Open Access
Full Length Article

ORIGINAL ARTICLE

Two Fold Image Forgery Detection System Using Combined Key point based method and Block based method

Fatima Akhtar[1], Huma Qayyum[2]

Department of Software Engineering. UET Taxila, Taxila, Pakistan

ABSTRACT

In this paper to detect image forgery, two standard methods, Key point based method and block based method, are combined to form a two fold method which gives more accuracy. This method first use segmentation method that is used in block based method. Features are extracted on these small patches of segmentation; by means of key points based method. Then these patches are compared with each other and distance is measured between them. If two patches have same distance then a region of image is copied and paste on the same image and the image is forged. This process is done in two segments to ensure good and accurate detection. A good and reliable working of the algorithm is ensured by comparing the proposed algorithm with some state of the art standard public available datasets.

Keywords: Copy Move forgery; Passive forgery technique; key point Detection; segmentation-based CMF

Author`s Contribution
[1,2]Manuscript writing, Data analysis, interpretation, Conception, synthesis, planning of research, Interpretation and discussion, Data Collection

Address of Correspondence
Fatima Akhtar
Fatimaakhtar93@hotmail.com

Article info.
Received: April, 2018
Accepted: Dec 07, 2018
Published: Dec 30, 2018

***Cite this article**: Akhtar F, Qayyum H, Two fold Image Forgery Detection system Using Combined Key point based method and Block based method. J. Inf. commun. technol. robot. appl.2018; 9(2):62-70*

***Funding Source:** Nil*
***Conflict of Interest:** Nil*

INTRODUCTION

In image manipulation techniques copy-move forgery is a most commonly and much used forgery technique. It works by copying some scenes from an image and moves them to a same image or a different image. This destroys the correlation between the main characteristics of the image by duplication of image areas. The techniques to detect image forged region are produced to compete with the cope up with the uprising of multimedia security. These approached as described in 1,2,3 are mainly fall into two types: active and passive-blind approaches. Active methods described in4 can be further divides into data hiding technique or digital signature technique. In data hiding or digital watermark technique at source end a secondary data is or watermark is inserted .This mark is verified at the source side .when image is embedded with this watermark it cannot be separated. Image quality is degraded when watermark is inserted. When features are extracted from image at the source side forgery is digital signature approach .these features further are encoded into the image to form digital signatures.

Shortcoming of this approach is that watermarks must be inserted at the time of recording of image so when image go the transformation their quality is degraded. The second type of forgery is digital passive or blind forgery5,6,7 that works by detecting tempering that although they have no visual clue may change the underlying statistics of an image. There are five categories of image forensics tools 1)statistical variances introduced at pixel level; 2) compression scheme that control the statistical correlations is format-based techniques; 3) artifacts that can be exploited by camera

lens and some high sensors, or some on-chip post processing technique that change them c; 4) errors detected by interaction between x-y-z planes and physical objects, light, and the camera; 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera.

LITERATURE REVIEW

2.1. The Need for Detection of Digital Image Forgeries

When someone intentially manipulate a digital image for the idea of changing semantic meaning of the image it is called digital image forgery. In today's age there are many high technology software's such as Photoshop [10]that make it very easy to create forged images from one or multiple selected images. The authenticity of photographs has a key role in many areas of image forgery which includes forensic investigation, surveillance systems, criminal investigation, journalism, medical imaging, and intelligent systems.

2.2. Related Work

Recently, a lot of work has been done in the field of forgery detection. In this section main frameworks of CMFD [11] are described. Most technique that are used to detect forgery are derived from Block based matching method and key point based method. These techniques are described in detail by [12] in which some are frequency transform[13], texture ,moment invariant and log polar transforms[14].

Block based Matching Method

Weiqi Luo et al. [15]uses a robust algorithm based on the characteristics of shift vectors. The methodology separates the picture into small overlapped pieces and finds the closeness of these overlapped pieces through distinguished copied locals. After that the characteristics vectors of image squares are obtained by applying division process. An approach of lexicographical sorting is applied on the array of these divided squares and similar block pair is obtained from it. However in many cases correct matched blocks is difficult to obtain as not all comparable block pairs are similar that are originating from two copied areas.

