the detection of copy-move forgery far more challenging. Lee *et al*.[12] proposed a method using Histogram of Orientated Gradients. (HOG) features of each block of the image are extracted using HOG descriptors which are implemented as a matrix of the same size of the block, similar block pairs are matched, a map of duplicated regions is created and similar features are located in different blocks. Finally, identify regions that are similar by using the Euclidian distance and that would reduce the time. In this study, the author adopted two databases; the first was obtained from the CoMoFoD database and the second dataset contained 30 high resolution images obtained from a Google image search then manipulate using copy-move forgery and then apply different attacks like translation, rotation, blurring, brightness change and color reduction. To illustrate the performance of the proposed algorithm, the author introduced two evaluation criteria: the correct detection ratio and the false detection ratio. The method gets detection results accuracy in general >0.9. The proposed algorithm is able to detect and accurately locate multiple instances of copy-move forgery in a single image and achieve good results against attacks such as translation, small rotation, blurring, adjustment of brightness and color reduction. The proposed method does not perform particularly well in the detection of duplications with slight rotation and slight scaling only.

Key point-based image forgery detection techniques: Image key points which are regions with high-entropy are extracted and matched over the whole image for identifying copied regions and the key point techniques are such as Scale Invariant Feature Transform SIFT and Speeded-up Robust Features SURF. This algorithms uses a fewer features which reduce computational complexity[13]. Most keypoint-based methods have the same main steps as shown in the common workflow Fig. 7. Firstly, key point-based method finds image key points to obtain image features[14]. Key points are locations that contain distinct information of the image content. Each key point is characterized by a feature vector that consists of a set of image statistics collected at the local neighborhood of the corresponding key point then a similarity measure is applied to get results. Amerini *et al*.[15] proposed a method using Scale Invariant Features Transform (SIFT) which allows to indicate if a copy-move attack has occurred. In addition, recover the geometric transformation used to perform cloning and

Fig. 7: Typical workflow for keypoint based frogery detection

also to deal with multiple cloning. Detection performance was measured in terms of True Positive Rate (TPR) and False Positive Rate (FPR) where TPR is the fraction of tampered images correctly identified while FPR is the fraction of original images that are not correctly identified. Algorithm is evaluated according to different attacks types. The maximum accuracy of 99.37. In case of JPEG compression maximum accuracy of 93.42 and by Gaussian noise addition with detected their forgery by maximum accuracy of 94.14. The proposed method is evaluated using two datasets: a small dataset named MICC-F220 and a larger dataset named MICC-F2000. This paper limitation in detection phase with respect to the cloned image patch with highly uniform texture where noticeable keypoints are not recovered by this method. Sudhakar *et al*.[16] proposed a method to detect copy move forgery using SIFT.

The proposed method is invariant scale and rotation of the copied object and effective detection for multiple forgery. This study concentrates on reducing the number of key points required for detection of forgery which will reduce the time complexity that takes on matching process. Kiruthika *et al*.[17], proposed method using Speeded Up Robust Features(SURF). Its main objective is to detect the multiple copies of the same region and different regions. Detection performance was measured by calculating the number of correctly detected forged images and the number of images that have been erroneously detected as forged, detection result the True Positive Rate (TPR) average 94% but in that paper, there is no estimation of the accuracy rate for applied geometric transformation to evaluate real performances of the methodology. Raj and Joseph[18] proposed a method for copy move forgery using SURF. This paper varies from other key point method. The image is segmented into small non-overlapped patches before matching to improve the efficiency of detected forged regions. The proposed method is applied to images in the MICC-F600 database. This study limitation needs to improve the detection speed.

Hybrid features image forgery detection techniques: Copy-move forgeries are difficult to detect if the duplicated regions affected by different types of attacks[19] as shown in previous two-section block based algorithms are mostly ineffective in some cases such as large amounts of rotation or scaling in these types of attacks. The keypoint-based methods achieve more accurate result. On the other hand, key point based method is not accurate when the duplicated regions are smooth because there are not enough keypoints. The better choice here is block based methods. Thus, we need to combine both techniques. Yang *et al*.[20] proposed a method based on hybrid features by combining A robust interest point detector KAZE and SIFT to extract more feature points with different types of attacks like rotation, scaling, JPEG compression and adding noise. Mohamadian *et al*.[14] also proposed a hybrid feature using SIFT feature and Zernike moments composing these two method to increase the precision and robustness.

