JNNCE Journal of Engineering & Management – A Peer Reviewed Bi-annual Journal
Available online @ https://jjem.jnnce.ac.in
ISSN: 2582-0079 (O)
Indexed in International Scientific Indexing (ISI)
Impact Factor Value: 1.025 for 2018-19
Volume: 3, Number: 1
January – June 2019

Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching

H R Arpita
M.Tech Student
DECS
JNNCE, Shimoga
arpitahr300@gmail.com

Shwetha B
Assistant Professor
Dept. of ECE
JNNCE, Shimoga
shwethab@jnnce.ac.in

Dr. S V Sathyanarayana
Professor
Dept. of ECE
JNNCE, Shimoga
svs@jnnce.ac.in

ABSTRACT-From the early days, images are generally accepted as a proof of occurrence of the past events. Digital image is a part of the real world which is generated after many processes of image generation. The availability of low cost hardware and software tools makes easy to create and manipulate digital images with no traces. This has led to the situation where one can no longer take the integrity and authenticity of the digital images for granted. So it is important to have an image forgery detection tools to know whether the digital image is authentic or not. In this regard, adaptive oversegmentation and feature point matching is used to detect copy move forgery. First, adaptive oversegmentation algorithm segments the source image into nonoverlapping and irregular blocks. Then, block feature extraction algorithm extracts the feature points from each image block as block features using SIFT(Scale Invariant Feature Transform) and SURF (Speed Up Robust Features) methods and find the matched feature points by matching the feature points with one another by using block feature matching algorithm. After that, forgery region extraction algorithm is used, which replaces the feature points with small superpixels and merges the neighboring blocks which is having similar local color features to generate the merged regions. Lastly, morphological operation is applied to generate the forged regions. Based on precision, recall, F1measure and accuracy parameters obtained from different detection methods, the comparative analysis of copy-move forgery detection method is performed.

Keywords- Copy-Move Forgery Detection, Adaptive Oversegmentation, SIFT, SURF, Block Feature Matching, Local Color Feature, Forgery Region Extraction.

I.INTRODUCTION

Recent days, images are widely used in communication media with the latest tools. In ancient days, it was very hard to change the image contents. In today's world, the manipulation of the images can be easily done. One of the image manipulation methods is cloning where image portion is duplicated on the host image. Hence, authenticity of the images is not permitted. As day passes, image editing software tools have been increased which helps to forge the images. So, digital image forensics answers the issue of authenticity. The authenticity verification of image is required in various fields such as defense, court etc.

To authenticate the content of image, digital watermarking was proposed. The limitation of this approach is that watermark has to be embedded at the time of recording which limits the use of this approach to specially equipped digital cameras. So the research community has found an alternative way of authenticating the images and named it as digital image forensics.

Forgery detection technique is one of the authentication methods, which assumes that the original image has some inherent patterns, which are introduced by the various imaging devices or processing. These patterns are always consistent in the original image and altered after some forgery operations. Cloning (copy-move) is one of the image manipulations technique in which, part of the image is copied on the same image. In this background, exploration is going on and written works are disclosed which are mainly focus on detection of image duplication. With this view, this paper is intended in the study and implementation of detection of copy-move forged images which are one of the most commonly observed forgery. To make forgeries, some image processing methods and geometrical transformations are performed. The color features and other properties of forged portion are similar to the original portion. To detect cloning, block based and feature point based methods are used.

The remainder of this paper is organized as follows. Section II reviews the related literatures on block based and feature point based methods. Section III deals with the methodology of the work in which detailed explanation of implementation of adaptive oversegmentation and feature point matching is discussed. In section IV, comparative analysis of forgery detection methods are listed.

II. BACKGROUND WORK

Image forensics field answers the issue of authenticity in digital images. Hanyfarid briefly explained about image forensic field and tools used in image forensics. Classification of tools can be done in five different categories: format based, pixel based, physical based, geometric based and camera based methods [1]. In this paper, cloning based image forensic detection is dealt and detection algorithms make use of both block based and feature point based method. Hence following section reviews literatures on block and feature point based methods.