Myna et al. in [16] conducted a two phase copy move forgery technique, that uses Discrete Wavelet Transform (DWT) on original image and obtain a reduced dimension representation of exhaustive search for the identical blocks. For each position of block, sliding is done on pixel bases from upper left corner and down to the lower right corner of the block. Log-polar coordinates are calculated for these blocks. Each sliding block corresponds to single position of each row. Match blocks are obtained after lexicographically sorting of these rows. Phase correlation is used to obtain maximum phase correlation value, so that if its value exceeds a preset threshold value the pixels are altered.

Another forgery detection algorithm based on block based algorithms is described in [17, 18]that use a bucket of blocks and after comparison with each other, it divides them into small overlapping blocks. To perform the block comparisons, all blocks are compared with other blocks from the bucket for computing block size and to gain average gray value as the dominant feature. Two blocks overlap if their block size is less than pixel away from another block. If the result of this comparison gives zeros, in the column/row of matrix, then this block is removed and total area is recomputed. Discard all remaining area if minimum area is greater than the total area otherwise duplicated region is part of remaining blocks .The major drawback of this approach is the lengthy computation occur when comparing an entire block with another entire block. As a result of this lengthy computation the system becomes unnecessary very slow.

A system based on block based method is suggested in[19], in which overlapping blocks features are extracted by Local Binary Pattern Histogram Fourier . Euclidean similarity measure is used to decide whether images are forged or not. In [20] researcher analyses segmentation based forgery method that segments the image into overlapping patches of irregular shape .This algorithm is good as it overcome the missing block problem by multi scale segmentation. But this algorithm is very slow due to matching overlapping blocks. YuSun et al [21] divide the image into texture region and smooth regions instead of overlapping all blocks. However when the system deals with very smooth blocks it did not differentiate the regions which gives false results.

In paper [22, 23]forged regions are detected by using DCT-based method. Fixed-size overlapping blocks are obtained by segmenting the image, on bases of DCT. Thus sorted list of forged image regions are obtained that consist of lexicographically sorted feature vectors. Mehdi

Ghorbani et al. [24]also used DCT (Discrete Cosine Transform) technique with QCD (Quantization Coefficient Decomposition) method. Here the length of image vector is reduced in lexicographically sorted form. Another DCT coefficient analysis method is proposed by Zhouchen et al. [25]that inspect the two fold quantization consequences for JPEG pictures. Fraud detection in JPEG picture is done in three stages. In first step decompression of picture in lattice squares form is done. The new content is replaced by a curved line region. Tempered image is recompressed by which we obtain unchanged doubly compressed image as well as singly compressed image.

Inconsistencies of Local Noise Level

One such method is Local noise level inconsistencies that is used by [26] Babak et al. It detects forged regions by measuring inconsistencies of local noise level of image. The non-overlapping block of image which has the highest resolution is tiled by high pass diagonal wavelet coefficients. These coefficients then estimate the inconsistencies of local noise level. The standard deviation of noise is estimated by wavelet-based technique. Gradient-based methods are used in wavelet decomposition, which provide gradient amplitudes for noise estimation.

In this paper[27],a method based on resampling and confidence score is combined to demonstrate an effecting image tempering method. It take Methods like classic up sampling, rotations, shearing and down sampling method are combined with a JPEG compression detector to form a heat map that show inconsistencies in the image.

Key point based Detection Method

Hailing et al. [28]and Irene et al. [29] proposed SIFT based forgery detection method that is able to estimate the geometrical transformation of image. In order to differentiate the cloned areas of image clusters, a robust feature matching procedure is adopted. Another SIFT detection based algorithm is proposed by Pan et al [30]that uses lighting geometry [31]for capturing the statistical correlation of interpolation[32], and for the location of duplication. This approach however failed to give good results and therefore becomes ineffective in practical scenarios. One simple approach that is also used for detecting image forgery is to locate duplicated regions in an image. In image auto-correlation function it identify off-origin peaks of the image by using fast Fourier transform[33].