CONCLUSION

This survey presents copy-move image forgery detection methods which are classified into two main categories that are block based and key-point based. The key-point based methods can be very efficiently executed. Its main advantage is low computational complexity, combined with good performance especially in case of geometric transformation like rotation and scaling. Key-point-based methods are sensitive to low-contrast regions and repetitive image content. Here, block-based methods can clearly improve the detection results. To achieve more robust methods against all types of attacks, it is recommended to use hybrid techniques which combine more than one method. It is recommended to use a moment-based technique from the block-based methods integrated with a key-point technique. The main reason behind this is that the moment-based techniques also have the benefit of low computation complexity and give good accuracy with most of attacks types, especially, in intensity level of the images. So, this merging will improve a lot the accuracy of forgery detection affected with different attacks types and keep the aspect of low computational complexity and calculation time which is also a very important factor when comparing the different techniques. Finally, the study shows that there is a clear lack in the available data sets that are used to evaluate the detection algorithm for copy-move forgery in addition to the trivial forgery performed for testing purposes. So, it is recommended to develop more complicated data sets with some sophisticated transformations to match the real case problems.

REFERENCES

01. Kaur, A. and R. Sharma, 2013. Copy-move forgery detection using DCT and SIFT. Intl. J. Comput. Appl., 70: 30-34.

02. Oommen, R.S., M. Jayamohan and S. Sruthy, 2015. A survey of copy-move forgery detection techniques for digital images. Intl. J. Innovations Eng. Technol., 5: 419-426.
03. Al-Qershi, O.M. and B.E. Khoo, 2013. Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic Sci. Intl., 231: 284-295.
04. Dixit, A. and R.K. Gupta, 2016. Copy-move image forgery detection a review. Intl. J. Image Graphics Signal Process., 8: 29-40.
05. Warif, N.B.A., A.W. Abdul Wahab, M.Y.I. Idris, R. Ramli, R. Salleh, S. Shamshirband and K.K.R. Choo, 2016. Copy-move forgery detection: Survey, challenges and future directions. J. Network Comput. Applic., 75: 259-278.
06. Bhullar, L.K., S. Budhiraja and A. Dhindsa, 2014. DWT and SIFT based passive copy-move forgery detection. Intl. J. Comput. Appl., 95: 14-18.
07. Kumar, S., J. Desai and S. Mukherjee, 2013. A fast DCT based method for copy move forgery detection. Proceedings of the 2013 IEEE 2nd International Conference on Image Information Processing (ICIIP'13), December 9-11, 2013, IEEE, Shimla, India, ISBN:978-1-4673-6099-9, pp: 649-654.
08. Ryu, S.J., M. Kirchner, M.J. Lee and H.K. Lee, 2013. Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE. Trans. Inf. Forensics Secur., 8: 1355-1370.
09. Warbhe, A., R. Dharaskar and V. Thakare, 2015. Block based image forgery detection techniques. Int. J. Eng. Sci. Res. Technol., 4: 289-297.
10. Ting, Z. and W. Rang-Ding, 2009. Copy-move forgery detection based on SVD in digital image. Proceedings of the 2nd International Congress on Image and Signal Processing, October 17-19, 2009, Tianjin, pp: 1-5.
11. Lee, J.C., 2015. Copy-move image forgery detection based on Gabor magnitude. J. Visual Commun. Image Represent., 31: 320-334.
12. Lee, J.C., C.P. Chang and W.K. Chen, 2015. Detection of copy-move image forgery using histogram of orientated gradients. Inf. Sci., 321: 250-262.
13. Warbhe, A.D., R.V. Dharaskar and V.M. Thakare, 2016. A survey on keypoint based copy-paste forgery detection techniques. Procedia Comput. Sci., 78: 61-67.
14. Mohamadian, Z. and A.A. Pouyan, 2013. Detection of duplication forgery in digital images in uniform and non-uniform regions. Proceedings of the UKSim 15th International Conference on Computer Modelling and Simulation (UKSim'13), April 10-12, 2013, IEEE, Cambridge, UK., ISBN: 978-1-4673-6421-8, pp: 455-460.
15. Amerini, I., L. Ballan, R. Caldelli, A.D. Bimbo and G. Serra, 2011. A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE. Trans. Inf. Forensics Secur., 6: 1099-1110.
16. Sudhakar, K., V.M. Sandeep and S. Kulkarni, 2014. Speeding-up SIFT based copy move forgery detection using level set approach. Proceedings of the International Conference on Advances in Electronics, Computers and Communications (ICAECC'174), October 10-11, 2014, IEEE, Bangalore, India, ISBN:978-1-4799-5497-1, pp: 1-6.
17. Kiruthika, K., S.D. Mahalakshmi and K. Vijaylakshmi, 2014. Detecting multiple copies of copy-move forgery based on SURF. Intl. J. Innovative Res. Sci. Eng. Technol., 3: 2276-2281.
18. Raj, R. and N. Joseph, 2016. Keypoint extraction using SURF algorithm for CMFD. Procedia Comput. Sci., 93: 375-381.
19. Christlein, V., C. Riess, J. Jordan, C. Riess and E. Angelopoulou, 2012. An evaluation of popular copy-move forgery detection approaches. IEEE. Trans. Inf. Forensics Secur., 7: 1841-1854.
20. Yang, F., J. Li, W. Lu and J. Weng, 2017. Copy-move forgery detection based on hybrid features. Eng. Appl. Artif. Intell., 59: 73-83.