The existing block based forgery detection methods divide the input images into overlapping and regular image blocks. Then, the tampered region can be obtained by matching blocks of image pixels or transform coefficient.The authors in [2] used DCT technique. Here, Qfactor is calculated to find quantization steps required for the DCT coefficients. Larger Q-factor gives better matching results but smaller values results in erroneous matches. DCT and quantized coefficients are calculated for each image blocks. After quantization, coefficients are accumulated in the matrix as one row. Coefficients of DCT are arranged lexicographically and identical blocks withsame spatial offset are used to detect tampered regions. The authors in [3] used PCA to get a diminished image block representation. This technique locates the forged regions effectively. PCA can detect the forgeries even under small changes in the image content. By sorting PCA coefficients of each image blocks, tampered regions can be detected. The results from PCA basis gives better discriminating features than DCT method. The authors in [4] used color features from each image blocks to detect the duplication region. Compared to DCT and PCA methods, this technique is less complex and more efficient. In this method, color features are matched to find similar blocks and detect the tampered region. The authors in [5], used DWT and SVD to identify tampered region. In this method, singular value vectors are sorted and used in detection of duplication region. This method reduces complexity and identifies the tampered region effectively. The authors in [6], used SVD for identification of duplication region. In this technique, SVD generates the robust features which are used to identify the duplication region effectively. The authors in [7], used FMT method for feature extraction. This method improved the computational complexity. Instead of lexicographic sorting, this approach used bloom filters. The features extracted from FMT method are robust to geometrical transformations which are efficiently identify the tampered region. Use of bloom filters helps in reduction of time consumption. The authors in [8], used features from circle blocks to detect the tampered region efficiently. Using this technique, the number of blocks can be reduced. The authors in [9], used features which are color dependent to identify tampered regions even geometrical transformations are present. Feature vectors are sorted and matched based on color features which results in reduction of number of comparison blocks and efficient localization of tampered region. The authors in [10], used □ernike moments for identification of tampered region. This algorithm helps in reduction of false positive rate. This algorithm robust to geometrical transformation and effectively localize the tampered region.

In key point-based forgery detection methods, image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions.The authors in [11], used SIFT technique to detect duplication in an images. In this approach, SIFT descriptors are extracted which are robust to geometrical transformations and matched with one another to localize the tampered region. The authors in [12], used robust features to locate the tampered region. Here, SIFT feature points are extracted. This method identifies the transform between original and tampered key points. These are invariant to geometrical transformation and successfully locate the duplication region. The authors in [13], used SURF method to identify the tampered region. This method processes fast compared to the other key point based techniques. SURF descriptors are robust to geometrical transformations. This method used Hessian matrix to identify the SURF descriptors. The authors in [14], used SIFT to find whether cloning is done or not and find the transform which are used between actual and tampered features. Since these features are invariant to geometrical transformations, this method locates the tampered region more accurately and multiple cloning detection also possible. The authors in [15], used invariant features to identify the cloned region. Features are extracted by MPEG-7 image signature tools. These features are robust to transformations which help in identifying the tampered region efficiently. Accuracy of this method is more than 90% and gains high recall rate.

Existing block based forgery detection techniques segments host images into regular and overlapping segments. By matching image segments, tampered portion will be located. In feature point based forgery detection techniques, feature points are extracted from whole image and compared with one another to identify forged region. But block based techniques have three main drawbacks:

Input image is divided into overlapping and regular blocks which increase the computational complexity. The methods fail to define geometrical transformations used in tampered regions. Since segmentation method is regular, recall rate is very poor.

The key point-based forgery detection techniques decrease the complexity and identify the duplication even when transformations exist but it gains low recall rate. To overcome from these problems, cloning detection method using adaptive oversegmentation and feature point matching is used [16]. This technique performs based on both block and feature point based detection methods.

III. METHODOLOGY

Figure 1 shows the framework of cloning detection using adaptive over segmentation and feature point matching.

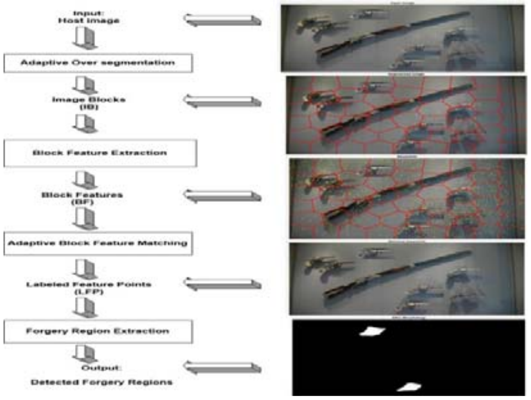

Figure 1: Framework of cloning detection using adaptive over segmentation and feature pointmatching.