Another copy move detection method described in [34]that use a combination of Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT) to sustained various pre-processing attacks. Initially DyWT is applied on the image that divides the image into four parts i.e. LL, LH, HL, and HH. After that SIFT is applied on LL part that contain most of the information of image. Key features are extracted to find a descriptor vector. These descriptor vectors are then used to find copy move forgery in image.

A compound based statistical features extraction approach is adopted by Fei et al [6]or the detection of image copy-move forgery. At first a colored image is transformed into a grayscale image. De-noising filter is used to extract the sensor pattern noise features of image. This filter is then passes through more patterns to obtain variance of the pattern noise, the ratio of de-noised image to signal noise, the information entropy and the average energy gradient of the original grayscale image. Number of overlapping sliding window operations is performed on image that divides the image into different sub-blocks. Thus tampered areas of image are detected by finding correlation of features, obtained from sub blocks and the whole image. However, the posed plan is only viable in case of image copy move forensics that exists between various images. The greatest downside of the plan is that it does not have self-adaptively which can conform the threshold.

METHODOLOGY

For the implementation of our work, we have merged two basic methods of copy move forgery detection. These methods includes block based method that divides the image into same size of overlapping blocks for feature extraction and second one is key point based method which extracts features from whole complete image at a time. The goal behind this hybrid approach is to gain significantly better results. At initial step the image is segmented through block based method and on each block we further imply key point based method to extract features from each segment. The extracted features are then used to find Forgery regions. The implementation details are further discussed in following sections.

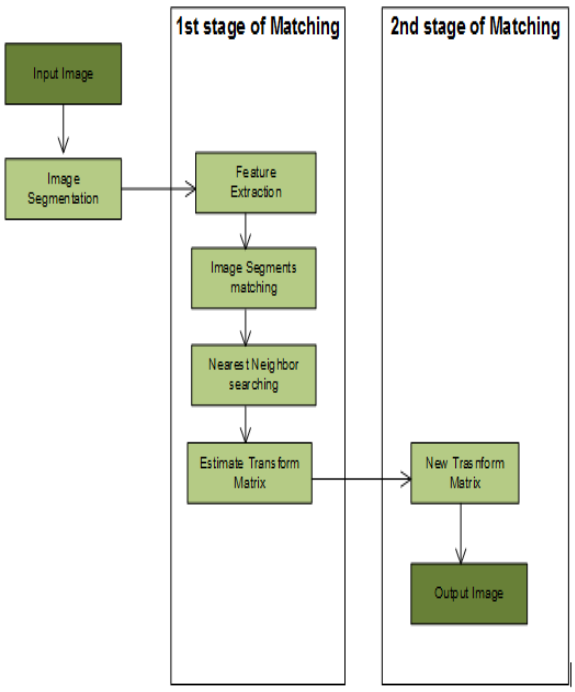

Figure 1. Proposed Methodolgy

Image that have forged regions have to undergo extensive search for the detection of local patterns or patch matches. One preliminary idea that help to separate CMF region is to slice the image into semantically independent patches. These patches can be used like matching blocks for the comparison of forged regions. There is an assumption that patch size should be selected in such a way that its size should be smaller than the size of minimum patch of tampering. When tampering is done in the same image there is chance that the copied region and pasted region form a correlation between them. This correlation can be detected by extensive search on these patches. For our implementation work, a self-collected dataset images both from copying regions and target region are taken. For each image, forgery detection is made after segmenting the image into small semantically independent [35]patches. For the purpose of segmentation default settings of VI-feat [24] known as vl-Slic is used to slice the image into 100 or more patches. To get useful information from these patches, CMF region is calculated which can be found in one or more than one patches. Thus each patch information given a chance for finding the tampering regions.

3.1. Feature Extraction

This implementation uses dense SIFT (DSIFT) detector to extract key points from the image. Extracted key points are then used to create feature descriptor. When the key points were extracted, they are compared with each other to find out the similar key points (the kd-tree[36] algorithm is used for the matching stage[37]).

3.2. Key point Detection

Dense SIFT (DSIFT) give some assumptions based on SIFT algorithm that helps us to achieve better and more results in less time. a) The location of key point is measured from a predefined location, not from the gradient feature of the pixel. (b) Scales of each key points are predefined and same. (c)Zero is the default orientation of each key point.