In first stage, image is divided into non-overlapping irregular and regular blocks using adaptive oversegmentation algorithm which are called as image blocks (IB). Further, SIFT and SURF is used for extracting feature points from each segment which are referred as block features (BF) [18]. Using feature matching algorithm, BF are compared with other features which helps in determining the Labeled Feature Points (LFP), which are indication to suspected tampered regions. In last stage, detection of tampered region is done by using forgery region extraction algorithm.

The detailed explanation about each algorithm is discussed in the following section.

Adaptive Oversegmentation Algorithm

The existing block based detection techniques, segment the host image into regular and overlapping blocks and they consider the fixed block size. The tampered portions are found by matching similar block coefficients. The identified tampered regions consist of regular block information which fails to detect accurate tampered region since in most of the cases, forged region will be in irregular shape and this results in poor recall rate. The matching operation of overlapping blocks is more complex. To overcome from these problems, adaptive oversegmentation algorithm is used, which divides the host image into non-overlapping irregular and regular blocks which are referred as image blocks. Different segmentation methods are shown in figure 2 where (a) represents overlapping regular block segmentation, (b) represents overlapping circular block segmentation and (c) represents non-overlapping irregular block segmentation using SLIC blocking method.

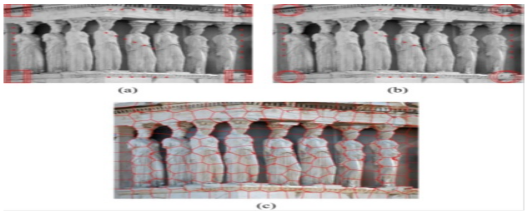

Figure 2: Different segmentation methods

Overlapping regular block segmentation
Overlapping circular block segmentation
Non-overlapping irregular block segmentation

Figure 3 shows flow chart of adaptive overegmentation algorithm. Selection of proper size of the super pixel is very crucial in forgery detection methods. Presently, there is no proper method to calculate the size of super pixels. But based on image properties, proposed method determines the size of super pixels. Size of super pixel is large in case of smoothened image, which generates less blocks and decrease the complexity while performing matching process. In detailed image, the size of super pixels is small to gain accurate results. To estimate the frequency distribution of the input image, DWT is used. When the low frequency energy information is more, the image appears as smoothened image. If the low frequency energy information is less then image will be a detailed image.

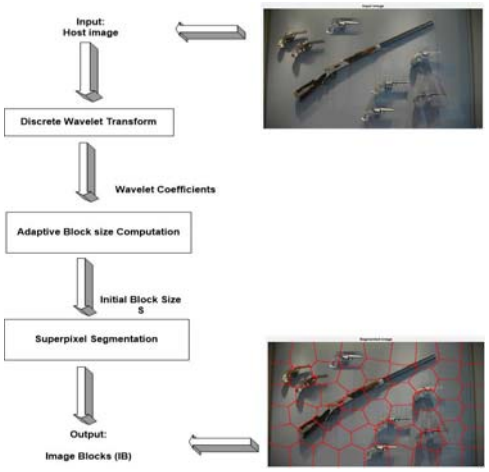

Figure 3: Flowchart of the adaptive oversegmentation algorithm

In this algorithm, DWT uses 'Haar' wavelet of 4 levels. Energy of low frequency, ELF and high frequency, EHF can be computed using equations (1) and (2), respectively. Using these equations, low frequency distribution percentage, PLF can be computed using equation (3) which helps in finding the size S of the superpixels which is given in equation (4) and (5).

$$\mathrm{ELF}=\sum |\mathrm{CA4}| \qquad (1)$$

$$\mathrm{EHF} = \sum \left(\sum |\mathrm{Cdi}| + \sum |\mathrm{Chi}\ | + \sum |\mathrm{Cvi}| \right) \qquad (2)$$

where CA4 is 4th level approximation coefficients of DWT; Cdi, Chi and Cvi are ithdetailed coefficients of DWT, I = 1, 2, …,4.

$$\mathrm{PLF}= \frac{\mathrm{ELF}}{\mathrm{ELF+EHF}} \times 100 \qquad (3)$$

$$\mathrm{S}=\{\sqrt{0.02 \times M \times N}\ \}\ \mathrm{PLF}>50\% \qquad (4)$$

$$\mathrm{S}=\{\sqrt{0.01 \times M \times N}\ \}\ \mathrm{PLF}\leq 50\% \qquad (5)$$

Where Sis the size of the superpixels; $M \times N$ is the size of the host image.

Block Feature Extraction Algorithm

Figure 4 shows flow chart of feature extraction algorithm. Feature extraction is a method used to collect the features from images. This method represents image in the form of features. Major requirements for extracting the feature are reduced dimensionality and redundancy avoidance. Block based techniques use pixels as features. But, these features are variant to geometrical transformations. So, each image blocks are considered for extraction process to collect features and these features must be invariant to transformations. Now a days, SURF and SIFT are commonly used feature extraction techniques in digital field. Features which are extracted from SURF and SIFT are invariant to geometrical transformations such as scaling, rotation, compression and blurring. But the main drawback of using SURF method is, it can label the same key points but fails in locating the tampered regions accurately which results in poor recall rate. In this paper, both SIFT and SURF are chosen for feature extraction from each irregular and regular image blocks.

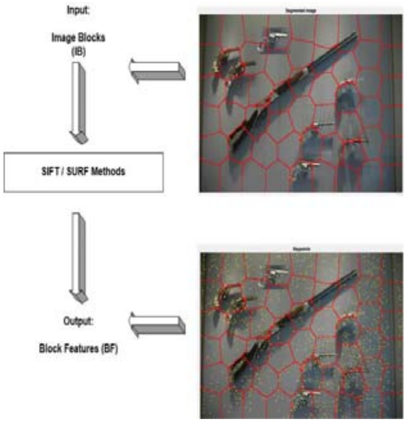

Figure 4: Flowchart of feature extraction algorithm

Block Feature Matching Algorithm

Figure 5 shows flow chart of feature matching algorithm. In block matching operation, block pairs with same shift vector is identified. These identified blocks can be considered as suspected tampered region only when the shift vector is greater than the threshold value. Since each segment contains the number of feature points, feature point matching algorithm is used to find the similar blocks. Correlation coefficient map represents the total number of matched feature points among the pair of blocks. Based on correlation coefficient values, block matching threshold is computed. Matched block pairs are identified based on the calculated threshold value. After locating the matched blocks, matched feature points are labeled within the matched blocks to identify the location of the suspected tampered region. The thresholds values TRp and TRb are considered to avoid false matches.

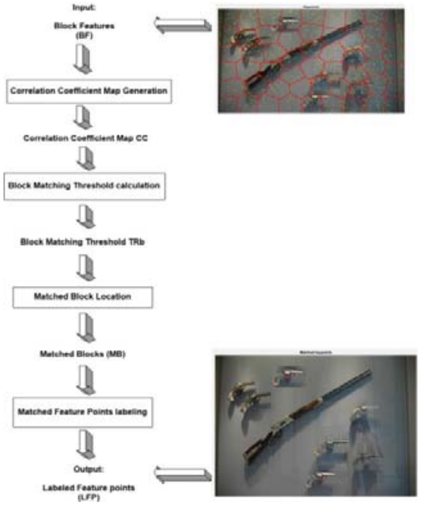
Input:
Block Features (BF)
Correlation Coefficient Map Generation
Correlation Coefficient Map CC
Block Matching Threshold calculation
Block Matching Threshold TRb
Matched Block Location
Matched Blocks (MB)
Matched Feature Points labeling
Output:
Labeled Feature points (LFP)

Figure 5: Flowchart of feature matching algorithm

The detailed steps are explained as follows:
Algorithm:
Input: Block Features (BF)
Output: Labeled Feature Points (LFP)
STEP-1: Load the block features.
Assuming that block features can be represented as BF= (BF1, BF2.........BFn), where n refers total number of image blocks. Correlation coefficients, CC of the image blocks are computed. CC represents number of matched feature points between the pair of blocks. If adaptive oversegmentation algorithm results with N blocks, then N(N-1)/2 CC can be formed which are used to generate CC map. The two feature points said to be matched only when their □ernike□n distance is greater than feature point matching threshold TRp. This can also be interpreted as the feature point fa(xa, ya) is matched to the feature point fb(xb, yb) only if the condition in (6) is satisfied.

$$D(fa ,fb) \times TRp \le d(fa ,fi) \quad (6)$$

where d(fa ,fb) is the □ernike□n distance between the feature points fa and fb, d(fa ,fi) indicates the □ernike□n distances between the key points fa and other key points in block pair. I indicates the ith feature point.