Difference of Gaussian (DoG)[38] pyramid is used to achieve key point detection .This is worth mentioning that retinal center-surround ganglion cells relates to DoG. Corners, Blobs and edges are very responsive to DoG but edges are removed from DoG as they are not localizable. Edges are removed by taking analysis of local gradients by Harris corner [39]leaving only blobs and corners. A maxima point is picked within a sub octave pyramid by taking 3x3x3 volume of the pyramid. This ensures scale invariant features. Points around key points orientations are find within image gradient field to introduce rotation invariance. All resulting preparation of the image happens in the separate frames of reference of each given key point.

In this way it makes the algorithm invariant to scale and rotation, of images or objects. VI-Feat [40] software has very good default setting of detection and description namely DSIFT [41]that is why we use these setting without changing them .This algorithm has good performance about selected forged regions .Thus it makes sure that the key points give good performance. For this we set the key point extraction to be 2000.

3.3. Segments Matching

For segments matching we have to consider all segments. We have to calculate the difference between them by measuring the L-2 norm of distance (Euclidean) between them[41]. This has to be done to extract forged segments of image from the rest. The segments are compared with each other and the rest remaining segments. Consider the algorithm takes a segment and its key points. As we have also the distance between each key point we search for a similar key point with the

same distance between them. In simple words we search nearest neighbor of each key point located on other segments. If there are some key point present we take these into consideration. Then we set a value of matched point. As we have set to be k=10 in this algorithm. Does not bother to take all key point but only those having difference smaller than the threshold (0.04).As source and target regions have fair amount of matched key points located between them .Consider these points A and B points . These points are called CMF located area and the forged area of the image .So to find matched key points threshold ϵ is defined. As in this case the threshold ϵ is set at value 10 times the average number of key points in each segments

$$\varepsilon = 10\frac{Keypo\,int\,s}{Patches} \quad (1)$$

3.4. Nearest Neighbor Search

Best-bin-first algorithm is used in matching feature vectors that are detected from DSIFT key points. If a key point is located at position x then its features f.(A) is matched with B by obtaining their L2 (Euclidean) distance as its feature vector B is the nearest neighbor to A. Usually nearest best match of a key point is obtained from its nearby area, as natural images are smooth. So to obtain nearest neighbor that are not from the same area, search is performed outside 11 x 11 pixel window of key point. However we just keep those key points with distinct likenesses. In particular, we require that for whatever other component vector C other than A and B the separation amongst A and B must be little. A preset threshold ϵ is introduced that control the distinctiveness of the matching. To give a good tradeoff between matching accuracy and ratio of outliers the default value of threshold is set to be ϵ = 0.04.After the stage of Nearest neighbor the majority of patches are eliminated from the estimation of transform matrix. This can be done with the help of threshold. As vl-Feat software is used to decrease the computational complexity of nearest neighbor. This is done by construction of a K-d tree in vl-Feat software that lower its complexity from O (n2) to O (nlogn).

3.5. Affine Transform Estimation

When there are some forged segments present in in an image we have to estimate the relation between copy region and target region. This is done by estimating a transform matrix between these two regions such that

$$A = XB \quad (2)$$

Where A and B are the coordinates of the source and target regions .As most forgers don't do much post processing on copied regions but do a little on target regions to hide their work. Which employs that error of key point extraction is possible in target region. Transform estimation only take very few key point (5) into consideration to enhance the detection accuracy. If CMF region is very small say 32 × 32it becomes very difficult to precisely pin point forged regions. Another stage of matching is needed to have a accurate estimation of the matching process

3.6. New Correspondences

As we have computed some new pixels A and B in the target and source region .It is done by using dense SIFT which makes very easy to extract dense key points .These key points have same size and exact orientation .The distance between A and B are calculated by L2 – norm .So in first stage we have find the pixel A of source and pixel B of target nearby. They have really small dense difference between them