If the value of TRp is too large, then error probability is very high. So, in the experiments TRp = 2 is chosen to gain better matching accuracy and reduced error probability.

STEP-2: Calculate the block matching threshold Trbaccording to the distribution of correlation coefficients.
After generating the CC map, elements present in the map are arranged in ascending order which can be represented as CC_S = {CC1, CC2 …………CCt}, where t ≤N(N-1)/2, which helps in finding TRb. After sorting the CC elements, first and second derivative of CC_S i.e. Δ (CC_S) and Δ2 (CC_S) also mean value of the first derivative vector Δ(CC_ S)1 are computed. To find TRb, select the minimum correlation coefficient from among those whose second derivative is larger than the mean value of the corresponding first derivative vector, i.e., Δ2 (CC S) >Δ(CC_ S)1. The selected CC value is defined as TRb.

STEP-3: Locate the matched blocks MB according to TRb.
With the calculated TRb, if the CC of the block pair is larger than TRb, the corresponding block pair will be determined to be matched blocks.
STEP-4: Label the matched feature points in the MB to indicate the suspected forgery regions.
Forgery Region Extraction Algorith- m
Figure 6 shows flow chart of forgery region extraction algorithm. Labeled feature points

(LFP) are extracted from feature matching algorithm which indicates suspected forged portions. To locate actual tampered portions, this algorithm is used. In this algorithm, LFP are replaced by super pixels to identify suspected regions (SR) which contains labeled super pixels. By measuring the color feature of neighboring super pixels of SR, precision and recall results can be improved. Merging will take place only when color feature of SR is similar to neighboring super pixels of SR which results in generation of merged regions (MR). To identify the forgery regions, close morphological method is performed on MR.

The detailed steps are explained as follows:
Algorithm:
Input: Labeled Feature Points (LFP)
Output: Detected Forgery Regions

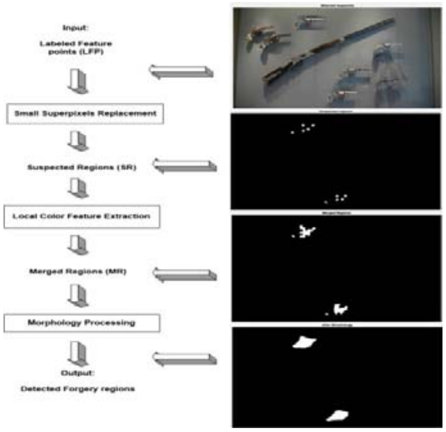

Figure 6: Flowchart of forgery region extraction algorithm

Step 1: Load LFP and perform SLIC method

SLIC method divides the input image into small super pixels. To generate SR, LFP are replaced by corresponding super pixel blocks. Assuming that LFP = {(LP1, LP11), (LP2, LP21)….......................(LPn, LPn1)}, where (Lpi ,Lpi1) indicates matched feature point pair, I indicates ith LFP pair and n is number of feature points in LFP. SR are represented by SR= {(LS1, LS11), (LS2 , LS21)……… {(LSn, LSn1)}. Based on the size of the input image, SLIC calculates super pixel size S to segment the input image into super pixels. S=20 is selected when image is of size approximately 3000×3000 and S=10 is selected when image is of size approximately 1500×1500.

Step-2: Measure the color feature of SR and its neighbor super pixels and merge the neighbor blocks.

The color features of neighboring super pixels to SR which are called as neighbor blocks are measured. When SR and neighbor blocks are having similar color feature, merge the neighbor blocks with SR which generates MR. For each Sri = (Lsi, Lsi1), the neighboring blocks can be represented as Srineighbor= (LsiѲ , LsiѲ1), where Ѳ ={450, 900, 1350, 1800, 2250, 2700, 3150, 3600 }

The color feature of Sri and Srineighbor is measured using equations (7), (8), (9) and (10).

$$\text{Fc\_ Lsi} = \frac{R(\text{Lsi})+G(\text{Lsi})+B(\text{Lsi})}{3} \quad (7)$$

$$\text{Fc\_ Lsi1} = \frac{R(\text{Lsi1})+G(\text{Lsi1})+B(\text{Lsi1})}{3} \quad (8)$$

$$\text{Fc\_ Lsi}\theta = \frac{R(\text{Lsi}\theta)+G(\text{Lsi}\theta)+B(\text{Lsi}\theta)}{3} \quad (9)$$

$$\text{Fc\_ Lsi}\theta 1 = \frac{R(\text{Lsi}\theta 1)+G(\text{Lsi}\theta 1)+B(\text{Lsi}\theta 1)}{3} \quad (10)$$

where R, G and B indicates the RGB components of blocks.