3.7. Re-estimation of the Transform Matrix

In the early stage the algorithm evaluate the detected key points in the source segment and target segment by using the transform matrix. To find more refined key points another estimation is to be done. This is done to see all the matched points in the matched segment X. A new relationship is developed between these regions

$$f(A) = f(X^{-1}B) \quad (3)$$

In this relation the f (A) is used to distinguish the function and pixels of the image. To achieve some advance image features like image intensity or to employ robustness to the image descriptors dense SIFT descriptors are used. To detect the likelihood a pixel at source point A is located at the CMF region, a variable Q is introduces as a random variable .This random variable gives us the idea how much is the likelihood of a pixel at that point.(Q=1 or Q=0) which gives us the result of probability that is

$$P\left(A \mid Q=1, X\right) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(f(A)-f(X^{-1}B))^T (f(A)-f(X^{-1}B))}{2\sigma^2}} \quad (4)$$

This equation gives very good result after some

varied experiments. It works on a condition that works on the idea that distinction between two matched segments takes Gaussian distribution (mean = 0 and difference of 2)

EXPERIMENTAL RESULTS

To propose and test the image forgery detection algorithm Matlab (R2015b) in 64-bit system is used. The system is integrated with OpenCV. Test Image Databases presents three public available image databases and 1 dataset created by us is used to check the validity and working of our proposed copy move algorithm. Two of the first datasets are constructed by Amerini et al [42]and the 3rd image database consist of 200 images that consist of 100 original and 100 tempered images. It is noted that algorithm work best on originals dimensions. If the tempered areas is resized in key point based scheme there is very much difficulty of extracting key points from the forged regions. The images in the datasets are segmented by using function of vlFeat software [using a vlFeat function vl-slic, which gives us most efficient result]. Vl-slic function has two parameters that should be adaptive to the image size. Regulator is 0.8 that regulate the patches and region size that is related to segmentation patches. Following the approach we proposed, Performance of the CMFD scheme is also tested by detection error at image level. Accuracy, specificity and sensitivity is used to evaluate the performance of our proposed system. The detection error at the image level is measured by,

- T P (True Positive): When copied images are copied images
- TN (True Negative): when the images are genuine and algorithm is detecting correctly.
- FP (False Positive): when algorithm perceive authentic image to be a copied image.
- FN (False Negative): when algorithm ignores the copied region and take it as authentic image

Mathematically,

$$\text{SENSITIVITY} = \frac{TP}{TP+FN} * 100$$

$$\text{ACCURACY} = \frac{TP+TN}{TP+TN+FN+FP} * 100$$

$$\text{SPECIFICITY} = \frac{TN}{FP+TN} * 100$$

Image level detection is used to evaluate the performance of CMFD algorithm. If copy move attack is on more than 50% of block the block is considered forged. The performance of our algorithm is compared with two other algorithm that are widely used described in [43] .Another algorithm that uses Sift with J-linkage [44] is also compared with this algorithm. We use SIFT-based forensic method and Sift with J-linkage method for comparison with the forgery algorithm.

4.1. Test Results on Image Databases

Setting the proper value of threshold ϵ give a vital role in making the value of false positive rate high. ϵ is adjusted well to make a tradeoff between FP and FN. It is seen by running the algorithm that false negative FN rate is increased to 0.33 if the FN rate becomes less than 0.15.To satisfy different requirements of algorithm ϵ is adjusted well. However this method does not impose any change on detection algorithm thus ϵ is set to 10(ϵ = 10).We examine the ability of algorithm on MICC-F200 which consist of 220 images; in which half images that are 110 are tampered and half 110 are originals. The results are shown by a table. The values are given in Table I

Table I. Results of Proposed Algorithm

Table Head	Result of CMF detection algorithms				
	Dataset	FN%	FP%	TP%	TN%
	MICC-F200	3.6	5.4	94.5	96.3
	MICC-F600	11.9	13.8	88.13	86.14
	Proposed dataset	11.1	0	88.9	100

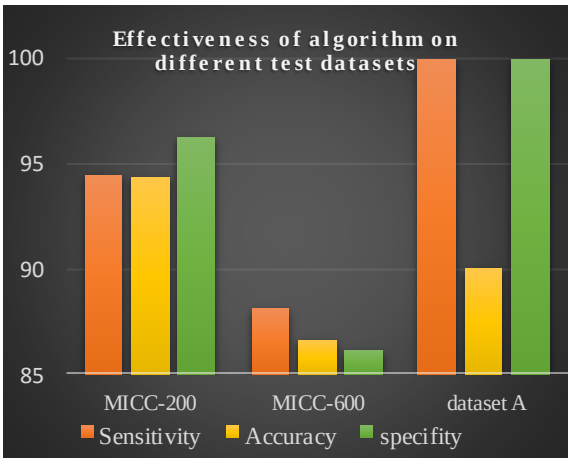

Figure 2. Result on different datasets

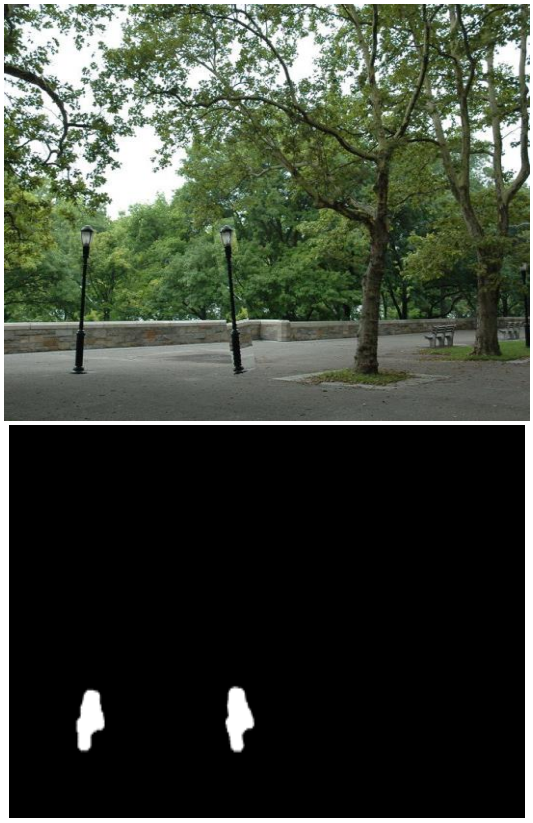

Figure 3. Sample image of lamp from MICC-600

Figure 5.Cloned face of boy from dataset A

Figure 4. Sample images from Micc-200

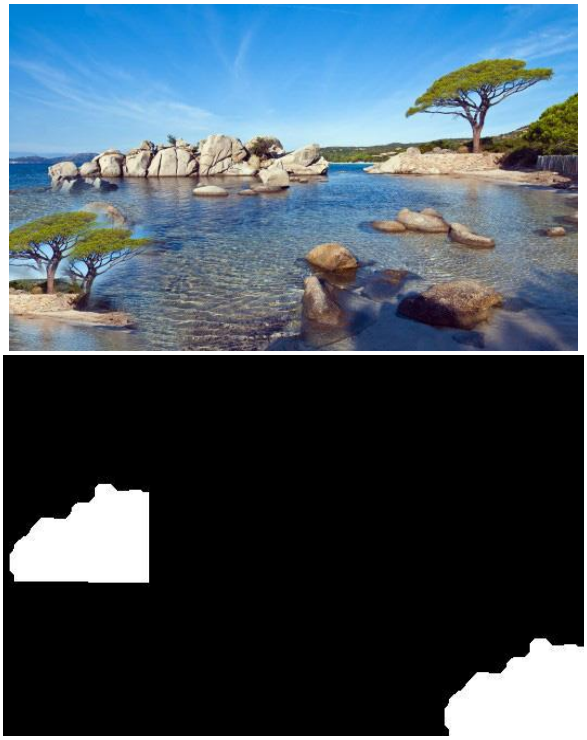

Figure 6. Sample images from proposed dataset (dataset A)