Merging is done only when the conditions defined in (11) and (12) are satisfied.

$$|\text{Fc\_ Lsi- Fc\_ Lsi}\theta| \leq \text{Trsim} \quad (11)$$

$$|\text{Fc\_ Lsi1 - Fc\_ Lsi}\theta 1| \leq \text{Trsim} \quad (12)$$

Where Fc_ Lsi and Fc_ Lsi1 are color features of Sri, Fc_ LsiѲ and Fc_ LsiѲ1are the color features of Srineighbor. Trsimis the threshold which is used to compute the similarity between color features. In the experiments, Trsim= 15 is selected.

Step-3: Apply morphological operation to MR to locate forgery regions.

Close morphological operation uses structuring element as a circle whose radius depends on image size. This operation helps in filling the gaps in the MR and shape of the forged region is kept as it is.

IV. RESULTS

In this section, series of experiments are conducted to check the performance of detection methods. The image dataset MICC-F220 is used to test the methods. This dataset consists of 220 images, in that 110 are tampered and 110 are originals. The image size differs from 722×480 to 800×600 and tampered patch covers 1.2% of whole image. But images in MICC-F220 dataset are limited to rotation and scaling and it doesn't contain source files. To overcome from these issues, benchmark database is used. This dataset contains total 96 images, in that 48 are original and 48 are tampered. This dataset is created by 48 color images which are in PNG format with high resolution.

Precision and recall rate are used for performance evaluation. Precision is defined as the ratio of number of correctly identified forged images to totally identified forged images. Recall is also called as true positive rate which is defined as the ratio of number of correctly identified forged images to total forged images in database. In general, the important measures considered for the calculation of precision and recall rate are [17]:

1. True Positive (TP): represents the number of correctly identified forged images.
2. False Negative (FN): represents number of wrong detection of forged images.
3. False Positive (FP): represents the number of wrong detection of original images.
4. True Negative (TN): represents the number of correctly detected original images.

Precision and Recall can be calculated using equations (13) and (14).

Precision = TP/(TP + FP) (13)

Recall = TP/(TP + FN) (14)

Along with precision and recall, F1 measure is used to measure the forgery detection results which can be computed using equation (15).

F1 = 2×(precision×recall) / (precision + recall) (15)

By considering these parameters, accuracy of the methods can be evaluated using equation (16).

Accuracy = (TP + TN) / (TP + TN + FP + FN) (16)

Tables 1 and 2 show the forgery detection results of different methods under cloning. Table 1 shows the forgery detection results for MICC-F220 dataset. It is shown that SIFT with irregular blocking method achieved precision=81.4%, recall=73.33%, F1=77.15% and accuracy=74%, which is much better than the other detection methods. Table 2 shows the detection of forgery results for benchmark database. It can be observed that SIFT with irregular block segmentation achieved precision=100%,recall=93.75%,F1=96.7% and accuracy= 96.87%. It is observed that SIFT with irregular blocking method gives better results than other duplication detection methods like SIFT with regular blocking, SURF with irregular blocking and SURF with regular blocking.

Table 1: Comparison of detection methods using MICC-F220 dataset

Methods (Extraction/ Segmentation)	Precision (%)	Recall (%)	F1 (%)	Accu r-acy (%)
SIFT / irregular	81.4	73.33	77.15	74
SIFT / regular	83.33	66.66	74.06	72
SURF / irregular	75	20	31.75	48
SURF / regular	80	13.33	22.85	46

Table 2: Comparison of detection methods using benchmark database

Methods (Extraction/Segmentation)	Precision (%)	Recall (%)	F1 (%)	Accuracy (%)
SIFT /irregular	100	93.75	96.77	96.87
SIFT / regular	97.61	85.41	90.95	91.66
SURF/ irregular	97.05	68.75	80.48	83.33
SURF / regular	96.96	66.66	79	82.29