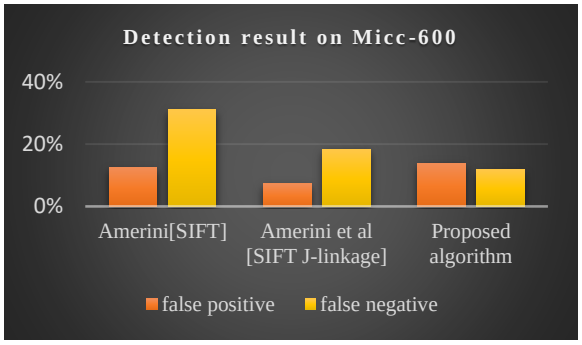

Figure 7. Comparison with different algorithm

The proposed CMFD scheme is also computed on standard benchmark dataset .It contain 600 images in which 160 are changed images and 440 are originals. The rate of error is given in table I. It is clear that the proposed algorithm is good with detecting forgery. It has high rate of false positive but yet it gives lowest false negative rate. Which gives us the conclusion that the algorithm which we have proposed gives good result in detection of tempered regions. The proposed CMFD is also evaluated on a dataset made by us for convenience lets called it dataset A. It consist of 50 images in which 45 are forged images and 5 are original images. No type of rotation or blurring are applies on it. We see in table 1 that it gives us best result when no processing is done on images.

Limitations and Conclusion

This research present a hybrid two fold forgery detection algorithm based on key point based method and block based approach. As both techniques have some good aspects as well as drawbacks we suggest a more accurate approach. The features are extracted and forged regions are detected from the image by means of key point based methods. We cannot classify this method in key point based one .It is viewed as a combination of both methods, we conclude our work as follows.

CMF region contain certain amount of information .Thus the images are segmented into semantically independent segments. A major concern of this algorithm is that if a segment of images obtain by segmenting the image is very small, it is difficult to extract forged region from it. CMF region will be smaller than patch and it works by matching the distance of patches. If we set patch level high then many forged segments will go unnoticed due to high certainty. A tradeoff is to set carefully to detect forged patches in images.

The algorithm consist of two stages. Accurate region detection can be done by re estimation of transform matrix.

As earlier algorithm has no segmentation step one may concern that it has more computational complexity from regular key point based methods. But it gives more accurate results, and the segmentation complexity can be reduced by using some fast Quick shift and kernel methods or Slice techniques. The forgery detection method play a key role in many areas of images which includes forensic investigation, surveillance systems, criminal investigation, journalism, medical imaging, and intelligent systems

REFERENCES

1. N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband, et al., "Copy-move forgery detection: Survey, challenges and future directions," Journal of Network and Computer Applications, vol. 75, pp. 259-278, 2016.
2. A. Shahroudnejad and M. Rahmati, "Copy-move forgery detection in digital images using affine-SIFT," Proceedings - 2016 2nd International Conference of Signal Processing and Intelligent Systems, ICSPIS 2016, 2017.
3. S. Bayram, H. Taha Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1053-1056, 2009.
4. 4B. L. Shivakumar and S. S. Baboo, "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods," Global Journal of Computer Science and Technology, vol. 10, pp. 61-65, 2011.
5. H. Farid, "Image Forgery Detection A survey," Ieee Signal Processing Magazine, vol. 26, pp. 16-25, 2009.
6. F. Peng, Y. Y. Nie, and M. Long, "A complete passive blind image copy-move forensics scheme based on compound statistics features," Forensic Science International, vol. 212, pp. e21-e25, 2011.
7. B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Signal Processing: Image Communication, vol. 25, pp. 389-399, 2010.
8. S. Panda and M. Mishra, "Passive Techniques of Digital Image Forgery Detection : Developments and Passive Techniques of Digital Image Forgery Detection : Developments and Challenges," 2018.
9. S. V. Sathyanarayana, "Digital image forgery detection techniques : a survey Digital image forgery detection techniques : a survey," 2017.
10. G. F. Leanne Schinkel "Digital Photo Editing," ed.
11. Z. Zhang, C. Wang, and X. Zhou, "A Survey on Passive Image Copy-Move Forgery Detection," vol. 14, pp. 6-31, 2018.

12. S. Mushtaq, "Image Copy Move Forgery Detection : A Review Image Copy Move Forgery Detection : A Review," pp. 10-22, 2018.
13. C. Reads, "Chapter 2 Fourier Analysis of Signals," 2016.
14. R. Dixit, "Copy – move forgery detection utilizing Fourier – Mellin transform log-polar features Rahul Dixit," 2018.
15. L. Weiqi, H. Jiwu, and Q. Guoping, "Robust detection of region-duplication forgery in digital image," Proceedings - International Conference on Pattern Recognition, vol. 4, pp. 746-749, 2006.
16. A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, "Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping," International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), pp. 371-377, 2007.
17. A. Langille and M. Gong, "An efficient match-based duplication detection algorithm," Third Canadian Conference on Computer and Robot Vision, CRV 2006, vol. 2006, pp. 1-8, 2006.
18. G. Lynch, F. Y. Shih, and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Information Sciences, vol. 239, pp. 253-265, 2013.
19. B. Soni, P. K. Das, and D. M. Thounaojam, "Dual System for Copy-move Forgery Detection using Block-based LBP-HF and FWHT Features," 2018.
20. M. Ikhlayel, M. Hariadi, and K. E. Pumama, "A Study of Copy-Move Forgery Detection Scheme Based on Segmentation," vol. 18, pp. 27-32, 2018.
21. Y. Sun, R. Ni, and Y. Zhao, "Nonoverlapping Blocks Based Copy-Move Forgery Detection," vol. 2018, 2018.
22. Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206, pp. 178-184, 2011.
23. J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copy-move forgery in digital images," 2008 11th IEEE Singapore International Conference on Communication Systems, ICCS 2008, pp. 362-366, 2008.
24. M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) Based Copy-move Image Forgery Detection," 2011.
25. Z. Lin, J. He, X. Tang, and C. K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," Pattern Recognition, vol. 42, pp. 2492-2501, 2009.
26. B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," Image and Vision Computing, vol. 27, pp. 1497-1503, 2009.
27. T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, and B. S. Manjunath, "Boosting Image Forgery Detection using Resampling Features and Copy-move Analysis," pp. 1-7, 2018.
28. H. Hailing, G. Weiqiang, and Z. Yu, "Detection of copy-move forgery in digital images using sift algorithm," Proceedings - 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA 2008, vol. 2, pp. 272-276, 2008.
29. I. Amerini, L. Ballan, S. Member, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," vol. 6, pp. 1-12, 2011.
30. X. P. X. Pan and S. L. S. Lyu, "Region Duplication Detection Using Image Feature Matching," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 857-867, 2010.
31. M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Transactions on Information Forensics and Security, vol. 2, pp. 450-461, 2007.
32. A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling Resampling Detecting resampling Experiment results," vol. 53, pp. 758-767, 2005.
33. A. Rauf, M. A. Pasha, and S. Masud, "A Novel Split Radix Fast Fourier Transform Design for an Adaptive and Scalable Implementation," pp. 116-121, 2016.
34. M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," International Conference on Intelligent Systems Design and Applications, ISDA, pp. 188-193, 2014.
35. X. Liu, Z. Deng, and Y. Yang, "Recent progress in semantic image segmentation," Artificial Intelligence Review, 2018.
36. R. Panigrahy, "An improved algorithm finding nearest neighbor using Kd-trees," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 4957 LNCS, pp. 387-398, 2008.
37. S. Zellmann and U. Lang, "Rapid k-d Tree Construction for Sparse Volume Data Rapid k -d Tree Construction for Sparse Volume Data," vol. D, 2018.
38. D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," vol. 60, pp. 91-110, 2004.
39. C. Harris and M. Stephens, "A Combined Corner and Edge Detector," Procedings of the Alvey Vision Conference 1988, pp. 23.1-23.6, 1988.
40. A. Khayeat, A. Retha, H. Khayeat, X. Sun, and P. L. Rosin, "Improved DSIFT Descriptor Based Copy- Rotate-Move Forgery Detection," 2015.
41. D. Eklund, "The Numerical Algebraic Geometry Of Bottlenecks," Arxiv, 26 April 2018.
42. MICC-dataset. Available: http://www.lambertoballan.net/research/image-forensics/
43. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, pp. 1099-1110, 2011.
44. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," Signal Processing: Image Communication, vol. 28, pp. 659-669, 2013.
45.