V. CONCLUSION

Now-a-days, internet and other applications widely uses the digital images. With the advanced tools, duplicating the images without leaving any traces is very easy. This advancement in techniques results in issues related to authenticity of image. The solution for image tampering is evolved by digital forensics. In most of the cases, the portion of the image is duplicated on the same image which is referred as cloning. With this background, this paper focuses on cloning detection using adaptive oversegmentation and feature point matching method. This method uses SLIC method to divide the image into non-overlapping irregular and regular blocks. Selection of initial block size can be done by SLIC method which results in improvement of accuracy and reduction in complexity. Feature points are extracted from each irregular and regular blocks using SIFT and SURF methods. To detect the labeled feature points, feature matching algorithm are used which finds the labeled feature points. Labeled feature points indicate the location of tampered regions. To locate the accurate tampered region, forgery region extraction algorithm is considered which replaces labeled feature points with super pixels. If the color feature of feature block is similar to the neighboring blocks, then blocks are merged to form the merged regions. To identify the accurate tampered portion, close morphological method is used.

In most of the cases, tampered regions are in irregular shape. So, irregular block segmentation gives the better accuracy compared to the regular block segmentation. Compared to SIFT method, SURF method fails to identify the duplication portion in most of the cases. Therefore SIFT method gives better results compared to SURF method. Experimental results shows that the SIFT method with irregular block segmentation achieved much better results compared with the other tampering detection methods such as SIFT with regular block segmentation and SURF with irregular and regular block segmentation. Future work could focus on applying the forgery detection scheme based on adaptive oversegmentation and feature point matching on other types of forgery, such as splicing or other types of media, for example, video and audio.

REFERENCES

[1] H. Farid, “image forgery detection”,IEEE signal processing magazine, 2009.

[2] B. D. S. A. J. Fridrich and A. J. Luk, “Detection of copy-move forgery in digital images,” Digital Forensic Research Workshop, 2003.

[3] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” IEEE Trans.Med. Imag., 2004.

[4] J. H. W. Luo and G. Qiu, “Robust detection of region-duplication forgery in digital image,” 18th International Conference,pp. 746-749, 2006.

[5] D. T. G. Li, Q. Wu and S. Sun, “A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd,” IEEE InternationalConference,pp. 1750-1753, 2007.

[6] X. Kang and S. Wei, “Identifying tampered regions using singular value decomposition in digital image forensics,”

International Conference on, pp. 926-930, 2008.

[7] H. T. S. S. Bayram and N. Memon, "An efficient and robust method for detecting copy-move forgery," IEEE International Conference on, pp. 1053-1056, 2009.

[8] H. L. Y. D. J. Wang, G. Liu and Z. Wang, "Detection of image region duplication forgery using model with circle block," MINES'09 International Conference on, pp. 25-29, 2009.

[9] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling", Speech and Signal Processing, IEEE International Conference on, pp. 1880-1883, 2011.

[10] M. J. L. S. J. Ryu, M. Kirchner and H. K. Lee, "Rotation invariant localization of duplicated image regions based on ernike moments," Ieee Transactions on Information Forensics and Security, vol. 8, pp. 1355-1370, 2013.

[11] W. G. H. Huang and Y. Zhang, "Detection of copy-move forgery in digital images using sift algorithm," PACIIA'08.Pacific-Asia Workshop on, pp. 272-276, 2008.

[12] X. Y. Pan and S. Lyu, "Region duplication detection using image feature matching," Ieee Transactions on Information Forensics and Security, vol. 5, pp. 857-867, 2010.

[13] L. G. X. Bo, W. Junwen and D. Yuewei, "Image copy-move forgery detection based on surf," Multimedia Information Networking and Security (MINES),International Conference on, pp. 889-892, 2010.

[14] R. C. A. D. B. I. Amerini, L. Ballan and G. Serra, "A sift-based forensic method for copy-move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.

[15] P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform-invariant features," Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1018-1028, 2012.

[16] X.-C. Y. C.-M. Pun and X.-L. Bi, "Image forgery detection using adaptive oversegmentation and feature point matching," IEEE Transaction on Information Forensics and Security, 1705-1716, 2015.

[17] Vijayalakshmi V S, "Comparative Study of Splicing Based ImageForensic Detection Using KNN, Fuzzy and SVM Classifiers", Master's thesis, Visvesvaraya Technological University, 2015.

[18] H R Arpita, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching", Master's thesis, Visvesvaraya Technological University, 2019.

***